CYB101 Project 5

(🔗 Instructions Page)

👤 Student Name: Hrshit Garg
✉️ Student Email: iharshit.garg.cs@gmail.com

Reflection (Required)

🤔 **Reflection Question #1:** If I had to **explain "how is malware detected?" in 3 emojis,** they would be...
(Feel free to put other comments about your experience in this unit here, too!)

😁😎🔍

👾**Reflection Question #2:** If someone sent you an unknown file, how would you go about checking if it contains a virus?

I will scan it through an anti-virus before installing or downloading it.

📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

Required Challenge Screenshots (Required)

Use the answer boxes below to paste in your screenshots from completing the project. Clarifying notes are optional.
(You don't need any screenshots for **Part 1** or **Part 2.**)

Step 1: Simple Message Virus

Screenshot #1: The commands and output of creating your message virus file

```
codepath@lab000000:~$ msfvenom -a x86 --platform windows -p windows/messagebox TEXT="Virus Executed" -f exe -o messageVirus.exe
No encoder specified, outputting raw payload
Payload size: 267 bytes
Final size of exe file: 73802 bytes
Saved as: messageVirus.exe
codepath@lab000000:~$
```

Notes (Optional)**:**

Project Question #1: Fill in blanks in the **`msfvenom`** command to create the following virus:

- Payload: the (fictional) macOS/messagebox payload with a message of "OOF"
- Target: an x86 architecture laptop running macOS
- Virus File: a osx-app file named appleVirus ending in the .app extension

`msfvenom -a`	x86	**`--platform`**	osx	**`-p`**	macOS/messagebox
`TEXT="OOF"`		**`-f`**	app	**`-o`**	appleVirus.app

Step 2: Multi-Payload Virus

Screenshot #2: The commands and output of creating your multi-payload virus file

```
codepath@lab000000:~$ msfvenom -a x86 --platform windows \
>   -p windows/messagebox TEXT="Virus Executed" \
>   -f raw > messageBox
No encoder specified, outputting raw payload
Payload size: 267 bytes

codepath@lab000000:~$ msfvenom -c messageBox -a x86 --platform windows \
>   -p windows/speak_pwned -f exe -o pwnedVirus.exe
Adding shellcode from messageBox to the payload
No encoder specified, outputting raw payload
Payload size: 830 bytes
Final size of exe file: 73802 bytes
Saved as: pwnedVirus.exe
codepath@lab000000:~$
```

Notes (Optional)**:**

Project Question #2: In a few words, what does the payload **`windows/speak_pwned`** do?

The "payload/windows/speak_pwned" is a Metasploit payload that, when executed on a target system, makes the system "speak" or produce audio output, typically to alert the user that their system has been compromised or "pwned" (hacked).

Step 3: Encrypted Virus

Screenshot #3: The commands and output of creating your encrypted virus file

```
codepath@lab000000:~$ msfvenom -a x86 --platform Windows \
>   -p windows/messagebox TEXT="Encrypted Virus" \
>   -e x86/shikata_ga_nai -i 3 -f python -o messageEncrypted
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 294 (iteration=0)
x86/shikata_ga_nai succeeded with size 321 (iteration=1)
x86/shikata_ga_nai succeeded with size 348 (iteration=2)
x86/shikata_ga_nai chosen with final size 348
Payload size: 348 bytes
Final size of python file: 1722 bytes
Saved as: messageEncrypted
codepath@lab000000:~$ msfvenom -c messageEncrypted -a x86 \
>   --platform windows -p windows/speak_pwned -f exe -o pyVirus.exe
Adding shellcode from messageEncrypted to the payload
No encoder specified, outputting raw payload
Payload size: 2290 bytes
Final size of exe file: 73802 bytes
Saved as: pyVirus.exe
codepath@lab000000:~$
```

Notes (Optional)**:**

Project Question #3: MSFVenom's encoder **`x86/shikata_ga_nai`** is a… (Fill in the blank)

"polymorphic **XOR** **additive feedback encoder"**