16 级《网络安全实训》项目指导

广州国为信息科技 主讲

目录

项目一　部署网络安全平台桌面客户端环境

一、项目目标 ：

1. 配置客户端网络基本参数；
2. 安装云平台客户端软件 vSphere Client；
3. 登录到云平台；

二、实施步骤

任务 1：配置客户端网络基本参数

任务 2：安装云平台客户端软件 vSphere Client

任务 3：登录到云平台

项目二 熟悉网络安全云平台拓扑

一、项目目标 ：

1. 还原平台设备至初始状态；
2. 启动平台内各设备；
3. 认识网络安全云平台拓扑；
4. 访问网络安全云平台内的系统；
5. 访问网络安全云平台内的设备；

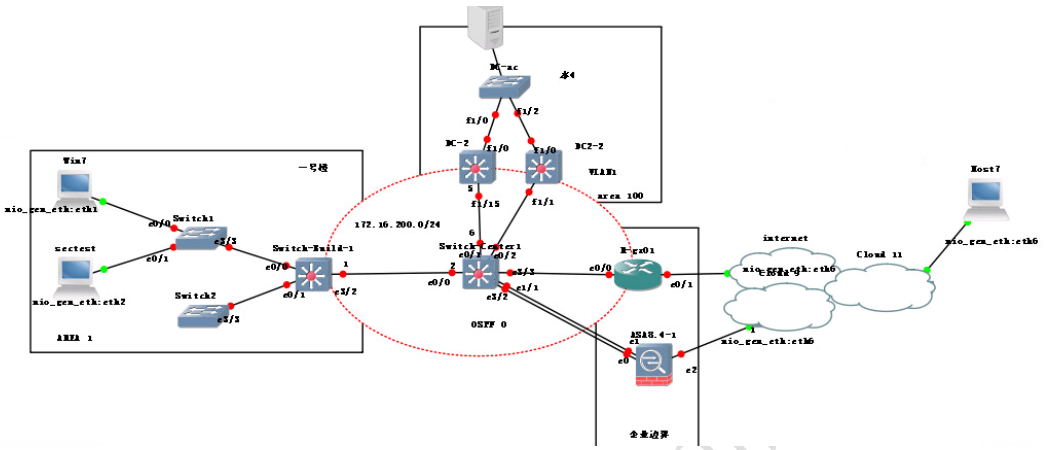
二、实施步骤

任务 1：还原平台设备至初始状态

任务 2：启动平台内各设备

任务 3：认识网络安全云平台拓扑

1. 认识网络安全云平台拓扑图，如下图所示：



从拓扑图上，我们可以看到，在每组的设备及计算机，以及端口连接情况：

2. 每组计算机及设备清单如下表所示：

序号	名称	类型	用途
1	Winxp	PC	测试用主机，同时用来连接网络设备
2	Linux	PC	已安装 BT 系统，进行入侵、扫描等测试
3	Server	服务器	拥有漏洞的服务器，测试目标
4	SW01	多层交换	用来连接各设备，并规划流量
5	R1	智能路由	连接不同网段，提供基本安全保障
6	ASA1	硬件防火墙	执行专业的安全防护
7	IDS	入侵防御	入侵防御系统

任务 4:访问网络安全云平台内的系统

任务 5:访问网络安全云平台内的设备

项目三　为拓扑配置基本的网络参数

一、项目目标

1. 配置 PC 和服务器的 TCP/IP 参数；
2. 使用 SecureCRT 配置网络设备；
3. 配置网络设备 SW01 和路由器 R1 的基本参数；

二、实施步骤

任务 1：配置 PC 和服务器的 TCP/IP 参数

任务 2：使用 SecureCRT 配置网络设备

任务 3：配置网络设备 SW01 和路由器 R1 的基本参数

项目四　协议分析软件的使用

一、项目目标

1. 安装协议分析软件 Wireshark；
2. 使用 Wireshark 抓包；
3. 对海量数据包过滤；
4. 分析敏感数据包；

二、实施步骤

任务 1：安装协议分析软件 Wireshark

任务 2：使用 Wireshark 抓包

任务 3：对海量数据包过滤：

任务 4：分析敏感数据包

项目五 配置路由器连接互联网

一、项目目标

1. 配置路由器 R1 的外网接口；

2. 配置路由器 R1 的 NAT；

3. 测试内网 PC 和 Server 的互联网访问；

二、实施步骤

任务 1：配置路由器 R1 的外网接口

任务 2：配置路由器 R1 的 NAT

任务 3：测试内网 PC 和 Server 的互联网访问

项目六 网络信息搜集

一、项目目标

1. DNS 类信息常规搜集；
2. 使用 dnsenum 探测 DNS 信息；
3. 使用 dnsmap 探测 DNS 信息
4. 路由信息搜集；

二、实施步骤任务 1：DNS 类信息常规搜集

任务 2：使用入侵检测工具 dnsenum 探测 DNS 信息

任务 3：使用 dnsmap 探测 DNS 信息

任务 4：路由信息搜集

项目七 主机信息搜集

一、项目目标

1. 确定目标主机是否存活；
2. 探测互联网主机；

3. 探测操作系统指纹；

二、实施步骤

任务 1：确定目标主机是否存活

任务 2：探测互联网主机

任务 3：使用 xprobe2 探测操作系统指纹

项目八 常用扫描测试工具

一、项目目标

1. Autoscan 的使用；
2. Netifera 的使用；
3. Nmap 的使用；
4. 路由信息搜集；

二、实施步骤

任务 1：Autoscan 的使用

任务 2：Netifera 的使用

任务 3：nmap 的使用

项目十一 企业内网攻击（一）

一、项目目标

1. Unknown Unicast Flooding 攻击；
2. 基于 CDP 协议的攻击；
3. 针对 DHCP 服务器的攻击

二、实施步骤

任务 1：Unknown Unicast Flooding 攻击

任务 2：基于 CDP 协议的攻击

项目十二 企业内网攻击（二）

一、项目目标

1. 针对 STP 的攻击；
2. ARP 欺骗综合攻击；

二、实施步骤

任务 1：针对 STP 的攻击

任务 2：ARP 欺骗综合攻击

项目十三 网络设备安全优化

一、项目目标

1. 优化网络设备密码安全；
2. 优化网络设备远程访问安全；
3. 执行自动安全配置；

二、实施步骤

任务 1：优化网络设备密码安全

任务 2：优化网络设备远程访问安全

任务 3：执行自动安全配置

项目十四 配置硬件防火墙

一、项目目标

1. 初始化硬件防火墙 ASA；
2. 为企业网规划安全区域；

二、实施步骤

任务 1：初始化硬件防火墙 ASA

任务 2：为企业网规划安全区域

项目十五 在企业网内实现 VPN

一、项目目标

1. 实现出差人员的 VPN 内网访问；
2. 实现分公司的内网访问；

项目十六 实现企业内的整体身份认证

一、项目目标

1. 在企业内实现整体身份认证；
2. 配置 AAA 服务器完成认证；
3. 配置企业内的 AAA 客户端；
4. 实现企业内设备访问的身份认证
5. 实现上网身份认证；

项目十七 企业内实现流量管理与控制

一、项目目标

1. 安装部署流控系统；
2. 配置基于 Web 的流控；
3. 配置流控策略；
4. 测试流控效果；