

软件与系统安全分析

欺骗攻击及其防御技术

国家计算机网络入侵防范中心

张玉清

本章内容安排

- **5.1** 概述
- **5.2 IP**欺骗及防御技术
- **5.3 ARP**欺骗及防御技术
- **5.4** 电子邮件欺骗及防御技术
- **5.5 DNS**欺骗及防御技术
- **5.6 Web**欺骗及防御技术
- **5.7** 小结



5.1 概述

- 在**Internet**上计算机之间相互进行的交流建立在两个前提之下：
 - 认证（Authentication）
 - 信任（Trust）

5.1 概述

□ 认证:

认证是网络上的计算机用于相互间进行识别的一种鉴别过程，经过认证的过程，获准相互交流的计算机之间就会建立起相互信任的关系。

5.1 概述

□ 信任：

信任和认证具有逆反关系，即如果计算机之间存在高度的信任关系，则交流时就不会要求严格的认证。而反之，如果计算机之间没有很好的信任关系，则会进行严格的认证。

5.1 概述

- 欺骗实质上就是一种冒充身份通过认证骗取信任的攻击方式。攻击者针对认证机制的缺陷，将自己伪装成可信任方，从而与受害者进行交流，最终攫取信息或是展开进一步攻击。

5.1 概述

□ 目前比较流行的欺骗攻击主要有**5**种：

- **IP欺骗**：使用其他计算机的**IP**来骗取连接，获得信息或者得到特权；
- **ARP欺骗**：利用**ARP**协议的缺陷，把自己伪装成“中间人”，效果明显，威力惊人；
- **电子邮件欺骗**：电子邮件发送方地址的欺骗；
- **DNS欺骗**：域名与**IP**地址转换过程中实现的欺骗；
- **Web欺骗**：创造某个万维网网站的复制影像，从而达到欺骗网站用户目的的攻击。

5.2 IP欺骗及防御技术

- 5.2.1 基本的IP欺骗
- 5.2.2 IP欺骗的高级应用——TCP会话劫持
- 5.2.3 IP欺骗攻击的防御

5.2.1 基本的IP欺骗

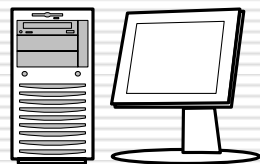
- 最基本的**IP**欺骗技术有三种：
 - 简单的**IP**地址变化
 - 源路由攻击
 - 利用Unix系统的信任关系
- 这三种**IP**欺骗技术都是早期使用的，原理比较简单，因此效果也十分有限。

简单的**IP**地址变化

- ❑ 攻击者将一台计算机的**IP**地址修改为其它主机的地址，以伪装冒充其它机器。
- ❑ 首先了解一个网络的具体配置及**IP**分布，然后改变自己的地址，以假冒身份发起与被攻击方的连接。这样做就可以使所有发送的数据包都带有假冒的源地址。

简单的IP地址变化(2)

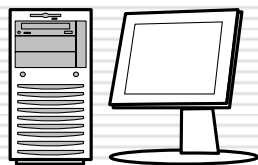
攻击者使用假冒的IP地址向一台机器发送数据包，但没有收到任何返回的数据包，这被称之为盲目飞行攻击（**flying blind attack**），或者叫做单向攻击（**one-way attack**）。因为只能向受害者发送数据包，而不会收到任何应答包。



攻击者
10.50.50.50

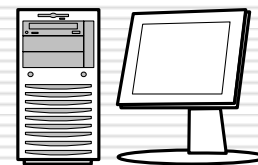
IP欺骗

源地址：10.10.20.30
目标地址：10.10.5.5



被冒充地址
10.10.20.30

返回到10.10.20.30的应答



受害者
10.10.5.5

简单的**IP**地址变化(3)

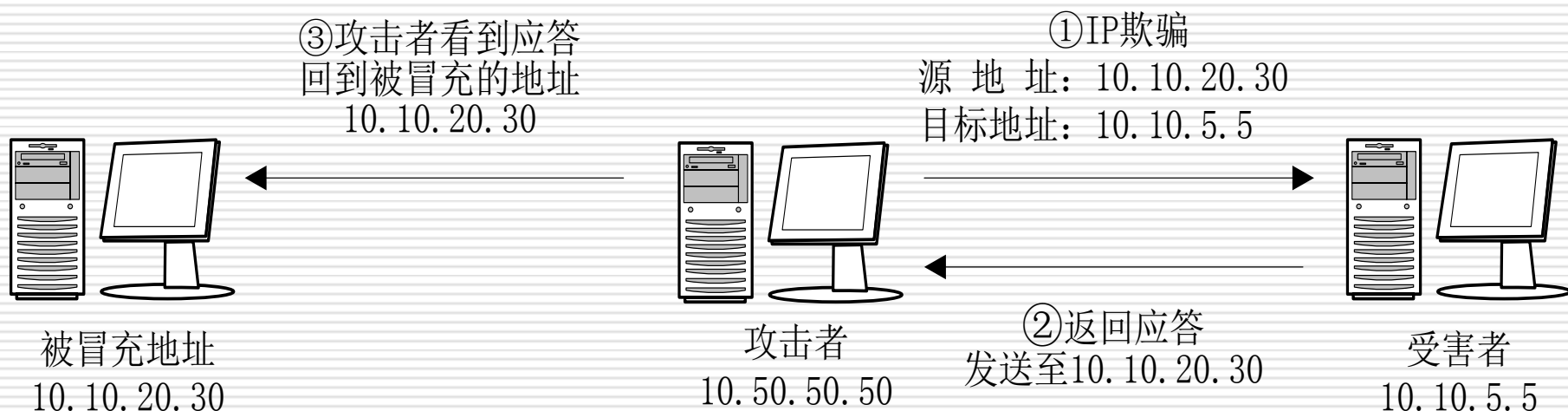
- 利用这种方法进行欺骗攻击有一些限制，比如说无法建立完整的**TCP**连接；但是，对于**UDP**这种面向无连接的传输协议就不会存在建立连接的问题，因此所有单独的**UDP**数据包都会被发送到受害者的系统中。

源路由攻击

- 简单的**IP**地址变化很致命的缺陷是攻击者无法接收到返回的信息流。为了得到从目的主机返回源地址主机的数据流，有两个方法：
 - 一个方法是攻击者插入到正常情况下数据流经过的通路上；
 - 另一种方法就是保证数据包会经过一条给定的路径，而且作为一次欺骗，保证它经过攻击者的机器。

源路由机制(2)

□ 第一种方法其过程如图所示：



但实际中实现起来非常困难，互联网采用的是动态路由，即数据包从起点到终点走过的路径是由位于此两点间的路由器决定的，数据包本身只知道去往何处，但不知道该如何去。

源路由机制(3)

- ❑ 第二种方法是使用源路由机制，保证数据包始终会经过一条经定的途径，而攻击者机器在该途径中。
- ❑ 源路由机制包含在**TCP/IP**协议组中。它允许用户在**IP**数据包包头的源路由选项字段设定接收方返回的数据包要经过的路径。
- ❑ 某些路由器对源路由包的反应是使用其指定的路由，并使用其反向路由来传送应答数据。这就使一个入侵者可以假冒一个主机的名义通过一个特殊的路径来获得某些被保护数据。

源路由机制(4)

□ 它包括两种类型的源路由：

- 宽松的源站选择（**LSR**）：发送端指明数据流必须经过的**IP**地址清单，但是也可以经过除这些地址以外的一些地址。
- 严格的源路由选择（**SRS**）：发送端指明**IP**数据包必须经过的确切地址。如果没有经过这一确切路径，数据包会被丢弃，并返回一个**ICMP**报文。

源路由机制的应用

- ❑ 源站选路给攻击者带来了很大的便利。
- ❑ 攻击者可以使用假冒地址**A**向受害者**B**发送数据包，并指定了宽松的源站选路或者严格路由选择(如果确定能经过所填入的每个路由的话)，并把自己的**IP**地址**X**填入地址清单中。
- ❑ 当**B**在应答的时候，也应用同样的源路由，因此，数据包返回被假冒主机**A**的过程中必然会经过攻击者**X**。
- ❑ 这样攻击者不再是盲目飞行了，因为它能获得完整的会话信息。

利用信任关系

- 在 **Unix**世界中，不同主机的账户间可以建立一种特殊的信任关系，以方便机器之间的访问。这常常用于对大量机器的系统管理。
- 单位里经常指定一个管理员管理几十个区域或者甚至上百台机器。管理员一般都会使用信任关系和**UNIX**的**r***命令从一个系统方便的切换到另一个系统。**r***命令允许一个人登录远程机器而不必提供口令。
- 这里的信任关系是基于**IP**地址进行认证的，而不是询问用户名和口令。也就是说将会认可来自可信**IP**地址的任何人。

利用信任关系(2)

- ❑ 从便利的角度看，信任的关系是非常有效的，但是从安全的角度来看，是不可取的。
- ❑ 如果攻击者获得了可信任网络里的任何一台的机器，他就能登录信任该**IP**的任何机器上。
- ❑ 下面是经常使用的一些**r***命令：
 - (1) rlogin: remote login, 远程登录;
 - (2) rsh: remote shell, 远程shell;
 - (3) rcp: remote copy, 远程拷贝。

利用信任关系(3)

- 例子:
- 主机**A**、**B**上各有一个账户，在使用当中，在**A**上使用时需要输入**A**上的相应账户，在**B**上使用时必须输入在**B**上的账户，主机**A**和**B**把用户当作两个互不相关的用户。
- 为了减少切换时的反复确认，可以在主机**A**和主机**B**中建立起两个账户的全双工信任关系。这可通过在**A**、**B**的登陆目录上各建立一个**hosts**文件达到。
- 在主机**A**的登陆目录下建立一个**.rhosts**文件：
 ‘**echo "B usernameB" > ~/.rhosts**’
这就建立起了**A**对**B**的信任关系。从主机**B**中就可以直接使用任何**r***命令直接登陆到主机**A**中，而不用向远程主机提供密码认证。
B对**A**的信任关系与之类似。
- 这些**r***命令允许基于地址的认证方式，它们会根据服务请求者的**IP**地址决定同意还是拒绝访问。

利用信任关系(4)

- 这种方法一度被认为是**IP**欺骗最主要的方法。
- 但是，这种欺骗方法只能在**Unix**环境下使用，而且也比较陈旧了。

5.2.2 IP欺骗高级应用—TCP会话劫持

- 基本原理
- 相关基础
- **TCP**会话劫持过程
- **TCP**会话劫持的危害
- 实现**TCP**会话劫持的两个小工具

基本原理

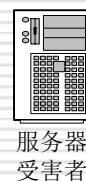
- 会话劫持就是接管一个现存动态会话的过程，换句话说，攻击者通过会话劫持可以替代原来的合法用户，同时能够监视并掌握会话内容。
- 此时，攻击者可以对受害者的回复进行记录，并在接下来的时间里对其进行响应，展开进一步的欺骗和攻击。
- 会话劫持结合了嗅探及欺骗技术。

基本原理(2)

- 在一般的欺骗攻击中攻击者并不是积极主动地使一个用户下线来实现他针对受害目标的攻击，而是仅仅装作是合法用户。此时，被冒充的用户可能并不在线上，而且它在整个攻击中不扮演任何角色，因此攻击者不会对它发动进攻。
- 但是在会话劫持中，为了接管整个会话过程，攻击者需要积极攻击使被冒充用户下线。

基本原理(3)

一般的欺骗



你好，我是A

会话劫持



正常会话

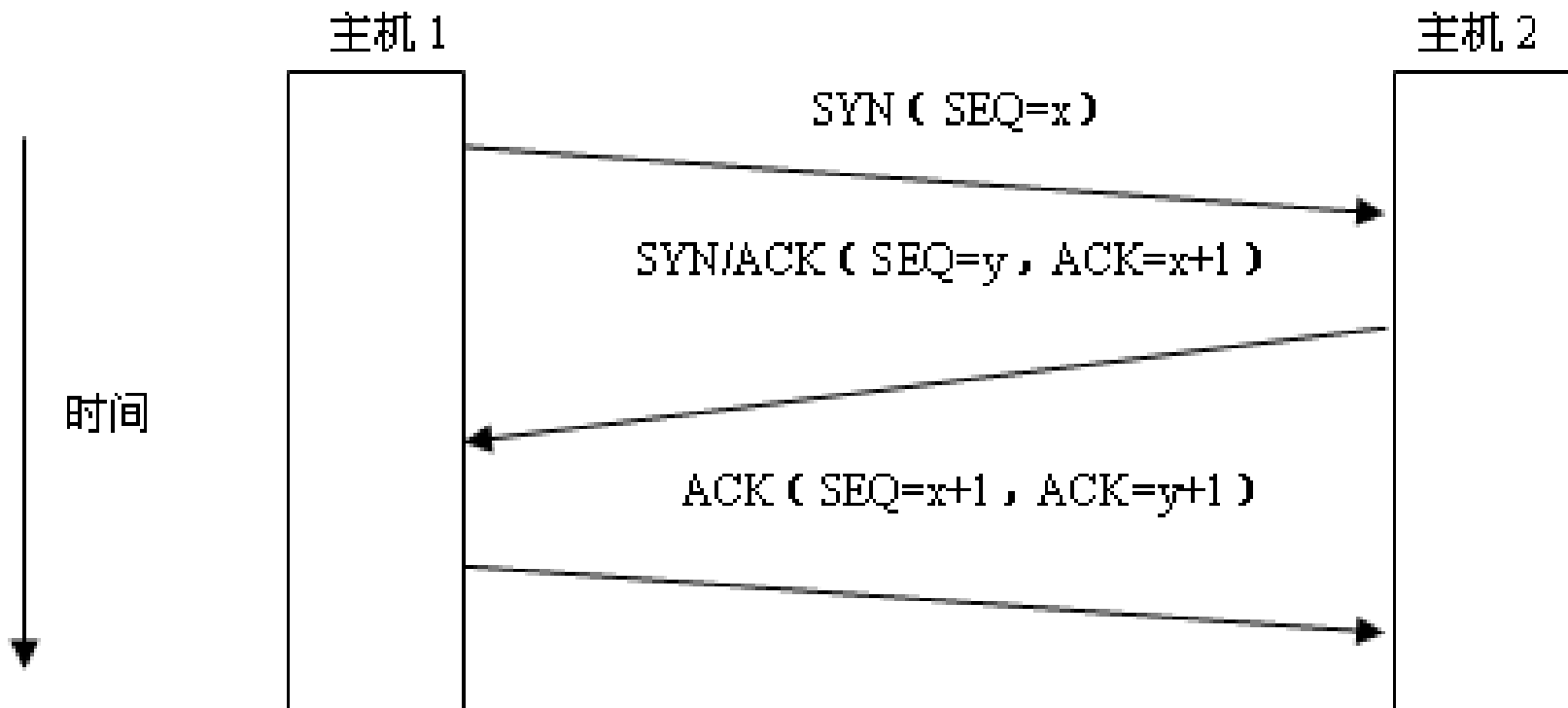
下线!

你好，我是A

相关基础

- **TCP**三步握手连接建立
- 序列号机制

TCP三步握手连接建立



序列号机制

- 序列号是一个**32**位计数器，这就意味着可以有大于**4**亿种的可能性组合。
- 简单地说，序列号用来说明**接收方下一步将要接收的数据包的顺序**。也就是说，序列号设置了数据包放入数据流的顺序，接收方就可以利用序列号告诉发送方哪些数据包已经收到，哪些数据包还未收到，于是发送方就能够依此重发丢失的数据包。

序列号机制(2)

- 例如，如果发送方发送了**4**个数据包，它们的序列号分别是**1258**、**1256**、**1257**和**1255**，接收方不但可以根据发送方发包的序列号将数据包进行归序，同时接收方还可以用发送方的序列号确认接收的数据包。
- 在这种情况下，接收方送回的确认信息是**1259**，这就等于是说，“下一个我期望从发送方收到的是序列号为**1259**的数据包”。

序列号机制(3)

- 实际上为了完成上述目的，这里存在：一个属于发送方的序列号和另一个是属于接收方的应答号。
- 发送方发送数据包使用发送方的序列号，同时当接收方确认从发送方接收数据包时，它也用发送方的序列号来进行确认。在另一方面，接收方用属于自己的序列号送回数据。

序列号机制(4)

□ 数据传输过程中序列号和应答号之间的关系:

- 第二个数据包 (B→A) 的SEQ = 第一个数据包 (A→B) 的ACK;
- 第二个数据包 (B→A) 的ACK = 第一个数据包 (A→B) 的SEQ + 第一个数据包 (A→B) 的传输数据长度。

序列号机制(5)

- 再进一步推广，对于整个序列号计数体制，我们可以得到下面这个结论：序列号是随着传输数据字节数递增的。
- 如果传输数据字节数为**10**，序列号就增加**10**；若传输的数据为**20**字节，序列号就应该相应增加**20**。

序列号机制(6)

- ❑ 从上面的讲解中，我们可以清楚地认识到：序列号和应答号之间存在着明确的对应关系。
- ❑ 因此序列号和应答号是完全有可能预测的，只需要获取最近的会话数据包，就可以猜测下一次通话中的**SEQ**和**ACK**。
- ❑ 这一局面是**TCP**协议固有缺陷造成的，由此带来的安全威胁也是无法回避的。

TCP会话劫持过程

- ❑ **step1:** 发现攻击目标
- ❑ **step2:** 确认动态会话
- ❑ **step3:** 猜测序列号
- ❑ **step4:** 使客户主机下线
- ❑ **step5:** 接管会话

step1: 发现攻击目标

- 对于寻找合适的目标有两个关键的问题。
- 首先，通常攻击者希望这个目标是一个准予**TCP**会话连接（例如**Telnet**和**FTP**等）的服务器。
- 其次，能否检测数据流也是一个比较重要的问题，因为在攻击的时候需要猜测序列号。这就需要嗅探之前通信的数据包，对于交换网络环境，可能还需要使用**ARP**欺骗。

step2: 确认动态会话

- ❑ 攻击者如何寻找动态会话？
- ❑ 与大多数攻击不同，会话劫持攻击适合在网络流通量达到高峰时才会发生的。
- ❑ 首先，他有很多供选择的会话；其次，网络流通量越大则被发现的可能就越小。
- ❑ 如果只有一个用户进行连接并数次掉线，那么就很有可能引起那个用户的怀疑。但是，如果网络流通量很大并且有很多的用户进行连接，那么用户们很有可能忽略掉线后面隐藏的问题，也许只是认为这是由于网络流通过大而引起的。

step3: 猜测序列号

- ❑ **TCP**区分正确数据包和错误数据包仅通过它们的**SEQ/ACK**序列号。序列号却是随着时间的变化而改变的。因此，攻击者必须成功猜测出序列号。
- ❑ 通过嗅探或者**ARP**欺骗，先发现目标机正在使用的序列号，再根据序列号机制，可以猜测出下一对**SEQ/ACK**序列号。
- ❑ 同时，攻击者若以某种方法扰乱客户主机的**SEQ/ACK**，服务器将不再相信客户主机正确的数据包，从而可以伪装为客户主机，使用正确的**SEQ/ACK**序列号，现在攻击主机就可以与服务器进行连接，这样就抢劫一个会话连接。

step4: 使客户主机下线

- ❑ 当攻击者获得了序列号后，为了彻底接管这个会话，他就必须使客户主机下线。
- ❑ 使客户主机下线最简单的方式就是对其进行拒绝服务攻击，从而使其不再继续响应。
- ❑ 服务器会继续发送响应给客户主机，但是因为攻击者已经掌握了客户主机，所以该机器就不再继续响应。

step5: 接管会话

- 既然攻击者已经获得了他所需要的一切信息，那么他就可以持续向服务器发送数据包并且接管整个会话了。
- 在会话劫持攻击中，攻击者通常会发送数据包在受害服务器上建立一个账户，甚至留下某些后门。通过这种方式，攻击者就可以在任何时候轻松进入系统了。

TCP会话劫持的危害

- ❑ 就其实现原理而言，任何使用**Internet**进行通信的主机都有可能受到这种攻击。
- ❑ 会话劫持在理论上是非常复杂的，但是现在产生了简单适用的会话劫持攻击软件，技术门槛的降低导致了很多人“少年攻击者”的诞生。

TCP会话劫持的危害(2)

□ 会话劫持攻击的危害性很大是有原因的。

- 一个最主要的原因就是它并不依赖于操作系统。
- 另一个原因就是它可以被用来进行积极的攻击，通过攻击行为可以获得进入系统的可能。

实现TCP会话劫持的两个小工具

□ Juggernaut

- Juggernaut是由Mike Schiffman开发的自由软件，这个软件是开创性的，是最先出现的会话攻击程序之一。它运行在Linux操作系统的终端机上，攻击者能够窥探网络中所有的会话，并且劫持其中任何一个，攻击者可以像真正用户那样向服务器提交命令。

实现TCP会话劫持的两个小工具(2)

□ Hunt

- 由Pavel Krauz制作的Hunt，是一个集嗅探、截取和会话劫持功能与一身的强大工具。它可以在无论共享式网络还是交换式网络中工作，不仅能够在混杂模式和ARP欺骗模式下进行嗅探，还具有中断和劫持动态会话的能力。

5.2.3 IP欺骗攻击的防御

- ❑ 防范地址变化欺骗
- ❑ 防范源路由欺骗
- ❑ 防范信任关系欺骗
- ❑ 防范会话劫持攻击

防范地址变化欺骗

有办法防止攻击者使用你的地址发送消息吗？可以说，你没有办法阻止有人向另一方发送消息时不用自己的而使用你的地址。

但是，采取一些措施可以有效保护自己免受这种攻击的欺骗。

防范地址变化欺骗(2)

- 方法**1**: 限制用户修改网络配置
- 方法**2**: 入口过滤
- 方法**3**: 出口过滤

方法1：限制用户修改网络配置

为了阻止攻击者使用一台机器发起欺骗攻击，首先需限制那些有权访问机器配置信息的人员。这么做就能防止员工执行欺骗。

方法2：入口过滤

大多数路由器有内置的欺骗过滤器。过滤器的最基本形式是，不允许任何从外面进入网络的数据包使用单位的内部网络地址作为源地址。

因此，如果一个来自外网的数据包，声称来源于本单位的网络内部，就可以非常肯定它是假冒的数据包，应该丢弃它。

这种类型的过滤可以保护单位的网络不成为欺骗攻击的受害者。

方法3：出口过滤

为了执行出口过滤，路由器必须检查数据包，确信源地址是来自本单位局域网的一个地址。

如果不是那样，这个数据包应该被丢弃，因为这说明有人正使用假冒地址向另一个网络发起攻击。离开本单位的任何合法数据包须有一个源地址，并且它的网络部分与本单位的内部网络相匹配。

防范源路由欺骗

- ❑ 保护自己或者单位免受源路由欺骗攻击的最好方法是设置路由器禁止使用源路由。
- ❑ 事实上人们很少使用源路由做合法的事情。因为这个原因，所以阻塞这种类型的流量进入或者离开网络通常不会影响正常的业务。

防范信任关系欺骗

- 保护自己免受信任关系欺骗攻击最容易的方法就是不使用信任关系。但是这并不是最佳的解决方案，因为便利的应用依赖于信任关系。
- 但是能通过做一些事情使暴露达到最小：
 - 限制拥有信任关系的人员。
 - 不允许通过外部网络使用信任关系。

防范会话劫持攻击

- 会话劫持攻击是非常危险的，因为攻击者能够直接接管合法用户的会话。
- 在其他的攻击中可以处理那些危险并且将它消除。但是在会话劫持中，消除这个会话也就意味着禁止了一个合法的连接，从本质上来说这么做就背离了使用**Internet**进行连接的目的。

防范会话劫持攻击(2)

□ 没有有效的办法可以从根本上防范会话劫持攻击，以下列举了一些方法可以尽量缩小会话攻击所带来的危害：

- 进行加密
- 使用安全协议
- 限制保护措施

进行加密

- 如果攻击者不能读取传输数据，那么进行会话劫持攻击也是十分困难的。因此，任何用来传输敏感数据的关键连接都必须进行加密。

使用安全协议

- 无论何时当用户连入到一个远端的机器上，特别是当从事敏感工作或是管理员操作时，都应当使用安全协议。
- 一般来说，有像**SSH (Secure Shell)**这样的协议或是安全的**Telnet**都可以使系统免受会话劫持攻击。此外，从客户端到服务器的**VPN (Virtual Private Network)**也是很好的选择。

限制保护措施

- 允许从网络上传输到用户单位内部网络的信息越少，那么用户将会越安全，这是个最小化会话劫持攻击的方法。
- 攻击者越难进入系统，那么系统就越不容易受到会话劫持攻击。在理想情况下，应该阻止尽可能多的外部连接和连向防火墙的连接。

5.3 ARP欺骗攻击与防御技术

- **5.3.1 ARP背景知识介绍**
- **5.3.2 ARP欺骗攻击原理**
- **5.3.3 ARP欺骗攻击实例**
- **5.3.4 ARP欺骗攻击的检测与防御**

5.3.1 ARP背景知识介绍

- **ARP**基础知识

- **ARP**工作原理

 - 局域网内通信

 - 局域网间通信

ARP基础知识

- ❑ **ARP(Address Resolution Protocol):** 地址解析协议，用于将计算机的网络地址（**IP地址32位**）转化为物理地址（**MAC地址48位**）**[RFC826]**。属于链路层的协议。
- ❑ 在以太网中，数据帧从一个主机到达局域网内的另一台主机是根据**48位**的以太网地址（硬件地址）来确定接口的，而不是根据**32位**的**IP**地址。
- ❑ 内核（如驱动）必须知道目的端的硬件地址才能发送数据。

ARP基础知识

□ ARP协议有两种数据包

- **ARP请求包**：ARP工作时，送出一个含有目的IP地址的以太网广播数据包，这也就是ARP请求包。它表示：我想与目的IP通信，请告诉我此IP的MAC地址。ARP请求包格式如下：
- `arp who-has 192.168.1.1 tell 192.168.1.2`
- **ARP应答包**：当目标主机收到ARP请求包，发现请求解析的IP地址与本机IP地址相同，就会返回一个ARP应答包。它表示：我的主机就是此IP，我的MAC地址是某某某。ARP应答包的格式如下：
- `arp reply 192.168.1.1 is-at 00:00:0c:07:ac:00`

ARP基础知识

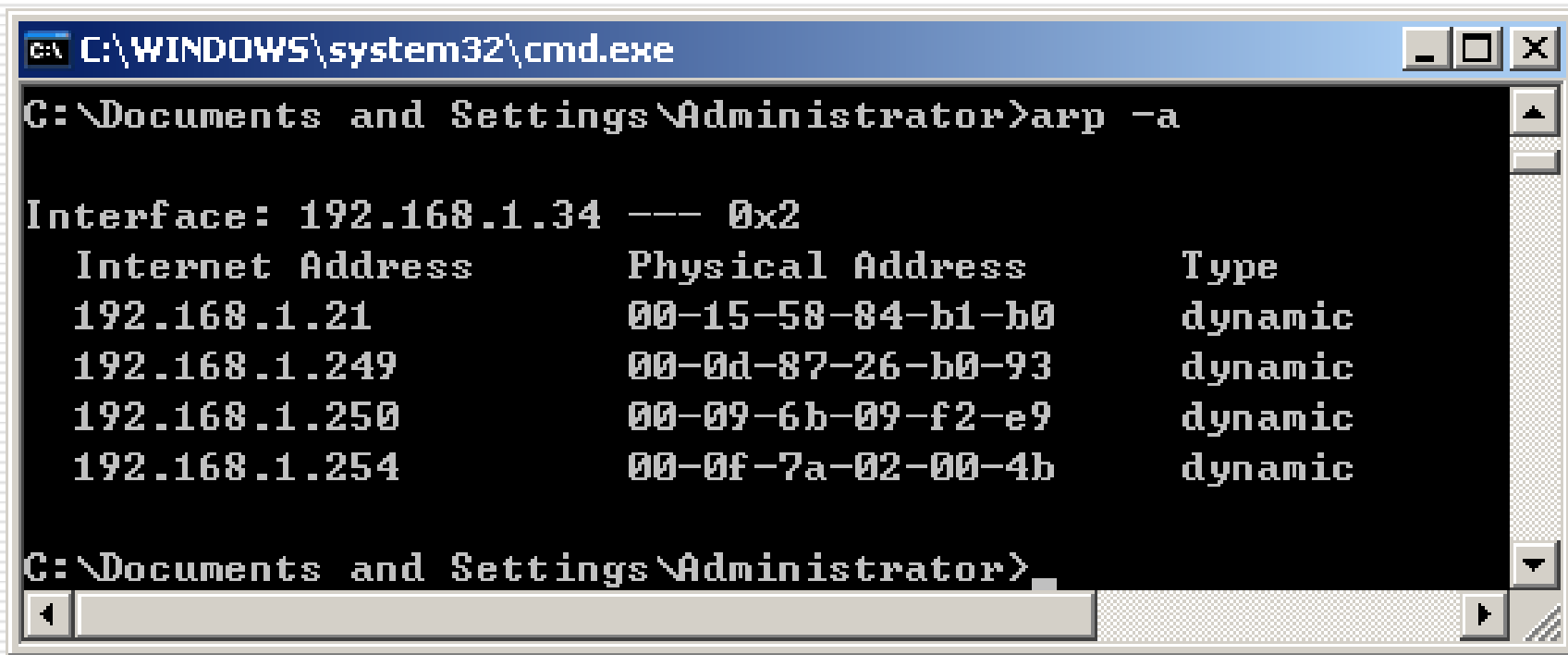
□ ARP缓存表

- ARP缓存表用于存储其它主机或网关的IP地址与MAC地址的对应关系。
- 每台主机、网关都有一个ARP缓存表。
- ARP缓存表里存储的每条记录实际上就是一个IP地址与MAC地址对，它可以是静态的，也可以是动态的。如果是静态的，那么该条记录不能被ARP应答包修改；如果是动态的，那么该条记录可以被ARP应答包修改。

ARP基础知识

□ 在Windows下查看ARP缓存表的方法

➤ 使用命令：arp -a



The screenshot shows a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe". The command prompt is at the directory "C:\Documents and Settings\Administrator>". The command "arp -a" has been entered, and the output is displayed as follows:

```
Interface: 192.168.1.34 --- 0x2
Internet Address      Physical Address      Type
192.168.1.21          00-15-58-84-b1-b0     dynamic
192.168.1.249         00-0d-87-26-b0-93     dynamic
192.168.1.250         00-09-6b-09-f2-e9     dynamic
192.168.1.254         00-0f-7a-02-00-4b     dynamic
```

The command prompt is now at "C:\Documents and Settings\Administrator>".

ARP工作原理

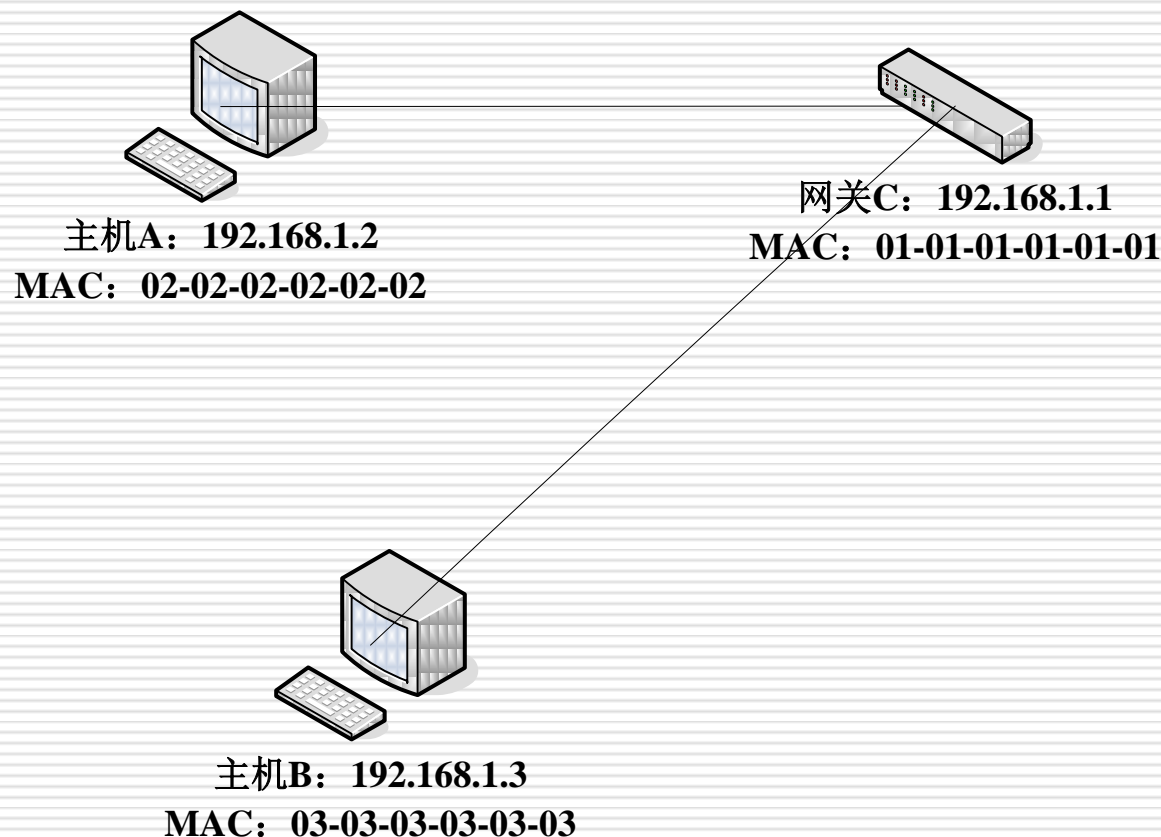
- 局域网内通信
- 局域网间通信

局域网内通信

- 假设一个局域网内主机**A**、主机**B**和网关**C**，它们的**IP**地址、**MAC**地址如下。

主机名	IP地址	MAC地址
主机A	192.168.1.2	02-02-02-02-02-02
主机B	192.168.1.3	03-03-03-03-03-03
网关C	192.168.1.1	01-01-01-01-01-01

局域网内通信—网络结构图



局域网内通信—通信过程

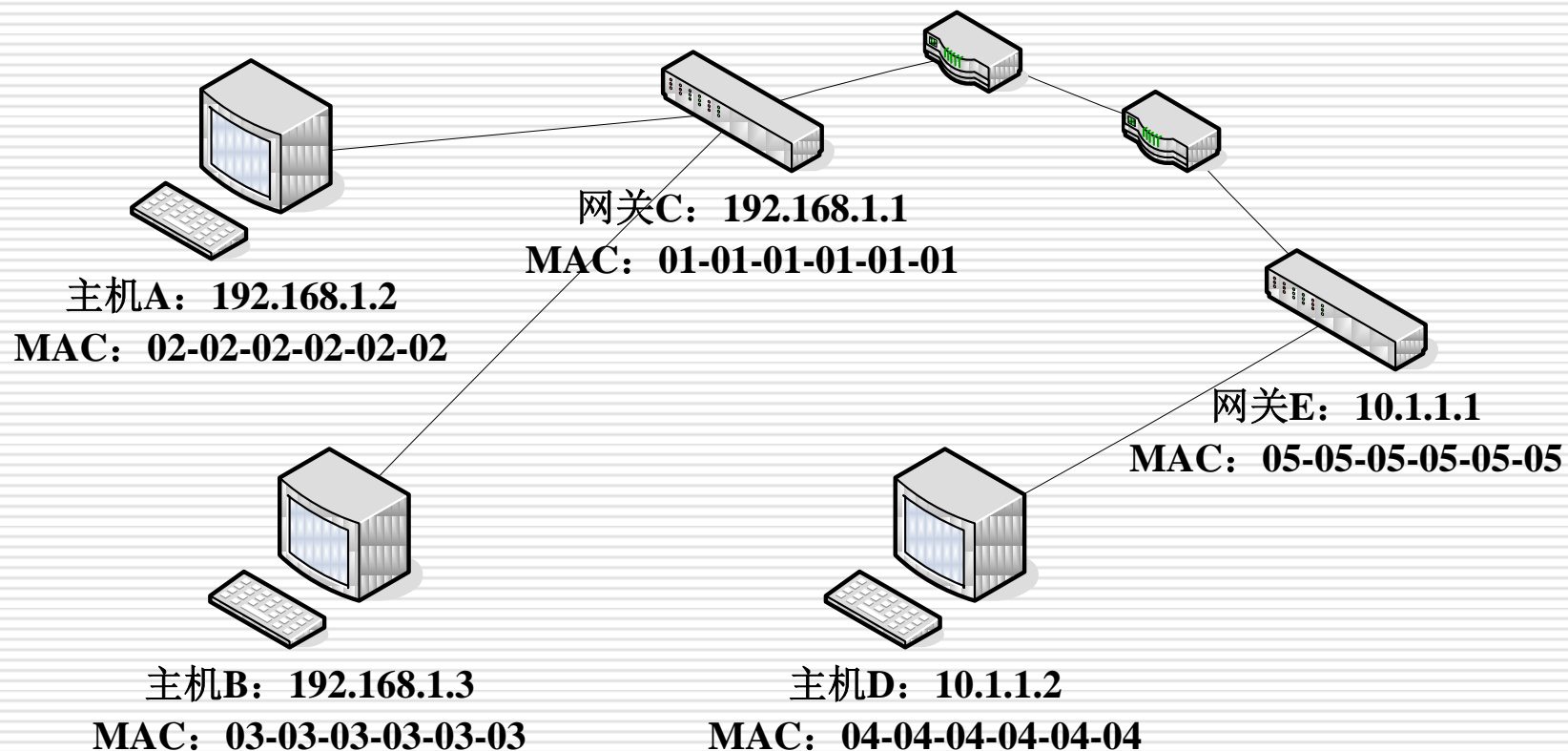
- ❑ 假如主机主机**A(192.168.1.2)**要与主机主机**B(192.168.1.3)**通讯，它首先会检查自己的**ARP**缓存中是否有**192.168.1.3**这个地址对应的**MAC**地址。
- ❑ 如果没有它就会向局域网的广播地址发送**ARP**请求包，大致的意思是**192.168.1.3**的**MAC**地址是什么请告诉**192.168.1.2**。
- ❑ 而广播地址会把这个请求包广播给局域网内的所有主机，但是只有**192.168.1.3**这台主机才会响应这个请求包，它会回应**192.168.1.2**一个**arp**包，告知**192.168.1.3**的**MAC**地址是**03-03-03-03-03-03**。
- ❑ 这样主机**A**就得到了主机**B**的**MAC**地址，并且它会把这个对应的关系存在自己的**ARP**缓存表中。
- ❑ 之后主机**A**与主机**B**之间的通讯就依靠两者缓存表里的记录来通讯，直到通讯停止后两分钟，这个对应关系才会被从表中删除。

局域网间通信

- 假设两个局域网，其中一个局域网内有主机**A**、主机**B**和网关**C**，另一个局域网内有主机**D**和网关**C**。它们的**IP**地址、**MAC**地址如下。

主机名	IP地址	MAC地址
主机A	192.168.1.2	02-02-02-02-02-02
主机B	192.168.1.3	03-03-03-03-03-03
网关C	192.168.1.1	01-01-01-01-01-01
主机D	10.1.1.2	04-04-04-04-04-04
网关E	10.1.1.1	05-05-05-05-05-05

局域网间通信—网络结构图



局域网间通信—通信过程

- ❑ 假如主机**A(192.168.1.2)**需要和主机**D(10.1.1.2)**进行通讯，它首先会发现这个主机**D**的**IP**地址并不是自己同一个网段内的，因此需要通过网关来转发。
- ❑ 这样的话它会检查自己的**ARP**缓存表里是否有网关**192.168.1.1**对应的**MAC**地址，如果没有就通过**ARP**请求获得，如果有就直接与网关通讯，然后再由网关**C**通过路由将数据包送到网关**E**。
- ❑ 网关**E**收到这个数据包后发现有是送给主机**D (10.1.1.2)**的，它就会检查自己的**ARP**缓存（网关也有自己的**ARP**缓存），看看里面是否有**10.1.1.2**对应的**MAC**地址，如果没有就使用**ARP**协议获得，如果有就是用该**MAC**地址与主机**D**通讯。

5.3.2 ARP欺骗攻击原理

- ARP欺骗攻击原理
- ARP欺骗攻击的危害

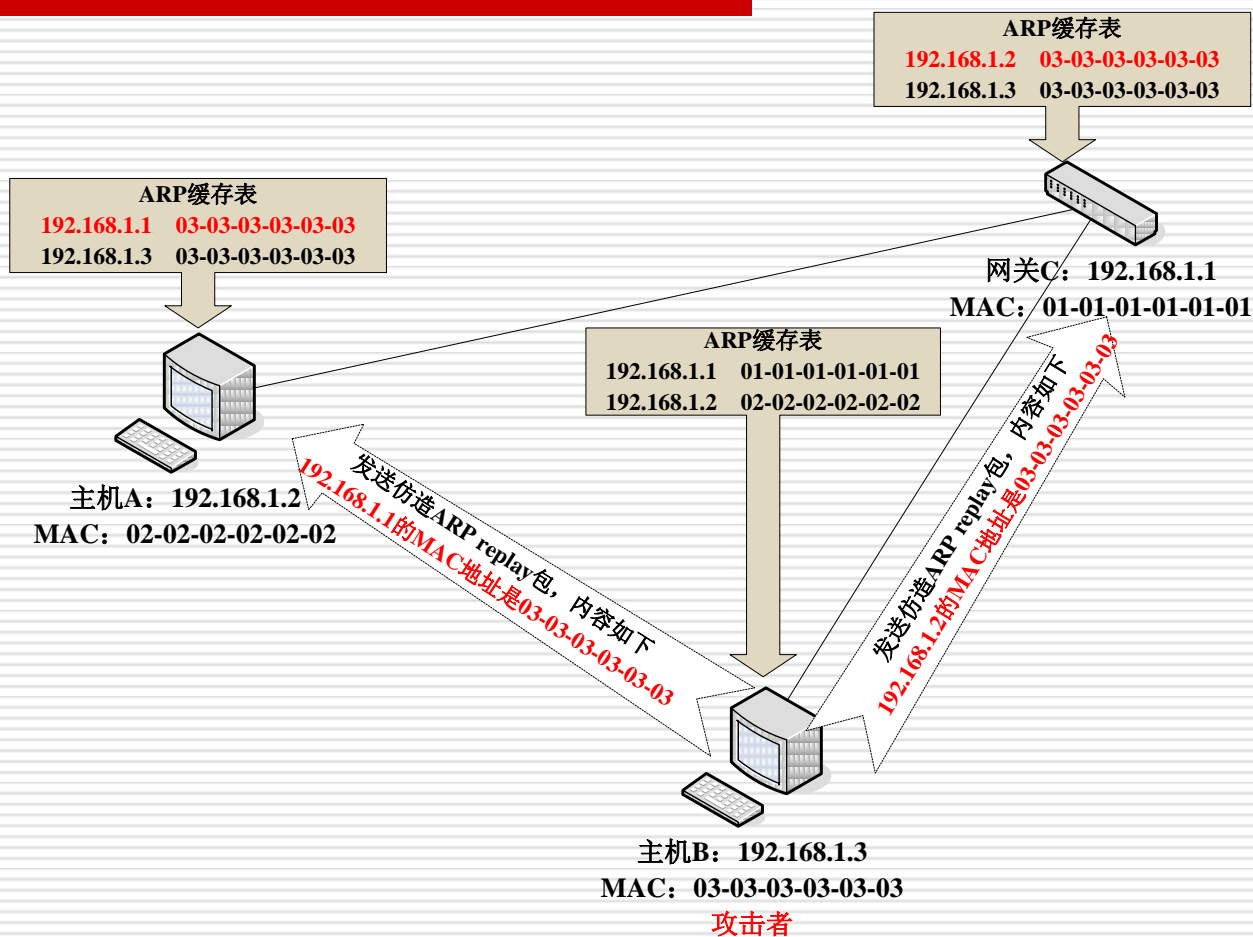
ARP欺骗原理

- **ARP欺骗攻击**是利用**ARP**协议本身的缺陷进行的一种非法攻击，目的是为了在全交换环境下实现数据监听。
- 通常这种攻击方式可能被病毒、木马或者有特殊目的的攻击者使用。

ARP欺骗原理(2)

- ❑ 主机在实现**ARP**缓存表的机制中存在一个不完善的地方，当主机收到一个**ARP**应答包后，它并不会去验证自己是否发送过这个**ARP**请求，而是直接将应答包里的**MAC**地址与**IP**对应的关系替换掉原有的**ARP**缓存表里的相应信息。
- ❑ **ARP**欺骗正是利用了这一点。

ARP欺骗原理—原理图



ARP欺骗原理—欺骗过程

- ❑ 主机**B(192.168.1.3)**向网关**C**发送**ARP**应答包说：我是**192.168.1.2**，我的**MAC**地址是**03-03-03-03-03-03**，主机**B**同时向主机**A**发送**ARP**应答包说：我是**192.168.1.1**，我的**MAC**地址是**03-03-03-03-03-03**。
- ❑ 这样，**A**发给**C**的数据就会被发送到**B**，同时获得**C**发给**A**的数据也会被发送到**B**。
- ❑ 这样，**B**就成了**A**与**C**之间的“中间人”。

ARP欺骗攻击的危害

□ **ARP欺骗攻击在局域网内非常奏效，其危害有：**

- 致使同网段的其他用户无法正常上网（频繁断网或者网速慢）。
- 使用**ARP**欺骗可以嗅探到交换式局域网内所有数据包，从而得到敏感信息。
- **ARP**欺骗攻击可以对信息进行篡改，例如，可以在你访问的所有网页中加入广告。
- 利用**ARP**欺骗攻击可以控制局域网内任何主机，起到“网管”的作用，例如，让某台主机不能上网。

5.3.3 ARP欺骗攻击实例

□ 使用工具：Arp cheat and sniffer V2.1

- 国内开源软件，它是一款arp sniffer工具，可以通过arp欺骗嗅探目标主机TCP、UDP和ICMP协议数据包。

□ 攻击环境：在一个交换式局域网内

- 受害者IP为210.77.21.53，MAC为00-0D-60-36-BD-05；
- 网关IP为210.77.21.254，MAC为00-09-44-44-77-8A；
- 攻击者IP为210.77.21.68，MAC为00-07-E9-7D-73-E5。

□ 攻击目的：攻击者想得知受害者经常登陆的**FTP**用户名和密码。

ARP攻击实例--工具参数介绍

- **-si** 源ip
- **-di** 目的ip *代表所有,多项用,号分割
- **-sp** 源端口
- **-dp** 目的端口 *代表所有
- **-w** 嗅探方式, **1**代表单向嗅探[**si->di**], **0**代表双向嗅探[**si<->di**]
- **-p** 嗅探协议[**TCP,UDP,ICMP**]大写
- **-m** 最大记录文件,以**M**为单位
- **-o** 文件输出
- **-hex** 十六进制输出到文件
- **-unecho** 不回显
- **-unfilter** 不过虑**0**字节数据包
- **-low** 粗略嗅探,丢包率高,cpu利用率低 基本**0**
- **-timeout** 嗅探超时,除非网络状况比较差否则请不要调高,默认为**120**秒

ARP攻击实例--工具参数介绍（2）

- **-sniffsmtp** 嗅探**smtp**
- **-sniffpop** 嗅探**pop**
- **-sniffpost** 嗅探**post**
- **-sniffftp** 嗅探**ftp**
- **-snifftelnet** 嗅探**telnet**，以上5个嗅探不受参数
si,sp,di,dp,w,p影响。
- **-sniffpacket** 规则嗅探数据包,受参数**si,sp,di,dp,w,p**影响
- **-sniffall** 开启所有嗅探
- **-onlycheat** 只欺骗
- **-cheatsniff** 欺骗并且嗅探
- **-reset** 欺骗后恢复
- **-g** [网关**ip**]
- **-c** [欺骗者**ip**] [mac]
- **-t** [受骗者**ip**]
- **-time** [欺骗次数]

ARP攻击实例--工具参数介绍（3）

□ 使用举例：

➤ `arpsf -p TCP -dp 25,110 -o f:\1.txt -m 1 -sniffpacket`

➤ 说明：嗅探指定规则数据包并保存到文件

➤ `arpsf -sniffall -cheatsniff -t 127.0.0.1 -g 127.0.0.254`

➤ 说明：欺骗并且嗅探127.0.0.1与外界的通讯，输出到屏幕

➤ `arpsf -onlycheat -t 127.0.0.1 -c 127.0.0.2002211445544 -time 100 -reset`

➤ 说明：对目标欺骗一百次，欺骗后恢复

➤ `arpsf -cheatsniff -t 192.168.0.54 -g 192.168.0.254 -sniffpacket -p TCP -dp 80,25,23,110 -o d:\siff.txt -w 0 -m 1`

说明：嗅探192.168.0.54与外网的tcp连接情况并指定目的端口是80，23，25，110，嗅探方式是双向嗅探，最大记录文件是1M，输出到d盘sniff.txt文件中。其中192.168.0.254是网关的地址。也可以改成同网段中其他的地址，那就是网内嗅探了。

ARP攻击实例--攻击过程

- ❑ 在**Windows XP**下通过命令行启动软件，运行命令：**arpsf -cheatsniff -t 210.77.21.53 -g 210.77.21.254 -sniffpacket -p TCP -dp 21 -o c:\siff.txt -w 0 -m 1。**
- ❑ 含义是：嗅探**210.77.21.53**与其它主机的**tcp**连接情况并指定目的端口是**21**，嗅探方式是双向嗅探，最大记录文件是**1M**，结果输出到**C盘 sniff.txt**。其中**210.77.21.254**是网关的地址。
- ❑ 运行效果见下页图。

C:\WINDOWS\system32\cmd.exe - arpsf -cheatsniff -t 210.77.21...

C:\arp_cheap_sniff_v2.1>arpsf -cheatsniff -t 210.77.21.53 -g 21
fpacket -p TCP -dp 21 -o c:\siff.txt -w 0 -m 1

输入命令

=====
Arp Cheat And Sniffer V2.1
powered by shadow ©2005/6/15
my web:http://www.codehome.6600.org
=====

输出版本信息

+Choose a method to get adapter list:
->0.Get By Winpcap Driver!
->1.Get By IpHelpAPI (Can use this in 2003)!
Please input your choose num:1

选择获取网卡
的方法

+Adapater List:

Try to get adapter list by iphelpapi...

0:\Device\NPF_{892EC0CD-EA7E-4CF7-932D-045693860E95}

Please choose a adapter with num:0

选择用于欺
骗的网卡

>>This is user define:

Protocol: [TCP]

Source IP: [210.77.21.53

]

Source Port: [*]

ARP攻击实例--攻击过程（2）

- 当**Arp cheat sniff**获取了目标机器、网关和本机的**MAC**之后，就开始欺骗目标机器和网关。
- 见下页图。

C:\WINDOWS\system32\cmd.exe - arpsf -cheatsniff -t 210.77.21...

+Ok

欺骗主机210.77.21.53

-->开始欺骗第一个目标主机...

欺骗源ip: 210.77.21.254

欺骗源mac: 0007e97d73e5

受骗主机: 210.77.21.53

受骗的mac: 000d6036bd05

-->开始欺骗第二个目标主机...

欺骗源ip: 210.77.21.53

欺骗源mac: 0007e97d73e5

受骗主机: 210.77.21.254

受骗的mac: 00094444778a

欺骗网关210.77.21.254

<--双向欺骗完成

+Cheat ok,start sniff...

Press any key to stop :>

.....

ARP攻击实例--攻击过程（3）

- ❑ 当受害者机器上的用户登陆了**FTP**之后，**Arp cheat sniff**就可以把用户的操作记录下来。
- ❑ 下页是当软件运行了一段时间之后捕获到的有用信息，存储在**C:\sniff.txt**中。

TCP 210.45.121.114 21 --> 210.77.21.53 2256 49 Bytes 2007-5-5 17:56:24

220-Serv-U FTP Server v6.0 for WinSock ready...

服务器返回的版本信息

TCP 210.45.121.114 21 --> 210.77.21.53 2256 79 Bytes 2007-5-5 17:56:24

220-欢迎使用lcgftpserver
220-movie:movie
220 上载用户名/密码upload:upload

服务器返回的欢迎信息

TCP 210.77.21.53 2256 --> 210.45.121.114 21 12 Bytes 2007-5-5 17:56:24

USER movie

用户输入的**USER**命令

TCP 210.45.121.114 21 --> 210.77.21.53 2256 36 Bytes 2007-5-5 17:56:24

331 User name okay, need password.

服务器返回的确认

TCP 210.77.21.53 2256 --> 210.45.121.114 21 12 Bytes 2007-5-5 17:56:24

PASS movie

用户输入的**PASS**命令

TCP 210.45.121.114 21 --> 210.77.21.53 2256 30 Bytes 2007-5-5 17:56:24

230 User logged in, proceed.

服务器返回的登陆成功信息

ARP攻击实例--攻击过程（4）

- 非常明显，我们能够得知，主机 **210.77.21.53**上有用户登陆了 **ftp:// 210.45.121.114:21**。
- 用户名和密码都是**movie**。

5.3.4 ARP欺骗攻击的检测与防御

- 如何检测局域网中存在**ARP**欺骗攻击
- 如何发现正在进行**ARP**攻击的主机
- **ARP**欺骗攻击的防范

如何检测局域网中存在**ARP**欺骗攻击

- ❑ 网络频繁掉线
- ❑ 网速突然变慢
- ❑ 使用**ARP -a**命令发现网关的**MAC**地址与真实的网关**MAC**地址不相同
- ❑ 使用**sniffer**软件发现局域网内存在大量的**ARP reply**包

如何发现正在进行**ARP**攻击的主机

- ❑ 如果你知道正确的网关**MAC**地址，通过**ARP -a**命令看到的列出的网关**MAC**与正确的**MAC**地址不同，那就是攻击主机的**MAC**。
- ❑ 使用**Sniffer**软件抓包发现大量的以网关的**IP**地址发送的**ARP reply**包，包中指定的**MAC**就是攻击主机的**MAC**地址。
- ❑ 使用**ARP**保护程序发现攻击主机的**MAC**:
<ftp://166.111.8.243/tools/ArpFix.rar>

ARP欺骗攻击的防范

- ❑ **MAC**地址绑定，使网络中每一台计算机的**IP**地址与硬件地址一一对应，不可更改。
- ❑ 使用静态**ARP**缓存，用手工方法更新缓存中的记录，使**ARP**欺骗无法进行。
- ❑ 使用**ARP**服务器，通过该服务器查找自己的**ARP**转换表来响应其他机器的**ARP**广播。确保这台**ARP**服务器不被黑。
- ❑ 使用**ARP**欺骗防护软件，如**ARP**防火墙。
- ❑ 及时发现正在进行**ARP**欺骗的主机并将其隔离。

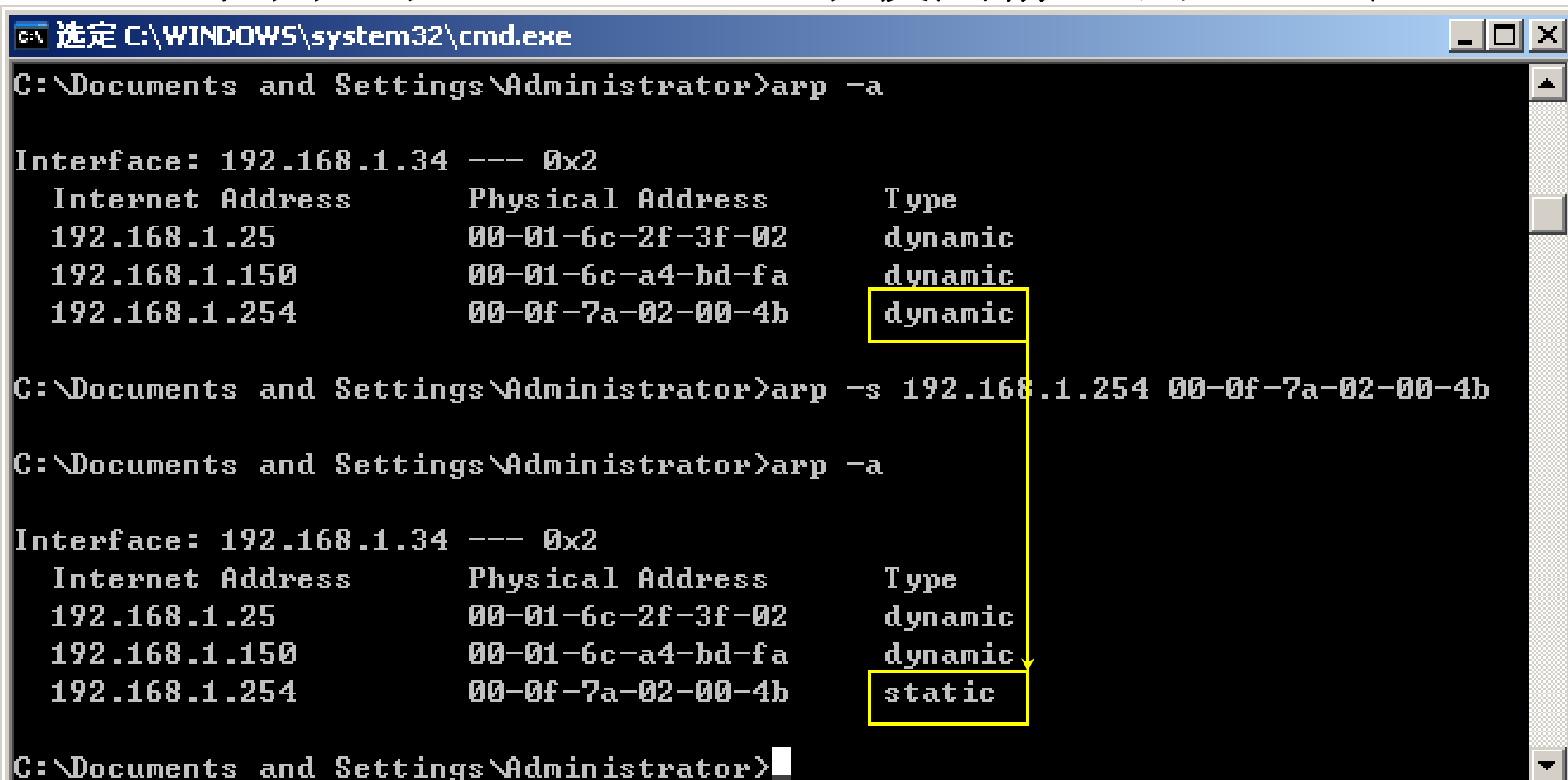
ARP欺骗攻击的防范

□ 示例：在Windows下使用静态的ARP表

- 假设我们事先已知网关192.168.1.254的MAC地址为：00-0f-7a-02-00-4b
- 查看主机当前的ARP表，命令为`arp -a`，可以查看到当前的ARP表中的记录，都是动态的
- 把网关的arp记录设置成静态，命令为`arp -s 192.168.1.254 00-0f-7a-02-00-4b`
- 再次用`arp -a`命令查看ARP表，发现网关的ARP记录已经设置成静态，操作过程见下页

ARP欺骗攻击的防范

❑ 示例：在Windows下使用静态的ARP表



The screenshot shows a Windows command prompt window with the title bar '选定 C:\WINDOWS\system32\cmd.exe'. The command prompt is running the 'arp -a' command, which displays the current ARP table. The table has three columns: 'Internet Address', 'Physical Address', and 'Type'. The entries are for 192.168.1.25, 192.168.1.150, and 192.168.1.254, all with 'dynamic' types. Then, the command 'arp -s 192.168.1.254 00-0f-7a-02-00-4b' is entered, adding a static entry for 192.168.1.254 with physical address 00-0f-7a-02-00-4b. Finally, 'arp -a' is run again, and the entry for 192.168.1.254 now shows 'static' in the 'Type' column. A yellow box highlights the 'dynamic' and 'static' entries, with an arrow pointing from the first to the second.

```
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.34 --- 0x2
    Internet Address      Physical Address      Type
    192.168.1.25          00-01-6c-2f-3f-02    dynamic
    192.168.1.150        00-01-6c-a4-bd-fa    dynamic
    192.168.1.254        00-0f-7a-02-00-4b    dynamic

C:\Documents and Settings\Administrator>arp -s 192.168.1.254 00-0f-7a-02-00-4b

C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.34 --- 0x2
    Internet Address      Physical Address      Type
    192.168.1.25          00-01-6c-2f-3f-02    dynamic
    192.168.1.150        00-01-6c-a4-bd-fa    dynamic
    192.168.1.254        00-0f-7a-02-00-4b    static

C:\Documents and Settings\Administrator>
```

ARP欺骗攻击的防范

□ 示例：ARP防火墙(www.antiarp.com)

ARP防火墙单机个人版 v4.2beta2 【试用版】

文件(E) 动作(A) 工具(T) 帮助(H)

开始 停止 最小化 隐藏 追踪 设置 退出 论坛

统计数据

ARP统计

	总数	已拦截	速度	抓包	抑制
接收ARP	10	0	0	0	放行
└ 广播	7	0	0	0	
└ 非广播	3	0	0	0	
发送ARP	12	0	0	N/A	0 秒
└ 广播	12	0	0	N/A	
└ 非广播	0	0	0	N/A	

IP/MAC

网关IP/MAC 00-09-44-44-77-8A:210.77.21.254

本机IP/MAC 00-11-5B-F3-94-AB:210.77.21.111

IP数据统计

	总数	已拦截	速度	抑制
发送UDP	6	0	0	0 秒
发送ICMP	0	0	0	0 秒
发送TCP SYN	67	0	0	0 秒

攻击统计

	总数	已拦截	速度	状态
接收ARP攻击	0	0	0	拦截
接收IP冲突攻击	0	0	0	拦截
发送ARP攻击	0	0	0	拦截
发送伪造IP攻击	0	0	0	拦截

主动防御

设定速度(个/秒) 10

实际速度(个/秒) 0

防御状态 警戒-待命

2007-07-12 星期四 | 已试用1天(共15天) | Copyright 2003-2007 ColorSoft.

5.4 电子邮件欺骗及防御技术

□ **5.4.1** 电子邮件欺骗的原理

□ **5.4.2** 电子邮件欺骗的防御

5.4.1 电子邮件欺骗的原理

- 攻击者使用电子邮件欺骗有三个目的：
 - 第一，隐藏自己的身份。
 - 第二，如果攻击者想冒充别人，他能假冒那个人的电子邮件。
 - 第三，电子邮件欺骗能被看作是社会工程的一种表现形式。

5.4.1 电子邮件欺骗的原理

- 一个邮件系统的传输包含**用户代理**（**User Agent**）、**传输代理**（**Transfer Agent**）及**投递代理**（**Delivery Agent**）三大部分。
- **用户代理**是一个用户端发信和收信的程序，负责将信件按照一定的标准包装，然后送到**邮件服务器**，将信件发出或由邮件服务器的收回。**传输代理**则负责信件的交换和传输，将信件传送到适当的邮件服务器。再由**投递代理**将信件分发至最终用户的邮箱。
- 在正常的情况下，邮件会尽量将发送者的名字和地址包括进邮件头信息中，但是，有时候，发送者希望将邮件发送出去而不希望收件者知道是谁发的，这种发送邮件的方法称为匿名邮件。
- 实现匿名的一种最简单的方法，是简单地改变电子邮件软件里的发送者的名字，但通过邮件头的其它信息，仍能够跟踪发送者。
- 另一种比较彻底的匿名方式是让其他人发送这个邮件，邮件中的发信地址就变成了转发者的地址了。现在互联网上有大量的匿名转发者（或称为匿名服务器）。

5.4.1 电子邮件欺骗的原理

- 执行电子邮件欺骗有三种基本方法，每一种有不同难度级别，执行不同层次的隐蔽。它们分别是：
 - 利用相似的电子邮件地址
 - 直接使用伪造的E-mail地址
 - 远程登录到SMTP端口发送邮件

利用相似的电子邮件地址

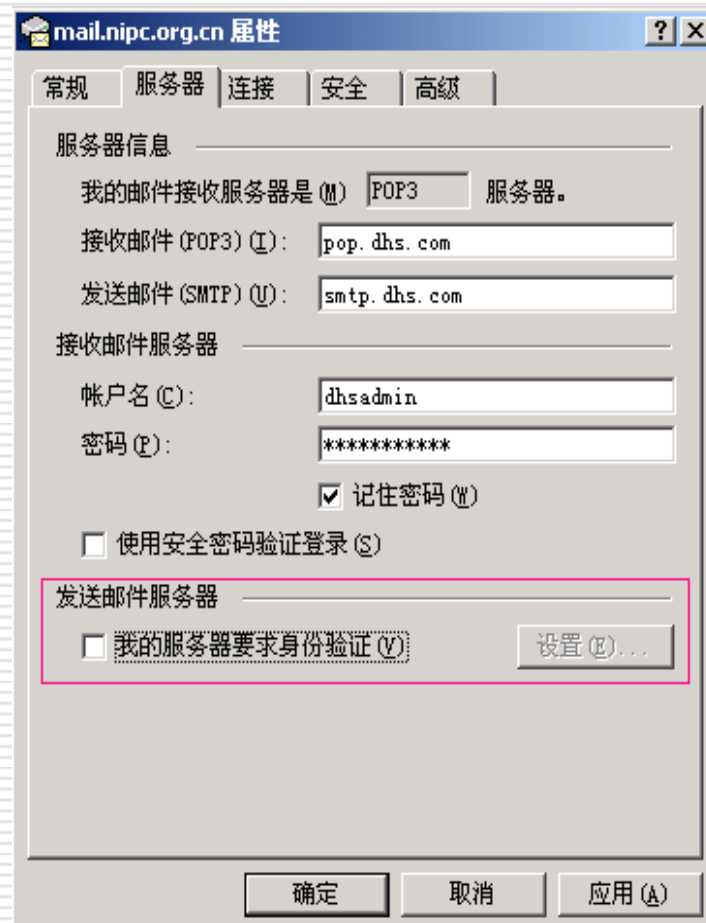
- 这主要是利用人们的大意心理。
- 攻击者找到一个受害者熟悉的名字。有了这个名字后，攻击者注册一个看上去像受害者熟悉的名字的邮件地址。这样收信人很可能会回复这个邮箱发来信，这样攻击者就有得到想要信息的可能性。

直接使用伪造的**Email**地址

- ❑ **SMTP**协议（即简单邮件传输协议）有着一个致命的缺陷：它所遵循过于信任的原则，没有设计身份验证系统。**SMTP**建立在假定人们的身份和他们所声称一致的基础之上，没有对邮件发送者的身份进行验证。
- ❑ 这使得人们可以随意构造发件人地址来发送邮件。下页我们通过修改邮件客户端软件的安装来示例这一点。

直接使用伪造的Email地址

对于那些没有设置**SMTP**身份验证功能的邮件服务器，例如右图所示的**Outlook**邮件客户软件就不需要做相应的设置，当用户使用邮件客户软件发出电子邮件时，发送邮件服务器不会对发件人地址进行验证或者确认，因此攻击者能够随意指定他想使用的所有地址，而这些地址当然会作为邮件源出现在收件人的信中。



直接使用伪造的Email地址

此外，在右图所示的例子中，攻击者还能够指定他想要的任何邮件返回地址。因此当用户回信时，答复回到攻击者所掌握的邮箱**test@test**，而不是回到被盗用了地址的人那里。



远程登录到**SMTP**端口

- ❑ **SMTP**协议一般使用**25**号端口，邮件服务器通过它在互联网上发送邮件。
- ❑ 执行电子邮件欺骗的一个比较复杂的方法是远程登录到邮件服务器的**25**号端口发送邮件。

远程登录到25号端口(2)

- ❑ 攻击者首先找到邮件服务器的**IP**地址，或者通过运行端口扫描程序来判断哪些机器是**25**号端口开放的邮件服务器。
- ❑ 在攻击者有了一台**25**号端口开放的机器和一台正在运行的邮件服务器后，输入下面的命令：**telnet *IP地址* 25**
- ❑ 在连接上以后，再输入下面的内容：
HELO
MAIL FROM: *欺骗伪装的mail地址*
RCPT TO: *收件的危害者mail地址*
DATA
邮件的内容

示例：远程登录25端口的Email欺骗

□ 实验环境

- 局域网mail服务器为192.168.1.250
- Mail服务器不需要身份验证
- 内有两个用户分别为：
 - liuy@lan.nipc
 - chensl@lan.nipc

□ 实验方式

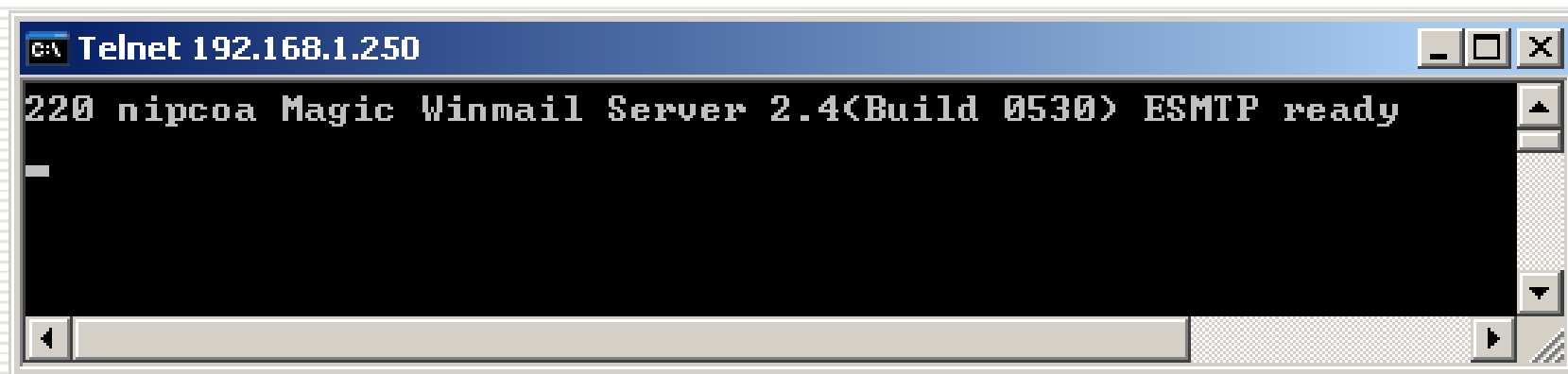
- 伪装成liuy@lan.nipc给chensl@lan.nipc发邮件

Email欺骗过程—telnet到服务器

- 通过**telnet**，连接到邮件服务器的**25**端口。
在**cmd.exe**下使用的命令：

telnet 192.168.1.250 25

- 结果如图所示，说明已经连接到了**25**端口



Email欺骗过程—发送邮件内容

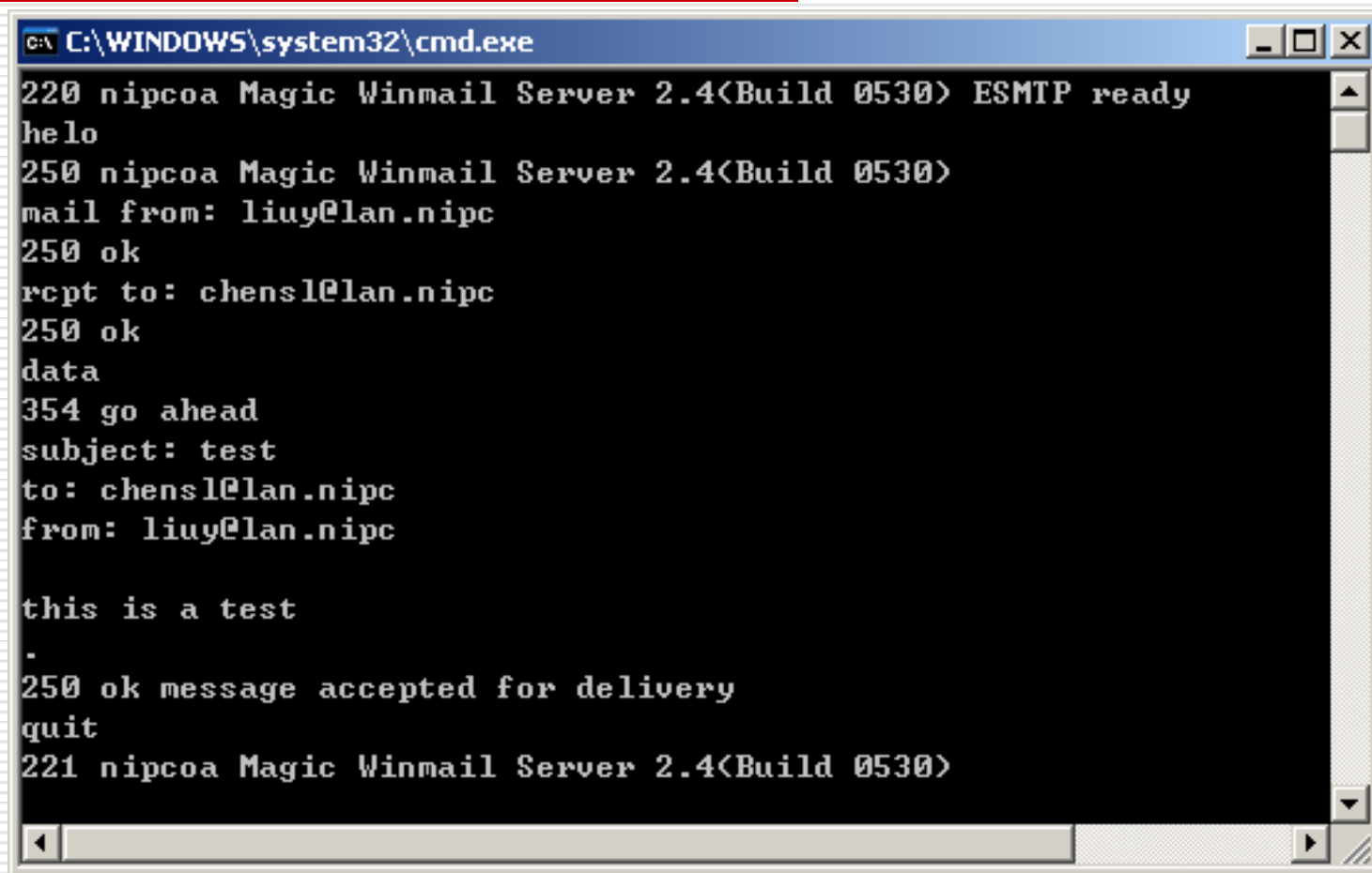
- 220 nipcoa Magic Winmail Server 2.4(Build 0530) ESMTP ready
- **helo**
- 250 nipcoa Magic Winmail Server 2.4(Build 0530)
- **mail from: liuy@lan.nipc**
- 250 ok
- **rcpt to: chensl@lan.nipc**
- 250 ok
- **data**
- 354 go ahead
- **subject: test**
- **to: chensl@lan.nipc**
- **from: liuy@lan.nipc**

- **this is a test**
- **.**
- 250 ok message accepted for delivery
- **quit**
- 221 nipcoa Magic Winmail Server 2.4(Build 0530)



红色部分是根据**SMTP**协议自行输入的内容；黑色部分是服务器的返回信息。

Email欺骗过程—发送邮件内容截屏

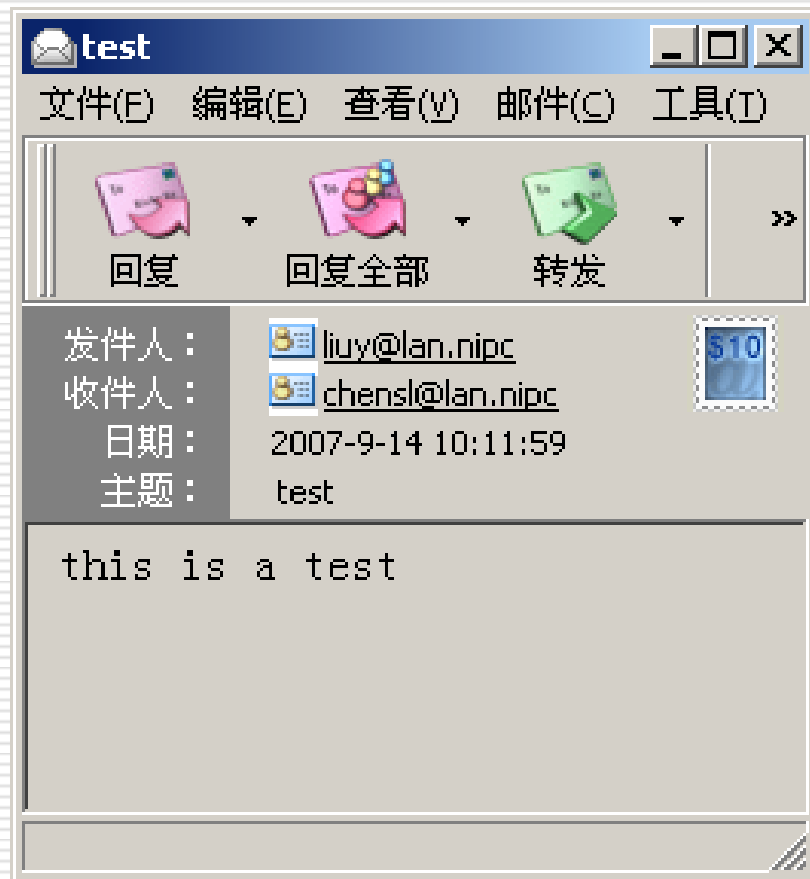


```
C:\WINDOWS\system32\cmd.exe
220 nipcoa Magic Winmail Server 2.4<Build 0530> ESMTP ready
helo
250 nipcoa Magic Winmail Server 2.4<Build 0530>
mail from: liuy@lan.nipc
250 ok
rcpt to: chensl@lan.nipc
250 ok
data
354 go ahead
subject: test
to: chensl@lan.nipc
from: liuy@lan.nipc

this is a test
.
250 ok message accepted for delivery
quit
221 nipcoa Magic Winmail Server 2.4<Build 0530>
```

Email欺骗过程—结果

- ❑ 用户 **chensl@lan.nipc** 将收到来自 **liuy@lan.nipc** 的邮件，如图所示。
- ❑ 但是 **liuy@lan.nipc** 并不知道自已发送了邮件。
- ❑ 试想，如果邮件的内容里有病毒或者其它恶意代码，且 **chensl@lan.nipc** 信任 **liuy@lan.nipc**，那么将会是一件多么危险的事情啊。



5.4.2 电子邮件欺骗的防御

- 做为互联网用户，必须时刻树立风险意识，不要随意打开一个不可信任的邮件。
- 此外，下面介绍几种防范方法分别从这几个方面入手：
 - 邮件接收者
 - 邮件发送者
 - 邮件服务器
 - 邮件加密

防范方法—邮件接收者

- 做为邮件接收者来说，用户需要合理配置邮件客户端，使每次总能显示出完整的电子邮件地址，而不是仅仅显示别名，完整的电子邮件地址能提供一些迹象表明正在发生一些不平常的事情。
- 用户应该注意检验发件人字段，不要被相似的发信地址所蒙蔽。

防范方法—邮件发送者

- 做为邮件发送者来说，如果你使用 **foxmail** 或者 **outlook** 之类的邮件客户端，你必须保护好这些邮件客户端，防止他人对客户端的设置进行修改。

防范方法—邮件服务器

- 对于邮件服务器提供方来说，采用的**SMTP**身份验证机制。
- 原来使用**SMTP**协议发送邮件的时候并不需要任何验证，身份欺骗极易实现。现在将**POP**协议收取邮件需要用户名/密码验证的思想移至到**SMTP**协议，发送邮件也需要类似的验证。绝大多数邮件服务提供商都是采用的这种做法，通常是使用与接收邮件相同的用户名和密码来发送邮件。
- 采用这种方法之后，虽然**SMTP**协议安全性的问题仍然无法从根本上得到解决，但是电子邮件欺骗已经变得不像过去那么容易了。

防范方法—PGP加密

- 还有一种可能的解决方法是使用公钥加密，其中应用最广泛的的就是**PGP**邮件加密。
- **PGP (Pretty Good Privacy)** 是一个可以让您的电子邮件拥有保密功能的程序。藉此你可以将你的邮件加密，一旦加密后，邮件看起来是一堆无意义的乱码。**PGP** 提供了极强的保护功能，即使是最先进的解码分析技术也无法解读加密后的文字。
- **PGP** 加密与解密不像其它传统加密的方式，而是以公钥密码学为基础的。

防范方法—PGP加密（2）

- 举例来说，当你要传送一封保密信或档案给某人时，必须先取得那人的公钥（**Public Key**），然后利用这个公钥将信件加密。当某人收到您加密的信件后，他必须利用相应的私钥（**Secret Key**）来解密。因此，除非其它人拥有收信者的私钥，否则无法解开发信人所加密的信件。同时，收信人在使用私钥解密时，还必须输入通行码，如此又对加密后的邮件多了一层保护。

5.5 DNS欺骗及防御技术

- **5.5.1 DNS工作原理**
- **5.5.2 DNS欺骗的原理及实现步骤**
- **5.5.3 DNS欺骗的局限性及防御**

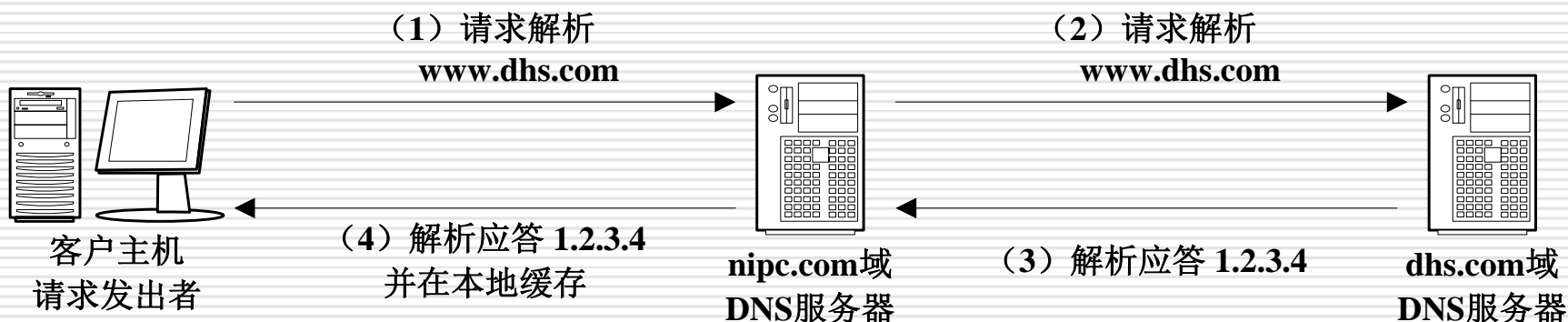
5.5.1 DNS工作原理

- **DNS**的全称是**Domain Name Server**即域名服务器，当一台主机发送一个请求要求解析某个域名时，它会首先把解析请求发到自己的**DNS**服务器上。
- **DNS**的功能是提供主机名字和**IP**地址之间的转换信息。
- **DNS**服务器里有一个“**DNS缓存表**”，里面存储了此**DNS**服务器所管辖域内主机的域名和**IP**地址的对应关系。

5.5.1 DNS工作原理

- ❑ 例如，客户主机需要访问**www.dhs.com**时，首先要知道**www.dhs.com**的**IP**地址。
- ❑ 客户主机获得**www.dhs.com** **IP**地址的唯一方法就是向所在网络设置的**DNS**服务器进行查询。
- ❑ 查询过程分四步进行，见下页图。

5.5.1 DNS工作原理



上图中有三台主机：客户主机、**nipc.com**域**DNS**服务器和**dhs.com**域**DNS**服务器。其中**nipc.com**域**DNS**服务器直接为客户主机提供**DNS**服务。下面对这四个过程进行解释。

DNS域名解析过程

- **1)** 客户主机软件(例如**Web浏览器**)需要对**www.dhs.com**进行解析, 它向本地**DNS**服务器(**nipc.com**域)发送域名解析请求, 要求回复**www.dhs.com**的**IP**地址;
- **2)** 由于本地**DNS**服务器的数据库中没有**www.dhs.com**的记录, 同时缓存中也没有记录, 所以, 它会依据**DNS**协议机器配置向网络中的其他**DNS**服务器提交请求。这个查询请求逐级递交, 直到**dhs.com**域的真正权威**DNS**服务器收到请求(这里省略了寻找**dhs.com**域**DNS**服务器的迭代过程, 假定本地**DNS**服务器最终找到了所需要的信息);

DNS域名解析过程（2）

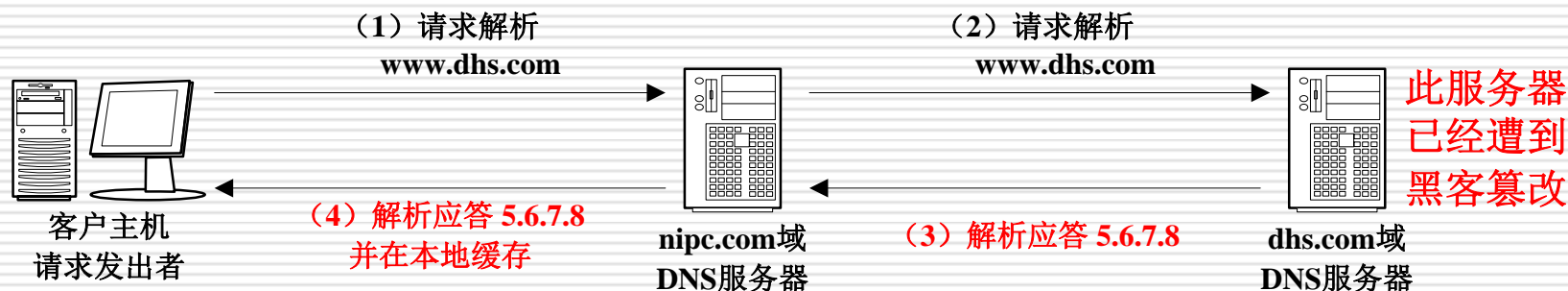
- **3) dhs.com域DNS服务器将向nipc.com域DNS服务器返回IP查询结果(假定为1.2.3.4);**
- **4) nipc.com域的本地DNS服务器最终将查询结果返回给客户主机浏览器，并将这一结果存储到其DNS缓存当中，以便以后使用。在一段时间里，客户主机再次访问www.dhs.com时，就可以不需要再次转发查询请求，而直接从缓存中提取记录向客户端返回IP地址了。**

经过上面几步，客户主机获得了它所期待的**www.dhs.com**网站的**IP**地址，这样整个域名解析过程就结束了。

5.5.2 DNS欺骗的原理及实现步骤

- 当客户主机向本地**DNS**服务器查询域名的时候，如果服务器的缓存中已经有相应记录，**DNS**服务器就不会再向其他服务器进行查询，而是直接将这条记录返回给用户。
- 而入侵者欲实现**DNS**欺骗，关键的一个条件就是在**DNS**服务器的本地**Cache**中**缓存一条伪造**的解析记录。

5.5.2 DNS欺骗的原理及实现步骤



- 在上面例子中，假如**dhs.com**域**DNS**服务器返回的是经过攻击者篡改的信息，比如将**www.dhs.com**指向另一个**IP**地址**5.6.7.8**，**nipc.com**域**DNS**服务器将会接受这个结果，并将错误的信息存储在本地**Cache**中。

5.5.2 DNS欺骗的原理及实现步骤

- 以后在这条缓存记录的生存期内，再向 **nipc.com** 域 **DNS** 服务器发送的对 **www.dhs.com** 的域名解析请求，所得到的 **IP** 地址都将是被篡改过的。

5.5.2 DNS欺骗的原理及实现步骤

- 有了对**DNS**服务器进行欺骗的可能，攻击者怎样伪造**DNS**应答信息就成了问题的焦点。
- 目前有两种可能情况下的实现办法：
 - 攻击者可以控制本地的域名服务器
 - 攻击者无法控制任何**DNS**服务器

第一种可能情况

- 一种可能是，攻击者可以控制本地的域名服务器(假定是**nipc.com**域的权威)，在其数据库中增加一个附加记录，将攻击目标的域名(例如**www.dhs.com**)指向攻击者的欺骗**IP**。
- 紧接着，攻击者向**dhs.com**域**DNS**服务器发送对**some.nipc.com**域名的解析请求。**dhs.com**域的**DNS**服务器自然转而向**nipc.com**域的**DNS**服务器发送请求。

第一种可能情况(2)

- 这时候，本地的域名服务器除了返回正常的 **some.nipc.com** 的 **IP** 地址外，还会在返回包中附加 **www.dhs.com** 的映射记录。如果 **dhs.com** 域的 **DNS** 服务器允许缓存所有收到的信息的话，发过来的 **www.dhs.com** 的伪造映射记录便“注射”到其 **Cache** 中了。

第二种可能情况

- 另一种更现实的情况，就是攻击者无法控制任何**DNS**服务器，但他可以控制该服务所在网络的某台主机，并可以监听该网络中的通信情况。这时候，黑客要对远程的某个**DNS**服务器进行欺骗攻击，所采用的手段很像**IP**欺骗攻击：
- 首先，黑客要冒充某个域名服务器的**IP**地址；
- 其次，黑客要能预测目标域名服务器所发送**DNS**数据包的**ID**号。
- 确定目标**DNS**服务器的**ID**号即为**DNS**欺骗攻击的关键所在

第二种可能情况(2)

- **DNS**数据是通过**UDP**协议传递的，在**DNS**服务器之间进行域名解析通信时，请求方和应答方都使用**UDP 53**端口，而这样的通信过程往往是并行的，也就是说，**DNS**域名服务器之间同时可能会进行多个解析过程，既然不同的过程使用相同的端口号，那靠什么来彼此区别呢？
- 答案就在**DNS**报文里面。**DNS**报文格式头部的**ID**域，是用于区别不同会话过程的，这有点类似于**TCP**中的序列号，域名解析的请求方和应答方只有使用相同的**ID**号才能证明是同一个会话(由请求方决定所使用的**ID**)。
- 不同的解析会话，采用不同的**ID**号。

第二种可能情况(3)

- 在一段时期内，**DNS**服务器一般都采用一种有章可循的**ID**生成机制，例如，对于每次发送的域名解析请求，依次将数据包中的**ID**加**1**。
- 如此一来，攻击者如果可以在某个**DNS**服务器的网络中进行嗅探，他只要向远程的**DNS**服务器发送一个对本地某域名的解析请求，通过嗅探得到的来自目标**DNS**服务器的请求数据包（因为远程**DNS**服务器肯定会转而请求本地的**DNS**服务器），攻击者就可以得到想要的**ID**号了。

第二种可能情况(4)

□ 例子:

nipc.com域的**DNS**服务器向**dhs.com**域的**DNS**服务器请求解析，如果攻击者所伪造的**DNS**应答包中含有正确的**ID**号，并且抢在**dhs.com**域的**DNS**服务器之前向**nipc.com**域的**DNS**服务器返回伪造信息，欺骗攻击就将获得成功的。

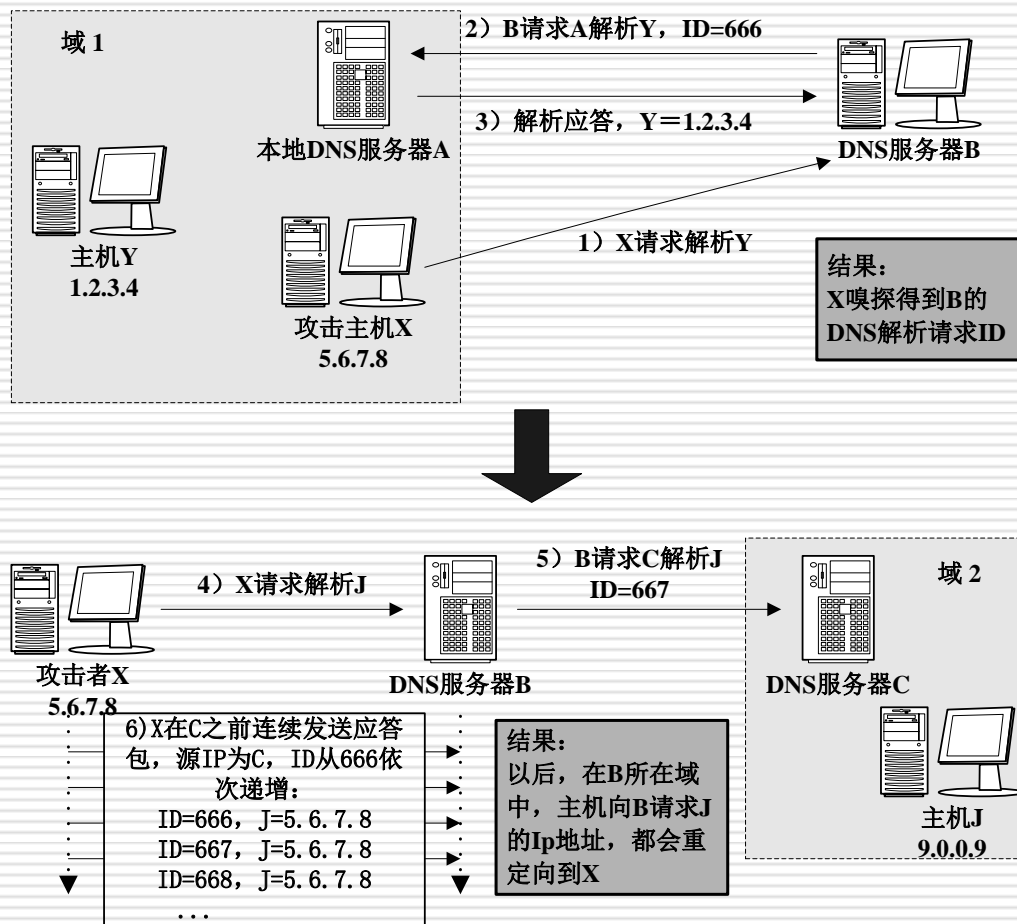
第二种可能情况(5)

- 其实，即使攻击者无法监听某个拥有**DNS**服务器的网络，也有办法得到目标**DNS**服务器的**ID**号。
 - 首先，他向目标**DNS**服务器请求对某个不存在域名地址（但该域是存在的）进行解析。
 - 然后，攻击者冒充所请求域的**DNS**服务器，向目标**DNS**服务器连续发送应答包，这些包中的**ID**号依次递增。
 - 过一段时间，攻击者再次向目标**DNS**服务器发送针对该域名的解析请求，如果得到返回结果，就说明目标**DNS**服务器接受了刚才黑客的伪造应答，继而说明黑客猜测的**ID**号在正确的区段上，否则，攻击者可以再次尝试。

第二种可能情况(6)

- 实际攻击中，第二种攻击方法实现比较复杂。
- 知道了**ID**号，并且知道了**ID**号的增长规律，以下的过程类似于**IP**欺骗攻击。

一次DNS欺骗攻击的完整过程



5.5.3 DNS欺骗的局限性及防御

□ DNS欺骗主要存在两点局限性:

- 攻击者不能替换缓存中已经存在的记录
- DNS服务器存在缓存刷新时间问题

5.5.4 DNS欺骗的局限性及防御

□ 在配置DNS服务器的时候注意：

- 使用最新版本DNS服务器软件并及时安装补丁；
- 关闭DNS服务器的递归功能：DNS服务器利用缓存中的记录信息回答查询请求或是DNS服务器通过查询其它服务器获得查询信息并将它发送给客户机，这两种查询方式称为**递归查询**，这种查询方式容易导致DNS欺骗。
- 限制区域传输范围：限制域名服务器做出响应的地址、限制域名服务器做出响应的递归请求地址、限制发出请求的地址；
- 限制动态更新；
- 采用分层的DNS体系结构。

5.6 Web欺骗及防御技术

- 5.6.1 Web欺骗的概念
- 5.6.2 Web欺骗的工作原理
- 5.6.3 Web欺骗案例
- 5.6.4 Web欺骗的防御

5.6.1 Web欺骗的概念

- **Web**站点给用户提供了丰富多彩的信息，**Web**页面上的文字、图画与声音可以给人深刻的印象。在计算机世界中，我们往往都习惯各类图标、图形，代表各类不同的含义。
- 人们往往还会在事件的时间先后顺序中得到某种暗示。如果在单击银行的网页时**username**对话框同时出现了，用户自然会认为应该输入在该银行的账户与口令。如果你在单击了一个文档链接后，立即开始了下载，那么你很自然地会认为该文件正从该站点下载。然而，以上的想法不一定总是正确的。

5.6.1 Web欺骗的概念

- ❑ **Web**欺骗是一种电子信息欺骗，攻击者创造了一个完整的令人信服的**Web**世界，但实际上它却是一个虚假的复制。
- ❑ 虚假的**Web**看起来十分逼真，它拥有相同的网页和链接。然而攻击者控制着这个虚假的**Web**站点，这样受害者的浏览器和**Web**之间的所有网络通信就完全被攻击者截获。

5.6.1 Web欺骗的概念

- 由于攻击者可以观察或者修改任何从受害者到**Web**服务器的信息，同样地，也控制着从**Web**服务器发至受害者的返回数据，这样攻击者就有发起攻击的可能性。
- 攻击者能够监视被攻击者的网络信息，记录他们访问的网页和内容。当被攻击者填完一个表单并发送后，这些数据将被传送到**Web**服务器，**Web**服务器将返回必要的信息，但不幸的是，攻击者完全可以截获并使用这些信息。

5.6.1 Web欺骗的概念

- 在得到必要的数据后，攻击者可以通过修改受害者和**Web**服务器两方任何一方数据，来进行破坏活动。攻击者可以修改受害者的确认数据，攻击者还可以修改**Web**服务器返回的数据。

5.6.2 Web欺骗的工作原理

- **Web**欺骗能够成功的关键是在受害者和真实**Web**服务器之间插入攻击者的**Web**服务器，这种攻击常被称为“中间人攻击(**man-in-the-middle**)”。

5.6.2 Web欺骗的工作原理

- ❑ 为了建立这样的**Web**服务器，攻击者要完成以下工作：
- ❑ 攻击者改写**Web**页中的所有**URL**地址，使它们指向攻击者的**Web**服务器不是真正的**Web**服务器。例如，
http://www.dhs.com将变为
http://www.hacker.net/。

5.6.2 Web欺骗的工作原理

- 当用户单击改写过的
http://www.dhs.com/连接，将进入
的是**http://www.hacker.net/**，再由
http://www.hacker.net/向
http://www.dhs.com/发出请求并获得
真正的文档，这样攻击者就可以改写文档
中的所有链接，最后经过
http://www.hacker.net/返回给用户的
浏览器。

5.6.2 Web欺骗的工作原理

□ 工作流程如下所示：

- 用户访问伪造过的<http://www.hacker.net/>
- <http://www.hacker.net/>向
<http://www.dhs.com/>请求文档；
- <http://www.dhs.com/>向
<http://www.hacker.net/>返回文档；
- <http://www.hacker.net/>改写文档中的所有URL；
- <http://www.hacker.net/>向用户返回改写后的文档。

5.6.3 Web欺骗案例

- **网络钓鱼** 很多人是闻其名而色变，因为它经常扮演成一只幕后黑手伸向人们的口袋.....
- 确切地讲，网络钓鱼就是那些黑客们借用电子邮件或是模仿网上银行、网上购物等一切网上交易的页面而制作出假的网页页面，以假乱真，让用户在毫不知情的情况下泄露出自己的相关账户信息（账号、密码），一旦这些黑客们得到了用户的账号信息，后果可想而知。
- 经典案例：工商银行网上银行被黑客多次伪造

网络钓鱼乔装银行，众网友自动上钩



2005年1月，一个假冒中国工商银行网站出现在互联网上，诱骗银行卡持有人的帐户和密码，并导致多人的银行存款被盗，直接经济损失达80万元人民币。

中国工商银行网址: <http://www.icbc.com.cn>
假冒工商银行网址: <http://www.1cbc.com.cn>

工商银行网站被仿造又一例



URL露出了马脚

5.6.4 Web欺骗的防御

□ 防范Web欺骗的方法:

- 配置网络浏览器使它总能显示目的URL，并且习惯查看它。
- 检查源代码，如果发生了URL重定向，就一定会发现。不过，检查用户连接的每一个页面的源代码对普通用户来说是不切实际的想法。
- 使用反网络钓鱼软件。
- 禁用JavaScript、ActiveX或者任何其他在本地执行的脚本语言。
- 确保应用有效和能适当地跟踪用户。无论是使用cookie还是会话ID，都应该确保要尽可能的长和随机。
- 培养用户注意浏览器地址线上显示的URL的好习惯。培养用户的安全意识和对开发人员的安全教育。

5.7 小结

- ❑ 本章讲述了各种形式的欺骗攻击技术，包括**IP**欺骗、**ARP**欺骗、电子邮件欺骗、**DNS**欺骗和**Web**欺骗，所有这些攻击技术都是得到广泛应用的，当然也因此造成了许多麻烦。理解它们的实现原理有助于防范这些欺骗攻击活动。
- ❑ 这些基本的攻击技术也经常和其他一些攻击相结合，试图造成更大的混乱。
- ❑ 因此本章还介绍了对应以上各种攻击的防范方法。

谢谢各位!