TryHackMe Report: *Further Nmap*

Room: https://tryhackme.com/room/furthernmap

Objective

The goal of this room was to explore advanced capabilities of **Nmap**, a powerful network scanning tool. The tasks focused on scan types, firewall evasion, the Nmap Scripting Engine (NSE), and practical reconnaissance against a live host.

Tools & Techniques Used

- **Nmap** for network scanning and enumeration
- **Kali Linux**

Key Tasks & Findings

✔ **Scan Techniques**

- Used various Nmap scan types:
    - **TCP Connect** (-sT)
    - **SYN Scan** (-sS)
    - **UDP Scan** (-sU)
    - **Xmas Scan** (-sX)
    - **Ping Sweep** (-sn)
- Xmas scan returned all **open|filtered** due to lack of response from target (common firewall behavior).
- SYN scan identified 5 open ports: **FTP**, **DNS**, **HTTP**, **MSRPC**, **RDP.**

✔ **NSE Scripts**

- Used --script=ftp-anon on port 21 and confirmed **anonymous login was allowed**.
- Explored categories like vuln, safe, and discovery.

✔ **Firewall Evasion**

- Applied techniques like -Pn, --data-length, and -D to bypass ICMP block and hide scans.

✔ **Packet Capture**

Conclusion

This room provided hands-on experience with advanced Nmap features, including stealth scanning, NSE scripting, and evasion techniques. It demonstrated how to effectively fingerprint and enumerate targets even in the presence of basic firewall protections.