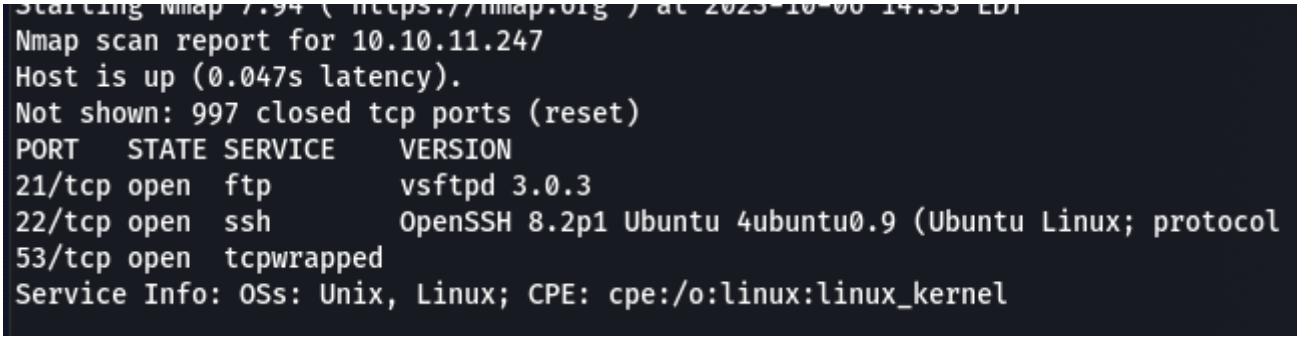
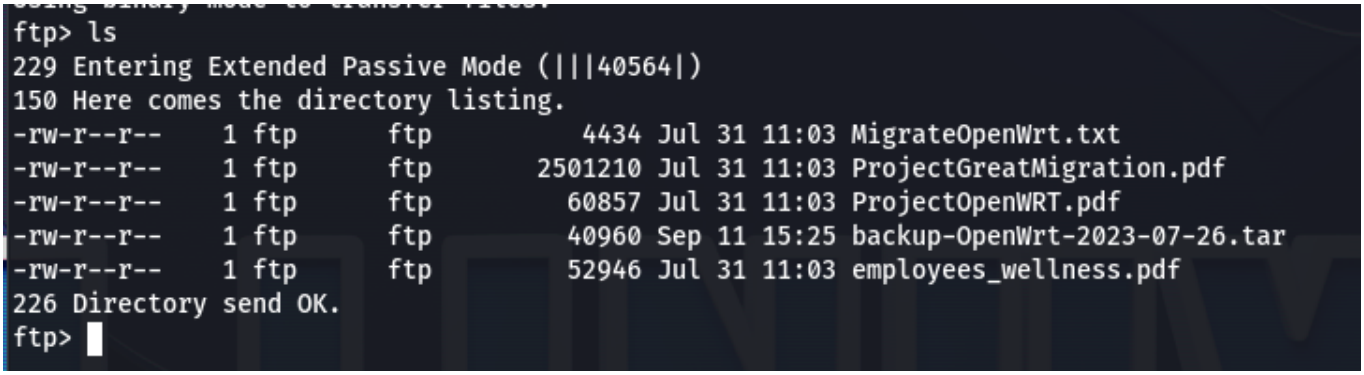
Recon

Running an nmap scan revealed 3 open ports:



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.

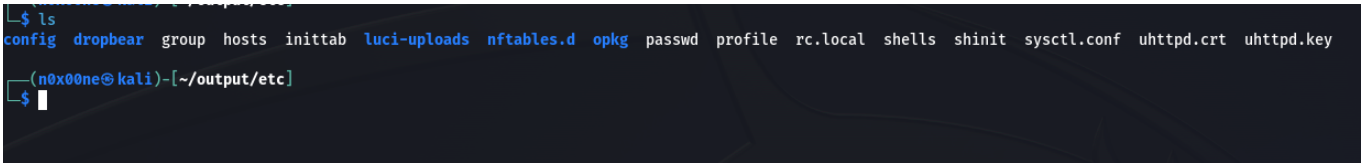


FTP

There were some pdf documetns and a .tar file which seemed to be OpenWrt, which is a linux distro for embedded systems, often used for cpe-routers.

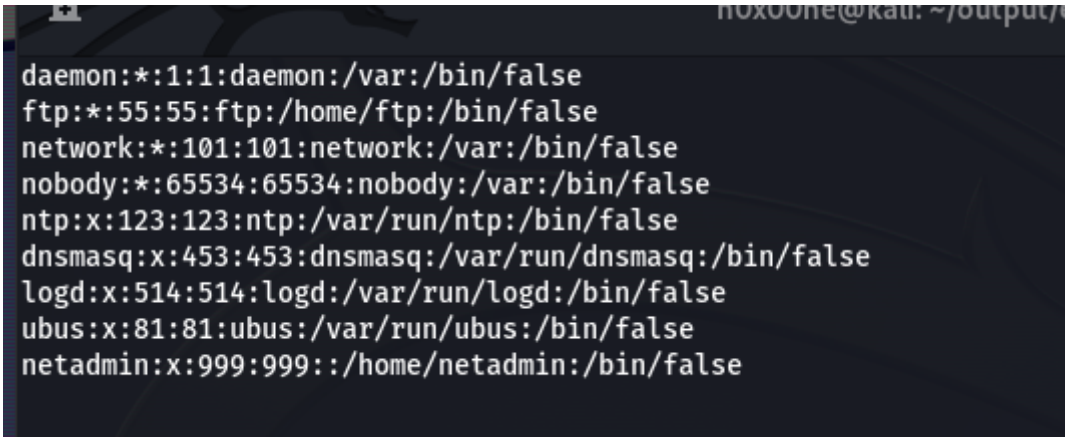
Most of the files were indicating that the company wanted to migrate from openwrt to debin, which was some nice lore, but at this point pretty useless. One thing these file showed was the domain **wifinetic.htb**.

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:

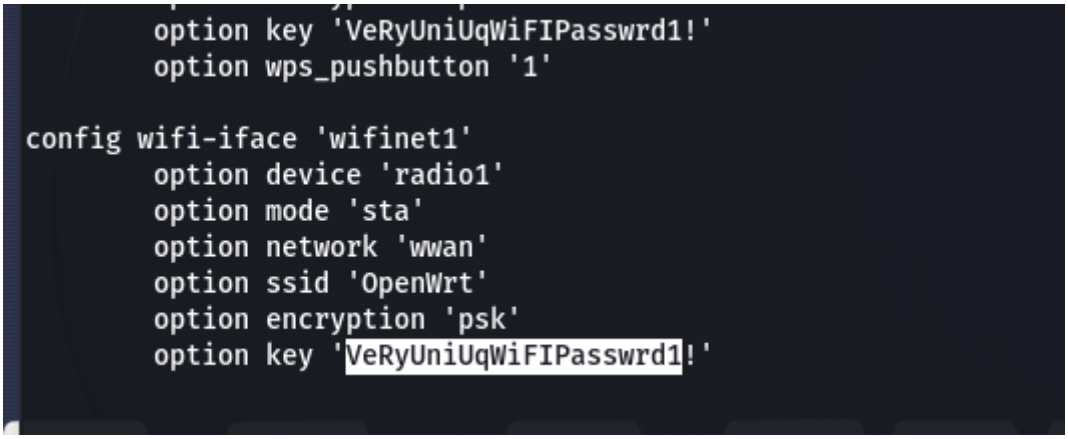


User flag

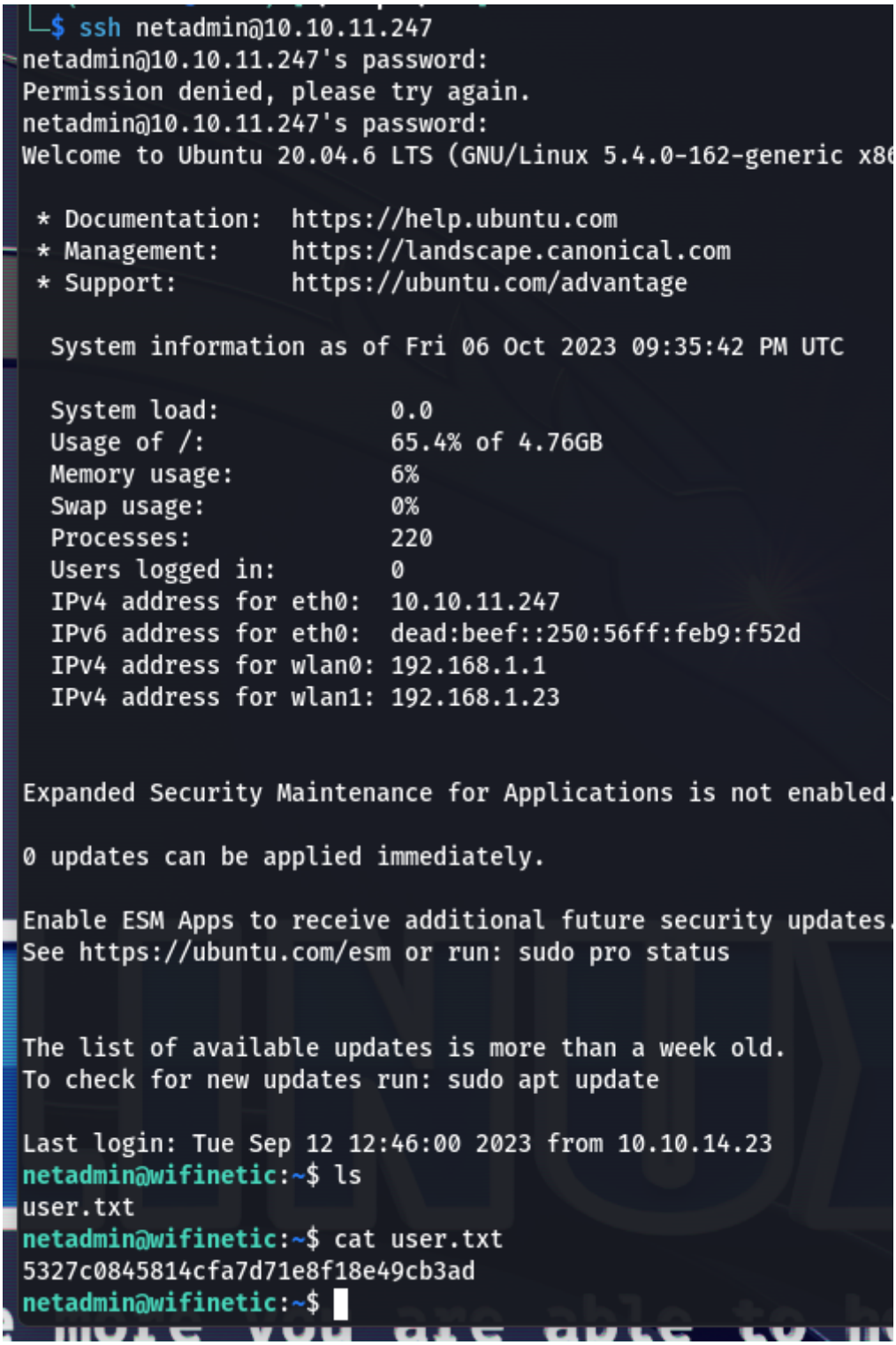
This allowed me to enumerate the users on the system:



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



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:

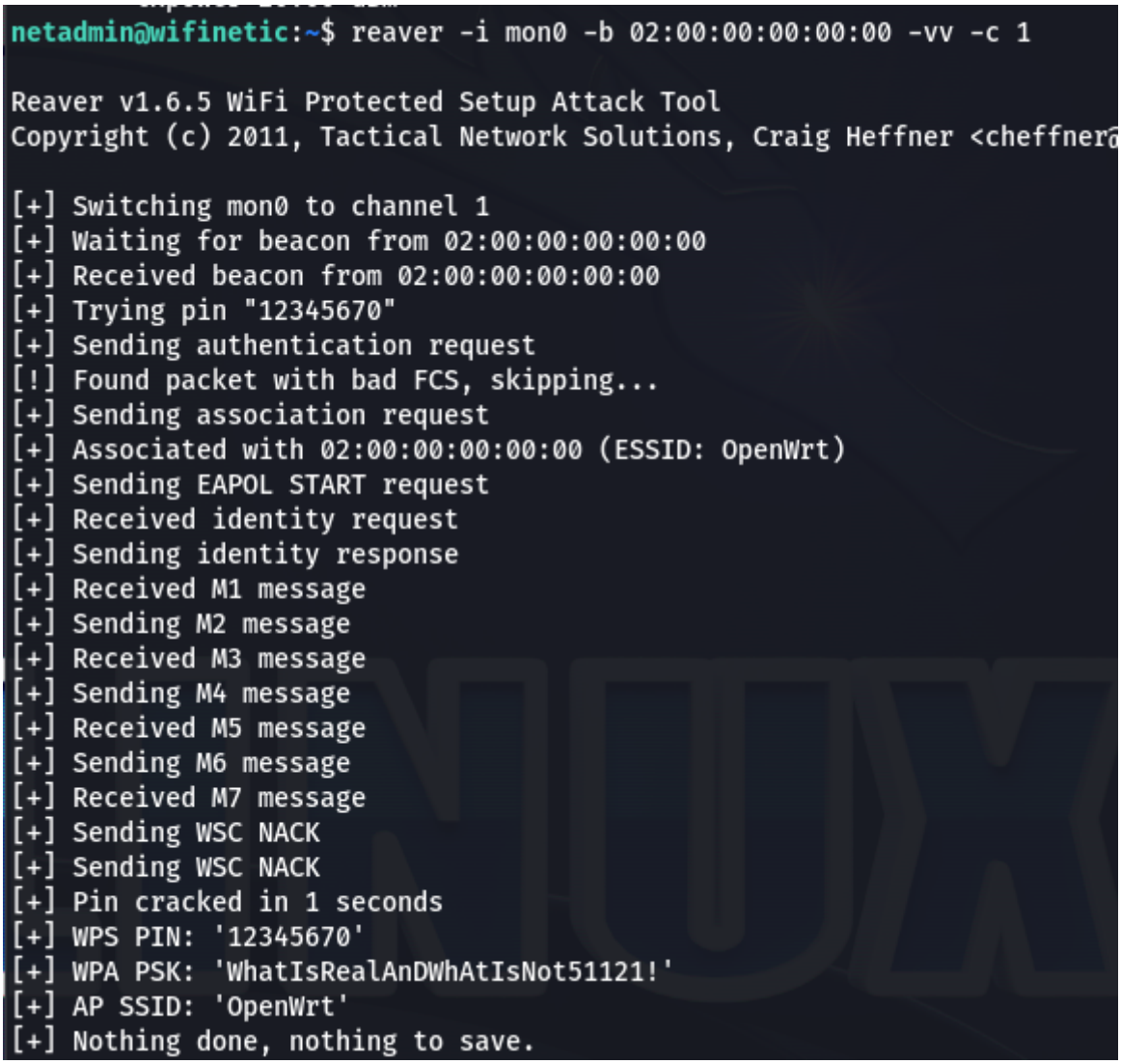


Root

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:

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



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:~#