PRÁCE NA SÍTI

DIAGNOSTIKA I

- **ifconfig – nastavení síťového rozhraní**
  - > ifconfig wlps1s0 ---> výpis informací o zařízení

```
wlp1s0: flags=4163<AKTIVOVÁNO,VŠESMĚR,BĚŽÍ,MULTICAST>  mtu 1500
        inet 192.168.80.91 síťová_maska 255.255.248.0  všesměr 192.168.87.255
        inet6 2001:718:1602:80:6257:18ff:fe5e:ef70  délka_prefixu 64  scopeid 0x0<globální>
        inet6 fe80::6257:18ff:fe5e:ef70  délka_prefixu 64  scopeid 0x20<linka>
        ether 60:57:18:5e:ef:70 délka_odchozí_fronty 1000  (Ethernet)
        RX packetů 159492  bajtů 79954395 (76,2 MiB)
        RX chyb 0  zahozeno 0  přetečení 0  rámců 0
        TX packetů 43841  bajtů 7600664 (7,2 MiB)
        TX chyb 0  zahozeno 0  přetečení 0  přenos 0  kolizí 0
```

  - > sudo ifconfig eth0 up/down ---> zapnutí/vypnutí zařízení eth0
  - > ifconfig eth0 13.13.13.13 ---> nastavení statické adresy
  - > sudo ifconfig eth0 192.168.2.5 netmask 255.255.255.0 broadcast 192.168.2.7 ---> nastavení masky a broadcastu
- **dhclient – dynamické přidělení IP adresy od serveru**

DIAGNOSTIKA II

- **Program ip, podobné ifconfig**
  - > ip addr list ---> výpis stavu zařízení
  - ip [link|adress|route ..] [addr,delete,show(list), set ..] zařízení
  - > ip link set eth0 down ---> shození rozhraní
  - > ip route show ---> výpis routování
- **Wireless tools**
  - ifrename -přejmenování rozhraní (nespuštěné)
  - iwconfig – rozšíření ifconfig pro wireles
    - > iwconfig wlp1s0
  - Iwlist – skenování dostupných wlan sítí
    - > iwlist wlp1s0 scan
  - Iwgetid – informace o používaném přístupovém bodě
    - > iwgetid
  -

DIAGNOSTIKA III

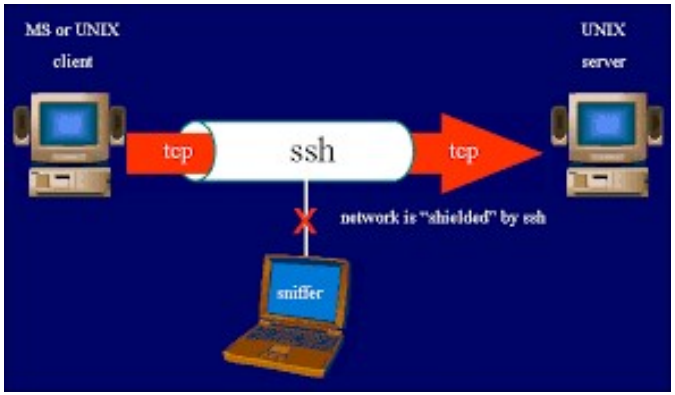
- **ping – test spojení, standardně po 1 sec (lze zkrátit -i)**
  - > ping -c 5 seznam.cz ---> pošle 5 paketů
  - >sudo ping -f localhost (nebo jiná IP :-)) ---> flood (DDOS útok)
- **netstat – stav připojení**
  - > netstat -a | less ---> všechna síťová připojení
  - > netstat -s ---> statistické informace
  - > sudo netstat -nlp --->procesy a spojení
- **Trasování**
  - traceroute -posílá UDP packety s různým TTL (Time To Live)
    - Někdy to neprojde firewally a cesta pak není nalezena
    - >traceroute seznam.cz
  - tcptraceroute (sudo) – posílá TCP packety
    - >sudo tcptraceroute seznam.cz

Šedá zóna

- **tcpdump – odchytávání paketů na síti (sniffer)**
  - > sudo tcpdump -i wlp1s0 --- základní použití
  - >sudo tcpdump -n -i wlp1s0 net 192.168.80.0/24
    - Zachytí všechny packety kde cíl, nebo zdroj je 192.168.80.0/24
- **nmap - scannování portů**
  - > sudo nmap -sS -O ADRESA
    - Použije Stealth scanning (-sS)
    - TCP connect scann (-sT) – je snáze odhalitelný, logování->ban
    - Analyzuje a pokusí se vypsat OS (-O)

SSH

- **Secure Shell (SSH)-protokol i program**
  - Umožňuje šifrovanou obousměrnou komunikaci
  - Standardně běží na portu 22
  - > ssh uživatel@stroj
  - > ssh uživatel@stroj:port
  - > ssh uživatel@stroj 'echo $USER'
    - Provedení jednoho příkazu na straně serveru
  - > ssh -X uživatel@stroj
    - Forwardování X11 – běží na serveru, ale zobrazuje se u mne
  - > ssh uživatel@stroj1 -L 2346:stroj2:3389
    - Pomocí stroj1 (brána do privátní sítě) je mapován port 3389 (RDP) na stroji2(privátní síť) na lokální zařízení na port 2346



- **putty – windowsí ssh klient**

Přenos dat po síti SCP/SFTP protokol

- **scp – bezpečný přenos souborů (scp)**
  - >scp co kam
    - co user1@stroj1:\cesta1
    - kam user2@stroj2:\cesta2
- **sftp – modernější než scp**
    - Příkazy put, get, mget
- **mc – (midnight commander)– SFTP**
- **winscp-ve světě windows**
- **okenní správci souborů**
    - nautilus