Gotta Catch'em All!

34

Gotta Catch'em All!

This room is based on the original Pokemon series. Can you obtain all the Pokemon in this room?

auto-recon-scan

auto-recon.sh available at https://github.com/aingram702/auto-recon-script

```
------------------------------------------------------------------------------------------------------------------------
----- NMAP -----
PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
|   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 httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Can You Find Them All?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel


--------------- DIRS ---------------
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/index.html (Status: 200)
/server-status (Status: 403)


--------------- WEB ---------------
WhatWeb report for ␛[1m␛[34mhttp://10.10.204.56␛[0m
Status    : 200 OK
Title     : Can You Find Them All?
IP        : 10.10.204.56
Country   : RESERVED, ZZ

Summary   : Script text/javascript HTML5 HTTPServer Ubuntu Linux Apache/2.4.18 (Ubuntu) Apache 2.4.18

Detected Plugins:
Apache
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.4.18 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ mHTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS          : Ubuntu Linux
        String       : Apache/2.4.18 (Ubuntu) (from server string)

[ Script]
        This plugin detects instances of script HTML elements and
        returns the script language/type.

        String       :text/javascript

HTTP Headers:
        HTTP/1.1 200 OK
        Date: Wed, 12 Aug 2020 12:34:41 GMT
        Server: Apache/2.4.18 (Ubuntu)
        Last-Modified: Wed, 24 Jun 2020 18:36:27 GMT
        ETag: "2bd1-5a8d8c0fe5140-gzip"
        Accept-Ranges: bytes
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Content-Length: 3174
        Connection: close
        Content-Type: text/html
```

writeup

--ran my new custom enumeration script auto-recon.sh https://github.com/aingram702/auto-recon-script
--found open ports on 22 and 80, no interesting directories, and an Ubuntu OS running Apache 2.4.18
--closely examined web page source code and found a few intersting things:
--a comment <!--(Check console for extra surprise!)→ and possible credentials <pokemon>:<hack_the_pokemon>
--console output gives a list of pokemon characters:
Bulbasaur
Charmander
Squirtle
Snorlax
Zapdos
Mew
Charizard
Grimer
Metapod
Magikarp

--logged in to SSH with ssh pokemon@<IP> and password hack_the_pokemon
--looked around on box and found file /home/pokemon/Desktop/P0kEmOn.zip and ran unzip and got P0kEmOn/grass-type.txt
--ran cat P0kEmOn/grass-type.txt and hex string 50 6f 4b 65 4d 6f 4e 7b 42 75 6c 62 61 73 61 75 72 7d
--decoded with Cyberchef and got flag:
PoKeMoN{Bulbasaur}

--searched for other interesting files and found /var/www/html/water-type.txt
--ran cat /var/www/html/water-type.txt and found a string Ecgudfxq_EcGmP{Ecgudfxq}

--tried decoding with ROT13 without success, then changed rotation to ROT14 and got flag:
Squirtle_SqUaD{Squirtle}

--continued to search and found file /home/pokemon/Videos/Gotta/Catch/Them/ALL!/-Could_this_be_what_Im_looking_for?.cplusplus
--ran cd /home/pokemon/Videos/Gotta/Catch/Them/ALL! && cat Could_this_be_what_Im_looking_for?.cplusplus and it gave me:

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

--tried to run sudo -l unsuccessfully, so I tried to login with the possible credentials from the file Could_this_be_what_Im_looking_for?.cplusplus
--ran ssh ash@<IP> with password pikapika and got access
--ran sudo -l and got:

```
User ash may run the following commands on root:
    (ALL : ALL) ALL
```

--I then ran sudo bash to get a root shell
--I remembered seeing a file called /home/roots-pokemon.txt so I ran cat /home/roots-pokemon.txt and got root flag:
Pikachu!

--I continued searching for the Fire-Type Pokemon flag for a long time and I finally Googled for a better way to find it
--I found the command find / -name '*fire*' -type f 2>/dev/null | grep -ivE "(firefox|firewall)" which gave me:

```
/etc/why_am_i_here?/fire-type.txt
```

--ran cat /etc/why_am_i_here?/fire-type.txt and got a string UDBrM20wbntDaGFybWFuZGVyfQ==
--decoded with Cyberchef base64 and got flag:
P0k3m0n{Charmander}

[Task 1] Can You Catch'em All?

Remember to connect to the VPN network using OpenVPN, It may take some time for the machine to properly deploy.
You can also deploy your own Kali Linux machine, and control it in your browser using the provided Kali machine (Subscription Required).

Enjoy the room!

#1
Find the Grass-Type Pokemon

PoKeMoN{Bulbasaur}

#2
Find the Water-Type Pokemon

Squirtle_SqUaD{Squirtle}

#3
Find the Fire-Type Pokemon

P0k3m0n{Charmander}

#4
Who is Root's Favorite Pokemon?

Pikachu!

#5
Congratulations! Thank You So Much For Completing The Pokemon Room!

No answer needed