**第十六届山东省职业院校技能大赛中职组**

**“网络安全”赛项竞赛试题**

# 一、竞赛时间

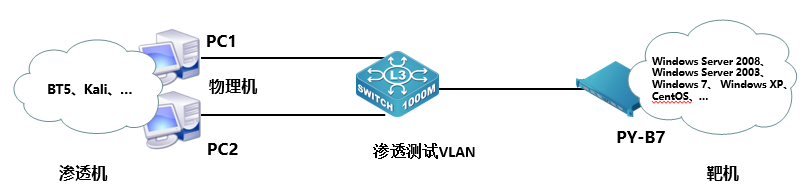
总计：360分钟

# 二、竞赛阶段

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **竞赛阶段** | **任务阶段** | **竞赛任务** | **竞赛时间** | **分值** |
| A、B模块 | A-1 | 登录安全加固 | 180分钟 | 200分 |
| A-2 | 本地安全策略设置 |
| A-3 | 流量完整性保护 |
| A-4 | 事件监控 |
| A-5 | 服务加固 |
| A-6 | 防火墙策略 |
| B-1 | Linux系统渗透提权 | 400分 |
| B-2 | 内存取证 |
| B-3 | 页面信息发现 |
| B-4 | 数字取证调查 |
| B-5 | 网络安全应急响应 |
| B-6 | Python代码分析 |
| B-7 | 逆向分析 |
| C、D模块 | C模块 | CTF夺旗-攻击 | 180分钟 | 200分 |
| D模块 | CTF夺旗-防御 | 200分 |

# 三、竞赛任务书内容

## （一）拓扑图



## （二）A模块基础设施设置/安全加固（200分）

一、项目和任务描述：

假定你是某企业的网络安全工程师，企业服务器可能被黑客攻击， 进行了未知操作，为了确保服务器正常运行，请按照网络安全岗位实 施规范，进行相关操作。通过综合运用用户安全管理与密码策略、Nginx安全策略、日志监控策略、中间件服务安全策略、本地安全策略、防火墙策略等多种安全策略来提升服务器系统的网络安全防御能力。本模块要求根据竞赛现场提供的A模块答题模板对具体任务的操作进行截图并加以相应的文字说明，以word文档的形式书写,以PDF格式保存。

二、服务器环境说明

AServer08(windows)、 用户名：administrator，密码：123456

AServer09(linux) 用户名：root，密码：123456

三、说明：

1.所有截图要求截图界面、字体清晰，并粘贴于相应题目要求的位置；

2.文件名命名及保存：网络安全模块A-XX（XX为工位号），PDF格式保存；

3.文件保存到U盘提交。

**A-1：登录安全加固（Windows, Linux）**

请对服务器Windows、Linux按要求进行相应的设置，提高服务器的安全性。

1.密码策略（Windows, Linux）

a.最小密码长度不少于13个字符（Windows）；

b.密码必须符合复杂性要求（Linux）。

2.用户安全管理(Windows)

a.设置取得文件或其他对象的所有权，将该权限只指派给administrators组；

b.禁止普通用户使用命令提示符;

c.设置不显示上次登录的用户名。

**A-2：Nginx安全策略（Linux）**

3.禁止目录浏览和隐藏服务器版本和信息显示；

4.限制HTTP请求方式，只允许GET、HEAD、POST；

5.设置客户端请求主体读取超时时间为10；

6.设置客户端请求头读取超时时间为10；

7.将Nginx服务降权，使用www用户启动服务。

**A-3：日志监控（Windows）**

8.安全日志文件最大大小为128MB，设置当达到最大的日志大小上限时，按需要覆盖事件（旧事件优先）；

9.应用日志文件最大大小为64MB，设置当达到最大的日志大小上限时将其存档，不覆盖事件；

10.系统日志文件最大大小为32MB，设置当达到最大的日志大小上限时，不覆盖事件（手动清除日志）。

**A-4：中间件服务加固SSHD\VSFTPD\IIS（Windows, Linux）**

11.SSH服务加固（Linux）

a.修改ssh服务端口为2222；

b.ssh禁止root用户远程登录；

c.设置root用户的计划任务。每天早上7:50自动开启ssh服务，22:50关闭；每周六的7:30重新启动ssh服务；

d.修改SSHD的PID档案存放地。

12.VSFTPD服务加固（Linux）

a.设置运行vsftpd的非特权系统用户为pyftp；

b.限制客户端连接的端口范围在50000-60000；

c.限制本地用户登录活动范围限制在home目录。

13.IIS加固（Windows）

a.开启IIS的日志审计记录(日志文件保存格式为W3C,只记录日期、时间、客户端IP地址、用户名、方法)；

b.关闭IIS的WebDAV功能增强网站的安全性。

**A-5：本地安全策略（Windows）**

14.禁止匿名枚举SAM帐户；

15.禁止系统在未登录的情况下关闭；

16.禁止存储网络身份验证的密码和凭据；

17.禁止将Everyone权限应用于匿名用户；

18.在超过登录时间后强制注销。

**A-6：防火墙策略（Linux）**

19.设置防火墙允许本机转发除ICMP协议以外的所有数据包；

20.为防止SSH服务被暴力枚举，设置iptables防火墙策略仅允许172.16.10.0/24网段内的主机通过SSH连接本机；

21.为防御拒绝服务攻击，设置iptables防火墙策略对传入的流量进行过滤，限制每分钟允许3个包传入，并将瞬间流量设定为一次最多处理6个数据包（超过上限的网络数据包将丢弃不予处理）；

22.只允许转发来自172.16.0.0/24局域网段的DNS解析请求数据包。

## （三）B模块安全事件响应/网络安全数据取证/应用安全（400分）

### B-1：Linux系统渗透提权

* 服务器场景：Server2214（关闭链接）
* 用户名：hacker 密码：123456

1. 使用渗透机对服务器信息收集，并将服务器中SSH服务端口号作为flag提交；
2. 使用渗透机对服务器信息收集，并将服务器中主机名称作为flag提交；
3. 使用渗透机对服务器信息收集，并将服务器中系统内核版本作为flag提交；
4. 使用渗透机对服务器管理员提权，并将服务器中root目录下的文本内容作为flag提交；
5. 使用渗透机对服务器管理员提权，并将服务器中root的密码作为flag提交；
6. 使用渗透机对服务器管理员提权，并将服务器中root目录下的图片内容作为flag提交。

### B-2：内存取证

* 服务器场景：win20230306（关闭链接）
* FTP用户名：user，密码：123456

1. 在服务器中下载内存片段，在内存片段中获取主机信息，将管理员密码作为Flag值提交；
2. 在内存片段中获取主机信息，将此片段的地址作为Flag值提交；
3. 在内存片段中获取主机信息，将此片段的主机名作为Flag值提交；
4. 在内存片段中获取主机信息，将挖矿程序的地址及端口号作为Flag值提交；（若为多个用;分开）
5. 在内存片段中获取主机信息，将后台恶意程序所用的程序名称作为Flag值提交；
6. 在内存片段中获取主机信息，将此时的浏览器搜寻的关键词作为Flag值提交。

### B-3：页面信息发现

* 服务器场景：win20230305（关闭链接）

1. 在渗透机中对服务器信息收集，将获取到的服务器网站端口作为Flag值提交；
2. 访问服务器网站页面，找到主页面中的Flag值信息，将Flag值提交；
3. 访问服务器网站页面，找到主页面中的脚本信息，并将Flag值提交；
4. 访问服务器网站页面，找到登录页面信息，将登录成功后的信息作为Flag值提交；
5. 访问服务器网站页面，找到转化页面信息，将Flag值提交；
6. 访问服务器网站页面，找到对比页面信息，将Flag值提交。

### B-4：数字取证调查

* 服务器场景：FTPServer20221010（关闭链接）
* 服务器场景操作系统：未知
* FTP用户名:attack817密码：attack817

1. 分析attack.pcapng数据包文件，通过分析数据包attack.pcapng找出恶意用户第一次访问HTTP服务的数据包是第几号，将该号数作为Flag值提交；
2. 继续查看数据包文件attack.pcapng，分析出恶意用户扫描了哪些端口，将全部的端口号从小到大作为Flag值（形式：端口1,端口2,端口3…,端口n）提交；
3. 继续查看数据包文件attack.pcapng分析出恶意用户登录后台所用的密码是什么，将后台密码作为Flag值提交；
4. 继续查看数据包文件attack.pcapng分析出恶意用户写入的一句话木马的密码是什么，将一句话密码作为Flag值提交；
5. 继续查看数据包文件attack.pcapng分析出恶意用户下载了什么文件，将该文件内容作为Flag值提交。

### B-5：网络安全应急响应

* 服务器场景：Server2228（开放链接）
* 用户名：root，密码：p@ssw0rd123

1. 找出系统中被植入的后门用户删除掉，并将后门用户的账号作为Flag值提交（多个用户名之间以英文逗号分割，如：admin,root）；
2. 找出黑客在admin用户家目录中添加的ssh后门，将后门的写入时间作为Flag值（提交的时间格式为：2022-01-12 08:08:18）
3. 找出黑客篡改过的环境变量文件并还原，将文件的md5值作为Flag值提交；
4. 找出黑客修改了bin目录下的某个文件，将该文件的格式作为Flag值提交；
5. 找出黑客植入系统中的挖矿病毒，将矿池的钱包地址作为Flag值（提交格式为：0xa1d1fadd4fa30987b7fe4f8721b022f4b4ffc9f8）提交。

### B-6：Python代码分析

* 服务器场景：Server2023111301（开放链接）
* 用户名：administrator，密码：123456

1. 完善Server2023110901桌面上的Flag.py文件，填写该文件当中空缺的Flag1字符串，并将该字符串作为Flag值提交；（Flag.py在Python代码分析文件夹中）
2. 继续完善Flag.py文件，填写该文件当中空缺的Flag2字符串，并将该字符串作为Flag值提交；
3. 继续完善Flag.py文件，填写该文件当中空缺的Flag3字符串，并将该字符串作为Flag值提交；
4. 继续完善Flag.py文件，填写该文件当中空缺的Flag4字符串，并将该字符串作为Flag值提交；
5. 将完善好的脚本文件在Kali上执行，将执行成功后的回显内容作为Flag值提交。

### B-7：逆向分析

* 服务器场景：Server2023111301（开放链接）
* 用户名：administrator，密码：123456

1. 在 JavaScript 语言中，将给定的长字符串转换为一个数组的方法，将该方法应用于逆向解码操作（可执行文件位于Server2023111301桌面逆向分析文件夹中），所得的结果进行Base64运算，将过程中使用的方法作为Flag值提交（例如：array.splice()）；
2. 写出在字符串中匹配连续的四个字符，且每两个字符之间用空格分隔的正则匹配表达式，将该正则表达式应用于逆向解码操作，所得的结果进行Base64运算，将过程中使用的方法作为Flag值提交（例如：array.splice()）；
3. 使用 JavaScript 中的方法，将迭代器中的每个匹配项取出第一个字符，也就是每个四字符组的第一个字符。将该方法应用于逆向解码操作，所得的结果进行Base64运算，将过程中使用的方法作为Flag值提交（例如：array.splice()）；
4. 使用 JavaScript 中的方法，对上一个步骤中得到的结果的字符进行操作，将它们用空格分隔、反转顺序，然后再连接起来。所得的结果进行Base64运算，将过程中使用的方法作为Flag值提交（例如：array.splice()）；
5. 使用 JavaScript 中的方法，将倒序排列后的字符解释为十六进制数字，然后将其右移2位。所得的结果进行Base64运算，将过程中使用的方法作为Flag值提交（例如：array.splice()）；
6. 将上一步处理后的数字转换为相应的Unicode字符。并将所有转换后的Unicode字符连接成一个字符串。所得的结果进行Base64运算，将运算后得到的结果作为Flag值提交。

## （四）模块C CTF夺旗-攻击

**（本模块200分）**

一、项目和任务描述：

假定你是某企业的网络安全渗透测试工程师，负责企业某些服务器的安全防护，为了更好的寻找企业网络中可能存在的各种问题和漏洞。你尝试利用各种攻击手段，攻击特定靶机，以便了解最新的攻击手段和技术，了解网络黑客的心态，从而改善您的防御策略。

请根据《赛场参数表》提供的信息，在客户端使用谷歌浏览器登录答题平台。

二、操作系统环境说明：

客户机操作系统：Windows 10/Windows7

靶机服务器操作系统：Linux/Windows

三、漏洞情况说明：

1.服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

2.靶机服务器上的网站可能存在命令注入的漏洞，要求选手找到命令注入的相关漏洞，利用此漏洞获取一定权限;

3.靶机服务器上的网站可能存在文件上传漏洞，要求选手找到文件上传的相关漏洞，利用此漏洞获取一定权限;

4.靶机服务器上的网站可能存在文件包含漏洞，要求选手找到文件包含的相关漏洞，与别的漏洞相结合获取一定权限并进行提权;

5.操作系统提供的服务可能包含了远程代码执行的漏洞，要求用户找到远程代码执行的服务，并利用此漏洞获取系统权限;

6.操作系统提供的服务可能包含了缓冲区溢出漏洞，要求用户找到缓冲区溢出漏洞的服务，并利用此漏洞获取系统权限;

7.操作系统中可能存在一些系统后门，选手可以找到此后门，并利用预留的后门直接获取到系统权限。

四、注意事项：

1.不能对裁判服务器进行攻击，警告一次后若继续攻击将判令该参赛队离场；

2.flag值为每台靶机服务器的唯一性标识，每台靶机服务器仅有1个；

3.在登录自动评分系统后，提交靶机服务器的flag值，同时需要指定靶机服务器的IP地址；

4.赛场根据难度不同设有不同基础分值的靶机，对于每个靶机服务器，前三个获得flag值的参赛队在基础分上进行加分，本阶段每个队伍的总分均计入阶段得分；

5.本环节不予补时。

## （五）模块D CTF夺旗-防御

**（本模块200分）**

一、项目和任务描述：

假定各位选手是某安全企业的网络安全工程师，负责若干服务器的渗透测试与安全防护，这些服务器可能存在着各种问题和漏洞。你需要尽快对这些服务器进行渗透测试与安全防护。每个参赛队拥有专属的堡垒机服务器，其他队不能访问。参赛选手通过扫描、渗透测试等手段检测自己堡垒服务器中存在的安全缺陷，进行针对性加固，从而提升系统的安全防御性能。

请根据《赛场参数表》提供的信息，在客户端使用谷歌浏览器登录需要加固的堡垒服务器。

二、操作系统环境说明：

客户机操作系统：Windows 10/Windows7

堡垒服务器操作系统：Linux/Windows

三、漏洞情况说明：

1.堡垒服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

2.堡垒服务器上的网站可能存在命令注入的漏洞，要求选手找到命令注入的相关漏洞，利用此漏洞获取一定权限;

3.堡垒服务器上的网站可能存在文件上传漏洞，要求选手找到文件上传的相关漏洞，利用此漏洞获取一定权限;

4.堡垒服务器上的网站可能存在文件包含漏洞，要求选手找到文件包含的相关漏洞，与别的漏洞相结合获取一定权限并进行提权;

5.操作系统提供的服务可能包含了远程代码执行的漏洞，要求用户找到远程代码执行的服务，并利用此漏洞获取系统权限;

6.操作系统提供的服务可能包含了缓冲区溢出漏洞，要求用户找到缓冲区溢出漏洞的服务，并利用此漏洞获取系统权限;

7.操作系统中可能存在一些系统后门，选手可以找到此后门，并利用预留的后门直接获取到系统权限。

四、注意事项：

1.每位选手需要对加固点和加固过程截图，并自行制作系统防御实施报告，最终评分以实施报告为准;

2.系统加固时需要保证堡垒服务器对外提供服务的可用性；

3.不能对裁判服务器进行攻击，警告一次后若继续攻击将判令该参赛队离场；

4.本环节不予补时。

二、说明：

1.所有截图要求截图界面、字体清晰；

2.文件名命名及保存：网络安全模块D-XX（XX为工位号），PDF格式保存；

3.文件保存到U盘提交。