2023年全国行业职业技能竞赛——第二届全国工业和信息化技术技能大赛网络与信息安全管理员（工业互联网安全方向）赛项
广东省选拔赛

实操赛题（样例）

2023年9月

工位号：_____

选手须知：

1、任务书共14页，如出现任务书缺页、字迹不清等问题，请及时向裁判申请更换任务书。

2、本场比赛总共五项任务，采用三人团体赛，时间为3小时；选手在竞赛过程中所需的赛题文件或工程文件位于SCADA监控主机“C:\技能大赛”文件夹下。

3、参赛选手应针对每道题目提供详尽的解题说明，包括解题过程中所涉及的所有操作步骤的文字说明与操作结果或执行效果截图，因缺少操作步骤导致操作结果或执行效果无法复现的，本题不得分。解题说明以word文档的形式书写，以PDF格式保存，文件命名格式为“工位号-任务X-子任务X-题目X”（X为对应的任务、子任务或题目序号）。

4、选手在比赛过程中应及时提交答案文件。裁判宣布比赛结束后选手将无法再提交新的答案文件或更改已提交的答案文件。

5、选手提交的答案文件内容不得出现学校、企业、姓名等与身份有关的信息，否则成绩无效。

6、请根据大赛所提供的比赛环境，检查所列的软件及工具组件清单是否齐全，设备是否能正常使用。

7、在完成任务过程中，请及时保存程序及数据。

任务描述：

假定你是某集成电路制造企业的网络安全工程师，对于企业的集成电路生产业务，根据任务要求完成网络架构安全设计、业务安全加固实施、业务安全评估评测、安全事件应急处置、安全事件分析研判等工作。

竞赛平台基本信息如下：

（1）工业互联网平台

IP地址	172.16.1.120/16
操作系统用户名及口令	用户名：root 口令：123
Web界面登录方式	登录地址：http://172.16.1.120:9000 用户名：admin 口令：admin

（2）MES

IP地址	172.16.1.100/16
操作系统用户名及口令	用户名：root 口令：123456
Web界面登录方式	登录地址：http://172.16.1.100/site2 用户名：admin 口令：123456

（3）SCADA监控主机

IP地址	192.168.2.86/24
操作系统用户名及口令	用户名：admin 口令：admin123

（4）HMI

IP地址	192.168.2.37/24
VNC连接口令	111111

（5）PLC

IP地址	192.168.2.25/24

（6）数采网关

IP地址	192.168.2.97/24
Web界面登录方式	登录地址：https://192.168.2.97/user/login 用户名：adm 口令：123456

（7）交换机1、交换机2

Web界面登录方式	登录地址：http://192.168.0.1 用户名：admin 口令：admin

（8）工业防火墙

IP地址	192.168.11.12/24
Web界面登录方式	登录地址：https://192.168.11.12/ 用户名：operator 口令：admin@123456

（9）工业日志审计

IP地址	192.168.11.11/24
Web界面登录方式	登录地址：https://192.168.11.11/ 用户名：operator 口令：admin@123456

（10）智能摄像头

IP地址	192.168.2.64/24
Web界面登录方式	登录地址：http://192.168.2.64/ 用户名：admin 口令：abc123456

任务一：网络架构安全设计

根据图1中给出的网络拓扑图，完成以下任务：

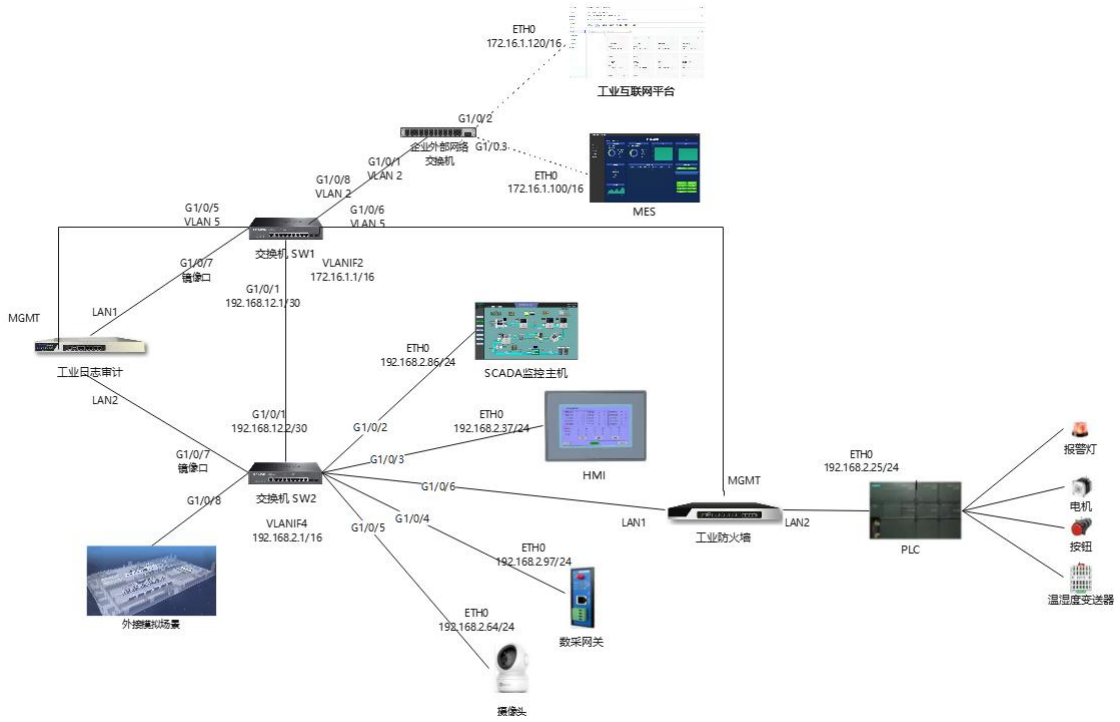

图1 竞赛平台网络拓扑

（一）网络拓扑构建

根据任务书提供的竞赛平台网络拓扑图完成竞赛网络拓扑构建：

设备	接口	VLAN	IP地址	对端设备
交换机SW1	G1/0/1	/	192.168.12.1/30	SW2 G1/0/1
	G1/0/5	5	192.168.11.11/24	工业日志审计MGMT
	G1/0/6	5	192.168.11.12/24	工业防火墙MGMT
	镜像口 G1/0/7	/	/	工业日志审计LAN1
	G1/0/8	2	/	企业外部网络交换机
	VLANIF1	1	192.168.0.1/24	/
	VLANIF2	2	172.16.1.1/16	/

交换机SW2	G1/0/1	/	192.168.12.2/30	SW1 G1/0/1
	G1/0/2	4	192.168.2.86/24	SCADA Eth0
	G1/0/3	4	192.168.2.37/24	HMI Eth0
	G1/0/4	4	192.168.2.97/24	数采网关Eth0
	G1/0/5	4	192.168.2.64/24	智能摄像头Eth0
	G1/0/6	4	网桥	工业防火墙LAN1
	镜像口G1/0/7	/	/	工业日志审计LAN2
	VLANIF4	4	192.168.2.1/24	/
工业防火墙	MGMT	/	192.168.11.12/24	SW1 G1/0/6
	LAN2	/	网桥	SW2 G1/0/6
	LAN3	/	网桥	PLC Eth0
工业日志审计	MGMT	/	192.168.11.11/24	SW1 G1/0/5
	LAN1	/	/	SW1 G1/0/7
	LAN3	/	/	SW2 G1/0/7

（二）网络设备配置

对竞赛平台中的网络设备进行配置，完成该任务应能够实现以下效果：

1.MES、工业互联网平台同处于VLAN 2下，工业防火墙、工业日志审计的管理口同处于VLAN 5下，操作人员可通过三层交换机SW1的G1/0/2访问MES、工业互联网平台的Web页面，通过G1/0/3访问工业日志审计管理页面、工业防火墙管理页面；

2.SCADA、HMI、数采网关、摄像头同处于VLAN 4下，操作人员可通过三层交换机SW2的G1/0/8可以访问数采网关Web页面和摄像头Web页面；

3.通过工业互联网平台可以查看已接入的摄像头列表，并可实时显示监控画面；

4.通过工业日志审计能够监控流经交换机SW1和交换机SW2的流量数据。

（三）安全设备配置

对竞赛平台中的工业防火墙与工业日志审计进行配置，完成该任务应能够实现以下效果：

1.数采网关仅能访问PLC的102端口，不允许访问PLC的504端口；

2.允许HMI控制PLC，控制PLC清零累计用电量；

3.允许SCADA控制PLC，控制PLC的启动、停止；

4.通过工业日志审计能够查看到从HMI发出的清零累计用电量的指令；

5.通过工业日志审计能够查看到从SCADA发出的启动PLC的指令。

任务二：业务安全加固实施

（一）工业互联网平台安全加固实施

对竞赛平台中的工业互联网平台进行安全加固，完成该任务应能够实现以下效果：

1.对其所使用的操作系统重设root账户口令，开启口令复杂度检查，至少包含小写字母、大写字母、数字、特殊字符4类字符，设置最小口令长度为8位，且新口令必须与旧口令有3位不同；

2.对其所使用的数据库配置访问策略，使其仅允许工业互联网平台所在系统访问；

3.在工业互联网平台配置管理页面中进行账户权限划分，新增综合管理岗用户，用户名zhgl，仅授予“物联网”模块的“设备管理”和“运维管理”；新增监控管理岗用户，用户名jkgl，仅授予“视频平台”模块的管理权限。

（二）MES安全加固实施

对竞赛平台中的MES进行安全加固，完成该任务应能够实现以下效果：

1.对其所使用的操作系统删除无用账户test1、test2及其主目录，允许test3账户使用su命令切换到root账户，不允许test4账户使用su命令切换到root账户；

2.对其所使用的操作系统禁止SSH的root账户登录，关闭TCP端口转发和X11转发；

3.对其所使用的数据库删除默认安装数据库test，删除匿名账户，重设root账户口令，要求使用复杂口令，修改默认端口3306为13306，设置数据库root账户仅允许本地连接，上述配置完成后通过数据看板能获取数据。

（三）SCADA安全加固实施

对竞赛平台中的SCADA进行安全加固，完成该任务应能够实现以下效果：

1.对其所使用的操作系统进行账户管理，禁用Guest账户，重设系统账户admin的登录口令，启用口令复杂性要求策略，最短口令长度为8个字符，最长使用期限为31天；

2.对其所使用的操作系统配置账户锁定策略，6次无效登录锁定账户

5分钟；

3.对其所使用的操作系统配置日志功能，记录用户登录使用的账号，登录是否成功，登录时间，以及远程登录时用户使用的IP地址；

4.对SCADA工程组态软件配置画面用户权限控制，添加admin账户，设置口令长度为至少8位，口令包含大写字母、小写字母及数字。

（四）HMI安全加固实施

对竞赛平台中的HMI进行安全加固，完成该任务应能够实现以下效果：

1.新增用户权限，添加“工程师”账户，设置登录口令长度为至少8位，包含大写字母、小写字母及数字。

（五）PLC安全加固实施

对竞赛平台中的PLC系统进行安全加固，完成该任务应能够实现以下效果：

1.对PLC项目的程序块进行加密，需正确输入口令方可查看该程序块程序，要求口令长度为10位；

2.为上传下载当前PLC中的程序设置权限，仅当输入正确口令时方可传输程序块，要求口令长度为10位。

（六）交换机安全加固实施

对竞赛平台中的交换机进行安全加固，完成该任务应能够实现以下效果：

1.设置从用户模式切换到特权模式的管理级密码为ABCabc123!@#

2.配置允许连接到HTTP服务器的最大用户数，管理员和访客登录到

HTTP服务器的最大数量为5和3，配置HTTP连接超时时间为15分钟；

3.绑定SCADA主机的IP地址、MAC地址、VLAN和交换机端口。

（七）数采网关安全加固实施

对竞赛平台中的数采网关进行安全加固，完成该任务应能够实现以下效果：

1.进行用户权限管理，新建操作员账号，仅允许访问概览、网络、重启、工具模块，操作员账户名称为czy，登录口令为1qaz@WSX

2.修改管理页面默认端口，设定HTTPS监听端口为20443，超时时间为3分钟，停用远程控制、SSH、Telnet以及开发者模式。

（八）智能摄像头安全加固实施

对竞赛平台中的摄像头进行安全加固，完成该任务应能够实现以下效果：

1.修改admin账户口令，配置页面显示口令认证强度为“强”；

2.开启非法登录锁定，设置错误尝试次数6次，配置锁定时间5分钟。

任务三：业务安全评估评测

（一）安全配置基线核查

对竞赛平台中的工业互联网平台进行安全配置基线核查，核查内容包括：

1.检查操作系统密码策略是否符合基线要求，基线要求为最长有效期不长于90天，密码修改间隔时间不长于10天，口令失效前不短于7天通知用户修改密码；

2.检查登录策略，要求普通用户5分钟之内登录失败次数超过5次锁定5分钟，root用户5分钟之内登录失败超过5次锁定5分钟；

3.检查SSH配置，基线要求禁用SSH空密码登录，空闲超时退出时间至多为15分钟，登入显示上次登录时间及IP地址。

4.检查安全审计功能，基线要求开启系统已有的audit功能，监控SSH终端的操作，包括写操作和属性变化；

5.检查文件用户权限，基线要求对重点文件进行权限控制，其中/etc/group和/etc/passwd所有者有读和写的权限，群组用户、其他用户只有读权限，/etc/shadow和/etc/gshadow仅所有者有读权限。

（二）安全漏洞测试验证

对竞赛平台中的SCADA监控主机进行安全漏洞测试验证，验证内容包括：

1.检查SCADA上是否存在漏洞CVE-2020-0796，是否可以远程利用获取SCADA的终端命令行；

2.检查SCADA上是否存在漏洞CVE-2023-21554，是否会导致mqsvc.exe崩溃。

（三）代码安全审计

对竞赛平台中MES如下图所示的一段代码进行安全审计：

```python
@app.route("/get_log", methods=["POST"])
def get_log():
    filename = request.json.get("name")

    file = f"{abs_path}/{filename}"
    if not os.path.isdir(file):
        if os.path.exists(file):
            response = make_response(send_file(file))
            response.headers['Content-Type'] = 'application/json'
            return response
        else:
            return "文件不存在", 400
    else:
        return Response(
            json.dumps(os.listdir(f"{abs_path}/{filename}")),
            content_type="application/json",
            headers=[("Content-Type", "application/json")]
        )

```

1. 请指出存在漏洞的代码位置；

2. 请指出该行代码存在的漏洞类型（应按照GB/T 30279-2020《信息安全技术 网络安全漏洞分类分级指南》中的类别进行描述，需精确至最低一级子类别）。

任务四：安全事件应急处置

（一）有害程序事件应急处置

对竞赛平台中的有害程序进行处置，完成该任务应能够实现以下效果：

1. 查找并删除攻击者在SCADA监控主机中留下的“Hack$”账户。

（二）网络攻击事件应急处置

对竞赛平台中的网络攻击事件进行处置，完成该任务应能够实现以下效果：

1. 业务系统正常情况为电机旋钮处于自动状态下，当HMI屏幕显示累计量小于设定量时，步进电机持续自动运行。现遭到攻击，步进电机停止转动，请消除攻击行为，重新配置设定值为9999，使步进电机能够持

续正常运行。

（三）信息破坏事件应急处置

对竞赛平台中的信息破坏事件进行处置，完成该任务应能够实现以下效果：

1.业务系统正常情况为MES数据看板的“翻转装配”状态与SCADA的“翻转装配”状态相同。现遭到攻击，MES数据看板的“翻转装配”状态显示与SCADA不同。请消除攻击行为，恢复上述正常情况。

任务五：安全事件分析研判

（一）有害程序事件分析研判

对竞赛平台中的有害程序进行网络分析，任务文件名为“wk.zip”，完成该任务应能够实现以下效果：

1.找出挂载木马的IP地址；

2.找出矿池域名地址。

（二）网络攻击事件分析研判

对竞赛平台中的网络攻击事件进行分析，任务文件名为“attack.pcap”，完成该任务应能够实现以下效果：

1.找出攻击者利用哪个协议进行攻击；

2.找出攻击者所使用主机的MAC地址。

（三）信息破坏事件分析研判

对竞赛平台中的信息破坏事件进行分析，任务文件名为“broken.raw”，完成该任务应能够实现以下效果：

1. 找出攻击者所使用主机的IP地址和留下的shell后门程序名称；

2. 查找攻击者利用被攻击主机执行了哪些操作。