# Koadic - COM命令和控制框架

Koadic-COM框架可以说是一个专门针对，windows无文件落地攻击了。他的攻击模块都是使用wmic,msth,powershell。虽然现在这款工具都被AMSI整个拉入黑名单，不过学习一下怎么使用还是不错的

Github仓库:https://github.com/zerosum0x0/koadic

安装过程是这样的：

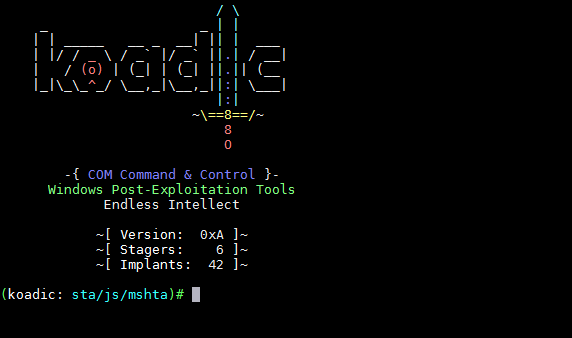
Git clone <https://github.com/zerosum0x0/koadic>

Apt-get install python3-pip

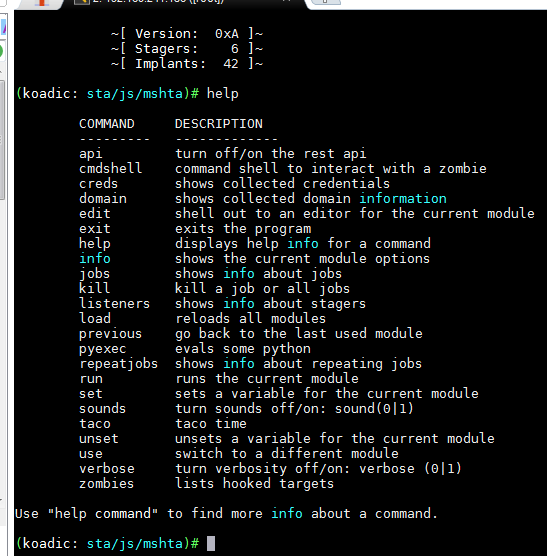
Pip3 install -r requirements.txt

运行：

Python3 koadic.py



help可以看到帮助



他的模块有以下这些

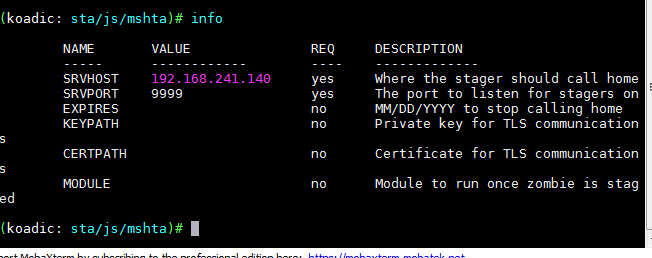
|  |  |
| --- | --- |
| stager/js/mshta | 使用MSHTA.exe HTML应用程序提供有效负载 |
| stager/js/regsvr | 使用regsvr32.exe COM + scriptlet提供有效负载 |
| stager/js/wmic | 使用WMIC XSL提供有效载荷 |
| stager/js/rundll32\_js | 使用rundll32.exe提供有效负载 |
| stager/js/disk | 使用磁盘上的文件提供有效负载 |

Payload模块有这些

后渗透模块有

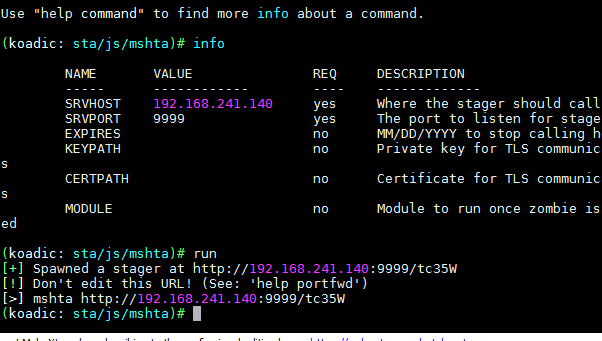
|  |  |
| --- | --- |
| implant/elevate/bypassuac\_eventvwr | 使用enigma0x3的eventvwr.exe漏洞绕过Windows 7,8和10上的UAC and 10. |
| implant/elevate/bypassuac\_sdclt | 使用enigma0x3的sdclt.exe漏洞绕过Windows 10上的UAC。 |
| implant/fun/zombie | 最大音量并在隐藏的窗口中打开蔓越莓YouTube |
| implant/fun/voice | 通过文本转语音播放消息。 |
| implant/gather/clipboard | 检索用户剪贴板的当前内容。 |
| implant/gather/enum\_domain\_info | 检索有关Windows域的信息。 |
| implant/gather/enum\_printers | 检索有关打印机连接的信息。 |
| implant/gather/hashdump\_sam | 从SAM配置单元检索散列密码。 |
| implant/gather/hashdump\_dc | |  | | --- | | 域控制器哈希来自NTDS.dit文件。 | |
| implant/gather/user\_hunter | 找到登录到域计算机的用户（使用Dynamic Wrapper X）。namic Wrapper X). |
| implant/inject/mimikatz\_dynwrapx | 注入一个反射加载的DLL来运行powerkatz.dll（使用Dynamic Wrapper X）。. |
| implant/inject/mimikatz\_dotnet2js | 注入一个反射加载的DLL来运行powerkatz.dll（@tirannido DotNetToJS）。 |
| implant/inject/shellcode\_excel | 运行任意shellcode有效负载（如果安装了Excel）。 |
| implant/manage/enable\_rdesktop | 在目标上启用远程桌面。 |
| implant/manage/exec\_cmd | 在目标上运行任意命令，并可选择接收输出。 |
| implant/persist/add\_user | 创建本地/域用户。 |
| implant/persist/registry | 将Koadic有效负载添加到注册表。 |
| implant/persist/schtasks | 添加Koadic有效负载作为计划任务。 |
| implant/persist/wmi | 添加Koadic有效负载作为WMI订阅。 |
| implant/phishing/password\_box | 提示用户输入密码。 |
| implant/pivot/stage\_wmi | 使用WMI将僵尸挂在另一台机器上。 |
| implant/pivot/exec\_psexec | 使用sysinternals中的psexec在另一台计算机上运行命令。 |
| implant/scan/tcp | 使用HTTP扫描目标僵尸LAN上的打开TCP端口。 |
| implant/utils/download\_file | 从目标僵尸下载文件。 |
| implant/utils/multi\_module | 连续运行一些植入物。 |
| implant/utils/upload\_file | 将文件从侦听服务器上载到目标僵尸。 |

使用info可以查看模块使用的帮助

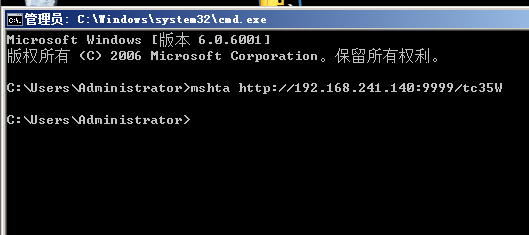


PS:只需要设置REQ有YES的即可

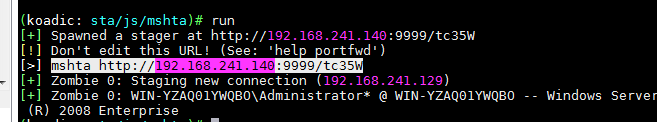
Run运行模块生成荷载



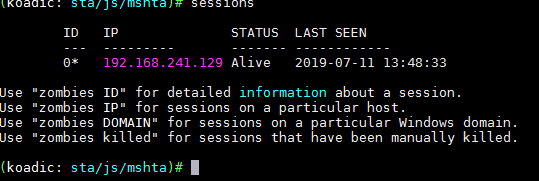
将这条命令在目标机子上执行



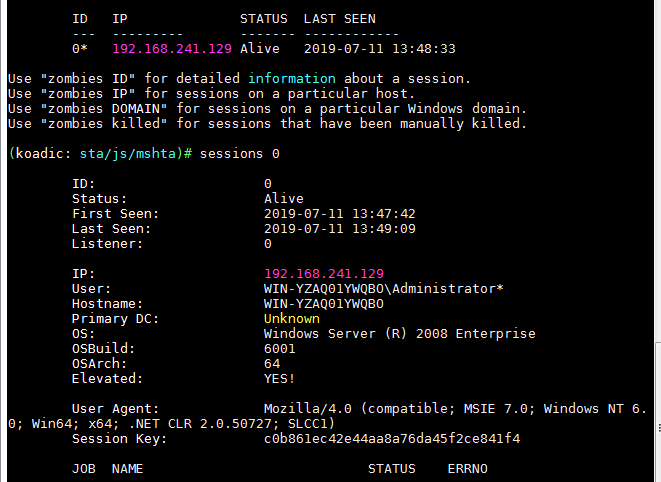
反弹到的sessions



输入sessions可以查看到反弹回来分配的ID



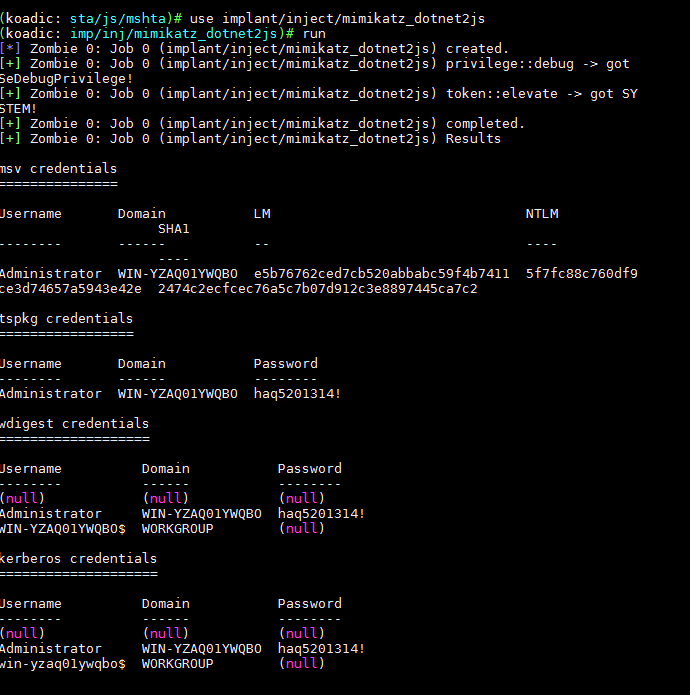
Sessions <ID>可以看到机子详细的帮助信息



那么可以用一些后渗透模块了

use implant/inject/mimikatz\_dotnet2js #加载mimikatz抓取密码

Run



执行命令

