

# آموزش sub seven

از Subseven می‌توان به عنوان یک ابزار مدیریت از راه دور یا به عنوان ابزاری برای Hack کردن استفاده نمود. Subseven شامل ۳ فایل است :  
Sub7.exe، Server.exe، و EditServer.exe. برای استفاده از Sub7،

Server.exe را روی کامپیوتر قربانی اجرا کنید (اینکه چگونه اینکار انجام

گیرد بعهدہ 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 نماند...

سپس Sub7.exe را از کامپیوتر خودتان اجرا کنید. پس از آن می‌توانید

اوقات خوشی با کامپیوتر قربانی داشته باشید. شما می‌توانید قبل از

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

پیکربندی کنید.

parsi e-book  
WWW.PARSIBOOK.4T.COM

## Subseven چگونه کار می کند؟

بسیار ساده است. اولین باری که Server.exe را روی کامپیوتر اجرا می کنید،

برنامه در حافظه نصب می شود و با هر بار راه اندازی مجدد ویندوز، آن

نیز راه اندازی می شود Sub7.exe. برنامه اصلی است که شما برای ارتباط با

Server از آن استفاده می کنید.

### پارامترهای خط فرمان

شما می توانید Server.exe را با پارامترهای خط فرمان زیر اجرا کنید:

Password کلمه عبور برای برقرار ارتباط /PASS:Password

مثلاً "Server.exe/pass:HPass/port:1777" ،سرویس دهنده را روی

پورت ۱۷۷۷ با استفاده از کلمه رمز "HPass" نصب می کند.

parsi e-book  
WWW.PARSIBOOK.4T.COM

## ویژگیها

• **Setup Server:** شما می‌توانید قبل از ارسال سرویس دهنده به

قربانی، آن را پیکربندی کنید. برای انجام این کار از

**EditServer.exe** استفاده کنید. برای مثال، اگر شما **Sub7** را در

شماره **ICQ** خود نصب کنید، زمانی که سرویس دهنده روی

کامپیوتر قربانی اجرا شود **Sub7**، شماره **IP** قربانی را برای شما

می‌فرستد.

• **Pack** کردن **Server.exe** با فایل دیگر **EXE** یا با یک تصویر.

• شما می‌توانید **Resolution** صفحه نمایش قربانی را تغییر دهید .

**Sub7** لیستی از تمام **Resolution** های موجود روی کامپیوتر قربانی

را نشان می‌دهد و شما فقط یکی را انتخاب کنید و "**Changit**" را

بزنید.

• **E-mail Notify** به شما اجازه می‌دهد تا **Email و Email Server**

خود را مشخص کنید.

• شما می‌توانید تمام پردازش‌های اجرا شده (**Visiable** یا

**Non Visiable**) را ببینید. برای مثال، در صورتی که **Trojan** دیگری

بر روی کامپیوتر قربانی نصب شده باشد، از این امکان می‌توان برای

مشاهده آن استفاده کرد.

• **ویژگی چاپ**: به شما اجازه می‌دهد تا یک متن مشخص را به روی

چاپگر قربانی (به همراه **Style** و **Size** متن) چاپ نمایید.

• **Registry Editor**: هر چیزی در **Registry** را مشاهده، ایجاد، حذف

و یا عوض کنید.

• **ویژگی یافتن فایلها**: هر فایلی را روی دیسک سخت قربانی می‌یابد.

همچنین می‌توانید از کاراکترهای عمومی (x و ؟) هم استفاده کنید.

• **Scroll Lock، Capslock و Numlock** می‌توانند خاموش یا

روشن شوند.

- **Disconnect Victim:** ارتباط قربانی با شبکه را قطع می‌کند.

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

می‌شود.

- می‌توانید کیفیت پیش نمایش تصویر و تصویر **Screenshot** را تعیین

کنید. این امر در ارتباطات کند و آهسته موثر است، پایین تر بودن

کیفیت معادل سریعترین بودن انتقال است.

- **Auto Notify** روی **UIN** تعیین شده، هنگامی که اولین بار سرویس

دهنده اجرا می‌شود. بنابراین کار چنین پیش می‌رود: شما سرویس

دهنده را قبل از ارسال پیکربندی می‌کنید و شماره **ICQ** خود و یک

نام (در صورتی که سرویس دهنده را به پیش از یک قربانی ارسال

می‌کنید) را تعیین می‌کنید. سپس سرویس دهنده را می‌فرستید و

منتظر می‌مانید. هنگامی که یک کاربر برای اولین بار بر روی آن

کلیک می‌کند، شما از شماره **IP** قربانی، پورت و نامی که برای **ICQ**

تعیین کرده بودید، باخبر می‌شوید.

- **ویژگی نمایش تصویر:** به شما اجازه می‌دهد تا از روی دیسک

سخت قربانی یک تصویر را نمایش دهید. این تصویر می‌تواند **JPG**

**WFM، ICO، GIF، BMP** و یا **EFM** باشد.

- شما می‌توانید طرف چند ثانیه ببینید که قربانی روی **Desktop** خود

چه کاری انجام می‌دهد. این درست شبیه یک ویدئوی زنده از صفحه

نمایش قربانی است و این ویژگی با دیگر ویژگیها هیچ تداخلی ندارد.

بنابراین شما در واقع می‌توانید مشاهده کنید که قربانی چه کلیدهایی

را می‌زند، فایل‌های او را **Download** کنید و **Desktop** او را ببینید.

- **لغزش شدید صفحه نمایش:** شما می‌توانید صفحه نمایش قربانی

را بطور افقی و عمودی و یا هر دو بلغزانید. زمانی که قربانی هر جا

روی صفحه نمایش، دکمه سمت چپ را دوبار کلیک کند **Desktop**،

مجدداً احیا می‌شود.

- پنهان یا آشکار ساختن آیکنهای **Desktop** قربانی

• **برنامه:** (Subseven.exe) هر زمان که نسخه‌های جدیدی منتشر

می‌شود (از ۳ را به بالا) شما را باخبر می‌سازد. این برنامه نسخه‌های

جدید را چک می‌کند و در صورتی که نسخه جدید منتشر شده باشد،

یک پنجره (خوب و زیبا) در ارتباط با فایل جدید، اندازه فایل جدید

تاریخ انتشار و حتی لیستی با تمام تغییرات به شما ارائه می‌دهد. تمام

اینها حتی بدون اجرای مرورگر صورت می‌گیرد.

• **FTP Server:** دیسک سخت قربانی را به **FTP Server** تغییر

می‌دهد. شما می‌توانید با استفاده از یک برنامه **FTP** شبیه

(**CuteFTP**) به هر فایلی دسترسی داشته باشید. این اساساً یک

**Serv-U Clone** است که به شما اجازه دسترسی کامل به هر چیزی

را می‌دهد. هنگامی که **ServerFTP** را تنظیم می‌کنید، می‌توانید

شماره پورت، **Password** مورد نیاز برای ارتباط و حداکثر تعداد

سرویس گیرنده‌هایی که می‌توانند در یک زمان ارتباط برقرار کنند را

تعیین کنید.

• **Message Manager:** شما می‌توانید پیام‌های سفارشی را به قربانی

بفرستید و می‌توانید نوع پنجره (سوالی، خبری و یا اخطاری)، عنوان

پنجره، متن و حتی دکمه‌ها را مشخص کنید. شما دکمه‌ای را که

توسط قربانی کلیک می‌شود را دریافت خواهید کرد.

پارسی‌بوک  
www.parsibook.com

• **Online Notification** را **On** یا **Off** کنید.

• فقط **Uin** خود را وارد کنید و **Enable** را فشار دهید.

• فعال و یا غیرفعال کردن **Ctrl-Alt-Del**: هنگامی که

**Ctrl+Alt+Del** غیرفعال است، قربانی دیگر قادر به فشار دادن این

دکمه‌ها نخواهد بود. این مسئله در مورد **Alt-Tab** نیز کار می‌کند.

• **Send Keys:** شما می‌توانید کلیدهای مخصوص خود را تایپ کنید.

• پیام‌ها یا سوالات را بصورت مشخص شده به کامپیوتر قربانی

بفرستید. شما از پاسخ قربانی مطلع خواهید شد.

• مرورگر پیش فرض را در آدرس مشخص شده باز کنید.

پارسی‌بوک  
www.parsibook.com

- از Desktop قربانی یک Screenshot بگیرید. تصویر بصورت

desktop.jpg ذخیره و نشان داده می‌شود.

- دکمه Start را آشکار یا مخفی کنید.

- صفحه کلید را غیرفعال کنید.

- Chat کردن با قربانی: یک پنجره کوچک مانند ICQ Chat در هر

دو کامپیوتر ظاهر می‌شود. تفاوت در این است که روی کامپیوتر

قربانی، این پنجره Chat همیشه بصورت Stay-on-top خواهد بود.

هنگام Chat کردن می‌توانید چند کار انجام دهید؛ مانند پنهان کردن

فضای تایپ قربانی (بدین معنی که پنجره کوچکی که محل تایپ

قربانی است ناپدید می‌شود Start) (و یا Stop کردن بلندگویی

کامپیوتر قربانی.

- قربانی قادر به متوقف کردن آن Chat نمی‌باشد، بنابراین تا زمانی

که شما این Chat را متوقف نکنید، قربانی مجبور است تمام مدت در

آنجا بماند.

- **Start** و یا **Stop** کردن بلند گوی قربانی.

- راه اندازی مجدد ویندوز. (اما از این کار سوء استفاده نکنید).

- باز و بسته کردن **CD-ROM**.

- قراردادن **Password** برای سرویس دهنده. (این در صورتی است

که شما نخواهید افراد دیگری که **Subseven** دارند از آن سرویس

دهنده استفاده کنند).

- طولی **Mouse Trail** قربانی را تنظیم کنید.

- بدست آوردن تمام پنجره های فعال روی کامپیوتر قربانی، پس از آن

می توانید:

-یک پنجره خاص را ببندید.

-یک پنجره مشخص را فعال یا غیر فعال کنید.

-دکمه **Close** روی یک پنجره خاص را غیر فعال کنید.

-پنجره مشخصی را پنهان یا آشکار سازید.

- بدست آوردن لیستی از تمام درایوهای موجود در کامپیوتر قربانی.

- خاموش و روشن کردن مانیتور، این ویژگی در مورد مانیتورهای

کار می‌کند که می‌توانند بطور نرم‌افزاری خاموش شوند.

- آشکار یا پنهان کردن **Taskbar**.

- بدست آوردن اطلاعات بیشتر در مورد کامپیوتر قربانی: مانند نسخه

ویندوز، نام کاربر، نام شرکت **Resolution**، صفحه نمایش و غیره.

- تغییر دادن نام سرویس دهنده: سرویس دهنده نام مشخص شده را

ذخیره می‌کند.

- دیدن تمام کلیدهای فشار داده شده: شما تمام کلیدهای را که

توسط قربانی فشار داده می‌شوند خواهید دید. این ویژگی برای

بدست آوردن **Password** مفید است.

- ضبط کردن صداهایی که از بلندگوی کامپیوتر قربانی شنیده می‌شود.

- **File Manager:** شما می‌توانید به راحتی تمام فایلها و فولدرها را

روی کامپیوتر قربانی ببینید. هنگامی که شما روی یک دایرکتوری

دوبار کلیک می‌کنید، سرویس دهنده به آن دایرکتوری می‌رود.

زمانی که فایلی را انتخاب می‌کنید می‌توانید:

-اندازه فایل را بدست آورید.

-آن را بصورت **Wallpaper** تنها در صورتی که یک فایل **JPG** یا

**BMP** باشد) در آورید. کپی برداری بدون ذکر نام منبع مجاز نیست

**parsi e-book**

-آن را **download** کنید.

-آن را حذف کنید.

-آن را روی کامپیوتر قربانی **Play** کنید (تنها در صورتی که آن یک

فایل **WAV** باشد).

-آن را اجرا کنید (برنامه‌ای که برای باز کردن آن فایل اختصاص داده

شده، روی کامپیوتر قربانی اجرا خواهد شد).

• معکوس کردن دکمه‌های ماوس.

• بستن سرویس دهنده روی کامپیوتر قربانی (توجه: سرویس دهنده

دفعه دیگر با **Start** شدن ویندوز قربانی **Start** می‌شود).

**parsi e-book**  
**WWW.PARSIBOOK.AT.COM**

- پاک کردن سرویس دهنده از کامپیوتر قربانی، این ویژگی سرویس دهنده را کاملاً از حافظه پاک خواهد کرد.
- تغییر پورت استفاده شده: شما می‌توانید این عمل را به دو صورت انجام دهید: اجرای "Server.exe/port:\*\*\*\*" و یا اتصال به سرویس دهنده با Sub7 و کلیک کردن "Changport".
- اسکنر IP: این اسکنر تنها سرویس دهنده‌های Sub7 را اسکن می‌کند و به همین دلیل است که شما به پورت نیاز ندارید. (این اسکنر روش مخصوص خود را برای تشخیص سرویس دهنده دارد.) اگر شما یک IP آلوده را یافتید، بدین معنی نیست که شما می‌توانید ارتباط برقرار کنید. شما هنوز هم نیاز به پورت (در صورتی که غیر از ۱۲۴۳ باشد) و Password در صورت Set شدن دارید.
- بدست آوردن Password ها: شما از زمان راه‌اندازی، لیستی با تمام Password های ضبط شده از روی کامپیوتر قربانی بدست خواهید آورد.

• Offline Key Logger : "get offline keys" از زمان راه اندازی

ویندوز، لیستی از تمام کلیدهای فشرده شده را بازیابی می کند.

البته تمامی امکانات گفته شده، برای نفوذ به سیستم دیگران نیست، بلکه ما

این موارد را توضیح دادیم تا شما بدانید نفوذگران با چه روشهایی می توانند

به کامپیوتر شما نفوذ کرده و بعضاً صدمه برسانند.

به نقل از : ماهنامه رایانه



parsi e-book  
WWW.PARSIBOOK.4T.COM