# 考试科目1：网络信息安全基础知识和技术 （上午选择题）

150分钟 75道单选 其中5题英语 75分总分 45分过关

**（选择题区域快速过，重点在主观题）**

**（很多东西只要大概了解就行）**

## 第1章 网络信息安全概述

网络安全基本属性：机密性、完整性、可用性、抗抵赖性、可控性

CIA

法律：

《中华人民共和国网络安全法》 于 2017 年 6 月 1 日起实施

《中华人民共和国密码法》 于 2020 年 1 月 1 日起实施

- 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存 相关的网络日志不少于六个月。

- 网络安全等级保护的主要工作可以概括为定级、备案、建设整改、等级测评、运营维护。

部门：

国家计算机网络应急技术处理协调中心(CNCERT) -- 是国家级应急中心.

职责：积极预防、及时发现、快速响应、力保恢复

## 第2章 网络攻击原理与常用方法

网络攻击一般过程

| 一般过程 | 内容 |
| --- | --- |
| 隐藏攻击源 | 隐藏黑客主机位置使得系统管理无法追踪 |
| 收集攻击目标信息 | 确定攻击目标并收集目标系统的有关信息 |
| 挖掘漏洞信息 | 从收集到的目标信息中提取可使用的漏洞信息 |
| 获取目标访问权限 | 获取目标系统的普通或特权账户的权限 |
| 隐蔽攻击行为 | 隐蔽在目标系统中的操作，防止入侵行为被发现 |
| 实施攻击 | 进行破坏活动或者以目标系统为跳板向其他系统发起新的攻击 |
| 开辟后门 | 在目标系统中开辟后门，方便以后入侵 |
| 清除攻击痕迹 | 避免安全管理员的发现、追踪以及法律部门取证 |

## 第3章 密码学基本理论

密码学是一门研究信息安全保护的科学，

以实现信息的 **保密性、完整性、可用性及抗抵赖性。**

PS：比较　网络安全基本属性：**机密性、完整性、可用性、抗抵赖性、可控性**

明文（M）、密文（C）、

加密（E）、解密（D）、

加密密钥（Ke）、解密密钥（Kd）

| 密码分析攻击类型 | 内容 |
| --- | --- |
| **唯密文**攻击 | 密码分析者只拥有一个或多个用同一个密钥加密的密文，没有其他可利用的信息 |
| **已知明文**攻击 | 密码分析者仅知道当前密钥下的一些明文及所对应的密文 |
| **选择明文**攻击 | 密码分析者能够得到当前密钥下自己选定的明文所对应的密文 |
| **密文验证**攻击 | 密码分析者对于任何选定的密文，能够得到该密文"是否合法"的判断。 |
| **选择密文**攻击 | 除了挑战密文外，密码分析者能够得到任何选定的密文所对应的明文 |

选择明文攻击：选择明文得到密文

选择密文攻击：选择密文得到明文

### 国产商用密码算法

SM1　对称加密算法

SM2　椭圆曲线数字签名算法

SM3　杂凑算法　　消息分组长度为512位 ，输出256

SM4　对称加密算法　　无线局域网产品使用

SM9　标识数字签名算法

SM2椭圆曲线数字签名算法　和 SM9　标识数字签名算法是我国国家密码管理局发布的数字签名标准。

2006 年我国政府公布了自己的商用密码算法，成为我国密码发展史上的一件
大事。

PGP用来保护**邮件**，密钥管理算法选用了IDEA

## 第3章 网络安全体系和网络安全模型

网络安全等级保护工作主要包括　**定级、备案、建设整改、等级测评、监督检查**　五个阶段。

**安全保护五个等级：**

第一级（用户自主保护级）

第二级（系统保护审计级）

第三级（安全标记保护级）

第四级（结构化　　保护级）

第五级（访问验证保护级）

**智慧城市**安全技术保障的功能要素包括**防护、检测、响应和恢复**。

ISO27000 信息安全管理体系

**信息安全管理系统（ISMS）**按照 PDCA 不断循环改进。

其主要步骤阐述如下：

**计划**（Plan）:建立 ISMS，识别信息资产及其相关的安全需求;评估信息安全风险;选择合适的安全控制措施，管理不可接受的风险。

**执行**（Do）:实现和运行 ISMS，实施控制和运维管理。

**检查**（Check）:监测和评估 ISMS。

**处理**（Act）:维持和改进 ISMS。

## 第4章 物理与环境安全技术

物理安全规范-信息系统物理安全分级

第一级物理安全平台为第一级 **用户自主保护级** 提供基本的物理安全保护。

第二级物理安全平台为第二级 **系统审计保护级** 提供适当的物理安全保护。

第三级物理安全平台为第三级 **安全标记保护级** 提供较高程度的物理安全保护。

第四级物理安全平台为第四级 **结构化保护级** 提供更高程度的物理安全保护。

PS:与安全保护五个等级比较，少了最后一个 **访问验证保护级**，其他相同。

----------已经完成了五分之一了， 加油!----------

## 第6章 认证技术原理与应用

认证机制是网络安全的基础性保护措施，是实施访问控制的前

提。

认证一般由**标识（Identification）**和**鉴别（Authentication）**两部分组成

常见的认证依据主要有四类

| 认证依据 | 概念 | 应用 |
| --- | --- | --- |
| 所知道的秘密信息 | 实体（声称者）所掌握的秘密信息 | 如用户口令、验证码等 |
| 所拥有的实物凭证 | ~所持有的不可伪造的物理设备 | 如智能卡、U 盾等 |
| 所具有的生物特征 | ~所具有的生物特征 | 如指纹、声音、虹膜、人脸等 |
| 所表现的行为特征 | ~所表现的行为特征 | 如鼠标使用习惯、键盘敲键力度、 地理位置等 |

Kerberos 网络认证协议，使用对称密码提供认证服务

//PKI Kerberos 重要，必背！

## PKI 公钥基础设施 （Public Key Infrastructurc）

就是有关创建、管理、分发和撤销公钥证书所需要的的硬件、软件、人员、策略和过程的安全服务设施。

PKI提供了一种系统化的、可扩展的、统一的、容易控制的公钥分发方法。

PKI包含五个实体部分：

1. CA（Certification Authority）：证书授权机构，主要进行证书的颁发、废止和更新；（可信第三方机构）
2. RA （Registration Authority）： 证书登记权威机构，将公钥和对应的证书持有者的身份及其他属性联系起来，进行注册和担保；可以充当 CA 和它的终端用户之间的中间实体，辅助 CA 完成其他绝大部分的证书处理功能。

3. **客户端**：使用者、进程服务等
4. **终端实体**：需要认证的对象，例如服务器、打印机、用户等
5. **目录服务器**：CA通常使用一个目录服务器提供证书管理和分发的服务。

单点登录（Single Sign On）：

是指用户访问使用不同的系统时，只需要进行一次身份认证，就可以根据这次登录的认证身份访问授权资源。

FIDO快速在线认证

路由器认证有OSPF、RIP 、 EIGRP

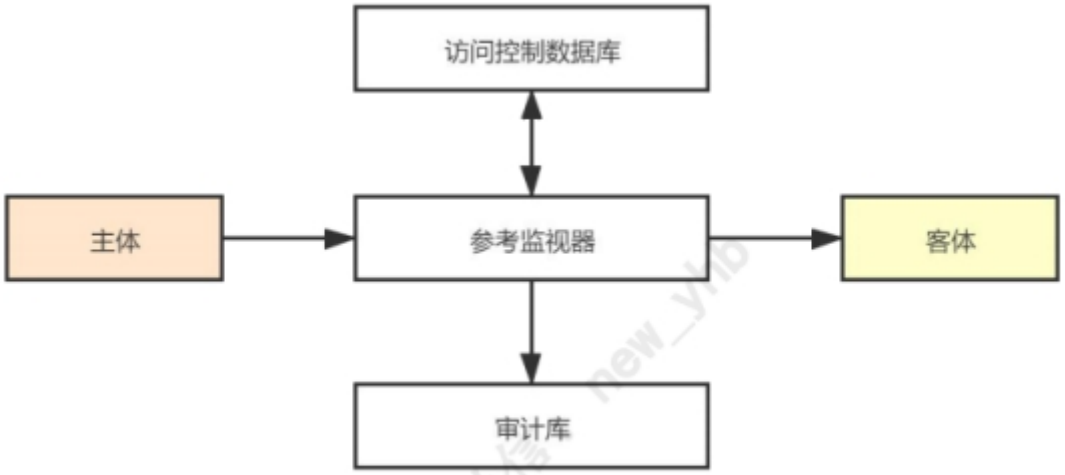
公民网络电子身份标识 eID,是国家网络安全的重要保障.

与个人真实身份具有一一对应关系，用于在线识别公民真实身份的网络电子身份。由一对非对称密钥和含有其公钥及相关信息的数字证书组成

# 第7章　访问控制技术原理与应用

访问控制参考模型

组成要素主要有主体（Subject）、参考监视器（Reference Monitor）、客体（Object）、访问控制数据库、审计库




图：访问控制参考模型

**主体**：是客体的操作实施者。实体通常是人、进程或设备等，一般是代表用户执行操作
的进程。比如编辑一个文件，编辑进程是存取文件的主体，而文件则是客体。

**客体**：是被主体操作的对象。通常来说，对一个客体的访问隐含着对其信息的访问。

**参考监视器**：是访问控制的决策单元和执行单元的集合体。控制从主体到客体的每一次
操作，监督主体和客体之间的授权访问行为，并将重要的安全事件存入审计文件之中。

**访问控制数据库**：记录主体访问客体的权限及其访问方式的信息，提供访问控制决策判断的依据，也称为访问控制策略库。该数据库随着主体和客体的产生、删除及其权限的修改而动态变化。

**审计库**：存储主体访问客体的操作信息，包括访问成功、访问失败以及访问操作信息。

**自主访问控制**：（Discretionary Access Control，DAC）是指客体的所有者按照自己的安全策略授予系统中的其他用户对其的访问权

自主访问控制的实现方法有两大类，即**基于行的自主访问控制和基于列的自主访问控制。**

基于行的自主访问控制：

三种形式明细表：　　能力表、前缀表、口令

基于列的自主访问控制：

两种形式明细表：保护位、访问控制表

强制访问控制：

是指系统根据主体和客体的安全属性，以强制方式控制主体对客体的访问。

与自主访问控制相比较，强制访问控制更加严格。用户使用自主访问控制虽然能够防止其他用户非法入侵自己的网络资源，但对于用户的意外事件或误操作则无效。因此，自主访问控制不能适应高安全等级需求。在政府部门、军事和金融等领域，常利用强制访问控制机制，将系统中的资源划分安全等级和不同类别，然后进行安全管理

基于角色的访问控制：

所谓基于角色的访问控制（RBAC）就是指根据完成某些职责任务所需要的访问权限来进行授权和管理。

访问控制策略设计与实现：P147

• 访问控制策略：访问控制策略用于规定用户访问资源的权限，防止资源损失、泄密或非法使用.

• 访问控制规则类型：

基于用户身份的访问控制规则

基于角色的访问控制规则

基于地址的访问控制规则

基于时间的访问控制规则

基于异常事件的访问控制规则

基于服务数量的访问控制规则

用户管理是网络安全管理的重要内容之一，其主要工作包括用户登记、用户权限分配、访问记录、权限监测、权限取消、撤销用户。

口令选择应至少在 8 个字符以上，应选用大小写字母、数字、特殊字符组合禁止使用与账号相同的口令。

7.7 访问控制技术应用：

• 普通的 UNIX、Linux 等系统中，实现自主访问控制技术的基本方法是在每个文件上使用"9 比特位模式"来标识访问控制权限信息，这些二进制位标识了"文件的拥有者、与文件拥有者同组的用户、其他用户"对文件所具有的访问权限和方式。

• Windows 访问控制应用：Windows 用户登录到系统时，WinLogon 进程为 用户创建访问令牌，包含用户及所属组的安全标识符（SID），作为用户的身份标识。文件等客体则含有自主访问控制列表（DACL），标明谁有权访问，还含有系统访问控制列表（SACL）

7.7.6 web服务访问控制应用

以Apache httpd的服务器为例，假设要保护/secret目录资源，只有特点IP地址、IP子网或域名可以访问，则需要在access.con中加入一个类似下面的目录控制段。

```
<Directory /full/path/to/secret>
<Limit GET POST>
            deny from all
        allow    from x.y.z      XXX.XXX.XXX.cn
        allow    a.b.c.d
</Limit>
</Directory>
```

# 第8章 防火墙技术原理与应用

## 8.2 防火墙类型与实现技术 -- 重点

~~防火墙类型可分为包过滤防火墙、代理防火墙、下一代防火墙、 数据库防火墙、Web 应用防火墙、工控防火墙。~~

（教程上下有点歧义）

基于防火墙产品形态分类：软件防火墙、硬件防火墙

基于防火墙应用领域分类：网络防火墙、Web防火墙、工控防火墙

概述中：

防火墙的实现技术主要有

包过滤、

状态检测、

应用服务代理、

网络地址转换、

协议分析、

深度包检查等

考纲中：

防火墙的实现技术：

包过滤技术

应用服务代理技术

网络地址转换技术

WEB防火墙技术

数据库防火墙技术

工控防火墙技术

下一代防火墙技术

### 8.5.3 iptables配置

```
删除所有规则：
iptables -F

设置默认规则，全禁止：
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP


```

由于教程和考纲不一致第九章开始主要是按考纲来进行整理了，注意区分内容的小标层级来区分重要性

# 第9章 VPN技术原理与应用

9.1

**VPN概念：**

VPN（Virtual Private Network），中文翻译为"虚拟专用网"，其基本技术原理是把需要经过公共网传递的报文（packet）加密处理后，再由公共网络发送到目的地。

利用 VPN 技术能够在不可信任的公共网络上构建一条专用的安全通道，经过VPN 传输的数据在公共网上具有保密性。

所谓"虚拟"指网络连接特性是逻辑的而不是物理。VPN 是通过密码算法、标识鉴别、安全协议等相关的技术，在公共的物理网络上通过逻辑方式构造出来的安全网络。

**VPN安全服务功能：**

VPN的主要安全服务有以下三种

- **保密性服务**：防止传输的信息被监听
- **完整性服务**
- **认证服务** ： 提供用户和设备的访问认证，防止非法接入

**9.2 VPN类型和实现技术**

•**VPN类型**：　　**链路层**VPN、**网络层**VPN、**传输层**VPN等

•**VPN实现技术**：密码算法、秘钥管理、认证访问控制、IPSec协议、SSL协议等

(等：**PPTP**、**L2TP**)

其他/不重要：SSL协议是介于应用层和TCP层之间的安全通信协议。

## 9.3 VPN主要技术指标与产品

**主要产品特征如下：**

**IPSec VPN**：IPS工作模式应支持**隧道模式和传输模式**，其中隧道模式适用于主机和网关实现，传输模式是可选功能，仅适用于主机实现。

**SSL VPN**：工作模式分**为客户端-服务端模式**、**网关-网关模式**两种。

**•功能技术指标：**

**IPSec VPN 的主要功能包括：**随机数生成、密钥协商、安全报文封装、身份鉴别、NAT 穿越。身份认证数据应支持数字证书或公私密钥对方式，IP 协议版本应支持 IPv4 协议或IPv6 协议。

**SSL VPN 的主要功能包括：**随机数生成、密钥协商、安全报文传输、身份鉴别、访问控制、密钥更新、客户端主机安全检查。

**•性能技术指标：**

**IPSec VPN 主要性能指标如下：**加解密吞吐率、加解密时延、加解密丢包率、每秒新建连接数

**SSL VPN 主要性能指标如下：**最大并发用户数、最大并发连接数、每秒新建连接数、吞吐率

**•安全技术指标：**

## 9.4 VPN技术应用

根据 VPN 的用途，VPN 可分为三种应用类型：

远程访问虚拟网（**Access VPN**）、
企业内部虚拟网（**Intranet VPN**）、
企业扩展虚拟网（**ExtranetVPN**）。

**•远程安全访问**（远程访问虚拟网 Access VPN）

> 远程安全访问:**Access VPN** 主要解决远程用户安全办公问题，远程办公用户既要能远程获取到企业内部网信息，又要能够保证用户和企业内网的安全。远程用户利用VPN技术，通过拨号、ISDN 等方式接入公司内部网。AccesVPN 一般包含两部分，远程用户 VPN 客户端软件和 VPN 接入设备。

**• 构建内部安全专网**（企业内部虚拟网 Intranet VPN ）

> 随着业务的发展变化，企业办公不再集中在一个地点，而是分布在各个不同的地理区域，甚至是跨越不同的国家。因而，企业的信息环境也随之变化。针对企业的这种情况，Intranet VPN 的用途就是通过公用网络，如因特网，把分散在不同地理区域的企业办公点的局域网安全互联起来，实现企业内部信息的安全共享和企业办公自动化。

**• 外部网络安全互联** （企业扩展虚拟网 ExtranetVPN）

> 由于企业合作伙伴的主机和网络分布在不同的地理位置，传统上一般通过专线互连实现信息交换，但是网络建设与管理维护都非常困难，造成企业间的商业
> 交易程序复杂化。Extranet VPN 则是利用 VPN 技术，在公共通信基础设施（如因特网）上把合作伙伴的网络或主机安全接到企业内部网，以方便企业与合作伙伴共享信息和服务。Extranet VPN 解决了企业外部机构接入安全和通信安全的问题，同时也降低了网络建设成本。

# 第10章 入侵检测技术原理与应用

## 10.1 入侵检测概述

· 入侵检测概念

入侵检测通过收集**操作系统**、**系统程序**、**应用程序**、**网络包**等信息，发现系统中**违背　安全策略**或**危及系统安全**的行为。

· 入侵检测模型

CIDF:该模型认为入侵检测系统由以下四部分组成：

事件产生器、事件分析器、响应单元、事件数据库

（CIDF将需要分析的数据统称为事件；事件产生器从整个计算环境中获得事件）

·入侵检测作用

（就是发现入侵行为）

1.发现受保护系统中的入侵行为或异常行为

2.检验安全保护措施的有效性

3.分析受保护系统所面临的的威胁

4.有利于阻止安全事件扩大，及时报警触发网络安全应急响应

5.可以为网络安全策略的制定提供重要指导

6.报警信息可用作网络犯罪取证

## 10.2 入侵检测技术

·基于**误用**的入侵检测技术

·基于**异常**的入侵检测技术

·基于**规范**的检测方法

·基于**生物免疫**的检测方法

·基于**攻击诱骗**的检测方法

·基于**入侵报警**的关联检测方法

·基于误用的入侵检测技术

基于特征检测,依赖于攻击模式库。

·基于异常的入侵检测技术

将系统运行的数值与“正常轨迹”比较。（**例如CPU、内存使用率**）

·基于规范的检测方法

介于误用检测和异常检测之间，若特权程序的操作序列不符合已定义的操作序列，就进行入侵检测报警。能够发现已知和未知的攻击。

·基于生物免疫的检测方法

综合误用与异常两种检测方法，构造系统“自我”标志，识别“非自我”的入侵行为。

·基于攻击诱骗的检测方法

类似于蜜罐

·基于入侵报警的关联检测方法

（**其实就是多加了一个关联性分析**）

对原始IDS报警事件的分类及相关性分析来发现复杂攻击行为

## 10.3 入侵检测系统组成与分类

**大纲：**

- 入侵检测系统组成
- 基于**主机**的入侵检测系统
- 基于**网络**的入侵检测系统
- 分布式入侵检测系统

**详解：**

· 入侵检测系统组成

1.数据采集模块

2.入侵分析引擎模块

3.应急处理模块

4.管理配置模块

5.相关辅助模块

- 基于**主机**的入侵检测系统　　**H**IDS (**Host**-based Intrusion Detection System)

  相关软件：SWATCH、Tripwire、网页防篡改系统

- 基于**网络**的入侵检测系统　　**N**IDS(**Network** Intrusion detection system)

- **分布式**入侵检测系统

  它可以跨越**多个子网**检测攻击行为，特别是大型网络。

> 可以解决以下问题：
> ·系统漏洞分散在网络中的各个主机上
> ·入侵行为不再单一，而是相互协作
> ·网络传输速度加快，流量增大

## 10.4 入侵检测系统主要技术指标与产品

### 10.4.1入侵检测主要技术指标

· **功能**技术指标

· **性能**技术指标

· **安全**技术指标

入侵检测系统的主要指标有**可靠性**、**可用性**、**可扩展性**、**时效性**、**准确性**和**安全性。**

**10.4.2** 入侵检测产品工作机制分析、入侵检测产品标准理解、入侵检测产品适用场景等

常见入侵检测相关**产品**有以下几类：

1.主机入侵检测系统

2.网络入侵检测系统

3.统一威胁管理

4.高级持续威胁检测系统

·入侵检测产品适用场景：

1.上网保护

2.网站入侵检测与保护

3.网络攻击阻断

4.主机/终端恶意代码检测

5.网络安全监测预警与应急处置

6.网络安全等级保护

**10.5 入侵检测系统应用** (感觉10.5 10.4这两节没啥内容，比较乱)

10.5.1 入侵检测系统部署方法与步骤

10.5.2 主机入侵检测 (H IDS)

10.5.3 网络系统内部入侵检测 (N IDS)

10.5.4 网络系统外部入侵检测 (N IDS)

# 第11章 网络物理隔离技术原理与应用

## 11.1 网络物理隔离概述

· 网络物理隔离概念

既能满足内外网信息及数据交换需求，又能防止网络安全事件出现。

· 网络物理隔离工作原理

避免两台计算机之间直接的信息交换以及物理上的连通，以阻断两台计算机之间的直接在线网络攻击。

## 11.2 网络物理隔离系统与类型

- 网络物理隔离系统组成

  按照隔离的对象，分为单点隔离系统 和 区域隔离系统。

  按照信息传递方向，分为**双向物理隔离系统、单向网络隔离系统。**

- **双向网络物理隔离系统**
- **单向网络物理隔离系统**

- 终端物理隔离系统

## 11.3 网络物理隔离机制与实现技术 （总感觉这个考纲弄得不是很靠谱）

· 专用计算机
· 多PC
· 外网代理服务
· 内外网线路切换器
· 单硬盘内外分区
· 双硬盘
· 网闸
· 协议隔离技术
· 单向传输部件
· 信息摆渡技术
· 物理断开技术

## 11.4 网络物理隔离主要技术指标与产品

### 11.4.1 入侵检测主要技术指标

· **功能**技术指标

| **产品名称** | **功能要求** |
| --- | --- |
| 终端隔离产品 | 访问控制、不可旁路和客体重用 |
| 网络隔离产品 | 访问控制、抗攻击、安全管理、标识和鉴别、审计、域隔离、容错、数据完整性和密码支持 |
| 网络单向导入 | 访问控制、抗攻击、安全管理、标识和鉴别、审计、域隔离、配置数据保护和运行状态监测 |

· **性能**技术指标

对网络和终端隔离产品应达到的性能指标作出规定，包括交换速率和硬件切换时间。

· **安全**技术指标

关于产品的质量和服务器保障要求，入配置管理、交付和运行、开发和指导性文档、测试、脆弱性评定等。

**11.4.2** 网络物理隔离产品**工作机制分析**、网络物理隔离**产品标准理解**、网络物理隔离**产品适用场景**等

*没啥东西，直接把书那块内容看一下就知道了 P222*

主要产品：

**1.终端隔离产品**

采用**物理断开技术,**连接两个不同的安全域。

**2.网络隔离产品**

实现安全域之间的**应用代理服务**、协议转换、信息流访问控制、内容过滤和信息摆渡等功能。

**3.网络单向导入产品**

两个安全域之间信息单向导入

**11.5 网络物理隔离应用** （没啥东西）

· 内网用户安全访问互联网

· 业务生产网与互联网隔离

· 内外网安全物理隔离

· 不同安全区域信息交换

# 第12章 网络安全审计技术原理与应用

12.1 网络安全审计概述

·网络安全审计概念

**网络安全审计是指对网络信息系统的安全相关活动信息进行获取、记录、存储、分析和利用的工作。**

·网络安全审计用途

网络安全审计的作用在于**建立“事后”安全保障措施，保存网络安全事件及行为信息，为网络安全事件分析提供线索及证据，以便于发现潜在的网络安全威胁行为，开展网络安全风险分析及管理。**

12.2 网络安全审计系统组成与类型

· 网络安全审计系统**组成**

网络安全审计系统一般包括审计**信息获取、审计信息存储、审计信息分析、审计信息展示及利用、系统管理** **等**组成部分。

· 网络安全审计系统**运行机制**

· 网络安全审计系统**类型** **（重点）**

**网络通信**安全审计

**操作系统**安全审计

**数据库**　安全审计

**应用系统**安全审计

**运维**　　安全审计

## 12.3 网络安全审计机制与实现技术

- **网络流量数据采集**技术：交换机端口、镜像、网络嗅探等
  libcap、winpcap、tcpdump、wireshark

- **系统日志数据采集**技术：syslog、FTP、snmp

- **Tcpdump的使用**　**考纲中有，注意一下**

- **网络审计数据分析技术**
  1.字符串匹配
  2.全文搜索
  3.数据关联
  4.统计报表
  5.可视化分析

- **网络审计数据保护技术**　重点，把下面几个记一下
  1.系统用户分区管理
  2.审计数据**强制访问**
  3.审计数据**加密**
  4.审计数据**隐私保护**
  5.审计数据**完整性保护**
  6.审计数据**备份**　（这一点考纲有，教程里没有）

### 12.4 网络安全审计主要产品与技术指标 （教程无内容，乱七八糟的）

### 12.5 网络安全审计应用 （把下面几个应用点记住就行了）

· 网络合规使用

· 网络电子取证

· 网络安全运维保障

# 第13章 网络安全漏洞防护技术原理与应用

### 13.1 概述

- 网络安全漏洞概念

网络安全漏洞又称为脆弱性，简称漏洞。漏洞一般是致使网络信息安全策略相冲突的缺陷，这种缺陷通常称为安全隐患。

- 网络安全漏洞危害 （教程里只有前四项）

**敏感信息泄露**

**非授权访问**

**身份假冒**

**拒绝服务**

普通用户权限提升

获取远程管理员权限

拒绝服务

服务器信息泄露

非授权访问

读取受限文件

口令恢复

欺骗

· 国家信息安全漏洞库 CNNVD

· 国家信息安全漏洞共享平台 CNVD

标准规范:

《信息安全技术 安全漏洞**分类**（GB/T 33561-2017）》

《信息安全技术 安全漏洞**等级划分指南**（GM/T 30279-2013）》

《信息安全技术 安全漏洞**标识与描述规范**（GM/T 28458-2012）》

《信息安全技术 信息安全**漏洞管理规范**（GB/T 30276-2013）》

## 13.2 网络安全漏洞分类与管理

- 网络安全漏洞来源:

非技术性安全漏洞

技术性安全漏洞

- **非技术性安全漏洞**

1.网络安全责任主体不明确

2.网络安全策略不完备

3.网络安全操作技能不足

4.网络安全监督缺失

5.网络安全特区控制不完备

- **技术性安全漏洞**

1.设计错误

2.输入验证错误

3.缓冲区溢出

4.意外情况处置错误

5.访问验证错误

6.配置错误

7.竞争条件

8.环境错误

- **网络安全漏洞命名规范**

  **CVE**

  **CNNVD**

  **CNVD**

- **网络安全漏洞命名规范**

  CVE 、 CNNVD 、 CNVD

- **网络安全漏洞分类分级**

  ~~· CVE漏洞分类~~

  · CVSS　通用漏洞计分系统

  · CNNVD漏洞分类

  · CNVD　漏洞分类

  · OWASP　TOP 10 Web应用漏洞

- **网络安全漏洞发布**

  **漏洞发布方式**：

  网站、电子邮件、安全论坛

  **漏洞信息公布内容**：

  漏洞编号、发布日期、安全危害级别、发布日期、安全危害级别、漏洞名称、漏洞影响平台。

- **网络安全漏洞获取**

  来源：

  1. 网络安全应急响应机构

2. 网络安全厂商

3. IT产品或系统提供商

4. 网络安全组织

内容：

- **网络安全漏洞信息来源**

  国家信息安全漏洞库CNNVD

  国家信息安全漏洞共享平台CNVD

  Bugtra漏洞库

  CERT

  Security Focus Vulnerability Database

  厂商漏洞信息

- **网络安全漏洞管理过程**

  1.网络信息资产确认

  2.网络安全漏洞采集

  3.网络安全漏洞评估

  4.网络安全漏洞消除和控制

  5.网络安全漏洞变化跟踪

## 13.3 网络安全漏洞扫描技术与应用

· 主机　漏洞扫描技术　（类似于病毒查杀）

· 网络　漏洞扫描技术　　(nessus)

· Web　漏洞扫描技术　　(awvs)

· 数据库漏洞扫描技术

应用：

网络安全漏洞扫描常用于 网络信息系统**安全检查**和**风险评估。**

### 13.4 网络安全漏洞处置技术与应用

网络安全漏洞处置技术：

网络安全漏洞**发现技术**

网络安全漏洞**修补技术**

网络安全漏洞**利用防范技术**

13.5（网络安全漏洞防护）主要产品与技术指标

产品：

网络安全漏洞扫描器

网络安全漏洞服务平台

网络安全漏洞防护网关

## 第14章 恶意代码防范技术原理

（这章都是类似的内容，快速过？）

（重点是自己要弄清楚各类恶意代码的特征及区别，及运行机制，但不要局限于文字描述）

14.1 概述

· 概念与分类

**概念：是一种违背目标系统安全策略的程序代码，会造成目标系统信息泄露、资源滥用，破坏系统的完整性及可用性。**

它能够进过存储介质或网络进行传播，从一台计算机系统传到另一台计算机系统，未经授权认证访问或破坏计算机系统。

分类：

（主动传播）蠕虫

（被动传播）计算机病毒、特洛伊木马、逻辑炸弹、间谍软件、恶意脚本、ActiveX控件等

· 恶意代码攻击模型

分为6个步骤：

第一步 侵入系统

第二步 维持或提升已有的权限

第三步 隐蔽

第四步 潜伏

第五步 破坏

第六步 重复前五步

· 恶意代码生存技术

1.反跟踪技术

2.加密技术

3.模糊变换技术

4.自动生产技术

5.变形技术

6.三线程技术

7.进程注入技术

8.通信隐藏技术

9.内核隐藏技术

· 恶意代码攻击技术

1.进程注入技术

2.超级管理技术

3.端口反向连接技术

4.缓冲区溢出技术

· 恶意代码分析技术

1.静态分析

2.动态分析

· 恶意代码防范策略

## 14.2 计算机病毒分析与防护

· 概念与特性

是一组具有自我复制、传播能力的代码

四个特点：

1.隐蔽性

2.传染性

3.潜伏性

4.破坏性

·组成与运行机制

计算机病毒由三部分组成：复制传染部件、隐藏部件、破坏部件。

生命周期：第一阶段 复制传播阶段

第二阶段 激活阶段

· 计算机病毒常见类型与技术

1.引导性病毒

2.宏病毒

3.多态病毒

4.隐蔽病毒

· 计算机病毒防范策略与技术

计算机病毒检测

计算机病毒防范

计算机病毒应急响应

· 计算机病毒防护模式

1.基于计算机病毒防护

2.基于网络计算机病毒防护

3.基于网络分级病毒防护

4.基于邮件网关病毒防护

5.基于网关防护

## 14.3 特洛伊木马分析与防护

**概念：**

具有伪装能力、隐蔽执行非法功能的恶意程序，而受害用户表面上看到的是合法功能的执行。

**特点：**

伪装成合法文件

不具有自我传播能力

攻击者可以远程控制受害机

**• 特洛伊木马运行机制**

1.寻找攻击目标

2.收集目标系统的信息

3.将木马植入目标系统

4.木马隐藏

5.攻击意图实现，**激活木马**

- **特洛伊木马技术**

特洛伊木马植入技术

特洛伊木马隐藏技术

特洛伊木马存活技术

- **特洛伊木马防范技术**

1. 基于查看开放端口检测特洛伊木马技术
2. 基于重要系统文件检测特洛伊木马技术
3. 基于系统注册表　检测特洛伊木马技术
4. 检测具有隐藏能力的特洛伊木马技术
5. 基于网络检测特洛伊木马技术
6. 基于网络阻断特洛伊木马技术
7. 清除特洛伊木马技术

## 14.4 网络蠕虫分析与防护

· 概念/特点：

网络蠕虫是一种具有自我复制和传播能力、可独立运行的恶意程序。

**1988年 “小莫里斯”蠕虫事件， 首例蠕虫攻击**

· 网络蠕虫组成部件

四个构成模块：探测、传播、蠕虫引擎、负载

· 运行机制

第一阶段：已感染蠕虫的主机再网络上搜索易感染目标主机

第二阶段：已经感染蠕虫的主机把蠕虫代码传送到易感染目标主机上

第三阶段：执行蠕虫代码，感染目标主机系统

· 网络蠕虫常用技术

1.网络蠕虫扫描技术

随机扫描

顺序扫描

选择性扫描

2.网络蠕虫漏洞利用技术

·主机间的信任关系漏洞

·目标主机的程序漏洞

·目标主机的默认用户和口令漏洞

·目标主机的用户安全意识和薄弱漏洞

·目标主机的客户端程序配置漏洞

·网络蠕虫防范技术

1.网络蠕虫检测与预警技术

2.网络蠕虫传播抑制技术

3.网络系统漏洞检测与系统加固技术

4.网络蠕虫免疫技术

5.网络蠕虫阻断与隔离技术

6.网络蠕虫清除技术

## 14.5 僵尸网络分析与防护

·概念

僵尸网络是指攻击者利用入侵手段将僵尸程序植入目标计算机上，进而操纵受害机执行恶意活动的网络。

**（其实就是抓肉鸡）**

·特性

·运行机制 （尽可能精简）

第一步：僵尸程序的传播

第二步：对僵尸程序进行远程命令操作和控制，将受害者组成一个网络

第三步：总控发送指令

·防范技术

1.僵尸网络威胁检测

2.僵尸网络检测

3.僵尸网络主动遏制

4.僵尸程序查杀

## 14.6 其他恶意代码分析与防护

·逻辑炸弹

·陷门（理解为程序后门、程序漏洞点）

·细菌（顾名思义，自我复制，消耗系统资源）

·间谍软件

## 14.7 恶意代码防护主要技术指标与产品（重要性高点 ★★★）

· 恶意代码防护主要技术指标

1.恶意代码**检测能力**

2.恶意代码**检测准确性**

3.恶意代码**阻断能力**

· 恶意代码防护产品

终端防护类产品

安全网关产品

恶意代码检测类产品

补丁管理系统

恶意代码应急响应 类产品

### 14.8 恶意代码防护技术应用 ★★★★

·终端恶意代码防护

·APT防护

(电子文档及电子邮件恶意代码防护)

# 第15章 网络安全主动防御技术与应用

(就是入侵防御系统 IPS)

### 15.1

·入侵阻断技术原理

~~· IPS 入侵防御系统的工作基本原理是根据网络包的特性及上下文 进行攻击行为判断来控制包转发~~ (其实就是检测到攻击行为并阻断)

· SPS基于旁路阻断

·入侵阻断技术应用

IPS/SPS的主要作用是过滤掉有害的网络信息流，阻断入侵者对目标的攻击行为。

### 15.2

·软件白名单技术原理

**(原理已经知道了，不记录)**

·软件白名单技术应用

1.构建安全、可信的移动互联网安全生态环境

2.恶意代码防护

3.“白环境”保护

PS:提醒 时刻牢记，这里是选择题部分，所以内容不需要记太细。

15.3

·网络流量清洗技术原理

1. 流量监测
2. 流量牵引与清洗
3. 流量回注

·网络流量清洗技术应用

1.畸形数据报文过滤
2.抗拒绝服务供给
3.Web应用保护
4.DDoS高防IP服务

15.4

·可信计算技术原理

首先构建一个信任根，再建立一条信任链，从信任根开始到硬件平台，到操作系统，再到应用，一级认证一级，一级信任一级，把这种信任扩展到整个计算机系统，从而确保整个计算机系统的可信。

·可信计算技术应用

1.计算平台安全保护
2.可信网络连接
3.可信验证

15.5

数字水印技术原理

数字水印是指通过数字信号处理方法，在数字化的媒体文件中嵌入特定的标记。

水印分为**可感知的**和**不易感知的。**

数字水印技术通常由**水印的嵌入**和**水印的提取**两个部分组成。

嵌入方法：

空间域方法

变换域方法

**数字水印技术应用 ★★**

1.版权保护

2.信息隐藏

3.信息溯源

4.访问控制

15.6

网络攻击陷阱技术原理

1. 蜜罐主机技术

2. 陷阱网络技术（多蜜罐+网络复杂版）

网络攻击陷阱技术应用

1.恶意代码监测

2.增强抗攻击能力

3.网络态势感知

15.7

入侵容忍及系统生存技术原理

假定遭受乳清的情况下，保障网络信息系统仍能按用户要求完成任务。

入侵容忍及系统生存技术应用

1. 弹性CA系统

2. 区块链

15.8

隐私保护技术原理

隐私保护技术应用

1.匿名化处理个人信息

2.对个人信息去标识化处理

**15.9 网络安全前沿技术发展动向 ★★★**

·网络威胁情报服务

·域名服务安全保障

·同态加密技术

# 第16章 网络安全风险评估技术原理与应用

16.1 网络安全风险评估概述

· 网络安全风险评估概念

评估威胁者利用网络**资产的脆弱性** 造成**网络资产损失**的**严重程度。**

• **网络安全风险评估要素 ★★★★★**

资产、威胁、脆弱性、安全措施、风险

· 网络安全风险评估模式

1.自评估

2.检查评估

3.委托评估

16.2 评估过程

网络安全风险评估准备

网络资产识别

网络安全威胁识别

网络安全脆弱性识别

已有安全措施确认

网络安全风险计算与分析

网络安全风险应对措施

16.3 网络安全风险评估技术方法与工具

· 资产信息收集

· 网扩扑发现

· 网络安全漏洞扫描

· 人工检查

· 网络安全渗透测试

· 问卷调查

· 网络安全访谈

· 审计数据分析

· 入侵监测

16.4 网络安全风险评估流程和工作内容

· 评估工程前期准备

· 评估方案设计与论证

· 评估方案实施

· 风险评估报告撰写

· 评估结果评审与认可

16.5 网络安全风险评估技术应用

· 网络安全风险评估应用场景

· OWASP风险评估方法参考

· ICT供应链安全威胁识别参考
· 工业控制系统平台脆弱性识别参考
· 网络安全风险处理措施参考
· 人工智能安全风险分析参考

# 第17章 网络安全应急响应技术原理与应用 ★★★★★

17.1

网络安全应急响应概念

网络安全应急响应是指为应对网络安全事件，相关人员或组织机构对网络安全事件进行**监测**、**预警**、**分析**、**响应**和**恢复**的工作。

网络安全应急响应作用

及时**响应**和**处理**网络中随时可能出现的安全事件。

网络安全应急响应相关规范

《信息安全技术 信息系统安全管理要求》
《信息安全技术 信息安全事件分类分级指南》
《信息安全技术 信息系统灾难恢复规范》
《信息安全技术 灾难恢复中心建设与运维管理规范》

17.2

网络安全应急响应组织建立

网络安全应急响应组织工作机制

网络安全应急响应组织类型

1. 公益性应急响应组

2. 内部应急响应组

3. 商业性应急响应组

4. 厂商应急响应组

17.3

**网络安全事件分类：** ★★★★★

**2017**年**中央网信办**发布**《国家网络安全事件应急预案》**，将网络信息安全事件定为以下7个基本分类。

网络攻击事件

恶意程序事件

信息破坏事件

信息内容安全事件

设备设施故障

灾害性事件

其他信息安全实际

**网络安全事件分级：** ★★★★★

| 网络安全事件级别 | 描述 |
| --- | --- |
| **特别重大**网络安全事件（Ⅰ级） | 特别严重威胁、特别严重影响 |
| **重大**网络安全事件（Ⅱ级） | 严重威胁、严重影响 |
| **较大**网络安全事件（Ⅲ级） | 较严重威胁、较严重影响 |
| **一般**网络安全事件（Ⅳ级） | 一定威胁、一定影响 |

**17.3 网络安全应急响应预案内容** （不重要）

·详细列出系统紧急情况的类型及处理措施

·事件处理基本工作流程

·应急处理所采取的具体步骤及操作顺序

·执行预案有关人员的姓名、住址、电话号码以及有关职能的联系方法。

网络安全应急响应预案类型

**17.4**

常见网络安全应急事件处理流程

第一步：安全事件报警

第二步：安全事件确认

第三步：启动应急预案

第四步：安全事件处理

第五步：撰写安全事件报告

第六步：应急工作总结

网络安全事件应急演练类型

按组织形式分：

桌面应急演练

实战应急演练

按内容分：

单项应急演练

综合应急演练

按目的与作用分：

检验性应急演练

示范性应急演练

研究性应急演练

演练方式：CTF夺旗赛/红蓝对抗赛、网络攻防平台

17.5 网络安全应急响应技术与常见工具

· 访问控制

· 网络安全评估

~~1.恶意代码检测~~

~~2.漏洞扫描~~

~~3.文件完整性检测~~

~~4.系统配置文件检测~~

~~5.网卡混杂模式检查~~

~~6.文件系统检查~~

~~7.日志文件审查~~

· 网络安全监测

工具：tcpdump、wireshark、tcpview、netstat

windows自带：

进程：任务管理器、PsTools

网络：netstat、net、fport

Unix/Linux：

进程：ps

网络：netstat、lsof

· 系统恢复

1.系统紧急启动

2.恶意代码清除

3.系统漏洞修补

4.文件删除恢复

5.系统备份容灾

· 入侵取证

1.证据获取 ： 日志、ipconfig等命令

2.证据安全保护： md5sum、Tripwire等

3.证据分析: grep find 、 gdb 等

17. 6 网络安全应急响应参考案例

# 第18章 网络安全测评技术与标准

18.1 **（这种基本概念不用怎么记，过一遍就行。有个大致了解，选择题不会选错就行。）**

网络安全测评概念：

获取状况信息，给出判定。

网络安全测评发展：

网络安全测评作用：

18.2 网络安全测评类型 **（感觉也记不下来呀）**

·基于测评目标分类

1.网络信息系统安全等级测评

2.网络信息系统安全验收测评

3.网络信息系统安全风险测评

·基于测评内容分类

1.技术安全测评

2.管理安全测评

·基于实施方式分类

1.安全功能检测

2.安全管理检测

3.代码安全审查

4.网络安全渗透

5.信息系统攻击测试

·基于测评对象保密性分类

1.涉密信息系统测评

2.非涉密信息系统测评

18.3网络安全测评流程与内容 **（内容多而杂，直接忽略）**

18.4测评技术与工具

18.5网络安全测评质量管理与标准

第19章 操作系统安全保护

19.1

19.2

19.3

**19.4 国产操作系统安全分析与防护 （国产嘛，应该会重要点）**

国产操作系统在自主可控、安全可信方面，对开源Linux进行安全增强。

包括管理员分权、最小特权、结合角色的基于类型的访问、细粒度的自主访问控制、多级安全。

下列系统都过了第三级、第四级保护：

1.中科方德安全操作系统

2.中标麒麟安全操作系统

3.中标麒麟可信操作系统

# 第20章 数据库保护

Mssql、 Mysql、**Oracle、DB2**

数据库安全隐患

1.数据库用户账号和密码隐患

- oracle内部密码：**ORCL**
- oracle监听进程密码保存在listener.ora中
- ……

2.数据库系统扩展存储过程隐患

对于Sybase和Sql Server，入侵者只要登录为“sa”,就可以使用扩展存储过程xp_cmdshell,从而执行系统命令。

……

7.MS SQL Server不能删除sa账户，sa默认是空口令。

**国产数据库**

**神舟数据、人大金仓、达梦（DM）、安捷**

# 第21章 网络设备安全

（交换机、路由器）

## 21.1

**交换机安全威胁**

1.MAC地址泛洪

伪造大量的虚假mac地址，填满交换机有限的mac地址表，致使其不再记录其他mac地址。

2.ARP欺骗

3.口令威胁

4.漏洞利用

**路由器安全威胁**

1.漏洞利用

2.口令安全威胁

3.路由协议安全威胁

4.DOS/DDOS威胁

5.依赖性威胁：破坏路由器依赖的服务或环境

## 21.2 网络设备安全机制与实现技术

> ·认证机制
> ·访问控制
> ·信息加密
> ·安全通信
> ·日志审计
> ·安全增强
> ·物理安全

## 21.3 网络设置安全增强技术方法

·交换机安全增强技术方法

1. 配置交换机访问口令和ACL以限制安全登录
2. 利用镜像技术监测网络流量
3. MAC地址控制技术
4. 安全增强

·路由器安全增强技术方法

1. 及时审计操作系统和打补丁
2. 关闭不需要的网络服务
3. 明确禁止不使用的端口
4. 禁止IP直接广播和源路由
5. 增强路由器VTY安全
6. 阻断恶意数据包
7. 路由器口令安全
8. 传输加密
9. 增强路由器SNMP的安全

## 21.4 网络设备厂家漏洞与解决方法

· 网络设备常见漏洞

1. 拒绝服务漏洞
2. 跨站伪造请求CSRF

3.格式化字符漏洞

4.XSS

5.旁路

6.代码执行

7.溢出

8.内存破坏

·解决方法

1.及时获取网络设备漏洞信息

2.网络设备漏洞扫描

3.网络设备漏洞修补

**（再次提醒：选择题区域快速过，重点在主观题）**

考纲例题：

BCC

## 三、题 型 举 例

### 考试科目 1：网络信息安全基础知识和技术

1. 攻击者利用 John the Ripper 工具对目标服务器进行攻击，则此攻击者所利用的方法是__（1）__。

（1）A. 会话劫持　　B. 口令破解

C. 端口扫描　　D. 拒绝服务

2. VPN 产品的安全实现技术主要是__（2）__。

（2）A. RFC、IPSec　　B. XML、BGP

C. SSL、IPSec　　D. BGP、OSPF

3. 网络中的明文传输容易造成信息泄露，为了抵御网络监听，常用的技术方法是__（3）__。

（3）A. SSL、OSPF　　B. IPSec、SNMP

C. SSL、IPSec　　D. OSPF、SNMP

4. Network firewalls operate at different layers of the __(4)__ and TCP/IP network models. The lowest layer at which a firewall can operate is the third level which is the network layer for the OSI model and the Internet Protocol layer for TCP/IP. At this layer a firewall can determine if a packet is from a __(5)__ source but cannot grant or deny access based on what it contains. Firewalls that operate at the highest layer, which is the application layer, know a large amount of information including the source and the packet __(6)__. Therefore, they can be much more selective in granting access. This may give the impression that firewalls functioning at a higher layer must be better, which is not necessarily the case. The lower the layer at which the packet is intercepted, the more secure the system is. If the __(7)__ cannot get past the third layer, it is impossible to gain control of the operating system.

Application level gateways or proxies operate at the application layer. Packets received or leaving cannot access services for which there is __(8)__. Stateful multilayer inspection firewalls combine aspects of the other three types of firewalls.

(4) A. OSI　　B. ISO
　　C. SMTP　　D. IDS

(5) A. active　　B. old
　　C. trusted　　D. new

(6) A. virus　　B. address
　　C. contents　　D. password

(7) A. dog　　B. bird
　　C. intruder　　D. tiger



(8) A. no proxy　　B. no OS
　　C. no VPN　　D. no Desktop