Diagnostyka protokołów TCP i UDP

netstat -t <- wypisuje aktywne połączenia tcp (przychodzące i wychodzące)
podając nazwy komputerów i portów w kolumnach „Local Address” i „Foreign Address”
netstat -tn <- wypisuje aktywne połączenia tcp (przychodzące i wychodzące)
podając adresy komputerów i numery portów w powyższych kolumnach

Powyższe polecenia nie wypisują nasłuchujących serwerów tcp

netstat -lt <- wypisuje nasłuchujące serwery tcp (nazwy)
netstat -ltn <- wypisuje nasłuchujące serwery tcp (adresy i numery)
netstat -lu <- wypisuje nasłuchujące serwery udp (nazwy)
netstat -lun <- wypisuje nasłuchujące serwery udp (adresy i numery)

Ćwiczenie 1
Otworzyć kilka połączeń ssh do komputera B (z innego lub innych niż B komputerów)
Na komputerze B wydać polecenia "netstat -tn" i "netstat -ltn"
Pierwsze z tych poleceń w kolumnach "local address" i "foreign address" wypisuje adresy i porty obu stron poszczególnych połączeń tcp wychodzących z B lub przychodzących do B
Drugie z nich wypisuje serwery tcp nasłuchujące na B.

Na komputerze B wydać polecenie "systemctl stop sshd" zatrzymujące serwera ssh
Zauważyć, że otwarte wcześniej połączenia do serwera ssh działającego na B są nadal aktywne, ale nie można otwierać nowych połączeń do B
Na komputerze B wydać polecenie "systemctl start sshd" uruchamiające ponownie serwera ssh

Ćwiczenie 2

Napisać skrypt monitorujący liczbę połączeń tcp nawiązanych do serwera określonej usługi działającego na lokalnej maszynie. Skrypt ma wypisywać liczbę połączeń przy jego uruchomieniu i przy każdej zmianie tej liczby. Oprócz tego skrypt ma ostrzegać o osiągnięciu lub przekroczeniu przez liczbę połączeń określonej wartości progowej, oraz informować o spadku liczby połączeń poniżej tej wartości. Numer portu serwera i wartość progowa mają być podawane jako argumenty przy uruchamianiu skryptu.

Polecenie zatrzymania serwera nasłuchującego na porcie o danym numerze (np. 22), jeśli serwer był uruchomiony przez mechanizm systemd:

```
systemctl stop `netstat -tln -p|awk '$1~"tcp$"'|awk '$4 ~ ":22$" {print $7}'|cut -f2 -d/`
```

Uwaga 1: instrukcja języka awk składa się z warunku i czynności wykonywanej na wierszach tekstu spełniających dany warunek, w powyższym przykładzie awk '$1~"tcp$"' wypisuje wiersze, których pierwsza kolumna kończy się znakami tcp, natomiast czynność nie jest określona, więc zostaną wypisane całe wiersze

Uwaga 2: polecenie awk '$4 ~ ":22$" {print $7}' wypisuje siódmą kolumnę tych wierszy tekstu, które spełniają warunek $4 ~ ":22$" oznaczający, że czwarta kolumna wiersza kończy się znakami :22

Uwaga 3: w części warunkowej instrukcji języka awk, szukany wzorzec musi być ujęty w cudzysłów

Uwaga 4: gdyby serwer ssh nie został zatrzymany przez mechanizm systemd, ale np. "zabity" poleceniem kill w następujący sposób:

```
kill -9 `netstat -tln --program|awk '$1~"tcp$"'|awk '$4 ~ ":22$" {print $7}'|cut -f1 -d/`
```

to po pewnym czasie mechanizm systemd uruchomi go ponownie, jeśli w pliku konfigurującym serwer ssh w mechanizmie systemd, czyli w pliku

/etc/systemd/system/multi-user.target.wants/sshd.service

jest dyrektywa Restart=on-failure

Uwaga 5: po zmianie w pliku konfiguracyjnym jakiegoś serwera uruchamianego przez mechanizm systemd, należy wydać polecenie

systemctl daemon-reload

Konfiguracja samego serwera ssh jest zapisana w pliku /etc/ssh/sshd_config
Jedną z dyrektyw konfiguracyjnych jest PermitRootLogin yes,
która określa czy root może się logować do serwera ssh.
Po ewentualnych zmianach w powyższym pliku, aktywujemy je poleceniem
systemctl reload sshd

Polecenie nmap skanujące komputery i porty

nmap -sP 213.135.45.0/28 <- skanowanie komputerów o adresach z podanego zakresu
(wielokrotny ping)

nmap -sS sz123.wsisiz.edu.pl <- skanowanie portów TCP na wskazanym komputerze (tylko root)

nmap -sT sz123.wsisiz.edu.pl <- skanowanie portów TCP na wskazanym komputerze (dowolny użytk.)

nmap -sT -p 20-30 sz123.wsisiz.edu.pl <- skanowanie portów TCP z podanego zakresu na wskazanym komp.

nmap -sU sz123.wsisiz.edu.pl <- skanowanie portów UDP na wskazanym komputerze (tylko root)

nmap -sU -p 20-30 sz123.wsisiz.edu.pl <- skanowanie portów UDP z podanego zakresu na wskazanym komp. (tylko root)

skanowanie portów oznacza wykrywanie otwartych portów

Ćwiczenie 3
Na komputerze B sprawdzić czy działa na nim mechanizm iptables (systemctl status iptables). Jeśli tak, to zatrzymać iptables na B (systemctl stop iptables). Aktywować usługę echo na B (edycja plików echo-stream i echo-dgram w katalogu /etc/xinetd.d i polecenie "systemctl reload xinetd").
Na komputerze A wydać polecenia

netstat -sS -p 1-200 <adres lub nazwa B>

netstat -sU -p 1-10 <adres lub nazwa B>

Następnie wznowić działanie iptables na B (systemctl start iptables) i ponownie wydać powyższe polecenia na komputerze A. Zaobserwować różnice. Uwaga: skanowanie portów UDP trwa dłużej niż portów TCP, dlatego podany zakres portów UDP jest mniejszy niż zakres portów TCP.