# 网络攻防技术与实践课程

# 课程5. TCP/IP网络协议攻击

**诸葛建伟**

**zhugejw@gmail.com**

# 内容

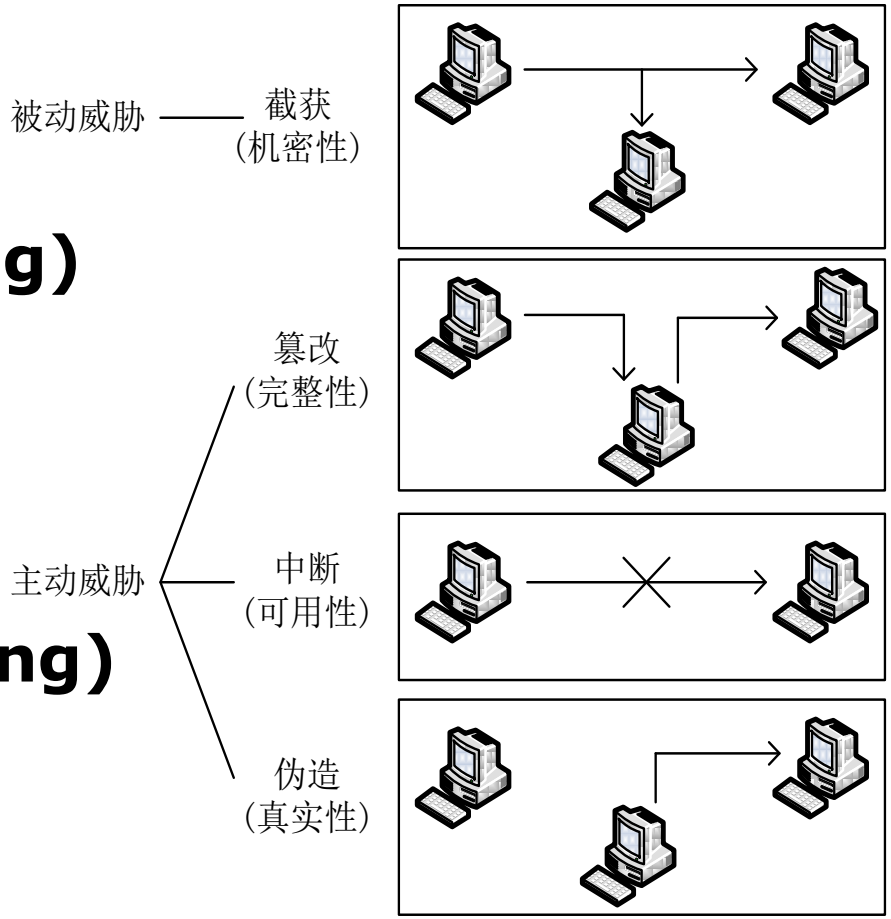
1. TCP/IP网络协议栈攻击概述
2. 网络层协议攻击
3. 传输层协议攻击
4. TCP/IP网络协议栈攻击防范措施
5. 作业5－TCP/IP协议栈重点协议的攻击实验

# 网络安全属性

- 网络安全**CIA**属性
  - **机密性(Confidentiality)**
  - **完整性(Integrity)**
  - **可用性(Availability)**
- 其他两个补充属性
  - **真实性(Authentication)**
  - **不可抵赖性(Non-Repudiation) – 可审查性(Accountability)**

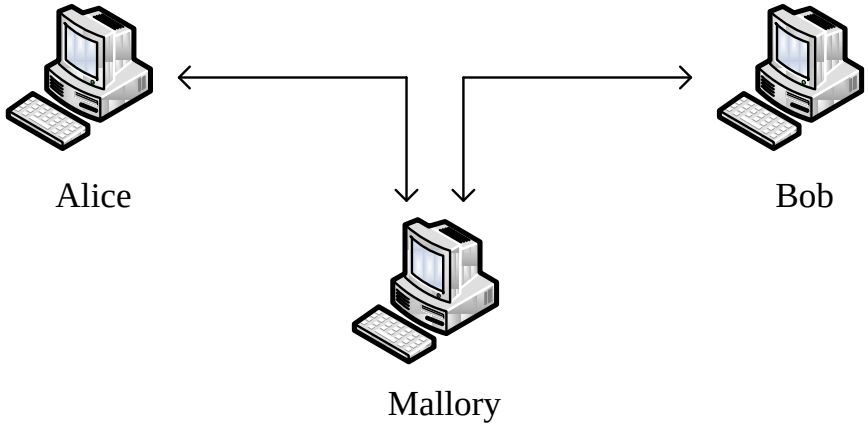
# 网络攻击基本模式

- 截获
  - 嗅探(sniffing)
  - 监听(eavesdropping)
- 中断
  - 拒绝服务(DoSing)
- 篡改
  - 数据包篡改(tampering)
- 伪造
  - 欺骗(Spoofing)



# 中间人攻击(MITM攻击)

- 通信双方
  - **Alice & Bob**
- 中间人
  - **Mallory**
  - 与通信双方建立起各自独立的会话连接
  - 对双方进行身份欺骗
  - 进行消息的双向转发
  - 必要前提：拦截通信双方的全部通信(截获)、转发篡改消息(篡改)、双方身份欺骗(伪造)
  - 现实世界中的中间人攻击 – 国际象棋欺骗术

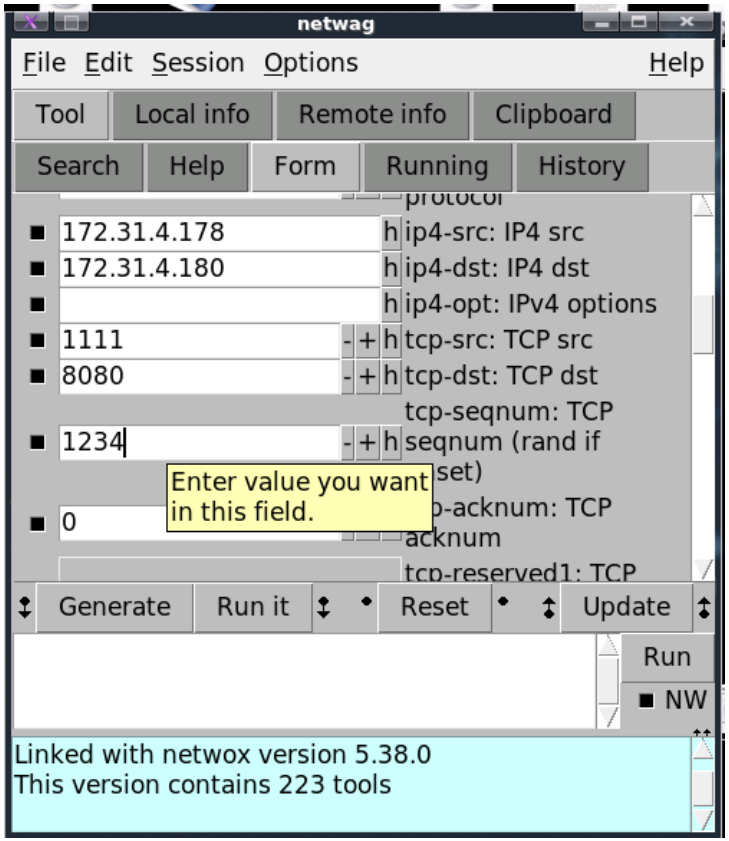


# TCP/IP网络协议栈安全缺陷与攻击技术

| TCP/IP 协议栈层次 | 网络协议 | 存在安全缺陷 | 对应攻击技术 | 破坏安全属性 |
|---|---|---|---|---|
| 网络接口层 | 以太网协议 | 共享传输媒介并明文传输 | 网络嗅探与协议分析 | 机密性 |
| | 以太网协议 | 缺乏MAC身份认证机制 | MAC欺骗攻击 | 真实性 |
| | PPP协议 | 明文传输 | 网络嗅探与协议分析 | 机密性 |
| 互联层 | IPv4 | 缺乏IP地址身份认证机制 | IP地址欺骗 | 真实性 |
| | | 处理IP分片时的逻辑错误 | IP分片攻击 | 可用性 |
| | ICMP | ICMP路由重定向缺乏身份认证 | ICMP路由重定向 | 完整性, 真实性 |
| | | 广播地址对Ping的放大器效应 | Ping Flood, Smurf | 可用性 |
| | ARP | 采用广播问询且无验证机制 | ARP欺骗 | 真实性 |
| | BGP等 | 缺乏较强的身份认证机制 | 路由欺骗攻击 | 完整性, 真实性 |
| 传输层 | TCP | TCP三次握手存在连接队列瓶颈 | TCP SYN Flood | 可用性 |
| | | TCP会话对身份认证不够安全 | TCP RST攻击 | 真实性, 可用性 |
| | | TCP会话对身份认证不够安全 | TCP会话劫持 | 真实性, 可用性 |
| | UDP | N/A | UDP Flood | 可用性 |
| 应用层 | DNS | DNS验证机制不够安全 | DNS欺骗 | 完整性, 真实性 |
| | SMB | SMB协议的NTLM认证机制存在安全缺陷 | SMB中间人攻击 | 真实性, 可用性 |
| | HTTP | URL明文, 缺乏完整性保护, 编码滥用等 | 钓鱼 | 完整性, 真实性 |
| | | 内嵌链接滥用 | 网页木马攻击 | 完整性 |

# 原始报文伪造技术及工具

- 原始报文伪造技术
  - 伪造出特制的网络数据报文并发送
  - 原始套接字(**Raw Socket**)
- **Netwox/Netwag***
  - 超过**200**个不同功能的网络报文生成与发送工具
  - **#netwox number [parameters ... ]**



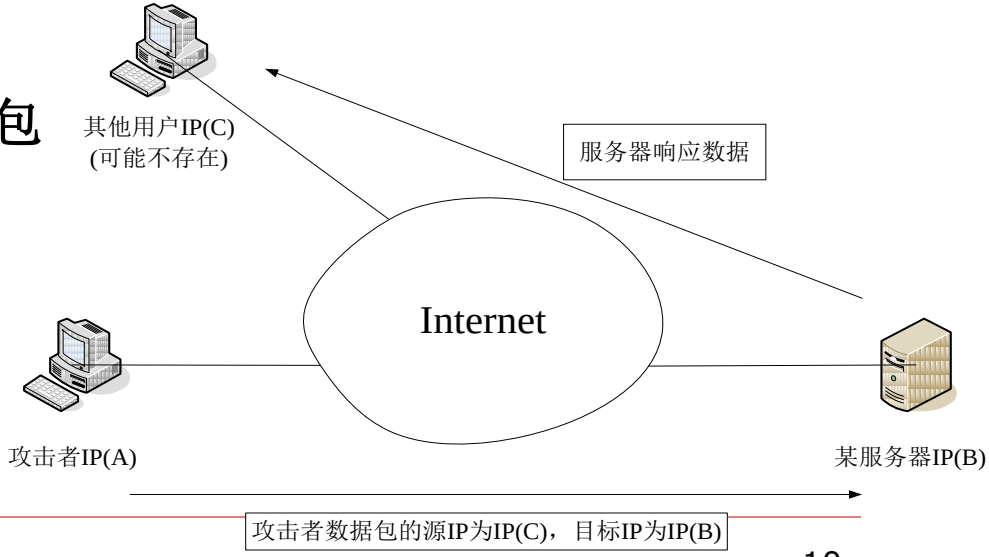
# Netwox工具使用演示

# 内容

1. TCP/IP网络协议栈攻击概述
2. 网络层协议攻击
3. 传输层协议攻击
4. TCP/IP网络协议栈攻击防范措施
5. 作业5－TCP/IP协议栈重点协议的攻击实验

# IP源地址欺骗

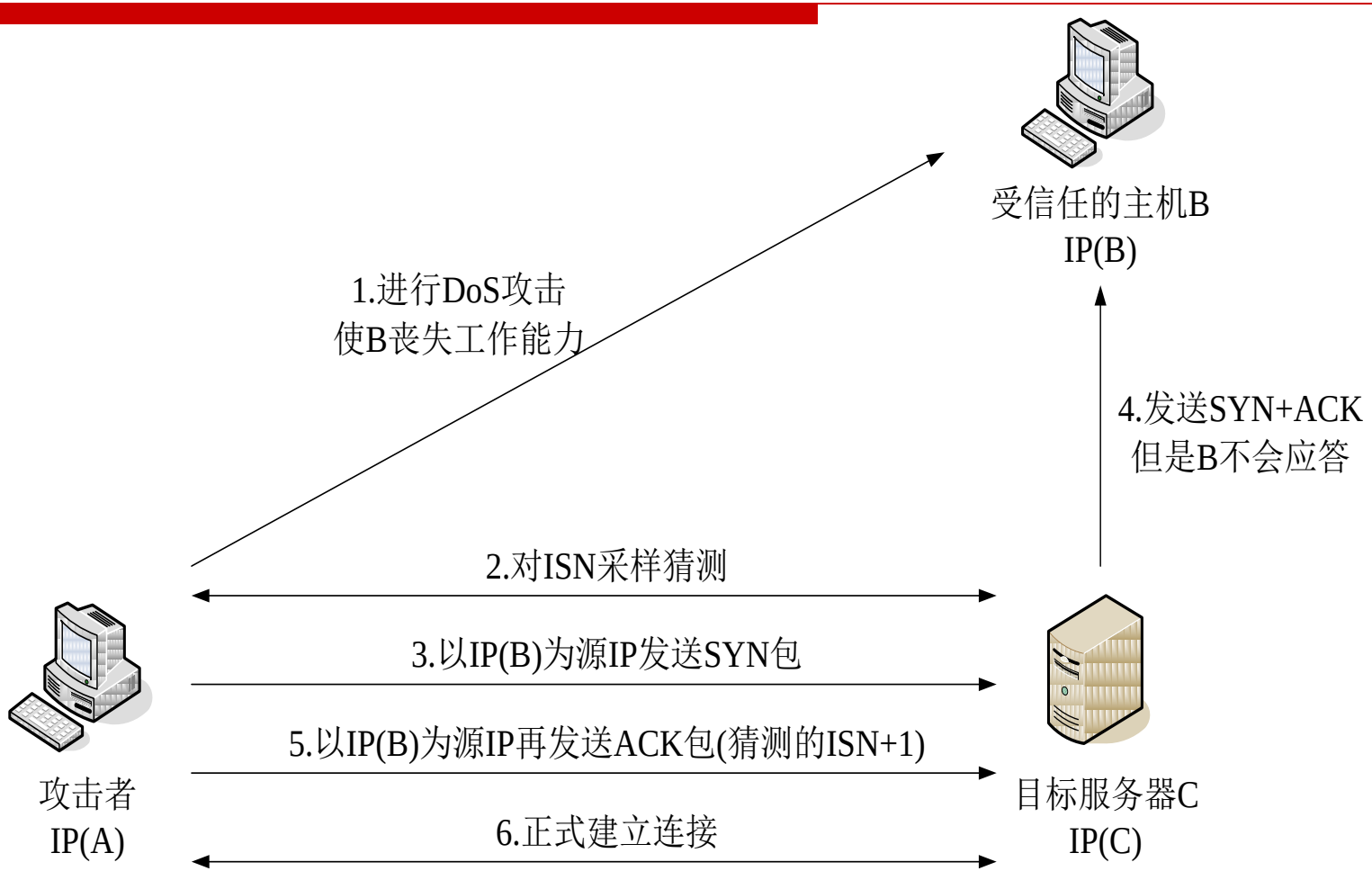
- **IP源地址欺骗**
  - 伪造具有虚假源地址的**IP**数据包进行发送
  - 目的：隐藏攻击者身份、假冒其他计算机
- **IP源地址欺骗原理**
  - 路由转发只是用目标**IP**地址，不对源做验证
  - 现实世界中的平信
  - 通常情况：无法获得响应包



# IP源地址欺骗 – 假冒IP攻击

- 可以嗅探响应包的环境
  - 同一局域网
  - ARP欺骗、重定向攻击劫持响应包
- 盲攻击(blind attack)
  - Robert T. Morris在1985年提出
  - Kevin Mitinick在1995年仍使用
  - 通过猜测TCP三次握手中所需的信息，假冒IP建立起TCP连接

# 盲攻击过程



# IP源地址欺骗技术的应用场景

- 普遍应用场景
  - 拒绝服务攻击：无需或不期望响应包，节省带宽，隐藏攻击源
  - 网络扫描(nmap -D)：将真正扫描源隐藏于一些欺骗的源IP地址中
- 假冒IP攻击场景
  - 对付基于IP地址的身份认证机制
    - 类Unix平台上的主机信任关系
    - 防火墙或服务器中配置的特定IP访问许可
  - 远程主机IP欺骗-盲攻击，较难成功

# 利用Netwox进行IP源地址欺骗

```
################## help for tool number 41 ##################
Title: Spoof Ip4Icmp4 packet
+--------------------------------------------------------------------+
| This tool sends a fake packet on the network.                      |
+--------------------------------------------------------------------+
Synonyms: hping, send
Usage: netwox 41 [-c uint32] [-e uint32] [-f|+f] [-g|+g] [-h|+h] [-i uint32] [-j
 uint32] [-k uint32] [-l ip] [-m ip] [-n ip4opts] [-o uint32] [-p uint32] [-a sp
oofip] [-r uint32] [-s uint32] [-t uint32] [-u uint32]
################## running tool number 41 ##################
Enter optional tool parameters and press Return key.
netwox 41 -j 128 -k 1 -l 172.31.4.180 -m 172.31.4.200 -o 8
IP_____________________________________________________________.
|version|  ihl  |      tos      |            totlen             |
|___4___|___5___|____0x00=0_____|_____________0x001C=28_____________|
|            id               |r|D|M|       offsetfrag            |
|__________0x40DF=16607__________|0|0|0|________0x0000=0_________|
|      ttl      |   protocol    |          checksum             |
|___0x80=128____|____0x01=1_____|_____________0x1848_____________|
|                         source                                 |
|_____________________________172.31.4.180_____________________________|
|                       destination                              |
|_____________________________172.31.4.200_____________________________|
ICMP4_echo request_____________________________________________________.
|     type      |     code      |          checksum             |
|____0x08=8_____|____0x00=0_____|__________0xE5AB=58795__________|
|            id               |            seqnum             |
|__________0x99E9=39401__________|__________0x786A=30826__________|
| data:                                                          |
|________________________________________________________________|
```

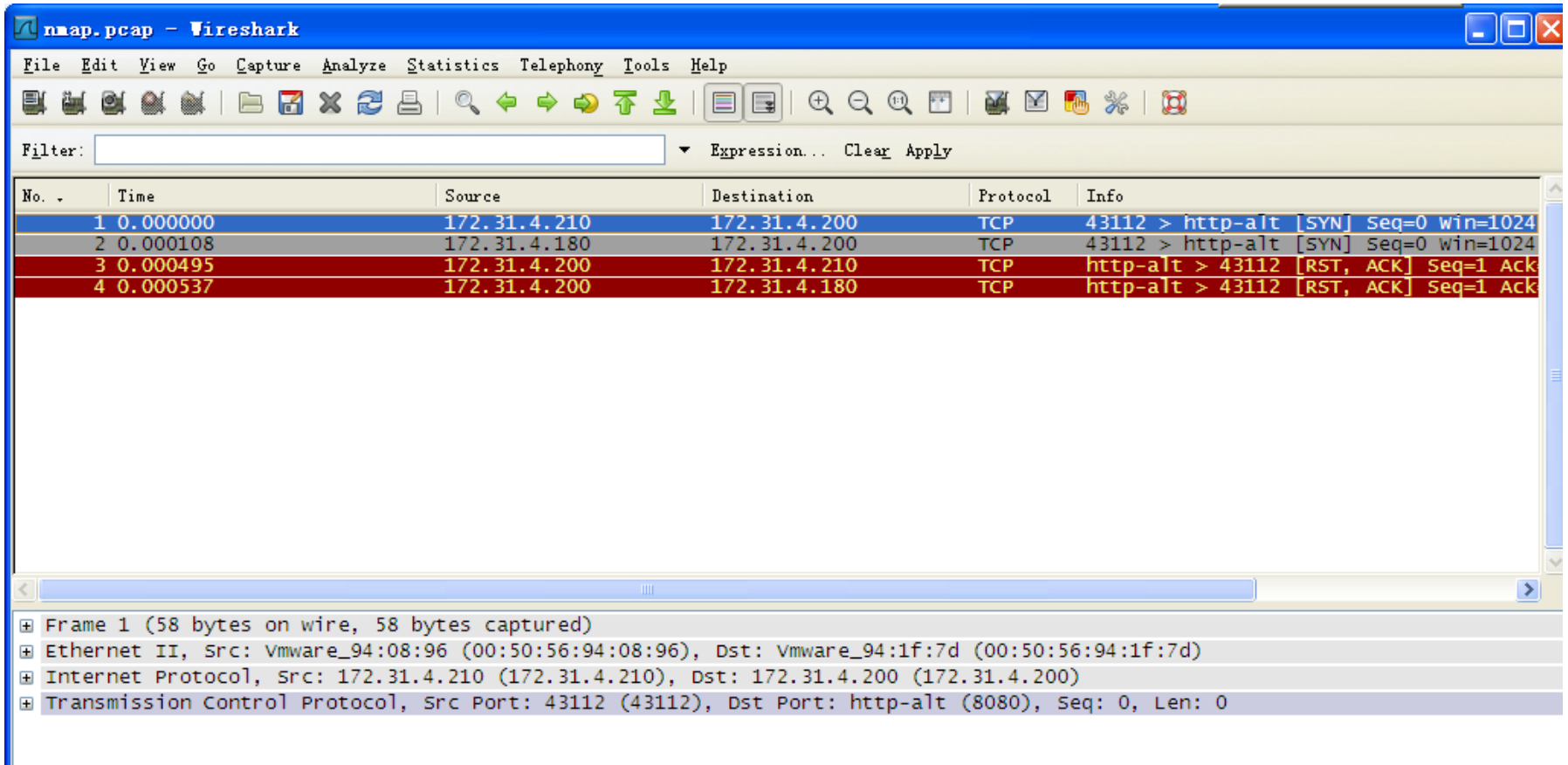
真实源IP：172.31.4.210

↓

欺骗源IP：172.31.4.180

# Nmap进行源IP地址欺骗扫描

- nmap -sS -p 8080 172.31.4.200 -D 172.31.4.180



# IP源地址欺骗的防范措施

- 使用随机化的初始序列号 →避免远程的盲攻击
- 使用网络层安全传输协议如**IPsec**
  - 避免泄露高层协议可供利用的信息及传输内容
- 避免采用基于**IP**地址的信任策略
  - 以基于加密算法的用户身份认证机制来替代
- 在路由器和网关上实施包检查和过滤
  - 入站过滤机制**(ingress filtering)**
  - 出站过滤机制**(egress filtering)**

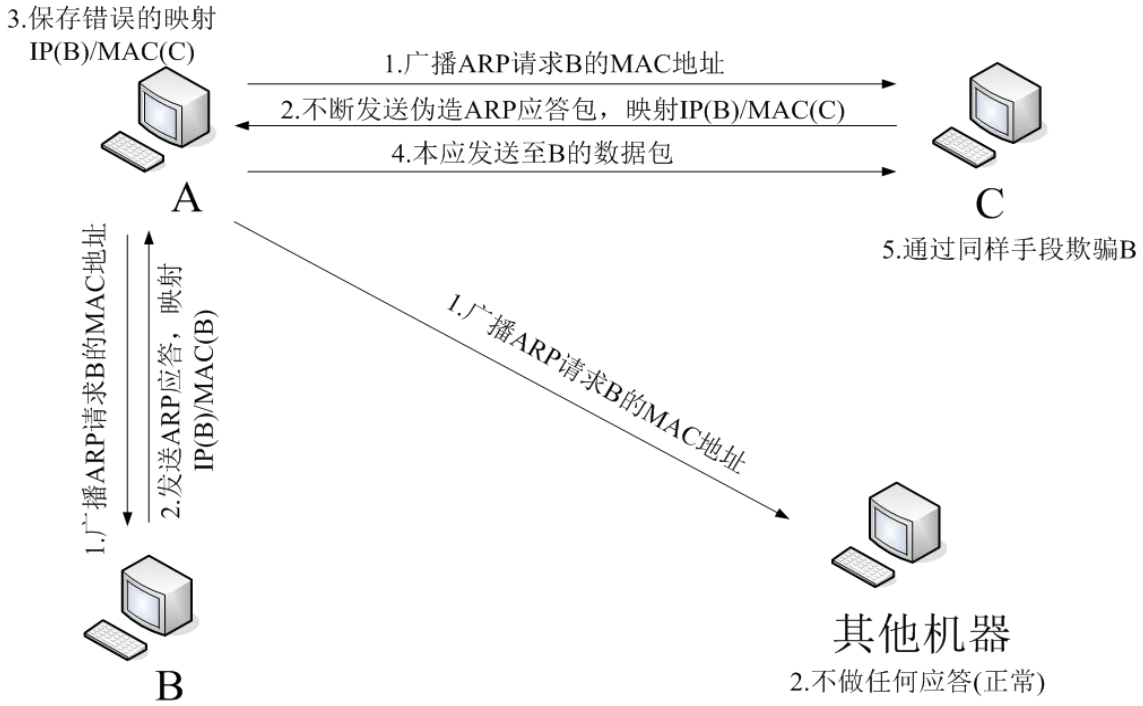
# ARP欺骗(ARP Spoofing)

- **ARP协议工作原理**
  - 将网络主机的**IP**地址解析成其**MAC**地址
  - ① 每台主机设备上都拥有一个**ARP**缓存**(ARP Cache)**
  - ② 检查自己的**ARP**缓存，有，直接映射，无，广播**ARP**请求包
  - ③ 检查数据包中的目标**IP**地址是否与自己的**IP**地址一致，如一致，发送**ARP**响应，告知**MAC**地址
  - ④ 源节点在收到这个**ARP**响应数据包后，将得到的目标主机**IP**地址和**MAC**地址对映射表项添加到自己的**ARP**缓存中


- **ARP欺骗：发送伪造ARP消息，对特定IP所对应的MAC地址进行假冒欺骗，从而达到恶意目的**

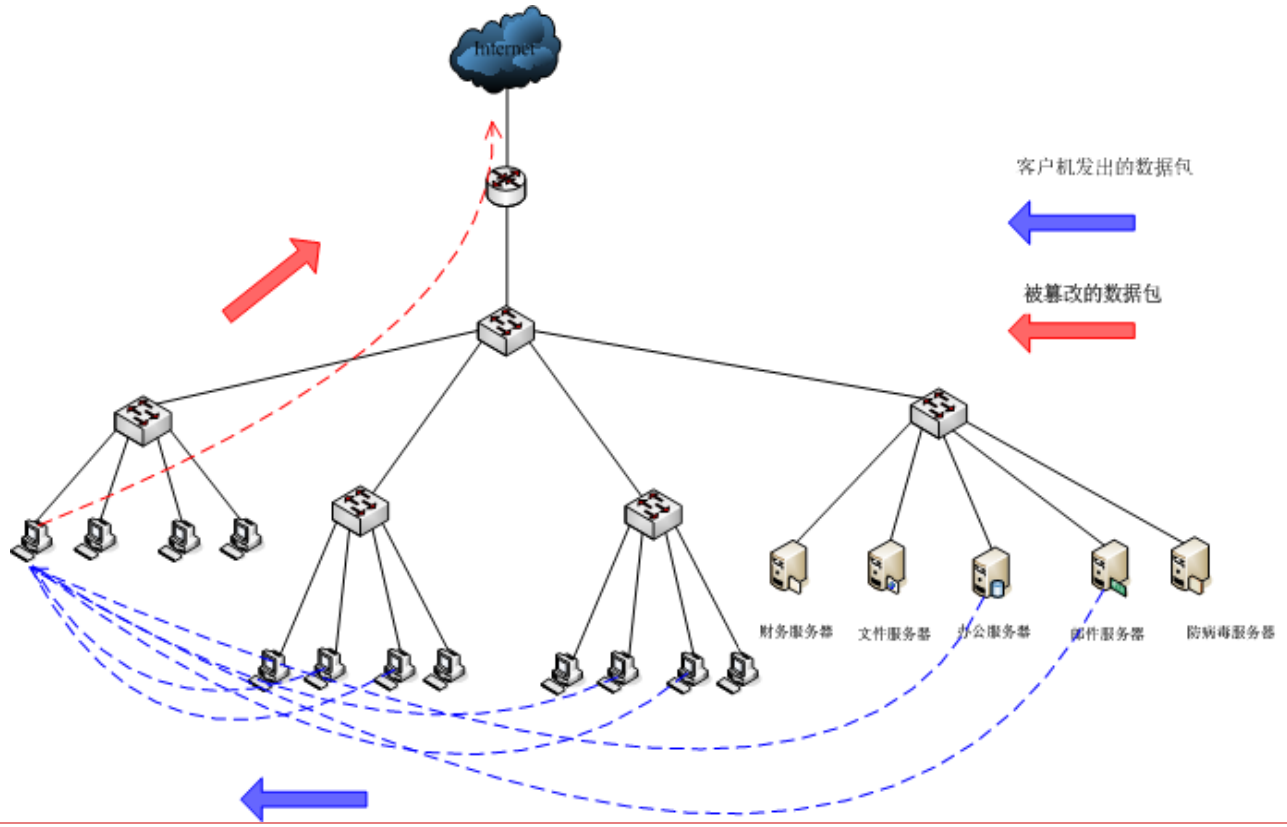
# ARP欺骗攻击技术原理

- “郭靖&黄蓉——黄蓉的诡计1”
- “Offer盗窃假冒门”



# 网关ARP欺骗

- “黄蓉的诡计2”



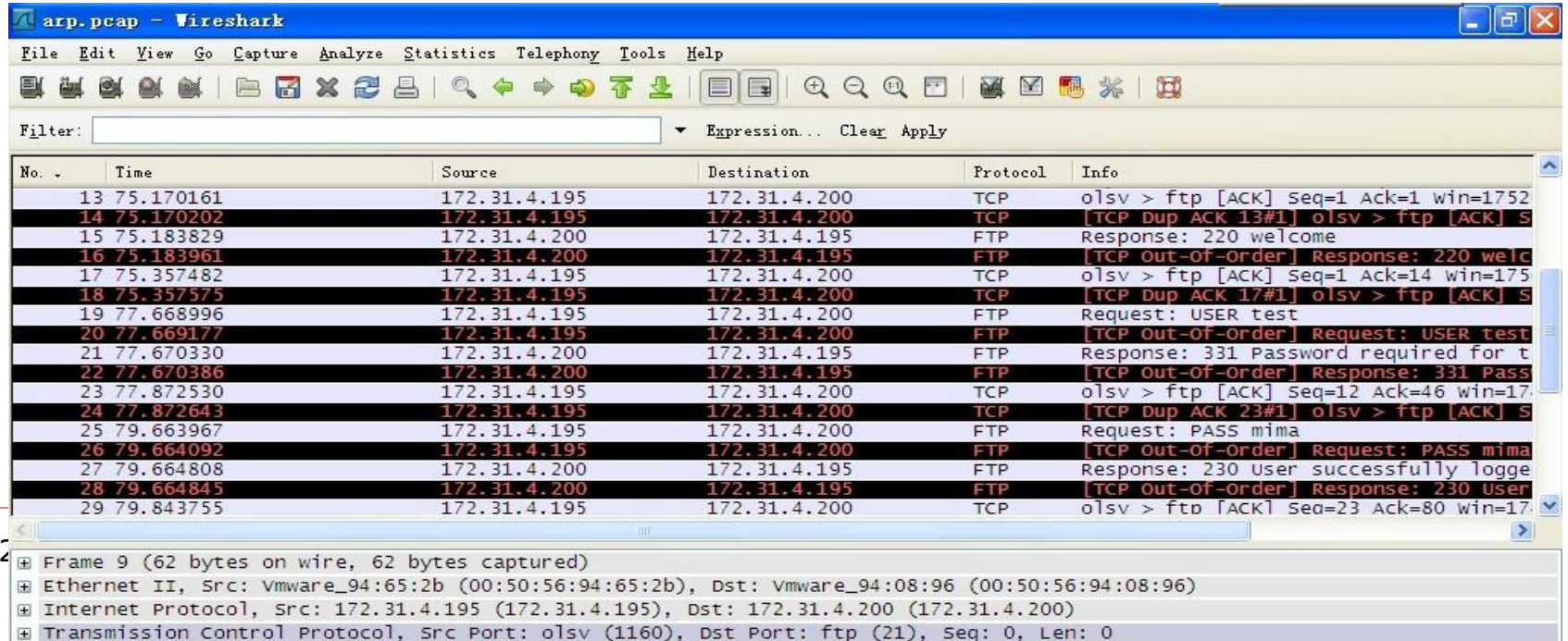
# ARP欺骗技术的应用场景

- 利用ARP欺骗进行交换网络中的嗅探
- ARP欺骗构造中间人攻击，从而实施TCP会话劫持
- ARP病毒
- ARP欺骗挂马

# 利用Netwox进行ARP欺骗演示

| 主机 | 角色 | IP地址 | MAC地址 |
|---|---|---|---|
| A | 通信方 | 172.31.4.200 | 00:50:56:94:1F:7D |
| B | 通信方 | 172.31.4.195 | 00:50:56:94:65:2B |
| C | 攻击机 | 172.31.4.210 | 00:50:56:94:08:96 |

netwox 33 -b 00:50:56:94:1F:7D -g 172.31.4.195 -h 00:50:56:94:1F:7D -i 172.31.4.200

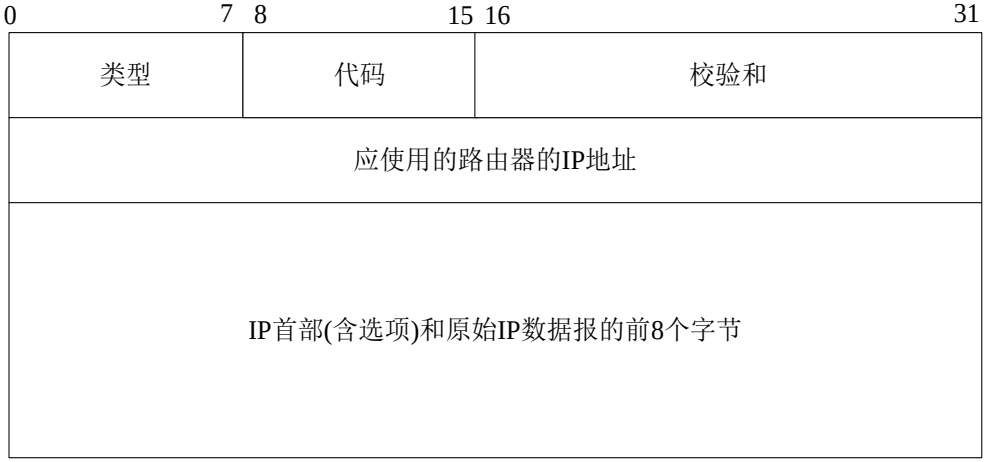


# ARP欺骗攻击防范措施

- 静态绑定关键主机的IP地址与MAC地址映射关系
  - 网关/关键服务器
  - "arp -s IP地址 MAC地址 类型"
- 使用相应的ARP防范工具
  - ARP防火墙
- 使用VLAN虚拟子网细分网络拓扑
- 加密传输数据以降低ARP欺骗攻击的危害后果

# ICMP路由重定向攻击

- **ICMP路由重定向攻击**
  - 伪装成路由器发送虚假的**ICMP**路由路径控制报文
  - 使受害主机选择攻击者指定的路由路径
  - 攻击目的：嗅探或假冒攻击
- **技术原理**
  - 路由器告知主机：“应该使用的路由器**IP**地址”

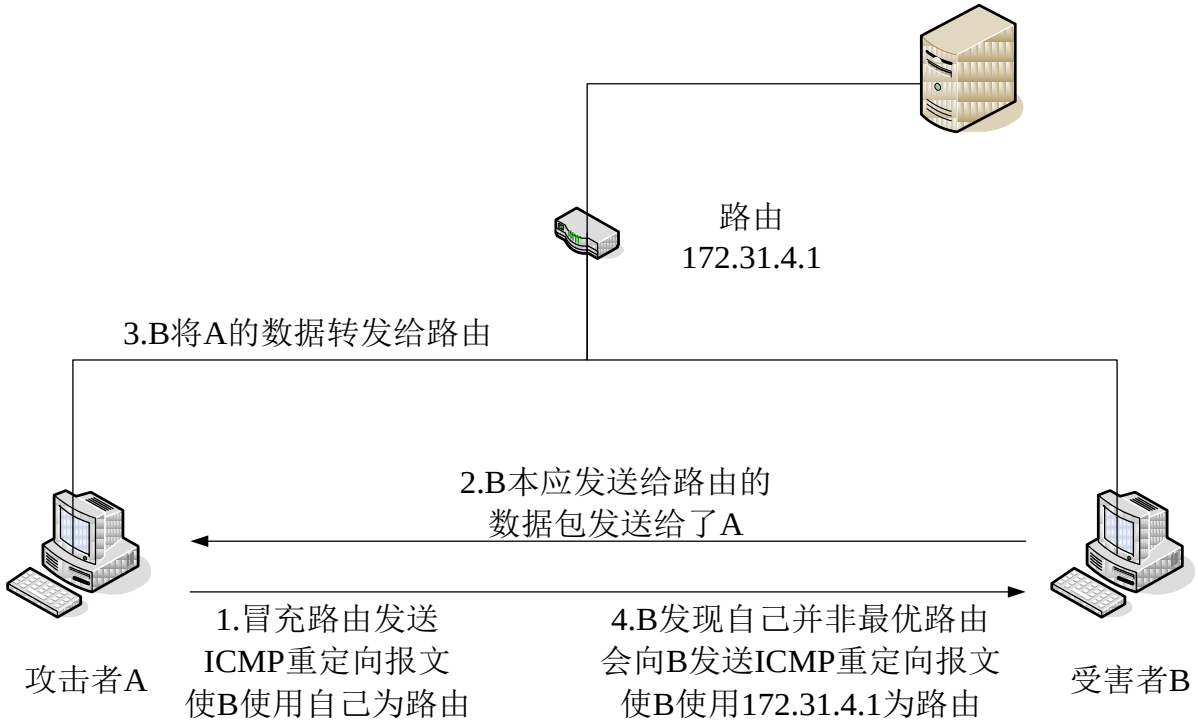


# ICMP路由重定向攻击技术

- 攻击节点冒充网关IP，向被攻击节点发送ICMP重定向报文，并将指定的新路由器IP地址设置为攻击节点
- 被攻击节点接受报文，选择攻击节点作为其新路由器(即网关)
- 攻击节点可以开启路由转发，实施中间人攻击
- “谎言还是真话”？

# 利用Netwox进行ICMP路由重定向攻击 – 演示

- **netwox 86 -f "host 172.31.4.200" -g 172.31.4.210 -i 172.31.4.1**



# 实施重定向攻击前后受害主机路由表的对比情况

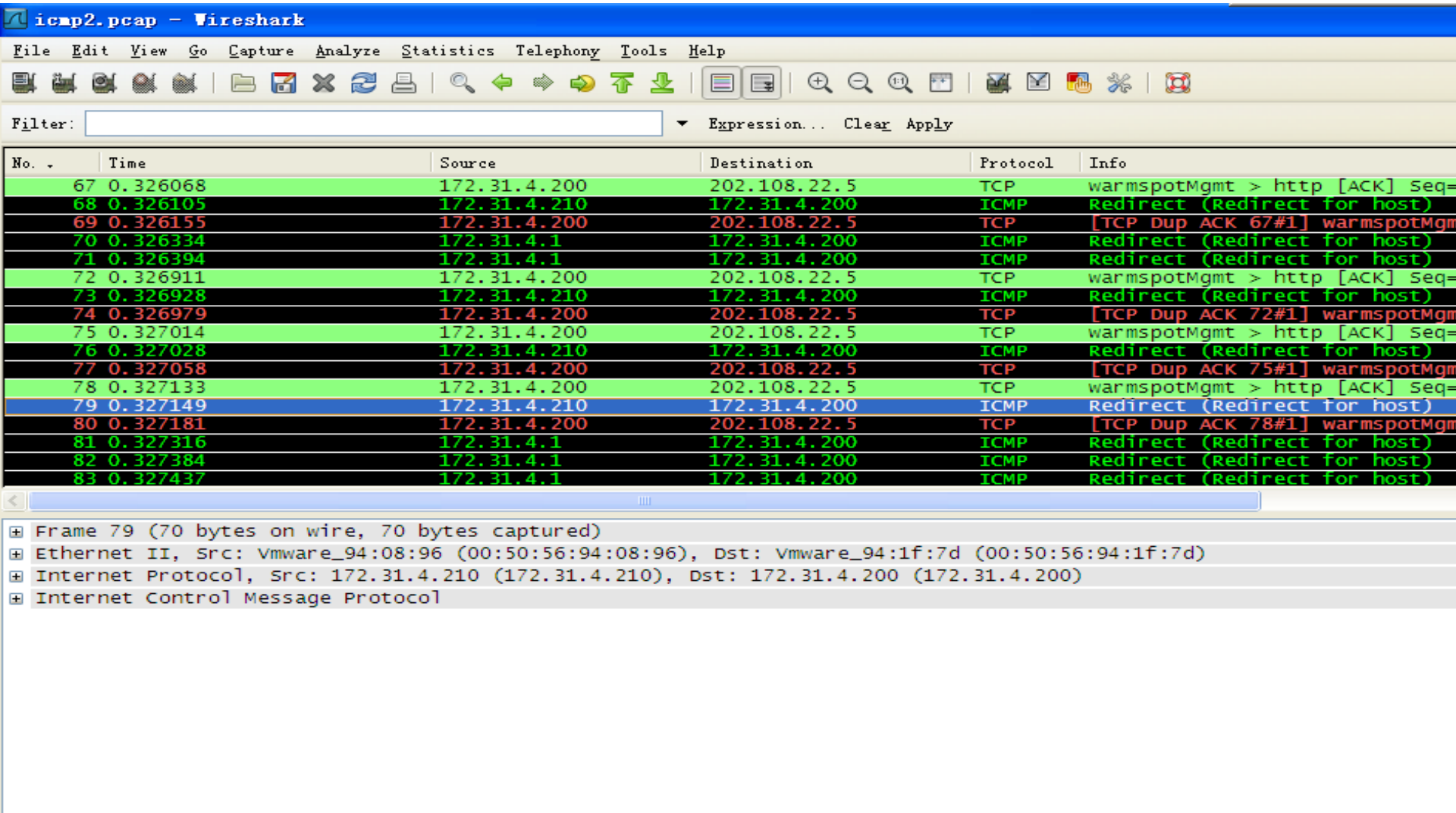
**重定向攻击前的受害主机路由表**

```
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.31.4.1    172.31.4.200      30
        127.0.0.0        255.0.0.0        127.0.0.1      127.0.0.1       1
      172.31.4.0    255.255.255.0    172.31.4.200    172.31.4.200      30
    172.31.4.200  255.255.255.255        127.0.0.1      127.0.0.1      30
  172.31.255.255  255.255.255.255    172.31.4.200    172.31.4.200      30
        224.0.0.0        240.0.0.0    172.31.4.200    172.31.4.200      30
  255.255.255.255  255.255.255.255    172.31.4.200    172.31.4.200       1
Default Gateway:        172.31.4.1
===========================================================================
Persistent Routes:
  None
```

**重定向攻击后的受害主机路由表**

```
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.31.4.1    172.31.4.200      30
        127.0.0.0        255.0.0.0        127.0.0.1      127.0.0.1       1
      172.31.4.0    255.255.255.0    172.31.4.200    172.31.4.200      30
    172.31.4.200  255.255.255.255        127.0.0.1      127.0.0.1      30
  172.31.255.255  255.255.255.255    172.31.4.200    172.31.4.200      30
    202.106.0.20  255.255.255.255    172.31.4.210    172.31.4.200       1
    202.108.22.5  255.255.255.255    172.31.4.210    172.31.4.200       1
        224.0.0.0        240.0.0.0    172.31.4.200    172.31.4.200      30
  255.255.255.255  255.255.255.255    172.31.4.200    172.31.4.200       1
Default Gateway:        172.31.4.1
===========================================================================
Persistent Routes:
  None
```

# Wireshark分析ICMP重定向攻击过程



# ICMP路由重定向攻击防范

- 根据类型过滤一些ICMP数据包
- 设置防火墙过滤
- 对于ICMP重定向报文判断是不是来自本地路由器

# 内容

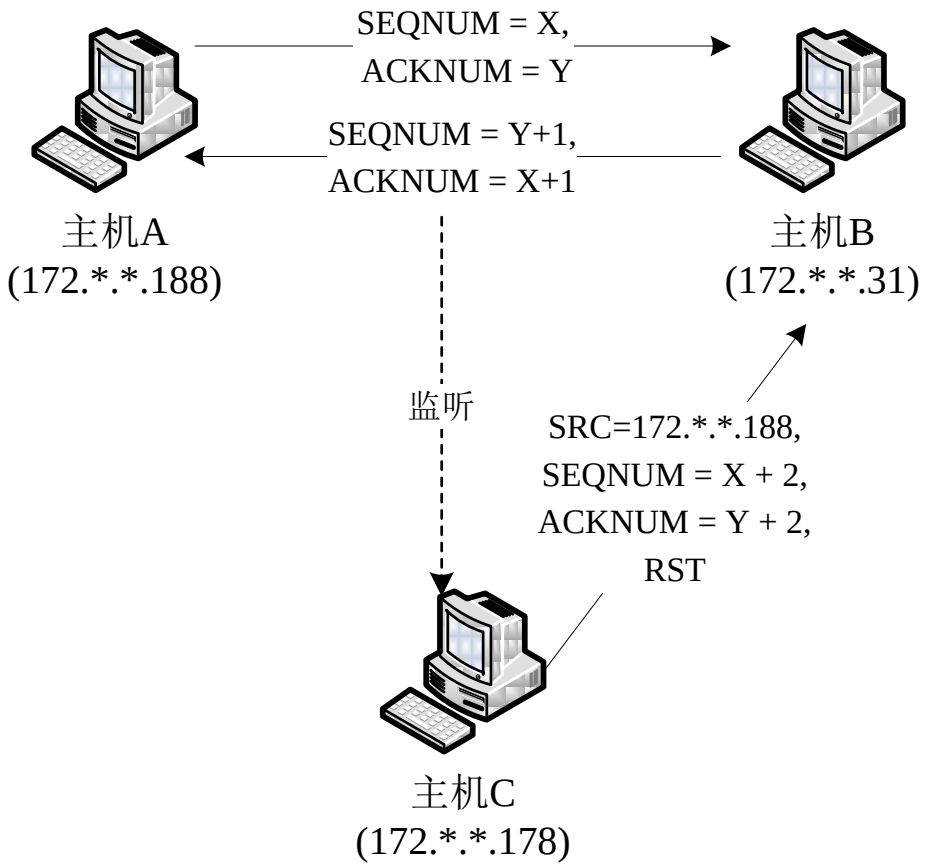
1. TCP/IP网络协议栈攻击概述
2. 网络层协议攻击
3. 传输层协议攻击
4. TCP/IP网络协议栈攻击防范措施
5. 作业5－TCP/IP协议栈重点协议的攻击实验

# TCP RST攻击

- 中断攻击
- 伪造TCP重置报文攻击(spoofed TCP reset packet)
  - TCP重置报文将直接关闭掉一个TCP会话连接
  - 限制条件：通讯目标方接受TCP包
    - 通讯源IP地址及端口号一致
    - 序列号(Seq)落入TCP窗口之内
  - 嗅探监视通信双方的TCP连接，获得源、目标IP地址及端口
  - 结合IP源地址欺骗技术伪装成通信一方，发送TCP重置报文给通信另一方
- 应用场景：恶意拒绝服务攻击、重置入侵连接、GFW
  - GFW: “net::ERR_CONNECTION_RESET”

# TCP RST攻击演示

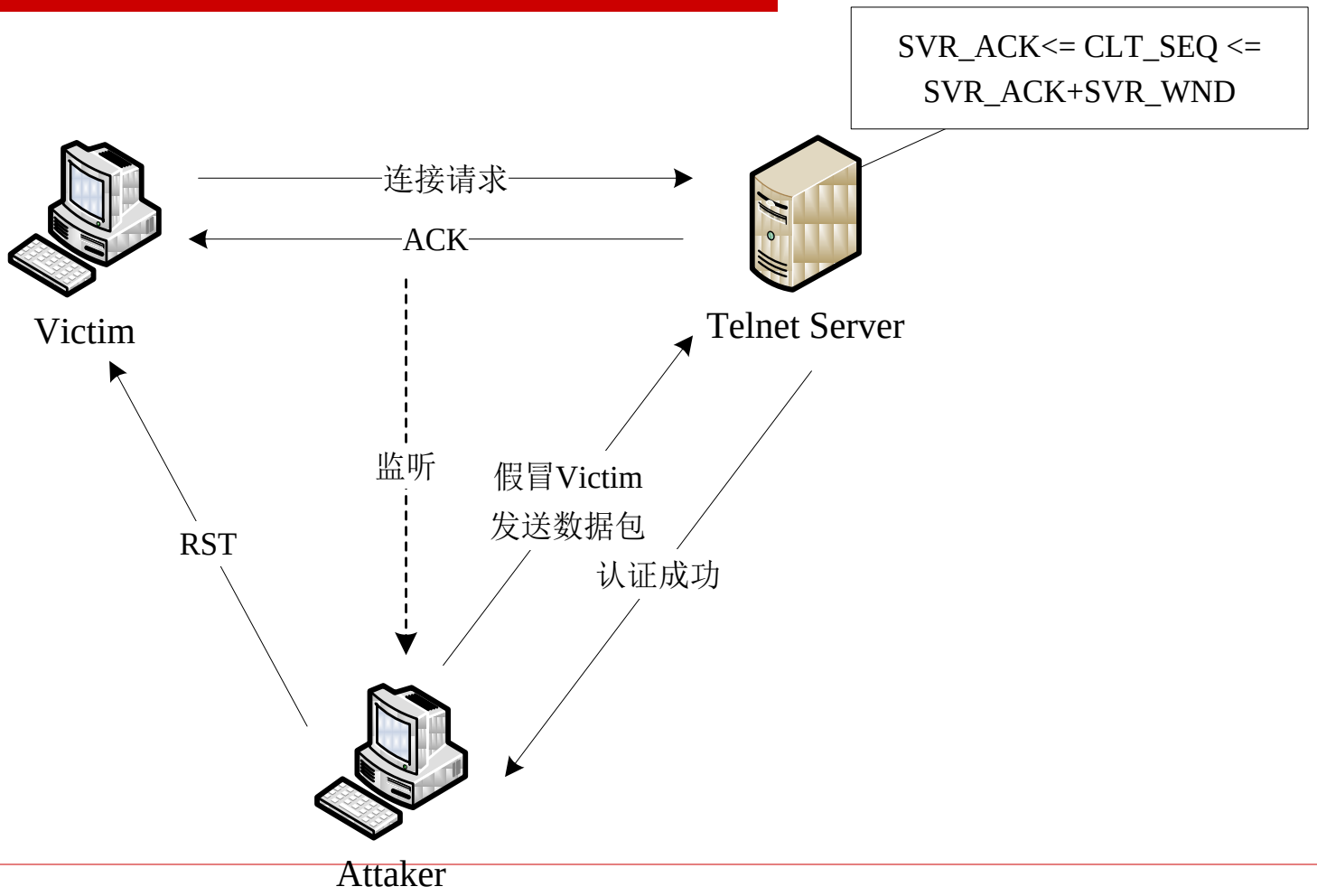
- **Netwox #78 tool**
  - **Reset every TCP packet**
  - **Usage: netwox 78 [-d device] [-f filter] [-s spoofip] [-i ips]**
  - **netwox 78 -i "172.*.*.188"**



# TCP会话劫持

- 结合嗅探、欺骗技术
- 中间人攻击：注射额外信息，暗中改变通信
- 计算出正确的**seq ackseq**即可
- **TCP**会话攻击工具
  - **Juggernaut、Hunt、TTY watcher、IP watcher**

# TCP会话劫持攻击过程



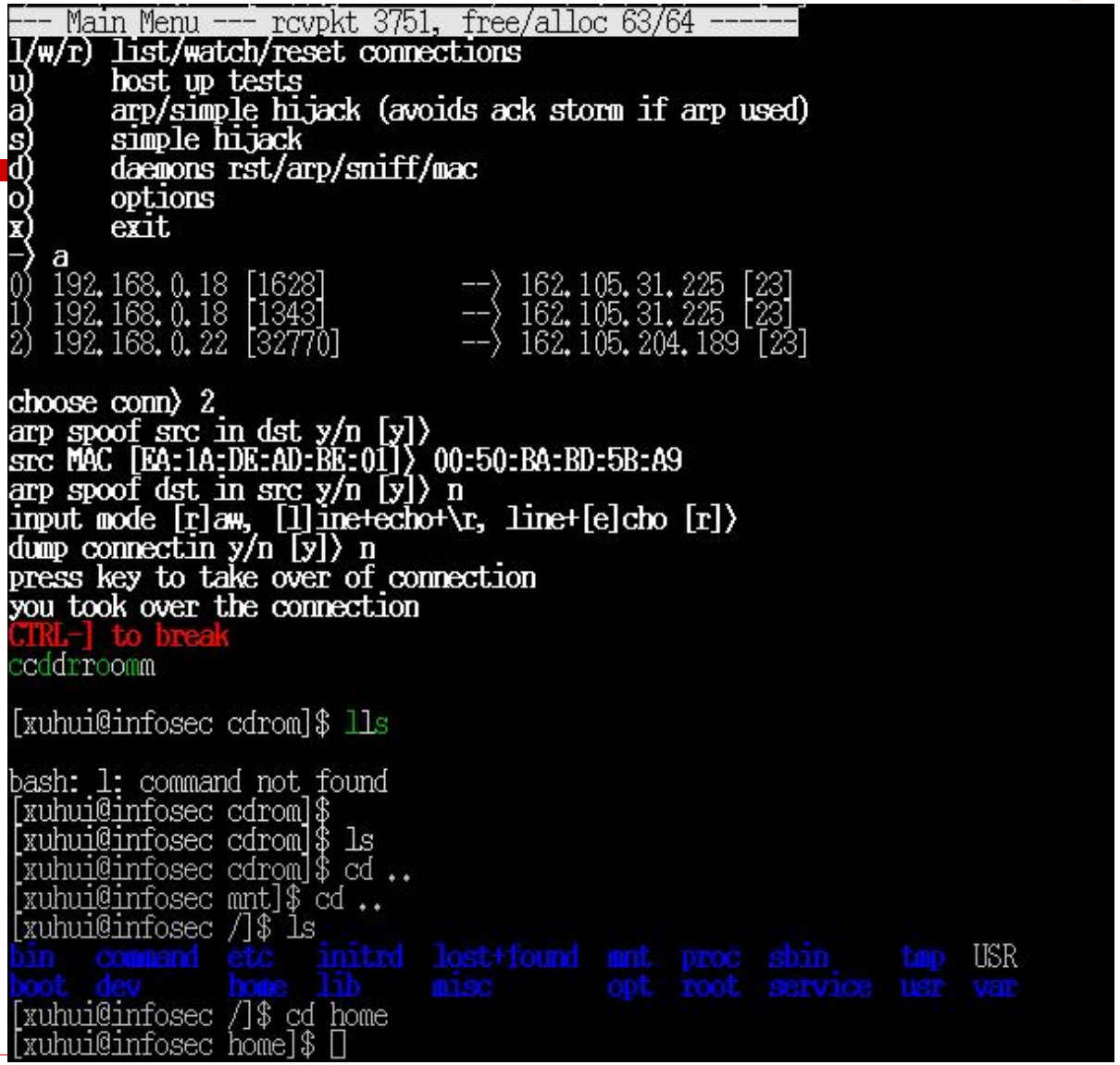
# Hunt工具介绍

- 源码开放的自由软件，可运行在**Linux**平台上
- 功能特点
  - 监听当前网络上的会话
  - 重置会话**(reset a session)**
  - 劫持会话
    - 在劫持之后，使连接继续同步
  - 确定哪些主机在线
  - 四个守护进程
    - 自动**reset**
    - **Arp**欺骗包的转发
    - 收集**MAC**地址
    - 具有搜索功能的**sniffer**

# Hunt主菜单

l/w/r) list/watch/reset connections
u)  host up tests
a)  arp/simple hijack (avoids ack storm if arp used)
s)  simple hijack
d)  daemons rst/arp/sniff/mac
o)  options
x)  exit
->

# 用hunt接管会话


--- Main Menu --- rcvpkt 3751, free/alloc 63/64 ------
l/w/r) list/watch/reset connections
u) host up tests
a) arp/simple hijack (avoids ack storm if arp used)
s) simple hijack
d) daemons rst/arp/sniff/mac
o) options
x) exit
-> a
0) 192.168.0.18 [1628] --> 162.105.31.225 [23]
1) 192.168.0.18 [1343] --> 162.105.31.225 [23]
2) 192.168.0.22 [32770] --> 162.105.204.189 [23]
choose conn> 2
arp spoof src in dst y/n [y]>
src MAC [EA:1A:DE:AD:BE:01]> 00:50:BA:BD:5B:A9
arp spoof dst in src y/n [y]> n
input mode [r]aw, [l]ine+echo+\r, line+[e]cho [r]>
dump connectin y/n [y]> n
press key to take over of connection
you took over the connection
CTRL-] to break
ccddrroomm
[xuhui@infosec cdrom]$ lls
bash: lls: command not found
[xuhui@infosec cdrom]$
[xuhui@infosec cdrom]$ ls
[xuhui@infosec cdrom]$ cd ..
[xuhui@infosec mnt]$ cd ..
[xuhui@infosec /]$ ls
bin command etc initrd lost+found mnt proc sbin tmp USR
boot dev home lib misc opt root service usr var
[xuhui@infosec /]$ cd home
[xuhui@infosec home]$

# 用hunt接管并重置会话

```
d)      daemons rst/arp/sniff/mac
o)      options
x)      exit
-> a
0) 192.168.0.18 [1628]          --> 162.105.31.225 [23]
1) 192.168.0.18 [1343]          --> 162.105.31.225 [23]
2) 192.168.0.22 [32770]         --> 162.105.204.189 [23]

choose conn> 2
arp spoof src in dst y/n [y]>
src MAC [EA:1A:DE:AD:BE:01]> 00:50:BA:BD:5B:A9
arp spoof dst in src y/n [y]> n
input mode [r]aw, [l]ine+echo+\r, line+[e]cho [r]>
dump connectin y/n [y]> n
press key to take over of connection
you took over the connection
CTRL-] to break
ccddrroomm

[xuhui@infosec cdrom]$ lls

bash: l: command not found
[xuhui@infosec cdrom]$
[xuhui@infosec cdrom]$ ls
[xuhui@infosec cdrom]$ cd ..
[xuhui@infosec mnt]$ cd ..
[xuhui@infosec /]$ ls
bin   command  etc   initrd  lost+found  mnt  proc  sbin     tmp  USR
boot  dev      home  lib     misc        opt  root  service  usr  var
[xuhui@infosec /]$ cd home
[xuhui@infosec home]$
[r]eset connection/[s]ynchronize/[n]one [r]>
done
```

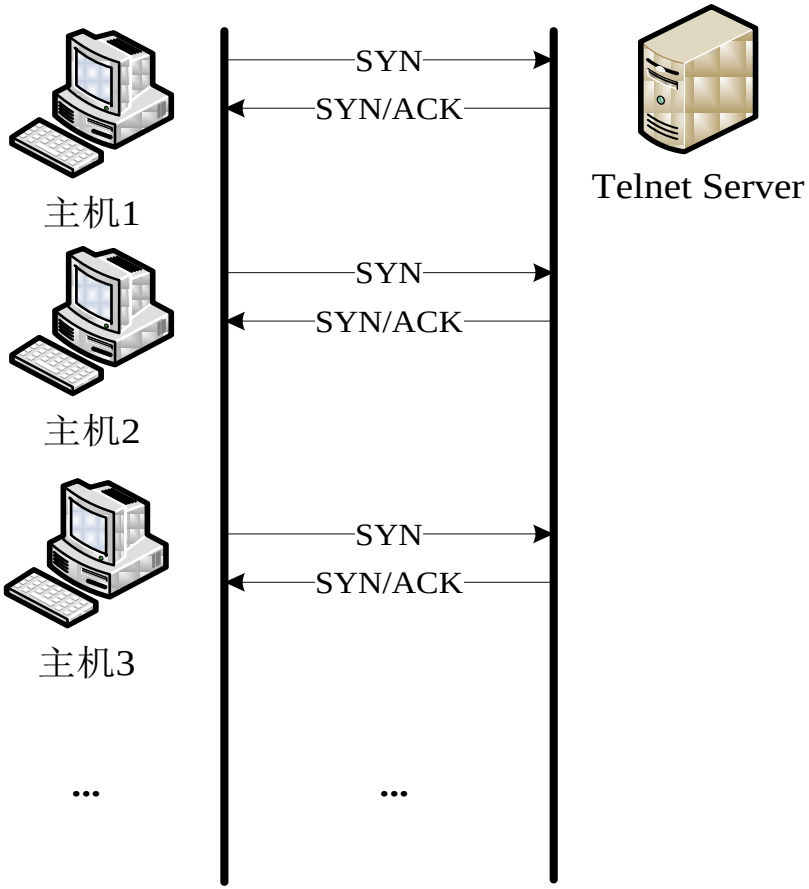
# Hunt劫持会话时听到ACK风暴

# 如何防止会话劫持

- 避免攻击者成为通信双方的中间人
  - 部署交换式网络，用交换机代替集线器
  - 禁用主机上的源路由
  - 采用静态绑定IP-MAC映射表以避免ARP欺
  - 过滤ICMP重定向报文
- TCP会话加密(IPsec协议)
  - 避免了攻击者在得到传输层的端口及序列号等关键信息
- 防火墙配置
  - 限制尽可能少量的外部许可连接的IP地址
- 检测
  - ACK风暴：ACK包的数量明显增加

# TCP SYN Flood

- 拒绝服务攻击(DoS)
  - 破坏可用性
- **TCP SYN Flood**
  - **SYN**洪泛攻击
  - 利用**TCP**三次握手协议的缺陷
  - 大量的伪造源地址的**SYN**连接请求
  - 消耗目标主机的连接队列资源
  - 不能够为正常用户提供服务



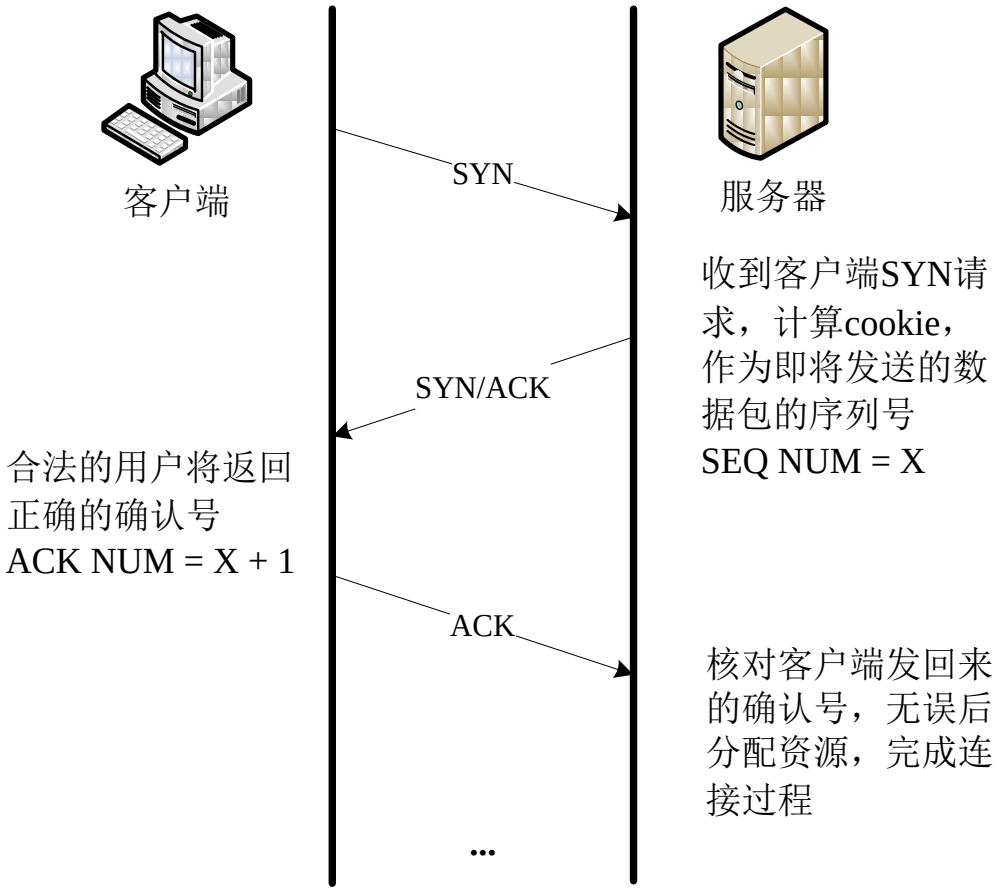
# 利用Netwox进行TCP SYN Flood攻击演示

```
    ################### running tool number 76 ###################
Title: Synflood
+-------------------------------------------------------------------+
| This tool sends a lot of TCP SYN packets.                         |
+-------------------------------------------------------------------+
Usage: netwox 76 -i ip -p port [-s spoofip]
Parameters:
 -i|--dst-ip ip              destination IP address {5.6.7.8}
 -p|--dst-port port          destination port number {80}
 -s|--spoofip spoofip        IP spoof initialization type {linkbraw}
Example: netwox 76 -i "5.6.7.8" -p "80"
Example: netwox 76 --dst-ip "5.6.7.8" --dst-port "80"
Enter optional tool parameters and press Return key.
netwox 76 -i "172.*.*.188" -p 80
```

此时再使用主机A向服务器B发送连接请求，服务器会回应**"Unable to connect to remote host: Connection timed out"**

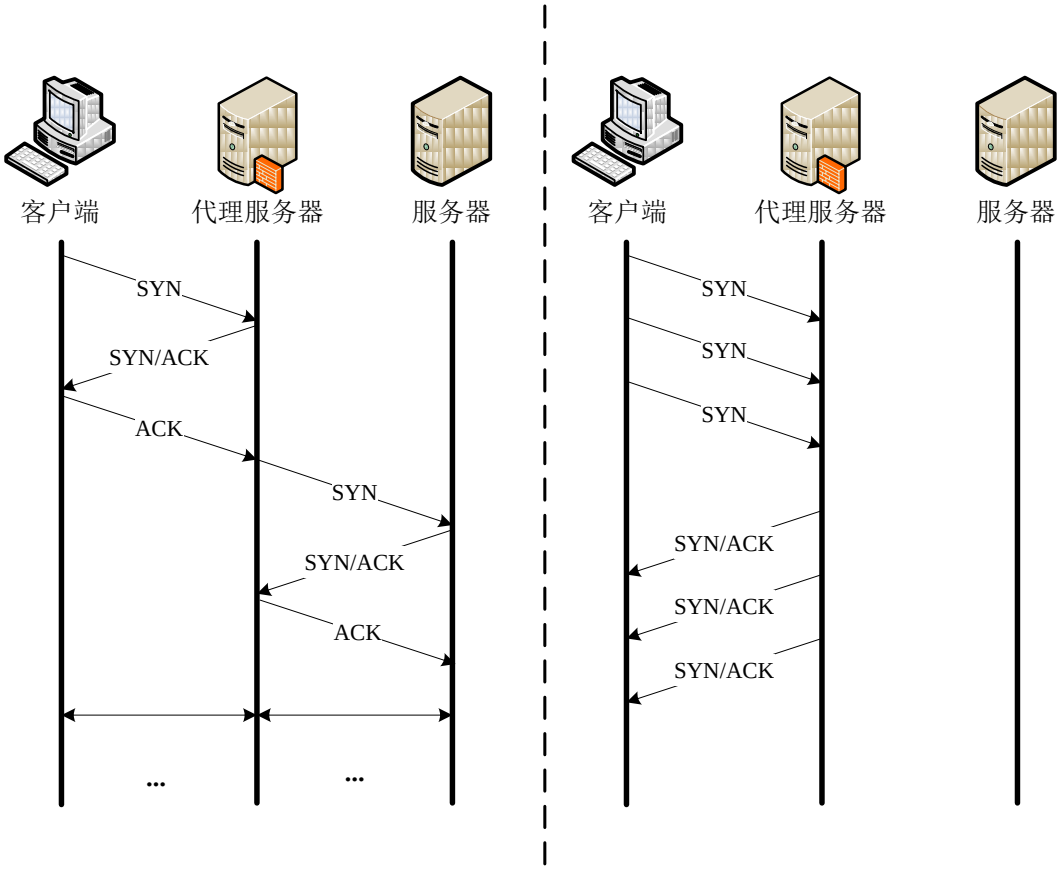
# SYN Flood攻击防范措施 -Syn Cookie

- 弥补TCP连接建立过程资源分配这一缺陷
- “无状态的三次握手”
  - 服务器收到一个SYN报文后,不立即分配缓冲区
  - 利用连接的信息生成一个cookie, 作为SEQ
  - 客户端返回ACK中带着ACK = cookie+1
  - 服务器端核对cookie, 通过则建立连接，分配资源



# 防火墙地址状态监控技术

- 有状态防火墙
  - 网络中的**TCP**连接进行状态监控和处理
  - 维护**TCP**连接状态：**NEW**状态、**GOOD**状态、**BAD**状态…
  - **"**三次握手**"**代理



# UDP Flood攻击

- UDP协议
  - 无状态不可靠
  - 仅仅是传输数据报
- UDP Flood
  - 带宽耗尽型拒绝服务攻击
  - 分布式拒绝服务攻击(DDoS)
  - 利用僵尸网络控制大量受控傀儡主机
  - 通常会结合IP源地址欺骗技术

# UDP Flood攻击防范措施

- 禁用或过滤监控和响应服务
- 禁用或过滤其它的 **UDP** 服务
- 网络关键位置使用防火墙和代理机制来过滤掉一些非预期的网络流量
- 遭遇带宽耗尽型拒绝服务攻击
  - 终端无能为力
  - 补救措施：网络扩容、转移服务器位置
  - 事件响应：汇报给安全应急响应部门、追溯和处置
  - 流量清洗解决方案：**ISP**为关键客户/服务所提供

# 内容

1. TCP/IP网络协议栈攻击概述
2. 网络层协议攻击
3. 传输层协议攻击
4. TCP/IP网络协议栈攻击防范措施
5. 作业5－TCP/IP协议栈重点协议的攻击实验

# 监测、预防与安全加固

- 网络接口层 – 主要安全威胁是网络嗅探
  - 局域网中的监听点检测
  - 网络设计上尽量细分和优化网络结构
  - 关键路径上的网关、路由器等设备的严格安全防护
  - 各类网络采用上层的加密通信协议
- 互联层
  - 多种检测和过滤技术来发现和阻断网络中欺骗攻击
  - 增强防火墙、路由器和网关设备的安全策略**(egress filtering)**
  - 关键服务器使用静态绑定**IP-MAC**映射表、使用**IPsec**协议加密通讯等预防机制
- 传输层：加密传输和安全控制机制**(**身份认证，访问控制**)**
- 应用层：加密，用户级身份认证，数字签名技术，授权和访问控制技术以及主机安全技术如审计、入侵检测

# 网络安全协议

- 网络接口层
  - 无线：**WPA/WPA2**
  - 统一认证：**802.1X**
- 网络互联层
  - **IPsec**协议簇
  - **AH**协议：完整性、认证、抗重放攻击
  - **ESP**协议：机密性、数据源验证、抗重放、完整性
- 传输层
  - **TLS/SSL:** 加密、可靠
- 应用层
  - **HTTPS、S/MIME、SET**

| | |
|---|---|
| 应用层 | shell: SSH<br>ftp: SFTP<br>http: HTTPS<br>email: S/MIME<br>PKI/SET |
| 传输层 | SSL<br>TLS |
| 网络互连层 | IPsec |
| 网络接口层 | 统一认证协议：802.1x<br>WLAN: WEP/WPA |

# 下一代因特网协议

- 下一代因特网协议
  - **IPv6**为代表
  - **ICMPv6、DHCPv6……**
  - 没有了**ARP**
- **IPv6**优势
  - **IPv6**具有更大的地址空间：主动扫描和主动传播受到抑制
  - **IPv6**使用更小的路由表
  - **IPv6**增加了增强的组播**(Multicast)**支持以及对流的支持**(Flow Control) – 提升QoS**
  - **IPv6**加入了对自动配置**(Auto Configuration)**的支持
  - **IPv6**具有更高的安全性：网络层的数据进行加密,...

# 内容

1. TCP/IP网络协议栈攻击概述
2. 网络层协议攻击
3. 传输层协议攻击
4. TCP/IP网络协议栈攻击防范措施
5. 作业5－TCP/IP协议栈重点协议的攻击实验

# 作业5-TCP/IP协议栈重点协议的攻击实验(团队作业)

- 请在网络攻防实验环境(以SEED_VM作为攻击机，Linux Metasploitable/Windows Metasploitable作为靶机)中完成TCP/IP协议栈重点协议的攻击实验。
  - 详细描述见第5章讲义(+勘误)
- 网络层攻击
  - ARP缓存欺骗(3分)
  - ICMP重定向攻击(2分)
- 传输层攻击
  - SYN flood攻击(2分)
  - TCP RST攻击(3分)
  - TCP会话劫持 (bonus 2分)
- 提交详细实验报告-deadline: 11月10日

# 作业5-勘误

- (2)对telnet与ssh连接的TCP RST攻击
- TCP RST攻击可以中断两个被攻击主机之间的TCP连接。举例来说，主机A和主机B之间已经建立了一个telnet(TCP)的连接，那么攻击者可以伪造一个由A发往B的TCP包，从而破坏已经建立起来的连接。要成功地实施这一攻击，攻击者需要正确地构造TCP RST数据包。
- 在这一个实验中，你需要对两台相互之间已经建立起telnet连接的主机(称为主机A和主机B)实施TCP RST攻击。完成之后，可以尝试将同样的攻击实施于一个ssh连接。请描述你观察到的现象。为了简化任务，我们还是假设攻击机与目标主机A、B均处于同一局域网内，也就是说攻击机可以得到A和B之间TCP通信的数据。

# Thanks

诸葛建伟

zhugejw@gmail.com