پیش گزارش ۴

کیان پورآذر ۴۰۱۳۱۴۰۳

سوال اول:

پروتکل HTTP (Hypertext Transfer Protocol)

HTTP (پروتکل انتقال ابرمتن) پروتکلی است که برای انتقال اطلاعات در وب استفاده می‌شود. این پروتکل به کاربران اجازه می‌دهد تا درخواست‌های خود را به سرورها ارسال کنند و پاسخ‌هایی شامل صفحات وب، تصاویر، و فایل‌های دیگر دریافت کنند HTTP .به صورت پیش‌فرض از پورت 80 استفاده می‌کند و ارتباطات آن به صورت متن ساده و بدون رمزنگاری انجام می‌شود، بنابراین اطلاعات بین کاربر و سرور می‌توانند در معرض جاسوسی قرار بگیرند.

پروتکل(FTP (File Transfer Protocol

FTP (پروتکل انتقال فایل) پروتکلی است که برای انتقال فایل‌ها بین کامپیوترها در یک شبکه استفاده می‌شود. این پروتکل به کاربران اجازه می‌دهد تا فایل‌ها را از سرور دانلود یا به آن آپلود کنند FTP .معمولاً از پورت‌های 20 و 21 استفاده می‌کند و می‌تواند به دو حالت فعال و غیرفعال تنظیم شود. همانندHTTP ، ارتباطات FTP نیز بدون رمزنگاری است، بنابراین اطلاعات حساس مانند نام کاربری و رمز عبور ممکن است در معرض خطر قرار گیرند.

مزایای استفاده از HTTPS به جایHTTP

HTTPS (پروتکل انتقال ابرمتن امن) نسخه‌ی امن HTTP است که از رمزنگاری SSL/TLS استفاده می‌کند تا داده‌های رد و بدل شده بین کاربر و سرور را محافظت کند. استفاده از HTTPS به جای HTTP چندین مزیت دارد:

1 .امنیت بیشتر HTTPS :داده‌ها را رمزنگاری می‌کند، بنابراین اگر حتی داده‌ها در مسیر انتقال رهگیری شوند، قابل خواندن نیستند.

2 .تأیید هویت HTTPS :تأیید می‌کند که کاربر به وب‌سایت واقعی متصل شده است و از حملات نوع "فریبکارانه " (Phishing)جلوگیری می‌کند.

3 .حریم خصوصی HTTPS :مانع از دیدن محتوای انتقالی توسط شخص ثالث می‌شود، بنابراین حریم خصوصی کاربران حفظ می‌شود.

4 .اعتماد کاربران: وب‌سایت‌های دارای HTTPS بیشتر به عنوان وب‌سایت‌های ایمن شناخته می‌شوند و کاربران به آن‌ها اعتماد بیشتری دارند.

5 .تأثیر مثبت برSEO : گوگل و دیگر موتورهای جستجو به وب‌سایت‌های دارای HTTPS امتیاز بیشتری می‌دهند و این می‌تواند رتبه‌بندی آن‌ها را بهبود بخشد.

سوال ۲:

درHTTP ، پیام‌ها و کدهای وضعیت (Status Codes) متعددی وجود دارند که نشان‌دهنده نتیجه درخواست‌های کاربر به سرور هستند. در زیر چهار مورد از کدهای وضعیت پر تکرار HTTP و توضیحات مختصری درباره هر یک آورده شده است:

۱.کد 200 (OK)

- معنی: این کد نشان‌دهنده این است که درخواست کاربر به‌درستی انجام شده و سرور با موفقیت پاسخ داده است.
- کاربرد**: زمانی که صفحه وب یا منبع مورد نظر کاربر به‌درستی دریافت می‌شود، این کد بازگردانده می‌شود.

۲. کد 301 (Moved Permanently)

- معنی: این کد نشان می‌دهد که منبع مورد درخواست کاربر به آدرس جدیدی منتقل شده است و این انتقال دائمی است.
- کاربرد: برای تغییر دائمی آدرس یک صفحه وب استفاده می‌شود. سرور آدرس جدید را به مرورگر اعلام می‌کند و درخواست‌ها به آدرس جدید هدایت می‌شوند.

۳. کد 404 (Not Found)

- معنی: این کد نشان‌دهنده این است که منبع درخواستی کاربر (مانند صفحه وب یا فایل) در سرور وجود ندارد یا قابل یافتن نیست.
- کاربرد: زمانی که کاربر سعی در دسترسی به یک صفحه یا فایل غیرفعال یا حذف شده دارد، این کد نمایش داده می‌شود.

۴. کد 500 (Internal Server Error)

- معنی: این کد نشان‌دهنده خطایی در سرور است که مانع از انجام موفقیت‌آمیز درخواست کاربر شده است.
- کاربرد: زمانی که خطای غیرمنتظره‌ای در سرور رخ دهد (مانند مشکل در اسکریپت‌ها یا تنظیمات سرور)، این کد نمایش داده می‌شود.

سوال سوم:

وایرشارک نمیتواند ترافیک مربوط به آدرس های Loopback را شنود کند ولی Rawcap توانایی اینکار را دارد.
Wireshark یک ابزار تحلیل شبکه بسیار قدرتمند است که قابلیت ضبط و تحلیل ترافیک شبکه را دارا می‌باشد. با استفاده ازWireshark ، می‌توانیم بسته‌های شبکه را ضبط کنید و جزئیات مربوط به پروتکل‌ها، آدرس‌ها، پورت‌ها و سایر اطلاعات مرتبط را بررسی کنید. Wireshark قابلیت تحلیل و نمایش داده‌های ضبط شده را در قالب یک رابط کاربری گرافیکی (GUI) ارائه می‌دهد و امکانات متنوعی برای فیلترینگ، جستجو و تجزیه و تحلیل داده‌ها فراهم می‌کند.
از سوی دیگر، RawCap یک ابزار ساده‌تر است که به ما امکان می‌دهد ترافیک شبکه را به صورت بسته‌بندی نشده (raw)ضبط کنیم. RawCap ساده‌ترین روش برای ضبط ترافیک شبکه است و بدون نیاز به نصب، وابستگی‌های خاصی یا تنظیمات پیچیده کار می‌کند. با استفاده ازRawCap ، می‌توانیم بسته‌های شبکه را به فایل‌های PCAP ذخیره کنیم. این فایل‌ها بعداً می‌توانند توسط ابزارهای دیگری مانند Wireshark برای تحلیل و بررسی استفاده شوند.