山东大学 计算机科学与技术 学院
云计算技术 课程实验报告

学号：201900130133	**姓名：**施政良	**班级：**四班
实验题目： 云安全相关知识理解以及博客的撰写和发布		
实验学时：2	**实验日期：**2020-03-22	
实验目的：熟悉云安全相关知识点 **具体包括：云使能技术相关问题回答、个人博客的发布**		
硬件环境： 联网计算机一台		
软件环境： Windows or Linux		

实验步骤与内容：

实验步骤概述：

本次实验内容包括基本云安全的相关问题回答以及使用 hexo 发布个人博客，实验步骤为：

（1） 回答有关基本云安全的相关问题，包括威胁作用者，基本威胁的分类。**同时，作为扩展，在本实验中还了解了云安全中的其他考量因素并进行整理。**

（2） 将步骤一中问题的答案发布在实验三中搭建的个人博客上

（3） 作业地址：云计算第二次作业基本云安全问题 - shizhengliang (shizhl.github.io)

具体实验内容如下所示：

具体实验内容

1. 威胁作用者分类

（1） 定义以及基本分类

云安全威胁作用者是引发威胁的实体，能够实施攻击，主要包括：

1. 匿名攻击者(anonymous attacker)
2. 恶意服务实施者(malicious service agent)
3. 授信的攻击者(trusted attacker)

4. 恶意的内部人员(malicious insider)

（2）威胁作用者简要说明

1. **匿名攻击者(anonymous attacker)：**是云中没有权限、不被信任的云服务用户。（不是起一个假名字）
    1. 通常是一个外部软件程序，通过公网发动网络攻击。
    2. 特点：往往诉诸绕过用户账号或窃取用户证书的手段，同时使用能确保匿名性或需要大量资源才能被检举的方法。

2. **恶意服务实施者(malicious service agent)：**能截取并转发云内的网络流量。（不是提供恶意服务）
    1. 通常是带有被损害的或恶意逻辑的服务代理（或伪装成服务代理的程序）
    2. 也可能是能够远程截取并破坏消息内容的外部程序

3. **授信的攻击者(trusted attacker)：**又称恶意租户(malicious tenant)，与同一云环境中的云用户共享 IT 资源，试图利用合法的证书来把云提供者、以及与他们共享 IT 资源的云租户作为攻击目标。
    1. 特点：滥用合法证书、挪用敏感和保密信息
    2. 常见攻击方式：非法入侵认证薄弱的进程、破解加密、往电子邮件账号发送垃圾邮件、发起拒绝服务

4. **恶意的内部人员(malicious insider)：**是人为的威胁作用者，他们的行为代表云提供者，或者与之有关
    1. 通常是现任或前任雇员，或是能够访问云提供者资源范围的第三方
    2. 会带来极大的破坏可能性，因为恶意的内部人员可能拥有访问云用户 IT 资源的管理特权。

（3）威胁作用者辨析

1. 匿名攻击者是不被信任的威胁作用者，通常试图从云边界的外部进行攻击
2. 恶意服务作用者截取网络通信，试图恶意地使用或篡改数据。
3. 授信的攻击者是经过授权的云服务用户，具有合法的证书，他们会使用这些证书来访问基于云的 IT 资源或攻击其他资源。
4. 恶意的内部人员是试图滥用对云资源范围的访问特权的人。

2. 云安全威胁

（1） 云安全威胁分类

云安全威胁主要包括：

1. 流量窃听(traffic eavesdropping)
2. 恶意媒介(malicious intermediate)
3. 拒绝服务(DoS)
4. 授权不足
5. 虚拟化攻击(Virtualization attack)
6. 信任边界重叠

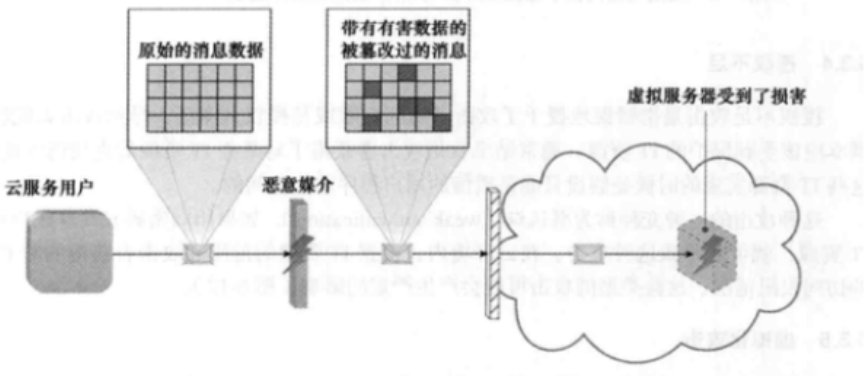
（2） 简要说明

- **流量窃听(traffic eavesdropping)**

1. 指当数据在传输到云中或在云内部传输时（通常是从云用户到云提供者），被恶意的服务作用者被动地截获，用于非法的信息收集，破坏保密性。
2. 由于这种攻击被动的性质，其更容易长时间进行而不被发现。
3. 特点：被动截取通信流量的攻击
4. 例子：美国的“上游”计划：企图通过监听海底光缆截取流经海底光缆及通信基础设施的信息，以便量子计算机出现之后，进行开发。

- **恶意媒介(malicious intermediate)**

1. 是指消息被恶意服务作用者截获并篡改，因此可能会破坏消息的保密性和完整性
2. 它还有可能在把消息转发到目的地之前插入有害数据



恶意的服务作用者截获并修改云服务用户发往位于虚拟服务器上的云服务（图中未显示）的消息。因为有害数据被打包进了消息，虚拟服务器受到了损害

· **拒绝服务(DoS)**

主要指攻击的目标是使 IT 资源过载至无法正确运行，发起形式包括：

1. 云服务上的负载由于伪造的消息或重复的通信请求不正常的增加。
2. 网络流量过载，降低了响应性，性能下降。
3. 发出多个云服务请求，每个请求都设计成消耗过量的内存和处理资源。

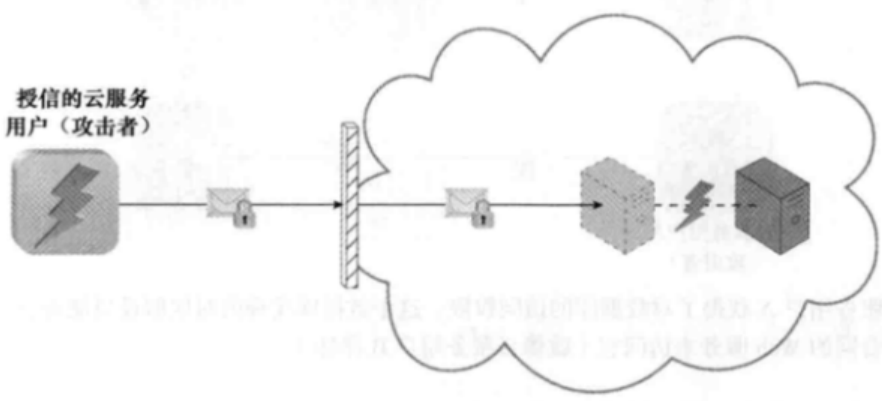
· **授权不足**

主要是指错误的授予了攻击者访问权限，或是授权太宽泛，导致攻击者能够访问本应该受到保护的 IT 资源。

这种攻击的一种变种称为弱认证(weak authentication)，如果用弱密码或共享账户来保护 IT 资源，就可能导致这种攻击。

· **虚拟化攻击(Virtualization attack)**

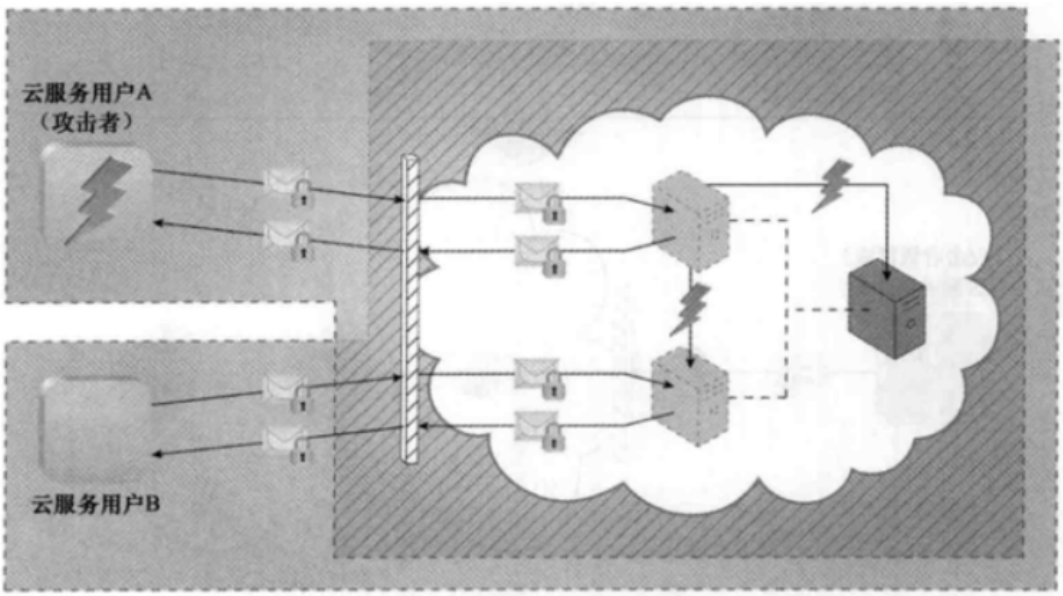
主要是指利用虚拟化平台的漏洞来危害虚拟化平台的保密性、完整性和可用性。



授权的云服务用户发动了一场虚拟化攻击，滥用了他对虚拟服务器的管理权限来获取底层硬件

· **信任边界重叠**

如果云中的物理 IT 资源是由不同的云服务共享的，那么这些云服务用户的信任边界是重叠的。恶意的云服务用户可以把目标设定为共享的 IT 资源，意图损害其他共享同样信任边界的云服务用户或 IT 资源。



云服务用户 A 是被云授信的，因此获得了对虚拟服务器的访问权限，然后它再意图攻击底层的物理服务器以及云服务用户 B 使用的虚拟服务器

（3） 关于各种云安全威胁的辨析

1.流量窃听和恶意媒介攻击通常是由截取网络流量的恶意服务作用者实施的

2.拒绝服务攻击的发生是当目标 IT 资源由于请求过多而载过重，这些请求意在使 IT 资源性能陷入瘫痪或不可用。

3.授权不足攻击是指错误的授予了攻击者访问权限或是授权太宽泛，或是使用了弱密码。

4. 虚拟化攻击利用的是虚拟化环境的漏洞，获得了对底层物理硬件未被授权的访问。

5. 重叠的信任边界潜藏了一种威胁，攻击者可以利用多个云用户共享的、基于云的 IT 资源。

3. 个人博客的发布

3.1 文本编辑器的选取

Hexo 博客的默认语法是使用 Markdown 进行编写，在撰写博客时可以先使用本地 Markdown 进行编写，之后利用 hexo 进行发布。

快捷键	作用	快捷键	作用
Ctrl+1	一阶标题	Ctrl+B	字体加粗
Ctrl+2	二阶标题	Ctrl+I	字体倾斜
Ctrl+3	三阶标题	Ctrl+U	下划线
Ctrl+4	四阶标题	Ctrl+Home	返回Typora顶部
Ctrl+5	五阶标题	Ctrl+End	返回Typora底部
Ctrl+6	六阶标题	Ctrl+T	创建表格
Ctrl+L	选中某句话	Ctrl+K	创建超链接
Ctrl+D	选中某个单词	Ctrl+F	搜索
Ctrl+E	选中相同格式的文字	Ctrl+H	搜索并替换
Alt+Shift+5	删除线	Ctrl+Shift+I	插入图片

3.2 hexo 的目录结构分析

首先分析 hexo 的目录以及各个文件夹的作用

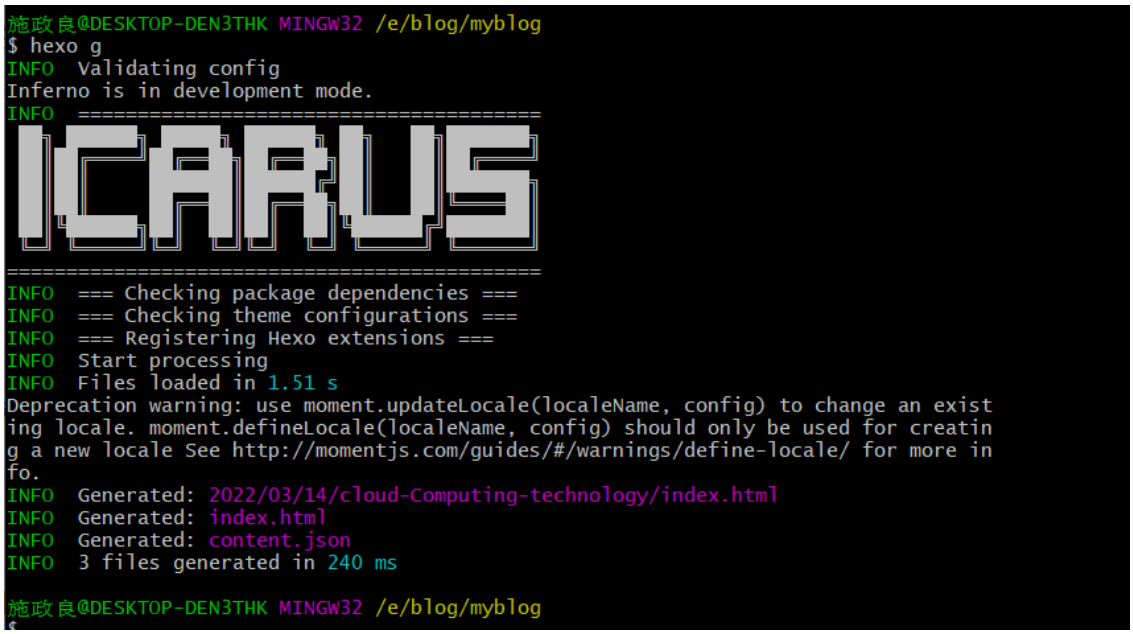
- deploy_git:执行 hexo d 命令 后生成的,主要存放部署的信息.
- node_modules:存放一些插件包
- public :执行 hexo g 后生成的, hexo 会将"/blog/source/" 下面的.md 后缀的文件编译为.html 后缀的文件,存放在"/blog/public/ " 路径下
- scaffolds:用来存放模板文件。模板文件的正文部分一般为空，一般在模板文件顶部有一个区域 (以 --- 分隔的区域) 称作 Front-matter,在这里配置的变量主要有 title(即文章标题), date(即文章创建日期),comment(是否开启评论), tags(文章标签), categories(文章所属分类)等. 当新建文章时，Hexo 会根据 scaffold 来建立文件，即会在创建的每个文件顶部自动加上模板文件中配置的这些内容.
- source:存放文章(.md 后缀的文件)
- themes:此目录是存放主题 (默认主题是 landscape, 目前使用最多的是 next 主题)
- .gitignore:这个文件和 git 有关, 在这个文件里面可以配置哪些文件不被提交(例如: 配置 *.log ,那么在 hexo d 命令的时候, 任何以.log 为后缀的文件将不会被提交到 github)
- _admin-config.yml:安装 hexo 后台管理插件后生成
- _config.yml:这个文件是 hexo 的核心配置文件(也称站点配置文件)

- package.json:应用程序的信息

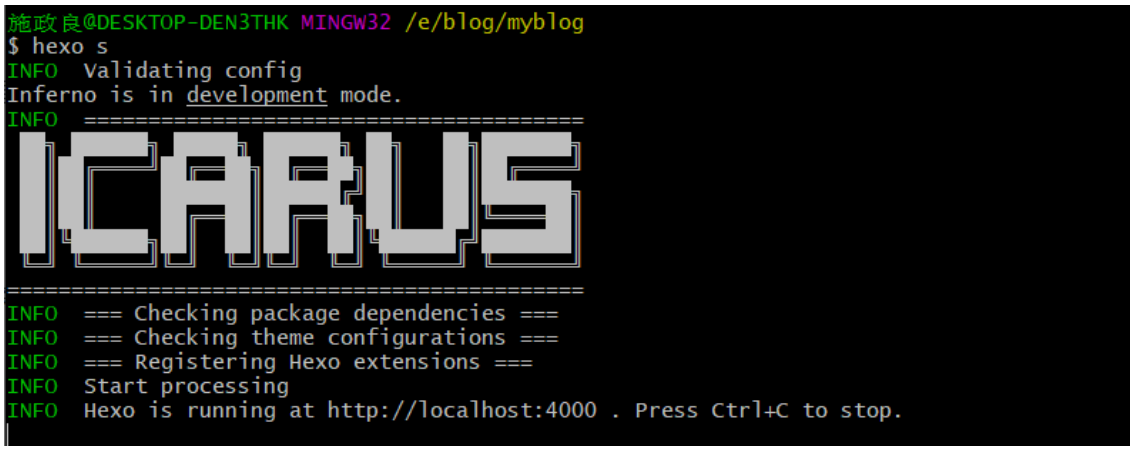
3.3 使用 hexo 进行发布

（1） 首先使用 hexo new [layout] title 指令新建一篇文章:Hexo 有三种默认布局：post、page 和 draft，它们分别对应不同的路径。自定义的其他布局和 post 相同，都将储存到 source/_posts 文件夹

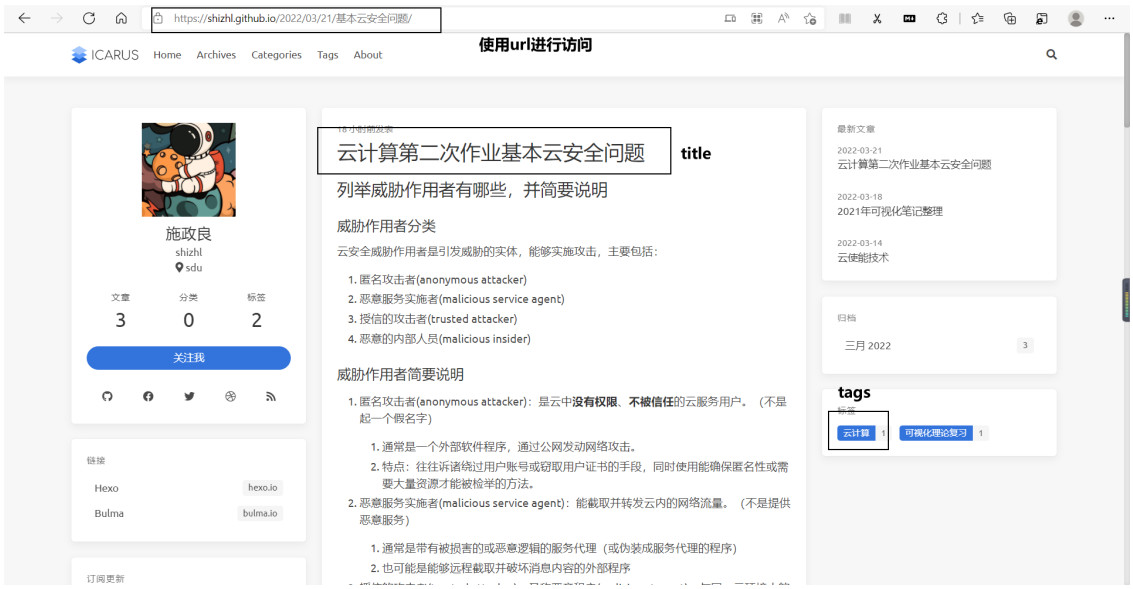
（2） 使用 hexo g 命令进行渲染和生成：在 hexo 中会将 Markdown 格式的文件自动的转化为.html 格式的文件。在实验中具体过程如下图所示



（3） 使用 hexo s 命令在本地打开服务器进行预览：默认服务器的端口是 4000，可以通过浏览器，输入对应的 url 进行访问和预览



本地预览如下所示：



结论分析与体会：

结论分析：

1. 云安全威胁主要包括：流量窃听(traffic eavesdropping)、恶意媒介(malicious intermediate)、拒绝服务(DoS)、授权不足、虚拟化攻击(Virtualization attack)、信任边界重叠等分类。
2. 云安全中除了威胁作用者还有其他考量，例如

（1） 云用户需要意识到，部署有缺陷的基于云的解决方案，可能会引入安全风险。

（2） 在选择云提供厂商时，理解云提供者如何定义和强加所有权，以及可能的不兼容的云安全策略，是形成评估标准的关键部分。

（3） 在云用户和云提供者签署的法律协议中，需要明确定义和相互理解对潜在的安全泄露的责任、免责和问责。

（4） 对于云用户来说，在理解具体针对某个特定云环境的安全相关的可能问题之后，对识别出的风险进行相应的评估是很重要的。

3. Markdown 是一种文本编辑的语法格式，相比于所见即所得的 word 或者 wps，Markdown 需要掌握一定的语法基础，相比于 Latex 专业排版，Markdown 更加的便捷。
4. Typora 是一款支持实时预览的 Markdown 编辑器，同时可以直接生成对应的文本内容。相比于其他 Markdown 编辑器，例如 visual studio code，sublime 以及一起 IDE 的 Markdown 插件，typora 更加的轻量，更加方便使用。

5. Hexo 为个人博客的搭建提供了同一的框架，使用同一的命令即可对文章进行渲染、生成相应的页面并上传。

体会

通过本次实验，我复习了基本云安全的相关知识，对云安全中威胁作用者、基本威胁的分类以及安全领域中的其他考量有了更深刻的认识。

在本次实验中，我熟悉了 Markdown 语法，同时选择了轻量级的 typora 作为文本编辑器，完成了博客内容的撰写。

附录

个人 github 仓库：shizhl/shizhl.github.io

个人博客主页：shizhengliang (shizhl.github.io)

第二次作业网址： 云计算第二次作业基本云安全问题 - shizhengliang (shizhl.github.io)