کیدا همزه فایی ۴۰۰۱۳۰۱۴۳

Subject: تمرین ۴ Year: Month: Day:

۱- با استفاده از فیلتر tcp.stream== .... نتوانستم به flag برسم و با دستور follow هم نشد پس همه پکت ها را یک به یک گشتم و در پکت ۱۲۴ پروتکل ICMP به flag رسیدم.

۲- فیلترهای متفاوتی را می‌شود امتحان کرد اول از همه این فایل ۱۹۱ پکت داشت و ۵۱ stream داشت. با روش سرچ protocol مورد نظر مثل tcp یا http یا ICMP و... می‌شود به پروتکل مورد نظر رسید. یا برای پیدا کردن ip خاصی که می‌خواهیم می‌توانیم ip.addr== .... را وارد کردن این عبارت و دادن آی‌پی دلخواه مثل در این فایل ip.addr==193.105.191.196 آی‌پی‌های مرتبط را نمایش می‌دهد، یا می‌توانیم ترکیبی عمل کنیم و از && یا || استفاده کرد و هر چیزی که مد نظرمان است را and یا or کرد. مثل ip.add==... || ... و ... با پورت‌های ۱۹۱ معمول برای پروتکل SNMP که برای مدیریت و نظارت بر دستگاه‌های شبکه است استفاده می‌شود. نمایش تمام بسته‌ها 80 که به پورت tcp.port==80 tcp ارسال شده‌اند.

Subject: Year: Month: Day:

با فیلتر frame.time_relative می‌شود به زمان دسترسی داشت. مثلاً اگر

frame.time_relative == 0 را بزنیم در این قابل به کلیت های دسترسی پیدا می‌کنیم

که time آن‌ها برابر صفر است.