

بسم الله الرحمن الرحيم

نگاهی بر Sniffer ها

مقدمه:

امنیت در شبکه های کامپیوتری و امن ماندن اطلاعات منتقل شده از کامپیوتری به کامپیوتر دیگر از نگرانی های مسئولان این شبکه ها است. در این مقاله نگاهی بر یکی از ابزارهای تهدید امنیت شبکه های کامپیوتری به نام Sniffer ها و راه های مقابله با آن ها را بررسی خواهیم کرد. همچنین در آخر مقاله ، چند Sniffer معروف را با توضیحات کوتاهی معرفی خواهیم کرد. اگر می خواهید راه های مقابله با این برنامه ها را به طور کامل یاد بگیرید ، باید نگاهی به مقالات و کتاب های جامع امنیتی بیندازید.

Packer Sniffer چیست؟

Packer Sniffer برنامه ای است که ترافیک و اطلاعات رد و بدل شده در شبکه را کنترل می کند. Packet Sniffer ای که بر روی کامپیوتر شما در حال اجرا باشد و شما به وسیله ی یک مودم به اینترنت وصل شده باشید ، می تواند به شما IP فعلی تان را به همان خوبی بگوید که آدرس های IP سایت هایی را که شما بازدید می کنید را می گوید. شما می توانید تمامی اطلاعات رمزنگاری نشده را که از کامپیوتر شما به اینترنت منتقل می شود را نگاه کنید. این اطلاعات شامل کلمات عبور و سایر اطلاعاتی می شود که به صورت رمزنگاری شده در آورده نشده اند. شما می توانید تمامی اطلاعاتی را که از به وسیله ی Router منتقل می شوند را با قراردادن یک Packet Sniffer درون یک Router در آن ببینید. این اطلاعات شامل اطلاعات خاصی می شوند که هر فرد به وسیله ی این Router منتقل می کند. Sniffer ها در واقع برنامه هایی هستند که جلوی اطلاعات را می گیرند. آن ها به این دلیل که اترنت بر اساس قسمتی از اشتراک گذاری عمده ساخته شده است ، کار می کنند. یعنی عمده ی کار اترنت اشتراکی است. بیشتر شبکه ها از چیزی که به عنوان تکنولوژی Broadcast شناخته شده است ، استفاده می کنند ، به این معنی که هر پیامی که توسط یک کامپیوتر دز یک شبکه منتقل می شود ، توسط دیگر کامپیوترهای موجود در آن شبکه نیز می تواند خوانده شود. در واقع ، همه ی کامپیوترهای دیگر ، منتظر یک پیام هستند و اگر پیامی برای آن ها مفهومی نداشته باشد ، آن را نمی پذیرند. به هر حال ، کامپیوتر ها می توانند به وسیله ی Sniffer پیام هایی را برای قبول کردن درست کنند در حالی که ، حتی اگر پیامی برای آن ها مفهومی نداشته باشد. به طور معمول ، Sniffer برنامه ای تاثیر پذیر است ، به طوری که فقط اطلاعات را جمع آوری می کند. به همین دلیل به شدت پیدا کردن یک Sniffer سخت است. وقتی که یک Sniffer بر روی کامپیوتری نصب شود ، مقدار کوچکی از ترافیک شبکه را به خود اختصاص می دهد و به وجود می آورد ، و به این ترتیب ، قابل شناسایی است. البته در صورتی این کار امکان پذیر است که Sniffer در حال اجرا باشد. چند روش پیدا کردن یک Sniffer در زیر توضیح داده شده است :

1) Ping Method:

روشی که در اینجا استفاده شده است ، به گونه است که یک درخواست ping به آدرس IP ماشین مورد نظر و نه آدرس MAC آن فرستاده می شود. به صورت ایده آل و طبیعی ، هیچ ماشینی نباید این پکت را ببیند ، همان گونه که هر Ethernet Adaptor ای از زمانی که آدرس MAC ارسالی آن با آدرس های MAC موجود در شبکهو آدرس مقصد یکسان نباشد ، آن را پس می زند. حال اگر بر روی ماشینی Sniffer در حال اجرا باشد ، این پکت را با این وجود که آدرس MAC مقصد متفاوتی از آدرس MAC دستگاهی که بر روی آن در حال اجرا است را دارد ، پس نمی زند و نگه می دارد. طبق همان چیزی که گفته شد ، اگر پکتی برای کامپیوترهای عادی مفهومی نداشته باشد آن را پس می زنند اما برای یک Sniffer چنین چیزی صدق نمی کند و تمامی پکت ها را جمع آوری می کند. این یک روش قدیمی است.

2) Address Resolution Protocol (ARP) Method:

در این روش ، ما می توانیم ARP غیر Broadcast را به ماشینی که ARP ها را نگه می دارد ، ارسال کنیم. ماشین در این حالت آدرس ARP شما را ذخیره می کند. همراه این درخواست آدرس IP و آدرس MAC شما نیز فرستاده می شود. سپس ، ما با آدرس IP خودمان اما با آدرس MAC متفاوتی ، یک پکت ping از نوع Broadcast به آدرسی ارسال می کنیم. حال تنها ماشینی قادر به دریافت درخواست ما خواهد بود که آدرس IP ما را از ARP دزدیده شده به دست آورده باشد. پس بر روی این ماشین یک Sniffer نصب است.

3) On Local Host:

هنگامی که کامپیوتر شما شناسایی شد ، هکرها سعی در خارج کردن Sniffer و نصب آن بر روی دیگر کامپیوترها را دارند. بر روی کامپیوتر میزبان ، ifconfig را اجرا کنید.

4) Latency Method:

این روش بر پایه ی فرضیه بنا شده است که بیشتر Sniffer ها تجزیه می شوند. در این روش به آسانی با بررسی مقدار زیادی از اطلاعات را که در شبکه فرستاده شده اند ، نتیجه ی ping ماشین هدف و زمان انتقال اطلاعات ، می توان فرضی را مبنی بر این که بر روی کدام کامپیوتر یک Sniffer در حال اجرا است دست یافت. اگر بر روی ماشینی یک Sniffer نصب شده باشد ، زمان اضافه ای را بعد از ping کردن برای پاسخ به آن نسبت به دیگر کامپیوترها خواهد برد. این زمان در واقع همان زمانی است که Sniffer برای گرفتن و نشان دادن محتویات پکت صرف می کند. البته زمان جواب دادن یک کامپیوتر به ping بستگی به فاصله از طرف کامپیوتر ping کننده ، نوع کابل ، نوع شبکه دارد.

راه جلوگیری از اجرای درست یک Sniffer:

بهترین راه برای امن کردن شبکه از Sniffer ، رمزبندی اطلاعات رد و بدل شده در شبکه است. تا زمانی که این کار اتفاق نیفتد ، نمی توان مطمئن شد که آیا در یک شبکه Sniffer در حال اجرا است یا نه.

معروف ترین Sniffer ها:

در زیر نام چند Sniffer معروف به همراه توضیح کوتاهی در مورد هر یک آورده شده است :

1) TCP Dump:

این برنامه یکی از قدرتمندترین Sniffer ها است که به ما اجازه می دهد تا پکت های موجود در شبکه را به آسانی مشاهده کنیم. این Sniffer بعد از دزدیدن پکت ، بررسی های مقدماتی و استاتیکی را از پکت ها دزدیده شده به ما می دهد. یکی از قابلیت های TCP Dump ، تهیه گزارش از نتیجه ی دزدیدن پکت ها است. همچنین خد ما می توانیم برای کنترل ترافیک شبکه به طور جداگانه اسکرپیت های مختلفی نوشته و برای اجرا به Sniffer بدهیم.

2) Sniffit:

این برنامه ، Sniffer ساده همراه با فیلترینگ خوب ترافیک شبکه می باشد.

3) Ethereal:

این برنامه در واقع یک بررسی کننده ی پروتکل ها برای ویندوز و یونیکس است. این برنامه اجازه ی بررسی اطلاعات دزدیده شده از یک شبکه ی زنده و یا از درون یک فایل موجود بر روی کامپیوتر میزبان را می دهد.

4) Hunt:

اولین نسخه از این Sniffer برای استفاده از آسیب پذیری های شناخته شده در پروتکل TCP/IP بود.

5) Dsniff:

این Sniffer مجموعه ای از ابزارها برای تست کردن و یافتن آسیب پذیری های موجود در شبکه است. Dsniff ، Filesnarf ، Mailsnarf ، msgsnarf ، webspay از جمله ابزارهای موجود در این مجموعه می باشند که برای دزدیدن اطلاعات مهمی همچون کلمه ی عبور به کار می روند. arpspoof ، dnsspoof ، macof از دیگر ابزارهای موجود در این مجموعه برای Spoof کردن و یا دزدیدن اطلاعاتی مانند اطلاعات موجود در لایه ی 2 پروتکل TCP/IP که اطلاعات را در شبکه از کامپیوتری به کامپیوتر دیگر منتقل می کند به کار می روند. webmitm و sshmitm ابزارهای حمله هستند که در این مجموعه قرار دارند و برای دسترسی به Session های SSH و HTTPS فعال هستند به وسیله ی استفاده از آسیب پذیری های موجود در آن ها به کار می روند.

منابع :

<http://www.securitysoftwaretech.com/antisniff/tech-paper.html>

<http://www.robertgraham.com/pubs/sniffing-faq.html>

<http://www.fernando.org.uk/sniffer.html>

<http://www.linuxjournal.com>

Copyright© by Siahacker
2005-2006 All Rights Reserved
Email:Siahacker@gmail.com