**آزمایشگاه شبکه - جلسه اوّل - پاسخ سؤالات فصل ۲ لایه‌ی کاربرد**

**امیرمحمّد آقاپور ۹۶۳۱۰۰۸**

**سوال ۱: سایتی که ایجاد کرده‌اید نمایش داده نمی‌شود، چرا؟**

زیرا آدرس host در DNS محلی ویندوز و یا سایر DNS ها وجود ندارد بنابراین مرورگر نمی‌تواند IP مربوط به آن که 127.0.0.1 هست را پیدا کند.

**سوال ۲: آدرس سایت خود را در مرورگر وارد کنید و ارتباط خود را با استفاده از wireshark شنود کنید. آیا می‌توانید مشخص کنید کدام بسته مربوط به سایت شما است؟ چه اتفاقی افتاده است؟**

اگر در WireShark واسط شبکه را آداپتور خارجی مانند Ethernet یا Wifi مشخص کرده باشیم بسته ها توسط برنامه capture نمی‌شوند و قابل مشاهده نیستند. دلیل این امر آن است که سیستم عامل آدرس مقصد هایی که local هستند را به سایر آداپتور ها نمی‌فرستد. امّا اگر آداپتور را loopback انتخاب کنیم، که تمام بسته ها به آن فرستاده می‌شوند، بسته به مقصد 127.0.0.1:80 قابل مشاهده خواهد بود.

**سوال ۳: آدرس پورت‌های مبدا و مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص می‌دهد؟**

پورت مبدأ یک پورت دلخواه، که توسط مرورگر گرفته شده است، می‌باشد(در یک اجرا برابر 4779 بود) و پورت مقصد برابر 80 که پورتی است که وب سرور روی آن listen می‌کند.

برای برقراری ارتباط ابتدا یک اتصال TCP با handshake تشکیل می‌شود(که شامل SYN و ACK آن است) و سپس پیام HTTP توسط کلاینت فرستاده می‌شود که شامل method و ورژن و آدرس و بدنه است.

با هدر Host. پیام های درخواست در HTTP شامل header هایی هستند که یکی از آن ها Host است که در آن آدرس سایت مقصد مشخّص می‌شود و می‌توان از آن برای میزبانی چند سایت با یک وب سرور استفاده کرد.(virtual hosting)

**سوال ۴: مقدار بخش Connection چیست؟ درخواست HTTP از نوع GET بوده است یا از نوع POST؟ مقدار User Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟**

مقدار connection برابر keep-alive است که یعنی مرورگر درخواست داده که وب سرور اتصال TCP را نبندد و برای سایر درخواست ها از آن استفاده شود. می‌توانست مقدار close را داشته باشد که اتصال بسته شود.

از نوع GET، برای مشاهده صفحه و دریافت object از آن استفاده می‌شود.

user agent برابر Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 است که مشخصات سیستم عامل و مرورگر را به سرور اعلام می‌کند.

**سوال ۵: در پنجره باز شده، اولین بسته را انتخاب کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟**

اولین بسته‌ی HTTP در نظر گرفته شده که درواقع اولین بسته بعد از ارسال SYN و دریافت ACK آن می‌باشد.

در این بسته فلگ های push و acknowledgment ست شده‌اند که اوّلی یعنی فرستنده و مقصد بسته را بافر نکنند و منتظر جمع شدن بسته ها تا رسیدن به یک اندازه مشخص نشوند. فلگ دوم یعنی acknowledgment number در بسته معتبر بوده که برابر ۱ است(یعنی تا بسته seq=0 دریافت شده و منتظر بسته seq=1 می‌باشیم)

سایر فلگ ها مقدار صفر دارند مانند fin, urgent, syn, reset, cwr .

**سوال ۶: یک سایت دیگر با نام دلخواه ایجاد کنید و بسته‌های مربوط به آن را شنود کنید. چه تفاوتی بین این دو سایت وجود دارد؟**

مقدار host در header متفاوت است و برابر آدرس سایت جدید است.

**سوال ۷: در مرورگر آدرس ۱۲۷.۰.۰.۱ را تایپ کنید. چرا هیچ‌کدام از سایت‌ها نمایش داده نمی‌شوند؟**

زیرا وب سرور از مقدار host در header تشخیص می‌دهد که محتوی کدام سایت را برگرداند و با وارد کردن آدرس IP به جای نام host مرورگر این header را نمی‌تواند مقدار دهی کند.

**سوال ۸: آیا با مشکلی مواجه شدید؟ اگر با مشکل مواجه شده‌اید با استفاده از rawcap، مشخص کنید که چه مشکلی وجود دارد.**

به دلیل معتبر نبودن گواهی(به گواهی های root ارجاع نمی‌دهد) ارائه شده توسط سایت در تشکیل ارتباط TLS مشکل ایجاد می‌شود. البته اگر گواهی را در ویندوز به گواهی‌نامه‌های root اضافه کنیم این مشکل پیش نمی‌آید.

**سوال ۹: مشخص کنید که گواهی را چه کسی برای چه کسی صادر کرده، مدت‌زمان اعتبار گواهی چقدر است، کلید عمومی صادرکننده چیست و امضای دیجیتال انجام شده با چه الگوریتم‌هایی انجام شده است.**

مطابق اطلاعات موجود در گواهی، صادر کننده همان Issuer و برابر آدرس خود سایت که موقع ساخت گواهی داده شد می‌باشد که net.lab است.(مگر آنکه گواهی را در ویندوز به عنوان root نصب کرده باشیم) در مرور گر آن را به صورت " The original certificate provided by the web server is untrusted" نشان می‌دهد. کسی که برای آن صادر شده همان Subject است و برابر net.lab است که آدرس سایت جهت تست است. مدّت زمان اعتبار از 8/26/2020 (not before) و تا 8/26/2021 (not after) تعریف شده است. در قسمت public key info مشاهده می‌شود کلید از نوع RSA 2048 و مقدار modulus برابر :

B7:5D:70:80:A3:F1:5E:E3:F4:BD:52:CD:CD:95:16:16:49:CB:0C:3B:4D:27:5C:96:11:0F:0F:DD:D4:66:6
8:0A:C8:D0:41:30:50:D4:59:FF:08:BF:68:94:24:6F:6F:44:D5:46:63:88:8B:5C:FD:D9:64:CE:D2:A5:1E:
2B:D8:52:49:D4:18:42:1E:35:E7:51:3B:75:8F:35:20:FD:7B:2A:76:BE:3F:FD:44:C6:10:79:68:84:61:DE
:AC:3A:42:71:52:90:F4:DB:00:17:73:E3:B8:9E:FA:BC:15:8A:C4:A5:C3:39:E9:46:9F:52:B1:1B:9D:A5:C
5:14:4E:23:2C:9A:88:CE:E3:84:5D:C9:3B:76:DE:A7:59:1C:17:85:54:D7:B8:DA:1B:ED:B3:C6:03:C1:B3:
13:D1:CC:BF:8C:C5:DD:F2:76:12:F7:4A:C5:BB:40:D9:0C:D2:1A:29:C0:97:E6:12:0B:90:52:D3:2A:00:10
:C9:19:73:14:66:D5:E6:D4:CE:5E:9A:F5:5C:7D:F7:04:E9:39:43:EA:A5:48:A5:55:86:0D:5E:E0:52:CC:F7
:7D:15:DB:5A:70:9C:E8:64:4A:78:0A:23:DF:5D:DA:19:31:5C:0A:6D:7D:67:81:E5:1D:9E:91:1B:51:63:6
C:4E:FD:9B:24:FD:AA:03:45:30:11

و مقدار exponent برابر 65537 است. الگوریتم امضای دیجیتال SHA-256 with RSA Encryption ذکر شده است.

(این اطلاعات از طریق مرورگر و بخش Certificate info for net.lab به دست آمده است.)

**سوال ۱۰: آیا می‌توانید متن ارتباط را بخوانید؟ چرا؟**

خیر؛ زیرا تمام متن ارتباط غیر از handshake اولیه با الگوریتم RSA رمزگذاری شده و تنها کسی که کلید خصوصی را دارد می‌تواند رمزگشایی کند.

**سوال ۱۱: به یک سایت مانند https://google.com وصل شده، گواهی آن را بررسی کنید. گواهی آن سایت با گواهی سایت شما چه تفاوت‌هایی دارد؟**

مقدار common name که آدرس سایت است برابر www.google.com است. مدت زمان اعتبار آن نیز فرق دارد. کلید عمومی از الگوریتم Elliptic Curve با اندازه کلید 265 و خم استاندارد P-256 استفاده می‌کند. این الگوریتم با اندازه کلید بسیار کوچکتر نسبت به RSA، امنیت و کارآیی(سرعت محاسبه) بهتری دارد. تفاوت مهم تر آنکه به یک root certificate اشاره می‌کند که نام آن ESET SSL Filter CA است.

**سوال ۱۲: مشخص کنید چه دستوری برای لیست کردن فایل‌های دایرکتوری استفاده شده است. مشخص کنید چه نام کاربری برای دسترسی به سایت استفاده شده است. پروتکل لایه Transport استفاده شده برای این بسته‌ها چیست؟ آدرس پورت مبدا و مقصد ارتباط را مشخص کنید.**

از دستور LIST برای دریافت فایل ها استفاده شده است. بعد از وارد کردن آدرس در مرورگر نام کاربری پرسیده شد که نام کاربری تعریف شده در قسمت admin که برابر am.a است وارد شده و محتوی بسته هم برابر USER am.a است. پروتکل استفاده شده TCP است. پورت مبدأ 12371 که پورت رندوم مرورگر است و پورت مقصد 21 است که پورت مورد استفاده برای تبادل دستورات در FTP است.

**سوال ۱۳: آیا نام کاربری و پسورد قابل خواندن است؟**

بله؛ زیرا ارتباط رمزگذاری نشده است. دستور PASS 1234 برای ارسال رمز عبور استفاده شده است و پاسخ با کد 230 و متن Logged on دریافت شده است.

**سوال ۱۴: به FTP Authentication و FTP Authorization وارد شوید و مشخص کنید چه سطح دسترسی برای چه کاربرانی تعریف شده است.**

یک کاربر با نام am.a تعریف شده که دسترسی به پوشه C:\Users\ دارد. دسترسی از نوع خواندن و list کردن دایرکتوری و subdirectory ها را دارد. اجازه نوشتن و پاک کردن و ایجاد فایل را ندارد.

**سوال ۱۵: سعی کنید دوباره سایت را از مرورگر باز کنید. آیا می‌توانید به سایت وارد شوید؟ (حذف شده)**

**سوال ۱۶: در مرورگر فایرفاکس خطای نمایش داده شده در شکل (۲۳-۲) نشان داده می‌شود. معنی این خطا چیست؟ (حذف شده)**