14. Biztonságos kapcsolat SSH-val (Johanyák Zsolt Csaba)

A gyakorlat célja az, hogy begyakoroljuk azt, hogy hogyan tudunk egy szerverre SSH segítségével bejelentkezni a szerver helyével azonos alhálózatból valamint egy másik alhálózatból.

14.1. Előkészítés

A feladat megoldásához három alhálózatot hozunk létre LAN1, LAN2 és LAN3 néven. Hozzunk létre egy M0n0wall router M1 néven. Ezen a gépen keresztül kapcsolódik a LAN1 alhálózat a külvilághoz, azaz a router WAN interfésze a VMware-en keresztül eléri a külső hálózatot (NAT), míg LAN interfésze a LAN1-re kapcsolódik 192.168.1.254/24 rögzített IPv4 címmel. M1 nem kell DHCP szolgáltatást nyújtson.

A LAN2 és LAN3 hálózatokat egy-egy M0n0wall router választja el a külvilágtól. A LAN2 hálózat esetén a router neve legyen M2, és belső (LAN) interfészének IPv4 címe legyen 192.168.2.254/24. A router DHCP kiszolgálóként is működjön úgy, hogy a kiosztott címtartomány legyen 192.168.2.1..240. Ebben a hálózatban egy Ubuntu Server virtuális gépet (S2) fogunk használni a 192.168.2.253 rögzített IPv4 címmel. Emellett egy Ubuntu Desktop virtuális gépünk (D2) is lesz, amit túgy állítsunk be, hogy DHCP protokollal fogadja a konfigurációt, amit az M2 gép fog neki szolgáltatni. Az M2 router WAN interfésze a LAN1 hálózatra csatlakozzon (LAN segment) és a 192.168.1.252/24 rögzített IPv4 címmel rendelkezzen. Ezt csak webes felületen tudjuk beállítani a D2 gépről.

D2-n a következő előkészítő lépéseket kell megtenni:
- A web böngészőben kapcsoljuk ki a proxy-t.
- http://192.168.2.254, User Name: admin, Password: mono
- System/General setup: Hostname: M2; DNS servers: 192.168.1.254, 10.1.51.23; Save
- Interfaces/WAN: Type: Static; IP address: 192.168.1.252/24; Gateway: 192.168.1.254; a Block provate networks legyen kikapcsolva; Save
- Engedélyezzük, hogy az M2 gép válaszoljon a Ping csomagokra: Firewall/Rules/WAN fül: + Protocol: ICMP; Save, Apply changes

D2-n a következő előkészítő lépéseket kell megtenni:
- IPv4 konfiguráció beállítása az /etc/network/interfaces állományban
- Gép újraindítása (erre azért van szükség, mert néha megmarad az /etc/resolv.conf-ban az eredetileg DHCP-vel kiosztott névkiszolgáló – 192.168.2.254 elsődlegesként.

Ellenőrzés:
- M1-ről próbáljuk meg ping-gel elérni a külső hálózat névszerverét (10.1.51.23)
- M1-ről próbáljuk meg ping-gel elérni M2-t
- M2-ről próbáljuk meg ping-gel elérni M1-t
- M2-ről próbáljuk meg ping-gel elérni a külső hálózat névszerverét (10.1.51.23)
- M2-ről próbáljuk meg ping-gel elérni S2-t

- D2-ről próbáljuk meg ping-gel elérni a külső hálózat névszerverét (10.1.51.23)
- S2-n ifconfig és cat /etc/resolv.conf
- S2-ről próbáljuk meg ping-gel elérni a külső hálózat névszerverét (10.1.51.23)
- S2-n próbáljuk ki a névfeloldást (nslookup ubuntu.com)
- D2-ről próbáljuk meg ping-gel elérni S2-t

A LAN3 hálózat esetén a router neve legyen M3, és belső (LAN) interfészének IPv4 címe legyen 192.168.3.254/24. A router DHCP kiszolgálóként is működjön úgy, hogy a kiosztott címtartomány legyen 192.168.3.1..240. Ebben a hálózatban egy Ubuntu Desktop virtuális gépünk lesz (D3), amit úgy állítsunk be, hogy DHCP protokollal fogadja a konfigurációt, amit az M3 gép fog neki szolgáltatni. Az M3 router WAN interfésze a LAN1 hálózatra csatlakozzon (LAN segment). Ezt csak webes felületen tudjuk beállítani a D2 gépről.

A D3 gépet most még ne hozzuk létre, akésőbbiekben a D2 másolataként fogjuk azt létrehozni.

14.2. Az SSH szolgáltatás telepítése és konfigurálása a szerveren

Frissítsük a csomag adatbázist az S2 gépen.

```
$ sudo apt-get update
```

Telepítsük az OpenSSH szerver csomagot.

```
$ sudo apt-get install openssh-server -y
```

A telepítést követően a szerver automatikusan elindul. Állítsuk le.

```
$ sudo service ssh stop
```

Az autentikációt RSA kulcs alapúra szeretnénk beállítani (a felhasználó nem kell a későbbiekben megadjon külön jelszót amikor távolról bejelentkezik). Továbbá csak az `ssh_users` csoport tagjai használhatják a szolgáltatást. Ehhez megnyitjuk szerkesztésre a `/etc/ssh/sshd_config` állományt.

```
$ sudo nano /etc/ssh/sshd_config
```

```
PubkeyAuthentication yes      # ez alapból be van állítva
RSAAuthentication yes         # ez alapból be van állítva
AllowGroups ssh_users
PasswordAuthentication yes    # ezt ki kell venni megjegyzésből
```

Bár a későbbiekben a jelszó használat elhagyását tervezzük, de most még engedélyezzük a jelszó alapú autentikásást egészen addig amíg a kliensről fel nem másoltuk a felhasználó nyílvános kulcsát a szerverre.

Mentsük el az `sshd_config` állományt, majd hozzuk létre az `ssh_users` csoportot és vegyük fel a hallgató felhasználót.

```
$ sudo addgroup ssh_users
$ sudo usermod –a –G ssh_users hallgato
```

Amennyiben a szerveren aktív a tűzfal, akkor az alábbi utasítással engedélyezhetjük a az SSH bejövő kapcsolatot. Megj.: a tűzfal az alap telpítésnél még nem aktív.

```
$ sudo ufw allow OpenSSH
```

Indítsuk el az szerver szolgáltatást

```
$ sudo service ssh start
```

Ellenőrizzük le, hogy fut-e és fogad-e kapcsolatot

```
$ ps –A | grep sshd
$ sudo netstat --inet –lpn
```

14.3. Az SSH kliens

Az SSH kiszolgálót a D3 gépről szeretnénk elérni. Bár az ügyfélszoftver alapból telepítve van, de ha esetleg utólag vagy újra kellene telapítenünk, akkor az alábbi utasítással tehetjük.

```
$ sudo apt-get install openssh-client
```

Hozzunk létre egy kulcspárt RSA titkosítással (Enter,Enter,Enter), majd töltsük be a memóriába a titkos kulcsot. A kulcsot külön jelszóval is védhetnénk, de ettől most eltekintünk. A kulcspár a `/home/hallgató/.ssh` könyvtárban jön létre.

```
$ ssh-keygen –t rsa
$ ssh-add –l
```

Másoljuk a felhasználói nyilvános kulcsot a szerverre. Ehhez a lépéshez hagytuk meg a szerveren a `PasswordAuthentication yes` beállítást az előző alfejezetben

```
$ ssh-copy-id  hallgato@192.168.2.253
```

Amennyiben sierkes volt a másolási művelet `Number of key(s) added: 1` üzenetet kapunk. Jelentkezzünk be a szerverre, majd ott az `/etc/ssh/sshd_config` állományban állítsuk át `PasswordAuthentication no`-ra a hitelesítést. Ezt követően indítsuk újra a szolgáltatást.

```
$ ssh hallgato@192.168.2.253
```

14.4. Bejelentkezés másik hálózatból

A gyakorlat utolsó részében a másik hálózatból történő bejelentkezést szeretnénk megvalósítani. Ehhez létrehozzuk a D3 virtuális gépet. Mivel a D3 gépről történő bejelentkezéshez szükségünk lesz a kulcspárosunkra, aminek az egyik virtuális gépről (D2) a másikra (D3) történő máűsolása körülményes lenne, ezért D3-at úgy hozzuk létre, hogy D2-ről egy másolatot készítünk. Így az új virtuális gép alapból tartalmazni fogja a szükséges kulcsokat. A msáolatkészítéshez először állítsuk le a D2 gépet.

A másolat elkészítését követően a D3 gépről hajtsuk végre ugyanazokat a webes konfigurálási és ellenőrzési lépéseket M3 vonatkozásában, mint amiket a D2-ről végrehajtottunk az M2 vonatkozásában. Továbbá a D2 gépet indítsuk újra.

Ahhoz, hogy a D3 gépről az S2 szerver elérhető legyen SSH kapcsolattal az M2 gépen egy NAT szabályt kell létrehoznunk, ami gondoskodik a 22-es porton bejövő SSH kérés továbbításáról a 192.168.2.253-as gép felé. Ennek érdekében a D2 gépen jelentkezzünk be ismét az M2 webes konfiguráló felületére, majd Firewall/NAT, Inbound fül, + (hozzáadás), External port range from: SSH, to: SSH; NAT IP: 192.168.2.253; Auto-add a firewall rule to permit traffic through this NAT rule (pipa bekapcsolva); Save; Apply changes

Próbaként a D3 gépről jelentkezzünk be.

```
$ ssh hallgato@192.168.1.252
```

Itt az M2 címét adtuk meg. Az automatikusan továbbítani fogja a 192.168.2.253-ra a kérést.