

Scanning Practice

This assignment is all about hands-on practice in the scanning phase. I have located three great TryHackMe rooms, each focusing on one of the different scanning techniques we discussed. For this assignment, select one of the rooms depending on your specific area of interest.

Instructions

Choose Your Focus: Select one of the three rooms based on your interest—network scanning, vulnerability scanning, or web application scanning.

Complete the Room: Follow the instructions within the chosen room to complete the exercises. Take your time to understand each concept and practice hands-on. Use this opportunity to hone your skills in a safe environment.

Reflect: After completing the room, reflect on what you've learned. Consider the challenges you faced and how you overcame them.

Room Options

Network Scanning

Nmap Live Host Discovery
<https://tryhackme.com/room/nmap01>

In this room, you'll be learning the ins and outs of Nmap, one of the most powerful tool for network discovery. You will have a chance to practice ARP scans, ICMP scans, and TCP/UDP ping scans to identify live hosts on a network. This exercise is perfect for those wanting to sharpen their network scanning skills.

Vulnerability Scanning

OpenVAS Basics
<https://tryhackme.com/room/openvas>

If you're interested in vulnerability scanning, this room provides a great introduction with OpenVAS. In this room, you will learn the basics of threat and vulnerability management by conducting OpenVAS scans. Just as a heads up, this room does require some initial configuration to get OpenVAS properly working but the process is completely laid out for you. As a bonus, this room will also give you a peek into some of the reporting capabilities that OpenVAS has to offer.

Web Exploit Scanning

OWASP Juice Shop
<https://tryhackme.com/room/owaspjuiceshop>

For those looking to delve into web application scanning, the OWASP Juice Shop is a popular starting place. If you're unfamiliar with the OWASP juice shop, it is essentially a web application that has numerous hacking challenges of varying difficulty built into it. It is a popular starting place, and one of my personal favorites. The THM room will walk you through everything, but if you want to explore the juice shop more on your own (and make your way onto the 'secret' scoreboard), you can check out the link below:

<https://juice-shop.herokuapp.com/#/>

Happy hacking, and may the packets be ever in your favor!