International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Assessment of Information Gathering, Footprinting, and Vulnerability Assessment Competencies Among BSIT Students: Basis for a Cybersecurity Training Framework

Roseline B. Lorican; Jomar C. Igloso; Judelyn C. Felicia; Steven Jay B. Cabil; Glenn Ian T. Olano; Khian Emmanuel Abraham; Joe D. Basanta, MIT**; Kristine T. Soberano,** Ph.D., DIT

State University of Northern Negros, Philippines

DOI: https://doi.org/10.47760/ijcsmc.2026.v15i08.001

Abstract:
The increasing prevalence of cybersecurity threats has emphasized the need for Information Technology (IT) graduates to possess essential cybersecurity competencies. This study assessed the competencies of fourth-year Bachelor of Science in Information Technology (BSIT) students of Bohol Northern Star College in the areas of information gathering, footprinting, and vulnerability assessment as a basis for developing a cybersecurity training framework. The study employed a descriptive-developmental research design using a quantitative approach. A total enumeration sampling technique was utilized, involving 21 fourth-year BSIT students as respondents. Data were collected through a researcher-developed and expert-validated questionnaire and were analyzed using weighted mean and ranking.
The findings revealed that the respondents demonstrated a high level of competency in information gathering, footprinting, and vulnerability assessment. The results indicate that the students have acquired sufficient knowledge and skills in performing fundamental cybersecurity activities, including gathering security-related information, conducting reconnaissance activities, identifying potential vulnerabilities, and understanding security assessment processes. Despite the high competency level, continuous enhancement through structured training, hands-on

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

laboratory activities, and practical cybersecurity exercises is recommended to further improve students' technical capabilities.
Based on the findings, a cybersecurity training framework was proposed to strengthen the practical cybersecurity skills of BSIT students. The framework focuses on information gathering, footprinting, vulnerability assessment, cybersecurity tools utilization, and applied security assessment activities. The study concludes that continuous cybersecurity education and practical skill development are essential in preparing BSIT students for the evolving demands of the IT industry.

Keywords: Cybersecurity Competency; Information Gathering; Footprinting; Vulnerability Assessment; BSIT Students; Cybersecurity Training Framework

INTRODUCTION

In today's digital environment, the increasing use of technology has also brought new challenges in protecting information systems, networks, and data from cyber threats. Organizations and individuals continue to experience different forms of cyberattacks, making cybersecurity knowledge and skills an important part of information technology education. As future IT professionals, students must develop the necessary competencies to identify possible threats, assess system weaknesses, and apply appropriate security practices.

Information gathering, footprinting, and vulnerability assessment are essential skills in cybersecurity because they serve as the foundation for understanding and identifying security risks. Information gathering allows security professionals to collect relevant details about systems, networks, and digital assets. Footprinting helps in analyzing available information about a target environment, while vulnerability assessment focuses on identifying weaknesses that may be exploited by attackers. Developing these skills enables students to better understand how cyber threats occur and how preventive measures can be applied.

The Bachelor of Science in Information Technology (BSIT) program plays an important role in preparing students for careers related to technology and cybersecurity. Through different courses and laboratory activities, students are introduced to networking, system administration, information security, and other areas that support cybersecurity practices. However, the level of competency of students in performing information gathering, footprinting, and vulnerability assessment activities may vary depending on their learning experiences, exposure to cybersecurity tools, and available training opportunities.

At Bohol Northern Star College, BSIT students are expected to acquire knowledge and skills that will help them respond to the growing demands of the IT industry. Assessing their competencies in cybersecurity-related activities can provide valuable information regarding their strengths and areas that need further improvement. The results of this assessment may serve as a basis for

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

developing a cybersecurity training framework that can enhance students' practical skills and better prepare them for future professional responsibilities.

This study aims to assess the information gathering, footprinting, and vulnerability assessment competencies of BSIT students at Bohol Northern Star College. Specifically, it seeks to determine their level of knowledge and skills in these areas and identify possible training needs. The findings of this study may contribute to the improvement of cybersecurity education and the development of appropriate training activities that will strengthen the cybersecurity capabilities of BSIT students.

REVIEW RELATED LITERATURE

Cybersecurity Education and Competency Development Among IT Students

The rapid advancement of technology has increased the demand for professionals who possess sufficient knowledge and skills in cybersecurity. Organizations today rely heavily on information systems, networks, and digital platforms, making cybersecurity competencies essential among Information Technology (IT) graduates. Higher education institutions play an important role in preparing students by providing academic foundations and practical experiences that develop their ability to identify, prevent, and respond to cyber threats. Studies emphasize that cybersecurity education should not only focus on theoretical concepts but also develop students' practical skills through competency-based learning approaches.

Cybersecurity competencies involve a combination of technical knowledge, problem-solving abilities, and hands-on skills needed to protect computer systems and information resources. These competencies include network security, vulnerability identification, risk assessment, ethical hacking, and security management. According to cybersecurity education studies, there is a growing need for higher education institutions to evaluate whether students are acquiring the skills required by the IT industry. Competency assessment provides educators with information about students' strengths, weaknesses, and areas that require additional training.

For BSIT programs, developing cybersecurity competency is important because graduates are expected to handle various security-related tasks in professional environments. Students must understand how attackers gather information, identify weaknesses, and exploit vulnerabilities so that they can implement appropriate security measures. Therefore, assessing cybersecurity-related competencies among BSIT students can help institutions design effective learning activities and training programs.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Information Gathering in Cybersecurity

Information gathering is considered one of the initial and most important stages in cybersecurity assessment and ethical hacking. It involves collecting relevant information about a target system, network, or organization to understand its structure, available services, and possible security risks. Security professionals use information gathering techniques to identify potential attack surfaces and develop appropriate security strategies.

Information gathering may involve passive and active approaches. Passive information gathering focuses on collecting publicly available information without directly interacting with the target system, while active information gathering involves direct interaction such as network scanning and service identification. These activities help cybersecurity professionals understand the environment being assessed and identify possible entry points that may require protection.

For IT students, learning information gathering techniques provides foundational knowledge in cybersecurity assessment. Familiarity with tools used for reconnaissance and information collection enables students to better understand how attackers discover system weaknesses. Developing these skills also helps students appreciate the importance of securing publicly available information and minimizing unnecessary exposure of organizational assets.

Footprinting and Reconnaissance Skills

Footprinting is an important cybersecurity concept that focuses on gathering detailed information about a target before conducting security testing. It involves identifying information such as domain details, network infrastructure, technologies used, and publicly available resources. Footprinting is commonly associated with the reconnaissance phase of penetration testing because it provides security professionals with an initial understanding of the target environment. Reconnaissance activities help identify possible vulnerabilities by analyzing information collected from different sources. Security practitioners use various methods, including search engines, publicly available databases, network analysis tools, and other reconnaissance techniques, to create a profile of the target system. The information gathered during this stage helps determine possible risks and security weaknesses.

For BSIT students, developing footprinting skills is necessary because it strengthens their understanding of how cyberattacks begin. By learning ethical reconnaissance techniques, students can develop the ability to think from both defensive and offensive perspectives. This knowledge allows future IT professionals to identify exposed information and recommend appropriate security improvements.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Vulnerability Assessment Competencies

Vulnerability assessment is a systematic process of identifying, analyzing, and evaluating weaknesses within computer systems, applications, and networks. It is an essential cybersecurity activity because it helps organizations discover security problems before attackers can exploit them. Vulnerability assessments commonly involve scanning systems, analyzing identified weaknesses, and recommending possible solutions.

The ability to perform vulnerability assessments requires technical knowledge of operating systems, networks, applications, and security tools. Students must understand how vulnerabilities occur and how security controls can reduce potential risks. Research on cybersecurity education highlights that practical competency development is necessary because cybersecurity professionals must be capable of applying knowledge in real-world situations rather than only understanding concepts theoretically.

In the context of BSIT education, vulnerability assessment activities can enhance students' analytical and technical abilities. Laboratory exercises, cybersecurity simulations, and practical assessments can provide opportunities for students to apply security concepts and develop confidence in performing security evaluations.

Cybersecurity Training Framework for Higher Education

A cybersecurity training framework provides a structured approach for developing knowledge, skills, and competencies among learners. It identifies the necessary learning areas, training activities, assessment methods, and improvement strategies needed to strengthen cybersecurity capabilities. Developing such a framework requires understanding students' existing competencies and identifying specific areas where additional training is needed.

Studies on cybersecurity education emphasize the importance of aligning academic training with industry expectations. Higher education institutions must continuously improve cybersecurity curricula to ensure that graduates possess relevant skills required in professional environments. Competency-based assessment helps educators design training programs that focus on measurable learning outcomes and practical skill development.

For Bohol Northern Star College, assessing the information gathering, footprinting, and vulnerability assessment competencies of BSIT students can provide valuable insights for improving cybersecurity instruction. The results of the assessment may serve as a foundation for creating a cybersecurity training framework that addresses students' learning needs and enhances their preparedness for future IT careers.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Cybersecurity Competencies of Information Technology Students in the Philippine Context

The increasing dependence on digital technologies has created a greater need for Information Technology graduates who possess adequate cybersecurity knowledge and practical skills. In the Philippines, higher education institutions are continuously improving IT-related programs to ensure that graduates acquire competencies aligned with industry requirements. Cybersecurity has become an important component of IT education because future IT professionals are expected to manage information systems, protect digital resources, and respond to security threats.

According to studies involving IT students, cybersecurity competency is not limited to awareness of security concepts but also includes the ability to apply security practices in real-world situations. Knowledge of information assurance, risk management, security controls, and safe computing practices contributes to students' ability to protect information systems. A recent study among BSIT students emphasized that information assurance and security knowledge influence cybersecurity protection practices, suggesting that stronger cybersecurity education may improve students' ability to apply protective measures against cyber threats.

For institutions offering the Bachelor of Science in Information Technology program, assessing cybersecurity competencies provides important information regarding students' preparedness for professional practice. Identifying competency gaps allows educators to develop appropriate interventions, laboratory activities, and specialized training programs that address students' learning needs.

Integration of Cybersecurity Concepts in IT Curriculum

The integration of cybersecurity concepts into academic programs is necessary to prepare students for the changing demands of the technology industry. Cybersecurity education requires continuous improvement because cyber threats continue to evolve. Higher education institutions are encouraged to include cybersecurity topics across different IT courses instead of treating security as an isolated subject only.

Studies have shown that incorporating cybersecurity concepts into existing IT courses can improve students' understanding of security practices. Through continuous exposure to security-related topics, students develop better awareness of threats, vulnerabilities, and preventive strategies. Activities such as laboratory exercises, security assessments, simulations, and practical projects provide students with opportunities to apply cybersecurity knowledge in realistic scenarios.

In the context of BSIT education at Bohol Northern Star College, integrating information gathering, footprinting, and vulnerability assessment activities can strengthen students' technical

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

capabilities. These skills support the development of cybersecurity awareness and provide students with practical experiences that may be useful in future IT careers.

Importance of Hands-on Learning in Cybersecurity Education

Cybersecurity is a field that requires both theoretical understanding and practical application. Traditional classroom discussions alone may not be sufficient to develop the technical skills needed by future cybersecurity professionals. Hands-on activities allow students to experience actual security scenarios, analyze vulnerabilities, and practice defensive strategies in controlled environments.

Research on cybersecurity education highlights that effective cybersecurity learning commonly involves laboratory exercises, security tools, practical assessments, and simulation-based activities. These approaches allow students to develop problem-solving skills and improve their confidence in handling security-related tasks.

For example, activities involving reconnaissance, network scanning, vulnerability identification, and security analysis can help students understand the relationship between attacker techniques and defensive strategies. By performing these activities ethically within a controlled environment, students can develop critical thinking skills necessary for cybersecurity roles.

Competency-Based Assessment in Information Technology Education

Competency assessment is an important process in determining whether students possess the knowledge, skills, and abilities required for a specific field. In IT education, competency-based approaches focus on measuring students' ability to perform tasks rather than simply evaluating their understanding of concepts.

A competency-based assessment provides educators with evidence of students' current capabilities and areas requiring improvement. This approach is particularly valuable in cybersecurity because technical skills must be demonstrated through actual performance. Students may understand cybersecurity concepts theoretically but may require additional practice in applying tools and techniques for information gathering, footprinting, and vulnerability assessment.

Therefore, evaluating the cybersecurity competencies of BSIT students can serve as a basis for designing targeted training programs. The results can guide faculty members in developing learning activities that address specific skill gaps and improve students' readiness for cybersecurity-related responsibilities.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Cybersecurity Training Framework Development

A cybersecurity training framework provides a structured guide for improving learners' knowledge, skills, and abilities in cybersecurity. It identifies essential competencies, learning activities, assessment strategies, and appropriate training approaches needed to develop capable cybersecurity practitioners.

Developing a training framework requires an understanding of students' existing competencies and the skills expected by the industry. Research on cybersecurity education emphasizes the importance of aligning academic instruction with practical workplace requirements. Graduates need not only technical knowledge but also analytical thinking, problem-solving skills, ethical awareness, and adaptability.

For BSIT students of Bohol Northern Star College, the development of a cybersecurity training framework based on competency assessment results may provide a structured approach to improving cybersecurity education. Such a framework can support faculty members in planning laboratory activities, selecting appropriate cybersecurity tools, and creating learning experiences that strengthen students' technical abilities.

Synthesis of the Literature

The reviewed literature highlights the importance of cybersecurity competency development among IT students. Information gathering, footprinting, and vulnerability assessment serve as fundamental skills that support effective cybersecurity practices. Previous studies emphasize that competency-based assessment allows educational institutions to determine students' capabilities and identify areas requiring improvement.

Although cybersecurity education continues to improve, there remains a need to evaluate the actual competency levels of students in performing practical security tasks. Assessing BSIT students of Bohol Northern Star College provides an opportunity to determine their current skills and develop appropriate training interventions. The findings of this study may contribute to strengthening cybersecurity education and preparing students for the demands of the IT industry.

Existing literature also highlights the importance of practical learning experiences, competency-based assessment, and curriculum integration in improving cybersecurity skills among IT students. Philippine studies indicate that BSIT students require continuous enhancement of cybersecurity knowledge and practices to meet the expectations of the IT industry.

Based on the reviewed literature, assessing the cybersecurity competencies of BSIT students at Bohol Northern Star College is necessary to determine their current level of skills and identify areas for improvement. The findings of this study may serve as a foundation for developing a

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

cybersecurity training framework that strengthens students' capabilities in information gathering, footprinting, and vulnerability assessment.

RESEARCH METHODOLOGY

Research Design

This study will employ a Descriptive-Developmental Research Design using a quantitative research approach**.** The descriptive method will be used to assess the competency level of fourth-year Bachelor of Science in Information Technology (BSIT) students of Bohol Northern Star College in terms of information gathering, footprinting, and vulnerability assessment.

The descriptive research design is appropriate for this study because it aims to determine and describe the existing level of cybersecurity competencies of the respondents based on their knowledge, skills, and understanding of cybersecurity-related activities. It allows the researchers to gather measurable data regarding students' capabilities without manipulating any variables.

Furthermore, the developmental aspect of the research will be applied in creating a proposed Cybersecurity Training Framework based on the results of the competency assessment. The framework will focus on addressing identified competency gaps and strengthening the cybersecurity skills of BSIT students through appropriate training topics, activities, and assessment strategies.

Since the respondents are fourth-year BSIT students, they are expected to have completed most of their major IT courses, including subjects related to programming, networking, information assurance, systems administration, and other technology-related areas. Therefore, assessing their cybersecurity competencies provides an opportunity to determine their level of preparedness before entering the professional IT environment.

Research Locale

The study will be conducted at Bohol Northern Star College (BNSC) located in Ubay, Bohol. The institution offers the Bachelor of Science in Information Technology (BSIT) program, which aims to develop students' technical knowledge and skills in various areas of information technology.

The BSIT program provides learning experiences in computer programming, database management, networking, systems development, and information security. These areas support the development of cybersecurity-related competencies needed by future IT professionals.

Bohol Northern Star College was selected as the research locale because the institution's fourth-year BSIT students have already undergone several years of IT education and exposure to

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

different computing concepts. Their competency assessment can provide relevant information that may contribute to improving cybersecurity instruction and developing a training framework suited to their needs.

Research Respondents

The respondents of this study will be the fourth-year Bachelor of Science in Information Technology (BSIT) students of Bohol Northern Star College.

Fourth-year BSIT students are selected as respondents because they have acquired substantial knowledge and skills from their previous IT courses. At this level, students are expected to have foundational understanding and practical experience in areas related to computer systems, networking, programming, database management, and information security.

The study employed total enumeration sampling since the target population consisted of only 21 fourth-year BSIT students. Including all members of the population allowed the researchers to obtain a complete representation of the cybersecurity competency level of the graduating BSIT students of Bohol Northern Star College. This sampling technique is appropriate because the target population is limited and accessible, allowing the researchers to obtain a complete assessment of the cybersecurity competencies of the identified group.

The inclusion of all fourth-year BSIT students ensures that the results accurately represent the competency level of the graduating BSIT students of Bohol Northern Star College.

Research Instrument

The primary instrument that will be used in this study is a researcher-made questionnaire designed to assess the cybersecurity competencies of fourth-year BSIT students in the areas of information gathering, footprinting, and vulnerability assessment.

The questionnaire will be developed based on related literature, cybersecurity competency frameworks, and essential skills required in cybersecurity practices. The indicators included in the instrument will focus on students' understanding and ability to perform cybersecurity-related tasks.

The questionnaire will consist of three major sections:

Section I: Information Gathering Competency

This section aims to assess the students' competency in collecting and analyzing information related to computer systems, networks, and digital assets.

The indicators include:

- Understanding the concepts and importance of information gathering;

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

- Identifying sources of information for cybersecurity assessment;
- Applying passive and active information gathering techniques;
- Recognizing publicly available information that may expose security risks;
- Familiarity with information gathering tools used in cybersecurity.

This section determines whether students possess the foundational skills needed in conducting reconnaissance activities.

Section II: Footprinting Competency

This section evaluates the students' ability to perform ethical reconnaissance and gather information about a target environment.

The indicators include:

- Understanding footprinting concepts and processes;
- Gathering information related to domains and networks;
- Identifying publicly available information about systems and organizations;
- Understanding DNS, WHOIS, and other reconnaissance techniques;
- Recognizing possible security risks caused by excessive information exposure.

Footprinting competency is assessed because it represents an essential skill in cybersecurity assessment and penetration testing activities.

Section III: Vulnerability Assessment Competency

This section determines the students' ability to identify, analyze, and evaluate security weaknesses in computer systems and networks.

The indicators include:

- Understanding vulnerability assessment concepts;
- Identifying common system and network vulnerabilities;
- Applying vulnerability scanning techniques;
- Interpreting vulnerability assessment results;
- Recommending appropriate security measures to address identified weaknesses.

This section measures the students' ability to apply cybersecurity knowledge in evaluating possible security risks.

Validation of Research Instrument

To ensure the validity and reliability of the research instrument, the researcher-made questionnaire will undergo expert validation before its administration.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

The instrument will be evaluated by selected experts in the fields of:

- Information Technology;
- Cybersecurity;
- Networking;
- Research methodology.

The validators will assess the questionnaire based on the following criteria:

- Relevance of the indicators to the research objectives;
- Clarity and understanding of each statement;
- Appropriateness of the content for fourth-year BSIT students;
- Completeness and alignment with cybersecurity competencies.

The comments and recommendations provided by the experts will be considered in revising and improving the instrument before the final distribution.

Data Gathering Procedure

The researchers will follow a systematic procedure in gathering the required data for the study. First, the researchers will request approval from the administration of Bohol Northern Star College to conduct the study among fourth-year BSIT students.

Second, coordination will be conducted with the BSIT Program Chairperson and concerned faculty members regarding the schedule and administration of the research instrument.

Third, the purpose and significance of the study will be explained to the respondents. They will be informed that their participation is voluntary and that all gathered information will be treated with confidentiality.

Fourth, the validated questionnaire will be distributed to the fourth-year BSIT students. The researchers will provide instructions on how to answer the instrument properly.

Finally, the collected data will be organized, analyzed, and interpreted using appropriate statistical tools. The findings will serve as the basis for developing the proposed Cybersecurity Training Framework.

Statistical Treatment of Data

The collected data will be analyzed using appropriate statistical tools.

Weighted Mean

The weighted mean will be used to determine the overall competency level of fourth-year BSIT students in information gathering, footprinting, and vulnerability assessment.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

The formula is:

$$WM = \frac{\sum fx}{N}$$

Where:
WM = Weighted M
f = Frequency
x = Assigned sc
N = Total number of responses

The computed weighted mean will determine the students' competency level based on the following interpretation:

Scale	Mean Range	Interpretation
5	4.21 – 5.00	Highly Competent
4	3.41 – 4.20	Competent
3	2.61 – 3.40	Moderately Competent
2	1.81 – 2.60	Slightly Competent
1	1.00 – 1.80	Not Competent

Ranking

Ranking will be used to determine the highest and lowest competency areas among information gathering, footprinting, and vulnerability assessment.

The ranking results will help identify priority areas that require additional training and improvement. These results will serve as the basis for designing the proposed Cybersecurity Training Framework.

Development of the Cybersecurity Training Framework

The primary output of this study will be a proposed Cybersecurity Training Framework for Fourth-Year BSIT Students of Bohol Northern Star College. The framework will be developed based on the identified competency levels and areas requiring improvement.

The proposed framework will include the following components:

1. Training Objectives

The objectives will define the expected cybersecurity knowledge and skills that students should acquire after completing the training.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

2. Training Modules
The framework may include the following modules:

Module 1: Information Gathering and Open-Source Intelligence (OSINT)
- Introduction to information gathering
- Passive and active reconnaissance
- OSINT techniques and tools

Module 2: Footprinting and Reconnaissance
- Domain and network footprinting
- DNS information gathering
- Identifying exposed information

Module 3: Vulnerability Assessment
- Vulnerability concepts
- Vulnerability scanning techniques
- Security risk identification and analysis

Module 4: Practical Cybersecurity Activities
- Hands-on laboratory exercises
- Security assessment activities
- Cybersecurity simulation exercises

3. Assessment Strategies
The training framework will incorporate evaluation activities such as:
- Practical demonstrations;
- Laboratory exercises;
- Skills-based assessments;
- Cybersecurity challenges.

The proposed framework aims to enhance the cybersecurity capabilities of fourth-year BSIT students and provide additional learning opportunities that will prepare them for future IT and cybersecurity-related careers.

RESULTS AND DISCUSSION

This section presents the results and discussion of the assessment conducted among the 21 fourth-year Bachelor of Science in Information Technology (BSIT) students of Bohol Northern Star College regarding their competencies in information gathering, footprinting, and vulnerability assessment**.**

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Result

The study utilized total enumeration sampling, wherein all 21 fourth-year BSIT students enrolled during the conduct of the study were included as respondents. This approach was employed because the target population was limited and accessible, allowing the researchers to obtain a complete assessment of the cybersecurity competencies of the graduating BSIT students.

The data gathered from the respondents were analyzed using weighted mean and ranking to determine their level of competency in the identified cybersecurity areas. The findings served as the basis for developing a proposed Cybersecurity Training Framework intended to further strengthen the cybersecurity skills of BSIT students of Bohol Northern Star College.

Level of Competency in Information Gathering

Table 1: Level of Competency of Fourth-Year BSIT Students in Information Gathering (n=21)

Indicators	Weighted Mean	Interpretation
Understands the purpose and importance of information gathering in cybersecurity	4.38	Highly Competent
Can identify relevant information sources for security assessment	4.29	Highly Competent
Understands passive and active information gathering techniques	4.19	Competent
Can apply basic information gathering methods using appropriate tools	4.24	Highly Competent
Can analyze collected information to identify possible security risks	4.14	Competent
Overall Weighted Mean	**4.25**	**Highly Competent**

Discussion

The results showed that the 21 fourth-year BSIT students obtained an overall weighted mean of **4.25**, interpreted as **Highly Competent**, in information gathering. This indicates that the respondents possess sufficient knowledge and skills in collecting, organizing, and analyzing information needed for cybersecurity assessment activities.

The highest-rated indicator was related to understanding the purpose and importance of information gathering in cybersecurity, with a weighted mean of **4.38**. This implies that students recognize information gathering as an essential foundation in identifying possible security threats and understanding target environments.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

The respondents also demonstrated competency in identifying relevant information sources and applying basic information gathering techniques. This may be attributed to their exposure to different BSIT courses involving networking, system administration, programming, and information security concepts.

However, analyzing collected information obtained a slightly lower rating compared with other indicators. Although still interpreted as competent, this suggests that students may need additional practical exercises focused on interpreting gathered information and transforming it into meaningful security assessments.

Overall Cybersecurity Competency Level

Table 2: Overall Competency Level of Fourth-Year BSIT Students in Cybersecurity Areas (n=21)

Competency Area	Weighted Mean	Rank	Interpretation
Footprinting	4.27	1	Highly Competent
Information Gathering	4.25	2	Highly Competent
Vulnerability Assessment	4.23	3	Highly Competent
Overall Weighted Mean	**4.25**		**Highly Competent**

Discussion

The overall findings revealed that the 21 fourth-year BSIT students of Bohol Northern Star College obtained an overall weighted mean of 4.25, interpreted as Highly Competent in information gathering, footprinting, and vulnerability assessment.

The result indicates that the respondents have developed essential cybersecurity competencies expected from graduating BSIT students. Their high competency level may be associated with their accumulated knowledge and experiences from major IT courses, laboratory activities, and academic projects throughout the BSIT program.

Among the three competency areas, footprinting ranked first with a weighted mean of 4.27, indicating that students have strong understanding of reconnaissance activities and the importance of identifying publicly available information that may affect system security.

Information gathering ranked second with a weighted mean of 4.25, showing that students are capable of collecting and analyzing information required for cybersecurity assessment. Meanwhile, vulnerability assessment ranked third with a weighted mean of 4.23, which still indicates a high level of competency but suggests that additional practical exposure to vulnerability scanning tools and security assessment activities may further improve their skills.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

The results support the need for continuous cybersecurity enhancement activities despite the high competency level of students. A structured training framework can provide additional opportunities for students to strengthen their practical skills and improve their readiness for cybersecurity-related roles in the IT industry.

Basis for the Cybersecurity Training Framework

Although the assessment revealed that fourth-year BSIT students are highly competent in cybersecurity fundamentals, the development of a Cybersecurity Training Framework remains beneficial in sustaining and improving their skills.

The proposed framework will focus on enhancing practical cybersecurity capabilities through:

1. **Advanced Information Gathering and OSINT Techniques**
   - Search engine intelligence
   - Public information analysis
   - Reconnaissance methodologies
2. **Footprinting and Network Reconnaissance**
   - DNS enumeration
   - Domain analysis
   - Network information gathering
3. **Vulnerability Assessment Practices**
   - Vulnerability scanning
   - Risk identification
   - Security recommendation development
4. **Hands-on Cybersecurity Activities**
   - Laboratory exercises
   - Cybersecurity simulations
   - Capture-the-Flag (CTF) activities

The framework will serve as a supplemental training guide for the BSIT program of Bohol Northern Star College to further develop students' cybersecurity competencies and prepare them for professional IT practice.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

CONCLUSION

Based on the findings of the study, it was concluded that the fourth-year Bachelor of Science in Information Technology (BSIT) students of Bohol Northern Star College possess a high level of competency in information gathering, footprinting, and vulnerability assessment**.** The results indicate that the students have acquired sufficient knowledge and skills related to fundamental cybersecurity practices that are essential for future IT professionals.

The assessment revealed that the respondents demonstrated strong competency in information gathering, showing their ability to understand the importance of collecting relevant information, identifying available resources, and applying basic techniques used in cybersecurity assessment. This indicates that students have developed foundational skills necessary for analyzing systems, networks, and digital information.

Furthermore, the respondents showed a high level of competency in footprinting, which suggests that they understand the importance of reconnaissance activities in identifying publicly available information and potential security risks. Their ability to recognize information exposure and analyze target environments reflects their awareness of cybersecurity principles and ethical security practices.

The study also found that students are highly competent in vulnerability assessment, demonstrating their understanding of identifying system weaknesses, analyzing security issues, and recommending possible improvements. This implies that the BSIT program has contributed to developing students' awareness of security risks and the importance of maintaining secure information systems.

Although the overall competency level of the respondents was assessed as highly competent, the findings also indicate the importance of continuous enhancement of practical cybersecurity skills. Areas such as advanced tool utilization, vulnerability analysis, and hands-on security assessment activities may require further development to ensure that students are fully prepared for the evolving demands of the IT industry.

Based on the results, the development of a Cybersecurity Training Framework is considered appropriate and beneficial. The proposed framework can serve as a supplementary guide for strengthening cybersecurity education among BSIT students of Bohol Northern Star College. It may provide structured training activities, practical exercises, and learning opportunities that will further enhance students' capabilities in information gathering, footprinting, and vulnerability assessment.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

The study concludes that the fourth-year BSIT students of Bohol Northern Star College possess the necessary foundational cybersecurity competencies; however, continuous training and practical exposure remain essential to further improve their technical skills and industry readiness.

RECOMMENDATIONS

Based on the findings and conclusions of the study entitled "Assessment of Information Gathering, Footprinting, and Vulnerability Assessment Competencies Among BSIT Students: Basis for a Cybersecurity Training Framework," the following recommendations are proposed:

1. **For the Administration of Bohol Northern Star College**
   The administration may consider supporting the implementation of cybersecurity enhancement programs for BSIT students by providing adequate resources, facilities, and learning opportunities. The institution may allocate resources for cybersecurity laboratories, updated computer equipment, and relevant software tools that will allow students to perform practical activities related to information gathering, footprinting, and vulnerability assessment.
   The administration may also consider establishing partnerships with cybersecurity organizations, industry professionals, and training providers to expose students and faculty members to current cybersecurity practices, trends, and industry requirements.
2. **For the BSIT Program and Faculty Members**
   The BSIT faculty members may integrate more hands-on cybersecurity activities into existing courses related to networking, information assurance, programming, and system administration. Although the study revealed that fourth-year BSIT students possess a high level of competency, continuous practical training is necessary due to the rapidly changing nature of cybersecurity threats.
   Faculty members may utilize cybersecurity laboratories, simulation activities, penetration testing exercises, and ethical hacking scenarios to enhance students' practical skills. Activities such as Open-Source Intelligence (OSINT), network reconnaissance, vulnerability scanning, and security assessment exercises may be incorporated to strengthen students' technical capabilities.
   Furthermore, the proposed Cybersecurity Training Framework may be considered as a supplementary learning guide to support the continuous improvement of cybersecurity education within the BSIT program.
3. **For the Fourth-Year BSIT Students**
   Students are encouraged to continuously enhance their cybersecurity knowledge and skills through self-learning, certifications, seminars, workshops, and practical cybersecurity activities.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Since cybersecurity is a continuously evolving field, students should develop the habit of exploring new security tools, techniques, and industry practices.

Students are also encouraged to participate in cybersecurity competitions, Capture-the-Flag (CTF) activities, internships, and community-based technology programs to gain additional practical experience and improve their confidence in applying cybersecurity concepts.

4. **For Future Implementation of the Cybersecurity Training Framework**

   The proposed Cybersecurity Training Framework may be implemented and evaluated to determine its effectiveness in improving students' cybersecurity competencies. The framework may include structured modules focusing on:

- Information Gathering and Open-Source Intelligence (OSINT);
- Footprinting and Reconnaissance Techniques;
- Vulnerability Assessment and Security Analysis;
- Cybersecurity Tools Application;
- Practical Security Assessment Activities.

The implementation of the framework may be conducted through laboratory sessions, workshops, or specialized cybersecurity training programs to provide students with more opportunities for experiential learning.

5. **For Future Researchers**

   Future researchers may conduct similar studies involving a larger number of respondents from different academic levels, institutions, or programs to obtain broader findings regarding cybersecurity competencies among IT students.

Future studies may also consider additional cybersecurity competency areas such as penetration testing, incident response, digital forensics, network defense, and security management. Researchers may also evaluate the effectiveness of the proposed Cybersecurity Training Framework through pre-test and post-test assessments to determine its impact on students' actual cybersecurity skills.

References

[1]. Hanson, J., Taylor, B., & Kaza, S. (2025). *The use of competency-based statements in assessing student knowledge, skills, and abilities: A study in a network security class*. Information Systems Education Journal, 23(2), 62–81.

[2]. Banoth, R., & Godiishala, A. G. (2026). *Information gathering and vulnerability scanning*. In Cybersecurity Red Teaming. Springer Nature.

[3]. Vykopal, J., Švábenský, V., Lopez II, M. T., & Čeleda, P. (2024). *Cybersecurity study programs: What's in a name?*

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Roseline B. Lorican *et al*, Volume 15, Issue 8, August 2026, pg. 1-21
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

[4]. Calimbo, A. L., Ramos, R. F., Navalta, J. R. D., Rodriguez, P. M., Avena, L. B., & Campo, M. L. (2025). *CyberSAFE: A gamified web platform with analytics to promote cybersecurity literacy among IT students*. International Workshop on Artificial Intelligence and Education.

[5]. Laviña, C. G., & Erise, M. G. (2000). *A proposed competency-based process for the College of Information Technology Education students of TIP Manila*. Philippine E-Journals.

[6]. Mades, M. R., Brao-Yruma, R. M., Fermin, A. F. E., Bautro, E. B., Nieves, J. L., & San Pascual, J. Jr. (2026). *Information assurance and security knowledge as a predictor of cybersecurity protection practices among BSIT students*. International Journal of Education, Research, and Innovation Perspectives.

[7]. Švábenský, V., Vykopal, J., & Čeleda, P. (2019). *What are cybersecurity education papers about? A systematic literature review of SIGCSE and ITiCSE conferences*.

[8]. Azzeh, M., Altamimi, A. M., Albashayreh, M., & Al-Oudat, M. A. (2022). *Adopting the cybersecurity concepts into curriculum: The potential effects on students' cybersecurity knowledge*.

