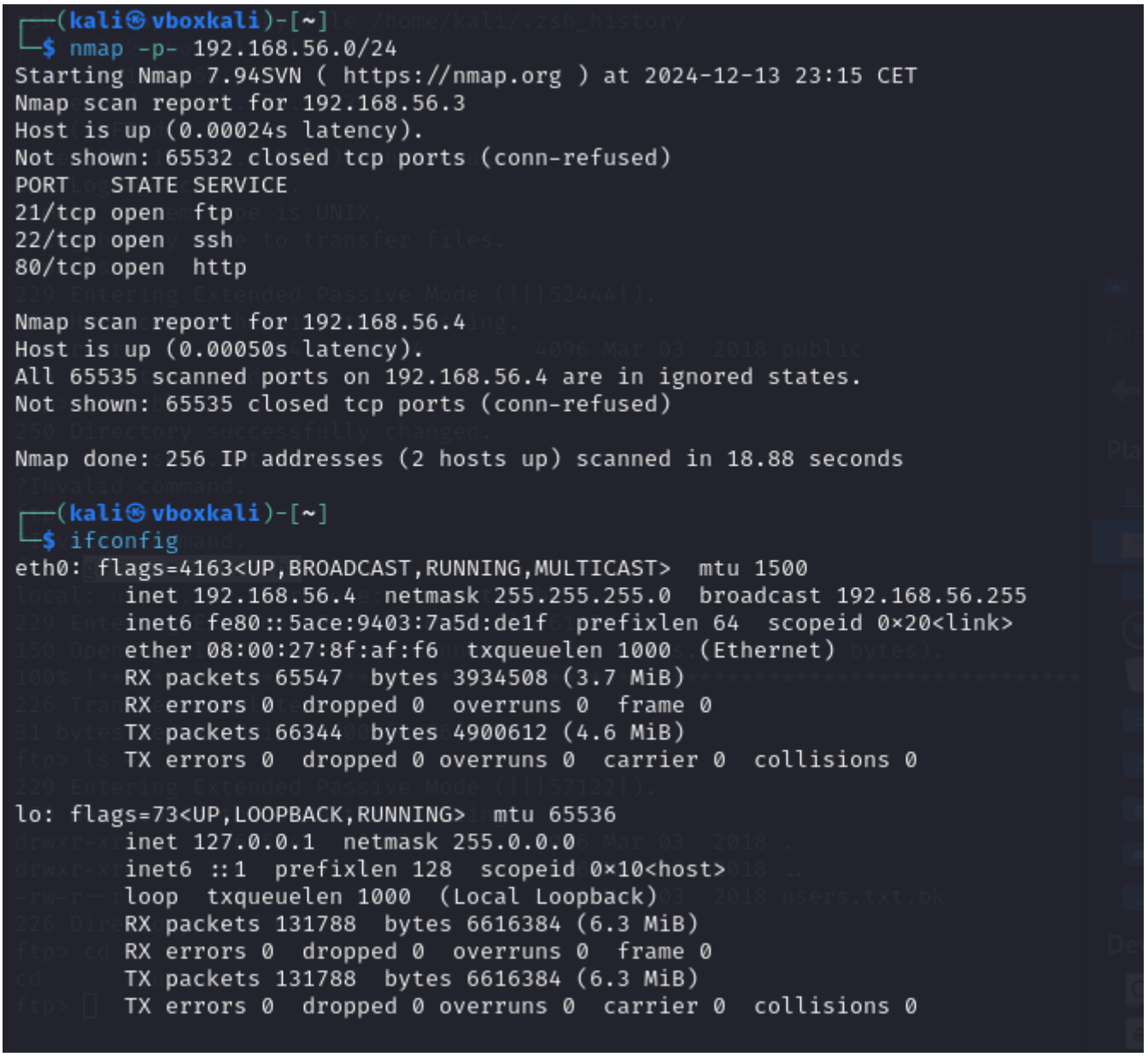
Hacking VM BlackBox corretta.

La Missione: Scatena le tue abilità per conquistare i privilegi di root. Ci sono almeno due percorsi segreti per raggiungere il dominio totale su questa macchina. Durante il tuo viaggio, esplora a fondo ogni angolo nascosto per svelare tutti i suoi misteri.

BSides-Vancouver-2018

Innanzitutto ho scaricato l'ova della macchina virtuale e l'ho importata all'interno di VirtualBox, ho controllato le impostazioni di rete ed ho notato che erano configurate in "scheda solo host", di conseguenza ho proceduto ad impostare anche la rete della Kali in "scheda solo host."
Avviata la macchina ho notato che richiedeva login e password per poter accedere ed ho cominciato a lavorare sul modo per potervi accedere.
Ho cominciato sin da subito a lavorare con nmap ed ho lanciato il comando -p- per scansire tutte le porta presenti sulla rete su cui risiede la Kali e ho notato che oltre al mio ip (192.168.56.4, verificato tramite il comando ifconfig) ce n'era un altro, quindi 192.168.56.3.



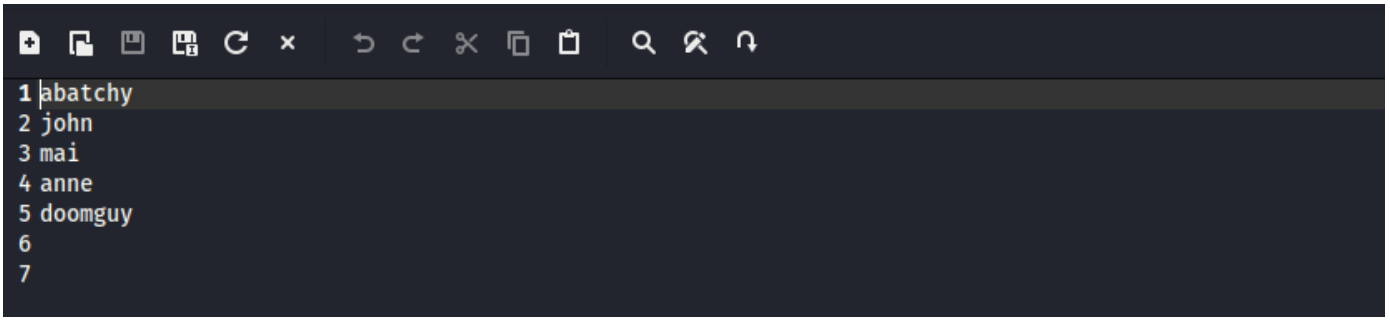
Successivamente ho eseguito il comando nmap -A, dove -A permette una scansione dettagliata del target da esaminare.

```
┌──(kali㉿vboxkali)-[~]
└─$ nmap -A 192.168.56.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 23:15 CET
Nmap scan report for 192.168.56.3
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (conn-refused)
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 192.168.56.4
|      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 2
|      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-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
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 19.83 seconds
```

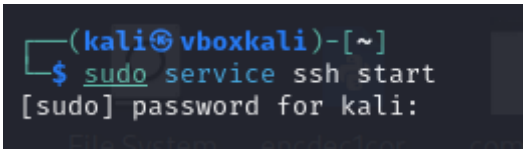
Ho notato subito qualcosa di sospetto, cioè che nella porta ftp risiedevano delle cartelle quindi ho proceduto con una connessione ftp tramite terminale verso l'IP della macchina da scansire. La connessione l'ho stabilits tramite "anonymous" sennò non mi avrebbe permesso l'accesso.

Ho notato che l'unica cartella in cui potevo entrare era "public" e, aprendola, ho trovato il file backup users.txt.bk, quindi l'ho scaricato tramite il comando get.
Aprendolo mi è apparsa una lista di nomi.



Dopo aver ragionato ho deciso di utilizzare ssh per verificare se potessi acquisire il comando del

sistema di uno dei nomi da remoto.
Innanzitutto ho avviato il servizio ssh.

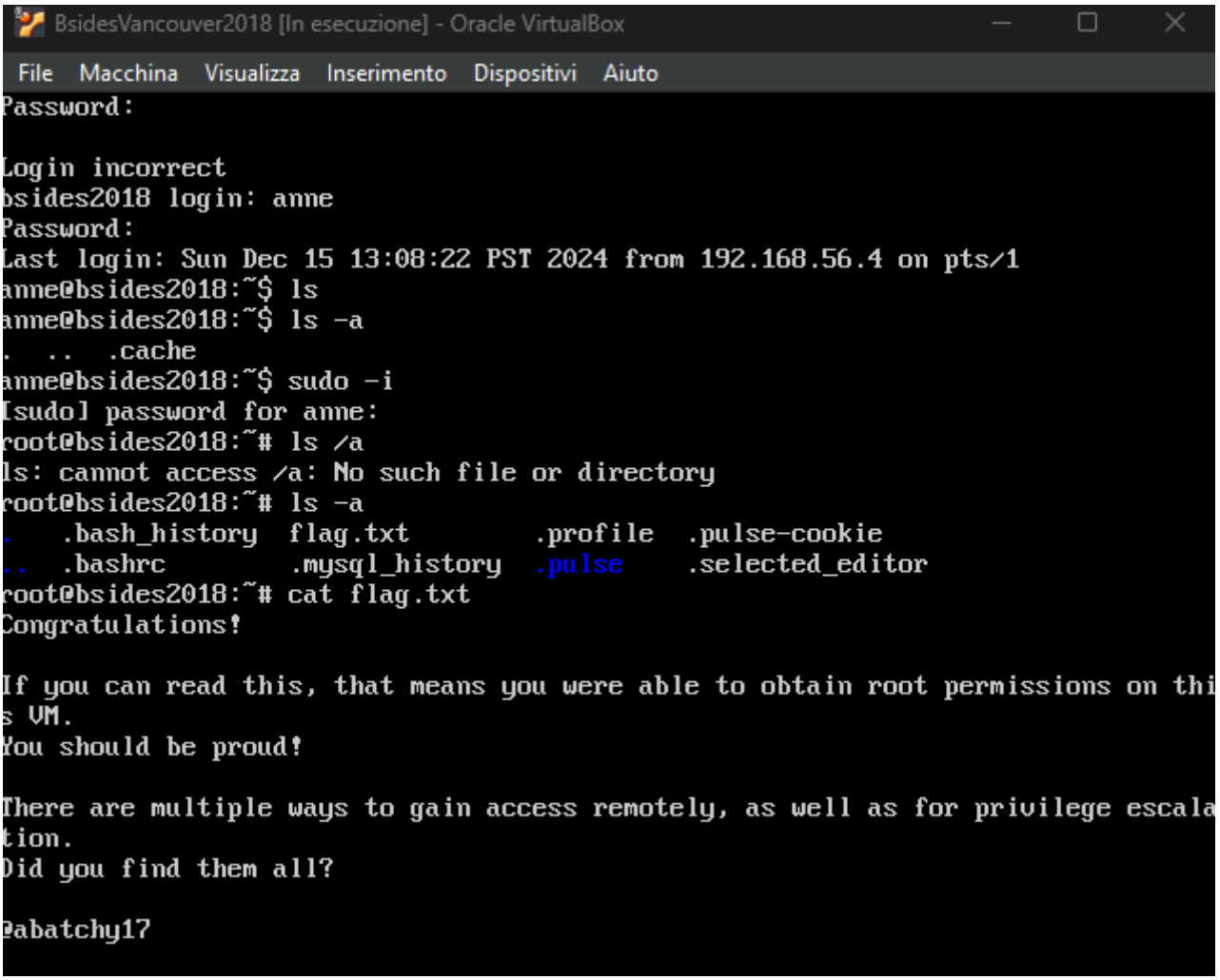


Dopodiche ho testato le connessioni notando che l'unico sistema di cui potevo acquisire il controllo da remoto era quello di *anne*.

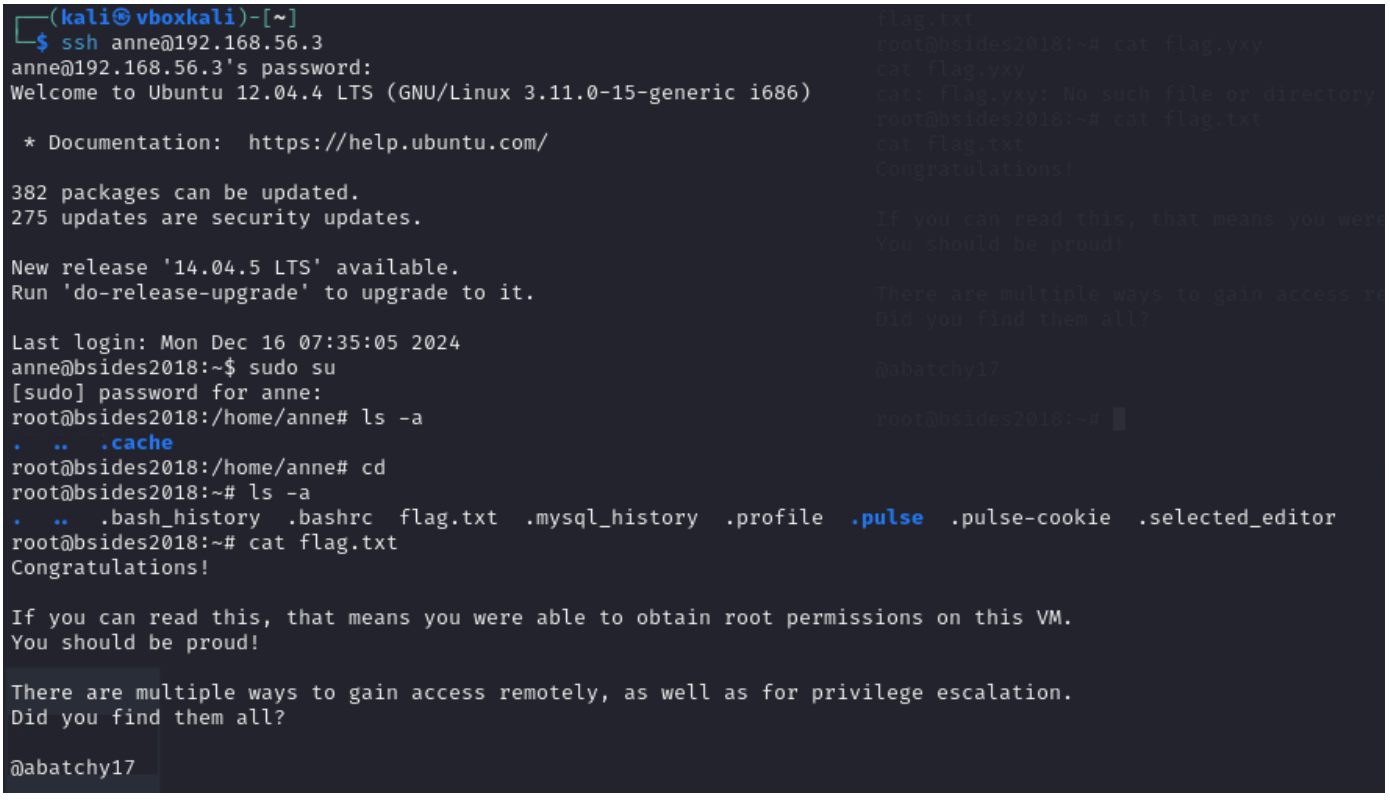
Sapendo ora il nome dell'utente, ho eseguito il tool hydra per trovare la password.

Ora avendo la il nome utente e la password sono riuscita ad entrare:

- sulla macchina tramite login e password



- da ssh tramite il terminale della kali

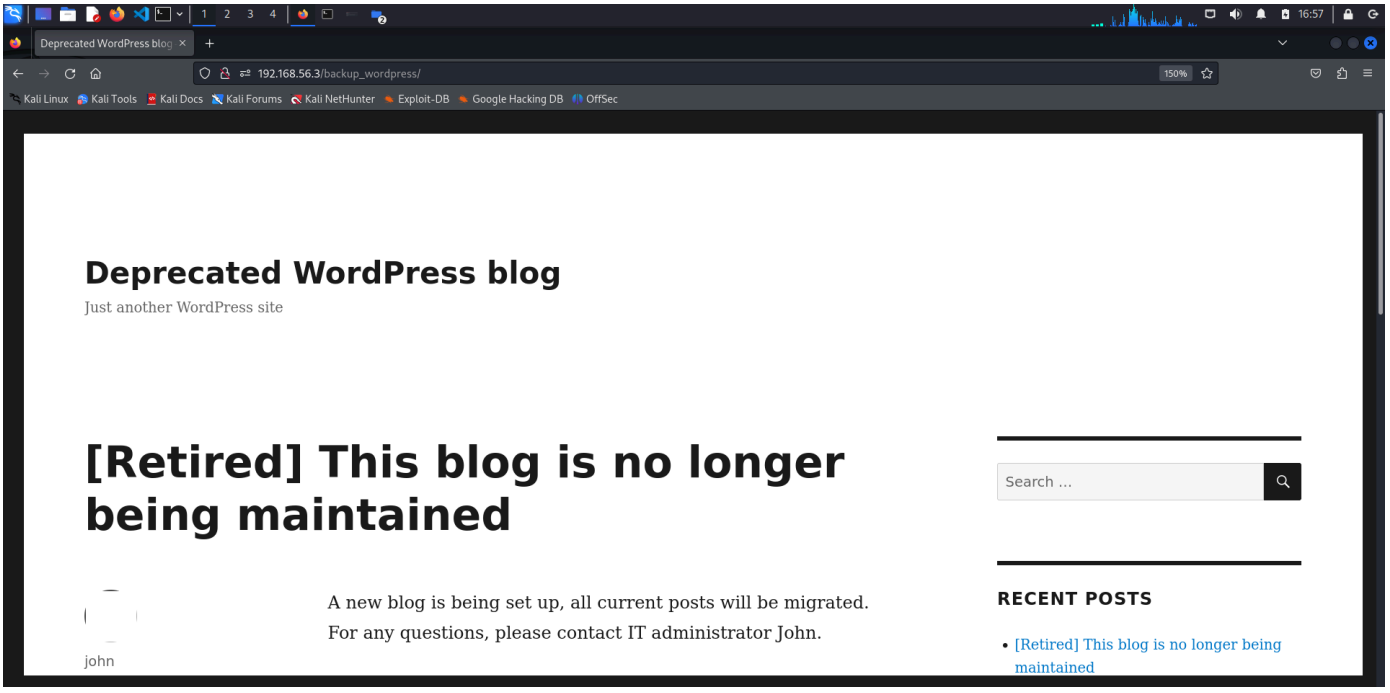


Ritornando poi a nmap -A ho fatto caso alla presenza di altri file

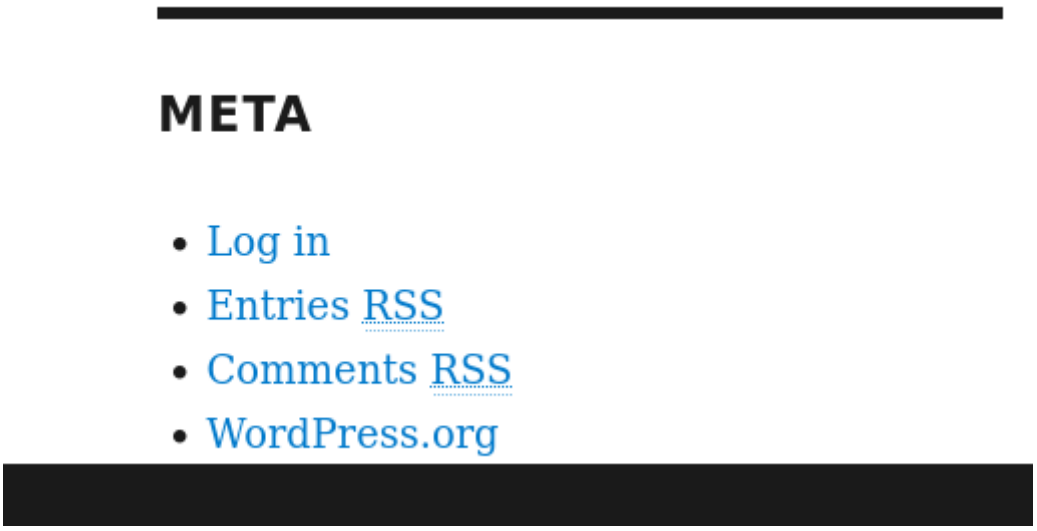
```
┌──(kali㉿vboxkali)-[~]
└─$ nmap -A 192.168.56.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 23:15 CET
Nmap scan report for 192.168.56.3
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
| ftp-anon: 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 192.168.56.4
|      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 2
|      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-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
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 19.83 seconds
```

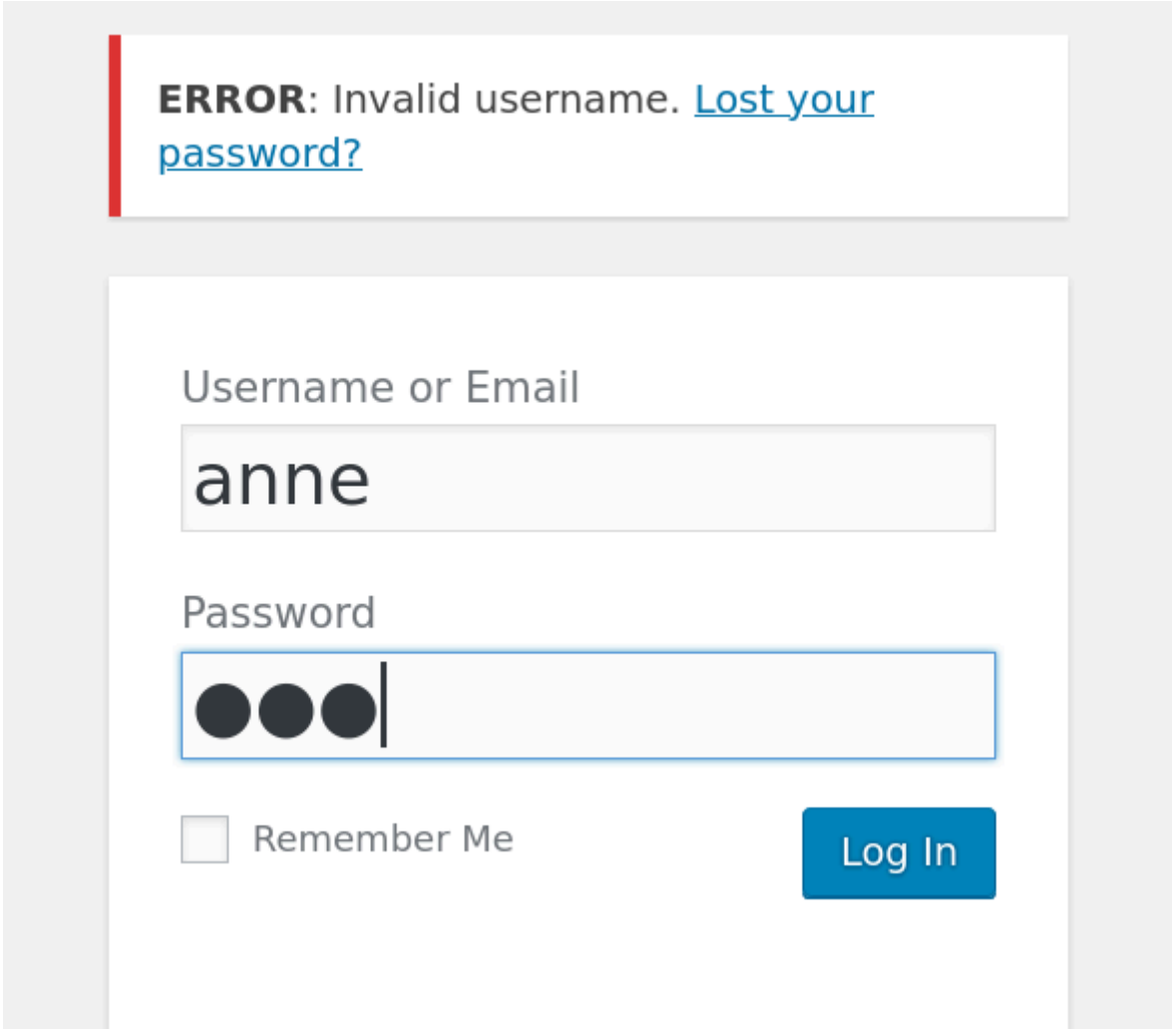
- *robots.txt* che, inserito nell'url, mi ha riportato al sito *backup_wordpress*



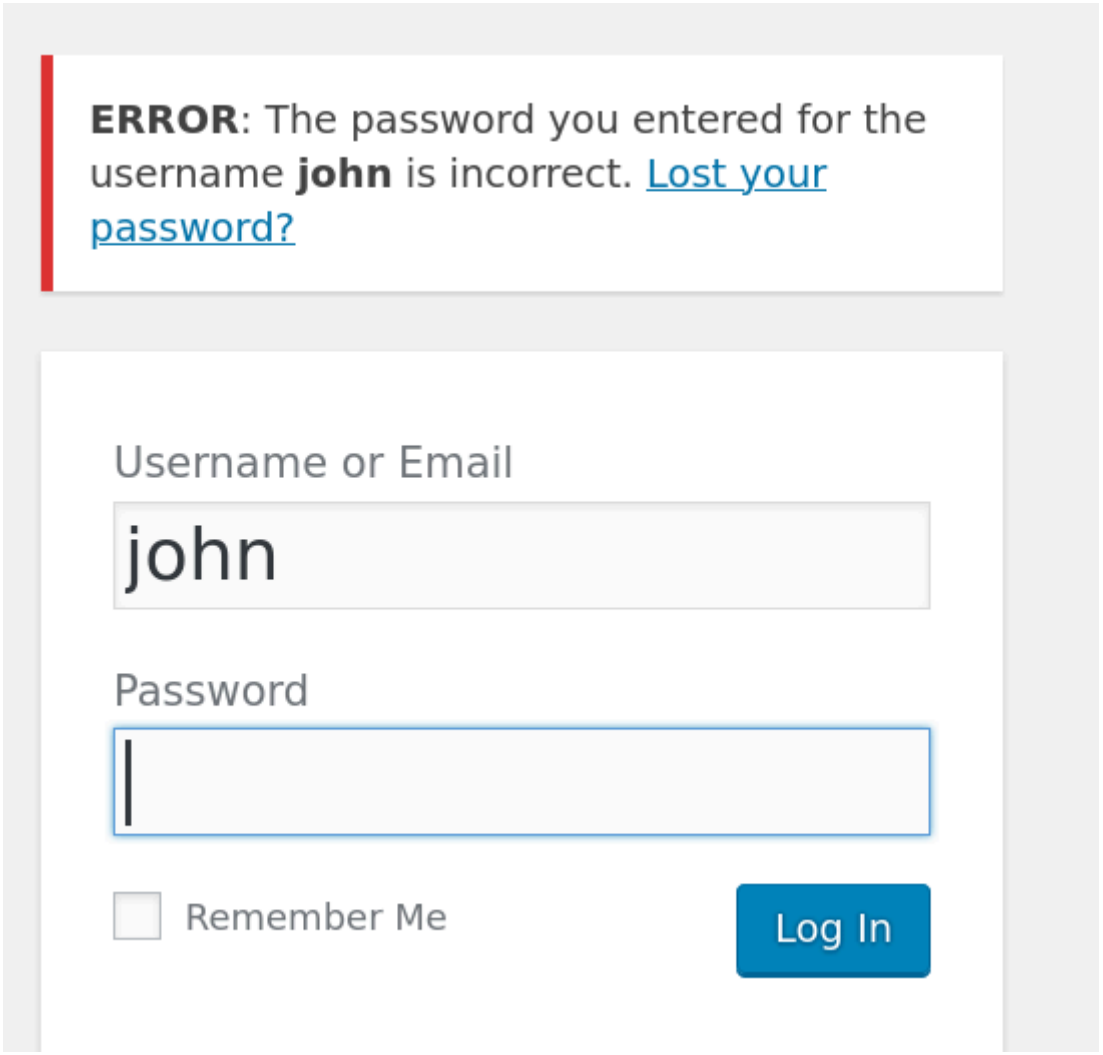
Infondo alla pagina c'era una sezione log in su cui ho cliccato



Provando a inserire anne mi sono accorta che dava messaggio di errore: **invalid username**

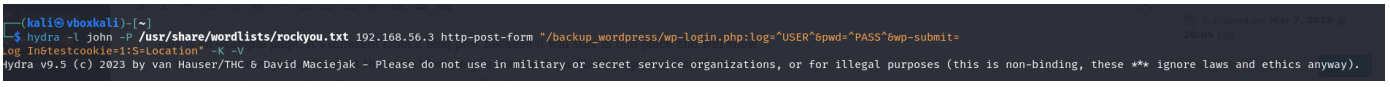


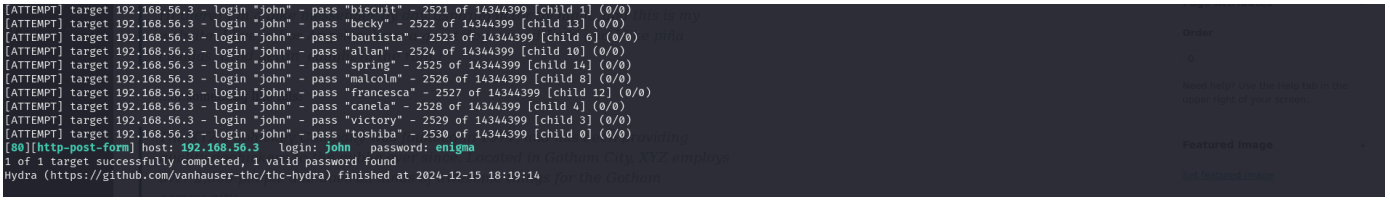
Mentre inserendo john dava il messaggio di errore: **invalid password**



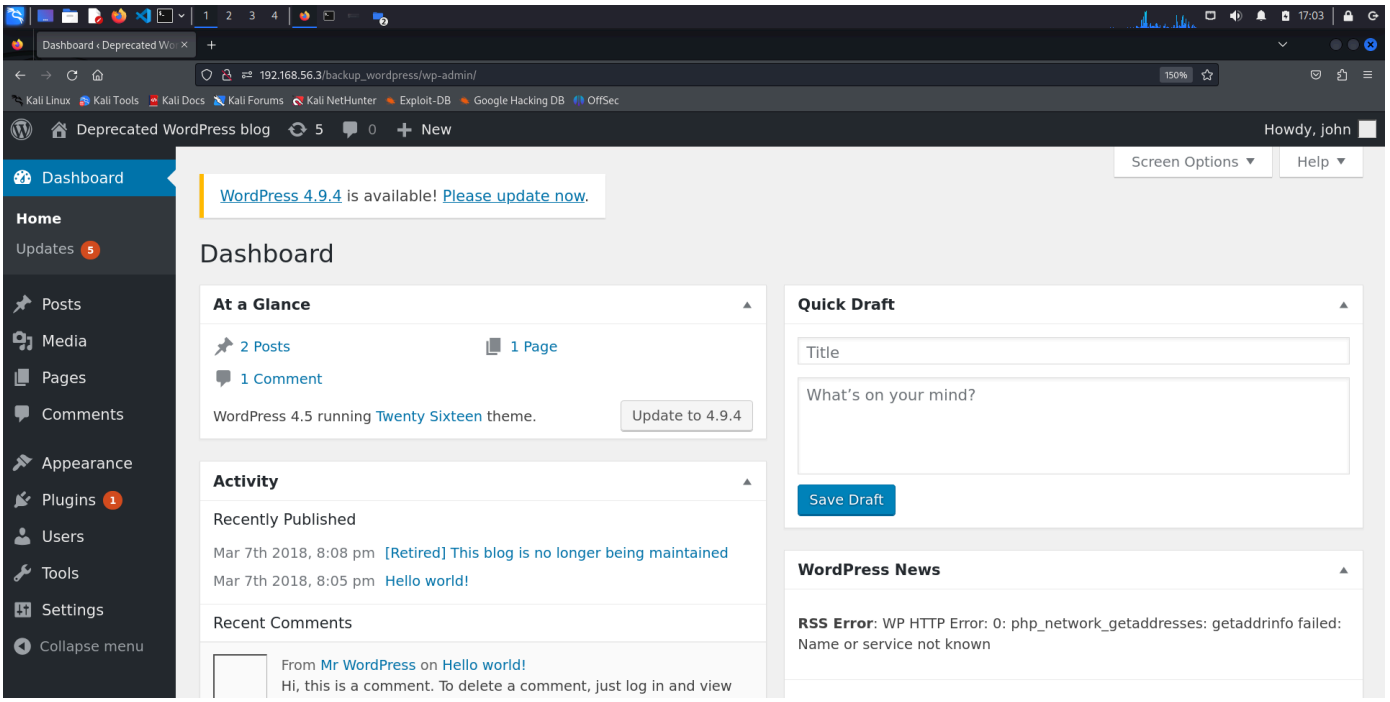
Questo mi ha fatto dedurre che l'unico utente registrato era john

Quindi ho deciso di utilizzare il tool hydra con il servizio http per riuscire ad avere la password per accedere al sito.
La parte http-post-form l'ho estratta tramite l'analisi con burpsuite.

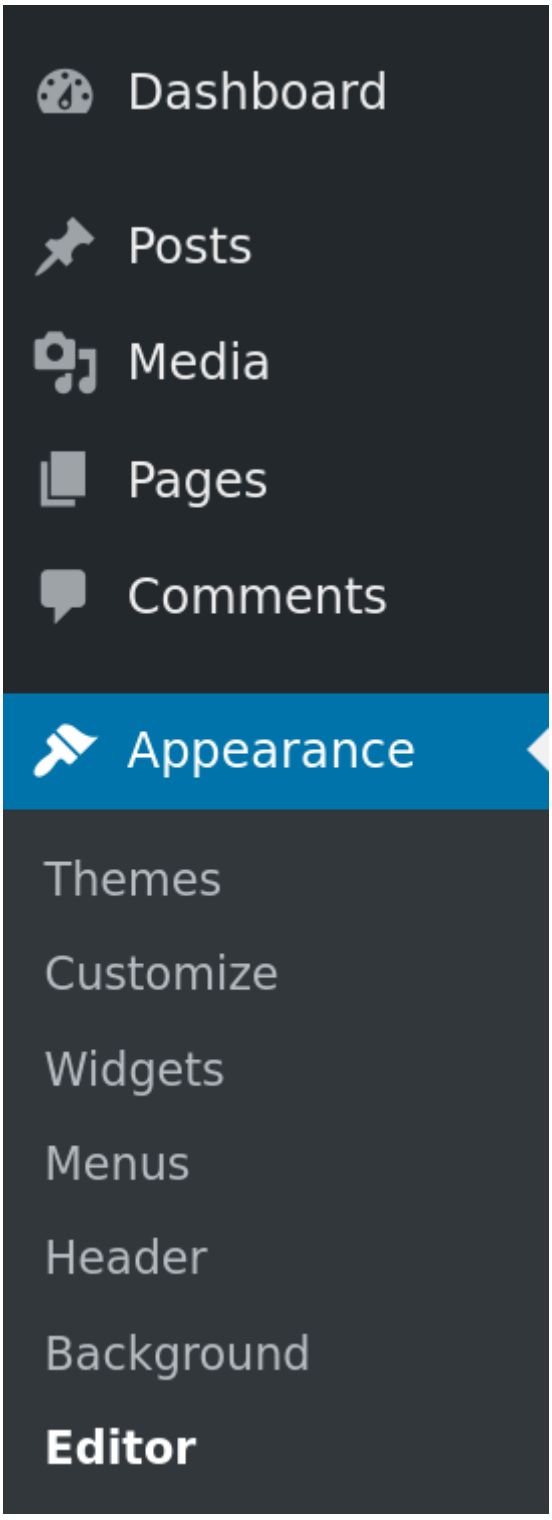




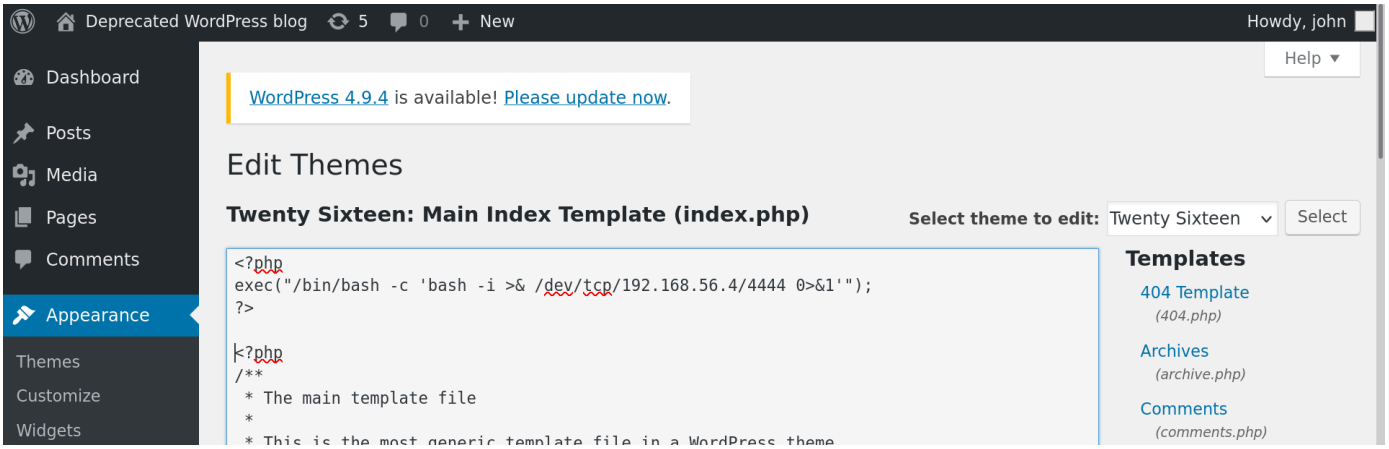
Dopo aver trovato la password ho inserito le credenziali nel sito, trovandomi nella dashboard.



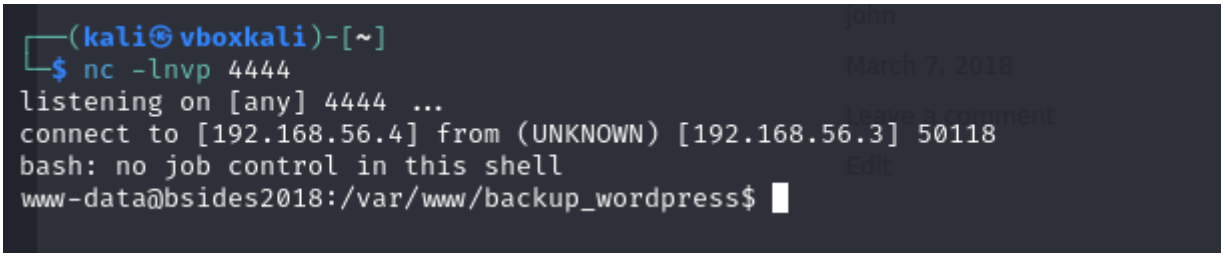
Ragionando su come fare ho deciso di rpovare ad inserire un codice php per una reverse shell in uno dei temi



In particolare sono andata nell'editor ed ho inserito il codice php nel template index



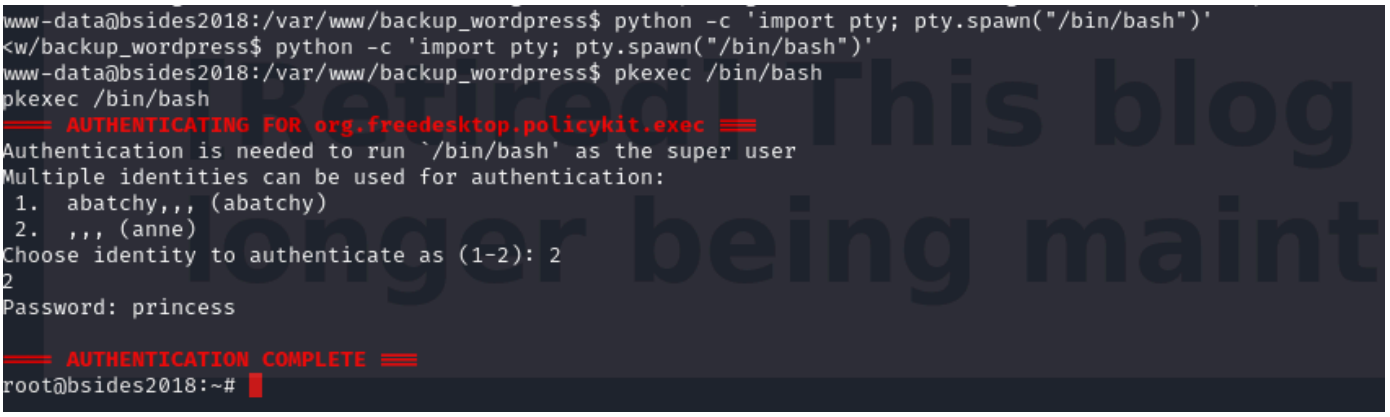
Ho avviato net cat per la reverse shell dal terminale della kali cercando di acquisire privilegi di root una volta dentro

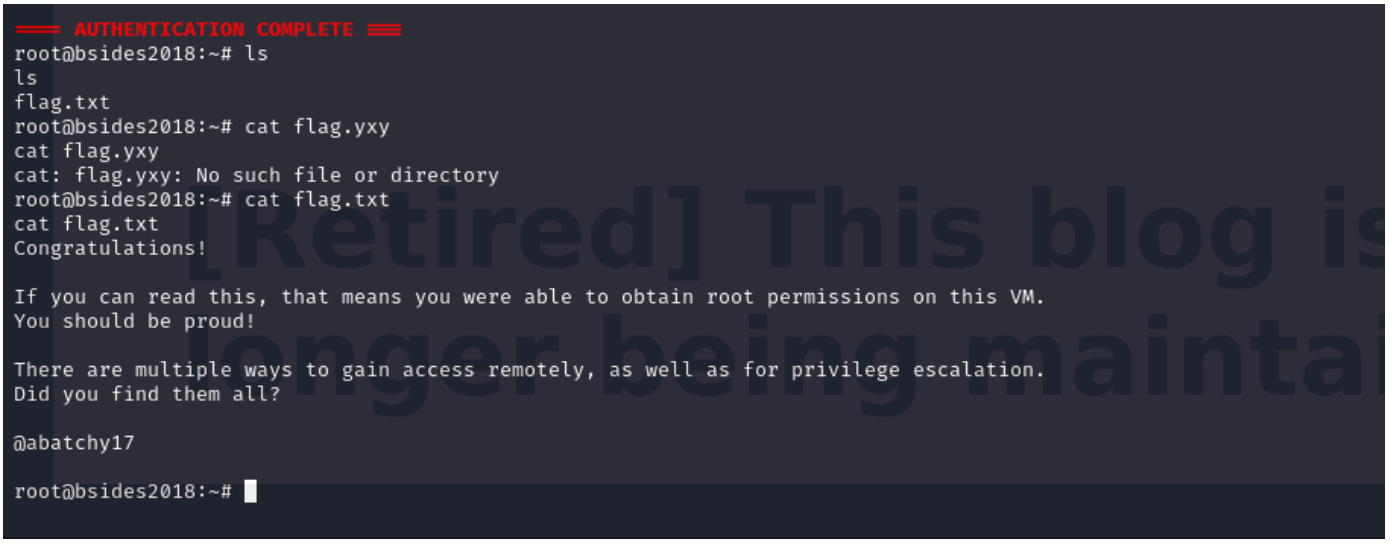


Dopo diversi tentativi ho deciso di:

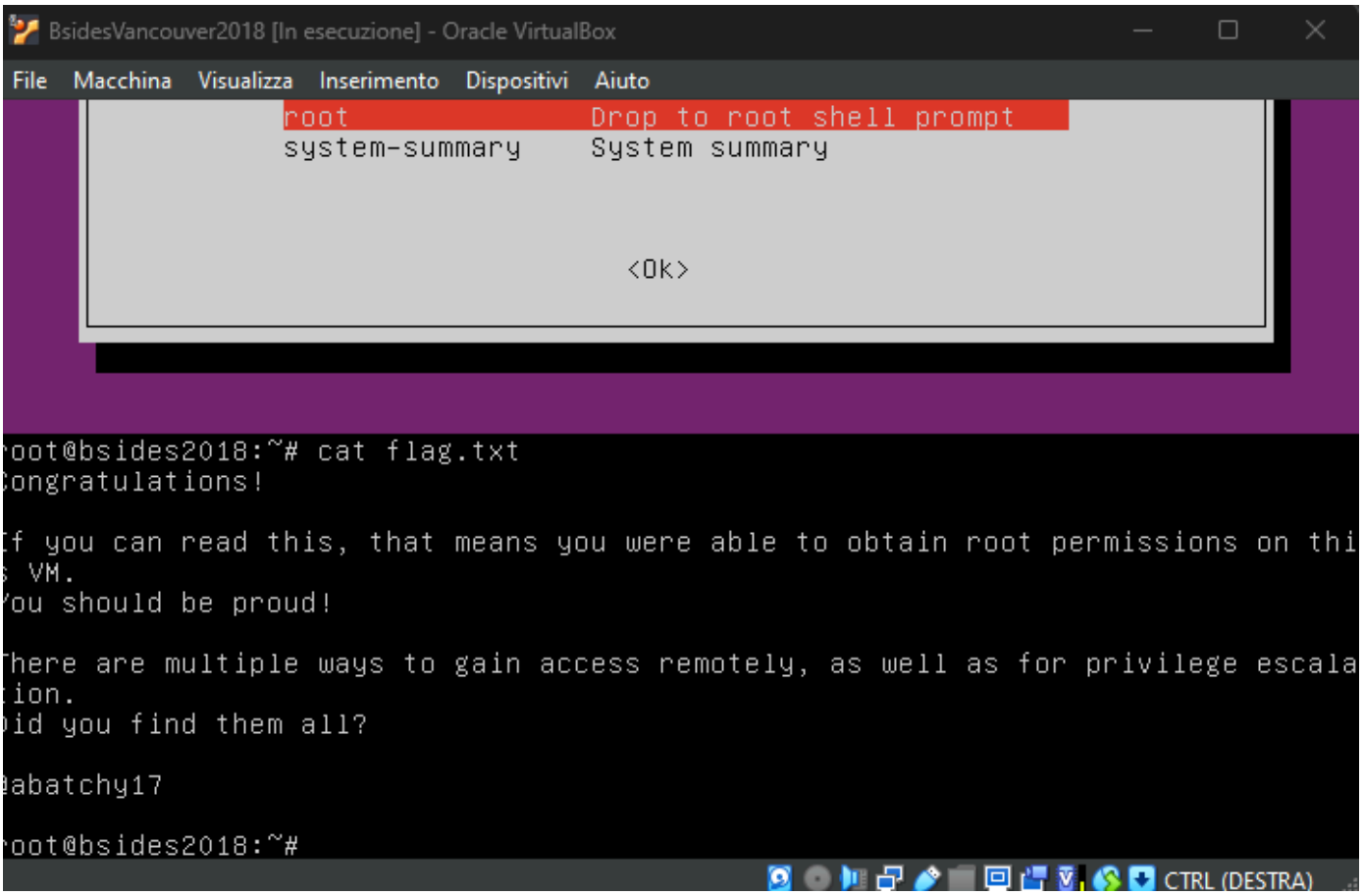
- lanciare il comando in python che migliora l'interattività di una shell limitata ottenuta su un sistema remoto:
  `python -c 'import pty; pty.spawn("/bin/bash")'`
- e successivamente
  `pkexec /bin/bash` per eseguire una shell Bash con privilegi di superutente (root) utilizzando pkexec, che è un comando del package PolicyKit (polkit).

Conoscendo già la password di anne l'ho inserita, ottenendo così il privilegio di root.





Un'altro modo in cui sono riuscita a trovare la flag è stato riavviare la macchina in modalità recovery e poi selezionando root.


BsidesVancouver2018 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
root Drop to root shell prompt
system-summary System summary
<Ok>
oot@bsides2018:~# cat flag.txt
ongratulations!
f you can read this, that means you were able to obtain root permissions on thi
VM.
ou should be proud!
here are multiple ways to gain access remotely, as well as for privilege escala
ion.
id you find them all?
abatchy17
oot@bsides2018:~#
CTRL (DESTRA)