w1r3s

首先从vulnhub把靶机下载下来，然后解压打开虚拟机，设置成NAT模式

一、主机发现

打开攻击机Kali，ifconfig查看本机ip为：192.168.19.145

用nmap扫描C段

```
nmap -sn 192.168.19.0/24
```

经扫描发现目标靶机ip为192.168.19.155

二、端口扫描

首先扫一下全部端口

nmap扫描全部端口 Bash 复制代码

```
┌──(root💀kali)-[~/w1r3s]

└─# nmap --min-rate 10000 -p- 192.168.19.155
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 08:16 CST
Nmap scan report for 192.168.19.155
Host is up (0.00012s latency).
Not shown: 55528 filtered tcp ports (no-response), 10003 closed tcp ports
(reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:0C:29:24:9B:CC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 12.44 seconds
```

然后进行TCP扫描

TCP扫描 Bash 复制代码

```
┌──(root💀kali)-[~/w1r3s]
└─# nmap -sT -sV -O -p21,22,80,3306 192.168.19.155
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 08:21 CST
Nmap scan report for 192.168.19.155
Host is up (0.00050s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:0C:29:24:9B:CC (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5.1
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9, Linux 5.1
Network Distance: 1 hop
Service Info: Host: W1R3S.inc; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.84 seconds

```

参数解释：sT是指定TCP传输，sV是寻求版本号，O是指操作系统，p是指端口

（值得一提的是：用kali进行小于1024的端口号的相关操作时，必须要有root权限才可以，所以如果不是root用户，需要在命令前面加上sudo）

我们可以发现这四个端口所对应的一些服务

再进行UDP扫描

UDP扫描 Bash 复制代码

```
┌──(root💀kali)-[~/w1r3s]
└─# nmap -sU -sV -O -p21,22,80,3306 192.168.19.155
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 08:21 CST
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.19.155
Host is up (0.00034s latency).

PORT     STATE         SERVICE VERSION
21/udp   open|filtered ftp
22/udp   open|filtered ssh
80/udp   open|filtered http
3306/udp closed        mysql
MAC Address: 00:0C:29:24:9B:CC (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 103.23 seconds
```

接下来用nmap自动的漏洞扫描脚本进行漏扫

`nmap --script=vuln -p21,22,80,3306 192.168.19.155`

扫描结果：

nmap漏洞扫描结果 Bash 复制代码

```
┌──(root💀kali)-[~/w1r3s]
└─# nmap --script=vuln -p21,22,80,3306 192.168.19.155
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 08:27 CST
Nmap scan report for 192.168.19.155
Host is up (0.00028s latency).

PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /wordpress/wp-login.php: Wordpress login page.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
3306/tcp open  mysql
MAC Address: 00:0C:29:24:9B:CC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 304.74 seconds

```

发现可能存在wordpress，先拿小本本记一下。

三、FTP渗透

然后我们往回梳理一下，我们先试一下FTP有没有匿名登陆

（FTP匿名登陆，用户名是anonymous，密码一般为空）

`ftp 192.168.19.155`

FTP匿名登陆 Bash 复制代码

```
┌──(root💀kali)-[~/w1r3s]
└─# ftp 192.168.19.155
Connected to 192.168.19.155.
220 Welcome to W1R3S.inc FTP service.
Name (192.168.19.155:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jan 23  2018 content
drwxr-xr-x    2 ftp      ftp          4096 Jan 23  2018 docs
drwxr-xr-x    2 ftp      ftp          4096 Jan 28  2018 new-employees
226 Directory send OK.
```

可以发现成功登录