تمرین چهارم – سوده زارعی – ۴۰۱۱۳۰۳۹۳

سوال ۱) یافتن Flag.

۱. ابتدا پروتکل‌هایی که داریم را چک می‌کنیم و حدس میزنیم که به احتمال زیاد flag باید در TCP باشد پس در قسمت فیلتر tcp را وارد می‌کنیم.
۲. برای دسته‌بندی کردن tcp ها، تو قسمت فیلتر دستور tcp.stream == 0 را می‌نویسیم.
۳. در بین tcp های فیلتر شده، تک تک از قسمت tcp stream چک می‌کنیم تا فلگ را بیابیم. (تو قسمت packet display هم فلگ را می‌توانیم پیدا کنیم.)
۴. اگه فلگ در بین آنها نبود، عدد داخل فیلتر را افزایش می‌دهیم و همین روند را ادامه می‌دهیم. (tcp.stream == i)

فلگ در پکت شماره ۵ قرار دارد. Flag{COE1GM9}

سوال ۲) تحلیل فایل داده شده.

در این فایل پروتکل‌های پکت‌ها، ICMP ، IPV4 ، UDP و TCP هستند.

در پکت‌هایی که پروتکل ICMP را دارند شاهد ارورهایی هستیم که نشان می‌دهند در هنگام برقرار کردن پینگ، بازخوردی دریافت نکرده است و این به معنای عدم دسترسی به دستگاه مقصد می‌باشد.

تعدادی بسته در ساختار نادرست (malformed packet) ارسال شده‌اند که می‌توان در ترافیک این را مشاهده کرد.

اگر فیلتر tcp.port == 80 را اعمال کنیم می‌توانیم مشاهده کنیم که بسته‌های زیادی با طول 0 از پورت ۲۰ به پورت ۸۰ ارسال شده‌اند. پورت ۸۰ به طور معمول برای HTTP استفاده می‌شود.

اگر فیلتر udp را اعمال کنیم می‌توانیم مشاهده کنیم که تمامی بسته‌های udp از پورت ۵۳ برای مبدا و مقصد استفاده کرده‌اند که این پورت معمولا برای DNS به کار می‌رود.

به طور کلی به نظر می‌رسد که ترافیکی در شبکه در حال ارسال و دریافت داده‌ها و درخواست‌ها بین انواع مختلفی از دستگاه‌ها در شبکه است.