Biohazard

Enumaration

Port Scan

nmap -p- -vv -Pn 10.10.99.76

Discovered open port 21/tcp on 10.10.99.76

Discovered open port 22/tcp on 10.10.99.76

Discovered open port 80/tcp on 10.10.99.76

Ran default script on 21 but was not able to utilize anonymous login

VERSION INFORMATION

PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
Service Info: OS: Unix

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 c9:03:aa:aa:ea:a9:f1:f4:09:79:c0:47:41:16:f1:9b (RSA)
| 256 2e:1d:83:11:65:03:b4:78:e9:6d:94:d1:3b:db:f4:d6 (ECDSA)
|_ 256 91:3d:e4:4f:ab:aa:e2:9e:44:af:d3:57:86:70:bc:39 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Beginning of the end

GOBUSTER INFORMATION

gobuster dir -u http://10.10.99.76 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Task 1

open ports

3

Team name

STARS alpha team

We click on mansion and start to work our way to the next room
We are asked where is the room

Task 2

Inspect element and we can see that it is in the /diningRoom/
After going to the dining room inspect element showed us this

SG93IGFib3V0IHRoZSAvdGVhUm9vbS8

I do not know what it is for yet

Update 1: tried stego but found nothing with that passphrase

Update 2: Tried a base64 decode

and it came back with this

echo SG93IGFib3V0IHRoZSAvdGVhUm9vbS8 | base64 -d

How about the /teaRoom/

I said yes to go through the tunnel and I ended up here

emblem{fec832623ea498e20bf4fe1821d58727}

I believe there is an emblem flag, and yes there is so lets put that in first
Look like you can put something on the emblem slot, refresh /diningRoom/
I do not understand what it is trying to tell me with refresh diningRoom

Alright we moved on to the **/teaRoom/**

We can see that we can either go to the **/artRoom/** or use a **Lockpick**

I start off with Lockpick and get a flag

lock_pick{037b35e2ff90916a9abf99129c8e1837}

Alright time to move into the artRoom

In here we can see that there is something on the wall

This is a map, it shows us all of the different areas we can go to

Lets Underline the ones we already went through
Look like a map

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

There first place I went was /barRoom/

I then entered the lockpick flag we already found

Now i see that we need to play the piano, however we do not have a piano or music flag

We see that moonlight somata is written on a note, that should be some musical flags

NV2XG2LDL5ZWQZLFOR5TGNRSMQ3TEZDFMFTDMNLGGVRGIYZWGNSGCZLDMU3GCMLGGY3TMZL5

That is not a flag tht we wanted...

After putting the above into google we quickly found out it was base32

Here we go echo NV2XG2LDL5ZWQZLFOR5TGNRSMQ3TEZDFMFTDMNLGGVRGIYZWGNSGCZLDMU3GCMLGGY3TMZL5 | base32 -d

and the output... **music_sheet{362d72deaf65f5bdc63daece6a1f676e}**

Alright we have the next flag

We are now in a secret bar room

we find another flag

gold_emblem{58a8c41a9d08b8a4e38d02a4d7ff4843}

We are not done yet though, it says to put the emblem flag in, for that I used the regular emblem flag

I was able to a name rebecca which I believe to be a username

Alright, time to look back through all the rooms and figure out what the hell rebecca is, starting from the beginning

I went back to the diningRoom and put the gold key in this time, and i got this back

klfvg ks r wimgnd biz mpuiui ulg fiemok tqod. Xii jvmc tbkg ks tempgf tyi_hvgct_jljinf_kvc

Lets put that into Google

We have ourselves a Vigenere cipher, which we have seen before

Since I have seen these before I know that you can try to crack them without a password / try to find the password

Or you can use a password, rebecca may not be a username after all and it may be a password

we crack the cipher to show the following

there is a shield key inside the dining room. The html page is called the_great_shield_key

http://10.10.99.76/diningRoom/the_great_shield_key.html

And we get another key

shield_key{48a7a9227cd7eb89f0a062590798cbac}

Off to the next room

We are now going to the diningroom2f

we find this

Lbh trg gur oyhr trz ol chfuvat gur fgnghf gb gur ybjre sybbe. Gur trz vf ba gur qvavatEbbz svefg sybbe. Ivfvg fnccuver.ugzy

alright, time to crack that one

Looks like we are dealing with ROT13

I have show before how to do ROT13 using the command line, lets see if we can do it again, and then do it the easier way which is using the web

cat rot.txt | tr '[a-z][A-Z]' '[n-za-m][N-ZA-M]'

Or just go online and you will be able to decode a ROT13

We get this

You get the blue gem by pushing the status to the lower floor. The gem is on the diningRoom first floor. Visit sapphire.html

Ok lets go there

http://10.10.99.76/diningRoom/sapphire.html

blue_jewel{e1d457e96cac640f863ec7bc475d48aa}

Next room is /tigerStatusRoom/

Looks like you can put a gem in the tigers eye, lets use the blue jewel

Alright we are in

crest 1:
S0pXRkVVS0pKQkxIVVdTWUpFM0VTUlk9

Hint 1: Crest 1 has been encoded twice

Hint 2: Crest 1 contanis 14 letters

Note: You need to collect all 4 crests, combine and decode to reavel another path
The combination should be crest 1 + crest 2 + crest 3 + crest 4. Also, the combination is a type of encoded base and you need to decode it

CREST 1

Base 64 then base 32

RlRQIHVzZXI6IG (I NEED TO FIND THE REST OF THEM THEN REINSERT THEM BACK UP HERE)

CREST 2

Alright we found crest 2 that was in galleryRoom/ aftet looking at the note, lets figure this one out

crest 2:

GVFWK5KHK5WTGTCILE4DKY3DNN4GQQRTM5AVCTKE
Hint 1: Crest 2 has been encoded twice
Hint 2: Crest 2 contanis 18 letters
Note: You need to collect all 4 crests, combine and decode to reavel another path
The combination should be crest 1 + crest 2 + crest 3 + crest 4. Also, the combination is a type of encoded base and you need to decode it

Now we need to do a base 32 to base 58

h1bnRlciwgRlRQIHBh

CREST 3

Into the armorRoom we go, we do not have the key for other room
Now click on note.txt and we see some crazy stuff now
crest 3:

MDAxMTAxMTAgMDAxMTAwMTEgMDAxMDAwMDAgMDAxMTAwMTEgMDAxMTAwMTEgMDAxMDAwMDAgMDAxMTAxMDAgMDExM
Hint 1: Crest 3 has been encoded three times
Hint 2: Crest 3 contanis 19 letters
Note: You need to collect all 4 crests, combine and decode to reavel another path
The combination should be crest 1 + crest 2 + crest 3 + crest 4. Also, the combination is a type of encoded base and you need to decode it

YOU ARE GOING TO WANT TO USE CYBERCHEF FOR THIS ONE!!!!

Lets break this down, first doing the above to a base 64 gives us a binary view
Ok, whats next...
From binary to hex
from hex we get the following

c3M6IHlvdV9jYW50X2h

CREST 4

Final crest, here we go
Lets go to the last room we can actually get in, which is the attic

crest 4:
gSUERauVpvKzRpyPpuYz66JDmRTbJubaoArM6CAQsnVwte6zF9J4GGYyun3k5qM9ma4s
Hint 1: Crest 2 has been encoded twice
Hint 2: Crest 2 contanis 17 characters
Note: You need to collect all 4 crests, combine and decode to reavel another path
The combination should be crest 1 + crest 2 + crest 3 + crest 4. Also, the combination is a type of encoded base and you need to decode it

For this one we are doing a to hex to base 58 and we get the following

pZGVfZm9yZXZlcg==

Now we have everything, lets see what is says

RlRQIHVzZXI6IGh1bnRlciwgRlRQIHBhc3M6IHlvdV9jYW50X2hpZGVfZm9yZXZlcg==

Looks like we have a base64, decoding it we get the following

FTP user: hunter, FTP pass: you_cant_hide_forever

DONE WITH TASK 2, MAN THAT WAS A LONG ONE

Task 3

Lets FTP into 10.10.99,76 using the credentials we obtained
We see quite a few files in there, get all of the them

the first one I looked at was important.txt which showed the following

Jill,

I think the helmet key is inside the text file, but I have no clue on decrypting stuff. Also, I come across a /

hidden_closet/ door but it was locked.

From,
Barry

The next thing I tried was to use gpg2john, but that didnt work the way I planned it to, so I decided to move on the .jpg files
jpg 001 showed me there was a file embedded in it called key-001.txt
kali@kali:~/Desktop$ steghide info 001-key.jpg
"001-key.jpg":
format: jpeg
capacity: 376.0 Byte
Try to get information about embedded data ? (y/n) y
Enter passphrase:
embedded file "key-001.txt":
size: 15.0 Byte
encrypted: rijndael-128, cbc
compressed: yes
Did it without a password and we can get the txt file
kali@kali:~/Desktop$ steghide extract -sf 001-key.jpg
Enter passphrase:
wrote extracted data to "key-001.txt".
kali@kali:~/Desktop$ cat key-001.txt
cGxhbnQ0Ml9jYW
For the second one we need a passphrase
Decided to say screw steg and lets do strings
we find out second part
5fYmVfZGVzdHJveV9
Now onto the third one
We need a key to get all the info, which we do not have yet
I do a strings for 003 and see that there are key.txt files
we can use binwalk to try and extract those files out without a password, lets make sure binwalk can see them first
kali@kali:~/Desktop$ binwalk 003-key.jpg

DECIMAL HEXADECIMAL DESCRIPTION
---
0 0x0 JPEG image data, JFIF standard 1.01
1930 0x78A Zip archive data, at least v2.0 to extract, uncompressed size: 14, name: key-003.txt
2124 0x84C End of Zip archive, footer length: 22

Alright he can, now lets extract them

binwalk -e 003-key.jpg

kali@kali:~/Desktop$ cat _003-key.jpg.extracted/key-003.txt
3aXRoX3Zqb2x0

Time to combine all of these guys now
cGxhbnQ0Ml9jYW5fYmVfZGVzdHJveV93aXRoX3Zqb2x0
We have a base64 string
plant42_can_be_destroy_with_vjolt
Now we have the password for helmetkey.txt
gpg helmet..... and put in the password
after that cat helmetkey.txt
helmet_key{458493193501d2b94bbab2e727f8db4b}
We are not done yet because we still need to look at that hidden closet we found out about earlier
we got to the hidden clost and click on mo1
wpbwbxr wpkzg pltwnhro, txrks_xfqsxrd_bvv_fy_rvmexa_ajk
looks like vigenere cipher again, however this time without a key
lets try to auto decrypt it
31855 albert weasker login password stars members are my guinea pig
No idea what the hell that means, but it looks like the key is albert
Alright, we put albert in the key field and we get the following, look like above was a URI
weasker login password, stars_members_are_my_guinea_pig
weasker may also be a name, we shall see. this may be for ssh!!!
Examine the wolf medal we get ssh password

SSH password: T_virus_rules

Alright not getting far with the stars members thing, lets keep moving

Ok, for a while I was confused, but then I remember we didn't go to all the rooms!!! We still need to go to the study room!!!

We go back to that room and download doom (I like doom more anyways)

gunzip doom....

tar -xvf doom....

cat eagle....

and we find our user

SSH user: umbrella_guest

SSH password: T_virus_rules

we log in and we cannot run sudo as umbrella_guest, that sucks

Task 4 and 5

ls -la
cd .jailcell
cd ..
cd ..
ls -la
cd weasker
more stuff in here
We also see what the ultimate lifeform is...

Now it wants us to find the login password for the traitor, we already found that

stars_members_are_my_guinea_pig

su weasker

stars_members_are_my_guinea_pig

User weasker may run the following commands on umbrella_corp:
(ALL : ALL) ALL

This means that we can run all privleges as sudo root

sudo -u root cat /root/root.txt

AND WE ARE DONE!!!!