به نام خدا

گزارش کار پروژه درس شبکه های کامپیوتری ترم بهار 1400 -1399

تهیه کننده : محمد لکزایی

کد دانشجویی : 9722762473

فاز صفر :

تهیه گزارش در مورد مفاهیم زیر

1- Packet sniffing

2- Packet analyzing

3- کتابخانه های موجود برای انجام اعمال فوق

Packet snifferچیست و بررسی عملکرد تحلیل گر بسته های شبکه(Packet Analyzers)

تحلیل گر بسته های شبکه که بطور معمول با نام های متفاوتی تعریف می شود، در این مقاله مورد بررسی قرار خواهد گرفت.
ابتدا به این موضوع می پردازیم که Packet sniffer چیست و سپس به بررسی عملکرد آن خواهیم پرداخت.

Packet sniffer چیست ؟

تحلیل گر بسته های شبکه یا آنچه که به طور معمول با نامهایی چون تحلیل گر شبکه (Network Analyzer) ، تحلیلگر پروتکل(Protocol Analyzer) یا Packet sniffer و یا آنچه در شرایطی برای شبکه های خاص با نامهایی چون Ethernet sniffer یا wireless sniffer شناخته می شود در حقیقت یک برنامه نرم افزاری یا قسمتی از سخت افزار کامپیوتر است که میتواند ترافیک شبکه یا بخشی از شبکه را رهگیری و فایل های گزارش بر این اساس تهیه نماید.
هنگامی که جریان داده ها در یک شبکه از مسیری در جریان است ، Snifferبسته های اطلاعاتی در طی این مسیر را گرفته و اگر نیاز باشد ، داده های خام آن بسته را Decode نموده و فیلد های مختلف به همراه داده های آن را از داخل بسته اطلاعاتی استخراج و نمایش میدهد و سپس تحلیل های لازم را بر اساس مشخصات و یا متود های (request for comments)RFC بر روی این اطلاعات انجام میدهد.

قابلیت های Packet Sniffing

در شبکه های LAN بسته به نوع ساختار آن (Hub یا Switch) ، فرد میتواند جریان داده ها بر روی بخشی از این شبکه یا Client خاص بر روی این شبکه را مانیتور نماید ، هر چند متود های وجود دارد که از دسترسی دیگر سیستم های شبکه و احاطه آنها بر روی جریان داده فوق الذکر جلوگیری می نماید. برای مثال میتوان روش ARP Spoofing را مثال زد که در واقع تکنیکی

است که حمله کننده در آن (ARP (Address Resolution Protocol های جعلی را در سطح شبکه LAN ارسال نموده و قصد دارد تا MAC Address خود را به IPAddress میزبانی دیگر نسبت دهد تا ارسال داده ها برای IP آدرس مذکور برای سیستم حمله کننده ارسال شود.

جهت مانیتور کردن یک شبکه حتی میتوان کلیه بسته های اطلاعاتی شبکه LAN را توسط یک سوییچ به همراه یک پورت جهت مانیتورینگ (Monitoring Port) استفاده کرد که می تواند تمام بسته های ارسالی از طریق port های دیگر را هنگام اتصال یک سیستم به یکی از port های سوییچ مورد نظر کپی برداری نماید.

در شبکه های بیسیم Wireless LAN ، میتوان ترافیک شبکه مورد نظر را بر روی یک و یا چندین کانال مختلف مانیتور نمود .

برخی برنامه های Sniffer هنگامی که ترافیک به صورت Multicast ارسال می شود با قرار گرفتن در مد promiscuous mode یا بی قاعده میتوانند همه ترافیک مورد نظر را دریافت نمایند (لازم به ذکر است همه ی Sniffer ها از این مد پشتیبانی به عمل نمی آورند.)

در Sniffer ها اطلاعات دریافتی از داده های خام دیجیتال ، رمز گشایی شده و به زبان قابل خواندن توسط انسان یا در اصطلاح زبان human-readable تبدیل می شوند که به کاربر این اجازه را می دهند که به راحتی اطلاعات رد و بدل شده را تحلیل نمایند. Sniffer ها در نمایش اطلاعات داده ها امکانات مختلفی را برای نمایش اطلاعات به کاربر عرضه میدارند مانند :

- نمایش ریشه خطاهای بوجود آمده
- نمایش نمودار زمانی
- بازسازی داده های TCP وUDP

برخی Sniffer ها خود میتوانند ترافیک ایجاد نموده و خود نقش دستگاه منبع را ایفا نمایند و در تست و تحلیل پروتکل های سیستم کارآمد باشند. این تست کننده ها در برخی مواقع این امکان را به کاربر میدهند تا عمدا برخی خطاها مربوط به DUT را ایجاد نمایند تا کارایی و قابلیت های سیستم در شرایط مشابه بررسی شود.

برخی از تحلیلگر ها نیز ممکن است سخت افزاری باشند ، این سخت افزار ها بسته های اطلاعاتی و یا قسمتی از آن را کپی برداری و بر روی دیسک سخت خود ذخیره می نمایند.

موارد استفاده از Packet Sniffing

موارد استفاده از Packet Sniffer ها میتواند متغییر باشد که در زیر میتوان به آنها اشاره نمود:

- تحلیل مشکلات شبکه ای
- تشخیص حمله های نفوذی
- تشخیص سوء استفاده از شبکه توسط کاربران داخلی و خارجی
- بدست آوردن اطلاعات مربوط به یک شبکه برای نفوذ به آن
- مانیتور کردن پهنای باند شبکه هایWAN
- مانیتور کردن استفاده های کاربران خارجی و داخلی شبکه
- مانیتور کردن داده های موجود در جریان داده یک شبکه
- مانیتور کردن وضعیت های امنیتی شبکهWAN
- جمع آوری و گزارش آمار های مربوط به شبکه
- فیلتر سازی اطلاعات مشکوک از ترافیک شبکه
- جاسوسی بر روی شبکه های دیگر برای جمع آوری اطلاعات حساس مانند رمز های عبور (بسته به نوع رمز نگاری این داده ها)
- مهندسی معکوس داده های بر روی شبکه
- اشکال زدایی مربوط به ارتباط Client/Server بر روی شبکه
- اشکال زدایی طراحی پروتکل های شبکه
- کنترل و تایید سیستم های داخلی از نظر صحت کارکرد مانند Firewallها

برخی از Sniffer های معروف (Packet Analyzers)

- Capsa Network Analyzer
- Cain and Abel
- Carnivore (FBI)
- dSniff
- ettercap
- Fiddler
- Lanmeter
- Microsoft Network Monitor

- NarusInsight
- ngrep Network Grep
- SkyGrabber
- snoop
- tcpdump
- Wireshark

راه های مقابله با Packet Sniffing و Sniffer ها

- یکی از کاربردی ترین راه های مقابله با Sniffing ، استفاده از رمز نگاری در داده های رد و بدل شده در شبکه است و در واقع میتوانید داده های خود را با الگوریتم های معروف Hash نمایید
- استفاده از نرم افزار های AntiSniff که در واقع حضور هر گونه مانیتور بر روی شبکه شما را شناسایی مینمایند مانند برنامه های زیر:

1. sniffdet
2. Sniffer.Detectors
3. ntop

- و در آخر میتوان با استفاده از یک Switch در شبکه هایی مانند Ethernet بسته های موجود در جریان داده های شبکه را به مقصد درست آنها راهنمایی کرد و این کار را نیز میتوان با یک پورت نظارتی و ایجاد یک Mirror انجام داد.

کتابخانه ها :

یکی از کتابخانه هایی که می توان به وسیله ی آن یک packet sniffer را در زبان C کد نویسی کرد Libpcap است .

انتخاب زبان برنامه نویسی برای اجرای پروژه و ذکر دلیل آن :

در مقدمه ی کتاب Packt.Hands-On.Network.Programming.with.C دلایل مفید بودن انتخاب زبان C را برای برنامه نویسی شبکه به شکل زیر بیان شده است .

1- زبان C نسبت به دیگر زبان های سطح بالا شما را به زبان ماشین نزردیکتر می کند .

2- برنامه نویسی شبکه یک موضوع سرگرم کنند است ، در عین حال بسیار عمیق است و دارای سطوح بسیار است . برخی زبان های برنامه نویسی این انتزاع ها را پنهان می کنند . به عنوان مثال ، در زبان برنامه نویسی پایتون می توانید کل صفحه وب را فقط با استفاد از یک خط کد بارگیری کنید . در C اینگونه نیست ! در C ، اگر بخواهید یک صفحه وب را بارگیری کنید ، باید بدانید که همه چیز چگونه کار می کند. شما باید سوکت ها را بشناسید، باید پروتکل کنترل انتقال (TCP) را بدانید و HTTP را بدانید. در برنامه نویسی شبکه با زبان C ، هیچ چیز پنهان نیست.

3- C یک زبان عالی برای یادگیری برنامه نویسی شبکه است. این فقط به این دلیل نیست که همه جزئیات را می بینیم ، بلکه همچنین به این دلیل است که سیستم عامل های محبوب همه از هسته های نوشته شده در C استفاده می کنند. هیچ زبان دیگری همان دسترسی سطح اول را به شما نمی دهد . در C ، همه چیز تحت کنترل شما است - شما می توانید ساختار داده های خود را به طور دقیق تنظیم کنید. شما می توانید ، دقیقاً حافظه را مطابق میل خود مدیریت کنید

4- استفاده از زبان برنامه نویسی C در همه جا وجود دارد. تقریباً هر پشته شبکه در زبان C برنامه نویسی شده است . این موضوع برای ویندوز ، لینوکس و macOS هم صدق می کند. اگر تلفن همراه شما از Android یا iOS استفاده می کند ، حتی اگر برنامه های این برنامه به زبان دیگری برنامه ریزی شده باشند (Java and Objective C) ، هسته و کد شبکه به زبان C نوشته شده است. به احتمال زیاد روترهای شبکه که داده های اینترنت شما از آنها عبور می کنند با C برنامه ریزی می شوند. حتی اگر رابط کاربری و عملکردهای سطح بالاتر مودم یا روتر شما به زبان دیگری برنامه ریزی شده باشد ، درایورهای شبکه هنوز هم احتمالاً در C پیاده سازی می شوند.

منابع فاز اول پروژه :

1- کتاب Packt.Hands-On.Network.Programming.with.C

2- https://www.binarytides.com/packet-sniffer-code-c-libpcap-linux-sockets/

3- https://iranhost.com/blog/بررسی-عملکرد-تحلیل-گر-بسته-های-شبکه-packet-analyzers/