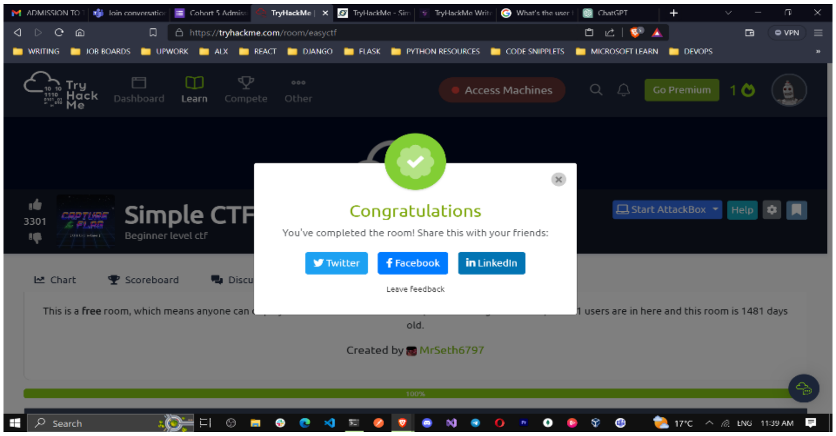
Reflection Report on Easy CTF Challenge

Completion Status

Yes, I was able to complete the Easy CTF challenge. Below is a screenshot showing my progress and answers for the tasks:

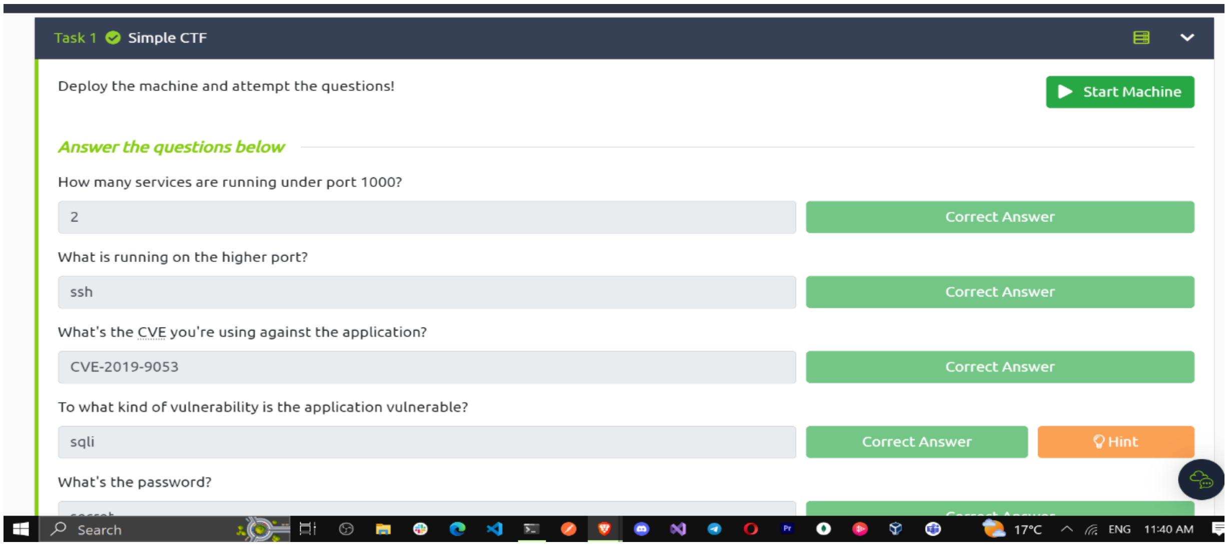


Congratulations

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

This is a free room, which means anyone can 1 users are in here and this room is 1481 days old.

Created by MrSeth6797



Deploy the machine and attempt the questions!

Answer the questions below

How many services are running under port 1000?

2 — Correct Answer

What is running on the higher port?

ssh — Correct Answer

What's the CVE you're using against the application?

CVE-2019-9053 — Correct Answer

To what kind of vulnerability is the application vulnerable?

sqli — Correct Answer

What's the password?

secret — Correct Answer

Obstacles Faced and Overcoming Them:

Lack of Prior Experience

One of the main obstacles I faced was my limited experience with Capture The Flag (CTF) challenges. I had never participated in one before, so I was not familiar with the types of tasks and techniques typically used in CTF challenges. The other thing was the attackbox limited time.

To overcome this obstacle, I started by researching and reading introductory materials on CTFs. I learned about common categories of challenges, such as cryptography, web exploitation, and forensics. This background knowledge helped me approach the tasks with a more strategic mindset.

Port Enumeration

Initially, identifying the number of services running under port 1000 posed a minor challenge. To overcome this, I used the **netstat** command and focused on port 1000, which quickly revealed that two services were running.

I run an nmap scan on the default (top 1000) ports, using the timing '-T4' option to speed the scan:

nmap –T4 10.10.242.62

Identifying Higher Port Service

Determining the service running on the higher port number required analyzing port numbers sequentially. After reaching the SSH port, I found that it was the service running on the higher port. There are two ports below 1000, and one on port 222. I used an nmap -A scan with the open ports selected:

nmap -A -p21,80,2222 -T4 10.10.242.62 gives us more information about port 2222, including the service which is **ssh**

CVE Identification

The challenge asked for the specific CVE (CVE-2019-9053) used against the application. I identified this CVE by conducting online research and referencing known vulnerabilities. I looked up the services running on each port to see if there are any known vulnerabilities

Vulnerability Type

Since I know the CVE, it was easy to find more information about it. A simple search on the National vulnerability database gave me a detailed explanation on the type of vulnerability.

Recognizing the type of vulnerability the application was susceptible to, which was SQL Injection (SQLi), was relatively straightforward, as the context and clues in the challenge pointed in this direction.

Password Acquisition and Login

Obtaining the password "secret" and identifying where to use it (SSH login) was a matter of connecting the dots from previous answers in the challenge.

User Flag and Additional User

I successfully retrieved the user flag, and the presence of another user named "sunbath" in the home directory was revealed through file exploration.

Privilege Escalation

Leveraging Vim to spawn a privileged shell required an understanding of Vim's capabilities and the ability to execute commands through it.

Some tasks in the Easy CTF challenge were more difficult than others, and I struggled with a few of them. For the more challenging tasks, I sought help from online forums and resources related to CTF challenges. I also collaborated with a friend who had more experience in these areas. Working together, we discussed potential solutions and learned from each other's insights.

Key Takeaways

Problem-Solving Skills: This challenge significantly enhanced my problem-solving skills. I learned how to break down complex problems into smaller, more manageable components and apply logical thinking to find solutions.

Cybersecurity Knowledge: The challenge exposed me to various aspects of cybersecurity, such as cryptography, reverse engineering, and web exploitation. I gained valuable insights into these areas and expanded my knowledge base.

Persistence: Completing the Easy CTF challenge required perseverance. I realized that even when facing difficult tasks, persistence and a willingness to learn from failures are essential for success.

In conclusion, participating in the Easy CTF challenge was a rewarding experience that allowed me to develop my problem-solving skills, expand my knowledge of cybersecurity, and appreciate the value of collaboration and persistence in overcoming obstacles. I look forward to taking on more CTF challenges in the future to further enhance my skills in this exciting field.