CYB101 Project 4

(🔗 Instructions Page)

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

Reflection (Required)

> 🤔 **Reflection Question #1:** If I had to **explain this project's exploit in 3 emojis,** they would be...
> (Feel free to put other comments about your experience this unit here, too!)

🌐🔎🚪

> 🔌**Reflection Question #2:** This project uses a vulnerability on port 21 (FTP). What other ports would you check for vulnerabilities?
> (Tip: The more commonly a port is used, the more likely it is to be vulnerable!)

22 (SSH), 53(DNS), 80 (HTTP), 443 (HTTPS)

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

Required Challenge Video (Required)

Use the answer box below to paste in your Video / GIF(s) completing the project. Clarifying notes are optional.

> **GIF demonstrating the `vsftpd` backdoor exploit**
>
> 🎬 Week_5_Project_4.mp4
>
> **Notes** (Optional)**:**

Stretch Challenge (Optional)

Use the answer box below to paste in your GIF(s) completing the stretch challenge. Clarifying notes are optional.

> **(Optional Stretch Challenge) GIF demonstrating a Metasploit exploit on a different port**
>
> **[Insert GIF Here]**
>
> **Notes** (Optional)**:**

Submission Checklist

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

Reflection

- ☑ ~~Reflection Question #1 answered above~~
- ☑ ~~Reflection Question #2 answered above~~
- ☐ Shoutouts Completed

Required Challenge GIF, showing:

- ☑ ~~Running `lsb_release -a` on both Kali and Metasploitable~~
- ☑ ~~Using `nmap` to verify the vulnerability on port 21~~
- ☑ ~~Running `msfconsole`, then loading and executing the exploit~~
- ☑ ~~Running `lsb_release -a` from inside the exploited shell to prove access to Metasploitable~~

Stretch Challenge GIF

- ☐ GIF showing a Metasploit exploit on a different port