

INFORMATION SECURITY MANAGEMENT

LAB ASSESSMENT – 05

NAME: HARIKRISHNAKUMAR S

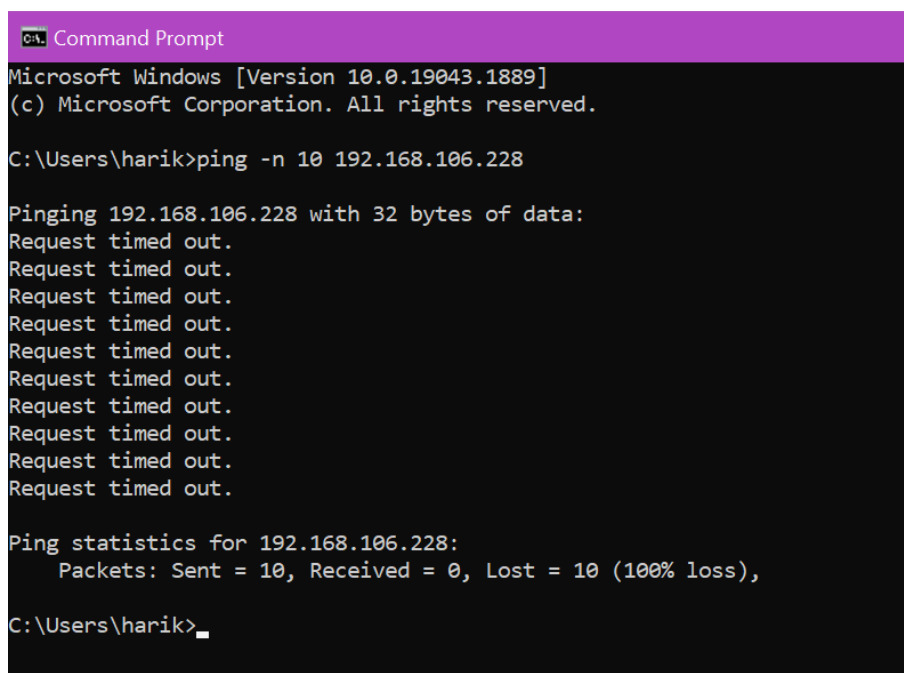
REG NO: 20MIS0166

1) Create different scenarios to troubleshoot internal and external attacks by correlating commands and wireshark.

These occur when the threat originates from outside the organization's network or infrastructure. External attacks are typically perpetrated by individuals or entities who do not have authorized access to the organization's systems. External attackers may attempt to breach the organization's defenses through various means, such as exploiting software vulnerabilities, launching phishing attacks, conducting distributed denial-of-service (DDoS) attacks, or infiltrating the network through social engineering tactics.

This involves simulating an external attack by flooding a laptop with ICMP packets. The attacker is my friend using his laptop, continuously pings the target (Me) laptop's IP address, causing network congestion and potential disruption. The objective is to understand the impact of ICMP flooding on network performance and security.

“ping -n 10 192.168.106.228”

A screenshot of a Windows Command Prompt window. The title bar is purple and says "C:\ Command Prompt". The window content shows the following text: "Microsoft Windows [Version 10.0.19043.1889] (c) Microsoft Corporation. All rights reserved. C:\Users\harik>ping -n 10 192.168.106.228". This is followed by ten lines of "Request timed out." and then "Ping statistics for 192.168.106.228: Packets: Sent = 10, Received = 0, Lost = 10 (100% loss),". The prompt ends with "C:\Users\harik>".

```
C:\ Command Prompt
Microsoft Windows [Version 10.0.19043.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Users\harik>ping -n 10 192.168.106.228

Pinging 192.168.106.228 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.106.228:
    Packets: Sent = 10, Received = 0, Lost = 10 (100% loss),

C:\Users\harik>
```

No.	Time	Source	Destination	Protocol	Length	Info
6	2.992369	172.16.110.205	172.16.110.205	ICMP	84	Destination unreachable (Host unreachable)
7	7.005852	172.16.110.205	172.16.110.205	ICMP	84	Destination unreachable (Host unreachable)
8	14.865465	:::1	:::1	TCP	65	64263 → 8889 [ACK] Seq=1 Ack=1 Win=10141 Len=1
9	14.865490	:::1	:::1	TCP	76	8889 → 64263 [ACK] Seq=1 Ack=2 Win=10179 Len=0 SLE=1 SRE=
10	14.998779	172.16.110.205	172.16.110.205	ICMP	84	Destination unreachable (Host unreachable)
11	21.319123	:::1	:::1	TCP	65	64307 → 8889 [ACK] Seq=1 Ack=1 Win=10224 Len=1
12	21.319144	:::1	:::1	TCP	76	8889 → 64307 [ACK] Seq=1 Ack=2 Win=10230 Len=0 SLE=1 SRE=
13	30.030128	:::1	:::1	TCP	66	8889 → 64142 [PSH, ACK] Seq=3 Ack=7 Win=10052 Len=2
14	30.030167	:::1	:::1	TCP	64	64142 → 8889 [ACK] Seq=7 Ack=5 Win=10139 Len=0
15	30.030285	:::1	:::1	TCP	70	64142 → 8889 [PSH, ACK] Seq=7 Ack=5 Win=10139 Len=6
16	30.030320	:::1	:::1	TCP	64	8889 → 64142 [ACK] Seq=5 Ack=13 Win=10052 Len=0
17	34.848249	:::1	:::1	TCP	65	64262 → 8889 [ACK] Seq=1 Ack=1 Win=10191 Len=1
18	34.848270	:::1	:::1	TCP	76	8889 → 64262 [ACK] Seq=1 Ack=2 Win=10192 Len=0 SLE=1 SRE=
19	36.640396	:::1	:::1	TCP	65	64008 → 8889 [ACK] Seq=1 Ack=1 Win=10029 Len=1
20	36.640424	:::1	:::1	TCP	76	8889 → 64008 [ACK] Seq=1 Ack=2 Win=10230 Len=0 SLE=1 SRE=

A packet with Response and reply received from the attacker is displayed below:

Certain packets had its TTL exceeded and couldn't reach.

Remaining packets couldn't get any response.

▼ Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_Loopback, id 0	
Section number: 1	
<ul style="list-style-type: none"> Interface id: 0 (\Device\NPF_Loopback) Encapsulation type: NULL/Loopback (15) Arrival Time: Apr 26, 2024 22:10:44.203862000 India Standard Time UTC Arrival Time: Apr 26, 2024 16:40:44.203862000 UTC Epoch Arrival Time: 1714149644.203862000 [Time shift for this packet: 0.000000000 seconds] [Time delta from previous captured frame: 0.000000000 seconds] [Time delta from previous displayed frame: 0.000000000 seconds] [Time since reference or first frame: 0.000000000 seconds] Frame Number: 1 Frame Length: 84 bytes (672 bits) Capture Length: 84 bytes (672 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: null:ip:icmp:ip:tcp] [Coloring Rule Name: ICMP errors] [Coloring Rule String: icmp.type in { 3..5, 11 } icmpv6.type in { 1..4 }] 	
▼ Null/Loopback	
Family: IP (2)	
▼ Internet Protocol Version 4, Src: 172.16.110.205, Dst: 172.16.110.205	
0100 = Version: 4	
.... 0101 = Header Length: 20 bytes (5)	
<ul style="list-style-type: none"> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 80 Identification: 0x00cb (203) 000. = Flags: 0x0 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 128 Protocol: ICMP (1) Header Checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] 	

With this packet we can find who the attacker is along with his IP and device name as marked in the below image

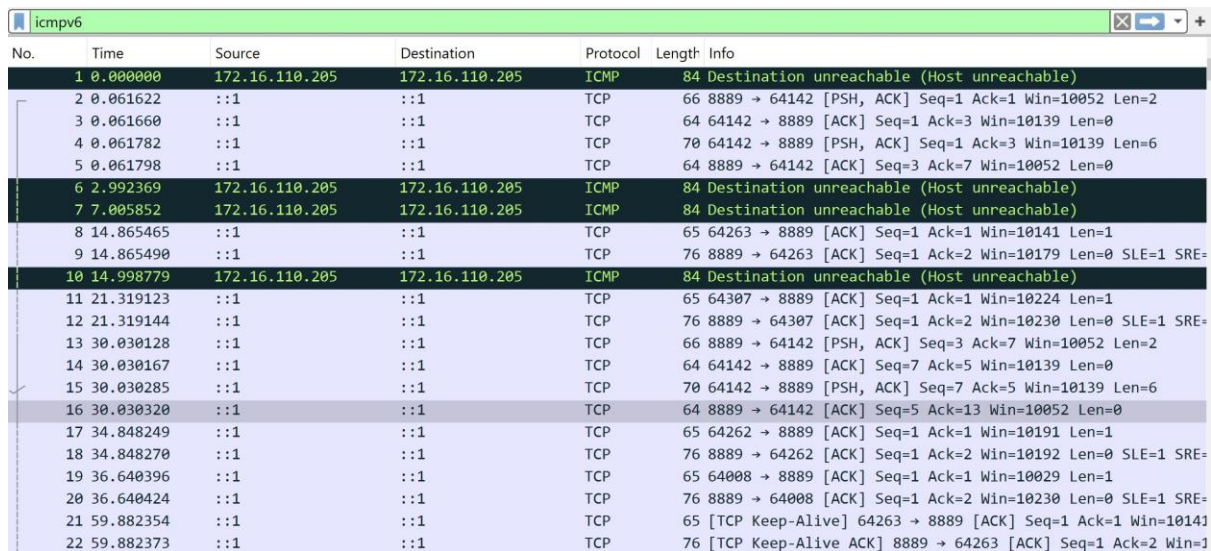
We can also retrieve the user name of this attacker.

Neighbour Solicitation (NS):

1. NS messages are sent by an IPv6 node to request the link-layer address (MAC address) of another node on the same link.
2. NS messages are typically sent in two scenarios:
 - When a node wants to resolve the link-layer address of a neighbor for which it has an IPv6 address.
 - When a node performs Duplicate Address Detection (DAD) to check if its own IPv6 address is already in use on the network.

Neighbour Advertisement (NA):

1. NA messages are sent in response to NS messages to provide the link-layer address (MAC address) to the sender.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.110.205	172.16.110.205	ICMP	84	Destination unreachable (Host unreachable)
2	0.061622	::1	::1	TCP	66	8889 → 64142 [PSH, ACK] Seq=1 Ack=1 Win=10052 Len=2
3	0.061660	::1	::1	TCP	64	64142 → 8889 [ACK] Seq=1 Ack=3 Win=10139 Len=0
4	0.061782	::1	::1	TCP	70	64142 → 8889 [PSH, ACK] Seq=1 Ack=3 Win=10139 Len=6
5	0.061798	::1	::1	TCP	64	8889 → 64142 [ACK] Seq=3 Ack=7 Win=10052 Len=0
6	2.992369	172.16.110.205	172.16.110.205	ICMP	84	Destination unreachable (Host unreachable)
7	7.005852	172.16.110.205	172.16.110.205	ICMP	84	Destination unreachable (Host unreachable)
8	14.865465	::1	::1	TCP	65	64263 → 8889 [ACK] Seq=1 Ack=1 Win=10141 Len=1
9	14.865490	::1	::1	TCP	76	8889 → 64263 [ACK] Seq=1 Ack=2 Win=10179 Len=0 SLE=1 SRE=
10	14.998779	172.16.110.205	172.16.110.205	ICMP	84	Destination unreachable (Host unreachable)
11	21.319123	::1	::1	TCP	65	64307 → 8889 [ACK] Seq=1 Ack=1 Win=10224 Len=1
12	21.319144	::1	::1	TCP	76	8889 → 64307 [ACK] Seq=1 Ack=2 Win=10230 Len=0 SLE=1 SRE=
13	30.030128	::1	::1	TCP	66	8889 → 64142 [PSH, ACK] Seq=3 Ack=7 Win=10052 Len=2
14	30.030167	::1	::1	TCP	64	64142 → 8889 [ACK] Seq=7 Ack=5 Win=10139 Len=0
15	30.030285	::1	::1	TCP	70	64142 → 8889 [PSH, ACK] Seq=7 Ack=5 Win=10139 Len=6
16	30.030320	::1	::1	TCP	64	8889 → 64142 [ACK] Seq=5 Ack=13 Win=10052 Len=0
17	34.848249	::1	::1	TCP	65	64262 → 8889 [ACK] Seq=1 Ack=1 Win=10191 Len=1
18	34.848270	::1	::1	TCP	76	8889 → 64262 [ACK] Seq=1 Ack=2 Win=10192 Len=0 SLE=1 SRE=
19	36.640396	::1	::1	TCP	65	64008 → 8889 [ACK] Seq=1 Ack=1 Win=10029 Len=1
20	36.640424	::1	::1	TCP	76	8889 → 64008 [ACK] Seq=1 Ack=2 Win=10230 Len=0 SLE=1 SRE=
21	59.882354	::1	::1	TCP	65	[TCP Keep-Alive] 64263 → 8889 [ACK] Seq=1 Ack=1 Win=10141
22	59.882373	::1	::1	TCP	76	[TCP Keep-Alive ACK] 8889 → 64263 [ACK] Seq=1 Ack=2 Win=1

Internal Attacks:

Considering I work for the Google organisation. Internal attacks occur when the threat originates from within the organization's network or infrastructure. Internal attacks are typically carried out by insiders, such as employees, contractors, or partners who have authorized access to the organization's systems. Internal attackers may exploit vulnerabilities in the system, abuse their privileges, or engage in malicious activities for personal gain or other motives.

```
C:\Users\harik>ping -n 50 www.google.com

Pinging www.google.com [142.250.196.68] with 32 bytes of data:
Reply from 142.250.196.68: bytes=32 time=13ms TTL=58
Reply from 142.250.196.68: bytes=32 time=143ms TTL=58
Reply from 142.250.196.68: bytes=32 time=11ms TTL=58
Reply from 142.250.196.68: bytes=32 time=10ms TTL=58
Reply from 142.250.196.68: bytes=32 time=12ms TTL=58
Reply from 142.250.196.68: bytes=32 time=13ms TTL=58
Reply from 142.250.196.68: bytes=32 time=8ms TTL=58
Reply from 142.250.196.68: bytes=32 time=12ms TTL=58
Reply from 142.250.196.68: bytes=32 time=39ms TTL=58
Reply from 142.250.196.68: bytes=32 time=52ms TTL=58
Reply from 142.250.196.68: bytes=32 time=7ms TTL=58
Request timed out.
Reply from 142.250.196.68: bytes=32 time=88ms TTL=58
Reply from 142.250.196.68: bytes=32 time=58ms TTL=58
Reply from 142.250.196.68: bytes=32 time=32ms TTL=58
Reply from 142.250.196.68: bytes=32 time=46ms TTL=58
Reply from 142.250.196.68: bytes=32 time=33ms TTL=58
Reply from 142.250.196.68: bytes=32 time=96ms TTL=58
Reply from 142.250.196.68: bytes=32 time=25ms TTL=58
Reply from 142.250.196.68: bytes=32 time=15ms TTL=58
Reply from 142.250.196.68: bytes=32 time=58ms TTL=58
Reply from 142.250.196.68: bytes=32 time=5ms TTL=58
Reply from 142.250.196.68: bytes=32 time=10ms TTL=58
Request timed out.
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.110.205	172.16.110.205	ICMP	84	Destination unreachable (Host unreachable)
2	0.061622	:::1	:::1	TCP	66	8889 → 64142 [PSH, ACK] Seq=1 Ack=1 Win=10052 Len=2
3	0.061660	:::1	:::1	TCP	64	64142 → 8889 [ACK] Seq=1 Ack=3 Win=10139 Len=0
4	0.061782	:::1	:::1	TCP	70	64142 → 8889 [PSH, ACK] Seq=1 Ack=3 Win=10139 Len=6
5	0.061798	:::1	:::1	TCP	64	8889 → 64142 [ACK] Seq=3 Ack=7 Win=10052 Len=0
6	2.992369	172.16.110.205	172.16.110.205	ICMP	84	Destination unreachable (Host unreachable)
7	7.005852	172.16.110.205	172.16.110.205	ICMP	84	Destination unreachable (Host unreachable)
8	14.865465	:::1	:::1	TCP	65	64263 → 8889 [ACK] Seq=1 Ack=1 Win=10141 Len=1
9	14.865490	:::1	:::1	TCP	76	8889 → 64263 [ACK] Seq=1 Ack=2 Win=10179 Len=0 SLE=1 SRE=
10	14.998779	172.16.110.205	172.16.110.205	ICMP	84	Destination unreachable (Host unreachable)
11	21.319123	:::1	:::1	TCP	65	64307 → 8889 [ACK] Seq=1 Ack=1 Win=10224 Len=1
12	21.319144	:::1	:::1	TCP	76	8889 → 64307 [ACK] Seq=1 Ack=2 Win=10230 Len=0 SLE=1 SRE=
13	30.030128	:::1	:::1	TCP	66	8889 → 64142 [PSH, ACK] Seq=3 Ack=7 Win=10052 Len=2
14	30.030167	:::1	:::1	TCP	64	64142 → 8889 [ACK] Seq=7 Ack=5 Win=10139 Len=0
15	30.030285	:::1	:::1	TCP	70	64142 → 8889 [PSH, ACK] Seq=7 Ack=5 Win=10139 Len=6
16	30.030320	:::1	:::1	TCP	64	8889 → 64142 [ACK] Seq=5 Ack=13 Win=10052 Len=0
17	34.848249	:::1	:::1	TCP	65	64262 → 8889 [ACK] Seq=1 Ack=1 Win=10191 Len=1
18	34.848270	:::1	:::1	TCP	76	8889 → 64262 [ACK] Seq=1 Ack=2 Win=10192 Len=0 SLE=1 SRE=
19	36.640396	:::1	:::1	TCP	65	64008 → 8889 [ACK] Seq=1 Ack=1 Win=10029 Len=1
20	36.640424	:::1	:::1	TCP	76	8889 → 64008 [ACK] Seq=1 Ack=2 Win=10230 Len=0 SLE=1 SRE=
21	59.882354	:::1	:::1	TCP	65	[TCP Keep-Alive] 64263 → 8889 [ACK] Seq=1 Ack=1 Win=10141
22	59.882373	:::1	:::1	TCP	76	[TCP Keep-Alive ACK] 8889 → 64263 [ACK] Seq=1 Ack=2 Win=1

Use Wireshark's analysis features to pinpoint the source of the problem. Look for issues like misconfigurations, packet loss, network congestion, or protocol errors.

```
Destination Address: 172.16.110.205
▼ Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 1 (Host unreachable)
  Checksum: 0x588c [correct]
  [Checksum Status: Good]
  Unused: 00000000
▼ Internet Protocol Version 4, Src: 172.16.110.205, Dst: 172.16.107.52
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 0x9f5d (40797)
  > 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.16.110.205
  Destination Address: 172.16.107.52
▼ Transmission Control Protocol, Src Port: 64546, Dst Port: 7680, Seq: 3300122665
  Source Port: 64546
  Destination Port: 7680
  Sequence Number: 3300122665
  [Stream index: 0]
  > [Conversation completeness: Incomplete, SYN_SENT (1)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
```

Once the problem is identified, take appropriate action to resolve it. This may involve adjusting network configurations, updating software, or contacting network administrators.

Verify Solutions: After implementing solutions, monitor network traffic to ensure the problem is resolved. Use Wireshark to verify that the issue no longer exists and that network traffic is functioning as expected.