

信息安全从业之路--操作系统

1 掌握的知识内容

Windows 服务器的基础知识、IS 配置与维护、DNS 配置与维护、DHCP 配置与维护、安全策略使用、AD 域维护、操作系统脆弱性检查、操作系统安全加固。

1.1 目的

- 掌握操作系统安全检查
- 掌握操作系统安全加固
- 掌握操作系统安全维护的内容

1.2 应用

- 操作系统脆弱性检查
- 操作系统安全加固
- 风险评估
- 等级保护整改
- 安全基线检查

2 虚拟机使用

2.1 windows 虚拟机

2.2 Linux 虚拟机

3 Windows 系统

3.1 基础知识

掌握 Windows 操作系统基础的内容，安装、维护、升级、病毒查杀、基本的 DOS 命令(不需要都掌握，powershell 命令单独讲解)、密码重置、IPC\$连接等。

3.2 IIS 安全

3.3 DNS 安全

3.4 DHCP 安全

3.5 安全策略说明

3.6 AD 域安全

3.7 数据防护

3.8 脆弱性检查(重点)

3.9 安全加固(重点)

4 Linux 系统

4.1 基础知识

4.1.1 安装与界面说明

4.1.2 启动流程

4.1.3 基本命令

4.1.4 编辑器使用

4.1.5 文件属性

4.1.6 特殊权限

4.1.7 账户管理

4.1.8 文件安装与卸载

4.2 服务器配置

4.2.1 Apache+PHP+Mysql 安全配置

4.2.2 NGINX 安全配置

4.3 DNS 安全配置

4.4 FTP 安全配置

4.5 监控平台

cacti+nagios+zabbix

4.6 数据防护

4.7 脆弱性检查(重点)

4.8 安全加固(重点)

5 作业

5.1 Windows2012 脆弱性检查与加固

5.2 Centos 脆弱性检查与加固