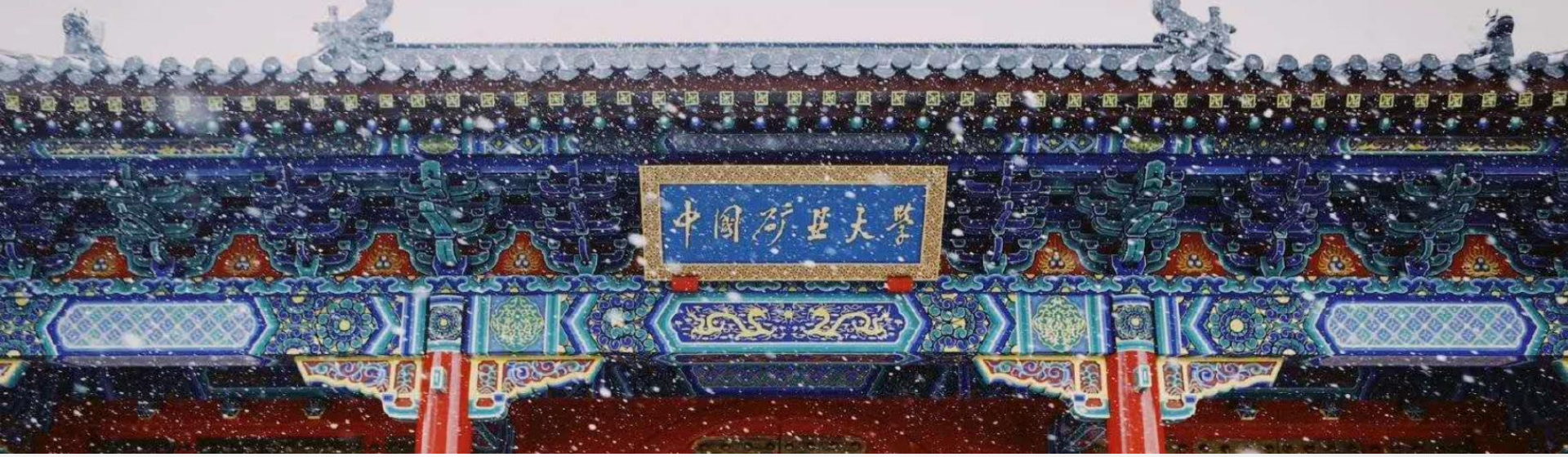


网络攻击与防御

CH05—欺骗攻击与防御

中国矿业大学 网络空间安全系

is.cumt.edu.cn

知己知彼，百战不殆；不知彼而知己，一胜一负；不知彼不知己，每战必败。

——《孙子兵法》

法无定法

——《金刚经》

warning: 请不要轻易出手

目录（Contents）

欺骗攻击

- **欺骗**：冒充身份通过认证以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，从而与受害者交流，以**获取信息或者展开进一步攻击**
- **常见的欺骗攻击：**
  - **IP欺骗**
  - **ARP欺骗**
  - **电子邮件欺骗**
  - **DNS欺骗**
  - **Web欺骗**

假作真时真亦假，无为有处有还无

ARP欺骗

ARP基础知识

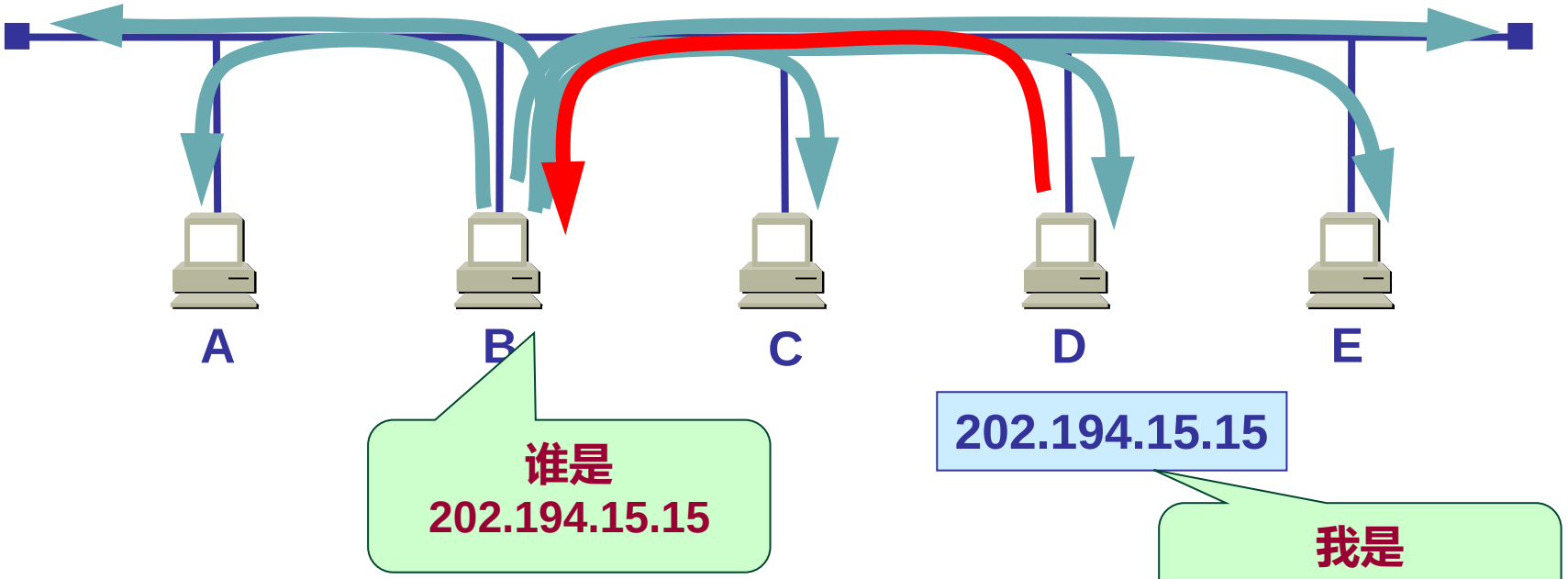
- ARP(Address Resolution Protocol)：地址解析协议，用于将IP地址（32位）转化为网卡的物理地址（MAC地址48位）,属于数据链路层的协议。
- 在以太网中，数据帧从一个主机到达局域网内的另一台主机是根据48位的以太网地址（MAC地址）来确定的，而不是根据IP地址。

ARP基础知识

- ARP地址解析的工作原理：

IP地址 —ARP→ MAC地址

建立在网络互相信任的基础上



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：

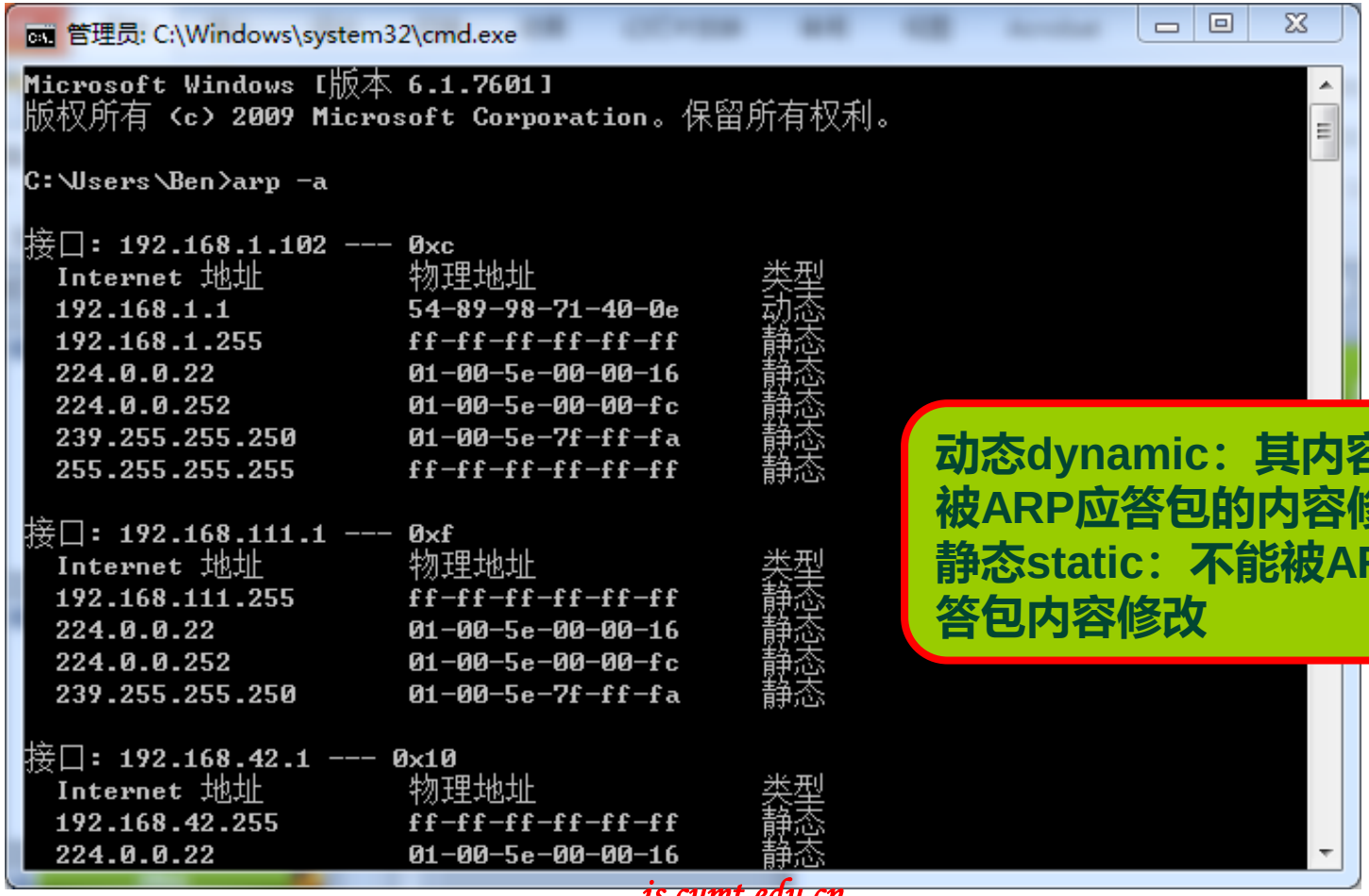
    arp reply 192.168.1.1 is-at 00:00:0c:07:ac:00

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欺骗

- 每台主机、网关都有一个**ARP缓存表**，用于存储局域网内的主机或网关**IP—MAC的对应关系**
  - **arp –a**

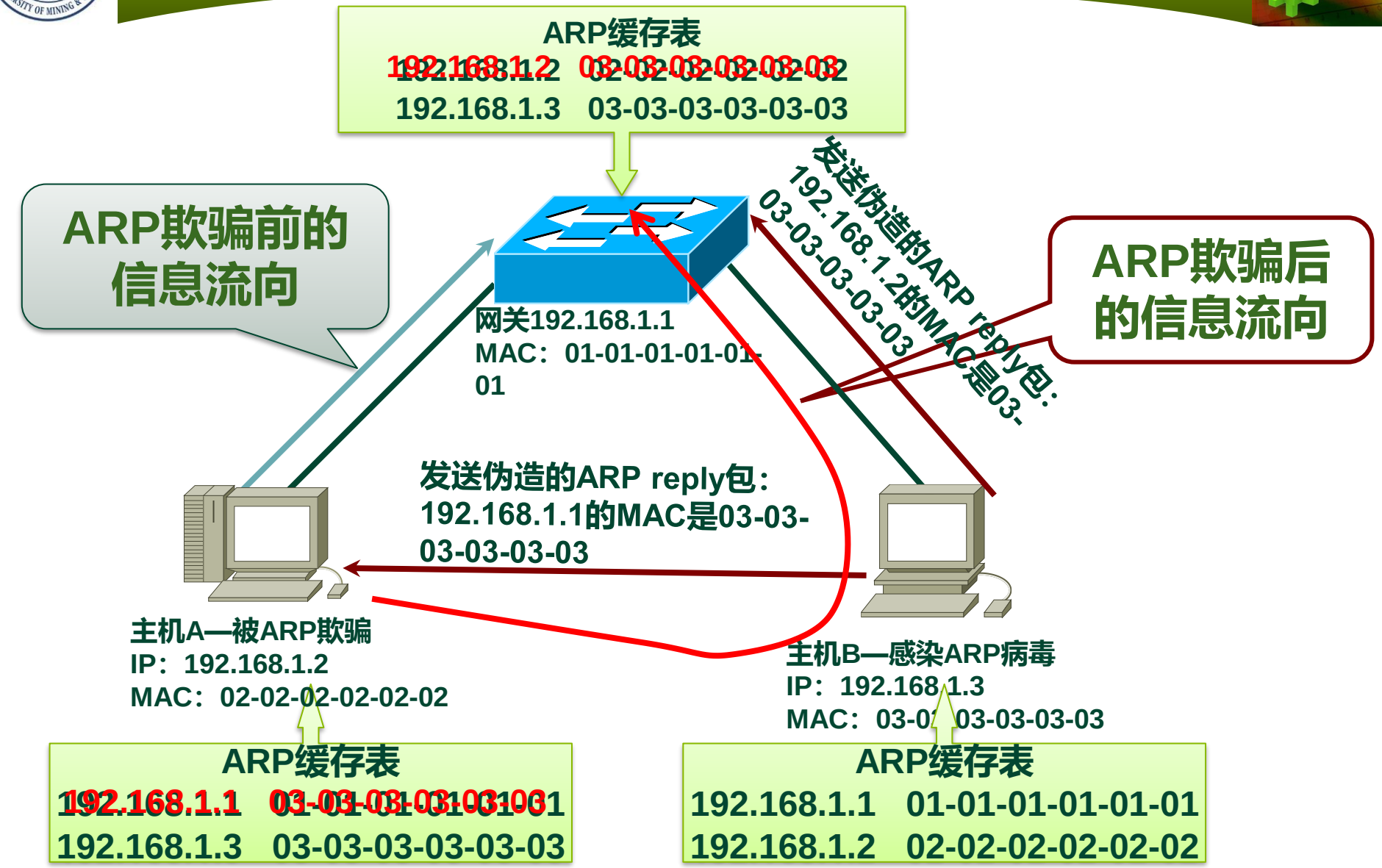


动态dynamic：其内容可以被ARP应答包的内容修改
静态static：不能被ARP应答包内容修改

ARP欺骗

- **ARP的缺陷**：主机收到应答包后
  - **不验证**自己**是否发送**过对应的ARP请求
  - **不验证**该回应包**是否可信**
  - **直接**用应答包里的信息**替换**ARP缓存表中的原有信息

ARP欺骗原理 —ARP缓存中毒（ARP poisoning）



ARP欺骗

- **ARP欺骗的后果**：
  - 导致同网段的其他用户无法正常上网（频繁断网或网速慢）
  - 嗅探交换式局域网内的所有数据包，从而获取敏感信息
  - 对信息进行篡改，修改重要信息，进而控制受害者会话

- E
- d

ettercap 0.8.0

Start Targets Hosts View Mitm Filters Logging Plugins ?

Host List

IP Address	MAC Address	Description
192.168.149.1	00:50:56:C0:00:08	
192.168.149.2	00:50:56:F9:3B:D6	
192.168.149.134	00:0C:29:85:1E:49	
192.168.149.254	00:50:56:FF:78:58	

driftnet：抓取图片等

Delete Host | Add to Target 1

Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.149.2 added to TARGET1
Host 192.168.149.134 added to TARGET2

ARP poisoning victims:

GROUP 1 : 192.168.149.2 00:50:56:F9:3B:D6

GROUP 2 : 192.168.149.134 00:0C:29:85:1E:49
Starting Unified sniffing...

HTTP : 58.218.185.21:80 -> USER: kuangyedaxue@cumt.edu.cn PASS: 123456789 INFO: http://mail.cumt.edu.cn/
CONTENT: action%3Alogin=&uid=kuangyedaxue%40cumt.edu.cn&nodetect=false&password=123456789&locale=zh_CN

HTTP : 58.218.185.87:80 -> USER: 0003343 PASS: 234444 INFO: http://cwc.cumt.edu.cn/web30/index.aspx
CONTENT: uid=0003343&pwd=234444

HTTP : 58.218.185.52:80 -> USER: admin PASS: admin INFO: http://cs.cumt.edu.cn/admin/
CONTENT: username=admin&password=admin&lbtnEnter.x=43&lbtnEnter.y=27

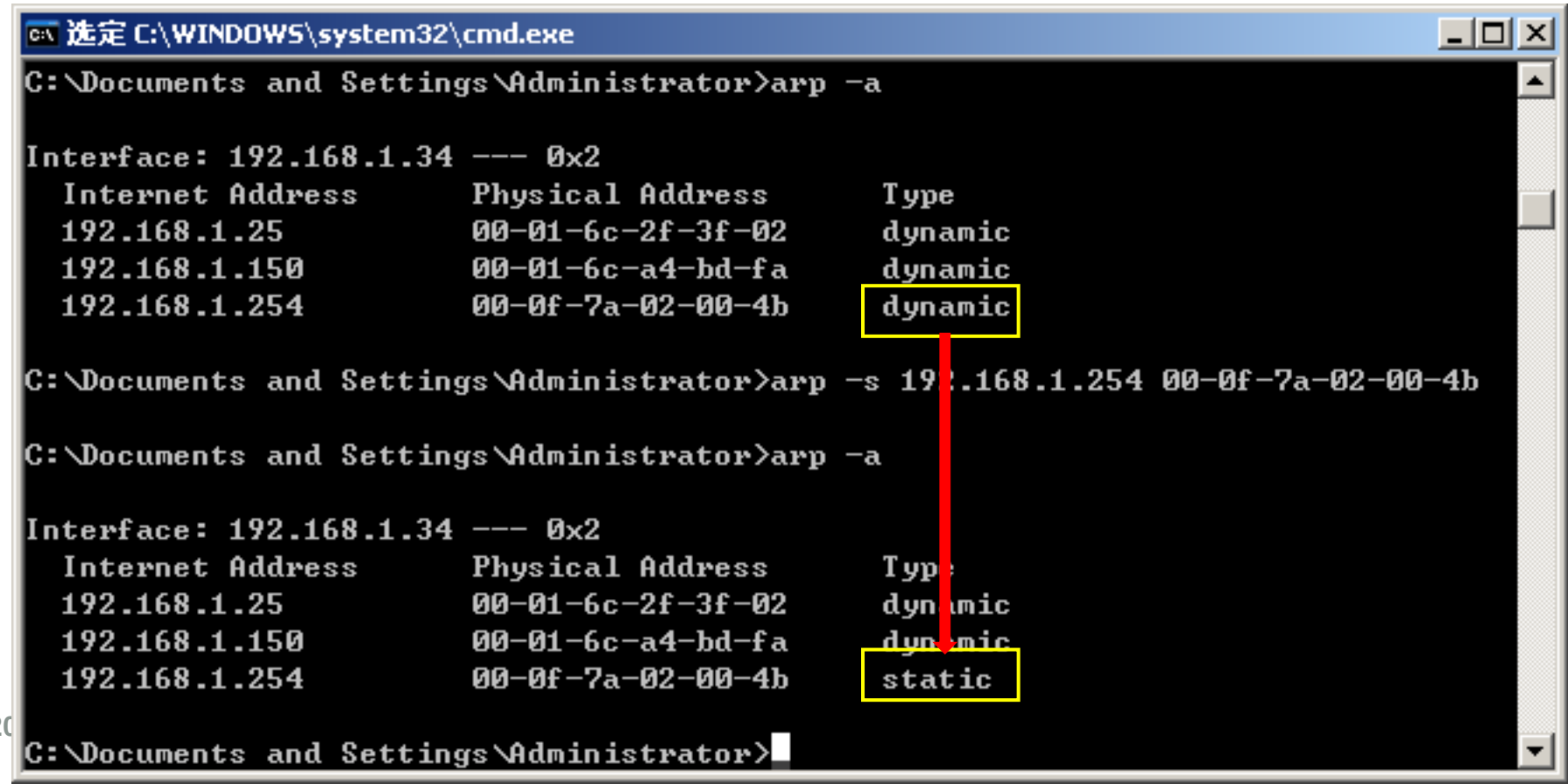
ARP欺骗

- **ARP欺骗的检测**：
  - 网络频繁掉线
  - 网络突然莫名其妙的慢
  - 使用arp –a命令发现网关的MAC地址与真实的网关MAC地址不同
  - 使用网络嗅探软件发现局域网存在大量ARP响应包
- **ARP欺骗的防御**：
  - MAC地址绑定
  - 使用静态ARP缓存
  - 使用ARP服务器（确保该服务器不被控制）
  - 使用ARP欺骗防护软件，如ARP防火墙
  - 及时发现进行ARP欺骗的主机，并将其隔离

ARP欺骗

- **Example：** 在Windows下使用静态的ARP表
  - 假设网关192.168.1.254的MAC为：00-0f-7a-02-00-4b
  - 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



IP欺骗

- **IP协议**：非面向连接，两台计算机的信任连接主要依靠双方的IP地址

- **IP欺骗的方式**：
  - **简单的IP地址更改欺骗**
  - **源路由攻击**
  - **TCP会话劫持**

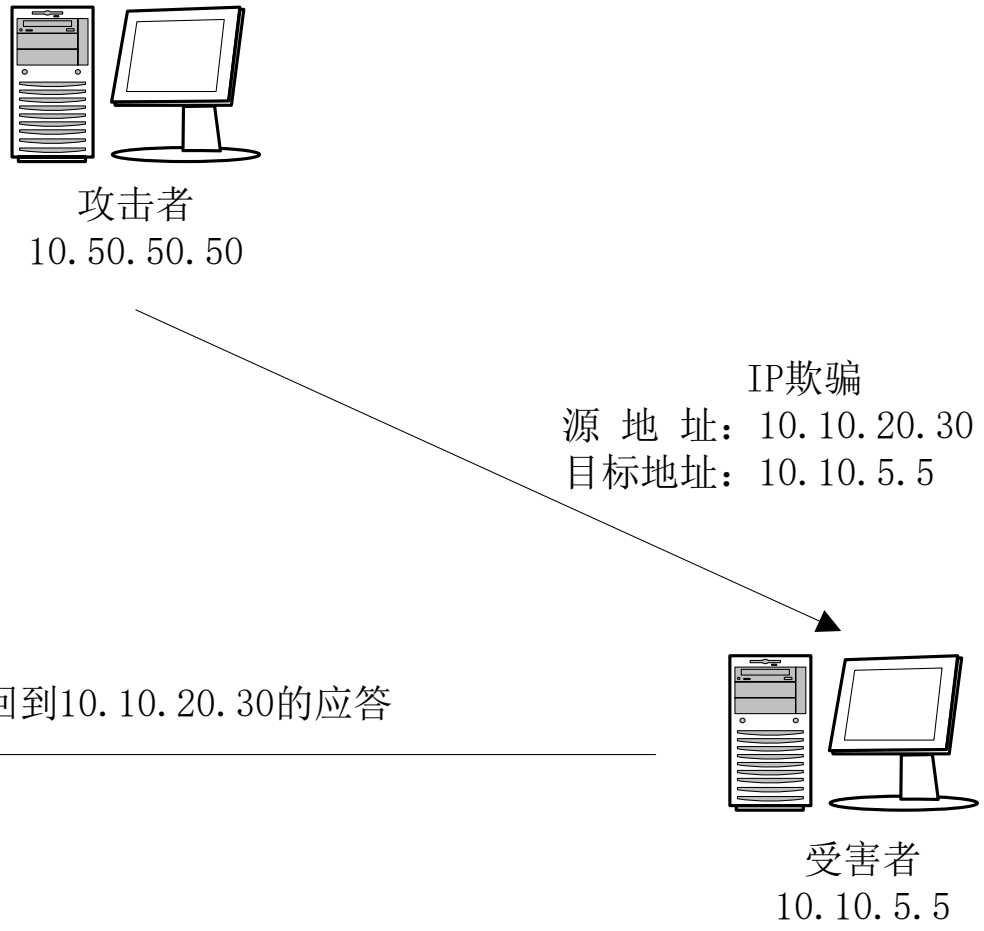
简单的IP地址欺骗

- 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。

- 首先需要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。
- 该欺骗攻击方法的限制：无法建立完整的TCP连接。
- 但适用于UDP（无连接的传输协议），所有单独的UDP数据包都会被发送到受害者的机器中。

简单的IP地址欺骗

攻击者使用假冒的IP地址向一台机器发送数据包，但不会收到任何返回的数据包，这称为盲目飞行攻击（flying blind attack），或者叫单向攻击（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。

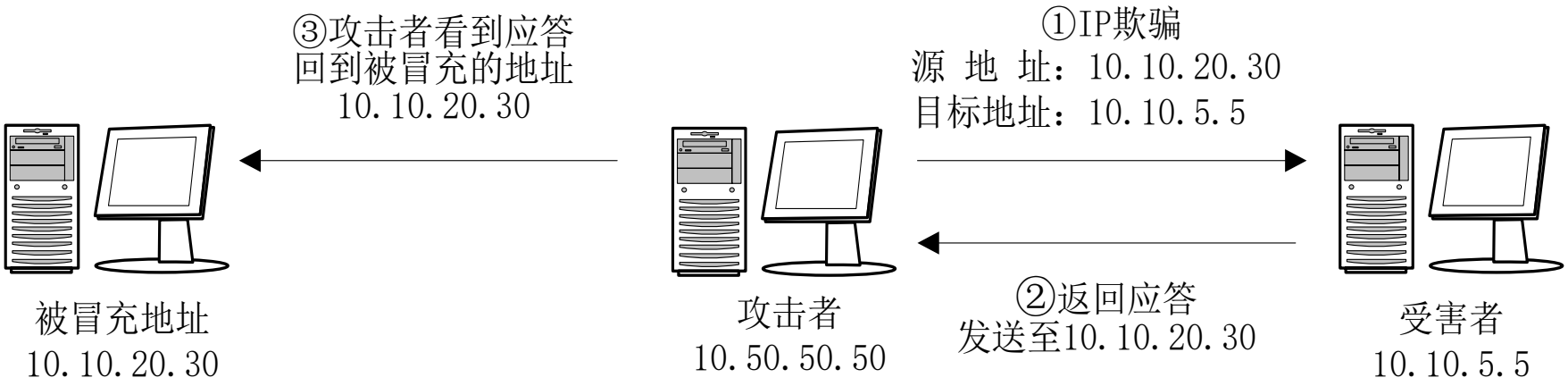


IP 欺骗

- 简单的IP地址欺骗的缺陷是：攻击者无法接收到返回的信息流，为得到从目的主机返回源主机的数据流，有两个方法：
  1. 攻击者插入到正常情况下数据流经过的通路上（中间人攻击）；
  2. 保证数据包会经过一条给定的路径，而且作为一次欺骗攻击，保证它经过攻击者的机器。

IP 欺骗

- 第一种方法其过程如图所示:



但实际实现起来非常困难，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

- 第二种方法：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

- 有两种类型的源路由机制：
  - 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

- 源路由机制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，并指定了源路由机制，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，因为它能获得返回的会话信息。

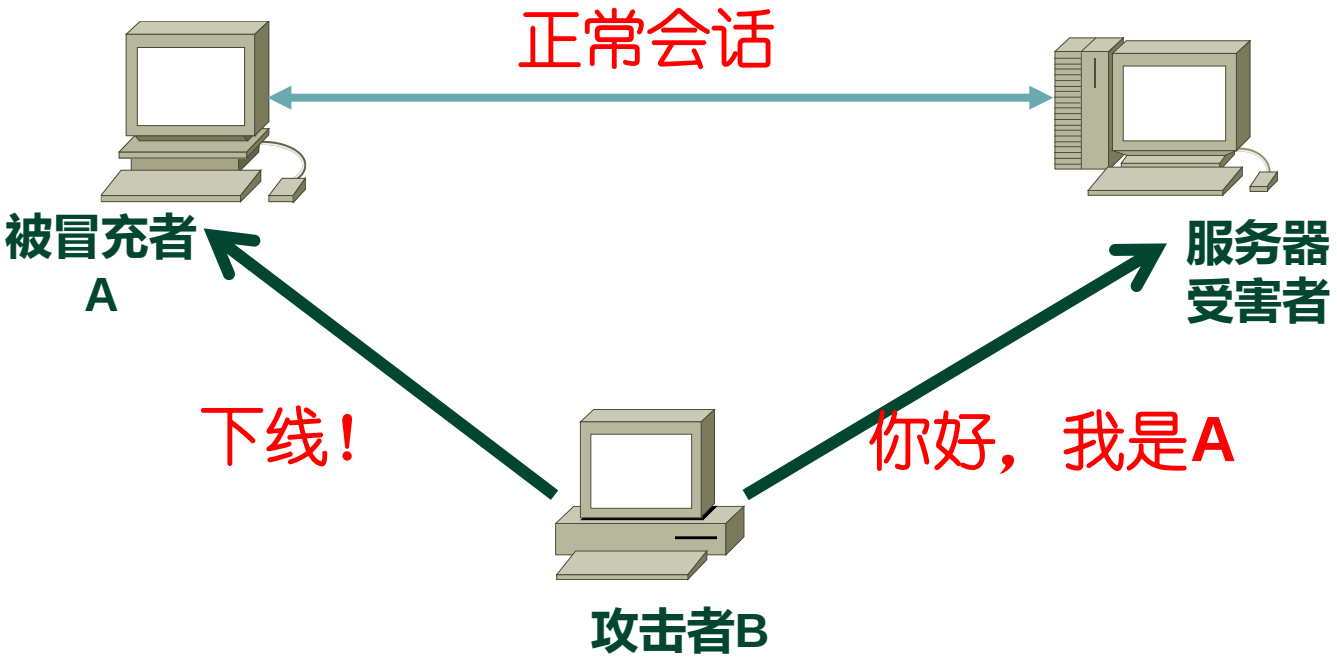
- Remark:源路由机制最多定义8个IP；目前多数路由器已经限制源路由机制；

IP欺骗（高级）---TCP会话劫持

- **会话（Session）：就是两台主机之间的一次通信。**
- 例如通过Telnet登录某台服务器，就建立了一次Telnet会话。
- 会话劫持是一种结合了嗅探和欺骗技术的攻击手段。
- 例如，在一次正常的会话过程当中，攻击者作为第三方参与其中，并在正常数据包中插入恶意数据，或者在双方的会话当中进行监听，甚至代替某一方主机接管会话。

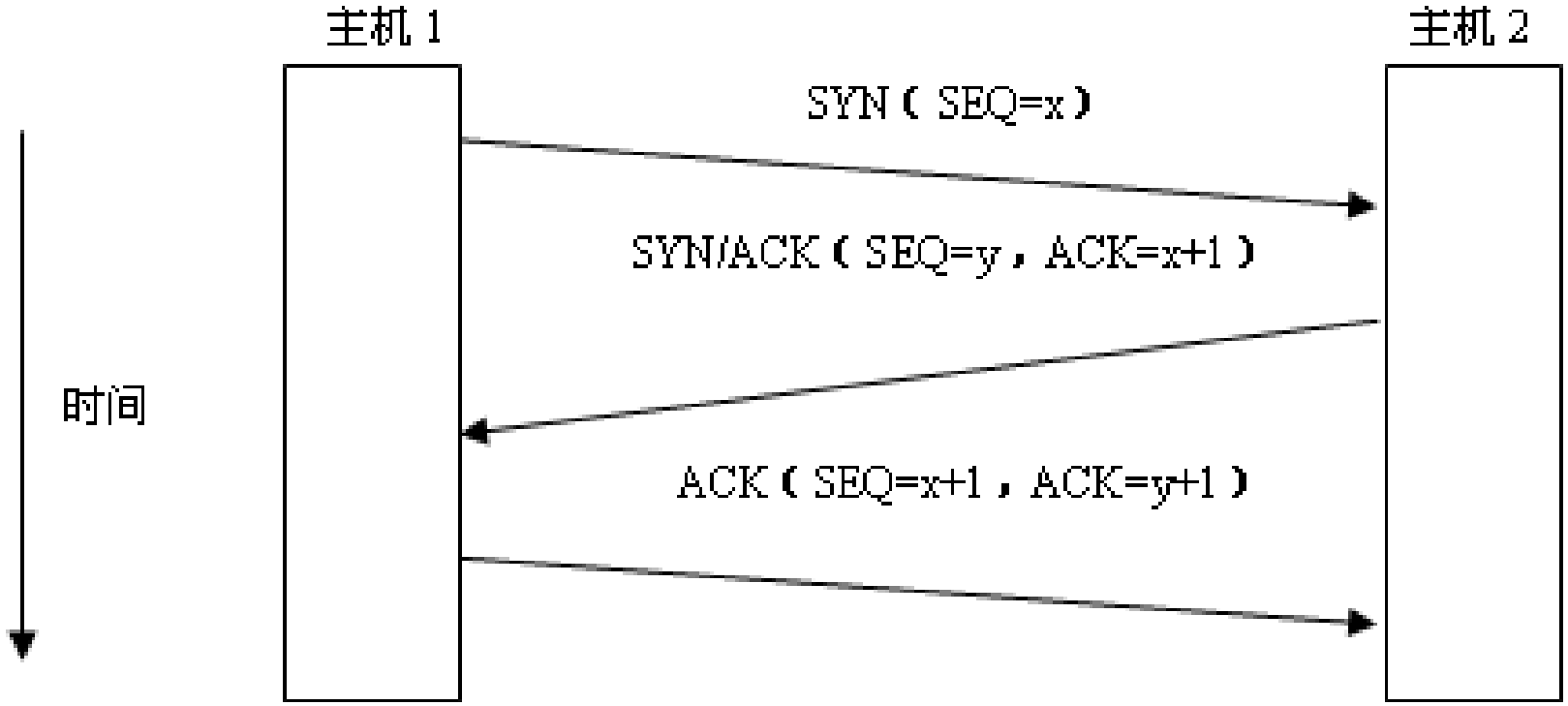
IP欺骗（高级）---TCP会话劫持

- **TCP会话劫持(Session Hijack)：接管现存动态会话的过程，即攻击者可以替代原来的合法用户，同时监视并掌握会话内容**
  - ✓ **会话劫持一般伴随着拒绝服务DoS，且不依赖于操作系统**



- 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，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。
- 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

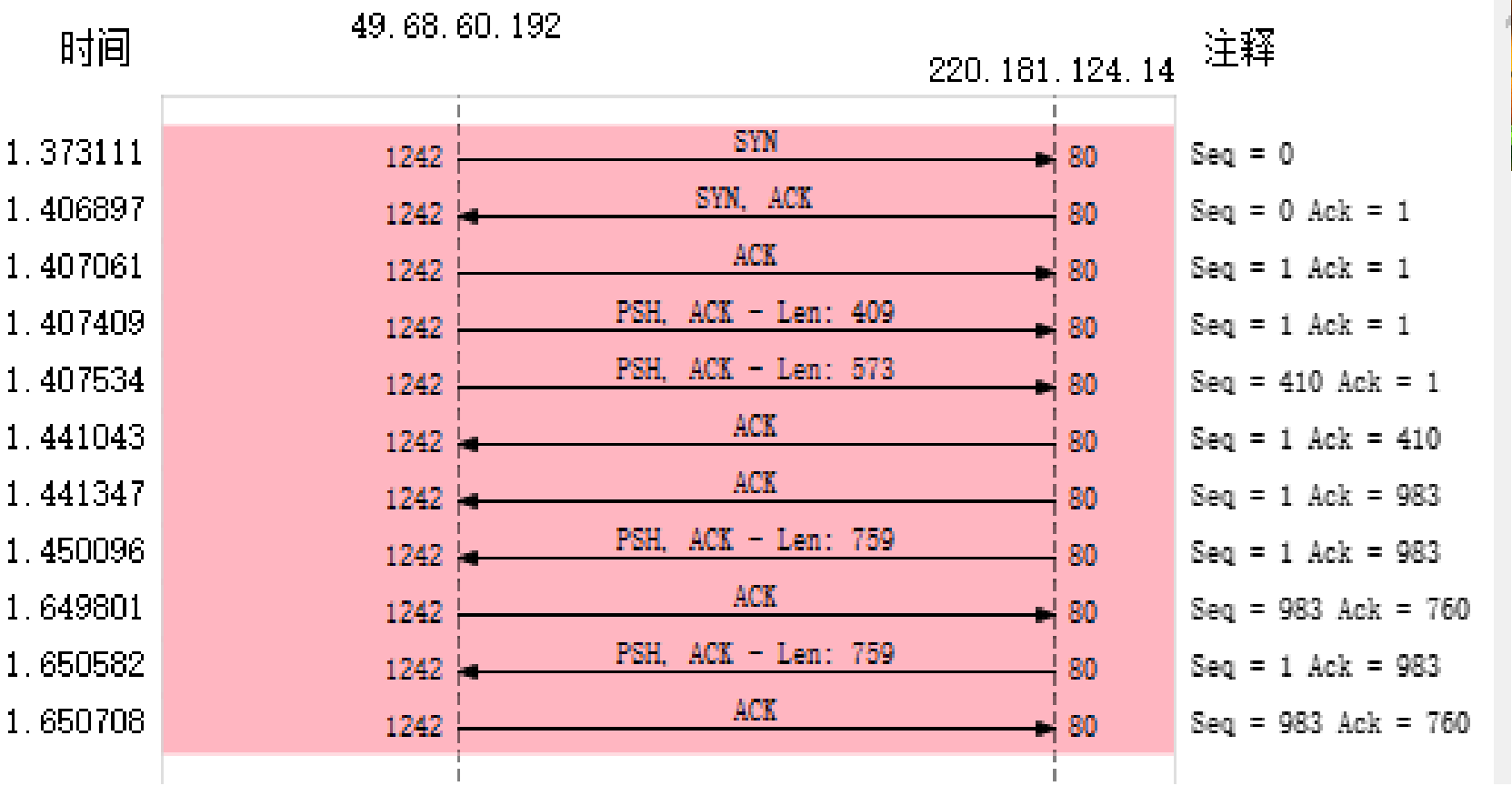
- 为完成上述目的：一个属于发送方的序列号和另一个属于接收方的应答号。
- 发送方发送数据包使用发送方的序列号，同时当接收方确认从发送方接收数据包时，它也用发送方的序列号来进行确认。另一方面，接收方用属于自己的序列号送回数据。

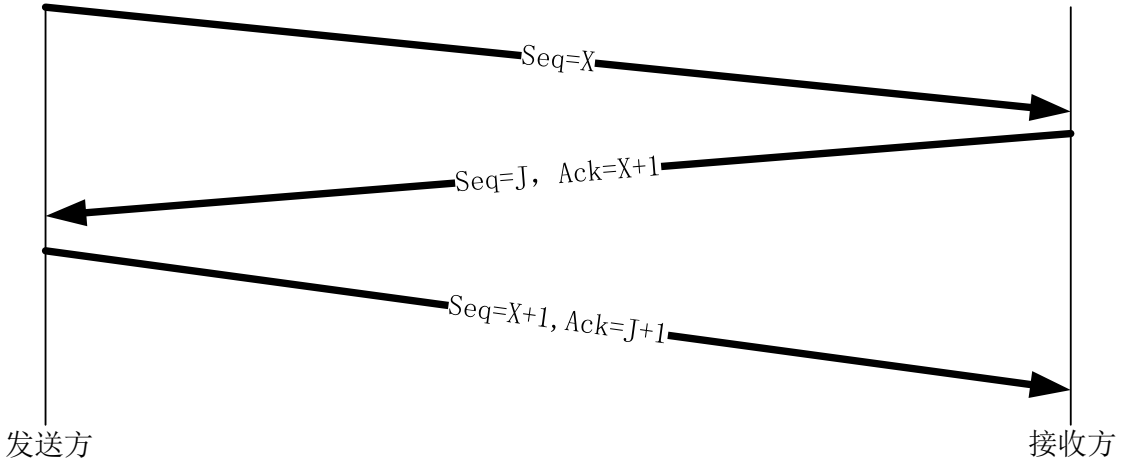
序列号机制

- 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

- 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。


时间
49.68.60.192
220.181.124.14
注释
1.373111
1242
SYN
80
Seq = 0
1.406897
1242
SYN, ACK
80
Seq = 0 Ack = 1
1.407061
1242
ACK
80
Seq = 1 Ack = 1
1.407409
1242
PSH, ACK - Len: 409
80
Seq = 1 Ack = 1
1.407534
1242
PSH, ACK - Len: 573
80
Seq = 410 Ack = 1
1.441043
1242
ACK
80
Seq = 1 Ack = 410
1.441347
1242
ACK
80
Seq = 1 Ack = 983
1.450096
1242
PSH, ACK - Len: 759
80
Seq = 1 Ack = 983
1.649801
1242
ACK
80
Seq = 983 Ack = 760
1.650582
1242
PSH, ACK - Len: 759
80
Seq = 1 Ack = 983
1.650708
1242
ACK
80
Seq = 983 Ack = 760

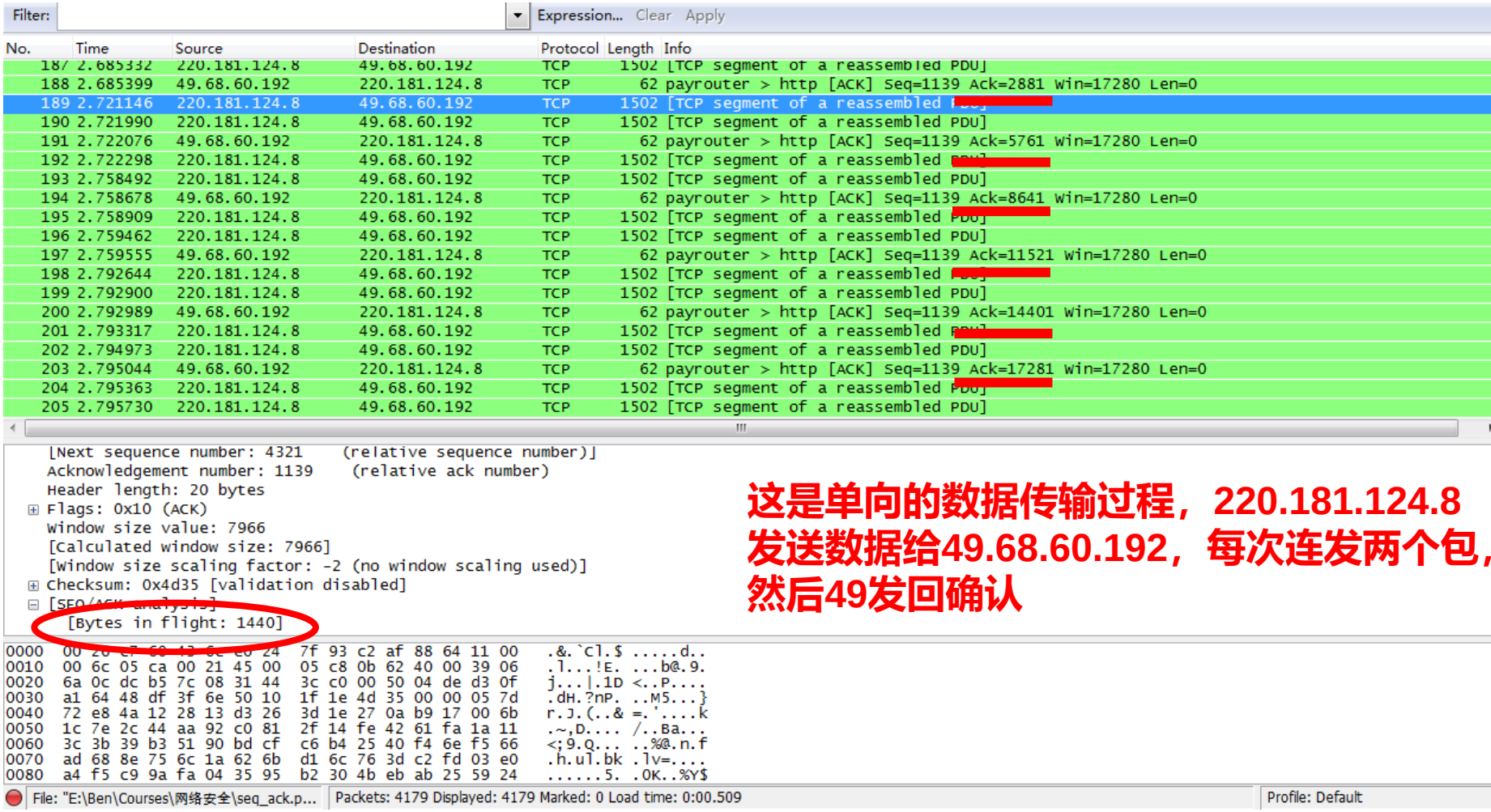

Seq=X
Seq=J, Ack=X+1
Seq=X+1, Ack=J+1
发送方
接收方

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

IP欺骗

❖ 会话劫持的关键之一——TCP序列号猜测:



这是单向的数据传输过程，220.181.124.8发送数据给49.68.60.192，每次连发两个包，然后49发回确认

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

- 寻找合适的目标
- 首先，攻击者希望目标是一个允许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量达到高峰时才会发生的。
- 首先，有很多供选择的会话；其次，网络流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，如果网络流量很大并且有很多的用户进行连接，那么用户很有可能忽略掉线后面隐藏的问题，认为是由于网络流量过大而引起的现象。

step3：猜测序列号

- TCP连接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，猜测出下一对SEQ/ACK序列号。

step3：猜测序列号

- 如何预测序列号?
- 攻击者一般先与被攻击主机的一个端口建立起正常的连接。通常，这个过程被重复若干次，并将目标主机最后所发送的序列号存储起来。
- 攻击者估计他与被信任主机之间的RTT时间（往返时间），这个RTT时间是通过多次统计平均求出的，RTT对于估计下一个序列号是非常重要的。而且某些平台的序列号存在一些规律。比如BSD和Linux系统每秒钟将序列号增加128000，大约经过9.32小时序列号就会折返一次，这些规律都有助于序列号猜测。

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，他必须使客户机下线。
- 使客户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机，但是因为攻击者已经掌握了客户机，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，不依赖任何操作系统。
- 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“少年攻击者”的诞生。

实现TCP会话劫持的工具软件

- Juggernaut
  - Juggernaut是由Mike Schiffman开发的自由软件，是最先出现的会话攻击程序之一，运行在Linux操作系统上，攻击者能窥探网络中所有的会话，并且劫持其中任何一个，攻击者可以像真正的用户那样向服务器提交命令。
- Hunt
  - 由Pavel Krauz开发，是一个集嗅探、截取和会话劫持功能与一身的强大工具。它可以在共享式网络和交换式网络中工作，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。

IP欺骗的防御

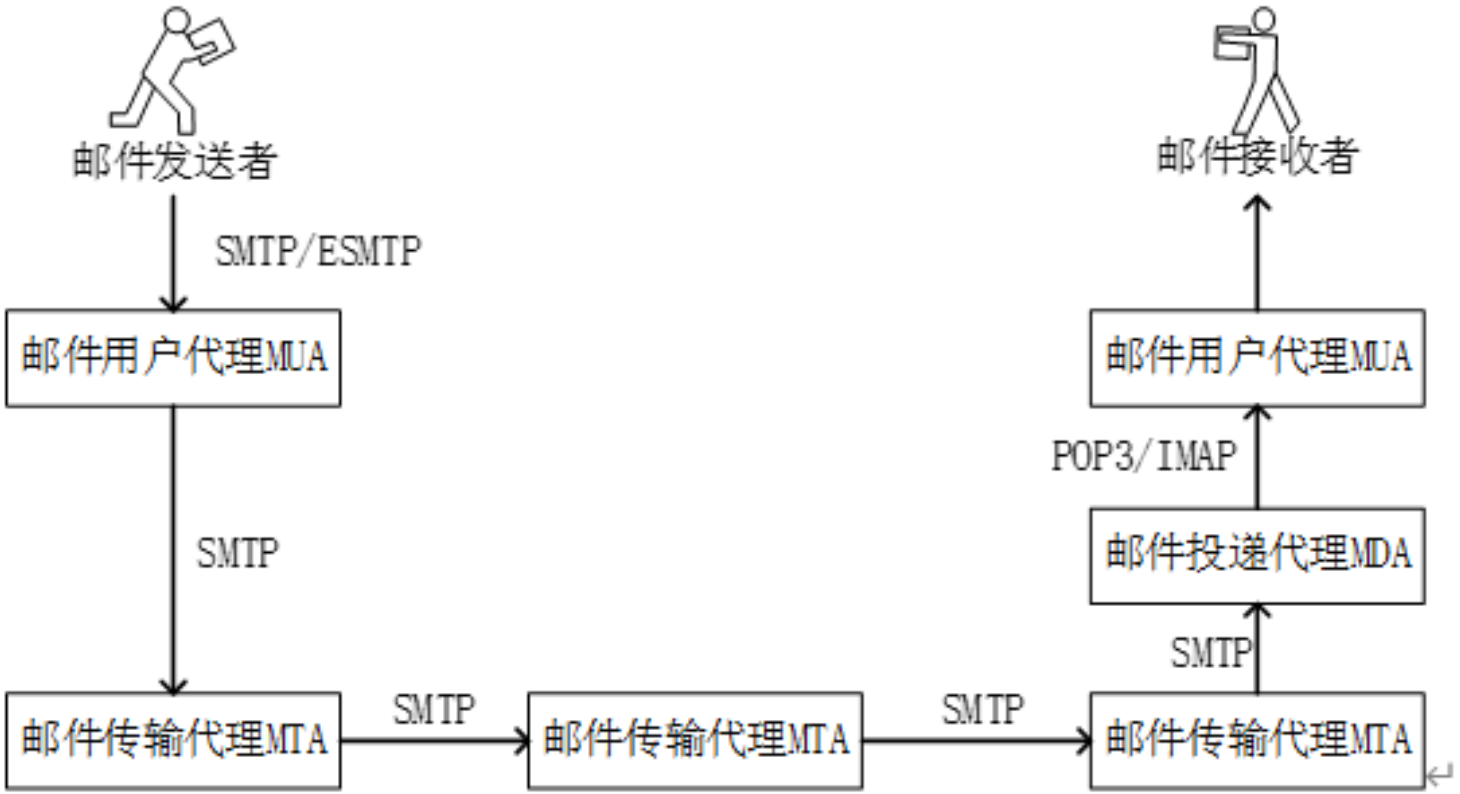
- **路由器过滤**：
  - **防范基本的IP欺骗：**
    - 入口过滤：不允许任何从外面进入网络的数据包使用单位内部地址作为源地址
    - 出口过滤：从内网主机到内网主机的流量不允许流到本网络之外
  - **防范源路由欺骗**：设置路由器禁用源路由
  - **防范会话劫持（**没有有效的办法可以根本上防范会话劫持攻击，只能尽量减少攻击带来的危害**）**：
    - 加密：
    - 使用安全协议：使用SSH，而不使用Telnet
    - 限制保护：允许外网到内网的信息越少，内网越安全

邮件系统组成:

- **用户代理（User Agent）**: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，或由邮件服务器收回
- **传输代理（Transfer Agent）**:负责信件的交换和传输，将信件传送至适当的邮件服务器
- **投递代理（Delivery Agent）**:将信件分发至最终用户的邮箱

正常情况下，邮件会将发送者的名字和地址包括进邮件头中，但有时发送者不希望收件者知道是谁发的**(匿名邮件)**：

- 最简单的方法：改变电子邮件发送者的名字，但通过邮件头的其它信息仍能够跟踪发送者
- 彻底的方式：让其他人发送这个邮件，发信地址就变成转发者的地址。现在因特网上有大量的**匿名服务器**


邮件发送者
SMTP/ESMTP
邮件用户代理MUA
SMTP
邮件传输代理MTA
SMTP
邮件传输代理MTA
SMTP
邮件传输代理MTA
SMTP
邮件投递代理MDA
POP3/IMAP
邮件用户代理MUA
邮件接收者

电子邮件攻击的两种方式：

（1）电子邮件轰炸，指的是用伪造的IP地址和电子邮件地址向同一信箱发送数以千计内容相同的垃圾邮件，致使受害人邮箱被“炸”，严重者可能给电子邮件服务器带来危险，甚至导致系统崩溃，造成拒绝服务攻击。

垃圾邮件是指将不需要的消息（通常是未经请求的广告）发送给收件人。如收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件或含有虚假的信息的邮件。

（2）电子邮件欺骗，攻击者假称自己是管理员（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，从而对目标实施攻击。

- 电子邮件欺骗的方法：

（1）利用相似的电子邮件地址

- 找到一个受害者熟悉的名字，然后注册一个像该名字的邮件地址。收件人很可能会回复这个邮箱，攻击者就有得到想要信息的可能性，或者使用别名。

（2）冒充回复地址

- 在各种电子邮件服务系统中，发件人地址和回复地址都可以不一样，在配置账户属性或撰写邮件时，可以使用与发件人地址不同的回复地址。由于用户在收到某个邮件时并回复时，并不会对回复地址仔细检查。
- 鉴于邮件地址欺骗的易于实现和危险性，用户必须随时提高警惕，认真检查邮件的发件人邮件地址、发件人IP地址、回复地址等邮件信息内容是防范黑客的必要措施。

（3）利用附件欺骗

- 我们知道不能轻易打开电子邮件里的可执行文件类的附件，但我们可能会以为那些文本文件或是图像文件的附件是没有危险的。由于目前大多数人使用的是windows系列操作系统，windows的默认设置是隐藏已知文件扩展名的，当去点击那个看上去很友善的文件时，很可能包含蠕虫、木马病毒。

（3）利用附件欺骗

- 例如，收到的邮件附件中有一个看起来是这样的文件：QQ宠物放送.txt，然而它实际的文件名却可以是QQ宠物放送.txt.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}
- {3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}在注册表里是HTML文件关联的意思。但是存成文件名的时候它并不会显现出来，看到的就是个.txt文件，该文件实际上等同于“QQ靓号放送.txt.html”。当双击这个伪装起来的.txt时候，就会以html文件的形式运行。

（3）利用附件欺骗

- 在收到的邮件中有附件时，不仅要看附件显示出来的扩展名，还要注意其实际显示的图标是什么。识别的办法是打开我的电脑-工具-文件夹选项，选中“在文件夹中显示常见任务”，查看附件时在“我的电脑”左面会显示出其文件名全称，此时可以看到它不是真正的txt文件。此外，还可以将附加下载后用鼠标右键选择“用记事本打开”，这样看会更安全。

（4）远程登录到SMTP端口发送邮件

- 攻击者连接到一台25端口开放的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：

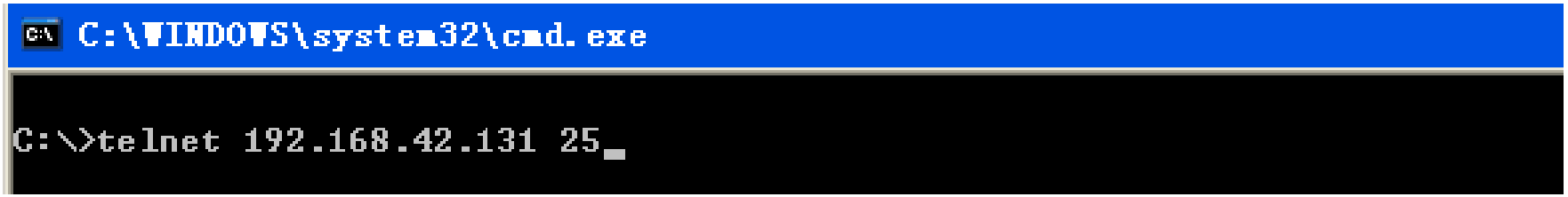
  HELO

  MAIL FROM: *欺骗伪装的mail地址*

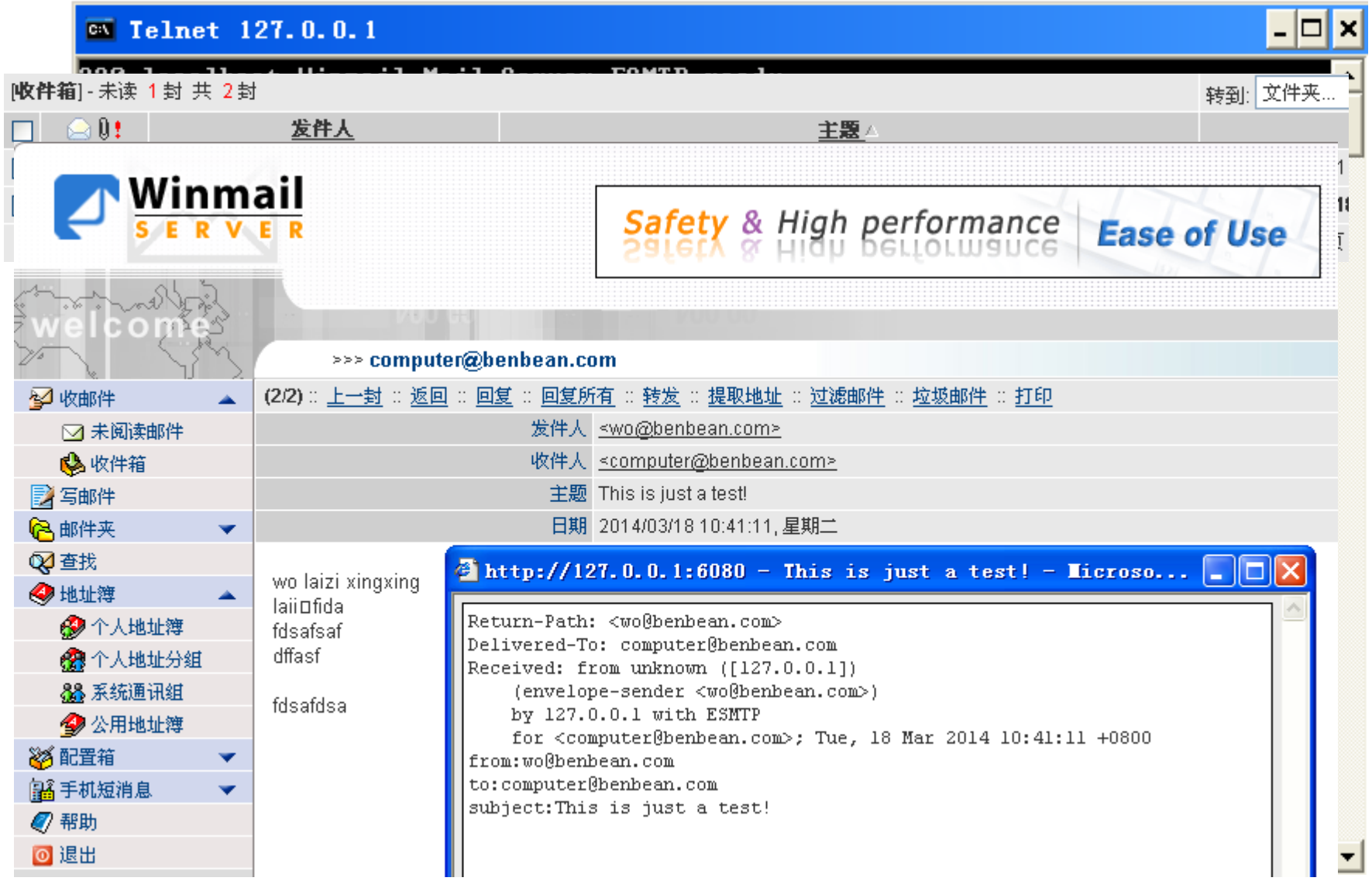
  RCPT TO: *收件的受害者mail地址*

  DATA

  邮件的内容

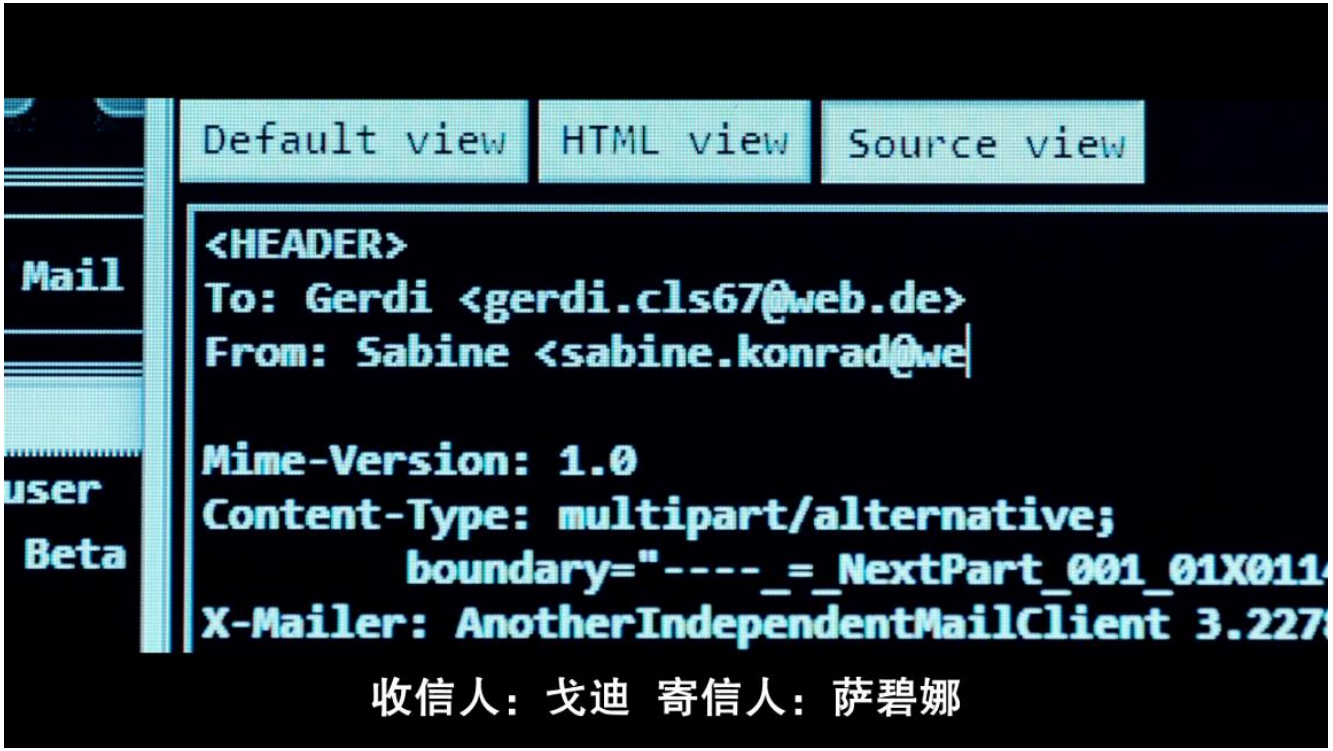


电子邮件欺骗及防御技术

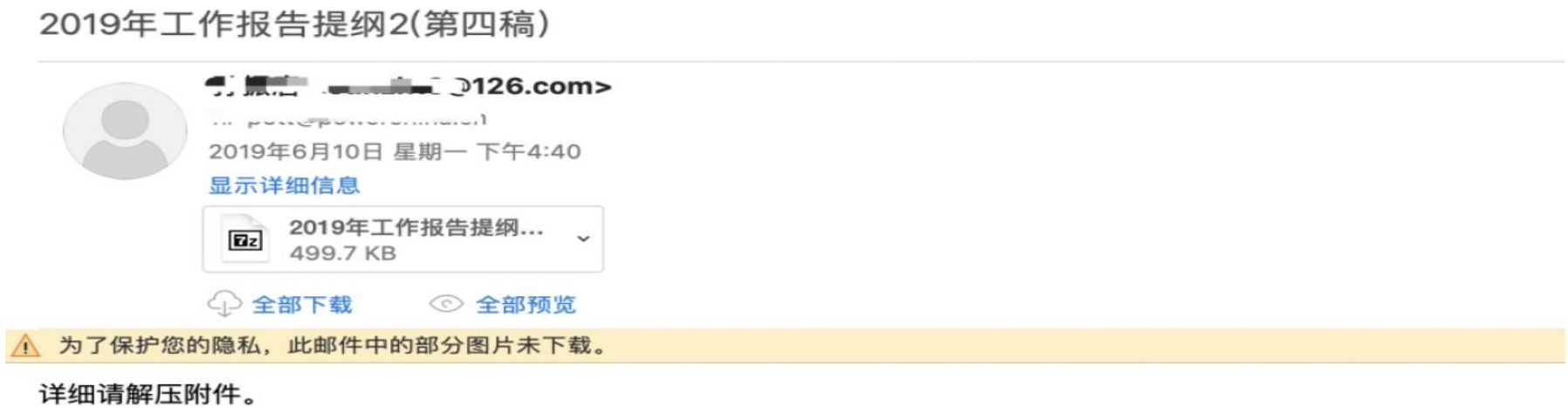


钓鱼邮件与鱼叉式钓鱼攻击

- 钓鱼（Phishing）邮件：利用伪装的电邮，欺骗收件人将账号、口令等信息回复给指定的接收者；或引导收件人连接到特制的网页，如银行的网页，令登录者信以为真，输入信用卡或银行卡号码、账户名称及密码等而被盗取
- 鱼叉式网络钓鱼（Spear Phishing）：一种只针对特定目标进行攻击的网络钓鱼攻击



钓鱼邮件与鱼叉式钓鱼攻击



海莲花APT组织发送的钓鱼邮件

电子邮件欺骗的防御:

- 树立风险意识，不要随意打开一个不信任的邮件
- 从如下角度介绍几种防范方法:
  - 邮件接收者
  - 邮件发送者
  - 邮件服务器
  - 邮件加密

- **邮件接收者：**
  - 合理配置邮件客户端，使总能显示完整的电子邮件地址，而不仅仅显示别名，完整的电子邮件地址能提供表明正在发生一些不平常事情的一些迹象
  - 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

- **邮件发送者：**如使用foxmail或者outlook之类的邮件客户端，必须保护好邮件客户端，防止他人修改客户端设置

- **邮件服务器提供方：**
  - **采用SMTP身份验证机制：**新SMTP协议规范新增2个命令**(VRFY,EXPN)**，对**发件人进行身份认证**，一定程度上降低了匿名/垃圾邮件的风险
- **邮件加密**——安全邮件标准：
  - **OpenPGP(RFC 4880):**
  - **S/MIME（RFC 2311,Secure/Multipurpose Internet Mail Extension）安全/多用途因特网邮件扩展**
    - **PGP (Pretty Good Privacy，相当好的隐私，商业版)**
    - **GnuPG(GPG，C): 开源项目, 支持OpenPGP,S/MIME**

DNS欺骗

- **DNS欺骗**，又称DNS域名重定向或域名劫持。
- 是通过拦截域名解析请求或篡改域名服务器上的数据，使得用户在访问相关域名时返回虚假IP地址或使用户的请求失败的攻击方式。

DNS欺骗的工作原理

- 用户对Web站点的访问是基于浏览器/服务器模式的，其基本过程是：用户通过Web浏览器用统一资源定位器URL查询域名系统DNS，DNS服务器返回IP地址，浏览器用该IP地址建立一次TCP/IP连接；通过该连接向Web服务器发送HTTP请求；Web服务器基于请求的内容找到相应的文件，形成HTTP应答，发送给浏览器，然后关闭本次连接；浏览器按某种方式显示该文件内容。
- 客户机从指定的域名服务器中获取域名对应的IP地址后，才能访问对应的服务器。

DNS欺骗的工作原理

- 如果本地域名服务器中没有包含相应数据，则由域名服务器在网络中进行递归查询，在其他域名服务器上获取地址信息。
- 由于客户机将域名查询请求首先发送到本地DNS服务器，服务器将在本地数据库中查找客户机要求的映射，如果本地DNS服务器的缓存中有相应的记录，则DNS服务器就直接将这条记录返回给用户。
- 如果攻击者改变本地DNS服务器的数据库，在服务器缓存中注入一条伪造的域名解析目录，把网站的域名重定向(劫持)到另一个网站的IP地址上，则用户访问的就是该虚假IP对应的服务器。

DNS欺骗的工作原理

- DNS欺骗的**关键**是在DNS服务器的本地Cache中缓存一条伪造的解析记录
- 如何才能在本地域名服务器中注入伪造的域名解析记录?
- 如果攻击者通过其他攻击方法已经获得了DNS服务器的控制权，则增加一条伪造记录就易如反掌。
  - Remark: 这种理想状态并不多见

确定目标DNS服务器的ID号为DNS欺骗攻击的关键

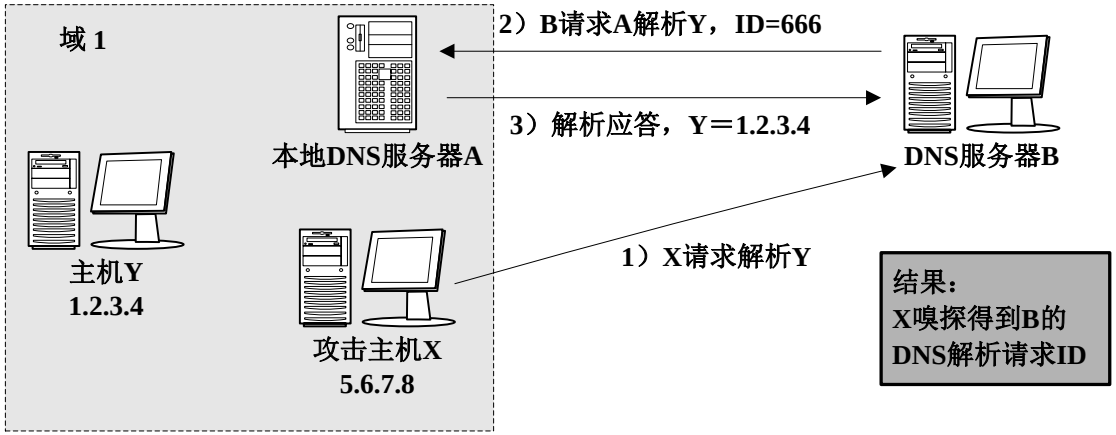
- DNS数据通过UDP（53端口）协议传递，通信过程往往是并行的，即域名服务器之间同时可能会进行多个解析过程
- **Q：靠什么来彼此区别呢?**
- ***A*：DNS报文的ID域**
  - 请求方和应答方使用相同的ID号证明是同一个会话
    - 在一段时期内，DNS服务器一般都采用一种有章可循的ID生成机制，如对每次发送的域名解析请求ID依次加1

DNS 欺骗

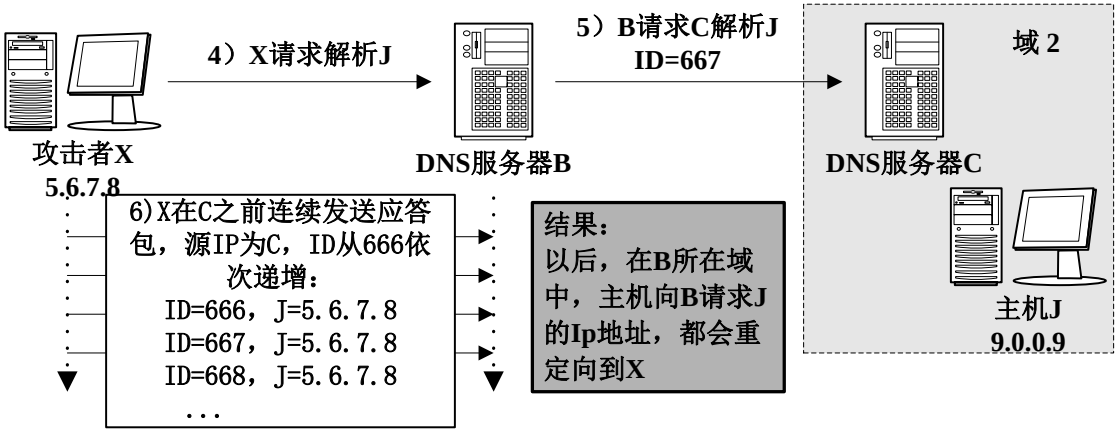
- 攻击者可以在某个DNS服务器的网络中进行嗅探，他只要向远程某DNS服务器发送一个对本地域名的解析请求，得到来自远程DNS服务器的请求数据包（因为远程DNS服务器肯定会向本地的DNS服务器请求DNS解析），攻击者就可以得到想要的ID号

DNS 欺骗

例：乙域的DNS服务器向甲域的DNS服务器请求解析，如果伪造的DNS应答包中含有正确的ID号，并抢在甲域的DNS服务器之前向乙域的DNS服务器返回伪造信息，欺骗就将成功



一次DNS欺骗攻击的完整过程



Ettercap进行dns-spoof

```
C:\Documents and Settings\ben>ping www.baidu.com

Pinging www.a.shifen.com [180.97.33.107] with 32 bytes of data:

Reply from 180.97.33.107: bytes=32 time=12ms TTL=128
Reply from 180.97.33.107: bytes=32 time=12ms TTL=128
Reply from 180.97.33.107: bytes=32 time=11ms TTL=128
Reply from 180.97.33.107: bytes=32 time=11ms TTL=128

Ping statistics for 180.97.33.107:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 12ms, Average = 11ms
```

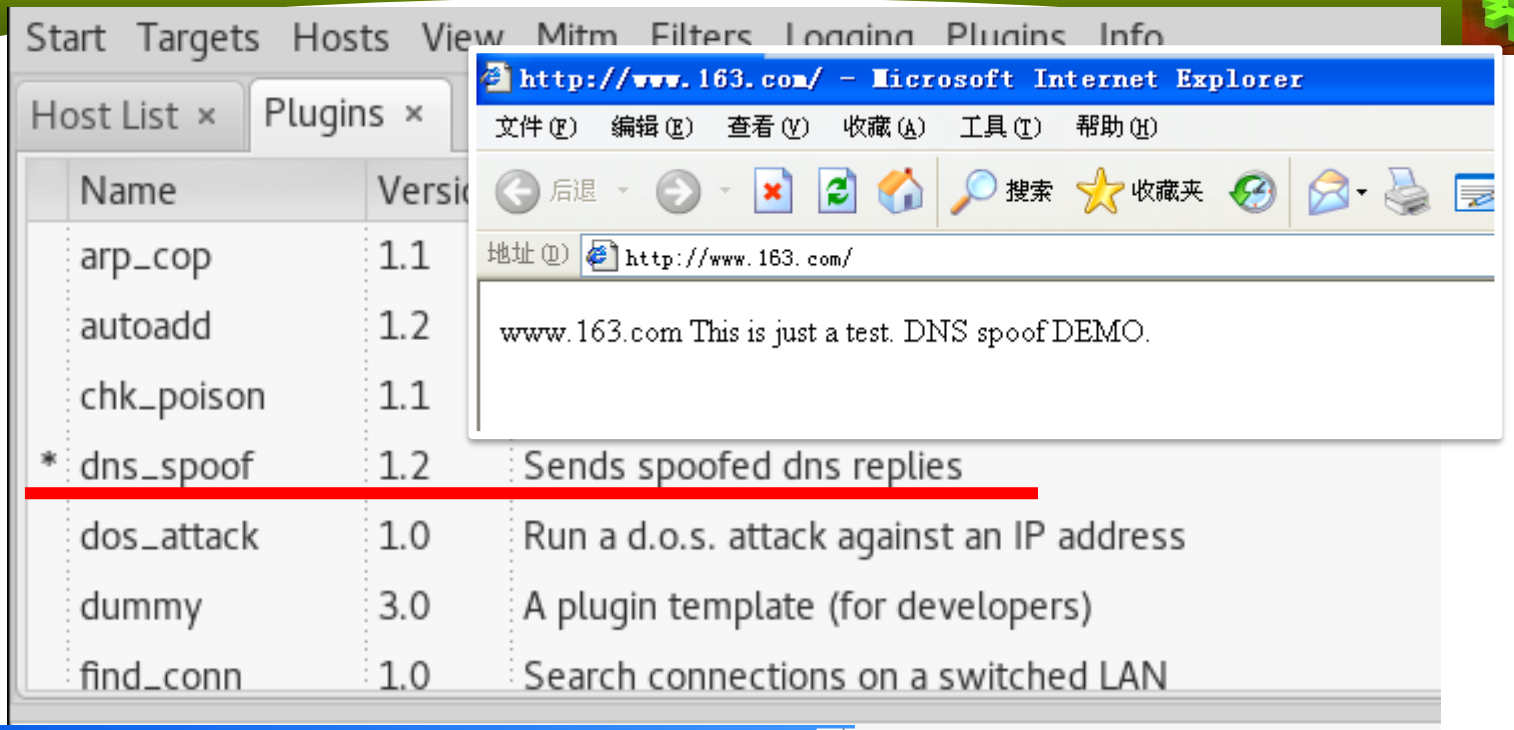
Applications ▾ Places ▾ Text Editor ▾ Sun 21:49 1

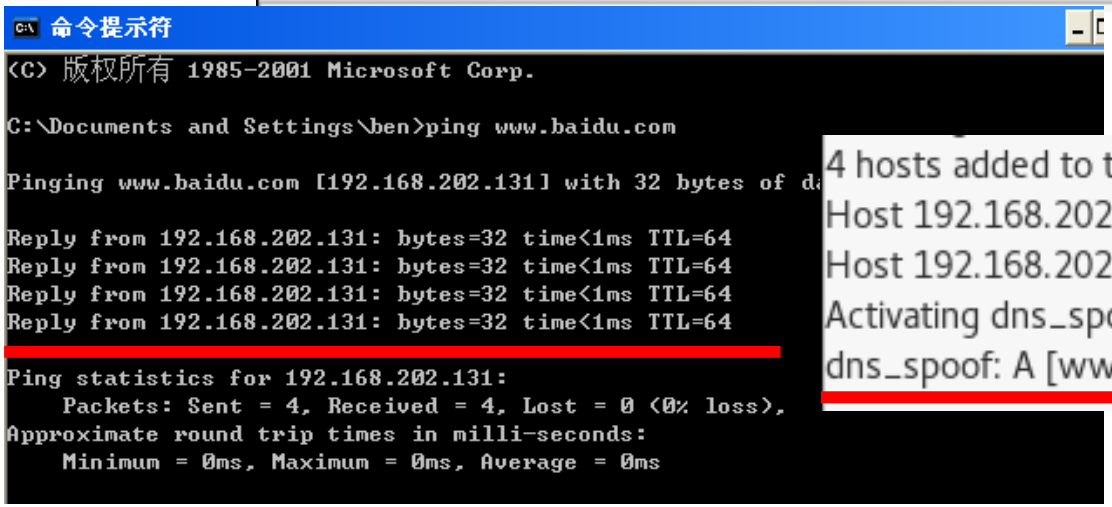
Open ▾ | etter.dns /etc/ettercap | Save

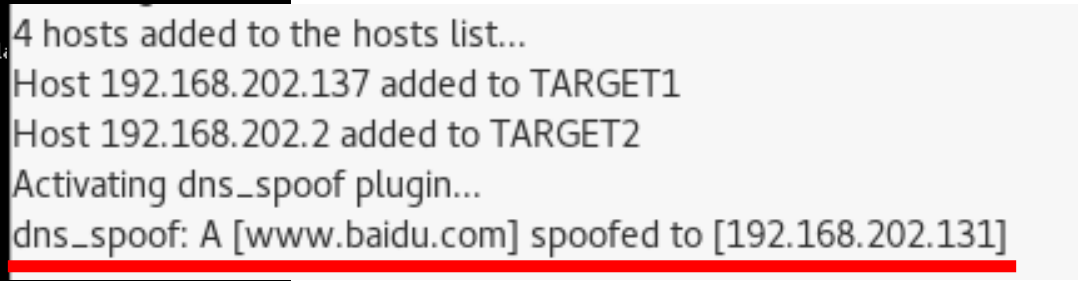
```
# redirect it to www.linux.org
#

microsoft.com      A   107.170.40.56
*.microsoft.com    A   107.170.40.56
www.microsoft.com  PTR 107.170.40.56      # Wildcards in PTR are not allowed
www.baidu.com      A   192.168.202.131
```

Ettercap进行dns-spoof







- **DNS欺骗的局限性：**
  - 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
- **配置DNS服务器的时候要注意：**
  - 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：**利用缓存中的记录信息或通过查询其它服务器获得信息并发送给客户机，称为递归查询——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
  - **限制动态更新**
  - **采用分层的DNS体系结构**

Web 欺骗与防御

- **Web欺骗：**创造一个完整的令人信服的Web世界，但实际是一个虚假的复制

- **网络钓鱼：**借用电子邮件或模仿网上银行、网上购物等网上交易的页面而制作出假的网页，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

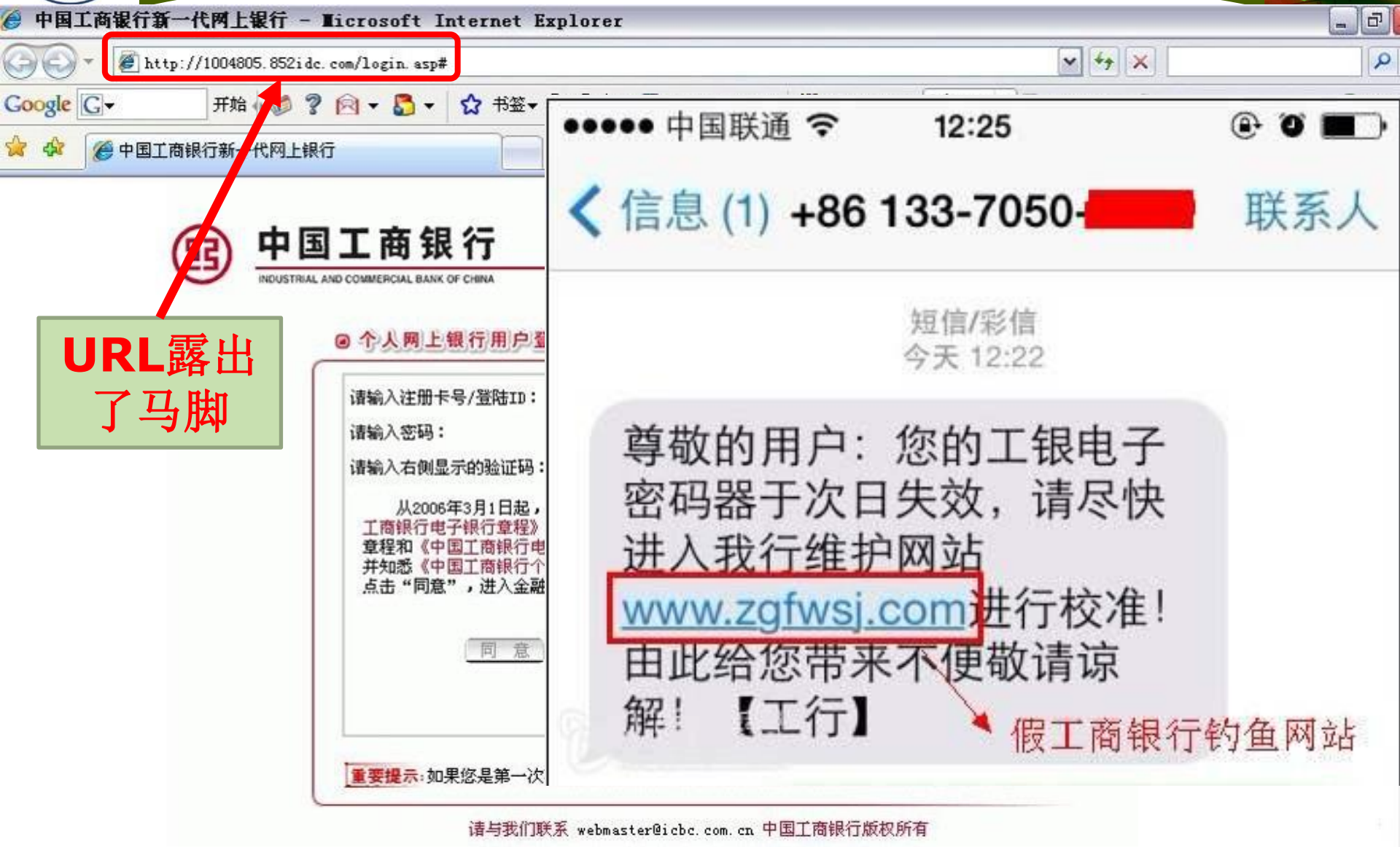
Web 欺骗与防御

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

Web 欺骗与防御


中国工商银行新一代网上银行 - Microsoft Internet Explorer
http://1004805.852idc.com/login.asp#
中国工商银行新一代网上银行
中国工商银行
INDUSTRIAL AND COMMERCIAL BANK OF CHINA
个人网上银行用户登
请输入注册卡号/登陆ID：
请输入密码：
请输入右侧显示的验证码：
从2006年3月1日起，
工商银行电子银行章程》
章程和《中国工商银行电
并知悉《中国工商银行个
点击“同意”，进入金融
同 意
重要提示:如果您是第一次
请与我们联系 webmaster@icbc.com.cn 中国工商银行版权所有
URL露出了马脚
中国联通
12:25
信息 (1) +86 133-7050-
联系人
短信/彩信
今天 12:22
尊敬的用户：您的工银电子密码器于次日失效，请尽快进入我行维护网站
www.zgfwsj.com进行校准！
由此给您带来不便敬请谅解！【工行】
假工商银行钓鱼网站

Web 欺骗与防御


中国移动4G 13:51 90%
http://wap.ccbxvt.cc
中国建设银行
China Construction Bank
建行手机网
简洁版
完整
客户服务热线：95533
导航
动态
查询
行情
微博
欢迎登录建行手机网
1、建行积分兑换现金活动正式举办中，使用建行账户的客户都可参与积分兑换现金活动。
2、兑换现金是按照积分的百分之八进行兑换。
3、例：积分10000分可以兑换800元现金，也就是积分的百分之八。现在可登录手机银行（积分兑换）进行兑换。
4、活动截止时间：2016年11月01日至2016年11月12日
手机银行（积分兑换）
信用卡用户
储蓄卡用户
优惠与服务
最新公告
新闻中心
生日一起过，礼物你来拿——建行网银15周年主题...
微创新让网银页面“活”起来
建行微信狂欢季 缤纷豪礼乐翻天
更多 >>
中国移动4G 11:48 99%
中国农业银行
AGRICULTURAL BANK OF CHINA
首页
产品服务
农行动态
微博
活动中心
积分兑换现金活动规则：
1、中国农业银行积分兑换现金活动正式举办中，使用中国农业银行的客户都可以参加积分兑换现金活动。
2、兑换现金是按照积分的百分之五进行兑换。
3、10000积分可以兑换500元人民币，也就是积分的百分之五。现在可以登录手机银行进行兑换。
4、活动截止时间：2016年10月29日-2016年11月12日。
储蓄卡用户
信用卡用户
掌上银行
客户端下载
快捷注册
业务说明
安全提示
便捷服务
理财
基金
信用卡特惠商户
电子银行
立即购买
加入购物车

Web 欺骗与防御


[redacted]
生活简单但要精致。
今日
火爆公测
该好友正在使用QQ for iPhone，您的消息将发送到对方手机，点击查看详情
交谈中请勿轻信汇款、中奖信息、陌生电话，勿使用外挂软件。
[redacted]013/1/21 23:11:59
问你个事情，你认识这个人吗，我看她空间有你和她的合影，
在第2个相框 这是她的博客地址，你看看
http://www.tongfangpc.com\xml\9)6^:.asp?x=/s08/?id=
62510225
拍拍网
隐藏广告
彩钻价
39元

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。对普通用户来说是不切实际的
- 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
- 培养用户的安全意识和对开发人员的安全教育

Web 欺骗与防御


中国工商银行中国网站 - 搜狗高速浏览器
http://www.icbc.com.cn/icbc/
中国工商银行中国网站
Baidu 百度
中国银行
百度一下
网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»
百度为您找到相关结果约22,500,000个
搜索工具
中国银行全球门户网站 官网
中国银行是中国国际化和多元化程度最高的银行,在中国内地、香港、澳门、台湾及37个国家为客户提供全面的金融服务。主要经营商业银行业务,并通过附属机构开展投资银行、...
www.boc.cn/ - 百度快照 - 65%好评
中国银行 BANK OF CHINA
客户服务
短信银行服务 电话服务
常见问题 服务价目表
金融@家
电子银行微博
加关注
贵宾尊享
新闻·动态
工行风貌
财经新闻
优惠活动
新品推荐 NEW
中国工商银行华沙分行正式开业
波兰当地时间2012年11月22日，中国工商银行华沙分行在…[详细]
工商银行认真学习贯彻十八大精神
工商银行收购阿根廷标准银行获得阿根廷中央银行批准
[投资者关系] [工行荣誉] [工行股价] [企业社会责任]
人民网：工商银行认真学习十八大精神 三方面…
新华社：工行收购阿根廷标准银行80%股份获…
新华网：工行前10个月
人民网：10日起工行
360网购保镖提醒您
设置
安全检测已完成！
本次检测未发现风险，现在可以放心网购了！
http://www.icbc.com.cn/icbc/%e7%bd%91%e9%93%b6%e7%b3%bb%e7%bb%9f/alert.htm
2012/11/25

Summary

- 常见的欺骗攻击的基本原理：
  - IP欺骗
  - ARP欺骗
  - 电子邮件欺骗
  - DNS欺骗
  - Web欺骗