تشخیص Packet Sniffing در یک شبکه

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 ، ساختیافته 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 جهت 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 . این موضوع در رابطه با packet sniffing نیز صدق می کند .

packet sniffing چیست ؟

یکی از قدیمی ترین روش های سرقت اطلاعات در یک شبکه ، استفاده از فرآیندی موسوم به packet sniffing است . در این روش مهاجمان از تکنیک هائی به منظور تکثیر بسته های اطلاعاتی که در طول شبکه حرکت می کنند ، استفاده نموده و در ادامه با آنالیز آنان از وجود اطلاعات حساس در یک شبکه آگاهی می یابند . 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 اینترفیش مشخص شده در شبکه ارسال می گردند را جمع آوری 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 sniffer packet 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 .

نحوه کار packet sniffing

نحوه کار packet sniffing به روشی برمی گردد که شبکه های اترنت بر اساس آن کار می کنند . در یک شبکه اترنت ، هر زمان که کامپیوتری یک بسته اطلاعاتی را ارسال می نماید ، بسته اطلاعاتی به عنوان یک broadcast ارسال می گردد . این بدان معنی است که هر کامپیوتر موجود در شبکه بسته های اطلاعاتی ارسالی را مشاهده نموده و بجزء کامپیوتر مقصد سایر دستگاه های موجود از بسته اطلاعاتی صرفنظر خواهند کرد . sniffing packet با کپی یک نسخه از بسته های اطلاعاتی ارسالی در شبکه، فعالیت خود را سازماندهی می نماید .

آیا روش هائی به منظور تشخیص وجود یک packet sniffer در شبکه وجود دارد ؟

تشخیص وجود یک packet sniffer بر روی شبکه کار آسانی نخواهد بود . برنامه های فوق به صورت passive در شبکه عمل نموده و به سادگی اقدام به جمع آوری بسته های اطلاعاتی می نمایند .خوشبختانه ، امروزه با استفاده از روش هائی می توان وجود احتمالی یک packet sniffer را در شبکه تشخیص داد .

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 Network Monitor Users Identify 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 Network Monitor 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 DNS lookup 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 packet sniffing 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** sniffing packet **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 .**