三级《网络及安全技术》考试大纲（2019版）

# 考试目标

学生通过计算机网络及安全技术的学习和实践，掌握计算机网络的基本知识、基本原理、常用协议、基本的管理配置及实践操作方法，掌握网络及安全的基本原理和应用技术，具备分析和解决网络工程问题的能力，具有基本的网络信息安全管理与实践应用能力。

# 基本要求

1、掌握计算机网络基础知识。

2、掌握局域网的基本工作原理及组网技术。

3、熟练掌握互联网TCP/IP体系及各层典型网络协议。

4、基本掌握常见的互联网应用协议与服务。

5、掌握常用网络服务的应用与配置，掌握网络安全、系统安全和应用安全的基本知识和实践技能。

6、掌握计算机网络信息安全的基本理论与方法及常用的安全防护技术。

7、理解物联网、云计算、5G网络、区块链等网络新技术。

# 考试内容

一、计算机网络体系结构

1、计算机网络的产生和发展

2、计算机网络基本概念

计算机网络的定义，分类，计算机网络的主要功能及应用。

3、计算机网络的组成

网络边缘部分和网络核心部分，网络的传输介质，分组交换技术。

4、网络体系结构与网络协议

网络体系结构，网络协议，ISO/OSI参考模型，TCP/IP网络模型。

二、网络信息安全概况

1、信息安全基础

（1）信息安全基本属性

机密性、完整性、可用性、可控性、不可抵赖性（不可否认性）

（2）信息安全基本模型

信息保障模型PDR与P2DR，信息安全保障技术框架IATF，信息技术安全评估CC准则，信息系统安全等级保护模型。

（3）信息安全基本法规

国外法规，国内的网络安全法、密码法、网络安全等级保护制度。

2、密码应用基础

（1）密码算法

古典密码、现代密码；加密模式、分组密码、流加密；公钥密码、哈希函数、数字信封。

（2）密码分析

古典密码破译，中间相遇攻击，中间人攻击，唯密文攻击，已知明文攻击，已知密文攻击，选择明文攻击，选择密文攻击。

（3）密码应用

数字签名，访问控制与授权，身份认证。

（4）密钥管理

对称密钥管理，非对称密钥管理（PKI）。

（5）密码协议概述

**3、**网络安全技术

实体硬件安全，软件系统安全，网络安全防护和反病毒技术研究（入侵检测、防火墙、审计、恢复等），数据信息安全，安全产品。

三、局域网技术及安全

1、局域网基本概念

局域网的定义、特点，局域网的分类与标准。

2、以太网组网技术

共享以太网：载波侦听多路访问/冲突检测，以太网帧格式，集线器组网；

交换局域网：交换机组网；

虚拟局域网：定义、特点及配置。

3、无线局域网技术

无线局域网组成，载波侦听多路访问/冲突避免，WiFi；

无线个人区域网: 蓝牙、ZigBee、超带宽UWB。

4、局域网安全

Sniffer抓包分析，ARP攻击，WiFi密码破解，WiFi劫持, 。

四、互联网协议及安全

1、Internet的构成

Internet组成， Internet基本服务及工作原理。

2、IP协议

IP协议概述，IP服务，IP地址，掩码，IP报文，差错与差错控制报文。

3、路由与路由选择

路由表，路由转发，静态路由选择，动态路由选择包括RIP路由协议、OSPF路由协议，广播路由，多播路由。

4、IPv6协议

IPv6组成结构，IPv6地址类型，IPv6协议，IPv6/IPv4双协议栈技术，隧道技术。

5、NAT地址解析协议

NAT概念，NAT实现方式，NAT工作原理，NAT配置方式。

6、TCP协议与UDP协议

端对端通信，TCP协议，UDP协议。

7、网络协议安全攻击

ARP欺骗，IP泪滴攻击，TCP会话劫持，SYN Flood洪水攻击，UDP泛洪攻击，DoS拒绝服务攻击和DDoS分布式拒绝服务攻击。

8、安全协议

IPSec，SSL协议。

五、互联网应用及安全

1、应用进程通信模型

C/S模型概念与结构，P2P模型概念与结构，其他应用进程通信模型。

2、域名系统

DNS协议概述，层次域名空间，域名服务器，域名解析过程。

3、远程登录服务

Telnet协议概述，远程登陆服务过程，Telnet传输格式。

4、电子邮件服务

电子邮件格式，电子邮件服务协议包括SMTP、POP3、IMAP。

5、Web服务

Web服务概述， HTTP协议，HTTP协议基本格式。

6、DHCP服务

DHCP协议概述，DHCP协议功能，DHCP协议工作原理

7、应用安全

电子邮件安全协议，DNS域名服务安全，安全远程登录服务SSH，HTTPS安全连接，Web应用安全（网络钓鱼、SQL注入、跨站攻击等）。

六、网络系统管理及安全

1、网络操作系统及安全

（1）Windows服务器

用户与组，活动目录，中断服务，网络管理配置，系统管理配置，系统备份，防火墙。

（2）Linux服务器

网络安全配置，用户管理配置，文件与目录安全，日志安全，权限控制和行为审计。

（3）数据库安全

用户口令设置，主机安全配置，网络访问安全配置。

2、网络配置及安全管理

网络服务器基本配置，网络服务器安全设置，Web服务安全配置，DNS服务安全配置和服务器安全测试。

3、网络管理协议及安全防护

网络管理基本协议SNMP、CMIP，网络管理协议工作原理，网络管理工具及应用基础，网络安全防护管理，分布式网络管理。

七、安全防护技术

（1）防火墙

防火墙工作原理，防火墙的分类，防火墙安全策略。

（2）入侵检测

入侵检测工作原理，入侵检测策略配置，入侵检测方法（异常检测、误用检测）。

（3）恶意代码检测

软件逆向（静态分析、动态分析），基于特征扫描检测， 沙箱检测。

（4）安全漏洞扫描

主机扫描技术，端口扫描技术，服务及系统识别技术。

（5）网络渗透测试

主机侦察、数据库攻击、WebShell。

（6）VPN技术

VPN概念，VPN常用技术（MPLS VPN, SSL VPN，IPSec VPN，PPTP），VPN应用（远程访问VPN，内联网VPN，外联网VPN）。

（7）其他安全技术

蜜罐系统，网络备份，匿名网络。

八、网络新技术及安全挑战

物联网，云计算，大数据，人工智能，区块链，5G+工业互联网，软件定义网络SDN，软件定义安全SDS。