Nmap

Introduction

Nmap (Network Mapper) is a powerful and widely used open-source tool for network scanning, discovery, and security auditing. It plays a significant role in penetration testing by helping security professionals identify open ports, running services, and possible vulnerabilities in a target system.

The Further Nmap TryHackMe room is designed to extend the learner's knowledge beyond the basics of Nmap, introducing advanced scanning techniques, the use of the Nmap Scripting Engine (NSE), and firewall evasion methods. This report documents the completion of each task, explaining the relevant concepts, command usage, and key observations.

Objective

The main objective of this lab exercise is to explore the advanced functionalities of Nmap. The specific goals include:

- Understanding and applying advanced scan switches.
- Learning different types of scan techniques (TCP, SYN, UDP, etc.).
- Using the Nmap Scripting Engine for automation, enumeration, and vulnerability detection.
- Experimenting with firewall evasion methods such as decoys, fragmentation, and IP spoofing.
- Gaining practical experience in applying these techniques in a simulated penetration testing scenario.

Summary of Tasks

Task 1–2: Setup and Introduction

The initial tasks focus on deploying the lab environment and reviewing the purpose of Nmap.

Task 3: Advanced Nmap Switches

This task introduces important switches, such as:

- `-p` → Specify ports for scanning.
- `-A` → Perform aggressive scanning (includes service and OS detection).
- `-O` → Conduct OS fingerprinting.

Task 4–9: Scan Types

- Task 4: Overview of various scan techniques.
- Task 5: TCP Connect Scan – establishes a full TCP handshake, accurate but easily detectable.
- Task 6: SYN Scan – initiates only SYN packets without completing the handshake, offering stealth.
- Task 7: UDP Scan – sends empty datagrams to detect open UDP ports; slower due to retries and lack of reliable responses.
- Task 8: NULL, FIN, and Xmas Scans – manipulate TCP flags to bypass basic firewall detection.
- Task 9: ICMP Scanning – identifies live hosts without focusing on ports.

Task 10–12: Nmap Scripting Engine (NSE)

- Task 10: Introduction to NSE and its automation capabilities.
- Task 11: Running scripts using the --script=<name> option.
- Task 12: Searching for scripts by keyword or category.

Task 13: Firewall Evasion

Explores evasion strategies such as packet fragmentation, using decoy addresses, and spoofing IPs to avoid detection.

Task 14: Practical Exercise

Applies all previously learned techniques in a simulated penetration testing scenario to reinforce hands-on skills.

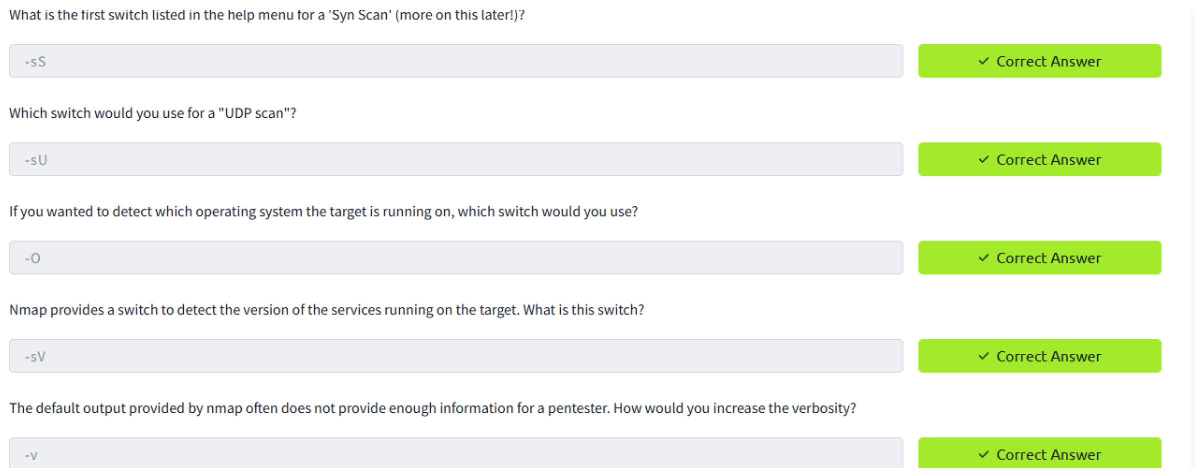
Task 15: Conclusion

Summarizes the learnings and emphasizes the importance of continuous practice and referring to Nmap’s documentation for mastering advanced features.

Conclusion

The Further Nmap room provides a transition from basic to advanced usage of Nmap, enabling learners to develop penetration testing skills. By combining scan types, scripting capabilities, and evasion strategies, Nmap proves to be a versatile tool for reconnaissance, enumeration, and vulnerability assessment. This hands-on experience builds confidence in using Nmap effectively for real-world security testing.

Screenshots



What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

-sS

Which switch would you use for a "UDP scan"?

-sU

If you wanted to detect which operating system the target is running on, which switch would you use?

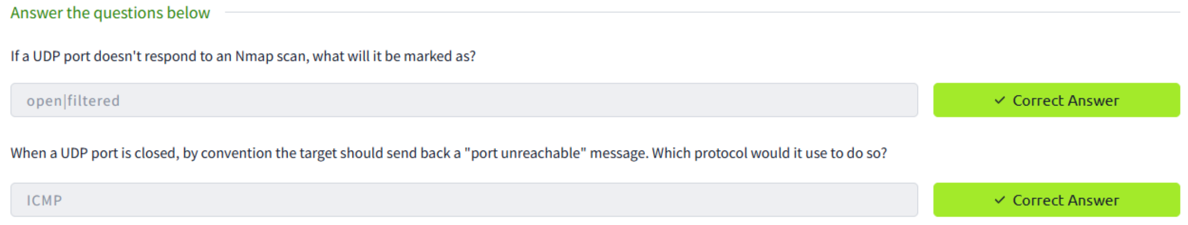
-O

Nmap provides a switch to detect the version of the services running on the target. What is this switch?

-sV

The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

-v



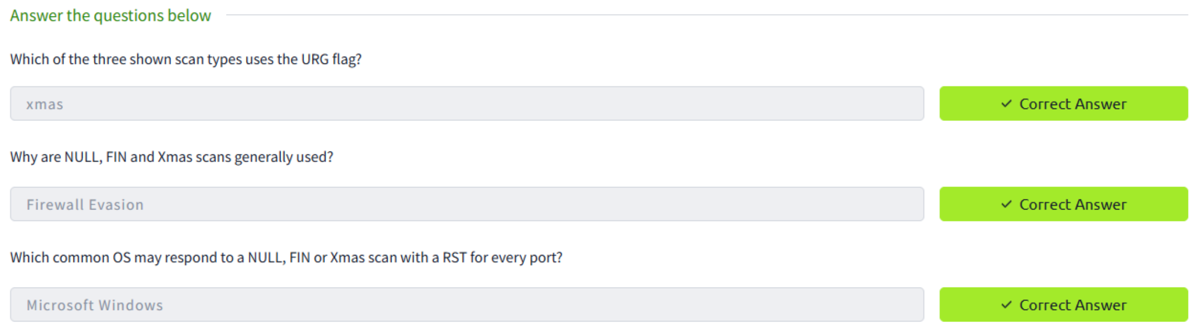
Answer the questions below

If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

open|filtered

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?

ICMP



Answer the questions below

Which of the three shown scan types uses the URG flag?

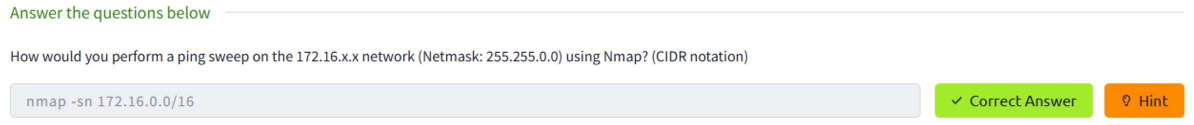
xmas

Why are NULL, FIN and Xmas scans generally used?

Firewall Evasion

Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

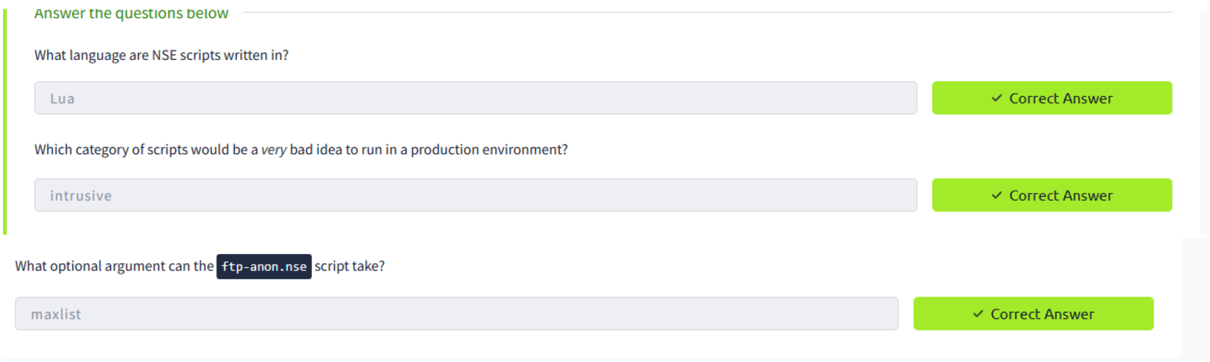
Microsoft Windows



Answer the questions below

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

nmap -sn 172.16.0.0/16



Answer the questions below

What language are NSE scripts written in?

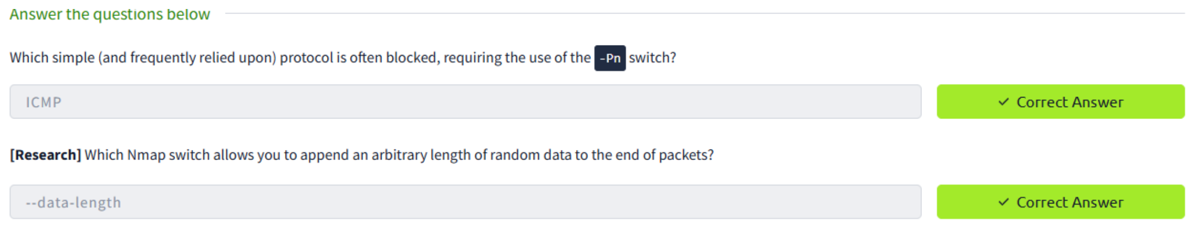
Lua

Which category of scripts would be a *very* bad idea to run in a production environment?

intrusive

What optional argument can the `ftp-anon.nse` script take?

maxlist



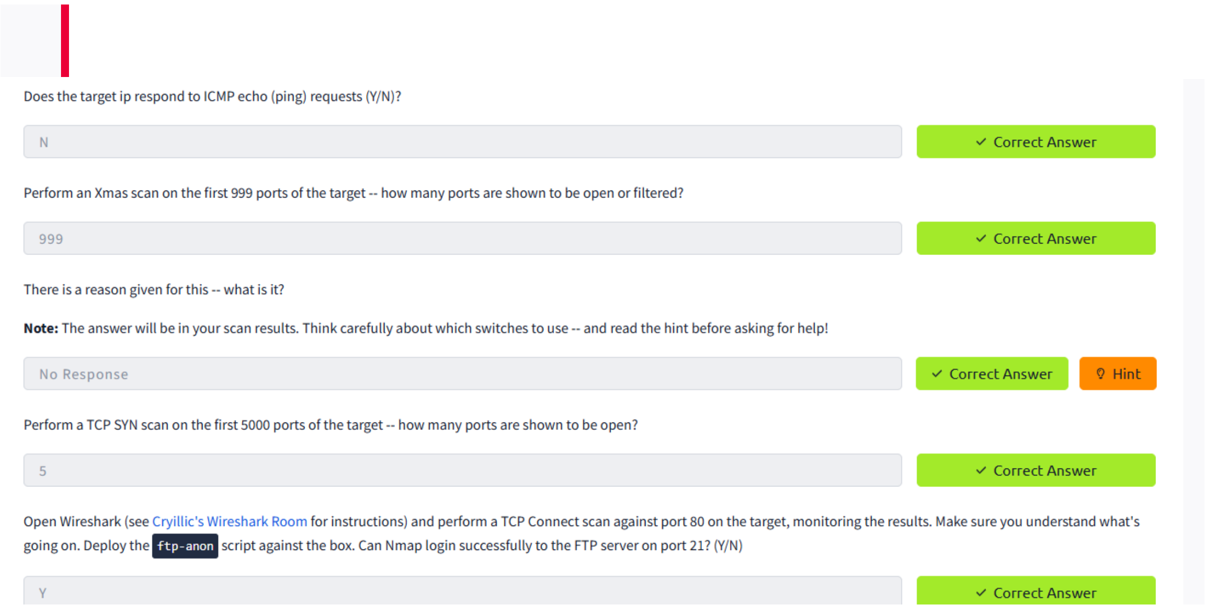
Answer the questions below

Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the `-Pn` switch?

ICMP

[Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

--data-length



Does the target ip respond to ICMP echo (ping) requests (Y/N)?

N

Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered?

999

There is a reason given for this -- what is it?

Note: The answer will be in your scan results. Think carefully about which switches to use -- and read the hint before asking for help!

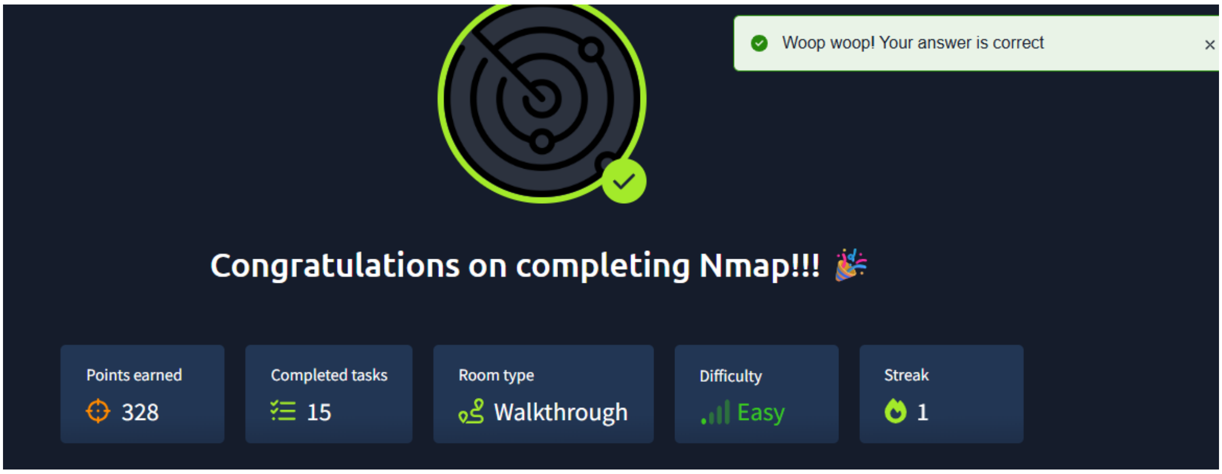
No Response

Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?

5

Open Wireshark (see Cryillic's Wireshark Room for instructions) and perform a TCP Connect scan against port 80 on the target, monitoring the results. Make sure you understand what's going on. Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Y



Woop woop! Your answer is correct

Congratulations on completing Nmap!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
328	15	Walkthrough	Easy	1