**CYB101 Prework (🔗**[**Instructions Page**](https://courses.codepath.org/snippets/cyb101/prework)**)**

👤 Student Name: Sila Tamang

✉️ Student Email: stamang3@uco.edu

For this prework, you’re going to be challenged to explore the giant world of cybersecurity. Don’t worry, there are no “right answers” to these questions – it’s just to get you thinking! Use your search engines and explore!

**Exploratory Questions (Required)**

| **❓ Question #1:** Pick a **🔗**[famous historical hack](https://en.wikipedia.org/wiki/List_of_security_hacking_incidents). What happened and why? (100+ words) |
| --- |
| One famous historical hack is the Stuxnet cyberattack on Iran's nuclear program in 2010. The attack, which was widely believed to have been carried out by the US and Israel, was designed to target and infect the computer systems controlling Iran's nuclear enrichment facilities. The virus was able to spread undetected for months and eventually caused significant damage to Iran's nuclear centrifuges, setting back their nuclear program by several years. The reasons behind the attack remain controversial and classified, but it is widely believed to have been an attempt to prevent Iran from acquiring nuclear weapons. The Stuxnet attack was notable for its sophistication and the level of access it was able to gain to its targets, and it served as a wake-up call for the vulnerability of critical infrastructure to cyberattacks. |

| **❓ Question #2:** If you had a time machine, and could go back and talk to the security team for the hack in Question #1, what advice would you give them on preventing the hack? (100+ words) |
| --- |
| If I could talk to the security team for the Stuxnet hack, I would advise them to prioritize cybersecurity and implement the following steps to prevent a similar attack:   1. Conduct regular security assessments and vulnerability scans to identify and address any potential weaknesses. 2. Implement multi-layered security defenses, including firewalls, antivirus software, and intrusion detection systems. 3. Train employees on cyber security best practices, including how to recognize and avoid phishing attacks. 4. Regularly update software and systems to ensure they are protected against the latest threats. 5. Monitor and log all network activity to detect any unusual or suspicious behavior. 6. Implement strict access control and authentication measures, including unique passwords and two-factor authentication, to limit access to sensitive systems. 7. Regularly back up all critical data and systems to minimize the impact of a potential attack. 8. Work with trusted security experts to stay up-to-date on the latest threats and best practices for protecting against them. |

| **❓ Question #3:** You’ve been tasked with inventing the EASIEST to hack possible device – how would you do it? (What OS would you run, what features would it have, etc.) (100+ words) |
| --- |
| To invent the easiest to hack device, I would create a device with the following characteristics:   1. Run an outdated or unsupported operating system with known vulnerabilities that have not been patched. 2. No security updates or patches available, or not installed. 3. No firewalls or antivirus software installed, or weak and easily bypassable security measures. 4. Weak or easily guessable passwords, with no two-factor authentication or access control measures. 5. No logging or monitoring in place to detect malicious activity. 6. No encryption or secure communication protocols used to protect sensitive data. 7. Little to no user education on cyber security best practices, such as avoiding phishing scams or downloading suspicious software. 8. By creating a device with these features, it would be extremely vulnerable to cyberattacks, making it easy for malicious actors to gain unauthorized access and steal sensitive information or disrupt operations. |

Nice job, that’s everything for the prework!

**Submission Checklist**

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

**Exploratory Questions**

* ~~Question #1 answered above (100+ words)~~
* ~~Question #2 answered above (100+ words)~~
* ~~Question #3 answered above (100+ words)~~

**Submit your work!**

| Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can comment.      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**  | Exploratory Questions | Total Received | Total Possible | | --- | --- | --- | | Question #1 answered above | 4 | 4 | | Question #2 answered above | 4 | 4 | | Question #3 answered above | 4 | 4 | | **Total Points** | 12 | **12** |   **Grader Feedback** **👍 Nice work! You've successfully completed the prework and taken your first step towards building a Cybersecurity mindset!****You'll hear from us soon with more information about the rest of the selection process. In the meantime, feel free to explore the topics from this prework further!** **If you have any particular questions about the prework in general or on any of the feedback, feel free to post on the [Prework Slack channel](https://go.codepath.org/preworkslack).****If you have any technical questions about the project or concepts covered this week, we encourage you to post a question on the course [Prework Slack channel](https://go.codepath.org/preworkslack). For any questions about your application, email us at admissions@codepath.org** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |