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:

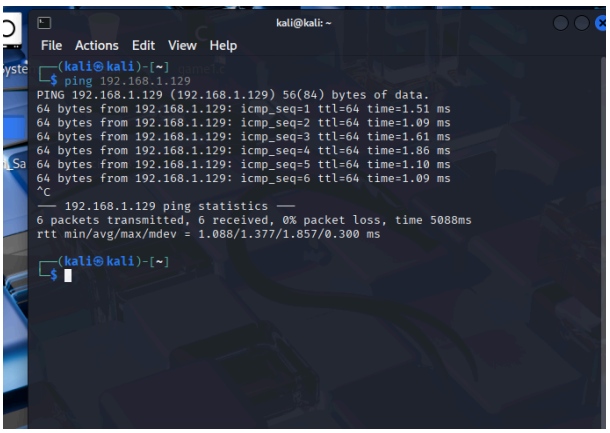
1. Accesso remoto SSH riuscito su un sistema obsoleto (Ubuntu 12.04.x).
2. Esposizione di metadati web tramite intestazione ETag.
3. Brute-force login riuscito con credenziali deboli via SSH.

Tutte le vulnerabilità sono state sfruttate con successo e documentate.

Verifica Connettività e Scansione Preliminare

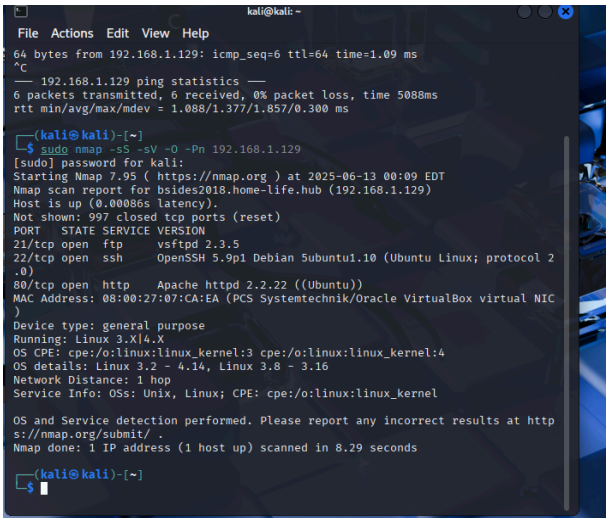
Verifica connettività tra Kali e la macchina target:

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



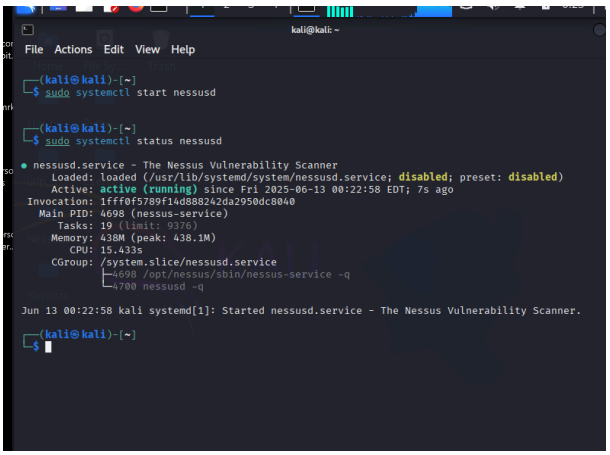
Scansione iniziale con Nmap:

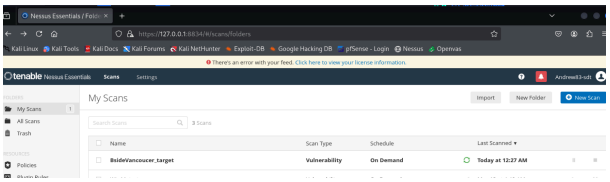
- Comando utilizzato: nmap -sS -sV -O -Pn 192.168.1.129
- Obiettivi: identificazione porte aperte, servizi attivi, sistema operativo.
- Porte rilevate: 21 (FTP) 22 (SSH), 80 (HTTP)



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.





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 Ubuntu Linux SEoL 12.04.x	Critica	Sistema operativo obsoleto non più supportato, esposto a vulnerabilità note.
2	Apache ETag Header	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

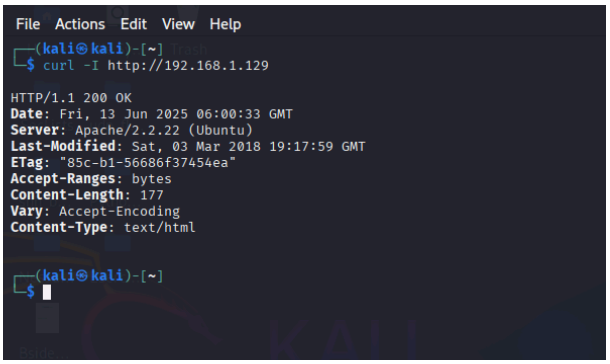
- Sistema: Ubuntu 12.04.x – EOL (End of Life)
- Servizio vulnerabile: OpenSSH 5.9p1
- Tecnica: Accesso remoto SSH con credenziali valide
- Credenziali trovate:
    - username: anne
    - password: princess
- Comando eseguito:
- **ssh anne@192.168.1.129**
- Conferma: Shell remota attiva con privilegi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

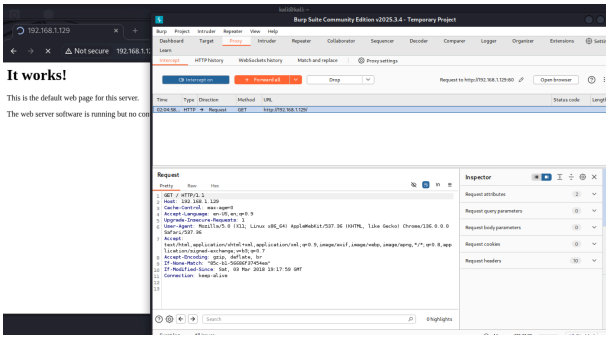
Impatto: Compromissione completa dell'host remoto.

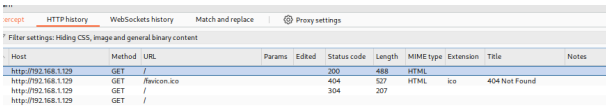
Apache ETag Header Disclosure – Fingerprinting

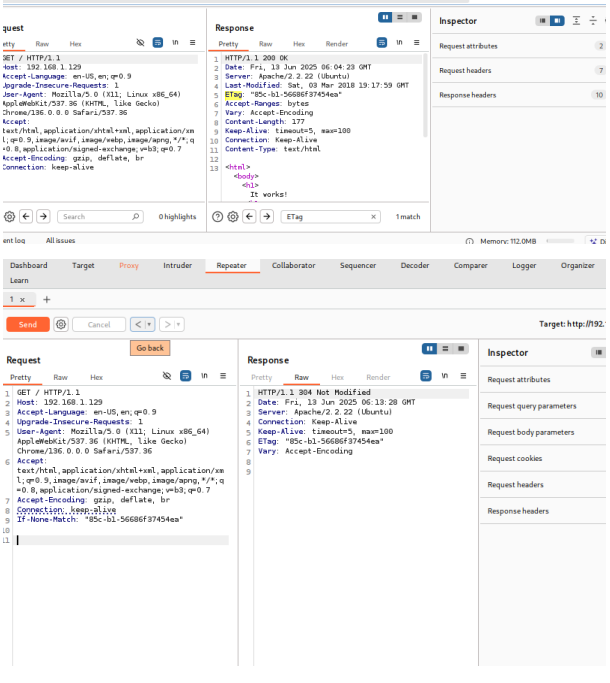
- Web server: Apache 2.2.22
- Metodo di rilevamento: Burp Suite
- Header ricevuto: **ETag: "85c-b1-56686f37454ea"**
- Procedura:
    - Richiesta con If-None-Match
    - Risposta 304 Not Modified → file invariato
- Rischio:
    - Tracciamento file statici
    - Analisi modifiche di contenuto
    - Bypass 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 con
Burp Suite Community Edition v2025.3.4 - Temporary Project


HTTP history
WebSockets history
Match and replace
Proxy settings
Filter settings: Hiding CSS, image and general binary content
Host Method URL Params Edited 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
http://192.168.1.129 GET /


Response
HTTP/1.1 200 OK
Date: Fri, 13 Jun 2025 06:04:23 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Sat, 03 Mar 2018 19:17:59 GMT
ETag: "85c-b1-56686f37454ea"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 177
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
<html>
<body>
<h1>
It works!
Inspector
Request attributes
Request headers
Response headers
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
Learn
Send Cancel
Go back
Request
GET / HTTP/1.1
Host: 192.168.1.129
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/136.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
If-None-Match: "85c-b1-56686f37454ea"
Response
HTTP/1.1 304 Not Modified
Date: Fri, 13 Jun 2025 06:13:28 GMT
Server: Apache/2.2.22 (Ubuntu)
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
ETag: "85c-b1-56686f37454ea"
Vary: Accept-Encoding
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers

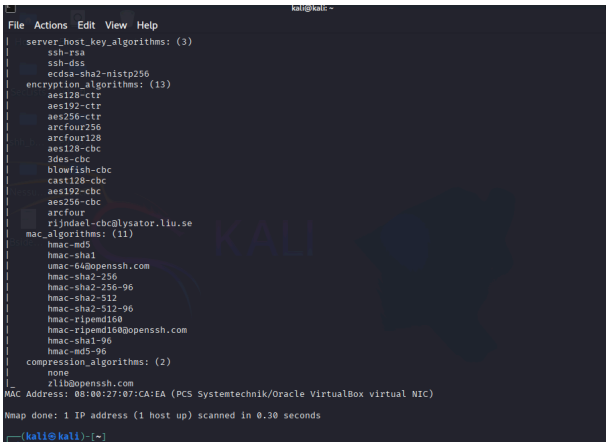
Hydra Brute-Force SSH – Attacco riuscito

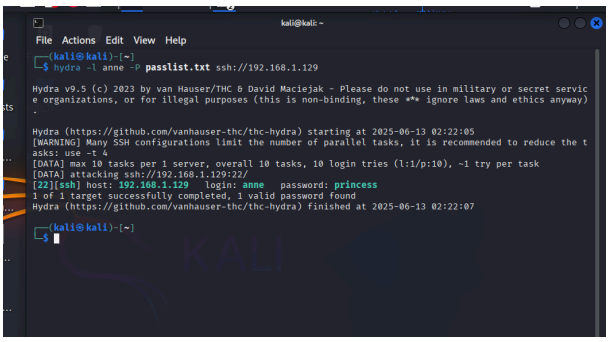
- Strumento: Hydra
- Obiettivo: Forzare password dell'utente anne
- Wordlist personalizzata (passlist.txt):

  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.





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