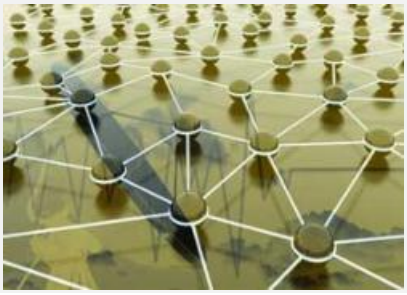

دوشنبه 25 اردیبهشت 1391 - 07:48

استراق سمع در محيط مجازي

در شماره قبل با انواع حملات شبکه‌ای آشنا شديم؛ در اين مطلب می‌خواهيم جزئيات بيشتري، بويژه درباره حملات استراق سمع را مورد بررسی قرار دهيم.

جام جم آنلاين: در شماره قبل با انواع حملات شبکه‌ای آشنا شديم؛ در اين مطلب می‌خواهيم جزئيات بيشتري، بويژه درباره حملات استراق سمع را مورد بررسی قرار دهيم.
استراق سمع (sniffing)

به دريافت پکت‌های شبکه در حال ارسال، استراق سمع و به برنامه‌ای که اين کار را انجام می‌دهد sniffer گفته می‌شود. پروتکل‌هايی مانند HTTP، SMTP، NNTP، FTP، Relogin، Telnet و IMAP همگی از طريق اين حمله آسيب‌پذيرند، چراکه در اين پروتکل‌ها، ارسال اطلاعات به صورت متن ساده انجام می‌شود.

استراق سمع هم می‌تواند به صورت قانونی باشد (مثلا برای نظارت بر ترافيک شبکه يا مسائل امنيتی) و هم به صورت غيرقانونی (برای سرقت اطلاعاتی مانند رمز عبور يا فايل‌های شبکه).

برنامه‌های زيادی برای اين کار توليد شده است و شما هم می‌توانيد به صورت Command Line و هم به صورت واسط گرافيکی از آنها استفاده کنيد.

بسياری از مهندسان شبکه، متخصصان امنيت و حتی هکرها از اين ابزار برای استراق سمع استفاده می‌کنند و همچنين از اين تکنيک برای هک‌کردن اخلاقی (Ethical Hacking) نيز استفاده می‌شود. در ادامه به بررسی جزئيات روش‌های استراق سمع می‌پردازيم.

رايانه‌های يک شبکه فعال هميشه در حال ارسال و دريافت اطلاعات هستند. اگر رايانه‌ها به صورت LAN از يک شبکه اشتراکی استفاده کنند از طريق HUB به يکديگر متصلند و اگر شبکه سوئيچی استفاده شود، بايد از يک (يا چند) سوئيچ استفاده کنند؛ در هر حالت snifferها با روش‌های متفاوت عمل می‌کنند.

در شبکه‌هايی که از HUB استفاده می‌شود، فريم‌ها و پکت‌ها را به همه دستگاه‌های موجود در شبکه می‌فرستد و به اصطلاح broadcast می‌کند؛ هر دستگاه با دريافت فريم، آدرس گيرنده را چک می‌کند و اگر با آدرس خود يکی بود آن را قبول می‌کند و اگر نباشد از دريافت آن صرف نظر می‌کند.

در چنين شبکه‌ای، هکر فقط بايد خود را به گونه‌ای به HUB متصل کند تا جزئی از شبکه شود و از آن به بعد خود به خود فريم‌ها را دريافت می‌کند بنابراين می‌تواند فريم‌های قربانی را نيز پردازش کند.

برای انجام اين کار او به ابزار استراق سمع نياز دارد تا بدون اين‌که شناسايی شود، ترافيک قربانی را بخواند.

شبکه‌هايی که از سوئيچ استفاده می‌کند، عملکرد متفاوتی دارد و در آنها از انتشار داده‌ها برای ارسال آنها استفاده نمی‌شود. در عوض، سوئيچ فريم‌ها را با توجه به آدرس گيرنده، آن را به مقصد می‌فرستد و بقيه دستگاه‌ها از اين ترافيک کاملا بی‌خبرند بنابراين يک هکر علاوه بر اين‌که بايد به سوئيچ متصل باشد، راه‌حلی پيدا کند که سوئيچ داده‌های را که بايد به دستگاه قربانی بفرستد را از طريق هکر ارسال کند.

راه حل متداولی که برای اين حمله وجود دارد ARP poisoning نام دارد که از اين طريق سوئيچ را فريب می‌دهند. همچنين راه‌هايی مانند DHCP spoofing، سرقت درگاه وDNS spoofing نيز ممکن هستند.

در شبکه‌های محلی بی‌سيم، تعدادی دستگاه از طريق امواج راديويی به يک access point متصل می‌شوند که معمولا با استفاده از سيم به يک HUB يا سوئيچ متصل است.

يک شبکه بی‌سيم ممکن است بدون هيچ امکانات امنيتی و بازدارنده‌ای به هر دستگاه اجازه دهد به شبکه وارد شود يا ممکن است با استفاده از ابزارهای امنيتی و رمزگذاری، فقط به تعدادی دستگاه خاص که رمز دارد، اجازه ورود به شبکه را بدهد.

در چنین شبکه‌ای، هکر باید مانند یک شبکه سیمی همان مراحل را طی کند، با این تفاوت که باید اول سعی کند وارد شبکه شود. اگر شبکه امن نباشد هکر فقط باید یک کارت شبکه بی‌سیم داشته باشد و در حوزه دید access point باشد تا بتواند براحتی وارد شبکه شود.

اما اگر شبکه امن باشد و رمزگذاری شده باشد، هکر اول باید کلید را پیدا کند و بعد می‌تواند وارد شبکه شود که البته به دست آوردن کلید شبکه با توجه به الگوریتم رمزگذاری و طول و پیچیدگی کلید ممکن است کار ساده یا دشواری باشد.

وقتی که هکر وارد شبکه بی‌سیم شد، به صورت نامحسوس مشغول دریافت پکت‌های شبکه می‌شود. اگر access point به یک متصل باشد بدون کارهای اضافی می‌تواند پکت‌ها را دریافت کند.

اما اگر access point به یک سوئیچ وصل شده باشد، باید از ARP poisoning و حملات مشابه استفاده کند تا حمله خود را کامل کند. در چنین شبکه‌ای تنظیمات access point اهمیت بسیاری دارد تا جلوی چنین حملاتی را بگیرد.

استراق سمع در اینترنت

بسته‌ها و پکت‌هایی که از طریق شبکه اینترنت به مقصد می‌رسد از روترهای زیادی عبور می‌کند. در چنین شبکه‌ای، هکر در یک شبکه محلی مانند مثال‌های قبل نیست و به قربانی دسترسی مستقیم ندارد.

برای استراق سمع در چنین شرایطی هکر دو راه دارد. اولین راه این است که هکر از نقاط ضعف پروتکل مسیریابی BGP سوءاستفاده کند.

وقتی یک کاربر می‌خواهد سایتی را ببیند، سرور DNS به رایانه کاربر آدرس IP مقصد را می‌دهد. این IP در جدول BGP ارائه‌کننده خدمات اینترنت شما بررسی می‌شود تا بهترین مسیر برای انتقال داده‌ها مشخص شود.

با این حال BGP بر اساس اعتماد کار می‌کند و به همه ارائه‌کنندگان خدمات اینترنت یا شبکه اجازه می‌دهد برای هر مبدأ یک محدوده IP یا مسیر را پیشنهاد کنند.

یک هکر می‌تواند با پیشنهاد یک مسیر برای یکی از گره‌های مسیر قربانی که داده‌ها را از طریق هکر عبور می‌دهد، مسیر انتقال داده‌ها را در دست بگیرد و استراق سمع را شروع کند.

دوم این‌که مدیر شبکه یک سرویس‌دهنده اینترنت، به تمام روترهایش دسترسی کامل دارد و محتوای داده‌هایی را که از آنها می‌گذرد می‌تواند بخواند؛ بنابراین مدیر این شبکه می‌تواند بدون اجازه فرستنده و گیرنده، محتوای پکت‌های رمزگذاری نشده را ببیند.

جلوگیری از استراق سمع

در هر شبکه، با توجه به تنوع آن، جلوگیری از استراق سمع، روش متفاوتی دارد. برای مثال شبکه‌هایی که از HUB استفاده می‌کنند، ذاتاً به این نوع حمله آسیب پذیرند.

برای این‌که در چنین شبکه‌اي استراق سمع کرد باید کارت شبکه را در حالت promiscuous قرار داد. در این حالت دستگاه همه پکت‌ها را از خود عبور می‌دهد و می‌تواند آنها را بخواند و حتی پکت‌هایی را نیز که گیرنده آن نیست، دریافت کند.

برای جلوگیری از این کار ابزارهایی مانند Anti Sniff است که در یک شبکه چنین دستگاه‌هایی را شناسایی می‌کند.

برای شبکه‌هایی که از سوئیچ استفاده می‌کنند، باید اول نوع حمله مشخص شود تا راه مناسب آن ارائه شود. برای مثال اگر از روش ARP poisoning استفاده شود، در این روش هکر از ضعف پروتکل ARP استفاده می‌کند که با استفاده از ابزارهای دفاعی در لایه شبکه و برنامه‌هایی مانند Xarp در رایانه‌ها می‌توان جلوی دستکاری جدول ARP از راه دور را گرفت.

در شبکه‌های بی‌سیم، به علت این‌که شبکه در حوزه خود برای همه قابل دسترسی است، کمی‌آن را در معرض خطر قرار می‌دهد.

برای جلوگیری از ورود افراد بیگانه به شبکه باید از روش‌های رمز گذاری قابل اعتماد مانند WPA استفاده کرد و از آنجا که رمز این پروتکل‌ها از لحاظ تئوری قابل شکستن است، باید از کلیدهای بزرگ (حداقل 128 بیت) و از کلمات عبور قوی استفاده کرد.

بعلاوه باید شبکه را مانند یک شبکه سوئیچی که در قسمت قبل توضیح داده شد نیز نسبت به این حملات مقاوم کرد.

محمدعلی زارعی‌فر