۱- راه‌اندازی سرویس‌های Web و FTP

۱-۱- هدف آزمایش

هدف این آزمایش، آشنایی با تنظیمات مقدماتی مربوط بـه راه‌انـدازی سـرویس‌هـای Web و FTP و تحلیل بسته‌های HTTP و FTP است.

۱-۲- قطعات و ابزارهای موردنیاز

ابزارهای موردنیاز در این آزمایش عبارت‌اند از:

- کامپیوتر شخصی با سیستم‌عامل ویندوز 7 به بعد برای هر شخص
- برنامه Filezila آخرین نسخه

۱-۳- شرح آزمایش

۱-۳-۱- تنظیمات سرور Web

۱. آدرس سایت خود را در مرورگر وارد کنید بسته‌های مربوط به سـایت را پیـدا کنیـد. بـر روی یکی از آن‌ها کلیک راست کرده و follow HTTP Stream را انتخاب کنیـد. شـکلی مشابه شکل (۱-۱) نمایش داده خواهد شد.

No.	Time	Source	Destination	Protocol	Length	Info
58	5.996343	127.0.0.1	127.0.0.1	TCP	48	7391 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=65495 SACK_PERM=1
59	5.996343	127.0.0.1	127.0.0.1	TCP	48	80 → 7391 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=65495 SACK_PERM=1
60	5.996343	127.0.0.1	127.0.0.1	TCP	40	7391 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
61	5.996343	127.0.0.1	127.0.0.1	HTTP	580	GET / HTTP/1.1
62	5.996343	127.0.0.1	127.0.0.1	TCP	40	80 → 7391 [ACK] Seq=1 Ack=541 Win=7652 Len=0
63	5.998343	127.0.0.1	127.0.0.1	HTTP	337	HTTP/1.1 200 OK (text/html)
64	5.998343	127.0.0.1	127.0.0.1	TCP	40	7391 → 80 [ACK] Seq=541 Ack=298 Win=7895 Len=0

شکل (۱-۱) نمونه‌ای از خروجی Follow HTTP Stream

سوال ۱: آدرس پورت‌های مبدا و مقصد چیست؟ رونـد برقـراری ارتبـاط در پروتکـل HTTP چگونـه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص می‌دهد؟

۲. بر روی اولین بسته در پنجره باز شده کلیک کنید. بخش‌های مختلف پروتکـل HTTP را مشاهده کنید.

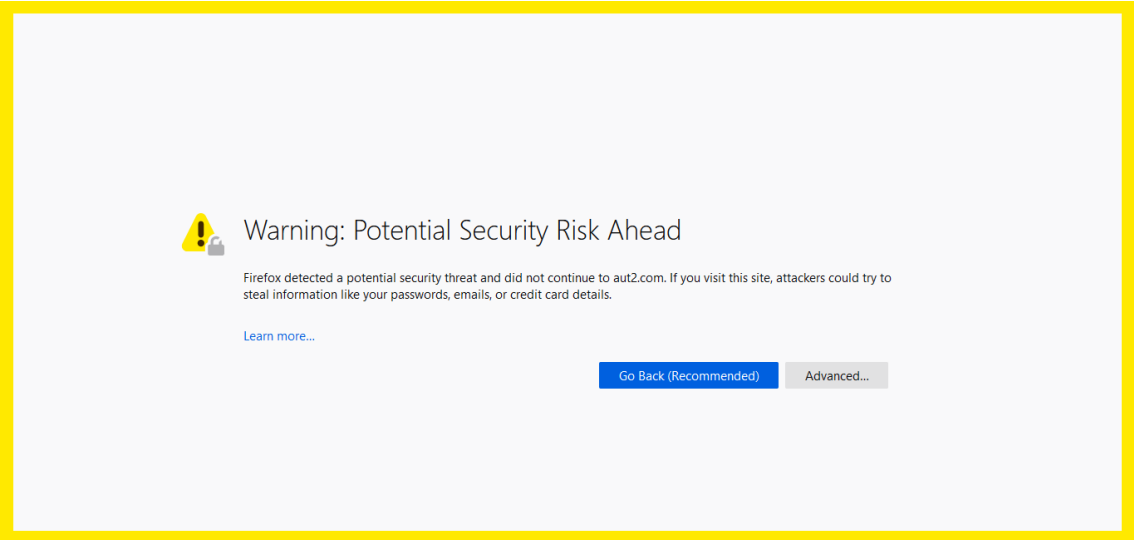
سوال ۲: مقدار بخش Connection چیست؟ درخواست HTTP از نـوع GET بـوده اسـت یـا از نـوع POST؟ مقدار User Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟

سوال ۳: 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؟

سوال ۴: یک سایت دیگر با نام دلخواه ایجاد کنید و بسته‌های مربوط به آن را شنود کنید. چه تفاوتی بین این دو سایت وجود دارد؟

۳. حال آدرس https://www.example.com/ را در مرورگر خود باز کنید. دقت کنید که به‌جای test.com آدرس سایت خود را قرار دهید.

۴. سایت را در مرورگر باز کنید. خطای نشان داده شده در شکل (۱-۲) نمایش داده می‌شود.



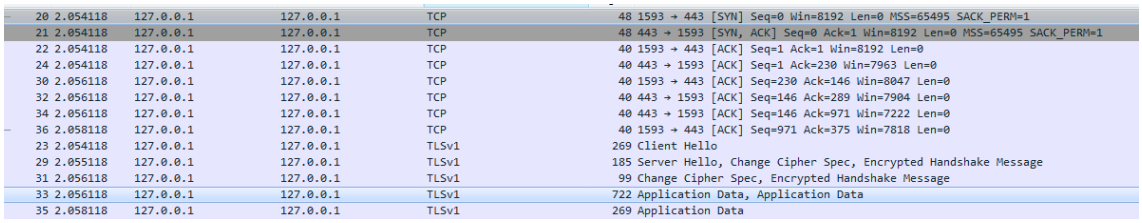
شکل (۱-۲) خطای نمایش داده شده

۵. بر روی Advanced کلیک کرده و دکمه View Certificate را فشار دهید.

سوال ۵: 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.

۶. حال ارتباط را با وایرشارک شنود کنید. بر روی بسته TLS مربوط به این ارتباط کلیک راست کرده و Follow SSL Stream را انتخاب کنید. صفحه‌ای مطابق شکل (۱-۳) نمایش داده می‌شود.

سوال ۶: آیا می‌توانید متن ارتباط را بخوانید؟ چرا؟



شکل (۱-۳) نمونه خروجی Follow SSL Stream

به یک سایت مانند https://google.com وصل شده، گواهی آن را بررسی کنید. برای اینکار بر روی علامت قفل در کنار آدرس سایت کلیک کنید. سپس بر روی علامت > در روبروی عبارت Connection Secure و سپس More Information کلیک کنید. در پنجره جدید باز شده از طریق View Certificate اطلاعات مربوط به گواهی وبسایت https://www.google.com/ قابل مشاهده است.

سوال ۷: گواهی آن سایت با گواهی سایت شما چه تفاوت‌هایی دارد؟

۱-۳-۲- تنظیمات سرور FTP

۷. ابتدا از طریق XAMPP ماژول FileZilla را استارت کنید. سپس طبق آموزش یک اکانت با رمز عبور دلخواه ایجاد کنین. سپس مسیر دلخواه برای به اشتراک‌گذاری را مشخص کنید.

۸. به آدرس ftp://127.0.0.1/ بروید. ارتباط را با وایرشارک شنود کنید.

سوال ۸: 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.

۹. تنظیمات مربوط به استفاده از SSL برای FTP را از طریق XAMPP فعال کنید.

سوال ۹: سعی کنید دوباره سایت را از مرورگر باز کنید. آیا می‌توانید به سایت وارد شوید؟

۱۰. برنامه Filezilla را از آدرس https://filezilla-project.org/ دانلود کنید. پس از نصب، در قسمت Host، 127.0.0.1 را بنویسید. نام کاربری و پسورد کاربری را که ایجاد کرده‌اید، وارد کنید و بر روی Quickconnect کلیک کنید. ارتباط را با وایرشارک شنود کنید. آیا نام کاربری و پسورد قابل‌خواندن است؟

۱-۳-۳- پروتکل HTTP

۱. عمل شنود را آغاز کنید، مرورگر را باز کرده و به آدرس http://aut.ac.ir بروید. شنود را متوقف کرده و بسته‌ها را بررسی کنید:

۲. بر روی یکی از بسته‌های پروتکل HTTP کلیک راست کـرده و Follow HTTP Stream را انتخاب کنید. اگر Wireshark شما این گزینه را ندارد آن را به روز کنید.

۳. بر روی اولین بسته در پنجره باز شده کلیک کنید. بخش های مختلف پروتکل HTTP را مشاهده کنید. مقدار بخش Connection چیست؟ درخواست HTTP از نـوع GET بـوده است یا از نوع POST؟ مقدار User Agent چیست؟ به نظر شما ایـن مقـدار بیـانگر چـه چیزی است؟

۴. در پنجره باز شده، بسته هایی با پروتکل TCP هم مشخص شـده اسـت. اولـین بسـته را انتخاب کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید. چه مقـادیری بـرای این بسته تنظیم شده است؟

۱-۳-۴- پروتکل FTP

۱. عمل شنود را آغاز کرده و مرورگر را باز کرده و به آدرس ftp://ftp.lip6.fr/ بروید. شنود را متوقف کنید. یک بسته مربوط به پروتکل FTP را انتخاب کرده، بر روی آن کلیک راست کنید و Follow TCP Stream را انتخاب کنید.

۲. پروتکل لایه Transport استفاده شده برای این بسته هـا چیسـت؟ آدرس پـورت مبـدا و مقصد ارتباط را مشخص کنید.

۳. در یکی از بسته ها مقدار Username و در بسته دیگر مقدار Password به سـمت سـرور ارسال شده است. این مقادیر را مشخص کنید.