Lab 04: Writing and Testing Firewall (IPTables) and IDS (Snort) Rules with Scapy

Dr. Sherif Saad

March 11, 2025

Purpose

This lab aims to introduce the students to the basics of IPTables and SNORT. The student will install, configures, write and test IPTables and SNORT rules

1 Lab Instructions

1.1 Task 1: Writing and Testing Firewall Rules with IPTables

1.1.1 Step 1: Reset IPTables

Ensure that no existing rules interfere.

1.1.2 Step 2: Create Firewall Rules

Write IPTables rules to:

- Allow outgoing HTTP traffic (port 80).
- Block ICMP (Ping) requests.
- Block MySQL connections from remote IPs except local IPs.

Provide a brief description explaining the purpose of each rule you write. Support your answers with screenshots.

1.2 Task 2: Writing and Testing Snort IDS Rules

1.2.1 Step 1: Add Snort Rules

Write Snort rules to:

- Detect SSH brute-force attacks.
- Detect unauthorized MySQL root login attempts.
- Detect unencrypted MySQL passwords.

1.2.2 Step 2: Restart Snort to Apply Rules

Restart Snort after adding the rules.
Provide a brief description explaining the purpose of each rule you write. Support your answers with screenshots.

1.3 Task 4: Testing with Scapy

1.3.1 Step 1: Test Firewall Rules

Use Scapy to:

- Verify HTTP traffic is allowed.
- Verify ICMP (Ping) is blocked.
- Test MySQL connection filtering.

Provide a brief explanation of how your tests confirm the functionality of the rules. Support your answers with screenshots.

1.3.2 Step 2: Test Snort Rules

Use Scapy to:

- Trigger SSH brute force detection.
- Simulate MySQL root login attempt.
- Test unencrypted password detection.

Provide a brief explanation of how your tests confirm the functionality of the rules. Support your answers with screenshots.

2 Example Answer

Firewall Rule: Blocking ICMP Requests

- Rule: Block all incoming ICMP packets to prevent ping-based reconnaissance.
- IPTables Command:

```
sudo iptables -A INPUT -p icmp -j DROP
```

- Explanation: This rule ensures that the system does not respond to ping requests, making it less susceptible to network scans.
- Screenshot: [Provide a screenshot showing the rule in the IPTables list]

3 Deliverables

- IPTables Configuration: Provide evidence of your configured rules.
- Snort Alerts: Provide logs from your testing.
- Scapy Test Results: Output from your Scapy commands.
- Snort Rule for SSH Brute Force Detection: The rule you wrote with a description.
- Screenshots: Supporting images for all responses.