Hálózati operációs rendszerek
NGB_TA047_1
6. kisZH

2015. 10. 19.

FIGYELEM! Nem működő Linux parancsot vagy `iptables` szabályt nem fogadunk el! Ügyeljenek a kis- és nagybetűk használatára is! Ahol másként nem jeleztük, minden feladat helyes megoldása 1 pontot ér. Értékelés: 6 ponttól elégséges, 7-től közepes, 8-tól jó, 9-től jeles.

1. Írjon olyan **`iptables`** szabályt, amely a géphez érkező **`ssh`** kapcsolódási kéréseket "**`ssh: `** " prefix-szel naplózza.

2. Milyen biztonsági megfontolás szól az **`inetd`** használata ellen?

3. Kérdezze le egy megfelelő parancssor segítségével, hogy számítógépén milyen számítógépekkel áll fenn TCP kapcsolat.

4. Kérdezze le egy megfelelő parancssor segítségével, hogy számítógépének 3128-as TCP portján milyen program szolgáltat.

5. Mit ír a **`sysklogd`** konfigurációs állományába ahhoz, hogy a legalább **`err`** szintű események a rendszergazda terminálra kiíródjanak (ha be van jelentkezve)?

6. A **`sysklogd`** használata esetén Debian alatt melyik fájlban és milyen opcióval tudja beállítani, hogy az összes (pontosan) **`warning`** szintű üzenet a **`/var/log/warnings`** fájlba naplózódjon?

7. Mit eredményez a **`sysklogd`** konfigurációs állományában a következő bejegyzés?
   `*.=info;syslog.none  /var/log/info.log`

8. Debian Linux alatt hol és milyen néven található a **`syslog-ng`** konfigurációs fájlja?

9. Adja meg az alábbi **`sysklogd`** konfigurációs bejegyzéseknek megfelelő **`syslog-ng`** beállításokat! Használja az **`s_all`** forrásdefiníciót, és adjon meg minden mást! (**2x1 pont**)
   `lpr.crit  printadm`

   `auth.=err  /var/log/auth-errors.log`