Research Inventy: International Journal of Engineering And Science
Vol.15, Issue 5 (May 2025), PP 76-81
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

A Study On The Benefits And Effectiveness Of A Deep Analysis Model In Implementing Hands-On Exercises For DDoS Attack Detection And Prevention

Le Kim Trong
Vietnam Korea University of Information and Communications Technology – Danang University, Vietnam

Abstract: Nowadays, the increasing complexity and sophistication of Distributed Denial of Service (DDoS) attacks necessitate the development of advanced practical training systems. These systems are essential for students majoring in Network and Information System Security to gain hands-on experience in detecting, preventing, and thoroughly analyzing DDoS attacks. Traditional training environments are often limited in scope, lack scalability, and fail to incorporate comprehensive analytical tools. To address these shortcomings, this paper proposes a robust and scalable practical model that integrates the Zeek network monitoring platform, an ELK stack-based Security Information and Event Management (SIEM) system, and an attack simulation toolkit comprising Hping3, SlowHTTPTest, and custom Python-based botnet scripts. The system supports an intuitive Kibana-based interface that facilitates early detection and flexible response strategies. Experimental evaluations, including quantitative surveys and statistical analysis, demonstrate a significant improvement in students' analytical and incident response capabilities when utilizing the proposed system compared to traditional models.

Keywords: Network and Information System Security, DDoS Attack, Practical Cybersecurity Training, Intrusion Detection and Prevention, SIEM, Attack Simulation.

Date of Submission: 10-05-2025 Date of Acceptance: 20-05-2025

I. Introduction

In the context of increasingly complex cybersecurity challenges, Distributed Denial of Service (DDoS) attacks continue to pose one of the most persistent and disruptive threats to Internet-based infrastructures. However, most Information Technology training programs - both in Vietnam and globally - still lack modern, scalable, and analytically robust practical platforms. Existing models are frequently constrained by limited student capacity, insufficiently intuitive user interfaces, and a lack of support for realistic attack simulations or customizable botnet scripting environments.

This paper highlights the critical need for a comprehensive, hands-on training system designed to equip students with systematic skills in DDoS detection, prevention, and in-depth attack analysis. The proposed system leverages advanced monitoring and simulation tools to provide a realistic and interactive learning environment, aiming to bridge the gap between theoretical cybersecurity education and practical incident response capabilities.

II. Related Work

In recent years, various studies have explored the development of DDoS attack simulation platforms for both educational and testing purposes. While these efforts have contributed valuable insights, many existing systems rely heavily on manually configured tools, suffer from limited scalability, and lack integrated capabilities for deep traffic analysis [15]. Some implementations utilize virtualized environments; however, they often lack objectivity in evaluation and provide minimal support for effective data visualization [9], [10]. Moreover, to the best of my knowledge in the context of Vietnam, no existing practical training platform provides a fully integrated toolchain that supports the complete cycle of DDoS detection, analysis, and incident response within a hands-on educational environment.

III. System Deployment Model

The proposed system adopts a scalable architecture, comprising several integrated components designed to simulate real-world DDoS scenarios while supporting hands-on analysis and response activities.

Deployment Infrastructure: The environment includes a designated web server as the attack target, a centralized log collection server, a deep analysis node, and multiple attacker machines.

Monitoring and Analysis: Zeek serves as the primary network traffic sensor, capturing and analyzing detailed packet-level behaviors. Zeek logs are forwarded to a centralized ELK stack (Elasticsearch, Logstash, and Kibana) via Filebeat for structured processing and storage.

Visualization Interface: Kibana is deployed as the main visualization tool, enabling students to monitor attack progress in real time. It provides intuitive dashboards for visualizing packet flows, identifying anomalous patterns, and tracking source IP addresses.

Attack Simulation Toolkit: The attacker machines are equipped with various tools including Hping3, SlowHTTPTest, and custom Python-based botnet scripts. These tools are used to generate a variety of DDoS attack patterns such as HTTP Flood, UDP Flood, and Slowloris, etc.

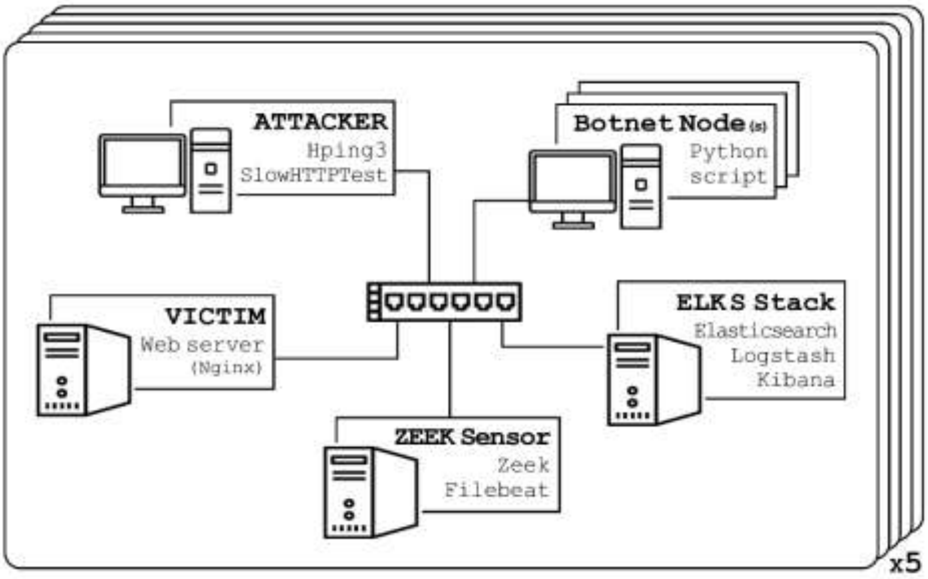

Figure 1.Basic system architecture designed for student groups in the hands-on laboratory environment for DDoS detection and prevention.

Response and Mitigation (Advanced Optional Exercise Extension): The model was further extended to include a router and firewall component, allowing students to engage in advanced hands-on practice involving the configuration of firewalls, Iptables rules, or Zeek policies. These configurations supported both manual and automated responses based on log analysis results. Additionally, the extended model is designed to be compatible with the integration of Security Orchestration, Automation, and Response (SOAR) systems, providing students with exposure to modern security automation practices.

IV. Implementation And Detailed Evaluation

4.1. Participant Description

The study was conducted within the Information System Security course, involving 70 undergraduate students. The course comprised 8 theoretical sessions and 7 practical sessions. Participants were randomly divided into two equal groups:

Control Group (CG): Consisting of 35 students, organized into 5 teams. These students practiced using a traditional model in which teams manually launched DDoS attacks utilizing tools such as Slowloris and Linux commands. Packet capturing and analysis were conducted using Wireshark and Tcpdump without centralized logging or visualization tools.

Experimental Group (EG): Also comprising 35 students, divided into 5 teams. This group engaged with the newly proposed deep analysis model, as described in section System Deployment Model, enabling enhanced monitoring, visualization, and automated detection features.

4.2. **Dependent Variables**

The evaluation focused on the following dependent variables:Pre-test and post-test assessment scores,time required to detect DDoS attacks and complete incident reports, accuracy in identifying abnormal or malicious network packets,analytical and response skills demonstrated during diverse DDoS scenarios.

4.3. **Research Instruments**

The study employed the following instruments:A hands-on laboratory environment specifically designed for practicing DDoS detection and prevention;Structured pre-test and post-test assessments.The pre-test measured students' understanding of foundational concepts introduced during theoretical lectures. The post-test evaluated their ability to apply these concepts in practical scenarios, particularly with regard to detecting, analyzing, and mitigating DDoS attacks using the tools provided in their respective environments.

4.4. **Monitoring and Statistical Methods**

In the Control Group (CG), continuous monitoring proved to be challenging due to the reliance on manual packet analysis and the absence of a centralized traffic analysis and visualization system.

In contrast, the Experimental Group (EG) benefited from real-time monitoring capabilities through a centralized monitoring server. This infrastructure allowed students to observe complete network traffic flows, detect anomalous packets promptly, and initiate appropriate responses to simulated threats.

To ensure the objectivity and accuracy of the evaluation process, statistical analysis was conducted using IBM SPSS Statistics. The main purpose is to analyze the results of the activities, the results of the tests clearly and objectively, to determine whether there is a statistically significant difference in the collected data.

V. RESULTS

5.1. **Pre-Test Results**

To ensure objectivity in the study and eliminate the influence of prior knowledge on the practical performance outcomes, the research team conducted a short theoretical test before the practical phase. The test content focused on fundamental concepts such as the definition of DDoS, common attack methods, the operating principles of detection tools, and log monitoring mechanisms.

Table 1. Statistical Summary of Pre-Test Average Scores for the Two Groups

Group Statistics					
	Group	N	Mean	Std. Deviation	Std. Error Mean
Theory test (Pre-test)	CG	35	6.931	1.4754	.2494
	EG	35	6.891	1.1994	.2027

As shown in Table 1, the pre-test results indicate no significant difference between the control group (CG), with a mean score of 6.931 (standard deviation: 1.4754), and the experimental group (EG), with a mean score of 6.891 (standard deviation: 1.1994).

Table 2. Independent Samples T-Test Results for Pre-Test Scores

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Theory test (Pre-test)	Equal variances assumed	3.010	.087	.124	68	.901	.0400	.3214	-.6013	.6813
	Equal variances not assumed			.124	65.277	.901	.0400	.3214	-.6018	.6818

The Levene's F-test for equality of variances yielded a significance value (Sig.) of 0.087, which is greater than 0.05, indicating no significant difference in variance between the CG and EG groups. Therefore, we use the results from the t-test assuming equal variances. The significance value (Sig.) of the t-test is 0.901, also greater than 0.05, allowing us to accept the null hypothesis that there is no significant difference between the CG and EG groups. This indicates that both groups had equivalent foundational knowledge before the practical training phase.

5.2. **Average Time to Detect and Complete the Attack Report**

To evaluate students' ability to respond to cyberattacks, this study measured the average time required by each student team to detect and complete a report on a Distributed Denial of Service (DDoS) attack. The measurement started from the onset of the attack and ended when the student teams - acting as cybersecurity defense units - successfully identified abnormal network traffic, confirmed the presence of a DDoS attack on the web server, and submitted a comprehensive incident report using the provided template.

Table 3. Time to Detect and Complete the Attack Report (unit: minutes)

Group	Team 1	Team 2	Team 3	Team 4	Team 5	Team 6	Team 7	**Average**
Control Group Lab	121	146	189	138	138	118	145	142,14
Experimental Group Lab	85	91	107	110	96	100	115	100,57

The statistical results indicate that the experimental groups (EG) completed the task in an average of 100.57 minutes, whereas the control groups (CG) required an average of 142.14 minutes. This substantial difference is attributed to the advantage provided by enhanced monitoring tools available to the EG students - specifically, real-time data visualization through the Kibana dashboard and automated alerts generated by Zeek. These tools significantly improved their ability to identify anomalies and extract relevant information efficiently, thereby accelerating the report completion process.

5.3.Post-Test Results

Following the practical training, a post-test was conducted to evaluate whether the CG and EG students, after gaining additional hands-on experience and applied knowledge, had equivalent understanding of advanced theoretical concepts. As shown in Table 4, the results indicate a significant difference between the control group (CG), which had an average score of 6.889 (standard deviation: 1.0312), and the experimental group (EG), which achieved a higher average score of 7.731 (standard deviation: 0.9499).

Table 4. Statistical Summary of Post-Test Average Scores for the Two Groups

Group Statistics					
	Group	N	Mean	Std. Deviation	Std. Error Mean
Theory Test (Post-Test)	CG	35	6.889	1.0312	.1743
	EG	35	7.731	.9499	.1606

Table 5. Independent Samples T-Test Results for Post-Test Scores

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Theory Test (Post-Test)	Equal variances assumed	.467	.497	-3.557	68	.001	-.8429	.2370	-1.3157	-.3700
	Equal variances not assumed			-3.557	67.546	.001	-.8429	.2370	-1.3158	-.3699

The Levene's F-test for equality of variances yielded a significance value (Sig.) of 0.497, which is greater than 0.05, indicating no significant difference in variance between the CG and EG groups. Therefore, we use the t-test results under the assumption of equal variances. The t-test significance value (Sig.) was 0.001, which is less than 0.05, indicating a statistically significant difference between the two groups.

This result suggests that students in the experimental group, who practiced in a lab equipped with a comprehensive model for monitoring and in-depth analysis, acquired significantly more knowledge during the practical training compared to those in the traditional lab setting. This can be attributed to the fact that the experimental group worked with a more diverse, interactive, and detailed practice model, which was built upon the Zeek monitoring platform, an ELK stack-integrated SIEM system, and a wide range of attack simulation tools including Hping3, SlowHTTPTest, and custom Python-based botnet scripts.

5.4. Results of the Combined practice test

The combined practice test was designed to assess students' practical skills by simulating a DDoS attack scenario requiring detection, analysis, and response. The grading criteria included: the ability to identify abnormal traffic, analyze and visualize collected data, configure alerts, implement countermeasures, and compile a final report.

Table 6. Statistical Summary of Average Scores on the Combined practice test for Both Groups

Group Statistics					
	Group	N	Mean	Std. Deviation	Std. Error Mean
Combined practice test	CG	35	7.274	.9237	.1561
	EG	35	8.371	.8594	.1453

As shown in Table 6, the results indicate a significant difference between the control group (CG), which had a mean score of 7.274 with a standard deviation of 0.9237, and the experimental group (EG), which achieved a higher mean score of 8.371 with the same standard deviation of 0.8594.

Table 7. Independent Samples T-Test Results for the Combined practice test

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Combined practice test	Equal variances assumed	.031	.861	-5.145	68	.000	-1.0971	.2133	-1.5227	-.6716
	Equal variances not assumed			-5.145	67.650	.000	-1.0971	.2133	-1.5227	-.6716

The Levene's F-test for equality of variances returned a significance value (Sig.) of 0.861, which is greater than 0.05, indicating no significant difference in variances between the CG and EG groups. Therefore, the t-test result under the assumption of equal variances was used. The t-test yielded a significance value (Sig.) of 0.000, which is less than 0.05, indicating a statistically significant difference between the two groups.

In addition to the test scores, observations during the practical sessions revealed that students in the EG group demonstrated greater flexibility, responded more quickly to Zeek logs, knew how to configure alerts, and could write detection rules tailored to each attack scenario. In contrast, many students in the CG group appeared passive, failed to detect attacks within the allotted time, or were only able to review logs without implementing timely responses.

These results confirm that a standardized training environment equipped with specialized tools significantly enhanced students' ability to apply knowledge and solve problems in simulated network security situations.Moreover, due to reduced time spent on basic tasks, two teams within the EG group were able to proceed to implement an extended response model (as part of the optional advanced practice), using Iptablesand Zeek policy scripts to configure automated responses based on log analysis results.

V. Conclusion And Future Directions

This study provides clear empirical evidence of the effectiveness of a hands-on training model for detecting and mitigating DDoS attacks through the integration of powerful security monitoring tools such as Zeekand the ELK Stack, combined with a diverse set of attack simulation tools including Hping3**,**SlowHTTPTest**,** and custom Python-based botnet scripts**.** Beyond improving academic performance, the model also demonstrated its comprehensive impact on the development of critical skills such as data analysis, rapid incident response, alert configuration, and the ability to write customized detection rules for specific scenarios. These are essential competencies for information security professionals in real-world environments.

Through statistical analyses such as the t-test, the research team demonstrated statistically significant differences between the control and experimental groups in both theoretical understanding and practical skills. The model enabled EG students to detect attacks faster, respond more accurately, and show greater proficiency in analyzing Zeek logs and building customized dashboards using Kibana.

Based on the research results and real-world evaluations, this can be considered a comprehensive and modern solution with high applicability and scalability for IT education institutions - particularly in advanced cybersecurity training in the digital era.

In the future, the system can be extended with the following developments:

- Integration of Security Orchestration, Automation, and Response (SOAR) systems.
- Development of instructor dashboards for real-time performance evaluation of teams.
- Application of AI and machine learning to enhance the analysis of abnormal behaviors.

The full implementation of these models in practical exercises related to network security, digital forensics, and system safety will significantly enhance the quality of education and students' preparedness to respond to real-world threats.

References

[1]. Abdelsayed, S., Glimsholt, D., Leckie, C., Ryan, S., & Shami, S. (2003). An efficient filter for denial-of-service bandwidth attacks. In Proceedings of the 46th IEEE Global Telecommunications Conference (GLOBECOM'03), 1353–1357.

[2]. Barford, P., Kline, J., Plonka, D., & Ron, A. (2002). A signal analysis of network traffic anomalies. In Proceedings of the 2nd ACM SIGCOMM Internet Measurement Workshop, November 2002.

[3]. Bekeneva, Y., Borisenko, K., Shorov, A., & Kotenko, I. (2015). Investigation of DDoS Attacks by Hybrid Simulation. In Information and Communication Technology (pp. 179–189). Springer.

[4]. Brooks, R.R., & Özçelik, I. (2020). DDoS research: testing. In Distributed Denial of Service Attacks, pp. 93–106. Chapman and Hall/CRC.

[5]. Cheng, C.-M., Kung, H. T., & Tan, K.-S. (2002). Use of spectral analysis in defense against DoS attacks. In Proceedings of IEEE GLOBECOM 2002, 2143–2148.

[6]. Cisco, & Riverhead Networks. (2001). Diversion and Sieving Techniques to Defeat DDoS Attacks. NANOG23.

[7]. Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. Computer Networks, 44(5), 643–666.

[8]. Froutan, P. (2004). How to Defend Against DDoS Attacks. Computerworld.

[9]. Furfaro, A., Pace, P., Parise, A., & Valdiviezo, L.M. (2014). Modelling and Simulation of a Defense Strategy to Face Indirect DDoS Flooding Attacks. In Internet and Distributed Computing Systems (pp. 263–274). Springer.

[10]. Machaka, P., & Bagula, A. (2021). Statistical properties and modelling of DDoS attacks. In Vinh, P.C., & Rakib, A. (Eds.), ICCASA/ICTCC -2020, LNICSSITE, vol. 343, pp. 44–54. Springer, Cham.

[11]. Machaka, P., Ajayi, O., Kahenga, F., Bagula, A., & Kyamakya, K. (2022). Modelling DDoS Attacks in IoT Networks Using Machine Learning. In Emerging Technologies for Developing Countries – AFRICATEK 2022 (pp. 145–157). Springer.

[12]. Patrikakis, C., Masikos, M., & Zouraraki, O. (2004). Distributed Denial of Service Attacks. The Internet Protocol Journal, 7(4), 13–35.

[13]. Reddy, R. P. (2024). A Survey of Distributed Denial of Service (DDoS) Attack Mitigation Techniques. International Journal of Computer Trends and Technology, 72(12), 69–77.

[14]. Revathi, M., Ramalingam, V.V., & Amutha, B. (2022). A Machine Learning Based Detection and Mitigation of the DDoS Attack by Using SDN Controller Framework. Wireless Personal Communications, 127, 2417–2441.

[15]. Sinha, S., & Mahadev Prasad, N. (2021). Distributed Denial of Service Attack Detection and Prevention in Local Area Networks. In Innovative Data Communication Technologies and Application (pp. 321–330). Springer.

[16]. Zaed, M., & Al-Mousa, A. (2024). Detection of Real-Time Distributed Denial-of-Service (DDoS) Attacks on Internet of Things (IoT) Networks Using Machine Learning Algorithms. Computers, Materials & Continua, 78(2), 1234–1245.