整理（of Im）

概述

1. CVSS3.0 计算分值共有三种维度：

1. 基础度量。分为 可利用性 及 影响度 两个子项，是漏洞评估的静态分值。

2. 时间度量。基础维度之上结合受时间影响的三个动态分值，进而评估该漏洞的动态分值。

3. 环境度量。根据用户实际环境需求结合时间及基础两个维度的分值，是根据用户环境情况重新评估的分值。

基本（Base）：代表着漏洞的原始属性，不受时间与环境的影响，又由 Exploitability 可执行性与影响程度 Impact 度量。

时间（Temporal）：反应漏洞随着时间推移的影响而不受环境影响，举个简单的例子，随着一个漏洞软件的补丁不断增加，该漏洞的 CVSS 分数会随之减少。

环境（Environmental）：代表特定环境下执行漏洞的分数，允许根据相应业务需求提高或者降低该分值。

· Attack Vector：攻击媒介

· Scope：作用域（Unchanged：同一安全权限下）

· Available Impact：可用性（由于可用性是指信息资源的可访问性，因此消耗网络带宽，处理器周期或磁盘空间的攻击都会影响受影响的组件的可用性）

Temporal Score Metrics：时间分数指标

3.1 Exploitability可执行性块

攻击向量（AV）	网络（N）/邻居（A）/本地（L）/物理（P）
攻击复杂度（AC）	低（L）/高（H）
权限要求（PR）	无（N）/低（L）/高（H）
用户交互（UI）	不需要（N）/需要（R）
影响范围（UI）	不改变（U）/改变（C）

3.2 Impact影响指标

机密性（C）	无（N）/低（L）/高（H）
完整性（I）	无（N）/低（L）/高（H）
可用性（A）	无（N）/低（L）/高（H）

4.Time具体计算方法

利用代码的成熟度（E）	未验证（U）/PoC（P）/EXP（F）/自动化利用（H）
修复方案（RL）	正式补丁（O）/临时补丁（T）/缓解措施（W）/不可用（U）
来源可信度（RC）	未知（U）/未完全确认（R）/已确认（C）

5.Environmental具体计算方法

环境分数（可选）	
机密性要求(CR)	未定义(X) 低(L) 中(M) 高(H)
完整性要求(IR)	未定义(X) 低(L) 中(M) 高(H)
可用性要求(AR)	未定义(X) 低(L) 中(M) 高(H)
修改基础度量指标 (Modified Base Metrics)	Modified Attack Vector (MAV) Modified Attack Complexity (MAC) Modified Privileges Required (MPR) Modified User Interaction (MUI) Modified Scope (MS) Modified Confidentiality (MC) Modified Integrity (MI) Modified Availability (MA)

2. C4I：

C4I 系统是指指挥、控制、通讯、电脑和情报的集成，以前一直被运用在军事领域，它以计算机为核心，综合运用各种信息技术，对军队和武器进行指挥与控制。在军事领域中，C4I 的应用是重要的。

3. 安全的目标：

（1）安全保护能力：采取积极的防御措施，保护网络免受攻击、损害；具有容侵能力，使得网络在即使遭受入侵的情况下也能够提供安全、稳定、可靠的服务；

（2）隐患发现能力：能够及时、准确、自动地发现各种安全隐患特别是系统漏洞，并及时消除安全隐患；

（3）应急反应能力：万一网络崩溃，或出现了其它安全问题，能够以最短的时间、最小的代价恢复系统，同时使用户的信息资产得到最大程度的保护；

（4）信息对抗能力：信息对抗能力已经不只是科技水平的体现，更是综合国力的体现。未来的战争无疑是始于信息战，以网络为基础的信息对抗将在一定程度上决定战争的胜负。

4. 安全网络通信模型

公开密钥加密，又称非对称加密。在这个加密过程中，需要一对密钥，不公开的密钥称为私钥，公开的那一个密钥称为公钥。如 RSA，DSA，EIGamal

从以上的介绍中可以看出，各种加密算法都有其特点和适用性：

（1）使用非对称加密，发送者 A 使用私钥加密，接受者 B 能够验证数据的发送者 A 是谁，由于所有人都能使用发布者 A 公钥解密，这种方法只能适合发布公开的信息。（2）接受者 B 的公钥是公开的，用它加密数据后发给 B，有可能被截获掉包。（3）非对称加密算法，加密速度很慢，强度高。对称加密算法，速度快，但是密钥交换是个问题。（4）单向加密不可逆，接收者无法还原到明文。那么，就需要一种通信模型能够扬长避短，解决通信安全的问题，于是便有了下面的模型：

通信工作流程

1、发送者 A 准备好信息明文。2、发送者 A 对信息进行哈希运算（单向加密算法），得到一个信息摘要。3、发送者 A 使用自己的私钥（SK）对信息摘要进行加密，即数字签名，之后将其附件在发送的信息上。（实现不可否认性）4、发送者 A 随机生成一个对称加密密钥，并使用它对发送的信息包括摘要进行对称加密，生成密文。5、发送者 A 再使用接收方的公钥（PK）对第 4 步使用的随机对称密钥进行加密，之后将其附加至第 4 步生成的密文上，一并发给接收者 B。6、接收者 B 收到发送者 A 的密文后，首先使用自己的私钥（SK）解密出对称加密的密钥。7、接收者 B 使用对称密钥解密密文，得到附加摘要的信息明文。8、接收者 B 使用发送者的公钥（PK）解密摘要，获得哈希值 9、接收者 B 使用同样的哈希算法再次对信息明文计算，得到新的信息摘要，与解密后的摘要比对，如果一致，则说明收到的信息明文未被篡改。（保证数据完整性）

以上的通信模型很好的解决了数据完整性、不可否认性，但这个模型的依赖的关键点是双方公钥。这个模型中双方公钥来源无法验证，而且在通讯前，如何获得每个人的可信任的公钥也成了整个系统的关键。因此，需要一套系统，能够解决以上存在的种种问题：身份认证、数据完整性、密钥交换、操作的不可否认性，它就是 PKI。

- PKI：Public Key Infrastructure，公钥基础设施。
- CA：Certificate Of Authority，认证中心。
- 数字证书：提供了一种发布公钥的简便途径；
  一个数字证书包括：拥有者身份信息、公钥、CA 数字签名、有效期等其他信息。

- 数字签名：用来确认信息发送者的身份，保证信息的完整性和抗否认性。

5. P2DR：

P2DR 模型包括四个主要部分：Policy(安全策略)、Protection(防护)、Detection(检测)和 Response(响应)。

（1）策略：定义系统的监控周期、确立系统恢复机制、制定网络访问控制策略和明确系统的总体安全规划和原则。

（2）防护：通过修复系统漏洞、正确设计开发和安装系统来预防安全事件的发生；通过定期检查来发现可能存在的系统脆弱性；通过教育等手段，使用户和操作员正确使用系统，防止意外威胁；通过访问控制、监视等手段来防止恶意威胁。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网（VPN）技术、防火墙、安全扫描和数据备份等。

（3）检测：是动态响应和加强防护的依据，通过不断地检测和监控网络系统，来发现新的威胁和弱点，通过循环反馈来及时做出有效的响应。当攻击者穿透防护系统时，检测功能就发挥作用，与防护系统形成互补。

（4）响应：系统一旦检测到入侵，响应系统就开始工作，进行事件处理。响应包括紧急响应和恢复处理，恢复处理又包括系统恢复和信息恢复。

攻击行径：

1. 黑客社会工程学攻击实例解析：

常见的黑客社会工程学攻击方式包括伪造邮件攻击方式、网络钓鱼攻击方式、诱骗点击恶意挂马网页方式、社交网站利用方式、利用社工字典实施暴力破解、利用搜索引擎收集敏感信息、辅助安全问题利用方式等。

2. 再答抹去攻击痕迹：

既然你发起了攻击，当然会在各个链条留下证据，最多证据一般在头尾上，即你的电脑及被攻击者的网络或服务器。自己电脑攻击完可以来个硬盘低格或硬盘清零来消除证据，嫌麻烦可以使用虚拟硬盘、虚拟机、无硬盘使用 DVD 启动电脑等等技术。

至于目标的网络或服务器，就需要考虑清除网络设备的日志，服务器的日志，日志服务器的数据，监控系统的数据等等 。但最难的还是清除运营商的记 录，这个一般靠时间，毕竟运营商的存储空间也是有限的。

至于最后一个被定位的可能问题：

牵涉到很多方面，如社会学，你和被攻击目标最近有过节或存在利益关系，那不用任何技术也会怀疑你。技术方面就是一层层的追踪你的原始 IP 地址或 MAC 地址来定位，公众场所就看登记的证件或摄像头。

3. 反跟踪：

基础：加密程序加密敏感/私人数据；网络痕迹清除；logs 日志的清除；肉鸡上使用稳妥、安全、隐蔽的后门；

高级：sniffer 嗅探、跳板、堡垒主机：它是你的多层跳板中直接和你正在使用的主机建立了连接的主机，也就是和你最近的一层跳板、好的蜜罐系统。

网络侦察：

1. 网络监听的基本原理

以太网可以把相邻的计算机、终端、大容量存储器的外围设备、控制器、显示器以及为 连接其他网络而使用的网络连接器等相互连接起来，具有设备共享、信息共享、高速数据通 讯等特点。以太网这种工作方式，如同有很多人在一个大房间内，大房间就像是一个共享的 信道，里面的每个人好像是一台主机。人们所说的话是信息包，在大房间中到处传播。当我 们对其中某个人说话时，所有的人都能听到。正常情况下只有名字相同的那个人才会做出反 应，并进行回应。其他人了解谈话的内容，也可对所有谈话内容做出反应。因此，网络监听 用来监视网络的状态、数据流动情况以及网络上传输的信息等。当信息以明文的形式在网络 上传输时，使用监听技术进行攻击并不是一件难事，只要将网络接口设置成监听模式，便可 以源源不断地将网上传输的信息截获。

1.1 广播式以太网中的网络监听

广播式以太网在逻辑上由一条总线和一群挂在总线上的节点组成。任何一个节点主机发出 的数据包都是在共享的以太网传输介质上进行传输的，每个数据包的包头部分都包含了源地 址和目的地址。网络上所有节点都通过网络接口（网卡）负责检查每一个数据包，如果发现 其目的地址是本机，则接收该数据包并向上层传递，以进行下一步的处理；如果目的地址不 是本机，则数据包将被丢弃不作处理。以太网数据包过滤机制分为链路层、网络层和传输层 。在链路层，网卡驱动程序判断收到包的目标 MAC 地址是否是自己的 MAC 地址；在网络层判断 目标 IP 地址是否为本机所绑定的 IP 地址；在传输层如 TCP 层或者 UDP 层判断目标端口是否在本 机已经打开。如果以上判断否定，数据包将被丢弃。

在进行网络数据包的“监听”时，首先通过将系统的网络接口设定为“混杂模式”，网 络监听程序绕过系统正常工作的处理机制，直接访问网络底层。不论数据包的目的地址是否 是本机，都能够截获并传递给上层进行处理（只能监听经过自己网络接口的那些包），通过 相应的软件进一步地分析处理，就能够得到数据包的一些基本属性，如包类型、包大小、目 的地址、源地址等，可以实时分析这些数据的内容，如用户名、口令以及所感兴趣的内容。

同理，正确地使用网络监听技术也可以发现入侵并对入侵者进行追踪定位，在对网络犯罪 进行侦查取证时获取有关犯罪行为的重要信息，成为打击网络犯罪的有力手段。

1.2 交换式以太网中的监听

交换机的工作原理不同于 HUB 的共享式报文方式，交换机转发的报文是一一对应的，能 够隔离冲突域和有效的抑制广播风暴的产生。由此看来，交换环境下再采用传统的共享式以 太网下网络监听是不可能了，由于报文是一一对应转发的，普通的网络监听软件此时无法监 听到交换环境下其他主机任何有价值的数据。但是，以太网内主机数据包的传送完成不是依 靠 IP 地址，而是依靠 ARP 找出 IP 地址对应的 MAC 地址实现的。而 ARP 协议是不可靠和无连接的 ，通常即使主机没有发出 ARP 请求，也会接受发给他的 ARP 回应，并将回应的 MAC 和 IP 对应关 系放入自己的 ARP 缓存中。因此利用 ARP 协议，交换机的安全性也面临着严峻的考验。

1.2.1 交换机缓冲区溢出攻击

交换机大多使用存贮转发技术，工作时维护着一张 MAC 地址与端口的映射表，这个表中记 录着交换机每个端口绑定的 MAC 地址。他的工作原理是对某一段数据包进行分析判别寻址， 并进行转发，在发出前均存贮在交换机的缓冲区内。但是，交换机缓冲区是有限的。如用大 量无效 IP 包，包含错误 MAC 地址的数据帧对交换机进行攻击。该交换机将接收到大量的不符 合分装原则的包，造成交换机处理器工作繁忙，从而导致数据包来不及转发，进而导致缓 冲区溢出产生丢包现象。这时交换机就会退回到 HUB 的广播方式，向所有的端口发送数据包 。这样，监听就变得非常容易了。

1.2.2 ARP 协议和欺骗

在以太网中传输的数据包是以太包，而以太包的寻址是依据其首部的物理地址（MAC 地址 ）。仅仅知道某主机的逻辑地址（IP 地址）并不能让内核发送一

帧数据给此主机，内核必须知道目的主机的物理地址才能发送数据。ARP 协议的作用就是在于把逻辑地址变换成物理地址，也既是把 32 b 的 IP 地址变换成 48 b 的以太地址。每一个主机都有一个 ARP 高速缓存，此缓存中记录了最近一段时间内其他 IP 地址与其 MAC 地址的对应关系。如果本机想与某台主机 通信，则首先在 ARP 高速缓存中查找此台主机的 IP 和 MAC 信息，如果存在，则直接利用此 MAC 地址构造以太包；如果不存在，则向本网络上每一个主机广播一个 ARP 请求包。其意义是“ 如果你有此 IP 地址，请告诉我你的 MAC 地址”，目的主机收到此请求包后，发送一个 ARP 响应 包，本机收到此响应包后，把相关信息记录在 ARP 高速缓存中。可以看出，ARP 协议是有缺点的，第三方主机可以构造一个 ARP 欺骗包，而源主机却无法分辨真假。

假定 A 为进行监听的主机，B 为被监听的主机，C 为其他网络主机。当 A 收到 B 向 C 发出的 ARP 请求包后，向 B 回应一个 ARP 应答。向 C 主动发送一个应答，修改 C 缓存中的关于 B 的 IPMAC 映射。当 A 收到 C 向 B 发出的 ARP 请求时，向 B 主动发送一个应答，修改 B 缓存中的关于 C 的 IPMAC 映射。这样，构造了 ARP 欺骗包 (欺骗 B 对 C 的连接)。事实上，A 成了 B 的代理 可以全部捕获到 B 和 C 的相关数据。

2. 网络监听的检测及防范

网络监听是很难被发现的，因为运行网络监听的主机只是被动地接收在局域网上传输的信 息，不主动与其他主机交换信息，也没有修改在网上传输的数据包。

2.1 网络监听的检测

(1)对于怀疑运行监听程序的机器，向局域网内的主机发送非广播方式的 ARP 包（错误的 物理地址)，如果局域网内的某个主机响应了这个 ARP 请求，我们就可以判断该机器处于杂 乱模式。而正常的机器不处于杂乱模式，对于错误的物理地址不会得到响应。

（2）网络和主机响应时间测试。向网上发大量不存在的物理地址的包，处于混杂模式下 的机器则缺乏此类底层的过滤，由于监听程序要分析和处理大量的数据包会占用很多的 CPU 资源，骤然增加的网络通讯流量会对该机器造成较明显的影响，这将导致性能下降。通过比 较前后该机器性能加以判断是否存在网络监听。

（3）使用反监听工具如 antisniffer 等进行检测。

2.2 网络监听的防范

2.2.1 网络分段

网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是防范网络监听的一 项重要措施。将网络划分为不同的网段，其目的是将非法用户与敏感的网络资源相互隔离， 从而防止可能的非法监听。

2.2.2 以交换式集线器代替共享式集线器

对局域网的中心交换机进行网络分段后，局域网监听的危险仍然存在。这是因为网络最终 用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，

两台机器之间的数据包(单播包)还是会被同一 台集线器上的其他用户监听。因此，应该以交换式集线器代替共享式集线器，使 单播包仅在两个节点之间传送，从而防止非法监听。

2.2.3 使用加密技术

数据经过加密后，通过监听仍然可以得到传送的信息,但显示的是乱码。使用加密技术的 缺点是影响数据传输速度以及使用一个弱加密术比较容易被攻破。

2.2.4 划分 VLAN

运用 VLAN（虚拟局域网）技术，将以太网通信变为点到点通信，VLAN 子网隔离了广播风暴 ，可以防止大部分基于网络监听的侵入，对一些重要部门实施了安全保护。且当某一部门物 理位置发生变化时，只需对交换机进行设置，就可以实现网络的重组，非常方便、快捷，同 时节约了成本。为保证不同职能部门管理的方便性和安全性以及整个网络运行的稳定性，可 采用 VLAN 技术进行虚拟网络划分。

3 结语

网络监听技术在信息安全领域中显得非常重要，他又是一把双刃剑，总是扮演着正反两方 面的角色。对于网络管理员来说，网络监听技术可以用来分析网络性能，检查网络是否被入 侵发挥着重要的作用；对于入侵者来说，网络监听技术可以很容易地获得明文传输的密码和 各种机密数据。为了保护网络信息的安全，必须采用网络监听技术进行反跟踪，时刻探明现 有网络的安全现状，掌握先机，才能保证网络的信息安全。

3. ARP 欺骗：

ARP 欺骗的运作原理是由攻击者发送假的 ARP 数据包到网上，尤其是送到网关上。其目的是要让送至特定的 IP 地址的流量被错误送到攻击者所取代的地方。因此攻击者可将这些流量另行转送到真正的网关（被动式数据包嗅探，passive sniffing）或是篡改后再转送（中间人攻击，man-in-the-middle attack）。攻击者亦可将 ARP 数据包导到不存在的 MAC 地址以达到阻断服务攻击的效果，例如 netcut 软件。

(ARP 协议是“Address Resolution Protocol”（地址解析协议）的缩写。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的 MAC 地址的。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的 MAC 地址。但这个目标 MAC 地址是如何获得的呢？它就是通过地址解析协议获得的。所谓“地址解析”就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。所以说从某种意义上讲 ARP 协议是工作在更低于 IP 协议的协议层。这也是为什么 ARP 欺骗更能够让人在神不知鬼不觉的情况下出现网络故障，他的危害更加隐蔽。)

防制方法

最理想的防制方法是网上内的每台计算机的 ARP 一律改用静态的方式，不过这在大型的网上是不可行的，因为需要经常更新每台计算机的 ARP 表。

另外一种方法，例如 DHCP snooping，网上设备可借由 DHCP 保留网络上各计算机的 MAC 地址，在伪造的 ARP 数据包发出时即可侦测到。此方式已在一些厂牌的网上设备产品所支持。

有一些软件可监听网络上的 ARP 回应，若侦测出有不正常变动时可发送邮箱通知管理者。例如 UNIX 平台的 Arpwatch 以及 Windows 上的 XArp v2 或一些网上设备的 Dynamic ARP inspection 功能。

正当用途

ARP 欺骗亦有正当用途。其一是在一个需要登录的网上中，让未登录的计算机将其浏览网页强制转向到登录页面，以便登录后才可使用网上。另外有些设有备援机制的网上设备或服务器，亦需要利用 ARP 欺骗以在设备出现故障时将讯务导到备用的设备上。

4. 口令破解：

密码需要足够的强度才能够抵抗尝试性攻击，即通常所说的“暴力破解”。暴力破解有两种模式：在线模式，攻击者必 须使用和用户应用程序相同的登录入口；与在线模式相对的是离线模式，攻击者需要首先窃取密码文件，但能够进行不受约束的破解尝试，并且没有应用程序和网络 的破解速度限制（即单位时间内允许口令输入次数的限制）。

离线破解指：破解过程中，已经获得加密密文，在不与目标服务器交互的的情况下，利用在线网站或本地程序对密文进行破解。

离线不会触发密码锁定机制，不会产生大量登录失败日志引起管理员注意

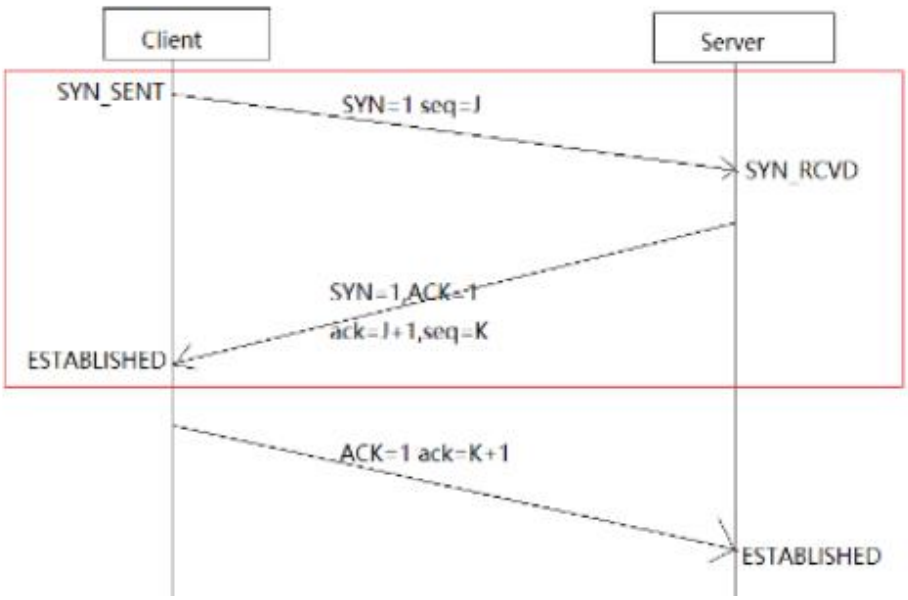
在线破解：账号密码---需要认证 用户名已知，用户名未知---密码未知 用户名未知，密码已知

离线破解：密文还原---明文

crunch hydra 在线破解、 medusa

拒绝服务攻击：

SYN flooding：SYN Flooding 攻击是一种很古老的攻击，其实质是 DOS（即拒绝服务攻击），该攻击是利用 TCP/IP 的三次握手（后面会说到详细的过程），利用大量虚假的 IP 身份建立不完整连接，消耗目标主机的 CPU。从而使目标主机近于瘫痪。



攻击者向服务器或者目标主机发送 SYN 请求连接，服务器或者目标主机在收到连接请求时会进行请求确定，即向攻击者进行连接确认，此时攻击者便会停止向服务器发送确认连接的确认包，因此，服务器或目标主机就处在了等待确认的阶段，在正常情况下，服务器或目标主机在等待一定时间后就会停止等待，此次连接也就自然而然的结束了，也就不会造成什么危害。但是攻击者会在短时间里伪造大量的 SYN 请求连接包发给服务器或目标主机，即使每条 SYN 请求包会在很短时间内被丢弃，但是大量的请求包在同一时间进行请求连接，服务器或目标主机没有足够的时间去处理这些请求包，因此就会使服务器或目标主机的 CPU 利用率下降，甚至使服务器或目标主机瘫痪。

Smurf：

Smurf 拒绝服务攻击是以最初发动这种攻击的程序名 Smurf 来命名的。这种攻击方法结合使用了 IP 欺骗和 ICMP 回复方法使大量网络数据充斥目标系统，引起目标系统拒绝为正常请求进行服务。

Smurf 攻击的原理如图 3-37 所示，攻击者主要使用 IP 广播和 IP 欺骗的方法，发送伪造的 ICMPECHOREQUEST 包给目标网络的 IP 广播地址。

ICMP 是用来处理错误和交换控制信息的，并且可以用来确定网络上的某台主机是否响应。在一个网络上，可以向某个单一主机，也可以向局域网的广播地址发送 IP 包。当攻击者自某个网络的广播地址发送 ICMPECHOREQUEST 包时，如果网络的路由器对发往网络广播地址的 ICMP 包不进行过滤，则网络内部的所有主机都可以接收到该 ICMP 包，并且都要向 ICMP 包所指示的源地址发送 ICMPECHOREPLY 响应包。如果攻击者将发送的 ICMP 包的源地址伪造成被攻击者的地址，则该网络上所有主机的 ICMPECHOREPLY 包都要发往被攻击的主

机。这种攻击不仅造成被攻击主机流量过载、减慢甚至停止正常的服务，而且发出 ICMP 响应包的中间受害网络也会出现拥塞甚至网络瘫痪。可以说， Smurf 攻击的受害者是攻击者的攻击目标和无辜充当攻击者攻击工具的第三方网络。

对于被攻击者利用的"无辜"中间网络和被攻击的目标，无论它们的内部网络还是与因特网的连接， Smurf 攻击都会使网络性能受到影响，严重时这个网络都无法使用。而且，为这些网络提供服务的中小 ISP 也会因此降低其网络效率和服务质量。对于大型 ISP 而言，其骨干网可能出现饱和现象顶部分影响其服务庚量。

Ping of death:

在因特网上，ping of death 是一种畸形报文攻击，方法是由攻击者故意发送大于 65535 字节的 ip 数据包给对方。 导致内存溢出，这时主机就会出现内存分配错误而导致 TCP/IP 堆栈崩溃，导致死机！TCP/IP 的特征之一是分片；它允许单一 IP 包被分为几个更小的数据包。

Teardrop：

Teardrop 攻击是一种畸形报文攻击。是基于 UDP 的病态分片数据包的攻击方法，其工作原理是向被攻击者发送多个分片的 IP 包（IP 分片数据包中包括该分片数据包属于哪个数据包以及在数据包中的位置等信息），某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。

Winnuke：

WinNuke 攻击是一种拒绝服务攻击。WinNuke 攻击又称带外传输攻击，它的特征是攻击目标端口，被攻击的目标端口通常是 139、138、137、113、53，而且 URG 位设为“1”，即紧急模式。

电子邮件轰炸：

电子邮件轰炸是最早的一种拒绝服务攻击，它的表现形式是在很短时间内收到大量无用的电子邮件。因为所有的邮件都需要空间来保存，同时收到的邮件需要系统来处理。过多的邮件会加酣网络连接负担、消耗大量的存储空 f 曰:过多的投递会导致系统日志文件变得巨大，甚至溢出文件系统，这将给许多操作系统(如 UNIX 和 Windows)带来危险。而且，大量到来的邮件将消耗大量的处理器时间，占用大量的带宽，延缓甚至阻止系统的正常处理活动。这都影响了正常业务的运行，严重时使系统死机、网络瘫痪。

电子邮件轰炸实质上也是一种针对服务端口(SMTP 端口，即 25 端口)的攻击方式，它的原理是：连接到邮件服务器的 SMTP(25)端口，按照 SMTP 协议发送几仔头信息加上一堆文字垃圾，就算只发送了一封邮件，反复多次，就形成了邮件炸弹。在这种攻击中，攻击者需要谨慎的是隐藏自己的踪迹，也就是隐藏自己的 IP。

对付电子邮件轰炸的办法不是很多，可以识别邮件炸弹的源头，配置路由器，不使其通过。可以配置防火墙，但防火墙最多只能防止从攻击者源头发来的信息。另外需要保证防火墙能使外头的 SMTP 连接只能到达指定服务器，而不能影响其他系统。当然，这并不能防止攻击，只是减少轰炸对其他系统的影响。使用最新版本的电子邮件服务软件，提高系统记账能力，有利于对发生的事件进行追踪。

由于电子邮件轰炸不一定是 100%的匿名行动，因此可能根据头信息来跟踪发出地。但如果攻击者真的要攻击的话，就会远程登录到 SMTP 端口，然后直接发出 SMTP 命令，如果主机正在运行，入侵可能会遇到障碍，不过入侵者可以冒充他人，因此也会得逞。

DDOS 攻击防御方法：(PPT 也有)

1. 过滤不必要的服务和端口：可以使用 Inexpress、Express、Forwarding 等工具来过滤不必要的服务和端口，即在路由器上过滤假 IP。比如 Cisco 公司的 CEF(Cisco Express Forwarding)可以针对封包 Source IP 和 Routing Table 做比较，并加以过滤。只开放服务端口成为目前很多服务器的流行做法，例如 WWW 服务器那么只开放 80 而将其他所有端口关闭或在防火墙上做阻止策略。

2. 异常流量的清洗过滤：通过 DDOS 硬件防火墙对异常流量的清洗过滤，通过数据包的规则过滤、数据流指纹检测过滤、及数据包内容定制过滤等顶尖技术能准确判断外来访问流量是否正常，进一步将异常流量禁止过滤。单台负载每秒可防御 800-927 万个 syn 攻击包。

3. 分布式集群防御：这是目前网络安全界防御大规模 DDOS 攻击的最有效办法。分布式集群防御的特点是在每个节点服务器配置多个 IP 地址（负载均衡），并且每个节点能承受不低于 10G 的 DDOS 攻击，如一个节点受攻击无法提供服务，系统将会根据优先级设置自动切换另一个节点，并将攻击者的数据包全部返回发送点，使攻击源成为瘫痪状态，从更为深度的安全防护角度去影响企业的安全执行决策。

4. 高防智能 DNS 解析：高智能 DNS 解析系统与 DDOS 防御系统的完美结合，为企业提供对抗新兴安全威胁的超级检测功能。它颠覆了传统一个域名对应一个镜像的做法，智能根据用户的上网路线将 DNS 解析请求解析到用户所属网络的服务器。同时智能 DNS 解析系统还有宕机检测功能，随时可将瘫痪的服务器 IP 智能更换成正常服务器 IP，为企业的网络保持一个永不宕机的服务状态。

缓冲区溢出攻击：

shellcode：

在计算机安全中，shellcode 是一小段代码，可以用于软件漏洞利用的载荷。被称为“shellcode”是因为它通常启动一个命令终端，攻击者可以通过这个终端控制受害的计算机，但是所有执行类似任务的代码片段都可以称作 shellcode。……Shellcode 通常是以机器码形式编写的。

shellcode 是一段可用于漏洞利用载荷的机器码。

举例：

```
void exploit(char *data)
{
    char buffer[20];      // 缓冲区位于栈上
    strcpy(buffer, data); // 使用strcpy复制数据
}
```

利用此漏洞的主要思路如下：

1）向应用程序发送长度超过 20 字节的字符串，其中包含 shellcode。

2）由于写入数据越过静态分配缓冲区的边界，栈结构遭到破坏。同时，shellcode 也会被放置在栈上。

3）字符串通过自定义的内存地址重写栈上某块重要数据（如保存的 EIP 或函数指针）

4）程序会从栈上跳转到你的 shellcode，开始执行其中的机器码指令。

如果可以成功的利用此漏洞，你也能够运行自己的 shellcode，并实际利用该漏洞做点有用的事情，而不仅仅是让程序崩溃。比如 shellcode 可以打开一个命令终端，下载并执行文件，重启计算机、启用远程桌面、或其他操作。

shellcode 特点：

不能是任意的机器码。在编写自己的 shellcode 时，我们必须需要注意 shellcode 的一些限制：

1）不能使用字符串的直接偏移。

2）不能确定函数的地址（如 printf）

3）必须避免一些特定字符（如 NULL 字节）

关于上述的每个问题，让我们进行一个简短的讨论。

1）字符串的直接偏移

即使你在 C/C++代码中定义一个全局变量，一个取值为“Hello world”的字符串，或直接把该字符串作为参数传递给某个函数。但是，编译器会把字符串放置在一个特定的 Section 中（如.rdata 或.data）。

2）函数地址

在 shellcode 中，我们却不能以逸待劳了。因为我们无法确定包含所需函数的 DLL 文件是否已经加载到内存。受 ASLR (地址空间布局随机化) 机制的影响，系统不会每次都把 DLL 文件加载到相同地址上。而且，DLL 文件可能随着 Windows 每次新发布的更新而发生变化，所以我们不能依赖 DLL 文件中某个特定的偏移。

我们需要把 DLL 文件加载到内存，然后直接通过 shellcode 查找所需要的函数。幸运的是，Windows API 为我们提供了两个函数：LoadLibrary 和 GetProcAddress。我们可以使用这两个函数来查找函数的地址。

3）空字节（NULL）的取值为：0×00。在 C/C++代码中，空字节被认为是字符串的结束符。正因如此，shellcode 存在空字节可能会扰乱目标应用程序的功能，而我们的 shellcode 也可能无法正确地复制到内存中。

虽然不是强制的，但类似利用 strcpy()函数触发缓冲区溢出的漏洞是非常常见的情况。该函数会逐字节拷贝字符串，直至遇到空字节。因此，如果 shellcode 包含空字节，strcpy 函数便会在空字节处终止拷贝操作，引发栈上的 shellcode 不完整。正如你所料，shellcode 当然也不会正常的运行。

例如 MOV EAX,0; XOR EAX,EAX; 两条指令从功能上来说是等价的，但你可以清楚地看到第一条指令包含空字节，而第二条指令却包含空字节。虽然空字节在编译后的代码中非常常见，但是我们可以很容易地避免。

还有，在一些特殊情况下，shellcode 必须避免出现类似\r 或\n 的字符，甚至只能使用字母数

Linux 平台与 Windows 平台的 shellcode 对比

相对于 Windows 平台，编写针对 Linux 平台的 Shellcode 可能更为简单。这是因为在 linux 平台上，我们可以轻松地通过 0×80 中断执行类似 write、execve 或 send 的系统调用。

shellcode 构造：

shellcode 实质是指溢出后执行的能开启系统 shell 的代码。但是在缓冲区溢出攻击时，也可以将整个触发缓冲区溢出攻击过程的代码统称为 shellcode，按照这种定义可以把 shellcode 分为四部分：

1、核心 shellcode 代码，包含了攻击者要执行的所有代码。

2、溢出地址，是触发 shellcode 的关键所在。

3、填充物，填充未使用的缓冲区，用于控制溢出地址的位置，一般使用 nop 指令填充——0x90 表示。

4、结束符号 0，对于符号串 shellcode 需要用 0 结尾，避免溢出时字符串异常。

欺骗攻击：

DNS 工作过程：

DNS 是一种实现 Domain Name 和 IP Address 之间转换的系统，它的工作原理就是在两者间进行相互映射，相当于起到翻译作用，所以称为域名解析系

统。DNS System 分为 Server 和 Client 两部分，Server 的通用 Port 是 53。当 Client 向 Server 发出解析请求时，Local DNS Server 第一步查询自身的 Database 是否存在需要的内容，如果有则发送应答数据包并给出相应的结果; 否则它将向上一层 DNS Server 查询。如此不断查询，最终直至找到相应的结果或者将查询失败的信息反馈给客户机。如果 Local DNS Server 查到信息,则先将其保存在本机的高速缓存中，然后再向客户发出应答。日常我们上网是通过 Browser 方式来申请从 Domain Name 到 IP Address 的解析,即 Client 向 DNS Server 提交域名翻译申请，希望得到对应的 IP Address。

DNS 欺骗攻击原理：

Client 的 DNS 查询请求和 DNS Server 的应答数据包是依靠 DNS 报文的 ID 标识来相互对应的。在进行域名解析时，Client 首先用特定的 ID 号向 DNS Server 发送域名解析数据包，这个 ID 是随机产生的。DNS Server 找到结果后使用此 ID 给 Client 发送应答数据包。Client 接收到应答包后，将接收到的 ID 与请求包的 ID 对比，如果相同则说明接收到的数据包是自己所需要的，如果不同就丢弃此应答包。根据攻击者的查询和应答原理，可使用不同方法实现攻击，如：

(1)因为 DNS Message 仅使用一个简单的认证码来实施真实性验证，认证码是由 Client 程序产生并由 DNS Server 返回结果的，客户机只是使用这个认证码来辨别应答与申请查询是否匹配，这就使得针对 ID 认证码的攻击威胁成为可能。

(2)在 DNS Request Message 中可以增加信息，这些信息可以与客户机所申请查询的内容没有必然联系，因此攻击者就能在 Request Message 中根据自己的目的增加某些虚假的信息，比如增加其它 Domain Server 的 Domain Name 及其 IP Address。此时 Client 在受到攻击的 Domain Server 上的查询申请均被转向此前攻击者在 Request Message 中增加的虚假 Domain Server，由此 DNS 欺骗得以产生并对网络构成威胁。

(3)当 DNS Server 接收到 Domain Name 和 IP Address 相互映射的数据时，就将其保存在本地的 Cache 中。若再有 Client 请求查询此 Domain Name 对应的 IP Address，Domain Server 就会从 Cache 中将映射信息回复给 Client，而无需在 Database 中再次查询。如果黑客将 DNS Request Message 的存在周期设定较长时间，就可进行长期欺骗。

三、DNS 欺骗检测和防范思路

3.1 检测思路

发生 DNS 欺骗时，Client 最少会接收到两个以上的应答数据报文，报文中都含有相同的 ID 序列号，一个是合法的，另一个是伪装的。据此特点，有以下两种检测办法：

(1)被动监听检测。即监听、检测所有 DNS 的请求和应答报文。通常 DNS Server 对一个请求查询仅仅发送一个应答数据报文(即使一个域名和多个 IP 有映射关系，此时多个关系在一个报文中回答)。因此在限定的时间段内一个请求如果会收到两个或以上的响应数据报文，则被怀疑遭受了 DNS 欺骗。

(2)主动试探检测。即主动发送验证包去检查是否有 DNS 欺骗存在。通常发送验证数据包接收不到应答，然而黑客为了在合法应答包抵达客户机之前就将欺

骗信息发送给客户，所以不会对 DNS Server 的 IP 合法性校验，继续实施欺骗。若收到应答包，则说明受到了欺骗攻击。

3.2 防范思路

在侦测到网络中可能有 DNS 欺骗攻击后，防范措施有：①在客户端直接使用 IP Address 访问重要的站点，从而避免 DNS 欺骗; ②对 DNS Server 和 Client 的数据流进行加密，Server 端可以使用 SSH 加密协议，Client 端使用 PGP 软件实施数据加密。

对于常见的 ID 序列号欺骗攻击，采用专业软件在网络中进行监听检查，在较短时间内，客户端如果接收到两个以上的应答数据包，则说明可能存在 DNS 欺骗攻击，将后到的合法包发送到 DNS Server 并对 DNS 数据进行修改，这样下次查询申请时就会得到正确结果。

四、DNS 防护方案

4.1 进行 IP 地址和 MAC 地址的绑定

(1)预防 ARP 欺骗攻击。因为 DNS 攻击的欺骗行为要以 ARP 欺骗作为开端，所以如果能有效防范或避免 ARP 欺骗，也就使得 DNS ID 欺骗攻击无从下手。例如可以通过将 Gateway Router 的 Ip Address 和 MAC Address 静态绑定在一起，就可以防范 ARP 攻击欺骗。

(2)DNS 信息绑定。DNS 欺骗攻击是利用变更或者伪装成 DNS Server 的 IP Address，因此也可以使用 MAC Address 和 IP Address 静态绑定来防御 DNS 欺骗的发生。由于每个 Network Card 的 MAC Address 具有唯一性质，所以可以把 DNS Server 的 MAC Address 与其 IP Address 绑定，然后此绑定

信息存储在客户机网卡的 Eprom 中。当客户机每次向 DNS Server 发出查询申请后，就会检测 DNS Server 响应的应答数据包中的 MAC Address 是否与 Eprom 存储器中的 MAC Address 相同,要是不同,则很有可能该网络中的 DNS Server 受到 DNS 欺骗攻击。这种方法有一定的不足，因为如果局域网内部的客户主机也保存了 DNS Server 的 MAC Address，仍然可以利用 MAC Address 进行伪装欺骗攻击。

4.2 使用 Digital Password 进行辨别

在不同子网的文件数据传输中，为预防窃取或篡改信息事件的发生，可以使用任务数字签名(TSIG)技术即在主从 Domain Name Server 中使用相同的 Password 和数学模型算法，在数据通信过程中进行辨别和确认。因为有 Password 进行校验的机制，从而使主从 Server 的身份地位极难伪装，加强了 Domain Name 信息传递的安全性。

安全性和可靠性更好的 Domain Name Service 是使用域名系统的安全协议(Domain Name System Security, DNSSEC))，用 Digital Signature 的方式对搜索中的信息源进行分辨，对 DATA 的完整性实施校验，DNSSEC 的规范可参考 RFC2605。因为在设立 Domain 时就会产生 Password，同时要求上层的 Domain Name 也必须进行相关的 Domain Password Signature，显然这种方法很复杂，所以 InterNIC 域名管理截至目前尚未使用。然而就技术层次上讲，DNSSEC 应该是现今最完善的 Domain Name 设立和解析的办法，对防范 Domain Name 欺骗攻击等安全事件是非常有效的。

4.3 优化 DNS SERVER 的相关项目设置

对于 DNS Server 的优化可以使得 DNS 的安全性达到较高的标准，常见的工作有以下几种：①对不同的子网使用物理上分开的 Domain Name Server,从而获得 DNS 功能的冗余;②将外部和内部 Domain Name Server 从物理上分离开并使用 Forwarders 转发器。外部 Domain Name Server 可以进行任何客户机的申请查询，但 Forwarders 则不能，Forwarders 被设置成只能接待内部客户机的申请查询;③采用技术措施限制 DNS 动态更新;④将区域传送(zone transfer)限制在授权设备上;⑤利用事务签名对区域传送和区域更新进行数字签名;⑥隐藏服务器上的 Bind 版本;⑦删除运行在 DNS 服务器上的不必要服务，如 FTP、telnet 和 Http;⑧在网络外围和 DNS 服务器上使用防火墙,将访问限制在那些 DNS 功能需要的端口上。

4.4 直接使用 IP 地址访问

对个别信息安全等级要求十分严格的 WEB 站点尽量不要使用 DNS 进行解析。由于 DNS 欺骗攻击中不少是针对窃取客户的私密数据而来的，而多数用户访问的站点并不涉及这些隐私信息，因此当访问具有严格保密信息的站点时，可以直接使用 IP 地址而无需通过 DNS 解析，这样所有的 DNS 欺骗攻击可能造成的危害就可以避免了。除此，应该做好 DNS Server 的安全配置项目和升级 DNS 软件，合理限定 DNS Server 进行响应的 IP 地址区间，关闭 DNS Server 的递归查询项目等。

4.5 对 DNS 数据包进行监测

在 DNS 欺骗攻击中，Client 会接收到至少两个 DNS 的数据响应包，一个是真实的数据包，另一个是攻击数据包。欺骗攻击数据包为了抢在真实应答包之前回复给 Client，它的信息数据结构与真实的数据包相比十分简单，只有应答域，

而不包括授权域和附加域。因此，可以通过监测 DNS 响应包，遵循相应的原则和模型算法对这两种响应包进行分辨，从而避免虚假数据包的攻击。

自主访问控制机制允许对象的属主来制定针对该对象的保护策略。通常 **DAC** 通过授权列表（或访问控制列表）来限定哪些主体针对哪些客体可以执行什么操作。如此将可以非常灵活地对策略进行调整。由于其易用性与可扩展性，自主访问控制机制经常被用于商业系统。

访问控制技术：

自主访问控制机制允许对象的属主来制定针对该对象的保护策略。通常 **DAC** 通过授权列表（或访问控制列表）来限定哪些主体针对哪些客体可以执行什么操作。如此将可以非常灵活地对策略进行调整。由于其易用性与可扩展性，自主访问控制机制经常被用于商业系统。大多数系统仅基于自主访问控制机制来实现访问控制，如主流操作系统(**Windows NT Server, UNIX** 系统)，防火墙（**ACLs**）等。

依据 Bel l-Lapad uła 安全模型所制定的原则是利 用不上读/不下写来保证数据的保密性。即不允许低信任级别的用户读高敏感度的信息，也不允许高敏感度的信息写入低敏感度区域，禁止信息从高级别流向低级别。强制访问控制通过这种梯度安全标签实现信息的单向流通 。

依据 Bib a 安全模型所制定的原则是利用不 下读/不上写来保证数据的完整性。在实际应用中，完整性保护主要是为了避免应用程序修改某些重要的系统程序或系统 数据库。

MAC 通常用于多级安全军事系统 。

强制访问控制对专用的或简单的系统是有效的，但对通用、大型系统并不那么有效。一般强制访问控制采用以下几种方 法:

6、为什么自主访问控制无法抵御木马攻击？举例

木马是一段计算机程序，镶嵌在合法用户的应用程序中，当用户运行这个应用程序的时候，它就悄无声息运行非法操作，一般察觉不到，使得 DAC 无法识别。

7、什么是强制访问控制方式?如何防止木马的非法访问?

强制访问控制是通过无法回避的访问限制来防止某些对系统的非法入侵。

强制访问控制一般与自主访问控制结合使用，并实施一些附加的、更强的访问限制。一个主体只有通过了自主与强制访问控制检查后，才能访问某个客体。用户利用自主访问控制来防范其他用户对客体的攻击。强制访问控制则提供一个不可逾越的、更强的防护，以防止其他用户偶然或故意滥用自主访问控制。强制访问控制不可避免的对用户的客体十佳一些严格的限制，使得用户无意泄漏机密信息的可能性大大减少

RBAC 实例:

（RBAC0：。在这个模型中，我们把权限赋予角色，再把角色赋予用户。用户和角色，角色和权限都是多对多的关系。用户拥有的权限等于他所有的角色持有权限之和。）譬如我们做一款企业管理产品，如果按传统权限模型，给每一个用户赋予权限则会非常麻烦，并且做不到批量修改用户权限。这时候，可以抽

象出几个角色，譬如销售经理、财务经理、市场经理等，然后把权限分配给这些角色，再把角色赋予用户。这样无论是分配权限还是以后的修改权限，只需要修改用户和角色的关系，或角色和权限的关系即可，更加灵活方便。此外，如果一个用户有多个角色，譬如王先生既负责销售部也负责市场部，那么可以给王先生赋予两个角色，即销售经理+市场经理，这样他就拥有这两个角色的所有权限。

（RBAC1-继承）：基于之前 RBAC0 的例子，我们又发现一个公司的销售经理可能是分几个等级的，譬如除了销售经理，还有销售副经理，而销售副经理只有销售经理的部分权限。这时候，我们就可以采用 RBAC1 的分级模型，把销售经理这个角色分成多个等级，给销售副经理赋予较低的等级即可。

（RBAC2-互斥、先决条件：RBAC2 同样建立在 RBAC0 基础之上，仅是对用户、角色和权限三者之间增加了一些限制。这些限制可以分成两类，即静态职责分离 SSD(Static Separation of Duty)（互斥角色限制、基数限制、先决条件限制）动态职责分离 DSD(Dynamic Separation of Duty)（运行时约束））：

还是基于之前 RBAC0 的例子，我们又发现有些角色之间是需要互斥的，譬如给一个用户分配了销售经理的角色，就不能给他再赋予财务经理的角色了，否则他即可以录入合同又能自己审核合同；再譬如，有些公司对角色的升级十分看重，一个销售员要想升级到销售经理，必须先升级到销售主管，这时候就要采用先决条件限制了。

基于 RBAC 模型，还可以适当延展，使其更适合我们的产品。譬如增加用户组概念，直接给用户组分配角色，再把用户加入用户组。这样用户除了拥有自

身的权限外，还拥有了所属用户组的所有权限。譬如，我们可以把一个部门看成一个用户组，如销售部，财务部，再给这个部门直接赋予角色，使部门拥有部门权限，这样这个部门的所有用户都有了部门权限。用户组概念可以更方便的给群体用户授权，且不影响用户本来就拥有的角色权限。

- **5-7 简述 Kerberos 认证协议的设计思想和实现方法。**

- 参考答案： Keberos 引入票据准许服务器作为认证框架，实现了认证和服务访问许可的分离式管理，其基本目的 是避免口令在网络上的传递，并减少口令的使用次数 。具体实现方法简要描述如下：用户通过认证服务器验证身份，获取票据准许服务器的许可票据，票据准许服务器验证用户的许可票据，通过则获取服务许可票据，持服务许可票据就可以访问特定的服务。依据此过程，无论用户需要访问多少个服务，都是通过认证服务器认证和票据准许服务器的许可，无需与需要访问的服务间进行直接的认证，从而避免重复出示用户名和口令的问题 。

- **Kerberos 优缺点（PPT 有优点）。**

1. 安全的防护多种不同的侵入攻击，比如 Impersonation 和 replay attach 等。
2. 使用票据的传输，在认证过程中可以不需要传输任何长效密钥，而且客户端和应用服务器之间可以不需要知道对方的密钥信息
3. 有很好的互操作性，不同的平台可以基于 Kerberos 认证协议进行广泛的互操作。

4. 可以实现双向验证。其他的类似 NTLM 的认证协议，都是基于一个假设，即远程的服务是可信的。实际上，仿冒服务器在如今的 Internet 是一个比较常见的。Kerberos 认证协议很好的解决了服务身份认证的问题。

1. 存在单点故障。Kerberos 身份认证过程需要 KDC 的持续可用。到 KDC 出现问题时，用户就不能被认证登录或者使用依赖 Kerberos 的服务。一般情况下，这种单点故障可以通过部署多台 KDC 并通过认证过程的 Failover 机制可以解决。
2. Kerberos 需要各个实体采用相同并且严格的时间戳。这就需要各个实体必须配置相同的时钟或者通过类似 NTP 的机制进行时钟同步。
3. 如果在 Kerberos 环境中使用对称密钥则存在很大的安全隐患。黑客一旦控制了 KDC，则他可以仿冒所有实体。
4. 需要所有实体在 Kerberos KDC 中被信任，无法满足网络中非信任实体的访问认证。

身份认证方式的对比：

身份认证的认证形式来分，目前有：用户名/密码认证、智能卡认证、动态口令认证、USB Key 认证、生物特征认证等。

（1）用户名/密码是最简单也是最常用的身份认证方法，是基于“what you know”的验证手段。每个用户的密码是由用户自己设定的，只有用户自己才知道。只要能够正确输入密码，计算机就认为操作者就是合法用户。实际上，由于许多用户为了防止忘记密码，经常采用诸如生日、电话号码等容易被猜测的字符串作

为密码，或者把密码抄在纸上放在一个自认为安全的地方，这样很容易造成密码泄漏。即使能保证用户密码不被泄漏，由于密码是静态的数据，在验证过程中需要在计算机内存中和网络中传输，而每次验证使用的验证信息都是相同的，很容易被驻留在计算机内存中的木马程序或网络中的监听设备截获。因此，它是一种单因素的认证,安全性依赖于密码，从安全性上讲，用户名/密码方式一种是极不安全的身份认证方式。

（2）智能卡是一种内置集成电路的芯片，芯片中存有与用户身份相关的数据，智能卡由专门的厂商通过专门的设备生产，是不可复制的硬件。智能卡由合法用户随身携带，登录时必须将智能卡插入专用的读卡器读取其中的信息，以验证用户的身份。智能卡认证是基于“what you have”的手段，通过智能卡硬件不可复制来保证用户身份不会被仿冒。基于智能卡的认证方式是一种双因素的认证方式(PIN+智能卡),即使 PIN 或智能卡被窃取,用户仍不会被冒充。然而由于每次从智能卡中读取的数据是静态的，通过内存扫描或网络监听等技术还是很容易截取到用户的身份验证信息，因此还是存在一定的安全隐患。

（3）动态口令技术是一种让用户密码按照时间或使用次数不断变化、每个密码只能使用一次的技术。它采用一种叫作动态令牌的专用硬件，内置电源、密码生成芯片和显示屏，密码生成芯片运行专门的密码算法，根据当前时间或使用次数生成当前密码并显示在显示屏上。认证服务器采用相同的算法计算当前的有效密码。用户使用时只需要将动态令牌上显示的当前密码输入客户端计算机，即可实现身份认证。由于每次使用的密码必须由动态令牌来产生，只有合法用户才持有该硬件，所以只要通过密码验证就可以认为该用户的身份是可靠的。而用户

每次使用的密码都不相同，即使黑客截获了一次密码，也无法利用这个密码来仿冒合法用户的身份。

动态口令技术采用一次一密的方法，有效保证了用户身份的安全性。但是如果客户端与服务器端的时间或次数不能保持良好的同步，就可能发生合法用户无法登录的问题。并且用户每次登录时需要通过键盘输入一长串无规律的密码，一旦输错就要重新操作，使用起来非常不方便。

（6）生物识别技术主要是指通过可测量的身体或行为等生物特征进行身份认证的一种技术。生物特征是指唯一的可以测量或可自动识别和验证的生理特征或行为方式。生物特征分为身体特征和行为特征两类。身体特征包括：指纹、掌型、视网膜、虹膜、人体气味、脸型、手的血管和 DNA 等；行为特征包括：签名、语音、行走步态等。目前部分学者将视网膜识别、虹膜识别和指纹识别等归为高级生物识别技术；将掌型识别、脸型识别、语音识别和签名识别等归为次级生物识别技术；将血管纹理识别、人体气味识别、DNA 识别等归为“深奥的”生物识别技术。基于生物特征的认证方式是以人体惟一的,可靠的,稳定的生物特征(如指纹,虹膜,脸部,掌纹等)为依据,采用计算机的强大功能和网络技术进行图像处理和模式识别.该技术具有很好的安全性,可靠性和有效性,与传统的身份确认手段相比,无疑产生了质的飞跃。

网闸：（网闸的数据传输都是基于应用层代理）

物理隔离网闸是使用带有多种控制功能的固态开关读写介质连接两个独立主机系统的信息安全设备。由于物理隔离网闸所连接的两个独立主机系统之间，

不存在通信的物理连接、逻辑连接、信息传输命令、信息传输协议，不存在依据协议的信息包转发，只有数据文件的无协议“摆渡”，且对固态存储介质只有“读”和“写”两个命令。所以，物理隔离网闸从物理上隔离、阻断了具有潜在攻击可能的一切连接，使“黑客”无法入侵、无法攻击、无法破坏，实现了真正的安全。

网闸是在两个不同安全域之间，通过协议转换的手段，以信息摆渡的方式实现数据交换，且只有被系统明确要求传输的信息才可以通过。其信息流一般为通用应用服务。

3、简述口令认证技术的认证方法？提高口令认证技术的安全性方法？

提高方法：采用通行短语代替通行字，通过密码碾压技术，可将易于记忆的足够长的短语变换成较短的随机性密钥

4、网络的物理隔离技术包含哪些方面？他们各自采用什么技术？

客户端的物理隔离：集线器级的物理隔离:服务器端的物理隔离：

防火墙：

2、防火墙规则的处理方式中，“reject”和“drop”的区别？

Reject：拒绝数据包或信息通过，并且通知信息源该信息被禁止

Drop：直接将数据包丢弃，并且不通知信息源

3、防火墙产品的两条基本原则？（只采用其中一种）

（1）一切未被允许的就是禁止的（安全性高，但限制了用户能使用的服务种类，缺乏方便性）（2）一起未被禁止的就是允许的（使用方便、规则配置灵活、安全性低）

4、源 IP=192.168.1.1 目的 IP=192.168.2.1 协议=TCP 源端口>1024 目的端口=80 表示怎样的数据包?

表示该数据包是由 IP 地址为 192.168.1.1 的主机发送、由 IP 为 192.168.2.1 的主机接收的一个 tcp 包，其产生的数据包应用程序占用 1024 以上端口，需要传递至 80 号端口的应用程序。（小于 1024 表示传递到系统端口）

5. 典型防火墙设计（看书）

1、屏蔽路由器模式

这是最初的防火墙设计方案，它不是采用专用的设备部署的，而是在原有的路由器上进行包过滤部署的。具备这种包过滤技术的路由器也称为”屏蔽路由器“。

一个屏蔽路由器是最简单的防火墙策略。这个方法在防火墙概念提出初期非常流行，主要是因为很多公司已经具备了这样的硬件条件，也没有专门的防火墙

设备推出。原有路由器设备的公司只需要进行一些另外的包过滤配置即可实现防火墙安全策略。这种防火墙方案拓扑结构如图 4 所示。

在图中担当屏蔽路由器角色的就是原有路由器，在其中的防火墙包过滤配置中，可以根据数据包包头信息中的 IP 地址、UDP 和 TCP 端口来过滤数据。

这种防火墙方案有个最大的缺点就是配置复杂，非专业人员很难正确、有效地配置。如果采用这种措施，就需要对 TCP/IP 有很好的理解，并能够在路由器上正确地进行有关数据包过滤的设置。如果不能够正确地进行配置，危险的数据包就有可能透过防火墙进入内部局域网。如果这是唯一的安全设备，那么黑客们将非常容易地攻破系统，在局域网里为所欲为。另外一点值得注意的就是采用这种措施，内部网络的 IP 地址并没有被隐藏起来，并且它不具备监测，跟踪和记录的功能。

当然，如果经费有限而且非常急切地需要一个防火墙的解决方案，这个方法能够使花费最少，并可以使用现有的路由器。同时，这也是进一步进行防火墙措施的一个良好开端。当增加别的网络安全设备的时候，它也还可以使用。

2、 双宿主机模式

这种模式也有称”双穴主机模式“。它是一种非常简单的防火墙模式，它不是用真正的硬件防火墙来实现的，它是通过在一台俗称为”堡垒主机“的计算机上安装有配置网络控制软件来实现的。所谓”双宿主机“，就是指堡垒主机同时连接着一个内、外部网络，担当起全部的网络安全维护责任。网络拓扑结构如图 5 所示。

在图中起安全防护作用的堡垒主机其实就是一台计算机，为了自身的安全，在这台堡垒主机上安装的服务最少，只需要安装一些与包过滤功能有关的软件，满足一般的网络安全防护即可。它所拥有权限最少，这样就可避免一旦黑客攻占了堡垒主机后，迅速控制内部网络的不良后果。因为控制权限低，黑客虽然攻陷了堡垒主机，但仍不能拥有什么过高的网络访问权限，也就不至于给内部网络造成太大危害。

在这种双宿主机模式还有的，应用于对多个内部网络或网段的维护。就是一个堡垒主机同时连接着一个外部网络和两个或以上内部网络(或网段)。这就需要在堡垒主机上安装多块网卡。

3、屏蔽主机模式

由于前一种”屏蔽路由器“防火墙方案过于单调，很容易被黑客攻击，所以在后期的防火墙技术中，又增加一道安全防线，在路由器后增加了一个用于应用安全控制的计算机，充当堡垒主机角色。这就是所谓的”屏蔽主机防火墙“模式，又有称”屏蔽主机“模式。屏蔽主机防火墙模式网络网络拓扑结构如图 6 所示。

这种设计采用屏蔽路由器和堡垒主机双重安全设施，所有进出的数据都要经过屏蔽路由器和堡垒主机，保证了网络级和应用级的安全。路由器进行包过滤，堡垒主机进行应用安全控制。这是一种很可靠的设计，一个黑客必须穿透路由和堡垒主机才能够到达内部网络。为了使堡垒主机具备足够强的抗攻击性能，在堡垒主机上只安装最小的服务、并且所拥有的权限也是最低的。

采用这种设计作为应用级网关(代理服务器)，可以使用网络地址转换(NAT)技术来屏蔽内部网络。可以更进一步，建立”屏蔽多宿主机防火墙“模式。在这种结构中，堡垒主机可以连接多个内部网络或网段，也就需在堡垒主机上安装多块网卡。它同样可以使内部网络在物理上和外部网络断开，所以也可以达到保护内部网络的目的。多宿主机防火墙网络拓扑结构如图 7 所示。

看课本