

## Day 3 – Traffic Control & Firewall Hardening (UFW)

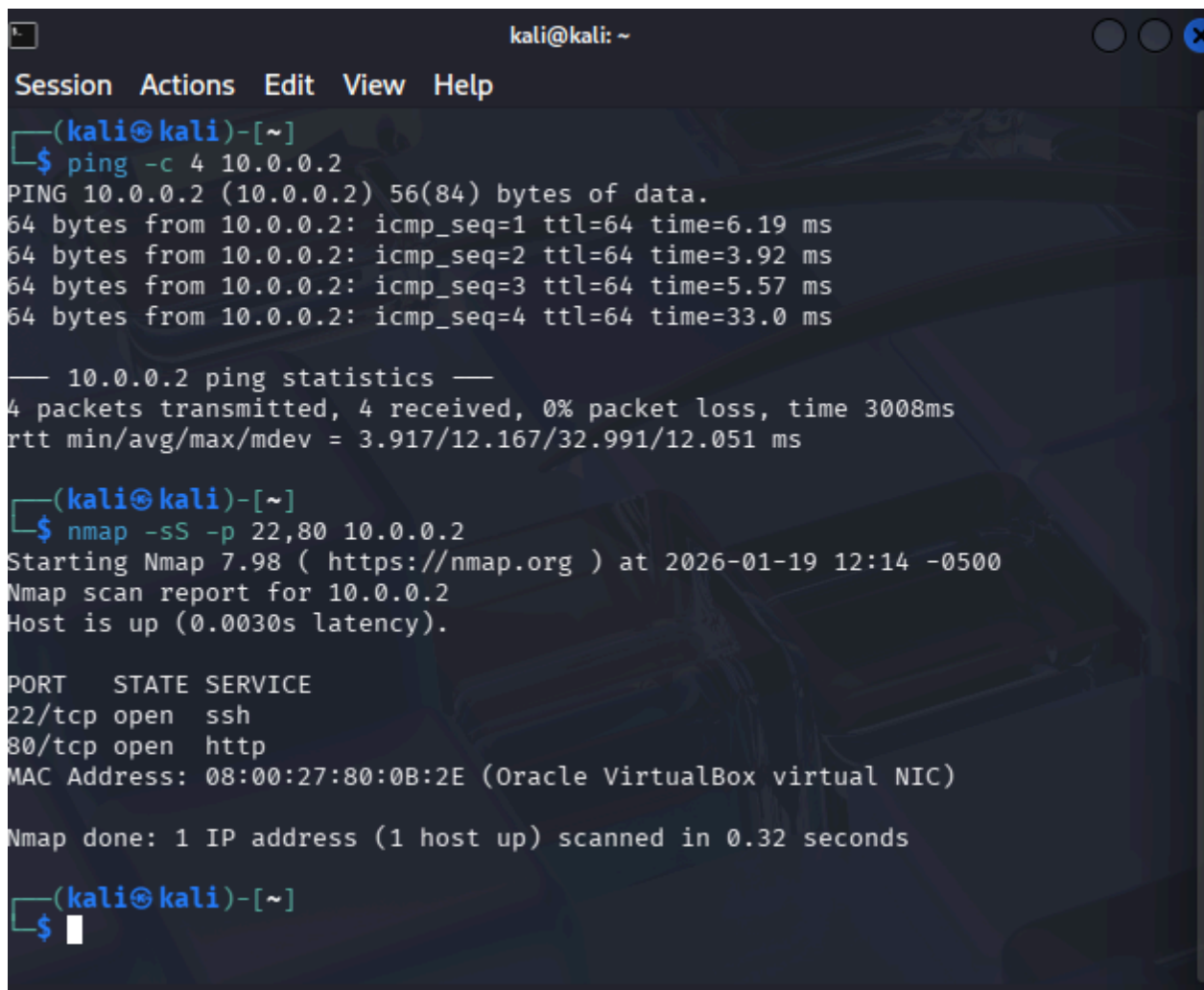
### Mindset today:

You are defending a server in a real company.  
Nothing is trusted. Everything must be proven.

### STEP 1: Baseline Scan (PROOF OF INSECURITY):

The command we have use in step 1 is nmap(network mapper) to find the open ports  
(Nmap -sS -p 22,80 10.0.0.2) :(-sS is stealth scan (fast n quite) -p this tell nmap to check only two ports 20,80,and my target is (10.0.0.2)ubuntu

Proof:

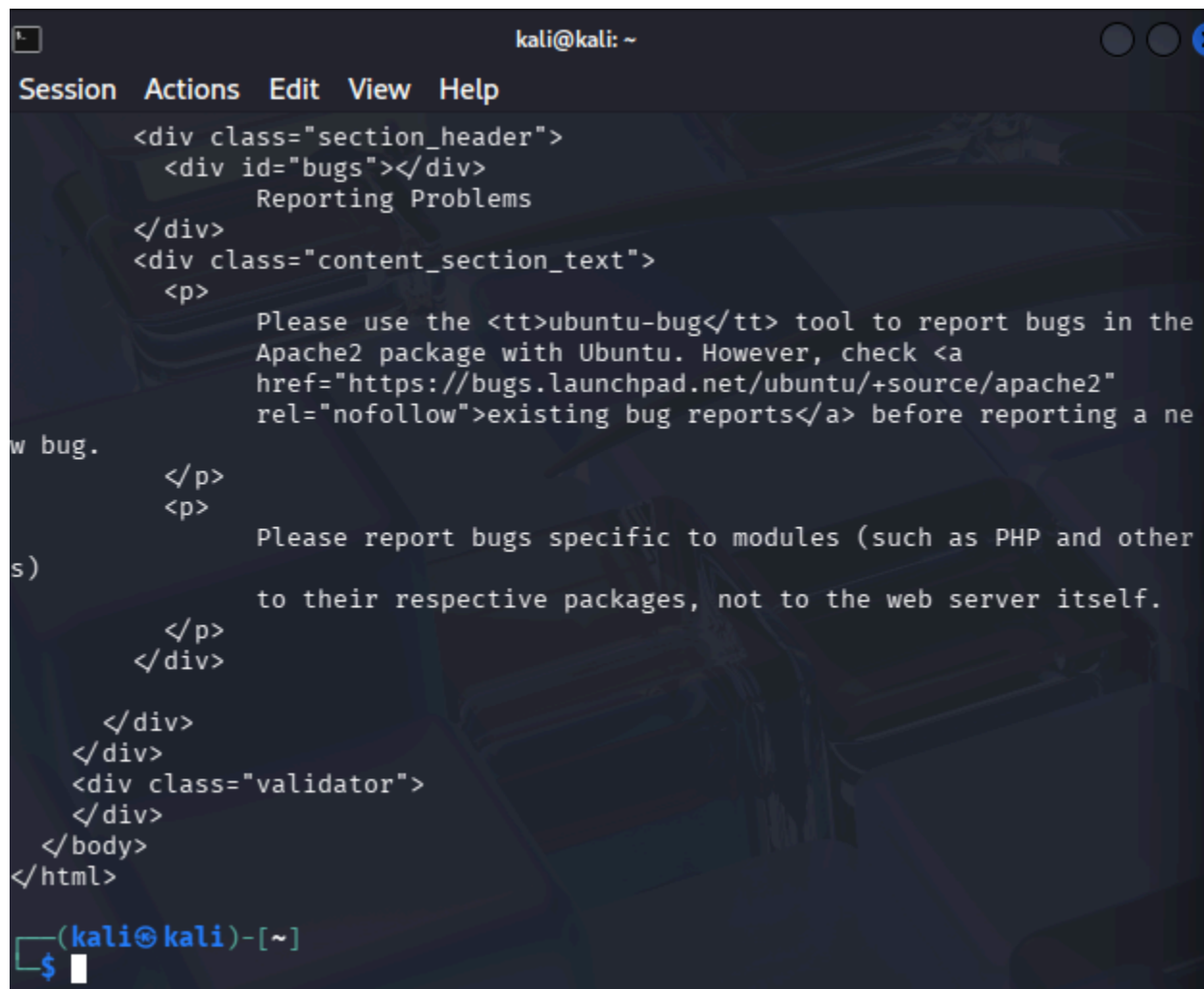
A terminal window titled 'kali@kali: ~' showing the execution of network scanning commands. The first command is 'ping -c 4 10.0.0.2', which shows four successful ping responses with varying times. The second command is 'nmap -sS -p 22,80 10.0.0.2', which shows the Nmap scan report for 10.0.0.2, indicating that ports 22/tcp (ssh) and 80/tcp (http) are open. The terminal output is as follows:

```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ ping -c 4 10.0.0.2  
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.  
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=6.19 ms  
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=3.92 ms  
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=5.57 ms  
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=33.0 ms  
  
— 10.0.0.2 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3008ms  
rtt min/avg/max/mdev = 3.917/12.167/32.991/12.051 ms  
  
(kali@kali)-[~]  
$ nmap -sS -p 22,80 10.0.0.2  
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-19 12:14 -0500  
Nmap scan report for 10.0.0.2  
Host is up (0.0030s 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 0.32 seconds  
  
(kali@kali)-[~]  
$
```

### STEP 2: Confirm Web Access (Kali)

The command we are using in this is( curl <http://10.0.0.2>)  
(curl) client url ,this tools act like a web browser in terminal to capture websites data

Proof



The screenshot shows a terminal window with a dark background. At the top, the prompt is 'kali@kali: ~'. Below it is a menu bar with 'Session', 'Actions', 'Edit', 'View', and 'Help'. The main content is a block of HTML code. It starts with a 'div' class 'section\_header' containing a 'div' id 'bugs' with the text 'Reporting Problems'. This is followed by another 'div' class 'content\_section\_text' containing two paragraphs. The first paragraph says: 'Please use the <tt>ubuntu-bug</tt> tool to report bugs in the Apache2 package with Ubuntu. However, check <a href="https://bugs.launchpad.net/ubuntu/+source/apache2" rel="nofollow">existing bug reports</a> before reporting a new bug.' The second paragraph says: 'Please report bugs specific to modules (such as PHP and others) to their respective packages, not to the web server itself.' The code ends with closing tags for the 'div' elements and the 'html' body. At the bottom, the prompt is '(kali@kali)-[~]' followed by a '\$' and a cursor.

```
kali@kali: ~
Session Actions Edit View Help
<div class="section_header">
  <div id="bugs"></div>
    Reporting Problems
  </div>
  <div class="content_section_text">
    <p>
      Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
      Apache2 package with Ubuntu. However, check <a
      href="https://bugs.launchpad.net/ubuntu/+source/apache2"
      rel="nofollow">existing bug reports</a> before reporting a ne
      w bug.
    </p>
    <p>
      Please report bugs specific to modules (such as PHP and other
      s)
      to their respective packages, not to the web server itself.
    </p>
  </div>
</div>
</div>
<div class="validator">
</div>
</body>
</html>
(kali@kali)-[~]
$
```

STEP 3: Move to Defense (Ubuntu)

The command we are using is (sudo ufw status)

ufw(uncomplicated firewall)

**Mission Report:** Run that command on Ubuntu now. Does it say **Status: inactive?**

**Proof:**

```
File Machine View Input Devices Help

Ubuntu 24.04.3 LTS target-server tty1

target-server login: dawood
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

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

System information as of Sun 18 Jan 18:51:09 UTC 2026

System load: 0.0          Memory usage: 10%   Processes:    118
Usage of /:  41.0% of 11.21GB Swap usage:   0%     Users logged in: 1

Expanded Security Maintenance for Applications is not enabled.

57 updates can be applied immediately.
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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings.

dawood@target-server:~$ sudo ufw status
[sudo] password for dawood:
Status: inactive
dawood@target-server:~$ _
```

#### STEP 4: Enable Firewall (CRITICAL MOMENT)

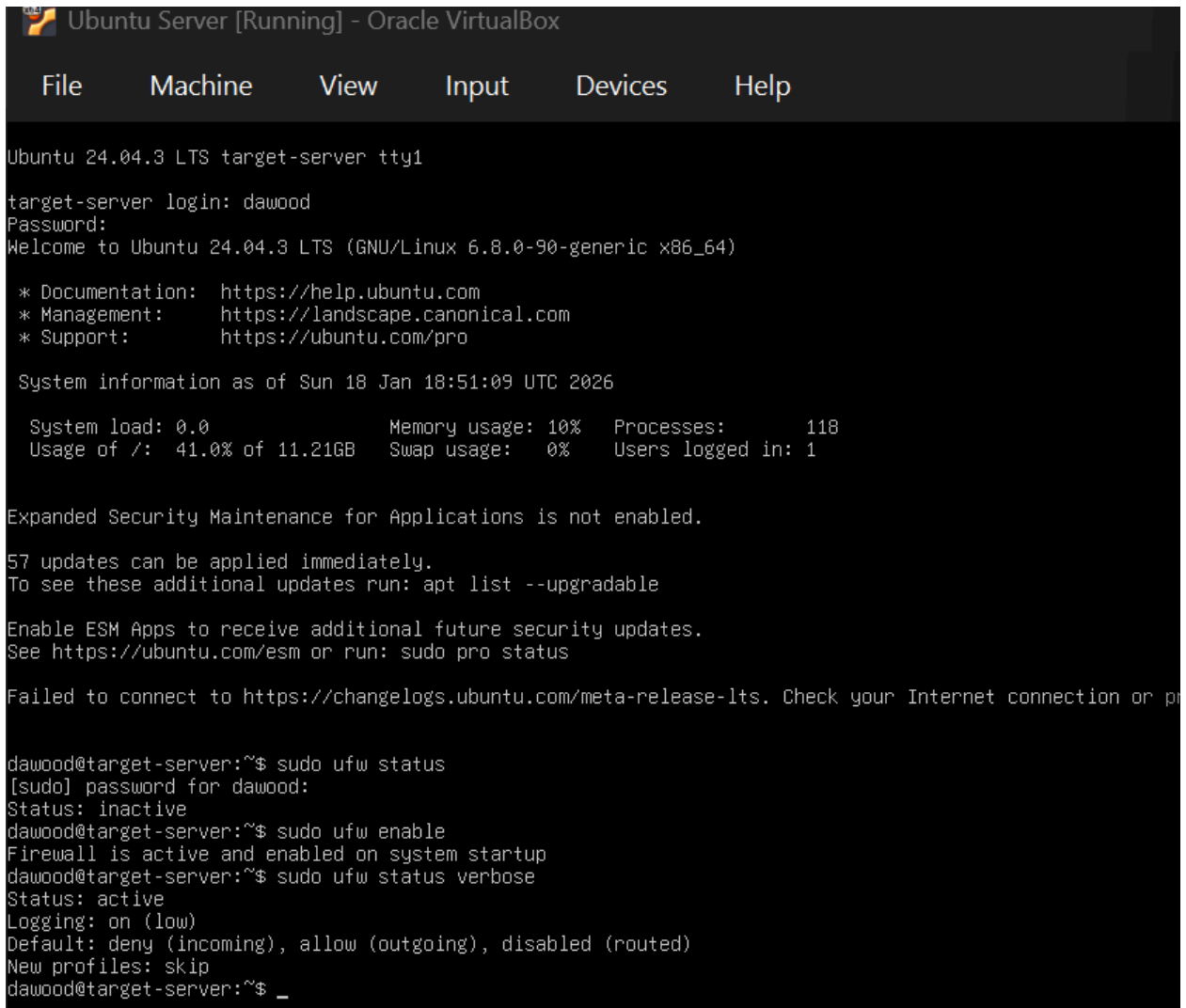
The command we are using is (sudo ufw enable)

To see full detail use this command (sudo ufw status verbose)

Look closely at the output to confirm these three things:

- Status: **active**
- Logging: **on (low)** (usually)
- Default: **deny (incoming), allow (outgoing), disabled (routed)**

## Proof



```
Ubuntu 24.04.3 LTS target-server tty1
target-server login: dawood
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

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

System information as of Sun 18 Jan 18:51:09 UTC 2026

System load: 0.0               Memory usage: 10%   Processes:      118
Usage of /:  41.0% of 11.21GB  Swap usage:   0%   Users logged in: 1

Expanded Security Maintenance for Applications is not enabled.

57 updates can be applied immediately.
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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings.

dawood@target-server:~$ sudo ufw status
[sudo] password for dawood:
Status: inactive
dawood@target-server:~$ sudo ufw enable
Firewall is active and enabled on system startup
dawood@target-server:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
dawood@target-server:~$ _
```

## STEP 5: Test the Block (ATTACK FAILS)

The command we are using in this is (nmap -p 80 10.0.0.2)

**The Tool Nmap & Curl** — We use the same tools as before to show the difference between "Unprotected" and "Protected".

Now user experience verification(curl) command is (curl --connect-timeout 10 <http://10.0.0.2>)

## Proof

```
kali@kali: ~
Session Actions Edit View Help

</div>

</div>
</div>
<div class="validator">
</div>
</body>
</html>

(kali@kali)-[~]
$ nmap -p 80 10.0.0.2
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-19 12:35 -0500
Nmap scan report for 10.0.0.2
Host is up (0.0021s latency).

PORT      STATE      SERVICE
80/tcp    filtered  http
MAC Address: 08:00:27:80:0B:2E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds

(kali@kali)-[~]
$ curl --connect-timeout 10 http://10.0.0.2
curl: option --connect-timeout: is unknown
curl: try 'curl --help' or 'curl --manual' for more information

(kali@kali)-[~]
$
```

## STEP 6: Allow HTTP (CONTROLLED ACCESS)

The command we are using in this is (sudo ufw allow 80/tcp)

The command we use for active rule is (sudo ufw status)

📌 **The Tool UFW (Uncomplicated Firewall)** — We are adding a specific "Allow" exception to the "Default Deny" wall you built in Step 4.

Proof

```
File      Machine  View    Input   Devices  Help

Ubuntu 24.04.3 LTS target-server tty1

target-server login: dawood
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

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

System information as of Sun 18 Jan 18:51:09 UTC 2026

System load: 0.0           Memory usage: 10%    Processes:      118
Usage of /:  41.0% of 11.21GB Swap usage:   0%    Users logged in: 1

Expanded Security Maintenance for Applications is not enabled.

57 updates can be applied immediately.
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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings.

dawood@target-server:~$ sudo ufw status
[sudo] password for dawood:
Status: inactive
dawood@target-server:~$ sudo ufw enable
Firewall is active and enabled on system startup
dawood@target-server:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
dawood@target-server:~$ sudo ufw allow 80/tcp
Rule added
Rule added (v6)
dawood@target-server:~$ sudo ufw status
Status: active

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

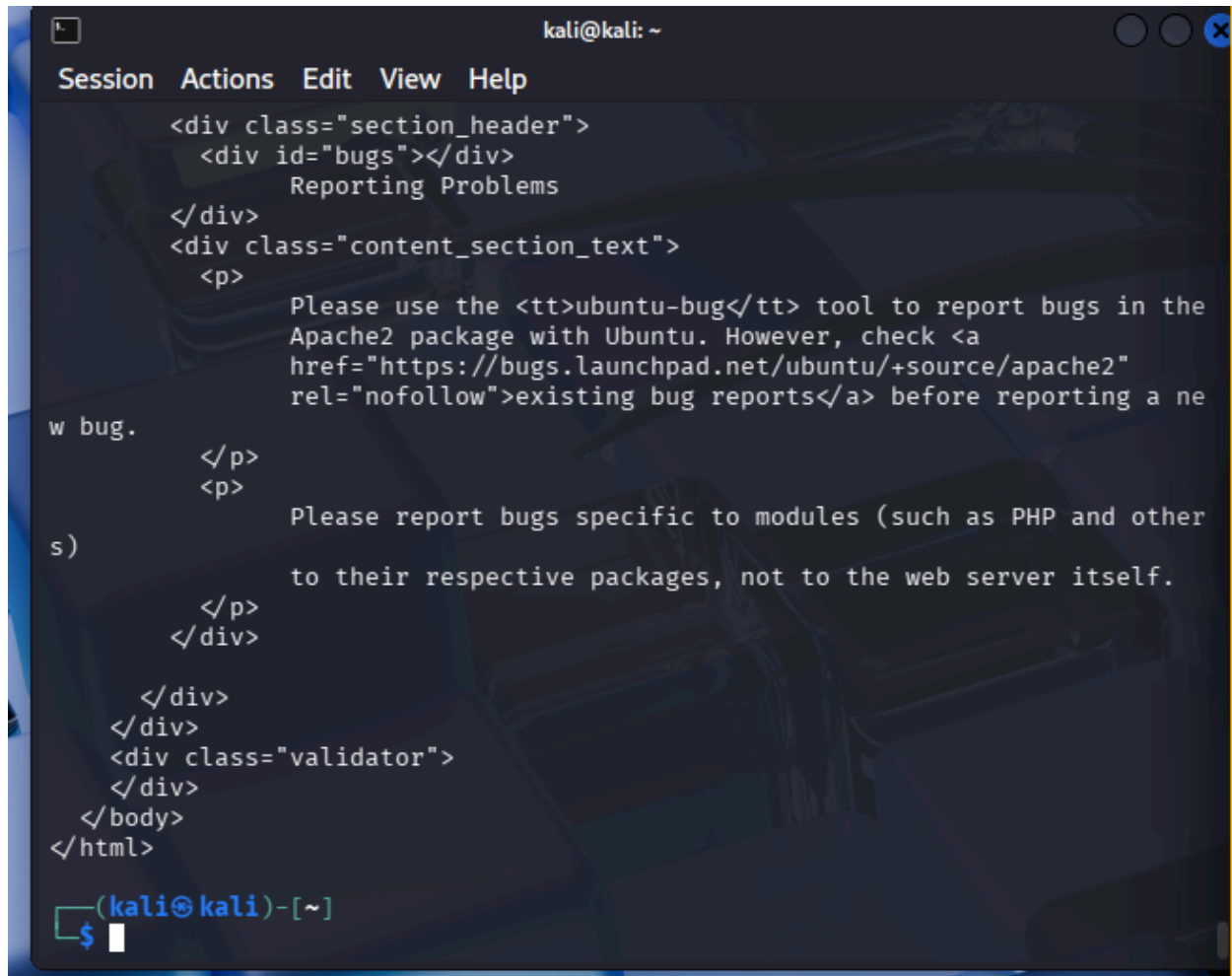
dawood@target-server:~$ _
```

## STEP 7: Retest Access (CONTROL RESTORED)

The command we use is (curl <http://10.0.0.2>)

🔴 **The Tool curl** — You are using this to prove that the "Allow" rule you just created on Ubuntu is working.

Proof



```
kali@kali: ~  
Session Actions Edit View Help  
<div class="section_header">  
  <div id="bugs"></div>  
    Reporting Problems  
</div>  
<div class="content_section_text">  
  <p>  
    Please use the <tt>ubuntu-bug</tt> tool to report bugs in the  
    Apache2 package with Ubuntu. However, check <a  
    href="https://bugs.launchpad.net/ubuntu/+source/apache2"  
    rel="nofollow">existing bug reports</a> before reporting a ne  
w bug.  
  </p>  
  <p>  
    Please report bugs specific to modules (such as PHP and other  
s)  
    to their respective packages, not to the web server itself.  
  </p>  
</div>  
</div>  
</div>  
<div class="validator">  
</div>  
</body>  
</html>  
(kali@kali)-[~]  
$
```

#### STEP 8: Restrict Access (ENGINEER MOVE)

The command we are using is (sudo ufw delete allow 80/tcp)

After this now we will create specialized rule that only kali vm to see (sudo ufw allow from 10.0.0.1 from any port 80 proto tcp)

The command to see configuration (sudo ufw status)

📌 **The Concept** Instead of saying "Everyone can see my website," you are saying "Only the administrator at IP 10.0.0.1 (Kali) can see my website". Everyone else on the network will still see a brick wall.

Proof

```
Ubuntu Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

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

System information as of Sun 18 Jan 18:51:09 UTC 2026

System load: 0.0          Memory usage: 10%   Processes:      118
Usage of /:  41.0% of 11.21GB Swap usage:   0%       Users logged in: 1

Expanded Security Maintenance for Applications is not enabled.

57 updates can be applied immediately.
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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings.

dawood@target-server:~$ sudo ufw status
[sudo] password for dawood:
Status: inactive
dawood@target-server:~$ sudo ufw enable
Firewall is active and enabled on system startup
dawood@target-server:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
dawood@target-server:~$ sudo ufw allow 80/tcp
Rule added
Rule added (v6)
dawood@target-server:~$ sudo ufw status
Status: active

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

dawood@target-server:~$ sudo ufw delete allow 80/tcp
Rule deleted
Rule deleted (v6)
dawood@target-server:~$ sudo ufw allow from 10.0.0.1 to any port 80 proto tcp
Rule added
dawood@target-server:~$ _
```

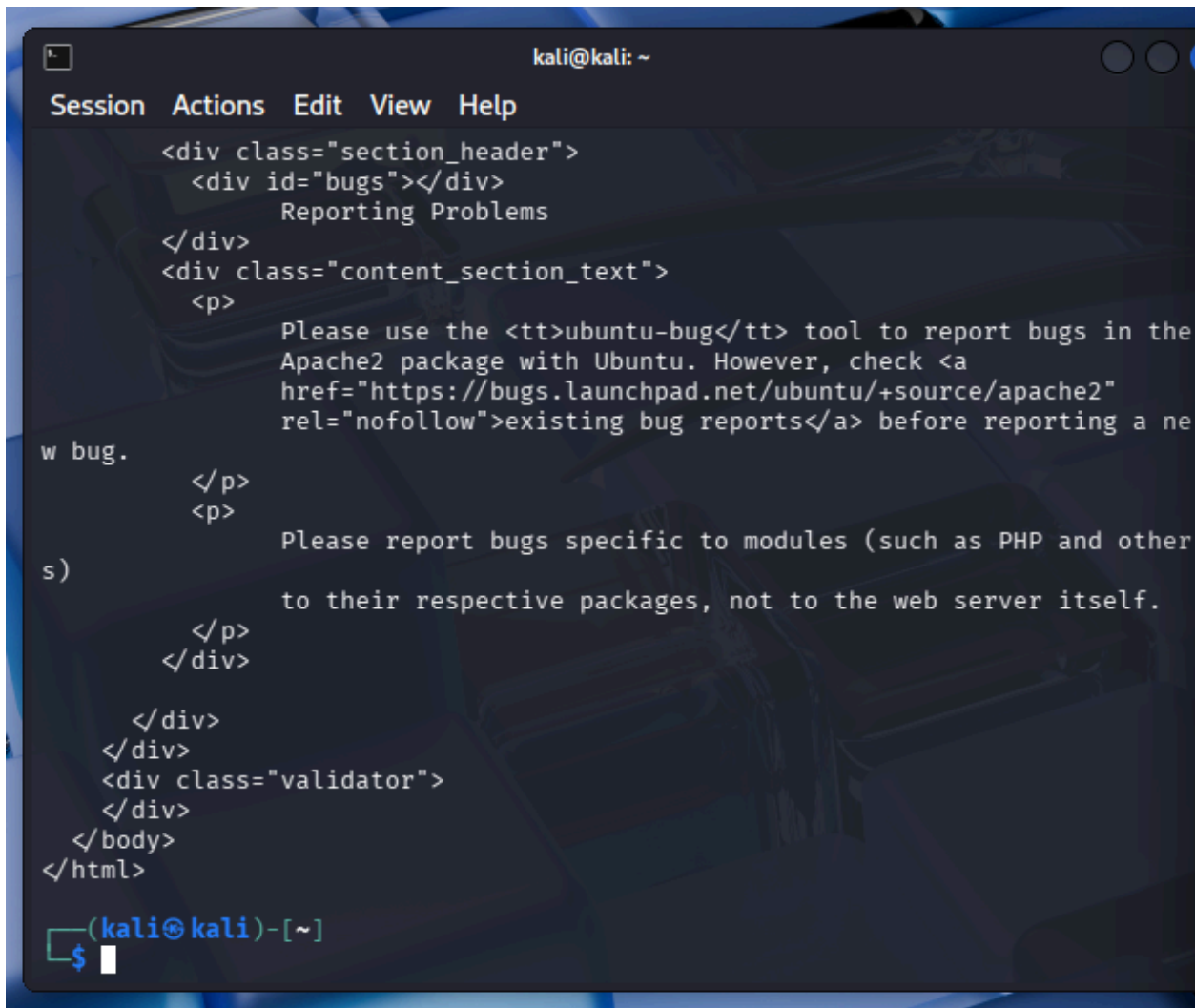
## STEP 9: Final Proof (CONTROLLED SECURITY)

The command we are using is (curl <http://10.0.0.2>)

📌 **The Concept** In Step 8, you told the firewall: "Only talk to 10.0.0.1 (Kali)". Now, we confirm that Kali still has its special "VIP" access while everyone else is locked out.



Proof



```
kali@kali: ~  
Session Actions Edit View Help  
<div class="section_header">  
  <div id="bugs"></div>  
    Reporting Problems  
</div>  
<div class="content_section_text">  
  <p>  
    Please use the <tt>ubuntu-bug</tt> tool to report bugs in the  
    Apache2 package with Ubuntu. However, check <a  
      href="https://bugs.launchpad.net/ubuntu/+source/apache2"  
      rel="nofollow">existing bug reports</a> before reporting a ne  
w bug.  
  </p>  
  <p>  
    Please report bugs specific to modules (such as PHP and other  
s)  
    to their respective packages, not to the web server itself.  
  </p>  
</div>  
</div>  
</div>  
<div class="validator">  
</div>  
</body>  
</html>  
(kali@kali)-[~]  
$
```

Step	Task Name	Command Executed	Goal / Purpose	Result (Success Proof)

1	<b>Baseline Scan</b>	<code>nmap -sS -p 22,80 10.0.0.2</code>	Find open doors before security	<b>Success:</b> Port 22 & 80 shown as <code>open</code>
2	<b>Service Audit</b>	<code>curl http://10.0.0.2</code>	Confirm web server is reachable	<b>Success:</b> Raw HTML code received
3	<b>Health Check</b>	<code>sudo ufw status</code>	Check initial firewall state	<b>Success:</b> Status confirmed as <code>inactive</code>
4	<b>Shield Up</b>	<code>sudo ufw enable</code>	Activate the system's defense	<b>Success:</b> Firewall is <code>active &amp; deny incoming</code>
5	<b>Attack Test</b>	<code>nmap -p 80 10.0.0.2</code>	Verify that firewall blocks access	<b>Success:</b> Port 80 shown as <code>filtered</code>
6	<b>Open Access</b>	<code>sudo ufw allow 80/tcp</code>	Allow everyone to see the site	<b>Success:</b> Rule added to the table
7	<b>Access Proof</b>	<code>curl http://10.0.0.2</code>	Prove site is back online	<b>Success:</b> HTML page loads again

8	Engineering	sudo ufw allow from 10.0.0.1 to any port 80	Restrict access to ONLY Kali IP	<b>Success:</b> Precision rule applied
9	Final Victory	curl http://10.0.0.2	Final proof of authorized access	<b>Success:</b> Site loads ONLY for Kali