Σε αυτήν την εργαστηριακή άσκηση έχουμε 3 εικονικές μηχανές μου τρέχουν σε περιβάλλον vmware, την debian0,debian1 και debian.Σκοπός της άσκησης είναι να παρεμβληθούμε στην κρυπτογραφημένη επικοινωνία μεταξύ των μηχανών debian και debian1 μέσω της debian0 η οποία θα μεταμφιεστεί στο ένα ή το άλλο μέρος προκειμένου να επιτεθούμε στον αλγόριθμο ανταλλαγής των κλειδιών.

Αρχικά εκκινούμε την debian.Κάνουμε login με δικαιώματα root.Ύστερα μπαίνουμε στον κατάλογο user (cd /home/user) και εκκινούμε την μηχανή debian0 εκτελώντας ./linux0 και ./linux1 για την debian1 κάνουμε login και στις 2 μηχανές με δικαιώματα user.Πληκτρολογούμε και στις 3 μηχανές ifconfig eth0(eth0 το interface),για να πάρουμε τις αντίστοιχες διευθύνσεις IP και MAC.Το αποτέλεσμα της εντολής έχει ως εξής:

	IP	MAC
Debian	192.168.148.137	00:0c:29:3b:cf:d3
Debian0	192.168.148.138	2a:22:23:90:a0:9f
Debian1	192.168.148.139	4e:32:24:ce:0a:81

Στην συνέχεια εκτελούμε

debian ping 192.168.139(για έλεγχο επικοινωνίας με debian1)
debian ping 192.168.148.138(για έλεγχο επικοινωνίας με debian0)
debian0 ping 192.168.148.139(για έλεγχο επικοινωνίας με debian1)

Αφού βεβαιωθούμε για την επικοινωνία προβαίνουμε στην φάση του ARP Poising.Δημιουργούμε ουσιαστικά απαντήσεις ARP στοχοποιώντας την debian έτσι ώστε να πιστεύει οτι η debian1 έχει την MAC διεύθυνση της debian0(επιτιθέμενος) και αντίστοιχα να πιστεύει η debian1 οτι η debian έχει την MAC διεύθυνση της debian0(επιτιθέμενος).

Για την πραγματοποίηση της διαδικασίας αυτής θα χρειαστούμε την εφαρμογή arp από το πακέτο nemesis που βρίσκεται στο μηχάνημα debian0.Για να δούμε τις παραμέτρους του προγράμματος εκτελούμε:

nemesis arp help

Στα πλαίσια των απαιτήσεων της παρούσας άσκησης θα χρησιμοποιήσουμε τα πεδία -SDhmrdHM. Όσον αφορά τις παραμέτρους:

-S η IP διεύθυνση της debian0(επιτιθέμενος)
-D η IP διεύθυνση της debian/debian1(στις οποίες επιτιθόμαστε)
-h η MAC διεύθυνση της debian0(επιτιθέμενος)
-m η MAC διεύθυνση της debian/debian1(στις οποίες επιτιθόμαστε)
-r ενεργοποίηση της επανεκπομπής των πακέτων
-d το interface που χρησιμοποιούμε(eth0)
-H η MAC διεύθυνση της debian/debian1(από όπου θέλουμε να πιστεύει η debian/debian1 οτι προέρχονται τα πακέτα)
-M η MAC διεύθυνση της debian/debian1(όπου θέλουμε να πηγαίνουν τα πακέτα)

Δημιουργούμε ένα script το οποίο θα επαναλαμβάνει την διαδικασία κάθε 10 δευτερόλεπτα(nemesis.sh ο κώδικας του οποίου παρατίθεται στο αντίστοιχο αρχείο).

Αν είναι επιτυχής η αποστολή των πακέτων θα δούμε στην debian0 να εμφανίζεται κάθε 10 δευτερόλεπτα ARP Packet Injected.
Μεταβαίνουμε στην συνέχεια στην φάση man-in-the-middle-attack.Το πρωτόκολλο ssh χρησιμοποιεί την default θύρα 22.Εμείς για την επίτευξη της επίθεσης θα χρησιμοποιήσουμε το πρόγραμμα mint-ssh αλλά πρέπει να ανακατευθύνουμε κάθε σύνδεση ssh από την default θύρα 22 στην θύρα 2222 που ακούει το mint-ssh.Αρχικά εκτελούμε enable_redir από την debian0 και στην συνέχεια τρέχουμε την εντολή mint-ssh 22 -v -n -p 2222.Στην φάση αυτή η debian0 περιμένει εισερχόμενες αιτήσεις ssh μεταξύ της debian και debian1.

Εκτελούμε από την debian ssh 192.168.148.139.
Στο τερματικό 2(μηχάνημα debian0) εμφανίζεται η σύνδεση και ο κωδικός της σύνδεσης μεταξύ των 2 μηχανημάτων.Συνεπώς, η παρεμβολή ήταν επιτυχής.