یکشنبه 13 بهمن 1387 - 08:51

انواع حمله‌های کامپیوتری چیست؟

هر کامپیوتری که عضوی از شبکه است، نسبت به حملات کامپیوتری آسیب‌پذیر است.

حمله کامپیوتری زمانی رخ می‌دهد که یک یا چند هکر، برای نفوذ به یک سیستم یا شبکه، با مطالعه و شناسایی رخنه‌های امنیتی سعی در شکستن موانع ورود به آن شبکه می‌کنند.

حمله کننده‌ها می‌توانند با سرعت بسیار زیادی میلیون‌ها کامپیوتر در یک شبکه را آلوده سازند یا مورد حمله قرار دهند. در بزرگترین شبکه جهان، اینترنت، بعضی از شایع‌ترین حملات در هر ثانیه ده‌ها کامپیوتر را آلوده می‌سازد. حملات در اینترنت معمولاً از کامپیوترهایی که آلوده به ویروس هستند کنترل می‌شود و در بیشتر مواقع کاربر نمی‌داند که هکرها کامپیوترش را به خدمت درآورده‌اند و از آن برای انجام حملات به کامپیوترهای دیگر استفاده می‌کنند.

اولین قدم برای مقابله با حملات کامپیوتری، شناخت مقاصد هکرها و روش‌های حمله است.

اهداف حملات را می‌توان به صورت زیر دسته بندی کرد:

- دسترسی به اطلاعات یک سیستم کامپیوتری
- دستبرد به اطلاعات حساس و محرمانه‌ای که در دل یک کامپیوتر نگه‌داری می‌شود
- مطالعه و سرقت اطلاعات شخصی کاربران
- سرقت اطلاعات بانکی
- مطالعه و زیرنظر گرفتن یک سازمان به صورت غیر مجاز
- ایجاد اختلال در یک سرور
- به کارگرفتن کامپیوتر افراد به عنوان سپر
- ورود به اتصال اینترنتی که پهنای باند زیادی دارد

انواع حملات نیز بستگی به مقاصد هکرها دارد. حملات زیر چند مثال از شایع‌ترین و خطرناک‌ترین حملات مشاهده شده‌هستند:

- دسترسی به بدنه اصلی سیستم (Physical Access): این حملات به صورت مستقیم و با حضور فیزیکی هکر در یک شبکه صورت می‌گیرد. هکرها به این ترتیب می‌توانند حملاتی مانند قطع کردن برق شبکه، تخریب فیزیکی قطعات، دزدیدن هارددیسک‌ها و ابزار ذخیره اطلاعات، و مانیتور کردن ترافیک شبکه را انجام دهند.
- قطع کردن ارتباط (Communication Interception): می‌تواند شامل Session Hijacking، تغییر هویت هکر به عنوان یکی از اعضای شبکه (Identity Spoofing) و تغییر مسیر دادن به بسته‌های دیتا باشد. Session Hijacking روشی است که در آن هکر خود را به عنوان مسئول و مدیر شبکه جا می‌زند و کنترل تمام بخش‌های شبکه را به دست می‌گیرد. حملات فیشینگ هم زیرمجموعه‌ای از همین نوع حملات است.
- Denial Of Service: معمولاً هدف اصلی این حملات مسيرياب و صفحات پيكربندی آن‌هاست. بعضي از مسيرياب‌ها در صفحه پيكربندي خود نوعي دستور دارند كه به يك استفاده كننده مشخص، اجازه فرستادن درخواست‌هاي مكرر براي دسترسي به حجم زيادي از اطلاعات را نمي‌دهد.با اين كار از كندشدن سرورها براي مدت طولاني و ايجاد ترافيك در شبكه جلوگيري مي‌شود.

در سال 2000 حمله‌هايي به چند سايت معروف مانند yahoo و MSN توسط هكرها انجام شد. حمله كننده‌ها از اين پيش‌فرض مسيرياب‌ها اطلاع داشتند. آنها برنامه‌اي را روي تعدادي كامپيوتر ارسال كردند كه كار اصلي حمله را بر عهده داشتند.اين برنامه‌ها به هر كدام از بسته‌هاي ديتا كه از كامپيوتر به سمت مسيرياب و سرور مي‌رفت آدرس IP مستقلي مي‌دادند. هر بار كه اين برنامه‌ها به طور همزمان اجرا مي‌شد؛ سرورها براي ساعت‌ها مشغول پاسخگويي به حجم زيادي از درخواست‌ها مي‌شدند كه بسيار بيشتر از ظرفيت‌شان بود و به اين‌ترتيب حمله موسوم به Denial Of Service به سرورهاي اين سايت‌ها انجام مي‌شد.

- دسترسی غیرمجاز به شبکه (Intrusion): یکی از معمول‌ترین ابزار این حملات، اسکن کردن پورت‌هاست. روش دیگر، بدست آوردن سطوح دسترسی غیرمجاز با فرستادن درخواست‌هایی است که توسط مدیر و طراح وب‌سایت، سرور و یا شبکه پیش‌بینی نشده‌است. حملات Buffer Overflow نیز با همین روش کار می‌کند. ویروس‌های مخرب نیز می‌توانند این اهداف را دنبال کنند.
- "بزرگترین تهدید خود کاربر است!"، این شعار متخصصان امنیت شبکه است. به سادگی می‌توان دید که اگر اطلاعات لازم برای یک حمله توسط خود کاربر به هکر داده‌شود، هیچ راهی برای نجات کاربر و مقابله با نفوذ هکر به شبکه وجود نخواهد داشت.
- Trapdoors: هکرها با استفاده از Backdoor یا رخنه امنیتی یک برنامه به کامپیوترها و شبکه‌ها وارد می‌شوند. رخنه‌ها معمولاً به دلیل سهل‌انگاری برنامه‌نویسان و عدم اطلاع از خطاهای برنامه‌نویسی خطرناک ایجاد می‌شوند.

با این که انواع متعدد و پیچیده‌ای از حملات وجود دارند، ولی شرکت‌های امنیتی سایبر تمام ابزار مقابله با هکرها را معمولاً در یک یا دو نرم‌افزار جا می‌دهند. به همین دلیل نیز موثرترین راه ایمن ماندن در برابر حملات، استفاده از نسخه‌های اصل نرم‌افزارهای امنیتی، مرورگرهای معتبر و ایمن، و شناخت و مطالعه وب‌سایت‌ها و پایگاه‌های اینترنتی حاوی مطالب مخرب است.[روش‌هایی برای حفظ حریم شخصی در دنیای مجازی]

یکی دیگر از نگرانی‌های متخصصان امنیت سایبر، رواج شبکه‌ها بی‌سیم است. در چند سال اخیر، مهندسان شبکه رخنه‌های متعددی در شبکه‌های بی‌سیم یافته‌اند،

به‌طوری که در بعضی مواقع، کاربران مبتدی نیز می‌توانند از رخنه‌های شبکه بی‌سیم عبور کنند.

همشهری آنلاین- رشید عسگری