Exercise 1 – Installing and Configuring the SSH Server and Client

Verification of the installation and functionality of the OpenSSH server

Exercise 1.1: Tasks to Perform on AlmaLinux:

1. Verify that the **OpenSSH server** is installed and started on the **AlmaLinux server.**

```
[root@server12 ~]# dnf list openssh-server
Last metadata expiration check: 4:28:23 ago on Mon 31 Mar 2025 09:37:16 AM.
Installed Packages
openssh-server.x86_64                                          8.7p1-43.el9.alma.2
[root@server12 ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-03-30 16:11:37 EDT; 21h ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 1043 (sshd)
      Tasks: 1 (limit: 22830)
     Memory: 2.7M
        CPU: 37ms
     CGroup: /system.slice/sshd.service
             └─1043 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 30 16:11:37 server12 systemd[1]: Starting OpenSSH server daemon...
Mar 30 16:11:37 server12 sshd[1043]: Server listening on 0.0.0.0 port 22.
Mar 30 16:11:37 server12 sshd[1043]: Server listening on :: port 22.
Mar 30 16:11:37 server12 systemd[1]: Started OpenSSH server daemon.
[root@server12 ~]#
```

2. Identify the folder that contains the SSH daemon **(sshd)** configuration files.

```
[root@server12 ~]# cd /etc/ssh/
[root@server12 ssh]# ll
total 600
-rw-r--r--. 1 root root     578094 Mar  1 03:46 moduli
-rw-r--r--. 1 root root       1921 Mar  1 03:46 ssh_config
drwxr-xr-x. 2 root root         28 Mar  1 03:47 ssh_config.d
-rw-------. 1 root root       3667 Mar  1 03:46 sshd_config
drwx------. 2 root root         28 Mar  1 03:47 sshd_config.d
-rw-r-----. 1 root ssh_keys    492 Mar 27 13:37 ssh_host_ecdsa_key
-rw-r--r--. 1 root root        162 Mar 27 13:37 ssh_host_ecdsa_key.pub
-rw-r-----. 1 root ssh_keys    387 Mar 27 13:37 ssh_host_ed25519_key
-rw-r--r--. 1 root root         82 Mar 27 13:37 ssh_host_ed25519_key.pub
-rw-r-----. 1 root ssh_keys   2578 Mar 27 13:37 ssh_host_rsa_key
-rw-r--r--. 1 root root        554 Mar 27 13:37 ssh_host_rsa_key.pub
[root@server12 ssh]#
```

3. What is the name of the **main configuration file used** by the sshd server?

   sshd_config

4. How many **public/private keys** does this server have?

   3 private and 3 public keys

5. Type the following command and leave it listening:
   sudo tcpdump -i *ens192* -XX -s 0 tcp port 22 *(where **ens192** is the name of the interface connected to the Ubuntu machine)*

```
[root@server12 /]# sudo tcpdump -i ens192 -XX -s 0 tcp port 22
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens192, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

6. Leave the **AlmaLinux** session open and switch to the **Ubuntu** machine.

```
root@client12: ~
File  Edit  View  Search  Terminal  Help
root@client12:~#
```

Verification of the installation and functionality of the OpenSSH client

Exercise 1.2: Tasks to Perform on Ubuntu and AlmaLinux:

1. Verify that the **OpenSSH client** is installed on the **Ubuntu** system.

```
root@client12:~# apt list openssh-client
Listing... Done
openssh-client/jammy-updates,jammy-security,now 1:8.9p1-3ubuntu0.11 amd64 [installed,automatic]
openssh-client/jammy-updates,jammy-security 1:8.9p1-3ubuntu0.11 i386
root@client12:~#
```

2. From the **Ubuntu** client, use the **ssh** command to connect remotely to the **AlmaLinux** server remotely with your **AlmaLinux user account.**

```
root@client12:~# ssh lmohammed@192.168.50.10
The authenticity of host '192.168.50.10 (192.168.50.10)' can't be established.
ED25519 key fingerprint is SHA256:V/ZH5DdCbtlgZur1VdBl8Mobp9OPjCxam9im/JBjNys.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.10' (ED25519) to the list of known hosts.
lmohammed@192.168.50.10's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun Mar 30 16:12:06 2025
[lmohammed@server12 ~]$
```

3. Were you successful? What happened when you attempted to connect to the AlmaLinux server using the ssh command?

   Yes. AlmaLinux server sent it's public key, signed by it's private key and the server was added to the list of known hosts on the client. The host 192.168.50.10 (Alma) was then added to the list of known hosts in the ~/.ssh/ directory for future connections.

4. Run the command: **cat /etc/*-release**. If the connection is successful, the AlmaLinux version should be displayed.

```
[lmohammed@server12 ~]$ cat /etc/*-release
AlmaLinux release 9.5 (Teal Serval)
NAME="AlmaLinux"
VERSION="9.5 (Teal Serval)"
ID="almalinux"
ID_LIKE="rhel centos fedora"
VERSION_ID="9.5"
PLATFORM_ID="platform:el9"
PRETTY_NAME="AlmaLinux 9.5 (Teal Serval)"
ANSI_COLOR="0;34"
LOGO="fedora-logo-icon"
CPE_NAME="cpe:/o:almalinux:almalinux:9::baseos"
HOME_URL="https://almalinux.org/"
DOCUMENTATION_URL="https://wiki.almalinux.org/"
BUG_REPORT_URL="https://bugs.almalinux.org/"

ALMALINUX_MANTISBT_PROJECT="AlmaLinux-9"
ALMALINUX_MANTISBT_PROJECT_VERSION="9.5"
REDHAT_SUPPORT_PRODUCT="AlmaLinux"
REDHAT_SUPPORT_PRODUCT_VERSION="9.5"
SUPPORT_END=2032-06-01
AlmaLinux release 9.5 (Teal Serval)
AlmaLinux release 9.5 (Teal Serval)
[lmohammed@server12 ~]$
```

5. Leave the session open on **Ubuntu** and go back to the **AlmaLinux** server to review the output of the **tcpdump** command.

```
        0x0030:  00f9 e5d9 0000 0101 080a a442 61a1 e9af  ...........Ba...
        0x0040:  af28 8e61 ba63 1418 6170 b438 2875 3f3d  .(.a.c..ap.8(u?=
        0x0050:  440e 46d3 7b17 811e f1f8 83df 3b75 d92c  D.F.{.......;u.,
        0x0060:  c5ce f657 14a1 cfa8 eedf d877 ef44 b9bd  ...W.......w.D..
        0x0070:  1a75 f6bd 8aa6 2798 1e9a cd63 daf4 3b6a  .u....'....c..;j
        0x0080:  6313 2d7b dde7                           c.-{..
14:26:36.452544 IP 192.168.50.20.48118 > server12.ssh: Flags [.], ack 5994, win 473, opti
th 0
        0x0000:  000c 29ad 32d1 000c 2939 ec06 0800 4510  ..).2...)9....E.
        0x0010:  0034 d67a 4000 4006 7eca c0a8 3214 c0a8  .4.z@.@.~...2...
        0x0020:  320a bbf6 0016 c7aa b058 4240 851d 8010  2........XB@....
        0x0030:  01d9 f547 0000 0101 080a e9af af2b a442  ...G.........+.B
        0x0040:  61a1                                     a.
14:33:49.585935 IP 192.168.50.20.48118 > server12.ssh: Flags [P.], seq 3367:3435, ack 599
755813793], length 68
        0x0000:  000c 29ad 32d1 000c 2939 ec06 0800 4510  ..).2...)9....E.
        0x0010:  0078 d67b 4000 4006 7e85 c0a8 3214 c0a8  .x.{@.@.~...2...
        0x0020:  320a bbf6 0016 c7aa b058 4240 851d 8018  2........XB@....
        0x0030:  01d9 b48c 0000 0101 080a e9b6 4b06 a442  ............K..B
        0x0040:  61a1 9062 519b 79b1 5cec 25c8 3e8f ba15  a..bQ.y.\.%.>...
        0x0050:  611f d114 b6a0 9f8e c667 c4c3 8b35 88fd  a........g...5..
        0x0060:  73ff a412 22d0 920c 996c cf4a 4f4d d72a  s..."....l.JOM.*
        0x0070:  bc03 d9ca 12f5 b317 028f 7c09 c91b 1d51  ..........|....Q
        0x0080:  a81d a993 3712                           ....7.
14:33:49.620842 IP server12.ssh > 192.168.50.20.48118: Flags [P.], seq 5994:6062, ack 343
921038086], length 68
        0x0000:  000c 2939 ec06 000c 29ad 32d1 0800 4548  ..)9....).2...EH
        0x0010:  0078 686d 4000 4006 ec5b c0a8 320a c0a8  .xhm@.@..[..2...
        0x0020:  3214 0016 bbf6 4240 851d c7aa b09c 8018  2.....B@........
        0x0030:  00f9 e5d9 0000 0101 080a a448 fdb2 e9b6  ...........H....
        0x0040:  4b06 b42c f920 ed0a fb31 314e cfe0 a3f3  K..,.....11N....
        0x0050:  5014 ced8 62c9 fb91 775e b1f5 f62a 2d8d  P...b...w^...*-.
        0x0060:  6107 5e5b 1b7b be4b d15e f8ab 1ba2 e724  a.^[.{.K.^.....$
        0x0070:  118d 343b 44f3 962a fffd 527a 6da3 3aac  ..4;D..*..Rzm.:.
        0x0080:  79bc 9e96 58f1                           y...X.
```

6. Can you see your username and password? Why or why not?

   No. Because SSH uses encryption to secure the connection between the host and the client. Everything is encrypted before it's transmitted. This is why SSH is used over Telnet today.

7. Stop the **tcpdump** command on **AlmaLinux** and return to the **Ubuntu** client.

```
90 packets captured
96 packets received by filter
6 packets dropped by kernel
[root@server12 /]#
```

8. Log out from the **sshd server.**

```
[lmohammed@server12 ~]$ exit
logout
Connection to 192.168.50.10 closed.
root@client12:~#
```

9. Open the user's **.ssh** directory and list its contents.

```
root@client12:~/.ssh# ls -l
total 8
-rw------- 1 root root 978 Mar 31 14:20 known_hosts
-rw-r--r-- 1 root root 142 Mar 31 14:20 known_hosts.old
root@client12:~/.ssh#
```

10. Does it contain files? If yes, what is the name of this file and what does it contain?

Yes, it contains 2 files. Files known_hosts and known_hosts.old

Generation of Public/Private keys on the SSH client

Exercise 1.3: Tasks to Perform on Ubuntu:

1. From the **Ubuntu** client, connect to the **AlmaLinux** server again using **ssh** with your **AlmaLinux user account.**

```
root@client12:~/.ssh# ssh lmohammed@192.168.50.10
lmohammed@192.168.50.10's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Mar 31 14:20:22 2025 from 192.168.50.20
[lmohammed@server12 ~]$
```

2. Were you able to log in without entering a password?

   No, I still needed to input my password.

3. **Close the SSH connection using the exit command.**

You will now generate a public/private key pair on the client and copy the public key to the server in order to enable passwordless SSH authentication using the authorized_keys mechanism.

```
[lmohammed@server12 ~]$ exit
logout
Connection to 192.168.50.10 closed.
root@client12:~/.ssh#
```

4. On the **Ubuntu** client, generate a public/private key pair using the **RSA** algorithm.

```
lmohammed@client12:/etc$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/lmohammed/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/lmohammed/.ssh/id_rsa
Your public key has been saved in /home/lmohammed/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:e44odsLgTg0W/ZH/x2LmtsHpzdYl5f5s4gEwX2PJt0g lmohammed@client12
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|   .   .     . . |
|  . . o   o  E* .|
|   . . o   +.o.oo|
|  o   . S   o. + |
| ..o     + o .. o|
| ..o.   . X o..+ |
| .. = .. O.*. ooo|
| ... +. ..=oo..o+|
+----[SHA256]-----+
lmohammed@client12:/etc$
```

5. Use an SSH tool to copy the client's public key to the server.

```
lmohammed@client12:~/.ssh$ ssh-copy-id -i id_rsa.pub lmohammed@192.168.50.10
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "id_rsa.pub"
The authenticity of host '192.168.50.10 (192.168.50.10)' can't be established.
ED25519 key fingerprint is SHA256:V/ZH5DdCbtlgZur1VdBl8Mobp9OPjCxam9im/JBjNys.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/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 prompted now it is to install the new keys
lmohammed@192.168.50.10's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'lmohammed@192.168.50.10'"
and check to make sure that only the key(s) you wanted were added.

lmohammed@client12:~/.ssh$
```

6. Try connecting to the remote SSH server again.

```
lmohammed@client12:~/.ssh$ ssh lmohammed@192.168.50.10
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Mar 31 14:48:14 2025 from 192.168.50.20
[lmohammed@server12 ~]$
```

7. You should now be able to log in without a password. If not, review the previous steps to ensure everything was completed correctly.

   I was able to.

8. **Close the SSH connection using the exit command.**

```
[lmohammed@server12 ~]$ exit
logout
Connection to 192.168.50.10 closed.
lmohammed@client12:~/.ssh$
```

Modification of the OpenSSH server configuration

Exercise 1.4: Tasks to Perform on AlmaLinux and Ubuntu:

1. From the **Ubuntu** client, try to connect to the **AlmaLinux** server using **SSH** with the **root** account? Are you able to connect?

```
root@client12:~# ssh root@192.168.50.10
root@192.168.50.10's password:
Permission denied, please try again.
```

   No

2. On the **AlmaLinux** server, open the **OpenSSH server configuration file** and modify a **keyword** that allows the **root** user to connect to the sshd server.

```
# To modify the system-wide sshd configuration, create a  *.conf  fi
#  /etc/ssh/sshd_config.d/  which will be automatically included belo
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux system, you have to te
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#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
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

3. Reload the **SSH service** to apply the new configuration.

```
[root@server12 ssh]# systemctl reload sshd
[root@server12 ssh]#
```

4. Type the following command, to **audit** the connection between client and server:

   tail -f /var/log/audit/audit.log

```
[root@server12 ssh]# tail -f /var/log/audit/audit.log
```

5. Switch back to **Ubuntu** and try connecting again as **root** via SSH.

```
root@192.168.50.10's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Mar 31 15:22:21 2025 from 192.168.50.20
[root@server12 ~]#
```

6. If your configuration was correctly updated, you **should be able to log in with the root account.**

   I was able to log in.

7. Go back to the **AlmaLinux** server and examine the output in **audit.log.**

```
[root@server12 ssh]# tail -f /var/log/audit/audit.log
type=CRED_ACQ msg=audit(1743448941.427:488): pid=4536 uid=0 auid=0 ses=9 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:setcred gr
ntors=pam_unix acct="root" exe="/usr/sbin/sshd" hostname=192.168.50.20 addr=192.168.50.20 terminal=ssh res=success'UID="root" AUID="root"
type=USER_LOGIN msg=audit(1743448941.487:489): pid=4513 uid=0 auid=0 ses=9 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=0 e
e="/usr/sbin/sshd" hostname=? addr=192.168.50.20 terminal=/dev/pts/1 res=success'UID="root" AUID="root" ID="root"
type=USER_START msg=audit(1743448941.487:490): pid=4513 uid=0 auid=0 ses=9 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=0 e
e="/usr/sbin/sshd" hostname=? addr=192.168.50.20 terminal=/dev/pts/1 res=success'UID="root" AUID="root" ID="root"
type=CRYPTO_KEY_USER msg=audit(1743448941.491:491): pid=4513 uid=0 auid=0 ses=9 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy
kind=server fp=SHA256:57:f6:47:e4:37:42:6e:d9:60:66:ea:f5:55:d0:65:f0:ca:1b:a7:d3:8f:8c:2c:5a:9b:d8:a6:fc:90:63:37:2b direction=? spid=4537
uid=0  exe="/usr/sbin/sshd" hostname=? addr=? terminal=? res=success'UID="root" AUID="root" SUID="root"
type=BPF msg=audit(1743448941.546:492): prog-id=59 op=LOAD
type=BPF msg=audit(1743448941.547:493): prog-id=60 op=LOAD
type=SERVICE_START msg=audit(1743448941.864:494): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=syste
md-hostnamed comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1743448971.908:495): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=syste
d-hostnamed comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=BPF msg=audit(1743448971.992:496): prog-id=60 op=UNLOAD
type=BPF msg=audit(1743448971.992:497): prog-id=59 op=UNLOAD
type=USER_END msg=audit(1743448998.557:498): pid=4513 uid=0 auid=0 ses=9 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=0 exe
"/usr/sbin/sshd" hostname=? addr=? terminal=/dev/pts/1 res=success'UID="root" AUID="root" ID="root"
type=USER_LOGOUT msg=audit(1743448998.557:499): pid=4513 uid=0 auid=0 ses=9 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=0
xe="/usr/sbin/sshd" hostname=? addr=? terminal=/dev/pts/1 res=success'UID="root" AUID="root" ID="root"
type=CRYPTO_KEY_USER msg=audit(1743448998.560:500): pid=4513 uid=0 auid=0 ses=9 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy
```

8. Which log message indicates a successful login by the root user?

```
type=USER_LOGIN msg=audit(1743449016.491:531): pid=4566 uid=0 auid=0 ses=11 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=0 e
xe="/usr/sbin/sshd" hostname=? addr=192.168.50.20 terminal=/dev/pts/1 res=success'UID="root" AUID="root" ID="root"
type=USER_START msg=audit(1743449016.491:532): pid=4566 uid=0 auid=0 ses=11 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=0 e
xe="/usr/sbin/sshd" hostname=? addr=192.168.50.20 terminal=/dev/pts/1 res=success'UID="root" AUID="root" ID="root"
```

9. Stop the **tail** command on the **AlmaLinux** server by pressing **Ctrl+C.**

```
[root@server12 ssh]#
```

10. . Return to **Ubuntu** and disconnect the root session from the SSH server.

```
[root@server12 ~]# exit
logout
Connection to 192.168.50.10 closed.
root@client12:~#
```

X11 FORWARDING

Exercise 1.5: Tasks to Perform on Ubuntu:

1. From Ubuntu, start an SSH session with X11 forwarding enabled:

```
  GNU nano 5.6.1                        ssh_config
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

# Host *
#   ForwardAgent no
   ForwardX11 yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
```

```
[root@server12 ssh]# systemctl restart sshd
[root@server12 ssh]#
```

```
lmohammed@client12:~$ ssh -X lmohammed@192.168.50.10
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Mar 31 16:53:12 2025 from 192.168.50.20
```

2. Once connected, type the following command to launch Firefox: **firefox &**

```
[lmohammed@server12 ~]$ firefox&
[1] 3148
[lmohammed@server12 ~]$
```

3. If the **Firefox** browser opens and displays the AlmaLinux website, **X11 forwarding** is working correctly.

4. Go back to the AlmaLinux server and verify if the **firefox process** is running.

```
[root@server12 ssh]# ps -a | grep firefox
   3148 pts/2    00:00:15 firefox
[root@server12 ssh]#
```

5. Return to **Ubuntu** and close the **Firefox** application.

6. Log out of the ssh session.

```
[lmohammed@server12 ~]$ exit
logout
Connection to 192.168.50.10 closed.
[lmohammed@server12 ~]$
```