ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
Τομέας Επικοινωνιών, Ηλεκτρονικής & Συστημάτων Πληροφορικής
Εργαστήριο Διαχείρισης και Βέλτιστου Σχεδιασμού Δικτύων Τηλεματικής - NETMODE

Ηρώων Πολυτεχνείου 9, Ζωγράφου, 157 80, Τηλ: 772.1448, Fax: 772.1452
e-mail: maglaris@netmode.ntua.gr, URL: http://www.netmode.ntua.gr

18 Δεκεμβρίου 2023

Διαχείριση Δικτύων – Ευφυή Δίκτυα

6η Ομάδα Ασκήσεων

Άσκηση 1

Στο αρχείο trace_b.cap έχουν καταγραφεί τα πακέτα που πέρασαν από τον κόμβο cornuto.netmode.ece.ntua.gr σε ένα χρονικό διάστημα κάποιων δευτερολέπτων. Για την καταγραφή των πακέτων χρησιμοποιήθηκε το πρόγραμμα tcpdump. Στο διάστημα αυτό έτρεξαν τέσσερις εντολές ping, και ζητήθηκαν πληροφορίες DNS από τον Name Server ulysses.noc.ntua.gr. Με τη χρήση του προγράμματος wireshark αναζητήστε στο παραπάνω αρχείο τις απαντήσεις στα παρακάτω ερωτήματα:

- Ο διαχειριστής του cornuto.netmode.ntua.gr έσβησε τον πίνακα ARP του κόμβου και στην συνέχεια πραγματοποίησε δύο ping ερωτήματα. Σε ποιους κόμβους - προορισμούς (IP address & DNS name) έγιναν τα ping ερωτήματα (τα δύο πρώτα); Τι πληροφορίες - πακέτα ανταλλάχθηκαν πριν την πραγματοποίηση των ping ερωτημάτων; Εξηγήστε
- Τι πληροφορία ζητήθηκε από τον Name Server ulysses.noc.ntua.gr; Ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε; Καταγράψτε τα identification numbers της IP επικεφαλίδας των πακέτων της απάντησης. Αποτέλεσμα ποιας εντολής είναι η ακουλουθία των πακέτων;
- Αναφορικά με το ping στον κόμβο www.uoa.gr: Τι πληροφορία ενθυλακώθηκε στην απάντηση του ερωτήματος; Εξηγήστε. Αποτέλεσμα ποιας εντολής είναι η ακολουθία των πακέτων;
- Αναφορικά με το ping στον κόμβο www.auth.gr: Γιατί παρατηρούνται πολλαπλά πακέτα ερώτησης / απάντησης; Εξηγήστε. Αποτέλεσμα ποιας εντολής είναι η ακολουθία των πακέτων;

Άσκηση 2

Πριν ξεκινήσετε την άσκηση, πρέπει να εκτελέσετε τις παρακάτω εντολές στο home directory της ομάδας σας:

```
mkdir newcerts
touch  ~/index.txt
touch  ~/index.txt.attr
echo "01" > ~/serial
```

Με τη βοήθεια του εργαλείου «openssl» ζητούνται να εκτελεστούν τα παρακάτω βήματα και να απαντηθούν οι αντίστοιχες ερωτήσεις:

a. Δημιουργία ενός πιστοποιητικού το οποίο να είναι υπογεγραμμένο από την αρχή πιστοποίησης (certificate authority) που βρίσκεται στο μηχάνημα maria.netmode.ntua.gr. Εξηγήστε τα βήματα που απαιτούνται και καταγράψτε τις αντίστοιχες εντολές.

b. Με χρήση της εντολής

```
openssl s_client -state -host netmg.netmode.ntua.gr -port 443 –tls1
```

δοκιμάστε να συνδεθείτε στον secure web server που λειτουργεί στο μηχάνημα netmg.netmode.ntua.gr (port 443). Εξηγήστε τι συμβαίνει.

c. Στη συνέχεια δοκιμάστε ξανά τη σύνδεση με χρήση της εντολής

```
openssl s_client -state –host netmg.netmode.ntua.gr -port 443    -cert <certificate file>
-key <private key file> -tls1
```

και του πιστοποιητικού που δημιουργήσατε στο πρώτο βήμα. Εξηγήστε τι συμβαίνει σε αυτήν την περίπτωση. Ποιο είναι το Common Name (CN) του web server; Ποια αρχή πιστοποίησης έχει υπογράψει το πιστοποιητικό του web server; Από ποια πιστοποιημένη αρχή πρέπει να είναι υπογεγραμμένα τα πιστοποιητικά των χρηστών ώστε να μπορούν να συνδεθούν με τον συγκεκριμένο web server;

d. Αφού γίνει η σύνδεση πληκτρολογήστε:

```
GET /netmg.php HTTP/1.0 <Enter> <Enter>
```

Τι εμφανίζεται με την εκτέλεση της παραπάνω εντολής;

Άσκηση 3

Δημιουργείστε στον κόμβο ***maria*** ένα ζεύγος κλειδιών RSA με χρήση των εντολών ssh-keygen ή openssl. Επίσης, δημιουργείστε το αρχείο ***~/.ssh/authorized_keys*** και εισάγετε σε αυτό το public key του ζεύγους.
Κατεβάστε το στον υπολογιστή σας με scp / sftp / sftp client.
Πλέον μπορείτε να συνδεθείτε στον κόμβο ***maria*** με χρήση του private key αντί για password.
Παράδειγμα από περιβάλλον UNIX:
ssh netmgXXX@maria.netmode.ntua.gr –i /<path>/<to>/<private_key>

Χρήσιμες εντολές: ssh-keygen, openssl, mkdir, touch, cat, chmod, scp, sftp, ssh