SLIIT

Discover Your Future

Systems and Network Programming - IE2012

YEAR 2 , SEMESTER 1

TRYHACKME ROOM

IT22315496
Chamod Anuradha

✓ **Topic**

- TryHackMe room

✓ **TryHackMe room link**

- tryhackme.com/jr/tryhackmeroom

✓ **Course code**

- IE2012

TERMS OF REFERENCE

A report submitted in fulfilment of the requirement for the module IE2012, Sri Lanka Institute of Information Technology.

1) Contents

Abstract

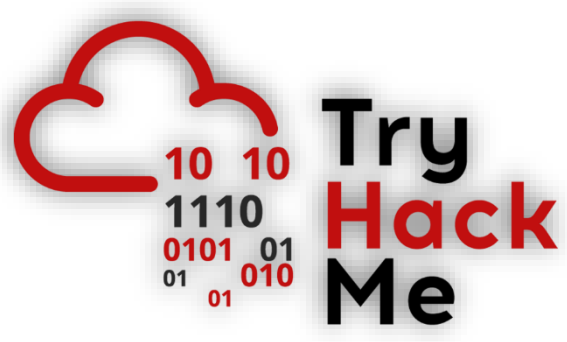
The purpose of this project is to provide a clear, understandable explanation of how to create a TryHackMe room for beginners. TryHackMe is a well-liked resource for practicing and acquiring cybersecurity skills through practical exercises. We will dissect the fundamental processes needed to create and release a TryHackMe room in this project, enabling users to interact, practice, and gain knowledge about a variety of cybersecurity topics. With the help of this project, you may create your own TryHackMe room and contribute to the expanding cybersecurity community, regardless of whether you're an enthusiast, instructor, or simply wanting to share your expertise.

Introduction

Developing a TryHackMe room project lets you create and share your own cybersecurity challenges with the community, which is an intriguing undertaking. You may create unique exercises and situations for a particular project that will assist others in learning and honing their security and hacking abilities. Creating a TryHackMe room is an excellent method to advance the cybersecurity community and develop your own skills, regardless of your level of experience. Now let's delve in and examine the fundamentals of getting started on this path of creativity and education.

TryHackMe room

What is TryHackMe?



When it comes to Cybersecurity education, TryHackMe is an online platform that excels in providing hands-on virtual laboratories. No of your level of expertise in the field of security, you can benefit from the information presented in a virtual room setting. We collaborate with schools all over the world to give students a hand in applying classroom knowledge to real-world scenarios. [1]

Members of TryHackMe get access to a private network of susceptible PCs and cloud technologies, providing a safe and regulated environment for learning and practicing pentesting methods. The site offers a variety of learning resources, including themed rooms for OSCP certificates and Linux and web fundamentals, to cater to users with varying degrees of expertise.

Why should we use tryhackme?

TryHackMe now offers 217 public rooms where people may converse about helpful and engaging subjects. As part of our virtual laboratory, you will be able to access challenge or walkthrough-style material via your own computer on our network. There won't be any loud neighbors or dead parrots to worry about. In addition to the community-provided articles and blogs, we also provide videos that cover the fundamentals of cybersecurity technologies and practices for those with a preference for more visual learning. Reach new heights on the leaderboards and gain experience by completing goal-based activities.

Got that competitive spirit? You can now hack against other players on the same system in our latest game mode, King of the Hill (KoTH). Infiltrate, bodge your way in, and ascend to the throne! [3]

What is penetration testing?

A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF). [4]

7 Steps and Phases of Penetration Testing

- Information Gathering
- Reconnaissance
- Discovery and Scanning
- Vulnerability Assessment
- Exploitation
- Final Analysis and Review
- Utilize the Testing Results

Information Gathering

Information collecting is the first of the seven steps in the penetration testing process. The penetration tester will receive generic target information from the organization under test. In this penetration test step, open-source intelligence (OSINT) is also employed with respect to the in-scope environment.

Reconnaissance

For a comprehensive security test, the reconnaissance phase is essential because penetration testers can find extra data that might have been missed, misplaced, or withheld. Although we don't usually carry out this reconnaissance in web application, mobile application, or API penetration testing, it is particularly useful in internal and/or external network penetration testing.

Discovery and Scanning

One method to check for perimeter vulnerabilities is through discovery scanning. Using the information obtained, discovery operations are carried out to find out what ports and services were open for targeted hosts, or subdomains, accessible to web applications. Our pen testers then examine the scan data and devise an exploit strategy. Many organizations end their penetration testing with the findings of the discovery scan, but you won't fully understand the extent of your attack surface unless you manually analyze and exploit the data.

Vulnerability Assessment

To gather preliminary information and find any potential security flaws that would enable an outside attacker to access the system or environment under test, a vulnerability assessment is carried out. However, a vulnerability assessment can never take the place of a penetration test.

Exploitation

Our skilled penetration testers will validate, attack, and exploit those vulnerabilities using manual methods, human intuition, and their backgrounds after analyzing the vulnerability assessment results. An competent pen tester can do tasks that automation and machine learning cannot. A skilled penetration tester can take advantage of weaknesses that an automated system would likely overlook.

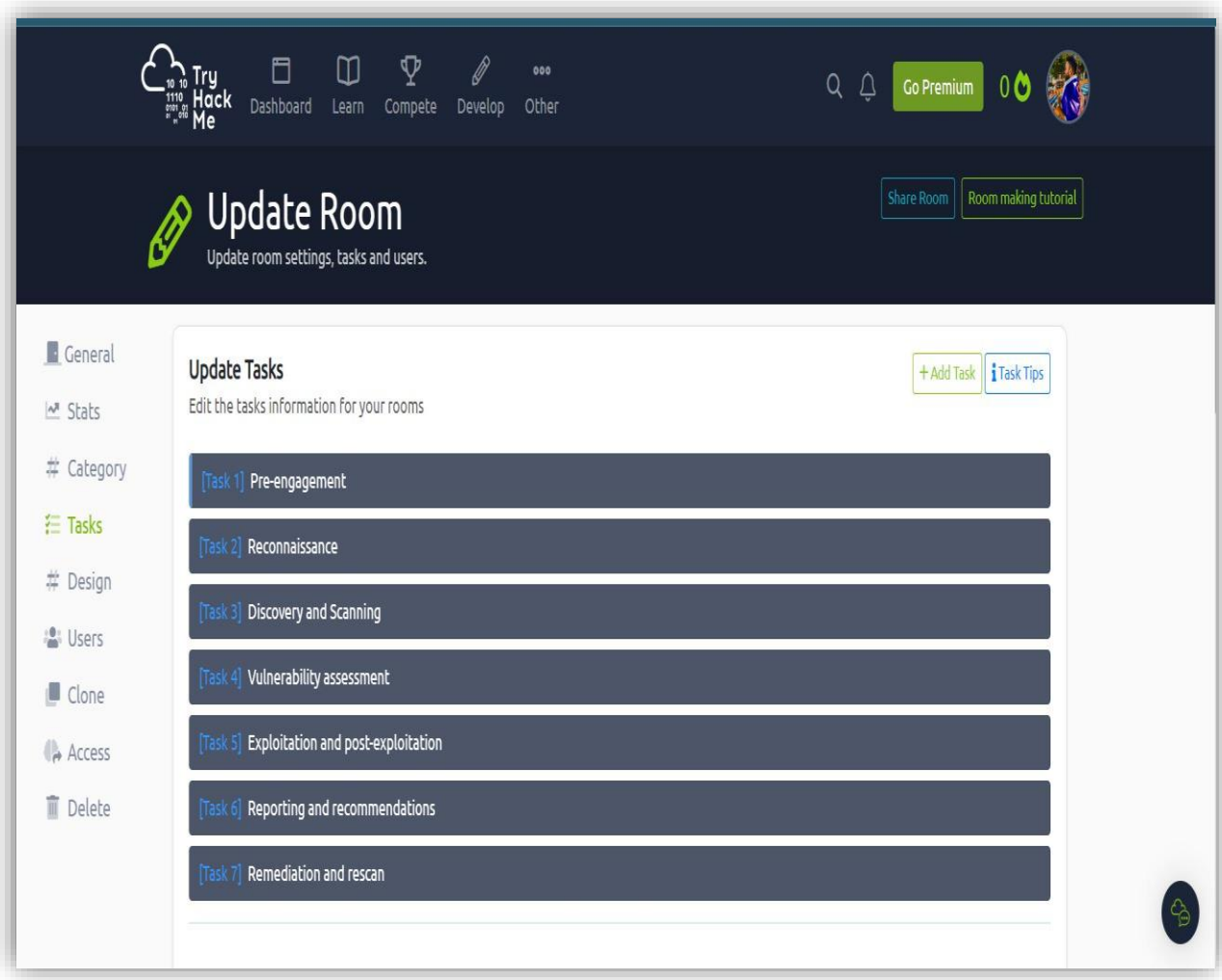
Final Analysis and Review

This thorough report provides descriptions of our testing process, where we began, how we discovered vulnerabilities, and how we took advantage of them. The breadth of the security testing, testing procedures, results, and repair suggestions are also included.

It will also provide the penetration tester's assessment, if relevant, of how closely your penetration test complies with the relevant framework specifications.

Utilize the Testing Results

The final step in the seven-step penetration testing process is crucial. The organization undergoing the security testing actually needs to apply the results of the testing to risk rank vulnerabilities, assess the possible consequences of vulnerabilities discovered, establish repair plans, and guide future decision-making.


Try Hack Me
Dashboard
Learn
Compete
Develop
Other
Go Premium
Update Room
Update room settings, tasks and users.
Share Room
Room making tutorial
General
Stats
Category
Tasks
Design
Users
Clone
Access
Delete
Update Tasks
Edit the tasks information for your rooms
+ Add Task
Task Tips
[Task 1] Pre-engagement
[Task 2] Reconnaissance
[Task 3] Discovery and Scanning
[Task 4] Vulnerability assessment
[Task 5] Exploitation and post-exploitation
[Task 6] Reporting and recommendations
[Task 7] Remediation and rescan

Conclusion

Building a TryHackMe room project is a fun project that lets you challenge others in the cybersecurity community and impart your expertise. To sum up, starting this path offers a fantastic chance to develop your own talents while learning from, teaching, and supporting the cybersecurity community. So go ahead and start creating your space; there are many options, and it might have a big influence. Have fun hacking!

References

[1] tryhackme.com,
[Online].Available:https://docs.tryhackme.com/docs/general/welcome.

[2] docs.tryhackme.com,
[Online]. Available: https://docs.tryhackme.com/docs/general/why-should-i-join.

[3] [Online]. Available: https://news.gallup.com/poll/184649/telecommuting-work-climbs.aspx

[4] Richardson, L. (2023, March 14). *What is Penetration Testing | Step-By-Step Process & Methods | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/penetration-testing/


THANK YOU!