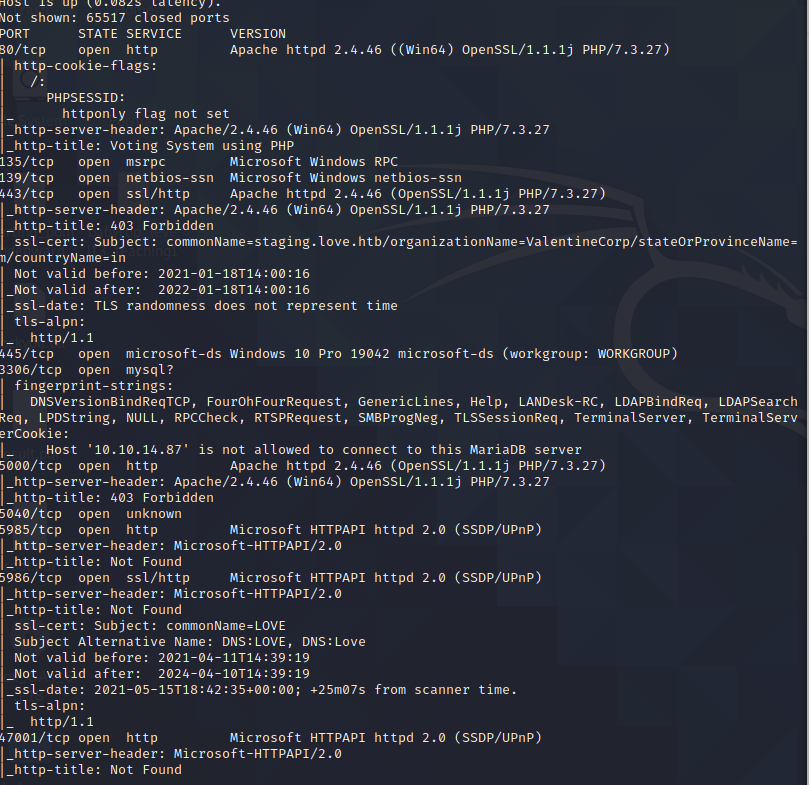
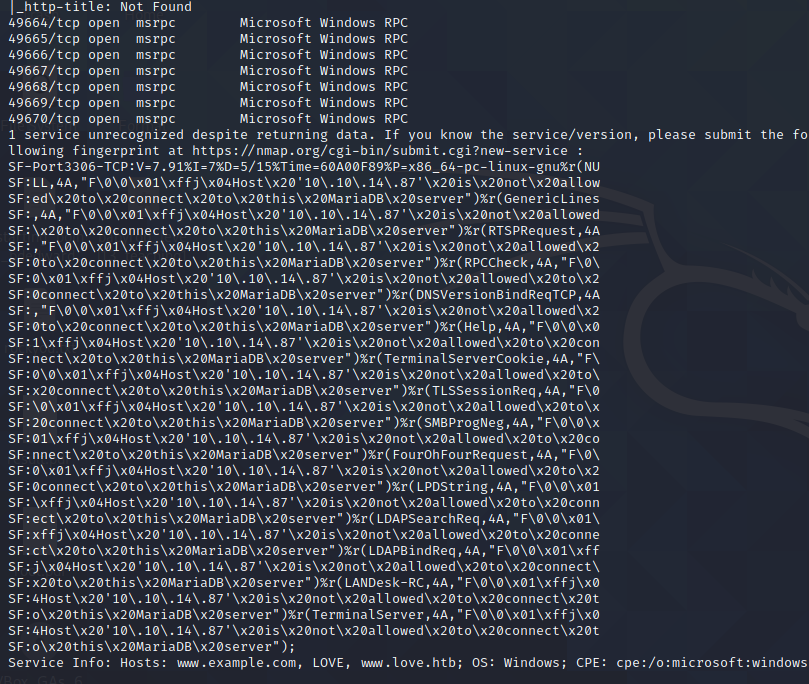
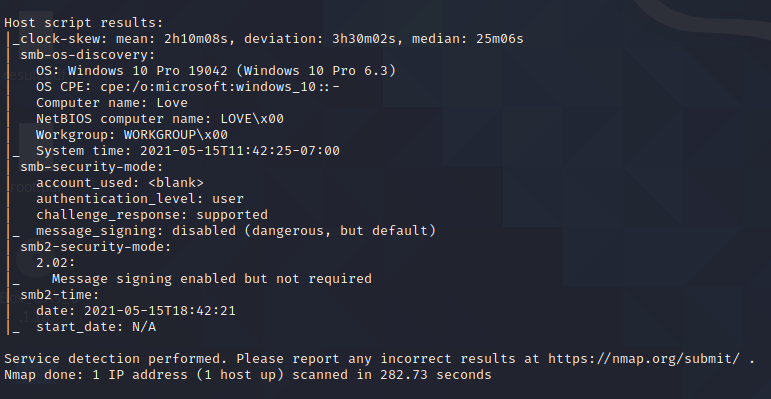
HTB - Love

10.10.10.239 Windows machine

Nmap

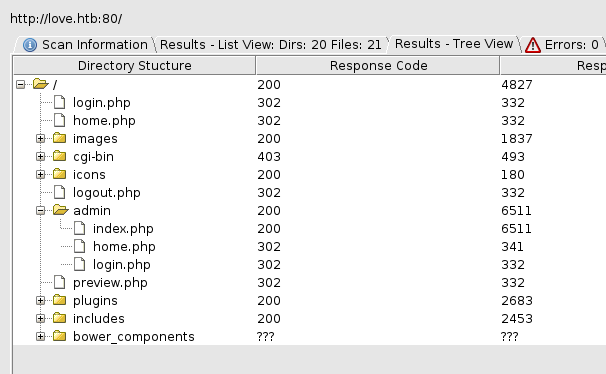




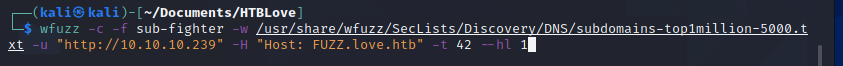


Nikto

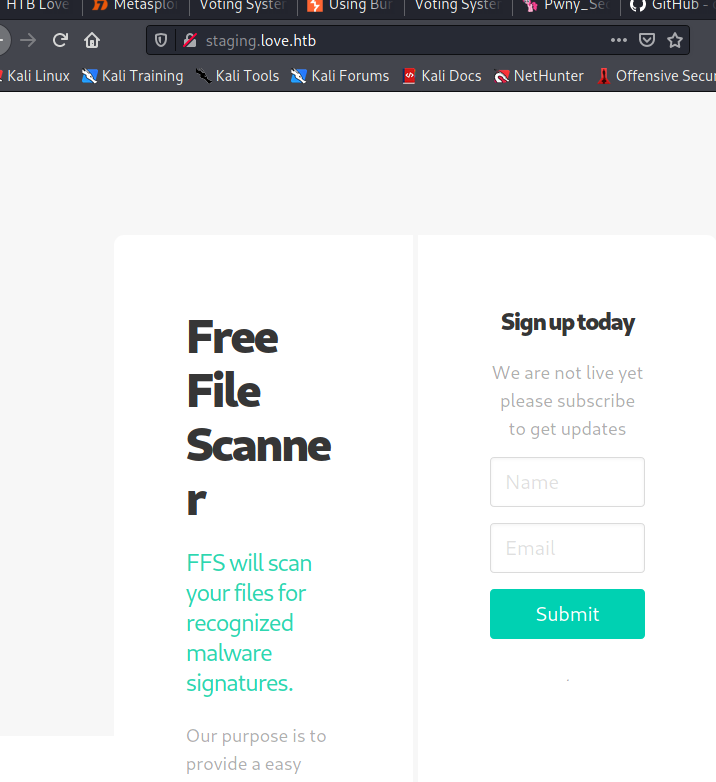
Dirbuster



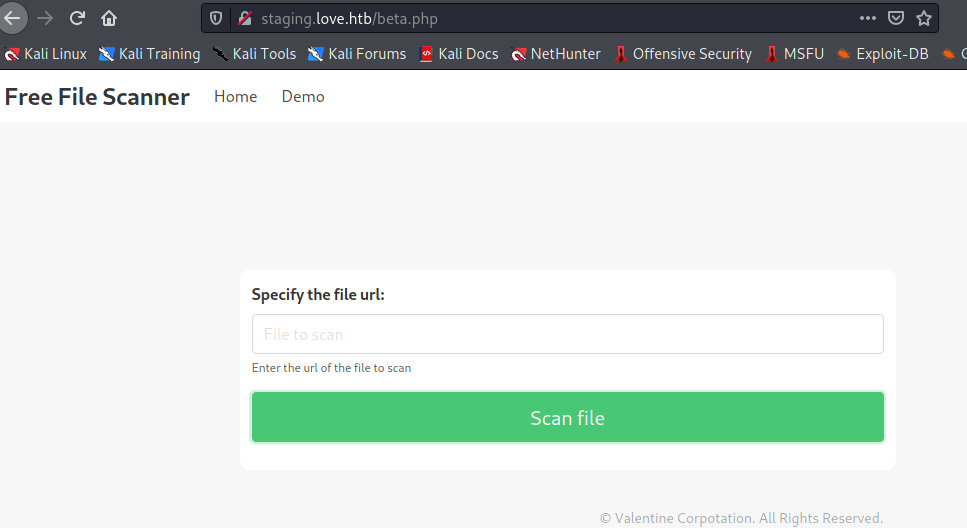
Wfuzz



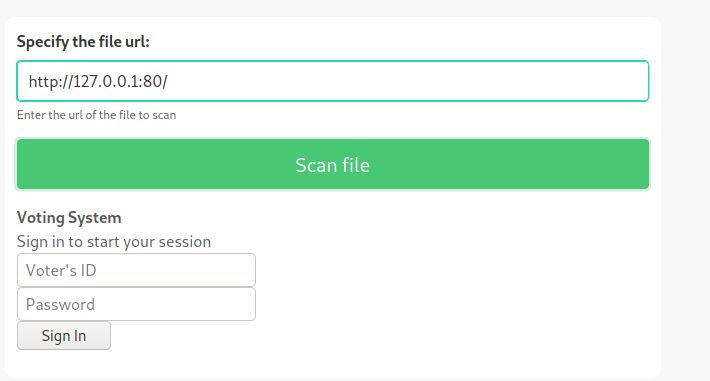
Using the above wfuzz command let me scan love.htb for any other possible subdomains. The word “staging” came back with a longer response length than others, so I tried staging.love.htb and we have a new host:



Clicking on Demo we seemingly are able to scan any file using a URL:

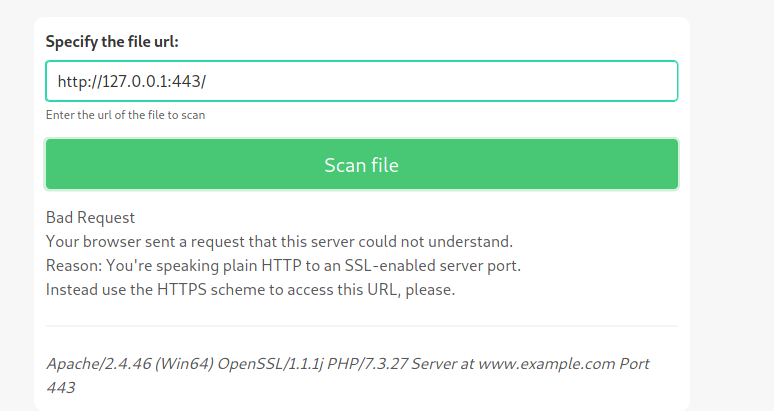


It seems we can scan local files on the host with this scanner. Using the ports from nmap I started scanning around to see what might be on the host:

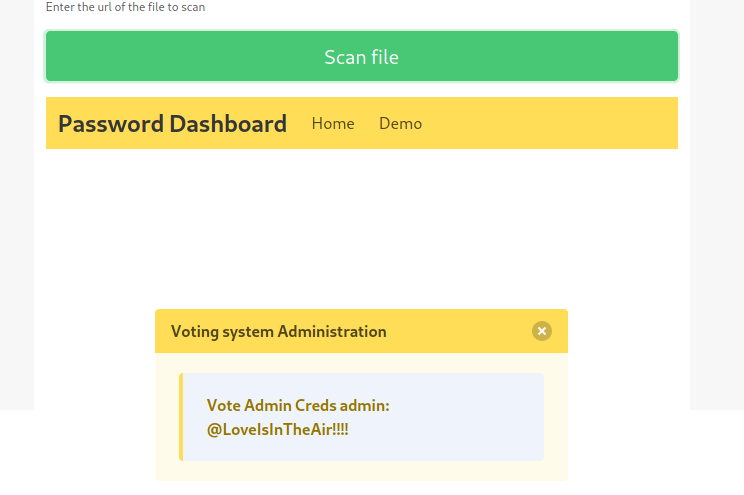


Scanning port 80 just gives us the standard login page we encountered at love.htb

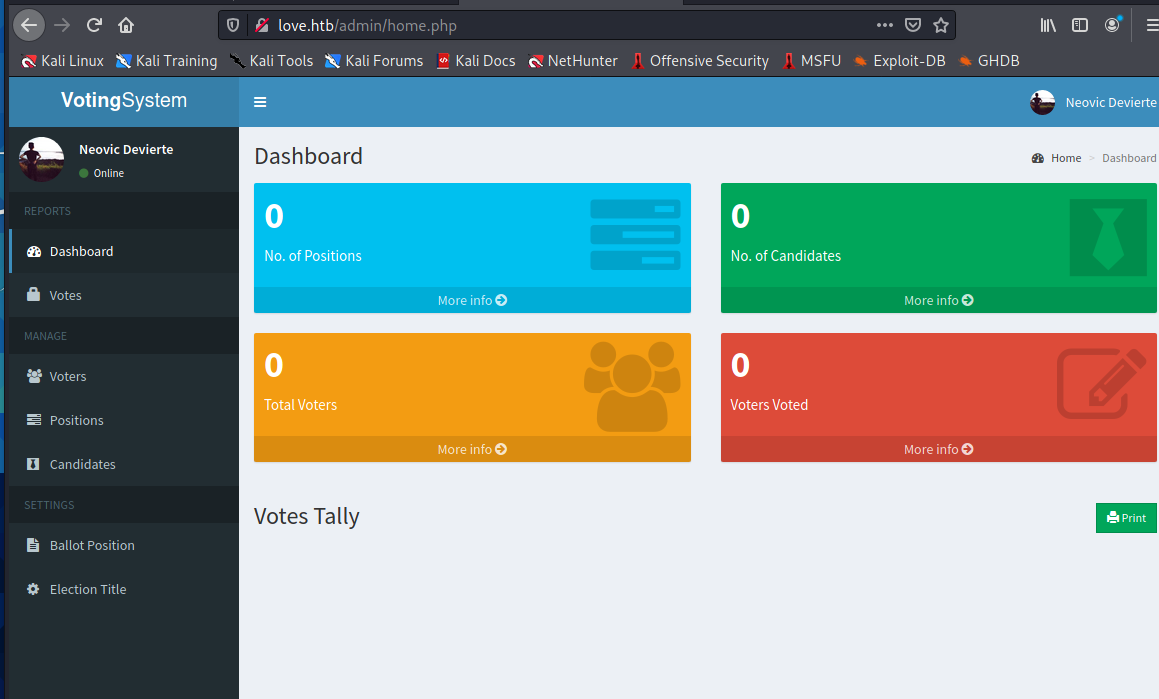
Scanning other ports



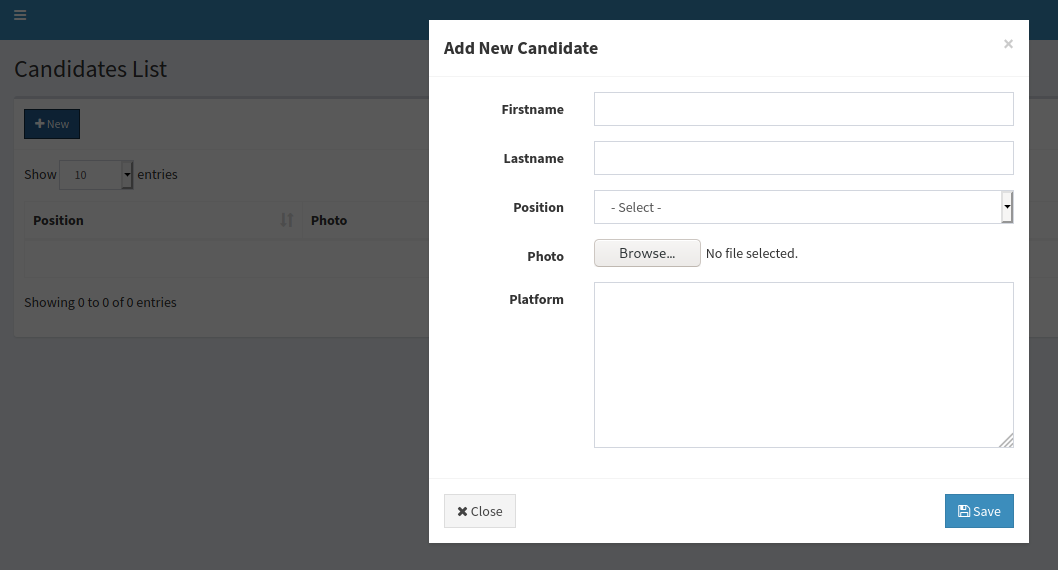
Finally, port 5000 gave us a Password Dashboard with admin creds:



We should now be able to login as admin on love.htb/admin/index.php:



As admin under Candidates it appears we can upload a file, potentially allowing us to trigger a reverse shell attack if we can trigger the php file when uploaded:

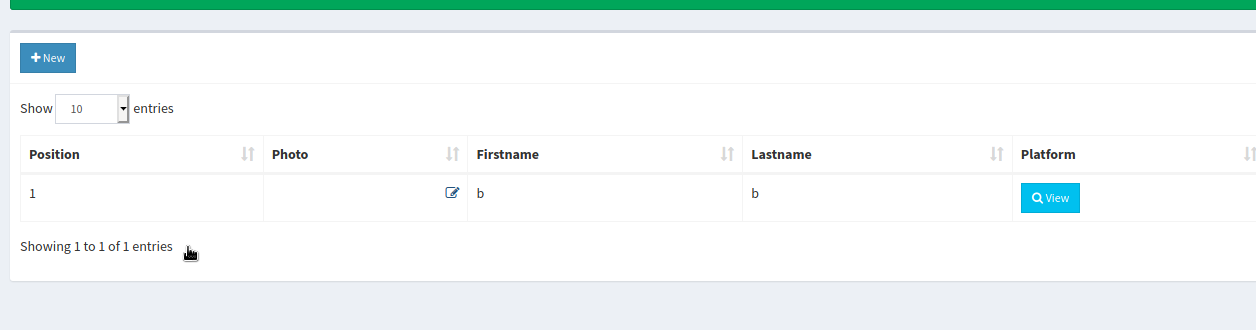


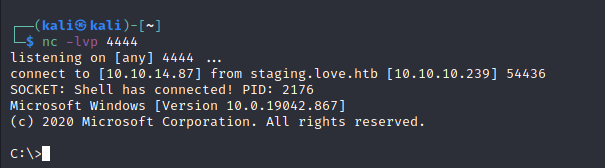
There are many different reverse shells out there, I will try one to see if we can trigger the php file.

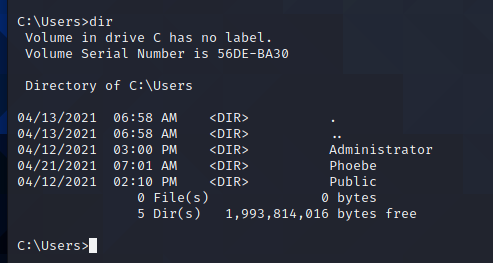
I uploaded the php\_reverse\_shell.php with ip address as the HTB VPN and on port 4444. I then opened a nc -lvp 4444 listener.

I first had to create a position in order to upload the file.

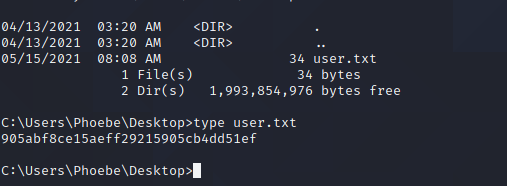
Once I uploaded and click the photo the reverse shell was triggered:



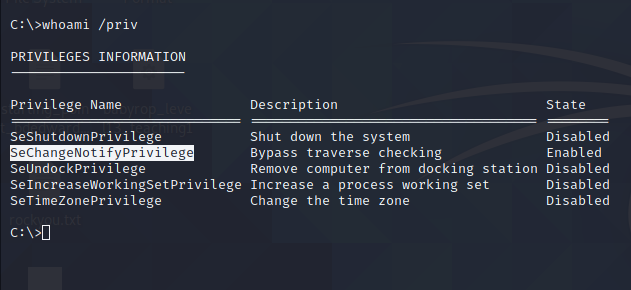




The user flag was stored on “Phoebe” Desktop:



Running whoami /priv



Searching This privilege I found a good resource about Windows Privilege Escalation here:

[Windows - Hack$Notes (ed4m4s.blog)](https://ed4m4s.blog/privilege-escalation/windows)

Which led to this privilege escalation:

[Always Install Elevated - Hack$Notes (ed4m4s.blog)](https://ed4m4s.blog/privilege-escalation/windows/always-install-elevated)

This led to creating another shell which we upload to the host and execute to gain another reverse shell with elevated privileges.

