



جلسه دوم - آشنایی با نرم افزار Wireshark

۱ مقدمه

نرم افزار Wireshark ابزاری متن‌باز برای تحلیل شبکه‌های رایانه‌ای است که جریان داده‌ی در حال عبور از واسط شبکه را دریافت کرده و در قالبی مشخص و قابل فهم برای انسان به نمایش می‌گذارد. این برنامه را می‌توان مانند یک چاقوی سوئیسی همه کاره در نظر گرفت و از آن برای اهداف مختلفی مانند تحلیل شبکه، عملیات امنیتی، اشکال‌یابی، اعمال مهندسی معکوس بر روی پروتکل‌ها و فهمیدن جزئیات درون آنها و ... استفاده کرد. برخی از مزیت‌های مهم استفاده از این ابزار به شرح زیر است:

- پشتیبانی از چندین پروتکل: محدوده‌ای بسیار گسترده از پروتکل‌های شبکه مانند پروتکل‌های TCP، UDP و HTTP تا پروتکل‌های پیشرفته مانند AppleTalk را پشتیبانی می‌کند.
- رابط کاربر پسند: رابط کاربری گرافیکی (GUI) بسیار قدرتمندی دارد که به متخصصین اجازه می‌دهد بسته‌های ضبط شده خود را به ساده‌ترین شکل ممکن تحلیل کنند. همچنین چندین گزینه پیشرفته از قبیل فیلتر کردن بسته‌ها، صادر کردن بسته‌ها و تفکیک‌کننده اسامی هم به ما ارائه می‌دهد.
- تحلیل زنده ترافیک: می‌تواند به صورت زنده جریان عبوری از واسط شبکه را دریافت کرده و به سرعت اطلاعات پروتکل، جریان رسانه، کانال‌های ارتباطی و... را در خروجی برای ما تولید کند.
- پروژه متن‌باز: ویرشارک پروژه‌ای متن‌باز است و توسعه‌دهندگان آن بیش از ۵۰۰ نفر از اقصی نقاط جهان هستند. حتی شما هم می‌توانید یکی از توسعه‌دهندگان این برنامه باشید.

۱.۱ نحوه کار Wireshark

شنود ترافیک شبکه زمانی ممکن است که واسط شبکه (کارت شبکه) بر روی حالت انتقال بی‌قاعده قرار گیرد. این حالت موجب می‌شود رابط شبکه تمامی ترافیک دریافتی را به واحد پردازشگر مرکزی انتقال دهد. در نهایت می‌توان شنود شبکه توسط Wireshark را به سه گام کلی تقسیم کرد که به شرح زیر هستند:

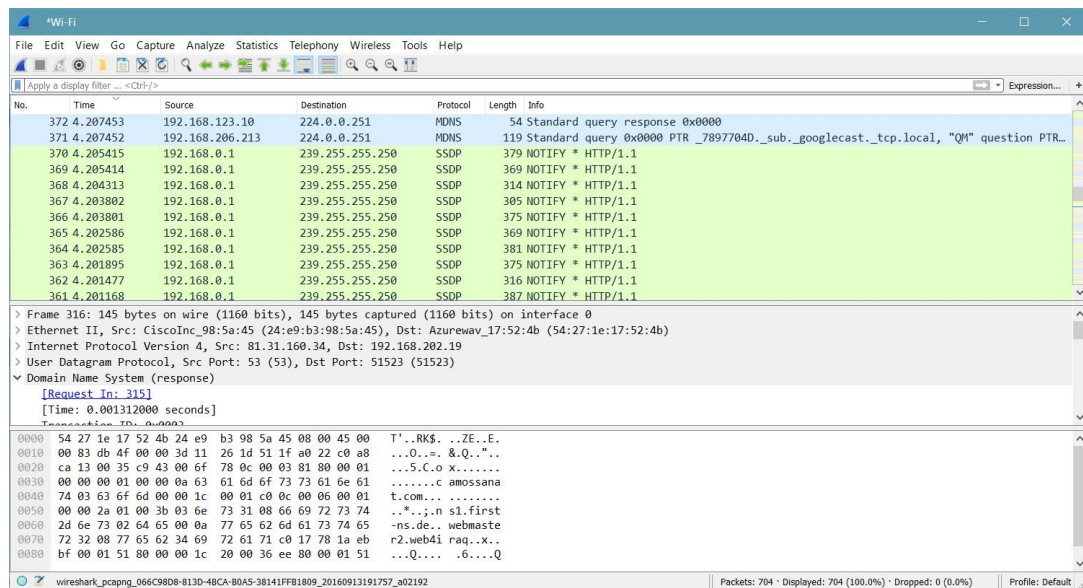
۱. جمع‌آوری: در گام اول، Wireshark رابط شبکه را به حالت بی‌قاعده انتقال می‌دهد تا بتواند داده‌های باینری خام بر روی واسط شبکه را دریافت کند.
۲. تبدیل: در گام دوم داده‌های باینری جمع‌آوری شده به یک قالب قابل فهم برای انسان تبدیل می‌شوند. همچنین بسته‌ها بر مبنای عدد سلسله مراتبی خود دوباره مونتاژ می‌گردند.
۳. تحلیل: گام آخر شامل تحلیل بسته‌های دریافت شده و داده‌های دوباره مونتاژ شده می‌گردد. تحلیل اولیه بسته‌ها شامل شناسایی نوع پروتکل، کانال ارتباطی، شماره درگاه و... می‌شود. همچنین در یک سطح پیشرفته سرآیندهای متفاوت پروتکل می‌توانند برای یک درک عمیق‌تر نیز مورد تحلیل قرار گیرند.

برخی از اهداف مورد نظر این برنامه عبارتند از:

- از بین بردن مشکلات به وجود آمده در شبکه
- بازبینی مشکلات امنیتی شبکه
- اشکال‌زدایی پیاده‌سازی پروتکل‌ها
- یادگیری کارکرد پروتکل‌ها

Wireshark این کارها را نمی‌تواند انجام دهد:

- عدم توانایی در تشخیص نفوذ به سیستم: این برنامه زمانی که شخصی عملیات غیرعادی که مجاز به انجام آنها نیست را در شبکه انجام دهد، هیچ خطاری برای ما در خروجی صادر نخواهد کرد. در هر صورت، به هنگام رخ دادن اتفاقات عجیب، Wireshark در دریافتن آنچه در حال رویدادن است فقط می‌تواند به متخصصین کمک کند.
- عدم توانایی در دستکاری شبکه: کار این نرم‌افزار فقط اندازه‌گیری در شبکه است؛ یعنی هیچ بسته‌ای را روی شبکه نمی‌فرستد یا فعالیت دیگری روی شبکه انجام نمی‌دهد. (به جز تفکیک اسامی، ولی حتی این ویژگی هم می‌تواند غیرفعال گردد)



شکل ۱: تصویری از محیط نرم‌افزار Wireshark

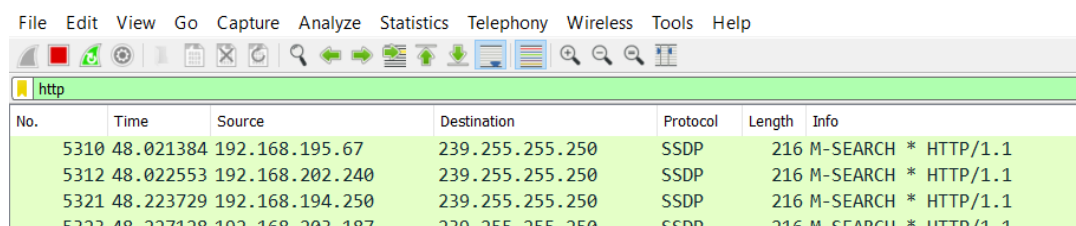
۲ بخش اول (فهم اولیه از HTTP)

در این آزمایش در کنار آشنایی با محیط نرم‌افزار، به انجام برخی عملیات ساده خواهیم پرداخت. در شکل ۱ نمای کلی این نرم‌افزار را می‌بینید که پیام‌های رد و بدل را شده لیست کرده است.

۱.۲ شرح آزمایش

عملیات زیر را انجام دهید:

- مرورگر دلخواهتان را باز کنید.
- Wireshark را در حالت Capture قرار دهید
- یک سایت دلخواه (که حاوی تصاویر نیز باشد) را باز کنید. (مثلا sharif.edu)
- پس از بارگذاری کامل به نرم‌افزار Wireshark برگردید و ضبط اطلاعات را متوقف کنید.
- برای مشاهده بهتر پیام‌های مربوط به پروتکل HTTP، کلمه “http” را درون نوار filter وارد کنید. مشاهده می‌کنید که تنها پیام‌های از نوع HTTP نمایش داده می‌شوند.



No.	Time	Source	Destination	Protocol	Length	Info
5310	48.021384	192.168.195.67	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
5312	48.022553	192.168.202.240	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
5321	48.223729	192.168.194.250	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
5323	48.227128	192.168.202.187	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

شکل ۲: فیلتر کردن پروتکل http

- اولین پیام با عنوان GET HTTP را انتخاب کنید و توجه کنید که اطلاعات سرآیندهای مختلفی که در Packet موجود هستند در قسمت پایین قابل دسترسی‌اند. اطلاعات مربوط به پروتکل HTTP را مشاهده کنید و Host مربوط به سایتی که در مرورگر خود باز کردید را پیدا کنید. اگر این Host با آدرس صفحه مورد نظر شما مطابقت دارد، پس این درخواست مربوط به شما است.

۲.۲ سوالات

۱. حجم عمده پیام‌های رد و بدل شده مربوط به کدام پروتکل‌ها است؟ هرکدام را به تفکیک اعلام کنید. (راهنمایی: از امکانات آماری تعبیه شده در نرم‌افزار استفاده کنید)
۲. اختلاف زمانی بین ارسال درخواست GET HTTP و دریافت پاسخ OK HTTP چقدر است؟ شماره ترتیب مطلق (absolute sequence number) اولین ارتباط TCP در این فایل را پیدا کنید. (در نظر داشته باشید که مطلق و نسبی (relative) دو کلمه متناقض هستند)
۳. نوع کوثری درخواست‌های DNS و پاسخ آن‌ها چیست؟
۴. عکس‌هایی که در این ارتباط از سرور دانلود شده‌اند را از طریق Wireshark بازیابی کنید.

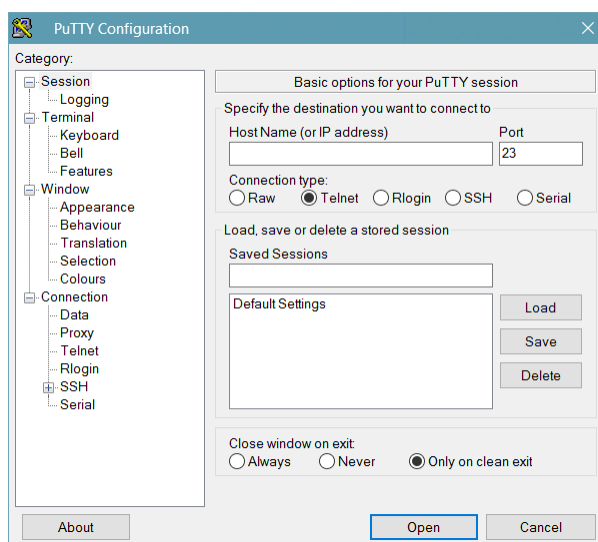
۳ بخش دوم (بررسی ارتباط از طریق Telnet)

۱.۳ مقدمه

تلنت یک پروتکل شبکه است که در اینترنت و شبکه های محلی برای ارائه یک ارتباط دوطرفه متنی با استفاده از اتصال پایانه های مجازی استفاده می شود. Telnet یا Telecommunication network نرم افزاری است که به افراد توانایی کنترل قسمت های مختلف یک کامپیوتر را از راه دور می دهد. در این پروتکل دستورات جا به جا شده بین کامپیوتر میزبان و میهمان، به صورت متن منتقل می شوند و بنابراین امنیت کمی خواهند داشت. پورت پیش فرض برنامه Telnet، عدد ۲۳ است.

۲.۳ شرح آزمایش

برای اتصال از طریق Telnet در سیستم عامل ویندوز نیاز دارید تا این ویژگی را در تنظیمات فعال کنید. همچنین نرم افزار Putty نیز برای فراهم آوردن این امکان در دسترس قرار دارد.



شکل ۳: محیط نرم افزار Putty

سپس عملیات زیر را انجام دهید:

- Wireshark را در حالت capture قرار دهید
- به آدرس telehack.com از طریق Telnet متصل شوید و چند دستور را امتحان کنید.
- بعد از اتمام کار، ارتباط را قطع و ضبط اطلاعات در Wireshark را متوقف کنید. و پیام های ضبط شده را بررسی نمایید.
- مشاهدات خود را اعلام کنید.

۳.۳ سوالات

فایل telnet.pcap حاوی اطلاعات ضبط شده یک ارتباط Telnet است. موارد زیر را در مورد این فایل پاسخ دهید:

۱. آدرس IP کلاینت و سرور را پیدا کنید.
۲. رمز عبوری که کلاینت برای لاگین استفاده کرده را بازیابی کنید.

۳. دستوراتی که توسط کلاینت اجرا شده‌اند را مشخص کنید.

۴ بخش سوم (بررسی درخواست و پاسخ‌های DNS)

۱.۴ مقدمه

یکی از دستورات بسیار مهم که برای اطلاع از وضعیت کنونی Host و بسیاری عملیات دیگر از آن استفاده می‌شود، `ipconfig` در ویندوز و `ifconfig` در یونیکس است. برای شروع می‌توانید دستور "`ipconfig -a`" در یونیکس (یا "`ipconfig /all`" در ویندوز) را استفاده کنید تا تمامی اطلاعات مربوط به واسط‌های مختلف رایانه شما نمایش داده شود. در یونیکس با اجرای دستور `dig` (یا `nslookup` در ویندوز) بر روی دستگاه، یک پرسش برای سرور DNS ارسال می‌شود و پاسخ آن برای کاربر نمایش داده می‌شود. سیستم DNS یک سیستم توزیع‌شده است که از مجموعه‌ای از `nameserver`ها تشکیل شده است و بخش مرکزی آن را `Root nameserver` ها تشکیل می‌دهند. برای هر دامنه اینترنتی نیز یک `Authorative nameserver` وجود دارد که حضور آن را در اینترنت تضمین می‌کند.

۲.۴ شرح آزمایش

برای ارسال پرسش می‌توان فرمان "`dig [hostname]`" (و یا "`nslookup [hostname]`") را وارد کرد، که در آن `hostname` نام دامنه مورد نظر است. در ادامه چگونگی اجرای این دستور را مشاهده خواهیم کرد:

- قبل از شروع آزمایش، `cache` مربوط به Host خود را پاک کنید. برای این کار در لینوکس دستور "`sudo /etc/init.d/networking restart`" و در ویندوز دستور "`ipconfig /flushdns`" را وارد نمایید.
- با استفاده از دستور `dig` یا `nslookup` درخواستی را مبنی بر آدرس IP یک سایت ارسال کنید. (توجه کنید که پاسخ را از کدام سرور دریافت می‌کنید)
- ضبط اطلاعات را در Wireshark متوقف کنید و با استفاده از نوار `filter` و عبارت "`ip.addr == YOUR_IP`" پیام‌هایی را نمایش دهید که فرستنده یا گیرنده آن‌ها دستگاه شما است. از بین این پیام‌ها، پیام‌های از نوع DNS پیام‌هایی هستند که توسط برنامه `dig` یا `nslookup` دریافت یا ارسال شده‌اند.

۳.۴ سوالات

به سوالات زیر پاسخ دهید:

۱. در دستور `dig` (یا `nslookup`) درخواست برای کدام سرور ارسال می‌شود؟ پاسخ‌ها از کدام سرور دریافت می‌شود؟ (این اطلاعات را از طریق Wireshark دریافت کنید)
۲. هدر پیام‌های `request` و `reply` مربوط به پروتکل DNS را تحلیل کنید.

موفق باشید