

(ITS64904 Computer Intrusion Detection)

Practical 2: Perform Footprinting Through Ping Command

Date: 11/10/2024

1. Using the Command Prompt window and type in **ping www.watsons.com.my** and press Enter to get its IP address. The result below will show that the target domain's IP address is (23.51.36.41). It will also show the Ping Statistics such as packet sent, packet received, packet lost, and approximately round trip times.

```
C:\Users\User>ping www.watsons.com.my

Pinging e9073.a.akamaiedge.net [23.51.36.41] with 32 bytes of data:
Reply from 23.51.36.41: bytes=32 time=59ms TTL=53
Reply from 23.51.36.41: bytes=32 time=119ms TTL=53
Reply from 23.51.36.41: bytes=32 time=106ms TTL=53
Reply from 23.51.36.41: bytes=32 time=219ms TTL=53

Ping statistics for 23.51.36.41:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 59ms, Maximum = 219ms, Average = 125ms
```

Screenshot 1

2. Next part is to type in **ping www.watsons.com.my -f -l 1500**. This ping will show the response needs to be fragmented, but the DF set means the frame is too large to be on the network. The packet was not sent as we used the -f switch with the ping command, which returned that kind of error.

```
C:\Users\User>ping www.watsons.com.my -f -l 1500

Pinging e9073.a.akamaiedge.net [23.51.36.41] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 23.51.36.41:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Screenshot 2

3. The output will be different if using the **ping www.watsons.com.my -f -l 1300** as the maximum packet size is less than 1500 bytes and more than 1300 bytes.

```
C:\Users\User>ping www.watsons.com.my -f -l 1300

Pinging e9073.a.akamaiedge.net [23.51.36.41] with 1300 bytes of data:
Reply from 23.51.36.41: bytes=1300 time=41ms TTL=53
Reply from 23.51.36.41: bytes=1300 time=69ms TTL=53
Reply from 23.51.36.41: bytes=1300 time=2114ms TTL=53
Reply from 23.51.36.41: bytes=1300 time=43ms TTL=53

Ping statistics for 23.51.36.41:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 41ms, Maximum = 2114ms, Average = 566ms
```

Screenshot 3

4. With different values like **ping www.watsons.com.my -f -l 1472** it replies with a successful ping. While **ping www.watsons.com.my -f -l 1473** replies with Packets need to be fragmented but DF set. This indicates 1472 bytes is the maximum frame size on this machine's network.

```
C:\Users\User>ping www.watsons.com.my -f -l 1473

Pinging e9073.a.akamaiedge.net [23.51.36.41] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 23.51.36.41:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Screenshot 4

```
C:\Users\User>ping www.watsons.com.my -f -l 1472

Pinging e9073.a.akamaiedge.net [23.51.36.41] with 1472 bytes of data:
Reply from 23.51.36.41: bytes=1472 time=1167ms TTL=55
Reply from 23.51.36.41: bytes=1472 time=272ms TTL=55
Reply from 23.51.36.41: bytes=1472 time=108ms TTL=55
Reply from 23.51.36.41: bytes=1472 time=338ms TTL=55

Ping statistics for 23.51.36.41:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 108ms, Maximum = 1167ms, Average = 471ms
```

Screenshot 5

5. In the Command Prompt with the **ping www.watsons.com.my -i 3** it will set the time to live (-i) value as 3. **Reply from 10.99.4.65: TTL expired in transit**, which means that the router (10.99.4.65, students will have some other IP address) discarded the frame because its TTL has expired which means it reached 0.

```
C:\Users\User>ping www.watsons.com.my -i 3

Pinging e9073.a.akamaiedge.net [23.51.36.41] with 32 bytes of data:
Reply from 10.99.4.65: TTL expired in transit.
Reply from 10.99.4.65: TTL expired in transit.
Reply from 10.99.4.65: TTL expired in transit.
Reply from 10.99.4.65: TTL expired in transit.

Ping statistics for 23.51.36.41:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Screenshot 6

6. The **ping www.watsons.com.my -i 2 -n 1** will set the TTL to 2 and the -n value to 1 to check the packet's life span. The same is true for the **ping www.watson.com.my -i 3 -n 1**, which will set the TTL value to 3. The **ping www.watsons.com.my -i 4 -n 1** also sets the TTL value to 4.

```
C:\Users\User>ping www.watsons.com.my -i 2 -n 1

Pinging e9073.a.akamaiedge.net [23.51.36.41] with 32 bytes of data:
Reply from 10.99.4.33: TTL expired in transit.

Ping statistics for 23.51.36.41:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

C:\Users\User>ping www.watsons.com.my -i 3 -n 1

Pinging e9073.a.akamaiedge.net [23.51.36.41] with 32 bytes of data:
Reply from 10.99.4.65: TTL expired in transit.

Ping statistics for 23.51.36.41:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

C:\Users\User>ping www.watsons.com.my -i 4 -n 1

Pinging e9073.a.akamaiedge.net [23.51.36.41] with 32 bytes of data:
Reply from 10.99.4.84: TTL expired in transit.

Ping statistics for 23.51.36.41:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

Screenshot 7

7. The successful ping to reach www.watsons.com.my is 13 hops. This will reach the IP address of www.watsons.com.my (23.51.36.41). The ping www.watsons.com.my -i 12 -n 1 will show **Reply from 218.100.44.170: TTL expired in transit**. This implies that the destination host receives the reply at a time-to-live value of 13 (23.51.36.41).

```
C:\Users\User>ping www.watsons.com.my -i 13 -n 1
Pinging e9073.a.akamaiedge.net [23.51.36.41] with 32 bytes of data:
Reply from 23.51.36.41: bytes=32 time=51ms TTL=53

Ping statistics for 23.51.36.41:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 51ms, Maximum = 51ms, Average = 51ms

C:\Users\User>ping www.watsons.com.my -i 14 -n 1
Pinging e9073.a.akamaiedge.net [23.51.36.41] with 32 bytes of data:
Reply from 23.51.36.41: bytes=32 time=46ms TTL=53

Ping statistics for 23.51.36.41:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 46ms, Maximum = 46ms, Average = 46ms
```

Screenshot 8

```
C:\Users\User>ping www.watsons.com.my -i 12 -n 1
Pinging e9073.a.akamaiedge.net [23.51.36.41] with 32 bytes of data:
Reply from 218.100.44.170: TTL expired in transit.

Ping statistics for 23.51.36.41:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

Screenshot 9

8. To summarize from this report:

Maximum hops are: 13

Maximum frame size of the packet: 1472 bytes (23.51.36.41)