به نام خدا

گلنوش نعمت‌بخش - پرتو سبزواری

2-pkt_sender

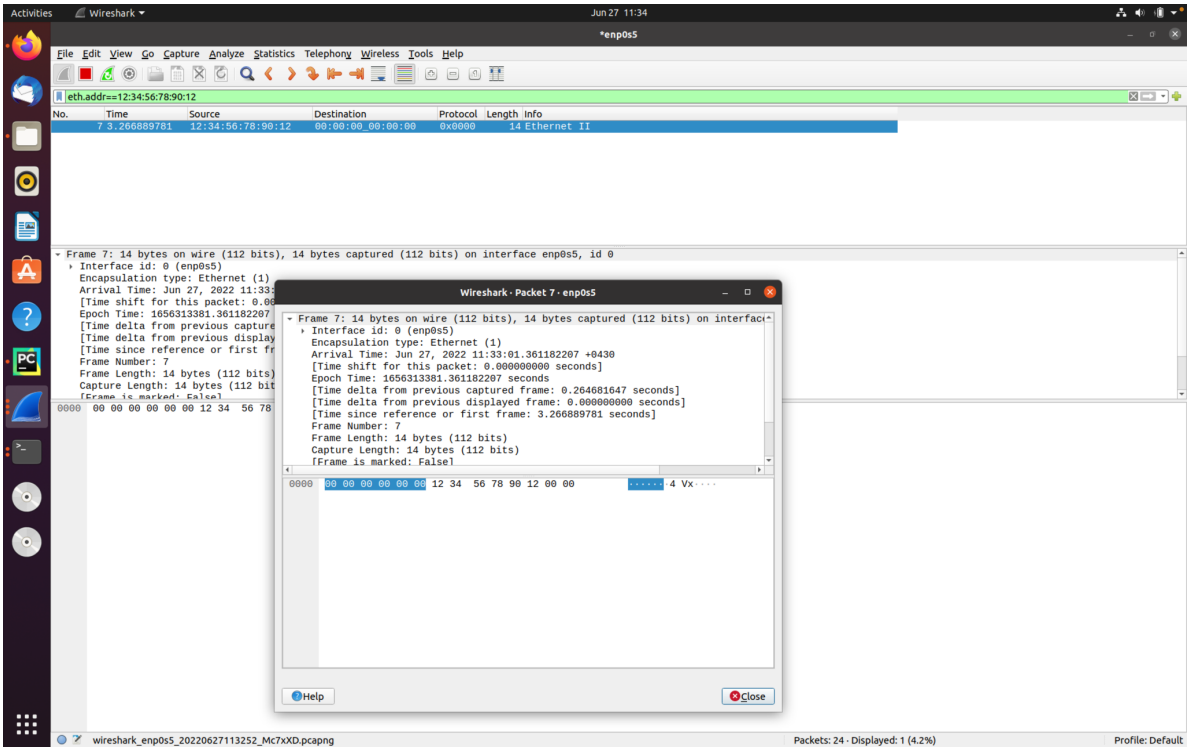
۱-حداقل طول بسته باید چند بایت باشد تا برنامه شما بتواند آن را ارسال کند؟ چرا؟

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 اترنت‌تایپ.

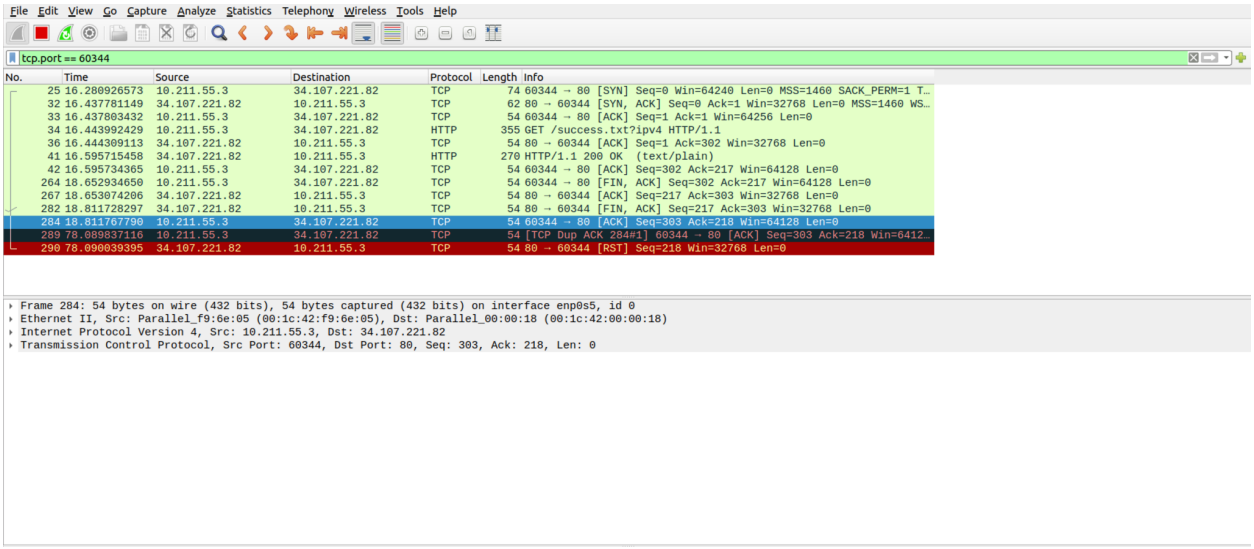
۲-برای ارسال یک بسته اترنت که توسط وایرشارک شناسایی شود، بسته شما باید چه فرمتی داشته باشد؟

طول هدر ۱۴ بایت است که شامل ۶ بایت آدرس مک مبدا، ۶ بایت آدرس مک مقصد و ۲ بایت اترنت تایپ است. سپس بخش payload است که حداقل ۴۶ و حداکثر ۱۵۰۰ بایت است و در نهایت بخش checksum می‌باشد 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 وایرشاک آن را دریافت کنید. تصویر ترمینال که در برگیرنده ورودی و خروجی برنامه شما هست به همراه تصویر وایرشاک 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.



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.

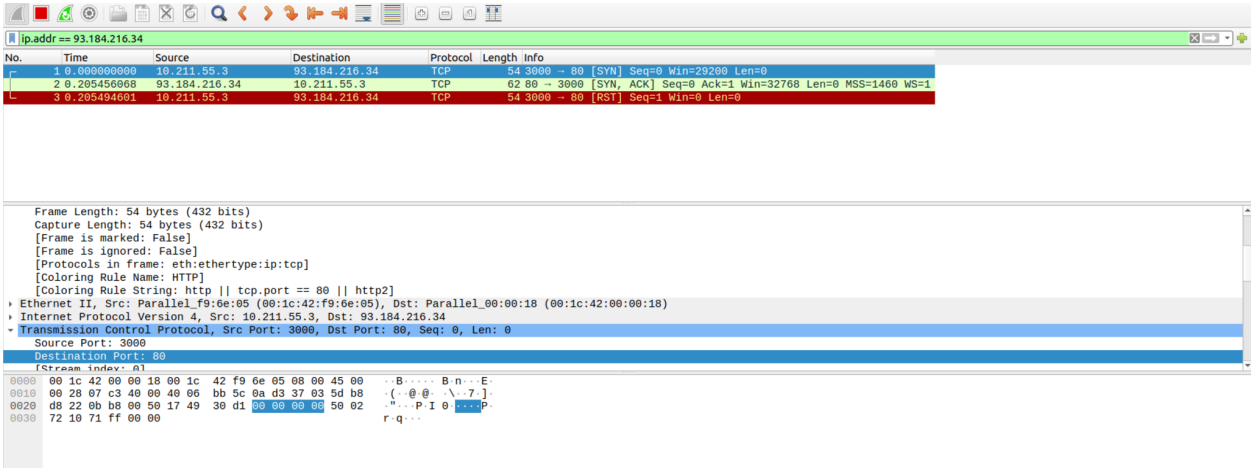
3-tcp-syn-sender

۱-از بین مقادیری که در شکل بالا برای فیلدهای مختلف بسته مقداردهی 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 میابست قرار بگیرد را به عنوان پاسخ به این قسمت قرار دهید.



۳-در سوال قبل اصولا 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؟

بسته‌ی tcp SYN که توسط tcp_syn_sender ارسال شده ، بسته‌ی SYN-ACK که توسط وبسایت ارسال می شود و پاسخ به بسته دریافتی SYN است و بسته‌ی RST که tcp_syn_sender ارسال می کند و نشان دهنده‌ی خاتمه دریافت و ارسال پیام است.

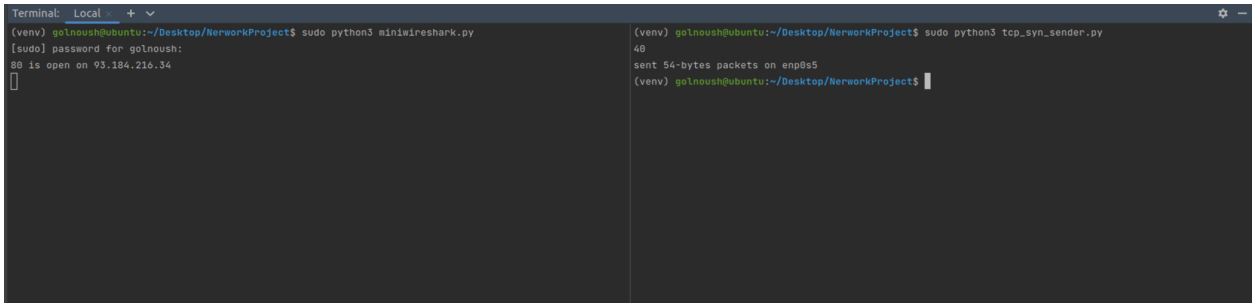
4-mini_wireshark

۱- با توجه به کدهای بالا، طول هدر اترنت چند بایت است؟ 14 بایت (6s6s2s = ۲+۶+۶)

۲-با توجه به کدهای بالا، طول هدر آیپی چند بایت است؟ 20 بایت(BSH2s2sBB2s4s4s = ۴+۴+۲+۱+۱+۲+۲+۲+۱+۱)

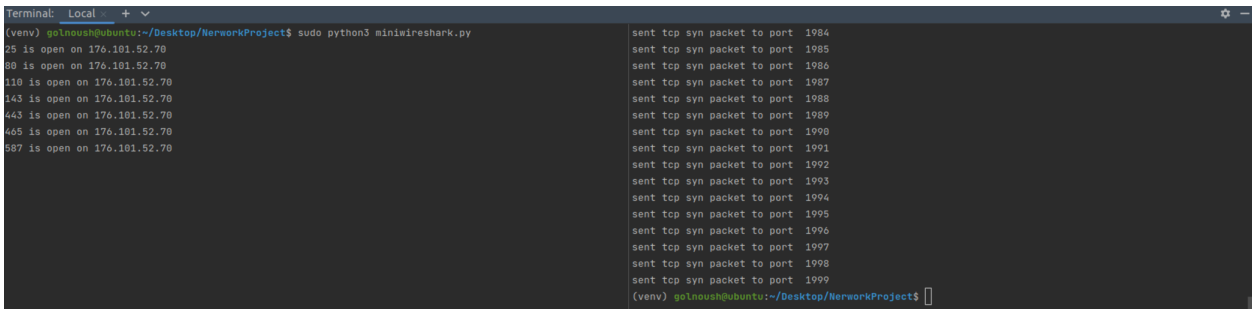
۳- در برنامه miniwireshark چگونه باید مطمئن شد که بسته های دریافتی SYN-ACK هستند؟ با توجه به فلگ های هدر tcp اگر فلگ SYN و ACK یک بودند (010010) یعنی SYN-ACK است.

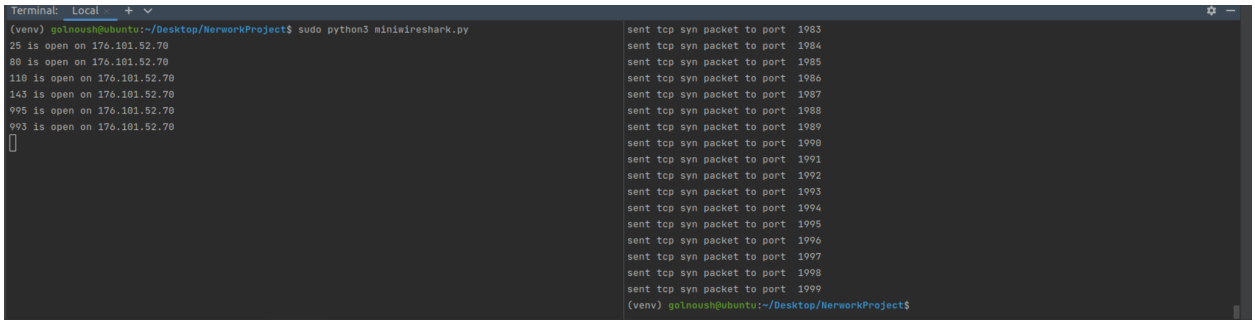
۴-برنامه خود را با کار کردن در مجاورت برنامه tcp_syn_sender.py را آزمایش کنید. نمونه ای از این همکاری بین این دو برنامه در شکل زیر نشان داده شده است.



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؟





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

پورت 443 و HTTPS : 80 و HTTP (وب)

پورت 25 و 587 و SMTP : 465 (ایمیل)

پورت 110 و POP3 : 995 (ایمیل)

پورت 143 و IMAP : 993 (ایمیل)