TRYHACKME - ROOTME ROOM

Successfully completed TryHackMe RootMe room, Here's a detailed step-by-step breakdown of how I tackled the challenges:

Step 1: Reconnaissance
i. Port Scanning: Utilised nmap to conduct a comprehensive scan of the target machine. Discovered 2 open ports: SSH (22) and HTTP (80).

ii. Service Version Detection: Leveraged nmap's -sV ability to identify the version of services running on open ports. Found Apache version 2.4.29 running on port 80.

iii. Directory Enumeration: Employed GoBuster to enumerate directories on the web server. Discovered a hidden directory "/panel/" which hinted at potential entry points.

Step 2: Getting a Shell
i. Exploration of Hidden Directory: Accessed <ip_addr>/panel/ via web browser to explore the hidden directory and found an upload form.

ii. Reverse Shell Payload: Created a shell.php file using the reverse shell payload.

iii. File Upload: Uploaded the shell.php file to the /panel/ directory, after altering its extension to .php5 to evade server restrictions.

iv. Listener Setup: Initiated a netcat listener to intercept the reverse shell connection.

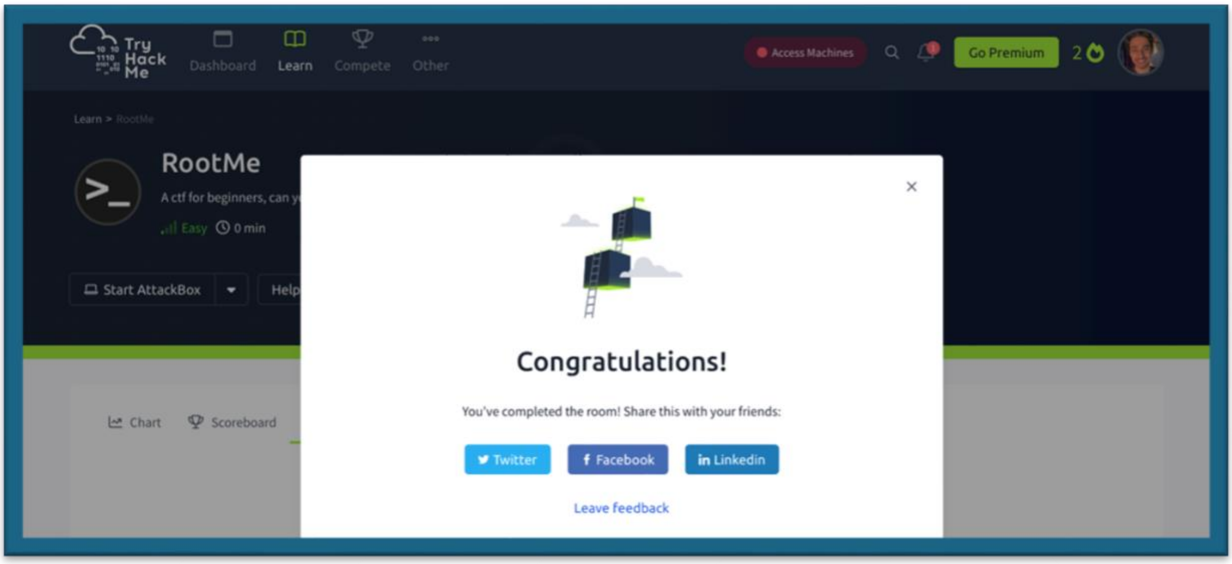
v. Access Gained: Clicked on the uploaded shell in the /uploads/ directory to establish a connection and gain access to the system.

vi. User Flag Retrieval: Located user.txt using the find command to retrieve the user flag.

Step 3: Privilege Escalation
i. SUID Permission Analysis: Conducted a search for files with SUID permission using the find command. Identified /usr/bin/python as having SUID permission.

ii. Exploitation: Referenced GTFOBins to identify a privilege escalation technique using Python. Executed the command to escalate privileges.

Each step involved meticulous analysis, creative problem-solving, and effective utilization of tools and resources. Thrilled to have completed the challenge and I am eager to continue learning and exploring the cybersecurity realm!



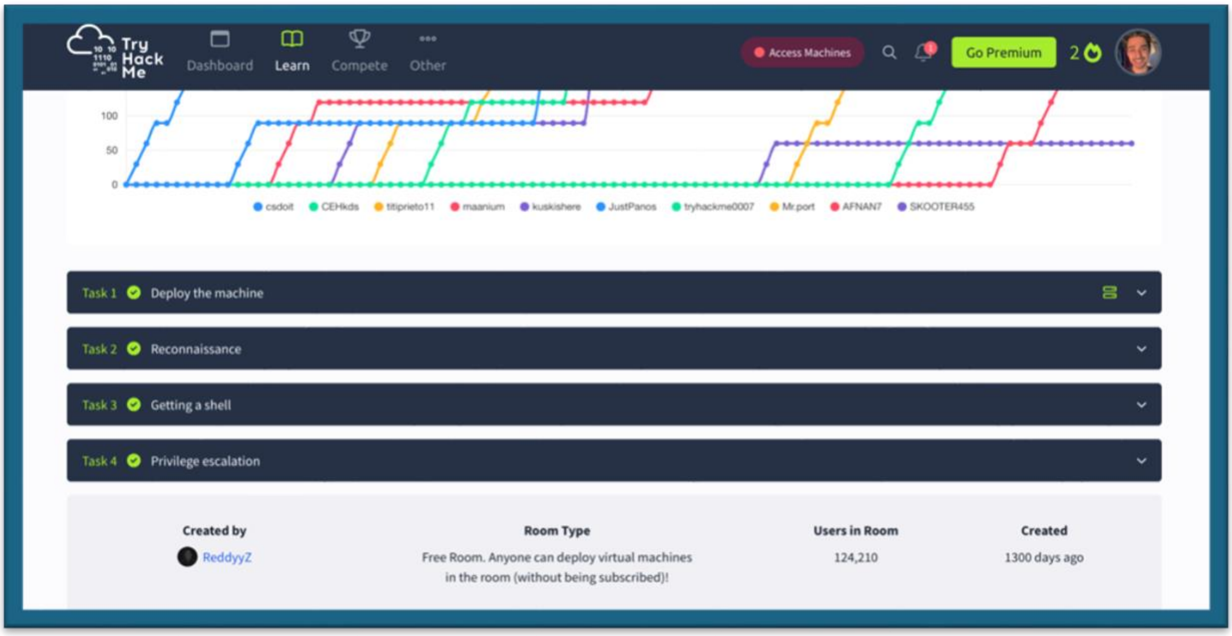
RootMe

A ctf for beginners, can y

Easy 0 min

Congratulations!

You've completed the room! Share this with your friends:



Task 1 ✓ Deploy the machine

Task 2 ✓ Reconnaissance

Task 3 ✓ Getting a shell

Task 4 ✓ Privilege escalation

Created by	Room Type	Users in Room	Created
ReddyyZ	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	124,210	1300 days ago