1.信息安全的五种基本属性（保密性，完整性，可用性，抗抵赖性，可靠性）的理解。

信息安全金三角：保密性、完整性、可用性

e.g. DoS破坏了信息安全中的可用性。

攻击者截获信息后进行篡改破坏了完整性。

信息加密处理是为了保障信息的保密性。

2.网络的逻辑安全。

3.网络不安全的主要原因。

网络自身的缺陷、网络开发、黑客攻击

4.常见的网络攻击技术和防御技术，网络攻击的一般流程。

网络攻击技术：漏洞扫描，网络嗅探技术，伪装技术

网络防御技术：漏洞扫描，IDS、IPS，防火墙，VPN

一般流程

6.网络攻击形式（主动攻击，被动攻击）；缓冲区溢出攻击，钓鱼攻击，D。S攻击，SQL攻击与XSS攻击，IP地址欺骗，木马与病毒。

7.控制类网络攻击，阻塞类网络攻击各有哪些方式。

控制类网络攻击：口令攻击、木马、缓冲区溢出

阻塞类网络攻击：DoS、ICMP、Smurf、LAND

8.防火墙的功能和局限性，防火的四种体系结构，防火墙的四种技术。

9.IDS（IDS形式，误报与漏报）

10.身份认证、消息认证。基于口令的认证，生物智能认证。11.网络扫描及种类。

12.计算机病毒，蠕虫，木马的联系与区别。