信息安全技术第一章作业

学号：2017218007　　姓名：文华　　班级：物联网工程 17-2 班

1、阐述信息安全的定义、目的和属性

答：

定义：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。

目的：在系统实现过程中，对组织、合作伙伴、及其客户的 IT 相关风险给出应有的关心考虑，从而帮助组织实现其使命/业务（Mission/Business）的全部目的。

属性：机密性、完整性、可用性、可控性、不可否认性。

2、在 TCP/IP 模型的各个层次上分别面临着哪些安全威胁？

答：

应用层：利用操作系统和网络协议上的漏洞进行的各种攻击。措施：加强安全服务，如安全协议、检测、加密等。

传输层与网际层：身份假冒、权限滥用、欺骗（IP 和 TCP）欺骗、路由侦听、重定向等。措施：实施安全控制技术，如身份认证、审计、网络管理等。

数据接口层：自然灾害、电磁辐射、数据监听、窃取、删除等。措施：物理安全技术，如容灾、屏蔽、监控等。

3、什么是高级持续性渗透攻击？为什么说零日攻击的危害性最大？

答：

高级持续性渗透攻击：高级持续性渗透攻击（Advanced Persistent Threat, APT）是指组织(特别是政府)或者小团体利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。

零日攻击的危害性最大的原因：由于漏洞刚被发现，没有任何相应的补丁可以补救，因此零日攻击行为的危险性极大，成功率也极高。

4、说说你所听到或遇到的印象深刻的信息安全事件

答：

①超 2 亿中国求职者简历疑泄露，数据“裸奔”将近一周

2019 年 1 月，HackenProof 的网络安全人员 Bob Diachenko 在推特上爆料称，一个包含 2.02 亿中国求职者简历信息的数据库泄露，被称为中国有史以来最大的数据曝光之一。

据称，包含 854GB 数据的 MongoDB 数据库无人看管，处于不受保护的状态。共计 202,730,434 条简历详尽记录了大量敏感信息，包括个人全名家庭住址，手机号码，电子邮件，婚姻状况，子女数量，政治关系，身高，体重，驾驶执照，识字水平，薪水期望、教育背景、过去的工作经验等等。

该机构通过对比简历的数据模式，发现 GitHub 项目 xzfan/data-import(目前该项目已经被删除)疑似为收集这些简历数据的爬虫。该爬虫会收集来自国内多个求职平台的简历。

②拼多多现优惠券漏洞，遭黑产团伙盗取数千万元

2019 年 1 月 20 日凌晨，拼多多被曝出现重大 BUG，用户可领 100 元无门槛券。网友称“有大批用户开始‘薅羊毛’，一晚上 200 多亿都是话费充值”。

当天上午 9 点，拼多多已经把 100 元无门槛优惠券的领取方式全部下架，之前领到未使用的优惠券也全部下架。

在“薅羊毛”事件发生几个小时后，1 月 20 日中午 12 点，认证为拼多多微博客服的@拼多多客户服务终于对此事发布了官方回应《关于“黑灰产通过平台优惠券漏洞不正当牟利”的声明》，声明全文如下：

1 月 20 日晨，有黑灰产团伙通过一个过期的优惠券漏洞盗取数千万元平台优惠券，进行不正当牟利。针对此行为，平台已第一时间修复漏洞，并正对涉事订单进行溯源追踪。同时我们已向公安机关报案，并将积极配合相关部门对涉事黑灰产团伙予以打击。

③京东金融 APP 被曝获取用户隐私

2019 年 2 月 16 日凌晨，一网友在微博发布视频称，京东金融 APP 疑似会获取用户的截图和照片并上传。京东金融随后回应称，图片缓存为方便客户投诉或建议使用，不会上传京东金融后台，不会未经允许获取手机用户隐私。

该微博网友发布的视频显示，京东金融 APP 在手机后台运行期间，该网友打开手机中的一个银行 APP 并进行了页面截图。随后，该网友在手机文件管理器中，打开京东金

融 APP 的文件目录，在一个文件夹中找到了刚刚保存的银行 APP 页面截图。不久后，该网友再次发布一个视频显示，京东金融 APP 在手机后台运行期间，用手机其他应用拍摄照片，也在京东金融的文件目录中找到。该网友发布视频之后，多位网友使用同样的操作，也得到相似的结果。

上述事件在微博获得广泛关注，2 月 17 日，“京东金融客服”官方发布声明称，图片缓存为方便客户投诉或建议使用，不会上传京东金融后台，不会未经允许获取手机用户隐私。经排查，发现安卓系统上的 APP5.0.5 以后版本存在该问题，并已定位问题且下线修复，该功能属于需求错误开发。