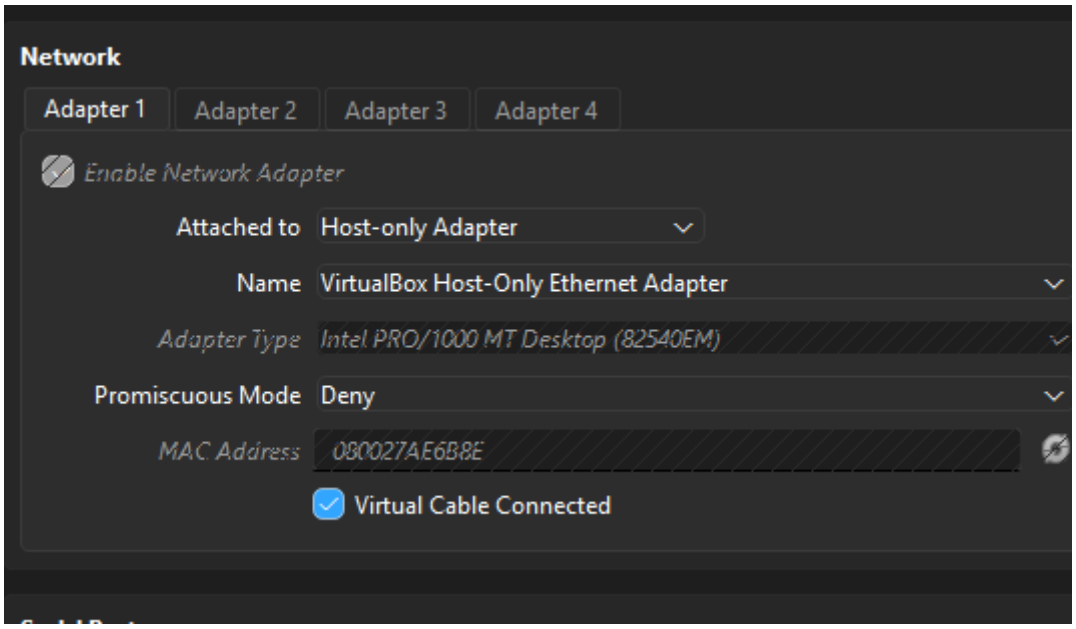
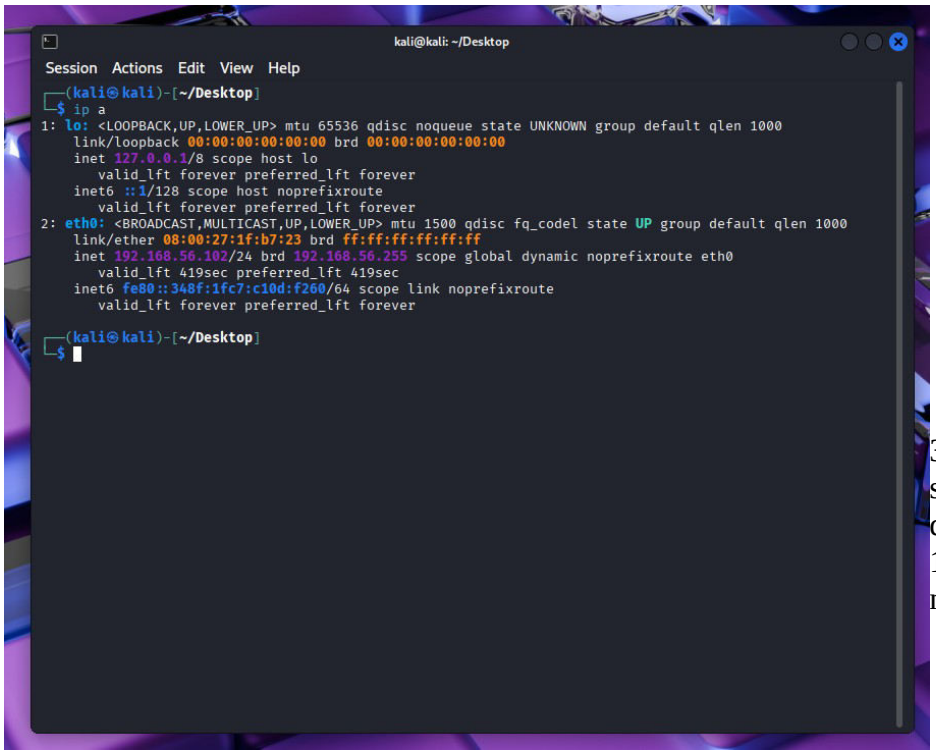
W16d4- FRANCESCO MONTALTO

1. Ho scaricato la macchina virtuale vulnerabile BSides Vancouver 2018 in formato OVA, ed ho preparato l'ambiente di lavoro avviando correttamente la macchina Kali Linux e la macchina bersaglio BSides Vancouver. Ho configurato la rete delle macchine virtuali in modalità Host-only per consentire la comunicazione diretta tra Kali Linux e la macchina bersaglio all'interno di un ambiente isolato.

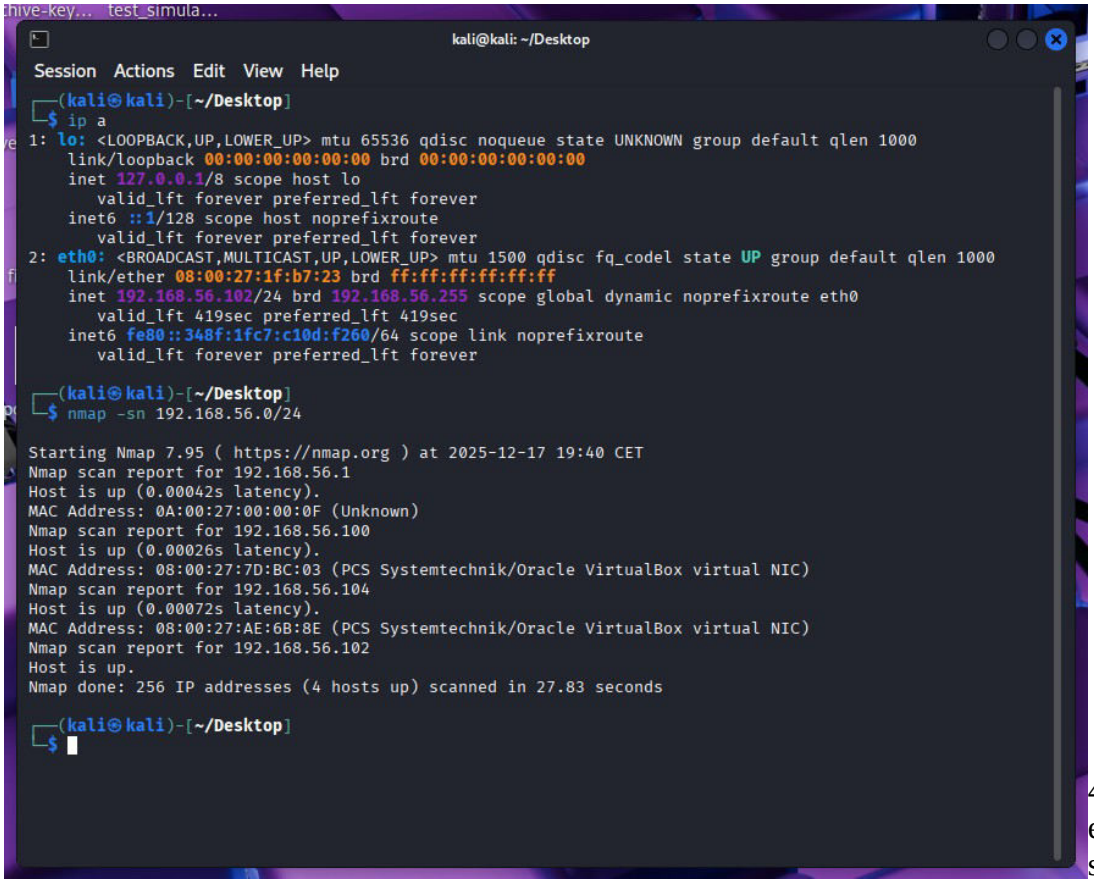


2. Ho configurato la rete delle macchine Kali Linux e BSides Vancouver 2018 in modalità Host-only, utilizzando lo stesso adattatore di rete del virtualizzatore. In questo modo ho creato un ambiente isolato, in cui l'attaccante e il bersaglio possono comunicare direttamente senza accesso alla rete esterna.
Ho verificato la configurazione di rete della macchina Kali Linux controllando l'indirizzo IP assegnato all'interfaccia di rete. Ho riscontrato che Kali si trova sulla subnet 192.168.56.0/24, informazione necessaria per eseguire correttamente la scansione della rete e individuare la macchina bersaglio.



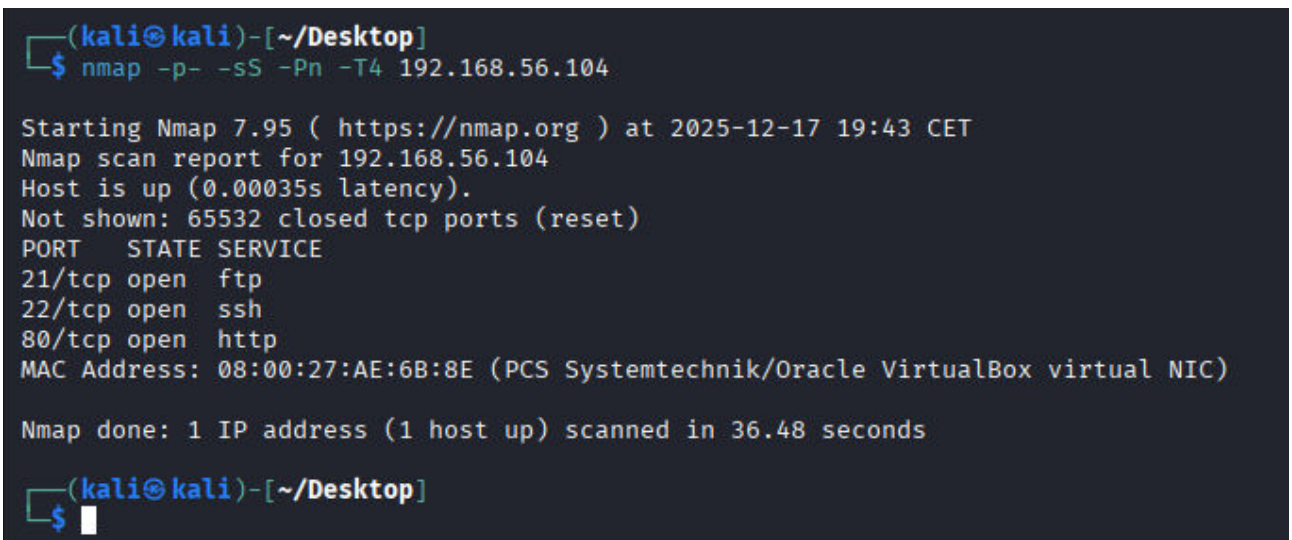
3. Ho eseguito una scansione di network discovery sulla subnet 192.168.56.0/24 dalla macchina Kali Linux per

individuare gli host attivi presenti sulla rete. Grazie a questa scansione ho identificato correttamente l’indirizzo IP della macchina bersaglio BSides Vancouver 2018, pari a 192.168.56.104.



4. Ho eseguito una scansione completa delle porte TCP della macchina bersaglio utilizzando Nmap. La scansione ha evidenziato la presenza di tre porte aperte, corrispondenti ai servizi FTP (porta 21), SSH (porta 22) e HTTP (porta 80), che rappresentano la superficie di attacco del sistema.

5. Ho eseguito una fase di enumerazione dei servizi individuati sulla macchina bersaglio utilizzando Nmap. L’analisi ha evidenziato la presenza di un servizio FTP vsftpd 2.3.5 con accesso anonimo



abilitato, un servizio SSH OpenSSH 5.9p1 e un server web Apache 2.2.22. Tra questi, il servizio FTP è risultato particolarmente interessante in quanto consente l'accesso senza autenticazione e permette l'esplorazione di una directory pubblica.

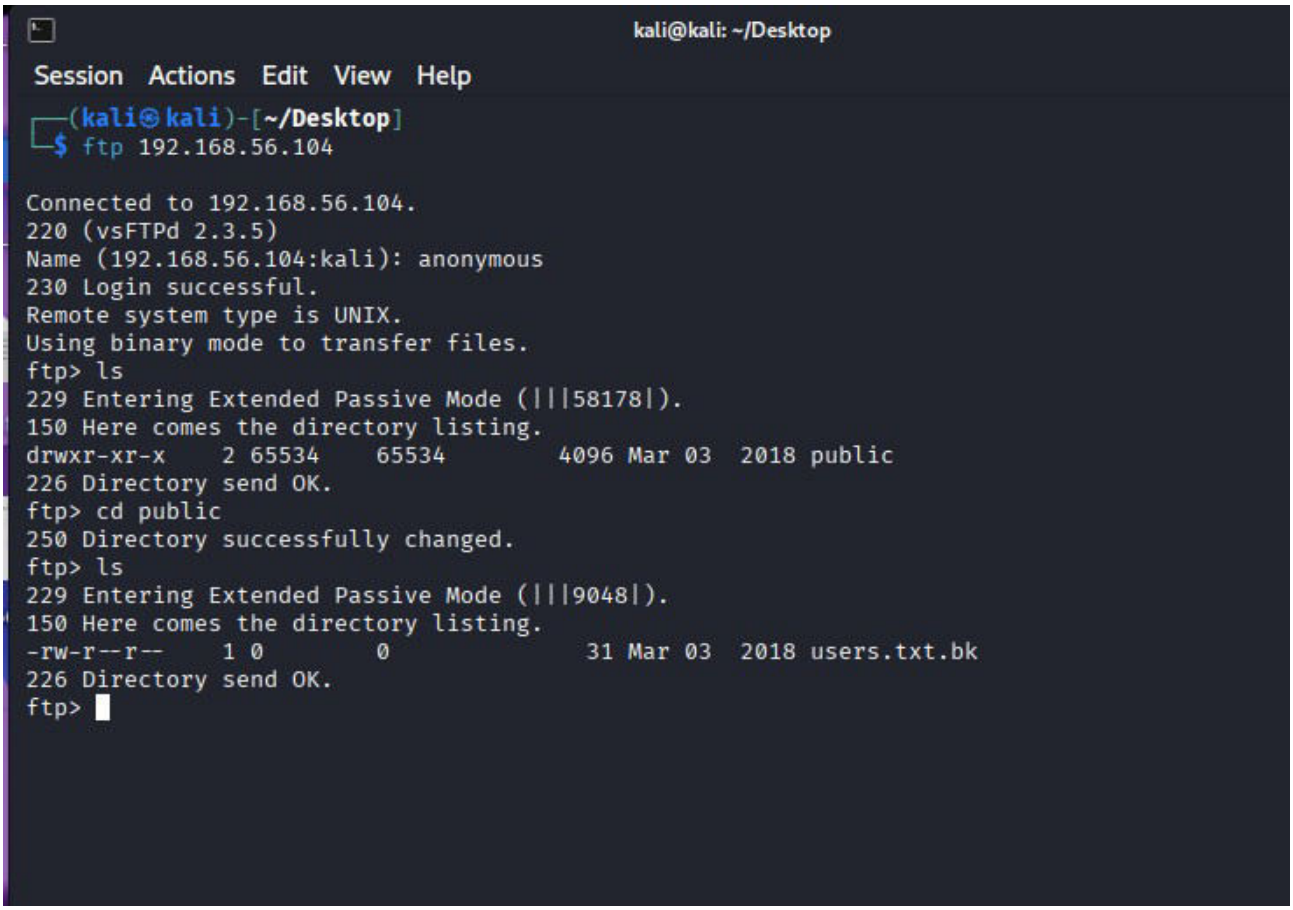
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sC -sV -Pn -p 21,22,80 192.168.56.104

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 19:47 CET
Nmap scan report for 192.168.56.104
Host is up (0.0013s latency).

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 192.168.56.102
|      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 4
|      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:AE:6B:8E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.94 seconds
```

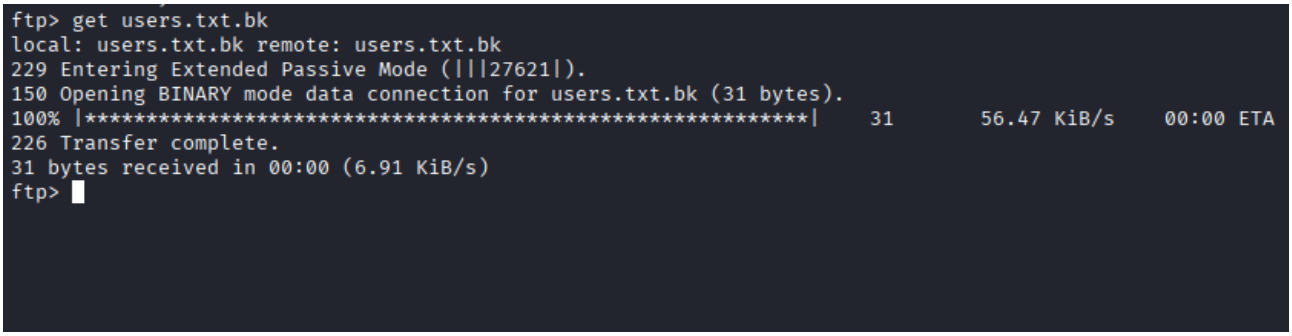
6. Ho effettuato l’accesso al servizio FTP della macchina bersaglio utilizzando l’utente anonimo, poiché il server consentiva il login senza l’inserimento di credenziali. Dopo l’accesso, ho elencato le directory disponibili e ho esplorato la directory pubblica con l’obiettivo di individuare eventuali file o informazioni accessibili che potessero risultare utili per le successive fasi del test.



Una volta effettuato l’accesso, ho elencato le directory disponibili e ho individuato una directory denominata “public”, accessibile all’utente anonimo.

Ho quindi esplorato la directory “public” e ho identificato la presenza di un file denominato “users.txt.bk”, presumibilmente un file di backup. La presenza di un file di questo tipo accessibile pubblicamente rappresenta una configurazione non sicura, in quanto potrebbe contenere informazioni sensibili utili per compromettere ulteriormente il sistema. Questa fase ha permesso di individuare una potenziale vulnerabilità senza la necessità di sfruttare exploit o credenziali valide.

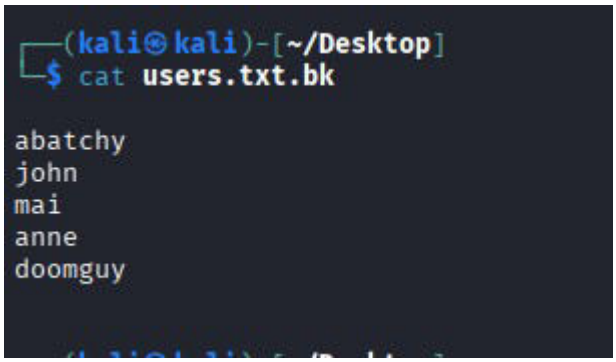
7. Dopo aver individuato un file di backup denominato “users.txt.bk” all’interno della directory pubblica del servizio FTP, ho scaricato il file sulla macchina Kali Linux utilizzando il comando di trasferimento FTP. L’operazione è stata eseguita con successo utilizzando l’account anonimo, senza la necessità di autenticazione.



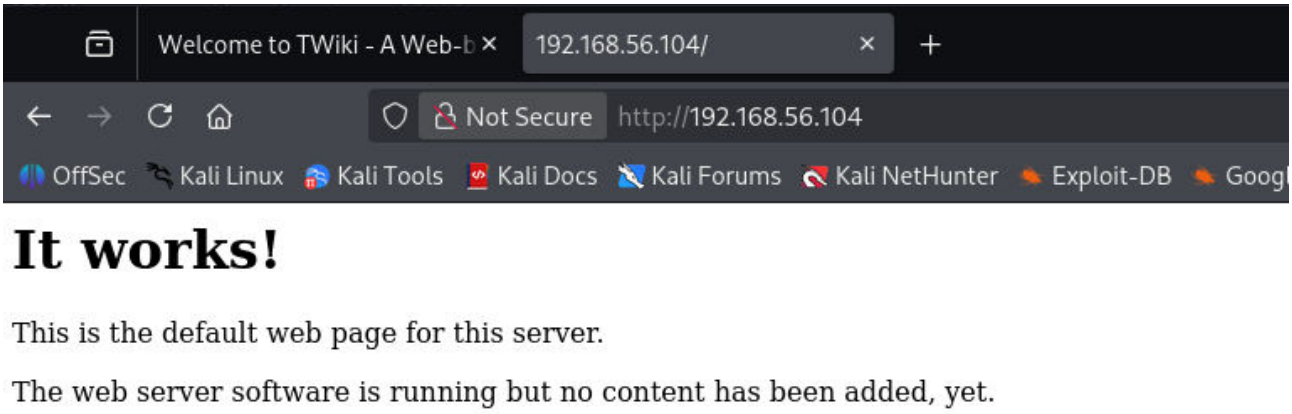
Questo passaggio ha dimostrato che il server FTP consente a utenti non autenticati di scaricare file dal sistema, esponendo potenzialmente informazioni sensibili. La presenza di un file di backup accessibile pubblicamente rappresenta una configurazione non sicura e costituisce una vulnerabilità che può facilitare ulteriori fasi di compromissione del sistema.

8. Dopo aver scaricato il file “users.txt.bk” dal servizio FTP sulla macchina Kali Linux, ho analizzato il contenuto del file in locale. L’analisi ha evidenziato la presenza di una lista di nomi utente, tra cui “abatchy”, “john”, “mai”, “anne” e “doomguy”.

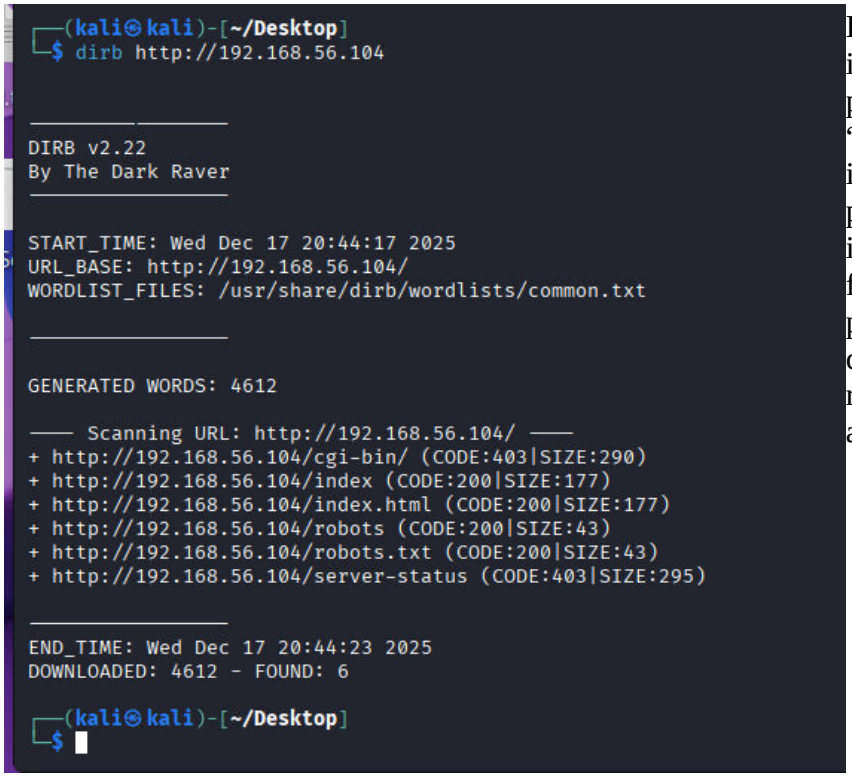
Sebbene il file non contenesse password, la divulgazione di nomi utente rappresenta comunque una vulnerabilità di tipo information disclosure, in quanto tali informazioni possono essere utilizzate per facilitare attacchi mirati contro altri servizi esposti sulla macchina, come SSH o applicazioni web. La possibilità di ottenere queste informazioni tramite accesso anonimo al servizio FTP evidenzia una configurazione non sicura del sistema.



9. Ho effettuato una prima analisi manuale del servizio HTTP accedendo alla root del server tramite browser. La pagina visualizzata risulta essere la pagina di default di Apache, indicando che il web server è correttamente in esecuzione ma che il contenuto applicativo non è esposto sulla directory principale.

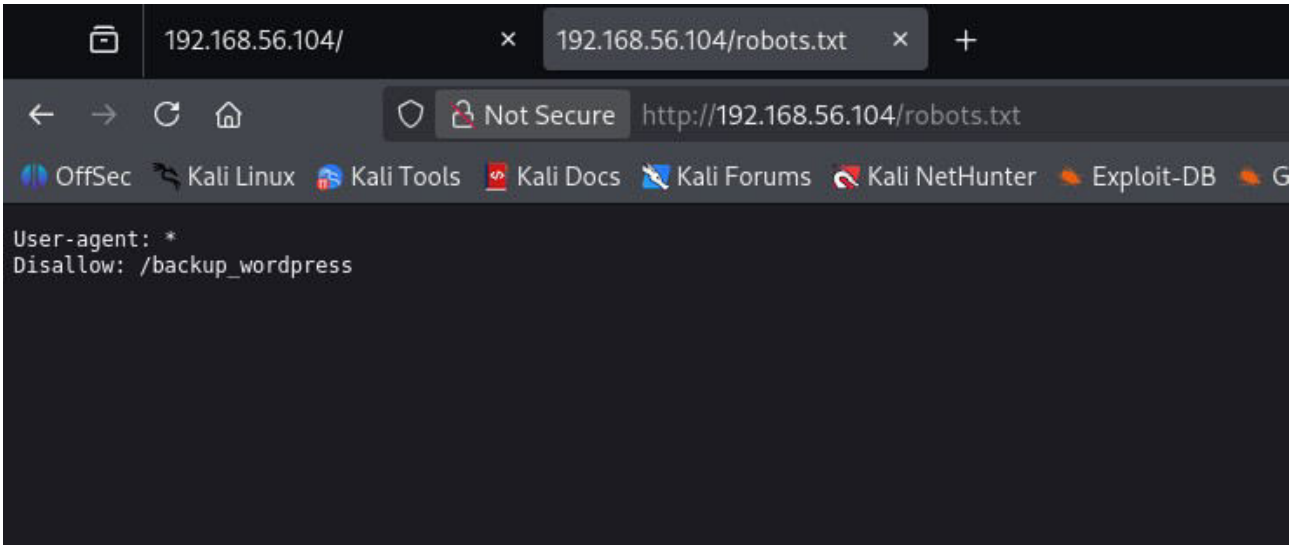


10. Dopo aver identificato il servizio HTTP attivo sulla porta 80 e aver verificato che la root del sito mostrava la pagina di default di Apache, ho eseguito una fase di enumerazione delle directory utilizzando lo strumento Dirb. L'obiettivo era individuare eventuali directory o file nascosti contenenti l'applicazione web reale o risorse sensibili.

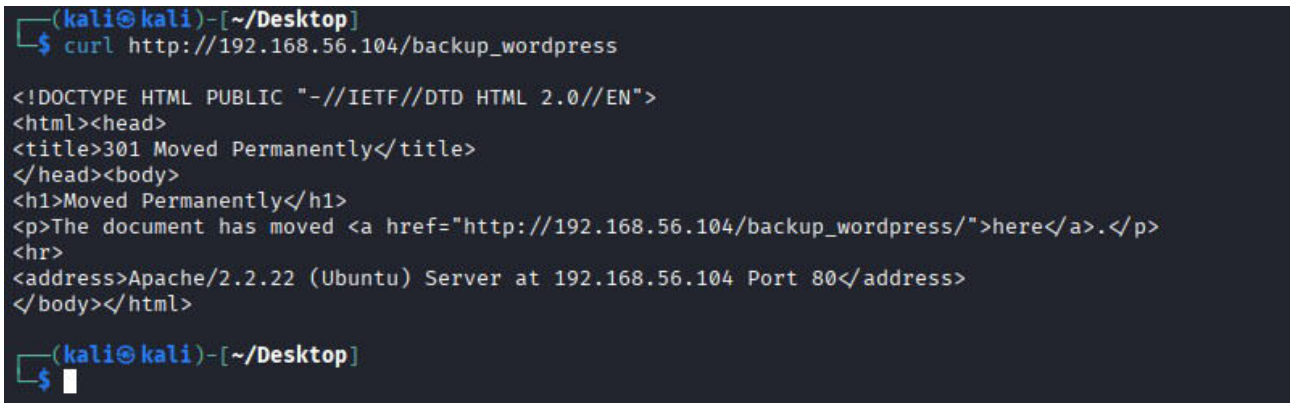


L'enumerazione ha permesso di identificare diverse risorse, tra cui la presenza dei percorsi "/cgi-bin/" e "/server-status", entrambi protetti ma indicativi di una configurazione potenzialmente sensibile. È stata inoltre individuata la presenza del file "robots.txt", accessibile pubblicamente, che potrebbe contenere riferimenti a directory o risorse non esposte direttamente all'utente.

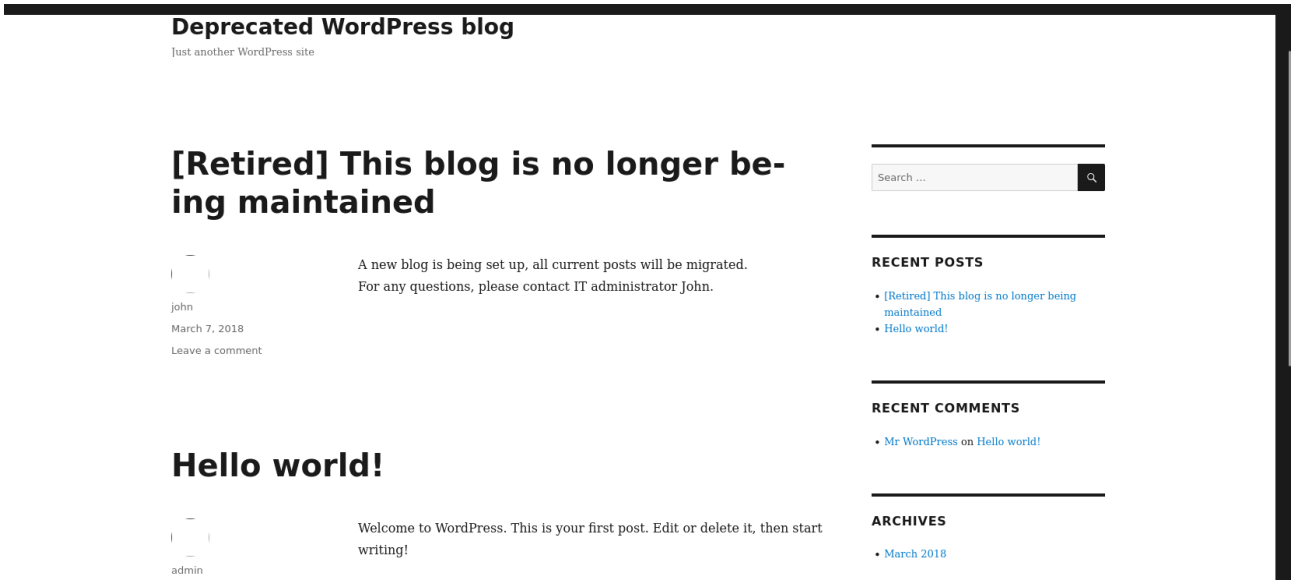
11.Durante la fase di enumerazione del servizio HTTP ho analizzato il file robots.txt, individuando un percorso esplicitamente escluso dall'indicizzazione, denominato "/backup_wordpress". La presenza di tale riferimento suggerisce l'esistenza di una directory contenente dati di backup relativi a WordPress, potenzialmente contenente informazioni sensibili o file di configurazione. Poiché il file robots.txt non rappresenta un meccanismo di sicurezza, il percorso risulta comunque accessibile a un attaccante.



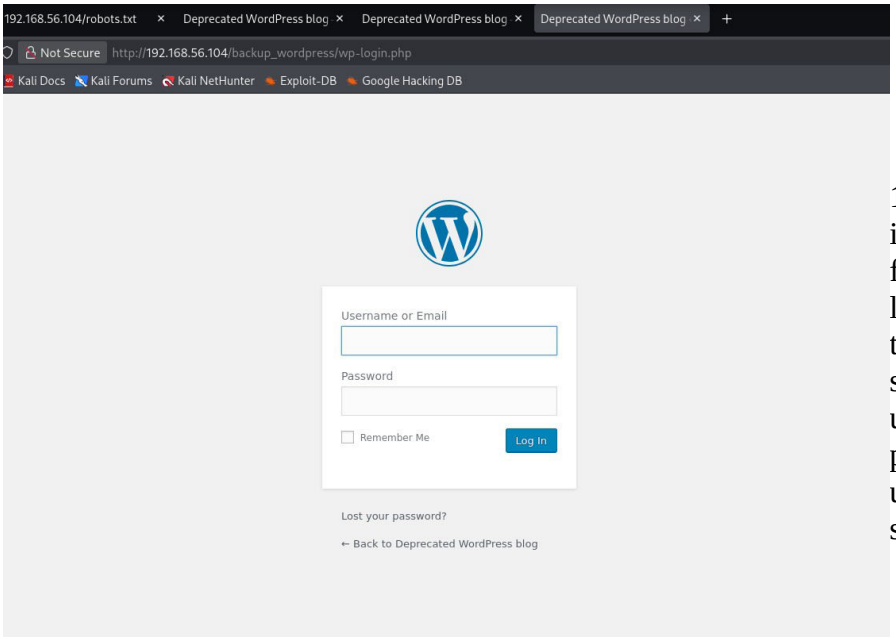
12. Dopo aver individuato il percorso "/backup_wordpress" tramite il file robots.txt, ho verificato manualmente l'accessibilità della directory. Il server ha risposto con un redirect HTTP 301 verso "/backup_wordpress/", confermando l'esistenza della directory e indicando che si tratta di una risorsa valida sul server web.



13. Accedendo alla directory “/backup_wordpress/” ho individuato un’installazione WordPress accessibile pubblicamente. Il sito risulta dichiarato come non più mantenuto, suggerendo la possibile presenza di vulnerabilità note non corrette. All’interno dei contenuti è inoltre presente un riferimento all’amministratore IT “John”, confermando la validità di uno degli utenti precedentemente individuati tramite l’analisi del servizio FTP.



14. Accedendo alla directory di backup individuata tramite il file robots.txt, ho identificato un’installazione WordPress non mantenuta e accessibile pubblicamente. L’applicazione espone la pagina di autenticazione wp-login.php, confermando la presenza di un punto di ingresso per utenti registrati. Considerando la precedente enumerazione degli utenti e la mancanza di manutenzione dichiarata del sistema, l’applicazione risulta potenzialmente vulnerabile ad attacchi di autenticazione e compromissione applicativa.Sebbene l’applicazione WordPress fosse attaccabile tramite diverse tecniche (brute force, analisi dei file di backup o compromissione applicativa), tali approcci non sono stati perseguiti in quanto non necessari al raggiungimento dell’obiettivo principale dell’esercizio, ovvero l’accesso alla macchina bersaglio.

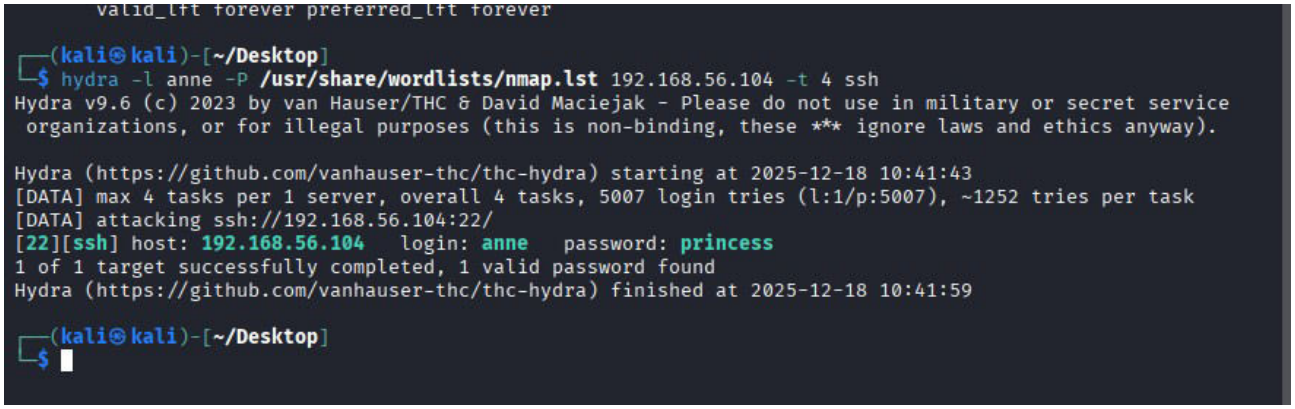


15. Considerando le informazioni raccolte nelle fasi precedenti, in particolare la lista di nomi utente ottenuta tramite l’accesso anonimo al servizio FTP e la presenza di un servizio SSH esposto sulla porta 22, ho deciso di tentare un attacco di forza bruta sul servizio SSH.

L’obiettivo era verificare se uno degli utenti individuati utilizzasse credenziali deboli o riutilizzate

Come ho strutturato il comando?

hydra
strumento per l’esecuzione di attacchi di autenticazione automatizzati



-l anne
specifica un singolo username

-P /usr/share/wordlists/nmap.lst
wordlist di password comuni
l’uso di una lista standard simula un attaccante che sfrutta password deboli o riutilizzate

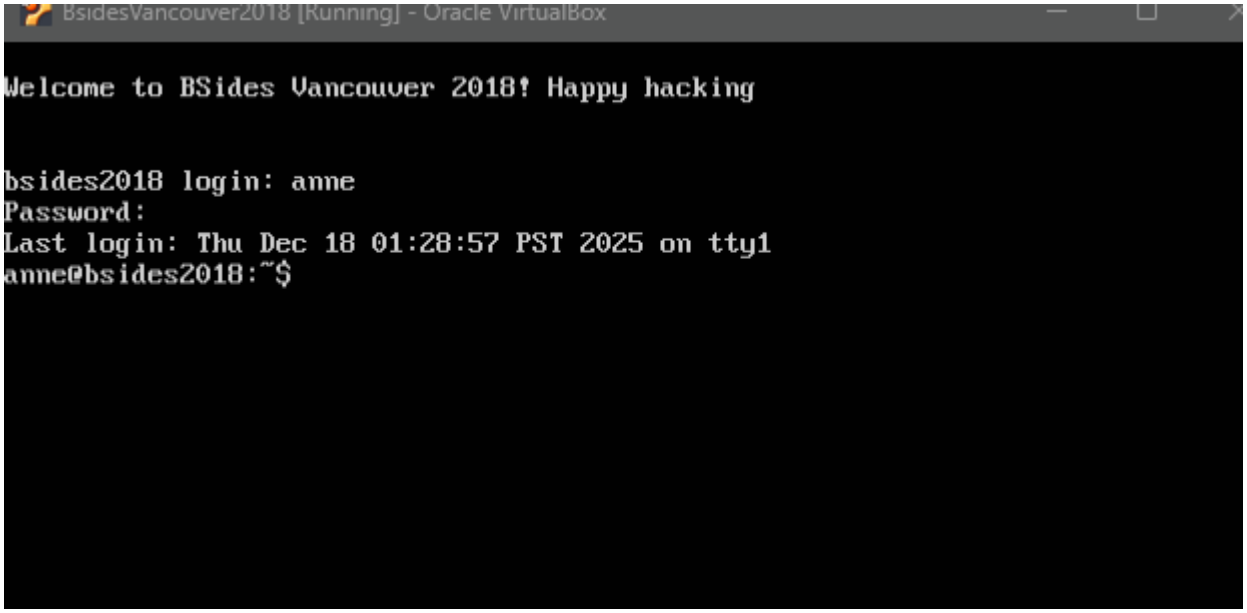
192.168.56.104
indirizzo IP della macchina bersaglio

-t 4
numero di thread simultanei
valore moderato per evitare blocchi o instabilità del servizio

ssh
specifica che l’attacco è diretto al servizio SSH

Stando ai risultati, la password è “princess”.

16. Ho tentato, con successo.


BsidesVancouver2018 [Running] - Oracle VirtualBox
Welcome to BSides Vancouver 2018! Happy hacking
bsides2018 login: anne
Password:
Last login: Thu Dec 18 01:28:57 PST 2025 on tty1
anne@bsides2018:~$