N-MAP
WALKTHROUGH

Module-9
TRYHACKME

Prepared by: Keerthi TR
Approved by: Ayush Singh

TABLE OF CONTENT

Task 1: Deploy the Virtual Machine

Objective:

- Deploy the virtual machine (VM) for scanning purposes, which will be used in subsequent tasks.

Instructions:

1. Press the green button labeled "Start Machine" to deploy the virtual machine.
2. Note that the machine is intended only for scanning and does not require login or exploitation of vulnerabilities.
3. If using the TryHackMe AttackBox, deploy it separately by clicking the "Start AttackBox" button located at the top right of the interface.

Outcome:

- **The virtual machine has been successfully deployed. No answer input was required for this task.**

Task 2: Introduction to Port Scanning and Enumeration

Objective:

- Understand the significance of port scanning in network reconnaissance and learn the basics of using Nmap as a scanning tool.

Concept Summary:

- Port scanning is crucial for establishing a "landscape" of the target network. It helps identify which services are running and which ports are open, which is necessary for successful exploitation.
- Each computer has 65535 available ports. The first 1024 of these are known as "well-known ports," reserved for specific services (e.g., HTTP on port 80, HTTPS on port 443).
- Nmap is highlighted as the industry standard for port scanning due to its extensive functionalities and powerful scripting engine.

Questions and Answers:

1. What networking constructs are used to direct traffic to the right application on a server?
   - Answer: *****
2. How many of these are available on any network-enabled computer?
   - Answer: *****
3. [Research] How many of these are considered "well-known"?
   - Answer: ****

Conclusion: The first two tasks in the Nmap room provide foundational knowledge essential for any cybersecurity professional. Deploying the VM sets the stage for practical scanning exercises, while understanding port scanning lays the groundwork for effective enumeration. Mastery of these concepts is crucial for successful network assessments and vulnerability exploitation.

Task 3: Nmap Switches

Objective:

- Familiarize yourself with Nmap command switches that control its behavior and output during network scanning.

Instructions:

- Use the Nmap help menu (nmap -h) or the Nmap manual page (man nmap) to answer the questions regarding various switches. Each answer should include the complete switch, including the hyphen (-) at the start.

Conclusion: Task 3 effectively equips users with the necessary knowledge of Nmap command switches, enabling them to customize their scans according to specific requirements. Mastery of these switches is essential for conducting thorough and efficient network reconnaissance.

Nmap Switches and Their Functions:

1. **First switch for 'Syn Scan':**
   - **Switch: -sS**
2. **Switch for a "UDP scan":**
   - **Switch: -sU**
3. **Switch to detect the operating system:**
   - **Switch: -O**
4. **Switch to detect the version of services:**
   - **Switch: -sV**
5. **Increase verbosity level (default):**
   - **Switch: -v**
6. **Set verbosity level to two:**
   - **Switch: -vv**
7. **Switch to save Nmap results in three major formats:**
   - **Switch: -oA**
8. **Switch to save Nmap results in "normal" format:**
   - **Switch: -oN**
9. **Switch to save results in "grepable" format:**
   - **Switch: -oG**
10. **Activate "aggressive" mode (service detection, OS detection, traceroute, script scanning):**
    - **Switch: -A**
11. **Set timing template to level 5 (fastest):**
    - **Switch: -T5**
12. **Tell Nmap to only scan port 80:**
    - **Switch: -p 80**
13. **Tell Nmap to scan ports 1000-1500:**
    - **Switch: -p 1000-1500**
14. **Tell Nmap to scan all ports:**
    - **Switch: -p-**
15. **Activate a script from the Nmap scripting library:**
    - **Switch: --script**
16. **Activate all scripts in the "vuln" category:**
    - **Switch: --script=vuln**

Task 4: Scan Types Overview

Key Scan Types:

1. TCP Connect Scans (-sT):
   - This is the most basic scan type, which attempts to establish a full TCP connection with the target. If a connection is established, the port is considered open. If it fails, the port is either closed or filtered.
2. SYN "Half-open" Scans (-sS):
   - This type of scan sends a SYN packet to the target port. If it receives a SYN-ACK response, the port is open. If an RST packet is received, the port is closed. This scan is stealthier than a TCP connect scan because it does not complete the handshake.
3. UDP Scans (-sU):
   - UDP scans send UDP packets to target ports. If a port is open, there may be no response or an ICMP "port unreachable" message may be sent back if the port is closed. These scans can be more challenging to interpret due to the nature of the UDP protocol.

Less Common Scan Types:

- TCP Null Scans (-sN): Sends a packet with no flags set. Open ports typically ignore the packet, while closed ports respond with an RST.
- TCP FIN Scans (-sF): Sends a FIN packet to the target. Similar to null scans, open ports ignore it, while closed ports respond with an RST.
- TCP Xmas Scans (-sX): Sends a packet with the FIN, URG, and PUSH flags set. Open ports ignore it, while closed ports respond with an RST.

Additional Notes:

- In addition to these scans, ICMP (Internet Control Message Protocol) scanning, often referred to as "ping" scanning, can be used to determine if a host is up and reachable.

Conclusion: Task 4 provides an overview of the various scan types available in Nmap, equipping users with the knowledge needed to choose the appropriate scan method based on their objectives. Familiarity with these scan types enhances the effectiveness of network assessments and vulnerability detection.

Task 5: Scan Types - TCP Connect Scans

Key Concepts:

- TCP Three-Way Handshake:
  - The TCP connection process involves three steps:
    i. SYN: The client (attacking machine) sends a TCP request with the SYN flag set to the target server.
    ii. SYN-ACK: The server responds with a SYN-ACK packet, acknowledging the request.
    iii. ACK: The client completes the handshake by sending an ACK packet back to the server.
- TCP Connect Scan (-sT):
  - A TCP Connect scan utilizes the three-way handshake to assess the state of each specified TCP port on the target server:
    - Open Port: If the port is open, the server responds with a SYN-ACK. Nmap then completes the handshake by sending an ACK.
    - Closed Port: If the port is closed, the server responds with a TCP packet containing the RST (Reset) flag, indicating that the connection does not exist.
    - Filtered Port: If the port is protected by a firewall, Nmap may receive no response, leading to the conclusion that the port is filtered.
- Challenges with Firewalls:
  - Firewalls can be configured to drop incoming packets or respond with RST packets, complicating the ability to accurately determine the state of a port.

Questions and Answers:

1. Which RFC defines the appropriate behavior for the TCP protocol?
   - Answer: ********
2. If a port is closed, which flag should the server send back to indicate this?
   - Answer: ***

Conclusion: Task 5 provides a detailed understanding of TCP Connect scans and the underlying TCP protocol. Familiarity with the three-way handshake and its implications for network scanning enhances the effectiveness of using Nmap for security assessments.

Task 6: Scan Types - SYN Scans

Key Concepts:

- SYN Scans (-sS):
  - SYN scans, often referred to as "Half-open" scans or "Stealth" scans, are a method for scanning TCP ports on a target. Unlike TCP Connect scans, SYN scans do not complete the full three-way handshake.
  - When a SYN scan sends a SYN request to a target port:
    - If the port is open, the server responds with a SYN-ACK. The scanner then sends back an RST packet to avoid completing the handshake.
    - If the port is closed, the server responds with an RST packet.
    - If the port is filtered by a firewall, the SYN packet may be dropped, or the server might respond with an RST.

Advantages of SYN Scans:

1. Bypass Detection: SYN scans can evade older Intrusion Detection Systems (IDS) that are focused on monitoring full handshakes.
2. Minimal Logging: Applications listening on open ports typically do not log SYN requests, which adds to the stealthiness of this scanning method.
3. Speed: SYN scans are generally faster than TCP Connect scans since they do not require establishing a full connection for every port.

Disadvantages of SYN Scans:

1. Sudo Permissions: SYN scans require root privileges in Linux due to the need for raw packet creation.
2. Service Disruption: Unstable services may be negatively affected by SYN scans, potentially impacting production environments.

Overall, the benefits of SYN scans often outweigh their drawbacks, which is why they are the default scan type in Nmap when run with sudo permissions. If run without sudo, Nmap defaults to TCP Connect scans.

Questions and Answers:

1. There are two other names for a SYN scan, what are they?
   - Answer: *********, *******
2. Can Nmap use a SYN scan without sudo permissions (Y/N)?
   - Answer: *

Conclusion: Task 6 emphasizes the significance of SYN scans in network security assessments. By understanding their mechanics and advantages, users can leverage SYN scans effectively while being mindful of the permissions required for their execution.

Task 7: Scan Types - UDP Scans

K**ey Concepts:**

- UDP Scans (-sU):
  - Unlike TCP, which establishes a connection through a three-way handshake, UDP connections are stateless. This means that packets are sent to a target port without expecting a response.
  - When performing a UDP scan:
    - If a packet is sent to an open UDP port, there is typically no response. Nmap labels these ports as open|filtered, indicating uncertainty about whether the port is truly open or if it is being protected by a firewall.
    - If a packet is sent to a closed UDP port, the target responds with an ICMP (ping) packet indicating that the port is unreachable. Nmap then marks these ports as closed.

Challenges with UDP Scans:

- Identifying open UDP ports can be significantly slower than TCP scans. Scanning the first 1,000 UDP ports can take around 20 minutes due to the nature of the protocol.
- To optimize scan times, it is advisable to use the --top-ports <number> option with Nmap, which scans only the most commonly used UDP ports. For example, running:

fig : 7.1 Port scan

```
nmap -sU --top-ports 20 <target>
```

would scan the top 20 UDP ports, resulting in a more efficient scanning process.

Scanning Techniques:

- Nmap typically sends empty UDP requests. However, for well-known services, it may send a protocol-specific payload to increase the likelihood of receiving a response, which can provide more accurate results.

Questions and Answers:

1. If a UDP port doesn't respond to an Nmap scan, what will it be marked as?
   - Answer: **********
2. When a UDP port is closed, by convention, the target should send back a "port unreachable" message. Which protocol would it use to do so?
   - Answer: ****

Conclusion: Task 7 highlights the complexities involved in scanning UDP ports. The stateless nature of UDP makes it challenging to determine the state of ports, requiring additional strategies to optimize the scanning process. Understanding how Nmap handles UDP scans is vital for effective network security assessments.

Task 8: Scan Types - NULL, FIN, and Xmas

Key Concepts:

- NULL Scans (-sN):
  - A NULL scan sends a TCP request with no flags set at all. According to the relevant RFC, if a port is closed, the target should respond with a RST (Reset) packet.
- FIN Scans (-sF):
  - FIN scans function similarly to NULL scans but send a packet with the FIN flag set, which is typically used to gracefully close an existing connection. Nmap expects a RST response if the port is closed.
- Xmas Scans (-sX):
  - Xmas scans send a malformed TCP packet with the PSH, URG, and FIN flags set. The name derives from the packet's appearance resembling a blinking Christmas tree in tools like Wireshark. As with the other two scans, Nmap expects a RST response for closed ports.

Response Behavior:

- For all three scans:
  - If the port is open, there is typically no response to the malformed packet.
  - If the port is closed, the target responds with a RST packet.
  - If the port is filtered, an ICMP unreachable packet may be received, indicating that the firewall is blocking the scan.

Challenges and Limitations:

- While RFC 793 dictates that hosts should respond appropriately to these scan types, some operating systems, particularly Microsoft Windows and certain Cisco devices, are known to respond with a RST to all malformed packets. This results in all ports appearing closed, which can lead to inaccurate results.
- The primary advantage of these scans is firewall evasion, as many firewalls are configured to block packets with the SYN flag set, thereby allowing scans that do not initiate a new connection to bypass these filters. However, modern Intrusion Detection Systems (IDS) may still detect these scans.

Questions and Answers:

1. Which of the three shown scan types uses the URG flag?
   - Answer: ****
2. Why are NULL, FIN, and Xmas scans generally used?
   - Answer: **********
3. Which common OS may respond to a NULL, FIN, or Xmas scan with a RST for every port?
   - Answer: **********

Conclusion: Task 8 underscores the stealth capabilities of NULL, FIN, and Xmas scans in the context of network security assessments. While they offer a means of evading certain firewall configurations, their reliability can be compromised by the behavior of specific operating systems. Understanding these scan types is crucial for effectively navigating network security environments.

Task 9: Scan Types - ICMP Network Scanning

Key Concepts:

- Objective of ICMP Network Scanning:
  - In a black box penetration test, the initial goal is to determine which IP addresses in a network contain active hosts. This process is known as mapping the network structure.
- Ping Sweep:
  - A ping sweep is performed by sending ICMP packets to each IP address within a specified range. When a response is received, the corresponding IP address is marked as alive.
- Nmap Command for Ping Sweep:
  - The Nmap command for executing a ping sweep is constructed using the -sn switch, which instructs Nmap to skip port scanning and rely primarily on ICMP echo requests and ARP requests on local networks.
  - Example commands for a ping sweep include:
    - Using a range: nmap -sn 192.168.0.1-254
    - Using CIDR notation: nmap -sn 192.168.0.0/24
- Additional Requests:
  - In addition to ICMP echo requests, the -sn switch causes Nmap to send:
    - A TCP SYN packet to port 443
    - A TCP ACK (or TCP SYN if not run as root) packet to port 80

Questions and Answers:

1. How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)
   - Answer: **********

Conclusion: Task 9 highlights the utility of ICMP Network Scanning in the reconnaissance phase of penetration testing. By employing ping sweeps, security professionals can quickly identify active hosts and establish a foundational understanding of the network structure.

Task 10: NSE Scripts Overview

Key Concepts:

- Nmap Scripting Engine (NSE):
  - The NSE is a feature that allows users to write scripts in the Lua programming language to automate various tasks in Nmap, enhancing its capabilities beyond basic scanning.
- Uses of NSE Scripts:
  - NSE scripts can perform a wide range of functions, including scanning for vulnerabilities, automating exploits, and conducting reconnaissance.
- Categories of NSE Scripts:
  - The NSE script library is extensive and categorized for different use cases. Some of the useful categories include:
    - safe: Scripts that won't affect the target.
    - intrusive: Scripts that are likely to affect the target; should be avoided in production environments.
    - vuln: Scripts designed to scan for vulnerabilities.
    - exploit: Scripts that attempt to exploit a discovered vulnerability.
    - auth: Scripts that attempt to bypass authentication for running services (e.g., logging into an FTP server anonymously).
    - brute: Scripts that attempt to brute-force credentials for running services.
    - discovery: Scripts that query running services for further information about the network (e.g., querying an SNMP server).

Questions and Answers:

1. What language are NSE scripts written in?
   - Answer: Lua
2. Which category of scripts would be a very bad idea to run in a production environment?
   - Answer: Intrusive

Conclusion: Task 10 emphasizes the significance of the Nmap Scripting Engine in enhancing the functionality of Nmap for various tasks, especially in penetration testing and network reconnaissance. Understanding the different script categories and their potential impact on target environments is crucial for responsible usage.

Task 11: NSE Scripts Working with the NSE

Key Concepts:

- Activating NSE Scripts:
  - Scripts can be activated using the --script switch. For example, using --script=vuln runs all applicable scripts from the vuln category. Similarly, --script=safe runs safe scripts.
  - To run a specific script, use the syntax --script=<script-name>. For example, --script=http-fileupload-exploiter.
  - Multiple scripts can be executed simultaneously by separating them with commas: --script=smb-enum-users,smb-enum-shares.

Questions and Answers:

1. What optional argument can the ftp-anon.nse script take?
   - Answer: maxlist

Conclusion: Task 11 emphasizes the versatility of the Nmap Scripting Engine, highlighting how to effectively activate and manage scripts to enhance network scanning and vulnerability assessment. Understanding how to pass arguments and access help information can significantly improve the efficiency and effectiveness of using Nmap in security assessments.

- Passing Arguments to Scripts:

Some scripts require additional arguments. This can be done using the --script-argsoption. For example:

```
nmap -p 80 --script http-put --script-args http-put.url='/dav/shell.php',http-put.file='./shell.php'
```

- In this command, the arguments are separated by commas and connected to the script with periods.

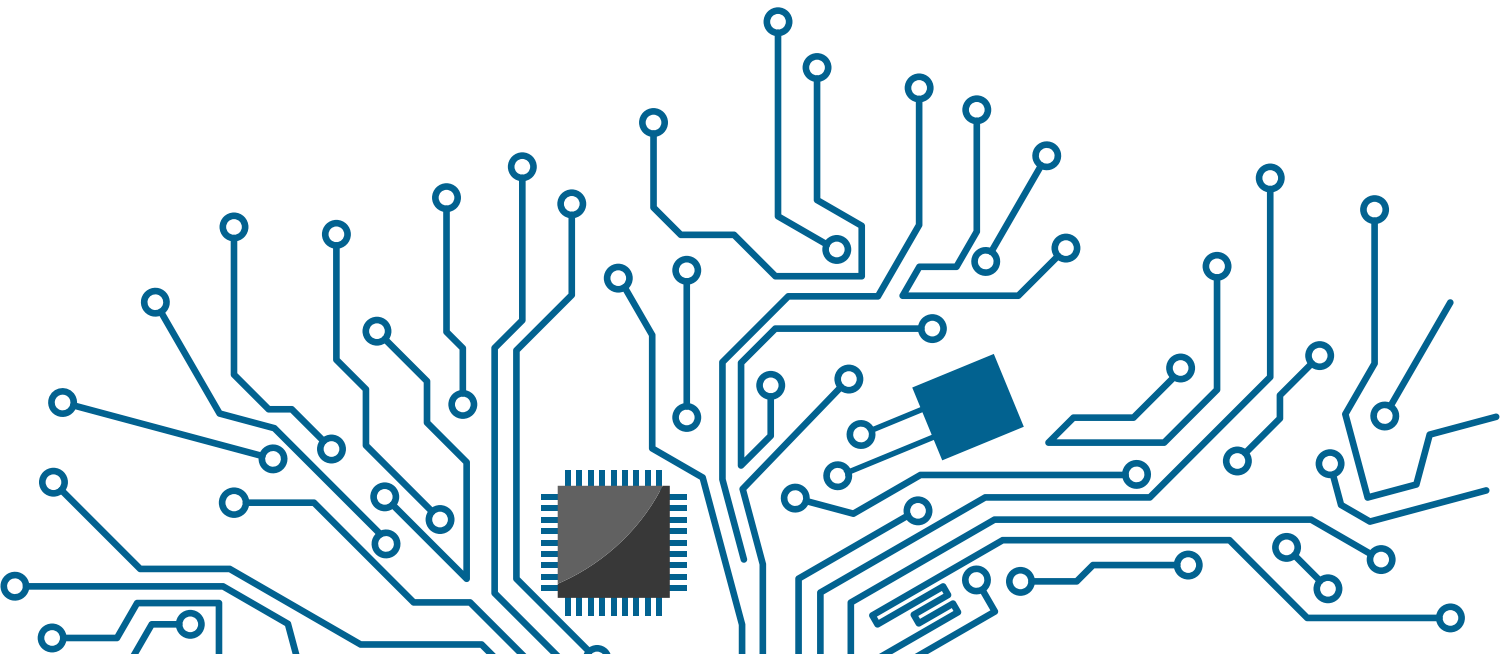
- Accessing Help for Scripts:

Each Nmap script has a built-in help menu, which can be accessed using:

css

```
nmap --script-help <script-name>
```

- This help menu provides basic information about the script's function and usage.



Task 12: NSE Scripts Searching for Scripts

Key Concepts:

- **Locating Scripts:**
  - Nmap scripts are typically stored in the directory: /usr/share/nmap/scripts.
  - To find scripts, you can use:
    i. The script.db file: This file contains a list of available scripts. You can search for scripts using:
    ii. **grep "smb" /usr/share/nmap/scripts/script.db**
    iii. The ls command: This command allows you to list scripts directly. For example, to find SMB-related scripts:
    iv. **ls -l /usr/share/nmap/scripts/*smb***

- **Searching for Categories:**
  - You can also search for specific categories of scripts in the same way:
  - **grep "safe" /usr/share/nmap/scripts/script.db**

- **Installing New Scripts:**
  - If a script is missing from your local directory, you can update Nmap with:
  - **sudo apt update && sudo apt install nmap**
  - Alternatively, download a specific script manually:
  - **sudo wget -O /usr/share/nmap/scripts/<script-name>.nse https://svn.nmap.org/nmap/scripts/<script-name>.nse**
  - After adding a new script, run:
  - **nmap --script-updatedb**
  - This updates the script.db to recognize the new script.

Questions and Answers:

1. What is the filename of the script which determines the underlying OS of the SMB server?
    - Answer: smb-os-discovery.nse
2. Read through this script. What does it depend on?
    - Answer: smb-brute

Conclusion: Task 12 emphasizes the importance of effectively locating and managing NSE scripts to enhance the functionality of Nmap. Understanding how to search for existing scripts and install new ones is crucial for conducting thorough and effective network scans.

Task 13: Firewall Evasion

Key Concepts:

- ICMP Blocking:
- Default Windows firewalls block all ICMP packets, which poses a challenge for network scanning because:
  - Nmap uses ICMP echo requests (ping) to check if a host is alive before scanning.
  - If a host is perceived as dead, Nmap will skip scanning it entirely.
- Bypassing ICMP Block:
- To bypass this configuration, use the -Pn switch:
  - -Pn: Treats all hosts as alive, skipping the ping check. This can prolong the scanning process if the host is actually dead, as Nmap will still attempt to scan all specified ports.
- ARP Requests:
- If directly on a local network, Nmap can utilize ARP requests to determine host activity, which is not affected by ICMP blocking.

U**seful Nmap Switches for Firewall Evasion:**

1. -f:
   - Fragments packets into smaller pieces to reduce the likelihood of detection by firewalls or IDS.
2. --mtu <number>:
   - Allows you to set a specific maximum transmission unit size for packets. Must be a multiple of 8.
3. --scan-delay <time>ms:
   - Introduces a delay between packets, useful for managing unstable networks and evading time-based triggers in firewalls or IDS.
4. --badsum:
   - Generates packets with invalid checksums. Real TCP/IP stacks would drop these packets, but some firewalls may respond without checking the checksum, helping to identify their presence.

Questions and Answers:

1. Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?
   - Answer: ICMP
2. Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?
   - Answer: --data-length

Conclusion: Task 13 highlights the importance of understanding firewall configurations and provides Nmap options that can help evade detection. Mastery of these techniques can greatly enhance scanning effectiveness in restricted environments.

Task 14: Practical Task Overview:

In this task, we applied various scanning techniques learned in previous tasks to gather information about a target machine. The focus was on determining responsiveness to ICMP, scanning ports, and exploring FTP service capabilities.

Questions and Answers:

1. Does the target IP respond to ICMP echo (ping) requests (Y/N)?
   - Answer: N
   - Explanation: The target machine does not respond to ICMP echo requests, indicating that the host may have ICMP blocking configured (common in firewalls).
2. Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered?
   - Answer: 999
   - Explanation: All 999 ports were shown as open or filtered, suggesting that the response to the Xmas scan was consistent with firewall rules, leading to no clear indication of port statuses.
3. There is a reason given for this -- what is it?
   - Answer: No Response
   - Explanation: The lack of response to the Xmas scan means that the ports could either be filtered by a firewall or simply not responding to the malformed packets used in the Xmas scan.
4. Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?
   - Answer: 5
   - Explanation: The TCP SYN scan revealed 5 ports as open, which indicates active services listening on those ports.
5. Deploy the ftp-anon script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)
   - Answer: Y
   - Explanation: The FTP server allowed an anonymous login, confirming that the server is configured to permit unauthenticated access.

Practical Insights:

- ICMP Responses: The absence of ICMP responses highlighted the importance of recognizing firewall configurations in a network scanning context.
- Xmas Scan Findings: The use of Xmas scans can be misleading in determining open ports, particularly when firewalls are in place that may block or drop packets.
- SYN Scan Efficiency: The SYN scan proved effective in identifying open ports compared to the more ambiguous Xmas scan results.
- FTP Service Access: The successful anonymous login to the FTP server suggests potential avenues for further exploration, such as examining available files or services.

PROOF OF CONCEPT [POC]

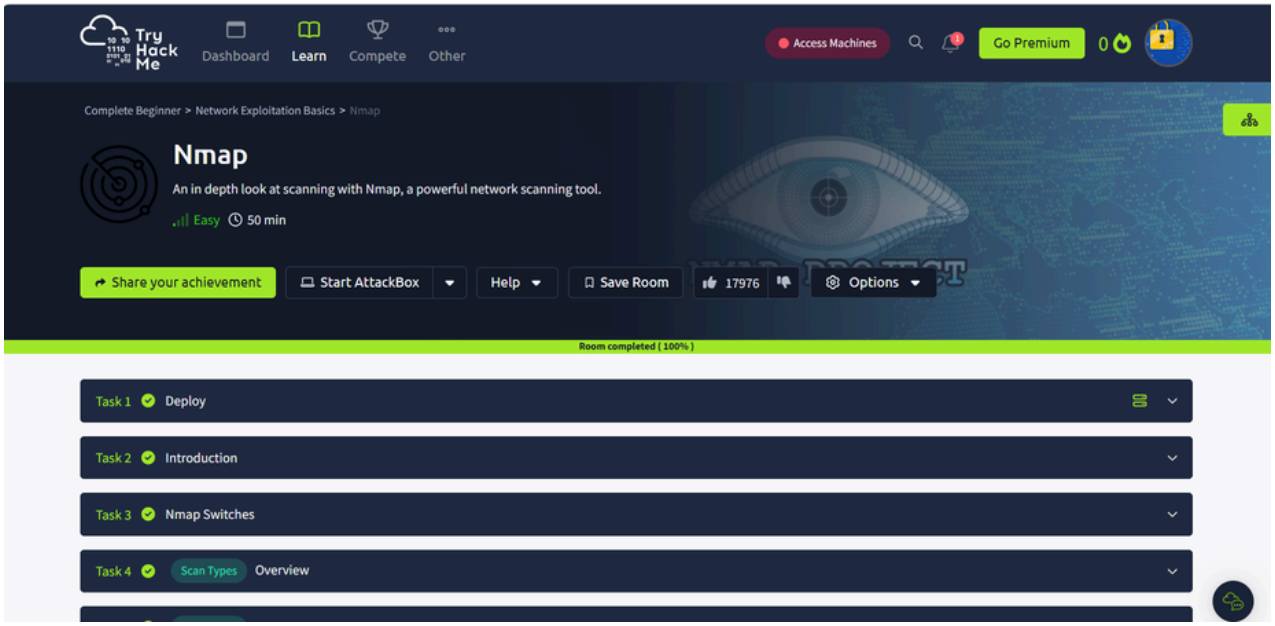


FIG: 15.1 Completion of room