信息安全从业之路—网络知识

1 掌握的知识内容

以华为设备为介绍对象，毕竟安全还是要考虑国内的环境。

OSI 模型、TCP/IP 模型、无线局域技术、路由技术、交换技术、协议安全、数据包分析技术、网络架构设计与实现、网络设备脆弱性检查、网络设备安全加固

1.1 目的

- 掌握网络设备安全检查方法
- 掌握网络设备安全加固方法
- 掌握网络设备安全维护的内容

1.2 应用

- 网络设备脆弱性检查
- 网络设备安全加固
- 风险评估使用
- 等级保护整改
- 安全基线检查

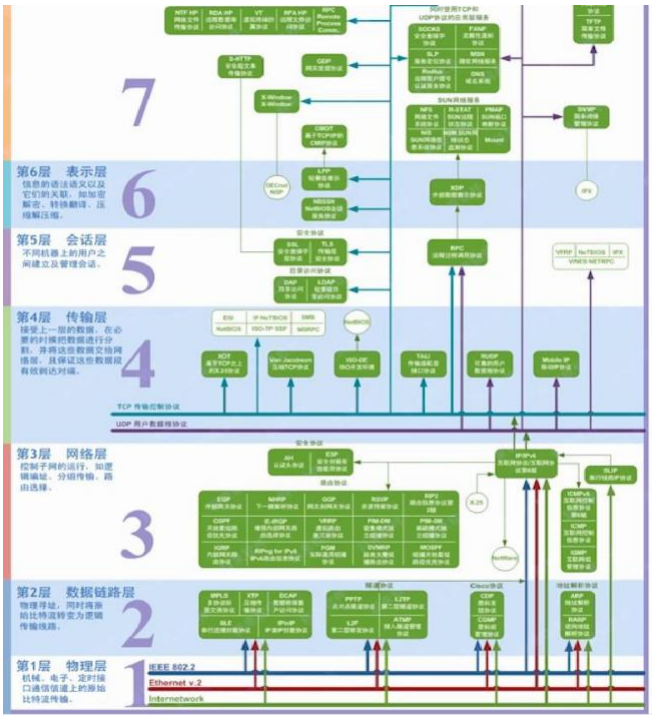
2 虚拟软件使用

2.1 华为 ensp]

3 OSI 模型与 TCP/IP 模型基础与安全点

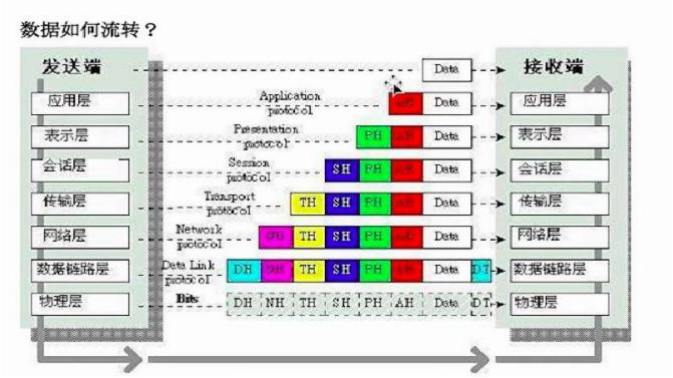
3.1 OSI 模型【 OSl(Open System Interconnection)】

参考模型是国际标准化组织(ISO)制定的一个用于计算机或通信系统间互联的标准体系，一般称为 OSI 参考模型或七层模型。



3.2 TCP/IP 模型

OSI七层网络模型	TCP/IP四层概念模型	对应网络协议
应用层（Application）	应用层	HTTP、TFTP, FTP, NFS, WAIS、SMTP
表示层（Presentation）		Telnet, Rlogin, SNMP, Gopher
会话层（Session）		SMTP, DNS
传输层（Transport）	传输层	TCP, UDP
网络层（Network）	网络层	IP, ICMP, ARP, RARP, AKP, UUCP
数据链路层（Data Link）	数据链路层	FDDI, Ethernet, Arpanet, PDN, SLIP, PPP
物理层（Physical）		IEEE 802.1A, IEEE 802.2到IEEE 802.11



3.3 问题点

1.物理层 提供比特流传输

设备被盗、设备老化、意外故障、无线电磁辐射泄密、搭线监听等

2. 链路层 提供介质访问，链路管理【ARP、MAC】

流量劫持、欺骗、DDOS、ARP 攻击、中间人攻击、广播风暴等

3. 网络层 寻址和路由【RIP、OSPF\BGPIGRP\ISIS、IPSECVPN、ICMP】

路由协议自身的安全性、流量劫持、欺骗、DDOS、中间人攻击、重定向等

4.传输层 建立主机端到端的连接[TCP、UDP、IPX、TLS、SSL]

协议本身的安全性、流量劫持、欺骗、链路重置、阻塞等

5.会话层 建立，维护，管理会话【SESSION 、COOKIE、SOCKET】

6.表示层 处理数据格式，数据加密等[加解密、编码转换、格式转换、解压缩]

7.应用层 提供应用程序间的通信【WEB 安全(http)】[FTP\smtp\DNS\telhet]