Τμήμα Μηχ Η/Υ & Πληροφορικής **Άνοιξη 2014**
Πανεπιστήμιο Ιωαννίνων **Διδάσκων: Σ. Β. Αναστασιάδης**

ΠΛΕ036 Ασφάλεια Υπολογιστικών και Επικοινωνιακών Συστημάτων
Ανακοίνωση: Δευτέρα, 5 Μαΐου, Παράδοση: Παρασκευή, 23 Μαΐου στις 21:00

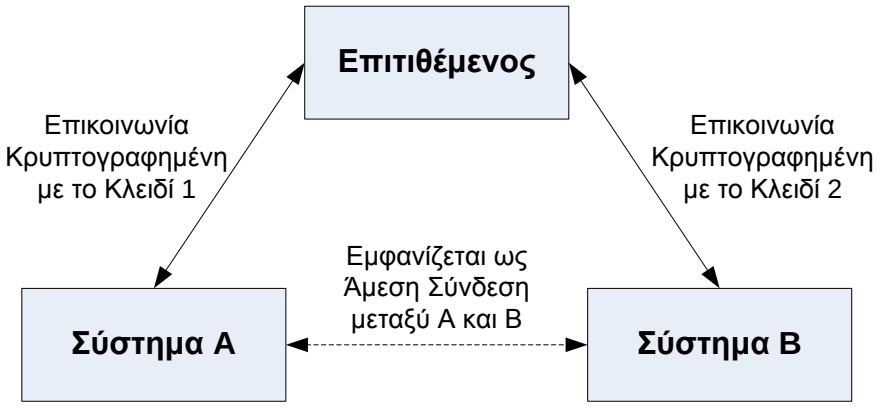
Εργαστήριο 2: Επίθεση Man-in-the-Middle στο SSH του Linux

1. Εισαγωγή

Ένα υβριδικό κρυπτοσύστημα συνδυάζει τη συμμετρική και την ασύμμετρη κρυπτογραφία. Χρησιμοποιεί έναν ασύμμετρο κώδικα για την ανταλλαγή τυχαίου κλειδιού, το οποίο χρησιμοποιεί για την υπόλοιπη επικοινωνία με βάση κάποιο συμμετρικό κώδικα. Έτσι προσφέρει την ταχύτητα του συμμετρικού κώδικα, ενώ λύνει το πρόβλημα της ασφαλούς ανταλλαγής κλειδιών. Οι υβριδικές προσεγγίσεις χρησιμοποιούνται από τις περισσότερες κρυπτογραφικές εφαρμογές, όπως SSL, SSH και PGP. Εφόσον οι κώδικες που εφαρμόζονται είναι ανθεκτικοί στην κρυπτανάλυση, ο επιτιθέμενος συνήθως προτιμά να παρεμβληθεί στην επικοινωνία μεταξύ δύο μερών και να μεταμφιεστεί το ένα ή το άλλο μέρος προκειμένου να επιτεθεί στον αλγόριθμο ανταλλαγής κλειδιών.

1.1 Επίθεση Man-in-the-Middle

Όταν εγκαθιστούμε μια κρυπτογραφική σύνδεση μεταξύ δύο μερών, δημιουργείται ένα μυστικό κλειδί και ανταλλάσσεται με ασύμμετρο κώδικα. Εφόσον το κλειδί αποστέλλεται με ασφάλεια και διασφαλίζει την επακόλουθη επικοινωνία, λογικά η ανταλλασσόμενη πληροφορία δεν μπορεί να αποκρυπτογραφηθεί από κάποιον που απλώς την αντιγράφει. Κατά την επίθεση man-in-the-middle ο επιτιθέμενος βρίσκεται μεταξύ των δύο επικοινωνούντων μερών και κάνει το καθένα να πιστεύει ότι επικοινωνεί με το άλλο, ενώ στην πραγματικότητα και οι δύο επικοινωνούν με τον επιτιθέμενο. Επομένως, όταν ο Α διαπραγματεύεται μια κρυπτογραφημένη επικοινωνία με τον Β, ο Α ανοίγει κρυπτογραφημένη σύνδεση με τον επιτιθέμενο. Αντίστοιχα, ο Β ανοίγει κρυπτογραφημένη επικοινωνία με τον επιτιθέμενο και όχι άμεσα με τον Α.

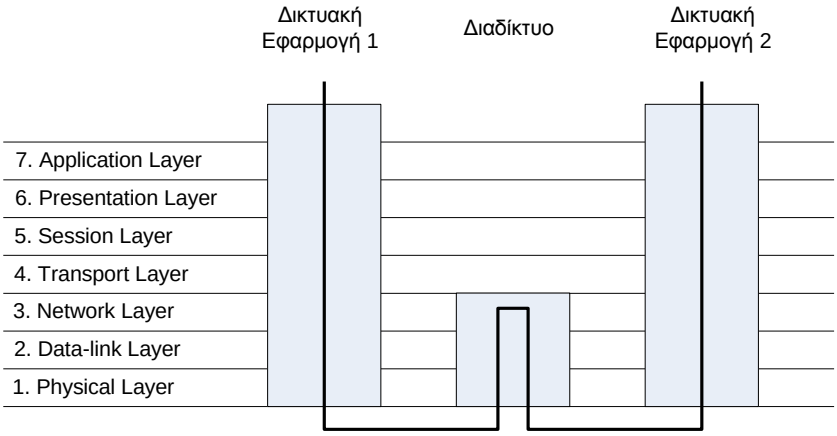


Ουσιαστικά, τα πακέτα του Α κρυπτογραφούνται με το Κλειδί 1 και στέλνονται στον επιτιθέμενο. Τότε, ο επιτιθέμενος αποκρυπτογραφεί τα πακέτα και τα επανακρυπτογραφεί με το Κλειδί 2, πριν τα στείλει στον Β. Έτσι ο επιτιθέμενος υποκλέπτει και ενδεχομένως τροποποιεί τα πακέτα.

1.2 Μοντέλο OSI (Open Systems Interconnection)

Όταν δύο υπολογιστές μιλούν ο ένας στον άλλο, χρειάζονται κάποια κοινή γλώσσα. Η δομή της γλώσσας αυτής περιγράφεται με τα επίπεδα του μοντέλου OSI. Το *φυσικό επίπεδο (physical)*

ασχολείται με τη φυσική σύνδεση μεταξύ δύο σημείων. Το *επίπεδο διασύνδεσης δεδομένων (data-link)* διαχειρίζεται τη μεταφορά δεδομένων μεταξύ δύο σημείων. Το Ethernet λειτουργεί στο επίπεδο αυτό για να προσφέρει πρότυπη διευθυνσιοδότηση σε όλες τις συσκευές Ethernet. Οι αντίστοιχες διευθύνσεις είναι γνωστές ως διευθύνσεις Ελέγχου Πρόσβασης Μέσου (Media Access Control, MAC). Το *επίπεδο δικτύου* (*network)* υποστηρίζει τη διευθυνσιοδότηση και δρομολόγηση, π.χ. μέσω του Πρωτοκόλλου Διαδικτύου (Internet Protocol, IP). Κάθε σύστημα στο Διαδίκτυο (έκδοση 4) διαθέτει μια διεύθυνση IP που αποτελείται από τέσσερα bytes με τη μορφή xx.xx.xx.xx. Το *επίπεδο μεταφοράς* (*transport)* προσφέρει αξιόπιστη επικοινωνία μεταξύ διαφορετικών συστημάτων, π.χ. το Πρωτόκολλο Ελέγχου Μετάδοσης (Transmission Control Protocol, TCP). Τέλος, το *επίπεδο συνεδρίας (session)* εγκαθιστά συνδέσεις μεταξύ εφαρμογών, το *επίπεδο παρουσίασης* (*presentation)* επιτρέπει λειτουργίες όπως η κρυπτογράφηση και συμπίεση, ενώ το *επίπεδο εφαρμογών* (*application)* διαχειρίζεται απαιτήσεις εξειδικευμένες για κάθε εφαρμογή.



1.3 ARP Cache Poisoning

Στο επίπεδο διασύνδεσης, ένα δίκτυο εκπομπής (unswitched) στέλνει τα πακέτα σε κάθε συσκευή του δικτύου, περιμένοντας ότι κάθε συσκευή θα ανοίξει μόνο τα πακέτα που ορίζουν τη δική της διεύθυνση MAC ως προορισμό. Σε ένα δίκτυο μεταγωγής (switched), όμως, τα πακέτα στέλνονται μόνο στη θύρα προορισμού τους, σύμφωνα με τη διεύθυνση MAC. Παρόλο που η δεύτερη περίπτωση έχει κάποια επιπλέον δυσκολία, είναι δυνατό σε ένα δίκτυο μεταγωγής μία συσκευή να υποκλέψει τα πακέτα άλλων συσκευών.

Προκειμένου να συσχετίσει τη διεύθυνση IP με τη διεύθυνση MAC μιας δικτυακής συσκευής, το Ethernet εφαρμόζει μια μέθοδο γνωστή ως Address Resolution Protocol (ARP). Μια αίτηση ARP είναι μήνυμα που στέλνεται στο δίκτυο και καθορίζει μία διεύθυνση IP, ενώ ζητά την αντίστοιχη διεύθυνση MAC. Η απάντηση ARP είναι το αντίστοιχο μήνυμα που στέλνεται πίσω από τη συσκευή που έχει την καθορισμένη διεύθυνση IP. Η απάντηση προσδιορίζει τη διεύθυνση MAC που ζητήθηκε και τη σχετική διεύθυνση IP. Οι περισσότερες υλοποιήσεις αποθηκεύουν προσωρινά τα ζεύγη MAC/IP που καθορίστηκαν σε πρόσφατες απαντήσεις ARP. Για παράδειγμα, έστω το σύστημα Α έχει διεύθυνση IP 192.168.148.137 και διεύθυνση MAC 00:00:00:aa:aa:aa, ενώ το σύστημα Β έχει διεύθυνση IP 192.168.148.139 και διεύθυνση MAC 00:00:00:bb:bb:bb.

Τώρα, αν τα δύο συστήματα βρίσκονται στο ίδιο δίκτυο, χρειάζονται το καθένα τη διεύθυνση MAC του άλλου για να επικοινωνήσουν. Ο επιτιθέμενος μπορεί να δημιουργήσει απαντήσεις ARP που στοχοποιούν συγκεκριμένη συσκευή Β και την κάνουν να πιστεύει ότι η συσκευή Α έχει τη διεύθυνση MAC του επιτιθέμενου *(ARP cache poisoning)*. Παρομοίως, ο επιτιθέμενος μπορεί να στείλει απαντήσεις ARP στη συσκευή Α και να την κάνει να πιστεύει ότι η συσκευή Β έχει τη

διεύθυνση MAC του επιτιθέμενου. Συνεπώς, ο επιτιθέμενος λαμβάνει όλα τα πακέτα που ανταλλάσσονται μεταξύ των A και B πριν τα προωθήσει στο άλλο μέρος.

2. Περιβάλλον Εργαστηρίου

Προκειμένου να πετύχετε επίθεση man-in-the-middle σε εργαστηριακό περιβάλλον, σας δίνεται μια συμπιεσμένη εικονική μηχανή (PLE036-L2.zip) που τρέχει Linux με πυρήνα 2.6.26. Η μηχανή λέγεται **debian** και έχει διεύθυνση IP **192.168.148.137**. Μέσα στην εικονική μηχανή θα βρείτε δύο άλλες εικονικές μηχανές, που ονομάζονται **debian0** και **debian1** με αντίστοιχες διευθύνσεις IP **192.168.148.138** και **192.168.148.139**. Προκειμένου να τις ξεκινήσετε, θα χρειαστεί να καλέσετε ως **user** από τον κατάλογο **~user** τις εντολές

debian>./linux0
debian>./linux1

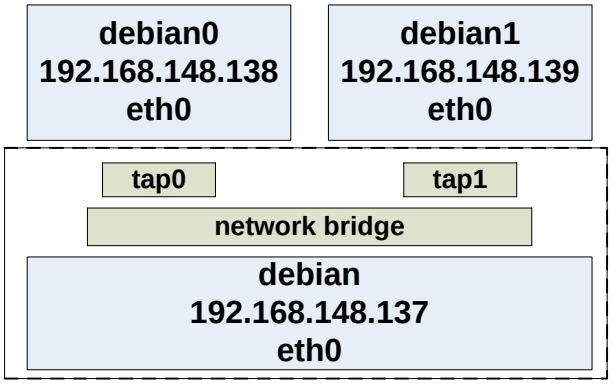
Μπορείτε να χρησιμοποιήσετε τερματικά που είναι διαφορετικά από την κονσόλα του **debian** πιέζοντας ALT-F2 και ALT-F3. Κάθε μηχανή έχει ένα λογαριασμό **root** με συνθηματικό **root** και λογαριασμό χρήστη **user** με συνθηματικό **user**.

2.1 Δικτυακές Επικοινωνίες

Οι τρεις μηχανές διασυνδέονται η καθεμία με τις άλλες μέσω μιας εικονικής συσκευής γέφυρας (bridge). Στη μηχανή **debian**, αν καλέσετε ως **root**

debian# ifconfig |less

θα δείτε τέσσερις δικτυακές συσκευές, **eth0**, **tap0**, **tap1** και **bridge**. Η **eth0** είναι η κάρτα δικτύου Ethernet της **debian**, ενώ η συσκευή **bridge** υπάρχει για να προσφέρει συνδεσιμότητα στις άλλες δύο μηχανές, μέσω των εικονικών δικτυακών καρτών **tap0** και **tap1** αντίστοιχα.



Μπορείτε να επαληθεύσετε την επικοινωνία των διαφορετικών συσκευών με χρήση της εντολής **ping**, π.χ. για να ελέγξετε ότι η **debian** μιλά με τις **debian0** και **debian1**

debian# ping 192.168.148.138
debian# ping 192.168.148.139

Επιπλέον, μπορείτε να χρησιμοποιήσετε **ssh** για να επικοινωνήσετε από το μία μηχανή στην άλλη.

2.2 Το Εργαλείο Nemesis

Στη μηχανή **debian0**, μπορείτε να καλέσετε την εντολή **nemesis** που σας επιτρέπει να δημιουργήσετε απαντήσεις ARP με τα πεδία που ορίζετε εσείς. Επίσης, μπορείτε να καλέσετε

debian0# nemesis arp help

για να λάβετε την περιγραφή των πεδίων που δέχεται ως είσοδο. Για την κλήση της εντολής **nemesis** θα πρέπει να είστε **root**.

Μπορείτε να χρησιμοποιήσετε το **nemesis** από το **debian0** προκειμένου να στείλετε πλαστές απαντήσεις ARP στις **debian** και **debian1**. Για το σκοπό αυτό, θα πρέπει να χρησιμοποιήσετε τα πεδία **-DhmrdHM** και να αγνοήστε τα **-sRP**. Μπορείτε να μάθετε τις διευθύνσεις MAC των **debian0** και **debian1** καλώντας **ifconfig eth0** μέσα στις αντίστοιχες μηχανές. Επιπλέον, θα χρειαστείτε τη διεύθυνση MAC της **debian**, και τις διευθύνσεις IP και των τριών μηχανών.

Αν η αλλαγή της κρυφής μνήμης ARP (ARP cache poisoning) είναι επιτυχής, η **debian** θα στείλει στη **debian0** τα πακέτα που κανονικά κατευθύνονται στη **debian1**, ενώ η **debian1** θα στείλει στη **debian0** τα πακέτα που κανονικά κατευθύνονται στη **debian**. Μπορείτε να ελέγξετε τη διεύθυνση MAC που σχετίζεται με γνωστές διευθύνσεις IP στις **debian0** και **debian1** καλώντας ως **root** την εντολή **arp**, π.χ.

debian# arp -na
debian1# arp -na

Προκειμένου να παραμείνουν οι αλλαγές στην κρυφή μνήμη ARP, θα πρέπει να δημιουργήσετε ένα script που καλεί τις αναγκαίες εντολές **nemesis** περιοδικά κάθε 10 δευτερόλεπτα.

2.3 Η Υπηρεσία mitm-ssh

Στη μηχανή **debian0**, θα πρέπει να καλέσετε μια υπηρεσία που ακούει για εισερχόμενες αιτήσεις **ssh** από την **debian** προς την **debian1**. Αυτό προϋποθέτει ότι οι κρυφές μνήμες ARP των **debian** και **debian1** έχουν τροποποιηθεί επιτυχώς από την **debian0**. Για την παρεμβολή, θα χρειαστείτε την υπηρεσία **mitm-ssh**, που είναι τροποποιημένο λογισμικό **ssh** διαθέσιμο στον παγκόσμιο ιστό. Μπορείτε να δείτε τις επιλογές του **mitm-ssh** με την εντολή **mitm-ssh**. Για τις ανάγκες της άσκησης, θα χρειαστείτε τις επιλογές **-vnp** και θα αγνοήσετε τις **-dfcso**. Ειδικότερα, θα πρέπει να επισυνάψετε το **mitm-ssh** στη θύρα 2222 της **debian0**. Προκειμένου να ανακατευθύνετε την κυκλοφορία που φτάνει από τη θύρα 22 της **domain0** στη θύρα 2222, όπου ακούει το **mitm-ssh**, θα χρειαστεί να καλέσετε στη **debian0** ως **root** την εντολή

debian0# enable_redir

Τέλος, θα κάνετε **ssh** από τη **debian** προς τη **debian1**:

debian> ssh 192.168.148.139

Αν η επίθεση είναι επιτυχής, θα δείτε τις πληροφορίες ταυτοποίησης και το συνθηματικό, στη **debian0**. Επιπλέον, θα βρείτε όλη την κυκλοφορία της συνεδρίας **ssh** μεταξύ των **debian** και **debian1** αποθηκευμένη σε ένα αρχείο του καταλόγου **/usr/local/var/log/mitm-ssh** στη μηχανή **debian0**.

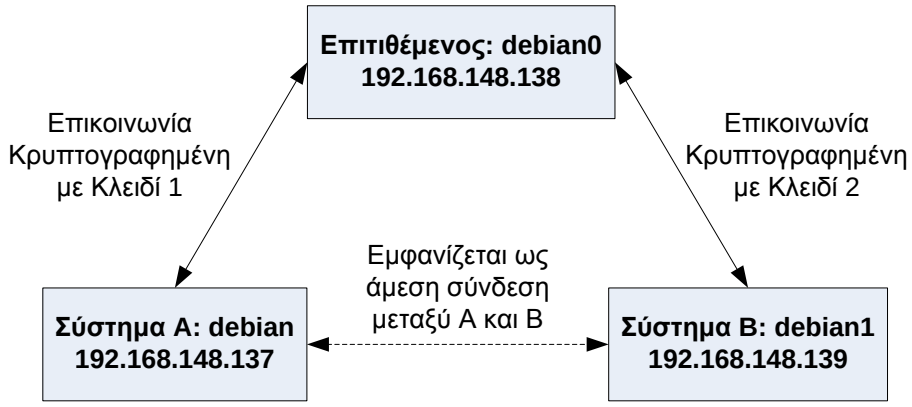
3. Προετοιμασία

Κατεβάστε το αρχείο PLE036-L2.zip (~1.1GB) και αποσυμπιέστε το (με **unzip**) σε μνήμη USB ελάχιστης χωρητικότητας 2GB. Εκκινήστε την εικονική μηχανή. Σε δύο ξεχωριστά τερματικά που θα βρείτε πιέζοντας ALT-F2 και ALT-F3, μπείτε στο σύστημα ως **user**. Στα τερματικά 2 και 3, εκκινήστε τις εικονικές μηχανές **debian0** και **debian1** με τις εντολές **./linux0** και ./**linux1**. Επαληθεύστε ότι οι τρεις μηχανές μιλάνε οι καθεμία στις άλλες δύο με **ping**.

4. Εργασία

Για να κάνετε παρεμβολή στην επικοινωνία **ssh** από τη **debian** στη **debian1** μέσω της **debian0**, χρησιμοποιήστε τα παρακάτω βήματα

1. Δοκιμάστε να συνδεθείτε με κανονικό **ssh** από τη **debian** στη **debian1** και βεβαιωθείτε ότι δουλεύει. Στη συνέχεια, τερματίστε τη παραπάνω σύνδεση **ssh**.
2. Βρείτε τις επιλογές του **nemesis** για κάνετε τη **debian0** να φανεί ως **debian1** στη **debian**.
3. Επαναλάβετε το βήμα (2) προκειμένου η **debian0** να εμφανίζεται ως **debian** στη **debian1**.
4. Χρησιμοποιήστε ένα απλό script για να επαναλάβετε τα βήματα (2-3) κάθε 10 δευτερόλεπτα.
5. Καλέστε **enable-redir** στη **debian0**.
6. Στο τερματικό 2, καλέστε **mitm-ssh** με κατάλληλες επιλογές για να παρεμβληθείτε στην επικοινωνία **ssh** από τη **debian** στη **debian1.**
7. Προσπαθήστε να συνδεθείτε από τη **debian** στη **debian1** με κανονικό **ssh**. Στην προτροπή, εισάγετε μερικά λάθος συνθηματικά, πριν χρησιμοποιήστε το σωστό. Αν λάβετε μήνυμα για επίθεση man-in-the-middle, προχωρήστε στις αναγκαίες αλλαγές του αρχείου **~user/.ssh/known_hosts** της **debian**.
8. Επαληθεύστε ότι η παρεμβολή πέτυχε, εξετάζοντας την έξοδο στο τερματικό 2.



4 Τι θα παραδώσετε

Θα ετοιμάσετε τη λύση ατομικά. Υποβολή μετά την προθεσμία μειώνει το βαθμό 10% κάθε ημέρα μέχρι 50%. Υποβάλλετε τη λύση σας με την εντολή

turnin lab2_14@ple036 group README.pdf file1 …

Το αρχείο **group** περιέχει μία γραμμή με τον κωδικό και το όνομα του φοιτητή με λατινικούς χαρακτήρες. Αρχείο **README.pdf** περιέχει μια περιγραφή των εντολών που χρησιμοποιήσατε στην εργασία. Συμπεριλάβετε όλα τα scripts που προσθέσατε ή τροποποιήσατε. Ο κώδικάς σας πρέπει να τρέχει σε περιβάλλον VMware πανω σε Debian μηχανές του Τμήματος.