INTERVENTO CON LA BCC TECH TASK

Benvenuti alla presentazione ufficiale della nuova piattaforma bancaria di Crypto Banking.

La piattaforma che permetterà di poter conservare e gestire i propri Crypto asset è ospitata in un server Linux con servizio DHCP attivo.

La presente CTF Challenge presenta diverse flag da poter ottenere:

-Root flag del server

-Creazione di un account

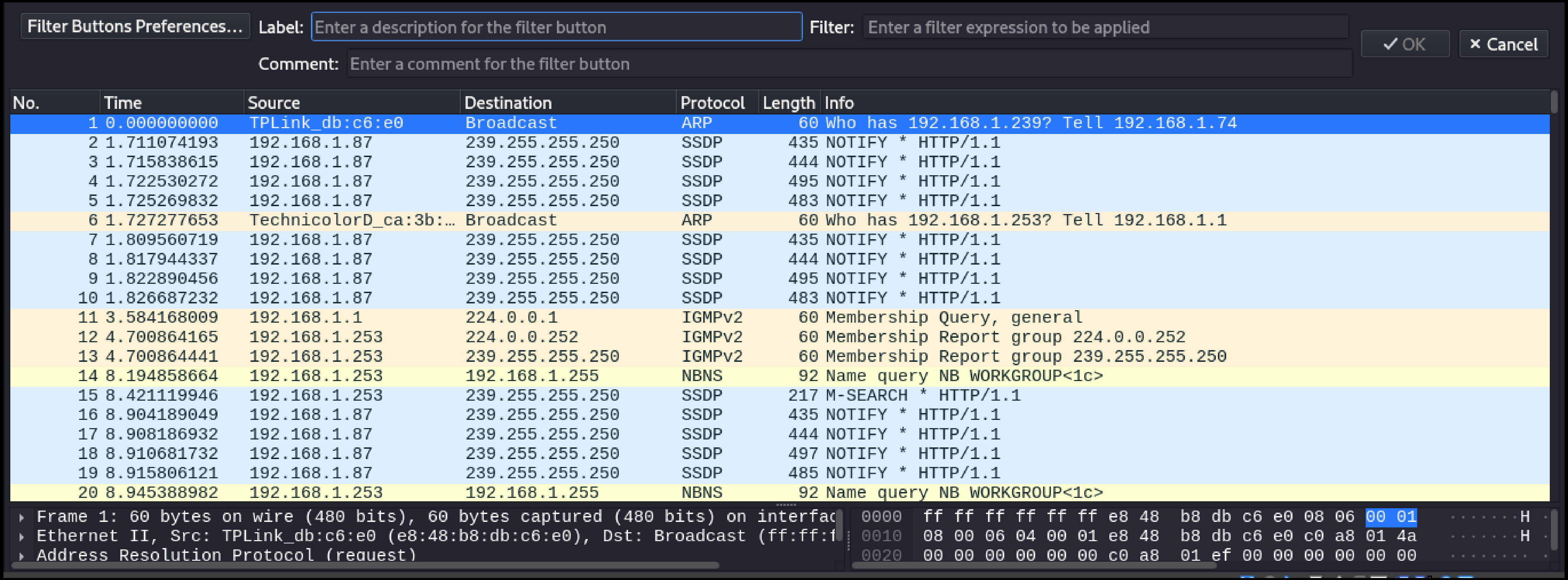
-Dump delle credenziali OS

-Dump delle credenziali WebApp

-Schedulare un Task/Job

Portare effettiva evidenza dell'ottenimento di ogni risultato.

COME PRIMO STEP HO PROVATO ATTRAVERSO IL TOOL DI WIRESHARK A RICAVARMI L'INDIRIZZO IP DELLA MACCHINA TARGET E CORRISPONDE A 192.168.1.87



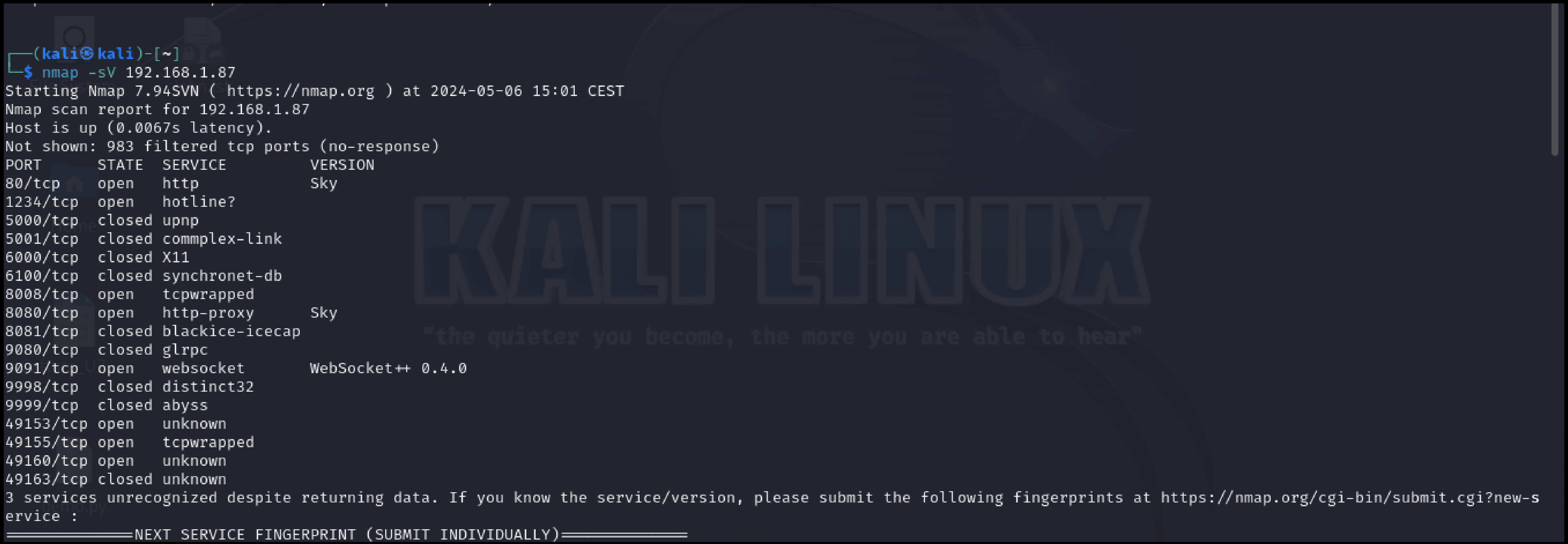
Filter Buttons Preferences…
Label: Enter a description for the filter button
Filter: Enter a filter expression to be applied
✓ OK
✕ Cancel
Comment: Enter a comment for the filter button

```
No.     Time          Source                 Destination       Protocol  Length Info
      1 0.000000000   TPLink_db:c6:e0        Broadcast         ARP           60 Who has 192.168.1.239? Tell 192.168.1.74
      2 1.711074193   192.168.1.87           239.255.255.250   SSDP         435 NOTIFY * HTTP/1.1
      3 1.715838615   192.168.1.87           239.255.255.250   SSDP         444 NOTIFY * HTTP/1.1
      4 1.722530272   192.168.1.87           239.255.255.250   SSDP         495 NOTIFY * HTTP/1.1
      5 1.725269832   192.168.1.87           239.255.255.250   SSDP         483 NOTIFY * HTTP/1.1
      6 1.727277653   TechnicolorD_ca:3b:…   Broadcast         ARP           60 Who has 192.168.1.253? Tell 192.168.1.1
      7 1.809560719   192.168.1.87           239.255.255.250   SSDP         435 NOTIFY * HTTP/1.1
      8 1.817944337   192.168.1.87           239.255.255.250   SSDP         444 NOTIFY * HTTP/1.1
      9 1.822890456   192.168.1.87           239.255.255.250   SSDP         495 NOTIFY * HTTP/1.1
     10 1.826687232   192.168.1.87           239.255.255.250   SSDP         483 NOTIFY * HTTP/1.1
     11 3.584168009   192.168.1.1            224.0.0.1         IGMPv2        60 Membership Query, general
     12 4.700864165   192.168.1.253          224.0.0.252       IGMPv2        60 Membership Report group 224.0.0.252
     13 4.700864441   192.168.1.253          239.255.255.250   IGMPv2        60 Membership Report group 239.255.255.250
     14 8.194858664   192.168.1.253          192.168.1.255     NBNS          92 Name query NB WORKGROUP<1c>
     15 8.421119946   192.168.1.253          239.255.255.250   SSDP         217 M-SEARCH * HTTP/1.1
     16 8.904189049   192.168.1.87           239.255.255.250   SSDP         435 NOTIFY * HTTP/1.1
     17 8.908186932   192.168.1.87           239.255.255.250   SSDP         444 NOTIFY * HTTP/1.1
     18 8.910681732   192.168.1.87           239.255.255.250   SSDP         497 NOTIFY * HTTP/1.1
     19 8.915806121   192.168.1.87           239.255.255.250   SSDP         485 NOTIFY * HTTP/1.1
     20 8.945388982   192.168.1.253          192.168.1.255     NBNS          92 Name query NB WORKGROUP<1c>
```

```
▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interfac
▸ Ethernet II, Src: TPLink_db:c6:e0 (e8:48:b8:db:c6:e0), Dst: Broadcast (ff:ff:f
▸ Address Resolution Protocol (request)
```

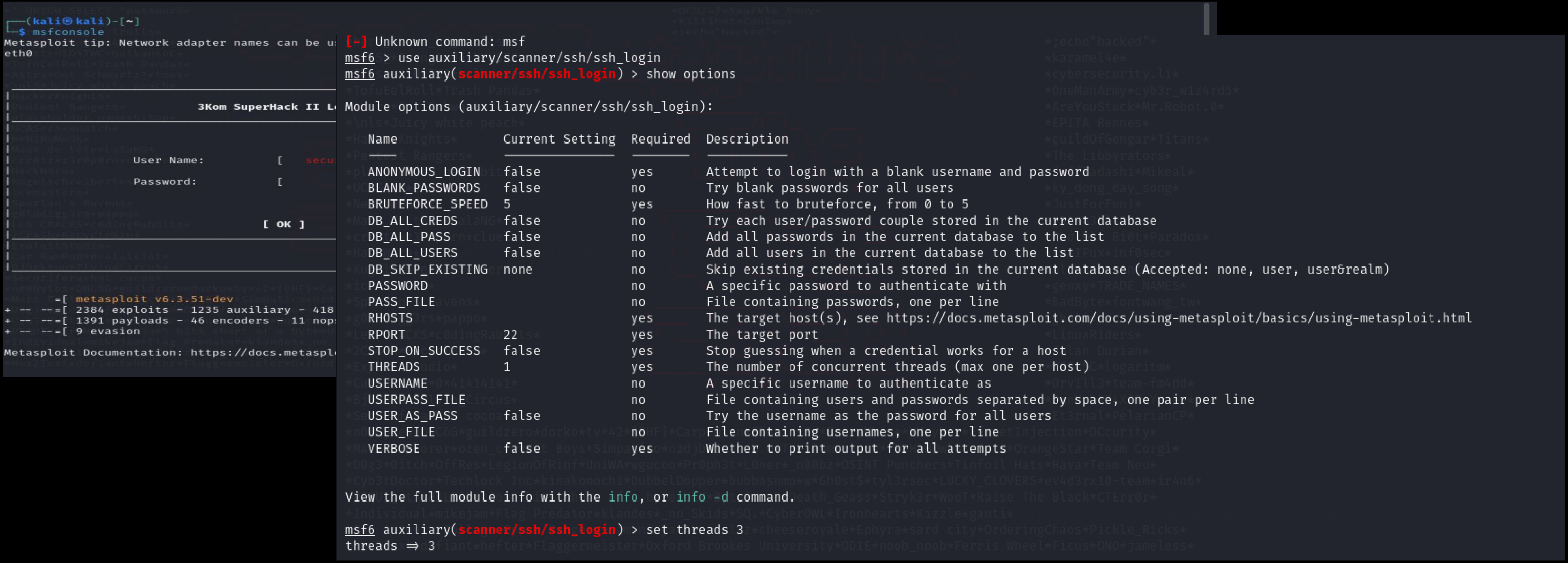
```
0000  ff ff ff ff ff ff e8 48  b8 db c6 e0 08 06 00 01   ·······H ·
0010  08 00 06 04 00 01 e8 48  b8 db c6 e0 c0 a8 01 4a   ·······H ·
0020  00 00 00 00 00 00 c0 a8  01 ef 00 00 00 00 00 00   ········ ·
```

DOPODICHE CON IL TOOL DI NMAP SONO ANDATO AD ANALIZZARE TUTTE LE PORTE ATTIVE



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.87
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 15:01 CEST
Nmap scan report for 192.168.1.87
Host is up (0.0067s latency).
Not shown: 983 filtered tcp ports (no-response)
PORT      STATE  SERVICE         VERSION
80/tcp    open   http            Sky
1234/tcp  open   hotline?
5000/tcp  closed upnp
5001/tcp  closed commplex-link
6000/tcp  closed X11
6100/tcp  closed synchronet-db
8008/tcp  open   tcpwrapped
8080/tcp  open   http-proxy      Sky
8081/tcp  closed blackice-icecap
9080/tcp  closed glrpc
9091/tcp  open   websocket       WebSocket++ 0.4.0
9998/tcp  closed distinct32
9999/tcp  closed abyss
49153/tcp open   unknown
49155/tcp open   tcpwrapped
49160/tcp open   unknown
49163/tcp closed unknown
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-s
ervice :
=============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=============
```

HO PROVATO AD EFFETTUARE UN BRUTEFORCE UTILIZZANDO IL MSFCONSOLE



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Network adapter names can be u
eth0

 ───────────────────────────────────────────
|
|                       3Kom SuperHack II L
 ───────────────────────────────────────────
|
|
|
|          User Name:          [   secu
|
|          Password:           [
|
|
|
|                            [ OK ]
 ───────────────────────────────────────────
|
|
|
 ───────────────────────────────────────────


       =[ metasploit v6.3.51-dev
+ -- --=[ 2384 exploits - 1235 auxiliary - 418
+ -- --=[ 1391 payloads - 46 encoders - 11 nop
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metaspl
```

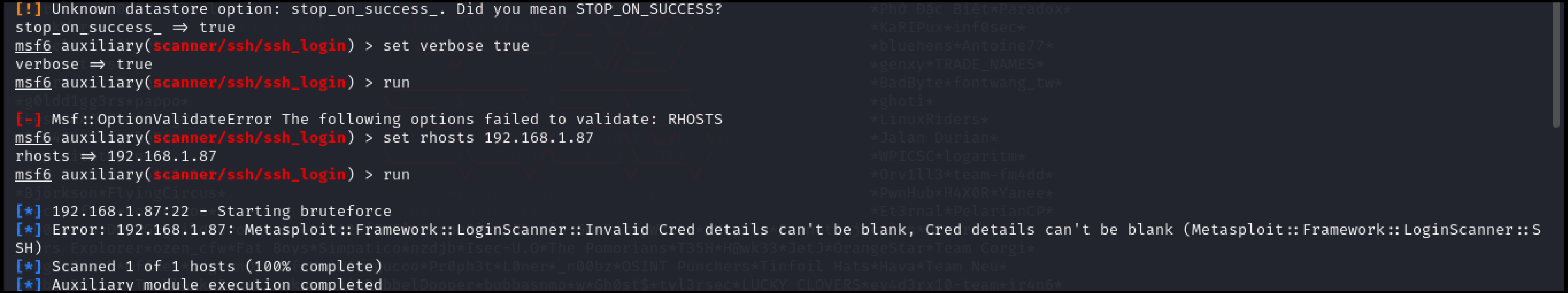
```
[-] Unknown command: msf
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > set threads 3
threads ⇒ 3
```



```
[!] Unknown datastore option: stop_on_success_. Did you mean STOP_ON_SUCCESS?
stop_on_success_ => true
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.1.87
rhosts => 192.168.1.87
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.1.87:22 - Starting bruteforce
[*] Error: 192.168.1.87: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::S
SH)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```