CYB101 Project 5

Step 1: Simple Message Virus

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

```
codepath@idx-cyb101-idx-1743190681714:~$ 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
```

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 osx/messagebox TEXT="OOF"
         -f macho              -o appleVirus.app
```

Step 2: Multi-Payload Virus

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

```
codepath@idx-cyb101-idx-1743457161963:~$ 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@idx-cyb101-idx-1743457161963:~$ 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: 843 bytes
Final size of exe file: 73802 bytes
Saved as: pwnedVirus.exe
```

Notes (Optional)**:**

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

The payload says “You got Pawned”

Step 3: Encrypted Virus

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

```
codepath@idx-cyb101-idx-1743457161963:~$ 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@idx-cyb101-idx-1743457161963:~$ 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: 2288 bytes
Final size of exe file: 73802 bytes
Saved as: pyVirus.exe
```

Notes (Optional)**:**

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

“polymorphic XOR additive feedback encoder”