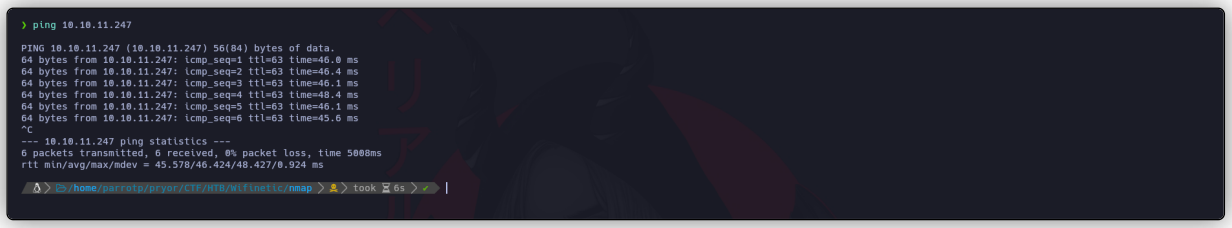
# 250- WIFINETIC


- 1. WIFINETIC
  - 1.1. Preliminar
  - 1.2. Nmap
  - 1.3. Files via FTP
    - 1.3.1. Brute-forcing SSH user
  - 1.4. Privesc via brute-forcing Wi-Fi PSK with Reaver

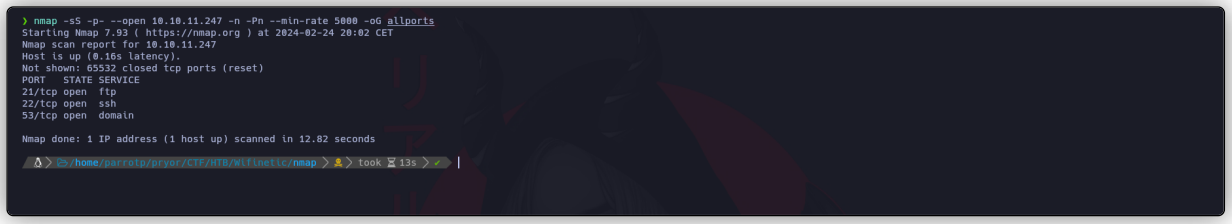

## 1. WIFINETIC

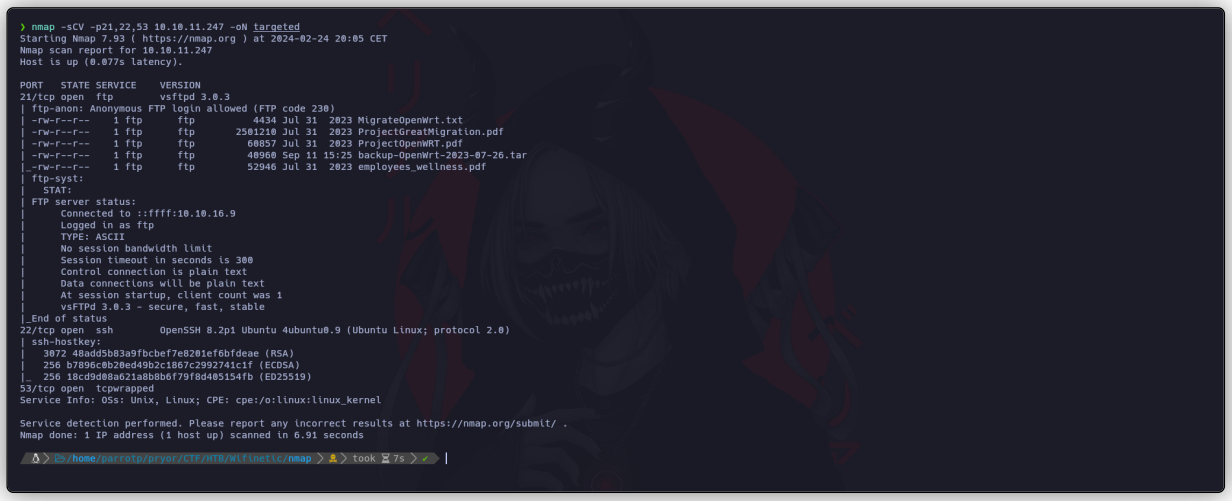
https://app.hackthebox.com/machines/Wifinetic


## 1.1. Preliminar

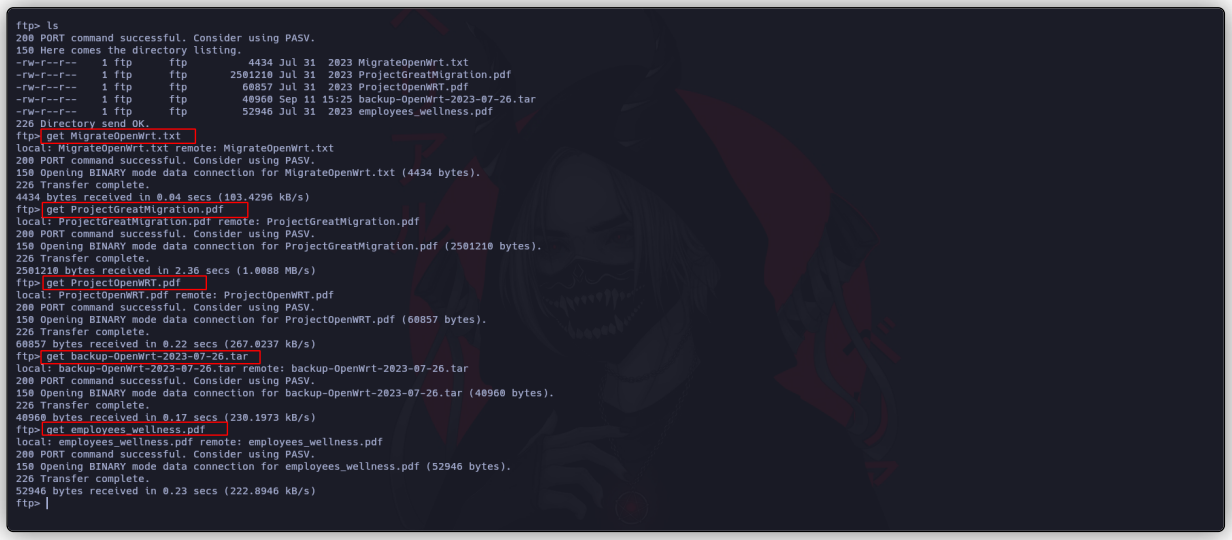
- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Parece que nos enfrentamos a una máquina *Linux*.
  - 

## 1.2. Nmap

- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos los *puertos 21, 22 y 53* abiertos.
  - 
```
❯ nmap -sS -p- --open 10.10.11.247 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-24 20:02 CET
Nmap scan report for 10.10.11.247
Host is up (0.16s latency).
Not shown: 65532 closed tcp ports (reset)
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 12.82 seconds
```

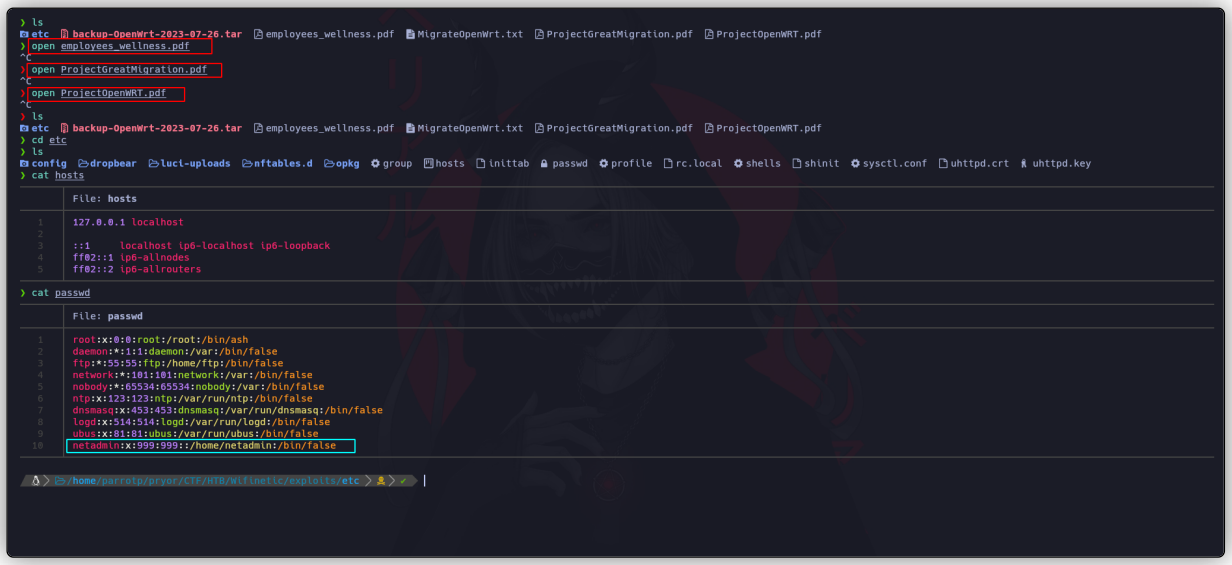
- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante `extractPorts`. El usuario *Anonymous* está habilitado en el servicio **FTP**.
  - 
```
❯ nmap -sCV -p21,22,53 10.10.11.247 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-24 20:05 CET
Nmap scan report for 10.10.11.247
Host is up (0.077s latency).

PORT   STATE SERVICE    VERSION
21/tcp open  ftp        vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 ftp      ftp          4434 Jul 31  2023 MigrateOpenWrt.txt
| -rw-r--r--    1 ftp      ftp       2501210 Jul 31  2023 ProjectGreatMigration.pdf
| -rw-r--r--    1 ftp      ftp         60857 Jul 31  2023 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  2023 employees_wellness.pdf
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.16.9
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48add5b83a9fbcbef7e8201ef6bfdeae (RSA)
|   256 b7896c0b20ed49b2c1867c2992741c1f (ECDSA)
|_  256 18cd9d08a621a8b8b6f79f8d405154fb (ED25519)
53/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 6.91 seconds
```

## 1.3. Files via FTP

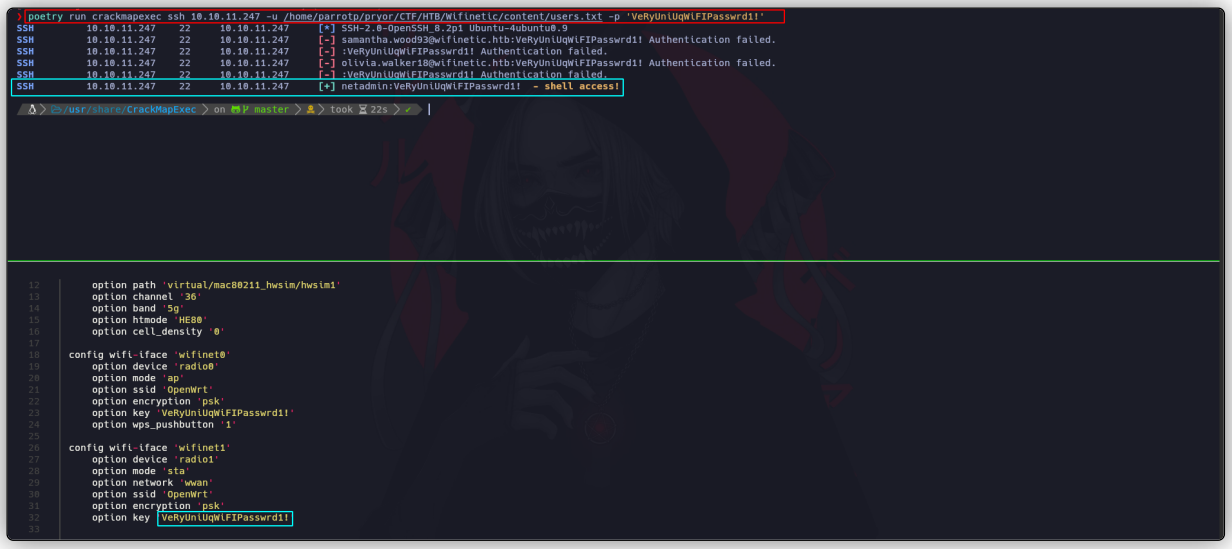
- Entramos por **FTP** como usuario *Anonymous* y descargamos unos cuantos ficheros que pensamos que pueden ser interesantes.
  - 
```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp          4434 Jul 31  2023 MigrateOpenWrt.txt
-rw-r--r--    1 ftp      ftp       2501210 Jul 31  2023 ProjectGreatMigration.pdf
-rw-r--r--    1 ftp      ftp         60857 Jul 31  2023 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  2023 employees_wellness.pdf
226 Directory send OK.
ftp> get MigrateOpenWrt.txt
local: MigrateOpenWrt.txt remote: MigrateOpenWrt.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for MigrateOpenWrt.txt (4434 bytes).
226 Transfer complete.
4434 bytes received in 0.04 secs (103.4296 kB/s)
ftp> get ProjectGreatMigration.pdf
local: ProjectGreatMigration.pdf remote: ProjectGreatMigration.pdf
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ProjectGreatMigration.pdf (2501210 bytes).
226 Transfer complete.
2501210 bytes received in 2.36 secs (1.0088 MB/s)
ftp> get ProjectOpenWRT.pdf
local: ProjectOpenWRT.pdf remote: ProjectOpenWRT.pdf
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ProjectOpenWRT.pdf (60857 bytes).
226 Transfer complete.
60857 bytes received in 0.22 secs (267.0237 kB/s)
ftp> get backup-OpenWrt-2023-07-26.tar
local: backup-OpenWrt-2023-07-26.tar remote: backup-OpenWrt-2023-07-26.tar
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup-OpenWrt-2023-07-26.tar (40960 bytes).
226 Transfer complete.
40960 bytes received in 0.17 secs (230.1973 kB/s)
ftp> get employees_wellness.pdf
local: employees_wellness.pdf remote: employees_wellness.pdf
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for employees_wellness.pdf (52946 bytes).
226 Transfer complete.
52946 bytes received in 0.23 secs (222.8946 kB/s)
ftp>
```

- Primero, analizamos los **metadatos** de los archivos *.pdf*: `exiftool (pdf)`, pero no encontramos nada interesante. Posteriormente, leemos estos mismos archivos: `open (pdf)`. Encontramos varios nombres de usuario que apuntamos en un archivo en nuestro sistema. Descomprimimos ahora el

archivo *.tar*: `tar -xvf backup-OpenWrt-2023-07-26.tar`. Este comprimido parece ser un backup del directorio /etc de Linux. Encontramos otros usuarios en el /etc/passwd que apuntamos en el archivo que creamos anteriormente.

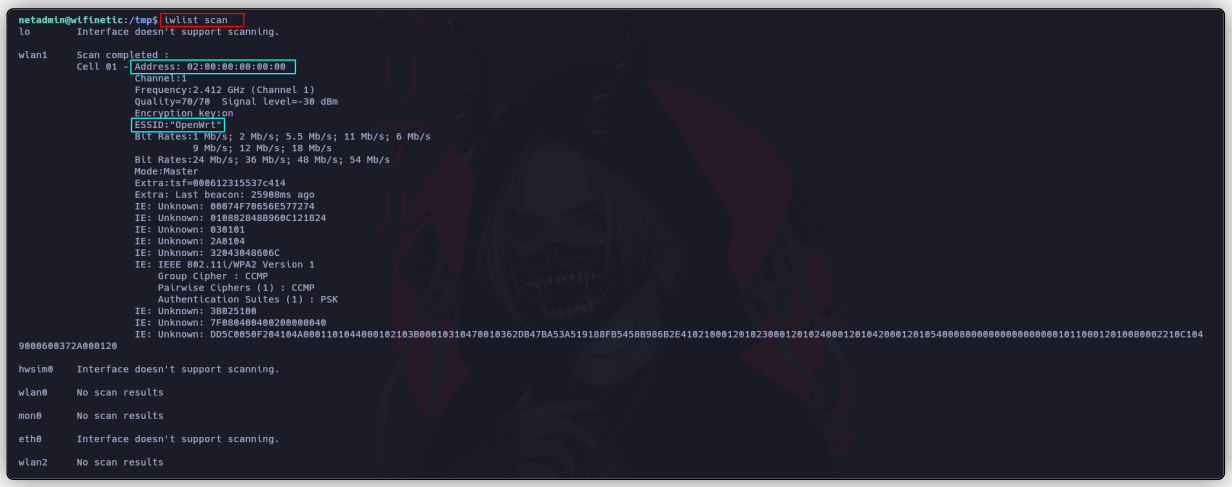
- 


## 1.3.1. Brute-forcing SSH user

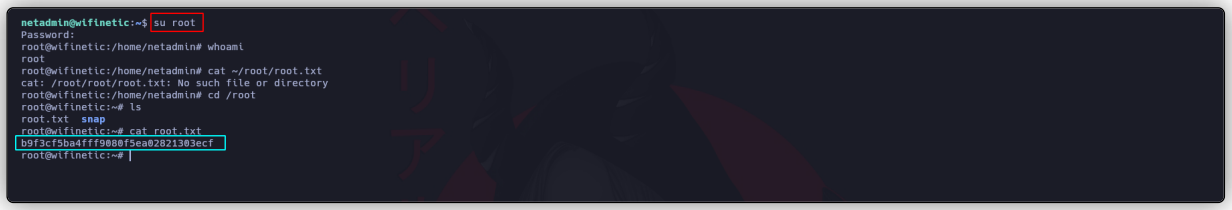
- Por otro lado, nos topamos también con lo que parece ser una contraseña. Como el único servicio que tenemos para acceder es SSH, realizamos un pequeño ataque de fuerza bruta para probar esta contraseña con los diferentes usuarios que encontramos. Para ello, usamos CrackMapExec con `poetry run crackmapexec ssh 10.10.11.247 -u /home/parrotp/pryor/CTF/HTB/Wifinetic/content/users.txt -p 'VeRyUniUqWiFIPasswrd1!'`. Descubrimos que esta contraseña pertenece al usuario *netadmin*. Conectamos por SSH a la máquina.
- 


## 1.4. Privesc via brute-forcing Wi-Fi PSK with Reaver

- Tras examinar los directorios, recurrimos a LinPEAS para detectar vías potenciales de elevar nuestros privilegios. Consideramos interesante que /usr/bin/reaver tenga CAP_NET_RAW+ep asignada. Reaver se usa para realiza ataques de fuerza bruta a redes Wi-Fi protegidas por WPA.
  - 


- Sabiendo esto, enumeraremos las redes inalámbricas del sistema con `iwlist scan`. De aquí, nos interesa especialmente el nombre de la red (ESSID) y su identificador (BSSID).
  - 


- Llegados a este punto, usamos Reaver: `reaver -i mon0 -b 02:00:00:00:00:00`. De este modo, tratamos de romper la seguridad de una red Wi-Fi realizando un ataque de fuerza bruta contra el PIN (de ocho dígitos) de WPS. Asimismo, especificamos en el comando al interfaz de de red *mon0*, la cual se usa comúnmente en modo monitorización para escanear y analizar redes Wi-Fi. Al cabo de unos segundos, obtenemos la contraseña. La guardamos en un archivo en nuestro directorio de trabajo.
  - 


- Migramos la sesión a root y probamos esta contraseña. Conseguimos acceso. Encontramos la última flag.
  - 


> - **Reaver** es una herramienta de código abierto diseñada para realizar ataques de **fuerza bruta** contra **redes Wi-Fi** protegidas por el estándar de

seguridad **WPA (Wi-Fi Protected Access)** o **WPA2**. Este programa se utiliza para intentar descifrar la **clave de seguridad precompartida (PSK)** de una red Wi-Fi utilizando un método conocido como ataque de fuerza bruta por PIN de **WPS (Wi-Fi Protected Setup)**. El objetivo de Reaver es aprovechar una vulnerabilidad en la configuración por defecto de muchos enrutadores Wi-Fi que admiten WPS. Esta vulnerabilidad permite que un atacante realice intentos repetidos para adivinar el PIN de ocho dígitos utilizado para autenticar dispositivos en la red. Reaver automatiza este proceso, intentando diferentes combinaciones de PIN hasta encontrar el correcto y así obtener acceso a la red Wi-Fi.

> - **ESSID**:
>   - El **ESSID (Extended Service Set Identifier)** es el nombre único que identifica una red inalámbrica **WLAN (Wireless Local Area Network)** dentro de un área de cobertura determinada. En otras palabras, es el nombre de la red Wi-Fi. El ESSID es utilizado por los dispositivos inalámbricos para identificar y conectarse a una red Wi-Fi específica. Cuando un dispositivo escanea las redes Wi-Fi disponibles, cada red detectada tiene un ESSID asociado que se muestra como el nombre de la red en la lista de redes disponibles. El ESSID puede ser configurado por el administrador de la red al configurar el enrutador inalámbrico o el punto de acceso. Por defecto, muchos dispositivos vienen con un ESSID predeterminado asignado por el fabricante, como "Linksys", "NETGEAR", "TP-LINK", etc. Sin embargo, es una práctica recomendada cambiar el ESSID predeterminado a un nombre único y fácil de recordar para identificar la red de manera más segura y conveniente.
> - **BSSID**:
>   - El **BSSID (Basic Service Set Identifier)** es una identificación única asignada a cada **punto de acceso (AP)** dentro de una red inalámbrica **WLAN (Wireless Local Area Network)**. Es un identificador de hardware que representa de manera única a un punto de acceso inalámbrico y se utiliza para distinguir entre diferentes puntos de acceso que pueden estar dentro del alcance de un dispositivo cliente. En una red Wi-Fi, el BSSID está vinculado a la **dirección MAC (Media Access Control)** del punto de acceso. La dirección MAC del BSSID es la dirección física de la interfaz de red inalámbrica del punto de acceso y se utiliza para identificar de manera única al punto de acceso en la red. El BSSID es especialmente útil en entornos donde hay múltiples puntos de acceso Wi-Fi cercanos, ya que permite a los dispositivos cliente distinguir y seleccionar el punto de acceso al que desean conectarse. Cuando un dispositivo cliente escanea las redes Wi-Fi disponibles, obtiene una lista de BSSIDs junto con los SSIDs correspondientes.

> Esto permite al dispositivo cliente identificar cada punto de acceso individualmente, lo que facilita la conexión a la red Wi-Fi deseada.