Τμήμα Μηχανικών Η/Υ & Πληροφορικής **Χειμερινό 2021**
Πανεπιστήμιο Ιωαννίνων **Διδάσκων: Σ. Αναστασιάδης**

ΜΥΕ007 Ασφάλεια Υπολογιστικών και Επικοινωνιακών Συστημάτων
Ανακοίνωση: Τετάρτη, 1 Δεκεμβρίου, Παράδοση: Παρασκευή, 17 Δεκεμβρίου στις 21:00

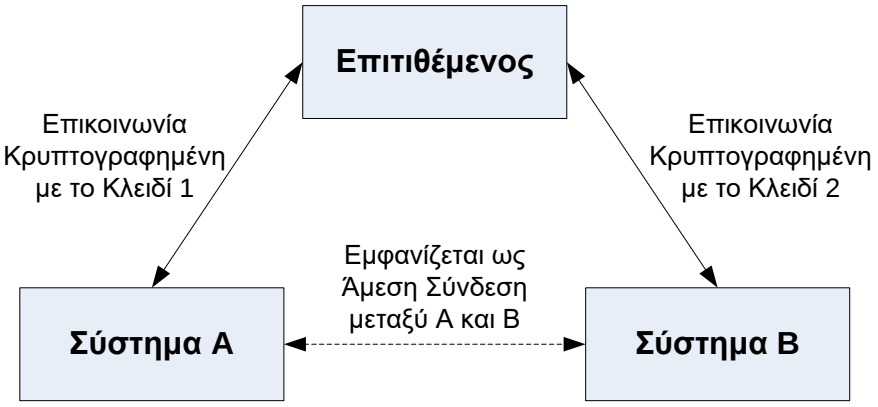
Εργαστήριο 2: Επίθεση Man-in-the-middle στο SSH του 64-bit Linux

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.

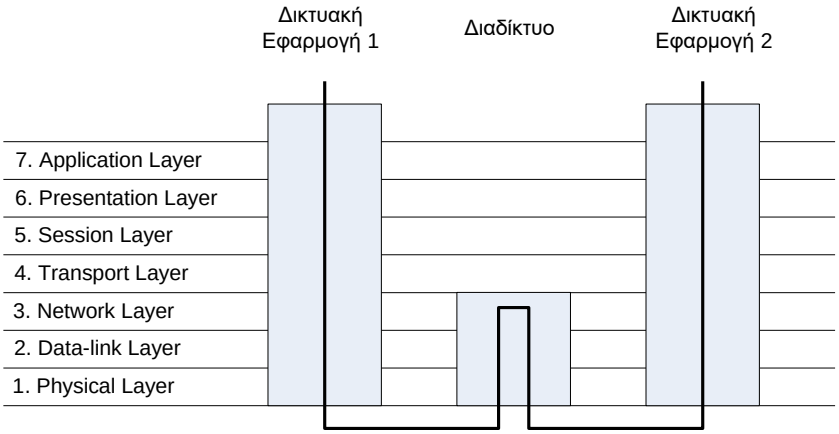


Ουσιαστικά, τα πακέτα του Α κρυπτογραφούνται με το Κλειδί 1 και στέλνονται στον επιτιθέμενο. Τότε, ο επιτιθέμενος αποκρυπτογραφεί τα πακέτα και τα επανακρυπτογραφεί με το Κλειδί 2, πριν τα στείλει στον Β. Έτσι ο επιτιθέμενος υποκλέπτει και ενδεχομένως τροποποιεί τα πακέτα.

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 192.168.122.105 και διεύθυνση MAC 00:00:00:aa:aa:aa, ενώ το σύστημα Β έχει διεύθυνση IP 192.168.122.57 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 (MYE007-L2.zip) που τρέχει Linux με πυρήνα 3.16.0. Η μηχανή λέγεται **mye007** και έχει διεύθυνση IP **192.168.73.143**. Η μηχανή έχει ένα πλήρως λειτουργικό γραφικό περιβάλλον στο οποίο μπορείτε να μπείτε ως **root** (με κωδικό πρόσβασης mye007). Για διευκόλυνσή σας, μπορείτε να κάνε αντιγραφή και επικόλληση μεταξύ της εικονικής μηχανής και του υπολογιστή που την φιλοξενεί εφόσον είναι ενεργοποιημένη η δικτυακή τους σύνδεση.

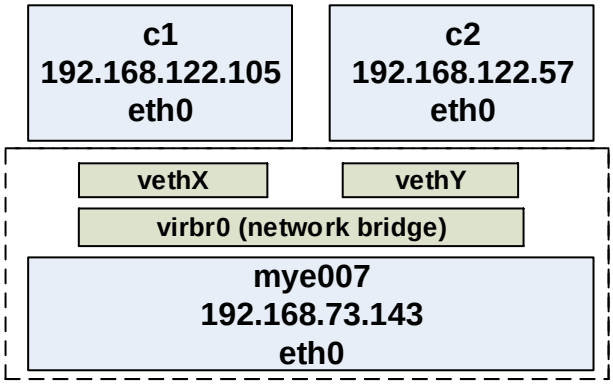
Μέσα στην εικονική μηχανή θα βρείτε δύο άλλες εικονικές μηχανές, που ονομάζονται **c1** και **c2** με αντίστοιχες διευθύνσεις IP **192.168.122.105** και **192.168.122.57**. Μπορείτε να τις ξεκινήσετε με τις εντολές **lxc-start -n c1 -d** και **lxc-start -n c2 -d**. Μπορείτε να συνδεθείτε με αυτές χρησιμοποιώντας **ssh** ή απλώς καλώντας **lxc-attach** (π.χ., lxc-attach -n c1) και να τις σταματήσετε με **lxc-stop** (π.χ., lxc-stop -n c1). Κάθε μηχανή έχει έναν λογαριασμό root προσβάσιμο με κωδικό πρόσβασης mye007.

2.1 Δικτυακές Επικοινωνίες

Οι τρεις μηχανές διασυνδέονται η καθεμία με τις άλλες μέσω μιας εικονικής συσκευής γέφυρας (bridge). Στη μηχανή **mye007**, αν καλέσετε ως **root**

mye007# ifconfig

θα δείτε τέσσερις δικτυακές συσκευές, **eth0**, **vethX**, **vethY** (τα X και Y είναι τυχαίες συμβολοσειρές του συστήματος) και **virbr0**. Η **eth0** είναι η κάρτα δικτύου Ethernet της **mye007**, ενώ η συσκευή **virbr0** υπάρχει για να προσφέρει συνδεσιμότητα στις άλλες δύο μηχανές, μέσω των εικονικών δικτυακών καρτών **vethX** και **vethY** αντίστοιχα.



Μπορείτε να επαληθεύσετε την επικοινωνία των διαφορετικών συσκευών με χρήση της εντολής **ping**, π.χ. για να ελέγξετε ότι η **mye007** μιλά με τις **c1** και **c2**

mye007# ping 192.168.122.105
mye007# ping 192.168.122.57

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

2.2 Το Εργαλείο Wireshark Network Analyzer

Στη μηχανή **mye007**, μπορείτε να καλέσετε την εντολή **wireshark** που σας επιτρέπει να δείτε τα πακέτα που περνάνε από μία κάρτα δικτύου της επιλογής σας. Για παράδειγμα, μπορείτε να καλέσετε

mye007# wireshark &

και αν επιλέξετε την δικτυακή κάρτα **virbr0**, να ξεκινήσετε την παρακολούθηση πατώντας **Start**. Δείτε την λειτουργία σε εξέλιξη εκτελώντας μια δικτυακή εντολή, π.χ., **ping 192.168.122.105** από τη **mye007**. Για να φιλτράρετε την κυκλοφορία και να δείξετε μόνο ένα συγκεκριμένο τύπο πρωτοκόλλου πρέπει να εισάγετε στο πλαίσιο **Filter** το όνομα του πρωτοκόλλου (π.χ., **arp**). Μπορείτε να πειραματιστείτε περαιτέρω με το εργαλείο ξεκινώντας μια σύνδεση **ssh** από το **c1** στο **c2** και να παρακολουθήσετε την κυκλοφορία που περνάει από τη γέφυρα.

2.3 Το Εργαλείο ettercap

Στη μηχανή **mye007**, μπορείτε να καλέσετε την εντολή **ettercap** προκειμένου να ξεκινήσετε το εργαλείο **ettercap**. Αυτό το εργαλείο μπορεί να χρησιμοποιηθεί για να παρακολουθήσει την κυκλοφορία σε μια δικτυακή κάρτα της επιλογής σας και επίσης για να εκτελέσει επιθέσεις man-in-the-middle. Το εργαλείο δέχεται τις επιλογές –T ή –G για να ξεκινήσει σε κατάσταση κειμένου ή γραφικών, π.χ., **ettercap -G &**. Μπορείτε να εξοικειωθείτε με το εργαλείο χρησιμοποιώντας το μενού **Info** και επιλέγοντας τη βοήθεια με την τεκμηρίωση του **ettercap**.

Μπορείτε να επιλέξετε **Unified Sniffing** σε κατάλληλη δικτυακή κάρτα κάτω από την επιλογή **Sniff** και μετά να αναζητήσετε υπάρχοντα μηχανήματα κάνοντας **Scan** κάτω από την επιλογή **Hosts** και να επιλέξετε κάποια από αυτά ως στόχους. Μετά μπορείτε να ξεκινήσετε την μόλυνση **ARP Poisoning** ως επίθεση ενδιάμεσου και να παρακολουθήσετε την δικτυακή κυκλοφορία με το εργαλείο **Wireshark**.

2.4 Η Υπηρεσία mitm-ssh

Στη μηχανή **mye007**, θα πρέπει να καλέσετε μια υπηρεσία που ακούει για εισερχόμενες αιτήσεις **ssh** από την **c1** προς την **c2**. Αυτό προϋποθέτει ότι οι κρυφές μνήμες ARP των **c1** και **c2** έχουν τροποποιηθεί επιτυχώς από την **mye007** όπως περιγράφηκε παραπάνω με το **ettercap**. 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** στη μηχανή **mye007**. 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 **mye007**. Προκειμένου να ανακατευθύνετε την κυκλοφορία που φτάνει από τη θύρα 22 της **mye007** στη θύρα 2222, όπου ακούει το **mitm-ssh**, θα χρειαστεί να καλέσετε στη **mye007** ως **root** την εντολή

mye007# enable_redir

Τέλος, θα κάνετε **ssh** από τη **c1** προς τη **c2**:

c1# ssh 192.168.122.57

Αν η επίθεση είναι επιτυχής, θα δείτε τις πληροφορίες ταυτοποίησης και το συνθηματικό, στη **mye007**. Επιπλέον, θα βρείτε όλη την κυκλοφορία της συνεδρίας **ssh** μεταξύ των **c1** και **c2** αποθηκευμένη σε ένα αρχείο του καταλόγου **/usr/local/var/log/mitm-ssh** στη μηχανή **mye007**.

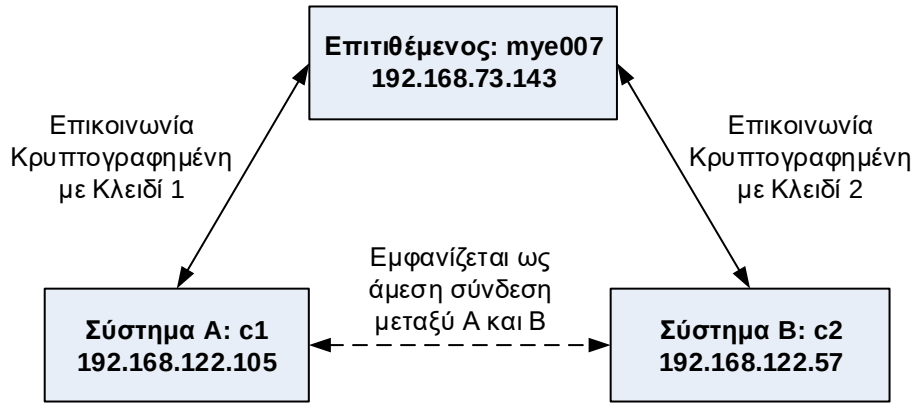
3. Προετοιμασία

Κατεβάστε το αρχείο MYE007-L2.zip και αποσυμπιέστε το (με **unzip**) σε μνήμη USB ελάχιστης χωρητικότητας 8GB. Εκκινήστε την εικονική μηχανή και εισέρθετε από το γραφικό περιβάλλον ως **root**. Ξεκινήστε δύο ξεχωριστά τερματικά και βάλετε σε λειτουργία τις εικονικές μηχανές **c1** και **c2** με τον τρόπο που περιγράφηκε παραπάνω. Επαληθεύστε ότι οι τρεις μηχανές μιλάνε οι καθεμία στις άλλες δύο με **ping**.

4. Εργασία

Για να κάνετε παρεμβολή στην επικοινωνία **ssh** από τη **c1** στη **c2** μέσω της **mye007**, χρησιμοποιήστε τα παρακάτω βήματα

1. Δοκιμάστε να συνδεθείτε με κανονικό **ssh** από τη **c1** στη **c2** και βεβαιωθείτε ότι η σύνδεση δουλεύει. Στη συνέχεια, τερματίστε τη παραπάνω σύνδεση **ssh**. Μπορείτε να σβήσετε το αρχείο **/root/.ssh/known_hosts** της **c1** για να αποφύγετε παράπονα ότι έχει τροποποιηθεί το κλειδί του προορισμού με αποτέλεσμα να αποτυγχάνει η σύνδεση.
2. Βρείτε τις επιλογές του **ettercap** για κάνετε τη **mye007** να φανεί ως **c2** στη **c1** και ως **c1** στη **c2** και επαληθεύστε με **Wireshark** (μπορείτε να πάρετε ένα screenshot).
3. Προσπαθήστε να συνδεθείτε με **ssh** από την **c1** στην **c2** και εξηγήστε την αποτυχία της σύνδεσης αξιοποιώντας κατάλληλα την κυκλοφορία που παίρνετε από το **Wireshark**.
4. Καλέστε **enable_redir** στη **mye007**.
5. Ξαναπροσπαθήσετε το βήμα 3 και εξηγήστε.
6. Σε ένα διαφορετικό τερματικό της **mye007**, καλέστε **mitm-ssh** με κατάλληλες επιλογές για να παρεμβληθείτε στην επικοινωνία **ssh** από τη **c1** στη **c2.**
7. Προσπαθήστε να συνδεθείτε από τη **c1** στη **c2** με **ssh**. Στην προτροπή, εισάγετε μερικά λάθος συνθηματικά, πριν χρησιμοποιήστε το σωστό.
8. Επαληθεύστε ότι η παρεμβολή πέτυχε, εξετάζοντας την έξοδο στο τερματικό που εκτελεί την **mitm-ssh** και το αρχείο καταγραφής της **mitm-ssh** καθώς και αξιοποιώντας την έξοδο του **Wireshark**.



5. Τι θα παραδώσετε

Θα ετοιμάσετε τη λύση ατομικά ή σε ομάδα των 2. Υποβολή μετά την προθεσμία μειώνει το βαθμό 10% κάθε ημέρα μέχρι 50%. Υποβάλλετε τη λύση σας με την εντολή

turnin lab2_21@mye007 Documentation.pdf file1 …

Το αρχείο **Documentation.pdf** περιέχει μια αναλυτική περιγραφή των βημάτων που ακολουθήσατε και των εντολών που χρησιμοποιήσατε στην εργασία. Μπορείτε να παραθέσετε τις δυσκολίες που αντιμετωπίσατε και πώς καταλήξατε στην λύση που προτείνετε. Συμπεριλάβετε όλα τα scripts που προσθέσατε για να ολοκληρώσετε την επίθεση. Ο κώδικάς σας πρέπει να τρέχει σε περιβάλλον VMware πάνω σε Debian μηχανές του Τμήματος ή τον προσωπικό σας υπολογιστή.