



Nastavni predmet	KONFIGURIRANJE RAČUNALNIH MREŽA I SERVISA
Naslov jedinice	Vježba 13: SSH na Linux Mintu

CILJ VJEŽBE

Učenik će znati instalirati i konfigurirati SSH servis na Linux Mint distribuciji, testirati i analizirati SSH promet uz pomoć alata PuTTY i Wireshark te na kraju izvršiti vježbu LV12 pomoću PuTTY-ja.

IZVOĐENJE VJEŽBE

Sve postupke i dobivene rezultate po točkama zadataka zapisivati u bilježnicu.

Odgovoriti u bilježnicu na postavljena pitanja vezana uz ovu vježbu.

1. Inicijalne postavke

- 1) Pokrenuti VMware Workstation Pro
- 2) Postaviti snapshot u VMware-u za poslužitelj (Linux Mint) na **cleanInstall** kako bi započeli čistu konfiguraciju SNMP servisa
- 3) Pokrenuti Poslužitelj (Linux Mint)

User : **osboxes.org**

Password : **osboxes.org**

- 4) Na Poslužitelju (Linux Mint) u Network adapter postavkama odaberite **NAT** kako bi mogli pristupiti internetu kod instalacije Linux Mint paketa nadogradnje.
- 5) Na Poslužitelju (Linux Mint) postavite tipkovnicu na **Croatia (Layout)** zbog prilagodbe tipkovnice hrvatskoj verziji (ostale tipkovnice možete obrisati).
- 6) U Terminalu upisati sljedeće naredbe:

```
$ sudo su
```

```
$ apt-get update
```

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

// instalacija ssh paketa

2. Provjera statusa SSH servisa

- 1) Nakon instalacije, SSH bi trebao biti funkcionalan, no to možemo i provjeriti uz naredbu:

```
$ systemctl is-enabled ssh
```

Ukoliko odgovor nije **enabled**, omogućiti ga pomoću **systemctl enable ssh**.

- 2) Također, je li SSH aktivan možemo provjeriti uz naredbu:

```
$ systemctl is-active ssh
```

Ukoliko odgovor nije **active**, pokrenuti ga pomoću **systemctl start ssh**.

Za detaljniji status servisa, koristiti naredbu **systemctl status ssh**.

3. Postavljanje mrežne konfiguracije Linux Mint poslužitelja

- 1) Nakon uspješne instalacije, mrežne postavke Poslužitelja u VMware-u podesiti na **Lan segment 1**.
- 2) U Advanced Network Configuration kod Linux Mint poslužitelja podesiti statičku IP adresu računala:

```
Advanced Network Configuration -> Edit -> IPv4 tab -> Manual -> Add -> Save
```

Address: **172.16.2.30** **Netmask:** **24** **Gateway:** **PRAZNO zbog lokalne mreže**

Provjerite jel serverski mrežni priključak **ens33** ima potrebnu IP adresu 172.16.2.30, subnet masku 255.255.255.0 i broadcast adresu 172.16.2.255. Server i klijent moraju biti u istoj mreži 172.16.2.x:

```
$ ifconfig
```

4. Download PuTTY terminala na Windows 10 klijent

- 1) Postaviti snapshot u VMware-u za Klijenta (Windows 10) na **cleanInstall** da započnete čistu konfiguraciju PuTTY terminala.
- 2) Pokrenuti Klijent (Windows 10)

```
User : ne koristi se
```

Password : ne koristi se

- 3) Na Klijentu (Windows 10) u Network adapter postavkama odaberite **NAT** kako bi mogli pristupiti internetu kod instalacije PuTTY terminala.
- 4) Otvorite Microsoft Edge preglednik te na sve upite za customizaciju odgovorite s NE i završite postavljanje preglednika.
 - Otiđite na službeni site: <https://www.PuTTY.org/>
 - Preuzmite PuTTY terminal instalaciju: **Download** [PuTTY-64bit-0.83-installer.msi](#)
 - Pokrenite i izvršite instalaciju PuTTY-ja.
- 5) Nakon uspješne instalacije PuTTY-ja, mrežne postavke Klijenta u podesiti na **Lan segment 1**.
- 6) Na Klijentu Windows 10 postaviti statičku IP adresu:
 - Win + R > ncpa.cpl > Ethernet0 > Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties

Postavi statičku IP adresu:

- Odaberi **Use the following IP address** i unesi sljedeće:
 - **IP address:** **172.16.2.20** (ili bilo koja slobodna IP adresa u tvojoj mreži 172.16.2.x).
 - **Subnet mask:** **255.255.255.0**
 - **Default gateway:** **Ostaviti prazno**
- Klikni **OK**.

Postavi DNS servere (opcionalno):

- Ne treba postavljati.

Provjera IP adrese:

- Otvori **cmd** i upiši:

ipconfig

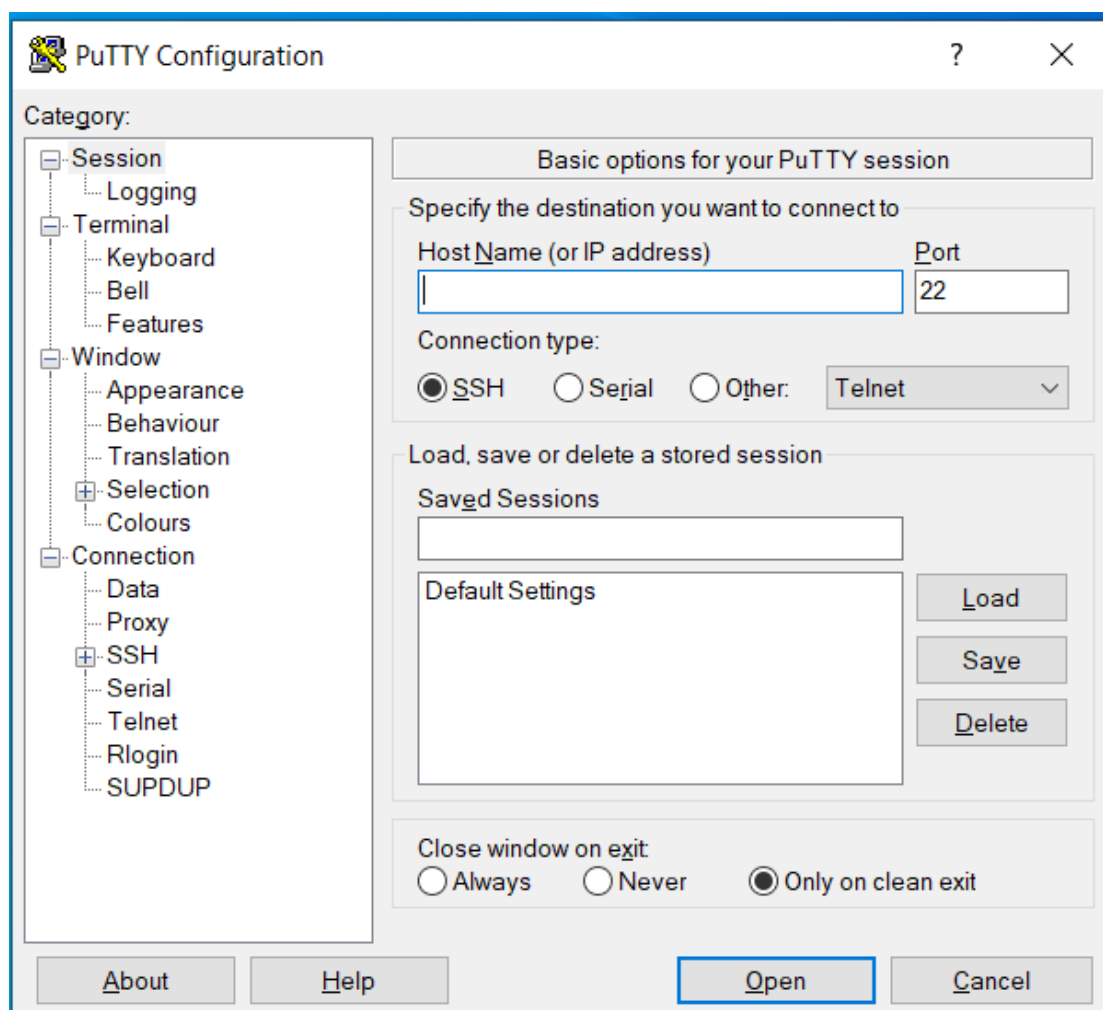
- Provjeri da li je statička IP adresa ispravno postavljena u odgovoru.
- Napravite ping Poslužitelja Linux Mint:

ping 172.16.2.30

- **NAPOMENA:** Ukoliko niste dobro postavili mrežne postavke servera i klijenta ping neće proći te morate popraviti postavke, što je nužno za nastavak vježbe

5. Testiranje SSH servisa (logiranje s korisničkim računom i lozinkom)

- 1) Pokrenite PuTTY na Windows 10 klijentu
- 2) Proučiti mogućnosti i opcije koje aplikacija nudi.



- 3) Pokrenite alat **Wireshark**, analizirajte SSH promet između dva virtualna računala. Možete li pronaći **sadržaj** komunikacije između dva računala? Objasnite odgovor profesoru kad dobijete rezultate.
- 4) Upisati adresu poslužitelja Linux Mint u za to predviđeno polje Host name (or IP address), Port 22 te pokrenuti konekciju.
- 5) Potrebno je upisati korisničko ime i lozinku računa na poslužitelju Linux Mint:

Korisničko ime (Login as): **osboxes**

Lozinka ([osboxes@172.16.2.30's](mailto:osboxes@172.16.2.30) password): **osboxes.org**

Ukoliko je sve ispravno uneseno, dobiva se pristup terminalu poslužitelja i možete analizirati SSH Wireshark promet.

6) Pokažite profesoru logiranje kroz PuTTY

7) Zavorite PuTTY i krenite dalje s vježbom.

6. Testiranje SSH servisa (logiranje bez lozinke samo s ključem)

Koraci za konfiguraciju PuTTY-a s parom ključeva:

Ključeve generirati pomoću alata **PuTTYgen** (dolazi uz PuTTY).

1) Pokrenite PuTTYgen:

- Na Windowsu potražite **PuTTYgen** (obično je instaliran zajedno s PuTTY-jem).
- Pokrenite ga.

2) Generirajte novi par ključeva:

- U PuTTYgenu odaberite vrstu ključa (odaberite EdDSA > **ED25519 (255 bits)**).
- Kliknite na **Generate**.
- Pomaknite mišem po prozoru kako biste generirali entropiju (slučajnost) za ključ.

3) Spremite privatni ključ:

- Nakon generiranja ključa, kliknite na **Save private key**.
- Spremite privatni ključ u sigurnu lokaciju (npr. C:\Users\tsrb\ImePrezime\.ssh\id_rsa.ppk).
- **Napomena:** PuTTY koristi .ppk format za privatne ključeve.

4) Kopirajte javni ključ:

- Javni ključ će biti prikazan u polju **Public key for pasting into OpenSSH authorized_keys file**.
- Kopirajte cijeli javni ključ (počinje s ssh-rsa ili ssh-ed25519).

5) Dodajte javni ključ na poslužitelj:

- Prijavite se na poslužitelj (Linux Mint) putem SSH-a koristeći lozinku.
- U direktoriju ~/.ssh/ stvorite datoteku authorized_keys (ako već ne postoji):
 - a) Provjera jel .ssh direktorij postoji u vašem home (osboxes) direktoriju:

```
$ [ -d ~/.ssh ] && echo "Direktorij .ssh postoji" || echo  
"Direktorij .ssh ne postoji" //komanda u jednom redu
```

b) Ako direktorij `.ssh` **ne postoji** nastavi dalje, kreiraj direktorij i prava za njega:

```
$ mkdir -p /home/osboxes/.ssh
```

```
$ sudo chmod 700 /home/osboxes/.ssh
```

c) Dodajte javni ključ u `/home/osboxes/.ssh/authorized_keys`:

```
$ sudo nano /home/osboxes/.ssh/authorized_keys
```

Zalijepite javni ključ i spremite datoteku (Ctrl+X, Y, Enter).

d) Postavite prava pristupa:

```
$ sudo chmod 600 /home/osboxes/.ssh/authorized_keys
```

```
$ sudo chown -R osboxes:osboxes /home/osboxes/.ssh
```

e) Provjera prava pristupa:

```
$ ls -la /home/osboxes/.ssh
```

Dobit ćete ovakav odgovor:

```
drwx----- 2 osboxes osboxes 4096 Feb 21 15:21 .
```

```
drwxr-x--- 15 osboxes osboxes 4096 Feb 21 15:17 ..
```

```
-rw----- 1 osboxes osboxes 100 Feb 21 15:20 authorized_keys
```

6) Konfiguriranje PuTTY-a za korištenje privatnog ključa

1) Pokrenite PuTTY:

- Otvorite PuTTY na Windows 10 klijentu.

2) Unesite podatke o poslužitelju:

- U polju **Host Name (or IP address)** unesite IP adresu poslužitelja (npr. `172.16.2.30`).
- Provjerite je li **Port** postavljen na 22.

3) Konfigurirajte privatni ključ:

- U lijevom izborniku proširite **Connection > SSH > Auth > Credentials**
- Kliknite na **Browse** pored polja **Private key file for authentication**.
- Odaberite privatni ključ (.ppk datoteku) koji ste spremili ranije.

4) Spremite sesiju:

- Vratite se na **Session** u lijevom izborniku.
- Unesite naziv sesije u polje **Saved Sessions** (npr. Linux Mint SSH).
- Kliknite na **Save** kako biste spremili konfiguraciju za buduće korištenje.

5) Povežite se na poslužitelj:

- Kliknite na **Open** kako biste pokrenuli vezu.

- Ako je sve ispravno konfigurirano, PuTTY će koristiti privatni ključ za autentifikaciju i neće tražiti lozinku.

7. Obavite vježbu LV12 - SNMP servis na Linux Mintu v2025v3 kroz PuTTY

8. Pokažite profesoru obavljenju vježbu snimanje SNMP prometa

9. Bravo!!! Zaslužili ste najbolju ocjenu Tehničari za računalstvo! Budite ponosni na sebe!

10. Vratite računala na cleanInstall i Home, uspješno ste završili vježbu.