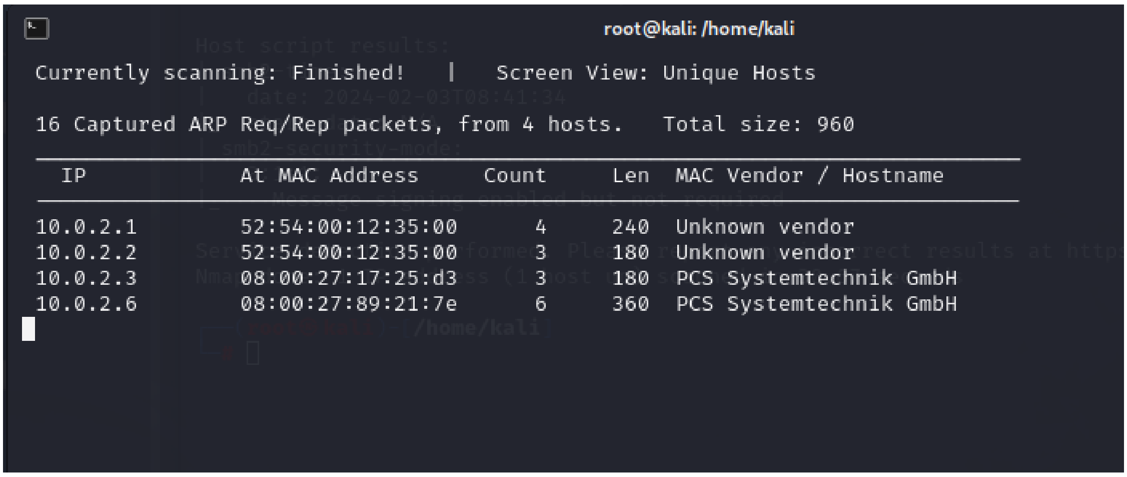
CAPTURE THE FLAG

Submitted To : Nikist Education **Submitted by : Sameer Kumar**
Date : 03-02-2024

CTF FILE : DOUBLETROUBLE 1 vulnhub-web

CTF steps are these :

1. I began by using Netdiscover to find the machine's IP address.

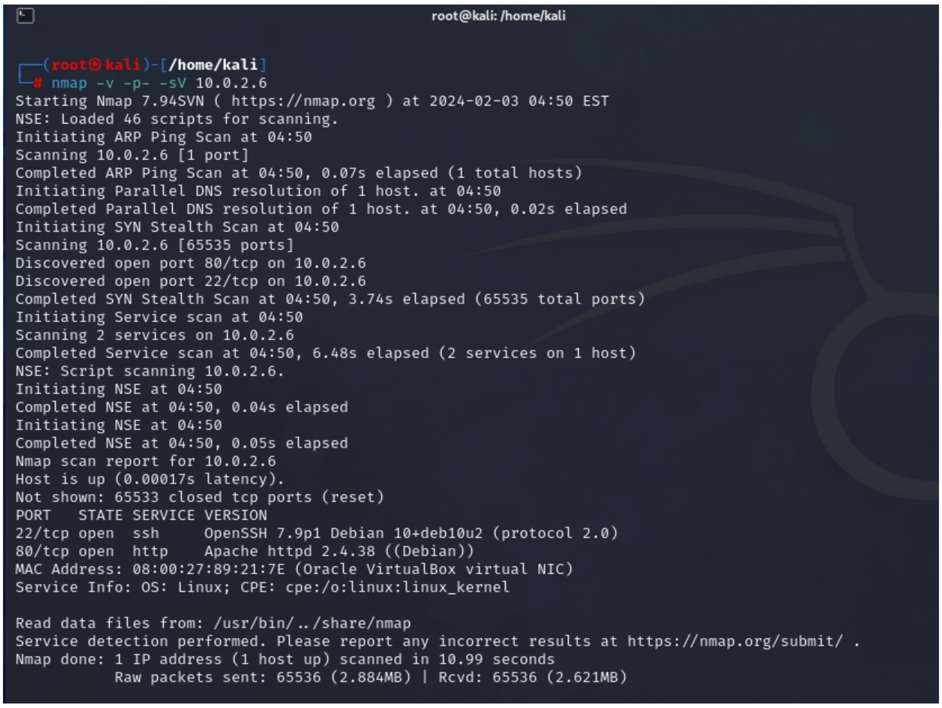


root@kali: /home/kali

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

16 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 960
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      4     240  Unknown vendor
10.0.2.2        52:54:00:12:35:00      3     180  Unknown vendor
10.0.2.3        08:00:27:17:25:d3      3     180  PCS Systemtechnik GmbH
10.0.2.6        08:00:27:89:21:7e      6     360  PCS Systemtechnik GmbH
```

I discovered these IP addresses here. I next look up each IP address and discover that my target device's IP address is 10.0.0.6.

2. I then used nmap to do a ports scan.

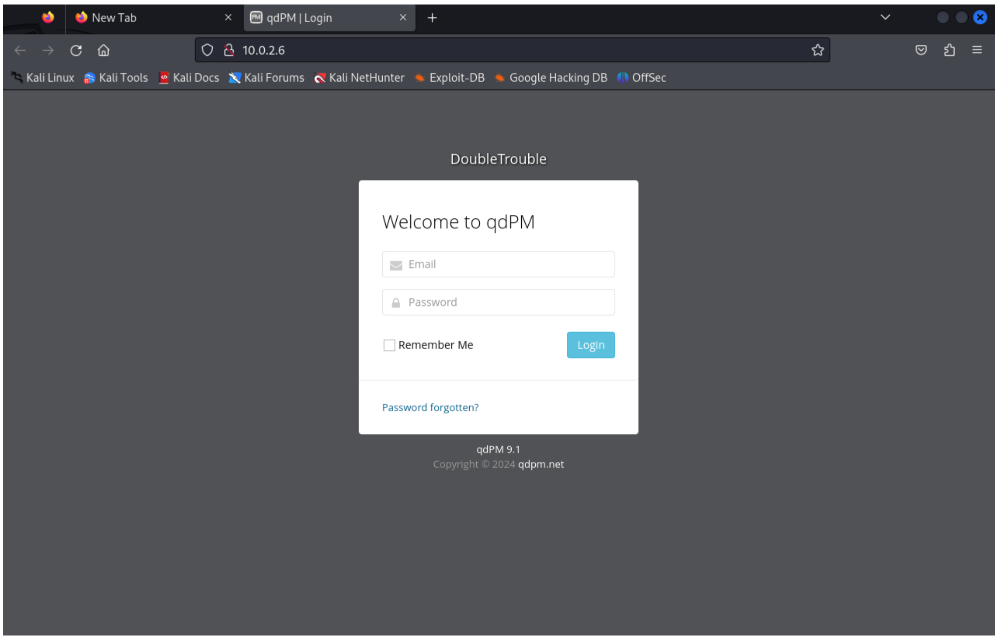


root@kali: /home/kali

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -v -p- -sV 10.0.2.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-03 04:50 EST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 04:50
Scanning 10.0.2.6 [1 port]
Completed ARP Ping Scan at 04:50, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:50
Completed Parallel DNS resolution of 1 host. at 04:50, 0.02s elapsed
Initiating SYN Stealth Scan at 04:50
Scanning 10.0.2.6 [65535 ports]
Discovered open port 80/tcp on 10.0.2.6
Discovered open port 22/tcp on 10.0.2.6
Completed SYN Stealth Scan at 04:50, 3.74s elapsed (65535 total ports)
Initiating Service scan at 04:50
Scanning 2 services on 10.0.2.6
Completed Service scan at 04:50, 6.48s elapsed (2 services on 1 host)
NSE: Script scanning 10.0.2.6.
Initiating NSE at 04:50
Completed NSE at 04:50, 0.04s elapsed
Initiating NSE at 04:50
Completed NSE at 04:50, 0.05s elapsed
Nmap scan report for 10.0.2.6
Host is up (0.00017s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
MAC Address: 08:00:27:89:21:7E (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.99 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

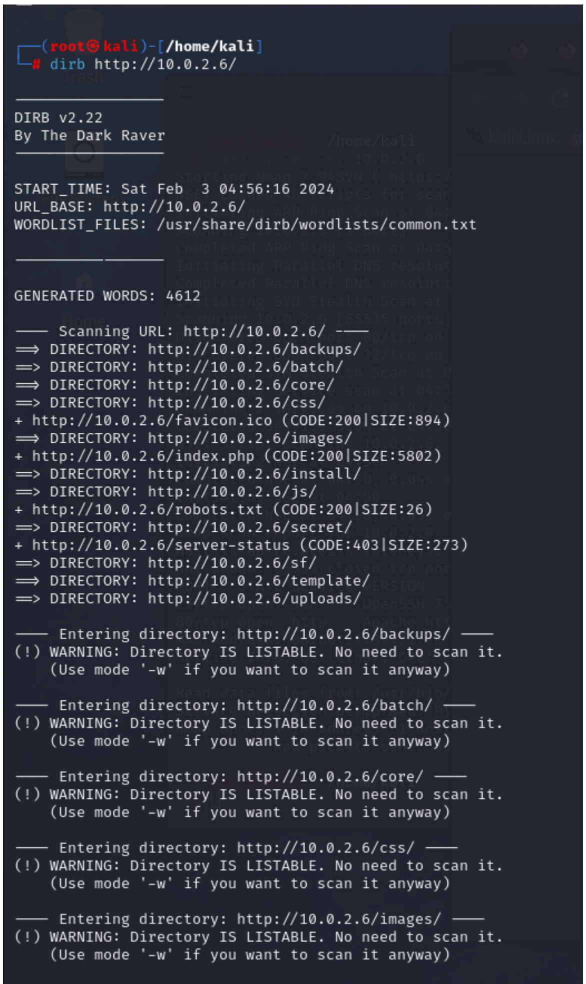
In nmap scanning I used the flags -v for verbose, -sV to see services running on ports that are open, and -p- to scan all 65535 ports.

I see that there are two ports here. Port 22/tcp which is running ssh service, port 80/tcp which is running http service or the web application.

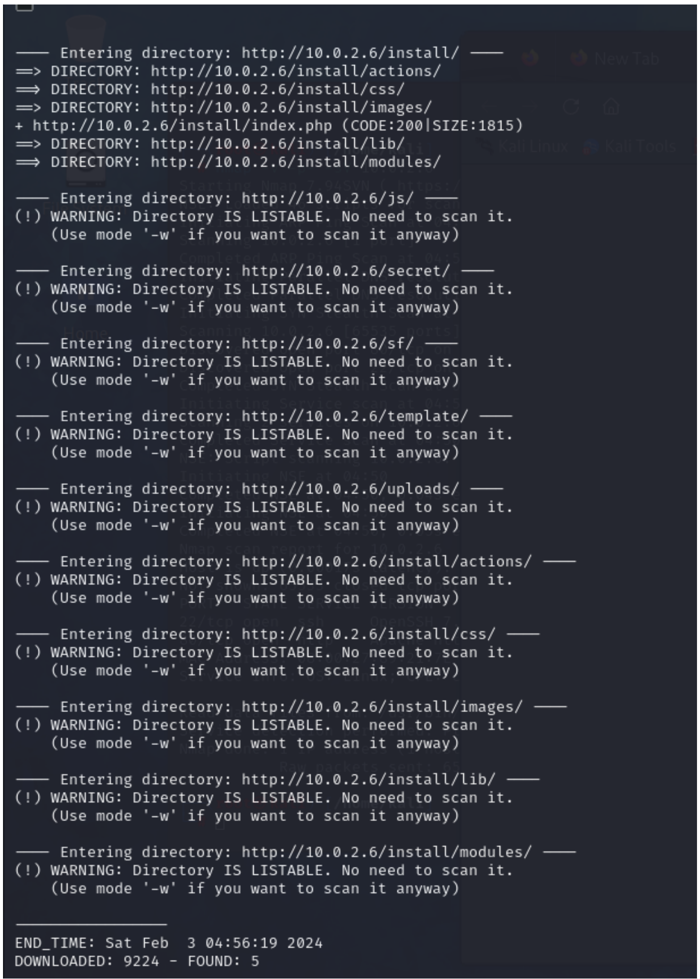


After visiting the http://10.0.2.6/ or target machine web app. I got log-in page.

3. I then attempted to log in using a couple well-known credentials. but, none of them were successful. I began by performing a brute force scan of a web application to list hidden files and directories. For this, I used the Dirb tool. Below are the scan command and results.

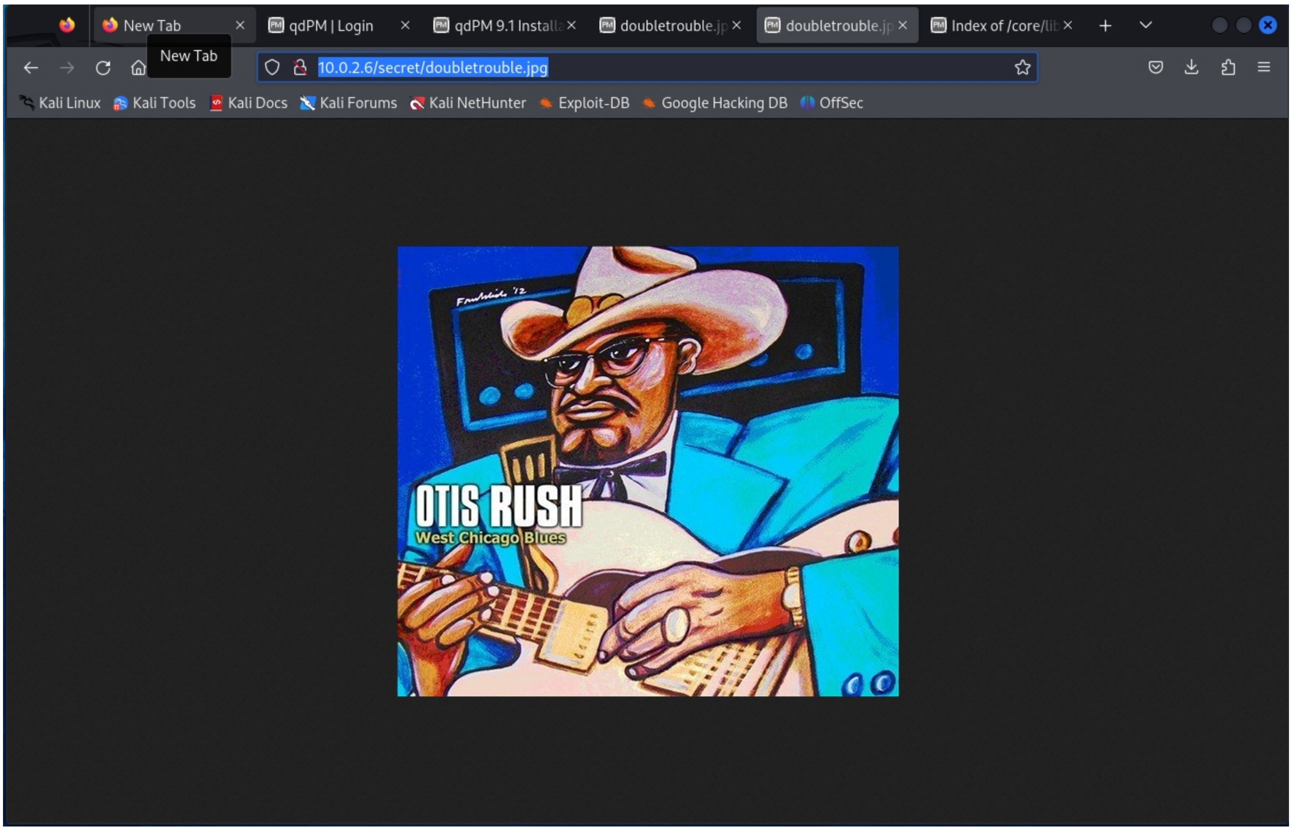


```
┌──(root㉿kali)-[/home/kali]
└─# dirb http://10.0.2.6/

-----------------

DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Feb  3 04:56:16 2024
URL_BASE: http://10.0.2.6/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.6/ ----
==> DIRECTORY: http://10.0.2.6/backups/
==> DIRECTORY: http://10.0.2.6/batch/
==> DIRECTORY: http://10.0.2.6/core/
==> DIRECTORY: http://10.0.2.6/css/
+ http://10.0.2.6/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://10.0.2.6/images/
+ http://10.0.2.6/index.php (CODE:200|SIZE:5802)
==> DIRECTORY: http://10.0.2.6/install/
==> DIRECTORY: http://10.0.2.6/js/
+ http://10.0.2.6/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://10.0.2.6/secret/
+ http://10.0.2.6/server-status (CODE:403|SIZE:273)
==> DIRECTORY: http://10.0.2.6/sf/
==> DIRECTORY: http://10.0.2.6/template/
==> DIRECTORY: http://10.0.2.6/uploads/

---- Entering directory: http://10.0.2.6/backups/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/batch/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/core/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```



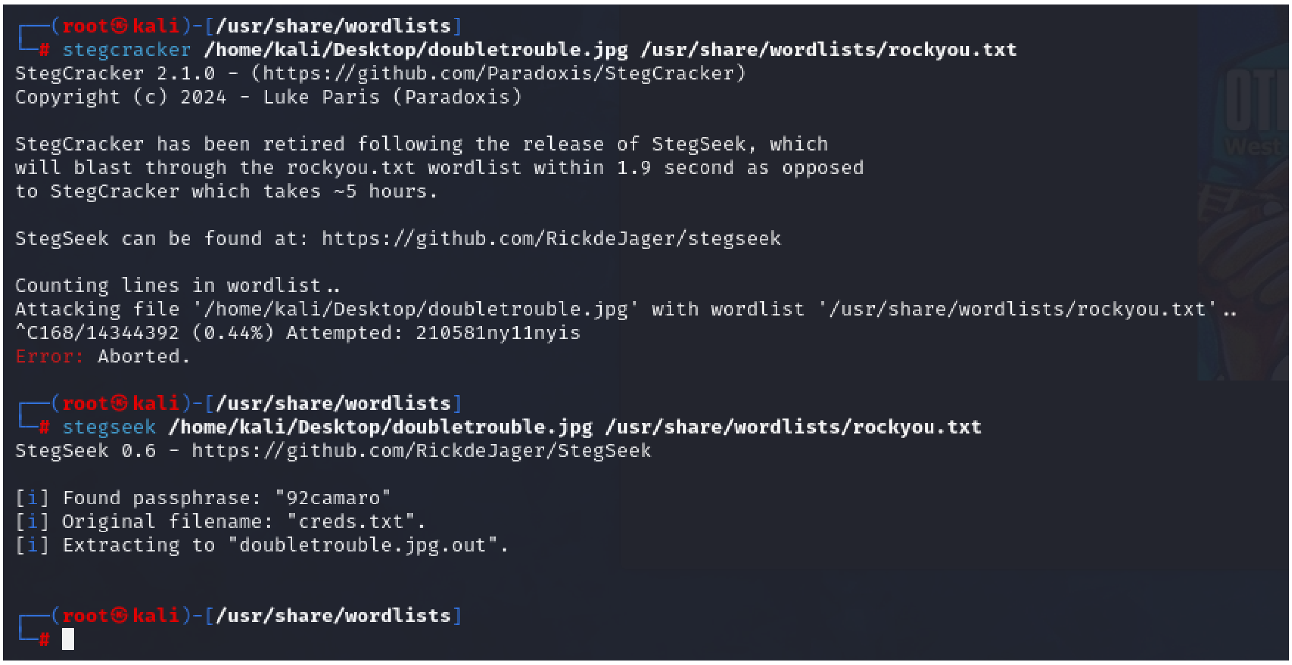
```
---- Entering directory: http://10.0.2.6/install/ ----
==> DIRECTORY: http://10.0.2.6/install/actions/
==> DIRECTORY: http://10.0.2.6/install/css/
==> DIRECTORY: http://10.0.2.6/install/images/
+ http://10.0.2.6/install/index.php (CODE:200|SIZE:1815)
==> DIRECTORY: http://10.0.2.6/install/lib/
==> DIRECTORY: http://10.0.2.6/install/modules/

---- Entering directory: http://10.0.2.6/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/secret/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/sf/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/template/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/install/actions/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/install/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/install/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/install/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/install/modules/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Sat Feb  3 04:56:19 2024
DOWNLOADED: 9224 - FOUND: 5
```

4. During my directory scan for the web application enumeration, I discovered a picture in a directory named as secret.

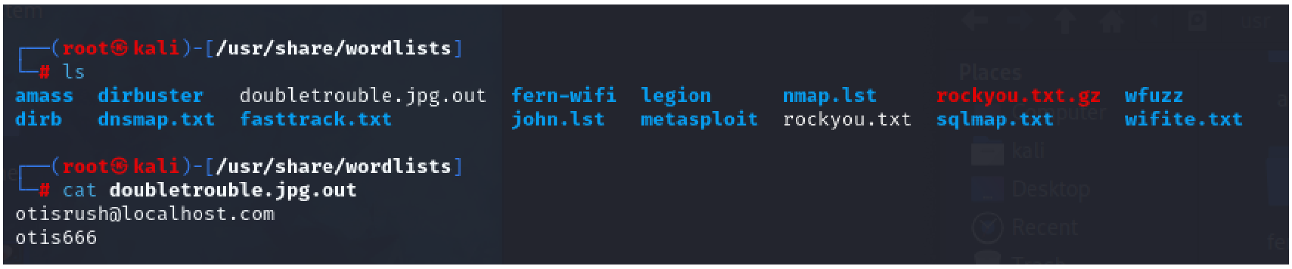


I opened the image file into the browser, but nothing interesting could be identified there.

5. then I used Stegcracker to perform a password check on this picture file. Stegcracker seemed extremely slow to me. I used stegseek and received a creds.txt file with valid credentials in a matter of seconds.

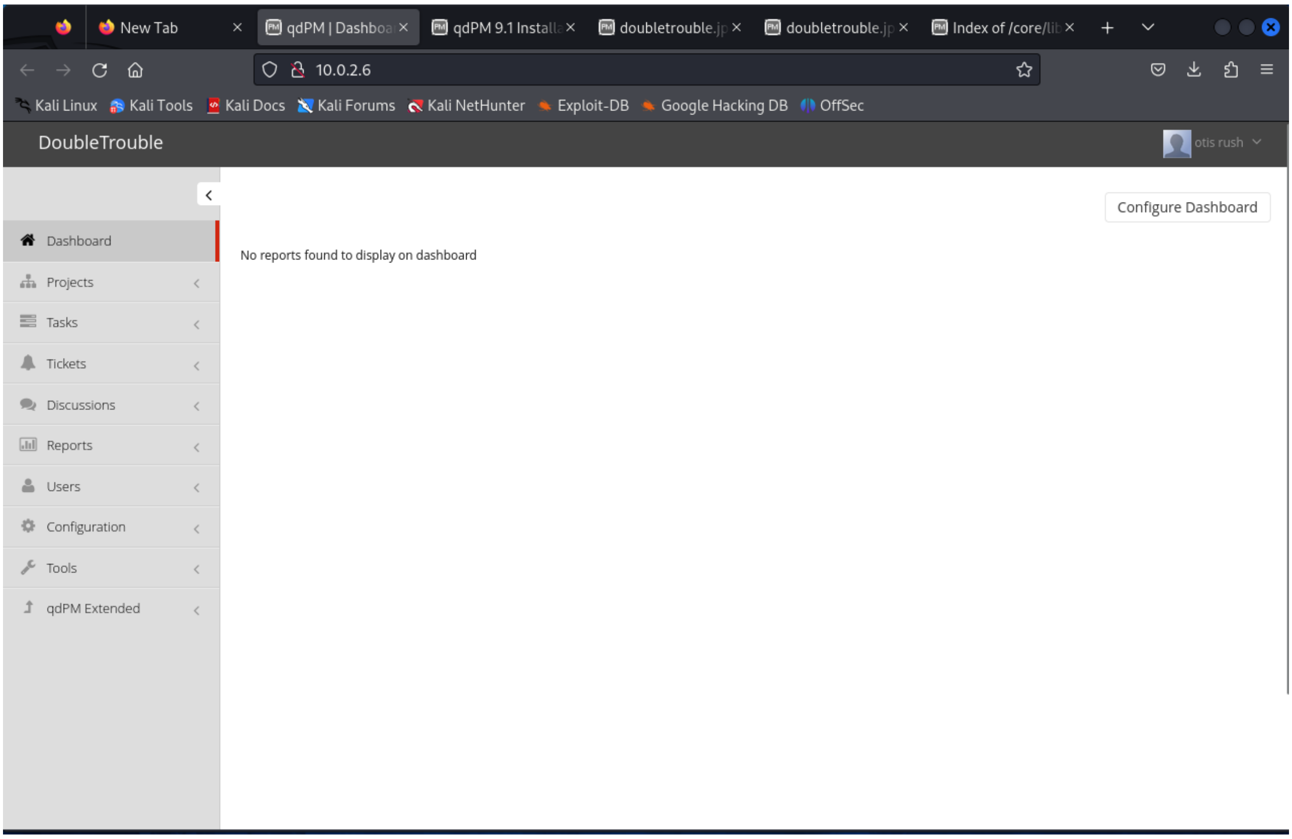


```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# stegcracker /home/kali/Desktop/doubletrouble.jpg /usr/share/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2024 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file '/home/kali/Desktop/doubletrouble.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
^C168/14344392 (0.44%) Attempted: 210581ny11nyis
Error: Aborted.

┌──(root㉿kali)-[/usr/share/wordlists]
└─# stegseek /home/kali/Desktop/doubletrouble.jpg /usr/share/wordlists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "92camaro"
[i] Original filename: "creds.txt".
[i] Extracting to "doubletrouble.jpg.out".


┌──(root㉿kali)-[/usr/share/wordlists]
└─# █
```



```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass  dirbuster   doubletrouble.jpg.out  fern-wifi  legion      nmap.lst     rockyou.txt.gz  wfuzz
dirb   dnsmap.txt  fasttrack.txt          john.lst   metasploit  rockyou.txt  sqlmap.txt      wifite.txt

┌──(root㉿kali)-[/usr/share/wordlists]
└─# cat doubletrouble.jpg.out
otisrush@localhost.com
otis666
```

To try these credential, i tried to log-in with these. And i was in as shown in screenshot below.



No reports found to display on dashboard

SUMMARY :

These steps required in solving this CTF:

1. Getting the target machine IP address by using Netdiscover
2. Getting open port details by using the Nmap tool
3. Identifying Vulnerabilities in running web application
4. Enumerating application with Drib Utility
5. Cracking password with StegCracker/Stegseek