# CYB101 Project 5

(🔗 Instructions Page)

👤 Student Name: Weicong Xie
✉️ Student Email: Weicongx.wx@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 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?

Upload the file onto VirusTotal

> 📣 **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`** | osx-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: 833 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?

It says "Virus Executed" while playing the audio "You Got Pwned!"

## 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: 2298 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"**

## Stretch Challenge (Optional)

**Stretch Challenge #1:** A screenshot showing the results of using **`vt-cli`** to evaluate at least one virus file.

```
codepath@lab000000:~$ vt file e72509072f7912bc882e6d66f66c78f54c3df51b
File "e72509072f7912bc882e6d66f66c78f54c3df51b" not found
codepath@lab000000:~$ vt file 128ac2c4d53c1e8288b211397d488c17594a4721
File "128ac2c4d53c1e8288b211397d488c17594a4721" not found
codepath@lab000000:~$ vt file d48ab783f880e584ca90d46f8348c4af20cbe0e9
File "d48ab783f880e584ca90d46f8348c4af20cbe0e9" not found
codepath@lab000000:~$
```

**Notes** (Optional)**:**

**Stretch Question #1:** Was **`vt-cli`** able to detect your file? Based on what you've learned this unit, what do you think is the reason why or why not?

**Since the virus is new, it isn't on their database.**

> **Stretch Challenge #2:** A screenshot showing the results of uploading one of the virus files to the VirusTotal website.
>
> **[Insert Screenshot Here]**
>
> **Notes** (Optional)**:**

> **Stretch Question #2:** Was VirusTotal able to detect your file?  Based on what you've learned this unit, what do you think is the reason why or why not?

---

## Submission Checklist

👉*Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

**Reflection**

- [x] ~~Reflection Question #1 answered above~~
- [x] ~~Reflection Question #2 answered above~~
- [ ] Shoutouts Completed

**Required Challenge Screenshots and Questions**

- [x] ~~Screenshot #1~~
- [x] ~~Project Question #1~~
- [x] ~~Screenshot #2~~
- [x] ~~Project Question #2~~
- [x] ~~Screenshot #3~~
- [x] ~~Project Question #3~~

**Stretch Challenge**

- [x] ~~Screenshot showing `vt-cli` results~~
- [x] ~~Stretch Question #1~~
- [ ] Screenshot showing VirusTotal.com results
- [ ] Stretch Question #2