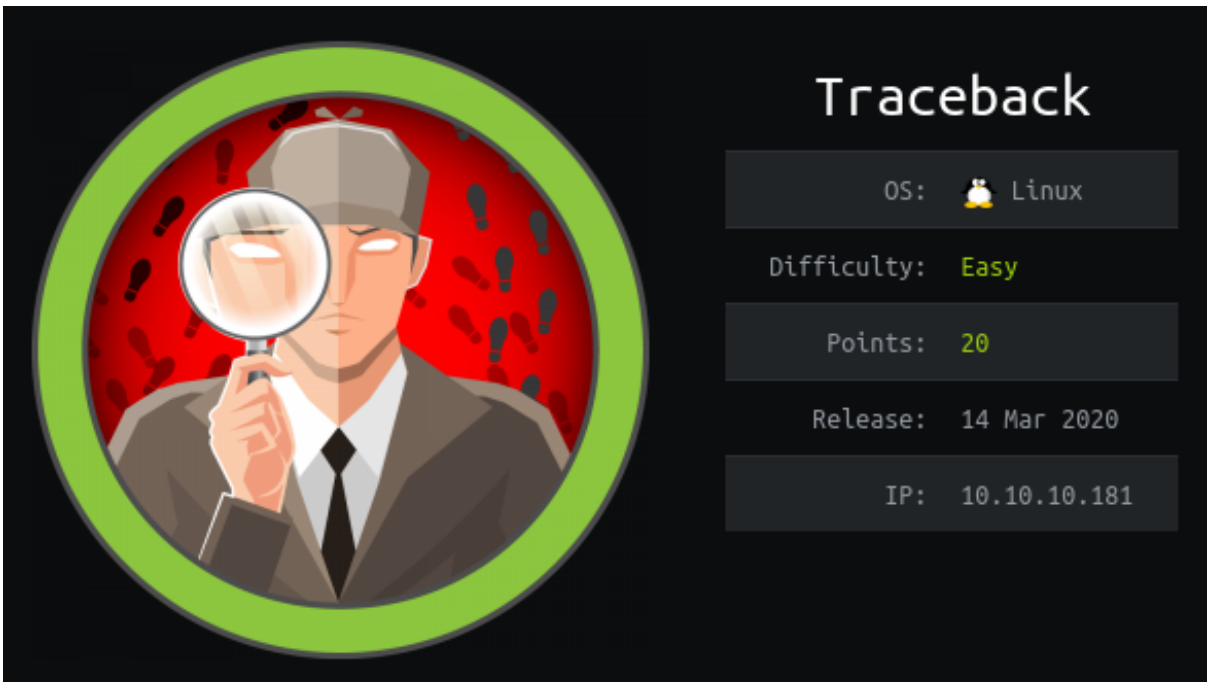
Traceback Cookbook



Learning Outcomes

At the end of this challenge, you learned how to setup hack-the-box VPN connection, perform port and vulnerabilities scanning, 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, DirBuster/GoBuster, Nikto
- Gain Access: Php-Reverse-Shell, Netcat, GTFOBins Lua ,
- Password cracker : SSH-Keygen
- Escalate Privileges : Pspy64s, Netcat one liner reverse-shell
- Web browser: Search Engine, Tools used Manuals

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 (Don't forget to full port scan)
- 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 webserver
- If nothing significant was found, why not try and access the website?
- Apparently the site was hack and there's a backdoor. Time to trace it. You can start from reading the HTML code.
- Based on the clue found, detective, try to trace it on your web browser search engine. Your target is on a blue bird site that leads you to a octocat page built for developers.
- Try access those files one by one until you are prompt to a login page
- Don't worry detective, you know the access code, it's written on the octocat file page
- Checklist time: had login into the webshell page?

Gain Access

- To gain access, we shall upload a reverse shell and listen patiently until we receive intel.
- Once the preparation was done, we shall get into action and execute the reverse shell file
- Checklist time: did you get connection as webadmin?
- Now that you have connection as webadmin, let's upgrade our shell to a better one.
- Unfortunately, interaction shell was disabled. Try a way to get SSH shell.
- Perform functional and relational analysis to get what you want and 'echo' your keys
- Once it done, try and port forwarding as webadmin via port 22, SSH.
- Checklist time: had you achieve SSH connection?

Local Enumeration

- Time to inspect this user (services running, kernel & version, open ports, privileges)
- Did you found the artefact left by the hacker?
- Follow the hacker instruction and it will leads to a horizontal privileges escalation
- Checklist time: did you manage to privEs into sysadmin user?

Escalate Privileges

- Examine this user (services running, kernel & version, open ports, privileges)
- Let's interrogate root by using pspy64s for suspicious activity
- Did you found the suspicious activity that being launch by root often?
- Let's pay a visit to the directory that was mentioned
- Apparently it was a backup files so let's visit the original source
- Is there a way to make use of message of the day to privEs?

- You may need to open up some reference book supported by VulnHub
- With this one liner reverse shell code, you are able to get reverse shell connection
- If that particular one liner doesn't works, you are targeting at the wrong version. Just search for alternative
- Prepare yourself before executing the mission! Everything needed to be execute swiftly with no mistake being made. Else mission fail.
- Checklist time: did you receive connection as root?
- Congratulation detective and it's time to hunt for the evidence, root.txt.

Fun Fact

- We can gain access as webadmin by replacing the authorized_key file at the webshell page and access it thru port 22, SSH instead.

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
- If you have issue during installation of tools to your hacking machine, make sure your machine and service used is up to date.
- If you have issue to install or run the tools, feel free to search for alternative that does the same job. They might be even mightier.
- Your hacking machine may not know the DNS of the box, you can go to etc/hosts and add the IP address of the box.
- The aim of this challenge is to gain access and not disrupt HTB machine thru DOS attack.
- Is cool that you found the files that you need but don't be mischievous and delete them. If you couldn't find valuable information during enumeration, always reset the box. It's better than falling into the rabbit hole.