

Cyber Security and Digital
Forensics Internship

ASSIGNMENT 9

NMAP

SWASTIK GONDHI

DOON UNIVERSITY

Drive Link -

<https://drive.google.com/drive/folders/1WCK00ki1F3lFPT07y5tdSmeKcrDeWjvs?usp=sharing>

TRYHACKME ROOM – 1

The screenshot shows the completion page for the 'Nmap Live Host Discovery' room on TryHackMe. At the top, a browser window displays the URL 'tryhackme.com/room/nmap01'. The main content area features a large circular icon with a stylized eye and a green checkmark. Below this, a congratulatory message reads: 'Congratulations on completing Nmap Live Host Discovery!!! 🎉'. A row of five dark blue boxes displays the following statistics: 'Points earned' (160), 'Completed tasks' (9), 'Room type' (Walkthrough), 'Difficulty' (Medium), and 'Streak' (1). At the bottom of the main content area, there are two buttons: 'Leave Feedback' and 'Next'. The Windows taskbar at the bottom shows various application icons and the system clock indicating 01:49 PM on 08-05-2025.

tryhackme.com/room/nmap01

Congratulations on completing Nmap Live Host Discovery!!! 🎉

Points earned 🔥 160	Completed tasks ✅ 9	Room type 📖 Walkthrough	Difficulty 📊 Medium	Streak 🔥 1
------------------------	------------------------	----------------------------	------------------------	---------------

[Leave Feedback](#) [Next](#)

01:49 PM 08-05-2025

The screenshot shows the main interface of the 'Nmap Live Host Discovery' room on TryHackMe. The browser window at the top shows the URL 'tryhackme.com/room/nmap01'. The room title 'Nmap Live Host Discovery' is prominently displayed, along with a subtitle: 'Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.' Below the title, a progress bar indicates 'Room completed (100%)'. A list of nine tasks is shown, each with a green checkmark indicating completion: 'Task 1 Introduction', 'Task 2 Subnetworks', 'Task 3 Enumerating targets', 'Task 4 Discovering Live Hosts', 'Task 5 Nmap Host Discovery Using ARP', 'Task 6 Nmap Host Discovery Using ICMP', 'Task 7 Nmap Host Discovery Using TCP and UDP', 'Task 8 Using Reverse DNS Lookup', and 'Task 9 Summary'. At the bottom, a table provides room details: 'Created by' (tryhackme, strategos), 'Room Type' (Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)), 'Users in Room' (204/885), and 'Created' (1304 days ago). The Windows taskbar at the bottom shows various application icons and the system clock indicating 01:50 PM on 08-05-2025.

tryhackme.com/room/nmap01

Nmap Live Host Discovery
Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.

Room completed (100%)

Task 1	Introduction	✓
Task 2	Subnetworks	✓
Task 3	Enumerating targets	✓
Task 4	Discovering Live Hosts	✓
Task 5	Nmap Host Discovery Using ARP	✓
Task 6	Nmap Host Discovery Using ICMP	✓
Task 7	Nmap Host Discovery Using TCP and UDP	✓
Task 8	Using Reverse DNS Lookup	✓
Task 9	Summary	✓


Created by tryhackme strategos	Room Type Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)	Users in Room 204/885	Created 1304 days ago
-----------------------------------	--	--------------------------	--------------------------

01:50 PM 08-05-2025

TRYHACKME ROOM – 2

tryhackme.com/room/furthermap

Woop woop! Your answer is correct



Congratulations on completing Nmap!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
0	0	Walkthrough	Easy	1

Leave Feedback

Next

tryhackme.com/room/furthermap

Nmap

An in depth look at scanning with nmap, a powerful network scanning tool.

50 min

Share your achievement

Start Attackbox

Help

Save Room

19099

Options

Room completed (100%)

- Task 1: Deploy
- Task 2: Introduction
- Task 3: Nmap Switches
- Task 4: Scan Types: Overview
- Task 5: Scan Types: TCP Connect Scans
- Task 6: Scan Types: SYN Scans
- Task 7: Scan Types: UDP Scans
- Task 8: Scan Types: NULL, FIN and Xmas
- Task 9: Scan Types: ICMP Network Scanning
- Task 10: NSE Scripts: Overview
- Task 11: NSE Scripts: Working with the NSE
- Task 12: NSE Scripts: Searching for Scripts
- Task 13: Firewall Evasion
- Task 14: Practical
- Task 15: Conclusion

Created by: DarkStar7471, YairlandOracle, SecurityNomad, arebel

Room Type: Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)

Users in Room: 430,321

Created: 1624 days ago

