تمرین یک : Wireshark برای اندروید ؟

WireShark متاسفانه برای اندروید در دسترس نیست. اما ابزارهای جایگزینی در اندروید وجود دارد که عبارتند از:

1. CloudShark

2. برنامه cSploit

3. zAnti

4. Packet Capture

برخی از این نرم افزار ها تست شد.

تمرین 2 : طراحی شبکه سازمانی در نرم افزار Packet Tracer ؟



تمرین 3 : حملات مربوط به VLAN و Trunk و حملات لایه 2 OSI ؟

VLAN Hopping

همانطور که می دانید دسترسی از یک VLAN به VLAN دیگر در لایه دو امکان پذیر نیست و تنها در لایه سه با استفاده از روتر و VLAN Routing این امکان فراهم می شود. VLAN Hopping نوعی از حملات است که توسط آن هکر می تواند در لایه دو شبکه از یک VLAN به VLAN دیگر دسترسی پیدا کند. این حملات به دو شیوه Switch spoofing و Double Tagging قابل اجراست.

راهکارهای جلوِگیری از حملات VLAN Hopping

* غیرقعال سازی DTP روی پورتهای سوئیچ به جز پورت های ترانک
* عدم اجازه کلیه VLAN ها به جز VLAN های استفاده شده در پورتهای ترانک
* عدم استفاده از VLAN 1 (Native VLAN)
* تغییرID Native VLAN به یک VLAN غیر کاربردی
* اعمال پیکربندی Native VLAN Tagging در سوئیچ ها
* Shutdown کردن پورتهای بلا استفاده و قرار دادن آنها در یک VLAN غیر کاربردی

MAC Flooding

از آنجایی که MAC پروتکلی است که در لایه دو مورد استفاده قرار می گیرد، بدون در نظر گرفتن تمهیدات امنیتی برای این پروتکل، یک هکر می تواند با هدف قرار دادن CAM Table سوئیچ ها باعث بوجود آمدن CAM Overflow شده در نتیجه می تواند به شنود ترافیک شبکه بپردازد. این ترافیک می تواند حاوی اطلاعات حساس شرکت از جمله اطلاعات مالی، ترافیک صدا در شبکه، پسورد سیستم ها، سرورها، تجهیزات و … باشد.

راهکارهای جلوگیری از MAC Attacks

اجرای Port Security

در اجرای این پیکربندی ملاحظات مربوط به voice Vlan نیز در نظر گرفته می شود.

DHCP Attacks

DHCP Starvation و Rogue DHCP: در این حملات، مهاجم با برادکست نمودن درخواست های DHCP توسط آدرس های مک جعلی و ساختگی باعث استفاده شدن تمام آدرس های DHCP Address Pool می شود در نتیجه DHCP آدرسی برای اختصاص به سایر درخواست های DHCP ندارد. اینجاست که هکر با راه اندازی یک DHCP جعلی (Rogue DHCP) براحتی می تواند سیستم های یک شبکه را مورد سوء استفاده قرار دهد.

ARP Table Poisoning

همه ما با نحوه عملکرد پروتکل ARP در شبکه آشنایی داریم اما یک نکته جالب در مورد این پروتکل وجود دارد و آن اینست که هر کلاینت اجازه دارد یک ARP Reply را بدون اینکه کلاینتی ARP Request بفرستد بصورت برادکست ارسال کند در اصطلاح به این فریم ارسالی Gratuitous ARP گفته می شود و صرفا جهت معرفی آدرس مک کلاینت توسط خود کلاینت به سایر کلاینت ها استفاده می شود.

یک هکر می تواند از این ویژگی استفاده کند و خود را به عنوان یک کلاینت دیگر در شبکه بطور مثال گیت وی شبکه معرفی کند در نتیجه آدرس مک هکر به جای آدرس مک گیت وی شبکه در ARP Table کلاینت ها قرار می گیرد. بدین ترتیب درخواست کلاینت ها به جای ارسال به گیت وی به سمت هکر هدایت می شود. با این روش ترافیک شبکه که می تواند حاوی اطلاعات حساس از جمله پسورد سیستم ها و … باشد توسط هکر مورد شنود قرار گیرد.

راهکارهای جلوِگیری از ARP Attacks

DAI (Dynamic ARP Inspection)

این قابلیت به بررسی درخواست ها و پاسخ های ARP می پردازد و این درخواست ها و پاسخ ها را با دیتابیس و جدول DHCP Snooping (این جدول خود از درخواست های DHCP تشکیل می شود) مقایسه می کند در صورتیکه ترکیب IP و MAC موجود در فریم های ARP در جدول DHCP Snooping وجود داشته باشد، این فریم یک فریم معتبر شناخته شده و درنتیجه توسط سوئیچ به مقصد مورد نظر هدایت و در غیر این صورت فریم drop می شود.

\*همانطور که متوجه شدید پیش نیاز اجرای DAI راه اندازی DHCP Snooping و Port Security می باشد به همین دلیل اجرای کلیه این پیکربندی ها به ترتیبی که ذکر می شود ضروری است.

\*در صورتیکه در شبکه ای DHCP راه اندازی نشده باشد، باز هم امکان پیاده سازی DAI با استفاده از ARP ACL یا DHCP Static entry وجود دارد.

MAC Spoofing

تکنیک استفاده از آدرس مک سیستمی درگیر در شبکه جهت مقاصد خراب کارانه تحت عنوان MAC Spoofing شناخته می شود.

تصور کنید در شبکه ای یک هکر آدرس مک خود را به آدرس مک یکی از سیستم ها در شبکه تغییر دهد در این شرایط CAM table سوئیچ نیر تغیر می کند. با این عمل، ترافیک شبکه به آن سیستم خاص به سیستم هکر هدایت شده و در این صورت هکر می تواند ترافیک ارسالی به سیستم مورد نظر را بطور موقت شنود کند.

راهکارهای جلوِگیری از IP/MAC Spoofing Attacks

IP Source Guard

این قابلیت همانند DAI عمل می کند با این تفاوت که علاوه بر بررسی فریم های ARP، سایر پکت ها و فریم ها را نیز بررسی می کند.

IPSG (IP Source Guard) جهت جلوگیری از حملات IP Spoofing از اطلاعات جدول DHCP Snooping استفاده می کند اما جهت جلوگیری از حملات MAC Spoofing وابسته به اجرای پیکربندی های ذیل است:

فعال سازی DHCP option 82 در سرور DHCP (در ویندوز سرور ۲۰۱۲ برخلاف ورژن های گذشته ویندوز سرور این قابلیت اضافه شده است)

پیکربندی Trust نمودن Option 82 در سوئیچ های لایه سه بین کلاینت ها و سرور DHCP (سوئیچ هایی که نقش DHCP relay را بازی میکنند)

STP Attacks

در شبکه همواره لینک های Redundant از اهمیت ویژه ای برخورد بوده اند این اهمیت در لینک های Redundant بین سوئیچ ها نیز کاملا محسوس است. اما در این شرایط امکان ایجاد لوپ در شبکه وجود دارد بنابراین پروتکلSTP برای جلوگیری از Loop در لایه دو شبکه بوجود آمد. این پروتکل در صورت نادیده گرفتن تمهیدات امنیتی در این لایه براحتی می تواند مورد سوء استفاده قرار گیرد.

بطور خلاصه پروتکل STP در شبکه برای تعیین سوئیچ Root bridge و تعیین لینک فعال بین لینکهای Redundant از پروتکل BPDU استفاده می کند. Root bridge سوئیچی است که ترافیک شبکه از طریق این سوئیچ به سایر بخشهای شبکه منتقل می شود.

حال تصور کنید یک هکر در شبکه سیتسم خود را به عنوان یک سوئیچ در شبکه معرفی کند و در نهایت با ارسال فریم های BPDU با پارامترهایی خاص، خود را به عنوان Root Bridge می شناساند بنابراین قادر به شنود ترافیک شبکه خواهد بود.

راهکارهای جلوگیری از حملات مبتنی بر STP

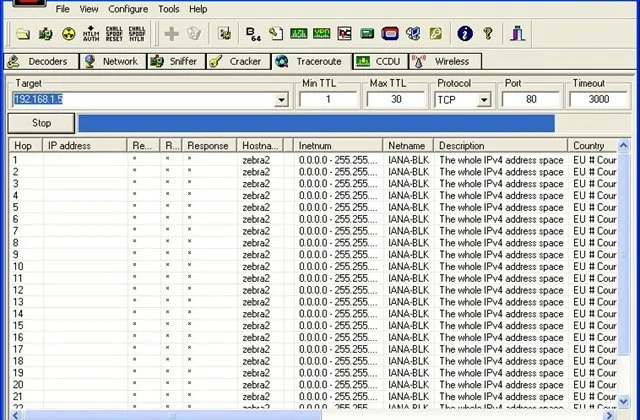
* Root Guard
* BPDU Guard
* CDP Attacks

در واقع از پروتکل CDP نه برای حمله بلکه جهت کسب و جمع آوری اطلاعاتی در خصوص شبکه (CDP Sender, IP Address, Software Version, Device Model,…) و توپولوژی شبکه مورد استفاده قرار می گیرد. علاوه بر جمع آوری اطلاعات، این پروتکل در IOS های سیسکو در ورژن های قبل از ۱۲٫۱(۱۰٫۱) آسیب پذیر بوده طوری که با ارسال پکت های بی شمار CDP به یک سوئیچ (CDP Flooding)، سوئیچ Crash کرده و نیاز به ریستارت داشته است.

راهکارهای جلوگیری از حملات مبتنی بر CDP

همانطور که ذکر شد هکرها از این پروتکل جهت جمع آوری اطلاعاتی در مورد شبکه استفاده می نمایند به عبارت دیگر این پروتکل مورد حمله قرار نمی گیرد بلکه از ان صرفا جهت جمع آوری اطلاعات بهره گیری می شود. بنابراین جهت جلوگیری از این اتفاق کافی است CDP روی پورتهای لایه Access غیرفعال شود.

تمرین 4: استفاده از Cain and Abel برای Arp Poisening



با استفاده از ابزار Cain and Abel شما می توانید فرآیندی به نام ARP Cache Poisoning را انجام دهید ، ARP Cache Poisoning به نوعی یک حمله از نوع MITM یا Man In The Middle می باشد که با استفاده از پروتکل ARP می توانید ترافیکی که بین دو سیستم رد و بدل می شود را به سمت سیستم مهاجم هدایت کند. زمانیکه قابلیت ARP Cache Poisoning بر روی Cain and Abel فعال باشد شما می توانید با استفاده از Sniffer موجود در این نرم افزار NTLM Hash های عبوری از سیستم های این بین را Sniff کنید.

تمرین 5 : انواع NAT :

Static NAT چیست؟

در این روش NAT به صورت یک به یک انجام می شود. اگر شما 100 کاربر داخلی و 100 ادرس global داشته باشید. می توانید از این روش استفاده کنید و برای هر یوزر مشخص کنید از چه آدرس global می تواند استفاده کند. به صورت معمول ما به اندازه کافی آدرس global برای هر کاربر نداریم. استفاده معمول از روش static NAT برای یک سرور در شبکه داخلی یا محیط DMZ است و می خواهیم به کاربران سطح اینترنت دسترسی به این سرور را بدهیم و با استفاده از static NAT می توانیم این دسترسی را فراهم کنیم.

Dynamic NAT چیست؟

در این حالت ما یک رنج از آدرس های global داریم و تنها این رنج آدرس ها را به شبکه داخلی اختصاص می دهیم تا زمانیکه هر دستگاه نیاز به استفاده از اینترنت را داشت از آنها استفاده کند. به طور مثال ، یک کاربر می خواهد از اینترنت استفاده کند با شروع به کار او یک آدرس global از این رنج به او اختصاص داده می شود و این کاربر با استفاده از این آدرس global ارتباطش با اینترنت برقرار می شود بعد از یک بازه زمانی کاربر کارش با اینترنت به اتمام می رسد و دیگر نیاز به استفاده از اینترنت را ندارد. در این دستگاهی مثل روتر که عمل NAT را انجام می دهد بعد از یک بازه زمانی مشخص در صورت عدم استفاده آدرس global این آدرس را آزاد خواهد کرد که سایر دستگاه ها بتوانند از آن استفاده کنند. تعداد آدرس های global با تعداد دستگاه های شبکه داخلی که می خواهند از اینترنت استفاده کنند باید برابر باشد.

(Dynamic PAT (NAT with overload چیست؟

این روش برای بیشتر کاربرانی که به اینترنت متصل می شوند استفاده می شود. در این روش از مزیت Dynamic NAT که تنها به کاربرانی که نیاز به استفاده از اینترنت دارند آدرس Global اختصاص داده می شود استفاده می کند و در کنار آن با استفاده از شماره پورت های مورد استفاده در ارتباط ، امکان استفاده جندین کاربر را از یک آدرس Global فراهم می کند. در این روش دستگاهی که عمل PAT را انجام می دهد اطلاعات پورت و IP ها را ردیابی می کند و براساس آنها جدول NAT را تشکیل می دهد.

Source NAT چیست؟

Source NAT بصورت معمول توسط کاربران داخلی شبکه استفاده میشه تا به اینترنت دسترسی پیدا کنن. اسمش رو چرا گذاشتن Source NAT ؟ بخاطر اینکه Source یا مبدا Packet توسط سرویس NAT دستکاری میشه و وقتی که Packet میخواد بره توی اینترنت IP Private برداشته میشه و جاش IP Public ای که روتر هست قرار میگیره. ما 3 نوع Source NAT داریم :

1- Dynamic IP and Port یا DIPP : در این نوع Source NAT ما کلاینت های مختلفی و در نتیجه با IP Private های مختلفی داریم که میخوان با یه IP Public پکت هاشون NAT بشن و برن توی اینترنت. اگه جایی PAT یا Port Address Translation شنیدید DIPP همون PAT هست. گاها بهش Network Address Port Translation یا NAPT هم میگن. DIPP کاری که می کنه اینه که به هر IP کلاینت یک Port تو NAT Pool خودش اختصاص میده و برای جا هایی که فقط یدونه IP Public دارن بسیار مناسبه. نمیخواد جای دوری برید ! شما توی خونه تون هم از این نوع Source NAT دارین استفاده می کنین !

2- Dynamic IP : خب شما توی سازمانی که دارید کار می کنید به احتمال زیاد بیشتر از یدونه IP Public دارید چون ممکنه سرور هایی داشته باشید که اگه اینترفیسی که روش IP Public هست Fail شد سرورتون بتونه از لینک دوم اینترنت تون استفاده کنه. در این نوع Source NAT سرویس NAT یک IP Private رو به یک IP Public مپ می کنه یعنی شما فرض کنید 5 تا IP Private توی NAT Pool دارین که هر کدوم از این IP ها مربوط به یک سرور در شبکه تون هست حالا NAT میاد و به هر کدوم (تاکید می کنم به هر کدوم) از این Private IP ها یه Public IP اختصاص میده تا بتونن Source NAT بشن و برن توی اینترنت. حالا اگه IP ششمی میاد تو وسط NAT بهش این اجازه رو نمیده و باید یه Private IP اتصالش رو قطع کنه تا Public IP اون آزاد بشه تا IP بعدی بتونه از اون Public IP استفاده کنه. البته تو فایروال هایی مثل Palo Alto قابلیت جالبی که به سرویس NAT اضافه کردن به شما این امکان رو میده که بتونید کاری کنید که وقتی این اتفاق افتاد IP بعدی که میخواد از Public IP استفاده کنه یکی از Public IP ها رو PAT یا DIPP کنه تا اون سرور بیکار نمونه و بره توی اینترنت کارشون بکنه.

3- Static IP : از اسمش هم مشخصه ! یعنی توی NAT Pool یک Private IP به یک Public IP مپ میشه. تفاوت Static IP با Dynamic IP در اینه که در Dynamic IP اگه IP یه کلاینت عوض بشه یا یه کلاینت دیگه جاش بیاد میتونه از Public IP ای که NAT در اختیارش قرار میده استفاده کنه اما توی Static IP همونطور که الان گفتیم یدونه Private IP به یدونه Public IP مپ میشه.

Destination NAT چیست؟

دوستان عزیزم همیشه توی ذهنتون بمونه Destination NAT برای زمانی هست که شما توی شبکه داخلی تون یک وب سرور ، فایل سرور یا هر چی راه اندازی کردید که میخواید از محیط اینترنت کاربراتون بتونن از اون سرورتون استفاده کنن. پس Destination NAT مستقیما داره با Incoming Packet ها پکت های ورودی به شبکه کار می کنه. میتونیم بگیم که Destination NAT درست عکس کاری رو انجام میده که Source NAT انجام میده.

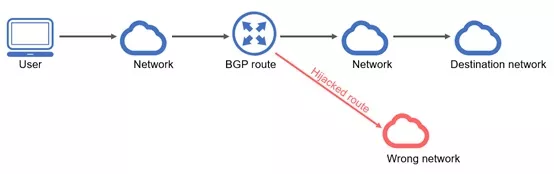
وقتی پکتی با Public IP میخواد وارد روتر بشه روتر به پورت موجود در پکت اون IP نگاه می کنه و میبینه که مثلا پورت 80 هست ( این یعنی اینکه شما توی شبکه داخلی تون وب سرور دارید ) و روتر از اونجا که براش NAT Rule نوشته شده و گفته شده که وقتی روی پورت 80 پکتی اومد بفرستش به وب سرور داخلی که از یه Private IP داره استفاده می کنه و این لازمش اینه که شما توی روتر یا فایروال تون Port Forwarding رو انجام داده باشید.

ممکنه که شما یک طرفه به این قضیه نگاه کنید و همین باعث بشه که نتونید این مطلب رو درک کنید همیشه وقتی Source NAT هست Destination NAT هم هست Source NAT نحوه دسترسی یک کلاینت یا یک سرور رو به اینترنت مشخص می کنه اما Destination NAT زمانی هست که سروری راه اندازی کردید که میخواید کاربرا از طریق اینترنت بتونن وارد اون سرور تو شبکه داخلی تون بشن. پس در هر دو طرف ما روتر رو داریم و عملیات NAT روی پکت ها انجام میشه تا بتونن به اینترنت و یا شبکه داخلی دسترسی داشته باشن.

وقتی شما Port Forwarding روی روتر انجام میدین یک Public IP به یه Private IP ترجمه میشه اما پورت مبدا اون پکت دست نمیخوره. یعنی شما فرض کنید پورت 80 رو فوروارد کردین و همین پورت 80 رو کلاینت توی اینترنت تو مرورگرش همراه با Public IP سرورتون میزنه و هدایت میشه به وب سرور داخلی شما اما تو Port Translation شما پورت 80 رو برای مثال روی روتر فوروارد کردین و توی NAT Rule تون گفتید که وقتی پکت روی پورت 80 اومد پورت 80 رو ترجمه کن به یه پورت دیگه مثلا 6080 . امیدوارم که تفاوت بین Source NAT و Destination NAT رو بخوبی درک کرده باشید.اگر در درک مفهوم کلی کار کردن سرویس NAT همچنان مشکل دارید ، پیشنهاد می کنم به دوره آموزش نتورک پلاس مهندسی نصیری قسمت NAT مراجعه کنید. اگه سئوالی یا ابهامی داشتید در زیر همین مطلب بپرسید تا بهتون پاسخ بدم.

تمرین 6: حمله BGP Neibour

این حمله زمانی رخ می‌دهد که مهاجمان بتوانند به طور مخرب به Traffic های اینترنت دست بیابند، اینکار با استفاده از تزریق آدرس های IP و Prefix های(به اصطلاح Prefix Injection) آن در داخل جدول Routing موجب مسیریابی نادرست Traffic ها به سمت دیگری می‌شوند(به سمت فرد مهاجم برای مثال). در این حمله فرد مهاجم توانایی پیاده سازی یک حمله MITM در سطح WAN را پیدا خواهد کرد. این حمله زمانی رخ می‌دهد که دو AS دو آدرس IP به همراه Prefix Length های یکسان را تبلیغ می‌کنند و از این رو BGP برای انتخاب بهترین مسیر، مسیری را انتخاب می‌سازد که AS Path آن کمتر باشد. حمله BGP Hijacking بر روی بستر شرکت ها و سرویس های مختلف و بزرگ دنیا پیاده سازی شده است برای مثال در روز یک‌شنبه 24 فوریه سال 2008 این حمله بر روی YouTube به علت پیکربندی های نادرست از سمت ISP پیاده سازی شد و این بستر را دچار اختلال کرد



برای درک بهتر حمله BGP Hijacking به مثال تصویر زیر توجه کنید که ماشین ها از مسیر اصلی اتوبان خارج شده و به سمت مسیر فرعی دیگری هدایت می‌شوند، دقیقا حمله BGP Hijacking به همین شکل است که Route هارا از مسیر اصلی خود خارج و به سمت یک مسیر نادرست هدایت کند

تمرین 7 : نصب Zone Alarm ، Comodo، Glasswire

نصب برنامه ها انجام پذیرفت.