



DAY 7 — Network Attacks & Detection

Role alignment: SOC Analyst + Network Security Engineer

Mindset: “If an attack happens, I can detect, explain, and prove it.”

Today we will assume as we are working in the big companies of the USA and today's role assigned by Ciso is ,if an attack happens in our systems ,how can you detect it ,which tools you will use ,and provide proof as well .



LAB SETUP (NO CHANGES)

First step we step up our lab , we will assume kali as an attacker and ubuntu as a target +defender. Make sure kali and ubuntu are connected to the same network which is the INTERNAL NETWORK ,they both should talk to each other ,to check that we will use this command on kali is (ping -c 4 10.0.0.2).after that we will check ssh is enable ,the command we will use to check that ssh is active or not active on ubuntu we will put this (sudo systemctl status ssh) if it is not enable we will use this command (sudo systemctl enable ssh). And if it is stopped by any chance we have to use this (sudo systemctl start ssh).after that we will check apache is running ,to check apache will insure this command (sudo systemctl status apache2) now we will use This command confirms that the server is specifically listening for web traffic on **Port 80**, command is (sudo ss -tuln | grep :80) After these we will check ufw status by using this command(sudo ufw status) on ubuntu .after that we will also check the status of fail2ban by using this command (sudo systemctl status fail2ban) on ubuntu .

Kali Linux → Attacker

Ubuntu Server → Target

SSH enabled

Apache running

UFW + Fail2Ban active.

● ATTACK 1 — NETWORK RECONNAISSANCE (SCAN)

STEP 1: Perform Scan (Kali)

In this first step we will scan the ports ,for scanning on the kali terminal we will type (nmap -sS -p 22,80 10.0.0.2),this command will confirm to us that both 22,80 ports are opened.



```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sS -p 22,80 10.0.0.2  
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-23 13:38 -0500  
Nmap scan report for 10.0.0.2  
Host is up (0.0013s latency).  
  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 08:00:27:80:0B:2E (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds  
(kali@kali)-[~]  
$
```

STEP 2: Detect Scan (Ubuntu Logs)

Now on the ubuntu terminal we will detect the scanning results by using this command (`sudo grep "UFW" /var/log/ufw.log`).we will see multiple logging is going on means it will provide criminal report like kali ip,block or allow detections .if the log is empty we will use this command first to turn on (`sudo ufw logging on`).

```
kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
Ubuntu Server [Running] - Oracle VirtualBox

File      Machine  View      Input      Devices    Help

TOS=0x18 PREC=0xA0 TTL=64 ID=55709 DF PROTO=TCP SPT=54548 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-21T20:27:13.892572+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=55710 DF PROTO=TCP SPT=54548 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-21T20:27:46.677149+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=55711 DF PROTO=TCP SPT=54548 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:45:46.042362+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=221 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:45:47.185559+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=222 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:45:53.385104+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=223 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:45:49.295516+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=224 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:45:50.341044+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=225 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:45:51.364096+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=226 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:45:53.706012+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=227 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:45:57.520144+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=228 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:46:05.706012+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=229 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:46:21.813253+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=230 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:46:55.081552+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=231 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:26.431015+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=28032 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:27.463433+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=28033 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:28.501312+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=28034 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:29.531030+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=28035 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:30.535042+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=28036 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:31.573535+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=28037 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:33.630167+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=28038 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:37.924993+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=28039 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:46.019185+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=28040 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:50:02.364132+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=28041 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:50:36.176246+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:0
TOS=0x18 PREC=0xA0 TTL=64 ID=28042 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
dawood@target-server:~$ _
```

STEP 3: Packet Evidence

Now in this step we skim packet evidence by typing this command on ubuntu (sudo tcpdump -i any tcp port 22 or 80) then the screen will wait. It is now your "digital microphone" listening for traffic. after this we have to switch to kali terminal and type this command (nmap -sS -p 22,80 10.0.0.2) .after that we go back to ubuntu to analyze some lines that are packet evidence.

```
kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
Ubuntu Server [Running] - Oracle VirtualBox

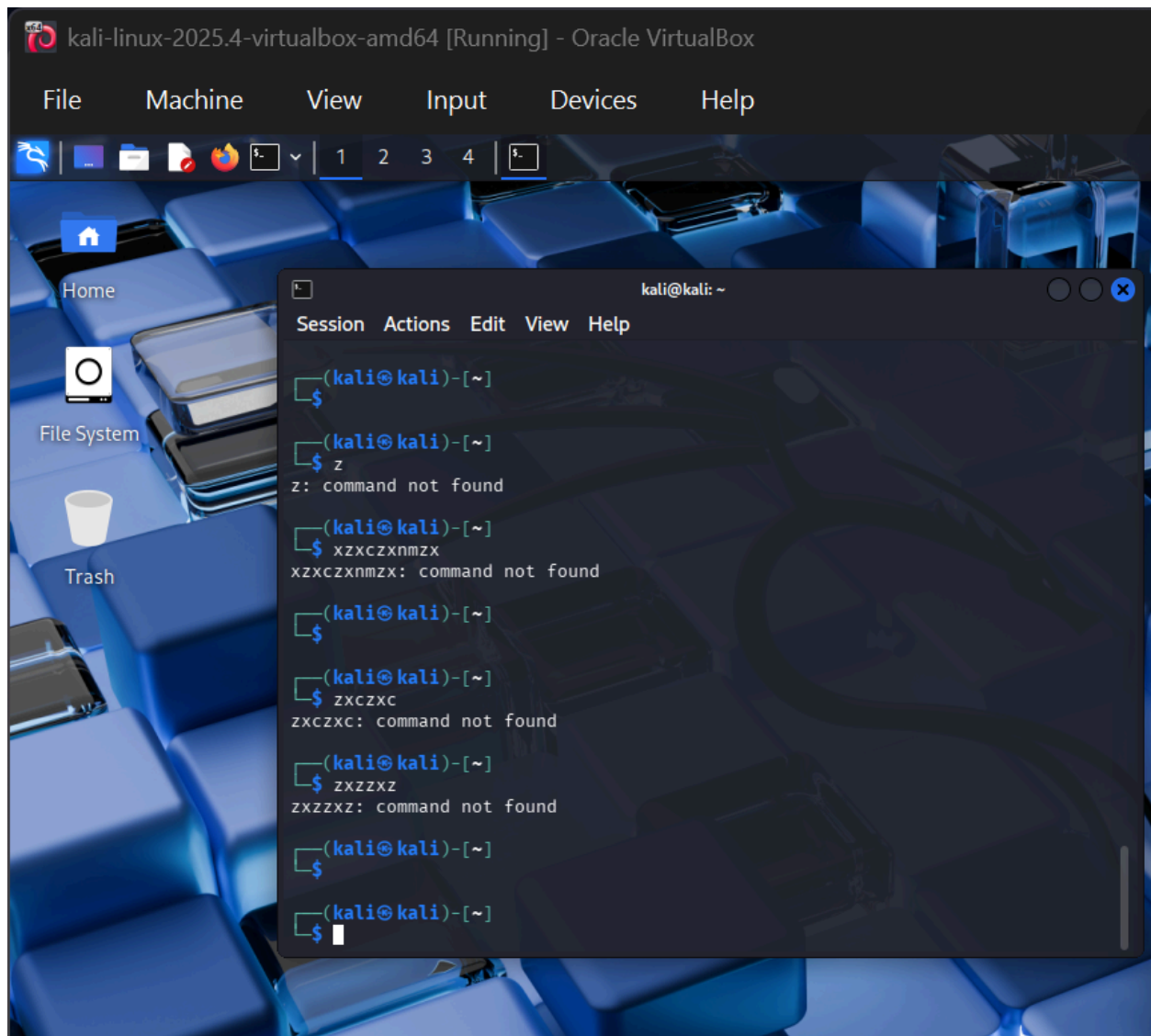
File Machine View Input Devices Help

TOS=0x18 PREC=0xA0 TTL=64 ID=225 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:45:51.364096+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=226 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:45:53.385104+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=227 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:45:57.520144+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=228 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:46:05.706012+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=229 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:46:21.813253+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=230 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:46:55.001552+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=231 DF PROTO=TCP SPT=51308 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:26.431015+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=28032 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:27.463433+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=28033 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:28.501312+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=28034 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:29.531030+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=28035 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:30.535042+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=28036 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:31.573535+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=28037 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:33.630167+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=28038 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:37.924993+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=28039 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:49:46.019185+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=28040 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:50:02.364132+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=28041 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
2026-01-22T19:50:36.176246+00:00 target-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:80:0b:2e:08:00
TOS=0x18 PREC=0xA0 TTL=64 ID=28042 DF PROTO=TCP SPT=58508 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0
dawood@target-server:~$ sudo tcpdump -i any tcp port 22 or 80
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
18:47:33.656985 enp0s3 In IP 10.0.0.1.43568 > target-server.ssh: Flags [S], seq 2863041091, win 1024, option
18:47:33.657039 enp0s3 Out IP target-server.ssh > 10.0.0.1.43568: Flags [S.], seq 805533261, ack 2863041092,
18:47:33.656985 enp0s3 In IP 10.0.0.1.43568 > target-server.http: Flags [S], seq 2863041091, win 1024, option
18:47:33.657114 enp0s3 Out IP target-server.http > 10.0.0.1.43568: Flags [S.], seq 4020622732, ack 2863041092
18:47:33.657820 enp0s3 In IP 10.0.0.1.43568 > target-server.ssh: Flags [R], seq 2863041092, win 0, length 0
18:47:33.657820 enp0s3 In IP 10.0.0.1.43568 > target-server.http: Flags [R], seq 2863041092, win 0, length 0
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
dawood@target-server:~$
```

● ATTACK 2 — BRUTE FORCE (CONTROLLED)

STEP 4: Launch Brute Attempts (Kali)

Before stopping pockets running on ubuntu we will type this command on kali for brute forcing which is called taking control of ubuntu terminal we will type (for i in {1..5}; do ssh fakeuser@10.0.0.2; done) after typing this we will type wrong passwords but 5 times ,after 5 time attacking with wrong password our ip should be blocked from ubuntu.



```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$  
(kali@kali)-[~]  
$ z  
z: command not found  
(kali@kali)-[~]  
$ xzxczxnmxz  
xzxczxnmxz: command not found  
(kali@kali)-[~]  
$ zxczxc  
zxczxc: command not found  
(kali@kali)-[~]  
$ zxzzxz  
zxzzxz: command not found  
(kali@kali)-[~]  
$ zxczxc  
zxczxc: command not found  
(kali@kali)-[~]  
$
```

STEP 5: Detect via Logs (Ubuntu)

In this step we will check the attached that has been done attacker ,we will check through logs ,we use command (sudo grep "Failed password" /var/log/auth.log)
Then we will use this command (sudo fail2ban-client status sshd) after typing both commands we will see how many times ip failed and 1 ip banned.

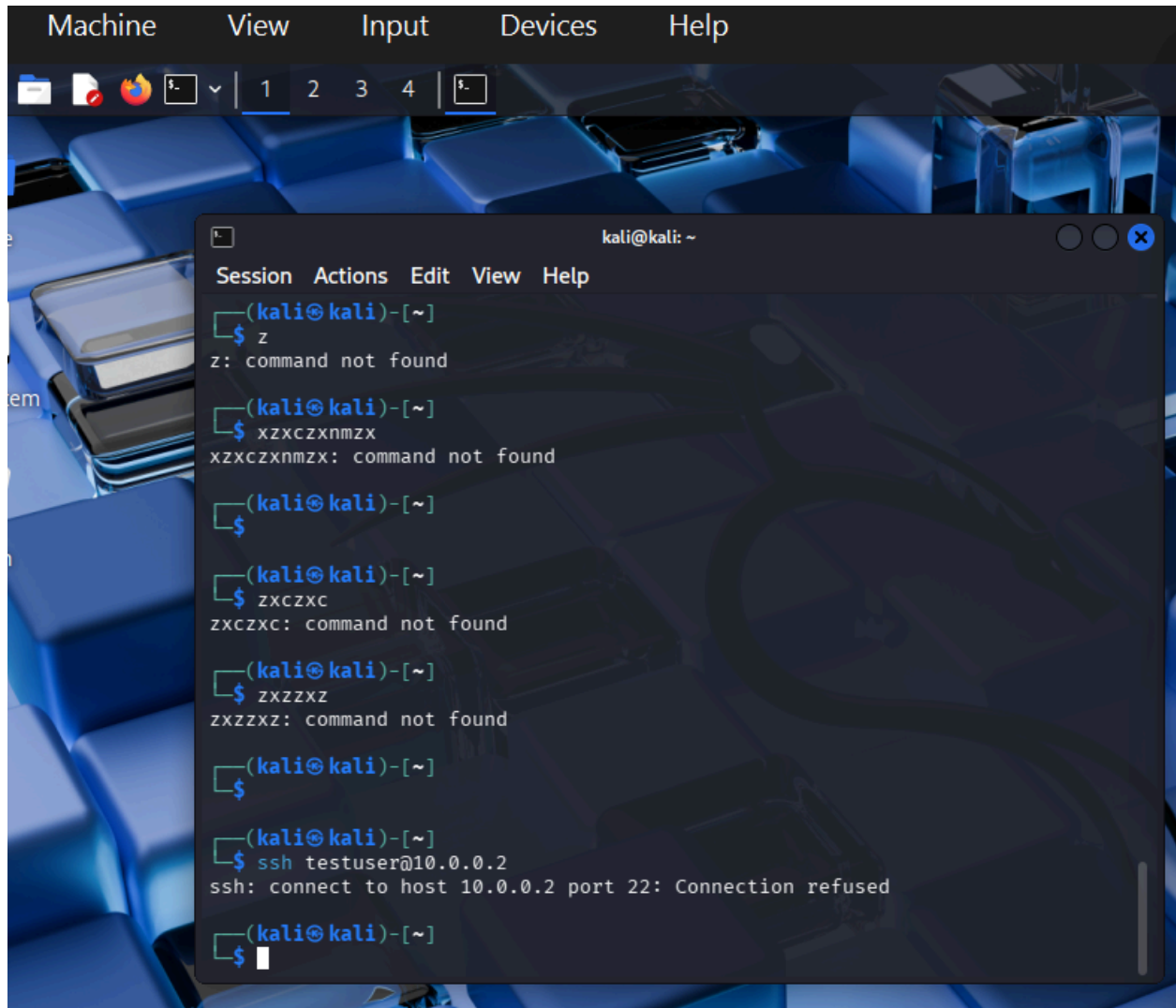
```
kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
Ubuntu Server [Running] - Oracle VirtualBox

File Machine View Input Devices Help

length 0
18:52:00.931620 enp0s3 In IP 10.0.0.1.55346 > target-server.ssh: Flags [.], ack 3161, win 252, options [nop,
^C
42 packets captured
42 packets received by filter
0 packets dropped by kernel
dawood@target-server:~$ sudo grep "Failed Password" /var/log/auth.log
2026-01-23T18:54:27.843105+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COM
log
dawood@target-server:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 4
| \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
| |- Currently banned: 0
| |- Total banned: 0
| \- Banned IP list:
dawood@target-server:~$ sudo grep "failed password" /var/log/auth.log
2026-01-20T20:16:16.347936+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COM
g
2026-01-20T20:19:01.314536+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COM
log
2026-01-20T20:39:03.835605+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COM
th.log
2026-01-23T18:57:56.368764+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COM
log
dawood@target-server:~$ sudo grep "failed password" /var/log/auth.log
2026-01-20T20:16:16.347936+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COM
g
2026-01-20T20:19:01.314536+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COM
log
2026-01-20T20:39:03.835605+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COM
th.log
2026-01-23T18:57:56.368764+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COM
log
2026-01-23T19:00:47.444648+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COM
log
dawood@target-server:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 5
| \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
| |- Currently banned: 1
| |- Total banned: 1
| \- Banned IP list: 10.0.0.1
dawood@target-server:~$ _
```

STEP 6: Verify Block (Kali)

Now we will officially verify that our ip is banned by typing this command on kali terminal (ssh testuser@10.0.0.2), output we will see timeout,refused.



The screenshot shows a Kali Linux desktop environment with a blue-themed background. A terminal window is open, displaying the following commands and their outputs:

```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ z  
z: command not found  
(kali@kali)-[~]  
$ xzxczxnmx  
xzxczxnmx: command not found  
(kali@kali)-[~]  
$  
(kali@kali)-[~]  
$ zxczxc  
zxczxc: command not found  
(kali@kali)-[~]  
$ zxzzxz  
zxzzxz: command not found  
(kali@kali)-[~]  
$  
(kali@kali)-[~]  
$ ssh testuser@10.0.0.2  
ssh: connect to host 10.0.0.2 port 22: Connection refused  
(kali@kali)-[~]  
$
```



CORRELATION (MOST IMPORTANT)

Answer these in your notes:

- How did logs show the attack?
UFW tool will show attacks
- How did packets show the attack?
With the help of tcpdump packet will show the attacks
- Which tool detected what?
In today's session we are using two tools for detection: ufw and fail2ban.
Ufw will block the unusual network traffic and fail2ban is like bouncer . It will throw you from the club and ban you ,if you are unauthorized and suspicious .
- Why correlation matters in real SOCs?
Correlation is very important in every field ,it will tell how much skills,understanding you have of your work and it will teach you many things after recognition or review from ciso or top tier analyst.
-
-
-

Security Command Glossary

Tool / Comm and	Full Form	Purpose in Lab
nmap	Network Mapper	Used to scan the target for open ports (22, 80).
ssh	Secure Shell	Used to attempt remote logins (and simulate brute force).
ufw	Uncomplicated Firewall	Used to log and block network traffic.
fail2ban-client	Fail to Ban Client	Used to monitor and manage the status of banned IPs.
grep	Global Regular Expression Print	Used to search logs for specific strings like "Failed password".
tcpdump	TCP Dump	Used to capture and display raw network packets in real-time.
sudo	Superuser DO	Used to run security commands with administrative privileges.

apt	Advanced Package Tool	Used to install the security software on Ubuntu.
------------	------------------------------	--

-