

Al-Najah National University
Department of Engineering and Information technology
Computer Network and Information Security

Packet Sniffing Spoofing

Mohammed Adnan
Sameh Sawan
Instructor: Dr. Ahmed Awad



6/3/2021

1 Photo

1. run tcpdump 1

```
mohammed@mohammed-VirtualBox:~/Desktop$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
10:28:02.993750 IP mohammed-VirtualBox.36838 > 93.184.220.29.http: Flags [..], ack 63041600, win 63920, length 0
10:28:02.994292 IP 93.184.220.29.http > mohammed-VirtualBox.36838: Flags [..], ack 1, win 65535, length 0
10:28:02.996097 IP mohammed-VirtualBox.35373 > superfast.domain: 5067+ [1au] PTR? 29.220.184.93.in-addr.arpa. (55)
10:28:03.076470 IP superfast.domain > mohammed-VirtualBox.35373: 5067 NXDomain 0/1/1 (126)
10:28:03.077055 IP mohammed-VirtualBox.35373 > superfast.domain: 5067+ PTR? 29.220.184.93.in-addr.arpa. (44)
10:28:03.080245 IP superfast.domain > mohammed-VirtualBox.35373: 5067 NXDomain 0/0/0 (44)
10:28:03.081437 IP mohammed-VirtualBox.32900 > superfast.domain: 51602+ [1au] PTR? 15.2.0.10.in-addr.arpa. (51)
10:28:03.084889 IP superfast.domain > mohammed-VirtualBox.32900: 51602 NXDomain 0/0/1 (51)
10:28:03.085115 IP mohammed-VirtualBox.32900 > superfast.domain: 51602+ PTR? 15.2.0.10.in-addr.arpa. (40)
10:28:03.089184 IP superfast.domain > mohammed-VirtualBox.32900: 51602 NXDomain 0/0/0 (40)
10:28:03.090243 IP mohammed-VirtualBox.41132 > superfast.domain: 1019+ [1au] PTR? 1.1.168.192.in-addr.arpa. (53)
10:28:03.093095 IP superfast.domain > mohammed-VirtualBox.41132: 1019* 1/0/1 PTR superfast. (76)
10:28:03.248536 IP mohammed-VirtualBox.60704 > ec2-44-238-41-205.us-west-2.compute.amazonaws.com.https: Flags [..], ack 62916008, win 63700, length 0
10:28:03.248961 IP ec2-44-238-41-205.us-west-2.compute.amazonaws.com.https > mohammed-VirtualBox.60704: Flags [..], ack 1, win 65535, length 0
10:28:03.249310 IP mohammed-VirtualBox.40716 > superfast.domain: 40786+ [1au] PTR? 205.41.238.44.in-addr.arpa. (55)
10:28:03.322707 IP superfast.domain > mohammed-VirtualBox.40716: 40786 1/0/1 PTR ec2-44-238-41-205.us-west-2.compute.amazonaws.com. (118)
^C
16 packets captured
16 packets received by filter
0 packets dropped by kernel
```

Figure 1

2. captuerd.log 2

```
Activities Text Editor Mar 8 10:31
Open captured.log ~/Desktop
1 tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
2 listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
3 10:28:02.993750 IP mohammed-VirtualBox.36838 > 93.184.220.29.http: Flags [..], ack 63041600, win 63920, length 0
4 10:28:02.994292 IP 93.184.220.29.http > mohammed-VirtualBox.36838: Flags [..], ack 1, win 65535, length 0
5 10:28:02.996097 IP mohammed-VirtualBox.35373 > superfast.domain: 5067+ [1au] PTR? 29.220.184.93.in-addr.arpa. (55)
6 10:28:03.076470 IP superfast.domain > mohammed-VirtualBox.35373: 5067 NXDomain 0/1/1 (126)
7 10:28:03.077055 IP mohammed-VirtualBox.35373 > superfast.domain: 5067+ PTR? 29.220.184.93.in-addr.arpa. (44)
8 10:28:03.080245 IP superfast.domain > mohammed-VirtualBox.35373: 5067 NXDomain 0/0/0 (44)
9 10:28:03.081437 IP mohammed-VirtualBox.32900 > superfast.domain: 51602+ [1au] PTR? 15.2.0.10.in-addr.arpa. (51)
10 10:28:03.084889 IP superfast.domain > mohammed-VirtualBox.32900: 51602 NXDomain 0/0/1 (51)
11 10:28:03.085115 IP mohammed-VirtualBox.32900 > superfast.domain: 51602+ PTR? 15.2.0.10.in-addr.arpa. (40)
12 10:28:03.089184 IP superfast.domain > mohammed-VirtualBox.32900: 51602 NXDomain 0/0/0 (40)
13 10:28:03.090243 IP mohammed-VirtualBox.41132 > superfast.domain: 1019+ [1au] PTR? 1.1.168.192.in-addr.arpa. (53)
14 10:28:03.093095 IP superfast.domain > mohammed-VirtualBox.41132: 1019* 1/0/1 PTR superfast. (76)
15 10:28:03.248536 IP mohammed-VirtualBox.60704 > ec2-44-238-41-205.us-west-2.compute.amazonaws.com.https: Flags [..], ack 62916008, win 63700, length 0
16 10:28:03.248961 IP ec2-44-238-41-205.us-west-2.compute.amazonaws.com.https > mohammed-VirtualBox.60704: Flags [..], ack 1, win 65535, length 0
17 10:28:03.249310 IP mohammed-VirtualBox.40716 > superfast.domain: 40786+ [1au] PTR? 205.41.238.44.in-addr.arpa. (55)
18 10:28:03.322707 IP superfast.domain > mohammed-VirtualBox.40716: 40786 1/0/1 PTR ec2-44-238-41-205.us-west-2.compute.amazonaws.com. (118)
19 ^C
20 16 packets captured
21 16 packets received by filter
22 0 packets dropped by kernel
```

Figure 2

3. compile getinterface [3](#)

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ gcc -o GetInterface GetInterface.c
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$
```

Figure 3

4. run Getinterface [4](#)

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ ./GetInterface enp0s3
Device: enp0s3
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$
```

Figure 4

5. compile sniffer [5](#)

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ sudo gcc Sniffer.c -L/path/to/libpcap -lpcap -o Sniffer
[sudo] password for mohammed:
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$
```

Figure 5

6. run sniffer [6](#)

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ sudo ./Sniffer
```

Figure 6

7. run sniffer after port 23 to 80 [7](#)

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ sudo ./Sniffer
Jacked a packet with length of [74]
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$
```

Figure 7

8. compile sniffex 8

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ sudo gcc sniffex.c -L/path/to/libpcap -lpcap -o sniffex
sniffex.c: In function 'main':
sniffex.c:529:3: warning: 'pcap_lookupdev' is deprecated: use 'pcap_findalldevs' and use the first device [-Wdeprecated-declarations]
  529 |     dev = pcap_lookupdev(errbuf);
      |           ^
In file included from /usr/include/pcap.h:43,
               from sniffex.c:199:
/usr/include/pcap/pcap.h:328:16: note: declared here
  328 | PCAP_API char *pcap_lookupdev(char *)
      |
```

Figure 8

9. run sniffex 9,10

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ sudo ./sniffex
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: enp0s3
Number of packets: 10
Filter expression: ip

Packet number 1:
    From: 10.0.2.15
    To: 34.217.242.117
    Protocol: TCP
    Src port: 37814
    Dst port: 443

Packet number 2:
    From: 34.217.242.117
    To: 10.0.2.15
    Protocol: TCP
    Src port: 443
    Dst port: 37814

Packet number 3:
    From: 10.0.2.15
    To: 192.168.1.1
    Protocol: UDP

Packet number 4:
    From: 192.168.1.1
    To: 10.0.2.15
    Protocol: UDP

Packet number 5:
    From: 10.0.2.15
    To: 192.168.1.1
    Protocol: UDP

Packet number 6:
    From: 192.168.1.1
    To: 10.0.2.15
    Protocol: UDP

Packet number 7:
    From: 10.0.2.15
    To: 192.168.1.1
```

Figure 9

```
Packet number 7:  
    From: 10.0.2.15  
    To: 192.168.1.1  
    Protocol: UDP  
  
Packet number 8:  
    From: 192.168.1.1  
    To: 10.0.2.15  
    Protocol: UDP  
  
Packet number 9:  
    From: 10.0.2.15  
    To: 192.168.1.1  
    Protocol: UDP  
  
Packet number 10:  
    From: 192.168.1.1  
    To: 10.0.2.15  
    Protocol: UDP  
  
Capture complete.
```

Figure 10

10. We try to connect a telnet connection between two virtual as figures 11,12 and 13 show , but login is incorrect .

```
char errbuf[PCAP_ERRBUF_SIZE];          /* error buffer */
pcap_t *handle;                          /* packet capture handle */

char filter_exp[] = "tcp port 23";      /* filter expression [3] */
struct bpf_program fp;                  /* compiled filter program (expression)
bpf_u_int32 mask;                       /* subnet mask */
```

Figure 11

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ telnet 10.0.2.15 23
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
Ubuntu 20.04.2 LTS
mohammed-VirtualBox login: mohammed-VirtualBox
Password:

Login incorrect
mohammed-VirtualBox login: █
```

Figure 12

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ sudo ./sniffex
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: enp0s3
Number of packets: 10
Filter expression: tcp port 23
```

Figure 13

11. create an ICMP echo [14](#)

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ sudo ./spoofer --payload='This is a bogus payload' --type=ping ** --src-ip=128.10.130.191
+-----+
| PURDUE Univ. CS528 - Network Security |
| Lab 1: Packet Sniffing and Spoofing   |
| Task 2: Spoof Ping packets and Ethernet frames |
+-----+
[+] Spoofed IP packet sent successfully!
```

Figure 14

12. create an ICMP echo (using tcpdump) [15](#)

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ sudo tcpdump
[sudo] password for mohammed:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
17:20:11.865060 IP 128.10.130.190 > 128.10.130.191: ICMP echo request, id 0, seq 0, length 31
17:20:11.866388 IP mohammed-VirtualBox.60622 > superfaster.domain: 21907+ [1au] PTR? 191.130.10.128.in-addr.arpa. (56)
```

Figure 15

13. Ethernet frame [16](#) , [17](#)

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ sudo tcpdump -vv
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
20:11:10.317793 IP (tos 0x0, ttl 64, id 9999, offset 0, flags [none], proto ICMP (1), length 40)
    128.10.130.190 > 128.10.130.191: ICMP echo request, id 0, seq 0, length 20
```

Figure 16

```
mohammed@mohammed-VirtualBox:~/Desktop/lab4/Exp4-Codes$ sudo ./spoofer --payload='march 8 2021' --type=all --src-mac=01:02:03:04:05:06 --dst-mac=99:99:99:99:99:99 --src-ip=128.10.130.190 --dst-ip=128.10.130.191
+-----+
| PURDUE Univ. CS528 - Network Security |
| Lab 1: Packet Sniffing and Spoofing   |
| Task 2: Spoof Ping packets and Ethernet frames |
+-----+
[+] Spoofed Ethernet frame sent successfully!
```

Figure 17