Got a catch'em all

Got a catchem All

Peguntas:

Find the Grass-Type Pokemon
50 6f 4b 65 4d 6f 4e 7b 42 75 6c 62 61 73 61 75 72 7d
Find the Water-Type Pokemon
Ecgudfxq_EcGmP{Ecgudfxq}
Find the Fire-Type Pokemon
UDBrM20wbntDaGFybWFuZGVyfQ==ash
Who is Root's Favorite Pokemon?

Congratulations! Thank You So Much For Completing The Pokemon Room!

Revisamos el
Puerto 80 , codigo fuente:

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

User:pokemon
pass: hack_the_pokemon

Me conecto por ssh

```
└─$ ssh pokemon@10.10.35.99
The authenticity of host '10.10.35.99 (10.10.35.99)' can't be established.
ED25519 key fingerprint is SHA256:pLr5hKfcRZWD4ZBMz/8vFWnJ2xslYHSX94C4KXwOLVg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.35.99' (ED25519) to the list of known hosts.
pokemon@10.10.35.99'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:~$
```

comienzo a sondear carpetas...

```
pokemon@root:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  Videos
```

```
pokemon@root:~$ cd Videos/
pokemon@root:~/Videos$ ls
Gotta
pokemon@root:~/Videos$ cd Gotta/
pokemon@root:~/Videos/Gotta$ ls
Catch
pokemon@root:~/Videos/Gotta$ cd Catch/
pokemon@root:~/Videos/Gotta/Catch$ ls
Them
pokemon@root:~/Videos/Gotta/Catch$ cd Them/
pokemon@root:~/Videos/Gotta/Catch/Them$ cd  All
-bash: cd: All: No such file or directory
pokemon@root:~/Videos/Gotta/Catch/Them$ ls
ALL!
pokemon@root:~/Videos/Gotta/Catch/Them$ cd ALL!
pokemon@root:~/Videos/Gotta/Catch/Them/ALL!$ ls
Could_this_be_what_Im_looking_for?.cplusplus
pokemon@root:~/Videos/Gotta/Catch/Them/ALL!$ file Could_this_be_what_Im_looking_for\?.cplusplus
Could_this_be_what_Im_looking_for?.cplusplus: C source, ASCII text
pokemon@root:~/Videos/Gotta/Catch/Them/ALL!$
```

encontramos un archivo llamado Could_this_be_what_Im_looking_for\?.cplusplus
veremos su contenido

```
cat Could_this_be_what_Im_looking_for\?.cplusplus

# include <iostream>

int main() {
	std::cout << "ash : pikapika"
	return 0;
```

User:Pass ash : pikapika
fue lo primero que se me vino a la mente por lo cual revisare si el usuario ash esta en los ficheros de passwd

```
pokemon@root:~/Videos/Gotta/Catch/Them/ALL!$ cat /etc/passwd | grep ash
root:x:0:0:root:/root:/bin/bash
pokemon:x:1000:1000:root,,,:/home/pokemon:/bin/bash
ash:x:1001:1001::/home/ash:
pokemon@root:~/Videos/Gotta/Catch/Them/ALL!$
```

si estaba

Sondeamos otros lugares y nos topamos con la siguiente ruta

```
pokemon@root:/$ cd home/
pokemon@root:/home$ ls
ash  pokemon  roots-pokemon.txt
pokemon@root:/home$ ls -l
total 12
drwx------  6 root    root    4096 Jun 24  2020 ash
drwxr-xr-x 19 pokemon pokemon 4096 Jan 15 13:20 pokemon
-rwx------  1 ash     root       8 Jun 22  2020 roots-pokemon.txt
```

ash tiene acceso a roots-pokemon.txt , probemos el user y la pass que conseguimos.

```
pokemon@root:/home$ 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$

User:Pass ash : pikapika
Abrimos el archivo mencionado
nano roots_pokemon.txt

Pikachu!

uhmmm... no se para que servira pero lo mantendremos guardo en caso de ser necesario...

ash@root:/home$ ls
ash pokemon roots-pokemon.txt
ash@root:/home$ cd pokemon/
ash@root:/home/pokemon$ ls -l
total 44
drwxr-xr-x 2 pokemon pokemon 4096 Jun 24 2020 Desktop
drwxr-xr-x 2 pokemon pokemon 4096 Jun 22 2020 Documents
drwxr-xr-x 2 pokemon pokemon 4096 Jun 22 2020 Downloads
-rw-r--r-- 1 pokemon pokemon 8980 Jun 22 2020 examples.desktop
drwxr-xr-x 2 pokemon pokemon 4096 Jun 22 2020 Music
drwxr-xr-x 2 pokemon pokemon 4096 Jun 22 2020 Pictures
drwxr-xr-x 2 pokemon pokemon 4096 Jun 22 2020 Public
drwxr-xr-x 2 pokemon pokemon 4096 Jun 22 2020 Templates
drwxr-xr-x 3 pokemon pokemon 4096 Jun 22 2020 Videos
ash@root:/home/pokemon$
ash@root:/home/pokemon$ cd Desktop/
ash@root:/home/pokemon/Desktop$ ls
P0kEmOn.zip
Encontramos un archivo que se ve interesante, levantare un simple server en python para traerlo al equipo con kali

ash@root:/home/pokemon/Desktop$ python3 -m http.server 8000

Serving HTTP on 0.0.0.0 port 8000 ...
Levantamos el servidor en el puerto 8000

10.2.92.229 - - [15/Jan/2024 13:49:55] "GET / HTTP/1.1" 200 -
10.2.92.229 - - [15/Jan/2024 13:49:56] code 404, message File not found
accedimos a la IP Victima en el nbavegador por el puerto 8000 y descargamos finalmente el zip.
10.2.92.229 - - [15/Jan/2024 13:49:56] "GET /favicon.ico HTTP/1.1" 404 -
10.2.92.229 - - [15/Jan/2024 13:49:58] "GET /P0kEmOn.zip HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
ash@root:/home/pokemon/Desktop$
abrimos el P0kemon.zip
el zip contenia un fichero de texto codificado en hexa
50 6f 4b 65 4d 6f 4e 7b 42 75 6c 62 61 73 61 75 72 7d

Lo desciframos con ciberchef, el resultado :

Primera flag : PoKeMoN{Bulbasaur}

luego de buscar sin direccion por un tiempo, se me ocurrio buscar ficheros con agua y fuego debido que el Planta ya lo tenemos, entonces parto con agua,
Buscamos :
ash@root:/$ find / -name *water* -type f 2>/dev/null
/var/www/html/water-type.txt
ahi hay una ruta con un Fichero , abrimos el archivo y nos encontramos con esto
Ecgudfxq_EcGmP{Ecgudfxq}

Parece alguna Codificacion de cifrado rotativo , ocupamos ciberchef llegando a las siguientes conclusiones
ROt13 - Lenguaje Ingles
Descifrado
Squirtle_SqUaD{Squirtle}

Hora de buscar el de fuego!! , debido a que si busco como era hace un rato , solo fire seria un error debido a saltarian coincidencias como firefox y sus archivos , como el anterior tambien decia -type aplicaremos la busqueda como fire-type,

ash@root:/$ find / -name *fire-type* -type f 2>/dev/null
/etc/why_am_i_here?/fire-type.txt
Abrimos el archivo y nos topamos con lo siguiente:
ash@root:/$ cat /etc/why_am_i_here?/fire-type.txt
UDBrM20wbntDaGFybWFuZGVyfQ==
Evidentemente es un cifrado de base64 por su estructura, decodifiquemos ,
ash@root:/$ echo "UDBrM20wbntDaGFybWFuZGVyfQ==" | base64 -d
P0k3m0n{Charmander}

ahora , no encontre mas pistas... wait... teniamos la ultima flag de las primeras!
 vamos a abrir roots_pokemon.txt para ver el contenido de el
el contenido era Pikachu!
que es la Flag y con eso terminamos la maquina
C:

Escaneos

sudo nmap -p- -sS -sC -sV --open --min-rate 5000 -n -vvv 10.10.35.99 -oN escaneo

[sudo] contraseña para kali:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-15 13:19 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 13:19
Completed NSE at 13:19, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 13:19
Completed NSE at 13:19, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 13:19
Completed NSE at 13:19, 0.00s elapsed
Initiating Ping Scan at 13:19
Scanning 10.10.35.99 [4 ports]
Completed Ping Scan at 13:19, 0.39s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:19
Scanning 10.10.35.99 [65535 ports]
Discovered open port 80/tcp on 10.10.35.99
Discovered open port 22/tcp on 10.10.35.99
Completed SYN Stealth Scan at 13:19, 21.73s elapsed (65535 total ports)
Initiating Service scan at 13:19
Scanning 2 services on 10.10.35.99
Completed Service scan at 13:19, 6.70s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.35.99.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 13:19
Completed NSE at 13:20, 14.45s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 13:20
Completed NSE at 13:20, 1.27s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 13:20
Completed NSE at 13:20, 0.01s elapsed
Nmap scan report for 10.10.35.99
Host is up, received echo-reply ttl 61 (0.53s latency).
Scanned at 2024-01-15 13:19:28 EST for 44s
Not shown: 52620 closed tcp ports (reset), 12913 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON   VERSION
22/tcp open ssh   syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 58:14:75:69:1e:a9:59:5f:b2:3a:69:1c:6c:78:5c:27 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC5csEY9HQAEkHk16FMvfJVYh4YzdcIRCQpv2IOon6FHy3la/
DkwscWsUIp7hXmMeW35Oa7OfI08LvyokxDX8bKgKUpU/dP05LNyDzv17MKB6rt3SkPbDv3XVMlu101/
wkIMIOdJ38TW0+vVlU89cjQ5XiSDep4kKm/+6fEl2zM5x60DKexOOYTQ3t8SRkBV4TnWmr9wDQCDH/
Kc8Pl2W9GM7hgAhVB9uUhN/EBCUbwZ8xE0ToOQz+QIkCTEuwD/AhDoURmRzv7EGut0TBrUPvFCK19v2Crw/
BVQc07taDkei4N0/MwpXvI4CnJ6jpGOgxTMePk/nZusz/XbnUtnIqD
| 256 23:f5:fb:e7:57:c2:a5:3e:c2:26:29:0e:74:db:37:c2 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP9bcehMnrIADUJHvNw7/
zastIegVYRSXcF40Pky1Yllzx872e/LUM6UdTNaC4gffBnEpKcmwE9wjR+J6lfR8Yk=
| 256 f1:9b:b5:8a:b9:29:aa:b6:aa:a2:52:4a:6e:65:95:c5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICabmX4EeiR66bXPzMHbCZpkcUu+GSkDJP1nZ2+30Vm+
80/tcp open http   syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)

| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Can You Find Them All?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 13:20
Completed NSE at 13:20, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 13:20
Completed NSE at 13:20, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 13:20
Completed NSE at 13:20, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.13 seconds
        Raw packets sent: 104404 (4.594MB) | Rcvd: 54664 (2.187MB)

┌──(kali㉿kali)-[~/Desktop/pokemon]
└─$ whatweb 10.10.35.99
http://10.10.35.99 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.35.99], Script[text/javascript], Title[Can You Find Them All?]

Walk