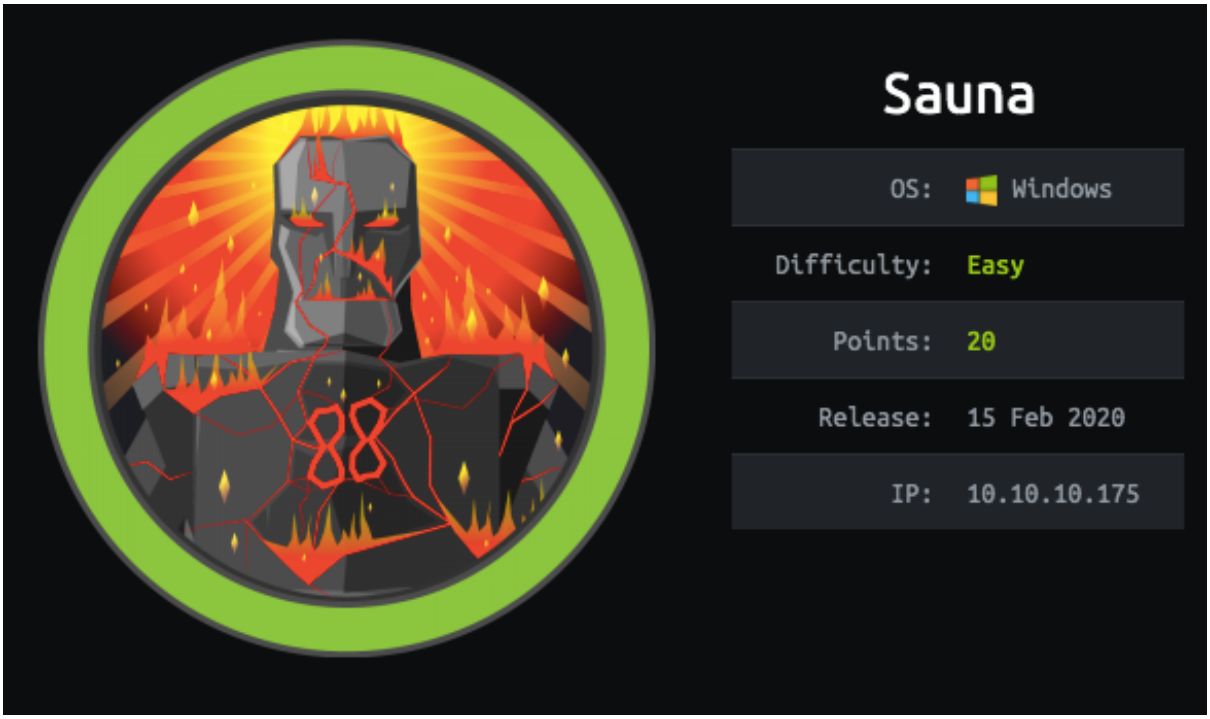
Sauna Cookbook



Learning Outcomes

At the end of this challenge, you learned how to setup hack-the-box VPN connection, perform port and vulnerabilities scanning, active directory enumeration, and escalate privileges in a Windows 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, KrbGuess, GetNPUsers, Bloodhound
- Gain Access: WinRM
- Password cracker : John the Riper, Wordlists
- Escalate Privileges : PowerUp/Powerless, WinPEAS, Mimikatz
- Web browser: Windows command manual, 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 and manuals?

Enumeration

- scan list of open ports, domain name, running OS & version (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 directory search tools for active and hidden directory (Hint: type the full url that you want to scan & use medium wordlist)
- Based on the directory found, access to the webserver and try to search for more clue.
- Try to connect or enumerate those open ports
- Did you get to connect/enumerate to one of the open ports?
- No result? It best to craft something from scratch for the best result (Hint: name)
- Now you had found the correct username, how to harvest the other half of the credential?
- Checklist time: do you have the credentials to login into Sauna-HTB?

Password Cracking

- The found hashes couldn't be used to access Sauna-HTB remotely.
- Ask john for some help
- Checklist time: had those keys got cracked?

Gain Access

- you need a devil who is evil to assist you in gaining access remotely
- Congratulation, you has successfully gain access to your first user. Time to capture user.txt flag.
- Now, power up and enumerate more! (services running, kernel & version, user group, privileges, registry)
- Keep digging until you found goldmine of a loan shark
- Checklist time: had you found credentials of the loan shark?

Local Enumeration

- Time to login as loan shark
- Check out the authority that the loan shark holds.
- Keep digging till you find the goldmine else sniff something bloody
- It can be a pain to acquire but a very useful ally to hunt for blood
- Sometimes trash = goldmine to others. (Hint: Dumpster diving)
- Checklist time: did you get the credential to Administrator?

Escalate Privileges

- time to access administrator account
- You owes the devil another favours
- Go read the devil's bible if you are unable to access.
- Had you successfully convince the devil and login as administrator? Congratulation and time to hunt for root.txt.
-

Fun Fact

- Sauna box is a little unstable, as the port that allows WinRM connection may be off after being reset. Suggestion: change server till you find it open.
- This challenge is a enumeration focus challenge
- There's a vast variety of tools that can be used to perform the same task. Feel free to explore and find the best that suit your style and needs.

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/host 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.