به نام یکتا سازنده هستی

پروژه دوم شبکه های کامپیوتری

شبکه های کامپیوتری

دانشگاه صنعتی اصفهان

خرداد ماه ۱۴۰۱

استاد درس:

دکتر محمدرضا حیدرپور

انجام دهندگان پروژه:

مصطفی دریس پور - احمد مردانی

۹۹۰۰۲۸۳ - ۹۹۳۰۵۷۳

۲ – راسال هر بسته دلخواه

۱) ۱۴ بایت زیرا حداقل طول هدر ethernet این مقدار است.

۲) فرمت بسته باید به صورت روبرو باشد: dest mac, src mac, length/type

۳)

```
mostafa@mostafa-IdeaPad-L3-15IML05:~/src/Term 4/Computer Network/Project2/code$ sudo python3 pkt_sender.py
What is your packet content? 123456789012342eb7bce8320800
Which interface do you want to use? wlp0s20f3
Sent 14-byte on wlp0s20f3
```

eth.addr == 12:34:56:78:90:12

No.	Time	Source	Destination	Protocol	Length	Info
11…	521.4777…	IntelCor_bc:e8…	12:34:56:78:90…	IPv4	14	[Malformed Packet]

۴) بسته پایین کپی شد

eth.addr == 12:34:56:78:90:12

No.	Time	Source	Destination	Protocol	Length	Info
11…	521.4777…	IntelCor_bc:e8…	12:34:56:78:90…	IPv4	14	[Malformed Packet]

بسته پایین مجددا ارسال شد

428	17.44507…	fe80::ca3a:35f…	fe80::f61a:f05…	ICMP…	142	Destination Unreachable (no route to destinat…
23…	192.4613…	fe80::f61a:f05…	2600:1901:0:38…	TCP	94	[TCP Retransmission] 58880 → 80 [SYN] Seq=0 W…

خروجی اجرای دستور:

```
mostafa@mostafa-IdeaPad-L3-15IML05:~/src/Term 4/Computer Network/Project2/code$ sudo python3 pkt_sender.py
What is your packet content? c83a3520b678342eb7bce83286dd6005da0300280640fe80000000000000f61a0f05f3d4ff0326001901000038d70000000000000000e60000
5085943d9300000000a002fd206e800000020405a00402080a8e9275b80000000001030307
Which interface do you want to use? wlp0s20f3
Sent 94-byte on wlp0s20f3
```

۵) حمله replay attack زمانی اتفاق می‌افتد که یک مجرم سایبری یک ارتباط شبکه امن را شنود می‌کند، آن را رهگیری می‌کند، و سپس با فریبکاری آن را به تأخیر می‌اندازد یا دوباره ارسال می‌کند تا گیرنده را به اشتباه هدایت کند تا آنچه را که هکر می‌خواهد انجام دهد.

معرفی ضمن یک مثال:

یکی از کارکنان یک شرکت با ارسال یک پیام رمزگذاری شده به مدیر مالی شرکت درخواست انتقال مالی می کند. یک مهاجم این پیام را شنود می‌کند و آن را ذخیره می کند و اکنون در موقعیتی است که می تواند آن را دوباره ارسال کند. از آنجا که این یک پیام معتبر است که به سادگی دوباره ارسال شده است، پیام قبلاً به درستی رمزگذاری شده است و برای مدیر مالی قانونی به نظر می رسد.

می‌توان از برنامه packet sender برای ارسال پکت های که توسط مهاجم ارسال می‌شوند و قانونی به نظر می‌رسند استفاده کرد زیرا این برنامه می‌تواند هر پکت دلخواهی را بفرستد.

۳ – ارسال بسته های TCP SYN

۱)

dest_ip می‌تواند مقدار دلخواهی باشد و بستگی دارد که به کجا بخواهیم بسته بفرستیم.

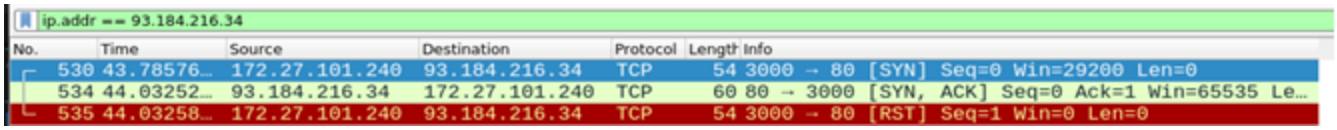
dest_port می‌تواند مقدار عددی پورتی باشد که در سرور باز است مثلاً اگر وب باشد ۸۰.

Flag نیز می‌تواند بسته به اینکه چه نوع بسته tcp می‌خواهیم بفرستیم مقادیر متفاوتی داشته باشد.

ttl نیز می‌تواند مقدار متفاوتی داشته باشد.

فیلد seq_num نیز می‌تواند مقدار دلخواهی داشته باشد.

۲)



۳) بسته دوم بسته ack ای هست که در پاسخ به بسته syn که توسط برنامه tcp_sender.py ارسال شده از سرور دریافت می‌شود.

پس از دریافت بسته دوم سیستم عامل که هیچ ایده ای ندارد که چرا این بسته دریافت شده است.

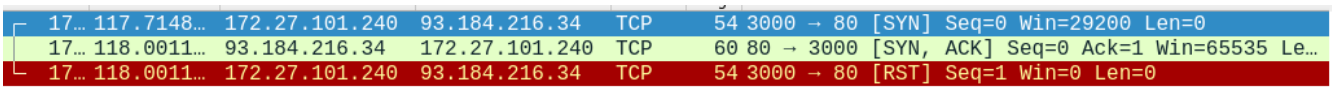
و خود او این hanshake را شروع نکرده است اتصال را ریست می‌کند.

منبع پاسخ اول در این فروم:

https://stackoverflow.com/questions/59612288/client-sends-rst-after-receive-syn-ack

راه حل در فروم زیر:

https://stackoverflow.com/questions/9058052/unwanted-rst-tcp-packet-with-scapy



٤) فایل ifinfo.sh به همراه سایر فایل‌ها در پروژه ضمیمه شده است.

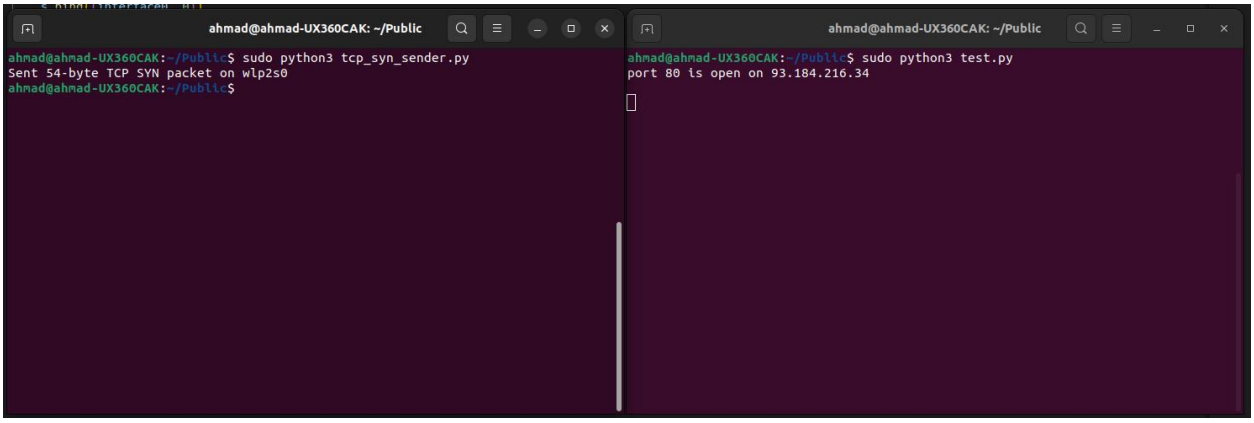
٤ - مینی وایرشارک

١) ١۴ بایت

٢) مینیمم ٢٠ بایت و ماکسیمم ۶٠ بایت

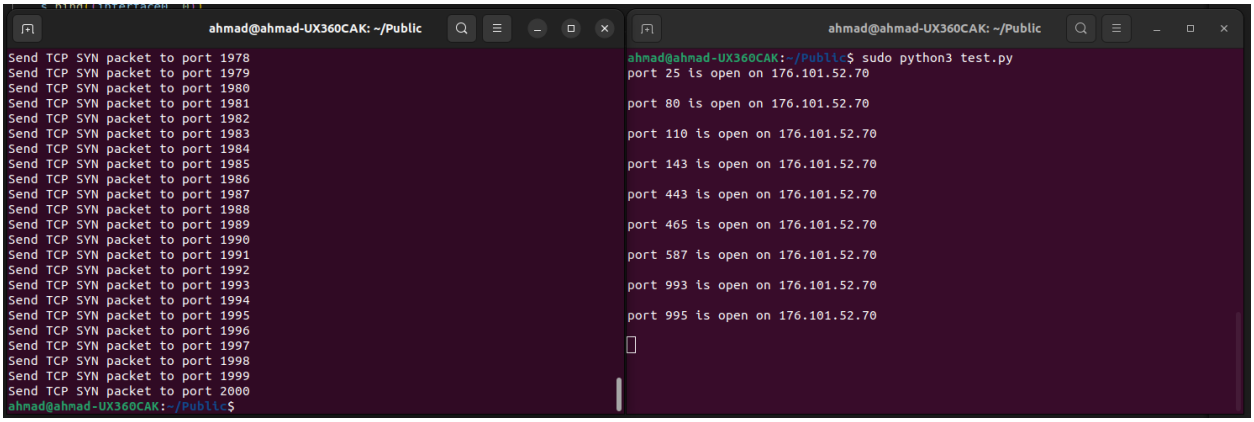
٣) با چک کردن فلگ های SYN و ACK

٤)



٥ – مینی-اِنمپ

١)



٢) پورت ٢۵ برای SMTP relaying

پورت ٨٠ برای http

پورت ۱۱۰ برای unencrypted access to electronic mail

پورت ۱۴۳ برای Internet Message Access Protocol

پورت ۴۴۳ برای (either https or http) to divert network traffic

پورت ۴۶۵ برای implicit TLS

پورت ۵۸۷ برای encrypt SMTP messages using STARTTLS

پورت ۹۹۳ برای IMAP over SSL/TLS (IMAPS)

پورت ۹۹۵ برای SSL-encrypted POP3 service for encrypted mail transfer

۳) به علت اینکه با سوکت tcp این کار را انجام میدهیم سرعت به شدت پایین تر میباشد.