信息安全导论试卷参考答案

信息安全导论试卷 (总分108')

（答案仅供参考）

一 名词解释；（18'每个3'）

信息安全：是指对信息的保密性、完整性和可用性的，可控性和不可否认性的保持，保护信息系统的硬件，软件，及相关数据，使之不应为偶然或者恶意侵犯而遭受破坏更改及泄漏，保证信息系统能够连续可靠正常的运行。
VPN：一般是指建筑在因特网上能够自我管理的专用网络，是一条穿过混乱的公共网络的安全稳定的隧道。通过对网络数据的封包和加密传输，在一个公用网络建立一个临时的，安全的连接，从而实现早公共网络上传输私有数据达到私有网络的级别。

数字证书：是指各实体（持卡人、个人、商户、企业、网关、银行等）在网上信息交流及交易活动中的身份证明
应急响应：是指安全技术人员在遇到突发事件后所采取的措施和行动。而突发事件是指影响一个系统正常工作的情况
风险评估：风险评估有时也称为风险分析，是组织使用适当的风险评估工具，对信息和信息处理设施的威胁，影响和

薄弱点及其可能发生的风险的可能行评估，也就是确定安全风险及其大小的过程。

入侵检测：对入侵行为的发觉。他通过对计算机网络和计算机系统的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。 二 选择题（36'每个2'）

1.按密钥类型，加密算法可以分为（D）

A.序列算法和分组算法 B.序列算法和公钥密码算法 C公钥密码算法分组算法 D公钥密码算法和对称密码算法 2.口令破解的最好攻击方法（C）；

A.暴力破解B.社会工程 C.字典攻击 D.生日攻击 3.杂凑码（长度

B.抵赖信息的递交行为 C.数据中途被攻击者窃听获取 D.数据在途中被攻击者篡改

12.利用TCP/IP三次握手的协议漏洞的攻击是（A）；（DOS,DDOS,DROS）

A.ARP（地址解析协议）欺骗 B.DNS（域名系统）欺骗

C.URL（统一资源定位符也被称为网页地址）攻击 D.源路由攻击

13.攻击溢出攻击的核心是：（C ）

A.修改堆栈记录中进程的返回地址 C.提升用户进程权限

B.利用shellcode D.捕捉程序漏洞

14.在被屏蔽主机体系结构中堡垒主机位于（A），所有的外部临界都有过滤路由器路由到它上面去；

A.内部网络 B.周边网络

C.外部网络

D.自由连接

5.会话侦听与劫持技术”是属于（B）技术；

A.密码分析还原 C.应用漏洞渗透与分析

B.协议漏洞渗透 D.DOS攻击

15.外部数据包过滤路由器只能阻止一种IP欺骗，即（D），而不能阻止DNS欺骗；

A.内部主机伪装成外部主机的IP B.内部主机伪装成内部主机的IP
C.外部主机伪装成外部主机的IP D.外部主机伪装成内部主机的IP

6.PKI（公钥基础设施）的主要组成不包括（B）；

A.证书授权CA B.SSL（安全套接层） C.证书授权RA D.证书存储库CR

7.恶意代码是（D）；

A.病毒蠕虫，木马和后门 B.****和**** C.广告插件

D.以上都是

16.关于防火墙的描述不正确的是（D）

A.防火墙不能防止内部攻击

B.如果一个公司的信息安全制度不明确，拥有再好的防火墙也没有用

C.防火墙可以防止伪装成外部信任主机的IP地址欺骗
D.防火墙可以防止伪装成内部信任主机的IP地址欺骗
17.ICMP数据包的过滤主要基于（C）； A.目标端口 B.源端口 C.消息类代码
D.ACK位

8.社会工程学常被黑客用于（A）；

A.口令获取 B.AKP欺骗 C.TCP会话劫持D.DDOS

9.windows中强制终止进程使用如下（C）指令； A.tasklist B.netsat C.taskkill
D.netshare ？10.现代病毒融入了（D）新技术；

A.进程注入 B.注册表隐藏 C.漏洞扫描D.都是

11.网络密罐技术是用于（引诱攻击）；

A.**** B.**** C.****

D.**** (引诱攻击)

18.网络安全的特征应具有：保密性，完整性，可用性

和可控性，四个方面。

三．问答题(46')

1.信息安全的常见威胁有哪些？信息安全的实现有哪些主要技术措施？（8'）

答：常见威胁有非授权访问、信息泄露、破坏数据完整性，拒绝服务攻击，恶意代码等等。

信息安全的实现可以通过物理安全技术，系统安全技术，网络安全技术，应用安全技术，数据加密技术，认证授权技术，访问控制技术，审计跟踪技术，防病毒技术，灾难恢复和备份技术

2.什么是密码分析，其攻击类型有哪些？DES算法中S盒的作用是什么？；（6’）

答：密码分析：虽然不知道系统所用的密钥，但通过分析可能从截获的密文推断出原来的明文，这一过程成为密码分析。
攻击类型有：唯密文攻击，已知明文攻击，选择明文攻击，选择密文攻击。

DES算法中S盒的作用是：压缩替换，8个s盒将48位输入变换为32位输出起到很好的混乱效果。 3.试画图说明Kerberos认证原理；（5’）

答：

图 3.11 Kerberos实现原理

4.用户A需要通过计算机网络安全地将一份机密文件传送给用户B，如何实现？如果此文件数据量较大，且B希望A

KS:会话密钥 KRA:A的私钥 EP:公钥加密 EC:常规加密

KRB:B的私钥 DP:公钥解密 DC:常规解密

KUA:A的公钥 KUB:B的公钥

5.防火墙有哪几种体系结构？其中堡垒主机的作用是什么？检测计算机病毒主要方法有哪些？（9'）

答：防火墙包括：包过滤防火墙，双重宿主主机防火墙，屏蔽主机防火墙，屏蔽子网防火墙，堡垒主机的作用有：①堡垒主机是一个被强化的、被暴露在被保护

网络外部的、
可以预防进攻的计算机。堡垒主机上运行着防火墙软件，可以转发应用程序，提供服务等。②堡垒主机安装在内部网络上，是外部网络唯一可以直接到达的主机，确保内部网络不受未被授权的外部用户的攻击。③堡垒主机作为唯一可访问点，支持终端交互或作为应用网关代理。

检测计算机病毒的主要方法有:病毒特征代码检测法，文件校验法，行为特征检测法，软件模拟法。 6.试说明黑客攻击的一般流程及其技术和方法；（ 6' ）

答：黑客入侵的一般的完整流程是：隐藏自身—踩点—扫描—查点—
分析并入侵—获取权限—提升权限—扩大范围

—安装后门—清除日志

技术方法：预攻击探测；密码破解攻击；缓冲区溢出攻击；欺骗攻击；DOS/DDOS 攻击；CGI攻击；SQL注入攻击；木马攻击；网络蠕虫；恶意软件；社会工程

附加题：解释PE文件格式和壳保护原理

答：PE是指可移植性文件，是32位windows下可执行文件的标准形式。

加壳的全称应该是可执行程序资源压缩,是保护文件的常用手段.
加“壳”其实是利用特殊的算法，对EXE、DLL文件里的资源进行压缩。在程序中加入一段保护层代码，是源程序代码失去本来的面目，从而保护程序不被非法修改和反翻译，形象的称之为程序的壳。加壳保证文件格式不改变，否则加壳后的文件不能执行，同时还要将壳加到文件中。很多加壳软件在夹克过程中，还对引入表做了破坏，以达到对文件的保护，加了壳的文件在运行时，壳先执行，这是因为加壳过程中，PE文件的入口点发生了变化，通常加壳程序包含多层代码，每层均有反跟踪解密还原下层代码的程序，层层紧扣，层层相关。

相关文档：

- 信息安全导论答案
- 信息安全导论论文
- 信息安全意识培训答案
- 信息安全概论课后答案
- 信息安全管理考试答案
- 信息安全管理答案
- 信息安全技术答案
- 信息安全导论试题
- 信息技术与信息安全公需科目考试答案
- 信息安全试题及答案