# Hacking Messaih -1: Vulnhub Walkthrough

Russell Murad · Follow

4 min read · Jan 6, 2021


Hello everyone. This is Russell Murad working as a Junior Security Engineer at Enterprise Infosec Consultants (EIC).

I just solved a vulnerable machine from Vulnhub named “Hacking Messaih-1”.

You can download it from here —

Hacking Messaih: 1 ~ VulnHub

Let’s begin.

1. First, we are going to check my victim machine's IP using arp-scan.

```
┌──(root💀kali)-[/home/kali]
└─# sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:ab:08:1c, IPv4: 192.168.0.103
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)

192.168.0.110   08:00:27:4e:aa:43       PCS Systemtechnik GmbH

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.198 seconds (116.47 hosts/sec). 5 responded
```

2. Then we need to find some open ports using nmap.

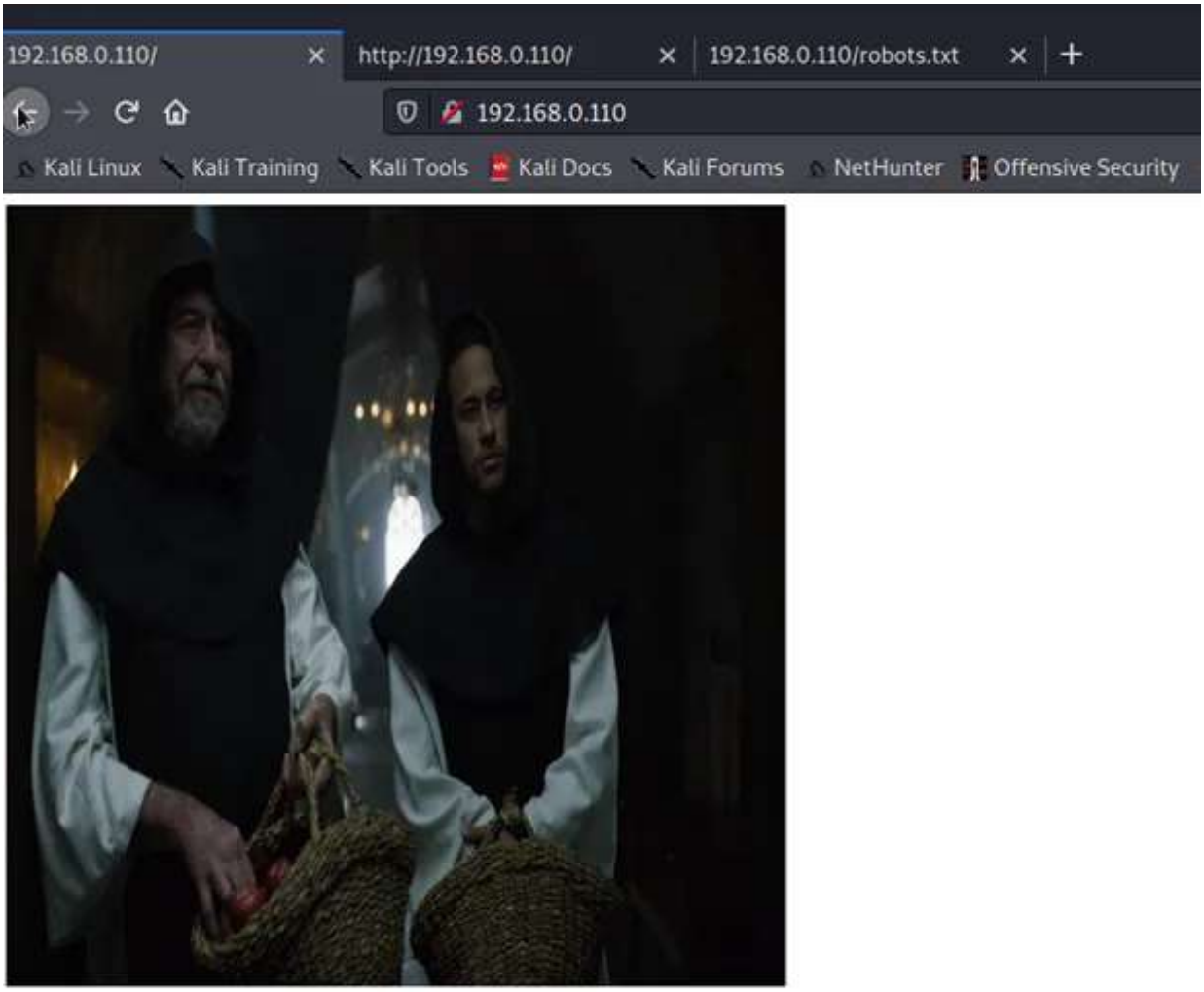
```
┌──(root💀kali)-[/home/kali]
└─# sudo nmap -sC -sV -A -O -p- --script http-enum 192.168.0.110
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-05 12:13 EST
Nmap scan report for 192.168.0.110
Host is up (0.00044s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.14 ((Ubuntu))
| http-enum:
|   /robots.txt: Robots file
|_  /icons/: Potentially interesting folder w/ directory listing
|_http-server-header: Apache/2.2.14 (Ubuntu)
MAC Address: 08:00:27:4E:AA:43 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.35
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.44 ms 192.168.0.110

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.26 seconds

┌──(root💀kali)-[/home/kali]
└─#
```

3. Here we've got two ports open. 80 for HTTP, 22 for SSH. we've also found robots.txt and /icons/ path. We'll investigate those later.

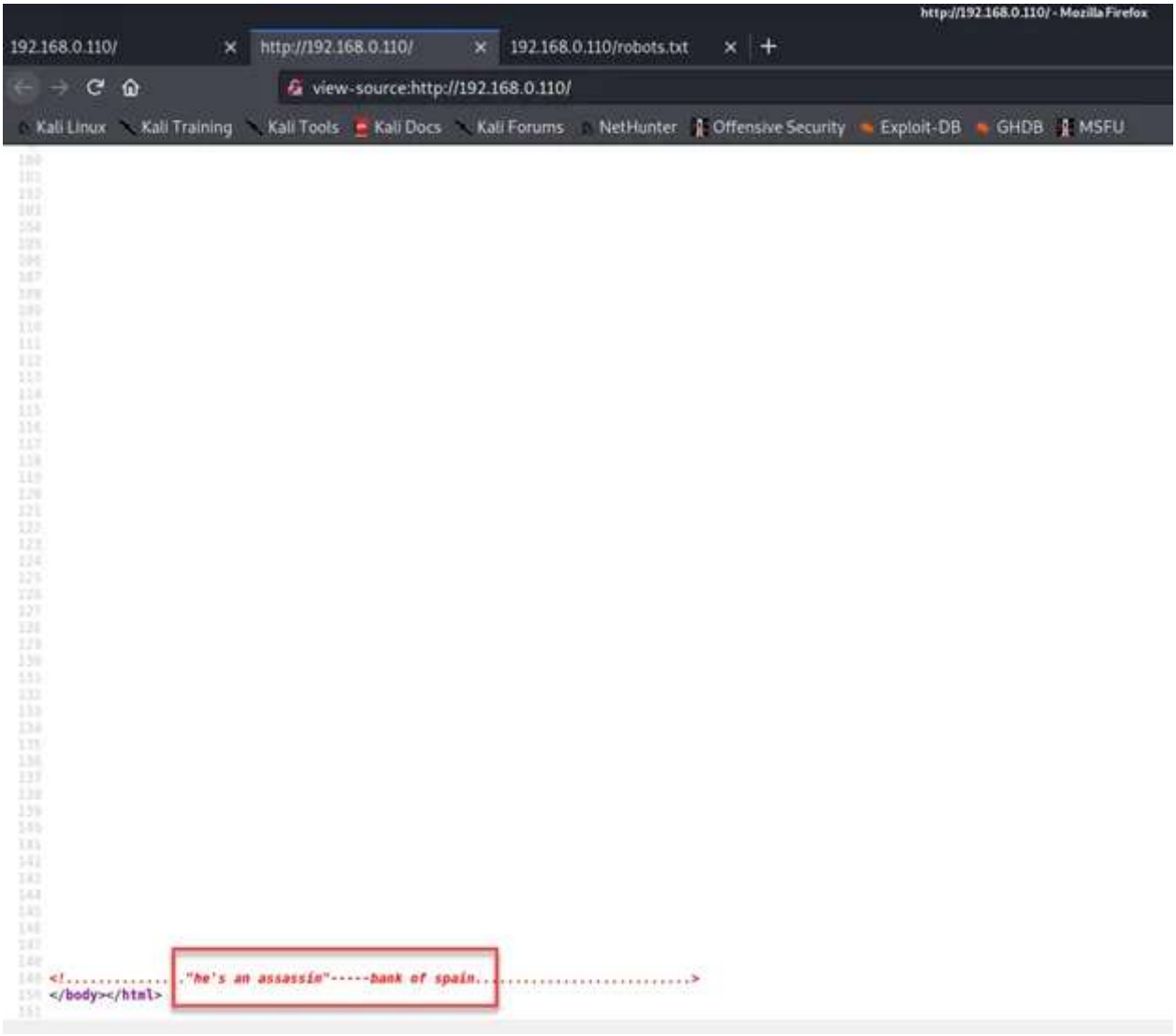
4. Now we intended to find more directories using GoBuster.

```
┌──(root💀kali)-[/home/kali]
└─# gobuster dir -u http://192.168.0.110 -w /home/kali/Desktop/Big.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.0.110
[+] Threads:        10
[+] Wordlist:       /home/kali/Desktop/Big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/01/05 12:33:25 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/cgi-bin/ (Status: 403)
/images1 (Status: 200)
/index (Status: 200)
/robots.txt (Status: 200)
/robots (Status: 200)
/server-status (Status: 403)
===============================================================
2021/01/05 12:33:49 Finished
===============================================================
```

5. Now, time to check some manual stuff. Lets, start Firefox to check the website. There is nothing but that photo, a static site.




6. Let’s check the source code of this site…

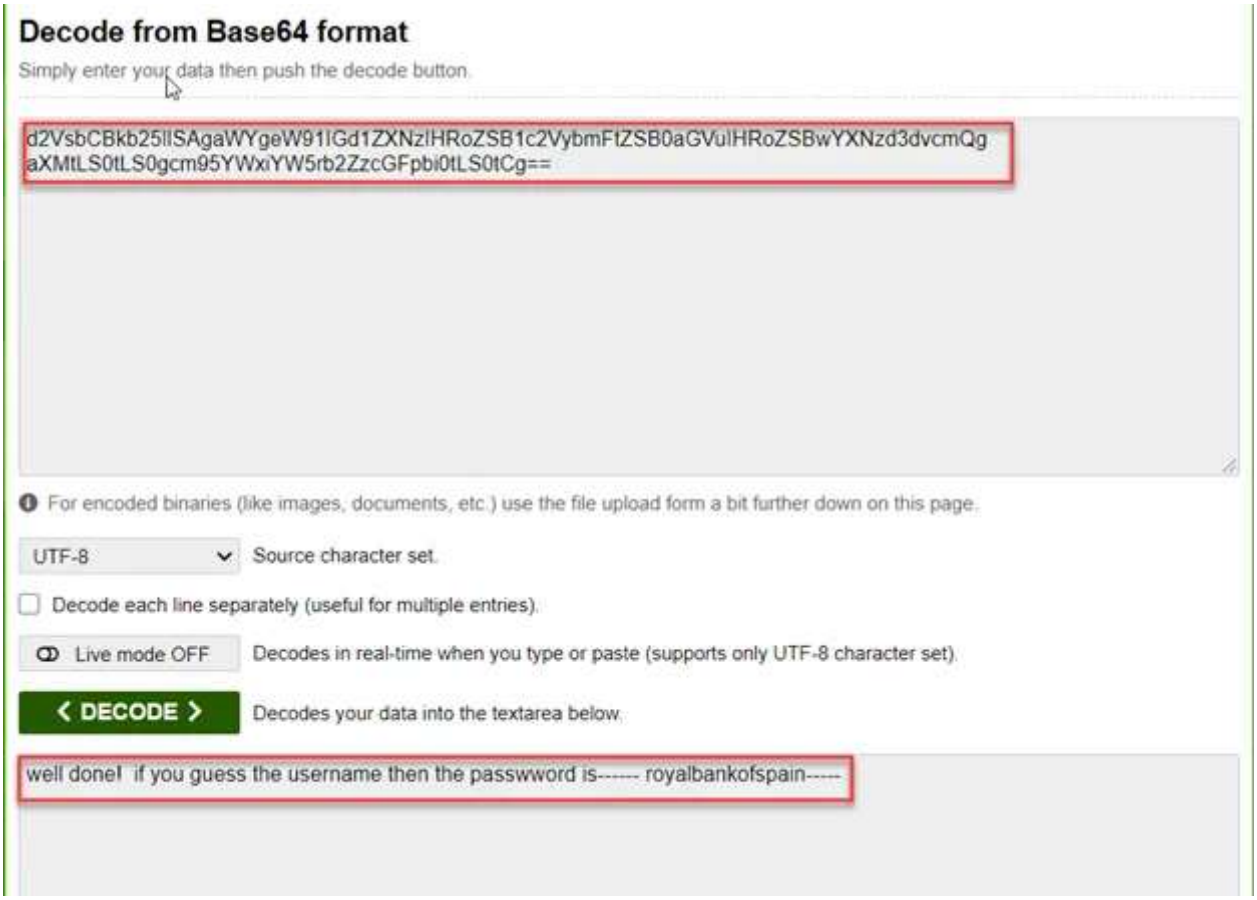



There's a hint...

It's clear down here... Some random guy, he's an assassin, there's a link up with the bank of pain. We'll keep that in mind. Hopefully, this information will useful for later.

7. We'd checked /icon directory. Nothing's there. But when we'd checked robots.txt, there a Base64 code.

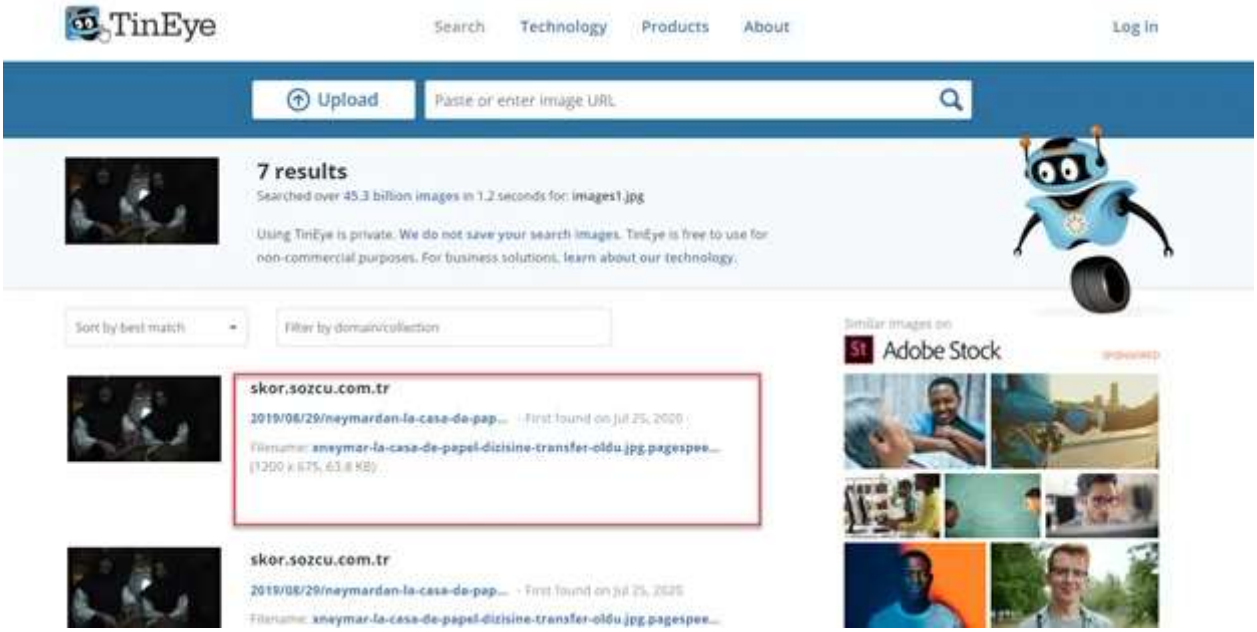
let's convert it...




okay... There's a password named "royalbankofspain". We might use it for login in SSH port. But first, we need a username. Where is it?

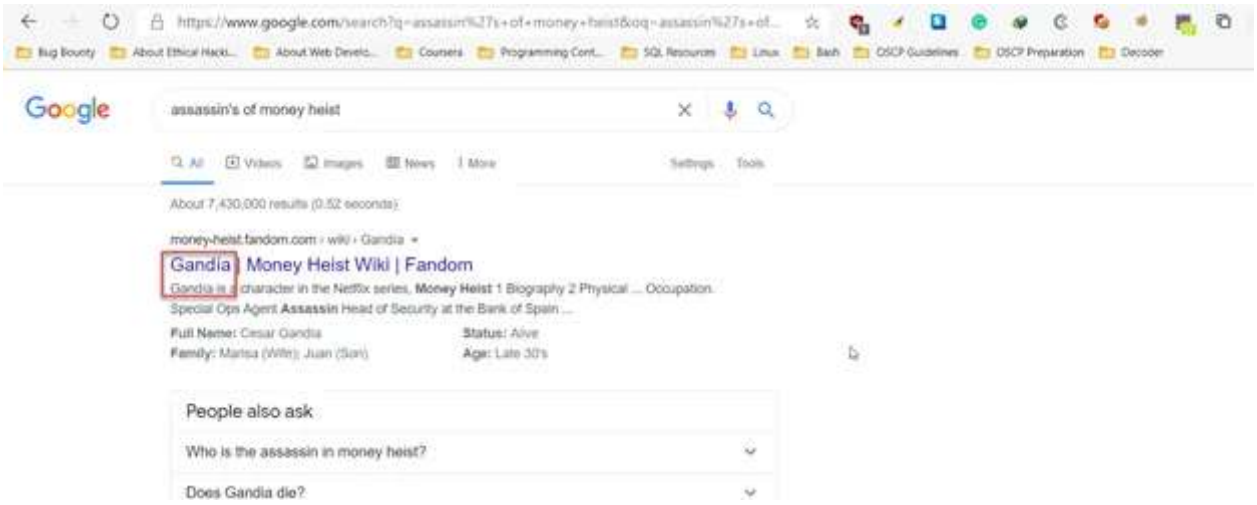
8. At this moment. We have only one option. That is the weird-looking creepy photo of our target site. We tried to see if there are any hidden data in that photo but it didn't work out.

So, I'm going to search on tineye.com using that photo.

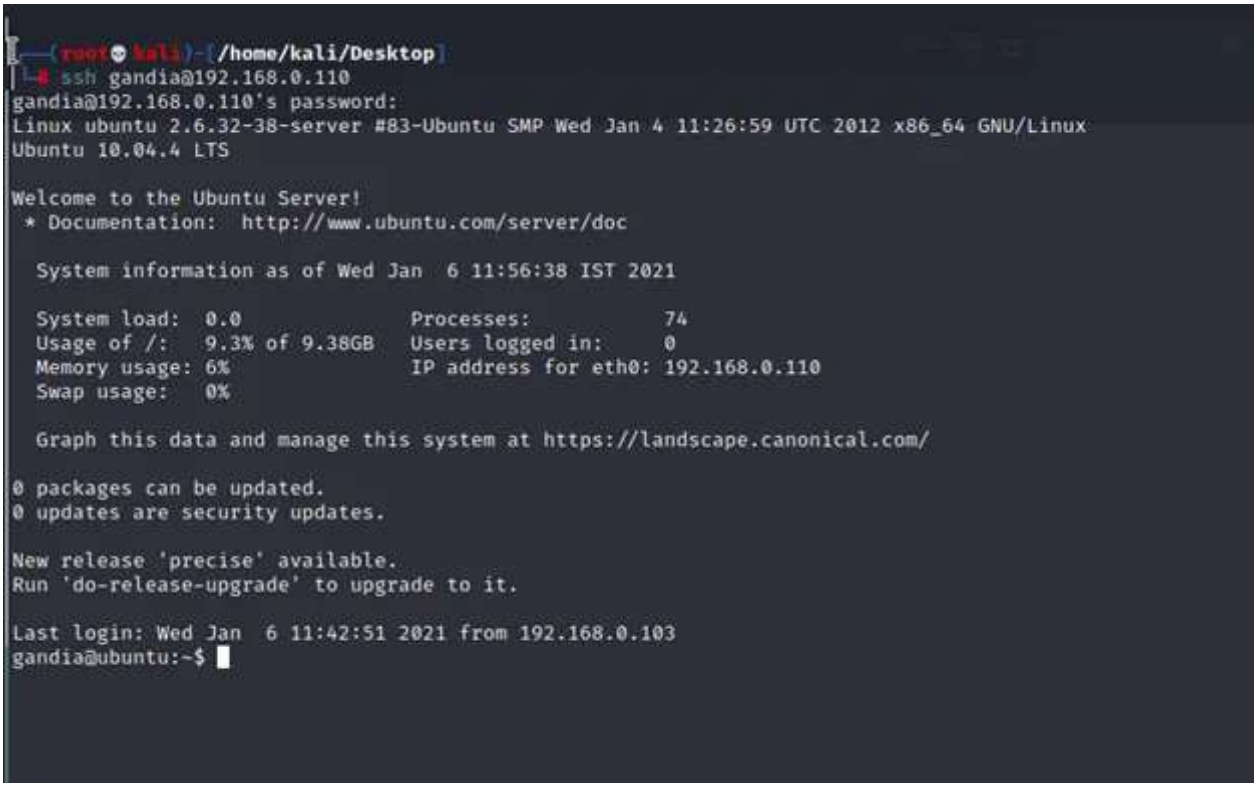




9. By analyzing those search results We've found that the photo is taken from the TV series Money Heist (Spanish: ***La casa de papel***). Neymar played a character there.

Anyway in the previous hint (Step:6) talks about an assassin. We'd google about it and find out that there was an assassin named "gandia" in the Money Heist.




10. Let's try that name as a username with the password from **Step-7** and login in SSH port of our target IP.

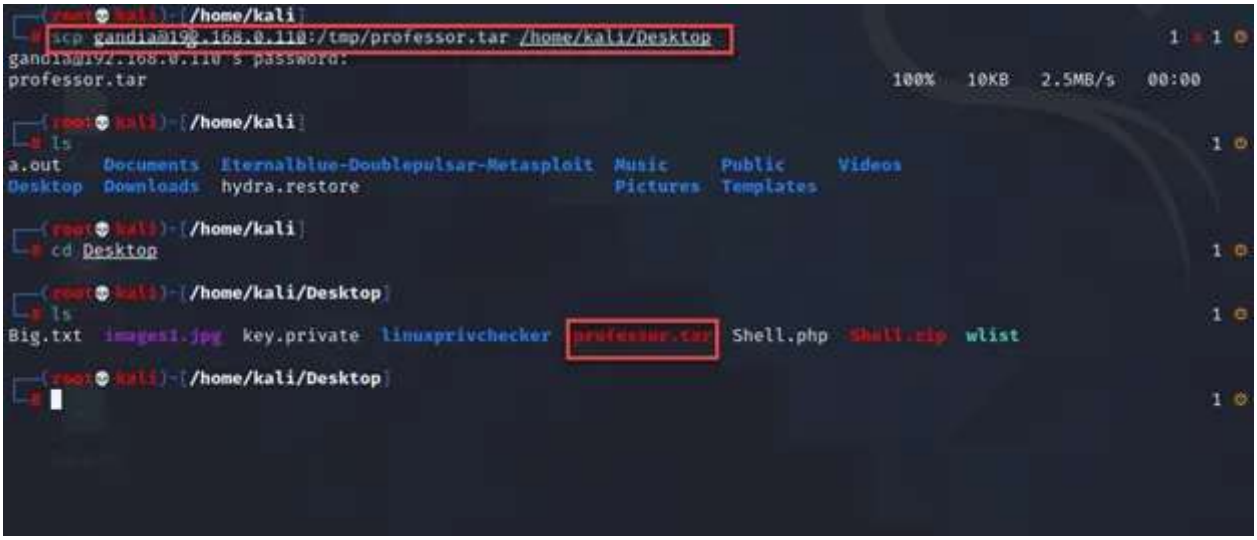



11. We'll discover *professor.tar* file in the berlin directory. Because of that file have Root Privilege we couldn't just decompress it in that folder.

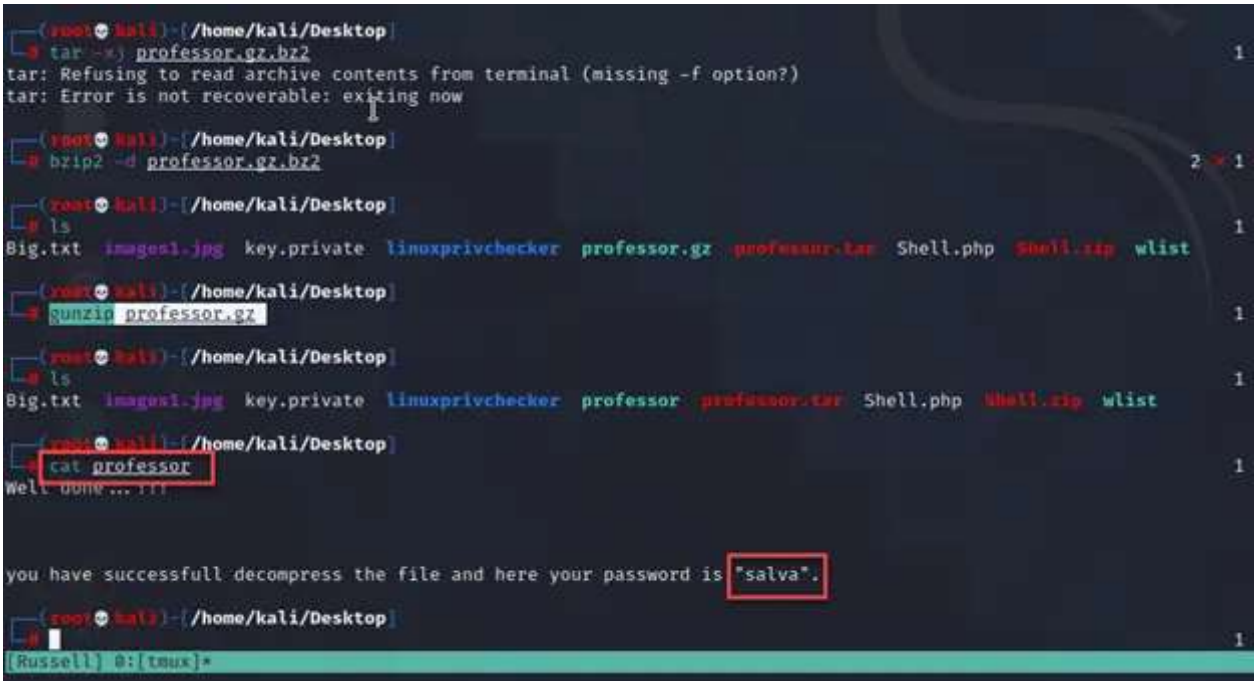
```
gandia@ubuntu:/home$ ls
berlin  gandia  professor
gandia@ubuntu:/home$ cd gandia
gandia@ubuntu:~$ ls
gandia@ubuntu:~$ ls -la
total 32
drwxr-xr-x 4 gandia gandia 4096 2020-08-01 11:35 .
drwxr-xr-x 5 root   root   4096 2020-08-01 07:15 ..
-rw------- 1 gandia gandia  134 2021-01-06 11:43 .bash_history
-rw-r--r-- 1 gandia gandia  220 2020-08-01 03:49 .bash_logout
-rw-r--r-- 1 gandia gandia 3103 2020-08-01 03:49 .bashrc
drwx------ 2 gandia gandia 4096 2020-08-01 04:34 .cache
-rw-r--r-- 1 gandia gandia  675 2020-08-01 03:49 .profile
drwx------ 2 gandia gandia 4096 2020-08-01 11:35 .ssh
gandia@ubuntu:~$ cd ../
gandia@ubuntu:/home$ cd berlin
gandia@ubuntu:/home/berlin$ ls -la
total 32
drwxr-xr-x 4 berlin berlin 4096 2020-08-01 05:14 .
drwxr-xr-x 5 root   root   4096 2020-08-01 07:15 ..
-rw------- 1 berlin berlin  135 2020-08-05 19:01 .bash_history
-rw-r--r-- 1 berlin berlin  220 2020-08-01 04:43 .bash_logout
-rw-r--r-- 1 berlin berlin 3103 2020-08-01 04:43 .bashrc
drwx------ 2 berlin berlin 4096 2020-08-01 04:58 .cache
drwxr-xr-x 2 root   root   4096 2020-08-01 12:30 i have something
-rw-r--r-- 1 berlin berlin  675 2020-08-01 04:43 .profile
gandia@ubuntu:/home/berlin$ cd i have something
-bash: cd: i: No such file or directory
gandia@ubuntu:/home/berlin$ cd i\ have\ something/
gandia@ubuntu:/home/berlin/i have something$ ls
[redacted]
gandia@ubuntu:/home/berlin/i have something$ tar -xvf professor.tar
professor.gz.bz2.gz
tar: professor.gz.bz2.gz: Cannot open: Permission denied
```

12. After some time we'll find out we can copy that into/tmp directory and then download it into our Kali Machine.

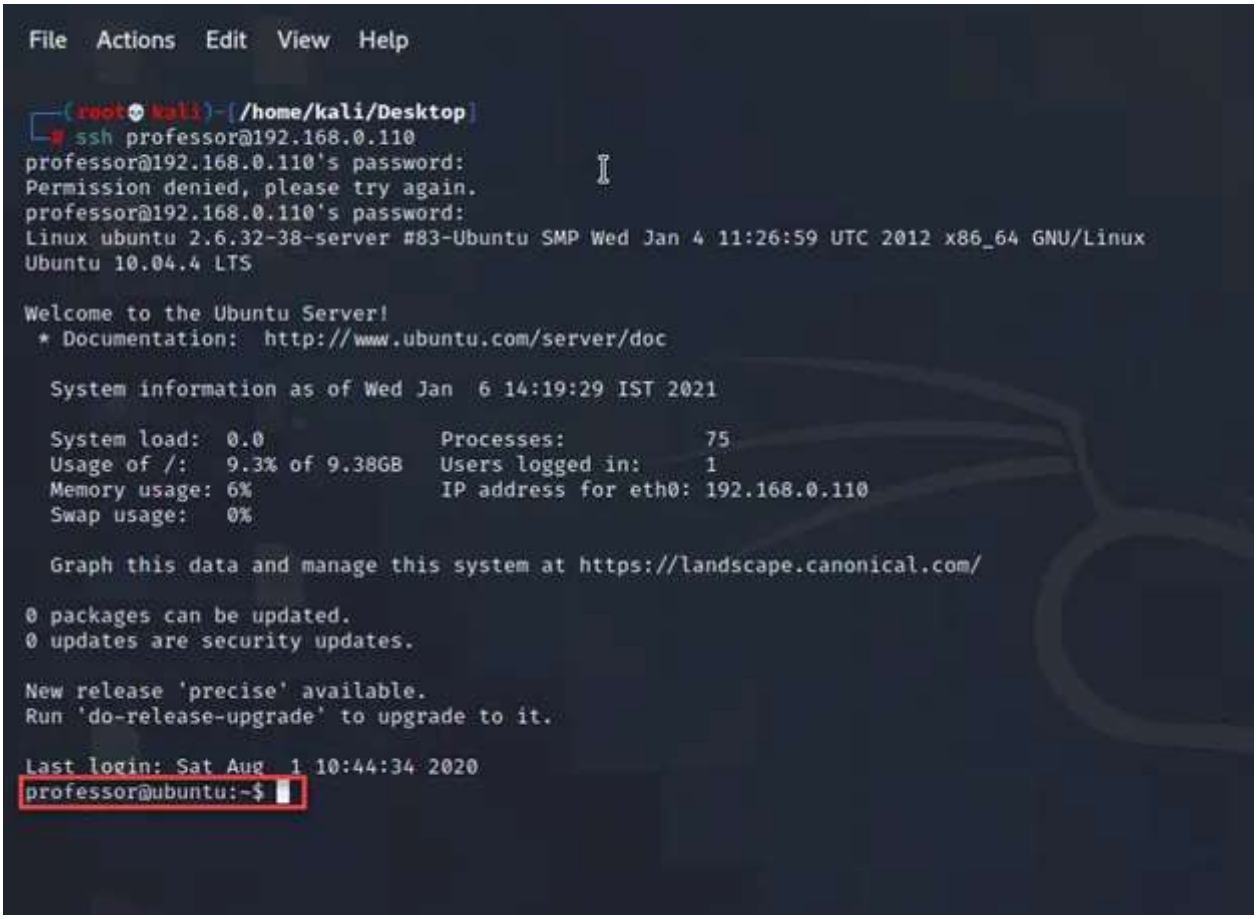
```
gandia@ubuntu:/home/berlin/i have something$ ls
professor.tar
gandia@ubuntu:/home/berlin/i have something$ cp professor.tar /tmp
gandia@ubuntu:/home/berlin/i have something$ cd ../../../
gandia@ubuntu:/$ ls
bin   cdrom  etc   initrd.img  lib64       media  opt   root  selinux  sys  usr  vmlinuz
boot  dev    home  lib         lost+found  mnt    proc  sbin  srv      tmp  var
gandia@ubuntu:/$ cd tmp
gandia@ubuntu:/tmp$ ls -la
total 20
drwxrwxrwt  2 root   root    4096 2021-01-06 13:59 .
drwxr-xr-x 22 root   root    4096 2021-01-06 11:17 ..
-rw-r--r--  1 gandia gandia 10240 2021-01-06 13:59 professor.tar
gandia@ubuntu:/tmp$
```



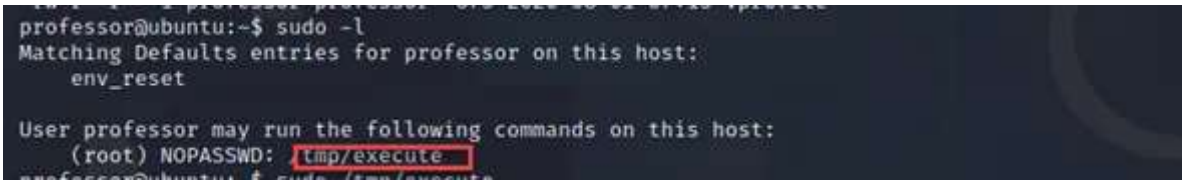

13. We'll decompress it and find a password.




14. Now we'll open a new terminal and login into SSH again using **professor** as a username.

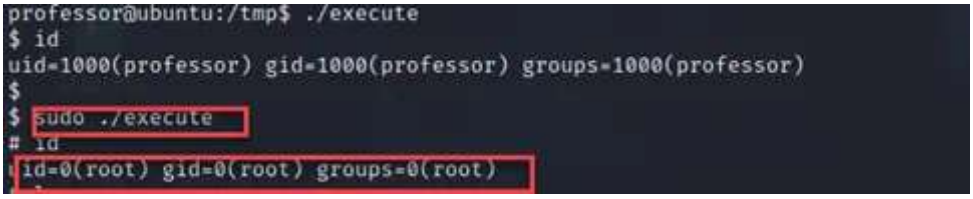



15. Now if we try to use "*sudo -l*" it'll say that the user professor can run "tmp/execute" file with root privilege.




16. now we'll go to that /tmp directory and a file named "execute" and put bin/sh command.


17. We'll run that program with sudo. Then if we check our id, we'll find out our root privilege.




18. Then, as usual, we'll import a python spawn tty shell. Go to /root and open our flag file. It's done.


So, guys, this is it!

Thank you for reading this write-up. Cheers!

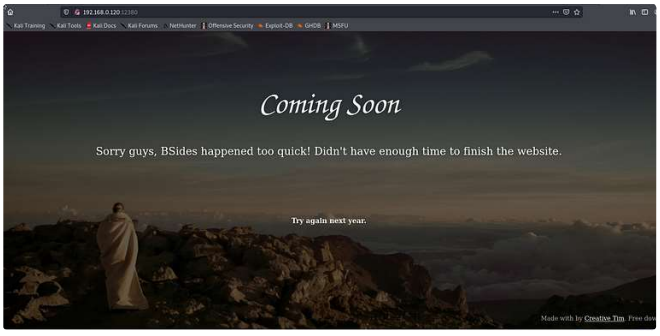
Vulnhub Messiah

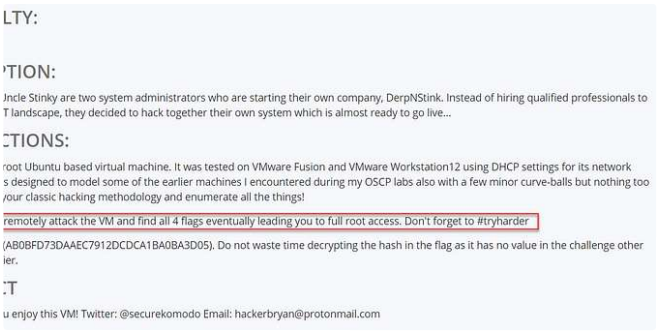
## Written by Russell Murad

16 Followers

Follow

### More from Russell Murad




Russell Murad

## Stapler-1: Vulnhub Walkthrough

Hello Guys! This is Russell Murad working as a Junior Security Engineer at Enterprise Infose...

Russell Murad

## DerpNStink-1: Vulnhub Walkthrough

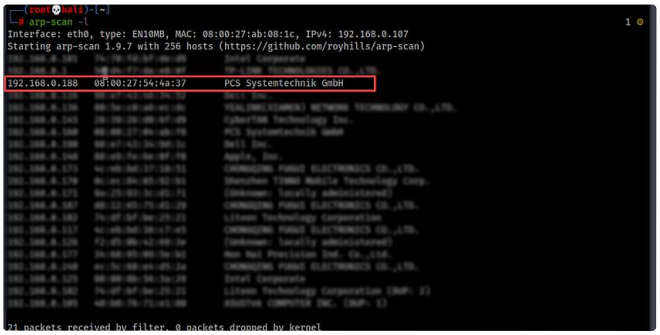
6 min read · Jan 31, 2021

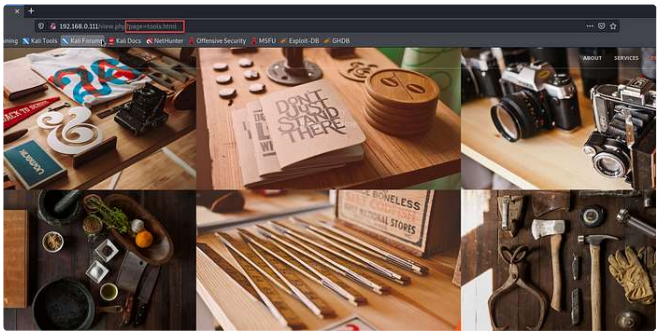
1

Hello Guys! It's me, Russell Murad, working as a Junior Security Engineer at Enterprise...

7 min read · Feb 8, 2021

50



Russell Murad

## Skytower-1: Vulnhub Walkthrough

Hello Guys! It's me, Russell Murad, working as a Junior Security Engineer at Enterprise...

4 min read · Feb 10, 2021

79

Russell Murad

## Zico2:Vulnhub Walkthrough

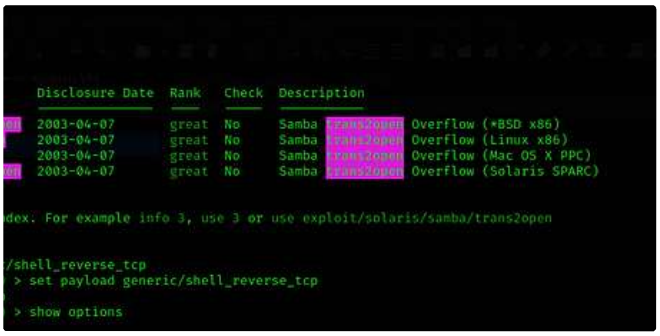
Hello Guys! It's me, Russell Murad, working as a Junior Security Engineer at Enterprise...

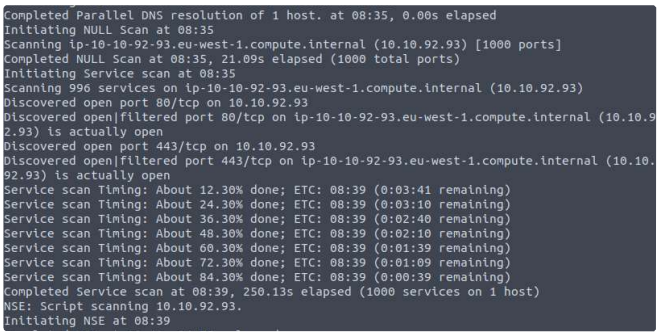
5 min read · Feb 28, 2021

46

See all from Russell Murad

## Recommended from Medium




Cybertech Maven

## Hacking Kioptrix Level 1 Write-up

Introduction

5 min read · Jul 28

3

Jasper Alblas

## TryHackMe: Mr Robot CTF Walkthrough

Hi! It is time to look at the Mr Robot CTF room on TryHackMe. This one is especially fun so...

✦ · 9 min read · Jul 6

249

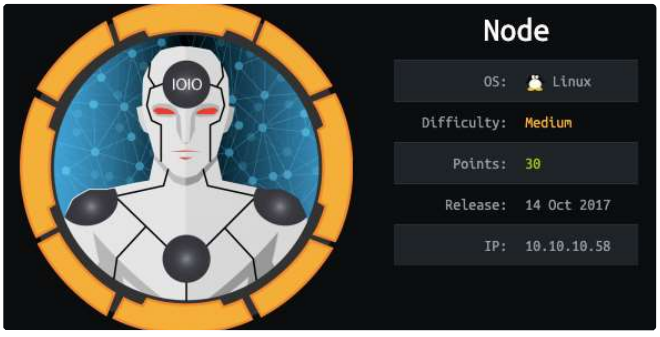
### Lists


**Staff Picks**
541 stories · 557 saves

**Stories to Help You Level-Up at Work**
19 stories · 376 saves

**Self-Improvement 101**
20 stories · 1077 saves

**Productivity 101**
20 stories · 979 saves




Sanaullah Aman Korai

## HackTheBox: Node—Walkthrough

Node is about enumerating a Express NodeJS application to find an API endpoint that...

9 min read · Jul 1

5

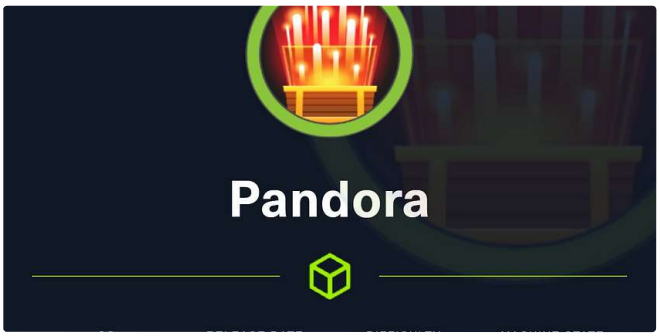
cyx

## Codify (Easy) CTF—HackTheBox

From the NMAP scan, ports 80, 22 and 3000 were discoverable. So I proceeded to go to...

3 min read · Nov 6

3




Tonee Marqus

## [ Pandora ] HTB Manual Walkthrough 2023 | OSCP Prep

Hi everyone!

5 min read · Sep 2

5


David Varghese in InfoSec Write-ups

## VulnHub - Kioptrix: Level 3 (1.2) (#3)

Learn the basic tools and techniques used in vulnerability assessment and exploitation in ...

13 min read · Jun 29

1

See more recommendations