



# 北京大学网络攻防技术与实践课程

---

## 3. 网络信息收集技术(下)

诸葛建伟

zhugejianwei@icst.pku.edu.cn

北京大学计算机研究所信安中心



# 内容

---

- 1. 网络扫描技术**
- 2. 课堂实践：nmap扫描**
- 3. 网络查点技术**
- 4. 作业3—搜索自己的互联网足迹/网络扫描实验**



# 系统类型探查

- 系统类型探查：探查活跃主机的系统及开放网络服务的类型
  - 目标主机上运行着何种类型什么版本的操作系统
  - 各个开放端口上监听的是哪些网络服务
- 目的
  - 为更为深入的情报信息收集，真正实施攻击做好准备
  - 如远程渗透攻击需了解目标系统操作系统类型，并配置

技术类型	技术目标与特性	经典工具
操作系统主动探测技术	主动与目标系统通信探测目标系统操作系统	nmap -O, queso
操作系统被动辨识技术	被动监测网络通信以识别目标系统操作系统	P0f, siphon
网络服务主动探测技术	主动与目标系统通信探测目标网络中开放端口上绑定的网络应用服务类型和版本	nmap -sV,
网络服务被动辨识技术	被动监测网络通信以识别目标网络中开放端口上绑定的网络应用服务类型和版本	PADS



# 操作系统类型探查

- 操作系统类型探查(**OS Identification**)
  - 通过各种不同操作系统类型和版本实现机制上的差异
  - 通过特定方法以确定目标主机所安装的操作系统类型和版本的技术手段
  - 明确操作系统类型和版本是进一步进行安全漏洞发现和渗透攻击的必要前提
- 不同操作系统类型和版本的差异性
  - 协议栈实现差异—协议栈指纹鉴别
  - 开放端口的差异—端口扫描
  - 应用服务的差异—旗标攫取
- 辨识方式
  - 主动—操作系统主动探测技术
  - 被动—被动操作系统识别技术



# 操作系统主动探测

## □ 操作系统主动探测技术

- 端口扫描
- 应用服务旗标攫取
- 主动协议栈指纹鉴别

## □ 主动协议栈指纹鉴别

- **Fyodor, Phrack, Remote OS detection via TCP/IP Stack Finger-Printing, 1998.**
- 鉴别项: **FIN, BOGUS flag, ISN采样, DF位, TCP初始窗口大小, ACK值, ICMP出错消息抑制, ICMP消息引用, ICMP出错消息回射完整性, TOS, 重叠分片处理, TCP选项**
- **nmap -O选项, qeuso, Xprobe**



# Nmap进行操作系统探测示例

```
[root@icstMySQL ~]# nmap -O 192.168.68.253
```

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2008-10-10 16:05 CST
```

```
Interesting ports on 192.168.68.253:
```

```
(The 1664 ports scanned but not shown below are in state: closed)
```

PORT	STATE	SERVICE
------	-------	---------

21/tcp	open	ftp
--------	------	-----

22/tcp	open	ssh
--------	------	-----

80/tcp	open	http
--------	------	------

111/tcp	open	rpcbind
---------	------	---------

992/tcp	open	telnets
---------	------	---------

2008/tcp	open	conf
----------	------	------

3306/tcp	open	mysql
----------	------	-------

3389/tcp	filtered	ms-term-serv
----------	----------	--------------

```
MAC Address: 00:90:0B:04:F8:96 (Lanner Electronics)
```

```
Device type: general purpose
```

```
Running: Linux 2.4.X|2.5.X|2.6.X
```

```
OS details: Linux 2.4.7 - 2.6.11
```

```
Uptime 27.368 days (since Sat Sep 13 07:15:51 2008)
```

```
Nmap finished: 1 IP address (1 host up) scanned in 5.038 seconds
```



# 被动操作系统识别

## □ 被动操作系统识别技术

- 流量监听(开放端口): **tcpdump**, ...
- 被动应用服务识别: **PADS**
- 被动协议栈指纹鉴别: **siphon**, **p0f**

## □ 被动协议栈指纹鉴别

- **Lance Spitzner, Passive fingerprinting**
- 四个常用特征: **TTL, Window Size, DF, TOS**
- **P0f v2: p0f.fp,**
  - ***www:ttt:D:ss:000...:QQ:OS:Details***
  - ***WWS:TTL:DF:Syn pkt size:option,order,...quirks***
  - ***OS genre, OS description***



# P0f进行被动操作系统识别示例

```
root@bt:~# p0f 'src host 172.**.**.188 or dst host 172.**.**.188'
```

p0f - passive os fingerprinting utility, version 2.0.8

(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns <wstearns@pobox.com>

p0f: listening (SYN) on 'eth0', 262 sigs (14 generic, cksum 0F1F5CA2), rule: 'src host 172.\*\*.\*\*.188 or dst host 172.\*\*.\*\*.188'.

172.\*\*.\*\*.188:42228 - **Linux 2.6 (newer, 1)** [high throughput] (up: 349 hrs)

-> 172.\*\*.\*\*.178:80 (distance 0, link: ethernet/modem)

172.\*\*.\*\*.188:45090 - Linux 2.6 (newer, 1) [high throughput] (up: 349 hrs)

-> 172.\*\*.\*\*.178:23 (distance 0, link: ethernet/modem)

172.\*\*.\*\*.178:51659 - Linux 2.6 (newer, 2) [high throughput] (up: 140 hrs)

-> 172.\*\*.\*\*.188:80 (distance 0, link: ethernet/modem)





# 网络服务类型探查

---

## □ 网络服务类型探查

- 确定目标网络中开放端口上绑定的网络应用服务类型 and 版本
- 了解目标系统更丰富信息, 可支持进一步的操作系统辨识和漏洞识别

## □ 网络服务主动探测

- 网络服务旗标抓取和探测: **nmap -sV**

## □ 网络服务被动识别

- 网络服务特征匹配和识别: **PADS**



# Nmap进行网络服务辨识示例

```
root@administrator-desktop:~# nmap -sV 173.***.188
```

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-7-23 00:09 CST
```

```
Interesting ports on localhost (172.***.188):
```

```
Not shown: 998 closed ports
```

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	ProFTPD 1.3.1
22/tcp	open	ssh	OpenSSH 4.7p1Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	Postgresql	PostgreSQL DB
8009/tcp	filtered	ajp13	
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

```
MAC Address:00:50:***.***.***:D1 (VMWare)
```

```
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux
```

```
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 22.68 seconds
```



# PADS进行网络服务被动辨识示例

```
[root@icstMySQL pads-1.2]# pads
pads - Passive Asset Detection System
v1.2 - 06/17/05
Matt Shelton <matt@mattshelton.com>

[-] Filter: (null)
[-] Listening on interface eth0

[*] Asset Found: IP Address - 192.168.68.241 / MAC Address - 0:90:0B:08:5F:3C
(Lanner Electronics)
[*] Asset Found: Port - 3306 / Host - 192.168.68.125 / Service - unknown / App
lication - unknown
[*] Asset Found: Port - 22 / Host - 192.168.68.125 / Service - ssh / Applicati
on - OpenSSH 3.9p1 (Protocol 1.99)
[*] Asset Found: IP Address - 192.168.68.125 / MAC Address - 0:90:0B:04:F8:92
(Lanner Electronics)
[*] Asset Found: IP Address - 192.168.68.243 / MAC Address - 0:90:0B:0A:21:86
(Lanner Electronics)
[*] Asset Found: IP Address - 192.168.68.242 / MAC Address - 0:90:0B:09:7D:34
(Lanner Electronics)
[*] Asset Found: IP Address - 192.168.68.14 / MAC Address - 0:E0:4C:B3:13:5A (
Realtek Semiconductor Corp.)
```



# 系统类型探查防范措施

---

- 并没有太多好办法
- 检测
  - 端口扫描监测工具
  - 对被动式静默监听并辨识系统类型行为则基本无能为力
- 挫败系统类型探查活动的防御机制也很难
- “不出声就不会被发现”这一古老格言并不适用于网络攻防领域
- 应立足于
  - 即使攻击者探查出了操作系统和网络服务类型，也不能轻易的攻破这道“坚固的防线”



# 什么是漏洞扫描？

---

## □ 漏洞

- **Security Vulnerability**，安全脆弱性
- 一般认为，漏洞是指硬件、软件或策略上存在的的安全缺陷，从而使得攻击者能够在未授权的情况下访问、控制系统。

## □ 漏洞扫描

- 检查系统是否存在已公布安全漏洞，从而易于遭受网络攻击的技术。
-



# 漏洞的不可避免

---

## □ 系统设计缺陷

- **Internet**从设计时就缺乏安全的总体架构和设计
- **TCP/IP**中的三阶段握手

## □ 软件源代码的急剧膨胀

- **Windows 95 1500**万行 **Windows 98 1800**万行
- **Windows XP 3500**万行 **Windows Vista 5000**万行
- **Linux** 内核**200**万行

## □ 软件实现的缺陷

- 微软开发人员的单体测试缺陷从超过**25**个缺陷/千行代码显著降低到**7**个缺陷/千行代码
-



# 漏洞扫描

## □ 漏洞扫描技术

- 检查系统是否存在已公布安全漏洞，从而易于遭受网络攻击的技术。
- 双刃剑
  - 网络管理员用来检查系统安全性，渗透测试团队(**Red Team**)用于安全评估。
  - 攻击者用来列出最可能成功的攻击方法，提高攻击效率。

## □ 已发布安全漏洞数据库

- 业界标准漏洞命名库**CVE** <http://cve.mitre.org>
- 微软安全漏洞公告**MSxx-xxx**  
<http://www.microsoft.com/china/technet/security/current.msp>
- **SecurityFocus BID**  
<http://www.securityfocus.com/bid>
- **National Vulnerability Database: NVD**  
<http://nvd.nist.gov/>



# 漏洞扫描软件

---

## □ ISS (Internet Security Scanner)

- 1993年: 第一个漏洞扫描软件, 商业化(Chris Klaus)
- 2006年被IBM以13亿美元收购

## □ SATAN/SAINT

- 1995年: Dan Farmer
- 第一个公开发布的漏洞扫描软件, 引发媒体负面报导

## □ Nessus\*

- 目前最优秀的共享漏洞扫描软件
- 1998-: Renaud Deraison, Nessus v2.x 开源
- 2005-: Tenable Network Security, Nessus v3.x, v4.x, freeware, plugin license





# Nessus

---

## □ 客户端/服务器模式

- 服务器端: **nessesd (Tcp 1241)**
- 客户端: **nessus -q** (命令行客户端), **nessus**(UNIX图形客户端), **Nessus Client**(Win32客户端)

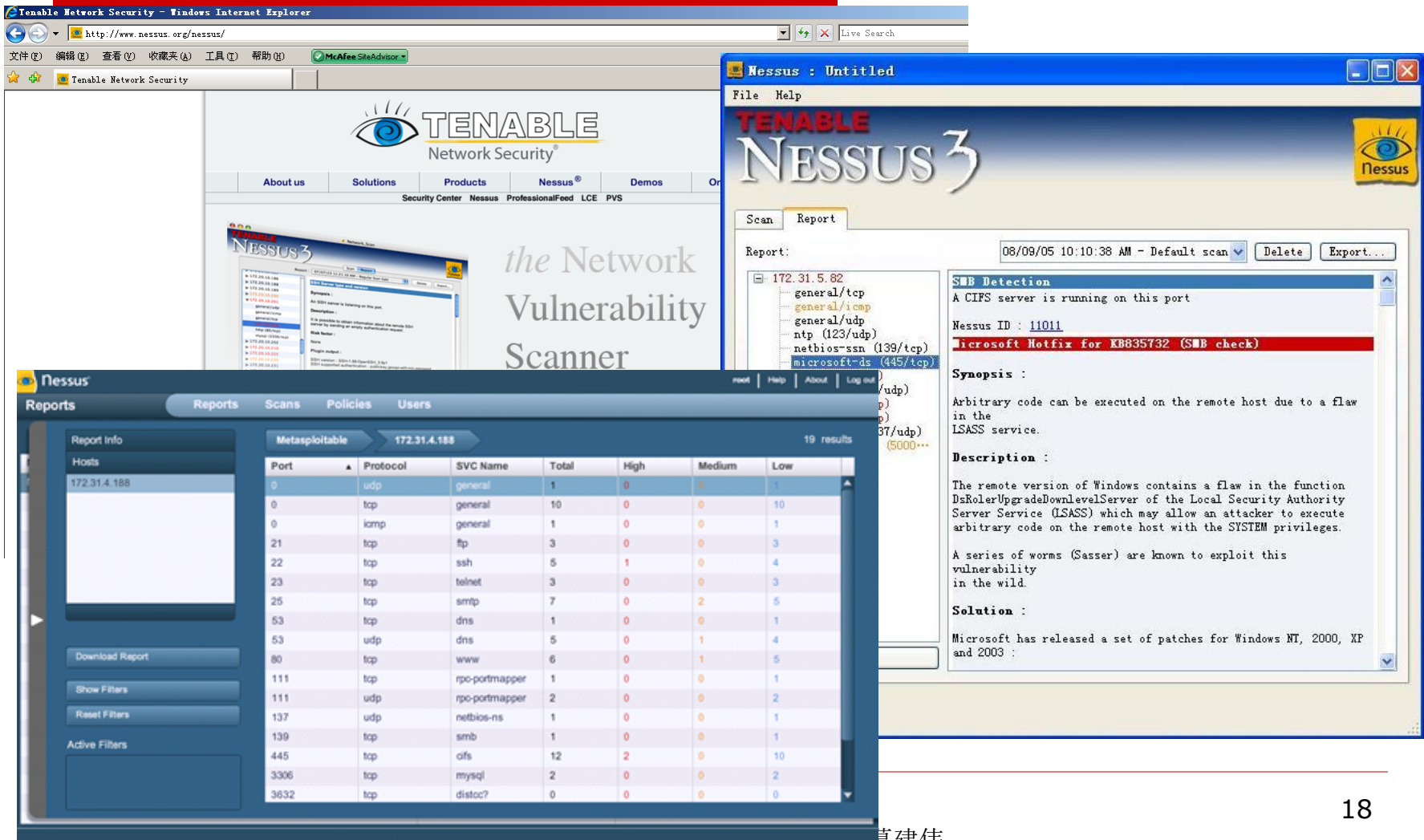
## □ 框架/插件模式

- **NASL语言(Nessus Attack Scripting Language)**
- 安全漏洞扫描插件: 使用**NASL**语言容易编写并集成至**Nessus**框架中
- 插件间可互相依赖和协同工作(端口探测—漏洞扫描插件)

## □ 多种报告方式:

- 文本/**LaTeX/HTML/DHTML/XML/SQL**等

# Nessus



**Tenable Network Security - Windows Internet Explorer**

http://www.nessus.org/nessus/

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H) McAfee SiteAdvisor

Tenable Network Security

**TENABLE Network Security®**

About us Solutions Products **Nessus®** Demos Or

Security Center Nessus ProfessionalFeed LCE PVS

**NESSUS 3**

the Network Vulnerability Scanner

**Nessus : Untitled**

File Help

**TENABLE NESSUS 3**

Scan Report

Report: 08/09/05 10:10:38 AM - Default scan Delete Export...

172.31.5.82

- general/tcp
- general/icmp
- general/udp
- ntp (123/udp)
- netbios-ssn (139/tcp)
- microsoft-ds (445/tcp)

**SMB Detection**

A CIFS server is running on this port

Nessus ID : 11011

**Microsoft Hotfix for KB835732 (SMB check)**

**Synopsis :**

Arbitrary code can be executed on the remote host due to a flaw in the LSASS service.

**Description :**

The remote version of Windows contains a flaw in the function DsRolerUpgradeDownlevelServer of the Local Security Authority Server Service (LSASS) which may allow an attacker to execute arbitrary code on the remote host with the SYSTEM privileges.

A series of worms (Sasser) are known to exploit this vulnerability in the wild.

**Solution :**

Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 :

**Reports** Reports Scans Policies Users

Report Info

Hosts

172.31.4.188

Download Report

Show Filters

Reset Filters

Active Filters

**Metasploitable 172.31.4.188** 19 results

Port	Protocol	SVC Name	Total	High	Medium	Low
0	udp	general	1	0	0	1
0	tcp	general	10	0	0	10
0	icmp	general	1	0	0	1
21	tcp	ftp	3	0	0	3
22	tcp	ssh	5	1	0	4
23	tcp	telnet	3	0	0	3
25	tcp	smtp	7	0	2	5
53	tcp	dns	1	0	0	1
53	udp	dns	5	0	1	4
80	tcp	www	6	0	1	5
111	tcp	rpc-portmapper	1	0	0	1
111	udp	rpc-portmapper	2	0	0	2
137	udp	netbios-ns	1	0	0	1
139	tcp	smb	1	0	0	1
445	tcp	cifs	12	2	0	10
3306	tcp	mysql	2	0	0	2
3632	tcp	distcc?	0	0	0	0

# Nessus使用演示

---



# 国内的商业漏洞扫描软件

---

## □ 开源软件

- **Xscan\***: “冰河” 黄鑫**2001**年开始开发
  - **2005年v3.3**之后无更新
  - 兼容**Nessus**的**NASL**语言开发插件

## □ 国内厂商

- 绿盟: “极光”
- 启明星辰: “天镜”
- ...



# XScan

**X-Scan Report - Microsoft Internet Explorer**

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

地址(地址栏): D:\TOOLS\X-Scan-v3.3\log\172\_31\_5\_82\_report

主机	检测结果
172.31.5.82	发现安全漏洞

主机摘要 - OS: Windows XP; PORT/TCP: 21, 80, 110, 135, 139, 445, 3128, 5000, 8080  
[返回顶部]

**主机分析: 172.31.5.82**

主机地址	端口/服务	服务漏洞
172.31.5.82	netbios-ssn (139/tcp)	发现安全警告
172.31.5.82	pop3 (110/tcp)	发现安全提示
172.31.5.82	http (80/tcp)	发现安全提示
172.31.5.82	ftp (21/tcp)	发现安全提示
172.31.5.82	HTTP proxy server (8080/tcp)	发现安全提示
172.31.5.82	HTTP proxy (3128/tcp)	发现安全提示
172.31.5.82	microsoft-ds (445/tcp)	发现安全漏洞
172.31.5.82	epmap (135/tcp)	发现安全漏洞
172.31.5.82	netbios-ns (137/udp)	发现安全提示
172.31.5.82	DCE/1ff70682-0a51-30e8-076d-740be8cee98b (1026/tcp)	发现安全提示
172.31.5.82	unknown (1028/udp)	发现安全提示
172.31.5.82	DCE/378e52b0-c0a9-11cf-822d-00aa0051e40f (1026/tcp)	发现安全提示

**X-Scan v3.3 GUI**

文件(F) 设置(S) 查看(V) 工具(T) Language 帮助(H)

172.31.5.82 (Windows)

- 开放服务
  - 139/tcp
  - 110/tcp
  - 80/tcp
  - 21/tcp
  - 8080/tcp
  - 3128/tcp
  - 445/tcp
  - 135/tcp
- NetBios信息
  - 服务器信息
  - 服务器时间
  - 网络共享资源列
- 漏洞检测脚本
  - 445/tcp
  - 135/tcp
  - 139/tcp
  - 137/udp
  - 1026/tcp
  - 1028/udp
  - 5000/tcp

主机	累计时间	插件时间	活动线程	当前进度
----	------	------	------	------

普通信息 漏洞信息 错误信息

[172.31.5.82]: 135/tcp - DCE Services Enumeration  
[172.31.5.82]: 1026/tcp - DCE Services Enumeration  
[172.31.5.82]: 1028/udp - DCE Services Enumeration  
[172.31.5.82]: 445/tcp - SMB 登陆  
[172.31.5.82]: 135/tcp - DCE Services Enumeration  
[172.31.5.82]: 445/tcp - SMB 登陆  
[172.31.5.82]: 1026/tcp - DCE Services Enumeration  
[172.31.5.82]: 1028/udp - DCE Services Enumeration  
[172.31.5.82]: 445/tcp - 可以通过SMB连接注册表  
[172.31.5.82]: 135/tcp - DCE Services Enumeration  
[172.31.5.82]: 445/tcp - ASN.1 Parsing Vulnerabilities (NTLM check)  
[172.31.5.82]: 445/tcp - 可以通过SMB连接注册表  
[172.31.5.82]: 1026/tcp - DCE Services Enumeration  
[172.31.5.82]: 445/tcp - ASN.1 Parsing Vulnerabilities (NTLM check)

扫描全部完成 Active thread: 0

08-2009 诸葛建伟



# 漏洞扫描防范措施

## □ 最简单对策:

- 假设黑客会使用漏洞扫描来发现目标网络弱点，那你必须在黑客之前扫描漏洞
- 补丁自动更新和分发：修补漏洞

## □ 联邦桌面核心配置计划(**FDCC**)

- 确保桌面计算机的安全漏洞及补丁自动管理
- 中国**2010**年才开始政务终端安全配置(**CGDCC**)标准的发展

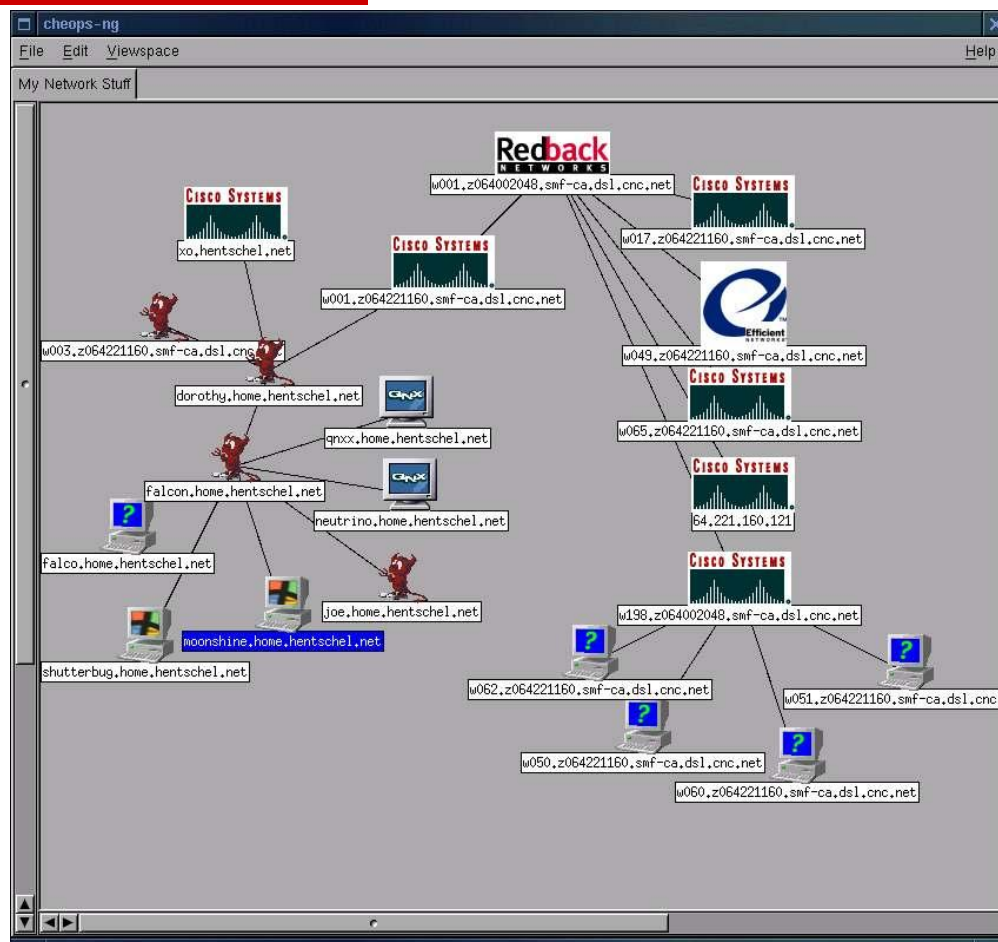
## □ 检测和防御漏洞扫描行为

- 网络入侵检测系统: **Snort**
- 仔细审查防火墙配置规则



# 完整解决方案-自动化侦察工具

- 自动化侦察工具
  - HP OpenView
  - Cheops
  - Cheops-ng
  - tkined





# 内容

---

- 1. 网络扫描技术**
- 2. 课堂实践：nmap扫描**
- 3. 网络查点技术**
- 4. 作业3—搜索自己的互联网足迹/网络扫描实验**





# 课堂实践：Nmap扫描

---

- 任务：使用**Nmap**开源软件对**Win32**靶机环境进行扫描，回答如下问题并给出操作命令：
  - 靶机**IP**地址是否活跃？
  - 靶机开放了那些**TCP**和**UDP**端口？
  - 靶机安装了什么操作系统？版本是多少？
  - 靶机上安装了哪些网络服务？



# 内容

---

- 1. 网络扫描技术**
- 2. 课堂实践：nmap扫描**
- 3. 网络查点技术**
- 4. 作业3—搜索自己的互联网足迹/网络扫描实验**



# 网络查点(enumeration)

## □ 网络查点技术

- 继网络踩点、扫描之后一项网络情报信息收集技术
- 网络查点：针对已知的弱点，对识别出来的服务进行**更加充分更具针对性的探查**，来寻找真正可以攻击的入口，以及攻击过程中可能需要的关键数据

## □ 与网络踩点、扫描的区别

- 与网络踩点技术的关键区别：攻击者的入侵程度
- 与网络扫描技术的关键区别：攻击者的针对性与信息收集的目标性



# 网络查点能够收集到的信息

---

- 看起来好像是无害的
  - 用户帐户名
  - 错误配置的共享资源
  - 网络服务版本号
- 但一旦这些信息被细心的高水平攻击者所掌握，就可能成为危害目标系统安全的祸根
  - 用户帐户名：口令猜测破解
  - 错误配置的共享资源：恶意程序上传
  - 老旧的网络服务版本：缓冲区溢出漏洞攻击



# 网络查点技术

---

- 最基础和通用的技术方法
  - 网络服务旗标(**banner**)抓取技术
- 常见服务网络查点技术
  - 通用网络服务
  - 类**Unix**平台网络服务
  - **Windows**平台网络服务



# 网络服务旗标攫取

- 利用客户端工具连接至远程网络服务并观察输出以收集关键信息的技术手段

- telnet

- netcat

- 实例

```
C:\>telnet www.baidu.com 80
```

```
HTTP/1.0 400 Bad Request
```

```
Content-Type: text/html; charset=UTF-8
```

```
Content-Length: 1350
```

```
Date: Thu, 05 Aug 2010 07:45:37 GMT
```

```
Server: GFE/2.0
```

```
<html><head>
```

```
    <meta                                http-equiv="content-type"  
content="text/html; charset=utf-8">
```

```
    <title>400 Bad Request</title>
```

```
...
```

```
</body></html>
```

```
Connection to host lost.
```



# 网络服务旗标攫取(2)

**E:\>nc -v www.google.com 80**

DNS fwd/rev mismatch: www-g-com-chn.l.google.com != hx-in-f104.1e100.net

DNS fwd/rev mismatch: www-g-com-chn.l.google.com != hx-in-f99.1e100.net

www-g-com-chn.l.google.com [74.125.71.104] 80 (http) open

**HEAD / HTTP/1.0**

HTTP/1.0 302 Found

Location: http://www.google.com.hk/url?sa=p&cki=PREF%3DID%3D2db251cd0e0e6d39:FF%

3D2:LD%3Dzh-CN:NW%3D1:TM%3D1280999902:LM%3D1280999902:S%3DfcwL07mJercsHMe8&q=htt

p://www.google.com.hk/&ust=1280999932693535&usg=AFQjCNExaNSNZE1kstPRavYn9EgfaYv1Dw

Cache-Control: private

Content-Type: text/html; charset=UTF-8

Set-Cookie: PREF=ID=2db251cd0e0e6d39:NW=1:TM=1280999902:LM=1280999902:S=t6YYGpuP

Ltobu-fx; expires=Sat, 04-Aug-2012 09:18:22 GMT; path=/; domain=.google.com

Set-Cookie: NID=37=gBkc8fT-y0BosuAXWM9kAJs8xnf6Gdw8WSa8Z\_-3IzuXIV7cbp-cwYHMmuLg2

u3GgFM6BOvdqW-TiWJ-u0jmX-H1qm80yNn\_xJzUV94nRTIKg06JfBRwkBb-oigMAHQE; expires=Fri

, 04-Feb-2011 09:18:22 GMT; path=/; domain=.google.com; HttpOnly

Date: Thu, 05 Aug 2010 09:18:22 GMT

**Server: gws**

Content-Length: 445

X-XSS-Protection: 1; mode=block



# 通用网络服务查点

---

## □ 通用网络服务

- 跨平台，常用服务
- **Web**服务、**FTP**文件传输服务、**POP3**及**SMTP**电子邮件收发服务

## □ **FTP**服务查点

- 控制协议**TCP 21**端口，没有任何加密，明文传输口令
- 匿名登录，甚至匿名上传与下载文件
- **FTP**查点很简单：使用**FTP**客户端程序连接即可
- **FTP**服务旗标、共享目录、可写目录等信息，可能还会提供**FTP**帐户名等信息
- 查点后攻击：弱口令猜测与破解、已知**FTP**服务漏洞渗透攻击





# 通用网络服务查点(2)

## □ SMTP电子邮件发送协议查点

- 最经典的网络服务查点技术之一
- 两类特殊指令**VRFY**和**EXPN**
- **VRFY**指令：对合法用户的名字进行验证
- **EXPN**指令：显示假名与邮件表实际发送地址
- 可验证和搜索邮件服务器上的活跃帐户

## □ SMTP电子邮件发送协议查点危害

- 伪造更具欺骗性电子邮件，社会工程学攻击
- 探测**SMTP**服务器枚举出其中有效的电子邮件地址列表，大量发生垃圾邮件



# 类Unix平台网络服务查点

---

- 古老的**finger, rwho, rusers**查点
  - 用户帐户和登录信息
  - 已不常用
- **RPC查点(TCP/UDP 111, 32771)**
  - **RPC远程过程调用: portmapper → rpcbind**
  - **RPC查点工具**
    - **rpcinfo -p HOST**: 枚举主机上提供的**RPC**服务
    - **rpcdump(Windows平台运行)**
    - **nmap -sS -sR HOST**
  - **RPC查点防御策略**
    - **Secure RPC, 111/32771**端口防火墙过滤



# 类Unix平台 RPC查点

```
[root@icstMySQL ~]# rpcinfo -p 192.168.68.125
    program vers proto  port
    100000    2    tcp    111  portmapper
    100000    2    udp    111  portmapper
    100024    1    udp    32768 status
    100024    1    tcp    32769 status
    100011    1    udp    646  rquotad
    100011    2    udp    646  rquotad
    100011    1    tcp    649  rquotad
    100011    2    tcp    649  rquotad
    100003    2    udp    2049 nfs
    100003    3    udp    2049 nfs
```

```
[root@icstMySQL ~]# nmap -ss -sR 192.168.68.125
starting Nmap 4.76 ( http://nmap.org ) at 2008-11-11 13:44 CST
Interesting ports on 192.168.68.125:
Not shown: 989 closed ports
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh
80/tcp    open  http
111/tcp    open  rpcbind (rpcbind v2)    2 (rpc #100000)
199/tcp    open  smux
2049/tcp   open  nfs (nfs v2-4)          2-4 (rpc #100003)
3306/tcp   open  mysql
5801/tcp   open  vnc-http-1
5901/tcp   open  vnc-1
6001/tcp   open  X11:1
32769/tcp  open  status (status v1)      1 (rpc #100024)
32770/tcp  open  nlockmgr (nlockmgr v1-4) 1-4 (rpc #100021)

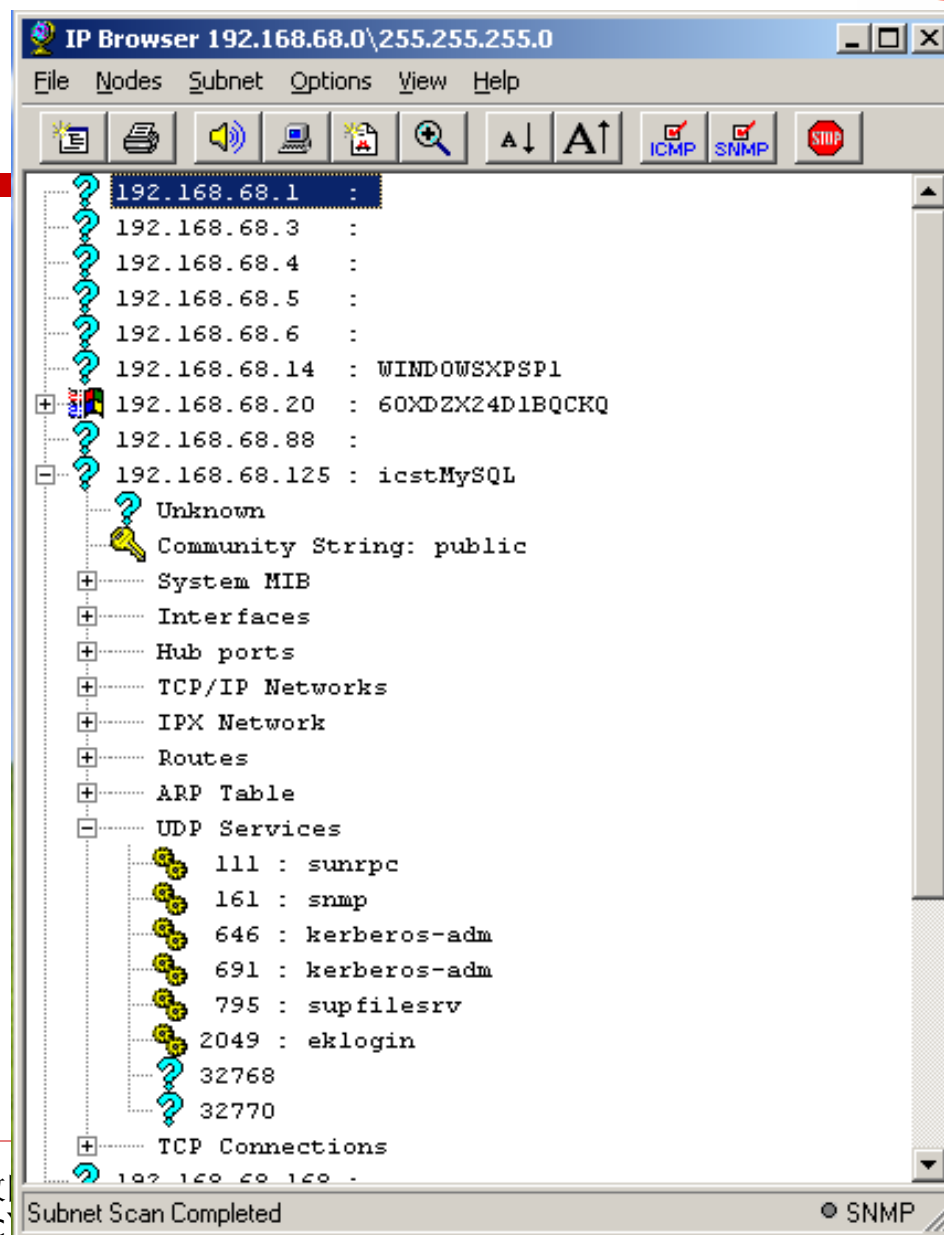
Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
```



# SNMP查点

## □ SNMP

- 简单网络管理协议  
**UDP 161**
- “Security Not My Problem”安全不管我的事
- **snmpwalk**  
**xxx.xxx.xxx.xxx**  
**public**
- **IP Network Browser**





# Windows平台网络服务查点

---

## □ Windows网络服务

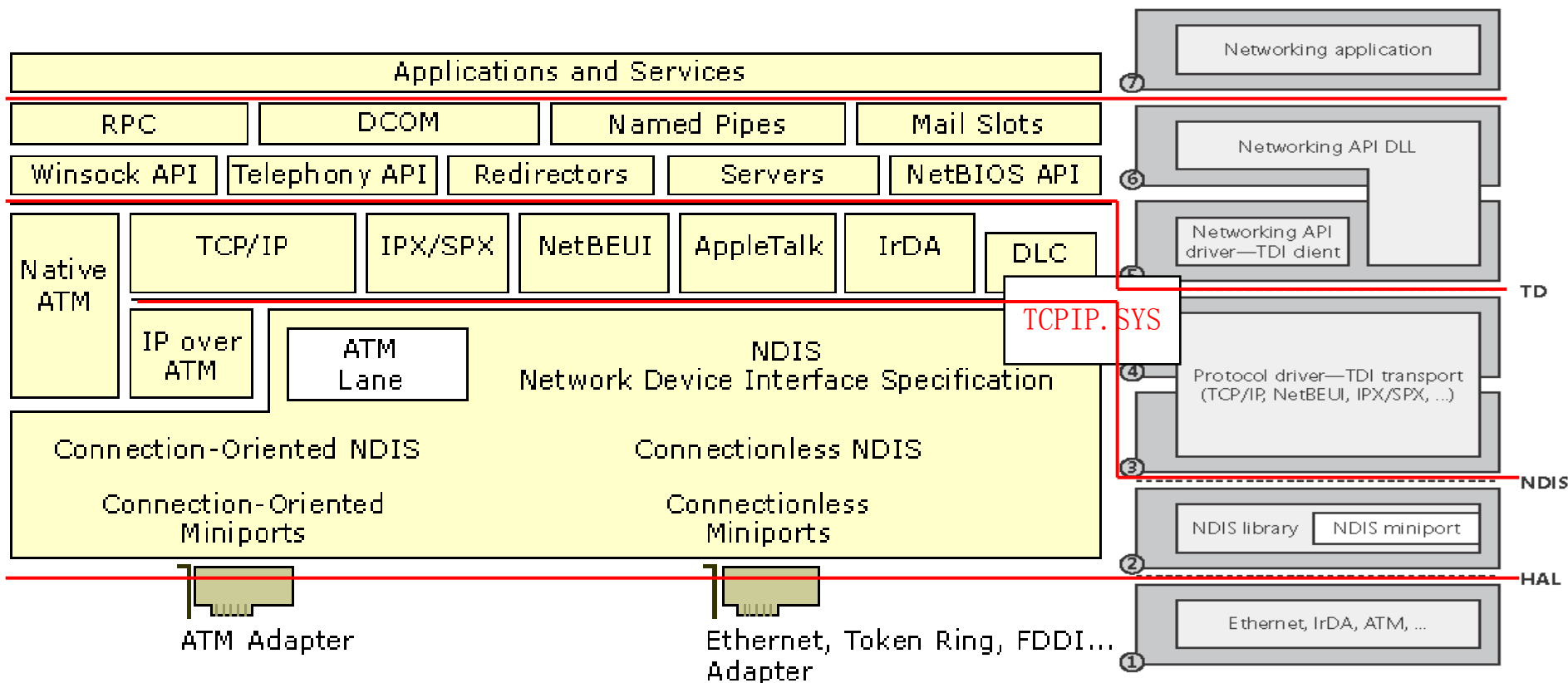
- **NetBIOS**网络基本输入输出系统服务
- **SMB**文件与打印共享服务
- **AD**活动目录与**LDAP**轻量级目录访问协议
- **MSRPC**微软远过程调用服务

## □ Windows平台网络服务查点

- **NetBIOS**主机查点
- **SMB**会话查点
- 目录查点
- **MSRPC**查点



# Windows NT5.x中的网络结构





# Windows Networking API

---

- **NetBIOS**—网络基本输入/输出系统
  - **Windows**独有的局域网组网协议
- **RPC** – 远过程调用
  - **PRC/DCOM**
- **WinSock API**
- **命名管道(Named Pipes)和邮件槽(Mail Slots)**
  - 命名管道：提供可靠双向通信，协议无关的标识**Windows**网络资源的方法
  - 邮件槽：提供不可靠的单向数据传输，支持广播
- **Web访问API**
  - **WinInet/WinHTTP/HTTP API**



# NetBIOS

- **NetBIOS(网络基本输入/输出系统)**: 最初由**IBM**开发, **MS**利用**NetBIOS**作为构建局域网的上层协议
- **NetBIOS**使得程序和网络之间有了标准的接口, 方便应用程序的开发。并且可以移植到其他的网络中
- **NetBIOS**位于**OSI**模型会话层, **TCP/IP**之上
- **NetBIOS**有两种通讯模式
  - 会话模式。一对一进行通讯, **LAN**中的机器之间建立会话, 可以传输较多的信息, 并且可以检查传输错误
  - 数据报模式。可以进行广播或者一对多的通讯, 传输数据大小受限制, 没有错误检查机制, 也不必建立通讯会话
- **NetBIOS over TCP/IP**, 支持三种服务
  - 名字服务 **UDP 137**
  - 会话服务 **TCP 139/445**
  - 数据报服务 **UDP 138**



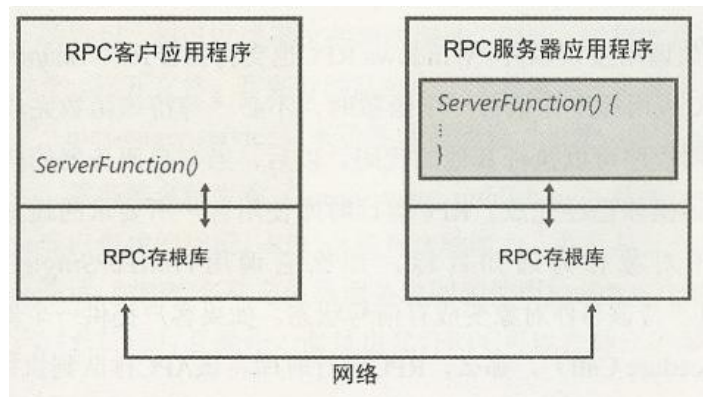
# MSRPC远程进程调用 / DCOM

## □ RPC (Remote Procedure Call)

- 网络编程标准
- 目的: 提供“能在某种程度上像应用程序开发人员隐藏有关网络编程细节”的编程模型

## □ RPC调用

- 允许程序员编写的客户应用程序跨网络调用远程计算机上服务器应用程序中的过程



## □ COM/DCOM

- **COM对象**: 使应用程序由不同组件构成, 导出面向对象接口, 提高软件模块化、可扩展性和可交互性。
- **DCOM**: 提供**COM**组件的位置透明性, 依赖于**RPC**
- **Know More**: 潘爱民著《**COM**组件技术》, 《组件技术讲义》



# 常用的**Windows**应用层网络服务

---

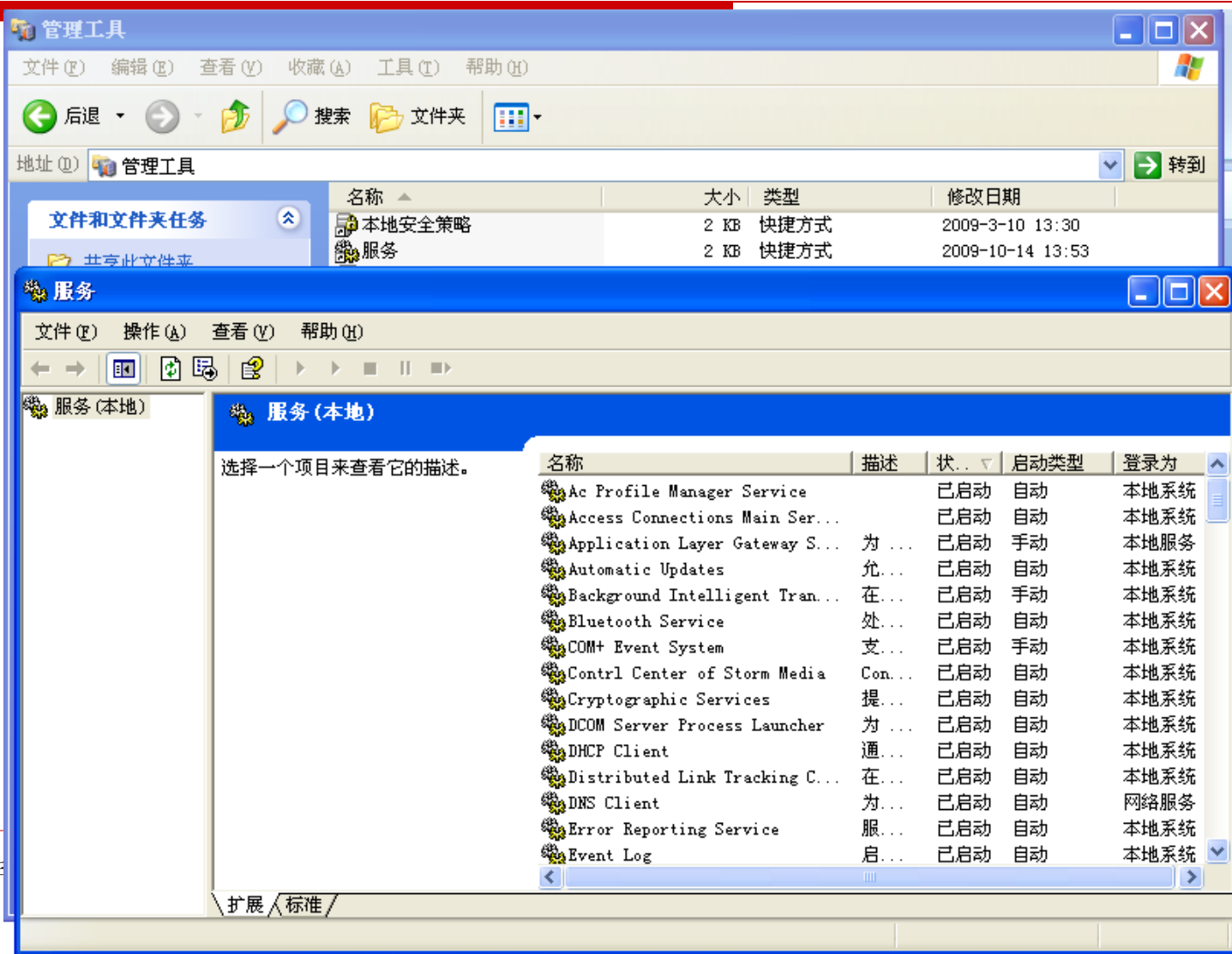
- ☐ **Network Applications**
- ☐ **IIS (Internet Information Services)**
  - HTTP/FTP/...
- ☐ **Email**
  - Exchange Server
- ☐ **Database**
  - MS SQL Server
- ☐ **RDP**
  - Remote Desktop Protocol
- ☐ 通常以**Windows**服务方式后台运行



# Windows服务

- **Windows**服务—系统启动时刻启动进程的机制，提供不依赖于任何交互式的服务。
- **Windows**服务
  - 服务应用程序
    - 注册服务**Advapi32.dll, CreateService/StartServices**
    - 注册表: **HKLM\SYSTEM\CurrentControlSet\Services**
    - 共享服务进程: 服务宿主**svchost.exe**
  - 服务控制管理器(**SCM, service control manager, services.exe**)
    - **Winlogon**进程在加载**GINA**之前执行**SCM**启动函数
    - **SCM**中的**ScCreateServiceDB**根据注册表分别启动服务
    - **SCM**中的**ScAutoStartServices**启动“自动启动”的服务
  - 服务控制程序(**SCP, service control program**)
    - 控制面板, 服务插件...

# Windows服务控制面板





# NetBIOS网络查点- 使用net view命令查点域

## □ 使用net view查点域

- 列出网络上的工作组和域: **net view /domain**

```
E:\>net view /domain
```

```
Domain
```

```
I***DOM
```

```
MSHOME
```

```
WORKGROUP
```

```
The command completed successfully.
```

- 列出指定组/域中的所有计算机: **net view /domain:DOMAIN\_NAME**

```
E:\>net view /domain:I***DOM
```

```
Server Name
```

```
Remark
```

```
\\I***SVR
```

```
i***svr
```

```
.....
```

```
The command completed successfully.
```



# NetBIOS网络查点- 查点域控制器

## □ Windows Resource Kit - nltest工具

```
C:\Program Files\Support Tools>net view /domain
```

```
Domain
```

```
-----  
HAPPY
```

```
HOLD
```

```
I***-V-***LEI
```

```
I***OM
```

```
MSHOME
```

```
WORKGROUP
```

```
The command completed successfully
```

```
C:\Program Files\Support Tools>nltest /dclist:I***OM
```

```
Get list of DCs in domain 'I*****OM' from '\\I***DC1'.
```

```
    i***dc1.i*****om.i***.pku.edu.cn [PDC] [DS] Site: Default-First-Site-Name
```

```
    i***dc01.i*****om.i***.pku.edu.cn    [DS] Site: Default-First-Site-Name
```

```
The command completed successfully
```



# NetBIOS网络查点- 查点主机上的NetBIOS名字表

## □ nbtstat工具

- 主机中的**NetBIOS**名字表
- 计算机名、所在域、当前登录用户、当前运行服务和网卡硬件**MAC**地址

```
E:\>nbtstat -A 172.17.175
```

本地连接:

Node IpAddress: [172.17.175] Scope Id: []

NetBIOS Remote Machine Name Table

Name	Type	Status
------	------	--------

ICST-XSP0EN	<00> UNIQUE	Registered
ICST-XSP0EN	<20> UNIQUE	Registered
MSHOME	<00> GROUP	Registered
MSHOME	<1E> GROUP	Registered
MSHOME	<1D> UNIQUE	Registered
.._MSBROWSE_.	<01> GROUP	Registered

MAC Address = 00-50-00-00-00-A3



# NetBIOS网络查点- 扫描主机上的NetBIOS名字表

## □ nbtscan工具

### ■ 对整个局域网进行快速的nbtstat查询

```
E:\Support>nbtscan.exe 172.***.0-255
```

```
Doing NBT name scan for addresses from 172.***.0-255
```

IP address	NetBIOS Name	Server	User	MAC address
------------	--------------	--------	------	-------------

172.***.2	ECRIS-VCENTER	<server>	<unknown>	00-**-0b-04-**-b3
-----------	---------------	----------	-----------	-------------------

172.***.3	Recvfrom failed: Connection reset by peer			
-----------	-------------------------------------------	--	--	--

172.***.4	Recvfrom failed: Connection reset by peer			
-----------	-------------------------------------------	--	--	--

172.***.9	Recvfrom failed: Connection reset by peer			
-----------	-------------------------------------------	--	--	--

172.***.31	Recvfrom failed: Connection reset by peer			
------------	-------------------------------------------	--	--	--

172.***.174	Recvfrom failed: Connection reset by peer			
-------------	-------------------------------------------	--	--	--

172.***.176	Recvfrom failed: Connection reset by peer			
-------------	-------------------------------------------	--	--	--

172.***.177	Recvfrom failed: Connection reset by peer			
-------------	-------------------------------------------	--	--	--

172.***.178	Recvfrom failed: Connection reset by peer			
-------------	-------------------------------------------	--	--	--

172.***.184	Recvfrom failed: Connection reset by peer			
-------------	-------------------------------------------	--	--	--

172.***.188	METASPLOITABLE	<server>	METASPLOITABLE	00-00-00-00-00-00
-------------	----------------	----------	----------------	-------------------





# NetBIOS网络查点工具与防范措施

---

## □ 其他工具

- **epdump, rpcdump, getmac, netdom, netviewx, Wininfo, nbt dump, ...**

## □ NetBIOS查点防范措施

- **网络：防火墙禁止外部访问TCP/UDP 135-139，445端口**
- **主机：配置IPSec过滤器，主机个人防火墙，禁用Alerter和Messenger服务**



# SMB会话服务

---

- **SMB(Server Message Block)服务**
  - 微软的文件与打印共享服务
  - **SMB over NetBIOS: 基于NetBIOS会话服务 TCP 139**
  - **SMB over TCP/IP: Direct Host, TCP 445**
- **Windows在处理默认共享等方面的缺省配置不安全**
  - 远程主机通过**API**访问**SMB**可以获取相关**Windows**系统非常丰富的信息



# SMB会话查点过程

---

- 第一步：匿名用户“空会话”(null session), 建立起了一条开放的会话信道
  - 空口令字("")
  - 内建的匿名用户(/u: "")
  - “进程间通信”隐蔽共享卷(IPC\$)
- 以未认证匿名用户进行各种会话查点
  - 网络信息查点
  - 共享情况查点
  - 用户、组查点
  - 注册表键值查点



# 建立“空会话”

```
C:\>net use \\172.*.*.175\IPC$ "" /u:""
```

The command completed successfully.

```
C:\>net view \\172.*.*.175
```

Shared resources at \\172.\*.\*.175

Share name	Type	Used as	Comment
------------	------	---------	---------

shared	Disk		
--------	------	--	--

SharedDocs	Disk		
------------	------	--	--

The command completed successfully.



# SMB会话查点

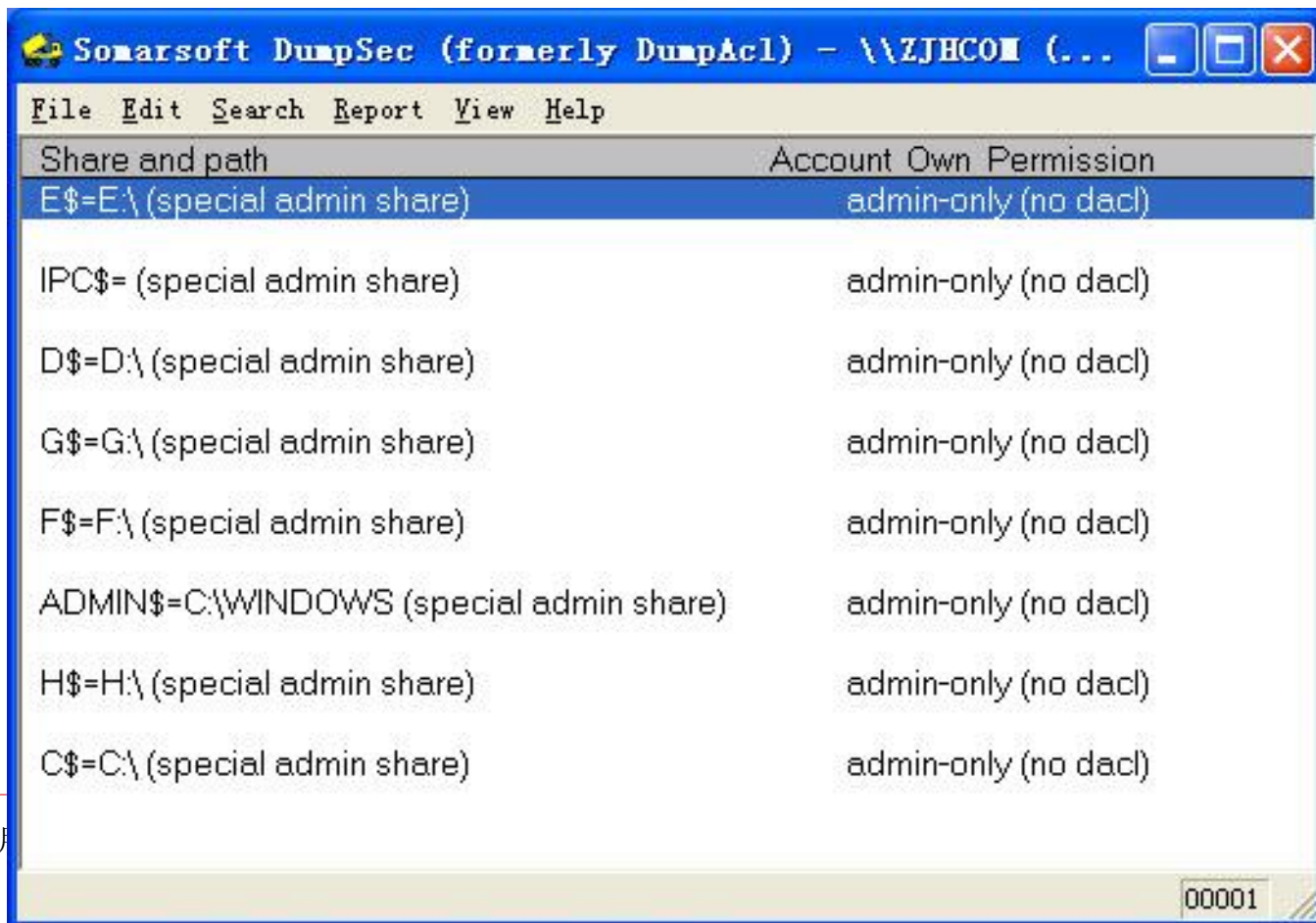
## -查点主机共享资源

---

- 权限配置错误的**Windows**文件共享卷
  - 包含敏感信息的共享目录(甚至是盘符共享)
  - 所有用户可读写的共享目录
- 内建命令
  - **net view \\HOST**
- 其他工具
  - **NTRK**资源包中的**rmtshare, srvcheck, srvinfo**
  - **DumpSec**

# 共享目录查点示例

## □ Dumpsec工具



Somarsoft DumpSec (formerly DumpAcl) - \\ZJHCOM (...)

Share and path	Account Own Permission
E\$=E:\ (special admin share)	admin-only (no dacl)
IPC\$= (special admin share)	admin-only (no dacl)
D\$=D:\ (special admin share)	admin-only (no dacl)
G\$=G:\ (special admin share)	admin-only (no dacl)
F\$=F:\ (special admin share)	admin-only (no dacl)
ADMIN\$=C:\WINDOWS (special admin share)	admin-only (no dacl)
H\$=H:\ (special admin share)	admin-only (no dacl)
C\$=C:\ (special admin share)	admin-only (no dacl)

00001



# SMB会话查点

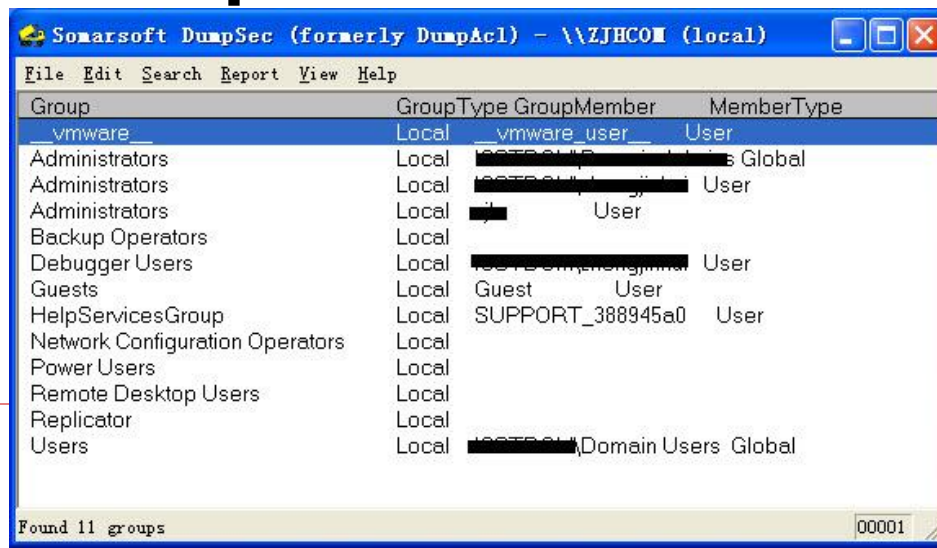
## -注册表查点

- 注册表查点工具
  - Windows Resource Kit中的regdmp工具
  - DumpSec的“Dump Services”功能
- Windows的默认配置
  - 只允许管理员访问注册表
  - 例外：HKLM\System\CurrentControlSet\Control\SecurePipeServer\Winreg\AllowedPaths键中指定了可以通过空会话访问的注册表键值
  - HKLM\Software\Microsoft\Windows NT\Current Version: 当前运行环境配置，如自启动项等

# SMB会话查点

## —信任域与用户查点

- 使用 **nltest** 查点受信任域
  - **nltest /server: SERVER\_NAME**
  - **nltest /trusted\_domain**
- 查询主机用户信息
  - **NTRK资源包: usrstat, showgrps, local, global**
  - 强大工具 **DumpSec**: 能够列出用户、组及权限 **GUI**







# 活动目录查点

---

- 活动目录(**Active Directory**)
  - 基于轻量级目录访问协议(**LDAP**)-**TCP/UDP: 389**
  - 活动目录全局编录端口**3268**
- 利用**LDAP**客户端进行活动目录查点
  - **Ldp**
  - 早期**Nt 4.x**仅用**guest**帐户可查询所有用户和组对象
- 活动目录查点防御对策
  - 网络边界限制对**TCP 389**和**3268**端口的访问
  - 从**Pre-Windows 2000 Compatible Access**组中删除**Everyone**组



# MSRPC查点

---

## □ MSRPC服务查点

### ■ MSRPC服务：远程过程调用服务端口映射器 TCP 135

□ 查询该服务获得目标主机上可用的应用程序和服务相关信息

### ■ Reskit工具包epdump工具

□ epdump HOST: 应用服务绑定IP地址和端口

## □ MSRPC查点防御策略

### ■ 限制非授权用户对TCP 135端口的访问



# 应对Windows查点的CheckList

---

- ❑ 关闭不必要的服务及端口
    - **msconfig/autoruns/**第三方软件
  - ❑ 如果不用网络共享：关闭打印与共享服务(**SMB**)
  - ❑ 不要让主机名暴露使用者身份(计算机名)
  - ❑ 查看共享目录，关闭不必要共享，特别是可写共享和**everyone**共享
    - 计算机管理- 共享文件夹
  - ❑ 关闭默认共享(根盘符**\$**, **Admin\$**)
    - 可能会影响一些依赖默认共享进行管理的应用服务
  - ❑ 限制**IPC\$**默认共享的匿名空连接
-



# 禁止所有不必要的服务

文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)

← → ↶ ↷ ↸ ↹

🔍

📄 📁 📂 📅 📆 📇 📈 📉 📊 📋 📌 📍 📎 📏 📐 📑 📒 📓 📔 📕 📖 📗 📙 📚 📛 📜 📝 📞 📟 📠 📡 📢 📣 📤 📥 📦 📧 📨 📩 📪 📫 📬 📭 📮 📯 📰 📱 📲 📳 📴 📵 📶 📷 📸 📹 📺 📻 📼 📽 📾 📿

计算机管理(本地)

系统工具

事件查看器

共享文件夹

本地用户和组

性能日志和警报

设备管理器

存储

可移动存储

磁盘碎片整理程序

磁盘管理

服务和应用程序

服务

WMI 控件

索引服务

服务

选择一个项目来查看它的描述。

名称	描述	状态	启...	登录为
Windows Management Instrumen...	与...	手动		本地系统
Wired AutoConfig	此...	手动		本地系统
WMI Performance Adapter	从 ...	手动		本地系统
Application Layer Gateway Se...	为 ...	已启动	手动	本地服务
COM+ Event System	支...	已启动	手动	本地系统
Logical Disk Manager	监...	已启动	手动	本地系统
Logical Disk Manager Adminis...	配...	已启动	手动	本地系统
Network Connections	管...	已启动	手动	本地系统
Network Location Awareness (...)	收...	已启动	手动	本地系统
Remote Access Connection Man...	创...	已启动	手动	本地系统
SSDP Discovery Service	启...	已启动	手动	本地服务
Telephony	提...	已启动	手动	本地系统
Terminal Services	允...	已启动	手动	本地系统
Windows Image Acquisition (WIA)	为...	已启动	手动	本地系统
Security Center	监...	手动		本地系统
Alerter	通...	已禁用		本地服务
ClipBook	启...	已禁用		本地系统
Computer Browser	维...	已禁用		本地系统
Human Interface Device Access	启...	已禁用		本地系统
Messenger	传...	已禁用		本地系统
Network DDE	为...	已禁用		本地系统
Network DDE DSDM	管...	已禁用		本地系统
Routing and Remote Access	在...	已禁用		本地系统
Telnet	允...	已禁用		本地系统
Wireless Zero Configuration	为...	自动		本地系统
Cryptographic Services	提...	已启动	自动	本地系统

# 关闭SMB网络文件与打印机共享服务



网络连接

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 高级(N) 帮助(H)

后退 搜索 文件夹

地址(0) 网络连接

**网络任务**

- 创建一个新的连接
- 更改 Windows 防火墙设置

**相关主题**

- 网络疑难解答程序

**其它位置**

- 控制面板
- 网上邻居
- 我的文档
- 我的电脑

**详细信息**

- 网络连接
- 系统文件夹

**LAN 或高速 Internet**

- 本地连接 已连接上, 有防火...  
Broadcom NetXtre...
- 无线网络连接 未连接, 有防火...  
Intel(R) PRO/Wir...
- 1394 连接 已连接上, 有防火...  
1394 网络适配器

**宽带**

- adsl 已连接上, 有防火...  
WAN 微型端口 (PP...

**高级设置**

适配器和绑定 提供程序顺序

连接按被网络服务访问的顺序排列。

连接(C):

- 本地连接
- 无线网络连接
- 1394 连接
- 1394 网络适配器

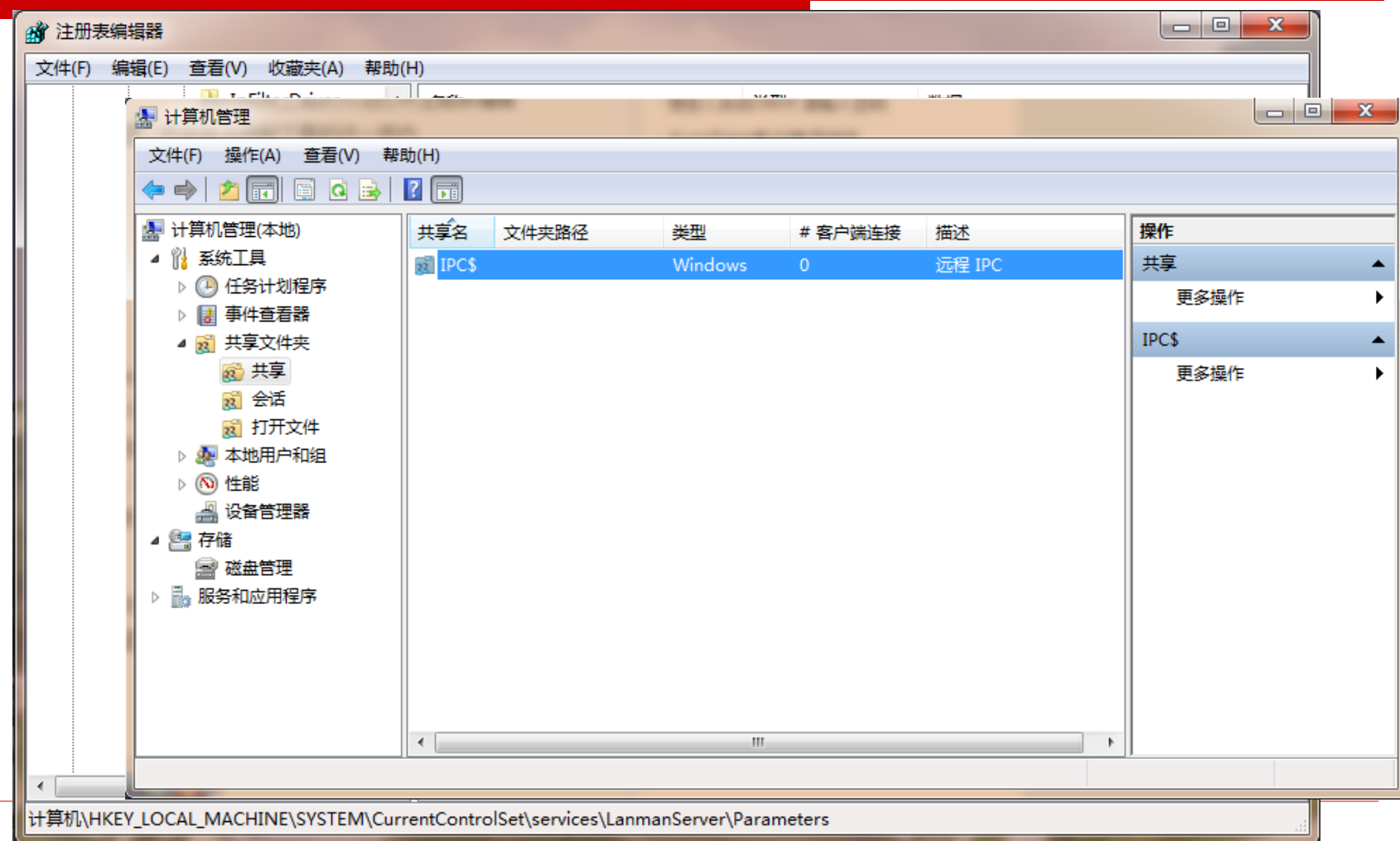
本地连接 的绑定(B):

- ☐ Microsoft 网络的文件和打印机共享
- ☐ Internet 协议 (TCP/IP)
- ☒ Microsoft 网络客户端
- ☒ Internet 协议 (TCP/IP)

确定 取消

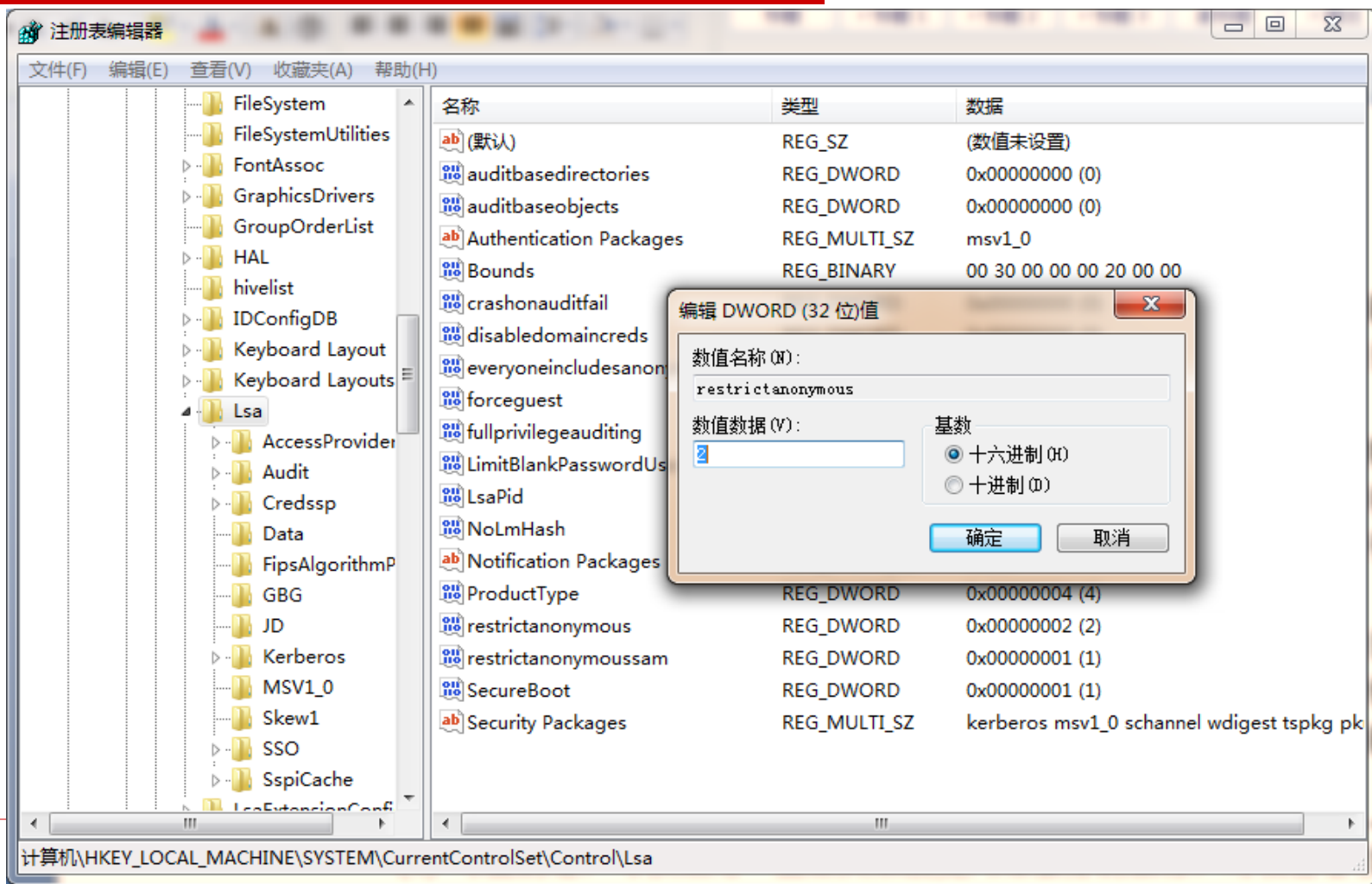


# 关闭盘符默认共享



设置HKLM/System/CurrentControlSet/Services/Lanmanserver/Parameters/AutoShareServer|AutoShareWks = 0

# 禁止SMB匿名空会话



设置HKLM/System/CurrentControlSet/Control/Lsa/restrictanonymous = 2



# 内容

---

1. 网络扫描技术
2. 课堂实践：nmap扫描
3. 网络查点技术
4. 作业3—搜索自己的互联网足迹/网络扫描实验





# 作业3 – 个人作业

- **3.1** 通过搜索引擎搜索自己在因特网上的足迹，并确认是否存在隐私和敏感信息泄露问题，如是，提出解决方法。（注，不要在提交作业中泄漏个人隐私☺）
  - 提示：**Google**你的名字、网名、**email**、电话...
- **3.2** 使用**Nmap**扫描某台靶机，给出并解读靶机环境的配置情况，撰写实验分析报告。
- **3.3** 使用**Nessus**扫描某台靶机，给出并解读靶机环境上网络服务及安全漏洞情况，撰写实验分析报告。
- 提交给助教: **zhanghuilin@icst.pku.edu.cn**
- **Deadline: 10月27日**

# Thanks

---

诸葛建伟

**zhugejianwei@icst.pku.edu.cn**