فصل چهارم

هک سیستم

مقدمه

در این فصل، در مورد جنبه‌های مختلف هک سیستم بحث خواهیم کرد. به یاد بیارید که چرخه هک شامل شش مرحله است. که در این فصل، در مورد پنج مرحله دیگر از چرخ هک که شامل شکستن پسورد، افزایش سطح دسترسی، اجرای برنامه‌ها، مخفی کردن فایل‌ها و پاک کردن رد پا بحث خواهیم کرد.

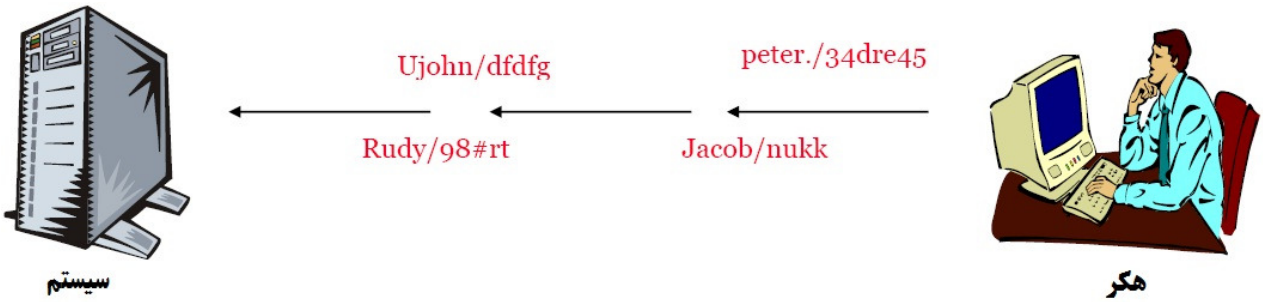
تکنیک‌های شکستن پسورد

پسوردها، شاه کلیدی از اطلاعات مورد نیاز برای دسترسی به سیستم است. زمانیکه کاربران، پسورد را ایجاد می‌کنند، معمولا پسوردی را انتخاب می‌کنند که قابلیت شکستن دارد. بسیاری از مردم، پسوردی را انتخاب می‌کنند که ساده باشد مثلا نام سگ‌شان را به عنوان پسورد انتخاب می‌کنند تا به خاطر آوردن آن ساده‌تر باشد. بخاطر این فاکتورهای انسانی، شکستن بسیاری از پسوردها موفقیت آمیز است و نقطه آغازی برای افزایش سطح دسترسی، اجرای برنامه‌ها، مخفی‌سازی فایل‌ها، و از بین بردن ردپا به شمار می‌رود. پسوردها می‌توانند بصورت دستی شکسته شوند و یا اینکه با استفاده از ابزارهایی از قبیل روش دیکشنری یا brute-force، بصورت اتوماتیک شکسته شوند.

شکستن دستی پسورد، شامل تلاش برای ورود به سیستم با پسوردهای مختلف است. هکر مراحل زیر را انجام می‌دهد:

۱. حساب کاربری معتبری را پیدا می‌کند (مثل Administrator یا Guest).
۲. لیستی از پسوردهای ممکن را تهیه می‌کند.
۳. پسوردها را به ترتیب احتمال مرتب می‌کند.
۴. پسوردها را امتحان می‌کند.
۵. تا جائی ادامه می‌دهد که پسورد صحیح را پیدا کند.

هکر می‌تواند فایل اسکریپتی تهیه کند که پسوردهای موجود در لیست را امتحان کند. این روش، کرک کردن پسورد بصورت دستی است که زمان گیر است و در بسیاری از موارد موفقیت آمیز نیست.



یک روش موثر برای شکستن پسورد، دسترسی به فایل حاوی پسوردها در سیستم است. بسیاری از سیستم‌ها، پسورد را برای ذخیره بر روی سیستم، hash می‌کند. در طول فرآیند ورود به سیستم، نام کاربری با استفاده از همان الگوریتم، hash می‌شود و سپس با پسوردی که قبلا بصورت hash در یک فایلی ذخیره شده است مقایسه می‌شود. هکر می‌تواند تلاش کند که به جای اینکه پسورد را حدس بزند، به الگوریتم hash که در سرور ذخیره شده است دسترسی پیدا کند و به پسوردهای ذخیره شده بر روی سرور دسترسی داشته باشد.

در سیستم ویندوزی، پسوردها در فایل SAM و در سیستم لینوکسی در فایل shadow ذخیره می‌شوند.

ابزارهای هک

Legion، حدس زدن پسورد را بصورت اتوماتیک در نشست‌های NetBIOS انجام می‌دهد. چندین بازه از آدرس‌های IP را اسکن می‌کند تا shareهای ویندوزی را پیدا کند و همچنین دارای ابزارهای حمله دیکشنری دستی نیز هست.

NTInfoScan، یک اسکنر امنیتی است که برای ویندوز NT 4.0 است. NTInfoScan، اسکنر آسیب پذیری است که گزارش‌هایی به فرمت HTML برای مشکلات امنیتی موجود در سیستم هدف تولید می‌کند.

Smbbf، ابزار بررسی SMB است که ابزاری برای بررسی پسوردها در ویندوز است. این نرم‌افزار، در هر دقیقه، ۵۳۰۰۰ پسورد را چک می‌کند.

L0phtCrack، بسته‌ای برای بررسی و بازیابی پسورد است. این نرم‌افزار، دارای قابلیت‌های حملات dictionary، brute-force، و hybrid است.

John the Ripper، ابزاری دستوری است که برای شکستن پسوردهای Unix و NT است. پسوردهای شکسته شده، بصورت case insensitive هستند که ممکن است پسورد واقعی نباشند.

KerbCrack، شامل دو برنامه است: kerbsniff و kerbcrack. که kerbsniff برای گوش دادن به شبکه و بدست آوردن لاگین‌های Windows 2000/XP است و kerbcrack، برای یافتن پسوردهای فایل بدست آمده با استفاده از حملات brute force و dictionary است.

LanManager Hash

ویندوز ۲۰۰۰، از NT Lan Manager (NTLM) hashing برای امن کردن پسوردها در طول ارسال استفاده می‌کند. بسته به پسورد، NTLM hashing می‌تواند ضعیف باشد. برای مثال، پسورد 123456abcdef ضعیف است. زمانیکه پسورد با الگوریتم NTLM رمزگذاری شد ابتدا به حروف بزرگ تبدیل می‌شود: 123456ABCDEF. پسورد با کاراکترهای blank پر می‌شود تا اینکه طول آن به ۱۴ کاراکتر برسد: 123456ABCDEF__. قبل از اینکه پسورد رمز شود، رشته ۱۴ کاراکتری به دو بخش تقسیم می‌شود: 123456A و BCDEF__. هر رشته بطور جداگانه رمز می‌شود و نتایج آن به هم وصل می‌شوند:

123465A = 6BF11E04AFAB197F

BCDEF__ = F1E9FFDCC75575B15

و نتیجه hash به صورت 6BF11E04AFAB197F F1E9FFDCC75575B15 خواهد بود.

مقایسه پروتکل‌های LM، NYLM v1 و NTLM v2

ویژگی	LM	NTLM v1	NTLM v2
حساسیت نسبت به حروف بزرگ و کوچک	خیر	بله	بله
طول کلید hash	56bit+56bit	-	-
الگوریتم hash پسورد	DES (ECB mode)	MD4	MD4
طول مقدار hash	64bit+64bit	128bit	128bit
طول کلید C/R	56bit+56bit+16bit	56bit+56bit+16bit	128bit
الگوریتم C/R	DES (ECB mode)	DES (ECB mode)	HMAC_MD5
طول مقدار C/R	64bit+64bit+64bit	64bit+64bit+64bit	128bit

شکستن پسوردهای ویندوز ۲۰۰۰

فایل SAM در ویندوز، شامل نام‌های کاربری و پسوردهای hash شده است که در مسیر Windows\system32\config قرار دارد. زمانیکه سیستم روشن می‌شود این فایل قفل می‌شود بنابراین هکر نمی‌تواند این فایل را کپی کند. یکی از گزینه‌ها برای کپی فایل SAM، این است که کامپیوتر را با سیستم عامل دیگری راه‌اندازی کنید از قبیل DOS یا Linux با CD راه انداز. در این حالت می‌توان فایل را از دایرکتوری repair کپی کرد. اگر مدیر سیستم از قابلیت RDISK ویندوز برای گرفتن پشتیبان سیستم (با استفاده از rdisk /s) استفاده

کند، یک کپی فشرده شده از فایل SAM که SAM.__ نام دارد در مسیر c:\windows\repair ایجاد می‌شود. برای بسط این فایل، از دستور زیر در cmd استفاده کنید:

```
C:\>expand sam.__ sam
```

پس از آنکه فایل از حالت فشرده خارج شد، می‌توان با استفاده از نرم‌افزار L0phtCrack، از حملات dictionary، brute-force، یا hybrid استفاده کرد.

ابزارهای هک

Win32CreatedLocalAdminUser، برنامه‌ای است که حساب کاربری جدیدی را با نام کاربری و پسورد x می‌سازد و آن را به گروه administrator اضافه می‌کند. این عمل، بخشی از پروژه Metasploit است و می‌تواند با Metasploit framework روی ویندوزها اجرا شود.

Offline NT Password Resetter روشی برای ریست کردن پسورد administrator است. معمول‌ترین روش این است که با CD راه‌انداز Linux دستگاه را راه‌اندازی کنید و به پارتیشن NTFS که اکنون بصورت محافظت شده نیست، دسترسی پیدا کنید و پسورد را تغییر دهید.

برنامه LCP، برای بررسی پسورد حساب‌های کاربر در ویندوزهای NT، 2000، XP و ۲۰۰۳ است که شامل هر سه نوع حمله Dictionary، Hybrid و Brute force است.

برنامه‌های دیگری نیز همچون SID&User، Ophcrack2، Crack، Access Pass View، Asterisk Logger، Asterisk Key نیز برای شکستن پسورد بکار می‌روند.

تغییر جهت SMB Logon به حمله کننده

روش دیگر برای کشف پسوردهای روی شبکه، تغییر مسیر SMB logon به کامپیوتر حمله کننده است تا پسوردها به هکر ارسال می‌شود. برای این منظور، هکر بایستی پاسخ‌های NTLM را از سرور احراز هویت، sniff کند

و قربانی را اغفال کند تا با کامپیوتر هکر احراز هویت کند. رایج‌ترین تکنیک، ارسال ایمیلی به قربانی است که دارای لینکی به SMB Server باشد است. زمانیکه قربانی بر روی لینک کلیک کرد، بدون آنکه متوجه شود اطلاعات احراز هویت خود را روی شبکه ارسال می‌کند.

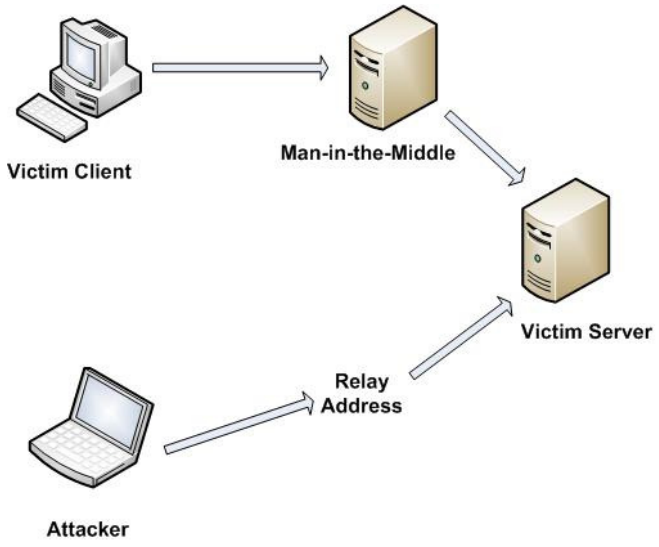
SMB Redirection

ابزارهای زیادی می‌توانند تغییر جهت SMB را پیاده‌سازی کنند:

ابزارهای هک
SMBRelay، یک SMB Server است که نام‌های کاربری و hashهای پسوردها را از ترافیک SMB ورودی بدست می‌آورد. SMBRelay، می‌تواند حملات man-in-the-middle را انجام دهد. SMBRelay2، مشابه SMBRelay است اما با این تفاوت که به جای آدرس‌های IP، از اسامی NetBIOS برای بدست آوردن نام‌های کاربری و پسوردها استفاده می‌کند. Pwdump2، برنامه‌ای است که hashهای پسوردها را از فایل SAM روی سیستم ویندوز استخراج می‌کنند. پسوردهای استخراج شده، از طریق L0phtCrack می‌توانند شکسته شوند. Samdump، برنامه‌ای برای استخراج پسوردهای NTLM که در فایل SAM، hash شده‌اند استفاده می‌شود. C2MYAZZ، یک برنامه جاسوسی است که سبب می‌شود کلاینت‌های ویندوزی، پسوردها را به صورت رمز نشده ارسال کند. نام‌های کاربری و پسوردهایی که کاربران برای اتصال به منابع سرور استفاده می‌کنند را نمایش می‌دهد.

حملات SMB Relay MITM و مقابله با آن

حمله SMB Relay MITM، زمانیکه حمله کننده یک سرور جعلی راه‌اندازی می‌کند، رخ می‌دهد. زمانیکه کلاینت قربانی، به سرور جعلی متصل می‌شود، شکل زیر، مثالی از این نوع حمله را نشان می‌دهد.



روش‌های مقابله با SMB relay، شامل پیکربندی ویندوز ۲۰۰۰ برای استفاده از SMB signing است که سبب می‌شود هر بلاک از ارتباطات SMB، رمزنگاری شود. این تنظیمات در Security Policies/Security Options وجود دارد.

ابزارهای هک
SMBGrind، سرعت نشست‌های L0phtCrack را روس استراق سمع dumpها افزایش می‌دهد. ابزار SMBDie، با ارسال درخواست‌های SMB جعلی، کامپیوترهایی که دارای سیستم عامل ویندوز ۲۰۰۰، XP، NT هستند را crash می‌کند. NBTdeputy، می‌تواند یک نام کامپیوتری NetBIOS را روی شبکه رجیستر کند و به درخواست‌های NetBIOS پاسخ دهد. همچنین این ابزار، استفاده از SMBRelay را ساده می‌کند.

مقابله با شکستن پسورد

برای مقابله با شکستن پسورد، باید از پسورد قوی استفاده شود. طول پسوردها، ۸ تا ۱۲ کاراکتر باشد. برای محافظت از شکستن الگوریتم hash برای پسوردهایی که در سرور ذخیره شده‌اند، باید مراقب باشید که سرور را بصورت فیزیکی مراقبت کنید. مدیر سیستم‌ها می‌تواند از ابزار خود ویندوز که SYSKEY نام دارد استفاده کند تا مراقبت بیشتری بر روی سرور یا دیسک داشته باشد. logهای سرور را بررسی کنید تا حملات brute-force روی حساب‌های کاربر را شناسایی کنید.

ویندوز برای ذخیره پسوردهای کاربران، از دو روش مختلف hash استفاده می‌کند. اگر طول پسورد کمتر از ۱۵ کاراکتر باشد، ویندوز از دو روش LM hash و NT hash استفاده می‌کند که LM hash نسبت به NT hash، ضعیف‌تر است و در مقابل حمله brute force راحت‌تر می‌شکنند. بنابراین، در پایگاه داده SAM، LM hashها را ذخیره نکنید. برای اینکه پروتکل‌های NTLM، NTLM v2 و Kerberos از NT hash استفاده می‌کنند ولی پروتکل LM، از LM hash استفاده می‌کند که ضعیف‌تر از NT hash است. بنابراین اگر در شبکه‌تان، ویندوز ۹۵، ۹۸ یا مکینتاش ندارید بهتر است به یکی از روش‌های زیر آن را غیر فعال کنید:

روش ۱: از Group Policy، وارد قسمت Security Options و Local Security Policy شوید و گزینه زیر را غیر فعال کنید: Network security: Do not store LAN Manager hash value on next password change

روش ۲: از طریق رجیستری وارد مسیر زیر شوید:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa و سپس کلیدی به نام NoLMHash ایجاد کنید.

روش ۳: پسوردی که طول آن بیشتر از ۱۵ کاراکتر است استفاده کنید.

همچنین برای مقابله با شکستن پسورد، موارد زیر را در نظر بگیرید:

۱. پسوردهای پیش فرض را تغییر دهید.
۲. پسوردهایی که در دیکشنری وجود دارند را استفاده نکنید.
۳. از پسوردی استفاده نکنید که مربوط به اسم دستگاه، اسم دامین، یا هر چیز دیگری که می توان در whois پیدا کرد باشد.
۴. پسوردی که مربوط به علایق شما یا تاریخ تولد شما است استفاده نکنید.
۵. اگر از کلمات دیکشنری می‌خواهید استفاده کنید، از کلمه‌ای که بیشتر از ۲۱ کاراکتر دارد استفاده کنید.

در بخش‌های بعدی، به دو معیاری که می‌توانید برای ساخت پسورد قوی بکار برید نگاهی خواهیم داشت.

بازه زمانی تغییر پسورد

پسوردها بایستی بعد از مدت زمان مشخصی، منقضی (expire) شوند بنابراین، کاربران باید پسوردشان را تغییر دهند. اگر طول پسورد بسیار کوتاه باشد، کاربران پسوردهایشان را فراموش می‌کنند در نتیجه، مدیر سیستم‌ها باید

پسوردهای کاربران را بارها reset کنند. از طرفی دیگر، اگر این مدت زمان بسیار طولانی باشد، امنیت به خطر می‌افتد. مدت زمان توصیه شده برای این بازه، ۳۰ روز است. علاوه بر این، توصیه می‌شود که کاربران نتوانند از سه پسورد قبلی‌شان دوباره استفاده کنند.

بررسی Event Viewer Logها

مدیران باید Event Viewer logها را بررسی کنند تا هر رخدادی را قبل از اتفاق یا در طول اتفاق تشخیص دهند. بطور کلی، چندین تلاش ناموفق می‌تواند در سیستم ثبت شود و تنها مدیران سیستم‌ها بتوانند آن را بررسی کنند.

ابزارهایی از قبیل VisualLast، مدیر شبکه را برای رمزگشایی و تحلیل فایل‌های log امنیتی، کمک می‌کند. این ابزار، دید بزرگتری را به NT event log ها باز می‌کند بنابراین مدیر شبکه می‌تواند به صورت دقیق‌تر و موثرتر به فعالیت‌های شبکه دسترسی داشته باشد. این برنامه برای این طراحی شده است که مدیران شبکه را قادر سازد گزارشات زمان‌های ورود و خروج کاربران را ببینند این وقایع، می‌توانند طبق فریم زمان جستجو شوند که برای تحلیل امنیتی بسیار مهم است.

Event logها در مسیر c:\\windows\system32\config\Sec.Event.Evt قرار دارند که شامل ردپاهای تلاش‌های brute-force حمله کننده است.

ابزار AccountAudit، به مدیران شبکه اجازه می‌دهد که پایگاه داده حساب‌های کاربران در اکتیو دایرکتوری را بررسی کنند تا ریسک‌های امنیتی رایج همچون کاربران بدون پسورد، یا ... را گزارش دهد.

انواع مختلف پسورد

برای دسترسی به سیستم‌ها، چندین نوع پسورد وجود دارد. کاراکترهایی که پسورد را تشکیل می‌دهند، چندین دسته بندی دارند:

- تنها حروف
- تنها اعداد
- تنها کاراکترهای خاص
- حروف و اعداد
- تنها حروف و کاراکترهای خاص

- تنها اعداد و کاراکترهای خاص
- حروف، اعداد، و کارکترهای خاص

یک پسورد قوی، احتمال کمتری برای شکسته شدن توسط هکر دارد. قوانین زیر که توسط EC Council ارائه شده است، بایستی برای ایجاد پسورد در نظر گرفته شوند تا در مقابل حملات محافظ باشد:

- نباید شامل بخشی از نام کاربری باشد
- حداقل طول آن باید ۸ کاراکتر باشد
- باید حداقل شامل سه قسمت از دسته‌های زیر باشد:
  - علائم غیر الفبایی (#!@%":,$)
  - اعداد
  - حروف بزرگ
  - حروف کوچک

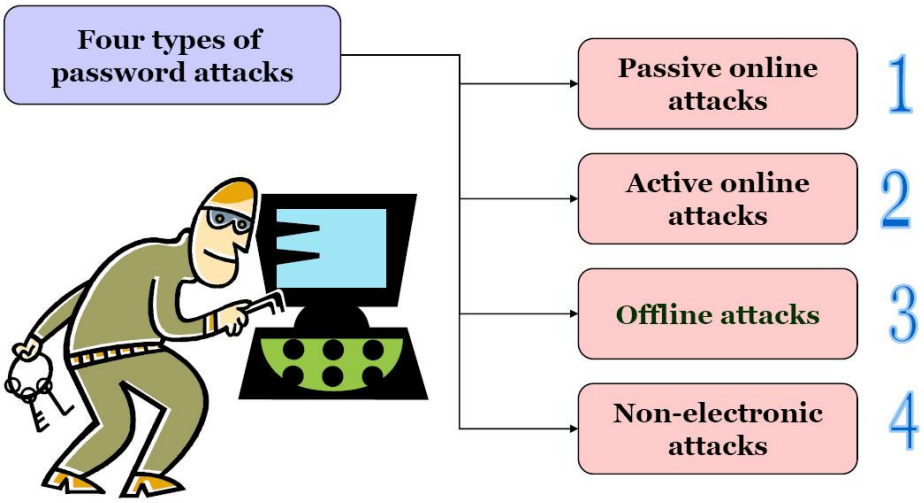
ممکن است هکر از انواع مختلف حملات برای شناسایی یک پسورد و برای ایجاد دسترسی بیشتر به یک سیستم استفاده کند. انواع حملات پسورد به شرح زیر است:

Passive online: مبادلات پسورد بر روی شبکه را استراق سمع می‌کند. حملات passive online، شامل حملات sniffing، man-in-the-middle، و reply است.

Active online: پسورد Administrator را حدس می‌زند. حملات active online، شامل حدس خودکار پسورد است.

Offline: حملات Dictionary، hybrid، و brute-force است.

Nonelectronic: Shoulder surfing، استراق سمع صفحه کلید، و مهندسی اجتماعی.



حملات Passive Online

حمله passive online، با نام استراق سمع پسورد روی شبکه‌های کابلی و وایرلس شناخته می‌شود. کاربر نهایی نمی‌تواند این گونه حملات را تشخیص دهد. در طول فرایند احراز هویت، پسورد بدست می‌آید و با فایل دیکشنری یا لیست کلمات مقایسه می‌شود. معمولا پسوردهای حساب‌های کاربران، در زمان ارسال روی شبکه hash و یا رمز می‌شوند تا جلوی دسترسی غیر مجاز را بگیرد. اگر پسورد توسط رمزگذاری یا hashing، محافظت شده باشد، آنگاه ابزارهای مخصوصی که در toolkit هکر وجود دارد برای شکستن الگوریتم می‌تواند مورد استفاده قرار گیرد.

حمله دیگر passive online، بنام man-in-the0-middle (MITM) نام دارد. در حمله MITM، هکر در درخواست احراز هویت دخالت می‌کند و آن را به سرور فروارد می‌کند. با وارد کردن یک sniffer بین کلاینت و سرور، هکر می‌تواند هم ارتباطات را sniff کند و هم پسورد را در این فرآیند بدست آورد.

حمله reply، نیز جز حملات passive online است که زمانیکه پسورد به سرور احراز هویت ارسال می‌شود با مداخله هکر رخ می‌دهد و سپس آن را دوباره برای احراز هویت‌های بعدی ارسال می‌کند. در این روش، هکر نیازی ندارد که پسورد را بشکند یا از طریق MITM آن را یاد بگیرد بلکه باید آن را بدست آورد و از بسته‌های احراز هویت-پسورد برای احراز هویت‌های بعدی استفاده کند.

حملات Active Online

ساده‌ترین روش برای دسترسی در سطح مدیر سیستم، حدس زدن یک پسورد ساده است با این فرض که مدیر سیستم، از یک پسورد ساده استفاده کرده است. حدس پسورد، یک نوع حمله active online است که بر مبنای فاکتور انسانی در ایجاد پسورد است و تنها بر روی پسوردهای ضعیف کار می‌کند.

فرض کنید که پورت NetBOIS TCP 139 باز است، موثرترین روش برای شکستن پسورد در سیستم‌های ویندوز ۲۰۰۰ و NT، حدس زدن پسورد است. این عمل با اتصال به پوشه به اشتراک گذاشته شده (IPC$ یا C$) و تلاش برای ترکیبی از نام کاربری و پسورد است. رایج‌ترین نام کاربری برای مدیر سیستم، Admin، Administrator، Sysadmin است.

هکر ابتدا سعی می‌کند که به پوشه‌هایی که بصورت پیش فرض به اشتراک گذاشته شده است، وصل شود. برای اتصال به پوشه‌های به اشتراک گذاشته مخفی درایو C، از دستور زیر استفاده کنید:

\\ip_address\c$

برنامه‌هایی وجود دارند که بصورت اتوماتیک فایل‌های دیکشنری، لیست کلمات یا ترکیبی از حروف، اعداد و کاراکترهای خاص تولید می‌کنند و تلاش می‌کنند تا به سیستم وصل شوند. اغلب سیستم‌ها، با استفاده از تنظیم حداکثر تعداد تلاش برای اتصال به سیستم، از این نوع حمله پیشگیری می‌کنند.

حدس پسورد به صورت اتوماتیک

برای تسریع بخشدین به عملیات حدس پسورد، هکرها از ابزارهای اتوماتیک استفاده می‌کنند. یک فرآیند ساده برای خودکارسازی حدس پسورد، استفاده از ابزار دستوری Windows shell است که مبتنی بر استاندارد NET USE است. برای ساخت یک اسکریپت ساده حدس پسورد، مراحل زیر را انجام دهید:

۱. با استفاده از برنامه Windows Notepad، یک فایل username و password ساده بسازید. ابزارهای خودکاری از قبیل Dictionary Generator، برای ساخت لیست این کلمات در دسترس هستند. فایل را در مسیر C: drive as credentials.txt ذخیره کنید.
۲. این فایل را با استفاده از دستور FOR، pipe کنید:

C:\> FOR /F “token=1, 2*” %i in (credentials.txt)

۳. دستور net use \\targetIP\IPC$ %i /u: %j را تایپ کنید تا از فایل credentials.txt استفاده کند و به پوشه share شده مخفی آن وارد شود.

مقابله با حدس پسورد

برای مقابله با حدس و حملات پسورد، دو گزینه وجود دارد. کارت‌های هوشمند و بیومتریک، یک لایه امنیتی اضافه می‌کنند. ممکن است کاربری با استفاده از بیومتریک، احراز هویت و شناسایی شود. بیومتریک‌ها از ویژگی‌های فیزیکی همچون اثر انگشت، اسکن کف دست، و اسکن قرنیه چشم برای شناسایی کاربران استفاده می‌کنند.

کارت‌های هوشمند و دستگاه‌های بیومتریک، از دو فاکتور برای احراز هویت استفاده می‌کنند که هنگام شناسایی کاربر، به دو نوع شناسایی نیاز دارند (مثلا کارت هوشمند و پسورد). با درخواست چیزی که کاربر بصورت فیزیکی آن را دارد (مثلا کارت هوشمند) و چیزی که می‌داند (پسوردشان)، امنیت افزایش می‌یابد و فرآیند احراز هویت در مقابل حملات پسورد، مقاوم می‌شود.

حملات آفلاین

حملات آفلاین از محلی به غیر از جائیکه کامپیوتر واقعی قرار دارد انجام می‌شود. معمولا حملات آفلاین نیاز به دسترسی فیزیکی به کامپیوتر و کپی فایل پسورد از سیستم به حافظه جانبی دارد. سپس هکر آن فایل را به کامپیوتر دیگری کپی می‌کند تا آن را بشکند. انواع مختلف از حملات آفلاین پسورد وجود دارد. جدول زیر هر کدام از این حملات را توضیح می‌دهد:

نوع حمله	ویژگی‌ها	مثال
Dictionary attack	پسوردها را از لیست کلمات دیکشنری استفاده کند	Administrator
Hybrid attack	برخی از علائم را با کاراکترهای پسورد جایگزین می‌کند	Adm1n1strator
Brute-force attack	تمام ترکیبات ممکن از حروف، اعداد، و کاراکترهای خاص را تست می‌کند	Ms!tr245@F5a

حمله دیکشنری، ساده‌ترین و سریعترین نوع حمله است. برای شناسایی پسوردی که یک کلمه‌ای که در دیکشنری است استفاده می‌شود. معمولا، هکر از یک فایل که حاوی تمام کلمات دیکشنری و hash آن کلمات با استفاده از همان الگوریتم است، استفاده می‌کند. سپس، کلمات دیکشنری که hash شده‌اند، با پسوردهای hash شده در مرحله لاگین، مقایسه می‌شود. حمله دیکشنری، تنها زمانیکه پسورد یکی از کلمات دیکشنری باشد کار می‌کند بنابراین، این نوع حمله، همان محدودیت‌ها را دارد یعنی اگر پسورد قوی انتخاب شده باشد، کار نمی‌کند. اگر هکر نتواند با استفاده از حمله دیکشنری، پسورد را پیدا کند، در مرحله بعدی از حمله hybrid استفاده می‌کند. این حمله،

با یک فایل دیکشنری که برخی از حروف آن با علائم جایگزین شده است، شروع می‌شود. برای مثال، بسیاری از کاربران، به آخر پسوردهایشان، عدد ۱ را اضافه می‌کنند تا پسوردشان قوی شود.

زمان‌گیرترین نوع حمله، حمله brute-force است که تمام حالات مختلف را امتحان می‌کند. حمله brute-force، آهسته‌ترین نوع حمله است برای اینکه تمام ترکیبات ممکن حروف، اعداد، و علائم را بررسی می‌کند. با این حال، موثرترین است برای اینکه اگر زمان کافی وجود داشته باشد، تمام پسوردها کشف می‌شوند.

نکات

بسیار کند است
تمام پسوردها را کشف می کند
حمله بر علیه NT hash بسیار سخت تر از NT hash است

Pre-Computed Hashes

تمام کلمات را از قبل hash می‌کند و در پایگاه داده ذخیره می‌شود و در زمان شکستن پسورد، از این پایگاه داده برای پیدا کردن پسورد استفاده می‌شود. ذخیره کردن hash، نیاز به فضای حافظه زیادی دارد و زمان بر نیز هست.

حملات Nonelectronic

حملات غیر الکترونیکی یا غیر فنی، حملاتی هستند که از هیچ دانش فنی استفاده نمی‌کنند. این نوع حمله، شامل مهندسی اجتماع، shoulder surfing، sniff کردن کیبورد، و آشغال گردی است.

مهندسی اجتماعی، هنر تعامل با مردم یا به صورت رو در رو یا تلفنی برای جمع‌آوری اطلاعات با ارزشی همچون پسوردها است. مهندسی اجتماعی، بر مبنای ذات خوب مردم که دوست دارند به بقیه کمک کنند، استوار است. اغلب اوقات، help deskها سوژه خوبی برای مهندسی اجتماعی هستند برای اینکه وظیفه آنها کمک به دیگران

است و پاک کردن یا reset کردن پسورد، جزئی از وظایف رایج انهاست. بهترین روش مقابله با این نوع حمله، آموزش آگاهی امنیتی برای همه کارکنان و فرآیندهای امنیتی برای reset کردن پسورد است.

Shoulder surfing، ایستادن در کنار شخص و نگاه کردن به پسوردی است که تایپ می‌کند. زمانیکه هکر نزدیک کاربر یا سیستم است، این روش موثر است. بعضی صفحات وجود دارند که نگاه کردن از گوشه به مانیتور را سخت می‌کنند بنابراین، جلوی این حمله را می‌گیرند. علاوه بر این، آموزش و آگاهی پرسنل، احتمال این نوع حمله را کاهش می‌دهد.

در آشغال گردی، هکر در زباله‌ها به دنبال اطلاعاتی از قبیل پسوردهایی که ممکن است در تکه‌ای کاغذ نوشته شود می‌گردد. برای مقابله با این حمله نیز آموزش و آگاهی کاربران می‌تواند هکر را از کسب اطلاعات پسوردها با آشغال‌گردی جلوگیری کند.

وب سایت‌هایی وجود دارند که شامل پایگاه داده‌هایی هستند که پسوردهای پیش فرض بسیاری از سازندگان مختلف را دارند:

http://www.defaultpassword.com

http://www.cirt.net/passwords

http://www.virus.org/default-password

نرم‌افزارهای PDF Password Cracker، و Abcom PDF Password Cracker، که قفل‌های امنیتی فایل‌های PDF را می‌شکنند.

تکنیک‌های keyloggerها و spyware

اگر همه تلاش‌ها برای جمع‌آوری پسورد، به شکست منجر شود، استفاده از ابزار keystroke logger، انتخاب بعدی هکرهاست. keystroke logger (keylogger)، می‌تواند بصورت سخت‌افزاری یا نرم‌افزاری انجام گیرد. keystroke loggerهای سخت‌افزاری، دستگاه‌های سخت‌افزاری کوچکی هستند که کیبورد را به کامپیوتر وصل می‌کنند و هر کلیدی که فشار داده می‌شود را داخل فایلی در حافظه ذخیره می‌کنند. برای نصب یک keylogger سخت‌افزاری، هکر باید دسترسی فیزیکی به سیستم داشته باشد.

Keylogger نرم‌افزاری، تکه‌ای از نرم‌افزار دزدی است که بین سخت‌افزار کیبورد و سیستم عامل قرار می‌گیرد بنابراین، می‌توانند هر کلیدی را ثبت کنند. Keyloggerهای نرم‌افزاری توسط تروجان‌ها یا ویروس‌ها توسعه می‌یابند.

ابزارهای هک

Spector، یک نرم‌افزار جاسوسی (spyware) است که تمام چیزهایی که در اینترنت انجام می‌شود را مثل دوربین ضبط می‌کند. این نرم‌افزار، بصورت خودکار در هر ساعت، صدها عکس از صفحه مانیتور می‌گیرد و آنها را در مکانی مخفی روی هارد سیستم ذخیره می‌کند. Anti-spector می‌تواند این نرم‌افزار را تشخیص دهد و آن را حذف کند.

eBlaster، یک نرم‌افزار جاسوسی اینترنتی است که ایمیل‌های ورودی و خروجی را دریافت می‌کند و بلافاصله آنها را به آدرس ایمیل دیگری فروارد می‌کند. eBloster، می‌تواند هر دو طرف یک مکالمه مسنجر را بگیرد و آنها را ثبت کند و همچنین وب سایت‌های مشاهده شده را ثبت کند.

SpyAnywhere، ابزاری است که به شما اجازه می‌دهد فعالیت سیستم و اعمال کاربر را ببینید، سیستم را خاموش، ریستارت کنید و حتی سیستم فایل سیستم راه دور را ببینید. SpyAnywhere، به شما اجازه می‌دهد برنامه‌ها و پنجره‌های باز را روی سیستم راه دور کنترل کنید و history اینترنتی و اطلاعات مربوطه را ببینید.

Fearless Key Logger، تروجانی است که در حافظه باقی می‌ماند تا تمام ضربات کلید کاربر را بدست آورد. کلیدهای زده شده، در فایل log ذخیره می‌شوند و می‌تواند توسط هکر بازیابی شود.

E-mail Keylogger، تمام ایمیل‌های فرستاده شده و دریافت شده روی سیستم هدف را ثبت می‌کند. ایمیل‌ها می‌توانند توسط ارسال‌کننده، دریافت‌کننده، موضوع، و تاریخ/ساعت مشاهده شوند. محتوای ایمیل و هر ضمیمه دیگر، ضبط می‌شود.

برخی دیگر از نرم افزارهای Keylogger عبارتند از:

- Revealer Keylogger
- Handy Key Logger
- Ardamax Keylogger
- Powered Keylogger
- ELITE Keylogger
- Quick Keylogger
- Spy-Keylogger
- Perferct Keylogger
- Invisible Keylogger
- Actual Spy
- Spytector FTP Keylogger
- IKS Software Keylogger
- Ghost Keylogger

دسترسی‌های ضروری

افزایش دسترسی، سومین مرحله در چرخه هک است. افزایش دسترسی، به این معناست که مجوزها و حقوق یک حساب کاربری افزایش یابد. در واقع، افزایش دسترسی، به معنای افزایش دسترسی یک حساب کاربری به اندازه حساب مدیر است.

بطور کلی، حساب‌های مدیر، باید دارای پسوردهای قوی‌تر باشد. اگر هکر نتواند نام کاربری و پسورد مدیر سیستم را پیدا کند، به دنبال حسابی با دسترسی پایین‌تری می‌گردد و در این حالت، هکر به دنبال افزایش سطح دسترسی این حساب است.

زمانیکه هکر اکانت و پسورد معتبری را بدست آورد، در مرحله بعدی به دنبال اجرای برنامه‌های است. بطور کلی، هکر نیاز دارد که حسابی با دسترسی administrator داشته باشد تا بتواند برنامه‌ها را نصب کند و به همین خاطر است که افزایش سطح دسترسی، بسیار مهم است.

ابزارهای هک
GetAdmin.exe، برنامه کوچکی است که کاربری را به گروه administrator اضافه می‌کند. این برنامه از هسته سطح پایین NT استفاده می‌کند تا به پردازش‌های در حال اجرا دسترسی پیدا کند. برای اجرای برنامه، ورود به کنسول سرور ضروری است. GetAdmin.exe، از طریق دستور یا مروگر اجرا می‌شود. تنها بر روی Windows NT 4.0 SP3 کار می کند. با استفاده از برنامه HK.exe، می‌توانید کاربری که admin نیست به گروه administrator اضافه شود. Active@ Password Changer، برای reset کردن پسورد حساب administrator بصورت local است. ابزار x.exe، زمانیکه بر روی سیستم راه دور اجرا می‌شود، کاربری با نام X و پسورد X می‌سازد و آن را عضو گروه administrator می‌کند.

اجرای برنامه‌ها

زمانیکه هکر توانست به حسابی با سطح دسترسی administrator، دسترسی پیدا کند، مرحله بعدی که انجام می‌دهد این است که برنامه‌ها را روی سیستم هدف اجرا کند. ممکن است هدف اجرای برنامه‌ها، نصب back door (در پشتی) روی سیستم، نصب یک keystroke logger برای جمع‌آوری اطلاعات محرمانه، کپی فایل‌ها، یا فقط برای آسیب رساندن به سیستم باشد.

زمانیکه هکر توانست برنامه‌ها را اجرا کند، هکر مالک سیستم می‌شود و تحت کنترل او می‌شود.

ابزارهای هک

PsExec، برنامه‌ای است که به سیستم راه دور متصل می‌شود و فایل‌ها را اجرا می‌کند. نیازی به نصب برنامه روی سیستم راه دور نیست.

Remoxec، برنامه‌ای است که با استفاده از سرویس RPC یا DCOM کار می‌کند. مدیرانی که پسورد ضعیف دارند ممکن است از طریق Task Scheduler یا DCOM مورد سو استفاده قرار گیرند.

Alchemy Remote Executer، ابزار مدیریتی برای مدیران است که بتوانند برنامه‌های را روی کامپیوترهای شبکه از راه دور اجرا کنند.

Esma FlexInfo Pro، ابزاری برای نمایش اطلاعات و تنظیمات سیستم‌ها است که شامل ابزارهایی همچون گراف CPU usage، مانیتور پهنای باند و ... است.

Buffer Overflows

Buffer overflows (سرریزی بافر)، تلاش هکر برای سو استفاده از عیب یک برنامه است. در اصل، حمله سرریزی بافر، اطلاعات بسیار زیادی را به یک فیلد متغیر در یک برنامه می‌فرستد که منجر به خطای برنامه می‌شود. اغلب اوقات، برنامه نمی‌داند که در این حالت چیکار کند بنابراین، یا دستورات را اجرا می‌کند یا دستور را رد می‌کند و به کاربر اجازه می‌دهد که دستور بعدی را وارد کند. برای هکر، cmd یا shell، کلید اجرای برنامه‌های دیگر است.

Rootkit ها

Rootkit، نوعی برنامه است که اغلب برای مخفی کردن برنامه‌ها روی سیستم قربانی به کار می‌رود. Rootkitها شامل back door هستند تا به هکر کمک کند بطور متوالی و راحت به سیستم دسترسی پیدا کند. همچنین یک back door ممکن است اجازه شروع پردازش‌ها را توسط یک حساب محدود را بدهد. Rootkit، بطور پیوسته توسط برنامه‌نویس rootkit مورد استفاده قرار می‌گیرد تا بتوانند نام‌های کاربری و اطلاعات لاگین سایت‌هایی که به آنها نیاز دارند را ببیند و دسترسی پیدا کنند.

چندین نوع rootkit وجود دارند که عبارتند از:

Kernel-level rootkits: این دسته از rootkit ها، کدی را به قسمتی از کد هسته اضافه می‌کنند یا آن را جایگزین می‌کنند تا back door را روی سیستم، مخفی نگه دارد. معمولا کد جدیدی را از طریق درایور دستگاه یا ماژول‌ها به کرنل اضافه می کند. Kernel-level rootkitها، بسیار خطرناک هستند برای اینکه بدون استفاده از نرم‌افزار مناسب، شناسایی آنها بسیار سخت‌تر است.

Library-level rootkits: این دسته از rootkitها، فراخوانی سیستم (library) را با نسخه‌ای دیگر که اطلاعات هکر را مخفی می‌کند، جایگزین می‌کنند.

Application-level rootkits: این دسته از rootkitها، بیت‌های باینری برنامه‌ها را با تروجان‌ها جایگزین می‌کند یا ممکن است که رفتار برنامه موجود را از طریق patchها، کدهای تزیق شده، یا ابزارهای دیگر، تغییر دهد.

نصب Rootkitها بر روی کامپیوترهای ویندوز ۲۰۰۰ و XP

Windows NT/2000 rootkit، بطور اتوماتیک هنگاه اجرای ویندوز، بارگذاری می‌شود. Rootkit، با دسترسی سیستمی در هسته NT kernel کار می‌کند بنابراین، به همه منابع سیستم عامل دسترسی دارد. Rootkit می‌تواند پردازش‌ها را مخفی کند، فایل‌ها را مخفی کند، مقادیر رجیستری را مخفی کند، وقفه ایجاد کند تا blue scrren ظاهر شود، و فایل های EXE را تغییر مسیر دهد.

Rootkit، شامل یک kernel mode device driver که _root_.sys نام دارد و یک برنامه اجرا کننده که DEPLOY.EXE نام دارد، است. پس از ایجاد دسترسی به سیستم هدف، هکر، _root_.sys و DEPLOY.EXE را از سیستم هدف کپی می‌کند و DEPLOY.EXE را اجرا می‌کند. سپس درایور دستگاه rootkit را نصب و شروع می‌کند. سپس DEPLOY.EXE را از سیستم هدف حذف می‌کند. سپس، با استفاده از دستور net stop _root_ و net start _root_، rootkit را stop و سپس restart می‌کند. زمانیکه rootkit شروع به کار کرد، فایل _root_.sys دیگر در لیست دایرکتوری ظاهر نمی‌شود.

مقابله با rootkitها

تمام rootkitها برای دسترسی به سیستم هدف، نیاز به دسترسی administrator دارند بنابراین، امنیت پسورد از اهمیت بالایی برخوردار است. اگر شما یک rootkit را شناسایی کردید، توصیه می‌شود که از اطلاعات حیاتی پشتیبان تهیه کنید و سیستم عامل و برنامه‌ها را دوباره از منبع قابل اعتماد نصب کنید.

روش دیگر این است که از ابزار MD5 checksum استفاده کنید. برای یک فایل، MD5 checksum، ۱۲۸ بیت است. اگر یکی از بیت‌های یک فایل تغییر کند، مقدار checksum در این الگوریتم متفاوت خواهد بود. این قابلیت برای مقایسه فایل‌ها و مطمئن شدن از یکپارچگی آنها، مفید است. قابلیت خوب دیگر، طول ثابت checksum است.

ابزارهای هک

Tripwire، برنامه بررسی یکپارچگی فایل برای سیستم عامل‌های یونیکس و لینوکس است. علاوه بر بررسی checksum بر روی فایل‌ها و دایرکتوری‌ها، Tripwire، دارای اطلاعاتی است که به شما اجازه می‌دهد مجوزهای دسترسی و تنظیمات فایل، نام کاربری مالک، تاریخ و ساعت آخرین دسترسی به آن، و آخرین اصلاح آن را بررسی می‌کند.

نحوه مخفی کردن فایل‌ها

ممکن است هکری بخواهد که فایلی را بر روی سیستم مخفی کند تا از شناسایی در امان بماند. سپس این فایل‌ها برای حمله به سیستم استفاده می‌شود. در ویندوز، دو روش برای مخفی کردن فایل‌ها وجود دارد. اولین روش، استفاده از دستور attrib است. برای مخفی کردن فایل با استفاده از دستور attrib، دستور زیر را تایپ کنید:

Attrib +h [file/directory]

دومین روش برای مخفی کردن فایل در ویندوز، با استفاده از خاصیت NTFS data streaming است. سیستم فایل NTFS، دارای قابلیتی است که alternate data streams نامیده می‌شود که داده‌ها را داخل فایل دیگری که قابل رویت است، مخفی می‌کند. بیشتر از یک فایل را می‌توان به فایل اصلی لینک کرد و نیز محدودیت اندازه ندارد.

NTFS File Streaming

برای ساخت و تست NTFS file stream، مراحل زیر را انجام دهید:

۱. در cmd، دستور noepad test.txt را تایپ کنید.
۲. فایل را با اطلاعاتی پر کنید و سپس آن را ببندید.
۳. در cmd، دستور dir test.txt را وارد کنید و به اندازه آن دقت کنید.
۴. در cmd، دستور notepad test.txt:hidden.txt را تایپ کنید. داخل فایل را با مطالبی پر کنید و آن را ذخیره کنید.
۵. دوباره اندازه فایل را بررسی کنید (باید نسبت به قبل تفاوتی نکرده باشد).
۶. Test.txt را باز کنید. باید فقط داده‌های اصلی را ببینید.
۷. دستور type test.txt:hidden.txt را در cmd تایپ کنید. پیام خطا نمایش داده می‌شود.
۸. برای اینکه محتوای Trojan.exe را به Readme.txt انتقال دهید، از دستور زیر استفاده کنید:

C:\> type c:\Trojan.exe > c:\Readme.txt:Trojan.exe

۹. برای اجرای Trojan.exe در Readme.txt، از دستور زیر استفاده کنید:

```
C:\> start c:\Readme.txt:Trojan.exe
```

۱۰. برای extract کردن Trojan.exe از Readme.txt از دستور زیر استفاده کنید:

```
C:\> cat c:\Readme.txt:Trojan.exe > Trojan.exe
```

ابزارهای هک
Makestrm.exe، برنامه‌ای است که داده‌ها را از یک فایل به یک alternate data stream که به فایل اصلی لینک است، منتقل می‌کند.

مقابله با NTFS Stream

برای حذف یک stream file، ابتدا آن فایل را به پارتیشنی که دارای سیستم فایل FAT باشد کپی کنید و سپس دوباره به پارتیشن NTFS برگردانید. زمانیکه فایلی را به پارتیشن FAT جابجا می‌کنید، خاصیت stream حذف می‌شود برای اینکه streaming یکی از قابلیت‌های NTFS است و تنها با این سیستم فایل وجود دارد.

ابزارهای هک
شما می‌توانید از LNS.exe برای شناسایی NTFS streams استفاده کنید. اگر فایل steam وجود داشته باشد، این برنامه، آن را شناسایی می‌کند و مکان آن را گزارش می‌دهد.

تکنولوژی‌های Steganography

Steganography، فرآیند مخفی کردن داده‌ها در نوع دیگری از فایل همچون عکس یا فایل متنی است. محبوب‌ترین روش برای مخفی کردن داده‌ها در فایل‌ها، استفاده از عکس‌های گرافیکی به عنوان محل مخفی کردن است. هکر می‌تواند با استفاده از steganography، هر اطلاعاتی را داخل فایل گرافیکی جاسازی کند.

ابزارهای هک

ImageHide، برنامه steganography است که مقادیر بزرگی از متن را داخل عکس مخفی می‌کند. حتی پس از اضافه کردن داده‌ها، اندازه فایل افزایش نمی‌یابد. در برنامه‌های گرافیکی معمولی، عکس به طور طبیعی نشان داده می‌شود. داده‌ها را داخل خودش بارگذاری و ذخیره می‌کند بنابراین snifferهای ایمیل، نمی‌توانند آن را تشخیص دهند.

Blindside، برنامه دستوری steganography است که اطلاعات را داخل عکس‌های BMP مخفی می‌کند.

MP3Stego، اطلاعات را داخل فایل‌های گرافیکی مخفی می‌کند. داده‌ها، فشرده و رمزگذاری می‌شوند و سپس در MP3 bit stream مخفی می‌شوند.

Snow، برنامه whitespace steganography است که پیام ها را در متن ASCII مخفی می‌کند که اینکار را با استفاده از ضمیمه کردن whitespace به انتهای خط ها انجام می دهد. از آنجائیکه whitespaceها در برنامه های متنی قابل مشاهده نیستند، پیام به راحتی مخفی می شود. اگر از رمزگذاری استفاده شود، حتی در صورت تشخیص، پیام قابل خواندن نیست.

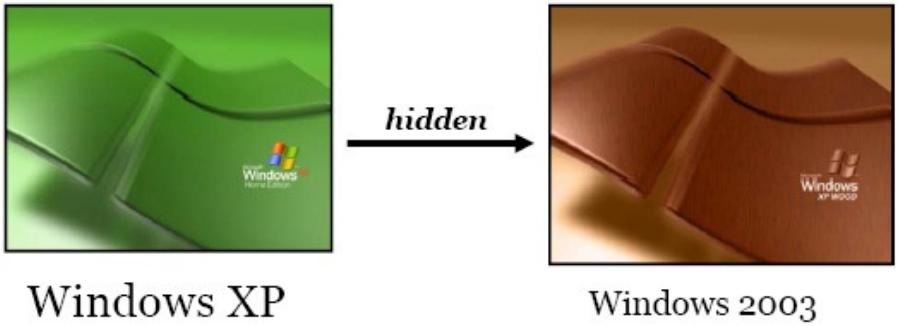
Camera/Shy، با ویندوز و IE کار می‌کند و به کاربران اجازه می‌دهد که اطلاعات حساس خود را داخل یک فایل عکس gif ذخیره کنند.

Merge Streams: فایل Word را داخل Excel و برعکس ادغام می‌کند.

Stealth Files، فایل‌های اجرایی را داخل فایل‌های دیگری همچون Word، Excel، PowerPoint و Acrobat ادغام می‌کند.

Masker Steganography، برنامه‌ای برای رمزگذاری و مخفی کردن فایل‌ها داخل فایل دیگر است.

DCPP: ابزاری برای مخفی کردن کل یک سیستم عامل داخل سیستم عامل دیگر است.



برنامه‌های دیگر که برای steganography استفاده می‌شود عبارتند از:

- Fort Knox
- Blindside
- S- Tools
- Steghide
- Steganos
- Pretty Good Envelop
- Gifshuffle
- JPHIDE and JPSEEK
- wbStego

- OutGuess
- Data Stash
- Hydan
- Cloak
- StegaNote
- Stegomagic
- FoxHole
- Video Steganography

برخی از برنامه‌ها می‌توانند steganography را شناسایی کنند هر چند که انجام آن سخت است.

ابزارهای مقابله

Stegdetect، ابزاری خودکار برای شناسایی محتوای steganographic در تصاویر است و می‌تواند روش‌های مختلف Steganography را برای جاسازی اطلاعات مخفی در تصاویر را تشخیص دهد.

Dskprobe، ابزاری در سی دی ویندوز ۲۰۰۰ است. که یک اسکنر سطح پایین هارد دیسک است و می‌تواند steganography رو شناسایی کند.

پاک کردن ردپاها و مدارک

زمانیکه هکر توانست به سیستمی دسترسی پیدا کند، تلاش خواهد کرد که ردپاها را بپوشاند تا از شناسایی در امان بماند. همچنین ممکن است که بخواهد مدارک شناسایی یا فعالیت‌های خود را بر روی سیستم پاک کند. معمولا هکرها تمام پیغام‌های خطا یا امنیتی که ثبت می‌شوند را پاک می‌کند تا از شناسایی خود ممانعت به عمل آورد.

غیر فعال کردن رسیدگی (Auditing)

اولین چیزی که هکر بعد از دسترسی به سیستم انجام می‌دهد، غیر فعال کردن auditing است. auditing ویندوز، رخدادهای مشخصی را در فایل log که در قسمت Windows Event Viewer قرار دارد، ذخیره می‌کند. این رخدادها شامل ورود به سیستم، یک برنامه، یا یک Event log است. یک مدیر سیستم می‌تواند سطح این ذخیره‌سازی رخدادها را انتخاب کند. هکر می‌خواهد که سطح ثبت رخدادها را مشخص کند تا ببیند آیا نیازی به پاک کردن رخدادهایی که حضور او را در سیستم ثبت کند وجود دارد یا نه.

AuditPol، ابزاری است که می‌تواند به صورت دستوری، auditing را در ویندوز، فعال یا غیر فعال کند. این ابزار، می‌تواند سطح ثبت رخدادها را که توسط مدیر سیستم‌ها تعیین شده است را نیز مشخص کند.

```
C:\> auditpol.exe /disable
Running. . . .

Local audit information changed successfully. .
New local audit policy. . .

   (0)   Audit Disabled

AuditCategorySystem         = No
AuditCategoryLogon          = Failure
AuditCategoryObjectAccess   = No
. . .


C:\> auditpol.exe /enable
Auditing enabled successfully.
```

پاک کردن Event Log

هکر می‌تواند به راحتی، رکوردهای موجود در Windows Event Viewer را پاک کند. اگر تنها یک یا چند رکورد در این قسمت وجود داشته باشد، مشکوک است برای اینکه نشان می‌دهد رخدادهای دیگر پاک شده است.

هنوز هم لازم است که پس از غیر فعال کردن auditing، قسمت Event Viewer را پاک کرد برای اینکه بعد از استفاده از ابزار AuditPol، رخدادی مبنی بر غیر فعال شدن auditing، در این قسمت ثبت می‌شود. برای پاک کردن event log، ابزارهای زیادی وجود دارد.

ابزارهای هک

Elsave.exe، ابزار ساده‌ای برای پاک کردن event log است. این ابزار به صورت دستوری است.

WinZapper، ابزاری است که هکر می‌تواند برای پاک کردن رکوردهای انتخابی از رخدادها در security log ویندوز ۲۰۰۰، به کار رود. WinZapper، اطمینان می‌دهد که در طول اجرای برنامه، هیچ رخداد امنیتی ثبت نمی‌شود.

Evidence Eliminator، یک سیستم data cleansing برای کامپیوترهای ویندوزی است که از مخفی شدن همیشگی داده‌ها در سیستم جلوگیری می‌کند. این نرم‌افزار، قسمت‌های Recycle bin، Internet cache، system files، temp folders و ... را پاک می‌کند. Evidence Eliminator، می‌تواند توسط هکر برای پاک کردن شواهد و مدارک هک سیستم مورد استفاده قرار گیرد.

ابزارهای دیگری نیز برای پاک کردن ردپاها وجود دارند که مهم‌ترین آنها عبارتند از:

- Traceless
- Tracks Eraser Pro
- Aromor
- ZeroTracks
- PhatBooster

نویسنده: محسن آذرنژاد

Mohsen_Azarnejad@yahoo.com