BioHazard

Enumaration

Port 21,22,80 open

on web we followed series of trails to find different directories

THis is estimated sitemap

/diningRoom/
/teaRoom/
/artRoom/
/barRoom/
/diningRoom2F/
/tigerStatusRoom/
/galleryRoom/
/studyRoom/
/armorRoom/
/attic/

after solving the puzzles i found these 4 crests and decoding the crests gave these 4 answers.

crest1 RlRQIHVzZXI6IG
crest2 h1bnRlciwgRlRQIHBh
crest3 c3M6IHlvdV9jYW50X2h
crest4 pZGVfZm9yZXZlcg==

I combined them as per instructions and found ftp credentials

we get pictures and a gpg encrypted file containing helmetflag

#enumarating three keys from three pictures and combining them then decdoing the base64 we get plant42_can_be_destroy_with_vjolt

#This is the password for gpg file

helmet_key{458493193501d2b94bbab2e727f8db4b}

we get ssh password and username after submitting helmet key

#

Nmap

limit 5000'.
Open 10.10.112.80:22
Open 10.10.112.80:21
Open 10.10.112.80:80
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

[~] Starting Nmap 7.91 (https://nmap.org) at 2021-06-26 08:19 EDT
Initiating Ping Scan at 08:19
Scanning 10.10.112.80 [4 ports]

```
Completed Ping Scan at 08:19, 0.49s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:19
Completed Parallel DNS resolution of 1 host. at 08:19, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 08:19
Scanning 10.10.112.80 [3 ports]
Discovered open port 22/tcp on 10.10.112.80
Discovered open port 80/tcp on 10.10.112.80
Discovered open port 21/tcp on 10.10.112.80
Completed SYN Stealth Scan at 08:19, 0.50s elapsed (3 total ports)
Nmap scan report for 10.10.112.80
Host is up, received echo-reply ttl 61 (0.46s latency).
Scanned at 2021-06-26 08:19:06 EDT for 1s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 61
22/tcp open  ssh     syn-ack ttl 61
80/tcp open  http    syn-ack ttl 61

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds
           Raw packets sent: 7 (284B) | Rcvd: 4 (160B)
```

Exploitation

Post Exploitation

After ssh we found that weasker is traitor and got a key for some cipher which is most probably we found in closet room link

The key is albert and we decode the cipher with viginere cipher and key

we get weasker credentials

weasker login password, stars_members_are_my_guinea_pig

we can run all commands as root

we get root

Loot

Credentials

possible user

rebecca

FTP Credentials

FTP user: hunter, FTP pass: you_cant_hide_forever

SSH credentials

umbrella_guest : T_virus_rules

weasker s: stars_members_are_my_guinea_pig

Flags

Root Flag

3c5794a00dc56c35f2bf096571edf3bf