# آموزِش sub seven



از Subseven مي‌توان به عنوان يک ابزار مدیریت از راه دور یا به عنوان

ابزاري براي Hack کردن استفاده نمود Subseven .شامل ۳ فایل است :

Sub7.exe ،Server.exeو .EditServer.exe براي استفاده از ،Sub7

Server.exeرا روي کامپيوتر قرباني اجرا کنيد (اینکه چگونه اینکار انجام

گیرد بعهده خواننده است). شماره IP او را بیابید و... در ادامه هر سوالی در

این باره داشته باشید پاسخ داده شده است و هیچ ابهامه باقی نمیماند...

سپس Sub7.exe را از کامپيوتر خودتان اجرا کنيد. پس از آن مي‌توانيد

اوقات خوشي با کامپيوتر قرباني داشته باشيد. شما مي‌توانيد قبل از

فرستادن ،Sub7 با استفاده از ،Editserver.exe سرویس دهنده را

پيکربندي کنيد.

## **Subseven**چگونه كار مي‌كند؟

بسيار ساده است. اولين باري كه Server.exe را روي كامپيوتر اجرا مي‌كنيد، برنامه در حافظه نصب مي‌شود و با هر بار راه‌اندازي مجدد ويندوز، آن نيز راه‌اندازي مي‌شود Sub7.exe. برنامه اصلي است كه شما براي ارتباط با Serverاز آن استفاده مي‌كنيد.



### پارامترهاي خط فرمان

شما مي‌توانيد Server.exe را با پارامترهاي خط فرمان زير اجرا كنيد:

/PASS:Password كلمه عبور براي برقرار ارتباط Password

مثلاً "Server.exe/pass:HPass/port:1777"، سرويس دهنده را روي پورت ۱۷۷۷ با استفاده از كلمه رمز "HPass" نصب مي‌كند.

ويژگيها



- **Setup Server:** شما مي‌توانيد قبل از ارسال سرويس دهنده به قرباني، آن را پيكربندي كنيد. براي انجام اين كار از **EditServer.exe** استفاده كنيد. براي مثال، اگر شما **Sub7** را در شماره **ICQ** خود نصب كنيد، زماني كه سرويس دهنده روي كامپيوتر قرباني اجرا شود **Sub7**، شماره **IP** قرباني را براي شما مي‌فرستد.
- **Pack** كردن **Server.exe** با فايل ديگر **EXE** يا با يک تصوير.
- شما مي‌توانيد **Resolution** صفحه نمايش قرباني را تغيير دهيد . **Sub7** ليستي از تمام **Resolution** هاي موجود روي كامپيوتر قرباني را نشان مي‌دهد و شما فقط يكي را انتخاب كنيد و **"Changit"** را بزنيد.

- **E-mail Notify:** به شما اجازه مي‌دهد تا **Email Server** و **Email** خود را مشخص کنید.

- شما مي‌توانيد تمام پردازش‌هاي اجرا شده **(Visiable** يا **Visiable)Non** را ببينيد. براي مثال، در صورتي که **Trojan** ديگري بر روي کامپيوتر قرباني نصب شده باشد، از اين امکان مي‌توان براي مشاهده آن استفاده کرد.

- **ويژگي چاپ :** به شما اجازه مي‌دهد تا يک متن مشخص را به روي چاپگر قرباني (به همراه **Style** و **Size** متن) چاپ نماييد.

- **Registry Editor:** هر چيزي در **Registry** را مشاهده، ايجاد، حذف و يا عوض کنيد.

- **ويژگي يافتن فايلها :** هر فايلي را روي ديسک سخت قرباني مي‌يابد. همچنين مي‌توانيد از کاراکترهاي عمومي (× و؟) هم استفاده کنيد.

- **Capslock، Scroll Lock** و **Numlock** مي‌توانند خاموش يا روشن شوند.

- **Disconnect Victim:** ارتباط قرباني با شبكه را قطع مي‌كند.

- **Focus Window:** در بخش **"Widnows Manager"** اضافه مي‌شود.

- مي‌توانيد كيفيت پيش نمايش تصوير و تصوير **Screenshot** را تعيين كنيد. اين امر در ارتباطات كند و آهسته موثر است، پايين‌تر بودن كيفيت معادل سريعترين بودن انتقال است.

- **Auto Notify** روي **UIN** تعيين شده، هنگامي كه اولين بار سرويس دهنده اجرا مي‌شود. بنابراين كار چنين پيش مي‌رود: شما سرويس دهنده را قبل از ارسال پيكربندي مي‌كنيد و شماره **ICQ** خود و يک نام (در صورتي كه سرويس دهنده را به بيش از يک قرباني ارسال مي‌كنيد) را تعيين مي‌كنيد. سپس سرويس دهنده را مي‌فرستيد و منتظر مي‌مانيد. هنگامي كه يک كاربر براي اولين بار بر روي آن كليک مي‌كند، شما از شماره **IP** قرباني، پورت و نامي كه براي **ICQ** تعيين كرده بوديد، باخبر مي‌شويد.

- **ويژگي نمايش تصوير** :به شما اجازه مي‌دهد تا از روي ديسک سخت قرباني يک تصوير را نمايش دهيد. اين تصوير مي‌تواند **JPG**، **BMP**، **GIF**، **ICO**، **WFM** و يا **EFM** باشد.



- شما مي‌توانيد طرف چند ثانيه ببينيد که قرباني روي **Desktop** خود چه کاري انجام مي‌دهد. اين درست شبيه يک ويدئوي زنده از صفحه نمايش قرباني است و اين ويژگي با ديگر ويژگيها هيچ تداخلي ندارد. بنابراين شما در واقع مي‌توانيد مشاهده کنيد که قرباني چه کليدهايي را مي‌زند، فايلهاي او را **Download** کنيد و **Desktop** او را ببينيد.



- **لغزش شديد صفحه نمايش** :شما مي‌توانيد صفحه نمايش قرباني را بطور افقي و عمودي و يا هر دو بلغزانيد. زماني که قرباني هرجا روي صفحه نمايش، دکمه سمت چپ را دوبار کليک کند **Desktop** ، مجدداً احيا مي‌شود.



- پنهان يا آشکار ساختن آيکنهاي **Desktop** قرباني.

- **برنامه :**(Subseven.exe) هر زمان که نسخه‌هاي جديدي منتشر مي‌شود (از ۳ را به بالا) شما را باخبر مي‌سازد. اين برنامه نسخه‌هاي جديد را چک مي‌کند و در صورتي که نسخه جديد منتشر شده باشد، يک پنجره (خوب و زيبا) در ارتباط با فايل جديد، اندازه فايل جديد تاريخ انتشار و حتي ليستي با تمام تغييرات به شما ارائه مي‌دهد. تمام اينها حتي بدون اجراي مرورگر صورت مي‌گيرد.

- **:**FTP Server ديسک سخت قرباني را به **FTP Server** تغيير مي‌دهد. شما مي‌توانيد با استفاده از يک برنامه **(FTP** شبيه **CuteFTP)** به هر فايلي دسترسي داشته باشيد. اين اساساً يک **Serv-U Clone** است که به شما اجازه دسترسي کامل به هر چيزي را مي‌دهد. هنگامي که **ServerFTP** را تنظيم مي‌کنيد، مي‌توانيد شماره پورت، **Password** موردنياز براي ارتباط و حداکثر تعداد سرويس گيرنده‌هايي که مي‌توانند در يک زمان ارتباط برقرار کنند را تعيين کنيد.

- **Message Manager:** شما مي‌توانيد پيامهاي سفارشي را به قرباني بفرستيد و مي‌توانيد نوع پنجره (سوالي، خبري و يا اخطاري)، عنوان پنجره، متن و حتي دكمه‌ها را مشخص كنيد. شما دكمه‌اي را كه توسط قرباني كليك مي‌شود را دريافت خواهيد كرد.
- **Online Notification:** را **On** يا **Off** كنيد.
- فقط **Uin** خود را وارد كنيد و **Enable** را فشار دهيد.
- **Ctrl-Alt-Del:** فعال و يا غيرفعال كردن هنگامي كه **Ctrl+Alt+Del** غيرفعال است، قرباني ديگر قادر به فشاردادن اين دكمه‌ها نخواهد بود. اين مسئله در مورد **Alt-Tab** نيز كار مي‌كند.
- **Send Keys:** شما مي‌توانيد كليدهاي مخصوص خود را تايپ كنيد.
- پيامها يا سوالات را بصورت مشخص شده به كامپيوتر قرباني بفرستيد. شما از پاسخ قرباني مطلع خواهيد شد.
- مرورگر پيش فرض را در آدرس مشخص شده باز كنيد.

- از **Desktop** قرباني يک **Screenshot** بگيريد. تصوير بصورت **desktop.jpg**ذخيره و نشان داده مي‌شود.
- دکمه **Start** را آشکار يا مخفي کنيد.
- صفحه کليد را غيرفعال کنيد.
- **Chat**کردن با قرباني: يک پنجره کوچک مانند **ICQ Chat** در هر دو کامپيوتر ظاهر مي‌شود. تفاوت در اين است که روي کامپيوتر قرباني، اين پنجره **Chat** هميشه بصورت **Stay-on-top** خواهد بود. هنگام**Chat** کردن مي‌توانيد چند کار انجام دهيد؛ مانند پنهان کردن فضاي تايپ قرباني (بدين معني که پنجره کوچکي که محل تايپ قرباني است ناپديد مي‌شود **Start**،(و يا **Stop** کردن بلندگوي کامپيوتر قرباني.
- قرباني قادر به متوقف کردن آن **Chat** نمي‌باشد، بنابراين تا زماني که شما اين **Chat** را متوقف نکنيد، قرباني مجبور است تمام مدت در آنجا بماند.

- **Start**و يا **Stop** كردن بلندگوي قرباني.
- راه‌اندازي مجدد ويندوز. (اما از اين كار سوءِ استفاده نكنيد).
- باز و بسته كردن **.CD-ROM**
- قراردادن **Password** براي سرويس دهنده. (اين در صورتي است كه شمانخواهيد افراد ديگري كه **Subseven** دارند از آن سرويس دهنده استفاده كنند).
- طولي **Mouse Trail** قرباني را تنظيم كنيد.
- بدست آوردن تمام پنجره‌هاي فعال روي كامپيوتر قرباني، پس از آن مي‌توانيد:

-يک پنجره خاص را ببنديد.

-يک پنجره مشخص را فعال يا غيرفعال كنيد.

-دكمه **Close** روي يک پنجره خاص را غيرفعال كنيد.

-پنجره مشخصي را پنهان يا آشكار سازيد.

- بدست آوردن ليستي از تمام درايوهاي موجود در كامپيوتر قرباني.

- خاموش و روشن کردن مانیتور، این ویژگي در مورد مانیتورهایي کار مي‌کند که مي‌توانند بطور نرم‌افزاري خاموش شوند.
- آشکار یا پنهان کردن **Taskbar.**
- بدست آوردن اطلاعات بیشتر در مورد کامپیوتر قرباني: مانند نسخه ویندوز، نام کاربر، نام شرکت **Resolution** ،صفحه نمایش و غیره.
- تغییردادن نام سرویس دهنده: سرویس دهنده نام مشخص شده را ذخیره مي‌کند.
- **دیدن تمام کلیدهاي فشار داده شده :**شما تمام کلیدهایي را که توسط قرباني فشار داده مي‌شوند خواهید دید. این ویژگي براي بدست آوردن **Password** مفید است.
- ضبط کردن صداهایي که از بلندگوي کامپیوتر قرباني شنیده مي‌شود.
- File Manager:شما مي‌توانید به راحتي تمام فایلها و فولدرها را روي کامپیوتر قرباني ببینید. هنگامي که شما روي یک دایرکتوري دوبار کلیک مي‌کنید، سرویس دهنده به آن دایرکتوري مي‌رود.

زماني كه فايلي را انتخاب مي‌كنيد مي‌توانيد:

-اندازه فايل را بدست آوريد.

-آن را بصورت(**Wallpaper** تنها در صورتي كه يک فايل **JPG** يا **BMP**باشد) در آوريد.



-آن را **download** كنيد.

-آن را حذف كنيد.

-آن را روي كامپيوتر قرباني **Play** كنيد (تنها در صورتي كه آن يک فايل **WAV** باشد).

-آن را اجرا كنيد (برنامه‌اي كه براي بازكردن آن فايل اختصاص داده شده، روي كامپيوتر قرباني اجرا خواهد شد).

- معكوس كردن دكمه‌هاي ماوس.
- بستن سرويس‌دهنده روي كامپيوتر قرباني (توجه: سرويس دهنده دفعه ديگر با **Start** شدن ويندوز قرباني **Start**، مي‌شود).

- پاک کردن سرويس دهنده از کامپيوتر قرباني، اين ويژگي سرويس دهنده را کاملاً از حافظه پاک خواهد کرد.

- تغيير پورت استفاده شده: شما مي‌توانيد اين عمل را به دو صورت انجام دهيد: اجراي **"Server.exe/port:****"** و يا اتصال به سرويس دهنده با **Sub7** و کليک کردن **."Changport"**

- اسکنر **:IP** اين اسکنر تنها سرويس دهنده‌هاي**Sub7** را اسکن مي‌کند و به همين دليل است که شما به پورت نياز نداريد. (اين اسکنر روش مخصوص خود را براي تشخيص سرويس دهنده دارد.) اگر شما يک **IP**آلوده را يافتيد، بدين معني نيست که شما مي‌توانيد ارتباط برقرار کنيد. شما هنوز هم نياز به پورت (در صورتي که غير از ۱۲۴۳ باشد) و**)Password** در صورت **Set** شدن) داريد.

- بدست آوردن**Password**ها: شما از زمان راه‌اندازي، ليستي با تمام **Password**هاي ضبط شده از روي کامپيوتر قرباني بدست خواهيد آوريد.

- Offline Key Logger : **"get offline keys"** از زمان راه‌اندازي

ويندوز، ليستي از تمام كليدهاي فشرده شده را بازيابي مي‌كند.

البته تمامي امكانات گفته شده، براي نفوذ به سيستم ديگران نيست، بلكه ما





اين موارد را توضيح داديم تا شما بدانيد نفوذگران با چه روشهايي مي‌توانند به كامپيوتر شما نفوذ كرده و بعضاً صدمه برسانند.

به نقل از : ماهنامه رايانه