Try Hack Me Solutions

tryhackme.com is a website containing cyber security problems/questions.

Try Hack Me is organized into rooms that might have many problems relating to a central theme. To attempt the problems, one needs to open a connection to AttackBox, a web-based connection to a Kali machine. Alternatively you can use OpenVPN. For free users there exists a time limit on using the machine, but people with subscriptions, it is unlimited max machine open is 3.

Path

1. Start with the tutorial which will help you set up
2. Next do an easy challenges such as Vulnversity although this one is a bit long ans something like Web Fundamentals might be easier
3. Do some more easy/tutorial ones to get your feet wet

Index

Tutorial

1. Start a machine, this will take ~ 1-2 minutes for pro accounts
2. (Recommended) have two windows if 2+ monitors, 1 for Kali Linux window and another for the instructions
3. Follow instructions to get the flag and submit it

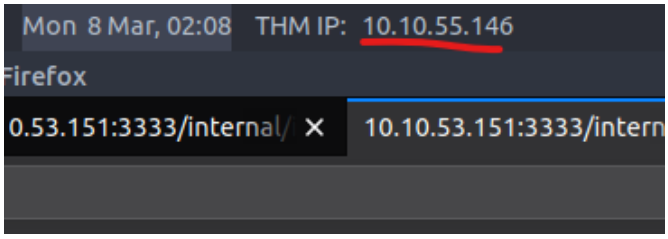
Web Fundamentals

Good place to start out

Instead of using curl in the command line, using postman to send requests might be easier

Vulnversity

1. Run `nmap -A -sC -p- -oN vul.nmap 10.10.IP ADDRESS HERE*` on the instance of Kali
2. Wait >10 minutes for it to resolve
3. Scan for hidden files by doing `gobuster dir -u http://<ip>:3333 -w /usr/share/wordlists`
4. Go to the <ip>/internal/index.html on firefox (**Make sure u aren't using http or https before the url**)
5. Follow the rest of the steps till yo get to injecting the PHP code
6. Make sure download the PHP file from GitHub, rename it to be a .phtml and change the IP to the TMP IP address



7. Save, upload, listen, then submit file
8. Then the netcat should allow you in such that you can gain control and find out things about the machine
9. Follow https://n0w4n.nl/vulnversity/#crayon-60458bd07482b875406373 to gain admin privileges
10. Follow the rest of the instructions and you should be done!

Resources:

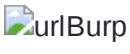
- https://n0w4n.nl/vulnversity/
- https://www.youtube.com/watch?v=hvYWCegfEZs&ab_channel=JohnHammond

Burp Suite

Follow instructions, mostly straight forward

Task 6 (some step in the middle) the question that starts with "Return to your web browser and navigate to the web application hosted on the VM we deployed just a bit ago", this web application is deployed/started in Task 6 (show below)

The URL to enter is the one at the top of the page in a red box (see below)



Linux Series

1. Part 1

Simple and easy -> do it in any Linux distro except for **Task 9**, but that's just my friend *pinguftw* for the answer if you can't be bothered to run the binary :p

2. Part 2

* Remember to start the machine (which is different from the attack box)

This one has a lot of useful information and here are some that I did not know:

- `;` operator is the same as `&&` but does not need to execute successfully

3. Part 3

This part goes through some more tools and commands for us to go into.

Task 7 -> `find / -name shiba4 2>/dev/null` (idk what `2>/dev/null` does but it works)

OpenVPN

1. Download OpenVPN and install it
2. Download the configuration files from TryHackMe
3. Load the config file onto OpenVPN
4. Connect
5. ssh into server

CI for PDF

Back to Top