Course	COMP 7003
Program	BScACS
Term	September 2024

- This is a **pair** assignment.
- ***You must work in pairs unless you have explicit permission from the instructor.***

Objective

- This assignment aims to deepen your understanding of network security mechanisms, explicitly focusing on the roles of a firewall (nftables) and an intrusion detection system (IDS) like Snort3. You will conduct network attacks, analyze traffic using Wireshark, and evaluate how each defensive mechanism handles different threats.

Learning Outcomes

- Analyze network traffic to identify attack signatures.
- Configure and utilize nftables (firewall) and Snort3 (IDS).
- Compare and contrast the capabilities of firewalls and IDS in detecting and blocking attacks.
- Use Wireshark to capture and analyze network traffic patterns.
- Demonstrate an understanding of network security principles and defensive strategies.

Details

Attack Scenarios

- The table below outlines the five attacks you will perform from Host A (Attacker) to Host B (Victim).

Attack	**Command**	**Description**
TCP SYN Flood	`hping3 -S -p 80 --flood <Victim IP>`	Floods the victim with SYN packets on port 80.
UDP Flood	`hping3 --udp -p 53 --flood <Victim IP>`	Floods the victim with UDP packets on port 53.

TCP Xmas Tree Scan	`nmap -sX <Victim IP>`	Sends packets with unusual TCP flags (FIN, PSH, URG).
Ping of Death	`ping -s 65500 <Victim IP>`	Sends oversized ICMP packets to cause a potential crash.
Buffer Overflow	`python3 -c 'print("A" * 1000)' | nc <Victim IP> 1234`	Sends an oversized payload of 1,000 'A' characters to the victim's port, potentially causing a buffer overflow if the receiving service does not correctly handle the input size.

- Replace <Victim IP> with the IP address of Host B.

Part 1: Baseline Analysis Without Defense

- Objective: Analyze the effects of attacks without any defensive measures in place.
- Steps:
  - Disable nftables and Snort3 on Host A and B.
  - Run each attack from Host A using the provided commands.
  - Capture the traffic using Wireshark on both Host A and Host B.
- Deliverables:
  - Wireshark captures (.pcap files).
  - Analysis of captured traffic, identifying attack patterns and anomalies.

Part 2: Defending with nftables (Firewall) and Snort3 (IDS)

- Objective: Configure both nftables and Snort3 on Host B (Victim) to block and detect attacks and compare the effectiveness of firewall rules and IDS alerts.
- Steps:
  - Research and implement nftables rules on Host B to block attacks that a firewall can typically handle (e.g., SYN Flood, Ping of Death).
  - Configure Snort3 on Host B with rules to detect attack signatures that the firewall may not block (e.g., Xmas Tree Scan, UDP Flood, Buffer Overflow).
  - Enable both nftables and Snort3 on Host B.
  - Rerun all attacks from Host A using the commands provided.
  - Capture the traffic using Wireshark on both Host A and Host B.
  - Review nftables logs and Snort3 alerts on Host B.
- Deliverables:
  - Wireshark captures (.pcap files) from both hosts.
  - Custom logs from nftables showing blocked traffic.
  - Snort3 alert logs indicating detected attacks.
  - Analysis of which attacks were blocked by the firewall, which Snort3 detected, and any differences observed between the two defence mechanisms.

Part 3: Attacker-Side Defense

- Objective: Implement nftables and Snort3 on Host A (Attacker) to block outgoing attacks and analyze what is prevented before reaching Host B (Victim).
- Steps:
  - Remove all firewall and IDS configurations from Host B.
  - Configure nftables on Host A to block certain types of outgoing traffic (e.g., SYN Flood, Ping of Death).
  - Configure Snort3 on Host A to detect attack signatures (e.g., UDP Flood, Xmas Tree Scan, Buffer Overflow).
  - Enable both nftables and Snort3 on Host A.
  - Rerun all attacks from Host A to Host B.
  - Capture the traffic using Wireshark on Host A.
  - Review nftables logs and Snort3 alerts on Host A.
- Deliverables:
  - Wireshark captures from Host A (.pcap files).
  - Custom logs from nftables and Snort3 show blocked and detected traffic.
  - Analysis of which attacks were blocked on Host A and why, along with an explanation of your configurations.

Part 4: Full Defense on Both Hosts

- Objective: Configure both nftables and Snort3 on both Host A and Host B.
- Steps:
  - Enable nftables and snort3 on both Host A and Host B.
  - Configure appropriate rules for both firewall and IDS.
  - Rerun all attacks and capture traffic using Wireshark.
- Deliverables:
  - Wireshark captures from both hosts.
  - Logs from nftables and Snort3 on both hosts.
  - Analysis of the combined effect of firewall and IDS on the attack outcomes.

Report Structure

Introduction

- Provide a brief overview of the assignment objectives and what you aim to demonstrate with the firewall (nftables) and IDS (Snort3) configurations.

Firewall and Snort Rules

- Before diving into the analysis, create a table that lists all the firewall (nftables) and Snort3 rules you configured.
- This section should include a brief explanation for each rule.

Example Table:

Tool	Rule	Description
nftables		Blocks TCP SYN Flood attack.
Snort3		Detects UDP Flood attacks on port 53.

- You will need two tables, one for the attacker and one for the victim.

Part 1: Baseline Analysis Without Defense

- Analyze each attack performed without any defensive measures in place.
- For each attack, include screenshots of Wireshark captures from Host A and Host B.
- Provide a detailed analysis of the observed traffic patterns and explain the attacks' signatures.

Part 2: Defending with nftables (Firewall) and Snort3 (IDS)

- Describe your configuration of nftables and Snort3 on Host B (Victim).
- Include screenshots of Wireshark captures, nftables logs, and Snort3 alerts for each attack.
- Analyze which attacks were blocked by the firewall detected by Snort3 and discuss any differences in detection and blocking.

Part 3: Attacker-Side Defense

- Explain your configuration of nftables and Snort3 on Host A (Attacker).
- Include screenshots of Wireshark captures, nftables logs, and Snort3 alerts.
- Analyze which attacks were blocked or detected before they reached Host B and discuss the effectiveness of your attacker-side defences.

Part 4: Full Defense on Both Hosts

- Describe your combined defence setup on Host A and Host B, including any adjustments to your rules.
- Include screenshots of Wireshark captures from both hosts and relevant logs and alerts.
- Analyze the impact of having defences on both sides and compare the results to earlier parts of the assignment.

Conclusion

- Summarize your findings from each part of the assignment.
- Discuss the differences between firewall and IDS capabilities, including:
    - Which attacks were more effectively blocked by the firewall?
    - Which attacks were better detected by Snort3?

    - The advantages of using both mechanisms together.
- Reflect on your challenges and what you learned about configuring and analyzing network security defences.

Constraints

- You must determine your firewall (nftables) and IDS (Snort3) rules.
- Ensure root permissions are used when configuring nftables and Snort3.
- Follow ethical guidelines and avoid affecting any network devices outside the lab environment.

Resources

- Wireshark documentation and tutorials
- nftables and Snort3 man pages
- Online guides for configuring nftables and Snort3

Submission

- Wireshark capture files (.pcap).
- Configuration files for nftables and Snort3 (only custom configurations).
- Log files from nftables and Snort3.
- A detailed report, including:
    - Analysis of network traffic with and without defences.
    - Explanation of which attacks were detected or blocked and why.
    - Observations on the differences between firewall and IDS capabilities.

Evaluation

Topic	Value
Baseline Analysis	15%
nftables Firewall	15%
Snort3 IDS	15%
Attacker-Side Defense	15%
Full Defense on Both Hosts	15%
Report Clarity and Completeness	25%

Total	100%

Hints

- Refer to online resources for nftables and Snort3 configurations.
- Use Wireshark filters to isolate relevant traffic for analysis.
- Organize your report systematically and ensure technical accuracy in your explanations.