Vulnerability Assessment & Penetration Test Report

Redatto da: Antonio Piredda
Ruolo: Studente – Cyber Security & Ethical Hacking
Corso: Epicode – Cyber Security & Ethical Hacking
Data: 26 Gennaio 2026

Executive Summary

Il presente documento riporta i risultati delle attività di Vulnerability Assessment (VA) e Penetration Testing (PT) condotte sulla macchina bersaglio *BSides Vancouver 2018 Workshop*, simulando uno scenario **realistico di attacco Black Box**, in cui l'analista non dispone di informazioni preliminari sull'infrastruttura analizzata.

L'obiettivo del test è stato quello di valutare il livello di esposizione del sistema a potenziali minacce, identificare vulnerabilità e debolezze di configurazione e fornire raccomandazioni concrete per la riduzione del rischio.

Le attività hanno evidenziato la presenza di più superfici d'attacco, legate principalmente a servizi non necessari, software obsoleto e informazioni esposte pubblicamente. Pur non essendo stato possibile ottenere un accesso non autorizzato al sistema, le vulnerabilità riscontrate potrebbero, in uno scenario reale, facilitare attacchi più avanzati qualora non adeguatamente mitigate.

Nel complesso, il sistema presenta un livello di sicurezza di base discreto, ma migliorabile attraverso l'adozione delle remediation proposte, che consentirebbero di ridurre significativamente il rischio complessivo.

Scope e Metodologia

Scope

- Sistema bersaglio: **BSides Vancouver 2018 Workshop**
- Tipologia di test: **Black Box Vulnerability Assessment & Penetration Test**
- Attaccante: Kali Linux
- Ambiente: rete virtualizzata e isolata

Metodologia

L'attività è stata suddivisa nelle seguenti fasi:

1. Host Discovery
2. Port Scanning
3. Service & Version Detection

4. Vulnerability Assessment
5. Tentativi di Penetration Testing
6. Analisi dei risultati e definizione delle remediation

Descrizione dell'Ambiente

Il laboratorio di test è stato configurato in un ambiente virtualizzato e isolato. L'attaccante utilizza una macchina Kali Linux, mentre il sistema bersaglio è una macchina virtuale basata su Linux Ubuntu. Le due macchine sono collegate alla stessa rete privata, senza accesso diretto a Internet.

Attività di Reconnaissance

Host Discovery

È stata eseguita una fase di host discovery tramite ARP scanning al fine di individuare i sistemi attivi sulla rete. L'attività ha portato all'identificazione di un host attivo all'indirizzo IP **192.168.50.101**, riconducibile a una macchina virtuale.

Port Scanning e Service Enumeration

Attraverso una scansione completa delle porte TCP sono stati individuati i seguenti servizi esposti:

- **21/tcp – FTP (vsftpd 2.3.5)**
- **22/tcp – SSH (OpenSSH 5.9p1)**
- **80/tcp – HTTP (Apache 2.2.22)**

L'analisi delle versioni dei servizi ha evidenziato l'utilizzo di componenti non aggiornati, potenzialmente vulnerabili.

Vulnerabilità Identificate

Riepilogo delle vulnerabilità

Vulnerabilità	Rischio	Stato	Remediation
FTP anonimo attivo	Medio	Aperta	Disabilitare accesso anonimo o rimuovere il servizio

Vulnerabilità	Rischio	Stato	Remediation
Directory di backup esposta	Medio	Aperta	Rimuovere o proteggere le directory sensibili
WordPress obsoleto	Medio-Alto	Aperta	Aggiornare o dismettere l'installazione
User enumeration possibile	Medio	Aperta	Disabilitare enumerazione utenti
XML-RPC attivo	Medio	Aperta	Disabilitare o limitare l'accesso
Servizi e software obsoleti	Medio	Aperta	Applicare patch e aggiornamenti

---

1. FTP anonimo attivo

Descrizione: Il servizio FTP consente l'accesso anonimo senza autenticazione.

Impatto: Un attaccante può enumerare directory e file esposti, ottenendo informazioni utili per attacchi successivi.

Rischio: Medio

Remediation:

- Disabilitare l'accesso FTP anonimo
- Limitare l'accesso al servizio tramite autenticazione forte o rimuovere il servizio se non necessario

---

2. Directory sensibile esposta via HTTP

Descrizione: Il file robots.txt indica la presenza della directory /backup_wordpress, contenente un'installazione WordPress dismessa e accessibile pubblicamente.

Impatto: Espone informazioni sull'architettura applicativa e aumenta la superficie d'attacco.

Rischio: Medio

Remediation:

- Rimuovere directory di backup non necessarie
- Limitare l'accesso tramite autenticazione o restrizioni IP

---

3. WordPress obsoleto

Descrizione: L'installazione WordPress individuata risulta obsoleta e non più mantenuta.

Impatto: Versioni obsolete possono contenere vulnerabilità note sfruttabili.

Rischio: Medio-Alto

Remediation:

- Aggiornare WordPress all'ultima versione stabile
- Rimuovere installazioni non più utilizzate

---

4. User Enumeration possibile

Descrizione: È stato possibile identificare utenti validi dell'installazione WordPress (admin, john) tramite tecniche di user enumeration.

Impatto: Facilita attacchi di brute force e credential stuffing.

Rischio: Medio

Remediation:

- Disabilitare l'enumerazione degli utenti
- Utilizzare username non prevedibili

---

5. XML-RPC attivo

Descrizione: Il file xmlrpc.php risulta accessibile.

Impatto: XML-RPC può essere sfruttato per attacchi di forza bruta e amplificazione.

Rischio: Medio

Remediation:

- Disabilitare XML-RPC se non necessario
- Limitare le richieste tramite firewall o plugin di sicurezza

---

6. Servizi e software obsoleti

Descrizione: Apache, OpenSSH e altri componenti risultano non aggiornati.

Impatto: Possibile esposizione a vulnerabilità note.

Rischio: Medio

Remediation:

- Aggiornare regolarmente il sistema operativo e i servizi
- Implementare un piano di patch management

Tentativi di Penetration Testing

Sono stati effettuati tentativi di accesso mirati al servizio SSH utilizzando gli utenti identificati. L'accesso tramite password è risultato disabilitato e il servizio accetta esclusivamente autenticazione tramite chiave pubblica, indicando una configurazione di sicurezza corretta.

Non è stato possibile ottenere un accesso non autorizzato al sistema.

Bonus – Scansione Automatizzata (Nessus)

A completamento dell'analisi manuale, è stata eseguita una scansione automatizzata tramite Nessus con finalità di verifica e confronto dei risultati. La scansione ha confermato la presenza di servizi obsoleti e potenziali debolezze già individuate durante l'analisi manuale.

Conclusioni

L'attività di Vulnerability Assessment e Penetration Testing ha evidenziato diverse debolezze di configurazione e superfici d'attacco, pur non portando alla compromissione del sistema.

Il sistema presenta una sicurezza di base discreta, in particolare per quanto riguarda il servizio SSH, ma risulta penalizzato dalla presenza di servizi non necessari, software obsoleto e informazioni esposte pubblicamente.

L'implementazione delle remediation suggerite consentirebbe di ridurre significativamente il rischio complessivo e migliorare il livello di sicurezza del sistema.

Appendice Tecnica

La presente appendice contiene gli screenshot e gli output completi delle attività svolte durante il Vulnerability Assessment e Penetration Test. Gli elementi sono organizzati in ordine cronologico e associati alle fasi metodologiche descritte nel report.

Per ciascuno screenshot è fornita una breve didascalia descrittiva, utile a contestualizzare l'attività svolta.

Appendice A – Host Discovery e Configurazione Rete

Figura A.1 – Verifica della configurazione di rete della macchina attaccante (Kali Linux) e identificazione dell'indirizzo IP.

```
┌──(pireddone㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ca:84:07 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::ce23:4b09:b272:ea2f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:4b:ae brd ff:ff:ff:ff:ff:ff
```

Figura A.2 – Attività di host discovery tramite ARP scanning per l'individuazione del sistema bersaglio.

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.50.101  08:00:27:22:6f:91      1      60  PCS Systemtechnik GmbH
```

Appendice B – Port Scanning e Service Enumeration

Figura B.1 – Scansione completa delle porte TCP del sistema bersaglio.

```
┌──(pireddone㉿kali)-[~]
└─$ nmap -sS -p- 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-24 10:30 CET
Nmap scan report for 192.168.50.101
Host is up (0.00021s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:22:6F:91 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.48 seconds
```

Figura B.2 – Analisi dei servizi e delle versioni rilevate tramite service detection.

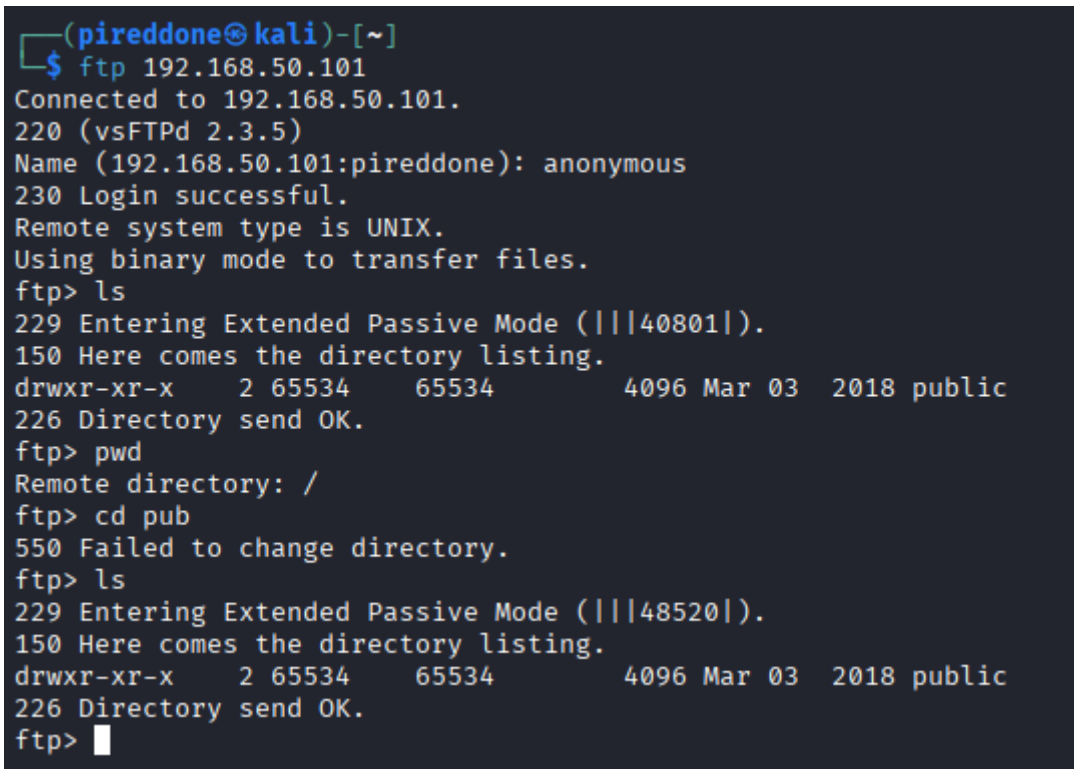
```
┌──(pireddone㉿kali)-[~]
└─$ nmap -sV -sC -A 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-24 10:32 CET
Nmap scan report for 192.168.50.101
Host is up (0.00075s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      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
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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
MAC Address: 08:00:27:22:6F:91 (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
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.75 ms 192.168.50.101

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 22.62 seconds
```

Appendice C – FTP Enumeration

Figura C.1 – Accesso al servizio FTP tramite autenticazione anonima e verifica dei permessi disponibili.



Appendice D – HTTP e WordPress Enumeration

Figura D.1 – Analisi del file robots.txt e individuazione della directory sensibile.

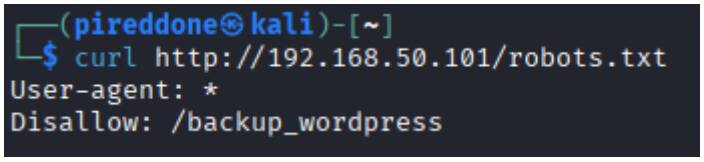


Figura D.2 – Directory enumeration del servizio HTTP tramite brute-force controllato.

```
┌──(pireddone㉿kali)-[~]
└─$ gobuster dir -u http://192.168.50.101 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.50.101
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 291]
/.hta                 (Status: 403) [Size: 286]
/.htaccess            (Status: 403) [Size: 291]
/cgi-bin/             (Status: 403) [Size: 290]
/index                (Status: 200) [Size: 177]
/index.html           (Status: 200) [Size: 177]
/robots.txt           (Status: 200) [Size: 43]
/robots               (Status: 200) [Size: 43]
/server-status        (Status: 403) [Size: 295]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
```

Figura D.3 – Accesso alla directory /backup_wordpress e identificazione dell'installazione WordPress.

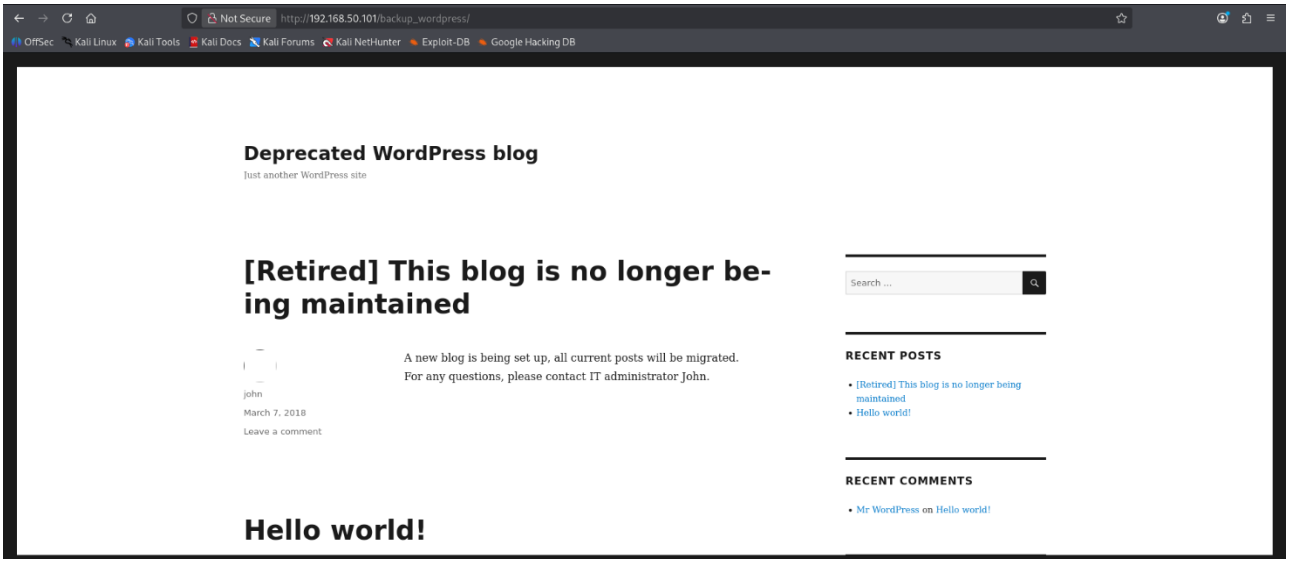


Figura D.4 – Tentativi di individuazione di file di configurazione WordPress.

```
┌──(pireddone㉿kali)-[~]
└─$ curl -i http://192.168.50.101/backup_wordpress/wp-config.php
HTTP/1.1 200 OK
Date: Mon, 26 Jan 2026 17:12:17 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Vary: Accept-Encoding
Content-Length: 0
Content-Type: text/html


┌──(pireddone㉿kali)-[~]
└─$ curl -i http://192.168.50.101/backup_wordpress/wp-config.php~
HTTP/1.1 404 Not Found
Date: Mon, 26 Jan 2026 17:12:26 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 309
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /backup_wordpress/wp-config.php~ was not found on this server.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 192.168.50.101 Port 80</address>
</body></html>

┌──(pireddone㉿kali)-[~]
└─$ curl -i http://192.168.50.101/backup_wordpress/wp-config.php.bak
HTTP/1.1 404 Not Found
Date: Mon, 26 Jan 2026 17:12:45 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 312
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /backup_wordpress/wp-config.php.bak was not found on this server.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 192.168.50.101 Port 80</address>
</body></html>
```

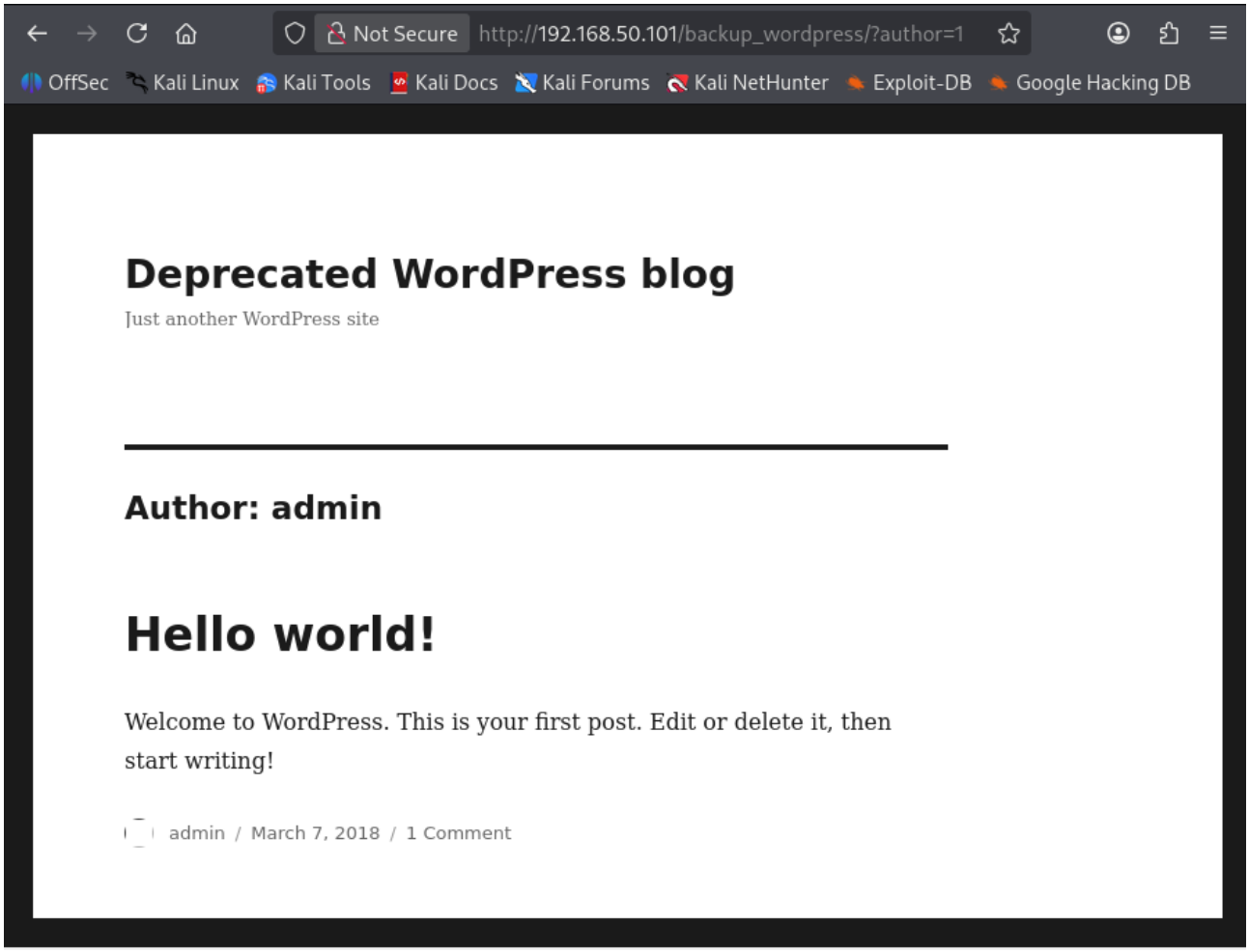
```
┌──(pireddone㉿kali)-[~]
└─$ curl -i http://192.168.50.101/backup_wordpress/wp-config.php.old
HTTP/1.1 404 Not Found
Date: Mon, 26 Jan 2026 17:12:56 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 312
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /backup_wordpress/wp-config.php.old was not found on this server.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 192.168.50.101 Port 80</address>
</body></html>
```

```
┌──(pireddone㉿kali)-[~]
└─$ gobuster dir \
> -u http://192.168.50.101/backup_wordpress \
> -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.50.101/backup_wordpress
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 303]
/.htaccess           (Status: 403) [Size: 308]
/.htpasswd           (Status: 403) [Size: 308]
/license             (Status: 200) [Size: 19935]
/readme              (Status: 200) [Size: 7358]
/wp-admin            (Status: 301) [Size: 336] [--> http://192.168.50.101/backup_wordpress/wp-admin/]
/wp-content          (Status: 301) [Size: 338] [--> http://192.168.50.101/backup_wordpress/wp-content/]
/wp-includes         (Status: 301) [Size: 339] [--> http://192.168.50.101/backup_wordpress/wp-includes/]
/wp-settings         (Status: 500) [Size: 0]
/index.php           (Status: 301) [Size: 0] [--> http://192.168.50.101/backup_wordpress/]
/index               (Status: 301) [Size: 0] [--> http://192.168.50.101/backup_wordpress/index/]
/wp-config           (Status: 200) [Size: 0]
/wp-cron             (Status: 200) [Size: 0]
/wp-load             (Status: 200) [Size: 0]
/wp-links-opml       (Status: 200) [Size: 233]
/wp-blog-header      (Status: 200) [Size: 0]
/wp-login            (Status: 200) [Size: 2373]
/wp-mail             (Status: 500) [Size: 3368]
/wp-signup           (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?action=register]
/wp-trackback        (Status: 200) [Size: 135]
/xmlrpc              (Status: 405) [Size: 42]
/xmlrpc.php          (Status: 405) [Size: 42]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
```

Appendice E – User Enumeration e XML-RPC

Figura E.1 – Identificazione degli utenti WordPress tramite tecniche di user enumeration.



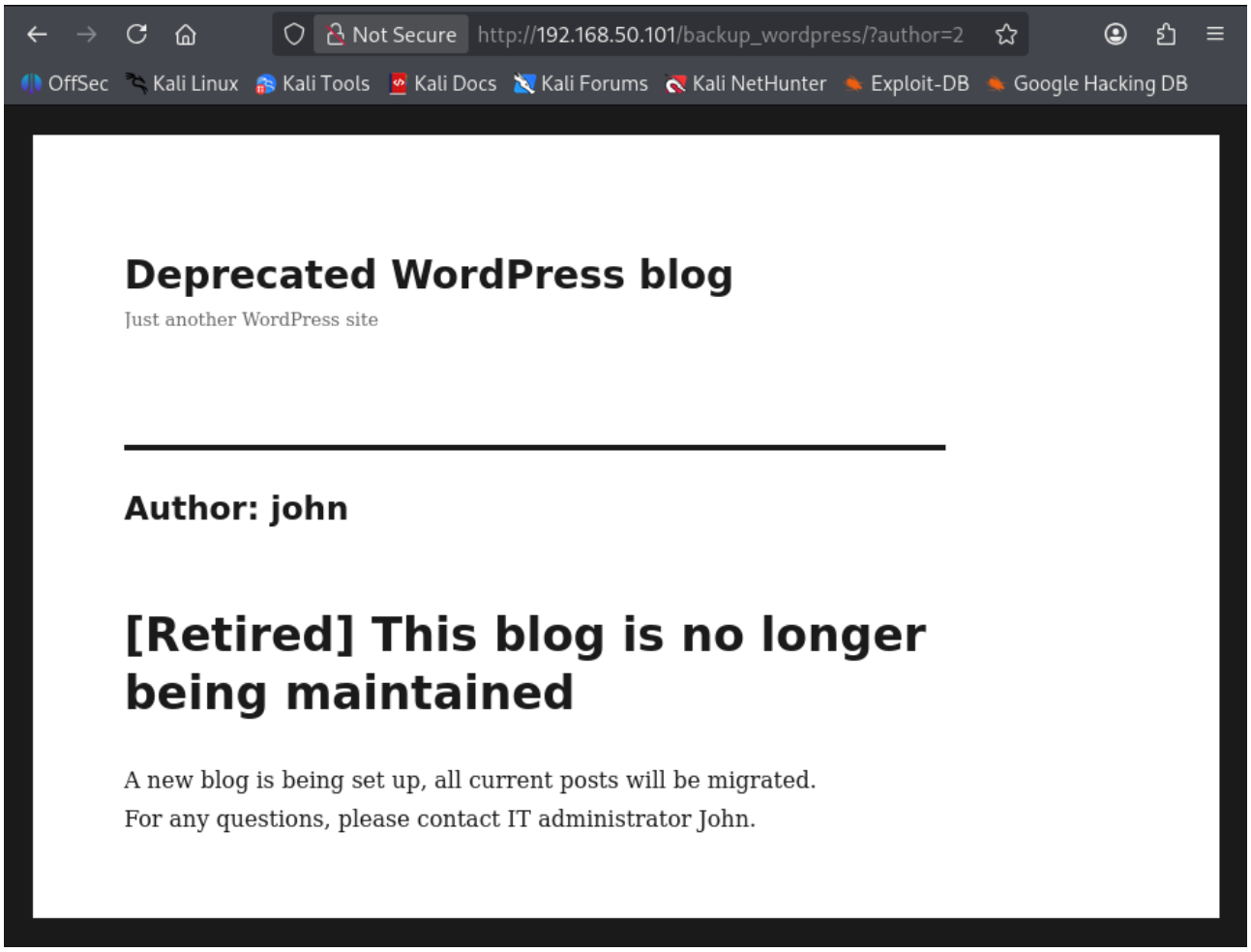


Figura E.2 – Verifica della disponibilità del servizio XML-RPC.

```
┌──(pireddone㉿kali)-[~]
└─$ curl -i http://192.168.50.101/backup_wordpress/xmlrpc.php
HTTP/1.1 405 Method Not Allowed
Date: Mon, 26 Jan 2026 17:33:09 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Allow: POST
Vary: Accept-Encoding
Content-Length: 42
Content-Type: text/plain

XML-RPC server accepts POST requests only.
```

Appendice F – Tentativi di Accesso SSH

Figura F.1 – Tentativo di accesso SSH all'utente identificato e risposta del servizio.

```
┌──(pireddone㉿kali)-[~]
└─$ ssh john@192.168.50.101
The authenticity of host '192.168.50.101 (192.168.50.101)' 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 '192.168.50.101' (ECDSA) to the list of known hosts.
john@192.168.50.101: Permission denied (publickey).
```

Appendice G – Scansione Automatizzata (Bonus)

Figura G.1 – Risultati della scansione automatizzata Nessus (panoramica delle vulnerabilità).

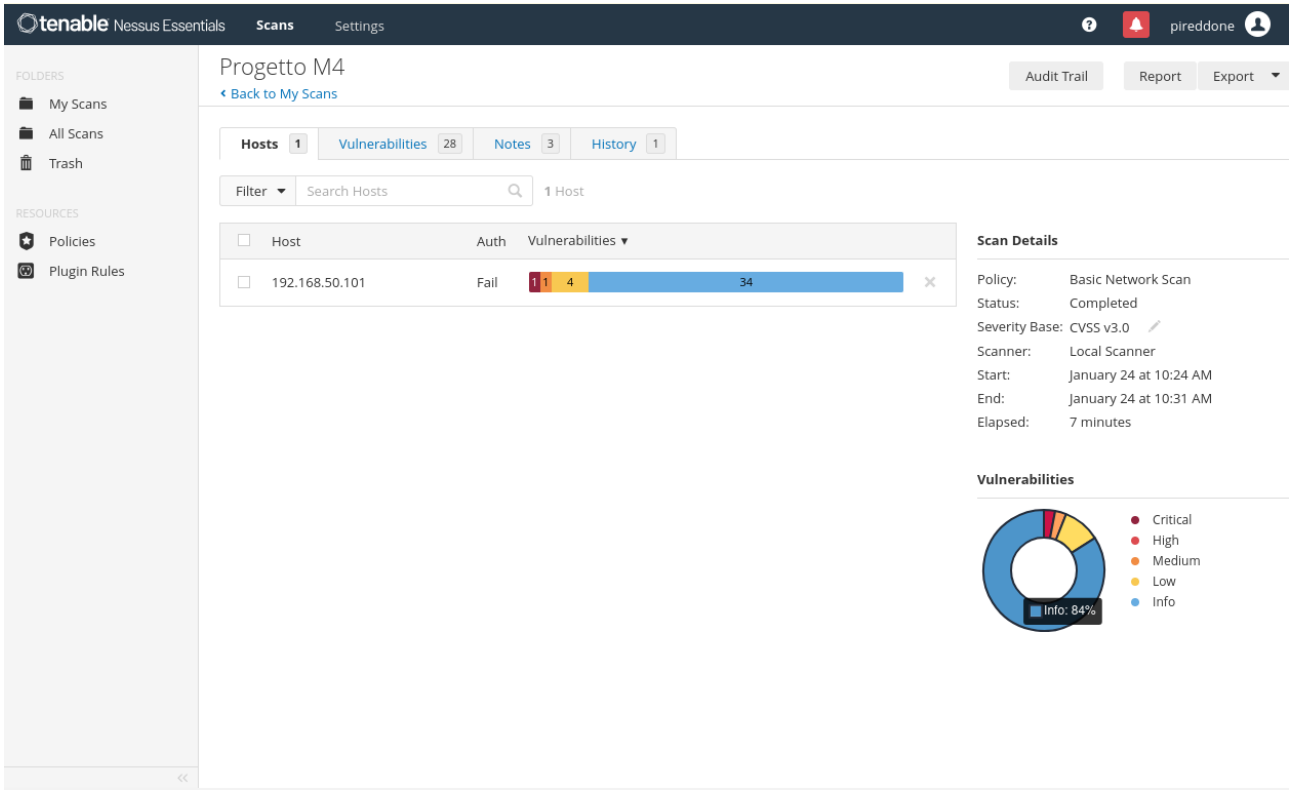


Figura G.2 – Dettaglio delle principali segnalazioni emerse dalla scansione Nessus.