VII. mérés Naplózás

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

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

   - Szerver telepítése:

apt-get install rsyslog

A /etc/rsyslog.conf állományban a következő sorok elől a # kitörlése:

module(load="imudp")

input(type="imudp" port="514")

module(load="imtcp")

input(type="imtcp" port="514")

Majd a syslog daemon újraindítása:

systemctl status rsyslog.service

   - Telepítse a klienset, majd az rsyslog konfigurációs állományhoz adja hozzá a következő sort:

*. * @Fekete_gép_IP_címe:514

Végül indítsa újra az rsyslog daemont!

   - Ellenőrizze a működést!

2. Töltse le a dev2.tilb.sze.hu/probalog.log fájlt, mely a labor publikus IPcím tartomány forgalmának egynapos naplója.

   - 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-re (tegyük fel, hogy senki nem használta aznap az ssh kapcsolatot)!
- Állapítsa meg, hány csomag érkezett a 193.224.130.173-as IP http portjára!