Group project format

(appendix1) Group project report format

|  |
| --- |
|  |
| 2025 CICT high quality class  Group Project Report |
| Network security |

|  |  |  |
| --- | --- | --- |
| Project  Title |  | |
| Project  Area |  | |
| Students | ID | Name |
|  |  |
|  |  |
| Reporting Date |  | |

**Ⅰ. Project Outline**

* **Title**
* Group Information

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Team Name | |  | | | |
| Team Composition | | Name | Belong | Department | Position  /year |
| Professor | | Nguyen Huu Hoa | CICT |  | Rector |
| Instructor | | Noh | CICT | IT Department |  |
| Student | Team Leader |  | CICT | Department of Computer Science |  |
| Team member 2 |  | CICT | Department of Computer Science |  |
| Team member 3 |  | CICT |  |  |
|  | | | | | |
| **Team Photos(essential)** | | | | | |

**Ⅱ. Project Information**

* **Purpose of Project**

This project aims at checking and complementing security vulnerabilities of IT system, capturing the packets to prevent the movement of security attacks, and examines how to forward the packets to the system. We can analyze the data packets in detail to prevent unnecessary packet generation. This project is designed to train basic skill of detection of hacking acks under networking environment.

**2. Project work flow(one model)**

* Telnet to the telnet server from the client
* Attacker Fedora assigned IP address and virtual MAC address of the target to attack
* Perform arp spoof and packet relay attacks on the victims
* Check Session Detection
* If session is detected, session hijacking is executed

**Ⅲ. Action Plan**

1. **Select Environment/IDE (multiple choice possible)**

|  |
| --- |
| 1. VM Ubuntu => activity => terminal => Ubuntu text editor 2. VM Ubuntu => activity => terminal => Ubuntu text editor => text editor Nano ( or other editor) 3. Window Python 4. Window PS 5. Mac OS– 6. Eclipse 7. Webbrowser -> Google Colab and Jupyter notebook 8. Conda 9. VSCode 10. OpenAI Gym 11. Python Pycharm 12. Python Flask/Flask Server with Ngrok 13. XAMPP server 14. Java Script 15. Others name? |

**2. Designing System Architecture(**Front end, Back end, resource)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Items | Resource |  |  |  |
| VM type |  |  |  |  |
| OS |  |  |  |  |
| IP/URL |  |  |  |  |
|  |  |  |  |
| Attacking type |  |  |  |  |
| Detecting type |  |  |  |  |
| Language & version |  |  |  |  |
| Libraries |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Library package |  |  |  |  |
| Algorithm |  |  |  |  |
| AI Technology type |  |  |  |  |
| Database type |  |  |  |  |
| Software tool |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Source code reference |  |  |  |  |
| Dataset reference |  |  |  |  |

3. Role arrangements

|  |  |  |
| --- | --- | --- |
| Student | Division | role |
| 1 | Plan &  design |  |
| 2 | Analysis |  |
| 3 | Implement & test |  |

**4. Project Schedule**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Division | Promotion contents | **Schedule** | | | | | | | |
|  |  |  |  |  |  |  |  |
| Plan | Role sharing and analysis software installation |  |  |  |  |  |  |  |  |
| Analysis | Software option analysis |  |  |  |  |  |  |  |  |
| Test | Analysis using Software function |  |  |  |  |  |  |  |  |
| Finish | Create result document through analysis |  |  |  |  |  |  |  |  |
| Offline meeting  Plan | Information sharing and progress confirmation of each other |  |  |  |  |  |  |  |  |

**Ⅳ. Expected Benefit**

**1. Performance Goals**

ㅇ The application program can be operated through process analysis.

ㅇ Traffic analysis and forensics provide insight into network flows, paths and points of vulnerability.

**2. Benefit**

ㅇ It is possible to identify the wrong route through the traffic self analysis.

ㅇ It can prevent the invasion of malicious code.

ㅇ Acquire expertise knowledge through this project

**Ⅴ. Practice Result**

**[step 1]**

**- Send packet from sender PC to receiver PC, using CMD Ping (or tcping)**

|  |
| --- |
| **“ Snap shote the practice result screen “** |

**[step 2]**

**- Analyze incoming packets on receiver PC using Wireshark tool**

**- Double-click the suspicious packet IP from Wireshark screen to diagnose the**

**detailed packet profile**

|  |
| --- |
| **“ Snap shote the practice result screen “** |

**[step 3]**

**- Block the suspicious incoming IP packets on receiver PC using Windows Firewall**

**(or snort tool) to block incoming packets**

|  |
| --- |
| **“ Snap shote the practice result screen “** |

**[step 4]**

**- Confirm whether the suspicious incoming packet on receiver PC is blocked using Wireshark**

|  |
| --- |
| **“ Snap shote the practice result screen “** |

**[step 5]**

**- Reanalysis of suspicious incoming packet is blocked on receiver PC using the**

**Wireshark tool**

|  |
| --- |
| **“ Snap shote the practice result screen “** |

**[step 6]**

**- Register the bad IP address using rule setting on Window Firewall**

**-> Search rule setting function of VN Window 10 menu and function**

|  |
| --- |
| **“ Snap shote the practice result screen “** |

**[step 7]**

**- Confirm whether the rule setting policy on Windows Firewall run normally**

**-> Search rule setting policy of VN Window10**

|  |
| --- |
| **“ Snap shote the practice result screen “** |

**Ⅵ. Problem and Solution**

**1. Technical issues during project development**

**○ If ICMP (ping) is blocked on the server or firewall ping can not work on the**

**blocked system**

**○ How to open port 80 on a Linux system**

**○ How to open port 80 on a window system**

**Please search the function on VN window 10 firewall**

**Inbound Setup, Inbound Setup and Verification**

**2. Solution(how to solve the problems)**

**Ⅶ. References**

**Appendix (in case of AI coding, submit Source code)**

**Source code file 1**

**Source code file 2**

**Source code file 3**