of common attack techniques such as SQLi, XSS, or DOS. The structure of the paper is as follows: Part II, we summarize some of the current cyber attack techniques; In Part III, we introduce the Cyber Demonstration software with functions and interfaces and finally, Conclusion.

2. CONTENT

2.1. Some common types of cyber-attacks

2.1.1. SQL Injection attack

SQL Injection (SQLi) is a cyber-attack technique that targets databases. Attackers often manipulate middleware with the ability to interact with the database, taking advantage of vulnerabilities that do not fully control the input data on computer software to execute SQL statements on the basis. database [3]. These SQL statements can allow a hacker to bypass login, collect and destroy all data. This is an attack technique that disrupts the translation and can also expose or lose all data.

Figure 1. Illustrating the basic steps in the SQLi attack. Accordingly, hackers will interact with the database through the functions available on the website and execute dangerous SQL statements to exploit the system.

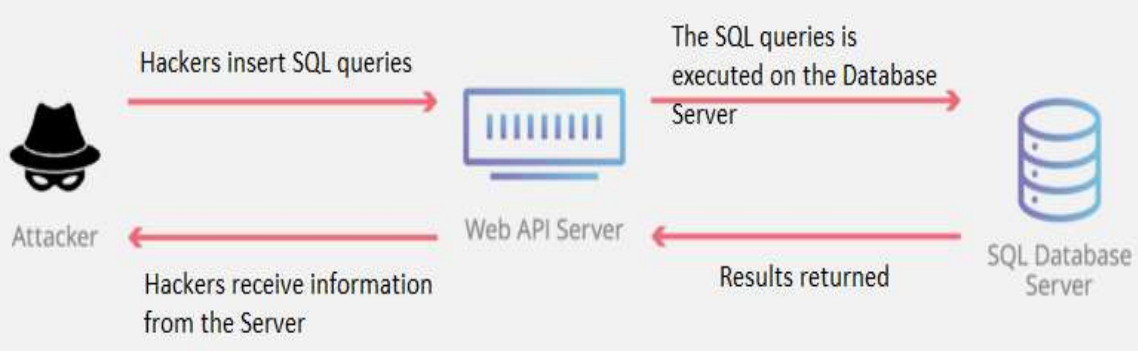

Figure 1. *Illustrating the basic steps in the SQLi attack*

SQLi attacks are classified into 4 primary groups as follows:

- Attack passing log;
- Attack using SELECT statement;
- Attack using INSERT statement;
- Attack using Stored Procedures.

SQLi vulnerabilities can be prevented by examining input data conditions, removing unusual characters and keywords, and limiting feedback from database servers.

2.1.2. Cross-Site Scripting Attack

Cross-Site Scripting (XSS) attack is a technique of inserting HTML tags or scripts that can be dangerous for users into websites. These include potential risks where users who may

have their Cookies stolen, their information typed or interacted on a fake Webpage [4]. Figure 2 depicts the basic steps in an XSS attack.

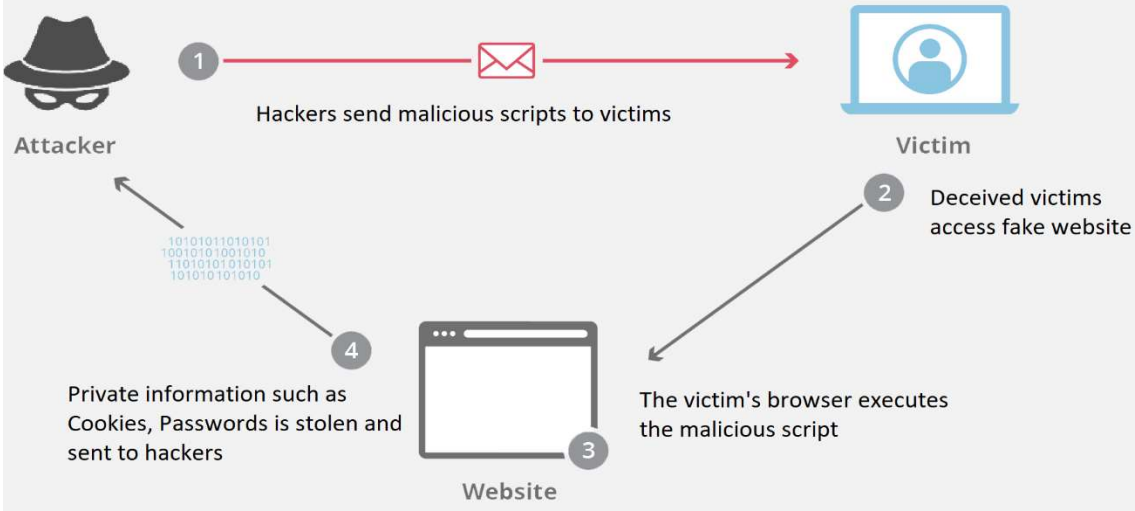

Figure 2. *Basic steps in XSS*

Unlike the SQLi vulnerability that affects database servers, the XSS vulnerability primarily affects Web users.

2.1.3. Password attacks

In most applications, information systems today, passwords are commonly used as an authentication method. Although more reliable authentication methods such as biometric authentication, asymmetric keys, OTP codes are being developed and applied more and more, password authentication still accounts for the majority.

Hackers are always looking for a user's password to gain access to their accounts. We have three techniques for discovering passwords:

- Brute Force: This is a technique that hackers will access the login interface of users, in turn, use the Username / Password pairs to check the probability of success [5]. In particular, the password is the sequence of characters that can be generated in turn in the password space. Hackers try every possible password in turn and stop when they find the right password. This technique has the advantage of undoubtedly yielding results; however, in the case of large password spaces, it takes much time to check, resulting in a lack of practical feasibility.

- Dictionary: This is a technique that tries passwords in turn, similar to Brute Force, but with a more limited password space. This space is made up of information about name, date of birth, personal information, or list of common passwords. Most users tend to set fairly common passwords or passwords related to personal information. Dictionary technology takes advantage of these trends to predict and find passwords faster than Brute Force. However, this technique does not always yield results.

- Keylogger: In this technique, hackers try to find the password from the data obtained from the user's keyboard [6]. To eavesdrop on keyboard data, the spyware will be secretly installed on the victim's device. When all keyboard data is recorded and sent to hackers, they have a high chance of filtering out passwords from this information.

2.1.4. Denial of service attacks

Denial of service is an attack in which hackers take advantage of the design of packets and protocols to execute unusual queries in large numbers, causing the recipient of that query to have resources exhausted, resulting in a usual inability to provide services.

Some techniques of denial of service attacks include SYN Flood, Smurft Attack, Teardrop, or ICMP Flooding [7].

- SYN Flood: In this technique, hackers take advantage of the loophole of the "three-step handshake" procedure in TCP communication to cause system flooding. Hackers will continuously send SYN packets to the receiving machine, receive SYN / ACK packets but do not respond with ACK packets as usual. This causes the victim machine to consistently allocate resources for these processes, resulting in exhaustion of system resources. 0illustrates the steps to attack the SYN Flood.

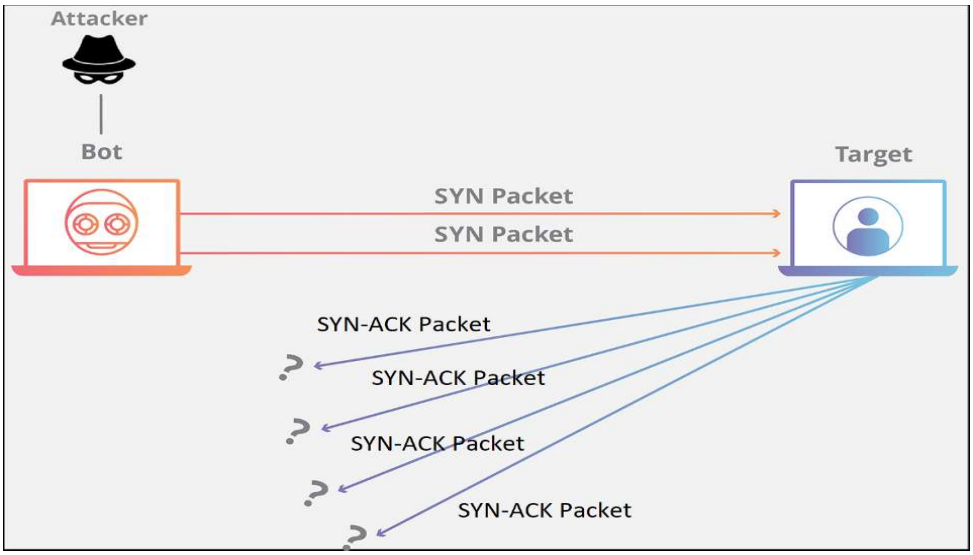

Figure 3. *Illustrates the steps to attack the SYN Flood*

- Smurf Attack: Hackers continuously send a large number of ICMP packets with the source IP address as the address of the victim machine to a network using a broadcast address, other computers in the network receiving ICMP messages will send back the response to the machine with the source IP address as the address of the victim machine; In the case of a vast number of computers in the network, the victim machine will be overloaded, resulting in the inability to operate normally.

- Teardrop attack: All data transmitted on the network to reach the target system must go through two processes: separation at source and reassembling at the destination. In the source system, the data will be divided into packets, each of which has a specific offset value to determine its position in the data. When these packets arrive at the destination, the system will rely on the value of offset to organize the packets to recreate the original data. In a Teardrop attack, hackers will send a series of packets with abnormal and non-renewable offset value to the target system. The destination system will not be able to rearrange the packets after receiving the packet; the system will spend much time to resolve, which results in flooding or errors.

In addition to the classic denial of service techniques, hackers now often use Botnets or servers on the Internet to increase the size of the attack, which is large enough to defeat the large systems in the network for a long time. DDOS -distributed denial of service and DRDOS- reflection denial of service are characteristic of these attacks.

2.2. Introducing the software supporting the training of cyber attack techniques

Besides traditional teaching methods, using whiteboard tools, chalk slides nowadays, new methods, using new tools are always encouraged to be applied to support learning, teaching, improve the vividness and visualization of the lessons.

In this section, we introduce the Cyber Demonstration software, a teaching aid tool built on the Windows operating system. Accordingly, the software will visually and vividly show the fundamental processes of a network attack technique such as SQLi, XSS ..., through scripts, objects, and motion effects designed based on the basis of the theory of that technique.

2.2.1. Platform and development process

Cyber Demonstration software is developed based on C # programming language, Microsoft .NET Framework 4.7.2 platform, Microsoft SQL Server 19 Database management system, and UI platform are Windows Presentation Foundation [8].

Figure 4. *The main steps in building Cyber Demonstration software*

The software development process follows a waterfall model [9], with the main stages described as 0

- Demand survey: Collecting, understanding users' needs;

- Software requirements specification: Defining the functions, environment and operating conditions of the software;

- Scenario design: Based on the theory of network attack techniques such as SQLi, XSS, DOS to build a suitable illustration scenario.

- Software programming: Using C # language, the .Net Framework platforms to design and build software;

- Testing, optimization: Testing and refining, optimizing content based on the opinions of students and teachers.

The software is designed and programmed in the 3-layer model, including GUI Layer, Business Layer, and Data Access Layer, with relationships shown in Figure 5.

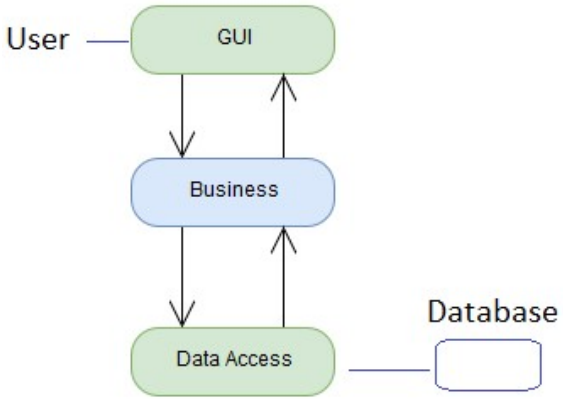

Figure 5. *The 3-layer model in software design*

- GUI Layer: A user interface layer, providing information display functions, providing objects for users to interact with the system.

- Business Layer: This layer receives requests from the GUI layer and accesses the Data Access layer to retrieve information and return to the GUI.

- Data Access Layer: This layer performs the access function to the database, serving queries sent from the Business layer.

2.2.2. The function of the software

Cyber Attack software is installed and operated on Windows operating system environments such as Windows 7, Windows 8.1, and Windows 10. With scenarios simulating standard network attack techniques today, including SQL Attack Injection, Cross-Site Scripting, Denial of Service, Keylogger, Password Detection, Distributed Service Denial, and Denial of Reflection Service. Details of the illustrative techniques are listed in Figure 6.

Each illustrated scenario includes the following components:

(1): Subjects: Including subjects representing objects in an attack such as Hackers (Attacker), Users (Users), Victims (Victim, Server), Control Server (C&C) Server), packets (Packet).

(2) Processes: Include behaviors, interactions between objects to illustrate each stage in a cyberattack.

(3) Descriptions and supporting tools for practice.

Cyber Demonstration	SQL Injection	Bypass
		SELECT
		INSERT
		Procedure Injection
	Cross-Site Scripting	Reflected XSS
		Stored XSS
		DOM-based XSS
	DOS	Tear Drop
		Smurf Attack
		Ping of Death
		SYN Flood
		ICMP Flood
	Password	Brute Force
		Dictionary
	Others	DDOS
		DRDOS
		Keylogger

Figure 6. *The techniques are presented in the software*

2.2.3. Software interface

The main interface of the software is divided into three primary columns. The left column is the list of attack techniques; The right column shows the attack steps, and the middle column is the illustrated scenario. The list of attack techniques presented by the software is listed in Section II.2.

An example of simulating the SYN Flood attack technique with users, hackers, victims, and packets is illustrated in Figure 7.

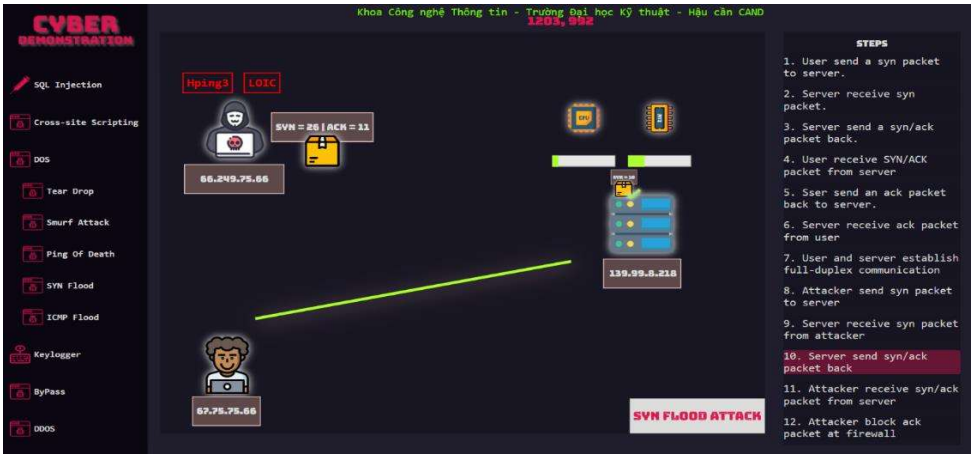

Figure 7. *Illustration interface of the SYN Flood attack technique*

Cyber Demonstration software can be installed simply through the graphical interface, stable operation on two popular operating systems today, Windows 7, and Windows 10. The software is compatible and stably operated with the following utilities: basic presentation tools such as projectors and projection pens.

3. CONCLUSION

In this article, we have summarized some common types of cyber-attacks, such as SQL Injection, Cross Site-Scripting, or Denial of Service. At the same time, we have introduced Cyber Demonstration software to support teachers and students in teaching and to learn about these offensive techniques. The objects, actions, events, and principles in an illustrated, simulated attack help learners gain a new approach when learning about cyber attacking techniques. In the coming time, the author group will continue to develop to upgrade and add new functions and techniques to make the software more useful for users.

REFERENCES

1. "Thủ tướng chính phủ, Quyết định số 99/QĐ-TTg, (2014), Phê duyệt Đề án 'Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020', ngày 14/01/2014."
2. S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Comput. Secur.*, vol. 24, no. 1, pp. 31–43, 2005.
3. J. Viegas and A. Orso (2006), "A classification of SQL-injection attacks and countermeasures," *Int'l Symp. Secur. Softw.*
4. J. Bozic and F. Wotawa (2013), "XSS pattern for attack modeling in testing," *2013 8th Int. Work. Autom. Softw. Test, AST 2013 - Proc.*, pp. 71–74.
5. M. J. H. Heule and O. Kullmann (2019), "The Science of Brute Force," *Best Writ. Math. 2018*, pp. 46–66.
6. M. Wazid et al (2013)., "A framework for detection and prevention of novel keylogger spyware attacks," in *7th International Conference on Intelligent Systems and Control, ISCO 2013*, pp. 433–

438.
7. E. Hugues-Salas *et al (2018).*, "Experimental demonstration of DDoS mitigation over a quantum key distribution (QKD) network using software defined networking (SDN)," *2018 Opt. Fiber Commun. Conf. Expo. OFC 2018 - Proc.*, pp. 1–3.
8. N. A. Roslan, R., & Mohd Zin, (2016) "Dot Net (. NET) Windows form application with Visual Studio.
9. Y. Bassil (2012), "A Simulation Model for the Waterfall Software Development Life Cycle" .

MỘT PHẦN MỀM HỮU ÍCH HỖ TRỢ CHO HỌC TẬP VÀ GIẢNG DẠY VỀ TẤN CÔNG MẠNG

Tóm tắt: *Hiện nay, vấn đề an ninh mạng đang nhận được nhiều quan tâm từ mọi người. Đồng thời, chuyên ngành An toàn thông tin cũng đang được đào tạo ngày càng nhiều ở các trường đại học trong cả nước. Trong bài báo này, chúng tôi trình bày một số kỹ thuật tấn công mạng phổ biến như SQL Injection, Cross Site-Scipting, Denial of Service... và giới thiệu một phần mềm mô phỏng các kỹ thuật đó thông qua các đối tượng, tiến trình và dữ liệu minh họa. Phần mềm hy vọng sẽ là một công cụ hữu ích hỗ trợ giáo viên, học sinh trong quá trình dạy và học.*

Từ khóa: *Công cụ giảng dạy, SQL Injection, Cross Site-Scripting, Denial of Service.*