Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**ΜΕΘΟΔΟΙ ΔΟΚΙΜΩΝ ΔΙΕΙΣΔΥΣΗΣ** **PENETRATION TESTING METHODS**
Ονοματεπώνυμο Φοιτητή	**ΣΤΑΛΙΟΣ ΔΗΜΗΤΡΙΟΣ**
Πατρώνυμο	**ΣΤΕΦΑΝΟΣ**
Αριθμός Μητρώου	**ΜΠΠΛ / 09007**
Επιβλέπων	**ΦΟΥΝΤΑΣ ΕΥΑΓΓΕΛΟΣ, ΚΑΘΗΓΗΤΗΣ**

Ημερομηνία Παράδοσης Σεπτέμβριος 2013

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα

Περιεχόμενα

Περίληψη

Στην παρούσα μεταπτυχιακή διατριβή , θα ασχοληθούμε με το θέμα της ασφάλειας των πληροφοριών και το penetration testing, καθώς και τους τρόπους που αυτό μπορεί να επιτευχθεί μέσω ειδικών εργαλείων ανίχνευσης των ευάλωτων σημείων διάφορων διαδικτυακών προγραμμάτων. Επίσης θα παρουσιάσουμε τα ορθά βήματα με τα οποία διεξάγεται ένα τέτοιο τεστ καθώς και θα παρουσιάσουμε παραδείγματα ανάλυσης των ευάλωτων σημείων διάφορων εφαρμογών που υπάρχουν σε συγκεκριμένους ιστότοπους κατάλληλα διαμορφωμένους για το σκοπό αυτό. Στο σημείο αυτό οφείλουμε να διευκρινίσουμε ότι η διαδικασία ενός penetration test, αποτελεί μία πράξη η οποία βρίσκεται πάντοτε ανάμεσα στα όρια του νόμιμου και του παράνομου, διότι προϋποθέτει ανάλυση και συλλογή εμπιστευτικών στοιχείων από τους οργανισμούς που ζητούν τη διεξαγωγή αυτού του τεστ. Για το λόγω αυτό πρέπει να γίνεται με μεγάλη προσοχή κα πάντοτε βασισμένο σε πρωτόκολλα κατάλληλα διαμορφωμένα με βάση ένα συγκεκριμένο νομικό πλαίσιο.

Abstract

This graduate thesis will deal with the issue of information security and penetration testing, and how this can be achieved through specific tools to detect vulnerabilities of various online programs. Also we will present the correct steps to conduct such a test and will present examples of analysis of vulnerabilities of different applications that exist on specific sites configured for this purpose only. At this point we should clarify that the process of a penetration test, is an act which is always between what is legal and illegal, because it involves analysis and collection of confidential information from agencies seeking to conduct this test. For this reason, it must be carefully conducted and always based on both properly configured protocols and a specific legal framework.

Πρόλογος

Ένα από τα σημαντικότερα ζητήματα που απασχολούν τις σύγχρονες επιχειρήσεις και οργανισμούς είναι εκείνο της ασφάλειας των εφαρμογών τους και ιδιαιτέρως εκείνων που «κρέμονται» στο διαδίκτυο και εξυπηρετούν είτε ανάγκες των ίδιων των οργανισμών , είτε αποτελούν υπηρεσίες εξυπηρέτησης πελατών. Οι εφαρμογές αυτές ως επί το πλείστον είναι μεγάλα πληροφοριακά συστήματα τα οποία διαχειρίζονται καθημερινά τεράστιο όγκο πληροφοριών , που πολλές από αυτές αποτελούν προσωπικά και εμπιστευτικά στοιχεία είτε των μελών του εκάστοτε οργανισμού είτε των τρίτων προσώπων που έρχονται σε επαφή με τα συστήματα αυτά. Πριν προχωρήσουμε όμως παρακάτω θα παρουσιάσουμε σύντομα τι σημαίνει ασφάλεια πληροφοριακών συστημάτων:

Ορισμός :

« **Ασφάλεια πληροφοριακών συστημάτων** νοείται η προστασία των υπολογιστών, των δικτύων που τους συνδέουν και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους.»

Στις μέρες μας η ασφάλεια είναι κάτι το οποίο δεν μπορεί να επιτευχθεί εύκολα και συνάμα επειδή υπάρχουν αρκετοί κακόβουλοι χρήστες των υπολογιστών που προκαλούν ζημιές ή απώλειες σε αυτά τα πληροφορικά συστήματα , απαραίτητη είναι η παρουσία και η διεξαγωγή ενός penetration test, δηλαδή ενός τεστ ανίχνευσης των ευάλωτων σημείων ενός τέτοιου συστήματος. Με λίγα λόγια το penetration test είναι μια μέθοδος για την αξιολόγηση της ασφάλειας ενός συστήματος ηλεκτρονικού υπολογιστή ή δίκτυου με προσομοίωση μιας επίθεσης από ένα κακόβουλο κώδικα, που είναι γνωστή ως Black Hat Hacker, ή Cracker.

Η διαδικασία περιλαμβάνει μια ενεργή ανάλυση του συστήματος για τυχόν τρωτά σημεία που θα μπορούσαν να προκύψουν από κακή ή αθέμιτη διαμόρφωση του συστήματος, γνωστά και άγνωστα ελαττώματα υλικού ή λογισμικού , ή λειτουργικές αδυναμίες σε διαδικασίες ή τεχνικά αντισταθμιστικά μέτρα. Η ανάλυση αυτή πραγματοποιείται από τη θέση ενός πιθανού εισβολέα και συνεπάγεται την ενεργό εκμετάλλευση κενών ασφαλείας. Τυχόν θέματα ασφαλείας που βρίσκονται θα παρουσιάζονται στον ιδιοκτήτη του συστήματος, μαζί με μια αξιολόγηση των επιπτώσεών τους, και συχνά με μια πρόταση για τον μετριασμό ή μια τεχνική λύση. Η πρόθεση μιας δοκιμής διείσδυσης είναι να προσδιοριστεί η σκοπιμότητα της επίθεσης και το ποσό των επιπτώσεων στις επιχειρήσεις αν τυχόν ανακαλυφθεί.

Όσον αφορά στο penetration test αξίζει να αναφέρουμε δύο διαφορετικούς τύπους τεστ:

1. το Black-Box testing και
2. το White-Box testing

Ο πρώτος τύπος τεστ, δηλαδή η προσέγγιση του «Μαύρου Κουτιού» είναι επίσης γνωστή ως εξωτερική δοκιμή. Κατά την εφαρμογή αυτής της προσέγγισης, ο ελεγκτής ασφαλείας θα αξιολογήσει την υποδομή δικτύου από μια απομακρυσμένη τοποθεσία και δεν θα πρέπει να γνωρίζει καμία αναπτυσσόμενη εσωτερική τεχνολογίες σχετικά με την οργάνωση. Με εφαρμογή ενός αριθμού τεχνικών των πραγματικών hacker και μετά μέσα από οργανωμένες φάσεις δοκιμής, μπορεί να αποκαλυφθούν κάποια γνωστά και άγνωστα σύνολα των τρωτών σημείων που μπορεί να υπάρχουν στο δίκτυο. Ένας ελεγκτής που ασχολείται με το μαύρο κουτί δοκιμών είναι επίσης γνωστός ως «Μαύρο Καπέλο».

Είναι σημαντικό για έναν ελεγκτή να κατανοήσει και να ταξινομήσει αυτές τις ευπάθειες ανάλογα με το επίπεδο του κινδύνου (χαμηλή, μεσαία ή υψηλή). Ο κίνδυνος σε γενικές γραμμές μπορεί να μετρηθεί σύμφωνα με τις απειλή που επιβάλλεται από την ευπάθεια και την οικονομική ζημία που θα προέκυπτε μετά από μια επιτυχημένη διείσδυση. Ένας ιδανικός tester θα μπορούσε να υπονομεύσει τυχόν πληροφορίες που θα μπορούσαν να διακυβεύσουν τον στόχο του. Μόλις η διαδικασία δοκιμής έχει ολοκληρωθεί, μια έκθεση δημιουργείται με όλες τις απαραίτητες πληροφορίες σχετικά με την αξιολόγηση της ασφάλειας, την κατηγοριοποίηση και τη μετάφραση των προσδιορισμένων κινδύνων σε επιχειρησιακό περιεχόμενο.

Ο δεύτερος τύπος τεστ τώρα , δηλαδή η προσέγγιση του «Λευκού Κουτιού» είναι επίσης γνωστή και ως εσωτερική δοκιμή. Ένας ελεγκτής που εμπλέκεται σε αυτό το είδος της διαδικασίας δοκιμών διείσδυσης θα πρέπει να είναι ενήμερος για όλες τις εσωτερικές και βασικές τεχνολογίες που χρησιμοποιούνται από το περιβάλλον-στόχο. Ως εκ τούτου, ανοίγει ένα ευρεία πύλη για έναν ελεγκτή για να δει και να αξιολογήσει την ευπάθειας της ασφαλείας με την

ελάχιστη δυνατή προσπάθεια. Ένας ελεγκτής που ασχολείται με το «Λευκό-Κουτί» είναι επίσης γνωστός ως «Λευκό-Καπέλο». Αυτό φέρνει περισσότερη αξία στον οργανισμό σε σύγκριση με την Blackbox προσέγγιση με την έννοια ότι θα εξαλείψει οποιαδήποτε θέματα εσωτερικής ασφάλειας που βρίσκονται στις υποδομές του περιβάλλοντος-στόχου, και ως εκ τούτου, καθιστά τον οργανισμό πιο ασφαλή και πιο δύσκολο για έναν κακόβουλο αντίπαλο να διεισδύσει από το εξωτερικό.

Ο αριθμός των βημάτων που απαιτούνται σε αυτό τον τύπον τεστ είναι λίγο πολύ παρόμοια με αυτά του μαύρου κουτιού, εκτός από τη χρήση του στόχου, το πεδίο εφαρμογής, τη συλλογή πληροφοριών, και την ταυτοποίηση των φάσεων που μπορούν να εξαιρεθούν. Επιπλέον, η προσέγγιση του «Λευκού Κουτιού» μπορεί εύκολα να ενσωματωθεί σε ένα κανονικό κύκλο ζωής ανάπτυξης για να την εξάλειψη τυχόν θεμάτων ασφαλείας στο αρχικό στάδιο προτού κλαπούν πληροφορίες, και γίνουν αντικείμενο εκμετάλλευσης από εισβολείς. Ο χρόνος και το κόστος που απαιτείται για την εξεύρεση και την επίλυση των τρωτών σημείων της ασφάλειας είναι συγκριτικά λιγότερος από την προσέγγιση του «Μαύρου Κουτιού».

Σε αυτό το σημείο άξιο αναφοράς είναι το γεγονός ότι ο συνδυασμός των δύο τύπων δοκιμών διείσδυσης παρέχει μια ισχυρή αντίληψη για τις εσωτερικές και εξωτερικές απόψεις ασφάλειας. Αυτός ο συνδυασμός είναι γνωστός ως «Γκρι - Κουτί» , και ο ελεγκτής που ασχολείται με αυτές τις δοκιμές είναι επίσης γνωστός και ως «Γκρι - καπέλο». Το βασικό κέρδος στον σχεδιασμό και την άσκηση μιας προσέγγισης «Γκρι – Κουτιού» είναι μια σειρά από πλεονεκτήματα που τίθενται από τις δύο προσεγγίσεις που αναφέραμε παραπάνω. Ωστόσο, αυτό απαιτεί έναν ελεγκτή, με περιορισμένη γνώση του εσωτερικού συστήματος, να επιλέξει τον καλύτερο τρόπο για την αξιολόγηση της συνολικής ασφάλεια. Από την άλλη πλευρά, τα εξωτερικά σενάρια δοκιμών από την προσέγγιση graybox είναι παρόμοια με αυτά του μαύρου κουτιού , αλλά μπορούν να βοηθήσουν στην λήψη καλύτερων αποφάσεων και επιλογών δοκιμής, επειδή ο ελεγκτής είναι ενημερωμένος και γνωρίζει την υποκείμενη τεχνολογία.

Κάθε οργανισμός λοιπόν ,που τον απασχολεί η ασφάλεια των υποδομών του και των εφαρμογών του, ανάλογα με το μέγεθός του , το αντικείμενο ασχολίας και το εύρος των υπηρεσιών-εφαρμογών μπορεί να επιλέξει μια από τις παραπάνω μεθόδους που αναφέραμε ή ένα συνδυασμό αυτών. Σε κάθε περίπτωση η θωράκιση ενάντια σε κακόβουλους εισβολείς είναι πολύ σημαντική για τη βιωσιμότητα και τη συνέχιση της λειτουργίας και κερδοφορίας του οργανισμού.

Κεφάλαιο 1° : Κίνδυνοι ασφάλειας.

Τελειώνοντας με τα εισαγωγικά στοιχεία και τι ακριβώς είναι η ασφάλεια πληροφοριακών συστημάτων καθώς και τι είναι το τεστ διείσδυσης (penetration test) στο παρόν κεφάλαιο θα παρουσιαστούν επιγραμματικά ποιοί είναι οι κίνδυνοι που μπορεί να αντιμετωπίσει ένα σύστημα ενός οποιουδήποτε οργανισμού. Οι κίνδυνοι αυτοί ασφαλείας που θα αναφέρουμε είναι εκείνοι που έχουν κατηγοριοποιηθεί και παρουσιαστεί από την OWASP (Open Web Application Security Project). Έτσι λοιπόν έχουμε τους ακόλουθους :

- **A1 - Injection**: Η κακόβουλη εισαγωγή δεδομένων που δίνεται από έναν εισβολέα για να εκτελέσει αυθαίρετες εντολές στο πλαίσιο ενός web server είναι γνωστή ως injection attack. Οι SQL, XML, LDAP injections είναι μερικά από τα γνωστά είδη. Δραπετεύοντας από τους ειδικούς χαρακτήρες από την είσοδο του χρήστη μπορεί να εμποδιστεί η εφαρμογή αυτής της κακόβουλης επίθεσης στα δεδομένα.
- **A2 - Cross-site scripting (XSS)**: Μια εφαρμογή που δεν επικυρώνει σωστά την είσοδο του χρήστη και προωθεί κακόβουλα «strings» στο πρόγραμμα περιήγησης του διαδικτύου, και τα οποία αν εκτελεστούν μία φορά μπορεί να οδηγήσουν σε εισβολή, κλοπή των cookies, ή παραμόρφωση στην ιστοσελίδα , είναι γνωστή ως cross-site scripting (XSS). Με διαφυγή όλων των μη αξιόπιστων μετα – χαρακτήρων που βασίζονται σε HTML, JavaScript, ή CSS μπορεί να εμποδιστεί η εφαρμογή μιας επίθεσης cross-site scripting.
- **A3 – Προβλήματα πιστοποίησης χρήστη και διαχείριση Session (Broken Authentication and Session Management)** : Χρήση επισφαλών ταυτοτήτων χρήστη και session management ρουτινών μπορεί να οδηγήσει στην «αεροπειρατεία» από άλλους λογαριασμούς χρηστών. Η ανάπτυξη ενός ισχυρού συστήματος διαχείρισης ταυτοτήτων μπορεί να αποτρέψει τέτοιες επιθέσεις. Η χρήση της κρυπτογράφησης, του hashing, και της ασφαλής σύνδεσης και μεταφοράς δεδομένων μέσω SSL ή TLS πρωτοκόλλων συνιστάται ιδιαίτερα.
- **A4 - Επισφαλής άμεσες αναφορές σε αντικείμενα**: Παροχή άμεσης αναφορά στο εσωτερικό αντικείμενο μιας εφαρμογής μπορεί να επιτρέψει σε έναν εισβολέα να χειριστεί τέτοιες αναφορές και να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, εκτός αν πιστοποιηθεί σωστά. Αυτό το εσωτερική αντικείμενο μπορεί να αναφέρεται σε τιμή παραμέτρου ενός λογαριασμού χρήστη, όνομα αρχείου, ή κατάλογο. Ο περιορισμός του χρήστη από κάθε προσπελάσιμο αντικειμένου πριν από την επικύρωση της πρόσβασης και του ελέγχου επαλήθευσης μπορεί να εξασφαλίσει την άδεια πρόσβασης στο ζητούμενο αντικείμενο.
- **A5 - Cross-Site Πλαστογράφηση Αίτησης (Cross-Site Request Forgery - CSRF)**: Ο εξαναγκασμός ενός εξουσιοδοτημένου χρήστη να εκτελέσει πλαστά αιτήματα HTTP κατά μια ευάλωτης web εφαρμογής ονομάζεται cross-site επίθεση πλαστογραφίας αιτήματος. Αυτά τα κακόβουλα αιτήματα εκτελούνται εντός των ορίων μιας θεμιτής συνεδρίας χρήστη, έτσι ώστε δεν μπορούν να ανιχνευθούν. Δεσμεύοντας λοιπόν ένα μοναδικό απρόβλεπτο token για κάθε αίτηση HTTP ανά συνεδρία, ο χρήστης μπορεί να μετριάσει τις επιθέσεις CSRF.
- **A6 – Εσφαλμένη ρύθμιση ασφαλείας (Security Misconfiguration)**: Μερικές φορές, χρησιμοποιώντας μια προεπιλεγμένη διαμόρφωση ασφάλειας μπορεί να αφήσει την εφαρμογή ανοικτή σε πολλαπλές επιθέσεις. Η διατήρηση των πιο γνωστών ρυθμίσεων για την διαμόρφωση μιας εφαρμογής, του web διακομιστή, του διακομιστή βάσης δεδομένων, του λειτουργικού συστήματος, των βιβλιοθηκών κώδικα, και όλων των άλλων σχετικών κατασκευαστικών στοιχείων μιας εφαρμογής είναι ζωτικής σημασίας. Αυτή η διαφανής ασφάλεια των εφαρμογών μπορεί να επιτευχθεί με τη θέσπιση μιας επαναλαμβανόμενης διαδικασίας για την ενημερώσεις λογισμικού, τα patches, και τη «σκλήρυνση» των κανόνων του περιβάλλοντος.
- **A7 - Επισφαλής Κρυπτογραφική αποθήκη (insecure Cryptographic storage)**: Οι αιτήσεις που δεν απασχολούν το κρυπτογραφικό σύστημα προστασίας των ευαίσθητων δεδομένων, όπως οι πληροφορίες υγειονομικής περίθαλψης, η πιστωτική κάρτα συναλλαγών, οι προσωπικές πληροφορίες, και τα στοιχεία ταυτότητας εμπίπτουν στην κατηγορία αυτή. Με την εφαρμογή των συνηθισμένων ισχυρών αλγορίθμων κρυπτογράφησης ή hashing μπορεί να εξασφαλιστεί η ασφάλεια των δεδομένων.

- **A8 - Αποτυχία περιορισμού πρόσβασης URL**: Οι web εφαρμογές που δεν ελέγχουν για τα δικαιώματα πρόσβασης με βάση το URL μπορεί να επιτρέψουν σε έναν εισβολέα τη μη εξουσιοδοτημένη πρόσβαση σε διάφορες σελίδες - ιστότοπους. Για να επιλυθεί αυτό το ζήτημα, περιορίζουμε την πρόσβαση σε ιδιωτικές διευθύνσεις URL με την εφαρμογή της κατάλληλης επαλήθευσης ταυτότητας και τους ελέγχους αδειών, και να αναπτύσσουμε μια πολιτική για συγκεκριμένους χρήστες και ρόλους που επιτρέπονται μόνο στην πρόσβαση της εξαιρετικά ευαίσθητης περιοχής.
- **A9 - Ανεπαρκής προστασία του επιπέδου μεταφοράς**: Η χρήση ασθενών αλγορίθμων κρυπτογράφησης, λανθασμένων πιστοποιητικών ασφαλείας, και ανάρμοστων ελέγχων ταυτότητας μπορεί να θέσουν σε κίνδυνο την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Αυτό το είδος των δεδομένων είναι πάντα ευάλωτο στις επιθέσεις υποκλοπής καθώς και στις επιθέσεις τροποποίησης. Η ασφάλεια των εφαρμογών αυτών μπορεί να βελτιωθεί με την εφαρμογή πρωτοκόλλων SSL για όλες τις ευαίσθητες σελίδες και τη ρύθμιση έγκυρων ψηφιακών πιστοποιητικών που εκδίδονται από εξουσιοδοτημένες αρχές πιστοποίησης.
- **A10 – Μη πιστοποιημένες ανακατευθύνσεις και προωθήσεις (unvalidated redirects and forwards)** : Υπάρχουν πολλές web εφαρμογές που χρησιμοποιούν δυναμική παράμετρο για να ανακατευθύνουν ή να προωθήσουν ένα χρήστη σε μια συγκεκριμένη διεύθυνση URL. Ένας εισβολέας μπορεί να χρησιμοποιήσει την ίδια στρατηγική για να δημιουργήσει ένα κακόβουλο URL για τους χρήστες και να τους κάνει να κατευθυνθούν προς phishing ή malware ιστοσελίδες. Η ίδια επίθεση μπορεί επίσης να επεκταθεί με την αποστολή αιτήματος για την πρόσβαση τοπικών μη εξουσιοδοτημένων ιστοσελίδων. Με την απλή επικύρωση μιας παρεχόμενης τιμής παραμέτρου και τον έλεγχο των δικαιωμάτων ελέγχου πρόσβασης για τους χρήστες με την υποβολή αίτησης μπορεί να αποφευχθεί η παράνομη ανακατεύθυνση και προώθηση.

Αυτοί οι δέκα τύποι επιθέσεων συναντώνται καθημερινά σε πλήθος εφαρμογών και ιστοσελίδων μεμονωμένα ή σε συνδυασμό. Αυτό όπως είναι κατανοητό καθιστά δύσκολη την ασφάλεια των δεδομένων και κατ ‘ επέκταση των εφαρμογών. Συνεχείς επιθέσεις σε κάποια εφαρμογή μπορεί να προκαλέσουν τον τερματισμό της και συνεπακόλουθα τη δημιουργία προβλημάτων στους χρήστες που τη χρησιμοποιούν. Για παράδειγμα μια εφαρμογή που χρησιμοποιείται για κάποια αγορά μέσω των στοιχείων πιστωτικής κάρτας. Μια επίθεση τύπου A7 για παράδειγμα (insecure cryptographic storage) μπορεί να οδηγήσει σε απώλεια προσωπικών δεδομένων ή ακόμα και χρημάτων. Μπορεί λοιπόν κάποιος να φανταστεί το μέγεθος των προβλημάτων που προκαλούνται από τις κακόβουλες επιθέσεις.

Για το λόγω αυτό κάθε οργανισμός ή χρήστης πρέπει να δίνει μεγάλη έμφαση στην ασφάλεια των δεδομένων και των εφαρμογών. Στην περίπτωση των οργανισμών απαιτείται η συνεχής παρακολούθηση και αναβάθμιση των εφαρμογών ως προς την ασφάλεια που παρέχουν στους εκάστοτε χρήστες και όσον αφορά στους χρήστες χρειάζεται ιδιαίτερη προσοχή στα δεδομένα που παρέχουν στις διάφορες ιστοσελίδες. Βεβαίως πρέπει να τονίσουμε ότι ο χρήστης οφείλει να γνωρίζει τη σελίδα που επισκέπτεται ειδάλλως μπορεί να οδηγηθεί σε σελίδες με κακόβουλο περιεχόμενο που μπορούν να προκαλέσουν απώλεια δεδομένων ή και καταστροφή ζωτικών πληροφοριών στο σύστημά του, όπως για παράδειγμα η διαγραφή των δεδομένων του σκληρού δίσκου εξαιτίας κάποιου ιού.

Η ασφάλεια των δεδομένων πρέπει να βρίσκεται στις υψηλές προτεραιότητες όλων όσων ασχολούνται με τη διαχείριση πληροφοριών και δεδομένων μέσω web εφαρμογών , ιστοσελίδων ή οποιονδήποτε άλλων λογισμικών. Το κόστος της απώλειας δεδομένων ή της καταστροφής μιας εφαρμογής είναι πολύ μικρότερο από το κόστος για την ασφάλεια αυτών. Συνιστάται λοιπόν η διεξαγωγή penetration tests ανά τακτά χρονικά διαστήματα ώστε να προλαμβάνονται οι επιθέσεις και οι απώλειες.

Κεφάλαιο 2ο : Τα βήματα ενός penetration test.

Αφού τελείωσε η αναφορά στους κινδύνους και τους τύπους επιθέσεων που μπορούν να αναγνωριστούν, στο παρόν κεφάλαιο θα παρουσιαστούν ποιά είναι τα ορθά βήματα με τα οποία διεξάγεται ένα τεστ διείσδυσης ή αλλιώς pen test. Πριν όμως ξεκινήσει η αναφορά μας θα τονιστεί ότι ένα τεστ διείσδυσης γίνεται με τη βοήθεια κάποιων εργαλείων-προγραμμάτων που έχουν κατασκευαστεί για να βοηθήσουν τον εκάστοτε ελεγκτή στη διεξαγωγή του τεστ. Ένα από τα πιο διαδεδομένα και φημισμένα προγράμματα είναι το «BackTrack». Για την αναφορά των βημάτων, αλλά και μετέπειτα στην πρακτική εφαρμογή αυτών θα χρησιμοποιηθεί το «BackTrack 4 R2». Είναι η πιο πρόσφατη και ενημερωμένη έκδοση και κατ 'επέκταση η πιο ολοκληρωμένη. Επίσης το πρόγραμμα αυτό βασίζεται στο λειτουργικό σύστημα Linux και μπορεί να χρησιμοποιηθεί είτε ως ξεχωριστό λειτουργικό είτε μέσω Live cds και USB format. Η επιλογή εξαρτάται πάντα από το σκοπό που χρησιμοποιείται και βρίσκεται πάντα στην ευχέρεια του ελεγκτή εκτός και αν πρωτύτερα έχει συμφωνηθεί κάτι διαφορετικό από τον προς έλεγχο οργανισμό.

Στο σημείο αυτό ξεκινάει η παρουσίαση των βημάτων με τα οποία διεξάγεται ένα penetration test ή σε συντομία pen test. Παρακάτω αναφέρονται επιγραμματικά τα βήματα και στη συνέχεια θα προχωρήσουμε σε ανάλυση του καθενός καθώς και παρουσίαση των εντολών που χρησιμοποιούνται στο καθένα ξεχωριστά. Τα βήματα λοιπόν είναι τα ακόλουθα :

- Οριοθέτηση στόχου (target scoping)
- Συλλογή πληροφοριών (information gathering)
- Ανακάλυψη στόχου (target discovery)
- Καταμέτρηση στόχου (enumerating target)
- Χαρτογράφηση της ευπάθειας (vulnerability mapping)
- Κοινωνική Μηχανική (social engineering)
- Εκμετάλλευση του στόχου (target exploitation)
- Κλιμάκωση προνομίων (privilege escalation)
- Διατήρηση της πρόσβασης (maintaining access) και
- Τεκμηρίωση και Πληροφόρηση (documentation and reporting)

Σε επόμενο στάδιο θα παρουσιαστεί το κάθε βήμα ξεχωριστά και αναλυτικά αναφέροντας συγκεκριμένα το τι σημαίνει, το τι περιλαμβάνει και τις εντολές με τις οποίες εκτελείται. Επίσης επισημαίνεται ότι για τα περισσότερα βήματα στο BackTrack χρησιμοποιείται το command promt για την πληκτρολόγηση συγκεκριμένων εντολών.

2.1 : Οριοθέτηση στόχου ή Target Scoping.

Στην παράγραφο αυτή θα παρουσιαστεί το 1ο βήμα ενός penetration test το οποίο είναι η οριοθέτηση του στόχου ή διαφορετικά target scoping. Με τον όρο οριοθέτηση στόχου νοείται μια εμπειρική διαδικασία για τη συλλογή απαιτήσεων για την αξιολόγηση ενός στόχου καθώς και το χαρακτηρισμό κάθε μία από τις παραμέτρους της διαδικασίας αυτής ώστε να δημιουργηθεί ένα σχέδιο δοκιμών, περιορισμών, επιχειρηματικών στόχων και σαφέστατα ένα χρονοδιάγραμμα. Αυτή η διαδικασία διαδραματίζει έναν σημαντικό ρόλο στον καθορισμό σαφών στόχων προς οποιοδήποτε είδος αξιολόγησης της ασφάλειας. Με τον προσδιορισμό αυτών των βασικών στόχων μπορεί κανείς να καταλήξει εύκολα σε ένα πρακτικό «χάρτη πορείας» για το τι θα δοκιμαστεί, πώς θα πρέπει να ελεγχθεί, τι πόροι θα διατεθούν, τι περιορισμοί θα εφαρμοστούν, τι επιχειρηματικοί στόχοι θα επιτευχθούν, και πώς το δοκιμαστικό έργο θα σχεδιάζεται και προγραμματίζεται. Έτσι, συνδυάζοντας όλα αυτά τα στοιχεία και τα συμπεριλαμβάνουμε σε μια τυποποιημένη διαδικασία για να επιτευχθεί ο απαιτούμενος στόχος.

Μερικά από τα στοιχεία που περιλαμβάνει το target scoping είναι :

- Η συγκέντρωση των απαιτήσεων του πελάτη που σχετίζεται με τη συσσώρευση πληροφοριών σχετικά με το περιβάλλον και το στόχο μέσα από μια προφορική ή γραπτή επικοινωνία.
- Προετοιμασία του σχεδίου δοκιμής, το οποίο βεβαίως εξαρτάται από διαφορετικά σύνολα μεταβλητών. Αυτά μπορεί να περιλαμβάνουν τη

διαμόρφωση των πραγματικών αναγκών σε δομημένη διαδικασία ελέγχου, τις νομικές συμφωνίες, την ανάλυση κόστους και την κατανομή των πόρων.

- Δημιουργία του προφίλ των ορίων του τεστ, το οποίο καθορίζει τους περιορισμούς που συνδέονται με τη διαδικασία του τεστ διείσδυσης. Αυτά τα όρια μπορεί να είναι ο περιορισμός της τεχνολογίας, της γνώσης, ή ένας επίσημος περιορισμός του IT περιβάλλοντος ίδιου του πελάτη.
- Καθορισμός των επιχειρηματικών στόχων , που είναι μια διαδικασία ευθυγράμμισης των άποψη των επιχειρήσεων με τους τεχνικούς στόχους του προγράμματος δοκιμών διείσδυσης.
- Η διαχείριση του σχεδίου και ο προγραμματισμός του κατευθύνει κάθε βήμα της διαδικασίας διείσδυσης με ένα κατάλληλο χρονοδιάγραμμα για την εκτέλεση των απαιτούμενων δοκιμών. Αυτό μπορεί να επιτευχθεί χρησιμοποιώντας μια σειρά από προηγμένα εργαλεία διαχείρισης έργου.

Συνιστάται ιδιαίτερα η χρήση της διαδικασίας της οριοθέτησης του στόχου ώστε να εξασφαλίζεται μια δοκιμή – τεστ με συνέπεια και μεγαλύτερη πιθανότητα επιτυχίας. Επιπλέον, η διαδικασία αυτή μπορεί επίσης να προσαρμόζεται ανάλογα με τη συγκεκριμένη κατάσταση και τους παράγοντες της δοκιμής. Χωρίς τη χρήση οποιασδήποτε τέτοιας διαδικασίας, θα υπάρξει μια μεγαλύτερη πιθανότητα αποτυχίας, καθώς οι απαιτήσεις που συγκεντρώθηκαν δεν θα έχουν κανένα σωστό ορισμό και διαδικασίες που θα ακολουθήσουν. Επομένως η σειρά με την οποία πρέπει να οριοθετηθεί ο στόχος μας με βάση τα παραπάνω που αναφέραμε αναπαριστάται παρακάτω :

Όπως φαίνεται στο παραπάνω σχήμα, κάθε βήμα αποτελεί μοναδικές πληροφορίες διότι είναι ευθυγραμμισμένο με μια λογική σειρά με σκοπό να συνεχιστεί η εκτέλεση των δοκιμών με επιτυχία. Πρέπει να θυμάται κανείς, ότι όσο περισσότερες πληροφορίες συγκεντρώνονται και όσο πιο σωστή διαχείριση γίνεται με αυτές, τόσο πιο εύκολο θα είναι για τον πελάτη αλλά και το σύμβουλο των Penetration tests να κατανοήσουν περαιτέρω τη διαδικασία των δοκιμών. Αυτό ρυθμίζει επίσης τυχόν νομικά θέματα που πρέπει να επιλυθούν σε πρώιμο στάδιο.

Όπως γίνεται αντιληπτό από τα παραπάνω για τη σωστή διεξαγωγή ενός τεστ διείσδυσης, απαραίτητη είναι η σωστή συλλογή πληροφοριών μέσω της διαδικασίας της καταγραφής απαιτήσεων από τον πελάτη. Όσο πιο αναλυτική είναι αυτή η διαδικασία τόσο περισσότερες πληροφορίες μπορούν να συλλεχθούν και να αξιοποιηθούν, ώστε να αποκτηθεί μια καλύτερη και πιο σφαιρική εικόνα για το περιβάλλον στο οποίο θα γίνει το τεστ , αλλά και την καλύτερη οριοθέτηση του στόχου μας. Ας μη λησμονείται το γεγονός ότι πολλές φορές η διαφορά κρίνεται από μικρές λεπτομέρειες. Περισσότερες πληροφορίες οδηγούν σε καλύτερα αποτελέσματα και όπως είναι φυσικό η διαδικασία του τεστ αποκτά περισσότερες πιθανότητες επιτυχίας. Θυμίζουμε ότι ένα pen test κινείται μέσα στα όρια του νόμιμου και του παράνομου οπότε η διεξαγωγή του θα πρέπει να γίνεται με μεγάλη προσοχή και τα βήματα που θα ακολουθηθούν θα πρέπει να είναι μελετημένα και πλήρως tester πλήρως ενημερωμένος για το στόχο του.

Τέλος όσον αφορά το Target scoping, εκτός του ότι είναι μια πολύ σημαντική διαδικασία για τη διεξαγωγή του τεστ διείσδυσης, μιας και αποτελεί το πρώτο βήμα της όλης διαδικασίας, αποτελεί και ένα μέσω βελτίωσης και ενημέρωσης όσον αφορά το Penetration testing γενικότερα. Κάθε τέτοια ολοκληρωμένη διαδικασία αποτελεί πηγή έμπνευσης και εμπειρίας καθώς οι πληροφορίες που αντλούνται βοηθούν στην καλύτερη κατανόηση του στόχου , αλλά και στη βελτίωση της διαδικασίας του τεστ. Επαναλαμβανόμενα τεστ μέσα σε τακτά χρονικά διαστήματα όχι μόνο καθιστούν την εφαρμογή ασφαλή , αλλά ταυτόχρονα προσδίδουν και μια μορφή ρουτίνας στην όλη διαδικασία μιας και το περιβάλλον πλέον έχει γίνει γνωστό και έχουν μελετηθεί όλες οι παράμετροί του. Αυτό βέβαια δε σημαίνει ότι η «ρουτινοποίηση» αυτή θα αποτελέσει τροχοπέδη ως προς τη σπουδαιότητα , την ακεραιότητα και την αποτελεσματικότητα του τεστ. Μη αξιόπιστο τεστ σημαίνει αρκετές φορές και μη αξιόπιστος αναλυτής. Για το λόγο

αυτό χρειάζεται ιδιαίτερη προσοχή με έμφαση πάντα στο να έχουμε σωστά αποτελέσματα και συνεπώς καλύτερη και περισσότερη ασφάλεια.

2.2 : Συλλογή πληροφοριών ή Information Gathering.

Παρακάτω ακολουθεί η συλλογή πληροφοριών ή οποία είναι η δεύτερη φάση στη διαδικασία δοκιμής διείσδυσης μας. Σε αυτή τη φάση, προσπαθεί ο ελεγκτής να συλλέξει όσες περισσότερες πληροφορίες μπορεί για το στόχο, για παράδειγμα δυναμικά ονόματα χρηστών, διευθύνσεις IP, ονόματα εξυπηρετητών και ούτω καθεξής. Κατά τη διάρκεια της συλλογής πληροφοριών, κάθε κομμάτι των πληροφοριών είναι σημαντικό.

Με βάση τη μέθοδο που χρησιμοποιείται, μπορεί να χωριστεί η συλλογή πληροφοριών σε δύο κατηγορίες: την ενεργή συλλογή πληροφοριών και την παθητική συλλογή πληροφοριών. Στην ενεργή μέθοδο συλλογής πληροφοριών, συλλέγονται πληροφορίες από την εισαγωγή της κίνησης του δικτύου με το δίκτυο του στόχου, όπως να γίνει ένα ICMP ping, και μια σάρωση θύρας TCP. Ενώ σε παθητική συλλογή πληροφοριών, συλλέγονται πληροφορίες σχετικά με ένα δίκτυο-στόχο με τη χρήση υπηρεσιών τρίτων μερών, όπως η μηχανή αναζήτησης Google, και ούτω καθεξής. Στο παρόν τμήμα θα εξεταστούν και οι δύο μέθοδοι και θα παρουσιαστούν σε command promt οι εντολές που χρησιμοποιούν ειδικά εργαλεία του προγράμματος BackTrack.

2.2.1 : Metagoofil

Ξεκινώντας από την παθητική συλλογή πληροφοριών θα παρουσιαστεί ένα εργαλείο που χρησιμοποιεί την υπηρεσία του Google για να συλλέξει πληροφορίες. Το εργαλείο αυτό ονομάζεται **Metagoofil** και αξιοποιεί τη μηχανή αναζήτησης του Google για να συλλέξει μεταδεδομένα από έγγραφα, παρουσιάσεις, pdfs κ.λπ. Μέσα από αυτά τα μεταδεδομένα μπορούμε να βρούμε πληροφορίες για ονόματα χρηστών , διαδρομών και διευθύνσεων MAC.

Χρησιμοποιώντας το BackTrack εντοπίζεται το συγκεκριμένο εργαλείο στο μενού Information gathering => Archive => Metagoofil. Στη συνέχεια σε command promt πληκτρολογούνται οι ακόλουθες εντολές :

 # cd /pentest/enumeration/google/metagoofil

 # ./metagoofil.py

 # ./metagoofil.py -d targetdomain -l 20 -f all -o test.html -t test

Εκτελώντας τις παραπάνω εντολές και παίρνοντας ως targetdomain το unipi.gr ,για περισσότερη ευκολία, έχουμε τα ακόλουθα αποτελέσματα :

[+] Command extract found, proceeding with leeching

[+] Searching in unipi.gr for: pdf

9060

[+] Total results in google: 9060

[+] Limit: 30

[+] Searching results: 0

[+] Searching results: 20

[+] Directory test already exist, reusing it

[1/38] http://www.unipi.gr/noc/mail/OEsetup.pdf

Can't download

Can't Download http://www.unipi.gr/noc/mail/OEsetup.pdf

[2/38]

http://www.unipi.gr/akad_tmhm/org_dioik_epix/simeiwseis/epixeirimatikotita_2004.pdf

Can't download

Can't Download

http://www.unipi.gr/akad_tmhm/org_dioik_epix/simeiwseis/epixeirimatikotita_2004.pdf

[3/38] http://www.unipi.gr/faculty/migl/aoke/aoke_notes_set_2.pdf

2.2.2 : Goorecon

Συνεχίζοντας με την παθητική συλλογή πληροφοριών παρουσιάζεται ένα άλλο παρεμφερές πρόγραμμα που χρησιμοποιεί το Google ως βάση για την εξαγωγή βασικών πληροφοριών για το στόχο που θέτουμε εμείς. Το πρόγραμμα ονομάζεται **Goorecon**. Και πάλι μέσω του Backtrack βρίσκεται το πρόγραμμα αυτό στην ακόλουθη διαδρομή :

Backtrack / Information Gathering / Searchengine / Goorecon

Θέτοντας ξανά το unipi.gr ως στόχο και πληκτρολογώντας σε command promt τις εντολές :

 # cd /pentest/enumeration/goorecon

 # ./goorecon.rb

 # ./goorecon.rb -s unipi.gr

Εξάγονται τα εξής :

root@bt:/pentest/enumeration/goorecon# ./goorecon.rb -s unipi.gr

maritime-unipi.gr.hypestat.com,208.87.241.248

root@bt:/pentest/enumeration/goorecon# ./goorecon.rb -e unipi.gr

nil

Και από τα δύο προγράμματα συλλέγονται όπως είναι φανερό πληροφορίες ως προς κάποια e-mails , διευθύνσεις DNS και στοιχεία που βρίσκονται σε αρχεία doc, pdf ,ppt κ.λπ.

2.2.3 : Dnsrecon.

Αφού έγινε αναφορά σε δύο παραδείγματα σχετικά με την παθητική συλλογή πληροφοριών ακολουθεί η ενεργητική συλλογή. Και πάλι στο σημείο αυτό θα παρουσιαστούν ενδεικτικά κάποια προγράμματα μέσω του BackTrack που βοηθούν σε αυτή την ενδιαφέρουσα και σημαντική διαδικασία. Ως πρώτο παράδειγμα θα χρησιμοποιηθεί το Dnsrecon. Μέσω της διαδρομής **Backtrack / Information Gathering / DNS / Dnsrecon** ανοίγει μια γραμμή εντολών και πληκτρολογούνται τα παρακάτω:

 # cd /pentest/enumeration/dnsrecon

 # ./dnsrecon.rb

 # ./dnsrecon.rb -s unipi.gr

Τα αποτελέσματα της εκτέλεσης αυτής είναι τα ακόλουθα:

root@bt:/pentest/enumeration/dnsrecon# ./dnsrecon.rb -s unipi.gr

query failed: NXDOMAIN

ns.unipi.gr,195.251.229.5,SOA

sns1.grnet.gr,83.212.5.22,NS

sns0.grnet.gr,83.212.5.18,NS

ns.unipi.gr,195.251.229.5,NS

mailhost.unipi.gr,195.251.229.9,MX,5

Στο σημείο αυτό παρατηρείται ότι εμφανίζονται πληροφορίες για τις διευθύνσεις DNS του στόχου, unipi.gr .

2.2.4 : Dnsenum.

Συνεχίζοντας λοιπόν , υπάρχει ένα δεύτερο εργαλείο εξίσου αποτελεσματικό με το προηγούμενο , το οποίο δίνει τη δυνατότητα να αντληθούν πληροφορίες σχετικά με DNS διευθύνσεις , hosts που υπάρχουν στο συγκεκριμένο target domain , καθώς και ονόματα server που λειτουργούν σε αυτό το στόχο. Το εργαλείο αυτή τη φορά είναι το Dnsenum, το οποίο εντοπίζεται στη διαδρομή

: **Backtrack / Information Gathering / DNS / Dns Enum** . Εκτελώντας τις παρακάτω εντολές αποσπώνται οι πληροφορίες που αναφέρθηκαν παραπάνω και οι οποίες παρουσιάζονται κάτωθι :

 # cd /pentest/enumeration/dnsenum

 # ./dnsenum.pl

 # ./dnsenum.pl unipi.gr

Και εξάξονται τα ακόλουθα :

```
root@bt:/pentest/enumeration/dnsenum# ./dnsenum.pl unipi.gr
dnsenum.pl VERSION:1.2
-----   unipi.gr   -----
-----------------
Host's addresses:
-----------------
-------------
Name servers:
-------------
 sns0.grnet.gr.       46383   IN      A       83.212.5.18
 ns.unipi.gr.  407     IN      A       195.251.229.5
 sns1.grnet.gr.       54222   IN      A       83.212.5.22
-----------
MX record:
-----------
 mailhost.unipi.gr.    500     IN      A       195.251.229.9
---------------------
Trying Zonetransfers:
---------------------

 trying zonetransfer for unipi.gr on ns.unipi.gr ...
 unipi.gr.     500     IN      SOA     ns.unipi.gr. root.unipi.gr. (
                               2011072501      ; Serial
                               1200    ; Refresh
                               7200    ; Retry
                               2419200 ; Expire
                               86400 ) ; Minimum TTL
 unipi.gr.     500     IN      NS      ns.unipi.gr.
 unipi.gr.     500     IN      NS      sns0.grnet.gr.
 unipi.gr.     500     IN      NS      sns1.grnet.gr.
 unipi.gr.     500     IN      MX      5 mailhost.unipi.gr.
 4th-conference-hfaa.unipi.gr. 500     IN      CNAME   iweb.xrh.unipi.gr.
 adm.unipi.gr. 500     IN      NS      ns.unipi.gr.
 aeefa.unipi.gr.       500     IN      CNAME   xrhlab01.xrh.unipi.gr.
 antispam.unipi.gr.    500     IN      A       195.251.229.2
 antispam.unipi.gr.    500     IN      A       195.251.229.11
 antispam.unipi.gr.    500     IN      A       195.251.229.12
 apcups.unipi.gr.      500     IN      A       195.251.229.44
 apcups.unipi.gr.      500     IN      MX      5 mailhost.unipi.gr.
```

attica.unipi.gr. 500 IN CNAME zina.cs.unipi.gr.

attika.unipi.gr. 500 IN CNAME neel.cs.unipi.gr.

career.unipi.gr. 500 IN CNAME diasynsrv.naf.unipi.gr.

www.career.unipi.gr. 500 IN CNAME diasynsrv.naf.unipi.gr.

cc.unipi.gr. 500 IN NS ns.unipi.gr.

trying zonetransfer for unipi.gr on sns1.grnet.gr ...

trying zonetransfer for unipi.gr on sns0.grnet.gr ...

brute force file not specified, bay.

2.2.5 : Tcptraceroute.

Επιπροσθέτως, θα αναφερθεί και ένα τρίτο εργαλείο ενεργητικής συλλογής πληροφοριών, που όπως και τα προηγούμενα δίνει σημαντικές πληροφορίες για το περιβάλλον-στόχο που έχει επιλεγεί. Το εργαλείο αυτό είναι το **Tcptraceroute** , το οποίο βρίσκεται στη διαδρομή **Backtrack / Information Gathering / Route / tcptraceroute.** Το εργαλείο αυτό λοιπόν έχει το πλεονέκτημα ότι εάν υπάρχει τείχος προστασίας μεταξύ ελεγκτή διείσδυσης και στόχου και είναι κλειδωμένη η χρήση της απλής traceroute επιτρέπει ακόμα εισερχόμενο πακέτο TCP σε ορισμένες θύρες TCP, και έτσι με τη χρησιμοποίηση της tcptraceroute θα εξακολουθεί να είναι σε θέση να επιτύχει το στόχο πίσω από το τείχος προστασίας. Έχοντας αυτό υπόψη ο ελεγκτής πληκτρολογεί σε γραμμή εντολών:

 # tcptraceroute

 # traceroute www.unipi.gr

Τα αποτελέσματά είναι τα παρακάτω:

root@bt:~# tcptraceroute www.unipi.gr

Selected device eth0, address 192.168.2.4, port 55672 for outgoing packets

Tracing the path to www.unipi.gr (195.251.229.6) on TCP port 80 (www), 30 hops max

1 192.168.2.1 0.900 ms 0.732 ms 0.723 ms

2 loopback2004.med01.dsl.hol.gr (62.38.0.170) 18.774 ms 19.470 ms 17.400 ms

3 62.38.40.181 17.565 ms 33.334 ms 17.463 ms

4 62.38.97.173 53.573 ms 18.329 ms 18.912 ms

5 62.38.96.189 22.516 ms 22.021 ms 20.649 ms

6 tengigaeth02-01.adr01.ar.hol.gr (62.38.96.118) 18.133 ms 18.109 ms 18.707 ms

7 vlan23.grix00.core.hol.gr (62.38.96.218) 17.997 ms 19.052 ms 18.655 ms

8 grnet.gr-ix.gr (83.212.8.1) 18.106 ms 17.568 ms 17.657 ms

9 clientRouter.unipi.eie-2.access-link.grnet.gr (195.251.24.134) 18.304 ms 19.085 ms 18.428 ms

10 spider.unipi.gr (195.251.229.6) [open] 19.470 ms 21.718 ms 22.872 ms

2.2.6: Dmitry

Σε συνέχεια της παρουσίασης των εργαλείων της συλλογής πληροφοριών, θα αναλυθεί και ένα ακόμη, το Dmitry. Το εργαλείο αυτό, το επονομαζόμενο και από τα αρχικά του Deep Magic Information Gathering Tool, βοηθά στη συλλογή μιας πληθώρας πληροφοριών, όπως:

- πληροφορίες για τους hosts από το Netcraft.com
- πληροφορίες για υπο-τομείς σε συγκεκριμένο στόχο – προορισμό
- διευθύνσεις ηλεκτρονικού ταχυδρομείου που διαθέτει ο στόχος
- ανοιχτές , κλειστές οι φιλτραρισμένες θύρες που διαθέτει το μηχάνημα – στόχος

Μέσω του BackTrack και της διαδρομής **Backtrack | Information Gathering | Route | DMitry,** βρίσκεται το συγκεκριμένο εργαλείο και μέσω της γραμμής εντολών πληκτρολογείται η εντολή:

dmitry -iwnse targethost και πιο συγκεκριμένα με ένα παράδειγμα

dmitry -iwnse 192.168.2.1, όπου ως στόχος τίθεται το δίκτυο στο οποίο κινούμαστε. Τα αποτελέσματα της εκτέλεσης είναι τα παρακάτω:

root@bt:/usr/local/bin# dmitry -iwnse 192.168.2.1
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host Name for 192.168.2.1
Continuing with limited modules
HostIP:192.168.2.1
HostName:

Gathered Inet-whois information for 192.168.2.1
----

inetnum: 192.168.0.0 - 192.168.255.255
netname: IANA-CBLK-RESERVED1
descr: Class C address space for private internets
descr: See http://www.ripe.net/db/rfc1918.html for details
country: EU # Country is really world wide
org: ORG-IANA1-RIPE
admin-c: RFC1918-RIPE
tech-c: RFC1918-RIPE
status: ALLOCATED UNSPECIFIED
remarks: Country is really worldwide
remarks: This network should never be routed outside an enterprise
remarks: See RFC1918 for further information
mnt-by: RIPE-NCC-HM-MNT
mnt-lower: RIPE-NCC-HM-MNT
source: RIPE # Filtered

organisation: ORG-IANA1-RIPE
org-name: Internet Assigned Numbers Authority
org-type: IANA
address: see http://www.iana.org
remarks: The IANA allocates IP addresses and AS number blocks to RIRs
remarks: see http://www.iana.org/ipaddress/ip-addresses.htm
remarks: and http://www.iana.org/assignments/as-numbers
admin-c: IANA1-RIPE
tech-c: IANA1-RIPE
mnt-ref: RIPE-NCC-HM-MNT
mnt-by: RIPE-NCC-HM-MNT
source: RIPE # Filtered

role: RFC1918 Role
address: Singel 258
address: 1016 AB Amsterdam
address: The Netherlands
remarks: trouble: See http://www.ripe.net/db/rfc1918.html
admin-c: RFC1918-RIPE
tech-c: RFC1918-RIPE
nic-hdl: RFC1918-RIPE
mnt-by: RFC1918-MNT
source: RIPE # Filtered

2.2.7: Maltego

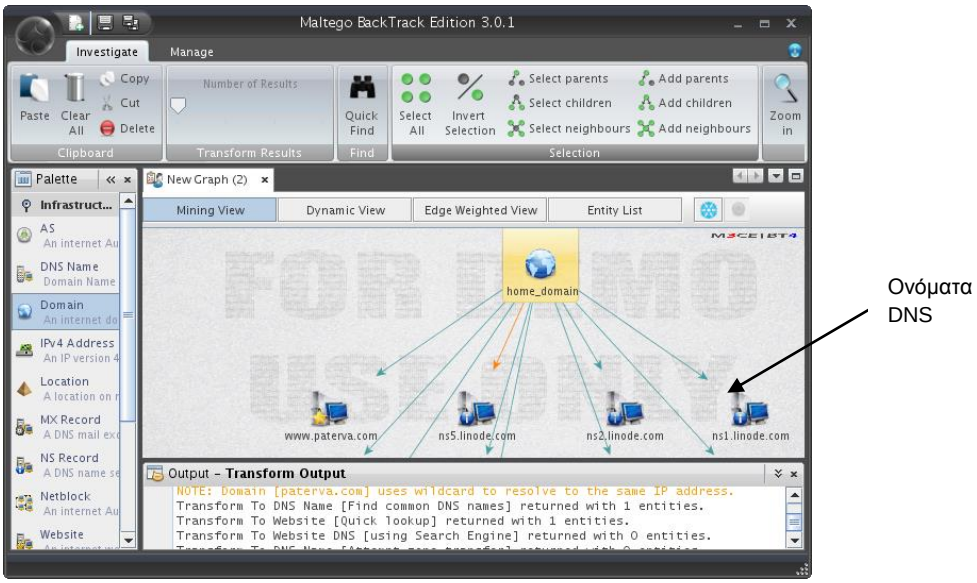
Φθάνοντας στο τέλος του 2ου βήματος, της συλλογής πληροφοριών δηλαδή θα αναλυθεί ένα τελευταίο εργαλείο που βοηθά στη συγκέντρωση πληροφοριών αναλύοντας το δίκτυο – στόχο, το Maltego. Πρόκειται ουσιαστικά για μια εφαρμογή ανοιχτού κώδικα και βοηθά στην «εξόρυξη» και τη συλλογή πληροφοριών ενώ παράλληλα τις παρουσιάζει με έναν αρκετά παραστατικό τρόπο. Με τον όρο ανοιχτός κώδικας δεν νοείται ότι η ίδια η εφαρμογή είναι φτιαγμένη από τέτοιο κώδικα, αλλά ότι λαμβάνει τις απαραίτητες πληροφορίες από διάφορες πηγές ανοιχτού κώδικα. Το Maltego επιτρέπει την απαρίθμηση πληροφοριών της υποδομής του δικτύου που έχει τεθεί ως στόχος, όπως:

- ονόματα domain
- ονόμτα DNS
- Block δικτύου
- διευθύνσεις IP

Επίσης μπορεί να χρησιμοποιηθεί για την συλλογή πληροφοριών σχετικά με συγκεκριμένα άτομα. Πιο συγκεκριμένα απαριθμούνται στοιχεία όπως:

- εταιρίες και οργανισμοί που συνδέονται με ένα συγκεκριμένο άτομο
- διευθύνσεις ηλεκτρονικού ταχυδρομείου που συνδέονται με αυτό το άτομο
- ιστοσελίδες, κοινωνικά δίκτυα καθώς και τηλέφωνα μου ανήκουν ή συνδέονται με κάποιο συγκεκριμένο άτομο.

Παρακάτω με ένα απλό παράδειγμα θα παρουσιαστεί η λειτουργία του Maltego και η αναπαράσταση των πληροφοριών που συλλέγει. Μέσω της διαδρομής **Backtrack | Information Gathering | Paterva Maltego CE** εμφανίζεται ένα παραθυρικό περιβάλλον το οποίο επιτρέπει μέσω επιθυμητών ρυθμίσεων να συλλεχθούν οι απαραίτητες πληροφορίες. Πιο συγκεκριμένα στην εικόνα που ακολουθεί φαίνεται η αναπαράσταση των πληροφοριών σχετικά με τα ονόματα DNS στο δίκτυο που ανιχνεύει:



Εικόνα 1: Maltego με DNS ονόματα

Στο σημείο αυτό πρέπει να τονιστεί για άλλη μια φορά η σπουδαιότητα και η σημαντικότητα της συλλογής πληροφοριών. Όσο καλύτερα γνωρίζει ο ελεγκτής το στόχο του και τι περιλαμβάνει τόσο καλύτερα θα μπορέσει να διεξάγει το τεστ διείσδυσης. Ας μη λησμονείται και το γεγονός ότι κάθε βήμα είναι αλληλένδετο και με το προηγούμενό του , αλλά και με το επόμενό του. Επομένως μια μικρή παράβλεψη σε κάποια παράμετρο ή κάποιο στοιχείο δε θα αποδυναμώσει μόνο τη διαδικασία του συγκεκριμένου βήματος που εκτελείται, αλλά θα δημιουργήσει σοβαρό πρόβλημα σε ολόκληρο το τεστ αυξάνοντας έτσι τα ποσοστά αποτυχίας και ίσως και την επιβολή κυρώσεων στον ελεγκτή από τον οργανισμό , ο οποίος ζήτησε τη διεξαγωγή του τεστ. Όπως έχει αναφερθεί και παραπάνω πριν από το τεστ γίνεται και έλεγχος

και αναφορά των επιχειρηματικών κινδύνων όχι μόνο λόγο κάποιας επίθεσης , αλλά και εξαιτίας ενός πιθανώς αποτυχημένου penetration test. Επισημαίνεται λοιπόν το πόσο σοβαρά πρέπει να λαμβάνεται υπόψη η διαδικασία ενός τέτοιου τεστ.

Ενδεικτικά αναφέρονται παρακάτω και κάποια άλλα εργαλεία του BackTrack που βοηθούν στη διαδικασία συλλογής πληροφοριών τόσο στην ενεργητική όσο και στην παθητική, τα οποία για να μη μακρηγορούμε άνευ λόγου δεν αναφέρουμε στην ανάλυσή μας. Αυτά είναι τα κάτωθι:

- **Tctrace**
- **Traceroute**
- **itrace**
- **0trace**
- **Dnsmap-bulk**
- **Dnsmap**
- **Theharvester**
- **Fierce κλπ.**

2.3 : Ανακάλυψη στόχου ή target discovery.

Η ανάλυση συνεχίζει τώρα στο 3ο βήμα της διαδικασίας του τεστ διείσδυσης που είναι η ανακάλυψη του στόχου ή αλλιώς target discovery. Μετά τη συλλογή των πληροφοριών για το δίκτυο - στόχο από τρίτες πηγές, όπως οι μηχανές αναζήτησης που αναφέρθηκαν στην προηγούμενη ενότητα, θα πρέπει να ανακαλυφθούν και οι μηχανές - στόχοι. Σκοπός λοιπόν του παρόντος βήματος της ανακάλυψης του στόχου είναι:

1. Να βρεθεί ποιά μηχανή ή μηχάνημα στο δίκτυο-στόχο είναι στη διάθεσή του tester. Εάν το μηχάνημα δεν είναι διαθέσιμο, δεν μπορεί να συνεχιστεί η διαδικασία της δοκιμής διείσδυσης, και πρέπει να κινηθεί ο ελεγκτής στο επόμενο μηχάνημα.
2. Να βρεθεί το υποκείμενο λειτουργικό σύστημα που χρησιμοποιείται από το μηχάνημα-στόχο.

Για να μπορέσει να υλοποιηθεί η διαδικασία ανακάλυψης στόχου, μπορούν να χρησιμοποιήθούν τα εργαλεία που παρέχονται στο Backtrack 4. Τα περισσότερα από αυτά τα εργαλεία είναι διαθέσιμα στο μενού Χαρτογράφηση Δικτύου με τα ακόλουθα δευτερεύοντα μενού:

- Identify live hosts και
- OS-Fingerprinting

Τα εργαλεία που περιλαμβάνονται σε αυτή την κατηγορία χρησιμοποιούνται για τον εντοπισμό των μηχανημάτων-στόχων που είναι διαθέσιμα. Ωστόσο, πρώτα πρέπει να γνωρίζει ο ελεγκτής τους όρους και τις συμφωνίες του πελάτη του. Εάν οι συμφωνίες απαιτούν να κρύψει κάποιες pentesting δραστηριότητες, τότε θα πρέπει να τις αποκρύψει τις δραστηριότητες αυτές. Μια Stealth τεχνική μπορεί να εφαρμοστεί για τον έλεγχο της εισβολής Detection System (IDS) ή Σύστημα προστασίας της λειτουργικότητας από εισβολείς (IPS). Εάν υπάρχουν τέτοιες απαιτήσεις, μπορεί να μην χρειαστεί να αποκρύψουμε τις δραστηριότητές μας. Είναι σημαντικό λοιπόν ο εκάστοτε ελεγκτής να συμμορφώνεται με τις συμφωνίες που έχουν υπογραφεί ήδη από τη αρχή κατά τη διάρκεια κιόλας της ανάλυσης απαιτήσεων.

2.3.1 : Ping και Arping

Το εργαλείο ping είναι το πιο διάσημο εργαλείο για να ελέγξει κάποιος αν ένας συγκεκριμένος host είναι διαθέσιμος. Το ping λειτουργεί στέλνοντας ένα ICMP (Internet Protocol Control Message) ECHO πακέτο αίτησης στον κεντρικό υπολογιστή-στόχο. Αν ο στόχος αυτός είναι διαθέσιμος και δεν μπλοκάρει ένα αίτημα ping τότε θα απαντήσει με το πακέτο ICMP ECHO REPLY. Στο BackTrack σε ένα παράθυρο γραμμής εντολών πληκτρολογείται η διεύθυνση για να γίνει το ping για να εντοπιστοarρύν ποιοι hosts είναι διαθέσιμοι. Έτσι έχουμε :

#ping -c 2 -s 1000 IP address , κάνοντας ping στην IP διεύθυνση που θέλουμε , στέλνοντας μόνο 1000 Bytes και μόνο δύο πακέτα. Παρακάτω παρουσιάζονται δύο παραδείγματα με δύο διαφορετικές IP.

- **root@bt:~# ping -c 2 -s 1000 yahoo.gr**
  PING yahoo.gr (87.248.120.148) 1000(1028) bytes of data.
  1008 bytes from w2.rc.vip.ch1.yahoo.com (87.248.120.148): icmp_seq=1 ttl=54 time =80.6 ms
  1008 bytes from w2.rc.vip.ch1.yahoo.com (87.248.120.148): icmp_seq=2 ttl=54 time =79.6 ms

  --- yahoo.gr ping statistics ---
  2 packets transmitted, 2 received, 0% packet loss, time 1000ms
  rtt min/avg/max/mdev = 79.621/80.143/80.665/0.522 ms
- **root@bt:~# ping -c 2 -s 1000 www.unipi.gr**
  PING spider.unipi.gr (195.251.229.6) 1000(1028) bytes of data.

  --- spider.unipi.gr ping statistics ---
  2 packets transmitted, 0 received, 100% packet loss, time 999ms

Επίσης υπάρχει και το εργαλείο arping το οποίο χρησιμοποιείται για να γίνει ping σε έναν κεντρικό υπολογιστή προορισμού στο τοπικό δίκτυο (LAN) χρησιμοποιώντας το ARP (Address Resolution Protocol) αίτημα. Το arping είναι χρήσιμο για να εξεταστεί εάν μια συγκεκριμένη διεύθυνση IP είναι σε χρήση στο δίκτυο. Ακόμη το arping λειτουργεί στο δεύτερο επίπεδο του OSI (Open System Interconnection Layer 2 Network Layer) και είναι το μόνο που μπορεί να χρησιμοποιηθεί σε τοπικό δίκτυο. Παρόλα αυτά όμως το αίτημα ARP δεν μπορεί να δρομολογηθεί σε όλους τους δρομολογητές ή τις πύλες (routers and gateways). Το εργαλείο αυτό βρίσκεται στη διαδρομή **Backtrack / Network Mapping / Identify Live Hosts /Arping.** Για να το χρησιμοποιηθεί απλώς πληκτρολογούνται στη γραμμή εντολών :

#arping -c 3 IP address , σε συγκεκριμένη IP θέλουμε να στείλουμε 3 ανιχνευτές. Πιο συγκεκριμένο είναι το ακόλουθο παράδειγμα:

root@bt:~# arping -c 3 www.unipi.gr

ARPING 195.251.229.6 from 192.168.2.2 eth0

Sent 3 probes (3 broadcast(s))

Received 0 response(s)

2.3.2 : Genlist.

Ένα δεύτερο εργαλείο είναι και το Genlist. Αυτό επιτρέπει την συλλογή μιας λίστα από τους διαθέσιμους hosts οι οποίοι έχουν ανταποκριθεί στους ανιχνευτές που έχουν σταλεί με το arping. Έτσι μέσω της διαδρομής **Backtrack / Network Mapping / Identify Live Hosts / Genlist** εντοίζεται το εργαλείο και στο παράθυρο της γραμμής εντολών που ανοίγει πληκτρολογούνται τα παρακάτω :

#genlist -s 192.168.1.* και εξάγονται τα ακόλουθα αποτελέσματα:

root@bt:~# genlist -s 192.168.2.*

192.168.2.1

192.168.2.2

Άρα δύο μόνο hosts ανταποκρίθηκαν στους ανιχνευτές. Αυτά τα εργαλεία αναφέρονται όπως έγινε φανερό στην ανίχνευση των μηχανών που υπάρχουν σε ένα δίκτυο. Παρακάτω θα παρουσιαστεί ένα εργαλείο με το οποίο ανιχνεύονται τα λειτουργικά συστήματα αυτών των μηχανημάτων.

2.3.3 : Xprobe2.

Το εργαλείο Xprobe2 βοηθά στην ανίχνευση των λειτουργικών συστημάτων που λειτουργούν κάτω από τους hosts που έχουν βρεθεί κάνοντας τις παραπάνω ενέργειες που αναφέρθηκαν. Πιο συγκεκριμένα καταγράφει και συλλέγει τα «δακτυλικά αποτυπώματα» των λειτουργικών συστημάτων με τη χρήση ταιριάσματος ασαφών υπογραφών (fuzzy signature matching), πιθανοτικών εικασιών, ταυτόχρονων πολλαπλών ταιριασμάτων (multiple matches simultaneously), και μια βάση δεδομένων υπογραφών. Στη διαδρομή **Backtrack / Network Mapping / OSFingerprinting / Xprobe2** βρίσκεται το εργαλείο αυτό και πληκτρολογείται η εντολή:

#xprobe2 IP address, δηλαδή

 # xprobe2 www.unipi.gr και λαμβάνονται τα παρακάτω αποτελέσματα:

root@bt:~# xprobe2 www.unipi.gr

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is www.unipi.gr

[+] Loading modules.

[+] Following modules are loaded:

[x] [1] ping:icmp_ping - ICMP echo discovery module

[x] [2] ping:tcp_ping - TCP-based ping discovery module

[x] [3] ping:udp_ping - UDP-based ping discovery module

[x] [4] infogather:ttl_calc - TCP and UDP based TTL distance calculation

[x] [5] infogather:portscan - TCP and UDP PortScanner

[x] [6] fingerprint:icmp_echo - ICMP Echo request fingerprinting module

[x] [7] fingerprint:icmp_tstamp - ICMP Timestamp request fingerprinting module

[x] [8] fingerprint:icmp_amask - ICMP Address mask request fingerprinting module

[x] [9] fingerprint:icmp_port_unreach - ICMP port unreachable fingerprinting module

[x] [10] fingerprint:tcp_hshake - TCP Handshake fingerprinting module

[x] [11] fingerprint:tcp_rst - TCP RST fingerprinting module

[x] [12] fingerprint:smb - SMB fingerprinting module

[x] [13] fingerprint:snmp - SNMPv2c fingerprinting module

[+] 13 modules registered

[+] Initializing scan engine

[+] Running scan engine

[-] ping:tcp_ping module: no closed/open TCP ports known on 195.251.229.6. Module test failed

[-] ping:udp_ping module: no closed/open UDP ports known on 195.251.229.6. Module test failed

[-] No distance calculation. 195.251.229.6 appears to be dead or no ports known

[+] Host: 195.251.229.6 is up (Guess probability: 50%)

[+] Target: 195.251.229.6 is alive. Round-Trip Time: 0.02058 sec

[+] Selected safe Round-Trip Time value is: 0.04116 sec

[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)

[-] fingerprint:smb need either TCP port 139 or 445 to run

[-] fingerprint:snmp: need UDP port 161 open

[+] Primary guess:

[+] Host 195.251.229.6 Running OS: "Sun Solaris 10 (SunOS 5.10)" (Guess probability: 91%)

[+] Other guesses:

[+] Host 195.251.229.6 Running OS: "HP UX 11.0" (Guess probability: 91%)

[+] Host 195.251.229.6 Running OS: "Sun Solaris 2.5.1" (Guess probability: 83%)

[+] Host 195.251.229.6 Running OS: "Sun Solaris 6 (SunOS 2.6)" (Guess probability: 83%)

[+] Host 195.251.229.6 Running OS: "Sun Solaris 7 (SunOS 2.7)" (Guess probability: 83%)

[+] Host 195.251.229.6 Running OS: "Sun Solaris 8 (SunOS 2.8)" (Guess probability: 83%)

[+] Host 195.251.229.6 Running OS: "Sun Solaris 9 (SunOS 5.9)" (Guess probability: 83%)

[+] Host 195.251.229.6 Running OS: "HP UX 11.0x" (Guess probability: 83%)

[+] Host 195.251.229.6 Running OS: "NetBSD 1.4.2" (Guess probability: 75%)

[+] Host 195.251.229.6 Running OS: "NetBSD 1.4.3" (Guess probability: 75%)

[+] Cleaning up scan engine

[+] Modules deinitialized

[+] Execution completed.

2.3.4: Lanmap και lanmap 2.

Συνεχίζοντας της ανάλυση, παρουσιάζονται δύο εργαλεία ανίχνευσης στόχου το lanmap και το lanmap 2. Τα εργαλεία αυτά λειτουργούν «ακούγοντας» παθητικά για οποιαδήποτε δραστηριότητα στο δίκτυο και δημιουργούν μια εικόνα όλων των συστατικών του δικτύου που μπορεί να βρεθούν. Ειδικότερα το lanmap2 φιλτράρει το δίκτυο – στόχο για να εντοπίσει ανοιχτές θύρες ή συσκευές που είναι συνδεδεμένες κατά τη διάρκεια του τεστ. Πιο κατανοητό θα γίνει με ένα απλό παράδειγμα. Στη διαδρομή **Backtrack | Network Mapping | Identify Live Hosts | Lanmap** βρίσκονται τα εργαλεία και πληκτρολογώντας τις ακόλουθες εντολές:

#lanmap -i eth0, όπου eth0 το δίκτυο μέσα στο οποίο κινούμαστε και είναι και το δίκτυο στόχος. Έτσι εξάγονται τα παρακάτω:

root@bt:~# lanmap -i eth0
cmd:twopi -Tpng -o /tmp/tmp.lanmap lanmap.dot && mv /tmp/tmp.lanmap ./lanmap.png && rm lanmap.dot
BOOTP 1: mac:00:0C:29:5D:B3:38, client:192.168.150.130, your: 0.0.0.0, trans:3205877251, rel:0, df:1
BOOTP SIG type:3, ttl:64, flags:3(53,12,55), reqs:7(1,28,2,3,15,6,12)(msgtype:0)
BOOTP 2: mac:00:0C:29:5D:B3:38, client:192.168.150.130, your:192.168.150.130, trans:3205877251, rel:0, df:0
BOOTP SIG type:5, ttl:16, flags:9(53,54,51,1,28,3,15,6,0), reqs:0()(msgtype:0)

Και η απεικόνιση όλων των παραπάνω είναι η ακόλουθη:

Εικόνα 2: Απεικόνιση του lanmap.

Όσον αφορά στο lanmap2, μέσω της διαδρομής **Backtrack | Network Mapping | Identify Live Hosts | Lanmap2** ανοίγει μια γραμμή εντολών και αυτομάτως εμφανίζονται τα ακόλουθα:

Creating fingerprints...
data/gen-db.sql
data/map-BOOTP-Fingerprint.sql
data/map-BOOTP-VendorClass.sql
data/map-BROWSE.sql
data/map-CDP.sql
data/map-DNS-TXT.sql
data/map-ICMP-Echo-Fingerprint.sql
data/map-IPv4.sql
data/map-SSDP.sql
data/map-TCP-SYN.sql
Done.
rep_init OK
PROT_COUNT=44
map_children Logical <- 802.3
map_children 802.3 <- LLC
map_children Logical <- LLC
map_children 802.3 <- ARP
map_children 802.3 <- IPv4
map_children IPv4 <- ICMP
map_children IPv4 <- IGMP
map_children IPv4 <- UDP
map_children IPv6 <- UDP
map_children UDP <- BOOTP
map_children UDP <- SSDP
map_children UDP <- SSDP
map_children UDP <- NB-Dgm
map_children UDP <- NBNS
map_children NB-Dgm <- SMB
map_children NetBIOS <- SMB
map_children TCP <- SMB
map_children SMB <- BROWSE
map_children IPv4 <- TCP
map_children TCP <- HTTP
map_children TCP <- HTTP
map_children TCP <- HTTP
map_children TCP <- HTTPS
map_children UDP <- TiVoConn
map_children 802.3 <- IPv6
map_children UDP <- DNS
map_children UDP <- DNS
map_children 802.3 <- 0x8781
map_children LLC <- CDP
map_children 802.3 <- LLDP
map_children UDP <- RADIUS
map_children LLC <- STP
map_children LLC <- STP
map_children Linux-SLL <- IPX
map_children UDP <- SNMP
map_children UDP <- NTP
map_children UDP <- Rumor
map_children UDP <- RTSP
map_children UDP <- MSSQLM
map_children UDP <- RASADV

```
map_children UDP <- DHCPv6
map_children LLC <- NetBIOS
map_children IPX <- NetBIOS
map_children TCP <- BitTorrent
map_children UDP <- Storm
map_children TCP <- Gnutella
map_children TCP <- Gnutella
map_children TCP <- Gnutella
map_children TCP <- IRC
map_children UDP <- WSDD
map_children IPv4 <- WSDD
map_children IPv6 <- WSDD
map_children TCP <- DCERPC
map_children TCP <- DCERPC
map_children UDP <- ESP
sizeof(arp) -> 8
bootp.c:sanity_check... offsetof(bootp, cookie) -> 236
ok.
offsetof(nb_dgm, id) -> 2
offsetof(nb_dgm, srcport) -> 8
offsetof(nb_dgm, len) -> 10
sizeof Dgm -> 14
checking Types... 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x0a 0x0b 0x0c
0x0d 0x0e 0x0f 0x10 0x11 0x12 0x13 0x14 0x15 0x16 0x17 0x18 0x19 0x1a 0x1b 0x1c 0x1d
0x1e 0x1f 0x20 0x21
sizeof(smb_hdr) <- 32
sizeof(smb_mailslot) <- 8
sizeof(smb_trans_req) <- 38
RASADV_IP=0x0202ffef inet_addr(239.255.2.2)=0x0202ffef
dhcpv6.c:sanity_check... ok.
dhcpv6.c checking PerType... 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x0a
0x0b 0x0c 0x0d
dhcpv6.c checking PerOpt... 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x0a
0x0b 0x0c 0x0d 0x0e 0x0f 0x10 0x11 0x12 0x13 0x14
Devices
  eth0
  usbmon1         USB bus number 1
  usbmon2         USB bus number 2
  any           Pseudo-device that captures on all interfaces
  lo
Defaulting to dev 'eth0'
Adding dev 'eth0'...
opening dev 'eth0' in promiscuous mode...
interface 'eth0' net: 0x0096A8C0, mask: 0x00FFFFFF
Applying Filter_Str="not tcp port 22"...
len=60
\x00PV\xfd\x81\xdc\x00\x0c),\x1dI\x08\x00E\x00\x00(\xd3\xdf@\x00@\x06\x1c\x90\xc0\xa8\
x96\x84\xad\xc2Eq\xd2O\x00Pf\x90\x87\x11o\x0e\x07\x7fP\x11\xff\xff.\xa4\x00\x00\x00\x00
\x00\x00\x00\x00
linktype=1
parsed 802.3 len=60 bytes=14
parsed IPv4 len=46 bytes=20
test_ipv4 0x11=0x11 protocol=0x06
parsed TCP len=26 bytes=20
http_parse -> 6
parsed HTTP len=6 bytes=6
Logical id=0 type=1 bytes=60 when=0
```

802.3 src=00:0c:29:2c:1d:49 dst=00:50:56:fd:81:dc type=0x0800
IPv4 v=4 ihl=5 tos(prec=0 lodel=0 hithr=0 hirel=0 ect=0 ece=0) tlen=40 id=0xd3df flag=0x4000(evil=0 dontfrag=1 morefrag=0 fragoff=0) ttl=64 prot=0x06 chksum=0x1c90 192.168.150.132 -> 173.194.69.113
TCP srcport=53839 dstport=80 seqno=1720747793 ackno=1863190399 fin=1 syn=0 rst=0 psh=0 ack=1 urg=0 ecn=0 cwr=0 res=0x0 off=5 win=65535 chksum=0x2ea4 urgptr=0
HTTP data bytes=6

Από τα παραπάνω αποτελέσματα παρατηρούμε τις ανιχνεύσεις που γίνονται για ανοικτές θύρες και συσκευές που βρίσκονται στο δίκτυο, μέσω μιας βάσης δεδομένων που αυτόματα δημιουργεί το lanmap2, όπως φαίνεται από τις αρχικές εντολές παραπάνω.

Στο σημείο αυτό ολοκληρώθηκε και η παρουσίαση του 3ου βήματος ενός penetration test. Αναφέρθηκαν ενδεικτικά κάποια από τα εργαλεία που επιτρέπουν τη συλλογή πληροφοριών τόσο για τις μηχανές που βρίσκονται ενεργές στο δίκτυο-στόχο όσο και για τα λειτουργικά συστήματα τα οποία χρησιμοποιούν. Επιπροσθέτως τονίζεται ότι όπως και όλα τα προηγούμενα στάδια έτσι και αυτό χρήζει ιδιαίτερης προσοχής. Συλλογή όλων των στοιχείων με κάθε λεπτομέρεια οδηγεί σε πιο έγκυρα δεδομένα και σε καλύτερα τελικά αποτελέσματα όσον αφορά στο τεστ διείσδυσης. Ας μη ξεχνάμε ότι έτσι διευκολύνεται και η δουλειά που έχει να κάνει ο ελεγκτής που διεξάγει το τεστ. Τέλος θα συμπληρωθεί επιγραμματικά μια λίστα με κάποια παρεμφερή εργαλεία με αυτά που παρουσιάστηκαν στις παραπάνω υποενότητες. Αυτά είναι τα κάτωθι:

- **fping**
- **hping**
- **hping2**
- **hping3**
- **arping2**
- **nping**
- **nbtscan και**
- **onesixtyone**

2.4 : Καταμέτρηση στόχου ή enumerating target.

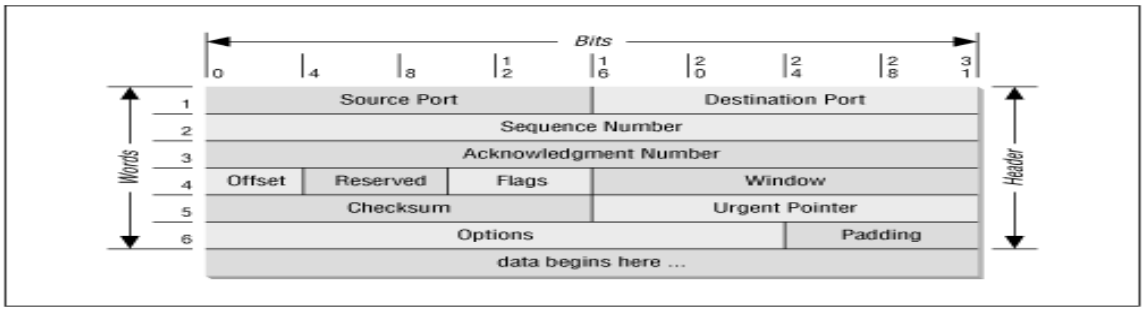
Η καταμέτρηση του στόχου είναι μια διαδικασία που χρησιμοποιείται για να βρεθούν και να συλλεχθούν πληροφορίες για τις θύρες και τις υπηρεσίες που είναι διαθέσιμες στο περιβάλλον - στόχο. Αυτή η διαδικασία γίνεται συνήθως αφού πρώτα έχει ανακαλυφθεί το περιβάλλον – στόχος και στη συνέχεια σαρώνεται για να ανιχνευθούν και να καταγραφούν οι διαθέσιμοι hosts. Συνήθως κατά τη διάρκεια των εργασιών δοκιμών διείσδυσης, η διαδικασία αυτή γίνεται ταυτόχρονα με η διαδικασία ανακάλυψης. Ουσιαστικά το 3ο (target discovery) και το 4ο βήμα (enumerating target) μπορούν να εφαρμοστούν μαζί σε μία φάση. Σε αυτήν εδώ την ενότητα θα αναλυθούν τα ακόλουθα ζητήματα :

- τα εργαλεία που μπορούν να χρησιμοποιηθούν για την πραγματοποίηση της σάρωσης των θυρών
- τα εργαλεία που μπορούν να χρησιμοποιηθούν για να βρεθούν οι υπηρεσίες που εκτελούνται στον στόχο, και
- τα εργαλεία για να ανιχνευθεί ένα Virtual Private Network (VPN), δυνατότητα που είναι διαθέσιμη στο στόχο

2.4α : Ανίχνευση θυρών.

Η σάρωση θυρών, μπορεί να οριστεί ως μια μέθοδος για τον προσδιορισμό των θυρών TCP και UDP που είναι ανοιχτές στα μηχανήματα-στόχους. Μια ανοιχτή θύρα σημαίνει ότι υπάρχει μια υπηρεσία δικτύου που «ακούει» στη θύρα. Αν μια υπηρεσία δικτύου είναι ευάλωτη, τότε ο εισβολέας μπορεί να είναι σε θέση να χρησιμοποιήσει τις πληροφορίες αυτές για να επιταχύνει τη διαδικασία ανάλυσης τρωτότητας. Για να γίνει πιο κατανοητή η ανάλυσή θα παρουσιαστεί εν συντομία η μορφή που έχει το TCP και το UDP πρωτόκολλο.

Ξεκινώντας με το TCP έχουμε το ακόλουθο σχεδιάγραμμα:

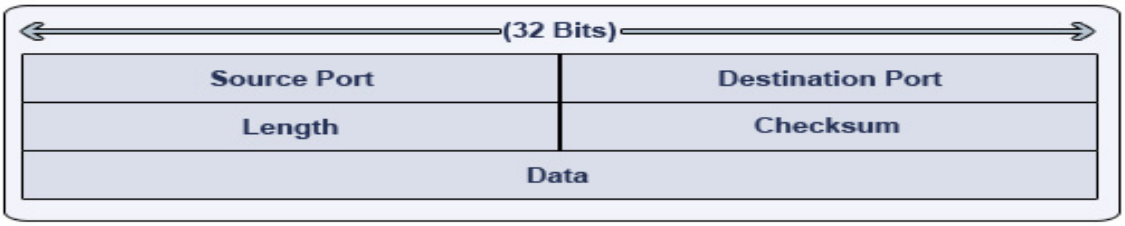


Εικόνα 3: TCP segment (πηγή από διαδίκτυο).

- Η Source port και η Destination port , η καθεμιά έχει μήκος 16 bits. Η θύρα source είναι η θύρα στο μηχάνημα που μεταδίδει το πακέτο, ενώ η θύρα προορισμού είναι η θύρα στο μηχάνημα-στόχο.
- Ο αύξων αριθμός(sequence number) (32 bits) και αριθμό αναγνώρισης (acknowledge number) (32 bits) επιτρέπουν στο TCP να παρακολουθεί τα πακέτα για να εξασφαλιστεί ότι φτάνουν αξιόπιστα στο στόχο.
- Offset είναι το μήκος της επικεφαλίδας TCP (4 bits).
- Το Rsvd είναι δεσμευμένο για μελλοντική χρήση. Είναι ένα πεδίο 4 bit και πρέπει να είναι μηδέν.
- Τα bit ελέγχου (flags) περιέχουν 8 του 1-bit σημαίες.
- Το Window (16 bits), καθορίζει τον αριθμό των bytes του δέκτη που είναι διατεθειμένος να αποδεχτεί.
- Το Checksum (16 bits) χρησιμοποιείται για τον έλεγχο σφαλμάτων του TCP τόσο των header όσο και των δεδομένων.

Ουσιαστικά το παραπάνω σχεδιάγραμμα δείχνει πώς είναι το πρωτόκολλο μεταφοράς TCP , από ποια τμήματα αποτελείται και στη συνέχεια θα δειχθεί πώς συμπεριφέρεται στην ανίχνευση θυρών. Βασικά διαφαίνεται ο τρόπος μεταφοράς των δεδομένων σε ένα δίκτυο.

Ομοίως παρουσιάζεται και το δεύτερο πρωτόκολλο, το UDP, το οποίο είναι σαφώς διαφορετικό από το TCP ως προς τη δομή και τη λειτουργία.



Εικόνα 4: UDP segment (πηγή από διαδίκτυο).

- Ομοίως με το TCP , η επικεφαλίδα του UDP έχει επίσης Source port και Destination port, καθένα από τα οποία έχει 16 bits μήκος. Η μεν πρώτη θύρα σχετίζεται με την μετάδοση του πακέτου από το μηχάνημα - πομπό, ενώ η δεύτερη είναι η θύρα στο μηχάνημα-στόχο.
- UDP Length είναι το μήκος της επικεφαλίδας UDP.
- το Checksum (16 bits) χρησιμοποιείται για τον έλεγχο σφαλμάτων της επικεφαλίδας UDP και των δεδομένων.

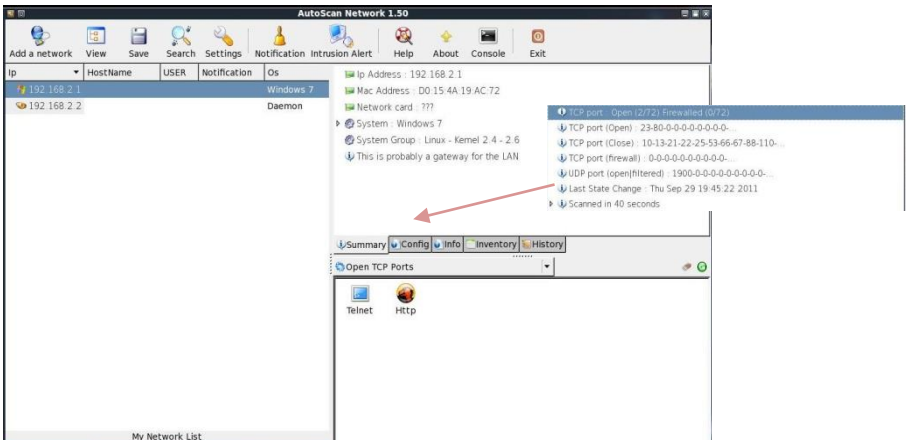
Παρατηρείται στο σημείο αυτό ότι δεν υπάρχει αριθμός σειράς και αναγνώρισης ενώ απουσιάζουν και τα Bits Ελέγχου. Σε μια επικείμενη κακόβουλη επίθεση ο εισβολέας μπορεί να παρατηρήσει τα ακόλουθα σε μια UDP θύρα. Πρώτον ότι το μηχάνημα - στόχος ανταποκρίνεται στέλνοντας ένα πακέτο UDP , το οποίο αν ληφθεί σημαίνει ότι η συγκεκριμένη θύρα είναι ανοικτή. Δεύτερον, αν η θύρα είναι κλειστή τότε το μηχάνημα – στόχος στέλνει ένα ICMP μήνυμα, όπως «ICMP port Unreachable». Παρόλα αυτά αν τα μηνύματα που εστάλησαν είναι και αυτά κάποια άλλα ICMP unreachable τότε αυτό είναι σημάδι ότι η θύρα φιλτράρεται μέσω του τείχους προστασίας. Τελευταία και τρίτη παρατήρηση είναι ότι αν η θύρα UDP δε στείλει

κανένα μήνυμα τότε σημαίνει ότι είτε είναι κλειστή, είτε το πακέτο μπλοκάρεται είτε η απάντηση-ανταπόκριση μπλοκάρεται.

Με βάση τα παραπάνω καταλήγουμε στο συμπέρασμα ότι η ανίχνευση μιας θύρας UDP είναι λιγότερο αξιόπιστη από την ανίχνευση μιας αντίστοιχης θύρας TCP. Παρακάτω φαίνεται πρακτικά μέσα από κάποια εργαλεία του BackTrack πώς είναι εφικτή η ανίχνευση θυρών.

2.4α.1 : Autoscan και Netifera.

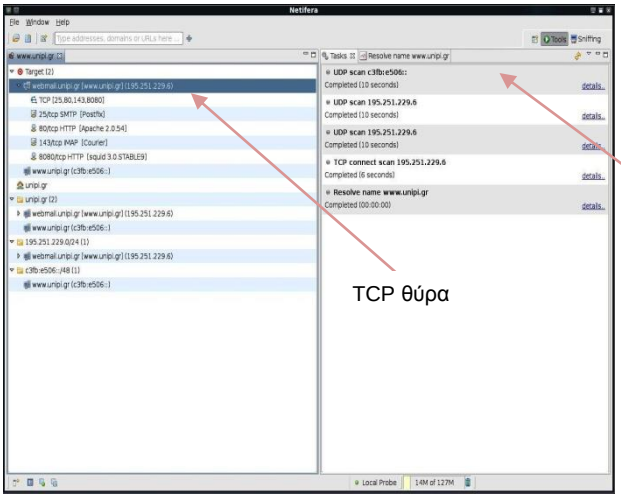
Το AutoScan είναι ένα γραφικό εργαλείο βασισμένο στη σάρωση δικτύου και μπορεί να χρησιμοποιηθεί για να βρει διαθέσιμους hosts σε ένα δίκτυο. Μπορεί επίσης να χρησιμοποιηθεί για να βρείτε ανοικτές θύρες και να συλλέξει πληροφορίες σχετικά με τον τύπο του λειτουργικού συστήματος που χρησιμοποιεί κάθε host. Επίσης το AutoScan χρησιμοποιεί έναν πράκτορα για το GUI για να συλλέξει και να σκιαγραφήσει τους hosts-στόχους και να στείλει τα αποτελέσματα πίσω στο GUI μέσω μιας εσωτερικής TCP σύνδεσης. Το πλεονέκτημα αυτού του εργαλείου είναι ότι είναι πολύ εύκολο στη χρήση του και μπορεί ταυτόχρονα να ανιχνεύει παραπάνω από ένα δίκτυα. Παρακάτω θα δειχθεί εν συντομία πως λειτουργεί ένα τέτοιο εργαλείο το οποίο βρίσκεται στο ακόλουθο μενού του BackTrack: **Backtrack / Network Mapping / Portscanning / Autoscan :**



Εικόνα 5 : Autoscan.

Ανοίγοντας την εφαρμογή ένας οδηγός - Wizard μας κατευθύνει στην όλη διαδικασία επιλέγοντας το δίκτυο που θέλουμε να ανιχνεύσουμε. Στο παράδειγμα που ακολουθεί ανιχνεύεται το δίκτυο μέσα στο οποίο κινείται ο υπολογιστής που χρησιμοποιούμε. Στην παραπάνω εικόνα μπορεί να παρατηρήσει κάποιος ότι το εργαλείο έχει αναγνωρίσει πολλά στοιχεία του δικτύου. Έχει βρει ποιο λειτουργικό σύστημα έχει ο υπολογιστής (μέσω του δικτύου), ποια είναι η MAC διεύθυνση, καθώς και στην καρτέλα Config φαίνεται ποια είναι η θύρα TCP και ποια η θύρα UDP. Επίσης παρέχει και κάποιες άλλες πληροφορίες που στο σημείο αυτό δε θα μας απασχολήσουν.

Παρόμοιο εργαλείο με το Autoscan είναι και το Netifera , το οποίο λίγο πολύ με κάπως διαφορετικό τρόπο παρέχει αντίστοιχες πληροφορίες. Εν συντομία φαίνονται στην παρακάτω εικόνα τα αποτελέσματα της λειτουργίας του , όπου το προς ανίχνευση δίκτυο είναι εκείνο στο οποίο ανήκει το Πανεπιστήμιο Πειραιώς:



Εικόνα 6: Netifera.

2.4α.2 : Nmap.

Άλλο ένα πολύ σημαντικό εργαλείο που βοηθά στην ανακάλυψη του στόχου, στο OS fingerprinting αλλά και στην ανίχνευση θυρών είναι και το Nmap. Το εργαλείο αυτό δίνει τη δυνατότητα να συλλεχθεί μια πληθώρα πληροφοριών για τη συγκεκριμένη IP που έχει τεθεί ως στόχος. Ένα παράδειγμα θα γίνει πιο κατανοητό και για το λόγο αυτό παρατίθεται το κάτωθι πληκτρολογώντας στη γραμμή εντολών :

 # nmap -v -A www.unipi.gr

Και εξάγονται τα ακόλουθα αποτελέσματα:

root@bt:~# nmap -v -A www.unipi.gr
Starting Nmap 5.35DC1 (http://nmap.org) at 2011-09-26 12:04 UTC
NSE: Loaded 49 scripts for scanning.
Initiating Ping Scan at 12:04
Scanning www.unipi.gr (195.251.229.6) [4 ports]
Completed Ping Scan at 12:04, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:04
Completed Parallel DNS resolution of 1 host. at 12:04, 0.92s elapsed
Initiating SYN Stealth Scan at 12:04
Scanning www.unipi.gr (195.251.229.6) [1000 ports]
Discovered open port 80/tcp on 195.251.229.6
Discovered open port 25/tcp on 195.251.229.6
Discovered open port 143/tcp on 195.251.229.6
Discovered open port 8080/tcp on 195.251.229.6
Completed SYN Stealth Scan at 12:04, 12.38s elapsed (1000 total ports)
Initiating Service scan at 12:04
Scanning 4 services on www.unipi.gr (195.251.229.6)
Completed Service scan at 12:04, 6.07s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against www.unipi.gr (195.251.229.6)
Retrying OS detection (try #2) against www.unipi.gr (195.251.229.6)
Initiating Traceroute at 12:04
Completed Traceroute at 12:04, 0.03s elapsed

Initiating Parallel DNS resolution of 10 hosts. at 12:04
Completed Parallel DNS resolution of 10 hosts. at 12:04, 0.39s elapsed
NSE: Script scanning 195.251.229.6.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 12:04
Completed NSE at 12:04, 1.00s elapsed
Nmap scan report for www.unipi.gr (195.251.229.6)
Host is up (0.021s latency).
rDNS record for 195.251.229.6: spider.unipi.gr
Not shown: 994 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Cisco PIX sanitized smtpd
80/tcp open http Apache httpd 2.0.54 ((Unix) DAV/2)
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-favicon: Unknown favicon MD5: A27C72D908D00A330B9D60A2B50EE240
|_html-title: \xD0\xC1\xCD\xC5\xD0\xC9\xD3\xD4\xC7\xCC\xC9\xCF \xD0\xC5\xC9\xD1\xC1\xC9\xD9\xD3 - \xC1\xF1\xF7\xE9\xEA\xDE \xD3\xE5\xEB\xDF\xE4\xE1
110/tcp closed pop3
143/tcp open imap Courier Imapd (released 2005)
|_imap-capabilities: THREAD=ORDEREDSUBJECT QUOTA THREAD=REFERENCES UIDPLUS ACL2=UNION SORT ACL IMAP4rev1 IDLE NAMESPACE CHILDREN
443/tcp closed https
8080/tcp open http-proxy Squid webproxy 3.0.STABLE9
Device type: general purpose
Running (JUST GUESSING) : Sun Solaris 10 (87%)
Aggressive OS guesses: Sun Solaris 10 (87%), Sun Solaris 10 (SPARC) (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 67.184 days (since Thu Jul 21 07:40:01 2011)
Network Distance: 10 hops
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Device: firewall
TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 7.26 ms netfaster.wlan (192.168.2.1)
2 26.00 ms loopback2004.med01.dsl.hol.gr (62.38.0.170)
3 24.58 ms 62.38.40.213
4 28.09 ms 62.38.97.165
5 25.34 ms 62.38.96.177
6 22.94 ms tengigaeth02-01.adr01.ar.hol.gr (62.38.96.118)
7 22.36 ms vlan23.grix00.core.hol.gr (62.38.96.218)
8 21.13 ms grnet.gr-ix.gr (83.212.8.1)
9 19.95 ms clientRouter.unipi.eie-2.access-link.grnet.gr (195.251.24.134)
10 19.39 ms spider.unipi.gr (195.251.229.6)
Read data files from: /usr/share/nmap

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 28.90 seconds

Raw packets sent: 3080 (139.108KB) | Rcvd: 49 (7.100KB)

Παρατηρείται λοιπόν πως λαμβάνονται πληροφορίες για live hosts , για λειτουργικά συστήματα που λειτουργούν στους hosts που ανιχνεύθηκαν, με ποιες θύρες TCP και UDP επικοινωνούν και λοιπά. Ένα εύκολο και πλήρες εργαλείο που ουσιαστικά συμπυκνώνει τα τρία βήματα σε ένα. Δηλαδή τη συλλογή πληροφοριών , την ανακάλυψη στόχου και την καταμέτρηση στόχου. Όπως γίνεται αντιληπτό η δουλειά του ελεγκτή γίνεται αρκετά πιο εύκολη. Καλό θα ήταν τα βήματα όμως να είναι πιο ξεκάθαρα και εργαλεία όπως το Nmap να χρησιμοποιούνται ως εργαλεία επαλήθευσης των όσων βρέθηκαν με προηγούμενες διαδικασίες και εντολές. Στην ίδια κατηγορία εργαλείων για την ανίχνευση θυρών ανήκουν τα :

- **Unicorn scan και**
- **Zenmap**

2.4β: Ανίχνευση υπηρεσιών.

Επόμενο στην ανάλυση είναι το δεύτερο μέρος της καταμέτρησης του στόχου, που είναι η ανίχνευση υπηρεσιών. Πρόκειται ουσιαστικά για μια μέθοδο που χρησιμοποιείται για να μάθει ο tester την έκδοση των υπηρεσιών που είναι διαθέσιμες σε μια συγκεκριμένη θύρα στο σύστημα προορισμού. Αυτές οι πληροφορίες έκδοσης είναι σημαντικές, γιατί με αυτές ο ελεγκτής διείσδυσης μπορεί να αναζητήσει την ασφάλεια των τρωτών σημείων που υπάρχουν για τη συγκεκριμένη έκδοση λογισμικού.

Ένα συχνό φαινόμενο που όσων αφορά στις θύρες είναι οι αλλαγές που μπορεί να υποστούν από τους administrators του συστήματος. Πολλοί αλλάζουν τον αριθμό της θύρας που «ακούει» μια υπηρεσία, όπως για παράδειγμα τη θύρα 22 σε 2222. Αυτό έχει ως αποτέλεσμα αν ο ελεγκτής κάνει μόνο μια ανίχνευση θυρών τότε μπορεί να μη βρει την υπηρεσία. Πρόβλημα αντιμετωπίζει και όταν ασχολείται με ιδιόκτητες εφαρμογές που τρέχουν σε μη τυπικές θύρες. Με την εφαρμογή μιας ανίχνευσης υπηρεσιών αυτά τα δύο προβλήματα λύνονται και η υπηρεσία υπάρχει πιθανότητα να βρεθεί έστω και αν «ακούει» σε διαφορετική θύρα.

2.4β.1 : Amap.

Για να μπορέσει να διεξαχθεί μια ανίχνευση υπηρεσιών και να συνεχιστεί στο δεύτερο μέρος του βήματος της καταμέτρησης του στόχου θα χρησιμοποιηθούν δύο πολύ απλά εργαλεία. Το πρώτο ονομάζεται Amap και είναι ένα εργαλείο που μπορεί να χρησιμοποιηθεί για να ελέγξει την εφαρμογή που εκτελείται σε μια συγκεκριμένη θύρα . Βασικά λειτουργεί στέλνοντας ένα πακέτο – σκανδάλη (trigger packet) στη θύρα και ύστερα κάνει τη σύγκριση των απαντήσεων που παίρνει στην βάση δεδομένων του. Τέλος θα εκτυπώσει την ταύτιση που βρίσκει. Μέσω του BackTrack το βρίσκεται στη διαδρομή **Backtrack / Network Mapping / Service Fingerprinting / Amap** και σε μια γραμμή εντολών πληκτρολογούνται τα εξής:

#amap -bq target IP port , βάζοντας την IP που θέλουμε να ανιχνεύσουμε και την αντίστοιχη θύρα που ακούει. Τα αποτελέσματα της διαδικασίας αυτής είναι τα ακόλουθα:

root@bt:~# amap -bq www.unipi.gr 80

amap v5.2 (www.thc.org/thc-amap) started at 2011-09-30 20:00:47 - MAPPING mode

Protocol on 195.251.229.6:80/tcp matches http - banner: HTTP/1.1 200 OK\r\nDate Fri, 30 Sep 2011 165900 GMT\r\nServer Apache/2.0.54 (Unix) DAV/2\r\nSet-Cookie SessId=e30fa90a350aea; expires=Mon, 27 Sep 2021 165900 GMT\r\nConnection close\r\nContent-Type text/html\r\n\r\n\n<!DOCTYPE HTML PUBLIC "-//W3C//DTD HT

Protocol on 195.251.229.6:80/tcp matches http-apache-2 - banner: HTTP/1.1 200 OK\r\nDate Fri, 30 Sep 2011 165900 GMT\r\nServer Apache/2.0.54 (Unix) DAV/2\r\nSet-Cookie SessId=e30fa90a350aea; expires=Mon, 27 Sep 2021 165900 GMT\r\nConnection close\r\nContent-Type text/html\r\n\r\n\n<!DOCTYPE HTML PUBLIC "-//W3C//DTD HT

Protocol on 195.251.229.6:80/tcp matches webmin - banner: HTTP/1.1 200 OK\r\nDate Fri, 30 Sep 2011 165901 GMT\r\nServer Apache/2.0.54 (Unix) DAV/2\r\nSet-Cookie SessId=e30fa90a350aea; expires=Mon, 27 Sep 2021 165901 GMT\r\nConnection close\r\nContent-Type text/html\r\n\r\n\n<!DOCTYPE HTML PUBLIC "-//W3C//DTD HT

amap v5.2 finished at 2011-09-30 20:00:53

Παρατηρείται από τα παραπάνω ότι τα αποτελέσματα που επιστρέφει το Amap απαρτίζονται από κάποιες υπηρεσίες που ακούν στη θύρα 80, που έχουμε ως παράδειγμα , μέσω του πρωτοκόλλου TCP.

2.4β.2 : Httpsquash.

Συνεχίζοντας ένα δεύτερο εργαλείο είναι το επονομαζόμενο Httpsquash. Είναι ένα εργαλείο για τη σάρωση του διακομιστή HTTP, για banner grapping, και ανάκτηση δεδομένων. Επιπλέον υποστηρίζει IPv6, προσαρμοσμένους τύπους αιτημάτων, και προσαρμοσμένων διευθύνσεων URL αιτημάτων. Πηγαίνοντας στο μενού **Backtrack / Network Mapping /Service Fingerprinting / Httpsquash** και πληκτρολογώντας την εντολή :

#./httpsquash -r IP address , έχουμε τα κάτωθι

root@bt:/pentest/enumeration/complemento/httpsquash# ./httpsquash -r www.unipi.gr

FOUND: 195.251.229.6 80

HTTP/1.1 200 OK

Date: Fri, 30 Sep 2011 17:01:57 GMT

Server: Apache/2.0.54 (Unix) DAV/2

Set-Cookie: SessId=e30fa90a350aea; expires=Mon, 27 Sep 2021 17:01:57 GMT

Transfer-Encoding: chunked

Content-Type: text/html

2.4γ : Ανίχνευση VPN (virtual private network).

Στην υποενότητα αυτή θα εξεταστεί το τρίτο κομμάτι της καταμέτρησης στόχου που είναι η ανίχνευση ενός VPN δικτύου. Τι είναι όμως το VPN; Η απάντηση θα είναι πιο κατανοητή ένα μικρό παράδειγμα. Αρκετά χρόνια πριν, όταν ένα γραφείο ήθελε να συνδεθεί με το γραφείο του επικεφαλής, χρειαζόταν να οριστεί μια ειδική γραμμή δικτύου μεταξύ των γραφείων. Το κύριο μειονέκτημα αυτής της μεθόδου ήταν το κόστος. Μια συγκεκριμένη γραμμή δικτύου ήταν αρκετά ακριβή. Η χρήση ενός VPN δικτύου επιτρέπει σε ένα γραφείο να συνδεθείτε με τα κεντρικά κάνοντας χρήση του δημόσιου δικτύου (Internet). Το κόστος της χρήσης ενός δημόσιου δικτύου είναι πολύ φθηνότερο από ό, τι χρησιμοποιώντας μια ειδική γραμμή. Με το VPN, το γραφείο θα είναι σε θέση να χρησιμοποιήσει την εφαρμογή, στο κεντρικό γραφείο, σαν να βρίσκεται στο τοπικό δίκτυο (LAN). Η σύνδεση αυτή προστατεύεται από κρυπτογράφηση. Όσον αφορά στο VPN υπάρχουν τρείς κατηγορίες:

1. **IPSec-based VPN**
2. **OpenVPN και**
3. **SSL-based VPN**

2.4γ.1 : IKE-scan.

Όσον αφορά στην ανίχνευση ενός VPN δικτύου θα χρησιμοποιηθεί το IKE-scan. Πρόκειται για ένα εργαλείο ασφάλειας που μπορεί να χρησιμοποιηθεί για να ανακαλύψει, να αποτυπώσει και να κάνει τεστ σε IPSec VPN συστήματα. Λειτουργεί με την αποστολή IKE φάση-1 πακέτα με το VPN server και εμφανίζει τις απαντήσεις που έλαβε. Το Internet Key Exchange (IKE) είναι το κλειδί ανταλλαγής και ταυτότητας, ένας μηχανισμός δηλαδή που χρησιμοποιείται από το IPsec. Στη διαδρομή **Backtrack / Network Mapping / VPN / Ike-scan** βρίσκεται αυτό το εργαλείο. Σε ένα παράθυρο γραμμής εντολών πληκτρολογείται η ακόλουθη εντολή:

#ike-scan -M -v IP address

Ως παράδειγμα θα χρησιμοποιηθεί η IP του VPN που παρέχεται από το πανεπιστήμιο Πειραιώς.

#ike-scan -M -v 191.251.224.73

Τα αποτελέσματα της ανίχνευσης είναι τα παρακάτω:

DEBUG: pkt len=336 bytes, bandwidth=56000 bps, int=52000 us

Starting ike-scan 1.9 with 32 hosts (http://www.nta-monitor.com/tools/

ike-scan/)

192.168.109.99 Main Mode Handshake returned HDR=(CKYR=

4c6950d4ff3bede2) SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024

LifeType=Seconds LifeDuration=28800) VID=afcad71368a1f1c96b8696

fc77570100 (Dead Peer Detection v1.0)

Από τα παραπάνω παρατηρείται ότι εξάγονται κάποιες πολύ βασικές πληροφορίες όπως οι ακόλουθες:

- Κρυπτογράφηση με 3DES (triple DES)
- Κατακερματισμός με SHA1
- Authentication με PSK
- Diffie-Hellman group 2 και
- SA lifetime = 28800

Στην παρούσα ενότητα της καταμέτρησης του στόχου παρουσιάστηκαν τα επιμέρους μέρη και τα ειδικά εργαλεία που δίνουν στον ελεγκτή τη δυνατότητα να τα χρησιμοποιήσει μέσω του BackTrack για την εξαγωγή συμπερασμάτων και πληροφοριών. Το 4ο αυτό βήμα αποτελεί μια βασική πηγή πληροφοριών για να τη συνέχεια του τεστ διείσδυσης. Για μια ακόμη φορά επισημαίνεται η σημαντικότητα της ακεραιότητας του κάθε βήματος για τη σωστή διεξαγωγή του τεστ.

2.5 : Χαρτογράφηση της ευπάθειας ή vulnerability mapping.

Η χαρτογράφηση της ευπάθειας είναι μια διαδικασία αναγνώρισης και ανάλυσης των κρίσιμων ρωγμών ασφαλείας στο περιβάλλον - στόχο. Η ορολογία αυτή είναι επίσης γνωστή και ως «εκτίμηση τρωτότητας». Ουσιαστικά είναι ένας από τους βασικούς τομείς του προγράμματος διαχείρισης της ευπάθειας μέσω του οποίου οι έλεγχοι ασφαλείας της πληροφοριακής υποδομής μπορούν να αναλυθούν έναντι γνωστών και άγνωστων τρωτών σημείων. Μόλις οι εργασίες της συλλογής πληροφοριών, της ανακάλυψης, και της καταμέτρησης έχουν ολοκληρωθεί, είναι ώρα να διερευνηθούν τα τρωτά σημεία που μπορεί να υπάρχουν στην υποδομή-στόχο που θα μπορούσαν να θέσουν σε κίνδυνο το στόχο με την παραβίαση του απορρήτου, της ακεραιότητας, και της διαθεσιμότητας του συστήματος των επιχειρήσεων.

Βασικά η παρούσα ενότητα θα καταπιαστεί με:

- την έννοια των δύο γενικών κατηγοριών των τρωτών σημείων - **τοπική και απομακρυσμένη**
- την ταξινόμηση της ευπάθειας, που δείχνει με ποιά βιομηχανικά πρότυπα μπορεί να καταταχθεί κάθε ευπάθεια σύμφωνα με κοινό ενοποιητικό της μοτίβο και
- μια σειρά από εργαλεία για την ασφάλεια που μπορούν να βοηθήσουν στην εύρεση και την ανάλυση των τρωτών σημείων που υπάρχουν σε ένα περιβάλλον-στόχο. Τα εργαλεία που θα παρουσιάσουμε κατηγοριοποιούνται ανάλογα με τη βασική λειτουργία τους σε μια αξιολόγηση της διαδικασίας ασφάλειας.

Υπάρχουν τρεις κύριες κατηγορίες ευπαθειών με τις οποία μπορεί να γίνει η διάκριση για τους τύπους των ρωγμών (τοπική και απομακρυσμένη). Οι κατηγορίες αυτές χωρίζονται εν γένει στο σχεδιασμό, την υλοποίηση και τη λειτουργική κατηγορία. Τα τρωτά σημεία του σχεδιασμού ανακαλύπτονται λόγω των αδυναμιών που διαπιστώνονται στις προδιαγραφές του λογισμικού, τα τρωτά σημεία της εφαρμογής είναι οι τεχνικές δυσλειτουργίες ασφαλείας που

βρέθηκαν στον κώδικα ενός συστήματος, και τα επιχειρησιακά τρωτά σημεία είναι αυτά που μπορεί να προκύψουν λόγω της ακατάλληλης διαμόρφωσης και ανάπτυξης ενός συστήματος σε ένα συγκεκριμένο περιβάλλον. Με βάση αυτές τις τρεις αδυναμίες των συστημάτων, παρουσιάζονται δύο γενικές κατηγορίες τρωτών σημείων που μπορεί να χωρέσουν σε οποιαδήποτε κατηγορία ευπάθειας που αναφέρθηκε παραπάνω.

2.5.1α : Τοπικά τρωτά σημεία.

Θα ξεκινήσει η ανάλυση με την αναφορά στα τοπικά τρωτά σημεία ενός περιβάλλοντος - στόχου. Ένα σύστημα στο οποίο ο επιτιθέμενος απαιτεί τοπική πρόσβαση, ώστε να προκαλέσει την ευπάθεια εκτελώντας ένα κομμάτι κώδικα, είναι γνωστό και ως «τοπικό τρωτό σημείο» (local vulnerability). Εκμεταλλευόμενος αυτού του τύπου την ευπάθεια, ένας εισβολέας μπορεί να αυξήσει τα δικαιώματα πρόσβασης και να αποκτήσουν απεριόριστη πρόσβαση στο σύστημα ηλεκτρονικών υπολογιστών. Παρακάτω αναφέρεται ένα παράδειγμα για να γίνει πιο κατανοητό αυτό που αναφέρθηκε.

Έστω ότι ο Γιάννης έχει τοπική πρόσβαση σε MS Windows Server 2008 (32-bit πλατφόρμα). Η πρόσβασή του έχει περιοριστεί από τον διαχειριστή με την εμφύτευση μιας πολιτικής ασφάλειας που θα δεν του επιτρέπει να εκτελέσει την συγκεκριμένη εφαρμογή. Τώρα, κάτω από ακραίες συνθήκες ανακάλυψε ότι χρησιμοποιώντας ένα κακόβουλο κομμάτι κώδικα μπορεί να κερδίσει πρόσβαση σε επίπεδο συστήματος ή πυρήνα στο σύστημα του υπολογιστή. Αξιοποιώντας αυτό την πολύ γνωστή ευπάθεια (όπως για παράδειγμα την, CVE-2010-0232, GP παγίδα Handler nt! KiTrap0D) κερδίζει κλιμακωτά προνόμια, επιτρέποντάς του να εκτελεί όλα τα διοικητικά καθήκοντα και να αποκτήσει απεριόριστη πρόσβαση στην εφαρμογή. Αυτό δείχνει ένα σαφές πλεονέκτημα που λαμβάνεται από τον κακόβουλο αντίπαλο ή κάποιους τοπικούς χρήστες να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στο σύστημα.

2.5.1β : Απομακρυσμένα τρωτά σημεία.

Συνεχίζοντας, η ανάλυση προχωράει με τα απομακρυσμένα τρωτά σημεία που μπορεί να έχει ένα υπολογιστικό σύστημα. Με λίγα λόγια ένα σύστημα στο οποίο ο επιτιθέμενος δεν έχει καμία πρόσβαση, αλλά η ευπάθεια που μπορεί να εξακολουθεί να είναι αντικείμενο εκμετάλλευσης από την ενεργοποίηση της μέσω ενός κακόβουλου κομματιού κώδικα από το δίκτυο είναι γνωστή ως «απομακρυσμένη ευπάθεια». Αυτός ο τύπος ευπάθειας επιτρέπει σε έναν εισβολέα να αποκτήσει απομακρυσμένη πρόσβαση στο σύστημα ηλεκτρονικών υπολογιστών χωρίς να αντιμετωπίζει οποιοδήποτε φυσικό ή τοπικό εμπόδιο.

Ένα ακόμη παράδειγμα με το γνωστό από πριν Γιάννη θα καταστήσει τα πράγματα πιο κατανοητά. Ο Γιάννης και η Μαρία είναι συνδεδεμένοι στο Internet ατομικά. Και οι δύο έχουν διαφορετικές διευθύνσεις IP και είναι γεωγραφικά διασκορπισμένοι σε δύο διαφορετικές περιοχές. Υποτίθεται ότι ο υπολογιστής της Μαρίας με Windows XP λειτουργικό σύστημα κρατά μυστικές πληροφορίες βιοτεχνολογίας. Επίσης υποτίθεται ότι ο Γιάννης γνωρίζει ήδη το λειτουργικό σύστημα και τη διεύθυνση IP του μηχανήματος της Μαρίας. Ο Γιάννης τώρα απεγνωσμένα ψάχνει για μια λύση που μπορεί να του επιτρέψει να αποκτήσει απομακρυσμένη πρόσβαση στον υπολογιστή της. Εν τω μεταξύ, γνωρίζει ότι η MS08-067 Windows Server Service ευπάθεια μπορεί να εύκολα να αξιοποιηθεί ενάντια του μηχανήματος των Windows XP από απόσταση. Εκείνος τότε την ενεργοποιεί και κερδίζει πλήρη πρόσβαση στον υπολογιστή της Μαρίας.

Με τα παραπάνω μπορεί κάποιος να αντιληφθεί την σοβαρότητα των ευπαθειών και τις δυσκολίες που μπορεί να προκαλέσουν σε ένα υπολογιστικό σύστημα. Η πρόσβαση σε μη εξουσιοδοτημένες πληροφορίες μέσω κακόβουλου λογισμικού τοπικά ή απομακρυσμένα μπορεί να οδηγήσει σε ανεπανόρθωτες ζημιές και παράλληλα καταστρέφει την ασφάλεια και την αξιοπιστία του συστήματος. Για το λόγο αυτό η διεξαγωγή penetration tests γίνεται απαραίτητη για να αποφεύγονται τέτοια περιστατικά και αν τυχόν έχουν ήδη συμβεί να δίδεται κάποια λύση στο πρόβλημα.

2.5.2 : Ταξινόμηση ευπαθειών.

Έχει παρατηρηθεί ότι με μια αύξηση στον αριθμό των τεχνολογιών κατά τα τελευταία χρόνια, έχουν γίνει διάφορες προσπάθειες για την εφαρμογή των βέλτιστων ταξινομήσεων που θα μπορούσαν να κατηγοριοποιήσουν το κοινό σύνολο των τρωτών σημείων. Ωστόσο, καμιά ταξινόμηση δεν έχει παραχθεί για να αντιπροσωπεύσει όλα τα κοινά λάθη κωδικοποίησης, που μπορούν να επηρεάσουν την ασφάλεια ενός συστήματος. Αυτό οφείλεται στο γεγονός ότι μια ενιαία ευπάθεια μπορεί να εμπίπτει σε περισσότερες από μία κατηγορίες ή τάξεις. Επιπλέον, κάθε πλατφόρμα συστήματος έχει τη δική της βάση για την συνδεσιμότητα, την πολυπλοκότητα, και την επεκτασιμότητα ώστε να αλληλεπιδρά με το περιβάλλον της. Είναι επίσης σημαντικό να σημειωθεί ότι οι περισσότερες από τις ταξινομήσεις έχουν ήδη υλοποιηθεί σε μια σειρά εργαλείων για την αξιολόγηση της ασφάλειας για τη διερεύνηση των προβλημάτων λογισμικού ασφαλείας σε πραγματικό χρόνο.

Δεδομένου ότι η κύρια λειτουργία κάθε μιας από αυτές τις ταξινομήσεις είναι να οργανώσει σε ομάδες ασφαλείας τα τρωτά σημεία που μπορούν να χρησιμοποιηθούν από τους επαγγελματίες της ασφάλειας και της ανάπτυξη για να προσδιοριστούν τα συγκεκριμένα λάθη που μπορεί να έχουν αντίκτυπο στην ασφάλεια και την ακεραιότητα ενός υπολογιστικού συστήματος, καμιά μεμονωμένη ταξινόμηση δε θα πρέπει να θεωρείται πλήρης ή ακριβής.

2.5.3 : OpenVas (Open Vulnerability Assessment System).

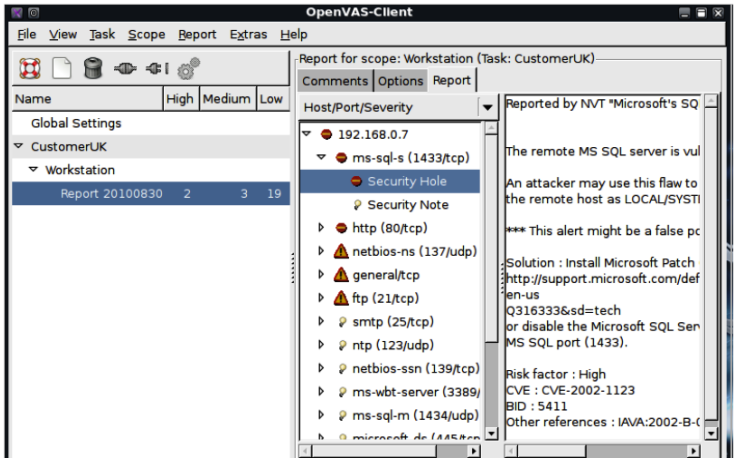
Αφού τελείωσε η αναφορά στις κατηγορίες των ευπαθειών και την ταξινόμησή τους σε κατηγορίες, η ενότητα αυτή θα ασχοληθεί με την παρουσίαση κάποιων εργαλείων που βοηθούν στον εντοπισμό και την ανάλυση τέτοιων ευπαθειών. Ένα πολύ σημαντικό εργαλείο όσον αφορά στην ανίχνευση ευπαθειών είναι το OpenVas. Ουσιαστικά είναι μια συλλογή ολοκληρωμένων εργαλείων και υπηρεσιών ασφαλείας, που προσφέρει μια ισχυρή πλατφόρμα για τη διαχείριση των ευπαθειών. Έχει αναπτυχθεί για την βάση της αρχιτεκτονικής client-server, όπου ο πελάτης θα ζητήσει ένα συγκεκριμένο σύνολο δοκιμών τρωτότητας του δικτύου έναντι του στόχου του από το διακομιστή. Η αρθρωτή και στιβαρή σχεδίασή του επιτρέπει την εκτέλεση δοκιμών ασφαλείας ενώ παράλληλα είναι διαθέσιμο για μια σειρά από λειτουργικά συστήματα (Linux/Win32). Κάποια από τα βασικά στοιχεία του OpenVas είναι τα παρακάτω:

- **OpenVAS Scanner**
- **OpenVAS Client**
- **OpenVAS Manager**
- **Greenbone Security Assistant και**
- **OpenVAS Administrator**

Στο σημείο αυτό επισημαίνεται ότι στην παρούσα ενότητα επιδιώκεται ο τρόπος λειτουργίας αυτού του εργαλείου και για το λόγο αυτό δεν γίνεται αναφορά εκτενώς και με ορισμούς στα βασικά του στοιχεία όπως παρατέθηκαν παραπάνω. Επίσης η συλλογή του OpenVas περιλαμβάνει και εργαλεία από αυτά που αναφέρθηκαν σε προηγούμενα βήματα του Penetration testing , όπως το amap , το ike-scan κλπ. Μέσω του BackTrack βρίσκεται το εργαλείο στην διαδρομή : **Backtrack / Vulnerability Identification / OPENVAS / OpenVas .** Πριν ξεκινήσει η ανίχνευση ευπαθειών όμως γίνονται κάποια βήματα για τη ρύθμιση του Openvas.

1. Δημιουργούμε ένα νέο πιστοποιητικό
2. Δημιουργούμε ένα νέο χρήστη
3. Ρυθμίζουμε το server
4. Συνδέουμε τον client με το server
5. Ορίζουμε τα κριτήρια ανίχνευσης
6. Ξεκινάμε την ανίχνευση

Έτσι κάνοντας τα παραπάνω το εργαλείο είναι έτοιμο για χρήση. Ορίζοντας τη διεύθυνση-στόχο και έχοντας βάλει όλες τις παραμέτρους εξάγεται το ακόλουθο αποτέλεσμα:



Εικόνα 7: Openvas results.

Τέλος το OpenVAS είναι ένα ισχυρό λογισμικό εκτίμηση τρωτότητας που μας επιτρέπει να αξιολογήσουμε το στόχο που έχουμε θέσει προς ανίχνευση ενάντια σε όλα τα κρίσιμα προβλήματα ασφάλειας, ενώ παράλληλα παρέχει μια ολοκληρωμένη έκθεση με τη μέτρηση του κινδύνου, τις λεπτομέρειες της ευπάθειας, λύσεις, και αναφορές σε online πόρους. Σημειώνεται ότι στην παρούσα φάση της εργασίας δε μας ενδιαφέρει η λεπτομέρεια όσον αφορά στα εργαλεία που παρουσιάζουμε. Πιο ουσιαστικά θα τα δούμε σε επόμενο μέρος κατά τη διάρκεια της ανάλυσης και της ανίχνευσης μιας εφαρμογής δηλαδή σε πιο πρακτικό κομμάτι.

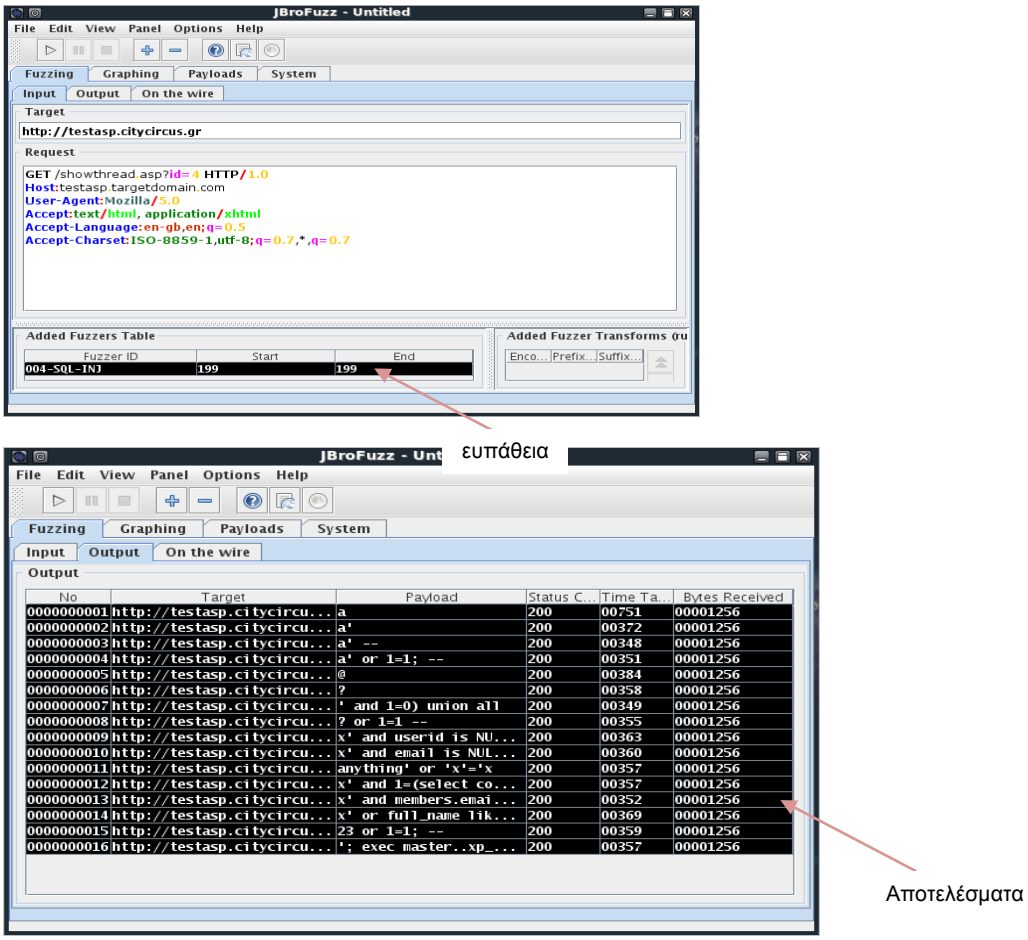
2.5.4 : Ασαφής ανάλυση με το JBroFuzz.

Στη χαρτογράφηση των ευπαθειών μια άλλη διαδεδομένη μέθοδος είναι και η ασαφής ανάλυση. Με τον όρο αυτό νοείται μια σκληρή τεχνική δοκιμής λογισμικού που χρησιμοποιείται από τους ελεγκτές και προγραμματιστές για να δοκιμάσουν τις εφαρμογές τους για απροσδόκητη, άκυρη, και τυχαία σειρά εισαγωγής δεδομένων. Η δραστηριότητα αυτή αποκαλύπτει ορισμένα από τα μεγαλύτερα τρωτά σημεία του λογισμικού, τα οποία διαφορετικά δεν θα ήταν δυνατόν να ανακαλύψουν. Αυτά τα τρωτά σημεία περιλαμβάνουν υπερχειλίσεις μνήμης, format strings, code injections, dangling pointers, race conditions, συνθήκες άρνησης παροχής υπηρεσιών, και πολλά άλλα είδη των τρωτών σημείων. Οποιαδήποτε αξιόπιστη πηγή δεδομένων εισόδου θεωρείται ότι είναι ανασφαλής και ασυνεπής. Για παράδειγμα, ένα όριο εμπιστοσύνης μεταξύ της εφαρμογής και του χρήστη του Διαδικτύου είναι απρόβλεπτο. Η ασαφής ανάλυση λοιπόν είναι μια σχετικά απλή και αποτελεσματική λύση που μπορεί να ενσωματωθεί σε μια διασφάλιση ποιότητας και διαδικασία δοκιμών ασφάλειας. Για το λόγο αυτό, είναι επίσης γνωστή και ως δοκιμή ευρωστίας ή αρνητικός έλεγχος.

Ένα από τα εργαλεία που χρησιμοποιούνται για την ασαφή ανάλυση είναι και το JBroFuzz. Είναι μια πολύ γνωστή πλατφόρμα για ασαφή έλεγχο web εφαρμογών. Υποστηρίζει αιτήματα web μέσω HTTP και HTTPS πρωτοκόλλων. Επίσης παρέχοντας μια απλή διεύθυνση URL για τον τομέα προορισμού και επιλέγοντας το τμήμα της αίτησης web για ασαφή ανάλυση, ένας ελεγκτής μπορεί είτε να επιλέξει για τα να κάνει τις δικές του ρυθμίσεις ή να χρησιμοποιήσει τις προκαθορισμένες που υπάρχουν ήδη στη βάση δεδομένων. (για παράδειγμα, cross-site scripting, SQL Injection, υπερχείλιση μνήμης, String Format Λάθη, και ούτω καθεξής) για να παράγει κακόβουλα αιτήματα βασισμένα σε παλαιότερο γνωστά τρωτά σημεία και να τα στείλει στον web server-στόχο. Οι αντίστοιχες απαντήσεις στη συνέχεια, θα καταγραφούν για περαιτέρω επιθεώρηση και ανάλυση. Με βάση το είδος των δοκιμών που εκτελούνται, αυτές τις απαντήσεις ή τα αποτελέσματα θα πρέπει να διερευνηθούν με το χέρι, προκειμένου να αναγνωρίσουν κάθε δυνατή κατάσταση.

Το εργαλείο αυτό όπως και όλα τα προηγούμενα διατίθεται από το BackTrack και εντοπίζεται μέσω του ακόλουθου μενού: **Backtrack / Vulnerability Identification /Fuzzers / JBroFuzz**. Βάζοντας την προς ανάλυση διεύθυνση URL, ρυθμίζοντας ποια ευπάθεια θέλει ο

tester να αναπαράγει και τι αιτήματα HTTP θέλει να «τρέχουν» στην εφαρμογή, εξάγονται τα ακόλουθα αποτελέσματα:



Εικόνα 8 : JBroFuzz.

Από τις παραπάνω εικόνες παρατηρούνται τα αποτελέσματα που εξάγονται για τη συγκεκριμένη ευπάθεια που επιλέχθηκε , μέσα από μια μεγάλη γκάμα τρωτών σημείων που παρέχει αυτό το εργαλείο , που εφαρμόστηκε σε ένα συγκεκριμένο στόχο. Θα μπορούσε να επιλέγεται κάθε φορά και διαφορετική ευπάθεια, αλλά για λόγους ευκολίας της ανάλυσης παρουσιάζεται μόνο μία.

Τέλος αναφέρονται με συντομία και κάποια άλλα εργαλεία που ανήκουν στην κατηγορία της χαρτογράφησης των ευπαθειών και είτε αυτά ανήκουν στην ασαφή ανάλυση είτε στη αξιολόγηση εφαρμογών είτε στην αξιολόγηση βάσεων δεδομένων. Αυτά τα εργαλεία είναι :

- Bunny
- SQLNinja
- SQLBrute
- Paros Proxy
- SQLMap
- SNMPenum
- Nikto2
- WebScarab

Επίσης ως προς τη χαρτογράφηση ευπαθειών υπάρχουν και εργαλεία για συγκεκριμένες εφαρμογές ,όπως της Cisco το Cisco auditing tool και άλλα τέτοια παρεμφερή. Έτσι τελειώνει και η ανάλυση του 5ου βήματος το οποίο ουσιαστικά εκφράζει την πραγματική ουσία του τεστ διείσδυσης που είναι η ανακάλυψη των τρωτών σημείων μιας εφαρμογής ώστε

να μπορέσουν να βρεθούν τρόποι για να αντιμετωπιστούν και να θωρακιστεί τελικά η εφαρμογή από μελλοντικές κακόβουλες επιθέσεις.

2.6: Κοινωνική μηχανική ή Social Engineering.

Στην ενότητα αυτή θα αναλυθεί ένα ακόμη βήμα που αφορά στη διαδικασία του penetration testing, αλλά που είναι αρκετά διαφορετικό με ότι έχει παρουσιαστεί μέχρι στιγμής. Δεν έχει να κάνει με εργαλεία και εφαρμογές ,αλλά κάτι πιο ουσιαστικό : τον ανθρώπινο παράγοντα. Θα παρουσιαστεί λοιπόν η λεγόμενη κοινωνική μηχανική. Με τον όρο αυτό νοείται η πρακτική της μάθησης και της απόκτησης πολύτιμων πληροφοριών από την αξιοποίηση των τρωτών σημείων που βασίζονται στον άνθρωπο. Είναι μια τέχνη εξαπάτησης που θεωρείται ότι είναι ζωτικής σημασίας για τον ελεγκτή διείσδυσης όταν υπάρχει έλλειψη διαθέσιμων πληροφοριών σχετικά με την στόχο που μπορεί να αξιοποιηθεί. Επειδή οι άνθρωποι είναι ο πιο αδύναμος κρίκος στην άμυνα της ασφάλειας σε οποιοδήποτε οργανισμό, αυτή είναι και το πιο ευάλωτο στρώμα στην υποδομή ασφαλείας. Οι άνθρωποι είναι κοινωνικά όντα και η φύση τους, τους καθιστά ευάλωτους σε επιθέσεις τύπου κοινωνικής μηχανικής. Αυτές οι επιθέσεις έχουν τη δυνατότητα να αποκτήσουν εμπιστευτικές πληροφορίες ή να αποκτήσουν πρόσβαση στην απαγορευμένη περιοχή. Η κοινωνική μηχανική λαμβάνει διάφορες μορφές επίθεσης, και η καθεμιά από αυτές περιορίζεται από τη φαντασία κάποιου με βάση την επιρροή και την κατεύθυνση σύμφωνα με τις οποίες αυτή η επίθεση εκτελείται.

Από την οπτική γωνία της ασφάλειας, η κοινωνική μηχανική είναι ένα ισχυρό όπλο που χρησιμοποιείται ως τέχνη για τη χειραγώγηση των ανθρώπων για να επιτευχθεί ο απαιτούμενος στόχος. Σε πολλούς οργανισμούς, αυτή η πρακτική μπορεί να αξιολογηθεί για να διασφαλίσει την ακεραιότητα της ασφάλειας των εργαζομένων και να διερευνήσει ταυτόχρονα τις αδυναμίες που μπορεί να βρίσκονται εντός των εκπαιδευμένων μέλη του προσωπικού. Είναι, επίσης, σημαντικό να σημειωθεί ότι η πρακτική της κοινωνικής μηχανικής είναι κάτι πάρα πολύ κοινό, και έχει εγκριθεί από μια σειρά από επαγγελματίες, συμπεριλαμβανομένων και των δοκιμαστών διείσδυσης, των κλεφτών ταυτότητας, των επιχειρηματικών εταίρων, των recruiters εργασίας, των πωλητών, των μεσαζόντων πληροφοριών, των κατασκόπων κυβέρνησης, των δυσαρεστημένων υπαλλήλων, ακόμα και των παιδιών στην καθημερινή τους ζωή. Στις κατηγορίες αυτές, αυτό που κάνει τη διαφορά είναι το κίνητρο με το οποίο εκτελείται η τακτική έναντι του στόχου.

Έχει παρατηρηθεί από επιστήμονες ότι οι ανθρώπινες ψυχολογικές ικανότητες εξαρτώνται από τον αριθμό των αισθήσεων του εγκεφάλου παρέχοντας στοιχεία για την αντίληψη της πραγματικότητας. Αυτό το φυσικό φαινόμενο κατηγοριοποιεί τις ανθρώπινες αισθήσεις στην όραση, ακοή, γεύση, αφή, όσφρηση, ισορροπία και επιτάχυνση, θερμοκρασία, τον πόνο, και την κατεύθυνση. Όλες αυτές οι αισθήσεις χρησιμοποιούν αποτελεσματικά, αναπτύσσουν, και διατηρούν τον τρόπο που βλέπουμε τον κόσμο. Από την προοπτική της κοινωνικής μηχανικής, κάθε πληροφορία που έχει ανακτηθεί ή εξαχθεί από το στόχο μέσω της δεσπόζουσας αίσθησης (οπτική ή ακουστική), τις κινήσεις των ματιών (οπτική επαφή, λεκτικές διαφορές), τις εκφράσεις του προσώπου (έκπληξη, ευτυχία, φόβος, θλίψη, θυμό, ή αηδία), και άλλες αφηρημένες οντότητες που παρατηρήθηκαν, μπορεί να προσθέσουν μεγαλύτερη πιθανότητα επιτυχίας. Τις περισσότερες φορές, είναι απαραίτητο για έναν κοινωνικό μηχανικό να επικοινωνεί με το στόχο άμεσα προκειμένου να λάβει εμπιστευτικές πληροφορίες ή πρόσβαση σε κάποια απαγορευμένη ζώνη. Η επικοινωνία αυτή μπορεί να γίνει είτε φυσικά ή με υποβοηθούμενη ηλεκτρονική τεχνολογία.

2.6.1 : Διαδικασία επίθεσης.

Στο σημείο αυτό επειδή η εφαρμογή της κοινωνικής μηχανικής δεν έχει καμία επίσημη διαδικασία ή προσέγγιση που μπορεί να ακολουθήσει κάποιος θα παρουσιαστούν εν συντομία κάποια βασικά βήματα που απαιτούνται για την έναρξη μιας κοινωνικής μηχανικής επίθεσης εναντίον κάποιου στόχου. Τα βήματα αυτά είναι τα κάτωθι:

- Συλλογή πληροφοριών: συγκομιδή εταιρικών διευθύνσεων e-mail στο Web με τη χρήση προηγμένων εργαλείων μηχανής αναζήτησης, συλλογή προσωπικών

πληροφοριών για τους ανθρώπους που εργάζονται , για την οργάνωση μέσω απευθείας σύνδεσης σε κοινωνικά δίκτυα και λοιπά.

- Εντοπισμός ευάλωτων σημείων: μόλις έχει επιλεγεί ο εξ ‘ απορρήτων, θα συνεχιστεί ο καθορισμός της σχέσης εμπιστοσύνης και φιλικότητας. Αυτό θα εξασφαλίσει ότι μια προσπάθεια επίθεσης σε εμπιστευτικές εταιρικές πληροφορίες δεν θα βλάψει ή προειδοποιήσει τον στόχο.
- Σχεδιασμός της επίθεσης: είτε άμεση είτε έμμεση επίθεση με ηλεκτρονικά μέσα, αυτό αποτελεί επιλογή του επιτιθέμενου. Με βάση τον προσδιορισμό των ευπαθών σημείων εισόδου, μπορεί εύκολα να προσδιοριστεί η διαδρομή και η μέθοδος της επίθεσης.
- Εκτέλεση της επίθεσης: κατά το τελικό στάδιο, σχεδιάζεται η επίθεση που θα πρέπει να εκτελεστεί με αυτοπεποίθηση και υπομονή για να παρακολουθηθούν και να αξιολογηθούν τα αποτελέσματα του στόχου.

Με βάση προηγούμενες πληροφορίες από κάποιες άλλες επιθέσεις κοινωνικής μηχανικής έχουν υπολογιστεί πέντε διαφορετικοί τύποι επίθεσης. Πρώτον υπάρχει η **μίμηση**. Σε αυτό το είδος επίθεσης πείθει ο «εισβολέας» το στόχο του προσποιώντας ότι είναι κάποιος άλλος ή ένα πρόσωπο πολύ γνωστό. Για παράδειγμα, για την απόκτηση πληροφοριών από μια τράπεζα-στόχο, το phishing θα ήταν η τέλεια λύση εκτός εάν ο στόχος δεν διαθέτει λογαριασμό ηλεκτρονικού ταχυδρομείου. Δεύτερον υπάρχει η **ανταπόδοση** (reciprocation). Με τούτο νοείται η πράξη της ανταλλαγής μια χάρης για να ληφθεί κάποιο αμοιβαίο πλεονέκτημα. Αυτός ο τύπος κοινωνικής μηχανικής δέσμευσης μπορεί να περιλαμβάνει μια απλή και μακροπρόθεσμη επιχειρηματική σχέση. Με την αξιοποίηση της εμπιστοσύνης μεταξύ των επιχειρηματικών φορέων θα μπορούσε εύκολα να χαρτογραφηθεί το στόχος για να αποκτηθούν οι απαραίτητες πληροφορίες.

Τρίτον υπάρχει η **«επιρρεαστική αρχή»** (influential authority), όπου είναι μια μέθοδος επίθεσης που κάποιος χειρίζεται τις επιχειρησιακές ευθύνες του στόχου. Αυτό το είδος της κοινωνικής επίθεσης είναι μερικές φορές μέρος μιας μεθόδου «μίμησης». Οι άνθρωποι, από τη φύση τους, ενεργούν με αυτοματοποιημένο τρόπο ώστε να δέχονται οδηγίες από την αρχή τους ή ανώτερα διευθυντικά στελέχη, ακόμη και αν το ένστικτό τους, δείχνει ότι ορισμένες οδηγίες δεν θα πρέπει να επιδιωχθούν. Η φύση όμως μας κάνει ευάλωτους σε ορισμένες τέτοιες απειλές. Ως επόμενος τύπος επίθεσης υπάρχει η «**έλλειψη»**. Λαμβάνοντας την καλύτερη ευκαιρία, ειδικά αν φαίνεται σπάνιο, είναι μια από τις πιο άπληστες καταστάσεις στη φύση των ανθρώπινων όντων. Η μέθοδος αυτή περιγράφει τον τρόπο να δώσει την ευκαιρία σε κάποιον για προσωπικό κέρδος τους. Ένα παράδειγμα θα κάνει πιο κατανοητό αυτό τον τύπο επίθεσης. Ο γνωστός και πάλι Γιάννης από τα προηγούμενα παραδείγματα θα καταστήσει τα πράγματα πιο κατανοητά. Έστω ότι θέλει να αποκτήσει προσωπικές πληροφορίες από τους φοιτητές του πανεπιστημίου του Πειραιά εκτός από τις ηλεκτρονικές τους διευθύνσεις τις οποίες ήδη γνωρίζει. Αποφασίζει λοιπόν να στείλει email σε όλους προσφέροντας το τελευταίο μοντέλο του IPHONE, θέλοντας μόνο οι φοιτητές να απαντήσουν στο email στέλνοντας τα στοιχεία τους (όνομα , επώνυμο κλπ). Επειδή λοιπόν το έχει σχεδιάσει σωστά πολλοί φοιτητές πιστεύουν ότι θα αποκτήσουν δωρεάν τη συσκευή, χωρίς αυτό βέβαια να είναι αλήθεια , και πολλοί από αυτούς πέφτουν σε αυτή την παγίδα. Σε μέγεθος επιχείρησης τέτοια τεχνάσματα χρησιμοποιούνται για τη μεγιστοποίηση του κέρδους από τις διαφημίσεις.

Τελευταίο ,αλλά όχι λιγότερο σημαντικό είναι οι **κοινωνικές σχέσεις**. Ο άνθρωπος από τη φύση του χρειάζεται κάποια μορφή κοινωνικής σχέσης για να μοιραστεί τις σκέψεις, τα συναισθήματα του, και τις ιδέες του. Η πιο ευάλωτη πλευρά της κάθε κοινωνικής σχέσης είναι η "σεξουαλικότητα". Όπως είναι γνωστό, το αντίθετο φύλο προσελκύει πάντα και απευθύνει έκκληση προς το άλλο. Λόγω αυτού του έντονου συναισθήματος και της εμπιστοσύνης μπορεί να καταλήξει κάποιος να αποκαλύψει οποιαδήποτε στοιχεία στον αντίπαλο. Είναι γνωστοί ήδη πολλοί ιστότοποι όπως το Facebook και το Twitter όπου αναπτύσσονται κοινωνικές σχέσεις. Και ας μη λησμονείται το γεγονός ότι όσο πιο αποτελεσματικές και γεμάτες εμπιστοσύνη σχέσεις δημιουργεί κάποιος τόσο πιο πολύ «κοινωνικά μηχανοποιεί» το στόχο του.

2.6.2 : Εργαλεία κοινωνικής μηχανικής.

Στην αρχή της ανάλυσής για την κοινωνική μηχανική αναφέρθηκε ότι δε θα υπάρχει αναφορά σε εφαρμογές και εργαλεία. Η ανάπτυξη της τεχνολογίας όμως έχει καταφέρει να δημιουργήσει λογισμικά τα οποία βοηθούν στον τομέα αυτό. Όπως και τα προηγούμενα εργαλεία έτσι και αυτά που θα παρουσιστούν παρακάτω διατίθενται μέσα από το BackTrack 4. Βρίσκεται στη διάθεση του tester το εργαλείο SET (social engineer tools) στη διαδρομή : **Backtrack / Penetration / Social Engineering Toolkit** . Στην οθόνη που εμφανίζεται , υπάρχει το ακόλουθο μενού από το οποίο επιλέγει κάποιος τι ακριβώς θέλει να κάνει.

Select from the menu:

1. Spear-Phishing Attack Vectors

2. Website Attack Vectors

3. Infectious Media Generator

4. Create a Payload and Listener

5. Mass Mailer Attack

6. Teensy USB HID Attack Vector

7 Update the Metasploit Framework

8. Update the Social-Engineer Toolkit

9. Help, Credits, and About

10. Exit the Social-Engineer Toolkit

Έστω ότι επιλέγεται το 1ο. Το εργαλείο καθοδηγεί στο πώς ακριβώς θα εργαστεί κάποιος χρησιμοποιώντας μια επίθεση phishing. Έτσι εμφανίζονται και οι παρακάτω επιλογές:

1. Perform a Mass Email Attack

2. Create a FileFormat Payload

3. Create a Social-Engineering Template

4. Return to Main Menu

Επιλέγοντας για άλλη μια φορά από το μενού που παρατίθεται ,έστω ότι επιλέγεται το 3, προχωρεί κάποιος σε διαδικασίες κοινωνικής μηχανικής. Για να μη μακρηγορούμε άνευ ουσίας κάθε επιλογή μεταφέρει το χρήστη σε διαφορετικό μενού επιλογών καλύπτοντας μια μεγάλη γκάμα από την ανάλυση της κοινωνικής μηχανικής όπως έχουμε αναφέρει και παραπάνω. Το τι θα χρησιμοποιήσει κάποιος εξαρτάται από το στόχο και από αυτό που έχει ζητηθεί από τον οργανισμό. Όπως έχει αναφερθεί και παραπάνω περισσότερες λεπτομέρειες οδηγούν σε καλύτερη ανάλυση και καλύτερα τελικά αποτελέσματα.

Όπως γίνεται φανερό υπάρχουν σε μια διαδικασία penetration testing και πτυχές εκτός των άψυχων μηχανημάτων , λειτουργικών συστημάτων και λοιπά. Υπάρχουν διαδικασίες που έχουν να κάνουν με τον ανθρώπινο παράγοντα. Άξιο υπενθύμισης είναι το γεγονός ότι ο άνθρωπος αποτελεί το πιο αδύνατο σημείο στην ασφάλεια πληροφοριών και για το λόγο αυτό πρέπει να εξετάζεται και ο τρόπος με τον οποίο μπορούν να αντληθούν πληροφορίες από εκείνους που εργάζονται σε έναν οργανισμό. Πολλές φορές ο κίνδυνος και οι διαρροές προέρχονται εκ των έσω και όχι απαραιτήτως από κακόβουλους εξωτερικούς παράγοντες. Οι «τρύπες» σε ένα σύστημα μπορεί να δημιουργηθούν και από κάποιον από το σύνολο εκείνων που το χρησιμοποιούν. Χρειάζεται λοιπόν ανάλυση όλων των δυνατών παραγόντων και υπολογισμός όλων των παραμέτρων για να οδηγηθούμε σε ένα επιτυχημένο τεστ και κατ' επέκταση σε αύξηση της ασφάλειας και μείωση του κινδύνου.

2.7 : Εκμετάλλευση του στόχου ή target exploitation.

Στην ενότητα αυτή θα αναπτυχθεί ένα πολύ σημαντικό κομμάτι των τεστ διείσδυσης που είναι η εκμετάλλευση του στόχου. Αφού έχει παρέλθει το στάδιο της ανίχνευσης των ευπαθειών και των τρωτών σημείων ενός συστήματος πρέπει να βρεθούν και τρόποι ώστε να γίνουν εκμεταλλεύσιμα και αξιοποιήσιμα όλα όσα έχουν βρεθεί . Για να εξερευνηθούν οι καλύτερες επιλογές που είναι διαθέσιμες για την εκμετάλλευση του στόχου θα πρέπει να πραγματοποιηθεί

προσεκτική εξέταση, έρευνα, και χρήση προηγμένων εργαλείων και τεχνικών. Η διαδικασία αξιοποίησης ολοκληρώνει ουσιαστικά τη λειτουργία διείσδυσης. Ωστόσο, θα μπορούσαν να υπάρξουν περιπτώσεις όπου ο ελεγκτής μπορεί να κληθεί να προσπαθήσει να αποκτήσει πρόσβαση σε βάθος μέσα στο δίκτυο κλιμακώνοντας τα προνόμιά του σε επίπεδο administrator, προκειμένου να αποδείξει την παρουσία του. Οι εν λόγω απαιτήσεις είναι προκλητικές και σίγουρα αβέβαιες. Ωστόσο, όσο ειδικός και ειδικευμένος επαγγελματίας και να είναι κάποιος, μπορεί πάντα να ψάχνει για αυτοματοποίηση και ελέγχους που θα μπορούσαν να βοηθήσουν στο να αποφευχθούν και τέτοιου είδους εμπόδια.

Η κατανόηση όμως των δυνατοτήτων ενός συγκεκριμένου λογισμικού ή ενός προϊόντος υλικού μπορεί να αποτελέσει την αφετηρία για τη διερεύνηση των τρωτών σημείων που θα μπορούσαν να υπάρξουν σε αυτό το προϊόν. Η διεξαγωγή της έρευνας μιας ευπάθειας δεν είναι εύκολο, ούτε εργασία που γίνεται με ένα κλικ. Έτσι, απαιτείται από τον ελεγκτή να έχει μια ισχυρή βάση για την ανάλυση της ασφάλειας. Ουσιαστικά θα πρέπει να έχει ή να γνωρίζει τα παρακάτω:

- **προγραμματιστικές ικανότητες-δεξιότητες**
- **αντίστροφη μηχανική**, δηλαδή να συναγάγει έναν κώδικα από ένα δεδομένο σύστημα, χωρίς προηγούμενη γνώση σχετικά με τις εσωτερικές του εργασίες
- **εξειδικευμένα εργαλεία**, όπως προγράμματα εντοπισμού σφαλμάτων, απαγωγείς δεδομένων, fuzzers, profilers.
- **Εκμεταλλευσιμότητα και κατασκευή** κώδικα για ένα ευπαθές μιας εφαρμογής.

Ανάλογα βέβαια με τον τύπο και την κατηγορία των ευπαθειών που ανακαλύπτεται, είναι πολύ σημαντικό να ακολουθείται μια συγκεκριμένη στρατηγική που μπορεί να επιτρέψει την εκτέλεση ενός αυθαίρετου κώδικα ή εντολής στο σύστημα - στόχο. Οι ελεγκτές διείσδυσης, μπορούν πάντα να ψάχνουν για «παραθυράκια» που θα μπορούσαν να έχουν ως αποτέλεσμα πρόσβαση στο λειτουργικό σύστημα του στόχου.

Για πολλά χρόνια, μια σειρά από ευπάθειες έχουν αναφερθεί δημόσια και μερικές από αυτές αποκαλύφθηκαν με την απόδειξη της ιδέας (Proof of Concept- PoC) και τον εκμεταλλεύσιμο κώδικα που παραγόταν (όπως είδαμε σε προηγούμενη ενότητα) για να αποδειχθεί η σκοπιμότητα και η βιωσιμότητα της ευπάθειας στο συγκεκριμένο λογισμικό ή την εφαρμογή που εντοπίστηκε. Παρόλα αυτά πολλές εξακολουθούν να παραμένουν χωρίς αντιμετώπιση. Αυτή η ανταγωνιστική εποχή της εξεύρεσης διαθέσιμων πληροφοριών για τις ευπάθειες καθιστά ευκολότερη για τους δοκιμαστές διείσδυσης τη γρήγορη αναζήτηση και την ανάκτηση των βέλτιστων διαθέσιμων τρόπων αντιμετώπισης που μπορεί να ταιριάζουν στο στόχο τους. Έτσι λοιπόν υπάρχουν στο διαδίκτυο βάσεις δεδομένων που κρατούν τέτοιου είδους πληροφορίες και μπορούμε οποιαδήποτε στιγμή να ανατρέξουμε εκεί για να δούμε λεπτομέρειες σχετικά με την ή τις ευπάθειες που έχουμε εντοπίσει. Τονίζεται βέβαια ότι δεν έχουν καταγραφεί όλες οι ευπάθειες ,γεγονός που κάνει την δουλειά ενός ελεγκτή διείσδυσης πιο ενδιαφέρουσα και προκλητική. Παρακάτω αναφέρονται ενδεικτικά κάποιες από αυτές τις διαθέσιμες βάσεις δεδομένων εκ των οποίων σε μία από αυτές στηρίζεται και το BackTrack.

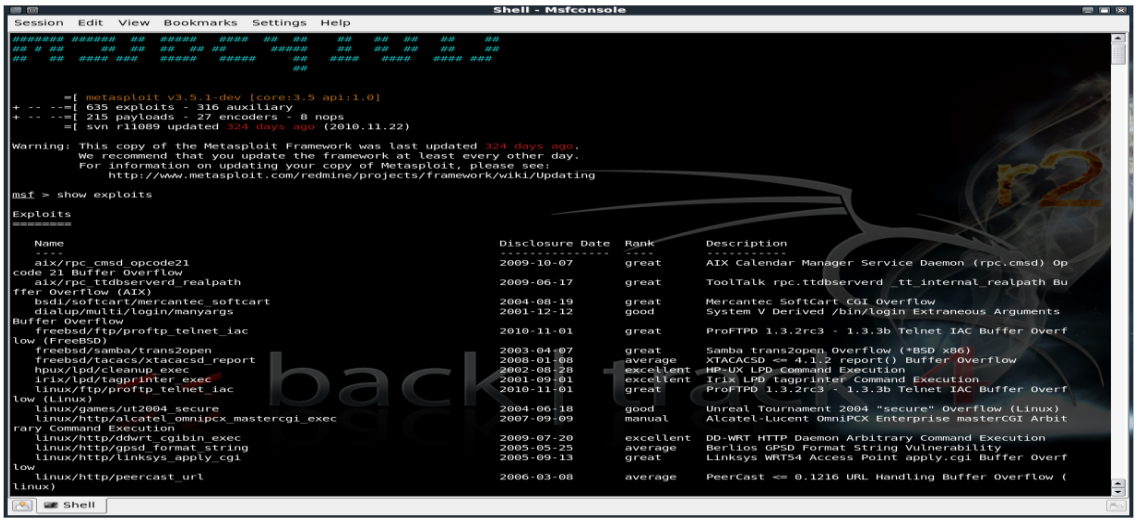
Βάση δεδομένων	**Ιστοσελίδα**
Bugtraq SecurityFocus	http://www.securityfocus.com
OSVDB Vulnerabilities	http://osvdb.org
Packet Storm	http://www.packetstormsecurity.org
VUPEN Security	http://www.vupen.com
National Vulnerability Database	http://nvd.nist.gov
Offensive Security Exploits Database	http://www.exploit-db.com

BackTrack

2.7.1 : Metasploit Framework.

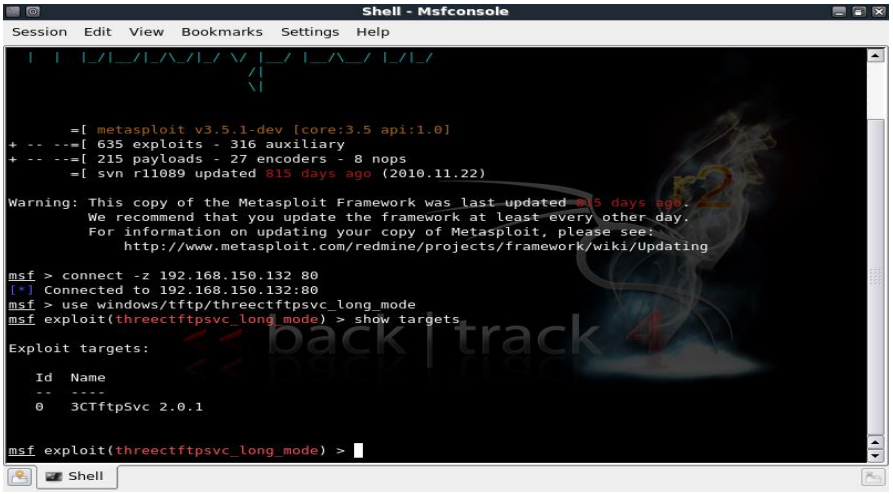
Για την εκμετάλλευση λοιπόν του στόχου και των ευπαθειών που έχουν ανακαλυφθεί σε αυτόν υπάρχουν εξειδικευμένα εργαλεία που βοηθούν σε αυτή τη διαδικασία. Ένα από αυτά και ίσως το πιο γνωστό είναι το **Metasploit Framework**. Έχει αναπτυχθεί σε γλώσσα προγραμματισμού Ruby και υποστηρίζει την διαμόρφωση και μοντελοποίηση, τέτοιες που να καθιστούν ευκολότερη για τον δοκιμαστή διείσδυσης με άριστη γνώση προγραμματισμού την επέκταση ή την ανάπτυξη προσαρμοσμένων plugins και εργαλείων. Επίσης είναι εύκολη η παραγωγή διάφορων σεναρίων που βοηθούν στην αύξηση της παραγωγικότητας και την απόκτηση εμπειρίας για έναν tester. Το εργαλείο μας λοιπόν είναι χωρισμένο σε βιβλιοθήκες , interfaces και λειτουργικές μονάδες (modules). Επίσης διαθέτει πολλά μικρότερα εργαλεία που μας βοηθούν στην εκμετάλλευση του στόχου. Ένα από τα πιο δυνατά εργαλεία που ανήκουν στο Metasploit είναι και το **Msfconsole**. Με αυτό θα καταπιαστεί η ανάλυση και θα παρουσιαστούν απλώς κάποια βασικά του στοιχεία.

Ξεκινώντας από τη διαδρομή **Backtrack / Penetration / Metasploit Exploitation Framework / Framework Version 3 / Msfconsole** . Στο παράθυρο που ανοίγει ο ελεγκτής μπορεί να πληκτρολογήσει ,show exploits, και έτσι να εμφανιστούν όλες οι λεπτομέρειες για τα εκμεταλλεύσιμα στοιχεία που υπάρχουν στη βάση δεδομένων του. Έτσι έχουμε ως ακολούθως:



Εικόνα 9: Msfconsole exploits.

Με αντίστοιχο τρόπο εμφανίζονται πληροφορίες για τα auxiliary modules ,για τα payloads για τις γεννήτριες NOP , για τα λειτουργικά συστήματα που υπάρχουν στο περιβάλλον – στόχο καθώς και πιο εξειδικευμένες ρυθμίσεις και επιλογές. Έτσι δίδεται μια μεγάλη γκάμα από στοιχεία που μπορούν να χρησιμοποιηθούν για να διεξαχθεί το τεστ διείσδυσης και συγκεκριμένα το βήμα της «εκμετάλλευσης του στόχου». Ένα πρώτο παράδειγμα όπως θα φανεί στην παρακάτω εικόνα είναι το πώς γίνεται η σύνδεση με μια συγκεκριμένη IP, η χρήση ενός συγκεκριμένου exploit καθώς και η εύρεση των στόχων:



Εικόνα 10: Σύνδεση με συγκεκριμένη IP/θύρα και χρήση συγκεκριμένου exploit.

Παρόμοια εργαλεία είναι το **Ninja 101 drills** , και το **Msfcli**. Στο σημείο αυτό θα τονίζεται ότι μέσα από το Metasploit και τα «υπο-εργαλεία» του μπορούν να διεξαχθούν ενέργειες όπως τις παρουσιάστηκαν σε προηγούμενα βήματα. Για παράδειγμα μπορούμε να εξαχθούν πληροφορίες σχετικά με τα λειτουργικά συστήματα όπως το αναφέρθηκε πιο πάνω σε προηγούμενη ενότητα μέσω της χαρτογράφησης των ευπαθειών και του OS-fingerprinting. Έτσι έχουμε:

msf > db_driver sqlite3

msf > db_connect , σύνδεση της βάσης δεδομένων

msf > load db_tracker

msf > db_nmap -T Aggressive -sV -n -O -v 192.168.0.7
Starting Nmap 5.00 (http://nmap.org) at 2010-11-11 22:34 UTC
NSE: Loaded 3 scripts for scanning.
Initiating ARP Ping Scan at 22:34
Scanning 192.168.0.7 [1 port]
Completed ARP Ping Scan at 22:34, 0.00s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:34
Scanning 192.168.0.7 [1000 ports]
Discovered open port 445/tcp on target IP
Discovered open port 135/tcp on target IP
Discovered open port 25/tcp on target IP
Discovered open port 139/tcp on target IP
Discovered open port 3389/tcp on target IP
Discovered open port 80/tcp on target IP
Discovered open port 443/tcp on target IP
Discovered open port 21/tcp on target IP
Discovered open port 1025/tcp on target IP
Discovered open port 1433/tcp on target IP
Completed SYN Stealth Scan at 22:34, 3.04s elapsed (1000 total ports)
Initiating Service scan at 22:34
Scanning 10 services on 192.168.0.7
Completed Service scan at 22:35, 15.15s elapsed (10 services on 1

host)
Initiating OS detection (try #1) against target IP
...
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
25/tcp open smtp Microsoft ESMTP 6.0.2600.2180
80/tcp open http Microsoft IIS httpd 5.1
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn
443/tcp open https?
445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open msrpc Microsoft Windows RPC
1433/tcp open ms-sql-s Microsoft SQL Server 2005 9.00.1399; RTM
3389/tcp open microsoft-rdp Microsoft Terminal Service
MAC Address: 00:0B:6B:68:19:91 (Wistron Neweb)
Device type: general purpose
Running: Microsoft Windows 2000|XP|2003
OS details: Microsoft Windows 2000 SP2 - SP4, Windows XP SP2 - SP3, or
Windows Server 2003 SP0 - SP2

Ομοίως υπάρχουν και άλλες λειτουργίες οι οποίες δεν θα αναφερθούν ,διότι δεν υπόκεινται στο σκοπό της συγκεκριμένης εργασίας. Όπως έχει αναφερθεί πολλάκις λεπτομέρειες θα υπάρξουν και πρακτικά διεξάγοντας ένα τεστ διείσδυσης σε μια ειδικά διαμορφωμένη Web εφαρμογή. Παρατηρείται συνεπώς πως υπάρχουν τρόποι και εργαλεία για να διασταυρώσει ένας tester τα στοιχεία που έχει ήδη συλλέξει. Όλα εξαρτώνται βεβαίως από το σύστημα που ελέγχεται , αλλά και από τι έχει ζητηθεί να γίνει , σε πιο βαθμό και σε τι βάθος. Ο ελεγκτής δεν πρέπει να λειτουργεί αυθαίρετα, αλλά πάντοτε μέσα στα πλαίσια που το έχει ορίσει ο οργανισμός και το συμβόλαιο που έχει υπογράψει.

2.8 : Κλιμάκωση προνομίων ή privilege escalation.

Η ενότητα αυτή θα ασχοληθεί με τη λεγόμενη, κλιμάκωση των προνομίων. Τι νοείται όμως με αυτό; Σε προηγούμενες ενότητες ακολουθήθηκαν κάποια βήματα και χρησιμοποιήθηκαν ειδικά εργαλεία που οδήγησαν στην ανακάλυψη ευπαθειών στο περιβάλλον – στόχο , αλλά και στην εκμετάλλευση των αποτελεσμάτων που βρέθηκαν, τα λεγόμενα **exploits** που αναφέρθηκαν και παραπάνω. Σκοπός λοιπόν είναι με τις ενέργειες που έχουν γίνει να βρεθούν λογαριασμοί και να αποκτηθούν ανώτερα δικαιώματα (του administrator για παράδειγμα) στο σύστημα. Κάτι τέτοιο δεν είναι εφικτό πάντοτε, οπότε εδώ έρχεται να βοηθήσει το επόμενο βήμα του pen test που είναι η κλιμάκωση προνομίων. Ουσιαστικά είναι η απόκτηση δικαιωμάτων σε επίπεδο διαχειριστή ξεφεύγοντας έτσι από τα περιορισμένα δικαιώματα που είχε ο ελεγκτής πριν. Κάτι τέτοιο είναι εφικτό μέσω :

- επίθεσης σε κωδικούς πρόσβασης που χρησιμοποιούν προνομιακοί λογαριασμοί
- sniffing στο δίκτυο για απόκτηση ονομάτων χρηστών και των κωδικών τους σε αυτούς τους λογαριασμούς
- spoofing σε πακέτα δικτύου προνομιακών λογαριασμών για να τρέξει μια συγκεκριμένη εντολή συστήματος

2.8α : Επίθεση σε κωδικούς πρόσβασης.

Ο κωδικός πρόσβασης αποτελεί μία μέθοδο αναγνώρισης ενός χρήστη από το σύστημα. Δίδοντας κάποιος το σωστό όνομα χρήστη και κωδικό πρόσβασης αποκτά πρόσβαση στο σύστημα και στις λειτουργίες του πάντα με βάση το τι έχει επιτραπεί στο συγκεκριμένο

λογαριασμό με αυτό το όνομα χρήστη. Η επίθεση λοιπόν σε κωδικούς πρόσβασης μπορεί να πάρει δύο μορφές:

1. την **επίθεση εκτός σύνδεσης,** όπου ο επιτιθέμενος παίρνει το φάκελο του κωδικού πρόσβασης και τον μεταφέρει από τη μηχανή - στόχο στη δική του μηχανή. Στη συνέχεια χρησιμοποιεί ένα εργαλείο που «σπάει» κωδικούς για να τον χρησιμοποιήσει. Σε αυτή την επίθεση δε χρειάζεται να ανησυχεί κάποιος για μηχανισμούς προφύλαξης και μπλοκαρίσματος των κωδικών από τη μηχανή – στόχο.
2. την **επίθεση εντός σύνδεσης,** όπου ο επιτιθέμενος ουσιαστικά μαντεύει τον κωδικό γεγονός που μπορεί να προκαλέσει την ενεργοποίηση αμυντικών μηχανισμών εάν έχουν παρέλθει αρκετές αποτυχημένες προσπάθειες.

Μπορεί η ανεύρεση κωδικών πρόσβασης να μη φαίνεται κάτι το τόσο σημαντικό σε μια διαδικασία διείσδυσης , αλλά μπορεί να προσφέρει στον ελεγκτή πολλά πλεονεκτήματα. Ως εκ τούτου δεν πρέπει να παραλείπεται αυτό το βήμα. Έτσι θα παρουσιαστούν κάποια αντιπροσωπευτικά εργαλεία για κάθε μορφή επίθεσης που αναφέρθηκε.

2.8α.1 Rainbowcrack.

Ένα γνωστό εργαλείο για την εκτός σύνδεση επίθεση σε κωδικούς πρόσβασης είναι το Rainbowcrack. Με τη βοήθεια αυτού του εργαλείου μπορεί κάποιος να «σπάσει» τη συνάρτηση κατακερματισμού που έχει ο κωδικός χρησιμοποιώντας τους ειδικούς πίνακες rainbow. Οι πίνακες συνήθως χρησιμοποιούνται για την ανάκτηση απλού κειμένου (plaintext) του κωδικού πρόσβασης, μέχρι ένα ορισμένο μήκος που αποτελείται από ένα περιορισμένο σύνολο χαρακτήρων. Είναι μια μορφή ανταλλαγής χρόνου - μνήμης, χρησιμοποιώντας λιγότερη CPU σε αντάλλαγμα περισσότερο χώρο αποθήκευσης. Για να λειτουργήσει το Rainbowcrack πρέπει να γίνουν τρεις ακολουθίες λειτουργιών:

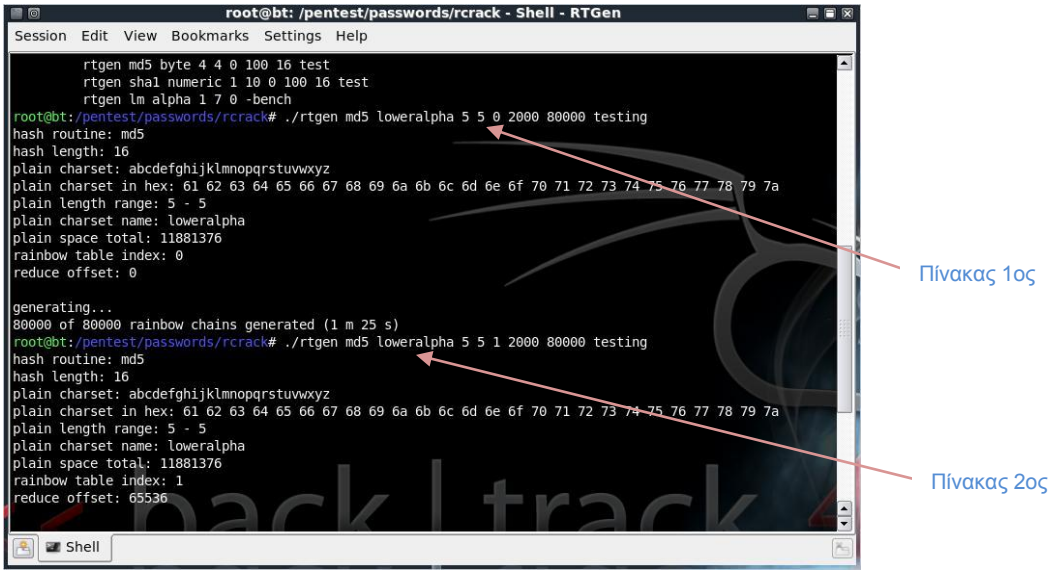
1. η παραγωγή των πινάκων rainbow με το **rtgen** (rainbow tables generators),
2. η ταξινόμηση των πινάκων αυτών με το **rtsort** και
3. το «σπάσιμο» της συνάρτησης κατακερματισμού μέσω του **rcrack**

Έτσι από το μενού **Backtrack / Privilege Escalation / Password Attacks / OfflineAttacks / RTGen** ξεκινάμε με το 1ο βήμα. Θα δημιουργηθούν δύο πίνακες χρησιμοποιώντας τις εντολές:

 # ./rtgen md5 loweralpha 5 5 0 2000 80000 testing , με συνάρτηση κατακερματισμού MD5 και ορίζοντας το μέγεθος του κειμένου και το όνομα του αρχείου που θα δημιουργηθούν οι πίνακες

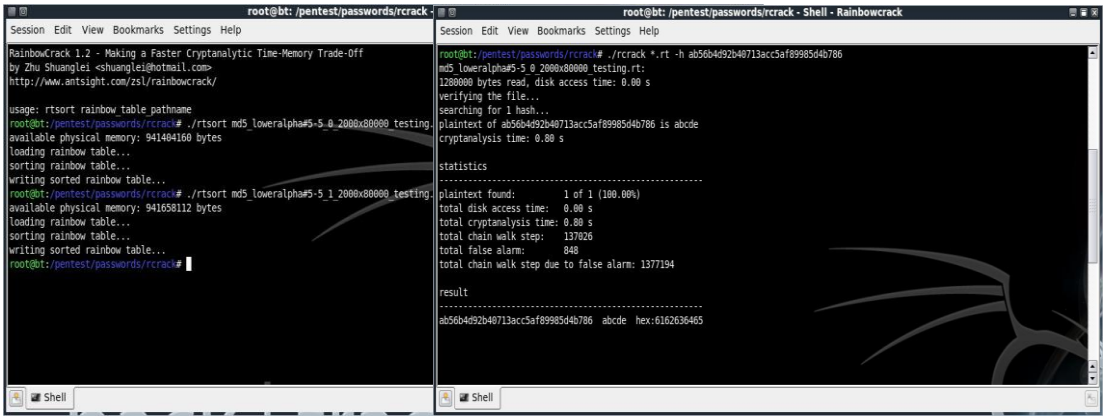
 # ./rtgen md5 loweralpha 5 5 1 2000 80000 testing , ομοίως για το δεύτερο πίνακα

Τα παραγόμενα αποτελέσματα φαίνονται στην παρακάτω εικόνα:



Εικόνα 11: Παραγωγή δύο πινάκων rainbow.

Στη συνέχεια οι δύο παραπάνω πίνακες που παρήχθησαν, σε σχετικά μικρό χρονικό διάστημα (1 λεπτό και 20 δευτ.) ταξινομούνται με το **rtsort** που βρίσκεται σε αντίστοιχο μενού με το **rtgen** και τέλος σπάει η συνάρτηση κατακερματισμού με το **rcrack**. Οι διαδικασίες αυτές γίνονται πολύ γρήγορα και τα αποτελέσματα φαίνονται παρακάτω:



Εικόνα 12: Ταξινόμηση των πινάκων rainbow και "σπάσιμο" της hash.

Αυτή όπως παρατηρείται είναι μια διαδικασία με τρία βήματα για να καταστεί εφικτό το «σπάσιμο» ενός κωδικού πρόσβασης. Σε περίπτωση που κάποιος ελεγκτής επιθυμεί να κάνει πιο γρήγορα τη διαδικασία αυτή υπάρχουν και άλλα εργαλεία σαν το Rainbowcrack που λειτουργούν με αντίστοιχο τρόπο. Αναφέρονται λοιπόν επιγραμματικά τα :

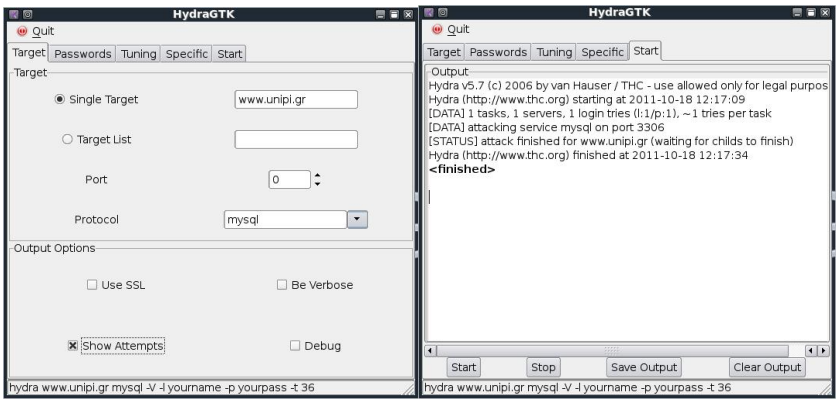
- Ophcrack
- Samdump2
- John (John the ripper)
- Crunch και
- Wyd

Όσον αφορά στο Ophcrack κυκλοφορεί και σε μορφή **live cd** οπότε μπορεί ο χρήστης να το λειτουργήσει ξεκινώντας τον υπολογιστή και κάνοντας boot πρώτα το cd. Αυτό του δίνει τη δυνατότητα να βρει τους κωδικούς πρόσβασης και να τους χρησιμοποιήσει για να μπει στο σύστημα. Εκτός από τη βοήθεια που προσφέρει στο penetration testing μπορεί να χρησιμοποιηθεί και σε περίπτωση που ο ίδιος ο χρήστης έχει ξεχάσει τον κωδικό με τον οποίο έχει κλειδώσει το λογαριασμό του στα Windows για παράδειγμα.

2.8α.2 : XHydra.

Η ακόλουθη υποενότητα, μετά το πέρας της αναφοράς των offline επιθέσεων, θα καταπιαστεί με ένα εργαλείο το οποίο βοηθά στις εντός σύνδεσης επιθέσεις. Το εργαλείο αυτό λέγεται **XHydra** και βοηθάει τον tester στο να μαντεύει ή να σπάει ονόματα χρήστη και κωδικούς πρόσβασης. Υποστηρίζει μια πληθώρα από πρωτόκολλα και προσπαθεί παράλληλα με τις πληροφορίες που έχει βρεί να συνδεθεί στο σύστημα. Στη διαδρομή **Backtrack / Privilege Escalation / Password Attacks / OnlineAttacks / XHydra** βρίσκεται το εργαλείο και κατά την έναρξή του εμφανίζεται ένα παράθυρο διεπαφής. Εκεί γίνονται όλες τις απαραίτητες ρυθμίσεις σχετικά με το στόχο , το πρωτόκολλο και άλλες προσαρμοσμένες ιδιότητες.

Στο ακόλουθο παράδειγμα θα χρησιμοποιηθεί η IP του πανεπιστημίου Πειραιώς (καταχρηστικά βέβαια και με προσοχή) με την επιφύλαξη ότι μπορεί να μη φανερωθούν αποτελέσματα λόγω του μηχανισμού ασφαλείας που πιθανόν να διαθέτει. Τα αποτελέσματα είναι τα ακόλουθα:



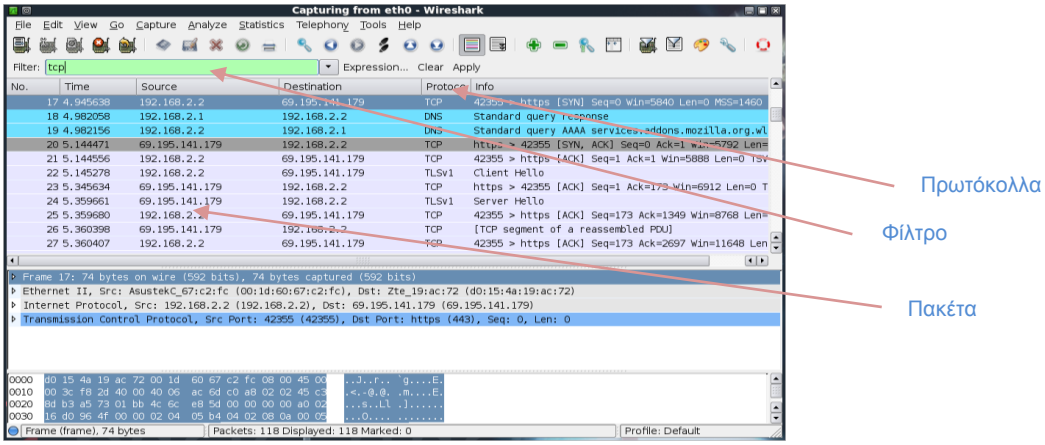
Εικόνα 13: XHydra.

Παρατηρείται λοιπόν ότι η επίθεση στην IP έγινε. Λόγω όμως αμυντικών μηχανισμών δεν υπάρχει πληθώρα αποτελεσμάτων. Ανάλογα με το τι έχει ζητηθεί από τον οργανισμό μπορεί ο ελεγκτής να χρησιμοποιεί διαφορετικά πρωτόκολλα για τις επιθέσεις του.

2.8β : Η διαδικασία του Sniffing.

Με τον όρο **sniffing**, νοείται η διαδικασία παρακολούθησης των δεδομένων που κυκλοφορούν και μεταδίδονται μέσα σε ένα δίκτυο. Τα αντίστοιχα εργαλεία για αυτή τη διαδικασία ονομάζονται sniffers και μπορεί να είναι είτε λογισμικό είτε υλικό. Επίσης η διαδικασία του sniffing δίδει τη δυνατότητα να δει ο ελεγκτής ποιες πληροφορίες είναι διαθέσιμες στο δικό του δίκτυο. Είναι πολύ σημαντικό για έναν ελεγκτή να μπορεί να ελέγξει το δίκτυο – στόχο και να βρει τις πληροφορίες εκείνες που τον ενδιαφέρουν για να μπορέσει να προχωρήσει τη διαδικασία του penetration test.

Ένα από τα πιο ευρέως διαδεδομένα εργαλεία αυτού του τύπου είναι το **Wireshark** το οποίο ουσιαστικά είναι ένα εργαλείο ανάλυσης πρωτοκόλλων. Ανιχνεύει τα πακέτα που κυκλοφορούν στο δίκτυο και δίνει πληροφορίες για το ποια πρωτόκολλα ακολουθούν ,όπως για παράδειγμα το TCP/IP ,το FTP, το SMTP και λοιπά. Επιπροσθέτως δίδει τη δυνατότητα γραφικού περιβάλλοντος και εξαγωγή των δεδομένων σε XML ή Postscript κλπ. Μέσω του BackTrack βρίσκουμε το Wireshark στη διαδρομή **Backtrack / Privilege Escalation / Sniffers / Wireshark.** Παρακάτω θα παρουσιαστεί εν συντομία η λειτουργία του η οποία είναι απλή χωρίς ιδιαίτερες λεπτομέρειες και δυσκολίες. Για τη διευκόλυνση της ανάλυσης παρατίθεται η ακόλουθη εικόνα:



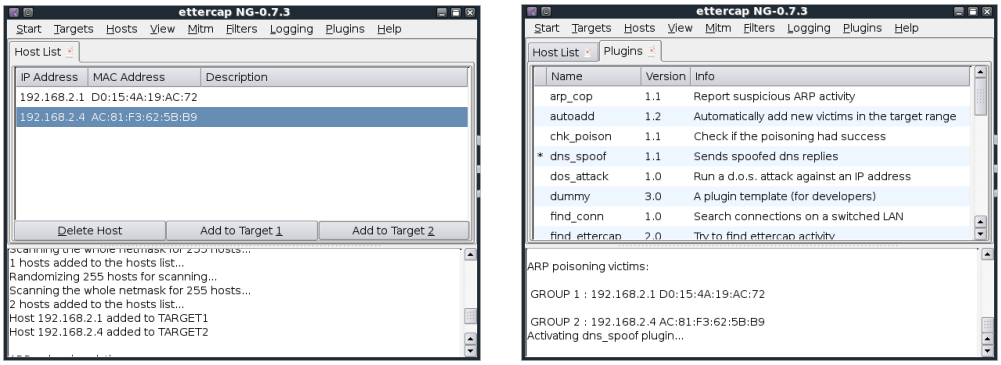
Εικόνα 14: Wireshark.

Παρατηρείται από τα παραπάνω μια πληθώρα από πληροφορίες σχετικά με τα πακέτα που «ταξιδεύουν» στο προς ανίχνευση δίκτυό. Ως δίκτυο έχει επιλεγεί να ανιχνευθεί αυτό στο οποίο λειτουργεί ο υπολογιστής στον οποίο έχει εγκατασταθεί το BackTrack. Επιπροσθέτως εμφανίζονται τα πρωτόκολλα τα οποία ακολουθεί κάθε πακέτο ενώ υπάρχει δυνατότητα εισαγωγής φίλτρου για να επιλεγεί ποιο πρωτόκολλο επιθυμεί ο tester να εμφανίζεται που τον ενδιαφέρει κάθε φορά. Λιτό στη λειτουργία του το Wireshark παρέχει ότι ακριβώς χρειάζεται για να επιτευχθεί ένα καλό sniffing στο δίκτυο – στόχο.

2.8γ : Η διαδικασία του Spoofing.

Με τον όρο **spoofing**, νοείται η διαδικασία της τροποποίησης των πληροφοριών , που συλλέγονται από ένα sniffer, όπως οι διευθύνσεις MAC , οι IP και ούτω καθεξής. Στόχος αυτής της διαδικασίας είναι να συλλεχθούν οι πληροφορίες από δύο συνδιαλεγόμενα μέρη στο δίκτυο. Για το σκοπό αυτό χρησιμοποιούνται εξειδικευμένα εργαλεία το κυριότερο από τα οποία είναι το Ettercap-GTK, το οποίο είναι ένα εργαλείο με γραφικό περιβάλλον. Το εργαλείο αυτό επιτρέπει την επίτευξη μιας επίθεσης στο τοπικό δίκτυο LAN γνωστή και ως «man in the middle attack».

Χρησιμοποιώντας για άλλη μια φορά το BackTrack, βρίσκεται το εργαλείο στη διαδρομή **Backtrack / Privilege Escalation / Spoofing / Ettercap.** Εύκολο στη χρήση του παρέχει τη δυνατότητα άντλησης πληροφοριών ώστε να διευρυθούν τα ήδη υπάρχοντα δικαιώματα που έχει αποκτήσει ο tester στην έως τώρα διαδρομή του στο τεστ διείσδυσης. Μια εικόνα βεβαίως θα καταστήσει πιο κατανοητή τη λειτουργία του Ettercap και έτσι τα αποτελέσματα φαίνονται παρακάτω:



Εικόνα 15 : Ettercap.

Όπως φαίνεται παραπάνω γίνεται spoofing στο eth0 το οποίο όπως και στη διαδικασία του sniffing είναι το δίκτυο του προς χρήση υπολογιστή. Στο δίκτυο αυτό υπάρχουν δύο hosts οι οποίοι ορίζονται ως 1ος και 2ος στόχος. Στη συνέχεια χρησιμοποιούνται κάποια εργαλεία για να γίνει ένα Arp Poisoning, δηλαδή ο ελεγκτής μπαίνει ενδιάμεσα στους hosts αφού η MAC

διεύθυνση του DNS server και του host τοποθετείται στη δική του MAC διεύθυνση, και συνεχίζεται η διαδικασία με ένα dns spoof για να γίνει ουσιαστικά ο «ενδιάμεσος άντρας».

Στο σημείο αυτό έχει ολοκληρωθεί η διαδικασία της κλιμάκωσης προνομίων εφόσον έχουν αναλυθεί και διερευνηθεί τόσο οι επιθέσεις σε κωδικούς επιβεβαίωσης online και offline , όσο και οι διαδικασίες του sniffining και spoofing. Σε κάθε περίπτωση οι πληροφορίες που λαμβάνονται είναι ζωτικής σημασίας για την διεξαγωγή ενός πετυχημένου τεστ διείσδυσης (pen test). Αφού λοιπόν έχει ολοκληρωθεί και αυτό το βήμα η ανάλυση προχωράει στο επόμενο στάδιο το οποίο είναι, η διατήρηση της πρόσβασης.

2.9 : Διατήρηση πρόσβασης ή maintaining access.

Όπως έγινε φανερό από όλη την παραπάνω ανάλυσή, η διαδικασία διεξαγωγής ενός τεστ διείσδυσης και η ακολουθία όλων των βημάτων μας οδηγεί στην απόκτηση πολύτιμων πληροφοριών για το σύστημα – στόχο ενώ ταυτόχρονα βοηθά μέσω ποικίλων εργαλείων στην απόκτηση πρόσβασης σε αυτό. Ένα μεγάλο ζήτημα που ανακύπτει είναι και η διατήρηση αυτής της πρόσβασης, δηλαδή η ανάγκη να παραμείνει το σύστημα «ανοιχτό» , ώστε να μπορεί ο tester να επανέλθει σε αυτό οποιαδήποτε στιγμή θελήσει χωρίς να χρειάζεται να επαναλάβει από την αρχή όλη τη διαδικασία του penetration test. Στην προσπάθειά αυτή υπάρχουν ειδικά εργαλεία που βοηθούν και σχετίζονται με :

- εργαλεία «σηρραγοποίησης» πρωτοκόλλων (protocol tunneling)
- εργαλεία μεσολάβησης (proxy tools) και ,
- end to end εργαλεία σύνδεσης

Όπως αναφέρθηκε και προηγουμένως σκοπός είναι η παράκαμψη του μηχανήματος – στόχου και η διατήρηση όλων των προνομίων και των προσβάσεων σε αυτό το σύστημα , ώστε να οποιαδήποτε στιγμή να είναι εφικτή η είσοδος σε αυτό. Γίνεται μια προσπάθεια ουσιαστικά να παρακαμφθούν τα όποια φίλτρα μπορεί να διαθέτει το σύστημα ή να δημιουργηθεί μια συγκεκαλυμμένη σύνδεση με το μηχάνημα αυτό και τον υπολογιστή του ελεγκτή.

2.9.1 : Protocol tunneling - Socat.

Πριν ξεκινήσουμε να περιγράφουμε τα εργαλεία αυτά ας δούμε πρώτα τι είναι το tunneling. Ο όρος tunneling ή αλλιώς ελληνιστί (καταχρηστικά βέβαια) «σηραγγοποίηση» είναι η μέθοδος της ενσωμάτωσης ενός πρωτοκόλλου μέσα σε ένα άλλο. Σε ότι αφορά τη δική μας περίπτωση χρησιμοποιείται αυτή η μέθοδος για να αποφευχθεί και να παρακαμφθεί η προστασία που διαθέτει το σύστημα – στόχος. Χαρακτηριστικό παράδειγμα αποτελεί η αποφυγή του firewall (τείχος προστασίας) το οποίο μπλοκάρει συνδέσεις από τον εξωτερικό κόσμο και επιτρέπει μόνο ορισμένα πρωτόκολλα όπως το HTTP και το HTTPS. Έτσι λοιπόν «τυλίγουμε» τα δικά μας πακέτα σε ένα από αυτά τα πρωτόκολλα και το τείχος προστασίας επιτρέπει στα πακέτα αυτά να συνδεθούν και σε εξωτερικά δίκτυα.

Στην κατεύθυνση αυτή ένα χρήσιμο εργαλείο είναι το λεγόμενο, **Socat**. Πρόκειται βασικά για ένα εργαλείο που καθορίζει δύο αμφίδρομα ρεύματα και μεταφέρει δεδομένα μεταξύ τους. Το κάθε ρεύμα μπορεί να είναι ένα συνδυασμός από τα παρακάτω:

- ένα αρχείο
- ένα πρόγραμμα
- μια συσκευή
- ένας περιγραφέας αρχείου (file descriptor)
- μια υποδοχή (IPv4, IPv6, SSL, TCP, UDP, UNIX)

Παράλληλα υπάρχουν οι ακόλουθες φάσεις που ακολουθεί η λειτουργία του Socat.

- η 1η φάση, όπου αναλύονται οι επιλογές της γραμμής εντολών
- σε 2η φάση το Socat ανοίγει και τις δύο διευθύνσεις, αφού όπως αναφέρθηκε και παραπάνω υπάρχουν δύο ρεύματα, άρα με μία συγκεκριμένη διεύθυνση το καθένα
- σε 3η φάση διαβάζονται και από τα δύο ρεύματα οι περιγραφείς αρχείων. Όταν τα δεδομένα από τη μία πλευρά είναι έτοιμα και μπορούν να γραφούν

στην άλλη, τότε τα γράφει στον write file descriptor και περιμένει για επιπρόσθετα δεδομένα

- σε 4η και τελευταία φάση όταν ένα από τα δύο ρεύματα φτάσει στο EOF (end of file), δηλαδή όταν δε μπορούν πλέον να μεταφερθούν άλλα δεδομένα από μια συγκεκριμένη πηγή, τότε ξεκινάει η διαδικασία κλεισίματος. Το Socat μεταφέρει την εντολή EOF και στο δεύτερο ρεύμα, για κάποιο μικρό χρονικό διάστημα μεταδίδει τα εναπομείναντα δεδομένα και στη συνέχεια κλείνει και τα δύο ρεύματα.

Πιο συνοπτικά στο ακόλουθο παράδειγμα παρουσιάζεται ενδεικτικά ο παραπάνω κύκλος των τεσσάρων φάσεων. Για τη διεκπεραίωση της λειτουργίας χρειάζονται δύο διαφορετικές IP, για να εμφανιστούν ουσιαστικά τα δύο ρεύματα που αναφέρθηκαν παραπάνω. Μέσω της διαδρομής **Backtrack | Maintaining Access | Tunneling | Socat** ανοίγει μια γραμμή εντολών στο ένα ρεύμα και πληκτρολογείται η εντολή:

socat – TCP4:192.168.2.2:80

HEAD / HTTP/1.0, εδώ σε συγκεκριμένη διεύθυνση αποσπώνται οι πληροφορίες για την κεφαλίδα του HTTP. Το αποτέλεσμα είναι το ακόλουθο:

200 OK

Content-Length: 848

Content-Type: text/html

Last-Modified: Wed, 13 Feb 2013 19:20:44 GMT

Client-Date: Wed, 13 Feb 2013 19:57:23 GMT

Prototype mismatch: sub main::__LONG_MAX__ () vs none at /usr/lib/perl/5.10/_h2ph_pre.ph line 291.

Constant subroutine __LONG_MAX__ redefined at /usr/lib/perl/5.10/_h2ph_pre.ph line 291.

200 (OK)

Cache-Control: private, no-cache, must-revalidate

Connection: Keep-Alive

Pragma: no-cache

Server: Oversee Turing v1.0.0

Content-Length: 1741

Content-Type: text/html

Expires: Mon, 26 Jul 1997 05:00:00 GMT

Client-Date: Wed, 13 Feb 2013 19:57:25 GMT

Client-Peer: 204.13.162.116:80

Client-Response-Num: 1

Keep-Alive: timeout=3, max=99

Στο δεύτερο ρεύμα τώρα σε αντίστοιχη γραμμή εντολών πληκτρολογείται η παρακάτω εντολή, ώστε να «ακούσει» σε μια συγκεκριμένη θύρα, για να λάβει και να ανοίξει αργότερα ένα αρχείο που θα σταλεί. Έτσι έχουμε τα ακόλουθα:

socat TCP4-LISTEN:1234 OPEN:testfile, create,append, πιο συγκεκριμένα η θύρα που «ακούσει» το ρεύμα είναι η 1234, ενώ το αρχείο που θα ανοιχθεί είναι το testfile, που αν υπάρχει θα βρεθεί μέσα από ευρετήριο, αλλιώς θα δημιουργηθεί εκείνη τη στιγμή.

Επιστρέφοντας στο πρώτο ρεύμα και στην πρώτη IP πληκτρολογείται η ακόλουθη εντολή:

cat test-sam | socat – TCP4:192.168.150.130:1234, το αποτέλεσμα αυτής της ενέργειας είναι να διαπιστωθεί ότι στο δεύτερο ρεύμα μεταφέρθηκε και δημιουργήθηκε το συγκεκριμένο αρχείο που στάλθηκε.

Παρατηρείται λοιπόν ότι με εύκολο, απλό και γρήγορο τρόπο μπορεί να δημιουργηθεί μια σύνδεση μεταξύ δύο διαφορετικών ρευμάτων (IPs), η οποία εν τέλει θα καταστήσει εφικτή την επικοινωνία δύο μηχανημάτων, που σε προκειμένη περίπτωση το ένα θα είναι το ελεγκτή για να μπορέσει να διαπιστώσει το κατά πόσο εύκολη είναι η πρόσβαση σε ένα ξένο μηχάνημα – στόχο. Σε παρόμοια φιλοσοφία με το παραπάνω εργαλείο που αναλύθηκε είναι και τα εξής:

- **3proxy**
- **proxychains**
- **ptunnel**
- **stunnel4**
- **cryptcat**
- **dns2tcp**

2.10 : Τεκμηρίωση και πληροφόρηση.

Στο σημείο αυτό έχει τελειώσει η ανάλυση με τα βήματα που ακολουθούνται για τη διεξαγωγή ενός τεστ διείσδυσης και έχουν παρουσιαστεί τα εργαλεία που χρησιμοποιούνται και οι διαδικασίες που λαμβάνουν χώρα σε καθένα από αυτά. Θυμίζουμε για άλλη μια φορά ότι πρόκειται για βήματα που το ένα διαδέχεται το άλλο και ως εκ τούτου είναι αλληλένδετα μεταξύ τους. Επίσης οι πληροφορίες που παρέχουν βοηθούν στο να εξάγονται καλύτερα και πιο σίγουρα αποτελέσματα σε ότι αφορά το σύστημα – στόχο.

Παρόλα αυτά υπάρχει και ακόμη μία σημαντική διαδικασία που μπορεί να ενσωματωθεί ως τελευταίο βήμα στη διαδικασία ενός penetration test. Η διαδικασία αυτή σχετίζεται με την τεκμηρίωση και την πληροφόρηση. Η παρακολούθηση των αποτελεσμάτων της αξιολόγησης μας είναι μια πολύ σημαντική πτυχή της μεθοδολογίας των δοκιμών διείσδυσης καθώς η καταγραφή κάθε εισόδου και εξόδου από τα εργαλεία ελέγχου που χρησιμοποιούμε και η επαλήθευση των ατομικών αποτελεσμάτων των δοκιμών πριν από την προσκόμισή τους στην αρμόδια αρχή είναι το κλειδί προς την κατεύθυνση του επιτυχημένου και σταθερού επαγγελματισμού. Για το λόγο αυτό λοιπόν η τεκμηρίωση, η προετοιμασία της έκθεσης, και η παρουσίαση είναι μερικά από τα πολλά βασικά στοιχεία που πρέπει να απευθύνονται με ένα συστηματικό, διαρθρωμένο, και συνεπή τρόπο.

Στο σημείο αυτό τονίζεται ότι τα παραπάνω στοιχεία πληροφόρησης αποτελούν μια ισχυρή βάση, ο ρόλος της οποίας αναδεικνύεται περισσότερο λόγω του ότι αναφέρεται κάθε φορά σε μεγάλους και έγκυρους οργανισμούς. Ένα μικρό λάθος μπορεί συχνά να οδηγήσει σε ένα νομικό πρόβλημα, μικρό ή μεγάλο. Η έκθεση λοιπόν που θα συνταχθεί στο τέλος θα πρέπει να δείξει με συνέπεια όλα τα ευρήματά, ενώ ταυτόχρονα θα επισημαίνει τις δυνατότητες αδυναμίες που βρέθηκαν στο συγκεκριμένο περιβάλλον - στόχο. Οφείλει μια τέτοια έκθεση, να είναι καλά προετοιμασμένη και να επιδείξει μια απόδειξη της υποστήριξης έναντι γνωστών απαιτήσεων συμμόρφωσης, εφόσον υπάρχουν, και απαιτούνται από τον πελάτη. Τονίζεται ότι όλα αυτά έχουν συζητηθεί και καταγραφεί στη σύλληψη απαιτήσεων. Επιπλέον η έκθεσή, θα πρέπει να αναφέρει με σαφήνεια τον τρόπο λειτουργίας του εισβολέα, τα εργαλεία και τις τεχνικές που χρησιμοποιήθηκαν, έναν κατάλογο με τις ευπάθειες που ανακαλύφθηκαν και τις μεθόδους επαλήθευσης. Άρα τις περισσότερες φορές έχει επίκεντρο τις αδυναμίες και όχι τις διαδικασίες που χρησιμοποιήθηκαν για να ανακαλυφθούν.

Ένα σημαντικό σημείο που πρέπει να αναφερθεί και να τονιστεί είναι ότι οι σημειώσεις σχετικά με τα αποτελέσματα που έχουν ληφθεί σχολαστικά και με τη βοήθεια αυτοματοποιημένων εργαλείων πάντα απαιτούν σημαντικό ποσό επαλήθευσης πριν να παρουσιαστούν στον πελάτη. Είναι μια κρίσιμη εργασία διότι αφορά τόσο τη φήμη όσο και την ακεραιότητα του ελεγκτή. Κάθε είδος ανευθυνότητας ως προς την αξιολόγηση μπορεί να οδηγήσει σε σοβαρές συνέπειες και να προκαλέσει ακόμη και την καταστροφή της σταδιοδρομίας του. Επιπροσθέτως θέτει και τον πελάτη σε κίνδυνο από την «πώληση» μιας ψεύτικης αίσθησης ασφάλειας. Έτσι λοιπόν, η ακεραιότητα των δεδομένων των δοκιμών δεν πρέπει σε καμιά περίπτωση να νοθεύεται με λάθη , ανακρίβειες και ανακολουθίες.

Για να συνταχθεί μια καλή έκθεση και η οποία θα μπορεί να σταθεί με ακεραιότητα μπροστά στον πελάτη , μπορεί κάποιος να ακολουθήσει τρεις βασικές πρακτικές συμβουλές:

1. να κάνει μια λεπτομερή καταγραφή κάθε επιλεκτικού βήματος που έχει γίνει στη διάρκεια του penetration test (συλλογή πληροφοριών , χαρτογράφηση ευπαθειών , κοινωνική μηχανική κλπ).
2. καταγραφή ενός προτύπου σχετικά με κάθε εργαλείο που έχει χρησιμοποιηθεί για να διεξαχθεί το τεστ. Το πρότυπο αυτό θα πρέπει να δηλώνει σαφώς το σκοπό του, τις επιλογές εκτέλεσης, και τα προφίλ που είναι ευθυγραμμισμένα για την αξιολόγηση του στόχου, και παράλληλα να παρέχει χώρο για την καταγραφή των αντίστοιχων αποτελεσμάτων των δοκιμών.
3. Τέλος σε καμιά περίπτωση δεν πρέπει να στηρίζεται μόνο σε ένα εργαλείο , διότι όχι μόνο δεν είναι πρακτικό , αλλά μπορεί να μην οδηγεί σε ορθά αποτελέσματα και ως εκ τούτου να υπάρχουν σημαντικές αποκλίσεις που να αλλοιώνουν τα πραγματικά στοιχεία. Έτσι θα πρέπει κάθε διαδικασία να γίνεται με διαφορετικά εργαλεία με αποτέλεσμα να κερδίζεται και η επαλήθευση των στοιχείων, η μείωση των σφαλμάτων και η αύξηση των θετικών αποτελεσμάτων.

Όσο λοιπόν αφορά στην τεκμηρίωση ενός τεστ διείσδυσης υπάρχουν τρεις διαφορετικοί τύποι έκθεσης που δίνουν πληροφορίες σχετικά με τα αποτελέσματα του τεστ και απευθύνονται σε συγκεκριμένη ομάδα στελεχών του οργανισμού που ζήτησε τη διεξαγωγή του. Έτσι λοιπόν υπάρχει η «**Εκτελεστική έκθεση**» ή πιο σωστά η **Executive report**. Αυτό το είδος της έκθεσης είναι το μικρότερο , αλλά το πιο περιεκτικό διότι περιλαμβάνει πληροφορίες σχετικά με τα αποτελέσματα του τεστ και τα παρουσιάζει κυρίως από τη στρατηγική οπτική γωνία της επιχείρησης-οργανισμού. Αναφέρεται ως επί το πλείστον στα στελέχη «C» κατηγορίας όπως οι διευθύνοντες σύμβουλοι (CEO. CIO, CTO).

Μία τέτοια έκθεση οφείλει να συμπεριλαμβάνει στοιχεία σχετικά με τους στόχους του έργου που έχουν συζητηθεί μεταξύ του πελάτη και του ελεγκτή και οι οποίοι στηρίζονται σε αμοιβαία αποδεκτά κριτήρια. Σε επόμενο στάδιο θα πρέπει να γίνεται αναφορά στην κατηγοριοποίηση των ευπαθειών και των κινδύνων που βρέθηκαν κατά τη διάρκεια της δοκιμής διείσδυσης ενώ θα δίνεται και ιδιαίτερη βαρύτητα του κάθε επιπέδου κινδύνου με βάση τη σοβαρότητά του. Ακόμη θα συμπεριλαμβάνει μια σύντομη περιεκτική παρουσίαση σχετικά με το στόχο και το σκοπό του τεστ που γίνεται με βάση κάποια συγκεκριμένη μεθοδολογία ενώ ταυτόχρονα θα υπογραμμίζει τις ευπάθειες που βρέθηκαν και αντιμετωπίστηκαν με επιτυχία. Ένα ακόμη στοιχείο είναι και τα στατιστικά στοιχεία που θα ακολουθούν αυτή την έκθεση σχετικά με τα τρωτά σημεία που εμφανίστηκαν στο στόχο και σχετίζονται με την υποδομή του δικτύου. Τέλος θα πρέπει να υπάρχει ένας πίνακας κινδύνων που θα ποσοτικοποιεί και θα κατηγοριοποιεί όλα τα θέματα ευπάθειας που ανακαλύφθηκαν, θα προσδιορίζει τους πόρους που ενδέχεται να πληγούν και βεβαίως θα παραθέτει τα ευρήματα, τις αναφορές και τις συστάσεις σχετικά με τα αποτελέσματα.

Ένα άλλο είδος έκθεσης πληροφόρησης και τεκμηρίωσης είναι και η «**Έκθεση διαχείρισης**» ή «**Management report**». Αυτός ό τύπος έκθεσης περιλαμβάνει στοιχεία σχετικά με ρυθμιστικές μετρήσεις σε όρους ασφαλείας. Απευθύνεται κυρίως σε στελέχη όπως το HR , αλλά και σε άλλους ανθρώπους της διαχείρισης καθώς τους βοηθά με τις νομικές διαδικασίες.

Πιο συγκεκριμένα η έκθεση διαχείρισης περιλαμβάνει στοιχεία όπως η λεγόμενη επίτευξη της συμμόρφωσης, σύμφωνα με την οποία ξεκινά η δημιουργία μιας λίστας γνωστών προτύπων και χαρτών σχετικά με τη διαθέσιμη ασφάλεια. Εδώ επισημαίνεται οποιαδήποτε κανονιστική παραβίαση έλαβε χώρα και μπορεί να αποτελέσει απειλεί για την υποδομή του στόχου. Ακολουθεί η μεθοδολογία του τεστ που πρέπει να παρουσιάζεται συνοπτικά και με απλά λόγια ώστε να γίνεται κατανοητή η διαδικασία και ο κύκλος ζωής του penetration testing. Σε επόμενο επίπεδο υπάρχει η αναφορά κάποιων παραδοχών και περιορισμών που μπορεί να εμπόδισαν τον ελεγκτή από το να φτάσει στην επίτευξη κάποιου συγκεκριμένου στόχου κατά τη διάρκεια της δοκιμής.

Εκτός από αυτά τα στοιχεία συμπεριλαμβάνεται και η διαχείρισης της αλλαγής, όπου θεωρείται από πολλούς μέρος της διαδικασίας αποκατάστασης του συστήματος. Κατά κύριο λόγω απευθύνεται στις στρατηγικές μεθόδους που διεκπεραιώνουν όλες τις αλλαγές μέσα σε ένα ελεγχόμενο περιβάλλον πληροφορικής. Τελευταίο τώρα στοιχείο αυτού του τύπου έκθεσης είναι και η διαχείριση των ρυθμίσεων, όπου εστιάζει κατά κύριο λόγο στη συνέπεια

της λειτουργίας και της απόδοσης ενός συστήματος. Στο πλαίσιο λοιπόν της ασφάλειας του συστήματος, ακολουθούνται τυχόν αλλαγές που μπορεί να έχουν εισαχθεί στο στόχο. Αυτές οι αλλαγές στις ρυθμίσεις θα πρέπει να παρακολουθούνται και να ελέγχονται ώστε να διατηρείται το επίπεδο ρυθμίσεων του συστήματος – στόχου.

Τελευταίο είδος έκθεσης πληροφόρησης αποτελεί, η **τεχνική έκθεση** (technical report). Ο τύπος αυτός έκθεσης αξιολόγησης διαδραματίζει έναν πολύ σημαντικό ρόλο στην αντιμετώπιση των θεμάτων ασφαλείας που τέθηκαν κατά τη δέσμευση, στην αρχή της δοκιμής διείσδυσης. Αυτό το είδος γενικά αναπτύχθηκε για προγραμματιστές που θέλουν να κατανοήσουν τα βασικά χαρακτηριστικά ασφαλείας του συστήματος, ποια χαρακτηριστικά είναι ευάλωτα, πώς μπορούν αυτά να αξιοποιηθούν, τι επιχειρηματικό αντίκτυπο θα μπορούσαν να έχουν τέτοιες ευπάθειες, και πώς μπορούν να αναπτυχθούν ανθεκτικές λύσεις που μπορούν να εμποδίσουν κάθε ορατή απειλή.

Σε μια τεχνική έκθεση λοιπόν θα πρέπει θέματα ασφάλειας που εγείρονται κατά τη διάρκεια της δοκιμής διείσδυσης να αναφέρονται λεπτομερώς, έτσι ώστε για κάθε μέθοδο που εφαρμόζεται αναφέρεται μια λίστα με τους επηρεαζόμενους πόρους του συστήματος - στόχου, τις επιπτώσεις της κάθε μεθόδου και λοιπά. Επίσης πρέπει να συμπεριλαμβάνεται ένας χάρτης ευπαθειών με μια λίστα με τα ευάλωτα σημεία που ανακαλύφθηκαν και βρίσκονται στην υποδομή του συστήματος. Κάθε ένα θα πρέπει να αναγράφεται παράλληλα προς τον αναγνωριστικό του πόρο δηλαδή για παράδειγμα, τη διεύθυνση IP ή το όνομα-στόχο. Παράλληλα θα πρέπει να συμπεριλαμβάνεται και ένας χάρτης «εκμεταλλεύσεων» (exploits map) που θα παρέχει μια λίστα με τα exploits εκείνα που με επιτυχία λειτούργησαν, ελέγχθηκαν και επαληθεύτηκαν εις βάρος του στόχου. Τέλος συμπεριλαμβάνονται στην έκθεση κάποιες βέλτιστες πρακτικές που τονίζουν τον καλύτερο σχεδιασμό, την υλοποίηση και τη λειτουργία των διαδικασιών ασφαλείας στις οποίες ο στόχος έχει έλλειψη. Για παράδειγμα, σε ένα μεγάλο επιχειρηματικό περιβάλλον, η ανάπτυξη της ασφάλειας σε πρώιμο στάδιο θα μπορούσε να μειώσει τον αριθμό των απειλών, πριν αυτές μπουν σε ένα εταιρικό δίκτυο.

Ένα τελευταίο, αλλά επίσης πολύ σημαντικό κομμάτι της πληροφόρησης είναι και η παρουσίαση. Δε φτάνει μόνο να έχει συγγραφεί μια ορθή και πλήρη έκθεση με κάποιον από τους παραπάνω τύπους έκθεσης που αναφέρθηκαν. Χρειάζεται αυτή την έκθεση να μπορεί ο tester να την παρουσιάσει σωστά και με κατανοητό τρόπο στους υπεύθυνους του οργανισμού. Πρέπει να δίδεται έμφαση στις ευπάθειες που βρέθηκαν και σε ποια σημεία του συστήματος εντοπίστηκαν για να καταλάβουν οι υπεύθυνοι τόσο την σοβαρότητα που ενέχει η ύπαρξη κάποιων εξωτερικών απειλών , όσο και την αναγκαιότητα για ασφάλεια στα συστήματά τους. Βασικό στοιχείο είναι να γνωρίζει σε ποιους απευθύνεται κάθε φορά και ανάλογα να παρουσιάζει τα ευρήματα του τεστ . Για παράδειγμα σε ένα διευθύνοντα σύμβουλο οι τεχνικές λεπτομέρειες τον αφήνουν αδιάφορο μιας και δεν έχει το υπόβαθρο να τις κατανοήσει σε αντίθεση με έναν προγραμματιστή ή τεχνικό που διαθέτει γνώσεις πληροφορικής.

Επιπροσθέτως στην παρουσίαση πρέπει να τονίζεται και η διαδρομή που έκαναν οι ελεγχόμενες επιθέσεις για να καταστεί δυνατό το πως μπορούν να εκμεταλλευτούν αυτές οι ευπάθειες που εντοπίστηκαν στο σύστημα – στόχο. Παρόλα αυτά δεν υπάρχει μια ακριβής συνταγή για το πώς θα παρουσιάσει κάποιος τα ευρήματά του. Το μόνο σίγουρο βέβαια είναι ότι θα πρέπει να γίνεται με επαγγελματισμό τόσο για το τεχνικό ή μη κοινό και παράλληλα η κατανόησή για το σύστημα να ωθεί το τεχνικό προσωπικό να καταλάβει όσο περισσότερο γίνεται την ανάγκη για ασφάλεια.

2.11 : Παραλληλισμός του Pen test.

Όπως φάνηκε στις παραπάνω ενότητες η ανάγκη για ασφάλεια σε ένα σύστημα οδήγησε στη δημιουργία μιας διαδικασίας που θα παρέχει εύρεση σφαλμάτων , απειλών και ευπαθειών καθώς και την παροχή λύσεων σε τέτοιου είδους ζητήματα και προβλήματα. Η διαδικασία αυτή ονομάστηκε **δοκιμή ή τεστ διείσδυσης** ή αγγλιστί **penetration testing.** Όπως ήδη έχει αναφερθεί από την αρχή αυτής της εργασίας ο ελεγκτής στον οποίο πέφτει το βάρος για να φέρει εις πέρας μια τέτοια δοκιμή λέγεται άσπρος hacker. Ως hacker λοιπόν πρέπει να «τεστάρει» το σύστημα για τυχόν ευπάθειες χωρίς να γίνει αντιληπτός. Όπως αναφέρουν και οι

Thomas Wilhelm και Jason Andress ένας hacker μπορεί να παρομοιαστεί , όσο και αν ακούγεται παράξενο, με έναν ninja.

Ως πρώτο άκουσμα μπορεί να φανεί περίεργο και ίσως να προκαλέσει γέλιο, αλλά αν μπορέσει κάποιος να φανταστεί λίγο τις δύο έννοιες θα καταλάβει ότι εκτός από τις έντονες διαφορές που υπάρχουν, έχουν και αρκετά κοινά τα οποία βοηθούν στον παραλληλισμό των δύο αυτών εννοιών. Για να γίνει πιο κατανοητό αυτό θα παρουσιαστεί σύντομα και περιεκτικά ο τρόπος δράσης και των δύο. Αρχικά το βασικό συνεκτικό στοιχείο είναι ότι και στις δύο περιπτώσεις υπάρχει δράση που γίνεται κεκαλυμμένα , ώστε να μην γίνει αντιληπτή στους άλλους οι παρουσία του δρώντος. Όπως παρατηρήθηκε και παραπάνω σε κάποιες περιπτώσεις που η ανάγκη επιτάσσει ο ελεγκτής να γίνει ο «ενδιάμεσος άντρας» χρειάζεται να κινηθεί με μυστικότητα για να μη γίνει αντιληπτός ο σκοπός του. Δεύτερο στοιχείο είναι ότι και στην περίπτωση του penetration testing ο ελεγκτής χρησιμοποιεί τα δικά του «όπλα», που όπως έχει αναφερθεί σε αρκετά σημεία είναι μικρά προγράμματα και εργαλεία που προμηθεύεται από το «οπλοστάσιο» του BackTrack.

Επίσης κοινό σημείο αποτελεί και η «μεταμφίεση». Στην περίπτωση του ελεγκτή (άσπρος hacker) ,και ιδιαίτερα όταν ασχολείται με την κοινωνική μηχανική, μεταμφιέζει τον εαυτό του για να μπορέσει να υποκλέψει σημαντικές πληροφορίες σχετικά με το περιβάλλον – στόχο που θέλει να ελέγξει. Είναι ένας πολύ καλός τρόπος άντλησης πληροφοριών χωρίς να γίνει αντιληπτός. Επιπροσθέτως μπορούν να συμπεριληφθεί στις ομοιότητες και ο τρόπος διείσδυσης σε ένα ξένο περιβάλλον. Όσον αφορά στον penetration tester , πολλές φορές χρειάζεται να «εισβάλλει» σε ένα σύστημα και να παρακάμψει τις άμυνες του χωρίς να αφήσει κανένα ίχνος πίσω του. Ακριβώς τι ίδιο συνέβαινε και με έναν Ninja, διείσδυση με μυστικότητα και χωρίς αποτυπώματα ή ίχνη. Μια καλή τακτική για οποιονδήποτε ελεγκτή.

Σε συνέχεια των παραπάνω ομοιοτήτων αναφέρεται και η χρήση του χρονισμού ή πιο γνωστή ως «timing». Πολύ σημαντική είναι η επιλογή του πότε θα γίνει μια δοκιμή διείσδυσης σε ένα σύστημα. Πολλές φορές αποκτώντας κλιμακούμενα προνόμια, όπως έχει παρατηρηθεί και πιο πάνω, ο tester αποκτά πρόσβαση ως νόμιμος χρήστης και έτσι αποφεύγεται οποιασδήποτε μορφής έλεγχος και πάνω απ' όλα παρακάμπτονται όλες οι ασφάλειες του συστήματος εφόσον πλέον αυτό τον αναγνωρίζει ως γνωστό και νόμιμο χρήστη. Τέλος θα αναφέρεται και η ικανότητα που έχει ο ελεγκτής να ανακαλύπτει τρωτά σημεία και ευπάθειες σε ένα σύστημα ή μηχάνημα , όπως ακριβώς και ένας παραδοσιακός ninja που θέλει να κάνει την επίθεσή του και να φέρει σε πέρας την αποστολή του. Παράλληλα βέβαια με όλα τα παραπάνω λειτουργεί και η μέθοδος της «κατασκοπείας». Με τούτο αρκεί να θυμηθούμε τα εργαλεία που έχουν χρησιμοποιηθεί κατά τη διάρκεια του penetration test τόσο για να διατηρηθεί η πρόσβαση σε ένα σύστημα, αλλά και εκείνα που επιτρέπουν στον ελεγκτή της δοκιμής να γίνει ο ενδιάμεσος δέκτης μηνυμάτων αφού έχει ρυθμίσει στην επικοινωνία μεταξύ δύο μερών να παρεμβάλλεται η δική του διεύθυνση IP.

Εν κατακλείδι , συνοψίζοντας όλα τα παραπάνω αυτό που συμπεραίνεται είναι ότι τελικά οι παραδοσιακές και παλαιές μέθοδοι διείσδυσης μπορεί μεν να αλλάζουν πρόσωπο και εργαλεία ανά τις εποχές , αλλά τελικά παραμένουν στη βάση τους ίδιες και το ίδιο αποτελεσματικές. Σε όλα αυτά παίζει σπουδαίο ρόλο και η ικανότητα εκείνου που τις χρησιμοποιεί η οποία βελτιώνεται ή και κάποιες φορές τελειοποιείται με την εξάσκηση και τη συχνή εφαρμογή. Συνεπώς ο παραλληλισμός του ελεγκτή και του παραδοσιακού πολεμιστή Ninja αποδεικνύεται ορθός και με νόημα και περιλαμβάνει πολλά ακόμη στοιχεία τα οποία είναι εκτός του σκοπού και του θέματος της εργασίας.

Κεφάλαιο 3: Ηθική

Στα προηγούμενα κεφάλαια αναφέρθηκε η διαδικασία με την οποία γίνεται ένα τεστ διείσδυσης, τα εργαλεία τα με τα οποία επιτυγχάνεται μια τέτοια διαδικασία καθώς και παραδείγματα χρήσης αυτών των εργαλείων. Παρακάτω θα αναφερθεί σύντομα το ζήτημα της ηθικής που περιβάλει τη διαδικασία ενός pen test. Σε προηγούμενη ενότητα αναφέρθηκε το γεγονός ότι η διεξαγωγή ενός τεστ διεισδύσεως κινείται ανάμεσα στα όρια του νόμιμου και του παράνομου και για το λόγο αυτό πρέπει να διέπεται από ορισμένους κανόνες. Η ηθική πλευρά των δοκιμών διείσδυσης αποτελείται από κανόνες δέσμευσης που πρέπει να ακολουθούνται από έναν ελεγκτή για να παρουσιάσει επαγγελματικές, ηθικές, και εξουσιοδοτημένες πρακτικές. Αυτοί οι κανόνες

καθορίζουν τον τρόπο με τον οποίο πρέπει να προσφέρονται οι υπηρεσίες ελέγχου, πως πρέπει να γίνονται οι δοκιμές, καθορίζουν τις νομικές συμβάσεις και διαπραγματεύσεις, καθορίζουν την εμβέλεια, το σκοπό των δοκιμών και την προετοιμασία του σχεδίου δοκιμής, το πώς θα ακολουθείται η διαδικασία δοκιμής και το πώς θα γίνει η διαχείριση μια συνεπούς δομής για την υποβολή εκθέσεων. Η αντιμετώπιση κάθε ενός από τα παραπάνω απαιτεί προσεκτική εξέταση και σχεδιασμό των επίσημων πρακτικών και διαδικασιών που πρέπει να ακολουθηθούν σε μια δοκιμή διείσδυσης.

Ορισμένα παραδείγματα αυτών των κανόνων αυτών αναφέρονται ακολούθως.

- Η προσφορά υπηρεσιών δοκιμών διείσδυσης με το ‘σπάσιμο’ του συστήματος-στόχου, πριν την πραγματοποίηση οποιασδήποτε επίσημης συμφωνίας μεταξύ του πελάτη και του ελεγκτή απαγορεύεται. Αυτή η πράξη ανήθικου μάρκετινγκ μπορεί να οδηγήσει στην αποτυχία μιας επιχείρησης και μπορεί να έχει νομικές επιπτώσεις, ανάλογα με τους νόμους κάθε χώρας.
- Η εκτέλεση μιας δοκιμής διείσδυσης εκτός του πεδίου των δοκιμών και η διέλευση εκτός των προσδιορισμένων ορίων χωρίς ρητή άδεια από τον πελάτη, απαγορεύεται.
- Πρέπει να υπογραφεί ένα δεσμευτικό νομικό συμβόλαιο που θα πρέπει να περιορίσει την ευθύνη του ελεγκτή, εκτός αν ανιχνευτεί οποιαδήποτε παράνομη δραστηριότητα. Στο συμβόλαιο αυτό πρέπει να αναφέρονται ρητά οι όροι και οι συνθήκες των δοκιμών, τα στοιχεία επικοινωνίας έκτακτης ανάγκης, η δήλωση της εργασίας, και οποιαδήποτε προφανής σύγκρουση συμφερόντων.
- Στο πεδίο ορισμού θα πρέπει να καθορίζονται με σαφήνεια όλες οι συμβατικές οντότητες και τα όρια που επιβάλλονται σε αυτές κατά τη διάρκεια της αξιολόγησης της ασφάλειας.
- Το σχέδιο δοκιμής αφορά το χρονικό διάστημα που απαιτείται για την αξιολόγηση της ασφάλειας του συστήματος-στόχου. Είναι ιδιαίτερα σημαντικό να καταρτιστεί ένα πρόγραμμα που δεν θα διακόψει την παραγωγή των εργάσιμων ωρών.
- Η διαδικασία δοκιμής καθορίζει το σύνολο των αναγκαία βημάτων που πρέπει να ακολουθηθούν κατά τη διάρκεια της δοκιμής διείσδυσης. Οι κανόνες αυτοί συνδυάζουν τεχνικές και διαχειριστικές απόψεις για να περιορίζουν τη διαδικασία ελέγχου με το περιβάλλον και τους ανθρώπους της.
- Τα αποτελέσματα των δοκιμών και η υποβολή εκθέσεων πρέπει να παρουσιάζονται με σαφή και συνεπή τρόπο. Στην έκθεση πρέπει να σημειώνονται όλα τα γνωστά και άγνωστα κενά ασφαλείας, και θα πρέπει να παραδοθεί εμπιστευτικά μόνο στο εξουσιοδοτημένο άτομο.

Όλοι οι παραπάνω κανόνες θα πρέπει να ακολουθούνται από τον εκάστοτε ελεγκτή ούτως ώστε να καθίσταται νόμιμο και βιώσιμο ένα τεστ διείσδυσης. Εξάλλου μια τέτοια διαδικασία αποτελεί και δείγμα επαγγελματισμού και σίγουρα κατανόησης της ασφάλειας που πρέπει να είναι θέμα προτεραιότητας κάθε οργανισμού που διαχειρίζεται πληροφοριακά συστήματα μικρού ή μεγάλου μεγέθους.

Κεφάλαιο 4 : Πρακτική προσέγγιση

Το κεφάλαιο αυτό που είναι και το τελευταίο της παρούσας διατριβής, θα καταπιαστεί με το πρακτικό κομμάτι ενός penetration test δηλαδή με την εφαρμογή της όλης διαδικασίας που περιγράφηκε σε όλες τις προηγούμενες ενότητες σε μια εφαρμογή ειδικά διαμορφωμένη για εκπαιδευτικούς σκοπούς. Στο σημείο αυτό υπενθυμίζεται το γεγονός ότι μια δοκιμή διείσδυσης θα πρέπει να γίνεται υπό συγκεκριμένες και νόμιμες συνθήκες, οπότε η αυθαίρετη δοκιμή σε οποιαδήποτε Web εφαρμογή είναι επικίνδυνη και για το λόγω αυτό πρέπει να αποφεύγεται.

Η διαδικασία που θα ακολουθηθεί είναι απλή, αλλά χρειάζεται προσοχή διότι θα χρησιμοποιηθούν περισσότερα του ενός μηχανήματα για την επίτευξη των βημάτων του τεστ. Αρχικά η όλη διαδικασία θα «στηθεί» σε έναν υπολογιστή που διαθέτει λειτουργικό σύστημα Windows 7. Σε αυτό το μηχάνημα θα δημιουργηθούν δύο εικονικοί υπολογιστές (virtual machines). Ο μεν πρώτος θα περιλαμβάνει το λειτουργικό DVL (Damn Vulnerable Linux) το οποίο είναι σχεδιασμένο να περιλαμβάνει «ατέλειες» για να μπορεί κάποιος να διενεργεί δοκιμές διαφόρων τύπων και κατά περίπτωση μπορεί να εναλλάσσεται με το Web Security Dojo το οποίο λειτουργεί με παρόμοιο τρόπο.

Ο δε δεύτερος εικονικός υπολογιστής θα περιλαμβάνει το βοήθημα σε αυτή τη διαδικασία που θα είναι το BackTrack 4 R2, το οποίο διαθέτει όλα τα απαραίτητα εργαλεία που θα βοηθήσουν στη διεξαγωγή του τεστ , όπως έχει παρουσιαστεί και αναφερθεί σε προηγούμενες ενότητες. Στο σημείο αυτό τονίζεται το γεγονός ότι πρόκειται για δύο υπολογιστές με λειτουργικό **Linux,** και έτσι δεν υπάρχουν ιδιαίτερες απαιτήσεις υπολογιστικής ισχύος και μνήμης. Παρόλα αυτά η όλη διαδικασία απαιτεί κάποιο χρόνο ώστε να γίνουν όλα τα βήματα. Έτσι ολοκληρώνεται από τεχνικής πλευράς η περιγραφή του penetration test.

Τέλος η όλη διαδικασία θα παρακολουθείται από ένα ειδικό πρόγραμμα, το **Wink**, το οποίο θα καταγράφει όλες τις κινήσεις και τις τεχνικές καθώς και τα εργαλεία που χρησιμοποιούνται κάθε φορά για την περάτωση του εκάστοτε βήματος. Η δοκιμή λοιπόν θα αποτυπωθεί σε μικρού μήκους videos, όπου θα αναπαριστάται τελικά η διενέργεια διείσδυσης. Επισημαίνεται και ξεκαθαρίζεται στο σημείο αυτό ότι κάποια από τα πρώτα βήματα που έχουν περιγραφεί στην παραπάνω ανάλυση, όπως η συλλογή απαιτήσεων και η οριοθέτηση στόχου, θα παραληφθούν και θα επικεντρωθεί η παρουσίαση στα κυρίως πρακτικά βήματα. Τα videos αυτά θα είναι διαθέσιμα σε ξεχωριστώ αρχείο, ενώ παρακάτω παρουσιάζεται μια σύντομη αναφορά στη διαδικασία και στα αποτελέσματα του τεστ, όπως αυτή θα παρουσιαζόταν σε μια εταιρία που θα είχε ζητήσει τη διεξαγωγή του τεστ:

ΑΝΑΦΟΡΑ ΤΕΣΤ ΔΙΕΙΣΔΥΣΗΣ

Επιθετική ασφάλεια μέσω του τεστ διείσδυσης ζητήθηκε να διεξαχθεί στο σύστημα DVL . Η αξιολόγηση διεξήχθη με τη χρήση επισφαλών παραγόντων στο σύστημα – στόχο με σκοπό:

1. Αν κάποιος εξωτερικός παράγοντας μπορεί να εισέλθει στο σύστημα
2. Να καθοριστούν οι επιπτώσεις από το ρήγμα στην ασφάλεια:

    α. στην ακεραιότητα των συστημάτων της εταιρίας

    β. στην εσωτερική υποδομή των πληροφοριακών συστημάτων της εταιρίας

Τα αποτελέσματα αυτής της αξιολόγησης θα χρησιμοποιηθούν για μελλοντικές αποφάσεις σχετικά με την κατεύθυνση του προγράμματος ασφάλειας πληροφοριών. Όλες οι δοκιμές και οι ενέργειες έγιναν κάτω από απολύτως ελεγχόμενο περιβάλλον.

Αναγνώριση δικτύου διεξήχθη στο χώρο διευθύνσεων που παρήχθησαν με την συμφωνία ότι ο χώρος αυτός θα αποτελεί και το πεδίο αυτής της αξιολόγησης. Προσδιορίστηκε επίσης ότι η εταιρία δε θα έχει καμία παρουσία στην όλη διαδικασία, δηλαδή δε θα παρέχει κάποιο υλικό ,όπως μια εξωτερική ιστοσελίδα για παράδειγμα, ως επιφάνεια επίθεσης στον καθορισμένο στόχο.

Κατά την εξέταση της ασφάλειας του συστήματος ανακαλύφθηκαν ευάλωτοι παράγοντες που μπορούσαν να εκμεταλλευθούν για πρόσβαση στο λειτουργικό σύστημα, αλλά και για κλιμάκωση δικαιωμάτων. Μέσω της επιθετικής ασφάλειας κατέστη δυνατή η αναγνώριση πόρων του εσωτερικού δικτύου. Ακόμη σημειώθηκαν ευπάθειες που θα μπορούσαν υπό μη ελεγχόμενες συνθήκες να τοποθετήσουν το σύστημα κάτω από τον έλεγχο κακόβουλων εισβολέων.

Κατά τη διάρκεια του τεστ ανακαλύφθηκαν κάποιες «τρύπες» στο σύστημα. Συγκεκριμένα εντοπίστηκαν ευπάθειες χαμηλού , μεσαίου και υψηλού κινδύνου. Πιο συγκεκριμένα εντοπίστηκε μια ευπάθεια «Heap-based buffer overflow» στην PHP, η οποία δημιουργήθηκε από ένα σφάλμα σε ένα συγκεκριμένο αρχείο, το **mbfilter_htmlent.c**. Για να εξάγουμε αυτό το αποτέλεσμα χρησιμοποιήσαμε το εργαλείο OpenVas. Ο αντίκτυπος που έχει αυτό το σφάλμα, είναι ότι μπορεί να αξιοποιηθεί από εισβολείς με αποτέλεσμα την εκτέλεση αυθαίρετου κώδικα μέσου μιας κατασκευασμένης συμβολοσειράς που περιέχει μια οντότητα HTML. Το προαναφερθέν σφάλμα εντοπίστηκε στην έκδοση 4.3.0 της PHP και μπορεί να διορθωθεί με αναβάθμιση σε πιο ενημερωμένη έκδοση. Μπορεί να φαίνεται σαν κάτι απλό αλλά παρόλα αυτά επισημαίνεται με δείκτη κινδύνου HIGH. Επαλήθευση του προβλήματος παρατηρήθηκε και με τη χρήση εργαλείου ασαφούς λογικής, του JBroFuzz. Στην κατηγορία αυτή εντοπίστηκαν ακόμη δύο σφάλματα.

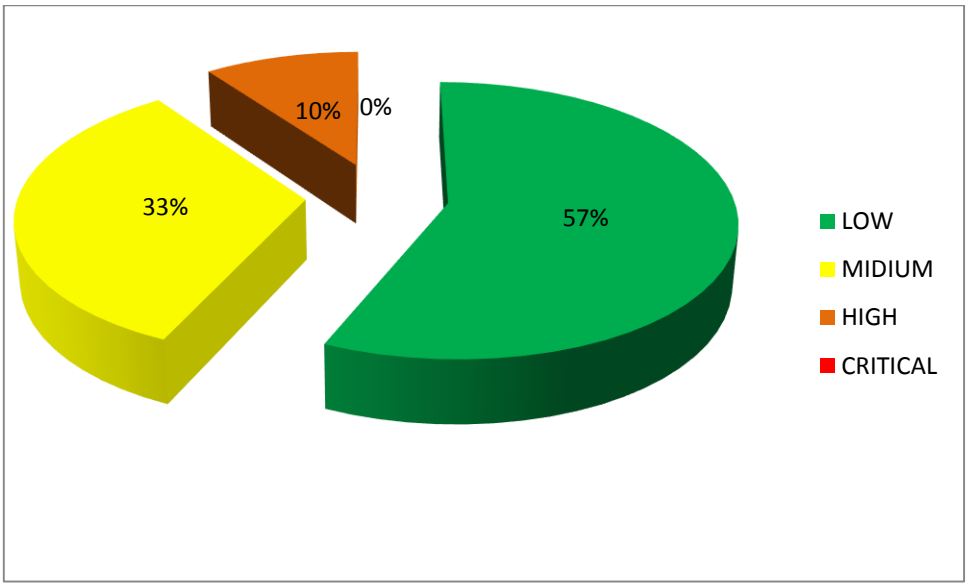
Σε συνέχεια του τεστ διείσδυσης ανακαλύφθηκε ευπάθεια που σχετίζεται με τον Apache Server που τρέχει στο DVL. Ειδικότερα το σφάλμα αυτό οφείλεται σε ελάττωμα του

mod_proxy_ajp , όταν διαχειρίζεται αντικανονικά, «δύσμορφα» αιτήματα POST. Επιτυχημένη εκμετάλλευση της ευπάθειας αυτής από κάποιο κακόβουλο εισβολέα επιτρέπει τη δημιουργία ενός ειδικού αιτήματος POST με τη βοήθεια του οποίου μπορεί να αποκτήσει «ευαίσθητες» πληροφορίες σχετικά με το server. Ο βαθμός επικινδυνότητας χαρακτηρίζεται ως MEDIUM. Λύση σε αυτό το πρόβλημα αποτελεί η ενημέρωση του **mod_proxy_ajp** μέσω του SVN[1] Repository. Τα αντίστοιχα σφάλματα παρόμοιου τύπου ανέρχονται σε δέκα.

Τέλος εντοπίστηκαν σφάλματα που σχετίζονται με τον «X server» και ανέρχονται σε δεκαεπτά στον αριθμό. Πιο συγκεκριμένα ο server απέκλεισε κάθε σύνδεση οποιουδήποτε client διότι δεν υπάρχει φιλτράρισμα των «πακέτων» που δέχεται. Υπάρχει πιθανότητα κάποιος εισβολέας να στείλει «garbage packets», δηλαδή πακέτα που περιέχουν μη αξιοποιήσιμες πληροφορίες με σκοπό να καθυστερεί τον server ή ακόμη να τον αναγκάσει να κλείσει. Αυτού του είδους τα σφάλματα έχουν δείκτη επικινδυνότητας LOW. Ανάκαμψη από αυτές τις ευπάθειες μπορεί να γίνει με ένα καλό φιλτράρισμα στα εισερχόμενα πακέτα σε συγκεκριμένες θύρες και ειδικότερα στις θύρες 6000-6009.

Παρακάτω παρουσιάζεται σχηματικά η ανάλυση και η συγκέντρωση των ευπαθειών που εντοπίστηκαν στο σύστημα:

VALUE	NUMBER OF RISKS
LOW	17
MIDIUM	10
HIGH	3
CRITICAL	0



Εικόνα 16: Πίνακας και γράφημα κινδύνων

[1] Subversion

ΣΥΜΠΕΡΑΣΜΑΤΑ

Κατά τη διάρκεια της διεξαγωγή του τεστ διείσδυσης έγινε φανερό ότι το σύστημα – στόχος υπήρχαν αρκετές ευπάθειες που το καθιστούσαν ανασφαλές. Με τη χρήση εξειδικευμένων εργαλείων εντοπίστηκαν σφάλματα και κίνδυνοι σχεδόν όλης της κλίμακας επικινδυνότητας (LOW-MEDIUM-HIGH). Κάθε σφάλμα με το δικό του τρόπο αν αξιοποιηθεί κακόβουλα μπορεί να προκαλέσει έως και ανεπανόρθωτες ζημιές, από απώλεια δεδομένων μέχρι καταστροφή τόσο του συστήματος όσο και των πολύτιμων δεδομένων που σχετίζονται με το αντικείμενο εργασίας της εταιρίας και τελικά να οδηγήσουν σε οικονομικά προβλήματα και προβλήματα αξιοπιστίας.

Παρόλα αυτά είναι δυνατή η λύση και η διόρθωση των ευπαθειών που εντοπίστηκαν κυρίως με ενημέρωση των υπαρχόντων εκδόσεων των προγραμμάτων που εμφάνισαν τα προβλήματα, όσο και με σωστή παρακολούθηση της κίνησης του δικτύου στο οποίο συνδέεται το σύστημα για αποφυγή κακόβουλων και μη χρήσιμων πακέτων πληροφοριών που μπορεί να βλάψουν το σύστημα. Σε κάθε περίπτωση βέβαια δεν πρέπει να λησμονείται το γεγονός ότι πολλά από αυτά τα προβλήματα πιθανόν να δημιουργούνται από κακόβουλους «εισβολείς» και εντός της εταιρίας, οπότε πρέπει να ελέγχεται και ο ανθρώπινος παράγοντας, ο οποίος ως επί το πλείστον είναι απρόβλεπτος.

Σε γενικότερο πλαίσιο παρατηρείται ότι η διεξαγωγή τεστ διείσδυσης για την αξιολόγηση ενός συστήματος καθίσταται σε πολλές περιπτώσεις απαραίτητη για τη βιωσιμότητα μιας εταιρίας διότι η ασφάλεια δεν είναι κάτι το οποίο μπορεί να θεωρηθεί ασήμαντο και να παραμεριστεί. Ρήγματα στην ασφάλεια μπορεί να οδηγήσουν σε ποικίλα προβλήματα αρκετά από τα οποία πολλές φορές μπορεί να οδηγήσουν σε μη αναστρέψιμες καταστάσεις, αν αυτά δε ληφθούν σοβαρά υπόψη.

Επιπροσθέτως η πρόληψη είναι πολύ σημαντική. Δε χρειάζεται να παρουσιαστούν προβλήματα για να γίνει ένα τεστ διείσδυσης. Μπορεί η εταιρία προληπτικά για λόγους ασφαλείας να διεξάγει σε τακτά χρονικά διαστήματα τεστ για να ελέγξει την ακεραιότητα και την ασφάλεια των συστημάτων της. Εξάλλου η πρόοδος της τεχνολογίας οδηγεί σε συνεχείς βελτιώσεις και ενημερώσεις και για το λόγω αυτό όσοι ασχολούνται με πληροφοριακά συστήματα και διαχείριση δεδομένων θα πρέπει να είναι ενήμεροι τόσο οι ίδιοι όσο και τα συστήματά τους για αποφυγή οποιασδήποτε ευπάθειας.

Τέλος, η παρούσα διατριβή με την ανάλυση των βημάτων και των εργαλείων που χρησιμοποιούνται σε ένα τεστ διείσδυσης, αλλά και με την παρουσίαση μιας σύντομης πρακτικής ανάλυσης θέλησε να καταστήσει σαφές το πόσο σημαντική είναι η ασφάλεια στα πληροφοριακά συστήματα είτε αυτά είναι απλοί ιστότοποι όπως ένα online κατάστημα είτε μηχανήματα – υπολογιστές που διαχειρίζονται κάποια εφαρμογή. Σε κάθε περίπτωση παραμέληση της ασφάλειας οδηγεί σε προβλήματα άλλες φορές επιλύσιμα και άλλες φορές όχι. Για το λόγο αυτό προτείνεται πρόληψη και συνεχής ενημέρωση για αποφυγή δυσάρεστων και ανεπιθύμητων παρενεργειών.

Ευρετήριο όρων :

Λέξεις κειμένου	Επεξήγηση
executive report	εκτελεστική έκθεση
firewall	τείχος προστασίας
FTP	File Transfer protocol – πρωτόκολλο για τη μεταφορά αρχείων.
Fuzzers	εργαλεία για την ανάλυση ασαφούς λογικής που χρησιμοποιείται κατά τη διάρκεια ενός Pen test.
IP address	Internet protocol address – ένας μοναδικός αριθμός που χρησιμοποιείται από συσκευές για τη μεταξύ τους αναγνώριση και συνεννόηση σε ένα δίκτυο υπολογιστών.
MAC address	Media Access Control – μοναδικός δεκαεξαδικός αριθμός για κάθε δικτυακή συσκευή.
Management report	έκθεση διαχείρισης
MD5	Message Digest Algorithm – αλγόριθμος για την εύρεση συναρτήσεων κατακερματισμού.
Penetration testing	δοκιμή διείσδυσης
phishing	ένας τρόπος απόκτησης δεδομένων όπως user names , passwords κλπ
POC	Proof of Concept – είναι η επίτευξη μιας μεθόδου ή μιας ιδέας για να αποδειχθεί το εφικτό της.
Port	θύρα
Privillage escalation	κλιμάκωση προνομίων
proxy tools	εργαλεία μεσολάβησης
SMTP	Simple Mail Transfer Protocol – πρωτόκολλο για τη μετάδοση μυνημάτων ηλεκτρονικού ταχυδρομίου.
SQL	Structured Query Language – είναι μία γλώσσα υπολογιστών στις βάσεις δεδομένων, που σχεδιάστηκε για τη διαχείριση δεδομένων, σε ένα σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων
TCP	transsmition control protocol – επιβεβαιώνει την αξιόπιστη λήψη και μεταφορά δεδομένων και βρίσκεται πάνω από το IP.
Technical report	τεχνική έκθεση
tunneling	ενσωμάτωση ενός πρωτοκόλλου μέσα σε ένα άλλο
UDP	user datagram protocol – χρησιμοποιείται για την αποστολή σύντομων μηνυμάτων και δεν εγγυάται την αξιόπιστη μεταφορά των δεδομένων.
URL	universal resource locator – δηλώνει μια διεύθυνση ενός πόρου του Παγκόσμιου Ιστού.
VPN	virtual private network – είναι ένα δίκτυο που χρησιμοποιεί κατά κύριο λόγο δημόσια τηλεπικοινωνιακή υποδομή, όπως το Διαδίκτυο, για την παροχή σε απομακρυσμένα γραφεία ή σε χρήστες που ταξιδεύουν πρόσβαση σε ένα κεντρικό οργανωτικό δίκτυο.

EOF	Τέλος του αρχείου (κοινώς συντετμημένο EOF) είναι μια κατάσταση όταν περισσότερα δεδομένα δε μπορούν να διαβαστούν από μια πηγή δεδομένων.
SVN APACHE	είναι μια έκδοση λογισμικού για την αναθεώρηση του ελέγχου του συστήματος και διανέμεται υπό τη μορφή ανοικτού κώδικα . Οι προγραμματιστές χρησιμοποιούν Subversion να διατηρήσουν τις σημερινές και ιστορικές εκδόσεις των αρχείων, όπως πηγαίο κώδικα , ιστοσελίδες και έγγραφα. Στόχος του είναι να είναι ως επί το πλείστον συμβατός διάδοχος του ευρέως χρησιμοποιούμενου Concurrent Version Systems (CVS).

Βιβλιογραφία – Παραπομπές

- BackTrack 4 : Assuring Security by Penetration Testing
- Ninja Hacking : Unconventional Penetration Testing Tactic
- www.linux.com
- Professional Penetration Testing : Creating and Operating a Formal Hacking Lab
- www.owasp.org/index.php/Category:OWASP_WebGoat_Project
- http://el.wikipedia.org/wiki/Ασφάλεια_πληροφοριακών_συστημάτων
- http://rightertrack.com/media/pdf/backtrack_tutorial.pdf
- http://www.exploit-db.com
- http://en.wikipedia.org/wiki/Tunneling_protocol
- http://www.unipi.gr/noc/vpn.html
- http://en.wikipedia.org/wiki/Vpn
- http://en.wikipedia.org/wiki/SQL
- http://el.wikipedia.org/wiki/Uniform_Resource_Locator
- http://en.wikipedia.org/wiki/Phishing
- http://en.wikipedia.org/wiki/IP_address
- http://en.wikipedia.org/wiki/End-of-file
- Κρυπτογραφία και εφαρμογές - Κ. Ε. Πατσάκης - Ε. Χ. Φούντας
- http://en.wikipedia.org/wiki/Apache_Subversion
- http://www.offensive-security.com/penetration-testing-sample-report.pdf