بهاران بصیری ۴۰۰۱۳۰۰۹۳

۱- در ابتدا نگاه میکنیم که در این فایل چه پروتکل هایی داریم.داریم: TCP، IPv4، UDP، ICMP، DNS

سپس برای پروتکل TCP بررسی میکنیم و در قسمت transmission control protocol میبینیم که stream index ما تا کجا ادامه دارد. (تا۲۹ )

بعد از قسمت فیلتر و دستور tcp.stream eq ? که در آن به جای ؟ مقادیر مختلف ایندکس قرار میگیرند استفاده میکنیم تا پروتکل ها مثلا TCPTرا دسته بندی کنیم و با کلیک راست و انتخاب گزینه فالو ببینیم که ایا فلگ در انجا وجود دارد یا خیر. به طور مشابه میتوان میتوان مثلا اینکار را برای UDP نیز انجام داد. یا مشابه کاری که من در اینجا کردم( به دلیل جواب ندادن راه دسته بندی) ، می توان همه را دانه به دانه چک کرد.(با کلیک راست و انتخاب گزینه فالو) : در نهایت میبینیم که در پروتکل DNS با No =81 یک فلگ وجود دارد: Flag{SZL0S8G}

۲- در این فایل ما ۱۱۳ تا پکت داریم. که همانطورکه عنوان شد، 5 نوع پروتکل در ان دیده می شود. که با روش سرچ پروتکل، اگر مثلا به عنوان فیلتر TCP را بزنیم که فقط پروتکل TCP را به ما بدهد. و اگر خودمان ویو سورس پورت را به پروفایل اضافه کنیم متوجه میشویم که ۳۰ تا پکت با این پروتکل وجود دارد که سورس پورت همگی برابر با ۲۰ است و قسمت اینفو همگی‌شان با هم برابر است. به طور مشابه میتوانیم از نظر بقیه پروتکل ها نیز بررسی را ادامه دهیم.

همچنین با اعمال فیلتر frame.time_relative < 0، فقط ان پکت هایی که زمان منفی دارند به ما نمایش داده میشود. (که از همه پروتکل های موجود در فایل هستند البته به جز دی ان اس). همچنین لازم به ذکر است زمان منفی نسبت به یک زمان مرجع به دست می آیند(مثلا زمان شروع ضبط)و اشاره به پکتی دارد که قبل از زمان مرجع رخ داده است. و به طور مشابه اگر برای زمان مثبت نیز فیلتر اعمال کنیم، داریم:

یک پکت با پروتکل TCP و یک پکت UDP ، و یک ICMP و چهارتا پکت با پروتکل IPV4 و یکی با پروتکل DNS . سرجمع ۷ تا. بنابراین در میابیم که اغلب پکت های ما دارای زمان منفی بوده یعنی قبل از زمان مرجع رخ داده اند.

همچنین ما بر اساس ادرس ایپی منبع و مقصد نیز میتوانیم جستجو را انجام دهیم، طبق دستور .. ip.address== .

همچنین با استفاده از علائم && یا || بین دستورهایی برای فیلترها، میتوانیم به صورت ترکیبی عمل کنیم و شرط " و " یا " یا " را اعمال کنیم.

همچنین با جستجو بر اساس طول (length) نیز میبینیم که بیشترین طول مربوط به پکت های IPv4 است .