PROGETTO EXTRA:

Penetration test con metodo Black-Box

Introduzione

Il presente documento è dedicato all'analisi tecnica e alle attività di Penetration Testing eseguite sulla macchina virtuale target, denominata **"BSides Vancouver 2018"**. L'obiettivo primario di questa attività è la valutazione della sicurezza del sistema attraverso la simulazione di un attacco reale. Lo scopo finale è l'identificazione di eventuali vulnerabilità critiche che potrebbero compromettere la confidenzialità, l'integrità e la disponibilità del sistema.

Scenario

L'analisi è stata condotta adottando l'approccio **BlackBox**. Questa metodologia prevede che l'analista operi senza accesso preventivo a informazioni sull'infrastruttura, sulle configurazioni software o sulle credenziali di accesso. Tale approccio simula accuratamente le azioni di un attaccante esterno o di un utente malintenzionato interno (*Insider Threat*) che cerca di espandere il proprio raggio d'azione all'interno della rete aziendale.

Le fasi del test hanno seguito lo standard operativo tipico del Penetration Testing:

- **Information Gathering & Network Scanning**
- **Vulnerability Assessment**

- **Exploitation**
- **Privilege Escalation**
- **Reporting**

Obiettivi del progetto

Gli obiettivi primari sono:

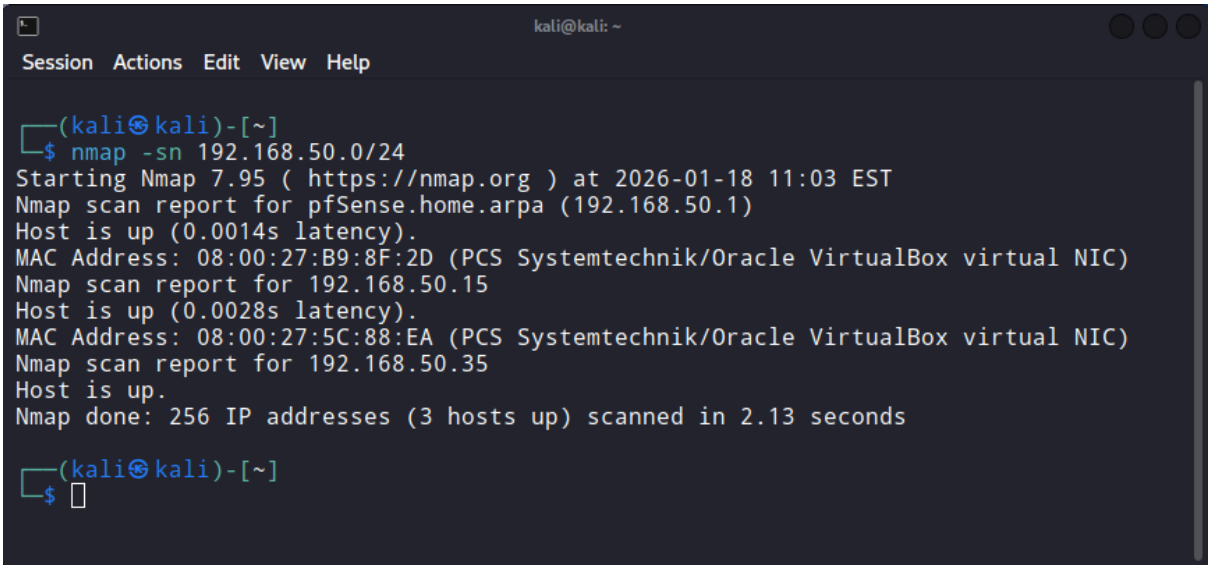
- **Enumerazione completa:** Mappare l'intera superficie di attacco esposta dal target.
- **Compromissione del sistema (Root):** Ottenere i privilegi amministrativi massimi (root) sul sistema target.

Prima fase: Information Gathering

Il nostro primo obiettivo è individuare la macchina nella rete e capire quali "porte" sono state lasciate aperte.

È stata effettuata una fase iniziale di Host Discovery utilizzando una scansione (***nmap -sn***) sull'intera sottorete per identificare l'indirizzo IP del target attivo, minimizzando il traffico di rete generato.

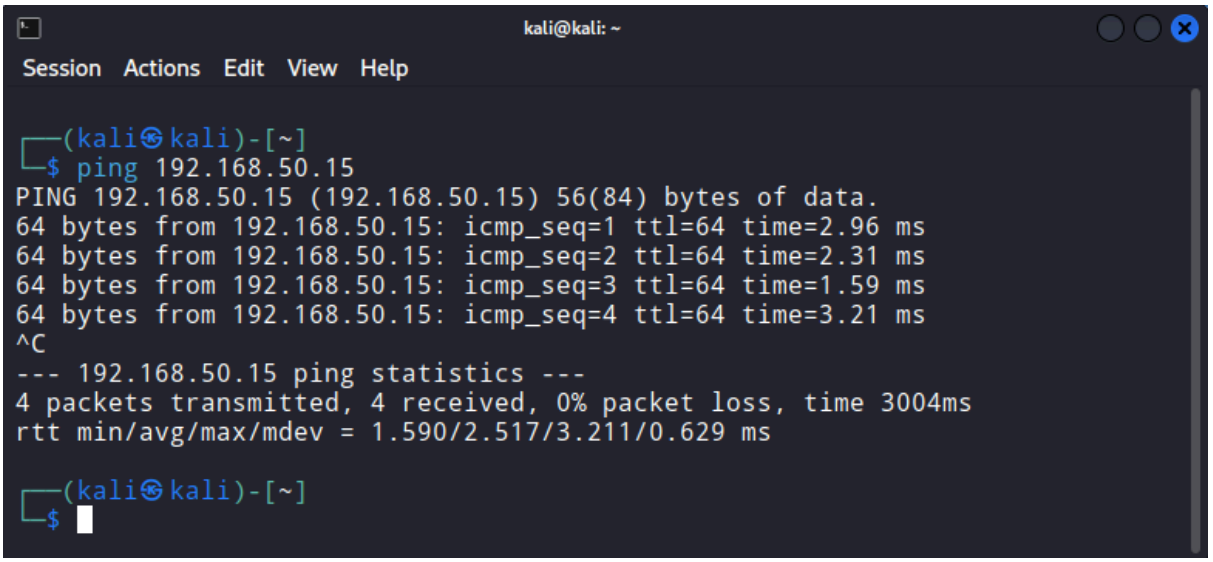
Risultato: Ip target trovato



Ip target: 192.168.50.15

Successivamente è stato effettuato un'operazione di tipo **ping** per verificare l'effettiva connessione con la macchina target:

Ping andato a buon fine



Scansione delle porte

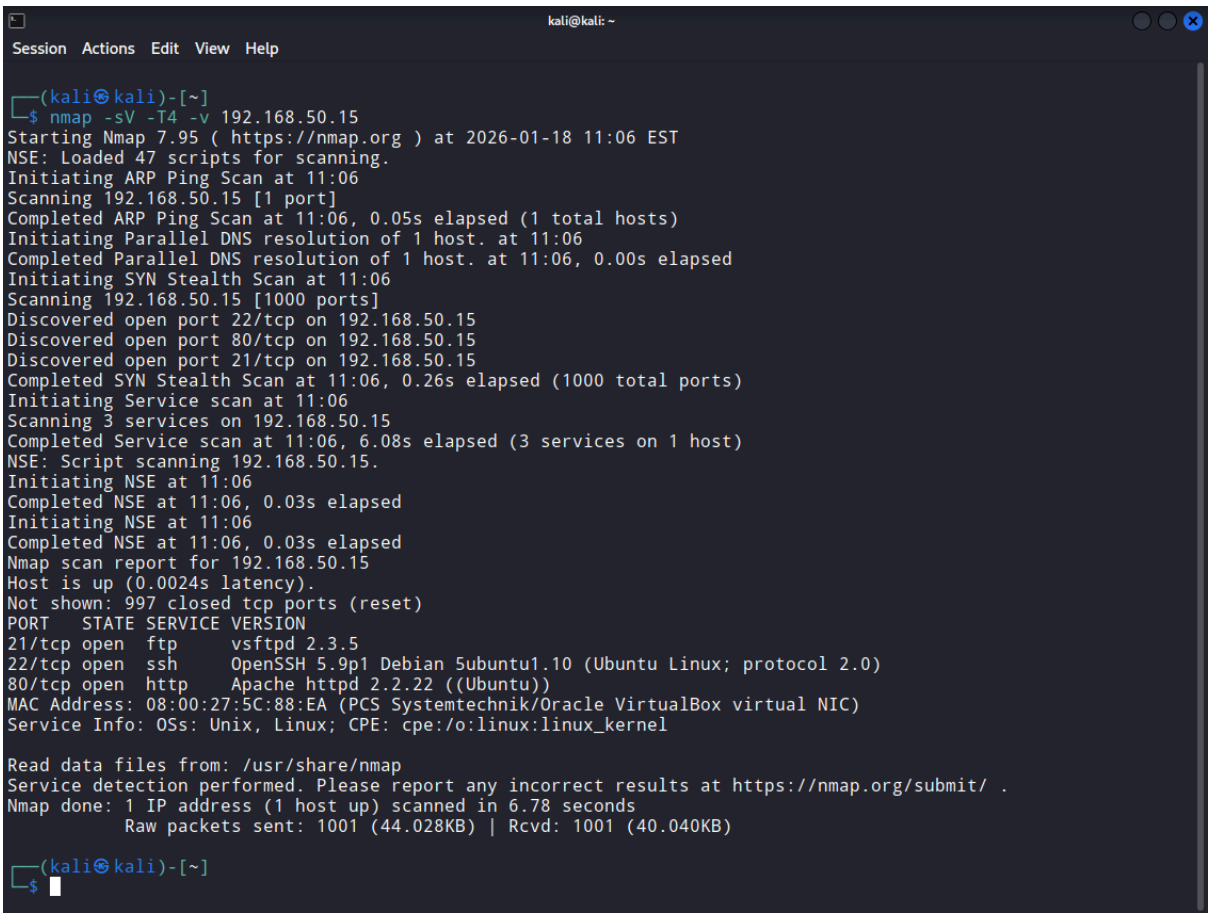
Una volta identificato l'indirizzo IP del target (192.168.50.15), è stata condotta una scansione approfondita delle porte **TCP** per mappare la superficie di attacco. L'obiettivo di questa fase è identificare i servizi in ascolto, le versioni del software in uso e potenziali configurazioni di default insicure.

È stato utilizzato lo strumento Nmap, in particolare è stato lanciato il seguente comando:

nmap -sV -T4 - v 192.168.50.15

Al fine di ottenere una panoramica immediata dei servizi principali esposti, è stata eseguita una scansione mirata sulle **Top 1.000 Porte TCP.** È stato utilizzato il flag **-T4** per ottimizzare le tempistiche di risposta in rete locale e il flag **-sV** per identificare le versioni specifiche dei demoni in ascolto, dato essenziale per la successiva fase di Vulnerability Assessment.

Risultato scansione



Riepilogo scansione

Porta	Stato	Servizio
21	Aperta	vsftpd
22	Aperta	ssh
80	Aperta	http

L'analisi iniziale dei servizi esposti dal sistema target ha rivelato un'importante configurazione errata sul servizio **FTP** (File Transfer Protocol), attivo sulla **porta 21**. Tale vulnerabilità ha consentito un accesso non autorizzato al **filesystem** remoto e la conseguente esfiltrazione di dati sensibili, inclusi file contenenti informazioni riservate sugli utenti del sistema.

Test di Accesso Anonimo (Anonymous Login)

È stato tentato l'accesso al servizio utilizzando le credenziali predefinite che spesso vengono lasciate attive per errore o negligenza amministrativa.

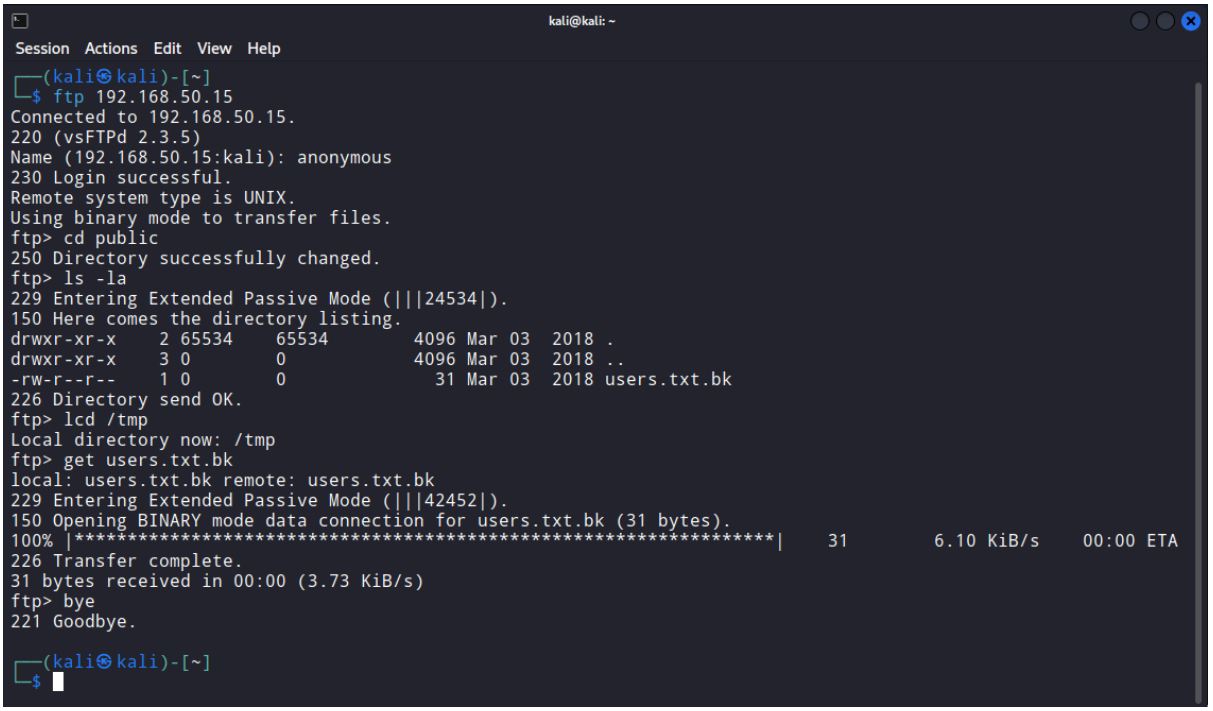
- **Comando:** `ftp 192.168.50.15`
- **User:** `anonymous`
- **Risultato:** Il server ha risposto con codice *230 Login successful,* garantendo l'accesso in lettura al server.

Navigazione ed Esplorazione (Directory Traversal)

Una volta stabilita la connessione, è stata eseguita una ricognizione della struttura delle directory.

- Il comando `ls -la` ha rivelato la presenza di una directory non standard denominata `public`.
- Accedendo alla directory (`cd public`), è stato individuato un file di backup sospetto denominato `users.txt.bk`.

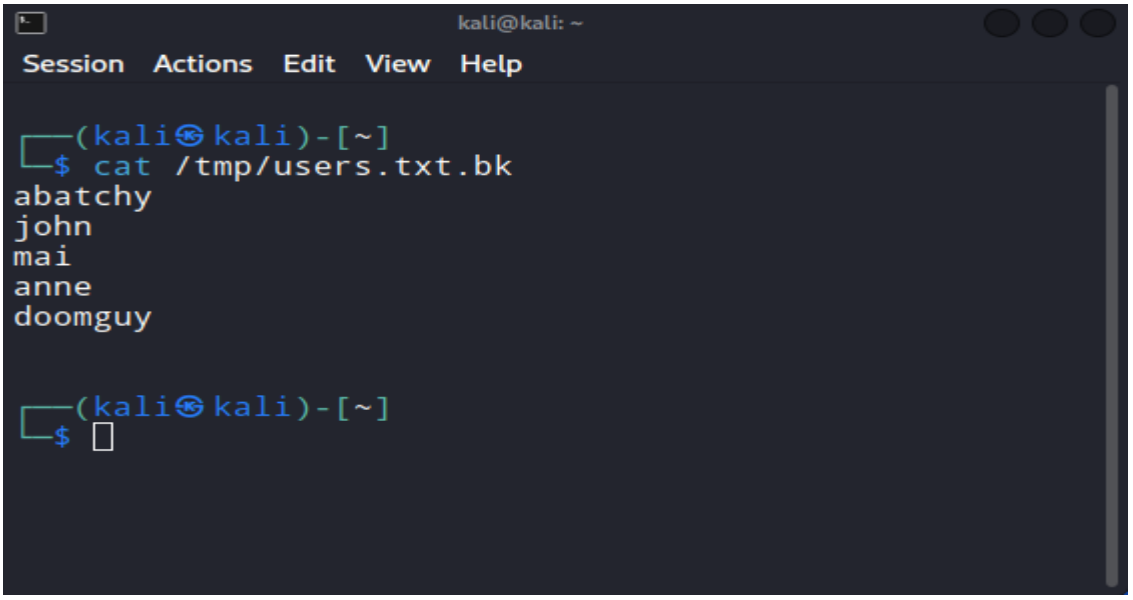
Il file identificato è stato scaricato sulla macchina attaccante per essere sottoposto ad analisi.



Analisi dei dati

Il file esfiltrato, denominato ***users.txt.bk***, è stato sottoposto ad analisi.

Il file si presenta come un documento di testo in chiaro (ASCII plain-text). La natura del nome (***users***) e l'estensione di backup (***.bk***) suggeriscono che si tratti di un residuo di un'operazione di amministrazione o migrazione del sistema.



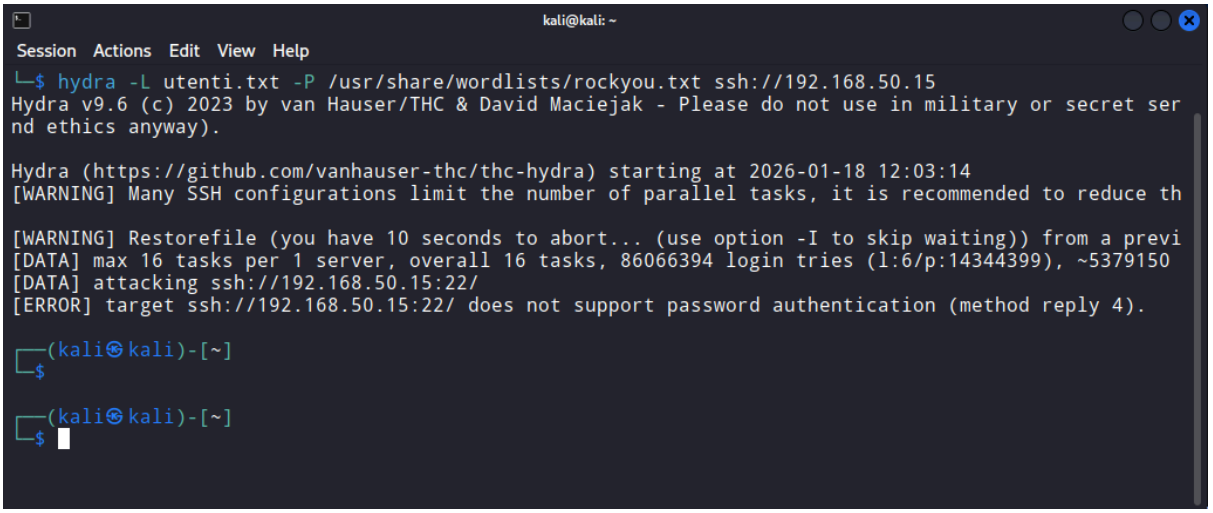
La presenza di questo elenco espone il sistema a una grave falla di sicurezza nota come **Username Enumeration**. Identificare gli account validi permette di affinare l'offensiva: invece di un attacco generico, si può lanciare un **Targeted Dictionary Attack** (Attacco a Dizionario Mirato), ottimizzando le risorse e focalizzandosi solo sui bersagli confermati.

Fase di Exploitation: Servizio SSH

A partire dagli username identificati, è stata avviata una verifica mirata delle credenziali sul servizio Secure Shell (SSH), attivo sulla porta 22. L'analisi è stata condotta con l'intento principale di scoprire account che utilizzavano password facilmente indovinabili o che presentavano problemi di configurazione.

Comando eseguito:

hydra -L utenti.txt -P /usr/share/wordlists/rockyou.txt ssh://192.168.50.15



Tentativo Accesso SSH

È stato tentato un attacco di forza bruta sul servizio **SSH** (Porta 22). L'utilizzo di una Wordlist (nello specifico ***`rockyou.txt`***, contenente 14 milioni di password comuni) è stato preferito per ottimizzare l'efficienza temporale. Questa tecnica sfrutta la tendenza degli utenti a scegliere password deboli o mnemoniche. Invece di testare miliardi di

combinazioni casuali (che richiederebbero anni), l'attacco si focalizza sulle stringhe statisticamente più probabili, riducendo i tempi di compromissione a pochi minuti.

Il server però è configurato per rifiutare l'autenticazione tramite **password**, accettando esclusivamente autenticazione tramite chiave pubblica (Public Key).

Verifica delle Policy di Autenticazione

È stato eseguito un test iterativo per ogni singolo utente della lista utilizzando il tool **Hydra**, al fine di verificare se ogni utente rifiutasse l'autenticazione tramite password.

Il comando lanciato è il seguente:

hydra -l John -P -usr/shar/wordlists/rockyou.txt -v -f ssh://192.168.50.15

Il risultato di questi test è stato sempre lo stesso.(ES. John)

Risultato del Test (Utenti: *`john, abatchy, may, doomguy`*): Il tentativo di attacco Brute Force su questi account è fallito preliminarmente.

- **Errore Rilevato:** `Does not support password authentication`.
- **Analisi Tecnica:** Il server SSH è configurato per rifiutare l'autenticazione tramite password per questi utenti ,richiedendo obbligatoriamente l'autenticazione tramite chiave pubblica (Public Key).

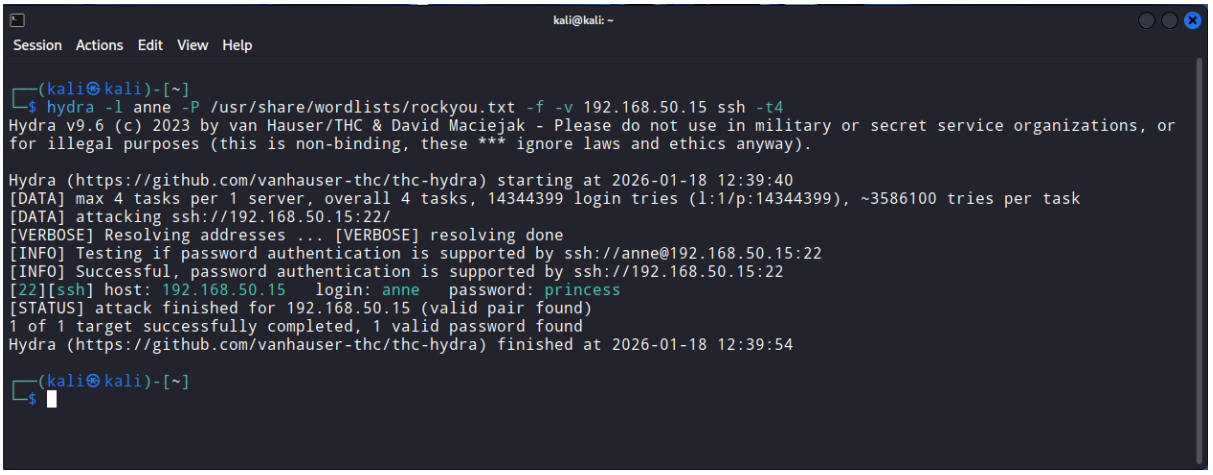
Proseguendo il test sull'utente **Anne**, è stata rilevata una grave incoerenza nella configurazione di sicurezza. A differenza degli altri account, il server **ha accettato la richiesta di password** per l'utente **Anne**.

- **Vulnerabilità:** Incoerenza nella configurazione SSH (Security Misconfiguration). L'account **Anne** è stato escluso dalle policy di restrizione che proteggono gli altri utenti, rimanendo esposto ad attacchi basati su password.

Sfruttando questa debolezza, è stato lanciato un attacco mirato esclusivamente contro l'utente.

Comando eseguito:

hydra -l anne -P /usr/share/wordlists/rockyou.txt -f -v 192.168.50.15 ssh -t 4



Credenziali trovate:

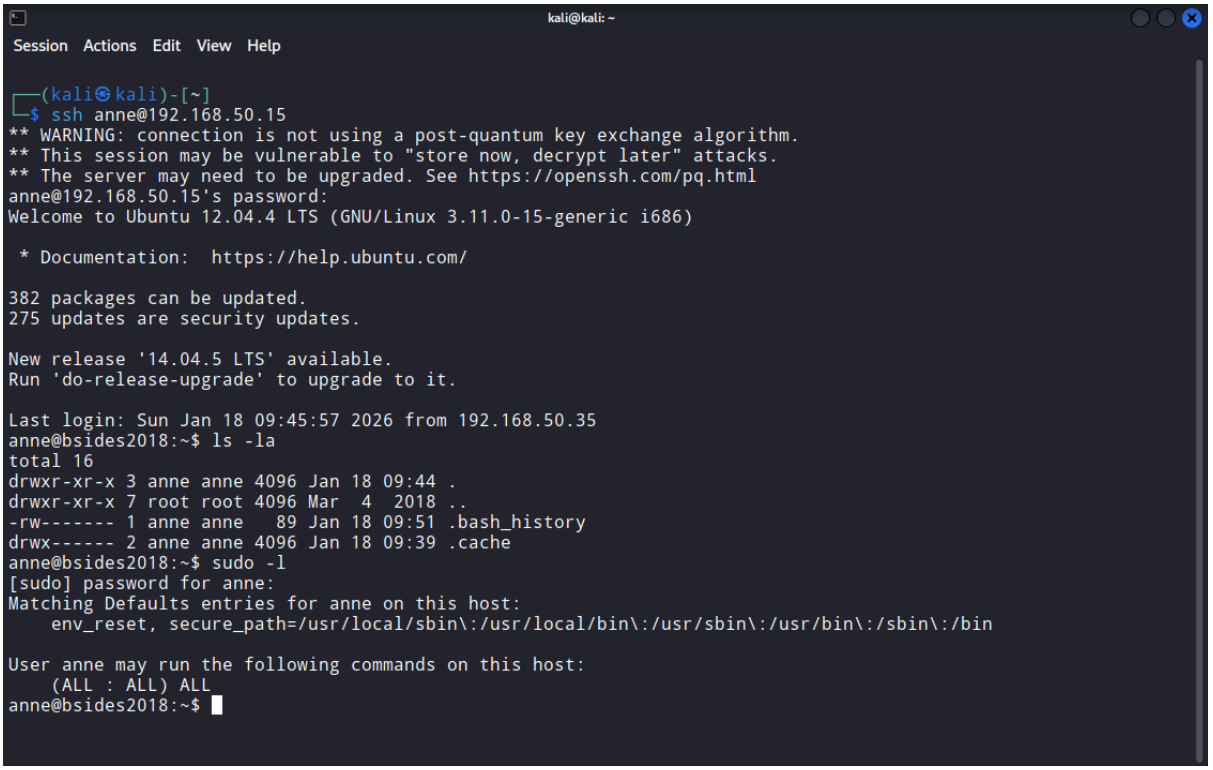
Login: ***anne*** Password: ***princess***

Privilege Escalation (Ottenimento Privilegi di Root)

Analisi dei Privilegi Sudo

Durante la fase di enumerazione post-exploitation, è stato verificato il livello di accesso dell'utente **Anne** tramite il comando **sudo -l**. L'output ha rivelato una configurazione estremamente permissiva nel file /etc/sudoers.

- **Configurazione Rilevata:** ***(ALL : ALL) ALL***
- **Spiegazione***: L'utente Anne è autorizzato a eseguire qualsiasi comando, agendo come qualsiasi utente (incluso* ***root****), senza restrizioni specifiche.*

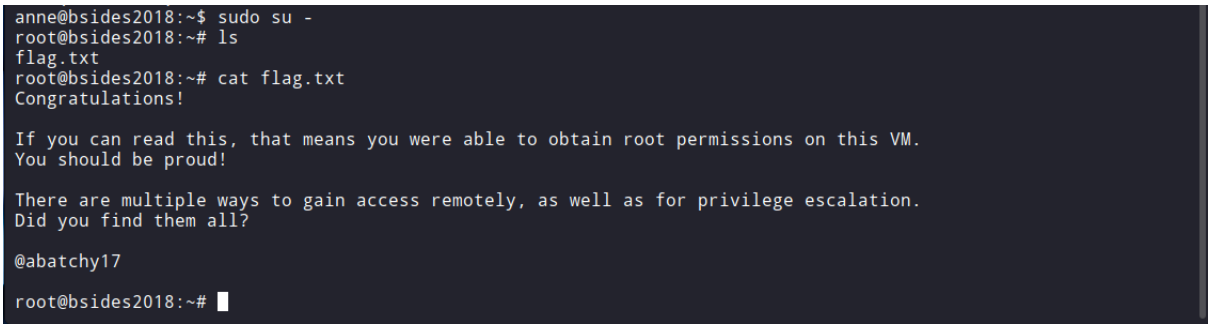


Exploitation e Accesso Root

Sfruttando questa configurazione (definita "**Full Sudo Access**"), è stata eseguita l'escalation dei privilegi per ottenere una shell amministrativa completa.

- **Comando Eseguito*:*** **`sudo su`**
- **Risultato*:*** **Transizione immediata all'utente `root` (UID 0).**

Con i privilegi di **root** acquisiti, è stato possibile accedere alla directory protetta `/root`, inaccessibile agli utenti standard. All'interno è stato recuperato il **flag finale** che conferma la completa compromissione del sistema.



Privilegi di root ottenuti.