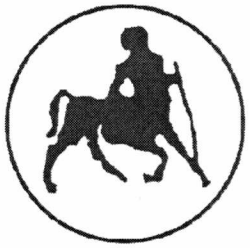


**ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ**
**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**
**ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ**
**ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ**
**«ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ**
**ΒΙΟΙΑΤΡΙΚΗ»**

# Ανθεκτικές αρχιτεκτονικές κυβερνοασφάλειας για εταιρικά περιβάλλοντα μικρο-μεσαίων επιχειρήσεων

# Αναπτυξη συστήματος Κυβερνοασφάλειας για ΜΜΕ βασισμένο σε προγράμματα-εφαρμογές ανοικτού λογισμικού

**Καλότυχου Κωνσταντίνα**
**Σακελλαρης Ιωάννης**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**
**Υπεύθυνος**
**Γεώργιος Σταμούλης**

**Λαμία, 25 Νοεμβρίου έτος 2016**

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79


**ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ**
**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**
**ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ**
**ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ**
**ΚΑΤΕΎΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ**


**«ΥΠΟΛΟΓΙΣΤΙΚΗ ΙΑΤΡΙΚΗ ΚΑΙ ΒΙΟΛΟΓΙΑ»**

**Ή**

**«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»**

**ΡΟΗ ΠΛΗΡΟΦΟΡΙΚΗΣ**

# Ανθεκτικές αρχιτεκτονικές κυβερνοασφάλειας για εταιρικά περιβάλλοντα μικρομεσαίων επιχειρήσεων

# Ανάπτυξη συστήματος Κυβερνοασφάλειας για ΜΜΕ βασισμένο σε προγράμματα-εφαρμογές ανοικτού λογισμικού


**Καλότυχου Κωνσταντίνα**
**Σακελλάρης Ιωάννης**


**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**Επιβλέπων**
**Γεώργιος Σταμούλης**


Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

16149.1

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ ΒΙΒΛΙΟΘΗΚΗ

**Λαμία, 25 Νοεμβρίου έτος 2016**

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο/Η ΔΗΛΩΝ/-ΟΥΣΑ

Ημερομηνία

Υπογραφή

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# Ανθεκτικές αρχιτεκτονικές κυβερνοασφάλειας για εταιρικά περιβάλλοντα μικρομεσαίων επιχειρήσεων

## Ανάπτυξη συστήματος Κυβερνοασφάλειας για ΜΜΕ βασισμένο σε προγράμματα-εφαρμογές ανοικτού λογισμικού

**Καλότυχου Κωνσταντίνα**
**Σακελλάρης Ιωάννης**

**Τριμελής Επιτροπή:**

Δρ. Σταμούλης Γεώργιος

Δρ. Λουκόπουλος Αθανάσιος

Δρ. Αντωνής Κωνσταντίνος

**Επιστημονικός Συμβουλος**

Δρ. Κίκιρας Παναγιώτης

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

**Ευχαριστίες**

Σε αυτό το σημείο θα θέλαμε με τη σειρά μας να πούμε ένα μεγάλο ευχαριστώ σε όλους τους διδάσκοντες του Πανεπιστήμιου Θεσσαλίας του Μεταπτυχιακού Τμήματος Ασφάλειας Υπολογιστικών Συστημάτων για τις πολύτιμες γνώσεις που μας πρόσφεραν και ειδικότερα στον κ. Παναγιώτη Κίκιρα που μας έδωσε το κίνητρο με τις γνώσεις του και τις διαλέξεις του να ασχοληθούμε με την ασφάλεια, μας στήριξε με τη συνεργασία και την καθοδήγηση του για την διεκπεραίωση αυτής της διπλωματικής, και ήταν δίπλα μας σε όλες μας τις δυσκολίες που αντιμετωπίζαμε κατά καιρούς.

Λαμία, Νοέμβριος 2016

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# Περίληψη

Στις μέρες μας η ανάγκη για την ασφάλεια των συστημάτων κρίνεται επιτακτική. Πόσο μάλλον όταν αυτά τα συστήματα αφορούν εταιρικά περιβάλλοντα και διαχειρίζονται πληθώρα λειτουργιών ζωτικής σημασίας, από διατραπεζικές συναλλαγές μέχρι απλά τιμολόγια, πελατολόγια κ.ο.κ. Η αυξανόμενη εξέλιξη του διαδικτύου και γενικότερα των τεχνολογιών επηρεάζει τις μικρομεσαίες επιχειρήσεις που με τη χρήση αυτών, μέσω των ηλεκτρονικών συναλλαγών, δημιουργούνται συνεχώς νέα ζητήματα ασφάλειας και προστασίας της ιδωτικότητας σε όλους τους τομείς. Έτσι η καθημερινότητα έχει εμπλουτιστεί με τη χρήση βασικών ορισμών όπως ιδιωτικότητα, εμπιστευτικότητα, αυθεντικοποίηση και ακεραιότητα.

Σημαντικό μέρος αποτελούν τα ζητήματα ασφαλείας και προστασίας που υφίστανται στα Δίκτυα και στα Πληροφοριακά Συστήματα. Τα θέματα ασφαλείας σε δικτυακές υποδομές και συστήματα, αποτελούν στοιχεία που μπορούν να επηρεάσουν συνολικά την πορεία, την εξέλιξη αλλά και την επιχειρησιακή στρατηγική ενός οργανισμού ή μιας επιχείρησης. Συνεπώς γίνεται αντιληπτό το μέγεθος της σημασίας μιας ασφαλέστερης τεχνολογικής υποδομής σε ένα εταιρικό περιβάλλον.

Το περιβάλλον των Δικτύων και των Πληροφοριακών Συστημάτων αναπτύσσεται και εξελίσσεται συνεχώς με αποτέλεσμα να αυξάνεται η πολυπλοκότητα της διαχείρισης των θεμάτων ασφαλείας. Παύουν πλέον τα κενά ασφαλείας να είναι εμφανή με έναν απλό τυπικό έλεγχο από τον υπεύθυνο ασφαλείας. Οι Απειλές που πλήττουν τις μικρό μεσαίες επιχειρήσεις αλλά και η διαχείριση αυτών, γίνεται ολοένα και πιο πολύπλοκη. Έτσι η ανάγκη για δημιουργία σύστασης ομάδας διαχείρισης περιστατικών σε μικρό μεσαίες επιχειρήσεις που οι συναλλαγές τους είναι κυρίως διαδικτυακές κρίνεται ζωτικής σημασίας.

Οι Απειλές Ασφαλείας, η Διαχείριση περιστατικών παραβίασης σε μικρό μεσαίες επιχειρήσεις, η ανθεκτικότητα επιχειρησιακών αρχιτεκτονικών δικτύου, καθώς και οι βέλτιστες πρακτικές σχετικά με τις ασφαλείς αρχιτεκτονικές δικτύων για μικρό μεσαίες επιχειρήσεις είναι μερικά από τα θέματα που θα αναλυθούν περαιτέρω παρακάτω.

Αυτό που αξίζει να σημειωθεί είναι η προσπάθεια εξοικείωσης του χρήστη με την ανάπτυξη συστήματος κυβερνοασφάλειας για μικρό μεσαίες επιχειρήσεις βασισμένο σε πρόγραμμα-εφαρμογή ανοιχτού λογισμικού. Ειδικότερα στη δεύτερη θεματική ενότητα γίνεται νύξη για το **Security Onion** που αν και είναι λογισμικό ανοιχτού κώδικα, αποτελεί και ένα εργαλείο τόσο για ιδιωτική όσο και για επαγγελματική χρήση.

Στόχος λοιπόν αυτής της Διπλωματικής Εργασίας είναι να δειχθεί τόσο η ανάγκη ύπαρξης της ασφάλειας των δικτύων σε μικρομεσαίες επιχειρήσεις, όσο και η προστασία αυτών. Για το σκοπό αυτό γίνεται η προβολή ενός λογισμικού ανοιχτού κώδικα.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# Abstract

Nowadays, the necessity of ensuring that IT systems are secure is paramount, and more important than ever. This is particularly evident in cases where those systems negotiate critical routines, such as interbank transactions, invoicing, clientelle management etc. The constant evolution of the Internet, along with other forms of technology, result in Small Medium Enterprises(SME) being affected as well; As SME opt to utilise online transactions, new security and broad-based privacy protection issues are emerging. As a result, terms such as privacy, confidentiality, authentification and integrity have now become commonplace.

The safety and security issues of networks and information systems constitute a very significant component. Security in network infrastructures and IT systems are factors that can affect overall progress, development, as well as operational strategy of an organization. Therefore, it is of great importance to create a safer technology infrastructure in any given corporate environment.

Networking and information systems are areas under constant evolution, and as a result, the complexity of managing security issues is increasing. SME are becoming more and more vulnerable to threats and management becomes ever more complex. Thus, the need for a Computer Incident Response Team (CIRT), the role of which is to deal with security issues affecting SME, is essential.

Security threats, incidents of violations of SME's infrastructure, durability operational network architectures and best practices for secure network architectures are some of the topics that will be discussed further below.

The attempt of familiarizing the user with a cyber system for SME development based on an open source software platform is also worth mentioning. The second part of this thesis in particular refers to Security Onion, which, being open source, is a tool for both private and professional use.

The main scope of the thesis is to demonstrate not only the need for security structures in SME, but their protection as well.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# Περιεχόμενα




Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

## Περιεχόμενα εικόνων



Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Συντομογραφίες

MME = Μικρές-Μεσσαίες Επιχειρήσεις

ACL = Access Control List

ADS = Application Database Servers

AFB = Autopsy Forensic Browser

ALF = Application Level Filters

ASC =Activeworx Security Center

BPF = Berkeley Packet Filter

CIDR = Classless Inter Domain Routing

CIF = Collective Intelligence Framework

COTS = Commercial Off The Shelf

DMZ = De Militarized Zone

DNS = Domain Name System

DOS = Denial Of Service

EA = Enterprise Architecture

ELSA = Enterprise Log Search and Archive

FDDM = Firewall Design Decision Making

GUI = Graphical User Interface

HIDS = Host-based Intrusion Detection System

IP = Internet Protocol

ISP = Internet Service Provider

MAC = Machine Address Control

MBSA = Microsoft Baseline Security Analyzer

MITM = Man In The Middle

NAT = Network Address Translation

NFAT = Network Forensic Analysis Tool

NIC = Network Interface Controller

NIDS = Network Interface Cards

NIDS = Network-based Intrusion Detection Systems

NSM = Network Security Monitoring

NTP = Network Time Protocol

OSSEC = Open Source Host-based Intrusion Detection System

PAT = Port Address Translation

PRADS = Passive Real Time Asset Detection System

SABSA = Sherwood Applied Business Architecture

SEC = Simple Event Correlator

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

SID = Security Identifier

SME =Small Medium Enterprise

SMTP =Simple Mail Transfer Protocol

SNMP = Simple Network Management Protocol

SOA = Service Oriented Architecture

Soho = Small Office Home Office

SPAN = Switch Port Analyzer

SSL = Secure Sockets Layer

SSS = Shared Services Subnet

TP = Transfer Protocol

TSK = Sleuth Kit

UTM = Unified Threat Management

VLAN = Virtual Local Area Network

VM = Virtual Machine

VPN = Virtual Private Network

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# Ανθεκτικές αρχιτεκτονικές κυβερνοασφάλειας για εταιρικά περιβάλλοντα μικρο-μεσαίων επιχειρήσεων

## 1. Ασφάλεια πληροφοριών για μικρό-μεσαίες επιχειρήσεις

### 1.1 Εισαγωγή

Οι Μικρό-μεσαίες επιχειρήσεις (ΜΜΕ) είναι η κινητήρια δύναμη της παγκόσμιας οικονομίας, με τη δημιουργία θέσεων απασχόλησης, με τις καινοτομίες καθώς και τον πλούτο τους. Επίσης, είναι ελκυστικό προμηθευτές για μεγαλύτερες επιχειρήσεις, που έχουν χαμηλότερα έξοδα διοικητικής λειτουργίας και ταχύτερες διαδικασίες έγκρισης, να μπορούν να ανταποκριθούν γρήγορα και αποτελεσματικά στις μεταβαλλόμενες απαιτήσεις των επιχειρήσεων. Η αχίλλειος πτέρνα, ωστόσο, είναι ότι ΜΜΕ δεν έχουν την γνώση και τους πόρους που απαιτούνται για την προστασία των συστημάτων πληροφορικής για την ασφάλεια που αναμένεται από μεγάλους πελάτες, όπως οι τράπεζες, οι εταιρείες πετρελαίου και τα υπουργεία της κυβέρνησης.

Η αδυναμία αυτή δεν θα έχει σημασία αν τα περιστατικά ασφαλείας είχαν περιοριστεί σε μεγαλύτερες επιχειρήσεις. Οι μικρές επιχειρήσεις είναι εξίσου πιθανό να πληγούν από ιούς υπολογιστών, απώλειες laptop, κλοπή ταυτότητας, και τις καταστροφές δεδομένων. Αλλά είναι λιγότερο πιθανό να εφαρμόσουν μέτρα ασφαλείας, είτε λόγω έλλειψης κατανόησης από την απουσία των κατάλληλων πόρων ή απλά από μια επιθυμία για να εξοικονομήσουν χρήματα. Λόγω αυτής της έκθεσης, πολλοί μεγάλοι οργανισμοί αναμένουν οι προμηθευτές να επιδείξουν ένα ισοδύναμο πρότυπο ασφάλειας για τα δικά τους δεδομένα.

Ως εκ τούτου, η ασφάλεια των πληροφοριών έχει γίνει μια απαίτηση για κάθε επιχείρηση, μικρή και μεγάλη. Δεν είναι μόνο θέμα των εγκλημάτων στον κυβερνοχώρο, αλλά και της παροχής βιώσιμων επιχειρηματικών δραστηριοτήτων ώστε να παραμείνουν ανταγωνιστικές. Σε αυτά τα σενάρια, οι ΜΜΕ που έχουν ανεπαρκείς εγγυήσεις για τα πιστωτικά δεδομένα των πελατών τους και είναι πραγματικά εκτεθειμένες περισσότερο από τις μεγάλες επιχειρήσεις. Μια τοπική επιχείρηση η οποία υποφέρει από ένα περιστατικό, ακόμα και ένα τόσο απλό όπως η μη διαθεσιμότητα της ιστοσελίδας ή η απώλεια των δεδομένων της, μπορεί να βλάψει τις επιχειρηματικές συνεργασίες και να θέσει σε κίνδυνο τις μελλοντικές προοπτικές μετά το πραγματικό περιστατικό.

Οι μικρότερες εταιρείες, ωστόσο, λειτουργούν με διαφορετικό τρόπο οπ' ότι οι μεγάλες επιχειρήσεις. Δεν απασχολούν το είδος των επίσημων μηχανισμών ελέγχου που βρίσκονται σε μεγάλους οργανισμούς, όπως εταιρικές πολιτικές, συντονιστικές επιτροπές ή διαχειριστές της ασφάλειας με πλήρη απασχόληση και εσωτερικούς ελεγκτές. Η έννοια ενός πληροφοριακού συστήματος διαχείρισης της ασφάλειας, όπως απαιτείται από το πρότυπο ISO/ IEC 27001, δεν είναι κάτι που αντηχεί σε μια μικρότερη επιχείρηση. Μεγάλα εταιρικά πρότυπα μπορούν να προσαρμοστούν για τις μικρότερες επιχειρήσεις, αλλά αυτό απαιτεί μια διαδικασία αξιολόγησης του κινδύνου, κάτι που οι μικρές επιχειρήσεις δεν είναι συνήθως εξοπλισμένες ή δεν έχουν το κίνητρο να πραγματοποιήσουν όταν ασχολούνται με τα θέματα της ασφάλειας των πληροφοριών. Αυτό ισχύει ιδιαίτερα για τις νεοσύστατες επιχειρήσεις

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

και πολύ μικρές επιχειρήσεις, που είναι και από τους πιο καινοτόμους και δυνητικά επικερδείς τομείς της οικονομίας.

Για να είναι αποτελεσματικά σε ένα περιβάλλον ΜΜΕ, τα πρότυπα ασφάλειας πρέπει να λαμβάνουν υπόψη τους περιορισμένους πόρους και τις διαθέσιμες επιλογές. Πρέπει να αποφεύγεται η ακατάλληλη γραφειοκρατία, και να εκφράζεται σε κοινή γλώσσα που είναι κατανοητή η νοοτροπία του συντονισμού μιας τυπικής μικρής εταιρείας. Αυτή η καθοδήγηση καθορίζει την επίτευξη αυτού του στόχου, προκειμένου να ενθαρρύνει ένα μεγαλύτερο επίπεδο υιοθέτησης των μέτρων ασφάλειας των πληροφοριών από τις ΜΜΕ.

## 1.2 Σκοπός

Το έγγραφο αυτό επιχειρεί να ξεκινήσει την αντιμετώπιση του προβλήματος της ασφάλειας των ΜΜΕ. Αυτό το πρώτο μέρος απαντά στις βασικές ερωτήσεις για το τι είναι το πρόβλημα και γιατί οι τρέχουσες προσπάθειες είναι ανεπαρκείς.

Αξίζει να σημειωθεί ότι αυτό δεν είναι ένα σύνολο εντολών που δίνονται και που πρέπει να εφαρμόζονται για την ασφάλεια. Στον κόσμο των μικρών επιχειρήσεων, δεν υπάρχει τέτοιο πράγμα. Ως εκ τούτου, έχουν αναπτυχθεί κατευθυντήριες γραμμές προκειμένου να χρησιμοποιηθούν επιλεκτικά για να βοηθήσουν και να καταλάβουν τα σημεία ελέγχου οι μικρό-μεσαίες επιχειρήσεις.

Ως εκ τούτου, το πρότυπο αυτό θέτει μια ιεραρχία τριών κατηγοριών του ελέγχου, που η καθεμία λεπτομερώς αναλύει τις βασικές αρχές της ασφάλειας των πληροφοριών που θα πρέπει να επιδιώκουν οι πολύ μικρές ή μεσαίες επιχειρήσεις. Κάθε αρχή είναι σχεδιασμένη για την ελαχιστοποίηση του διοικητικού φόρτου, που συνδέεται συχνά με την ασφάλεια των πληροφοριών, με επίκεντρο τις επιχειρηματικές διαδικασίες.

## 1.3 Τι είναι μια ΜΜΕ;

Οι ορισμοί διαφέρουν ελαφρώς ως προς το τι συνιστά μια ΜΜΕ. Τα κριτήρια μπορεί να είναι τα έσοδα ή ο αριθμός των απασχολούμενων. Αλλά το πιο σημαντικό θέμα από την άποψη της ασφάλειας είναι ο αριθμός των εργαζομένων. Για μια «πολύ μικρή επιχείρηση», ο αριθμός του προσωπικού γενικά μετριέται σε μονοψήφιο νούμερο. Για μια «μικρή επιχείρηση» ο αριθμός θα ανέρχεται σε αρκετές δεκάδες, και για ένα «μέσο οργάνωσης» μπορεί να φτάνει σε αρκετές εκατοντάδες. Σημαντικό σημείο που αξίζει να σημειωθεί είναι ότι οι μέθοδοι που χρησιμοποιούνται για να διέπουν μια ομάδα ανθρώπων ποικίλλουν ανάλογα με το μέγεθός της. Ειδικότερα, ο τρόπος που οργανώνεται η εργασία είναι διαφορετικός για μια χούφτα άτομα από ό, τι για μια μεγάλη κοινότητα. Αυτό συμβαίνει επειδή ο αριθμός των σχέσεων μέσα σε μια οργάνωση μεγαλώνει εκθετικά με το μέγεθός της, η οποία επηρεάζει την ταχύτητα και τη φύση της διαδικασίας λήψης αποφάσεων.

## 1.4 Γιατί θα πρέπει οι ΜΜΕ να εφαρμόσουν την ασφάλεια των πληροφοριών;

Πολλές ΜΜΕ βασίζονται σε πληροφοριακά συστήματα, τόσο των ηλεκτρονικών όσο και των εκτυπωμένων πληροφοριών, για βασικές επιχειρηματικές δραστηριότητες, όπως την παροχή διαφημιστικών υπηρεσιών, την καταγραφή των παραγγελιών, την επεξεργασία των πληρωμών και τη διατήρηση των λογαριασμών. Η καλή ασφάλεια των πληροφοριών εξασφαλίζει την ακριβή, αξιόπιστη και αδιάλειπτη λειτουργία των συστημάτων. Επίσης εμποδίζει καταστροφικές ζημιές από κλοπή του εξοπλισμού ή των δεδομένων. Μειώνει το χρόνο που σπαταλιέται στην αντιμετώπιση περιστατικών, όπως οι ιοί υπολογιστών. Και αυτό βοηθά ταχύτητα το χρόνο αποκατάστασης από βλάβες του εξοπλισμού. Είναι ήδη μια υποχρεωτική απαίτηση για τις εταιρείες που χειρίζονται ευαίσθητα δεδομένα (σχετικά με τους

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

πελάτες, τους υπαλλήλους ή τους πολίτες) και για λιανοπωλητές που διαχειρίζονται πιστωτικές κάρτες. Σε μεγαλύτερο χρονικό διάστημα, είναι πιθανό να γίνει βασικό μέρος μιας εταιρείας "license to operate" σε όλους τους τομείς που δίνουν αξία στην καλή ασφάλεια των πληροφοριών.

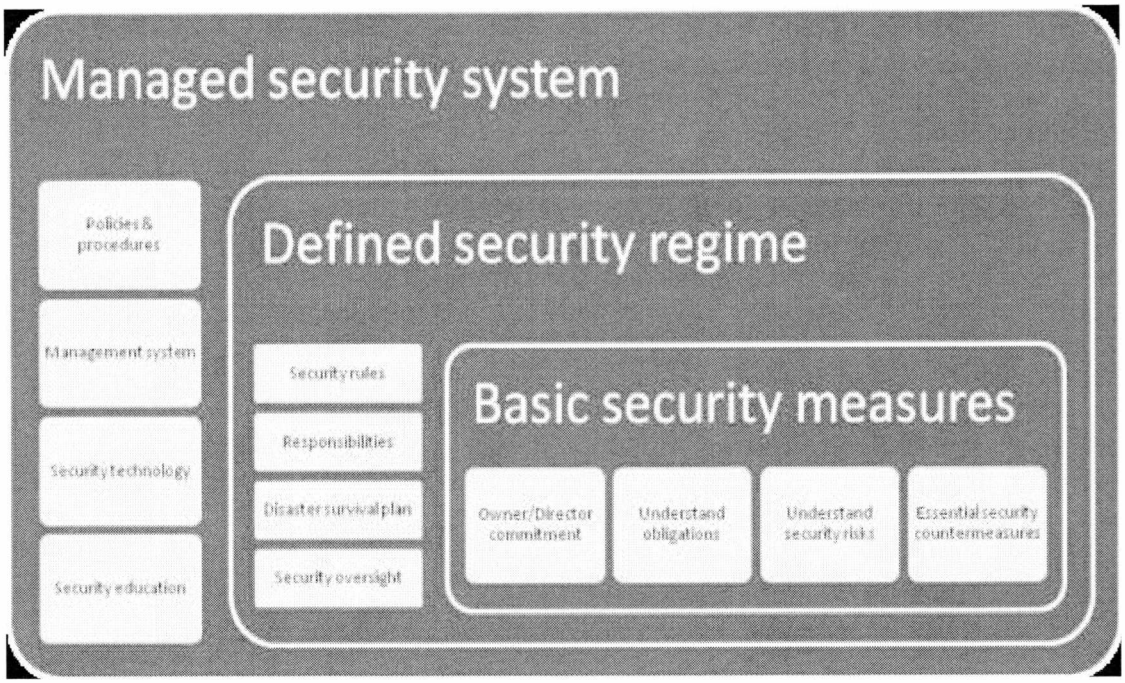
## 1.5 Τι είδους μέτρα ασφαλείας είναι κατάλληλα;

Οι ΜΜΕ δεν μπορούν να περιμένουν προστατευτικά μέτρα τα οποία είναι ακριβά, με γραφειοκρατικές διαδικασίες ή ζήτηση εξειδικευμένων δεξιοτήτων. Οι προτεινόμενες συστάσεις ασφαλείας πρέπει να είναι γρήγορες, απλές και φθηνές για να εφαρμοστούν και να διατηρηθούν. Σε αντίθετη περίπτωση θα πρέπει να αγνοηθούν ή να πέσουν σε αχρηστία. Οι Μικρό-επιχειρήσεις λειτουργούν με υψηλότερο το βαθμό του αυτοσχεδιασμού. Δεν απασχολούν επιτροπές για τη λήψη αποφάσεων ή καθοδήγηση από συμβουλευτικές γραπτές πολιτικές ασφαλείας. Τα τεχνικά ή διοικητικά μέτρα διασφάλισης πρέπει να είναι εύκολα στη λειτουργία και να μην απαιτούν εξειδικευμένες δεξιότητες ή γνώσεις, αν και μια μικρή αλλαγή εκτός από αυτή την τεχνογνωσία μπορεί συχνά να είναι επωφελής ώστε να βοηθήσει να επιδειχθούν και να εγκατασταθούν οι κατάλληλοι έλεγχοι.

Οι μεγαλύτερες ΜΜΕ απαιτούν κάποιο βαθμό επίσημης οργάνωσης, αλλά αυτό σίγουρα δεν θα είναι τόσο εκτεταμένο όπως τα ολοκληρωμένα συστήματα διαχείρισης που βρέθηκαν σε μεγάλους οργανισμούς. Καθώς ο αριθμός των εργαζομένων αυξάνεται και οι δραστηριότητες γίνονται πιο δομημένες, υπάρχει μεγαλύτερη ανάγκη για καθορισμένους ρόλους ασφαλείας, ευθύνες και εποπτεία. Ομοίως, καθώς η υποστήριξη των υποδομών γίνεται πιο εκτεταμένη και πολύπλοκη, θα υπάρξει ανάγκη για καλύτερο προγραμματισμό και αυστηρότερες προδιαγραφές. Η ανάγκη για επίσημες πολιτικές, διαδικασίες, επιτροπές, και ελέγχους αυξάνονται με το μέγεθος του οργανισμού.

Η εξεύρεση της σωστής ισορροπίας μεταξύ του έξυπνου αυτοσχεδιασμού και της αυστηρής τήρησης των τυπικών διαδικασιών είναι μια δύσκολη υπόθεση της ισορροπίας για κάθε ΜΜΕ, ειδικά για μια που φιλοδοξεί να αυξάνεται. Οι προτεραιότητες και οι έλεγχοι, ως εκ τούτου, θα πρέπει να αλλάξουν ανάλογα με το μέγεθος της επιχείρησης. Ο στόχος του ελέγχου θα μπορούσε να παραμένει σε μεγάλο βαθμό ο ίδιος, αλλά το επείγον και το προσιτό κόστος τους θα ποικίλει. Η ασφάλεια των πληροφοριών, οι συμβουλές, τα πρότυπα και οι λύσεις πρέπει, συνεπώς, να διαβαθμίζονται και να λαμβάνονται σύμφωνα με αυτές τις διαφορές.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79




Εικόνα 1: Παράδειγμα Διαχείρισης συστημάτων ασφαλείας[1]

Το πρότυπο αυτό καθορίζει μια τυπική ιεραρχία των ελέγχων ασφαλείας. Στην πράξη, ορισμένες ΜΜΕ θα απαιτήσουν υψηλότερο επίπεδο ασφαλείας, ανάλογα με τους κινδύνους, τις απαιτήσεις συμμόρφωσης και τις προσδοκίες των πελατών. Όπου είναι δυνατόν, αυτά τα επιπλέον στοιχεία συλλέγονται ούτος ώστε να δημιουργηθεί μια επαγγελματική εκτίμηση των κινδύνων, των απαιτήσεων καθώς και οι εφικτές λύσεις αυτών.

Η ιδανική λύση για τις ΜΜΕ είναι να ζητήσουν εξωτερικές, εξειδικευμένες συμβουλές προκειμένου να επιτύχουν τη σωστή ισορροπία. Αναγνωρίζεται, ωστόσο, ότι λίγες ΜΜΕ είναι πρόθυμες και ικανές να επενδύουν σε τέτοια υποστήριξη, και ότι υπάρχει μια γενική έλλειψη ειδικευμένων επαγγελματιών οι οποίοι είναι σε θέση να παραδώσουν τέτοια υποστήριξη.

Αντ 'αυτού, καθώς υπάρχουν λίγοι πόροι, που είναι προσιτό και κατανοητό, επιδιώκουν να παρέχουν κατεύθυνση για τους υπάρχοντες πόρους όπου ενδείκνυται.

## 1.6 Συμβατότητα με μεγάλα πρότυπα οργάνωσης

Τα διεθνή πρότυπα ασφαλείας, όπως το ISO / IEC 27001, έχουν ευρέως υιοθετηθεί από μεγάλους δημόσιους και ιδιωτικούς οργανισμούς σε όλο τον κόσμο. Το πρότυπο ISO καθορίζει περισσότερο από 130 επιμέρους ελέγχους ασφαλείας που ομαδοποιούνται σε 11 βασικούς τομείς. Δεν είναι όλοι οι έλεγχοι που πρέπει να εφαρμοστούν, δεδομένου ότι μπορούν να επιλεγούν με βάση επαγγελματικής αξιολόγησης του κινδύνου. Οι έλεγχοι που αναφέρονται ανωτέρω παρέχουν μια καλή αρχή για να πληρούν τις βασικές απαιτήσεις του ISO / IEC 27001, αλλά οι επιχειρήσεις θα πρέπει να πραγματοποιήσουν επίσημη αξιολόγηση του κινδύνου για τη δημιουργία και το επίπεδο συμμόρφωσής τους.

[1] Πηγή: ISSA UK, 2011

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# 2. Αρχές ασφάλειας των πληροφοριών για ΜΜΕ

Οι Αρχές της ασφάλειας των πληροφοριών που έχουν σημασία για τις μικρό-μεσαίες επιχειρήσεις χωρίζονται σε τρείς κατηγορίες. Οι κατηγορίες είναι κατά προσέγγιση και ανάλογες με το μέγεθος της ΜΜΕ.

Το πλαίσιο και το πεδίο εφαρμογής της κάθε επιχείρησης είναι οι τελικοί καθοριστικοί παράγοντες για το πώς πρέπει να τοποθετούνται τα μέτρα ασφάλειας των πληροφοριών, και το μέγεθος του οργανισμού είναι μόνο ένα μέτρο με το οποίο αυτό μπορεί να αξιολογηθεί. Άλλοι παράγοντες πρέπει να ληφθούν υπόψη, όπως η βιομηχανία των ΜΜΕ, το επίπεδο των ιδιόκτητων ή προσωπικών πληροφοριών που πρέπει να προστατεύονται, οι ρυθμιστικές εκθέσεις και συμβατικές απαιτήσεις. Ενώ εξειδικευμένες συμβουλές μπορούν να αναζητηθούν, αποτελώντας μια επιχειρηματική απόφαση, ως εκ τούτου η επιλογή του να αποφασίσει ποιες αρχές ισχύουν για κάθε επιμέρους ΜΜΕ και πώς να τις εφαρμόσουν, βρίσκεται ξεκάθαρα στον ιδιοκτήτη ή τον υπεύθυνο σύμβουλο.

Η απόφαση για το τι επίπεδο ελέγχου ασφαλείας είναι προνόμιο του ιδιοκτήτη της επιχείρησης. Είναι λογική και η υπόθεση ότι ο ιδιοκτήτης της επιχείρησης είναι υπεύθυνος για την ασφάλεια των επιχειρηματικών του λειτουργιών. Οι ΜΜΕ έχουν την ευθύνη για τους επιχειρηματικούς εταίρους και τους πελάτες, ώστε να λειτουργήσουν με ένα ασφαλές τρόπο. Αυτή είναι μια νομική ευθύνη σε πολλές χώρες, λόγω των διαφόρων μέτρων, όπως το Data Protection Act, και λόγω των κανονισμών, όπως PCI. Αυτό το πρότυπο έχει ως στόχο να παρέχει προσβάσιμες κατευθυντήριες που μπορεί να συντονιστούν για να εξασφαλίσουν στις ΜΜΕ τη διαχείριση των ευθυνών και εκ τούτου, τη βιωσιμότητα της επιχείρησής τους.

## 2.1. Βασικά μέτρα ασφαλείας

Βασικά μέτρα ασφάλειας είναι εκείνα που αναμένεται να εφαρμοστούν από όλες τις επιχειρήσεις, ανεξάρτητα από το μέγεθος ή τον τομέα. Σε πολλές περιπτώσεις, θα πρέπει να αυξηθούν με πρόσθετα μέτρα προκειμένου να μετριάσουν ιδιαίτερους κινδύνους ασφάλειας ή για να καλύψουν τις συγκεκριμένες ρυθμιστικές απαιτήσεις συμμόρφωσης.

### 2.1.1 Δέσμευση Ιδιοκτήτη / Διευθυντή

Η δέσμευση της επιχείρησης για την ασφάλεια των πληροφοριών θα πρέπει να προωθηθεί μέσω μιας γραπτής δέσμευσης ή υπόσχεσης. Ένα τέτοιο έγγραφο ενισχύει τη δέσμευση της διαχείρισης της ασφάλειας των πληροφοριών, και βοηθά τη διαβίβαση του προσωπικού και των ενδιαφερόμενων φορέων. Μπορεί να λάβει τη μορφή μιας επίσημης πολιτικής ασφαλείας ή μια απλής δήλωσης, υπογεγραμμένης από τον ιδιοκτήτη ή τον διευθύνοντα σύμβουλο, δηλώνοντας ότι η επιχείρηση θα έχει ως στόχο να εφαρμόσει-καταβάλει κάθε δυνατή προσπάθεια για τη διαφύλαξη των ευαίσθητων δεδομένων και κρίσιμων επιχειρηματικών συστημάτων από απειλές ασφάλειας.

### 2.1.2 Κατανόηση υποχρεώσεις

Οι διευθυντές και το προσωπικό που είναι υπεύθυνο για το χειρισμό ευαίσθητων επιχειρηματικών πληροφοριών ή τον έλεγχο των ουσιωδών συστημάτων των επιχειρήσεων πρέπει να έχουν μια καλή, up-to-date κατανόηση για τις σχετικές νομικές, ρυθμιστικές και εμπορικές απαιτήσεις. Είναι επίσης σημαντικό να διασφαλιστεί ότι οι εργαζόμενοι γνωρίζουν τις σχετικές απαιτήσεις ασφαλείας που συνδέονται με τις εμπορικές συμφωνίες, με τους πελάτες και με τους επιχειρηματικούς εταίρους, καθώς και τις απαιτήσεις των ρυθμιστικών αρχών και των επαγγελματικών ενώσεων.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

### 2.1.3 Απαντώντας σε κινδύνους ασφαλείας

Διευθυντές και διευθυντικά στελέχη πρέπει να κατανοήσουν και να αντιμετωπίσουν τους κινδύνους ασφαλείας των πληροφοριών σε περιουσιακά στοιχεία των επιχειρήσεων και των δραστηριοτήτων τους. Τακτικές αξιολογήσεις θα πρέπει να διεξάγονται για τις υφιστάμενες και αναδυόμενες απειλές για την ασφάλεια, όπως η κλοπή των δεδομένων ή του εξοπλισμού, πυρκαγιά ή πλημμύρες, βλάβες εξοπλισμού, ιοί υπολογιστών ή hacking. Θα πρέπει επίσης να δοθεί η τρωτότητα των συστημάτων, του εξοπλισμού και των χώρων σε συγκεκριμένες απειλές για την ασφάλεια, καθώς και τα μέτρα που απαιτούνται για να μειωθεί το επίπεδο του κινδύνου.

Μια σειρά από εξειδικευμένες τεχνικές υπηρεσίες είναι διαθέσιμες για τη σάρωση με σύνδεση στο Internet. Είναι απαραίτητο, όμως, να αναζητήσουν επαγγελματικές συμβουλές και να διασφαλίσουν ότι οι υπηρεσίες ή τα προϊόντα που χρησιμοποιούνται είναι κατάλληλα και γνήσια, όπως μερικοί διαφημίζουν προϊόντα που μπορούν να είναι πηγές malware.

### 2.1.4 Βασικά αντίμετρα ασφαλείας

Επιχειρήσεις θα πρέπει να εξασφαλίζουν ότι υπάρχουν τα κατάλληλα μέτρα ασφαλείας για την προστασία, τον εξοπλισμό και τα δεδομένα από κλοπή, βλάβη ή μη εξουσιοδοτημένη πρόσβαση. Αυτά θα πρέπει να περιλαμβάνουν το εξής.

Φυσικά μέτρα ασφαλείας για τις εγκαταστάσεις, όπως είναι η ασφαλής είσοδος, συναγερμούς για εισβολείς και κλείδωμα ευαίσθητων ή πολύτιμων περιουσιακών στοιχείων.

Έλεγχος διαδικασιών, όπως η επιλογή των κατάλληλων κωδικών πρόσβασης, που δεν μοιράζονται την είσοδο λογαριασμών, λαμβάνοντας τακτικά αντίγραφα back-up και κλείδωμα χαρτιών και φορητών υπολογιστών όταν τα γραφεία εκκενωθούν.

Τα τεχνικά μέτρα, όπως firewalls, anti-virus λογισμικά, αρχεία καταγραφής συμβάντων και back-up συσκευές αποθήκευσης.

Οι ενημερώσεις λογισμικού που εφαρμόζονται αμέσως.

Πολλές απώλειες συμβαίνουν έξω από το γραφείο ή σε κοινόχρηστα περιβάλλοντα. Είναι ως εκ τούτου, σημαντικό να διασφαλιστεί ότι οι κινητές συσκευές και τα δεδομένα προστατεύονται επαρκώς από απώλεια με φυσική ασφάλεια ή / και την κρυπτογράφηση των δεδομένων.

## 2.2 Ορισμός καθεστώτος ασφάλειας

Ένα καθορισμένο καθεστώς ασφάλειας εισάγει πρόσθετα μέτρα που θα απαιτηθούν σε μικρές έως μεσαίες επιχειρήσεις για να εξασφαλίσουν, ότι τα βασικά μέτρα ασφαλείας λειτουργούν με συνέπεια και αποτελεσματικότητα, με ελάχιστο κίνδυνο παρανοήσεων, λάθη ή αλληλοεπικάλυψη των προσπαθειών.

### 2.2.1 Κανόνες ασφαλείας

Ένας σαφής κατάλογος των "Do" και "Don'ts" θα πρέπει να διατηρηθεί για να διασφαλιστεί ότι οι εργαζόμενοι κατανοούν και θυμούνται να ακολουθούν τις βασικές διατάξεις που απαιτούνται για τη διασφάλιση των ευαίσθητων δεδομένων και των κρίσιμων επιχειρηματικών υπηρεσιών. Παραδείγματα μπορεί να περιλαμβάνουν: "Μην μοιράζεστε τα δεδομένα των πελατών»,« κλειδώστε τα laptops και τα ευαίσθητα δεδομένα, όταν το γραφείο είναι εκκενωμένο ", ή "Πάρτε τακτικά αντίγραφα των δεδομένων back-up". Οι κανόνες αυτοί θα πρέπει να επανεξετάζονται σε τακτά χρονικά διαστήματα και να ενημερώνονται από ανώτερα διοικητικά στελέχη.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

### 2.2.2 Αρμοδιότητες ασφαλείας

Ατομικές ευθύνες πρέπει να αποδοθούν για τη διασφάλιση των σημαντικών περιουσιακών στοιχείων, συμπεριλαμβανομένων των εγκαταστάσεων, του εξοπλισμού, των συστημάτων και των δεδομένων, καθώς και για την εκτέλεση συγκεκριμένων δραστηριοτήτων ασφαλείας, όπως είναι η λήψη εφεδρικών αντιγράφων ή η διαχείριση των δικαιωμάτων πρόσβασης σε επιχειρηματικά συστήματα και δεδομένα.

### 2.2.3 Σχέδιο επιβίωσης από καταστροφές

Οι επιχειρηματικές δραστηριότητες μπορεί να διαταραχθούν σοβαρά από απρόβλεπτους κινδύνους όπως φωτιά, πλημμύρες, hacking ή αποτυχίες εξοπλισμού. Είναι σημαντικό να εντοπιστούν εναλλακτικές ρυθμίσεις εργασίας, όπως εφεδρικά sites ή συστήματα, και να προβούν στις κατάλληλες προετοιμασίες για ένα τέτοιο γεγονός, όπως η εκπόνηση ενός απλού σχεδίου κρατώντας up-to-date αντίγραφα ασφαλείας των σημαντικών δεδομένων, και το λογισμικό σε μια ασφαλή εναλλακτική θέση.

### 2.2.4 Εποπτεία ασφάλειας

Η εμπειρία δείχνει ότι, στα πολυσύχναστα περιβάλλοντα εργασίας, οι κανόνες και οι διαδικασίες της ασφάλειας μπορούν εύκολα να αγνοηθούν. Παραδείγματα από αυτό μπορεί να περιλαμβάνουν και το προσωπικό, παραλείποντας να λάβει τα εφεδρικά αντίγραφά, αλλάζοντας τους κωδικούς πρόσβασης, ή εφαρμόζοντας κρίσιμες ενημερώσεις ασφαλείας του λογισμικού.

## 2.3 Υπεύθυνη διαχείριση του συστήματος ασφαλείας

Ένα διαχειριζόμενο σύστημα ασφαλείας εισάγει πρόσθετα μέτρα διακυβέρνησης που είναι χρήσιμα για μεγαλύτερες ΜΜΕ ή για εκείνες με μεγαλύτερο κίνδυνο. Τα μετρα αυτά επιτρέπουν μια πιο ολοκληρωμένη και αποτελεσματική διαχείριση της ασφάλειας. Παρέχει επίσης έναν υψηλότερο βαθμό διαβεβαίωσης ότι οι πολιτικές ασφαλείας και οι έλεγχοι έχουν υλοποιηθεί.

### 2.3.1 Πολιτικές & διαδικασίες

Ένας μεγάλος αριθμός των ad hoc κανόνων και πρακτικών ασφαλείας μπορεί να είναι δύσκολο να επικοινωνήσουν και να διαχειριστούν αποτελεσματικά. Επίσημες πολιτικές και διαδικασίες ασφαλείας, που καθορίζουν τις πολιτικές, τις ευθύνες και τους στόχους του ελέγχου, σε ένα δομημένο τρόπο, είναι ευκολότερο για το προσωπικό να τις συμβουλεύονται και για τους διαχειριστές να τους επιβλέπουν. Διαδικασίες για βασικές λειτουργίες, όπως η διαχείριση της πρόσβασης δικαιωμάτων, η έκδοση εξοπλισμού και η λήψη εφεδρικών αντιγράφων, πρέπει να τεκμηριώνονται βάση της καθοδήγησης.

### 2.3.2 Σύστημα Διαχείρισης

Εμπειρία σε μεγάλους οργανισμούς έχει δείξει ότι τα πιο αποτελεσματικά και αποδοτικά μέσα της διαχείρισης των απαιτήσεων και των δραστηριοτήτων ασφάλειας είναι μέσα από μια «διαδικασία προσέγγισης» παρόμοια με τα μοντέλα που χρησιμοποιούνται ευρέως για τη βελτίωση των επιχειρηματικών διαδικασιών. Η προσέγγιση αυτή ενθαρρύνει δραστηριότητες ασφαλείας που πρέπει να σχεδιάζονται, να υλοποιούνται, να ελέγχονται και να βελτιώνονται συνεχώς σε μια ενεργητική, στρατηγική βάση. Η υιοθέτηση ενός τέτοιου συστήματος διαχείρισης απαιτεί την καθιέρωση σαφών στόχων ασφαλείας ενός δομημένου πρόγραμμος δραστηριοτήτων της και ένος επίσημου συμβουλίου που θα επανεξετάσει την πρόοδο προς τους στόχους.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

### 2.3.3 Τεχνολογία ασφαλείας

Οι ΜΜΕ θα πρέπει να εξετάσουν τη χρήση εξειδικευμένων τεχνολογιών ασφαλείας για την προστασία ευαίσθητων κρίσιμων επιχειρηματικών συστημάτων δεδομένων, και να βοηθήσουν στην πρόληψη ή τον εντοπισμό πιθανών περιστατικών ασφαλείας. Τα παραδείγματα τεχνολογιών ασφαλείας είναι ολοένα και πιο απαραίτητα για την καθημερινή επαγγελματική χρήση και περιλαμβάνουν συσκευές με «ισχυρό έλεγχο ταυτότητας» για την ασφαλή, απομακρυσμένη σύνδεση από τους χρήστες στο σπίτι ή στο προσωπικό που ταξιδεύει. Επίσης συστήματα με «κρυπτογράφηση σκληρού δίσκου» για τη διασφάλιση των δεδομένων σε φορητούς υπολογιστές, και «συστήματα πρόληψης εισβολών» για να εντοπίσουν και να μπλοκάρουν τις εισερχόμενες δικτυακές επιθέσεις.

### 2.3.4 Εκπαίδευση Ασφαλείας

Η ασφάλεια είναι ευθύνη όλων μέσα σε μια σύγχρονη επιχείρηση, έτσι όλοι οι εργαζόμενοι πρέπει να εκπαιδεύονται και να ενημερώνονται τακτικά και να θυμούνται το φάσμα των απειλών κατά της ασφάλειας για τα επιχειρηματικά δεδομένα και τα συστήματα ασφαλείας, καθώς και τις ευθύνες τους για τη μείωση των κινδύνων σε ένα αποδεκτό επίπεδο. Η εκπαίδευση ασφαλείας θα πρέπει να αρχίσει με μια κατάλληλη συνεδρία επαγωγής για όλα τα νέα μέλη του προσωπικού και θα πρέπει να διατηρηθεί με τακτικές ενημερώσεις και δελτία.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# 3. Απειλές ασφάλειας που επηρεάζουν τις ΜΜΕ

## 3.1 Γενικά

Ανεξάρτητα από το πόσο ασφαλής είναι μια επιχείρηση και το σύστημά της, καθένας θα πρέπει να παραμένει σε επαγρύπνηση έναντι στις συνεχόμενες απειλές. Παρακάτω περιγράφονται οκτώ από τις περισσότερο κοινές επιθέσεις που συμβαίνουν στον κυβερνοχώρο.

### 3.1.1 Malware

**Τι είναι:** Είναι ένας όρος που καταλαμβάνει μια ποικιλία από απειλές όπως Trojans, worms και virus. Ως Malware ορίζεται απλά ένας κώδικας με κακόβουλες προθέσεις ο οποίος συνήθως κλέβει δεδομένα ή καταστρέφει κάτι στον υπολογιστή.

**Πως δουλεύει:** Τα Malware συνήθως εισάγονται στο σύστημα μέσω συνημμένων σε email, σε λήψεις λογισμικού ή ευπάθειες του λειτουργικού συστήματος.

**Πως αντιμετωπίζεται:** Ο καλύτερος τρόπος για την πρόληψη του κακόβουλου λογισμικού είναι να μην γίνει λήψη συνημμένων αρχείων από άγνωστους αποστολείς. Επίσης αυτό κατορθώνεται μερικές φορές με την ανάπτυξη firewalls τα οποία μπορούν να εμποδίσουν την μεταφορά μεγάλου όγκου δεδομένων μέσω του δικτύου. Είναι σημαντικό επίσης το λειτουργικό σύστημα του υπολογιστή (Windows, Mac, Linux) να είναι ενημερωμένο σχετικά με τις ενημερώσεις ασφαλείας. Οι προγραμματιστές των λογισμικών ενημερώνουν τα προγράμματα ώστε να αντιμετωπιστούν οι ευπάθειες.

### 3.1.2 Phishing

**Τι είναι**: Οι επιθέσεις τύπου fishing είναι ένα είδος Social engineering που είναι συνήθως ευκαιριακού χαρακτήρα και στοχεύουν ένα υποσύνολο της κοινωνίας. Ένα μήνυμα ηλεκτρονικού ταχυδρομείου τύπου fishing, είναι παρόμοιο με τις υπηρεσίες/εταιρείες που μιμείται(λογότυπα από μια γνωστή τράπεζα) και θα φαίνεται ως επίσημα απεσταλμένο από την εταιρεία. Όταν ο χρήστης ακολουθήσει τις οδηγίες στο μήνυμα ουσιαστικά κατευθύνεται στο να αποκαλύψει ευαίσθητες ή προσωπικές πληροφορίες όπως κωδικούς πρόσβασης, κωδικούς PIN, αριθμούς πιστωτικών καρτών.

**Πως δουλεύει**: Τα phishing emails περιλαμβάνουν μια σύνδεση που ανακατευθύνει τον χρήστη σε μια εικονική τοποθεσία που θα κλέψει τις πληροφορίες του χρήστη. Σε μερικές περιπτώσεις μόνο ένα απλό κλικ στον σύνδεσμο αρκεί.

**Πως αντιμετωπίζεται:** Βεβαιώνοντας ότι όλες οι αιτήσεις που λαμβάνονται έχουν αφιχθεί μέσω e-mail από το τηλέφωνο. Αν στο e-mail υπάρχει αριθμός τηλεφώνου μην κλιθεί αλλά να κλιθεί ο αριθμός που θα βρεθεί στο διαδίκτυο ή ο αριθμός που υπάρχει στα έγγραφα που λήφθηκαν από την επιχείρηση. Οι περισσότερες εταιρείες δεν ζητάνε ποτέ προσωπικά στοιχεία μέσω email. Ταυτόχρονα οι περισσότερες εταιρείες συνιστούν ότι χρήστες δε θα πρέπει να κοινοποιούν ευαίσθητες πληροφορίες. Ενώ μπορεί να φαίνεται σαν κόπος να πραγματοποιηθεί μια τηλεφωνική κλήση για να εξακριβωθεί αν κάτι είναι νόμιμο, η ταλαιπωρία από τις συνέπειες της επίθεσης θα είναι μεγαλύτερη.

### 3.1.3 Password Attacks

**Τι είναι**: Είναι μια επίθεση στην οποία ένας τρίτος προσπαθεί να αποκτήσει πρόσβαση στο σύστημά σας χρησιμοποιώντας τον κωδικό σας.

**Πως δουλεύει:** Αυτό το είδος της επίθεσης δεν απαιτεί κάποιο είδος λογισμικού ή κακόβουλου κώδικα. Υπάρχει λογισμικό το οποίο οι επιτιθέμενοι χρησιμοποιούν για

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

να σπάσουν τον κωδικό πρόσβασης αλλά αυτό το λογισμικό είναι εγκατεστημένο και λειτουργεί στο δικό τους σύστημα. Τα προγράμματα αυτά χρησιμοποιούν πολλές μεθόδους για να αποκτήσουν πρόσβαση σε λογαριασμούς, συμπεριλαμβανομένων επιθέσεων ωμής βίας(brute force attack) για να μαντέψουν τον κωδικό καθώς και την σύγκριση των διαφόρων συνδυασμών λέξεων.

**Πως αντιμετωπίζεται:** Οι ισχυροί κωδικοί πρόσβασης είναι ο μόνος τρόπος προστασίας από τέτοιου είδους επιθέσεις. Αυτό σημαίνει ότι θα χρησιμοποιείτε ένα συνδυασμό από πεζά και κεφαλαία γράμματα, σύμβολα, αριθμούς με οχτώ χαρακτήρες ή περισσότερους. Ένας επιτιθέμενος που χρησιμοποιεί brute force attack για να σπάσει έναν κωδικό μπορεί τυπικά να ξεκλειδώσει έναν κωδικό με όλα τα ψηφία σε πεζά σε μερικά λεπτά. Είναι επίσης προτεινόμενο να μην χρησιμοποιούνται λέξεις που υπάρχουν σε λεξικά, χωρίς να παίζει ρόλο το μέγεθός τους, γιατί αυτό κάνει την δουλειά του εισβολέα ακόμα πιο εύκολη. Τέλος επιβάλλεται να αλλάζονται οι κωδικοί σε τακτά χρονικά διαστήματα. Αν ένας hacker είναι σε θέση να αποκτήσει έναν παλαιότερο κωδικό πρόσβασης τότε δεν θα λειτουργήσει διότι θα έχει ήδη αντικατασταθεί.

### 3.1.4 Denial-Of-Service(DoS) Attacks

**Τι είναι:** Σε μια προσπάθεια να ελαχιστοποιηθεί το κόστος ή απλώς από αμέλεια, οι περισσότερες μικρές-μεσαίες επιχειρήσεις έχουν κενά ασφαλείας. Η Denial of Service ('Άρνηση Υπηρεσίας) είναι μια επίθεση που αποτρέπει τους νόμιμους χρήστες από την χρήση μιας υπηρεσίας και είναι αρκετά δύσκολη να αποτραπεί. Ειδικότερα εστιάζει στην διακοπή της υπηρεσίας σε ένα δίκτυο. Οι επιτιθέμενοι δηλαδή στέλνουν μεγάλο όγκο κυκλοφορίας δεδομένων στο δίκτυο (πολλά αιτήματα σύνδεσης) μέχρι το δίκτυο να υπερφορτωθεί και να μην μπορεί να λειτουργεί πλέον. Τα μέσα και τα κίνητρα για να πραγματοποιηθεί μια DoS επίθεση μπορεί να διαφέρουν, αλλά συνήθως οδηγεί τους νόμιμους πελάτες στο Downtime(το σύστημα δεν είναι διαθέσιμο) και στο να χάσουν την εμπιστοσύνη τους στην οργάνωση.

**Πως δουλεύει:** Υπάρχουν αρκετοί διαφορετικοί τρόποι με τους οποίους οι επιτιθέμενοι μπορούν να πραγματοποιήσουν DoS επιθέσεις, αλλά η περισσότερο γνωστή είναι η κατανεμημένη denial-of-service (DDoS) attack. Αυτή περιλαμβάνει τον επιτιθέμενο χρησιμοποιώντας πολλούς υπολογιστές για να αποστέλλει κίνηση ή δεδομένα που θα προκαλέσουν υπερφόρτωση του συστήματος. Σε πολλές περιπτώσεις ένα άτομο μπορεί να μην συνειδητοποιεί ότι ο υπολογιστής του χρησιμοποιείται στην επίθεση DDoS. Αυτή η επίθεση μπορεί να έχει σοβαρές συνέπειες για την ασφάλεια και την πρόσβαση στο διαδίκτυο. Σε πολλές περιπτώσεις επιθέσεων DDoS μεγάλης κλίμακας που έχουν χρησιμοποιηθεί ως ένδειξη διαμαρτυρίας προς την Κυβέρνηση ή σε κάποιο άτομο, οι ποινές είναι σοβαρές όπως φυλάκιση.

**Πως αντιμετωπίζεται:** Αν η εταιρεία είναι τεράστια, είναι σπάνιο να στοχοποιηθεί από μια εξωτερική ομάδα ή έναν επιτιθέμενο για επίθεση DoS. Η ιστοσελίδα ή το δίκτυο της εταιρείας θα μπορούσε να πέσει θύμα σε μία επίθεση, ειδικά αν μια άλλη οργάνωση στο δίκτυό της είναι στοχευμένη για επίθεση. Ο καλύτερος τρόπος για να αποφευχθεί η πρόσθετη παραβίαση είναι να διατηρηθεί το σύστημά όσο το δυνατόν πιο ασφαλές, με τακτικές ενημερώσεις του λογισμικού, online παρακολούθηση της ασφάλειας και παρακολούθηση της ροής των δεδομένων για τον εντοπισμό τυχόν ασυνήθιστων απειλών στην κυκλοφορία προτού να δημιουργηθεί πρόβλημα. Οι επιθέσεις DoS μπορούν να πραγματοποιηθούν απλά με την κοπή ενός καλωδίου ή την απόσπαση ενός βύσματος που συνδέει την ιστοσελίδα στο διαδίκτυο, συνεπώς και η παρακολούθηση των φυσικών συνδέσεων είναι επιβεβλημένη.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

### 3.1.5 "Man in the Middle" (MITM)

**Τι είναι:** Είναι η μίμηση των endpoints για την online ανταλλαγή πληροφοριών(δηλαδή την σύνδεση από το smartphone σε μια ιστοσελίδα), η MITM μπορεί να λάβει πληροφορίες από τον τελικό χρήστη και από τον χρήστη με τον οποίο επικοινωνεί. Για παράδειγμα, αν χρησιμοποιείτε online τραπεζικές συναλλαγές, ο MITM θα επικοινωνήσει με εσάς μιμούμενος την τράπεζα και μετά θα επικοινωνήσει με την τράπεζα μιμούμενος εσάς. Έτσι θα έχει λάβει όλες τις πληροφορίες μεταξύ εσάς και της τράπεζας όπως είναι ευαίσθητα προσωπικά δεδομένα και τραπεζικούς λογαριασμούς.

**Πως δουλεύει:** Συνήθως η MITM αποκτά πρόσβαση μέσω ενός μη-κρυπτογραφημένου σημείου προσβάσεως (ένα που δεν χρησιμοποιεί WAP,WPA,WPA2 ή άλλα μέτρα ασφαλείας). Έτσι έχει πρόσβαση σε όλες τις πληροφορίες που μεταφέρονται μεταξύ των δυο μεριών.

**Πως αντιμετωπίζεται**: Ο καλύτερος τρόπος για να αποφευχθεί η επίθεση είναι να χρησιμοποιηθούν μόνο κρυπτογραφημένα ασύρματα σημεία πρόσβασης με ασφάλεια WPA ή μεγαλύτερη. Αν χρειαστεί σύνδεση σε μια ιστοσελίδα, βεβαιωθείτε ότι χρησιμοποιεί σύνδεση HTTPS ή μεγαλύτερη ασφάλεια ή επενδύστε σε ένα εικονικό ιδιωτικό δίκτυο. Τα HTTPS χρησιμοποιούν πιστοποιητικά που επαληθεύουν την ταυτότητα του server που συνδέεται σε μια τρίτη εταιρεία όπως VeriSign, ενώ τα VPNs επιτρέπουν συνδεση σε ιστοσελίδες μέσω εικονικών προσωπικών δικτύων.

### 3.1.6 Drive-By Downloads

**Τι είναι:** Το κακόβουλο λογισμικό δεν εισάγεται πάντα χειροκίνητα ή συνειδητά. Βασικά πακέτα λογισμικού που έχουν εγκατασταθεί σε υπολογιστές όπως Internet Explorer, Firefox, Adobe Acrobat Reader ή Flash έχουν μερίδιο ευθύνης λόγω των τρωτών σημείων τους στην ασφάλεια. Αυτές οι ευπάθειες στην ασφάλεια είναι που εκμεταλλεύονται οι προγραμματιστές κακόβουλων λογισμικών ώστε να μολύνουν αυτόματα τους υπολογιστές των θυμάτων τους. Αυτές οι επιθέσεις είναι γνωστές ως drive-by downloads επειδή ο χρήστης δεν έχει γνώση των κακόβουλων αρχείων που εγκαθίστανται στον υπολογιστή του. Το 2007 η Google εξέδωσε ένα δελτίο το οποίο περιέγραφε 450.000 ιστοσελίδες που εγκαθιστούν κακόβολου λογισμικό χωρίς την έγκριση του χρήστη.

**Πως δουλεύει:** Συνήθως, ένα μικρό απόσπασα του κώδικα εγκαθίσταται στο σύστημα του χρήστη και στην συνέχεια ο κώδικάς του φτάνει σε ένα άλλο υπολογιστή ώστε να κατεβάσει το υπόλοιπο πρόγραμμα. Εκμεταλλεύεται συχνά τις ευπάθειες στο λειτουργικό σύστημα του χρήστη σε διαφορετικά προγράμματα όπως είναι η Java και το Adobe.

**Πως αντιμετωπίζεται:** Ο καλύτερος τρόπος είναι όλα τα λειτουργικά συστήματα και τα προγράμματα λογισμικού να είναι ενημερωμένα. Αυτό μειώνει τον κίνδυνο της τρωτότητας. Επιπλέον, θα πρέπει να γίνει προσπάθεια για ελαχιστοποίηση του αριθμού των browser add-ons οι οποίοι μπορούν εύκολα να παραβιαστούν. Για παράδειγμα, αν ο υπολογιστής δεν χρειάζεται το Flash ή το Java plug-in τότε ότι πρέπει να το απεγκατασταθεί.

### 3.1.7 Malvertising

**Τι είναι:** Είναι ένας τρόπος για να τεθεί σε κίνδυνο ο υπολογιστής με κακόβουλο κώδικα που έχει εγκατασταθεί από απλό κλικ σε μια διαφήμιση.

**Πως δουλεύει:** Οι επιτιθέμενοι στον κυβερνοχώρο ανεβάζουν κακόβουλες διαφημίσεις σε διάφορες ιστοσελίδες. Αυτές οι διαφημίσεις διανέμονται σε ιστοσελίδες που ταιριάζουν με ορισμένες λέξεις - κλειδιά και κριτήρια αναζήτησης. Μόλις ένας χρήστης κάνει κλικ σε μία από αυτές τις διαφημίσεις, θα κατεβάσει εν αγνοία του κάποιου είδους κακόβουλο λογισμικό. Κάθε ιστοσελίδα ή web publisher μπορεί να

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

υποβληθεί σε κακόβουλες διαφημίσεις και πολλοί δεν γνωρίζουν ότι έχουν παραβιαστεί.

**Πως αντιμετωπίζεται:** Ο καλύτερος τρόπος να αποφευχθεί αυτή η επίθεση είναι η κοινή λογική. Οποιαδήποτε διαφήμιση που υπόσχεται πλούτη, δωρεάν υπολογιστές ή κρουαζιέρες στις Μπαχάμες είναι πιθανώς πάρα πολύ καλό για να είναι αληθινό και συνεπώς θα κρύβει κάποιο κακόβουλο λογισμικό. Όπως πάντα, τα ενημερωμένα συστήματα και τα λογισμικά είναι η καλύτερη πρώτη γραμμή άμυνας.

### 3.1.8 Rogue Software

**Τι είναι:** Είναι λογισμικό κακόβουλο που παρουσιάζεται ως νόμιμο και απαραίτητο για την προστασία του συστήματος σας.

**Πως δουλεύει**: Εμφανίζεται σε pop-up παράθυρα και σε ειδοποιήσεις ώστε να φαίνεται νόμιμο. Αυτές οι ειδοποιήσεις συμβουλεύουν τον χρήστη να κατεβάσει λογισμικό ασφαλείας, να συμφωνήσει με τους όρους ή να ενημερώσει το τρέχον σύστημα σε μια προσπάθεια να μείνει προστατευμένο. Αποδεχόμενοι όλα αυτά το λογισμικό θα κατέβει στον υπολογιστή.

**Πως αντιμετωπίζεται:** Η καλύτερη άμυνα για αυτή την επίθεση είναι ένα ενημερωμένο Firewall. Βεβαιωθείτε ότι έχετε ένα firewall που λειτουργεί και σας προστατεύει από τέτοιου είδους επιθέσεις. Είναι επίσης καλή ιδέα να εγκαταστήσετε ένα αξιόπιστο anti spyware πρόγραμμα λογισμικού που μπορεί να ανιχνεύει τέτοιες απειλές.

## 3.2 Κακόβουλο περιεχόμενο στο Internet

Οι περισσότερες σύγχρονες μικρές ή μεσαίες επιχειρήσεις χρειάζονται μια σύνδεση στο Ιντερνέτ για να λειτουργήσουν. Αν εκλείψει αυτό το μέσο επικοινωνίας τότε πολλά τμήματα της επιχείρησης δεν θα είναι σε θέση να λειτουργήσουν σωστά ή να επιστρέψουν στα παλαιά όχι και τόσο αποτελεσματικά μέσα επικοινωνίας. Μόνο οι υπηρεσίες e-mail είναι από τα κύρια μέσα επικοινωνίας για τις επιχειρήσεις. Ακόμα και η επικοινωνία μέσω τηλεφώνου έχει αντικατασταθεί από το ηλεκτρονικό ταχυδρομείο.

Οι περισσότεροι οργανισμοί έχουν υπάρξει θύματα μιας επίθεσης ιού του υπολογιστή. Παρόλο που έχουν προστασία από ιούς, δεν είναι ασυνήθιστο για μια επιχείρηση με δέκα ή περισσότερους εργαζόμενους να χρησιμοποιούν το e-mail ή το Διαδίκτυο χωρίς καμία μορφή προστασίας. Ακόμη και οι μεγάλες επιχειρήσεις δεν αποτελούν εξαίρεση. Για παράδειγμα τρία νοσοκομεία στο Λονδίνο έπρεπε να θέσουν τα δίκτυά τους εκτός λειτουργίας λόγω της μόλυνσης από μια έκδοση worm με το όνομα Mytob. Τις περισσότερες φορές, δεν γνωστοποιούνται οι επιθέσεις σε μικρομεσαίες επιχειρήσεις διότι δεν είναι προς το συμφέρον τους να δημοσιοποιήσουν αυτά τα περιστατικά. Αρκετές μικρές και μεσαίες επιχειρήσεις δεν μπορούν να στηρίξουν οικονομικά τους μηχανισμούς πρόληψης όπως είναι ο διαχωρισμός του δικτύου. Αυτοί είναι μερικοί παράγοντες βάση των οποίων είναι εύκολο ένα worm να εξαπλωθεί σε ολόκληρη την επιχείρηση.

Μια επιχείρηση που λειτουργεί με τρόπο αποδοτικό, συνήθως έχει εδραιώσει τρόπους να μοιράζεται αρχεία και περιεχόμενα σε ολόκληρη την έκτασή της. Αυτές οι μέθοδοι μπορούν συνεπώς να μολυνθούν από worms για να μολύνουν περαιτέρω τα συστήματα υπολογιστών στο δίκτυο.

Επίσης υπάρχουν και επιθέσεις τύπου Social engineering. Αυτός ο όρος αναφέρεται σε ένα σύνολο τεχνικών όπου οι επιτιθέμενοι εκμεταλλεύονται κυρίως τα ανθρώπινα σφάλματα παρά τις ευπάθειες της τεχνολογίας.

Ωστόσο, οι εργαζόμενοι και οι υπολογιστές δεν είναι οι μοναδικοί στόχοι σε μια επιχείρηση. Οι περισσότερες μικρού ή μεσαίου μεγέθους επιχειρήσεις

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

χρησιμοποιούν τους servers για ηλεκτρονικό ταχυδρομείο, διαχείριση πελατειακών σχέσεων και για τα αρχεία που μοιράζονται. Αυτοί οι server κατέχουν κρίσιμες πληροφορίες και μπορούν εύκολα να γίνουν ο στόχος μιας επίθεσης. Επιπλέον, η επιλογή των web-εφαρμογών εισήγαγε ένα μεγάλο αριθμό ευπαθειών στην ασφάλεια που εκμεταλλεύονται οι επιτιθέμενοι. Όταν αυτές οι υπηρεσίες παραβιάζονται υπάρχει μεγάλος κίνδυνος οι ευαίσθητες πληροφορίες να διαρρεύσουν και να χρησιμοποιηθούν από εγκληματίες του κυβερνοχώρου για απάτη.

## 3.3 Επιθέσεις σε physical systems

Οι επιθέσεις στο Διαδίκτυο δεν είναι το μόνο θέμα ασφαλείας που αντιμετωπίζουν οι επιχειρήσεις. Στους φορητούς υπολογιστές και στα κινητά τηλέφωνα συνήθως αποθηκεύονται ευαίσθητα δεδομένα της επιχείρησης. Οι συσκευές αυτές είτε είναι ιδιοκτησία της εταιρείας, είτε του προσωπικού, που συχνά περιέχουν έγγραφα της εταιρείας και επίσης χρησιμοποιούνται για την σύνδεση με το δίκτυο της εταιρείας. Συχνότερα, τα κινητά τηλέφωνα χρησιμοποιούνται κατά την διάρκεια συνεδρίων και επαγγελματικών ταξιδιών και είναι ευάλωτα σε κλοπή.

Ενδεικτικά ο αριθμός των φορητών υπολογιστών και κινητών που κλέβονται αυξάνεται κάθε χρόνο. Η *Attrition.org* είχε πάνω από 400 άρθρα το 2008 που σχετίζονταν με την απώλεια δεδομένων, πολλά από τα οποία αναφεράταν σε κλεμμένους φορητούς υπολογιστές και δίσκους. Αν αυτό συμβαίνει σε μεγάλα νοσοκομεία και σε κυβερνητικούς οργανισμούς που διαθέτουν πρωτόκολλα αντιμετώπισης τέτοιων περιστάσεων, θα συμβαίνει ακόμα πιο εύκολα σε μικρές και μεσαίες επιχειρήσεις.

Μια άλλη απειλή είναι τα απροστάτευτα τερματικά σημεία ή κοινώς endpoints. Οι θύρες USB και οι οδηγοί δίσκων DVD μπορούν να χρησιμοποιηθούν για την διαρροή δεδομένων και για την εισαγωγή κακόβουλου λογισμικού στο δίκτυο. Ένα USB stick που χρησιμοποιείται κυρίως για την εργασία και ίσως να περιέχει ευαίσθητα έγγραφα γίνεται ένα ρίσκο για την ασφάλεια όταν μεταφερθεί στην οικία και χρησιμοποιηθεί από άλλα μέλη της οικογένειας για τους υπολογιστές στο σπίτι. Ενώ ο εργαζόμενος μπορεί να κατανοήσει την αξία των εγγράφων που είναι αποθηκευμένα στο USB stick η υπόλοιπη οικογένεια δεν το αντιλαμβάνεται. Ίσως να αντιγράψουν τα αρχεία χωρίς να λάβουν υπόψη τις συνέπειες. Πρόκειται για μια περίπτωση αμέλειας αλλά μπορεί να αποτελέσει τον στόχο μιας στοχευόμενης επίθεσης όπου οι εργαζόμενοι μεταφέρουν αρκετές πληροφορίες της εταιρείας έξω από αυτήν.

Οι μικρές και μεσαίες επιχειρήσεις δεν πρέπει να παραβλέψουν την σημασία της φυσικής ασφάλειας του δικτύου και του server ώστε να αποτρέψουν την είσοδο μη εξουσιοδοτημένων προσώπων.

## 3.4 Αυθεντικοποίηση και ιδιωτικές επιθέσεις

Οι κωδικοί πρόσβασης παραμένουν το νούμερο ένα θέμα ευπάθειας σε αρκετά συστήματα. Δεν είναι εύκολη υπόθεση να έχουμε ένα ασφαλές σύστημα όπου είμαστε υποχρεωμένοι να επιλέξουμε έναν μοναδικό κωδικό που οι επιτιθέμενοι δεν θα μπορούν να τον μαντέψουν και ταυτόχρονα να τον θυμόμαστε. Σήμερα οι περισσότεροι άνθρωποι έχουν τουλάχιστον πέντε κωδικούς που πρέπει να θυμούνται και οι κωδικοί στις επιχειρήσεις δεν θα πρέπει να ταιριάζουν με τους κωδικούς των λογαριασμών webmail. Οι εισβολές στους λογαριασμούς των δικτύων κοινωνικής ενημέρωσης δείχνουν σαφώς ότι οι κωδικοί πρόσβασης είναι ο αδύναμος κρίκος της ασφάλειας και οι επιτιθέμενοι εκμεταλλεύονται ακριβώς αυτήν την αδυναμία και δεν απαιτούν τόσο τεχνογνωσία όσο φαντασία.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Οι πολιτικές των κωδικών πρόσβασης μπορούν να συντελέσουν στον μετριασμό του κινδύνου αλλά αν δεν είναι αρκετά αυστηροί τότε ο επιτιθέμενος θα βρει τα μέσα και τον τρόπο να τους παρακάμψει. Οι εργαζόμενοι θα καταγράψουν τον κωδικό σε χαρτί, θα τον μοιραστούν με τους συναδέλφους ή απλά θα βρουν μια πατέντα στο πληκτρολόγιο (1q2w3e4r5t) που είναι εύκολο να το θυμούνται αλλά και εύκολο να το μαντέψουν. Περισσότερο σύνθετες πολιτικές κωδικών πρόσβασης μπορούν να αχρηστευθούν από μη-τεχνολογικά μέσα.

Στις μικρές και μεσαίες επιχειρήσεις, οι διαχειριστές του συστήματος συχνά παίρνουν τον ρόλο των διαχειριστών του δικτύου και του έργου καθώς και των αναλυτών ασφαλείας. Συνεπώς ένας δυσαρεστημένος διαχειριστής συστήματος θα είναι ένα κύριο πρόβλημα ασφαλείας λόγω του φόρτου εργασίας και του ποσού ευθύνης που κατέχει. Με τα δικαιώματα της πλήρης πρόσβασης, ένας διαχειριστής μπορεί να σχεδιάσει μια λογική βόμβα, απροστάτευτους λογαριασμούς ή να συντελέσει στην διαρροή ευαίσθητων πληροφοριών που μπορούν να επηρεάσουν την σταθερότητα και την φήμη της επιχείρησης σε μεγάλο βαθμό.

Επιπλέον, σε πολλές περιπτώσεις ο διαχειριστής συστήματος είναι το πρόσωπο που ορίζει τους κωδικούς πρόσβασης για σημαντικές υπηρεσίες ή servers. Όταν αποχωρεί από την οργάνωση αυτοί οι κωδικοί δεν αλλάζουν και συνεπώς δημιουργείται κενό ασφαλείας.

Μια νεοσύστατη εταιρεία που ονομάζεται Journal Space δεν διέθετε αντίγραφα ασφαλείας και ο πρώην διαχειριστής αποφάσισε να εξαφανίσει την κύρια βάση δεδομένων. Αυτό αποδείχτηκε καταστροφικό για την εταιρεία η οποία κατέληξε να ζητάει από τους χρήστες να ανακτήσουν το περιεχόμενό της από την μνήμη του Google. Η ομάδα διαχείρισης της εταιρείας μπορεί επίσης να έχει διοικητικά προνόμια στους προσωπικούς υπολογιστές ή στους φορητούς. Οι λόγοι ποικίλλουν, αλλά μπορεί να θέλετε να εγκαταστήσετε νέο λογισμικό ή απλά να έχετε τον έλεγχο των μηχανημάτων σας. Το πρόβλημα με αυτό το σενάριο είναι ότι μια μηχανή που έχει παραβιαστεί είναι το μόνο που χρειάζεται ένας επιτιθέμενος για να επιτεθεί στην εταιρεία.

Ο λόγος που μια εταιρεία γίνεται στόχος επίθεσης είναι μια συγκεκριμένη ευπάθεια ενός πακέτου λογισμικού. Ακόμα και όταν οι λογαριασμοί χρηστών στο δίκτυο υποτίθεται ότι έχουν μειωμένα προνόμια, υπάρχουν φορές στις οποίες προκύπτουν αυξημένα προνόμια. Παραδείγματος χάριν, ένας διαχειριστής που παραδίδει μια εργασία σε έναν άλλον διαχειριστή, μπορεί να διατηρήσει τα προνόμια για αρκετά χρόνια μετά την παράδοση. Οπότε αν ο λογαριασμός του παραβιαστεί τότε ο εισβολέας αποκτά πρόσβαση στην εργασία. Οι εργαζόμενοι με φορητές συσκευές και φορητούς υπολογιστές μπορούν να θέσουν σε σοβαρό κίνδυνο τα δεδομένα της εταιρείας ειδικά όταν συνδέονται μέσω του ασυρμάτου δικτύου ή του δικτύου του ξενοδοχείου τους.

Σε πολλές περιπτώσεις, ανεπαρκής ή καθόλου κρυπτογράφηση χρησιμοποιείται και οποιοσδήποτε "ενδιάμεσος" μπορεί να δει και να τροποποιήσει την κίνηση του δικτύου. Αυτή μπορεί να είναι η αρχή μιας εισβολής που οδηγεί την εταιρεία σε συμβιβασμό των δικτύων και των λογαριασμών.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# 4. Διαχείριση περιστατικών παραβίασης σε ΜΜΕ

Η αντιμετώπιση περιστατικών είναι κάτι περισσότερο από την διαχείριση της παραβίασης που πραγματοποιήθηκε από έναν εξωτερικό εισβολέα. Είναι η ικανότητα της διαχείρισης μιας ποικιλίας περιστατικών τα οποία κυμαίνονται από έναν μικρό ιό έως μια σημαντική απώλεια δεδομένων της επιχείρησης, που ξεκίνησε από έναν κακόβουλο χρήστη εντός ή εκτός της επιχείρησης. Πολλές επιχειρήσεις θεωρούν τους εαυτούς τους ασφαλείς από τέτοια περιστατικά επειδή επεξεργάζονται δεδομένα τα οποία δεν είναι ιδιαίτερα χρήσιμα σε εξωτερικούς παράγοντες, είτε επειδή είναι τόσο μικρές επιχειρήσεις που δεν μπορούν να φανταστούν ότι κάποιος θα τους εντοπίσει και τους επιτεθεί ή απλά πιστεύουν ότι δεν έχουν αρκετούς πόρους ώστε να προσελκύσουν κακόβουλους χρήστες. Όλες αυτές οι υποθέσεις είναι εσφαλμένες.

Μια ιδιαίτερη σκληρή πραγματικότητα είναι ότι σύμφωνα με το τμήμα Ηλεκτρονικής Δίωξης του FBI, η κατάχρηση εμπιστευτικών πληροφοριών της πρόσβασης στο δίκτυο ή στο email αποτελούσε το 72% έως το 79% του συνόλου των περιστατικών. Είναι σημαντικό για τις επιχειρήσεις να λάβουν μια καθολική προσέγγιση για την κατάλληλη ασφάλεια που είναι για όλους τους τύπους των απειλών, όχι μόνο για τις απειλές που γίνονται πρωτοσέλιδα. Αργά ή γρήγορα, όλες οι επιχειρήσεις θα αντιμετωπίσουν ένα περιστατικό και αυτές που είναι καλά προετοιμασμένες θα επιβιώσουν με το ελάχιστο δυνατό κόστος σε απώλειες.

## 4.1 Επισκόπηση των Έξι βημάτων:

### 4.1.1 Preparation (Προετοιμασία)

Το πρώτο βήμα για την αντιμετώπιση οποιουδήποτε περιστατικού είναι η καλή προετοιμασία. Όταν το περιστατικό συμβεί, επικρατεί πανικός και φόβος γι αυτό είναι καλύτερα η γνώση του τι πρέπει να γίνει ακριβώς. Σε ένα περιστατικό επίθεσης δεν είναι εύκολο να ληφθούν δραστικές αποφάσεις για την εξέλιξη αυτού. Παραδοσιακά αυτό το βήμα περιλαμβάνει πολλές πολιτικές καθώς και μηνιαίες εκθέσεις, επιλογή της ομάδας αντιμετώπισης του περιστατικού, σχέδια αντιμετώπισης, σχέδια επικοινωνίας και πακέτα λογισμικού που μπορούν να χρησιμοποιηθούν στην περίπτωση του περιστατικού.

### 4.1.2 Identification (Αναγνώριση)

Το δεύτερο βήμα της διαχείρισης των περιστατικών είναι η φάση της αναγνώρισης. Κατά την διάρκεια αυτής, η επιχείρηση συλλέγει δεδομένα, αναλύσεις, και στη συνέχεια προσδιορίζει εάν έχει συμβεί κάποιο περιστατικό. Ο χειριστής του περιστατικού πρέπει ήρεμα να εκτιμήσει την κατάσταση, να είναι έτοιμος να επικοινωνήσει, και να είναι έτοιμος να χειριστεί όλα τα αποδεικτικά στοιχεία έτσι ώστε να μπορέσουν να χρησιμοποιηθούν αργότερα.

### 4.1.3 Containment (Περιορισμός)

Ο στόχος της φάσης του περιορισμού είναι να αποτραπεί κάθε περαιτέρω ζημιά. Εάν ένα περιστατικό έχει συμβεί, είναι πιθανόν να έχει ήδη προκληθεί κάποιο ποσοστό ζημιάς. Σε αυτή την φάση η ζημιά περιορίζεται ώστε να μην μπορεί να εξαπλωθεί σε άλλα δεδομένα, συστήματα ή δίκτυα. Οι αρχικές δραστηριότητες που θα συμβούν σε αυτήν την φάση περιλαμβάνουν κι εκείνες όπως είναι η αποσύνδεση των καλωδίων του δικτύου ή της ισχύος, η τροποποίηση των κανόνων του Firewall και η αλλαγή στις πληροφορίες του DNS. Μόλις η εξάπλωση έχει σταματήσει, τότε είναι καιρός να δημιουργηθεί ένα αντίγραφο ασφαλείας του συστήματος το οποίο να μπορεί να χρησιμοποιηθεί για ανάλυση. Είναι επίσης καλή ιδέα να δημιουργηθεί ένα δεύτερο αντίγραφο του συστήματος που θα αποθηκευτεί ή θα χρησιμοποιηθεί για εγκληματολογική ανάλυση. Αν το σύστημα που παραβιάστηκε πρέπει να παραμείνει στην παραγωγή, τότε θα πρέπει να συμβούν επιπρόσθετες ενέργειες περιορισμού . Αυτές έχουν ως στόχο να κρατήσουν προσωρινά το σύστημα σε λειτουργία ενώ ένα

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

άλλο σύστημα είναι υπό κατασκευή ή όσο λαμβάνονται οι αποφάσεις ως προς το μακροπρόθεσμο σχέδιο αποκατάστασης για το σύστημα που είναι σε κίνδυνο.

### 4.1.4 Eradication (Εξάλειψη)

Η φάση της εξάλειψης είναι αρκετά δύσκολη, καθώς απαιτεί την πλήρη αφαίρεση κάθε κακόβουλου κώδικα και τα δεδομένα που άφησε ο εισβολέας, αλλά απαιτεί επίσης και την διόρθωση των τρωτών σημείων που εκμεταλλεύτηκαν οι hackers για να εισβάλουν. Αυτό είναι δύσκολο, γιατί δεν μπορεί να γίνει μέχρι να καθοριστεί η αιτία του συμβάντος. Μόλις η αιτία έχει καθοριστεί, το σύστημα μπορεί να ανακατασκευαστεί από ένα αντίγραφο ασφαλείας. Σε περίπτωση που δεν υπάρχει αντίγραφο ασφαλείας, τότε το σύστημα θα πρέπει να επανεγκατασταθεί από το μηδέν, συμπεριλαμβανομένου και του λειτουργικού συστήματος.

### 4.1.5 Recovery (Ανάκαμψη)

Στην φάση της ανάκαμψης, οι εργασίες επιστρέφουν στους κανονικούς τους ρυθμούς. Το σύστημα είτε έχει ξαναχτιστεί από το μηδέν είτε από ένα αντίγραφο ασφαλείας και είναι έτοιμο να επικυρωθεί για την παραγωγή. Αυτό περιλαμβάνει την επαλήθευση ότι το σύστημα είναι ασφαλές και ότι δε θα ξανά προσβληθεί από την ίδια ή παρόμοια επίθεση μόλις ξανά τεθεί σε σύνδεση.

### 4.1.6 Lessons learned (Διδάγματα)

Το τελικό στάδιο της αντιμετώπισης των περιστατικών είναι η γνώση από τα λάθη του παρελθόντος. Κανένας οργανισμός δεν είναι τέλειος και ως εκ τούτου είναι σημαντικό να αφιερωθεί ο χρόνος που απαιτείται για την αξιολόγηση του περιστατικού, τι το προκάλεσε και αν αυτό θα συμβεί ξανά. Παραδοσιακά δημιουργείται μια αναφορά και μια συνεδρίαση όταν εξετάζονται αυτές οι πληροφορίες.

## 4.2 Analysis of the Six Steps for Small to Medium Enterprises.

### 4.2.1 Preparation (Προετοιμασία):

Όπως αναφέρθηκε προηγουμένως η προετοιμασία είναι το κλειδί για τον επιτυχή χειρισμό οποιουδήποτε περιστατικού. Οι μικρές και μεσαίες επιχειρήσεις θα έχουν μια ελαφρώς διαφορετική προετοιμασία από τις μεγάλες επιχειρήσεις με περισσότερους πόρους. Θα περιγραφούν οι βασικοί άξονες της προετοιμασίας:

Διαχειριστής περιστατικού

Το πρώτο βήμα στο στάδιο της προετοιμασίας είναι να οριστεί το ποιος θα χειριστεί το περιστατικό. Μερικές μικρές και μεσαίες επιχειρήσεις επιλέγουν να χειριστούν περιστατικά οι ίδιες, κάποιοι επιλέγουν ένα έμπιστο τρίτο πρόσωπο και κάποιοι έναν συνδυασμό των εσωτερικών και εξωτερικών πόρων. Είναι ζωτικής σημασίας αυτό να καθοριστεί πριν εκδηλωθεί το περιστατικό, ώστε να αντιμετωπιστεί με τον καλύτερο δυνατό τρόπο. Μόλις ληφθεί αυτή η απόφαση, οι οδηγίες χειρισμού του περιστατικού θα πρέπει να δημιουργηθούν. Αυτές οι οδηγίες θα χρησιμεύσουν ως μια έγκυρη πηγή για τους χειριστές του περιστατικού και θα περιλαμβάνουν μια ολοκληρωμένη βήμα προς βήμα διαδικασία.

Σχεδιασμός των οδηγιών διαχείρισης του περιστατικού

Οι οδηγίες αντιμετώπισης περιστατικών είναι εκείνα τα έγγραφα που χρησιμοποιούνται από όλα τα άτομα που εμπλέκονται στον χειρισμό του περιστατικού και πρέπει να αφήνουν όσο το δυνατόν λιγότερες αποφάσεις που

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

λήφθηκαν στην μέση του συμβάντος. Τα κομμάτια που αναγράφονται παρακάτω είναι ένα πλήρες επεισόδιο χειρισμού με οδηγίες για καθένα από τα έξι στάδια. Τα στοιχεία περιλαμβάνουν τα ακόλουθα :

**Call list:** Η λίστα των κλήσεων είναι ποιος θα κληθεί και πότε. Εάν το περιστατικό χρησιμοποιεί εσωτερικούς πόρους η λίστα θα πρέπει να περιλαμβάνει τους τεχνικούς που έχουν εκπαιδευτεί στην διαχείριση των περιστατικών. Θα πρέπει να περιλαμβάνει και την διοίκηση επίσης. Οι διευθυντές των μικρών και μεσαίων επιχειρήσεων θα πρέπει να εκπαιδεύονται στην ασφάλεια και να κατανοούν την διαδικασία που θα χρησιμοποιήσει η επιχείρησή τους στην περίπτωση μιας παραβίασης. Επιπλέον θα πρέπει να περιλαμβάνουν τοπικές αρχές επιβολής του νόμου στην περίπτωση που η παραβίαση επηρεάζει και την τοπική κοινότητα στο σύνολό της. Εάν χειρίζεται το περιστατικό ένα έμπιστο τρίτο μέλος τότε θα πρέπει να συμπεριλαμβάνονται τα στοιχεία επικοινωνίας για αυτόν. Τέλος, αν η επιχείρηση έχει καθορίσει τα περιστατικά ιών να αντιμετωπίζονται εσωτερικά και οι εισβολές να αντιμετωπίζονται εξωτερικά τότε ο σχεδιασμός θα είναι σαφής στις οδηγίες χειρισμού του περιστατικού.

**Initial response:** Η αρχική απάντηση είναι τι πρέπει να κάνετε την στιγμή που υποψιάζεστε ένα περιστατικό. Αυτό θα πρέπει να περιλαμβάνει ερωτήσεις που βοηθούν το χειριστή του περιστατικού να προσδιορίσει εάν υπάρχει πραγματικά περιστατικό. Επίσης θα πρέπει να περιλαμβάνει οδηγίες για κάθε τύπο συστήματος σε όλη την επιχείρηση. Για παράδειγμα, η επιχείρηση μπορεί να θέλει να αποσυνδέσει την βάση οικονομικών δεδομένων από το δίκτυο, εάν υπάρχει περιστατικό, αλλά μπορεί να θέλει να παραμείνει συνδεδεμένος ο web server. Κάθε ενέργεια που πραγματοποιείται από τον χειριστή του περιστατικού θα πρέπει να λαμβάνεται υπόψιν και να διατηρείται. Όπως αναφέρθηκε και πάνω, ένα μέρος της αρχικής απάντησης είναι η επικοινωνία με τους σωστούς ανθρώπους οι οποίοι πρέπει να είναι ορισμένοι με σαφήνεια.

**Response strategy:** Τώρα που έχει επιβεβαιωθεί το περιστατικό και τα κατάλληλα άτομα έχουν ειδοποιηθεί, το επόμενο βήμα είναι το πως ο οργανισμός θα επιλέξει να διαχειριστεί το περιστατικό. Στην περίπτωση που έχει οριστεί ένα έμπιστο τρίτο πρόσωπο για τον χειρισμό των περιστατικών τότε η στρατηγική της απάντησης είναι δική του υπόθεση. Αν χειρίζεται η εταιρεία τα περιστατικά τότε η στρατηγική απάντηση θα πρέπει να καθοριστεί και να δοκιμαστεί.

**Recovery:** Σε αυτήν την ενότητα περιλαμβάνονται πληροφορίες για το πως θα ανακάμψει πλήρως μια λειτουργική κατάσταση (ένα λειτουργικό σύστημα) και περιλαμβάνει τα πέντε από τα έξι συνολικά βήματα. Περιλαμβάνει επιχειρησιακές λεπτομέρειες για κάθε βασικό σύστημα εντός του οργανισμού. Σε αυτό το κομμάτι, ακόμα και αν χρησιμοποιηθεί ένα αξιόπιστο τρίτο πρόσωπο, θα πρέπει να συντονιστεί με τους εσωτερικούς τεχνικούς πόρους. Αυτή η ενότητα αποτελεί την γέφυρα μεταξύ της κατάστασης εκτάκτου ανάγκης και την επάνοδο σε μια σταθερή κατάσταση αφότου το περιστατικό έχει αντιμετωπιστεί.

**Lessons Learned report:** Περιλαμβάνει μια σύντομη έκθεση που περιγράφει το συμβάν και ποιες ενέργειες λαμβάνονται ώστε να συνεχίσει η επιχείρηση την λειτουργία της και να αποφευχθεί η επανάληψη του συμβάντος.

Εργαλεία στη φάση της προετοιμασίας

Εκτός του ότι πρέπει να είναι προετοιμασμένοι για το περιστατικό γνωρίζοντας ποιος θα το χειριστεί και ποια βήματα θα ακολουθήσει, η επιχείρηση πρέπει επίσης να παρέχει στον χειριστή του περιστατικού τον απαραίτητο εξοπλισμό. Σε αυτήν την ενότητα θα δοθούν παραδείγματα των εργαλείων που μπορούν να χρησιμοποιηθούν.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

**Event logs:** Μία από τις πιο σημαντικές πηγές δεδομένων όταν συμβεί ένα περιστατικό είναι οι καταγραφές των αρχείων, οι οποίες για να προστατευθούν από τον εισβολέα αποστέλλονται σε ένα κεντρικό υπολογιστή. Μια καλή λύση για τα διαφορετικά περιβάλλοντα είναι το Snare. Το **Snare** παρέχει παράγοντες για πολλά λειτουργικά συστήματα συμπεριλαμβανομένων των Windows, Unix και λιγότερο συχνά σύστημα όπως το Tru64. Το Snare δεν είναι δωρεάν επομένως αν δεν επιθυμείτε την αγορά του μπορείτε να χρησιμοποιήσετε μια διαφορετική λύση. Μια πιθανή λύση είναι να εγκατασταθεί Linux υποδοχή και να χρησιμοποιηθεί syslog-ng όπου θα αποθηκευτούν οι καταγραφές. Το sys-log είναι εύκολο στην δημιουργία και θα συλλέγει τα αρχεία καταγραφής, ωστόσο δεν κάνει καμία ανάλυση. Η ανάλυση θα πρέπει να συμπληρωθεί ξεχωριστά. Μία καλή λύση για την ανάλυση των αρχείων καταγραφής είναι το **SEC**(Simple Event Correlator), είναι ένα αρκετά ευέλικτο εργαλείο αλλά απαιτεί εξειδικευμένη ρύθμιση. Αφού έχει επιλεχθεί η λύση, θα πρέπει να ρυθμιστεί ώστε να αποστέλλονται μόνο τα περισσότερο σημαντικά γεγονότα. Παραδείγματα από σημαντικά γεγονότα είναι:

επιτυχείς και ανεπιτυχείς προσπάθειες σύνδεσης,

πρόσβαση σε σημαντικά αρχεία ή καταλόγους

έλεγχος διαδικασίας

αλλαγές στα δικαιώματα των χρηστών

διαχείριση του λογαριασμού

αλλαγές στην πολιτική ασφαλείας

διακοπή λειτουργίας του συστήματος ή επανεκκίνηση

Οι servers δεν είναι τα μόνα συστήματα στο δίκτυο που παράγουν χρήσιμα αρχεία καταγραφής. Οι δρομολογητές είναι επιπλέον γεμάτοι από ενδιαφέρουσες πληροφορίες, αλλά και πάλι οι καταγραφές είναι που θα αποθηκευτούν στην κεντρική υποδοχή των καταγραφών για γρήγορη και αξιόπιστη πρόσβαση. Τα αρχεία καταγραφής αποστέλλονται από τους δρομολογητές στον syslog-ng server και μπορεί να χρησιμοποιηθεί το SEC για να ερευνηθούν ενδιαφέροντα περιστατικά όπως μη εξουσιοδοτημένη κίνηση.

**Network-based Intrusion Detection Systems (NIDS)**: Τα Network-based Intrusion Detection Systems (NIDS) είναι αρκετά χρήσιμα για την αποτροπή των επιτυχημένων παραβιάσεων στα συστήματα ασφαλείας, αλλά επίσης και για την διερεύνηση των περιστατικών. Υπάρχουν διάφορα εμπορικά προϊόντα αλλά υπάρχουν και μερικές καλές δωρεάν λύσεις ή χαμηλού κόστους. Ένα από τα πιο ευρέως διαδεδομένα είναι το **Snort**. Το λογισμικό του Snort παρακολουθεί έναν host και παράγει προειδοποιήσεις εάν ένα πακέτο ταιριάζει με μια συγκεκριμένη υπογραφή-περιγραφή. Η ειδοποίηση αυτή αποθηκεύεται ώστε να εξεταστεί και από τον διαχειριστή του συστήματος. Αυτό από μόνο του δεν είναι αρκετό, γιατί η ειδοποίηση πρέπει να είναι προσβάσιμη και ο τρόπος με τον οποίο επιτυγχάνεται αυτό είναι η εγκατάσταση του συστήματος βάσης δεδομένων BASE σε συνδυασμό με το Snort. Με αυτόν τον τρόπο οι ειδοποιήσεις ταξινομούνται και επιτρέπεται στους διαχειριστές να τις παρακολουθούν ή να τις αφαιρούν αναλόγως με την περίπτωση. Ωστόσο αυτό το πακέτο λογισμικού δεν έχει ενημερωθεί εδώ και αρκετό καιρό οπότε ίσως χρειαστεί να εξεταστούν μερικές εναλλακτικές λύσεις. Μία καλή λύση είναι το **Activeworx Security Center**. Πρόκειται για μια ολοκληρωμένη λύση που επιτρέπει την απλοποιημένη διαχείριση των συμβάντων. Επίσης προσφέρει μια λύση στην καταγραφή των αρχείων που καλύπτει τις ανάγκες που περιγράφονται στην προηγούμενη ενότητα. Μια άλλη πιθανή λύση είναι αυτή του **Nessus**. Υποστηρίζει

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

την ασφάλεια των δικτύων και έχει μια ολοκληρωμένη λύση παρακολούθησης της ασφάλειας, σαν το Activeworx, που θα ενσωματώσει τον αισθητήρα διαχείρισης με την διαχείριση του αρχείου καταγραφής για μια ενιαία και εύχρηστη λύση. Ωστόσο αυτή η λύση είναι αρκετά ακριβή. Για μια εντελώς δωρεάν λύση για ένα μικρό δίκτυο με έναν μόνο αισθητήρα Snort και έναν syslog host μπορεί να δοκιμαστεί και το **Anval**. Η σωστή διαμόρφωση των αισθητήρων είναι σημαντική για να τους αξιοποιήσει η επιχείρηση ενώ οι κακώς ρυθμισμένοι δεν προσφέρουν καμία αξία. Το πρώτο βήμα για την εξασφάλιση μιας καλής λύσης είναι να υπάρχουν αισθητήρες στα κρίσιμα σημεία του δικτύου. Αν ο οργανισμός είναι αρκετά μικρός ώστε να έχει μόνο ένα τμήμα τότε ένας αισθητήρας είναι αρκετός. Ωστόσο αν ο οργανισμός έχει πολλαπλά τμήματα και μια DMZ θα χρειαστεί να εγκατασταθούν περισσότεροι από έναν αισθητήρες. Είναι μια καλή ιδέα να υπάρχει ένας αισθητήρας στην DMZ όπου θα παρακολουθεί την κίνηση και θα λαμβάνει πολλαπλές ειδοποιήσεις. Ο εσωτερικός αισθητήρας θα λάβει λιγότερες ειδοποιήσεις αλλά αυτές θα είναι πιο κρίσιμες. Αν ο DMZ αισθητήρας δει μια προσπάθεια επίθεσης, ίσως να μην είναι έκπληξη καθώς θα είναι προσβάσιμη στο διαδίκτυο. Εάν ένας από τους εσωτερικούς αισθητήρες δει μια επίθεση από το εξωτερικό περιβάλλον δεν υπάρχει λόγος ανησυχίας. Οι εσωτερικοί hosts θα πρέπει να προστατεύονται από την άμεση πρόσβαση στο Internet στις περισσότερες περιπτώσεις(εκτός της περιήγησης στο διαδίκτυο φυσικά).

**Host-based Intrusion Detection System (HIDS):**'Ενα άλλο χρήσιμο εργαλείο για την ανάλυση ενός περιστατικού είναι ένα σύστημα ανίχνευσης βασισμένο σε host. Αυτό το εργαλείο θα ελέγξει τα κρίσιμα αρχεία και θα ενημερώσει εάν κάποιο αρχείο (όπως το ps executable σε Unix ή το lsass.exe στα Windows) έχει τροποποιηθεί. Το πιο εμπορικό εργαλείο είναι το **Tripwire** αλλά είναι πολύ ακριβό. Εναλλακτική λύση αποτελεί το **Samhain**. Για να το χρησιμοποιήσετε θα εγκαταστήσετε τους παράγοντές του στους servers και θα εγκαταστήσετε ένα μόνο server ως κονσόλα διαχείρισης. Είναι εύκολο στην ρύθμιση και στην χρήση και λειτουργεί και σε Unix και Windows. Ο Yule log server θα συλλέξει τα δεδομένα και τις καταγραφές από τους πελάτες και θα παρακολουθεί τα αρχεία των ρυθμίσεων για κάθε παράγοντα. Οι εκθέσεις αποθηκεύονται σε μια βάση δεδομένων, Oracle, MySQL, PostgreSQL. Τέλος η **web-based Beltane** κονσόλα θα πρέπει να εγκατασταθεί στον server. Επιτρέπει την απλή διαχείριση των πελατών και των αναφορών. Το Samhain μπορεί να ρυθμιστεί ώστε να ελέγχει πολλά ενδιαφέροντα πράγματα μερικά από τα οποία είναι:

ακεραιότητα του πυρήνα

ανοιχτές θύρες

κρυφές διεργασίες

ακεραιότητα αρχείων

**Time synchronization:** Είναι σημαντικό να συγχρονιστεί η ώρα της συσκευής καθώς οι διάφορες συσκευές διαφωνούν μεταξύ τους για την ώρα εκδήλωσης ενός συμβάντος και παράγουν πληροφορίες χωρίς νόημα. Το πρωτόκολλο **Network Time Protocol(NTP)** μπορεί να χρησιμοποιηθεί για τον συγχρονισμό των ρολογιών στις συσκευές. Αν και τα περισσότερα σύστηματα το διαθέτουν ήδη το NTP, στην περίπτωση που δεν είναι εγκατεστημένο μπορείτε να το βρείτε στην διεύθυνση ntp.org project. Μια καλή σύσταση αρχιτεκτονικής είναι να επιλεχθεί ένα ή δύο time servers που θα συγχρονιστούν με τους time servers του διαδικτύου. Στη συνέχεια οι υπόλοιπες συσκευές στο δίκτυο θα συγχρονιστούν με ένα ή δύο από τους τοπικούς time servers.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

### 4.2.2 Identification (Αναγνώριση)

Σε κάθε οργανισμό η ταυτοποίηση του περιστατικού δεν είναι ευθύνη μόνο του προσωπικού IT. Αυτό ισχύει ακόμη περισσότερο σε μικρές και μεσαίες επιχειρήσεις. Σε μικρότερους οργανισμούς το προσωπικό IT θα είναι πιο πιθανό να παρατηρήσει ορισμένα είδη δραστηριοτήτων αλλά το υπόλοιπο προσωπικό ίσως να παρατηρήσει τα συμπτώματα μιας επίθεσης όπως αργό δίκτυο ή αργή απόδοση στο σύστημα. Είναι σημαντικό να ληφθούν τα παραπάνω σοβαρά υπόψη καθώς μπορεί να είναι δείκτες περιστατικών.

Τα περιστατικά συμβαίνουν μερικές φορές πολύ γρήγορα και για αυτό είναι σημαντικό ο χειριστής του περιστατικού να είναι πρόθυμος να τα αντιμετωπίσει και να σημάνει ψευδή συναγερμό αν αυτό υφίσταται. Ένας οργανισμός είναι σε καλύτερη θέση όταν αντιδράσει γρήγορα σε ένα ύποπτο περιστατικό (ακόμα και ακίνδυνο) παρά να παραμείνει αδρανής μέχρι να επέλθει σοβαρή ζημιά. Μόλις ένα περιστατικό είναι ύποπτο ο χειριστής θα πρέπει να συμβουλευτεί τις οδηγίες αντιμετώπισης περιστατικού που δημιουργήθηκαν στο στάδιο της προετοιμασίας και να αρχίσει την συμπλήρωση των πληροφοριών. Είναι κρίσιμης σημασίας ο χειριστής του περιστατικού να γράψει όσο το δυνατόν περισσότερες πληροφορίες μπορεί. Αν ο χειριστής καταφέρει και καταγράψει πολύ γρήγορα τις ενέργειές του τότε γρήγορα θα επιλύσει και το περιστατικό. Οι σημειώσεις είναι το κλειδί για την κατανόηση του περιστατικού και δίνουν την δυνατότητα στο να αποτραπούν παρόμοια περιστατικά στο μέλλον. Είναι μια καλή ιδέα να εκτυπωθούν αντίγραφα των φύλλων και να τα συμπεριλάβουν μαζί με τις οδηγίες χειρισμού του περιστατικού. Κάνουν πολύ συγκεκριμένες συστάσεις και οργανώνονται ως εξής:

Ασυνήθιστες διαδικασίες και υπηρεσίες (Unix)

Ψάξτε για ασυνήθιστες διαδικασίες με ps-aux

Ερευνήστε για ασυνήθιστες διαδικασίες με lsof-p [pid]

Ασυνήθιστες διαδικασίες και υπηρεσίες (Windows)

Ψάξτε για ασυνήθιστες διαδικασίες στην Διαχείριση Εργασιών(taskmgr.exe)

Ψάξτε για ασυνήθιστες υπηρεσίες δικτύου(net start)

Ασυνήθιστα αρχεία και κλειδιά μητρώου(Unix)

Ψάξτε για ασυνήθιστα αρχεία SUID root με find /-uid 0-perm-4000-print

Ψάξτε για ασυνήθιστα μεγάλα αρχεία με find/-size +1000K-print

Ψάξτε για αρχεία με τελείες και κενά στην ονομασία τους:

Βρείτε / -όνομα `` `` ... -print

Βρείτε / -όνομα `` `` .. -print

Βρείτε / όνομα ``. `` -print

Βρείτε / -όνομα `` -print

Ασυνήθιστα αρχεία και κλειδιά μητρώου(Windows)

Ελέγξτε για σημαντική μείωση στον ελεύθερο χώρο στον δίσκο με dir c:\

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Ψάξτε για ασυνήθιστα μεγάλα αρχεία χρησιμοποιώντας το εργαλείο αναζήτησης και στην επιλογή του μεγέθους τουλάχιστον 10000KB

Ασυνήθιστη χρήση του δικτύου(Unix)

Ψάξτε για ετερόκλητη λειτουργία με σύνδεση ip | grep PROMISC.

Ψάξτε για ασυνήθιστες θύρες με lsof-i v netstat-nap

Ψάξτε για ασυνήθιστες καταχωρήσεις ARP με arp-a

Ασυνήθιστη χρήση του δικτύου(Windows)

Ψάξτε για φακέλους με net view 127.0.0.1

Ψάξτε για ανοιχτές συνεδρίες και ποιος τις έχει

Ψάξτε τι συνεδρίες έχει ο υπολογιστής με το δίκτυο

Ψάξτε την δραστηριότητα NetBIOS με nbstat-S

Ψάξτε για ασυνήθιστες θύρες με netstat-na

Ασυνήθιστες προγραμματισμένες εργασίες(Unix)

Ψάξτε για cron jobs με crontab-u root-l

cat/etc/crontab

ls/etc/cron

Ασυνήθιστες προγραμματισμένες εργασίες(Windows)

Ψάξτε για προγραμματισμένες εργασίες με at

Επίσης ελέγξτε τις προγραμματισμένες εργασίες στα εργαλεία του συστήματος.

Ασυνήθιστους λογαριασμούς(Unix)

Ψάξτε στο /etc/passwd για νέους λογαριασμούς, ειδικά εκείνους με UID ή GID του 0 με less/etc/passwd και grep :0: /etc/passwd

Ασυνήθιστους λογαριασμούς(Windows)

Ψάξτε για λογαριασμούς στην ομάδα διαχειριστών με lusrmgr.msc

Ασυνήθιστες καταχωρήσεις ημερολογίου (Unix)

Ψάξτε για ύποπτα περιστατικά όπως "εισαγωγή σε ετερόκλητη λειτουργία, μεγάλο αριθμό αποτυχιών ελέγχου ταυτότητας, προγράμματα RPC με μεγάλο αριθμό από παράξενους χαρακτήρες, μεγάλο αριθμό σε λάθη του δικτύου".

Ασυνήθιστες καταχωρήσεις ημερολογίου(Windows)

Εκτελέστε το **event viewer** με το eventvwr.msc και αναζητήστε ύποπτα γεγονότα όπως "Η υπηρεσία καταγραφής γεγονότων σταμάτησε", "η προστασία των αρχείων Windows δεν είναι ενεργή", "η υπηρεσία telnet ξεκίνησε" ή μεγάλο αριθμό αποτυχημένων προσπαθειών σύνδεσης.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Επίσης χρησιμοποιήστε τα εργαλεία που αναφέρθηκαν στην ενότητα της προετοιμασίας. Εάν έχει εγκατασταθεί το Snare, Snort και Samhain θα υπάρχει ένα πλούτος πληροφοριών. Θα μπορείτε με ευκολία να δείτε μέσω του Samhain αν τα κρίσιμα αρχεία έχουν αλλάξει. Με το Snort μπορείτε να δείτε αν κακόβουλα πακέτα έχουν εισέλθει στο δίκτυό και με το Snare μπορείτε να ελέγξετε για ασυνήθιστα συμβάντα στο σύστημά σας γρήγορα και αποτελεσματικά.

Κανένα από αυτά τα στοιχεία δεν είναι ένδειξη ύπαρξης ενός συμβάντος. Μάλλον αυτά τα κομμάτια των πληροφοριών θα πρέπει να θεωρούνται στο σύνολο όταν ένα περιστατικό έχει συμβεί.

Οι οδηγίες χειρισμού του περιστατικού περιλαμβάνουν μορφές που θα βοηθήσουν τους χειριστές να διατηρούν τις πληροφορίες που συνέλεξαν κατά την διάρκεια αυτής της φάσης. Όπως επιτάσσει το δείγμα της διαχείρισης του περιστατικού, θα πρέπει να απαντηθούν ερωτήσεις από τον χειριστή του περιστατικού για να τον βοηθήσει να θεωρήσει την έκταση και την σοβαρότητα αυτού. Αυτά τα ερωτήματα βοηθούν τον χειριστή του περιστατικού να καταλάβει πως θα ανταποκριθεί και ποιες στρατηγικές θα ακολουθήσει αμέσως μετά την αναγνώριση.

### 4.2.3 Containment (Περιορισμός)

Στην φάση αυτήν ο χειριστής ξεκινάει να κάνει αλλαγές στο σύστημα ή στο δίκτυο. Αυτές οι αλλαγές γίνονται με στόχο τον περιορισμό του περιστατικού από το να λάβει διαστάσεις. Σύμφωνα με την διαδικασία των έξι σταδίων, ο περιορισμός έχει τρεις φάσεις: βραχυπρόθεσμος, δημιουργία αντιγράφων ασφαλείας και μακροπρόθεσμος.

Βραχυπρόθεσμος περιορισμός

Είναι οι ενέργειες που κάνει ο χειριστής για να σταματήσει απλά τον εισβολέα (πρόσωπο, ιούς, κακόβουλο λογισμικό) από το να κάνει μεγαλύτερη πρόοδο. Τα παρακάτω βήματα κατά πάσα πιθανότητα θα ειδοποιήσουν τον επιτιθέμενο ότι η επιχείρηση έχει ανακαλύψει την παράβαση. Έτσι πριν την ανάληψη δράσης, η επιχείρηση χρειάζεται να αποφασίσει αν θέλει να αναλύσει την κατάσταση χωρίς να προειδοποιήσει τον επιτιθέμενο και να τον συλλάβει επ' αυτοφώρω ή αν θέλει να σταματήσει αμέσως το περιστατικό και να αρχίσει τις φάσεις εξάλειψης το συντομότερο δυνατόν. Στην περίπτωση που η οργάνωση δεν ανησυχεί για να ειδοποιήσει τον hacker για την έρευνα, μερικοί τρόποι δράσης είναι οι παρακάτω:

αποσύνδεση του καλωδίου δικτύου

αποσυνδέοντας το καλώδιο της τροφοδοσίας(καταστρέφει την μνήμη και ίσως τον σκληρό δίσκο)

απομόνωση του συστήματος μέσω του διακόπτη ή άλλα εργαλεία διαχείρισης του δικτύου όπως φίλτρα firewall.

αλλαγή του DNS έτσι ώστε το όνομα να δείχνει άλλη διεύθυνση IP.

Όλες οι ενέργειες θα πρέπει να γίνονται βάσει των οδηγιών της αντιμετώπισης του περιστατικού. Έχοντας ένα αναπτυγμένο σχέδιο που επιτρέπει στους χειριστές των περιστατικών να ανταποκριθούν άμεσα σε επείγουσες καταστάσεις με αυτοπεποίθηση και αξιοπιστία. Ο χειριστής του περιστατικού πρέπει να χρησιμοποιήσει τις οδηγίες χειρισμού για την παρακολούθηση των πληροφοριών του περιστατικού και στην συνέχεια τις πιθανές πορείες δράσης, σύμφωνα με τις συστάσεις. Κάθε ενέργεια που κάνει ο χειριστής του περιστατικού θα επηρεάσει το υπόλοιπο της επιχείρησης, έτσι είναι πολύ σημαντικό να έχει ληφθεί ή έγκρισή τους πρώτα.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Αν η οργάνωση θέλει να διερευνήσει την κατάσταση χωρίς να προειδοποιήσει τον hacker θα πρέπει να ληφθεί μεγάλη προσοχή. Τα τυποποιημένα εργαλεία για την ανάλυση μπορούν να προειδοποιήσουν έναν hacker γρήγορα. Χρησιμοποιώντας **ping, traceroute, nslookup** και άλλα εργαλεία θα ειδοποιηθεί ο hacker ειδικά αν προσέχει τι διαδικασίες και εντολές δίνονται σε ένα σύστημα. Ο καλύτερος τρόπος για να αναλυθεί ένα σύστημα είναι να γίνει ένα αντίγραφο ασφαλείας του συστήματος και έπειτα να αναλυθεί. Εάν η παράβαση προξενεί άμεση βλάβη, τότε θα ήταν καλό η επιχείρηση να θέσει σε περιορισμό το σύστημα ακόμα και αν ειδοποιηθεί ο hacker. Ωστόσο, πολλές παραβιάσεις δεν είναι τόσο επιζήμιες και μπορούν να παρακολουθηθούν στενά όσο συμβαίνει και η ανάλυση.

Σε όλες τις περιπτώσεις ένα ή περισσότερα αντίγραφα ασφαλείας θα πρέπει να δημιουργηθούν. Τα καλύτερα αντίγραφα ασφαλείας για αυτήν την κατάσταση είναι bit-by-bit του σκληρού δίσκου. Αυτό μπορεί να γίνει χρησιμοποιώντας μια ποικιλία εργαλείων όπως **dd** ή **Ghost**. Το DD είναι ένα πανίσχυρο εργαλείο που πρέπει να χρησιμοποιείται με προσοχή. Είναι αρκετά εύκολο να διαγραφούν παντελώς τα δεδομένα από έναν ολόκληρο δίσκο απλά αντιστρέφοντας τις παραμέτρους για την πηγή και για τον στόχο. Εκτός από την δημιουργία αντιγράφων ασφαλείας του συστήματος, εάν η οργάνωση σχεδιάζει να κάνει εγκληματολογική ανάλυση ένα αντίστοιχο αντίγραφο θα πρέπει να δημιουργηθεί.

Υπάρχουν διάφορα εργαλεία διαθέσιμα για αυτό, αλλά το περισσότερο διαδεδομένο είναι το **EnCase**. Πρόκειται για ένα πολύ ακριβό λογισμικό και ίσως οι μικρές ή μεσαίες επιχειρήσεις δεν θα θέλουν να πληρώσουν για αυτό. Μια εναλλακτική λύση είναι ένα έμπιστο τρίτο μέλος. Το τρίτο μέλος έχει πληρώσει για το λογισμικό οπότε η εταιρεία μπορεί να το χρησιμοποιήσει μέσω αυτού. Μόλις τα αντίγραφα ασφαλείας και τα αντίγραφα της εγκληματολογικής αναφοράς είναι έτοιμα, θα γίνει η ανάλυσή τους. Σε αυτό το σημείο, ο χειριστής του περιστατικού μπορεί να ερευνήσει τις καταγραφές και τα άλλα δεδομένα ώστε να κάνει συστάσεις σχετικά με την καλύτερη στρατηγική που θα ακολουθηθεί.

Αν η επιχείρηση αποφασίσει να θέσει το σύστημα εκτός σύνδεσης, τότε ο χειριστής μπορεί να αφιερώσει χρόνο ώστε να σιγουρευτεί ότι το σύστημα είναι καθαρό και έτοιμο για επανένταξη. Στην περίπτωση που η επιχείρηση αποφασίσει ότι το σύστημα δεν μπορεί να τεθεί εκτός σύνδεσης, τότε ο χειριστής πρέπει να βρει ένα τρόπο να καθαρίσει το σύστημα όσο το δυνατόν περισσότερο. Αυτό μπορεί να είναι δύσκολο και ριψοκίνδυνο και θα πρέπει να γίνεται μόνο όταν είναι η έσχατη λύση καθώς είναι σχεδόν αδύνατο να μην έχει ανακαλύψει ο hacker μία ακόμη ανασφάλεια που θα του επιτρέψει την είσοδο στο σύστημα. Παρακάτω αναφέρονται μερικά περιστατικά και οι αντίστοιχες ενέργειες:

| Είδος Περιστατικού: | Ενέργειες: |
|---|---|
| Κλοπή πληροφοριών | Εξέταση των καταγραφών και του συστήματος για να προσδιοριστεί ποιες πληροφορίες εκλάπησαν και πως |
| Άρνηση υπηρεσίας | Επαναρύθμιση του λειτουργικού συστήματος TCP/IP<br>Ρύθμιση των παραμέτρων του firewall<br>Διαμόρφωση των upstreams δρομολογητών να μπλοκάρουν/ εκτρέψουν την επίθεση<br>Επιβεβαίωση του προσφάτου |

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

| | |
|---|---|
| | αντίγραφου ασφαλείας πριν από την επίθεση DoS |
| Κακόβουλο Λογισμικό/Ιοί | Απομόνωση των μολυσμένων μηχανημάτων από το δίκτυο ή απενεργοποίηση email / web servers<br>Τροποποίηση των ρυθμίσεων του firewall, επαναδιαμόρφωση του email, εγκατάσταση patches<br>Ενημέρωση της προστασίας από ιούς |
| Ακατάλληλη χρήση | Συλλογή όλων των σχετικών πληροφοριών όπως τα αρχεία καταγραφών, μηνύματα email, κίνηση δικτύου<br>Δημιουργία ιατροδικαστικού αντιγράφου της μηχανής<br>Καταγραφή σε CD των αποδείξεων για διατήρηση |
| Φυσική εισβολή | -Έλεγχος αν οι μηχανές απαιτούν κωδικό πρόσβασης<br>-Έλεγχος ότι το μηχάνημα έχει κωδικό οθόνης<br>-Έλεγχος των μηχανημάτων για σημάδια φυσικής παραβίασης<br>-Έλεγχος των αρχείων καταγραφής για μη εξουσιοδοτημένη χρήση. |

### 4.2.4 Eradication (εξάλειψη)

Η εξάλειψη είναι η πλήρης απομάκρυνση όλων των αντικειμένων που άφησε ο επιτιθέμενος, είτε αυτός ήταν άνθρωπος, είτε πρόγραμμα. Πρόκειται για μία δύσκολη διαδικασία. Το πρώτο βήμα είναι να καθοριστεί η αιτία του συμβάντος. Αυτό είναι κρίσιμο διότι δεν έχει σημασία πόση ενέργεια θα διατεθεί για τον καθαρισμό ενός συστήματος, εάν η αιτία δεν βρεθεί και συνεπώς η ευπάθεια, τότε το σύστημα θα παραβιαστεί ξανά.

Το **EnCase** μπορεί να βοηθήσει σε μεγάλο βαθμό σε αυτό το βήμα. Αυτά τα εργαλεία μπορούν να βοηθήσουν τον χειριστή να βρει τα κακόβουλα λογισμικά και να βοηθήσουν με την ανάλυση των αρχείων καταγραφής στην εύρεση κρυμμένων αρχείων που ίσως ο επιτιθέμενος χρησιμοποιεί. Ωστόσο το EnCase είναι δαπανηρό εργαλείο.

Μια ελεύθερη επιλογή είναι το **Autopsy Forensic Browser**, ένα γραφικό περιβάλλον για τα συνήθη **Sleuth Kit(TSK)**. Μπορούν να χρησιμοποιηθούν για την ανάλυση εικόνων στον δίσκο παρέχοντας πολλές ίδιες λειτουργίες με το EnCase. Υπάρχουν δύο κύριες επιλογές στην φάση της εξάλειψης. Να αποκατασταθεί το

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

σύστημα από τα αντίγραφα ασφαλείας ή να ξαναχτιστεί το σύστημα από το μηδέν. Εάν η οργάνωση έχει καλό αντίγραφο ασφαλείας το οποίο είχε δημιουργηθεί πριν την παραβίαση, τότε το σύστημα μπορεί να ανακατασκευαστεί χρησιμοποιώντας το. Αυτό είναι επικίνδυνο. Οι επιτιθέμενοι έχουν παραβιάσει το σύστημα πολύ πριν ανακαλυφθούνε. Οι στατιστικές δείχνουν ότι τα περισσότερα κρούσματα παρέμειναν κρυμμένα για αρκετούς μήνες. Ένας επιτιθέμενος μπορεί να εγκαταστήσει μια backdoor και να μην την χρησιμοποιεί για αρκετούς μήνες. Σιγουρευτείτε να ψάξετε για κακόβουλο λογισμικό ακόμα και στα αντίγραφα ασφαλεία. Ελέγξτε για rootkis, ιούς και backdoors. Οι ιοί μπορούν να αντιμετωπιστούν σχετικά εύκολα, αλλά αν βρείτε ένα rootkit τότε ο δίσκος θα πρέπει να διαμορφωθεί(format) και το λειτουργικό σύστημα πρέπει να επανεγκατασταθεί από την αρχή. Ανεξάρτητα αν το σύστημα ανοικοδομήθηκε από ένα αντίγραφο ασφαλείας ή από την αρχή, ο χειριστής του περιστατικού πρέπει να βελτιώσει τις άμυνες του συστήματος και να το θωρακίσει έτσι ώστε να μην κινδυνεύσει ξανά. Αυτό σημαίνει εγκατάσταση patches και λειτουργικού συστήματος και επίπεδων εφαρμογής. Σημαίνει επίσης, αλλαγές στο firewall, κλείδωμα υπηρεσιών και αλλαγή λογαριασμών. Όταν το σύστημα τεθεί πάλι σε σύνδεση, θα πρέπει να επικυρωθεί η ασφάλειά του. Το σύστημα θα πρέπει να σαρωθεί με ένα εργαλείο όπως το **Nessus** ή **MBSA** για τον έλεγχο υπολειπόμενων ευπαθειών. Έπειτα το σύστημα είναι έτοιμο να επανέλθει. Τώρα διαθέτετε ένα καλό αντίγραφο ασφαλείας του συστήματος. Αν ξανά βρεθεί σε κίνδυνο, θα έχετε ήδη ένα καθαρό σημείο εκκίνησης.

### 4.2.5 Recovery (Ανάκαμψη)

Το σύστημα που έχει ήδη επικυρωθεί για λόγους ασφαλείας, θα πρέπει να επικυρωθεί και για λόγους λειτουργικότητας της επιχείρησης. Θα πρέπει να ελεγχθούν όλες οι λειτουργίες που είναι απαραίτητες για την λειτουργία πριν από την επανέναρξη της παραγωγής. Μόλις και η ασφάλεια και η λειτουργικότητα της επιχείρησης είναι εξασφαλισμένες, τότε το σύστημα μπορεί να τεθεί πάλι σε σύνδεση. Το τελικό βήμα για την ανάκαμψη είναι να διασφαλιστεί ότι το σύστημα παρακολουθείται έτσι ώστε τα μελλοντικά προβλήματα να ανιχνεύονται έγκαιρα. Ακόμα και στις μικρές επιχειρήσεις, τα συστήματα παρακολουθούνται εύκολα. Μια λύση σε περιβάλλον Windows είναι να χρησιμοποιήσουμε το **Snare** για την ανάλυση των καταγραφών. Ενώ σε περιβάλλον Unix, το **syslog-ng** μπορεί να χρησιμοποιηθεί για την εδραίωση των καταγραφών και το **Simple Event Correlator** για την ανάλυση.

### 4.2.6 Lessons Learned (Διδάγματα)

Οι βέλτιστες πρακτικές περιλαμβάνουν την ανάπτυξη της έκθεσης του περιστατικού ως ένα μέρος των διδαγμάτων της διαδικασίας. Μια λεπτομερής έκθεση μπορεί να μην είναι εφικτή σε μικρές και μεσαίες επιχειρήσεις, αλλά ακόμα και σε μια μικρή εταιρεία μια μικρή έκθεση είναι σημαντική. Ο χειριστής καλείται να περιγράψει με σαφήνεια τα ακόλουθα:

ποιά συστήματα διακυβεύονται;

ποιός είναι ο καλύτερος συμβιβασμός που θα προκύψει;

ποιά μέτρα ελήφθησαν για να περιορίσουν το περιστατικό;

ποιά μέτρα ελήφθησαν για να καθαρίσουν το σύστημα ;

ποιά μέτρα έχουν ληφθεί για να διασφαλιστεί ότι η παραβίαση δεν θα ξανασυμβεί;

## 4.3 Συμπεράσματα

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Εν κατακλείδι, η διαδικασία των έξι-βημάτων μπορεί να τροποποιηθεί ώστε να είναι αποτελεσματική και για τις μικρές και μεσαίες επιχειρήσεις. Μια επισκόπηση των βημάτων και πως μια μικρή και μεσαία επιχείρηση μπορεί να τα ακολουθήσει.

**Preparation (Προετοιμασία):**

Να είστε προετοιμασμένοι. Δημιουργήστε τις οδηγίες αντιμετώπισης περιστατικών που μπορούν να χρησιμοποιηθούν όταν αυτό συμβεί. Αυτό είναι ένα κρίσιμο βήμα, ειδικά για τις μικρές επιχειρήσεις που δεν διαθέτουν αρκετούς πόρους για την διαχείριση περιστατικών. Οι καλές οδηγίες αντιμετώπισης περιστατικών θα βοηθήσουν στην γρήγορη και αποτελεσματική αντιμετώπιση του περιστατικού.

**Identification (Αναγνώριση):**

Χρησιμοποιήστε τα έντυπα στις οδηγίες αντιμετώπισης περιστατικού ώστε να αναγνωρίσετε το περιστατικό και επικοινωνήστε με τα κατάλληλα άτομα τόσο εντός όσο και εκτός του οργανισμού.

**Containment (Περιορισμός):**

Με βάση τα δεδομένα στην φάση αναγνώρισης, περιορίζεται το περιστατικό αναλόγως. Αυτό μπορεί να σημαίνει την αφαίρεση του συστήματος από το δίκτυο. Δημιουργήστε ένα αντίγραφο ασφαλείας του συστήματος που μπορεί να χρησιμοποιηθεί για ανάλυση και ενδεχομένως για ένα εγκληματολογικό αντίγραφο επίσης. Τέλος, αποφασίστε κατά πόσον το σύστημα θα πρέπει να καθαριστεί ή να ανακατασκευαστεί. Από άποψη της ασφάλειας είναι προτιμότερο να ξαναδημιουργηθεί το σύστημα, αν και αυτό δεν είναι ότι καλύτερο για την επιχείρηση.

**Eradication (Εξάλειψη):**

Καθαρίστε το σύστημα ή δημιουργήστε το ξανά. Έπειτα, επικυρώστε ότι το σύστημα είναι ασφαλές με την βοήθεια των εργαλείων Nessus ή MBSA. Επίσης, δημιουργήστε ένα αντίγραφο ασφαλείας του καθαρού συστήματος και αποθηκεύστε το σε περίπτωση που μια άλλη παραβίαση συμβεί.

**Recovery (Ανάκτηση):**

Τοποθετήστε το νέο σύστημα ξανά στην παραγωγή και βεβαιωθείτε ότι παρακολουθείται για μελλοντικά προβλήματα.

**Lessons Learned (Διδάγματα):**

Τέλος συντάξτε μια έκθεση-αναφορά η οποία περιγράφει την κατάσταση και τι έχει γίνει για την πρόληψη των μελλοντικών παραβιάσεων.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# 5. Ανθεκτικότητα και Επιχειρησιακές Αρχιτεκτονικές για ΜΜΕ

Προκειμένου να οριστεί βιώσιμη μια ΜΜΕ, η ανθεκτικότητα ως έννοια κρίνεται ζωτικής σημασίας και ίσως η ουσία της βιωσιμότητας να είναι η ανθεκτικότητα, η ικανότητά δηλαδή να αντισταθεί στην διαταραχή. Ως εκ τούτου, μια βιώσιμη οικονομία πρέπει να βασίζεται σε μια δυναμική άποψη για τον κόσμο στον οποίο η ανάπτυξη και η αλλαγή είναι αναπόφευκτες για τις ΜΜΕ, οι οποίες πρέπει να ενστερνιστούν τις αρχές της βιωσιμότητας.

Λαμβάνοντας υπόψη τα παραπάνω, καθώς και ότι είναι μια καλά καθορισμένη και άμεσα διαθέσιμη αρχιτεκτονική της επιχείρησης, που υποστηρίζει την ένταξη της, επιτρέποντας την κοινή παρακολούθηση των επιχειρηματικών διαδικασιών, δεδομένων και συστημάτων σε ολόκληρη την επιχείρηση και τους συνεργάτες της. Οι Επιχειρησιακές Αρχιτεκτονικές είναι μια διαδικασία που κάνει την ανθεκτικότητα προβλέψιμη, και θα πρέπει να υποστηρίξει και να συνεργάζεται με άλλες διαδικασίες για την ανθεκτικότητα. Ωστόσο, τα πλαίσια της αρχιτεκτονικής επιχείρησης δεν δίνουν σημασία για τις δραστηριότητες που συμβάλλουν περισσότερο στην επιχειρηματική ανθεκτικότητα.

Ως εκ τούτου, ο στόχος είναι να αποσαφηνιστούν οι διαστάσεις και οι δραστηριότητες που σχετίζονται με την ανάπτυξη μιας αρχιτεκτονικής επιχείρησης και τα κοινά σημεία με άλλες διαδικασίες σε ολόκληρη την επιχείρηση, προκειμένου να διασφαλιστεί ότι οι απαιτήσεις της ανθεκτικότητας ικανοποιούνται στις ΜΜΕ. Για το σκοπό αυτό, θα παρουσιαστεί μια πρόταση που υποστηρίζεται σε τέσσερις κύριες διαστάσεις, καθώς και μια προσέγγιση για μια σειρά από δραστηριότητες domain με σκοπό για την ανάπτυξη των επιχειρηματικών και οργανωτικών Αρχιτεκτονικών.

## 5.1 Διαστάσεις

Αντιμετωπίζοντας τις ανάγκες των διαφόρων ενδιαφερομένων σε μια επιχείρηση, βλέπουμε ότι οι επιχειρησιακές αρχιτεκτονικές χωρίζονται σε διάφορες συνιστώσες: των επιχειρήσεων, της οργάνωσης, της πληροφόρησης και της τεχνολογίας που συνδέονται με αυτές :

**Επιχειρήσεις** - Ο τομέας αυτός ασχολείται με τη λειτουργία των επιχειρήσεων, που έχουν να κάνουν με θέματα όπως τα προϊόντα και τις υπηρεσίες, τους πελάτες και την αλληλεπίδραση μαζί τους, το οικονομικό μοντέλο που διέπει την επιχείρηση, και τις σχέσεις με το περιβάλλον (κανάλια πωλήσεων, της αγοράς, ανταγωνιστές καθώς και τα ενδιαφερόμενα μέρη). Η επιχειρησιακή αρχιτεκτονική καθοδηγεί τον τρόπο με τον οποίο η επιχείρηση πρέπει να αξιοποιηθεί και να διερευνηθεί.

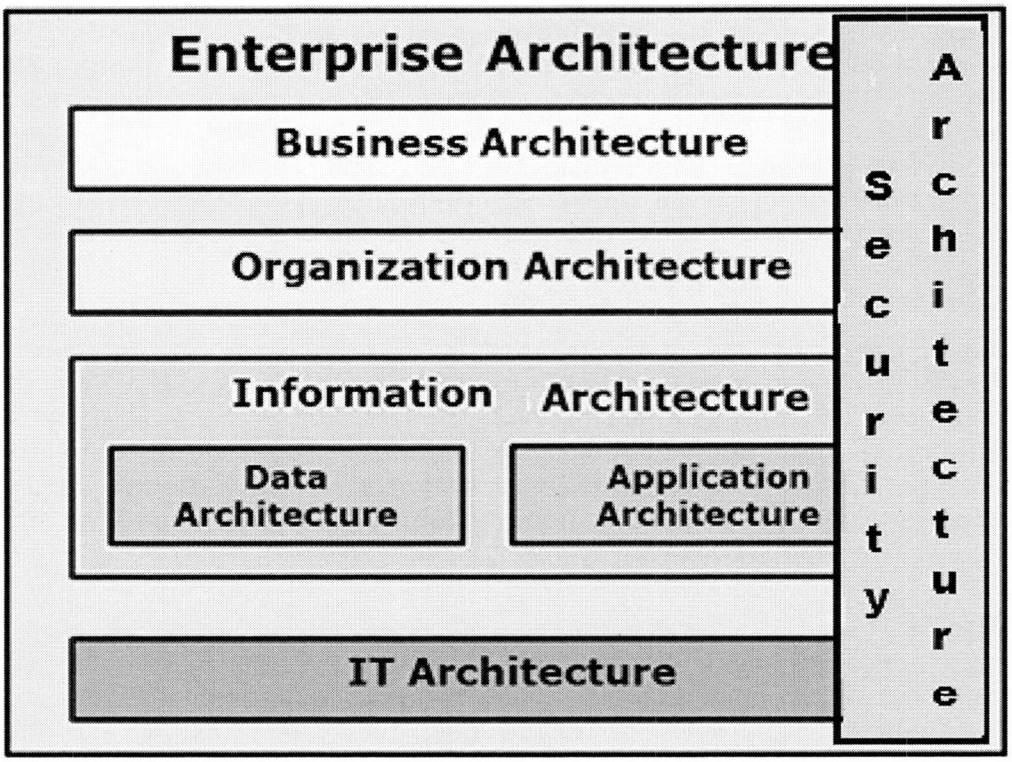
**Οργανισμοί** - Ο τομέας της οργάνωσης έχει να κάνει με την εσωτερική διαρρύθμιση της επιχείρησης, για παράδειγμα, με τις διαδικασίες, τη συμπεριφορά των εργαζομένων, την πολιτική της επιχείρησης, τις πρακτικές διαχείρισης/ηγεσίας, τις διάφορες δομές και τα συστήματα.

**Πληροφορίες** - Οι πληροφορίες είναι ένας κρίσιμος παράγοντας στο πλαίσιο τόσο στον τομέα του σχεδιασμού των επιχειρήσεων όσο και την οργάνωση. Πολλές πτυχές της πληροφόρησης παίζουν ρόλο εδώ, όπως η δομή και η ποιότητα των πληροφοριών, η διαχείριση των πληροφοριών (συλλογή, αποθήκευση, διανομή), και η χρήση των πληροφοριών. Ο τομέας του σχεδιασμού των πληροφοριών έχει να κάνει με την κατασκευή της επιχείρησης. Η αρχιτεκτονική των πληροφοριών ελέγχει τον τρόπο με τον οποίο οι πληροφορίες (τα δεδομένα) πρέπει να χρησιμοποιηθούν.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Έτσι οι αρχές της, αφορούν τον χειρισμό των δεδομένων των πελατών και του προμηθευτή, ή τον τρόπο ενημέρωσης των λειτουργικών συστημάτων.

**Τεχνολογία** - Η τεχνολογία είναι απαραίτητη για τις επιχειρήσεις, την υποστήριξη των πληροφοριακών συστημάτων, καθώς και για τη μελλοντική ανάπτυξη των επιχειρήσεων. Η τεχνολογία είναι ένα σημαντικό μέρος της ανάπτυξης της επιχείρησης. Ως εκ τούτου, για κάθε τεχνολογία, υπάρχει μια σχετική αρχιτεκτονική, καθοδηγώντας τον σχεδιασμό της.




Εικόνα 2: Επιχειρησιακές Αρχιτεκτονικές[2]

## 5.2 Προσέγγιση

Μια συστηματική προσέγγιση είναι αναγκαία για την ανάπτυξη της επιχείρησης, μέσω της αλλαγής του περιβάλλοντος και τον συστηματικό σχεδιασμό της επιχείρησης καθώς επίσης και την σχέση της επιχείρησης με το περιβάλλον. Οι βασικές υποθέσεις είναι ότι το περιβάλλον μπορεί να αλλάξει, και ότι τα συστήματα-στο-περιβάλλον και η συν-εξέλιξη είναι απαραίτητα για την αποτελεσματική εκτέλεση της στρατηγικής. Έτσι, για τις Επιχειρήσεις και την Οργανωτική Αρχιτεκτονική της ΕΑ, ο αρχιτέκτονας της επιχείρησης πρέπει να είναι σε θέση να προωθήσει τις διαδικασίες εκείνες οι οποίες οδηγούν στην εκμάθηση.

Από τις τέσσερις αρχιτεκτονικές που αναφέρονται παραπάνω, των επιχειρήσεων, την οργανωτική, των πληροφοριών, και την τεχνολογική, θα παρουσιαστούν οι δραστηριότητες που σχετίζονται με την ανάπτυξη των επιχειρήσεων της Οργανωτικής Αρχιτεκτονικής, και τα σημεία επαφής με άλλες διαδικασίες σε ολόκληρη την επιχείρηση, προκειμένου να διασφαλιστεί ότι οι απαιτήσεις της ανθεκτικότητας πληρούνται στις ΜΜΕ.

[2]Πηγή: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752015000300525

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

## 5.3 Ανάπτυξη Επιχειρησιακής Αρχιτεκτονικής

Η πρώτη είναι η επιχειρησιακή αρχιτεκτονική και οι δραστηριότητες που σχετίζονται με την ανάπτυξη της είναι: στρατηγική ευελιξία, επιχειρηματικές επιταγές μέσω SOA, και τα συναφή με την αρχιτεκτονική ασφαλείας.

## 5.4 Ανάπτυξη Στρατηγικής Ευελιξίας

Η έννοια της ευελιξίας δημιουργήθηκε για να αποφανθεί πως οι επιχειρήσεις μπορούν να λειτουργήσουν και να αναπτυχθούν σε περιβάλλοντα που χαρακτηρίζονται από αναταράξεις. Αντί να περιορίζεται η λειτουργία τους σε ένα μόνο τρόπο ανταπόκρισης, η έννοια της ευελιξίας έχει ως στόχο να ενθαρρύνει τις επιχειρήσεις στην προσέγγισή τους στην αγορά. Δεδομένης της μεγαλύτερης ευελιξίας της ΜΜΕ, η υιοθέτηση μιας ευέλικτης προσέγγισης κάνει καλή αίσθηση. Η ανάπτυξη προληπτικών στρατηγικών ευνοεί μια προσέγγιση «από πάνω προς τα κάτω», σύμφωνα με την οποία η στρατηγική σκέψη και η πράξη του σχεδιασμού δρουν ως πρωταρχικά μέσα για να επαινέσουν επιχειρησιακές δυνατότητες. Η τάση είναι για τις μικρομεσαίες επιχειρήσεις να συμπεριφέρονται αντιδραστικά και όχι προληπτικά. Συνίσταται η χρήση του πλαισίου το οποίο λαμβάνει ως αφετηρία το γεγονός ότι η υιοθέτηση μιας στρατηγικής προσέγγισης συσχετίζεται με βελτιωμένη απόδοση. Επίσης υφίσταται ότι οι ΜΜΕ είναι σε καθαρά μειονεκτική θέση σε περιβάλλοντα που υπάρχουν διαταραχές, όπου υπάρχει ελάχιστη ή καμία ικανότητα στρατηγικού σχεδιασμού. Η προσέγγιση αυτή βασίζεται στην παραδοχή ότι η ανθεκτικότητα εμφανίζεται ως αποτέλεσμα της εφαρμογής επιχειρησιακών και στρατηγικών ικανοτήτων. Πριν την ανάληψη μιας στρατηγικής ανάλυσης, τα χαρτοφυλάκια των προϊόντων και των υπηρεσιών εξετάζονται σε σχέση με τις οικονομικές συνεισφορές και αντιλαμβάνονται προοπτικές για ανάπτυξη. Η στρατηγική περιγράφεται λεπτομερώς στα ακόλουθα βήματα:

1 - κατανόηση παραγόντων διαφοροποίησης για την επιχείρηση

2 - εξέταση των τάσεων της βιομηχανίας και των επιπτώσεων

3 - τοποθέτηση σε σχέση με ανταγωνιστικά πλεονεκτήματα και τις αδυναμίες

4 - καθορισμός στόχων και εκλογή των επιλογών ανάπτυξης

5 - αξιολόγηση και ιεράρχηση των επιλογών ανάπτυξης

6 - εξέλιξη των σχεδίων ανάπτυξης και

7 - εφαρμογή και αναθεώρηση.

## 5.5 Κίνητρα Ανάπτυξης Στόχων Επιχείρησης

Οι στόχοι της επιχείρησης παρέχουν τα κίνητρα για την αναζήτηση ενός νέου τρόπου για την επίτευξη της IT ευελιξίας μέσω της Service Oriented Architecture (SOA).

Για τον εντοπισμό των SOA στόχων, γίνονται οι εξής δραστηριότητες:

1. αξιολόγηση του εξωτερικού περιβάλλοντος,

2. επανεξέταση της τρέχουσας οργάνωσης της στρατηγικής της επιχείρησης και του μοντέλου επιχειρηματικής λειτουργίας,

3. αναθεώρηση της στρατηγικής του IT και του λειτουργικού μοντέλου αυτής,

4. κατανόηση της θέσης της αγοράς

5. γνωστοποίηση των προϊόντων και των υπηρεσιών που εξυπηρετούν τους πελάτες

6. κατανόηση των άμεσων και προγραμματισμένων επιχειρηματικών πρωτοβουλιών

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

7. προσδιορισμός βασικών επιχειρηματικών δραστηριοτήτων από τις επιχειρηματικές μονάδες.

Με την υιοθέτηση μιας προσέγγισης SOA και την εφαρμογή της, χρησιμοποιώντας τεχνολογίες υποστήριξης, οικοδομούνται ευέλικτα συστήματα και εφαρμόζονται αλλάζοντας τις επιχειρηματικές διαδικασίες γρήγορα και κάνοντας εκτεταμένη χρήση των επαναχρησιμοποιήσιμων εξαρτημάτων. Η αυξημένη λειτουργικότητα, η αυξημένη ευθυγράμμιση της επιχείρησης και της τεχνολογίας, η αυξημένη απόδοση της επένδυσης, και η αυξημένη ευελιξία είναι όλα τα οφέλη της προσέγγισης μέσω SOA.

## 5.6 Ορισμός της συναφής αρχιτεκτονικής ασφάλειας

Η αποτελεσματική ανθεκτικότητα ξεκινά με την κατανόηση τι ακριβώς χρειάζεται μια επιχείρηση με στρατηγική ευελιξία, προκειμένου να επιβιώσει σε απροσδόκητα γεγονότα και να σχεδιάσει το μέλλον για τις επερχόμενες προκλήσεις. Αν ένα γεγονός είναι σχετικό με το τμήμα IT, ή με την επιχείρηση, ή με μια φυσική καταστροφή, πάντα θα υπάρχουν προκλήσεις για να ξεπεραστούν. Εάν υπάρχουν σχέδια στρατηγικής για αυτά τα γεγονότα, ο πραγματικός αντίκτυπος σε μια επιχείρηση μπορεί να μειωθεί. Η ασφάλεια μιας επιχείρησης περιλαμβάνει τρεις βασικούς τομείς: την ασφάλεια των πληροφοριών, τη συνέχεια της επιχείρησης και τη φυσική και περιβαλλοντική ασφάλεια.

Μία από τις σημαντικές πτυχές της ποιότητας της αρχιτεκτονικής της επιχείρησης είναι το ρίσκο για την ασφάλεια των πληροφοριών, καθώς και ο τρόπος με τον οποίο μπορεί να αντιμετωπιστεί. Είναι η κοινή εμπειρία πολλών εταιρικών οργανισμών το γεγονός ότι η ασφάλεια των πληροφοριών θα πρέπει συχνά να σχεδιάζεται και να εγκαθίσταται σε τακτική βάση. Σε αυτή τη διαδικασία, δεν υπάρχει καμία εγγύηση ότι το αποτέλεσμα θα είναι συμβατό και λειτουργικό .

Για την δημιουργία μιας περιγραφής του πλαισίου της επιχείρησης στην οποία τα συστήματα ασφαλείας σχεδιάζονται, κατασκευάζονται και λειτουργούν, συνίσταται η χρήση της "**SABSA**" μεθοδολογίας (Sherwood Applied Business Architecture 2005). Η μεθοδολογία αυτή ασχολείται με την επιχείρηση και την προστασία των περιουσιακών στοιχείων και των επιχειρηματικών αναγκών για την ασφάλεια των πληροφοριών (ασφάλεια ως επιχειρηματικό εργαλείο, ασφαλή ηλεκτρονικό επιχειρείν, λειτουργική συνέχεια και σταθερότητα, τη συμμόρφωση με τη νομοθεσία).

Η επιλογή της SABSA μεθοδολογίας είναι γιατί η ανάπτυξη της εταιρείας γίνεται με γνώνομα τον κίνδυνο της ασφάλειας των πληροφοριών και την διασφάλιση των αρχιτεκτονικών(συστημάτων) για την παροχή λύσεων της υποδομής της ασφάλειας που υποστηρίζουν οι επιχειρήσεις.

## 5.7 Ανάλυση της ανθρώπινης παρέμβασης εντός της επιχείρησης

Οι ανθεκτικές αρχιτεκτονικές ΜΜΕ πρέπει επίσης να διαθέτουν το κατάλληλο ανθρώπινο δυναμικό, επειδή δεν μπορεί κανείς να διαχωρίσει μια επιχείρηση από τους ανθρώπους που την αποτελούν. Τέσσερα σημαντικά χαρακτηριστικά της ανθεκτικότητας είναι: η ευελιξία, τα κίνητρα, η επιμονή και η αισιοδοξία. Η ανασκόπηση της βιβλιογραφίας επιτρέπει να εντοπιστούν και να συνοψιστούν τα πιο σημαντικά χαρακτηριστικά για ένα ευκίνητο εργατικό δυναμικό. Με βάση τα μοντέλα Griffin-Hesketh (Griffin και Hesketh 2003) και Dyer-Shafer (Dyer και Shafer 2003), τα χαρακτηριστικά του ευκίνητου εργατικού δυναμικού ομαδοποιήθηκαν σε τρεις διαστάσεις: πρόληψη, προσθετικότητα και ανθεκτικότητα. Η ανθεκτικότητα περιγράφει την ικανότητα να λειτουργήσουν αποτελεσματικά κάτω από την πίεση και παρά το μεταβαλλόμενο περιβάλλον, ή όταν εφαρμόζονται στρατηγικές χωρίς αποτέλεσμα. Τα ακόλουθα γνωρίσματα ανήκουν σε αυτή τη διάσταση: (1) θετική

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

στάση προς τις αλλαγές, νέες ιδέες και τεχνολογία και (2) ανοχή σε αβέβαιες και απρόβλεπτες καταστάσεις, και διαφορές στις απόψεις.

Δημιουργώντας μια ευέλικτη Οργανωτική Δομή

Ένας οργανισμός πρέπει να έχει σχεδιαστεί για να εφαρμόσει με συνέπεια τις συστάσεις του επιχειρηματικού μοντέλου, χωρίς να επηρεάζει αρνητικά την παραγωγικότητα. Συνεπώς, η ανάλυση του σχεδιασμού ενός οργανισμού, για να διασφαλίσει ότι υπάρχει η δυνατότητα και ικανότητα να ενστερνιστεί την αλλαγή, αποτελεί μια διαδικασία. Το κλειδί σε αυτή τη διαδικασία είναι να συνειδητοποιηθεί ότι ο σχεδιασμός ενός οργανισμού αποτελείται από πολλά συστατικά που πρέπει να αναλυθούν ως σύνολο ιεραρχικών σχέσεων σε ένα οργανόγραμμα, σε οργανωτικούς ρόλους / αρμοδιότητες, μέτρα απόδοσης, και στο σχεδιασμό της ομάδας εργασίας και την ένταξη σε μηχανισμούς.

Ανάλυση της αξίας SOA

Η ανάλυση της αξίας SOA βοηθά στον εντοπισμό των τομέων εστίασης για τις πρωτοβουλίες SOA με τον προσδιορισμό των επιχειρήσεων και των διαδικασιών που παρουσιάζουν ιδιαίτερο ενδιαφέρον για τις προσπάθειες βελτίωσης των επιχειρήσεων. Μόλις υπάρχει κάποια έννοια πεδίου εφαρμογής για τις αρχικές προσπάθειες SOA, η διαδικασία ταυτοποίησης των υπηρεσιών μπορεί να προχωρήσει (Mark και Bell 2006). Ο αρχιτέκτονας πρέπει να εξετάσει τα ακόλουθα αντικείμενα τα οποία είναι ιδιαίτερα σημαντικά για SOA, διότι συμβάλλουν στον καθορισμό των δομικών στοιχείων της SOA.

Ανάλυση Αξίας του Cloud Computing

Το cloud computing προσφέρει στην ΜΜΕ μια επεκτάσιμη υποδομή δυνατοτήτων που διατίθενται ως υπηρεσίες. Κατά την επιλογή των παροχών υπηρεσιών cloud, οι οργανισμοί και οι επιχειρήσεις των ΜΜΕ πρέπει να αναπτύξουν κατάλληλες πολιτικές και διαδικασίες ασφάλειας, που χρειάζονται για να χρησιμοποιήσουν αυτές τις κατευθυντήριες γραμμές για την αξιολόγηση των πάροχων υπηρεσιών cloud (Williams 2010). Δεν είναι πάντα η σωστή λύση, και υπάρχουν πολλές μορφές cloud computing που έχουν διαφορετικά πλεονεκτήματα σε διαφορετικές καταστάσεις. Το δέντρο απόφασης των αγοραστών του cloud (Skilton και Gordon 2010) μπορεί να βοηθήσει να καθορίσει εάν θα χρησιμοποιηθεί το cloud computing ως δημόσιο ή ως ιδιωτικό και ποια από τα cloud IaaS, PaaS, ή SaaS θα ανταποκρίνονται καλύτερα στις επιχειρηματικές και τεχνικές ανάγκες.

## 5.8 Συμπεράσματα

Με βάση την σημασία της ανθεκτικότητας για τις ΜΜΕ, διευκρινίστηκαν οι διαστάσεις και οι δραστηριότητες που σχετίζονται με την ανάπτυξη μιας Επιχειρησιακής Αρχιτεκτονικής(ΕΑ), καθώς και τα σημεία επαφής με άλλες διαδικασίες σε ολόκληρη την επιχείρηση, προκειμένου να διασφαλιστεί ότι η ανθεκτικότητα και οι απαιτήσεις της ικανοποιούνται στις ΜΜΕ. Επικεντρώνοντας στις επιχειρήσεις, τις οργανωτικές Αρχιτεκτονικές, και τις αντίστοιχες στρατηγικές ανάπτυξής τους. Ένα σύνολο εργαλείων προτάθηκε, ότι θα επιτρέψει τα θέματα να αξιολογηθούν από την άποψη της αποτελεσματικότητάς τους και της οργανωτικής ανθεκτικότητάς τους.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# 6. Βέλτιστες Πρακτικές για Μικρομεσαίες Επιχειρήσεις και Κρατικές Υπηρεσίες

## Εισαγωγή

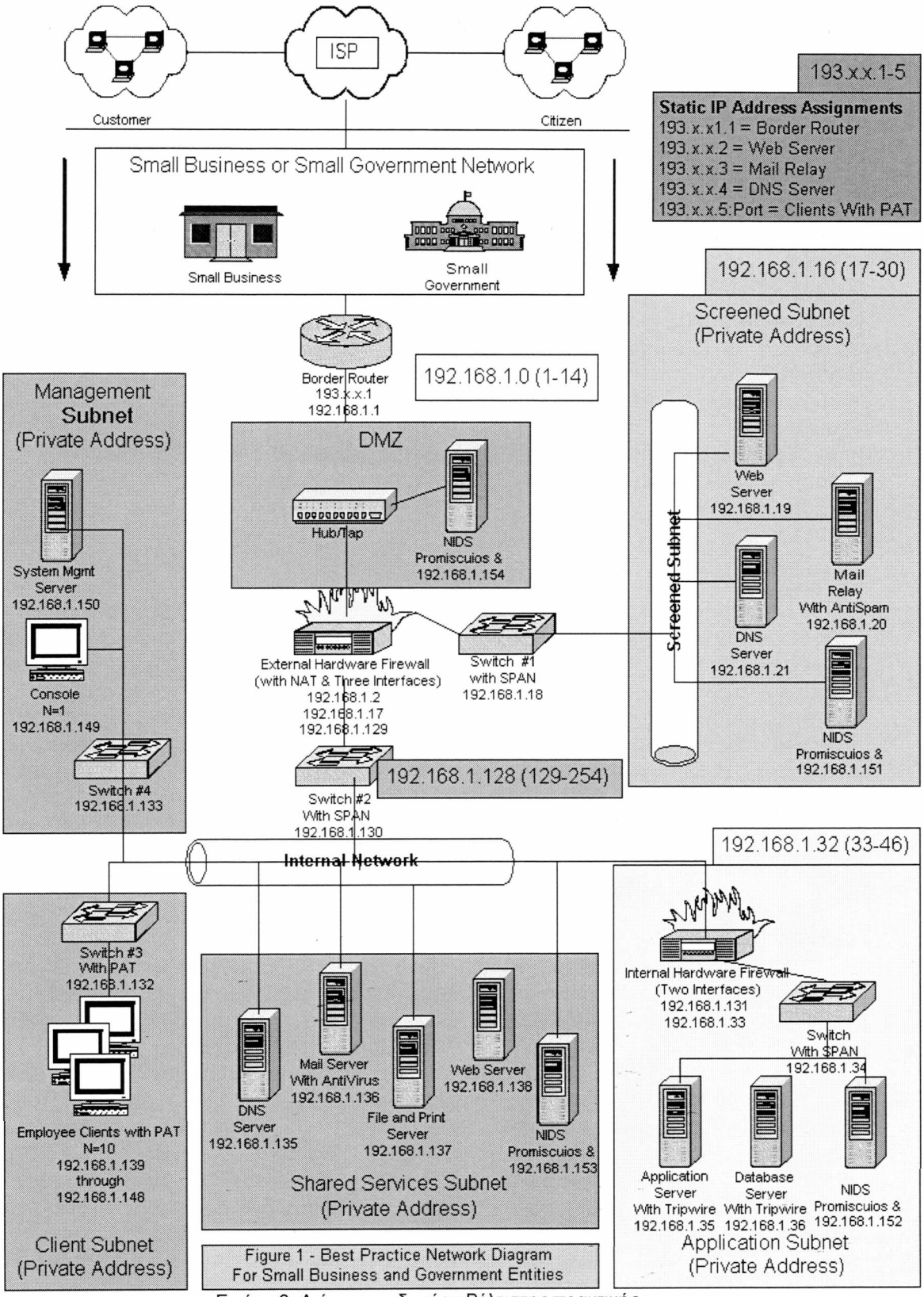
Οι ανησυχίες σχετικά με την ασφάλεια των δικτύων δεν ήταν ποτέ μεγαλύτερες, ωστόσο τα περισσότερα επιχειρηματικά δίκτυα, εταιρικά δίκτυα και τα δίκτυα της κυβέρνησης εξακολουθούν να είναι σε μεγάλο κίνδυνο. Η κατάσταση αυτή οφείλεται κυρίως στο γεγονός ότι τα περισσότερα δίκτυα είχαν υλοποιηθεί σε μια εποχή που η ασφάλεια δεν ήταν μια ισχυρή επιχειρηματική προτεραιότητα. Για να αντιμετωπιστεί το θέμα αυτό, τα δίκτυα θα πρέπει να επανασχεδιαστούν με γνώμονα την ασφάλεια. Διαμορφώσεις του δικτύου θα πρέπει να τροποποιηθούν, πρόσθετο υλικό και λογισμικό θα απαιτηθεί και οι ευθύνες θα αυξηθούν. Ακόμα και σε αυτούς τους καιρούς των αυστηρών περιορισμών του προϋπολογισμού, είναι υποχρέωση των επιχειρήσεων και της κυβέρνησης για την αντιμετώπιση αυτής ως επιτακτικής ανάγκης. Ολική ή μερική αποφυγή αυτής της ευθύνης δεν είναι πλέον αποδεκτή.

Θα παρουσιαστούν για κάθε τμήμα του δικτύου οι καλύτερες πρακτικές για ένα σωστά σχεδιασμένο δίκτυο. Μέσα από στοχαστική και σκόπιμη εφαρμογή αυτών των βέλτιστων πρακτικών ενός ασφαλούς περιβάλλοντος που μπορεί να δημιουργηθεί.

## 6.1 Διάγραμμα Δικτύου

Το διάγραμμα δικτύου, που απεικονίζεται στο Σχήμα 1, απεικονίζει ένα διάγραμμα δικτύου βέλτιστης πρακτικής. Πολλές μικρές επιχειρήσεις και μικρές κυβερνητικές υπηρεσίες θα πρέπει να είναι σε θέση να αξιοποιήσουν αυτό το βασικό σχεδιασμό του δικτύου για να εξασφαλίσουν την καλύτερη ασφάλεια των υφιστάμενων δικτύων τους.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79




Εικόνα 3: Διάγραμμα δικτύου Βέλτιστης πρακτικής

## 6.2 Client Access(Πρόσβαση του Πελάτη):

Οι πελάτες και οι πολίτες θα έχουν πρόσβαση σε συστήματα που βασίζονται στο Internet μέσω διαφόρων **Internet Service Provider** (Παροχών Υπηρεσιών

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Διαδικτύου) (**ISP**). Η ταχύτητα με την οποία έχουν πρόσβαση στο Internet θα ποικίλει επίσης (π.χ. dial-in, ψηφιακή γραμμή, καλώδιο, κ.λπ.). Επιπλέον, είναι πολλές διαφορετικές μάρκες και εκδόσεις των διασυνδέσεων του προγράμματος περιήγησης. Είναι ζωτικής σημασίας, ακόμη και σε ετερογενές περιβάλλον, να είναι γνωστό ότι οι ενδιαφερόμενοι έχουν υψηλό βαθμό εμπιστοσύνης στην ασφάλεια της σύνδεσης. Επιπλέον, η προστασία της ιδιωτικής ζωής των ενδιαφερομένων θα πρέπει να προστατεύεται με το ίδιο ποσό της δέουσας επιμέλειας.

Οι Επιχειρήσεις και οι κυβερνητικές υπηρεσίες θα πρέπει να δημοσιεύουν το περιεχόμενο που σαφώς επικοινωνεί-συνδέει τις προσπάθειές τους για την ασφάλεια των δεδομένων και την προστασία της ιδιωτικής ζωής των ενδιαφερομένων μερών. Τα παραδείγματα περιλαμβάνουν "security seals", τα οποία αναφέρουν ότι η παρουσία web μιας οικονομικής οντότητας έχει πιστοποιηθεί από ένα έμπιστο τρίτο μέρος και οι δηλώσεις προστασίας προσωπικών δεδομένων θα πρέπει να προστατεύονται. Και οι δύο αυτές μέθοδοι αποτελούν εξαιρετικό τρόπο για την επικοινωνία και την παροχή, με ισχυρή εταιρική δέσμευση, των δεδομένων με εχεμύθεια και ακεραιότητα. Η χρήση άλλων λιγότερο υπολογίσιμων τεχνολογιών, όπως **Secure Sockets Layer** (**SSL**) και κρυπτογραφημένων cookies συνεδρίας, δημιουργεί ένα κλίμα εμπιστοσύνης μεταξύ των ενδιαφερομένων.

## 6.3 ISP:

Επιχειρήσεις και κρατικοί φορείς προμηθεύονται πρόσβαση στο Internet μέσω διαφόρων μέσων. Συμφωνίες με τοπικές εταιρείες τηλεπικοινωνιών ή με μεγάλες κυβερνητικές υπηρεσίες (που παρέχουν τηλεπικοινωνιακές υπηρεσίες ως ενδιάμεσοι πάροχοι υπηρεσιών) είναι κλασικά παραδείγματα τέτοιων ρυθμίσεων. Ταχύτητες μετάδοσης ποικίλλουν από low-end συνδέσεις των 64kbps, σε μέτριες T1 συνδέσεις, σε υψηλότερες ταχύτητες σύνδεσης των T3, OC3, ή ακόμα και μεγαλύτερη. Η ISPs υπηρεσία αναθέτει την απαραίτητη στατική δημόσια **Internet Protocol** (**IP**) για να επιτρέπει στις επιχειρήσεις να επικοινωνούν με το κοινό. Οι επιχειρήσεις και η εγγραφή τους σε αυτές τις διευθύνσεις IP, σε συγκεκριμένους τομείς, καθορίζουν τις εν λόγω διευθύνσεις IP / domains για τους κατάλληλους **DNS** servers.

## 6.4 Border Router:

Το Διαδίκτυο δεν μπορεί να λειτουργήσει χωρίς δρομολογητές(routers), στην πραγματικότητα χρησιμοποιούνται υψηλής απόδοσης routers για να υποστηρίξουν τη ραχοκοκαλιά του Διαδικτύου. Λειτουργικά, η κίνηση των τους γίνεται χρησιμοποιώντας τις διευθύνσεις IP. Οι Border routers γενικά θεωρείται ότι αποτελούν το εξωτερικό πλέον άκρο ενός perimeter δικτύου. Σε ορισμένες περιπτώσεις, ο **ISP** μπορεί να διαχειριστεί τους δρομολογητές σε περίπτωση που οι επιχειρήσεις και η κυβέρνηση μπορεί να χρειαστούν να ζητήσουν ορισμένες αλλαγές που πρέπει να γίνουν στο router από τον ISP. Οι Border Router γενικά θεωρούνται ότι είναι η πρώτη γραμμή άμυνας του δικτύου και μπορεί να υποχρεωθούν να επεξεργαστούν ένα μεγάλο ποσό της κίνησης IP. Για το λόγο αυτό, είναι μια βέλτιστη πρακτική να καθοριστεί ένα περιορισμένο σύνολο κανόνων υψηλού επιπέδου στην **Access Control List** (Λίστα δρομολογητή ελέγχου πρόσβασης) (**ACL**). Αυτή η μέθοδος εφαρμογής κανόνα κρατά την επίδραση της απόδοσης στο ελάχιστο, ενώ την ίδια στιγμή παρέχει ένα αρχικό σημείο φιλτραρίσματος για ανεπιθύμητες ή ύποπτες κινήσεις. Οι κανόνες της ACL είναι που εφαρμόζονται στην κυκλοφορία IP καθώς δρομολογούνται στο δίκτυο της υπηρεσίας.

Θα πρέπει να ληφθεί ειδική μέριμνα για να εξασφαλιστεί ότι οι δρομολογητές δεν περιλαμβάνονται. Για κάθε μέτρο του δυνατού, ο δρομολογητής ACL πρέπει να

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

ορίζεται σε πλεονασμό σε εσωτερικές συσκευές παρέχοντας έτσι ένα επιπλέον επίπεδο άμυνας.

## 6.5 DMZ:

Μια 'αποστρατικοποιημένη ζώνη' (De-Militarized Zone) ορίζεται γενικά σαν μια ανεξέλεγκτη ζώνη μεταξύ ελεγχόμενων ζωνών. Στο παρελθόν ο όρος DMZ χρησιμοποιήθηκε καταχρηστικά από την IT βιομηχανία. Πιο πρόσφατα, η κοινότητα της πληροφορικής χρησιμοποιεί τον όρο DMZ με περισσότερη ακρίβεια ως την περιοχή μεταξύ του δρομολογητή border και του εξωτερικού firewall. Λόγω του γεγονότος ότι οι DMZ είναι ανασφαλείς πρέπει να χρησιμοποιούνται μιας χρήσης ή γρήγορα ανακτήσιμες συσκευές/υπολογιστές σε μια τέτοια ζώνη. Είναι σημαντικό να σημειωθεί ότι οι συσκευές μπορεί να μην είναι "φθηνές" αλλά είναι το ίδιο διαθέσιμες. Η DMZ περιέχει ένα κομβικό σημείο επικοινωνίας με ένα σύστημα ανίχνευσης εισβολών στο δίκτυο.

## 6.6 NIDS:

Τα **NIDS** λειτουργούν παρόμοια με ένα ενεργοποιημένο σύστημα συναγερμού το οποίο παρατηρεί γνωστές **signatures** (υπογραφές) οι οποίες υποδηλώνουν ύποπτη δραστηριότητα ή ακόμα εισβολές στο δίκτυο. Τα NIDS είναι ζωτικής σημασίας για οποιαδήποτε ασφαλή αρχιτεκτονική δικτύου, παρέχοντας έτσι ένα βασικό επίπεδο άμυνας σε ένα σωστά σχεδιασμένο δίκτυο. Συνήθως αναπτύσσονται σε στρατηγικά σημεία του δικτύου, με μία προφανή θέση στην DMZ. Ένας αισθητήρας NIDS τοποθετημένος στην DMZ έχει την δυνατότητα να παρακολουθεί ολόκληρη την κίνηση προτού περάσει στο firewall. Ο αισθητήρας θα πρέπει να είναι τουλάχιστον ευαίσθητος και περισσότερο ενεργός από τις υπόλοιπες εφαρμογές του NIDS στο δίκτυο. Για αυτό το λόγο, ο αισθητήρας στην DMZ θα είναι πιθανόν ο περισσότερο ενεργός και θα αναφέρει ακόμα και τις πιο ψευδείς ειδοποιήσεις.

Τα δίκτυα που βασίζονται σε IDS υπερέχουν σε ορισμένους τομείς ανάλυσης και προσφέρουν ιδιαίτερες δυνατότητες, τις οποίες οι άλλες μορφές IDS(όπως Host και Stack)δεν προσφέρουν. Συγκεκριμένα, παρέχονται οικονομίες κλίμακας λόγω του γεγονότος ότι ένας μικρός αριθμός αισθητήρων NIDS που μπορεί να αναλύσει την κίνηση για ολόκληρο το δίκτυο, με ελάχιστες απαιτήσεις σε λογισμικό και σε διαχείριση. Η ανάλυση των πακέτων σε πραγματικό χρόνο διευκολύνει τον εντοπισμό κακόβουλων ή ύποπτων δεδομένων τόσο για την πλήρη όσο και για την κατακερματισμένη κίνηση IP. Τα πακέτα μπορούν να αναλυθούν για **signatures** από συγκεκριμένες επιθέσεις. Επιπλέον, η ανίχνευση σε πραγματικό χρόνο αναστέλλει σημαντικά την ικανότητα ενός hacker να καλύψει τα ίχνη του και υπάρχει η δυνατότητα επίσης της απάντησης στην απειλή σε πραγματικό χρόνο μόλις ανιχνευτεί. Άλλα οφέλη περιλαμβάνουν την ασφάλεια στην πολιτική της επαλήθευσης και επικύρωσης και ανεξάρτητο λειτουργικό σύστημα(δηλαδή τα NIDS δεν εξαρτώνται από το λειτουργικό σύστημα).

Το λογισμικό **COTS**(**commercial-off-the-shelf**) των NIDS μπορεί να είναι ακριβό. Από την άλλη, πολλά προϊόντα NIDS διατίθενται δωρεάν. Ενώ το λογισμικό **COTS** αυξάνει το επιπλέον κόστος, τα οφέλη που προκύπτουν αξίζουν την επένδυση. Η προστιθέμενη αξία από τα εμπορικά προϊόντα περιλαμβάνει εξελιγμένη ανάλυση από άκρη σε άκρη και ενοποιημένη λειτουργικότητα αναφοράς. Το προφανές πλεονέκτημα του εν λόγω λογισμικού είναι διττό. Καταρχάς, οι επιθέσεις του δικτύου μπορούν να παρακολουθούνται ενεργά και μπορούν να ληφθούν προληπτικά μέτρα για την προστασία τόσο της εκούσιας όσο και της ακούσιας κακόβουλης ζημιάς. Δεύτερον, θα πρέπει να λαμβάνουν λιγότερους πόρους προσωπικού για την αναθεώρηση και την απόκριση σε καλά σχεδιασμένες εγκαταστάσεις αναφοράς. Εάν μια επιχείρηση ή μια κρατική οντότητα λειτουργεί με έναν ελάχιστο προϋπολογισμό τότε τα λογισμικά **NIDS**, που διατίθενται δωρεάν, είναι

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

μια βιώσιμη επιλογή. Τα πλεονεκτήματα αυτής της λύσης είναι ότι οι αρχικές δαπάνες είναι ελάχιστες, το προσωπικό οικειοποιείται με την τεχνογνωσία, και αργότερα όταν οι προϋπολογισμοί περιλαμβάνουν πόρους για εμπορικές λύσεις NIDS τότε μια περισσότερο πεπειραμένη αξιολόγηση, επιλογή και εφαρμογή μπορεί να συμβεί.

Ο τυπικός αισθητήρας του **NIDS** έχει δύο κάρτες διασύνδεσης δικτύου (**Network Interface Cards**). Στην πρώτη έχει ανατεθεί μια συγκεκριμένη διεύθυνση IP και η άλλη **NIC** τρέχει σε ετερόκλητη λειτουργία(χωρίς να έχει ανατεθεί διεύθυνση IP). Ολόκληρη η κυκλοφορία διέρχεται μέσα από τον αισθητήρα και το φίλτρο του πρώτου επιπέδου καθορίζει ποια κίνηση θα απορριφθεί. Η υπολειπόμενη κίνηση αποστέλλεται σε μια μονάδα αναγνώρισης επίθεσης που σαρώνει την κυκλοφορία IP για ύποπτη κίνηση χρησιμοποιώντας, μια ανωμαλία ή ένα μοτίβο ή διάφορες τεχνικές συχνότητας. Ένας αισθητήρας NIDS είναι συνήθως συνδεδεμένος σε έναν διανομέα ή σε κόμβο ή σε ένα **Switch Port Analyzer**(**SPAN**). Ένας κόμβος(hub) διαρρύθμισης είναι πολύ οικονομικός και λιγότερο περίπλοκος για να διαμορφωθεί. Η κύρια αδυναμία αυτού του σχεδιασμού είναι ότι οι κόμβοι ίσως δυσλειτουργούν σε περιόδους κυκλοφορίας υψηλού όγκου κίνησης. Οι **taps**(κρουνοί) είναι πιο δαπανηρή λύση, ωστόσο παρέχουν ανοχή σε σφάλματα. Μπορούν επίσης παρακολουθούν πολλαπλές θύρες χωρίς την προσθήκη επιπλέον ρυθμίσεων στο δίκτυο. Όπως οι κόμβοι(hubs), έτσι και οι διαμορφώσεις **SPAN** είναι σχετικά απλοί στην εγκατάσταση και στην διαχείριση και δεν απαιτούν επιπλέον υλικό. Το κυριότερο μειονέκτημα της **SPAN** είναι ότι μπορεί να υπάρξει μόνο μία θύρα για κάθε διακόπτη.

Οι αισθητήρες του δικτύου **IDS** στο **Shared Services Subnet** θα πρέπει να είναι πολύ ευαίσθητοι και οι ειδοποιήσεις που εμφανίζονται συχνά σε αυτό το υποδίκτυο, θα πρέπει να θεωρούνται ως εχθρικές μέχρις αποδείξεως του εναντίον. Οι ψευδείς ειδοποιήσεις σε αυτήν την ζώνη θα πρέπει να είναι περιορισμένες και η απάντηση σε οποιαδήποτε ειδοποίηση θα πρέπει να είναι άμεση και εστιασμένη.

## 6.7 Firewall:

Τα Firewalls χρησιμοποιούνται για να αποτρέψουμε ή να επιτρέψουμε την κυκλοφορία IP σε ένα δίκτυο. Ακριβώς όπως συμβαίνει και με την DMZ, η χρήση αυτής της ορολογίας δεν είναι όπως ακριβώς αναμένεται. Στον κλάδο των κατασκευών, το Firewall είναι ένα μέσο προστασίας από ένα στερεό τοίχο. Οι δύο κύριοι σκοποί του firewall είναι η σταθεροποίηση του κτιρίου και η επιβράδυνση της εξάπλωσης της φωτιάς. Στην κατασκευαστική βιομηχανία τα Firewall δεν θα έχουν σχεδόν ποτέ "τρύπες" που να επιτρέπουν την "ελεγχόμενη πρόσβαση". Στο χώρο της πληροφορικής τα Firewall εξυπηρετούν ένα παρόμοιο σκοπό, που είναι η σταθεροποίηση της υποδομής και ο περιορισμός ανεπιθύμητων ή δυνητικά επιβλαβών κακόβουλων κυκλοφοριών IP. Ωστόσο, τα Firewalls πρέπει να επιτρέπουν την ελεγχόμενη πρόσβαση, ως εκ τούτου ο σκοπός του Firewall δεν είναι ο ίδιος με τον αντίστοιχο σκοπό στην κατασκευαστική βιομηχανία. Στο χώρο της πληροφορικής τα Firewall είναι "door-keepers" που επιτρέπουν την είσοδο μόνο όταν τηρούνται οι προϋποθέσεις στους κανόνες σε μια **ACL**. Οι κανόνες του Firewall δεν είναι ποτέ τέλειοι και δεν μπορούν να αποφανθούν με ακρίβεια αν η εισερχόμενη κίνηση είναι επικίνδυνη. Ως εκ τούτου θα χρειαστούν και άλλοι μηχανισμοί υποστήριξης για να αντιμετωπιστεί το θέμα αυτό. Υπάρχουν τρεις βασικοί τύποι Firewall:**packet filtering**, **stateful packet inspection** και **proxy**. Τα packet filtering firewalls θεωρούνται "ανόητα" λόγω του ότι οι συνθήκες με την πάροδο του χρόνου δεν λαμβάνονται υπόψιν και οι κανόνες που εφαρμόζονται βασίζονται σε ένα περιορισμένο σύνολο πληροφοριών. Τα Stateful packet filtering firewalls είναι "έξυπνα", δεδομένου ότι η κατάσταση της κυκλοφορίας μπορεί να αναλυθεί. Περιλαμβάνουν το απαραίτητο λογισμικό ώστε να διατηρείται η κατάσταση και να καθοριστεί εάν η εισερχόμενη ή εξερχόμενη κίνηση είναι νόμιμη με βάση την προηγούμενη ροή κυκλοφορίας. Για μικρές επιχειρήσεις, τα firewalls θα πρέπει να

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

έχουν γενικώς δύο ή τρεις διασυνδέσεις. Τα firewalls με περισσότερα από τρία interface μπορεί να είναι περίπλοκα στην διαχείρισή τους και μπορεί να έχουν κενά ασφαλείας εάν ρυθμιστούν εσφαλμένα.

## 6.8 VLANS:

Τα εικονικά τοπικά δίκτυα (**Virtual Local Area Networks**) διαχωρίζουν ένα φυσικό **LAN** στα λογικά του μέρη. Αυτό επιτρέπει στον διαχειριστή του δικτύου να εγκαταστήσει εικονικά **LANs** τα οποία αντικατοπτρίζουν τις ανάγκες και τα γεωγραφικά χαρακτηριστικά της επιχείρησης. Τα **VLANs** απομονώνουν την κυκλοφορία του δικτύου και ως εκ τούτου βελτιώνουν την απόδοσή του. Επίσης προσφέρουν το πρόσθετο όφελος της λογικής του διαχωρισμού του δικτύου, το οποίο έχει πλεονεκτήματα που σχετίζονται με την ασφάλεια. Ωστόσο ο διαχωρισμός του δικτύου δεν είναι ακόμα τόσο καλός όσο ο φυσικός διαχωρισμός. Συνεπώς, η χρήση των **VLANs** είναι μια αποδεκτή πράξη αλλά δεν πρέπει να θεωρείται ως ο ακρογωνιαίος λίθος της στρατηγικής ασφαλείας.

## 6.9 Switches:

Ένα **switch** είναι μια βασική συσκευή του δικτύου που συνδέει υπολογιστές(**servers**, **workstations**) στο δίκτυο. Το switch λαμβάνει κίνηση στο δίκτυο από συσκευές όπως routers, firewalls, και άλλα switch και την μεταβιβάζει στο κατάλληλο δίκτυο με βάση ένα **Machine Address Control** (**MAC**). Κάθε συσκευή υποδοχής έχει μοναδική **MAC** διεύθυνση, καθώς και μοναδικό αριθμό πρωτοκόλλου TCP/IP που έχει εκχωρηθεί. Η πρωταρχική διαφορά στην λειτουργία μεταξύ της διεύθυνσης IP και της διεύθυνσης MAC, είναι ότι η διεύθυνση MAC έχει ανατεθεί μόνιμα στον κεντρικό υπολογιστή, ενώ η TCP/IP διεύθυνση μπορεί να αλλάξει με την πάροδο του χρόνου. Αυτά τα δυο κομμάτια των πληροφοριών όταν συνδυάζονται μαζί δημιουργούν μια μοναδική ψηφιακή διεύθυνση που δεν μοιάζει με καμία άλλη.

## 6.10 Screened Subnet

Είναι φυσικά τμήματα του δικτύου που έχουν οριστεί να φιλοξενήσουν μόνο servers που επιτρέπουν την πρόσβαση από και προς το Διαδίκτυο. Το φιλτραρισμένο δευτερεύον δίκτυο είναι εκεί όπου οι πληροφορίες της τεχνολογίας, όπως τα συστήματα ή τα υλικά που χρησιμοποιούνται κατά την διάρκεια της επιχειρηματικής δραστηριότητας, φιλοξενούνται. Αυτό συμβαίνει επειδή, χωρίς να είναι απόλυτα ασφαλείς, οι servers μπορούν να ασφαλιστούν μέχρι ένα επαρκές επίπεδο για την διεξαγωγή των επιχειρήσεων με ένα αποδεκτό ποσό κινδύνου. Οι αιτήσεις πρόσβασης μπορεί να προέρχονται από εξωτερικές πηγές όπως πελάτες ή πολίτες καθώς και από το προσωπικό που βρίσκεται στο εσωτερικό Δίκτυο. Αυτό το δευτερεύον δίκτυο θα χρησιμοποιήσει ένα από τα τρία interface του δικτύου στο εξωτερικό τείχος προστασίας. Το φιλτραρισμένο δεύτερον δίκτυο φιλοξενεί ένα **Domain Name System**(**DNS**) server, mail server, web server και αισθητήρα δικτύου IDS. Οι στατικές διευθύνσεις IP έχουν εκχωρηθεί στον Web Server, Mail Server και στον DNS Server. Η αναγκαία καταχώριση domain και οι εγγραφές DNS πρέπει να γίνουν έτσι ώστε ο πελάτης να μπορεί να έχει πρόσβαση στους servers μέσω του Διαδικτύου. Το firewall θα πρέπει να ρυθμιστεί έτσι ώστε αυτές οι έγκυρες διευθύνσεις IP να μεταφράζονται στις κατάλληλες ιδιωτικές διευθύνσεις χρησιμοποιώντας **Network Address Translation** (**NAT**).

## 6.11 Web Server(Internet):

Στις περισσότερες περιπτώσεις η πρόσβαση στο Διαδίκτυο θα πρέπει να χρησιμοποιεί μόνο την θύρα 80 και την 443. Μπορεί να είναι αναγκαίο να επιτραπούν οι θύρες 20 και 21 για το αρχείο **Transfer Protocol**(**File Transfer Protocol**). Ωστόσο είναι απολύτως κρίσιμο ότι καμία περιττή θύρα ή υπηρεσία δεν θα λειτουργεί άσκοπα στο Web Server. Επιπλέον, μόνο προκαθορισμένες και αξιόπιστες υπηρεσίες/θύρες

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

θα πρέπει να επιτρέπονται μέσω του εξωτερικού firewall στους **Application Database Servers.** Η διοίκηση του Server του λειτουργικού συστήματος θα πρέπει να εκτελείται τοπικά. Εάν είναι δυνατόν, άλλη χρήση του απομακρυσμένου ελέγχου μπορεί να είναι απαραίτητη αλλά θα πρέπει να επιτρέπεται από την διοίκηση του υποδικτύου.

## 6.12 Mail Relay Server:

Ένα επιπλέον επίπεδο προστασίας μπορεί να εισαχθεί στο σχεδιασμό του δικτύου με την τοποθέτηση του Mail Relay μέσα στο φιλτραρισμένο δευτερεύον δίκτυο. Αυτός ο server λειτουργεί ως μεσάζων και λαμβάνει την κυκλοφορία **SMTP** τόσο από το διαδίκτυο όσο και από το εσωτερικό δίκτυο και έπειτα προωθεί την κίνηση στον κατάλληλο προορισμό. Το firewall θα πρέπει να επιτρέπει την κυκλοφορία **SMTP** και να ρέει μέσα και έξω από το φιλτραρισμένο δευτερεύον δίκτυο. Θα πρέπει επίσης να επιτρέπει την ροή κυκλοφορίας από το Relay Mail στο εσωτερικό διακομιστή αλληλογραφίας(**Internal Mail Server**) και το αντίστροφο. Η προσθήκη ενός Mail Relay επιτρέπει το μήνυμα να αποσταλεί και να ληφθεί από το Διαδίκτυο, ενώ παράλληλα τοποθετεί τα κρίσιμα μηνύματα ηλεκτρονικού ταχυδρομείου στις κοινόχρηστες υπηρεσίες υποδικτύου. (**Shared Services Subnet**). Αυτός ο server θα πρέπει επίσης να διαθέτει antispam λογισμικό για την εξάλειψη ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου.

## 6.13 DNS Server:

Η ίδια αρχή που εφαρμόζεται στον Mail Server εφαρμόζεται και στον **DNS Server**. Μέσα από την δημιουργία μιας διαμόρφωσης Split DNS, οι ευάλωτες πληροφορίες DNS μπορούν να τοποθετηθούν στις κοινόχρηστες υπηρεσίες του Υποδικτύου(**Shared Services Subnet**) ενώ οι δημόσιες πληροφορίες DNS θα βρίσκονται στο φιλτραρισμένο δευτερεύον υποδίκτυο. Η διαμόρφωση μπορεί να καθοριστεί έτσι ώστε οι εσωτερικοί πελάτες που χρειάζονται πληροφορίες DNS από το Διαδίκτυο να μπορούν να προμηθευτούν τις απαραίτητες πληροφορίες από τον DNS Server στο φιλτραρισμένο δευτερεύον δίκτυο. Για να διασφαλιστεί η ασφάλεια των πληροφοριών που είναι αποθηκευμένες σε αυτόν τον server, δεν θα πρέπει να επιτρέπονται οι DNS Zone Transfers.

## 6.14 Shared Services Subnet:

Οι κοινές υπηρεσίες του υποδυκτίου **Shared Services Subnet** (SSS) πρέπει να είναι προσβάσιμες μόνο από τους υπολογιστές που είναι συνδεδεμένοι φυσικά στο εσωτερικό δίκτυο ή από συγκεκριμένους servers στο φιλτραρισμένο δευτερεύον δίκτυο. Η μόνη αξιοσημείωτη εξαίρεση σε αυτό θα είναι ότι οι συνδέσεις απομακρυσμένης πρόσβασης γίνονται μέσω μιας σύνδεσης **VPN** με το εσωτερικό δίκτυο από έναν πιστοποιημένο και εξουσιοδοτημένο telecommuter ή μετακινούμενο εργαζόμενο. Ορισμένες εταιρίες όπως η CISCO, κατασκευάζουν VPN λύσεις στα firewall προϊόντα τους. Οι εσωτερικές DNS, Mail, Web και File και Print Servers συνήθως είναι η καρδιά αυτού του τμήματος του δικτύου.

### 6.14.1 Mail Server:

Το εσωτερικό Mail Server λαμβάνει mail από τους πελάτες του εσωτερικού ταχυδρομείου καθώς και από το Mail Relay στο φιλτραρισμένο δευτερεύον δίκτυο. Ο Mail Server είναι συχνά ένα ισχυρό προσανατολισμένο προϊόν λογισμικού, όπως το **Microsoft Exchange** ή **IBM Lotus Notes/Domino**. Άλλες λύσεις διακομιστή αλληλογραφίας θα μπορούσαν να χρησιμοποιήσουν προγράμματα με λιγότερες απαιτήσεις(όπως **Sendmail**). Σε κάθε περίπτωση, το βασικό σημείο είναι ότι τα μηνύματα ταχυδρομείου κρίσιμης σημασίας αποθηκεύονται πίσω από το εξωτερικό firewall και είναι πολύ πιο προστατευμένα από την επίθεση. Επίσης, θα ήταν μια

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

καλύτερη πρακτική να εγκατασταθεί λογισμικό προστασίας από ιούς και να εκτελείται στον server ώστε να τον προστατεύει.

### 6.14.2 DNS Server:

Όπως ήδη συζητήθηκε στο φιλτραρισμένο δευτερεύον δίκτυο, ο **DNS** Server που είναι εγκατεστημένος στο **Shared Services Subnet** περιέχει τις πληροφορίες σχετικά με τις κρίσιμες εφαρμογές, βάσεις δεδομένων και υποδομές. Είναι κρίσιμο ότι αυτές οι πληροφορίες δεν θα είναι άμεσα διαθέσιμες μέσα στο Διαδίκτυο. Οποιαδήποτε διαρροή ή έκθεση αυτών των ευαίσθητων πληροφοριών θα μπορούσε να είναι εξαιρετικά χρήσιμη για κάποιον hacker. Ακριβώς όπως συνέβη στην περίπτωση του **DNS** Server στο φιλτραρισμένο δευτερεύον δίκτυο, οι **DNS** Zone Transfers δεν θα πρέπει να επιτρέπονται από αυτόν τον διακομιστή.

### 6.14.3 Web Server:

Ο εσωτερικός Web Server εκτελεί Intranet συσχετιζόμενα καθήκοντα και δεν θα πρέπει να είναι προσβάσιμα από το Διαδίκτυο. Όλες οι περιττές θύρες και υπηρεσίες θα πρέπει να κλείσουν και οι servers να ασφαλιστούν. Οι κωδικοί πρόσβασης του χρήστη και του διαχειριστή θα πρέπει να είναι δυνατοί. Είναι πολύ πιθανό ότι αυτός ο server θα πρέπει να επικοινωνεί με τους **Application** και **Database Servers** στο **Application Subnet**. Το λειτουργικό σύστημα της διοίκησης θα πρέπει να εκτελείται τοπικά ή μέσω του διοικητικού Subnet.

### 6.14.4 File and Print:

Οι κρίσιμοι servers αρχείων και εκτύπωσης πρέπει επίσης να βρίσκονται στο **Shared Services Subnet** (SSS) και να μην είναι διαθέσιμοι μέσω του Διαδικτύου. Οι servers των αρχείων προφανώς περιέχουν περιουσιακά στοιχεία ζωτικής σημασίας για την εταιρεία, όπως τις πληροφορίες ευρεσιτεχνιών, την εταιρική στρατηγική, έγγραφα, εταιρικές οικονομικές καταστάσεις. Οι server εκτύπωσης μπορούν εύκολα να εκμεταλλευθούν από επιθέσεις. Δεν είναι ασυνήθιστο για τον server να λειτουργεί μια παρωχημένη έκδοση ενός λειτουργικού συστήματος που οφείλεται σε συγκεκριμένες απαιτήσεις υλικού ή της επιχείρησης. Είναι εξ ολοκλήρου δυνατό ένας εκτυπωτής δικτύου να παραβιαστεί και να χρησιμοποιηθεί για την αποθήκευση ανεπιθύμητων γραφικών εικόνων σε μεγάλες μονάδες δίσκου που είναι γενικώς αχρησιμοποίητες.

### 6.14.5 Application Subnet:

Είναι όπου βρίσκονται μερικά από τα πιο πολύτιμα περιουσιακά στοιχεία(δεδομένα της επιχείρησης). Στην περίπτωση των επιχειρήσεων, η κλοπή της αίτησης της επιχειρηματικής λογικής ή τα δεδομένα της εφαρμογής, θα μπορούσε να θέσει σε κίνδυνο πολύτιμα επιχειρησιακά μυστικά, πιθανώς να θέσει σε κίνδυνο το ανταγωνιστικό πλεονέκτημα ή να εκθέσει τους πελάτες της σε πιθανό έγκλημα όπως η κλοπή της πιστωτικής κάρτας/ταυτότητας. Για τις κυβερνήσεις η απώλεια δεδομένων θα μπορούσε να εκθέσει τις ευαίσθητες οικονομικές ή ιατρικές πληροφορίες ενός πολίτη. Και στις δύο περιπτώσεις, η απώλεια της εμπιστοσύνης από τον πελάτη/πολίτη είναι μια βεβαιότητα. Επιπλέον ο πελάτης/πολίτης μπορεί να αναλάβει νομική δράση και να αναζητήσει αποζημίωση για οποιαδήποτε ζημιά έχει συμβεί. Η κλοπή δεδομένων είναι μόνο ένας από τους πολλούς τρόπους ζημιάς. Ένα άλλο παράδειγμα είναι το κακόβουλο λογισμικό το οποίο υπάρχει σε πολλές μορφές(ιοί, worms, trojans) και μπορεί να προξενήσει σοβαρή ζημιά. Οποιαδήποτε τέτοια βλάβη συχνά απαιτεί εκτεταμένη προσπάθεια για θεραπεία. Δεν είναι ασυνήθιστο για τους πληγέντες servers να ξαναχτιστούν και τα δεδομένα να μεταφορτωθούν από ένα σταθερό backup. Για τους ανωτέρω λόγους, το **Application Subnet** θα πρέπει να είναι ένα από τα πιο προστατευμένα τμήματα του δικτύου. Στο σχήμα1 παρατηρούμε ότι το τμήμα είναι φυσικά χωρισμένο από το εσωτερικό δίκτυο

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

από ένα πρόσθετο εσωτερικό Firewall. Αυτό το επιπλέον επίπεδο προστασίας παρέχει ένα πρόσθετο στρώμα άμυνας κατά των επιθέσεων σε κρίσιμες πληροφορίες της επιχείρησης. Για ακόμη μια φορά, το Λειτουργικό σύστημα της διοίκησης θα πρέπει να εκτελείται τοπικά ή μέσω του **Management Subnet**.

## 6.15 Application Server:

Το σύνολο των κανόνων του firewall θα πρέπει να επιτρέπει μόνο την κυκλοφορία IP από ένα συγκεκριμένο Web Server στο φιλτραρισμένο δευτερεύον δίκτυο ώστε να αποκτήσει πρόσβαση στο **Application Server** στο Δευτερεύον δίκτυο εφαρμογών (**Application Subnet**). Οι Application servers θα πρέπει να προστατεύονται μέσω της χρήσης των λογισμικών IDS Host(όπως **Tripwire, RealSecure Server Sensor**) για να προσδιοριστεί εάν έχουν λάβει χώρα μη-εξουσιοδοτημένες αλλαγές ή ύποπτη δραστηριότητα στο δίκτυο που στοχεύουν σε έναν συγκεκριμένο host. Ο κώδικας εφαρμογής(κανόνες των επιχειρήσεων) θα πρέπει να γραφτούν με ασφάλεια και δεν θα πρέπει να είναι επιρρεπής σε κοινές προσπάθειες αποκωδικοποίησης από hackers όπως τα buffer overflows και SQL Injection. Η πρόσβαση στις βάσεις δεδομένων μέσω της εφαρμογής θα πρέπει να πραγματοποιείται χρησιμοποιώντας τις ενδεδειγμένες τεχνικές τις επιχείρησης. Ο κώδικας εφαρμογής θα πρέπει να αποθηκεύεται μόνο με κρυπτογραφημένους κωδικούς πρόσβασης , σχεδιασμένους κατάλληλα ώστε να αποκτά πρόσβαση στις βάσεις δεδομένων. Η απομακρυσμένη διοίκηση του **Application Server** θα πρέπει να επιτρέπεται μόνο από το υποδίκτυο διαχείρισης (**Management** Subnet). Θα πρέπει να καθιερωθούν και να ακολουθούνται αυστηρά μέτρα ελέγχου για την μετακίνηση του κώδικα στην παραγωγή.

## 6.16 Database Server:

Οι servers των βάσεων δεδομένων(**database servers**) θα πρέπει να είναι από τους περισσότερο προστατευόμενους servers σε ολόκληρη την επιχείρηση. Θα πρέπει να λαμβάνεται μεγάλη φροντίδα για την καταγραφή όλων των αλλαγών στα δεδομένα παραγωγής. Οι ταυτότητες του χρήστη που δίνουν προνόμια στην επιλογή, εισαγωγή, ενημέρωση και διαγραφή θα πρέπει διατηρούνται στο ελάχιστο.

Οι πολιτικές των κωδικών πρόσβασης θα πρέπει να είναι ισχυρές και να ακολουθούνται αυστηρά. Αν αποφασιστεί ότι μια βάση δεδομένων έχει παραβιαστεί ή εκτεθεί, τότε το άμεσο ερώτημα που τίθεται είναι : "τι έκανε ο hacker για να αποκτήσει πρόσβαση στις βάσεις δεδομένων και ποια δεδομένα έχει κλέψει ή καταστρέψει;". Για να απαντήσουμε σε αυτό το ερώτημα, οι μηχανισμοί ελέγχου των βάσεων δεδομένων θα πρέπει να είναι ενεργοποιημένοι. Ένα ιδιαίτερο χαρακτηριστικό στο **Oracle 9i**, το **Flashback Query**, προσφέρει την ικανότητα να καθοριστεί η κατάσταση των δεδομένων σε μία συγκεκριμένη χρονική στιγμή. Τα χαρακτηριστικά των βάσεων δεδομένων είναι: τι ακριβώς χρειάζεται για να βοηθηθεί το σύστημα και πως οι διαχειριστές των βάσεων δεδομένων προσδιορίζουν πόσο επεμβατικό ένα συγκεκριμένο περιστατικό ήταν. Πρέπει να υπάρχει μια αντίληψη ότι οι εγγραφές ελέγχου αυτοκαταγράφονται, συνεπώς μπορεί να έχουν χειραγωγηθεί σε μια προσπάθεια του hacker να καλύψει τα ίχνη του. Σε καμία περίπτωση δεν θα πρέπει οι χρήστες να έχουν την δυνατότητα της πρόσβασης ή ενημέρωσης στις βάσεις δεδομένων χωρίς να χρησιμοποιούν την εφαρμογή **front-end**. Το backup και διαδικασίες ανάκτησης είναι ζωτικής σημασίας. Είναι κρίσιμο τα αντίγραφα ασφαλείας (**backups**) να είναι επικυρωμένα συστηματικά και να αποθηκεύονται σε κατάλληλο χρόνο, έτσι ώστε να μπορούν να ανακτηθούν σε περίπτωση συμβάντος. Τα αντίγραφα ασφαλείας(**backups**) επίσης θα πρέπει να είναι και φυσικώς ασφαλή ώστε να μην υπάρχει κίνδυνος κλοπής τους. Η χρήση των Host IDS τεχνολογιών στον server της βάσης δεδομένων θεωρείται επίσης μια βέλτιστη πρακτική ασφάλειας.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

## 6.17 Management Subnet:

Η διοίκηση υποδικτύου(**Management Subnet**) είναι μια περιοχή που πολλά χαρακτηριστικά του δεν έχουν οριστεί προς το παρόν. Αυτό όμως είναι ένα πολύ σημαντικό υποδίκτυο το οποίο θα πρέπει να δημιουργηθεί και να χρησιμοποιηθεί για να φιλοξενήσει το **Network IDS System Management Server** καθώς και εξ αποστάσεως διαχείριση άλλων συσκευών σε όλο το δίκτυο από μία μόνο κονσόλα. Η διαχείριση θα πρέπει να πραγματοποιείται από τα εργαλεία που παρέχουν ασφαλή μετάδοση της ταυτότητας του χρήστη και κωδικό πρόσβασης όταν εκτελείται έλεγχος ταυτότητας του διαχειριστή. Μέσω της δημιουργίας ενός δικτύου διαχείρισης(**Management Subnet**) της **ACL** μπορούν να οριστούν σε κατάλληλες συσκευές(όπως firewalls, switches, hosts) που αρνούνται την πρόσβαση από οποιαδήποτε συσκευή που δεν έχει οριστεί στο **Management Subnet.**

## 6.18 System Management Server:

Το **System management Server** λειτουργεί ως ένα κεντρικό αποθετήριο πληροφοριών για όλες τις απομακρυσμένες **NIDS** εντός του δικτύου. Συχνά αυτός ο server θα έχει μια βάση δεδομένων όπως η MySQL(είναι ανοιχτού κώδικα σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων) εγκατεστημένη σε αυτόν, παρέχοντας εξελιγμένες λειτουργίες ανάλυσης και αναφοράς. Αυτή η πρόσθετη λειτουργικότητα απλοποιεί σε μεγάλο βαθμό την ανάγκη για ανάλυση των πληροφοριών.

## 6.19 Console:

Η κονσόλα προφανώς χρησιμοποιείται για την απομακρυσμένη διαχείριση συσκευών στα υπόλοιπα διάφορα υποδίκτυα. Ιδανικά **SHH** ή **Telnet**(μέσω **VPN**) θα μπορούσαν να χρησιμοποιηθούν για την απομακρυσμένη διαχείριση των συσκευών του δικτύου. Εάν η τοπική διαχείριση των servers δεν είναι εφικτή, τότε το λογισμικό απομακρυσμένου ελέγχου θα μπορέσει να χρησιμοποιηθεί από αυτόν τον σταθμό εργασίας. Η διοίκηση του Web Server μέσω HTTPS είναι μια άλλη λειτουργία που θα μπορούσε να εκτελεστεί από αυτόν τον σταθμό εργασίας. Η φυσική πρόσβαση σε αυτή την συσκευή θα πρέπει να ελέγχεται αυστηρά. Οι συνήθεις προφυλάξεις ασφαλείας, όπως η είσοδος στο δίκτυο, η ενεργοποίηση ενός κωδικού και ίσως ένας κωδικός πρόσβασης BIOS θα μπορούσαν να χρησιμοποιηθούν ως ένα επιπλέον επίπεδο προστασίας.

## 6.20 Client Subnet:

Για να ελαχιστοποιηθεί ο αριθμός των έγκυρων διευθύνσεων IP που απαιτούνται για την πρόσβασης των πελατών στο δίκτυο, θα πρέπει να χρησιμοποιηθεί **Port Address Translation** (**PAT**). Αυτό μπορεί να γίνει πολύ εύκολα με την εκχώρηση σε κάθε πελάτη μιας **α-routable** ιδιωτικής διεύθυνσης και στη συνέχεια κάνοντας τις απαραίτητες ρυθμίσεις στο firewall, για να αναθέσει την έξοδο κυκλοφορίας της δρομολόγησης της διεύθυνσης 193.c.x.x.5 μαζί με έναν μοναδικό αριθμό θύρας. Μπορούν επίσης να ληφθούν επιπλέον μέτρα άμυνας για την περαιτέρω διασφάλιση των εσωτερικών πελατών. Πρόσθετα μέτρα θα πρέπει να περιλαμβάνουν την εγκατάσταση ενός firewall με βάση τις ανάγκες του πελάτη, λογισμικό προστασίας από ιούς και κρυπτογράφηση των ευαίσθητων δεδομένων. Η χρήση της τεχνολογίας με αυτόν τον τρόπο παρέχει ένα επιπλέον επίπεδο προστασίας των πελατών από οποιαδήποτε κακόβουλο λογισμικό που μπορεί να γλιστρήσει μέσα από τις άμυνες προστασίας του δικτύου. Αυτές οι άμυνες μπορούν επίσης να προστατεύουν τους εσωτερικούς τους πελάτες από τις δικές τους εσφαλμένες ενέργειες. Με άλλα λόγια, δεν είναι ασυνήθιστο για τους εσωτερικούς πελάτες να παραβιάζουν την πολιτική και ως αποτέλεσμα να γίνονται ευάλωτοι σε επιθέσεις. Παραδείγματα τέτοιων δράσεων περιλαμβάνουν την χρήση άμεσων μηνυμάτων ή εγκατάστασης και χρήση εξωτερικών modem. Πρόσθετα φυσικά μέρα

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

τα οποία θα πρέπει να ληφθούν περιλαμβάνουν μεθόδους ασφαλείας για την προστασία από φυσική κλοπή των φορητών υπολογιστών και τακτική δημιουργία αντιγράφων ασφαλείας τυχόν εταιρικών δεδομένων που είναι αποθηκευμένα σε έναν υπολογιστή.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# 7. Ασφάλεια Δικτύων

**Περίληψη:**

Ασφάλεια Δικτύων γίνεται ένα σημαντικό πρόβλημα για τους διαχειριστές των ΜΜΕ. Η Έλλειψη του χρόνου, ο μικρός προϋπολογισμός και η περιορισμένη εμπειρία είναι μερικά από τα κοινά προβλήματα που αντιμετωπίζουν σήμερα οι περισσότερες μικρές και μεσαίες επιχειρήσεις.

## 7.1 Εισαγωγή

Η μεγάλη πλειοψηφία των σημερινών μικρών και μεσαίων επιχειρήσεων εξαρτώνται από τα IT systems και τα περισσότερα από αυτά πρέπει να έχουν πρόσβαση στο διαδίκτυο για να ελέγξουν την επιχείρησή τους. Ωστόσο, οι απειλές κατά της ασφάλειας στον κυβερνοχώρο γίνονται όλο και πιο πολύπλοκες στοχεύοντας επιχειρήσεις οποιουδήποτε μεγέθους. (McAfee 2008) Κλοπή δεδομένων, διακοπής λειτουργίας του υπολογιστή, μείωση της παραγωγικότητας και απώλεια φήμης δεν είναι πλέον θέματα μόνο μιας μεγάλης εταιρείας. Αν και οι Μικρές και οι Μεσαίες Επιχειρήσεις φαίνονται να αντιμετωπίζουν τους ίδιους κινδύνους με τις μεγάλες εταιρείες, δεν έχουν την ίδια εμπειρία και τον προϋπολογισμό για την αντιμετώπισή τους. Αλλά κύρια δυσκολία τους είναι η έλλειψη χρόνου για να σχεδιάσουν την κατάλληλη περίμετρο ασφαλείας και να διαχειρίζονται τα θέματα ασφαλείας. Παρακάτω θα παρουσιαστεί μια μέθοδος που θα βοηθήσει τους διαχειριστές των ΜΜΕ να σχεδιάσουν μια περίμετρο ασφαλείας που να ταιριάζει στις ανάγκες της εταιρείας.

## 7.2 Το Firewall ως κλειδί για την ασφάλεια της περιμέτρου

Μια περίμετρος ασφαλείας είναι μια ζώνη επιβολής γύρω από το ιδιωτικό δίκτυο για την προστασία των περιουσιακών στοιχείων της εταιρείας. Γενικά αποτελείται από πολλές διαφορετικές συσκευές ή υπηρεσίες ασφαλείας, όπως anti-virus, φιλτράρισμα περιεχομένου, εικονικά ιδιωτικά δίκτυα, συστήματα ανίχνευσης εισβολής, διακομιστές ελέγχου ταυτότητας, σαρωτές ευπαθειών κ.λπ. Ωστόσο, το θεμέλιο κάθε περιμέτρου ασφαλείας είναι το τείχος προστασίας. Πράγματι, το firewall είναι το σημείο εισόδου του ιδιωτικού δικτύου και έτσι η πρώτη γραμμή άμυνας δημιουργεί ένα φραγμό (ή όριο) ανάμεσα στο αξιόπιστο δίκτυο (το ιδιωτικό δίκτυο) και το εξωτερικό (internet) ελέγχοντας όλη την εισερχόμενη και εξερχόμενη κίνηση. Ο σχεδιασμός του τείχους προστασίας είναι ένα ορόσημο για την οικοδόμηση μιας αποτελεσματικής περιμέτρου ασφαλείας.

## 7.3 Η επιλογή του Firewall ώς ένα δύσκολο έργο

Λαμβάνοντας υπόψη τις βασικές λειτουργίες του τείχους προστασίας, η επιλογή του είναι ζωτικής σημασίας για την ασφάλεια μιας εταιρείας. Αλλά δεν είναι χωρίς δυσκολίες. Επιλέγοντας την αρχιτεκτονική και το προϊόν το οποίο ταιριάζει πραγματικά στις ανάγκες της εταιρείας είναι γενικά μια συντριπτική και χρονοβόρα διαδικασία. Η διαδικασία περιλαμβάνει δύο κύριες φάσεις: τον καθορισμό των αναγκών και την αξιολόγηση των διάφορων προϊόντων που διατίθενται στην αγορά. Πριν από την επιλογή firewall, μια αξιολόγηση του κινδύνου πρέπει να εκτελεστεί για να εκτιμηθεί η ανάγκη ασφάλειας. Αυτό το βήμα συνίσταται στον εντοπισμό των κρίσιμων στοιχείων της εταιρείας δηλαδή ότι έχει αξία για την εταιρεία. Επιτρέπει, επίσης να προσδιοριστούν οι αδυναμίες της ασφάλειας της επιχείρησης και έτσι διευκολύνεται η ιεράρχηση των κινδύνων. Ωστόσο, αυτό το βήμα συχνά παρακάμπτεται από τις μικρομεσαίες επιχειρήσεις. Αυτό γενικά συνετέλεσε στις

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

firewall λύσεις, που είτε υπό-εκτιμούν, είτε υπέρ-εκτιμούν τις ανάγκες της εταιρίας. Οι ανάγκες για ασφάλεια πρέπει να εντοπιστούν και η αξιολόγηση των διαθέσιμων προϊόντων είναι το επόμενο λογικό βήμα αλλά όχι το ευκολότερο. Ο λόγος για τον οποίο τα firewalls εκδίδονται σε πολλές διαφορετικές εκδόσεις (hardware, Software, εμπορικές, open-source), είναι ότι ο κάθε πωλητής προσθέτει την δική του έκδοση, τα δικά του ιδιόκτητα εμπορικά σήματα και προσφέρει υποστήριξη με συμβάσεις (Taylor 2002, Shinder 2008, Chapple 2005). Όλα αυτά κάνουν τη σύγκριση πολύπλοκη. Αν το πρωταρχικό βήμα δεν είναι ολοκληρωμένο και σαφές, τότε είναι εύκολο να επηρεαστεί από τις firewall προσφορές και να αγοράσει ένα τείχος προστασίας που φαίνεται να ταιριάζει αλλά δεν είναι πραγματικά αυτό που ψάχνει η εταιρεία. Η αυξανόμενη πολυπλοκότητα των νέων απειλών, που γενικά σχετίζεται στενά με τη συνεχή εξέλιξη των νέων τεχνολογιών, έχει επιταχύνει σημαντικά την ανάπτυξη των firewalls όλο και πιο πολύπλοκα για το σχεδιασμό και τη συντήρηση τους. Παρά το γεγονός ότι οι ΜΜΕ σκέφτονται να εξοικονομήσουν χρόνο αγοράζοντας firewall ως ένα fit-all προϊόν, το αποτέλεσμα είναι εις βάρος της ασφάλειας της επιχείρησης. Η κύρια αιτία είναι η έλλειψη του χρόνου. Η έκθεση της McAfee δείχνει ότι το ένα τρίτο των βρετανικών ΜΜΕ δαπανούν μόνο μία ώρα την εβδομάδα για την ασφάλεια IT. (McAfee 2008) Προκειμένου να αντιμετωπιστεί αυτό το επαναλαμβανόμενο πρόβλημα στις ΜΜΕ, θα πρέπει να δοθεί μεγαλύτερη στήριξη για να τους βοηθήσει να εφαρμόζουν και να διατηρούν το σύστημα ασφαλείας τους πιο αποτελεσματικά.

## 7.4 Οι Απόφασεις Σχεδίασης του Firewall (FDDM)

Η Απόφαση Σχεδίασης του firewall είναι μια προσέγγιση, η οποία τείνει να παρέχει υποστήριξη στις ΜΜΕ, στο έργο τους για την επιλογή ενός σχεδιασμού της αρχιτεκτονικής του firewall, με firewall τεχνολογίες (ή το επίπεδο ελέγχου) και τέλος προϊόντα firewall. Η μέθοδος είναι βασισμένη σε ένα τρόπο που να αντανακλά τις ανάγκες της εταιρείας. Στηρίζεται σε βασικά κριτήρια που είναι γνωστό ότι είναι αρκετά αποφασιστικά για να οδηγήσουν σε μια συγκεκριμένη σχεδιαστική λύση firewall. Αυτή η μέθοδος είναι ένα ερωτηματολόγιο βασισμένο σε 4 απλά βήματα:

**Βήμα** 1: προσπαθεί να προσδιορίσει την έκταση της εταιρείας και την ασφάλεια των αντικειμένων της

**Βήμα** 2: προτίθεται να καθορίσει ποια αρχιτεκτονική Firewall ταιριάζει καλύτερα με την ανάγκη της εταιρείας

**Βήμα** 3: καθορίζει ποια τεχνολογία firewall (Filter) είναι η περισσότερο κατάλληλη.

**Βήμα** 4: ερευνά ποιο προϊόν και ποια χαρακτηριστικά ταιριάζουν με τις τεχνικές απαιτήσεις.

### 7.4.1 Step 1: Το πεδίο δράσης της επιχείρησης

Ο σχεδιασμός του τείχους προστασίας εξαρτάται περισσότερο ή λιγότερο από την ειδικότητα της εταιρίας, το μέγεθος, τον τομέα δραστηριότητας, τη γεωγραφία της, την πολυπλοκότητα του δικτύου της, το προσωπικό της και τους επιχειρηματικούς στόχους της. Όμως η πιο σημαντική πτυχή είναι το προφίλ κινδύνου. Αυτό το τελευταίο είναι που καθορίζει το επίπεδο προστασίας που απαιτείται από την εταιρεία. Το προφίλ κινδύνου είναι η σύνθεση των τριών παραμέτρων που σχετίζονται με τα στοιχεία ζωτικής σημασίας όπως η κρισιμότητά τους για την επιχείρηση, η έκθεσή τους και η πιθανότητά τους να είναι κατεστραμμένα. Οι πληροφορίες αυτές είναι το αποτέλεσμα του Κινδύνου Αξιολόγησης, εξ ου και η σημασία να διεξάγεται μια τέτοια διαδικασία πριν από το σχεδιασμό ασφαλείας.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

### 7.4.2 Step 2:Η αρχιτεκτονική ενος Firewall

Τρεις είναι βασικοί τύποι αρχιτεκτονικής τείχους προστασίας που υπάρχουν: Η απλή αρχιτεκτονική **Screening**, η οποία συνίσταται σε ένα μοναδικό κουτί με δύο interface, που χωρίζει το αξιόπιστο δίκτυο από το διαδίκτυο. Η αρχιτεκτονική **Multi-Screening** στην οποία ένα κουτί με περισσότερες από 2 interface επιτρέπουν να συνδεθούν τα δίκτυα διαφορετικού επιπέδου ασφαλείας, και η Διπλή αρχιτεκτονική που κάνει χρήση των δύο firewalls για το διαχωρισμό των εσωτερικών υπηρεσιών και εξωτερικών υπηρεσιών. Οι πρόσθετες ζώνες που δημιουργούνται στην Multi-Screening και στην διπλή Αρχιτεκτονική κοινώς ονομάζονται DMZ (αποστρατικοποιημένη ζώνη). Μια DMZ είναι γενικά μια εξαιρετικά ασφαλή ζώνη, χρησιμοποιείται για την παροχή υπηρεσιών στους χρήστες του διαδικτύου, και έτσι αποφεύγεται μια άμεση επικοινωνία μεταξύ του αξιόπιστου και του μη αξιόπιστου διαδικτύου. Παρά το γεγονός ότι πολλά κριτήρια, όπως η τεχνογνωσία και ο διαθέσιμος χρόνος μπορεί να τεθούν σε εξέταση, επιλέγοντας μια αρχιτεκτονική τείχους προστασίας, η **FDDM** προσέγγιση χρησιμοποιεί μόνο το επικρατέστερα κριτήρια:

**1)**το είδος των υπηρεσιών

**2)**το προφίλ κινδύνου

Η Αρχιτεκτονική του firewall εξαρτάται σαφώς από το είδος των υπηρεσιών που παρέχονται. Με εσωτερικές υπηρεσίες μόνο (πρόσβαση στο Internet σε εσωτερικούς χρήστες), το εύρος των επιθέσεων είναι κάπως περιορισμένο, και η επιλογή της **Simple Screening architecture** έρχεται σχεδόν ως αποδεικτικό στοιχείο. Ωστόσο, αν η εταιρεία αποφασίσει να ανοίξει το δίκτυό της σε εξωτερικούς χρήστες, όπως τηλε-εργαζόμενους, προμηθευτές, εργολήπτες ή τους χρήστες του Διαδικτύου, η **Simple Screening** Firewall δεν αρκεί. Το προφίλ κινδύνου που θα οριστεί, θα πρέπει να αποφασίσει μεταξύ αυτών των δυο. Αν έχει οριστεί σε Υψηλό, τότε το Dual Firewall θα ταιριάζει καλύτερα στην απαίτηση, αλλιώς το Multi-Screening θα είναι αρκετό.

### 7.4.3 Step 3: Η Τεχνολογία του Firewall

Υπάρχουν τέσσερις βασικοί τύποι επιθεώρησης του firewall:

**Packet filtering Inspection, Stateful Inspection, Proxy-level Inspection and Deep Inspection**. Τα προϊόντα του firewall γενικά χρησιμοποιούν ένα συνδυασμό αυτών των τεχνολογιών για να καταστεί δυνατή περισσότερη ασφάλεια, ωστόσο, πολλά προϊόντα πέφτουν σε επικρατέστερη κατηγορία.

Packet filtering Inspection and Stateful Inspection συμβαίνουν στο Network Layer και κυρίως επιθεωρούν την επικεφαλίδα κάθε πακέτου IP και φιλτράρουν βασισμένα στους κανόνες του πρωτόκολλου, την πηγή διεύθυνσης/προορισμού και πηγή/προορισμού port. Το πρώτο είναι στατικό, ενώ το δεύτερο παρακολουθεί την κατάσταση της σύνδεσης ώστε να απορρίψει πακέτα που δεν ανήκουν στις καθιερωμένες συνεδρίες.

Proxy-Level and Deep Inspection filter στην Application Layer είναι ικανά να ανιχνεύσουν κακόβουλο κώδικα και ιούς που περιέχονται στο ωφέλιμο φορτίο των πακέτων. Τα Proxies είναι τα πιο ασφαλή firewall αλλά είναι πολύ συγκεκριμένα και αργούν να προσαρμοστούν σε όλες τις περιπτώσεις. Η Deep Inspection έρχεται στην συνέχεια ως μια εναλλακτική που συνδυάζει υψηλή ασφάλεια και ευελιξία.

Δύο κριτήρια επιτρέπουν να προσδιοριστεί η επιθεώρηση εφαρμογής ή η επιθεώρηση δικτύου που είναι η πιο κατάλληλη.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ ΒΙΒΛΙΟΘΗΚΗ

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Η πολιτική του Firewall

Είναι η βάση για την εφαρμογή μιας λύσης firewall. Θα πρέπει να καθοριστεί με περισσότερες λεπτομέρειες ποιες υπηρεσίες θα πρέπει να επιθεωρούνται, γιατί και ποια μέτρα θα εφαρμόζονται σε περίπτωση **non-respect**. Σε γενικές γραμμές, όσο πιο ακριβή και περίπλοκη είναι μια πολιτική, τόσο περισσότερο είναι επιβεβλημένη η επιθεώρηση των Εφαρμογών. Και όσο πιο επικίνδυνες είναι οι υπηρεσίες, τόσο περισσότερη είναι η ανάγκη για επιθεώρηση της Εφαρμογής.

Το προφίλ κινδύνου

Το προφίλ κινδύνου που καθορίζεται στο παρελθόν, παρέχει πληροφορίες σχετικά με το πόσο καλά η εταιρεία χρήζει προστασίας. Οι Υψηλού επιπέδου ασφαλείας επιχειρήσεις θα πρέπει να εξετάσουν Φίλτρα επίπεδων εφαρμογής(**Application Level Filters**) ενώ οι χαμηλού επιπέδου ασφαλείας επιχειρήσεις πιθανόν να μην χρειαστούν αρκετή επιθεώρηση Δικτύου.

Μόλις το επίπεδο ελέγχου προσδιορίζεται, η επιλογή για την επιθεώρηση είναι θέμα τεχνικών απαιτήσεων. Γενικά δίνει προτεραιότητα σε μία από τις εξής παραμέτρους: τιμή και ταχύτητα ασφάλειας.

Μια περίληψη όλων των επιθεωρήσεων του firewall:

| NETWORK INSPECTION | | APPLICATION INSPECTION | |
|---|---|---|---|
| **Profile 1**<br>Basic Network Filter<br>- Stateless<br>+ Very Fast<br>- Not Flexible<br>- Low security<br>+ Cheap | **Profile 2**<br>Basic Network Filter<br>+ Stateful<br>+ Fast<br>- Not Flexible<br>Medium security<br>+ Relatively cheap | **Profile 3**<br>Advanced Filter<br>+ Stateful<br>- Slow<br>+ Flexible<br>+ High Security<br>- Expensive | **Profile 4**<br>Application specific Filter<br>+ Stateful<br>- Very Slow<br>- Not Flexible<br>+ Very High Security<br>- Expensive |

Εικόνα 4: Πίνακας κατηγοριοποίησης προφίλ Firewall

### 7.4.4 Step 4:Το Firewall και τα χαρακτηριστικά του

Όταν έρχεται η στιγμή να επιλέξετε ένα προϊόν firewall, πολλά είναι τα εκκρεμή ερωτήματα. Η μέθοδος **FDDM** επικεντρώνεται στις έξι ερωτήσεις. Ένα δέντρο απόφασης γενικά βοηθά στην επιλογή της κατάλληλης λύσης :

#### 7.4.4.1 Τι είδους προιόν επιλέγεται;

Τα προϊόντα κυρίως χωρίζονται σε τέσσερις κατηγορίες:

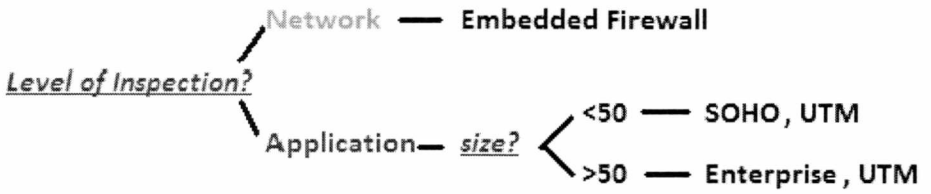
**Embedded Firewalls,** τα οποία είναι συσκευές δικτύου, όπως router ή switches με δυνατότητες firewall

**Soho**(**Small Office Home Office**) Firewalls, σχεδιασμένα να προστατεύουν μικρά δίκτυα

**Enterprise Firewalls,** σχεδιασμένα για μεγάλες επιχειρήσεις με ανάγκες παρακολούθησης και διαχείρισης

**Unified threat Management(UTM)**σχεδιασμένα τόσο για **Soho** και Enterprise profiles, προστατεύουν από την πλειονότητα των απειλών στο διαδίκτυο. Η μέθοδος **FDDM** καθορίζει ποιο από το προϊόν είναι καταλληλότερο με βάση το επίπεδο του ελέγχου(είτε με το δίκτυο, είτε με εφαρμογή based)και το μέγεθος της εταιρείας.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79




Εικόνα 5: Γραφικό επιπεδο επιθεώρησης Firewall

**7.4.4.2 Τι πλατφόρμα Firewall:Hardware ή Software;**

Όλα τα firewalls είναι λογισμικά τα οποία εκτελούνται σε κάποιο είδος hardware, ωστόσο για την πώληση/αγορά μπορεί να αγοράστει ένα λογισμικό ή μια hardware λύση. Ποιές είναι οι διαφορές;

Το Software firewall είναι πρόγραμμα που τρέχει πάνω σε ένα υπάρχον λειτουργικό σύστημα. Μπορεί να εγκατασταθεί σε οποιονδήποτε υπάρχοντα διακομιστή στην εταιρεία αλλά θα πρέπει κατά προτίμηση να έχει την δική του ιδιαίτερη μηχανή. Το πλεονέκτημα αυτής της λύσης είναι ότι είναι συνήθως φθηνότερα στην αγορά και κλιμακωτή(ή επέκτασης) για την κάλυψη των μελλοντικών απαιτήσεων του δικτύου. Το μειονέκτημα είναι ότι είναι πιο επιρρεπείς σε βλάβη υλικού, ευάλωτα σε επιθέσεις OS και είναι δύσκολο να διατηρηθεί δεδομένου ότι χρειάζεται να κρατήσει μέχρι και την ημερομηνία του συστήματος OS καθώς και το λογισμικό του firewall.

Το hardware firewall είναι προγράμματα που εκτελούνται σε αποκλειστικές συσκευές που έχουν σχεδιαστεί ειδικά για τους σκοπούς του firewall. Παρέχουν ένα μεγάλο πλεονέκτημα σε σχέση με τις λύσεις του λογισμικού. Επίσης ονομάζονται **turn-key** λύση, είναι plug and play συσκευές, εύκολες στη χρήση και τη συντήρηση. Επιπλέον, περιέχουν μόνο ό, τι χρειάζονται για να εκτελεστούν, σε σύγκριση με την υπολογιστική λύση που αποτελείται από πολλά άλλα συστατικά που υπόκεινται σε πολλές περισσότερες αποτυχίες. Οι εγγυήσεις κατασκευαστή και η παρακολούθηση των προϊόντων και των σφαλμάτων κάνουν τα Firewalls Hardware τον πιο αξιόπιστο υπολογιστή ακόμα και από τον υπολογιστή που έχετε σπίτι σας. Τα μειονέκτηματα είναι το κόστος και η έλλειψη της αναβάθμισης. Εάν η μελλοντική ανάπτυξη της εταιρείας δεν λαμβάνεται υπόψη, κατά την επιλογή της συσκευής, αυτή κατά πάσα πιθανότητα δεν θα ταιριάζει με τις μελλοντικές ανάγκες.

**7.4.4.3 Δωρεάν ή εμπορικό Software;**

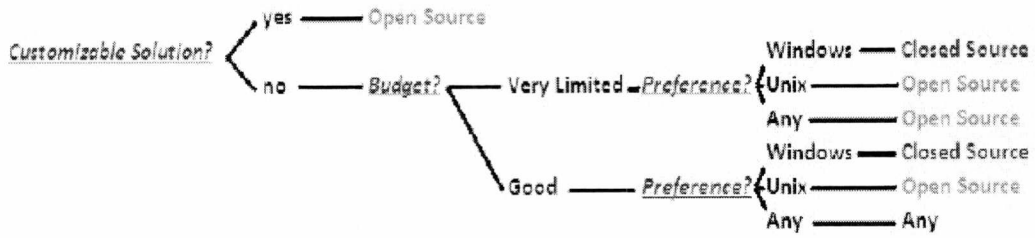
Ενώ η λύση hardware είναι πάντα εμπορική, η Software λύση μπορεί να είναι είτε εμπορική είτε δωρεάν. Κατά την επιλογή αυτών των δύο, το καλύτερο πράγμα που πρέπει να γίνει είναι να εκτιμηθεί συνολικά το κόστος, τα χαρακτηριστικά και η διαθέσιμη υποστήριξη. Η παγίδα συνίσταται στην παραδοχή ότι επειδή μια λύση είναι δωρεάν είναι η πιο αποτελεσματική. Ωστόσο το κόστος υλοποίησης θα μπορούσε να αντιστρέψει την ισορροπία. Δεν υπάρχει ένα γενικό δέντρο αποφάσεων σε αυτή την περίπτωση λόγω της ποικιλίας των προϊόντων. Πράγματι τα δωρεάν firewalls μπορούν να ξεπεράσουν κάποιο από τα αντίστοιχα εμπορικά.

**7.4.4.4 Ανοιχτού ή Κλειστού κώδικα;**

Υπάρχει συχνά μια λανθασμένη αντίληψη ότι Open- source σημαίνει δωρεάν, αλλά δεν είναι αληθής. Open Source μπορεί να είναι η βάση για εμπορικά προϊόντα. Μερικά από τα παραδείγματα είναι **Untangle**, **Vyatta**, **Sourcefire,** οι οποίες είναι όλες εμπορικές Firewalls λύσεις χτισμένες σε OpenSource αρχιτεκτονική (Directorym.net 2008). **Open- source software** σημαίνει ότι ο πηγαίος κώδικας είναι διαθέσιμος σε όποιον τον θέλει. Αντίθετα, κλειστού κώδικα ή **Proprietary** Λογισμικό

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

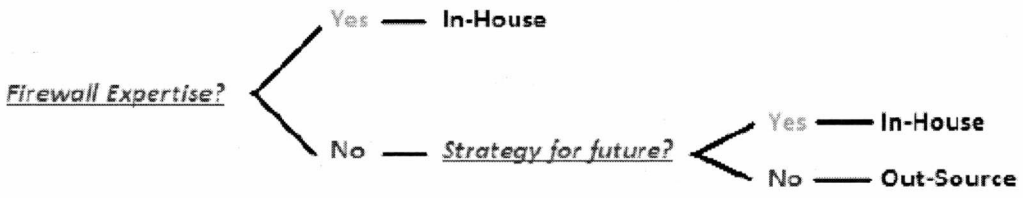
κρατά μυστικό τον κωδικό τους για τον τελικό χρήστη. Μπορεί να είναι δελεαστικό να ζητήσετε την απάντηση από την ερώτηση "ποιος από τους δύο είναι ο πιο ασφαλής". Ωστόσο, αυτό είναι πιθανώς ο λάθος τρόπος για την αντιμετώπιση του προβλήματος. Ο σωστός τρόπος είναι πιθανόν να γνωρίζετε πώς η λύση θα πρέπει να είναι ευέλικτη και πόσο σίγουροι είστε για τις δύο στρατηγικές. Το δέντρο απόφασης όπως εφαρμόζεται σε **FDDM** έχει ως εξής:




Εικόνα 6: Γραφικό δέντρο απόφασης

### 7.4.4.5 Εσωτερική ή Εξωτερική Ρύθμιση και διαχείριση του Firewall;

Τα Firewalls είναι εξίσου ασφαλή όσο μπορείτε να τους πείτε να είναι. Με άλλα λόγια, ένα καλό firewall δεν θα παρέχει καλή ασφάλεια, αν δεν είναι σωστά ρυθμισμένο. Η Διαμόρφωση τείχους προστασίας και η συντήρηση δεν είναι ένας εύκολος στόχος και απαιτεί ικανότητες και εμπειρίες. Η επιλογή να αφήσετε αυτό το καθήκον σε τρίτους θα μπορούσε να είναι μια εναλλακτική λύση για μικρές και μεσαίες επιχειρήσεις, χωρίς in-house εμπειρία. Επιτρέπει να απαλλαγείτε από την διαμόρφωση του firewall την διαχείριση και την συντήρηση. Ωστόσο, αυτό δεν απαλλάσσει την εταιρεία από το να καθορίσει την πολιτική του firewall ή να εφαρμόσει και να ελέγξει ότι το outsourcing συμμορφώνεται με τον όρο της πολιτικής. Αν και δελεαστικό, το out-sourcing γενικά προσφέρει περιορισμένες υπηρεσίες και μπορεί να μην είναι τόσο ευέλικτη λύση, όπως η διαχείριση του ίδιου του τείχους προστασίας. Επιπλέον, η επιλογή αυτή συνεπάγεται να εμπιστεύονται την out-sourcing εταιρεία πράγμα που δεν είναι μια βιώσιμη επιλογή για κανέναν. Για την ανάγκη της αξιολόγηση σχετικά με την εξωτερική ανάθεση ή όχι του τείχους προστασίας, πρέπει να ζητηθεί απάντηση από στα ακόλουθα ερωτήματα: Έχετε firewall τεχνογνωσία για να διασφαλίσετε τη διατήρηση και τη διαχείριση του firewall; Είναι μέρος της στρατηγικής της εταιρείας η εξειδίκευση της ανάπτυξης του τείχους προστασίας;



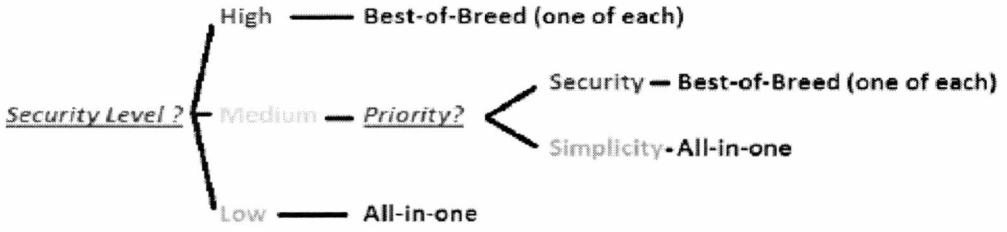

Εικόνα 7: Γραφικό δέντρο Εξειδίκευσης Firewall

### 7.4.4.6 Το Καλύτερο του Είδους ή Όλα σε Ένα;

Από την εμφάνιση της **UTMS**, οι αριθμοί των συζητήσεων μεταξύ **Best of Breed** και **All in one** έχουν αυξηθεί. Η διαμόρφωση **best-of-breed** συνίσταται στην εφαρμογή του καλύτερου από κάθε προϊόν ασφαλείας με την ιδέα για τη δημιουργία διάφορων στρωμάτων προστασίας. Με άλλα λόγια, αυτό σημαίνει ότι η αγορά ενός

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

firewall είναι η πρώτη γραμμή της άμυνας, η αγορά ενός ξεχωριστού anti-virus είναι η δεύτερη, έπειτα έρχεται η αγορά ενός ξεχωριστού anti-spam, ακολουθεί ένα ξεχωριστό σύστημα πρόληψης εισβολής και οποιαδήποτε άλλη συσκευή ασφαλείας απαιτείται, ανάλογα με το επίπεδο ασφάλειας που χρειάζεται η εταιρεία. Από την άλλη πλευρά, η **All-in-one** λύση που το καλύτερο παράδειγμα αυτής είναι το **UTM**, είναι ένα συμπύκνωμα όλων των συσκευών ασφαλείας σε ένα μοναδικό παράθυρο. Το άμεσο πλεονέκτημα είναι η μειωμένη τιμή και η εύκολη διαχείριση της ασφάλειας. Το μειονέκτημα όμως είναι η έλλειψη της άμυνας σε βάθος με ένα μοναδικό σημείο της αποτυχίας.




Εικόνα 8: Γραφικό δέντρο Ασφάλειας Επιπέδου Firewall

## 7.5 Συμπεράσματα

Η εξέλιξη των τεχνολογιών συνοδεύτηκε με πολλαπλασιασμό των απειλών όλο και περισσότερο δύσκολο να διαχειριστούν. Η εξασφάλιση της περιμέτρου παραμένει μία από τις καλύτερες πρακτικές για να κρατήσει μακριά τους εισβολείς. Ωστόσο, όπως οι απειλές έχουν γίνει πιο περίπλοκες, ενώ η περίμετρος έγινε επίσης πιο δύσκολη να σχεδιαστεί και να διατηρηθεί. Τα κύρια θύματα όλων αυτών είναι Μικρές και Μεσαίες Επιχειρήσεις για τις οποίες οι παράγοντες χρόνος και προϋπολογισμός δεν επιτρέπουν να ανταποκριθούν αποτελεσματικά σε αυτά τα θέματα ασφαλείας. Η μεθοδολογία αυτή, αν δεν έχει ήδη δοκιμαστεί, προτίθεται για να βοηθήσει τις ΜΜΕ στην επιλογή πιο αποτελεσματικού τείχους προστασίας δίνοντας τους μια λύση που θα ταιριάζει στις ανάγκες τους. Η **Firewall Design Decision Making (FDDM)** θα πρέπει να εξοικονομήσει χρόνο με το διαχειριστή του συστήματος, δεδομένου ότι έχει προσανατολισμένη λύση και προσέγγιση. Ωστόσο, θα πρέπει επίσης να γίνουν κατανοητά τα όρια της προσέγγισης αυτής. Η FDDM είναι μια βοήθεια για την απόφαση του τείχους προστασίας, αλλά όχι για την υλοποίησή του. Δεν έχει σημασία πόσο καλό είναι το firewall, αν η ρύθμισή του δεν είναι καλή. Επιπλέον, μπορει η εξασφάλιση της περιμέτρου να ειναι μια βέλτιστη πρακτική ,ωστόσο οι περισσότερες πρόσφατες απειλές δείχνουν να προέρχονται απο το εσωτερικό δίκτυο. Είναι σαφές ότι η προστασία της περιμέτρου δεν είναι η μόνη πρόκληση για την ασφάλεια που αντιμετωπίζουν Μικρές και Μεσαίες Επιχειρήσεις, ωστόσο, οποιαδήποτε συνεισφορά μπορεί να σας βοηθήσει να κάνετε την ασφάλεια πιο προσιτή για τις ΜΜ

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

## 8 Κατηγοριοποίηση open source και εμπορικών εργαλείων

Σε αύτη την ενότητα θα παρουσιαστεί ένας πίνακας με τα σχετικά **open source** καθώς και μερικά εμπορικά εργαλεία τα οποία σχετίζονται με τα πλαίσια της εργασίας. Επιπλέον θα αναγράφονται το είδος άδειας(**open source ή μη**) καθώς και το λειτουργικό σύστημα που τα υποστηρίζει.

| Κατηγορίες Λειτουργίας | | Εργαλείο | Είδος Άδειας | Λειτουργικό Συστημα |
|---|---|---|---|---|
| | | | | |
| Network Enumerators | Dns | dnswalk | Open Source | Debian 5<br>Ubuntu 10.04 |
| | | dnstracer | Open Source | Debian 5<br>Ubuntu 10.04 |
| | | dnsutils (dig,nslookup,nsupdate) | Open Source | Debian 5 |
| | | fierce | Open Source | Debian 5<br>Ubuntu 10.04 |
| | | dnsenum | Open Source | Debian 5<br>Ubuntu 10.04 |
| | | nslookup | Open Source | Windows XP |
| | Route | TCPtraceroute | Open Source | Debian 5<br>Ubuntu 10.04 |
| | | TCtrace | Open Source | Debian 5<br>Ubuntu 10.04<br>Windows XP |
| | | Ndisc6 | Open Source | Debian 5<br>Ubuntu 10.04 |
| | Firewall | Firewalk | Open Source | Ubuntu 10.04 |
| | | Ftester | Open Source | Ubuntu 10.04 |
| | | Nmap | Open Source | Debian 5 |
| | | netcat | Open Source | Debian 5<br>Windows XP |
| | Hosts Identification | Nmap | Open Source | Debian 5 |
| | | Hping3 | Open Source | Debian 5 |
| | | arping | Open Source | Debian 5 |
| | | Scapy | Open Source | Debian 5 |
| | | nemesis | Open Source | Debian 5 |
| | | TCPtraceroute | Open Source | Debian 5 |
| | Port Scanner | Nmap | Open Source | Debian 5 |
| | | Zenmap | Open Source | Debian 5<br>Windows |
| | | Scapy | Open Source | Debian 5 |
| | | Nmapsi4 | Open Source | Debian 5 |
| | | doscan | Open Source | Debian 5 |
| | | psad | Open Source | Debian 5 |
| | | pnscan | Open Source | Debian 5 |
| | | cports | Open Source | Windows XP |
| | | Angry IP Scanner | Open Source | Windows XP |
| | | SuperScan | Open Source | Windows XP |

Εικόνα 9: Εργαλεία Αποτίμησης και Διαχείρισης Ασφάλειας

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

| | | | |
|---|---|---|---|
| **Network Management** | LanHelper | Εμπορικό | Windows XP |
| | NetworkView | Εμπορικό | Windows XP |
| | NetCrunch | Εμπορικό | Windows XP |
| | WS_Ping ProPack | Εμπορικό | Windows XP |
| **Active (OS) fingerprint** | Zenmap | Open Source | Debian 5 Windows XP |
| | p0f | Open Source | Debian 5 |
| | Scapy | Open Source | Debian 5 |
| | Cheops-ng | Open Source | Debian 5 |
| | xprobe | Open Source | Debian 5 |
| | SinFP | Open Source | Debian 5 |
| **Passive fingerprint** | pads | Open Source | Debian 5 |
| | ettercap | Open Source | Debian 5 |
| | SinFP | Open Source | Debian 5 |
| | p0f | Open Source | Debian 5 |
| | Archaeoptervx | Open Source | Windows NT |
| **Enterprise Network Mapping Tools** | Rocket NetCure | Εμπορικό | Windows XP |
| | 10-Strike LANState | Εμπορικό | Windows XP |
| | Zabbix | Open Source | OpenSuse |
| | Dia | Open Source | Windows XP |
| **Web & Application Server Fingerprint** | Nikto | Open Source | Debian 5 |
| | Wikto | Open Source | Windows XP |
| | AppPrint | Free For Non-Commercial Use/ Εμπορικό | Windows XP |
| | Httprint | Open Source | Windows XP |
| **Network Vulnerability Scanners** | Nessus | Free For Non-Commercial Use/ Εμπορικό | Windows XP Debian 5 |
| | NeXpose | Εμπορικό | Ubuntu 10.04 |
| | GFI LANguard | Εμπορικό | Windows XP |
| | Open Vulnerability Assessment System (OpenVAS) | Open Source | Debian 5 |
| | Microsoft Baseline Security Analyzer (MBSA) | Open Source | Windows XP |
| **Vulnerability Management** | NeXpose | Εμπορικό | Ubuntu 10.04 |
| | GFI LANguard | Εμπορικό | Windows XP |
| **Exploitation Engines** | Metasploit Framework | Open Source | Windows XP Debian 5 |

Εικόνα 10: Εργαλεία Αποτίμησης και Διαχείρισης Ασφάλειας

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# Ανάπτυξη συστήματος Κυβερνοασφάλειας για MME βασισμένο σε προγράμματα-εφαρμογές ανοικτού λογισμικού

## 1. Εισαγωγή στο Security Onion

Το Security Onion είναι ένα λογισμικό ανοιχτού κώδικα, τόσο για εταιρικά όσο και για ιδιωτικά δίκτυα. Ειδικότερα το Security Onion αποτελεί μια διανομή Linux προσανατολισμένη στο intrusion detection, στην επισκόπηση της ασφάλειας δικτύων, καθώς και στη διαχείριση αρχείων καταγραφής. Βασίζεται στο 64bit Ubuntu Server 12.04 LTS και περιλαμβάνει μια σειρά από εφαρμογές IDS (Snort, Suricata, Bro κ.ά.), καθώς και συστήματα οργάνωσης και παρακολούθησης "alerts" κι αρχείων καταγραφής (Squil, Snorby, ELSA κ.ά.). Η ρύθμισή του, μετά τη βασική εγκατάσταση του λειτουργικού, γίνεται από το περιβάλλον γραφικών και με τη βοήθεια ενός φιλικού script.

Η αλήθεια είναι πως το Security Onion δεν προορίζεται για μικρά, οικιακά δίκτυα. Αντίθετα, τα πιθανά σενάρια χρήσης εμπλέκουν ένα ή και περισσότερα μεγάλα δίκτυα, σε στρατηγικά σημεία των οποίων βρίσκονται ανεπτυγμένοι οι λεγόμενοι sensors. Ένας sensor μπορεί να 'ναι μια άλλη εγκατάσταση του Security Onion ή κάποιο μεμονωμένο IDS, όπως είναι το Snort. Σε κάθε περίπτωση, τα sensors αναφέρουν πληροφορίες σε έναν Security Onion server — και είναι γνωστό ότι οι clients (sensors) και οι server επιτρέπεται να βρίσκονται όλοι στο ίδιο host.

Αναλυτικότερα, θα δειχθεί παρακάτω πώς εγκαθίσταται και πώς ρυθμίζεται σωστά το Security Onion. Για όποιον ενδιαφέρετε για την ασφάλεια δικτύων καθώς και για τη διαχείριση δικτυακών assets, τότε σίγουρα αξίζει να ασχοληθεί με το Security Onion.

Network Security Monitoring

Το Security Onion αποτελεί είναι ένα λογισμικό σχετιζόμενο με την παρακολούθηση του δικτύου που αφορά την ασφάλεια. Πέρα από την Παρακολούθηση της Ασφάλειας των Δικτύων , κοινώς ονομαζόμενο και ως Network Security Monitoring(NSM), θα μπορούσε και προληπτικά να χρησιμοποιηθεί για την εντόπιση τρωτών σημείων, ή λήξη των πιστοποιητικών SSL, καθώς και στην αντιμετώπιση περιστατικών ασφαλείας.

Το NSM δίνει τη δυνατότητα είτε για παρακολούθηση ενός αντίπαλου, είτε για να κρατήσει ένα κακόβουλο λογισμικό μακριά, καθώς το NSM παρέχει το πλαίσιο, τη νοημοσύνη και την επίγνωση της κατάστασης του δικτύου. Υπάρχουν ορισμένες εμπορικές λύσεις κοντά σε αυτό που παρέχει το Security Onion, αλλά πολύ λίγοι περιέχουν τις τεράστιες δυνατότητες του Security Onion σε ένα πακέτο.

Πολλοί πιστεύουν ότι τα NSM είναι μια λύση που μπορεί να αγοράσει κάποιος για να καλύψει ένα κενό. Τα δεδομένα μπορούν να συλλέγονται και να αναλύονται, αλλά δεν φαίνονται όλες οι κακόβουλες δραστηριότητες με την πρώτη ματιά ότι είναι κακόβουλες. Ενώ η αυτοματοποίηση και η συσχέτιση μπορεί να ενισχύσει την νοημοσύνη και να βοηθήσει στη διαδικασία της διαλογής μέσα από ψευδώς θετικούς και κακόβουλους δείκτες. Το Security Onion δεν είναι ενα λογισμικό που μπορείτε να ρυθμίσετε και να νιώθετε ασφαλείς. Το Security Onion θα παρέχει ορατότητα στην κυκλοφορία του δικτύου και το πλαίσιο γύρω από τις ειδοποιήσεις και τις περίεργες κινήσεις, αλλά απαιτεί μια δέσμευση από τον διαχειριστή ή τον αναλυτή να

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

επανεξετάσει τις ειδοποιήσεις, να παρακολουθεί τη δραστηριότητα του δικτύου, και το σημαντικότερο, να έχει τη θέληση, το πάθος και την επιθυμία να μάθει.

## Βασικά Στοιχεία

Το Security Onion συνδέει άψογα μαζί τρεις βασικές λειτουργίες:

Full packet capture (πλήρης σύλληψη πακέτων)

συστήματα ανίχνευσης εισβολής υποδοχής με βάση το δίκτυο που βασίζεται και (NIDS και HIDS, αντίστοιχα)

και ισχυρά εργαλεία ανάλυσης.

Το *Full packet capture* επιτυγχάνεται μέσω netsniff-ng (http://netsniff-ng.org/). Το netsniff-ng συλλαμβάνει όλη την κυκλοφορία με τους αισθητήρες από το Security Onion. Το *Full packet capture* είναι σαν μια βιντεοκάμερα για το δίκτυό, αλλά καλύτερα, διότι όχι μόνο μπορεί να πει ποιος ήρθε και πήγε, αλλά και ακριβώς πού πήγε και τι έφερε ή πήρε μαζί του.

*Network-based and host-based intrusion detection systems* (IDS) (συστήματα ανίχνευσης εισβολής με βάση το δίκτυο που βασίζεται και (IDS)) αναλύει τα συστήματα κίνησης του δικτύου ή υποδοχής, αντίστοιχα, και παρέχει καταγραφή και δεδομένα συναγερμού για να ανιχνεύονται εκδηλώσεις και δραστηριότητες.

Το Security Onion παρέχει πολλαπλές επιλογές IDS:

### NIDS:

**Rule-driven NIDS**. Για κανόνα με γνώμονα την ανίχνευση εισβολής δίκτυο, το Security Onion προσφέρει την επιλογή του **Snort** (http://snort.org/) ή **Suricata** (http://suricata-ids.org/). Αυτά είναι συστήματα κανόνων που βασίζονται στην προβολή της κυκλοφορίας του δικτύου για τα δακτυλικά αποτυπώματα και τα αναγνωριστικά που ταιριάζουν με γνωστά κακόβουλα λογισμικά και ασυνήθιστη ύποπτη κίνηση. Θα μπορούσε να ειπωθεί ότι είναι παρόμοια με υπογραφές ιών για το δίκτυο, αλλά είναι λίγο βαθύτερα και πιο ευέλικτα από ό, τι αυτό.

**Analysis driven NIDS**. Το Security Onion προσφέρει το **Bro Network Security Monitor**, επίσης γνωστό ως **Bro IDS**. Το Bro αναπτύσσεται και συντηρείται από το Διεθνές Ινστιτούτο Επιστήμης Υπολογιστών στο Πανεπιστήμιο της Καλιφόρνια στο Μπέρκλεϋ και υποστηρίζεται με χρηματοδότηση από το Εθνικό Ίδρυμα Επιστημών. Σε αντίθεση με τα rule-based συστήματα τα οποία βασίζονται σε κανόνες που αναζητούν δυσεύρετα δεδομένα, το Bro είναι σαν να σας λέει "Εδώ είναι τα δεδομένα σας και αυτό είναι ότι έχω δει. Κάνετε ότι θέλετε με αυτά και εδώ είναι ένα πλαίσιο ώστε να το πραγματοποιήσετε". Το Bro παρακολουθεί την δραστηριότητα του δικτύου και καταγράφει τις όποιες συνδέσεις, τις αιτήσεις DNS, τις ανιχνεύσιμες υπηρεσίες δικτύου και λογισμικού, τα πιστοποιητικά SSL, HTTP, FTP, IRC, SMTP, SSH, SSL και την δραστηριότητα Syslog που βλέπει. Έτσι παρέχει ένα πραγματικό βάθος για την ορατότητα μέσα στο πλαίσιο των δεδομένων και των γεγονότων στο δίκτυό. Επιπρόσθετα, το Bro περιλαμβάνει αναλυτές για αρκετά πρωτόκολλα και εξ ορισμού έχει την ικανότητα να ελέγχει τα ποσά MD5 για λήψεις αρχείων HTTP ενάντια στο έργο της Team Cymru's Malware Hash Registry. Πέρα απο τη δυνατότητα της καταγραφής της δραστηριότητας και των αναλυτών της κυκλοφορίας, το Bro περιλαμβάνει ένα πλαίσιο το οποίο παρέχει έναν πολύ επεκτάσιμο τρόπο για να αναλυθούν τα δεδομένα του δικτύου σε πραγματικό χρόνο. Η πρόσφατη συνεργασία με REN-ISAC's Collective Intelligence Framework(CIF) παρέχει σε πραγματικό χρόνο την συσχέτιση της δραστηριότητας του δικτύου με την up-to-date κοινότητα των υπηρεσιών για να ειδοποιεί όταν οι χρήστες έχουν πρόσβαση σε

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

γνωστές κακόβουλες διευθύνσεις IP και τομείς ή διευθύνσεις URL. Το πλαίσιο εισροών επιτρέπει να τροφοδοτείτε το Bro με δεδομένα τα οποία μπορούν να προγραμματιστούν. Το πλαίσιο ανάλυσης των αρχείων, παρέχει το πρωτόκολλο ανάλυσης ανεξάρτητων αρχείων, που επιτρέπει να καταγράψετε τα αρχεία καθώς διέρχονται μέσα από το δίκτυό και αυτόματα να τα περάσει σε ένα sandbox ή σε ένα κοινόχρηστο αρχείο για την σάρωση προστασίας από ιούς. Με την ευελιξία του Bro έχετε έναν απίστευτα ισχυρό σύμμαχο στην διάθεσή σας.

HIDS:

Για την **host -based** ανίχνευση εισβολής το Security Onion προσφέρει την OSSEC μία ελεύθερη open Source HIDS για Windows, Linux και Mac OS X. Όταν προστεθεί ο πράκτορας OSSEC στις απολήξεις του δικτύου, δίνει την πολύτιμη δυνατότητα για ορατότητα από την απόληξη του δικτύου μέχρι το σημείο εξόδου από αυτό. Το OSSEC εκτελεί ανάλυση καταγραφής, έλεγχο ακεραιότητας του αρχείου, παρακολούθηση της πολιτικής, ανίχνευση rootkit, ειδοποίηση σε πραγματικό χρόνο και ενεργή ανταπόκριση. Αρχικά δημιουργήθηκε από τον Daniel Cid και αποκτήθηκε από την Trend-Micro το 2009. Έκτοτε το OSSEC συνεχώς προσφέρεται σαν μια open Source λύση. Η συσχέτιση των host-based events με network-based events μπορεί να είναι η διαφορά στον εντοπισμό μιας επιτυχημένης επίθεσης.

## Εργαλεία Ανάλυσης

Με την πλήρη καταγραφή των πακέτων, τις IDS καταγραφές και τα δεδομένα από το Bro, διαθέτετε ένα τρομακτικό ποσό διαθέσιμων στοιχείων προς ανάλυση. Ευτυχώς το Security Onion ενσωματώνει τα ακόλουθα εργαλεία για να βοηθήσει στην επεξεργασία αυτών των δεδομένων:

**Sguil**: δημιουργημένο από τον Bamm Visscher. Είναι το δεξί χέρι του αναλυτή, παρέχοντας ορατότητα στα δεδομένα των events που συλλέγονται και για το πλαίσιο στο οποίο γίνεται η επικύρωση της ανίχνευσης. Το Sguil παρέχει μια ενιαία GUI (γραμμένη σε TCL/TK) στην οποία μπορείτε να προβάλετε Snort ή Suricata ειδοποιήσεις, ειδοποιήσεις OSSEC, Bro HTTP events, και ειδοποιήσεις τύπου PRADS(Passive Real Time Asset Detection System). Το πιο σημαντικό είναι ότι το Sguil επιτρέπει να στραφείτε κατευθείαν από μια ειδοποίηση σε μια σύλληψη πακέτου(μέσω Wireshark ή NetworkMiner) ή ένα αντίγραφο της συνεδρίας που προκάλεσε την ειδοποίηση. Έτσι αντί να βλέπει μόνο ένα πακέτο που σχετίζεται με μια ειδοποίηση και να υπάρχουν αναπάντητα ερωτήματα τι κάνουμε τώρα και τι συνέβη στην συνέχεια μπορείτε να δείτε ολόκληρη την συσχετιζόμενη κυκλοφορία και να δώσετε απαντήσεις σε αυτά τα ερωτήματα. Επιπλέον το Sguil επιτρέπει στον αναλυτή να διερευνήσει όλα τα πακέτα που καταγράφηκαν, όχι μόνο τα συσχετιζόμενα με την ειδοποίηση, ώστε να μπορείτε να αποφανθείτε για την κίνηση που δεν προκάλεσε την ειδοποίηση, αλλά μπορεί να είναι συνδεδεμένη με κακόβουλο ή ανεπιθύμητο λογισμικό. Τέλος το Sguil επιτρέπει στον αναλυτή να διεξάγει αντίστροφη DNS και Whois αναζητήσεις διευθύνσεων IP που σχετίζονται με ειδοποιήσεις.

Η διαφορά του Sguil από τα άλλα interfaces ειδοποιήσεων είναι ότι επιτρέπει την συνεργασία μεταξύ των αναλυτών επιτρέποντας τις ειδοποιήσεις να σχολιάζονται και να κλιμακώνονται σε περισσότερους αναλυτές οι οποίοι μπορούν να λάβουν δράση για αυτές. Το Sguil είναι το κύριο εργαλείο του Security Onion για να παρέχει το πιο δεδομένο πλαίσιο σχετικά με μια ειδοποίηση.

**Squert:** δημιουργήθηκε από τον Paul Halliday, είναι μια εφαρμογή του διαδικτύου για την βάση δεδομένων του Sguil. Αν και δεν προορίζεται να είναι ένα interface σε πραγματικό χρόνο(ή σχεδόν πραγματικό χρόνο) ούτε μια αντικατάσταση του Sguil,

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

επιτρέπει την διερεύνηση της βάσης δεδομένων του Sguil και παρέχει πολλές επιλογές απεικόνισης για δεδομένα όπως "παραστάσεις χρονοσειρών οι οποίες σταθμίζονται λογικά και ομαδοποιούνται σύμφωνα με τους κανόνες" και χαρτογράφηση geo-IP.

**Snorby**[3]: δημιουργημένο από τον Dustin Webber, είναι μια διαδικτυακή εφαρμογή για την προβολή, την αναζήτηση και την ταξινόμηση ειδοποιήσεων Snort και Suricata και την δημιουργία διάφορων αναφορών όπως οι πιο ενεργές IDS signatures, οι πιο ενεργοί αισθητήρες και οι κορυφαίες πηγές και προορισμοί των IP διευθύνσεων. Με την βοήθεια του capeME! plugin δίνεται η δυνατότητα στον αναλυτή να στραφεί σε ένα αντίγραφο της συνεδρίασης που περιέχει το πακέτο που προκάλεσε την ειδοποίηση, αρκεί μόνο να είναι σε θέση να δει μόνο το πακέτο που τον προκάλεσε(παρόμοια με την προβολή του αντιγράφου του Sguil).

**Enterprise Log Search and Archive(ELSA)**: δημιουργήθηκε από τον Martin Holste είναι συγκεντρωτικό πλαίσιο syslog χτισμένο σε Syslog-NG, MySQL και Sphinx. Παρέχει μια πλήρως ασύγχρονη web-based interface που ομαλοποιεί τα αρχεία καταγραφής και κάνει την αναζήτηση αυτών πάρα πολύ εύκολη και γρήγορη. Επίσης περιλαμβάνει εργαλεία για εκχώρηση δικαιωμάτων, για προβολή των αρχείων καταγραφής καθώς και emails ειδοποιήσεων, προγραμματισμένες ερωτήσεις και γραφικές παραστάσεις. Με απλά ελληνικά το ELSA είναι ένα εργαλείο αναζήτησης που επιτρέπει χωρίς ιδιαίτερο κόπο να επεξεργαστείτε όλα τα δεδομένα που συλλέγονται από το Security Onion καθώς και τις πρόσθετες syslog πηγές που προωθεί, δίνοντάς έτσι την ορατότητα σε σχετικά syslog δεδομένα να μπορείτε να τα στείλετε στο ELSA. Επιπλέον το ELSA προσφέρει γραφήματα και γραφικές παραστάσεις μέσω του Google Visualization API. Είναι δύσκολο να κατανοηθεί το έργο του ELSA χωρίς να δειχθεί στην πράξη.

## Deployment Scenarios

Το Security Onion είναι βασισμένο σε ένα κατανεμημένο μοντέλο client-server. Ένας αισθητήρας(sensor) του Security Onion είναι ο πελάτης(client) και ο server είναι ο ίδιος. Τα στοιχεία του server και του αισθητήρα μπορούν να λειτουργήσουν σε μια φυσική μηχανή ή σε μια εικονική. Οι πολλαπλοί αισθητήρες μπορούν να διανεμηθούν σε όλη την υποδομή και να ρυθμιστούν ώστε να υποβάλουν έκθεση στον καθορισμένο server. Ένας αναλυτής μπορεί να συνδέεται με τον server από έναν σταθμό εργασίας client για να εκτελεί ερωτήματα και να ανακτά δεδομένα.

Τα τρία ακόλουθα είναι τα σενάρια ανάπτυξης του Security Onion:

**Standalone:** Μια εγκατάσταση standalone αποτελείται από ένα μοναδικό φυσικό ή εικονικό μηχάνημα που εκτελεί ο server, ο αισθητήρας, και όλες οι σχετικές διαδικασίες. Μπορεί να έχει πολλαπλά interfaces για την παρακολούθηση διαφορετικών τμημάτων του δικτύου. Είναι ο ευκολότερος και ο πιο βολικός τρόπος για την παρακολούθηση του δικτύου ή των δικτύων που είναι προσβάσιμα από ένα μόνο σημείο.

**Server-sensor:** Μια εγκατάσταση του αισθητήρα του server αποτελείται από ένα μόνο μηχάνημα που εκτελεί τα στοιχεία του server με μια ή περισσότερες μηχανές που υποβάλουν εκθέσεις πίσω στον server. Οι αισθητήρες είναι που εκτελούν όλες

---

[3] Σχόλιο: Το Snorby έχει αφαιρεθεί από το νέο Security Onion 14.04 και η παράγραφος βρίσκεται μόνο για εγκυκλοπαιδικούς λόγους.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

τις διαδικασίες sniffing και αποθηκεύουν το σχετικό πακέτο με τις καταγραφές, με τις ειδοποιήσεις IDS, με τις βάσεις δεδομένων για το Sguil, το Snorby και το ELSA. Ο αναλυτής συνδέεται με τον server από ένα ξεχωριστό μηχάνημα του client και όλες οι ερωτήσεις αποστέλλονται στον server και διανέμονται στους κατάλληλους αισθητήρες μαζί με τις πληροφορίες που ζητούνται, και στο τέλος κατευθύνονται πίσω στον client. Αυτό το μοντέλο μειώνει την κυκλοφορία του δικτύου, διατηρώντας τον όγκο των δεδομένων που συλλέγονται στους αισθητήρες μέχρι να ζητηθούν από τον client του αναλυτή. Όλη η κυκλοφορία μεταξύ του server, των αισθητήρων και του client προστατεύονται με SSH κρυπτογράφηση.

**Hybrid:** Αποτελείται από standalone-εγκατάσταση και έχει επίσης ένα ή περισσότερους ξεχωριστούς αισθητήρες που δίνουν αναφορά στον server της μηχανής που έχει την standalone(αυτόνομη) εγκατάσταση.

Το σενάριο εγκατάστασης του Security Onion επιτρέπει εύκολα να ρυθμιστεί η βέλτιστη εγκατάσταση η οποία ταιριάζει με τις ανάγκες της επιχείρησης.

## Συνοπτικά

Υπάρχει πλήρη καταγραφή πακέτων, Snort ή Suricata, rule-driven αναγνώριση εισβολής, Bro-event-driven αναγνώριση εισβολής και OSSEC host-based αναγνώριση εισβολής. Αυτά τα ανόμοια συστήματα με διάφορες εξαρτήσεις και πολυπλοκότητες εκτελούνται ομαλά όλα μαζί, αλλιώς θα ήταν πολύ χρονοβόρο και θα απαιτούσε ώρες, μέρες ακόμα και βδομάδες για την συγκέντρωση και την ενσωμάτωσή τους. Αυτό που κάποτε ήταν φαινομενικά ακατόρθωτο έργο τώρα είναι τόσο απλό όσο και μια εγκατάσταση των Windows.

## 1.2 Tools[4]

**argus:** πρόκειται για ένα εργαλείο για τον λογιστικό έλεγχο των συναλλαγών του δικτύου, το οποίο κατηγοριοποιεί τα πακέτα του δικτύου που ταιριάζουν με το Libpcap φίλτρο σε ένα συγκεκριμένο πρωτόκολλο συναλλαγών του διαδικτύου. Το argus παρουσιάζει τις συναλλαγές που ανακαλύπτει, όπως τα περιοδικά δεδομένα του δικτύου, τα οποία είναι κατάλληλα τόσο για ιστορικό όσο και για επεξεργασία Forensics σε πραγματικό χρόνο. Αν επιθυμείτε να γνωρίζετε τι συμβαίνει στο διαδίκτυό σας, τώρα ή γενικά, το argus είναι το κατάλληλο εργαλείο.

**barnyard2:** είναι ένας open Source διερμηνέας για τα δυαδικά αρχεία εξόδου τύπου Snort unified2. Η κύρια χρήση του είναι να επιτρέπει στο Snort να γράψει στον δίσκο με τρόπο αποτελεσματικό, αφήνοντας έτσι το έργο της ανάλυσης των διαδίκων δεδομένων σε διάφορες μορφές, ώστε το Snort να μην χάσει την κίνηση του δικτύου.

**Bro:** είναι ένα ισχυρό framework ανάλυσης δικτύου που διαφέρει αρκετά από τα συνηθισμένα IDS που γνωρίζετε. Το εργαλείο αυτό εστιάζει στην παρακολούθηση της ασφάλειας του δικτύου και ταυτόχρονα παρέχει μία ολοκληρωμένη πλατφόρμα για γενικότερη ανάλυση της κίνησης στο δίκτυο.

**chaosreader:** είναι ένα εργαλείο το οποίο μεταφέρει τα δεδομένα της εφαρμογής από Snoop ή tcpdump logs. Υποστηριζόμενα πρωτόκολλα περιλαμβάνουν TCP, UDP, IPv4, IPv6, ICMP, telnet, FTP, HTTP, SMTP, IRC, X11 και VNC.

---

[4] Πηγή: https://github.com/Security-Onion-Security Onionlutions/security-onion/wiki/Tools

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

**Daemonlogger:** είναι ένα καταγραφικό πακέτο και Soft tap που αναπτύχθηκε από τον Martin Roesch

**driftnet**: είναι ένα πρόγραμμα το οποίο παρακολουθεί το δίκτυο κυκλοφορίας και ξεχωρίζει εικόνες από TCP streams τις οποίες παρατηρεί.

**dsniff**: είναι μια συλλογή από εργαλεία για τον έλεγχο του δικτύου και των δοκιμών στις εισβολές. Τα εργαλεία dsniff, filesnarf, mailsnarf, msgsnarf, urlsnaf και WebSpy παρακολουθούν το δίκτυο για ενδιαφέροντα στοιχεία όπως κωδικούς πρόσβασης, emails και αρχεία. Τα εργαλεία arpsproof, dnsspoof, macof διευκολύνουν την διακοπή της κίνησης του δικτύου που δεν είναι διαθέσιμη σε έναν εισβολέα.

**ELSA**: είναι ένα κεντρικό πλαίσιο syslog δομημένο με Syslog-NG, MySQL και Sphinx full-text search. Παρέχει μία πλήρως ασύγχρονη web-based interface η οποία ομαλοποιεί τα αρχεία καταγραφής (logs) και καθιστά την αναζήτησή τους τόσο εύκολη όσο την αναζήτηση στο διαδίκτυο. Περιλαμβάνει επίσης εργαλεία για την εκχώρηση αδειών για την προβολή των αρχείων καταγραφής και ειδοποιήσεις μέσω email, προγραμματισμένων ερωτήσεων και γραφικές αναπαραστάσεις.

**hping**: είναι μία εντολή προσανατολισμένη στα πακέτα TCP/IP συναρμολόγησης και ανάλυσης. Ο ρόλος της είναι να στέλνει αιτήσεις ICMP αλλά και να υποστηρίζει πρωτόκολλα TCP, UDP, ICMP και RAW-IP. Υποστηρίζει επίσης λειτουργία tracerout και έχει την δυνατότητα να στείλει αρχεία μεταξύ καναλιών και πολλά άλλα χαρακτηριστικά.

**hunt**: είναι ένα εξελιγμένο πακέτο sniffer και connection intrusion. Εισβάλλετε σε μία σύνδεση, την παρατηρείτε και την επαναφέρετε. Το hunt λειτουργεί καλύτερα με Ethernet και χρησιμοποιείται για συνδέσεις που το χρησιμοποιούν.

**labrea:** αναλαμβάνει αχρησιμοποίητες διευθύνσεις IP και δημιουργεί εικονικούς servers που είναι στόχοι για worms, hackers και άλλες απειλές στο διαδίκτυο. Το πρόγραμμα απαντά σε προσπάθειες σύνδεσης με τέτοιο τρόπο ώστε ο υπολογιστής στο άλλο άκρο να συνδεθεί μαζί του για μεγάλο χρονικό διάστημα.

**mergecap**: είναι ένα πρόγραμμα που συνδυάζει πολλαπλά αποθηκευμένα αρχεία καταγραφής σε ένα ενιαίο αρχείο εξόδου το οποίο καθορίζεται από το -w argument. Το mergecap ξέρει πως να διαβάσει αρχεία καταγραφής, συμπεριλαμβανομένων και εκείνων των tcpdump, Wireshark και άλλα αρχεία που καταγράφουν αρχεία πακέτων σε αυτήν την μορφή.

**netsed:** είναι μία μικρή αλλά χρήσιμη εφαρμογή σχεδιασμένη για να μεταβάλλει το περιεχόμενο των πακέτων που μεταβιβάζονται μέσω του δικτύου σε πραγματικό χρόνο. Είναι πραγματικά χρήσιμο για τους hackers του διαδικτύου στις ακόλουθες εφαρμογές: έλεγχος του πρωτοκόλλου black-box, πειράματα Fuzz-alike, δοκιμές ακεραιότητας(όταν θέλετε να ελέγξετε την σταθερότητα της εφαρμογής και να δείτε πώς θα εξασφαλίζεται η ακεραιότητα των δεδομένων σας), άλλες κοινές εφαρμογές όπως εξαπάτηση χρηστών και φιλτράρισμα περιεχομένου. Ταιριάζει απόλυτα με ngrep, netcat και tcpdump .

**netsniff-ng:** είναι ένα εργαλείο δικτύωσης Linux. Η αύξηση της απόδοσης επιτυγχάνεται με μηχανισμούς zero-copy, έτσι ώστε η υποδοχή των πακέτων και η μετάδοση του kernel να μην απαιτεί να αντιγράψετε πακέτα από τον χώρο του kernel και αντίστροφα. Μπορεί επίσης να χρησιμοποιηθεί για την ανάπτυξη του δικτύου, την ανάλυση και τον εντοπισμό σφαλμάτων καθώς και έλεγχο ή αναγνώριση του δικτύου. Η εργαλειοθήκη του netsniff-ng αποτελείται από τα ακόλουθα βοηθητικά προγράμματα:

- **netsniff-ng**, ένας γρήγορος αναλυτής zero-copy, εργαλείο λήψης pcap και αναπαραγωγής

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

- **trafgen**, μία χαμηλού επιπέδου γεννήτρια πακέτων τύπου zero-copy
- **mausezahn**, γεννήτρια πακέτων υψηλού επιπέδου για συσκευές HW/SW
- **bpfc**, ένα compiler Berkeley Packet Filter, Linux BPF, KOE
- **ifpps**, **flowtop**, ένα εργαλείο δικτύωσης στατιστικών του πυρήνα
- **curvetun**, ένα ελαφρύ curve25519 βασισμένο σε IP tunnel
- **astraceroute**, ένα αυτόνομο σύστημα βοηθητικό traceroute.

**NetworkMiner:** είναι εργαλείο Network Forensic Analysis Tool(NFAT) για τα Windows. Μπορεί να χρησιμοποιηθεί ως εργαλείο σύλληψης sniffer/packet προκειμένου να εντοπίσει λειτουργικά συστήματα, sessions, hostnames, open ports χωρίς να κάνετε καμία κίνηση στο δίκτυο. Μπορείτε επίσης να αναλύσετε τα αρχεία PCAP για ανάλυση offline και να επανασυναρμολογήσετε μεταδιδόμενα, αρχεία και πιστοποιητικά από τα αρχεία PCAP.

**ngrep**: προσπαθεί να παρέχει το μεγαλύτερο μέρος των κοινών χαρακτηριστικών του GNU grep σε επίπεδο δικτύου. Είναι ένα εργαλείο pcap-aware που θα σας επιτρέψει να καθορίσετε τις κανονικές μορφές δεκαεξαδικών εκφράσεων ώστε να ταιριάξουν με τα πακέτα των payloads. Αναγνωρίζει IPv4/6, TCP, UDP, ICMPv4/6, IGMP και Ethernet, PPP, SLIP, FDDI, Token Ring, και μηδενικές διεπαφές και αναγνωρίζει BPF filter logic με τον ίδιο τρόπο όπως τα περισσότερα πακέτα εργαλείων sniffing όπως tcpdump και Snoop.

**OSSEC**: είναι Open Source Host-based Intrusion Detection System. Εκτελεί ανάλυση της καταγραφής, έλεγχο της ακεραιότητας του αρχείου, παρακολούθηση της πολιτικής, ανίχνευση rootkit, ειδοποίηση σε πραγματικό χρόνο και ενεργή ανταπόκριση.

**p0f**: είναι ένα εργαλείο που χρησιμοποιεί μία σειρά εξελιγμένων μηχανισμών λήψης αποτυπωμάτων κυκλοφορίας ώστε να εντοπίσει τους υπεύθυνους πίσω από οποιονδήποτε τυχαία επικοινωνία TCP/IP, χωρίς να παρεμβαίνει με οποιοδήποτε τρόπο. Συνήθεις χρήσεις του p0f περιλαμβάνουν αναγνώριση των δοκιμών εισβολής, συστηματική παρακολούθηση του δικτύου, ανίχνευση απαγορευμένων διασυνδέσεων του δικτύου σε εταιρικά περιβάλλοντα και διάφορα στοιχεία εγκληματολογίας.

**Reassembler**: Αν παρέχετε στον reassembler.py με pcap που περιέχει θραύσματα πακέτων, θα συγκεντρώσει εκ νέου τα πακέτα, χρησιμοποιώντας κάθε μία από τις πέντε μηχανές επανασυρναμολόγησης, και θα σας δείξει το αποτέλεσμα.

**scapy**: είναι ένα ισχυρό διαδραστικό πρόγραμμα επεξεργασίας πακέτων. Είναι ικανό να δημιουργήσει ή να αποκωδικοποιήσει πακέτα ενός μεγάλου αριθμού πρωτοκόλλων. Χειρίζεται εύκολα τα πιο κλασσικά καθήκοντα όπως σάρωση, tracerouting, probing, έλεγχος μονάδων, επιθέσεις ή ανακάλυψη δικτύων (μπορεί να αντικαταστήσει το hping, το 85% του nmap, arpspoof, arp-sk, arping, tcdump, tethereal, p0f). Εκτελεί πολύ αποτελεσματικά ειδικότερα καθήκοντα τα οποία άλλα εργαλεία δεν μπορούν. Αυτά είναι η αποστολή invalid frames, εισαγωγή δικών σας 802.11 frames, συνδυάζοντας τεχνικές (VLAN hopping+ARP cache poisoning)

**sguil**: το κύριο συστατικό του είναι μια διαισθητική GUI που παρέχει πρόσβαση σε γεγονότα σε πραγματικό χρόνο, session data και καταγραφές πακέτων. Το εργαλείο διευκολύνει την πρακτική της παρακολούθησης της Ασφάλειας του Δικτύου. Ο Sguil client είναι σε TCL/TK και μπορεί να τρέξει σε οποιοδήποτε λειτουργικό σύστημα που υποστηρίζει TCL/TK.

**sniffit:** είναι ένα κατανεμημένο Sniffer σύστημα το οποίο επιτρέπει στους χρήστες να καταγράφουν την κυκλοφορία του δικτύου μέσω ενός ειδικού μηχανήματος χρησιμοποιώντας μια γραφική εφαρμογή. Αυτό το χαρακτηριστικό είναι πολύ χρήσιμο

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

σε δίκτυα με switches διότι οι παραδοσιακοί sniffers επέτρεπαν μόνο στους χρήστες να καταγράφουν την κίνηση στο δικό τους δίκτυο.

**Snorby**: είναι μία εφαρμογή που επιτρέπει την παρακολούθηση της ασφάλειας των δικτύων που συνδέονται με δημοφιλή συστήματα ανίχνευσης εισβολής όπως Snort, Suricata, Sagan. Οι βασικές θεμελιώδεις έννοιες πίσω από το Snorby είναι η απλότητα, η οργάνωση και η δύναμη. Ο στόχος της εφαρμογής είναι η δημιουργία ενός δωρεάν open source κώδικα ιδιαίτερα ανταγωνιστικό για την παρακολούθηση του δικτύου τόσο σε ιδιωτική όσο και σε και επιχειρηματική χρήση.

**Snort**: είναι ένα σύστημα πρόληψης και ανίχνευσης της εισβολής στο δίκτυο(IDS/IPS). Το Snort είναι η περισσότερο διαδεδομένη τεχνολογία IDS/IPS σε όλο τον κόσμο.

**Squert**: χρησιμοποιείται για την αναζήτηση και προβολή των δεδομένων που αποθηκεύονται στην βάση δεδομένων Sguil(συνήθως δεδομένα ειδοποιήσεων IDS). Είναι ένα οπτικό εργαλείο που επιχειρεί να παρέχει πρόσθετο πλαίσιο για τα γεγονότα μέσω της επεξεργασίας των metadata, παραστάσεις χρονοσειρών και λογικά ομαδοποιημένων αποτελεσμάτων.

**ssldump**: είναι ένας SSLv3/TLS αναλυτής πρωτοκόλλων του δικτύου. Προσδιορίζει τις συνδέσεις TCP και επιχειρεί να τις ερμηνεύσει ως SSLv3/TLS . Όταν εντοπίζει την SSLv3/TLS κίνηση αποκωδικοποιεί τα αρχεία και τα εμφανίζει σε μορφή κειμένου στο stdout. Εάν παρέχεται με το κατάλληλο υλικό μπορεί επίσης να αποκρυπτογραφήσει τις συνδέσεις και να εμφανίσει την κίνηση των δεδομένων της εφαρμογής.

**sslsniff**: έχει σχεδιαστεί για να δημιουργήσει man-in the-middle (MITM) επιθέσεις για συνδέσεις SSL/TLS. Το sslsniff υποστηρίζει και άλλες επιθέσεις όπως null-prefix ή OCSP ώστε να κατορθώσει διακοπές στην σύνδεση.

**Suricata**: είναι μία μηχανή ανίχνευσης και πρόληψης της εισβολής. Δεν προορίζεται στο να αντικαταστήσει ή να μιμηθεί τα υπάρχοντα εργαλεία, αλλά να φέρει νέες ιδέες και τεχνολογίες στον τομέα αυτό.

**tcpdump**: εκτυπώνει μια περιγραφή του περιεχομένου των πακέτων σε ένα interface του δικτύου ώστε να ταιριάζουν με το boolean expression. Επίσης τρέχει με την -w flag που αποσκοπεί στην αποθήκευση των πακέτων σε δεδομένα για την μετέπειτα ανάλυση και με την r-flag η οποία προτιμά να διαβάσει το αποθηκευμένο αρχείο του πακέτου παρά το πακέτο στο διαδίκτυο. Σε όλες τις περιπτώσεις μόνο τα πακέτα που ταιριάζουν με την expression θα υποβληθούν σε επεξεργασία tcpdump.

**tcpick**: είναι textmode sniffer libpcap που μπορεί να εντοπίσει, επανασυρναμολογήσει και αναδιατάξει τα tcp streams. Το tcpick είναι σε θέση να αποθηκεύσει τα ληφθέντα πακέτα σε διαφορετικά αρχεία ή να τα εμφανίζει στο τερματικό και γι αυτό είναι χρήσιμο να διεξάγουμε sniff σε αρχεία τα οποία μεταδίδονται μέσω FTP ή HTTP. Μπορεί να εμφανίσει όλα τα stream στο τερματικό ακόμα και όταν η σύνδεση είναι κλειστή, με διάφορους τρόπους εμφάνισης όπως hexdump, hexdump+ascii, εκτυπώσιμους χαρακτήρες και ούτω καθεξής. Έχει ρύθμιση για χρωματική επιλογή ώστε να κατανοηθεί καλύτερα η έξοδος του προγράμματος. Μπορεί να διαχειριστεί πολλές συνδέσεις συμπεριλαμβανομένων καρτών ethernet και PPP. Είναι χρήσιμο για να παρακολουθείτε τι κάνουν οι χρήστες του δικτύου και μπορεί να χρησιμοποιηθεί με τα εργαλεία textmode όπως grep, sed, awk.

**tcpreplay**: είναι suite GPLv3 το οποίο δίνει την δυνατότητα να χρησιμοποιήσετε προηγούμενες ληφθείσες κινήσεις του δικτύου σε μορφή libpcap για να δοκιμάσετε μια ποικιλία συσκευών του δικτύου. Σας επιτρέπει να ταξινομήσετε την κυκλοφορία ως client ή server, να ξαναγράψετε Layer 2, 3, 4 και τελικά να επαναλάβετε την κίνηση πίσω στο δίκτυο και μέσω άλλων συσκευών, όπως switches, routers,

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

firewalls, NIDS, IPS's. Το tcpreplay υποστηρίζει μονούς και διπλούς τρόπους για έλεγχο και sniffing συσκευών inline.

**tcpslice**: είναι εργαλείο για την εξαγωγή τμημάτων των αρχείων trace των πακέτων που δημιουργούνται χρησιμοποιώντας tcpdump -w flag. Μπορεί να συνδυάσει πολλαπλά αρχεία trace και να εξάγει κομμάτια από ένα ή περισσότερα τμήματα βασισμένα στον χρόνο.

**tcpstat**: εκθέτει συγκεκριμένες στατιστικές διασύνδεσης ορισμένων δικτύων όπως το tcpstat κάνει για τα στατιστικά στοιχεία του συστήματος. Το tcpstat παίρνει τις πληροφορίες είτε από την παρακολούθηση ενός ειδικού interface είτε από την ανάγνωση προηγουμένων αποθηκευμένων δεδομένων σε tcpdump από ένα αρχείο.

**tcpxtract**: είναι εργαλείο για την εξαγωγή αρχείων από την κυκλοφορία του δικτύου και βασίζεται στις υπογραφές των αρχείων.

**tshark**: είναι ένας αναλυτής πρωτοκόλλων του δικτύου. Σας επιτρέπει να καταγράψετε πακέτα δεδομένων από διαδίκτυο σε πραγματικό χρόνο, ή να διαβάσετε πακέτα από ένα προηγουμένως αποθηκευμένο αρχείο καταγραφής, ή να εκτυπώσετε μια αποκωδικοποιημένη μορφή αυτών των πακέτων στην έξοδο, ή καταγράφοντας τα πακέτα σε αρχεία. Η μορφή του αρχείου Tshark είναι libpcap και είναι η μορφή που χρησιμοποιείται από tcpdump και άλλα εργαλεία.

**u2boat**: Κομμάτι του Snort το u2boat μετατρέπει τα unified2 αρχεία σε pcaps.

**u2spewfoo**: Κομμάτι του Snort, μετατρέπει τα unified2 αρχεία σε κείμενο.

**Wireshark**: είναι ένας αναλυτής πρωτοκόλλων δικτύου GUI. Σας επιτρέπει να περιηγηθείτε διαδραστικά στα δεδομένα των πακέτων από το δίκτυο σε πραγματικό χρόνο ή από ένα υπάρχον αρχείο καταγραφής μορφή που καταγράφει τα πακέτα είναι libpcap η οποία χρησιμοποιείται από tcpdump και άλλα εργαλεία.

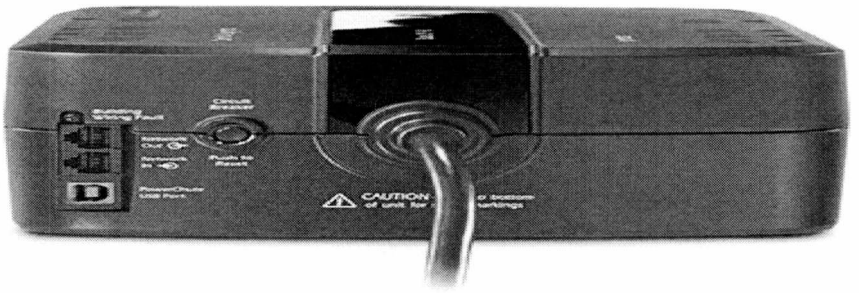
**Xplico**: ο στόχος του είναι να εξάγει από μια κίνηση στο διαδίκτυο τα δεδομένα που περιέχονται σε εφαρμογές. Για παράδειγμα από ένα αρχείο pcap Xplico εξάγει σε κάθε email (πρωτόκολλα POP, IMAP, SMTP), όλα τα περιεχόμενα HTTP, κάθε κλήση VoIP(SIP), FTP, TFTP. Το Xplico δεν είναι ένας αναλυτής πρωτοκόλλων δικτύου αλλά ένα open Source Network Forensic Analysis Tool.

## 1.3 Απαιτήσεις Υλικού

**32-bit vs 64-bit:** 'Ολα τα πακέτα μας είναι διαθέσιμα σε δυο εκδόσεις 32-bit και 64-bit, αλλά τα 64-bit συνίστανται ιδαίτερα λόγω της αυξημένης απόδοσης τους.

**UPS**: 'Όπως και τα περισσότερα συστήματα πληροφορικής έτσι και το Security Onion έχει βάσεις δεδομένων που είναι ευαίσθητες σε διακοπές ρεύματος και μη ασφαλείς τερματισμούς λειτουργίας. Για αυτούς τους λόγους είναι σημαντική η ύπαρξη του UPS.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79



**Master Server**: Σε μια επιχείρηση που διανέμεται ανάπτυξη, ένας master server θα πρέπει να αφήσει το sniffing και την καταγραφή δεδομένων σε ξεχωριστά κουτιά αισθητήρων. Σε αυτό το σενάριο, ένας master server δεν απαιτεί τόσο πολύ υλικό όσο ένας αισθητήρας. Ο master server θα πρέπει να διαθέτει 1-4CPU πυρήνες, 8-16GB RAM, 100GB-1TB ελεύθερο χώρο στον δίσκο. Πολλοί χρήστες επιλέγουν να εγκαταστήσουν τον master server στην VM farm λόγω των χαμηλών απαιτήσεων από τους αισθητήρες αλλά χρειάζεται περισσότερη αξιοπιστία και διαθεσιμότητα.

**Sensors**: Οι ακόλουθες απαιτήσεις ισχύουν μόνο για αισθητήρες.

**CPU** Snort, Suricata, Bro έχουν αρκετές απαιτήσεις. Όσο περισσότερη κίνηση παρακολουθείτε όσο περισσότερους πυρήνες θα χρειαστείτε. Μια πρόχειρη εκτίμηση είναι 200Mbps ανά Snort instance, Suricata/Bro worker. 'Ετσι αν έχετε σύνδεση με 1Gbps και εκτελούνται Snort και Bro θα χρειαστείτε τουλάχιστον 5 Snort instances και 5 Bro Workers πράγμα που σημαίνει ότι θα χρειαστείτε τουλάχιστον 10 πυρήνες CPU για Snort και Bro με επιπρόσθετους CPU πυρήνες για netsniff-ng και άλλες υπηρεσίες.

**RAM** η μνήμη RAM εξαρτάται από πολλές μεταβλητές όπως:

- τις υπηρεσίες που ενεργοποιείτε

- τα είδη των κινήσεων που παρακολουθείτε

- το πραγματικό ποσό της κίνησης που παρακολουθείτε(πχ αν παρακολουθείτε 1Gbps link αλλά χρησιμοποιεί μόνο 200Mbps)

- το ποσό των απωλειών των πακέτων που είναι αποδεκτό από την εταιρεία σας.

Οι ακόλουθες εκτιμήσεις της RAM είναι πρόχειρες και υποθέτουμε ότι θα εκτελείτε Snort/Suricata ,Bro και netsniff-ng (πλήρης καταγραφή πακέτων) και θέλετε να ελαχιστοποιήσετε την απώλεια των πακέτων.

Αν θέλετε απλώς να αξιολογήσετε το Security Onion σε ένα VM, τότε το ελάχιστο ποσό μνήμης RAM που απαιτείται είναι 3GB. Περισσότερο είναι προφανώς καλύτερα!

Αν επιθυμείτε την ανάπτυξη ενός μικρού δικτύου (50Mbps ή λιγότερα) θα πρέπει να προγραμματίσετε για 8GB RAM ή περισσότερη.

Αν επιθυμείτε την ανάπτυξη ενός μεσαίου δικτύου (50Mbps-500Mbps) θα πρέπει να προγραμματίσετε για 16GB-128GB μνήμης RAM ή περισσότερο.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Αν επιθυμείτε την ανάπτυξη ενός μεγάλου δικτύου(500Mbps-1000Mbps)θα πρέπει να προγραμματίσετε για 128-256GB μνήμης RAM.

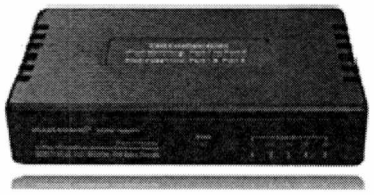
Αν αγοράσετε έναν νέο server πρέπει να επιλέξετε το μέγιστο GB σε μνήμη RAM.

**Storage**: Οι αισθητήρες που ελέγχουν την πλήρη καταγραφή των πακέτων (και/ή ELSA) χρειάζονται μεγάλο χώρο αποθήκευσης. Παραδείγματος χάρην, αν παρακολουθείτε μια σύνδεση 50Mb εδώ είναι μερικοί γρήγοροι υπολογισμοί: 50Mb / s = 6,25 MB / s = 375 MB / λεπτό = 22.500 MB / ώρα = 540.000 MB / ημέρα.' Αρα θα χρειαστούμε 540GB για την ημερήσια αξία της pcaps (πολλαπλασιάστε αυτό με τον αριθμό των ημερών που θέλετε να κρατήσετε στο δίσκο). Σημειώστε ότι αυτό είναι μόνο pcaps (άλλες καταγραφές θα καταλαμβάνουν επιπλέον χώρο αποθήκευσης) έτσι θα θέλετε να στρογγυλοποιήσετε προς τα πάνω τον αριθμό terabyte ώστε να εξασφαλίσετε επαρκή χώρο για αποθήκευση. Όσο περισσότερο χώρο έχετε στον δίσκο, τοσο περισσότερο χρόνο θα έχετε για την έρευνα των καταγραφών.

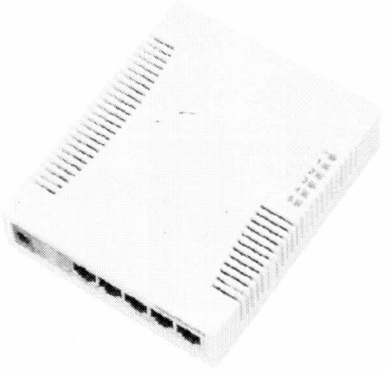
**NIC:** Θα χρειαστείτε τουλάχιστον δύο interfaces: μία για την διαχείριση(κατά προτίμηση συνδέεται με ένα ειδικό δίκτυο διαχείρισης) και στη συνέχεια ένα η περισσότερα για sniffing. Βεβαιωθείτε ότι έχετε μια καλή κάρτα δικτύου.

**Packets**:Θα πρέπει με κάποιο τρόπο να πάρετε τα πακέτα από τους αισθητήρες σας. Για μια εγκατάσταση παραγωγής θα χρειαστείτε μια tap ή SPAN/monitor θύρα. Εδώ παρατίθενται μερικές λύσεις:

-Sheer Simplicity and Portability (USB-powered):



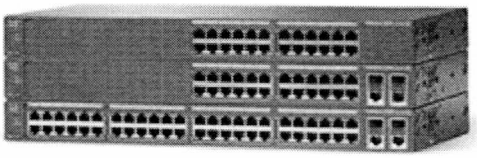
-Dirt Cheap and Versatile:



Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

-Netgear GS105E (requires Windows app for config):


-More exhaustive list of enterprise switches with port mirroring:



Tap Solutions:

Net Optics/Ixia

Arista Tap Aggregation Feature Set

Gigamon

cPacket

Bigswitch Monitoring Fabric

## 1.4 Download/Install

Για να εγκαταστήσετε το Security Onion, θα εγκαταστήσετε είτε το ISO του Security Onion ή ένα Ubuntu 14.04 ISO και στην συνέχεια θα προσθέσετε το Security Onion PPA και τα πακέτα. Λάβετε υπόψη ότι το PPA και τα πακέτα είναι συμβατά μόνο με Ubuntu 14.04.

Σημαντικό: Πάντα να επαληθεύετε την υπογραφή οποιουδήποτε κατεβασμένου ISO αρχείου. Ανεξάρτητα από τον αν κατεβάζετε το ISO αρχείο του Security Onion ή το ξεκινάτε με Ubuntu 14.04 ISO, θα πρέπει πάντα να επαληθεύετε την ISO εικόνα.

→ Αν κατεβάσετε το Security Onion 14.04.3.1 ISO image, παρακαλείστε να το επικυρώσετε χρησιμοποιώντας τις παρακάτω οδηγίες

ισχύων ISO image:

https://github.com/Security-Onion-Solutions/security-onion/releases/download/v14.04.3.1/securityonion-14.04.3.1.iso

Signature για το ισχύων ISO image:

https://github.com/Security-Onion-Solutions/security-onion/raw/master/securityonion-14.04.3.1.iso.sig

Signing Key:

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

https://raw.githubusercontent.com/Security-Onion-Solutions/security-onion/master/KEYS

Για παράδειγμα, μπορείτε να ακολουθήσετε τα επόμενα βήματα στα περισσότερα συστήματα Linux για να κατεβάσετε και να επικυρώσετε το Security Onion ISO image.

Κατεβάστε το signing key:

```
wget https://raw.githubusercontent.com/Security-Onion-Solutions/security-onion/master/KEYS
```

Εισάγετε το signing key:

```
gpg --import KEYS
```

Κατεβάστε το αρχείο signature για το ISO:

```
wget https://github.com/Security-Onion-Solutions/security-onion/raw/master/securityonion-14.04.3.1.iso.sig
```

Κατεβάστε στο ISO image:

```
wget https://github.com/Security-Onion-Solutions/security-onion/releases/download/v14.04.3.1/securityonion-14.04.3.1.iso
```

Επικυρώστε το ISO image χρησιμοποιώντας το signature file:

```
gpg --verify securityonion-14.04.3.1.iso.sig securityonion-14.04.3.1.iso
```

## 1.5 Booting Issues

Γιατί το ISO image δεν λειτουργεί στον υπολογιστή μου;

Υποστηρίζει ο υπολογιστής σας 64-bit; (Εάν προσπαθείτε να εκτελέσετε μια 64-bit VM, τότε ο επεξεργαστής σας θα πρέπει να υποστηρίζει virtualization και θα πρέπει να είναι ενεργοποιημένη στα BIOS) Αν όχι, τότε θα πρέπει να αποκτήσετε ένα μηχάνημα 64-bit ώστε να χρησιμοποιήσετε το 64-bit ISO image ή να χρησιμοποιήστε το 32-bit μηχάνημά σας με την εγκατάσταση του Ubuntu 14.04 και να προσθέσετε το PPA και τα πακέτα όπως περιγράφεται στην σελίδα Installation.

Αν νομίζετε ότι το μηχάνημά σας δεν υποστηρίζει 64-bit αλλά εξακολουθείτε να έχετε προβλήματα με το 64-bit ISO image, δοκιμάστε να εγκαταστήσετε το Ubuntu 14.04. 64-bit ISO image και να δείτε αν λειτουργεί. Αν δεν γίνεται αυτό τότε θα πρέπει να εξακριβώσετε την 64-bit συμβατότητά σας.

Αν το ISO image λειτουργήσει αλλά το Live Desktop δεν εμφανίζεται κανονικά, τότε ίσως υπάρχει θέμα με την κάρτα γραφικών σας. Δοκιμάστε την επιλογή nomodeset

Συμβουλευτείτε και τα παρακάτω links:

http://blog.securityonion.net/2014/02/security-onion-12044-iso-image-now.html
https://groups.google.com/d/topic/security-onion/UKE5-dqybQ4/discussion
https://groups.google.com/d/topic/security-onion/51JZWXZfBho/discussion

Αν αυτό λειτουργεί αλλά έχετε ως αποτέλεσμα χαμηλή ανάλυση και έχετε nvidia graphics chipset, τότε μπορείτε να κάνετε τα ακόλουθα μετά την εγκατάσταση:

```
sudo apt-get remove nvidia-173
sudo apt-get remove nvidia-96
sudo apt-get install nvidia-current
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

After Installation:

Βεβαιωθείτε ότι οι υπηρεσίες εκτελούνται: `sudo service nsm status`

Αν δεν εκτελούνται, προσπαθήστε να τις εκκινήσετε : `sudo service nsm start`

Tuning/Miscellaneous:

Αν παρακολουθείτε IP διευθύνσεις εκτός των ιδιωτικών RFC1918 διευθύνσεων(192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12) θα πρέπει να ενημερώσετε τον αισθητήρα σας με τις σωστές IP. Τα αρχεία ρυθμίσεων του αισθητήρα μπορούν να βρεθούν στο /etc/nsm/$HOSTNAME-$INTERFACE/. Τροποποιήστε είτε το Snort.conf ή Suricata.yaml(ανάλογα με ποια μηχανή IDS επιλέξατε κατά την διάρκεια του sosetup) και ενημερώστε την μεταβλητή HOME_NET. Επίσης ενημερώστε την μεταβλητή home_nets στο prads.conf. Τέλος ενημερώστε την διαμόρφωση του δικτύου Bro στην /opt/bro/etc/networks.cfg. Επανεκκινήστε την διαδικασία του αισθητήρα:

```
sudo nsm_sensor_ps-restart
```

Αν διαθέτετε πρόσβαση στο διαδίκτυο, δημιουργήστε μια ειδοποίηση IDS πληκτρολογώντας τα ακόλουθα σε ένα τερματικό:

```
curl http://testmyids.com
```

Οι αναλυτές πλήρους απασχόλησης θα πρέπει να εγκαταστήσουν το Security Onion σε VM στον σταθμό εργασίας τους(εκτελείται μέσω του Ubuntu installer, αλλά δεν εκτελείται με οδηγό εγκατάστασης). Αυτό σας δίνει ένα τοπικό αντίγραφο του Wireshark, NetworkMiner, και του Sguil client. Ξεκινήστε τον Sguil client και συνδεθείτε στο IP/hostname του αισθητήρα του Sguil. Αυτό σας επιτρέπει να διερευνήσετε pcaps χωρίς τον φόβο ότι θα επηρεαστούν ο server ή οι ασθητήρες σας. Για να αλλάξετε την ασφάλεια του Security Onion VM, εγκαταστήστε τα εικονικά εργαλεία για την virtualization ή χρησημοποιήστε xrandr. Για μία λίστα με τις διαθέσιμες αναλύσεις οθόνης απλά εκτελέστε το xrandr. Για να ρυθμίσετε την ανάλυση της οθόνης(αντικαταστήστε το W με το H με τα πραγματικά πλάτη και ύψη που επιθυμείτε.)

```
xrandr -s WxH
```

Συνδεθείτε με το Sguil και επιθεωρήστε της IDS ειδοποιήσεις. Μπορείτε να έχετε πρόσβαση σε Squert, ELSA από την https://server/ για επιπλέον ρυθμίσεις στην ανάλυση.

Ενισχύστε τον server και τους αισθητήρες σας με την απενεργοποίηση περιττών υπηρεσιών και βγάλτε το firewall από αχρησιμοποίητες θύρες.

Εκτελέστε τα παρακάτω για να δείτε πως ο αισθητήρας σας αντιμετωπίζει το φορτίο.Θα πρέπει να το ελέγχετε σε καθημερινή βάση για να βεβαιωθείτε ότι ο αισθητήρας σας δεν χάνει πακέτα. Σκεφτείτε την προσθήκη σε cronjob και να σας το αποστείλουν μεσω mail.(δείτε τον σύνδεσμο "configure email" παρακάτω.)

```
sudo sostat | less
```

Παρακαλώ σημείωστε ότι το κάθε σύστημα IDS/NSM πρέπει να είναι συντονισμένο στο δίκτυο το οποίο παρακολουθεί. Παρακαλείστε να δείτε Managing Alerts. Θα πρέπει να εκτελέστε μόνο τις signatures που σας ενδιαφέρουν.

Επίσης σημειώστε ότι θα πρέπει να εξετάζετε και να κατηγοριοποιείτε events καθημερινά. Ακόμα κι αν δεν χρησιμοποιείτε την κονσόλα Sguil για την κύρια

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

ανάλυσή σας, θα πρέπει να συνδέεστε περιοδικά και να πατήσετε F8 που δείχνει τα παλιά events για να κρατήσετε σε πραγματικό χρόνο την ουρά. Αν το παραμελήσετε, τότε ο αριθμός των μη-κατηγοριοποιημένων events θα αυξηθεί και θα συνεχίζει κάθε μέρα να αυξάνεται.

Στον server που εκτελείται το Sguil ρυθμίσετε την μεταβλητή DAYSTOKEEP σε /etc/nsm/securityonion.conf σε πόσες ημέρες επιθυμείτε να το κρατήσετε στο αρχείο σας.Η προεπιλογή είναι 365 αλλά θα πρέπει να το προσαρμόσετε στις ανάγκες και στην πολιτική της εταιρίας σας καθώς και στο μέγεθος του ελεύθερου χώρου στον δίσκο.

Θα πρέπει επίσης να ρυθμίσετε την http-agent. Αν χρησιμοποιείτε ELSA έχετε ήδη όλα τα αρχεία καταγραφής HTTP Bro διαθέσιμα εκεί, οπότε ίσως να θελήσετε να απενεργοποιήσετε τον http_agent ώστε να αποφευχθεί η επανάληψη αυτών των αρχείων καταγραφής στην βάση δεδομένων του Sguil:

```
# Terminate the running http_agent
sudo nsm_sensor_ps-stop --only-http-agent
# Disable http_agent
sudo sed -i 's|HTTP_AGENT_ENABLED="yes"|HTTP_AGENT_ENABLED="no"|g'
/etc/nsm/*/sensor.conf
```

Απενεργοποιήστε οποιεσδήποτε μη-απαραίτητες διαδικασίες του αισθητήρα.

Ρυθμίστε τον αριθμό των PF_RING instances για Snort/Suricata/Bro.

Προαιρετικό αποκλείστε την περιττή κυκλοφορία από την παρακολούθησή σας χρησιμοποιώντας BPF.

Προαιρετικό: προσθήκη νέων λογαριασμών χρηστών Sguil με τα ακόλουθα:

```
sudo nsm_server_user-add
```

Προαιρετικό αλλά συνίσταται ιδιαίτερα: ρυθμίστε το Email για ειδοποιήσεις και αναφορές

Προαιρετικό αλλά συνίσταται ιδιαίτερα :τοποθετήστε /etc υπό τον έλεγχο έκδοσης. Αν η εταιρεία σας δεν έχει έναν έλεγχο έκδοσης μπορείτε να χρησιμοποιήσετε: bazaar, git, etckeeper:

```
sudo apt-get install etckeeper
```

Προαιρετικό: χρειάζεται το remote desktop να αποκτά πρόσβαση στον server ή στον αισθητήρα; Σας συνίσταται SSH X-Forwarding όπως φαίνεται παραπάνω αλλά μπορείτε να εγκαταστήσετε και FreeNX ή xrdp:

```
sudo apt-get install xrdp
```

Σημειώστε ότι δεν ενθαρρύνουμε την χρήση FreeNX ή xrdp.

Δείτε περισσότερα για τα εργαλεία του Security Onion στην ενότητα Tools

## 1.6 After Installation

Βεβαιωθείτε ότι οι υπηρεσίες εκτελούνται: `sudo service nsm status`

Αν ορισμένες υπηρεσίες δεν εκτελούνται, προσπαθήστε να τις εκκινήσετε: `sudo service nsm start`

Tuning/Miscellaneous:

Αν παρακολουθείτε την κίνηση του δικτύου που έχει VLAN tags, ελέγξτε την σελίδα VLAN(https://github.com/Security-Onion-Solutions/security-onion/wiki/VLAN-Traffic)

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Αν παρακολουθείτε διευθύνσεις IP που κυμαίνονται εκτός του ιδιωτικού RFC1918 (192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12) θα πρέπει να ενημερώσετε τις ρυθμίσεις του αισθητήρα σας με το σωστό εύρος των διευθύνσεων IP. Αυτές οι ρυθμίσεις βρίσκονται σε /etc/nsm/$HOSTNAME-$INTERFACE/. Τροποποιήστε `snort.conf` ή `suricata.yaml` (ανάλογα με ποια IDS μηχανή επιλέξατε κατά την διάρκεια του sosetup) και ενημερώστε την τιμή HOME_NET. Επίσης ενημερώστε την μεταβλητή home_nets στην prads.conf. Έπειτα ενημερώστε την ρύθμιση δικτύου του Bro σε opt/bro/etc/networks.cfg και επανεκκινήστε την διαδικασία των αισθητήρων: sudo nsm_sensor_ps-restart.

Αν έχετε πρόσβαση σε διαδίκτυο, δημιουργήστε ειδοποίηση IDS πληκτρολογώντας ακόλουθα σε ένα τερματικό: curl http://testmyids.com

Στην εγκατάσταση του Security Onion (20120912-0ubuntu0securityonion201) έχει μόνο την προεπιλογή στο άνοιγμα της θύρας 22 στον firewall. Αν χρειαστεί να συνδέσετε OSSEC agents, syslog συσκευές ή αναλυτές VM, μπορείτε να εκτελέσετε την νεα Security Onion-allow δραστηριότητα που σας καθοδηγεί στην δημιουργία κανόνων για το firewall ώστε να επιτρέψει σε αυτές τις συσκευές να συνδεθούν.

Οι αναλυτές πλήρους απασχόλησης θα πρέπει να εγκαταστήσουν το Security Onion σε ένα VM(Virtual Machine) στον σταθμό εργασίας τους(εκτελείται μέσω Ubuntu, μην εκτελέσετε τον οδηγό εγκατάστασης). Αυτό σας δίνει ένα τοπικό αντίγραφο του Wireshark, NetworkMiner, και του προσαρμοσμένου Sguil client. Ξεκινήστε τον Sguil client και συνδεθείτε στο IP/hostname του αισθητήρα παραγωγής Sguil (ίσως χρειαστεί να εκτελέσετε το Security Onion-allow όπως περιγράψαμε και πριν).Αυτό σας επιτρέπει να διερευνήσετε τα pcaps χωρίς τον φόβο ότι επηρεάζουν τον server/αισθητήρα παραγωγής .Για να αλλάξετε την ανάλυση του Security Onion, εγκαταστήστε τα Virtual Tools για την virtualization λύση ή χρησιμοποιήσετε το xrandr.

Συνδεθείτε στο Sguil για να προβάλλετε τις IDS ειδοποιήσεις. Τα Squert και ELSA μπορούν να εκτελεστούν από το https://server/ για περεταίρω ανάλυση σε βάθος.

Εκτελέστε το ακόλουθο για να δείτε πως ο αισθητήρας σας αντιμετωπίζει το φορτίο. Θα πρέπει να το ελέγχετε σε καθημερινή βάση για να βεβαιωθείτε ότι ο αισθητήρας σας δεν χάνει πακέτα. Προσθέστε το σε μια cronjob το οποίο θα σας αποσταλεί μέσω email.

sudo sostat | less.

Παρακαλώ σημειώστε ότι κάθε σύστημα IDS/NSM πρέπει να είναι συντονισμένο για το δίκτυο το οποίο παρακολουθεί .Δείτε την ενότητα Managing Alerts. Θα πρέπει να εκτελείτε μόνο τις signatures που σας ενδιαφέρουν.

Επίσης σημειώστε ότι θα πρέπει να ψάχνετε και να κατηγοριοποιείτε γεγονότα κάθε μέρα με στόχο να κατηγοριοποιήσετε όλα τα γεγονότα ανά ημέρα. Ακόμα κι αν δεν επιθυμείτε να χρησιμοποιήσετε την κονσόλα Sguil για την κύρια ανάλυσή σας, θα πρέπει να συνδέεστε με αυτήν περιοδικά και F8 τα παλιά γεγονότα ώστε να αποτρέπετε την ουρά γεγονότων να μεγαλώνει σε πραγματικό χρόνο. Η παραμέληση αυτού θα οδηγήσει σε θέματα στην βάση δεδομένων του Sguil καθώς ο αριθμός των μη-προσδιορισμένων γεγονότων συνεχίζει να αυξάνει σε καθημερινή βάση. Δείτε http://nsmwiki.org/Sguil_Client.

Στον server που εκτελείται η βάση δεδομένων Sguil, ρυθμίστε την μεταβλητή DAYSTOKEEP σε /etc/nsm/securityonion.conf για όσες ημέρες θέλετε να διατηρήσετε στο αρχείο σας. Η προεπιλογή είναι 365 αλλά μπορεί να χρειαστεί να το ρυθμίσετε με βάση την πολιτική της εταιρείας σας και τον διαθέσιμο χώρο στον δίσκο σας.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Θα πρέπει επίσης να ρυθμίσετε το hhtp_agent.Αν εκτελείτε ELSA, ήδη έχετε όλα τα αρχεία καταγραφής Bro HTTP εκεί, οπότε ίσως θέλετε να απενεργοποιήσετε τον http_agent για να αποφευχθεί η επανάληψη των καταγραφών στην βάση δεδομένων του Sguil.

```
# Terminate the running http_agent

sudo nsm_sensor_ps-stop --only-http-agent

# Disable http_agent

sudo sed -i 's|HTTP_AGENT_ENABLED="yes"|HTTP_AGENT_ENABLED="no"|g'
/etc/nsm//sensor.co
```

Απενεργοποιήστε οποιεσδήποτε διαδικασίες αισθητήρων δεν χρειάζεστε.

Ρυθμίστε τον αριθμό των συμβάντων PF_RING για το Snort/Suricata/Bro.

Προαιρετικό: εξαιρέστε οποιαδήποτε κίνηση από την παρακολούθηση σας χρησιμοποιώντας το BPF.

Προαιρετικό: προσθέστε νέους λογαριασμούς χρηστών Sguil με το ακόλουθο: sudo nsm_server_user-add

Προαιρετικό, αλλά συνίσταται ιδιαίτερα: ρυθμίστε το Email για αναφορές και ειδοποιήσεις.

Προαιρετικό αλλά συνίσταται ιδιαίτερα: τοποθετήστε /etc κάτω από την version control. Αν η οργάνωσή σας δε έχει version control tool, μπορείτε να χρησιμοποιήσετε bazaar, git, etckeeper: sudo apt-get install etckeeper.

## 1.7 UTC and Time Zones

Όταν εκτελείται η εγκατάσταση του Security Onion, θέτει την χρονοζώνη σε UTC/GMT επειδή είναι συνιστώμενη/προτεινόμενη για την ρύθμιση του Sguil:

http://osdir.com/ml/security.sguil.general/2008-09/msg00003.html

Προσπαθώντας χρησιμοποιήσετε μια μη-UTC ζώνη ώρα μπορεί οδηγηθείτε στα επόμενα:

Οι ζώνες θερινής ώρας που έχουν μια με δυο ώρες διαφοράς κάθε χρόνο. Αυτό καθιστά το Sguil μη-ικανό να καταγράψει τα γεγονότα εντός της χρονικής περιόδου μιας ώρας. Για να αποφευχθεί αυτό, συνίσταται η χρήση του UTC δεδομένου ότι δεν υπάρχει θερινή ώρα.

Κάτι παρόμοιο μπορεί να συμβεί σε καθημερινή βάση υπό ορισμένες προϋποθέσεις. Αν υπάρξει ασυμφωνία μεταξύ της OS ζώνης ώρας και τις ρυθμίσεις UTC του Sguil, το Sguil θα είναι μη ικανό να καταγράψει δεδομένα για τα γεγονότα σε ένα "παράθυρο" της ώρας γύρω στα μεσάνυχτα το οποίο συμπίπτει με την ζώνη ώρας από το UTC.

Επιπλέον, η UTC είναι αρκετά βολική όταν έχετε αισθητήρες σε διαφορετικές ζώνες ώρας και προσπαθούν να συσχετίσουν γεγονότα με άλλα συστήματα ή ομάδες. Οι τρεις κύριες διαδικτυακές interfaces(Snorby, Squirt, ELSA) σας επιτρέπουν να καταστήσετε χρονικές σημάνσεις στην εκδήλωση της τοπικής ζώνης της ώρας σας. Η ELSA από προεπιλογή θα καταστήσει τις χρονικές σημάνσεις στην ζώνη ώρας του τοπικού προγράμματος της περιήγησής σας και το Squirt και Snorby θα σας επιτρέψουν να αλλάξετε την ζώνη της ώρας σας.

1. Πως αλλάζει η ώρα στα Ubuntu?

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Όταν εκτελείτε τον οδηγό εγκατάστασης, αυτομάτως θα θέσει την ζώνη ώρας σας σε UTC. Αν ήδη έχετε εκτελέσει την εγκατάσταση και έχετε αλλάξει χειροκίνητα την ζώνη ώρας σας σε μη-UTC και επιθυμείτε να θέσετε UTC, μπορείτε να εκτελέσετε sudo dpkg-reconfigure tzdata. Πηγαίνετε στο τέλος της σελίδας και επιλέξτε None of the above. Στην δεύτερη λίστα, επιλέξτε UTC .

2. Πως αλλάζει η ώρα στο Snorby?

Επιλέξτε Settings στην πάνω δεξιά γωνία

Κάντε κλικ στο κουτί δίπλα στο 'Time zone'

Επιλέξτε την ζώνη ώρας από την λίστα

Κάντε κλικ "Update Settings" στο κουμπί

Επιλέξτε την ίδια ζώνη ωρας στο CapMe's timezone.php

3. Πως αλλάζει η ώρα στο Squert?

Κάντε κλικ στο χρονικό διάστημα

Στην δεξιά μεριά, κάντε κλικ στα δυο βέλη που δείχνουν δεξιά

Απενεργοποιήστε UTC

Θέστε την ζώνη ώρας offset

Κάντε κλικ στο κουμπί "save TZ"

3. Γιατί η ώρα στο ELSA δεν υπάρχει στο UTC?

Από προεπιλογή το ELSA παρουσιάζει τις χρονικές σημάνσεις στη ζώνη ώρας του τοπικού browser σας. Μπορείτε να αναγκάσετε το ELSA να εμφανίζει πάντα τις χρονικές σφραγίδες σε UTC/GMT ρυθμίζοντας το use_utc στο Preferences panel της ELSA.

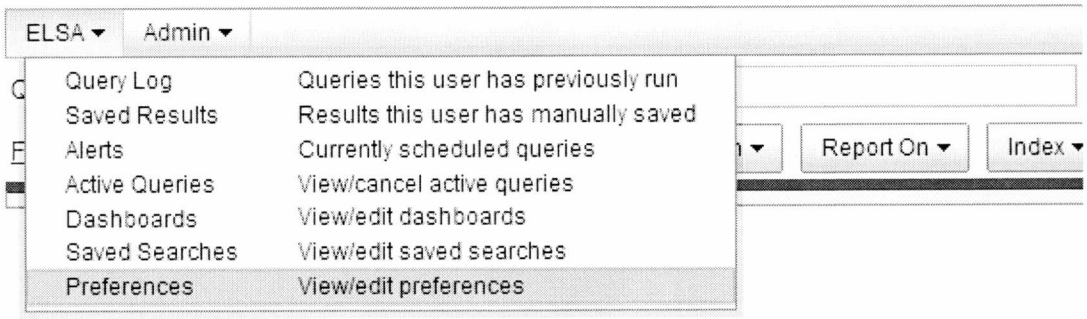
Εάν έχετε πρόσβαση στο ELSA από ένα πρόγραμμα περιήγησης του οποίου η τοπική ώρα δεν είναι UTC και δεν έχετε ενεργοποιήσει την ρύθμιση use_utc, τότε σε κάθε αναζήτηση ο χρόνος κυλά από πίσω από τον ίδιο αριθμό ωρών ως UTC offset.

Για παράδειγμα, υποθέτουμε ότι συνδέεστε στο ELSA και παρατηρείτε την προεπιλογή σε 2013-05-05 18:01:50. Όταν διεξάγετε έρευνα η προεπιλογή αλλάζει σε 2013-05-05 14:01:50.

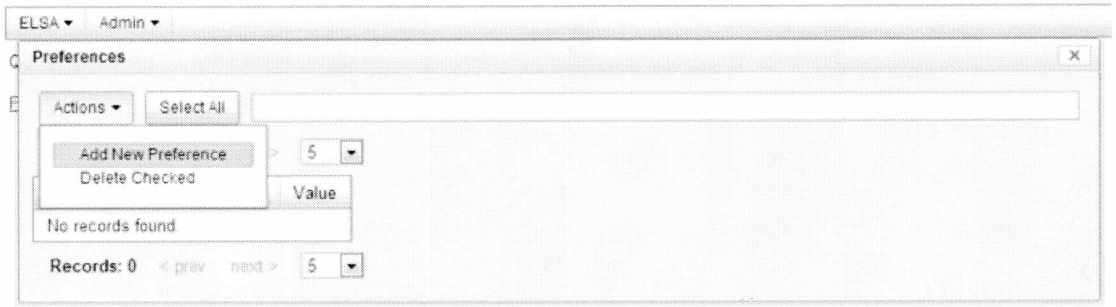
Η λύση είναι να καταστεί δυνατή η ρύθμιση use_utc στο Preferences του ELSA (το οποίο είναι πιθανώς μια καλή ιδέα για να εξασφαλιστεί ότι οι χρονικές σημάνσεις στο ELSA ταιριάζουν με τις χρονικές σημάνσεις στα Sguil/Squert/Snorby):

1) Περιηγηθείτε στην ELSA → Preferencses:

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

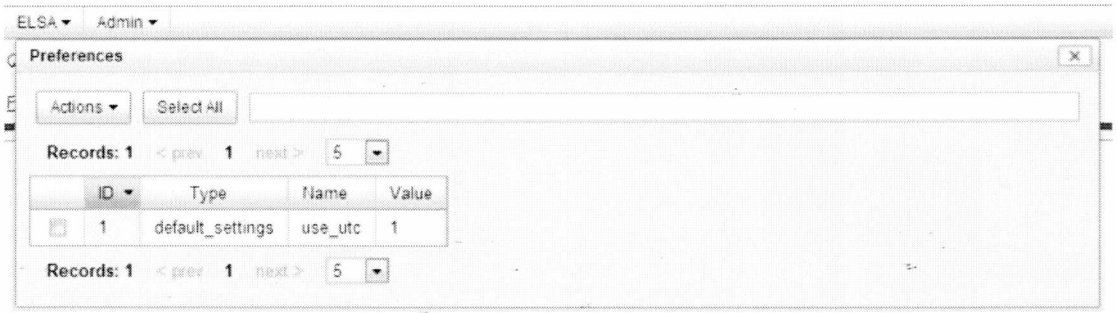



2) Επιλέξτε Actions → Add New Preference:




3) Εισάγετε το ακόλουθο στο New Preference:

```
Type = default_settings
Name = use_utc
Value = 1
```




## 1.8 Υπηρεσίες

Οι υπηρεσίες ελέγχονται από τα σενάρια NSM.

Ελέγξτε την κατάσταση όλων των υπηρεσιών:

```
sudo service nsm status
```

Εκκινήστε όλες τις υπηρεσίες:

```
sudo service nsm start
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Διακόψτε όλες τις υπηρεσίες:

```
sudo service nsm stop
```

Επανεκκινήστε όλες τις υπηρεσίες:

```
sudo service nsm restart
```

Server Services:

Ελέγξτε την κατάσταση του Sguild(Sguil server):

```
sudo nsm_server_ps-status
```

Εκκινήστε το Sguild:

```
sudo nsm_server_ps-start
```

Διακόψτε το Sguild:

```
sudo nsm_server_ps-stop
```

Επανεκκινήστε το Sguild:

```
sudo nsm_server_ps-restart
```

Sensor services:

Οι υπηρεσίες των αισθητήρων ελέγχονται από nsm_sensor_ps-*.

Λίστα με τις ελεγχόμενες υπηρεσίες:

```
sudo nsm_sensor_ps-* -?
```

Τα ακόλουθα παραδείγματα είναι για το Bro, αλλά μπορείτε να αντικαταστήσετε οποιαδήποτε υπηρεσία αισθητήρα προσπαθείτε να ελέγξετε:

Ελέγξτε την κατάσταση του Bro:

```
sudo nsm_sensor_ps-status --only-bro
```

Εκκινήστε το Bro:

```
sudo nsm_sensor_ps-start --only-bro
```

Διακόψτε το Bro:

```
sudo nsm_sensor_ps-stop --only-bro
```

Επανεκκινήστε το Bro:

```
sudo nsm_sensor_ps-restart --only-bro
```

## 1.9 Updating

Security Onion Update Procedure:

Initiating an update over SSH:

Αν ενημερώνετε το Security Onion σε μία σύνδεση SSH και η σύνδεση διακοπεί, τότε η διαδικασία εγκατάστασης μπορεί να μείνει σε ασυνεπή κατάσταση. Συνεπώς συνίσταται να εκτελέσετε byobu έτσι ώστε η συνεδρία σας να συνεχίσει να τρέχει στο Security Onion ακόμη κι όταν η σύνδεση διακοπεί. Το Byobu[5] είναι πολύ χρήσιμο και σας συνίσταται να εκτελείται συνεχώς για να αποφευχθεί η μη-συμμετοχή του στην ενημέρωση.

```
# install byobu
sudo apt-get install byobu
```

[5] Για περισσότερες πληροφορίες σχετικά με το byobu

https://help.ubuntu.com/community/Byobu

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
# enable byobu
byobu-enable

# you're now ready to update
```

**soup-** Security Onion UPdate:

Σας προτείνουμε να χρησιμοποιείτε το σενάριο soup για να εγκαταστήσετε αυτόματα όλες τις διαθέσιμες ενημερώσεις του Security Onion και των Ubuntu. Το soup θα αποφύγει όλα τα MySQL/PF_RING θέματα που περιγράφονται παρακάτω:

**Σημειώστε:** αν χρησιμοποιείτε ακόμα το παλιό Security Onion 12.04, το soup θα συνεχίσει να εγκαθιστά όλες τις ενημερώσεις για Ubuntu έως η Ubuntu σταματήσει να κυκλοφορεί ενημερώσεις για την έκδοση 12.04. Ωστόσο δεν θα υπάρξουν περισσότερες ενημερώσεις για την έκδοση του Security Onion 12.04, καθώς οι ενημερώσεις θα εκδίδονται μόνο για την έκδοση 14.04. Συνίσταται η αναβάθμιση από έκδοση 12.04 σε 14.04.

```
sudo soup
```

Παρακαλείστε να δώσετε προσοχή στην έξοδο αυτής της εντολής καθώς μπορεί να σας ζητήσει να λάβετε συγκεκριμένες δράσεις όπως η χειροκίνητη επανεκκίνηση των υπηρεσιών

Αν λάβετε το ακόλουθο σφάλμα:

```
sudo: soup: command not found
```

Μετά κάντε το ακόλουθο[6]:

```
sudo apt-get update && sudo apt-get install securityonion-sostat
```

Κατανεμημένες Επεκτάσεις

**Σημαντικό:** Πάντα ενημερώστε τον **master server** προτού την ενημέρωση των αισθητήρων:

Χρησιμοποιείτε το salt και soup για να ενημερώσετε ολόκληρη την ανάπτυξή σας.

salt and soup

[6] Για περισσότερες πληροφορίες δείτε εδώ: http://blog.securityonion.net/2013/08/new-securityonion-packages.html

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# 2. Interfaces

## 2.1 Snorby[7]

.Αν χρησιμοποιείται το Snorby στην 12.04 εγκατάστασή σας, θα πρέπει να προχωρήσετε στην μετάβαση σε Squert/Sguil και/ή ELSA. Για την απενεργοποίηση του Snorby στην υπάρχουσα εγκατάστασή σας, παρακαλούμε δείτε: https://github.com/Security-Onion-Solutions/security-onion/wiki/DisablingProcesses

Αρχικά αναπτύχθηκε από τον Dustin Webbe

Συνδεθείτε στο Snorby χρησιμοποιώντας την email address και το password που ορίσατε στην εγκατάσταση.

Το Snorby έχει δικές του MySQL βάσεις δεδομένων (ξεχωριστά από το Sguil και το ELSA).

Η βάση δεδομένων του Snorby αποθηκεύει **μόνο** ειδοποιήσεις NIDS από το Snort ή το Suricata.

Περιστραφείτε γύρω από μια ειδοποίηση NIDS του Snorby στο CapME για να αποκτήσετε πρόσβαση σε μια πλήρη καταγραφή πακέτων.

Περιστραφείτε από μια διεύθυνση IP του Snorby στο ELSA για σχετικές καταγραφές (Bro, OSSEC, syslog)

Αν επιθυμείτε να εξαλείψετε την βάση δεδομένων του Snorby δείτε στο: https://github.com/Security-Onion-Solutions/security-onion/wiki/WipingSnorby

## 2.2 Squert

Αναπτύχθηκε από τον Paul Halliday.

PHP web interface στην βάση δεδομένων του Sguil

Δουλεύει καλύτερα σε Chromium/Chrome browser.

Το Squert πιστοποιείται με την βάση δεδομένων του χρήστη του Sguil, επιτρέποντάς σας έτσι να συνδεθείτε στο Squert χρησιμοποιώντας τα ίδια username/password με το Sguil.

Σας δίνει πρόσβαση στα επόμενα δεδομένα: → ειδοποιήσεις NIDS → ειδοποιήσεις HIDS → Asset Data από PRADS (αν τα PRADS και pads_agent είναι ενεργοποιημένα) → HTTP καταγραφές από το Bro (εάν το http_agent είναι ενεργοποιημένο)

Μπορεί να περιστρέφεται σε μία πλήρη καταγραφή πακέτων για TCP κίνηση. Για να το πραγματοποιήσετε αυτό κάντε κλικ στο Event ID.

Μπορεί να περιστραφεί από το ELSA για την αναζήτηση αρχείων καταγραφής του Bro. Για να το κάνετε αυτό κάντε κλικ σε μία διεύθυνση IP, ή σε signature και στη συνέχεια κάντε κλικ στο ELSA. Στο Security Onion 14.04, το Squert περιστρέφεται στο ELSA χρησιμοποιώντας ένα σχετικό hyperlink έτσι ώστε να χρησιμοποιεί το ίδιο όνομα host ή την ίδια IP διεύθυνση που χρησιμοποιούνται και στην σύνδεση για το Squert. Αν χρησιμοποιείτε ακόμα το Security Onion 12.04, θα πρέπει να αλλάξετε την διεύθυνση IP που χρησιμοποιεί το Squert για να περιστραφεί στο ELSA. Μπορείτε να

[7] Το Snorby θεωρείται πλέον μη διατηρητέο και δεν περιλαμβάνεται πλέον στο Security Onion έπειτα από την έκδοση 14.04

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

χρησιμοποιήσετε τον ακόλουθο κώδικα από /usr/bin/sosetup (αντικαθιστώντας το $IP με την κανονική σας διεύθυνση ή όνομα host:

# Pivot from Squert to ELSA

URL="https://$IP:3154/?query_string=\"\${var}\"%20groupby:program"

HEXVAL=$(xxd -pu -c 256 <<< "$URL")

mysql -uroot -Dsecurityonion_db -e "INSERT IGNORE INTO filters (type,username,global,name,notes,alias,filter) VALUES ('url','','1','454C5341','','ELSA','$HEXVAL');"

## 2.3 Squil

Αναπτύχθηκε από τον Bamm Visscher.

TCL/TK (όχι web-based).

Ενιαία κεντρική βάση δεδομένων MySQL.

Σύνδεση: Χρησιμοποιήστε το username/password που ορίσατε στον οδηγό εγκατάστασης

→Μπορείτε να εισάγετε λογαριασμούς ως εξής(τα ονόματα του Sguil πρέπει να είναι αλφαριθμητικά)

```
sudo nsm_server_user-add
```

→Μπορείτε να αλλάξετε passwords χρησιμοποιώντας το Sguil client(File→Change Password) ή ώς εξής :

```
sudo nsm_server_user-passwd
```

→Μπορείτε να απενεργοποιήσετε λογαριασμούς ως εξής:

```
sudo nsm_server_user-disable
```

Τύποι δεδομένων: → ειδοποιήσεις NIDS από Snort/Suricata(αν snort_agent ενεργός) → ειδοποιήσεις HIDS από OSSEC(αν ossec_agent ενεργός) → session data από PRADS(αν PRADS και sancp_agent ενεργά) → asset data από PRADS(αν PRADS και pads_agent ενεργά) → HTTP καταγραφές από Bro (αν http_agent ενεργός)

Μπορείτε να περιστραφείτε στο transcript/Wireshark/NetworkMiner κάνοντας δεξί κλικ στο Alert ID

Μπορείτε να περιστραφείτε στο ELSA κάνοντας δεξί κλικ σε μια διεύθυνση IP και επιλέγοντας "ELSA IP Lookup"

Μπορείτε να αλλάξετε τα φόντα κάνοντας κλικ → Change Font.

Μπορείτε να αλλάξετε το μέγεθος των στηλών κάνοντας κλικ στην επικεφαλίδα της στήλης.

Είναι σημαντικό να εξασφαλίσετε ότι τα γεγονότα που εμφανίζονται στο Sguil ταξινομούνται τακτικά ή αλλιώς μπορεί να προκληθούν προβλήματα με την βάση δεδομένων του Sguil. Εξετάστε το ενδεχόμενο δημιουργίας ενός κανόνα autocat για να σας βοηθήσει με αυτό.

Ρυθμίσετε τις ειδοποιήσεις μέσω email του Sguil

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Ρυθμίστε τις κρατήσεις για το Sguil

## 2.4 ELSA

Αναπτύχθηκε από τον Martin Holste.

Web interface για το κυνήγι μέσω καταγραφών (Bro, Snort, OSSEC, Syslog)

Δουλεύει καλύτερα με Chromium/Chrome browser.

Περισσότερους τύπους δεδομένων από τα άλλα interfaces

Μπορεί να περιστραφεί στο CapME για την είσοδο σε πλήρη πακέτα καταγραφών.

Στο Security Onion 14.04, το ELSA έχει ιστογράμματα και πίνακες.

Πολύ γρήγορο και επεκτάσιμο (κάθε αισθητήρας έχει την δικιά του βάση δεδομένων MySQL και δείκτη sphinx)

Όταν διερευνάται το ELSA web interface, διερευνά όλες τις βάσεις δεδομένων ELSA ταυτόχρονα και σας δίνει συγκεντρωτικά τα αποτελέσματα.

Μπορείτε να συνδεθείτε στο ELSA χρησιμοποιώντας τα ίδια username/password με το Sguil.

Μπορείτε να χρησιμοποιήσετε την γραμμή εντολών του ELSA στο /opt/elsa/contrib/securityonion/contrib και χρησιμοποιώντας το σενάριο cli.sh :

```
sh cli.sh "example.com"
```

Το αποτέλεσμα είναι σε JSON έτσι θα χρειαστεί να εγκαταστήσετε jq και να στείλετε τα αποτελέσματα σε αυτό:

```
sh cli.sh "example.com" | jq '.'
```

## 2.5 CapMe

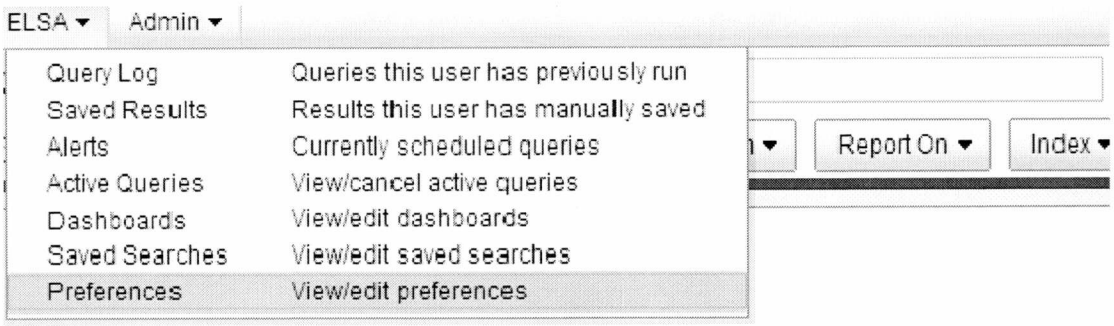
CapMe Authentication:

Η εγκατάστασή ρυθμίζει αυτόματα και το Snorby και το ELSA ώστε να μπορούν να περιστρέφονται στο CapME για πλήρεις μεταγραφές. Η σελίδα CapME θα σας ζητήσει το username και το password σας και θα δώσετε το κανονικό username/password από τα Sguil/ Squert/ ELSA. 'Εχετε την επιλογή της αυτόματης γνησιότητας αλλά να προσέχετε γιατί αυτό θα στείλει το username και το password σας στην αίτηση GET και θα εμφανίζεται στην μπάρα της περιήγησης σε απλό κείμενο.

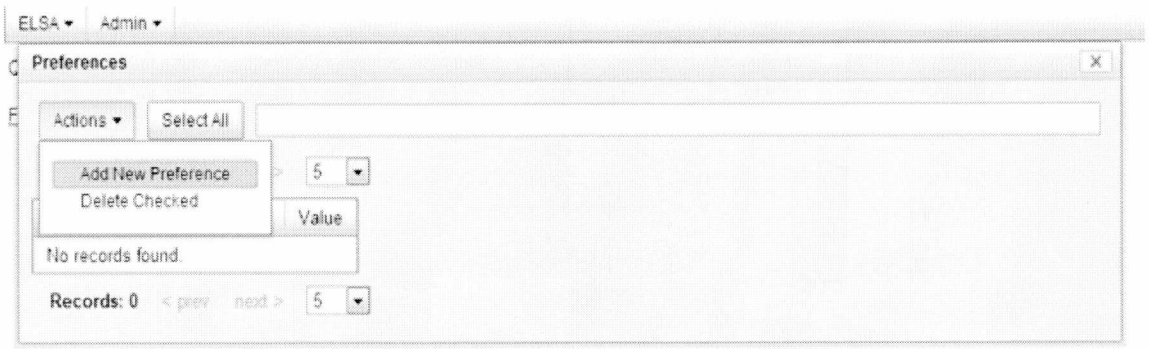
Configurin ELSA To auto-authenticate to CapME:

Μεταβείτε στο ELSA→Preferences:

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79




Επιλέξτε Actions→Add New Preference:




Εισάγετε το ακόλουθο στο New Preference:

```
Type = custom
Name = openfpc_username
Value = "your Sguil username"
```

Κλείστε το παράθυρο με τις Preferences και επαναφορτώστε την σελίδα ELSA ( F5)

Configuring Snorby to auto - authenticate to CapME:

Κάντε κλικ στο "Administration and General Settings"

Κάτω από το OpenFPC, επιλέξτε "Packet capture auto-authenticate" και εισάγετε το username/password που έχετε στο Sguil.

Επιλέξτε "Save Settings"

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# 3. Πηγές Δεδομένων

## 3.1 NIDS

Το Security Onion σας παρέχει την επιλογή για Snort ή Suricata ως σύστημα εντοπισμού της διαδικτυακής εισβολής. Έχουμε συγκεντρώσει και τα δύο αυτά με PF_RING για να σας επιτρέψει να γυρίσει σε πολλαπλές περιπτώσεις ώστε να χειριστείτε περισσότερη κυκλοφορία.

Snort[8]: Πρόκειται για ένα σύστημα πρόληψης εισβολών σε πραγματικό χρόνο και επίσης καταγραφή πακέτων.

Suricata[9]: είναι ένα υψηλής απόδοσης Network IDS, IPS και μηχανή Network Security Monitoring. Το Suricata έχει αναπτυχθεί από την OISF και από την υποστήριξη των προμηθευτών του.

Τρεις Λόγοι να επιλέξετε Suricata:

1)Εξαιρετικά εύχρηστο

2)Αναγνώριση Πρωτοκόλλου

3)Αναγνώριση Αρχείου, MD5 Checksums, Εξαγωγή Αρχείων

## 3.2 Bro

Bro*n

/opt/bro/etc/node.cfg

Συντάσσουμε Bro με PF_RING έτσι ώστε να μπορείτε να χρησιμοποιείτε πολλαπλούς Bro workers για να διαχειρίζεστε περισσότερη κίνηση.

Custom Scripts

/opt/bro/share/bro/site/local.bro

Μπορείτε να προσθέσετε επιπλέον προσαρμοσμένα σενάρια στο /opt/bro/share/bro/site/local.bro

Για να ελέγξετε και να δείτε αν το Bro σενάριο εμφάνισε μια ειδοποίηση, πηγαίνετε στο ELSA, επιλέξτε Ειδοποίηση και μετά επιλέξετε "Top Notice Types".

Email

Για να ρυθμίσετε ειδοποιήσεις των email επεξεργαστείτε: /opt/bro/etc/broctl.cfg και ορίστε τα ακόλουθα: MailTo = YourUsername@yourDomain.com

sendmail= /usr/sbin/sendmail

Έπειτα συγχρονίστε και επανεκκινήστε το Bro: sudo nsm_ps-restart -- only-bro

Θα δέχεστε κάθε ώρα connection summary emails. Εαν δεν επιθυμείτε τα connection summary emails, μπορείτε να προσθέσετε το ακόλουθο στο broctl.cfg και να συγχρονίσετε και επανεκκινήσετε το Bro όπως δείξαμε επάνω.

---

[8] http://snort.org

[9] http://suricata-ids.org/

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

tracesummary=

Εαν επιθυμείτε να λαμβάνετε emails για τις ειδοποιήσεις του Bro θα προσθέσετε το : /opt/bro/share/bro/site/local.bro και να συγχρονίσετε και επανεκκινήσετε ώς εξής:

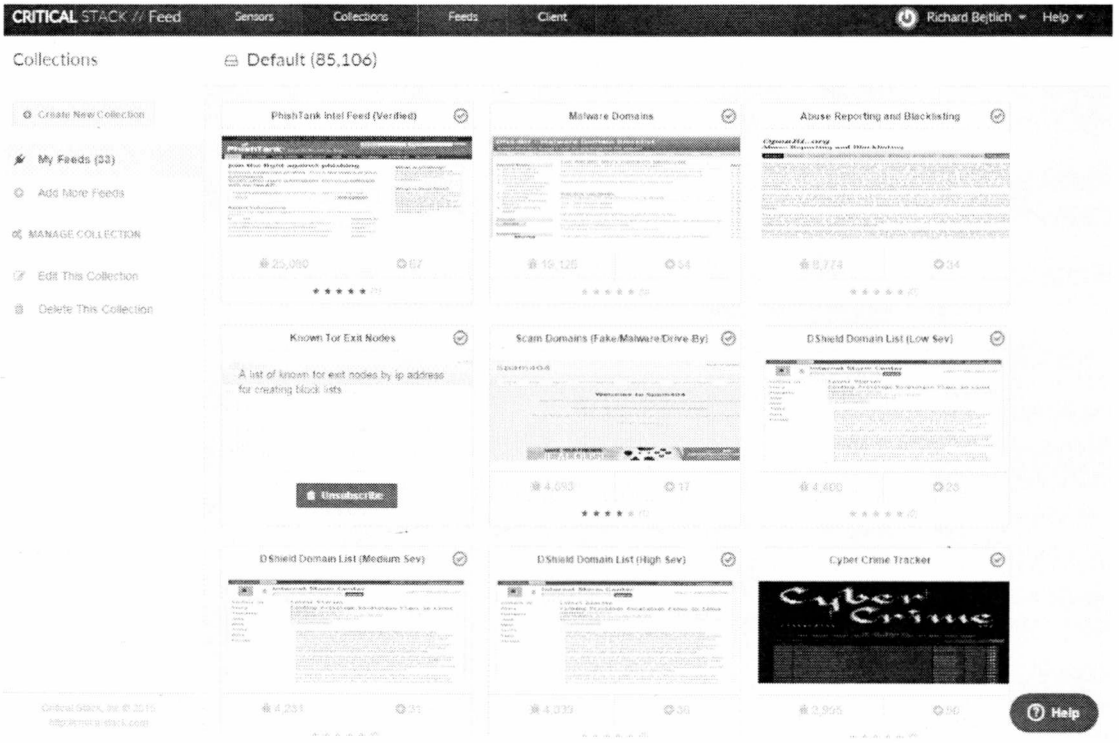
```
hook Notice::policy(n: Notice::Info)
    {
    add n$actions[Notice::ACTION_ALARM];
    }
```

Intel:

Το Bro περιλαμβάνει ένα πλαίσιο νοημοσύνης το οποίο διευκολύνει την ενσωμάτωση διαφόρων πηγών στο Bro. Οι πηγές αυτές μπορούν να περιλαμβάνουν περισσότερα πράγματα από απλές IP διευθύνσεις.

Intel::ADDR
Intel::URL
Intel::SECURITYSOFTWARE
Intel::EMAIL
Intel::DOMAIN
Intel::USER_NAME
Intel::FILE_HASH
Intel::FILE_NAME
Intel::CERT_HASH

Το Critical Stack Intel Client σας διευκολύνει να γίνετε συνδρομητής σε πάνω από 30 Threat Feeds στο πλαίσιο νοημοσύνης του Bro. Το παρακάτω screenshot σας δείχνει μερικά από τα feeds:




Logs:

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

/nsm/bro/logs

Το Bro παρακολουθεί την κίνηση του διαδικτύου σας και δημιουργεί logs όπως οι παρακάτω:

CONN.LOG

Αυτό το σενάριο διαχειρίζεται την παρακολούθηση/καταγραφή των γενικών πληροφοριών σχετικά με τα πρωτόκολλα TCP, UDP και ICMP. Για συνδέεις UDP και ICMP η ερμηνεία τους γίνεται με την χρήση μιας ακολουθίας πακέτων από την πηγή προς τον προορισμό. Επίσης τα ICMP ερμηνεύονται ως source port που σημαίνει ότι το είδος του μηνύματος ICMP και η θύρα προορισμού είναι ο κωδικός του μηνύματος ICMP.

Namespace: Conn

Imports: base/utils/site.bro

Source File: /scripts/base/protocols/conn/main.bro

Summary:

Types:

Conn:Info.record περιέχει στοιχεία απο τις καταγραφές των συνδέσεων

Redefinitions:

Log: ID enum Το αναγνωριστικό της σύνδεσης εισόδου.

connection: record

Events:

Conn: log_conn:event: το event που χρησιμοποιείται για την είσοδο στο Conn: info record

Detailed Interface:

Type: record

ts: time &log: η ώρα καταγραφής του πρώτου πακέτου.

uid: string &log ένας μοναδικός κωδικός αναγνώρισης για την σύνδεση

id: conn_id &log The connection's 4-tuple of endpoint addresses/ports.

proto: transport_proto &log Το πρωτόκολλο μεταφοράς της σύνδεσης.

service: string &log &optional ένα αναγνωριστικό της εφαρμογής του πρωτοκόλλου που αποστέλλεται για την σύνδεση

duration: interval &log &optional Πόσο διήρκησε η σύνδεση.

orig_bytes: count &log &optional Ο αριθμός των payload bytes που απέστειλε ο εντολέας.

resp_bytes: count &log &optional Ο αριθμός των payload bytes που ο αποστολέας έστειλε.

conn_state: string &log &optional

conn_state: ερμηνεία

S0 προσπάθεια σύνδεσης, καμία απάντηση

S1 σύνδεση εδραιώθηκε, δεν τερματίστηκε

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

SF κανονική εγκατάσταση και τερματισμός. Πρόκειται για το ίδιο σύμβολο με την κατάσταση S1 αλλά στο S1 δεν υπάρχει καταμέτρηση των bytes.

REJ προσπάθεια σύνδεσης, απορρίπτεται

S2 σύνδεση εγκαταστάθηκε και η προσπάθεια είναι ορατή από τον εντολέα (χωρίς απάντηση από τον responder)

S3 σύνδεση εγκαταστάθηκε και η προσπάθεια είναι ορατή από τον ανταποκριτή (αλλά οχι απάντηση από τον εντολέα originator)

RSTO σύνδεση εγκαταστάθηκε originator aborted (εστάλθη RST)

RSTR εγκαταστάθηκε, responder aborted

RSTOS0 ο originator έστειλε SYN ακολοθούμενο από FIN, δεν είδαμε ποτέ SYN-ACK από τον responder

RSTRH Ο responder έστειλε ενα SYN ACK ακολοθούμενο από RST, δεν είδαμε ποτέ SYN από τον originator

SH Ο originator έστειλε ενα SYN ακολοθούμενο από ενα FIN, ποτέ δεν είδαμε SYN ACK από τον responder

SHR Ο responder έστειλε ένα SYN ACK ακολοθούμενο από ενα FIN, ποτέ δεν είδαμε SYN από τον originator

OTH δεν είδαμε SYN

local_orig: bool &log &optional: εάν η σύνδεση βρίσκεται τοπικά,η τιμή αυτή θα είναι T. Αν προήλθε από απόσταση θα είναι F. Σε περίπτωση που το Site::local_nets variable ειναι απροσδιόριστο, αυτό το πεδίο θα παραμείνει κενό.

local_resp: bool &log &optional: εάν η σύνδεση απάντησε σε τοπικό επίπεδο αυτή η τιμή θα είναι T. Αν απάντησε από απόσταση τότε θα είναι F. Στην περίπτωση που το Site::local_nets variable ειναι απροσδιόριστο, το πεδίο θα παραμείνει κενό.

missed_bytes: count &log &default = 0 &optional: Δείχνει τον αριθμό των bytes που απωλέσθηκαν και είναι αντιπροσωπευτική της απώλειας των πακέτων.Μια τιμή διάφορη του μηδενός κανονικά θα προκαλέσει αποτυχία ανάλυσης του πρωτοκόλλου εκτός αν κάποια ανάλυση έχει ολοκληρωθεί πριν από την απώλεια των πακέτων.

history: string &log &optional: Καταγράφει την κατάσταση της ιστορίας των συνδέσεων ως μία σειρά από γράμματα. Η έννοια των γραμμάτων είναι η εξής:

s SYN w/o the ACK bit set

h a SYN+ACK

a a pure ACK

d packet with payload

f packet with FIN bin set

r packet with RST bit set

c packet with a bad check sum

i inconsistent packet (FIN+RST)

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

q multi flag packet(SYN+FIN or SYN+RST)

Όταν το γεγονός προέρχεται από τον originator το γράμμα είναι κεφαλαίο. Ενώ όταν προέρχεται από τον responder είναι πεζό. Πολλαπλά πακέτα του ιδίου τύπου θα εμφανιστούν μία φορά.

orig_pkts: count &log &optional Ο αριθμός των πακέτων που απέστειλε ο originator. ισχύει μόνο όταν: use_conn_size_analyzer =T.

orig_ip_bytes: count &log &optional ο αριθμός των bytes που έστειλε ο originator. ισχύει μόνο όταν: use_conn_size_analyzer = T.

resp_pkts: count &log &optional Ο αριθμός των πακέτων που έστειλε ο responder. ισχύει μόνο όταν : use_conn_size_analyzer = T.

resp_ip_bytes: count &log &optional ο αριθμός των IP που έστειλε ο responder. ισχύει μόνο όταν : use_conn_size_analyzer = T.

vlan: int &log &optional η εξωτερική VLAN για αυτήν την σύνδεση, αν ισχύει.

inner_vlan: int &log &optional η εσωτερική VLAN για αυτήν την σύνδεση, αν ισχύει

Events:

Conn: : log_conn

Type: event(rec:Conn::Info)

Γεγονός που μπορεί να αντιμετωπιστεί για να αποκτήθεί πρόσβαση στο Conn::Info record καθώς αποστέλλεται στο logging framework.

DNS.LOG:

παρακολουθεί και καταγράφει τα ερωτήματα DNS μαζί με τις απαντήσεις τους.

Namespace: DNS

Imports: base/protocols/dns/consts.bro.base/utils/queue.bro

Source File: /scripts/base/protocols/dns/main.bro

Summary:

Options:

DNS::max_pending_msgs: count &redef: Όταν ο αριθμός των αναπάντητων ερωτήσεων συμπληρωθεί η περαιτέρω προσπάθεια θα αποφευχθεί. (αυτό δεν θα

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

πρέπει να συμβεί εκτός αν ο DNS server έχει πρόβλημα και το Bro δεν βλέπει όλη την DNS κυκλοφορία ή ένα ερώτημα AXFR βρίσκεται σε εξέλιξη.

DNS::max_pending_query_ids: count &redef όταν υπάρχει έστω και μία αναπάντητη ερώτηση ή απάντηση

## 3.3 OSSEC HIDS

Το Security Onion χρησιμοποιεί τον OSSEC ώς Host Intrusion Detection System ( HIDS). Το OSSEC παρακολουθεί και υπερασπίζεται το Security Onion, μπορείτε επίσης να προσθέσετε και άλλους OSSEC agents να παρακολουθούν άλλους κεντρικούς υπολογιστές στο δίκτυό σας. Επιπρόσθετα ίσως χρειάζεστε να:

Ρυθμίσετε το OSSEC να στέλνει ειδοποιήσεις μέσω email.

Αποστέλλετε καταγραφές του OSSEC σε έναν εξωτερικό syslog συλλέκτη.

Active Response:

Μερικές φορές το OSSEC ίσως αναγνωρίσει κάποια νόμιμη δραστηριότητα ώς κακόβουλη και να συμμετάσχει στην Active Response ώστε να εμποδίσει την σύνδεση.Αυτό μπορεί να οδηγήσει σε απρόβλεπτες συνέπειες και στην αποτροπή σύνδεσης με αξιόπιστες IPs.Μπορείτε να επιτρέψετε την σύνδεση με αυτές τις IPs και να αλλάξετε άλλες ρυθμίσεις στο /var/ossec/etc/ossec.conf

```
<global>
<white_list>desired_ip</white_list>
</global>
```

Adding Agents:

Μπορείτε να κατεβάσετε εκδόσεις σε Windows/ Unix/ Linux/ FreeBSD για την πλατφόρμα OSSEC από την επίσημη σελίδα. Μόλις έχετε εγκαταστήσει τον OSSEC στο σύστημα που πρέπει να παρακολουθείτε, εκτελέστε τα βήματα που καθορίζονται εδώ:http://ossec-docs.readthedocs.org/en/latest/manual/agent/agent-management.html#managing-agents

Μπορεί να χρειαστεί να επιτρέψετε την κίνηση της κυκλοφορίας από την IP διεύθυνσή του OSSEC σας.

Automated Deployment[10]:

Πολλοί χρήστες προτιμούν την δυνατότητα να αναπτύξουν OSSEC agents στα συστήματά τους. Αν και αυτό δεν έχει δοκιμαστεί ούτε υποστηρίζεται, το Auto-OSSEC παρέχει μια μέθοδο για την επίτευξη αυτού του στόχου.

[10] Για περισσότερες πληροφορίες δείτε: https://github.com/binarydefense/auto-ossec.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

## 3.4 Syslog[11]

Το Security Onion χρησιμοποιεί syslog-ng ως τον κύριο syslog συλλέκτη.

Το αρχείο των ρυθμίσεων βρίσκεται σε `/etc/syslog-ng/syslog-ng.conf`

Το Security Onion χρησιμοποιεί syslog-ng για να προωθήσει Bro, IDS, OSSEC καταγραφές στο ELSA.

Το syslog-ng μπορεί να συνεργαστεί και με συστήματα τρίτων ώστε να διαβιβάσει ειδοποιήσεις Bro, OSSEC και IDS.

Το syslog-ng συνδέεται στην θύρα 514 (TCP και UDP) για τις εισερχόμενες syslog από άλλες συσκευές. Μπορείτε να χρησιμοποιήσετε την εκτέλεση του Security Onion-allow για να επιτρέψετε την κίνηση απο τη IP Address στο δικό σας syslog sender. Αυτό σας δίνει την συλλογή των αρχείων καταγραφής. Αν θέλετε αυτά τα αρχεία καταγραφής που συλλέγονται από άλλες συσκευές να αναλυθούν, μία άλλη επιλογή είναι να ρυθμίσετε το OSSEC να λαμβάνει syslog απευθείας σε μία θύρα διαφορετική από την syslog-ng θύρα του 514.

---

[11] http://ossec-docs.readthedocs.org/en/latest/syntax/head_ossec_config.remote.html
http://www.ossec.net/ossec-docs/OSSEC-book-ch3.pdf

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# 4. Προσαρμογή για το δίκτυό σας

## 4.1 Διαμόρφωση Δικτύου

Απενεργοποίηση του γραφικού "Network Manager" και ρύθμιση του δικτύου από την γραμμή εντολών. Αν χρησιμοποιείτε το Security Onion 12.04/14.02 η ρύθμιση αυτή θα γίνει αυτομάτως αν επιλέξετε "Yes,configure /etc/network/interfaces" στον οδηγό εγκατάστασης. Σημαντικό: ίσως να χάσετε την συνδεσιμότητα σας με το δίκτυο κατά την διάρκεια αυτής της διαδικασίας. Συνίσταται η ύπαρξη ενός εφεδρικού σχεδίου.

Διακοπή Network Manager:

```
sudo /etc/init.d/network-manager stop
```

Αποτροπή εκκίνησης του Network Manager:

```
sudo mv /etc/init/network-manager.conf /etc/init/network-
manager.conf.DISABLED
```

'Επειτα ρυθμίστε τις network interfaces σε : `/etc/network/interfaces`

Management interface:

Θα χρειαστείτε ένα management interface που να χρησιμοποιεί είτε DHCP είτε στατική IP.

Sniffing interface(s):

Χρειάζεστε μια ή περισσότερες interfaces που να κάνουν sniffing (όχι σε IP διευθύνσεις). Λειτουργίες εκφόρτωσης NIC(offloading functions) όπως tso, gso, gro θα πρέπει να είναι απενεργοποιημένες ώστε να διασφαλίσετε ότι τα Snort/Suricata λαμβάνουν μια ακριβή παρακολούθηση της κίνησης.

Δείγμα /etc/network/interfaces:

```
auto lo
iface lo inet loopback

# Management interface using DHCP (not recommended due to Bro issue
described above)
auto eth0
iface eth0 inet dhcp

# OR
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
# Management interface using STATIC IP (instead of DHCP)
auto eth0
iface eth0 inet static
  address 192.168.1.14
  gateway 192.168.1.1
  netmask 255.255.255.0
  network 192.168.1.0
  broadcast 192.168.1.255
  # If running Security Onion 12.04, you'll need to configure DNS here
  dns-nameservers 192.168.1.1 192.168.1.2

# AND one or more of the following

# Connected to TAP or SPAN port for traffic monitoring
auto eth1
iface eth1 inet manual
  up ifconfig $IFACE -arp up
  up ip link set $IFACE promisc on
  down ip link set $IFACE promisc off
  down ifconfig $IFACE down
  post-up for i in rx tx sg tso ufo gso gro lro; do ethtool -K $IFACE $i
off; done
  # If running Security Onion 12.04, you should also disable IPv6 as
follows:
  post-up echo 1 > /proc/sys/net/ipv6/conf/$IFACE/disable_ipv6
```

Πιθανόν να χρειάζεται να ρυθμίσετε το μέγεθος του RX buffer όπως στην επόμενη εντολή:

```
post-up ethtool -G $IFACE rx 4096; for i in rx tx sg tso ufo gso gro lro;
do ethtool -K $IFACE $i off; done
```

Παρατηρείστε ότι το 4096 είναι μόνο ένα παράδειγμα και το NIC σας να έχει διαφορετικό μέγιστο rx μέγεθος. Για να το εντοπίσετε θα χρησιμοποιήσετε:

```
ethtool -g ethX
```

Αν κριθεί απαραίτητο, ρυθμίστε το DSN σε `/etc/resolv.conf`:

Επανεκκινήστε το δίκτυο:

```
sudo /etc/init.d/networking restart
```

Αν είχατε ήδη αισθητήρες να λειτουργούν σε αυτά τα interfaces, θα πρέπει να τους επανεκκινήσετε:

```
sudo nsm_sensor_ps-restart
```

## 4.2 Proxy Configuration

Ρυθμίστε τον proxy server στο /etc/environment ώς εξής:

```
export http_proxy=https://server:port
export https_proxy=https://server:port
export ftp_proxy=https://server:port
export PERL_LWP_ENV_PROXY=https://server:port
export no_proxy="localhost,127.0.0.1"
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Αν πρόκεται να εκτελέσετε οτιδήποτε χρησιμοποιώντας sudo, θυμηθείτε να χρησιμοποιήσετε την επιλογή 'i' για να την αναγκάσει να επεξεργαστεί τις μεταβλητές του περιβάλλοντος. Για παράδειγμα:

```
sudo -i rule-update
```

Για συγκεκριμένες proxies(Bluecoat) ίσως χρειαστεί να αλλάξετε από https σε http στο /etc/nsm/pulledpork/pulledpork.conf. Για παράδειγμα δείτε:

## 4.3 Firewall / Hardening

Το προεπιλεγμένο εργαλείο διαμόρφωσης του firewall για το Ubuntu είναι το ufw. Είναι ενεργοποιημένο από προεπιλογή στο Security Onion.

Enable/Disable:

```
sudo ufw enable

sudo ufw disable
```

Allow/Deny:

Για παράδειγμα: Επιτρέπει την θύρα 9876 για Xplico

```
sudo ufw allow 9876/tcp
```

**Για παράδειγμα:** Επιτρέπει την irc σε εύρος θυρών 6667-7000

```
sudo ufw allow 6667:7000
```

**Για παράδειγμα:** Άρνηση των https:

```
sudo ufw deny 443
```

What Ports Are Opened/Listening:

Παράδειγμα:

```
sudo ufw status
```

Παράδειγμα εξόδου:

```
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
8000/tcp                   ALLOW       Anywhere
7734/tcp                   ALLOW       Anywhere
7736/tcp                   ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
3000/tcp                   ALLOW       Anywhere
172.30.15.16 80/tcp        ALLOW       172.30.15.10
3154/tcp                   ALLOW       Anywhere
```

Παραπάνω μπορείτε να δείτε ότι υπάρχει ένας κανόνας που περιορίζει την κίνηση στην πηγή IP, στον προορισμό IP και στην θύρα TCP. Αυτός ο κανόνας προστέθηκε μετά την εγκατάσταση του DVWA στο ίδιο VM προκειμένου να δοκιμαστεί η ανίχνευση ορισμένων βασικών επιθέσεων εφαρμογών του δικτύου. Ο κανόνας είναι ο εξής :

```
sudo ufw allow proto tcp from 172.30.15.10/32 to 172.30.15.16 port 80
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Tightening the firewall on a master server:

Από προεπιλογή ο master server επιτρέπει συνδέσεις στις ακόλουθες θύρες από οποιεσδήποτε ip διευθύνσεις:

22 - SSH

443 - Squert/ELSA/CapMe

514 - Syslog

1514/udp - OSSEC

7734 - Sguil client

7736 - sensor connection to sguild

Μπορεί να θέλετε να περιορίσετε αυτές τις θύρες μόνο για την αποδοχή συνδέσεων από ένα υποσύνολο των διευθύνσεων IP. Πριν επιχειρήσετε οποιαδήποτε αλλαγή στο firewall, θα πρέπει να βεβαιωθείτε ότι έχετε ένα εφεδρικό σχέδιο, σε περίπτωση που κατά λάθος μπλοκάρετε την δική σας σύνδεση. Έτσι βεβαιωθείτε ότι έχετε DRAC/KVM/physical ή άλλη μορφή πρόσβασης.

Firewall rules to allow sensors to connect to master:

Καταρχήν προσθέστε έναν κανόνα όπως ο παρακάτω για κάθε αισθητήρα σας(αντικαθιστώντας a.b.c.d. με την πραγματική διεύθυνση IP του αισθητήρα) για να συνδέσετε στη θύρα 22(SSH) και 7736(Sguild):

```
sudo ufw allow proto tcp from a.b.c.d to any port 22,7736
```

ή

αν εκτελείτε Salt, τότε οι αισθητήρες πρέπει να είναι συνδεδεμένοι στις θύρες 4505/tcp και 4506/tcp:

```
sudo ufw allow proto tcp from a.b.c.d to any port 22,4505,4506,7736
```

Firewall rules to allow syslog devices:

'Επειτα προσθέστε έναν κανόνα  σαν τον επόμενο για τις διευθύνσεις IP που θα στέλνουν syslog (θύρα 514tcp και udp):

```
sudo ufw allow from a.b.c.d to any port 514
```

Firewall rules to allow OSSEC agents:

Προσθέστε έναν κανόνα σαν τον επόμενο για τις διευθύνσεις IP οι οποίες θα εκτελούν OSSEC (θύρα 1514 udp):

```
sudo ufw allow proto udp from a.b.c.d to any port 1514
```

Firewall rules to allow analysts/administrators to connect to master:

Προσθέστε έναν κανόνα σαν τον ακόλουθο για τις διευθύνσεις IP ή για το υποδίκτυο που θα χρησιμοποιείτε για να συνδέεστε με τον master ως αναλυτής/διαχειριστής στις θύρες 22(SSH), 443 (Squert/ELSA/CapMe), 7743(Sguil client):

```
sudo ufw allow proto tcp from a.b.c.d to any port 22,443,7734
```

Remove default "allow from Anywhere" rules:

Μόλις προσθέσετε αυτούς τους νέους κανόνες, μπορείτε να αφαιρέσετε τους προεπιλεγμένους "allow from Anywhere" κανόνες:

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
sudo ufw delete allow 22/tcp
sudo ufw delete allow 443/tcp
sudo ufw delete allow 444/tcp
sudo ufw delete allow 514
sudo ufw delete allow 1514/udp
sudo ufw delete allow 3154/tcp
sudo ufw delete allow 7734/tcp
sudo ufw delete allow 7736/tcp
```

Tightening the firewall on a sensor:

Από προεπιλογή, ένας αισθητήρας επιτρέπει τις συνδέσεις στις ακόλουθες θύρες από οποιαδήποτε IP διεύθυνση:

22 - SSH

514 - Syslog

1514/udp - OSSEC

'Ισως να θέλετε να περιορίσετε αυτές τις θύρες να αποδέχονται συνδέσεις μόνο από ένα υποσύνολο από διευθύνσεις IP. Πριν επιχειρήσετε οποιαδήποτε αλλαγή στο firewall, θα πρέπει να βεβαιωθείτε ότι έχετε ένα εφεδρικό σχέδιο, σε περίπτωση που κατά λάθος μπλοκάρετε την δική σας σύνδεση. 'Ετσι βεβαιωθείτε ότι έχετε DRAC/KVM/physical ή άλλη μορφή πρόσβασης

Firewall rules to allow syslog devices:

Προσθέστε έναν κανόνα σαν τον επόμενο για τις διευθύνσεις IP που θα στέλνουν syslog (θύρα 514 tcp και udp):

```
sudo ufw allow from a.b.c.d to any port 514
```

Firewall rules to allow OSSEC agents:

Προσθέστε έναν κανόνα για τις διευθύνσεις IP που θα εκτελούν OSSEC (θύρα 1514 udp):

```
sudo ufw allow proto udp from a.b.c.d to any port 1514
```

Firewall rules to allow analysts/administrators to connect to master:

Προσθέστε έναν κανόνα για τις διευθύνσεις IP ή το υποδίκτυο που θα χρησιμοποιείτε για να συνδέεστε στον αισθητήρα σαν αναλυτής/διαχειριστής στην θύρα 22:

```
sudo ufw allow proto tcp from a.b.c.d to any port 22
```

Remove default "allow from Anywhere" rules:

Μόλις προσθέσετε αυτούς τους κανόνες, αφαιρέστε την προεπιλογή "allow from Anywhere" :

```
sudo ufw delete allow 22/tcp
sudo ufw delete allow 514
sudo ufw delete allow 1514/udp
```

## 4.4 Email Configuration

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Σε αυτήν την ενότητα περιγράφεται ο τρόπος ρύθμισης των email για τις ειδοποιήσεις και τις αναφορές. Εφαρμογές όπως το Sguil και OSSEC διαθέτουν τις δικες τους ρυθμίσεις email και δεν βασίζονται σε στο email του λειτουργικού συστήματος. Ωστόσο μπορείτε να εγκαταστήσετε αν το επιθυμείτε, έναν server με email στο λειτουργικό σύστημα ώστε να μπορείτε να λαμβάνετε καθημερινά μηνύματα email από την sostat script και από το Bro.

How do I configure the OS itself to send emails?

Εγκαταστήστε και ρυθμίσετε τον αγαπημένο σας email server. Ανάλογα με τις ανάγκες σας, μπορεί να είναι κάτι απλό όπως `nullmailer` (συνίσταται) ή κάτι περίπλοκο όπως `exim4` .

Εδώ είναι μερικές nullmailer ρυθμίσεις:

```
sudo apt-get install nullmailer
# edit /etc/mailname to hold your "from" domain name. (If you were google,
you'd use "gmail.com".)
# edit /etc/nullmailer/adminaddr to contain the address you want mail to
root to be routed to.
# edit /etc/nullmailer/remotes to contain the mail server to forward email
to.
```

Εναλλακτικά, εδώ είναι μερικές οδηγίες για exim4:

```
sudo apt-get -y install mailutils
sudo dpkg-reconfigure exim4-config
```

Μόλις ρυθμίσετε τον email server σας και διαπιστώσετε ότι μπορεί να στείλει email σωστά, ίσως θέλετε να δημιουργήσετε μια καθημερινή cronjob για να εκτελείτε `/usr/bin/sostat` και να σας αποστέλει με email το μήνυμα:

```
# /etc/cron.d/sostat
#
# crontab entry to run sostat and email its output

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
EMAIL=YourUsername@YourDomain.com

01 12    * * *   root    HOSTNAME=`hostname`; /usr/bin/sostat 2>&1 | mail -
s "$HOSTNAME stats" $EMAIL
```

Αν δεν έχετε ήδη το βοηθητικό πρόγραμμα email, μπορείτε να δοκιμάσετε να εγκαταστήσετε:

```
sudo apt-get install mailutils
```

How do i configure Sguil to send alerts via email?

Τροποποιήστε `/etc/nsm/securityonion/sguild.email` (στον master server) όπως απαιτείται και επανεκκινήστε το Sguild:

```
sudo nsm_server_ps-restart
```

Μπορείτε να επαληθεύσετε τις ρυθμίσεις email, ψάχνοντας στο πάνω μέρος του αρχείου καταγραφής του Sguild:

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
head -20 /var/log/nsm/securityonion/sguild.log
```

Να γνωρίζετε ότι το Sguil θα στείλει ειδοποιήσεις μέσω email για αυτά που θεωρεί νέα γεγονότα. Βεβαιωθείτε ότι έχετε ταξινομήσει τα γεγονότα στο εσωτερικό της κονσόλας του Sguil, ή εξετάστε το ενδεχόμενο για την δημιουργία ενός κανόνα Autocat ο οποίος να κατατάσει αυτόματα τα γεγονότα ή αν προτιμάτε να λαμβάνετε μηνύματα email για όλες τις περιπτώσεις ειδοποιήσεων. Διαφορετικά ενδέχεται να μην λαμβάνετε ειδοποιήσεις όπως θα έπρεπε.

How do i configure OSSEC to send emails?

Τροποποιήστε /var/ossec/etc/ossec.conf ως εξής:

```
<global>
    <email_notification>yes</email_notification>
    <email_to>YourUsername@YourDomain.com</email_to>
    <smtp_server>YourMailRelay.YourDomain.com</smtp_server>
    <email_from>ossec@YourDomain.com</email_from>
    <email_maxperhour>100</email_maxperhour>
  </global>
```

Μετά επανεκκινήστε τον OSSEC:

```
sudo service ossec-hids-server restart
```

How do i configure ELSA to send emails?

Προσθέστε την διεύθυνση email σας στο user_info table του securityonion_db database(αντικαθιστώντας FIRSTLAST@YOURDOMAIN.COM με την πραγματική σας διεύθυνση και το FIRSTLAST με το όνομα χρήστη του Sguil/ELSA):

```
mysql -uroot -Dsecurityonion_db -e "update user_info set
email='FIRSTLAST@YOURDOMAIN.COM' where username='FIRSTLAST';"
```

Επανεκκινήστε το Apache:

```
sudo service apache2 restart
```

Μπορείτε να λαμβάνετε email για ειδοποιήσεις από το ELSA κάνοντας τα εξής βήματα:

εκτελέστε ένα ερώτημα(query)

κάντε κλίκ στο "Result Options"

κάντε κλικ στο "Alert or Schedule"

επιλέξτε τις παραμέτρους σας και κάντε κλικ στο κουμπί Υποβολή(Submit)

How do i configure Bro to send emails?

Επεξεργαστείτε `/opt/bro/etc/broctl.cfg` και ορίστε τα ακόλουθα:

```
MailTo = YourUsername@YourDomain.com
sendmail = /usr/sbin/sendmail
```

'Επειτα ενημερώστε και επανεκκινήστε το Bro:

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
sudo nsm_sensor_ps-restart --only-bro
```

Στη συνέχεια θα πρέπει να αρχίσετε να λαμβάνετε ωριαία emails σύνοψης της σύνδεσης. Αν δεν επιθυμείτε emails με σύνοψη της σύνδεσης, μπορείτε να προσθέσετε τα ακόλουθα στο `broctl.cfg` και να ενημερώσετε και να επανεκκινήσετε το Bro:

```
tracesummary=
```

Αν επιθυμείτε να λαμβάνετε emails για τις ειδοποιήσεις του Bro,θα πρέπει να προσθέσετε το ακόλουθο στο `opt/bro/share/bro/site/local.bro` και να ενημερώσετε/επανεκκινήσετε το Bro όπως και παραπάνω:

```
hook Notice::policy(n: Notice::Info)
            {
            add n$actions[Notice::ACTION_ALARM];
            }
```

How can i get an email alert when my sensor stops seeing traffic?

Αν ρυθμίσατε το OSSEC και το Bro όπως δείχθηκε παραπάνω, θα το κάνουν αυτομάτως για εσάς.

## 4.5 Αλληλεπίδραση με άλλα συστήματα

Πολλές εταιρείες επιθυμούν να λαμβάνουν δεδομένα από το Security Onion και να τα αποστέλλουν σε τρίτους.

How do I send Bro and OSSEC logs to an external syslog collector?

Ρυθμίστε `/etc/syslog-ng/syslog-ng.conf` με νέο destination για να διαβιβάσει την εξωτερική syslog και στην συνέχεια κάντε επανεκκίνηση `syslog-ng`.

How do I send IDS alerts to an external system?

Υπάρχουν δύο επιλογές:

α) επεξεργαστείτε όλα τα αρχεία `/etc/nsm/HOSTNAME-INTERFACE/barnyard2*.conf` σε όλους τους αισθητήρες με μια νέα output ώστε να στέλνει IDS ειδοποιήσεις στα εξωτερικά σας συστήματα και μετά επανεκκινήστε όλα τα barnyard2 instances:

```
sudo nsm_sensor_ps-restart --only-barnyard2
```

ή

β) Στον master server (που εκτελείται το Sguild), ρυθμίστε `/etc/syslog-ng/syslog-ng.conf` με ένα νέο `Source` για να παρακολουθεί `/var/log/nsm/securityonion/sguild.log` για `Alert Received lines` και ένα νέο `destination` για να στέλνουν στο εξωτερικό σας σύστημα και μετά επανεκκινήστε `syslog-ng`. Για να το κάνετε αυτό τροποποιήστε `/etc/syslog-ng/syslog-ng.conf` και προσθέστε τις ακόλουθες γραμμές:

```
# This line specifies where the sguild.log file is located, and informs
syslog-ng to tail the file, the program_override inserts the string
sguil_alert into the string
Source s_sguil { file("/var/log/nsm/securityonion/sguild.log"
program_override("sguil_alert")); };
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
# This line filters on the string “Alert Received”
filter f_sguil { match("Alert Received"); };

# This line tells syslog-ng to send the data read to the IP address of
10.80.4.37, via UDP to port 514
destination d_sguil_udp { udp("10.80.4.37" port(514)); };

# This log section tells syslog-ng how to structure the previous ‘Source /
filter / destination’ and is what actually puts them into play
log {
        Source(s_sguil);
        filter(f_sguil);
        destination(d_sguil_udp);
};
```

## 4.6 Changing IP Addresses

Αν χρειαστεί να ενημερώσετε την διεύθυνση IP του server ή του αισθητήρα σας ώστε να το μετακινήσετε σε μια διαφορετική περιοχή του δικτύου σας, θα πρέπει να κάνετε μερικά πράγματα:

ενημερώστε τα αρχεία NSM config να αποκρίνονται στην νέα διεύθυνση IP

ενημερώστε την πραγματική διεύθυνση IP του interface διαχείρισης

Update the actual IP address of the management interface:

Για να ενημερώσετε την πραγματική IP διεύθυνση έχετε δύο επιλογές:

χειροκίνητη ενημέρωση `/etc/network/interfaces`

εκτελέστε ξανά την `FIRST` φάση της εγκατάστασης("Yes,configure /etc/network/interfaces)

Update NSM config file to reflect the new IP address:

εκτελέστε ξανά την `SECOND` φάση της εγκατάστασης σε όλους τους server/αισθητήρες `(wiping all data and config)`

χειροκίνητα ενημερώστε όλες τις IP διευθύνσεις όπως φαίνεται παρακάτω¨

Files to update when changing the IP address:

Changing Server IP:

- /etc/nsm/HOSTNAME-INTERFACE/http_agent.conf:
- `set SERVER_HOST [SERVER-IP]`
- /etc/nsm/HOSTNAME-INTERFACE/pads_agent.conf:
- `set SERVER_HOST [SERVER-IP]`
- /etc/nsm/HOSTNAME-INTERFACE/pcap_agent.conf:
- `set SERVER_HOST [SERVER-IP]`
- /etc/nsm/HOSTNAME-INTERFACE/sancp_agent.conf:
- `set SERVER_HOST [SERVER-IP]`

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

- /etc/nsm/HOSTNAME-INTERFACE/sensor.conf:
- `SENSOR_SERVER_HOST="[SERVER-IP]"`
- /etc/nsm/HOSTNAME-INTERFACE/snort_agent-N.conf:
- `set SERVER_HOST [SERVER-IP]`
- /etc/nsm/ossec/ossec_agent.conf:
- `set SERVER_HOST [SERVER-IP]`
- /root/.ssh/securityonion_ssh.conf
- `SERVERNAME=[SERVER-IP]`
- etc/elsa_web.conf
- `"pcap_url": "https://[SERVER-IP]/capme"`
- /etc/salt/minion.d/onionsalt.conf
- `master: [SERVER-IP]`

Automating the change of the server IP:

Μπορεί να είστε σε θέση να χρησιμοποιήσετε sed ώστε να ενημερώσετε όλα τα αρχεία ταυτόχρονα χρησιμοποιώντας κάτι σαν αυτό :

```
sudo service nsm stop
sudo sed -i 's|OLD.SERVER.IP.ADDR|NEW.SERVER.IP.ADDR|g' /etc/nsm/*/*agent*
/etc/nsm/*/sensor.conf /root/.ssh/securityonion_ssh.conf
/etc/salt/minion.d/onionsalt.conf /etc/elsa_web.conf
sudo service nsm start
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# 5. Tuning

## 5.1 Managing Alerts

**Επισκόπηση:** Το Security Onion παράγει πολλές πολύτιμες πληροφορίες για εσάς από την στιγμή που θα το συνδέσετε σε μια θύρα TAP ή SPAN. Μεταξύ των καταγραφών του Bro, δεδομένα συνεδρίας από prads, και καταγραφή πακέτων από netsniff-ng έχετε σε πολύ σύντομο χρονικό διάστημα αρκετές πληροφορίες για να εντοπίσετε τους τομείς που σας ενδιαφέρουν και να κάνετε θετικές αλλαγές στην ασφάλειά σας. Ωστόσο η παρακολούθηση της ασφάλειας του Δικτύου ως πρακτική δεν είναι μια λύση που μπορείτε να συνδέετε στο διαδίκτυό σας. Γι αυτόν τον λόγο βεβαιωθείτε ότι βλέπετε τις ενδείξεις των λυχνιών που λένε ότι είστε ασφαλείς. Απαιτείται ενεργή παρέμβαση από έναν αναλυτή ώστε να προσδιορίσει την ποσότητα των πληροφοριών που παρουσιάζονται.

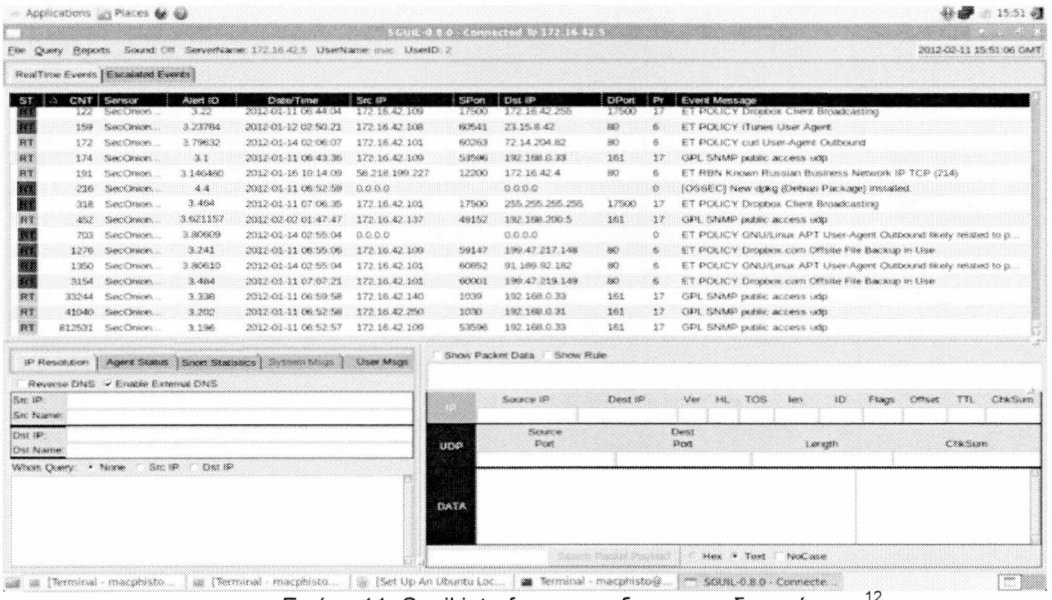
**A)Identifying overly active signatures:** Λόγω του μεγάλου αριθμού των εργαλείων ανάλυσης που είναι διαθέσιμα στο Security Onion, υπάρχουνε πολλοί τρόποι ώστε να δείτε τις signatures που παράγουν πάρα πολλές ειδοποιήσεις. Θα δοθεί έμφαση στον εντοπισμό των ειδοποιήσεων μέσω των Squert, Sguil και της command line.

**From Squert:** Μπορείτε να αποκτήσετε πρόσβαση στο Squert interface μέσω ενός web browser χρησιμοποιώντας το URL https://IP_ADDRESS/squert/. Μπορείτε να συνδεθείτε χρησιμοποιώντας τα ίδια username και password που έχετε στο Sguil. Επιλέξετε στην καρτέλα Summary και στην συνέχεια κοιτάξετε την καρτέλα TOP SIGNATURES .

**From Sguil:** θα χαρακτηριζόταν ως ένα εργοστάσιο παραγωγής ειδοποιήσεων δεδομένου ότι επιτρέπει πιο άμεση αλληλεπίδραση με την βάση δεδομένων που χειρίζεται τις ειδοποιήσεις σας. Συνεπώς μπορείτε να κερδίσετε σαφέστερη εικόνα σχετικά με τις ειδοποιήσεις, τις συναφείς διευθύνσεις IP και τους κανόνες γενικότερα.

Στην παρακάτω εικόνα βλέπετε ότι έχει συνδεθεί στο Sguil interface και επιλέγοντε την στήλη CNT ώστε να ταξινομηθούν οι ειδοποιήσεις κατά αριθμό με τις συσχετιζόμενες ειδοποιήσεις.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79



Εικόνα 11: Squil interface για ταξινομιση ειδοποιήσεων[12]

**From the Command Line:** Αν υπάρχει μεγάλος αριθμός των Uncategorized events στην securityonion_db βάση δεδομένων, το Sguil μπορεί να αντιμετωπίσει δυσκολίες στην διαχείριση του τεράστιου όγκου των δεδομένων που χρειάζεται για να επεξεργαστεί και να παρουσιάσει μια συνολική επισκόπηση των ειδοποιήσεων σε αυτές τις περιπτώσεις. Επίσης μπορεί να είναι χρήσιμο να αναζητήσετε την βάση δεδομένων μέσω της command line. Η αλληλεπίδραση με την βάση δεδομένων MySQL απαιτεί προσοχή. Η επιλογή SELECT στα ερωτήματα μπορεί να μην έχει επιπτώσεις στην βάση δεδομένων, αλλά αν προσπαθήσετε να UPDATE ενώ τα διάφορα εργαλεία στο NSM framework αποκτούν ταυτόχρονα πρόσβαση στην βάση δεδομένων, τότε ενδέχεται να δημιουργηθεί φθορά.

Μπορείτε να αποκτήσετε πρόσβαση στο mysql shell ή να εκδώσετε mysql one-liner's από την command line.Για να εισάγετε το mysql shell, δώστε την ακόλουθη εντολή:

```
mysql -uroot -Dsecurityonion_db
```

Για την έκδοση της commandline one-liners χρησιμοποιήστε το ακόλουθο πρότυπο:

```
mysql -uroot -Dsecurityonion_db -e "QUERY"
```

**Listing the top 20 signatures:** Δίνοντας το ακόλουθο ερώτημα για την mysql θα σας επιστραφεί ένας πίνακας όπως ο κάτωθι: Εδώ ζητάμε το MySQL να επιστρέψει τις στήλες "signature and signature_id" καθώς και μία καταμέτρηση κάθε σειράς που επέστρεψε. Θέλουμε επίσης την έξοδο ομαδοποιημένη με την signature και την καταμέτρηση σε φθίνουσα σειρά.

```
SELECT COUNT(*) AS cnt, signature, signature_id FROM event WHERE status=0
GROUP BY signature ORDER BY cnt DESC LIMIT 20;
```

[12] Πηγή: https://github.com/Security-Onion-Solutions/security-onion/wiki/ManagingAlerts

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

| cnt | signature | signature_id |
|---|---|---|
| 900286 | GPL SNMP public access udp | 2101411 |
| 4709 | ET POLICY Dropbox.com Offsite File Backup in Use | 2012647 |
| 2334 | ET POLICY GNU/Linux APT User-Agent Outbound likely related to package manageme | 2013504 |
| 1169 | GPL SHELLCODE x86 inc ebx NOOP | 1390 |
| 464 | ET POLICY Dropbox Client Broadcasting | 2012648 |
| 343 | ET POLICY iTunes User Agent | 2002878 |
| 270 | ET POLICY Executable served from Amazon S3 | 2013437 |
| 216 | [OSSEC] New dpkg (Debian Package) installed. | 2902 |
| 191 | ET RBN Known Russian Business Network IP TCP (214) | 2406426 |
| 188 | ET POLICY curl User-Agent Outbound | 2013028 |
| 119 | [OSSEC] Integrity checksum changed. | 550 |
| 106 | ET GAMES STEAM Connection (v2) | 2003089 |
| 84 | GPL ICMP_INFO PING *NIX | 2100366 |
| 69 | GPL CHAT MISC Jabber/Google Talk Outgoing Traffic | 100000230 |
| 65 | ET CHAT Google IM traffic Jabber client sign-on | 2002334 |
| 59 | ET CHAT Google Talk (Jabber) Client Login | 2002327 |
| 56 | [OSSEC] Attempt to login using a non-existent user | 5710 |
| 47 | ET SCAN Potential SSH Scan OUTBOUND | 2003068 |
| 44 | ET SCAN Potential SSH Scan | 2001219 |
| 38 | GPL ICMP_INFO PING BSDtype | 2100368 |

20 rows in set (32.65 sec)

Μπορείτε να διακρίνετε ότι η αρχική signature είναι "GPL SNMP public access udp" ειδοποίηση και υπάρχουν πάνω από 900.000 Uncategorized events. Κατά την επεξεργασία αυτών θα επιβραδύνουν την χρήση των εργαλείων κάτι που θα κοστίσει χρόνο στον αναλυτή ο οποίος θα μπορούσε να χρησιμοποιηθεί καλύτερα για την αντιμετώπιση των ειδοποιήσεων μεγαλύτερης σημασίας. Για την καλύτερη αντιμετώπιση πρέπει να διασφαλιστεί ότι αυτές οι ειδοποιήσεις είναι καλοήθεις. Τα μηχανήματα τα οποία είναι χρήσιμα στην λήψη αυτής της απόφασης είναι τα ακόλουθα:

```
SELECT COUNT(*) AS ip_cnt, INET_NTOA(src_ip) FROM event WHERE status=0
AND signature_id=2101411 GROUP BY src_ip ORDER BY ip_cnt DESC;
```

| ip_cnt | INET_NTOA(src_ip) |
|---|---|
| 824459 | 172.16.42.109 |
| 41643 | 172.16.42.250 |
| 33732 | 172.16.42.140 |
| 452 | 172.16.42.137 |

4 rows in set (9.60 sec)

Μπορείτε να συγκεντρώσετε περισσότερες πληροφορίες χρησιμοποιώντας ένα query που επιστρέφει την διεύθυνση IP του προορισμού.

```
SELECT COUNT(*) as ip_cnt, INET_NTOA(src_ip), INET_NTOA(dst_ip) FROM
event WHERE status=0 and signature_id=2101411 GROUP BY dst_ip ORDER BY
ip_cnt DESC;
```

| ip_cnt | INET_NTOA(src_ip) | INET_NTOA(dst_ip) |
|---|---|---|
| 858191 | 172.16.42.109 | 192.168.0.33 |
| 41643 | 172.16.42.250 | 192.168.0.31 |
| 226 | 172.16.42.137 | 192.168.200.5 |
| 226 | 172.16.42.137 | 192.168.200.51 |

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
+--------+------------------+------------------+
4 rows in set (9.65 sec)
```

**Identifying rule categories:** Τόσο το Snort VRT όσο και οι επερχόμενες απειλές έρχονται με ένα μεγάλο αριθμό ενεργοποιημένων κανόνων(άνω των 15.000). Θα πρέπει να εκτελέσετε μόνο τους απαραίτητους κανόνες για το περιβάλλον σας. Γι αυτό μπορεί να θέλετε να απενεργοποιήσετε ολόκληρες κατηγορίες κανόνων που δεν ισχύουν για εσάς. Εκτελέστε την ακόλουθη εντολή για να λάβετε μία λίστα των κατηγοριών και του αριθμού των κανόνων.

```
cut -d\" -f2 /etc/nsm/rules/downloaded.rules | awk '{print $1, $2}'|Sort
|uniq -c |Sort -nr
```

**Β)Επόμενα Βήματα:** Πρώτον στην ρύθμιση του αισθητήρα σας πρέπει να καταλάβετε κατά πόσο η λήψη ή μη διορθωτικών μέτρων στην signature θα ελαττώσει την συνολική στάση της ασφάλειας. Για μερικές ειδοποιήσεις η κατανόηση του δικτύου και οι εργασίες που πραγματοποιούνται θα είναι οι καθοριστικοί παράγοντες. Παραδείγματος χάρη, αν δεν σαν ενδιαφέρει ότι άλλοι χρήστες έχουν πρόσβαση στον λογαριασμό σας στο facebook, μπορείτε να απενεργοποιήσετε τις signatures που θα προκαλέσουν τις αντίστοιχες ειδοποιήσεις. Η υπογραφή SID : 1411 είναι χρήσιμη να βρίσκεται σε ετοιμότητα. Οι επιτιθέμενοι συχνά αναζητούν για ενεργοποιημένες SNMP συσκευές. Σε αυτήν την περίπτωση οι ειδοποιήσεις παράγονται από καλοήθη κυκλοφορία αλλά δεν είναι σίγουρο ότι θα είναι και οι περαιτέρω ειδοποιήσεις.

Μια άλλη παρατήρηση που πρέπει να ληφθεί υπόψη είναι να καθοριστεί εάν η όχι η κίνηση παράγεται από ένα ελαττωματικό κομμάτι του εξοπλισμού. Αν ναι, το αποδοτικότερο μέτρο είναι να ρυθμίσετε σωστά τον εν λόγω εξοπλισμό και να επανεξετάσετε την ρύθμιση.

Υπάρχουν πάρα πολλοί τρόποι να χειριστείτε τις υπερβολικές signatures και θα γίνει μια προσπάθεια για να καλυφθούν όσο το δυνατόν καλύτερα.

**Disable the sid:** Το Security Onion χρησιμοποιεί PulledPork που κατεβάζει signatures κάθε βράδυ και τις επεξεργάζεται σύμφωνα με μια λίστα δημιουργημένων ρυθμίσεων από χρήστες. Σε ένα Server/Slave Securiy Onion περιβάλλον το μόνο που χρειάζεται να αλλαχθεί είναι το αρχείο των ρυθμίσεων του server και το rule-update script που θα συγχρονιστεί με τις signatures από τον server. Όπως αναφέρθηκε προηγουμένως, φροντίστε να απενεργοποιήσετε τις υπογραφές καθώς μία καταλληλότερη απάντηση είναι εξουσιοδοτημένη.

Επεξεργαστείτε το αρχείο ρυθμίσεων disablesid.conf:

```
sudo vi /etc/nsm/pulledpork/disablesid.conf
```

Προσαρτήστε την signature που επιθυμείτε να απενεργοποιήσετε σε μορφή gid:sid. Η ταυτότητα της γεννήτριας πιθανότατα θα είναι "1" στις περισσότερες περιπτώσεις. Μπορείτε να ελέγξετε το αναγνωριστικό της γεννήτριας ελέγχοντας την ακριβή signature. Εάν το gid δεν περιλαμβάνεται στην λίστα, υποτίθεται ότι είναι "1".

```
# Disable the GPL SNMP public access udp signature
    1:2101411
```

Εκτελέστε το rule update στον κύριο server.

```
sudo /usr/bin/rule-update
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Αν τρέχετε salt στην ανάπτυξή σας, τότε το σύνολο των κανόνων θα αντιγραφεί στους αισθητήρες σας αυτόματα εντός 15 λεπτών. Σε διαφορετική περίπτωση μπορείτε να εκτελέσετε τον rule-update στις slave machines.

```
sudo /usr/bin/rule-update
```

**Rewrite the signature:** Μερικές φορές μία Signature είναι γραμμένη πάρα πολύ ευρέως για χρήση σε έναν συγκεκριμένο αισθητήρα. Στην περίπτωση αυτή, μια μικρή επανεγγραφή της signature μπορεί να είναι η λύση. Στο Security Onion, οι τοπικοί κανόνες αποθηκεύονται σε /etc/nsm/rules/local.rules.

Επεξεργαστείτε το αρχείο /etc/nsm/rules/local.rules

```
sudo vi /etc/nsm/rules/local.rules
```

Οι κανόνες του Snort είναι απίστευα ευέλικτοι, όπως φαίνεται:

```
Action Protocol SrcIP SrcPort Direction DestIP DestPort (rule options)
```

Ο κανόνας που παράγει τόσες πολλές ειδοποιήσεις σχετικά με τον αισθητήρα σας:

```
macphisto@SecOnion-Dev:~$ grep -i "GPL SNMP public access udp"
/etc/nsm/rules/downloaded.rules

alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"GPL SNMP public access
udp"; content:"public"; fast_pattern:only; reference:bugtraq,2112;
reference:bugtraq,4088; reference:bugtraq,4089; reference:cve,1999-0517;
reference:cve,2002-0012; reference:cve,2002-0013; classtype:attempted-
recon; sid:2101411; rev:11;)
```

Αρχικά δημιουργείτε κάποιες μεταβλητές σε /etc/nsm/rules/local.rules για να καθορίστεί η κίνηση. Θα ορίσετε μια μεταβλητή, για τους ενεργούς host, που ονομάζεται OVERACTIVE.

```
var OVERACTIVE [192.168.0.31,192.168.0.33,192.168.0.5,192.168.0.51]
```

Μπορείτε να συνδέσετε αυτές τις πληροφορίες στο Snort σε μορφή κανόνα.

```
alert udp $HOME_NET any -> !$OVERACTIVE any (msg:"GPL SNMP public
access udp"; content:"public"; fast_pattern:only; reference:bugtraq,2112;
reference:bugtraq,4088; reference:bugtraq,4089; reference:cve,1999-0517;
reference:cve,2002-0012; reference:cve,2002-0013; classtype:attempted-
recon; sid:9001411; rev:1;)
```

Δίνετε επίσης στην ειδοποίηση ένα μοναδικό id signature (sid) σε εύρος 90.000.000 και αναθεώρηση προς 1.

Τώρα έχετε μία signature που θα δημιουργήσει ειδοποιήσεις λίγο πιο επιλεκτικά και απαιτείται να απενεργοποιήσετε την πρωτότυπη signature. Όπως προαναφέραμε μπορείτε να επεξεργαστείτε το αρχείο disablesid.conf και να προσθέσετε :

```
1:2101411
```

Εκτελέστε μια rule update.

```
sudo /usr/bin/rule-update
```

**modifysid.conf**: Εναλλακτική επιλογή είναι να χρησιμοποιήσετε το modifysid.conf του PulledPork για να εκτελέσετε τα παραπάνω. Επεξεργαστείτε το αρχείο ρυθμίσεων modifysid.conf:

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
sudo vi /etc/nsm/pulledpork/modifysid.conf
```

**Threshold:** Δείτε /etc/nsm/rules/threshold.conf

**Suppressions:** σας επιτρέπει να κάνετε λεπτομερειακές αποφάσεις σχετικά με ορισμένους κανόνες χωρίς να τους ξαναγράφετε. Με αυτήν την λειτουργία μπορείτε να καταστείλετε κανόνες των signatures, την διεύθυνση προέλευσης ή προορισμού, ακόμη και την IP ή CIDR network block. Με αυτόν τον τρόπο εξακολουθείτε να έχετε το βασικό ruleset αλλά οι καταστάσεις στις οποίες προκαλούν ειδοποιήσεις εξαλείφονται. Είναι σημαντικό να σημειωθεί ότι με αυτήν την λειτουργία οι καταστολές που γράφονται δεν θα πρέπει να τερματίζουν τις νόμιμες ειδοποιήσεις.

Σχετικά με το παράδειγμα της απενεργοποίησης του "GPL SNMP public access udp" μπορείτε να οικοδομήσετε έναν κανόνα καταστολής που περιορίζει αυτήν την signature από το να προκαλέσει ειδοποιήσεις σε μηχανήματα στα οποία η συμπεριφορά θεωρείται αποδεκτή. Υπηρεσίες όπως το Nagios παράγουν έναν μεγάλο αριθμό από ειδοποιήσεις. Στο ακόλουθο παράδειγμα θα ενεργοποιηθούν τα ακόλουθα στοιχεία:

Source IP Address 172.16.42.109

Generator ID 1

Signature ID 2101411

Η μορφή για καταστολή είναι πολυ απλή. Παρακάτω είναι η βασική μορφή για έναν καταστολέα με τις διευθετήσιμες περιοχές που σημειώνονται με έντονους χαρακτήρες κειμένου:

suppress gen_id gen-id, sig_id sid-id, track [by_src|by_dst], ip IP/MASK-BITS

Μπορείτε απλά να αντικαταστήσετε τις γνωστές πληροφορίες για τους έντονους χαρακτήρες και να τοποθετήσετε το εξής στο /etc/nsm/rules/threshold.conf :

```
suppress gen_id 1, sig_id 2101411, track by_src, ip 172.16.42.109
```

Μόλις η σωστή καταστολή έχει τοποθετηθεί σε threshold.conf, κάντε επανεκκίνηση την μηχανή ειδοποιήσεων.

```
sudo nsm_sensor_ps-restart --only-snort-alert
```

**Autocategorize events:** Ο Sguild server μπορεί να ρυθμιστεί ώστε να συμβάλλει στην αυτόματη κατηγοριοποίηση των events καθώς τα επεξεργάζεται. Αυτός είναι ένας πολύ καλός τρόπος για να επεξεργάζεται το sguil τα events για εσάς και να γλιτώνετε την επίπονη κατηγοριοποίηση. Τα σύγχρονα Sguil έχουν Autocat builder στο web interface. Για παλαιότερες εκδόσεις του Sguil επεξεργαστείτε: /etc/nsm/securityonion/autocat.conf στον Sguild server.

→ επεξεργαστείτε /etc/nsm/securityonion/autocat.conf. Το αρχείο autocat.conf απαιτεί να χρησιμοποιήσετε την ακόλουθη μορφή για να προσδιορίσετε τα γεγονότα που θέλετε να κατηγοριοποιούνται αυτομάτως.

```
   <erase
time>||<sensorName>||<src_ip>||<src_port>||<dst_ip>||<dst_port>||<proto>||<
sig msg>||<cat value>
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

→ Η τελική τιμή στον κανόνα είναι η τιμή κατηγοριοποίησης. Εδώ είναι ο πίνακας των κατηγοριών:

```
  status_id   description                 long_desc
   ----------+--------------------------+------------------------------
-------------
           0   New                       Real Time Event
           1   No Further Action Required   No Further Action Required
           2   Escalated                 Escalated
          11   Category I                Unauthorized Root Access
          12   Category II               Unauthorized User Access
          13   Category III              Attempted Unauthorized Access
          14   Category IV               Successful Denial of Service
Attack
          15   Category V                Poor Security Practice or
Policy Violation
          16   Category VI               Reconnaissance/Probes/Scans
          17   Category VII              Virus Infection
```

→ Μια καταχώρηση του δείγματος που θα κατηγοριοποιεί αυτόματα όλα τα events που ταιριάζουν "GPL SNMP public access udp" όπως ο τύπος 1 θα είναι ως εξής:

```
   none||ANY||172.16.1.245||ANY||ANY||ANY||17||GPL SNMP public access
udp||1
```

→ Εαν πρόκειται να βάλετε λιγη περισσότερη δουλειά σε αυτό, θα μπορούσατε να χρησιμοποιήσετε την αυτόματη κατηγοριοποίηση και να διατηρήσετε αυτήν την χρήση της signature.

→ Αν επιθυμείτε να έχετε μονο αυτά τα end point conversations να κατηγοριοποιούνται αυτόματα τότε θα έπρεπε να δημιουργήσετε μια καταχώρηση για κάθε ζεύγος src_ip and dst_ip conversations.

```
none||ANY||172.16.42.109||ANY||192.168.0.33||ANY||1||GPL SNMP public access
udp||1
   none||ANY||172.16.42.250||ANY||192.168.0.31||ANY||1||GPL SNMP public
access udp||1
   none||ANY||172.16.42.137||ANY||192.168.0.5||ANY||1||GPL SNMP public
access udp||1
   none||ANY||172.16.42.137||ANY||192.168.0.51||ANY||1||GPL SNMP public
access udp||1
```

→επανεκκίνηση του sguil server.

```
   sudo /usr/sbin/nsm_server_ps-restart
```

Αν η σύνταξή σας είναι σωστή τότε είναι πιθανό να προσπαθείτε να απενεργοποιήσετε έναν κανόνα που έχει θέσει flowbits.

Δείτε τους επόμενους κανόνες :

```
   alert tcp $HOME_NET any -> $EXTERNAL_NET !1433 (msg:"ET POLICY Outbound
MSSQL Connection to Non-Standard Port - Likely Malware";
flow:to_server,established; content:"|12 01 00|"; depth:3; content:"|00 00
00 00 00 00 15 00 06 01 00 1b 00 01 02 00 1c 00|"; distance:1; within:18;
content:"|03 00|"; distance:1; within:2; content:"|00 04 ff 08 00 01 55 00
00 00|"; distance:1; within:10; flowbits:set,ET.MSSQL; classtype:bad-
unknown; sid:2013409; rev:3;)
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 1433 (msg:"ET POLICY Outbound
MSSQL Connection to Standard port (1433)"; flow:to_server,established;
content:"|12 01 00|"; depth:3; content:"|00 00 00 00 00 00 15 00 06 01 00
1b 00 01 02 00 1c 00|"; distance:1; within:18; content:"|03 00|";
distance:1; within:2; content:"|00 04 ff 08 00 01 55 00 00 00|";
distance:1; within:10; flowbits:set,ET.MSSQL; classtype:bad-unknown;
sid:2013410; rev:4;)

   alert tcp $HOME_NET any -> $EXTERNAL_NET !1433 (msg:"ET TROJAN Bancos.DV
MSSQL CnC Connection Outbound"; flow:to_server,established;
flowbits:isset,ET.MSSQL; content:"|49 00 B4 00 4D 00 20 00 54 00 48 00 45
00 20 00 4D 00 41 00 53 00 54 00 45 00 52 00|"; classtype:trojan-activity;
sid:2013411; rev:1;)
```

Αν προσπαθήσετε να απενεργοποιήσετε τους δυο πρώτους rules χωρίς να κάνετε το ίδιο για τον τρίτο τότε ο τρίτος κανόνας δεν θα μπορούσε ποτέ να λειτουργήσει αφού δεν λειτουργούν οι δύο πρώτοι. Το pulledpork πρόθυμα επιλύει όλες τις εξαρτήσεις flowbit και σε αυτήν την περίπτωση είναι κανόνας "εκ νέου ενεργοποίησης". Απενεργοποιώντας τους τρεις από τους κανόνες αυτούς και προθέτοντας τα εξής στο disabledsid.conf έχει αρνητικό αποτέλεσμα.

```
1:2013409
1:2013410
1:2013411
```

'Οταν εκτελείτε sudo rule update, παρακολουθήστε την ενότητα "setting Flowbit State.." όπου μπορείτε να δείτε ότι εάν απενεργοποιήσετε τα τρια, η "Enabled flowbits XX" γραμμή μειώνεται και όλοι οι τρεις κανόνες θα πρέπει στη συνέχεια να απενεργοποιηθούν στο downloaded.rules.

Sguil Days To Keep:

Μπορείτε να ρυθμίσετε την διατήρηση βάσης δεδομένων του Sguil από την επεξεργασία του securityonion.conf και αλλάζοντας την ρύθμιση DAYSTOKEEP(με προεπιλογή 365 μέρες).

```
/etc/nsm/securityonion.conf
```

Μπορείτε επίσης να χρησιμοποιήσετε την ρύθμιση για να εκτελέσετε μια Sguil εκκαθάριση βάσης δεδομένων με την μείωση της μεταβλητής DAYSTOKEEP σε ένα μικρό αριθμό (όπως 7 ή 1 ) και να λειτουργήσει manually:

```
sudo sguil-db-purge
```

## 5.2 Adding Local Rules

**Εισαγωγή:** Η προσθήκη τοπικών κανόνων ασφαλείας στο Security Onion είναι μάλλον μία απλή διαδικασία. Ωστόσο καμιά φορά είναι πρόκληση.

Βήματα:

→ Ανοίγετε το `/etc/nsm/rules/local.rules` χρησιμοποιώντας όποιον επεξεργαστή κειμένου επιθυμείτε:

→ Προσθέσετε έναν απλό κανόνα που θα ειδοποιεί την ανίχνευση μιας συμβολοσειράς σε tcp session.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
alert tcp any any -> $HOME_NET 7789 (msg: "Vote for Security Onion
Toolsmith Tool of 2011!"; reference:
url,http://holisticinfosec.blogspot.com/2011/12/choose-2011-toolsmith-tool-
of-year.html; content: "toolsmith"; flow:to_server; nocase; sid:9000547;
rev:1)
```

→Ενημερώστε `sid-msg.map` και επανεκκινήστε τα Snort/Suricata και barnyard.

```
sudo rule-update
```

→ Αν δημιουργήσετε σωστά τον κανόνα το Snort θα επανέλθει στην λειτουργία του.

→ Δημιουργήστε κάποια κίνηση για την ενεργοποίηση των ειδοποιήσεων. Για την κυκλοφορία χρησιμοποιούμε python library scapy και για επεξεργαστεί τα πακέτα με συγκεκριμένες πληροφορίες ώστε να εξασφαλίσετε την ειδοποίηση με τις πληροφορίες που επιθυμείτε.

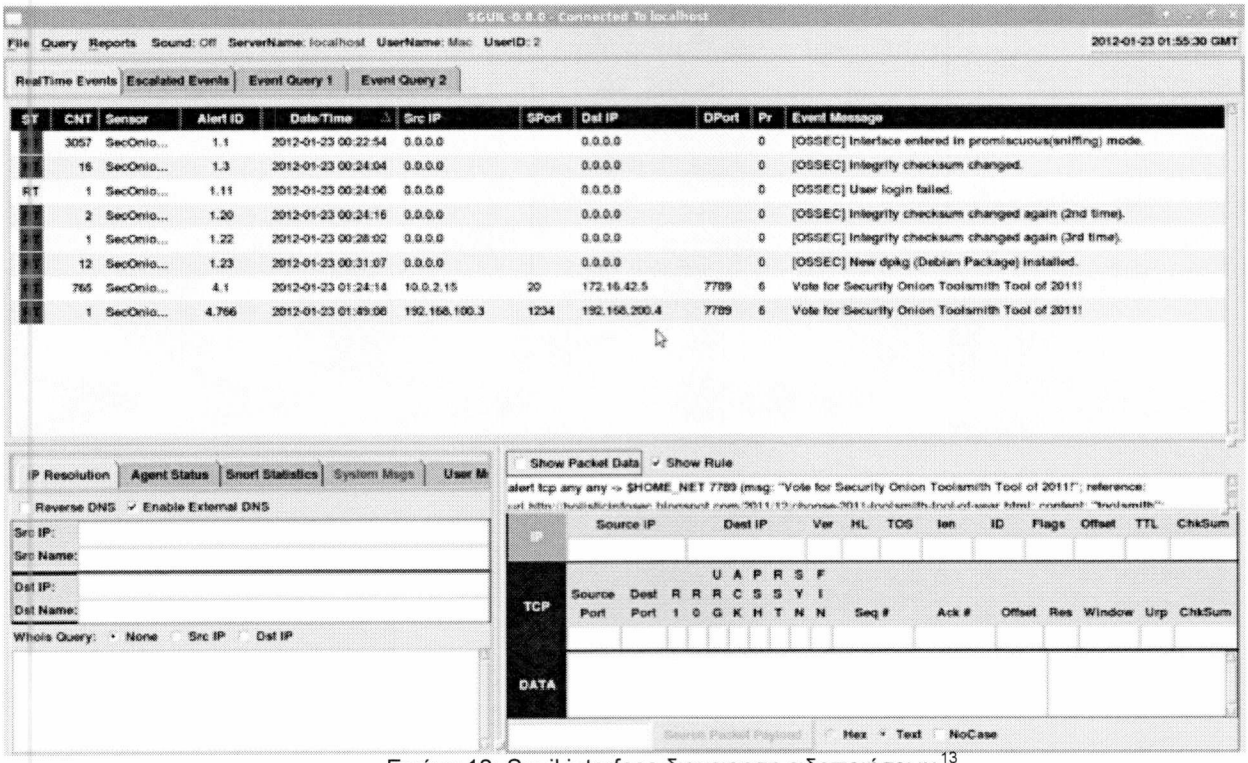
```
sudo scapy
```

→ Εισάγετε το ακόλουθο δείγμα σε μία γραμμή μια φορά. Κάθε γραμμή που ξεκινάει με # μπορεί να αγνοηθεί δεδομένου ότι είναι ένα σχόλιο.

```
# Craft the layer 2 information.
# The ip addresses can be random, but I would suggest sticking to RFC1918
ip = IP()
ip.dst = "192.168.200.4"
ip.src = "192.168.100.3"

# Craft the layer 3 information.
# Since we specified port 7789 in our snort rule,
tcp = TCP()
tcp.dport = 7789
tcp.sport = 1234

# Set the playload
payload = "Toolsmith"

# Use the / operator to compose our packet and transfer it with the send()
method.
send(ip/tcp/payload)
```

→ Ελέγξετε το Sguil για την αντίστοιχη ειδοποίηση.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79



Εικόνα 12: Squil interface διαχειρηση ειδοποιήσεων [13]

→ Μπορείτε να δείτε ότι έχετε μια ειδοποίηση με τις IP adresses και με τις TCP ports που καθορίσατε. Αν επιλέξετε στην στήλη **Alert ID** → "Transcript" θα επαληθεύσετε το payload που στείλατε.

## 5.3 Disabling Processes

**Disabling a process:** Εάν έχετε ήδη εκτελέσει το πρόγραμμα εγκατάστασης και επιθυμείτε να απενεργοποιήσετε μια συγκεκριμένη υπηρεσία του αισθητήρα, μπορείτε απλά να διακόψετε την εκτέλεση της υπηρεσίας και να αλλάξετε την αντίστοιχη τιμή config από "ναι" σε "όχι" ώστε να αποτραπεί η λειτουργία της την επόμενη φορά που τα NSM scripts θα τρέξουν.

Για παράδειγμα, έστω ότι έχετε πρόσβαση στα HTTP logs του Bro μέσω ELSA, και θέλετε να απενεργοποιήσετε το http_agent να αποτρέπει αυτά από το να αντιγράφονται στην βάση δεδομένων του Sguil. Πρώτα θα παύσετε την λειτουργία του http_agent:

```
sudo nsm_sensor_ps-stop --only-http-agent
```

Στην συνέχεια θα επεξεργαστείτε /etc/nsm/$HOSTNAME-$INTERFACE/sensor.conf και θα αλλάξετε:

```
HTTP_AGENT_ENABLED="yes"
```

σε:

```
HTTP_AGENT_ENABLED="no"
```

[13] Πηγή: https://github.com/Security-Onion-Solutions/security-onion/wiki/ManagingAlerts

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

ώστε να αποτρέψετε το http_agent να λειτουργήσει την επόμενη φορά που τα NSM scripts θα τρέξουν. Ένας γρήγορος τρόπος να το κάνετε αυτό για όλα τα αρχεία /etc/nsm/*/sensor.conf είναι να χρησιμοποιήσετε την sed εντολή ώς εξής:

```
sudo sed -i 's|HTTP_AGENT_ENABLED="yes"|HTTP_AGENT_ENABLED="no"|g'
/etc/nsm/*/sensor.conf
```

**Sguil Agent:** Εάν χρησιμοποιείτε το Sguil και θέλετε να καταργήσετε τον agent από την Sguil's Agent Status καρτέλα, τότε διακόψετε την λειτουργία του Sguild, και θέσετε το `active` field του αισθητήρα στο `N` στην βάση δεδομένων και επανεκκίνηστε το `sguild`

```
# Stop sguild
sudo nsm_server_ps-stop

# Set active="N", replacing HOSTNAME-INTERFACE-INSTANCE with your actual
HOSTNAME, INTERFACE, and INSTANCE
mysql -uroot -Dsecurityonion_db -e 'update sensor set active="N" where
hostname="HOSTNAME-INTERFACE-INSTANCE";'

# Restart sguild
sudo nsm_server_ps-start
```

Disabling Snorby:

**1)** Απενεργοποιήστε το Snorby στην Apache configuration:

```
sudo a2dissite snorby
```

**2)** Reload Apache configuration:

```
sudo service apache2 reload
```

**3)** Αποτρέψετε το Snorby worker από την λειτουργία του στο boot θέτοντας `SNORBY_ENABLED=no` στην `/etc/nsm/securityonion.conf`.

**4)** Comment out την έξοδο στην γραμμή της database σε όλα τα `barnyard2.conf` αρχεία σε ΟΛΟΥΣ τους αισθητήρες :

```
sudo sed -i 's|output database: alert, mysql, user=root dbname=snorby
host=127.0.0.1|#output database: alert, mysql, user=root dbname=snorby
host=127.0.0.1|g' /etc/nsm/*/barnyard2*.conf
```

**5)** Επανεκκινήστε το barnyard2 σε όλους τους αισθητήρες:

```
sudo nsm_sensor_ps-restart --only-barnyard2
```

Disabling OSSEC:

Μπορείτε να απενεργοποιήσετε το OSSEC ως εξής:

```
# Stop the running OSSEC processes
sudo service ossec-hids-server stop

sudo update-rc.d -f ossec-hids-server disable
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Ωστόσο να έχετε κατά νου ότι εκτός από την παροχή endpoint visibility από τους OSSSEC agents, ο OSSEC server επίσης παρακολουθεί και προστατεύει το ίδιο το Security Onion. Παραδείγματος χάρην, ας υποθέσουμε ότι έχετε μια ενεργή απειλή που προσπαθεί να παραβιάσει το Security Onion. ΤΟ Ossec μπορεί να αναγνωρίσει αυτές τις προσπάθειες και να ενεργοποιήσει `Active Response` ώστε να μπλοκάρει την IP του επιτεθέμενου στο firewall.

## 5.4 Filtering with BPF

**BPF:** τα αρχικά σημαίνουν Berkeley Packet Filter.

Configuration:

→ **Global bpf.conf** Μπορείτε να καθορίσετε το BPF στο `/etc/nsm/rules/bpf.conf` στον master server και από προεπιλογή θα ισχύει για Snort/Suricata/Bro/netsniff-ng/prads σε όλες τις συνδέσεις. Αν έχετε ξεχωριστούς αισθητήρες που αναφέρουν στον master server, αυτοί θα αντιγράψουν `/etc/nsm/rules/bpf.conf` ως ένα μέρος της καθημερινής rule update cron job η οποία επίσης θα επανεκκινήσει τα Snort/Suricata. Με αυτόν τον τρόπο οι αλλαγές στο BPF θα τεθούν σε ισχύ. Το Bro παρακολουθεί αυτομάτως το bpf.conf για αλλαγές και θα ενημερώσει τον εαυτό του όπως και χρειάζεται. Άλλες υπηρεσίες (όπως prads/netsniff-ng) πρέπει να γίνουν επανεκκίνηση χειροκίνητα ώστε η αλλαγή να τεθεί σε ισχύ.

→ **Granular bpf.conf** Κάθε διαδικασία πρέπει να έχει στο interface τον δικό της φάκελο bpf, αλλά από προεπιλογή τα αρχεία bpf είναι συνδεδεμένα με το interface bpf το οποίο με την σειρά του είναι συνδεδεμένο με την global bpf.conf.

```
lrwxrwxrwx 1 root  root     8 Jan 13 21:47 bpf-bro.conf -> bpf.conf
lrwxrwxrwx 1 root  root    23 Jan 13 21:47 bpf.conf ->
/etc/nsm/rules/bpf.conf
lrwxrwxrwx 1 root  root     8 Jan 13 21:47 bpf-ids.conf -> bpf.conf
lrwxrwxrwx 1 root  root     8 Jan 13 21:47 bpf-pcap.conf -> bpf.conf
lrwxrwxrwx 1 root  root     8 Jan 13 21:47 bpf-prads.conf -> bpf.conf
```

Αν δεν επιθυμείτε οι αισθητήρες να λάβουν το bpf.conf από τον master server και χρειάζεστε να καθορίσετε ένα bpf-interface, μπορείτε απλά να αντικαταστήσετε την default symlink με τα επιθυμητά bpf αρχεία και να επανεκκινήσετε της υπηρεσίες όπως απαιτείται. Για παράδειγμα αν θέλετε να εφαρμόσετε το BPF μόνο για το Snort:

```
# Remove the default Snort BPF symlink
sudo rm bpf-ids.conf
# Create a new Snort BPF file and add your custom BPF
sudo vi bpf-ids.conf
# Restart Snort
sudo nsm_sensor_ps-restart --only-snort-alert
```

→ **Argus:** Επί του παρόντος η διαμόρφωση του Argus δεν προέρχεται από το global bpf.conf. Θα πρέπει να μπορείτε να προσθέσετε το bpf στο `argus.conf` αρχείο στο `/etc/nsm/$HOSTNAME-$INTERFACE/`.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

## 5.5 Ρυθμίζοντας το PF_RING για την κίνηση του δικτύου:

**Εγκατάσταση:** Εάν διαθέτετε πολλαπλούς CPU cores, κατά την εγκατάσταση θα ερωτηθείτε πόσα PF_RING instances επιθυμείτε για Snort/Sucirata (IDS engine processes) και το Bro θα σας ενημερώσει για τις ρυθμίσεις που απαιτούνται.

**Tuning:** Εάν επιθυμείτε να αλλάξετε τον αριθμό των PF_RING instances μετά από την εγκατάσταση μπορείτε να εκτελέσετε τα ακόλουθα βήματα:

Snort/Suricata:

→ Παύση της διαδικασίας αισθητήρα(stop sensor processes)

```
sudo nsm_sensor_ps-stop
```

→ Επεξεργασία `/etc/nsm/$HOSTNAME-$INTERFACE/sensor.conf` και μεταβάλλετε την `IDS_LB_PROCS` στον αριθμό των πυρήνων(cores) που επιθυμείτε.

→ Εκκίνηση της διαδικασίας του αισθητήρα.

```
sudo nsm_sensor_ps-start
```

Αν εκτελείτε το Snort, το σενάριο αυτομάτως δημιουργεί $IDS_LB_PROCS instances του Snort (χρησιμοποιώντας το PF_RING), barnyard και snort_agent.

Αν εκτελείτε το Suricata, το σενάριο αυτομάτως αντιγράφει $IDS_LB_PROCS στο Suricata.yaml και μετά το Suricata χρησιμοποιεί τα PF_RING instances.

Bro:

→ Παύση λειτουργίας του Bro:

```
sudo nsm_sensor_ps-stop --only-bro
```

→ Επεξεργασία του `/opt/bro/etc/node.cfg` και αλλάξετε την μεταβλητή `lb_procs` στον αριθμό των πυρήνων που επιθυμείτε.

→ Εκκίνηση του Bro:

```
sudo nsm_sensor_ps-start --only-bro
```

## 5.6 MySQL Tuning

**mysqltuner:** Εκτελέστε το mysqltuner ώστε να λάβετε μερικές συστάσεις:

```
# Install mysqltuner if you haven't already
sudo apt-get install mysqltuner

# Run mysqltuner
sudo mysqltuner
```

/etc/mysql/my.cnf **vs** `/etc/mysql/conf.d/`

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Εφαρμόστε τις συστάσεις του mysqltuner στο `/etc/mysql/my.cnf` ή δημιουργήστε ένα νέο αρχείο στο `/etc/mysql/conf.d/` μαζί με τις αλλαγές. Προτείνουμε το `/etc/mysql/conf.d/`

ώστε οι αλλαγές να μην χαθούν κατά την διάρκεια του MySQL upgrade.

Επανεκκινήστε το MySQL.

Οι αλλαγές δεν θα τεθούν σε εφαρμογή μέχρι να επανεκκινήσετε το MySQL. Επίσης πρέπει να διασφαλίσετε, ότι το Sguil και άλλες υπηρεσίες δεν λειτουργούν το MySQL, πριν επανεκκινήσετε την λειτουργία του.

Variables:

Η πρώτη μεταβλητή που θα ρυθμίσετε είναι `open-files-limit` error code 24 out-of-resources . Εδώ παραθέτονται μερικές μεταβλητές που ίσως χρειαστεί το σύστημα σας:

table_cache

key_buffer

max_connections

MySQL slow to start on boot:

Κατά την έναρξη το MySQL ελέγχει όλους τους πίνακες κάτι που μπορεί να πάρει χρόνο. Αν επιθυμείτε να απενεργοποιήσετε αυτόν τον έλεγχο αποκλείστε το `check_for_crashed_tables` στο `/etc/mysql/debian-start`

## 5.7 Adding a new disk

Adding a new disk for /nsm

Προτού προβείτε σε αυτήν την ενέργεια, σιγουρευτείτε ότι εργάζεστε σε ένα non production system: Υπάρχουν δύο τρόποι για να το επιτύχετε:

**Μέθοδος 1η**: Ορίστε έναν ξεχωριστό δίσκο στο /nsm. Αυτό μπορεί να επιτευχθεί με Unbuntu installer ή με το πέρας της εγκατάστασης. Αν το κάνετε μετά το πέρας της εγκατάστασης τότε πρέπει να αντιγράψετε τα υπάρχοντα δεδομένα στο /nsm στον νέο δίσκο χρησιμοποιώντας το εξής:

Παύση όλων των υπηρεσιών:

```
sudo service nsm stop
```

Καθορίσετε το νέο drive path:

```
sudo fdisk -l
```

Ορίσετε τον νέο drive σε μία προσωρινή τοποθεσία στο σύστημα φακέλων:

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
sudo mount /dev/sdb2 /mnt
```

Αντιγράψετε τα υπάρχοντα δεδομένα από το /nsm στην προσωρινή τοποθεσία:

```
sudo cp -av /nsm/* /mnt/
```

Αποσυνδέστε το drive από την προσωρινή τοποθεσία:

```
sudo umount /mnt
```

Μετονομάστε το υπάρχονο /nsm:

```
sudo mv /nsm /nsm-backup
```

Ενημερώστε /etc/fstab στο mount στο νέο drive στο /nsm:

```
sudo vi /etc/fstab
```

Μπορείτε να χρησιμοποιήσετε blkid για να βρείτε το UUID του drive σας:

```
sudo blkid /dev/sdb2
```

Ορίσετε το νέο /nsm:

```
sudo mount /nsm
```

Εκκινήστε όλες τις υπηρεσίες:

```
sudo service nsm start
```

**Μέθοδος 2η:** Δημιουργήσετε /nsm symlink σε μία νέα τοποθεσία. Αν το κάνετε αυτό θα χρειαστεί να κάνετε κάτι σαν τα παρακάτω ώστε να αποφύγετε τα θέματα με AppArmor :

Παύση όλων των υπηρεσιών:

```
sudo service nsm stop
```

Αντιγραφή των υπάρχοντων δεδομένων από /nsm σε ένα νέο σημείο mount:

```
sudo cp -av /nsm/* /mnt/nsm
```

Μετονομασία τα υπάρχοντα /nsm:

```
sudo mv /nsm /nsm-backup
```

Δημιουργήστε ένα /nsm symlink στην νέα θέση σύνδεσης:

```
sudo ln -s /mnt/nsm /nsm
```

Εισέρχεστε στο /etc/apparmor.d/local/:

```
cd /etc/apparmor.d/local/
```

Επεξεργαστείτε το `usr.sbin.mysqld` αντιγράψετε τις /nsm σειρές και αλλάξετε /nsm στην νέα τοποθεσία:

```
sudo vi usr.sbin.tcpdump
```

Επανεκκινήστε το apparmor:

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
sudo service apparmor restart
```

Εκκινήστε όλες τις υπηρεσίες:

```
sudo service nsm start
```

## 5.8 Moving the MySQL Databases:

**Σύνοψη:** Παρουσίαση του πώς μπορείτε να μετακινήσετε τις MySQL databases που περιέχουν όλες τις ειδοποιήσεις και τα αρχεία των events σε ένα άλλο μέρος. Θα μετακινήσετε τις databases σε έναν μεγάλο εξωτερικό drive τον οποίο έχετε κάνει mount ως /nsm .

**Διαδικασία:** Οι MySQL databases αποθηκεύονται σε `/var/lib/mysql`. Πρέπει να μετακινήσουμε αυτόν τον φάκελο και τα περιεχόμενα του σε έναν προορισμό. Αρχικά διακόπτουμε όλες τις διαδικασίες που χρησιμοποιούν τις databases:

```
sudo service nsm stop
sudo service mysql stop
sudo service sphinxsearch stop
```

Τώρα αντιγράφουμε τα δεδομένα στην νέα τοποθεσία αφήνοντας τα αυθεντικά ανεπηρέαστα. Μπορείτε να χρησιμοποιήσετε cp ή rsync ή παρόμοια εργαλεία. Σιγουρευτείτε ότι διατηρείτε permissions(-p) και αντιγράφετε αναδρομικά (-r).

Παρακάτω δίδονται παραδείγματα:

επιλέξετε ένα

```
sudo cp -rp /var/lib/mysql /nsm
sudo rsync -avpr var/lib/mysql /nsm
```

Μετά επονομάστε ή κάντε backup το αυθεντικό σε περίπτωση που κάτι πάει στραβά.

```
sudo mv /var/lib/mysql /var/lib/mysql.bak
```

Στο επόμενο βήμα δημιουργείστε ένα συμβολικό link από `/var/lib/mysql` στη νέα τοποθεσία:

```
sudo ln -s /nsm/mysql /var/lib/mysql
```

Τα Ubuntu χρησιμοποιούν το AppArmor για επιπλέον προστασία στις εφαρμογές. Πρέπει να ενημερώσετε το apparmor σχετικά με τις νέες mysql databases αλλιώς θα αποτρέψει το σύστημα από το να τις χρησιμοποιήσει.

```
sudo service apparmor stop
```

Επεξεργαστείτε `/etc/apparmor.d/usr.sbin.mysqld` ώστε να προσθέσετε την νέα τοποθεσία:

```
sudo vim /etc/apparmor.d/usr.sbin.mysqld
```

```
--- a/apparmor.d/usr.sbin.mysqld
+++ b/apparmor.d/usr.sbin.mysqld
@@ -19,8 +19,8 @@

/etc/hosts.allow r,
/etc/hosts.deny r,
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
+  /nsm/mysql/ r,
+  /nsm/mysql/** rwk,
+  /nsm/elsa/data/mysql/ r,
+  /nsm/elsa/data/mysql/** rwk,
/etc/mysql/*.pem r,
/etc/mysql/conf.d/ r,
/etc/mysql/conf.d/* r,
```

Τελικώς , ξεκινήστε την διαδικασία:

```
sudo service apparmor start
sudo service mysql start
sudo service sphinxsearch start
sudo service nsm start
```

# 6. Tricks and Tips

## 6.1 Βέλτιστες Πρακτικές

Το Security Onion 14.04 έρχεται με την επιλογή να εφαρμόσει αυτό που θεωρεί ώς ένα σύνολο από βέλτιστες πρακτικές κατά την διάρκεια της εγκατάστασης. Για πολλούς χρήστες είναι ένας γρήγορος και εύκολος τρόπος να διασφαλίσουν ότι διαμορφώνονται οι ρυθμίσεις ώστε να απενεργοποιήσουν όλες τις υπηρεσίες που πιθανώς δεν χρειάζονται ή που θα διπλασίαζαν την δουλειά και τα δεδομένα. Η επιλογή Βέλτιστων Πρακτικών όχι μόνο απενεργοποιεί τις περιττές υπηρεσίες αλλά και ενεργοποιεί το Salt ώστε να επιτρέψει την ευκολία διαχείρισης του αισθητήρα.

Στις παρακάτω ενότητες θεωρείτε ότι έχετε ήδη εγκαταστήσει αυτές τις υπηρεσίες και οπότε γίνετε μια αναφορά σε χρήσιμες συμβουλές σχετικά με το πώς θα τις απενεργοποιήσετε. Απενεργοποιήστε οποιεσδήποτε μη-χρήσιμες υπηρεσίες.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Στην Συνέχεια οι περισσότεροι χρήστες θα επιθυμείτε να απενεργοποιήσετε τις εξείς υπηρεσίες:

prads (prads δημιουργεί session data και asset data, τα οποία ήδη παρέχονται από το Bro)

pads_agent (δεν χρειάζονται αν τα prads είναι απενεργοποιημένα)

sancp_agent (δεν χρειάζονται αν τα prads είναι απενεργοποιημένα)

argus (argus δημιουργεί session data, τα οποία ήδη παρέχονται από το Bro)

http_agent (αντιγράφει Bro http.log στην Sguil database, το οποίο μπορεί να προκαλέσει θέματα στην απόδοση)

Για να το επιτύχετε,διακόψετε τις υπηρεσίες¨

```
sudo nsm_sensor_ps-stop --only-prads
sudo nsm_sensor_ps-stop --only-pads-agent
sudo nsm_sensor_ps-stop --only-sancp-agent
sudo nsm_sensor_ps-stop --only-argus
sudo nsm_sensor_ps-stop --only-http-agent
```

Και στην συνέχεια απενεργοποιήστε τις ώστε να μην ξεκινήσουν στο boot:

```
sudo sed -i 's|PRADS_ENABLED="yes"|PRADS_ENABLED="no"|g'
/etc/nsm/*/sensor.conf
sudo sed -i 's|PADS_AGENT_ENABLED="yes"|PADS_AGENT_ENABLED="no"|g'
/etc/nsm/*/sensor.conf
sudo sed -i 's|SANCP_AGENT_ENABLED="yes"|SANCP_AGENT_ENABLED="no"|g'
/etc/nsm/*/sensor.conf
sudo sed -i 's|ARGUS_ENABLED="yes"|ARGUS_ENABLED="no"|g'
/etc/nsm/*/sensor.conf
sudo sed -i 's|HTTP_AGENT_ENABLED="yes"|HTTP_AGENT_ENABLED="no"|g'
/etc/nsm/*/sensor.conf
```

## 6.2 Using Salt to manage sensors:

**Salt:** Το Salt είναι ένα εργαλείο σχεδιασμένο για να χειρίζεται πολλαπλούς αισθητήρες του Security Onion.

Best Practices:

```
securityonion-iso syslog-ng-core
```

Για το Security Onion 14.04 ISO, `securityonion-onionsalt` είναι προεγκατεστημένο (μέσω `securityonion-iso syslog-ng-core`) και το Salt είναι ρυθμισμένο από προεπιλογή όταν επιλέγετε Best Practices κατά την διάρκεια της εγκατάστασης.

Salt and OnionSalt are optional packages:

```
securityonion-all syslog-ng-core
```

Αν επιλέξετε να εγκαταστήσετε το Security Onion μέσω PPA χωρίς να εγκαταστήσετε `securityonion-iso syslog-ng-core` να έχετε υπόψη ότι το Salt είναι εντελώς προαιρετικό. Αν είστε ευχαριστημένοι με την τρέχουσα κατάσταση διαχείρισης του αισθητήρα, τότε δεν υπάρχει λόγος να εγκαταστήσετε το `securityonion-onionsalt` και τίποτα δεν θα αλλάξει για εσάς. Σε αντίθετη

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ ΒΙΒΛΙΟΘΗΚΗ

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

περίπτωση εγκαταστήσετε το `securityonion-onionsalt` προτού ξεκινήσετε την εγκατάσταση ώστε να ενεργοποιήσετε το Salt για την ανάπτυξή σας.

**Προσοχή** Σας ενημερώνουμε ότι η ενσωμάτωση του Salt θεωρείται ακόμη πειραματική.

**Firewall Requirements:** Οι αισθητήρες πρέπει να είναι ικανοί να συνδέονται με τον master server στις θύρες 4505/tcp και 4506/tcp.

**Installation:** Για λιγότερο έμπειρους η Best Practices ελέγχει να δει εάν `securityonion-onionsalt` πακέτα είναι εγκατεστημένα και αν είναι, ενεργοποιεί το Salt από προεπιλογή. Αν επιλέξετε "Custom" ρυθμίσεις απλώς απαντήστε "Ναι" στην υπενθύμιση και η εγκατάσταση θα ρυθμίσει τις salt-master και salt-minion υπηρεσίες και θα ανοίξει τις firewall ports όπως χρειάζονται.

**Checking Status:** Εάν επιθυμείτε να πιστοποιήσετε ότι όλοι οι αισθητήρες λειτουργούν:

```
sudo salt '*' test.ping
```

**Remote Execution:** Εάν επιθυμείτε να χειρίζεστε όλους τους αισθητήρες σας ταυτόχρονα:

```
sudo salt '*' cmd.run 'InsertYourCommandHere'
```

**Features:** Μόλις εγκαταστήσετε και ενεργοποιήσετε το security-onion salt, τα επόμενα δεδομένα θα αντιγραφούν από τον master server στους αισθητήρες κάθε 15 λεπτά.

**Using Salt to Install Updates Across Your Entire Deployment:** Μπορείτε να χρησιμοποιήσετε το Salt και το Soup για να εγκαταστήσετε ενημερώσεις (updates) σε ολόκληρη την ανάπτυξή σας, αλλά θυμηθείτε να ενημερώσετε πρώτα τον master server:

```
# Update Master first
# If MySQL and/or kernel updates are installed, it will reboot
sudo soup -y

# After Master server is fully updated, now update the rest of the
deployment
# If MySQL and/or kernel updates are installed, the sensors will reboot
sudo salt '*' cmd.run 'soup -y'
```

## 6.3 Automating Setup

Μπορείτε να αυτοματοποιήσετε την εγκατάσταση χρησιμοποιώντας sosetup.conf.

Αντιγράψετε το παράδειγμα στο σύστημά σας:

```
cp /usr/share/securityonion/sosetup.conf ~
```

Επεξεργαστείτε το νέο sosetup.conf χρησιμοποιώντας nano στον αγαπημένο σας text editor:

```
nano ~/sosetup.conf
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Εκκινήστε την εγκατάσταση με το -f switch και την διαδρομή του αρχείου:

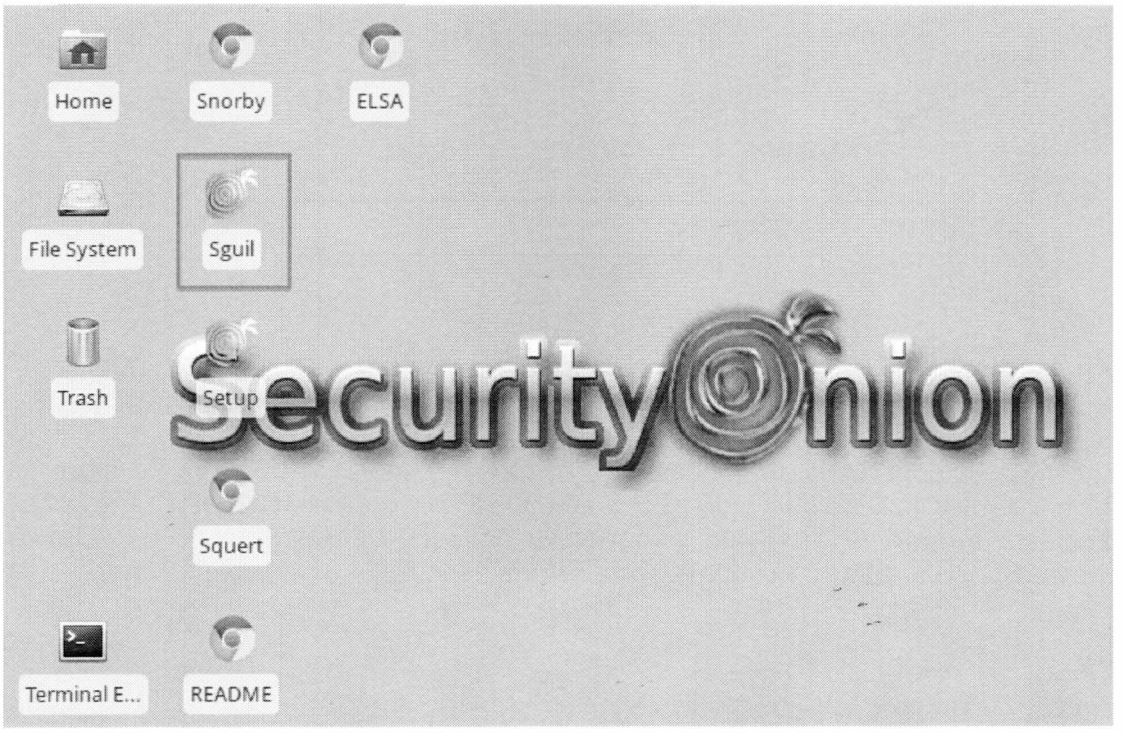
```
sudo sosetup -f ~/sosetup.conf
```

## 6.4 Connecting to Sguild

**Εισαγωγή**: Δείτε πώς να συνδεθείτε με τον Sguil server για να παρακολουθείτε ειδοποιήσεις ασφάλειας σε πραγματικό χρόνο.

Σύνδεση στο Sguil:

Επιλέξετε το εικονίδιο Sguil στην επιφάνεια εργασίας σας στο server του Security Onion:




Στην συνέχεια επιλέξετε ποιους αισθητήρες επιθυμείτε να παρακολουθείτε και επιλέξετε Έναρξη.

Connect Remotely via SSH w/ X11 Forwarding:

Αυτή η μέθοδος απαιτεί SSH και X11 server εγκατεστημένο στην μηχανή από την οποία θα συνδεθείτε.

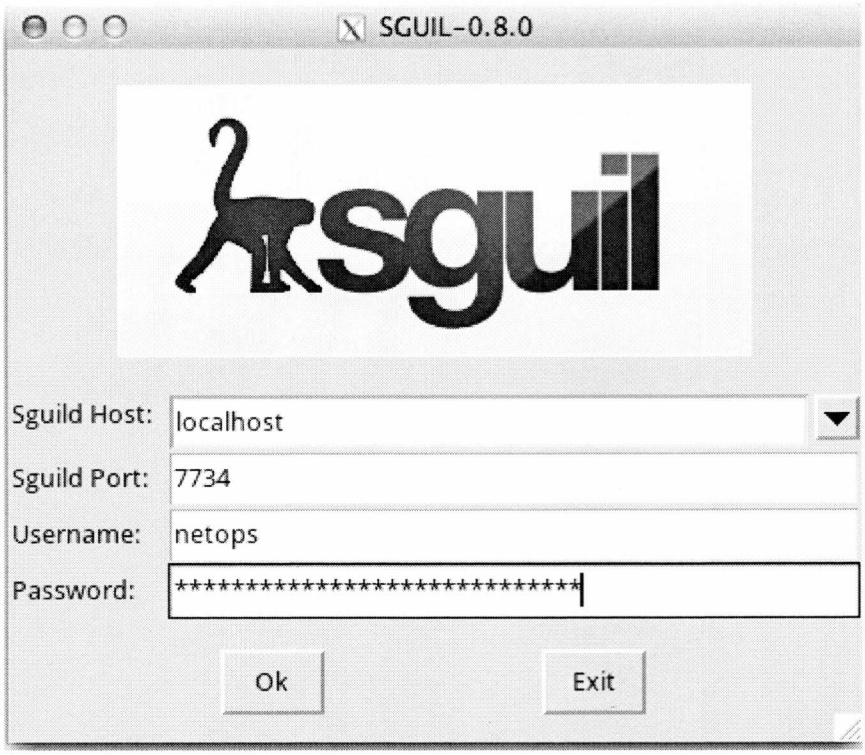
Αν χρησιμοποιήτε OSX εγκαταστήσετε το XQuartz package, Windows δοκιμάστε ciXwin, Linux και BSD δοκιμάστε Xorg. Συνδεθείτε στο server του Security Onion μέσω SSH περνώντας την επιλογή προώθησης X11 (-X).

```
ssh -X user@nsm
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Μόλις συνδεθείτε ως απλός χρήστης ανοίξετε την εφαρμογή sguil client. Η εικόνα θα σταλθεί στο μηχάνημα σας χρησιμοποιώντας το πρωτόκολλο X11 πάνω από το SSH.

```
sguil.tk
```



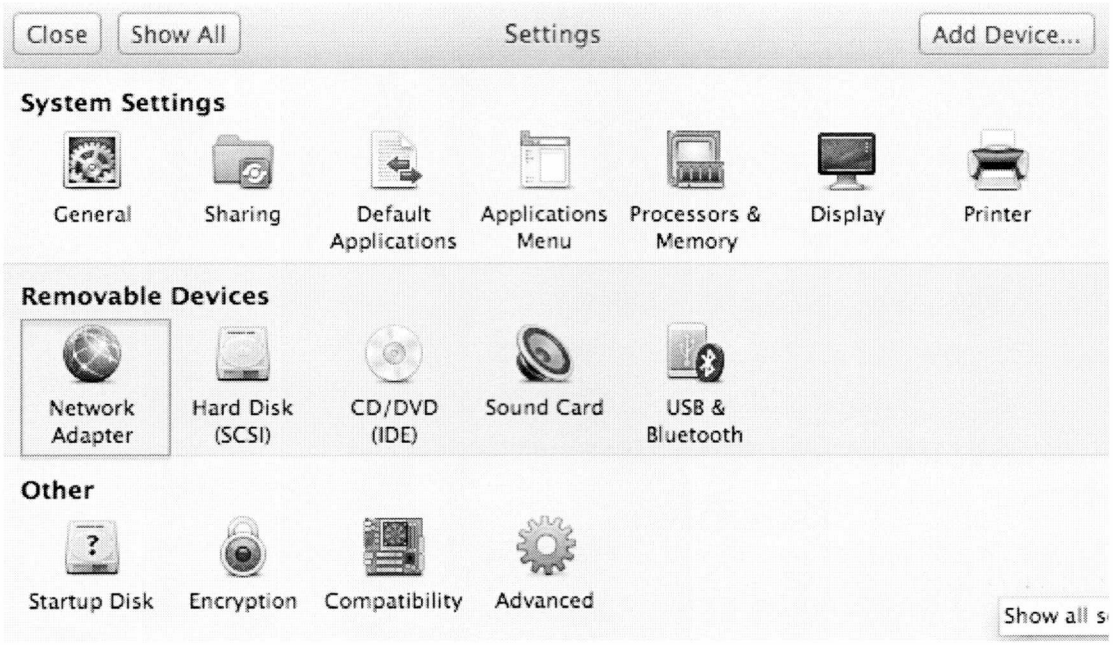

Σας παραθέτουμε μόνο το window της εφαρμογής. Μόλις συνδεθείτε θα είστε σε θέση να επιλέξετε ποιους αισθητήρες επιθυμείτε να παρακολουθήσετε. Στο τέλος επιλέξετε Έναρξη Sguil. Τώρα μπορείτε να δείτε τις ειδοποιήσεις σε πραγματικό χρόνο, SQL ερωτήματα ,εφαρμογές όπως Wireshark, ELSA και Network Minor.

Directly Connecting to Sguild Remotely

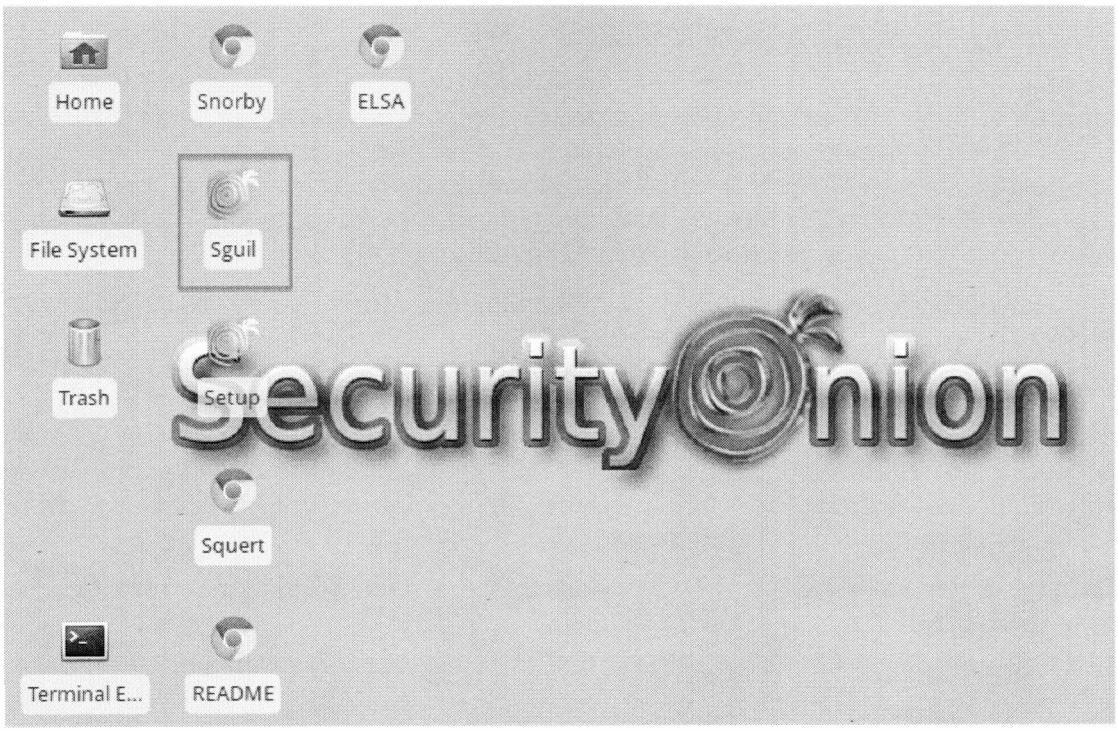
Για να συνδεθείτε απευθείας με ένα Sguil Server πρέπει να διαθέτετε έναν ενεργό Sguil client. Το Sguil ίσως να μην είναι εύκολο ή διαθέσιμο για εγκατάσταση σε ορισμένα λειτουργικά συστήματα. Σας συστήνουμε την εικονική εγκατάσταση του Security Onion στην μηχανή σας και την χρήση του για την σύνδεση με το Sguil. Στο παρακάτω παράδειγμα θα χρησιμοποιήσετε VMware Fusion on OSX.

Εγκαταστήσετε το Security Onion σε μία εικονική μηχανή και ρυθμίσετε τον προσαρμογέα δικτύου για να χρησιμοποιήσει την λειτουργία NAT(πιο εύκολος) με την μετάβαση στις VM ρυθμίσεις σας. Αυτό θα λειτουργήσει αν έχετε για κάθε IP/host ACL την ίδια IP adress που θα χρησιμοποιηθεί.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79




Τώρα επιλέξετε το εικονίδιο Sguil για να εκκινήσετε το Sguil client:




Συμπληρώστε την IP address ή DNS name του Security Onion server και εφαρμόστε τα πιστοποιητικά σας. Τέλος επιλέξτε τους αισθητήρες που επιθυμείτε να παρακολουθείτε και εκκινήστε το Sguil.

## 6.5 Pcaps for Testing

**/opt/samples/:** Το Security Onion περιέχει πολλά pcap δείγματα στο `/opt/samples/`

http://www.malware-traffic-analysis.net/

http://digitalcorpora.org/corpora/network-packet-dumps

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

https://www.openpacket.org/ (Security Onion 12.04 contains some pcaps from openpacket.org. You can find them at `/opt/samples/`.)

http://www.netresec.com/?page=PcapFiles

http://old.honeynet.org/scans/

http://www.novell.com/connectionmagazine/laurachappell.html

http://cctf.shmoo.com/

http://ee.lbl.gov/anonymized-traces.html

https://www.openpacket.org/post/showthread/49

https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Public_Data_Sets

http://wiki.wireshark.org/SampleCaptures#Sample_Captures

http://forensicscontest.com/puzzles

https://www.evilfingers.com/repository/pcaps.php

https://www.openpacket.org/capture

http://www.honeynet.org/node/504

https://github.com/markofu/hackeire/tree/master/2011/pcap

http://www.defcon.org/html/links/dc-ctf.html

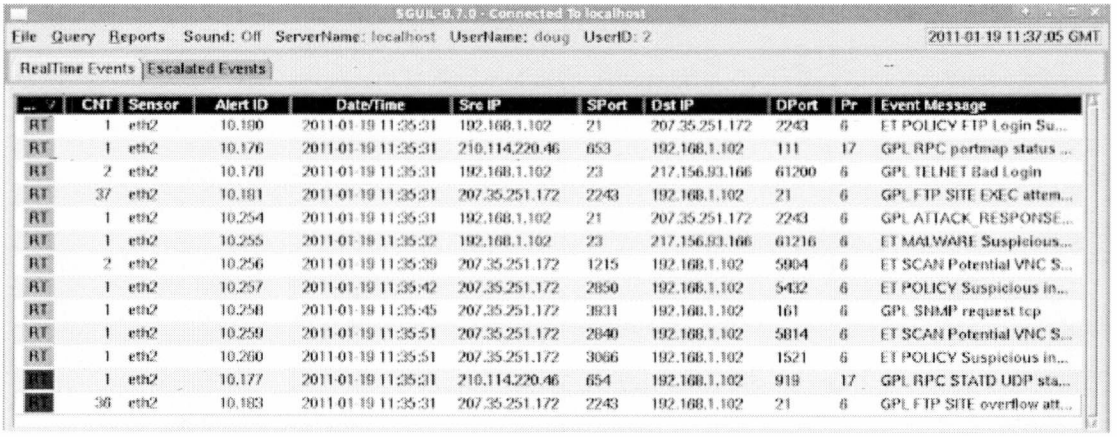
**tcpreplay:** Μπορείτε να χρησιμοποιήσετε το tcpreplay σε οποιοδήποτε από αυτά τα pcaps στον αισθητήρα του Security Onion. Η δυνατότητα του Sguil είναι να λάβει ειδοποίηση και να ξεκινήσει μια πλήρης διαδικασία αντιγραφής. Με τον τρόπο αυτό όχι μόνο βλέπουμε την κίνηση που προκάλεσε την ειδοποίηση αλλά και την κυκλοφορία που έλαβε χώρα πριν και μετά την ειδοποίηση.

Παραδείγματος χάρην: Κατεβάστε : "Scan of the Month 19" από το Honeynet Project.

Εντοπίστε το tar zxvf scan19.tar.gz

Αν δεν το έχετε κάνει ήδη, συνδεθείτε στο Sguil έτσι ώστε να είστε σε θέση να δείτε τις ειδοποιήσεις καθώς δημιουργούνται. Τώρα χρησιμοποιήστε το tcpreplay για να επαναλάβει newdat3.log στο eth0 interface. (ίσως χρειαστείτε άλλο interface, απλά βεβαιωθείτε ότι παρακολουθείται από το Sguil.)

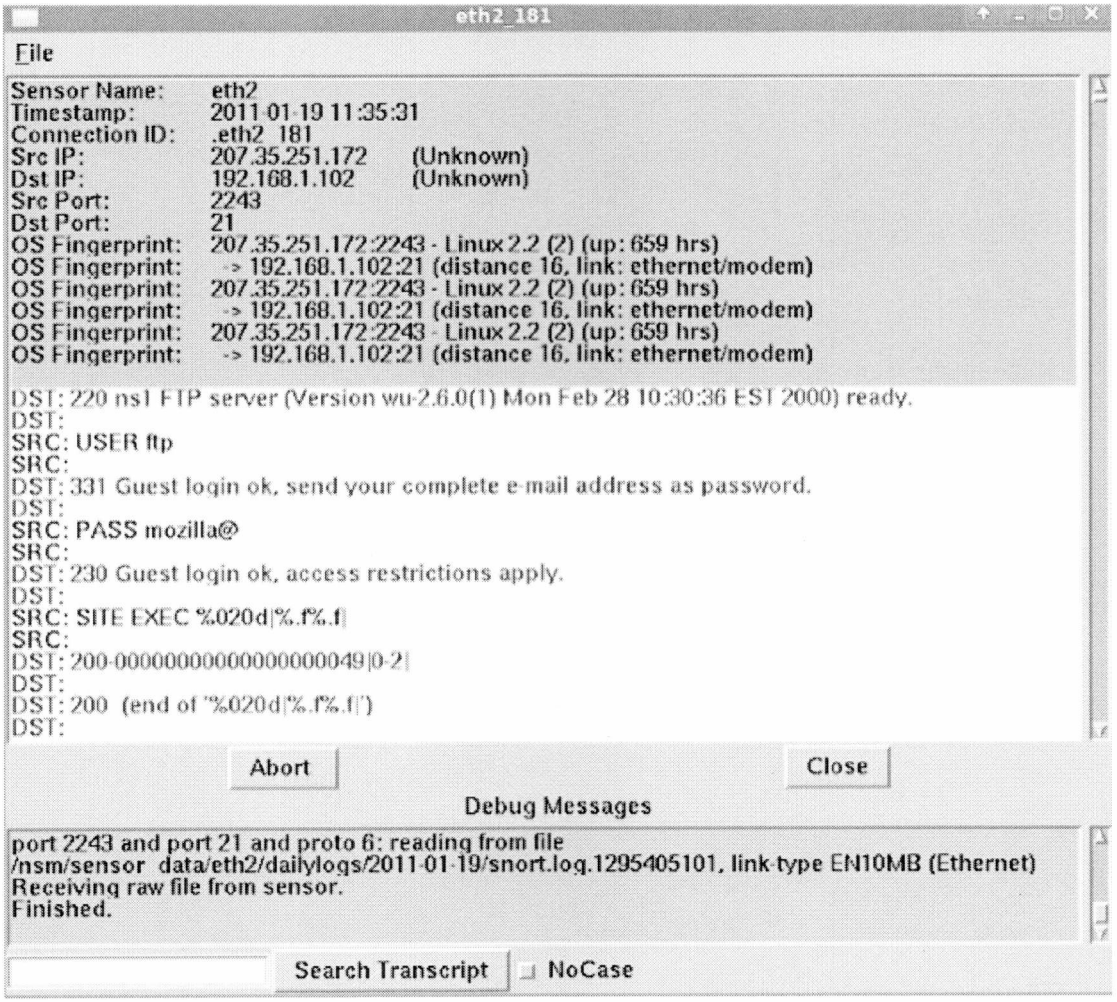
Πατήστε Enter και επιλέξετε την Sguil console ώστε να βλέπετε ειδοποιήσεις. Θα δείτε το εξής:




| ... | CNT | Sensor | Alert ID | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|---|---|---|---|---|---|---|---|---|---|---|
| RT | 1 | eth2 | 10.190 | 2011-01-19 11:35:31 | 192.168.1.102 | 21 | 207.35.251.172 | 2243 | 6 | ET POLICY FTP Login Su... |
| RT | 1 | eth2 | 10.176 | 2011-01-19 11:35:31 | 210.114.220.46 | 653 | 192.168.1.102 | 111 | 17 | GPL RPC portmap status ... |
| RT | 2 | eth2 | 10.178 | 2011-01-19 11:35:31 | 192.168.1.102 | 23 | 217.156.93.166 | 61200 | 6 | GPL TELNET Bad Login |
| RT | 37 | eth2 | 10.181 | 2011-01-19 11:35:31 | 207.35.251.172 | 2243 | 192.168.1.102 | 21 | 6 | GPL FTP SITE EXEC attem... |
| RT | 1 | eth2 | 10.254 | 2011-01-19 11:35:31 | 192.168.1.102 | 21 | 207.35.251.172 | 2243 | 6 | GPL ATTACK_RESPONSE... |
| RT | 1 | eth2 | 10.255 | 2011-01-19 11:35:32 | 192.168.1.102 | 23 | 217.156.93.166 | 61216 | 6 | ET MALWARE Suspicious... |
| RT | 2 | eth2 | 10.256 | 2011-01-19 11:35:39 | 207.35.251.172 | 1215 | 192.168.1.102 | 5904 | 6 | ET SCAN Potential VNC S... |
| RT | 1 | eth2 | 10.257 | 2011-01-19 11:35:42 | 207.35.251.172 | 2850 | 192.168.1.102 | 5432 | 6 | ET POLICY Suspicious in... |
| RT | 1 | eth2 | 10.258 | 2011-01-19 11:35:45 | 207.35.251.172 | 3931 | 192.168.1.102 | 161 | 6 | GPL SNMP request tcp |
| RT | 1 | eth2 | 10.259 | 2011-01-19 11:35:51 | 207.35.251.172 | 2840 | 192.168.1.102 | 5814 | 6 | ET SCAN Potential VNC S... |
| RT | 1 | eth2 | 10.260 | 2011-01-19 11:35:51 | 207.35.251.172 | 3066 | 192.168.1.102 | 1521 | 6 | ET POLICY Suspicious in... |
| RT | 1 | eth2 | 10.177 | 2011-01-19 11:35:31 | 210.114.220.46 | 654 | 192.168.1.102 | 919 | 17 | GPL RPC STATD UDP sta... |
| RT | 36 | eth2 | 10.183 | 2011-01-19 11:35:31 | 207.35.251.172 | 2243 | 192.168.1.102 | 21 | 6 | GPL FTP SITE overflow att... |

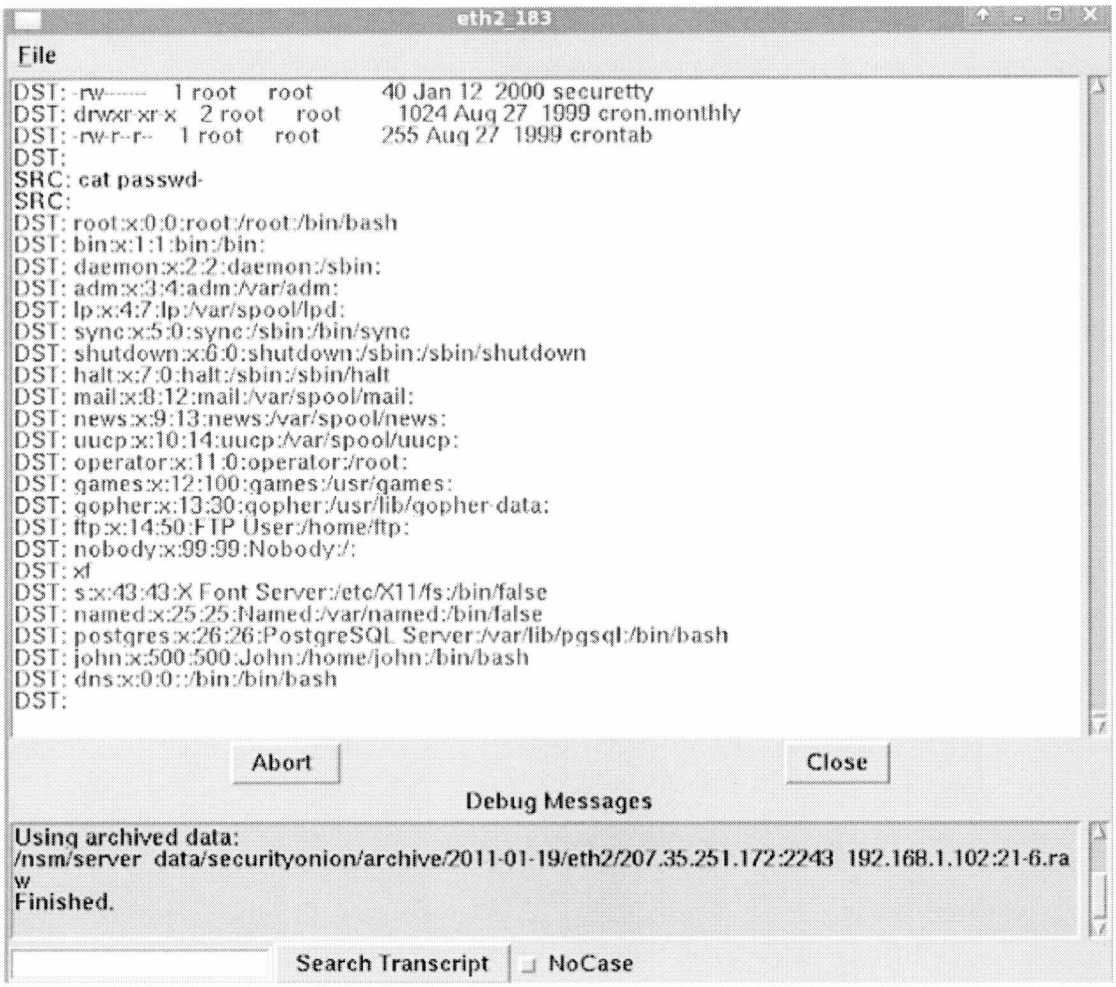
Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Μεταβείτε στο "GPL FTP SITE...",events κάντε δεξί κλικ στο Alert ID και επιλέξετε Transcript A. Ένα νέο παράθυρο αναδύεται:




Ίσως χρειαστούν μερικά δευτερόλεπτα για ολόκληρο το transcript. Τότε θα δείτε ολόκληρη την επίθεση FTP από την buffer overflow στον εισβολέα και στην κοπή του password αρχείου

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79




## 6.6 Removing a Sensor

Παρακάτω θα δείτε τα βήματα που ακολουθούμε σε περίπτωση που θέλουμε να απενεργοποιήσουμε το interface ενός αισθητήρα, διαγραφή των ρυθμίσεων ενός αισθητήρα ή να ξεφορτωθούμε έναν αισθητήρα και όλα του τα δεδομένα.

Disable sensor interface:

Για να απενεργοποιήσετε το interface ενός αισθητήρα απλά απαλείφετε την λέξη interface στο `/etc/nsm/sensortab` και στο `/opt/bro/etc/node.cfg`

Επανεκκινήστε τις NSM services `sudo service nsm restart` και/ή κάνετε επανεκκίνηση τον υπολογιστή ώστε οι αλλαγές να ισχύουν.

Delete Sensor configuration:

Εκτελέστε το `/usr/sbin/nsm_sensor_del` στο sensor box στο οποίο επιθυμείτε να διαγράψετε τις ρυθμίσεις.

Wipe sensor configuration and data:

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Για να εξαλείψετε πλήρως τις ρυθμίσεις του αισθητήρα και των δεδομένων, εκτελέστε `/usr/bin/sosetup` στο sensor box για το οποίο επιθυμείτε να διαγράψετε τα δεδομένα και τις ρυθμίσεις.

Remove sensor reference from master server:

Στον master server επεξεργαστείτε `/etc/elsa_web.conf`, αφαιρέστε τον αισθητήρα από τα peers και επανεκκινήστε την υπηρεσία Apache ( `sudo service apache2 restart` )

Στην MySQL database securityonion_db,επεξεργαστείτε τον πίνακα με τους αισθητήρες (απλά θέτετε το active='N') και επανεκκινήστε το sguild.

→ Παύση του Sguild

sudo nsm_server_ps-stop

→ Εμφάνιστε τις εισόδους των αισθητήρων

mysql -uroot -Dsecurityonion_db -e 'select * from sensor';

→ Ρυθμίστε τον αισθητήρα ως ανενεργό

mysql -uroot -Dsecurityonion_db -e "update sensor set active='N' where sid in (<SID1>,<SID2>)";

→ Εκκινήστε το Sguild

sudo nsm_server_ps-start

Αν εκτελείτε το Salt, αφαιρέστε τον αισθητήρα από `/opt/onionsalt/salt/top.sls`.

## 6.7 Airgapped Networks

Ορισμένες οργανώσεις έχουν airgapped networks χωρίς σύνδεση στο Internet. Το Security Onion δουλεύει άψογα σε αυτά τα δίκτυα ωστόσο χάνει μερικές ενημερώσεις λόγω της έλλειψης του Internet. Υπάρχουν μία σειρά απο σενάρια για να βοηθήσουν στην ενημέρωση της εγκατάστασης airgapped Security Onion.

**Σκοπός:** Είναι να χειριστείτε την ανάπτυξη του Security Onion μέσα σε ένα air gapped network.

Considerations:

1)Snort:

Snort Rule ενημερώσεις. Το Security onion έρχεται με ένα παλιό σετ κανόνων. Είναι όμως προορισμένο να ενημερωθεί κατά την διάρκεια sosetup και μετά από cron job.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Χρησιμοποιώντας άλλους κανόνες. Οταν το Security onion IDS είναι ρυθμισμένο σε offline mode, η ενημέρωση των κανόνων γίνεται βάση των emerging threats.

2)SQueRT:

ip2c updates: το SQueRT αναγνωρίζει μόνο τις RFC1918 addresses, Όταν εκτελείται το sosetup, οι updates γίνονται από Regional Internet Registries και προστίθενται στο securityonion_db.ip2c MySQL πίνακα. Έπειτα ενημερώνεται από το cron job.

3)Bro:

GeoIP updates. Το Bro βασίζεται στα δεδομένα αρχείων GeoIP και αναθέτει κωδικούς χωρών στις log καταχωρήσεις. Το Security Onion χρησιμοποιεί παλαιότερες εκδόσεις του GeoIP.dat και GeoIPv6.dat. Δεν χρησιμοποιεί GeoIPCity.dat.

4)Ubuntu:

OS updates. Ενημερώνεται από aptget/soup.

Components:

1) Online Downloader( securityonion_airgap_download.py)

χειρίζεται την διαδικασία του download και τα updates των packaging

απαιτεί BeautifulSoup4 Python library.

απαιτεί αιτήματα από Python library

2) Offline Updater:

χειρίζεται την decompressing tarball από τον downloader και περνάει switches σε sub-script updaters.

i) SQueRT Updater(squert_ip2c_update.py)

απαιτεί mysql.connector Python Librar

απαιτεί MySQL root(SELECT,DROP,CREATE,INSERT,LOAD) αλλά όχι OS root

Master server μόνο

Βασισμένο σε ip2.tcl και squert.sql σε /var/www/so/squert/.scripts/

ii)Snort & Bro Updater(ids_offline_update.py)

απαιτεί OS root για την είσοδο σε προνομιακούς φακέλους.

Master Server για Snort rules και αρχεία GeoIP

Sensor server για GeoIP αρχεία.

Example Download:

```
$ python securityonion_airgap_download.py -e *****@*****.com
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Η διεύθυνση email έχει αφαιρεθεί.

```
Output Dir: Security Onion-airgap-20160109-1757

[GeoIP]
Downloading GeoIP.dat.gz...
Decompressing GeoIP.dat.gz...
Downloading GeoIPv6.dat.gz...
Decompressing GeoIPv6.dat.gz...
Downloading GeoLiteCity.dat.gz...
Decompressing GeoLiteCity.dat.gz...
Downloading GeoLiteCityv6.dat.gz...
Decompressing GeoLiteCityv6.dat.gz...

[RIR]
Downloading delegated-afrinic-extended-latest...
Downloading delegated-afrinic-extended-latest.md5...
Downloading delegated-apnic-extended-latest...
Downloading delegated-apnic-extended-latest.md5...
Downloading delegated-arin-extended-latest...
Downloading delegated-arin-extended-latest.md5...
Downloading delegated-lacnic-extended-latest...
Downloading delegated-lacnic-extended-latest.md5...
Downloading delegated-ripencc-extended-latest...
Downloading delegated-ripencc-extended-latest.md5...
Checking MD5 for delegated-afrinic-extended-latest...
  MD5 OK
Checking MD5 for delegated-apnic-extended-latest...
  MD5 OK
Checking MD5 for delegated-arin-extended-latest...
  MD5 OK
Checking MD5 for delegated-lacnic-extended-latest...
  MD5 OK
Checking MD5 for delegated-ripencc-extended-latest...
  MD5 OK

[Snort Static]
Downloading community-rules.tar.gz...
Downloading md5s...
Downloading ip-filter.blf...
Downloading compromised-ips.txt...
Checking MD5 for community-rules.tar.gz...
  MD5 OK

[Snort ET Dynamic]
Downloading emerging.rules.tar.gz...
Downloading emerging.rules.tar.gz.md5...
Checking MD5 for emerging.rules.tar.gz...
  MD5 OK
Downloading emerging.rules.tar.gz...
Downloading emerging.rules.tar.gz.md5...
Checking MD5 for emerging.rules.tar.gz...
  MD5 OK

[Snort VRT Dynamic]
Snort.org E-mail: *****@*****.com
Password:
Signed in successfully.
Downloading snortrules-snapshot-2962.tar.gz...
Downloading snortrules-snapshot-2976.tar.gz...
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

```
Downloading snortrules-snapshot-2980.tar.gz...
Downloading md5s...
Checking MD5 for snortrules-snapshot-2962.tar.gz...
  MD5 OK
Checking MD5 for snortrules-snapshot-2976.tar.gz...
  MD5 OK
Checking MD5 for snortrules-snapshot-2980.tar.gz...
  MD5 OK

[Final]
Compressing Security Onion-airgap-20160109-1757...
  MD5: be1581f3c9f58402978d1a2968624c88

$ du -ch so-airgap-20160109-1757

40M so-airgap-20160109-1757/GeoIP
20M so-airgap-20160109-1757/RIR
384K    so-airgap-20160109-1757/Snort/VRT_Community
448K    so-airgap-20160109-1757/Snort/Blacklist
1.9M    so-airgap-20160109-1757/Snort/ET_GPL
1.8M    so-airgap-20160109-1757/Snort/ET_NonGPL
101M    so-airgap-20160109-1757/Snort/VRT_Registered
106M    so-airgap-20160109-1757/Snort
165M    so-airgap-20160109-1757
165M    total

$ ls -lh so-airgap-20160109-1757.*

-rw-r--r-- 1 skitheslicer skitheslicer 131M Jan  9 18:02 so-airgap-
20160109-1757.tar.gz
-rw-r--r-- 1 skitheslicer skitheslicer   63 Jan  9 18:02 so-airgap-
20160109-1757.tar.gz.md5
```

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# 7. Αποτελέσματα

Εφόσον το σύστημα έχει εγκατασταθεί και λειτουργεί σωστά, είναι καιρός να βρεθούν τα πλεονεκτήματα και τα μειονεκτήματα αυτού.

Δεν υπάρχουν τόσα πολλά μειονεκτήματα, και ακόμη και τα υφιστάμενα προβλήματα μπορούν να λυθούν εύκολα.

## 7.1 Πλεονεκτήματα

Το Security Onion είναι ένα αρκετά πολύπλοκο σύστημα. Κανένα IDS / IPS σύστημα δεν προσφέρει τόσες πολλές λειτουργίες και λογισμικα. Σε αυτό το σημείο το Security Onion με το Snort είναι πολύ ευέλικτο περιβάλλον.

Επιτρέπει στο χρήστη να ρυθμίσει την ασφάλεια του δικτύου του, όπως ο ίδιος επιθυμεί.

Είναι πιο ευκολο στη χρήση, καθώς υπάρχουν πολλά προεγκατεστημένα εργαλεία και διαμορφώσεις. Όταν ο χρήστης εγκαθιστά καθαρό Snort χωρίς Security Onion, ο χρήστης πρέπει να κατεβάσει όλα τα πακέτα και τα σενάρια. Στη συνέχεια, ο χρήστης πρέπει να ρυθμίσεί preprocessors, detectors, sniffers, agents και sensors και να τους καταχωριστουν ο ένας στον άλλο. Απαιτεί πολύ χρόνο και βαθιά γνώση των συστημάτων Unix. Στο Security Onion ο χρήστης μπορεί να χρησιμοποιήσει αυτές τις λειτουργίες μέσω SO Wizard.

Το Security Onion έχει εργαλεία διαχείρισης προεγκατεστημένων αισθητήρων, αναλυτές της κυκλοφορίας και sniffers πακέτων. Μπορεί να λειτουργήσει χωρίς κανένα πρόσθετο λογισμικό IDS / IPS.

Είναι εύκολο σε update rules και πολλά έτοιμα rules που μπορεί να βρεθούν στο Internet και αυτό το IDS / IPS το σύστημα είναι πολύ χρήσιμο για την προστασία των δικτύων.

Η ταχεία ανάπτυξη της Snort και του Security Onion παρέχει πολλές ενημερώσεις, που βελτιώνουν το επίπεδο ασφάλειας.

## 7.2 Μειονεκτήματα

Από την άλλη πλευρά, το σύστημα αυτό έχει επίσης μερικά μειονεκτήματα. Στο Security Onion to Snort κάνει να μην λειτουργούν σαν IPS μετά την εγκατάσταση, μόνο ως IDS και ο χρήστης δεν μπορεί να βρεί οδηγίες σχετικά με αυτό σε ιστοσελίδες για το Security Onion. Ως εκ τούτου, πρέπει να αναπτύξει πολλές πληροφορίες που σχετίζονται με το Snort για να το ρυθμίσει ως IPS.

Επίσης το Security Onion δεν υποστηρίζει το δίκτυο Wi-Fi (WLAN) για τη διαχείριση των λειτουργιών του.

Κατά την εγκατάσταση του Security Onion απενεργοποιούνται οι συνδέσεις διαχειριστή δικτύου και Wi-Fi στο σύστημα. Για να χρησιμοποιηθεί το WLAN ο χρήστης πρέπει να παραλείψει την εγκατάσταση του Οδηγού και να το κάνει manually, χωρίς οποιεσδήποτε οδηγίες.

Πολλά ολοκληρωμένα λογισμικά απαιτούν πολύ χρόνο για να μαθευτούν. Έτσι, για να λειτουργήσει πιο αποτελεσματικά ο χρήστης, πρέπει να ξέρει πώς να συνεργαστεί με διαφορετικά προγράμματα.

Ένα σοβαρό ελάττωμα του συστήματος είναι ότι το Security Onion δεν έχει πλήρη αντίγραφα ασφαλείας των αρχείων ρυθμίσεων. Κάνει μόνο αντίγραφο ασφαλείας των κανόνων αυτομάτως. Ως εκ τούτου, για να κάνει αντίγραφα ασφαλείας ο χρήστης, πρέπει να χρησιμοποιήσει εξωτερικό λογισμικό.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# Συμπεράσματα και Σχόλια

Σε αυτό το κεφάλαιο, παρουσιάζονται τα κύρια ερευνητικά αποτελέσματα της διατριβής. Το κεφάλαιο αυτό εξετάζει επίσης την αξιοπιστία και την εγκυρότητα της μελέτης, και ορίζει θέματα για μελλοντικό έργο. Ο στόχος είναι να συνοψίσει τις διαδικασίες αποτροπής μιας επίθεσης, καθώς και την διαχείριση του περιστατικού από μικρό μεσαίες επιχειρήσεις. Ακολουθεί μια συνοπτική συγκριτική μελέτη σχετικά με το ανοιχτό λογισμικό που παρουσιάστηκε παραπάνω και αυτά που προσφέρουν οι εταιρείες. Επίσης γίνεται μια προσπάθεια προσέγγισης βέλτιστων λύσεων για μικρομεσαίες εταιρείες, καθώς και για την αξιολόγηση της ποιότητας της εργασίας και την ερευνητική διαδικασία.

## 1. Προβλήματα που αντιμετωπίστηκαν

Κατά την εκπόνηση της παρούσας μελέτης παρουσιάστηκαν κάποια προβλήματα όσο αφορά το λογισμικό που επιλέχθηκε να χρησιμοποιηθεί. Το κύριο πρόβλημα αυτής της έρευνας ήταν να περιγράψει πώς η αρχιτεκτονική ασφάλειας στον κυβερνοχώρο για την τακτική δικτύωσης των μικρών-μεσαίων επιχειρήσεων θα πρέπει να σχεδιάζεται χρησιμοποιώντας τα χαρακτηριστικά των δικτύων. Ο κύριος σκοπός ήταν η ανάπτυξη μιας αρχιτεκτονικής που πληροί τις απαιτήσεις ασφαλείας και χρησιμοποιεί γνωστικές δυνατότητες δικτύωσης.

Όσον αφορά το τεχνικό κομμάτι αυτής παρουσιάστηκε πρόβλημα όχι τόσο στην εγκατάσταση του Security Onion σε virtual machine όσο στη χρήση αυτού. Καθώς οι απαιτήσεις του συστήματος για τη διαχείριση των εργαλείων απαιτούν πραγματική μνήμη RAM κάτι που στα συστήματα που δοκιμάστηκε κολλούσε και έκλεινε. Αρχικά δηλώνοντας από τα 4GB συνολικά του συστήματος δόθηκαν τα 2GB στο Security Onion. Και αν και δοκιμάστηκαν και άλλες λύσεις, όπως υπήρξε επικοινωνία με τον okeano (https://okeanos.grnet.gr/home/) και με το Synnefo.org, δεν υπήρξε η δυνατότητα να σηκωθεί σε cloud το Security Onion.

Αξίζει να τονισθεί η άμεση ανταπόκριση του Doug Burks (CEO at Security Onion Solutions, LLC) σε οποιαδήποτε απορία σχετικά με το σύστημα.

## 2. Αποτελέσματα έρευνας

Σε αυτό το κεφάλαιο θα γίνει μια προσπάθεια διύλισης της παρούσας κατάστασης. Είναι πλέον γεγονός ότι η ασφάλεια των δικτύων αποκτά όλο και μεγαλύτερη σημασία στις μέρες μας, εν όψει των διάφορων επιθέσεων, που θέτουν την ασφάλεια των επιχειρήσεων λιγότερο αποτελεσματική αλλά συνάμα και αρκετά ευάλωτη. Αρχικά περιγράφηκαν οι βασικές απειλές σε συστήματα, καθώς και οι τρόποι αντιμετώπισης τους. Βάσει των παραπάνω, λόγω της ραγδαίας εξέλιξης των επικοινωνιών, αλλά κυρίως και η αυξανόμενη χρήση του διαδικτύου, οδηγεί στην ανάγκη για συνεχόμενη ασφάλεια που την κάνει ολοένα και πιο υποχρεωτική.

Κρίνεται απαραίτητο, η ομάδα διαχείρισης περιστατικών ασφαλείας, να μπορεί να είναι σε θέση να κατανοεί και να αντιλαμβάνεται τέτοιες επιθέσεις, τόσο για τη βιωσιμότητα της εταιρείας όσο και για τη μείωση του αντίκτυπου της επίθεσης.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Παρόλα αυτά, οι μέθοδοι αντιμετώπισης των επιθέσεων αυτών είναι γνωστοί και πρέπει να είναι σε θέση να μπορούν να αντιμετωπιστούν μέσα από την υπάρχουσα υποδομή και τεχνολογία. Η καλή εφαρμογή των κανόνων ασφαλείας είναι που πρέπει να ληφθούν πολύ σοβαρά υπ' όψιν, καθώς διαφορετικά υπολογίζεται οτι το κόστος υποκλοπής δεδομένων θα είναι πολύ μεγάλο. Για το λόγο αυτό, η εξοικίωση και η συνεχόμενη αναβάθμιση των ήδη υπαρχόντων μεθόδων θεωρείται επιβεβλημένη, ώστε να μπορεί να λειτουργεί σωστά, αποδοτικά και αξιόπιστα το δίκτυο.

Ιδιαίτερα σημαντική κρίνεται η ασφάλεια των δικτύων μεταφοράς δεδομένων στις μέρες μας. Ο αντίκτυπος που μπορεί να έχει μια επίθεση στην οικονομία και στην φήμη της επιχείρησης είναι κάτι που πρέπει να ληφθεί σοβαρά υπόψη. Ιδιαίτερα μεγάλες επιχειρήσεις ή και κρατικά δίκτυα έχουν υπάρξει στόχοι επιθέσεων. Η πρόληψη μαζί με την ενημέρωση των χρηστών και των διαχειριστών δικτύων είναι απαραίτητη. Στα πλαίσια της πτυχιακής αυτής εργασίας, έγινε αναφορά τόσο σε στοιχειώδεις έννοιες, σε πιθανές απειλές, όσο και σε απλές συμβουλές που μπορούν να ακολουθήσουν απλοί χρήστες του διαδικτύου, αλλά ακόμα και προχωρημένες οδηγίες για τους διαχειριστές δικτύων των επιχειρήσεων .

Ένα σημαντικό μέρος της μελέτης ήταν ο έλεγχος της αξιοπιστίας του ενδεδειγμένου λογισμικού, για να διαπιστωθεί ότι οι αρχιτεκτονικές παρέχουν τις επιθυμητές δυνατότητες ασφάλειας. Σύμφωνα με τα συμπεράσματα του προηγούμενου κεφαλαίου προκύπτει ότι η αποτροπή επίθεσης στο δίκτυο της εταιρείας είναι ένα δύσκολο έργο. Οι απειλές και οι επιθέσεις στον κυβερνοχώρο, είναι τα σημαντικότερα προβλήματα στον σημερινό δικτυωμένο κόσμο. Ο κυβερνοχώρος εκτείνεται παντού με ολοκληρωμένα κυκλώματα και με υπολογιστές. Η λειτουργία του φυσικού κόσμου είναι συνυφασμένη με τον κυβερνοχώρο. Το Διαδίκτυο είναι ο ακρογωνιαίος λίθος για την ύπαρξη των μικρών-μεσαίων επιχειρήσεων και των συστημάτων τους. Σύγχρονες και προχωρημένες μέθοδοι επιθέσεων μπορούν να στοχεύουν τα δίκτυα των επιχειρήσεων. Τα δίκτυα των μικρομεσαίων επιχειρήσεων στηρίζονται σε παλαιότερες τεχνολογίες έτσι είναι αρκετά ευάλωτα στις νέες και εξελιγμένες επιθέσεις. Αργότερα προστέθηκαν επιπλέον αμυντικά μέτρα ασφαλείας προκαλώντας σύγχυση στην διαχείριση του συστήματος. Τα συστήματα αυτά υποφέρουν από την έλλειψη της συνολικής διαχείρισης της ασφάλειας και th διαμόρφωση αυτής, καθώς και από την αξιολόγηση της απειλής. Περαιτέρω, οι στατικές διαμορφώσεις και οι δομές του συστήματος είναι ευκολότεροι στόχοι για την νοημοσύνη του εχθρού.

Το Security Onion που εισήχθη στο κεφάλαιο 2 είναι ένα λογισμικό με πολλές προδιαγραφές, και πολλά υποσχόμενο προϊόν για την παροχή μιας έξυπνης, δυναμικής και αυτο-δημιούργητης(self learning) λύσης. Με αυτόν τον τρόπο η ασφάλεια των δικτύων καθίσταται περισσότερο αποτελεσματική. Λόγω των αδυναμιών των υπαρχόντων μοντέλων δικτυακής ασφαλείας παρουσιάστηκε στο κεφάλαιο 2 το S.O. Στην θεωρία, το πρόγραμμα που περιγράφεται επιλύει το μεγαλύτερο μέρος των προβλημάτων που προκύπτουν με την ασφάλεια της εταιρείας. Οι ενσωματωμένες λειτουργίες επιτρέπουν μια κατανεμημένη και αξιόπιστη υπηρεσία ασφαλείας.

Αναγκαία καθίσταται η αξιολόγηση του λογισμικού κάτι που αποτελεί και ένα δύσκολο έργο. Στην ανάλυση της συνολικής ποιότητας του λογισμικού θα βοηθήσουν η ποσοτικοποίηση της λειτουργικότητας και της απόδοσης των στοιχείων της ασφαλείας.

Τέλος, στα πλαίσια των απειλών που αντιμετωπίζουν οι μικρομεσαίες επιχειρήσεις η παρούσα διατριβή εστίασε κυρίως επόμενα ζητήματα:

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

1. Η κυβερνο απειλή είναι ταχέως αναπτυσσόμενη και μεταβαλλόμενη πράγμα που σημαίνει ότι απαιτούνται οι νέες προσεγγίσεις για να θωρακιστούν τα συστήματα ασφαλείας των μικρών-μεσαίων επιχειρήσεων.

2. Τα χαρακτηριστικά του λογισμικού θα πρέπει να βελτιώσουν τις δυνατότητες δικτύωσης και συνολικής ασφάλειας του δικτύου για την καταπολέμηση και τη διαχείριση της απειλής.

## 3. Συμπεράσματα Security Onion

Ο σκοπός της μελέτης ήταν η παρουσίαση και η εξοικείωση με τα εργαλεία του Security Onion.

Το Security Onion είναι ένα μεγάλο σύστημα για την παροχή της ασφάλειας του δικτύου. Διαθέτει διάφορα IDS και IPS εργαλεία και πολλαπλά περιβάλλοντα όπως το Snort που είναι λιγότερο ευέλικτο εργαλείο. Μπορεί να διαμορφωθεί κατάλληλα ως IPS ή IDS, για την ανίχνευση του ιού, ακόμη και για την προστασία DDoS.

Από την άλλη πλευρά το SO αναφέρεται και σε αρχάριους, κάνοντας αυτές τις διαδικασίες πιο γρήγορα, και παρέχοντας περισσότερες ευκαιρίες για τους εμπειρογνώμονες, σε σύγκριση με πολλές άλλες IDS και IPS. Επίσης, είναι μια καλή εναλλακτική λύση για το υλικό IDS / IPS για τις μικρές επιχειρήσεις που έχουν περιορισμένο προϋπολογισμό.

Τέλος, η διατριβή αυτή μπορεί να χρησιμοποιηθεί ως πρότυπο για την εγκατάσταση του Security Onion, καθώς αποτελεί έναν αναλυτικό οδηγό τόσο των εργαλείων όσο και των ζητημάτων διαχείρισης περιστατικών μέσω αυτού, παρέχοντας τις σχετικές γνώσεις σε κάθε τομέα.

## 4. Συγκριτική Μελέτη Λογισμικών με το Security Onion

Σε αυτή την ενότητα ακολουθεί η συγκριτική μελέτη μιας ειδικής κατηγορίας λειτουργικών συστημάτων και λογισμικών για το χώρο της ασφάλειας. Ειδικότερα κύριος σκοπός είναι η σύγκριση του Security Onion με το AlienVault, το SmoothSec και το SELKS V2.0. Ιδιαίτερη βαρύτητα θα δοθεί στις ομοιότητες και τις διαφορές τους, όσον αφορά τις τεχνικές που απαιτούνται και τα εργαλεία που παρέχουν για την υποστήριξη της ασφάλειας.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

## 4.1 Security Onion vs AlienVault[14]

Τα λογισμικά Security Onion και AlienVault είναι παρόμοια σε πολλές λειτουργίες ωστόσο έχουν διαφορετικές δυνατότητες. Το AlienVault συλλαμβάνει καταγραφές από πολλές διαφορετικές πηγές δεδομένων όπως: syslog από συσκευές, Windows Event Logs, αποτελέσματα από σαρώσεις ευπαθειών, Snort/Surricata, κτλπ. Δεν διαφέρει και πολύ από το Security Onion, αλλά το AlienVault συσχετίζει και επαληθεύει πολλαπλά συμβάντα και πηγές. Τα δεδομένα απο τα Open Threat Exchange (threat intelligence data) επιτρέπουν πράγματα να εμφανίζονται επάνω σε συναγερμούς, με βάση την βαθμολογία των κινδύνων που υπολογίζεται μέσω της διαδικασίας της συσχέτισης. Στην πραγματικότητα το AlienVault είναι εξαιρετικά αποτελεσματικό στο να ξεχωρίζει ενδιαφέροντα δεδομένα και καταγραφές. Όσο αφορά την διατήρηση της καθημερινής ορατότητας μέσα στο δίκτυο ερευνώντας τις ειδοποιήσεις, το Security Onion διαθέτει τα καταλληλότερα εργαλεία.

Τα AlienVault και Security Onion μοιράζονται πολλά κοινά συστατικά, αλλά το AlienVault διαθέτει κατάλληλη διαμόρφωση στην σάρωση ευπαθειών, και μερικά αρκετά καλά χαρακτηριστικά εντοπισμού.(asset tracking)

Το AlienVault υπογράφει και καταγράφει τα πάντα αλλά δεν διατηρεί τις καταγραφές των πακέτων όπως κάνει το Security Onion. Επίσης το AlienVault διαθέτει εξαιρετικές αναφορές.

Συμπεράσματα:

Το AlienVault δεν αντικαθιστά το Security Onion, ούτε το Security Onion αντικαθιστά το AlienVault. Είναι παρόμοια σε πολύ μεγάλο ποσοστό, αλλά τα τελικά αποτελέσματα είναι αρκετά διαφορετικά και συμπληρώνουν το ένα το άλλο.


PRODUCT INFORMATION

AlienVault Unified Security Management v4.4

★★★★½

April 01, 2014

Vendor:
AlienVault

Product:
AlienVault Unified Security Management

Website:
http://www.alienvault.com

Price
$17,700 (hardware), plus support.

Εικόνα 13: Αξία προγράμματος AlienVault[15]

Τέλος, το AlienVault εγκαθίσταται γρήγορα, αλλά κοστίζει αρκετά, ενώ το Security Onion είναι δωρεάν, και ο Doug Burks(που είναι ο δημιουργός) έχει κάνει μια

[14] Πηγή: https://groups.google.com/forum/#!topic/security-onion/LlU6IdXftP0

[15] Πηγή: http://www.scmagazine.com/alienvault-unified-security-management-v44/review/4143/

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

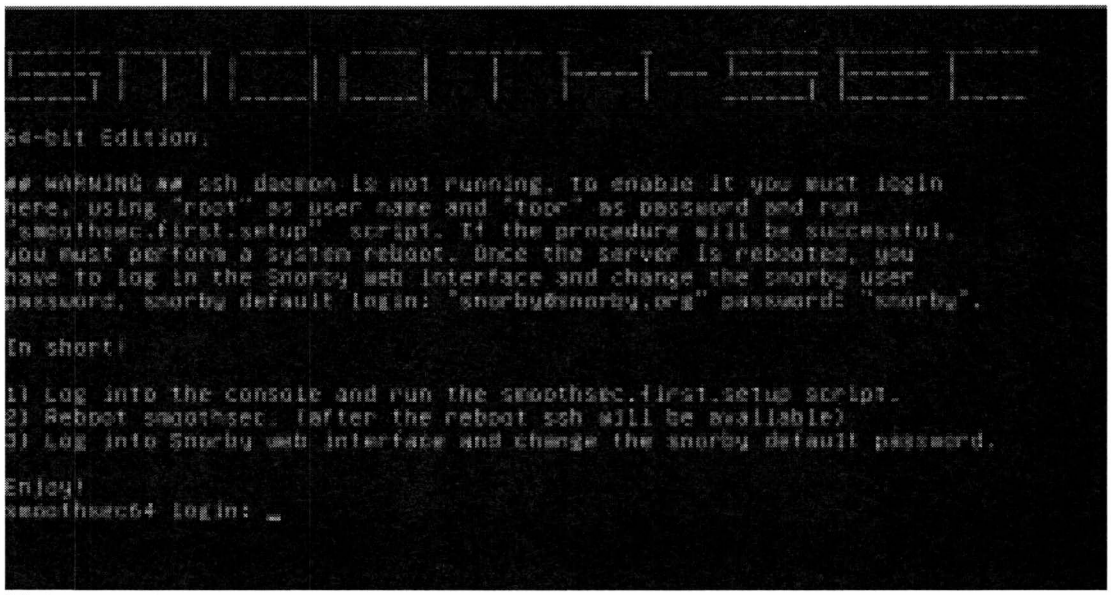
πραγματικά εξαιρετική δουλειά εμπεριέχοντας σχεδόν τα πάντα σε ένα προϊόν και κάνοντας το ακριβώς τόσο απλό και συνάμα καλό όσο ένα πολύ ακριβό εμπορικό προϊόν. Αυτό και μόνο κάνει το Security Onion να υπερέχει.

## 4.2 Security Onion vs Smooth-Sec[16]

Τα Smooth-Sec και Security Onion. Και τα δυο είναι IDS/IPS linux distribution εξοπλισμένα με όλα τα εργαλεία που είναι απαραίτητα για το NSM.

Συνοπτική Σύγκριση:

Smooth-Sec




Links

Official website http://www.smoothsec.org/

SVN https://github.com/smoothsec

Download page https://sourceforge.net/projects/smoothsec/

βασισμένο σε Debian

2 network intrusion sensors (Snort, Suricata)

1 GUI (Snorby)

manual rule management

**SecurityOnion**


Links

[16] Πηγή: http://truica-victor.com/smoothsec-vs-securityonion/

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Official website https://securityonion.net/

SVN https://github.com/security-onion-solutions/security-onion

Download page https://sourceforge.net/projects/security-onion/

βασισμένο σε Ubuntu

2 network intrusion sensors + 1 host intrusion sensor (Snort, Suricata, OSSEC)

3 GUIs (Snorby, Squert, Sguil)

automated rule management

includes multiple log analysis/management tools

Απόψεις μετά την χρήση:

Και τα δύο λειτουργικά συστήματα έχουν την ίδια "back-engine", διαθέτοντας έτσι την δυνατότητα να τρέχουν είτε το Snort είτε το Suricata ή και τα δυο. Όσο αφορά την εγκατάσταση, η διαδικασία είναι ίδια και εκτελείται όπως κάθε Debian/Ubuntu Linux distributor.

Το Smooth-Sec μπορεί να αναπτυχθεί λίγο γρηγορότερα, καθώς δεν διαθέτει desktop graphical interface. Συνεπώς εκτελώντας την "smoothsec.first.startup" εντολή, όλα θα είναι στην θέση τους σε διάρκεια λίγων λεπτών.

Το SecurityOnion μπορεί να ρυθμιστεί αμέσως μετά το πρώτο boot, χρησιμοποιώντας intuitive GUI το οποίο καθοδηγεί τον χρήστη στην διαδικασία tool installation. Ο χρήστης μπορεί να επιλέξει ένα "typical" ή ένα "advanced" τύπο εγκατάστασης, όπου ζητούνται επιλογές σχετικά με major tools.

Στο Smooth-Sec το rule management γίνεται manual, ενώ στο SecurityOnion είναι πλήρως automated, ο χρήστης έχει την δυνατότητα να επιλέξει μεταξύ αρκετών sources (περιλαμβάνοντας Snort VRT όπου ένας προσωπικός oinkmaster κωδικός απαιτείται). 'Ενα άλλο πλεονέκτημα είναι ότι υπάρχουν cronjobs(=scheluded tasks) προγραμματισμένα να ενημερώνουν τα rules καθημερινά.

Το toolbox του Smooth-Sec είναι το ενδεδειγμένο για NSM λύσεις (sensor, rule management, database, GUI) ενώ το αντίστοιχο toolbox του Security Onion είναι πλήρως εξοπλισμένο για NSM, NSM testing (e.g. inundator) log dissection, packet crafting, σκανάρισμα δικτύου και άλλα.

Και οι δύο είναι network-based IDS λύσεις, αλλά το Security Onion επίσης προσφέρει δυνατότητες για host-based IDS ανάπτυξη, χρησιμοποιώντας OSSEC. Όσο για την τοποθέτηση, το Smooth-Sec επίσης προσφέρει την πιθανότητα για in-line ανάπτυξη, μεταμορφώνοντάς σε IPS

Συμπεράσματα:

Το Security Onion είναι καλύτερο όσο αφορά τα τεχνικά χαρακτηριστικά και την υποστήριξη, περισσότερο αυτοματοποιημένο, και έχει περισσότερα εργαλεία και online υποστήριξη και πόρους.

Το Smooth Sec είναι μια κοινοτυπία για NSM λύσεις για σχετικά μικρό δίκτυο.

Συνεπώς αν χρειαστεί μια περισσότερο επαγγελματική προσέγγιση για λύση NSM, ανεξάρτητα το μέγεθος του δίκτυου-συστήνεται το Security Onion.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

## 4.3 Security Onion vs ELK[17]

Το SELKS V2.0 είναι ένα ανοιχτό λογισμικό (open source NSM) που βασίζεται σε ένα ELK framework: Elasticsearch (search and analytics engine) Logstash (log normalization) Kibana (visualization NSM core περιγράφεται από το S που σημαίνει Suricata (NetworkIDS) και το τελευταίο S που σημαίνει Scirius (management GUI for Suricata). Το SELKS παρέχεται ως Linux distribution βασισμένο σε Debian 8.

Μια βασική διαφορά με το SO είναι ότι χρησιμοποιεί το Suricata αντίθετα με το SO που χρησιμοποιεί το Snort και ποτέ το Suricata (παρόλο που είναι διαθέσιμο). Η διαδικασία εκμάθησης είναι αυστηρή, αλλά μόνο μέχρι να συνειδητοποιήσετε οτι έχει αρκετές ομοιότητες με το Snort όπως κανόνες, ρυθμίσεις καθώς και λειτουργίες.

Έτσι γίνεται πιο εύκολο στην κατανόηση. Το Suricata διαφέρει από το Snort σε πολλά χαρακτηριστικά, για παράδειγμα θεωρείται περισσότερο αποδοτικό διότι υποστηρίζει multithreading. Χρησιμοποιώντας Suricata (SELKS) και Snort (SO) ταυτόχρονα σε σύντομο χρονικό διάστημα παρατηρήθηκε ότι κατέγραψαν τις ίδιες ειδοποιήσεις.

Πλεονεκτήματα : SELKS v2.0

- έγκαιρη κι έγκυρη υποστήριξη
- το περιβάλλον είναι καινούργιο (Debian, σταθερές εκδόσεις από software)
- το framework είναι γρήγορα εκτελέσιμο χάρη στο ELK και το Suricata
- Το Scirius διευκολύνει την χρήση του Suricata και των IDS rules
- λόγω της μη-πλήρης καταγραφής των πακέτων διαθέτετε ελεύθερο χώρο στον δίσκο,
- Τα Kibana Dashboards είναι εύκολα στην κατανόηση, την πλοήγηση
- Αυτά τα dashboards παρέχουν το γενικό πλαίσιο που περιγράφει την κίνηση στο δίκτυό σας, όχι μόνο τις ειδοποιήσεις ασφαλείας. Είναι χρήσιμο να αντιλαμβάνεστε καλά τι συμβαίνει στο δίκτυό σας, όχι μόνο από την οπτική της ασφαλείας

Μειονεκτήματα : SELKS v2.0

- Η υποστήριξη για το SO είναι σημαντική γιατί είναι άμεση και πιο ταχεία συγκρινόμενη με την υποστήριξη του SELK.
- Ο χώρος στον σκληρό δίσκο είναι ένα ακόμα μειονέκτημα του SELKS (no pcap = low disk space). Το να μην έχετε το pcap διαθέσιμο σημαίνει:

a) οτι δεν μπορείτε να επαναλάβετε τις ειδοποιήσεις που σήμαναν συναγερμό, μπορείτε να εξάγετε το pcap από το SO όμως.

b) οτι μερικές φορές, εαν μια ειδοποίηση παρουσιάζει ενδιαφέρον, το να είστε σε θέσει να επαναλάβετε αυτήν την ειδοποίηση μέσω wireshark παρέχει χρήσιμα συμπεράσματα. Το SO έχει το Sguil το οποίο μπορεί εύκολα να εξάγει μια ειδοποίηση pcap στο wireshark για περαιτέρω επεξεργασία. Αυτή η δυνατότητα λείπει από το SELKS.

- Το threshold.conf (ή threshold.config για το Suricata) δεν λειτουργεί αν προσπαθήσετε να τερματίσετε έναν κανόνα για περισσότερες από μια IP. Αυτό θεωρείται ένα σημαντικό ελάττωμα που εμποδίζει το SELKS να είναι πραγματικά

[17] Πηγή: http://www.elysiumsecurity.com/blog/IDS/post5.html

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

χρήσιμο. Ο λόγος είναι οτι χρειάζονται αυτό το επίπεδο λεπτομέρειας για κάθε χρήσιμο NSM.

Ανάλογα με τις πολιτικές της εταιρείας, δεν μπορείτε απλά να απενεργοποιήσετε ένα θορυβώδη κανόνα Dropbox για όλες τις συσκευές του δικτύου, ή ένα κανόνα TOR για το θέμα αυτό. Μπορεί να έχετε κάποιες συσκευές για τις οποίες να υπάρχει μια ωραία κίνηση dropbox ή TOR, αλλά για όλες τις άλλες συσκευές αυτό θα μπορούσε να είναι ένα πρόβλημα που θα θέλατε να ξέρετε. Αυτή τη στιγμή, θα πρέπει είτε να δημιουργήσετε έναν κανόνα καταστολής για κάθε IP στη whitelist ή να τα καταστείλει με ένα κανόνα όλοι μαζί, αυτό δεν είναι σωστό και θ αποτελεί κάτι που θα πρέπει να επιλυθεί σύντομα. Και αν μπορούσε να διαχειριστεί αυτούς τους κανόνες σε καταστολή με μια λίστα IP από Scirius αυτό θα ήταν ένα πρόσθετο πλεονέκτημα σε σύγκριση με το SO.

• Δεν υπάρχουν δυνατότητες δημιουργίας καινοτόμων αναφορών out of the box, πράγμα που σημαίνει ότι δεν θα λάβετε ημερήσια/εβδομαδιαία/μηνιαία αναφορά ούτε μπορείτε να ειδοποιηθείτε όταν ένας συγκεκριμένο περιστατικό συμβεί.

**Συμπεράσματα:**

.

Το SO είναι περισσότερο εξελιγμένο, και διαθέτει πιο γρήγορη υποστήριξη. Το SO δουλεύει πολύ καλά με ELSA, BRO και SGUIL εγκαταστημένα, και εξ ορισμού μπορείτε να έχετε πρόσβαση σε όλα τα δεδομένα που χρειάζεστε.

Το SELKS φαίνεται περισσότερο μοντέρνο, πολύ εύκολο σε σύνδεση και χρήση, λειτουργεί χωρίς ιδιαίτερη εγκατάσταση, εύκολο στην χρήση και οι dashboards είναι εύχρηστοι καθώς παρέχουν χρήσιμα συμπεράσματα για το τι συμβαίνει στο δίκτυό σας. Οι αναφορές είναι το αδύνατό του σημείο αλλά με την κατάλληλη ρύθμιση το πρόβλημα επιλύεται.

Τελικά, το αν θα επιλέξετε το SELKS ή το SO εξαρτάται από την επιχείρησή και τις ανάγκες της εταιρείας και με ποιον τρόπο επιθυμείτε να χρησιμοποιήσετε τις πληροφορίες που προκύπτουν. Ωστόσο, είναι ξεκάθαρο οτι το SELKS έχει κέρδος απο την πρώτη έκδοση έως την πιο πρόσφατη, και τουλάχιστον είναι μια διανομή NSM που έχει τον έλεγχο και αξίζει να ασχοληθεί και να αφιερώσει χρόνο κάποιος.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# 5. Μελλοντική Έρευνα

Τα αποτελέσματα αυτής της μελέτης θα δημιουργήσουν πολλές ανάγκες για περαιτέρω ερευνητικές εργασίες. Οι Μελλοντικές εργασίες μπορούν χονδρικά να χωριστούν σε τρείς κατηγορίες.

Η πρώτη είναι να βελτιωθεί το προτεινόμενο λογισμικό S.O. με περισσότερες λειτουργίες και ορισμούς. Είναι περισσότερο από απαραίτητο για να προγραμματίσετε και να σχεδιάσετε τις λεπτομέρειες και λειτουργίες για κάθε εργαλείο του λογισμικού. Η μελλοντική εργασία θα πρέπει να περιλαμβάνει την ανάπτυξη τυποποιημένων περιγραφών για τις λειτουργίες αυτές.

Η δεύτερη είναι η ανάπτυξη των διαδικασιών αξιολόγησης. Αυτή θα περιλαμβάνει είτε τη βελτίωση των εφαρμοζόμενων μεθόδων ή την εισαγωγή νέων μεθόδων. Αναπτύσσοντας το σενάριο που βασίζεται στην αξιολόγηση, που σημαίνει περισσότερη έρευνα σχετικά με τις ευπάθειες και τις επιπτώσεις που προκύπτουν από κάθε απειλή. Για τις νέες μεθόδους αξιολόγησης, τα κοινά κριτήρια θα μπορούσαν να μελετηθούν και να αναπτυχθούν περισσότερο, έτσι ώστε να εφαρμοστεί για την αξιολόγηση της απόδοσης του λογισμικού.

Η τρίτη κατηγορία είναι οι δυνατότητες του λογισμικού. Πολλά χαρακτηριστικά του βασίζονται στην γνωστική διαδικασία.

Η τρίτη κατηγορία περιλαμβάνει το έργο που ανέπτυξε το σενάριο της απειλής. Η ανάπτυξη των σεναρίων θα βελτίωνε τα αποτελέσματα της αξιολόγησης και την αξιοπιστία τους. Περισσότερο λεπτομερή σενάρια απειλής θα απεικονίζουν καλύτερα τις πραγματικές καταστάσεις της ζωής του κυβερνοχώρου και των απειλών σε αυτόν.

Η μελλοντική εργασία θα μπορούσε να περιλαμβάνει επίσης προσομοιώσεις και δημιουργία πρωτοτύπων που είναι σημαντικά όταν η ανάπτυξη της τεχνολογίας αξιολογείται. οι προσομοιώσεις μπορούν να διεξαχθούν χρησιμοποιώντας μια προσέγγιση βήμα-βήμα στο κάθε ένα πρόγραμμα του λογισμικού που δοκιμάζεται.

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

# Αναφορές


**Ξένη Βιβλιογραφία**

1. Network Security, Guidelines to Build a Security Perimeter for SMEs (S. Gordon and P.S.Dowland)
2. Practical Threat Management and Incident Response for the Small- to Medium-Sized Enterprises (SANS Institute Written by Jacob Williams June 2014)
3. Information Security for Small and Medium Sized Enterprises (ISSA-UK 5173, March 2011)
4. Secure Network Architecture: Best Practices for Small Business and Goverment Entities (Stan Jenkins, April 3, 2003)
5. Incident Handling for SMEs (SANS Institute, Terry Morreale, May 12, 2008)
6. Guidelines for IT Security in SMEs (United Nations Interregional Crime and Justice Research Institute (UNICRI), 2015)
7. Intrusion Detection System and Intrusion Prevention System with Snort provided by Security Onion (Bezborodov Sergey, May 2016)
8. Towards an Analysis of Onion Routing Security (Paul Syverson, Gene Tsudik, Michael Reed, Carl Landwehr)
9. A comparative analysis of open-source intrusion detection systems (Mauno Pihelgas, Tallinn 2012)

**Ελληνική Βιβλιογραφία**

1. Ασφάλεια Δικτύων και Firewall (Κώστας Αθανάσιος, 2010-2011)
2. Αρχιτεκτονικές Δικτύων & Πρωτόκολλα Ι (Δημήτριος Λυμπερόπουλος, Σπύρος Δενάζης, Παν. Πατρών)
3. Μέθοδοι και εργαλεία ανάλυσης ευπαθειών δικτύων και εφαρμογών(Γιαλούρης Παναγιώτης, Πειραιάς 2011)
4. Δίκτυα Η/Υ 3, (Περικλής Χατζημίσιος, Σέρρες 2007)
5. Μελέτες-Εφαρμογές και Υλοποίηση Δικτύων Η/Υ (Γ. Μπάρδης)

**Ηλεκτρονικές Πηγές**

http://www.computerweekly.com/feature/The-top-five-SME-security-challenges
http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752015000300525
http://quickbooks.intuit.com/r/technology-and-security/8-types-of-cyber-attacks-your-business-needs-to-avoid/
https://isc.sans.edu/forums/diary/IDS+NSM+and+Log+Management+with+Security+Onion+12043/16652/
https://security-onion-solutions.github.io/security-onion/
https://securityonionsolutions.com/
http://blog.securityonion.net/
https://resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_90218.pdf
https://www.youtube.com/watch?v=fsMCpTdeAn8
https://www.youtube.com/watch?v=dyLbgrdagaA&list=PLMN5wm-C5YjyieO63g8LbaiWTSJRj0DBe
https://github.com/Security-Onion-Solutions/security-onion/wiki
http://www.toptenreviews.com/software/security/best-small-business-antivirus/
http://manual.snort.org/node26.html
https://deltahacker.gr/snort-pfsense-snorby-seconion/
http://www.secdev.org/projects/scapy/



Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79

Δ
005.8
ΚΑΠ

http://www.scmagazine.com/alienvault-unified-security-management-v44/review/4143/

http://www.darknet.org.uk/2013/07/smooth-sec-idsips-intrusion-detectionprevention-system-in-a-box/

**Εταιρείες**

1. Interga open source your business
http://www.interga.gr/index.php?option=com_content&view=article&id=51&Itemid=63&lang=el
2. Δίκτυο Τεχνικής Υποστήριξης
http://www.texnikoi.com/network-installation-data-cabling.html
3. Solutions It.gr
http://solutions-it.gr/
4. OEM.gr
http://oem.gr/main/index.php/diktiaka/1104-sistimata-firewalls-neas-genias
5. LOGIFER Εφαρμογές Πληροφορικής Ε.Π.Ε.

http://www.logifer.gr
6. Elementality
http://elementality.biz/consulting.php
7. Cardel New Technology Applications
http://www.cardel.gr/Default.aspx?ID=38

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΒΙΒΛΙΟΘΗΚΗ
004000131052

Institutional Repository - Library & Information Centre - University of Thessaly
20/04/2024 05:37:03 EEST - 3.14.13.79