==========Ledon==========

一、名词解释

1.**计算机安全**：为数据处理系统和采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。

2.**SOP**：标准作业程序，就是将某一事件的标准操作步骤和要求以统一的格式描述出来，用来指导和规范日常的工作。

3.**CSRF**:跨站请求伪造,是一种对网站的恶意利用。尽管听起来像跨站脚本(XSS)，但它与 XSS 非常不同，XSS 利用站点内的信任用户，而 CSRF 则通过伪装来自受信任用户的请求来利用受信任的网站。与 XSS 攻击相比，CSRF 攻击往往不大流行（因此对其进行防范的资源也相当稀少）和难以防范，所以被认为比 XSS 更具危险性。

4.**逻辑炸弹**：计算机中的“逻辑炸弹”是指在特定逻辑条件满足时，实施破坏的计算机程序，该程序触发后造成计算机数据丢失、计算机不能从硬盘或者软盘引导，甚至会使整个系统瘫痪，并出现物理损坏的虚假现象。

5.**漏洞**：漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。是受限制的计算机、组件、应用程序或其他联机资源的无意中留下的不受保护的入口点。

6.**Virus**：是编制者在计算机程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用，能自我复制的一组计算机指令或者程序代码。

7.**XSS**：跨站脚本攻击，为不和层叠样式表的缩写混淆，故将跨站脚本攻击缩写为 XSS。恶意攻击者往 Web 页面里插入恶意 Script 代码，当用户浏览该页之时，嵌入其中 Web 里面的 Script 代码会被执行，从而达到恶意攻击用户的特殊目的

二、简答题

一、栈溢出的原因及危害

1> 函数调用层次过深,每调用一次,函数的参数、局部变量等信息就压一次栈。

2> 局部静态变量体积太大

危害：带来的危害一种是程序崩溃导致拒绝服务， 另外一种就是跳转并且执行一段恶意代码

二、简述通常黑客攻击的步骤

a. 收集信息： 信息收集的目的是为了进入要攻击的目标网络的数据库.黑客会利用公开的协议或者工具(如用 RaceToute 获取到达目标主机所要经过的网络数和路由器数），收集驻留在网络系统中的各个主机系统的相关信息。 b. 系统安全弱点的探测：在收集到攻击目标的一批网络信息之后，黑客会探测网络上的每台主机，以寻求该系统的安全漏洞或者安全弱点，黑客可能使用自编程序或者利用公开的工具（像因特网的电子安全扫描程序 ISS 等）方式自动扫描驻留在联网上的主机。 c. 网络攻击：黑客使用上述方法，收集或者探测到一些“有用”信息之后，就可能会对目标系统实施攻击，如果黑客在某台受损系统上获得了特许权，那么他就可以读取邮件，搜索和盗窃私人文件，毁坏重要数据，从而破坏整个系统的信息，造成不堪设想的后果

三、拒绝服务攻击的手段

PING of death 、UDP flood、SYN flood 、Land Attack

四、主动攻击、被动攻击的特点及举例

主动攻击是攻击者通过网络线路将虚假信息或计算机病毒传入信息系统内部，破坏信息的真实性、完整性及系统服务的可用性，即通过中断、伪造、篡改和重排

信息内容造成信息破坏，使系统无法正常运行。被动攻击是攻击者非常截获、窃取通信线路中的信息，使信息保密性遭到破坏，信息泄露而无法察觉，给用户带来巨大的损失。

五、什么是防火墙？为什么要有防火墙？

防火墙是一种用来加强网络之间访问控制、防止外部网络用户以非法手段通过外部网络进入内部网络、访问内部网络资源，保护内部网络操作环境的特殊网络互连设备。简述防火墙的功能及不足之处。 答：防火墙的基本功能： （1）防火墙能够强化安全策略 （2）防火墙能有效地记录因特网上的活动 （3）防火墙限制暴露用户点 （4）防火墙是一个安全策略的检查站

防火墙的不足之处： （1）不能防范恶意的知情者 （2）防火墙不能防范不通过它的连接 （3）防火墙不能防备全部的威胁

意义：它可通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况， 以此来实现网络的安全保护。

在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，有效地监控了内部网和 Internet 之间的任何活动， 保证了内部网络的安全。

通过过滤不安全的服务，Firewall 可以极大地提高网络安全和减少子网中主机的风险。例如， Firewall 可以禁止 NIS、NFS 服务通过，Firewall 同时可以拒绝源路由和 ICMP 重定向封包。

六、软件漏洞产生的原因？（软件缺陷产生的原因？）

1 输入验证错误：大多数的缓冲区溢出漏洞和 CGI 类漏洞都是由于未对用户提供的输入数据的合法性作适当的检查。

2 访问验证错误：漏洞的产生是由于程序的访问验证部分存在某些可利用的逻辑错误，使绕过这种访问控制成为可能。上面提到的那个早期 AIX 的 rlogin 漏洞就是这种典型。

3 竞争条件：漏洞的产生在于程序处理文件等实体时在时序和同步方面存在问题，这处理的过程中可能存在一个机会窗口使攻击者能够施以外来的影响。早期的 Solaris 系统的 PS 命令存在这种类型的漏洞，PS 在执行的时候会在 tmp 产生一个基于它 PID 的临时文件，然后把它 Chown 为 Root，改名为 PS-Data。如果在 PS 运行时能够创建这个临时文件指向我们有兴趣的文件，这样 PS 执行以后，我们就可以对这个 Root 拥有文件做任意的修改，这可以帮助我们获得 Root 权限。

4 意外情况处置错误：漏洞的产生在于程序在它的实现逻辑中没有考虑到一些意外情况，而这些意外情况是应该被考虑到的。大多数的 tmp 目录中的盲目跟随符号链接覆盖文件的漏洞属于这种类型。例如：ScoUNIXopenserver 的 etcsysadm.dbinuserOsa 存在盲目覆盖调试日志文件的问题，而文件的名字是固定的，通过把文件名指向某些特权文件，可以完全破坏系统。

5 设计错误：这个类别是非常笼统的，严格来说，大多数的漏洞的存在都是设计错误，因此所有暂时无法放入到其他类别的漏洞，先放在这。

6 配置错误：漏洞的产生在于系统和应用的配置有误，或是软件安装在错误的地方，或是错误的配置参数，或是错误的访问权限，策略错误。

7 环境错误：由一些环境变量的错误或恶意设置造成的漏洞。如攻击者可能通过重置 shell 的内部分界符 IFS，shell 的转义字符，或其他环境变量，导致有问题的特权程序去执行攻击者指定的程序。上面提到的 RedHatLinux 的 Dump 程序漏洞就是这种类型。

七、DNS 欺骗基本原理及解决方案

原理：DNS 欺骗就是攻击者冒充域名服务器的一种欺骗行为。 原理：如果可以冒充域名服务器，然后把查询的 IP 地址设为攻击者的 IP 地址，这样的话，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了。
防范：使用最新版本的 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 服务器通过查询其他服务获得查询信息并将它发送给客户机，这两种查询成为递归查询，这种查询方式容易导致 DNS 欺骗。
保护内部设备：像这样的攻击大多数都是从网络内部执行攻击的，如果你的网络设备很安全，那么那些感染的主机就很难向你的设备发动欺骗攻击。
不要依赖 DNS：在高度敏感和安全的系统，你通常不会在这些系统上浏览网页，最后不要使用 DNS。如果你有软件依赖于主机名来运行，那么可以在设备主机文件里手动指定。
使用入侵检测系统：只要正确部署和配置，使用入侵检测系统就可以检测出大部分形式的 ARP 缓存中毒攻击和 DNS 欺骗攻击。
使用 DNSSEC： DNSSEC 是替代 DNS 的更好选择，它使用的是数字前面 DNS 记录来确保查询响应的有效性，DNSSEC 还没有广泛运用，但是已被公认为是 DNS 的未来方向，也正是如此，美国国防部已经要求所有 MIL 和 GOV 域名都必须开始使用 DNSSEC。

八、误用检测的原理及优缺点

原理：通过某种方式提前预先定义某种入侵行为。然后监视系统，从中找出符合预先定义规则的入侵行为
优点：算法简单、系统开销小、准确率高、效率高
缺点：被动：只能检测出已知攻击、新类型的攻击会对系统造成很大威胁。模式库的建立和维护难。知识依赖于：硬件平台、操作系统、系统中运行的程序

九、木马和后门的区别

木马：指一些程序设计人员在其可从网络上下载(Download)的应用程序或游戏中，包含了可以控制用户的计算机系统的程序，可能造成用户的系统被破坏甚至瘫痪。
后门：后门则是一个模块的秘密入口。在程序开发期间，后门的存在是为了便于测试、更改和增强模块的功能。当然，程序员一般不会把后门记入软件的说明文档，因此用户通常无法了解后门的存在。
按照正常操作程序，在软件交付用户之前，程序员应该去掉软件模块中的后门，但是，由于程序员的疏忽，或者故意将其留在程序中以便日后可以对此程序进行隐蔽的访问，方便测试或维护已完成的程序等种种原因，实际上并未去掉。这样，后门就可能被程序的作者所秘密使用，也可能被少数别有用心的人用穷举搜索法发现利用。

十、会话劫持

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。分为：中间人攻击和注射式攻击。处理会话劫持问题有两种机制：预防和检测。预防措施包括限制入网的连接和设置你的网络拒绝假冒本地地址从互联网上发来的数据包。
加密也是有帮助的。如果你必须要允许来自可信赖的主机的外部连接，你可以使用 Kerberos 或者 IPsec 工具。使用更安全的协议，FTP 和 Telnet 协议是最容易受到攻击的。SSH 是一种很好的替代方法。SSH 在本地和远程主机之间建立一个

加密的频道。同时，有些网站也用 Https 代替 Http 协议。Https 在本地和远程主机之间建立一个加密的频道。通过使用 IDS 或者 IPS 系统能够改善检测。交换机、SSH 等协议和更随机的初始序列号的使用会让会话劫持更加困难。此外，网络管理员不应该麻痹大意，有一种安全感。虽然会话劫持不像以前那样容易了，但是，会话劫持仍是一种潜在的威胁。允许某人以经过身份识别的身份连接到你的一个系统的网络攻击是需要认真对付的。

十一、ARP 欺骗

ARP 欺骗（英语：ARP spoofing），是针对以太网地址解析协议（ARP）的一种攻击技术。此种攻击可让攻击者获取局域网上的数据包甚至可篡改数据包，且可让网络上特定电脑或所有电脑无法正常连接。

1）什么是 ARP 欺骗？在局域网中，黑客经过收到 ARP Request 广播包，能够偷听到其它节点的（IP, MAC）地址，黑客就伪装为 A，告诉 B（受害者）一个假地址，使得 B 在发送给 A 的数据包都被黑客截取，而 B 浑然不知。

2）为什么黑客能够进行 ARP 欺骗？ ARP 是个早期的网络协议，RFC826 在 1980 就出版了。早期的互联网采取的是信任模式，在科研、大学内部使用，追求功能、速度，没考虑网络安全。尤其以太网的洪泛特点，能够很方便的用来查询。但这也为日后的黑客开了方便之门。黑客只要在局域网内阅读送上门来的 ARP Request 就能偷听到网内所有的（IP, MAC)地址。而节点收到 ARP Reply 时，也不会质疑。黑客很容易冒充他人

3）能够防止欺骗吗？不能。但这种伤害的伤害已经很小。因为局域网的工作环境有了改变， 服务器通常不会和终端主机在同一个局域网。但如果黑客对主机发送 ARP 欺骗分组，向它伪造了网关的地址，或对网关发送 ARP 欺骗分组，向网关伪造了主机的 mac 地址，则主机也无法正常和因特网上服务器交流。

十二、个人计算机面临的威胁有哪些？我们有哪些对策？

威胁 1.计算机病毒。种类繁多的计算机病毒，利用自身的“传染”能力，严重破坏数据资源，影响计算机使用功能，甚至导致计算机系统瘫痪。2.内部用户非恶意或恶意的非法操作。3.网络外部的黑客。这种人为的恶意攻击是计算机网络所面临的最大威胁，黑客一旦非法入侵资源共享广泛的政治、军事、经济和科学等领域，盗用、暴露和篡改大量在网络中存储和传输的数据，其造成的损失是无法估量的。

对策：1.要加强人员安全培训，制定网络操作和系统维护规程、建立健全应急预案，规范安全管理，同时利用各种技术手段加大自动化管理力度。2.保护计算机实体安全。采取防火、防水、防尘、防震、防静电等措施保证计算机场地符合安全要求，全方位，多角度地保障实体设备正常工作。3.保护计算机系统的安全。增强防病毒观念，对于不可预知的突发性计算机系统灾难，系统的备份与恢复也十分关键。