Detailed Report: Basic Firewall Configuration with UFW

1. Objective

The objective of this task is to configure a basic firewall using UFW (Uncomplicated Firewall) on a Linux system. The goal is to allow secure remote management (SSH) while denying unnecessary services (HTTP), then validate the configuration by checking the firewall status.

2. Tools Used

- **Operating System:** Kali Linux (VirtualBox VM)
- **Firewall Utility:** UFW (Uncomplicated Firewall)
- **Commands:** \`ufw allow\`, \`ufw deny\`, \`ufw enable\`, \`ufw status verbose\`

3. Steps Performed

Step	Command	Description
1	sudo apt install ufw -y	Install UFW (if not already installed).
2	sudo ufw allow ssh	Allow SSH traffic (port 22/tcp) for remote access.
3	sudo ufw deny http	Deny HTTP traffic (port 80/tcp) to block web traffic.
4	sudo ufw enable	Enable UFW and apply the configured rules.
5	sudo ufw status verbose	Verify that the rules are active and confirm firewall status.

4. Findings

After applying the firewall rules and enabling UFW, the status output confirmed the following:

Rule	Action	Protocol	Notes
22/tcp	ALLOW IN	IPv4 + IPv6	SSH traffic is allowed, ensuring remote access.
80/tcp	DENY IN	IPv4 + IPv6	HTTP traffic is blocked, preventing web access.

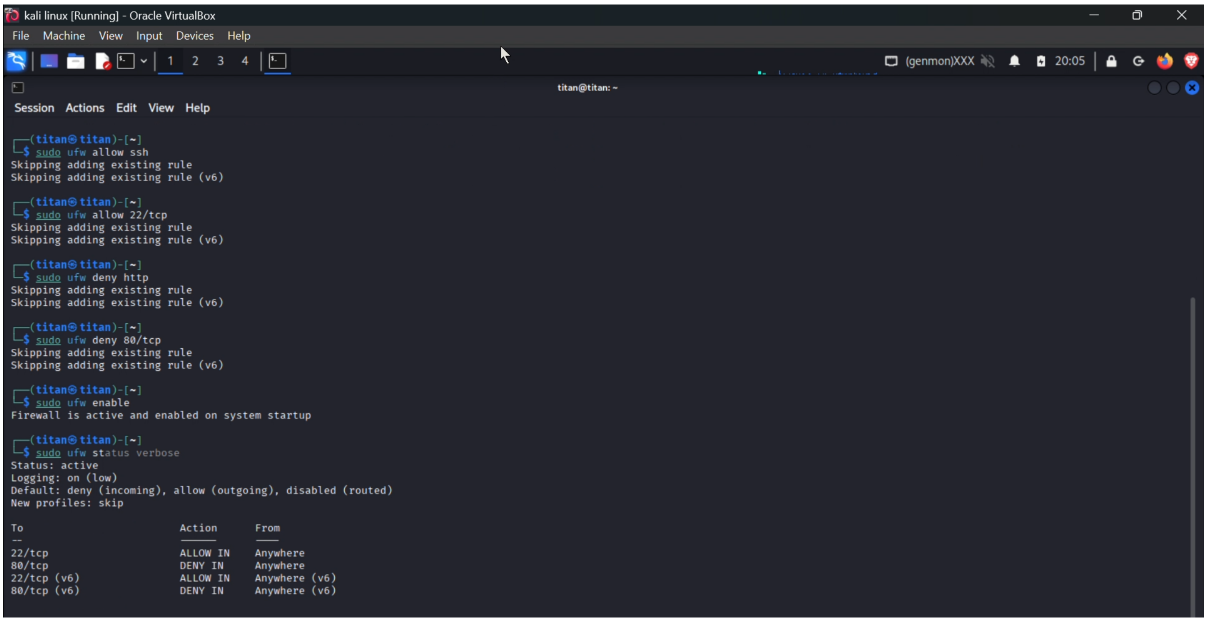
5. Significance of Configuration

- Allowing SSH ensures that administrators retain secure remote access to the server.
- Denying HTTP demonstrates how to restrict unwanted or unused services.
- Applying both IPv4 and IPv6 rules ensures consistency across modern network environments.
- Enabling the firewall at startup ensures rules persist after reboot.

6. Conclusion

The UFW firewall was successfully configured to allow SSH (22/tcp) and deny HTTP (80/tcp). The firewall is active and enabled at startup. This configuration represents a secure baseline: it allows necessary management access while blocking unwanted services. UFW provides a simple yet effective way to manage host-based firewall rules.

7. Screenshot Evidence



kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
(genmon)XXX
20:05
titan@titan: ~
Session Actions Edit View Help

```
┌──(titan㉿titan)-[~]
└─$ sudo ufw allow ssh
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(titan㉿titan)-[~]
└─$ sudo ufw allow 22/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(titan㉿titan)-[~]
└─$ sudo ufw deny http
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(titan㉿titan)-[~]
└─$ sudo ufw deny 80/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(titan㉿titan)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

┌──(titan㉿titan)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
80/tcp                     DENY IN     Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                DENY IN     Anywhere (v6)
```

8. Recommendations

- Always double-check firewall rules before enabling, especially SSH, to avoid lockouts.
- Regularly review firewall logs to ensure only intended traffic is allowed.
- Use UFW application profiles (e.g., `sudo ufw app list`) for more complex services.
- Extend rules to cover additional services only when required (e.g., HTTPS for secure web).