**2PC, 1 Client a 1 Server**

**Výpis IP**

*Ip a*

**Zmena IPs :**

Input :

*Vim /etc/hosts*

127.0.0.1 localhost localhost.domain localhost4 localhost4.localdomain

10.0.0.206 server

10.0.0.185 client

**Pingovanie clienta :**

*Ping client*

**Dajaky command na serveri :**

*Ip address add [192.168.60.10/24] broadcast + dev enp0s3*

(zatial nebude fungovať, nevie cestu)

**Nastavenie cesty**

*Ip route add [192.168.60.0/24] via [10.0.0.206] dev enp0s3*

**Odstránenie statickej cesty**

*Ip route del [192.168.60.0/24] via [10.0.0.206] dev enp0s3*

***Routy sa dajú nastaviť aj cez vim/nano***

*Nano enp0s3.nmconnection*

V časti [ipv4] treba napísať dajak

**Netstat a NMap**

**Nestat = Sledujem si svoje služby**

**Netmap = Port Scanner, väčšinou sledujeme vzdialený počítač**

**Netstat**

**Výpis veľa bordelu :**

*Netstat -a*

**Výpis všetkého o TCP protokole :**

*Netstat -at*

Ďalšie prepínače :

Netstat -atn

Netstat -atnp = aký program na tom porte počúva (PID+ProgramName)

Netstat -4 -ltnp = dačo to isté ako predtým ale zároveň nie či čo... L ako Listening

Netstat -4 -aunp = všetko o UDP

Netstat -4 -lunp = Vypíše

Netstat -naplut = výpis všetkých TCP a UDP portov

N = Chcem čísla

P = Chcem vidieť PID

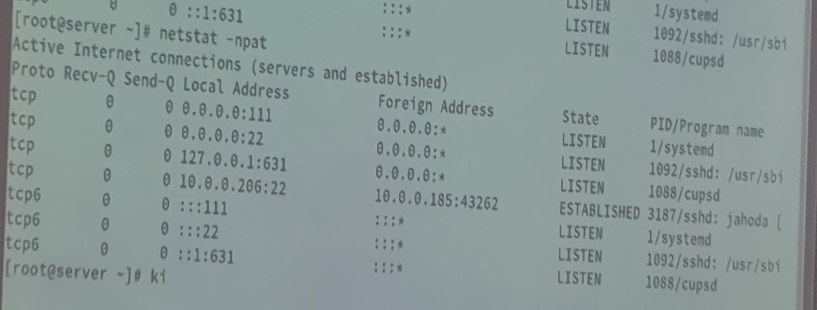
T = TCP protokol

U = UDP protokol

A = All

L = Listen

**Da do testu kto sa pripojil z akej IP adresy a aký to bol port**



**Pripojil sa jahoda, z IP 10.0.0.185, nahodny port bol 43262**

**Zrušíme ho :** kill 3187

**Systemctl**

*Systemctl is-active httpd* (či je zapnutý webserver)

*Systemctls is-enabled httpd* (či sa služba zapína pri štarte)

*Systemctl enable httpd* (zapnutie aby sa služba zapínala pri štarte)

*Stystemctl start httpd* (zapnutie webservera)

*Netstat -nltp* -> je tu nová vec na httpd (asi web server)

**Služba ešte nebude fungovať lebo mame zapnuty firewall**

**Shodan.io – stránka na advanced NMap (ak poznáme verejnú IP)**

**Nainštalujeme nmap :**

*Yum install nmap*

**Aké otvorené UDP Porty má pc server :**

*Nmap -sU server*

***Nenapíše nám to skoro nič, ale ak by sme dali napr.***

*Nmap -sU -p 1194 server*

***(scan portu na OpenVPN)***

***Tak output bude :***

*PORT STATE SERVICE*

*1193 /udp open openvpn*

**Aké otvorené TCP Porty má pc server :**

*Nmap -sT server*

***Output :***

*PORT STATE SERVICE*

*22/tcp open ssh*

*9090/tcp closed zeus-admin*

**Iný test – StealTest :**

*Nmap -sS server*

**Oskenujeme port :**

*Nmap -sS -p 22 server*

**Vypnutie Firewallu :**

*Systemctls stop firewalld*

**Pripojenie na ASI? telnet :**

*telnet server 80*

*(očakáva nejaký vstup)*

**Pripojenie na SSH :**

*telnet server 22*

*(dá banner, čaká na vstup)*

**Ktorý prokotol sa použije na to, aby sme zistili aké PC sú v našej sieti a aby nám odpovedali či čo?**

* Arp

**Ifconfig a Route**

* Už by sa nemali používať