

**Please complete all quizzes, guided exercises, and labs for each chapter. Insert YES for each completed quiz and your screenshots in appropriate locations for each guided exercise/lab**

## **Guided Exercise: Access the Remote Command Line**

In this exercise, you log in to a remote system as different users and execute commands.

### **Outcomes**

- Log in to a remote system.
- Execute commands with the OpenSSH secure shell.

As the `student` user on the `workstation` machine, use the `lab` command to prepare your system for this exercise.

This command prepares your environment and ensures that all required resources are available.

```
[student@workstation ~]$ lab start ssh-access
```



### Procedure 10.1. Instructions

1. From workstation, open an SSH session to the servera machine as the student user.

```
[student@workstation ~]$ ssh student@servera
[student@servera ~]$
```



SSH connection from the `servera` machine. If the `/home/student/.ssh/known_hosts` file does not exist, then it is created along with the new entry in it. The `ssh` command fails to execute properly if the remote host appears to have a different key from the recorded key.



```

[student@workstation ~]$ lab start ssh-access
Starting lab.
- Checking lab systems ..... SUCCESS
- Ensure the openssh-clients package is installed ..... SUCCESS
- Ensure the known hosts file does not exist ..... SUCCESS
- Backing up the /etc/ssh/sshd_config file on serverb ..... SUCCESS
- Permitting root login over SSH using password on serverb ..... SUCCESS

[student@workstation ~]$ ssh student@servera
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:51:26 2022 from 172.25.250.9
[student@servera ~]$ ssh student@serverb
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is SHA256:peU0gfxFNw0Jt0Wk4CB2rs+jq1I/LhA32MI+8zBawLi.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:53:44 2022 from 172.25.250.9
[student@serverb ~]$

```

3. Display the users that are currently logged in to the `serverb` machine. The `student` user is logged in to the system from the host with an IP address of `172.25.250.10`, which is the `servera` machine in the classroom network.

```

[student@serverb ~]$ w --from
03:39:04 up 16 min,  1 user,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@      IDLE        JCPU      PCPU      WHAT
student   pts/0    172.25.250.10  20:40      1.00s      0.01s     0.00s    w --
from

```

```

[student@workstation ~]$ lab start ssh-access
Starting lab.
- Checking lab systems ..... SUCCESS
- Ensure the openssh-clients package is installed ..... SUCCESS
- Ensure the known hosts file does not exist ..... SUCCESS
- Backing up the /etc/ssh/sshd_config file on serverb ..... SUCCESS
- Permitting root login over SSH using password on serverb ..... SUCCESS

[student@workstation ~]$ ssh student@servera
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:51:26 2022 from 172.25.250.9
[student@servera ~]$ ssh student@serverb
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is SHA256:peU6gfxFNw6Jt6W4CB2rs+jqll/LhA32M1+8z8awLI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:53:44 2022 from 172.25.250.9
[student@serverb ~]$ w --from
 22:00:45 up 3 min, 1 user, load average: 0.01, 0.02, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
student  pts/0    172.25.250.10 22:00   1.00s  0.01%  0.00% w --from
[student@serverb ~]$

```

- Exit the student user's shell on the serverb machine.

```

[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$

```

```

Red Hat
Activities Terminal Dec 10 22:01

student@servera:~
Starting lab.
- Checking lab system ..... SUCCESS
- Ensure the openssh-clients package is installed ..... SUCCESS
- Ensure the known hosts file does not exist ..... SUCCESS
- Backing up the /etc/ssh/sshd_config file on serverb ..... SUCCESS
- Permitting root login over SSH using password on serverb ..... SUCCESS

[student@workstation ~]$ ssh student@servera
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:51:28 2022 from 172.25.250.9
[student@servera ~]$ ssh student@serverb
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is SHA256:peU6gFxFhw6Jt6Wk4CB2rs+jq11/LhA32M1+8zHawLI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:53:44 2022 from 172.25.250.9
[student@serverb ~]$ w --from
 22:00:45 up 3 min, 1 user, load average: 0.01, 0.02, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
student  pts/0    172.25.250.10  22:00   1.00s  0.01s  0.00s  w --from
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$

```

- Open an SSH session to the `serverb` machine as the `root` user. Use `redhat` as the password of the `root` user. The command did not ask you to accept the host key, because it was found among the known hosts. If the identity of the `serverb` machine changes, then OpenSSH prompts you to challenge the new host key.

```

[student@servera ~]$ ssh root@serverb
root@serverb's password: redhat
...output omitted...
[root@serverb ~]#

```

```

Red Hat
Activities Terminal Dec 10 22:01

root@serverb:~# Permitting root login over SSH using password on serverb ..... SUCCESS

[student@workstation ~]$ ssh student@servera
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:51:26 2022 from 172.25.256.9
[student@servera ~]$ ssh student@serverb
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is SHA256:peU0gfxFhw6Jt6Wk4CB2rs+Jqll/LhA32MI+RzBawLI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:53:44 2022 from 172.25.250.9
[student@serverb ~]$ w --from
22:00:45 up 3 min, 1 user, load average: 0.01, 0.02, 0.00
USER      TTY      FROM          LOGIN@      IDLE        JCPU        PCPU WHAT
student pts/0    172.25.250.10 22:00      1.00s      0.01s      0.00s w --from
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$ ssh root@serverb
root@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:28:26 2022
[root@serverb ~]#

```

- Run the `w` command to display the users that are currently logged in to the `serverb` machine. The output indicates that the `root` user is logged in to the system from the host with an IP address of `172.25.250.10`, which is the `servera` machine in the classroom network.

```

[root@serverb ~]# w --from
03:46:05 up 23 min, 1 user, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@      IDLE        JCPU        PCPU WHAT
root      pts/0    172.25.250.10 20:44      1.00s      0.02s      0.00s w --from

```

The screenshot shows a Red Hat desktop environment with a terminal window open. The terminal displays the following sequence of commands and outputs:

```

root@serverb:~# insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:51:26 2022 from 172.25.250.9
[student@servera ~]$ ssh student@serverb
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is SHA256:peU0gfaFNw6J10Wk4CB2rs+jq1i/LhA32M1+8z8awLI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:53:44 2022 from 172.25.250.9
[student@serverb ~]$ w --from
 22:00:43 up 3 min,  1 user,  load average: 0.01, 0.02, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT
student pts/0    172.25.250.10 22:00   1.00s  0.01s  0.00s w --from
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$ ssh root@serverb
root@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:28:26 2022
[root@serverb ~]# w --from
 22:01:43 up 4 min,  1 user,  load average: 0.00, 0.01, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT
root     pts/0    172.25.250.10 22:01   1.00s  0.00s  0.00s w --from
[root@serverb ~]#

```

7. Exit the root user's shell on the serverb machine.

```

[root@serverb ~]# exit
logout
Connection to serverb closed.
[student@servera ~]$

```

```

Red Hat
Activities Terminal Dec 10 22:02

student@servera--
Last login: Sat Dec 10 21:51:26 2022 from 172.25.250.9
[student@servera ~]$ ssh student@serverb
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is SHA256:peU0gfxFNw6Jf6Wk4CB2rs+jq1l/LhA32M)+8zBawL1.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:53:44 2022 from 172.25.250.9
[student@serverb ~]$ w --from
 22:00:45 up 3 min,  1 user,  load average: 0.01, 0.02, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT
student pts/0    172.25.250.10  22:00   1.00s  0.01s  0.00s w --from
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$ ssh root@serverb
root@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:28:26 2022
[root@serverb ~]# w --from
 22:01:43 up 4 min,  1 user,  load average: 0.00, 0.01, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT
root     pts/0    172.25.250.10  22:01   1.00s  0.00s  0.00s w --from
[root@serverb ~]# exit
logout
Connection to serverb closed.
[student@servera ~]$

```

8. Remove the `/home/student/.ssh/known_hosts` file from the `servera` machine. This operation causes `ssh` to lose the recorded identities of the remote systems.

```
[student@servera ~]$ rm /home/student/.ssh/known_hosts
```

Host keys can change for legitimate reasons: perhaps the remote machine was replaced because of a hardware failure, or the remote machine was reinstalled. Usually, it is advisable to remove the key entry only for the particular host in the `known_hosts` file. Because this particular `known_hosts` file has only one entry, you can remove the entire file.

```

[student@servera ~]$ ssh student@serverb
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is SHA256:peU0gFsFNw6Jt6WK4CB2rs+jql1/LHA32MI+8zBawLI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:53:44 2022 from 172.25.250.9
[student@serverb ~]$ w --from
 22:00:45 up 3 min, 1 user, load average: 0.01, 0.02, 0.00
USER      TTY      FROM          LOGINS  IDLE  JCPU  PCPU  WHAT
student pts/0    172.25.250.10  22:00   1.00s  0.01s  0.00s w --from
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$ ssh root@serverb
root@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:28:26 2022
[root@serverb ~]# w --from
 22:01:43 up 4 min, 1 user, load average: 0.00, 0.01, 0.00
USER      TTY      FROM          LOGINS  IDLE  JCPU  PCPU  WHAT
root     pts/0    172.25.250.10  22:01   1.00s  0.00s  0.00s w --from
[root@serverb ~]# exit
logout
Connection to serverb closed.
[student@servera ~]$ rm /home/student/.ssh/known_hosts
[student@servera ~]$

```

- Open an SSH session to the `serverb` machine as the `student` user. If asked, accept the host key. Use `student` when prompted for the password of the `student` user on the `serverb` machine.

```

[student@servera ~]$ ssh student@serverb
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is
SHA256:h/hEJa/anxp6AP7BmB5azIPVbPNqieh0oKi4KWOTK80.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password: student
...output omitted...
[student@serverb ~]$

```

The `ssh` command asked for your confirmation to accept or reject the host key because it could not find one for the remote host.

```

Red Hat
Activities Terminal Dec 10 22:03

student@serverb:~$ w --from
22:00:45 up 3 min, 1 user, load average: 0.01, 0.02, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
student  pts/0    172.25.250.10  22:00    1.00s  0.01s  0.00s  w --from
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$ ssh root@serverb
root@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:28:26 2022
[root@serverb ~]# w --from
22:01:43 up 4 min, 1 user, load average: 0.00, 0.01, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
root      pts/0    172.25.250.10  22:01    1.00s  0.00s  0.00s  w --from
[root@serverb ~]# exit
logout
Connection to serverb closed.
[student@servera ~]$ rm /home/student/.ssh/known_hosts
[student@servera ~]$ ssh student@serverb
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is SHA256:peUGgfXfNm6Jf6Wk4CBZra+jqll/LhA32M1+8z8awLI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 22:00:26 2022 from 172.25.250.10
[student@serverb ~]$

```

10. Exit the student user's shell on the serverb machine and confirm that a new instance of `known_hosts` exists on the servera machine.

```

[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$ ls -l /home/student/.ssh/known_hosts
-rw----- . 1 student student 819 Mar 24 03:47
/home/student/.ssh/known_hosts

```

```

Red Hat
Activities Terminal Dec 10 22:03

student@servera:~
logout
Connection to serverb closed.
[student@servera ~]$ ssh root@serverb
root@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 21:28:26 2022
[root@serverb ~]# w --from
 22:01:43 up 4 min, 1 user, load average: 0.00, 0.01, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
root     pts/0    172.25.250.10 22:01   1.00s  0.00s  0.00s w --from
[root@serverb ~]# exit
logout
Connection to serverb closed.
[student@servera ~]$ rm /home/student/.ssh/known_hosts
[student@servera ~]$ ssh student@serverb
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519-key fingerprint is SHA256:peUGgFxFhw6Jt6Wk4CB2rs+jqli/LhA32MI+8zBawLI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 22:00:26 2022 from 172.25.250.10
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$ ls -l /home/student/.ssh/known_hosts
-rw-r----- 1 student student 819 Dec 10 22:03 /home/student/.ssh/known_hosts
[student@servera ~]$

```

11. Confirm that the new instance of the `known_hosts` file has the host key of the `serverb` machine. The following command output is an example; the actual output on your workstation might be different.

```

[student@servera ~]$ cat /home/student/.ssh/known_hosts
...output omitted...
serverb ecdsa-sha2-nistp256 AAAAB3NzaC1yc2EAAAADAQ...
...output omitted...

```

```

Red Hat
Activities Terminal Dec 10 22:04

student@servera:~
logout
Connection to serverb closed.
[student@servera ~]$ rm /home/student/.ssh/known_hosts
[student@servera ~]$ ssh student@serverb
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is SHA256:peUGgfxFNw6Jt8M4CB2rs+jq1l/LhA32MI+BzBawLI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 22:00:20 2022 from 172.25.250.10
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$ ls -l /home/student/.ssh/known_hosts
-rw-r-----. 1 student student 819 Dec 10 22:03 /home/student/.ssh/known_hosts
[student@servera ~]$ cat /home/student/.ssh/known_hosts
serverb ssh-ed25519 AAAAC3NzaC1lZDIIINTES4AAAAI0wllK0PExRns51g70TxsM0mgHud5GQ0uXhH
u0Gcv19uT
serverb ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC8MD00oY+rh6MPa9yhLsNQXBqcQknTL/W
Sd3zPvHLLd7KaC4IIEUxnpbflB1t8tRcirbQFxD20Am+6WJ2kpo34ZnIQYJz3AuLZjuvat7x9DxzQ2d
u5w50bLqtqteHt13v57RPUZlSn6QKuPrkclRwYZDQveC1iefy8Nysk}JYFXu7Csd3IA2EatCha18AUok
BF2XOC7R9wSb3D1sd1JvaavQ107YFLzDHppRncKI51PwbyICaCVq7Kv4LdrcwQfsAyobPizWgp7u3U1
/Narxk7ev58tmbE13nxdC6Fiec682qhbWnF1862kV9p+YMW0E}LEY1MRRJGJ20dAyfie72dp0uze+
LHG88NfoBj3n3Plxw+AvH9eeboJEu+h7KfqwLXrZzr5o7pdFBpM3f7+dEG9uwwaeznUc7N9KFXh+keV
xBJZk4PuySu2Ytqv9Fm4WVpvnX5uav9lfevt2Fe2XFj9RcVqTrUFJ7Zz/87V2JCa5ILGNbzR9z9mhc
HRMtxc=
serverb ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdzdhYnTYAAAAIbnIzdHAyNTYAAAB
BBCSBA5ZVCNeIbyG2JlhzCLq3RVW0oshNCBEG10+5ywTj/127A55gu0Z6LzyM0K1J4woTWHS4RfZz
vycnCBvt0=
[student@servera ~]$

```

- Run the `hostname` command remotely on the `serverb` machine without accessing the interactive shell.

```

[student@servera ~]$ ssh student@serverb hostname
student@serverb's password: student
serverb.lab.example.com

```

```

Red Hat
Activities Terminal Dec 10 22:05

student@servera:~$ ssh student@serverb
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is SHA256:peU0GtXFNw6J10Wk4C82rs+jql1/LhA32PI+RzBawLI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 22:00:26 2022 from 172.25.250.10
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$ ls -l /home/student/.ssh/known_hosts
-rw-r-----. 1 student student 819 Dec 10 22:03 /home/student/.ssh/known_hosts
[student@servera ~]$ cat /home/student/.ssh/known_hosts
serverb ssh-ed25519 AAAAC3NzaC1lZDI1MTE5AAAAI0eILKMEXRns51g70TxMs0mgHud5GQBzXrh
W0Gv19uT
serverb ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQC8W00ooY+rh6NPa9yHLSNQXBqcQknTL/W
Sd3zPvHLld7KqC4I1EUxnbFLB1t8tRc1rBQFxD20Am+6wJ2kpo34ZnIQYJz3AuIzjuvat7x9DxzQ2d
u5wS0bltqteM13v57RPUZ15n60XufRkCLrWYZDQveC11efyBhysk3YPPXu7Csd31A2EatCha18A0ok
0f2XQC7R9v5b5D1md13vaavQ107YF1zDhppRncw151PwbyICaCVq7Kv4Ldrcw0fsAye0PizWgp7u3U1
/Marxk7ev58tBmI3nznC8F1ec60zqhbwrnFI062kv9p+YMH0ExjLEYIwRRJGJ26dAylfieF2dp0uze+
LHG88Nfo0j3a3PLxw+AvH9eeboJEu+h7KfgwLXr2zr5s7pdFBpM3f7+dEG9uWaeznUc7N9KFXh+keV
xB2K4PUySu2Ytqv9Fm4WVpvnvX5mav9lfevtZFe2XFj9RcVqTrUFJ7Zz/87V23Ca5ILGmbzR9z9whc
H0Mtzc=
serverb ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlkbW1zdBHAYNTYAAAAIbElzdBHAYNTYAAAB
BRC5BA5ZYCneibYgGZJlh2CLq3RvNdXshNCBEG10+5ywTj/127A55gu0ZGLzyM0K1J4woTWHS4RfZz
vycsCBvto=
[student@servera ~]$ ssh student@serverb hostname
student@serverb's password:
serverb.lab.example.com
[student@servera ~]$

```

13. Return to the workstation system as the student user.

```

[student@servera ~]$ exit
logout
Connection to servera closed.

```



```

Red Hat
Activities Terminal Dec 10 22:05

student@workstation:~$ ssh student@serverb
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'serverb' (ED25519) to the list of known hosts.
student@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 22:00:26 2022 from 172.25.258.10
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$ ls -l /home/student/.ssh/known_hosts
-rw-r----- 1 student student 819 Dec 10 22:01 /home/student/.ssh/known_hosts
[student@servera ~]$ cat /home/student/.ssh/known_hosts
serverb ssh-ed25519 AAAAC3NzaC1lZDI1IbnTE3AAAAIOmllKMEXRns51g70TxFs0egInu500BUxHh
uU6cy19uT
serverb ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC8wD0ooY+rh6NPa9yhLsN0XBqcQknTL/W
5d3zPvMLLd7KaC4I1EUamwDfLB1tBTRc1rb0Fxo28Ae+6wJ2kpo34Znl0YJz3Au1Zjuvat7x9DxzQ2d
u5w5UBltqteMtL3v57RPuZl5nG0KuPrkclrWYZDQveC1lefyBhyskjJYPXu7Csd3IA2EntcNa18AUoK
8f2XQC7R9w5b50md13vaav0107YFlz0HppRncwI51PwbyICaCVq7Kv4LdrcmQfsAyobPizWgp7u3U1
/Narxk7ev58tmBnI3nxc6F1ec60zqbWrrnFI862kv9p+YMH0ExjLEY1WRRJ6J26dAylf2dp6uza+
LH088Nfo0j3m3Plxw+AvM9eebo3Eu+h7KfigW1Xr2z+5s7pdFBpH3f7+dE09uWaeznUc7N0XFXh+keV
xBJZK4F0y5u2Ytqv9F+4WVpnhvXSmaV9lfevtZFe2XFj9RcVqTrUFJ7Zz/B7VZJCa51L0NbzR9z9mhc
HRMtzc=
serverb ecdsa-sha2-nistp256 AAAAE2VjZHRhLXNoYTIibElzdHMyNTYAAAAIbElzdHMyNTYAAAB
BBC58A3ZvCNe15Yg02JlhZCLq3RVmDxxhNCBE610+5ywTj/127A55Gu820LzyPp6X134woThS4R7Zz
yycCBvt0=
[student@servera ~]$ ssh student@serverb hostname
student@serverb's password:
serverb.lab.example.com
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$

```

## Finish

On the workstation machine, change to the `student` user home directory and use the `lab` command to complete this exercise. This step is important to ensure that resources from previous exercises do not impact upcoming exercises.

```
[student@workstation ~]$ lab finish ssh-access
```

This concludes the section.

The screenshot shows a Red Hat terminal window with the following content:

```

student@workstation:~
Last login: Sat Dec 10 22:00:26 2022 from 172.25.256.10
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@servera ~]$ ls -l /home/student/.ssh/known_hosts
-rw----- 1 student student 819 Dec 10 22:03 /home/student/.ssh/known_hosts
[student@servera ~]$ cat /home/student/.ssh/known_hosts
serverb ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI0mLLKMEXRnsS1g70TxMs0mgHuU5G0BUxHh
uRGcv19uT
serverb ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCiBwD0ooY+rh6MPa9yHlUNQXBqc0knTL/W
5d3zPvHLd7KaC4IiE0xnbFLB11BTRc1rb0FxD20Ae+0WJ2Apo34Znl0YJz3AuLZjuva17x90xz02d
uSvSubLtqteMt13vS7RPuZ1SnGQKuPrkclrMYZDQveC11efyBhyskjJYPXu7Csd31A2EntcNa18AlJk
0f2X0C7R9v5b501ad1Jvaav0107YFLzDhppRncwI51PwbyICaCVq7Kv4Ldrc0f3AyobP1zWpp7u3U1
/Narxk7ev58tmbaI3nxc6Fjecd0zqhbWrfI062kv9p+YmQExjLEY1MMR36J26dAylief2dofuza+
LHG8BNf0j3m3Plxw+AvM9eeboJEu+h7KfgwLXr2zr5s7pdfBpM3f7+dEG9uWaeznuc7N9XFxh+keV
xBJ2K4P0y5u2Y1qv9Fm4WvnpvXSmav9lfvztZFe2XFj9RcVqTrUFJ7Zz/87V2JCe5ILGNbzR9z9mhc
HRHtXc=
serverb ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTU1bmlzdzRhaWNTYAAAAIbmlzdzRhaWNTYAAAB
BBC5BA5ZVCNe1bYg62JlhzCLq3RVhdXehNCBE010+5ywTj/127A55gu8ZGLzyMp6K134woTher54RfZz
vycmC8vto=
[student@servera ~]$ ssh student@serverb hostname
student@serverb's password:
serverb.lab.example.com
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$ Lab finish ssh-access

Finishing lab.

- Checking lab systems ..... SUCCESS
- Restoring original /etc/ssh/sshd_config on serverb ..... SUCCESS
- Remove the known hosts file on servera ..... SUCCESS

[student@workstation ~]$

```

## Guided Exercise: Configure SSH Key-based Authentication

In this exercise, you configure a user to use key-based authentication for SSH.

### Outcomes

- Generate an SSH key pair without passphrase protection.
- Generate an SSH key pair with passphrase protection.
- Authenticate with both passphrase-less and passphrase-protected SSH keys.

As the `student` user on the `workstation` machine, use the `lab` command to prepare your system for this exercise.

This command prepares your environment and ensures that all required resources are available.

```
[student@workstation ~]$ lab start ssh-configure
```



### Procedure 10.2. Instructions

## Chapter 10

1. Log in to the `serverb` machine as the `student` user.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$
```



2. Switch to the `operator1` user on the `serverb` machine. Use `redhat` as the password.

```
[student@serverb ~]$ su - operator1
Password: redhat
[operator1@serverb ~]$
```



3. Generate a set of SSH keys. Do not enter a passphrase.

```

[operator1@serverb ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/operator1/.ssh/id_rsa):
Enter
Created directory '/home/operator1/.ssh'.
Enter passphrase (empty for no passphrase): Enter
Enter same passphrase again: Enter
Your identification has been saved in /home/operator1/.ssh/id_rsa.
Your public key has been saved in /home/operator1/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:JainiQdnRosC+xXh operator1@serverb.lab.example.com
The key's randomart image is:
+---[RSA 3072]-----+
|E+*+ooo .          |
|. = o.o o .        |
|o.. = . . o        |
|+. + * . o .       |
|+ = X . S +        |
| + @ + = .         |
|. + = o            |

```

```
|.o . . . . |
|o   o..   |
+----[SHA256]-----+
```



4. Send the public key of the SSH key pair to the operator1 user on the servera machine, with redhat as the password.

```
[operator1@serverb ~]$ ssh-copy-id operator1@servera
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/home/operator1/.ssh/id_rsa.pub"
The authenticity of host 'servera (172.25.250.10)' can't be
established.
ED25519 key fingerprint is
SHA256:h/hEJa/anxp6AP7BmB5azIPVbPNqieh0oKi4KWOTK80.
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
operator1@servera's password: redhat
```

Number of key(s) added: 1

Now try logging into the machine, with: `"ssh 'operator1@servera'"` and check to make sure that only the key(s) you wanted were added.

5. Execute the `hostname` command on the `servera` machine remotely by using the `ssh` command without accessing the remote interactive shell.

```
[operator1@serverb ~]$ ssh operator1@servera hostname
servera.lab.example.com
```

The preceding `ssh` command does not prompt you for a password because it uses the passphrase-less private key against the exported public key to authenticate as the `operator1` user on the `servera` machine. This approach is not secure because anyone who has access to the private key file can log in to the `servera` machine as the `operator1` user. The secure alternative is to protect the private key with a passphrase, which is a following step.

```

Red Hat
Activities Terminal Dec 10 22:10

operator1@serverb:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/operator1/.ssh/id_rsa): Enter
Enter already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in Enter
Your public key has been saved in Enter.pub
The key fingerprint is:
SHA256:jkKV2LIRDwFDRYGXekkdVPBY5qF1z0gjiy6Vgrhmr3U operator1@serverb.lab.example.com
The key's randomart image is:
+---[RSA 3072]---+
 | .oB*o=ooo     |
 | .+..+..+     |
 | o o B o + + . |
 | + + + S + .   |
 | = . . . +     |
 | oo . E . . .  |
 | 0.0 . . .     |
 | . . .         |
+----[SHA256]-----+
operator1@serverb ~$ ssh-copy-id operator1@servera
/usr/bin/ssh-copy-id: ERROR: No identities found
operator1@serverb ~$ ssh operator1@servera hostname
The authenticity of host 'servera (172.25.250.10)' can't be established.
ED25519 key fingerprint is SHA256:peUGgfxFNw6Jt6MK4CB2rs+jq1l/LhA32M1+BzBawLI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'servera' (ED25519) to the list of known hosts.
operator1@servera's password:
servera.lab.example.com
operator1@serverb ~$

```

6. Generate another set of SSH keys with the default name and without a passphrase, overwriting the previously generated SSH key files. Try to connect to the `servera` machine by using the new SSH keys. The `ssh` command asks for a password, because it cannot authenticate with the SSH key. Run again the `ssh` command with the `-v` (verbose) option to verify it.

Send the new public key of the SSH key pair to the `operator1` user on the `servera` machine, to replace the previous public key. Use `redhat` as the password for the `operator1` user on the `servera` machine. Execute the `hostname` command on the `servera` machine remotely by using the `ssh` command without accessing the remote interactive shell to verify that it works again.

1. Again generate another set of SSH keys with the default name and without a passphrase, overwriting the previously generated SSH key files.

```
[operator1@serverb ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key
(/home/operator1/.ssh/id_rsa): Enter
/home/operator1/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): Enter
Enter same passphrase again: Enter
Your identification has been saved in /home/operator1/.ssh/id_rsa
Your public key has been saved in /home/operator1/.ssh/id_rsa.pub
...output omitted...
```

2. Try to connect to the `servera` machine by using the new SSH keys. The `ssh` command asks for a password, because it cannot authenticate with the SSH key. Press **Ctrl+c** to exit from the `ssh` command when it prompts for a password. Run again the `ssh` command with the `-v` (verbose) option to verify it. Press again **Ctrl+c** to exit from the `ssh` command when it prompts for a password.

```
[operator1@serverb ~]$ ssh operator1@servera hostname
operator1@servera's password: ^C
[operator1@serverb ~]$ ssh -v operator1@servera hostname
OpenSSH_8.7p1, OpenSSL 3.0.1 14 Dec 2021
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Reading configuration data /etc/ssh/ssh_config.d/01-
training.conf
...output omitted...
debug1: Next authentication method: publickey
debug1: Offering public key: /home/operator1/.ssh/id_rsa RSA
SHA256:ad597Zf64xckV26xht8bjQbzqSPuOXQPXksGEWVsP80
debug1: Authentications that can continue: publickey,gssapi-
keyex,gssapi-with-mic,password
debug1: Trying private key: /home/operator1/.ssh/id_dsa
debug1: Trying private key: /home/operator1/.ssh/id_ecdsa
debug1: Trying private key: /home/operator1/.ssh/id_ecdsa_sk
debug1: Trying private key: /home/operator1/.ssh/id_ed25519
debug1: Trying private key: /home/operator1/.ssh/id_ed25519_sk
```

```

debug1: Trying private key: /home/operator1/.ssh/id_xmss
debug1: Next authentication method: password
operator1@servera's password: ^C

```



- Send the new public key of the SSH key pair to the `operator1` user on the `servera` machine, to replace the previous public key. Use `redhat` as the password for the `operator1` user on the `servera` machine. Execute the `hostname` command on the `servera` machine remotely by using the `ssh` command without accessing the remote interactive shell to verify that it works again.

```

[operator1@serverb ~]$ ssh-copy-id operator1@servera
...output omitted...
operator1@servera's password: redhat

```

```
Number of key(s) added: 1
```

Now try logging into the machine, with: `"ssh 'operator1@servera'"` and check to make sure that only the key(s) you wanted were added.

```

[operator1@serverb ~]$ ssh operator1@servera hostname
servera.lab.example.com

```

7. Generate another set of SSH keys with passphrase-protection. Save the key as `/home/operator1/.ssh/key2`. Use `redhatpass` as the passphrase of the private key.

```
[operator1@serverb ~]$ ssh-keygen -f .ssh/key2
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase): redhatpass
Enter same passphrase again: redhatpass
Your identification has been saved in .ssh/key2.
Your public key has been saved in .ssh/key2.pub.
The key fingerprint is:
SHA256:OCtCjfPm5QrbPBgqb operator1@serverb.lab.example.com
The key's randomart image is:
+----[RSA 3072]-----+
|O=X*                |
|OB=.                |
|E*o.                |
|Booo .              |
|..= . o S           |
|+.o o               |
|+.oo+ o             |
|+o.O.+              |
|+ . =o.             |
+-----[SHA256]-----+
```



- Send the public key of the passphrase-protected key pair to the `operator1` user on the `servera` machine. The command does not prompt you for a password because it uses the public key of the passphrase-less private key that you exported to the `servera` machine in the preceding step.

```
[operator1@serverb ~]$ ssh-copy-id -i .ssh/key2.pub operator1@servera
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
".ssh/key2.pub"
/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
```

Number of key(s) added: 1

Now try logging into the machine, with: `"ssh 'operator1@servera'"`  
and check to make sure that only the key(s) you wanted were added.

The screenshot shows a terminal window on a Red Hat system. The user is in the `operator1@serverb` shell. They run `ssh-keygen -f .ssh/key2` to generate a new RSA key pair. The terminal shows the prompts for a passphrase and confirmation, followed by the key fingerprint: `SHA256:9JY4Nd0KrkJguu3Tu0eJLVFFJv001pq7wFlrbrZ2d8Y operator1@serverb.lab.example.com`. A randomart image is displayed for the key. Then, the user runs `ssh-copy-id -i .ssh/key2.pub operator1@servera`. The terminal shows the progress of copying the key to the remote server, including the message: `operator1@servera's password:`. Finally, the user runs `ssh 'operator1@servera'` to test the connection, and the terminal shows the prompt `operator1@servera:~$`.

- Execute the `hostname` command on the `servera` machine remotely by using the `ssh` command. Use the `/home/operator1/.ssh/key2` key as the identity file. Specify `redhatpass` as the passphrase, which you set for the private key in the preceding step.

The command prompts you for the passphrase that you used to protect the private key of the SSH key pair. If an attacker gains access to the private key, then the attacker cannot use it to access other systems because a passphrase protects the private key itself. The `ssh` command uses a different passphrase from the `operator1` user on the `servera` machine, and so users must know both.

```
[operator1@serverb ~]$ ssh -i .ssh/key2 operator1@servera hostname
Enter passphrase for key '.ssh/key2': redhatpass
servera.lab.example.com
```

Use the `ssh-agent` program, as in the following step, to avoid interactively typing the passphrase while logging in with SSH. Using the `ssh-agent` program is both more convenient and more secure when the administrators log in to remote systems regularly.

```

operator1@serverb:~$ ssh-keygen
Enter same passphrase again:
Your identification has been saved in .ssh/key2
Your public key has been saved in .ssh/key2.pub
The key fingerprint is:
SHA256:9JY4nd0KraJguu3TuDeJLVFFJw001pg7WFLrbrZ2d8Y operator1@serverb.lab.example.com
The key's randomart image is:
+---[RSA 3072]-----+
|
|..+..+
|o o . . . o
|.oo. .+.o
|o+o .S+
|..oo .. o
|.o+o.o. E
|..o+*. o
|..o+*
+---[SHA256]-----+
[operator1@serverb ~]$ ssh-copy-id -i .ssh/key2.pub operator1@servera
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ".ssh/key2.pub"
/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 promp
ted now it is to install the new keys
operator1@servera's password:
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'operator1@servera'"
and check to make sure that only the key(s) you wanted were added.

[operator1@serverb ~]$ ssh -i .ssh/key2 operator1@servera hostname
Enter passphrase for key '.ssh/key2':
servera.lab.example.com
[operator1@serverb ~]$

```

10. Run the `ssh-agent` program in your Bash shell and add the passphrase-protected private key (`/home/operator1/.ssh/key2`) of the SSH key pair to the shell session.

The command starts the `ssh-agent` program and configures the shell session to use it. Then, you use the `ssh-add` command to provide the unlocked private key to the `ssh-agent` program.

```
[operator1@serverb ~]$ eval $(ssh-agent)
Agent pid 1729
[operator1@serverb ~]$ ssh-add .ssh/key2
Enter passphrase for .ssh/key2: redhatpass
Identity added: .ssh/key2 (operator1@serverb.lab.example.com)
```



11. Execute the `hostname` command on the `servera` machine remotely without accessing a remote interactive shell. Use the `/home/operator1/.ssh/key2` key as the identity file.

The command does not prompt you to enter the passphrase interactively.

```
[operator1@serverb ~]$ ssh -i .ssh/key2 operator1@servera hostname
servera.lab.example.com
```

The screenshot shows a terminal window on a Red Hat workstation. The terminal displays the output of the `ssh-copy-id` command, which copies a public key from the local machine to the remote server. The output shows the key's fingerprint (RSA 3072) and the SHA256 hash. The user is prompted for their password on the remote server, and the key is successfully added. The terminal also shows the user running `ssh-agent` and `ssh-add` to add the key to the local SSH agent.

```

operator1@serverb ~$ ssh-copy-id -i .ssh/key2.pub operator1@servera
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ".ssh/key2.pub"
/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 promp
ted now it is to install the new keys
operator1@servera's password:
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'operator1@servera'"
and check to make sure that only the key(s) you wanted were added.

operator1@serverb ~$ ssh -i .ssh/key2 operator1@servera hostname
Enter passphrase for key '.ssh/key2':
servera.lab.example.com
operator1@serverb ~$ eval $(ssh-agent)
Agent pid 1641
operator1@serverb ~$ ssh-add .ssh/key2
Enter passphrase for .ssh/key2:
Identity added: .ssh/key2 (operator1@serverb.lab.example.com)
operator1@serverb ~$ ssh -i .ssh/key2 operator1@servera hostname
servera.lab.example.com
operator1@serverb ~$

```

- Open another terminal on the workstation machine and log in to the `serverb` machine as the `student` user.

```

[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$

```



13. On the `serverb` machine, switch to the `operator1` user and remotely log in to the `servera` machine. Use the `/home/operator1/.ssh/key2` key as the identity file to authenticate using the SSH keys.
  1. Use the `su` command to switch to the `operator1` user. Use `redhat` as the password for the `operator1` user.

```
[student@serverb ~]$ su - operator1
Password: redhat
[operator1@serverb ~]$
```

2. Log in to the `servera` machine as the `operator1` user.

The command prompts you to enter the passphrase interactively because you do not invoke the SSH connection from the same shell where you started the `ssh-agent` program.

```
[operator1@serverb ~]$ ssh -i .ssh/key2 operator1@servera
Enter passphrase for key '.ssh/key2': redhatpass
...output omitted...
```

```
[operator1@servera ~]$
```

```

operator1@servera:~$ ssh student@serverb
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 22:00:43 2022 from 172.25.250.9
[student@serverb ~]$ su - operator1
Password:
su: Authentication failure
[student@serverb ~]$ su - operator1
Password:
Last login: Sat Dec 10 22:07:15 EST 2022 on pts/8
Last failed login: Sat Dec 10 22:17:37 EST 2022 on pts/1
There was 1 failed login attempt since the last successful login.
[operator1@serverb ~]$ ssh -i .ssh/key2 operator1@servera
Enter passphrase for key '.ssh/key2':
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[operator1@servera ~]$

```

14. Exit and close all extra terminals and return to the `workstation` machine.

1. Exit and close extra terminal windows. The `exit` commands leave the `operator1` user's shell; terminate the shell session where `ssh-agent` is active; and return to the `student` user's shell on the `serverb` machine.

```

[operator1@servera ~]$ exit
logout
Connection to servera closed.
[operator1@serverb ~]$

```

2. Return to the `workstation` system as the `student` user.

```

[operator1@serverb ~]$ exit
logout
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$

```

## Finish

On the `workstation` machine, change to the `student` user home directory and use the `lab` command to complete this exercise. This step is important to ensure that resources from previous exercises do not impact upcoming exercises.

```
[student@workstation ~]$ lab finish ssh-configure
```

This concludes the section.



```
Red Hat
Activities Terminal Dec 10 22:18

student@workstation:~
ted now it is to install the new keys
operator1@servera's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'operator1@servera'"
and check to make sure that only the key(s) you wanted were added.

[operator1@serverb ~]$ ssh -i .ssh/key2 operator1@servera hostname
Enter passphrase for key '.ssh/key2':
servera.lab.example.com
[operator1@serverb ~]$ eval $(ssh-agent)
Agent pid 1641
[operator1@serverb ~]$ ssh-add .ssh/key2
Enter passphrase for .ssh/key2:
Identity added: .ssh/key2 (operator1@serverb.lab.example.com)
[operator1@serverb ~]$ ssh -i .ssh/key2 operator1@servera hostname
servera.lab.example.com
[operator1@serverb ~]$ ssh student@serverexit
ssh: Could not resolve hostname serverexit: Name or service not known
[operator1@serverb ~]$ exit
logout
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$ lab finish ssh-configure
Script ssh-configure not in course library rhcsa-classroom
[student@workstation ~]$ lab finish ssh-configure

Finishing lab.

- Checking lab systems ..... SUCCESS
- Remove operator1 user ..... SUCCESS

[student@workstation ~]$
```

## Guided Exercise: Customize OpenSSH Service Configuration

In this exercise, you disable direct logins as `root` and disable password-based authentication for the OpenSSH service on one of your servers.

### Outcomes

- Disable direct logins as `root` over `ssh`.
- Disable password-based authentication for remote users to connect over SSH.

As the `student` user on the `workstation` machine, use the `lab` command to prepare your system for this exercise.

This command ensures that all required resources are available.

```
[student@workstation ~]$ lab start ssh-customize
```



```
student@workstation:~  
[student@workstation ~]$ lab start ssh-customize  
Starting lab.  
- Checking lab system ..... SUCCESS  
- Ensuring the required packages are installed ..... SUCCESS  
- Creating required user operator2 on servera ..... SUCCESS  
- Creating required user operator3 on servera ..... SUCCESS  
- Creating required user operator2 on serverb ..... SUCCESS  
- Creating required user operator3 on serverb ..... SUCCESS  
- Removing temporary files ..... SUCCESS  
- Backing up the /etc/ssh/sshd config file on servera ..... SUCCESS  
- Permitting SSH as root on servera ..... SUCCESS  
- Recording the md5sum of /etc/ssh/sshd_config on servera ..... SUCCESS  
[student@workstation ~]$
```

### Procedure 10.3. Instructions

1. From workstation, open an SSH session to the `serverb` machine as the `student` user.

```
[student@workstation ~]$ ssh student@serverb  
[student@serverb ~]$
```



2. Use the `su` command to switch to the `operator2` user on the `serverb` machine. Use `redhat` as the password for the `operator2` user.

```
[student@serverb ~]$ su - operator2  
Password: redhat  
[operator2@serverb ~]$
```



- Use the `ssh-keygen` command to generate SSH keys. Do not enter any passphrase for the keys.

```

[operator2@serverb ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/operator2/.ssh/id_rsa):
Enter
Created directory '/home/operator2/.ssh'.
Enter passphrase (empty for no passphrase): Enter
Enter same passphrase again: Enter
Your identification has been saved in /home/operator2/.ssh/id_rsa.
Your public key has been saved in /home/operator2/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:LN5xlirX0OWxgyd/qhATNgZWotLUj16EZkM1JHkCR+I
operator2@serverb.lab.example.com
The key's randomart image is:
+---[RSA 3072]-----+
|          *+=       |
|          = =0.o.   |
|          . Eo=B  o  |
|          o +.=o+  o  |
|          . S..= =   |
+---+

```

```

|      . o +. + . |
|      . o + . . . |
|      . o . o |
|      . . . |
+-----[SHA256]-----+

```



4. Use the `ssh-copy-id` command to send the public key of the SSH key pair to the `operator2` user on the `servera` machine. Use `redhat` as the password for the `operator2` user on `servera`.

```

[operator2@serverb ~]$ ssh-copy-id operator2@servera
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/home/operator2/.ssh/id_rsa.pub"
The authenticity of host 'servera (172.25.250.10)' can't be
established.
ED25519 key fingerprint is
SHA256:h/hEJa/anxp6AP7BmB5azIPVbPNqieh0oKi4KWOTK80.
Are you sure you want to continue connecting (yes/no)? 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

```

```
operator2@servera's password: redhat
Number of key(s) added: 1
Now try logging into the machine, with: "ssh 'operator2@servera'"
and check to make sure that only the key(s) you wanted were added.
```

5. Confirm that you can successfully log in to the servera machine as the operator2 user with the SSH keys.
  1. Open an SSH session to the servera machine as the operator2 user.

```
[operator2@serverb ~]$ ssh operator2@servera
...output omitted...
[operator2@servera ~]$
```

The preceding `ssh` command used SSH keys for authentication.

2. Log out of servera.

```
[operator2@servera ~]$ exit
logout
Connection to servera closed.
```

```

Red Hat
Activities Terminal Dec 10 22:22
operator2@serverb:~
.0. .-
...0
.0.0.+
+0+ +.
S= 0*o0o
.o.=+==.E
.000+ +.
. . =
.00=.o]
+----[SHA256]-----+
[operator2@serverb ~]$ ssh-copy-id operator2@servera
/usr/bin/ssh-copy-id: ERROR: No identities found
[operator2@serverb ~]$ ssh operator2@servera
The authenticity of host 'servera (172.25.250.10)' can't be established.
ED25519 key fingerprint is SHA256:peU6gFxFNw6Jt6WK4CB2rs+jqll/LhA32M1+8zBawLI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'servera' (ED25519) to the list of known hosts.
operator2@servera's password:
[operator2@serverb ~]$ exit
logout
[student@serverb ~]$ ssh operator2@serverb
operator2@serverb's password:
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 22:28:05 2022
[operator2@serverb ~]$ ssh operator2@servera
operator2@servera's password:
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[operator2@servera ~]$ exit
logout
Connection to servera closed.
[operator2@serverb ~]$
```

6. Confirm that you can successfully log in to the `servera` machine as the `root` user with `redhat` as the password.
  1. Open an SSH session to the `servera` machine as the `root` user with `redhat` as the password.

```
[operator2@serverb ~]$ ssh root@servera
root@servera's password: redhat
...output omitted...
[root@servera ~]#
```

The preceding `ssh` command used the password of the superuser for authentication because SSH keys do not exist for the superuser.

2. Log out of the `servera` machine.

```
[root@servera ~]# exit
logout
Connection to servera closed.
[operator2@serverb ~]$
```



The screenshot shows a terminal window titled "Red Hat" with a date and time of "Dec 10 22:22". The terminal content shows a series of SSH commands and their outputs:

```
operator2@serverb:~$ ssh-copy-id operator2@servera
/usr/bin/ssh-copy-id: ERROR: No identities found
[operator2@serverb ~]$ ssh operator2@servera
The authenticity of host 'servera (172.25.258.18)' can't be established.
ED25519 key fingerprint is SHA256:peUGgfxF9w6Jt6MK4CB2rs+jq1l/LhA32M1+BzBawLI.
This key is not known by any other names
Are you sure you want to continue connecting [yes/no/[fingerprint]]? yes
Warning: Permanently added 'servera' (ED25519) to the list of known hosts.
operator2@servera's password:
[operator2@serverb ~]$ exit
logout
[student@serverb ~]$ ssh operator2@serverb
operator2@serverb's password:
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 22:20:05 2022
[operator2@serverb ~]$ ssh operator2@servera
operator2@servera's password:
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[operator2@servera ~]$ exit
logout
Connection to servera closed.
[operator2@serverb ~]$ ssh root@servera
root@servera's password:
Activate the web console with: systemctl enable --now cockpit.socket
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[root@servera ~]# exit
logout
Connection to servera closed.
[operator2@serverb ~]$
```

7. Confirm that you can successfully log in to the `servera` machine as the `operator3` user with `redhat` as the password.
  1. Open an SSH session to the `servera` machine as the `operator3` user with `redhat` as the password.

```
[operator2@serverb ~]$ ssh operator3@servera
operator3@servera's password: redhat
...output omitted...
[operator3@servera ~]$
```

The preceding `ssh` command used the password of the `operator3` user for authentication because SSH keys do not exist for the `operator3` user.

2. Log out of the `servera` machine.

```
[operator3@servera ~]$ exit
logout
Connection to servera closed.
[operator2@serverb ~]$
```



The screenshot shows a terminal window titled "operator2@serverb" with a Red Hat logo in the top left. The terminal output shows the following sequence of commands and responses:

```
Are you sure you want to continue connecting [yes/no/[fingerprint]]? yes
Warning: Permanently added 'servera' (ED25519) to the list of known hosts.
operator2@servera's password:
[operator2@serverb ~]$ exit
logout
[student@serverb ~]$ ssh operator2@serverb
operator2@serverb's password:
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 22:20:05 2022
[operator2@serverb ~]$ ssh operator2@servera
operator2@servera's password:
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[operator2@servera ~]$ exit
logout
Connection to servera closed.
[operator2@serverb ~]$ ssh root@servera
root@servera's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[root@servera ~]# exit
logout
Connection to servera closed.
[operator2@serverb ~]$ ssh operator3@servera
operator3@servera's password:
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[operator3@servera ~]$ exit
logout
Connection to servera closed.
[operator2@serverb ~]$
```

8. Configure the `sshd` service on the `servera` machine to prevent users from logging in as the `root` user. Use `redhat` as the password of the superuser when required.

1. Open an SSH session to the `servera` machine as the `operator2` user with the SSH keys.

```
[operator2@serverb ~]$ ssh operator2@servera
...output omitted...
[operator2@servera ~]$
```

2. On the `servera` machine, switch to the `root` user. Use `redhat` as the password for the `root` user.

```
[operator2@servera ~]$ su -
Password: redhat
[root@servera ~]#
```

3. Set `PermitRootLogin` to `no` in the `/etc/ssh/sshd_config` file and reload the `sshd` service. You can use the `vim /etc/ssh/sshd_config` command to edit the configuration file of the `sshd` service.

```
...output omitted...
PermitRootLogin no
...output omitted...
[root@servera ~]# systemctl reload sshd
```

4. Open another terminal on `workstation` and open an SSH session to the `serverb` machine as the `operator2` user. From the `serverb` machine, try to log in to the `servera` machine as the `root` user. This command should fail because you disabled the `root` user login over SSH in the preceding step.

## Note

For your convenience, password-less login is already configured between `workstation` and `serverb` in the classroom environment.

```
[student@workstation ~]$ ssh operator2@serverb
...output omitted...
[operator2@serverb ~]$ ssh root@servera
root@servera's password: redhat
Permission denied, please try again.
root@servera's password: redhat
Permission denied, please try again.
root@servera's password: redhat
root@servera: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

By default, the `ssh` command attempts to authenticate with key-based authentication first, and if that method fails, then with password-based authentication.

```

Red Hat
Activities Terminal Dec 10 22:24

root@servera:~
root@servera:~
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[operator2@servera ~]$ exit
logout
Connection to servera closed.
[operator2@serverb ~]$ ssh root@servera
root@servera's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[root@servera ~]# exit
logout
Connection to servera closed.
[operator2@serverb ~]$ ssh operator3@servera
operator3@servera's password:
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[operator3@servera ~]$ exit
logout
Connection to servera closed.
[operator2@serverb ~]$ ssh operator2@servera
operator2@servera's password:
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 22:22:19 2022 from 172.25.250.11
[operator2@servera ~]$ su -
Password:
Last login: Sat Dec 10 22:22:41 EST 2022 from 172.25.250.11 on pts/0
[root@servera ~]# systemctl reload ssh
Unknown command verb reload.
[root@servera ~]# systemctl reload sshd
Unknown command verb reload.
[root@servera ~]# systemctl reload sshd
[root@servera ~]#

```

9. Configure the `sshd` service on the `servera` machine to allow users to authenticate with SSH keys only, rather than with their passwords.
  1. Return to the first terminal with the `root` user's active shell on the `servera` machine. Set the `PasswordAuthentication` parameter to `no` in the `/etc/ssh/sshd_config` file and reload the `sshd` service. You can use the `vim /etc/ssh/sshd_config` command to edit the configuration file of the `sshd` service.

```

...output omitted...
PasswordAuthentication no
...output omitted...
[root@servera ~]# systemctl reload sshd

```
  2. Go to the second terminal with the `operator2` user's active shell on the `serverb` machine, and try to log in to the `servera` machine as the `operator3` user. This command should fail because SSH keys are not configured for the `operator3` user, and the `sshd` service on the `servera` machine does not allow the use of passwords for authentication.

```
[operator2@serverb ~]$ ssh operator3@servera
operator3@servera: Permission denied (publickey,gssapi-
keyex,gssapi-with-mic).
```

### Note

For more granularity, you can use the explicit `-o PubkeyAuthentication=no` and `-o PasswordAuthentication=yes` options with the `ssh` command. You can then override the `ssh` command's defaults and confidently determine that the preceding command fails based on the settings that you adjusted in the `/etc/ssh/sshd_config` file in the preceding step.

- Return to the first terminal with the `root` user's active shell on the `servera` machine. Verify that `PubkeyAuthentication` is enabled in the `/etc/ssh/sshd_config` file. You can use the `vim /etc/ssh/sshd_config` command to view the configuration file of the `sshd` service.

```
...output omitted...
#PubkeyAuthentication yes
...output omitted...
```

The `PubkeyAuthentication` line is commented. Any commented line in this file uses the default value. Commented lines indicate the default values of a parameter. The public key authentication of SSH is active by default, as the commented line indicates.

- Return to the second terminal with the `operator2` user's active shell on the `serverb` machine and try to log in to the `servera` machine as the `operator2` user. This command should succeed because the SSH keys are configured for the `operator2` user to log in to the `servera` machine from the `serverb` machine.

```
[operator2@serverb ~]$ ssh operator2@servera
...output omitted...
[operator2@servera ~]$
```

- From the second terminal, exit the `operator2` user's shell on both the `servera` and `serverb` machines.

```
[operator2@servera ~]$ exit
logout
Connection to servera closed.
[operator2@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

- Close the second terminal on the `workstation` machine.

```
[student@workstation ~]$ exit
```

7. From the first terminal, exit the `root` user's shell on the `servera` machine.

```
[root@servera ~]# exit
logout
```

8. From the first terminal, exit the `operator2` user's shell on both the `servera` and `serverb` machines.

```
[operator2@servera ~]$ exit
logout
Connection to servera closed.
[operator2@serverb ~]$ exit
logout
[student@serverb ~]$
```

9. Log out of `serverb` and return to the `student` user's shell on `workstation`.

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```



```

Red Hat
Activities Terminal Dec 10 22:28

student@workstation:~
operator@servera's password:
Permission denied, please try again.
operator@servera's password:

[operator3@servera ~]$ exit
logout
Connection to servera closed.
[operator3@servera ~]$ exit
logout
Connection to servera closed.
[root@servera ~]# exit
logout
[operator2@servera ~]$ exit
logout
Connection to servera closed.
[operator2@serverb ~]$ exit
logout
Connection to serverb closed.
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$ lab finish ssh-customize

Finishing lab.
- Checking lab systems ..... SUCCESS
- Restoring original /etc/ssh/sshd_config on servera ..... SUCCESS
- Killing user processes servera ..... SUCCESS
- Killing user processes serverb ..... SUCCESS
- Deleting operator2 user on servera ..... SUCCESS
- Deleting operator3 user on servera ..... SUCCESS
- Deleting operator2 user on serverb ..... SUCCESS
- Deleting operator3 user on serverb ..... SUCCESS

[student@workstation ~]$

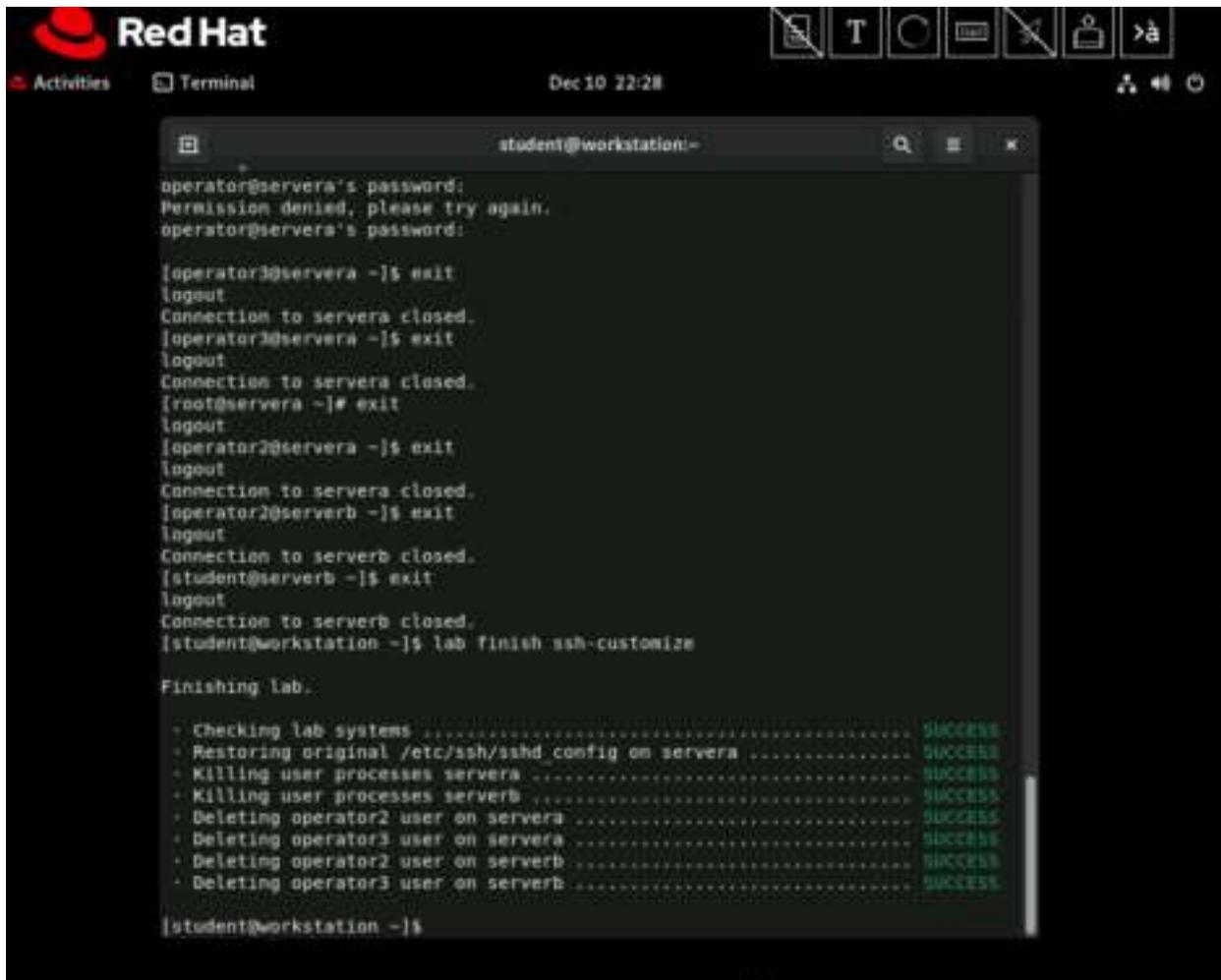
```

## Finish

On the `workstation` machine, change to the `student` user home directory and use the `lab` command to complete this exercise. This step is important to ensure that resources from previous exercises do not impact upcoming exercises.

```
[student@workstation ~]$ lab finish ssh-customize
```

This concludes the section.



```
operator@servera's password:
Permission denied, please try again.
operator@servera's password:

[operator3@servera ~]$ exit
logout
Connection to servera closed.
[operator3@servera ~]$ exit
logout
Connection to servera closed.
[root@servera ~]# exit
logout
[operator2@servera ~]$ exit
logout
Connection to servera closed.
[operator2@serverb ~]$ exit
logout
Connection to serverb closed.
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$ lab finish ssh-customize

Finishing lab.
- Checking lab systems ..... SUCCESS
- Restoring original /etc/ssh/sshd config on servera ..... SUCCESS
- Killing user processes servera ..... SUCCESS
- Killing user processes serverb ..... SUCCESS
- Deleting operator2 user on servera ..... SUCCESS
- Deleting operator3 user on servera ..... SUCCESS
- Deleting operator2 user on serverb ..... SUCCESS
- Deleting operator3 user on serverb ..... SUCCESS

[student@workstation ~]$
```

## Lab: Configure and Secure SSH

In this lab, you set up key-based authentication for users, and disable direct login as `root` and password authentication for all users for the OpenSSH service on one of your servers.

### Outcomes

- Authenticate with SSH keys.
- Prevent users from directly logging in as the `root` user over the `ssh` service.
- Prevent users from logging in to the system with SSH password-based authentication.

As the `student` user on the `workstation` machine, use the `lab` command to prepare your system for this exercise.

This command prepares your environment and ensures that all required resources are available.

```
[student@workstation ~]$ lab start ssh-review
```

```

Red Hat
Activities Terminal Dec 10 22:30

student@workstation-
  · Recording the md5sum of /etc/ssh/sshd_config on serverb ..... SUCCESS

[student@workstation ~]$ lab finish ssh-customize

Finishing lab.

  · Checking lab system ..... SUCCESS
  · Restoring original /etc/ssh/sshd_config on servera ..... SUCCESS
  · Killing user processes servera ..... SUCCESS
  · Killing user processes serverb ..... SUCCESS
  · Deleting operator2 user on servera ..... SUCCESS
  · Deleting operator3 user on servera ..... SUCCESS
  · Deleting operator2 user on serverb ..... SUCCESS
  · Deleting operator3 user on serverb ..... SUCCESS

[student@workstation ~]$ lab start ssh-review

Starting lab.

  · Checking lab system ..... SUCCESS
  · Ensuring the required packages are installed ..... FAIL
    - Command did not exit with the expected code
    - Expected: 0, Received: 1
    - Command did not exit with the expected code
    - Expected: 0, Received: 1
  · Creating required user production1 on servera ..... SUCCESS
  · Creating required user production2 on servera ..... SUCCESS
  · Creating required user production1 on serverb ..... SUCCESS
  · Creating required user production2 on serverb ..... SUCCESS
  · Removing temporary files on serverb ..... SUCCESS
  · Backing up the /etc/ssh/sshd_config file on serverb ..... SUCCESS
  · Permitting SSH as root on serverb ..... SUCCESS
  · Recording the md5sum of /etc/ssh/sshd_config on serverb ..... SUCCESS

[student@workstation ~]$
  
```

### Procedure 10.4. Instructions

## Chapter 10

1. From the workstation machine, log in to the `servera` machine as the `student` user.



```
Red Hat
Activities Terminal Dec 10 22:30

student@servera:~
[student@workstation ~]$ ssh student@servera
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 22:30:29 2022 from 172.25.250.9
[student@servera ~]$
```

2. Switch to the `production1` user on the `servera` machine. Enter `redhat` as the password.



```
production1@servera:~  
[student@workstation ~]$ ssh student@servera  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Register this system with Red Hat Insights: insights-client --register  
Create an account or view all your systems at https://red.ht/insights-dashboard  
Last login: Sat Dec 10 22:30:29 2022 from 172.25.256.9  
[student@servera ~]$ su - production1  
Password:  
[production1@servera ~]$
```

3. Generate passphrase-less SSH keys for the `production1` user on the `servera` machine.



The screenshot shows a terminal window titled "production1@servera:-" with the Red Hat logo and system information at the top. The terminal output shows the following commands and their results:

```
[student@workstation ~]$ ssh student@servera
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Dec 10 22:30:29 2022 from 172.25.250.9
[student@servera ~]$ su - production1
Password:
[production1@servera ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/production1/.ssh/id_rsa):
Created directory '/home/production1/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/production1/.ssh/id_rsa
Your public key has been saved in /home/production1/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:gDoAql12UxGGKVDbaFLP0kk7RyAYhPQR267yMFAmLEM production1@servera.lab.example.com
The key's randomart image is:
+---[RSA 3072]-----+
|
|=+++
|+..+
|+..+
|oB Bo. o
|+ o . . . $
| . = . +
| . . . B .
| . = - o
|_o _
+---[SHA256]-----+
[production1@servera ~]$ ssh-copy-
```

4. Send the public key of the SSH key pair to the `production1` user on the `serverb` machine.



The image shows a terminal window on a Red Hat system. The window title is "production1@servera:-". The terminal output shows the generation of an SSH key pair, the display of the key's randomart image, and the execution of the "ssh-copy-id" command to copy the public key to a remote host named "serverb". The output of "ssh-copy-id" includes a warning about the host's authenticity, a confirmation prompt, and a successful message that one key was added. The terminal ends with the prompt "[production1@servera ~]\$".

```
SHA256:gDoAq112UxGGKvDbafLP0kk7RyAYhP0HQ57ymFaH1EH production1@servera.lab.exas
ple.com
The key's randomart image is:
+---[RSA 3072]-----+
|+++++
|=E++++
|.BoB00
|oB Bo. o
|+ 0 ... 5
| . = . +
| ... B .
|. = . 0
|_ 0
+---[SHA256]-----+
[production1@servera ~]$ ssh-copy-id production1@serverb
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: */home/production
1/.ssh/id_rsa.pub*
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is SHA256:peUGgfxFNw6Jt6WK4CB2rs+Jq11/LhA32M1+8zBaw1I.
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 promp
ted now it is to install the new keys
production1@serverb's password:
Permission denied, please try again.
production1@serverb's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'production1@serverb'"
and check to make sure that only the key(s) you wanted were added.

[production1@servera ~]$
```

5. Verify that the `production1` user can successfully log in to the `serverb` machine with the SSH keys.

```

Red Hat
Activities Terminal Dec 10 22:33

production1@serverb:~$ ssh-copy-id production1@serverb
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: '/home/production1/.ssh/id_rsa.pub'
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ED25519 key fingerprint is SHA256:peU0gfxFNw6Jt6Wk4C82rs+jqll/LhA32Ml+8zBawLI.
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 proep
ted now it is to install the new keys
production1@serverb's password:
Permission denied, please try again.
production1@serverb's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh "production1@serverb"
and check to make sure that only the key(s) you wanted were added.

[production1@servera ~]$ ssh production1@serverb
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[production1@serverb ~]$

```

- Configure the `sshd` service on `serverb` to prevent users from logging in as the `root` user. Use `redhat` as the `root` password.



7. Configure the `sshd` service on the `serverb` machine to allow users to authenticate with SSH keys only, rather than with their passwords.

## Evaluation

As the `student` user on the `workstation` machine, use the `lab` command to grade your work. Correct any reported failures and rerun the command until successful.

```
[student@workstation ~]$ lab grade ssh-review
```

## Finish

On the `workstation` machine, change to the `student` user home directory and use the `lab` command to complete this exercise. This step is important to ensure that resources from previous exercises do not impact upcoming exercises.

## Chapter 10

```
[student@workstation ~]$ lab finish ssh-review
```

This concludes the section.



The screenshot shows a Red Hat desktop environment with a terminal window open. The terminal displays the command `lab finish ssh-review` and its output, which lists several tasks and their status, all marked as `SUCCESS`.

```
student@workstation:~  
[student@workstation ~]$ lab finish ssh-review  
Finishing lab.  
- Checking lab systems ..... SUCCESS  
- Restoring original /etc/ssh/sshd_config on serverb ..... SUCCESS  
- Deleting production1 user on servera ..... SUCCESS  
- Deleting production2 user on servera ..... SUCCESS  
- Deleting production1 user on serverb ..... SUCCESS  
- Deleting production2 user on serverb ..... SUCCESS  
- Removing backup file ..... SUCCESS  
- Disabling sshpass ..... SUCCESS  
[student@workstation ~]$
```