

网络与内容安全

IP网络安全威胁

参考书：

网络攻防技术与实践 诸葛建伟 电子
工业出版社，2011

- 要求：
 - 各种攻击常用于哪个攻击阶段
 - 有哪些主要攻击类型
- 课后练习1：
 - Wireshark 实验，了解一种协议，分析安全威胁
- 课后练习2（选）：
 - 一种攻击方式演示：利用工具（如 Netwox, Netwag, Nessus, Nmap等）

攻击的手段

- 预攻击阶段 (收集信息)
 - 扫描：主机扫描和端口扫描（nmap），漏洞扫描(Nessus)，无线...
 - 操作系统类型鉴别，网络拓扑分析，开放的服务...
 - 窃听，嗅探
 - 利用一些信息服务：搜索引擎,网站,出版物
 - 社会工程（SNS，）
 - 。。。

攻击的手段

- 攻击阶段
 - 网络扫描
 - 缓冲区溢出攻击
 - 脚本程序漏洞攻击
 - 口令攻击
 - 远程控制技术
 - 错误及弱配置攻击
 - 欺骗，伪造
 - 信息窃取、篡改，插入，删除，重发
 - 劫持
 - Man-In-The-Middle(MITM)
 - DOS/DDOS: 拒绝服务攻击
 - ...
- SNS BOTNET
- Zero-day
- spear phishing: 定向的phishing
- APT (Advance Persistent Threat)

IP网络面临的安全威胁

- 恶意攻击
 - 网络扫描
 - DDoS
 - 窃取机密数据（窃听，中间人），流量分析
 - 欺骗和网络钓鱼（Phishing）
 - 会话劫持
 - 消息篡改，插入，删除，重发
 - 物理破坏
- 误用和滥用（内部和外部）
 - 配置错误、缺省配置
 - 内部窃取：客户资料、充值卡等
 - 内部越权
 - 操作行为抵赖
 - 垃圾流量、邮件、电话和短信
- 恶意代码：
 - 病毒和蠕虫,木马
 - 逻辑炸弹,时间炸弹

应用层

UDP TCP

IP ICMP...

LLC

MAC

物理层

IP网络各层的主要威胁

查询CERT/CC –
CNCERT/CC – SANS官
方网站可以了解当前
最新的漏洞和安全事
件统计报告

物理层

- 物理破坏：线路，交换机。。。。
- 非法接入
- 欺骗、伪造、

链路层

- ARP
- DHCP, DHCPv6
- VLAN, MPLS VPLS
- STP (spanning tree protocol)

针对ARP协议的攻击

利用ARP协议的特点,可以实现针对内网主机的攻击.
典型的ARP攻击是利用Fake MAC的方式来进行的,代替
10. 10. 14. 10发送以下格式的ARP请求报文.

源IP	源MAC	目的IP	目的MAC
10. 10. 14. 10	00. 01. 02. 03. 04. 05	10. 10. 14. 100	FF. FF. FF. FF. FF. FF

或者主动发送gratuitous ARP

源IP	源MAC	目的IP	目的MAC
10. 10. 14. 10	00. 01. 02. 03. 04. 05	10. 10. 14. 100	00. F4. 4D. 39. 11. 4B

攻击目标是? ----→ 具体分析

针对ARP协议的攻击

ARP缓存会在较短时间内刷新,但是持续的ARP攻击的结果是使得目标机在内网主机（包括网关）的ARP缓存中的MAC地址不断被修改成错误的,在链路层即不可能实现正常的数据接收,目标机自身发现严重冲突后可能会禁用协议栈,具体的处理方式依赖于操作系统

针对网关的ARP攻击则可能切断所有内网与外部的数据交换

受害主机如果是Windows平台,则ARP攻击的现象很显著, 弹出地址冲突提示信息

针对ARP协议的攻击

相对来说, ARP Spoofing则是一种温良性质的攻击, 它通常用于针对目标机某一个具体连接过程的攻击, 受到攻击主机没有明显的不良反应, 但是连接非正常断开.

例如: 10. 10. 14. 10和10. 10. 14. 100之间存在一个TCP连接, 可以发送以下主动ARP应答报文来切断他们的连接

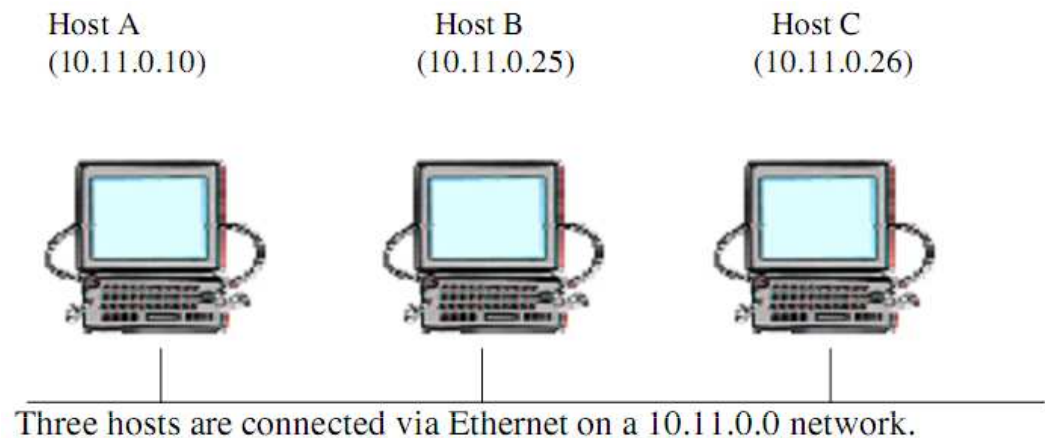
源IP	源MAC (faked)	目的IP	目的MAC
10. 10. 14. 100	00. 01. 02. 03. 04. 05	10. 10. 14. 10	00. F4. 4D. 39. 11. 4B

这个应答包修改了14. 10ARP缓存中14. 100的地址, 其后14. 10发送给14. 100的数据包中含有错误的目标地址, 被14. 100抛弃, 两者间的连接会因超时而断开.

对于连接的另一方不在本地网的情况ARP Spoofing同样有效, 此时需将源IP替换为网关IP即可. 因为网关充当ARP代理, 发送包的目标MAC是以网关MAC替代的

ARP cache poisoning

- Broadcast Request
- Multiple Responses
- Unsolicited Response



ARP cache on Host A

Windows : arp -a

```
[root@localhost /]# arp
```

Address	Hwtype	Hwaddress	Flags	Mask	Iface
10.11.0.26	ether	00:03:93:5A:74:FC	C		eth0

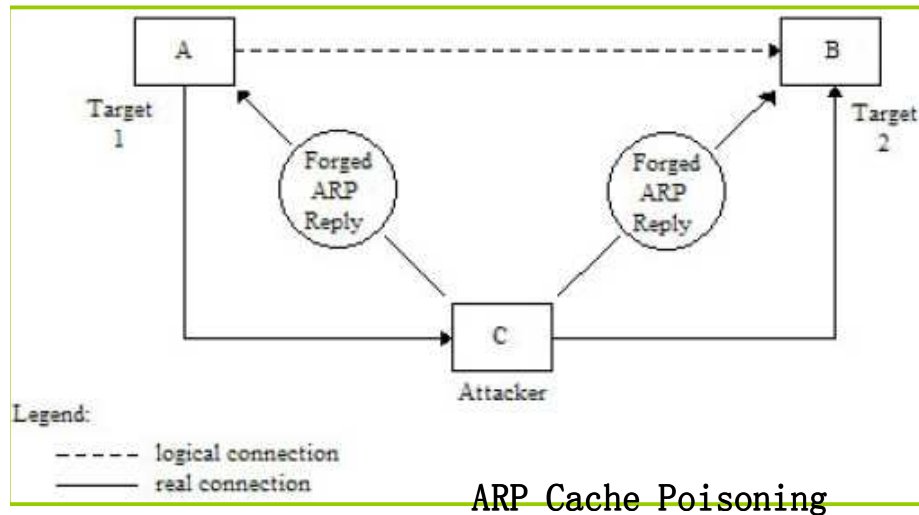
After B uses C's IP address and sends out a broadcast request

```
[root@localhost /]# arp
```

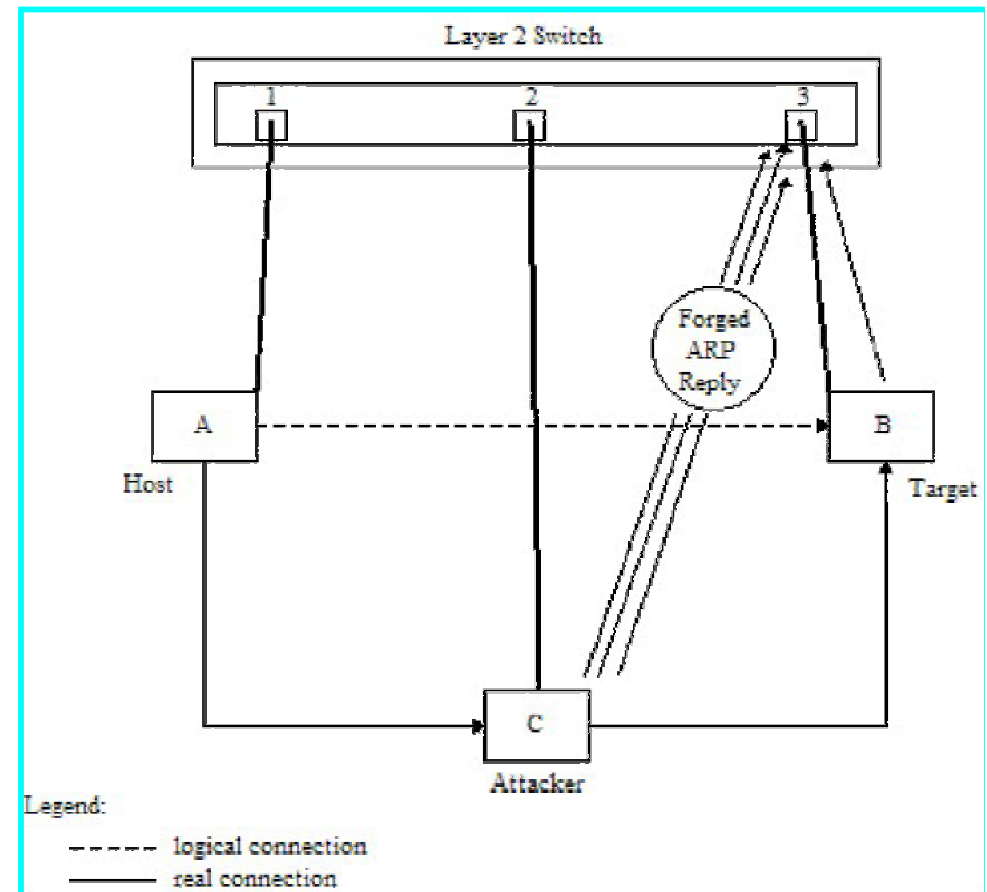
Address	Hwtype	Hwaddress	Flags	Mask	Iface
10.11.0.26	ether	00:30:65:D5:99:6E	C		eth0

- When a malicious host uses another host's IP address and sends out a broadcast request, Linux caches the new IP-to-Ethernet address mapping, thus causing ARP Cache poisoning.
- ARP cache could be poisoned when multiple ARP responses are received, as there is a **race condition** that the hacker might win. In this case, hacker's IP-to-Ethernet address mapping is cached by the victim's host causing its ARP cache to be poisoned.
- Since ARP is a **stateless protocol**, it does not keep track of outgoing requests and incoming responses. Hence, unsolicited responses are processed and can cause ARP cache poisoning.

ARP欺骗 - L2 Attacks



CAM 表被填满



Switch Port Stealing

MAC 洪泛攻击 (MAC flooding)

1. 交换机工作原理 (CAM表)

实现:

- 交换网络中的窃听
- MITM(Man-In-The-Middle) 攻击
- Switch Port Stealing

SQL蠕虫病毒利用组播目标地址, 构造假目标 MAC 来填满交换机 CAM

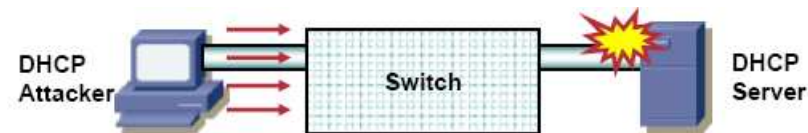
DHCP 攻击

- DHCP攻击也是二层攻击的一种
- DHCP为动态主机配置协议
- DHCP server 可以自动为用户设置网络 IP 地址、掩码、网关、DNS、WINS 等网络参数

DHCP 攻击

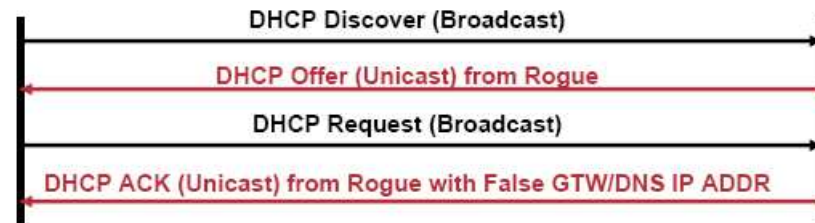
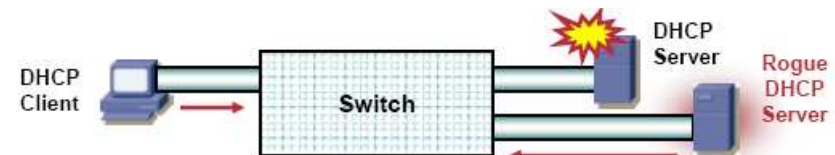
1.DOS(DHCP starvation

Attack): 如将正常的 DHCP 服务器所能分配的 IP 地址**耗尽**（Goobler的工具可以发出大量带有不同源MAC地址的DHCP请求）



2.欺骗(DHCP rogue attack):

冒充合法的 DHCP 服务器。如为用户分配一个经过修改的 DNS server，将用户引导到预先配置好的假金融网站或电子商务网站，骗取用户帐户和密码



可以实现这类攻击的工具，如Yersinia

- 例：

- **D-Link AirPlus DI-614+和DI-604 DHCP Server淹没攻击拒绝服务漏洞**

- 发布日期：2004-06-27

- 受影响系统：D-Link DI-614+ 2.30

- BUGTRAQ ID: [10621](#)

- CVE(CAN) ID: [CVE-2004-0661](#)

- D-Link AirPlus DI-614+和DI-604对大量DHCP请求缺少正确处理，远程攻击者可以利用这个漏洞对设备进行拒绝服务攻击。发送大量合法DHCP请求可导致设备消耗大量内存，需要重新启动获得正常服务。

- 厂商补丁：

- DI-614+ Revision B的firmware 3.41版本已经修正此问题，而DI-614+ Revision A和DI-604设备还没有新的固件来解决此问题，建议用户联系供应商获得升级程序：

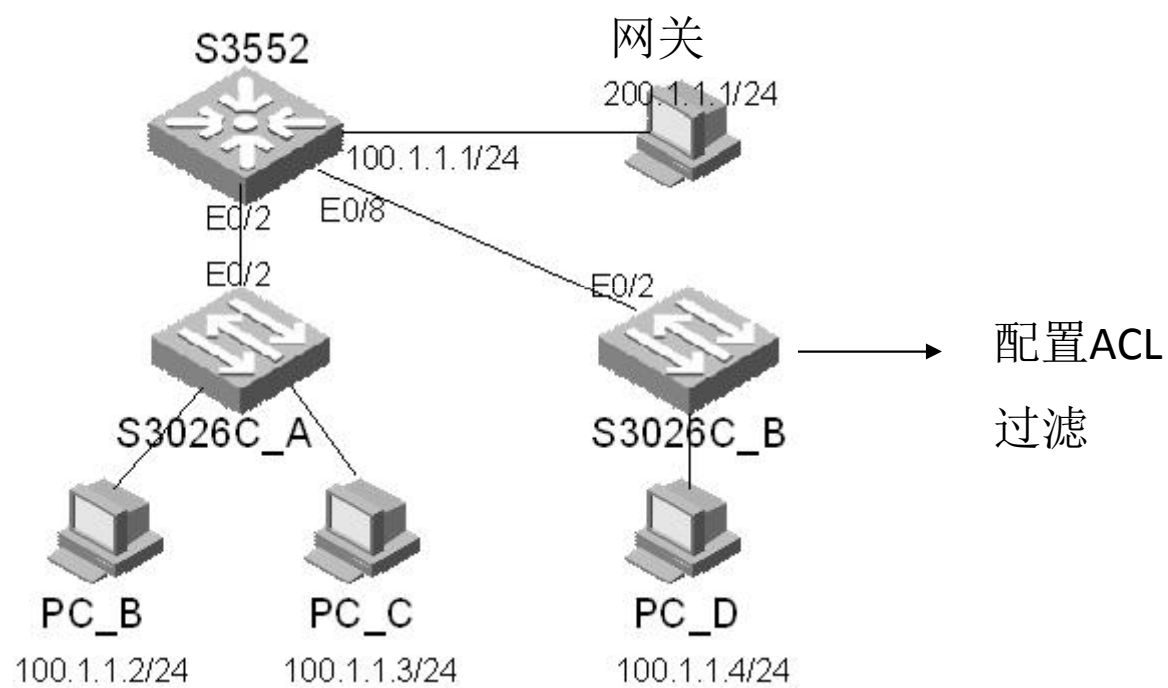
- 对策

- 对重要地址配置静态ARP

- 对于二层设备

- 可以配置IP+MAC+port绑定(包括IP-MAC, MAC-Port) ,
Sticky Port Security技术中交换机将学到的 mac 地址写到
端口配置中, 交换机重启后配置仍然存在。
 - 限制端口上最大可以通过的 MAC 地址数量
 - 可以配置访问控制列表, 过滤对重要节点的ARP报文
 - 使用Root Guard, 或BPDU (Bridge protocol data unit)
Guard这样的功能
 - 动态ARP inspect功能 (DAI)

- 例:



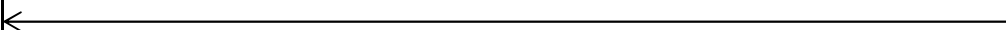
- CISCO VLAN上配置使用DHCP Snooping、DAI（dynamic arp inspection）等技术（三层交换机，针对）
- 例：
- ```
!
ip dhcp snooping vlan 100
ip dhcp snooping
ip arp inspection vlan 100
ip arp inspection filter static-arp vlan 100
!
!
!
arp access-list static-arp
 permit ip host 192.168.100.11 mac host aaaa.aaaa.aaaa
 permit ip host 192.168.100.12 mac host bbbb.bbbb.bbbb
 permit ip host 192.168.100.13 mac host cccc.cccc.cccc
 permit ip host 192.168.100.14 mac host dddd.dddd.dddd
!
```
- 课外资料： [cisco-L2-attack-mitigation](#)

# 网络层（IP层）

- IP源地址伪造
- 主机扫描：ICMP主机扫描
- 路由攻击：
  - ICMP路由重定向
  - AS hijack，利用BGP

## IPv4 头：IP源地址伪造，许多攻击的重要前提

### 原因：路由器不进行源地址检查

|                                                                                      |    |     |         |      |
|--------------------------------------------------------------------------------------|----|-----|---------|------|
| ver                                                                                  | HL | TOS | IP分组总长度 |      |
| 标识                                                                                   |    |     | F       | 分段偏移 |
| TTL                                                                                  |    | 协议  | 头校验     |      |
| 源IP地址                                                                                |    |     |         |      |
| 目的IP地址                                                                               |    |     |         |      |
| 选项                                                                                   |    |     |         | 填充   |
|  |    |     |         |      |
| 32bit                                                                                |    |     |         |      |

ver: 4 版本号

HL: 4 头长(单位:32bits)

## TOS: 8 服务类型

IP分组总长度: (单位:8bits)

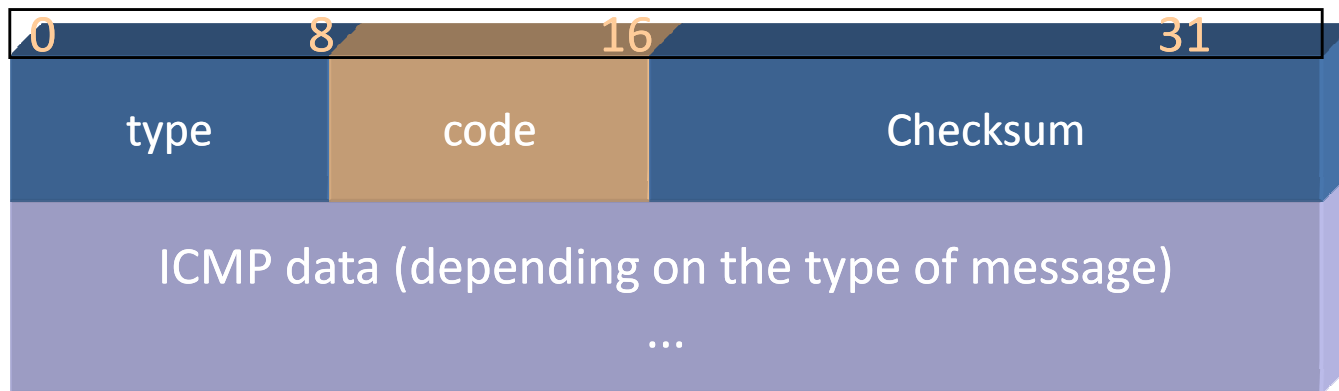
F: 3 分段标志

TTL: 4 生存时间

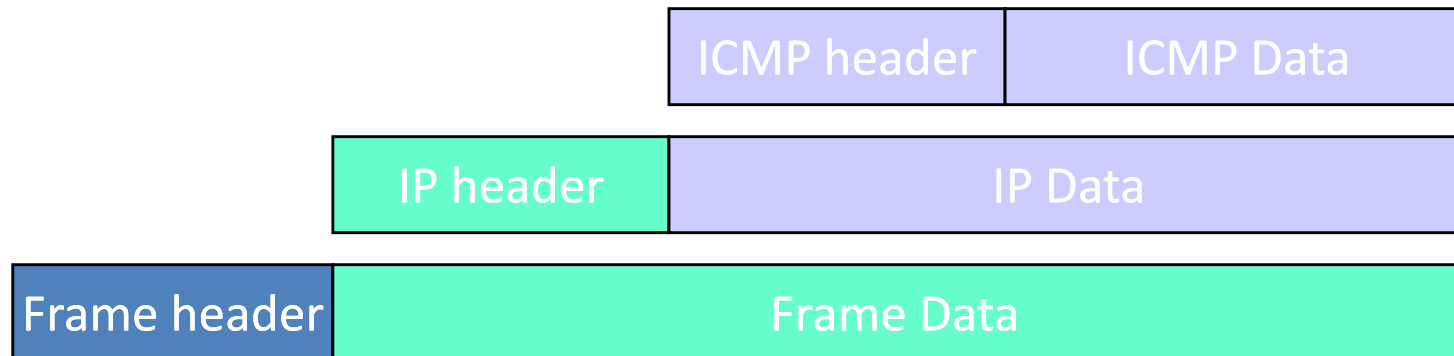
# ICMP (Internet Control Message protocol)

- 作用：
  - 网络诊断功能：
    - 网络节点利用该协议向源主机报告IP包转发中的问题
      - IP数据报中只包含了源主机的地址，并不会包含它所经过的路由
      - 只是利用该协议向源主机报告问题，问题的处理由源主机进行。
  - 辅助的路由功能
  - ....

- 格式



- 封装



# 一些早年的攻击

- 死ping: ping of death

早期版本中许多操作系统对网络数据包的最大尺寸有限制，对TCP/IP栈的实现现在ICMP包上规定为64KB 在读取包的报头后要根据该报头里包含的信息来为有效载荷生成缓冲区，当发送ping请求的数据包声称自己的尺寸超过ICMP上限，也就是加载的尺寸超过64K上限时，就会使ping请求接收方出现内存分配错误，导致TCP/IP堆栈崩溃致使接受方当机

- 防御

- 现在所有的标准TCP/IP实现都已实现对付超大尺寸的包并且大多数防火墙能够自动过滤这些攻击，包括从windows98之后的windows,NT(service pack 3之后) linux Solaris 和Mac OS都具有抵抗一般ping of death攻击的能力
- 此外对防火墙进行配置阻断ICMP以及任何未知协议都将防止此类攻击



# 一些早年的攻击

- 泪滴teardrop

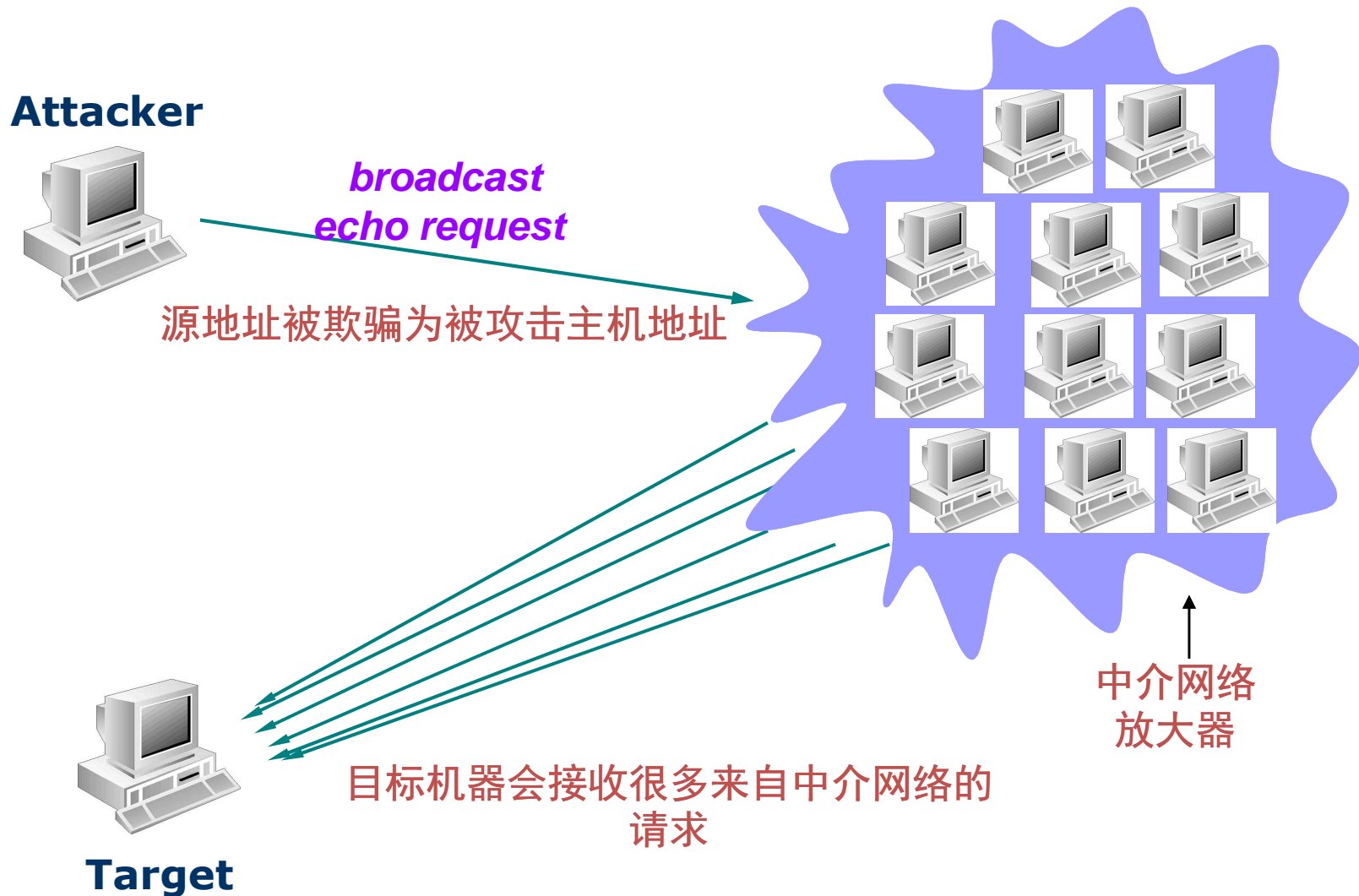
- 概览:

- IP分段含有指示该分段所包含的是原包的哪一段的信息某些TCP/IP 包括service pack 4以前的NT 在收到含有重叠偏移的伪造分段时将崩溃

- 防御:

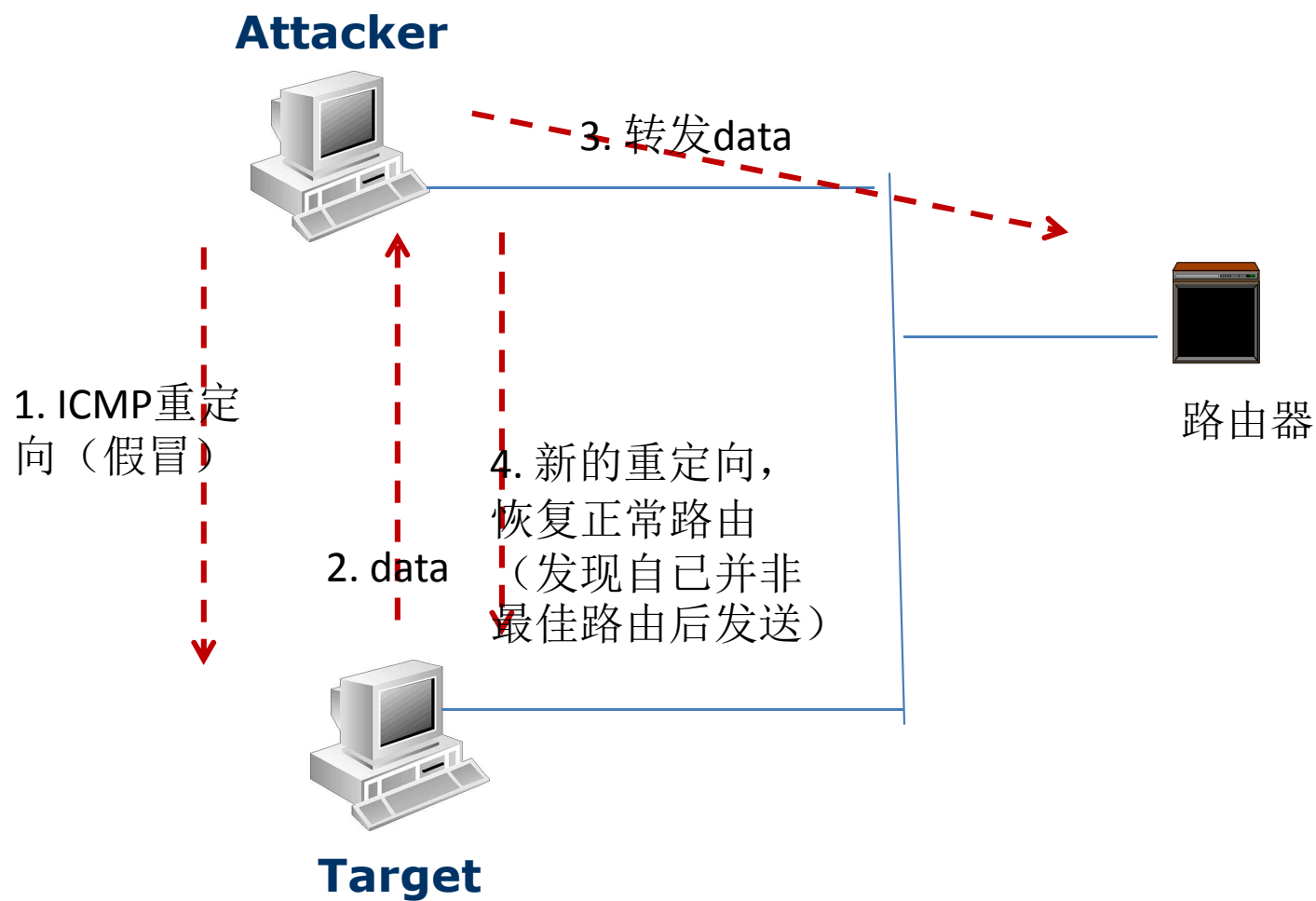
- 服务器应用最新的服务包或者在设置防火墙时对分段进行重组而不是转发它们

# 拒绝服务攻击—Smurf攻击



发源地址为受害者，对广播地址的ICMP应答请求，导致网络内的所有主机都对此ICMP应答请求作出答复，导致网络阻塞比ping of death洪水的流量高一或两个数量级

# ICMP路由重定向



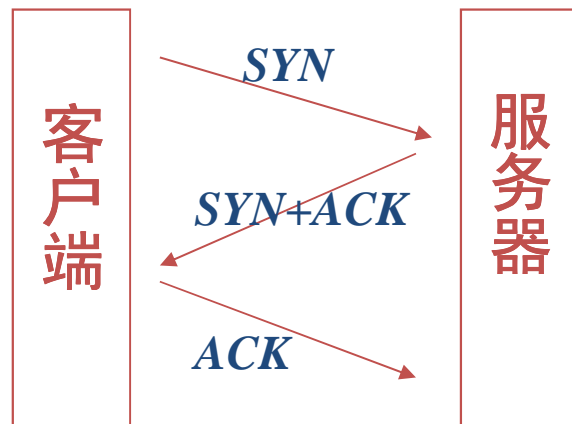
# 传输层

- SYN flooding
- UDP flooding
- 端口扫描
- 会话劫持

# 拒绝服务攻击—SynFlood

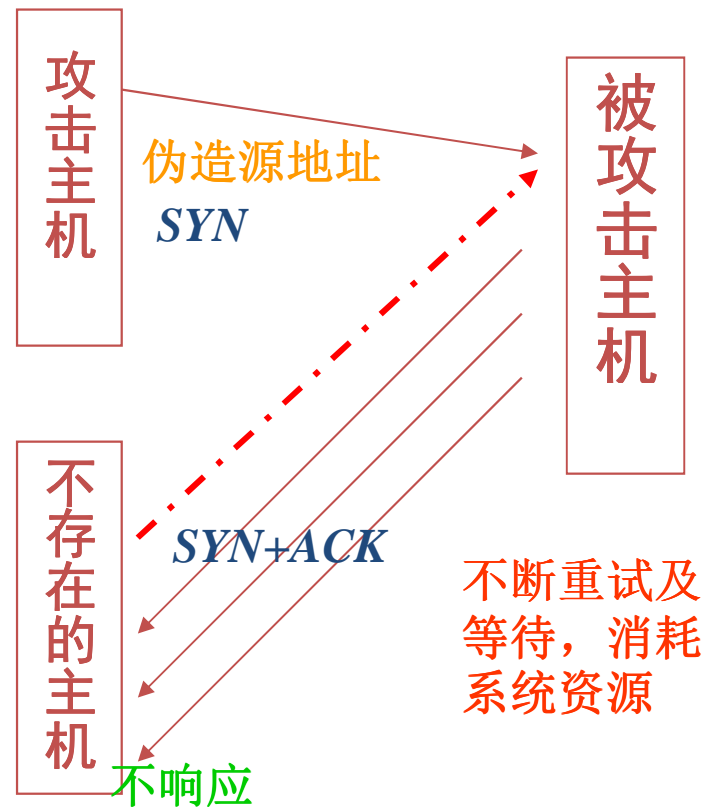
- 利用了TCP协议的三次握手漏洞。

- 正常的TCP/IP三次握手



握手完成，开始传送数据，系统消耗很少

- SynFlood攻击



# SYN Flood 攻击防范

- 有4个防范措施：
  - 其一，增加连接队列的大小；
  - 其二，缩短连接建立超时期限；
  - 其三，应用厂家的相关软件补丁、检测及规避潜在SYN攻击；
  - 最后，应用网络入侵检测软件IDS产品。IDS能主动发送RST分组响应初始SYN请求。

提示：设计无状态的协议

- 参考文献：Eddy, W., “TCP SYN Flooding Attacks and Common Mitigations,” RFC 4987, August 2007.

- Land攻击
- 概览:

在Land攻击中将一个SYN包的源地址和目标地址都设置成同一服务器地址，导致接收服务器向自己的地址发送SYN-ACK消息，结果这个地址又发回ACK消息并创建一个空连接每一个这样的连接都将保留直到超时掉，OS对Land攻击反应不同许多UNIX实现将崩溃

- 防御:
  - 打最新的补丁或者在防火墙进行配置
  - 将那些在外部接口上入站的含有内部源地址滤

# TCP会话持劫

在子网内实现TCP会话持劫的前提是必须首先能够截获会话双方发送的数据,然后抢在一方应答数据之前将伪装的数据发送给发送方.

会话持劫能够使得连接的A方以一种在它自己看来合法的方式断开,攻击者取而代之,获得与该连接所具有的权限来访问B,此后攻击者与B的数据交换全部依赖监听和TCP包伪装实现.

这种合法断开的方式就是攻击者在截获A发送给B的数据后,根据A的数据包,迅速计算出正确的顺序序号和应答号,并且回复一个TCP选项为TCP\_FIN的数据给A,让A认为B以合法的方式和它结束了连接.

以A的身份发的欺骗报文,其序列号计算是伪装能否成功的关键.

$\text{SeqNo} = \text{received. AckNo}$

$\text{AckNo} = \text{received. SeqNo} + \text{size}$

$\text{size} = \text{sizeof}(\text{Packet})$

If (size==0)

size=1;

sizeof(Packet) 是去掉TCP报头后的纯数据长度



# 应用层

- DNS
- HTTP协议
- WEB 应用:
  - 邮件
  - SNS应用
  - WEB搜索
  - . . .

# DNS协议结构

202.113.229.176 -> 202.113.16.10[Query]

NQY:1    NAN:0    NNS:0    NAD:0

QY:www.eyou.com    QID=1234

202.113.16.10 -> 202.113.229.176 [Answer]

NQY:1    NAN:0    NNS:0    NAD:0

QY:61.136.62.70    QID=1234

一个DNS应答报文能否被请求主机接受仅仅看其源地址是否是请求的DNS服务器以及QID是否与刚才发送的请求报文的QID一致.

# 监视获得的一次DNS解析过程

| Source IP       | Port | Destination IP  | Port | Syn--Ack | time    | Protocol | Data                                             |
|-----------------|------|-----------------|------|----------|---------|----------|--------------------------------------------------|
| 202.113.229.141 | 2457 | 202.113.16.10   | 53   | 0---0    | 9:35:22 | UDP      | it.nankai.edu.cn                                 |
| 202.113.229.147 | 2661 | 202.113.16.10   | 53   | 0---0    | 9:35:33 | UDP      | www.google.com                                   |
| 202.113.16.10   | 53   | 202.113.229.147 | 2661 | 0---0    | 9:35:34 | UDP      | www.google.com ? , 1&!e? F ns1?? F ns2?? F ns3?? |

# DNS欺骗

DNS协议从使用来说分为正向解析(域名->IP)和反向解析(IP->域名),相应的DNS欺骗也分正向和反向,可用于不同的攻击目的.

欺骗一个DNS正向解析报文可用于将被攻击主机引向一个非法的IP,在伪造Web欺骗中使用非常广.攻击者可以复制一个目标网站的Web页到自己的主机,然后通过DNS Spoof在受害机在以域名方式访问目标网站时给受害主机提供一个错误的IP解析结果(IP为攻击者),但是受害者却没有觉察,并且被诱使在网页上输入了一些敏感信息,这些信息则被攻击者记录下来.

而反向欺骗则常用在bbs中隐藏IP等.

# Web欺骗

- 何谓**Web**欺骗？

- 创建一个**Web**站点的映像，使得用户的连接被接入到**Hacker**的服务器，达到欺骗网络用户的目的。

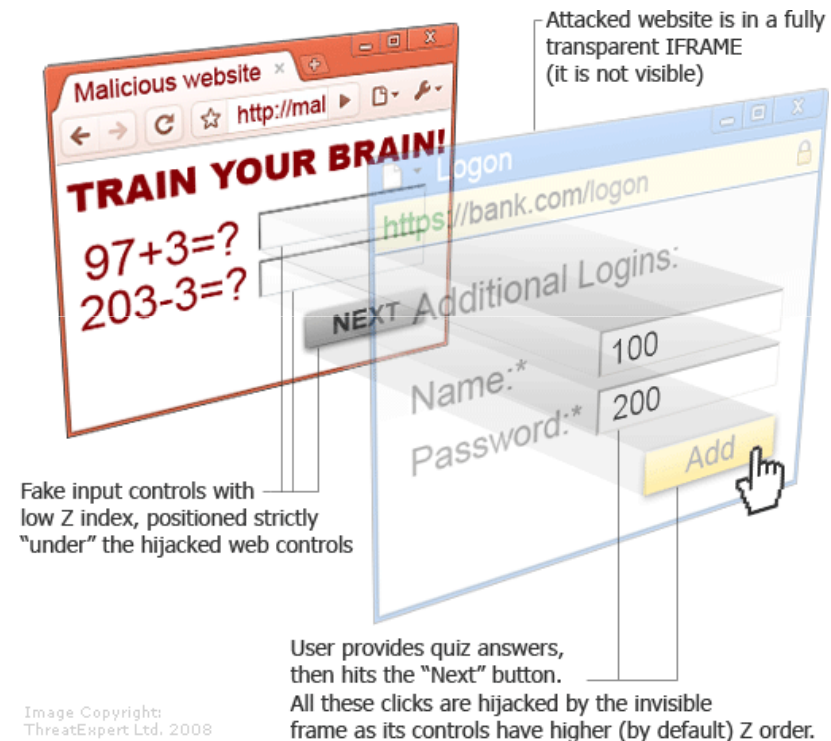
- 网站仿冒（**Phishing**, Xi shing）

- 建立假网站
- 通过垃圾邮件大量发信引诱用户访问
- 使用中奖、系统升级等手段诱使用户输入个人信息
- 主要针对银行和信用卡服务机构



# Clickjacking(点击劫持)

- 视觉上的欺骗手段。攻击者使用一个透明的、不可见的iframe，覆盖在一个网页上，诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击在iframe页面的一些功能性按钮上（开启电脑的镜头，进行偷窥或监视，导向某个网页下载恶意内容等。



<http://www.schneier.com/blog/archives/2008/10/clickjacking.html>

```

<!DOCTYPE html>
<html>
 <head>
 <title>CLICK JACK!!!</title>
 <style>
 iframe {
 width: 900px;
 height: 250px;

 /* Use absolute positioning to
line up update button with fake button
*/
 position: absolute;
 top: -195px;
 left: -740px;
 z-index: 2;

 /* Hide from view */
 -moz-opacity: 0.5;
 opacity: 0.5;
 filter: alpha(opacity=0.5);
 }
 </style>
 </head>
 <body>
 <iframe src="http://www.qidian.com"
scrolling="no"></iframe>
 <button>CLICK HERE!</button>
 </body>
</html>

```

```

•
 button {
 position: absolute;
 top: 10px;
 left: 10px;
 z-index: 1;
 width: 120px;
 }
</style>
</head>
<body>
 <iframe src="http://www.qidian.com"
scrolling="no"></iframe>
 <button>CLICK HERE!</button>
</body>
</html>

```

# Web欺骗及防范技术

## ——防范技术

- 检查页面的源代码
- 禁用JavaScript、ActiveX等脚本语言
- 确保应用有效和能适当地跟踪用户会话ID 使用尽可能长的随机数
- 教育是非常重要的



# 总结： 欺骗攻击

- 即使主机系统本身没有任何漏洞，黑客仍然可以使用各种欺骗手段达到攻击的目的。
- 一般情况下，黑客会利用TCP / IP协议本身的一些缺陷。如：IP欺骗攻击。
- 另外欺骗攻击：ARP欺骗、DNS欺骗、Web欺骗和Cookie欺骗。

# 网络欺骗技术在信息安全上的应用

- 利用网络欺骗作为信息安全的一种技术
  - Honey Pot
  - 分布式Honey Pot将欺骗(Honey Pot)散布在网络  
的正常系统和资源中，利用闲置的服务端口来  
充当欺骗
- 网络欺骗一般通过隐藏、安插错误信息等  
技术手段实现，前者包括隐藏服务、多路  
径和维护安全状态信息机密性；后者包括  
重定向路由、伪造假信息和设置圈套等。

# 总结： 网络扫描

- 目的
  - 信息收集： 端口服务， OS， 漏洞等
- 防范
  - 1. 关闭闲置和有潜在危险的端口
  - 2. 检查各端口， 有端口扫描的症状时， 立即屏蔽该端口（利用防火墙）

ICMP Usage in Scanning

<http://www.sys-security.com>

Nmap Remote OS Detection

<http://www.insecure.org/nmap/nmap-fingerprinting-article.html>

<http://www.iss.net.cn/downloads/document/Ss.ppt>

# 非技术手段

- 合法途径
  - 从目标机构的网站获取
  - 新闻报道，出版物
  - 新闻组或论坛
- 社会工程手段
  - 假冒他人，获取第三方的信任
- 搜索引擎:Google hacking

# 技术手段

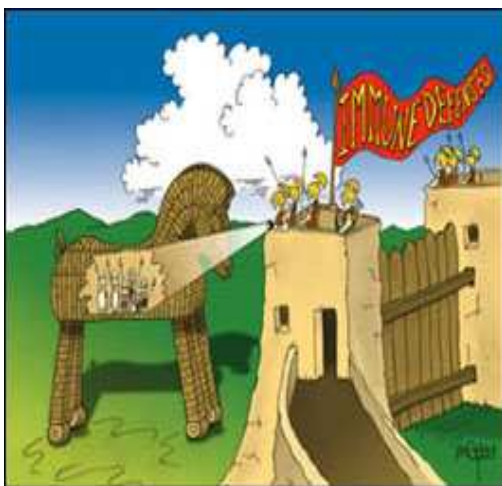
- 阶段1：主机扫描：如PING（Ping Sweep）：活动状态
- 阶段2：
  - 操作系统探测（Operating system identification）
  - 探测访问控制规则
  - 端口扫描（Port scan）
- 阶段3：漏洞扫描（vulnerability scan）

利用ICMP, IP, TCP,UDP各层协议

# 总结：远程控制技术

远程控制实际上是包含有服务器端和客户端的一套程序

植入，自启动（加载），隐藏、远程控制数据传输



特洛伊木马  
特洛伊木马的来历

来源于希腊神话中的特洛伊战争

# 总结：拒绝报务攻击

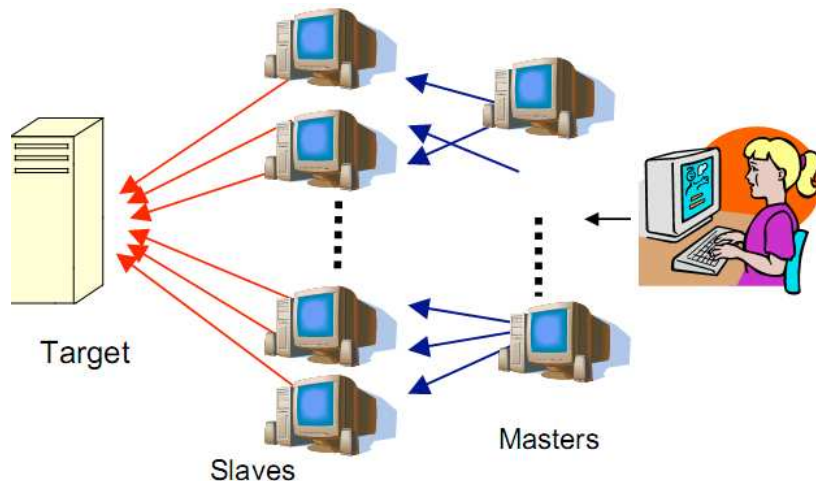
DoS (Denial of Service)

DDoS (Distributed Denial of Service) 分布式拒绝服务攻击

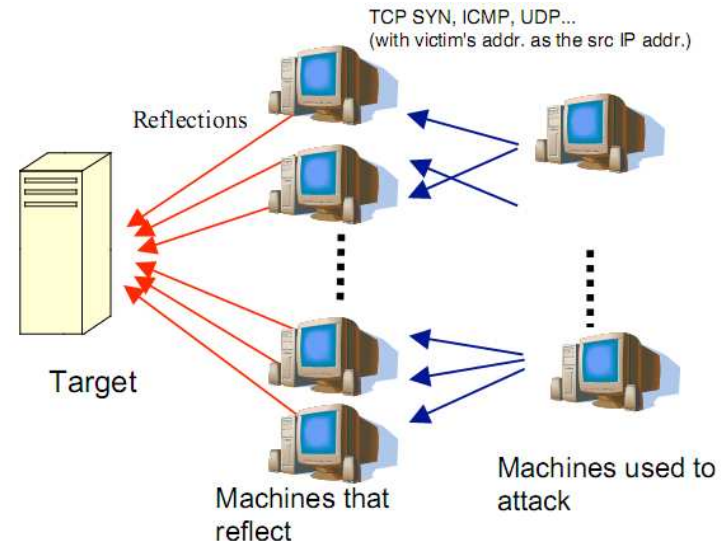
- 攻击目的：

使计算机或网络无法提供正常的服务，它们既不能及时接受外界的请求，也无法及时回应外界的请求。

Direct DDOS Attack



Reflector DDOS Attack



# 常见的DOS攻击：资源衰竭

- 攻击的目标是消耗系统的资源，如带宽,CPU利用率、内存容量、文件系统限额或系统进程总数等服务器资源。
  - 造成：网络拥塞，系统崩溃，文件系统变满或进程被挂起
  - 网络带宽耗尽：
    - 攻击者比目标网络拥有更多的可用带宽。
    - 以小带大：
      - 攻击者通过征用多个网点集中阻塞目标网络的连接以放大DOS的入侵效果。
      - 利用组播、广播地址
    - 常伪造源地址
  - CPU内存资源
    - Stateful协议
    - 计算的不对称性：如加密解密计算
    - 利用软件的bug

必须通过某种方式放大资源消耗，如：

不对称性

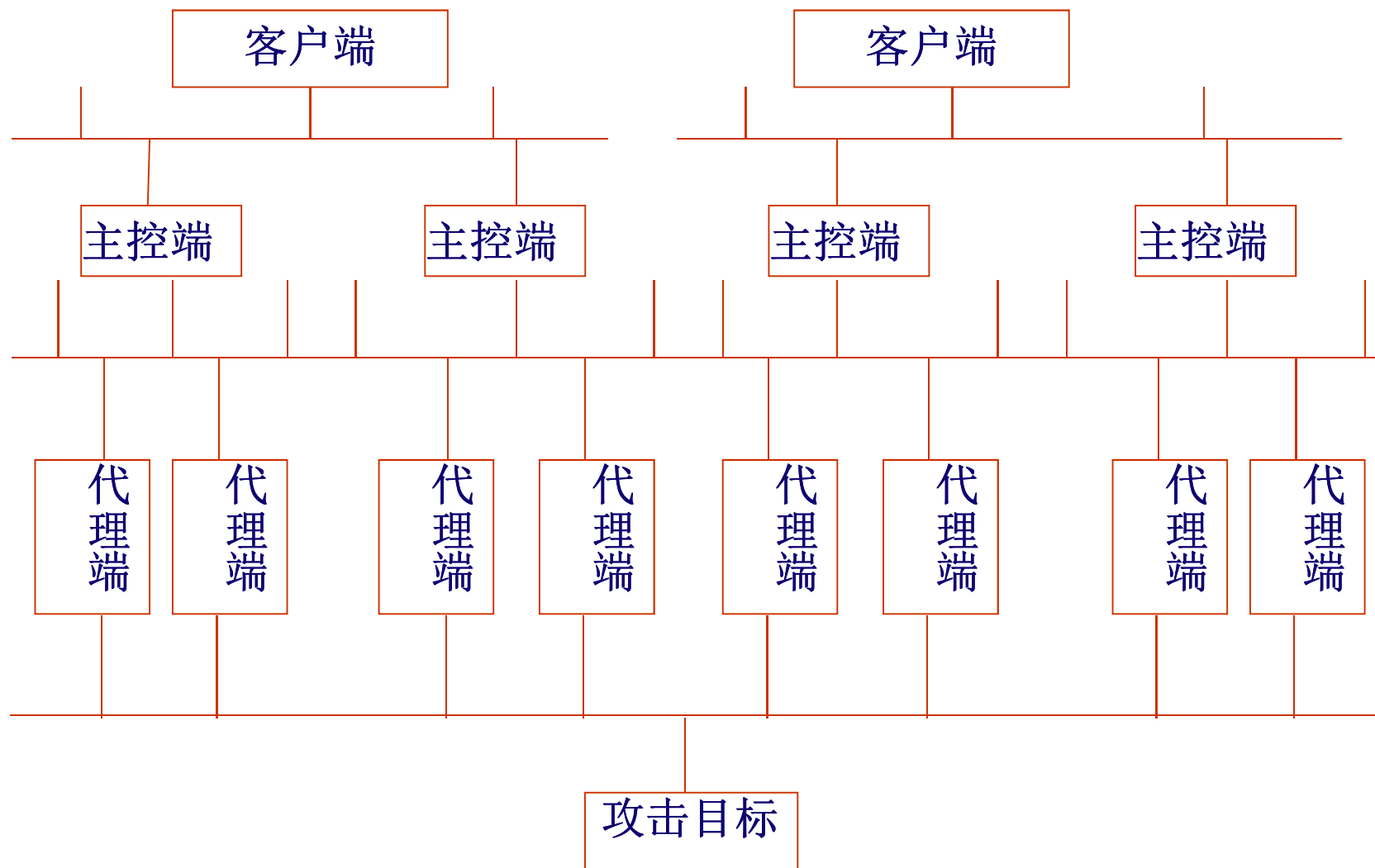
BOTNET



# 分布式拒绝服务攻击 - DDoS

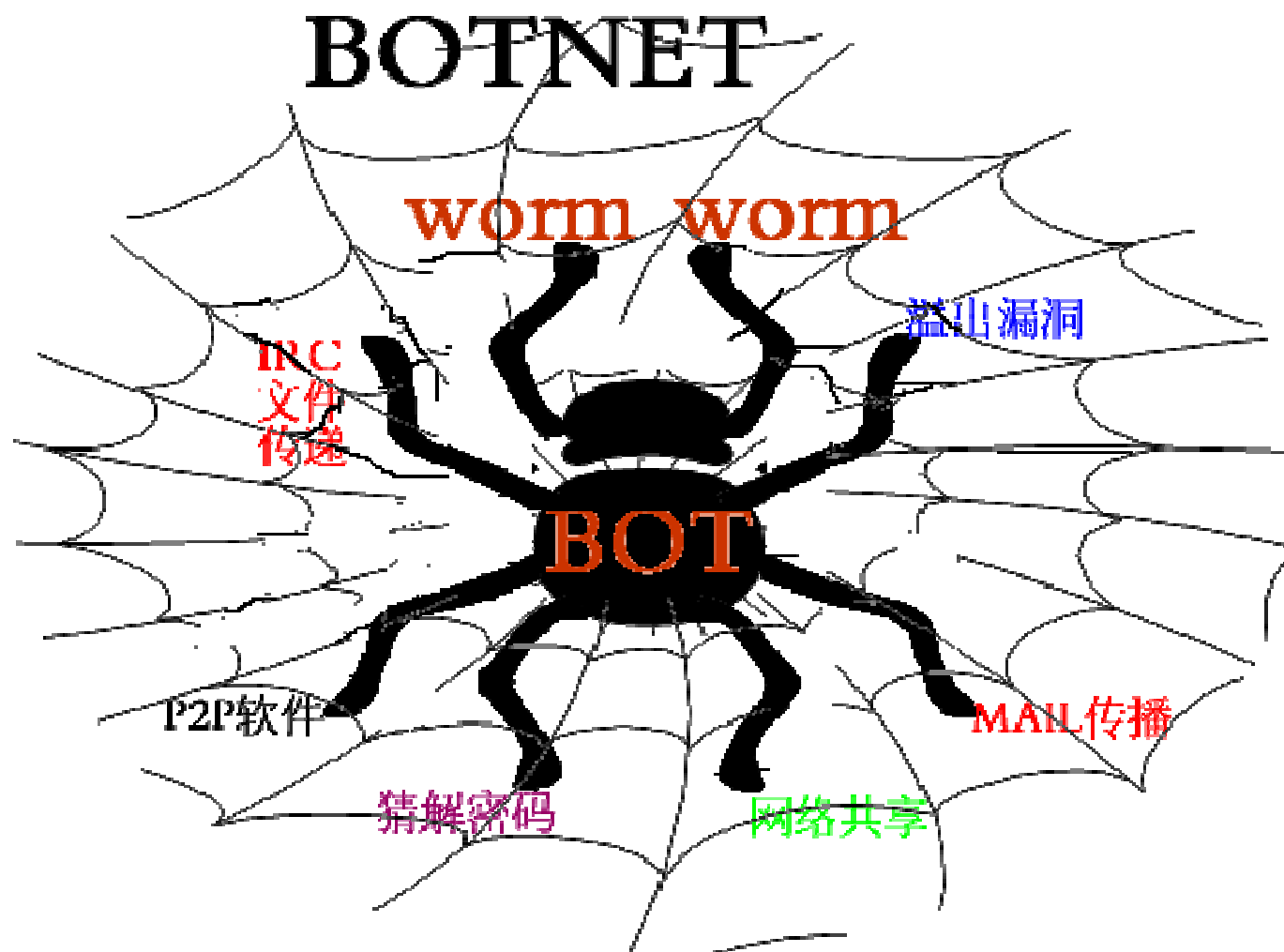
- 分布式拒绝服务攻击使用与普通的拒绝服务攻击同样的方法，但是发起攻击的源是多个。
- 主控端可以同时对一个目标发起几千个攻击。单个的拒绝服务攻击的威力也许对带宽较宽的站点没有影响，而分布于全球的几千个攻击将会产生致命的效果。
- 通常，攻击者先渗透无保护的主机，当获得该主机的适当的访问权限后，攻击者在主机中安装软件的服务或进程（以下简称代理）。这些代理保持睡眠状态，直到从它们的**主控**端得到指令。主控端命令代理对指定的目标发起拒绝服务攻击。

# 分布式拒绝服务攻击网络结构图



B0TNet – 僵尸网是当前互联网最大的威胁之

—



# DDoS 种类

- 应用层
  - 垃圾邮件、病毒邮件
  - VOIP spam(SPIT)
  - DNS
  - SNS
- 网络层
  - SYN Flood、ICMP Flood
  - 伪造
- 链路层
  - ARP 伪造报文
- 物理层
  - 直接线路破坏
  - 电磁干扰

- 堆栈突破型（利用主机/设备的漏洞）
  - 远程溢出拒绝服务攻击
  - 利用协议栈漏洞
- 流量型（利用 TCP/IP 协议缺陷）
  - SYN Flood
  - ACK Flood
  - ICMP Flood
  - UDP Flood、UDP DNS Query Flood
  - Connection Flood
  - HTTP Get Flood

# 防御措施

- 攻击者利用节点、主机或网站服务器的安全漏洞，因而要及时修补漏洞，升级系统。
- 其次，攻击者通常假冒源地址实施攻击，因此建议用户对所有结点进行入口过滤。
- 优化路由和网络结构，禁止所有不必要的服务；在多台主机中增设多IP地址，拒绝网络不用的UDP和ICMP数据包通过。

## 怎样对付正在进行的DDOS攻击？

- 检查攻击来源，通常黑客会通过很多假的IP地址发起攻击，此时，用户若能够分辨出哪些是真IP地址，哪些是假IP地址，然后了解这些IP来自哪些网段，再找网段管理员把机器关掉，即可消除攻击。
- 找出攻击者所经过的路由，把攻击屏蔽掉。若黑客从某些端口发动攻击，用户可把这些端口屏蔽掉，以狙击入侵。
- Filter
- 利用流量工程的方法
- 抗DOS产品 ， 流量清洗设备和服务