

T: Zapobieganie włamaniom.

Czynności ograniczające możliwość włamań do systemu:

- konfiguracja i analiza oprogramowania firewall,
- instalacja oprogramowania antywirusowego i antyspyware,
- aktualizacja systemu i oprogramowania,
- stosowanie bezpiecznej polityki haseł,
- kontrola stanu kont i uprawnień użytkowników w systemie,
- konfiguracja zabezpieczeń systemu plików,
- wyłączenie zbędnych usług w systemie,
- uszczelnianie usług sieciowych,
- ograniczenie praw usług,
- filtrowanie pakietów sieciowych,
- uszczelnianie fizycznej infrastruktury sieci,
- konfiguracja kart sieciowych,
- zabezpieczenie sieci bezprzewodowych.

Zadanie1:

Odszukaj informacje na temat programów snort i nessus.

http://pl.docs.pld-linux.org/uslugi_snort.html

<http://www.nessus.org/download/>

Zadanie2:

Do jakiego celu możemy wykorzystać poniższe polecenie?

```
netstat -nltup
```

Zadanie3:

W ramach powtórki przetestuj następujące polecenia:

```
top  
ps aux  
skill  
chkconfig
```

Ciekawostka

W celu zabicia aktywnego procesu skorzystaj z następującego polecenia:

```
fuser -k port/tcp
```

Na przykład w celu zabicia wszystkich połączeń z portem 22 (sshd) wydaj polecenie

```
fuser -k 22/tcp
```