



# 北京大学网络攻防技术与实践课程

---

实践讲解-**Win2K**系统被攻陷并加入僵尸网络

诸葛建伟

zhugejianwei@icst.pku.edu.cn

北京大学计算机研究所信安中心



# 实践-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。



# 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？**



# 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
- ❑ **Wireshark**流重组可能会丢失**session**内容，推荐**snort(session规则选项), tcpflow**
- ❑ 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
- ❑ 问题**6**和问题**7**



# 问题1- IRC是什么

---

- **IRC**指的是**Internet Relay Chat**。它是一种使用客户端-服务器架构的多用户聊天系统。客户端用户可以加入特定的频道(**channel**)与该频道中的所有用户聊天,也可以采用私聊的方式。
- **IRC**客户端
  - **Xchat**
  - **mirc**



# 问题1-IRC客户端申请加入一个IRC网络时将发送哪个消息

- 注册时需要发送的消息有三种，分别是口令，昵称和用户信息。格式如下：

**USER** <username> <hostname> <servername>  
<realname>

**PASS** <password>

**NICK** <nickname>

- 注册完成后，客户端就使用**JOIN**信息来加入频道，格式如下：

**JOIN** <channel>



# 问题1-IRC一般使用哪些TCP端口

---

- **IRC**服务器通常在**6667**端口监听，也会使用**6660—6669**端口
  
- 攻击者滥用**IRC**构建僵尸网络时，可能使用任意的端口构建**IRC**僵尸网络控制信道
  - 基于端口识别服务不再可靠
  - 基于应用协议特征进行识别
  - **IRC: USER/NICK**等注册命令



# 问题2-僵尸网络是什么

- 僵尸网络 (**botnet**) 僵尸网络(**BotNet**): 攻击者出于恶意目的, 传播僵尸程序控制大量主机, 并通过一对多的命令与控制信道所组成的网络。
  - 定义特性: 一对多的命令与控制通道的使用
  - 恶意性
  - 网络传播特性
- 僵尸程序(**Bot**)
  - **Robot**演化过来的词汇, 攻击者用以控制傀儡主机的程序
- 僵尸主机(**Zombie**, 或称为傀儡主机、肉鸡)
- 僵尸网络演化: 传统**IRC**→**HTTP & P2P**
  - 目前最流行的是**Storm worm**





## 问题2-僵尸网络通常用于什么

---

- 僵尸网络危害—提供通用攻击平台
  - 分布式拒绝服务攻击
  - 发送垃圾邮件
  - 窃取敏感信息
  - 点击欺诈
  - ...
- **Know More:** 综述文章-诸葛建伟等, 僵尸网络研究, 软件学报, **2008年3月期**。



# 问题3

---

- ❑ 蜜罐主机（**IP地址：172.16.134.191**）与哪些**IRC**服务器进行了通信？
- ❑ 思路：过滤出蜜罐主机尝试连接**6667**端口的**SYN**包
- ❑ 方法：  
**Wireshark: ip.src == 172.16.134.191 and tcp.dstport == 6667 and tcp.flags == 0x2 (SYN)**
- ❑ **5台IRC服务器：**  
**209.126.161.29 66.33.65.58 63.241.174.144**  
**217.199.175.10 209.196.44.172**



# 问题4

- 这段观察期间有多少不同的主机访问了以**209.196.44.172**为服务器的僵尸网络?
  - 估计方法**1**: 当前在线数**current\_global\_users (4752)**
  - 估计方法**2**: **IRC**广播加入和离开服务器的不同主机数
  - 估计方法**3**: 观察期间不同昵称出现个数

- 用**tcpflow**进行分流处理

**tcpflow -r pcap\_file 'host 209.196.44.172 and port 6667'**

估计方法**2**: 观察**JOIN**和**QUIT**僵尸网络的**IP**数量(注意重复主机)

```
grep JOIN 209.196.044.172.06667-172.016.134.191.01152 | cut -d '@'  
-f 2 | cut -d ' ' -f 1 | sort | uniq > join_hosts
```

```
grep QUIT 209.196.044.172.06667-172.016.134.191.01152 | cut -d '@'  
-f 2 | cut -d ' ' -f 1 | sort | uniq > quit_hosts
```

```
cat join_hosts > all_hosts; cat quit_hosts >> all_hosts; cat all_hosts |  
sort | uniq | wc -l
```

**5580 hosts**



# 问题4-估计方法3

```
$ cat 209.196.044.172.06667-172.016.134.191.01152 \  
| grep "^:irc5.aol.com 353" \  
| sed "s/^:irc5.aol.com 353 rgdiuggac @ #x[^x]*x ://g" \  
| tr ' '\n' \  
| tr -d "\15" \  
| grep -v "^$" \  
| sort -u \  
| wc -l
```

# 获取昵称输出行  
# 去除前缀，注：可能无法匹配  
# 将空格转换为新行  
# 去除\r  
# 去除空行  
# 排序并去除重复  
# 获得行数

**3457**



# 问题5-哪些IP地址被用于攻击

- 由于蜜罐特殊性，所有进入蜜罐的流量都被视为可疑流量
- IP地址数过多，wireshark等GUI工具不能胜任
- **tcpdump -nn -r pcap\_file dst host 172.16.134.191 | awk -F" " '{print \$3}' | cut -d '.' -f 1-4 | sort -t. -u -k1,1n -k2,2n -k3,3n -k4,4n > ip\_list.txt; wc -l ip\_list.txt**
- **165 ip\_list.txt**



# Snort

---

- ❑ 拿Snort跑一下pcap\_file pcap文件
  - Snort-2.6.1.4缺省配置, ALERTS: 1764
- ❑ 查看alert报警文件
  - `cat alert | grep "\[.*\]" | sort | uniq -c | sort -g`: 报警类型和条数
    - ❑ WEB-IIS, DIRECTORY TRAVERSAL, MS-SQL Worm
    - ❑ CodeRed v2, ISAPI .ida attempt, SMB-DS repeated logon, SAM Attempt
  - `cat alert | grep "03\/" | cut -d ' ' -f 2 | cut -d ':' -f 1 | sort | uniq -c | sort -g`: 报警攻击源IP和条数
    - ❑ 1531 24.197.194.106, 41 210.22.204.101, 12 61.150.72.7
  - `cat alert | grep "03\/" | cut -d ' ' -f 4 | cut -d ':' -f 2 | sort | uniq -c | sort -g`: 攻击目标端口报警条数
    - ❑ 1566 80, 165 1434, 22 445



# Top 3 Attacker分析

---

## □ Top 3 Attacker分析

- `cat alert | grep -B 2 "24.197.194.106" | grep "\[\\*\\*\\] \[" | sort | uniq -c | sort -g: Web-IIS探测`
- `cat alert | grep -B 2 "210.22.204.101" | grep "\[\\*\\*\\] \[" | sort | uniq -c | sort -g : 210.22.204.101: SMB查点、口令猜测`
- `cat alert | grep -B 2 "61.150.72.7" | grep "\[\\*\\*\\] \[" | sort | uniq -c | sort -g : 61.150.72.7: MS-SQL Worm`

# 问题6-攻击者攻击了哪些安全漏洞

□ 利用wireshark协议统计功能大致了解网络流分布情况

■ 只有IP包

■ UDP

□ NetBIOS Datagram

□ Data?

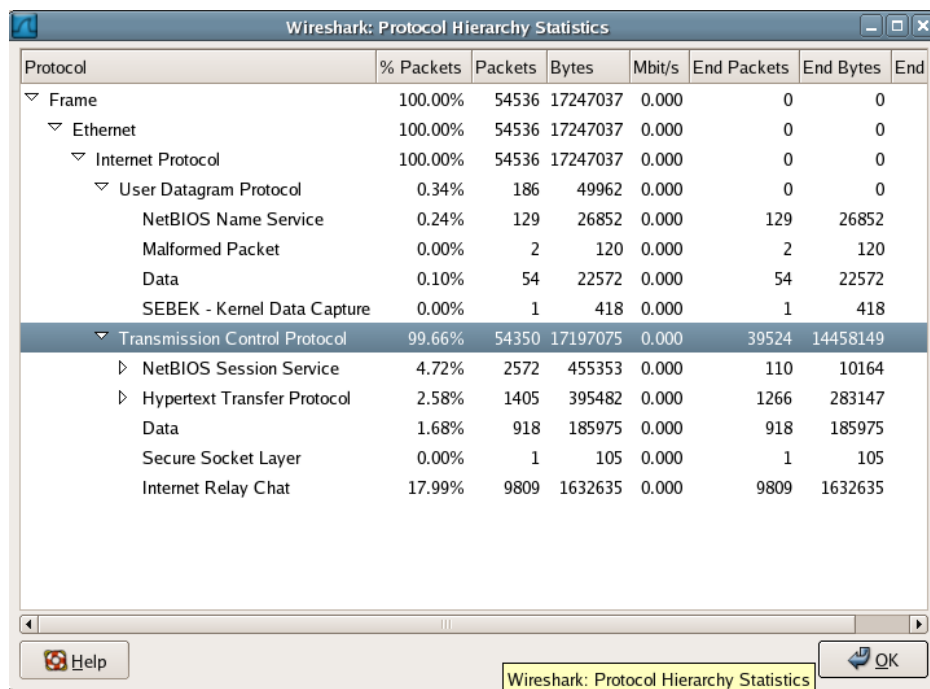
■ TCP

□ NetBIOS Session

□ HTTP

□ Data?

□ IRC



Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End
▼ Frame	100.00%	54536	17247037	0.000	0	0	
▼ Ethernet	100.00%	54536	17247037	0.000	0	0	
▼ Internet Protocol	100.00%	54536	17247037	0.000	0	0	
▼ User Datagram Protocol	0.34%	186	49962	0.000	0	0	
NetBIOS Name Service	0.24%	129	26852	0.000	129	26852	
Malformed Packet	0.00%	2	120	0.000	2	120	
Data	0.10%	54	22572	0.000	54	22572	
SEBEK - Kernel Data Capture	0.00%	1	418	0.000	1	418	
▼ Transmission Control Protocol	99.66%	54350	17197075	0.000	39524	14458149	
▶ NetBIOS Session Service	4.72%	2572	455353	0.000	110	10164	
▶ Hypertext Transfer Protocol	2.58%	1405	395482	0.000	1266	283147	
Data	1.68%	918	185975	0.000	918	185975	
Secure Socket Layer	0.00%	1	105	0.000	1	105	
Internet Relay Chat	17.99%	9809	1632635	0.000	9809	1632635	

□ →攻击者攻击了哪些目标端口?





# 攻击者攻击了哪些目标端口？

- 攻击者扫描的**TCP**端口: 90个端口
  - `tcpdump -r pcap_file -nn dst host 172.16.134.191 and tcp[tcpflags]== 0x2 | cut -d ' ' -f 5 | more | cut -d '.' -f 5 | cut -d ':' -f 1 | sort | uniq > scanned_tcp_ports; wc -l scanned_tcp_ports;`
- 哪些**TCP**端口是开放的, 响应的**TCP**端口
  - `tcpdump -r pcap_file -nn src host 172.16.134.191 and tcp[tcpflags]== 0x12 | cut -d ' ' -f 3 | cut -d '.' -f 5 | sort | uniq > responded_tcp_ports`
  - 135(rpc), 139(netbios-ssn), 25(smtp), 445(smb), 4899(radmin), 80(http)
- 攻击者扫描的**UDP**端口和蜜罐响应的**UDP**端口:
  - `tcpdump -r pcap_file -nn dst host 172.16.134.191 and udp | cut -d ' ' -f 5 | more | cut -d '.' -f 5 | cut -d ':' -f 1 | sort | uniq > scanned_udp_ports`
  - 137(netbios-ns), 1434(ms-sql-m), 28431(unknown)
  - `tcpdump -r pcap_file -nn src host 172.16.134.191 and udp | cut -d ' ' -f 3 | cut -d '.' -f 5 | sort | uniq | more > responded_udp_ports`
  - 137(netbios-ns)



- |      | Data (376 bytes)        |                         |                    |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|------|-------------------------|-------------------------|--------------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| 0020 | 86 bf 05 66 05 9a 01 80 | 37 b3 04 01 01 01 01 01 | .....f.... 7.....  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0030 | 01 01 01 01 01 01 01 01 | 01 01 01 01 01 01 01 01 | .....              |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0040 | 01 01 01 01 01 01 01 01 | 01 01 01 01 01 01 01 01 | .....              |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0050 | 01 01 01 01 01 01 01 01 | 01 01 01 01 01 01 01 01 | .....              |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0060 | 01 01 01 01 01 01 01 01 | 01 01 01 01 01 01 01 01 | .....              |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0070 | 01 01 01 01 01 01 01 01 | 01 01 01 01 01 01 01 01 | .....              |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0080 | 01 01 01 01 01 01 01 01 | 01 01 01 dc c9 b0 42 eb | .....B.            |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0090 | 0e 01 01 01 01 01 01 01 | 70 ae 42 01 70 ae 42 9b | ..... p.B.p.B.     |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 00a0 | 90 90 90 90 90 90 90 68 | dc c9 b0 42 b8 01 01 01 | .....h ..B.....    |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 00b0 | 01 31 c9 b1 18 50 e2 fd | 35 01 01 01 05 50 89 e5 | .l...P.. 5...P..   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 00c0 | 51 68 2e 64 6c 6c 68 65 | 6c 33 32 68 6b 65 72 6e | Qh.dllhe l32hkern  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 00d0 | 51 68 6f 75 6e 74 68 69 | 63 6b 43 68 47 65 74 54 | Ghounthi ckChg2_f  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 00e0 | 66 b9 6c 6e 51 68 33 32 | 2e 64 68 77 73 32 5f 66 | f.llQh32 ...dws2_g |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 00f0 | b9 65 74 51 68 73 6f 63 | 6b 66 b9 74 6f 51 68 73 | .etQhsoc kf.toQhs  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0100 | 65 6e 64 be 18 10 ae 42 | 8d 45 d4 50 ff 16 50 8d | end....B .E.P..P.  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0110 | 45 e0 50 8d 45 f0 50 ff | 16 50 be 10 10 ae 42 8b | E.E.P.E.P. T....B. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0120 | 1e 8b 03 3d 55 8b ec 51 | 74 05 be 1c 10 ae 42 ff | ....=U.Q t....B.   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0130 | 16 ff d0 31 c9 51 51 50 | 81 f1 03 01 04 9b 81 f1 | ...l.QQP .....     |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0140 | 01 01 01 01 51 8d 45 cc | 50 8b 45 c0 50 ff 16 6a | ...Q.E .P.E.P..j   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0150 | 11 6a 02 6a 02 ff d0 50 | 8d 45 c4 50 8b 45 c0 50 | .j.j...P .E.E.P.E  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0160 | ff 16 89 c6 09 db 81 f3 | 3c 61 d9 ff 8b 45 b4 8d | .....<a...E.       |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0170 | 0c 40 8d 14 88 c1 e2 04 | 01 c2 c1 e2 08 29 c2 8d | .@..... )....      |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0180 | 04 90 01 d8 89 45 b4 6a | 10 8d 45 b0 50 31 c9 51 | ...E.j .E.E.P.I.Q  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 0190 | 66 81 f1 78 01 51 8d 45 | 03 50 8b 45 ac 50 ff d6 | f...x.Q.E .P.E.P.. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 01a0 | eb ca                   |                         | ..                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

18



# TCP端口流量分析-135 & 25

```
[root@localhost exercise5]# tcpdump -r exercise5 -nn dst host 172.16.134.191 and dst port 135 | more
reading from file exercise5, link-type EN10MB (Ethernet)
10:55:34.426790 IP 195.36.247.77.4768 > 172.16.134.191.135: S 148910790:148910790(0) win 16384 <mss 1420,nop,nop,sackOK>
10:55:35.489754 IP 195.36.247.77.4768 > 172.16.134.191.135: . ack 2453546202 win 17040
10:55:35.507924 IP 195.36.247.77.4768 > 172.16.134.191.135: F 0:0(0) ack 1 win 17040
10:55:36.386712 IP 195.36.247.77.4768 > 172.16.134.191.135: . ack 2 win 17040
```

```
[root@localhost exercise5]# tcpdump -r exercise5 -nn dst host 172.16.134.191 and dst port 25 | more
reading from file exercise5, link-type EN10MB (Ethernet)
18:42:47.636184 IP 24.197.194.106.3729 > 172.16.134.191.25: S 1591356806:1591356806(0) win 16384 <mss 1460,nop,nop,sackOK>
18:42:47.706512 IP 24.197.194.106.3729 > 172.16.134.191.25: . ack 1256243764 win 17520
18:42:47.706514 IP 24.197.194.106.3729 > 172.16.134.191.25: F 0:0(0) ack 1 win 17520
18:42:47.706516 IP 24.197.194.106.3736 > 172.16.134.191.25: S 1591694689:1591694689(0) win 16384 <mss 1460,nop,nop,sackOK>
18:42:47.799981 IP 24.197.194.106.3736 > 172.16.134.191.25: . ack 1256323915 win 17520
18:47:46.085103 IP 24.197.194.106.2017 > 172.16.134.191.25: S 1750117730:1750117730(0) win 16384 <mss 1460,nop,nop,sackOK>
18:47:46.147902 IP 24.197.194.106.2017 > 172.16.134.191.25: . ack 1343866961 win 17520
18:48:03.639960 IP 24.197.194.106.2017 > 172.16.134.191.25: F 0:0(0) ack 1 win 17520
```

❑ **135 MSPRC/25 SMTP: 建立连接, 没数据 -> Connect() 扫描?**



# TCP端口流量分析-80

- 提取**80**端口的**Inbound**流量
  - **tcpdump -r pcap\_file -nn dst host 172.16.134.191 and dst port 80 -w port80inboundtraffic.pcap**
  - **tcpflow -r port80inboundtraffic.pcap**
- 查看连接**80**端口的**IP**地址
  - **ls -lS | awk -F" " '{print \$9}' | cut -d '-' -f 1 | cut -d '.' -f 1,2,3,4 | sort | uniq (7 hosts)**
    - **024.197.194.106: Web探测**
    - **066.008.163.125: 1个连接访问首页(User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600)**
    - **068.169.174.108: 2个连接访问首页(User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.0.2)**
    - **192.130.071.066: 1个HEAD /连接**
    - **210.022.204.101: ISAPI.ida攻击/HEAD /连接**
    - **213.023.049.158: 1个HEAD /连接**
    - **218.025.147.083: CodeRed**



# TCP端口80流量分析-Web探测

---

## □ 24.197.194.106

- 有交互的连接数: 883

- Snort报警数: 157类报警1531次报警

- 大部分为WEB-IIS、WEB-CGI、WEB-FRONTPAGE、WEB-MISC等类

- 大部分为xxx access和xxx attempt

## □ 结论: 24.197.194.106对蜜罐主机进行了疯狂的Web探测

- 进阶课程-Web应用的攻击及防御技术







# TCP端口139流量分析

## □ TCP 139端口

- NetBIOS Session Service (netbios-ssn)
- Server Message Block Protocol (SMB)

## □ 提取139端口的Inbound流量

- `tcpdump -r pcap_file -nn dst host 172.16.134.191 and dst port 139 -w port139inboundtraffic.pcap`
- `tcpflow -r port139inboundtraffic.pcap`

## □ 查看提取出的139端口session data

- `ll -IS | more`
- 相同的聚类: 使用md5sum工具
- 只剩下7个不同的session data, review

## □ 查看这7个139端口的不同攻击流

- `hexdump/vim (:%!xxd)`
- `wireshark` (源IP、目标IP、目标端口过滤)

## □ 结论: SMB查点(两次空会话连接)

```
[root@localhost 139inbound]# md5sum * |  
cut -d ' ' -f 1 | sort | uniq -c  
21 02bbacd7786a5de951a4f46416bcf2  
11 291ad8657f45a25942ba086a186a0e8c  
1 58f59ff84bb6eb10c38ea3ebe47d47fc  
1 7b15f30f5fd59c4a2ef3a12f430adfa7  
8 8a4ad4d4f3e4744e4fbfe9dcd79ab2b8  
11 d6bcefb3b55db1126b2fc413e0cc649f  
1 f01d05bbb249ec73f0d5ee1d20904efa  
[root@localhost 139inbound]# strings * |  
sort | uniq -c  
53 D  
FDECENDBDJDBCACACACACACACACACACA  
51 !\\PC0191\\C  
2  \\PC0191\\IPC$  
51 SMBu
```





# TCP端口445流量分析

## □ TCP 445端口

- Server Message Block Protocol (SMB)

## □ 提取445端口的Inbound流量

- `tcpdump -r exercise5 -nn dst host 172.16.134.191 and dst port 445 -w port445inboundtraffic.pcap`

- `tcpflow -r port445inboundtraffic.pcap`

## □ 分析来自8个不同IP的445端口流量

- 获取每个IP 445流量的所有数据包解码内容

```
for i in 129.116.182.239 195.36.247.77 209.45.125.69  
210.22.204.101 61.111.101.78 \  
> 66.139.10.15 66.8.163.125 80.181.116.202 ; do \  
> tshark -Vx -r ../pcap_file tcp and tcp.port ==445 and  
ip.addr == $i > tcp445-$i.txt ; done
```

- 从中分析SMB协议中最重要的请求命令和状态

```
grep -A 100 '\(Path:|Share:|File Name:|)' tcp445-[0-9]*.txt | grep '\(Path:|Share:|File Name:|Status:|'  
>tcp445-commands.txt  
cat tcp445-commands.txt | sort | uniq -c > tcp445-  
commands-uniq.txt
```

```
[root@localhost 445inbound]# ll -lS |  
awk -F" " '{print $9}' | cut -d '.' -f 1-4 |  
sort | uniq -c  
2 061.111.101.078  
1 066.008.163.125  
3 066.139.010.015  
1 080.181.116.202  
2 129.116.182.239  
2 195.036.247.077  
3 209.045.125.069  
4 210.022.204.101
```



# TCP端口445流量分析-攻击源发现

Attack IP (Port 445)	Path	FileName	Snort Alert	behavior	Success?
129.116.182.239	<a href="#">IPC\$</a> , C:\, C:\WINNT	<a href="#">C\$</a> , \samr, \srvsvc	portscan, IPC\$ access	查点	N
195.36.247.77	<a href="#">IPC\$</a> , <a href="#">ADMIN\$</a>	\samr	IPC\$ access, ADMIN\$ access	查点	N
209.45.125.69	<a href="#">IPC\$</a>	\samr	IPC\$ access, repeated logon failure	查点+失败的远 程口令猜测	N
210.22.204.101	<a href="#">IPC\$</a> , <a href="#">C\$</a>	\samr, <b>\svcctl</b> , <b>admdll.dll</b> , <b>raddrv.dll</b> , <b>r_server.exe</b>	IPC\$ access, repeated logon failure, portscan, C\$ access, ISAPI .ida, <b>cmd.exe access</b> , Unicode	查点+口令猜测 (成功) +exploit攻击 +shell访问	Y
61.111.101.78	<a href="#">IPC\$</a> , <a href="#">ADMIN\$</a>	\samr, <b>\svcctl</b> , <b>\psexecsvc</b> , <b>inst.exe</b> , <b>PSEXESVC.EXE</b>	IPC\$ access, ADMIN\$ access	上传 PSEXESVC, 植入并启动inst	Y
66.139.10.15	<a href="#">IPC\$</a>	\samr	IPC\$ access, repeated logon failure	查点+失败的远 程口令猜测	N
66.8.163.125	<a href="#">IPC\$</a>	\samr, <a href="#">c\$</a>	IPC\$ access, C\$ access, view source	查点	N
80.181.116.202	<a href="#">IPC\$</a>	\srvsvc	IPC\$ access	查点	N



# TCP端口445流量分析- 210.22.204.101

- 提取与该IP相关的流量
  - **tcpdump -r pcap\_file ip host 210.22.204.101 -w 210.22.204.101.pcap**
- **Wireshark分析网络流重构攻击场景**
  - **Nstreams**给出网络流时间线
  - 尝试连接**TCP 1433**端口**MS SQL Server**，未开放**RST**
  - **4个SMB 445**端口连接
    - **4473-445**: 查点**SMBR**库中的用户账号
    - **2831-445**: 建立空会话连接
    - **2927-445**: 猜测**ST-111\Administrator**口令字，空口令
    - **3945-445**: 成功通过网络身份认证，通过**\svcctl**上传**radmin**文件 (**r\_server.exe, raddrv.dll, admdll.dll**)并启动服务 **frame: 887**
    - **3月5日10:39:02 - 10:40:14**
  - 连接**4899 radmin: 10:44:24-10:47:02**
  - **11次ISAPI .ida attempt**失败: **10:39:23-10:40:47**
    - 攻击者连接期望给出**shell**的**99/6129/**端口，被**RST**，没有达到预期



# TCP端口4899流量分析

- **TCP 4899端口**
  - **Radmin**
  - 一个商业远程控制软件，被广泛破解和使用
- 提取**4899**端口的流量
  - **tcpdump -r pcap\_file -nn host 172.16.134.191 and port 4899 -w port4899traffic.pcap**
  - **tcpflow -r ../../port4899traffic.pcap**
- 两个**4899**端口连接
  - **210.022.204.101.02651 <> 172.016.134.191.04899**
  - **210.022.204.101.02773 <> 172.016.134.191.04899**
  - 二进制编码，**wirehark**没有**radmin**解码器，读不懂  
→ 你要协议破解?! orz
- **4899端口：210.022.204.101**通过上传的**radmin**对目标主机进行远程控制



# TCP端口445流量分析- 61.111.101.78

- 提取与该IP相关的流量
  - **tcpdump -r pcap\_file ip host 61.111.101.78 -w 61.111.101.78.pcap**
- **Wireshark**分析网络流重构攻击场景
  - **Nstreams**给出网络流时间线
  - **3月6日11:35:31-11:35:34 (1695-445): 查点**
  - **11:35:34-11:38:29 (1697-445):**
    - 1. 直接以空口令登录**Administrator**
    - 2. 上传**PSEXESVC**
    - 3. 调用/**svcctl** 启动**PSEXESVC**
    - 4. 上传**inst.exe**
    - 5. 启动**inst.exe**
- **Google "PSEXESVC inst.exe"**
  - **Worm.Dvldr (口令蠕虫)**
  - **Discovered by antiy lab. 2003年3月8日发现**
  - **<http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-03/0040.html>**



# 问题6-7解答

攻击端口	攻击漏洞	攻击源IP地址	攻击方式	Success?
UDP 137		多个IP	NetBIOS-NS查点	
UDP 1434	MS SQL MS02-039	多个IP55次尝试	Slammer	N
UDP 28431	N/A	62.150.170.134 232	Hack'a'Tack 木马连接尝试	N
TCP 80	大量IIS漏洞	024.197.194.106	疯狂的Web漏洞探测	N
TCP 80	ISAPI ida漏洞(MS01-033)	218.025.147.083	Code Red v2	N
TCP 80	ISAPI ida漏洞(MS01-033)	210.22.204.101	ISAPI ida攻击	N
TCP 139	空会话	多个IP	NETBIOS-SSN查点	
TCP 445	空会话+弱口令	209.45.125.69, 66.139.10.15	查点+失败的远程口令猜测	N
TCP 445	空会话+弱口令	210.22.204.101	远程口令猜测, 上传Radmin	Y
TCP 445	空会话+弱口令	61.111.101.78	Worm.Dvldr	Y
TCP 4899	N/A	210.22.204.101	Radmin远程控制	Y



## 进一步问题：哪次攻击导致蜜罐加入僵尸网络？

- 查看蜜罐主机向外发起的连接
  - **tcpdump -r pcap\_file src host 172.16.134.191 and tcp[tcpflags] == 0x2 -nn -tttt | more**
  - **2003-03-05 13:24:02-14:17:50: web访问**
    - 024.197.194.106的Web探测所引发的
  - **2003-03-06 11:36:42-12:23:18: IRC僵尸网络连接**
    - 时间上和61.111.101.78的口令蠕虫感染时间重叠
    - 口令蠕虫感染主机之后inst.exe会连接并加入僵尸网络，接受控制
  - **2003-03-06 13:22:59-13:23:08: 蜜罐主机尝试连接 199.107.7.2.31337，无应答，Back Orifice后门端口**
- 结论：
  - **3月5日10:39:02 - 10:40:14， 210.22.204.101攻陷蜜罐，上传 Radmin，并远程控制了主机**
  - **3月6日11:35:34-11:38:29， 61.111.101.78的口令蠕虫传播并感染蜜罐，并让其加入了拥有几K受控主机的僵尸网络**



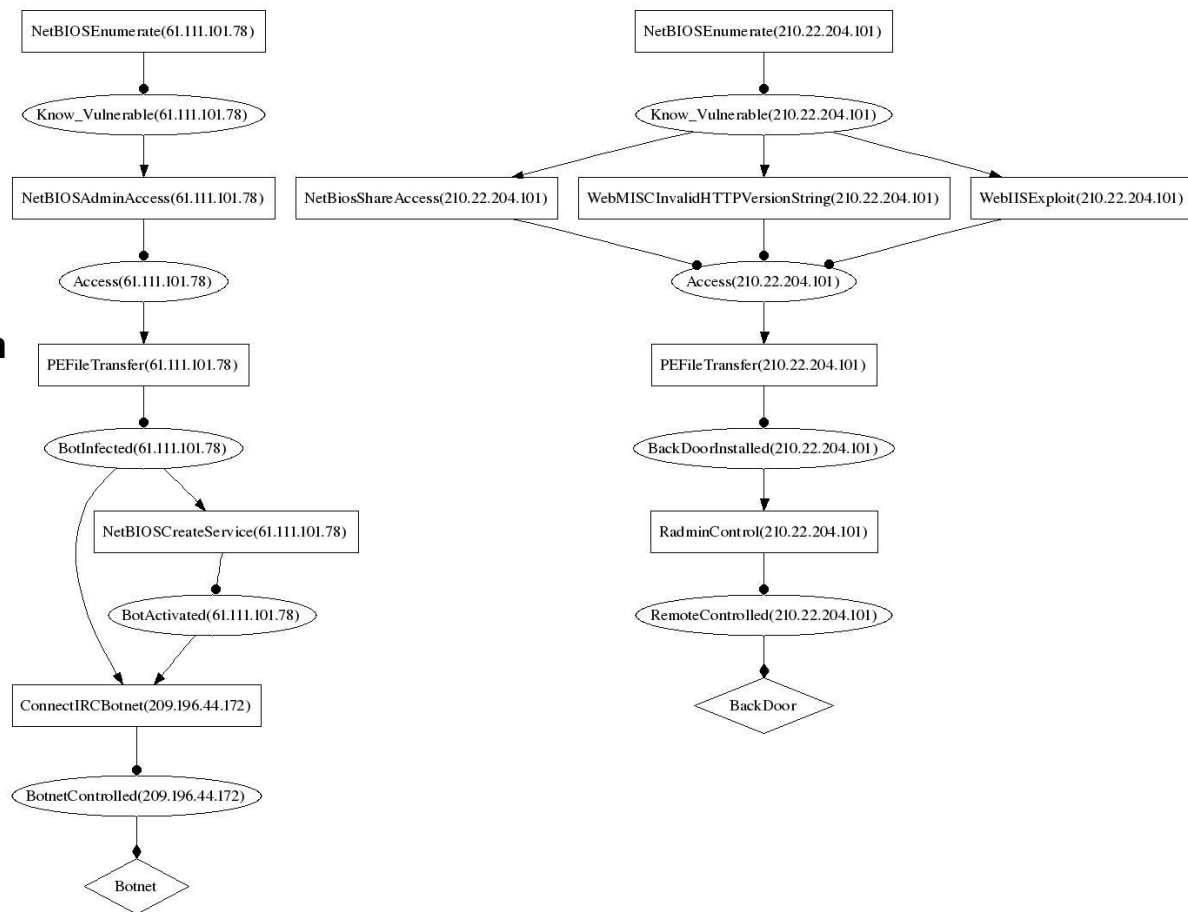
# You can play more with such a in-the-wild capture

- 提取并分析场景中知名的样本
  - **Slammer, CodeRed v2**, 口令蠕虫
  - **pehunter**: 从网络流原始日志中识别并提取**PE**可执行文件
  - 进阶课程-恶意代码基础知识与分析方法
- 分析场景中所使用的远程渗透攻击方法
  - **Slammer Exploit, ISAPI .ida exploit**, 远程口令猜测
  - **Exploit**网络报文分析, 深入理解漏洞触发和利用机理
  - **libemu**: 从网络流原始日志中识别并模拟执行**shellcode**
  - **nebula**: 从网络流会话内容中自动分析提取**snort**检测特征码
- 深入理解**NetBIOS, SMB**等常用应用层协议
- 未知应用层协议破解: **Radmin**协议破解
- 用于测试: 攻击场景自动关联方法-我的博士论文《网络入侵检测与行为关联分析技术研究》



# 博士论文和相关发表论文

- 博士论文, **2006.**
- 基于扩展目标规划图的网络攻击规划识别算法, 计算机学报.
- **Towards High Level Attack Scenario Graph through Honeynet Data Correlation Analysis, West Point Workshop, 2006.**
- 在**NIDS**报警记录基础上基于攻击知识库进行攻击场景重构



# Thanks

---

诸葛建伟

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