湖南省第一届“智赋万企”工业互联网安全大赛暨2024年中国工业互联网安全大赛湖南省选拔赛实操竞赛命题说明

一、实操竞赛命题方案

| 一级指标 | 二级指标 | 三级指标 |
| --- | --- | --- |
| 业务加固实施（5%） | 系统安全基线建设与实施 | 根据任务书完成对系统安全基线建设与实施 |
| 业务主机安全加固配置 | 根据任务书完成对业务主机安全加固配置 |
| 安全审计策略配置与部署 | 根据任务书完成对安全审计策略配置与部署 |
| 主机日志审计策略配置 | 根据任务书完成对主机日志审计策略配置 |
| 工业设施安全加固（10%） | 工业互联网平台安全加固实施 | 根据任务书完成滴哦工业互联网平台安全加固 |
| SCADA安全加固实施 | 根据任务书完成对SCADA安全加固 |
| PLC安全加固实施 | 根据任务书完成对PLC安全加固 |
| HMI安全加固实施 | 根据任务书完成对HMI安全加固 |
| 安全事件分析研判（5%） | 网络攻击风险预防与监控 | 根据任务书完成对网络攻击风险预防与监控 |
| 网络攻击行为捕捉 | 根据任务书完成对网络攻击行为捕捉 |
| 网络安全事件分析研判 | 根据任务书完成对网络安全事件分析研判 |
| 网络攻击行为溯源与定位 | 根据任务书完成对网络攻击行为溯源与定位 |
| 安全风险评估测评（10%） | 主机服务探测验证 | 根据任务书完成对主机服务探测验证 |
| 安全漏洞测试验证 | 根据任务书完成对安全漏洞测试验证 |
| 源代码安全风险评估 | 根据任务书完成对源代码安全风险评估 |
| 恶意程序利用验证 | 根据任务书完成对恶意程序利用验证 |
| 安全事件应急处置（10%） | 恶意程序事件应急处置 | 根据任务书完成对恶意程序类事件应急处置 |
| 网络攻击事件应急处置 | 根据任务书完成对网络攻击类事件应急处置 |
| 信息破坏事件应急处置 | 根据任务书完成对信息破坏类事件应急处置 |
| 安全漏洞修复 | 根据任务书完成对安全漏洞修复 |
| 数据分类分（10%） | 数据分类分级 | 考察选手对工业互联网数据的分类分级原则和方法的掌握，能够根据不同的数据特性和敏感度进行科学合理的分类分级 |
| 攻击渗透（50%） | 边界突破（10%） | VPN设备漏洞利用、工业防火墙设备漏洞利用、工业管理系统漏洞利用 |
| 权限提升（10%） | Windows提权、数据库提权、Linux系统提权、系统服务提权、工控系统提权 |
| 横向移动（10%） | 工控信息搜集、工控系统识别、隧道搭建 |
| 权限维持（10%） | Webshell免杀、Webshell流量加密、Windows后门免杀 |
| 漏洞利用（10%） | 利用工控系统、工控协议、工控设备等漏洞，对工业生产进行影响或者破坏 |

二、样题范例

假定你是某企业的安全工程师，对于企业的安全生产需要你来进行安全配置，完成包括业务加固实施、工业设施安全加固、安全事件分析研判、安全风险评估测评、安全事件应急处置等工作

##### 任务一：业务加固实施

###### 系统安全基线建设与实施

对竞赛平台中的存在的操作系统进行安全加固，完成以下效果

1. 检查系统口令复杂度，要求密码至少8位长度，并且不能与旧密码相同
2. 检查系统账户锁定周期，要求对指定次数的错误密码尝试进行锁定
3. 对系统中不需要的端口进行关闭

###### 业务主机安全加固配置

对竞赛平台中的存在的操作系统进行安全加固，完成以下效果

1. 开启SYN攻击保护
2. 禁止未登录前关闭主机
3. 关闭系统中文件夹共享

###### 主机日志与安全审计策略配置

对竞赛平台中的存在的系统主机进行检查，要求通过系统日志配置策略等相关操作完成本题，完成以下效果

1. 要求系统对错误失败的登录、事件进行审计
2. 要求对系统对象访问日志进行配置
3. 要求对审核系统中账户特权使用情况进行记录

##### 任务二：工业设施安全加固

###### SCADA安全加固实施

对竞赛平台中的存在的SCADA系统进行安全加固，完成以下效果

1. 要求恢复SCADA系统通讯，使操作员与SCADA系统能够通信

###### PLC安全加固实施

对竞赛平台中的存在的PLC系统进行安全加固，完成以下效果

1. 要求恢复PLC系统通讯，使操作员界面可正确显示动态参数
2. 排查并恢复PLC系统中被修改的工程文件

##### 任务三：安全事件分析研判

###### 安全事件分析研判

对竞赛平台中的存在的网络安全攻击进行安全监控，完成以下效果

1. 要求监控系统中存在的安全攻击行为，并分析目的地址
2. 要求捕捉系统中存在的安全攻击行为，并对攻击的成功与失败进行分析和研判

###### 网络攻击行为溯源与定位

对竞赛平台中的存在的网络安全攻击进行溯源与定位，完成以下效果

1. 根据监控到的攻击行为，完成对漏洞的定位，并提取攻击行为中利用的恶意攻击代码和目标

##### 任务四：安全风险评估测评

###### 主机服务探测验证

对竞赛平台中的存在的系统环境进行溯源与定位，完成以下效果

1. 根据竞赛平台提供的信息完成对主机服务的探测

###### 安全漏洞测试验证

对竞赛平台中的存在的系统环境进行安全漏洞测试验证，完成以下效果

1. 根据当前系统运行的应用排查系统版本号及对应存在的漏洞

###### 源代码安全风险评估

对竞赛平台中的存在的系统环境进行源代码安全风险评估，完成以下效果

1. 根据当前运行的应用排查源代码中存在的安全漏洞

###### 恶意程序利用验证

对竞赛平台中的存在的系统环境进行恶意程序利用验证，完成以下效果

1. 根据当前运行的系统应用程序排查系统中被利用的后门程序，并定位其存在的位置

##### 任务五：安全事件应急处置

###### 恶意程序事件应急处置

对竞赛平台中的存在的系统环境进行恶意程序事件应急处置，完成以下效果

1. 根据当前运行的系统应用程序排查系统中存在的恶意程序，并对其进行安全处置

###### 网络攻击事件应急处置

对竞赛平台中的存在的系统环境进行网络攻击事件应急处置，完成以下效果

1. 根据当前运行的系统应用程序遇到的网络攻击行为，分析其影响，并进行应急处置

###### 信息破坏事件应急处置

对竞赛平台中的存在的系统环境进行信息破坏事件应急处置，完成以下效果

1. 根据当前运行的系统应用程序，并分析系统中信息被破坏的事件，并分析信息破坏事件进行应急处置

###### 安全漏洞修复

对竞赛平台中的存在的系统环境进行安全漏洞修复 ，完成以下效果

1. 根据当前运行的系统应用程序，并分析系统中存在的安全漏洞，对漏洞进行修复