Cyber-Security-Bootcamp-Mulearn-OWASP-Kerala

Task 3 TryHackMe Room Report: Further Nmap

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

Report Prepared by: Yedhukrishna

Overview:

The "Further Nmap" room on TryHackMe is a continuation of Nmap fundamentals, aimed at diving deeper into advanced scanning techniques, scripting, and output manipulation. It teaches how to fine-tune scans for stealth, speed, and specificity, which is crucial for real-world penetration testing and network reconnaissance.

This room is particularly important in a cybersecurity journey as Nmap remains one of the most versatile and widely-used tools in ethical hacking and red teaming.

What I Learned:

1. Advanced Scan Techniques

- **SYN Scans (-sS):** Stealthy and fast; avoids full TCP handshake.
- **UDP Scans (-sU):** Useful for discovering non-TCP services but slower.
- **Scan Timing (-T0 to -T5):** How to control scan aggressiveness.
- **Fragmentation (-f):** Bypasses simple firewalls and IDS.

2. Using NSE Scripts (Nmap Scripting Engine)

- Learned to run scripts with `--script` flag.
- Explored categories like `vuln`, `auth`, `exploit`, and `default`.
- Example: `nmap --script=vuln -sV <target>` to find known vulnerabilities.

3. Output Formats

- Used `-oN`, `-oX`, `-oG`, and `-oA` for output in normal, XML, grepable, and all formats.
- This helps with logging and automation for future reports.

4. Evading Detection

- Used decoy scans (`-D`) and spoofed MAC addresses (`--spoof-mac`) to avoid detection.
- Learned about scan delays (`--scan-delay`) and packet rate limits (`--max-rate`) for stealth.

Practical Takeaways:

- I can now customize Nmap scans depending on the environment — whether it's a hardened system, firewalled network, or stealth operation.

- Nmap scripts can identify vulnerabilities before even launching Metasploit or other tools.
- Output formatting is crucial for long engagements or when automating via Bash or Python.

Challenges Faced:

- UDP scanning was significantly slower and sometimes unreliable, requiring patience and scan tuning.
- Choosing the correct script from the NSE library took trial and error.

Conclusion:

Completing this room has significantly boosted my confidence in using Nmap beyond just simple port scanning. I now understand how to use it efficiently for stealth, speed, and detailed enumeration. These skills will definitely help me in my cybersecurity learning and career.

Submitted by: Yedhukrishna