Εργαστήριο 2

Ασκήσεις: Αλληλεπίδραση με Δεδομένα HTTP (Web) Server και 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) Εκτυπώστε τα μόνο τα ονόματα των log files του HTTP server που δημιουργήθηκαν μέσα στο μήνα Ιανουάριο.

```
ls /var/log/apache2/ -l | grep Jan | tr -s ' ' | cut -d' ' -
f9
```

6) Επειδή τα log files στη μηχανή σας δεν έχουν πολλές πληροφορίες προς επεξεργασία, θα κατεβάσουμε δεδομένα από μια ιστοσελίδα που περιέχει traces από access logs. Πιο συγκεκριμένα θα κατεβάσουμε ένα access log file από ένα FTP server που βρίσκεται στο Research Triangle Park, NC στην Αμερική και περιέχει πληροφορίες αιτήσεων προς τον server για ένα 24 ωρο. Διαβάστε περισσότερα στοιχεία για το συγκεκριμένο access log file εδώ. Κατεβάστε το στη μηχανή σας και αποσυμπιέστε:

```
wget ftp://ita.ee.lbl.gov/traces/epa-http.txt.Z

uncompress epa-http.txt.Z
```

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
```

7) 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
```