دانشکده‌ی مهندسی کامپیوتر

شبکه‌های کامپیوتری مدرس: مهدی جعفری

لایه Application (عملی)

گردآورندگان: کسری امانی - مهدی علیزاده دوشنبه ۸ آبان ۱۴۰۲

جواب‌ها را حتما به صورت **تایپ شده** تحویل دهید.
لازم نیست که برای هر سوال یک پاراگراف بنویسید و صرفا **پاسخ کوتاه در حد یک یا حداکثر ۲ خط** بنویسید.
از تمام مراحل انجام سوالات **اسکرین‌شات** تهیه کنید و در پاسخ قرار دهید. در صورت نوشتن هر گونه کد، آنرا ضمیمه کنید.
قسمت‌های مشخص شده با علامت * سوالات و یا مطالب کاربردی هستند که جواب دادن و خواندن آنان اختیاری است اما نمره اضافی ندارد.

۱ Telnet

در این تمرین، شما با استفاده از پروتکل telnet برای اتصال به یک سرور و تجزیه و تحلیل پکت‌های شبکه با استفاده از ابزارهای sniffing، تجربه عملی کسب خواهید کرد.

۱.۱ اتصال از طریق Telnet

تلنت یک پروتوکل شبکه مبتنی بر متن است که قابلیت برقراری سشن‌های دوطرفه میان کلاینت و سرور را دارد. این مراحل را برای برقراری ارتباط از طریق تلنت بین شما و سرور telehack.com دنبال کنید:

۱. ابتدا یک ابزار کلاینت تلنت را نصب و اجرا کنید. (PuTTY - Telnet)

۲. کلاینت تلنت را باز کرده و به سرور `telehack.com` روی پورت ۲۳ متصل شوید.

۳. BBS تعاملی را با تایپ دستورات و پیمایش در رابط پس از اتصال، کاوش کنید. به عبارتی دیگر در ترمینال باز شده چندین برنامه را اجرا کنید و خروجی آن‌ها را مشاهده کنید.

۲.۱ بررسی پکت ها

از یک ابزار آنالیز پکت مانند Wireshark برای بررسی نشست تلنت با telehack.com استفاده کنید.

۱. ضبط فعالیت پکت‌ها در Wireshark را قبل از برقراری اتصال تلنت شروع کنید و از فیلترهای موجود برای حذف پکت‌های نامرتبط استفاده کنید.

۲. پکت‌ها را بررسی کرده و هدرها و محتوای آن را مشاهده کنید.

۳. مقدار throughput را بر اساس تعداد و حجم پکت‌ها محاسبه کنید.

۴. آیا بسته‌ها بدون رمزنگاری انتقال پیدا می‌کنند؟ این موضوع باعث می‌شود چه کارهایی با Telnet ایده‌ی خوبی و چه کارهایی ایده‌ی بدی باشد؟

۵. تحقیق کنید فرق اصلی SSH و Telnet در چیست.

۶. هر مشاهده جالب دیگری از بازرسی پکت‌ها را خلاصه کنید.

۲ مقایسه HTTP و HTTPS

در این تمرین، ترافیک شبکه HTTP و HTTPS را ضبط و تجزیه و تحلیل خواهید کرد تا تفاوت‌های امنیتی و رمزگذاری را مشاهده کنید.

۱.۲ بررسی ترافیک HTTP

The first website ever created is still running at CERN: info.cern.ch

۱. از یک ابزار تحت ترمینال مانند curl برای ارسال یک request با پروتوکل HTTP به این وبسایت استفاده کنید و درخواست و پاسخ ها را مشاهده کنید. برای استفاده از curl کافی است که دستوری مانند دستور زیر را اجرا کنید:

```
curl -v info.cern.ch
```

۲. محتوای ضبط شده مانند هدرها، کدهای وضعیت و متن خام را بررسی کنید.

۳. مشاهدات خود در مورد ذات ناامن HTTP را خلاصه کنید.

۲.۲ HTTP از طریق ncat

از ابزار شبکه ncat برای ارسال مستقیم یک درخواست HTTP به وبسایت دلخواه خود (مانند www.example.com) استفاده کنید و پاسخ سرور را مشاهده کنید. برای این کار می‌توانید دقیقا دیتایی که در قسمت قبل دیدید که curl به سایت مورد نظر می‌فرستد را با کمی تغییر به این سایت نیز بفرستید.

۳.۲ بررسی ترافیک HTTPS

۱. یک وبسایت که از HTTPS استفاده می‌کند را به دلخواه خود باز کرده و فعالیت شبکه را ضبط کنید.

۲. پکت‌های ردوبدل شده را مشاهده کنید و توضیح دهید که کدام بخش‌ها رمزگذاری نشده‌اند و دلیل آن را ذکر کنید.

۳. توضیح دهید که فیلد SNI در اولین پکت Client Hello چه چیزی را نشان می‌دهد و چه طور می‌توان از آن برای فیلترینگ استفاده کرد.

۴. (اختیاری) چرا فیلد SNI به صورت رمزنگاری نشده رد و بدل می‌شود؟*

۵. توضیح دهید که تفاوت عملکرد این دو پروتوکل چگونه باعث افزایش ایمنی خواهد شد.

۳ DNS

در این سوال قصد داریم با استفاده از دستور dig به تحلیل رکوردهای dns بپردازیم. به طور خلاصه با استفاده از این دستور می‌توانید اطلاعات مورد نیاز را درمورد دامنه‌های مختلف بدست بیاورید. برای مطالعه بیشتر برای نحوه کارکرد دستور dig می‌توانید به man page این دستور مراجعه کنید.

۱.۳

دستور زیر را در ترمینال وارد کنید و توضیح دهید خروجی این دستور چه اطلاعاتی به ما می‌دهد. تمام فیلدهای نمایش‌داده شده در خروجی را توضیح دهید که مربوط به چه چیزی هستند.

```
dig -t NS ce.sharif.edu +noall +answer
```

۲.۳

سوال‌های بالا را این بار برای دستور زیر پاسخ دهید.

```
dig ce.sharif.edu MX +noall +answer
```

در صورتی که از ویندوز استفاده می‌کنید از دو دستور زیر استفاده کنید:

```
nslookup -q=NS ce.sharif.edu
nslookup -q=MX ce.sharif.edu
```

۴ HTTP Proxy

در این سوال قصد داریم با استفاده از proxy آماده یک http proxy ساده راه‌اندازی کنیم و با استفاده از wireshark به تحلیل پکت‌ها بپردازیم.

۱.۴ راه اندازی

ابتدا با استفاده از gost یک proxy بر روی لپ تاپ خود راه‌اندازی کنید.

۲.۴ curl

حال wireshark را در حالت capture بر روی کارت شبکه‌ی local خود قرار دهید و با استفاده از دستور curl یک HTTP GET ریکوئست به آدرس sharif.edu بزنید. در آخر بسته‌های مربوط به این ریکوئست را پیدا کنید و آدرس و مبدا و مقصد و همچنین قسمت body این بسته‌ها را را مشخص کنید و این فرآیند رو به صورت مختصر توضیح دهید. (راهنمایی: برای ست کردن پروکسی در دستور curl می‌توانید از فلگ x- استفاده کنید.)
نکته: عکس‌هایی از نرم‌افزار wireshark و صفحه‌ی لاگ‌های gost در پاسخ خود قرار دهید.

۳.۴ gost (احتمالا به کارتان بیاید)*

بررسی کنید که gost دقیقا به چه دردی می‌خورد و کجا استفاده می‌شود.

۵ netstat

netstat یک CLI برای تحلیل شبکه و کانکشن‌ها در UNIX است. در این سوال قصد داریم با قابلیت‌های این دستور بیشتر آشنا شویم.

۱. با استفاده از این دستور تمام conection های ایجاد شده را پیدا کنید.

۲. با استفاده از این دستور تمام conection های tcp را پیدا کنید.

۳. با استفاده از این دستور تمام conection های udp که در حالت listen هستند را پیدا کنید.

۴. با استفاده از این دستور statistics مربوط به پروتکل arp را بدست آورید و به صورت خاص نشان‌دهید که چند ریکوئست broadcast تحت این پروتکل توسط دستگاه شما در شبکه ارسال شده است.

۶ HTTP Server (ساده ولی به شدت کاربردی!!)*

در این قسمت یاد می‌گیریم که چگونه بدون استفاده از فلش یا قطعه فیزیکی چندین فایل را بین چندین کامپیوتر که به یک شبکه وصل هستند جا به جا کنیم. برای این کار کافی است که پایتون نسخه ۳ را نصب داشته باشید.
بر روی کامپیوتری که قرار است که فایل‌ها از آن انتقال بیابند دستور زیر را در فولدری که فایل‌ها در آن هستند وارد کنید:

```
python3 -m http.server
```

با این کار یک HTTP server بر روی پورت ۸۰۰۰ کامپیوتر شما بالا می‌آید. در صورتی که می‌خواهید بر روی پورت دیگری سرور را اجرا کنید کافی است که از دستور زیر استفاده کنید:

```
python3 -m http.server 12345
```

با این کار یک پراکسی سرور بر روی پورت ۱۲۳۴۵ اجرا می شود.
حال می‌توانید از دستور ip a یا ipconfig استفاده کنید که آدرس آی‌پی داخلی خود را پیدا کنید. مثلا در اینترنت دانشگاه IP شما با ۱۷۲ شروع می‌شود. در صورتی که آی‌پی خود و پورت انتخابی را در آدرس بار مرورگر کامپیوتر دیگری که به همان اینترنت وصل است بزنید باید که بتوانید فایل‌های خود را ببینید و دانلود کنید. از این روش حتی برای جابه‌جایی فایل‌ها بین ماشین‌های مجازی خود نیز می‌توانید استفاده کنید.

۷ (بیشتر بدانید) *HTTP vs Socks Proxy

AI Multiple

FEATURES	HTTP(s) Proxies	SOCKS Proxies
Security	HTTP(s) proxies add an extra layer of security between a client and a web server.	SOCKS5 proxies are the only ones that use an encrypted tunneling method between a client and a proxy server.
Speed & Performance	HTTP proxies only support TCP connections. TCP sets up a connection between a user and a destination before sending data. It ensures that data reaches its intended destination. However, it slows down the data transmission process.	SOCKS proxies are faster than HTTP proxies. SOCKS proxies support both UDP and TCP connections. UDP is faster and more efficient than TCP because it does not require any connection to be established before sending data to the destination source.
Authentication	✗	✓
Encryption of data	✓	✗

موفق باشید