Indian Institute of Information Technology Surat

Lab Report on
Network Security (CS 702) Practical

Submitted by

[RAHUL KUMAR SINGH] (UI21CS44)

Course Faculty

Dr. Reema Patel

Department of Computer Science and Engineering
Indian Institute of Information Technology Surat
Gujarat-394190, India

Aug-2024

Lab No: 7

Aim:

Implement ICMP Flood (DoS) Attack in snort. Submit the pdf document mentioning snort rules, and other commands/processes to implement the ICMP flood attack in Snort.

Description:

1. **TCP SYN Flood Attack:** Detects a high number of SYN packets to port 80 from a single source, indicating a potential SYN flood DoS attack.
2. Exploits the TCP three-way handshake by sending excessive SYN requests to overwhelm the server.
3. Initiates SYN requests but does not send ACK responses, leaving connections half-open.
4. Consumes server resources, preventing legitimate connections and causing service disruptions.

Implementation:

Step 1: Install Snort

- `sudo apt-get update`
- `sudo apt-get install snort`

Step 2: Create Rule for SYN Flood Detection

- `alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"SYN Flood Detected"; flags:S; detection_filter:track by_src, count 100, seconds 1; sid:1000004;)`
- `alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Flood Detected"; detection_filter:track by_src, count 100, seconds 1; sid:1000001;)`

Step 3: Update Snort Configuration

- **Elevate folder privileges: sudo chmod 777** /etc/snort/rules/
- **Elevate file privileges: sudo chmod 777** /etc/snort/rules/tcp_syn_flood.rules
- **Edit tcp_syn_flood.rules:** sudo nano /etc/snort/rules/tcp_syn_flood.rules
- **Add rule to snort.conf:** sudo nano /etc/snort/snort.conf
- **Ensure:** include $RULE_PATH/tcp_syn_flood.rules

Step 4: Run Snort in IDS Mode

- `sudo snort -A console -c /etc/snort/snort.conf -i lo`

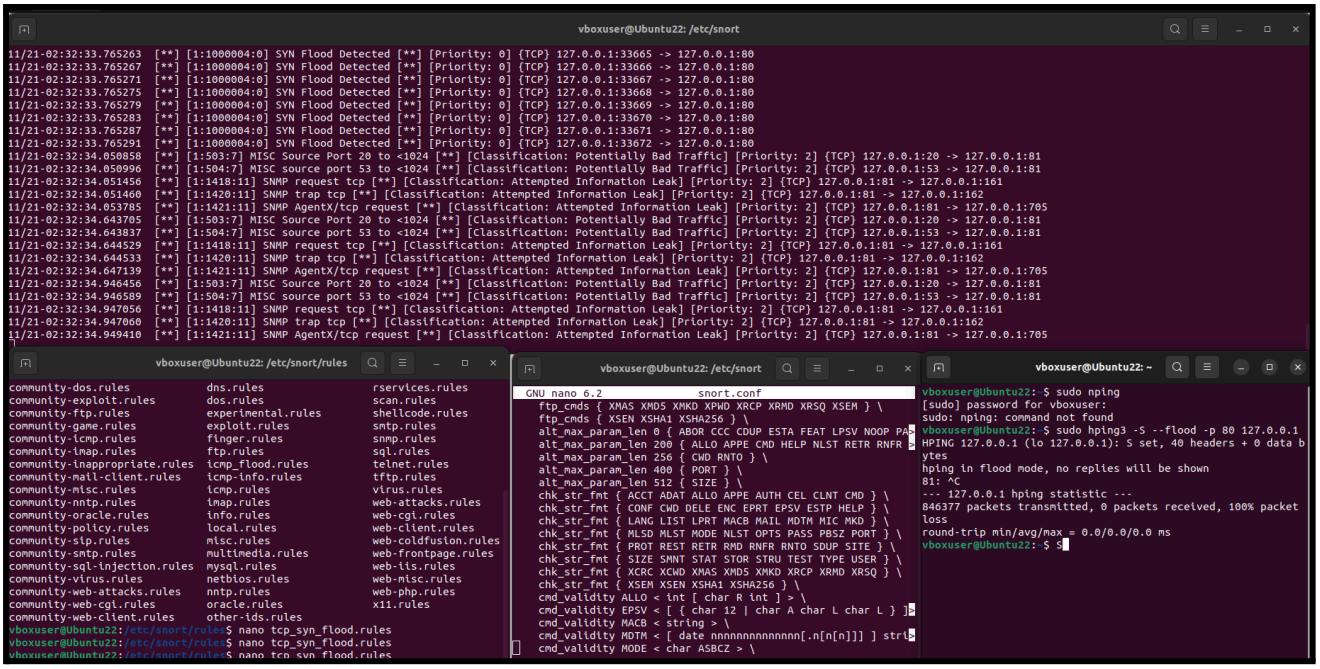
Step 5: Test Detection with hping3

- `sudo hping3 -S --flood -p 80 127.0.0.1`

Testcase 1: Testing TCP SYN Flood Attack

- **Rule:** `alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"SYN Flood Detected"; flags:S; threshold: type both, track by_src, count 100, seconds 1; sid:1000001;)`
- **Test Command:** `sudo hping3 -S --flood -p 80 127.0.0.1`
- **Explanation:** The rule detects a SYN flood by counting 100 SYN packets from the same source to port 80 within 1 second, triggering an alert for potential attack.

Output:



Conclusion:

- Snort rules efficiently detect SYN flood attacks and other network threats.
- It can be tailored to detect various protocols and attack types.
- It enables immediate alerts, allowing for quick incident response.
- It is suitable for both small and large networks with adjustable rule sets.
- It applies to intrusion detection, network monitoring, and traffic analysis.