网络安全期末复习总结
(from sotawhu)
+
cjs PPT后习题

网络安全复习

大家搜集来的往年资料

💡 关于每一章节知识点需要**精简索引**还是**内容丰富**的问题，参照罗敏说考试不超过ppt但不代表ppt能直接抄。所以我认为可能会涉及到**对于各种攻击的理解**，因此这里**放弃了精简索引**的整理方式，这里我会在课外搜集一些东西方便对于知识点的理解，因此整理完内容可能会偏多，以便考试的时候至少能够有话去瞎扯。

💡 本文档最终的目标是：

- [ ] 各章节知识点，书本04年写的，很多东西很老旧。这里通过整理网上的资料达到对ppt提到的重点知识点理解，内容偏多会比较繁杂。
- [ ] 完成ppt习题、课后习题的整理，这一块可以简单的用精简索引的方式，因为大概率不会有太多原题，这些习题的作用可能就是帮助对于之前整理知识点的利用和加深知识点的理解。

💡 开启了table of content，因为客户端notion没有侧边outline快速索引的功能，因此加入目录方便索引。建议使用chrome网页版notion，下载**notion boost**插件，打开其中的show outline功能。

TODO LIST 区域

若某人要完成某个未完成的todolist，则在某一个todo后面加入自己名字，防止多人做太多重复工作。比如pya在完成第一章 概述的知识点，则把名字放后面，完成后打勾即可。

PPT

- [x] ~~第一章 概述，彭雨昂~~
- [ ] 第二章ppt额外知识点
- [ ] 第三章cjs+lm 标红部分详细内容

- [x] ~~双/三网物理隔离~~
- [x] ~~第七章 欺骗攻击知识点~~
- [x] ~~第十章防火墙技术ppt知识点整理~~
- [x] ~~第十一章入侵检测技术~~

cjs思考题

- [x] ~~第1章思考题~~
- [x] ~~第2章思考题~~
- [x] ~~第3章思考题~~
- [x] ~~第4章思考题~~
- [x] ~~第5章思考题~~
- [x] ~~cjs无，lm第6章思考题~~
- [x] ~~第7章思考题~~
- [x] ~~cjs无，lm第8章思考题~~
- [x] ~~第9章思考题~~
- [x] ~~第10章思考题(openwhu原题)~~
- [x] ~~第11章思考题(无)~~
- [x] ~~第12章思考题(openwhu原题)~~
- [x] ~~cjs无，lm第16章思考题~~

往年试卷

- [ ] 20-21
- [ ] 18-19

第一章 概述

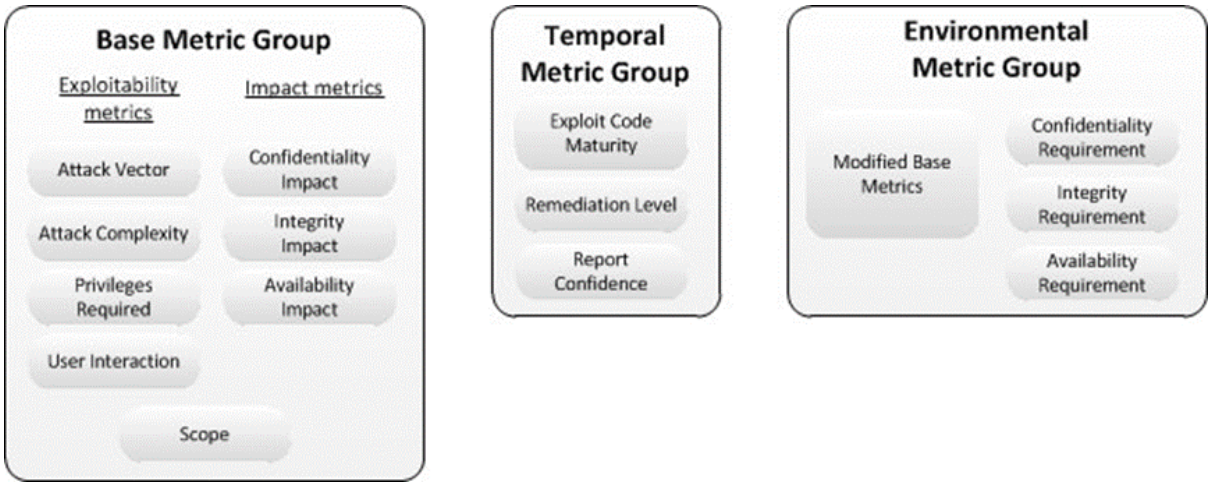
——一些重点的补充

CVSS评分表

CVSS（通用漏洞评分系统），作用是了解CVE漏洞的评分机制，好在以后出现了漏洞的时候利用CVSS标准对该漏洞的实际影响进行评估，从而指导进行下一步操作。

度量指标

CVSS由三个度量组：「基础-Base」，「时间-Temporal」和「环境-Environmental」组成，每一组又由一些度量指标组成，如下：



基础度量组反映了一个漏洞的固有特征——它不随着时间和用户环境的变化而变化。它由两组指标组成：可利用指标和影响指标。包括攻击向量，攻击复杂性，所需权限，用户交互，范围，机密性影响，完整性影响，可用性影响。

可利用指标反映了漏洞可以被利用的简单程度和技术手段。也就是说，它们代表了漏洞易受利用的特征，我们把它称为脆弱的部分。另一方面，**影响指标**反映了成功利用该漏洞可以导致的直接结果，以及受该影响产生的后续结果，我们将其正式称为受影响的组件。

虽然脆弱的组件通常是一个软件应用程序、模块、驱动程序等等(甚至可能是一个硬件设备)，但受影响的组件可能是一个软件应用程序、一个硬件设备或一个网络资源。衡量一个脆弱组件之外的弱点的潜在影响，是CVSS v3.0的一个关键特性。

BaseScore=IF(Scope="C",ROUNDUP(MIN(1.08*(Exp+Impact),10),1),ROUNDUP(MIN(Exp+Impact,10),1))

Impact = IF(Scope="C",7.52*(ISCbase-0.029)-3.25*((ISCbase-0.02)^15),6.42*ISCbase)

其中：ISCbase = 1 - ((1-C) * (1-I) * (1-A)) ； Exp = 8.22 * AV * AC * PR * UI

时间度量组反映了一个可能随时间而变化的漏洞的特征，但是不跨用户环境。例如，一个易于使用的漏洞利用工具包的出现会增加CVSS分数，而一个官方补丁的创建将会减少它。包括可利用性，补救水平，报告信心。

Temporal = Roundup(BaseScore*E*RL*RC）

环境度量组代表了一个与某个特定用户环境相关且独特的漏洞的特征。这些度量标准允许分析人员合并安全控制，这些控制可以减轻任何后果，也可以根据她的业务风险促进或降低一个脆弱系统的重要性。1包括攻击向量，攻击复杂性，所需权限，用户交互，范围，机密性影响，完整性影响，可用性影响，机密性要求，完整性要求，可用性要求。

Environmental = IF(Scope="C", Roundup(Roundup(Min(1.08*(M.Impact + M.E),10),1),1), Roundup(Min((M.Impact + M.Exp) ,10),1))

M.Impact = IF(Scope="C", 7.52*(M.ISC− 0.029)−3.25*(M.ISC-0.02)^15, 6.42*M.ISC)

其中：M.ISC = Min(1-((1-M.C*CR)*(1-M.I*IR)*(1-M.IA*AR)), 0.915) ； M.Exp = 8.22 * M.AV * M.AC * M.PR * M.UI

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）。

（lk补充）

（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。
P2DR模型是在整体安全策略的控制和指导下，在综合运用防护工具（如防火墙、操作系统身份认真、加密等）的同时，利用检测工具（如漏洞评估、入侵检测等）了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全。
该理论最基本的的原理就是，认为信息相关的所有活动，不管是攻击行为、防护行

为、检测行为和响应行为都要消耗时间。因此可以用时间来衡量一个体系的安全性和安全能力。

P2DR模型总结：及时的检测和响应就是安全；及时的检测和恢复就是安全。

P2DR缺点：忽略了内在的变化因素，如人员的流动、人员的素质和策略贯彻的不稳定性。实际上，安全问题牵涉面很广，除了涉及到的防护、检测和响应，系统本身的安全“免疫力”增强、系统和整个网络的优化以及人员这个在系统中最重要角色的素质的提升，都是该安全系统没有考虑到的问题。

第二章 网络攻击行径分析

Teardrop攻击

攻击原理

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。

它利用的是系统在实现时的一个错误，即攻击特定的IP协议栈实现片段重组代码存在的缺陷。当网络分组穿越不同的网络时，有时候需要根据网络最大传输单元MTU来把它们分割成较小的片，早期的Linux系统在处理IP分片重组问题时，尽管对片段是否过长进行检查，但对过短的片段却没有进行验证，所以导致了泪滴形式的攻击，会造成系统的死机或重新启动

防范措施

防御泪滴攻击的最好办法是**升级服务包软件**，如下载操作系统补丁或升级操作系统等。另外，在设置防火墙时对分组**进行重组而不进行转发**，也可以防止这种攻击

第三章 网络侦察知识点

第四章 拒绝服务知识点

拒绝服务攻击的概念

定义、攻击思想和方法 、分类（PPT+课本）

从某种程度上可以说，DoS攻击永远不会消失。而且从技术上，目前**还没有根本的解决办法**。

同步包风暴 SYN Flooding

攻击原理【课本P63】

黑客通常通过伪造的源IP地址或端口，向服务器发送大量的SYN报文，请求建立TCP连接。由于源IP地址或端口是伪造的，服务器发送的SYN-ACK报文永远不会被真实的客户端接收和回应。极少数情况下，黑客也会使用真实源IP地址，但他们只是通过攻击工具发送海量SYN报文，工具并不会响应来自服务器SYN-ACK报文。无论如何，服务器都接收不到ACK报文，产生了大量的半连接。此时服务器需要维持一张巨大的等待列表，不停地重试发送SYN-ACK报文，同时大量的资源无法释放。当服务器被这些恶意的半连接占满时，就不会再响应新的SYN报文，从而导致正常的用户无法建立TCP连接。

防范措施【课本P66】

优化系统配置
优化路由器配置
使用防火墙
主动监视
完善基础设施

Smurf攻击

攻击原理

课本P67

发送伪装的ICMP数据包，目的地址设为某个网络的广播地址，源地址设为要攻击的目的主机，使所有收到此ICMP数据包的主机都将对目的主机发出一个回应，使被攻击主机在某一段时间内收到 成千上万的数据包。

ping 风暴 课本P68

防范措施

（从三个方面回答，课本P69）

被攻击者利用进行攻击的中间网络应采取的措施

被攻击的目标应该采取的措施

攻击者攻击实际发起的网络应采取的措施

利用处理程序错误【课本P69】

- **ping of death**

防范：现在所有的标准TCP/IP实现都已实现对付超大尺寸的包，并且大多数防火墙能够自动过滤这些攻击，包括：从windows98之后的windows,NT(service pack 3之后)，linux、Solaris、和Mac OS都具有抵抗一般ping of death攻击的能力。此外，对防火墙进行配置，阻断ICMP以及任何未知协议，都能防止此类攻击。

- **Teardrop**

检测方法：对接收到的分片数据包进行分析，计算数据包的片偏移量（Offset）是否有误。

防范：网络安全设备将接收到的分片报文先放入缓存中，并根据源IP地址和目的IP地址对报文进行分组，源IP地址和目的IP地址均相同的报文归入同一组，然后对每组IP报文的相关分片信息进行检查，丢弃分片信息存在错误的报文。为了防止缓存溢出，当缓存快要存满时，直接丢弃后续分片报文。

添加系统补丁程序，丢弃收到的病态分片数据包并对这种攻击进行审计。尽可能采用最新的操作系统，或者在防火墙上设置分段重组功能，由防火墙先接收到同一原包中的所有拆分数据包，然后完成重组工作，而不是直接转发。

- **winnuke**

检测方法：检测数据包目的端口是否为139，并且检查TCP-URG位是否被设置

防范：此类攻击是由于利用软件开发过程中对某种特定类型的报文或请求没有处理，导致软件遇到这类型报文时运行出现异常，软件崩溃甚至系统崩溃。防范此类攻击的方法就是**升级系统或给系统打补丁**，也可以删除NetBIOS协议或关闭137、138、139端口。

- Land

检测方法:判断网络数据包的源地址和目标地址是否相同
防范:适当配置防火墙设备或路由器的过滤规则就可以防止这种攻击行为(一般是丢弃该数据包，记录事件发生的时间、源主机和目标主机的MAC地址以及IP地址并对这种攻击进行审计)

第七章 欺骗攻击知识点

DNS欺骗攻击

攻击原理

DNS 欺骗攻击，是**攻击者冒充域名服务器**，把用户查询的域名地址更换成攻击者的 IP 地址，然后攻击者将自己的主页取代用户的主页，这样访问用户主页的时候只会显示攻击者的主页，这就是DNS欺骗的原理。DNS欺骗并不是“黑掉”了真正的服务器的主页，而是替换成攻击者的主页，将真正的服务器主页隐藏起来无法访问而已。

DNS欺骗的实现，是利用了DNS协议设计时的一个安全缺陷：在一个局域网内，攻击者首先**使用ARP欺骗，使目标主机的所有网络流量都通过攻击者的主机**。之后攻击者通过**嗅探目标主机发出的DNS请求分组**，分析数据分组的ID和端口号后，向目标主机发送**攻击者构造好的 DNS 返回分组**，目标主机收到 DNS 应答后，发现 ID和端口号全部正确，即把返回的数据分组中的域名和对应的IP地址保存进DNS缓存，而后到达的真实DNS应答分组则被丢弃。

防范措施

首先，DNS攻击存在一定的局限性：

- 攻击者不能替换缓存中已存在的记录，这也就是我们为什么要在实验开始时刷新受害机的DNS缓存的原因
- DNS服务器缓存时间的刷新（每隔一段时间电脑中DNS缓存会重新刷新）

防范措施：

- 在DNS欺骗之前一般需要使用ARP攻击来配合实现，因此，首先可以做好**对ARP欺骗的防御工作**，如设置静态ARP映射、安装ARP防火墙等。
- 使用**代理服务器**进行网络通信，本地主机对通过代理服务器的所有流量都可以加密，包括DNS信息。
- 尽量访问带有https标识的站点，带有https标识的站点因为有SSL证书，难以伪造篡改，如果浏览器左上角的https为红色叉号，需要提高警惕。
- 使用DNSCrypt等工具，DNSCrypt是OpenDNS发布的加密DNS工具，可加密DNS流量，阻止常见的 DNS 攻击，如重放攻击、观察攻击、时序攻击、中间人攻击和解析伪造攻击。DNSCrypt支持Mac OS和Windows，是防止DNS污染的绝佳工具，如图5所示。DNSCrypt使用类似于SSL的加密连接向DNS服务器拉取解析，所以能够有效对抗DNS劫持、DNS污染以及中间人攻击。

- 关闭DNS服务器的递归功能（这个我没懂为什么，有懂的可以点击这一个block左边六饼的comment留言）
- 使用最新版本的DNS服务器软件，及时安装补丁
- 保护内网设备，DNS攻击一般都是从内网中发起的，如果你的内网设备很安全，那么也就不存在被感染的风险

缓冲区溢出攻击

未写****攻击原理

DNS 欺骗攻击，是**攻击者冒充域名服务器**，把用户查询的域名地址更换成攻击者的 IP 地址，然后攻击者将自己的主页取代用户的主页，这样访问用户主页的时候只会显示攻击者的主页，这就是DNS欺骗的原理。DNS欺骗并不是“黑掉”了真正的服务器的主页，而是替换成攻击者的主页，将真正的服务器主页隐藏起来无法访问而已。

DNS欺骗的实现，是利用了DNS协议设计时的一个安全缺陷：在一个局域网内，攻击者首先**使用ARP欺骗，使目标主机的所有网络流量都通过攻击者的主机**。之后攻击者通过**嗅探目标主机发出的DNS请求分组**，分析数据分组的ID和端口号后，向目标主机发送**攻击者构造好的 DNS 返回分组**，目标主机收到 DNS 应答后，发现 ID和端口号全部正确，即把返回的数据分组中的域名和对应的IP地址保存进DNS缓存，而后到达的真实DNS应答分组则被丢弃。

未写****防范措施

首先，DNS攻击存在一定的局限性：

- 攻击者不能替换缓存中已存在的记录，这也就是我们为什么要在实验开始时刷新受害机的DNS缓存的原因
- DNS服务器缓存时间的刷新（每隔一段时间电脑中DNS缓存会重新刷新）

防范措施：

- 在DNS欺骗之前一般需要使用ARP攻击来配合实现，因此，首先可以做好**对ARP欺骗的防御工作**，如设置静态ARP映射、安装ARP防火墙等。
- 使用**代理服务器**进行网络通信，本地主机对通过代理服务器的所有流量都可以加密，包括DNS信息。
- 尽量访问带有https标识的站点，带有https标识的站点因为有SSL证书，难以伪造篡改，如果浏览器左上角的https为红色叉号，需要提高警惕。
- 使用DNSCrypt等工具，DNSCrypt是OpenDNS发布的加密DNS工具，可加密 DNS流量，阻止常见的 DNS 攻击，如重放攻击、观察攻击、时序攻击、中间人

攻击和解析伪造攻击。DNSCrypt支持Mac OS和Windows，是防止DNS污染的绝佳工具，如图5所示。DNSCrypt使用类似于SSL的加密连接向DNS服务器拉取解析，所以能够有效对抗DNS劫持、DNS污染以及中间人攻击。

- 关闭DNS服务器的递归功能（这个我没懂为什么，有懂的可以点击这一个block左边六饼的comment留言）
- 使用最新版本的DNS服务器软件，及时安装补丁
- 保护内网设备，DNS攻击一般都是从内网中发起的，如果你的内网设备很安全，那么也就不存在被感染的风险

DNS欺骗攻击

攻击原理

DNS 欺骗攻击，是**攻击者冒充域名服务器**，把用户查询的域名地址更换成攻击者的 IP 地址，然后攻击者将自己的主页取代用户的主页，这样访问用户主页的时候只会显示攻击者的主页，这就是DNS欺骗的原理。DNS欺骗并不是“黑掉”了真正的服务器的主页，而是替换成攻击者的主页，将真正的服务器主页隐藏起来无法访问而已。

DNS欺骗的实现，是利用了DNS协议设计时的一个安全缺陷：在一个局域网内，攻击者首先**使用ARP欺骗，使目标主机的所有网络流量都通过攻击者的主机**。之后攻击者通过**嗅探目标主机发出的DNS请求分组**，分析数据分组的ID和端口号后，向目标主机发送**攻击者构造好的 DNS 返回分组**，目标主机收到 DNS 应答后，发现 ID和端口号全部正确，即把返回的数据分组中的域名和对应的IP地址保存进DNS缓存，而后到达的真实DNS应答分组则被丢弃。

防范措施

首先，DNS攻击存在一定的局限性：

- 攻击者不能替换缓存中已存在的记录，这也就是我们为什么要在实验开始时刷新受害机的DNS缓存的原因
- DNS服务器缓存时间的刷新（每隔一段时间电脑中DNS缓存会重新刷新）

防范措施：

- 在DNS欺骗之前一般需要使用ARP攻击来配合实现，因此，首先可以做好**对ARP欺骗的防御工作**，如设置静态ARP映射、安装ARP防火墙等。
- 使用**代理服务器**进行网络通信，本地主机对通过代理服务器的所有流量都可以加密，包括DNS信息。

- 尽量访问带有https标识的站点，带有https标识的站点因为有SSL证书，难以伪造篡改，如果浏览器左上角的https为红色叉号，需要提高警惕。
- 使用DNSCrypt等工具，DNSCrypt是OpenDNS发布的加密DNS工具，可加密DNS流量，阻止常见的 DNS 攻击，如重放攻击、观察攻击、时序攻击、中间人攻击和解析伪造攻击。DNSCrypt支持Mac OS和Windows，是防止DNS污染的绝佳工具，如图5所示。DNSCrypt使用类似于SSL的加密连接向DNS服务器拉取解析，所以能够有效对抗DNS劫持、DNS污染以及中间人攻击。
- 关闭DNS服务器的递归功能（这个我没懂为什么，有懂的可以点击这一个block左边六饼的comment留言）
- 使用最新版本的DNS服务器软件，及时安装补丁
- 保护内网设备，DNS攻击一般都是从内网中发起的，如果你的内网设备很安全，那么也就不存在被感染的风险

Email欺骗攻击

攻击原理

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）或在貌似正常的附件中加载病毒或其他木马程序。

Email欺骗实现步骤：

- 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

防范措施

- 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

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。

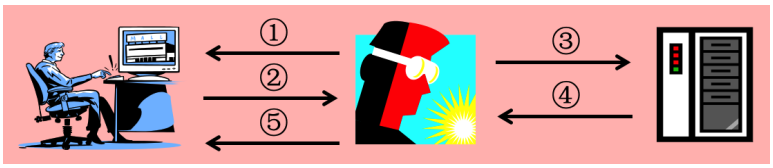
攻击者能够监视被攻击者的网络信息，记录他们访问的网页和内容。当被攻击者填完一个表单并发送后，这些数据将被传送到Web服务器，Web服务器将返回必要的信息，但不幸的是，攻击者完全可以截获并使用这些信息。在得到必要的数据后，攻击者可以通过修改受害者和Web服务器两方任何一方数据，来进行破坏活动。攻击者可以修改受害者的确认数据，攻击者还可以修改Web服务器返回的数据。

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“。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。

Web欺骗的形式：

- 使用相似的域名
- 改写URL
- 劫持Web会话

改写URL的工作流程：



- 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

劫持Web会话 会话劫持（Session hijacking），这是一种通过获取用户Session ID后，使用该Session ID登录目标账号的攻击方法，此时攻击者实际上是使用了目标账户的有效Session。会话劫持的第一步是取得一个合法的会话标识来伪装成合法用户，因此需要保证会话标识不被泄漏。

- 目标用户需要先登录站点；
- 登录成功后，该用户会得到站点提供的一个会话标识SessionID；
- **攻击者通过某种攻击手段捕获Session ID；（攻击的要点）**
- 攻击者通过捕获到的Session ID访问站点即可获得目标用户合法会话。

HTTP协议不支持会话(无状态)，Web会话如何实现？（ppt上提到Cookie、用url记录会话、用表单中的隐藏元素记录会话；目前有三种广泛使用的在Web环境中 维护会话\传递Session ID 的方法：URL参数，隐藏域和Cookie。）

- 基于 server 端 session 的管理方式
- cookie-base 的管理方式
- token-base 的管理方式

Web Session 是建立在 HTTP 层之上的服务管理机制，在实现 Session 机制时，必然会用到 HTTP 的某些特性，比如 cookie， 当然也可以实现不依赖于 cookie 的 Session 机制，尤其是 cookie 有可能会被人为的禁止；另一种技术是 URL 重写技术，就是把 session id 直接附加在 URL 路径的后面。

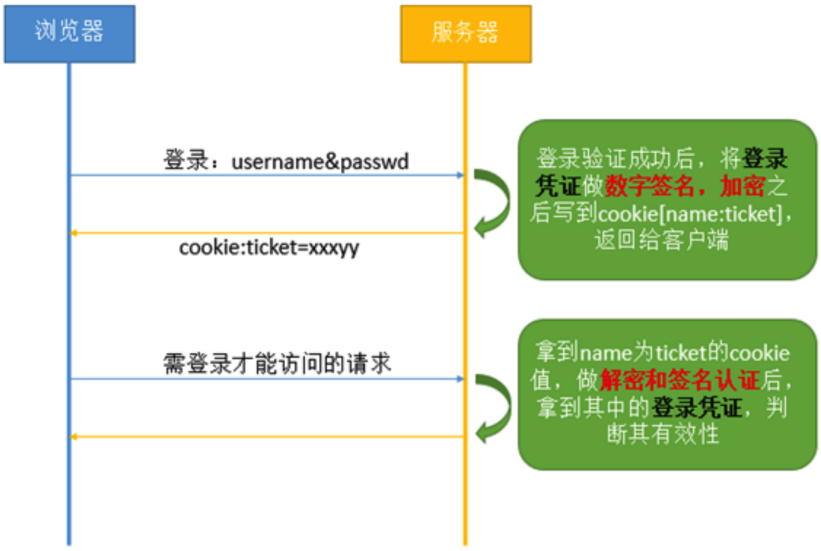
Cookie 由于前一种方式（基于 server 端 session 的管理方式）会增加服务器的负担和架构的复杂性，所以后来就有人想出直接把用户的登录凭证直接存到客户端的方案，当用户登录成功之后，把登录凭证写到cookie里面，并给cookie设置有效期，后续请求直接验证存有登录凭证的cookie是否存在以及凭证是否有效，即可判断用户的登录状态。使用它来实现会话管理的整体流程如下：

1）用户发起登录请求，服务端根据传入的用户密码之类的身份信息，验证用户是否满足登录条件，如果满足，就根据用户信息创建一个登录凭证，这个登录凭证简单来说就是一个对象，最简单的形式可以只包含用户id，凭证创建时间和过期时间三个值。

2）服务端把上一步创建好的登录凭证，先对它做数字签名，然后再用对称加密算法做加密处理，将签名、加密后的字串，写入cookie。cookie的名字必须固定（如ticket），因为后面再获取的时候，还得根据这个名字来获取cookie值。这一步添加数字签名的目的是防止登录凭证里的信息被篡改，因为一旦信息被篡改，那么下一步做签名验证的时候肯定会失败。做加密的目的，是防止cookie被别人截取的时候，无法轻易读到其中的用户信息。

3）用户登录后发起后续请求，服务端根据上一步存登录凭证的cookie名字，获取到相关的cookie值。然后先做解密处理，再做数字签名的认证，如果这两步都失败，说明这个登录凭证非法；如果这两步成功，接着就可以拿到原始存入的登录凭证了。然后

用这个凭证的过期时间和当前时间做对比，判断凭证是否过期，如果过期，就需要用户再重新登录；如果未过期，则允许请求继续。



防范措施

防范改写URL手段：

- 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。

防范劫持Web会话

目前有三种广泛使用的在Web环境中维护会话（传递Session ID）的方法：URL参数，隐藏域和Cookie。其中每一种都各有利弊，Cookie已经被证明是三种方法中最方便最安全的。从安全的观点，如果不是全部也是绝大多数针对基于Cookie的会话管理机制的攻击对于URL或是隐藏域机制同样适用，但是反过来却不一定，这就让Cookie成为从安全考虑的最佳选择。

1、 更改Session名称。PHP中Session的默认名称是PHPSESSID，此变量会保存在Cookie中，如果攻击者不分析站点，就不能猜到Session名称，阻挡部分攻击。

2、 关闭透明化Session ID。透明化Session ID指当浏览器中的Http请求没有使用Cookie来存放Session ID时，Session ID则使用URL来传递。

3、 设置HttpOnly。通过设置Cookie的HttpOnly为true，可以防止客户端脚本访问这个Cookie，从而有效的防止XSS攻击。

4、 关闭所有phpinfo类dump request信息的页面。

5、验证HTTP头部信息

6、养成显式注销的习惯

7、使用长的会话ID

IP欺骗攻击

攻击原理

IP 欺骗攻击指攻击行动产生的 IP 数据包为伪造的源 IP 地址，以便冒充其他系统或发件人的身份。这是一种黑客的攻击形式，黑客使用一台计算机上网，而借用另外一台机器的 IP 地址，从而冒充另外一台机器与服务器进行交互。

防范措施

IP 欺骗的防范，一方面需要目标设备采取更强有力的认证措施，不仅仅根据源 IP 就信任来访者，更多的需要强口令等认证手段；另一方面采用健壮的交互协议以提高伪装源 IP 的门槛。

有些高层协议拥有独特的防御方法，比如 TCP（传输控制协议）通过回复序列号来保证数据包来自于已建立的连接。由于攻击者通常收不到回复信息，因此无从得知序列号。不过有些老机器和旧系统的 TCP 序列号可以被探得。

虽然无法预防 IP 欺骗，但可以采取措施来阻止伪造数据包渗透网络。入口过滤是防范欺骗的一种极为常见的防御措施，如 BCP38（通用最佳实践文档）所示。入口过滤是一种数据包过滤形式，通常在网络边缘
设备上实施，用于检查传入的 IP 数据包并确定其源标头。如果这些数据包的源标头与其来源不匹配或者看上去很可疑，则拒绝这些数据包。一些网络还实施出口过滤，检查退出网络的 IP 数据包，确保这些数据包具有合法源标头，以防止网络内部用户使用 IP 欺骗技术发起出站恶意攻击。

（？不知道是什么）ActiveX control的安全性

- 下载ActiveX control
  - 通过数字签名来识别control的受信任程度
    - 验证数字签名，PKI中的可信任根CA
- 安装和注册ActiveX control
  - 已经在调用ActiveX control的代码了
  - 并且，它可以自己声明自己是安全的
    - 操纵注册表
- 对象的初始化
  - 创建对象，并且对对象进行初始化，ActiveX control是一个永久对象
- 对象的脚本操作
  - 通过脚本调用对象的方法
- -〉 Active Document

TCP Session Hijack

在现实生活中，比如你去市场买菜，在交完钱后你要求先去干一些别的事情，稍候再来拿菜；如果这个时候某个陌生人要求把菜拿走，卖菜的人会把菜给陌生人吗？！当然，这只是一个比喻，但这恰恰就是会话劫持的喻意。所谓会话，就是两台主机之间的一次通讯。例如你Telnet到某台主机，这就是一次Telnet会话；你浏览某个网站，这就是一次HTTP会话。而会话劫持（Session Hijack），就是结合了嗅探以及欺骗技术在内的攻击手段。例如，在一次正常的会话过程当中，攻击者作为第三方参与到其中，他可以在正常数据包中插入恶意数据，也可以在双方的会话当中进行简听，甚至可以是代替某一方主机接管会话。

我们可以把会话劫持攻击**分为两种类型：**

1）中间人攻击(Man In The Middle，简称MITM)（这也就是我们常说的“中间人攻击”，在网上讨论比较多的就是SMB会话劫持，这也是一个典型的中间人攻击。要想正

确的实施中间人攻击，攻击者首先需要**使用ARP欺骗**
或**DNS欺骗**，将会话双方的通讯流暗中改变，而这种改变对于会话双方来说是完全透明的。）

2）注射式攻击（Injection）（它不会改变会话双方的通讯流，而是在双方正常的通讯流插入恶意数据。在注射式攻击中，需要实现两种技术：1）IP欺骗；2）预测TCP序列号）

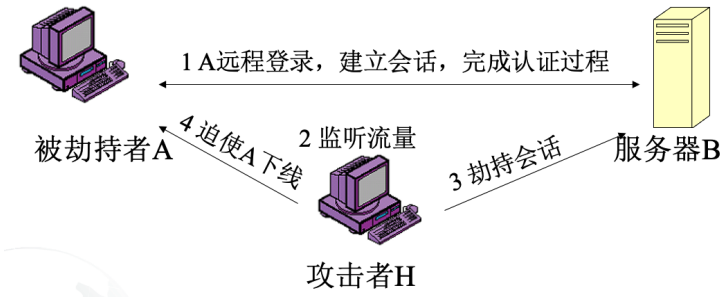
并且还可以把会话劫持攻击**分为两种形式：**

1）被动劫持，被动劫持实际上就是在后台监视双方会话的数据流，从中获得敏感数据

2）主动劫持，而主动劫持则是将会话当中的某一台主机“踢”下线，然后由攻击者取代并接管会话，这种攻击方法危害非常大，攻击者可以做很多事情

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。例如，在一次正常的会话过程当中，攻击者作为第三方参与到其中，他可以在正常数据包中插入恶意数据，也可以在双方的会话当中进行监听，甚至可以是代替某一方主机接管会话。

（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）



攻击原理

根据TCP/IP中的规定，使用TCP协议进行通讯需要提供两段序列号，TCP协议使用这两段序列号确保连接同步以及安全通讯，系统的TCP/IP协议栈依据时间或线性的产生这些值。

在通讯过程中，双方的序列号是相互依赖的，如果攻击者直接进行会话劫持，结果肯定是失败的。因为会话双方“不认识”攻击者，攻击者不能提供合法的序列号;所以，会话劫持的关键是预测正确的序列号，攻击者可以采取嗅探技术获得这些信息。

防范措施

- 不要把网络安全信任关系建立在IP基础上或者MAC基础上，（RARP同样存在欺骗的问题），理想的关系应该建立在IP+MAC基础上。
- 设置静态的MAC—>IP对应关系表，不要让主机刷新设定好的转换表。
- 停止使用ARP，将需要的ARP作为永久条目保存在对应表中。
- 建立防火墙来连续监控网络。

TCP ACK Storm

ppt很详细

Https会话劫持之SSLStrip

ppt很详细

第十章 防火墙技术知识点

（彭佳琳ver 不足再加）

- 防火墙
  - 模型-经典安全模型（书p231第一二段）
  - 概念-书p230概述的一二段；
  - 规则

    处理方式-ACCEPT，REJECT，DROP；注意REJECT和DROP的区别（ppt有）；

    基本原则-默认允许or默认拒绝

    默认拒绝安全性更好，在配置无误的情况下，通过的一定安全，但是安全的不一定能通过；

    默认允许服务性更强，在配置无误的情况下，通过的一定不安全，但是不安全的也可能通过；
  - 匹配条件

    网络层：源ip，目的ip，网络层（ICMP）以及传输层的协议号（例如标识了TCP，UDP等），匹配是否源路由数据报（指定必须经过某几个路由器的数据报）

    传输层：源端口，目的端口

应用层：各个应用不一样；比如拒绝ftp的PORT命令之类的。

信息流向：向外，向内（根据网络环境设定的）

- 分类

  实现技术（同防火墙技术方案）-数据包过滤&应用层代理（ppt我觉得够了）

  防范领域-个人防火墙&网络防火墙（ppt有提到设置的要点）

  按照实现的方式-软件&硬件（突然发现书上有，p238，包括安装在哪里和提供的服务，硬件包含一个芯片架构的名字）

- 两种技术方案的对比

  ppt上挺全的分点。

- 防火墙结构
  ppt蛮全的；

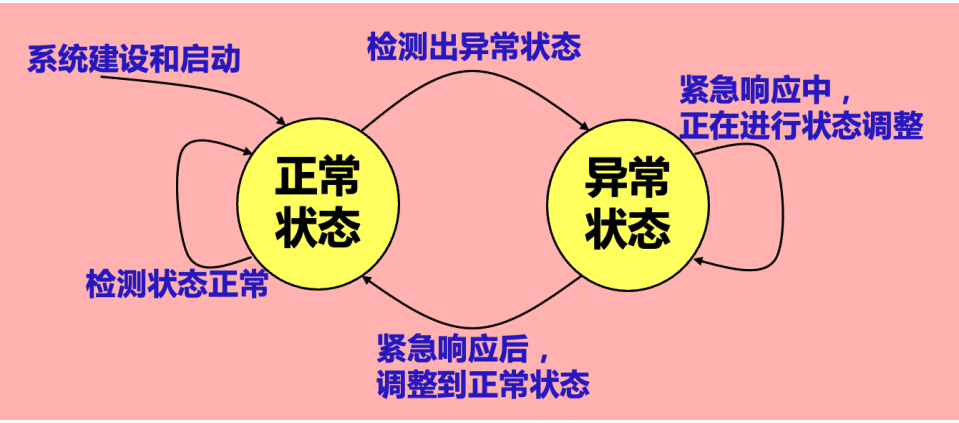
  就双重宿主主机，被屏蔽主机，被屏蔽子网三大架构

- 构建实例(最后的部分)

  ppt上有一个针对WWW，FTP，BBS，EMAIL，DNS进行配置的，不想蒙题了，对着仿写吧

第十一章 入侵检测技术

信息安全两态论



入侵检测系统是什么

入侵检测是一种动态的网络安全技术：

- 利用各种不同类型的引擎，实时地或定期地对网络中相关的数据源进行分析，依照引擎对特殊的数据或事件的认识，将其中具有威胁性的部分提取出来，并触发响应机制。
- 入侵检测的动态性反映在入侵检测的实时性、对网络环境的变化具有一定程度上的自适应性，这是以往静态安全技术无法具有的

入侵检测技术原理

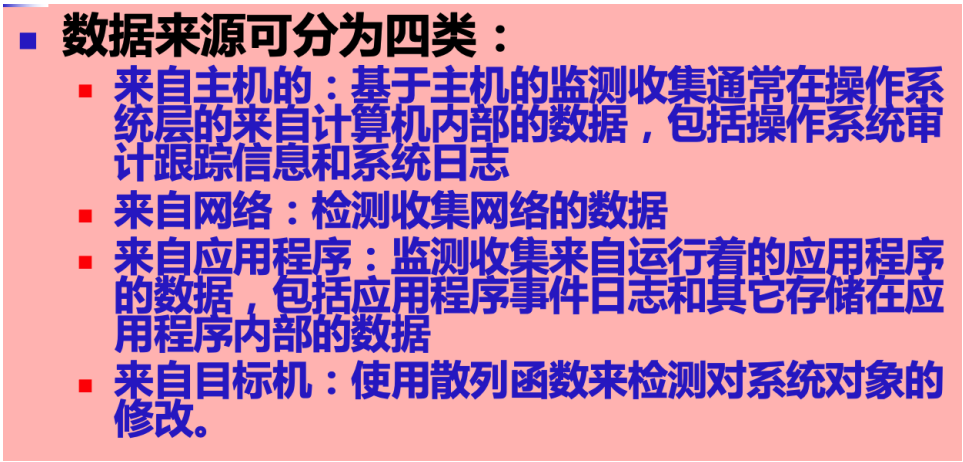
书p288

入侵分析

在一个环境中，审计信息必须与它要保护的系统分开来存储和处理

- 防止入侵者通过删除审计记录来使入侵检测系统失效
- 防止入侵者通过修改入侵检测器的结果来隐藏入侵的存在
- 要减轻操作系统执行入侵检测任务带来的操作负载

信息收集阶段，数据来源可分为四类：



入侵分析

- 误用检测
- 异常检测
- 完整性分析，往往用于事后分析

入侵检测的分类

入侵检测系统分类

- 离线和在线检测系统
- 误用检测和异常检测

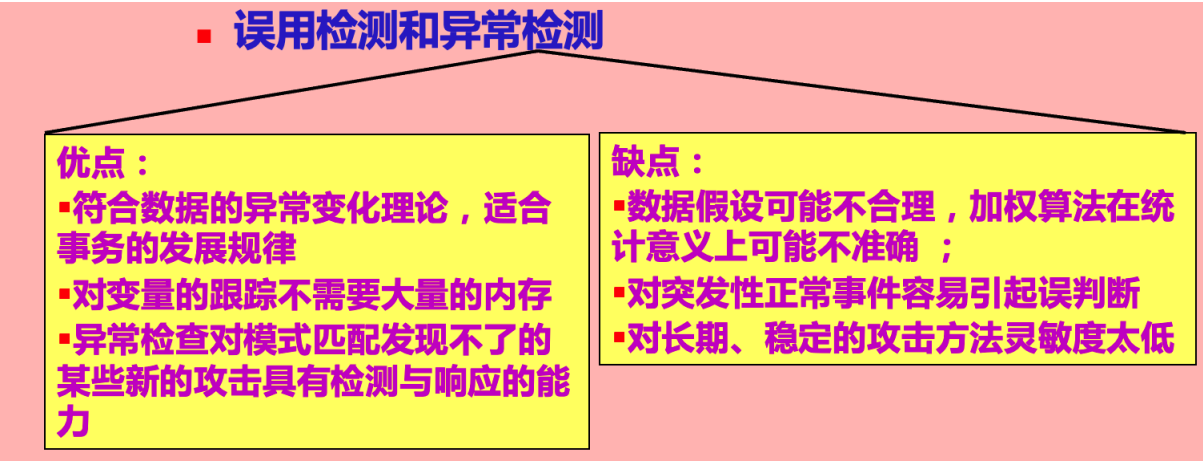
- **按照分析方法（检测方法）**
  - 异常检测模型（Anomaly Detection）:首先总结正常操作应该具有的特征（用户轮廓），当用户活动与正常行为有重大偏离时即被认为是入侵。
  - 误用检测模型（Misuse Detection）：收集非正常操作的行为特征，建立相关的特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵。

误用检测和异常检测的优缺点

- 误用检测和异常检测

优点：	缺点：
▪模式匹配具有很强的可分割性、独立性 ▪能提供更有效的入侵检测引擎 ▪模式匹配具有很强的针对性，对已知的入侵方法检测效率很高	▪可测量性与性能都和模式数据库的大小体系结构有关 ； ▪可扩展性差 ▪需要及时更新模式数据库 ▪通常不具备自学习能力 ▪攻击行为转化为模式比较困难

35

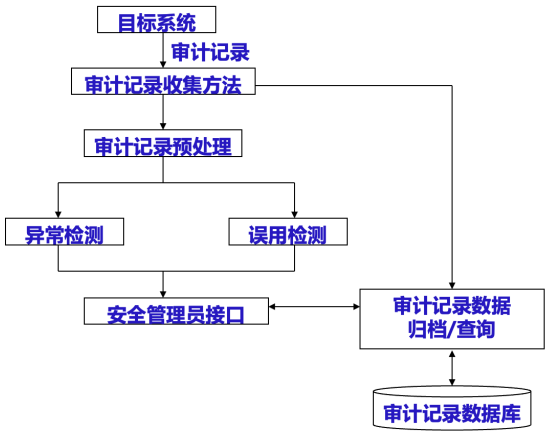


主机数据源和网络数据源的优缺点

ppt上

基于主机的入侵检测

优点和面临的问题也在ppt上



基于主机的入侵检测系统结构示意图

集中式的基于主机的入侵检测

分布式的基于主机的入侵检测

这三个的**优缺点和示意图**都在ppt上

基于网络的入侵检测系统

入侵检测问题

协同

目前DDS实现的功能是相对初级的

IDS也需要充分利用数据信息的相关性 IDS作为网络安全整体解决方案的重要部分，与其他安全设备之间应该有着紧密的联系 IDS需要一种新的系统体系来克服自身的不足并将IDs的各个功能模块与其他安全产品有机地融合起来，这就需要引入协同的概念

- 数据采集协同
- 数据分析协同
- 数据挖掘
- 响应协同

入侵检测的发展方向

IPS（入侵防御系统）

cjs思考题

第一章cjs ppt思考题

- 为什么看上去大公司会出现更多信息泄露事件
  1. 在正式公司里面，名气越小的被攻击的概率越低
  2. 产品和业务量的差距，大公司的产品和业务太多了，自然出现问题的概率更高
  3. 时代不同了，现在新的接口都会做管控，小公司小平台比较好调整。但是大公司太大了，pc时代存在的大量没有反爬的接口，许多老接口现在不维护了
- 从棱镜门事件，分析一下美国公共信息安全保障策略的特色

  IATF（Information Assurance Technical Framework） 1.0

  三个目标：

  - 准备和防范
  - 检测和响应
  - 建立牢固的根基

十个步骤

- 准备和防范

步骤1：确认关键基础设施资产以及相互依赖性，发现其脆弱性

- 检测与响应

步骤2：检测攻击和非法入侵

步骤3：开发稳健的情报和执法功能，保持法律的一致

步骤4：以实时的方式共享攻击警告和信息

步骤5：建立响应、重建和回复能力

- 建立牢固的根基

步骤6：为支持程序1－5，加强研究和开发

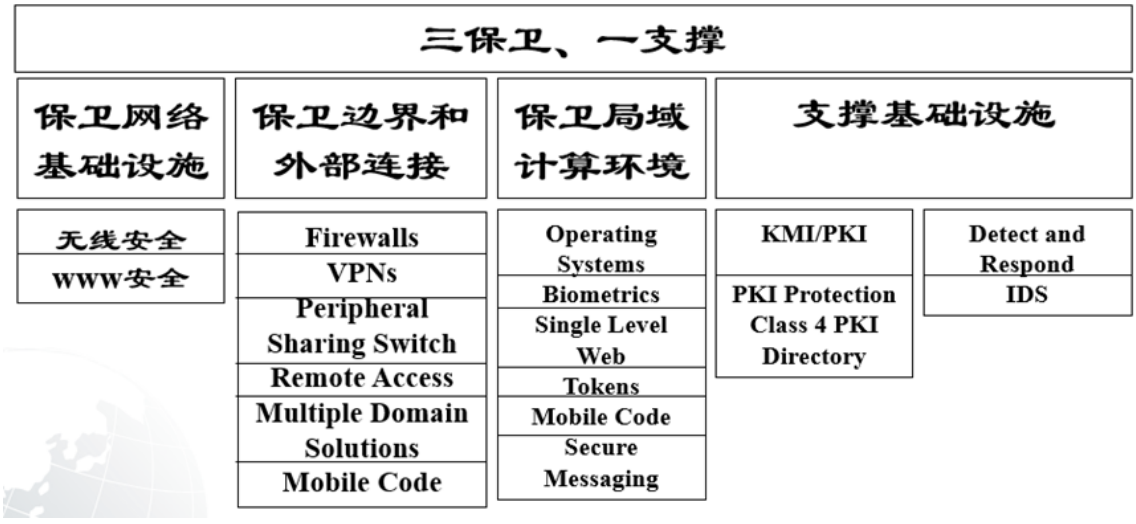
步骤7：培训和雇用足够数量的安全专家

步骤8：进行拓展，使公知晓提高计算机安全的必要性

步骤9：通过立法和拨款，支持程序1－8

步骤10：在计划的每一步骤和部分中，要完全保护公民的自由权、隐私权以及私有数据

IATF（Information Assurance Technical Framework） 3.0



第二章cjs ppt思考题

- 有哪些社工手段可以被用来获取对网络攻击有价值的信息

（这里彭佳琳觉得应该再加一个phishing；以及这里的朋友圈我不确定是算作信息手机还是社工攻击，感觉社工更像一个主动的过程，我先把phishing加进去）

1. 支付宝查询姓名

最终社工手法我想是极为常见的一种方式，它的先决条件是获取到对方电话，电话号已注册支付宝。方式很简单，只需要选择转账输入大额转账，就会弹出对方姓名，除去姓氏的验证方式，嗯，这时你可以进行简单的猜解，或进行短信伪装调查

2. 空间朋友圈查询信息

这个方式通常是使用最多的，也是最简单的，同时也是最难分析的，这一条的前提是由对方QQ或者微信且空间处于开放状态，我们对其进行信息收集时，需注意一下几种关键信息：

一是机车等票类图片信息

二是生日类信息

三是位置类信息

四是游戏分享类信息，可从游戏接近对方

五是爱好类信息，可从兴趣圈接近对方

六是对方常留言好友或情侣

3. 第三方信息收集

此类方式可称为金钱万能法，你只需找一名私家侦探划伤两三百即可查找户籍，此法唯一的问题是可能遇到骗子，所以一般情况不建议使用

4. 伪装调查

这种方式是最为实用的，成功率相对较高的方式，面对我们所需的各类信息，我们时常会缺少关键点，导致无法沿着线索向下继续查询，这时伪装调查往往会成为突破口，这里不介绍具体用什么身份，因为要视情况而定，我这里就讲几点伪装的要点

一是伪装的要素，第一印象很重要

面对各式各样的人，你想伪装的角色，一定要让你的目标第一眼就能看出你想要伪装的角色，例如伪装记者，你的胸口需要有一张假的记者证，并有录音笔笔记本正装等记者常见的装备要素

二是伪装的要素，语句用词把握细节

对于警惕性较高的人而言，你可能更需要把握细节，特别是你伪装的角色，涉及职业用语比较多的，你就需要对你的角色职业用语及一些关键的流程有所了解，

并在最快的情况下完成你的目的，但也不可急于求成，反而容易使对方心生警惕

三是伪装的细节，目的掩饰

对于你真正的目的，切不可直接表现，要先使用一些无关紧要的信息作为掩饰，如涉及更加私密的信息，最好的办法是收集与其有关联的信息进行分析或多次接触处调查，降低对方警惕性

四是伪装角色的选择

对于伪装什么角色，这个问题很重要，决定了你的成功几率，我们模拟一下以下情景

你最近想去一家牛排店，这个信息被我知道了，这个时候我伪装成牛排店员工，假装有实名抽奖活动，可抽优惠券或免单卡，我们基本可以轻易拿到你的身份信息，电话甚至家庭情况等，我们只要准备那家店的广告单，或是开设一个虚拟的网站

分析上述内容角色的选择，最好是选择目标，有需要的角色或是对方经常接触社会常见的角色，这样才更容易上手。

5. 网络钓鱼（phishing）

简单定义：网络钓鱼指的是使用精心布置的诱饵(如看起来很像来自一个真实公司或机构的E-mail以及异常相似的域名、网页)，这些诱饵是一些别有用心的人所设置，用于“钓取”用户的财政状况、信用卡详细情况和密码。钓鱼攻击使用的E-mail消息和网站看起来很像是来自一家合法的知名组织，其目的是骗取用户透露其个人、财政或计算机帐户信息。攻击者然后利用这些信息进行犯罪活动，如身分窃取、盗窃或欺诈。

常见手段：通过点击恶意电子邮件中假银行网站链接或是在浏览器的地址栏输错网站的某一个字符，都有可能误入网络骗子们精心设计的钓鱼网站，导致个人资料甚至是财物的丢失。面对层出不穷钓鱼网站，即使是高级的网络防火墙和强大的反病毒软件也无能为力。

攻击者身份伪造：诈骗者通常会将自己伪装成知名银行、在线零售商和信用卡公司等可信的品牌，因此来说，网络钓鱼的受害者往往也都是那些和电子商务有关的服务商和使用者。

- 如何搜集整理攻击相关工具
  1. 网上博客，整理好的攻击方法和攻击工具大全
  2. 技术论坛，大佬的讨论和前人的经验指引
  3. 自己进行实际操作，通过攻击的需要寻找攻击相关的工具
- 网络攻击行为经常会留下哪些痕迹

1. 网站自身日志、网站中多出的后门、被修改的磁盘文件、运营商的记录、黑客和同伙交流在社交工具上留下的痕迹
2. 系统日志、防火墙日志、数据库日志等，以及其他类似的日志，也包括网关之类的访问记录；其中对入侵者最危险的记录包含了IP地址等相关信息，所以一名合格的黑客，必须能够伪装自己的IP地址；对于网站来说，检查日志能够及时发现被入侵，所以对于网站安全人员来说要有合适的制度来检查日志；而入侵者为了避免安全人员察觉，必须能够清理可疑的日志。

- 网络攻击常用的反跟踪手段有哪些
  1. 如果知道确切IP地址，只有找相关地区的运营商，就可以确认你报装上网的地址
  2. 攻破或欺骗运营商网络，这种方式能最接近完美地隐藏自己，但难度极大
  3. 一般的来说，用网络跳板，比如在广州先将网络跳到北京，再跳到天津，再跳到上海，被攻击者记录的IP地址就是最后一跳的上海地址，极大的增加被追踪的可能性
  4. 在小咖啡馆等有无线的地方蹭网

第三章 cjs ppt思考题

- 哪里可以方便查询DNS，whois之类的信息

  DNS：使用nslookup工具，lm ppt第11和13页讲的挺细。

  whois：本身whois工具（Linux集成）就可以在线查询whois信息；一定要找一些代理跳板性质或者离线查询的工具，就有很多集成好的网站（https://www.whois.net/）和工具（Sam Spade，对于windows的操作系统，要执行whois命令需要的一个第三方的工具）

- 同样的域名，为什么我ping的ip地址和别人不同

  原因在于域名服务器实现了网络负载均衡机制。进一步说，这里常见的原因是DNS负载均衡的实现。DNS负载均衡技术是最早提出的用来解决负载平衡的技术，它的实现方式是通过DNS 服务中的名称随机的来解析，进而实现负载平衡。即同一个名字可以用于多个不相同的地址，当用户查询这个名字时，随机得到其中的一个地址。因此，不同的用户在查阅这个名字时将得到不同的地址，进一步访问不同地址的服务器，来达到负载均衡的目的。

- 连接80端口成功，一定是web服务器吗？连不通，一定没有web服务器吗？

前者：不一定，部分木马使用端（木马的client端）开启80端口，作为反弹连接的命令传输端口，绕过一些防火墙规则。

后者：首先，运行在443端口的https也算web服务提供以及8080端口是用于www代理服务的，也可以进一步连接www服务器提供web服务；其次，web服务可以开启在任意端口上，只是浏览器访问时需要连接形式为：域名：端口。

- 同一台机器可以允许两个抓包软件吗？

  可以同时运行多个抓包软件；

  - 抓包软件原理为设置网卡模式为混杂模式，接收全部的数据包并传送给上层调用进程。
  - 虽然LibCap和Wincap的驱动设计不尽相同，但是均允许多个进程设置网卡混杂模式并以计数器形式的底层实现保证混杂模式的设置互不干扰；最终实现多个抓包软件的运行。

- 跳板机对口令文件破解太慢，怎么办（摆烂了，真心不清楚）

  1、在本地进行口令文件破解

  2、使用多台跳板机进行协同口令破解

  3、根据社会工程学方法，缩小口令字典

- 哪里可以获得常用口令文件（同上）

  用户的名字、生日、电话号码、身份证号码、所居住街道的名字等

第四章cjs ppt思考题

▼ 外部用户针对网络连接发动拒绝服务攻击有哪几种模式？请举例说明。

▼ 对付分布式拒绝服务攻击的方法有哪些？举例说明。

同课后习题

第五章cjs ppt思考题

- 什么程序会发生缓冲区溢出？

  1. 根本原因：程序未检测缓冲区的边界，使得数据写入大小超出缓冲区大小以致溢出；
  2. 使用c/c++等的非类型安全编程语言编写的程序，导致对内存的直接操作；

3. 基于虚拟技术解释器模式（如JVM）类型安全编程语言的解释器本身存在的缓冲区漏洞；
4. 使用了各类不安全的函数库编写的程序；

- UNIX系统下，怎样使黑客即使成功溢出也不能获得root权限？
  1. 使得溢出后shellcode不可执行，数据段或堆栈不可执行；
  2. 使用编译保护技术，如Canary，保证程序发生溢出可以被检测到；
  3. 这里如果把Grsecurity这种高安全性的Unix衍生系统算进来，还可以结合访问控制模型，因为Grsecurity实现了一定程度上的MAC（强制访问控制）
- 在WINDOWS下的缓冲区溢出方法与UNIX下有什么不同？

  Windows系统和UNIX系统在内存空间分配上有很大不同,在溢出方法上也有很大区别。Windows系统的用户进程空间是0~2G,操作系统所占的空间为2 ~4G，事实上用户进程的加载位置为:0x00400000。这个进程的所有指令地址、数据地址和堆栈指针都会含有0,那么我们的返回地址就必然含有0。

  考虑到栈的生长方向为由低地址到高地址，同时一般使用小端序设备；windows下缓冲区溢出时需要将溢出的address部分需要放在payload的最后位置（NNNNSSSSAAAA），以保证payload字符串不会由于/x00被截断溢出。
- 想一想printf（）系列函数中有哪些可以利用来进行缓冲区溢出攻击的漏洞？

  格式化字符串漏洞
  如果输入的字符串格式由用户定制，攻击者就可以伪造任意格式串，利用*printf () 系列函数的特性就可以窥探堆栈空间的内容，超常输入可以引发传统的缓冲区溢出，或是用“%n”覆盖指针、返回地址等。

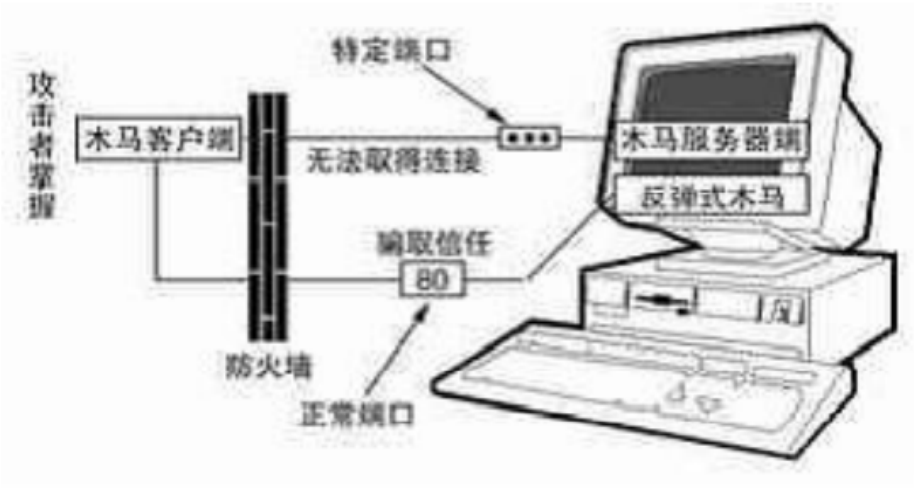
lm第六章习题

- 试说明逻辑炸弹与病毒有哪些相同点与不同点？书p109
- 为什么后来的木马制造者制造出反弹式木马，反弹式木马的工作原理是什么？画出反弹式木马的工作流程图

  为什么:书p134”然而,随着…\n于是木马设计者…反弹式木马”

  原理:书p134”它利用防火墙…其原理如图6-6所示”

  流程图:



- 嵌入式木马不同于主动型木马和反弹式木马的主要特点是什么？为什么这种木马更厉害，更不易被清除？

  特点:书p135-137(”嵌入式木马隐藏于…转发木马命令)

  为什么不易清除:从其嵌入网络程序异常性小,实现原本应有功能,dll嵌入式和网页嵌入式的特点三个角度回答

- 木马技术包括哪些，这些技术有什么特点

  自启动技术,隐藏技术,远程监控技术(书p140-p150,基本就是每一章节第一段话)

第七章cjs ppt思考题

- 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。
- 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？
- Web欺骗攻击有哪些具体形式？请简述其原理。

123对应openwhu的习题247

- 假如你负责开发、维护和管理某商业网站，面对潜在的Web欺骗攻击，你将采取哪些手段避免你的网站受到攻击

同web欺骗的对抗手段

lm第八章习题

- 简述用ASP编写的网站的常见攻击方式有哪些？

书p200-p206 8.2.3的各个章节标题

- 假如你现在要攻陷一个Windows server + IIS +ASP的网站，请描述一下你的初步想法、攻击步骤和策略

书p180攻击实例的general的表述,具体我也没设计

- 假如你现在要攻陷一个UNIX + CGI + Perl的网站，请描述一下你的初步想法、攻击步骤和策略

书p186攻击实例(不过没啥参考价值),具体没设计

- **!!!注意!!! 个人感觉二三只要提到使用代理跳板做扫描+端口扫描+操作系统版本扫描+操作系统漏洞POC验证+应用程序(IIS/CGI)漏洞POC测试+脚本注入漏洞测试(我记得ASP和PERL都有类似漏洞)**

第九章cjs ppt思考题

- 简述口令认证技术的认证方法。用哪些方法可以提高口令认证技术的安全性？
- 网络的物理隔离技术包含哪几方面？它们各自采用了什么样的技术？
- 什么是基于角色的访问控制技术？它与传统的访问控制技术有什么不同？
- 简述四种RBAC模型技术。它们各有什么特点？

分别对应openwhu的习题3 4 10 11

第10章思考题(openwhu原题)

- 防火墙规则的处理过程中，“REJECT”和“DROP“的区别是什么？
- 使用应用层代理访问外部Web站点时，会出现访问某些经典网站的相应速度较快，而其他站点相应速度较慢，原因何在？
- 如果防火墙允许周边网络上的主机访问内部网络上的任何基于TCP协议的服务，而禁止外部网络访
  问周边网络上的任何基于TCP协议的服务，给出实现的具体思路

分别对应openwhu的习题2 6 7

第12章思考题(openwhu原题)

- VPN的组成
- 比较PPTP与L2TP

- 简述IPSec中AH协议的功能
- 简述IPSec中ESP协议的功能

分别对应openwhu的习题2 8 9 10

lm第十六章习题

- 简述蜜罐的目的和蜜罐系统的工作原理
  书p414
- Honeynet与蜜罐有哪些相似和不同之处？

  具体可见书p426
  - Honeynet是专门为研究设计的高交互型蜜罐
  - 与其他大部分蜜罐不同的是：它不进行模拟，而是对真实的系统不进行修改或改动很小
  - 不是一个单独的系统而是由多个系统和多个攻击检测应用组成的网络

试卷

20-21

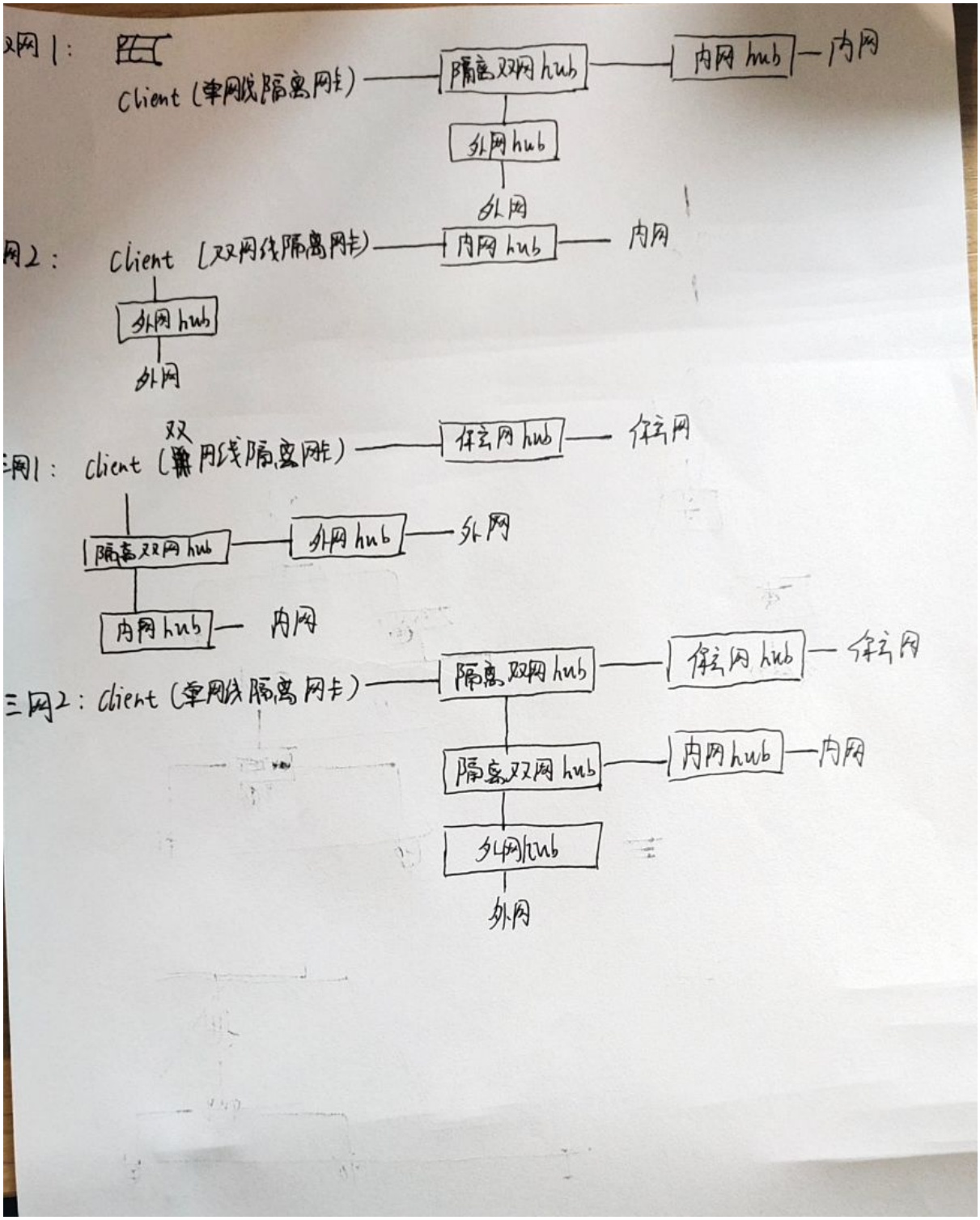
- 1. 简述DNS工作原理，面向DNS解析过程中，面临欺骗攻击的脆弱性分析。
- 2. 分别简述DOS、DDOS攻击原理，及对应技术缺陷。
- 3. 简述缓冲区溢出攻击的目标及步骤。
- 4.简述自主访问控制与强制访问控制的技术优缺点，并举例两种技术的融合应用案例。

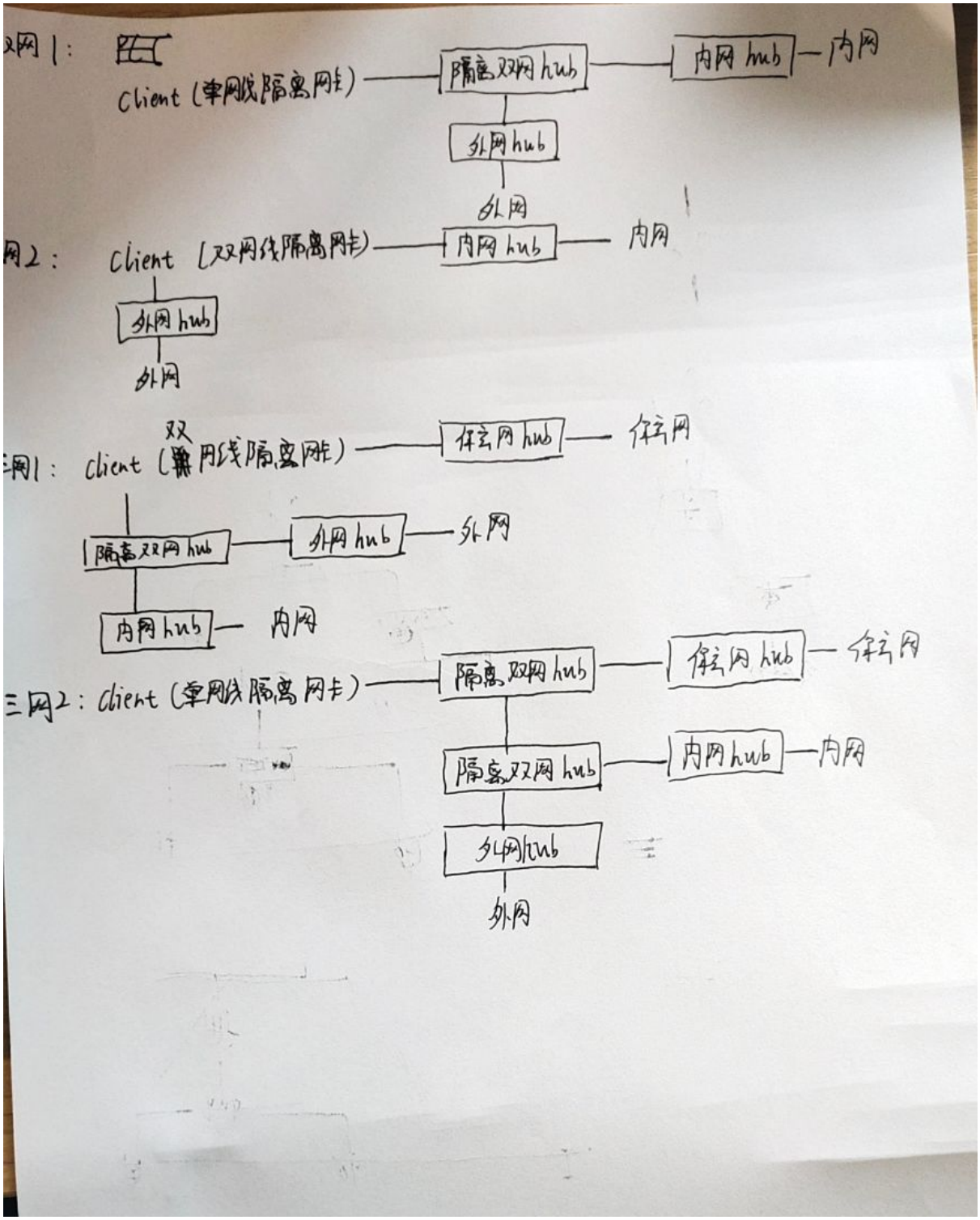
- 1. 论述: 针对大型网络场景中内部网络无交互需求原则，构建保障周边网络的防火墙体系结构。如果防火墙允许周边网络上的主机访问内部网络上的任何基于FTP协议的服务，而禁止外部网络访问周边网络上的任何基于FTP协议的服务，给出实现的思路。
- 2. 针对企业员工远程办公场景，构建基于VPN的方案设计，要求保障安全性并论述其可行性。提示：有线/无线方案均可。

18-19

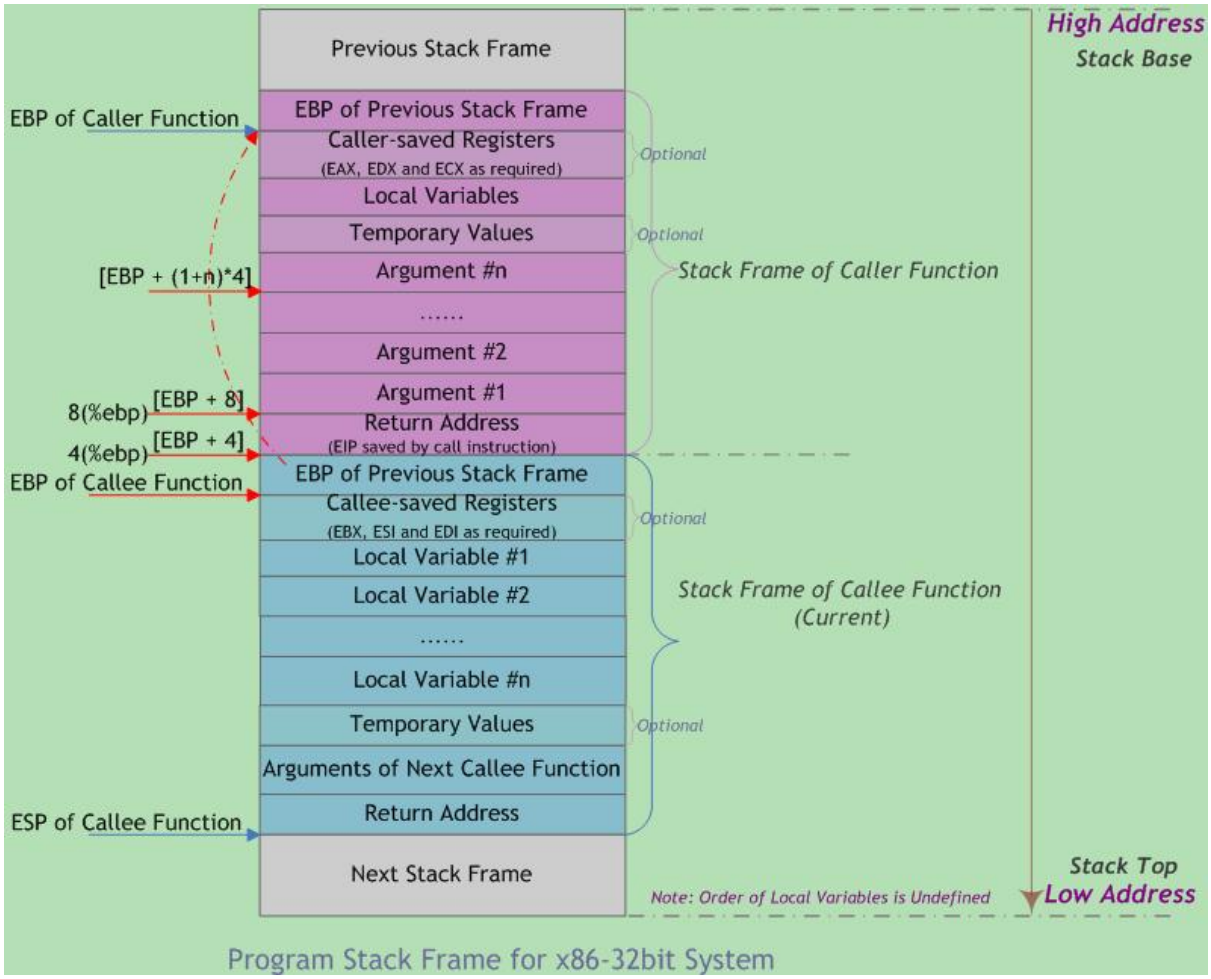
- 1．简述 TearDrop 攻击的原理及防范手段。
- 2．简述 DNS 欺骗攻击的原理及防范方法。
- 3．简述浏览器能够打开百度的主页而不能打开谷歌的主页可能的原因。
    - 防火墙过滤，本机防火墙将源地址为本机ip，目的地址为谷歌ip的数据包设为过滤，导致无法完成http请求；四个可能的过滤（本机向google的服务器请求/google对本机的响应分别被本区域防火墙/google所在区域防火墙给过滤掉，2*2=4）
    - DNS欺骗，本机提交给域名服务器的域名解析请求数据包被截获，替换为不可访问的ip
    - 某级的DNS Server故障或者被攻击，导致无法解析域名，能访问baidu是因为某个DNS Server或者本地host文件恰好存储这这个域名的页面；
    - host文件故障，导致google的ip被设置成奇怪的ip(通俗讲，本地存储的域名ip cache被替换了)
    - 攻击者籍由TCP劫持实现中间人攻击，拒绝转发google，但是转发了百度（看上去挺蠢的，而且代价挺高的，但是确实原理可行）
- 4．简述在配置成对的 VPN 网关时，交换证书的目的。
- 1．叙述反弹式木马的工作原理。
- 2．叙述交换式以太网中的监听方法。
- 3．请给出利用物理隔离网卡和隔离集线器组建双网和三网物理隔离系统的四种方案（请画图
  解答）。
- 4．叙述如何检测以太网络中进行网络监听的处于混杂模式的节点。

双/三网物理隔离


双网1：
Client（单网线隔离网卡）
隔离双网hub
内网hub
内网
外网hub
外网
网2：
Client（双网线隔离网卡）
内网hub
内网
外网hub
外网
三网1：
client（双网线隔离网卡）
保密网hub
保密网
隔离双网hub
外网hub
外网
内网hub
内网
三网2：client（单网线隔离网卡）
隔离双网hub
保密网hub
保密网
隔离双网hub
内网hub
内网
外网hub
外网



Honeynet是专门为研究设计的高交互型蜜罐



Program Stack Frame for x86-32bit System