Writeup: Anonymous - HackerDNA Cybersecurity Lab

Introduction

Anonymous FTP access is a common misconfiguration that has plagued servers for decades, allowing unauthenticated users to browse and download files—often exposing sensitive data like configs, backups, or in this case, flags. The *Anonymous* lab from HackerDNA spotlights this classic vulnerability, tasking you with enumerating a target server and exploiting an open FTP port to retrieve a hidden file. Hosted at HackerDNA, this easy challenge (ideal for beginners) simulates a basic web/FTP setup on a fictional system, emphasizing reconnaissance over complex exploits.

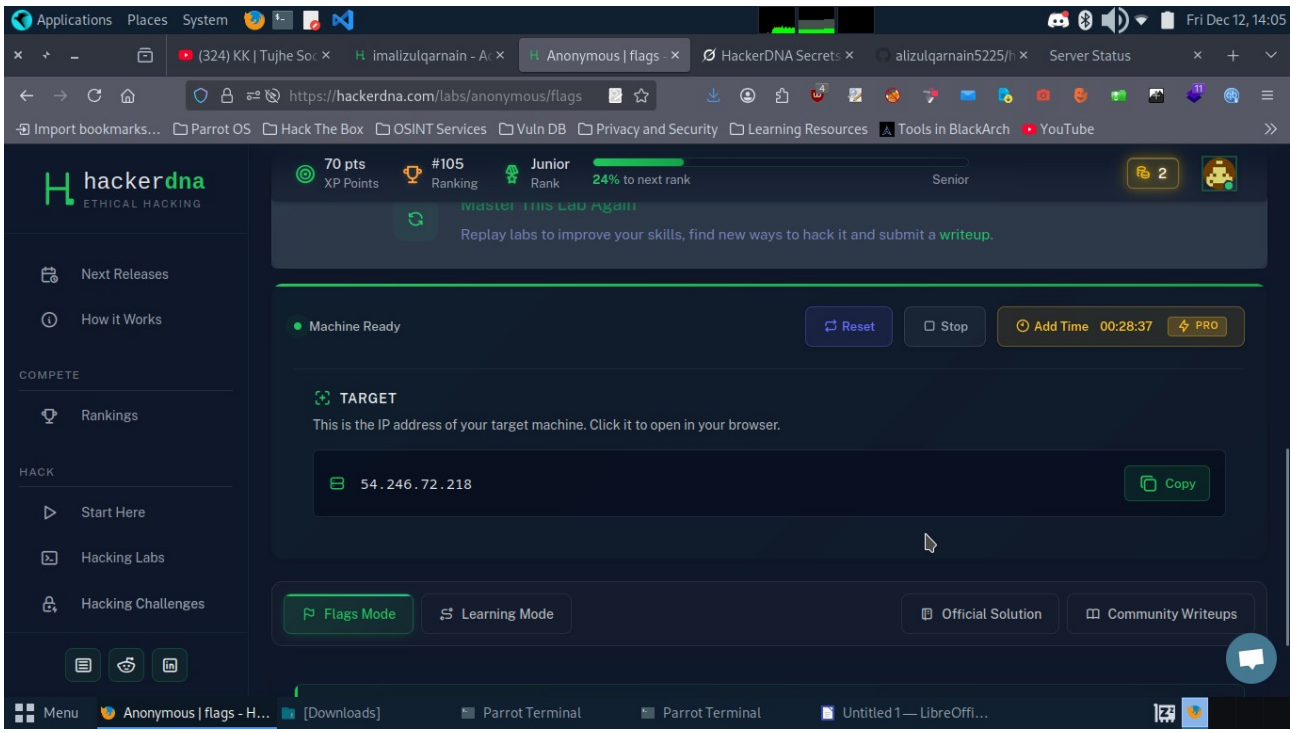
Objective: Launch the lab instance, perform port scanning to identify services, probe the FTP server for weaknesses, and use anonymous credentials to access and download flag.txt. This exercise underscores the risks of default or lax server configs in real-world scenarios.

Difficulty: Easy
Points: 10 (1 flag worth +10 pts)
Success Rate: ~71% (as of December 2025)
Estimated Time: 5-10 minutes (plus 1-2 min setup)
Skills Tested: Port scanning with Nmap, service enumeration, FTP anonymous login, basic network reconnaissance

HackerDNA's private instances ensure a safe, ephemeral environment with no external impact—perfect for honing ethical hacking fundamentals. It's a quick dive into why "anonymous" should never be synonymous with "secure."

Lab Setup

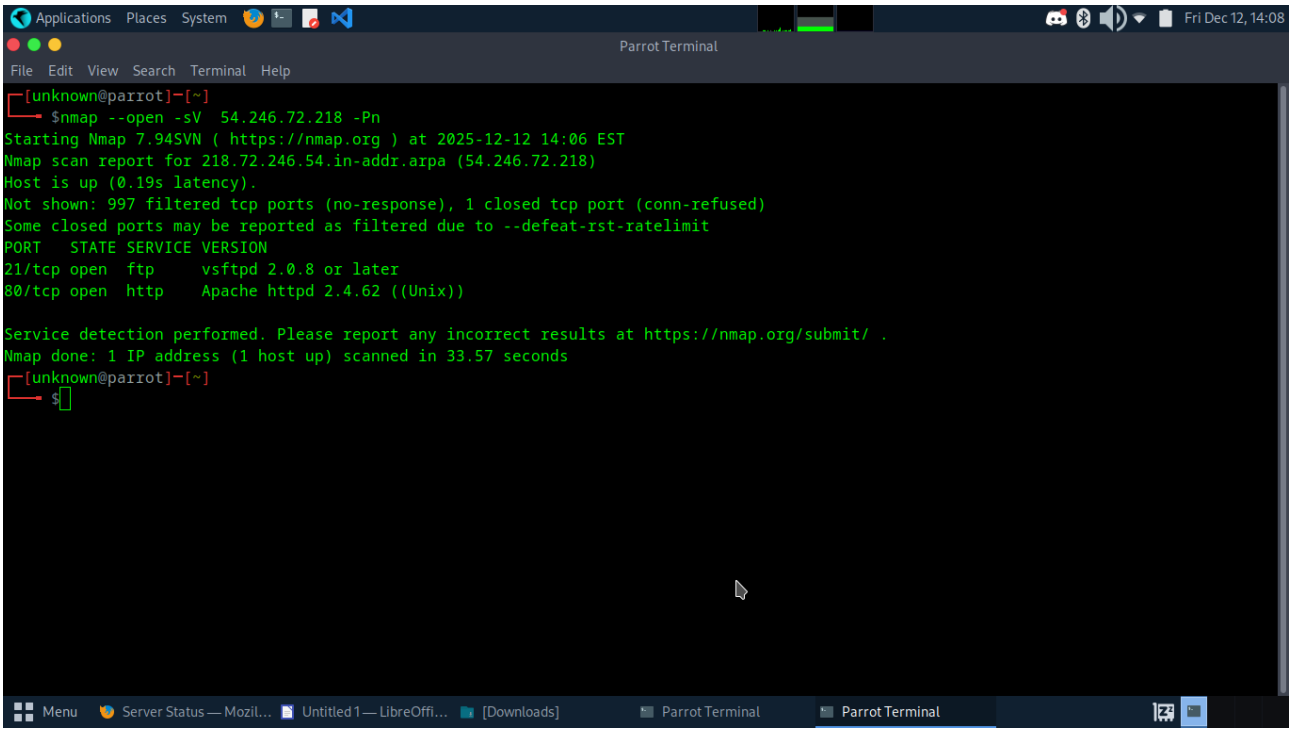
1. **Access the Lab**: Log into HackerDNA Labs and search for "Anonymous." Click "Start Lab" to provision your dedicated VM (ready in ~1-2 minutes). This spins up an isolated server with pre-configured tools like a terminal and browser.
2. **Retrieve the Target IP**: The dashboard displays the target IP (e.g., 54.246.72.218). Copy it—this is your attack surface. Keep the dashboard handy for submitting the flag.



Step 1: Initial Port Scanning

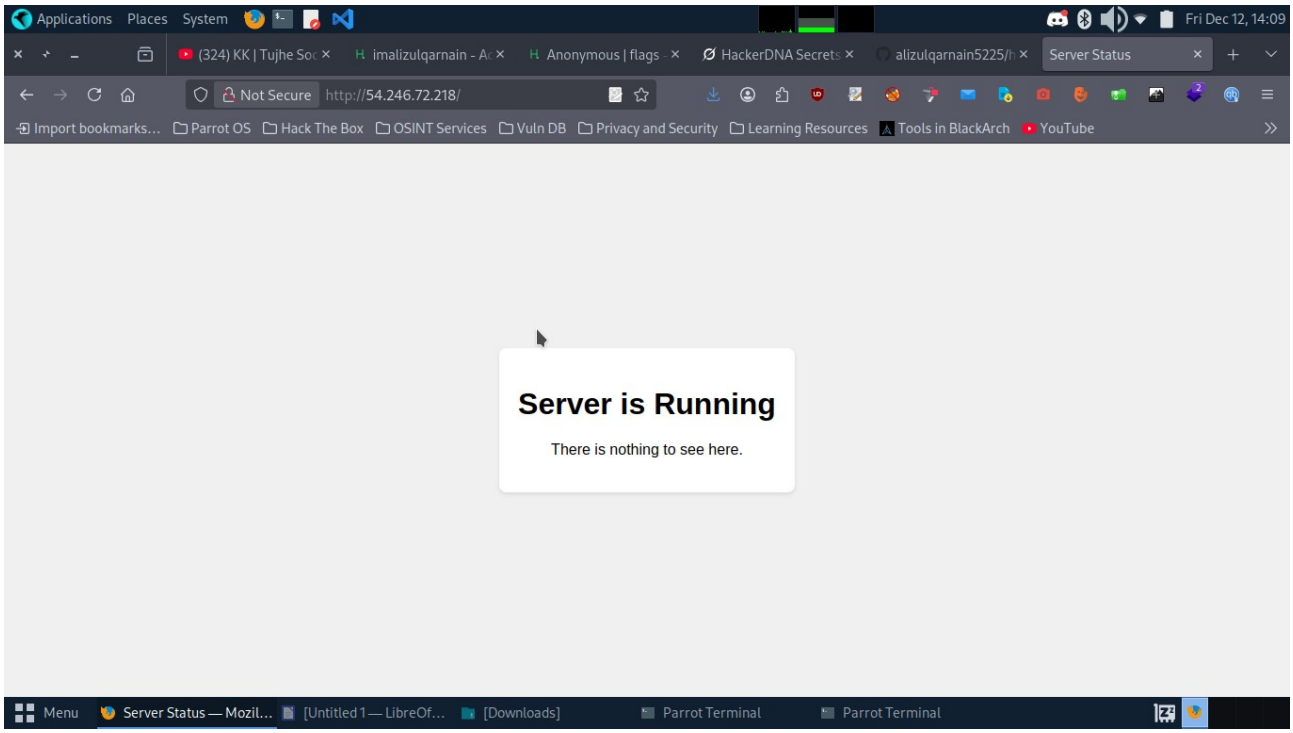
- Open a terminal in the lab environment (or your local machine if connected).
- Run a basic Nmap scan: nmap -sV <target_IP> (or nmap -Pn -p- <target_IP> for thoroughness).
- Results reveal two open ports: 21/tcp (FTP, vsftpd 3.0.2) and 80/tcp (HTTP, likely Apache or similar).

Nmap Port Scan



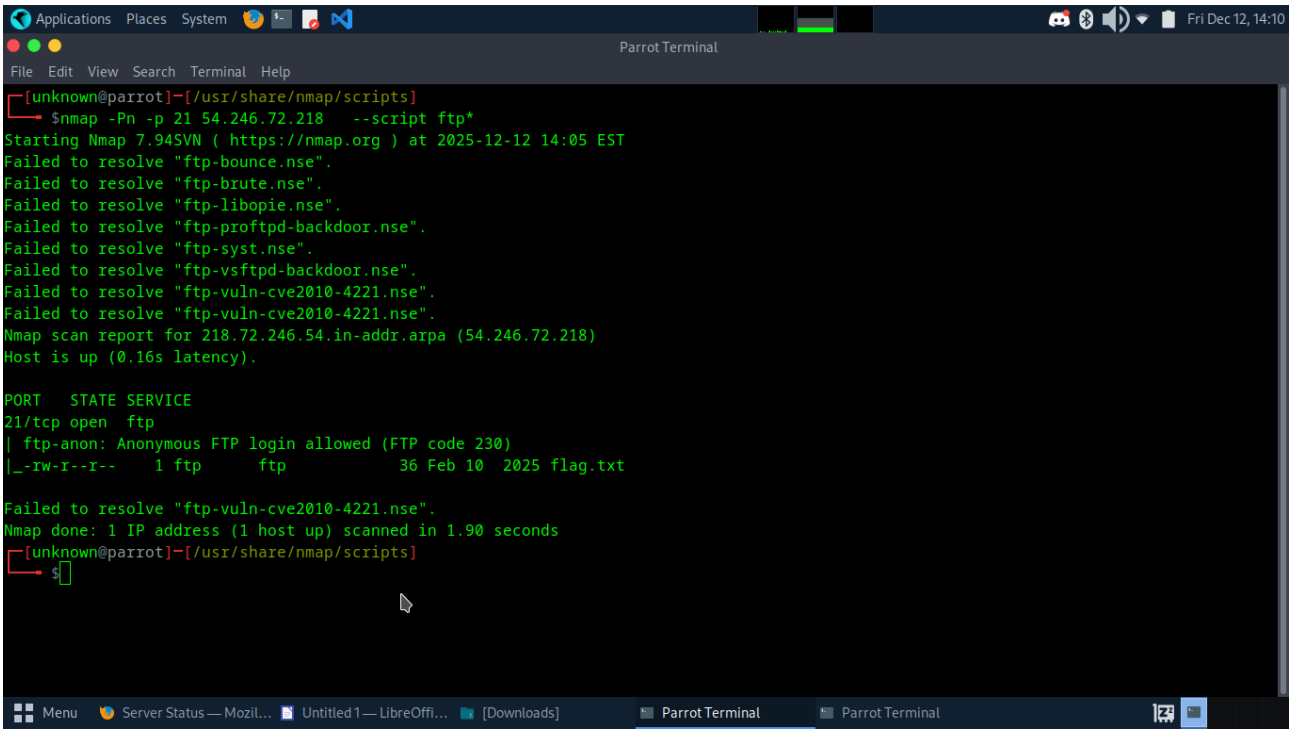
Step 2: Inspect the Web Service (Port 80)

- Navigate to http://<target_IP> in your browser.
- The page is bare: "Server is Running. There is nothing to see here." No forms, links, or hints—dead end for now.



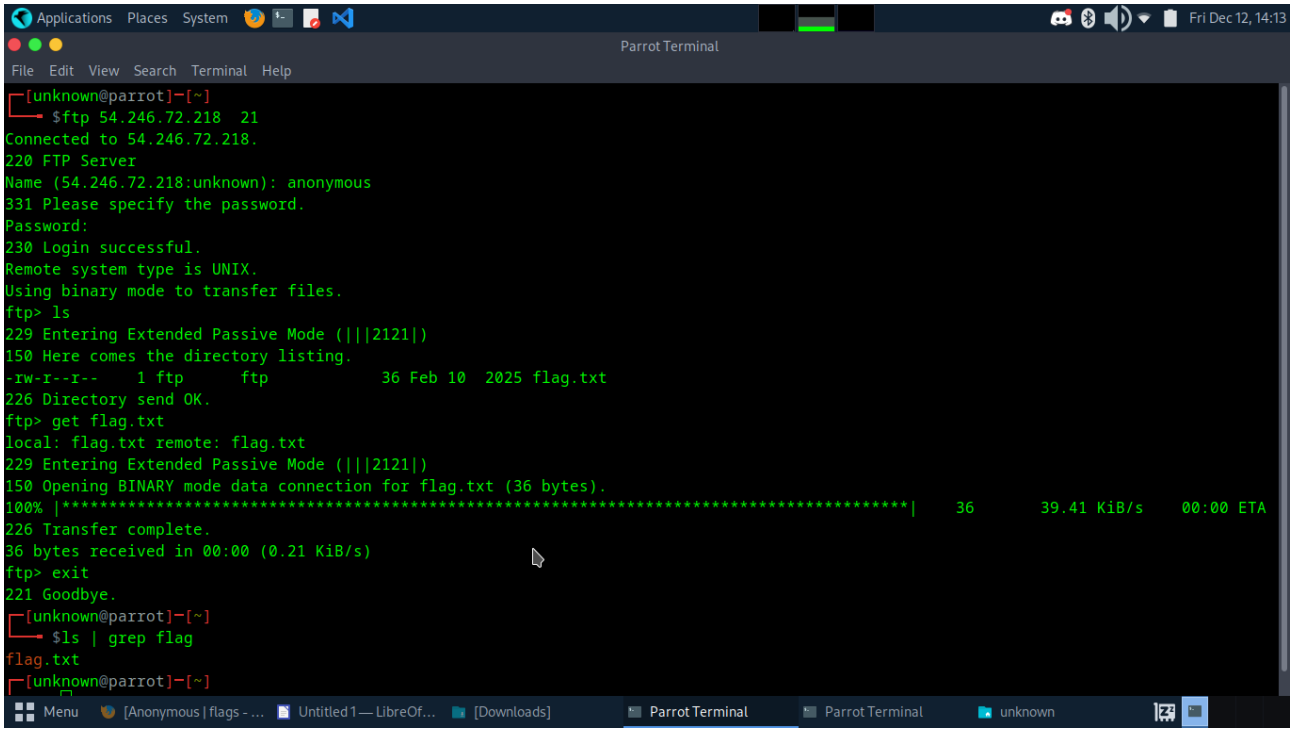
Step 3: Enumerate FTP Vulnerabilities (Port 21)

- Focus on FTP: Use Nmap scripts for deeper intel with nmap -Pn -p 21 <target_IP> --script ftp*.
- Output flags potential issues: vsftpd version info and, crucially, "Anonymous FTP login allowed (FTP code 230)"—bingo, no auth required.



Step 4: Exploit Anonymous Login and Retrieve the Flag

- Connect via FTP: ftp <target_IP> 21.
- At the prompt, enter anonymous as the username and anonymous as the password (or leave blank; both work here).
- Once in: ls lists directory contents, revealing flag.txt.
- Download it: get flag.txt.
- Exit with bye, then cat flag.txt locally to view the contents.



Submit the flag through the HackerDNA dashboard to claim your points.

Congratulation found a flag