



## COURSE OUTLINE: NASA104 - FUND OF NET SECURITY

Prepared: Sam Laitinen / Dan Kachur

Approved: Corey Meunier, Chair, Technology and Skilled Trades

<b>Course Code: Title</b>	NASA104: FUNDAMENTALS OF NETWORK SECURITY
<b>Program Number: Name</b>	2196: NETWRK ARCH & SEC AN
<b>Department:</b>	COMPUTER STUDIES
<b>Semesters/Terms:</b>	21F
<b>Course Description:</b>	This course provides an in-depth study of network security principles, standards, cryptography, best practices and current threats. Supported by extensive lab work, system vulnerabilities, network attacks will be investigated and solutions implemented using a variety of operating systems and security tools.
<b>Total Credits:</b>	4
<b>Hours/Week:</b>	4
<b>Total Hours:</b>	60
<b>Prerequisites:</b>	There are no pre-requisites for this course.
<b>Corequisites:</b>	There are no co-requisites for this course.
<b>Vocational Learning Outcomes (VLO's) addressed in this course:</b>	<b>2196 - NETWRK ARCH &amp; SEC AN</b>
<b>Please refer to program web page for a complete listing of program outcomes where applicable.</b>	VLO 2 Perform network monitoring, analysis and troubleshooting to determine efficient and secure operations.
	VLO 4 Design multi-site enterprise operating system infrastructures using a security architecture framework.
	VLO 6 Design and implement a virtualization and cloud computing focused infrastructure specifically addressing security risks associated with incorporating virtualization into an organizations infrastructure.
	VLO 7 Deploy servers to host web applications, focusing on securing the server and web from identified security risks.
<b>Essential Employability Skills (EES) addressed in this course:</b>	EES 1 Communicate clearly, concisely and correctly in the written, spoken, and visual form that fulfills the purpose and meets the needs of the audience.
	EES 2 Respond to written, spoken, or visual messages in a manner that ensures effective communication.
	EES 3 Execute mathematical operations accurately.
	EES 4 Apply a systematic approach to solve problems.
	EES 5 Use a variety of thinking skills to anticipate and solve problems.
	EES 6 Locate, select, organize, and document information using appropriate technology and information systems.
	EES 7 Analyze, evaluate, and apply relevant information from a variety of sources.
	EES 8 Show respect for the diverse opinions, values, belief systems, and contributions of others.

In response to public health requirements pertaining to the COVID19 pandemic, course delivery and assessment traditionally delivered in-class, may occur remotely either in whole or in part in the 2021-2022 academic year.



SAULT COLLEGE | 443 NORTHERN AVENUE | SAULT STE. MARIE, ON P6B 4J3, CANADA | 705-759-2554

	<p>EES 9 Interact with others in groups or teams that contribute to effective working relationships and the achievement of goals.</p> <p>EES 10 Manage the use of time and other resources to complete projects.</p> <p>EES 11 Take responsibility for ones own actions, decisions, and consequences.</p>
<b>Course Evaluation:</b>	<p>Passing Grade: 50%, D</p> <p>A minimum program GPA of 2.0 or higher where program specific standards exist is required for graduation.</p>
<b>Other Course Evaluation &amp; Assessment Requirements:</b>	<p>Grade Definition Grade Point Equivalent</p> <p>A+ 90 - 100% 4.00 A 80 - 89% B 70 - 79% 3.00 C 60 - 69% 2.00 D 50 59% 1.00 F (Fail)49% and below 0.00</p> <p>CR (Credit) Credit for diploma requirements has been awarded. S Satisfactory achievement in field /clinical placement or non-graded subject area. U Unsatisfactory achievement in field/clinical placement or non-graded subject area. X A temporary grade limited to situations with extenuating circumstances giving a student additional time to complete the requirements for a course. NR Grade not reported to Registrar's office. W Student has withdrawn from the course without academic penalty.</p> <p>Students are expected to be present to write all tests. If a student is unable to write a test due to illness or a legitimate emergency, that student must contact the professor prior to class and provide reasoning, which is acceptable to the professor. Should the student fail to contact the professor, the student shall receive a grade of zero on the test.</p> <p>Once the test has commenced, the student is considered absent and will not be given the privilege of writing the test.</p> <p>Students involved with academic dishonesty during a test will receive an automatic zero. Please refer to the College Academic Dishonesty Policy for further information.</p> <p>In order to qualify to write a missed test, the student shall have:</p> <ol style="list-style-type: none"> <li>attended at least 80% of the classes.</li> <li>provided the professor an acceptable explanation for his/her absence.</li> <li>been granted permission by the professor.</li> </ol> <p>NOTE: The missed test that has met the criteria above will be an end-of-semester test.</p> <p>Academic success is directly linked to attendance. Missing more than 1/3 of the course hours in a semester may result in an 'F' grade for the course.</p> <p>Labs and Assignments are due on the due-date indicated by the Professor. Notice by the professor will be written on the lab or verbally announced in the class and / or both. No late labs will be accepted beyond the due date. Once labs / assignments have been marked by the professor and returned to the student, no new labs / assignments will be accepted. It is the responsibility of the student who has missed a class to contact the professor immediately to</p>

In response to public health requirements pertaining to the COVID19 pandemic, course delivery and assessment traditionally delivered in-class, may occur remotely either in whole or in part in the 2021-2022 academic year.



SAULT COLLEGE | 443 NORTHERN AVENUE | SAULT STE. MARIE, ON P6B 4J3, CANADA | 705-759-2554

obtain the lab / assignment that is due at a future date. Students are responsible for doing their own work. Labs / assignments that are handed in and are deemed identical in content and personal wording to others may constitute academic dishonesty and result in a zero grade.

The total overall average of test scores combined must be 50% or higher in order to qualify to pass this course. In addition, combined tests, Labs / Assignments total grade must be 50% or higher.

**Books and Required Resources:**

Untangle Network Security by Monem - Bawab  
 Publisher: PackT Publishing  
 Open Source

Guide to Computer Network Security by Kizza  
 Publisher: Springer

Cyber Warfare - Techniques, Tactics and Tools by Andress - Winterfeld  
 Publisher: Syngress Edition: 2nd Edition

**Course Outcomes and Learning Objectives:**

<b>Course Outcome 1</b>	<b>Learning Objectives for Course Outcome 1</b>
Explain the basics of Cyber Security	<ul style="list-style-type: none"> <li>• Examine the dangers of security incidents</li> <li>• Examine the roles of those in the security industry</li> </ul>
<b>Course Outcome 2</b>	<b>Learning Objectives for Course Outcome 2</b>
Explore the Security Functions of the Windows Operating System	<ul style="list-style-type: none"> <li>• Explore Windows Security Patches and Updates</li> <li>• Identify Windows Architecture vulnerabilities</li> <li>• Perform hands-on steps to secure a Windows Operating System</li> <li>• Explain the automated update process for Windows Security</li> </ul>
<b>Course Outcome 3</b>	<b>Learning Objectives for Course Outcome 3</b>
Explore the Linux Operating System	<ul style="list-style-type: none"> <li>• Install and secure a Linux OS</li> <li>• Perform hands-on administration and security of Linux</li> <li>• Work with the Linux Shell</li> <li>• Explore Linux security strengths and weaknesses</li> </ul>
<b>Course Outcome 4</b>	<b>Learning Objectives for Course Outcome 4</b>
Explore Network Protocols and Services	<ul style="list-style-type: none"> <li>• Explore Network and Communication protocols</li> <li>• Explore IPV4 and IPV6 addressing</li> <li>• Explore the Address Resolution Protocol</li> <li>• Examine Network Services</li> <li>• Apply hands-on TCP / UDP implementation</li> </ul>
<b>Course Outcome 5</b>	<b>Learning Objectives for Course Outcome 5</b>
Plan Network Infrastructure	<ul style="list-style-type: none"> <li>• Examine then diagram components and resources required in a LAN / WAN and Enterprise Network</li> <li>• Install a Windows Server as part of the Network Infrastructure process</li> </ul>

In response to public health requirements pertaining to the COVID19 pandemic, course delivery and assessment traditionally delivered in-class, may occur remotely either in whole or in part in the 2021-2022 academic year.



	<ul style="list-style-type: none"> <li>Secure then Administer the Windows Server including Firewall</li> <li>Test Windows Security including setting up Alert Monitoring</li> <li>Review Network Security Policies and the the important role they play in helping keep the workplace safe from attacks</li> </ul>
<b>Course Outcome 6</b>	<b>Learning Objectives for Course Outcome 6</b>
Explore the Principles of Network Security	<ul style="list-style-type: none"> <li>Define the Principles of Security</li> <li>Overview of Attackers and tools that they use</li> <li>Explore Common Threats and Attacks</li> <li>Define and research attack types including Phishing, Ransomware and Social Engineering</li> <li>Explore the roles of Routers, Switches, Firewalls and VPNs</li> </ul>
<b>Course Outcome 7</b>	<b>Learning Objectives for Course Outcome 7</b>
Explore Network Attacks	<ul style="list-style-type: none"> <li>Examine Attackers and the tools they use</li> <li>Examine the attacks used on the foundation of the network</li> <li>Examine exposed services like email, databases, and http</li> <li>Research and explain current trends in Cyberattacks</li> <li>Research the potential future of Network attacks</li> </ul>
<b>Course Outcome 8</b>	<b>Learning Objectives for Course Outcome 8</b>
Explore ways to Protect the Network	<ul style="list-style-type: none"> <li>Examine defenses and security policies</li> <li>Explore Access Control</li> <li>Explore Threat Intelligence Services</li> <li>Explain CyberWarfare</li> </ul>
<b>Course Outcome 9</b>	<b>Learning Objectives for Course Outcome 9</b>
Explore Cryptography and PGP and its relation to Network Security	<ul style="list-style-type: none"> <li>Explain at the introductory level Cryptography and Encryption</li> <li>Explain Public and Private Key Infrastructure</li> </ul>
<b>Course Outcome 10</b>	<b>Learning Objectives for Course Outcome 10</b>
Explore Endpoint Security and Analysis	<ul style="list-style-type: none"> <li>Explore Malware Protection</li> <li>Explore Host based Intrusion Protection</li> <li>Explore an Endpoint Vulnerability Assessment</li> </ul>
<b>Course Outcome 11</b>	<b>Learning Objectives for Course Outcome 11</b>
Explore Security Monitoring	<ul style="list-style-type: none"> <li>Explore Monitoring Security Protocols</li> <li>Explore Log Files including end device and network logs</li> </ul>
<b>Course Outcome 12</b>	<b>Learning Objectives for Course Outcome 12</b>
Explore Intrusion Data Analysis	<ul style="list-style-type: none"> <li>Examine evaluating alerts</li> <li>Explore working with network security data</li> <li>Define and Explore Digital Forensics</li> </ul>
<b>Course Outcome 13</b>	<b>Learning Objectives for Course Outcome 13</b>
Explore Incident Response	<ul style="list-style-type: none"> <li>Examine Incident Response Models</li> </ul>

In response to public health requirements pertaining to the COVID19 pandemic, course delivery and assessment traditionally delivered in-class, may occur remotely either in whole or in part in the 2021-2022 academic year.



**Evaluation Process and Grading System:**

Evaluation Type	Evaluation Weight
Labs and Assignments	40%
Tests and Quizzes	60%

**Date:** July 30, 2021

**Addendum:** Please refer to the course outline addendum on the Learning Management System for further information.

In response to public health requirements pertaining to the COVID19 pandemic, course delivery and assessment traditionally delivered in-class, may occur remotely either in whole or in part in the 2021-2022 academic year.