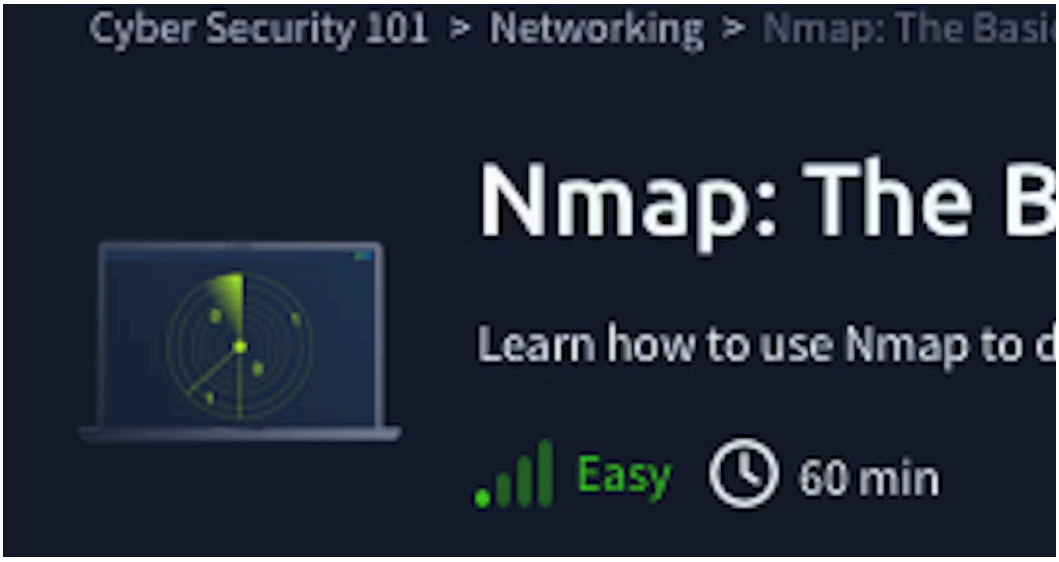
Follow



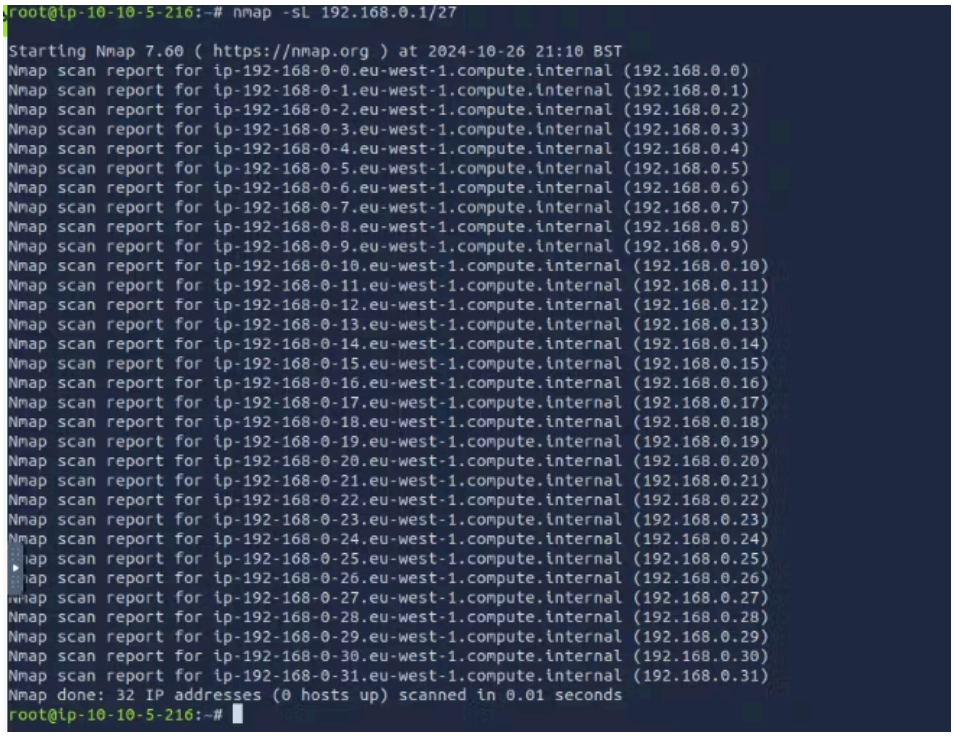
Networking: Nmap: The Basics (TryHackMe)

J3bitok

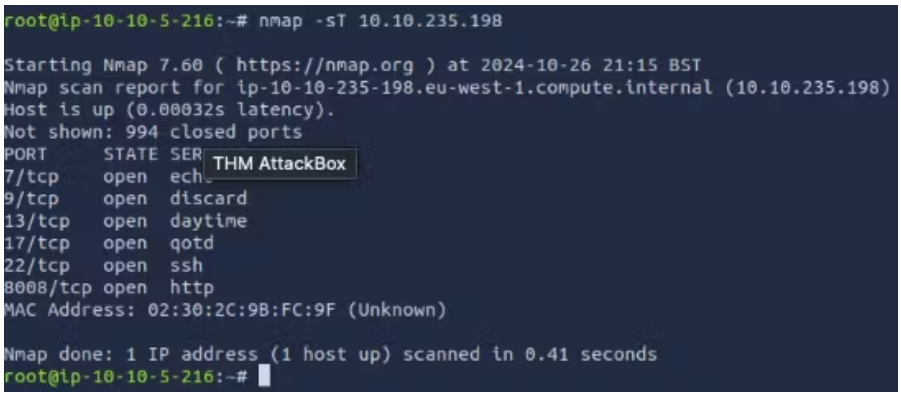
Oct 27, 2024 · 2 min read

In this article, I will write a write-up for Nmap: The Basics that covers Host Discovery: Who is Online, Port Scanning: Who is Listening, Version Detection: Extract More Information, Timing: How Fast is Fast, and Output: Controlling What You See.

1. What is the last IP address that will be scanned when your scan target is `192.168.0.1/27`? `192.168.0.31`



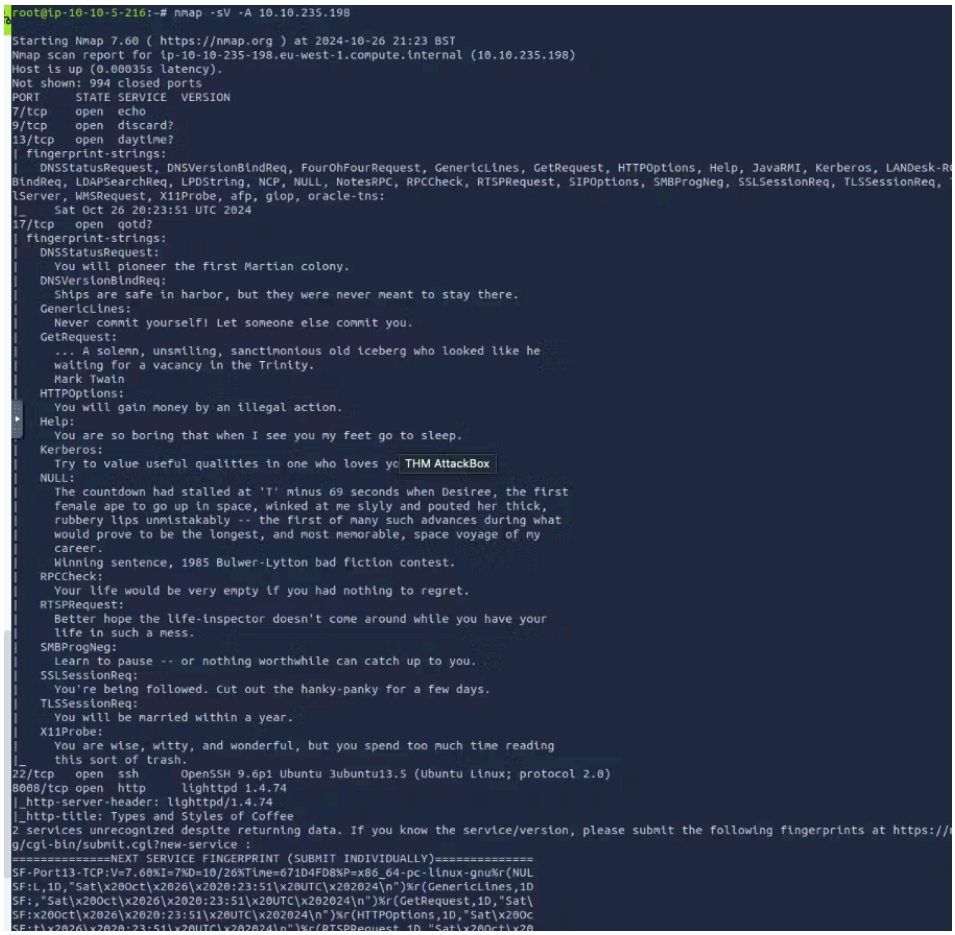
2. How many TCP ports are open on the target system at `10.10.235.198` ? 6

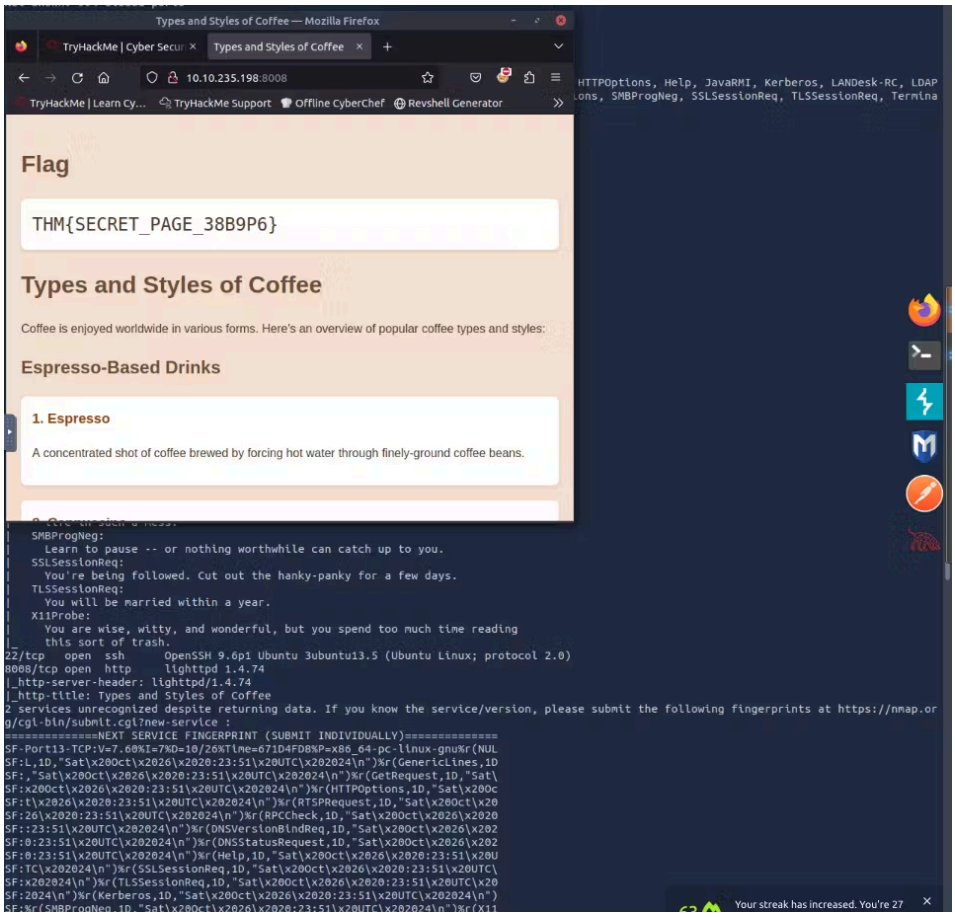


3. Find the listening web server on `10.10.235.198` and access it with your browser. What is the flag that appears on its main page?

   `THM{SECRET_PAGE_38B9P6}`

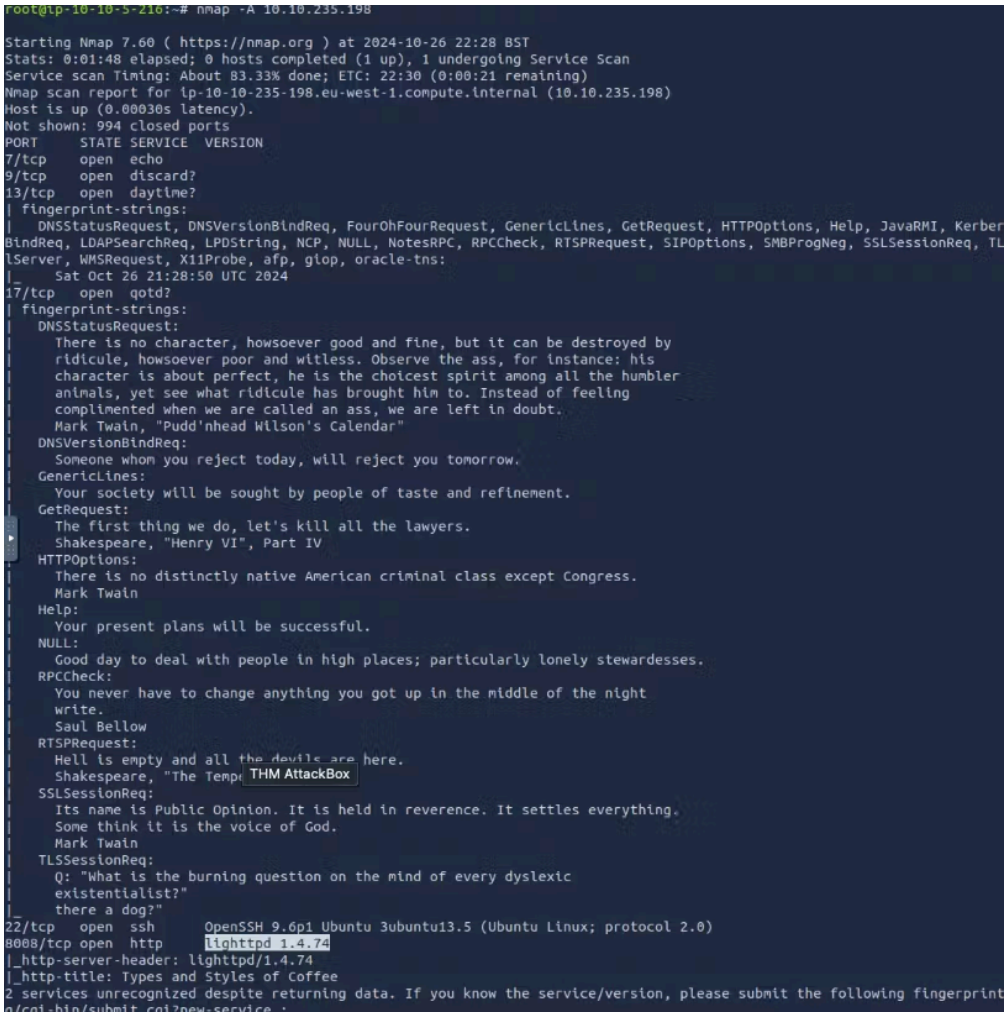
   to start there's a hint on the question that you should access via `http://ip_address:port_number` . Remember the computer has 65535 ports so I tried to use common ports like 80, 8080, etc, and the browser didn't open. I ran a command `nmap -sV -A 10.10.235.198` that gave us a comprehensive overview of our target machine IP which included open ports, 8008 showed `8008/tcp open http lighttpd/1.4.74` . On opening the browser `http://ip_address:8008` I got the flag





4. What is the name and detected version of the web server running on `10.10.235.198`? `lighttpd 1.4.74`

running `nmap -A ip_address` brings it up notice that our attack machine uses `lighttpd` and not the web servers like `nginx` so that a hint too



5. What is the non-numeric equivalent of `-T4` ? `-T aggressive`
6. What option must you add to your `nmap` command to enable debugging? `-d`
7. What kind of scan will Nmap use if you run `nmap MACHINE_IP` with local user privileges? `Connect Scan`

Thank you for reading my article. Please leave any questions or comments on improving my learning journey and the THM challenges. We can also connect more on **LinkedIn** or **X.**

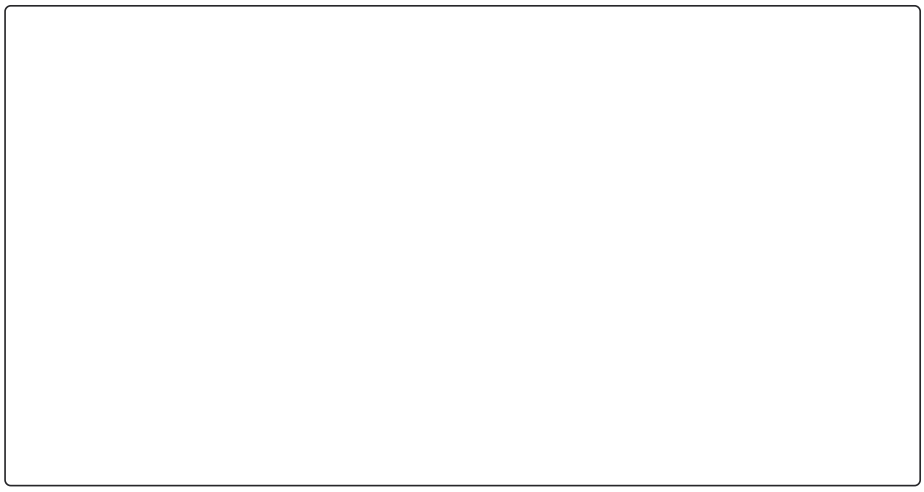
Subscribe to our newsletter

Read articles from **Sharon Jebitok** directly inside your inbox. Subscribe to the newsletter, and don't miss out.

nmap networking Write Up tryhackme

MORE ARTICLES

J3bitok



The Advent of Cyber: Day 16: Azure - Wareville's Key Vault grew three sizes that day. (TryHackMe)

In this article, we'll cover Azure - Wareville's Key Vault, which grew three sizes that day. The wri...

J3bitok

The Advent of Cyber: Day 10: Phishing - He had a brain full of macros, and had shells in his soul. (...

In this article, we'll cover Phishing - He had a brain full of macros and had shells in his soul wri...

The Advent of Cyber: Day 12: Web timing attacks: If I can't steal their money, I'll steal their joy!...

In this article, we'll cover Web Timing Attacks Attacks—If you'd like to WPA, press the star key! wr...