



NSFocus Information Technology Co. Ltd.

网络安全 黑客常见攻击技术及防御

Strictly Private & Confidential

提纲

- 攻击的一般过程
- 预攻击探测技术
- 口令破解与攻击
- 数据驱动式攻击
- 拒绝服务类攻击
- 欺骗与侦听技术
- 远程控制与后门
- 黑客的社会工程

攻击的一般过程

攻击的一般过程

- 预攻击探测

收集信息,如OS类型,提供的服务端口

- 发现漏洞,采取攻击行为

破解口令文件,或利用缓存溢出漏洞

- 获得攻击目标的控制权

- 继续渗透网络,直至获取机密数据或留下后门

进行权限的提升,寻找网络中其它主机的信息和漏洞

- 消灭踪迹

隐藏和删除所有曾经改动过的地方

攻击的常见手段

- 预攻击探测
- 口令猜测攻击
- 数据驱动攻击(Data Driven Attack)
- 拒绝服务攻击(Dos)
- 欺骗与侦听(Sniffer &Spooof)
- 后门(BackDoor)
- 恶意代码(Malicious)
- 权限提升(Privilege Escalation)

预攻击探测技术

预攻击探测技术

- 也称信息收集型攻击，并不对目标本身造成危害，这类攻击被用来为进一步入侵提供有用的信息。主要步骤包括：
 - 踩点 (footprinting)
 - 扫描 (scanning)
 - 调查 (enumeration)

踩点 (Footprinting)

- 确定攻击目标
- 使用简单的工具，通过各种途径，获取目标与安全相关的信息。主要包括：
 - 领导、技术人员的信息（姓名、电话、邮件、生日等）
 - 域名、IP地址范围；
 - DNS服务器、邮件服务器；拨号服务器；
 - 防火墙、路由器型号等

踩点方法

- 搜索引擎与信息库（常规）
 - www.google.com
 - www.networksolutions.com
 - www.cnnic.net
 - www.checkdomain.com
 - Whois数据库
- 具有强大功能的搜索引擎
 - www.netcraft.com
 - www.samspade.org

踩点方法

- 常用命令
 - Nslookup
 - Traceroute
 - Whois

扫描 (Scanning)

- 探测攻击途径
 - 扫描是攻击的前奏，是Internet上普遍存在的现象；
 - 在黑客攻击工具中，扫描器占的比重最大；
- 扫描收集的信息
 - 确定活动主机（Ping Sweep技术）；
 - 确定开放的端口与服务（Port Scan技术）；
 - 系统指纹识别（OS Identification / Fingerprinting技术）；

确定活动主机

- Ping Sweep
 - 需要在较短的时间中，在较大的网络范围内确定“活”的机器；
 - 主要利用的原理
 - ICMP sweeps (ICMP ECHO requests)
 - Broadcast ICMP
 - Non-ECHO ICMP
 - TCP Sweep/UDP Sweep

确定开放端口

- Port Scan
 - 端口扫描就是连接到目标系统的TCP或UDP端口上，确定那些服务正在运行。
- 主要目的：
 - 确定目标系统上的TCP和UDP服务；
 - 标识目标系统的OS类型；
 - 标识特定的应用程序或特定服务的版本。

端口扫描工具

- SuperScan;
- Fscan
- NmapNT
- NetScanTools Pro
- NetCat
- WinScan
- WUPS
- （各种扫描工具）

系统指纹识别

- Banner 识别;
 - FTP、telnet、SMTP、HTTP、POP3等
- 端口判别;
 - Windows(135, 139, 445, 3389, 6531, 1433)
 - Sun(32773 Sun RPC)
 - Redhat (98, 119)
- 协议栈指纹鉴别;
 - TTL、Ping、TraceRoute等

TELNET

```
c:\>telnet 192.168.0.241
Trying 192.168.0.241...
正在连接到192.168.0.241...
Escape character is '^]'.

SUN OS 5.6 (ttyp2)

login:
```

```
c:\>telnet 192.168.0.162
Microsoft (R) Windows 2000 (TM)
版本 5.00 (内部版本号 2195)

欢迎使用 Microsoft Telnet Client

Telnet Client 内部版本号
5.00.99203.1

Escape 字符为 'CTRL+]'
```

FTP

```
c:\>ftp 192.168.0.241
```

```
Connected to 192.168.0.162...
```

```
220 .goodwel FTP server (Version wu-2.4.2-VR17(1) Mon Apr ...ready
```

```
c:\>ftp 192.168.0.162
```

```
Connected to 192.168.0.162.
```

```
220 lost-my-self Microsoft FTP Service (Version 5.0).
```

```
User (192.168.0.162:(none)):
```

Ping

```
C:\>ping 192.168.0.162

Pinging 192.168.0.162 with 32 bytes of data:

Reply from 192.168.0.162: bytes=32 time<10ms TTL=128

Reply from 192.168.0.162: bytes=32 time<10ms TTL=128

C:\>ping 192.168.1.241

Pinging 192.168.1.241 with 32 bytes of data:

Reply from 192.168.1.241: bytes=32 time<10ms TTL=255

Reply from 192.168.1.241: bytes=32 time<10ms TTL=255
```

TraceRoute

- 一种诊断工具，用于察看一个IP分组从一台主机流动到另一台主机的路径。工作原理为：
 - Traceroute首批发送的探测分组TTL值为1，以后逐批增加1，直到探测到目的系统为止；
 - 途径上的路由器将TTL减1，把TTL减为0的路由器将丢弃探测分组，并回送ICMP超时信息；
 - 最后一跳到达目标主机，目的主机将回送ICMP
 - *destination unreachable (UDP探测)*
 - *ICMP Echo replay (ICMP echo request探测)*

指纹识别防范

- 去掉或修改各种Banner (OS&Service) ;
- 关闭不需要的端口或使用假端口;
- 利用评估软件进行自身的安全评估;
- 安装最新的补丁程序;
- 安装入侵检测软件;
- 边界路由器合理配置屏蔽攻击探测:
 - 只允许ICMP echo reply; host unreachable; time exceeded从外部进入内网。

- 重要的网络命令；
 - Ipconfig、Netstat 、 Net user、Nslookup、Tracert



- 网络资源与共享资源
 - Showmount -e ip
 - Net use ,net view,net share
- 用户和用户组
 - Finger、 rusers、 rwho
 - nbtstat

Net share (NT)

```
C:\>net share
```

共享名	资源	注释
-----	----	----

IPC\$		远程 IPC
D\$	D:\	默认共享
print\$	C:\WINNT\System32\spool\drivers	打印机驱动程序
C\$	C:\	默认共享
ADMIN\$	C:\WINNT	远程管理
E\$	E:\	默认共享
gwshare	C:\gwshare	
HPLaserJ	LPT1:	后台处理 HP LaserJet 6L

命令成功完成。

Nbtstat (NT)

```
C:\>nbtstat -a 192.168.0.163
```

```
本地连接:
```

```
Node IpAddress: [192.168.0.162] Scope Id: []
```

```
NetBIOS Remote Machine Name Table
```

Name	Type	Status
WORKSTATION <00>	UNIQUE	Registered
WORKSTATION <20>	UNIQUE	Registered
WORKGROUP <00>	GROUP	Registered
WORKGROUP <1E>	GROUP	Registered
WORKSTATION <03>	UNIQUE	Registered
ADMINISTRATOR <03>	UNIQUE	Registered
WORKGROUP <1D>	UNIQUE	Registered
.._MSBROWSE_ <01>	GROUP	Registered
INet~Services <1C>	GROUP	Registered
IS^WORKSTATION.<00>	UNIQUE	Registered

```
MAC Address = 00-80-C8-F6-3E-53
```

Null Session

- 预备知识
 - NetBios数据传输协议(135-139)
 - CIFS/SMB(SMB Over NetBios)
 - IPC\$(Inter-Process Communication)共享是Windows NT/2000系统上的一个标准的隐含共享，它是用于服务器之间的通信的
 - TCP 445(SMB Over TCP/IP)



Null Session

- Null Session（空连接）连接也称为匿名登陆，这种机制允许匿名用户通过网络获得系统的信息或建立未授权的连接。它常被诸如explorer.exe 的应用来列举远程服务器上的共享。
- 非授权主机可以是网络里所有的主机，即这个主机不需要有访问服务器的任何权限。
- 任何一台主机都可以和服务器之间建立一个NULL session，这个NULL session在服务器里属于everyone组。缺省情况下所有的用户都属于everyone这个组。everyone组没有很大的权力。但是可以利用它获取系统的用户信息。

Null Session

- `net use \\server\IPC$ "" /user:""`
 - 此命令用来建立一个空会话
 - 获得目标上的所有用户列表。包括服务器上有哪些组和用户。
 - 服务器的安全规则，包括帐户封锁、最小口令长度、口令使用周期、口令唯一性设置等。
 - 列出共享目录。
 - 读注册表。

Null Session

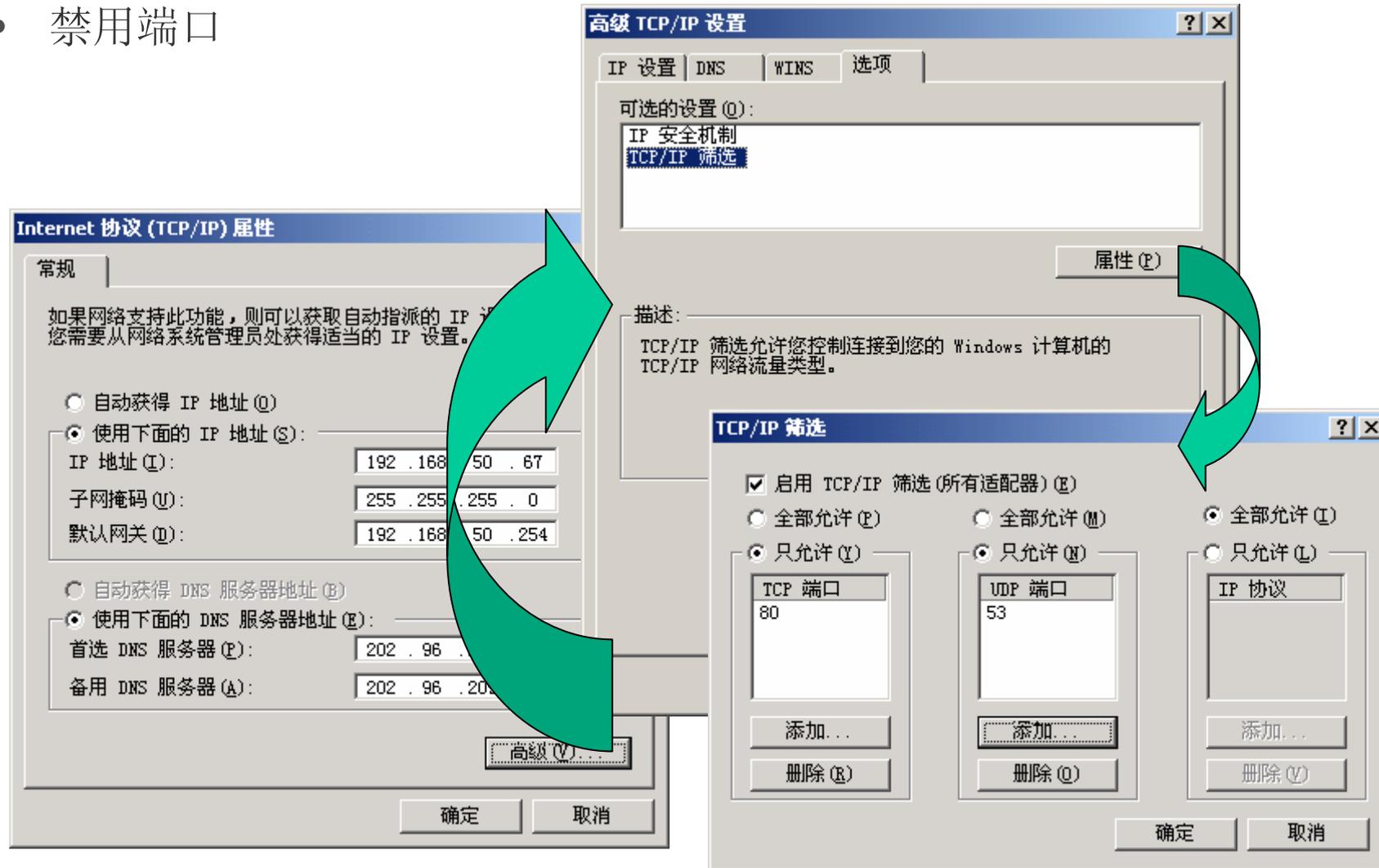
- `net view \\server`
 - 此命令用来查看远程服务器的共享资源
- `net time \\server`
 - 此命令用来得到一个远程服务器的当前时间。
- `At \\server`
 - 此命令用来得到一个远程服务器的调度作业

简单防御办法

- 屏蔽135-139, 445端口 (网络属性)
- 去除NetBios Over TCP/IP (在服务中去除server)
- 修改注册表
 - HKEY-LOCAL_MACHINE\SYSTEM\CurrentControSet\Control\LSA
 - Value Name: RestrictAnonymous
 - Data Type: REG_DWORD
 - Value: 1 (2 Win2000)
 - 参考KB articles Q143474, Q143475, Q161372, Q155363, Q246261

简单防御办法

- 禁用端口



Windows 共享保护方法

- NT/2000共享设置：
 - 设置共享专用目录并设置合理的访问权限；
 - 禁用空连接；
 - 取消默认共享：

禁止默认共享（增加）regedt32

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Name AutoShareServer

Type REG_DWORD

Value 0

参考**Q143474**、**Q246261**

口令破解攻击

口令问题

- 多数的系统，口令是进入系统的第一道防线，也是唯一防线；
- 决大多数的口令算法是可靠的；
- 获得口令的方式有多种；
- 口令问题多数出在管理与安全意识的问题上。

口令问题1：弱口令

- 用户趋向于选择容易的口令，即空口令；
- 用户会选择易于记住的东西做口令
 - Test、Password、guest、username等
 - 名字、生日、简单数字等
- 易于选择该系统的应用
 - Ntserver、orancle等
- 多数用户的安全意识薄弱

口令问题2：明文传输

- 使用明文密码传送的应用：
 - FTP、POP、Telnet、HTTP、SNMP、Socks
 - Mountd、Rlogin、NNTP、NFS、
 - ICQ、IRC、PcAnywhere、VNC等
 - MS SQL、Oracle等
- 上述服务都容易成为攻击对象

口令攻击的方式

- 手工猜测；
 - 方法：社会工程学、尝试默认口令
- 自动猜测；
 - 工具：NAT、LC等
- 窃听：登陆、网络截获、键盘监听
 - 工具：Dsniff、Sniffer Pro、IKS等

Windows常见的口令问题

- NT/2000的口令问题;
- 用户教育的问题;
- 管理员注意事项。

NT/2000的口令问题

- SAM (Security Accounts Manager)
 - LanManager散列算法 (LM)
 - 已被破解，但仍被保留
 - NT散列算法 (NTLM/NTLMv2)
 - 强加密、改良的身份认证和安全的会话机制
 - 自动降级
 - SYSKEY

NT/2000的口令问题

- SAM数据存放位置
 - %systemroot%\system32\config\sam
 - %systemroot%\repair\sam._(NT)Rdisk
 - %systemroot%\repair\sam (2000) ntbackup
 - 注册表HKEY_LOCAL_MACHINE\SAM\SAM 和
HKEY_LOCAL_MACHINE\SECURITY\SAM仅对system是可读写的

NT/2000的口令问题

- 获取SAM数据的方法
 - 使系统自举到另外的系统，copy SAM文件；
 - 从repair目录攫取备份的SAM；
 - 窃听口令交换

著名解密工具LC3



- L0phtcrack
- Crack v5
- John the Ripper

The screenshot shows the LC3 software interface. The main window displays a list of users and their corresponding passwords, LM passwords, and LM hashes. An "Auditing Options For This Session" dialog box is open, showing settings for Dictionary Crack, Dictionary/Brute Hybrid Crack, and Brute Force Crack.

User Name	LM Password	<B	NILM Password	LM Hash	NILM P
blankity	" empty "	x	" empty "	AAD3B435B51404EEAAD3B435B51404EE	31D6CF
boone.speed	EVILLYROUTED		evillyrouted	DB8C09462C4F6638E9672191318F6176	93FAD8
chris.sharma	MANIDALA		manidala	C9842ECC9AEE5DF27584248B8D2C9F9E	A18A76
dave.graham	SPECTER*		specter*	8D11726F08BB65A890004151ADA7B438	ED6051
dgoddard	_100%SERVICE		_100%service	84D9C453653F55AFA0FCB3F05FF7D4C5	9E2AB7
Guest	AUTHORITARIAN		AuthoRitarian	3A6A936A22348450BB4039FED87A09AE	384E30
jarry.moffat	PAPPYONSIGHT		pappyonsight	CF91ABBB4F88A1CB7BCA039B8EC202F	8969CF
klem.loscot	V14@BREAKFAST		v14@breakfast	37E3692864E489F3CBFEE74A5E12FB49	77E13D
lynn.hill	NOSEYD				
mike.beck	LINUS				
mike.call	SLIDESH				
patrick.edlinger	CHRYSA				
scott.franklin	SCARF-A				
yuji.hirajama	CRACKER				
_ablaze23	ABLAZE2				
_animosity1 /	ANIMUSI				
_cat0!	CAT0!				
_cat47	CAT47				
_zoology	ZOOLOG				

Auditing Options For This Session

Dictionary Crack

Enabled

Word file: C:\Program Files\@stake\LC3\words- [Browse...]

The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords.

Dictionary/Brute Hybrid Crack

Enabled

2 Characters to vary (more is slower)

The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in the word file. It finds passwords such as "Dana99" or "monkeys!". This test is fast and finds weak passwords.

Brute Force Crack

Enabled

Character Set: A-Z, 0-9 and !@#%&'&*()_+=""{}|~:;<>.,?/

Distributed

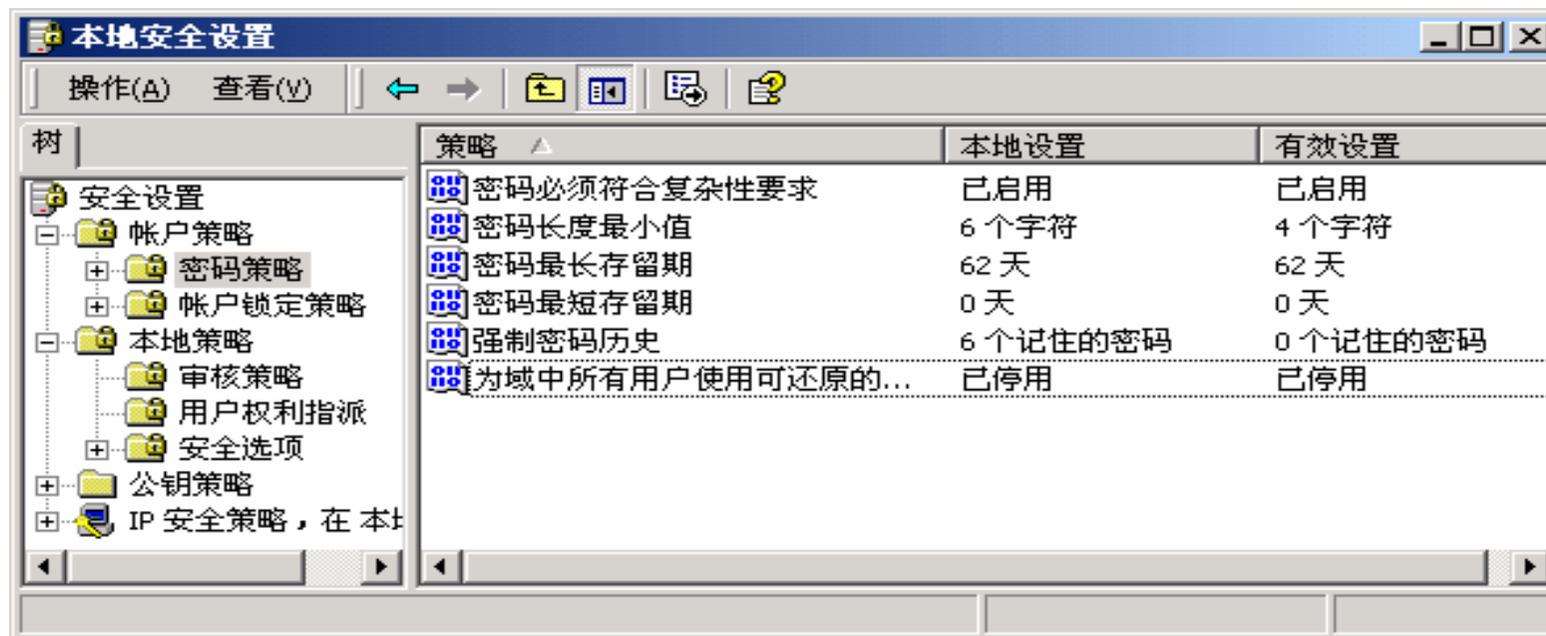
Part 2 Of 5

Custom Character Set (list each character):

The Brute Force Crack tests for passwords that are made up of the characters specified in the Character Set. It finds passwords such as "WeR3plT6s" or "vC5%69+12b". This test is slow and finds medium to strong passwords. Specify a character set with more characters to crack stronger passwords.

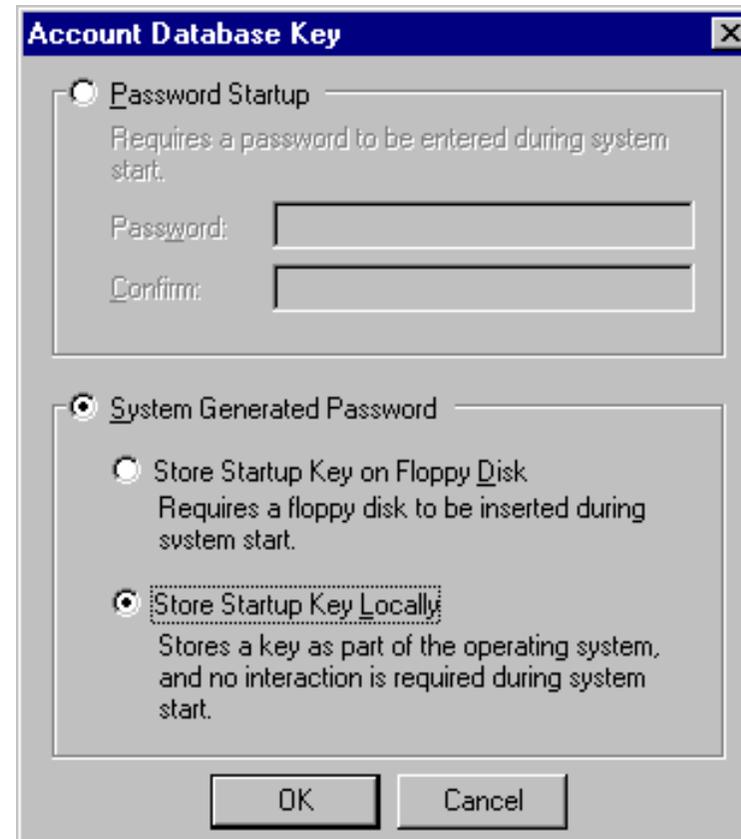
OK Cancel

- 使用密码强度及账户老化、锁定策略；
 - 设置最小的密码长度为8个字符，最短密码时间为1-7天，最长密码时间为42天，最小的密码历史轮回为6，失败登陆尝试为3，账户锁定为60分钟等。



口令加密建议

- 使用SYSKEY加密口令文件;



- 口令禁忌：
 - 不要选择可以在任何字典或语言中找到的口令
 - 不要选择简单字母组成的口令
 - 不要选择任何指明个人信息的口令
 - 不要选择包含用户名或相似类容的口令
 - 不要选择短于6个字符或仅包含字母或数字的口令
 - 不要选择作为口令范例公布的口令



- 好的口令
 - 选择至少6个字符长度的口令
 - 选择一个包含非字母字符的口令，包括数字或特殊字符
 - 选择一个容易记住而不必写下来的口令
 - 选一个不看键盘而迅速键入的口令，使偷看的人不能识别



- 如果非得写下口令时
 - 在折叠的纸条上写下口令并放在保险柜或安全的地方
 - 写在总放在钱包中的某些东西
 - 不把用户名和口令记在一起
 - 以能记住的方式把它改动，增加额外字符或改换顺序
 - 不要把口令贴到任何计算机的硬件上面



管理员注意事项

- 确保每个用户都有一个有效的口令；
- 对用户进行口令教育；
- 使用防止用户选择弱口令的配置与工具；
- 进行口令检查，确保没有弱口令；
- 确保系统与网络设备没有缺省账号和口令；
- 不要在多个机器上使用相同的口令；
- 从不记录也不与他人共享密码；

管理员注意事项

- 从不将网络登录密码用作其他用途；
- 域Administrators账户和 本地Administrators帐户使用不同的密码；
- 小心地保护在计算机上保存密码的地方；
- 对于特权用户强制30天更换一次口令，一般用户60天更换；
- 使用VPN、SSH、一次性口令等安全机制。

数据驱动式攻击

准备知识

- 特权程序
 - 特权程序是指执行时具有系统权限的程序。它的存在是为了让普通用户执行某些需要系统权限的任务。
- 服务进程
 - 为本机和网络提供服务。如邮件服务器、WWW服务器

- SUID程序

Unix中的SUID (Set User ID) 程序是指程序属性设置了SUID位的程序。这种程序在执行时具有文件属主的权限。

如passwd程序它的文件属性为：

```
-r-s--x--x  1 root  root    10704 Apr 15  1999 /usr/bin/passwd
```

^SUID程序

passwd程序执行时就具有root权限。

- 为什么要有SUID程序？

SUID程序是为了使普通用户完成一些普通用户权限不能完成的事而设置的。比如每个用户都允许修改自己的密码，但是修改密码文件又需要管理员权限。所以修改密码的程序需要以管理员权限运行。

数据驱动攻击

- 通过对某个活动中的服务发送数据，导致非“预期”的结果。
- 原因：
 - 边界情况；
 - 缓冲区溢出；
 - 意外组合；
 - 竞争情况

什么是Buffer Overflow?

- 又叫Stack Overflow。
- 1988年Robert Morris蠕虫事件
- 1996年, Phrack Magazine杂志发表“Smashing The Stack For Fun And Profit”对安全界产生深远影响
- 超过50%的攻击事件源于BO问题

缓冲区溢出

- 缓冲区(buffer): 用于临时存储数据的一段内存区域
- 溢出(overflow): 数据过长导致无法存储在预期区域内
- 边界检查(Boundary Check): 在向缓冲区中存储数据时, 确定数据长度是否会超出缓冲区边界

缓冲区溢出 - 术语(2)

- **堆栈(Stack)**: 一段内存区域, 用来临时存储信息, 后进先出。通常用来保存函数调用现场、局部变量。
- **堆(Heap)**: 应用程序动态分配的内存区域
- **BSS区**: 初始数据全为零, 保存未初始化的静态变量
- **函数返回地址**: 函数执行完毕返回时要去执行的下一条指令的地址。

缓冲区溢出 – 术语 (3)

- Shellcode: 通常指攻击者精心构造的一段汇编代码, 在溢出攻击时会诱使程序执行这段代码。

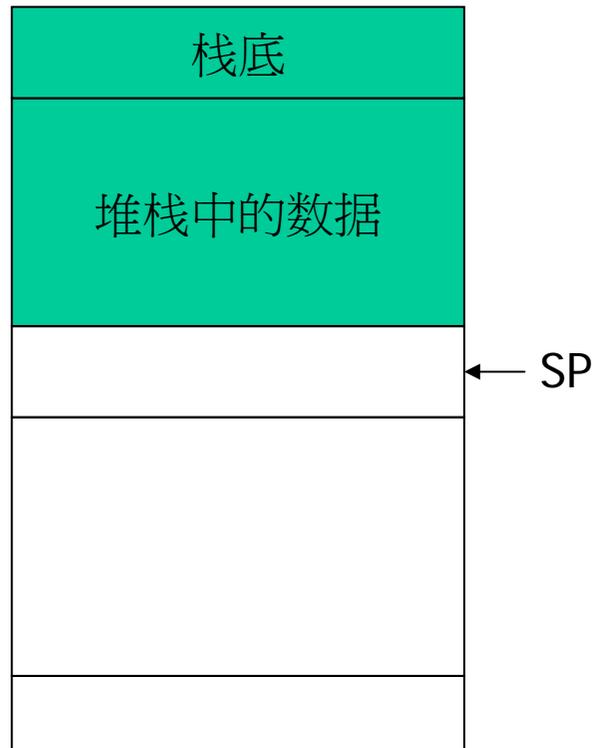
```
char shellcode[] =
```

```
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
```

```
"\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40xcd"
```

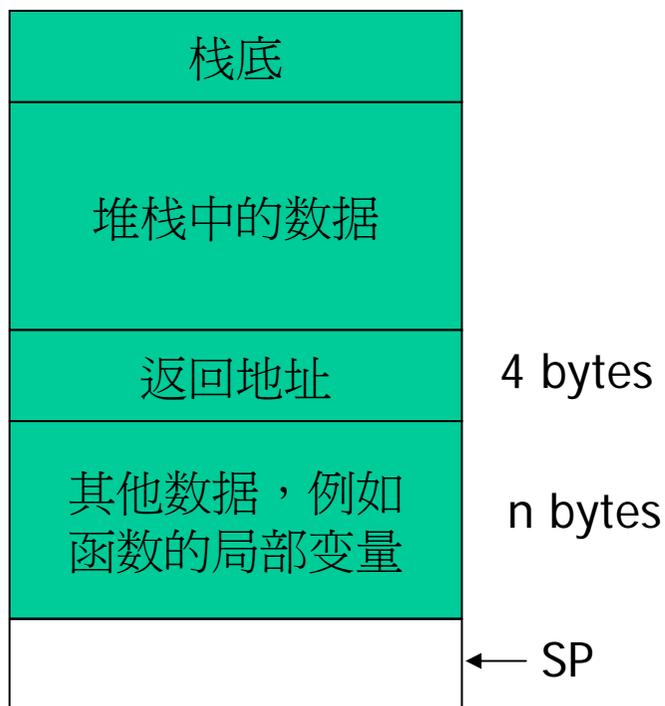
```
"\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

基于堆栈的缓冲区溢出

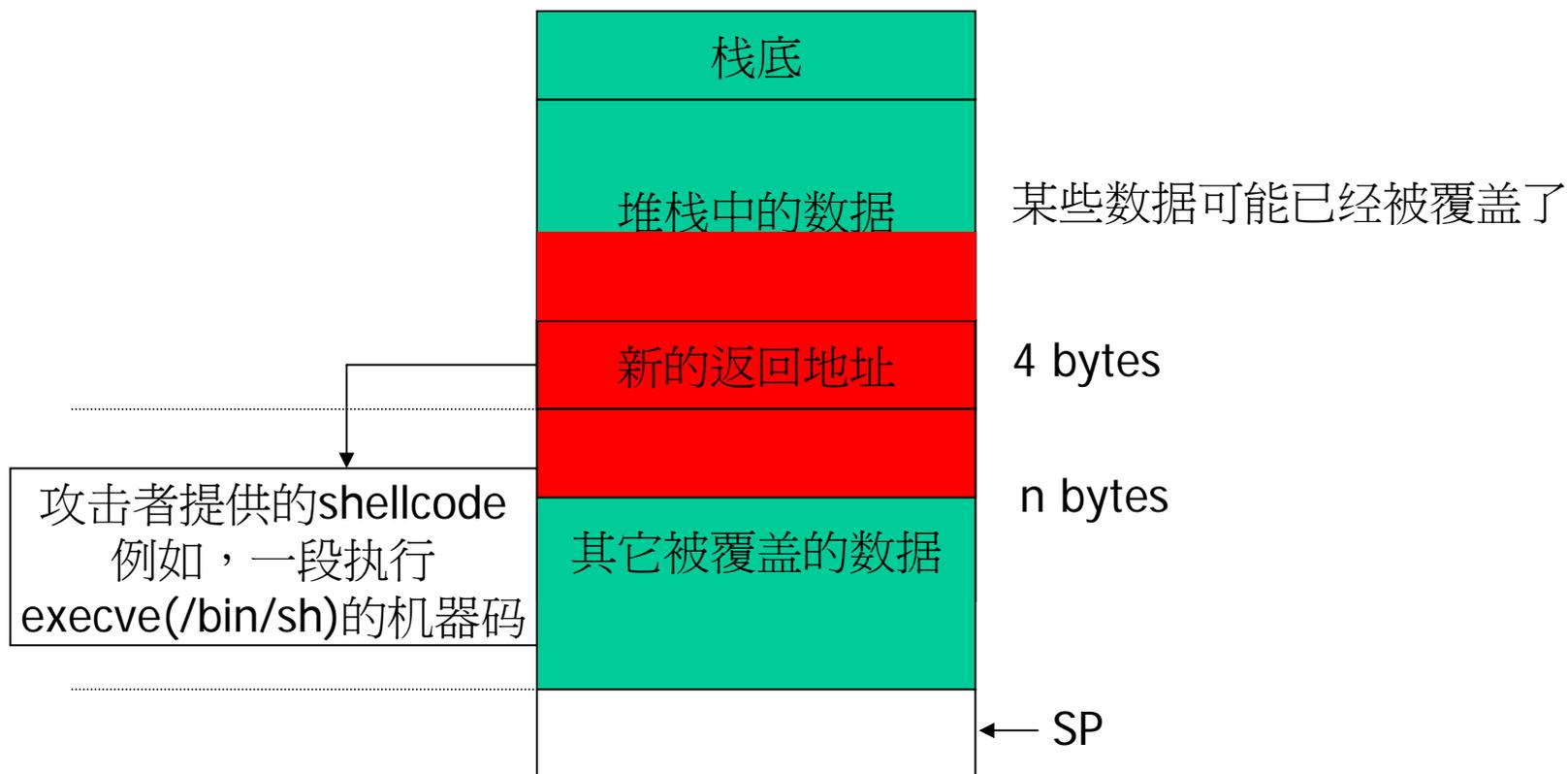


正常的堆栈分布

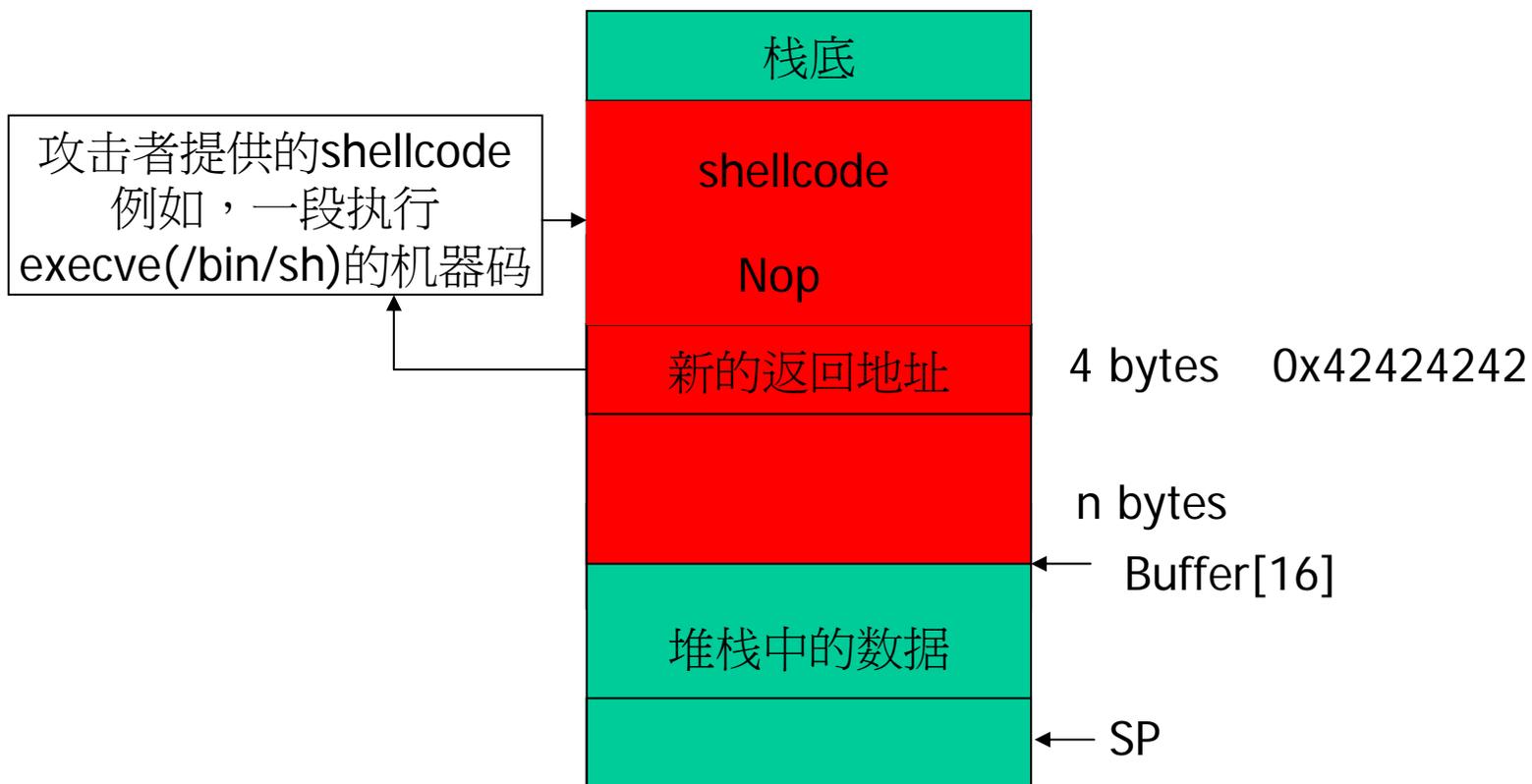
攻击者调用一个函数后，堆栈内容



如果这个函数发生了溢出...



堆栈缓冲区溢出攻击的方法



缓冲区溢出的后果

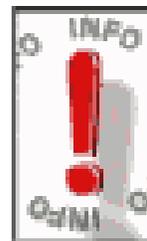
- 攻击者可以使远程服务程序或者本地程序崩溃
- 攻击者可以以被攻击的程序运行时的身份执行任意代码。如果该程序以特权用户身份运行，攻击者可以远程或者本地提升权限。

缓冲区溢出漏洞存在的原因

- 开发者没有进行边界检查
 - 开发者缺乏安全编程的意识
 - 认为分配的内存通常足够使用了
 - 使用不安全的数据拷贝函数
 - `strcpy`, `strcat`, `gets`, `sprintf`,
- 开发者没有进行正确的边界检查
 - 错误的使用一些“安全”拷贝函数也可能会导致缓冲区溢出，例如
 - `memcpy(dest, src, strlen(src))`

防止buffer overflow攻击

- 及时发现修补。
- 下载最新的程序和补丁。
- 去掉发生问题的SUID程序的SUID权限。
- 养成良好的编程风格。
- 检验参数的有效性。
- 测试并审计每个程序
- 禁用不用的或危险的服务



Buffer Overflow问题的影响

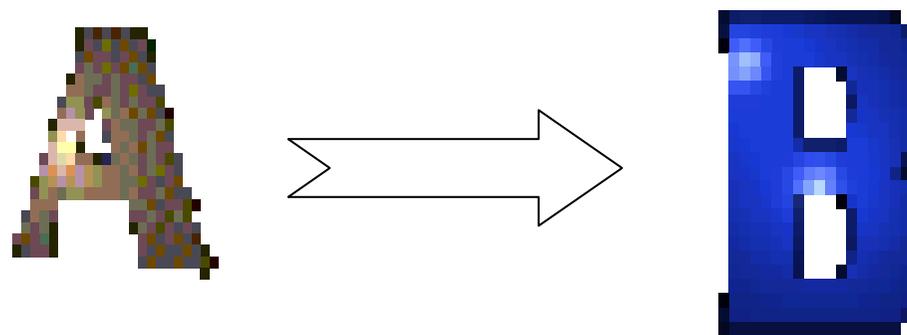
- 当前的安全机制无法很好的防御BO
- 越来越多的buffer overflow被发现。
- 互联网上可以查询到很多源代码，非常容易被利用。
- 一旦被成功攻击，攻击者往往可以获得系统的管理员权限。
- 堆栈溢出后程序也可以用作其他用途：
 - 崩溃产生的core文件覆盖系统文件（掩藏踪迹）。
 - DoS攻击等。

拒绝服务攻击

欺骗与侦听技术

什么是spoofing?

- 把数据传送的源地址伪装成别人的地址



主要的spoofing技术

- 硬件地址伪装 (ARP spoofing)
- IP地址伪装 (IP Spoofing)
- email地址伪装 (Anonymous Mail)
- 域名伪装 (DNS Spoofing)
- 陷阱伪装 (Honey Pot)

与spoofing相关的技术

- 拒绝服务 (DoS)
- 侦听 (sniffer)

Spoofing的目的

- 逃避检查和追踪
- 绕过防火墙
- 伪装成信任主机
- 伪装成路由器
- 切断别人的连接
- 接管别人的连接
- 节省带宽***

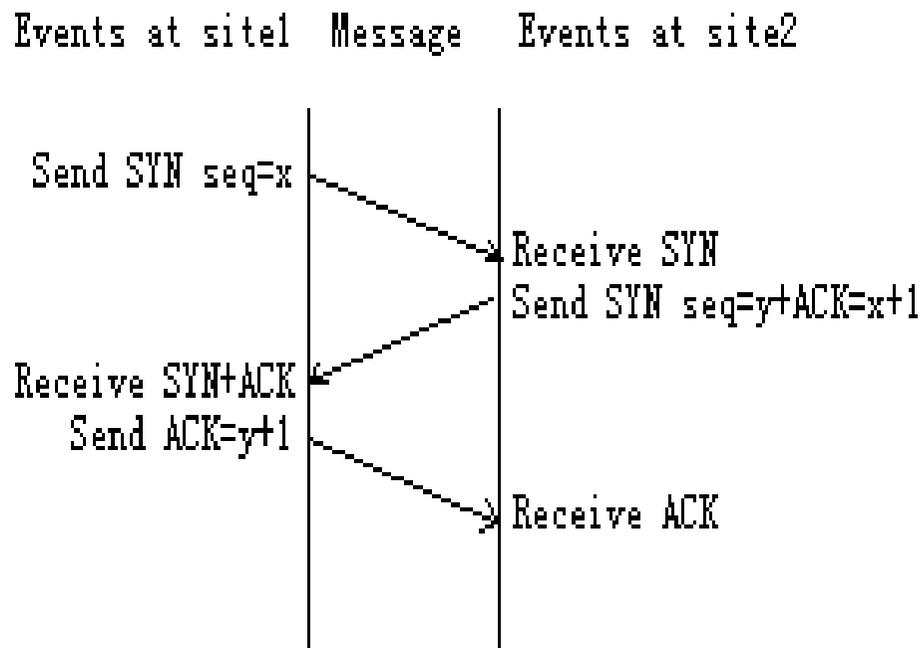
TCP连接欺骗 (Connect Hijack)

- 伪装成信任主机
- 一种比较复杂的攻击
- 盲攻击
- 较熟练的黑客才可能采用 (Mitnick)
- 行之有效

TCP连接欺骗 (Connect Hijack)

- 攻击过程

找出C的TCP报文中SYN序号 (seq=y) 的规律



TCP: Establish a connection.

TCP连接欺骗 (Connect Hijack)

- 攻击过程
 - A伪装成B向C发出TCP握手信号中的第一个信号 (Send SYN=x)。连接C的rsh服务。
 - A伪装成B发出TCP握手信号的第三个信号 (Send ACK=y+1)。其中这个y需要根据前面找出的规律进行猜测。如果猜测正确，C应该认为B已经连上。

TCP连接欺骗 (Connect Hijack)

- 攻击过程
 - C检查信任关系，发现B是可信主机，于是处于接收命令的状态。
 - A伪装成B向C的rsh服务发送一个命令。比如echo “+ +”>.rhosts。C执行这个命令。
 - 执行完这个命令以后A也成了C的信任主机，这样A就可以正常地用rlogin登录C。

TCP连接欺骗 (Connect Hijack)

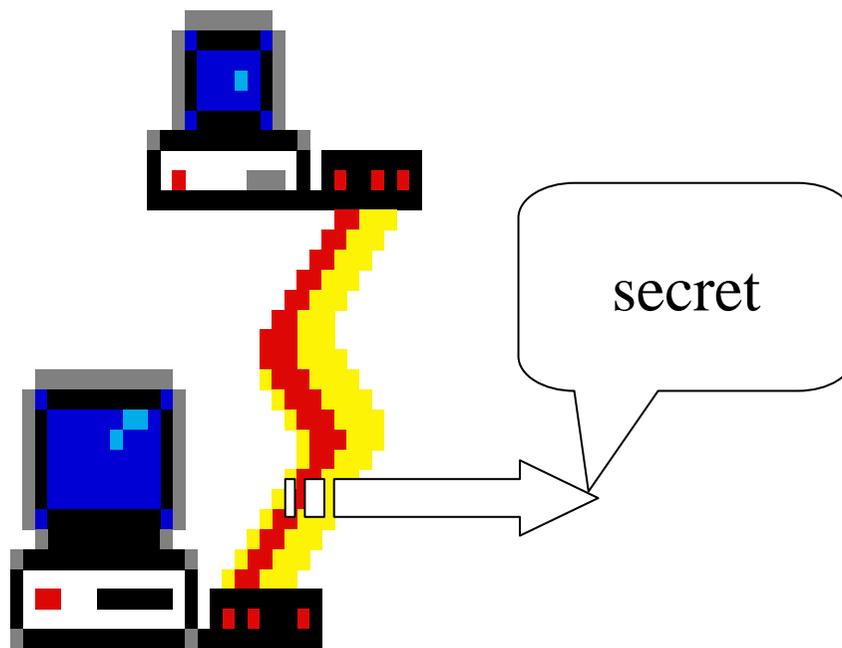
- 解决办法：
 - 尽量减少信任关系。
 - 升级操作系统，使用随机TCP序号，让黑客很难猜测序号。
 - 防火墙或路由器过滤声称来自信任主机的报文。

Sniffer: 古老而实用的技术

- 历史上的侦听
- 现代军事上的监听
- 网络中的广泛应用
 - 网络管理
 - 协议分析
 - 入侵检测

侦听的主要内容

- 侦听用户名和密码。
- 侦听访问内容。
- 隐私的泄漏。
- 击键记录等



侦听的发展

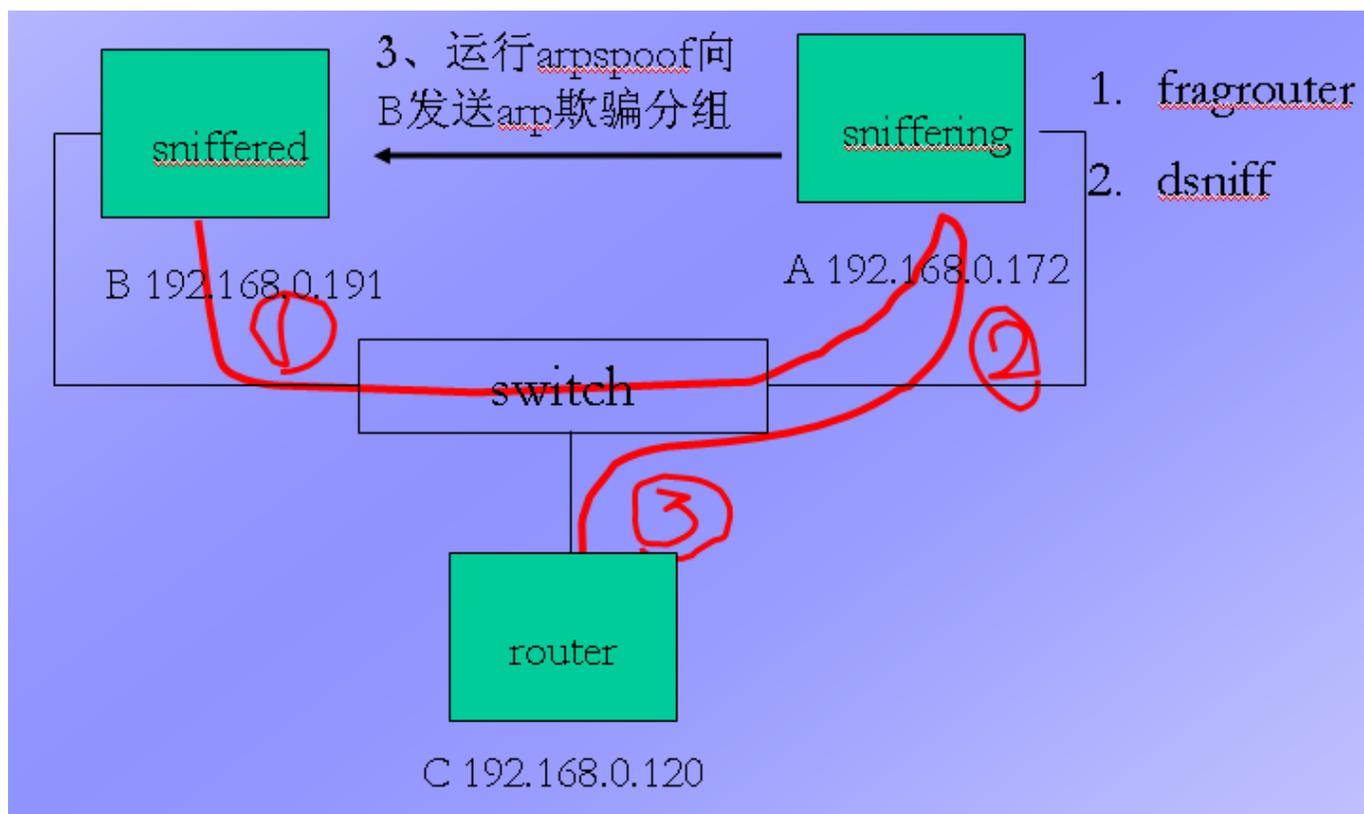
- 在交换模式大量使用的情况下，单独的Sniffer技术应用较少
- 常与Spoofing手法、后门技术配合使用

共享环境下的嗅探技术

- 原理
 - 在以太网中是基于广播方式传送数据
 - 网卡置于混杂模式下可以接收所有经的数据
- 工具
 - Sniffer pro、IRIS、netxray
 - tcpdump、snoop、dsniff

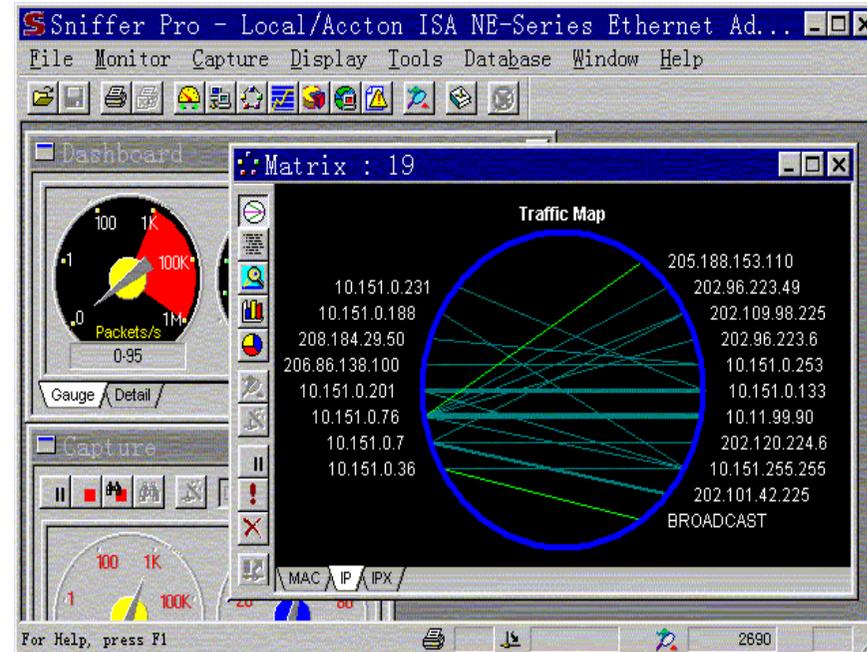
交换环境下的嗅探技术

- arpspoof, fragrouter, dsniff



侦听工具

- Unix平台：
 - TCPDump
 - Sniffit (Solaris、SGI和Linux)
 - snoop
 - Dsniff
- Windows平台
 - Sniffer Pro (NetXray)
 - Iris



发现侦听器

- 网络通讯掉包率反常的高.
- 网络带宽将出现反常.
- 系统运行速度减慢。
- Ps可以查看可疑的进程。
- 查看网卡是否处于侦听模式。
- 发现网络上的侦听器。

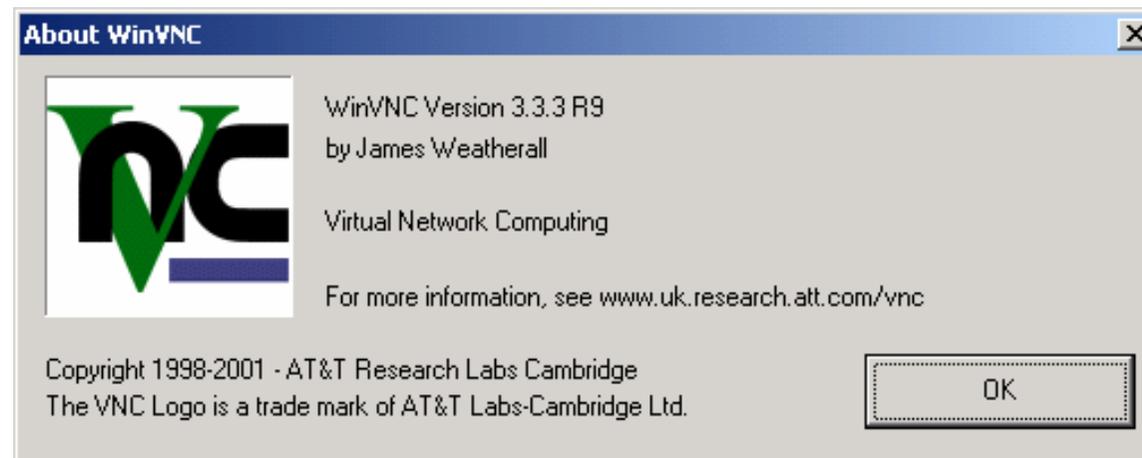
击败侦听器

- 定期检查网络流量；
- 把集线器换成交换机。
- 加密传输数据。（SSH、IPSec）

远程控制与木马

远程控制程序

- 著名的远端控制程序
 - Windows Terminal Server(3389)
 - pcAnywhere (5631、 5632)
 - ControlIT(799、 800)
 - VNC(Vitual Network Computing) (5800、 5801)



远程控制程序

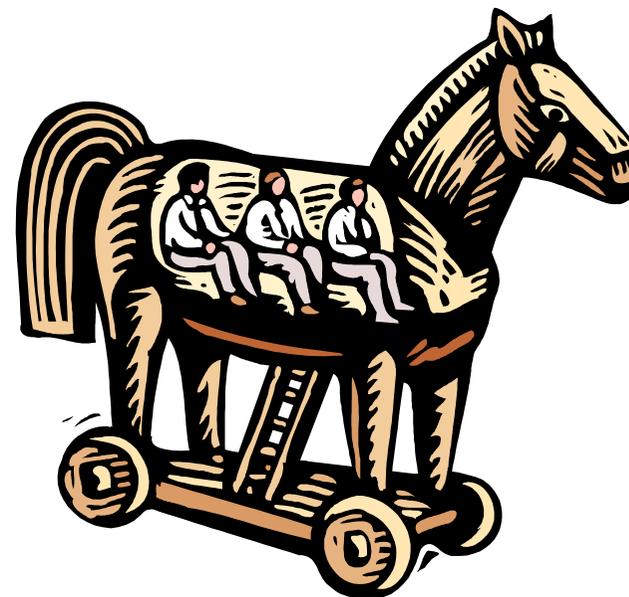
- 远程控制软件的陷序
 - 明文形式的用户名和密码
 - 弱加密的密码
 - 抓屏软件可以获取密码
 - 上传初始定制文件

远程控制程序

- 对远程控制程序的保护：
 - 加密会话分组
 - 限制登陆尝试次数
 - 登记失败的登陆尝试
 - 锁闭登陆失败的用户
 - 改变缺省监听端口

后门技术

- 攻击者在攻入系统后，创建其能迅速重新获得访问权的机制。包括：
 - 开启某种服务；
 - 用户账号；
 - 启动文件；
 - 受调度的作业；



后门技术

- 远程控制软件的利用
- Rootkit;
- 木马程序;
- 脚本后门;
- 隐藏程序及日志清除技术等

- 植入后门程序的方式
 - 利用已经获得的账户与口令;
 - 攻破系统后放入;
 - 利用浏览器软件的缺陷;
 - 欺诈的方式(邮件的附件或绑定某程序-木马)

后门

- 启动文件
 - NT: Startup文件夹下的All Users文件夹;
 - Unix: rc.d与inetd.conf
- 受调度的作业
 - At `\\192.168.50.10 12:00A /every:1 "nc -d -L -p8080 -e cmd.exe"`
 - Unix : crontab

后门程序的发现

- 审计超级用户特权或属于特权用户组的所有用户账号；
- 审查启动配置文件，查找让人怀疑的内容；
- 自动扫描工具
 - 模拟连接端
 - 端口扫描；
- 保留正常端口清单

后门程序的发现

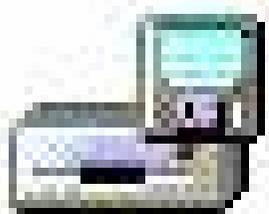
- 检查端口开放情况及相关的程序
 - `Netstat -an; fport; lsof`
- 检查系统进程
- 使用实时病毒扫描程序，并注意升级。

恶意代码

- 恶意代码—恶意破坏或非授权运行的程序或移动代码。主要包括病毒、蠕虫与木马及其他后门程序等



恶意代码的传播途径



磁盘到磁盘

程序到程序

文档到文档



通过电子邮件或浏览器

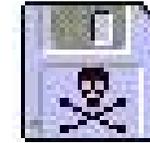


通过网络共享

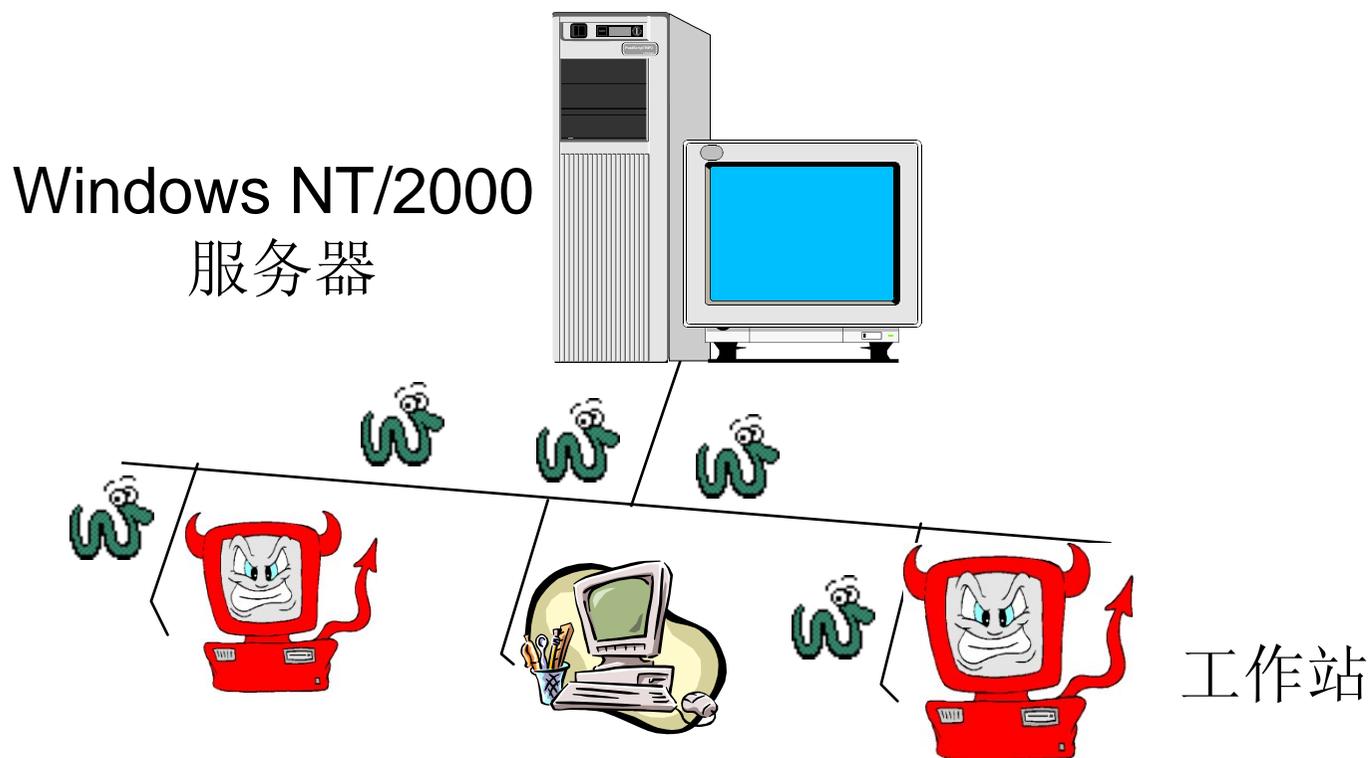
病毒 (Virus)



- BOOT 引导型病毒
- DOS 病毒
- Windows 病毒
- 宏病毒
- 脚本病毒
- Java 病毒



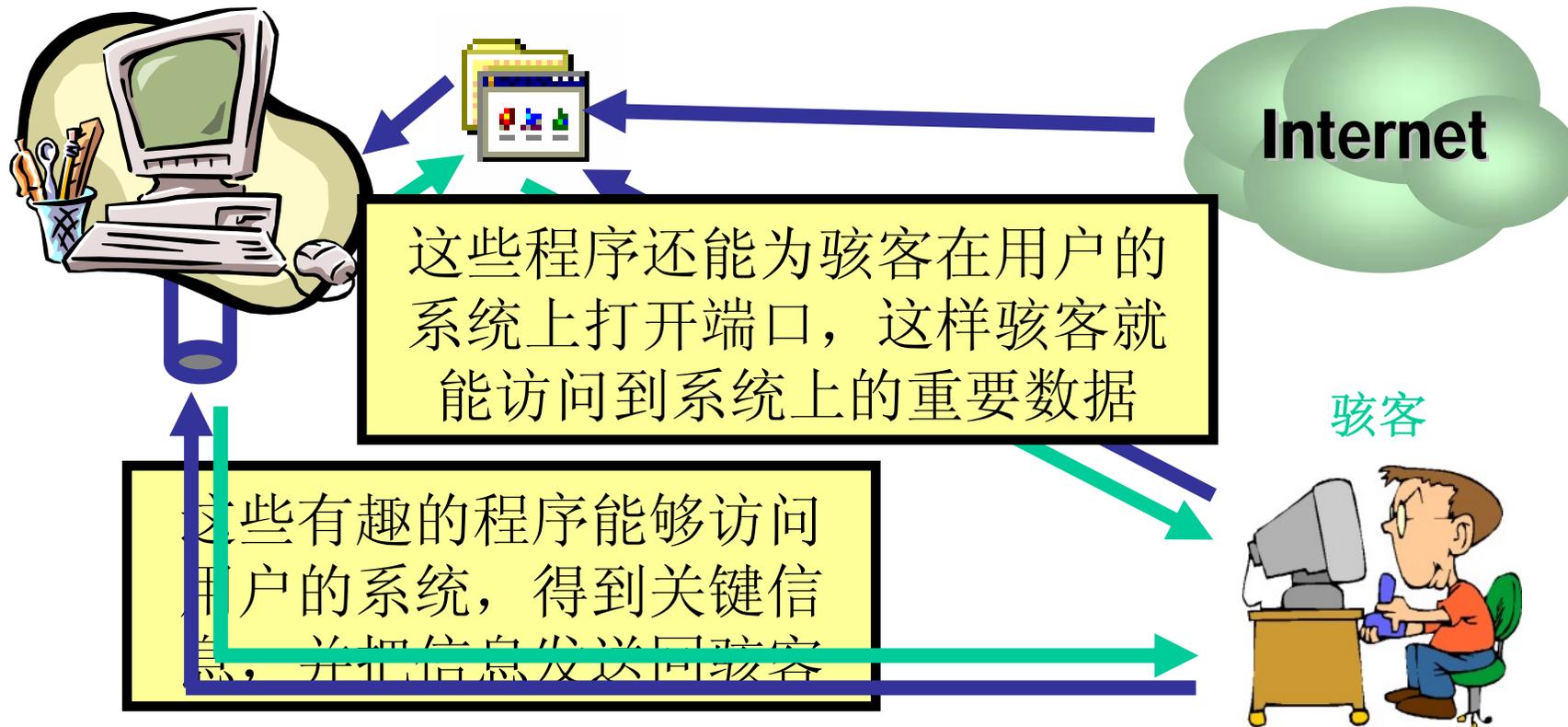
蠕虫 (Worm)



- 病毒借助载体进行传播；
- 蠕虫是一个自包含的程序，能够把自己自己的全功能拷贝传播到其它计算机系统中。

蠕虫 (Worm)

- 蠕虫一般由3个部分组成：
 - 感染 (Enabling Vulnerability)
 - 利用最新的漏洞获得系统的权限
 - 传播 (Spreading Mechanism)
 - 自动选择新目标并传播，速度非常快
 - Nimda、CodeRed
 - 携带 (Malicious Payload)
 - DOS Zombie、Backdoor、Rootkit等



网络骇客工具是恶意的程序，唯一的目的是远程控制计算机，探测某些系统的后门

木马

- 木马程序一般是C/S结构；
- Server端一般安装在被控主机上，字节较小，常使用较让人迷惑的名字，如patch.exe
- Client端一般是图形化界面；
- 常存在配置程序，可以按需要生成server程序。

常见的木马程序

- 冰河
 - 名称:
 - G_clind
 - G_server
 - 缺省端口
 - 7626 (TCP)



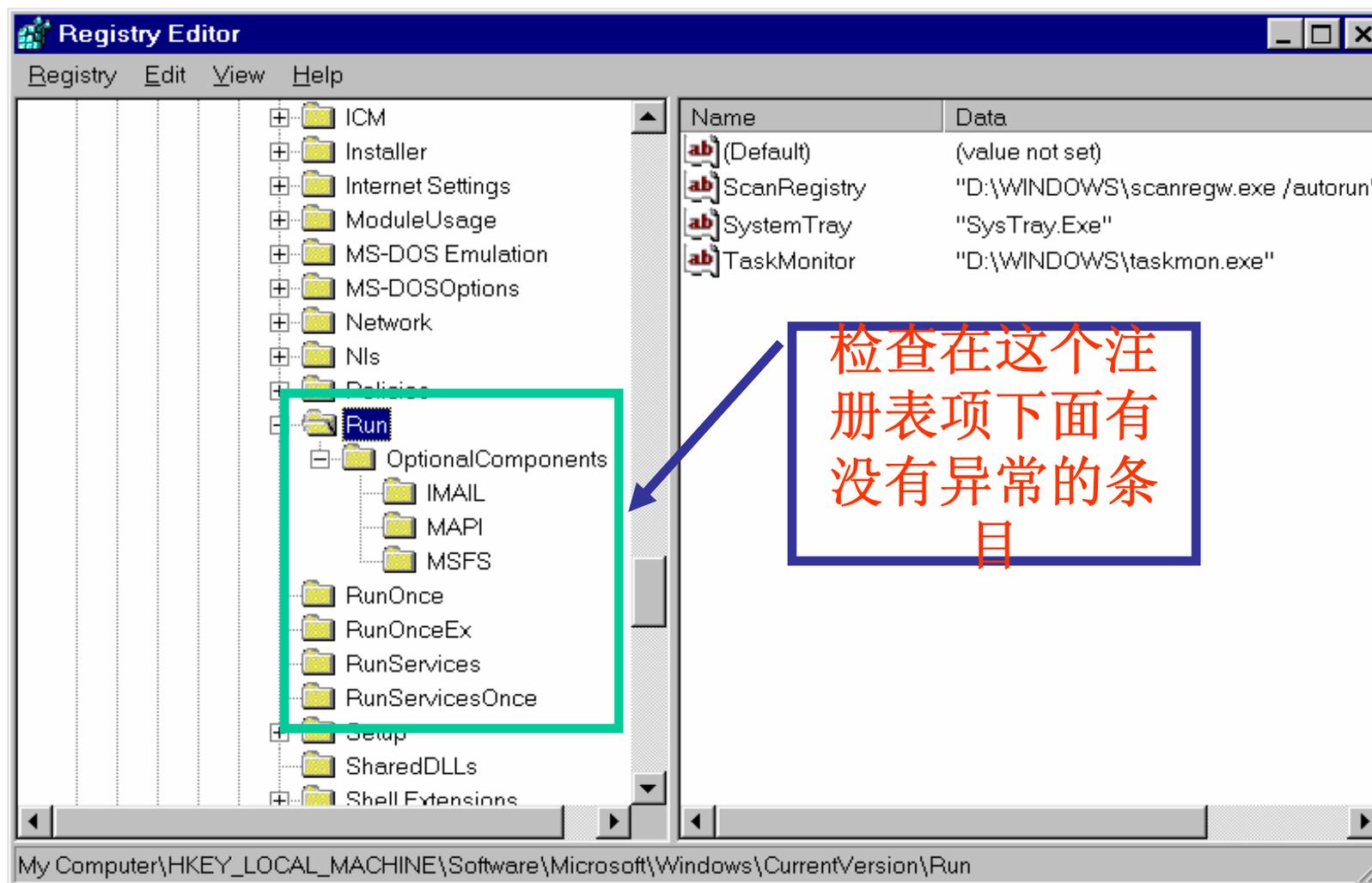
恶意代码的发现

- 检测这些恶意软件的方法与检测Windows 病毒的方法相同（注册表，任务管理器....）
 - 有时这些程序能够驻留在内存里
 - 这些程序能够通过网络或电子邮件对其它系统进行攻击
 - 系统速度异常降低
 - 系统或屏幕出现异常行为

恶意代码的发现

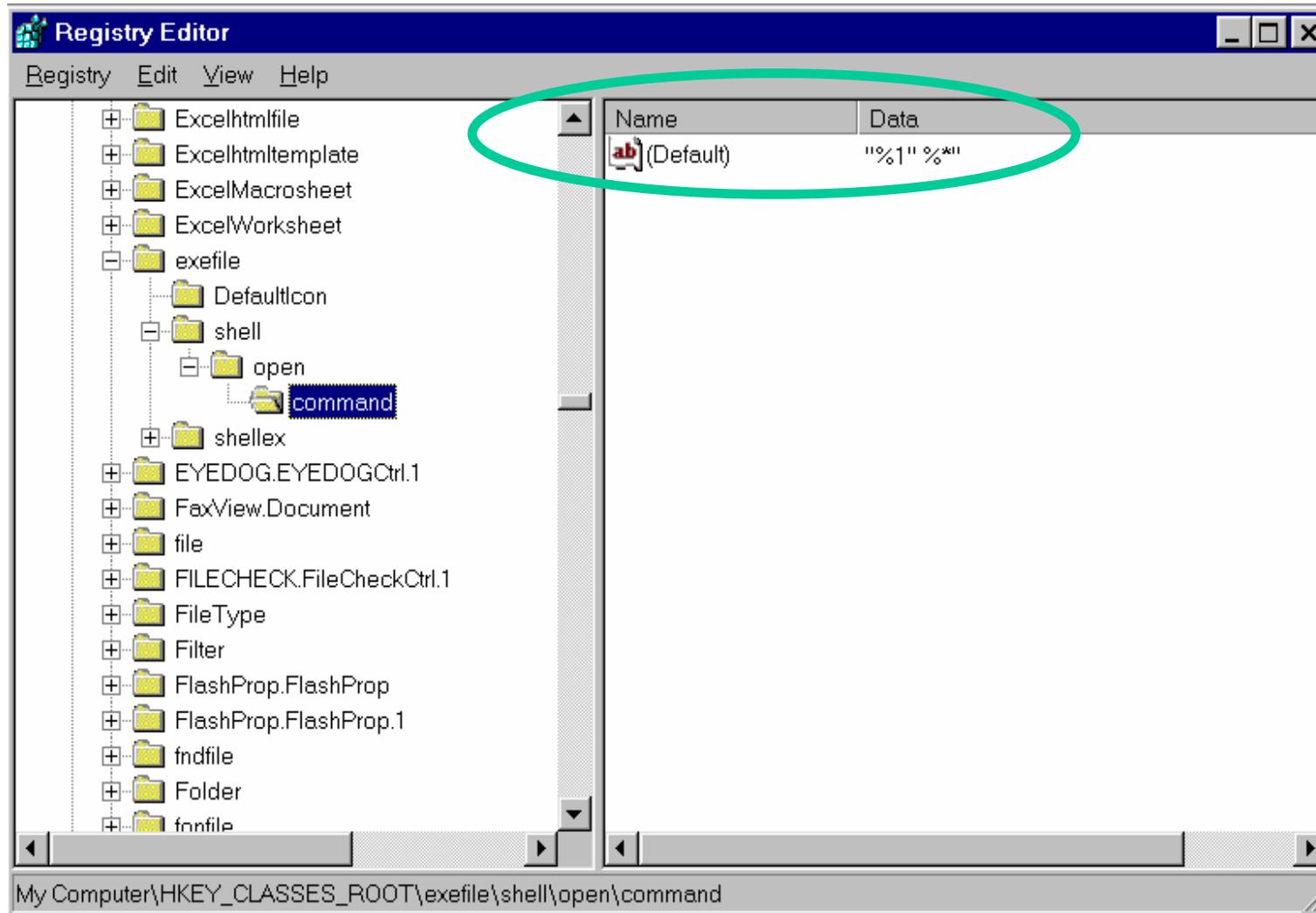
- 检测注册表，查找病毒可能存在的迹象
 - 运行注册表编辑 Regedit.exe，检测下列注册表项
 1. \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run: RunOnce: RunServices: RunServicesOnce
 2. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon

恶意代码的发现



恶意代码的发现

- 也可以检测这个位置



恶意代码的发现

- 检查启动文件；
 - %systemroot%\profiles\%username%\starmenu\programes\starup
 - Win.ini
 - SYSTEM.INI文件内加入load、run 可以调用程序
 - Autoexec.bat
 - Rc.d 目录与 inetd.conf文件(Unix)

恶意代码的发现

- 检查\System 与\System32 下的可执行文件，检查他们的属性，若无版本说明，多为可疑文件；
- 改变这些文件的属性。

黑客的社会工程学

-
- 黑客的社会工程



Thanks!