در این پروژه از چه زبانی استفاده میشود ؟

زبانی که من برای انجام پروژه در نظرم گرفتم ، c است . چند دلیل زیر را برای انتخاب خود مطرح میکنم :

- قابلیت پشتیبانی از row socket ها که در پروژه مطرح شد
- پیاده سازی انواع پشته پروتکل ها در آن امکان پذیر است
- به دلیل نزدیکی بیشتر به زبان ماشین ، نسبت به سایر زبان های سطح بالا همانند پایتون ، کار با این زبان در پیاده سازی مفاهیم شبکه ، در آموزش و یادگیری مفاهیم پایه ای تاثیر بسزایی دارد .
- امکان برنامه نویسی سطح پایین شبکه
- یک زبان مادر محسوب شده و کتابخانه ها و مفاهیم شبکه پیاده سازی شده در زبان های دیگر از این زبان مشتق شده اند
- سهولت اجرا در سیستم عامل لینوکس

تحقیق فاز 0

packet analyzing & Packet sniffing چیست ؟

از ابتدای بروز مسائل امنیتی و حملات به سرویس های اینترنتی و کامپیوتری استفاده از فرآیندی موسوم به packet sniffing مورد استفاده قرار گرفته است. هکرها از روش هایی جهت افزایش بسته های اطلاعاتی محرک در طول شبکه استفاده نموده و با آنالیز بسته های افزایش یافته از وجود اطلاعات حساس در یک شبکه مطلع میشوند، پروتکلی نظیر IPSec به منظور پیشگیری این فرآیند طراحی شده است که رمزنگاری بسته های اطلاعاتی را برعهده دارد. حال با استفاده از تکنولوژی IPSec بخش کوچکی از داده ها و بسته های اطلاعاتی رمزنگاری میگردند و همین امر باعث شده است که packet sniffing همچنان یکی از روش های متداول به منظور سرقت اطلاعات باشد. مدیران و ادمین های شبکه به منظور عیب یابی و مشاهده مشکلات ترافیکی به کمک packet sniffer که به عنوان network monitor یا network analyzer نیز یاد میشود، بسته های اطلاعاتی خطاگونه و گلوگاه های حساس شبکه را شناسایی کرده و بستر امن به منظور انتقال داده ها را فراهم می آورند. با

این تعاریف میتوان گفت packet sniffer تمامی بسته های اطلاعاتی ارسال شده از طریق یک اینترفیس مشخص را جمع آوری مینماید تا بررسی و آنالیز آن بسته ها در فرصت مقتضی فراهم گردد، پس برنامه های packet sniffer به منظور جمع آوری بسته های اطلاعاتی مقصدی خاص و یا صرف نظر از مقصد ، مورد استفاده قرار می گیرند.

هکر از طریق تولید یک packet sniffer در شبکه مورد نظر به جمع آوری و آنالیز تمامی ترافیک شبکه میپردازد، باتوجه به اینکه اطلاعات مربوط به نام و رمز عبور به صورت متن معمولی و رمز نشده در شبکه ارسال می گردد با آنالیز ترافیک شبکه امکان مشاهده اطلاعات حساس از این دست برای مهاجمان وجود خواهد داشت. این ترفند تنها قابلیت جمع آوری اطلاعات مربوط به بسته های اطلاعاتی درون یک subnet شبکه را دارد یعنی مهاجم با ایجاد packet sniffer در شبکه خود نمیتواند دسترسی به شبکه میزبان برای جمع آوری اطلاعات و سوء استفاده از آن را داشته باشد، پس این افراد اهداف مخرب خود را با نصب بدافزار ایجاد بسته اضافی برروی یک کامپیوتر موجود در شبکه میزبان عملی مینمایند .با این توضیحات متوجه خواهیم شد که packet sniffing با روش اترنت شبکه موازی کار میکند، به این صورت که هر زمان کامپیوتری یک بسته اطلاعاتی را ارسال می نماید آن بسته به عنوان یک broadcast بوده و بجز کامپیوتر مقصد تمامی دستگاه های موجود در شبکه این بسته را رؤیت کرده و کامپیوتری که مهاجم به آن دسترسی دارد یک کپی از بسته را برای سازماندهی عملیات هکر در خود نگهداری مینماید.

موارد استفاده از Packet Sniffer ها را میتوان به لیست زیر تقسیم کرد :

- تحلیل مشکلات شبکه ای
- تشخیص حمله های نفوذی
- استفاده غیر معمول از شبکه توسط کاربران داخلی و خارجی
- بدست آوردن اطلاعات مربوط به یک شبکه برای نفوذ به آن
- مانیتورینگ پهنای باند شبکه هایWAN
- مانیتورینگ استفاده های کاربران خارجی و داخلی شبکه
- مانیتورینگ داده های موجود در جریان داده یک شبکه
- مانیتورینگ وضعیت های امنیتی شبکهWAN

- جمع آوری و گزارش آمارهای مربوط به شبکه
- فیلتر سازی اطلاعات مشکوک از ترافیک شبکه
- جاسوسی بر روی شبکه های دیگر برای جمع آوری اطلاعات حساس مانند رمزهای عبور
- اشکال زدایی مربوط به ارتباط Client/Server بر روی شبکه
- اشکال زدایی طراحی پروتکل های شبکه

Shared Ethernet

در محیط های اینچنینی همه میزبان ها به یک باس وصل میشوند و برای رفتن پهنای باند با هم رقابت میکنند . در چنین وضعیتی یک پاکت را همه کامپیوتر ها دریافت میکنند . بدین ترتیب وقتی که کامپ یک بخواهد با کامپ دو صحبت کند آن هم در چنین محیطی پاکتش را روی شبکه میگذارد آن هم با ادرس مک سیستم مقصدش به همراه آدرس مک خود . کلیه کامپیوتر ها روی یه اترنت اشتراکی (کامپ های 3 و 4)ادرس مک پاکت مقصد را با ادرس خودشان مقایشه میکنند و اگر این دوتا با هم مچ نباشند این پاکت را دور می اندازند.

کامپیوتری که در حال انجام عمل اسنیف کردن است این قاعده و قانون را میشکند و همه پاکت ها را میگیرد .

و به کل ترافیک شبکه گوش میدهد .

در این وضعیت عمل اسنیف بسیار فعالانه انجام میشود و تشخیص آن بسیار سخت میشود.

Swiched Ethernet

در این شبکه کامپیوتر ها به جای وصل شدن به هاب به یک سوئیچ وصل میشوند که به آن اتنت سئویچ میگویند. سوئیچ جدولی را مدیریت میکند که داخلش رد ادرس مک کارت هایی را که به آن متصلند را دارند . در این جدول آدرس پورت فیزیکی را که روی سوئیچ است و به آن کارت با آدرس مک وصل است را هم نگه میدارد و پاکت های مقصد را روی آن پورت فیزیکی میگذارند و به مقصدش تحویل میدهند . در واقع موقعی که یک پاکت می خواهد ارسال بشود یه مسیر فیزیکی مستقیم و بدون واسطه بین آن و مقصدش برقرار میشود . در واقع سوئیچ ماشین هوشمندی است که میداند با این پاکت هایی که به آن وارد میشوند چه کار کند . به این علت سرعت سوئیچ از هاب بیشتر است و گرانتر نیر است . و همه پاکت ها را برود کست نمیکند . این سبب میشود تا پهنای باند هدر نرود و مصرف پهنای باند بهینه شود و امنیت بالاتر برود . حال اگر کامپیتوری را درون این شبکه قرار دهند در حالت

اسنیفر برای آنکه پاکت ها را جمع کنند این کار عملی نمیشود . به همین دلیل است که مدیران شبکه ها برای امنیت بیشتر این شبکه بندی را ترجیح میدهند.

انواع حملات Packet Sniffing

1- **حالت غیر فعال یا Passive** : مهاجم بر روی کلیه کامپیوترهای یک شبکه LAN نرم افزار شنود را راه اندازی مینماید ، البته باتوجه به افزایش اهمیت امنیت شبکه های کابلی امروزه این روش کمتر رخ میدهد ولی در شبکه های وایرلسی مهاجم با دسترسی به کارت شبکه وایرلس سیستم موجود در مجموعه امکان شنود و Capture اطلاعات را دارد. درگذشته باتوجه به مکانیزم فعالیتی که HUB ها داشتند، داده ها در کلیه پورت ها ارسال و نرم افزار Sniffer امکان شنود کلی و یکجا اطلاعات تبادلی در شبکه را داشتند. در اصطلاح به این نوع حملات Passive Sniffing گفته میشود چون هکر نیازی به انجام هیچ کاری برای دریافت اطلاعات از شبکه ندارد و عملاً کسی متوجه حضور مهاجم نمی شود.

2- **حالت فعال یا Active** : در این حالت تعداد فراوانی MAC Address جعلی به سمت سوییچ از طرف نرم افزار شنود ارسال میگردد و جدول آدرس MAC یا MAC Table سرریز شده که باعث تغییر وضعیت سوییچ به یک HUB خواهد شد، سوییچی که با هاب تبدیل گردیده است ترافیک را بر روی تمامی پورت های خود ارسال می کند و فرآیند شنود راه اندازی میگردد. شنود در این روش برای شبکه های وایرلس نیز ممکن است به اینصورت که درPassive Wireless Sniff ، مهاجم به محض ارسال بسته Access Point به سیستم مورد نظر همزمان درخواست های زیادی را به Access Point ارسال مینماید و این دستگاه مجبور به پاسخگویی شده و در نتیجه امکان شنود آن فراهم خواهد شد. تکنیک های Sniffing فعال عبارتند از MAC Flooding ، DHCP Attacks، DNS Poisoning، Spoofing Attacks و ARP Poisoning .

پروتکل های آسیب پذیر در مقابل حملات Packet Sniffing

با بهره گیری از این سرویس امکان دسترسی امن با رایانه کاری به سرور پست الکترونیکی یا پرونده ها محیا میشود.

- پروتکل HTTP که برای ارسال متن کارایی دارد.
- پروتکل SMTP که اساساً در انتقال ایمیل ها مورد استفاده قرار می گیرد.

- پروتکل NNTP که برای تمامی ارتباطات استفاده می شود و داده ها را بصورت متن واضح یا clear text بر روی شبکه ارسال مبادله مینماید.
- پروتکل POP که دریافت ایمیل از سرور را فراهم میسازد.
- پروتکل FTP که ارسال و دریافت فایل بصورت متن ساده را ممکن مینماید.
- پروتکل IMAP که همچون SMTP در عملیات ایمیل مورد استفاده قرار میگیرد.
- پروتکل Telnet که همه اطلاعات مانند نامهای کاربری و رمزهای عبور را بر روی شبکه به عنوان clear text ارسال می کند.

در حملات sniffing بطور معمول اطلاعات حساس زیر شنود میگردند :

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- پیکربندی روتر یا Router configuration
- جلسات گفتگو یا Chat sessions
- DNS traffic

ابزارهای پرکاربرد Packet Sniffer

با پیشرفت در علوم کامپیوتری ابزارهای متعدی برای sniff شبکه با ویژگی های خاص تولیده شده اند تا تجزیه و تحلیل ترافیک و اطلاعات بر اساس سلیقه افراد امکان پذیر باشد، برخی از این ابزار به شرح زیر میباشند :

- ابزار قدرتمند BetterCAP که انعطاف پذیر و قابل حمل بوده و برای انجام انواع حملات MITM علیه شبکه، دستکاری و HTTP HTTPS همچنین ترافیک TCP به صورت لایو به کار میرود.
- ابزار Ettercap که مجموعه جامع برای حملات میانی میباشد و قابلیت شنود ارتباطات زنده و فیلتر کردن محتوا از جمله ویژگی های آن است.

- ابزار Wireshark که معروف ترین sniffer به شمار میرود و دارای ویژگی کمک به تجزیه و تحلیل ترافیک و اطلاعات میباشد.
- ابزار Tcpdump که تجزیه و تحلیل ترافیک در خط فرمان را عهده دار است و توانایی پیگیری و مشاهده TCP /IP و دیگر بسته ها را در هنگام انتقال در شبکه فراهم میسازد.
- ابزار Dsniff که مجموعه ای از ابزارهای شنود با پروتکل های مختلف با هدف سرقت پسوردها در شبکه برای سیستم عامل های یونیکس و لینوکس را در اختیاز مهاجمان قرار میدهد.
- ابزار EtherApe که برای لینوکس یا یونیکس میباشد و نمایش گرافیکی اتصالات ورودی و خروجی سیستم را طراحی مینماید.

روش های تشخیص packet sniffing در شبکه :

- بررسی سرویس دهنده DNS
- اندازه گیری زمان پاسخ ماشین های مشکوک
- استفاده از ابزار های مختص AntiSniff

Packet analyzing چیست ؟

یکی از حوزه های بسیار مهیج و در حال پیشرفت در شبکه مساله مهم Packet Analysis می باشد. از این فن میتوان در تشخیص مشکلات شبکه و سعی در حل آنها استفاده کرد. هرچند هکر ها نیز میتوانند برای استراق سمق شبکه و پی بردن به راه های نفوذ به آن استفاده کنند. از مهم ترین مبانی آنالیز پکت ها در شبکه Sniff کردن دیتا در شبکه است که با Sniffer ها انجام میگیرد .

کتابخانه های مورد استفاده برای packet sniffing و packet analyzing

1- **Libpcap** : Packet Capture یا PCAP (که به آن libpcap نیز گفته می شود) یک رابط برنامه نویسی کاربردی (API) است که داده های بسته زنده شبکه را از مدل OSI لایه های 2-7 ضبط می کند. تحلیل گرهای شبکه

مانند Wireshark برای جمع آوری و ضبط داده های بسته از یک شبکه ، پرونده های .pcap ایجاد می کنند. PCAP در طیف وسیعی از قالب ها از جمله Libpcap، WinPcap و PCAPng وجود دارد.

از این پرونده های PCAP می توان برای مشاهده بسته های شبکه TCP / IP و UDP استفاده کرد. PCAP منبع ارزشمندی برای تجزیه و تحلیل پرونده و نظارت بر ترافیک شبکه شما است. ابزارهای جمع آوری بسته مانند Wireshark به شما امکان می دهد ترافیک شبکه را جمع آوری کرده و آن را به فرمت قابل خواندن توسط انسان ترجمه کنید. دلایل زیادی برای استفاده از PCAP برای نظارت بر شبکه ها وجود دارد. برخی از رایج ترین آنها شامل نظارت بر استفاده از پهنای باند ، شناسایی سرورهای متقلب DHCP ، شناسایی بدافزار ، وضوح DNS و پاسخ به حادثه است.

2- **Libtins** : یک کتابخانه بسته بندی و ساخت بسته های شبکه C با سطح چند سطح است. هدف اصلی آن فراهم آوردن توسعه دهنده C روشی آسان ، کارآمد ، پلتفرم و مستقل از پایان برای ایجاد ابزارهایی است که نیاز به ارسال ، دریافت و دستکاری بسته های شبکه دارند .

ویژگی های libtins

- ساخت بسته های شبکه
- بو کردن بسته ها و تفسیر بسته های خودکار
- خواندن و نوشتن پرونده های PCAP
- دنبال کردن و جمع آوری مجدد جریان های TCP در حال پرواز
- رمزگشایی WEP و WPA2 (TKIP و CCMP) داده های 802.11 را رمزگذاری کرده است فریم های در حال پرواز و تفسیر محتوای رمزگشایی شده
- حداقل بر روی معماری های زیر به درستی کار می کند: x86، x64، ARM و MIPS (احتمالاً بیشتر)

3- **Libcrafter** : یک کتابخانه سطح بالا برای C است که برای سهولت در ایجاد و رمزگشایی بسته های شبکه طراحی شده است. این امکان را دارد که بسته های متداول پروتکل های شبکه را طراحی و رمزگشایی کند ، آنها را از طریق سیم بفرستد ، آنها را ضبط کرده و درخواست ها و پاسخ ها را مطابقت دهد. این امکان ایجاد ابزارهای شبکه را در چند خط با رابط کاربری بسیار مشابه Scapy فراهم می کند. یک بسته به عنوان لایه هایی توصیف می شود که شما آنها را پشت هم قرار دهید. قسمتهای هر لایه مقادیر پیش فرض مفیدی دارند که می توانید بیش از حد بارگیری کنید. این کتابخانه

برای استفاده در برنامه های چند رشته ای طراحی شده است که می توانید همزمان چندین کار را با هم ترکیب کنید. به عنوان مثال ، شما می توانید به راحتی همزمان با انجام یک حمله ARP-Spoofing چیزی را که بو می کشد ، خرد می کند و می فرستد ، طراحی کنید. همچنین شامل اجرای بسیار ساده TCP است .

منابع

https://www.comparitech.com/net-admin/pcap-guide/

http://libtins.github.io/

https://code.google.com/archive/p/libcrafter/

https://www.techopedia.com/definition/25323/packet-analyzer

https://www.paessler.com/it-explained/packet-sniffing

https://www.parsdata.com/articles/what-is-packet-sniffing