

Day 3 – Traffic Control & Firewall Hardening (UFW)

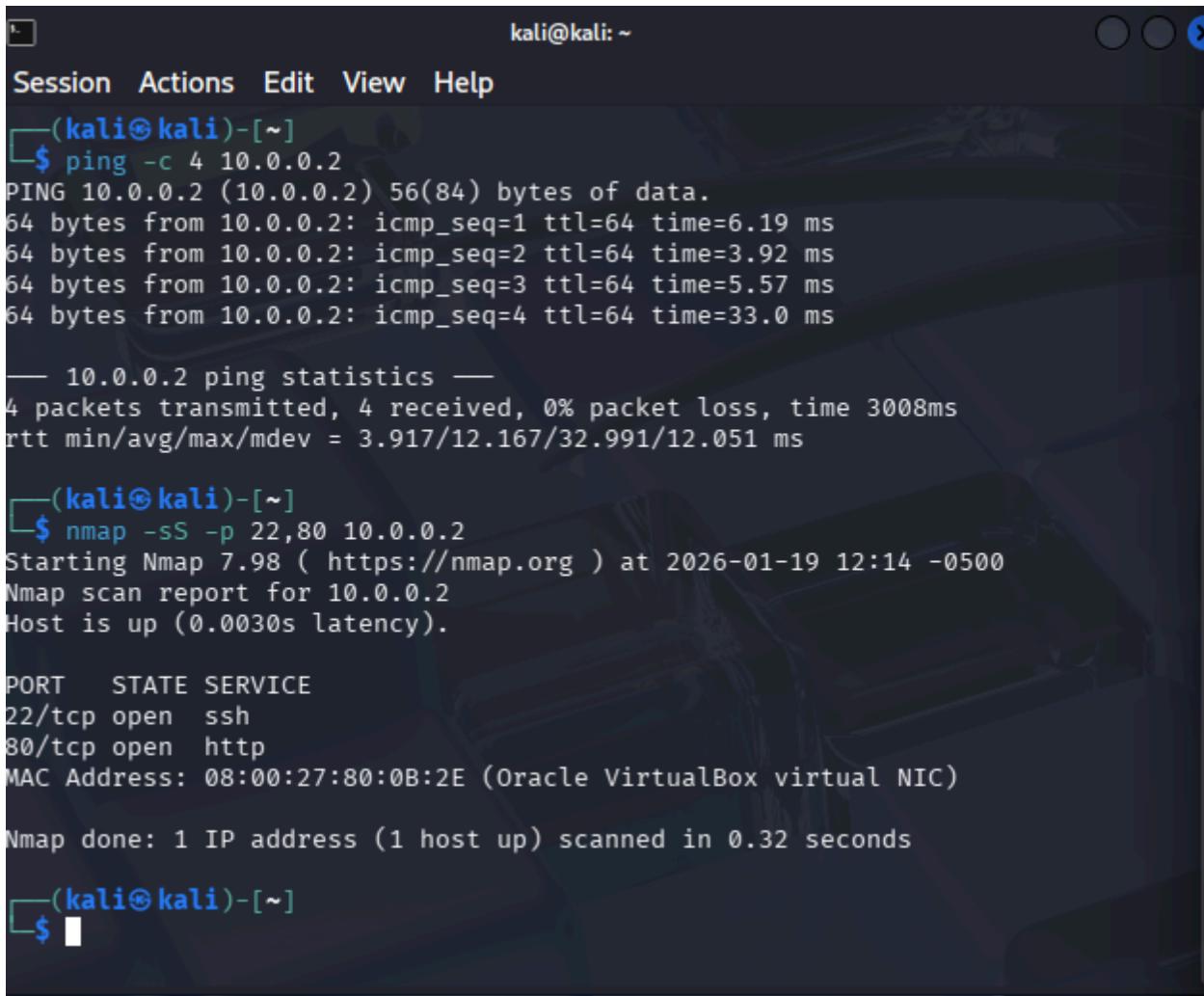
Mindset today:

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 screenshot of a terminal window titled "kali@kali: ~". The terminal shows the following commands and output:

```
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).

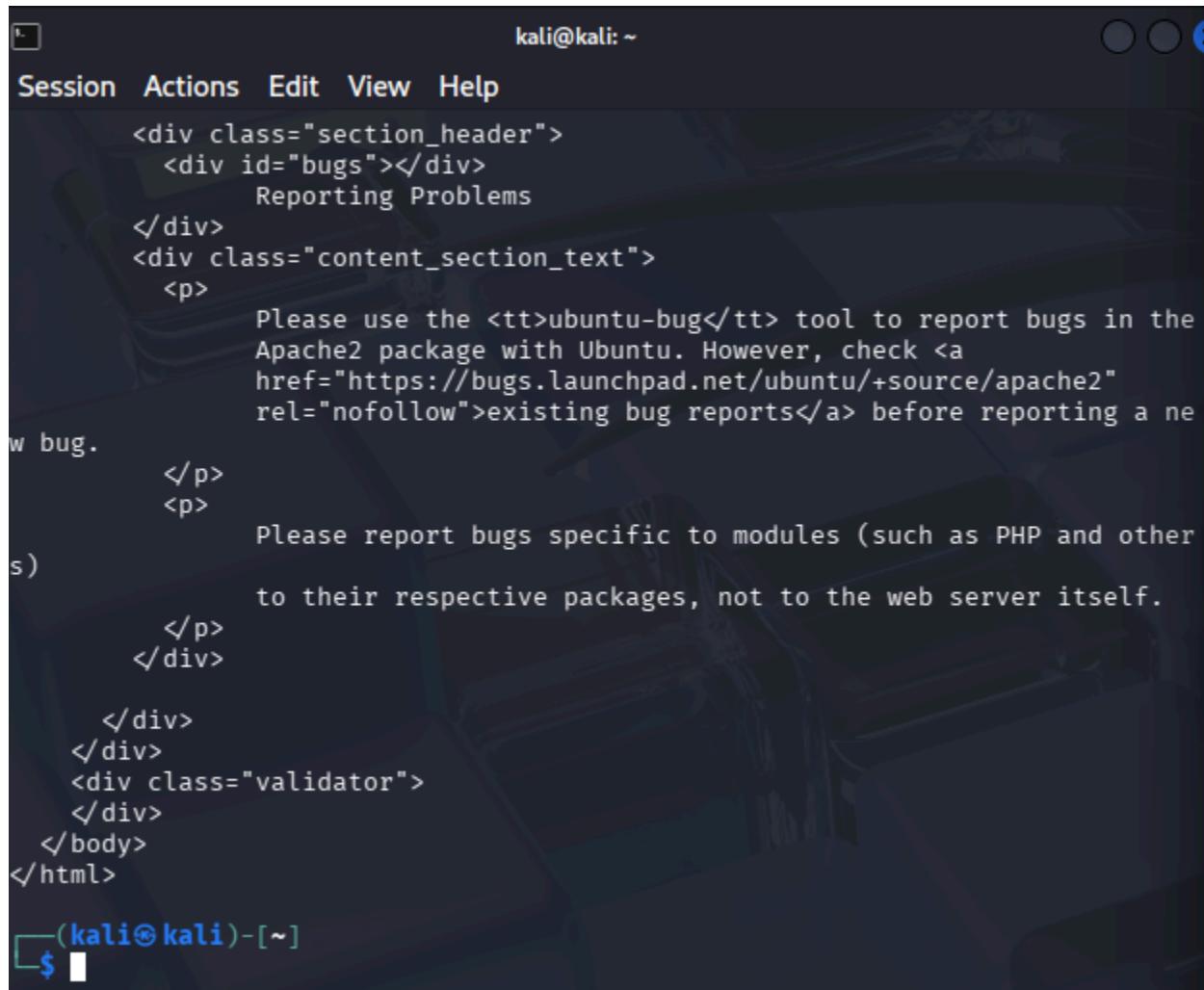
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:80:0B:2E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

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



A screenshot of a terminal window titled "Session Actions Edit View Help". The window displays a web page with HTML code. The code includes sections for reporting bugs, instructions for specific modules, and a note about the UFW firewall. The terminal prompt at the bottom shows the user is on Kali Linux.

```
<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 new bug.
  </p>
  <p>
    Please report bugs specific to modules (such as PHP and others)
    to their respective packages, not to the web server itself.
  </p>
</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 pr

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

STEP 4: Enable Firewall (CRITICAL MOMENT)

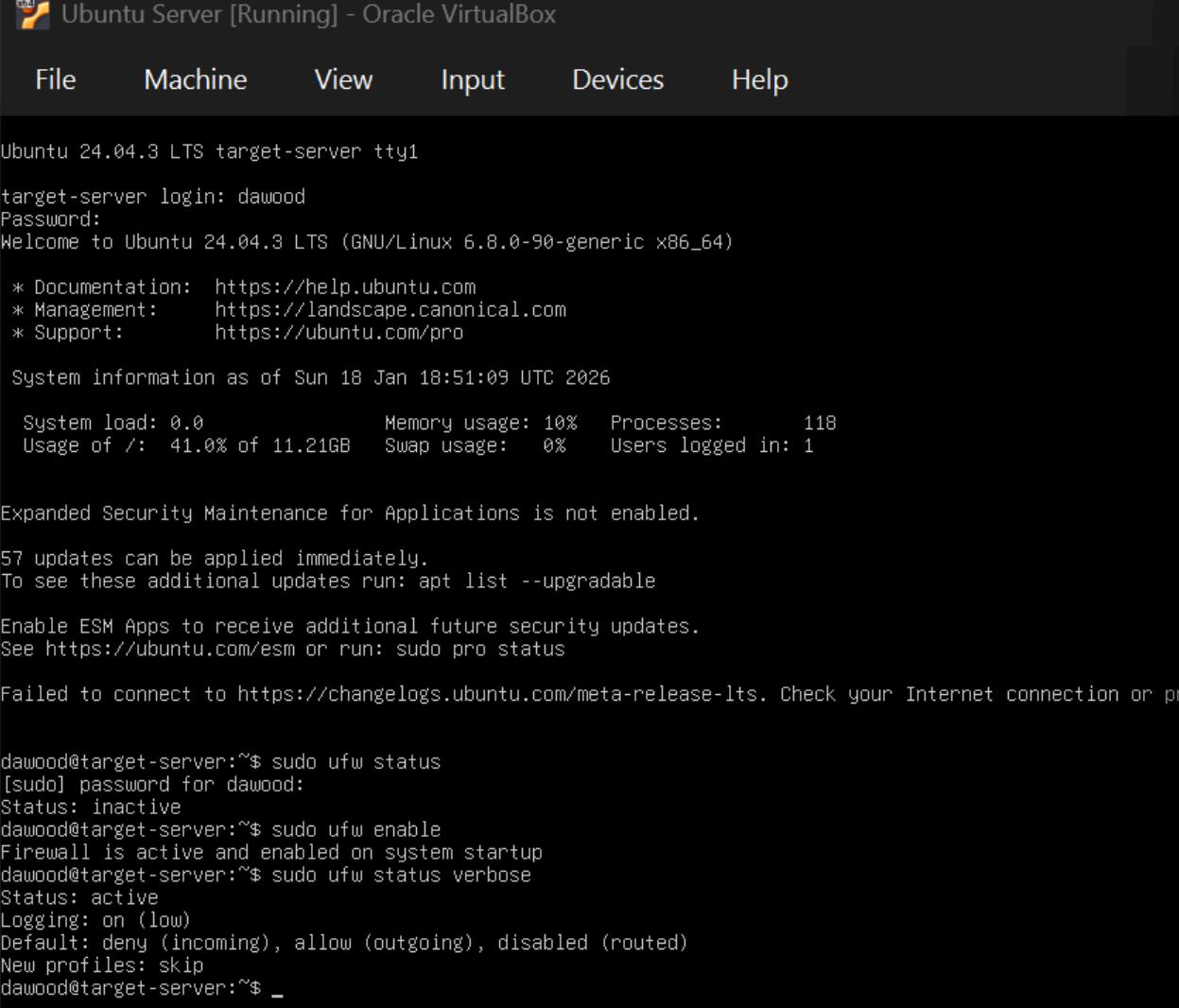
The command we are using is (sudo ufw enable)

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 Server [Running] - Oracle VirtualBox

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 p

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:~$ _
```

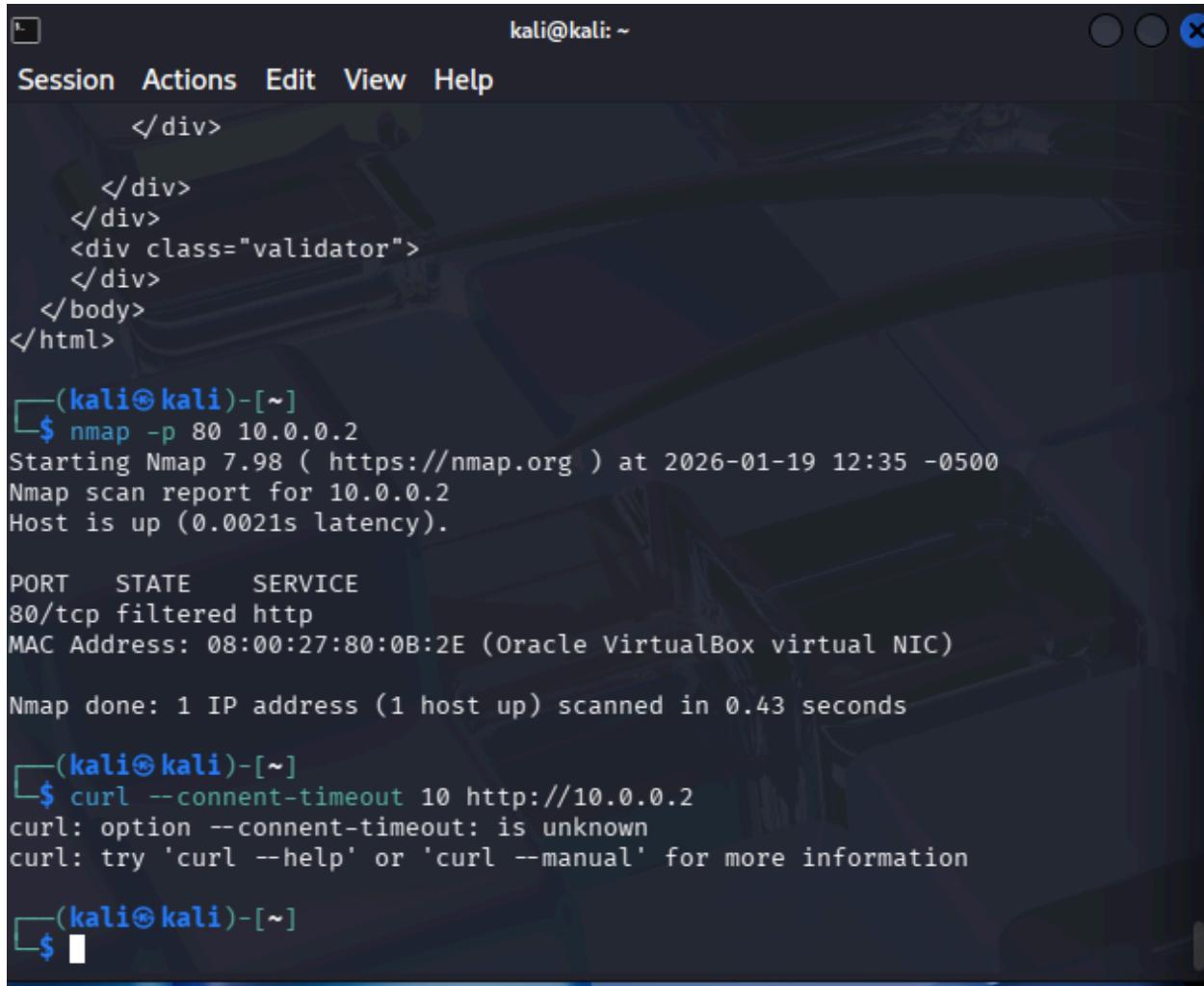
STEP 5: Test the Block (ATTACK FAILS)

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



The screenshot shows a terminal window titled "kali@kali: ~". The terminal displays the following session:

```
</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 --connent-timeout 10 http://10.0.0.2
curl: option --connent-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 p

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)

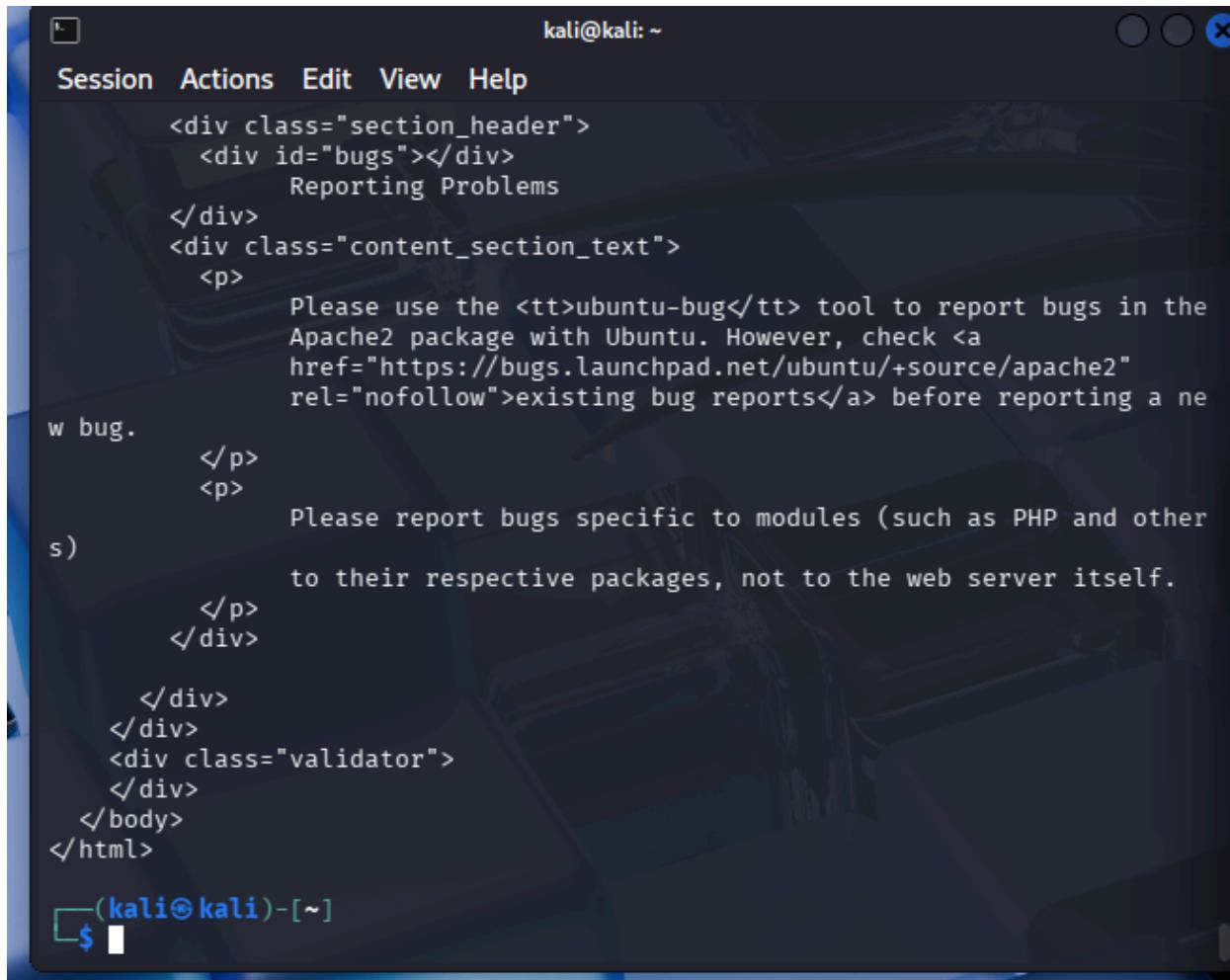
dawood@target-server:~$ _
```

STEP 7: Retest Access (CONTROL RESTORED)

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



A screenshot of a terminal window titled "Session Actions Edit View Help". The window displays a web page source code related to reporting bugs for the Apache2 package. The text includes instructions for using the `ubuntu-bug` tool, links to Launchpad, and advice on reporting specific module bugs rather than the web server itself. The terminal prompt at the bottom shows the user is on a Kali Linux system.

```
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  
      modules) to their respective packages, not to the web server itself.  
    </p>  
  </div>  
</div>  
<div class="validator">  
</div>  
</body>  
</html>  
└─(kali㉿kali)-[~]  
$
```

STEP 8: Restrict Access (ENGINEER MOVE)

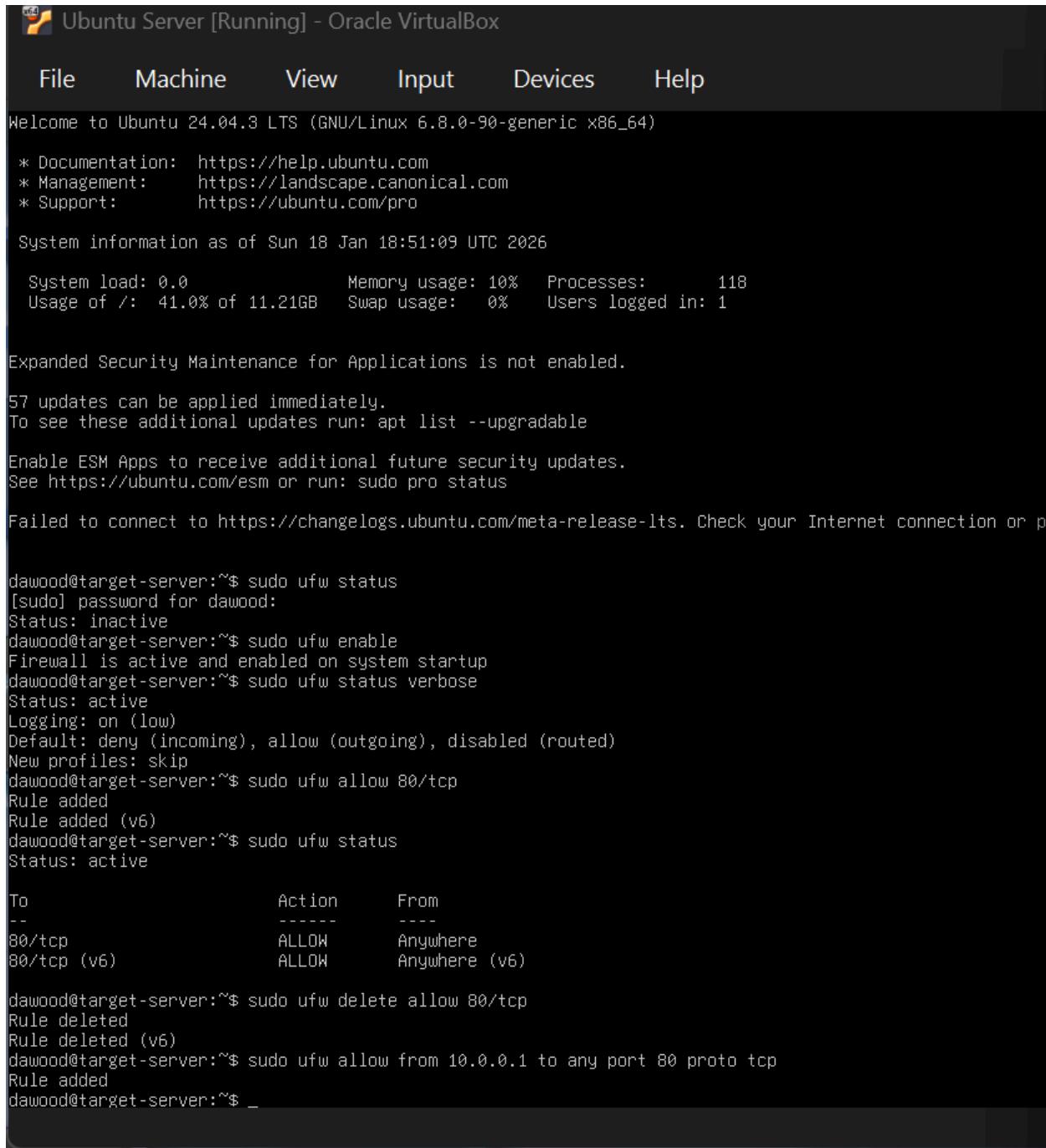
The command we are using is (`sudo ufw delete allow 80/tcp`)

After this now we will create specialized rule that only kali vm to see (`sudo ufw allow from 10.0.0.1 to 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)

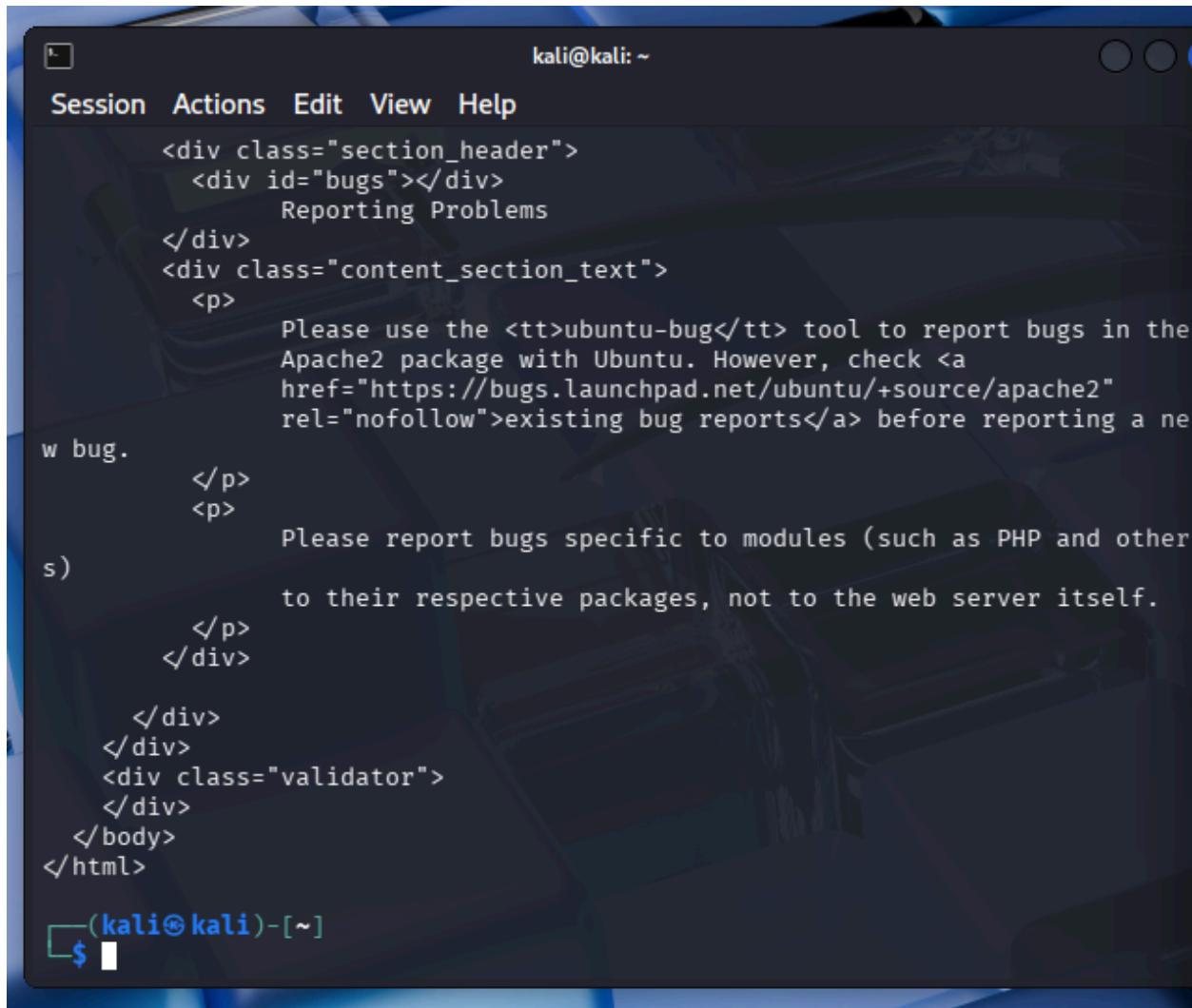
dawood@target-server:~$ sudo ufw delete allow 80/tcp
Rule deleted
Rule deleted (v6)
dawood@target-server:~$ sudo ufw allow from 10.0.0.1 to any port 80 proto tcp
Rule added
dawood@target-server:~$ _
```

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



A screenshot of a terminal window titled "kali@kali: ~". The window displays a web page with HTML code. The page is about reporting bugs for the Apache2 package in Ubuntu. It advises using the `ubuntu-bug` tool and checking for existing reports on Launchpad. It also specifies that bugs should be reported specific to modules like PHP, not to the web server itself. The terminal prompt at the bottom is `$`.

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

[(kali㉿kali)-[~]]$
```

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

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

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