

به نام خدا

گفتگو نعمت بخش - پرتو سبزواری

2-pkt_sender

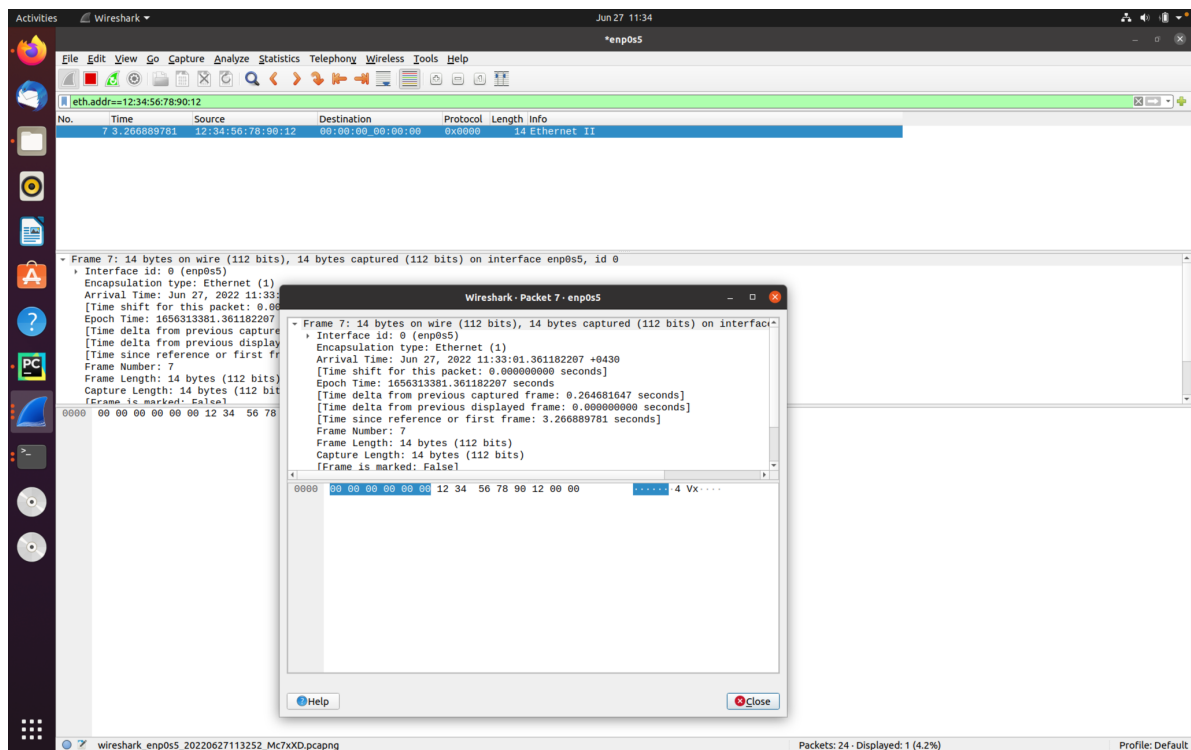
۱- حداقل طول بسته باید چند بایت باشد تا برنامه شما بتواند آن را ارسال کند؟ چرا؟

حداقل باید ۱۴ بایت باشد یعنی طول رشته هگزادسیمال باید ۲۸ بیت باشد که شامل ۶ بایت آدرس مک مبدا، ۶ بایت آدرس مک مقصد و ۲ بایت اترنت تاییپ.

۲- برای ارسال یک بسته اترنت که توسط وایرشارک شناسایی شود، بسته شما باید چه فرمتی داشته باشد؟

طول هدر ۱۴ بایت است که شامل ۶ بایت آدرس مک مبدا، ۶ بایت آدرس مک مقصد و ۲ بایت اترنت تاییپ است. سپس بخش payload است که حداقل ۴۶ و حداکثر ۱۵۰۰ بایت است و در نهایت بخش checksum می باشد که ۴ بایت است.

۳- برنامه خود را اجرا کنید و به نحوی به آن مقدار دهید که بسته مزبور را ارسال کند و در وایرشارک آن را دریافت کنید. تصویر ترمینال که در برگرفته ورودی و خروجی برنامه شما هست به همراه تصویر وایرشارک که بسته مزبور را دریافت کرده است را به عنوان جواب به این سوال در گزارش بیاورید.



۴- تصویر برنامه وایرشارک را به عنوان پاسخ به این سوال در گزارش خود بیاورید و مشخص کنید از بین بسته هایی که وایرشاک نشان میدهد کدام بسته، بسته تکراری است که برنامه شما ارسال کرده است.

No.	Time	Source	Destination	Protocol	Length	Info
25	16.288928573	10.211.55.3	34.107.221.82	TCP	74	60344 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
32	16.437781149	34.107.221.82	10.211.55.3	TCP	62	80 → 60344 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 WS...
33	16.437883432	10.211.55.3	34.107.221.82	TCP	54	60344 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
34	16.443992429	10.211.55.3	34.107.221.82	HTTP	355	GET /success.txt?ip=v4 HTTP/1.1
36	16.444309113	34.107.221.82	10.211.55.3	TCP	54	80 → 60344 [ACK] Seq=1 Ack=302 Win=32768 Len=0
41	16.595715458	34.107.221.82	10.211.55.3	HTTP	270	HTTP/1.1 200 OK (text/plain)
42	16.595734365	10.211.55.3	34.107.221.82	TCP	54	60344 → 80 [ACK] Seq=302 Ack=217 Win=64128 Len=0
264	18.652934650	10.211.55.3	34.107.221.82	TCP	54	60344 → 80 [FIN, ACK] Seq=302 Ack=217 Win=64128 Len=0
267	18.653074206	34.107.221.82	10.211.55.3	TCP	54	80 → 60344 [ACK] Seq=217 Ack=303 Win=32768 Len=0
282	18.811728297	34.107.221.82	10.211.55.3	TCP	54	80 → 60344 [FIN, ACK] Seq=217 Ack=303 Win=32768 Len=0
284	18.811767790	10.211.55.3	34.107.221.82	TCP	54	60344 → 80 [ACK] Seq=303 Ack=218 Win=64128 Len=0
289	78.089837110	10.211.55.3	34.107.221.82	TCP	54	[TCP Dup ACK 284#1] 60344 → 80 [ACK] Seq=303 Ack=218 Win=6412...
290	78.096039395	34.107.221.82	10.211.55.3	TCP	54	80 → 60344 [RST] Seq=218 Win=32768 Len=0

Frame 284: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface enp0s5, id 0
 Ethernet II, Src: Parallel_f9:6e:05 (00:1c:42:f9:6e:05), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)
 Internet Protocol Version 4, Src: 10.211.55.3, Dst: 34.107.221.82
 Transmission Control Protocol, Src Port: 60344, Dst Port: 80, Seq: 303, Ack: 218, Len: 0

بسته‌ی 284 را انتخاب کرده و توسط برنامه‌ی خود ارسال کردیم طبق عکس، 289 و 290 تکرار ارسال این بسته هستند.

۵- replay attack

این حمله بدین گونه صورت می‌گیرد که فرد حمله‌کننده داده‌های در حال انتقال را رهگیری می‌کند و به عنوان فرستنده اصلی بسته ها را برای مقصد می‌فرستد و گیرنده پیام آن را یک پیام تایید شده در نظر می‌گیرد و کلاینت پیام های خود را دوبار ارسال می‌کند

برای این کار می‌توان بسته های ارسالی را در وایرشارک capture کرده و می‌خوانیم و با جایگزین کردن ادرس‌های مقصد با ادرس‌های خود توسط برنامه pkt_sender باز ارسال می‌کنیم.

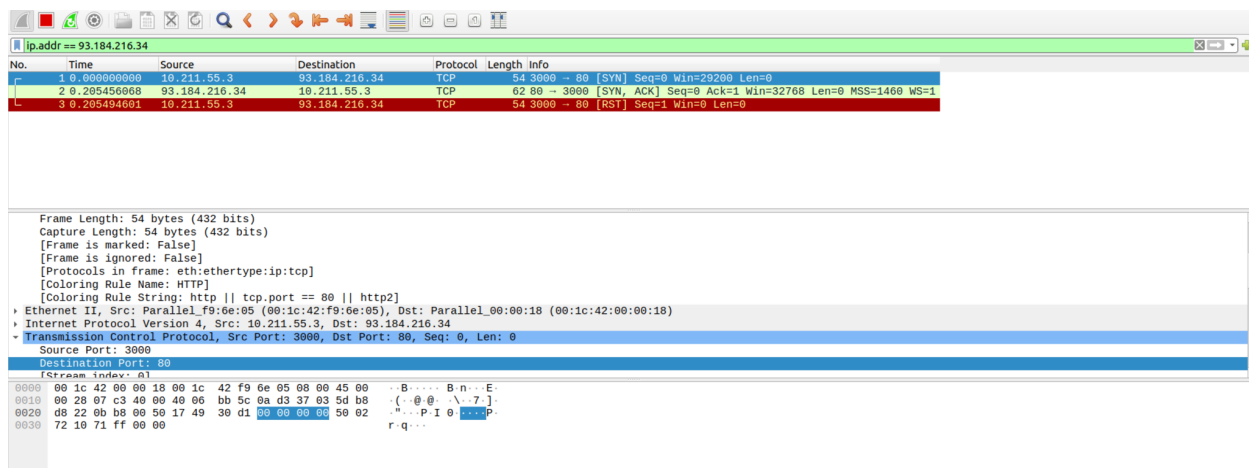
3-tcp-syn-sender

۱-از بین مقادیری که در شکل بالا برای فیلدهای مختلف بسته مقادردهی شده اند، کدامیک می توانند مقدار دلخواهی داشته باشند؟

در سگمنت tcp چون بیت های مربوط به urgent pointer و ack فعال نیستند پس مقادیر دلخواهی می‌توانند داشته باشند مقدار sequence number نیز می‌تواند در بسته‌ی syn دلخواه باشد.

در دیتاگرام ip نیز مقدار id که برای فرگمنتیشن بسته‌ها می‌باشد دلخواه است همچنین مقدار ttl از یک حداقلی که مانع گم شدن بسته ها بشود باید بیشتر باشد اما به جز این دلخواه است.

۲- برنامه خود را برای وبسایت `www.example.com` و پورت ۸۰ اجرا کنید. تصاویر وایرشارک با فیلتر `ip.addr == ip_addr` که در آن به جای `ip_addr` آدرس IP سایت `www.example.com` میبایست قرار بگیرد را به عنوان پاسخ به این قسمت قرار دهید.



۳- در سوال قبل اصولاً میبایست ۳ بسته به ازای یک ارسال بسته از دستگاه شما توسط وایرشارک نشان شده باشد. بسته اول همان بسته TCP SYN هست که دستگاه شما ارسال کرده است. دو بسته دیگر را تحلیل کنید (چه بسته هایی هستند و توسط چه برنامه ای ارسال شده اند؟

بسته ی TCP SYN که توسط `tcp_syn_sender` ارسال شده ، بسته ی SYN-ACK که توسط وبسایت ارسال می شود و پاسخ به بسته دریافتی SYN است و بسته ی RST که `tcp_syn_sender` ارسال می کند و نشان دهنده ی خاتمه دریافت و ارسال پیام است.

4-mini_wireshark

۱- با توجه به کدهای بالا، طول هدر اترنت چند بایت است؟ 14 بایت ($6 + 6 + 2 = 14$)

۲- با توجه به کدهای بالا، طول هدر آپی چند بایت است؟ 20 بایت ($1 + 1 + 2 + 2 + 2 + 1 + 1 + 2 + 4 + 4 + 2 + 2 = 20$)

۳- در برنامه `miniwireshark` چگونه باید مطمئن شد که بسته های دریافتی SYN-ACK هستند؟ با توجه به فلگ های هدر tcp اگر فلگ SYN و ACK یک بودند (010010) یعنی SYN-ACK است.

۴- برنامه خود را با کار کردن در مجاورت برنامه tcp_syn_sender.py را آزمایش کنید. نمونه ای از این همکاری بین این دو برنامه در شکل زیر نشان داده شده است.

```
Terminal: Local + -
(venv) golnoush@ubuntu:~/Desktop/NetworkProject$ sudo python3 miniwreshark.py
[sudo] password for golnoush:
80 is open on 93.184.216.34
[]

(venv) golnoush@ubuntu:~/Desktop/NetworkProject$ sudo python3 tcp_syn_sender.py
40
sent 54-bytes packets on enp0s5
(venv) golnoush@ubuntu:~/Desktop/NetworkProject$ []
```

5-mini_nmap

۱- با کدهایی که نوشته اید آزمایش کنید چه پورت‌هایی از آدرس 176.101.52.70 متعلق به دانشگاه صنعتی اصفهان در بازه ۰ تا ۲۰۰۰ باز هستند؟

```
Terminal: Local + -
(venv) golnoush@ubuntu:~/Desktop/NetworkProject$ sudo python3 miniwreshark.py
25 is open on 176.101.52.70
80 is open on 176.101.52.70
110 is open on 176.101.52.70
143 is open on 176.101.52.70
443 is open on 176.101.52.70
465 is open on 176.101.52.70
887 is open on 176.101.52.70

sent tcp syn packet to port 1984
sent tcp syn packet to port 1985
sent tcp syn packet to port 1986
sent tcp syn packet to port 1987
sent tcp syn packet to port 1988
sent tcp syn packet to port 1989
sent tcp syn packet to port 1990
sent tcp syn packet to port 1991
sent tcp syn packet to port 1992
sent tcp syn packet to port 1993
sent tcp syn packet to port 1994
sent tcp syn packet to port 1995
sent tcp syn packet to port 1996
sent tcp syn packet to port 1997
sent tcp syn packet to port 1998
sent tcp syn packet to port 1999
(venv) golnoush@ubuntu:~/Desktop/NetworkProject$ []
```

```
Terminal: Local + -
(venv) golnoush@ubuntu:~/Desktop/NetworkProject$ sudo python3 miniwreshark.py
25 is open on 176.101.52.70
80 is open on 176.101.52.70
110 is open on 176.101.52.70
143 is open on 176.101.52.70
995 is open on 176.101.52.70
993 is open on 176.101.52.70
[]

sent tcp syn packet to port 1983
sent tcp syn packet to port 1984
sent tcp syn packet to port 1985
sent tcp syn packet to port 1986
sent tcp syn packet to port 1987
sent tcp syn packet to port 1988
sent tcp syn packet to port 1989
sent tcp syn packet to port 1990
sent tcp syn packet to port 1991
sent tcp syn packet to port 1992
sent tcp syn packet to port 1993
sent tcp syn packet to port 1994
sent tcp syn packet to port 1995
sent tcp syn packet to port 1996
sent tcp syn packet to port 1997
sent tcp syn packet to port 1998
sent tcp syn packet to port 1999
(venv) golnoush@ubuntu:~/Desktop/NetworkProject$ []
```

۲- با توجه به قسمت قبل چه سرویس های شناخته شده ای بر روی این آدرس دانشگاه ارائه می شود؟

پورت 443 و 80 : HTTPS و HTTP (وب)

پورت 25 و 587 و 465 : SMTP (ایمیل)

پورت 110 و 995 : POP3 (ایمیل)

پورت 143 و 993 : IMAP (ایمیل)