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:

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 "41424344454647484494a4b4c4d4e4f505152535455565758414243444546474849 4a4b4c4d4e4f50" 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).

Testcase 9: Testing ICMP Superscan Echo

- **Rule:** `alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP superscan echo"; dsize:8; itype:8; content:"|00 00 00 00 00 00 00 00|"; sid:474;)`
- **Test Command:** `ping -p "0000000000000000" 127.0.0.0`
- **Explanation:** This rule triggers when an ICMP Echo Request contains exactly 8 bytes of specific content (00 00 00 00 00 00 00 00).

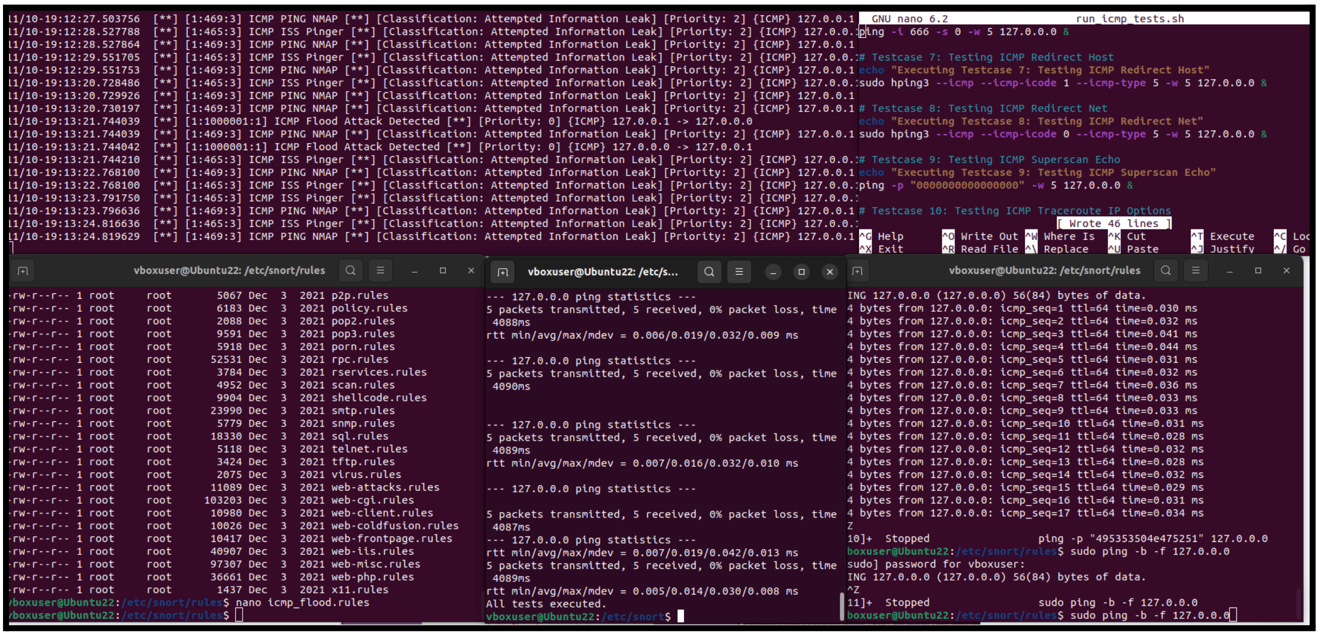
Testcase 10: Testing ICMP Traceroute IP Options

- **Rule:** alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP traceroute ipopts"; ipopts:rr; itype:0; sid:475;)
- **Test Command:** sudo traceroute -I 127.0.0.0
- **Explanation:** This rule triggers when an ICMP Echo Reply packet with a Record Route (RR) IP option is detected.

Testcase 11: Testing ICMP Webtrends Scanner

- **Rule:** alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP webtrends scanner"; icode:0; itype:8; content:"|00 00 00 00|EEEEEEEEEEEE"; sid:476;)
- **Test Command:** ping -p "00000000EEEEEEEEEEEE" 127.0.0.0
- **Explanation:** This rule triggers when an ICMP Echo Request contains the payload "EEEEEEEEEEEE".

Output:



```
11/10-19:12:27.503756  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.1
11/10-19:12:28.527788  [**] [1:465:3] ICMP ISS Pinger [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.
11/10-19:12:28.527864  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.1
11/10-19:12:29.551705  [**] [1:465:3] ICMP ISS Pinger [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.
11/10-19:12:29.551753  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.1
11/10-19:13:20.728486  [**] [1:465:3] ICMP ISS Pinger [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.
11/10-19:13:20.729926  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.1
11/10-19:13:20.730197  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.1
11/10-19:13:21.744039  [**] [1:1000001:1] ICMP Flood Attack Detected [**] [Priority: 0] {ICMP} 127.0.0.1 -> 127.0.0.0
11/10-19:13:21.744039  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.1
11/10-19:13:21.744042  [**] [1:1000001:1] ICMP Flood Attack Detected [**] [Priority: 0] {ICMP} 127.0.0.0 -> 127.0.0.1
11/10-19:13:21.744210  [**] [1:465:3] ICMP ISS Pinger [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.
11/10-19:13:22.768100  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.1
11/10-19:13:22.768100  [**] [1:465:3] ICMP ISS Pinger [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.
11/10-19:13:23.791750  [**] [1:465:3] ICMP ISS Pinger [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.
11/10-19:13:23.796636  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.1
11/10-19:13:24.816636  [**] [1:465:3] ICMP ISS Pinger [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.
11/10-19:13:24.819629  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 127.0.0.1
```

```
  GNU nano 6.2                    run_icmp_tests.sh
ping -i 666 -s 0 -w 5 127.0.0.0 &

# Testcase 7: Testing ICMP Redirect Host
echo "Executing Testcase 7: Testing ICMP Redirect Host"
sudo hping3 --icmp --icmp-icode 1 --icmp-type 5 -w 5 127.0.0.0 &

# Testcase 8: Testing ICMP Redirect Net
echo "Executing Testcase 8: Testing ICMP Redirect Net"
sudo hping3 --icmp --icmp-icode 0 --icmp-type 5 -w 5 127.0.0.0 &

# Testcase 9: Testing ICMP Superscan Echo
echo "Executing Testcase 9: Testing ICMP Superscan Echo"
ping -p "0000000000000000" -w 5 127.0.0.0 &

# Testcase 10: Testing ICMP Traceroute IP Options
                              [ Wrote 46 lines ]
^G Help       ^O Write Out ^W Where Is  ^K Cut        ^T Execute    ^C Loc
^X Exit       ^R Read File ^\ Replace   ^U Paste      ^J Justify    ^/ Go
```

vboxuser@Ubuntu22: /etc/snort/rules

```
-rw-r--r-- 1 root     root       5067 Dec  3  2021 p2p.rules
-rw-r--r-- 1 root     root       6183 Dec  3  2021 policy.rules
-rw-r--r-- 1 root     root       2088 Dec  3  2021 pop2.rules
-rw-r--r-- 1 root     root       9591 Dec  3  2021 pop3.rules
-rw-r--r-- 1 root     root       5918 Dec  3  2021 porn.rules
-rw-r--r-- 1 root     root      52531 Dec  3  2021 rpc.rules
-rw-r--r-- 1 root     root       3784 Dec  3  2021 rservices.rules
-rw-r--r-- 1 root     root       4952 Dec  3  2021 scan.rules
-rw-r--r-- 1 root     root       9904 Dec  3  2021 shellcode.rules
-rw-r--r-- 1 root     root      23990 Dec  3  2021 smtp.rules
-rw-r--r-- 1 root     root       5779 Dec  3  2021 snmp.rules
-rw-r--r-- 1 root     root      18330 Dec  3  2021 sql.rules
-rw-r--r-- 1 root     root       5118 Dec  3  2021 telnet.rules
-rw-r--r-- 1 root     root       3424 Dec  3  2021 tftp.rules
-rw-r--r-- 1 root     root       2075 Dec  3  2021 virus.rules
-rw-r--r-- 1 root     root      11089 Dec  3  2021 web-attacks.rules
-rw-r--r-- 1 root     root     103203 Dec  3  2021 web-cgi.rules
-rw-r--r-- 1 root     root      10980 Dec  3  2021 web-client.rules
-rw-r--r-- 1 root     root      10026 Dec  3  2021 web-coldfusion.rules
-rw-r--r-- 1 root     root      10417 Dec  3  2021 web-frontpage.rules
-rw-r--r-- 1 root     root      40907 Dec  3  2021 web-iis.rules
-rw-r--r-- 1 root     root      97307 Dec  3  2021 web-misc.rules
-rw-r--r-- 1 root     root      36661 Dec  3  2021 web-php.rules
-rw-r--r-- 1 root     root       1437 Dec  3  2021 x11.rules
vboxuser@Ubuntu22:/etc/snort/rules$ nano icmp_flood.rules
vboxuser@Ubuntu22:/etc/snort/rules$ 
```

vboxuser@Ubuntu22: /etc/s...

```
--- 127.0.0.0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time
 4088ms
rtt min/avg/max/mdev = 0.006/0.019/0.032/0.009 ms

--- 127.0.0.0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time
 4090ms


--- 127.0.0.0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time
 4089ms
rtt min/avg/max/mdev = 0.007/0.016/0.032/0.010 ms

--- 127.0.0.0 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time
 4087ms
--- 127.0.0.0 ping statistics ---
rtt min/avg/max/mdev = 0.007/0.019/0.042/0.013 ms
5 packets transmitted, 5 received, 0% packet loss, time
 4089ms
rtt min/avg/max/mdev = 0.005/0.014/0.030/0.008 ms
All tests executed.
vboxuser@Ubuntu22:/etc/snort$ 
```

vboxuser@Ubuntu22: /etc/snort/rules

```
ING 127.0.0.0 (127.0.0.0) 56(84) bytes of data.
4 bytes from 127.0.0.0: icmp_seq=1 ttl=64 time=0.030 ms
4 bytes from 127.0.0.0: icmp_seq=2 ttl=64 time=0.032 ms
4 bytes from 127.0.0.0: icmp_seq=3 ttl=64 time=0.041 ms
4 bytes from 127.0.0.0: icmp_seq=4 ttl=64 time=0.044 ms
4 bytes from 127.0.0.0: icmp_seq=5 ttl=64 time=0.031 ms
4 bytes from 127.0.0.0: icmp_seq=6 ttl=64 time=0.032 ms
4 bytes from 127.0.0.0: icmp_seq=7 ttl=64 time=0.036 ms
4 bytes from 127.0.0.0: icmp_seq=8 ttl=64 time=0.033 ms
4 bytes from 127.0.0.0: icmp_seq=9 ttl=64 time=0.033 ms
4 bytes from 127.0.0.0: icmp_seq=10 ttl=64 time=0.031 ms
4 bytes from 127.0.0.0: icmp_seq=11 ttl=64 time=0.028 ms
4 bytes from 127.0.0.0: icmp_seq=12 ttl=64 time=0.032 ms
4 bytes from 127.0.0.0: icmp_seq=13 ttl=64 time=0.028 ms
4 bytes from 127.0.0.0: icmp_seq=14 ttl=64 time=0.032 ms
4 bytes from 127.0.0.0: icmp_seq=15 ttl=64 time=0.029 ms
4 bytes from 127.0.0.0: icmp_seq=16 ttl=64 time=0.031 ms
4 bytes from 127.0.0.0: icmp_seq=17 ttl=64 time=0.034 ms
Z
10]+  Stopped                 ping -p "495353504e475251" 127.0.0.0
boxuser@Ubuntu22:/etc/snort/rules$ sudo ping -b -f 127.0.0.0
sudo] password for vboxuser:
ING 127.0.0.0 (127.0.0.0) 56(84) bytes of data.
^Z
11]+  Stopped                 sudo ping -b -f 127.0.0.0
boxuser@Ubuntu22:/etc/snort/rules$ sudo ping -b -f 127.0.0.0
```

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.