**CYB101 Project 4 (🔗** [**Instructions Page**](https://courses.codepath.org/courses/cyb101/unit/4#!projects)**)**

👤 Student Name: Sila Tamang

✉️ Student Email: stamang3@uco.edu

**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!) |
| --- |
| There are many different ports that could potentially be vulnerable, and the specific vulnerabilities may be present depending on the services running on those ports. Here are a few examples of commonly targeted ports and some of the associated vulnerabilities:   1. Port 22 (SSH): SSH servers can be vulnerable to brute-force attacks if weak passwords are used, or if the server is not configured securely. 2. Port 80 (HTTP): Web servers running on port 80 can be vulnerable to various attacks, such as SQL injection, cross-site scripting (XSS), and file inclusion vulnerabilities. 3. Port 443 (HTTPS): HTTPS services can also be vulnerable to various web-based attacks, as well as to issues such as certificate misconfigurations. 4. Port 445 (SMB): SMB servers can be vulnerable to various exploits, such as EternalBlue, which was famously used in the WannaCry ransomware attack. 5. Port 3389 (RDP): Remote Desktop Protocol (RDP) services can be vulnerable to brute-force attacks and other exploits if not properly secured. |

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

**Required Challenge GIF (Required)**

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

| **GIF demonstrating the vsftpd backdoor exploit** |
| --- |
|  |
| **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** |
| --- |
|  |
| **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~~

**Submit your work!**

| Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit. (This allows our grading team to input your grade below!)      Step 2: **Copy** the link to this document.    Step 3: **Submit** the link on the portal. |
| --- |

**Grader Comments**

| *Once your project has been assessed, our graders will leave feedback for you in this space. Please do not delete.* **Grading Rubric**  | Reflection Questions | Total Received Points | Total Possible | | --- | --- | --- | | Reflection Question #1 answered above | 2 | 2 | | Reflection Question #2 answered above | 2 | 2 | | **PART A TOTAL** | 4 | **4** | | Required Challenge GIF, showing: | Total Received Points | Total Possible | | Running lsb\_release -a on both Kali and Metasploitable | 3 | 3 | | Using nmap to verify the vulnerability on port 21 | 3 | 3 | | Running msfconsole, then loading and executing the exploit | 6 | 6 | | Running lsb\_release -a from inside the exploited shell to prove access to Metasploitable | 4 | 4 | | **PART B TOTAL** | **16** | **16** | | Stretch Challenge | Total Received Points | Total Possible | | GIF showing a Metasploit exploit on a different port | 4 | +4 bonus | | **Total Possible Points (Part A + Part B)** | **4** | **20** (+4) | |  | **24** |  |   **Grader Feedback** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |