Owasp x µLearn Bootcamp Task 3

TryHackMe Report: Nmap

Name: Ajay M Nambiar
Date:7/8/25
Platform: TryHackMe
Room Name: Further Nmap
CTF Type: Learning-based, Network Scanning

Objective : The goal of this room was to explore advanced Nmap features including scanning types, service detection, scripting, and evasion techniques. The challenge helps understand how attackers use different scan methods for enumeration and detection evasion.

Tool Used

- **Nmap** – Network Mapper used for port scanning, OS detection, NSE scripting, and evasion.

Tasks Completed

Task 1: Start the Machine

- Deployed the target machine.
- Confirmed accessibility via IP.

Task 2: Understand Ports

- Learned about port ranges and common ports.
- Answered questions based on Nmap documentation.

Task 3: Basic Nmap Flags

- Identified flags like -sS, -sU, -O, -sV, -A, -T4, -p-, --script.
- Saved scan results using -oN, -oG, and -oA.

Task 4–8: Scan Types

- Performed TCP Connect (-sT) and SYN (-sS) scans.
- Ran FIN (-sF), NULL (-sN), and Xmas (-sX) scans.

- Observed different firewall and OS responses.

Task 9: Ping Sweep

- Used nmap -sn 172.16.0.0/16 to identify live hosts.

Task 10–12: NSE Scripts

- Explored script categories.
- Ran ftp-anon and smb-os-discovery scripts.
- Verified script arguments and output.

Task 13: Firewall Evasion

- Used flags like -f, --data-length, --badsum, and -D RND:10.
- Simulated bypassing firewall rules.

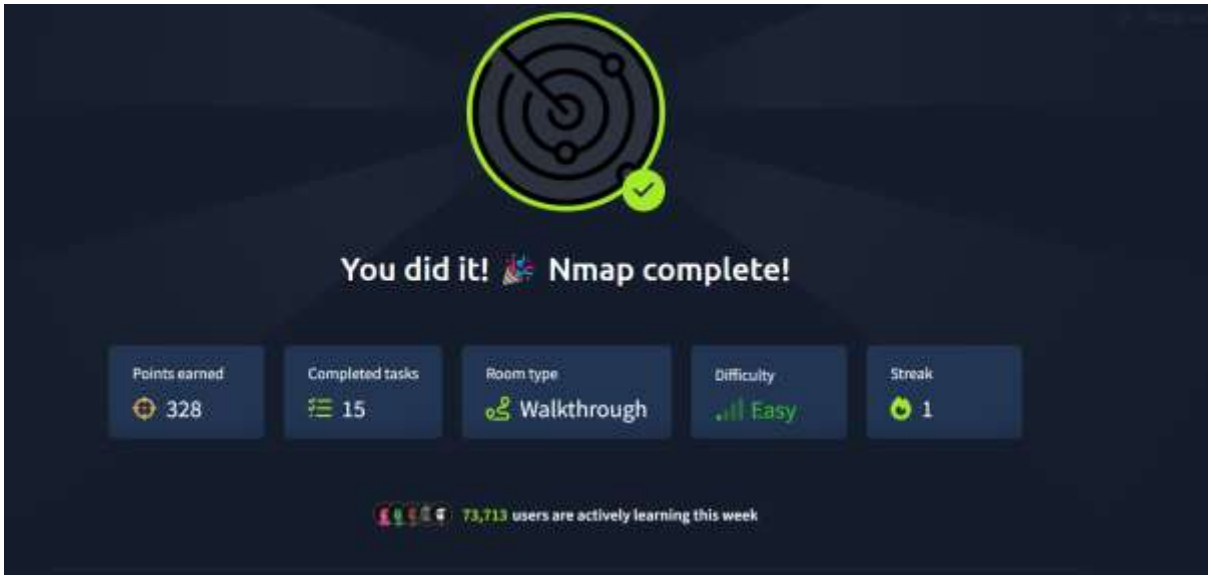
Task 14: Practical Scanning

- Completed hands-on scanning tasks:
    - ICMP disabled host detection
    - Xmas scan analysis
    - SYN scan over 5000 ports
    - Anonymous FTP access verification

Flag

✅ All answers submitted correctly in the room. No explicit flag string provided.

Screenshots



Conclusion

This room deepened my understanding of Nmap's scanning capabilities, including stealth and evasion techniques. Learning to interpret scan results and use scripts improves reconnaissance and vulnerability discovery skills.