

2024 HQ cyber security class

Individual project guideline
(modified version)

① Topics : Cyber security coding using ML,DL Python library

② Language : Python

③ Library : Scikit-learn, TensorFlow on python(choose one)

④ Format : guided format

⑤ Page volumes : 15pages at least

⑥ Submission address : class Google drive

⑦ Submission dead line : Sep 24, 25

⑧ Mission :

- Survey AI security Python source code example from ref. site
- Clone/download the code
- Execute the code, find the error and fix it as far as you do
- Explain the code

⑨ Reference site

AI chatbots: In Vietnam, various generative AI chatbots such as ChatGPT, Gemini AI and Bing Chat are popular.

✓ Gemini AI

Google's latest AI chatbot model, multimodal function
Understands and processes data in various formats.

- Gemini official site: [Gemini AI](#) 1
- DeepMind Gemini tech.page: [DeepMind Gemini](#) 2
- Gemini supporting: [Gemini 지원](#) 3
- Google Cloud Gemini : [Google Cloud Gemini](#) 4

<https://gemini.google.com/app/cae785ec9a0df194>

✓ **Bing AI Chat**

<https://www.bing.com/?toWww=1&redig=A519D80C0451458E816B246AB9A14D8D>

Microsoft's conversational AI service Bing Chat is an AI-based chat tool that can be used for various purposes in Vietnam. When a user asks a question or makes a request, this tool provides answers or helps generate the necessary information.

✓ **WRTN**

Korean site, a platform that provides useful information and opportunities for communication in Vietnam

<https://wrtm.io/en/overview/>

<https://wrtm.ai/>

<https://wrtm.ai/chat/u/663397a3208f03982f4f7dae/c/66c9955571626b4b88890188?type=u>

✓ **Chatgpt**

<https://chatgpt.com/share/f63baf30-74c6-4dcb-8908-f8a1893da6ad>

✓ **git HUB**

Repository exploration: On the main page of GitHub, you can search for topics or languages of interest to explore related repositories. You can check the project overview and usage through the README file of each repository.

✧ **Process of source code exercise**

Sign - up -> log-in -> search the topic code -
> compile the code -> find error -> explain the error -
> explain the code

Individual project topic

(Topic NO. 01) “code example of detecting DoS IP Spoofing using Python Scikit-learn”

(Topic NO. 02) “code example of detecting malware file on my computer using Scikit-learn”

(Topic NO. 03) “code example of detecting DDoS attack using Python Scikit-learn”

(Topic NO. 04) “code example of detecting DoS attacks using TensorFlow”

(Topic NO. 05) “SQL injection Python code example using TensorFlow”:
example

(Topic NO. 06) “malware detection code example on my computer using TensorFlow”

(Topic NO. 07) “code example of how to load other files(excel,html) on scikit learn program”

(Topic NO. 08) “code example of basic process of sklearn.preprocessing using Python Scikit-learn”

(Topic NO. 09) To perform an scanning test on a specific server IP (e.g., 111.111.111.111) using Scikit-Learn in Python

(Topic NO. 10) To perform an security risk analysis on a specific server IP (e.g., 111.111.111.111) using Scikit-Learn in Python

(Topic NO. 11) To perform a web system security check on a specific URL (e.g., https://test.com) using Scikit-Learn

Report format

class	
Student id	
Student name	
Student email	
Submitting date	

1. Title :

2. Purpose of study(under five lines)

(ex)

The purpose of this study is to establish the development direction about the system detecting and responding to the malicious codes. For this, we carried out a research on the domestic and foreign technologies that detect and deal with the spreading malicious codes.

3. Scope of survey(list up the scope of the searching by items)

4. Results of exercise

① Install Python Library

② Clone the Code

③ Execute the program

④ Check error and modify the logics

⑤ Explain your code

5. Conclusion

Feeling and opinion

Table 1. Comparative framework of Education VS. Training

*Source:NIST Special Publication 800-16



Figure 1. Information security learning continuum

*Source:NIST Special Publication 800-16

7. Reference

[1]

[2]