راه‌اندازی سرویس‌های Web و FTP

سوال ۱: آدرس پورت‌های مبدأ و مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص دهد؟

پورت مقصد = 80
پورت مبدأ = 52850
روند برقراری = کامپیوتر از طریق پورت 52850 یک درخواست برای پورت 80 ارسال می‌کند؛ سپس پورت 80 اطلاعات درخواستی را ارسال می‌کند.
نحوه تشخیص سایت درخواستی: در بخش Host، آدرس سایت درخواستی آمده‌است.

سوال ۲: 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؟

Connection = keep-alive

درخواست HTTP از نوع GET بوده‌است.

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36

مقدار User-Agent بیانگر سیستم‌عامل و مرورگر است.

سوال ۳: در پنجره باز شده، اولین بسته را انتخاب کنید. سپس مقدار Flags در پروتکل TCPرا مشاهده کنید. چه مقادیری برای این بسته تنظیم شده‌است؟

Flags: 0x011 (FIN, ACK) = Finish, Acknowledge

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؟

تفاوت بین بسته‌های آن دو سایت آدرس Host آن‌ها است که در اولی www.aut2.com و در دومی www.aut3.com است.
مقدار E-tag آن‌ها نیز متفاوت است.

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 انجام‌شده با چه الگوریتم‌هایی انجام شده‌است.

گواهی توسط localhost برای localhost صادر شده‌است.
مدت زمان اعتبار از 2009-11-11 تا 2019-11-09 است.
نوع کلید عمومی RSA(1024 bit) و پارامترهای آن 00 05 است.
امضای دیجیتال با استفاده از الگوریتم sha1RSA انجام شده‌است.

سوال۶: آیا می‌توانید متن ارتباط را بخوانید؟ چرا؟

خیر، به‌دلیل اینکه اطلاعات رمزگذاری شده‌اند.

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

تفاوت‌ها:

- صادرکننده آن: GTS CA 1O1
- تاریخ اعتبار: از 2021-01-12 تا 2020-10-20
- نوع کلید عمومی: ECC(255 bit) و پارامترهای آن: ECDSA_P256
- امضای دیجیتال با استفاده از الگوریتم sha256RSA انجام شده‌است.

سوال ۸: مشخص کنید چه دستوری برای لیست‌کردن فایل‌های دایرکتوری استفاده شده‌است. مشخص کنید چه نام کاربری برای دسترسی به سایت استفاده شده‌است. پروتکل لایه Transport استفاده‌شده برای این بسته‌ها چیست؟ آدرس پورت مبدأ و مقصد ارتباط را مشخص کنید.

دستور برای لیست‌کردن فایل‌های دایرکتوری: MLSD

نام کاربری: test

پروتکل لایه Transport: TCP

آدرس پورت مبدأ: 59444، آدرس پورت مقصد: 21

سوال ۹: سعی کنید دوباره سایت را از مرورگر باز کنید. آیا می‌توانید به سایت وارد شوید؟ آیا نام کاربری و پسورد قابل‌خواندن است؟

خیر، چیزی نمایش داده نمی‌شود.

نام کاربری و پسورد به دلیل رمزگذاری‌شدن قابل‌خواندن نیستند.

پروتکل HTTP

۳. 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؟

Connection = keep-alive

درخواست HTTP از نوع GET بوده‌است.

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36

مقدار User-Agent بیانگر سیستم‌عامل و مرورگر است.

۴. چه مقادیری برای این بسته تنظیم‌شده است؟

Flags: 0x012 (SYN, ACK) = Synchronization, Acknowledge

پروتکل FTP

۲. پروتکل لایه Transport برای این بسته‌ها چیست؟ آدرس پورت مبدأ و مقصد ارتباط را مشخص کنید.

پروتکل لایه Transport: TCP

آدرس پورت مبدأ: 61428، آدرس پورت مقصد: 21

۳. در یکی از از بسته‌ها مقدار Username و در بسته دیگر مقدار Password به سمت سرور ارسال شده‌است. این مقادیر را مشخص کنید.

مقدار Username: anonymous

مقدار Password: chrome@example.com