VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Návrh, správa a bezpečnost počítačových sítí 2020/2021

3. laboratórne cvičenie

3. marca 2021

Alex Sporni (xsporn01)

1 Zadanie

Celé zadanie laboratórnej úlohy je možné nájsť v e-learningu na karte predmetu alebo na Dropboxe[1]

- Nainstalujte SSH server.
- Seznamte se se základní konfigurací (důležité soubory).
- Vygenerujte asymetrické klíče a importujte veřejný klíč na server.
- Zakažte přihlášení superuživatele a přihlášení pomocí hesla pro všechny uživatele.
- Změňte port SSH na 2222.
- Vytvořte uživatele RemoteWorker a zablokujte jeho přihlášení.
- Na straně serveru nastavte jen silné kr. alg. (ne RC4).
- Zjistěte podporované kr. alg. u uživatele, nastavte šifrování na AES-128-CBC.
- Kam loguje hlášení server, s jakou prioritou.
- Povolte přístup uživateli (user) do SSH na serveru pomocí TCP Wrappers, ostatní zakažte (správné řešení!).

2 Nastavenie pracoviska

Príklad pre pracovisko	**Klient**	**Server**
IP	192.168.17.135	192.168.17.137
MAC	00:0C:29:5C:68:C5	00:0C:29:6E:65:F1

Tabuľka 1: Nastavenie pracoviska

3 Riešenie

V tejto sekcii bude vyriešené laboratórna úloha číslo 3.

[1] `https://paper.dropbox.com/doc/3-CV-ehSrtwIS4ajpWbnBcRD3H`

3.1 Instalace SSH serveru

Ako je možné vidieť na obrázku 1, tak SSH server sa nainštaloval a služba beží.

```
Preparing to unpack .../openssh-server_1%3a7.9p1-10+deb10u2_amd64.deb ...
Unpacking openssh-server (1:7.9p1-10+deb10u2) ...
Setting up openssh-sftp-server (1:7.9p1-10+deb10u2) ...
Setting up libwrap0:amd64 (7.6.q-28) ...
Setting up openssh-server (1:7.9p1-10+deb10u2) ...

Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
2048 SHA256:cSaXtYgTKqB4Csk1ODBK5EWkr1iVnD945BXSOZJGOrs root@debianServer (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:PrwCxg2X2uBw+r4rFDFLHac2HipAzazdQYXXUFyxUpg root@debianServer (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:vN+h8L0rGHuVkoQUrkY9HF4xQPBwYwBxRBnR2VkiSnA root@debianServer (ED25519)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.se
rvice.
rescue-ssh.target is a disabled or a static unit, not starting it.
Processing triggers for systemd (241-7~deb10u6) ...
Processing triggers for man-db (2.8.5-2) ...
Processing triggers for libc-bin (2.28-10) ...
root@debianServer:~# service sshd status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-03-02 14:58:18 EST; 46s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1224 (sshd)
    Tasks: 1 (limit: 2330)
   Memory: 2.5M
   CGroup: /system.slice/ssh.service
           └─1224 /usr/sbin/sshd -D

Mar 02 14:58:18 debianServer systemd[1]: Starting OpenBSD Secure Shell server...
Mar 02 14:58:18 debianServer sshd[1224]: Server listening on 0.0.0.0 port 22.
Mar 02 14:58:18 debianServer sshd[1224]: Server listening on :: port 22.
Mar 02 14:58:18 debianServer systemd[1]: Started OpenBSD Secure Shell server.
root@debianServer:~#
```

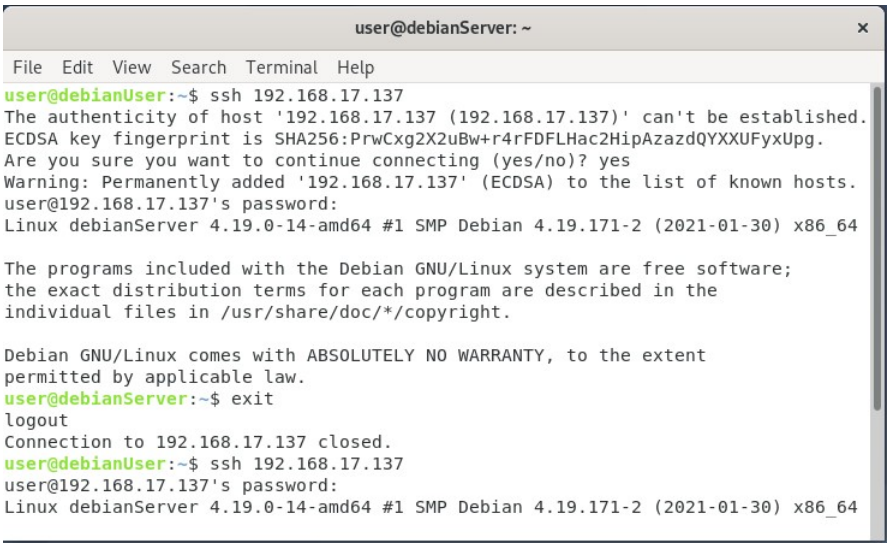
Obr. 1: Inštalácia SSH

3.2 Autentizace serveru

```
user@debianUser: ~
File  Edit  View  Search  Terminal  Help
root@debianUser:/home/user# ls -all
total 76
drwxr-xr-x 15 user user 4096 Mar  2 14:29 .
drwxr-xr-x  4 root root 4096 Mar  2 14:40 ..
-rw-r--r--  1 user user  220 Mar  2 14:27 .bash_logout
-rw-r--r--  1 user user 3526 Mar  2 14:27 .bashrc
drwx------  9 user user 4096 Mar  2 14:38 .cache
drwx------ 10 user user 4096 Mar  2 14:30 .config
drwxr-xr-x  2 user user 4096 Mar  2 14:28 Desktop
drwxr-xr-x  2 user user 4096 Mar  2 14:28 Documents
drwxr-xr-x  2 user user 4096 Mar  2 14:28 Downloads
drwx------  3 user user 4096 Mar  2 14:29 .gnupg
-rw-------  1 user user  330 Mar  2 14:28 .ICEauthority
drwx------  3 user user 4096 Mar  2 14:28 .local
drwxr-xr-x  2 user user 4096 Mar  2 14:28 Music
drwxr-xr-x  2 user user 4096 Mar  2 14:28 Pictures
-rw-r--r--  1 user user  807 Mar  2 14:27 .profile
drwxr-xr-x  2 user user 4096 Mar  2 14:28 Public
drwx------  2 user user 4096 Mar  2 14:29 .ssh
drwxr-xr-x  2 user user 4096 Mar  2 14:28 Templates
drwxr-xr-x  2 user user 4096 Mar  2 14:28 Videos
root@debianUser:/home/user#
```

Obr. 2: Obsah domovskej zložky

Na obrázku 3, je možné vidieť prvé úspešné prihlásanie na server `192.168.17.137` pomocou SSH. Keďže sa jedná o úplne prvé prihlásenie, tak je možné vidieť aj fingerprint debianServeru. Ten je možné si overiť na debianServeri pomocou príkazu `ssh-keygen -lf /etc/ssh/ssh_host_ecdsa_key.pub` ako je možné vidieť na obrázku 4.



Obr. 3: Úspešné prihlásenie sa na server pomocou SSH

Obr. 4: Fingerprint serveru

Pomocou príkazu `ssh-keygen -f ssh_host_ecdsa_key` si pregenerujeme[2] fingerprint ako je možné vidieť na obrázku 5.

Obr. 5: Vygenerovanie nového fingerprintu

[2]Pri opätovnom prihlásení na server cez SSH mi nevyskočila hláška v podobe REMOTE HOST IDENTIFICATION HAS CHANGED

Následne podsekciu *autentizácia serveru* 3.2 zakončíme ručným vymazaním fingerprint záznamu z `known_hosts` a prihlásením sa znovu na server.

```
user@debianServer: ~
File  Edit  View  Search  Terminal  Help
user@debianUser:~/.ssh$ ssh-keygen -R 192.168.17.137
# Host 192.168.17.137 found: line 1
/home/user/.ssh/known_hosts updated.
Original contents retained as /home/user/.ssh/known_hosts.old
user@debianUser:~/.ssh$ cat known_hosts
user@debianUser:~/.ssh$ ssh 192.168.17.137
The authenticity of host '192.168.17.137 (192.168.17.137)' can't be established.
ECDSA key fingerprint is SHA256:PrwCxg2X2uBw+r4rFDFLHac2HipAzazdQYXXUFyxUpg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.17.137' (ECDSA) to the list of known hosts.
user@192.168.17.137's password:
Linux debianServer 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Mar  2 15:52:03 2021 from 192.168.17.135
user@debianServer:~$
```

Obr. 6: Vymazanie fingerprintu a následné prihlásenie na server

3.3 Autentizace klienta využívající asymetrickou kryptografii

Najprv sa na klientovi vygeneruje pár verejného a súkromného kľúča, ako je možné vidieť na obrázku 7.

```
user@debianUser: ~/.ssh
File  Edit  View  Search  Terminal  Help
user@debianUser:~/.ssh$ ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_ecdsa.
Your public key has been saved in /home/user/.ssh/id_ecdsa.pub.
The key fingerprint is:
SHA256:a/1YqyD8BSPaRi9VOS7wl40mkhKxxRySuVu2BjygstI user@debianUser
The key's randomart image is:
+---[ECDSA 256]---+
|     o=o.         |
|   . o=o    .     |
| . oo..   +       |
|o   =.o+ o =      |
|.o  .*=.S * .     |
|o E .*o= X        |
|.   ..* = o .     |
|      . = o + .   |
|        . o.o     |
+----[SHA256]-----+
user@debianUser:~/.ssh$
```

Obr. 7: Vygenerovanie verejného a súkromného kľúča

Následne je možné pomocou ssh preniesť daný fingerprint na server ako je možné vidieť na ukážke 8.

```
user@debianUser:~/.ssh$ ssh-copy-id 192.168.17.137
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
user@192.168.17.137's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh '192.168.17.137'"
and check to make sure that only the key(s) you wanted were added.
```

Obr. 8: Prenesenie fingerprintu na server

Teraz je možné sa prihlásiť na server pomocou príkazu `ssh 192.168.17.137` bez hesla ako je možné vidieť na ukážke 9.

```
user@debianServer: ~
File  Edit  View  Search  Terminal  Help
user@debianUser:~/.ssh$ ssh 192.168.17.137
Linux debianServer 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Mar  2 16:37:09 2021 from 192.168.17.135
user@debianServer:~$
```

Obr. 9: Prihlásenie sa na server bez možnosti zadania hesla

Je možné si zobraziť tento autorizačný kľúč na serveri viď. ukážka 10

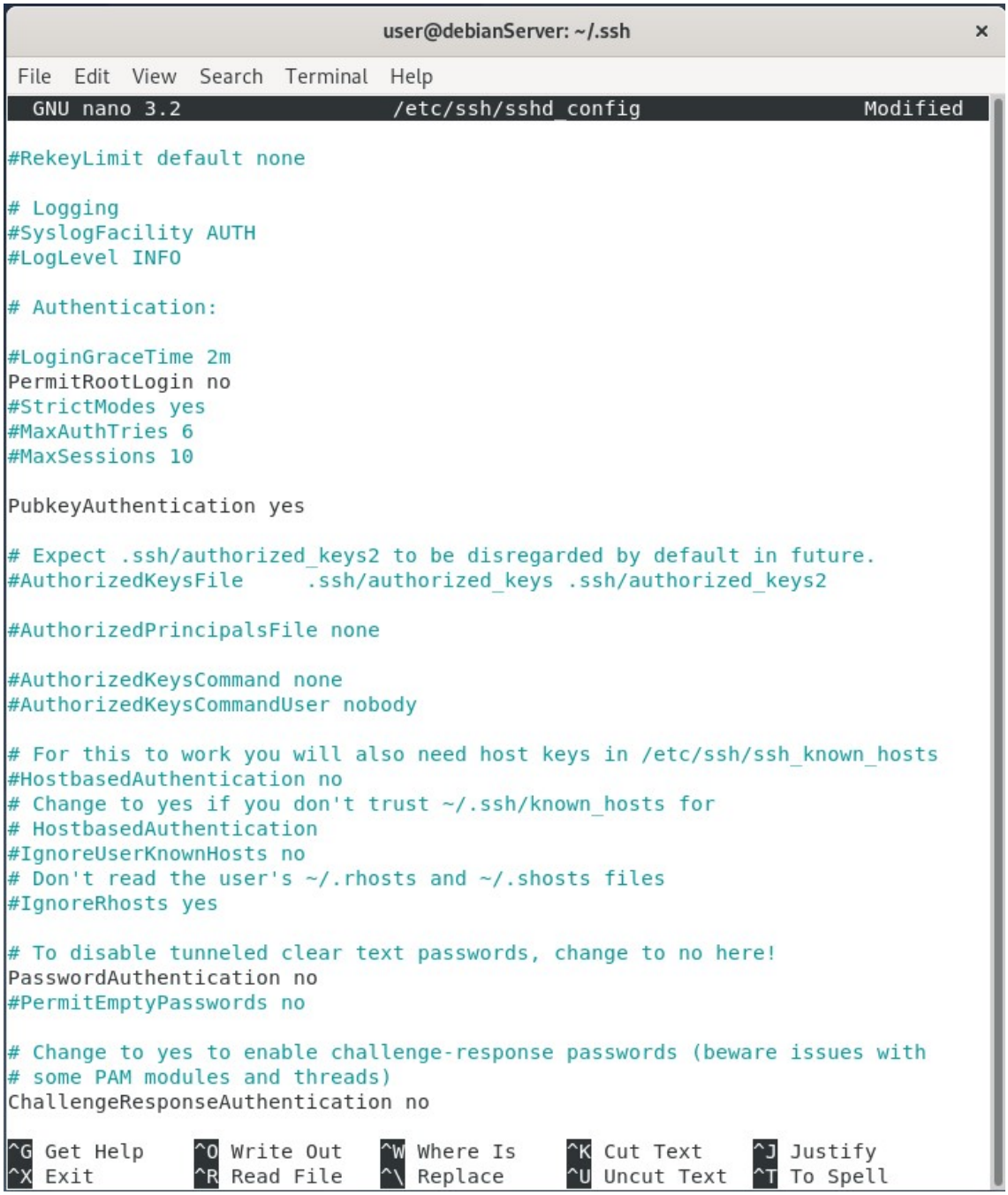
```
user@debianServer: ~/.ssh
File  Edit  View  Search  Terminal  Help
user@debianServer:~/.ssh$ ls -all
total 20
drwx------ 2 user user 4096 Mar  2 16:41 .
drwxr-xr-x 3 user user 4096 Mar  2 16:33 ..
-rw------- 1 user user  177 Mar  2 16:41 authorized_keys
-rw------- 1 user user  513 Mar  2 16:33 id_ecdsa
-rw-r--r-- 1 user user  179 Mar  2 16:33 id_ecdsa.pub
user@debianServer:~/.ssh$ cat authorized_keys
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHo+Y
N+En2XtFkjUPhkOMLTbPVUhsyK6FcvkmEWjK2bm9lkT4xF/OQiF2jIt7RRFHYGPrhQ3SLYAVRx3rn
Mh9mU= user@debianUser
user@debianServer:~/.ssh$
```

Obr. 10: Autorizačný kľúč debianUsera

3.4 Nastavení SSH serveru

V prvom rade je potrebné zakázať autentifikáciu na báze hesla pomocou. Nasledujúce zmeny budú prevedené v súbore `sshd_config`. Pomocou príkazu `nano /etc/ssh/sshd_config` editujeme daný súbor. Budeme editovať nasledujúce parametre 11.

- PasswordAuthentication no
- PermitRootLogin no
- PubKeyAuthentication yes



Obr. 11: Požadovaná konfigurácia

Po pokuse o prihlásenie je ssh na root odmietnuté viď 12.

```
user@debianUser: ~/.ssh
File  Edit  View  Search  Terminal  Help
user@debianUser:~/.ssh$ ssh root@192.168.17.137
root@192.168.17.137: Permission denied (publickey).
user@debianUser:~/.ssh$
```

Obr. 12: Permission denied

Na nasledujúcom obrázku je možné vidieť odmietnutie prihlásenie cez SSH port 22. Je možné sa prihlásiť cez povolený port 2222 viď 13.

```
user@debianServer: ~
File  Edit  View  Search  Terminal  Help
user@debianUser:~$ ssh 192.168.17.137
ssh: connect to host 192.168.17.137 port 22: Connection refused
user@debianUser:~$ ssh 192.168.17.137 -p 2222
Linux debianServer 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar  3 06:42:50 2021 from 192.168.17.135
user@debianServer:~$ ss -ntl
State      Recv-Q     Send-Q       Local Address:Port        Peer Address:Port
LISTEN     0          128                0.0.0.0:2222             0.0.0.0:*
LISTEN     0          128                   [::]:2222                [::]:*
user@debianServer:~$
```

Obr. 13: Odmietnutie prihlásenia a následné prihlásenie sa cez port 2222

Pridanie užívateľa 'Karel' 14 a následný pokus o prihlásenie sa na ssh server pod týmto užívateľom 15.

```
root@debianServer:~# adduser karel
Adding user `karel' ...
Adding new group `karel' (1001) ...
Adding new user `karel' (1001) with group `karel' ...
Creating home directory `/home/karel' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for karel
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root@debianServer:~# _
```

Obr. 14: Vytvorenie užívateľa Karel

```
user@debianUser: ~
File  Edit  View  Search  Terminal  Help
user@debianUser:~$ ssh karel@192.168.17.137
karel@192.168.17.137: Permission denied (publickey).
user@debianUser:~$
```

Obr. 15: Pokus o prihlásenie sa na server

```
karel@debianServer: ~
File  Edit  View  Search  Terminal  Help
user@debianUser:~$ ssh user@192.168.17.137
user@192.168.17.137's password:
Permission denied, please try again.
user@192.168.17.137's password:

user@debianUser:~$ ssh karel@192.168.17.137
karel@192.168.17.137's password:
Linux debianServer 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar  3 07:36:43 2021 from 192.168.17.135
karel@debianServer:~$
```

Obr. 16: Povolenie Karla a zakázanie usera

3.5 TCP Wrappers

Ukážka zakázanie klienta `192.168.17.135` v súbore `/etc/hosts.deny` 17.

```
  GNU nano 3.2                    /etc/hosts.deny

# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

sshd : 192.168.17.135
```

Obr. 17: Explicitne zakazanie klienta

Následne je možné si overiť, či k zakázaniu naozaj prislšlo viď 18.

```
user@debianUser: ~
File  Edit  View  Search  Terminal  Help
user@debianUser:~$ ssh user@192.168.17.137
ssh_exchange_identification: read: Connection reset by peer
user@debianUser:~$
```

Obr. 18: Pokus o pripojenie

Teraz zakážeme každého okrem klienta `192.168.17.135`

```
  GNU nano 3.2                          /etc/hosts.deny

# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

sshd : all
```

Obr. 19: Zakázanie všetkých spojení

```
  GNU nano 3.2                          /etc/hosts.allow

# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#

sshd : 192.168.254.129
```

Obr. 20: Povolenie klienta

3.6 Fail2Ban

Na obrázku 21 je možné vidieť schválne zadané zlé heslá a následne odmietnutie spojenia.

```
user@debianUser: ~
File  Edit  View  Search  Terminal  Help
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar  3 08:09:38 2021 from 192.168.17.135
user@debianServer:~$ exit
logout
Connection to 192.168.17.137 closed.
user@debianUser:~$ ssh karel@192.168.17.137
karel@192.168.17.137's password:

user@debianUser:~$ ssh karel@192.168.17.137
karel@192.168.17.137's password:
sPermission denied, please try again.
karel@192.168.17.137's password:
Permission denied, please try again.
karel@192.168.17.137's password:
karel@192.168.17.137: Permission denied (password).
user@debianUser:~$ ssh karel@192.168.17.137
ssh: connect to host 192.168.17.137 port 22: Connection refused
user@debianUser:~$
```

Obr. 21: Odmietnutie spojenia

```
root@debianServer:~# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
f2b-sshd   tcp  --  0.0.0.0/0            0.0.0.0/0            multiport dports 22

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain f2b-sshd (1 references)
target     prot opt source               destination
REJECT     all  --  192.168.17.135       0.0.0.0/0            reject-with icmp-port-unreachable
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
root@debianServer:~# _
```

Obr. 22: fail2ban ssh table

4 Samostatné Úkoly

4.1 Nastavenie šifrovania

Na ukážke 23 je možné vidieť, že klient podporuje šifrovanie AES-128-CBC

```
user@debianUser: ~
File  Edit  View  Search  Terminal  Help
user@debianUser:~$ ssh -Q cipher
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
rijndael-cbc@lysator.liu.se
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
user@debianUser:~$
```

Obr. 23: Podporované šifrovacie protokoly

Následne na serveri nastavíme šifrovanie AES128-CBC viď 24.

```
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
ciphers AES-128-CBC
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Obr. 24: Povolenie šifrovania na strane serveru

Následne sa prihlásime na server pomocou SSH a špecifikujeme použité šifrovanie viď. 25.

```
user@debianServer: ~
File  Edit  View  Search  Terminal  Help
user@debianUser:~$ ssh -c aes128-cbc 192.168.17.137
user@192.168.17.137's password:
Linux debianServer 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x
86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar  3 09:16:47 2021 from 192.168.17.135
user@debianServer:~$
```

Obr. 25: Prihlásenie sa

4.2 Logovanie

Logovanie je znovu potrebné nastaviť v `sshd_config` viď 26

```
  GNU nano 3.2                    /etc/ssh/sshd_config                    Mod

#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
ciphers aes128-cbc
#RekeyLimit default none

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:

#LoginGraceTime 2m

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line M-E Redo
```

Obr. 26: Povolenie logovania

Logy sa nachádzajú v súbore `/var/log/auth.log`

```
Mar  3 09:16:47 debianServer sshd[2264]: Accepted password for user from 192.168.17.135 port 50450 s
sh2
Mar  3 09:16:47 debianServer sshd[2264]: pam_unix(sshd:session): session opened for user user by (ui
d=0)
Mar  3 09:16:47 debianServer systemd-logind[428]: New session 41 of user user.
Mar  3 09:16:47 debianServer systemd: pam_unix(systemd-user:session): session opened for user user b
y (uid=0)
Mar  3 09:17:01 debianServer CRON[2280]: pam_unix(cron:session): session opened for user root by (ui
d=0)
Mar  3 09:17:01 debianServer CRON[2280]: pam_unix(cron:session): session closed for user root
Mar  3 09:41:32 debianServer sshd[2276]: Received disconnect from 192.168.17.135 port 50450:11: disc
onnected by user
Mar  3 09:41:32 debianServer sshd[2276]: Disconnected from user user 192.168.17.135 port 50450
Mar  3 09:41:32 debianServer sshd[2264]: pam_unix(sshd:session): session closed for user user
Mar  3 09:41:32 debianServer systemd-logind[428]: Session 41 logged out. Waiting for processes to ex
it.
Mar  3 09:41:32 debianServer systemd-logind[428]: Removed session 41.
Mar  3 09:41:42 debianServer systemd: pam_unix(systemd-user:session): session closed for user user
Mar  3 09:42:49 debianServer sshd[2310]: Accepted password for user from 192.168.17.135 port 50456 s
sh2
Mar  3 09:42:49 debianServer sshd[2310]: pam_unix(sshd:session): session opened for user user by (ui
d=0)
Mar  3 09:42:49 debianServer systemd-logind[428]: New session 44 of user user.
Mar  3 09:42:49 debianServer systemd: pam_unix(systemd-user:session): session opened for user user b
y (uid=0)
Mar  3 09:44:11 debianServer sshd[2322]: Received disconnect from 192.168.17.135 port 50456:11: disc
onnected by user
Mar  3 09:44:11 debianServer sshd[2322]: Disconnected from user user 192.168.17.135 port 50456
Mar  3 09:44:11 debianServer sshd[2310]: pam_unix(sshd:session): session closed for user user
Mar  3 09:44:11 debianServer systemd-logind[428]: Session 44 logged out. Waiting for processes to ex
it.
Mar  3 09:44:11 debianServer systemd-logind[428]: Removed session 44.
Mar  3 09:44:21 debianServer systemd: pam_unix(systemd-user:session): session closed for user user
Mar  3 09:57:03 debianServer sshd[2245]: Received signal 15; terminating.
Mar  3 09:57:03 debianServer sshd[2355]: Server listening on 0.0.0.0 port 22.
Mar  3 09:57:03 debianServer sshd[2355]: Server listening on :: port 22.
root@debianServer:~# _
```

Obr. 27: Logy