内网渗透

1. 操作系统信息收集

系统信息：Systeminfo

用户信息：whoami、query user、net user、net localgroup

网络信息：ipconfig /all、net share、net session、net view、netstat

文件信息：cmdkey /l、host文件、回收站、硬盘文件

1. Windows凭证收集

Windows hash

SAM提取

Lsass.exe