Task 4: Setup and Use a Firewall on Windows/Linux

Objective: Configure and test basic firewall rules to allow or block traffic.

Tools: Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

Deliverables: Screenshot/configuration file showing firewall rules applied.

IP addresses of machines:

Attacker machine: 172.19.96.1

Victim machine (ubuntu): 172.19.102.220

1. **Checking the version of UFW:**

```
root@DESKTOP-HGB3T9Q:~# ufw --version
ufw 0.36.2
Copyright 2008-2023 Canonical Ltd.
root@DESKTOP-HGB3T9Q:~#
```

2. Current Firewall rules list:

```
root@DESKTOP-HGB3T9Q:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     DENY        172.17.0.2

root@DESKTOP-HGB3T9Q:~#
```

3. Rule to block inbound traffic on a specific port (23/telnet).

```
root@DESKTOP-HGB3T9Q:~# ufw deny 23/tcp
Rule added
Rule added (v6)
root@DESKTOP-HGB3T9Q:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     DENY        172.17.0.2
23                         ALLOW       Anywhere
23/tcp                     DENY        Anywhere
23 (v6)                    ALLOW       Anywhere (v6)
23/tcp (v6)                DENY        Anywhere (v6)

root@DESKTOP-HGB3T9Q:~#
```

4. Attempting to Send Ping request to the target:
   In result the target machine is blocking the requests coming from the attacker machine.

```
2025-05-31T08:58:48.296480+00:00 DESKTOP-HGB3T9Q kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:15:5d:d7:14:5a:00:15:5d:d4:46:c
3:08:00 SRC=172.19.96.1 DST=172.19.102.220 LEN=44 TOS=0x00 PREC=0x00 TTL=51 ID=21015 PROTO=TCP SPT=40779 DPT=2003 WINDOW
=1024 RES=0x00 SYN URGP=0
2025-05-31T08:58:48.296482+00:00 DESKTOP-HGB3T9Q kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:15:5d:d7:14:5a:00:15:5d:d4:46:c
3:08:00 SRC=172.19.96.1 DST=172.19.102.220 LEN=44 TOS=0x00 PREC=0x00 TTL=46 ID=43397 PROTO=TCP SPT=40779 DPT=49153 WINDO
W=1024 RES=0x00 SYN URGP=0
2025-05-31T08:58:48.296484+00:00 DESKTOP-HGB3T9Q kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:15:5d:d7:14:5a:00:15:5d:d4:46:c
3:08:00 SRC=172.19.96.1 DST=172.19.102.220 LEN=44 TOS=0x00 PREC=0x00 TTL=38 ID=58009 PROTO=TCP SPT=40779 DPT=301 WINDOW=
1024 RES=0x00 SYN URGP=0
2025-05-31T08:58:48.296503+00:00 DESKTOP-HGB3T9Q kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:15:5d:d7:14:5a:00:15:5d:d4:46:c
3:08:00 SRC=172.19.96.1 DST=172.19.102.220 LEN=44 TOS=0x00 PREC=0x00 TTL=57 ID=8896 PROTO=TCP SPT=40779 DPT=6839 WINDOW=
1024 RES=0x00 SYN URGP=0
2025-05-31T08:58:48.296505+00:00 DESKTOP-HGB3T9Q kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:15:5d:d7:14:5a:00:15:5d:d4:46:c
3:08:00 SRC=172.19.96.1 DST=172.19.102.220 LEN=44 TOS=0x00 PREC=0x00 TTL=41 ID=2252 PROTO=TCP SPT=40779 DPT=22939 WINDOW
=1024 RES=0x00 SYN URGP=0
```

5. Adding rule to allow SSH (port 22):

```
root@DESKTOP-HGB3T9Q:~# ufw allow 22/tcp
Rule added
Rule added (v6)
root@DESKTOP-HGB3T9Q:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     DENY        172.17.0.2
23/tcp                     DENY        Anywhere
22/tcp                     ALLOW       Anywhere
23/tcp (v6)                DENY        Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)

root@DESKTOP-HGB3T9Q:~#
```

6. Removing the added rules:

```
root@DESKTOP-HGB3T9Q:~# ufw delete deny 23/tcp
Rule deleted
Rule deleted (v6)
root@DESKTOP-HGB3T9Q:~# ufw delete allow 22/tcp
Rule deleted
Rule deleted (v6)
root@DESKTOP-HGB3T9Q:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     DENY        172.17.0.2

root@DESKTOP-HGB3T9Q:~#
```

7. Commands Used:

i. For Adding rules:
   a) For blocking request: ufw deny 23/tcp
   b) For allowing request: ufw allow 22/tcp

ii. For Deleting added rules:
   ufw delete <rule name>

iii. Command used to detect the incoming traffic:
   sudo tail -f /var/log/ufw.log