Dear Hiring Manager at VTF,

I am writing to express my interest in the Advanced Red Team Engineer Internship position at Virtually Testing Foundation. I am a highly motivated and skilled cybersecurity professional with a passion for offensive security. I have a strong understanding of the cyber threat landscape and the latest attack techniques. I am also proficient in a variety of red team tools and techniques.

In my previous roles as a Red Team Engineer in current cohort at VTF, and Cloud VAPT Intern, I have gained valuable experience in conducting penetration tests, identifying and exploiting vulnerabilities, and developing and executing red team plans. I have also worked on a variety of projects related to cloud security, network security, and incident response.

I am confident that I have the skills and experience necessary to be successful in this role. I am a quick learner and I am always eager to take on new challenges. I am also a team player and I am confident that I can contribute to the success of your team.

I am currently pursuing a B.Tech Cybersecurity degree at Shri Ramdeobaba College of Engineering and Management, Nagpur. I am also a member of the Virtually Testing Foundation.I am available to start the internship immediately. I am eager to learn more about this opportunity and I am confident that I would be a valuable asset to your team.

Thank you for your time and consideration. I look forward to hearing from you soon.

Sincerely,
Gaurav singh

tryhackme.com/profile

$20,000 in prizes up for grabs! Claim yours by earning 3 matching tickets Start here

Try Hack Me | Dashboard | Learn | Compete | Other | 0

Your Profile

Manage your account

Public Profile

General | About you | Other

Click to update

Full Name

gaurav singh

Username

gaurav.singh692

Email

gaurav.singh@virtuallytestingfoundation.org

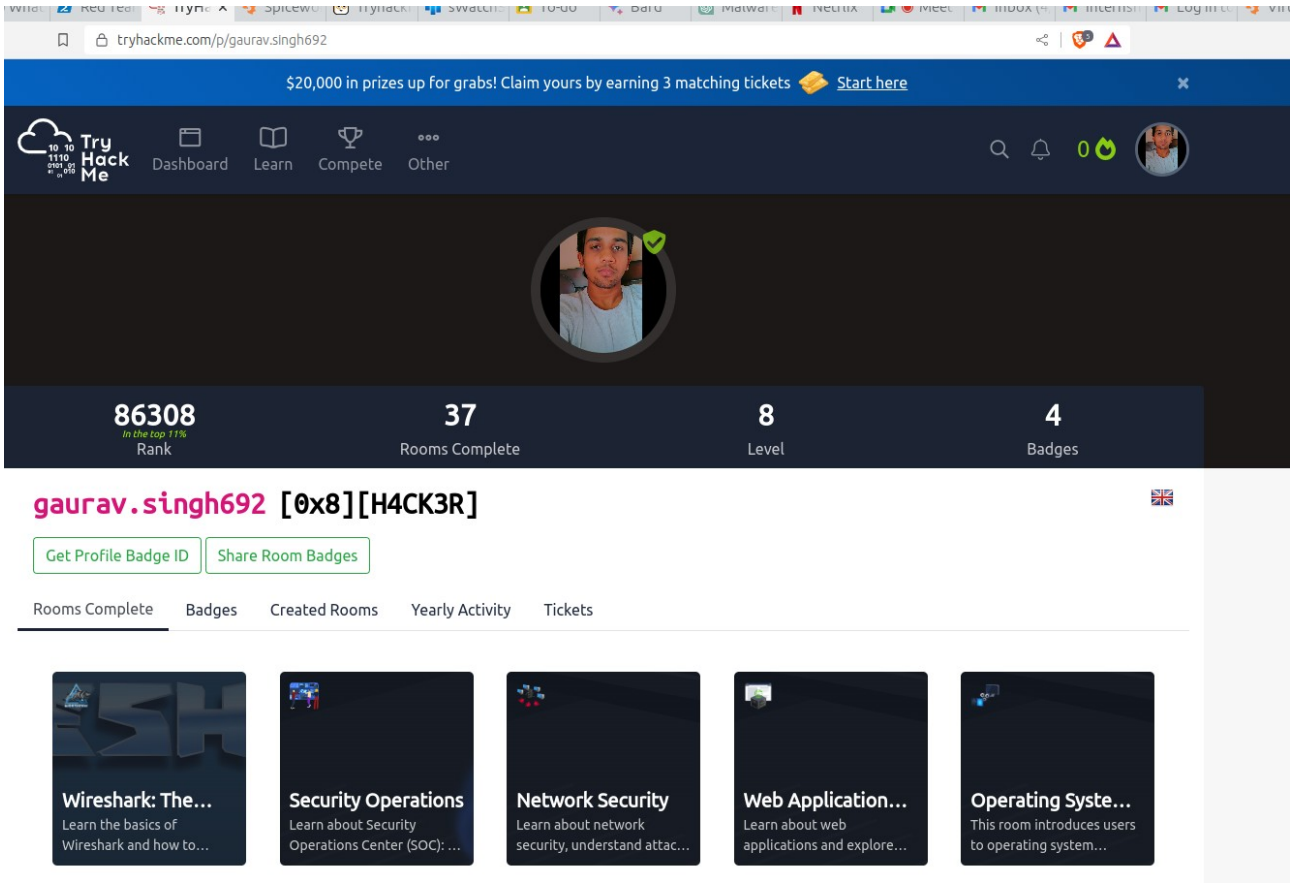
Save Changes

Subscribe

Your subscription will end on: `Dec 30, 2023`

Why stay subscribed?

✓ Access to all premium learning content


tryhackme.com/p/gaurav.singh692
$20,000 in prizes up for grabs! Claim yours by earning 3 matching tickets
Start here
Try Hack Me
Dashboard
Learn
Compete
Other
0
86308
In the top 11%
Rank
37
Rooms Complete
8
Level
4
Badges
gaurav.singh692 [0x8][H4CK3R]
Get Profile Badge ID
Share Room Badges
Rooms Complete
Badges
Created Rooms
Yearly Activity
Tickets
Wireshark: The...
Learn the basics of Wireshark and how to...
Security Operations
Learn about Security Operations Center (SOC): ...
Network Security
Learn about network security, understand attac...
Web Application...
Learn about web applications and explore...
Operating Syste...
This room introduces users to operating system...


$20,000 in prizes up for grabs! Claim yours by earning 3 matching tickets
Start here
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
0
11
VTF RED TEAM
Room for testing skills of new VTF Red Team members
Start AttackBox
Help
Chart
Scoreboard
Discuss
Writeups
More
Difficulty: Medium
1000
800
600
400
200
0
106Sam
abdulmoizquddus
Wcmoawq
sumitdas
officialjm
0xVulcan
Ephatah
CIPH3r
kaleem.ullah.vtf
gaurav.singh692
100%
Task 1 Introduction
Task 2 Reconnaisance
Task 3 FTP
Task 4 HTTP
Task 5 SSH
Task 6 PWN Flag

.

100%

Task 1 Introduction

Virtually Testing Foundation is World's first and only [unique] non-profit offering hands-on valuable cyber security internships

Follow us on LinkedIn, Twitter, Instagram, Facebook , GitHub and YouTube.

This room is intended for the applicants of Red Team Engineers intern at Virtually Testing Foundation. It contains multiple Tasks/Sections in which further Questions are present. Applicant needs to complete each of the Tasks for completing this room.

If you are new to THM (Try Hack Me). Complete this room to understand, how to connection to THM server to access the VM in this room
TRY HACK ME TUTORIALS (Recommended).

Answer the questions below

Let's get started!

No answer needed — Question Done

Task 2 Reconnaisance

Task 3 FTP

Task 2 Reconnaisance

In this first section, you are given an Attacker Machine and a Victim Machine. You need to first gather the information related to the services running on it. Then you need to exploit the machine using one of its vulnerabilities of any one of the services running on it.

Start Machine

A **Red Teamer** must be very familiar with the working of the network for exploiting it. As an exploit is any attack that takes advantage of vulnerabilities in applications, networks, operating systems, or hardware.

Start Your Attack Now :)

Answer the questions below

How many ports are open in the machine?

3 — Correct Answer

Which service is running on port 21 ?

ftp — Correct Answer

Which version of ftp is running on port 21 ?

vsftpd 2.0.8 — Correct Answer

Which service is running on port 100 ?

ssh — Correct Answer

Which version of SSH is running on port 100 ?

OpenSSH 6.6.1p1 — Correct Answer

Task 1 Introduction

Task 2 Reconnaisance

Task 3 FTP

Answer the questions below

What is the name of the file in FTP ?

note.txt — Correct Answer

What is the username ?

Jack — Correct Answer — Hint

Task 4 HTTP

Go through the website and gather following information.

Answer the questions below

Did you find any hidden directories ?

Yes — Correct Answer — Hint

Which directory looks suspicious ?

zip — Correct Answer

What is the name of the file inside the directory ?

credentials — Correct Answer

What is the name of the normal user's Mentor ?

Victor Monga — Correct Answer

What is version of Apache Server ?

2.4.7 — Correct Answer

Task 5 SSH

Login into SSH as normal user and escalate to a privileged user.

Answer the questions below

What is the password of normal user ?

Victor — Correct Answer — Hint

What is the username of privileged user?

goblin — Correct Answer — Hint

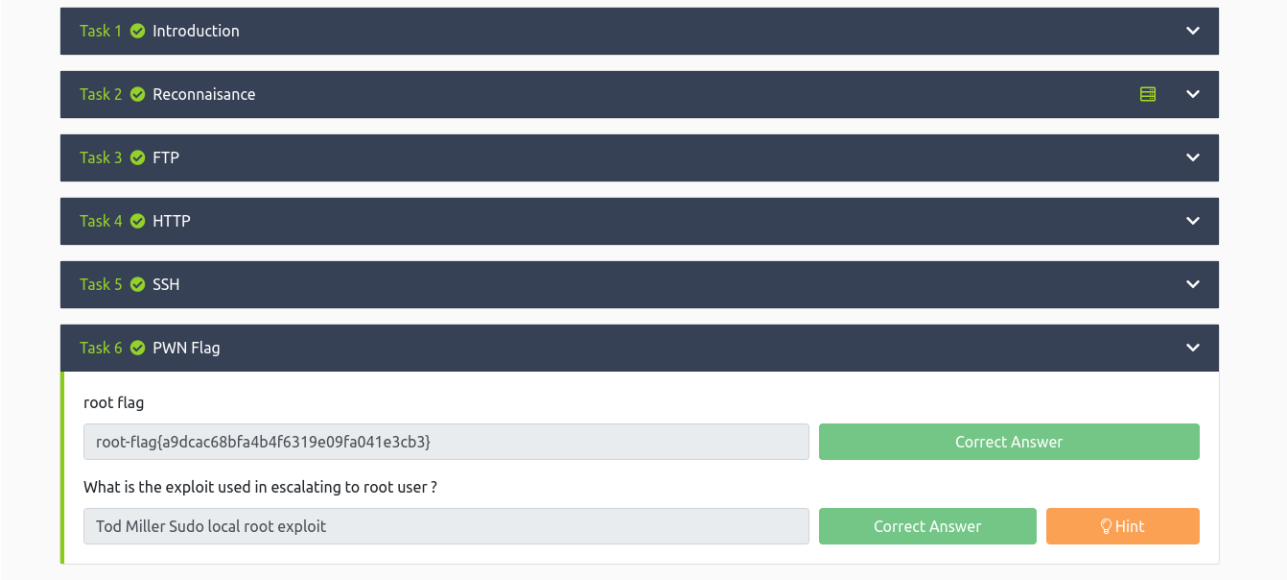
Where is the interesting file located ?

/usr/share/hs/final.sh — Correct Answer — Hint

What is the technique used in finding the password used of privileged user?

Brute Force — Correct Answer — Hint

Task 6 PWN Flag


Task 1 Introduction
Task 2 Reconnaisance
Task 3 FTP
Task 4 HTTP
Task 5 SSH
Task 6 PWN Flag
root flag
root-flag{a9dcac68bfa4b4f6319e09fa041e3cb3}
Correct Answer
What is the exploit used in escalating to root user ?
Tod Miller Sudo local root exploit
Correct Answer
Hint