

DOUBLE TROUBLE: CAPTURE THE FLAG

Submitted To: Nikist Education

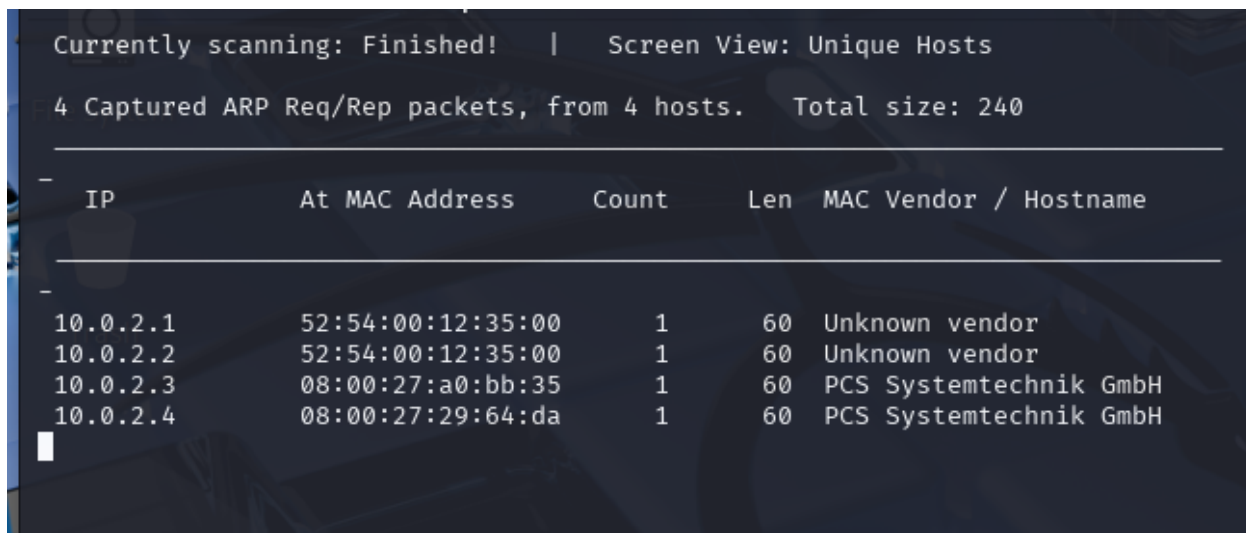
Submitted by: Sarah Marion Ndeti

Date : Fri 30-05-2025

1) Getting the target machine's IP address

Firstly, I identified the IP address of the target machine by running:-

```
sudo netdiscover -r 10.0.0.0/24
```



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
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:a0:bb:35	1	60	PCS Systemtechnik GmbH
10.0.2.4	08:00:27:29:64:da	1	60	PCS Systemtechnik GmbH

The IP address of the target machine is 10.0.2.4

2) Getting open port details by using the nmap tool

I checked the open ports on the target by `nmap -v -T4 -p- -sC -sV -oN nmap.log 10.0.0.26`

In Nmap scanning, I used the flags -v for verbose, -sV to display services running on open ports, and -p- to scan all 65535 ports. I see that there are two ports here. Port 22/tcp, which is running the SSH service, port 80/tcp, which is running http service or the web application.

```

└─$ nmap -v -T4 -p- -sC -sV -oN nmap.log 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-30 10:34 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:35
Completed NSE at 10:35, 0.00s elapsed
Initiating NSE at 10:35
Completed NSE at 10:35, 0.00s elapsed
Initiating NSE at 10:35
Completed NSE at 10:35, 0.00s elapsed
Initiating ARP Ping Scan at 10:35
Scanning 10.0.2.4 [1 port]
Completed ARP Ping Scan at 10:35, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:35
Completed Parallel DNS resolution of 1 host. at 10:35, 13.08s elapsed
Initiating SYN Stealth Scan at 10:35
Scanning 10.0.2.4 [65535 ports]
Discovered open port 80/tcp on 10.0.2.4
Discovered open port 22/tcp on 10.0.2.4
Completed SYN Stealth Scan at 10:35, 4.18s elapsed (65535 total ports)
Initiating Service scan at 10:35
Scanning 2 services on 10.0.2.4
Completed Service scan at 10:35, 6.08s elapsed (2 services on 1 host)
NSE: Script scanning 10.0.2.4.
Initiating NSE at 10:35
Completed NSE at 10:35, 0.59s elapsed
Initiating NSE at 10:35
Completed NSE at 10:35, 0.03s elapsed
Initiating NSE at 10:35
Completed NSE at 10:35, 0.01s elapsed
Nmap scan report for 10.0.2.4
Host is up (0.00037s 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)
|_ ssh-hostkey:
|   2048 6a:fe:d6:17:23:cb:90:79:2b:b1:2d:37:53:97:46:58 (RSA)
|   256 5b:c4:68:d1:89:59:d7:48:b0:96:f3:11:87:1c:08:ac (ECDSA)
|_  256 61:39:66:88:1d:8f:f1:d0:40:61:1e:99:c5:1a:1f:f4 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-title: qdPM | Login
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-favicon: Unknown favicon MD5: B0BD48E57FD398C5DA8AE8F2CCC8D90D
MAC Address: 08:00:27:29:64:DA (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 10:35
Completed NSE at 10:35, 0.00s elapsed

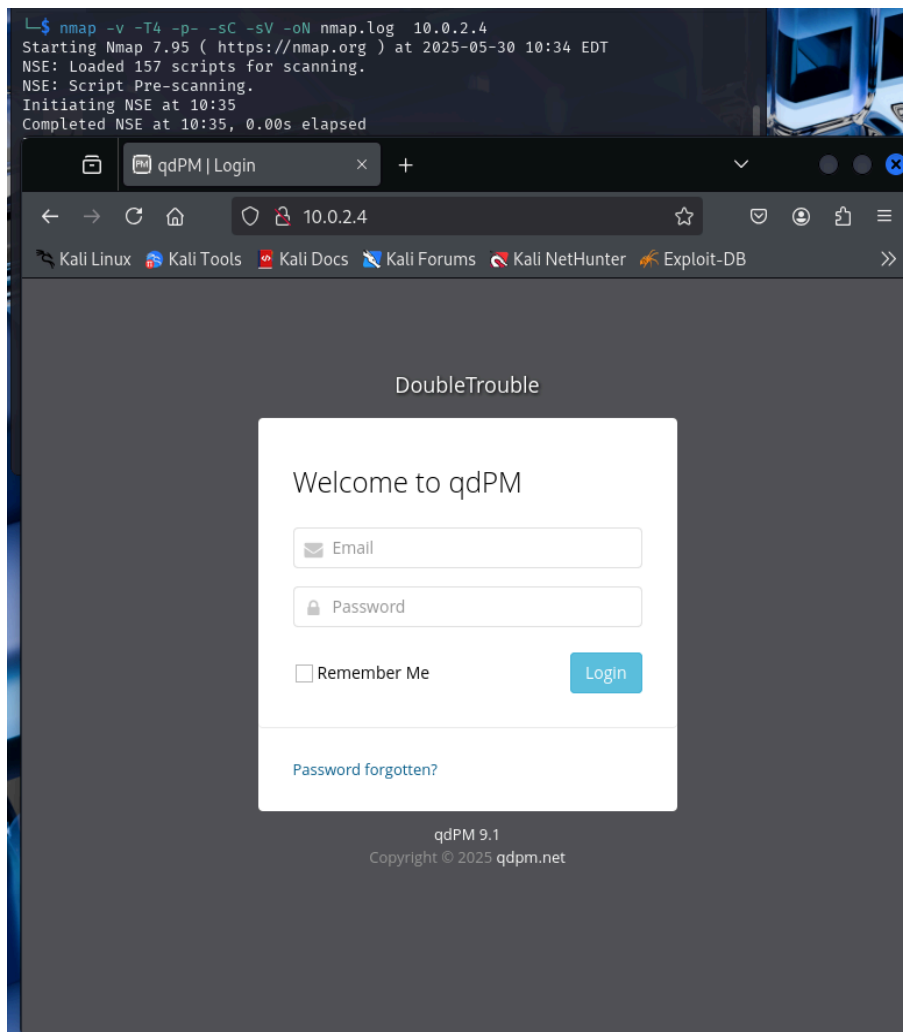
```

3)

Identifying the vulnerabilities in running web application

After visiting the `http://10/0.2.4/` or target machine web app. I got a login page.

The main page of the server leads us to qdPM login page. Furthermore, we also see its version at the bottom. Upon researching, we find that this version suffers from Authenticate RemoteCode Execution Via Insecure File Upload. Reference: <https://www.exploit-db.com/exploits/47954>



qdPM 9.1 login page

4) Enumerating application with Drib Utility

Afterwards, I attempted to log in using a couple of well-known credentials. But, wasn't 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 `dirb`

<http://10.0.2.4/>

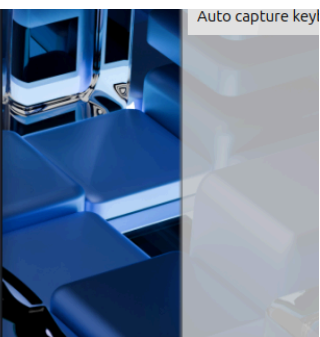
Noted in the directory scan for the web application enumeration, I discovered a picture in a directory named as secret. And found an image as shown

```
kali@kali: ~  
kali@kali: ~  
(kali@kali)-[~]  
$ dirb http://10.0.2.4/  
  
DIRB v2.22  
By The Dark Raver  
  
START_TIME: Fri May 30 11:21:59 2025  
URL_BASE: http://10.0.2.4/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
GENERATED WORDS: 4612  
  
— Scanning URL: http://10.0.2.4/ —  
  
⇒ DIRECTORY: http://10.0.2.4/backups/  
⇒ DIRECTORY: http://10.0.2.4/batch/  
⇒ DIRECTORY: http://10.0.2.4/core/  
⇒ DIRECTORY: http://10.0.2.4/css/  
+ http://10.0.2.4/favicon.ico (CODE:200|SIZE:894)  
⇒ DIRECTORY: http://10.0.2.4/images/  
+ http://10.0.2.4/index.php (CODE:200|SIZE:5802)  
⇒ DIRECTORY: http://10.0.2.4/install/  
⇒ DIRECTORY: http://10.0.2.4/js/  
+ http://10.0.2.4/robots.txt (CODE:200|SIZE:26)  
⇒ DIRECTORY: http://10.0.2.4/secret/  
+ http://10.0.2.4/server-status (CODE:403|SIZE:273)  
⇒ DIRECTORY: http://10.0.2.4/sf/  
⇒ DIRECTORY: http://10.0.2.4/template/  
⇒ DIRECTORY: http://10.0.2.4/uploads/  
  
— Entering directory: http://10.0.2.4/backups/ —  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)
```

```
kali@kali: ~  
kali@kali: ~  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
— Entering directory: http://10.0.2.4/sf/ —  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
— Entering directory: http://10.0.2.4/template/ —  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
— Entering directory: http://10.0.2.4/uploads/ —  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
— Entering directory: http://10.0.2.4/install/actions/ —  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
— Entering directory: http://10.0.2.4/install/css/ —  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
— Entering directory: http://10.0.2.4/install/images/ —  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
— Entering directory: http://10.0.2.4/install/lib/ —  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
— Entering directory: http://10.0.2.4/install/modules/ —  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
END_TIME: Fri May 30 11:22:12 2025  
DOWNLOADED: 9224 - FOUND: 5  
  
(kali@kali)-[~]
```

```
kali@kali: ~  
kali@kali: ~  
$ dirb http://10.0.2.4/  
  
DIRB v2.22  
By The Dark Raver  
  
START_TIME: Fri May 30 11:21:59 2025  
URL_BASE: http://10.0.2.4/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
GENERATED WORDS: 4612  
  
— Scanning URL: http://10.0.2.4/ —  
  
⇒ DIRECTORY: http://10.0.2.4/backups/  
⇒ DIRECTORY: http://10.0.2.4/batch/  
⇒ DIRECTORY: http://10.0.2.4/core/  
⇒ DIRECTORY: http://10.0.2.4/css/  
+ http://10.0.2.4/favicon.ico (CODE:200|SIZE:894)  
⇒ DIRECTORY: http://10.0.2.4/images/  
+ http://10.0.2.4/index.php (CODE:200|SIZE:5802)  
⇒ DIRECTORY: http://10.0.2.4/install/  
⇒ DIRECTORY: http://10.0.2.4/js/  
+ http://10.0.2.4/robots.txt (CODE:200|SIZE:26)  
⇒ DIRECTORY: http://10.0.2.4/secret/  
+ http://10.0.2.4/server-status (CODE:403|SIZE:273)  
⇒ DIRECTORY: http://10.0.2.4/sf/  
⇒ DIRECTORY: http://10.0.2.4/template/  
⇒ DIRECTORY: http://10.0.2.4/uploads/
```

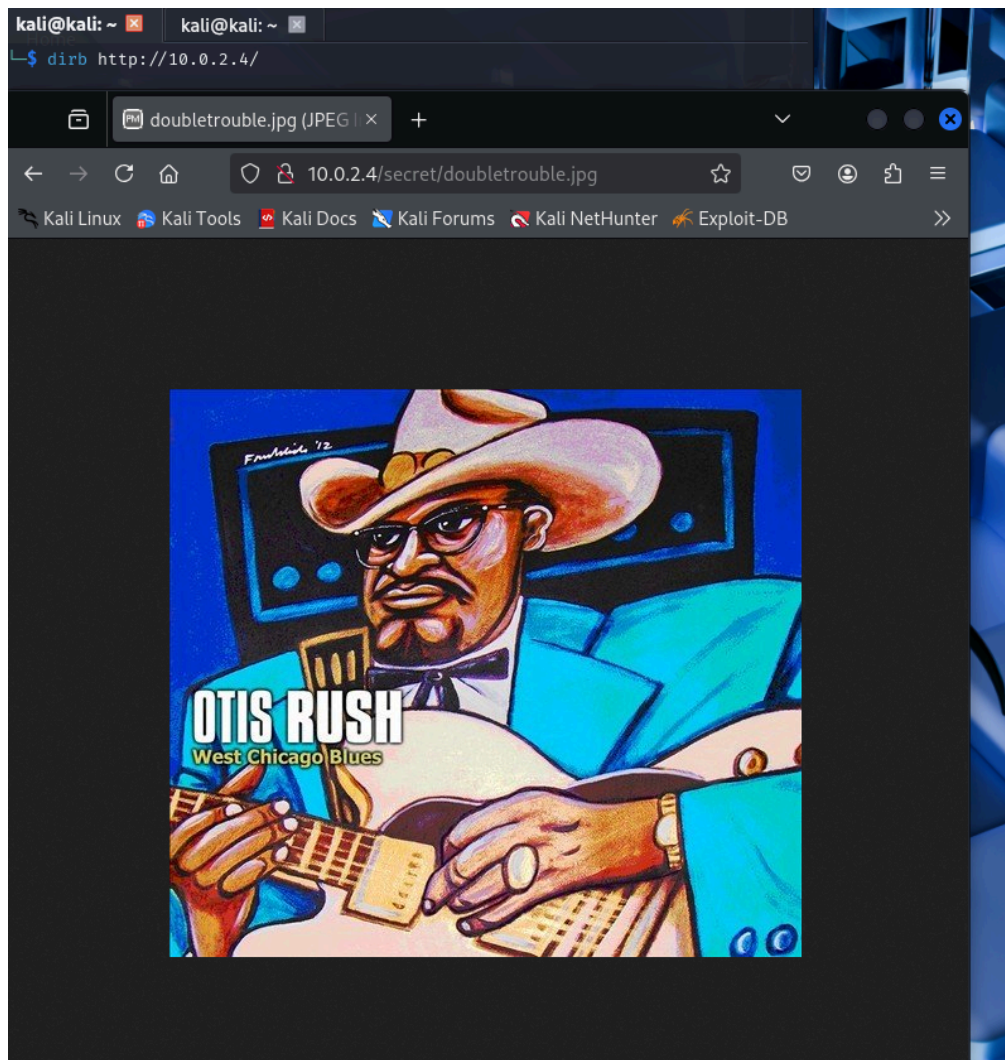
Auto capture key



Index of /secret

Name	Last modified	Size	Description
Parent Directory	-	-	-
doubletrouble.jpg	2021-09-11 10:39	81K	-

Apache/2.4.38 (Debian) Server at 10.0.2.4 Port 80



5) Cracking password with StegCracker

By installing and using Stegcracker to perform a password check on this picture file, `sudo apt install stegcracker` I noticed it was going to take a long time (5hrs) so I searched and found the tool Stegseek `sudo apt install stegcracker` instead and received valid credentials stored in a `creds.txt`, `doubletrouble.jpg.out`.

```

root@kali: /usr/share/wordlists
File Actions Edit View Help

(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) 2025 - 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'..
^C36/14344392 (0.02%) Attempted: candycane1
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

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

(root@kali)-[/usr/share/wordlists]

```



```
root@kali: /usr/share/wordlists
File Actions Edit View Help
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2025 - 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/sha
re/wordlists/rockyou.txt'..
^C36/14344392 (0.02%) Attempted: candycane1
Error: Aborted.

(root@kali)-[/usr/share/wordlists]
# stegseek /home/kali/Desktop/doubletrouble.jpg /usr/share/wordlists/rockyo
u.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]
# cat doubletrouble.jpg.out
otisrush@localhost.com
otis666

(root@kali)-[/usr/share/wordlists]
#
```

I then read the data in the doubletrouble.jpg.out file and used the data shown to log in and received a dashboard page as shown.

