网络安全赛项样题

模块 A 基础设施设置与安全加固

(本模块共 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，对于企业的服务器系统，根据任务要求确保各服务正常运行，并通过综合运用登录和密码策略、数据库安全策略、流量完整性保护策略、事件监控策略、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。本模块要求对具体任务的操作截图并加以相应的文字说明,并以 word 文档的形式书写,以 PDF 格式保存,并以赛位号作为文件名.

二、服务器环境说明

IDS:入侵检测系统服务器(Snort),操作系统为 Linux

LOG:日志服务器(Splunk),操作系统为 Linux

Web:IIS 服务器,操作系统为 Windows

Data:数据库服务器(Mysql),操作系统为 Linux

三、具体任务

任务一　登录安全加固

1. 密码策略（IDS,LOG,Web,Data）

a. 最小密码长度不少于 12 个字符;

2. 登录策略（IDS,LOG,Web,Data）

a.在用户登录系统时，应该有“For authorized users only”提示信息;

3. 用户权限分配(WEB)

a.禁止来宾账户登录和访问;

任务二　数据库加固（Data）

1.以普通帐户安全运行 mysqld，禁止 mysql 以管理员帐号权限运行;

2.删除默认数据库(test);

任务三　Web 安全加固(Web)

1.删除默认站点;

2.限制目录执行权限,对图片或者上传目录设置执行权限为无;

任务四　流量完整性保护（Web,Data）

1.HTTP 重定向 HTTPS，仅使用 HTTPS 协议访问网站（Web);

2.防止密码被窃取，仅使用证书登录 SSH（Data）。

任务五　事件监控

1. Web 服务器开启审核策略：

登录事件 成功/失败；

特权使用　成功；

策略更改　成功/失败；

进程跟踪　成功/失败；

模块 B 网络安全事件、数字取证调查和应用安全

（本模块共 400 分）

一、项目和任务描述：

假定你是某网络安全技术支持团队成员，某企业的服务器系统被黑客攻击，你的团队前来帮助企业进行调查并追踪本次网络攻击的源头，分析黑客的攻击方式，发现系统漏洞，提交网络安全事件响应报告，修复系统漏洞，删除黑客在系统中创建的后门，并帮助系统恢复正常运行。

二、服务器环境说明

操作系统：Windows/Linux

三、具体任务

任务一 应急响应

*任务说明：仅能获取 Server1 的 IP 地址

1.黑客通过网络攻入本地服务器，在 Web 服务器的主页上外挂了一个木马链接，请你找到此链接并删除链接，将删除链接后的主页第一排标题栏显示的第三个单词，作为 flag 提交。

2. 黑客攻入本地服务器的数据库服务器，并添加了除 admin 以外的具有一个管理员权限的超级用户，请你找到此用户并删除用户，将此用户的密码作为 flag 提交。

3. 黑客攻入本地服务器，在本地服务器建立了多个超级用户，请你删除除了 Administrator 用户以外的其他超级管理员用户，在命令行窗口输入 net user,将 Administrator 右边第一个单词作为 flag 提交。

4. 黑客修改了服务器的启动内容，请你删除不必要的启动内容，打开任务管理器的“启动”标签栏，将名称列中所有的名称作为 flag 提交。（提交形式:名称 1，名称 2，名称 3）

5. 黑客在服务器某处存放了一个木马程序，请你找到此木马程序并清除木马。打开任务管理器的“进程”标签栏，将应用名称中的第三个单词作为 flag 提交。

任务二 数据分析

*任务说明：仅能获取 Server2 的 IP 地址

1.使用 Wireshark 查看并分析 Server2 桌面下的 capture.pcapng

数据包文件，telnet 服务器是一台路由器，找出此台路由器的特权密码，并将密码作为 flag 值提交。

2.使用 Wireshark 查看并分析 Server2 桌面下的 capture.pcapng 数据包文件，FTP 服务器已经传输文件结束，将建立 FTP 服务器的数据连接的次数作为 flag 值提交。

3.使用 Wireshark 查看并分析 Server2 桌面下的 capture.pcapng 数据包文件，web 服务器地址是 192.168.181.250，将 web 服务器软件的版本号作为 flag 值提交。

4.使用 Wireshark 查看并分析 Server2 桌面下的 capture.pcapng 数据包文件，这些数据中有非常多的 ICMP 报文，这些报文中有大量的非正常 ICMP 报文，找出类型为重定向的所有报文，将报文重定向的数量作为 flag 值提交。

5.使用 Wireshark 查看并分析 Server2 桌面下的 capture.pcapng 数据包文件，这些数据中有 ssh 报文，由于 ssh 有加密功能，现需要将这些加密报文的算法分析出来，将 ssh 服务器支持的第一个算法的密钥长度作为 flag 值提交。

任务三 Windows 操作系统渗透测试

*任务说明：仅能获取 Server3 的 IP 地址

1.通过本地 PC 中渗透测试平台 Kali 对服务器场景 Server3 进行系统服务及版本扫描渗透测试，并将该操作显示结果中 445 端口对应的服务状态信息作为 flag 值提交；

2.找到网络适配器信息，将首选DNS服务器地址作为flag值提交；

3.找到桌面上111文件夹中后缀为.docx的文件，将文档内容作为flag值提交；

4.找到回收站内的文档，将文档内容作为flag值提交；

5.获取系统最高账户管理员的密码，将密码作为flag值提交。

任务四 Linux操作系统渗透测试

*任务说明：仅能获取Server4的IP地址

1.通过本地PC中渗透测试平台Kali对服务器场景Server4进行系统服务及版本扫描渗透测试，并将该操作显示结果中21端口对应的服务版本信息字符串作为flag值提交；

2.找到/var/www目录中的图片文件，将文件名称作为flag值提交；

3.找到/var/www目录中的图片文件，将图中的英文单词作为flag值提交；

4.找到/home/guest目录中的txt文件，将文件内容作为flag值提交；

5.找到/root目录中的txt文件，将文件内容作为flag值提交。

模块C CTF夺旗-攻击

（本模块共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攻击机。

二、操作系统环境说明

客户机操作系统：Windows 10

攻击机操作系统：Kali Linux 2019 版

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；

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.选手攻入靶机后不得对靶机进行关闭端口、修改密码、重启或者关闭靶机、删除或者修改 flag、建立不必要的文件等操作；

4.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；

5. 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，具体加分规则参照赛场评分标准；

6.本环节不予补时。

模块 D CTF 夺旗-防御

（本模块共 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

攻击机操作系统：Kali Linux 2019 版

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；

四、注意事项

1.每位选手需要对加固点和关键过程截图，并自行制作系统防御实施报告，最终评分以系统防御实施报告为准。

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。

（样卷完）