HW1

HW 1

1、信息安全的目标包括哪些？

答：信息安全的目标是保护网络与信息系统中信息的机密性、完整性、不可抵赖性、可用性和可控性等信息安全属性

2、信息安全面临的主要威胁有哪些？

答：①信息泄露
②非授权的篡改
③拒绝服务
④非法使用(非授权访问)
⑤假冒
⑥抵赖
⑦网络与系统攻击
⑧恶意代码
⑨自然灾害
⑩人为失误和故意破坏

3. 简述 DoS 和和缓冲区溢出攻击，论述二者破坏了哪些信息安全性

答：DoS：造成拒绝服务的攻击称为 DoS 攻击，目的是使计算机或网络无法提供正常的服务，通过故意地攻击网络协议实现的缺陷或直接通过野蛮手段耗尽被攻击对象的资源，使目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务停止响应或崩溃。

DoS 破坏了可靠性、可用性、保鲜性，通过使计算机或网络无法正常提供服务，信息系统运行的过程与结果不可信赖，进而可靠性与可用性不再。而被攻击时无法提供服务使得信息失去了时效，保鲜性不再。

缓冲区溢出攻击：利用缓冲区溢出漏洞进行的攻击行动，可导致程序运行失败，系统关机，重新启动的后果。最危险的是堆栈溢出，入侵者可利用此种溢出在函数返回时改变返回程序的地址，让其跳转到任意地址，使程序崩溃而拒绝服务。

缓冲区溢出攻击破坏了信息的完整性、可靠性、可用性、时效性、保鲜性。

由于此攻击可以修改函数的返回地址，则数据接收可能会是不完整的，而程序崩溃拒绝服务使可用性、可靠性、时控性就得不到保障。而信息失去时效性后，信息安全保鲜性也不存在。

4、以智能手机为例，列举2个访问控制的例子

①智能手机自带的杀毒软件或 App 带有防火墙，可通过防火墙控制实现访问控制。

②连接 WIFI 或开启热点时可进行网络权限控制，通过网络权限限制实现访问控制。