E-Security Cheat Sheet

آموزش بهتر **امنیت** بیشتر

Wireshark

By Ehsan Nikavar

http://esecuritv.ir

هدف

آشنایی با ابزار وایرشارک برای آنالیز بسته های داخل شبکه

این Cheat Sheet برای دوره های **PWK**، **CEH**، **ECSA** و **SEC 504** طراحی شده است.

ابزارها

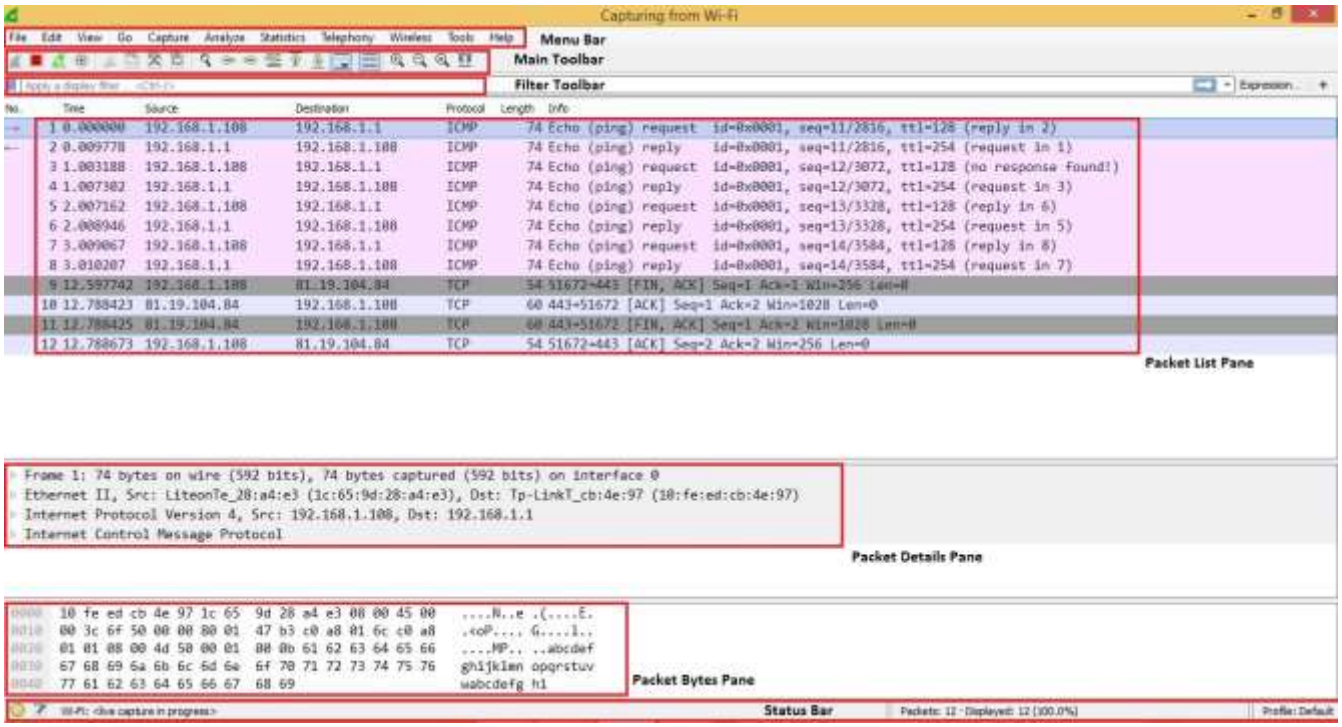
در این بخش با موارد زیر آشنا می شوید:

آشنایی با محیط وایرشارک

آنالیز بسته های شبکه

آشنایی با فیلترهای کاربردی

آشنایی با محیط Wireshark



Menu Bar: این بخش شامل منو های اصلی نرم افزار جهت نمایش، ذخیره و ضبط اطلاعات بسته ها می باشد.

Main Toolbar: این بخش دارای ابزارهای کاربردی به منظور مدیریت و شروع و پایان مانیتور نمودن بسته ها می باشد.

Filter Toolbar: در قسمت فیلتر شما می توانید مطابق با نیاز خود بسته های مورد نظر را فیلتر نمایید که این فیلتر می تواند بر اساس آدرس IP، Port، نوع پروتکل و محتویات بسته باشد.

Packet List Pane: در این بخش اطلاعات مربوط به ارسال و دریافت بسته ها مانند آدرس مبدا، مقصد و ... قابل مشاهده است.

Packet Details Pane: مشاهده جزئیات بیشتر بسته ها بر اساس لایه های مدل TCP/IP در این بخش به تفکیک لایه ها امکان پذیر خواهد بود.

Packet Byte Pane: در این بخش معادل Hex بسته ها قابل مشاهده خواهد بود.

Status Bar: در قسمت وضعیت هم می تواند از تعداد بسته های ردو بدل شده و وضعیت نرم افزار اطلاع حاصل کرد.

فیلترهای کاربردی عمومی

یکی از امکانات بسیار مهم و در وایرشارک، امکان فیلتر نمودن بسته ها با دستورات متنوع است.

فیلتر بر اساس آدرس IP خاص مانند 10.0.0.1

Ip.addr == 10.0.0.1

فیلتر بر اساس آدرس IP مبدا خاص مانند 10.0.0.1

Ip.src == 10.0.0.1

فیلتر بر اساس آدرس IP مقصد خاص مانند 10.0.0.1

Ip.dst == 10.0.0.1

فیلتر بر اساس آدرس پورت خاص TCP مانند 80

tcp.port == 80

فیلتر براساس آدرس پورت مبدا خاص مانند 80

tcp.srcport == 80

فیلتر براساس آدرس پورت مقصد خاص مانند 80

tcp.dstport == 80

نکته ۱: اگر قصد فیلتر نمودن بر اساس پورت های UDP را داشته باشید می توانید به جای TCP در فیلتر از UDP استفاده نمایید.

نکته ۲: برای هر نوع از دستورات بالا شما می‌توانید از عبارت منطقی =! هم استفاده نمایید.

ip.src != 10.0.0.1

tcp.srcport != 80

در مثال اول آدرس های IP مخالف 10.0.0.1 و در مثال دوم پورت های TCP و مخالف 80 لیست خواهند شد.

فیلترهای کاربردی عمومی

در وایرشارک علاوه بر فیلترینگ بر اساس آدرس های مختلف، فیلتر نمودن بر اساس پروتکل هم امکان پذیر می باشد. برای این منظور می توانید به صورت ساده، فقط نام پروتکل مانند dns، http، icmp و... را در قسمت فیلتر وارد کنید.

البته فیلتر پروتکل ها در وایرشارک، دارای زیر مجموعه هایی برای مشاهده اطلاعات جزئی تر هم می باشد که این اجزاء با وارد نمودن یک نقطه پس از نام پروتکل قابل مشاهده خواهند بود.

فیلتر برای لیست نمودن درخواست های GET در HTTP

http.request.method == GET

فیلتر برای لیست نمودن درخواست های POST در HTTP

http.request.method == POST

استفاده از دستور and و or برای ترکیب فیلترها

ip.dst == 10.0.0.1 and tcp.dstport == 80

نکته : به جای دستورات and و or می‌توان از معادل آن ها یعنی && و || استفاده نمود.

فیلتر بر اساس محتویات یک بسته

tcp contains windowsupdate.com

فیلتر بر اساس آدرس فیزیکی (MAC)

eth.addr == 5d:55:b8:88:84:e5

در مثال بالا به جای addr می توان برای آدرس مقصد از dst و برای آدرس مبدا از src استفاده کرد.

آنالیز شبکه

در ادامه به تحلیل ترافیک شبکه و شناسایی فرآیند های Scan در شبکه و حمله ARP Poisoning می پردازیم.

یکی از انواع اسکن، مربوط به اسکن پورت ها می‌باشد. در این اسکن بسته های مختلفی با flag های TCP ارسال می شود که در نتیجه آن می توان به باز یا بسته بودن پورت ها پی برد. نمونه ای از اسکن ها مانند FIN Scan، SYN Scan، XMAS Scan و Null Scan با استفاده از ابزارهایی مانند Nmap قابل انجام هستند.

انواع Flag های TCP عبارتند از SYN، FIN، RST، PUSH، URG و ACK که هر کدام وظیفه خاصی بر عهده دارند.

برای آنالیز اسکن در شبکه می توان از فیلتر های مخصوص Flag های TCP استفاده نمود:

tcp.flags == Hex Flags

در دستور بالا به جای Hex Flag شما می‌توانید از مقدار Hex آن استفاده نمایید.

0x00 NULL
0x01 FIN
0x02 SYN
0x04 RST
0x08 PSH
0x10 ACK
0x020 URG
tcp.flags == 0x01

برای شناسایی حمله ARP Poisoning از فیلتر زیر استفاده می کنیم:

arp.duplicate-address-detected