🛡️ DAY 5 — Defense & Active Response

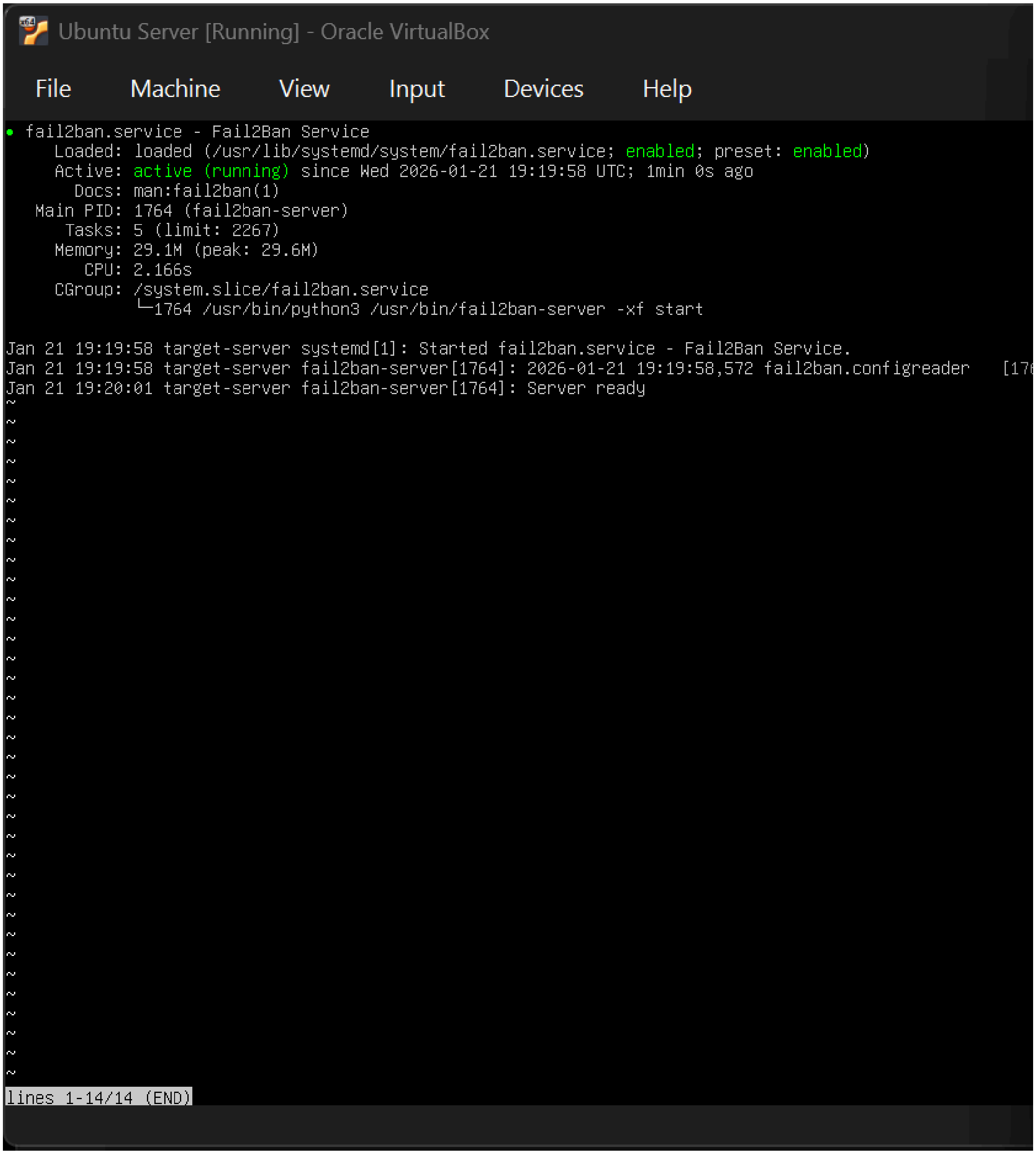
In today's session we will fix one common problem. Today some hacker tried to guess our password many times (brute force) ,and we have to protect them by hiring one bouncer on the door. If they tried to attack 3 to 4 times ,they would be kicked out for 10 to 15 minutes . bouncer 's name is (**fail2ban**).

STEP 1: Install Fail2Ban (Defender)

In this step we first install bouncer which is fail2ban. This tool will protect our system from hackers and kick them out after attacking 3 to 4 times .

The command we are using in this is (sudo apt install fail2ban -y) and one more ,if your lab network is internal we have to change this to (NAT) for downloading then set to (Internal network)again.after running first command we have also check is it installed by using this command (sudo systemctl status fail2ban)

Proof



```
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Wed 2026-01-21 19:19:58 UTC; 1min 0s ago
       Docs: man:fail2ban(1)
   Main PID: 1764 (fail2ban-server)
      Tasks: 5 (limit: 2267)
     Memory: 29.1M (peak: 29.6M)
        CPU: 2.166s
     CGroup: /system.slice/fail2ban.service
             └─1764 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Jan 21 19:19:58 target-server systemd[1]: Started fail2ban.service - Fail2Ban Service.
Jan 21 19:19:58 target-server fail2ban-server[1764]: 2026-01-21 19:19:58,572 fail2ban.configreader   [176
Jan 21 19:20:01 target-server fail2ban-server[1764]: Server ready
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
lines 1-14/14 (END)
```

STEP 2: Create Local Configuration (CRITICAL)

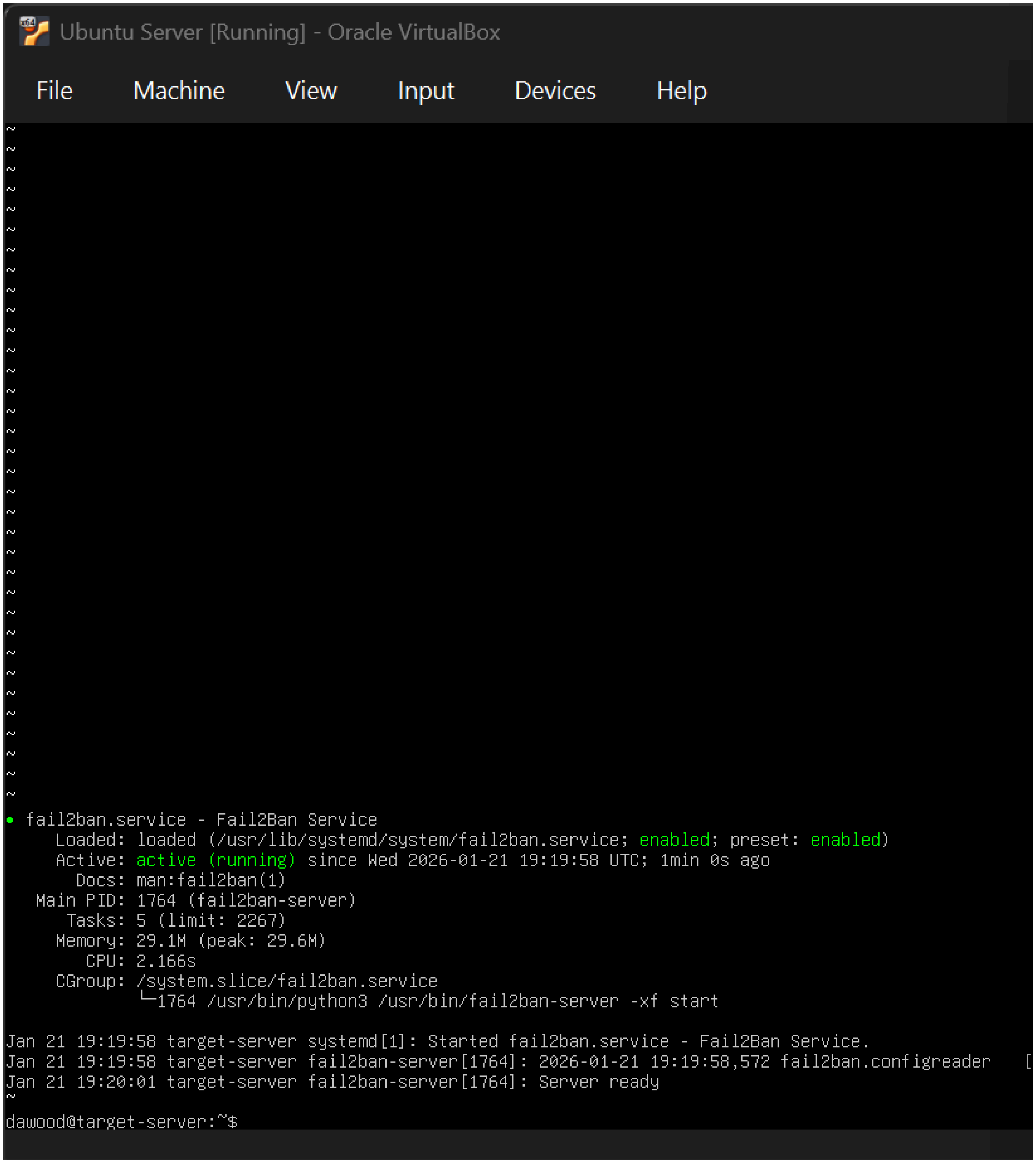
STEP 3: Configure SSH Protection

In these step we will provide some instruction to bouncer (fail2ban),then it will behave accordingly instruction

The command we are using in this is (sudo nano /etc/fail2ban/jail.local)
Then we have to find this section [sshd]
The rules we will typed inside `enabled = true`

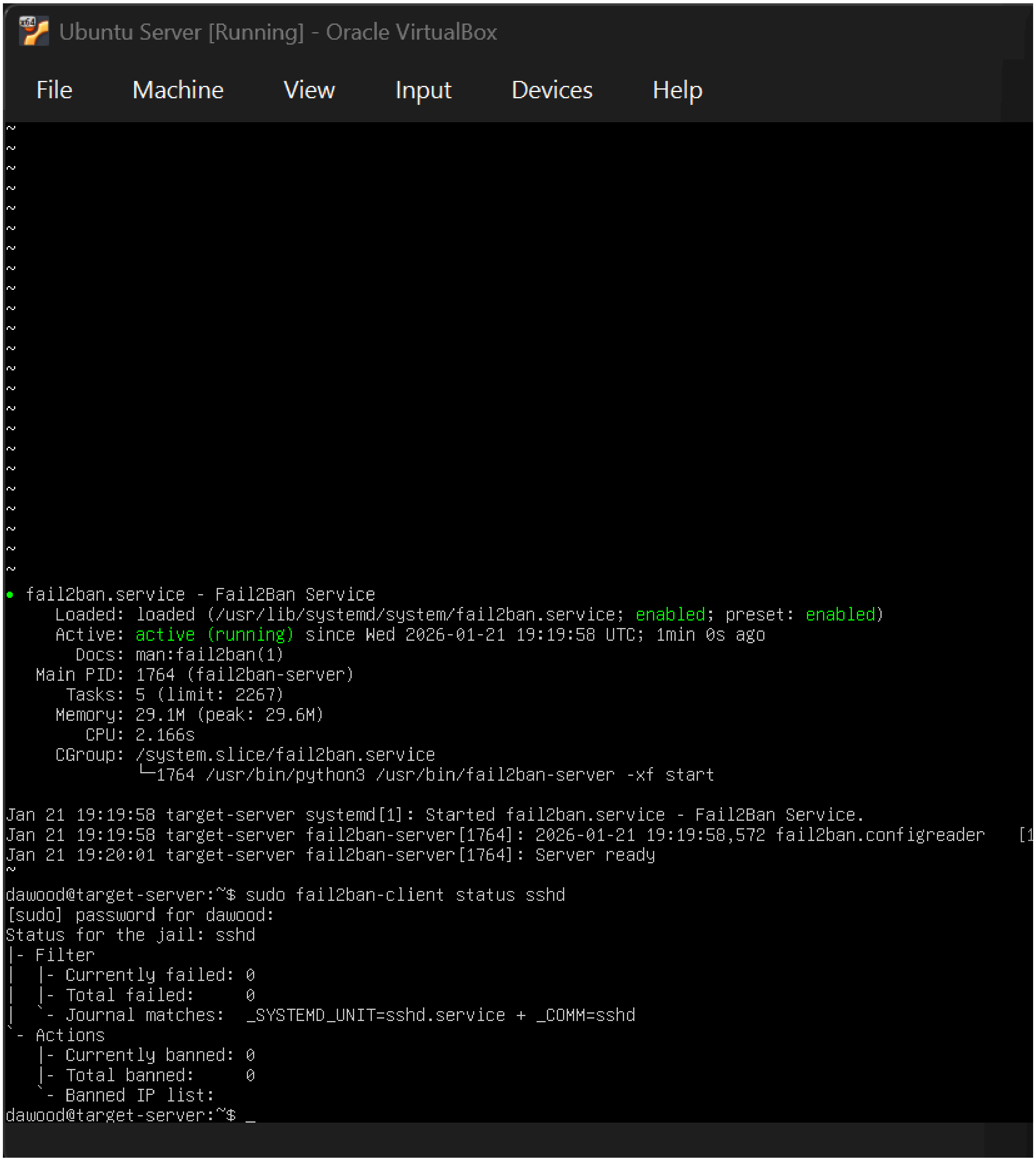
```
 maxretry = 3 (Ban after 3 fails)
 bantime = 10m (Lock for 10 minutes)
 backend = systemd (The Ubuntu 24.04 fix)
```

Proof



```
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Wed 2026-01-21 19:19:58 UTC; 1min 0s ago
       Docs: man:fail2ban(1)
   Main PID: 1764 (fail2ban-server)
      Tasks: 5 (limit: 2267)
     Memory: 29.1M (peak: 29.6M)
        CPU: 2.166s
     CGroup: /system.slice/fail2ban.service
             └─1764 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Jan 21 19:19:58 target-server systemd[1]: Started fail2ban.service - Fail2Ban Service.
Jan 21 19:19:58 target-server fail2ban-server[1764]: 2026-01-21 19:19:58,572 fail2ban.configreader    [
Jan 21 19:20:01 target-server fail2ban-server[1764]: Server ready
~
dawood@target-server:~$
```

Proof



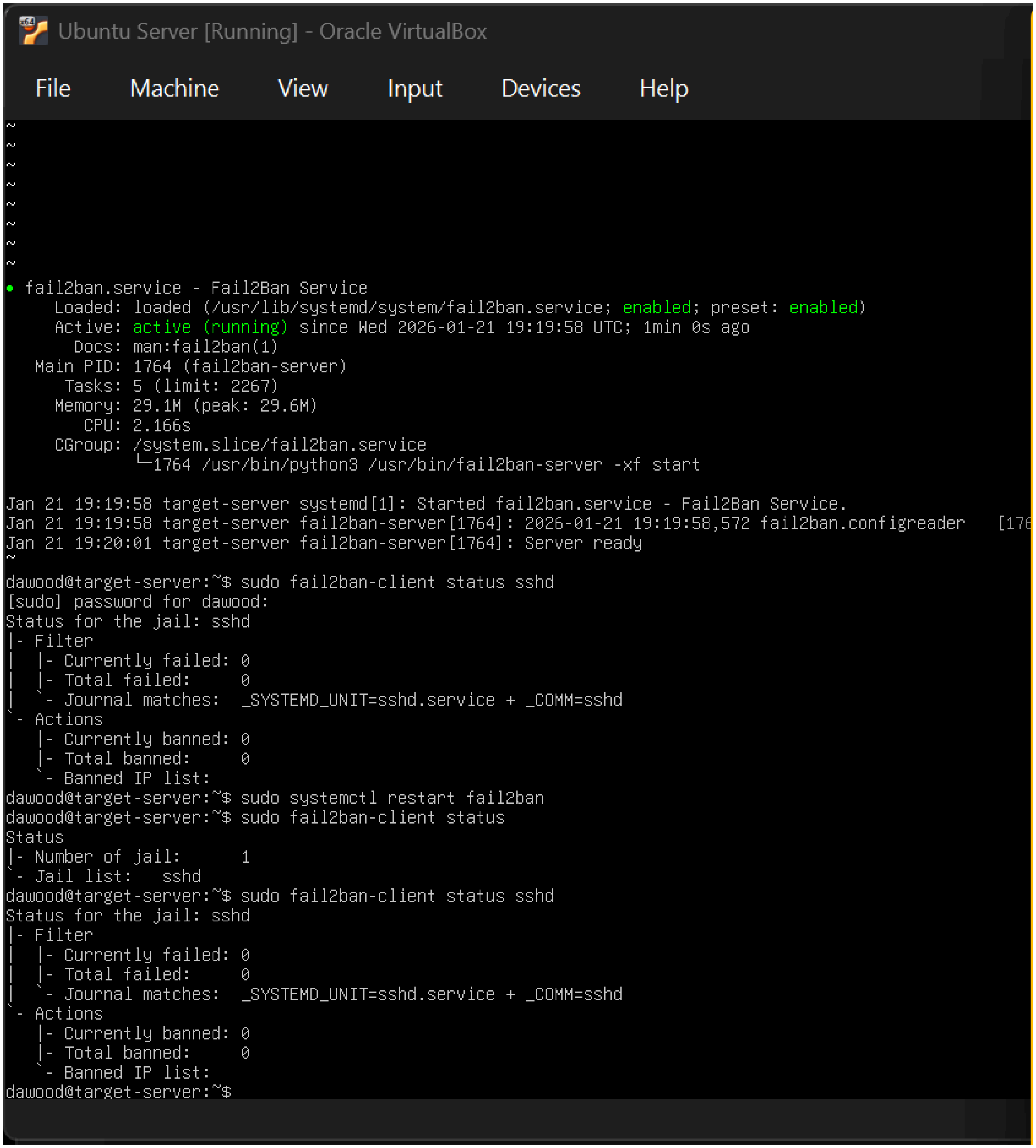
```
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Wed 2026-01-21 19:19:58 UTC; 1min 0s ago
       Docs: man:fail2ban(1)
   Main PID: 1764 (fail2ban-server)
      Tasks: 5 (limit: 2267)
     Memory: 29.1M (peak: 29.6M)
        CPU: 2.166s
     CGroup: /system.slice/fail2ban.service
             └─1764 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Jan 21 19:19:58 target-server systemd[1]: Started fail2ban.service - Fail2Ban Service.
Jan 21 19:19:58 target-server fail2ban-server[1764]: 2026-01-21 19:19:58,572 fail2ban.configreader   [1
Jan 21 19:20:01 target-server fail2ban-server[1764]: Server ready
~
dawood@target-server:~$ sudo fail2ban-client status sshd
[sudo] password for dawood:
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
dawood@target-server:~$ _
```

STEP 4: Restart Fail2Ban

In this we have check the whether it is working or not now we have to check banned 0 and jail sshd
The command we are using in this is (sudo systemctl restart fail2ban)

(sudo fail2ban-client status)
After these command we have check status then we will enter this command (sudo fail2ban-client status sshd)

Proof

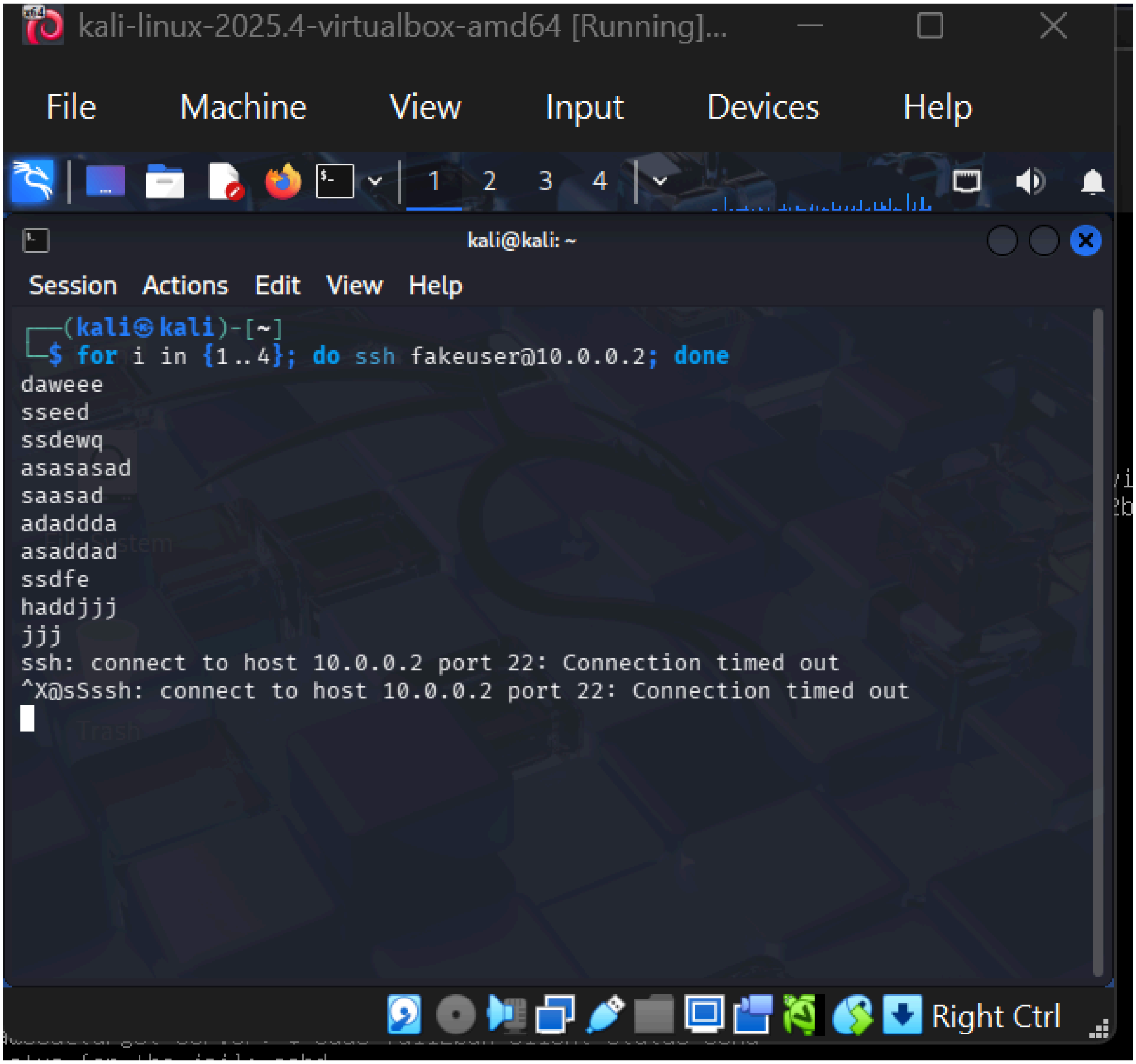


```
~
~
~
~
~
~
~
~
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Wed 2026-01-21 19:19:58 UTC; 1min 0s ago
       Docs: man:fail2ban(1)
   Main PID: 1764 (fail2ban-server)
      Tasks: 5 (limit: 2267)
     Memory: 29.1M (peak: 29.6M)
        CPU: 2.166s
     CGroup: /system.slice/fail2ban.service
             └─1764 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Jan 21 19:19:58 target-server systemd[1]: Started fail2ban.service - Fail2Ban Service.
Jan 21 19:19:58 target-server fail2ban-server[1764]: 2026-01-21 19:19:58,572 fail2ban.configreader   [176
Jan 21 19:20:01 target-server fail2ban-server[1764]: Server ready
~
dawood@target-server:~$ sudo fail2ban-client status sshd
[sudo] password for dawood:
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
dawood@target-server:~$ sudo systemctl restart fail2ban
dawood@target-server:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
dawood@target-server:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
dawood@target-server:~$
```

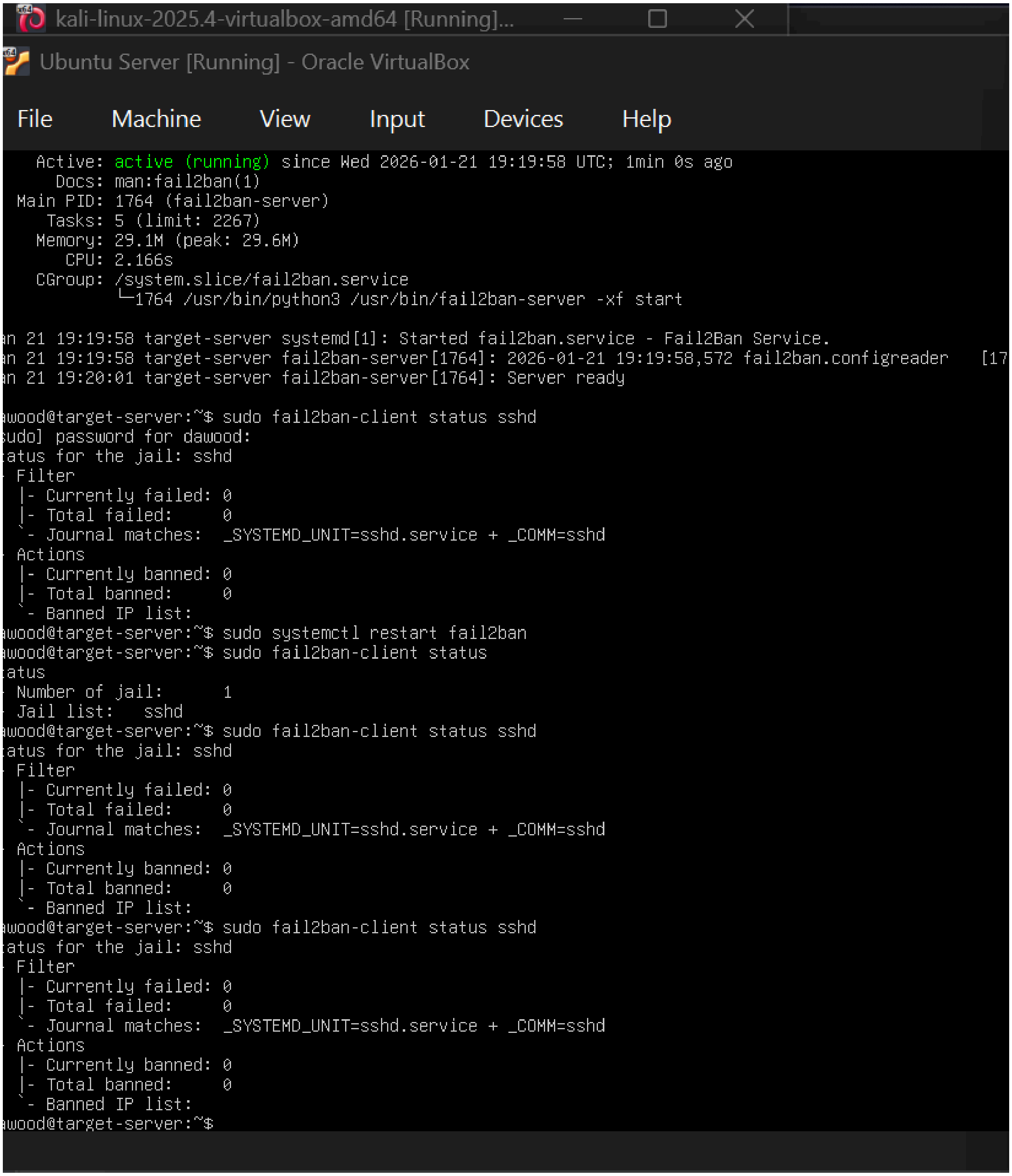
STEP 5: Trigger the Ban (Attack)

In this step we will change terminal to kali and start our testing process by attacking
The command we are using in this (for i in {1..4}; do ssh fakeuser@<UBUNTU-IP>; done)
After that we will enter fake password to check the working

Proof



```
┌──(kali㉿kali)-[~]
└─$ for i in {1..4}; do ssh fakeuser@10.0.0.2; done
daweee
sseed
ssdewq
asasasad
saasad
adaddda
asaddad
ssdfe
haddjjj
jjj
ssh: connect to host 10.0.0.2 port 22: Connection timed out
^X@sSssh: connect to host 10.0.0.2 port 22: Connection timed out
```


kali-linux-2025.4-virtualbox-amd64 [Running]...
Ubuntu Server [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help

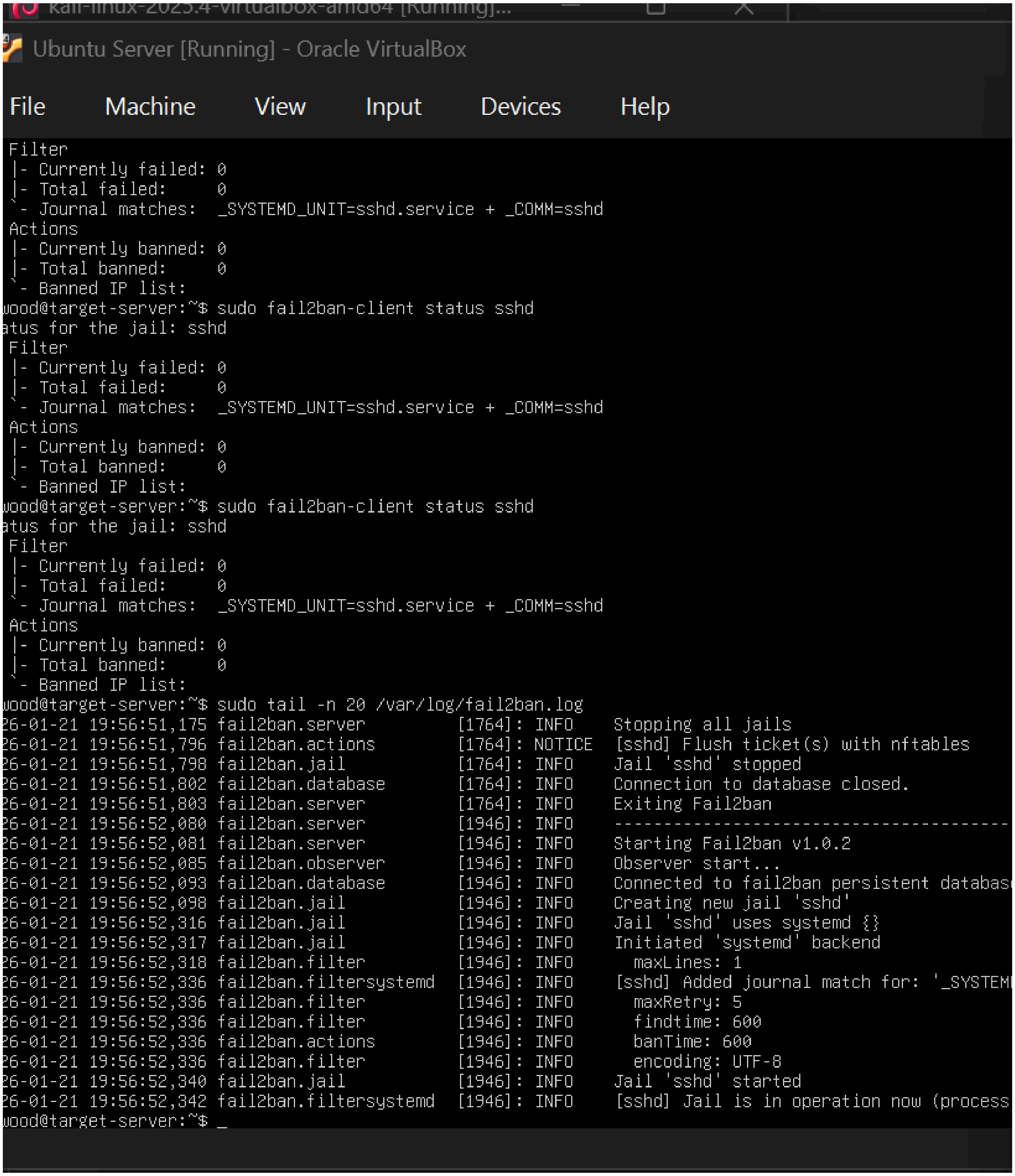
```
   Active: active (running) since Wed 2026-01-21 19:19:58 UTC; 1min 0s ago
     Docs: man:fail2ban(1)
 Main PID: 1764 (fail2ban-server)
    Tasks: 5 (limit: 2267)
   Memory: 29.1M (peak: 29.6M)
      CPU: 2.166s
   CGroup: /system.slice/fail2ban.service
           └─1764 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

an 21 19:19:58 target-server systemd[1]: Started fail2ban.service - Fail2Ban Service.
an 21 19:19:58 target-server fail2ban-server[1764]: 2026-01-21 19:19:58,572 fail2ban.configreader   [17
an 21 19:20:01 target-server fail2ban-server[1764]: Server ready

awood@target-server:~$ sudo fail2ban-client status sshd
sudo] password for dawood:
atus for the jail: sshd
- Filter
 |- Currently failed: 0
 |- Total failed:     0
 `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
 |- Currently banned: 0
 |- Total banned:     0
 `- Banned IP list:
awood@target-server:~$ sudo systemctl restart fail2ban
awood@target-server:~$ sudo fail2ban-client status
atus
- Number of jail:      1
- Jail list:   sshd
awood@target-server:~$ sudo fail2ban-client status sshd
atus for the jail: sshd
- Filter
 |- Currently failed: 0
 |- Total failed:     0
 `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
 |- Currently banned: 0
 |- Total banned:     0
 `- Banned IP list:
awood@target-server:~$ sudo fail2ban-client status sshd
atus for the jail: sshd
- Filter
 |- Currently failed: 0
 |- Total failed:     0
 `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
 |- Currently banned: 0
 |- Total banned:     0
 `- Banned IP list:
awood@target-server:~$
```

STEP 6: Confirm the Ban (Proof)

In this step we will go back to ubuntu terminal and check the status
For the status checking we will use this command (sudo fail2ban-client status

sshd)then we will also check log from this command (sudo tail -n 20 /var/log/fail2ban.log)

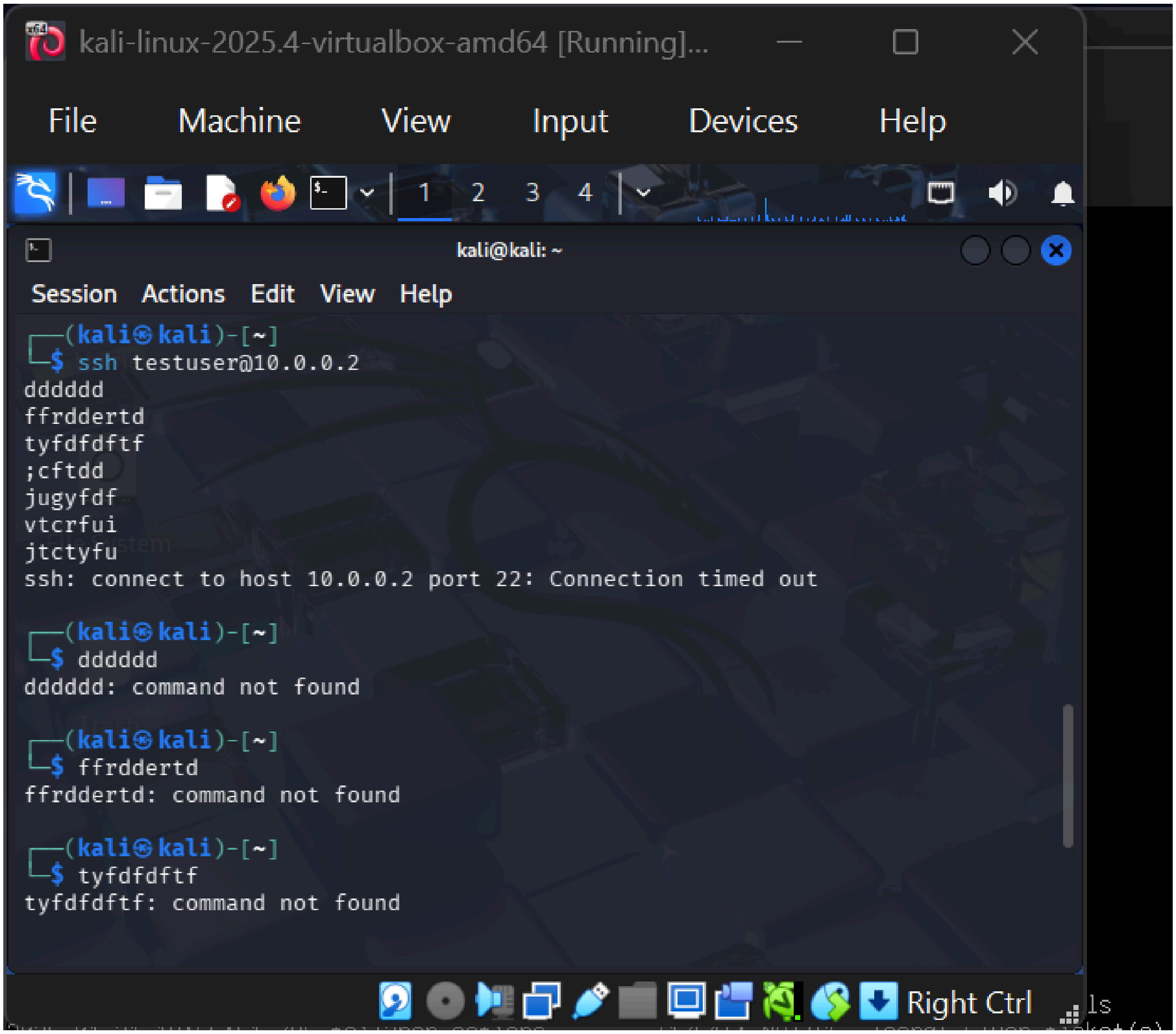
Proof


kali-linux-2025.4-virtualbox-amd64 [Running]...
Ubuntu Server [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help

```
 Filter
 |- Currently failed: 0
 |- Total failed:     0
 `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
 Actions
 |- Currently banned: 0
 |- Total banned:     0
 `- Banned IP list:
wood@target-server:~$ sudo fail2ban-client status sshd
atus for the jail: sshd
 Filter
 |- Currently failed: 0
 |- Total failed:     0
 `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
 Actions
 |- Currently banned: 0
 |- Total banned:     0
 `- Banned IP list:
wood@target-server:~$ sudo fail2ban-client status sshd
atus for the jail: sshd
 Filter
 |- Currently failed: 0
 |- Total failed:     0
 `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
 Actions
 |- Currently banned: 0
 |- Total banned:     0
 `- Banned IP list:
wood@target-server:~$ sudo tail -n 20 /var/log/fail2ban.log
26-01-21 19:56:51,175 fail2ban.server         [1764]: INFO    Stopping all jails
26-01-21 19:56:51,796 fail2ban.actions        [1764]: NOTICE  [sshd] Flush ticket(s) with nftables
26-01-21 19:56:51,798 fail2ban.jail           [1764]: INFO    Jail 'sshd' stopped
26-01-21 19:56:51,802 fail2ban.database       [1764]: INFO    Connection to database closed.
26-01-21 19:56:51,803 fail2ban.server         [1764]: INFO    Exiting Fail2ban
26-01-21 19:56:52,080 fail2ban.server         [1946]: INFO    ----------------------------------------
26-01-21 19:56:52,081 fail2ban.server         [1946]: INFO    Starting Fail2ban v1.0.2
26-01-21 19:56:52,085 fail2ban.observer       [1946]: INFO    Observer start...
26-01-21 19:56:52,093 fail2ban.database       [1946]: INFO    Connected to fail2ban persistent databas
26-01-21 19:56:52,098 fail2ban.jail           [1946]: INFO    Creating new jail 'sshd'
26-01-21 19:56:52,316 fail2ban.jail           [1946]: INFO    Jail 'sshd' uses systemd {}
26-01-21 19:56:52,317 fail2ban.jail           [1946]: INFO    Initiated 'systemd' backend
26-01-21 19:56:52,318 fail2ban.filter         [1946]: INFO      maxLines: 1
26-01-21 19:56:52,336 fail2ban.filtersystemd  [1946]: INFO    [sshd] Added journal match for: '_SYSTEM
26-01-21 19:56:52,336 fail2ban.filter         [1946]: INFO      maxRetry: 5
26-01-21 19:56:52,336 fail2ban.filter         [1946]: INFO      findtime: 600
26-01-21 19:56:52,336 fail2ban.actions        [1946]: INFO      banTime: 600
26-01-21 19:56:52,336 fail2ban.filter         [1946]: INFO      encoding: UTF-8
26-01-21 19:56:52,340 fail2ban.jail           [1946]: INFO    Jail 'sshd' started
26-01-21 19:56:52,342 fail2ban.filtersystemd  [1946]: INFO    [sshd] Jail is in operation now (process
wood@target-server:~$ _
```

STEP 7: Verify Attack is Blocked

In this step we have to verify the attack that has been blocked
By looking connection timeout
The command we are using in it is (ssh testuser@<UBUNTU-IP>)
Proof



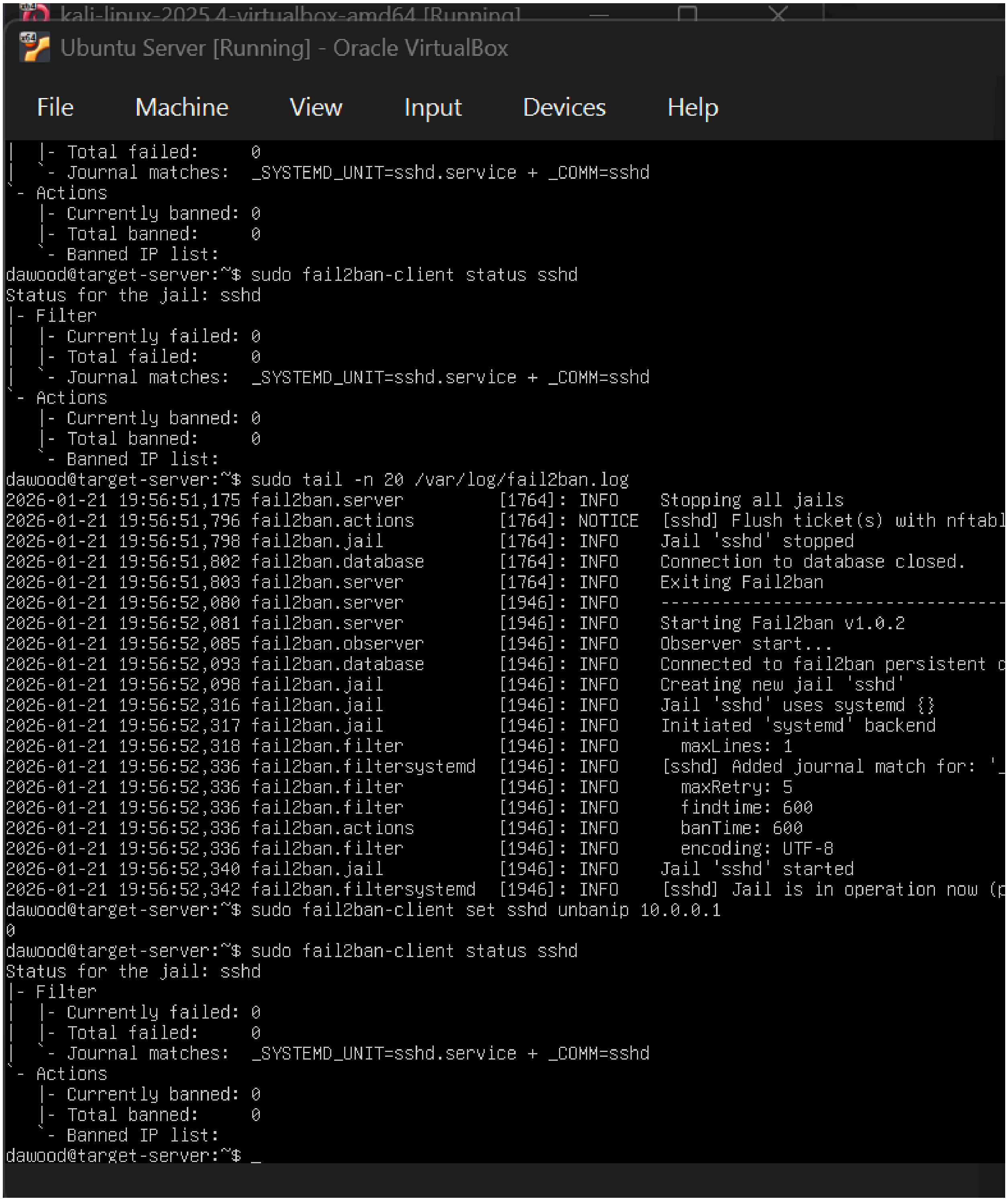
```
┌──(kali㉿kali)-[~]
└─$ ssh testuser@10.0.0.2
dddddd
ffrddertd
tyfdfdftf
;cftdd
jugyfdf
vtcrfui
jtctyfu
ssh: connect to host 10.0.0.2 port 22: Connection timed out

┌──(kali㉿kali)-[~]
└─$ dddddd
dddddd: command not found

┌──(kali㉿kali)-[~]
└─$ ffrddertd
ffrddertd: command not found

┌──(kali㉿kali)-[~]
└─$ tyfdfdftf
tyfdfdftf: command not found
```

STEP 8: (Optional) Unban Yourself

In this step we are giving mercy on attacker we going unblock them to reentering in the system

The command we are using in this is (sudo fail2ban-client set sshd unbanip <KALI-IP>)

Proof


kali-linux-2025.4-virtualbox-amd64 [Running]
Ubuntu Server [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help

```
|   |- Total failed:     0
|   `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
    |- Currently banned: 0
    |- Total banned:     0
    `- Banned IP list:
dawood@target-server:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed:     0
|   `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
    |- Currently banned: 0
    |- Total banned:     0
    `- Banned IP list:
dawood@target-server:~$ sudo tail -n 20 /var/log/fail2ban.log
2026-01-21 19:56:51,175 fail2ban.server         [1764]: INFO    Stopping all jails
2026-01-21 19:56:51,796 fail2ban.actions        [1764]: NOTICE  [sshd] Flush ticket(s) with nftabl
2026-01-21 19:56:51,798 fail2ban.jail           [1764]: INFO    Jail 'sshd' stopped
2026-01-21 19:56:51,802 fail2ban.database       [1764]: INFO    Connection to database closed.
2026-01-21 19:56:51,803 fail2ban.server         [1764]: INFO    Exiting Fail2ban
2026-01-21 19:56:52,080 fail2ban.server         [1946]: INFO    ----------------------------------
2026-01-21 19:56:52,081 fail2ban.server         [1946]: INFO    Starting Fail2ban v1.0.2
2026-01-21 19:56:52,085 fail2ban.observer       [1946]: INFO    Observer start...
2026-01-21 19:56:52,093 fail2ban.database       [1946]: INFO    Connected to fail2ban persistent d
2026-01-21 19:56:52,098 fail2ban.jail           [1946]: INFO    Creating new jail 'sshd'
2026-01-21 19:56:52,316 fail2ban.jail           [1946]: INFO    Jail 'sshd' uses systemd {}
2026-01-21 19:56:52,317 fail2ban.jail           [1946]: INFO    Initiated 'systemd' backend
2026-01-21 19:56:52,318 fail2ban.filter         [1946]: INFO      maxLines: 1
2026-01-21 19:56:52,336 fail2ban.filtersystemd  [1946]: INFO    [sshd] Added journal match for: '_
2026-01-21 19:56:52,336 fail2ban.filter         [1946]: INFO      maxRetry: 5
2026-01-21 19:56:52,336 fail2ban.filter         [1946]: INFO      findtime: 600
2026-01-21 19:56:52,336 fail2ban.actions        [1946]: INFO      banTime: 600
2026-01-21 19:56:52,336 fail2ban.filter         [1946]: INFO      encoding: UTF-8
2026-01-21 19:56:52,340 fail2ban.jail           [1946]: INFO    Jail 'sshd' started
2026-01-21 19:56:52,342 fail2ban.filtersystemd  [1946]: INFO    [sshd] Jail is in operation now (p
dawood@target-server:~$ sudo fail2ban-client set sshd unbanip 10.0.0.1
0
dawood@target-server:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed:     0
|   `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
    |- Currently banned: 0
    |- Total banned:     0
    `- Banned IP list:
dawood@target-server:~$ _
```

Step	Command	What it does (Purpose)
Precheck	sudo systemctl status ssh	Confirms the "door" (SSH) is open before we start.
Step 1	sudo apt install fail2ban -y	Downloads and installs the "Bouncer" software.
Step 2	sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local	Creates a safe copy of the rules so we don't break the original.
Step 2	sudo nano /etc/fail2ban/jail.local	Opens the rulebook so we can type our 3-strike policy.
Step 4	sudo systemctl restart fail2ban	Forces the Bouncer to wake up and read the new rules.
Step 4	sudo fail2ban-client status sshd	Asks the Bouncer: "Who are you watching and who is banned?".
Step 5	for i in {1..4}; do ssh user@IP; done	The "Attack" command used on Kali to trigger the ban.
Step 6	sudo tail -n 20 /var/log/fail2ban.log	Shows the secret security logs where the "Ban" is recorded.

Step 8	sudo fail2ban-client set sshd unbanip <IP>	The "Mercy" command to let a blocked user back in.