W16D4

Penetration test

Informazioni generali

- Progetto: Penetration Test in modalità black box
- Ip target: sconosciuto
- Data: 16/06 - 19/06
- Autore del report: Fabio Falato

Sommario

Introduzione

Obiettivo

Lo scopo del PT è un catch the flag su una macchina virtuale di cui non conosciamo ne Ip ne versione del sistema operativo.

Informazioni note

Sappiamo unicamente che la macchina si trova in una rete internal con la scheda di rete configurata in DHCP, inoltre sappiamo il Default gatway è il server server pfsense che ha anche un server Dhcp configurato.

Il pool di indirizzi sull'interfaccia 1 va da 192.168.50.100 a 192.168.50.110

Il poll di indirizzi sull'interfaccia 2 va da 192.168.51.100 a 192.168.51.110

Disclaimer: ho voluto impostare la macchina target sulla rete interna per sicurezza, ho anche testato con rete bridge usando il mio modem come server dhcpe il risultato era il medesimo.

Infine ho anche scelto un pool ridotto di indirizzi allocabili nel server DHCP in pfsense per velocizzare gli scan

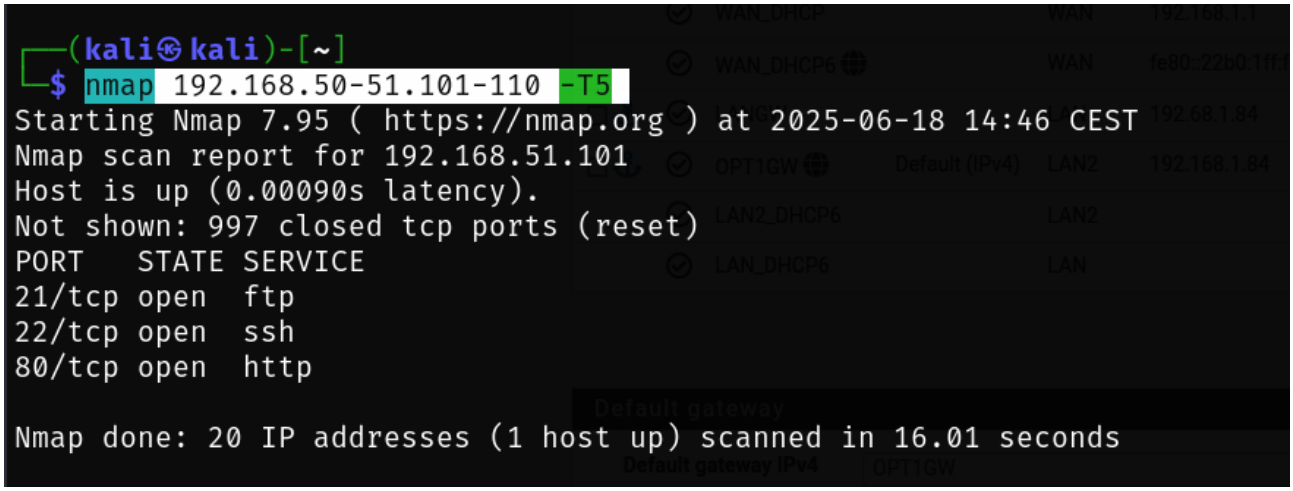
Enumerazione e identificazione della macchina Target

Metodologia di scansione e strumenti

Facciamo una prima scansione molto veloce con **Nmap** per visualizzare nel pool di indirizzi allocabili quali dispositivi sono presenti nella nostra rete

nmap 192.168.50-51.101-110 -T5

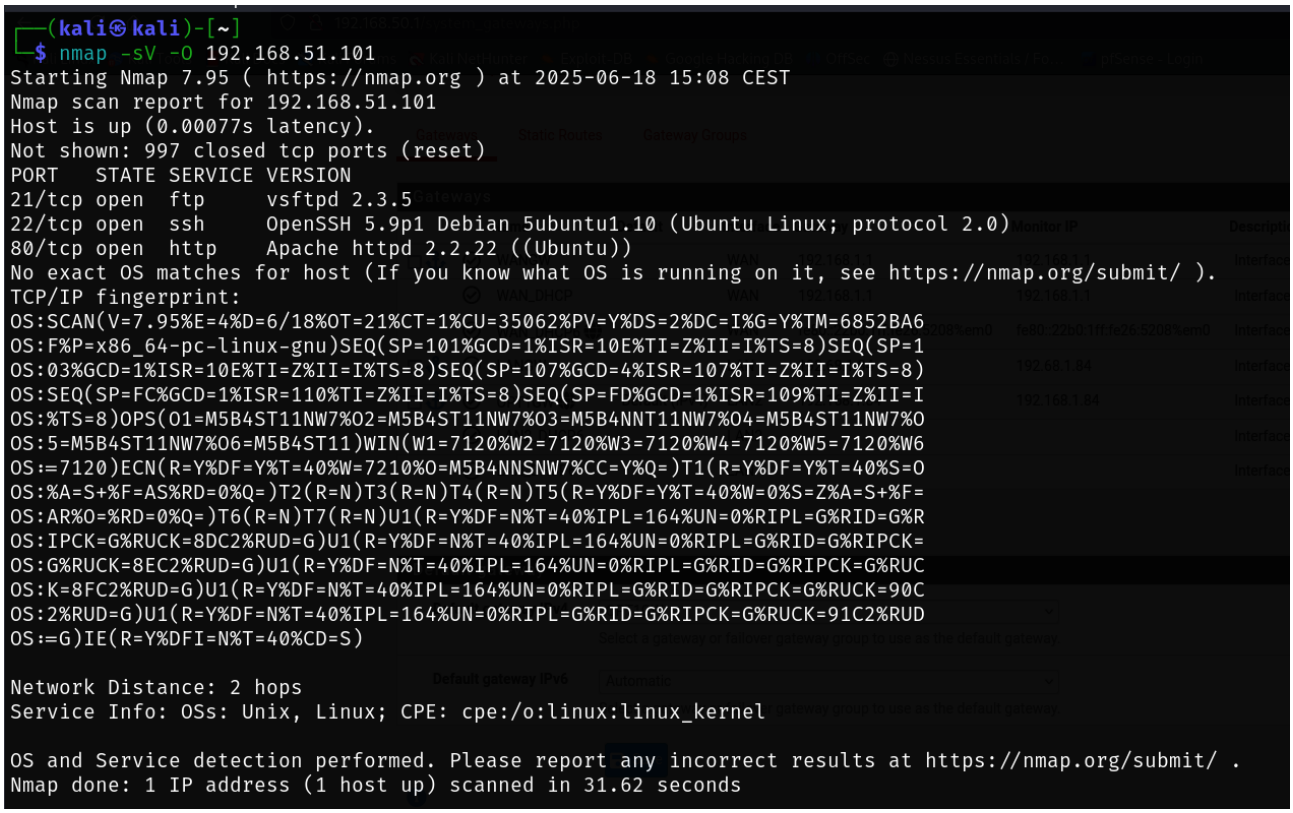
in questo caso aggiungo l'opzione -T5 per velocizzare le operazioni di scan e perché in questo scenario generare poca entropia non ci serve



La scansione è andata bene nella rete sono presenti solamente 1 Host con Ip 192.168.51.101, procediamo con una scansione più approfondita sempre con nmap per capire la versione dei servizi esposti ed il tipo di sistema operativo

Il comando stavolta della scansione è

nmap -sV -O 192.168.51.101



Informazioni ottenute

- Ip macchina target: 192.168.51.101
- Versione sistema operativo: sappiamo che la macchina è una linux ma è impossibile stabile con precisione la versione
- La macchina espone:
    1. un servizio ftp versione vsftpd 2.3.5
    2. server ssh versione OpenSSH 5.9p1
    3. server http versione Apache httpd 2.2.22

Vulnerability assesment

Tramite lo strumento Nessun facciamo una scansione delle vulnerabilità note della macchina.

La scansione è avvenuta usando principalmente la funzione **Basic Network Scan** di Nessus Essential versione 10.8.4

Minacce rilevate

Di seguito un elenco delle vulnerabilità rilevate, faccio presente che la lista sottostante è solamente un estratto di tutte le minacce rilevate

Titolo	**Canonical Ubuntu Linux SEoL (12.04.x)**
Descrizione	La versione Canonical Ubuntu Linux 12.04.x non è più supportata dal fornitore. Questo significa che non verranno rilasciate nuove patch di sicurezza, rendendo il sistema potenzialmente vulnerabile.
Gravità	Critica

Titolo	**mDNS Detection (Remote Network)**
Descrizione	Il servizio remoto utilizza il protocollo Bonjour (noto anche come ZeroConf o mDNS), che consente a chiunque di ottenere informazioni dal sistema remoto, come il tipo e la versione del sistema operativo, il nome host e l'elenco dei servizi in esecuzione.
Gravità	Media

Titolo	**SSH Weak Algorithms Supported**
Descrizione	Nessus ha rilevato che il server SSH remoto è configurato per utilizzare il cifrario Arcfour o nessun cifrario. La RFC 4253 sconsiglia l'uso di Arcfour a causa di problemi legati a chiavi deboli.
Gravità	Mixed

Titolo	**Apache Server ETag Header Information Disclosure**
Descrizione	Il server web remoto è vulnerabile alla divulgazione di informazioni a causa dell'intestazione ETag, che può rivelare dati sensibili come il numero di inode dei file richiesti, potenzialmente utili a un attaccante.
Gravità	Mixed

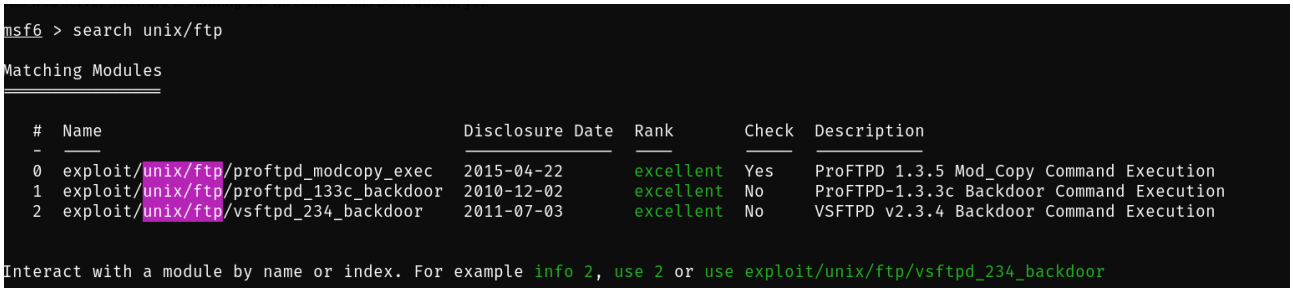
Titolo	**ICMP Timestamp Request Remote Date Disclosure**
Descrizione	Il sistema remoto risponde alle richieste ICMP di timestamp, permettendo a un attaccante di conoscere l'ora impostata sulla macchina. Questa informazione può aiutare un attaccante remoto e non autenticato ad aggirare protocolli di autenticazione basati sul tempo.
Gravità	Low

Exploit

Fase 1

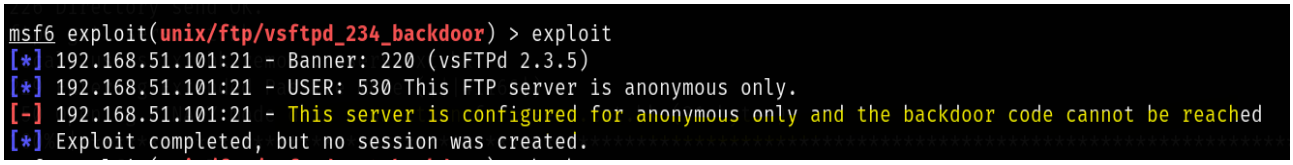
Recupero utenti

Avvio la console msfadmin e cerco le vulnerabilità unix Ftp

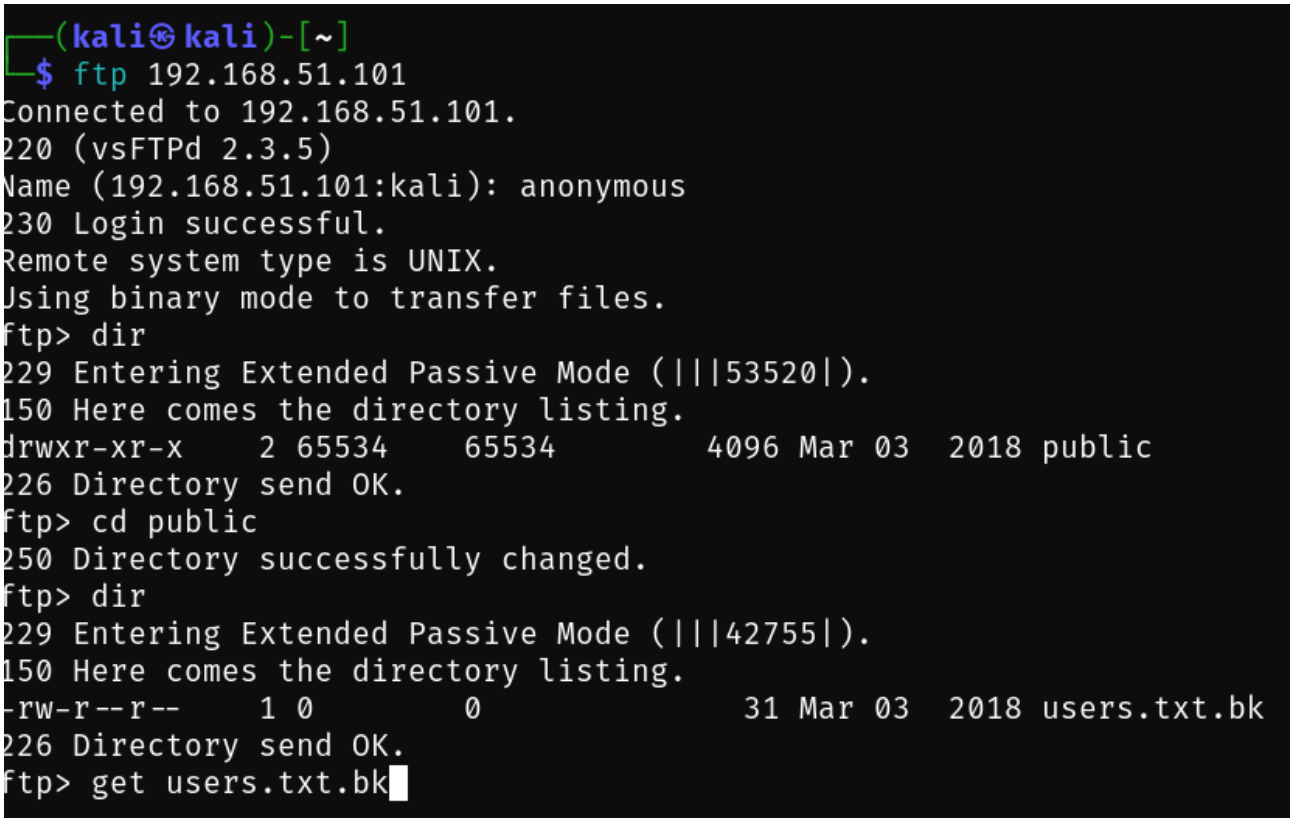


Noto che la numero 3 ha una versione molto simile a quella sulla macchina Target anche se è più aggiornata, pro vo lo stesso l'exploit

Dopo aver settato **rhost** provo a lanciare l'attacco che non va a buon fine mostrando l'errore



Provo dunque a connettermi in FTP in Anonymous.



Effettuato l'accesso, il server mi comunica che l'unica cartella condivisa è la public, in qui però è presente un file di backup in cui sono inseriti i nomi di alcuni utenti.

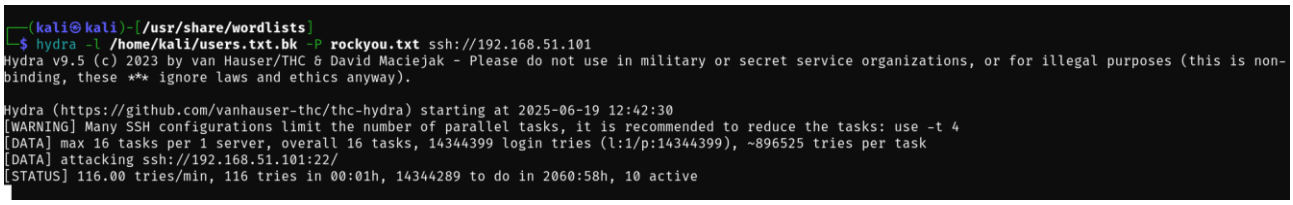
Fase 2

Attacco a dizionario

Provo a fare craccare la password degli utenti appena ottenuta con un attacco a dizionario utilizzando Hydra.

hydra -l /home/kali/users.txt.bk -P rockyou.txt ssh://192.168.51.101

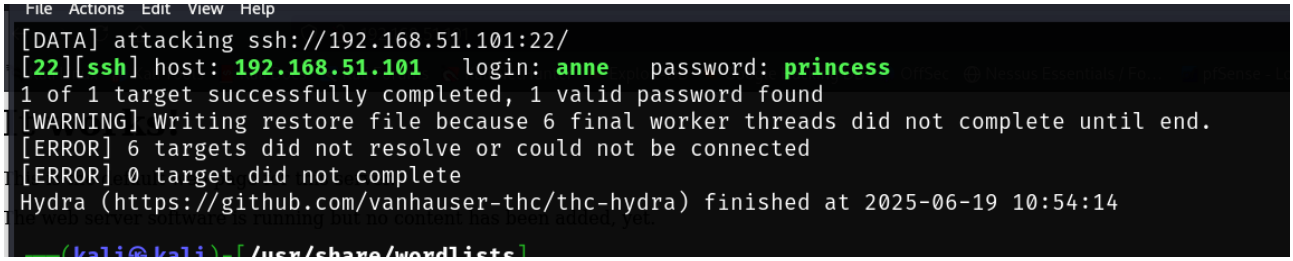
Nello specifico ho usato la wordlist rockyou.txt



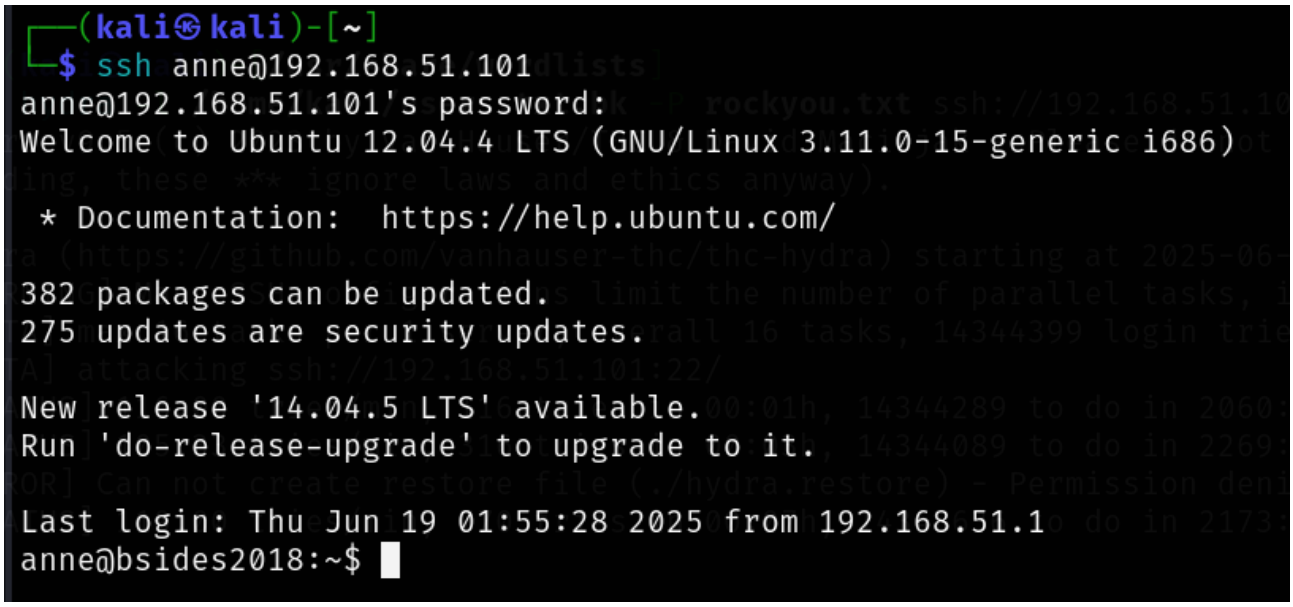
L'attacco ha successo e il programma trova una corrispondenza

User anne

Passw princess



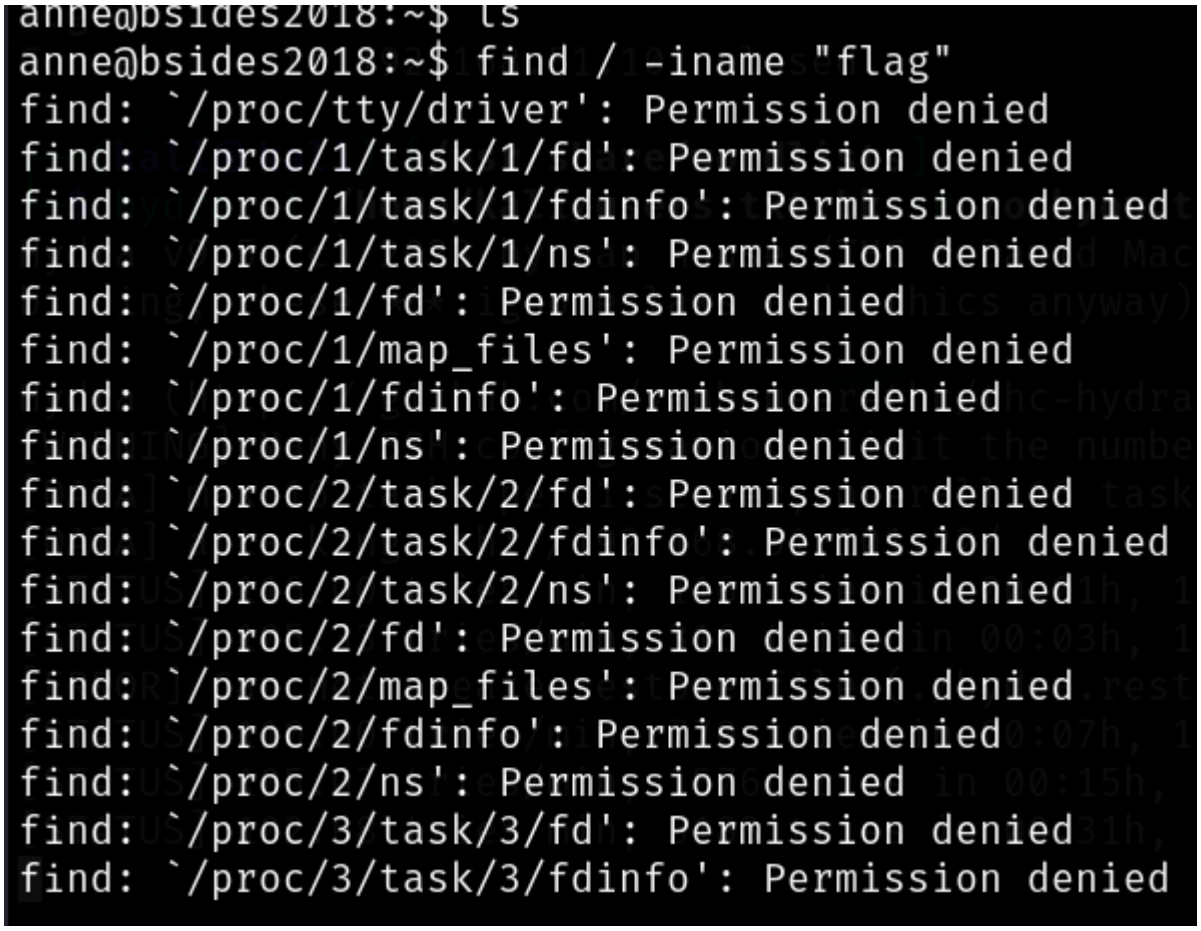
Proviamo l'accesso che avviene correttamente



Fase 3

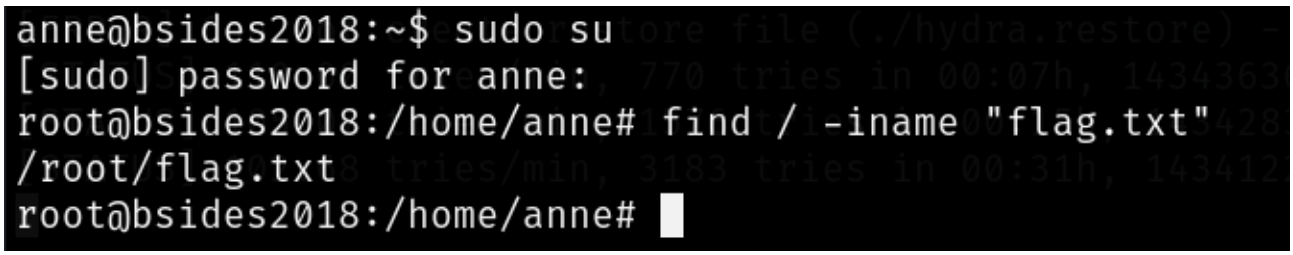
accesso come root e CTF

una volta fatto accesso con l'ìaccount anne cerchiamo di trovare un file col nome flag



Subito il comando ci mostra problemi ad accedere alle directory a causa dei privilegi insufficenti.

Proviamo allora a spostarci sull'account di root , fortunatamente l'account è sudoers e quindi con le credenziali craccate precedentemente riusciamo a fare l'accesso come root e ripetiamo il comando precedente



Il comando risulta stavolta efficace e ci mostra un unico file, che è quello che attesta la completa riuscita del PT