网络安全 – 欺骗攻击

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

上周回顾 - 1

缓冲溢出的原因

缓冲区溢出攻击的危害

缓冲溢出攻击的原理

缓冲区溢出攻击的防御技术

上周回顾 - 2

逻辑炸弹、木马、蠕虫、后门

特洛伊木马工作原理

主动，反弹，嵌入式木马

木马的启动技术和隐藏技术

DNS欺骗攻击

Email、Web欺骗攻击

IP欺骗攻击

DNS欺骗攻击

Email、Web欺骗攻击

IP欺骗攻击

为什么需要DNS

域名系统(Domain Name System,DNS)是Internet上解决网上机器命名的一种系统。

就像拜访朋友要先知道别人家怎么走一样，Internet上当一台主机要访问另外一台主机时，必须首先获知其地址，TCP/IP中的IP地址是由四段以“.”分开的数字组成(此处以IPv4的地址为例，IPv6的地址同理)，记起来总是不如名字那么方便，所以，就采用了域名系统来管理名字和IP的对应关系。

DNS工作原理

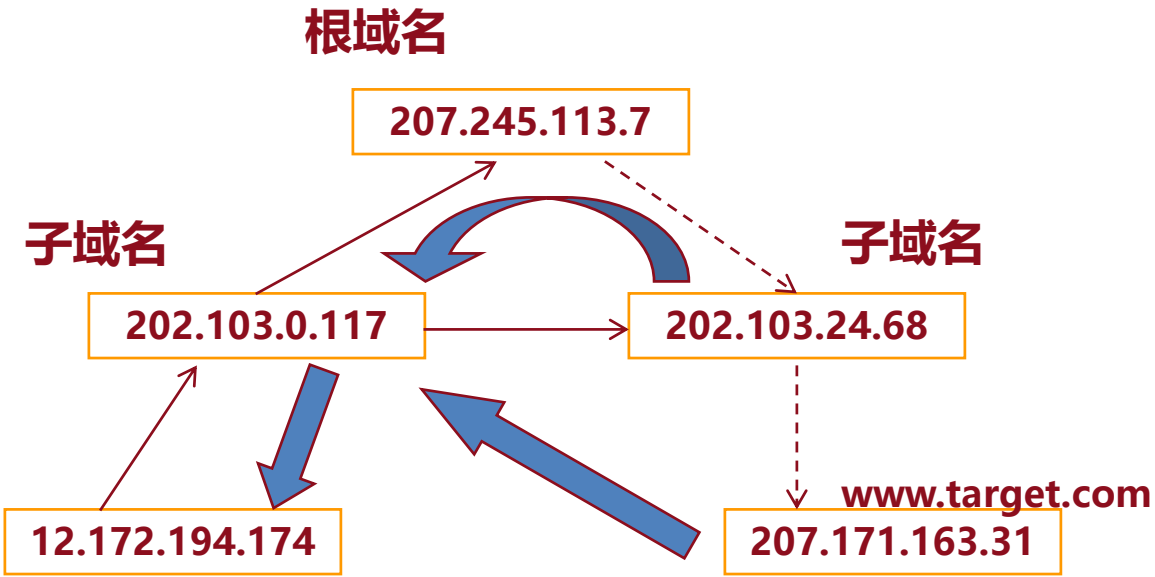
分布式、层次式的客户端/服务端数据库管理系统

提供域名与IP地址的转换

使用主机域名更方便，对服务提供方更容易将自身品牌内容反映在域名

每个登记的域将自己数据复制给整个网络

DNS查询


根域名
207.245.113.7
子域名
子域名
202.103.0.117
202.103.24.68
www.target.com
12.172.194.174
207.171.163.31

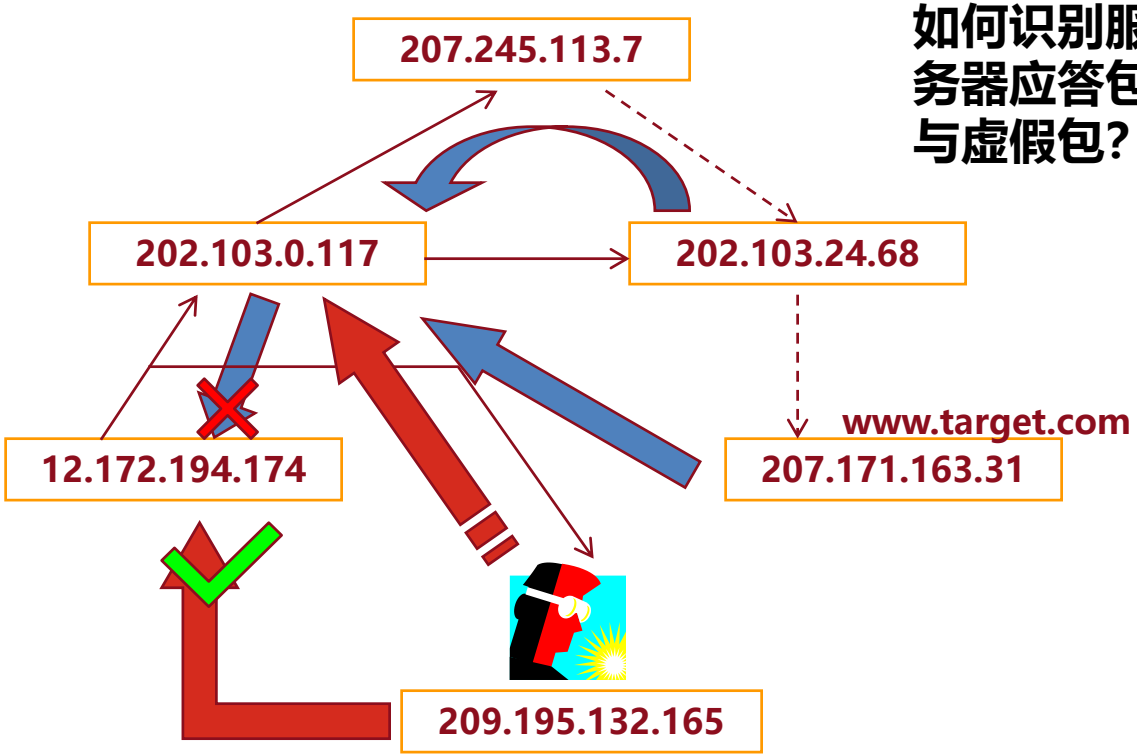
DNS欺骗 – 攻击原理

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 – 攻击实例



如何识别服务器应答包与虚假包?

执行DNS欺骗攻击的方法和防护

执行DNS欺骗攻击的方法包括：

- 中间人（MITM） - 拦截用户和DNS服务器之间的通信，以便将用户路由到不同的/恶意的IP地址。
- DNS服务器危害 - 直接劫持DNS服务器，该服务器配置为返回恶意IP地址。

域名服务器安全DNSSEC是一种通过添加其他验证方法来保护您的DNS的协议。该协议创建一个存储在DNS记录旁边的唯一密码签名，例如A记录和CNAME。然后，DNS解析器使用此签名来验证DNS响应，确保记录未被篡改。

DNS欺骗攻击

Email、Web欺骗攻击

IP欺骗攻击

Email欺骗

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）

在貌似正常的附件中加载病毒或其他木马程序

针对Email应用，除了Email欺骗，还有哪种攻击方式?

Email欺骗

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

应对

- 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 – 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

使受害者信任攻击者制造的虚假信息（页面，链接，图标，表单等）

- 决策
- 暗示

Web欺骗攻击 – 特征

欺骗根源：

- 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
- 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

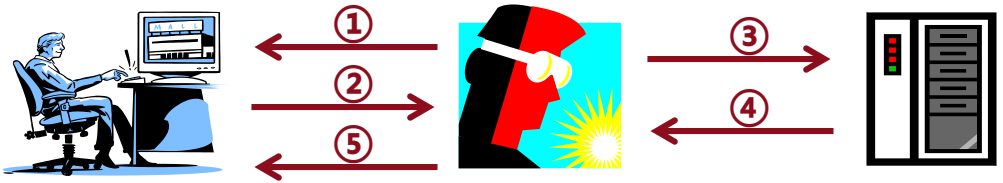
- 使用相似的域名
- 改写URL
- 劫持Web会话

Web欺骗 – 使用相似的域名

注册与目标公司或组织相似的域名，建立一个欺骗网站，骗取用户信任，以便得到用户信息

- 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。

Web欺骗 – 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

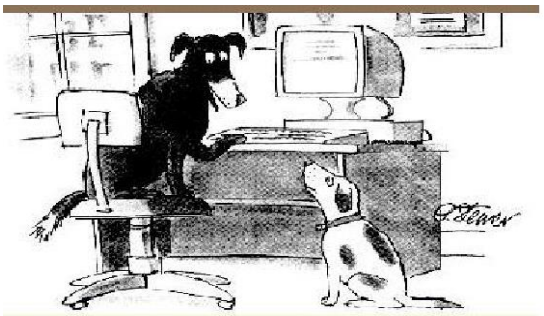
⑤ html page with links like :
http://www.attacker.org/http://g.microsoft.com

Web欺骗 – Web会话劫持

HTTP协议不支持会话(无状态)，Web会话如何实现?

- Cookie
- 认证

Web会话劫持的要点在于，如何获得或者猜测出会话ID



在网络上没有
人知道你
是一条狗

防止Web欺骗

短期方案

- 禁止浏览器JavaScript，各类改写信息原形毕露
- 确保浏览器连接状态可见，提供当前位置各类信息
- 不信任不可靠的URL信息

长期方案

- 改变浏览器，使之具有反应真是URL信息的功能
- 对于通过安全链接建立的Web，关注另一端身份

DNS欺骗攻击

Email、Web欺骗攻击

IP欺骗攻击

IP欺骗攻击

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

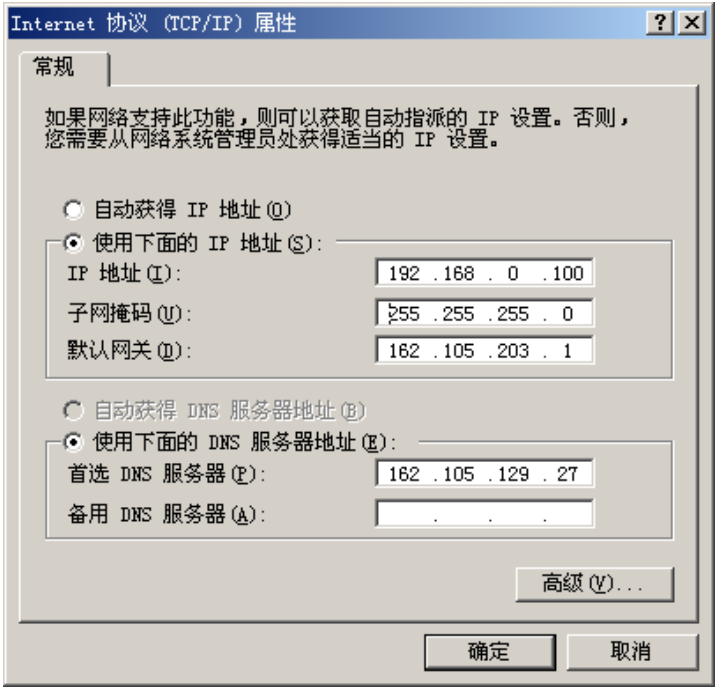
用网络配置工具改变机器的IP地址

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**



IP欺骗中的信任关系

- 两个主机A、B
- 用户C

用户在主机A、B上登录，需要输入自己的账户，主机将系统中的C的账户当成两个不相关的用户

创建.rhosts文件，使用户在A、B上可以使用远程调用命令，互相登录

冒充B的IP?

IP欺骗

通过伪造IP地址能够获得更多的收益或者权限

伪造的IP地址可以被接受而不被发现

```
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));
```

TCP会话劫持

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**

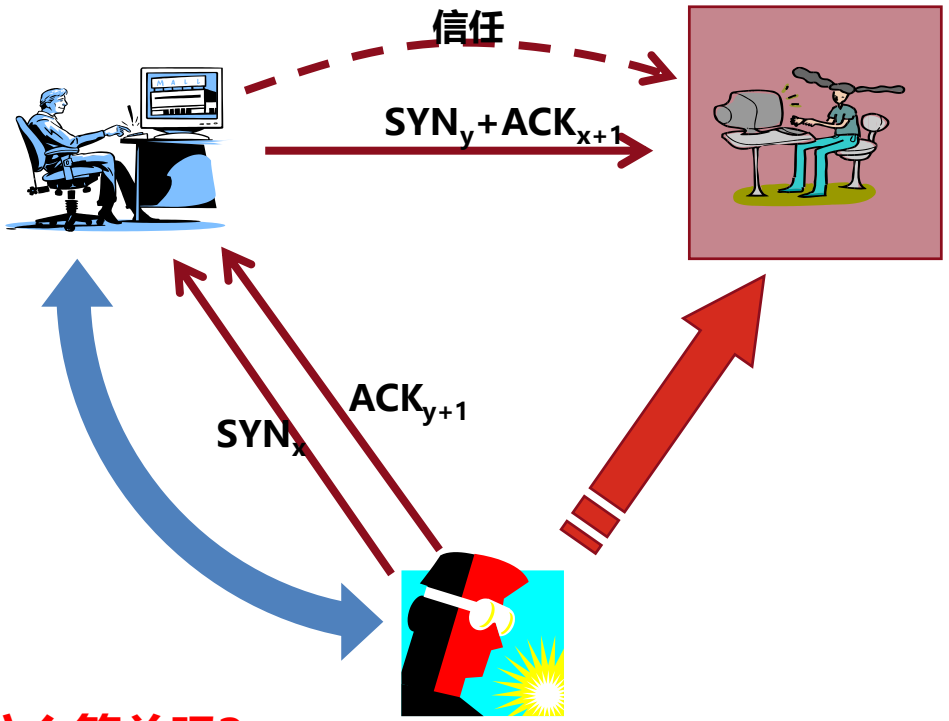
动机

- **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**

会话劫持分两种

- **被动劫持，实际上就是藏在后面监听所有的会话流量。常常用来发现密码或者其他敏感信息**
- **主动劫持，找到当前活动的会话，并且把会话接管过来。迫使一方下线，由劫持者取而代之，危害更大，因为攻击者接管了一个合法的会话之后，可以做许多危害性更大的事情**

基于TCP/IP的欺骗过程



真的这么简单吗?

IP欺骗 – 步骤

1. 首先使被信任主机的网络暂时瘫痪
2. 连接到目标机的某个端口来猜测SYN基值和增加规律
3. 把攻击者源址伪装成被信任主机，发送带有SYN标志的数据段请求连接
4. 等待目标机发送SYN+ACK包给已经瘫痪的主机
5. 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SYN
6. 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

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

TCP ACK风暴

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

例子

客户A，服务器B为正常通信双方，C为攻击者

A利用SYN1向B发起通话请求

C向B发送RST，同时向B发送SYN2

B与C间利用序列号2作为通信识别号

C已劫持B和A间的通信

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

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

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

如何防止会话劫持

部署交换式网络，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

课后习题

1. 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。

2. 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?

3. Web欺骗攻击有哪些具体形式？请简述其原理。

4. TCP/IP是否存在考虑其安全的地方？哪些建议?

谢谢!