

Medium

Welcome back! This Lab is a sequel of the lab "Anonymous". We cleverly called it "Anonymous 2". This time, the Administrator made sure to not put any confidential file (or flag!) in the anonymous folder.

Steps to Success

1. **Start the Machine:** Begin by running the provided virtual machine.
2. **Network Scanning:** Use tools like [Nmap](#) to scan the network and identify open ports and services.
3. **Exploit Vulnerabilities:** [Metasploit](#) can be useful to exploit discovered vulnerabilities and gain further access.

Hint

- **Nmap:** Use Nmap to discover open ports and services versions on the target machine.
 - Completing [this course on scanning](https://hackerdna.com/courses/ethical-hacking/scanning) may be beneficial for this challenge: <https://hackerdna.com/courses/ethical-hacking/scanning>
- **Metasploit:** Utilize Metasploit to exploit identified vulnerabilities.
- **File Locations:** Pay attention to files located in the `/root` directory.

Goal

Your goal is to find the hidden flag, which is a UUID located in the `/root/flag.txt` file. Use your skills and creativity to uncover it. Good luck and have fun!

▶ Start Machine

Start the Machine and the IP will show here

To attack the target machine, you must start the Machine first.

for this challenge we need to connect to vsftpd, doing an nmap scan we can see what version is the ftp service which is patched using "anonymous" username
so i opened my msfconsole and used this exploit `exploit/unix/ftp/vsftpd_234_backdoor`
you will get shell and then you will be able to get the flag