中国通信企业协会网络安全人员能力认证考试知识点大纲

技术类专业级(CACE-CPAC-PLT)

中国通信企业协会网络安全人员能力认证中心

2017 年 3 月

目录

第一部分综述

第1章 政策法规及道德规范

1.1 国家网络安全相关法律法规

了解国家安全委员会和中央网络安全和信息化领导小组，重点领会总书记“419”讲话内容和精神。

1.1.1我国网络安全管理体制

了解我国各级网络安全管理部门之间的关系和各自职责。

1.1.2网络安全相关法律法规

了解“国家网络空间主权”提法的出处，了解维护网络和信息安全的核心任务。了解《网络安全法》基本内容。了解《电信条例》基本内容。

1.1.3信息安全等级保护相关法规政策

了解《关于信息安全等级保护工作的实施意见》和《信息安全等级保护管理办法》的基本内容和要求。

1.2 电信和互联网行业网络安全管理政策

1.2.1通信网络安全相关法规政策

了解《通信网络安全防护办法》的基本内容和要求；了解《电信和互联网用户个人信息保护规定》基本内容和要求；了解《关于加强电信和互联网行业网络安全工作的指导意见》的八项工作任务。

1.2.2网络安全防护

了解安全防护的原则、方针和理念；了解定级备案的要求，了解符合性评测和风险评估的要求。了解网络安全防护监督检查工作内容。

1.2.3网络安全威胁治理

了解网络安全威胁治理相关的技术手段建设和管理情况。

1.2.4网络安全应急保障

了解《公共互联网网络安全应急预案》基本内容，了解预警分级、监测上报、应急响应的基本流程和要求。

1.3 道德规范

主要了解网络安全从业人员应当遵守的相关道德规范。相关道德规范具体可以分为通行道德规范和职业道德规范，无论通行道德规范和职业道德规范，网络安全从业人员都应遵守，道德规范是对网络安全从业人员的基本要求。

第2章 安全管理标准

2.1 国外主要标准介绍

1) 了解国外信息安全管理标准的演进历程
2) 了解各项安全标准的差异性

2.2 国内主要安全标准概述

了解我国发布关于信息安全的标准名称

2.3 国内外安全管理标准的对比

1) 了解国内外安全标准的差异

2) 了解国内外安全标准的共性

第3章 安全体系框架

3.1 安全体系设计的指导思想与理念

了解安全体系设计的指导思想与理念

3.2 安全技术体系框架及主要内容

1) 了解安全技术体系设计所具备的安全能力

2) 了解安全技术体系框架的五个维度，以及每个维度涉及的内容

3.3 安全技术体系框架设计的落地

1) 掌握设计实施路线图的方法

2) 了解几类方式触发对信息安全保障体系改进的方式

第二部分通用网络安全技术原理

第4章 密码技术

4.1 加密算法与编码技术

4.1.1对称加密算法与编码技术

1) 了解对称加密算法的概念和基础知识
2) 了解 DES 算法原理
3) 了解编码技术的知识和分类
4) 掌握对称加密与编码技术的区别

4.1.2非对称加密算法与编码技术

1) 了解非对称加密算法的概念、特点
2) 了解 RSA 算法原理
3) 了解编码技术的概念
4) 掌握非对称加密和编码技术的关系

4.2 常见密码技术原理

4.2.1经典加密算法

1) 了解经典加密算法的基础知识
2) 了解经典加密算法的分类
3) 掌握各类算法的原理

4.2.2现代加密算法

1) 了解现代加密算法的基础知识
2) 了解现代加密算法的分类
3) 掌握各类算法的原理

4.3 高级加密标准

4.3.1高级加密标准简介

1) 了解高级加密的标准
2) 了解高级加密算法的由来
3) 了解高级加密算法的定义

4.3.2实现

1) 了解高级加密算法 AES 的算法原理
2) 掌握 AES 原理的举例

4.3.3实用的攻击

1) 了解实际攻击的场景
2) 了解三个方面的技术原理

4.3.4链接模式

1) 了解高级加密中的链接模式的知识
2) 了解高级加密的五种工作体制

4.4 PKI 技术

4.4.1PKI 技术概述

1) 了解 PKI 技术的概念

2) 了解 PKI 技术在当今时代的重要性

4.4.2PKI 技术发展

1) 了解 PKI 的技术发展

2) 了解无限 PKI

4.4.3PKI 系统组成

1) 了解 PKI 域的标准

2) 了解 PKI 域的七个内容

4.4.4PKI 原理

1) 了解公钥基础设施的算法原理

2) 掌握公共密钥算法

4.4.5安全服务

1) 了解 PKI 在安全服务中的实施办法

2) 了解 PKI 能解决的问题

4.4.6PKI 与防火墙等其他技术

1) 了解 PKI 技术

2) 了解防火墙技术

3) 掌握 PKI 和防火墙的关系

4.5 密码破解技术

4.5.1密码分析学

1) 了解密码学的由来和概念

2) 了解密码学从古至今的发展状

4.5.2常用软件的口令加密和存储方法

1) 掌握 DES、AES、RSA、Base64、MD5、SHA1 的加密算法

2) 了解加密算法的存储方式

4.5.3密码破解实现

1) 了解密码破解的实现方式

2) 掌握常见的几种密码破解的方式

4.6 密钥管理、数字签名、散列函数与证书

4.6.1概述

1) 了解密钥管理的概念和具体实施办法

2) 了解数字签名的概念、特点及发展

3) 了解哈希函数的概念、原理

4) 了解数字证书认证机构的特点和认证流程

4.6.2密钥交换

1) 掌握密钥交换的两种实现机制

2) 了解密钥交换的基本概念

4.6.3可靠性

1) 掌握密码的传输可靠性
2) 了解密码的保护措施

4.6.4数字签名

1) 了解数字签名在安全领域的作用
2) 掌握数字签名的几种方式
3) 了解数字签名的标准

4.6.5公钥基础设施和证书

1) 了解 PKI 的标准
2) 了解 PKI 的一些基本组件
3) 了解不同组件提供的不同服务

4.7 密码学的的未来

4.7.1量子密码学简介

1) 了解量子密码学的概念
2) 了解量子密码学的由来
3) 了解量子密码学的发展

4.7.2量子系统概述

1) 了解量子系统的概念、原理
2) 掌握从数学角度分析量子系统的知识

4.7.3量子因子分解

1) 掌握影响因子分解的因素
2) 了解因子分解的过程

4.7.4量子密钥管理

1) 了解量子密钥有效的管理方法
2) 掌握三大实现方案和具体步骤

第5章 第五章安全协议

5.1 安全协议分析

5.1.1安全协议的安全性

1. 安全协议基础知识
    1) 了解当今网络安全形式
    2) 了解安全协议的概念
2. 安全协议的安全性
    1) 了解安全协议的安全性
    2) 了解安全协议的重要性及协议存在的各类缺陷问题

5.1.2安全分析的基本方法

1) 了解安全协议进行安全分析主要方法分类
2) 了解攻击检验方法进行安全分析的过程
3) 了解形式化分析方法进行安全分析的过程
4) 掌握攻击检测方法与形式化分析方法的具体内容

5.1.3典型网络安全协议分析

1) 了解现有网络安全协议中常见的安全协议
2) 了解 SSH 协议在网络协议中具体所处位置及功能
3) 了解 SSL 协议在网络协议中具体所处位置及功能
4) 了解 IPSEC 协议在网络协议中具体所处位置及功能

5.2 TCP/IP 协议分析

1) 了解 TCP/IP 协议的概念说明
2) 了解 TCP/IP 协议的层次划分
3) 了解 TCP/IP 协议与 OSI 七层参考模型的区别对比
4) 掌握 TCP/IP 协议各层次划分及主要内容
5) 掌握网络接口层的特点、功能及常见协议
6) 掌握网络层的特点、功能及常见协议
7) 掌握传输层的特点、功能及常见协议
8) 掌握应用层的特点、功能及常见协议

5.3 网络接口层协议分析

5.3.1WEP 协议

1) 了解 WEP 协议的概念、发展过程。
2) 了解 WEP 协议的两种类型方式
3) 掌握 WEP 协议的开放式系统认证类型的概念与实现过程
4) 掌握 WEP 协议的共有键认证类型的概念与实现过程
5) 掌握 WEP 协议的两种类型方式的区别

5.3.2WPA 协议

1) 了解 WAP 协议的概念与在系统内的功能体现

2) 了解 WAP 协议数据加密协议 TKIP 协议

3) 掌握 WAP 协议的加密过程

5.4 网际层协议分析--虚拟专用网络协议（IPSEC）

5.4.1VPN

1) 了解 VPN 的概念、功能

2) 了解不同的 VPN 技术在 OSI 各层协议的实现

3) 了解 PPTP 协议的具体实现过程

4) 掌握 PPTP 协议的工作方式

5) 了解 VPN 数据封装的模式

5.4.2IPSEC

1) 了解 IPSEC 的基本内容、功能特点

2) 了解 IPSEC 协议的组成部分

3) 了解 IPSEC 协议的工作模式及分类

4) 了解 IPSEC 协议密钥配置与协商方式

5) 了解掌握 IPSEC 的安全特性

6) 掌握加密方式及各种加密支持的安全特性

7) 掌握 IPSEC 密钥管理模式

5.5 传输层安全分析

5.5.1TLS/SSL 协议

1) 了解 TLS、SSL 协议的功能特点、发展过程。

2) 了解 TLS 协议的结构特点

3) 掌握 TLS 与 SSL 协议的差异

4) 掌握 TLS 相对于 SSL 协议主要增强的内容

5.5.2Socks 协议

1) 了解 Socks 协议的概念及功能
2) 了解 Socks 协议在 OSI 模型中的位置
3) 掌握 SOCKS 协议执行功能的过程
4) 了解 SocksV5 的特点

5.6 应用层协议分析

5.6.1SSH 协议

1) 了解 SSH 协议的概念、功能特点
2) 掌握 SSH 协议在网络层次中的应用
3) 掌握 SSH 协议框架的主要部分
4) 了解主机密钥机制
5) 掌握针对 SSH 协议常见攻击及协议防范对策

5.6.2SET 协议

1) 了解 SET 协议的功能和实现的目标
2) 了解 SET 协议交易参与方的内容
3) 了解 SET 协议的工作原理
4) 掌握 SET 协议应用的加密算法、密码技术等安全技术手段
5) 掌握 SET 协议加密、解密的方法
6) 了解 SET 协议的安全性分析

5.6.3kerberos 协议

1) 了解 kerberos 协议的基本原理
2) 了解 kerberos 协议具体工作流程
3) 了解 kerberos 协议存在哪些安全缺陷和相对应的弥补措施

5.7 几种常见安全协议的对比

5.7.1网络认证协议 Kerberos

1) 了解 kerberos 网络认证协议在 TCP/IP 协议栈中所处的层次
2) 了解 kerberos 协议所能承担的安全服务
3) 了解 Kerberos 协议的加密机制
4) 了解 Kerberos 协议的应用领域
5) 了解 Kerberos 协议的优缺点

5.7.2安全电子交易协议 SET

1) 了解 SET 安全电子交易协议在 TCP/IP 协议栈中所处的层次
2) 了解 SET 协议所能承担的安全服务
3) 了解 SET 协议的加密机制
4) 了解 SET 协议的应用领域
5) 了解 SET 协议的优缺点

5.7.3安全套接层协议 SSL

1) 了解 SSL 安全套接字协议在 TCP/IP 协议栈中所处的层次
2) 了解 SSL 协议所能承担的安全服务
3) 了解 SSL 协议的加密机制
4) 了解 SSL 协议的应用领域
5) 了解 SSL 协议的优缺点

5.7.4安全超文本传输协议 SHTTP

1) 了解 SHTTP 安全超文本传输协议在 TCP/IP 协议栈中所处的层次
2) 了解 SHTTP 协议所能承担的安全服务
3) 了解 SHTTP 协议的加密机制

4) 了解 SHTTP 协议的应用领域

5) 了解 SHTTP 协议的优缺点

5.7.5安全电子邮件协议 S/MIME

1) 了解 S/MIME 安全电子邮件协议在 TCP/IP 协议栈中所处的层次

2) 了解 S/MIME 协议所能承担的安全服务

3) 了解 S/MIME 协议的加密机制

4) 了解 S/MIME 协议的应用领域

5) 了解 S/MIME 协议的优缺点

5.7.6安全协议对比分析

1) 了解 SSL 与 IPSec 协议在功能、应用层次、系统需求等问题上的对比和不同

2) 了解 SSL 与 SET 协议在功能、应用层次、安全性、系统需求等问题上的对比和不同

3) 了解 SSL 与 S/MIME 协议在功能、应用效果、安全性、系统需求等问题上的对比与不同

4) 了解 SSL 与 SHTTP 协议在功能、应用效果、安全性、系统需求等问题上的对比与不同

5.7.7总结

1) 了解网络安全协议各自的优缺点

2) 了解各种安全协议的特性

3) 了解如何学习与对待各种安全协议

第6章 网络安全攻击技术

6.1 网络攻击技术原理

6.1.1网络欺骗

1) 掌握常见的欺骗方式

2) 了解电子邮件欺骗传输协议，SMTP 服务、网络钓鱼社会工程攻击

3) 了解 dns 缓存感染，DNS 信息劫持，DNS 重定向

4) 掌握常见的欺骗方式

6.1.2嗅探技术

1) 了解网络嗅探技术的会话劫持和 ip 欺骗

2) 掌握 arp 欺骗方式

6.1.3扫描技术

1) 了解扫描方法

2) 掌握使用扫描技术获取敏感信息

6.1.4口令破解技术

1) 了解常见的口令破解技术，暴力穷举、击键记录、屏幕记录、Sniffer 等等 13 中攻击技术

2) 掌握常见的暴力破解攻击方式，及社会工程学，撞库等造成的口令破解

6.1.5缓冲区溢出攻击

1) 了解超过缓冲区大小的数据造成破坏程序的堆栈

2) 掌握发现非正常内存空间，利用堆栈地址，执行溢出指令

6.1.6SQL 注入

1. SQL 注入

1) 了解常见 SQL 注入的产生原因，攻击方式的分类。

2) 了解 sql 注入造成的非法数据获取。及检查变量数据类型和格式、过滤特殊符号、绑定变量、使用预编译语句、数据库信息加密安全等防御方式

3) 掌握 sql 注入产生原因，判断存在 sql 注入的技巧，及特殊字符的过滤技巧

2. GET 型注入

1) 了解 GET 型注入的定义、以及请求方式

3. POST 注入

1) 了解 POST 注入概念、传递参数的方式。

2) 掌握 POST 注入的利用方法

4. 知识子域：Cookie 注入

1) 了解 Cookie 注入定义、参数提交方式

2) 掌握 Cookie 注入的利用方式

5. 二次注入以及伪静态注入

1) 了解二次注入以及伪静态注入的相关基础知识

2) 掌握二次注入以及伪静态注入的注入方法

6.1.7恶意代码

1) 了解恶意代码的定义及传播方式

2) 掌握媒介的传播方式，寄生和感染特性的恶意代的攻击方式

6.2 网络安全攻击事件案例和原理分析

6.2.1国内事件

1) 了解京东数据泄漏事件，Struts 2 漏洞相关信息导致大量数据泄露

2) 掌握常见攻击事件造成的影响

3) 京东数据泄漏事件

6.2.2国外事件

1) 了解 DNS 服务提供商 Dyn 的 DDoS 攻击事件的详细信息

2) 掌握常见攻击事件造成的影响

6.3 黑客与攻击技术实战分析

6.3.1僵尸网络

1) 了解僵尸网络的相关漏洞信生命周期
2) 了解采用扫描模块、驻留模块、功能模块的攻击方法
3) 了解僵尸网络的危害特点，传播方式，ZeroAccess 检测方法
4) 了解相关僵尸网络漏洞攻击事件
5) 掌握僵尸网络的攻击方式，检测方法，防护办法

6.3.2缓冲区溢出攻击

1) 了解缓冲区漏洞攻击缓冲区溢出可以获得系统的权限
2) 了解全局缓冲区攻击，相关堆栈溢出方式，函数调用时的堆栈变化，及利用代码
3) 掌握常见程序设计缺陷、获取程序乃至系统的控制权

6.3.3拒绝服务攻击

1) 了解带宽消耗型以及资源消耗型拒绝服务攻击方式
2) 了解相关 User Datagram Protocol（UDP）floods、ICMP floods、等僵攻击手段，针对入侵检测，流量过滤和多重验证等进行相关的防御
3) 掌握常见 dos 攻击攻击现象，漏洞工具，防范措施

6.3.4分布式拒绝服务攻击

1) 了解分布式服务攻击，基于 ARP、 ICMP、 IP、UDP、TCP 的攻击和基于应用层的攻击概述
2) 掌握并分析其特点，现象，攻击方式，相关利用工具，及防御方式
3) 什么是分布式拒绝服务攻击

6.4 网络安全入侵实战

6.4.1命令行下的入侵

1) 了解 mysql 配置不当配置不当导致的入侵，从基本端口探测，弱口令信息泄露。到进一步的提权，获取到最高权限。
2) 掌握常见的漏洞攻击方式

6.4.2图形界面的入侵等

1) 了解在使用漏洞扫描器发现漏洞进行入侵攻击的手段
2) 掌握一些工具的使用方法及利用方式

6.4.3流行远程控制木马的使用方法

1) 了解灰鸽子控制木马和之后衍生的远程控制软件的利用方法
2) 掌握灰鸽子的利用方式，及衍生的远程控制软件的自动上线
3) 灰鸽子概述
4) 灰鸽子简单的说它是远程监控软件,（黑客类）,当然也可以说他是一个病毒.木马或则说是后门之类的恶意软件

6.4.4键盘记录程序的使用方法

1) 了解 metasploit 获取到 meterperter 的 session 的键盘记录控制
2) 掌握常见的键盘记录工具的使用方法

6.5 网络安全攻击防范技术分析

6.5.1Windows 命令行工具

1) 了解防范 windows 命令行的攻击之组策略配置
2) 掌握常见的命令行获取敏感信息办法及对应的防范技术

6.5.2攻击检测和防范方法之日志分析

1) 了解 linux 进行日志设置，相关服务的详细配置，相关用户账户管理配置

2) 掌握日志审计工作的必要性，监测常见攻击技术手段

6.5.3针对 SOAP 的渗透测试与防护

1) 了解常见配置不当引起的漏洞进而获取敏感信息

2) 掌握针对 SOAP 的渗透测试与防护

第三部分风险评估

第7章 风险评估实施流程

7.1 风险评估准备工作

7.1.1组建风险评估项目团队

1) 了解直接或间接参与风险评估的角色
2) 理解参与风险评估人员的工作职责
3) 了解参与风险评估人员的关系

7.1.2确定风险评估范围

1) 理解信息安全的覆盖层面
2) 理解风险评估的对象
3) 理解风险评估的范围

7.1.3确定风险评估方式

1) 理解风险评估的形式
2) 理解自评估的内容
3) 理解检查评估的内容
4) 理解自评估与检查评估的区别

7.1.4制定风险评估计划

1) 掌握风险评估计划的内容
2) 掌握风险评估的过程

7.2 风险评估实施流程

7.2.1风险要素识别

1) 理解风险的基本要素
2) 理解风险要素之间的关系
3) 理解风险要素识别的内容

7.2.2风险分析

1) 理解风险计算模型
2) 理解可能性计算
3) 理解影响计算
4) 理解风险计算

7.2.3风险处置

1) 理解风险处理的方式
2) 理解每种方式的具体措施

7.3 建立风险评估工作长效机制

1) 理解风险评估是一个动态的过程
2) 理解建立风险评估的长效机制

第8章 风险识别与评价

8.1 资产识别

1) 理解资产的分类
2) 理解如何识别资产
3) 理解识别资产的重要性

8.2 威胁识别

1) 理解威胁的概念
2) 掌握威胁的分类
3) 掌握威胁度量的属性
4) 掌握威胁的获取
5) 理解识别威胁的过程

8.3 脆弱性识别

1) 理解脆弱性的概念
2) 掌握脆弱性识别的内容
3) 掌握脆弱性识别的手段
4) 理解脆弱性识别的过程
5) 掌握脆弱性的度量

8.4 已有安全措施的确认

1) 理解安全措施的分类
2) 掌握安全措施识别的方法
3) 理解安全措施识别的过程

8.5 风险评价

8.5.1风险计算原理

1) 理解风险计算的过程
2) 理解风险计算的要素
3) 掌握可能性的计算
4) 掌握影响的计算

5) 掌握风险的计算

8.5.2风险结果的判定

1) 理解风险结果的作用于意义
2) 理解风险的优先级

8.5.3控制措施的选择

1) 理解风险处理方式
2) 理解控制措施的分类
3) 理解控制措施的选择原则

8.5.4残余风险的评价

1) 理解残余风险的含义
2) 理解对残余风险的处理
3) 理解风险评估结果的输出

第9章 扫描、渗透及常用工具

9.1 扫描工具

9.1.1Nmap

1) 掌握 nmap 的安装
2) 理解 nmap 的功能
3) 掌握 nmap 的基本用法
4) 理解 nmap 的使用场景

9.1.2Nessus

1) 掌握 Nessus 的安装
2) 理解 Nessus 的功能
3) 掌握 nessus 的使用方式

9.1.3Appscan

1) 掌握 Appscan 的安装
2) 理解 Appscan 的功能
3) 掌握使用 Appscan 对 web 网站扫描

9.2 弱口令探测工具

9.2.1hydra

1) 理解 hydra 的功能
2) 掌握 hydra 的基本用法

9.2.2medusa

1) 理解 medusa 的功能
2) 掌握 medusa 的基本用法

9.2.3cain

1) 理解 cain 的功能
2) 掌握使用 Cain 嗅探欺骗基本用法

9.3 嗅探工具

9.3.1ettercap

1) 理解 ettercap 的功能

2) 掌握 ettercap 的用法

9.3.2wireshark

1) 理解 wireshark 的功能

2) 掌握 wireshark 的抓包分析用法

9.4 WEB 系统渗透工具

9.4.1BurpSuite

1) 理解 burp 的功能

2) 掌握 burp 的捕获分析数据包功能

9.4.2SQLmap

1) 理解 sqlmap 的功能

2) 掌握 sqlmap 的基本用法

9.5 漏洞利用工具

1) 理解 metasploit 工具的功能

2) 掌握 metasploit 的用法

第10章 风险评估报告

10.1 风险评估报告的形式

理解风险评估报告的内容

10.2 风险评估结果分析

1) 理解降低风险的方式
2) 理解风险控制的方法

第11章 安全加固与整改

11.1 技术加固安全基线

1) 理解加固基线的基本内容
2) 理解加固过程中存在的风险
3) 理解应对加固过程中风险的措施

11.2 加固内容

1) 理解网络设备加固要点
2) 理解操作系统的加固要点
3) 理解数据库加固要点

11.3 加固流程

1) 理解加固流程的阶段
2) 理解每个阶段的内容

第四部分网络安全防护

第12章 网络安全设备

12.1 防火墙

12.1.1 防火墙策略

1) 理解防火墙的安全策略作用
2) 理解防火墙的处理规则方式
3) 理解默认拒绝策略
4) 理解默认允许策略

12.1.2 防火墙配置和应用

1) 理解防火墙安装配置的内容
2) 理解防火墙的规则内容
3) 理解防火墙处理包的过程

12.1.3 防火墙日志分析

1) 理解防火墙日志的内容
2) 了解常见的防火墙日志分析工具

12.1.4 绕过防火墙的主要攻击方法

1) 了解防火墙攻击方法
2) 了解防火墙绕过的方法

12.2 IDS

12.2.1 IDS 核心技术

1) 理解入侵检测的作用

2) 理解入侵检测的两种分类：异常检测、误用检测

12.2.2 IDS 发展趋势

1) 了解 IDS 未来发展趋势

2) 了解 IDS 发展的不同方向

12.2.3 下一代 IPS

1) 了解 NIPS 的概念

2) 了解 NIPS 的发展

12.3 防病毒

12.3.1 病毒检测的基本原理

1) 了解病毒检测的方法

2) 理解特征码技术的原理

12.3.2 病毒查杀日志分析重点

了解病毒查杀日志分析重点内容

12.3.3 经典虚拟化防病毒技术方案

1) 了解虚拟化环境下防病毒方案模式

2) 了解虚拟化环境下不同方案的优缺点

12.4 DDOS 防护

1) 理解 DDOS 攻击的原理
2) 理解 DDOS 攻击的防护手段
3) 了解监测、流量清洗技术的原理
4) 理解监测、流量清洗设备的部署方式

第13章 安全体系架构设计

13.1 网络架构安全基础

1) 理解网络安全架构的含义
2) 理解网络安全架构的内容

13.2 网络架构安全设计

13.2.1 网络安全域划分应考虑的主要因素

1) 理解安全域的概念
2) 理解网络边界的概念
3) 理解安全域划分需要考虑的因素

13.2.2 IP 地址规划方法

1) 了解 IP 地址规划的方法
2) 理解静态地址分配
3) 理解动态地址分配
4) 理解 NAT

13.2.3 VLAN 划分的作用与策略

1) 理解 VLAN 的概念

2) 理解 VLAN 的作用

3) 理解 VLAN 划分策略

13.2.4 路由交换设备安全配置常见的要求

4) 理解交换机的安全配置

5) 理解路由器的安全配置

13.2.5 网络边界访问控制策略的类型

1) 理解网络边界

2) 理解不同的访问控制模式

13.2.6 网络冗余配置应考虑的因素

了解网络冗余配置的考虑

第五部分网络安全应急

第14章 网络安全事件的监测与发现

14.1 蜜罐技术

1) 了解蜜罐的定义
2) 了解蜜罐发展的三个阶段
3) 理解蜜罐的两种类型
4) 理解蜜罐技术的核心机制和辅助机制
5) 理解蜜罐的组成
6) 理解 Kippo 蜜罐的相关内容

14.2 入侵检测

1) 了解入侵检测的定义
2) 了解入侵检测的两种分类
3) 掌握异常检测的方法
4) 掌握误用检测的方法
5) 掌握常见的几种检测系统

14.3 APT

1) 了解 APT 攻击的流程
2) 理解 APT 与传统攻击的差异
3) 理解 APT 攻击对现有体系的挑战
4) 掌握 APT 攻击的应对方案

第15章 应急响应简介

15.1 应急响应的概念

理解应急响应的概念和目的

15.2 应急响应的组织机构

1) 了解 CCERT 的介绍和此组织的作用
2) 了解 FIRST 的介绍和此组织的作用
3) 了解 IRT 的介绍和此组织的作用

15.3 应急响应的特点

1) 了解技术专业性、经验依赖性和突发事件的描述

15.4 应急响应的流程

1) 理解准备阶段的作用和此阶段的工作内容
2) 理解检测阶段的作用和此阶段的工作内容
3) 理解分类阶段的作用和此阶段的工作内容
4) 理解抑制阶段的作用和此阶段的工作内容
5) 理解根除阶段的作用和此阶段的工作内容
6) 理解根除阶段的作用和此阶段的工作内容
7) 理解后续阶段的作用和此阶段的工作内容

第16章 常见安全事件应急处置

16.1 恶意代码型事件的处理

16.1.1 判别范例

了解恶意代码特性以及对应的影响和原始报警距离

16.1.2 蠕虫

1) 理解蠕虫的几种检测条件以及告警举例
2) 理解蠕病毒源如何定位的几种方式
3) 了解蠕虫的处理过程

16.1.3 病毒

1) 理解病毒的几种检测条件以及告警举例
2) 理解病毒源如何定位的几种方式
3) 了解病毒的处理过程

16.2 DDos 型事件处理

16.2.1 DDOS 攻击技术概述

理解 DDOS 攻击技术的概述

16.2.2 分布式拒绝服务攻击体系结构图

1) 带宽消耗型攻击
2) 理解带宽消耗型攻击的两个层次和特点
3) 了解带宽消耗型攻击常见攻击方式
4) 资源消耗型攻击

5) 了解资源消耗型攻击常见攻击方式

16.3 中间人攻击事件处理

1) 了解会话劫持、修改的简述和原理
2) 了解修改网页内容的简述和原理
3) 了解 DNS 欺骗的简述和原理
4) 了解针对 SSL 的中间人攻击的简述和原理
5) 了解 SSL 卸载的简述和原理
6) 了解伪造 SSL 证书的简述和原理
7) 了解 SSL/TLS 破解的简述和原理
8) 了解 ICMP 重定向攻击的简述和原理
9) 了解 DHCP 攻击的简述和原理
10) 了解端口盗用攻击的简述和原理
11) 了解 NDP 攻击的简述和原理
12) 了解邪恶的孪生 AP 攻击(Evil Twin AP)的简述和原理

第17章 应急响应分析技术手段

17.1 日志分析

17.1.1 日志分析的概念以及常见的日志类型

1) 了解日志的简述和意义
2) 理解常见的日志类型和类型简介

17.1.2 日志分析工具

了解 LogViewPro 的简介和特点

17.1.3 日志中的安全事件

1. 攻击特征相关的日志
   1) 理解常见攻击特征所对应的日志特征关键字
   2) 了解使用 LogViewPro 匹配查找包含所对应的关键字的日志
2. 安全性日志中的成功与失败
   1) 了解安全性日志中的成功与失败
3. Linux 系统相关的日志
   1) 理解 Linux 系统相关的日志
4. 其他一些记录
   1) 了解其他一些记录

17.2 后门检测

17.2.1 Windows 后门检测

1. Windows 常规检测
   1) 理解用户检查的办法
   2) 了解进程及启动项的使用
   3) 了解利用 wsyscheck.exe 工具检查服务、模块及驱动
   4) 理解各个日志的存放地和简介
   5) 理解使用 tcpview 可用于检测当前系统中的进程及其对应的连接状态
2. Windows 恶意代码检测
   1) 理解各个恶意代码的监测方式
3. Windows 检测工具包
   1) 理解工具的分类和对应的命令、文件及相关说明

17.2.2 UNIX/Linux 后门检测

1. UNIX/Linux 常规检测

1) 理解用户检查的办法

2) 了解进程及启动项的使用

3) 了解使用命令 chkconfig–list 工具检查服务、模块及驱动

4) 理解各个日志的存放地和简介

5) 理解 SUID 文件的检查方式、RPM 完整性检查、网络连接的检查方式

2. UNIX/Linu 恶意代码检测

1) 理解常见恶意代码检查工具的使用方法和技巧

3. UNIX/Linu 检测工具包

1) 理解工具的分类和对应的命令、文件及相关说明

17.2.3 Webshell 检测

1) 理解 Webshell 介绍

2) 理解一句话木马之“小马”

3) 理解一句话木马变形

4) 理解 Webshell 查杀

17.3 样本分析

17.3.1 静态分析

1) 理解静态分析概述

2) 理解反病毒引擎扫描

3) 了解哈希值（恶意样本的指纹）

4) 了解加壳与混淆恶意代码

17.3.2 动态分析

1) 理解动态分析概述

2) 了解利用沙箱分析样本行为

17.3.3 清理与查杀

1. Windows 样本手动查杀实例
    1) 理解样本分析和手动查杀方式
2. Linux 样本手动查杀实例
    1) 理解样本分析和手动查杀方式

17.4 流量分析

17.4.1 网络数据包抓取与分析原理

1) 了解网络技术与设备简介
2) 了解网络监听原理
3) 了解 sniffer 分类
4) 了解网络监听的目的

17.4.2 抓包工具

理解抓包工具有哪些

17.4.3 分析工具

理解抓包工具有哪些以及作用

17.4.4 不同网络攻击的流量表现特征

1. 异常流量的数据包类型
    1) 了解 NetFlow 的概念以及在本文中的含义
    2) 了解 NetFlow 数据的 NFC 格式说明
    3) 理解对异常流量的源、目的地址的解释
    4) 理解对异常流量的源、目的端口的解释
2. 内网僵尸、木马、蠕虫特点

1) 理解对内网僵尸、木马、蠕虫特点

2) 理解几种蠕虫病毒的 NetFlow 分析实例

3. ARP 安全攻击流量特点

1) 理解 ARP 安全攻击流量特点

4. DNS 安全攻击特点

1) 理解 DNS 安全攻击特点

5. 其它异常流量

1) 理解其它异常流量

17.4.5 处理异常流量的方法

1) 了解切断连接的方法的使用前提和作用

2) 了解过滤的方法的使用前提和作用

3) 了解静态空路由过滤的方法的使用前提和作用

4) 了解异常流量限定的方法的使用前提和作用