Task 1 & 2: Introduction and Nmap Switches

These are introductory tasks.

Task 3 & 4: Scan Types

This section covers the theory behind different Nmap scan types.

- **TCP Connect Scans (-sT):** These are reliable but noisy as they complete the full TCP three-way handshake.
- **SYN "Half-open" Scans (-sS):** These are stealthier as they don't complete the handshake. This is the default scan type for privileged users.
- **UDP Scans (-sU):** Used to find open UDP ports. These are slower than TCP scans.
- **NULL, FIN, and Xmas Scans (-sN, -sF, -sX):** These are used to bypass some firewalls and older intrusion detection systems.They send packets with different TCP flags set.

Task 5: ICMP Network Scanning

This task is about using ICMP to discover live hosts. You'll use the -sn switch to perform a "ping scan" which disables port scanning. This is useful for quickly identifying which hosts are online on a network. You'll be asked to construct a command to perform a ping sweep on a given network range.

Task 6 & 7: NSE (Nmap Scripting Engine)

The NSE allows you to use pre-written or custom scripts to automate a wide range of networking tasks. You'll learn:

- The scripting language used by NSE (Lua).
- How to run scripts from specific categories (e.g., --script=vuln).
- How to search for and use specific scripts, such as ftp-anon.nse to check for anonymous FTP access.

Task 8: Firewall Evasion

This section focuses on techniques to bypass firewalls. You will learn about:

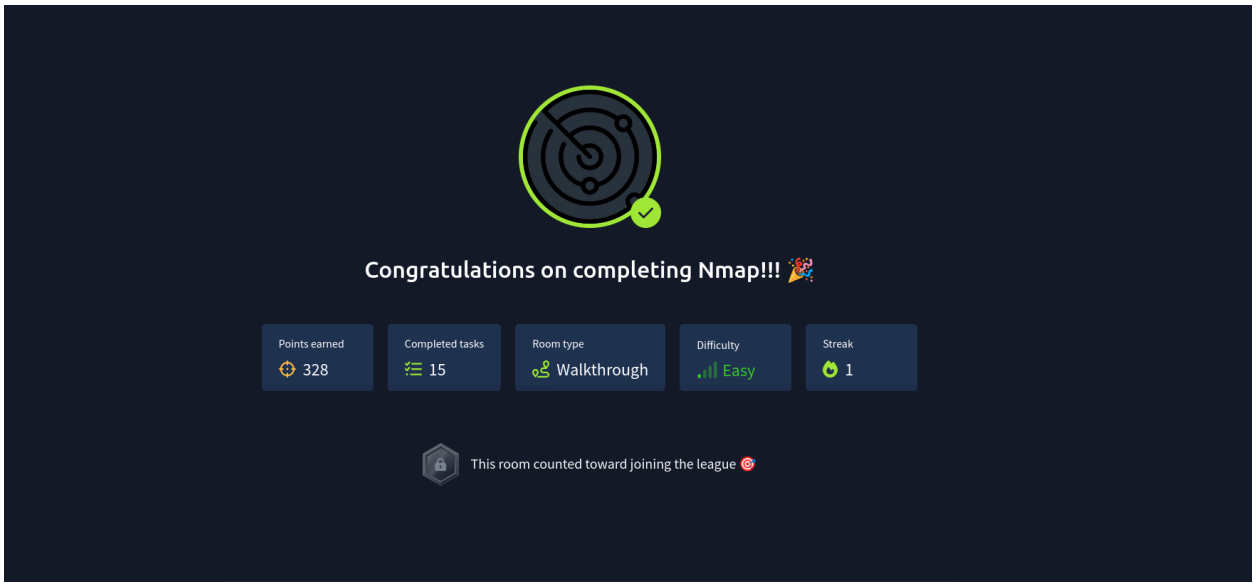
- The -Pn switch to skip the host discovery phase and scan for open ports even if the host doesn't respond to pings.
- Using the --data-length switch to append random data to packets.

Task 9: Practical

This is the hands-on portion where you'll apply what you've learned. You'll be given a target machine and asked to perform a series of scans to answer specific questions. This will involve:

- Performing Xmas and SYN scans to identify open ports.
- Using NSE scripts to find vulnerabilities, such as anonymous FTP login.

- While performing the Xmas scan I identified about 5 open ports.
- The vm was rejecting all of my ping scans and only the Xmas scans worked.



- Profile- https://tryhackme.com/p/Galahad070