

**CANSCRIBE**  
COLLEGE |   
**Cybersecurity Technician**

*Detailed Program Curriculum*  
*Program Code CSTI*

## Program Description

---

The program provides a comprehensive pathway for students seeking to build and advance their expertise in the rapidly evolving field of cybersecurity. The program begins with foundational training in IT concepts and system administration through CompTIA A+ Cyber, establishing core competencies in hardware, software, networking, and operating systems. Learners then progress to CompTIA Security+, acquiring the knowledge and practical skills necessary to secure networks, applications, and data, while ensuring system integrity and availability. Advanced coursework in CompTIA Cybersecurity Analyst (CySA+) focuses on threat detection, vulnerability management, incident response, and the application of industry frameworks to maintain operational resilience. Students further develop specialized expertise through Ethical Hacker Pro and CompTIA PenTest+, where they apply ethical hacking techniques, conduct penetration testing, and evaluate security across enterprise, cloud, and IoT environments.

In addition to technical proficiency, the program emphasizes communication, teamwork, and project management, preparing graduates to thrive in collaborative professional environments. Learners also develop career readiness skills, ensuring adaptability and ongoing professional growth. Graduates will be well-positioned to pursue roles such as cybersecurity technician, system analyst, or penetration tester, equipped with the knowledge, certifications, and practical experience to safeguard digital infrastructure in diverse organizations.

## Program Learning Objectives

---

Upon successful completion of the Cybersecurity Technician program, the student will be able to:

- apply foundational information technology, networking, and system administration principles to configure and maintain secure computing environments,
- implement and evaluate cybersecurity controls and risk management strategies to protect data, applications, and networks in compliance with security frameworks and policies,
- detect, investigate, and respond to cybersecurity incidents using monitoring tools, vulnerability assessments, and digital forensics techniques,
- conduct ethical hacking and penetration testing to identify and mitigate system vulnerabilities while adhering to legal, professional, and organizational standards,
- apply personal financial management and budgeting principles to make informed career and financial decisions that support professional and personal sustainability,
- communicate technical findings, risk analyses, and professional recommendations clearly and appropriately to diverse audiences using digital, written, and oral formats,
- use project management tools and methodologies to plan, track, and evaluate cybersecurity projects that align with organizational goals and timelines, and
- demonstrate professional, ethical, and adaptable behavior, showing initiative, collaboration, and a commitment to continuous learning within the cybersecurity field.

## Career Occupation

---

This program is intended to prepare a student for the following occupations:

- Cybersecurity Technician
- Data Analyst
- IT Manager
- eCommerce Analyst

- IT Project Manager
- Penetration Tester
- IT Auditor
- System Analyst

## Admission Requirements

---

Prior to admissions, applicants must have:

- Grade 12 diploma or equivalent.
- 19 years of age or older by the start of your program. If the applicant is under 19 years of age, a parent or guardian must sign on the applicant's behalf.
- A copy of a government-issued piece of photo identification, such as a driver's license, passport, or other, which shows the student's date of birth.
- Distance learning students must have a PC (Mac or Windows-based) with minimum computer requirements and internet access (high speed is recommended) as highlighted under the Computer Requirements section.
- Typing test confirming that applicants meet our minimum typing speed of 40 nwpm (net words per minute).
- Language Proficiency Requirements must be met as outlined below.

## Language Proficiency Requirements

Prior to admission, applicants must meet at least one of the following English language proficiency requirements:

### 1. Education

#### A) Secondary Education

Evidence of three (3) years of full-time secondary education (Grades 8-12), or two (2) years if the grades are 10, 11, or 12, have been successfully completed where English is the principal language of instruction.

OR

#### B) Post-Secondary Education

Evidence of two (2) years of full-time post-secondary education have been successfully completed where English is the principal language of instruction.

**OR**

### 2. Assessment

By achieving a recognized standardized language test/assessment.

- International English Language Testing System (IELTS) Academic: minimum overall score of 5.5
- Test of English as a Foreign Language (TOEFL) IBT: minimum overall score of 46
- Canadian Academic English Language Assessment (CAEL): minimum overall score of 40
- Canadian English Language Proficiency Index Program (CELPPI): Listening 6, Speaking 6, Reading 5, and Writing 5
- Duolingo English Test (DET): minimum overall score of 95
- Pearson Test of English (PTE) Academic: minimum overall score of 43
- Cambridge English Qualifications: B2 First exam (FCE): minimum overall score of 160 or 'C'
- Cambridge Linguaskill: minimum overall B2 level
- LANGUAGECERT Academic: minimum overall B2 level
- The Michigan English Test (MET): minimum overall B2 level
- iTEP Academic: minimum overall score of 3.5
- EIKEN: minimum placement of Grade Pre-1

## Instructors and Educational Assistants

---

All instructors and educational assistants at CanScribe College are experienced professionals who bring a wealth of industry knowledge and instructional expertise to the learning environment. Committed to student success, our team provides ongoing support throughout the program to ensure each learner has the guidance and resources needed to achieve their academic goals.

This program is designed to be delivered in an online format through synchronous and asynchronous learning. Whether instructor-led onsite and distance learning, or self-paced distance learning, students will have access to comprehensive support services, including instructional assistance, student services, and technical support, providing a supportive learning experience for every student.

## Required Textbooks, Reference Materials, and Industry Platforms

---

Students will access their course materials through a Learning Management System (LMS). Students will use both CompTIA's LMS and CanScribe's LMS throughout their program. Students will be provided with direct access to the CompTIA LMS through CanScribe's LMS in each course. Access to the CompTIA LMS is covered in students' program fees.

Enriched Academy is an external platform to which students will have portal access during school and post-graduation. Students will be provided with a link and login information when they begin the Personal Financial Planning course.

## Computer Requirements

---

A computer is required for the entire program. Computer requirements are as follows:

- Access to high-speed internet
  - o Minimum download speed of 15 mbps
  - o Minimum upload speed of 10 mbps
- A minimum of 8 gigabytes of RAM (Random Access Memory)
- For Windows Operating Systems:
  - o Windows 11 or newer
  - o Google Chrome or Firefox
- For Mac:
  - o Mac OS X Big Sur or newer
  - o Google Chrome, Firefox, or Safari

## Method of Evaluation

---

The Cybersecurity Technician program consists of 10 courses that each contribute to the final program grade, as shown below. Each course has its own individual method of evaluation, which may include assignments, quizzes, exams, or projects, depending on the course content and learning objectives. Detailed evaluation criteria is provided below in each course outline. Students have access to a grade book through the LMS. This tool allows students to access their grades throughout their program.

|                                   |        |
|-----------------------------------|--------|
| 1. Online Student Success         | 5%     |
| 2. Personal Financial Planning    | 5%     |
| 3. a+ Cyber                       | 11.25% |
| 4. Security+                      | 11.25% |
| 5. Foundations of Communication   | 11.25% |
| 6. Cybersecurity Analyst (CySA+)  | 11.25% |
| 7. Ethical Hacking                | 11.25% |
| 8. Project Management             | 11.25% |
| 9. Penetration Testing (PenTest+) | 11.25% |
| 10. Career Readiness              | 11.25% |

**TOTAL**

---

100%

## Graduation Requirements

To meet the graduation requirement for the Cybersecurity Technician program, the student must have achieved an overall grade of C (60% or higher) to pass. The following table denotes CanScribe's final grade percentages:

|    |           |             |
|----|-----------|-------------|
| A+ | 95 – 100% | Dean’s List |
| A  | 90 – 94%  | High Honors |
| A- | 85 - 89%  | Honors      |
| B+ | 80 – 84%  | Merit       |
| B  | 75 – 79%  |             |
| B- | 70 – 74%  |             |
| C+ | 65 – 69%  |             |
| C  | 60 – 64%  | Pass        |
| C- | 55 – 59%  | Fail        |
| D  | 50 – 54%  |             |
| F  | Below 50% |             |

## Program Timeline

Upon enrollment, each student is provided with a personalized timeline, including completion dates, to guide and assist with time management throughout the program. Students proceed at their own pace and are required to complete the program in approximately 44 weeks. An example of the basic timeline is as follows:

| Course Code | Course                        | Est Hours to Complete | Est Days to Complete |
|-------------|-------------------------------|-----------------------|----------------------|
| SSES1001    | Student Success Essentials    | 5                     | 2                    |
| BUAA3131    | Personal Financial Planning   | 25                    | 9                    |
| CMIT1031    | a+ Cyber                      | 76                    | 27                   |
| Milestone 1 |                               |                       |                      |
| CMIT1041    | Security+                     | 222                   | 78                   |
| BUAA1001    | Foundations of Communication  | 50                    | 17                   |
| Milestone 2 |                               |                       |                      |
| CMIT2051    | Cybersecurity Analyst (CySA+) | 167                   | 58                   |
| CMIT2061    | Ethical Hacker Pro            | 114                   | 40                   |
| BUAA1081    | Project Management            | 50                    | 17                   |
| Milestone 3 |                               |                       |                      |
| CMIT2071    | PenTest+                      | 124                   | 43                   |
| BUPD1021    | Career Readiness              | 50                    | 17                   |
| Total Hours |                               | 883                   | 309                  |

## Milestones

Milestones are key check-in points that occur three times during the program, each triggered when a student reaches a specific stage of their progression. At each milestone, students are invited to complete a brief survey reflecting on their experience and progress. A member of the instructional team reviews each survey and follows up with the student to offer support, address any questions or concerns, and ensure they are on track to meet program expectations. If a student does not complete the survey, instructors will still reach out to check in. Students are encouraged to reach out to instructors at any time during the program for additional guidance or support.

## Additional Information

---

CanScribe College is committed to the highest standards of academic integrity and honesty. Students are urged to avoid any behavior that could potentially result in suspicions of cheating, plagiarism, misrepresentation of facts, and/or participation in an offense. Academic dishonesty is a serious offense and can result in suspension or dismissal from the program. Please see further details under the **Appropriate Conduct/Dismissal Policy** section in the CanScribe Student Handbook.

### Extensions

Students may be able to extend their program by purchasing extensions if they have not been dismissed or withdrawn from the program. Eligible students can purchase 1-month (\$150.00) and 3-month (\$350.00) extension blocks. Extensions are always retroactive to the student's latest contract (or amended contract) end date. Extensions are not eligible for T2202 tax receipts.

### Referrals

Referral rewards will be paid to the referring party for a student's enrollment if the enrollment meets specific criteria. The referrer must be noted on the student contract before the program start date. Referral rewards will be paid to the referrer once the student has completed 50% of the program.

## Course Surveys

---

Upon completing each course, students are encouraged to fill out a brief course survey. It will ask for your experience with basic directions, activities, materials and resources, visual and audio elements, and instructor assistance for that course. There is room for comments, and all comments are welcome. Constructive feedback is viewed as an excellent opportunity for us to enhance the program.

## Program Outline

---

### Online Learning Success

**Course Code:** SSES1001

**Prerequisites:** There are no prerequisites for this course.

**Learning Objectives:** Upon successful completion of this course, students will be able to describe the key expectations and responsibilities of an online college learner and will navigate key digital tools used in online learning to complete learning tasks effectively and prepare for assessments, while demonstrating academic integrity. They will demonstrate professional and respectful communication using appropriate digital platforms in an online academic setting. Additionally, they will adopt and evaluate strategies to manage stress, stay motivated, and maintain a growth mindset, and will develop a personal plan for ongoing success as independent online learners. Students will apply effective time management and organizational techniques to plan their studies, and they will identify and reflect on their personal learning preferences to implement effective study and note-taking strategies.

**Required Course Materials:** No additional learning materials are required for this course.

**Length:** 5 hours

**Teaching Methods:** Based upon the delivery method selected at enrollment, there are three teaching methods offered:

1. Instructor-led onsite, in-person delivery.
2. Synchronous teaching for distance delivery.
3. Asynchronous teaching for distance delivery.

Additional instructional assistance, student support, and technical support are available during regular college hours via email, phone, or live chat.

**Method of Evaluation:** This course is evaluated based on content completion. Students will receive 100% on the course for completing all requirements outlined within the course. If all requirements are not completed, students will receive a final grade of 0%.

**Completion Requirement:** View all course material, submit required activities, complete the course final exam and course survey. Passing grade for this course is 100%.

### **Course Outline:**

1.0 Welcome to Online Learning

2.0 Technology and Digital Skills

- 3.0 Communication and Support in Online Learning
- 4.0 Time Management and Organization
- 5.0 Learning Strategies for Online Students

- 6.0 Test-Taking Skills and Academic Integrity
- 7.0 Motivation, Wellness, and Growth Mindset
- 8.0 Reflection and Success Plan

## Personal Financial Planning

**Course Code:** BUAA3131

**Prerequisites:** There are no prerequisites for this course.

**Learning Objectives:** In this course, the student will develop their knowledge and personal financial planning skills. This includes assessing the value of money and creating a clear foundation for better financial awareness. Students will identify what credit and credit history are and how they are built and managed. Further, students will analyze student loans before and after graduation, budgeting and managing their payments. Students will be able to explain the stock market and how to apply investing skills. Students will define various savings practices, such as the TFSA (Tax-Free Savings Account) and RRSP (Registered Retirement Savings Plan), and how to set up and handle them successfully. Students will identify real estate investment and the industry of financial advisors. This course will guide the student in mastering their career and protecting their personal brand.

**Required Course Materials:** Students will access their course material through Enriched Academy. Access to Enriched Academy will be granted through the LMS at the start of this course.

**Length:** 25 hours

**Teaching Methods:** Based upon the delivery method selected at enrollment, there are three teaching methods offered:

1. Instructor-led onsite, in-person delivery.
2. Synchronous teaching for distance delivery.
3. Asynchronous teaching for distance delivery.

Additional instructional assistance, student support, and technical support are available during regular college hours via email, phone, or live chat.

**Method of Evaluation:** Students have access to a workbook through the course to practice and test their knowledge. There are course tests for each course throughout the program to evaluate the students' learning.

**Completion Requirement:** View all course material, complete required reading, and attempt chapter quizzes. To pass this course, students must achieve a minimum grade of 60%.

### **Course Outline:**

- |                                               |                                       |
|-----------------------------------------------|---------------------------------------|
| 1.0 Money Myths                               | 8.0 Investment Properties             |
| 2.0 Understanding Credit                      | 9.0 Retirement Planning               |
| 3.0 How to Manage Student Loans               | 10.0 The Industry of Financial Advice |
| 4.0 Where Are You Today?                      | 11.0 Career Mastery                   |
| 5.0 Beginner's Stock Market Investing Systems | 12.0 Leveraging Equity                |
| 6.0 Advanced Stock Market Investing Systems   | 13.0 Private Lending                  |
| 7.0 TFSA vs. RRSP                             |                                       |

## a+ Cyber

**Course Code:** CMIT1031

**Prerequisites:** There are no prerequisites for this course.

**Learning Objectives:** Upon successful completion of this course, the students will be able to understand cybersecurity support roles and how teams collaborate to address threats. They will be able to configure and secure Linux and Windows systems, manage IP addresses and SOHO routers, and ensure safe web browsing. Students will gain insight into enterprise networks, including switches, firewalls, and virtualization. They will learn to apply cybersecurity controls such as intrusion detection, incident response, and vulnerability management, as well as develop Bash scripts to automate tasks. Emphasis will also be placed on protecting data through backups and database management. By the end of the course, students will be prepared to transition into Security+ training and further pursue a career in cybersecurity.

**Required Course Materials:** No additional learning materials are required for this course.

**Length:** 76 hours

**Teaching Methods:** Based upon the delivery method selected at enrollment, there are three teaching methods offered:

1. Instructor-led onsite, in-person delivery.
2. Synchronous teaching for distance delivery.

3. Asynchronous teaching for distance delivery.

Additional instructional assistance, student support, and technical support are available during regular college hours via email, phone, or live chat.

**Method of Evaluation:** Students will complete a Module Assessment at the end of each module throughout the course. Each Module Assessment will be weighted equally.

**Completion Requirement:** View all course material, attempt module assessments, and complete the course survey. To pass this course, students must achieve a minimum grade of 60%.

**Course Outline:**

- |     |                                               |     |                                   |
|-----|-----------------------------------------------|-----|-----------------------------------|
| 1.0 | Cybersecurity Support Roles                   | 6.0 | Cybersecurity Controls            |
| 2.0 | Microsoft Windows Administration Fundamentals | 7.0 | Linux App Server Fundamentals     |
| 3.0 | Secure Network Client Fundamentals            | 8.0 | Automation Scripting Fundamentals |
| 4.0 | Enterprise Campus Network Fundamentals        | 9.0 | Data Management Fundamentals      |
| 5.0 | Enterprise Network Application Fundamentals   |     |                                   |

Security+

**Course Code:** CMIT1041

**Prerequisites:** CMIT1031 A+ Cyber

**Learning Objectives:** Upon successful completion of this course, students will be able to compare a wide range of security controls and understand core cybersecurity principles, including the CIA triad, AAA, zero trust, and deception technologies. They will explain change management processes and apply cryptographic solutions, including encryption, PKI, hashing, and blockchain. Students will identify various threat actors, their motivations, and attack vectors, and assess vulnerabilities across systems and environments. They will analyze malicious activity, apply mitigation techniques, and compare infrastructure models like cloud, on-premises, IoT, and ICS. Emphasis will be placed on securing enterprise infrastructure, protecting data, ensuring resilience and recovery, and managing computing resources. Additionally, students will demonstrate skills in asset and vulnerability management, system monitoring, and configuring enterprise security tools. They will implement identity and access controls, understand automation and incident response processes, and use data sources for investigations. Finally, students will summarize security governance and compliance practices, conduct risk assessments, evaluate third-party risks, and promote security awareness throughout an organization.

**Required Course Materials:** No additional learning materials are required for this course.

**Length:** 222 hours

**Teaching Methods:** Based upon the delivery method selected at enrollment, there are three teaching methods offered:

1. Instructor-led onsite, in-person delivery.
2. Synchronous teaching for distance delivery.
3. Asynchronous teaching for distance delivery.

Additional instructional assistance, student support, and technical support are available during regular college hours via email, phone, or live chat.

**Method of Evaluation:** Students will complete module quizzes and live labs throughout the course. These quizzes and labs will be weighted equally, and the average of these assessments will account for 60% of the course final grade. The student will also complete a cumulative course exam, which will account for 40% of the course final grade.

**Completion Requirement:** View all course material, complete required labs and quizzes, complete course exam, and complete course survey. To pass this course, students must achieve a minimum combined grade of 60%.

**Course Outline:**

- |      |                                               |      |                                                   |
|------|-----------------------------------------------|------|---------------------------------------------------|
| 1.0  | Summarize Fundamental Security Concepts       | 11.0 | Enhance Application Security Capabilities         |
| 2.0  | Compare Threat Types                          | 12.0 | Explain Incident Response and Monitoring Concepts |
| 3.0  | Explain Cryptographic Solutions               | 13.0 | Analyze Indicators of Malicious Activity          |
| 4.0  | Implement Identity and Access Management      | 14.0 | Summarize Security Governance Concepts            |
| 5.0  | Secure Enterprise Network Architecture        | 15.0 | Explain Risk Management Processes                 |
| 6.0  | Secure Cloud Network Architecture             | 16.0 | Summarize Data Protection and Compliance Concepts |
| 7.0  | Explain Resiliency and Site Security Concepts | 17.0 | Final Exam                                        |
| 8.0  | Explain Vulnerability Management              |      |                                                   |
| 9.0  | Evaluate Network Security Capabilities        |      |                                                   |
| 10.0 | Assess Endpoint Security Capabilities         |      |                                                   |

## Foundations of Communication

**Course Code:** BUAA1001

**Prerequisites:** CMIT1041 Security+

**Learning Objectives:** Upon successful completion of this course, students will be able to communicate clearly and professionally in written, verbal, and digital formats. They will demonstrate effective listening, interpersonal, and team communication skills, and adapt their communication styles to different audiences and purposes. Students will apply the principles of proper grammar, formatting, and tone to create documents such as emails, memos, and reports. They will also analyze and interpret communication scenarios, identifying barriers and developing strategies to improve communication outcomes. Emphasis will be placed on respectful, inclusive communication practices that foster professionalism and collaboration.

**Required Course Materials:** No additional learning materials are required for this course.

**Length:** 50 hours

**Teaching Methods:** Based upon the delivery method selected at enrollment, there are three teaching methods offered:

1. Instructor-led onsite, in-person delivery.
2. Synchronous teaching for distance delivery.
3. Asynchronous teaching for distance delivery.

Additional instructional assistance, student support, and technical support are available during regular college hours via email, phone, or live chat.

**Method of Evaluation:** Students will complete a final project (60% of final grade) and complete the course exam (40% of final grade).

**Completion Requirement:** View all course material, submit required activities, complete the course exam, and complete the course survey. To pass this course, students must achieve a minimum combined grade of 60%.

### **Course Outline:**

- |                                               |                                                   |
|-----------------------------------------------|---------------------------------------------------|
| 1.0 Introduction to Communication Foundations | 6.0 Interpersonal & Team Communication            |
| 2.0 Communication Models, Channels & Barriers | 7.0 Digital Communication & Online Presence       |
| 3.0 Professional Writing Basics               | 8.0 Inclusive, Respectful & Ethical Communication |
| 4.0 Email, Memo & Report Writing              | 9.0 Applied Scenarios & Problem Solving           |
| 5.0 Verbal & Non-Verbal Communication         | 10.0 Final Exam                                   |

## Cybersecurity Analyst (CySA+)

**Course Code:** CMIT2051

**Prerequisites:** BUAA1001 Foundations of Communication

**Learning Objectives:** Upon successful completion of this course, the students will be able to explain core concepts of system and network architecture, including log ingestion, OS functions, IAM, encryption, and data protection. Students will identify indicators of malicious activity across networks, hosts, applications, and social engineering threats. Students will detect threats using tools like Wireshark, SIEM, and VirusTotal, apply analysis techniques, and use scripting languages for support. They will evaluate threat intelligence sources, improve processes, and conduct vulnerability scanning and assessment using various methods and tools. They will prioritize vulnerabilities, recommend appropriate mitigation controls, and explain response strategies, including patching and secure development practices. Students will apply frameworks such as MITRE ATT&CK and OWASP, perform incident response activities, and manage the full incident lifecycle. They will also produce clear reports on vulnerabilities and incidents, focusing on communication, analysis, and continuous improvement.

**Required Course Materials:** No additional learning materials are required for this course.

**Length:** 167 hours

**Teaching Methods:** Based upon the delivery method selected at enrollment, there are three teaching methods offered:

1. Instructor-led onsite, in-person delivery.
2. Synchronous teaching for distance delivery.
3. Asynchronous teaching for distance delivery.

Additional instructional assistance, student support, and technical support are available during regular college hours via email, phone, or live chat.

**Method of Evaluation:** Students will complete module quizzes and live labs throughout the course. These quizzes and labs will be weighted equally, and the average of these assessments will account for 60% of the course final grade. The student will also complete a cumulative course exam, which will account for 40% of the course final grade. A minimum grade of 80% is required to pass the course exam.

**Completion Requirement:** View all course material, complete required labs and quizzes, complete course exam, and complete course survey. To pass this course, students must achieve a minimum combined grade of 60%.

**Course Outline:**

- |                                                                    |                                                                              |
|--------------------------------------------------------------------|------------------------------------------------------------------------------|
| 1.0 Understanding Vulnerability Response, Handling, and Management | 8.0 Explaining Incident Response Activities                                  |
| 2.0 Exploring Threat Intelligence and Threat Hunting Concepts      | 9.0 Demonstrating Incident Response Communication                            |
| 3.0 Explain Important System and Network Architecture Concepts     | 10.0 Applying Tools to Identify Malicious Activity                           |
| 4.0 Understanding Process Improvement in Security Operations       | 11.0 Analyzing Potentially Malicious Activity                                |
| 5.0 Implementing Vulnerability Scanning Methods                    | 12.0 Understanding Application Vulnerability Assessment                      |
| 6.0 Performing Vulnerability Analysis                              | 13.0 Exploring Scripting Tools and Analysis Concepts                         |
| 7.0 Communicating Vulnerability Information                        | 14.0 Understanding Application Security and Attack Mitigation Best Practices |
|                                                                    | 15.0 Final Exam                                                              |

**Ethical Hacker Pro**

**Course Code:** CMIT2061

**Prerequisites:** CMIT2051 CySA+

**Learning Objectives:** Upon successful completion of this course, the students will be able to gather information about systems and networks and perform reconnaissance using tools such as Nmap and Wireshark. They will identify open ports, services, and vulnerabilities and conduct network scans to analyze results effectively. Students will learn to exploit vulnerabilities to test defenses, carry out ethical hacking and penetration testing, and assess web application security through SQL injection and cross-site scripting (XSS) tests. They will also evaluate wireless networks for weaknesses and implement secure configurations for access points. Finally, students will document their findings, create comprehensive penetration test reports, and develop actionable recommendations to enhance overall system security.

**Required Course Materials:** No additional learning materials are required for this course.

**Length:** 114 hours

**Teaching Methods:** Based upon the delivery method selected at enrollment, there are three teaching methods offered:

1. Instructor-led onsite, in-person delivery.
2. Synchronous teaching for distance delivery.
3. Asynchronous teaching for distance delivery.

Additional instructional assistance, student support, and technical support are available during regular college hours via email, phone, or live chat.

**Method of Evaluation:** Students will complete interactive labs throughout the course. These labs will be weighted equally and will account for 60% of the course final grade. The student will also complete a cumulative course exam, which will account for 40% of the course final grade. A minimum grade of 80% is required to pass the course exam.

**Completion Requirement:** View all course material, complete required labs, complete course exam, and complete course survey. To pass this course, students must achieve a minimum combined grade of 60%.

**Course Outline:**

- |                                              |                                                         |
|----------------------------------------------|---------------------------------------------------------|
| 1.0 Introduction to Ethical Hacking          | 8.0 System Hacking                                      |
| 2.0 Introduction to Penetration Testing      | 9.0 Malware                                             |
| 3.0 Social Engineering and Physical Security | 10.0 Sniffers, Session Hijacking, and Denial of Service |
| 4.0 Reconnaissance                           | 11.0 IDS, Firewalls, and Honeypots                      |
| 5.0 Scanning                                 | 12.0 Web Servers, Web Applications, and SQL Injections  |
| 6.0 Enumeration                              | 13.0 Wi-Fi, Bluetooth, and Mobile Devices               |
| 7.0 Analyze Vulnerabilities                  | 14.0 Cloud Computing and Internet of Things             |

### Project Management

**Course Code:** BUAA1081

**Prerequisites:** CMIT2061 Ethical Hacker Pro

**Learning Objectives:** Upon successful completion of this course, the students will be able to define key concepts, terminology, and roles within project management frameworks, including scope, time, cost, quality, and stakeholder considerations. They will describe and outline the stages of the project life cycle and explain how these stages interrelate. Learners will apply basic tools and techniques for project planning, scheduling, and documentation using standard templates, while analyzing common project risks and proposing appropriate mitigation or response strategies. The course also emphasizes the importance of effective communication, teamwork, and leadership in project environments. In addition, learners will summarize ethical, legal, and safety considerations relevant to project management practice and discuss how organizational policies, budgets, and quality assurance processes influence overall project success. Students will use digital project management tools to plan, track, and communicate project activities effectively. Finally, students will develop and present a project plan for a chosen case or scenario.

**Required Course Materials:** No additional learning materials are required for this course.

**Length:** 50 hours

**Teaching Methods:** Based upon the delivery method selected at enrollment, there are three teaching methods offered:

1. Instructor-led onsite, in-person delivery.
2. Synchronous teaching for distance delivery.
3. Asynchronous teaching for distance delivery.

Additional instructional assistance, student support, and technical support are available during regular college hours via email, phone, or live chat.

**Method of Evaluation:** Students will complete a final project (60% of final grade) and complete a course exam (40% of final grade).

**Completion Requirement:** View all course material, submit required activities, complete the course exam, and complete the course survey. To pass this course, students must achieve a minimum combined grade of 60%.

**Course Outline:**

- |                                                  |                                                            |
|--------------------------------------------------|------------------------------------------------------------|
| 1.0 Introduction to Project Management Concepts  | 6.0 Ethics, Contracts, Policies, and Professional Practice |
| 2.0 Project Life Cycle and Frameworks            |                                                            |
| 3.0 Project Planning Tools and Techniques        | 7.0 Technology in Project Management                       |
| 4.0 Risk, Safety, and Quality                    | 8.0 Project and Presentation                               |
| 5.0 Communication, Leadership, and Team Dynamics | 9.0 Final Exam                                             |

### Penetration Testing (PenTest+)

**Course Code:** CMIT2071

**Prerequisites:** BUAA1081 Project Management

**Learning Objectives:** Upon successful completion of this course, the students will be able to plan and scope penetration tests by defining rules of engagement, selecting targets, and establishing testing timelines. They will ensure legal and ethical compliance through proper authorization and adherence to relevant regulations. Students will communicate effectively with stakeholders, conduct peer reviews, and articulate risk clearly. They will perform both active and passive reconnaissance using OSINT, network sniffing, and tools like Nmap, Wireshark, and Shodan. Students will apply enumeration techniques and customize scripts in Python, PowerShell, and Bash for reconnaissance. They will carry out vulnerability scans (authenticated/unauthenticated, SAST/DAST), analyze results, and validate findings using tools like Nessus, Nikto, and OpenVAS. The course covers a range of attack methods, including network, authentication, host-based, web application, and cloud-based attacks, as well as emerging threats targeting AI systems. Students will engage in post-exploitation activities such as persistence, lateral movement, and cleanup, and will document attack narratives with remediation recommendations.

**Required Course Materials:** No additional learning materials are required for this course.

**Length:** 124 hours

**Teaching Methods:** Based upon the delivery method selected at enrollment, there are three teaching methods offered:

1. Instructor-led onsite, in-person delivery.
2. Synchronous teaching for distance delivery.
3. Asynchronous teaching for distance delivery.

Additional instructional assistance, student support, and technical support are available during regular college hours via email, phone, or live chat.

**Method of Evaluation:** Students will complete interactive labs and quizzes throughout the course. These labs and quizzes will be weighted equally and will account for 60% of the course final grade. The student will also complete a cumulative course exam, which will account for 40% of the course final grade.

**Completion Requirement:** View all course material, complete required labs, complete the final course exam, and complete the course survey. To pass this course, students must achieve a minimum combined grade of 60%.

**Course Outline:**

- |                                              |                                          |
|----------------------------------------------|------------------------------------------|
| 1.0 Penetration Testing: Before You Begin    | 7.0 Enterprise Attacks                   |
| 2.0 Applying Pre-Engagement Activities       | 8.0 Specialized Attacks                  |
| 3.0 Enumeration and Reconnaissance           | 9.0 Performing Penetration Testing Tasks |
| 4.0 Scanning and Identifying Vulnerabilities | 10.0 Reporting and Recommendations       |
| 5.0 Conducting PenTest Attacks               | 11.0 Final Exam                          |
| 6.0 Web-based Attacks                        |                                          |

Career Readiness

**Course Code:** BUPD1021

**Prerequisites:** CMIT2071 Penetration Testing (PenTest+)

**Learning Objectives:** Upon successful completion of this course, students will be able to build a strong professional foundation for the workplace by identifying their personal strengths and setting clear career goals. They will develop adaptability and a growth mindset to engage in lifelong learning, supporting sustainable career success. Students will gain an understanding of workplace culture, communication styles, and organizational structures, enabling them to navigate professional environments effectively. They will also learn to create and maintain a professional online presence that facilitates networking and career advancement. In addition, students will apply essential job search strategies, including crafting resumes and cover letters, and will prepare for interviews with confidence. The course will also equip students to interpret employment rights and workplace policies, with attention to social media and privacy considerations. Finally, students will demonstrate readiness for remote and hybrid work environments through effective communication, time management, and self-motivation, ensuring they are prepared to thrive in a dynamic and diverse employment landscape.

**Required Course Materials:** No additional learning materials are required for this course.

**Length:** 50 hours

**Teaching Methods:** Based upon the delivery method selected at enrollment, there are three teaching methods offered:

1. Instructor-led onsite, in-person delivery.
2. Synchronous teaching for distance delivery.
3. Asynchronous teaching for distance delivery.

Additional instructional assistance, student support, and technical support are available during regular college hours via email, phone, or live chat.

**Method of Evaluation:** Students will complete a cover letter and resume activity (36% of final grade), participate in a simulated employment interview (24% of final grade), and complete the course final exam (40% of final grade).

**Completion Requirement:** View all course material, submit required activities, attempt the course final exam, and complete the course survey. To pass this course, students must achieve a minimum combined grade of 60%.

**Course Outline:**

- |                                                                   |                                                         |
|-------------------------------------------------------------------|---------------------------------------------------------|
| 1.0 Building Your Professional Foundation and Workplace Readiness | 3.0 Caring for Yourself During Unemployment Transitions |
| 2.0 Lifelong Learning for Career Success                          | 4.0 Understanding Workplace Culture and Communication   |

5.0 Knowing Your Employment Rights and Workplace Policies  
6.0 Leveraging AI and Other Technology  
7.0 Using AI Ethically  
8.0 Preparing for Remote and Hybrid Work Environments  
9.0 Establishing a Professional Online Presence  
10.0 Resumes

11.0 Applications & Cover Letters  
12.0 Job Searching  
13.0 Interviewing  
14.0 Deepening Your Networking and Finding Mentors  
15.0 Building Resilience and Adaptability for Today's Job Market  
16.0 Final Exam



Training for the future you deserve.