# PORTFOLIO ASSESSMENT GUIDE for

# CYB 272 Cybersecurity II

**What is a Portfolio**:

A Portfolio is a formal means of requesting assessment of your prior work/life experience from which you have developed sufficient college-level learning to earn credit for a specific class.

**Purpose of this Guide**:

This document is intended for student self-assessment purposes only. Review it carefully to determine if you are ready to write and submit a Portfolio for the course indicated above. Your self-assessment is not a guarantee that you will be awarded credit for the course. Faculty with expertise in the subject matter will evaluate whether your Portfolio provides sufficient evidence that you have demonstrated appropriate college-level mastery of the course content through experiential learning.

# General Guidelines:

* All work must be word-processed, except for documentation provided.
* Written portions should demonstrate college-level writing skills, including appropriate citations for any quoted or paraphrased material from other sources.
* Use the provided template, located on **page 3** of the guide, to format the portfolio appropriately.
* Your Portfolio will not be returned. Make copies of the contents before you submit. You may include clear copies of documentation and keep the originals.
* Submit your completed Portfolio, along with the approved Course Portfolio Assessment Form, to the Adult Learning Programs Office.

# Determination of Portfolio Assessment Outcome:

You will need to do the following to be awarded credit through Portfolio Assessment for this course:

* Provide all required documentation as listed within the template to support the Learning Outcomes.
* Possibly participate in an interview with the Portfolio evaluator.
* When evaluated, students must demonstrate experience or proficiency in >=70% to earn credit in the course.

|  |
| --- |
| [Course Number]: Portfolio Assessment |
| Skill/Outcome | Score |
|  |  |
| **Provide documentation of successfully passing the CompTIA Security+ certification exam** | 100 |
|  |  |
| In extenuating circumstances competencies can be met through extensive industry experience confirmed by employer |  |
| Total Score | /100 |



CREDIT FOR PRIOR LEARNING PORTFOLIO

[COURSE NUMBER AND TITLE]

[DATE]

BY

[YOUR NAME]

Table of Contents

Contents

[Statement of Academic Honesty 3](#_Toc90467075)

[Course Description 3](#_Toc90467076)

[Learning Outcomes 4](#_Toc90467076)

[Educational Goals 6](#_Toc90467077)

[Chronological Resume 6](#_Toc90467078)

[Learning and Experience Autobiography 7](#_Toc90467079)

[Acquired Learning and Knowledge Narrative 8](#_Toc90467080)

[Bibliography 9](#_Toc90467081)

[Documentation 9](#_Toc90467082)

Statement of Academic Honesty

The material contained in this Portfolio honestly and accurately reflects my life, learning, and work experience. I understand that the penalty for falsifying any information or documentation will result in an award of no credit for the Portfolio with no resubmission allowed and may result in other sanctions as described in the Student Code of Conduct.

Print Name LCSC ID Number

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Date

Course Description

**CYB-272 Cybersecurity II - 4 Credits**

This course examines the tools and techniques used for traffic and intrusion analysis employed in today's cyber environment. This includes processes and procedures used by hackers, along with corresponding countermeasures that may be employed to protect against such attacks. Students will learn the skills necessary to take the CompTIA Security+ exam.

Pre-Req: CYB 271

Learning Outcomes

Upon successful completion of this course, you should be able to demonstrate the following competencies:

1. Use SET
2. Perform Website Reconnaissance
3. Crack a Linux Password Using the John the Ripper Tool
4. Simulate a DoS Attack
5. Use Rainbow Tables
6. Detect Rootkits
7. Create a Remote Access Trojan (RAT)
8. Use NetBus in Windows 10
9. Defend Against a Buffer Overflow Attack
10. Perform Session Hijacking Using Burp Suite
11. Exploit a Website Using SQL Injection
12. Use Ettercap for ARP Spoofing
13. Identify Search Options in Metasploit
14. Use OWASP ZAP
15. Set Up a Honeypot
16. Configure RAID 5
17. Take an Incremental Backup
18. Take a Full Backup
19. Observe an MD5-Generated Hash Value
20. Perform Symmetric Encryption
21. Examine Asymmetric Encryption
22. Hide Text Using Steganography
23. Configure an SSH Server
24. Configure DNSSEC on an Active Directory Integrated Zone
25. Use the ifconfig Command
26. Configure Inbound Rules for a Firewall
27. Use Windows Firewall
28. Configure a Tunnel Group for Clientless SSL VPN
29. Configure Clientless SSL VPNs on ASA
30. Configure Site-to-Site IPsec VPN Topology
31. Perform IDS Configuration with Snort
32. Use Performance Monitor
33. Create a VLAN and Viewing its Assignment to Port Mapping
34. Create a DMZ Zone
35. Set Up a VPN Server with Windows Server 2016
36. Implement Port Security
37. Configure a BPDU Guard on a Switch Port
38. Configure NetFlow and NetFlow Data Export
39. Turn on Airplane Mode of an iPhone
40. Set Up a VPN in Android
41. Perform a MITM Attack
42. Stop Permissions Inheritance
43. Manage NTFS Permissions
44. Create a User Account in the Active Directory
45. Configure IPSec
46. Create a Network Policy for 802.1X
47. Revoke and Export a Certificate
48. Examine PKI Certificates
49. Perform Memory Analysis with Volatility
50. Use Wireshark
51. Manipulate a File in Linux
52. Conduct Vulnerability Scanning Using Nessus
53. Use the Harvester Tool
54. Create Reverse and Bind Shells using Netcat
55. Use the netstat Command
56. Use the hping Program
57. Use pathping and ping Commands
58. Scan Live Systems Using Nmap
59. Use dig and nslookup Commands
60. Trace a Route Using Tracert
61. View the System Logs
62. Use Windows Event Viewer
63. Complete the Chain of Custody
64. Analyze Forensics with Autopsy

Topics Covered:

* Social Engineering Techniques
* Types of Attacks
* Application Attacks
* Network Attacks
* Threat Actors, Vectors, and Intelligence Sources
* Vulnerabilities
* Security Assessments
* Penetration Testing
* Security in an Enterprise Environment
* Virtual and Cloud Computing
* Secure Application Development, Deployment, and Automation
* Authentication and Authorization
* Cybersecurity Resilience
* Security Implications of Embedded and Specialized Systems
* Physical Security Controls
* Cryptographic Concepts
* Secure Protocols
* Host or Application Security Solutions
* Secure Network Designs
* Wireless Security Settings
* Secure Mobile Solutions
* Cybersecurity in the Cloud
* Management Controls
* Public Key Infrastructure
* Mitigation Techniques
* Digital Forensics
* Risk Management

Educational Goals

**Goals, Motivation, and Time Frame**

What are your goals? What are the reasons (professional and personal) you are pursuing your goals? What is a realistic time frame for completing your education?

**Prior Learning to Goals**

How will the prior learning credit you are requesting fit into your future educational and career goals?

Chronological Resume

Include a chronological resume that will support your request for prior learning. List all jobs held, including volunteer work, as they relate to the course that you are trying to receive credit. List duties, skills and expertise used in performing job tasks. When possible, use language similar to that used in the Learning Outcomes for the course.

Examples of Experience:

* Employment, Work Experience
* Workshops, Webinars, Training, Seminars, Professional Development
* Volunteer Activities, Community Service, Committees, Groups
* Military Experience, Occupations, Training
* Licenses, Certificates, Industry Credentials
* Non-credit Courses
* Publications

Learning and Experience Autobiography

The autobiography will serve as an introduction to the evaluator and help them understand the context of your learning for the particular course you are requesting. It is a complete picture of you and your experiences as it relates to the course for which you are creating this portfolio. Relate the relevant experiences to the course in a general explanation (Specifics will be included in the Acquired Learning and Knowledge Narrative). Demonstrate why you have selected this particular course and detail your work and life experiences using your resume as a guide.

This should be two+ pages and summarize the significant learning experiences in your life and describe how your experiences will validate your knowledge of the course content and meet the course outcomes being petitioned for credit.

Acquired Learning and Knowledge Narrative

The narrative is a detailed explanation of how your activities and the resulting competencies were achieved. This is to complement your resume and autobiography. Be sure to link your accomplishments to the course learning outcomes. This will be similar to your autobiography but will detail your chronological work and life experience history while focusing on the things you have already learned through training and experiences, as it relates to your target course.

Note that a key goal of this section is the learning process itself as you reflect on how your experience relates to key concepts within the learning outcomes in the target course. Clearly focus on the learning objectives (what you know and can do) rather than the experience.

For each experience indicated within the Portfolio, the student must:

* Label each heading, Learning Outcome 1, Learning Outcome 2, etc.
* Include the experience; time spent in activity; description of duties and activities.
* Describe the learning and how it relates to the Learning Outcomes for the course.
* Describe how the learning was acquired.
* Provide documentation as evidence of the experience in relation to the course learning outcomes, and as an indication of the level and appropriateness of content.
* Describe how this experience has influenced and impacted other areas of your life.

This will be 2+ pages in length. Make sure it is clear, concise, and free of errors in sentence structure, grammar, and spelling. It needs to demonstrate college-level writing and critical thinking.

Bibliography

**This is not required.** The bibliography will include any reading done on the course subject. If you have studied manuals or used other texts to gain your prior learning, include them here. References should be cited in American Psychological Association (APA) style, but your instructor may suggest another format.

Documentation

Each of your experiences and competencies will require verification (evidence). This evidence can take several forms:

* Completion of training programs, workshops, seminars, etc., may be verified through:
	+ Certificates
	+ Personnel records
* Performance reviews showing competencies
* Job descriptions
* Transcripts
* Samples of work
* A videotape of your speech, theatre work, or music recital
* Licenses
* Honors or Awards
* Samples of your painting, drawing, photography, or ceramics for a studio art course
* Certificates of attendance
* Letters of verification listing proven competencies from instructors or employers
* Products designed or created by you
* Military records

Each piece of documentation for a workshop or training program must be accompanied by a description page of content for each workshop, training program, or seminar and must show how the evidence relates to the course learning outcomes.