Εργαστήριο 2
Ασκήσεις: Διαχείριση Δικτύου (nmap, iptables)

1) Εκτυπώστε όλες τις πληροφορίες για τις ενεργές συνδέσεις της μηχανής σας που χρησιμοποιούν το πρωτόκολλο TCP

```
netstat | grep tcp ή netstat -t
```

2) Εκτυπώστε μόνο τα ονόματα (domain name) των μηχανών που είναι ενεργά συνδεδεμένες με τη μηχανή σας.

```
netstat | grep tcp | tr -s ' ' | cut -d' ' -f5 | cut -d":"
-f1
```

3) Εκτυπώστε μόνο τα ονόματα (domain name) των μηχανών που είναι ενεργά συνδεδεμένες με τη μηχανή σας έτσι ώστε το κάθε όνομα να εμφανίζεται μόνο μια φορά αλλά να φαίνεται και ο αριθμός των συνδέσεων της κάθε μηχανής.

```
netstat | grep tcp | tr -s ' ' | cut -d' ' -f5 | cut -d":"
-f1 | sort | uniq -c
```

4) Εκτυπώστε το όνομα της διεπαφής (interface) που έχει λάβει τα πιο πολλά πακέτα καθώς και τον αριθμό των εισερχόμενων πακέτων.

```
netstat -i | grep -v 'Iface' | grep -v 'Kernel' | tr -s ' ' |
sort -nrk 3 | head -1 | cut -d' ' -f1,3
```

5) Έστω ότι σας ενδιαφέρουν οι ανοικτές θύρες των υπηρεσιών της μηχανής σας. Να γράψετε σε αρχείο με το όνομα open_ports ΜΟΝΟ τους αριθμούς των θυρών, τη μία δίπλα στην άλλη χωρισμένες με κενό (space) π.χ. `22 11 631 3389 5910 5911`

```
nmap localhost | grep open | cut -d' ' -f1 | cut -d'/' -f1 |
tr '\n' ' ' > open_ports
```

Σημείωση: δε χρειάζεται `tr -s ' '` πριν το πρώτο `cut` διότι θέλουμε την πρώτη στήλη. Αν το βάλετε δε αλλάζει κάτι στο αποτέλεσμα και δεν θεωρείται λάθος.

6) Εκτυπώστε τις ανοικτές θύρες των υπηρεσιών της μηχανής σας. Θα πρέπει να τυπώσετε ΜΟΝΟ τα ονόματα των υπηρεσιών το ένα κάτω από το άλλο π.χ.

```
ssh
rpcbind
ipp
ms-wbt-server
cm
cpdlc
```

```
nmap localhost | grep open | tr -s ' ' | cut -d' ' -f3
```

7) α) Τυπώστε τα ονόματα (domain names) των 10 μηχανών που έκαναν τις πιο πολλές αιτήσεις GET στον HTTP server (μπορείτε να τυπώσετε και τον αριθμό των αιτήσεων).

```
cat epa-http.txt | grep GET | cut -d' ' -f1 | sort | uniq -c
| sort -nrk 1 | head
```

β) Τυπώστε τα ονόματα (domain names) των 10 μηχανών που έκαναν τις πιο πολλές αιτήσεις POST στον HTTP server (μπορείτε να τυπώσετε και τον αριθμό των αιτήσεων).

```
cat epa-http.txt | grep POST | cut -d' ' -f1 | sort | uniq -c
| sort -nrk 1 | head
```

8) Δώστε την εντολή που προσθέτει ένα κανόνα στην αλυσίδα INPUT για την απόρριψη πακέτων του πρωτοκόλλου TCP που κατευθύνονται στη θύρα 631:

```
iptables -A INPUT -p tcp --destination-port 631 -j DROP
```

Επιβεβαιώστε με την εντολή nmap ότι όντως η θύρα 631 δεν είναι πλέον ανοικτή:

```
nmap localhost
```