2023 年全国网络安全行业职业技能大赛

网络安全管理员

操作技能赛题（决赛卷）

2024. 01

内容

项目介绍

简介

网络安全管理员是保障网络系统安全的专业，需要掌握网络安全合规、攻防技术和运维知识。其职责包括确保系统遵循法规，防范网络攻击，及时处理安全隐患，以保障网络环境的可靠性。通过运用理论知识和技术技能，评估和提高网络安全水平，包括漏洞扫描、入侵检测等。网络安全管理员的工作有助于加强社会对网络安全和个人信息保护的认识，构建安全的网络环境，保护用户隐私和企业核心数据，为信息社会的可持续发展奠定基础。

任务描述

本项目需要运用不同的网络安全全技术，任务有以下部分：

- 网络安全防护
- 网络安全管理
- 网络安全处置

选手必须按照比赛要求对网络基础设施进行防护和管理，对一些网络设备进行安全配置。所有的设备和服务可以正常运行，但尚未采取任何安全防护措施，甚至有部分配置是错误的，需要选手找出错误。在项目中，会给出一部分相对直接的安全防护和管理实施要求。选手需要在设备条件的限制下尽力满足所有的比赛要求并符合行业规范操作。

选手指南

1. 在开始配置前详细阅读所有的任务。每一项任务都可能和前后任务的完成有所依赖。依赖于上一项或下一项的完成。
2. 本次比赛为局域网访问形式，在比赛前请确认设备是否能够正常访问，**在比赛中请时刻注意配置操作是否会影响系统的正常访问，如在比赛时因配置原因造成系统无法正常访问，需要选手自行解决。**
3. 比赛答题平台上提交 Flag 形式进行，Flag 必须与答题平台内**对应序号答题框**的预设完全匹配才能得分，**除赛题中特别要求外，所有 Flag 的内容以小写、去除空格后提交，无特殊提示的情况仅需提交指定内容即可。**
4. 比赛可采用任何自带设备和工具，但***禁止使用影响他人比赛或妨碍平台运行的工具、方法和手段，如有发现将立即取消成绩***。

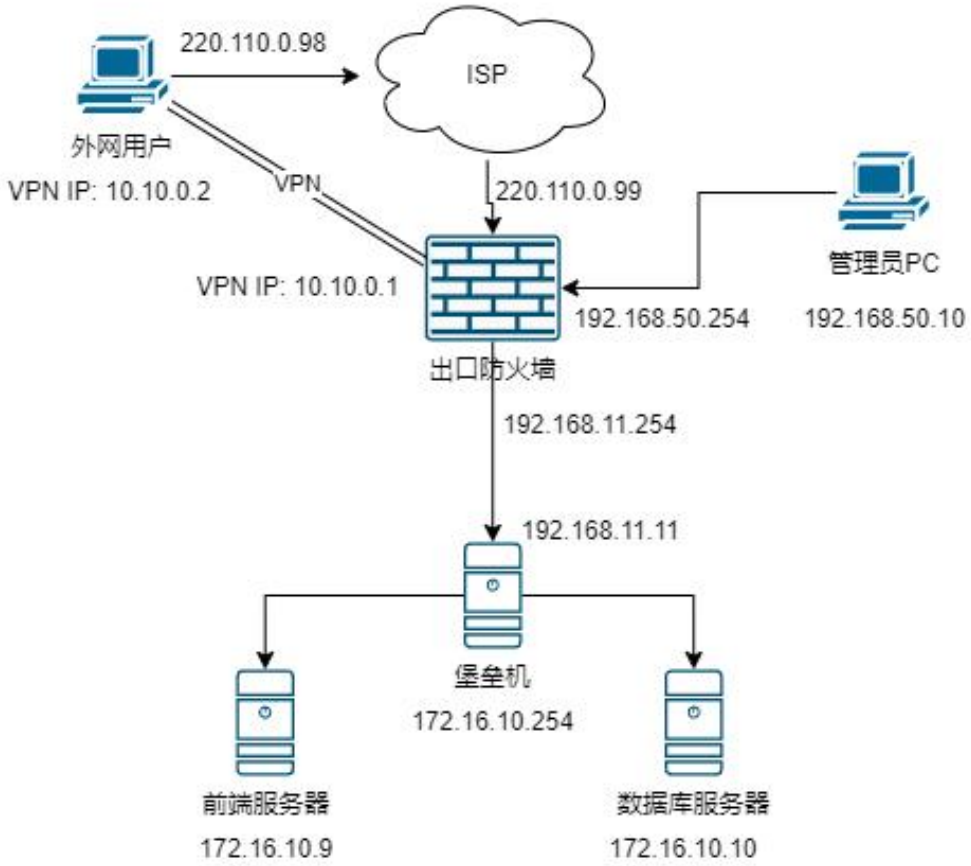
所需设备，安装和材料

选手工具以全部安装在虚拟机中，无需自行安装。

任务目标

项目信息

1. 所有设备和虚拟机的主机名称根据提供的图示已预先配置



2. 虚拟机 IP 地址列表

设备名	IP 地址	网关
出口防火墙	220.110.0.99	
	192.168.11.254	
	172.16.10.254	
堡垒机	172.16.10.254	
	192.168.11.11	192.168.11.254
前端服务器	172.16.10.9	172.16.10.254
数据库服务器	172.16.10.10	172.16.10.254

设备名	IP 地址	网关
管理员 PC	192.168.50.10	192.168.50.254
外网用户	220.110.0.98	220.110.0.99

3. 用户名和密码

设备名	用户名	密码
出口防火墙（web）	admin	Admin@123
堡垒机（web）	admin	Admin@123
外网用户	administrator	Admin@123
管理员 PC	administrator	Admin@123
前端服务器	root	Admin@123
数据库服务器	root	Admin@123

第一部分：网络安全防护

注：该部分题目在 虚拟化操作平台上完成，flag 在技能操作平台上提交。

网络安全是维护整个信息系统安全的关键环节之一。作为网络安全管理员，确保各个服务的稳定性和安全性是日常工作的重要组成部分。对服务器进行基线核查并验证服务配置和管理措施是否符合组织的安全标准和行业最佳实践，并将有问题的检查项的序号作为 flag 提交，顺序为从小到大排序。如：flag{12345678910}

1、 对前端服务器进行检查，将配置错误的 ID 以数字的形式提交；

ID	检查项
0	检查设备密码复杂度策略，是否符合大写、小写、数字、字符至少一位，配置过的为正确；
1	检查口令生存周期不大于 90 天，小于 90 天为正确；
2	检查全局文件，umask 是否设置为 077，077 为正确；
3	检查是否设置 ssh 登录前警告 Banner，有为正确；
4	检查是否记录成功登陆的日志，有日志记录的为正确；
5	查历史记录值是否小于 10，小于 10 的正确；

6	检查命令行界面超时时间是否配置为 600 秒，配置过的为正确；
7	检查历史命令记录是否小于 5，小于 5 为正确；
8	检查 FTP 是否禁用匿名用户，禁用为正确；
9	查 FTP 服务器是否开启日志记录，开启为正确；

2、 对数据库服务器进行检查，将配置错误的编号以数字的形式提交；

ID	检查项
0	检查 mysql 服务器是否禁用 root 账户的远程登录，禁用为正确；
1	除 root 账户外的账户，不得拥有对系统数据库的任何权限，不得拥有 grant，file，reload，shutdown，process 权限的任何一种， 没有的为正确；
2	检查 mysql 服务器是否开启日志记录功能，log-error、log、log-slow-queries 这三种日志状态为 ON，ON 为正确；
3	检查磁盘/dev/vdb 是否挂载到/mnt 下，正确挂载的为正确；
4	检查/dev/vdb 的的数据是否与前端服务器同步过，查看日志，有的为正确；
5	检查 crontab 的配置格式是否正确，是否为每天执行一次备份，每天执行一次为正确；
6	检查 SSH 服务器是否禁用 root 登录，禁用为正确；
7	检查 SSH 服务器公私钥配置是否正确，通过公私钥无密码登录为正确；
8	检查除 root 之外 UID 为 0 的用户，没有为正确；
9	查看 debian 系统的版本号是否是 12.1，是为正确；

3、 对管理员 PC 进行安全检查，将配置错误的编号以数字的形式提交；

ID	检查项
0	检查是否已启用密码复杂性要求，启用为正确；
1	检查是否已禁用来宾(Guest)帐户，禁用为正确；
2	检查系统是否禁用 U 盘，禁用为正确；
3	检查防火墙是否为开启状态，完全开启为正确；
4	检查防火墙是否放通“文件和打印机共享”，禁用为正确；
5	检查防火墙日志是否打开“记录被丢弃的数据包”，开启为正确；
6	检查系统是否关闭所有的文件共享，关闭为正确；
7	检查是否关闭自动更新服务，关闭为正确；

8	检查可被缓存保存的登录的个数不超过 5，小于 5 正确；
9	检查远程桌面登录用户是否设置为 1，1 为正确；

第二部分：网络安全管理

注：该部分题目在 虚拟化操作平台上完成，flag 在技能操作平台上提交。

配置 VPN 服务

1. 使用管理员 PC 访问出口防火墙，在防火墙中设置外网用户的 vpn 账号，设置为仅能访问堡垒机地址（192.168.11.11），外网用户终端可以通过拨入 openvpn 登录防火墙；
2. 外网用户通过 vpn 访问堡垒机，拿到堡垒机里的 flag，以 flag 名称提交；

配置堡垒机

1. 在堡垒机中创建命令过滤，对“poweroff”命令进行限制，对所有的操作系统中授权这些命令，在任意 Linux 资产中执行“poweroff”命令，返回值即为 flag；
2. 将前端服务器、数据库服务器加入到堡垒机的资产中，授权给 inspc 用户，能正常访问。
3. 在 pfsense 中设置 snort，在 WAN 口设置规则，启用 snort GPLv2 社区规则，在外网用户终端中使用命令（ping -l 5000 220.110.0.99）攻击防火墙，在 snort 的日志中能显示 alert 告警，即为成功，在 snort 日志中查看，找到被攻击的日志，以（ID,11,"PROTOCOL-ICMP PING Windows",协议,IP 地址）的方式提交 flag；

第三部分：网络安全处置

恶意样本分析

7. 已知附件为某恶意样本，请分析该样本，并提供外连的域名字符串（无需 http 或者 https）提交答案：flag{}

Linux 后门分析

8. 企业内网 Linux 服务器疑似被入侵，现从该服务器上提取到木马后门。请对附件木马进行分析，找出木马外联的 IP 地址，提交答案：flag{IP}。附件解压密码为“infected”

勒索程序分析

企业内部服务器遭到勒索程序攻击，现已提取到勒索程序样本。请对附件样本进行分析。回答以下问题:

9-1. 样本会提示受害者进行联系的网址，请问该网址是什么？提交答案：flag{URL}

9-2. 请找到样本在进行加密时，使用的 RSA 公钥的前 10 个字符，提交答案：flag{字符串}

9-3. 请分析该勒索程序在进行加密时，单次最多加密多少字节的数据？提交答案：flag{12345}

社工钓鱼分析（PE 类）

重保期间，单位员工遭到钓鱼邮件攻击，现已从钓鱼邮件的附件中提取出恶意程序样本。请对附件样本进行分析，回答以下问题：

10-1. 样本会尝试连接一个 URL 来判断当前的网络连接状态，该 URL 是什么？提交答案：flag{URL}

10-2. 请找到样本中，生成的一个 16 字节的密钥，提交答案：flag{0xabababababababababababababababab}

10-3. 样本会通过该密钥解密字符串生成文件并加载运行，请问该文件的文件名是什么？提交答案：flag{xxx.dll}

10-4. 问题 3 中的文件加载运行后会对系统进行相关配置，请问其中一项配置“%InstallationFileName%”的文件名是什么？提交答案：flag{文件名}

10-5. 问题 4 中的文件会将系统中收集到的信息回传 C2 服务器，请问 C2 服务器的 IP 是什么？提交答案：flag{IP}

社工钓鱼分析（文档类）

11. 重保期间，单位员工遭到钓鱼邮件攻击，现已从钓鱼邮件的附件中提取出恶意程序样本。请对附件样本进行分析，提取其中包含的恶意域名。提交答案：flag{域名}。附件解压密码为“infected”