No.: Date:

1、有哪些常见的威胁类型？有哪些技术因素？有哪些人为因素？

常见的威胁类型有：

① 侦听威胁、 ③伪造威胁、

② 中断威胁、 ④修改威胁、

技术因素：网络协议漏洞，网络服务漏洞，操作系统漏洞，应用系统漏洞

人为因素：计算机病毒、网络蠕虫等。

2、信息安全的属性有哪几种？相关的主要实现技术分别是什么？

根据受损害的类型，安全攻击大致包括侦听，中断，修改，伪装等。

① 机密性，物理保密技术、防电磁辐射泄露技术、网络防截获和防窃听技术、加密和解密技术等。

② 完整性，报文摘要、加密、数字签名等技术

③ 可用性，实时的备份与恢复、设备和线路冗余、集群和虚拟化等技术

④ 可控性，基于PKI/PMI的访问控制技术

⑤ 不可否认性，身份认证技术，数字证书，IC或US Bkey令牌，指纹、视网膜、掌形、脸形、来保证。

3、什么是高级持续性攻击？有哪几种类型？各自的特点是什么？

高级持续性渗透攻击是指组织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。

① 投入上的高级：全面信息收集与获取，目标明确的工作团队，社会工程学+物理方法相

② 技术上的高级：0DAY攻击，通道加密。

4、什么是零日攻击？什么是零日攻击的生命周期？

零日攻击是一种利用计算机系统或应用中未知漏洞的攻击，是一种与漏洞的发现几乎同时的攻击行为。

生命周期：存在漏洞的网络实体如操作系统和各种应用等 → 漏洞被研究发现捕捉来并在小范围内传播 → 网络实体提供商暂时没有能力提供补丁 → 漏洞被广泛传播。

NOTEBOOK

No: Date:

5. 阐述你对OSI安全服务和安全机制的认识。

安全服务是指为加强网络信息系统安全性和对抗网络攻击行为而采取的一系列技术措施。安全机制是安全服务的技术实现手段。一种安全服务可以通过多个安全机制加以实现；同样地，一个安全机制也可以为多种安全服务的实现提供实现的措施。

6. TCSEC和CC中分别制定了几个安全级别？我国的安全等级保护中的安全级别有哪几个级别以及是如何确定的？

TCSEC制定了四类安全级别，CC制定了7个安全级别。

我国的安全等级：①第一级(用户自主级) ②第二级(系统审计保护级)
③第三级(安全标记保护级) ④第四级(结构化保护级)
⑤第五级(访问验证保护级)

第一级：对用户实施自主访问控制，保护用户信息免受破坏。

第二级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级：信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级：信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级：信息系统受到破坏后，会对国家安全造成特别严重损害。

7. 什么是PDR模型？什么PPDR模型？各有什么特点？

美国ISS互联网安全系统公司提出的基于时间的安全模型，也是全球第一个体现了主动防御思想的安全模型，即保护-检测-响应模型。

特点：给出了新的安全观，指明了方向，直观、实用。各个时间的测量比较困难，而且对各种安全威胁的应对模式相对固定，无法适应瞬息万变的网络实际状况。

PDR强调在防护、检测和响应的每个环节都要依据安全策略进行实施。

8、举例说明可能会造成严重后果的针对物联网和工业网络的攻击

物联网的严重攻击：比如现在在研究的车辆的自动驾驶技术，如果自动驾驶系统一旦被攻破，那么被控制的车辆很容易就可以夺取人们的性命。

工业网络的攻击：比如对于制药厂等流水线的攻击，如果随意调整各种化学药品的剂量将产生严重后果。