全国大学生信息安全竞赛组织委员会

第十六届全国大学生信息安全竞赛
创新实践能力赛 Build 环节赛题说明

一、赛题描述

Build 环节比赛采用线上方式进行，重点考察各个参赛战队对互联网上资产与服务的测绘、全端口测绘、深度交互式测绘和蜜罐发现等网络空间资产测绘能力。主办方事先在互联网上部署一定数量的锚点资产（即应用指纹经过特殊设计的，主办方具有控制权限的资产或者主办方经过人工复核确认无误的网络资产），随机地分布于某些 IP 范围（CIDR 格式）。要求参赛队自主编写测绘工具，完成指定 IP 地址范围的网络空间资产测绘，按照主办方提供的模板，在规定时限内，提交测绘工具源码（包含完整的可运行 docker 环境）、设计报告及全量测绘结果数据。主办方通过考察参赛队测绘工具代码的原创性、规范性及功能的正确性，计算全量测绘结果数据中锚点资产的召回率、准确率等指标进行综合评分。

请自主编写网络空间测绘工具（编程语言不限），对以下 IP 地址范围（CIDR 格式，详见附录一）进行网络空间资产测绘，开展主机存活性探测、端口开放探测、协议识别、指纹识别、设备识别、蜜罐识别等方面的测绘。其中：

主机存活性探测需要在大赛提供的测绘目标范围内，利用有效手段探测出存活主机，并记录存活主机 ipv4 地址。

端口开放探测需要对存活主机进行端口开放状态探测，并记录存活主机开放端口信息。

协议识别需要对存活主机开放端口进行服务探测，并记录已知开放端口的协议信息。协议识别结果格式为：协议名称，例如：http。若协议未知，该项为 unknown。若无协议识别结果信息，该项为 null。

指纹识别需要对已知端口的开放服务进行指纹识别，并记录其指纹信息列表,指纹识别结果格式为：应用（服务）名称/版本信息，例如：[“nginx/1.1.1”,…,“WordPress/N”]，“N”：表示无精确版本信息。若无指纹识别结果信息，该项为 null。

设备识别需要对存活主机探测与应用识别，记录存活主机设备信息。设备识别结果格式为：设备类型/产品名称，例如：“webcam/Hikvision”。若无设备识别结果信息，该项为 null。竞赛中可能涉及的设备类型命名规范如表所示。若识别出的设备类型不在表 1 中，设备类型统一命名为 other，产品名称填写识别出的具体名称。

表 1　设备类型命名规范

设备类型	命名规范
摄像头	webcam
路由器	router
网关	gateway
虚拟专用网络	vpn

设备类型	命名规范
存储设备	storage
交换机	switch
打印机设备	printers
代理服务器	proxy server
虚拟化平台	kvm
内容分发平台	cdn
移动通信	phone
虚拟网络设备	bridge
安全防护设备	security

蜜罐识别需要对存活主机开放的服务进行分析，识别对应的服务是否为蜜罐，并记录蜜罐服务信息。蜜罐信息格式为：服务端口/蜜罐名称，例如：[“22/kippo”,“3306/N”,……]，N：表示无法精确蜜罐名称。若无蜜罐识别结果信息，该项为 null。

二、参赛要求

（1）比赛时间：2023 年 07 月 03 日 至 2023 年 07 月 16 日。

（2）参赛队伍需按要求提交测绘工具源码（docker 格式）、设计报告（doc 格式）、测绘结果文件（json 格式，示例见附录二）。

（3）比赛开始一周后，参赛队伍可在线提交成果。网址为：https://adworld.xctf.org.cn/。每支参赛队伍队长使用手机号实名注册，分项提交测绘工具源码、设计报告与测绘结果文件。

（4）比赛期间，每支参赛队伍共有三次提交测绘结果文件

的机会，测绘结果得分以三次提交结果中的最高得分计算。测绘工具源码及设计报告以最后一次提交为准，比赛结束后，统一组织专家评审。

（5）测绘工具原创性将作为评分的重要方面，参赛队需自主设计实现，禁止抄袭、串结果文件等作弊行为。一经发现，一律按零分处理。

三、评分规则

参赛队得分组成：测绘工具源码得分（10%）+ 设计报告得分（10%）+ 测绘结果文件得分（80%）。其中：

（1）测绘工具源码得分评判：专家评审，评审依据包含：原创性、可用性、规范性、代码效率。

（2）设计报告得分评判：专家评审，参照作品赛评分规则实施评审。“大赛”委派专人管理参赛作品的电子资料，按保密规则编号，由大赛组委会组织专家进行评审，并负责参赛作品评审结果的回收、统计工作。

（3）测绘结果文件得分评判：自动评判。通过判分程序对参数选手已提交的结果文件进行自动评分。

- 评分项：主机存活性探测（10 分）、端口开放探测（10 分）、协议识别（20 分）、指纹识别（20 分）、设备识别（10 分）、蜜罐识别（10 分）。
- 评判依据：计算测绘结果文件中锚点资产的召回率、准确率和 F1 值。

- 评分计算公式：Score（测绘结果文件） ＝F1（主机存活性探测）*10＋F1（端口开放探测）*10 +F1（协议识别）*20＋F1（指纹识别）* 20＋F1（设备识别）* 10＋F1（蜜罐识别）* 10。

四、其他

大赛组委会将根据实时情况，保留动态调整比赛规则的权利。另最终解释权归第十六届全国大学生信息安全竞赛——创新实践能力赛组委会所有。

全国大学生信息安全竞赛组织委员会

附录一　测绘 IP 地址范围

测绘 IP 范围	测绘 IP 范围	测绘 IP 范围
16.163.13.0/24	45.126.125.0/24	159.65.92.0/24
66.151.67.0/24	45.83.43.0/24	134.122.18.0/24
47.243.241.0/24	103.252.118.0/24	134.122.46.0/24
204.168.128.0/17	103.252.119.0/24	134.209.202.0/24
206.214.154.0/24	170.64.158.0/24	142.93.206.0/24
73.238.195.0/24	170.64.148.0/24	142.93.224.0/24
162.191.70.0/24	165.22.17.0/24	137.184.166.0/24
93.241.247.0/24	47.243.252.0/24	113.30.150.0/24
211.22.90.0/24	154.23.140.0/24	185.229.226.0/24
59.125.199.0/24	103.43.86.0/24	185.139.228.0/24
173.233.101.0/24	103.195.5.0/24	185.241.5.0/24
143.244.97.0/24	195.122.192.0/19	143.110.240.0/24
13.36.180.0/24	35.206.251.0/24	143.110.244.0/24
67.214.158.0/24	43.135.46.0/24	159.65.5.0/24
50.229.193.0/24	47.89.30.0/24	159.65.84.0/24
99.255.14.0/24	165.22.22.0/24	81.28.6.0/24
216.71.192.0/19	165.22.92.0/24	83.229.87.0/24
64.154.25.0/24	206.189.61.0/24	138.68.173.0/24
198.175.72.0/24	104.248.48.0/24	68.183.46.0/24
106.1.186.0/24	24.199.98.0/24	68.183.233.0/24
89.109.35.0/24	164.92.167.0/24	68.183.177.0/24
209.206.38.0/24	113.30.191.0/24	64.226.68.0/24
35.221.210.0/24	113.30.151.0/24	

全国大学生信息安全竞赛组织委员会

附录二　测绘结果数据文件格式示例（json 串）


```
{
    "192.108.10.11": {
        "services": [
            {
                "port": 22,
                "protocol": "ssh",
                "service_app": ["SSH/N"]
            },
            {
                "port": 23,
                "protocol": "telnet",
                "service_app": ["Telnet/N"]
            },
            {
                "port": 80,
                "protocol": "http",
                "service_app": ["Nginx/0.8.53", "WordPress/4.7"]
            }
        ],
        "deviceinfo":"route/fritz",
        "honeypot":["22/kippo","80/glastopf"],
        "timestamp":"2023-05-06 20:21:22"

    },
        "192.118.30.33": {
        "services": [
            {
                "port": 22,
                "protocol": "ssh",
                "service_app": ["SSH/N"]
            },
            {
                "port": 8888,
                "protocol": "http",
                "service_app": ["Apache/2.2.15", "Joomla/N"]
            },
            {
                "port": 3306,
```

```
                    "protocol": "mysql",
                    "service_app": ["mysql/N"]
                },
                {
                    "port": 3389,
                    "protocol": "rdp",
                    "service_app": ["rdp/N"]
                },
                {
                    "port": 9999,
                    "protocol": null,
                    "service_app": null
                }
            ],
              "deviceinfo":null,
                "honeypot":["22/kippo","80/glastopf","3306/N"],
              "timestamp":"2023-06-07 15:16:17"
        }
    }
```


字段及含义：

（1）ip: 目标 IP，例如：1.2.3.4

（2）services：包含多个 port、protocol、service_app 字段数据组合

（3）port：目标端口，例如：23

（4）protocol：端口开放协议（小写），例如：http。

（5）service_app：记录服务指纹信息，例如：["Nginx/0.8.53", "WordPress/4.7"]

（6）deviceinfo：记录设备信息，包含设备类型 /产品名

称，例如：route/fritz

（7）honeypot： 记录蜜罐信息，包含端口/蜜罐，例如：["22/kippo","80/glastopf","3306/N"]

（8）timestamp：记录测绘结果生成日期时间戳，格式：“YYYY-MM-DD HH:MM:SS”。