VII. mérés Naplózás

A mérés célja a Linux naplókezelésének megismerése, valamint a naplóelemzés elsajátítása.

1. Telepítse fel a syslog-ng csomagot a Fekete és DELL gépekre és oldja meg, hogy a DELL gépen található Debian rendszer a fekete gépre naplózzon.

Szerver telepítése (fekete gépen):

```
apt-get install syslog-ng
```

- A syslog-ng konfigurációs fájljában törölje a kettőskereszt (comment) jelet a s_net forrás deklarálásnál, majd cserélje ki az IP-t a fekete gép IP-jére

```
source s_net { tcp(ip(feketegépIPje) port(1000)); };
```

- Adja hozzá a dell nevű destination-t a „Destinations” szekcióban:

```
destination dell { file("/var/log/dell.log"); };
```

- Majd definiálja a naplózást a fenti paraméterekkel a „Log Path” szekcióban

```
log { source(s_net); destination(dell); };
```

- Majd indítsa újra a syslog-ng daemont!

```
systemctl restart syslog-ng
```

Telepítse a **klienst a DELL gépre,** majd az syslog-ng konfigurációs állományban végezze el a következő módosításokat:

```
apt-get install syslog-ng
```

- Definiálja a fekete gépet mint naplózási célt a „Destination” szekcióban:

```
destination d_net { tcp("feketegépIPje" port(1000) log_fifo_size(1000)); };
```

- Majd definiálja a naplózást a fenti paraméterekkel a „Log Path” szekcióban

```
log { source(s_src); destination(d_net); };
```

- Majd indítsa újra a syslog-ng daemont!

```
systemctl restart syslog-ng
```

- Ahhoz, hogy biztos legyen új log bejegyzés a Dell gépről kérjen új IP címet a következő paranccsal:

```
dhclient –v enp11s0
```

- Lépjen vissza a Fekete gépre, majd ellenőrizze, létrejött-e a dell.log és listázza ki a tartalmát:

```
cat /var/log/dell.log
```

- Ha mindent jól csinált az új IP cím kérése bekerült az újonnan létrejött log fájlba.

2. Töltse le a dev2.tilb.sze.hu/probalog.log fájlt, mely a labor publikus IP cím tartomány forgalmának egynapos naplója. Az eddig tanult eszközök (sed, awk, grep stb.) elemezze a logfájlokat és adjon választ a következő kérdésekre:

   - Nézze meg, milyen gyakran kapcsolódik a 92.52.216.17-es IP cím a laborhálózatba, és milyen célból?
   - Nézze meg, hány alkalommal kapcsolódik a laborhoz egy távoli gép HTTPS kapcsolaton.
   - Egy nap alatt kimenő vagy bejövő kapcsolatokból van több?
   - Állapítsa meg, a logfájl alapján melyik hálózati interfész kapcsolódik az internethez!
   - Állapítsa meg, hányan próbáltak meg belépni ssh segítségével 1 nap alatt a 193.224.130.177-es IP címre (tegyük fel, hogy senki nem használta aznap az ssh kapcsolatot)!
   - Állapítsa meg, hány csomag érkezett a 193.224.130.173-as IP cím http portjára!