# مقدمه ای بر packet sniffing و packet analyze

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

2 - 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 های WAN  
• مانیتورینگ استفاده های کاربران خارجی و داخلی شبکه  
• مانیتورینگ داده های موجود در جریان داده یک شبکه  
• مانیتورینگ وضعیت های امنیتی شبکه WAN  
• 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

3 - انواع حملات Packet Sniffing

1. حالت غیر فعال 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 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 در Passive 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.

لینک git

https://github.com/mahditavakoli1312/network.git