**Group project development guideline**

* Duration for developing :
* Member : three students per group
* Topics : 8 areas, 18 topics (choose one)
* Report format : MS word guided format
* Page volume : MS word at least 15 pages
* **Date for submitting : Nov.19, 20 2024**
* **Presentation day : Nov.26, 27 2024**

Topic List

|  |  |  |  |
| --- | --- | --- | --- |
| Area | No | Topic | Reference |
| Complex AI  security | 1 | DDoS Attacking, detecting, blocking, confirming coding, Using Tensorflow | * Modify and improve the original source code * Explain improved logic * Submit the source code |
| 2 | Scikit learn, Tensor flow paralled AI program coding for protecting intrusion attacks |
| 3 | Develop Python linked Machine learning for protecting intrusion attacks |
| 4 | Develop code for malicious code detection and protection system Using Complex AI |
| 5 | Develop code for analyzing velnerability of web system using Complex AI |
| 6 | Code how to protect the attacking of malicious infection using Complex AI |
| 7 | -Develop web security pen-test system, connect to cloud system  -Create a security code for securng cloud based application |
| 8 | Develop program for securing cloud application using Complex AI |
| 9 | Develop program for securing cloud application using Complex AI |
| 10 | Develop how to analyze the vulnerability of server system using Complex AI |
| Application | 11 | Introduce methods and procedures for applying Burpsuite | <https://portswigger.net/burp/communitydownload>  <https://portswigger.net/burp/documentation/desktop/penetration-testing> |
| 12 | How to Install and use Acutenix on  Ubuntu | <https://kifarunix.com/how-to-install-acutenix-on-ubuntu-18-04/> |
| Data  base | 13 | How to use OWASP-ZAP (kali linux) | <https://www.zaproxy.org/download/> |
| Network | 14 | How to use Snort3.0  on indow/linux | <https://www.snort.org/downloads> |
| Vulnerability  checking | 15 | Develop finding netwowk vulnerability method using Nessus on Windows/linux/mac | <https://docs.tenable.com/nessus/Content/InstallNessusWindows.htm> |
| Penetration test | 16 | Install Kali Linux Metasploit and practice Penetration | <https://metasploit.help.rapid7.com/docs/installing-the-metasploit-framework>  <https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html> |
| Ethical hacking | 17 | Ethical hacking tools usage | <https://www.edureka.co/blog/ethical-hacking-tools/> |
| Authentication | 18 | Install FreeRADIUS on Ubuntu | <https://computingforgeeks.com/how-to-install-freeradius-and-daloradius-on-ubuntu/> |

**Group project report format**

|  |
| --- |
|  |
| 2024 CICT high quality class  Group Project Report |
| Cyber security |

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

**Ⅰ. Project Outline**

* **Title**
* Group Information

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

**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**

* **Environments & resource**

|  |  |  |
| --- | --- | --- |
|  | | **Details** |
| S/W | OS | CentOS 7, Ubuntu 20, Kali\_Linux |
| IDE | Redhat Linux, Debian Linux |
| language |  |
| tool | Snort, WireShark, TCPdump, barnyard2, |
| H/W | device | Personal PC |
| sensor |  |
| communication |  |
|  |  |

2. Role arrangements

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

**3. 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**

1. **Source code full list**
2. **Running 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 “** |

**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 (Topic no.1-10 cases, submit Source code)**

**Source code file 1**

**Source code file 2**

**Source code file 3**