1.

With admin privilege:

Text

Description automatically generated

Without admin privilege:

Text

Description automatically generated

I see no difference on my Windows machine.

1).

A picture containing text, monitor, screen, screenshot

Description automatically generated

2).

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

3). stacking IP header over ICMP()

Text

Description automatically generated

Similary, UDP()

Text

Description automatically generated

4).

UDP segment:

Text

Description automatically generated

ICMP segment

Text

Description automatically generated

2. Sniffing Packets

Note, for this lab, I have to use dst instead of pkt[IP].src, as from my machine it is not accessible to 8.8.8.8

Text

Description automatically generated

3. Sniff function with BPF filters

Applied BPF filters as below:

pkt = sniff(filter='icmp and dst 8.8.8.8',prn=print\_pkt)

result:

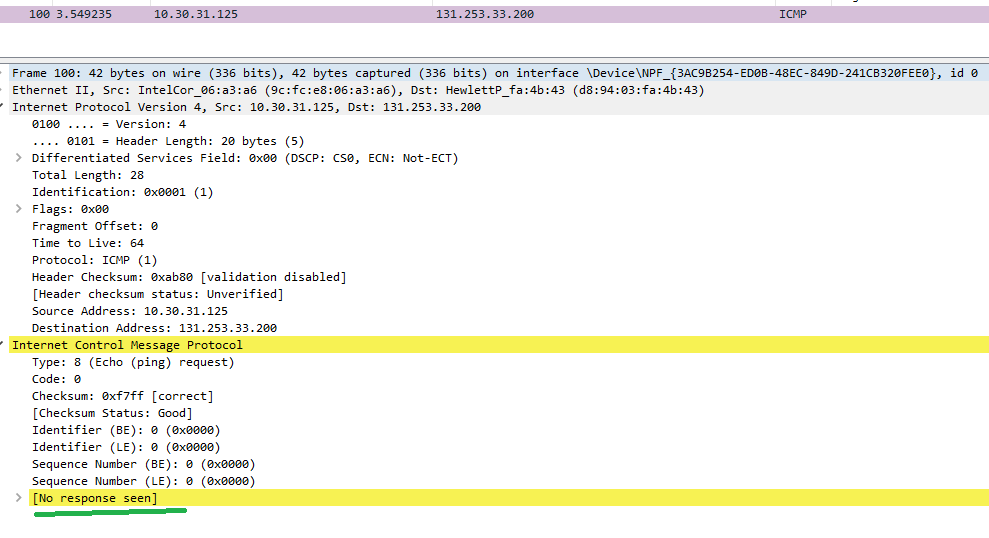
Text

Description automatically generated

4. Spoofing ICMP Packets

8.8.8.8 is not reachable from my machine, switching to [www.bing.com](http://www.bing.com)

From Wireshark no response was observed, as a fake src was in the request package, the response probably has been directed to the fake one rather than the real src.



5. sniffing-then-spoofing

8.8.8.8 is not reachable, therefore, using ‘10.5.40.12’ instead. So here are the code executed:

#!/usr/bin/python3

from scapy.all import \*

def spoof\_pkt(pkt):

  if ICMP in pkt and pkt[ICMP].type == 8:

    ip = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl)

    icmp = ICMP(type=0, id=pkt[ICMP].id, seq=pkt[ICMP].seq)

    data = pkt[Raw].load

    newpkt = ip/icmp/data

    print("Spoofed Packet.........")

    print("Source IP : ", newpkt[IP].src)

    print("Destination IP :", newpkt[IP].dst)

    send(newpkt,verbose=0)

pkt = sniff(filter='icmp and host 10.5.40.12',prn=spoof\_pkt)

and result in Wireshark, I observed there is an unreachable error after everything normal ping-response round.

Graphical user interface, text, application

Description automatically generated