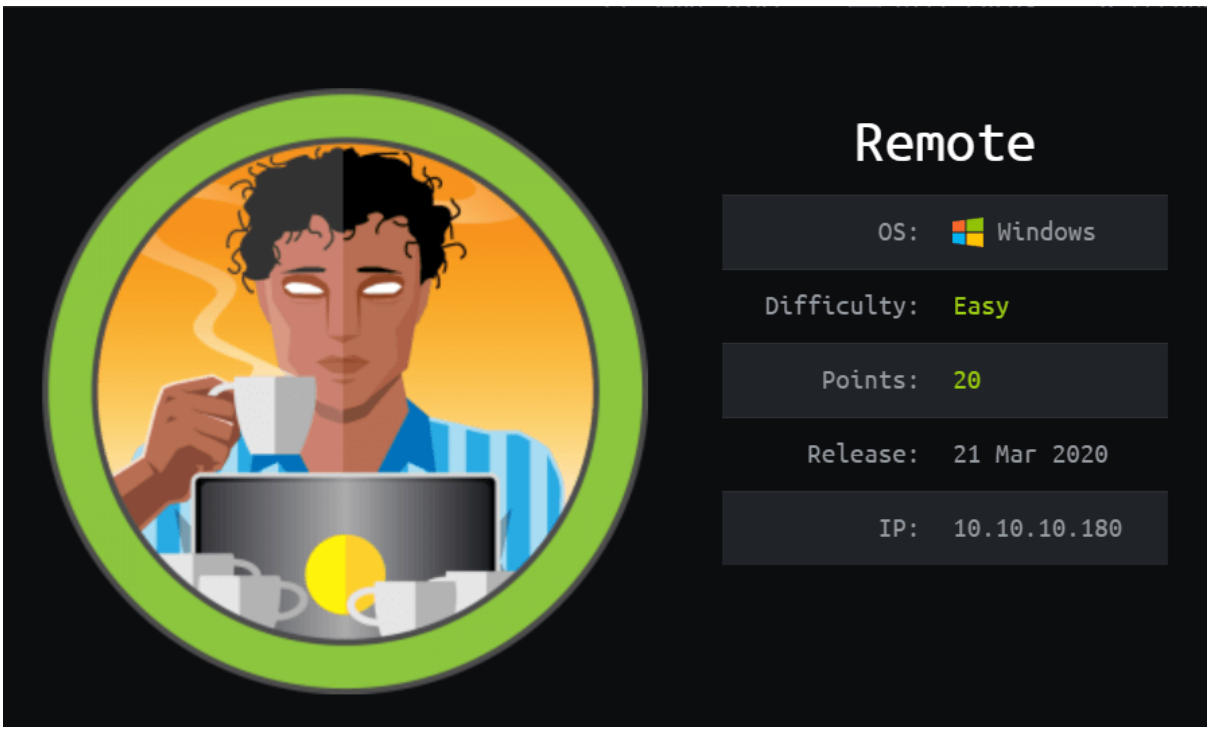
# Remote Cookbook




## Learning Outcomes

At the end of this challenge, you learned how to setup hack-the-box VPN connection, perform port and vulnerabilities scanning, create your own custom exploit, understand types of payload 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
- Gain Access: Dos2Unix, MSFvenom, Netcat ,Wireshark
- Password cracker : John the Riper, Wordlists
- Escalate Privileges : PowerUp/ AccessChk, WinRM/ Evil-WinRM
- Web browser: Windows command manual, ExploitDB, 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 on both TCP & UDP)
- 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
- Try to connect to open ports (Such as: FTP, SMB,NFS)
- Did you get to connect to one of the open ports? IF yes, continue digging for valuable information (Such as: site backup, configuration, username, password, service and version running)
- Found any interesting files? You need the "cat" to help fetching data.
- If a file data is huge, try input some copy command to save it at a specific file
- Did you found something useful in from that file? (Hint: username , password, hashes)
- If it is a hash, find John for help to crack those keys
- Checklist time: do you have username and password?

## Gain Access

- Search for vulnerabilities within the version of the running system in ExploitDB
- Understand the exploit and download it
- Don't forget that you are required to edit the exploit file to fulfil your purposes.
- Convert the exploit file using Dos2Unix
- Make sure the file is assign to the right permission
- Run the exploit. Did you gain remote shell?
- Maybe you can sniff around to see if they are talking silently
- You need to send a reverse TCP shell to your hacking machine to gain access (Hint: payload)
- Maybe you can try sending the reverse shell from Remote-HTB machine instead while listening from your hacker machine. (Hint: you can edit the exploit file)
- Did your listener receive some connection and miraculously provides you reverse shell and now you had gain access as user of Remote-HTB.
- Congratulation, you are able to capture user.txt flag.

## Local Enumeration

- Check out what and who is this user (services running, kernel & version, open ports, privileges)
- Did you found anything interesting on privileges or weak services?
- Try and "invoke" them thru a powerful shell or "query" the service
- Always read the tools manuals to see what you can do with it and what can you abuse.

- Checklist time: did you get username and password?

## Escalate Privileges

- time to access the newly created administrator account
- windows does not have run as function, you need a devil who is evil to assist you
- However, you can do something cool and learn something new by enabling a port that allows you to connect to Remote-HTB in GUI form.
- Had you login to the newly created administrator account? Congratulation and time to hunt for root.txt.

## Fun Fact

- There's an alternative way to escalate privileges to Administrator by stopping the service and launch a reverse shell payload. In the meantime, you listen patiently thru your hacker machine until connection pack receive.
- You can connect to Remote-HTB and root the box in GUI by enable port 3389, RDP.

## 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.