CAPTURE THE FLAG

L' indirizzo IP del target e' 192.168.50.8, dove é attivo un servizio ssh versione OpenSSH 7.6p1 sulla porta 22/tcp. (Fig.1)

```
┌──(kali㉿kali)-[~/Downloads/SecLists/Passwords]
└─$ sudo nmap -sV 192.168.50.8 -p22 -O
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 11:22 EDT
Nmap scan report for 192.168.50.8
Host is up (0.0011s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
MAC Address: 08:00:27:48:FE:AC (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.07 seconds
```

Fig.1

Per trovare le credenziali di accesso al server, ho tentato un attacco di tipo Brute Force con Hydra, dapprima inserendo username e password da un lista fornita da Seclists, con risultato negativo. Successivamente ho provato inserendo come username “user”, “root”, sempre con una lista di password di SecLists, ma con insuccesso. Mentre Hydra procedeva con la scansione, ho provato a cercare degli exploit sul servizio sopracitato servendomi di Exploit Database. Ho trovato che c'è un Exploit con codice CVE -2019-6111/6110 , ma per una questione di tempo non sono riuscito a procedere. Ho tentato anche un attacco di brute force tramite metaxploit (Fig.2), che non ha portato risultati.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.50.8
RHOSTS ⇒ 192.168.50.8
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME niko
USERNAME ⇒ niko
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Fig.2

Sicuramente con più tempo a disposizione, avrei proceduto con la scansione di Hydra, che è andata a rilento data la scarsa potenza della mia macchina virtuale e avrei continuato con la ricerca di vulnerabilità per tentare di aprire una shell nel database.