COURSE OUTLINE: NASA203 - SECURING THE EDGE

Prepared: Christopher Barnett
Approved: Corey Meunier, Chair, Technology and Skilled Trades

Course Code: Title	NASA203: SECURING THE EDGE & SECURITY ANALYTICS
Program Number: Name	2196: NETWRK ARCH & SEC AN
Department:	COMPUTER STUDIES
Semesters/Terms:	19W
Course Description:	This course will study theoretical and practical skills required to monitor and secure an organisation. Edge and internal security principles will be studied in order to protect an organisation from both external and internal threats. The course will explore the principles of Network Security Monitoring along with its implementation and configuration. It delivers theoretical and technical knowledge, insight, and hands-on training needed to prepare a network against and monitor a network for intrusion.
Total Credits:	5
Hours/Week:	4
Total Hours:	60
Prerequisites:	There are no pre-requisites for this course.
Corequisites:	There are no co-requisites for this course.
Essential Employability Skills (EES) addressed in this course:	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 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 9 Interact with others in groups or teams that contribute to effective working relationships and the achievement of goals. EES 10 Manage the use of time and other resources to complete projects. EES 11 Take responsibility for ones own actions, decisions, and consequences.
Course Evaluation:	Passing Grade: 50%, D
Other Course Evaluation & Assessment Requirements:	Grade Definition Grade Point Equivalent A+ 90 - 100% 4.00 A 80 - 89% 4.00 B 70 - 79% 3.00 C 60 - 69% 2.00 D 50 - 59% 1.00 F(Fail) below 50% 0.00

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.

OTHER EVALUATION CONSIDERATIONS

1. In order to pass this course the student must obtain an overall test/quiz average of 50% or better, as well as, an overall assignment average of 50% or better. A student who is not present to write a particular test/quiz, and does not notify the professor beforehand of their intended absence, may be subject to a zero grade on that test/quiz.

2. There will be no supplemental or make-up quizzes/tests in this course unless there are extenuating circumstances.

3. Assignments must be submitted by the due date according to the specifications of the professor. Late assignments will normally be given a mark of zero. Late assignments will only be marked at the discretion of the professor in cases where there were extenuating circumstances.

4. Any assignment/projects submissions, deemed to be copied, will result in a zero grade being assigned to all students involved in that particular incident.

5. It is the responsibility of the student to ask the professor to clarify any assignment requirements.

6. The professor reserves the right to modify the assessment process to meet any changing needs of the class.

Attendance:

Sault College is committed to student success. There is a direct correlation between academic performance and class attendance, therefore, for the benefit of all its constituents, all students are encouraged to attend all of their scheduled learning and evaluation sessions. This implies arriving on time and remaining for the duration of the scheduled session. It is the departmental policy that once the classroom door has been closed, the learning process has begun. Late arrivers may not be granted admission to the room.

Absences due to medical or other unavoidable circumstances should be discussed with the professor, otherwise a penalty may be assessed. The penalty depends on course hours and will be applied as follows:
Course Hours Deduction
5 hrs/week (75 hrs) 1.0% /hr
4 hrs/week (60 hrs) 1.5% /hr
3 hrs/week (45 hrs) 2.0% /hr
2 hrs/week (30 hrs) 3.0% /hr

Final penalties will be reviewed and assessed at the discretion of the professor.

Books and Required

The Practice of Network Security Monitoring by Richard Bejtlich

Resources:

Publisher: No Starch Press Edition: 4th
ISBN: 9781593275099
9781593275341

Course Outcomes and Learning Objectives:

Course Outcome 1	**Learning Objectives for Course Outcome 1**
Introduction to Network Security Monitoring	• Understand the goal of Network Security Monitoring • Understand the concepts of Network Security Monitoring • Understand the importance of time • Know the seven data types
Course Outcome 2	**Learning Objectives for Course Outcome 2**
Enterprise Security Life Cycle	• Understand the four phases of the ESLC • Understand the sub-phases of the Detection and Response phases • Know how to apply the ESLC
Course Outcome 3	**Learning Objectives for Course Outcome 3**
Operations & Building a Team	• Understand the Operational Trap • Learn how Computer Incident Response Teams are built • Learn about the different components of a CIRT • Learn about a Defensible Network Architecture
Course Outcome 4	**Learning Objectives for Course Outcome 4**
Cybersecurity Threats	• Review the attack vectors • Learn about the CIA Triad • Learn about the Destruction Triad • Understand the objectives of malware attacks • Understand the delivery mechanisms for malware attacks • Understand general protection mechanisms that fight malware attacks • Learn about a variety of kinds of malware attacks and specific prevention measures that fight those attacks
Course Outcome 5	**Learning Objectives for Course Outcome 5**
Social Engineering	• Understand what Social Engineering is • Understand the motivations of a social engineer • Discover how social engineers gather information • Understand the psychological principles behind social engineering • Know what social engineers seek to exploit • Understand how to combat social engineering
Course Outcome 6	**Learning Objectives for Course Outcome 6**
Threat Intelligence	• Understand what Threat Intelligence is • Understand the six phases of the Intelligence Cycle • Understand how Threat Intelligence relates to Security Operations • Understand the benefits of Threat Intelligence • Understand the Threat Intelligence frameworks.
Course Outcome 7	**Learning Objectives for Course Outcome 7**
Physical Security	• Understand the planning that goes into secure facility design • Identify key assets that require protection

	• Understand the three kinds of controls • Learn how to protect the four kinds of key asset • Learn the functional order of security control • Learn about the two classifications of physical threat
Course Outcome 8	**Learning Objectives for Course Outcome 8**
Collecting Network Traffic	• Learn about collecting network traffic via a NSM deployment case • Understand where collection mechanisms must be placed • Understand network data flow • Understand the concept of Network Address Translation • Understand the concept of IP Address Assignment • Understand the concept of Network Port Address Translation • Understand the methods of network traffic collection
Course Outcome 9	**Learning Objectives for Course Outcome 9**
Deploy Security Onion Network Security Monitoring suite	• Learn about capacity requirements • Understand the platform management principles • Learn about the two different deployment modes • Deploy a Security Onion VM
Course Outcome 10	**Learning Objectives for Course Outcome 10**
Command Line Packet Analysis	• Learn about the Data Presentation, Delivery, and Collection layers • Learn TCPDUMP in an interactive exercise • Learn about Dumpcap and Tshark • Learn about Argus RA
Course Outcome 11	**Learning Objectives for Course Outcome 11**
Graphical Packet Analysis	• Configure and learn about WireShark in an interactive exercise • Learn about and explore NetworkMiner • Participate in a professor-led interactive hunting exercise
Course Outcome 12	**Learning Objectives for Course Outcome 12**
Intrusion Detection Systems and Intrusion Prevention Systems	• Understand what an IDS/IPS is, where it is deployed, and what they can do • Understand how an IDS/IPS functions • Learn about the four kinds of IDS/IPS • Learn about Snort • Understand the difference between a signature, vulnerability, and exploit • Understand the limitations of IDS
Course Outcome 13	**Learning Objectives for Course Outcome 13**
NSM Consoles	• Recap the 7 data types • Learn about Sguil in an interactive professor-led demonstration • Explore Squert in an interactive professor-led demonstration
Course Outcome 14	**Learning Objectives for Course Outcome 14**
NSM Challenges	• Learn how proxies make NSM more difficult • Learn how IP checksums make NSM more difficult

	• Learn how encryption makes NSM more difficult
Course Outcome 15	**Learning Objectives for Course Outcome 15**
Snort Rule Writing	• Learn the components of a snort rule • Learn how to write snort rules
Course Outcome 16	**Learning Objectives for Course Outcome 16**
Lab Work	• Using case studies on topics such as malware infections and brute force attacks students will learn to: • Use tools like WireShark, NetworkMiner, Sguil, and Squert to review PCAP files • Identify indicators of compromise • Identify compromised assets • Attribute compromised assets to users • Write an incident report detailing findings • Write Snort rules to help identify indicators of compromise
Course Outcome 17	**Learning Objectives for Course Outcome 17**
Security Awareness Presentations (Group Assignment)	• Give an educational presentation on a cybersecurity topic focused on enhancing non-technical users understanding • Create an interactive exercise for the presentation • Create campaign materials for the cybersecurity topic and presentation • Create a plan for the delivery and implementation of the educational presentation and materials
Course Outcome 18	**Learning Objectives for Course Outcome 18**
Designing a Secure Data Centre (Individual Assignment)	• Design a secure data center focused on answering the following questions: • What do we want to protect? • What are we protecting against? • What are our vulnerabilities? • What are consequences of loss? • What level of protection is necessary? • What controls are appropriate?

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Class Participation	5%
Group Assignment	30%
In-Class Quizzes	5%
Individual Assignment	15%
Labs	18%
Tests	27%

Date: September 19, 2019

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