

```
[04/07/24]seed@VM:~/Labsetup-lab10$ python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> from scapy.all import *
>>> help(sniff)

>>>
```

```
[04/07/24]seed@VM:~/Labsetup-lab10$ ifconfig
br-682e2178e964: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.9.0.1 netmask 255.255.255.0 broadcast 10.9.0.255
    inet6 fe80::42:19ff:fe41:33ce prefixlen 64 scopeid 0x20<link>
    ether 02:42:19:41:33:ce txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27 bytes 3359 (3.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

br-682e2178e964

```
[04/07/24]seed@VM:~/.../volumes$ cat sniff.py
#!/usr/bin/env python3
from scapy.all import *
def print_pkt(pkt):
    pkt.show()
pkt = sniff(iface='br-682e2178e964', filter='', prn=print_pkt)
```

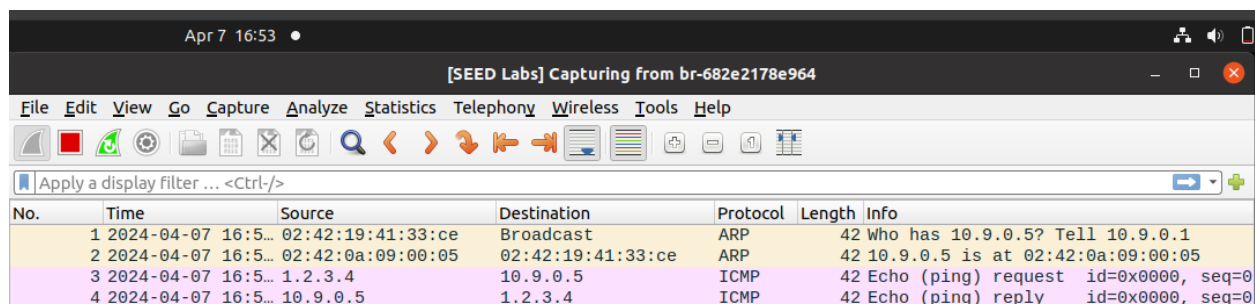
```

^[[A^Croot@VM:/volumes# python3 sniff.py
###[ Ethernet ]###
    dst      = 02:42:0a:09:00:05
    src      = 02:42:19:41:33:ce
    type     = IPv4
###[ IP ]###
    version  = 4
    ihl      = 5
    tos      = 0x0
    len      = 84
    id       = 50276
    flags    = DF
    frag     = 0
    ttl      = 64
    proto    = icmp
    chksum   = 0x622d
    src      = 10.9.0.1
    dst      = 10.9.0.5
    \options \
###[ ICMP ]###
    type     = echo-request

```

Q1. Is the spoofed request accepted by the receiver?

Yes it is accepted by the receiver:



No.	Time	Source	Destination	Protocol	Length	Info
1	2024-04-07 16:5...	02:42:19:41:33:ce	Broadcast	ARP	42	Who has 10.9.0.5? Tell 10.9.0.1
2	2024-04-07 16:5...	02:42:0a:09:00:05	02:42:19:41:33:ce	ARP	42	10.9.0.5 is at 02:42:0a:09:00:05
3	2024-04-07 16:5...	1.2.3.4	10.9.0.5	ICMP	42	Echo (ping) request id=0x0000, seq=0
4	2024-04-07 16:5...	10.9.0.5	1.2.3.4	ICMP	42	Echo (ping) reply id=0x0000, seq=0

o If it is accepted, is an echo reply packet sent to the spoofed IP

Yes, a ping echo was sent to '1.2.3.4' despite it actually being sent from the attacker ip? See no 4

Q2. Why is this considered a "spoofed" packet?

This is considered a spoofed packet because the source IP address of the packet is forged or falsified to appear as if it is coming from a different sender.

ping 8.8.8.8 (an existing host on the Internet)

Now when ping 8.8.8.8 there is duplicates as both the real and attack are sending packets back.

The screenshot shows a terminal window on the left and a Wireshark packet capture window on the right. The terminal window displays the output of a ping command to 8.8.8.8, showing multiple duplicate responses. The Wireshark window shows a capture of these ping requests and replies, with a filter applied to show only ICMP Echo (ping) requests and replies. The packet list shows multiple ICMP Echo (ping) requests and replies, indicating a flood of traffic.

```

root@24bb02ced36:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=13.0 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=64 time=62.0 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=7.13 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=64 time=80.9 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=6.93 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=64 time=115 ms (DUP!)

len      = 84
id       = 1
flags    =
frag     = 0
ttl      = 64
proto    = icmp
chksum   = 0x668d
src      = 10.9.0.5
dst      = 10.9.0.5
options  \
###[ ICMP ]###
type     = echo-reply
code     = 0
chksum   = 0x29f8
id       = 0x36
seq      = 0x3
###[ Raw ]###
load     = 's\r\x1f\x00\x00\x00\x00\x89\x88\x07\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"$%&'()*+,-./01234567'

Sent 1 packets.

```

Wireshark packet capture details:

No.	Time	Source	Destination	Protocol	Length	Info
1	2024-04-07 17:11:10.90.5	10.9.0.5	8.8.8.8	ICMP	98	Echo (ping) request
2	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
3	2024-04-07 17:11:02:42:19:41:33:ce	Broadcast	ARP	42	Who has 10.9.0.5?	
4	2024-04-07 17:11:02:42:0a:09:00:05	02:42:19:41:33:ce	ARP	42	10.9.0.5 is at 02:42:19:41:33:ce	
5	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
6	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
7	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
8	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
9	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
10	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
11	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
12	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
13	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
14	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
15	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
16	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
17	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
18	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
19	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
20	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
21	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
22	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
23	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
24	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
25	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
26	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
27	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
28	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
29	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply
30	2024-04-07 17:11:10.9.0.5	10.9.0.5	10.9.0.5	ICMP	98	Echo (ping) reply

ping 10.9.0.99 (a non-existing host on the LAN)

Nothing happens since it is not reachable and attacker which the attacker is trying to send packets from, so they're not received since the victim doesn't see a connection.

The screenshot shows a terminal window on the left and a Wireshark packet capture window on the right. The terminal window displays the output of a ping command to 10.9.0.99, showing that the destination is unreachable. The Wireshark window shows a capture of these ping requests, but no replies are received. The packet list shows ICMP Echo (ping) requests, but no replies are present.

```

root@24bb02ced36:~# ping 10.9.0.99
PING 10.9.0.99 (10.9.0.99) 56(84) bytes of data.
From 10.9.0.5 icmp_seq=1 Destination Host Unreachable
From 10.9.0.5 icmp_seq=2 Destination Host Unreachable
From 10.9.0.5 icmp_seq=3 Destination Host Unreachable
^C
--- 10.9.0.99 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4

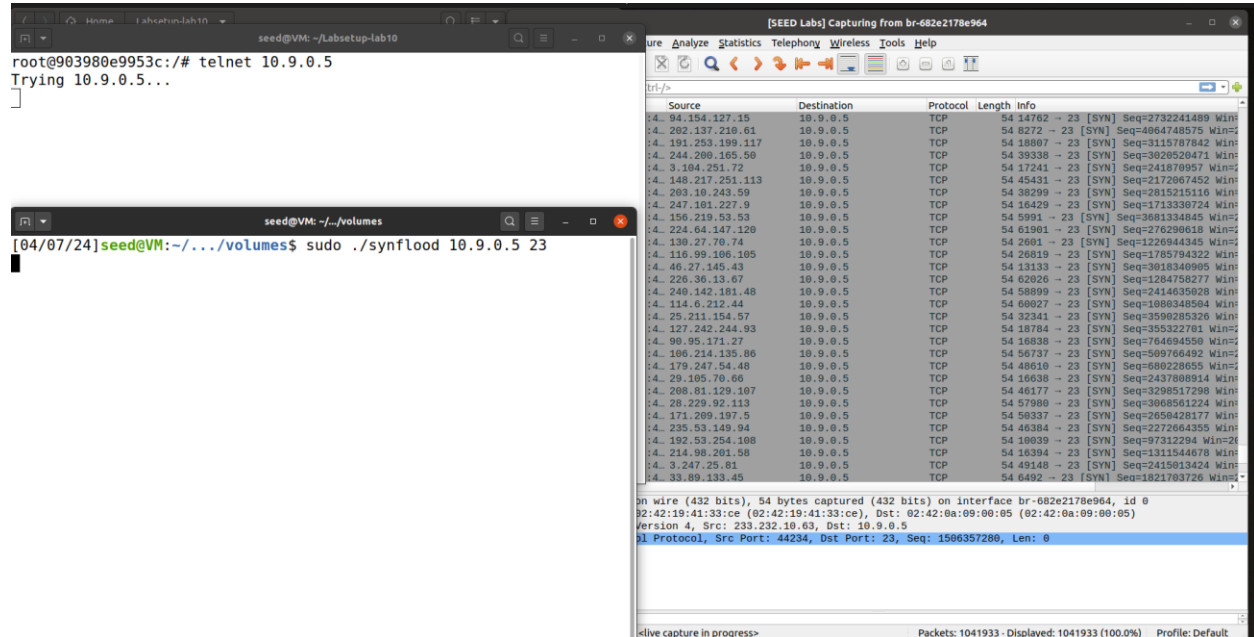
```

Wireshark packet capture details:

No.	Time	Source	Destination	Protocol	Length	Info
1	2024-04-07 17:11:02:42:0a:09:00:05	Broadcast	ARP	42	Who has 10.9.0.99?	
2	2024-04-07 17:11:02:42:0a:09:00:05	Broadcast	ARP	42	Who has 10.9.0.99?	
3	2024-04-07 17:11:02:42:0a:09:00:05	Broadcast	ARP	42	Who has 10.9.0.99?	
4	2024-04-07 17:11:02:42:0a:09:00:05	Broadcast	ARP	42	Who has 10.9.0.99?	
5	2024-04-07 17:11:02:42:0a:09:00:05	Broadcast	ARP	42	Who has 10.9.0.99?	
6	2024-04-07 17:11:02:42:0a:09:00:05	Broadcast	ARP	42	Who has 10.9.0.99?	

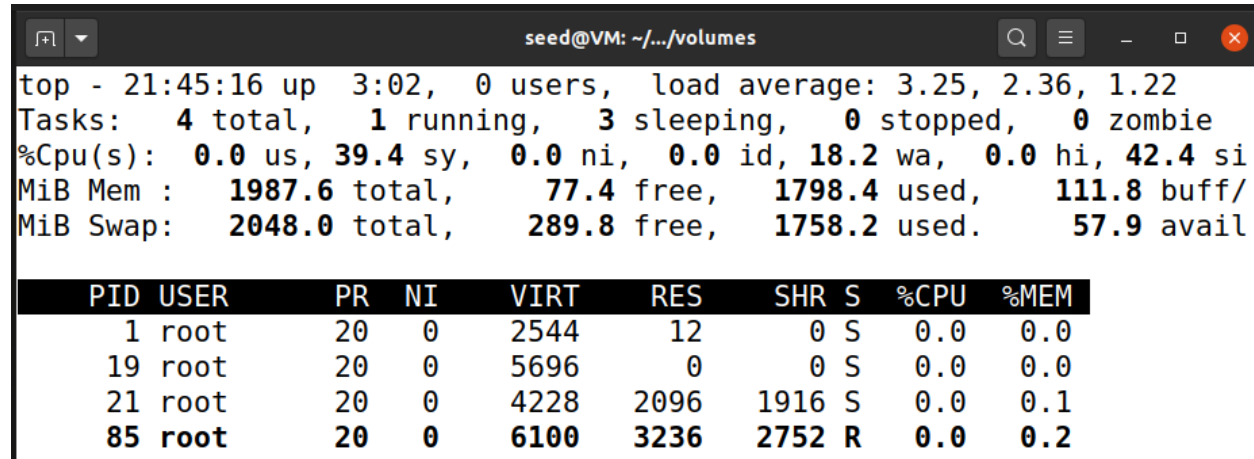
Q4. Explain what happens if you try to telnet from HostB to the victim's machine while the attack is running. Is the attack successful?

Yes the telnet command get hangs, this is because the victim is so overloaded with connections that we cannot connect to it:



- Q5. Does SYN flooding attack cause the victim server to freeze? (Hint: use top command and look at the CPU usage and memory usage in the table)

Yes, nearly all the memory is being used since initiation of the attack.



- Q6. Would any existing telnet session be affected by the SYN flood attack?

Existing Telnet sessions may not be directly affected by the SYN flooding attack. However, if the server becomes overwhelmed by the flood of SYN packets, it may impact the server's overall performance.

- Q7. Do you think you would be able to ssh to the victim machine while it's under attack?

Likely no, like the telnet, there are just too many connection and the machine is just too overwhelmed.