



MASTER COURSE OUTLINE

A. CPRO 2115 Offensive Security

B. COURSE DESCRIPTION:

The course combines an ethical hacking methodology with the hands-on application of security tools to better help students secure their systems. Students are introduced to common countermeasures that effectively reduce and/or mitigate attacks. Prerequisites: CPRO 2000 Network Security Fundamentals or Instructor Approval.

(3 Cr – 3 lect, 0 lab)

C. *Core Theme: Critical Thinking

D. RIVERLAND INSTITUTIONAL LEARNING OUTCOMES:

This course addresses the following Riverland Institutional Learning Outcome(s):

- ILO 1: critical thinking (*Core Theme Goal 2*)
- ILO 2: awareness of the larger global community (*Core Theme Goal 7 or 8*)
- ILO 3: ethical, engaged citizenship (*Core Theme Goal 9 or Goal 10*)
- ILO 4: communication and collaboration (*Discipline Goal 1 and by any learning outcome(s) involving communication or collaboration*)

E. MAJOR CONTENT AREAS:

At the completion of this course students will have knowledge and skills in:

- Penetration Testing Professional Certifications
- Hacking Techniques and Technologies
- Physical Security
- Wireless Security
- Web and Database Security
- Reconnaissance/Open Source Intelligence Gathering
- Scanning
- Securing Ports, Services, and Applications
- Enumeration
- Vulnerability Assessment
- Exploitation Methods
- Social Engineering
- Defensive Technologies and Countermeasures
- Incident Response
- Post-Exploitation Assessment and Remediation

F. GOAL TYPES, OBJECTIVES, AND OUTCOMES:

<u>GOAL</u>	<u>OBJECTIVES</u> Students will be able to:	<u>OUTCOMES</u> The student will successfully:
<u>*Critical Thinking</u>	imagine and seek out a variety of possible goals, assumptions, interpretations, or perspectives which can give alternative meanings or solutions to given situations or problems.	1. identify and analyze hacking techniques and technologies, then use this information to develop security policies and strategies to mitigate the identified threats to the information infrastructure.
<u>CS</u>	demonstrate knowledge and expertise in hacking techniques and technologies.	1. profile hackers and cyber criminals, describe the history of hacking, explain the evolution of hacking and why information systems and people are vulnerable to manipulation and exploitation.
<u>CS</u>	demonstrate knowledge and expertise in physical security.	1. define the role of physical security, identify and implement basic equipment and physical security controls.
<u>CS</u>	demonstrate knowledge and expertise in reconnaissance and intelligence gathering.	1. describe the information gathering process, perform information gathering using common techniques and technologies in a controlled laboratory environment.
<u>CS</u>	demonstrate knowledge and expertise in malware, viruses, worms, Trojans, spyware, adware, scareware, and hostgaware.	1. describe common types of malware, threats posed by malware, and techniques to detect, remove, and mitigate malware.
<u>CS</u>	demonstrate knowledge and expertise in incident response / post-exploitation assessment and remediation.	1. describe methods and technologies used to detect and identify security compromises, develop and execute an incident response plan to resolve identified security issues.
<u>CS</u>	demonstrate knowledge and expertise in social engineering.	1. describe methods and techniques used to implement social engineering attacks, develop and implement policies and best practices to mitigate social engineering attacks.
<u>CS</u>	demonstrate business and interpersonal skills.	2. collaborate with classmates to develop security policies and share information security techniques and strategies.

G. SPECIAL INFORMATION:

This course requires Internet access, the submission of electronically prepared documents and the use of a course management software program. Students who have a disability and need accommodations should contact Accessibility Services at the beginning of the semester.

H. COURSE CODING INFORMATION:

Course Code T/Class Maximum 30; Letter Grade

Revision date: 04/01/25

AASC Approval date: 12/13/16; 05/13/25

*These five MnTC Goals have been identified as Riverland Community College Core Themes. Every course in the Riverland Community College curriculum shall meet outcomes from one of these themes.

**These five MnTC Goals have been identified as Riverland Community College Disciplines. Riverland's MnTC courses also shall meet outcomes from a Discipline Area.

NOTE: The Minnesota Transfer Curriculum "10 Goal Areas of Emphasis" are reflected in the five required discipline areas and five core themes noted in the Riverland Community College program of study guide and/or college catalog.

*Riverland Community College Core Themes	MnTC Goal Number
Critical Thinking (CT)	2
Human Diversity (HD)	7A, 7B, 7A/B
Global Perspective (GP)	8
Ethical and Civic Responsibility (EC)	9
People and the Environment (PE)	10

**Riverland Community College Discipline Areas	MnTC Goal Number
Communication (CM)	1
Natural Sciences (NS)	3
Mathematics/Logical Reasoning (MA)	4
History and the Social & Behavioral Sciences (SS)	5
Humanities and Fine Arts (HU)	6