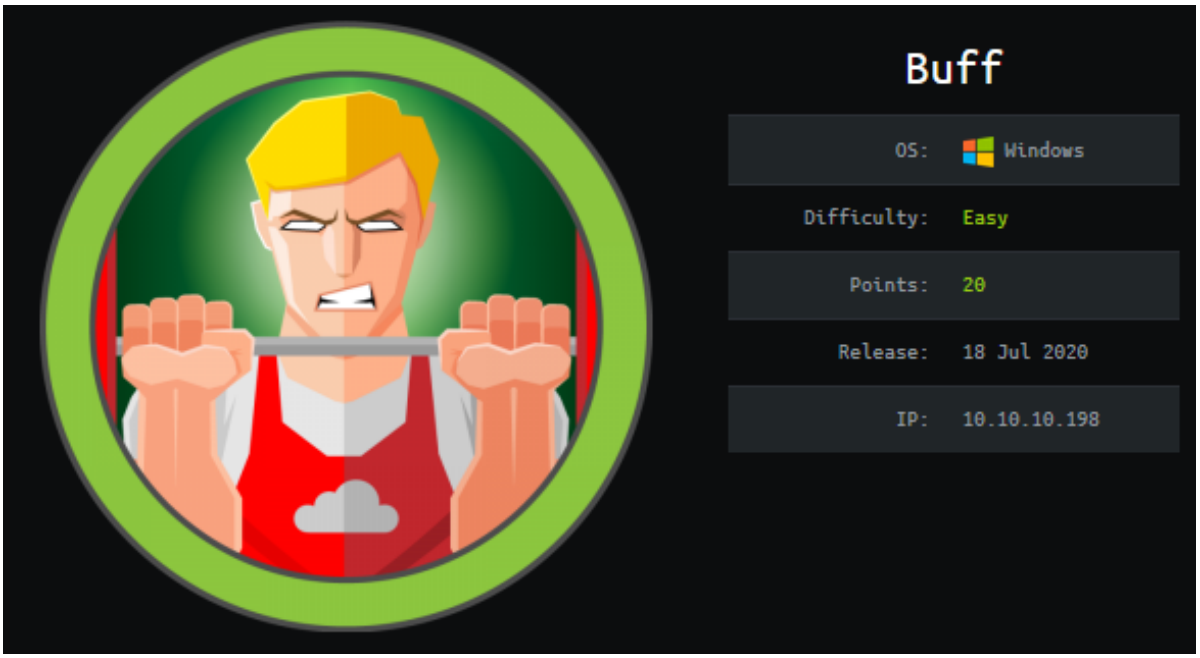
Buff Cookbook



Learning Outcomes

At the end of this challenge, you learned how to setup hack-the-box VPN connection, perform port and vulnerabilities scanning, exploit vulnerable system, port forwarding and pivoting, escalate privileges by launching buffer overflow on 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, DirBuster/GoBuster, Nikto
- Gain Access: Netcat, Plink, Exploit-DB
- Password cracker : SSH-Keygen
- Escalate Privileges : msfvenom, Exploit-DB
- 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?
- We found a login input header, we can try to bypass it via injection or guessing.
- Since we couldn't bypass the login system, enumerate harder by searching for more information. (e.g: owner, management system running, link, username)
- Google is your best bud, you can obtain lots of information from there.
- Don't forget about a good old pal with a spider database for hackers
  Checklist time: had you gather the information to gain shell access?

Gain Access

- To gain access, we shall grant permission to execute the exploit file.
- It seems that we are stuck in the same directory after exploiting it. Break it with all your strength! User.txt is all yours!
- No pain, no gain. There's multiple way to gain that strength. You can obtain it either from the web or terminal.
- Checklist time: have you gain enough strength to break the restrictions?
- Cheers, you did it! User.txt is now all yours.

Local Enumeration

- Time to reflect the new you by checking what you can do (services running, kernel & version, open ports, privileges)
- Have you found that one technique to get buffed up body?
- Find your best bud, they can give you some insight.
- Checklist time: have you found the instruction to get buffed up body?

Escalate Privileges

- Let's modify the suggested weights in that instruction to fits our needs. Which is to get as buffed as Arnold Schwarzenegger.
- Next, launch the buffed up program powered by python. However, the gym doesn't possessed any python.
- Why not perform a home workout instead? We have python at home.
- However, we need putty to forward our program remotely.
- Checklist time: have you connect the program from gym to home?
- Next, we shall grant permission to our program from out housing management

- Lastly, we shall execute our buffed up program and overload our muscle with numerous repetition.
- Checklist time: did you receive connection as root?
- Congratulation, you are now as buffed as Arnold Schwarzenegger and it's time to celebrate your achievement with root.txt
-

Fun Fact

- You can get user.txt without needing to send reverse shell. (Hint: you already got web shell)

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.