

Task 3

1. Melakukan akses server menggunakan terminal windows

Dengan menginstal openssh-server kemudian cek status ssh dan activekan

```
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
fauzan@dumbways:~$ sudo systemctl status ssh
[sudo] password for fauzan:
● ssh.service - OpenBSD Secure Shell server
    Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
    Active: active (running) since Thu 2025-11-20 10:07:35 UTC; 16h ago
      Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 2087 (sshd)
     Tasks: 1 (limit: 1011)
    Memory: 1.8M
       CPU: 12ms
      CGroup: /system.slice/ssh.service
              └─2087 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Nov 20 10:07:35 dumbways systemd[1]: Starting OpenBSD Secure Shell server...
Nov 20 10:07:35 dumbways sshd[2087]: Server listening on 0.0.0.0 port 22.
Nov 20 10:07:35 dumbways sshd[2087]: Server listening on :: port 22.
Nov 20 10:07:35 dumbways systemd[1]: Started OpenBSD Secure Shell server.
fauzan@dumbways:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d1:0d:14 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.100/24 brd 192.168.1.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fed1:d14/64 scope link
            valid_lft forever preferred_lft forever
fauzan@dumbways:~$
```

kemudian masuk ke terminal windows dengan memasukkan ssh username@ip server kita

```
fauzan@dumbways:~$ PS C:\WINDOWS\system32> ssh fauzan@192.168.1.100
The authenticity of host '192.168.1.100 (192.168.1.100)' can't be established.
ED25519 key fingerprint is SHA256:0x520kkPgHrVKXQs08rHRCT051ionV3f32qApMrQr4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.100' (ED25519) to the list of known hosts.
fauzan@192.168.1.100's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-119-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Fri Nov 21 02:23:33 AM UTC 2025

System load: 0.23           Processes:          105
Usage of /: 49.8% of 6.80GB  Users logged in:      1
Memory usage: 24%           IPv4 address for enp0s3: 192.168.1.100
Swap usage: 0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

172 updates can be applied immediately.
120 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Nov 20 08:27:21 2025
fauzan@dumbways:~$
```

2. Konfigurasi ssh agar bisa diakses menggunakan publikkey

Menggunakan ssh-keygen untuk mendapatkan kunci ssh dan memilih penyimpanan dan nama

```
PS C:\Users\acer> ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:/Users/acer/.ssh/id_ed25519): C:/Users/acer/.ssh/keyserver
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:/Users/acer/.ssh/keyserver
Your public key has been saved in C:/Users/acer/.ssh/keyserver.pub
The key fingerprint is:
SHA256:9MUrcQ4hhEBFMzYUf2zYuB6YBfLZBeVcWFOgldpLUYg acer@LAPTOP-IGIPM8U1
The key's randomart image:
+--[ED25519 256]--+
| .+ .+**o |
| o+.+oE++.. |
| o.++=.+o.. |
| .+= + ..S.o. |
| + o . . . |
| o o . . |
| o o . . |
| . . . . |
+----[SHA256]----+
PS C:\Users\acer> |
```

Kemudian memasukkan atau menambahkan kunci ssh tadi kedalam server

```
fauzan@dumbways:~/ssh  x + | 
fauzan@dumbways:~$ ls -la
total 44
drwxr-x--- 6 fauzan fauzan 4096 Nov 21 02:37 .
drwxr-xr-x  3 root   root   4096 Nov 18 05:50 ..
-rw-----  1 fauzan fauzan 16 Nov 21 02:37 .bash_history
-rw-r--r--  1 fauzan fauzan 220 Jan  6 2022 .bash_logout
-rw-r--r--  1 fauzan fauzan 3771 Jan  6 2022 .bashrc
drwx----- 2 fauzan fauzan 4096 Nov 18 05:53 .cache
drwxr-xr-x  2 fauzan fauzan 4096 Nov 20 09:03 folder1
drwxrwxr-x  3 fauzan fauzan 4096 Nov 20 03:17 .local
-rw-r--r--  1 fauzan fauzan 807 Jan  6 2022 .profile
drwx----- 2 fauzan fauzan 4096 Nov 18 05:51 .ssh
-rw-r--r--  1 fauzan fauzan 0 Nov 20 08:46 .sudo_as_admin_successful
-rw-----  1 fauzan fauzan 532 Nov 21 02:37 .viminfo
fauzan@dumbways:~$ cd .ssh
fauzan@.ssh:~$ ls
authorized_keys
fauzan@dumbways:~/.ssh$ nano authorized_keys
fauzan@dumbways:~/.ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAIOKycaM3KyHcXPQh+Qp1BZ6sRzG3hg6ucEpRcEAkvvry acer@LAPTOP-IGIPM8UI
fauzan@dumbways:~/.ssh$ |
```

Kemudian login dengan ssh -i (lokasi kunci) username@ipserver

```
fauzan@dumbways:~$ fauzan@acer: ssh -i .ssh/keyserver fauzan@192.168.1.100
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Fri Nov 21 02:52:45 AM UTC 2025

System load:  0.05      Processes:           104
Usage of /:   49.8% of 6.80GB  Users logged in:    1
Memory usage: 24%          IPv4 address for enp0s3: 192.168.1.100
Swap usage:   0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

172 updates can be applied immediately.
120 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

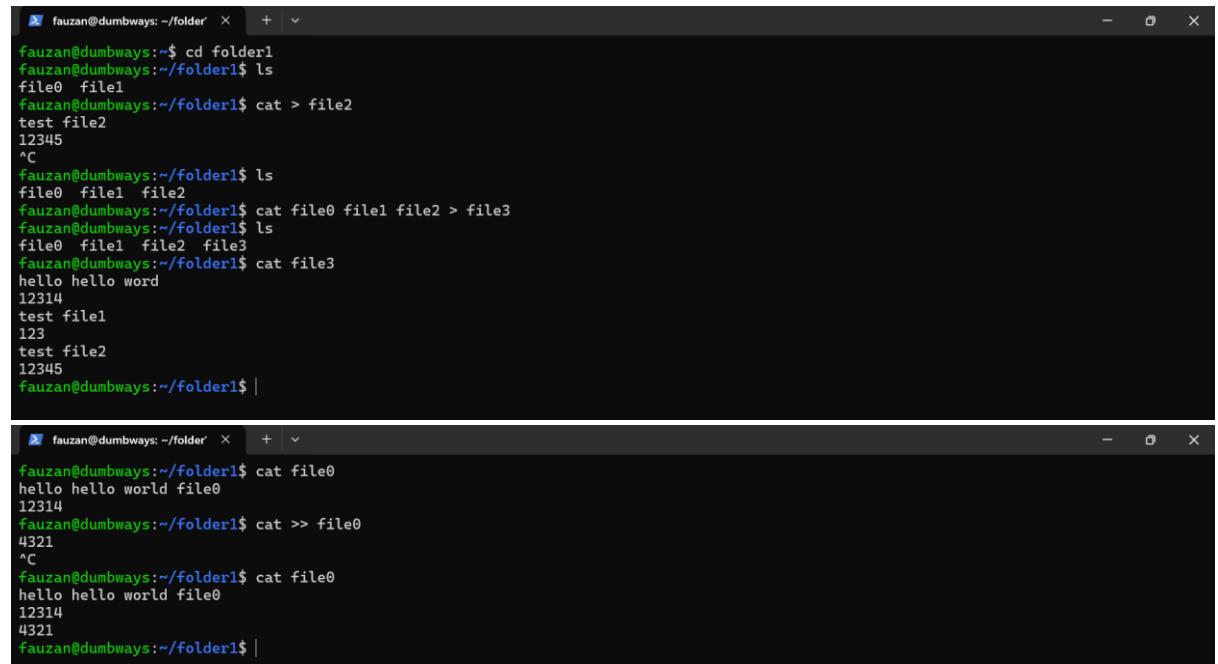
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Nov 21 02:46:24 2025 from 192.168.1.5
fauzan@dumbways:~$ |
```

3. Buat step by step penggunaan (grep, sed, cat, echo)

Penggunaan “**cat**” untuk melihat isi, untuk pembuatan file sekaligus isi, untuk menambahkan isi, untuk menggabungkan isi file sekaligus membuat

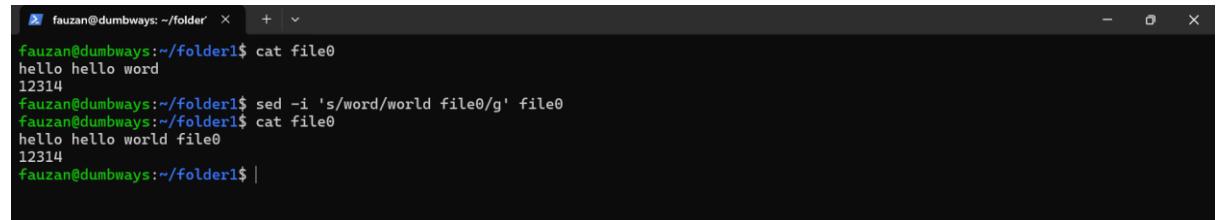


```
fauzan@dumbways:~/folder$ cd folder1
fauzan@dumbways:~/folder1$ ls
file0 file1
fauzan@dumbways:~/folder1$ cat > file2
test file2
12345
^C
fauzan@dumbways:~/folder1$ ls
file0 file1 file2
fauzan@dumbways:~/folder1$ cat file0 file1 file2 > file3
fauzan@dumbways:~/folder1$ ls
file0 file1 file2 file3
fauzan@dumbways:~/folder1$ cat file3
hello hello word
12314
test file1
123
test file2
12345
fauzan@dumbways:~/folder1$ |
```



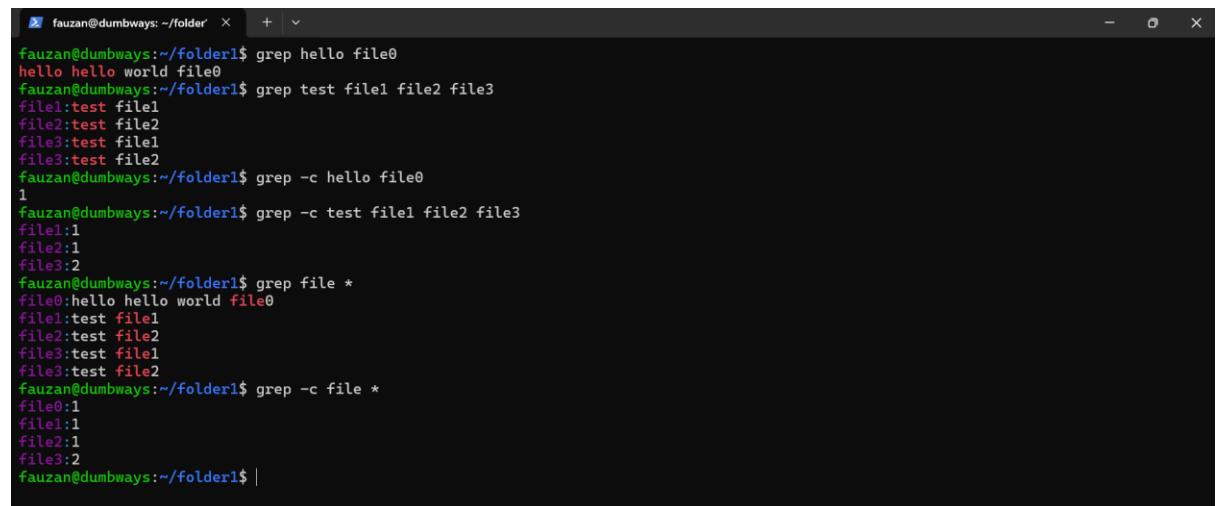
```
fauzan@dumbways:~/folder$ cat file0
hello hello world file0
12314
fauzan@dumbways:~/folder1$ cat >> file0
4321
^C
fauzan@dumbways:~/folder1$ cat file0
hello hello world file0
12314
4321
fauzan@dumbways:~/folder1$ |
```

Penggunaan “**sed**” untuk mereplace isi dari file yang dipilih



```
fauzan@dumbways:~/folder$ cat file0
hello hello word
12314
fauzan@dumbways:~/folder1$ sed -i 's/word/world/g' file0
fauzan@dumbways:~/folder1$ cat file0
hello hello world file0
12314
fauzan@dumbways:~/folder1$ |
```

Penggunaan “**grep**” untuk mencari kata atau kalimat dalam file atau folder



```
fauzan@dumbways:~/folder$ grep hello file0
hello hello world file0
fauzan@dumbways:~/folder1$ grep test file1 file2 file3
file1:test file1
file2:test file2
file3:test file1
file3:test file2
fauzan@dumbways:~/folder1$ grep -c hello file0
1
fauzan@dumbways:~/folder1$ grep -c test file1 file2 file3
file1:1
file2:1
file3:2
fauzan@dumbways:~/folder1$ grep file *
file0:hello hello world file0
file1:test file1
file2:test file2
file3:test file1
file3:test file2
fauzan@dumbways:~/folder1$ grep -c file *
file0:1
file1:1
file2:1
file3:2
fauzan@dumbways:~/folder1$ |
```

Penggunaan “sort” untuk melihat data sesuai dengan urutan terbesar atau terkecil

```
fauzan@dumbways:~/folder1$ nano angka
fauzan@dumbways:~/folder1$ cat angka
3
2
7
4
fauzan@dumbways:~/folder1$ sort angka
2
3
4
7
fauzan@dumbways:~/folder1$ sort -r angka
7
4
3
2
fauzan@dumbways:~/folder1$ cat angka
3
2
7
4
fauzan@dumbways:~/folder1$ |
```

Penggunaan “echo” untuk mereplace isi file sekaligus membuatnya atau menambahkan isi file dibawahnya

```
fauzan@dumbways:~/folder1$ ls
angka file0 file1 file2 file3
fauzan@dumbways:~/folder1$ echo "hello dumwais" > file4
fauzan@dumbways:~/folder1$ cat file4
hello dumwais
fauzan@dumbways:~/folder1$ echo "123456" > file4
fauzan@dumbways:~/folder1$ cat file4
123456
fauzan@dumbways:~/folder1$ echo "hello dumwais" >> file4
fauzan@dumbways:~/folder1$ cat file4
123456
hello dumwais
fauzan@dumbways:~/folder1$ |
```

4. Menyalakan akses ufw dengan memberikan akses untuk port 22,80, 443, 3000, 6969

Pertama dengan menjalankan ufw agar menjadi active

```
fauzan@dumbways:~$ sudo ufw status
Status: inactive
fauzan@dumbways:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
fauzan@dumbways:~$ sudo ufw status
Status: active
fauzan@dumbways:~$ sudo ufw allow 22
Rule added
Rule added (v6)
fauzan@dumbways:~$ sudo ufw status
Status: active

To                         Action      From
--                         --          --
22                         ALLOW       Anywhere
22 (v6)                     ALLOW       Anywhere (v6)

fauzan@dumbways:~$ sudo ufw allow "OpenSSH"
Rule added
Rule added (v6)
fauzan@dumbways:~$ sudo ufw reset
Resetting all rules to installed defaults. This may disrupt existing ssh
connections. Proceed with operation (y|n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20251121_074434'
Backing up 'before.rules' to '/etc/ufw/before.rules.20251121_074434'
Backing up 'after.rules' to '/etc/ufw/after.rules.20251121_074434'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20251121_074434'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20251121_074434'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20251121_074434'

fauzan@dumbways:~$ sudo ufw status
Status: inactive
fauzan@dumbways:~$ |
```

Kemudian baru bisa menambahkan (allow, deny, delete) app ufw dan port yang ada

```
fauzan@dumbways:~$ sudo ufw status
Status: active

To           Action    From
--           ----     ---
OpenSSH      ALLOW     Anywhere
OpenSSH (v6) ALLOW     Anywhere (v6)

fauzan@dumbways:~$ sudo ufw app list
Available applications:
  Nginx Full
  Nginx HTTP
  Nginx HTTPS
  OpenSSH
fauzan@dumbways:~$ sudo ufw allow 22
Rule added
Rule added (v6)
fauzan@dumbways:~$ sudo ufw allow 80
Rule added
Rule added (v6)
fauzan@dumbways:~$ sudo ufw allow 443
Rule added
Rule added (v6)
fauzan@dumbways:~$ sudo ufw allow 3000
Rule added
Rule added (v6)
fauzan@dumbways:~$ sudo ufw allow 6969
Rule added
Rule added (v6)
fauzan@dumbways:~$ sudo ufw status
Status: active

To           Action    From
--           ----     ---
OpenSSH      ALLOW     Anywhere
22          ALLOW     Anywhere
80          ALLOW     Anywhere
443         ALLOW     Anywhere
3000        ALLOW     Anywhere
6969        ALLOW     Anywhere
OpenSSH (v6) ALLOW     Anywhere (v6)
22 (v6)     ALLOW     Anywhere (v6)
80 (v6)     ALLOW     Anywhere (v6)
443 (v6)   ALLOW     Anywhere (v6)
3000 (v6)  ALLOW     Anywhere (v6)
6969 (v6)  ALLOW     Anywhere (v6)

fauzan@dumbways:~$ sudo ufw deny 22
Rule updated
Rule updated (v6)
fauzan@dumbways:~$ sudo ufw delete 80
ERROR: Could not find rule '80'
fauzan@dumbways:~$ sudo ufw delete allow 80
Rule deleted
Rule deleted (v6)
fauzan@dumbways:~$ sudo ufw status
Status: active

To           Action    From
--           ----     ---
OpenSSH      ALLOW     Anywhere
22          DENY     Anywhere
443         ALLOW     Anywhere
3000        ALLOW     Anywhere
6969        ALLOW     Anywhere
OpenSSH (v6) ALLOW     Anywhere (v6)
22 (v6)     DENY     Anywhere (v6)
443 (v6)   ALLOW     Anywhere (v6)
3000 (v6)  ALLOW     Anywhere (v6)
6969 (v6)  ALLOW     Anywhere (v6)

fauzan@dumbways:~$ |
```