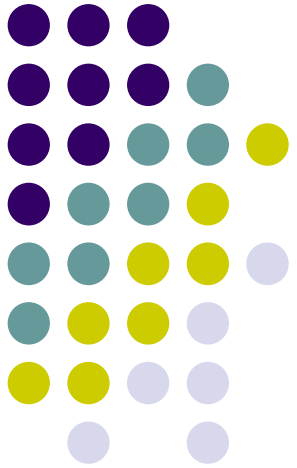
网络安全

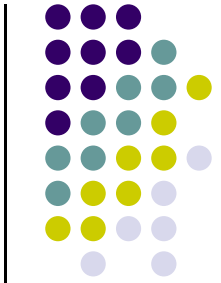
罗　敏

武汉大学计算机学院

mluo@whu.edu.cn



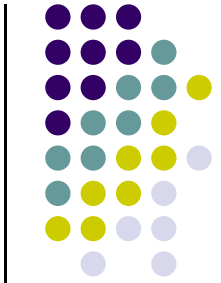
第6章 程序攻击 重点回顾



- 逻辑炸弹攻击
- 植入后门
- 病毒攻击
- 特洛伊木马攻击
- 其它程序攻击

第7章 欺骗攻击

- 欺骗攻击是网络攻击的一种重要手段。常见的欺骗攻击方式有：DNS欺骗攻击；Email欺骗攻击；Web欺骗攻击和IP欺骗攻击等。本章介绍这些主要欺骗攻击的原理、实现技术。

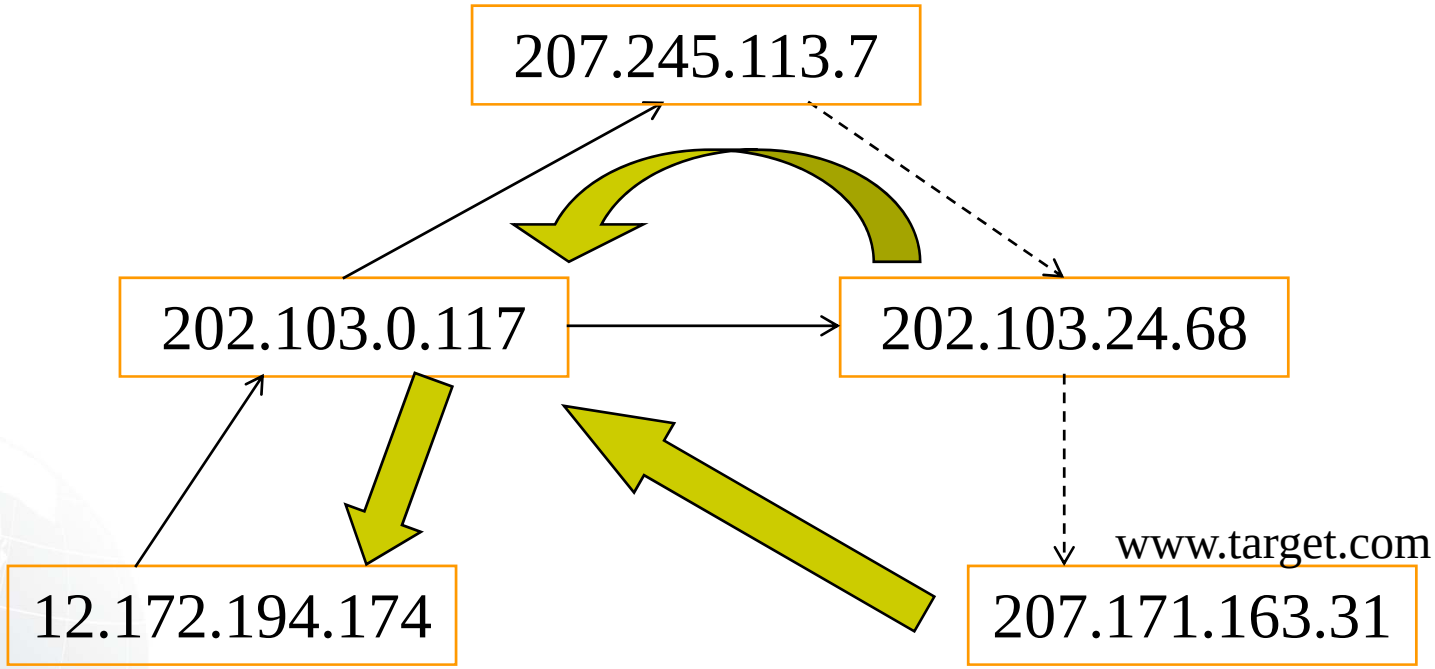


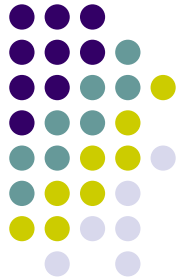
第7章 欺骗攻击

- 7.1 DNS欺骗攻击
- 7.2 Email欺骗攻击
- 7.3 Web欺骗攻击
- 7.4 IP欺骗攻击

DNS欺骗攻击

- DNS原理



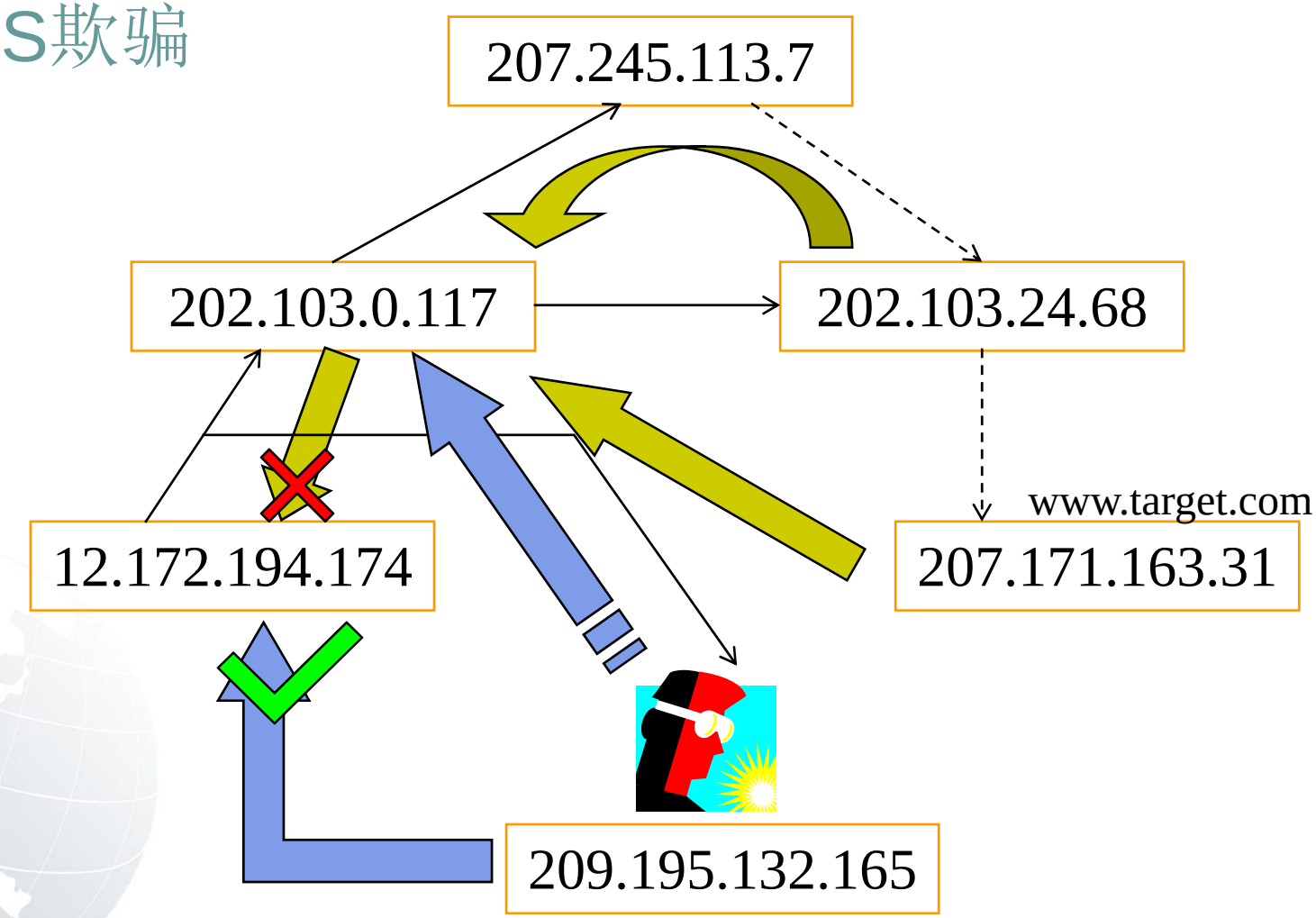


DNS欺骗攻击

- DNS欺骗原理
  - 假设当提交给某个域名服务器的域名解析请求的数据包被截获，然后按截获者的意图将一个虚假的IP地址作为应答信息返回给请求者，这时，原始请求者就会把这个虚假的IP地址作为它所要请求的域名而进行连接，显然它被欺骗到了别处而根本连接不上自己想要连接的那个域名
  - 对那个客户想要连接的域名而言，它就算是被黑掉了，因为客户由于无法得到它的正确的IP地址而无法连接上它

DNS欺骗攻击

- DNS欺骗

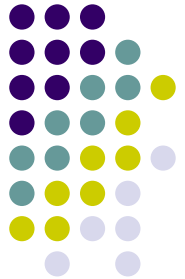


Email欺骗攻击

- Email欺骗方法
  - 攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令（口令可能为指定字符串）或在貌似正常的附件中加载病毒或其他木马程序

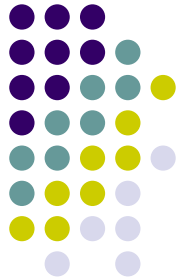
Email欺骗攻击

- Email欺骗实现步骤
  - SMTP服务器
    - 允许匿名登录
  - 填写假的名称和发信人地址
  - 使用web形式骗取密码，或者使用附件植入木马



Email欺骗攻击

- Email欺骗的防护
  - 查看邮件原文，检查真正的发件服务器地址
  - 通过邮件链接网页的时候，注意真正的网站地址
  - 在不同的应用中，尽可能使用不相同的、无关的密码



Web欺骗攻击

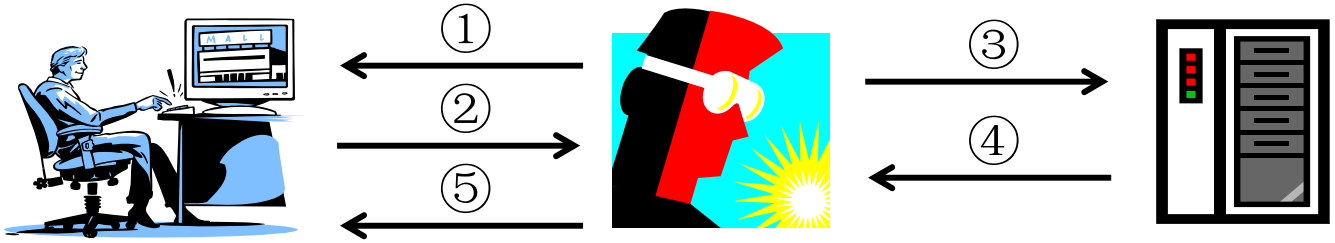
- Web欺骗攻击原理
  - 攻击者通过伪造某个WWW站点的影像拷贝，使该Web的入口进入到攻击者的Web影像服务器，并经过攻击者机器的过滤作用，从而达到攻击者监控受攻击者的任何活动以获取有用信息的目的

Web欺骗攻击

- Web是应用层上提供的服务，直接面向Internet用户，欺骗的根源在于
  - 由于Internet的开放性，任何人都可以建立自己的Web站点
  - Web站点名字(DNS域名)可以自由注册，按先后顺序
  - 并不是每个用户都清楚Web的运行规则
- Web欺骗的动机
  - 商业利益，商业竞争
  - 政治目的
- Web欺骗的形式
  - 使用相似的域名
  - 改写URL
  - 劫持Web会话

Web欺骗攻击

- 改写URL



① email with html links seems like Microsoft

② http://www.attacker.org/http://www.microsoft.com

③ http://www.microsoft.com

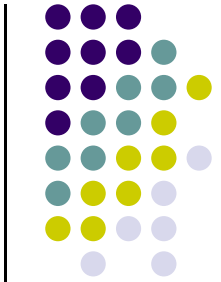
④ html page with links like : http://g.microsoft.com

⑤ html page with links like :
http://www.attacker.org/http://g.microsoft.com

使用类似的域名

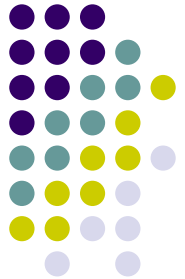
- 注册一个与目标公司或组织相似的域名，然后建立一个欺骗网站，骗取该公司的用户的信任，以便得到这些用户的信息
  - 例如，针对ABC公司，用abc.net来混淆abc.com
  - 如果客户提供了敏感信息，那么这种欺骗可能会造成进一步的危害，例如：
    - 用户在假冒的网站上订购了一些商品，然后出示支付信息，假冒的网站把这些信息记录下来(并分配一个cookie)，然后提示：现在网站出现故障，请重试一次。当用户重试的时候，假冒网站发现这个用户带有cookie，就把它的请求转到真正的网站上。用这种方法，假冒网站可以收集到用户的敏感信息。
  - 对于从事商业活动的用户，应对这种欺骗提高警惕

改写URL



- 一个HTTP页面从Web服务器到浏览器的传输过程中，如果其中的内容被修改了的话，则欺骗就会发生，其中最重要的是URL改写
  - URL改写可以把用户带到不该去的地方，例如： Welcom to Hollywood-Movie site.
  - http://3525999368 /
- 有一些更为隐蔽的做法
  - 直接指向一些恶意的代码
  - 把url定向放到script代码中，难以发现
- 改写页面的做法
  - 入侵Web服务器，修改页面
  - 设置中间http代理
  - 在传输路径上截获页面并改写
  - 在客户端装载后门程序

Web会话劫持



- HTTP协议不支持会话(无状态)，Web会话如何实现？
  - Cookie
  - 用url记录会话
  - 用表单中的隐藏元素记录会话
- Web会话劫持的要点在于，如何获得或者猜测出会话ID

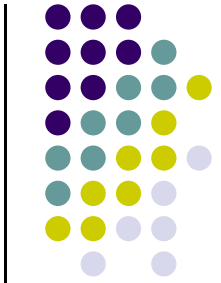
防止Web欺骗

- 使用类似的域名
  - 注意观察URL地址栏的变化
  - 不要信任不可靠的URL信息
- 改写URL
  - 查看页面的源文本可以发现
  - 使用SSL
- Web会话劫持
  - 养成显式注销的习惯
  - 使用长的会话ID
- Web的安全问题很多，我们需要更多的手段来保证Web安全

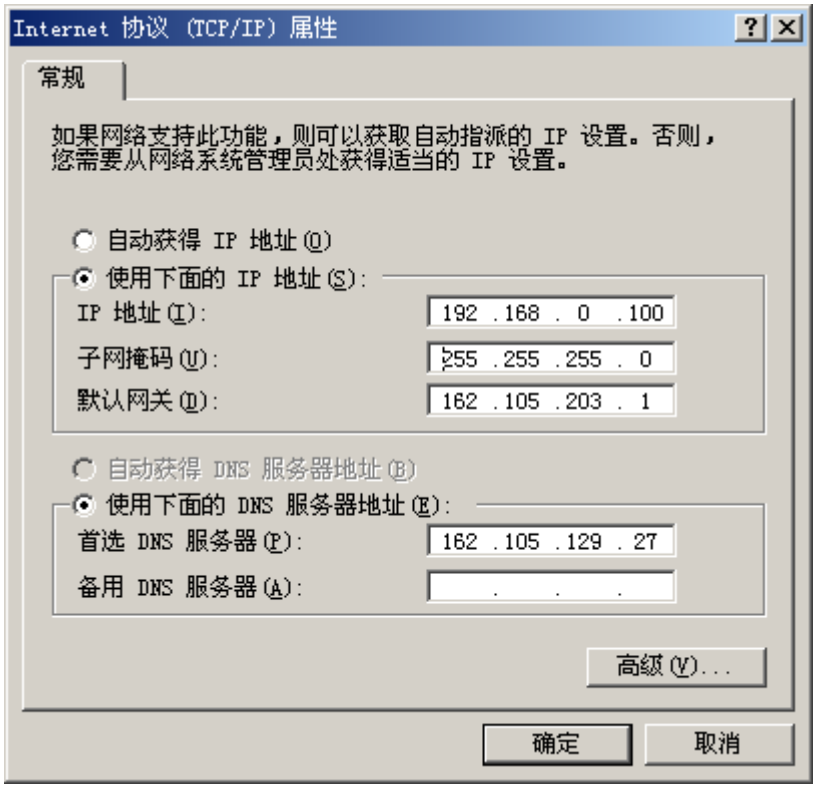
IP欺骗

- IP欺骗的动机
  - 隐藏自己的IP地址，防止被跟踪
  - 以IP地址作为授权依据
  - 穿越防火墙
- IP欺骗的形式
  - 单向IP欺骗：不考虑回传的数据包
  - 双向IP欺骗：要求看到回传的数据包
  - 更高级的欺骗：TCP会话劫持
- IP欺骗成功的要诀
  - IP数据包路由原则：根据目标地址进行路由

IP欺骗：改变自己的地址



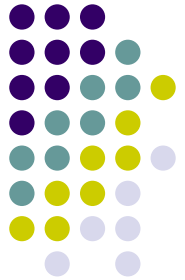
- 用网络配置工具改变机器的IP地址
- 注意：
  - 只能发送数据包
  - 收不到回包
  - 防火墙可能阻挡
- 在Linux平台上
  - 用ifconfig



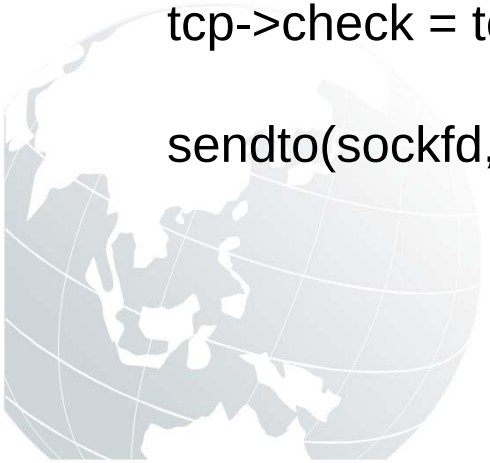
用程序实现IP欺骗

- 发送IP包，IP包头填上假冒的源IP地址
  - 在Unix/Linux平台上，直接用socket就可以发送，但是需要root权限
  - 在Windows平台上，不能使用Winsock
    - 可以使用winpcap
  - 可以用libnet构造IP包
- 代码示例
  - 在Linux平台上，打开一个raw socket，自己填写IP头和传输层数据，然后发送出去

用程序实现IP欺骗代码示例

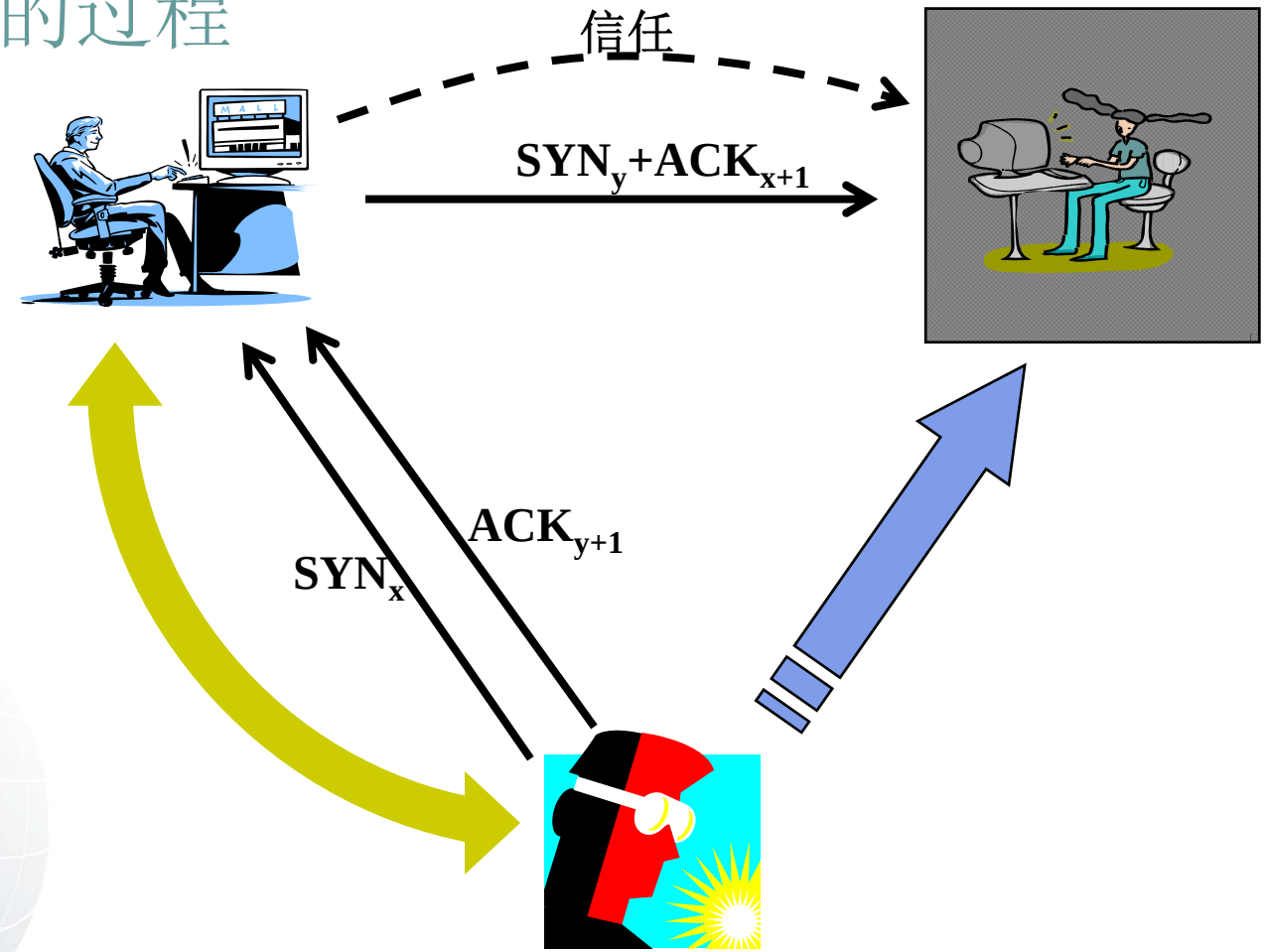


```
sockfd = socket(AF_INET, SOCK_RAW, 255);
setsockopt(sockfd, IPPROTO_IP, IP_HDRINCL, &on, sizeof(on));

struct ip *ip;
struct tcphdr *tcp;
struct pseudohdr pseudoheader;

ip->ip_src.s_addr = xxx;
// 填充IP和TCP头的其他字段，并计算校验和
pseudoheader.saddr.s_addr = ip->ip_src.s_addr;
tcp->check = tcpchksum((u_short *)&pseudoheader,
                                    12+sizeof(struct tcphdr)); //计算校验和
sendto(sockfd, buf, len, 0, (const sockaddr *)addr,
                                    sizeof(struct sockaddr_in));
```



IP欺骗攻击

- IP欺骗的过程



IP欺骗攻击

- IP欺骗的过程
  - 首先使被信任主机的网络暂时瘫痪
  - 连接到目标机的某个端口来猜测ISN基值和增加规律
  - 把源址址伪装成被信任主机，发送带有SYN标志的数据段请求连接
  - 等待目标机发送SYN+ACK包给已经瘫痪的主机
  - 再次伪装成被信任主机向目标机发送的ACK，此时发送的数据段带有预测的目标机的ISN+1
  - 连接建立，发送命令请求

如何避免IP欺骗

- 主机保护，两种考虑
  - 保护自己的机器不被用来实施IP欺骗
    - 物理防护、登录口令
    - 权限控制，不允许修改配置信息
  - 保护自己的机器不被成为假冒的对象
    - 无能为力
- 网络防护
  - 路由器上设置欺骗过滤器
    - 入口过滤，外来的包带有内部IP地址
    - 出口过滤，内部的包带有外部IP地址
- 保护免受源路由攻击
  - 路由器上禁止这样的数据包

会话(交易)劫持

- 在现实环境中，比如对于银行一笔交易
  如果营业员检查了顾客的身份证和账户卡
  抬起头来，发现不再是刚才的顾客
  他会把钱交给外面的顾客吗？

在网络上没有人知道
你是一条狗

TCP Session Hijack原理

- 所谓会话: 就是两台主机之间的一次通讯。例如你Telnet到某台主机，这就是一次Telnet会话；你浏览某个网站，这就是一次HTTP会话。
- 会话劫持（Session Hijack）：就是结合了嗅探以及欺骗技术在内的攻击手段。例如，在一次正常的会话过程当中，攻击者作为第三方参与到其中，他可以在正常数据包中插入恶意数据，也可以在双方的会话当中进行监听，甚至可以是代替某一方主机接管会话。

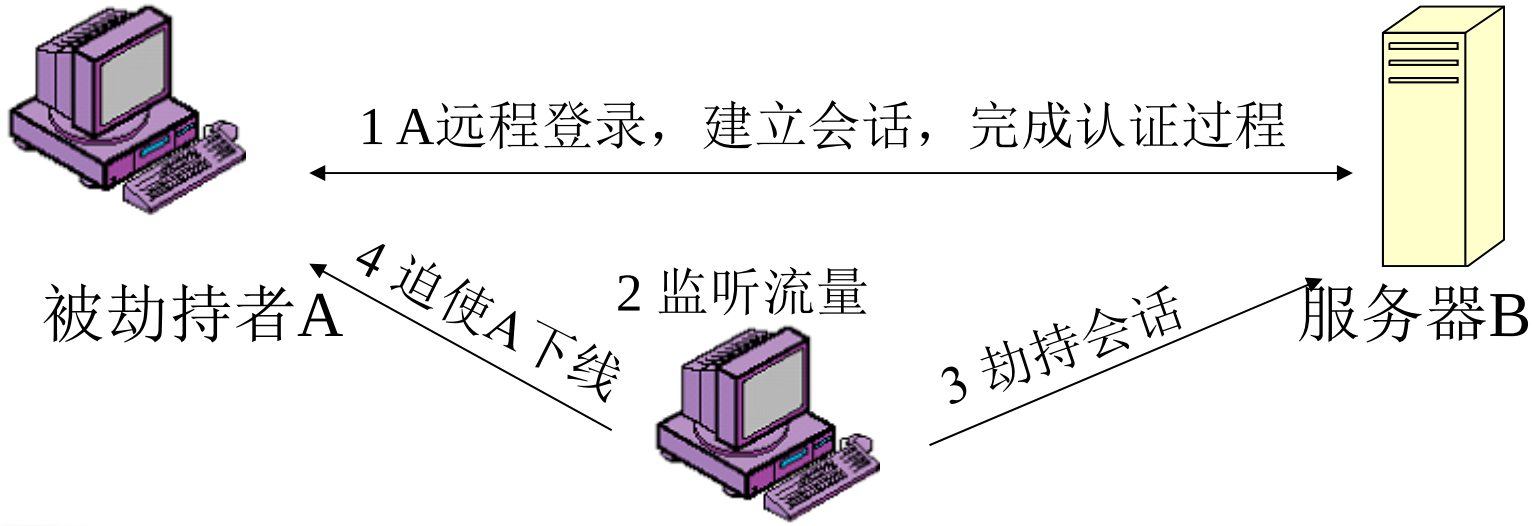
TCP会话劫持(session hijacking)

- 欺骗和劫持
  - 欺骗是伪装成合法用户，以获得一定的利益
  - 劫持是积极主动地使一个在线的用户下线，或者冒充这个用户发送消息，以便达到自己的目的
- 动机
  - Sniffer对于一次性密钥并没有用
  - 认证协议使得口令不在网络上传输

TCP Session Hijack方法

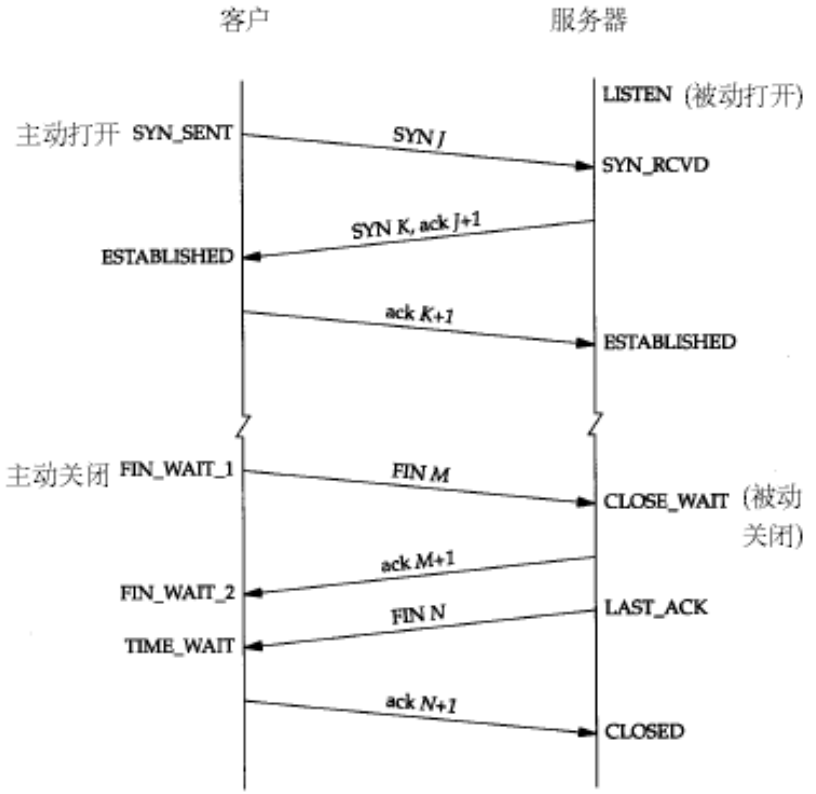
- 可以把会话劫持攻击分为两种类型：
  - 1）中间人攻击(Man In The Middle，简称MITM)；
  - 2）注射式攻击（Injection）；
- 还可以把会话劫持攻击分为两种形式：
  - 1）被动劫持:被动劫持实际上就是在后台监听双方会话的数据流，从中获得敏感数据。如在Telnet、FTP、HTTP、SMTP等传输协议中，用户和密码信息都是以明文格式传输的，若攻击者利用数据包截取工具便可很容易收集到帐户和密码信息。
  - 2）主动劫持:主动劫持则是将会话当中的某一台主机“踢”下线，然后由攻击者取代并接管会话，这种攻击方法危害非常大，攻击者可以做很多事情，比如“cat etc/master.passwd”（FreeBSD下的Shadow文件）

会话劫持示意图



会话劫持的原理

- TCP协议
  - 三次握手建立TCP连接(即一个TCP会话)
  - 终止一个会话，正常情况需要4条消息
  - 如何标识一个会话：
    状态：源IP:端口+SN <> 目标IP:端口+SN
- 从TCP会话的状态入手
  - 要了解每一个方向上的SN(数据序列号)
    - 两个方向上的序列号是相互独立的
    - TCP数据包，除了第一个SYN包之外，都有一个ack标志，给出了期待对方发送数据的序列号
  - 所以，猜测序列号是成功劫持TCP会话的关键



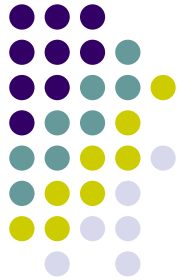
TCP Session Hijack原理

- 根据TCP/IP中的规定，使用TCP协议进行通讯需要提供两段序列号，TCP协议使用这两段序列号确保连接同步以及安全通讯，系统的TCP/IP协议栈依据时间或线性的产生这些值。
- 在通讯过程中，双方的序列号是相互依赖的，如果攻击者直接进行会话劫持，结果肯定是失败的。因为会话双方“不认识”攻击者，攻击者不能提供合法的序列号;所以，会话劫持的关键是预测正确的序列号，攻击者可以采取嗅探技术获得这些信息。

关于TCP协议的序列号

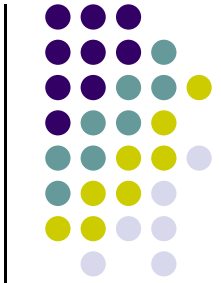
- 在每一个ACK包中，有两个序列号
  - 第一个(SEG_SEQ)是当前包中数据第一个字节的序号
  - 第二个(SEG_ACK)是期望收到对方数据包中第一个字节的序号
- 假设客户(CLT)向服务器(SVR)发起一个连接，我们用以下的表示
  - SVR_SEQ: 服务器将要发送的下一个字节的序号
  - SVR_ACK: 服务器将要接收的下一个字节的序号(已经收到的最后一个字节的序号加1)
  - SVR_WIND: 服务器的接收窗口
  - CLT_SEQ: 客户将要发送的下一个字节的序号
  - CLT_ACK: 客户将要接收的下一个字节的序号
  - CLT_WIND: 客户的接收窗口
- 关系
  - CLT_ACK <= SVR_SEQ <= CLT_ACK + CLT_WIND
  - SVR_ACK <= CLT_SEQ <= SVR_ACK + SVR_WIND
  - 只有满足这样条件的包，对方才会接收
  - 否则，该包被丢掉，并且送回一个ACK包(含有期望的序列号)

TCP滑动窗口



- 1，当TCP从文件中接收数据时，数据位于send窗口。TCP将一个带有序列号的报头加入数据包并将其交给IP，由IP将它发送到目标主机。
  2，当每一个数据包传送时，客户机设置重传计时器，描述在重新发送数据包之前将等待ACK多久。在SEND窗口中有每一个数据包的备分，直到收到ACK。
  3，当数据包到达服务器RECEIVE窗口，它们按照序列号放置。当接收到连续的段时间就向用户机发送一个关于数据的认可，其中带有当前窗口尺寸。
  4，一旦客户机接收到认可，SEND窗口将由已获得认可的数据滑动到等待发送的数据。如果在重发计时器设定的时间内，客户机没有接收到对现存数据的认可，数据将重新发送。重发数据包将加重网络和客户机的负担。
  5，如果数据包接收到时顺序错乱，那么将强制延迟ACK计时器发送认可。

关于TCP协议的序列号(续)



- 同步状态
  - SVR_SEQ = CLT_ACK
  - CLT_SEQ = SVR_ACK
- 不同步状态
  - SVR_SEQ != CLT_ACK
  - CLT_SEQ != SVR_ACK
- 如果TCP连接进入到一种不同步的状态
  - 客户发送一个包
    SVR_SEQ = CLT_SEQ
    SVR_ACK = CLT_ACK
    这个包不会被接收，因为CLT_SEQ != SVR_ACK
  - 相反，如果第三方(攻击者)发送一个包
    CLT_SEQ = SVR_ACK
    CLT_ACK = SVR_SEQ
    这个包可以被服务器接收
  - 如果攻击者能够伪造两边的包的话，还可以恢复客户和服务器之间的会话，使得回到同步状态

TCP ACK Storm

- 当一个主机接收到一个不期望的数据包的时候，它会用自己的序列号发送ACK，而这个包本身也是不可被接受的。于是，两边不停地发送ACK包，形成ACK包的循环，是为ACK风暴。
- 如果有一个ACK包丢掉，则风暴停止
- 在不同步的情况下，当服务器发送数据给客户
  - 如果攻击者不对这份数据响应ACK的话，这份数据会被重传，因为服务器收不到ACK，并且会形成ACK风暴，最终，连接会被终止
  - 如果攻击者对这份数据作出响应，则只有一个ACK风暴

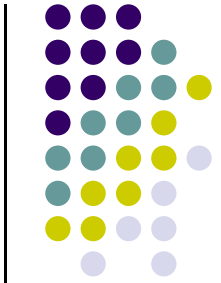
如何到达不同步的状态(一)

- 在建立连接的时候劫持会话
  - 当攻击者听到握手过程第二步的时候，它给服务器发送一个RST包，然后发送用同样的TCP和端口号构造的一个SYN包，但是序列号与前面的SYN包不同
  - 服务器关闭第一个连接，打开第二个连接，并且送回第二个SYN/ACK给客户，攻击者听到这个包之后，给服务器送出一个ACK包
  - 至此，客户、服务器、攻击者都进入到TCP ESTABLISHED状态，但是攻击者和服务器之间是同步的，而客户和服务器之间是不同步的
  - 注意，攻击者选择的序列号与客户的序列号一定要不同，否则不能成功

如何到达不同步的状态(二)

- 给一方发送空数据
  - 攻击者首先观察会话
  - 然后，给服务器发送一些无关紧要的数据，这些数据会导致服务器的序列号发生变化
  - 攻击者给客户也可以发送数据
- 这种手段成功的要点在于
  - 可以发送一些无关紧要的数据，并且能够把握发送的时机

不在一个子网中的劫持(欺骗)手法

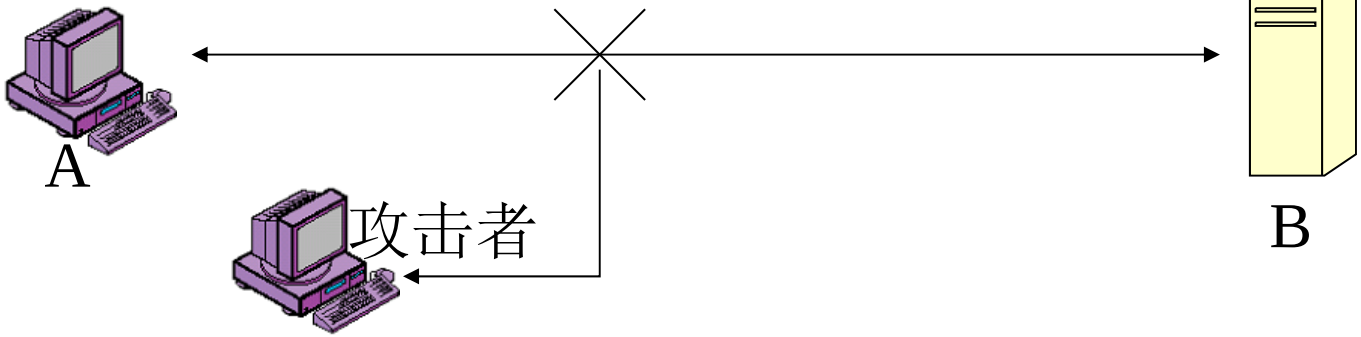


- 有时候也称作“Blind spoofing”
- 攻击者发送一个SYN包
- 然后猜测服务器的ISN
- 只要能够猜得到，就可以建立连接
- 但是攻击者收不到服务器给客户的包
  - 使用源路由技术？
- 条件：
  - 真正的客户不能发送RST包
  - 攻击者能够猜测服务器每个包的大小

实施会话劫持的一般性过程

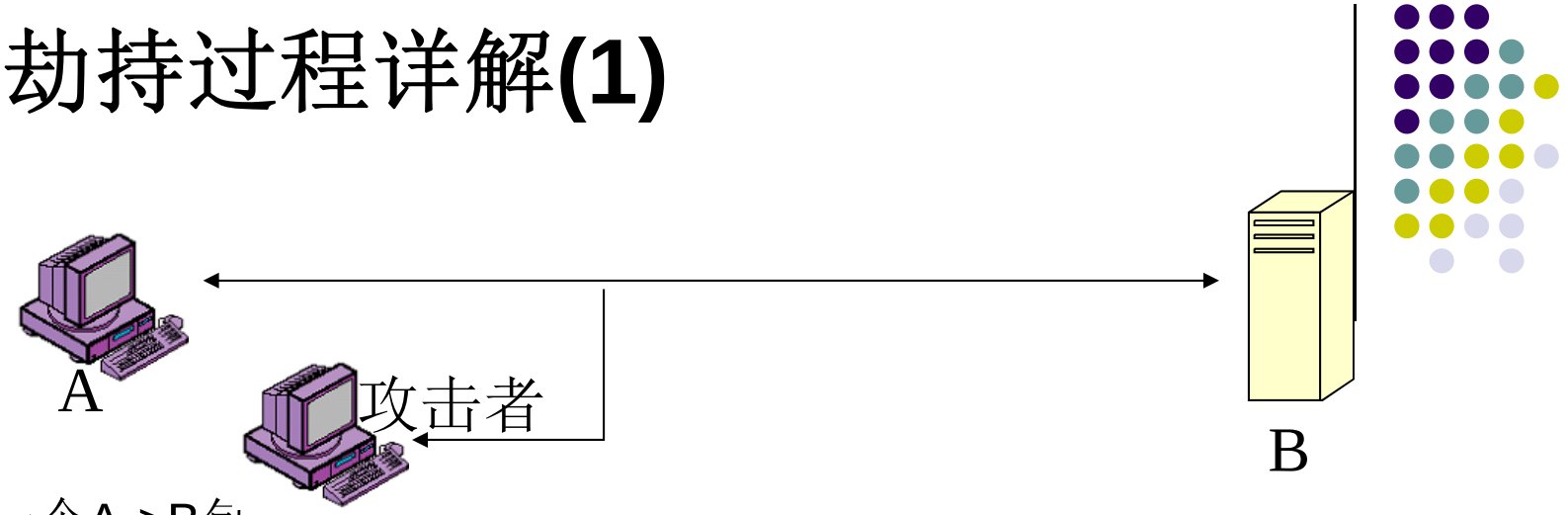
- 发现目标
  - 找到什么样的目标，以及可以有什么样的探查手段，取决于劫持的动机和环境
- 探查远程机器的ISN(初始序列号)规律
  - 可以用nmap，或者手工发起多个连接
- 等待或者监听会话
  - 最好在流量高峰期间进行，不容易被发现，而且可以有比较多可供选择的会话
- 猜测序列号
  - 这是最为关键的一步，如果不在一个子网中，难度将非常大
- 使被劫持方下线
  - ACK风暴，拒绝服务
- 接管会话
  - 如果在同一个子网中，则可以收到响应，否则要猜测服务器的动作

Kill a connection



- 攻击者发送一个RST包给B，并且假冒A的IP地址
  - 观察A和B之间的数据往来，算出A和B的序列号，在适当的时机插入一个RST包，只要在插入点上，序列号正确，则RST包就会被接受，从而达到目的
- 攻击者发送一个FIN包给B，并且假冒A的IP地址
  - 同样地，在适当的时机给B发送一个FIN包
  - 这时候，A怎么办？

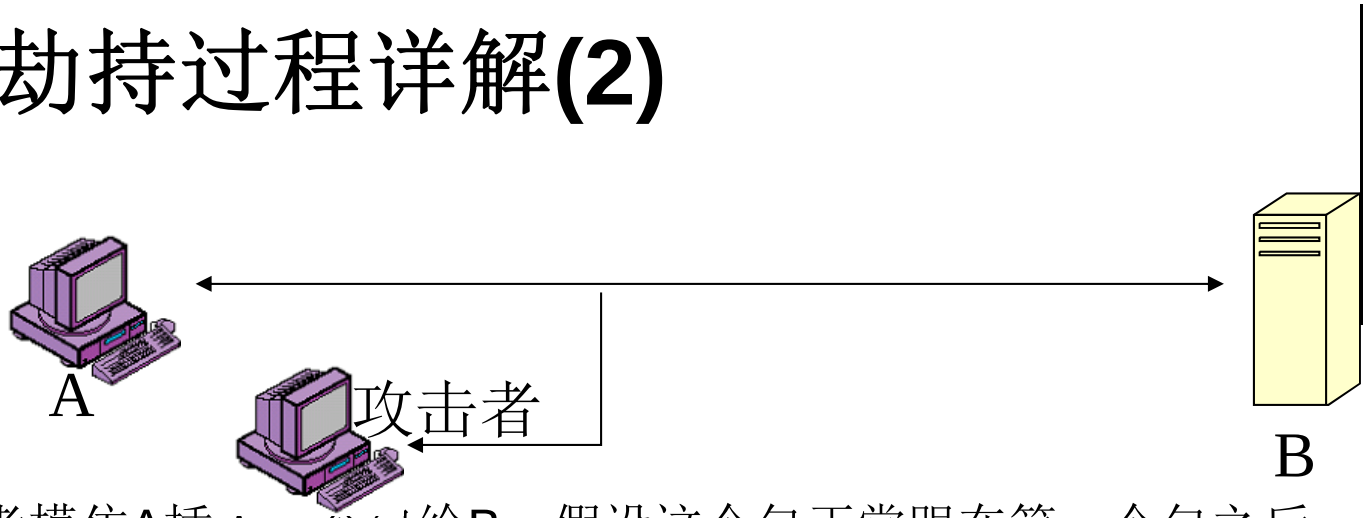
会话劫持过程详解(1)



- 看到一个A->B包
  TCP Packet ID (from_IP.port-to_IP.port): IP_A.PortA-IP_B.PortB
  SEQ (hex): 5C8223EA　ACK (hex): C34A67F6
  FLAGS: -AP---　Window: 7C00，包长为1

  - B回应一个包，B->A
    TCP Packet ID (from_IP.port-to_IP.port): IP_B.PortB-IP_A.PortA
    SEQ (hex): C34A67F6　ACK (hex): 5C8223EB
    FLAGS: -AP---　Window: 2238，包长为1
  - A回应一个包，A->B
    TCP Packet ID (from_IP.port-to_IP.port): IP_A.PortA-IP_B.PortB
    SEQ (hex): 5C8223EB　ACK (hex): C34A67F7
    FLAGS: -A----　Window: 7C00，包长为0

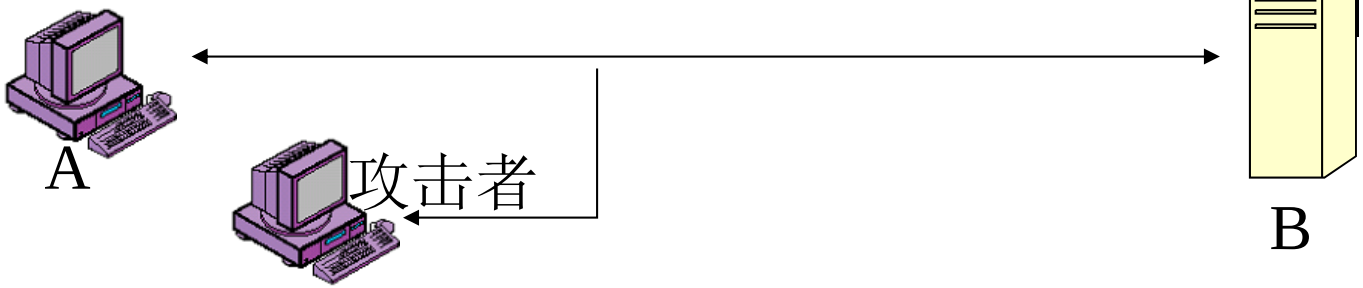
会话劫持过程详解(2)



- 攻击者模仿A插入一个包给B，假设这个包正常跟在第一个包之后
  TCP Packet ID (from_IP.port-to_IP.port): IP_A.PortA-IP_B.PortB
  SEQ (hex): 5C8223EB　ACK (hex): C34A67F7
  FLAGS: -AP---　Window: 7C00，包长为10(一定的长度)

- B回应一个包，B->A
  TCP Packet ID (from_IP.port-to_IP.port): IP_B.PortB-IP_A.PortA
  SEQ (hex): C34A67F7　ACK (hex): 5C8223F5
  FLAGS: -AP---　Window: 2238，包长不定(比如20)
- 此时，A会按照它所理解的SEQ/ACK发送包
  TCP Packet ID (from_IP.port-to_IP.port): IP_A.PortA-IP_B.PortB
  SEQ (hex): 5C8223EB　ACK (hex): C34A67F7
  FLAGS: -A----　Window: 7C00
  一阵广播风暴

会话劫持过程详解(3)

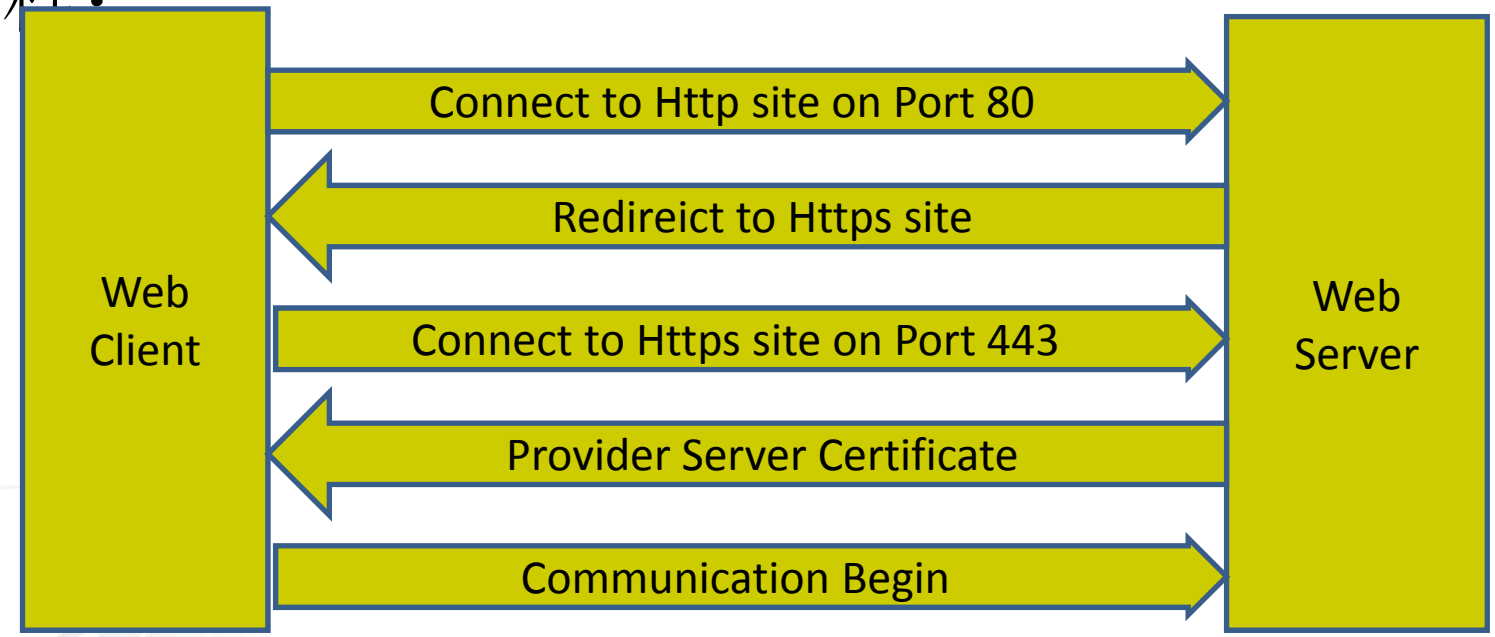


- 攻击者已经劫持了会话，它可以与B正常通讯(用A的地址)
  TCP Packet ID (from_IP.port-to_IP.port): IP_A.PortA-IP_B.PortB
  SEQ (hex): 5C8223F5　ACK (hex): C34A680B
  FLAGS: -AP---　Window: 7C00，包长不定(比如37)

  - B回应这个包，B->A
    TCP Packet ID (from_IP.port-to_IP.port): IP_B.PortB-IP_A.PortA
    SEQ (hex): C34A680B　ACK (hex): 5C82241A
    FLAGS: -AP---　Window: 2238，包长不定
  - ……

Https会话劫持之SSLStrip （1）

- 一般HTTPS通信过程：



Https会话劫持之SSLStrip （2）

以访问Gmail为例的基本过程如下：

1. 客户端浏览器使用HTTP连接到端口80的http://mail.google.com；
2. 服务器试用HTTP代码302重定向客户端HTTPS版本的这个网站；
3. 客户端连接到端口443的网站https://mail.google.com；
4. 服务器向客户端提供包含其电子签名的证书，该证书用于验证网址；
5. 客户端获取该证书，并根据信任证书颁发机构列表来验证该证书；
6. 加密通信建立。

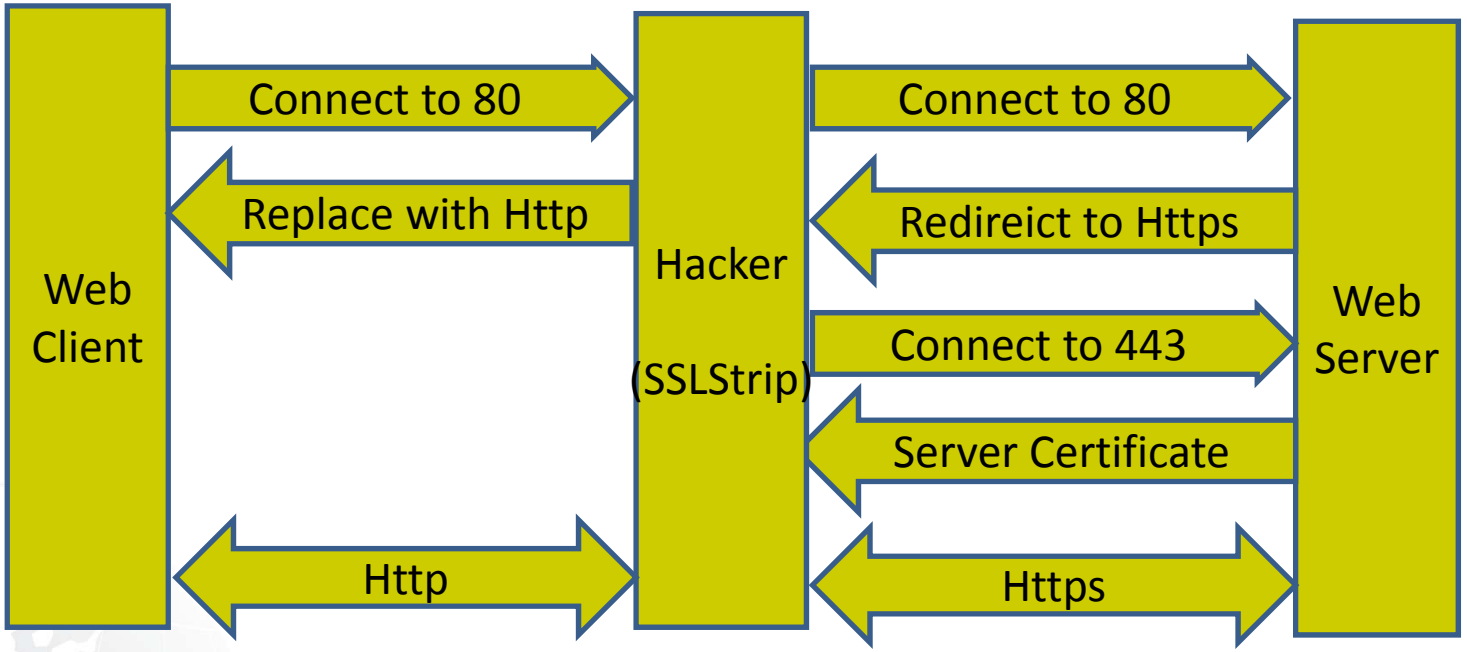
如果证书验证过程失败的话，则意味着无法验证网址的真实度。这样的话，用户将会看到页面显示证书验证错误，或者他们也可以选择冒着危险继续访问网站，因为他们访问的网站可能是欺诈网站。

Https会话劫持之SSLStrip （3）

- SSLstrip工作原理：
  - SSLstrip通过监视Http传输进行工作，当用户试图进入加密的https会话时它充当代理。当用户认为安全的会话已经开始时，SSLstrip也通过https连接到安全服务器，所有用户到SSLstrip的连接是http，这就意味着浏览器上警告提示已经被阻止，浏览器看起来正常工作，在此期间所有的用户敏感信息都可以轻易被截获。

Https会话劫持之SSLStrip （4）

SSLstrip工作原理:



Https会话劫持之SSLStrip （5）

- 劫持HTTPS通信

1. 客户端与web服务器间的流量被拦截;
2. 当遇到HTTPS URL时，sslstrip使用HTTP链接替换它，并保存了这种变化的映射;
3. 攻击机模拟客户端向服务器提供证书;
4. 从安全网站收到流量提供给客户端;

这个过程进展很顺利，服务器仍然在接收SSL流量，服务器无法辨别任何改变。用户可以感觉到唯一不同的是，浏览器中不会标记HTTPS，所以某些用户还是能够看出不对劲。

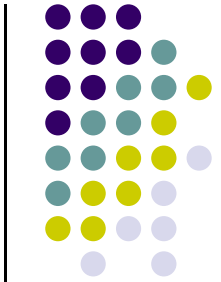
关于会话劫持的参考

- 三篇文章
  - Simple Active Attack Against TCP, http://www.insecure.org/stf/iphijack.txt
  - A short overview of IP spoofing: PART I, http://staff.washington.edu/dittrich/papers/IP-spoof-1.txt
  - A short overview of IP spoofing: PART II , http://staff.washington.edu/dittrich/papers/IP-spoof-2.txt
- **“Hackers Beware”**，中文版《黑客——攻击透析与防范》，第五章“会话劫持”

进行会话劫持的工具

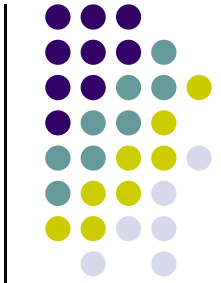
- 前页后两篇文章带了一些源码
- Juggernaut
  - 可以进行TCP会话攻击的网络sniffer程序
- Hunt
  - 功能与Juggernaut类似
- TTY Watcher
  - 免费程序，针对单一主机上的连接
- IP Watcher
  - 商用的会话劫持工具

Hunt工具介绍

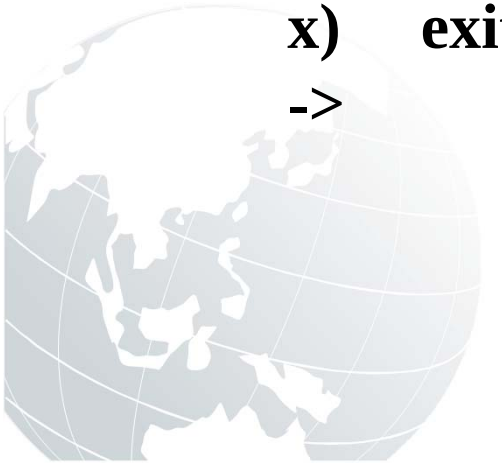


- 源码开放的自由软件，可运行在Linux平台上
- 功能特点
  - 监听当前网络上的会话
  - 重置会话(reset a session)
  - 劫持会话
    - 在劫持之后，使连接继续同步
  - 确定哪些主机在线
  - 四个守护进程
    - 自动reset
    - Arp欺骗包的转发
    - 收集MAC地址
    - 具有搜索功能的sniffer

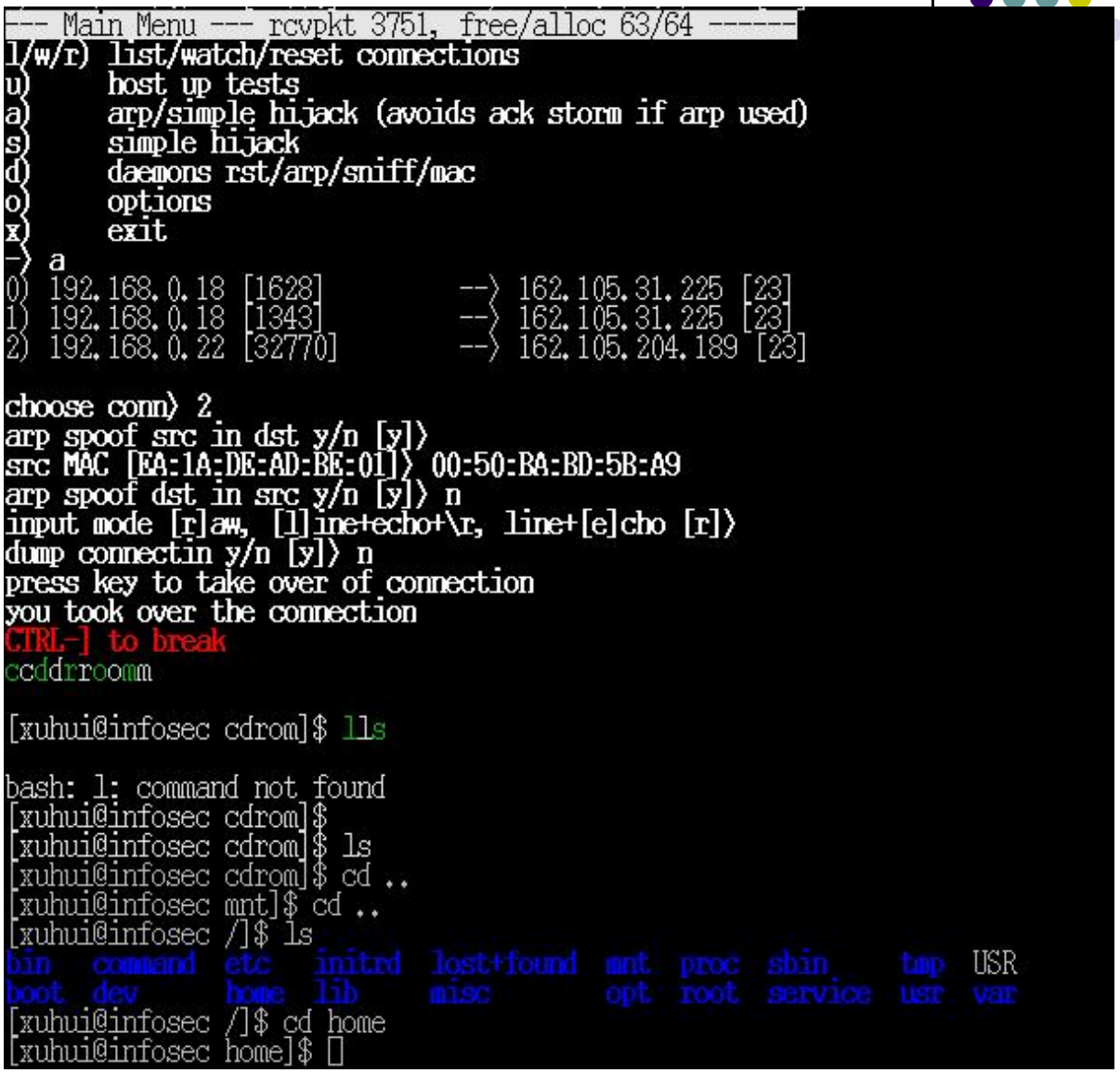
Hunt主菜单



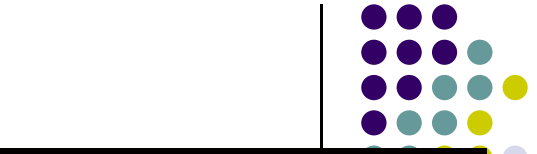
l/w/r) list/watch/reset connections
u) host up tests
a) arp/simple hijack (avoids ack storm if arp used)
s) simple hijack
d) daemons rst/arp/sniff/mac
o) options
x) exit
->



用hunt接管会话

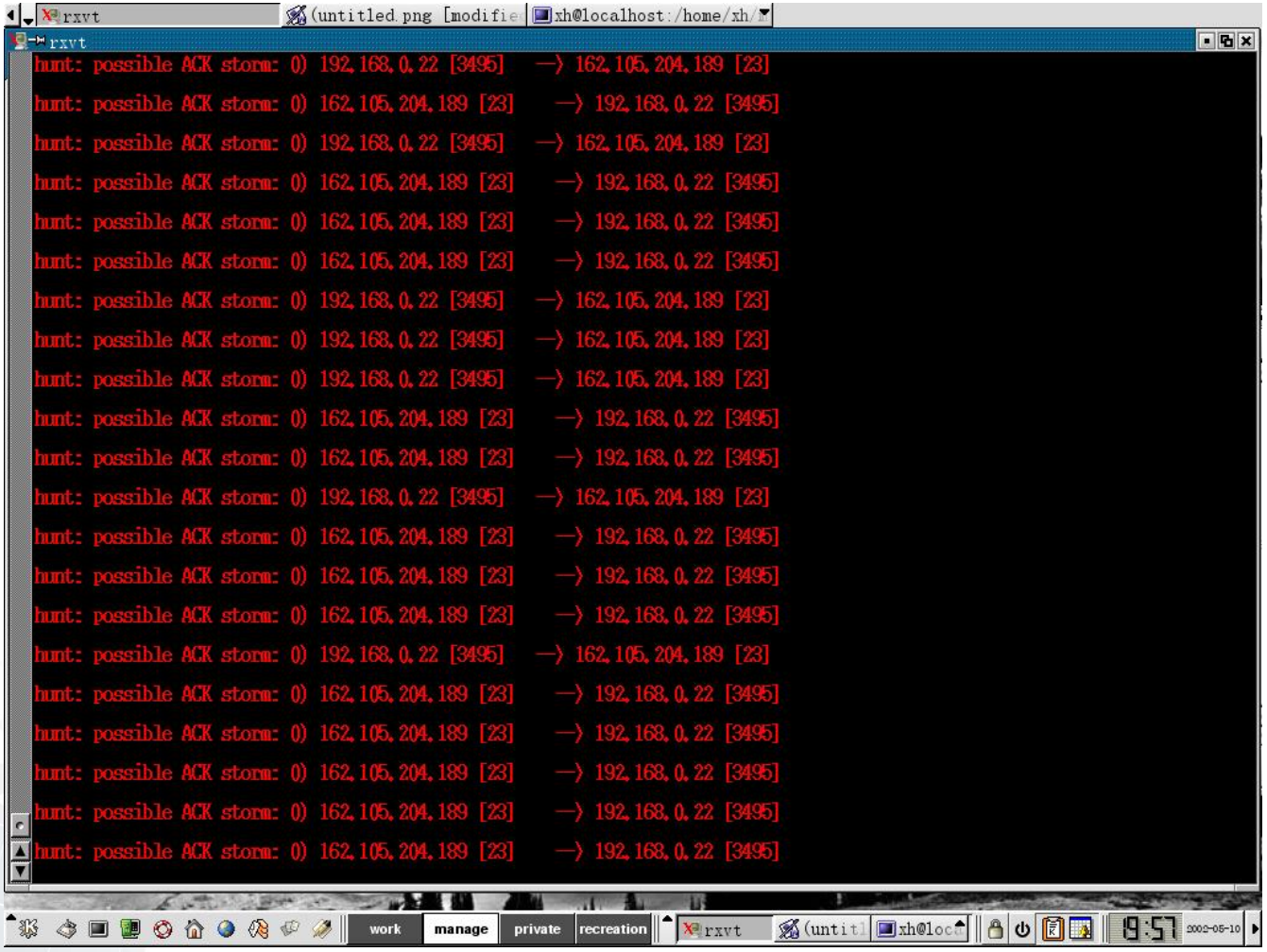

--- Main Menu --- rcvpkt 3751, free/alloc 63/64 ------
l/w/r) list/watch/reset connections
u) host up tests
a) arp/simple hijack (avoids ack storm if arp used)
s) simple hijack
d) daemons rst/arp/sniff/mac
o) options
x) exit
-> a
0) 192.168.0.18 [1628] --> 162.105.31.225 [23]
1) 192.168.0.18 [1343] --> 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: 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]$

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  shin    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劫持会话时听到的ACK风暴

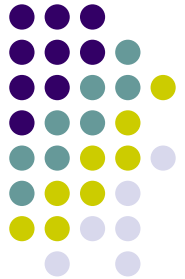


如何防止会话劫持

- 部署共享式网络，用交换机代替集线器
- TCP会话加密
- 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包的数量明显增加

第7章 欺骗攻击

- DNS欺骗攻击
- Email欺骗攻击
- Web欺骗攻击
- IP欺骗攻击



第7章 欺骗攻击

- 课后习题
  - 请简述DNS的工作原理，并指出在整个DNS解析过程中，可能存在的被欺骗攻击的地方。
  - 假如你的主机正在面临DNS欺骗攻击，你打算采取什么解决策略和方案？
  - Web欺骗攻击有哪些具体形式？请简述其原理。
  - 假如你负责开发、维护和管理某商业网站，面对潜在的Web欺骗攻击，你将采取哪些手段避免你的网站受到攻击？