TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky
a mezioborových studií

# Autentizace certifikáty

Datum zpracování: 7. 11. 2023

Zpracovali: Hynek Václav Svobodný, Kohout Daniel, Knespl Daniel, Koten Tomáš, Musilová Anežka

# Zadání

*Zapojte lokální síť s DHCP.*

1. Ve virtuálních strojích (nebo na vlastních počítačích) vytvořte každému členovi týmu uživatelský účet.
2. Zpřístupněte stroje pro přístup **ssh** z lokální sítě (konfigurace firewallu, ...).
3. Pomocí **ssh-keygen** vytvořte certifikáty a umístěte je na ostatní stroje.
4. Vytvořené certifikáty použijte i na router pro přístup bez hesla.
5. Proces dokumentujte screenshoty a kopiemi relevantních příkazů.

Úlohu zpracovávejte ve 2 - 5členných týmech.

Elaborát zpracujte do šablony v záhlaví kruzu, odevzdávejte ve formátu PDF.

**Do abecedně seřazeného seznamu řešitelů na úvodním listu uveďte reálné složení týmu!**

Adresa routeru je 192.168.1.1, login **root**, heslo **654321TUL**

Pokud ssh odmítne připojení s následující chybou:

```
Unable to negotiate with 192.168.1.1 port 22: no matching host key type found. Their offer: ssh-rsa
```

Nastavte v souboru ~/.ssh/config

```
HostKeyAlgorithms ssh-rsa
```

# Postup

1. Nejdříve jsme si na svých zařízeních vytvořili účty pro ostatní členy týmu nastavili jim heslo
    - Přidání uživatele → ***sudo adduser [uživatelské jméno] --force-badname***

```
student@virta:~$ sudo adduser anezka.musilova --force-badname
student@virta:~$ sudo adduser daniel.kohout   --force-badname
student@virta:~$ sudo adduser daniel.knespl   --force-badname
student@virta:~$ sudo adduser tomas.koten     --force-badname
student@virta:~$ sudo adduser hynek.svobodny  --force-badname
```

*Obrázek 1: Vytváření uživatelů*

2. Nastavili jsme firewall pro přístup **ssh** z lokální sítě
    - Nastavení firewallu → ***sudo ufw allow from [IP adresa] to any port 22***

```
student@virta: $ sudo ufw allow from 192.168.56.0/24 to any port 22
Rule added
student@virta: $ sudo ufw allow from 192.168.1.0/24 to any port 22
Rule added
```

*Obrázek 2: Nastavení firewallu*

3. Každý se přihlásil pod svým účtem a pomocí **ssh-keygen** jsme si každý vytvořili certifikát:

```
hynek.svobodny@virta: ~ — -ssh hynek.vaclav.svobodny@a0304.nti.tul.c...
hynek.svobodny@virta:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/hynek.svobodny/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/hynek.svobodny/.ssh/id_rsa
Your public key has been saved in /home/hynek.svobodny/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:nBhiDTCqg+32OuBB5r1+UuXJ77DHp5DzHM1VAOVaE9I hynek.svobodny@virta
The key's randomart image is:
+---[RSA 3072]----+
|  o..      o++   |
| . . o      oEo  |
|.   o o      + . |
|o+ . . = .  o o  |
|B o   = S  . .   |
|.= . . +. o .    |
|..+ o  =o. o     |
| o.+ .  B+..     |
|  o++  .o=o      |
+----[SHA256]-----+
hynek.svobodny@virta:~$
```

*Obrázek 3: Vytvoření certifikátu*

- Poté jsme pod svým účtem přihlásili na ostatní zařízení a přidali svůj certifikát
  - Přidání adresáře .ssh → ***mkdir ./.ssh***
  - Přidání vlastního certifikátu → ***nano ./.ssh/authorized_keys***


*Obrázek 4: Přidání certifikátu do ./.ssh/authorized_keys*

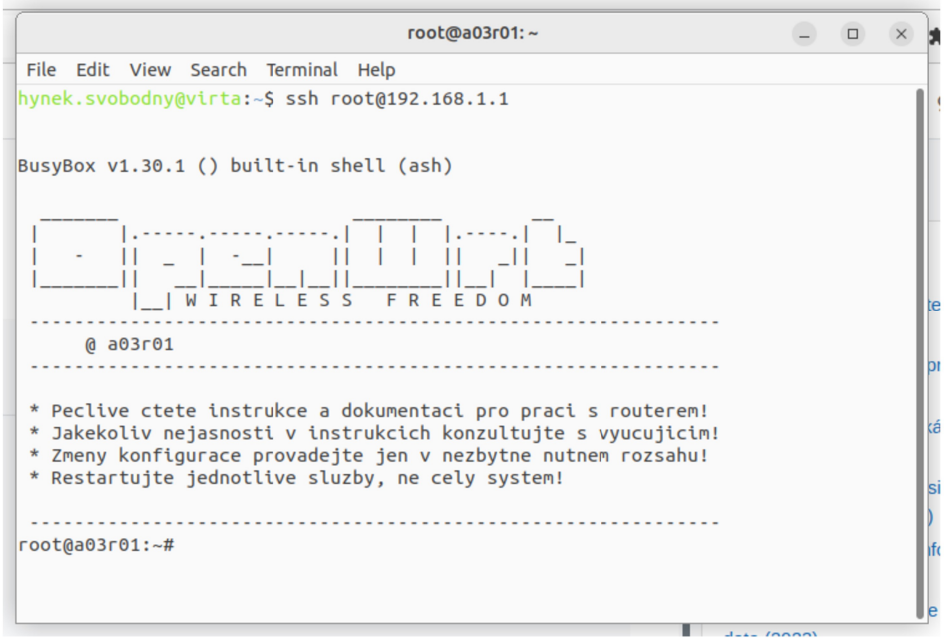
- Poté stačilo se na stroj přihlásit znovu a zkontrolovat, že to lze provést bez zadání hesla.

4. Přístup na router bez hesla
   - Nejdříve bylo ssh připojení odmítnuto s chybou:
     `Unable to negotiate with 192.168.1.1 port 22: no matching host key type found. Their offer: ssh-rsa`
   - Bylo potřeba přidat nastavení do konfiguračního souboru ~/.ssh/config

```
PubkeyAcceptedAlgorithms +ssh-rsa
HostkeyAlgorithms +ssh-rsa
StrictHostKeyChecking no
```

*Obrázek 5: Nastavení ssh připojení*

- Přihlášení na router → ***sudo ssh root@192.168.1.1***




*Obrázek 6: Přihlášení k routeru*

## Závěr

Při této úloze jsme pracovali jako pětičlenný tým, který měl dostupné jen čtyři zařízení. Přesto se všichni všichni přispěli k vypracování úlohy. Nejtěžší na této úloze byla organizace práce jednotlivých členů týmu, jelikož některé kroky, jako je vytváření uživatelů, musely být uskutečněny na všech zařízeních. Dalším problémem bylo nastavení přihlašování na router bez nutnosti zadávat heslo. Řešení leželo v úpravě nastavení konfiguračního souboru pro ssh.