

به نام خدا

پروژه دوم درس شبکه

علیرضا میرحسینی

ft

محمد یاسین کرباسیان

(بخش یکم)

۱. حداقل طول بسته برای ارسال باید ۱۴ بایت باشد چون یک بسته ethernet نیاز به ۱۴ بایت برای header دارد که شامل ۶ بایت برای source mac address و ۶ بایت برای destination mac address و ۲ بایت برای type است.

۲. بسته به هر فرمتی باشد توسط وایرشارک شناسایی میشود.

۳.

The image shows a Wireshark capture of an Ethernet II frame on the wlp3s0 interface. The frame has a source MAC address of 12:34:56:78:90:12 and a destination MAC address of 22:22:22:22:22:22. The protocol is 0x0000, and the length is 14 bytes. The packet details show the frame structure: Frame 349: 14 bytes on wire (112 bits), 14 bytes captured (112 bits) on interface wlp3s0, id 0. Ethernet II, Src: 12:34:56:78:90:12 (12:34:56:78:90:12), Dst: 22:22:22:22:22:22 (22:22:22:22:22:22). Destination: 22:22:22:22:22:22 (22:22:22:22:22:22). Source: 12:34:56:78:90:12 (12:34:56:78:90:12). Type: Unknown (0x0000).

The terminal window shows the execution of the pkt_sender.py script. The user is prompted for the packet content and the interface to use. The script sends a 14-byte packet on the wlp3s0 interface.

```
yasir@Hunter:~/Desktop/coding training/Mini-WireShark$ sudo python3 pkt_sender.py
What is your packet content? 2222222222221234567890120000
Which interface do you want to use? wlp3s0
Send 14-byte packet on wlp3s0
yasir@Hunter:~/Desktop/coding training/Mini-WireShark$
```

.۴

tcp.port == 54870						
No.	Time	Source	Destination	Protocol	Length	Info
366	9.634165014	192.168.1.4	167.235.247.9	TCP	74	54870 → 15443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=...
374	9.768736115	167.235.247.9	192.168.1.4	TCP	54	15443 → 54870 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

PKT

Frame 366: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp3s0, id 0

Ethernet II, Src: LiteonTe_a5:99:34 (48:d2:24:a5:99:34), Dst: D-LinkIn_db:f3:08 (fc:75:16:db:f3:08)

- Destination: D-LinkIn_db:f3:08 (fc:75:16:db:f3:08)
- Source: LiteonTe_a5:99:34 (48:d2:24:a5:99:34)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.1.4, Dst: 167.235.247.9

Transmission Control Protocol, Src Port: 54870, Dst Port: 15443, Seq: 0, Len: 0

0000	fc 75 16 db f3 08 48 d2	24 a5 99 34 08 00 45 00	..u...H. \$.4..E.
0010	00 3c df c5 40 00 40 06	fa 54 c0 a8 01 04 a7 eb	...@.@.T.....
0020	f7 09 d6 56 3c 53 04 06	25 eb 00 00 00 00 a0 02	...V<S..%.....
0030	fa f0 8a 68 00 00 02 04	05 b4 04 02 08 0a 32 91	...h....2.....
0040	f2 d8 00 00 00 00 01 03	03 07

این حمله به این صورت است که هکر یک بسته را که بین دو عدد end system در حال رد و بدل است را دریافت می‌کند و همان بسته را دوباره ارسال می‌کند. با وجود اینکه بسته رمزگذاری شده است اما بسته فقط باز ارسال می‌شود و اطلاعات آن صحیح است. با استفاده از این برنامه اگر ما با نرم افزاری مثل وایرشارک بسته ای را دریافت کنیم می‌توانیم با pkt_sender.py همان بسته را دوباره ارسال کنیم.

بخش دوم)

۱. قسمت sequence number می‌تواند مقداری دیگر را داشته باشد.

۲.

Capturing from wlp3s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 93.184.216.34

No.	Time	Source	Destination	Protocol	Length	Info
17	5.675048924	192.168.1.5	93.184.216.34	TCP	54	3000 → 80 [SYN] Seq=0 Win=29200 Len=0
18	5.866208737	93.184.216.34	192.168.1.5	TCP	58	80 → 3000 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400
21	6.874504968	93.184.216.34	192.168.1.5	TCP	58	[TCP Retransmission] 80 → 3000 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400
28	8.889696845	93.184.216.34	192.168.1.5	TCP	58	[TCP Retransmission] 80 → 3000 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400

Frame 17: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface wlp3s0, id 0

Ethernet II, Src: LiteonTe_a5:99:34 (48:d2:24:a5:99:34), Dst: D-LinkIn_db:f3:08 (fc:75:16:db:f3:08)

Internet Protocol Version 4, Src: 192.168.1.5, Dst: 93.184.216.34

Transmission Control Protocol, Src Port: 3000, Dst Port: 80, Seq: 0, Len: 0

```

0000  fc 75 16 db f3 08 48 d2 24 a5 99 34 08 00 45 00  -u....H. $.4..E.
0010  00 28 07 c3 40 00 40 06 3b 85 c0 a8 01 05 5d b8  -[...@-@- ;.....]-
0020  d8 22 0b b8 00 50 17 49 30 d1 00 00 00 00 50 02  -"...P-I 0.....P-
0030  72 10 f2 27 00 00                                r...*...
  
```

Frame (frame), 54 bytes

Packets: 988 - Displayed: 4 (0.4%)

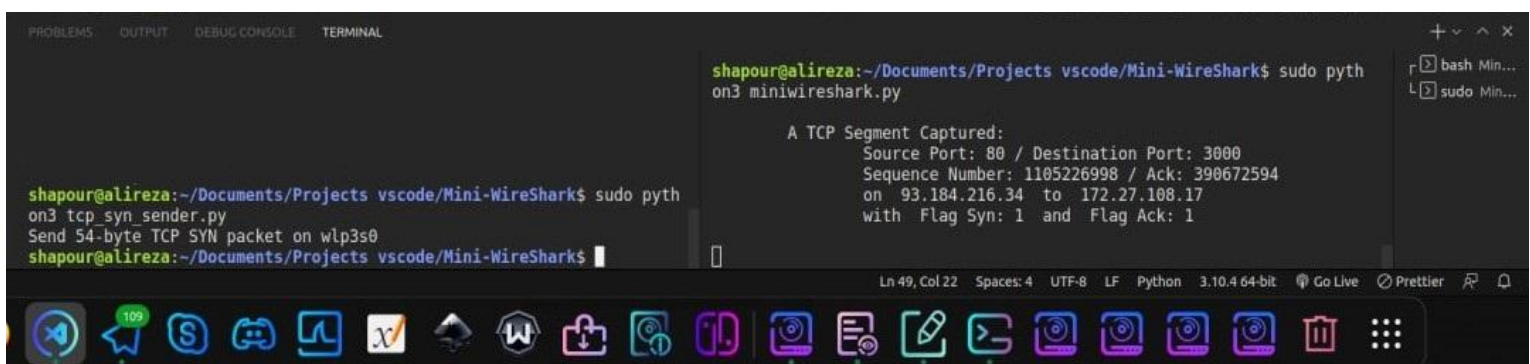
۳. خب بسته اول که از نوع TCP SYN, ACK است در جواب به TCP SYN ای که ما برای سرور ارسال کرده ایم. خب پس سرور از ما انتظار دارد که با دریافت این بسته برای او TCP ACK ارسال کنیم. اما چون برنامه ما فقط یک بسته TCP SYN ارسال می‌کند و متوقف می‌شود و کاری به بقیه بسته ها ندارد پس در جواب سرور چیزی ارسال نمی‌کند تا three-way-handshaking تکمیل بشود. پس مدتی سرور جوابی دریافت نمی‌کند و timeout می‌شود پس بسته را دوباره ارسال می‌کند(بسته دریافتی دوم) . سپس پس از مدتی دوباره timeout برای بسته دوم رخ می‌دهد و سرور بسته را دوباره ارسال میکند.

بخش سوم)

۱. با توجه به کدهای صورت پروژه طول هدر اترنت ۱۴ بایت - طول هدر IP برابر با ۲۰ بایت و طول هدر TCP در اصل ۲۰ بایت است ولی ما فقط با ۱۴ بایت آن کار داریم (آن مقداری که در کد ازش استفاده شده)

۲. با چک کردن flag_syn و flag_ack که مقدار این دو همزمان باید ۱ باشد.

۳.



```
shapour@alireza:~/Documents/Projects vscode/Mini-WireShark$ sudo python3 tcp_syn_sender.py
Send 54-byte TCP SYN packet on wlp3s0
shapour@alireza:~/Documents/Projects vscode/Mini-WireShark$
```

```
A TCP Segment Captured:
Source Port: 80 / Destination Port: 3000
Sequence Number: 1105226998 / Ack: 390672594
on 93.184.216.34 to 172.27.108.17
with Flag Syn: 1 and Flag Ack: 1
```

بخش چهارم (

۱.

```
yasin@Hunter:~/Desktop/coding training/Mini-WireShark$ sudo python3 mininmap_packet_sender.py
```

```
What is the target IP address? (default = 93.184.216.34) 176.101.52.70
Which ports do you want to scan? 0-2000
```

```
Send TCP SYN packet to port 0
Send TCP SYN packet to port 1
Send TCP SYN packet to port 2
Send TCP SYN packet to port 3
Send TCP SYN packet to port 4
Send TCP SYN packet to port 5
Send TCP SYN packet to port 6
Send TCP SYN packet to port 7
Send TCP SYN packet to port 8
Send TCP SYN packet to port 9
Send TCP SYN packet to port 10
Send TCP SYN packet to port 11
Send TCP SYN packet to port 12
Send TCP SYN packet to port 13
Send TCP SYN packet to port 14
Send TCP SYN packet to port 15
Send TCP SYN packet to port 16
Send TCP SYN packet to port 17
Send TCP SYN packet to port 18
Send TCP SYN packet to port 19
Send TCP SYN packet to port 20
```

```
Send TCP SYN packet to port 1973
Send TCP SYN packet to port 1974
Send TCP SYN packet to port 1975
Send TCP SYN packet to port 1976
Send TCP SYN packet to port 1977
Send TCP SYN packet to port 1978
Send TCP SYN packet to port 1979
Send TCP SYN packet to port 1980
Send TCP SYN packet to port 1981
Send TCP SYN packet to port 1982
Send TCP SYN packet to port 1983
Send TCP SYN packet to port 1984
Send TCP SYN packet to port 1985
Send TCP SYN packet to port 1986
Send TCP SYN packet to port 1987
Send TCP SYN packet to port 1988
Send TCP SYN packet to port 1989
Send TCP SYN packet to port 1990
Send TCP SYN packet to port 1991
Send TCP SYN packet to port 1992
Send TCP SYN packet to port 1993
Send TCP SYN packet to port 1994
Send TCP SYN packet to port 1995
Send TCP SYN packet to port 1996
Send TCP SYN packet to port 1997
Send TCP SYN packet to port 1998
Send TCP SYN packet to port 1999
Send TCP SYN packet to port 2000
```

```
yasin@Hunter:~/Desktop/coding training/Mini-WireShark$
```

```
yasin@Hunter:~/Desktop/coding training/Mini-WireShark$ sudo python3 mininmap_packet_capturer.py
```

پورت 80 که برای پروتکل HTTP می باشد و کار هایی مثل وب سایت و ...
و پورت 110 که مربوط به پروتکل POP3 هستش و برای ایمیل هستش پس
سرویس های وب و ایمیل ارائه می شود.