Pokemon

Enumaration

Found a hint to look inside browser console

FOund nothing there but we have a sus tag with some info which looks like credentials and it works in ssh

got ssh

Nmap

PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 23:f5:fb:e7:57:c2:a5:3e:c2:26:29:0e:74:db:37:c2 (ECDSA)
|_ 256 f1:9b:b5:8a:b9:29:aa:b6:aa:a2:52:4a:6e:65:95:c5 (ED25519)
80/tcp open http   Apache/2.4.18 (Ubuntu)
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Can You Find Them All?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|phone
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT   ADDRESS
1   ... 10
11 470.13 ms 10.10.237.147

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.82 seconds

http:80

FOund a hint in source page

```
  <pokemon>:<hack_the_pokemon>
      <!--(Check console for extra surprise!)-->
</div>
```

the pokemon and hack_the_pokemon is ssh credentials

```
┌──(root💀CyberJunkie)-[~/Tryhackme/Pokemon_THM]
└─# ssh pokemon@$ip
The authenticity of host '10.10.237.147 (10.10.237.147)' can't be established.
ECDSA key fingerprint is SHA256:mXXTCQORSu35gV+cSi+nCjY/W0oabQFNjxuXUDrsUHI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.237.147' (ECDSA) to the list of known hosts.
pokemon@10.10.237.147's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

84 packages can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

pokemon@root:~$
```

#

Exploitation

PostExploitation

NOw we are in machine as pokemon user

We get flag for green pokemon [GreenPokemon]

NOw e get a cpp file which conatins credentials for user ash and we ssh into ash

```
pokemon@root:~/Videos/Gotta/Catch/Them/ALL!$ cat Could_this_be_what_Im_looking_for\?.cplusplus
# include <iostream>

int main() {
        std::cout << "ash : pikapika"
        return 0;
}pokemon@root:~/Videos/Gotta/Catch/Them/ALL!$ su ash
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bash: /home/ash/.bashrc: Permission denied
ash@root:/home/pokemon/Videos/Gotta/Catch/Them/ALL!$
```

we can run all commands as root with as no passwd so i su into root

```
ash@root:/home/pokemon/Videos/Gotta/Catch/Them/ALL!$ id
uid=1001(ash) gid=1001(ash) groups=1001(ash),27(sudo)
ash@root:/home/pokemon/Videos/Gotta/Catch/Them/ALL!$ sudo -l
[sudo] password for ash:
Matching Defaults entries for ash on root:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User ash may run the following commands on root:
    (ALL : ALL) ALL
ash@root:/home/pokemon/Videos/Gotta/Catch/Them/ALL!$ sudo su
root@root:/home/pokemon/Videos/Gotta/Catch/Them/ALL!#
```

#

GreenPokemon

Found the first flag in hex form in /pokemon/Desktop/POkemon.zip

```
pokemon@root:~$ cd Desktop/
pokemon@root:~/Desktop$ ls -al
total 12
drwxr-xr-x  2 pokemon pokemon 4096 Jun 24  2020 .
drwxr-xr-x 19 pokemon pokemon 4096 Jun 14 22:37 ..
-rw-rw-r--  1 pokemon pokemon  383 Jun 22  2020 P0kEmOn.zip
pokemon@root:~/Desktop$ unzip P0kEmOn.zip
Archive:  P0kEmOn.zip
   creating: P0kEmOn/
  inflating: P0kEmOn/grass-type.txt
pokemon@root:~/Desktop$ ls -al
total 16
drwxr-xr-x  3 pokemon pokemon 4096 Jun 14 22:51 .
drwxr-xr-x 19 pokemon pokemon 4096 Jun 14 22:37 ..
drwxrwxr-x  2 pokemon pokemon 4096 Jun 22  2020 P0kEmOn
-rw-rw-r--  1 pokemon pokemon  383 Jun 22  2020 P0kEmOn.zip
pokemon@root:~/Desktop$ cd P0kEmOn/
pokemon@root:~/Desktop/P0kEmOn$ ls -al
total 12
drwxrwxr-x 2 pokemon pokemon 4096 Jun 22  2020 .
drwxr-xr-x 3 pokemon pokemon 4096 Jun 14 22:51 ..
-rw-rw-r-- 1 pokemon pokemon   53 Jun 22  2020 grass-type.txt
pokemon@root:~/Desktop/P0kEmOn$ cat  grass-type.txt
50 6f 4b 65 4d 6f 4e 7b 42 75 6c 62 61 73 61 75 72 7dpokemon@root:~/Desktop/P0kEmOn$
```

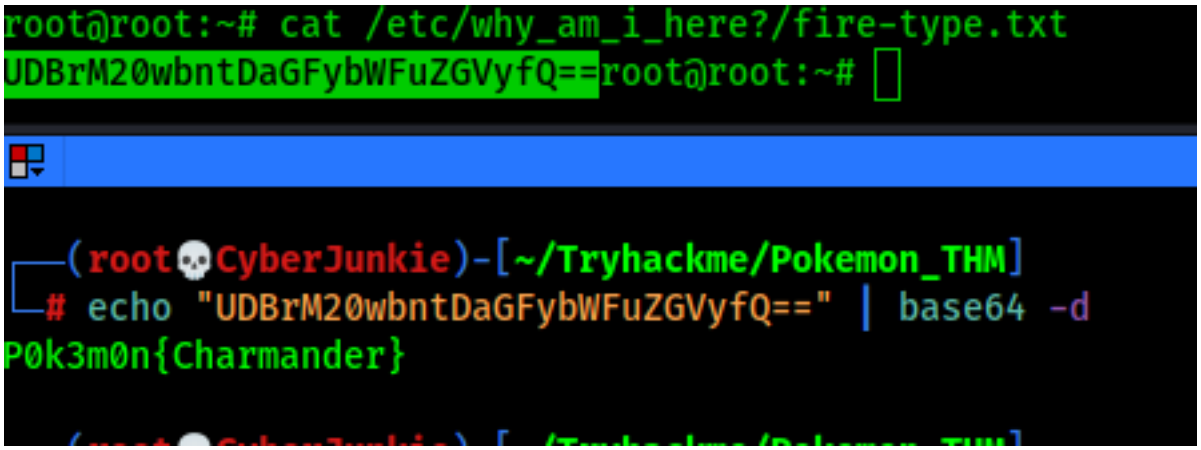
50 6f 4b 65 4d 6f 4e 7b 42 75 6c 62 61 73 61 75 72 7d : PoKeMoN{Bulbasaur}

FirePokemon

Searched for firetype and luckily got a txt file in /etc

```
root@root:~# find / -iname "fire-type*" 2>/dev/null
/etc/why_am_i_here?/fire-type.txt
```

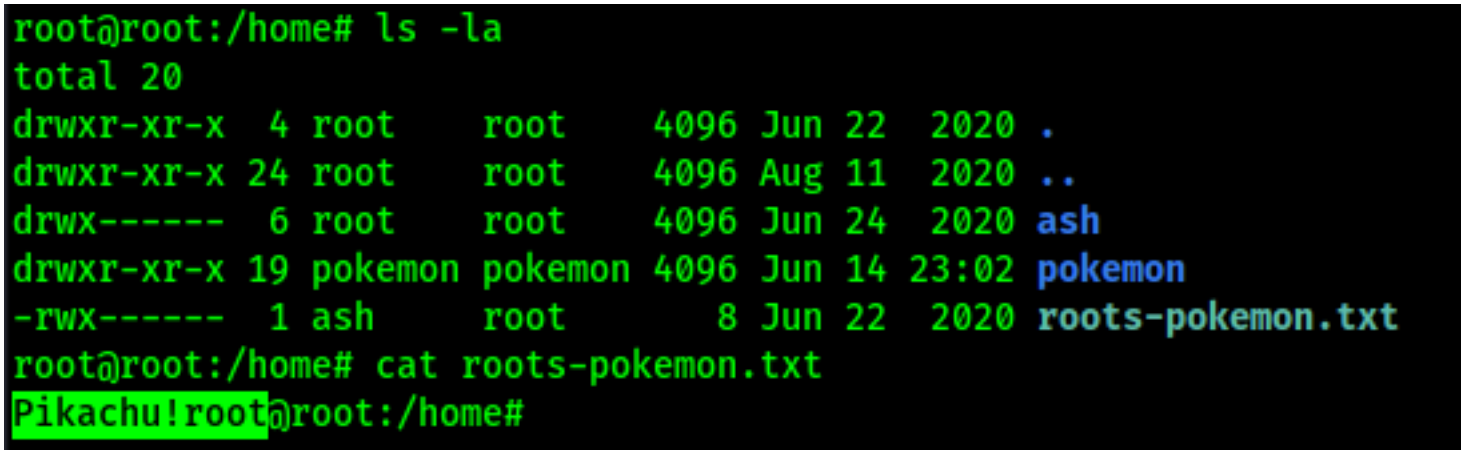
GOt a base64 code and decoded to get the fire flag
P0k3m0n{Charmander}



RootPokemon

FOund Root pokemon file in home directory

Root favourite pokemon is obviusly pikachuuu

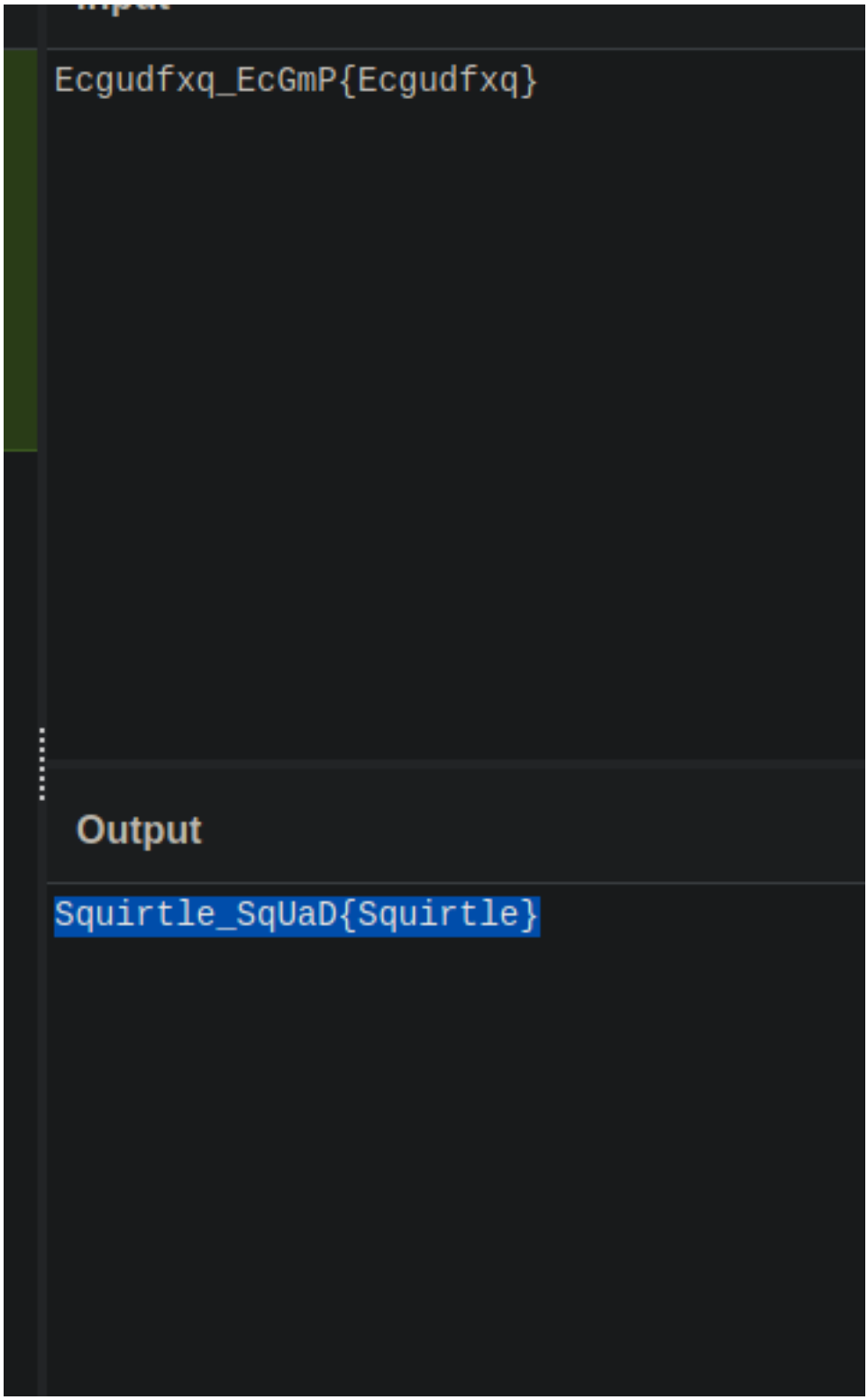


WaterPokemon

found water pokemon file in web root directory

text we got looks rot 13 but it didnt worked

i read a writeup and it said that rot 14 is being used so iget the flag



Loot

Credentials

SSH

pokemon : hack_the_pokemon

ash : pikapika

Flags

Green Pokemon

PoKeMoN{Bulbasaur}

Water Pokemon

Ecgudfxq_EcGmP{Ecgudfxq} - scrambled(rot14)

Squirtle_SqUaD{Squirtle}

FIre Pokemon

P0k3m0n{Charmander}

Root Pokemon

Pikachu!