Flag.1 رابیابید. در چه پکتی بود؟ پروسه یافتن آن را شرح دهید.

پس از واردشدن به اپلیکیشن وایرشارک و باز کردن فایل PCAP مورد نظر دیدیم که پکت های مختلفی با پروتکل های مختلف وجود دارد که ممکن است داخل هرپروتکلی باشد پس ازبررسی که کردم که اولین حدسی که زدم پروتکل TCP بود پس Stream های اونو بررسی کردم و دیدم که 21 استریم وجود دارد . سپس شروع کردم با دستور TCP.Stream eq0 بررسی و جستجو کردم و هربار یک عدد به صفر اضافه کردم تا عدد 21 که Flag موردنظر را داخل Flag 12 پیدا کردم پس دیگه بقیه پروتکل هارو بررسی نکردم چون گفته شده بود فقط یک فلگ وجود دارد البته که اگر نبود هم باید همین روند رو برای بقیه پروتکل ها اجرا میکردیم تا به Flag مورد نظر برسیم در نتیجه مراحل به یک صورت است .

Flag= {jGRG702}

IN Packet TCP ,Stream 12

2.فایل ترافیک ارائه شده را بااستفاده از فیلترهای مختلف تحلیل کنید و تاحد امکان ، جزئیات مختلف در موردش بیان کنید.

یکی از ابزار های تحلیل شبکه وایرشارک است.

فیلتر های مختلفی وجود دارد که میتوانیم بکارگیریم مثلا در اینجا ما 106 پکت و 4 نوع پروتکل داشتیم

که میتونستیم با سرچ کردن اسم پروتکل موردنظرمون بهش برسیم. همینطور برای پیدا کردن آی پی مورد نظرمون با دستور IP addr=... و در مقابلش آی پی دلخواهمان را قرار دهیم .

همچنین دستورات AND و OR وجود داشت که بااستفاده ازآنها نیز میتوانسیم به مورد دلخواهمون برسیم

همانند دستوربالا ولی برای AND از && و برای OR از || استفاده میشود.

شماره پورت مورد نظر==Port.اسم پروتکل ، بااین دستور نیز میتوان تمام بسته هایی که به پورت مورد نظر ارسال شده را مشاهده کرد.

و در نهایت باید نتایج تحلیل خود را گزارش دهیم که میتواند درباره فیلتر های مورد استفاده ،تاثیرات آنها برشبکه ،پیشنهاد برای امنیت یا بهبود شبکه و ... باشد.