آشنایی با نرم‌افزار Wireshark

سوال ۱: به یک بخش دلخواه از بسته‌های شنودشده مراجعه کنید. چه پروتکل‌هایی را مشاهده می‌کنید. لیست آن‌ها را یادداشت کنید.

TCP, HTTP/XML, UDP

سوال ۲:یک بسته را به‌دلخواه انتخاب کنید. مشخص کنید که چه پروتکل‌هایی در لایه‌های مختلف آن استفاده شده است.

Ethernet, IPV4, TCP

ترتیب قرارگیری بیت‌ها داخل بسته چه ارتباطی با لایه‌های مختلف دارد؟

پروتکل‌های لایه‌های اول مانند Ethernet از لایه Data Link و IPV4 از لایه Internet اول قرار می‌گیرند.

اندازه فریم لایه دو این بسته چقدر است؟

لایه دوم = IPV4، اندازه = ۲۹۰ بایت

اندازه بسته لایه ۳ چقدر است؟

لایه سوم = TCP، اندازه = ۲۵۰ بایت

سوال ۳: آیا می‌توانید بسته‌هایی را پیدا کنید که بدون پروتکل‌های Network, Transport و Application باشند؟ این بسته‌ها از چه پروتکلی استفاده کرده‌اند؟

بله، به عنوان مثال از پروتکل Ethernet از لایه Data Link

سوال ۴: از یکی از بسته‌ها بخش مربوط به پروتکل Internet Protocol (IP) را پیدا کنید. Checksum پروتکل IP را پیدا کنید و آن را یادداشت کنید.

Checksum = 0x9942

سوال ۵: از یکی از بسته‌ها بخش مربوط به پروتکل Transport Control Protocol (TCP) و یا User Datagram Protocol (UDP) را پیدا کنید. عدد مربوط به Port مبدأ و مقصد را یادداشت کنید. به نظر شما این اعداد در مبدأ و مقصد چه چیزی را مشخص می‌کند؟ Checksum مربوط به پروتکل‌های TCP و UDP را مشخص کنید.

مبدأ = 61175 که این Port برای پروتکل‌های TCP/UDP است.

مبدأ = 443 که این Port برای پروتکل HTTPS است.

Checksum = 0x1b14

سوال۶: یکی از بسته‌ها که از سیستم شما ارسال شده است را انتخاب کنید. پروتکل لایه Transport چیست؟ آدرس IP مقصد چیست؟ سرایند لایه دوم را انتخاب کنید. آدرس مبدأ و مقصد را یادداشت کنید.

پروتکل لایه Transport = TCP

آدرس IP مقصد = 192.168.1.1(Router's IP)

سرایند لایه دوم:

آدرس IP مبدأ = 192.168.1.6

آدرس IP مقصد = 192.168.1.1

سوال ۷: کدام‌یک از آدرس‌های پیدا کرده در بخش قبل را می‌توانید در خروجی دستور ipconfig /all مشاهده کنید؟

آدرس IP مبدأ (192.168.1.6) قابل مشاهده است که آدرس محلی کامپیوتری است که درخواست را ارسال کرده است.

سوال ۸: یک بسته مربوط به دستور Ping را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه Typeای انتخاب شده‌است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده‌است؟

Type = A

این درخواست برای انطباق آدرس و hostname است.

سوال ۹: یک بسته مربوط به دستور nslookup را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه Typeای انتخاب شده‌است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده‌است؟

Type = PTR (domain name PoinTeR)

این درخواست برای گرفتن hostname از طریق آدرس ورودی است.

سوال ۱۰: به نظر شما چه typeهای دیگری ممکن است وجود داشته‌باشد؟ سه مورد را یادداشت کنید.

- IP version 6 record (AAAA record)
- Canonical Name record (CNAME record)
- Mail eXchanger record (MX record)

سوال ۱۱: بعد از کلیک کردن بر روی OK چه اتفاقی می‌افتد؟

تنها بسته‌هایی که مبدأ یا مقصد آن‌ها برابر با آدرس واردشده است (5.144.130.115) نمایش داده می‌شوند.

در بسته‌هایی که مشخص شده‌اند چه پروتکل‌هایی را مشاهده می‌کنید؟

ICMP, IPV4, Ethernet

سوال ۱۲: اولین بسته را انتخاب کنید. به بخش پروتکل Internet Control Message Protocol بروید. مقدار type را مشخص کنید. به بخش مربوط به پروتکل IP بروید و مقدار TTL را یادداشت کنید.

Type = 8 (Echo (ping) request)
TTL = 16

برای بسته‌هایی که مبدأ آن‌ها ماشین شماست مقدار TTL را یادداشت کنید. این مقدار در حال تغییر است.

مقادیر TTL = 16, 16, 16, 50, 50, 50

سوال ۱۳: به نظر شما هدف از تغییر این مقدار چیست؟ می‌توانید با مراجعه به هدف دستور tracert آن را شرح دهید.

از آن‌جا که تعداد دستگاه‌های میانی بین مبدأ و مقصد به ازای همه‌ی درخواست‌ها یکسان نیست، TTL باید متناسب با تعداد دستگاه‌های میانی تغییر کند.

از بخش فیلتر، مقدار فیلتر را به دستور ip.proto == 6 را تغییر دهید.

سوال ۱۴: این فیلتر چه کاری انجام می‌دهد؟

این فیلتر تنها بسته‌هایی را نمایش می‌دهد که در آن‌ها از پروتکل شماره ۶ (TCP = Transmission Control Protocol) استفاده شده‌است.