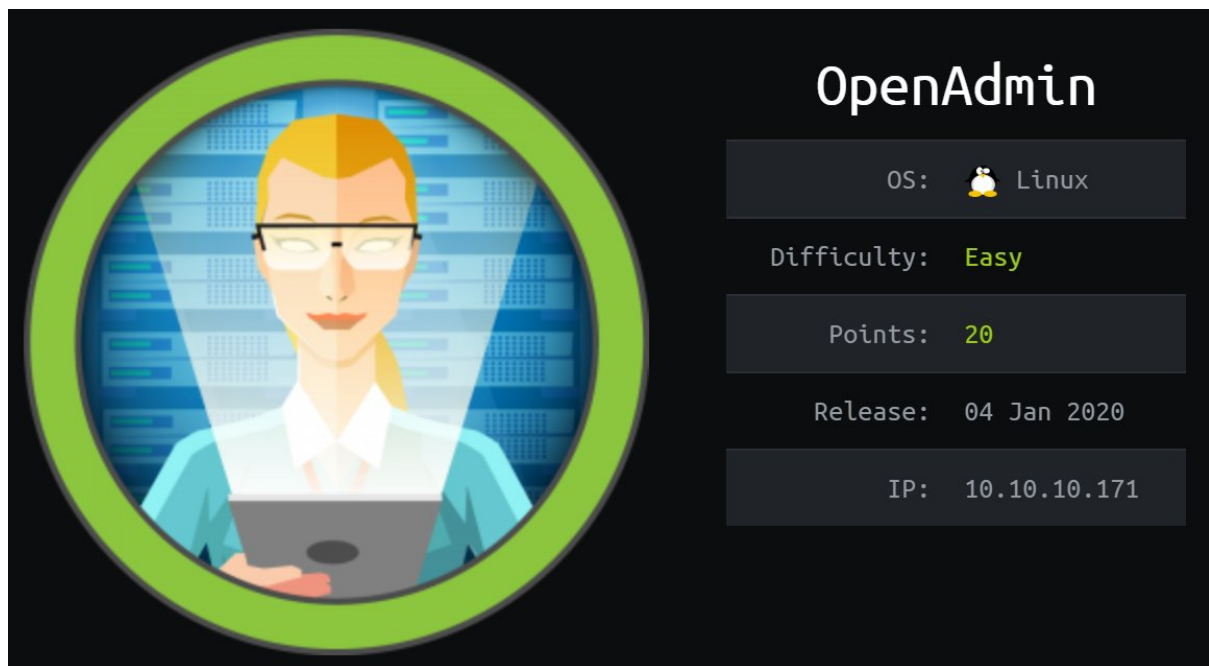# OpenAdmin Cookbook

Learning Outcomes

At the end of this challenge, you learned how to setup hack-the-box VPN connection, perform port and vulnerabilities scanning, exploit and escalate privileges in a Linux Server.   You are required to get user.txt and root.txt in order to gain points in hack-the-box, https://www.hackthebox.eu/ Once user.txt flag was submitted, you will be award 10 points and 20 points for root.txt flag.

Materials needed

- Preparation: Openvpn , HTB Connection pack
- Enumeration: Nmap , Nikto , Dirbuster/Gobuster
- Gain Access: Dos2Unix
- Password cracker : John the Riper, Wordlists , SSH Keygen
- Escalate Privileges : GTFOBins
- Web browser: Linux command manual, ExploitDB

Preparation

- Setup connection to the server (Hint: vpn)
- Check your connection if Tun0 is displayed
- Ping the machine
- Install the tools in the materials needed list (Hint: don't forget to 'sudo')
- Checklist: successful ping? Installed the tools?

Enumeration

- scan list of open ports, running OS & version via nmap
- use Nikto to search for vulnerabilities (hint: focus on the open port no. relate to web app)
- use Dirbuster/ Gobuster to search for present directory (Hint: type the full url that you want to scan & use medium wordlist)
- Based on the directory found in Dirbuster/Gobuster, access to the server Access Page
- Search for vulnerabilities within the version of the running database in ExploitDB
- Understand the exploit and download it

Gain Access

- Convert the exploit file using Dos2Unix
- Run the exploit and try and type id (hint: the result)
- can you get the password?? (Hint: do some digging)
- maybe you can/need to make the machine more stable to capture the data you want by downloading another exploit
- but how to download a php-reverse-shell to the OpenAdmin machine? (Hint: host a simple web server)
- Once the machine is more stable, continue digging for user id &password (Hint: /opt)
- Still yet to find user id? How about dig at another place? (Hint" Var logs)
- Checklist time: do you have the user id ? and password?? (Hint: pwd: related to Naruto)
- time to connect through SSH and access the user account that you found

Local Enumeration

- Check out what and who is this user (services running, kernel & version, open ports, what can he do / file he can access?)
- Why not listen to some gossips about tulip in the meantime? (Hint: networking)
- try to read some data of the files maybe you can find some clue (Hint: ask the cat for help)
- Had the cat had capture some useful information like key or other user? (Hint: try port forwarding + SSH)
- Checklist time: found the keys of other user and username?

Password Cracking

- Time to crack some key shape like "eggs" using ssh keygen
- decode the generated ssh keygen using John the riper (Hint: use the ssh file that require the snake to power)
- Can you get the answer that you want?

- If no, why not make your own wordlist based on the hint that keep on pop out while digging for file directory? (Hint: you need the cat help to grab the word and paste it on your wordlist file)
- Try again with your self-made wordlist and you will get the newly acquire user password hash
- Checklist: had you crack the key and store as a hash?

Escalate Privileges
- time to access the newly acquired user account
- go to the directory that you store the hash
- access it through ssh using the hash file (Hint: solve x : ssh (x) <filename.hash> username@ip)
- The password is the ripped key password
- Congratulation if you had accessed to this newly acquired account, you can find your user.txt flag here.
- But the fun part is yet to come, we need to root the plant for its delicacy and only superuser a.k.a admin get to enjoy.
- Maybe you can try some superman command
- You had been doing push up for some time, your arm might be strong like superman. Maybe you can carry some heavy stuff like superman do
- Did you found something? if yes? how about try to execute it like superman do?
- Oh, you had travel into a new spectrum, known as an interactive system shell.
- Try and see if you can find kryptonite maybe you will end up as G-girl from My Super Ex-girlfriend instead and don't forget about root.txt?

Extra Tips
- Don't forget to submit the captured flag.
- Always perform write-up before stopping or ending your hacking session.
- Check your hacking machine date and time when there's an error during installation or having trouble to access a websites
- The aim of this challenge is to gain access and not disrupt the HTB, OpenAdmin machine thru DOS attack.