Title:
Network Security Implementation Report

Table of Contents:

1. Introduction
2. Offensive and Defensive Techniques
    - 2.1 Firewall Rules and Nmap Scan Blocking with UFW
    - 2.2 Testing with Altered IP Address
    - 2.3 Snort Rule Configuration and Detection of Nmap Scans
3. Conclusion
4. References

---

1. Introduction

This report describes the setup and configuration of two virtual machines (VMs) used for testing network security techniques involving protocol analysis, firewall rules, and intrusion detection systems. The objective is to simulate and observe network vulnerabilities and how security mechanisms can prevent or alert on network scans, specifically focusing on using the Uncomplicated Firewall (UFW) and Snort intrusion detection system.

For this assignment, two VMs were set up:

- **Attacker Machine:** Linux OS (Kali GNU/Linux Rolling Release:2024.4), with IP address [192.168.140.128].
- **Target Machine:** Linux OS (Ubuntu 24.04.1 LTS Release: 24.04), with IP address [192.168.140.132].

The target machine is configured to observe packets and assess the effectiveness of security defenses against scans initiated from the attacker machine.

---

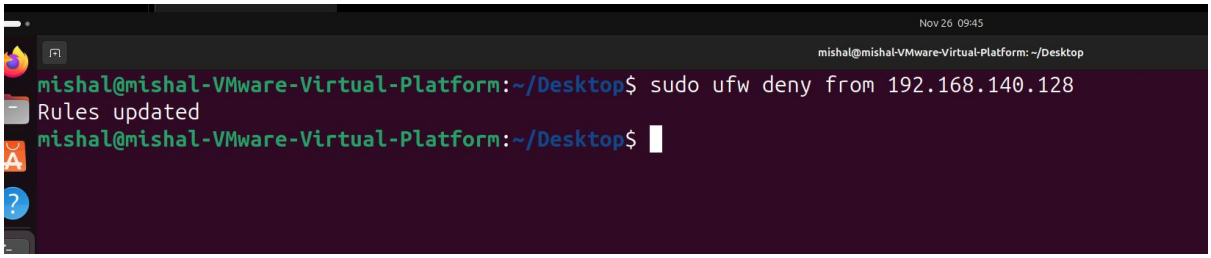
2. Offensive and Defensive Techniques

2.1 Firewall Rules and Nmap Scan Blocking with UFW

To prevent Nmap scans from the attacking machine, UFW firewall rules were configured on the target machine. UFW serves as an interface for managing the Linux kernel's `netfilter` system, enabling the specification of rules to control incoming and outgoing traffic.

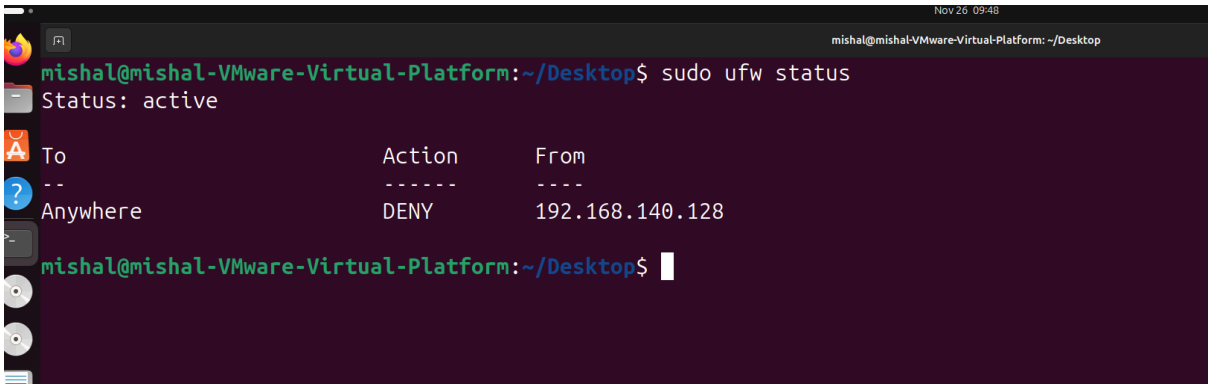
1. **Configuring the Firewall Rule**
    - The UFW rule was set to block all incoming Nmap scans by blocking the attacker machine's IP address. The following command was used:

      ```
      sudo ufw deny from 192.168.140.128
      ```



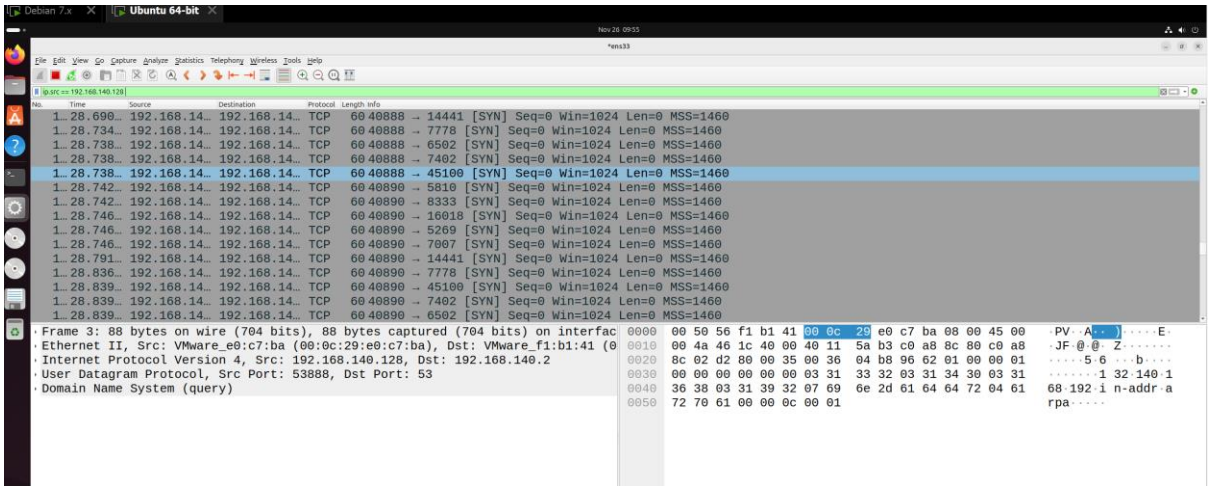
- **Screenshot 1:** Insert a screenshot of the UFW command execution here.

2. **Verifying the Firewall Rule**
   - To confirm that the rule was active, the UFW status was checked to verify the rule addition.



- **Screenshot 2:** Insert a screenshot of the firewall rule confirmation here.

3. **Running Nmap Scan and Observing with Wireshark**
   - An Nmap scan was initiated from the attacking machine to test if the firewall rule blocked the packets.
   - On the target machine, Wireshark was used to capture packets and observe any blocked or allowed connections.



- **Screenshot 3:** Insert screenshots of the Wireshark capture showing blocked packets here.

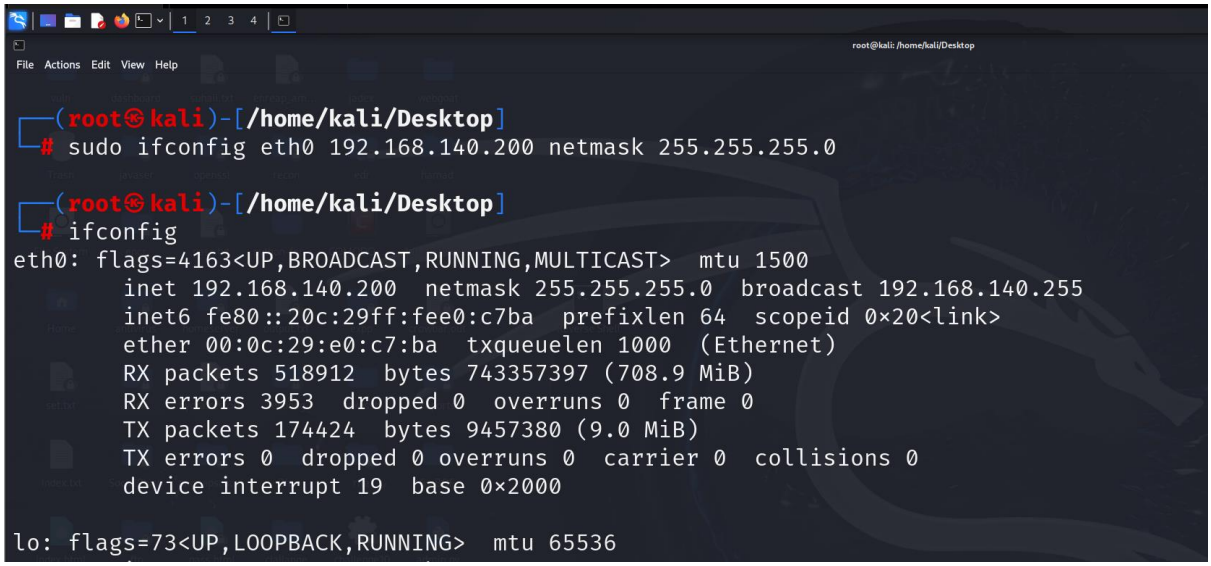
4. **Results of the Nmap Scan**
   - Following the configuration of the UFW rule, the Nmap scan's outcome was analyzed. Wireshark captures indicated that the firewall effectively blocked

packets from the attacker's IP address, as seen by the lack of response in the Wireshark capture.
- This result confirms that the UFW rule effectively prevented Nmap from gaining information about open ports on the target machine.

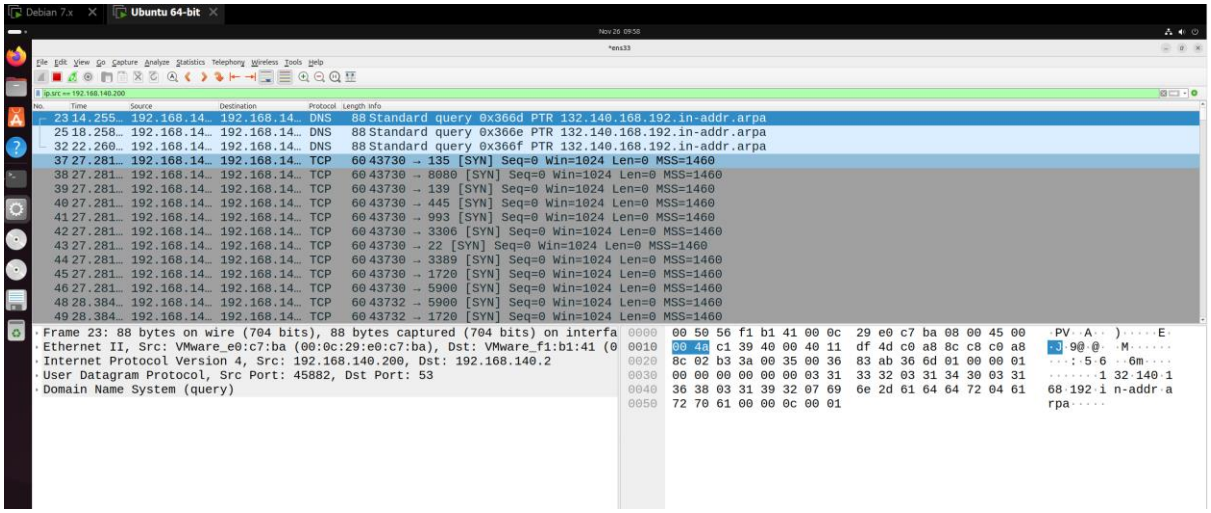
2.2 Testing with Altered IP Address

To further assess the UFW's filtering effectiveness, the IP address of the attacking machine was changed, followed by a repeat Nmap TCP scan to verify whether the firewall rule still applied.

1. **Changing the Attacker IP Address**
   - The attacker machine's IP was changed using network configuration tools.



   - **Screenshot 4:** Insert a screenshot showing the new IP address of the attacker machine.
2. **Nmap Scan with Changed IP Address**
   - After changing the IP, an Nmap TCP scan was run again. With no specific rule for this new IP in the firewall, the packets were not blocked by UFW.



- **Screenshot 5:** Insert Wireshark capture showing packets from the new attacker IP.

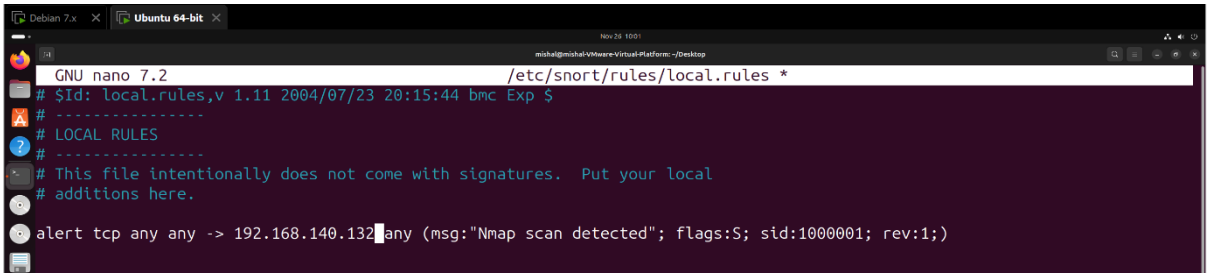
3. **Implications of IP Address Change**
   - This test illustrates the limitation of static IP-based firewall rules, as the attacker machine could bypass the firewall by changing its IP address. The results highlight the need for dynamic or behavioral-based detection systems, which are less dependent on IP address restrictions alone.

2.3 Snort Rule Configuration and Detection of Nmap Scans

To address the limitation of UFW's static IP filtering, Snort was used to write a rule that could detect the signature of an Nmap TCP scan, regardless of the attacker's IP address.

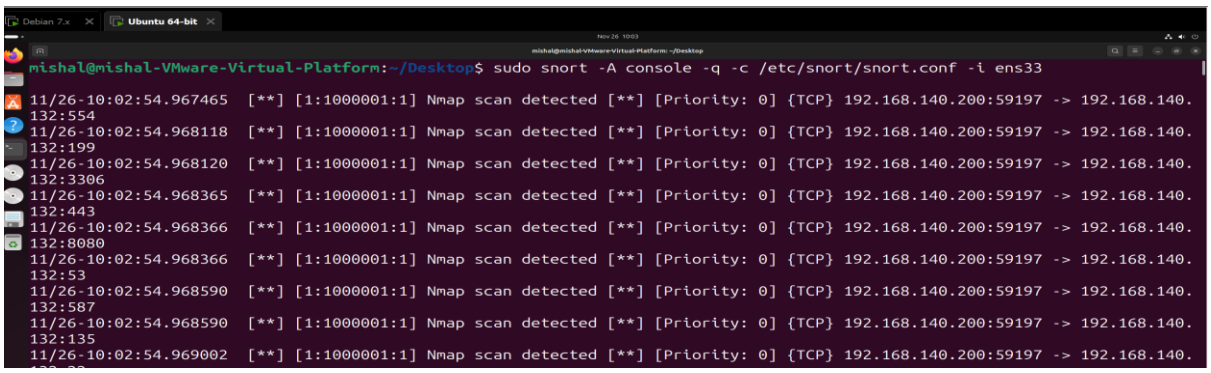
1. **Setting Up Snort**
   - Snort was installed and configured on the target machine as an intrusion detection system (IDS).
   - The Snort rule created was aimed at identifying the unique characteristics of an Nmap TCP scan, which typically includes a series of SYN packets probing various ports.
   - The rule to detect the Nmap scan was written as follows:

```
alert tcp any any -> [Enter Target IP here] any (msg:"Nmap scan detected"; flags:S; sid:1000001; rev:1;)
```



- **Screenshot 6:** Insert a screenshot of the Snort rule configuration file with the rule details.

2. **Testing the Snort Rule**
   - With the Snort rule in place, an Nmap TCP scan was initiated from the attacker machine.
   - When Snort detected the scan pattern, it generated an alert, indicating successful detection.



- **Screenshot 7:** Insert screenshots showing Snort alerts generated by the Nmap scan.

3. **Analysis of Snort's Detection Capabilities**
   - Snort's alert generation provided evidence that the Nmap TCP scan was successfully detected, showcasing Snort's strength in identifying attack patterns without relying on IP-based filtering.
   - This approach highlights the advantage of IDS systems like Snort in enhancing security by identifying behaviors rather than relying solely on static firewall rules.

---

3. Conclusion

The exercises detailed in this report demonstrate key principles in network security, including the detection and prevention of reconnaissance scans using UFW and Snort. UFW was effective in blocking traffic based on IP but had limitations when the attacker's IP address changed. Snort, however, provided a more flexible detection mechanism by monitoring packet behavior, which is more effective in scenarios with changing IP addresses or when attackers disguise their identities.

These findings underscore the importance of layered network defenses, where both firewalls and IDS systems work together to address various vulnerabilities. Through this hands-on exploration, insights were gained into protocol behavior, firewall rules, and intrusion detection techniques, furthering understanding of real-world network security practices.

---

4. References

Provide references to all tools, manuals, and sources used, such as:

- UFW documentation: https://launchpad.net/ufw
- Snort documentation: https://www.snort.org/
- Nmap reference guide: https://nmap.org/
- Relevant textbooks or articles on network security, if applicable.

Note: Throughout the report, remember to number each figure and add captions, such as "Figure 1: UFW command to block Nmap scan." This will keep the report organized and ensure it meets the formatting criteria.

This structure and content outline should provide a strong base for completing your report. Add the screenshots in the designated spots for a comprehensive and well-documented submission

- **UFW**: Used on the target machine to set up firewall rules intended to block traffic from the attacker.
- **Nmap**: Used on the attacker machine to conduct various scans on the target machine.
- **Wireshark**: Running on the target machine to capture and display network packets, providing visual confirmation of the UFW and Snort protections.
- **Snort**: Also on the target machine, Snort detects patterns like the Nmap scan itself and raises alerts if it recognizes potentially malicious scanning behavior.