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（淘汰赛 B 卷）

2023.12

内容

项目介绍

本比赛项目内容包含以下文件:

1. 全国网络与信息安全管理职业技能大赛–操作技能赛题（淘汰赛 B 卷）.docx

简介

网络安全管理员技能竞赛旨在测评参赛选手在网络与信息安全防护、网络与 信息安全管理、网络与信息安全处置的一系列理论知识和技术技能水平，以符合 网络与信息安全管理员职业的技能要求，需要选手掌握安装、配置、管理和强化 主机、终端设备、网络设备、网络安全设备和相关软件知识和操作技能。

任务描述

本项目需要运用不同的网络与信息安全技术，任务有以下部分：

- 网络与信息安全防护
- 网络与信息安全管理
- 网络与信息安全处置

选手必须按照比赛要求对网络基础设施进行防护和管理，对一些网络与信息安全事件进行应急处理。所有的设备和服务可以正常运作，但尚未采取任何安全防护措施。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，一部分则为开放式操作要求。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. 本次比赛为在线远程访问形式，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. 比赛以在答题平台上提交 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，除特殊说明以外，所有 Flag 字符以小写、去除空格形式提交。

   如解题答案为：/etc/apache2/apache2.conf ServerSignature Off，则 Flag 提交：

   /etc/apache2/apache2.confserversignatureoff
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

选手自行准备工具完成本项目所有要求实施的内容。

评分方案

本项目的最高分为 100 分。

- 网络与信息安全防护，30 分
- 网络与信息安全管理，30 分
- 网络与信息安全处置，40 分

分数结构：

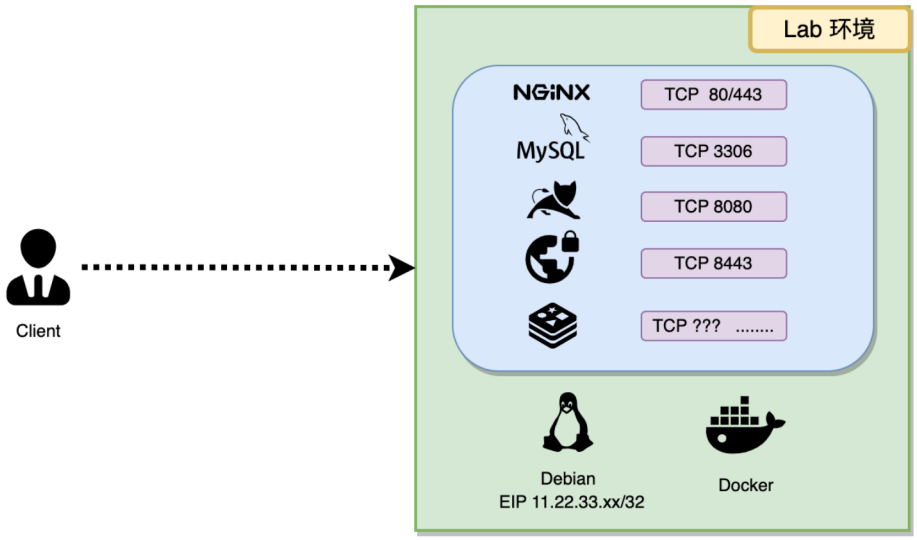
项目	任务	任务点	分值/flag	flag 数量	总分
1.网络与信息安全防护	1.1 网络安全防护	1.1.1 配置 iptables 策略	1	**4**	**4**
	1.2 系统安全防护	1.2.1 配置 pam-pwquality	2	**2**	**4**
		1.2.2 关闭不必要的应用	4	**1**	**4**
		1.2.3 配置 ssh 登录	3	**1**	**3**
		1.2.5 配置 auditd	2	**2**	**4**
		1.2.6 配置 Fail2ban	1	**3**	**3**
	1.3 应用安全防护	1.3.1 配置 rsync	2	**2**	**4**
		1.3.3 配置系统权限	2	**2**	**4**
2 网络	2.1 安全策略管理	2.1.1 配置口令策略	2	**2**	**4**

与信息安全管理		2.1.3 配置加密连接	5	**1**	**5**
	2.2 系统权限管理	2.2.1 配置最小权限	1	**4**	**4**
		2.2.2 配置日志记录	5	**1**	**5**
	2.3 系统审计管理	2.3.1 配置审计日志	3	**2**	**6**
	2.4 信息安全管理	2.4.3 配置 tomcat 安全加固	3	**2**	**6**
3 网络与信息安全处置	3.1 网络安全事件处置	3.1.1 提交攻击者来源 IP	4	**1**	**4**
		3.1.2 提交攻击者首次攻击的时间	4	**1**	**4**
		3.1.3 攻击识别	3	**4**	**12**
	3.2 互联网应用安全事件处置	3.2.1 流量分析	4	**5**	**20**
		统计		40	100

任务目标

项目基本信息：

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. 逻辑拓扑如下：



3. 虚拟机已根据以下角色预先安装：

- Debian 11.x 、Mysql 5.7 、tomcat 、wordpress
- Debian 默认账户密码 （root/Passw0rd）
- **第一部分、第二部分** 提交格式： Flag 格式为 flag{iptables 配置命令}。例如，如果答案是 iptables -A INPUT -p tcp --dport 3306 -s 192.168.1.100 -j ACCEPT，则提交 flag{iptables -A INPUT -p tcp --dport 3306 -s 192.168.1.100 -j ACCEPT}。

第一部分：网络与信息安全防护

总体要求：根据 A 企业业务需求，对 A 企业的网络、系统及应用配置主动及被动防御系统。

任务 1:网络安全防护（履行网络安全义务/个人信息保护）

1. 配置 iptables，以阻止所有对 MySQL 服务器（默认端口 3306）的未授权访问，同时允许来自指定 IP 地址（192.168.2.100）的访问。提交答案时，请提供具体的 iptables 规则配置命令。
2. 配置 iptables，以限制对 Web 服务器（默认端口 80）的过度访问。使用 iptables 实现简单的流量限制，允许每分钟最多 50 个新连接。请提交相应的 iptables 规则配置命令。

3. 配置 iptables，以确保 Redis 服务（默认端口 6379）只能被内部网络（例如 10.0.0.0/24）访问。同时，需要实现日志记录，对所有被拒绝的连接尝试进行记录。请提交完成此任务的 iptables 规则配置命令。
4. 配置 iptables，以防止任何形式的 SYN 洪泛攻击（一种常见的 DDoS 攻击）。要求设置合理的 SYN 接收队列长度，并记录所有可疑的 SYN 包。请提交相应的 iptables 规则配置命令。

任务 2:系统安全防护（履行网络安全义务/个人信息保护）

1. 配置 libpam-pwquality 以加强系统密码策略。要求设置密码至少包含 10 个字符，其中包括大小写字母、数字和特殊字符；在 5 次尝试失败后锁定账户 60 秒。请将所有的配置要求合并为一条命令提交(关键字包含但不限于 minlen 等 ，排列顺序字母为 m、d、u、c、o、r、l)。
2. 使用 libpam-pwquality 配置一个密码策略，该策略要求用户密码每 30 天更换一次，密码历史记忆 5 次，以防止用户重复使用近期的密码。同时，确保密码至少有一个大写字母和一个数字。请将所有要求合并为一条命令提交(关键字包含但不限于 minlen 等 ，排列顺序字母为 m、r、m、u、d)。
3. 公司考虑到服务器的安全性和效率，您的任务是审查正在运行的服务并停用任何与服务器当前功能无关的服务。假设服务器主要用于 Web 应用和数据库服务，需要停用邮件服务（如 Postfix）、打印服务（如 CUPS）和远程桌面服务（如 VNC）。请合并提交一个命令，展示如何使用 systemctl 命令停用这些服务（关键字包含 systemctl 包含";",服务首字母排列顺序为 p、c、v ）。
4. 公司加固服务器 SSH 服务的另一部分，您需要设置 SSH 的连接超时时间和最大认证尝试次数。要求配置 SSH，使得任何连接在 120 秒内无活动则自动断开，并且设置最大认证尝试次数为 3 次。请提交一条命令，展示如何编辑 SSH 配置文件以实现这些安全措施。Flag 格式为 flag{SSH 配置文件中的相关配置行} (关键数字排列顺序为 120、0、3)。
5. 您的任务是使用 auditd 服务对服务器进行安全审计。要求设置 auditd 以监控以下活动：所有对关键系统文件（例如/etc/passwd）的读取和修改。

6. 配置 auditd 以监控对系统重要安全配置文件的任何更改。重点关注 /etc/ssh/sshd_config（SSH 配置文件）和/etc/sudoers（sudo 权限配置）。请提交一条命令，展示如何配置 auditd 规则以追踪这些文件的所有读写操作(排列顺序为 sshd_xx 、sudoers-xx)。
7. 公司使用 Fail2ban 加固服务器安全。您的任务是创建一个 Fail2ban 规则，以防止针对 SSH 服务的暴力破解攻击。要求设置规则，使得任何 IP 在 5 分钟内对 SSH 服务尝试登录失败 5 次后，被自动禁止访问该服务 60 分钟。请提交一条命令，展示如何配置 Fail2ban 的 jail 规则来实现这个安全措施（日志路径为/var/log/auth.log 首字母或关键字排列顺序为 sshd 、port、filter、logpath、maxretry、findtime、bantime)。
8. 公司配置 Fail2ban 来防护 Nginx 服务器不受自动化扫描工具的恶意扫描。任务是创建一个规则，当从同一 IP 地址在 5 分钟内检测到超过 15 次对不存在页面的请求（404 错误）时，自动封禁该 IP 地址 1 小时。假设 Nginx 的日志文件路径为 /var/log/nginx/access.log。请提交一条命令，展示如何配置 Fail2ban 的 jail 规则以实现这个目标(首字母或关键字排列顺序为 nginx-http-auth、port、filter、logpath、maxretry、findtime、bantime)。
9. 公司设置 Fail2ban 以监控并防御针对邮件服务器（如 Postfix）的暴力破解攻击。任务是创建一个规则，用于在 30 分钟内若某个 IP 地址对邮件服务的登录尝试失败超过 20 次，则自动封禁该 IP 地址 3 小时。假设 Postfix 的日志文件路径为/var/log/mail.log。请提交一条命令，展示如何配置 Fail2ban 的 jail 规则以应对这种情况(首字母或关键字排列顺序为 postfix、port、filter、logpath、maxretry、findtime、bantime)。

任务 3:应用安全防护（履行网络安全义务/个人信息保护）

1. 公司配置 rsync 以安全同步文件。您的任务是设置 rsync 守护进程，确保仅特定用户（例如"user1"）可以访问和同步指定目录（例如/data/sync）。同时，需要配置 rsync 以使用 SSH 作为传输协议，并确保所有传输的数据都经过加密。请提交一条命令，展示如何配置 rsync 守护进程和 rsync 客户端以实现这些要求(首字母或关键字排列顺序为 path、hosts、use、read、transfer 、logging)。
2. 公司 linux 系统的/source/directory 目录下有很重要的业务内容需要定期备份到 /backup/directory，公司 it 人员决定使用 rsync 与 crontab 进行配合进行定期备份

（要求每天 3 点进行备份）。提交配置命令，每一条正确命令为一个 flag（命令中应包含 rsync ）；请提交 crontab 的配置行内容。

3. 公司配置 Linux 系统权限以提高安全性。您的任务是设置文件系统权限，使得普通用户（例如"user2"）无法读取或修改/etc/passwd 文件，同时确保 root 用户和系统服务仍然可以正常访问。请提交一条命令，展示如何使用 chmod 和 chown 命令来配置这些权限(首字母或关键字排列顺序为 chown、chmod)。
4. 公司 linux 系统中默认很多特殊命令和文件需要做权限控制，以便减少潜在的安全风险，现计划全盘寻找 perm 4000 和 perm 2000 的文件，并做 SUID、SGID 权限限制，提交配置命令，每一条正确命令为一个 flag（命令中应包含 chmod、find 并去除空格）；请提交限制 SGID 权限的命令（目标对象使用/path/to/file 替代）。

第二部分：网络与信息安全管理

总体要求：根据 A 公司业务需求，设置系统权限、数据库权限的分级管理。

任务 1:安全策略管理（履行网络安全义务）

1. 配置数据库密码策略，要求密码长度至少为 10 个字符，包含大小写字母、数字和特殊字符。包含 password 相关字段拼接提交。请提交设置密码复杂度的命令包含 MEDIUM 关键字。
2. 配置数据库密码策略，要求密码长度至少为 20 个字符，包含大小写字母、数字和特殊字符。包含 password 相关字段拼接提交。请提交设置密码最小长度的命令。
3. 配置数据库的 SSL/TLS 加密连接，增强数据传输的安全性，flag 关键字包含 ssl，cert、拼接提交；请提交配置增加证书配置的内容(ssl-key)。

任务 2:系统权限管理

1. 配置数据库创建一个具有最小必要权限的新用户，用于执行特定的任务。请提交创建新用户”new1_user”密码为”password10”的命令
2. 配置数据库创建一个具有最小必要权限的新用户，用于执行特定的任务。请提交授权本地”new_user001”用户允许对数据库”database_name”使用增删改查权限的命令。
3. 检查并取消数据库用户 user 的权限，确保 user 用户处于最小化必要的权限，不要授予过多的权限，赋权命令拼接后作为 flag 提交；请提交撤销不必要的权限的命令。

4. 配置数据库用户“user”密码为“PASSWORD”且更新周期为 360 天，确保密码定期更新，flag 关键字包含 PASSWORD， 拼接提交；请提交修改密码更新周期的命令。
5. 通过启用 mysql 的二进制日志，以便进行数据库更改的跟踪和恢复，提交关键 binlog 的拼接 flag,关键字包含 bin；请提交修改 MySQL 配置文件的命令。请提交配置 binlog 保存路径为/var/log/mysql/mysql-bin.log 的配置行内容。

任务 3:系统审计管理

1. 公司配置 MySQL 的安全审计插件 audit_log，以记录敏感操作和事件。文件路径为 /var/log/mysql/audit.log ,日志格式设置为 JSON，其中关键字包含 SET、GLOBAL、audit 等，将核心配置 信息作为 flag 提交。请提交安装审计插件的命令。
2. 公司配置 MySQL 的安全审计插件 audit_log，以记录敏感操作和事件。文件路径为 /var/log/mysql/audit.log ,日志格式设置为 JSON，其中关键字包含 SET、GLOBAL、audit 等，将核心配置 信息作为 flag 提交。请提交配置审计日志文件格式的命令。

任务 4:信息安全管理

1. 修改配置 Tomcat 的 conf/web.xml 配置文件，限制允许的 HTTP 方法（DELET），url-pattern 为/*，以减少安全风险。关键字包含<http-method>等作为 flag 提交。
2. 配置 Tomcat 以增强安全审计日志记录。您的任务是修改 Tomcat 配置，以记录关键安全事件，特别是关注使用 Valve 组件和 ExtendedAccessLogValve 功能。请提交一条命令，展示如何编辑 Tomcat 的 server.xml 文件，以实现对关键安全事件的详细记录（关键字以 Valve 开始 并以 pattern=”...”结尾结束）。

第三部分：网络与信息安全处置

在接到 A 公司员工反映对外开放的论坛在互联网被恶意攻击， A 公司立即启动应急响应，经初步分析，发现公司部分应用，业务系统，疑似遭受黑客攻击，并由可能已经发生了数据泄漏，请您协助对本次网络攻击事件进行追踪溯源，分析黑客的攻击手段、查找 WEB 应用及系统存在的漏洞。同时根据本次事件的调查分析结果，对存在的漏洞进行修复，确认并删除黑客隐藏在系统中的后门，恢复系统的正常运行。应用系统以容器化形式部署在系统内。部分流量已经提取并保存至容器内/root/dump.pcap。

任务 1:网络安全事件处置

1. 提交攻击者的来源 IP
2. 提交攻击者首次攻击的时间（形如：01/Mar/2023:01:01:01）
3. 提交攻击者尝试使用 SQL 注入时请求的完整 URL（形如：http://xxxxxx/abc.html?a=b&c=d）
4. 提交攻击者尝试条件竞争时上传请求的完整 URL（形如：http://xxxxxx/abc.html?a=b&c=d）
5. 提交攻击者尝试条件竞争时运行脚本请求的完整 URL（形如：http://xxxxxx/abc.html?a=b&c=d）
6. 提交攻击者尝试 SSRF 攻击时请求的完整 URL（形如：http://xxxxxx/abc.html?a=b&c=d）

任务 2:互联网应用安全事件处置

1. 在被攻击的 Web 服务器中查找并提交被注入恶意代码文件的绝对路径
2. 查找并提交 http 流中的恶意脚本的名称（形如：xxxx-xxxx-xxxx）
3. 查找并提交攻击者使用反弹 shell 回连后执行的第一条命令
4. 查找并提交黑客下载文件请求的 URL
5. 提交攻击者获取凭据后修改后的明文密码