دانشگاه فردوسی مشهد

دانشکده مهندسی

گروه مهندسی کامپیوتر

گزارش فاز صفر درس شبکه های کامپیوتری

عنوان

Packet sniffing & packet analyzing

نگارش

الهه متقین

استاد درس

دکتر یغمایی

بهمن ماه ۱۳۹۹

۱. مقدمه

همه روزه شاهد ابداع فن آوری های جدیدی در عرصه دنیای گسترده امنیت اطلاعات می باشیم. ابداع هر فن آوری جدید از یک طرف کارشناسان امنیت اطلاعات را امیدوار به برپاسازی و نگهداری یک شبکه ایمن می نماید و از طرف دیگر مهاجمان را امیدوار به تدارک حملاتی که شانس موفقیت بیشتری را داشته باشند. چراکه آنان نیز از آخرین فن آوری های موجود در این عرصه به خوبی استفاده خواهند کرد. شاید به همین دلیل باشد که بسیاری از کارشناسان فن آوری اطلاعات و ارتباطات بر این عقیده هستند، مادامیکه دانش مهاجمان بیش از کارشناسان امنیت اطلاعات است امکان مقابله منطقی، ساخت یافته و به موقع با بسیاری از حملات وجود نخواهد داشت. (چگونه می توان با چیزی مقابله نمود که نسبت به آن شناخت مناسبی وجود ندارد؟). این یک واقعیت تلخ در دنیای امنیت اطلاعات است که بسیاری از پتانسیل هائی که به منظور تسهیل در امر استفاده کامپیوتر و یا افزایش کارآئی سیستم ایجاد و یا به عنوان محصولات و ابزارهائی در جه حفاظت و ایمن سازی شبکه های کامپیوتری عرضه می گردند، توسط مهاجمان و به منظور برنامه ریزی حملات در شبکه های کامپیوتری نیز مورد استفاده قرار خواهند گرفت.

۲. Packet sniffing چیست؟

یکی از قدیمی ترین روش های سرقت اطلاعات در یک شبکه، استفاده از فرآیندی موسوم به packet sniffing است. کامپیوتری که به یک LAN وصل باشد دو آدرس دارد. اولی مک است که آدرس مک که برای هر سخت افزار که آدرس مک دارد یکتا است و دو تا کارت را پیدا نمی کنید که ادرس مک آن ها با یکی دیگر یکسان باشد. از این آدرس مک برای ساختن قاب های اطلاعاتی (Frame) برای ارسال اطلاعات به و یا از ماشین ها استفاده می شود. دومی آدرس، IP می باشد که در لایه سوم یعنی شبکه می باشد. برای ارسال اطلاعات به کامپیوتر دیگر سیستم اول داخل جدول ARP به دنبال آدرس مک سیستم مقابل می گردد و اگر هیچ مک آدرسی برای IP هدف پیدا نکند یک درخواست برای همه برودکست می کند و از همه می خواهد که هرکسی آی پی مورد نظر می باشد آدرس مک خود را اعلام کند. بدین وسیله اگر سیستم داخل شبکه آدرس آی پی پاکت را با خودش یکی ببیند آدرس مک را داخل یک پکت گذاشته و برای سیستم درخواست کننده ارسال می کند. حالا سیستم آدرس فیزیکی سیستم دیگر را دارد و این آدرس را به جدول ARP خودش اضافه می کند. از این به بعد کامپیوتر مبدا برای ارتباط با سیستم مقصد از این آدرس فیزیکی استفاده می کند. در لایه دوم که arp کار می کند دستگاه های switch و hub عمل می کنند. هکرها کارهایی انجام می دهد که این دستگاه ها اطلاعات را به سمت کامپیوتر آن ها می فرستند و هکر با گرفتن این پکت ها و بررسی آن ها اطلاعاتی را به دست می آورند نظیر پسوردها، سایت ها، ادرس ایمیل ها و ..... که در ادامه به آن ها خواهیم پرداخت.

امروزه پروتکل هائی نظیر IPSec به منظور پیشگیری از packet sniffing طراحی شده است که با استفاده از آن بسته های اطلاعاتی رمزنگاری می گردند. در حال حاضر تعداد بسیار زیادی از شبکه ها از تکنولوژی IPSec استفاده نمی نمایند و یا صرفا بخش اندکی از داده های مربوطه را رمزنگاری می نمایند و همین امر باعث شده است که packet sniffing همچنان یکی از روش های متداول به منظور سرقت اطلاعات باشد.

یک packet sniffer که در برخی موارد از آن به عنوان network monitor و یا network analyzer نیز یاد می شود، می تواند توسط مدیران شبکه به منظور مشاهده و اشکال زدائی ترافیک موجود بر روی شبکه استفاده گردد تا به کمک

آن بسته های اطلاعاتی خطاگونه و گلوگاه های حساس شبکه شناسائی و زمینه لازم به منظور انتقال موثر داده ها فراهم گردد. به عبارت ساده تر، یک packet sniffer تمامی بسته های اطلاعاتی که از طریق یک اینترفیس مشخص شده در شبکه ارسال می گردند را جمع أوری تا امکان بررسی و آنالیز آنان فراهم گردد. عموما از برنامه های packet sniffer به منظور جمع آوری بسته های اطلاعاتی به مقصد یک دستگاه خاص استفاده می گردد. برنامه های فوق قادر به جمع آوری تمامی بسته های اطلاعاتی قابل حرکت در شبکه صرفنظر از مقصد مربوطه نیز می باشند.

یک مهاجم با استقرار یک packet sniffer در شبکه، قادر به جمع آوری و آنالیز تمامی ترافیک شبکه خواهد بود. اطلاعات مربوط به نام و رمز عبور عموما به صورت متن معمولی و رمز نشده ارسال می گردد و این بدان معنی است که با آنالیز بسته های اطلاعاتی، امکان مشاهده اینگونه اطلاعات حساس وجود خواهد داشت. یک packet sniffer صرفا قادر به جمع آوری اطلاعات مربوط به بسته های اطلاعاتی درون یک subnet مشخص شده است. بنابراین یک مهاجم نمی تواند یک packet sniffer را در شبکه خود نصب نماید و از آن طریق به شبکه شما دستیابی و اقدام به جمع آوری نام و رمز عبور به منظور سوء استفاده از سایر ماشین های موجود در شبکه نماید. مهاجمان به منظور نیل به اهداف مخرب خود می بایست یک packet sniffer را بر روی یک کامپیوتر موجود در شبکه اجراء نمایند.

۳. در حملات sniffing چه چیزی می تواند شنود شود؟

می توان اطلاعات حساسی را که در لیست زیر قرار داده ایم را شنود کرد:

- ترافیک ایمیل(Email traffic)
- رمزهای عبور اف تی پی(FTP passwords)
- ترافیک وب(Web traffics)
- گذرواژههای تلنت(Telnet passwords)
- پیکربندی روتر(Router configuration)
- جلسات گفتگو(Chat sessions)
- ترافیک دی ان اس(DNS traffic)

۴. انواع Sniffing

Sniffing می تواند فعال (Active) یا غیر فعال (Passive) باشد.

۴/۱. حالت غیر فعال (Passive) در حملات Sniffing

در این نوع Sniff کردن مهاجم بر روی کلیه کامپیوترهای یک شبکه LAN نرم افزار شنود نصب می کند که تقریبا کمتر کسی این روزها امکان شنود به این روش را دارد. شنود کردن شبکه این روزها بسیار سخت شده است، قبلا با توجه به مکانیزم کاری که در HUB ها وجود داشت و داده ها در کلیه پورت ها ارسال می شدند، نرم افزار Sniffer هم می توانست داده های کل

شبکه LAN را به یک باره شنود کند اما این روزها از HUB استفاده نمی شود این نوع Sniff کردن شبکه را Passive Sniffing می نامند چون هکر نیازی به انجام هیچ کاری برای دریافت اطلاعات از شبکه ندارد.

ابزارهای Sniffing براحتی اطلاعات مورد نیازشان را در این محیط به دست می آورند. این نوع شنود در شبکه های بی سیم هم کاربرد دارد و وقتی صحبت از Passive Sniffing در شبکه های وایرلس می شود یعنی اینکه ما صرفا با یک کارت شبکه وایرلس نرم افزار شنود را اجرا می کنیم و منتظر می شویم که Packet ای به ما برسد تا آن را Capture کنیم. این روزها رسما Passive Sniffing در شبکه های کابلی منسوخ شده است اما در شبکه های وایرلس همچنان قابل استفاده است. نکته مهمی که در Passive Sniffing وجود دارد این است که کسی متوجه حضور مهاجم نمی شود. خبر خوب این است که Hubها امروزه منسوخ شده اند و بیشتر شبکه های مدرن از سوئیچ استفاده می کنند .از این رو، اسنیف Passive زیاد موثر نخواهد بود.

۴/۲. حالت فعال (Active) در حملات Sniffing

در این حالت نرم افزارهای شنود قادر هستند تعداد بسیار زیادی MAC Address جعلی را به سمت سویچ ارسال کنند و جدول آدرس MAC یا MAC Table را سرریز می کند و با سرریز شدن این جدول سوییچ ما تبدیل به یک HUB می شود و ترافیک را بر روی تمامی پورت های خودش ارسال می کند و فرآیند شنود ما کامل می شود. طبیعی است که با توجه به ایجاد شدن ترافیک بسیار زیاد احتمال شناسایی هکر بسیار زیاد است. اما همین مکانیزم برای شبکه های وایرلس نیز صادق است، در Passive Wireless Sniff شما منتظر می مانید که Access Point شما برای سیستم شما یک بسته ارسال کند که ممکن است مدت ها زمان ببرد، در Active Wireless Sniffing ما بصورت جعلی برای Access Point درخواست های زیادی ارسال می کنیم تا مجبور به پاسخگویی و در نتیجه امکان شنود آن شود. این روزها وقتی صحبت از شنود در شبکه می شود منظور Active Sniffing است.

تکنیک های Sniffing فعال عبادتند از:

- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Spoofing Attacks
- ARP Poisoning

۵. پروتکل های تحت تأثیر حملات Sniffing

به طور کلی تمام پروتکل هایی که از رمز نگاری استفاده نمی کنند به راحتی آسیب پذیر می باشند، در زیر برخی از آن ها را نام برده ایم.

- **HTTP** پروتکلی است که برای ارسال متن به کار میرود بدون استفاده از هیچ گونه رمزنگاری.
- **SMTP** اساسا در انتقال ایمیل ها مورد استفاده قرار می گیرد .این پروتکل کارآمد است، اما هیچگونه حفاظت در برابر sniffing را شامل نمی شود.

- **NNTP** این پروتکل برای تمامی ارتباطات استفاده می شود، اما اشکال اصلی این است که داده ها و حتی پسوردهای بر روی شبکه به عنوان متن واضح (clear text) ارسال می شوند.
- **POP** برای دریافت ایمیل از سرور استفاده می شود .این پروتکل هیچ محافظتی در برابر sniffing ندارد.
- **FTP** برای ارسال و دریافت فایل استفاده می شود، اما هیچ ویژگی امنیتی ارائه نمی دهد .تمام داده ها به صورت متن ساده ارسال می شوند.
- **IMAP** عملکردهای آن همانند SMTP است، اما در برابر اسنیف بسیار آسیب پذیر است.
- **Telnet** همه چیز (نامهای کاربری، رمزهای عبور و...) را بر روی شبکه به عنوان متن ساده (clear text) ارسال می کند و از این رو می توان به راحتی آن را اسنیف کرد.

۶. روش های تشخیص packet sniffing در شبکه

همانگونه که اشاره گردید تشخیص این موضوع که یک فرد در یک بازه زمانی محدود و همزمان با حرکت بسته های اطلاعاتی در شبکه از یک packet sniffer استفاده می نماید، کار مشکلی خواهد بود. با بررسی و آنالیز برخی داده ها می توان تا اندازه ای این موضوع را تشخیص داد :

- **استفاده از امکانات ارائه شده توسط برخی نرم افزارها** : در صورتی که مهاجمان دارای منابع محدودی باشند ممکن است از برنامه کاربردی Network Monitor برای packet sniffing استفاده نمایند . یک نسخه محدود از Network Monitor به همراه ویندوز NT و ۲۰۰۰ و یک نسخه کامل از آن به همراه SMS Server ارائه شده است . برنامه فوق ، گزینه ای مناسب برای مهاجمانی است که می خواهند در کوتاه ترین زمان به اهداف خود دست یابند چراکه استفاده از آن در مقایسه با سایر نرم افزارهای مشابه راحت تر است. خوشبختانه می توان بسادگی از اجرای این برنامه توسط سایر کاربران در یک شبکه، آگاهی یافت. بدین منظور کافی است از طریق منوی Tools گزینه Identify Network Monitor Users را انتخاب نمود.
- **بررسی سرویس دهنده DNS :** در صورتی که مهاجمان از یکی از صدها نرم افزار ارائه شده برای packet sniffing استفاده نمایند، امکان تشخیص سریع آن همانند برنامه Monitor Network وجود نخواهد داشت. توجه داشته باشید که یک روش صدرصد تضمینی به منظور تشخیص وجود یک برنامه packet sniffing در شبکه وجود ندارد ولی با مشاهده نشانه هائی خاص می توان احتمال وجود packet sniffing در شبکه را تشخیص داد. شاید بهترین نشانه وجود یک packet sniffing در شبکه به بانک اطلاعاتی سرویس دهنده DNS برگردد. سرویس دهنده DNS وظیفه جستجو در بانک اطلاعاتی به منظور یافتن نام host و برگرداندن آدرس IP مربوطه را بر عهده دارد. در صورتی که مهاجمی یک packet sniffing را اجراء نماید که اسامی host را نمایش می دهد (اکثر آنان چنین کاری را انجام می دهند)، ماشینی که فرآیند packet sniffing را انجام می دهد یک حجم بالا از درخواست های DNS را اجراء می نماید. در مرحله اول سعی نمائید ماشینی را که تعداد زیادی درخواست های DNS lookups را انجام می دهد، بررسی نمائید. با این که وجود حجم بالائی از درخواست های lookup DNS به تنهائی نشاندهنده packet sniffing نمی باشد ولی می تواند به عنوان نشانه ای مناسب در این زمینه مطرح گردد . در صورتی که به یک ماشین خاص در شبکه مشکوک شده اید، سعی نمائید یک ماشین طعمه را پیکربندی و آماده نمائید. ماشین فوق یک کامپیوتر شخصی است که کاربران از وجود آن آگاهی ندارد. پس از اتصال این نوع کامپیوترها به شبکه، یک حجم بالا ی ترافیک بر روی شبکه را ایجاد نموده و به موازات انجام این کار درخواست های DNS را بررسی نمائید تا

مشخص گردد که آیا ماشین مشکوک یک درخواست DNS را بر روی ماشین طعمه انجام می دهد. در صورتی که اینچنین است می توان با اطمینان گفت که ماشین مشکوک همان ماشین sniffing packet است.

- **اندازه گیری زمان پاسخ ماشین های مشکوک :** یکی دیگر از روش های متداول برای شناسائی افرادی که از packet sniffing استفاده می نمایند، اندازه گیری زمان پاسخ ماشین مشکوک است. روش فوق مستلزم دقت زیاد و تا اندازه ای غیرمطمئن است. بدین منظور از دستور Ping ماشین مشکوک به منظور اندازه گیری مدت زمان پاسخ استفاده می شود . بخاطر داشته باشید فردی که عملیات packet sniffing را انجام می دهد تمامی بسته های اطلاعاتی را کپی نخواهد کرد، چراکه حجم اطلاعات افزایش خواهد یافت. آنان با تعریف یک فیلتر مناسب، صرفا بسته های اطلاعاتی مورد علاقه خود را تکثیر می نمایند (نظیر آنانی که برای تائید کاربران استفاده می گردد) . بنابراین از تعدادی از همکاران خود بخواهید که چندین مرتبه عملیات log in و log out را انجام داده و در این همین وضعیت مدت زمان پاسخ کامپیوتر مشکوک را محاسبه نمائید. در صورتی که مدت زمان پاسخ زیاد تغییر نکند، آن ماشین احتمالا عملیات packet sniffing را انجام نمی دهد ولی در صورتی که زمان پاسخ کند گردد، این احتمال وجود خواهد داشت که ماشین مشکوک شناسائی شده باشد.

- **استفاده از ابزارهای مختص AntiSniff :** شرکت های متعددی اقدام به طراحی و پیاده سازی نرم افزارهائی به منظور ردیابی و شناسائی packet sniffing نموده اند. برنامه های فوق از روش های اشاره شده و سایر روش های موجود به منظور شناسائی packet sniffing در یک شبکه استفاده می نمایند.

۷. ابزارهای پرکاربرد برای حملات Sniffing

ابزارهای زیادی برای اسنیف شبکه وجود دارد و همه آنها ویژگی های خاص خود را دارند تا هر کس تجزیه و تحلیل ترافیک و اطلاعات را بر اساس سلیقه خود به دست آورد.

- **BetterCAP** یک ابزار قدرتمند، انعطاف پذیر و قابل حمل است که برای انجام انواع مختلف حملات MITM علیه شبکه، دستکاریHTTP ، HTTPS و ترافیک TCP به صورت لایو به کار می رود.
- **Ettercap** یک مجموعه جامع برای حملات مرد میانی است. دارای قابلیت هایی همچون اسنیف ارتباطات زنده، فیلتر کردن محتوا و... می باشد.
- **Wireshark** یکی از معروف ترین ابزارهای sniffing به شمار میرود.دارای ویژگی های مهمی همچون، کمک به تجزیه و تحلیل ترافیک و اطلاعات می باشد.
- **Tcpdump** یکی از ابزارهای تجزیه و تحلیل ترافیک در خط فرمان شناخته شده است .توانایی پیگیری و مشاهده TCP / IPو دیگر بسته ها را در هنگام انتقال از طریق شبکه فراهم می کند.
- **WinDump** یک ابزار خط فرمانی است که برای نمایش اطلاعات هدر مناسب است.
- **Dsniff** مجموعه ای از ابزارهای طراحی شده برای حملات اسنیف با پروتکل های مختلف و با هدف سرقت پسوردها میباشد. Dsniff برای سیستم عامل های یونیکس و لینوکس طراحی شده و معادل کامل در سیستم عامل ویندوز ندارد.
- **EtherApe** این یک ابزار لینوکس / یونیکس است که برای نمایش گرافیکی اتصالات ورودی و خروجی سیستم طراحی شده است.

- **NetWitness NextGen** یک Sniffer مبتنی بر سخت افزار، به همراه ویژگی های زیادی میباشد و برای نظارت و تجزیه و تحلیل تمام ترافیک در شبکه طراحی شده است .این ابزار توسط FBI و دیگر سازمان های اجرای قانون استفاده می شود.
- **NetworkMiner**
- **Kismet**
- **Fiddler**
- **EtherApe**
- **Packet Capture**
- **PRTG Network Monitor**
- **Steel Central Packet Analyzer**
- **SolarWinds Packet Analysis Bundle**
- و...

یک نفوذگر می تواند از هر یک از این ابزارهای تست نفوذ برای تجزیه و تحلیل ترافیک در شبکه استفاده کند و اطلاعات را تجزیه و تحلیل کند.

۸. کتابخانه های packet sniffing / analyzing

- **Libcap**
- کد نویسی packet sniffing به کمک socket نیز انجام می شود.

۹. منابع

- http://www.srco.ir/Articles/TipsView.asp?ID=374
- https://kaliboys.com/sniffing/
- https://www.geeksforgeeks.org/what-is-packet-sniffing/
- https://www.paessler.com/it-explained/packet-sniffing
- https://www.coursera.org/learn/intro-cyber-attacks/home/welcome
- https://www.binarytides.com/packet-sniffer-code-c-libpcap-linux-sockets/
- https://www.binarytides.com/packet-sniffer-code-c-linux/