آموزش رایگان دوره نتورک‌پلاس (Network+) (بخش 52)

در شماره گذشته آموزش نتورک‌پلاس با انواع مختلف شبکه‌های محلی مجازی و مباحث مرتبط با این شبکه‌ها آشنا شدیم. در ادامه مبحث جدیدی تحت عنوان مدیریت ریسک‌ها در شبکه و انواع مختلف ریسک‌ها و بردارهای حمله را بررسی کردیم. در این شماره مبحث فوق را ادامه خواهیم داد.

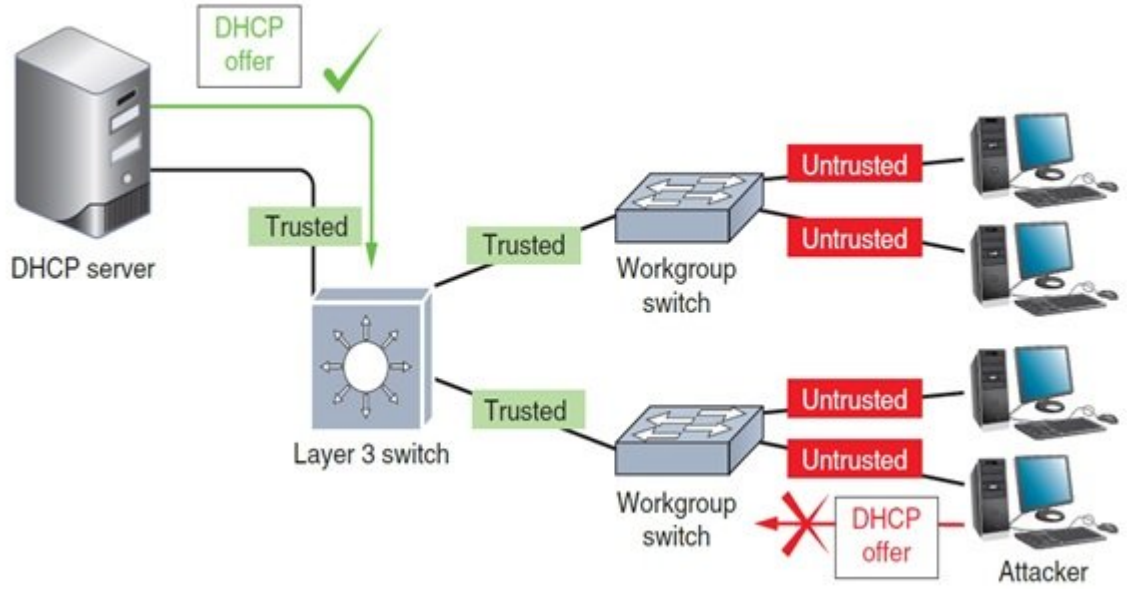
برای مطالعه بخش پنجاه و یکم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

• **مسموم‌سازی پروتکل تفکیک آدرس (ARP)** - همانند کش‌های DNS، جداول ARP را نیز می‌توان تغییر داد. ARP پروتکل IPv4 است و برای شناسایی آدرس MAC یک گره در شبکه محلی استفاده می‌شود. اطلاعات این پروتکل در پایگاه داده‌ای به نام جدول ARP یا کش ARP ذخیره می‌شود که آدرس‌های آی‌پی را به آدرس MAC در یک شبکه محلی ترسیم می‌کند. با این وجود، ARP فاقد مکانیزم احراز هویت است و بنابراین آسیب‌پذیری بالایی در برابر حملات دارد. هنگامی که مهاجمان از پاسخ‌های جعلی ARP برای تغییر جدول‌های ARP در یک شبکه استفاده می کنند، حمله مسموم‌سازی ARP یا ARP spoofing رخ می‌دهد. آسیب‌پذیری ARP به عنوان بستری برای پیاده‌سازی حملات دیگری همچون DoS یا MitM استفاده می‌شود.

• **حمله مرد میانی (MitM)** - حمله مرد میانی به معنای قطع کردن فرآیند انتقال بوده و می‌تواند به شکل‌های مختلفی پیاده‌سازی شود. در همه اشکال، یک هکر می‌تواند فرآیند انتقال را به مسیر دیگری هدایت کرده و داده‌ها را ضبط کند. به عبارت ساده‌تر، هکر خود را میان دو دستگاهی قرار می‌دهد که در حال تبادل اطلاعات با یکدیگر هستند و از این طریق به شنود اطلاعات می‌پردازد، بدون آن‌که سامانه قربانی متوجه این موضوع شود. به‌طور مثال، فرض کنید سیستم A در نظر دارد برای سیستم B پیامی را ارسال کند. در این حالت هکر به سیستم A اعلام می‌دارد که سیستم B است و به سیستم B اعلام می‌دارد که من سیستم A هستم. در این حالت هر دو سیستم اطلاعات خود را برای هکر ارسال می‌کنند.

• **حمله rogue DHCP server**- دستگاه‌های درون یک شبکه به شکل پیش‌فرض و بر پایه یک ارتباط دو طرفه با یکدیگر ارتباط برقرار می‌کنند، اما وجود یک رخنه به هکرها اجازه می‌دهد به کل شبکه دسترسی داشته باشند. به‌طور مثال، پیام‌های DHCP اجازه دارند آزادانه از طریق پورت‌ها روی سوئیچ‌ها انتقال پیدا کنند تا کلاینت‌ها بتوانند به درستی فعالیت‌های خود را انجام دهند. اما زمانی که یک سرور جعلی DHCP روی یک دستگاه کلاینت اجرا شود، این پتانسیل را دارد تا یک حمله MitM را از طریق پیکربندی آدرس آی‌پی هکر به عنوان یک گیت‌وی پیش‌فرض عادی پیاده‌سازی کند. هکر می‌تواند آدرس آی‌پی خود را به عنوان سرور DNS پیشنهاد داده و کاربر را به سمت سایت‌های

جعلی هدایت کند. پیام‌های DHCP باید توسط یک ویژگی امنیتی روی سوئیچ‌ها به نام snooping DHCP بررسی شوند تا هر پورت سوئیچ متصل به دستگاه کلاینتی اجازه نداشته باشند پیام‌های DHCP را انتقال دهد، در این حالت پیام‌ها از طریق سرور DHCP قابل اعتماد ارسال می‌شوند در شکل زیر سوییچ لایه 3 را مشاهده می‌کنید که از طریق یک سرور DHCP قابل اعتماد با سوییچ‌های ایستگاه کاری در ارتباط است.



در سمت راست تصویر یک DHCP را مشاهده می‌کنید که از سوی یک کلاینت غیرقابل اعتماد ایجاد شده است. بهترین راهکار مقابله با این تهدید استفاده از مکانیزم snooping DHCP و پیکربندی سوییچ با اجرای دستور ip dhcp snooping است.

• **حمله (deauthentication)**- زمانی‌که یک کلاینت وای‌فای به شکل معتبر به یک نقطه دسترسی بی‌سیم متصل است، AP یا کلاینت می‌توانند یک فریم deauthentication به معنای پایان یک نشست را برای یکدیگر ارسال کنند. این پیام به دلایل مختلفی همچون عدم فعالیت، دور شدن کلاینت از منطقه تحت پوشش، وجود کلاینت‌های بیش از اندازه برای AP یا دلایل نامشخصی ارسال می‌شود. این فریم‌ها رمزگذاری نمی‌شوند و به راحتی قابل جعل هستند. در حمله deauthentication، مهاجم فریم‌های جعلی deauthentication را برای AP، کلاینت یا هر دو (یا به صورت پخشی در کل شبکه بی‌سیم) ارسال می‌کند تا کنترل فرآیند deauthentication را به دست گرفته و ارتباط یک یا چند کلاینت از شبکه بی‌سیم را قطع کند.

• **پروتکل‌ها و سرویس‌های غیرایمن (insecure protocols and services)**- برخی از پروتکل‌های TCP / IP به‌طور ذاتی ناامن هستند. به‌طور مثال، آدرس‌های آی‌پی را می‌توان جعل کرد، فعالیت checksums را مختل کرد، UDP بدون احراز هویت کار می‌کند و TCP به یک احراز هویت ضعیف بسنده می‌کند. FTP به آسیب‌پذیر بودن معروف است. FTP Bounce یک اکسپلویت معروف این پروتکل است. از پروتکل‌های ناامن دیگر می‌توان به HTTP (جایگزینی با HTTPS)، Telnet با SSL / TLS (به‌کارگیری همراه با SLIP، IPsec) (جایگزینی با TFTP (PPP (جایگزینی با SNMPv1، SFTP و SNMPv2 (جایگزینی با SNMPv3) اشاره کرد.

• **درب‌های پشتی (back doors)**- نرم‌افزارها ممکن است درب‌های پشتی داشته باشند که نقص امنیتی است که به کاربران غیر مجاز امکان دسترسی به یک سیستم را می‌دهد. به همین دلیل مدیران شبکه باید به‌طور منظم نرم‌افزار را به‌روزرسانی کنند تا هکرها نتوانند از این رخنه‌ها استفاده کنند.

ریسک‌های بدافزاری

بدافزار (Malware) به هر برنامه یا قطعه کد طراحی شده برای نفوذ به یک سیستم یا منابع شبکه دلالت دارد. در این گروه ویروس‌ها، اسب‌های تروجان، کرم‌ها، روبات‌ها و باج‌افزارها قرار دارند. با مراجعه به آدرس

symantec.com/security_response/landing/threats.jsp فهرستی از بدافزارهای روز که شرکت سیمانتک آماده کرده است را مشاهده می‌کنید. در این‌جا به چند مورد از این موارد اشاره می‌کنیم.

• **ویروس** (virus)- برنامه‌ای است که می‌تواند خود را تکثیر کرده و کامپیوترهای زیادی که به شبکه‌ای متصل شده‌اند یا دستگاه‌هایی که به یک کامپیوتر آلوده وصل می‌شوند را قربانی کرده و به فایل‌ها یا سیستم‌ها آسیب وارد کند.

• **اسب تروجان** (Trojan) - برنامه‌ای است که در ظاهر خود را یک برنامه مفید نشان داده، اما در عمل به سیستم شما آسیب وارد می‌کند. از آنجایی که اسب‌های تروجان خود را تکرار نمی‌کنند، آن‌ها ویروس نیستند. یک نمونه از یک اسب تروجان یک فایل اجرایی است که فردی در قالب یک بازی و از طریق اینترنت برای شما می‌فرستد و امیدوار است شما آن‌را اجرا کنید، در حالی که برنامه ممکن است اطلاعات روی هارددیسک شما را پاک کرده یا ایمیل‌های هرزی را برای کاربرانی که آدرس آن‌ها درون دفترچه آدرس‌های برنامه ایمیلی قرار دارد ارسال کند.

• **کرم** (worm)- برنامه‌ای است که مستقل از سایر نرم‌افزارها اجرا شده و ممکن است توسط هر نوع رسانه انتقالی همچون فایل‌های ضمیمه شده به یک ایمیل کامپیوترها را آلوده کنند. عملکرد کرم‌ها متفاوت از ویروس‌ها است و برای انتقال ویروس‌ها از آن‌ها استفاده می‌شود. خصیصه بارز کرم‌ها در سرعت بالای آلوده‌سازی سامانه‌ها است.

• **بات** (bot) – بات که مخفف روبات (robot) است فرآیندی است که به‌طور خودکار اجرا می‌شود، بدون آن‌که فردی بر روند شروع یا توقف آن نظارت داشته باشد. روبات‌ها می‌توانند سودمند یا مخرب باشند. روبات‌ها نیازی ندارند تا کاربر با آن‌ها تعامل داشته باشد. در عوض، بات‌ها سامانه قربانی را به یک سرور مرکزی متصل می‌کنند (به نام سرور کنترل و فرمان‌دهی (C & C) معروف است) تا دستگاه قربانی به شبکه بات‌ها (botnet) متصل شده و دستورات را اجرا کند. بات‌ها می‌توانند برای آسیب رساندن یا خراب کردن داده‌ها یا فایل‌های سیستمی، راه‌اندازی حملات DoS یا باز کردن درب‌های پشتی روی سامانه‌ها استفاده شوند.

باج‌افزار (ransomware)- برنامه‌ای است که اطلاعات یا سیستم کامپیوتری کاربران را قفل کرده و مادامی که باج مربوطه از سوی کاربر پرداخت نشود، فایل‌ها را غیرقابل دسترس می‌کند. در اغلب موارد، فرآیند رمزنگاری داده‌ها روی کامپیوتر و هر دستگاهی که به کامپیوتر متصل شود انجام شده و حتا احتمال رمزگذاری فایل‌هایی که روی فضای ابری ذخیره‌سازی شده‌اند نیز وجود دارد. برای اطلاعات بیشتر در خصوص باج‌افزارها به مقاله "**ه[ک‌های ترسناک باج‌افزارها رو به افزایش است](#)**" مراجعه کنید.

برای اطلاعات بیشتر در خصوص انواع بدافزارها و ویژگی‌های مشترک آن‌ها همچون رمزگذاری، چندریختی بودن و.... پیشنهاد می‌کنم، به بخش **[امنیت سایت مجله شبکه](#)** مراجعه کنید.

ارزیابی امنیتی

قبل از آن‌که زمان و پول خود را صرف امنیت شبکه کنید، ابتدا وضعیت ریسک‌های امنیتی شبکه را بررسی کنید. به‌طور مثال تاثیر از دست دادن یا خراب شدن داده‌ها، برنامه‌ها یا عدم دسترسی به شبکه را بررسی کرده و پیامدهای بالقوه یک چنین شرایطی همچون زیان‌های مالی را بررسی کرده و بر مبنای این بررسی‌ها بودجه‌ای برای امنیت در نظر بگیرید. هر سازمانی باید مخاطرات امنیتی پیرامون زیرساخت‌های خود را بررسی کرده و بودجه‌ای برای این منظور تخصیص دهد. ارزیابی وضعیت باید حداقل سالیانه و ترجیحا سه ماهه انجام شود. ارزیابی‌ها همچنین باید پس از انجام تغییرات قابل توجه در شبکه دومرتبه انجام شوند. اگر بخش فناوری‌اطلاعات مهارت و زمان کافی برای انجام منظم ارزیابی‌ها را دارند، این‌کار به دور از سازمان نیز قابل انجام است. البته برخی از سازمان‌ها ترجیح می‌دهند از یک شرکت مشاوره امنیتی واجد شرایط برای ارزیابی امنیت شبکه خود استفاده کنند و نتیجه ممیزی امنیتی (security audit) را دریافت کنند.

ابزارهای پویش

برای اطمینان از اینکه تلاش‌های امنیتی شما سودبخش است، باید شبیه به یک هکر فکر کنید. به‌طور مثال، در طول ارزیابی وضعیت، شما ممکن است از برخی روش‌های مشابه با هکرها برای شناسایی رخنه‌های مستتر در معماری امنیتی خود استفاده کنید. در واقع، کارشناسان امنیتی معمولا حملات شبیه‌سازی شده به شبکه را برای تعیین نقاط

ضعف ترتیب می‌دهند. سه نوع رایج از این شبیه‌سازی‌ها به شرح زیر است:

پویش آسیب‌پذیری‌ها

• پویش یا ارزیابی آسیب‌پذیری‌ها (vulnerability scanning/ vulnerability assessment) - این روش برای شناسایی آسیب‌پذیری‌ها در یک شبکه و اغلب توسط کارکنان خود شرکت انجام می‌شود. پویش آسیب‌پذیری‌ها ممکن است اولین گام در شبیه‌سازی حملات یا پیاده‌سازی واقعی یک حمله باشد. در شبیه‌سازی حمله‌ها، دو نوع پویش با هدف شناسایی آسیب‌پذیرهای مرتبط با هویت تأیید شده و هویت تایید نشده انجام می‌شود.

• آزمایش نفوذ (penetration testing)- این شبیه‌سازی حمله با استفاده از ابزارهای مختلف برای پیدا کردن آسیب‌پذیری‌های شبکه و سپس تلاش برای بهره‌برداری از آسیب‌پذیری‌ها اجرا می‌شود.

• آزمایش تیم آبی تیم قرمز (red team-blue team exercise)- در طول این تمرین تیم قرمز حمله را انجام می‌دهد و تیم آبی تلاش می‌کند از شبکه دفاع کند. معمولا تیم قرمز یک مهاجم که یک مشاور یا سازمان امنیتی است را استخدام می‌کند و تیم آبی به سراغ تیم‌های فناوری‌اطلاعات، امنیت و سایر کارکنان خود می‌رود. در برخی موارد، تیم آبی هیچ هشداری در ارتباط با حمله قریب الوقوع به منظور ارزیابی و ایمن کردن مکانیزم دفاعی دریافت نمی‌کند. تیم قرمز نیز روی مبحث مهندسی اجتماعی متمرکز می‌شود.

هکرها و کارمندان شرکت در فرآیند شبیه‌سازی یک حمله یا پیاده‌سازی یک حمله به دنبال اهداف زیر هستند:

• شناسایی هر میزبان موجود و در دسترس

• خدمات، از جمله برنامه‌های در حال اجرا روی هر میزبان

• حمله به سیستم‌های عامل در حال اجرا روی هر میزبان

• بررسی وضعیت پورت‌های باز، بسته و فیلتر شده در هر میزبان

• بررسی وجود دیوارآتش و پیکربندی آن

• بررسی تنظیمات نرم‌افزارها

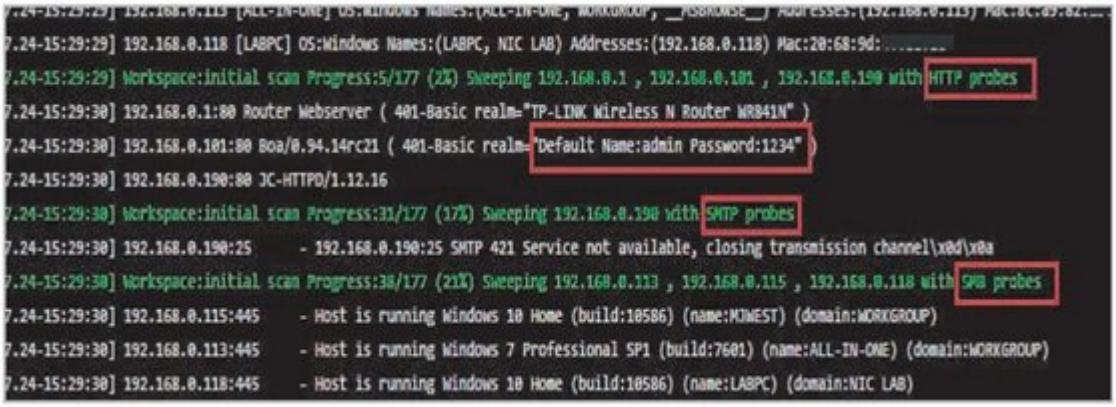
• بررسی اطلاعات رمزگذاری نشده و حساس

از جمله ابزارهای محبوبی که برای پویش شبکه‌ها استفاده می‌شوند به موارد زیر می‌توان اشاره کرد:

• Nmap- Nmap و نسخه گرافیکی آن (Zenmap) ابزاری است که برای پویش سریع شبکه‌های بزرگ و ارائه اطلاعاتی در مورد یک شبکه و میزبان آن طراحی شده است. **Nmap یک برنامه کاربردی است که یک دستگاه** را برای پورت‌های باز جست‌وجو می‌کند تا نشان دهد کدامیک از سرویس‌های دستگاه غیر ایمن هستند و در یک حمله ممکن است استفاده شوند.

• Nessus ابزاری است که Tenable Security آن‌را توسعه داده و برای شناسایی آسیب‌پذیری‌های پیچیده‌تر از آن استفاده می‌شود عملکرد این ابزار پیچیده‌تر از Nmap است. Nessus می‌تواند اطلاعات رمزگذاری نشده حساس همچون شماره کارت‌های اعتباری که روی میزبان‌های شبکه ذخیره شده‌اند را شناسایی کند.

• Metasploit - این ابزار تست نفوذ محبوب، دو رویکرد پویش‌های مرسوم و فناوری‌های ویژه شناسایی اکسپلویت‌ها را با یکدیگر ترکیب کرده و از آن‌ها برای شناسایی رخنه‌ها استفاده می‌کند. به‌طور مثال، شکل زیر وضعیت اسکن شبکه با ابزار Metasploit نشان می‌دهد. در شکل زیر ابزار فوق موفق به شناسایی نام کاربری و گذرواژه روتر SOHO در یک شبکه خانگی شده است.



Honeypots و Honeynets

تکنیک‌های حمله به‌طور مداوم در حال تکامل هستند. افرادی که به دنبال آشنایی بیشتر با مباحث آسیب‌پذیری‌ها، دفاع و حملات هستند به سراغ تکنیک‌های پیشرفته‌تری همچون ظرف عسل (honeypot) می‌روند. هانی‌پات‌ها محیطی را آماده می‌کنند که در ظاهر آسیب‌پذیر نشان می‌دهد و روی آن‌ها حتا محتوای حساس غیرواقعی همچون داده‌های مالی آپلود شده و از اسامی جذاب همچون نام یک سرور یا مکان ذخیره‌سازی اطلاعات محرمانه استفاده می‌شود. هنگامی که هکرها به honeypot دسترسی پیدا می‌کنند، مدیر شبکه می‌تواند از نرم‌افزار نظارت و ثبت گزارش برای پیگیری حرکات مزاحم استفاده کند. به این ترتیب، ممکن است سرپرست شبکه درباره آسیب‌پذیری‌ها نکات جدیدی یاد گرفته و روی میزبان‌های واقعی شبکه از آن‌ها استفاده کند. یک ظرف عسل باید از سیستم‌های امن جدا شود تا یک هکر باهوش نتواند به عنوان یک واسط از آن‌ها برای نفوذ به سایر سیستم‌ها یا پیاده‌سازی حملات استفاده کند. چندین honeypot ممکن است به یک شبکه عسل (honeynet) متصل شوند. نرم‌افزارهای KFSensor شرکت keyfocus.net)، Canary) شرکت (canary.tools) وHoneyd شرکت (honeyd.org) ابزارهای شاخص این حوزه هستند.

در شماره آینده آموزش **نتورک‌پلاس** مبحث ریسک‌ها را ادامه خواهیم کرد.

تاریخ انتشار:

27 اردیبهشت 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15352/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3-network-%D8%A8%D8%AE%D8%B4-52