## 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: 6

## 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. **ICMP Flood Attack**: Detects large volumes of ICMP Echo Requests, signaling potential DoS attack attempts.
2. **ICMP ISS Pinger**: Detected ICMP Echo Requests with "ISSPNGRQ" payload, signaling reconnaissance activity.
3. **ICMP L3retriever Ping**: Identified ICMP Echo Requests with a distinct payload, used for network scanning.
4. **ICMP Nemesis v1.1 Echo**: Triggered by ICMP packets with a 20-byte payload, typically used for diagnostics.
5. **ICMP PING NMAP**: Detected ICMP Echo Requests with zero data, common in network scans.
6. **ICMP icmpenum v1.1.1**: Recognized ICMP Echo Request with custom ID and sequence, indicating enumeration attempts.
7. **ICMP Redirect Host**: Captured ICMP Redirect messages, often used in host redirection attacks.
8. **ICMP Redirect Net**: Detected ICMP Redirect messages indicating network-level redirection attempts.
9. **ICMP Superscan Echo**: Identified 8-byte ICMP Echo Requests, often used by Superscan tools.
10. **ICMP Traceroute IP Options**: Triggered by ICMP Echo Reply with Record Route option, indicating traceroute activity.
11. **ICMP Webtrends Scanner**: Detected ICMP Echo Request with a specific payload, linked to web scanning tools.
12. **ICMP Destination Unreachable**: Captured ICMP Destination Unreachable messages, signaling network or administrative issues.

## Implementation:

### Step 1: Install Snort

* sudo apt-get update
* sudo apt-get install snort

### Step 2: Create Rule (Test Cases) for ICMP Flood Detection

* Copy the test case data into icmp\_flood.rules

### Step 3: Update Snort Configuration

* **Elevate folder privileges: sudo chmod 777** /etc/snort/rules/
* **Elevate file privileges: sudo chmod 777** /etc/snort/rules/icmp\_flood.rules
* **Edit icmp\_flood.rules:** sudo nano /etc/snort/rules/icmp\_flood.rules
* **Add rule to snort.conf:** sudo nano /etc/snort/snort.conf
* **Ensure:** include $RULE\_PATH/icmp\_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 ping -b -f 127.0.0.0

**Testcase 1: Testing ICMP Flood Attack**

* **Rule:** alert icmp any any -> any any (msg:"ICMP Flood Attack Detected"; threshold: type both, track by\_src, count 10, seconds 5; sid:1000001; rev:1;)
* **Test Command:** sudo ping -b -f 127.0.0.0
* **Explanation:** This rule triggers when an ICMP Echo Request (ping) packet with the payload ISSPNGRQ is detected. The payload ISSPNGRQ in hexadecimal is 495353504e475251, which you send as part of the ICMP Echo Request.

**Testcase 2: Testing ICMP ISS Pinger**

* **Rule:** alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ICMP ISS Pinger"; itype:8; content:"ISSPNGRQ"; depth:32; sid:465;)
* **Test Command:** ping -p "495353504e475251" 127.0.0.0
* **Explanation:** This rule triggers when an ICMP Echo Request (ping) packet with the payload ISSPNGRQ is detected. The payload ISSPNGRQ in hexadecimal is 495353504e475251, which you send as part of the ICMP Echo Request.

**Testcase 3: Testing ICMP L3retriever Ping**

* **Rule:** alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ICMP L3retriever Ping"; icode:0; itype:8; content:"ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI"; sid:466;)
* **Test Command:** ping -p "4142434445464748494a4b4c4d4e4f5051525354555657584142434445464748494a4b4c4d4e4f50" 127.0.0.0
* **Explanation:** This rule triggers when an ICMP Echo Request contains the string "ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI". The string in hexadecimal is the payload sent with the ping.

**Testcase 4: Testing ICMP Nemesis v1.1 Echo**

* **Rule:** alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ICMP Nemesis v1.1 Echo"; dsize:20; icmp\_id:0; icmp\_seq:0; itype:8; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; sid:467;)
* **Test Command:** ping -p "00000000000000000000000000000000000000000000000000" 127.0.0.0
* **Explanation:** This rule triggers when an ICMP Echo Request with a payload of 20 bytes and the specific content is detected. The content is |00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| in hexadecimal.

**Testcase 5: Testing ICMP PING NMAP**

* **Rule:** alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ICMP PING NMAP"; dsize:0; itype:8; sid:469;)
* **Test Command:** ping -s 0 127.0.0.0
* **Explanation:** This rule triggers on an ICMP Echo Request packet with no data (dsize:0).

**Testcase 6: Testing ICMP icmpenum v1.1.1**

* **Rule:** alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ICMP icmpenum v1.1.1"; dsize:0; icmp\_id:666; icmp\_seq:0; itype:8; sid:471;)
* **Test Command:** ping -i 666 -s 0 127.0.0.0
* **Explanation:** This rule triggers on an ICMP Echo Request with icmp\_id:666 and icmp\_seq:0.

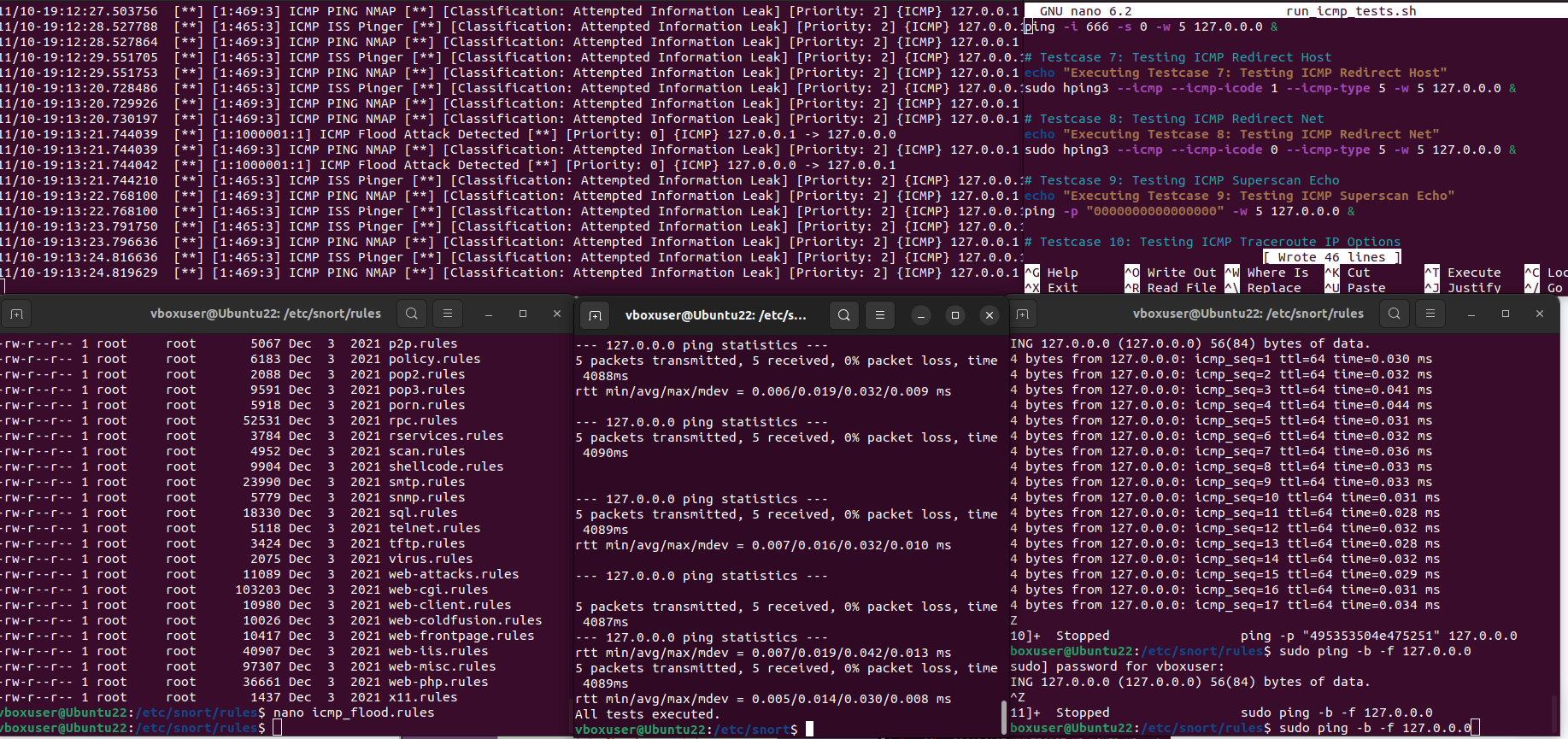
**Testcase 7: Testing ICMP Redirect Host**

* **Rule:** alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ICMP redirect host"; icode:1; itype:5; sid:472;)
* **Test Command:** sudo hping3 --icmp --icmp-icode 1 --icmp-type 5 127.0.0.0
* **Explanation:** This rule triggers when an ICMP Redirect message is sent, specifically for a host (icode:1).

**Testcase 8: Testing ICMP Redirect Net**

* **Rule:** alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ICMP redirect net"; icode:0; itype:5; sid:473;)
* **Test Command:** sudo hping3 --icmp --icmp-icode 0 --icmp-type 5 127.0.0.0
* **Explanation:** This rule triggers when an ICMP Redirect message is sent, specifically for a network (icode:0).

## Output:

****

## Conclusion:

* Snort rules quickly identify specific attack patterns and network anomalies.
* 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.