Washtenaw Community College Comprehensive Report

CNT 290 Network Forensics
Effective Term: Fall 2020

Course Cover

Division: Business and Computer Technologies
Department: Computer Science & Information Technology
Discipline: Computer Networking Technology
Course Number: 290
Org Number: 13400
Full Course Title: Network Forensics
Transcript Title: Network Forensics
Is Consultation with other department(s) required: No
Publish in the Following: College Catalog , Time Schedule , Web Page
Reason for Submission: Course Change
Change Information:
Course description
Pre-requisite, co-requisite, or enrollment restrictions
Outcomes/Assessment
Objectives/Evaluation
Rationale: Change in networking program that will now include this course, CNT 290, as a component.
Proposed Start Semester: Fall 2020
Course Description: In this course, students will be introduced to various tools and concepts associated with network forensics, including protocol and services monitoring, event detection and analysis. Network topologies include enterprise, LAN, WAN and wireless configurations. Hands-on configuration, monitoring and troubleshooting of various network services and after-event analysis of network intrusions is performed.

Course Credit Hours

Variable hours: No
Credits: 4
Lecture Hours: Instructor: 60 **Student:** 60
Lab: Instructor: 0 **Student:** 0
Clinical: Instructor: 0 **Student:** 0

Total Contact Hours: Instructor: 60 **Student:** 60
Repeatable for Credit: NO
Grading Methods: Letter Grades
Audit
Are lectures, labs, or clinicals offered as separate sections?: NO (same sections)

College-Level Reading and Writing

College-level Reading & Writing

College-Level Math

Requisites

Prerequisite
CNT 216 minimum grade "C"

or

Prerequisite

CSS 210 minimum grade "C"

General Education

General Education Area 7 - Computer and Information Literacy

Assoc in Arts - Comp Lit
Assoc in Applied Sci - Comp Lit
Assoc in Science - Comp Lit

Request Course Transfer

Proposed For:

Student Learning Outcomes

1. Build and configure LAN, WAN and Enterprise network environments for traffic pattern analysis.
   Assessment 1
   Assessment Tool: Departmentally-developed written exam
   Assessment Date: Winter 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Answer key
   Standard of success to be used for this assessment: 75% of students will score 75% or higher on the exam.
   Who will score and analyze the data: Departmental faculty
   Assessment 2
   Assessment Tool: A final hands-on project
   Assessment Date: Winter 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: 75% of the students will score 75% or higher on the project.
   Who will score and analyze the data: Departmental faculty

2. Monitor and analyze a network and perform after-event analysis of a network attack and determine if it was successful, where it originated, and the consequences to the target system or device.
   Assessment 1
   Assessment Tool: Departmentally-developed written exam
   Assessment Date: Winter 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Answer key
   Standard of success to be used for this assessment: 75% of students will score 75% or higher on the exam.
   Who will score and analyze the data: Departmental faculty
   Assessment 2
   Assessment Tool: A final hands-on project
   Assessment Date: Winter 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections

Number students to be assessed: All students
How the assessment will be scored: Departmentally-developed rubric
Standard of success to be used for this assessment: 75% of the students will score 75% or higher on the project.
Who will score and analyze the data: Departmental faculty

Course Objectives

1. Use packet analyzer, network maintenance and analysis tools to demonstrate how to baseline network performance and determine the most efficient configuration for a given topology.
2. Recognize and monitor network events such as an attack.
3. Perform after-event analysis of a network attack using open source tools such as Autopsy, monitoring scripts and examination of event logs.
4. Use open source network monitoring tools to determine the source or origination of a network attack.
5. Create incident responses to detected events in a practice network.
6. Identify an attack in progress.
7. Identify layer three devices in a network
8. Create a network attack graph based on vulnerability analysis and performance monitoring.

New Resources for Course

Course Textbooks/Resources

Textbooks
Manuals
Periodicals
Software

Equipment/Facilities

Level III classroom
Data projector/computer
Other: Computer networking classroom and lab

Reviewer	Action	Date
Faculty Preparer:		
James Lewis	*Faculty Preparer*	*Jan 13, 2020*
Department Chair/Area Director:		
Cyndi Millns	*Recommend Approval*	*Feb 04, 2020*
Dean:		
Eva Samulski	*Recommend Approval*	*Feb 25, 2020*
Curriculum Committee Chair:		
Lisa Veasey	*Recommend Approval*	*Apr 08, 2020*
Assessment Committee Chair:		
Shawn Deron	*Recommend Approval*	*Apr 23, 2020*
Vice President for Instruction:		
Kimberly Hurns	*Approve*	*Apr 24, 2020*

Washtenaw Community College Comprehensive Report

CNT 290 Network Forensics
Effective Term: Fall 2016

Course Cover

Division: Business and Computer Technologies
Department: Computer Instruction
Discipline: Computer Networking Technology
Course Number: 290
Org Number: 13400
Full Course Title: Network Forensics
Transcript Title: Network Forensics
Is Consultation with other department(s) required: No
Publish in the Following: College Catalog , Time Schedule , Web Page
Reason for Submission: Course Change
Change Information:
Consultation with all departments affected by this course is required.
Course title
Course description
Pre-requisite, co-requisite, or enrollment restrictions
Outcomes/Assessment
Objectives/Evaluation
Rationale: Name more accurately reflects course object and content. The word "Troubleshooting" in the course name seems to detract from the primary objective of the course, network forensics.
Proposed Start Semester: Fall 2016
Course Description: In this course, students will be introduced to various tools and concepts associated with network forensics to include monitoring, detection, analysis and mitigation. Network topologies include enterprise, LAN, WAN, VoIP and wireless configurations. Hands-on configuration, monitoring and troubleshooting of various network services and after-event analysis of network intrusions is performed. The title of this course was previously Network Troubleshooting and Forensics.

Course Credit Hours

Variable hours: No
Credits: 4
Lecture Hours: Instructor: 60 **Student:** 60
Lab: Instructor: 0 **Student:** 0
Clinical: Instructor: 0 **Student:** 0

Total Contact Hours: Instructor: 60 **Student:** 60
Repeatable for Credit: NO
Grading Methods: Letter Grades
Audit
Are lectures, labs, or clinicals offered as separate sections?: NO (same sections)

College-Level Reading and Writing

College-level Reading & Writing

College-Level Math

Requisites

Prerequisite
CNT 236 minimum grade "C"
or equivalent experience.
or
Prerequisite
CNT 224 minimum grade "C"
or experience in configuring Microsoft and Linux systems.
or

General Education

General Education Area 7 - Computer and Information Literacy
Assoc in Arts - Comp Lit
Assoc in Applied Sci - Comp Lit
Assoc in Science - Comp Lit

Request Course Transfer

Proposed For:

Student Learning Outcomes

1. Build and configure complex network environments and services with monitoring capabilities to include LAN, WAN, enterprise, remote, VoIP and wireless configurations.
   Assessment 1
   Assessment Tool: Departmentally-developed written exam
   Assessment Date: Winter 2017
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Answer Key
   Standard of success to be used for this assessment: 75% of students will score 75% or higher on the exam.
   Who will score and analyze the data: Departmental faculty
   Assessment 2
   Assessment Tool: A final hands-on assignment
   Assessment Date: Winter 2016
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All classes during winter term
   Number students to be assessed: All
   How the assessment will be scored: Departmentally-developed rubric.
   Standard of success to be used for this assessment: 75% of the students will score 75% or higher on the project.
   Who will score and analyze the data: Departmental faculty

2. Monitor and analyze a network and perform after-event analysis of a network attack and determine if it was successful, where it originated, and the consequences to the target system or device.
   Assessment 1
   Assessment Tool: A final hands-on assignment
   Assessment Date: Winter 2016
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All classes during winter term
   Number students to be assessed: All
   How the assessment will be scored: Departmentally-developed rubric.
   Standard of success to be used for this assessment: 75% of the students will score 75% or higher on the project.

Who will score and analyze the data: Departmental faculty

Assessment 2

Assessment Tool: Departmentally-developed written exam
Assessment Date: Winter 2017
Assessment Cycle: Every Three Years
Course section(s)/other population: All sections
Number students to be assessed: All students
How the assessment will be scored: Answer Key
Standard of success to be used for this assessment: 75% of students will score 75% or higher on the exam.
Who will score and analyze the data: Departmental faculty

Course Objectives

1. Use packet analyzer, network maintenance and analysis tools to demonstrate how to baseline network performance and determine the most efficient configuration for a given topology.
2. Demonstrate effective analysis, troubleshooting skills, and techniques to restore a malfunctioning or mis-configured network to full functional status.
3. Successfully troubleshoot instructor inserted faults and misconfigurations in a variety of switched, routed, VoIP, wireless and server based configurations.
4. Recognize and monitor network events such as an attack.
5. Perform after-event analysis of a network attack using open source tools such as wireshark, monitoring scripts and event logs and determine the consequences to the target system or device.
6. Use open source network monitoring tools such as Wireshark to determine the source or origination of a network attack.
7. Troubleshoot network devices and services and recommend techniques to restore service.

New Resources for Course

Course Textbooks/Resources

Textbooks
Manuals
Periodicals
Software

Equipment/Facilities

Level III classroom
Other: Computer networking classroom and lab

Reviewer	Action	Date
Faculty Preparer:		
James Lewis	*Faculty Preparer*	*Nov 23, 2015*
Department Chair/Area Director:		
John Trame	*Recommend Approval*	*Dec 16, 2015*
Dean:		
Kimberly Hurns	*Recommend Approval*	*Dec 30, 2015*
Curriculum Committee Chair:		
Kelley Gottschang	*Recommend Approval*	*Jan 21, 2016*
Assessment Committee Chair:		
Michelle Garey	*Recommend Approval*	*Jan 27, 2016*
Vice President for Instruction:		
Michael Nealon	*Approve*	*Feb 01, 2016*