试题2

*信息安全管理与评估 第一阶段*

*网络平台搭建与设备安全防护*

**目 录**

[第一阶段竞赛项目试题 3](#_Toc98108397)

[介绍 3](#_Toc98108398)

[所需的设备、机械、装置和材料 3](#_Toc98108399)

[评分方案 3](#_Toc98108400)

[注意事项 3](#_Toc98108401)

[项目和任务描述 3](#_Toc98108402)

[1. 网络拓扑图 3](#_Toc98108403)

[2. IP地址规划表 5](#_Toc98108404)

[任务1：网络平台搭建 6](#_Toc98108405)

[任务2：网络安全设备配置与防护 6](#_Toc98108406)

[第二阶段竞赛项目试题 13](#_Toc98108407)

[介绍 13](#_Toc98108408)

[所需的设备、机械、装置和材料 13](#_Toc98108409)

[评分方案 13](#_Toc98108410)

[项目和任务描述 13](#_Toc98108411)

[工作任务 14](#_Toc98108412)

[第一部分 网络安全事件响应 14](#_Toc98108413)

[任务1：应急响应 14](#_Toc98108414)

[本任务素材清单：Server服务器虚拟机。 14](#_Toc98108415)

[第二部分 数字取证调查 14](#_Toc98108416)

[任务2 ：操作系统恶意程序检测 14](#_Toc98108417)

[本任务素材清单：操作系统镜像、内存镜像。 14](#_Toc98108418)

[任务3： 网络数据包分析 15](#_Toc98108419)

[本任务素材清单：捕获的网络数据包文件。 15](#_Toc98108420)

[任务4： 计算机单机取证 15](#_Toc98108421)

[本任务素材清单：取证镜像文件。 16](#_Toc98108422)

[第三部分 应用程序安全 17](#_Toc98108423)

[任务5：Android恶意程序分析 17](#_Toc98108424)

[本任务素材清单：android的apk文件。 17](#_Toc98108425)

[任务6：恶意脚本代码分析 17](#_Toc98108426)

[本任务素材清单：恶意脚本文件或感染恶意脚本的普通用户文件。 17](#_Toc98108427)

[第三阶段竞赛项目试题 19](#_Toc98108428)

[介绍 19](#_Toc98108429)

[所需的设备、机械、装置和材料 19](#_Toc98108430)

[评分方案 19](#_Toc98108431)

[注意事项 19](#_Toc98108432)

[项目和任务描述 19](#_Toc98108433)

[工作任务 20](#_Toc98108434)

[分值分布表 22](#_Toc98108435)

[附录A 23](#_Toc98108436)

# 第一阶段竞赛项目试题

本文件为信息安全管理与评估项目竞赛-第一阶段试题，第一阶段内容包括：网络平台搭建与设备安全防护。

本次比赛时间为180分钟。

# 介绍

|  |  |  |
| --- | --- | --- |
| **竞赛阶段** | **任务阶段** | **竞赛任务** |
| 第一阶段  平台搭建与安全设备配置防护 | 任务1 | 网络平台搭建 |
| 任务2 | 网络安全设备配置与防护 |

# 所需的设备、机械、装置和材料

所有测试项目都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

# 评分方案

本项目阶段分数为30分。

# 注意事项

赛题第一阶段请按裁判组专门提供的U盘中的“XXX-答题模板”中的要求提交答案。选手需要在U盘的根目录下建立一个名为“GWxx”的文件夹（xx用具体的工位号替代），所完成的“XXX-答题模板”放置在文件夹中作为比赛结果提交。

# 项目和任务描述

## 网络拓扑图



## IP地址规划表

|  |  |  |  |
| --- | --- | --- | --- |
| **设备名称** | **接口** | **IP地址** | **对端设备** |
| 防火墙  FW | ETH0/1-2（AG1） | AG1.113  10.1.0.254/30  （Trust安全域） | CS ETH1/0/1  CS ETH1/0/2 |
| AG1.114  10.2.0.254/30  （Trust安全域） |
| ETH0/3 | 10.3.0.254/30  （Trust安全域） | BC ETH3 |
| ETH0/4 | 10.4.0.254/30  （Trust安全域） | BC ETH4 |
| ETH0/5 | 10.100.18.1/27  （untrust安全域） | IDC SERVER  10.100.18.2 |
| ETH0/6 | 200.1.1.1/28  （untrust安全域） | INTERNET |
| Loopback1 | 10.11.0.1/24  （Trust安全域） | - |
| Loopback2 | 10.12.0.1/24  （Trust安全域） |
| Loopback3 | 10.13.0.1/24  （Trust安全域） |
| Loopback4 | 10.14.0.1/24  （Trust安全域） |
| 路由交换机  CS | VLAN 40  ETH1/0/4-8 | 172.16.40.62/26 | PC2 |
| VLAN 50  ETH1/0/3 | 172.16.50.62/26 | PC3 |
| VLAN 51  ETH1/0/23 | 10.51.0.254/30 | BC ETH5 |
|  | VLAN 52  ETH1/0/24 | 10.52.0.254/24 | WAF ETH3 |
|  | VLAN 113  ETH1/0/1 | VLAN113 OSPF  10.1.0.253/30 | FW ETH0/1 |
|  | VLAN 114  ETH1/0/2 | VLAN114 OSPF  10.2.0.253/30 | FW ETH0/2 |
|  | VLAN 117  ETH E1/0/17 | 10.3.0.253/30 | BC ETH1 |
|  | VLAN 118  CS ETH E1/0/18 | 10.4.0.253/30 | BC ETH2 |
|  | ETH1/0/20 | VLAN 100  192.168.100.1/30  2001::192:168:100:1/112  VLAN115 OSPF  10.5.0.254/30  VLAN116 OSPF  10.6.0.254/30 | WS ETH1/0/20 |
| 无线控制器WS | ETH1/0/20 | VLAN 100  192.168.100.2/30  2001::192:168:100:2/112  VLAN 115 10.5.0.253/30  VLAN 116 10.6.0.253/30 | CS ETH1/0/20 |
| VLAN 30  ETH1/0/3 | 172.16.30.62/26 | PC1 |
| 无线管理VLAN  VLAN 101  ETH1/0/21 | 需配置 | AP |
| VLAN 10 | 需配置 | 无线1 |
| VLAN 20 | 需配置 | 无线2 |
| 网络日志系统BC | ETH1 | 网桥 | FW |
| ETH3 | CS ETH E1/0/17 |
| ETH2 | 网桥 | FW |
| ETH4 | CS ETH E1/0/18 |
| ETH5 | 10.51.0.253/30 | CS ETH E1/0/23 |
| WEB应用  防火墙  WAF | ETH3 | 10.52.0.253/30 | CS ETH E1/0/24 |
| ETH4 | 堡垒服务器 |

## 任务1：网络平台搭建

|  |  |
| --- | --- |
| **题号** | **网络需求** |
| 1 | 按照IP地址规划表，对防火墙的名称、各接口IP地址进行配置。 |
| 2 | 按照IP地址规划表，对三层交换机的名称进行配置，创建VLAN并将相应接口划入VLAN, 对各接口IP地址进行配置。 |
| 3 | 按照IP地址规划表，对无线交换机的名称进行配置，创建VLAN并将相应接口划入VLAN,对接口IP地址进行配置。 |
| 4 | 按照IP地址规划表，对网络日志系统的名称、各接口IP地址进行配置。 |
| 5 | 按照IP地址规划表，对WEB应用防火墙的名称、各接口IP地址进行配置。 |

### 任务2：网络安全设备配置与防护

1. CS开启telnet登录功能，用户名skills01，密码skills01，配置使用telnet方式登录终端界面前显示如下授权信息：“WARNING!!! Authorised access only, all of your done will be recorded! Disconnected IMMEDIATELY if you are not an authorised user! Otherwise, we retain the right to pursue the legal responsibility”；
2. 总部交换机SW配置简单网络管理协议，计划启用V3版本，V3版本在安全性方面做了极大的扩充。配置引擎号分别为62001；创建认证用户为skills01，采用3des算法进行加密，密钥为：skills01，哈希算法为SHA，密钥为：skills01；加入组ABC，采用最高安全级别；配置组的读、写视图分别为：2022\_R、2022\_W；当设备有异常时，需要使用本地的VLAN100地址发送Trap消息至网管服务器10.51.0.203，采用最高安全级别；
3. 对CS上VLAN40开启以下安全机制：

业务内部终端相互二层隔离，启用环路检测，环路检测的时间间隔为10s，发现环路以后关闭该端口，恢复时间为30分钟；如发现私设DHCP服务器则关闭该端口，配置防止ARP欺骗攻击；

1. 勒索蠕虫病毒席卷全球，爆发了堪称史上最大规模的网络攻击，通过对总部核心交换机CS所有业务VLAN下配置访问控制策略实现双向安全防护;
2. CS配置IPv6地址，使用相关特性实现VLAN50的IPv6终端可自动从网关处获得IPv6有状态地址；

WS配置IPv6地址，开启路由公告功能，路由器公告的生存期为2小时，确保VLAN30的IPv6终端可以获得IPv6无状态地址。

WS与CS之间配置RIPng， 使PC1与PC3可以通过IPv6通信；

IPv6业务地址规划如下，其它IPv6地址自行规划：

|  |  |
| --- | --- |
| **业务** | **IPV6地址** |
| VLAN30 | 2001:30::254/64 |
| VLAN50 | 2001:50::254/64 |

1. 尽可能加大CS与防火墙FW之间的带宽;配置使总部VLAN40业务的用户访问IDC SERVER的数据流经过FW 10.1.0.254, IDC SERVER返回数据流经过FW 10.2.0.254，且对双向数据流开启所有安全防护，参数和行为为默认;
2. FW、CS、WS之间配置OSPF area 0 开启基于链路的MD5认证，密钥自定义,传播访问INTERNET默认路由；
3. FW与CS建立两对IBGP邻居关系，使用AS 65500，FW上loopback1-4为模拟AS 65500中网络，为保证数据通信的可靠性和负载，完成以下配置，要求如下：

* CS通过BGP到达loopback1,2网路下一跳为10.3.0.254；
* CS通过BGP到达loopback3,4网络下一跳为10.4.0.254；
* 通过BGP实现到达loopback1,2,3,4的网络冗余；
* 使用IP前缀列表匹配上述业务数据流；
* 使用LP属性进行业务选路，只允许使用route-map来改变LP属性、实现路由控制，AS PATH属性可配置的参数数值为：65509

1. 如果CS E1/0/3端口的收包速率超过30000则关闭此端口，恢复时间5分钟，并每隔10分钟对端口的速率进行统计；为了更好地提高数据转发的性能，CS交换中的数据包大小指定为1600字节；
2. 为实现对防火墙的安全管理，在防火墙FW的Trust安全域开启PING,HTTP，SNMP功能（loopback接口除外），Untrust安全域开启SSH、HTTPS功能;
3. 总部VLAN业务用户通过防火墙访问Internet时，复用公网IP： 200.1.1.28/28，保证每一个源IP产生的所有会话将被映射到同一个固定的IP地址，当有流量匹配本地址转换规则时产生日志信息，将匹配的日志发送至10.51.0.253的 UDP 2000端口；
4. 配置L2TP VPN，名称为VPN，满足远程办公用户通过拨号登陆访问内网，创建隧道接口为tunnel 1、并加入untrust安全域，地址池名称为AddressPool，LNS 地址池为10.100.253.1/24-10.100.253.100/24，网关为最大可用地址，认证账号skills01,密码skills01；
5. FW 配置禁止所有人在周一至周五工作时间 9：00-18：00 访问京东www.jd.com 和淘宝 www.taobao.com;相同时间段禁止访问中含有“娱乐”、“新闻”的 WEB 页面；
6. 在FW开启安全网关的TCP SYN包检查功能，只有检查收到的包为TCP SYN包后，才建立连接；配置所有的TCP数据包每次能够传输的最大数据分段为1460，尽力减少网络分片；配置对TCP三次握手建立的时间进行检查，如果在1分钟内未完成三次握手，则断掉该连接；
7. 为保证总部Internet出口线路，在FW上使用相关技术，通过ping监控外网网关地址，监控对象名称为Track，每隔5S发送探测报文，连续10次收不到监测报文，就认为线路故障，直接关闭外网接口。FW要求内网每个IP限制会话数量为300；
8. Internet端有一分支结构路由器，需要在总部防火墙FW上完成以下预配，保证总部与分支机构的安全连接：

防火墙FW与Internet端路由器202.5.17.2建立GRE隧道，并使用IPSec保护GRE隧道，保证分支结构中2.2.2.2与总部VLAN40安全通信。

第一阶段 采用pre-share认证 加密算法:3DES；

第二阶段 采用ESP协议， 加密算法:3DES，预设共享秘钥: skills01

1. 已知原AP管理地址为10.81.0.0/15，为了避免地址浪费请重新规划和配置IP地址段，要求如下：

* 使用原AP所在网络进行地址划分；
* 现无线用户VLAN 10中需要127个终端，无线用户VLAN 20需要50个终端；
* WS上配置DHCP，管理VLAN为VLAN101,为AP下发管理地址，网段中第一个可用地址为AP管理地址，最后一个可用地址为WS管理地址，保证完成AP二层注册；为无线用户VLAN10,20下发IP地址，最后一个可用地址为网关；

1. 在NETWORK下配置SSID，需求如下：

* NETWORK 1下设置SSID 2022skills-2.4G，VLAN10，加密模式为wpa-personal,其口令为skills01；
* NETWORK 20下设置SSID 2022skills-5G，VLAN20不进行认证加密,做相应配置隐藏该SSID, 只使用倒数第一个可用VAP发送5.0G信号；

1. 配置一个SSID 2022skills\_IPv6，属于VLAN21用于IPv6无线测试，用户接入无线网络时需要采用基于WPA-personal加密方式，其口令为“skills01”，该网络中的用户从WS DHCP获取IPv6地址，地址范围为：2001:10:81::/112;
2. NETWORK 1开启内置portal+本地认证的认证方式，账号为GUEST密码为123456,保障无线信息的覆盖性，无线AP的发射功率设置为90%。禁止MAC地址为80-45-DD-77-CC-48的无线终端连接;
3. 通过配置防止多AP和WS相连时过多的安全认证连接而消耗CPU资源，检测到AP与WS在10分钟内建立连接5次就不再允许继续连接，两小时后恢复正常;
4. 为方便合理使用带宽，要求针对SSID为“2022skills-2.4”下的用户进行带宽控制。对用户上行速率没有限制，但是针对下行速率要求用户的带宽为2Mbps，在最大带宽可以达到4Mbps;
5. 配置所有Radio接口：AP在收到错误帧时，将不再发送ACK帧；打开AP组播广播突发限制功能；开启Radio的自动信道调整，每天上午10:00触发信道调整功能;
6. 配置所有无线接入用户相互隔离，Network模式下限制每天早上0点到4点禁止终端接入，开启ARP抑制功能；
7. 配置当AP上线，如果WS中储存的Image版本和AP的Image版本号不同时，会触发AP自动升级；配置AP发送向无线终端表明AP存在的帧时间间隔为1秒；配置AP失败状态超时时间及探测到的客户端状态超时时间都为2小时;
8. 在公司总部的BC上配置，设备部署方式为透明模式。增加非admin账户skills01，密码skills01，该账户仅用于用户查询设备的日志信息和统计信息；要求对内网访问Internet全部应用进行日志记录。
9. 为日志查询的时间准确性，要求在BC上配置NTP服务，NTP服务器设定为中国科学院国家授时中心(ntp.ntsc.ac.cn)。
10. 在公司总部的BC上配置，在工作日（每周一到周五上班）期间针对所有无线网段访问互联网进行审计，如果发现访问互联网的无线用户就断网20分钟，不限制其他用户在工作日（每周一到周五上班）期间访问互联网。
11. BC 配置应用“即时聊天”，在周一至周五8：00-20：00监控内网中所有用户的QQ账号使用记录，并保存QQ聊天记录数据包；
12. BC配置内容管理，对邮件内容包含“协议”、“投诉”字样的邮件，记录且邮件报警。
13. BC上配置报警邮箱，邮件服务器IP为172.16.10.33，端口号为25，账号为:skills01,密码: skills01，最大记录数量为50，同时把报警邮件抄送给Manager@ chinaskills.com;
14. 使用BC对内网所有上网用户进行上网本地认证，要求认证后得用户4小时候重新认证，并且对HTTP服务器172.16.10.45的80端口进行免认证；
15. BC上配置用户识别功能,对内网所有IP地址进行身份识别；
16. 在公司总部的WAF上配置，设备部署方式为透明模式。要求对内网HTTP服务器172.16.10.45/32进行安全防护;
17. 为更好对服务器172.16.10.45进行防护，我们定期对服务器进行Web漏洞扫描，来及时修改我们的防护规则。
18. 方便日志的保存和查看，需要在把WAF上攻击日志、访问日志、DDoS日志以JSON格式发给IP地址为172.16.10.200的日志服务器上;
19. 在WAF上配置基础防御功能，开启SQL注入、XXS攻击、信息泄露等防御功能，要求针对这些攻击阻断并发送邮件告警;
20. 在WAF上针对HTTP服务器进行URL最大个数为10，Cookies最大个数为30，Host最大长度为1024，Accept最大长度64等参数校验设置，设置严重级别为中级，超出校验数值阻断并发送邮件告警;
21. 在WAF上保护HTTP服务器上的www.2022skills.com网站爬虫攻击，从而影响服务器性能，设置严重级别为高级，一经发现攻击阻断并发送邮件告警;
22. 为防止www.2022skills.com网站资源被其他网站利用，通过WAF对资源链接进行保护，通过Referer方式检测，设置严重级别为中级，一经发现阻断并发送邮件告警;



*信息安全管理与评估 第二阶段*

*网络安全事件响应*

*数字取证调查*

*应用程序安全*

# 第二阶段竞赛项目试题

本文件为信息安全管理与评估项目竞赛-第二阶段试题，第二阶段内容包括：网络安全事件响应、数字取证调查和应用程序安全。

本次比赛时间为180分钟。

# 介绍

竞赛有固定的开始和结束时间，参赛队伍必须决定如何有效的分配时间。请认真阅读以下指引！

（1）当竞赛结束，离开时请不要关机；

（2）所有配置应当在重启后有效；

（3）除了CD-ROM/HDD/NET驱动器，请不要修改实体机的配置和虚拟机本身的硬件设置。

# 所需的设备、机械、装置和材料

所有测试项目都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

# 评分方案

本项目模块分数为35分。

# 项目和任务描述

随着网络和信息化水平的不断发展，网络安全事件也层出不穷，网络恶意代码传播、信息窃取、信息篡改、远程控制等各种网络攻击行为已严重威胁到信息系统的机密性、完整性和可用性。因此，对抗网络攻击，组织安全事件应急响应，采集电子证据等技术工作是网络安全防护的重要部分。现在，A集团已遭受来自不明组织的非法恶意攻击，您的团队需要帮助A集团追踪此网络攻击来源，分析恶意攻击攻击行为的证据线索，找出操作系统和应用程序中的漏洞或者恶意代码，帮助其巩固网络安全防线。

本模块主要分为以下几个部分：

* 网络安全事件响应
* 数字取证调查
* 应用程序安全

本部分的所有工作任务素材或环境均已放置在指定的计算机上，参赛选手完成后，填写在电脑桌面上“信息安全管理与评估竞赛-第二阶段答题卷”中。选手的电脑中已经安装好 Office 软件并提供必要的软件工具 （Tools 工具包）。

# 工作任务

## 第一部分 网络安全事件响应

### 任务1：应急响应

A集团的Linux应用服务器被黑客入侵，该服务器的应用系统被上传恶意软件，系统文件被恶意软件破坏，您的团队需要帮助该公司追踪此网络攻击的来源，在服务器上进行全面的检查，包括日志信息、进程信息、系统文件、恶意文件等，从而分析黑客的攻击行为，发现系统中的漏洞。

### 本任务素材清单：Server服务器虚拟机。

受攻击的Server服务器已整体打包成虚拟机文件保存，请选手自行导入分析。

注意：Server服务器的基本配置参见附录，若题目中未明确规定，请使用默认配置。

请根据赛题环境及任务要求提交正确答案。

|  |  |  |
| --- | --- | --- |
| **任务1：应急响应** | | |
| **序号** | **任务要求** | **答案** |
| 1 | 任务要求1 |  |
| 2 | 任务要求2 |  |
| 3 | 任务要求3 |  |
| 4 | ...... |  |

## 第二部分 数字取证调查

### 任务2 ：操作系统恶意程序检测

A集团某服务器系统感染恶意程序，导致系统关键文件被破坏，请分析A集团提供的系统镜像和内存镜像，找到系统镜像中的恶意软件，分析恶意软件行为。

### 本任务素材清单：操作系统镜像、内存镜像。

请根据赛题环境及任务要求提交正确答案。

|  |  |  |
| --- | --- | --- |
| **任务2：操作系统恶意程序检测** | | |
| **序号** | **任务要求** | **答案** |
| 1 | 任务要求1 |  |
| 2 | 任务要求2 |  |
| 3 | 任务要求3 |  |
| 4 | ...... |  |

### 任务3： 网络数据包分析

A集团的网络安全监控系统发现恶意份子正在实施高级可持续攻击（APT），并抓取了部分可疑流量包。请您根据捕捉到的流量包，搜寻出网络攻击线索，分解出隐藏的恶意程序，并分析恶意程序的行为。

### 本任务素材清单：捕获的网络数据包文件。

请根据赛题环境及任务要求提交正确答案。

|  |  |  |
| --- | --- | --- |
| **任务3：网络数据包分析** | | |
| **序号** | **任务要求** | **答案** |
| 1 | 任务要求1 |  |
| 2 | 任务要求2 |  |
| 3 | 任务要求3 |  |
| 4 | ...... |  |

### 任务4： 计算机单机取证

对给定取证镜像文件进行分析，搜寻证据关键字（线索关键字为“evidence 1”、“evidence 2”、……、“evidence 10”，有文本形式也有图片形式，不区分大小写），请提取和固定比赛要求的标的证据文件，并按样例的格式要求填写相关信息，证据文件在总文件数中所占比例不低于15%。取证的信息可能隐藏在正常的、已删除的或受损的文件中，您可能需要运用编码转换技术、加解密技术、隐写技术、数据恢复技术，还需要熟悉常用的文件格式（如办公文档、压缩文档、图片等）。

### 本任务素材清单：取证镜像文件。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务4： 计算机单机取证** | | |
| **证据编号** | **在取证镜像中的文件名** | **镜像中原文件Hash码（MD5，不区分大小写）** |
| evidence 1 |  |  |
| evidence 2 |  |  |
| evidence 3 |  |  |
| evidence 4 |  |  |
| evidence 5 |  |  |
| evidence 6 |  |  |
| evidence 7 |  |  |
| evidence 8 |  |  |
| evidence 9 |  |  |
| evidence 10 |  |  |

## 第三部分 应用程序安全

### 任务5：Android恶意程序分析

A集团发现其发布的Android移动应用程序文件遭到非法篡改，您的团队需要协助A集团对该恶意程序样本进行逆向分析、对其攻击/破坏的行为进行调查取证。

### 本任务素材清单：android的apk文件。

请根据赛题环境及任务要求提交正确答案。

|  |  |  |
| --- | --- | --- |
| **任务5：Android恶意程序分析** | | |
| **序号** | **任务要求** | **答案** |
| 1 | 任务要求1 |  |
| 2 | 任务要求2 |  |
| 3 | 任务要求3 |  |
| 4 | ...... |  |

### 任务6：恶意脚本代码分析

A集团发现其网络中的存在恶意脚本感染的情况，A集团保存了包含恶意脚本的文件，您的团队需要协助A集团对该文件样本进行代码分析，对其攻击/破坏的行为进行调查取证。

### 本任务素材清单：恶意脚本文件或感染恶意脚本的普通用户文件。

请根据赛题环境及任务要求提交正确答案。

|  |  |  |
| --- | --- | --- |
| **任务6：恶意脚本代码分析** | | |
| **序号** | **任务要求** | **答案** |
| 1 | 任务要求1 |  |
| 2 | 任务要求2 |  |
| 3 | 任务要求3 |  |
| 4 | ...... |  |



*信息安全管理与评估 第三阶段*

*夺旗挑战-攻击*

# 第三阶段竞赛项目试题

本文件为信息安全管理与评估项目竞赛-第三阶段试题。根据信息安全管理与评估项目技术文件要求，第三阶段为夺旗挑战-攻击。

本次比赛时间为180分钟。

# 介绍

夺旗挑战赛（CTF）的目标是作为一名网络安全专业人员在一个模拟的网络环境中实现网络安全渗透测试工作。

本模块要求参赛者作为攻击方，运用所学的信息收集、漏洞发现、漏洞利用等渗透测试技术完成对网络的渗透测试；并且能够通过各种信息安全相关技术分析获取存在的flag值。

# 所需的设备、机械、装置和材料

所有测试项目都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

# 评分方案

本项目阶段分数为35分。

# 注意事项

通过找到正确的flag值来获取得分，它的格式如下所示：

flag{<flag值 >}

这种格式在某些环境中可能被隐藏甚至混淆。所以，注意一些敏感信息并利用工具把它找出来。

# 项目和任务描述

在A集团的网络中存在几台服务器，各服务器存在着不同业务服务。在网络中存在着一定网络安全隐患，请利用你所掌握的渗透测试技术，通过信息收集、漏洞挖掘等渗透测试技术，完成指定项目的渗透测试，在测试中获取flag值。网络环境参考样例请查看附录A。

本模块所使用到的渗透测试技术包含但不限于如下技术领域：

• 信息收集

• 逆向文件分析

• 二进制漏洞利用

• 应用服务漏洞利用

• 杂项与密码学分析

所有设备和服务器的IP地址请查看现场提供的设备列表。

# 工作任务

**一、Web1服务器**

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| **任务一** | Web1系统存在隐藏信息，请找出隐藏信息，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务二** | Web1系统存在漏洞，请利用漏洞并找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务三** | Web1系统后台存在漏洞，请利用漏洞并找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |

**二、Web2服务器**

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| **任务四** | Web2系统存在漏洞，请利用漏洞并找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务五** | Web2系统后台存在漏洞，请利用漏洞并找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |

**三、****FTP服务器**

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| **任务六** | 请获取FTP服务器上对应的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务七** | 请获取FTP服务器上对应的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务八** | 请获取FTP服务器上对应的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务九** | 请获取FTP服务器上对应的流量包进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务十** | 请获取FTP服务器上对应的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务十一** | 请获取FTP服务器上对应的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务十二** | 请获取FTP服务器上对应的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务十三** | 请获取FTP服务器上对应的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |

**四、应用程序1服务器**

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| **任务十四** | 应用程序1服务器10000端口存在漏洞，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |

**五、应用程序2服务器**

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| **任务十五** | 应用程序2服务器10001端口存在漏洞，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |

# 分值分布表

表1 第三阶段分值分布

|  |  |  |
| --- | --- | --- |
| **序号** | **描述** | **分值** |
| C | 夺旗(攻击) |  |
| C1 | 信息收集 |  |
| C2 | 逆向文件分析 |  |
| C3 | 二进制漏洞利用 |  |
| C4 | 应用服务漏洞利用 |  |
| C5 | 杂项与密码学分析 |  |

# 附录A



图1 网络拓扑结构图