مدیریت ریسک در شبکه، پیکربندی، اشکال‌زدایی و ایمن‌سازی VLANها

آموزش رایگان دوره نتورک‌پلاس (Network+) (بخش 51)

در شماره گذشته آموزش نتورک‌پلاس با مفهوم زیرشبکه‌ها درIPv6 و شبکه‌های محلی مجازی آشنا و به تشریح تکنیک ترانک و ارتباط آن با سوییچ‌ها پرداختیم. در این شماره مبحث فوق را ادامه داده و به سراغ مبحث مدیریت ریسک در شبکه‌ها خواهیم کرد.

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

انواع شبکه‌های محلی مجازی

آدرس‌های آی‌پی مختلف (خصوصی، عمومی، loopback و APIPA IP برای مقاصد متفاوتی استفاده می‌شوند. همین قاعده در مورد VLANها نیز صدق کرده و هریک برای مقاصد مختلفی استفاده می‌شوند. از رایج‌ترین شبکه‌های محلی خصوصی به موارد زیر می‌توان اشاره کرد:

• VLAN پیش‌فرض- به‌طور معمول به شکل از پیش پیکربندی شده روی یک سوییچ قرار گرفته و همه پورت‌های سوییچ را شامل می‌شود. سایر VLANها نیز ممکن است به شکل از پیش پیکربندی شده تنظیم شده باشند که البته این موضوع به دستگاه و تولیدکننده دستگاه بستگی دارد. VLAN پیش‌فرض را نمی‌توان تغییر داده یا حذف کرد. با این حال، امکان تخصیص دوباره پورت‌های پیش‌فرض VLAN به سایر VLANها امکان‌پذیر است.

• VLAN بومی - تمامی فریم‌های برچسب‌گذاری نشده از پورت‌های بدون برچسب را دریافت می‌کند. در حالت پیش‌فرض یکسان با VLAN پیش‌فرض است. با این حال، این مدل پیکربندی زمانی که ترافیک برچسب‌گذاری نشده باشد، اجازه انتقال داده‌ها در یک شبکه VLAN مدیریت شده را در اختیار دارد ریسک‌های امنیتی به وجود می‌آورد. برای محافظت از شبکه در برابر مخاطرات امنیتی وضعیت VLAN محلی باید به VLAN استفاده نشده تغییر پیدا کند تا ترافیک برچسب‌گذاری نشده باعث نشود امنیت شبکه به خطر افتد. برای انجام این کار روی یک سوئیچ سیسکو می‌توان فرمان switchport trunk native vlan را استفاده کرد.

• VLAN داده‌ها (یا VLAN کاربر) - ترافیک تولید شده توسط کاربر مانند ایمیل، مرور وب یا به‌روزرسانی پایگاه داده را حمل می‌کند.

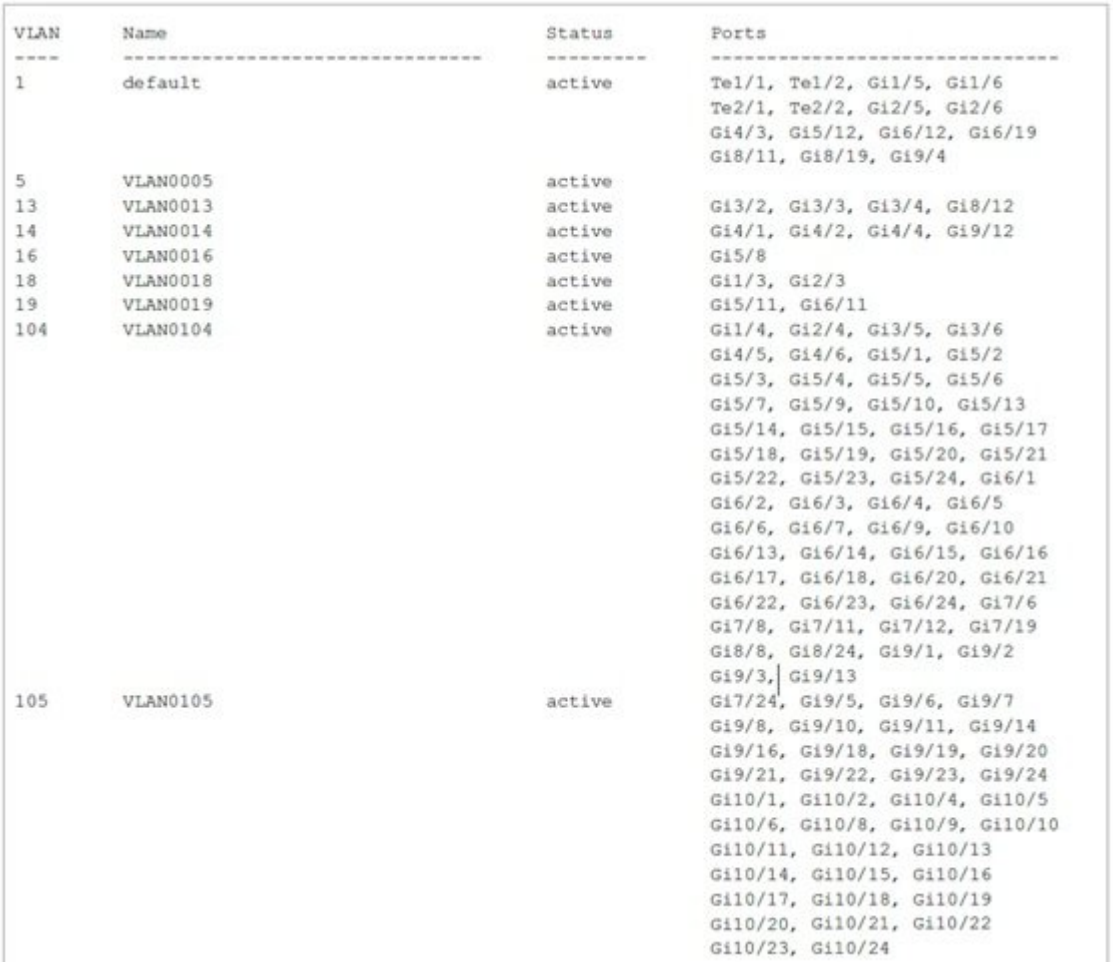
• VLAN مدیریتی - می‌تواند برای ارائه دسترسی مدیریتی به یک سوئیچ استفاده شود. به‌طور پیش‌فرض عملکرد این مدل شبیه به VLAN پیش‌فرض است؛ با این حال، یک خطر امنیتی به وجود می‌آورد و باید تغییر پیدا کند.

• VLAN صوتی - پشتیبانی از ترافیک VoIP که نیاز به پهنای باند بالا، مسیریابی انعطاف‌پذیر، اولویت‌بندی ترافیک و

تاخیر حداقلی دارد را ارائه کند.

پیکربندی VLANها

زمانی که یک VLAN را ایجاد کردید باید از طریق نرم‌افزار سوییچ آن‌را مدیریت کنید. شکل زیر نتیجه فرمان show vlan که روی یک سوییچ سازمانی سیسکو اجرا شده است را نشان می‌دهد. این فرمان فهرستی از VLANهای شناسایی شده با سوییچ را نشان می‌دهد. در شکل زیر 18 شبکه محلی خصوصی روی شبکه پیکربندی شده‌اند.



VLAN	Name	Status	Ports
1	default	active	Te1/1, Te1/2, Gi1/5, Gi1/6 Te2/1, Te2/2, Gi2/5, Gi2/6 Gi4/3, Gi5/12, Gi6/12, Gi6/19 Gi8/11, Gi8/19, Gi9/4
5	VLAN0005	active	
13	VLAN0013	active	Gi3/2, Gi3/3, Gi3/4, Gi8/12
14	VLAN0014	active	Gi4/1, Gi4/2, Gi4/4, Gi9/12
16	VLAN0016	active	Gi5/8
18	VLAN0018	active	Gi1/3, Gi2/3
19	VLAN0019	active	Gi5/11, Gi6/11
104	VLAN0104	active	Gi1/4, Gi2/4, Gi3/5, Gi3/6 Gi4/5, Gi4/6, Gi5/1, Gi5/2 Gi5/3, Gi5/4, Gi5/5, Gi5/6 Gi5/7, Gi5/9, Gi5/10, Gi5/13 Gi5/14, Gi5/15, Gi5/16, Gi5/17 Gi5/18, Gi5/19, Gi5/20, Gi5/21 Gi5/22, Gi5/23, Gi5/24, Gi6/1 Gi6/2, Gi6/3, Gi6/4, Gi6/5 Gi6/6, Gi6/7, Gi6/9, Gi6/10 Gi6/13, Gi6/14, Gi6/15, Gi6/16 Gi6/17, Gi6/18, Gi6/20, Gi6/21 Gi6/22, Gi6/23, Gi6/24, Gi7/6 Gi7/8, Gi7/11, Gi7/12, Gi7/19 Gi8/8, Gi8/24, Gi9/1, Gi9/2 Gi9/3, Gi9/13
105	VLAN0105	active	Gi7/24, Gi9/5, Gi9/6, Gi9/7 Gi9/8, Gi9/10, Gi9/11, Gi9/14 Gi9/16, Gi9/18, Gi9/19, Gi9/20 Gi9/21, Gi9/22, Gi9/23, Gi9/24 Gi10/1, Gi10/2, Gi10/4, Gi10/5 Gi10/6, Gi10/8, Gi10/9, Gi10/10 Gi10/11, Gi10/12, Gi10/13 Gi10/14, Gi10/15, Gi10/16 Gi10/17, Gi10/18, Gi10/19 Gi10/20, Gi10/21, Gi10/22 Gi10/23, Gi10/24

```
106      VLAN0106                         active          Gi6/8
107      VLAN0107                         active          Gi7/1, Gi7/2, Gi7/3, Gi7/4
                                                          Gi7/5, Gi7/7, Gi7/9, Gi7/10
                                                          Gi7/13, Gi7/14, Gi7/16, Gi7/17
                                                          Gi7/18, Gi7/21, Gi7/22, Gi8/1
                                                          Gi8/2, Gi8/3, Gi8/4, Gi8/5
                                                          Gi8/6, Gi8/7, Gi8/9, Gi8/10
                                                          Gi8/13, Gi8/14, Gi8/16, Gi8/17
                                                          Gi8/18, Gi8/21, Gi8/22
108      VLAN0108                         active          Gi7/15, Gi7/20, Gi7/23, Gi8/15
                                                          Gi8/20, Gi8/23
109      VLAN0109                         active
601      VLAN0601                         active
1002     fddi-default                     act/unsup
1003     token-ring-default               act/unsup
1004     fddinet-default                  act/unsup
1005     trnet-default                    act/unsup

VLAN  Type  SAID        MTU   Parent  RingNo  BridgeNo  Stp   BrdgMode  Trans1  Trans2
----  ----- ----------  ----- ------  ------  --------  ----  --------  ------  ------
1     enet  100001      1500  -       -       -         -     -         0       0
5     enet  100005      1500  -       -       -         -     -         0       0
13    enet  100013      1500  -       -       -         -     -         0       0
14    enet  100014      1500  -       -       -         -     -         0       0
16    enet  100016      1500  -       -       -         -     -         0       0
18    enet  100018      1500  -       -       -         -     -         0       0
19    enet  100019      1500  -       -       -         -     -         0       0
104   enet  100104      1500  -       -       -         -     -         0       0
105   enet  100105      1500  -       -       -         -     -         0       0
106   enet  100106      1500  -       -       -         -     -         0       0
107   enet  100107      1500  -       -       -         -     -         0       0
108   enet  100108      1500  -       -       -         -     -         0       0
109   enet  100109      1500  -       -       -         -     -         0       0
601   enet  100601      1500  -       -       -         -     -         0       0
1002  fddi  101002      1500  -       -       -         -     -         0       0
1003  tr    101003      1500  -       -       -         -     -         0       0
1004  fdnet 101004      1500  -       -       -         ieee  -         0       0
1005  trnet 101005      1500  -       -       -         ibm   -         v       0
```

نکته امتحانی: برای آزمون **نتورک‌پلاس** لازم است درباره پیکربندی VLANها و تحلیل آن‌ها اطلاعاتی داشته باشید. به همین دلیل پیشنهاد می‌کنم به مقاله **Displaying a switch VLAN configuration** رفته و دانش خود در این خصوص را افزایش دهید.

اشکال‌زدایی و ایمن‌سازی VLANها

خطاهای پیکربندی در شبکه‌های VLAN کاملا عادی است. فرمان show vlan که در پاراگراف قبل با آن آشنا شدید در تشخیص پیکربندی‌های اشتباه کمک فراوانی به شما می‌کند. از رایج ترین خطاهای پیکربندی می‌توان به تخصیص نادرست VLAN، وضعیت اشتباه پورت‌ها و VLAN ایزوله شده اشاره کرد. در بیشتر موارد هکرها سعی می‌کنند از VLANهای برچسب‌گذاری شده برای پیاده‌سازی یک حمله VLAN hopping استفاده کنند. برای اطلاعات بیشتر در خصوص دو بردار مرتبط با این حمله (double tagging و switch spoofing) به مقاله **VLAN hopping (virtual local area network hopping)** مراجعه کنید.

در چند شماره گذشته سعی کردیم تا حدودی مبحث تقسیم‌سازی شبکه‌ها، شبکه‌های محلی مجازی، زیرشبکه‌ها و زیرشبکه‌سازی را بررسی کنیم. بدیهی است برای آمادگی در آزمون **نتورک‌پلاس** باید از منابع بیشتری برای تسلط بر این مباحث و کار عملی استفاده کنید تا بدون مشکل در آزمون **نتورک‌پلاس** موفق شوید. اکنون اجازه دهید مبحث مدیریت ریسک در شبکه‌ها را آغاز کنیم.

مدیریت ریسک در شبکه‌ها

در چند شماره آینده اطلاعاتی در ارتباط با داده‌های شبکه و زیرساخت شبکه به دست خواهید آورد. در چند شماره آتی سعی می‌کنیم به شکل اجمالی نحوه مدیریت آسیب‌پذیری و محافظت از شبکه‌ها را به شما نشان دهیم.

ریسک‌های امنیتی

سازمان‌های مختلف به روش‌های مختلفی در معرض مخاطرات امنیتی قرار دارند. به‌طور مثال، اگر برای یک موسسه بزرگ مالی کار می‌کنید که به مشتریان خود اجازه می‌دهد وضعیت وام خود را به صورت آنلاین مشاهده کنند، باید مخاطرات مرتبط با نقص‌های داده‌ای را در نظر بگیرید. اگر شخصی دسترسی غیر مجاز به شبکه شما به دست آورد، همه اطلاعات شخصی مشتریان شما ممکن است فاش شوند. برای درک نحوه مدیریت امنیت شبکه، ابتدا باید بدانید که چگونه تهدیدهای پیرامون شبکه را تشخیص دهید. برای تشخیص این مسئله باید با اصطلاحات دنیای امنیت آشنا باشید. یک هکر، به معنی واقعی کلمه، فردی است که در زمینه کار با سخت‌افزارها و نرم‌افزارها استاد بوده و قادر است رخنه‌های امنیتی را شناسایی کرده و از آن‌ها سوء استفاده کند. امروزه واژه هکر برای توصیف افرادی استفاده می‌شود که غیرمجاز به سیستم یا شبکه یک سازمان نفوذ کرده و ممکن است خساراتی به بار آوردند. اصطلاح هک کردن نیز به معنای پیدا کردن راهی خلاقانه است که عملکرد یک دستگاه یا یک برنامه را از روند طبیعی خود خارج کرده و با دستکاری منابع مانع دسترسی کاربران به منابع شده یا منابع مالی یک شرکت را به تاراج ببرد. در دنیای امنیت هکرها به سه گروه زیر تقسیم می‌شوند.

هکر کلاه سفید (white hat hacker)- متخصصان امنیتی هستند که سازمان‌ها برای شناسایی تهدیدات و مخاطرات امنیتی و محافظت از منابع خود از وجود آن‌ها بهره می‌برند. این افراد یک هک اخلاقی انجام می‌دهند.

هکر کلاه سیاه (Black hat hacker) - این گروه افرادی هستند که از مهارت‌های خود برای دور زدن سامانه‌های امنیتی، آسیب رساندن به داده‌ها، سرقت داده‌ها یا نفوذ به حریم خصوصی کاربران استفاده می‌کنند.

هکر کلاه خاکستری (gray hat hacker)- این گروه از هکرها نیز از مهارت‌های خود به شیوه اخلاقی استفاده می‌کنند، اما این‌کار را به شیوه خاص خود انجام می‌دهند. به‌طور مثال یک هکر کلاه خاکستری سعی می‌کند گذرواژه ضعیف یک سازمان را شناسایی کرده و سپس گزارشی درباره نقص‌ها برای سازمان ارسال کند، بدون آن‌که از ضعف‌ها سوء استفاده کند.

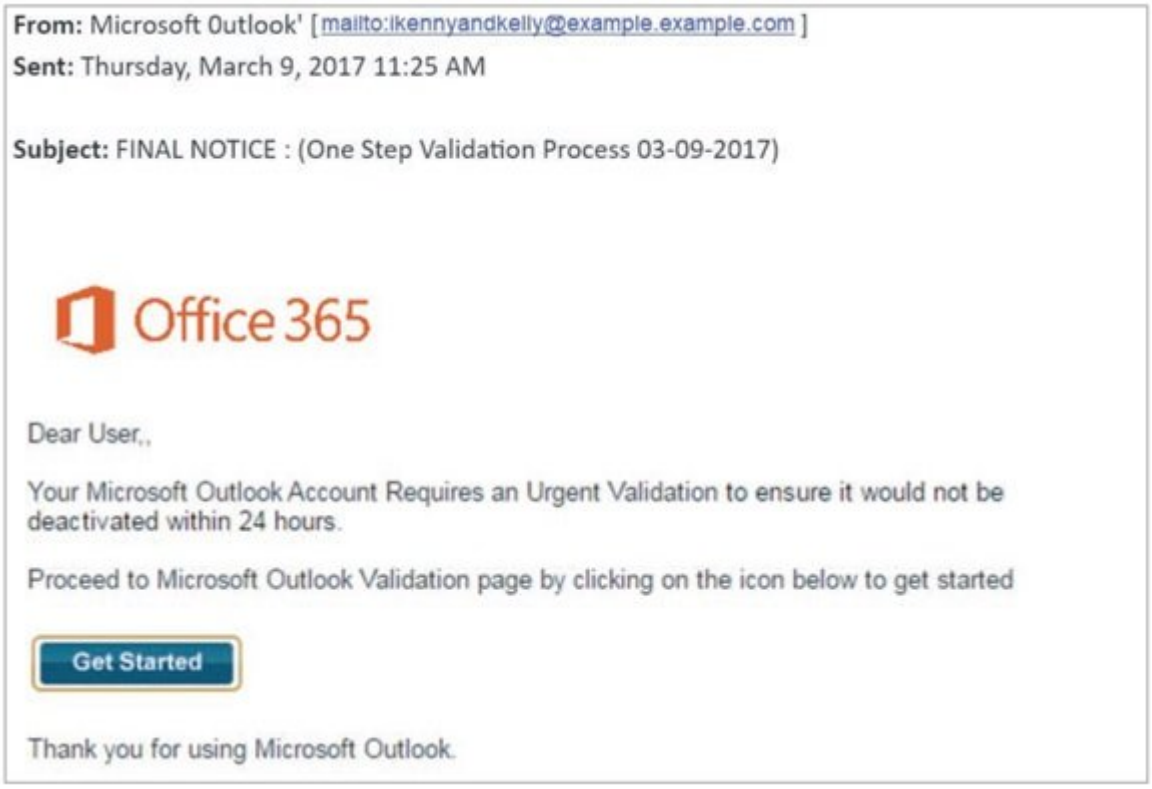
ضعف یک سیستم، فرآیند یا معماری که می‌تواند به اطلاعات خدشه وارد کرده یا به دسترسی غیر مجاز ختم شود، به نام آسیب‌پذیری (vulnerability) شناخته می‌شود. عمل استفاده از آسیب پذیری سوء استفاده (اکسپلویت) نامیده می‌شود. هکرها می‌توانند از طریق ایجاد نقاط دسترسی جعلی کاربران را ترغیب کنند که به شبکه‌های وای‌فایی که هویت آن‌ها معلوم نیست متصل شوند و به این شکل اطلاعات حساس آن‌ها را سرقت کنند. روش دیگر هک کاربران که مرتبط با شبکه‌های بی‌سیم است، حمله Evil Twin AP نام دارد. در این روش هکرها با ارائه SSID شبکه بی‌سیم خود به شکل یک نقطه دسترسی مجاز سعی می‌کنند کاربران را فریب دهند. HostAP، cqureAP و HermesAP از جمله نرم‌افزارهایی هستند که در این حوزه استفاده می‌شوند.

آسیب‌پذیری روز صفر (zero-day exploit) که به نام حمله روزصفر نیز شهرت دارد، بردار حمله دیگری است که در آن هکرها از آسیب‌پذیری نرم‌افزاری که جزییات آن هنوز به شکل عمومی فاش نشده است سوء استفاده می کنند. برای اطلاعات بیشتر در خصوص این بردار حمله به مقاله **حمله روز صفر چیست؟ آیا دفاعی در برابر آن وجود دارد؟** مراجعه کنید.

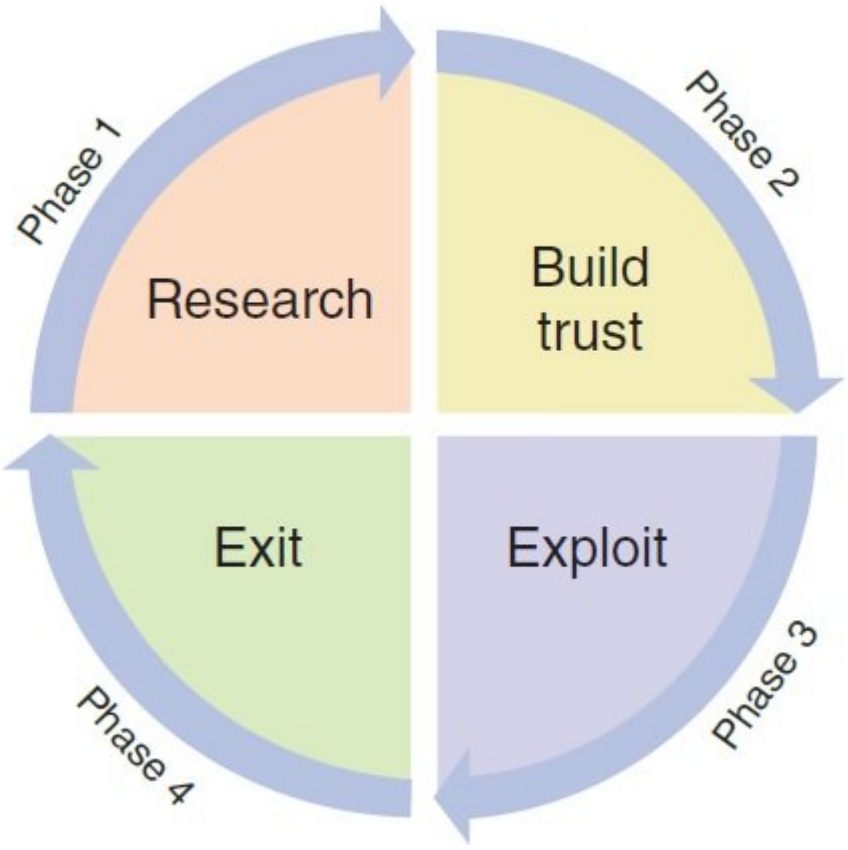
ریسک‌های انسانی

برآوردها نشان می‌دهند، خطاهای انسانی، سهل‌انگاری و کم اطلاعی عامل بیش از نیمی از نقص‌های امنیتی در شبکه‌ها است که به هکرها اجازه می‌دهد به ساده‌ترین شکل به شبکه‌ها نفوذ کنند. یکی از ساده‌ترین راه‌هایی که هکرها برای ورود به شبکه‌ها از آن استفاده می‌کنند، سوال کردن از کاربران در خصوص گذرواژه‌ای است که برای اتصال به شبکه از آن استفاده می‌کنند. در این روش هکرها خود را به جای یکی از افراد مهم یا بخش فنی شرکت معرفی می‌کنند تا اطلاعات موردنیاز را به دست آورند. به این تکنیک حمله مهندسی اجتماعی (social engineering) گفته می‌شود. از رایج‌ترین تکنیک‌های حمله مبتنی بر مهندسی اجتماعی می‌توان به فیشینگ، طعمه و سوییچ و دنبال‌روی (Tailgating) اشاره کرد. برای کسب اطلاعات بیشتر در این خصوص به " **10 تکنیک پایه هک که می‌تواند شما را از حمله هکرها مصون نگه دارد"** مقاله مراجعه کنید.

در تصویر زیر نمونه‌ای از یک حمله فیشینگ را مشاهده می‌کنید.



حملات مهندسی اجتماعی بر مبنای رویکردهای روان‌شناسی انجام می‌شوند. در تصویر زیر چرخه رایج حملات مهندسی اجتماعی را مشاهده می‌کنید.



فاز اول که تحقیق نام دارد؛ مهم‌ترین عنصر این چرخه است که اغلب به صرف زمان زیادی نیاز دارد. در فاز دوم هکرها اقدام به جمع‌آوری اطلاعات و داده‌هایی می‌کنند تا طعمه‌ای برای قربانی آماده کنند. فاز سوم، فاز اجرایی

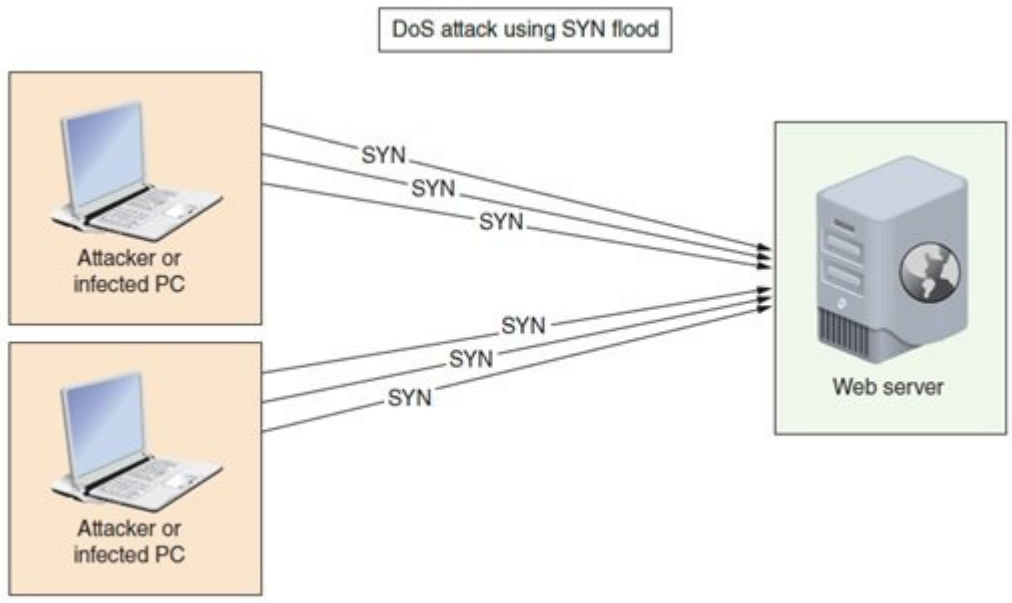
است که هکرها اطلاعات آماده شده را در اختیار قربانی قرار می‌دهند و به انتظار می‌نشینند تا او به دام افتد. سرانجام در فاز چهارم چرخه خروج را اجرا کرده و بدون آن‌که ردپایی از خود به جا بگذارند شبکه یک سازمان و قربانی را ترک می‌کنند. این چرخه برای دریافت اطلاعات عمیق‌تر ممکن است تکرار شود. مهم‌ترین دفاع در برابر چنین حملاتی آموزش کاربران است. گاهی اوقات کارمندان مورد اعتماد یک شرکت دست به اقدامات خرابکارانه‌ای می‌زنند که این مورد به نام تهدید داخلی (insider threat) شهرت دارد. در چنین شرایطی سازمان‌ها برای مقابله با تهدید شکل گرفته از روش‌هایی همچون راه‌حل جلوگیری از نشت داده‌ها (Data Loss Prevention)، اصل حداقل بودن اختیارات (Principle of least privilege) و بررسی سابقه کارمندی که استخدام کرده‌اند استفاده می‌کنند.

ریسک‌های فناوری اطلاعات

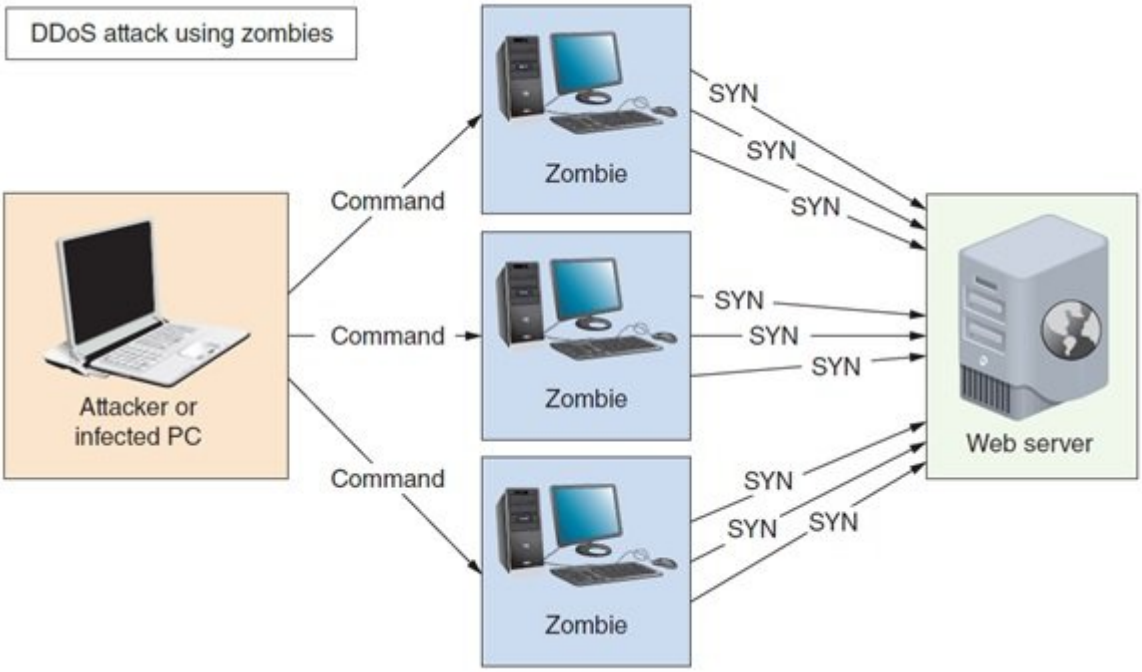
این گروه از مخاطرات امنیتی هر هفت لایه مدل OSI را شامل می‌شوند. حمله به رسانه انتقال، کارت شبکه، روش‌های دسترسی به شبکه، سوییچ‌ها، روترها، نقاط دسترسی و گیت‌وی‌ها در مقایسه با عامل انسانی به توجه بیشتری نیاز دارند. به‌طور مثال یک هکر ممکن است از نقص امنیتی روتر برای پیاده‌سازی یک حمله سیل‌آسا روی پروتکل TCP/IP استفاده کند که نتیجه آن یک ترافیک غیرقابل مهار خواهد بود. ریسک‌های امنیتی پیرامون سخت‌افزارها و طراحی شبکه به شرح زیر هستند:

• حمله جعل (spoofing attack)- آدرس‌های مک را می‌توان در یک حمله جعل هویت تغییر داد. انواع دیگر حملات جعل با هدف تغییر آدرس‌های آی‌پی پیاده‌سازی می‌شوند. جعل آدرس آی‌پی می‌تواند حملات محروم‌سازی از سرویس (DoS) سرنام denial of service یا پیام‌های تغییر یافته DNS را به وجود آورد.

•حمله محروم‌سازی از سرویس (denial of service) – حمله Dos هنگامی رخ می‌دهد که یک کاربر مشروع به دلیل مداخله مهاجم قادر به دسترسی به منابع عادی شبکه، مانند یک وب‌سرور نیست. اغلب این نوع حمله به دلیل هجمه سیل‌آسا که درخواست‌های زیادی مبنی بر دسترسی به سرویس‌ها ارائه می‌کنند و سرور را از پاسخ‌گویی به سرویس‌ها ناتوان می‌سازند رخ می‌دهد. شکل زیر این مدل حمله را نشان می‌دهد. در نتیجه، فرآیند انتقال داده‌ها مختل می‌شود.

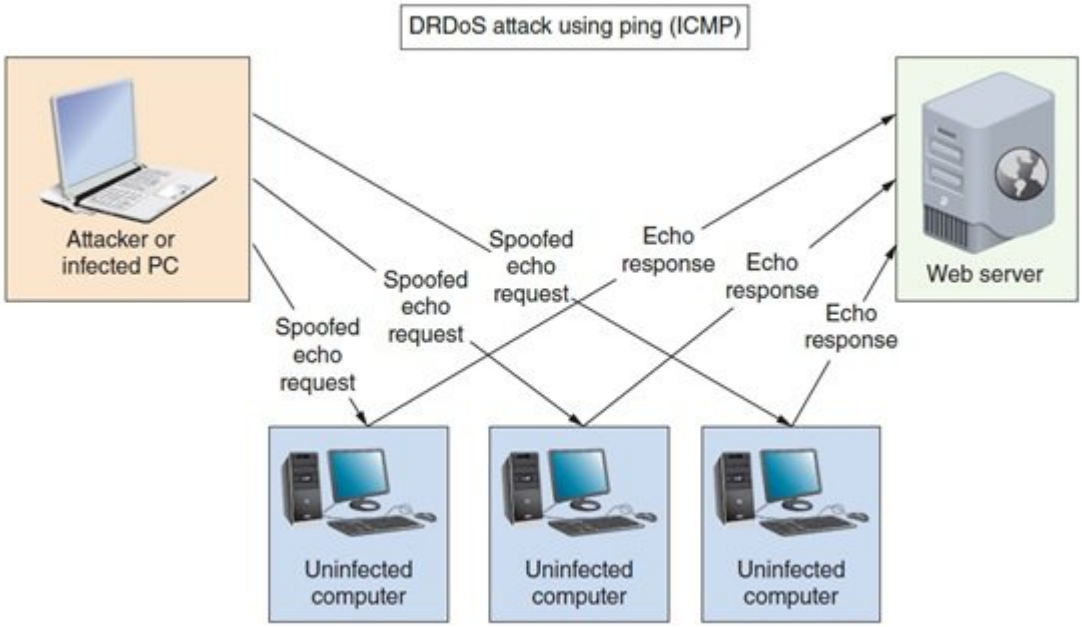


حمله منع سرویس توزیع شده (distributed DoS)- در حالی که یک حمله DoS از یک یا چند منبع متعلق به مهاجم نشات می‌گیرد، حملات DDoS از طریق منابع متعدد و هماهنگ شده به وجود می‌آیند. شکل زیر این مکانیزم حمله را نشان می‌دهد.



برای کسب اطلاعات جامع‌تر در ارتباط با این حمله به مقاله **راهکارهایی برای شناسایی و دفع حمله منع سرویس توزیع شده (DDoS)** مراجعه کنید.

○ حمله انسداد سرویس توزیع‌شده بازتابی DRDoS - یک حمله DRDoS در اصل یک حمله DDoS است که هدفش از دسترس خارج کردن سامانه‌های متصل به شبکه یا در حالت کلی خود شبکه است. این کار با جعل آدرس آی‌پی منبع انجام شده و باعث می‌شود که تمام درخواست‌های پاسخ توسط هدف ارسال شده و سپس تمام پاسخ‌ها به شکل بازتاب‌هایی برای هدف ارسال شود. به همین دلیل هدف با یک ترافیک سیلابی روبرو می‌شود.



از دیگر بردارهای حمله‌های توزیع شده می‌توان به amplified DRDoS، permanent DoS و friendly DoS اشاره کرد.

• حمله مسموم‌سازی سامانه نام دامنه (DNS poisoning) - با تغییر رکوردها DNS در سرور DNS در یک سرور DNS، مهاجم می‌تواند ترافیک اینترنت را از یک وب‌سرور قانونی به یک وبرسایت فیشینگ هدایت کند که مسمومیت

DNS یا جعل DNS نام دارد. به دلیل اینکه سرویس‌دهنده های DNS موجودیت‌های ذخیره شده را به‌اشتراک قرار می‌دهند، سوابق DNS آلوده می‌توانند به سرعت به سایر سرورهای ISP ،DNSها، شبکه‌های خانگی و تجاری و کامپیوترهای شخصی وارد شوند. در واقع، جعل DNS یکی از راه‌هایی است که برخی از کشورها تحت عنوان "فایروال بزرگ" از آن استفاده کرده و مانع از آن می‌شوند تا کاربرانشان به سایت‌های معروف دسترسی داشته باشند.

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

تاریخ انتشار:
28 اردیبهشت 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15312/%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%B4-51