آموزش CEH (هکر کلاه سفید): هکرها به چه ابزارهای شنودکننده‌ای دسترسی دارند؟

ابزارهای مختلفی برای شنود وجود دارد که برخی از آن‌ها رایگان و برخی دیگر ممکن است تا هزار دلار قیمت داشته باشند. ابزارهایی شبیه به Wireshark هر آن چیزی که یک هکر یا کارشناس امنیتی به آن نیاز دارند را در اختیارشان قرار می‌دهند، اما ابزارهای شنودکننده دیگری نیز در دسترس هستند. CACE Pilot و OmniPeek در گروه ابزارهای شنود کلی طبقه‌بندی می‌شوند، در حالی که The Dude Sniffer، Ace Password Sniffer و Bit Mother Email Sniffer به هکرها اجازه می‌دهند روی نوع خاصی از ترافیک متمرکز شوند.

برای مطالعه قسمت قبل آموزش رایگان **دوره CEH اینجا** کلیک کنید.

ARP تنها روش هکرها برای جعل نیست. دو روش دیگر جعل که به شکل گسترده از سوی هکرها استفاده می‌شود جعل سامانه نام دامنه و مک است. جعل مک می‌تواند برای دور زدن امنیت پورت استفاده شود. بسیاری از سازمان‌ها از رویکرد ایمن‌سازی پورت استفاده می‌کنند و تنها به مک‌آدرس‌های مورد تایید اجازه دسترسی به پورت‌های خاصی را می‌دهند. هنگامی که از رویکرد امنیت پورت استفاده می‌کنید به سادگی قادر به تخصیص یک یا چند مک‌آدرس به یک پورت ایمن هستید. اگر یک پورت به عنوان پروت ایمن پیکربندی شده باشد و مک آدرس معتبر نباشد، یک یک نقض امنیتی رخ می‌دهد. مهاجم می‌تواند از رویکرد جعل مک استفاده کرده، مانع بروز نقض امینی شده و به شکل غیر قانونی به ترافیک دست پیدا کند. جعل مک می‌تواند با تغییر تنظیم کامپیوتر از طریق رجیستری، یا اجرای یک فرمان در شل لینوکس استفاده کرده یا در حالت کلی‌تر از ابزارهایی شبیه به SMAC استفاده کند. SMAC ابزاری است که برای جعل مک استفاده شده و به یک مهاجم اجازه می‌دهد تا یک مک آدرس را جعل کند. مهاجم می‌تواند یک مک آدرس به مقادیر مختلفی تغییر دهد. برای دانلود ابزار SMAC به آدرس زیر مراجعه کنید.

http://www.klcconsulting.net/smac

سامانه نام دامنه مستعد جعل است. با جعل سامانه نام دامنه، به سرور سامانه نام دامنه اطلاعاتی درباره نام سرور که به ظاهر معتبر و قانونی است ارائه می‌کند. شکل زیر ابزار Cain and Abel که برای اجرای یک حمله سامانه نام دامنه روی یک سایت بانکی تنظیم شده است را نشان می‌دهد.

بردار حمله فوق می‌تواند کاربران را به سمت یک سایتی که به دنبال آن نیستند هدایت کرده، مسیریابی دوباره ایمیل را هموار کرده یا یا هر نوع تغییر مسیری که مدنظر هکرها را است انجام دهد. نام دیگر این حمله مسموم‌سازی سامانه نام دامنه است. WinDNSSpoof یکی از ابزارهای کاربردی در ارتباط با این حمله است. این ابزار شناسه سامانه نام دامنه را جعل کرده و مخصوص سیستم‌عامل ویندوز طراحی شده است. ابزار فوق از آدرس زیر قابل

دریافت است.

http://www.securiteam.com/tools/6X0041P5QW.html

برای مقابله با این حمله تکنیک‌های مختلفی به شرح زیر انجام می‌شود:

■ تبدیل تمامی محاوره‌های سامانه نام دامنه به شیوه محلی

■ پیاده‌سازی DNSSEC.

■ مسدودسازی درخواست‌های سامانه نام دامنه از طریق سرورهای سرورهای DNS خارجی.

■ پیاده‌سازی الگوهای دفاع در عمق با استفاده از سامانه‌های IDS برای شناسایی حملات و به‌کارگیری دیوارهای آتش با هدف ایجاد محدودیت در ارتباط با جست‌جوهای خارجی.

ابزارهایی برای شنود

ابزارهای مختلفی برای شنود وجود دارد که برخی از آن‌ها رایگان و برخی دیگر ممکن است تا هزار دلار قیمت داشته باشند. یکی از بهترین ابزارها در این زمینه Wireshark است.

Wireshark

ابزارهای شنودی شبیه به Wireshark می‌توانند نماهای مختلفی از ترافیک ضبط شده را نشان دهند. اطلاعات به سه شکل خلاصه، جزییات و کدهای هگزا نشان داده می‌شوند. شکل زیر سه نمای مختلف موجود در این ابزار را نشان می‌دهد.

پنجره بالایی خلاصه وضعیت را نشان می‌دهد و در هر خط اطلاعات مربوط به بسته را نشان می‌دهد. خط های‌لایت شده آدرس‌های مک منبع و مقصد، پروتکل ضبط شده، ARP و آدرس‌های آی‌پی منبع و مقصد را نشان می‌دهد. پنجره وسط جزئیات را نشان می‌دهد. در این پنجره محتوای بسته‌های های‌لایت شده را مشاهده می‌کنید. دقت کنید یک علامت مقابل فیلدها وجود دارد. با کلیک روی علامت ضمن مشاهده جزئیات به اطلاعات بیشتری دسترسی خواهید داشت. صفحه نمایش سوم نمایشگر اطلاعات به صورت هگز است.

صفحه نمایش هگزا نشان‌دهنده داده‌های خام است. سه بخش در پنل هگزا وجود دارد. اعداد سمت چپ نمایانگر افست اولین بایت افست را در قالب هگزا نشان می‌دهند. بخش میانی مقدار واقعی هگز هر بخش از سرآیند و داده‌ها را نشان می‌دهد. زمانی که با این بخش از رابط Wireshark کار می‌کنید با اعدادی در مبنای هگزا سروکار دارید. اگر در تبدیل مقادیر هگزا به مقادیر دودویی مشکل دارید، باید سطح دانش خود در این زمینه را بهبود بخشید. این‌کار به شما کمک می‌کند به سرعت بسته‌ها را تحلیل کرده و ناهنجاری‌های نقطه‌ای و ترافیک مخرب را تشخیص دهید. جدول زیر مقادیر هگزا و معادل باینری آن‌ها را نشان می‌دهند.

Hex	Binary	Decimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5

6	0110	6
7	0111	7
8	1000	8
9	1001	9
A	1010	10
B	1011	11
C	1100	12
D	1101	13
E	1110	14
F	1111	15

در سمت راست پنجره ترجمه مقادیر هگزا شنود شده در قالب اسکی نشان داده شده است. در این مکان می‌توانید به جست‌وجوی نام‌های کاربری و گذرواژه‌ها بپردازید.

نکته: رمزگذاري يكي از بهترين روش‌ها براي جلوگيري از شنود اطلاعات توسط افرادی است که به دنبال جمع‌آوری اطلاعات مهم در ارتباط با افراد هستند.

یکی از ویژگی‌های مهم ابزارهای شنودگری شبیه به Wireshark قابلیت تنظیم فیلترها برای مشاهده انواع خاصی از ترافیک است. فیلترها را می‌توان به یکی از دو روش تعریف کرد:

■ Capture filters: زمانی که می‌دانید به دنبال چه چیزی هستید باید از فیلتر فوق استفاده کنید. این فیلترها به شما اجازه می‌دهند نوع ترافیک ضبط شده را از پیش تعریف کنید. به عنوان مثال، می‌توانید فیلتر ضبط را تنظیم کنید تا فقط ترافیک HTTP را ضبط کنید.

■ Display filters: پس از ضبط ترافیک استفاده می‌شود. با توجه به این‌که ممکن است انواع مختلفی از ترافیک را ضبط کرده باشید، فیتلرهای فوق اجازه می‌دهند تنها ترافیک مربوط به بسته‌های ARP را مشاهده کنید. از جمله این فیلترها به موارد زیر می‌توان اشاره کرد:

■ فیلتر کردن بر مبنای آدرس آی‌پی (به‌طور مثال ip.addr == 192.168.123.1)

■ فیلتر کردن بر مبنای چند آدرس آی‌پی (به‌طور مثال ip.addr == 192.168.123.1 یا ip.addr == 192.168.123.2)

■ فیلتر بر مبنای پروتکل‌هایی شبیه به HTTP ، ICMP ، ARP یا BGP

■ فیلتر بر مبنای پورت (به‌طور مثال ، tcp.port == 23)

■ فیلتر بر مبنای فعالیت‌ها (به عنوان مثال ، tcp.flags.reset == 1)

اگرچه Wireshark برای مهاجمان ابزاری ایده‌آل برای شنود ترافیک شبکه است، اما به همان نسبت برای کارشناسان امنیتی نیز مفید است. ابزارهای شنود شما را قادر می‌سازند تا وضعیت آماری شبکه را به دقت زیر نظر داشته باشید و هرگونه حمله سیلابی مبتنی بر مک یا جعل ARP را کشف کنید. همچنین، می‌توانید از فیلترها برای محدود کردن مشاهده مقدار داده‌های ضبط شده استفاده کرده و روی نوع خاصی از ترافیک متمرکز شوید. تابع follow

TCO stream در نرم‌افزار Wireshark روش خوبی برای بازسازی دوباره ترافیک است. برای اطلاعات بیشتری در ارتباط با فیلترهای ابزار فوق به آدرس زیر مراجعه کنید.

http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf

اگر تمایلی به رابط گرافیکی ابزار فوق ندارید، نسخه خط فرمان این ابزار به‌نام TShark نیز در زمان نصب Wireshark نصب می‌شود تا کاربران بتوانند از محیط خط فرمان استفاده کنند.

سایر ابزارهای شنود

اگرچه ابزارهایی شبیه به Wireshark هر آن چیزی که یک هکر یا کارشناس امنیتی به آن نیاز دارند را در اختیارشان قرار می‌دهند، اما ابزارهای شنودکننده دیگری نیز در دسترس هستند. CACE Pilot و OmniPeek در گروه ابزارهای شنود کلی طبقه‌بندی می‌شوند، در حالی که The Dude Sniffer، Ace Password Sniffer و Bit Mother Email Sniffer به هکرها اجازه می‌دهند روی نوع خاصی از ترافیک متمرکز شوند. ابزارهای دیگری نیز وجود دارند که عملکردهای قابل قبولی ارائه می‌کنند. از جمله این ابزارها به موارد زیر می‌توان اشاره کرد:

■ RSA NetWitness: قابلیت ضبط ترافیک زنده بازرسی عمیق بسته‌ها را فراهم می‌کند.

■ OmniPeek: یک ابزار شنودکننده تجاری است که مجهز به رابط کاربری گرافیکی بوده و در سیستم‌عامل ویندوز قابل استفاده است.

■ Dsniff: ابزار فوق بخشی از یک مجموعه کارآمدتر از ابزارهایی است که برای ممیزی و هک شبکه استفاده می‌شود. این مجموعه شامل Urlsnarf ، Msgsnarf ، Mailsnarf ، Filesnarf ، Dnniff و Webspy است. این ابزارها به مهاجم این امکان را می‌دهند تا به شکل غیر فعال ترافیک خاصی از داده‌ها همچون گذرواژه‌ها، ایمیل‌ها، فایل‌ها و ترافیک وب را رصد کنند. ابزار فوق از آدرس زیر قابل دریافت است.

/http://www.monkey.org/~dugsong/dsniff

■ TCPdump: یکی از پر استفاده‌ترین و کاربردترین ابزارهای تحلیل‌کننده/ و شنودکننده مخصوص لینوکس است. TCPdump یک ابزار خط فرمان است که برای نمایش اطلاعات سرآیند استفاده می‌شود. ابزار فوق از آدرس http://www.tcpdump.org قابل دریافت است.

■ WinDump: بخشی از پلتفرم ویندوزی TCPdump است که در گذشته به عنوان یکی از پرکاربردترین ابزارهای در زمینه شنود و تحلیل شبکه در سیستم‌عامل یونیکس استفاده می‌شد. این ابزار شبیه به TCPdump دارای یک رابط کاربری خط فرمان است که اطلاعات سرآیند بسته‌ها را نشان می‌دهد. ابزار فوق از آدرس زیر قابل دریافت است.

http://www.winpcap.org/windump

شنود و اقدامات متقابل برای مقابله با شنود اطلاعات

شنود کردن یکی از قدرتمندترین راهکارهای در دسترس هکرها است و همان‌گونه که مشاهده کردید، ابزارهای مختلفی برای این منظور طراحی شده است. با این‌حال، کارشناسان شبکه می‌توانند اقدامات متقابلی برای مقابله با این پدیده انجام دهند. به‌طور مثال، امکان پیاده‌سازی ورودی‌های ایستای ARP وجود دارد، اما برای انجام این‌کار باید دستگاه‌های متصل به شبکه زیادی را پیکربندی کنید که به‌کارگیری روش فوق در شبکه‌های بزرگ را با دشواری همراه می‌کند. راه حل کارآمدتر در ایمن‌سازی پورت‌ها نهفته است. رویکرد ایمن‌سازی پورت را می‌توان از برنامه‌ریزی هر سوییچ انجام داد و به سوییچ اعلام کرد چه آدرس‌های مجاز به ارسال یا دریافت بوده و قادر به اتصال به پورت‌ها هستند. اگر از دستگاه‌های سیسکو استفاده می‌کنید، این فناوری با نام DAI سرنام Dynamic ARP Inspection شناخته می‌شود. DAI یک ویژگی امنیتی ارائه شده از سوی سیسکو است که امنیت و اعتبار ترافیک ARP را تأیید می‌کند. DAI با بازرسی، ضبط و دور انداختن بسته‌های ARP اجازه نمی‌دهد اتصالات نامعتبر مبتنی بر IP-to-MAC به راحتی در شبکه فعال باشند. این قابلیت از شبکه در برابر برخی حملات همچون مرد میانی محافظت می‌کند. یکی

دیگر از فناوری‌های مفید در این زمینه IP Source Guard است. یک ویژگی امنیتی که ترافیک آی‌پی را روی درگاه‌های غیرقابل اعتماد لایه 2 محدود می‌کند. این ویژگی هنگامی که میزبان سعی در جعل و استفاده از آدرس آی‌پی میزبان دیگری دارد مانع از جعل آدرس آی‌پی می‌شود. IP Source Guard می‌تواند به ویژه در برابر حملاتی همچون مسموم‌سازی و جعل سامانه نام دامنه مفید باشد. این امکان وجود دارد که با استفاده از رویکرد DNS Security Extensions (DNSSEC) سرنام از شبکه در برابر حملات دفاع کرد. تکنیک فوق تمامی پاسخ‌های سامانه نام دامنه را به شکل دیجیتالی امضا می‌کند تا اعتبار آن‌ها را تضمین کند. در RFC 4035 اطلاعات جامعی در ارتباط با این مکانیزم دفاعی وجود دارد.

نکته: برای آزمون CEH لازم است به خوبی درباره بازرسی پویا پروتکل ARP که یکی از راه‌های موثر در مسموم‌سازی ARP است اطلاعات کسب کنید.

در برخی موارد امکان به‌کارگیری عملی این راه‌حل‌ها در شبکه‌های بزرگ سازمانی امکان‌پذیر نیست، زیرا یک فرآیند کاملا وقت‌گیر است. آیا دفاع مقبول‌تری وجود دارد؟ بله، دو راهکاری که پیش‌تر به آن‌ها اشاره کردیم، یعنی port security و DHCP Snooping DHCP مجموعه‌ای از تکنیک‌های موثر بر ایمن‌سازی زیرساخت‌های موجود DHCP را ارائه کرده، در حالی که port security راهکارهایی برای نظارت دقیق‌تر بر زیرساخت لایه 2 ارائه می‌کند. در صورت عدم استفاده از راهکارهای فوق احتمال پیاده‌سازی و به‌کارگیری سرور DHCP سرکش وجود دارد. به عنوان یک کارشناس امنیتی باید دسترسی فیزیکی به کلیه سوئیچ‌ها و دستگاه‌های شبکه را محدود کرده و رمزگذاری را فراموش نکنید. IPsec، شبکه‌های خصوصی مجازی، SSL و زیرساخت‌های کلید عمومی (PKI) همه می‌توانند شنود ترافیک را برای هکرها دشوارتر کنند. ابزارهای لینوکسی شبیه به Arpwatch نیز مفید هستند. آرپاچ وضعیت آدرس آی‌پی و اترنت را بررسی کرده و تغییرات غیر معمول را گزارش می‌کند. سرانجام، روش‌هایی نیز برای تشخیص شنود توسط هکرها وجود دارد. شنود باعث می‌شود تا عملکرد سیستمها در وضعیت بی قاعده قرار گیرد. با استفاده از تکنیک‌های مختلفی می‌توان وضعیت بی قاعده در سیستم‌ها را تشخیص داد. از مهم‌ترین این تکنیک‌ها به موارد زیر می‌توان اشاره کرد:

■ بهرطور پیش‌فرض، Wireshark جست‌وجوی معکوس DNS را انجام می‌دهد. با تمرکز بر این موضوع که چه دستگاه‌هایی حجم بسیار زیادی از ترافیک جست‌وجوی معموس DNS را در شبکه وارد می‌کنند، احتمال شناسایی یک شنودکننده فعال وجود دارد.

■ دستگاهی که در حالت بی قاعده قرار می‌گیرد به‌طور معمول به یک پینگ با آدرس آی‌پی درست و مک آدرس اشتباه پاسخ می‌دهد. این مشکل از این جهت رخ می‌دهد که کارت شبکه مک آدرس اشتباه را رد نمی‌کند.

■ از ابزارهایی مانند Arpwatch ، Capsa Network Analyzer و PromqryUI می‌توان برای نظارت بر بسته‌های عجیب و غریب و غیر عادی استفاده کرد.

نکته: اطمینان حاصل کنید درباره راه‌هایی که اجازه می‌دهند مانع بروز شنود فعال شوید، اطلاعات لازم را کسب کرده‌اید. برنامه‌هایی مانند آرپاچ، هر دو جفت آدرس اترنت/ آی‌پی را رهگیری می‌کنند و می‌توانند تغییرات غیر معمول را گزارش دهند. همچنین می‌توانید از ورودی‌های ایستای ARP استفاده کرده، به IPv6 مهاجرت کنید (که این مورد در زمان نگارش این مقاله در دسترس شرکت‌های ایرانی نیست)، از رمزگذاری استفاده کنید یا حتا از سامانه‌های تشخیص نفوذ برای هشداردهی در ارتباط با تغییر آدرس مک برخی از دستگاه‌های خاص استفاده کنید.

در شماره آینده مبحث فوق را ادامه می‌دهیم.

برای مطالعه رایگان تمام بخش‌های **دوره CEH** روی لینک زیر کلیک کنید:

آموزش رایگان دوره CEH

تاریخ انتشار:

19 خرداد 1399

نشانی منبع:
https://www.shabakeh-mag.com/security/16937/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D9%87%DA%A9%D8%B1%D9%87%D8%A7-%D8%A8%D9%87-%DA%86%D9%87-%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1%D9%87%D8%A7%DB%8C-%D8%B4%D9%86%D9%88%D8%AF%DA%A9%D9%86%D9%86%D8%AF%D9%87%E2%80%8C%D8%A7%DB%8C-%D8%AF%D8%B3%D8%AA%D8%B1%D8%B3%DB%8C-%D8%AF%D8%A7%D8%B1%D9%86%D8%AF%D8%9F