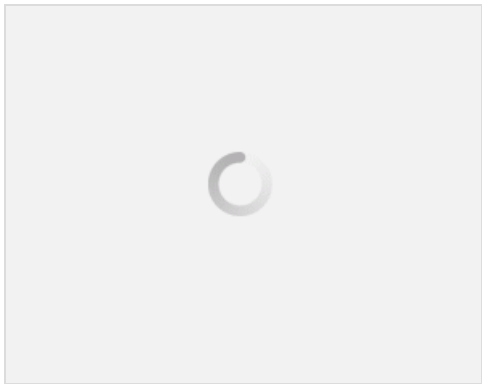
Meterpreter Shell چیست و چه کاربردی دارد؟ بخش دوم (نسخه PDF)

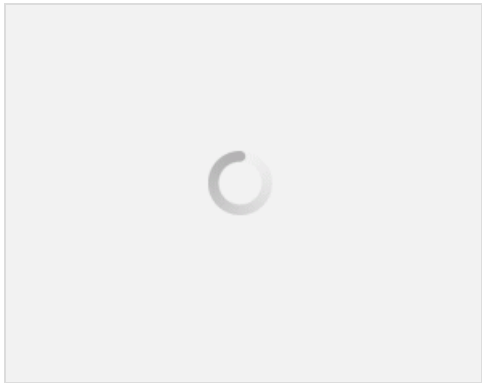
خوب دوستان عزیز در قسمت پیش آخرین بحثی را که مورد آموزش قرار دادیم، دسترسی به دایرکتوری سیستم لوکال در Meterpreter shell بود. گفتیم که با کمک دو دستور زیر میتوانیم اینکار را انجام دهیم :

- Getlwd & lpwd: به شما دایرکتوری موجود در سیستم لوکال را نشان خواهد داد.
- Lcd: مسیر دایرکتوری لوکال را تغییر میدهد.

اما قبل از شروع ادامه بحث، پیشنهاد میکنم مجددا مطالعه ای به قسمت اول این آموزش داشته باشید تا بتوانیم با خیالی راحت قسمت دوم را شروع کنیم. پس با ما همراه باشید : برای بررسی دایرکتوری لوکالی را که الان در آن هستیم و تغییر مسیر به دایرکتوری دسکتاپ بر روی سیستم کالی، مراحل زیر را باید انجام دهیم:



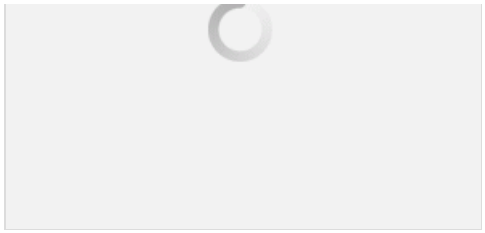
قابلیت دانلود به ما این امکان را میدهد تا بتوانیم فایل هایی را از سیستم هدف بر روی سیستم خود دانلود کنیم و بلعکس قابلیت آپلود به ما اجازه میدهد تا به سیستم ریموت یا همان هدف فایل ارسال کنیم.بنابراین اگر قصد آپلود فایل را دارید، فقط کافیست که به دایرکتوری های مورد نظر در سیستم لوکال (کالی) و سیستم ریموت وصل شویم و دستور آپلود را اجرایی کنیم. قالب این دستور بصورت زیر میباشد:



در شکل بالا ما به دسکتاپ کالی و جایی که میخواهیم فایل هایمان را در کالی برای آپلود انتخاب کنیم، وصل شدیم. سپس به پوشه تست در سیستم هدف وصل شدیم و خیلی ساده با استفاده از دستور "Upload" فرمان انتقال فایل را صادر کردیم.

- **نکته:** در خط هفتم در مجموعه فرمان های بالا و در فرمان "Upload tools"، عبارت "Tools" نام فایلی است که قصد آپلود ان را داریم.

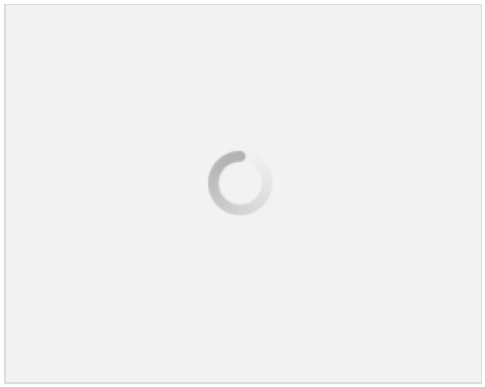
به عکس؛ عمل دانلود نیز در همان مسیری که گفته شد صورت می پذیرد؛ فقط کافیست که در دستور صادره عبارت download را جایگزین Upload کرده و در ادامه نام فایلی را که میخواهیم دانلود شود، بیاوریم. همه چیز برای دانلود فایل از سیستم ریموت یا همان هدف به سیستم کالی یا لوکالمان آماده ست:



خوب حالا میخواهیم در ادامه آموزشمان نگاهی بر Network Command بیاندازیم.

Network Commands

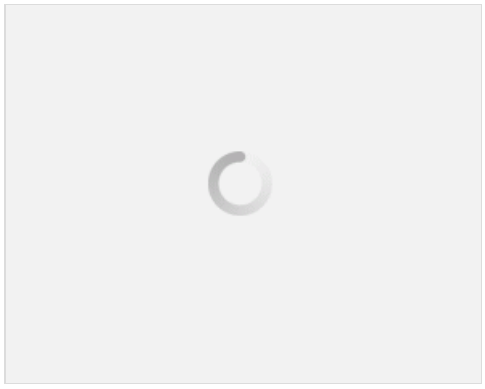
این دستورات بشما این امکان را میدهند تا برخی خصوصیات شبکه ای را ببینید و دستکاری کنید.



- Arp: لیستی از تناظر آدرس های مک سیستم های ریموت با ادرس IP واقعیشان را نشان میدهد.
- Ifconfig و ipconfig: هر دوی این دستورات مشخصات شبکه ای در سیستم ریموت را نشان میدهد. (ifconfig در لینوکس و ipconfig در ویندوز)
- Netstat: لیستی از کانکشن های فعال در شبکه را نشان میدهد.
- Portfwd and route: به شما این امکان را میدهد تا برخی از حملات پیشرفته routing را انجام دهید.

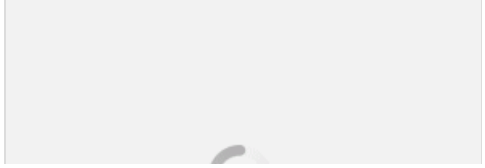
System Commands

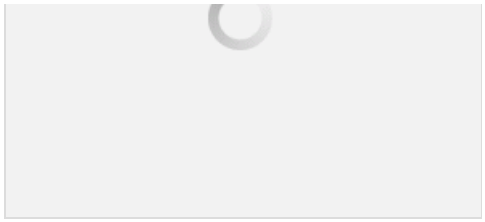
در زیر لیستی از دستورات سیستمی آورده شده است. در این آموزش مجال توضیح و پوشش تک تک آن ها را نداریم اما جهت اشنایی آن را مرور میکنیم:



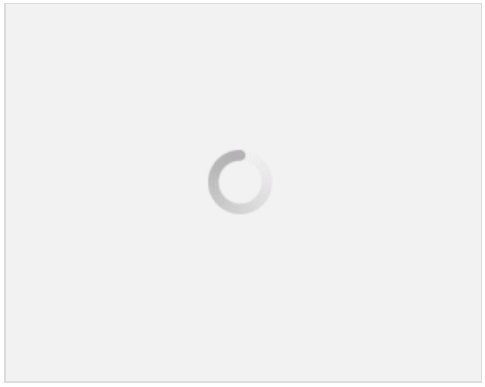
- CLEAREV: این دستور تلاش میکند تا لاگ های بجا مانده از شما را بر روی سیستم هدف پاکسازی کند.

ممکن است شـما بخواهیـد تا تمام آثار و ردپاهای بجا مانده از نفوذ خود را از روی سیسـتم هدف پاک نمایید. اگر به لاگ های موجود در ویندوز ۷ نگاهی بیاندازیم، متوجه خواهیم شد این لاگ ها پر از اتفاقات مختلف است:

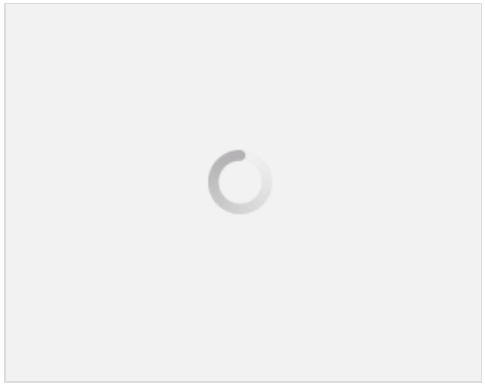




برخی از این event ها ممکن است شامل همان کارهایی باشـد که از نفوذ ما بجا مانده است. بنابراین میتوانیم بصورت ریموت و از راه دور از پشت سیستم کالی با تایپ عبارت "clearev" آن ها را پاک کنیم:



لاگ های اپلیکیشن، سیسـتم و امنیتی از بین میرونـد. اگر مجددا به لاگ های امنیتی نگاهی بیاندازیم، فقط یک رکورد را میتوانیم در آن مشاهده کنیم و آن رکورد "Log Clear" است:

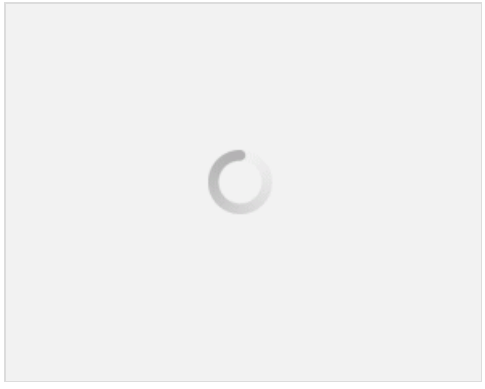


GETPID & PS COMMANDS

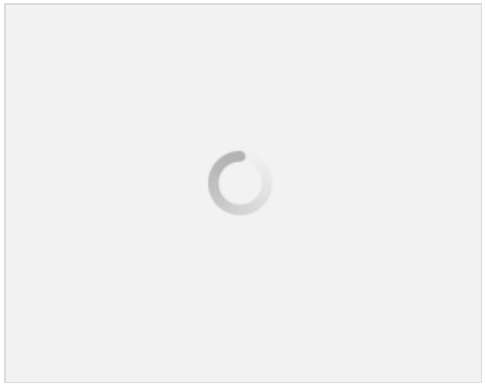
اگر از Meterpreter استفاده میکنید، با این دو فرمان زیاد برخورد خواهید کرد:

- Getpid: بشما میگوید که چه فرآیندی (ID آن(در شل در حال اجراست.
- Ps: لیستی از تمام فرآیند های در حال اجرا در سیستم هدف را نشان میدهد.

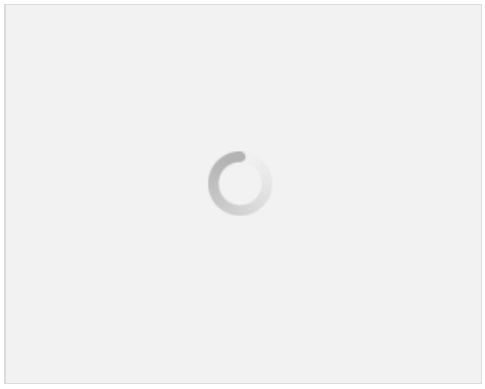
بنابراین اگر عبارت "getpid" را تایپ کنید، خواهید دید:



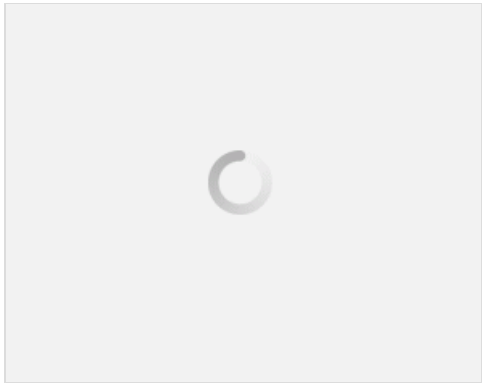
این شماره ID فرآینـدی است که شل شـما از آن اسـتفاده میکند. اگر عبارت "ps" را تـایپ کنیم، میتوانیم تمام فرآینـدهای در حال اجرا را ببینیم:



اگر لیست را بسمت پایین مرور کنیم، میتوانیم شماره ۳۸۲۴ pid را مشاهده کنیم:



در این شـکل همچنین مشاهده خواهیم کرد که این فرآیند تحت فرآیند "powershell.exe" و کاربری "Fred" در حال اجراست.این اطلاعات زمانی بکار میآیند که بخواهیم از یک فرایند با سـطح دسترسـی پایین به یک فرایند با سـطح دسترسی بالا تغیر حالت دهیم. ما میتوانیم شل فعالمان در این PID را به فرایندی که سطح دسترسی بالاتری دارد، منتقل (Migrate) کنیم. این انتقال که به "Migrating" معروف است، به ما این امکان را میدهد تا شل –مان- را در فرآیند پرکاربردتری دیگری ترکیب و یا مخفی کنیم و این در حالی است که این کار با ماهیت یک کانکشن مخفی صورت میپـذیرد. "Explorer.exe" یکی از فراینـدهای پرکاربردیست که معمولا به آن تغیر وضـعیت میدهند.برای مثال شماره PID فرایندی که میخواهید از آن استفاده کنید را پیدا کنید (در مثال ما ۱۷۳۶ است) و عبارت "Migrate <PID#>" را تایپ کنید:



در این مورد و دسـتورات Meterpreter در آینـده بیشتر صـحبت خواهیم کرد. فعلا قصـد داریم تا در بخش بعد از این آموزش به اسـکرین شات و استفاده از وب‌کم از راه دور بپردازیم.

ادامه دارد...

سربلند و مانا باشید.

پایان

نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

شرکت کنم و کپی برداری بدون ذکر منبع و نام نویسنده دارای اشکال اخلاقی می باشد.

Synaa۹۰
سلام تشکر می‌کنم بابت آموزش هاتون این بخش واقعا عالی بود و به ادامه آموزش بپردازید

مطلب اصلی