Hálózati operációs rendszerek
NGB_TA047_1
6. kisZH
A csoport
2012. 10. 18.

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 DNS feloldási kéréseket naplózza "**`BIND:`** " prefix-szel!

2. Miért előnyös, ha egy telephely összes gépe egyetlen naplószerverre naplóz? Legalább két dolgot említsen!

3. Mit ír a **`sysklogd`** konfigurációs állományába ahhoz, hogy a legalább **`alert`** szintű események a **`tty0`** terminálra kiíródjanak?

4. A **`sysklogd`** használata esetén Debian alatt melyik fájlban és milyen opcióval szokták beállítani, hogy távoli gépről naplózást fogadjon?

5. Távoli naplózásnál milyen biztonsági előnye van a **`syslog-ng`** használatának?

6. Mit eredményez a **`sysklogd`** konfigurációs állományában a következő bejegyzés?
   `*.debug;lpr,mail,news.none  -/var/log/debug.log`

7. Mit ír a **`sysklogd`** konfigurációs állományába ahhoz, hogy a levelezéssel kapcsolatos összes naplóeseményről értesítést kapjon a **`postmaster`** nevű felhasználó (ha be van jelentkezve)?

8. Adja meg az alábbi **`sysklogd`** konfigurációs bejegyzéseknek megfelelő **`syslog-ng`** beállításokat! Használja az **`s_all`** forrásdefiníciót, és adjon meg minden mást! (**2x1 pont**)
   `mail.err  @logserver`

   `lpr.*  printadm`

9. Ismétlő feladat: írjon reguláris kifejezést, amely a 64:ff9b::/96 NAT64 well-known prefixet használó IPv4-embedded IPv6 címekre illeszkedik!