Washtenaw Community College Comprehensive Report

CNT 290 Network Forensics
Effective Term: Winter 2024

Course Cover

College: Business and Computer Technologies
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: Three Year Review / Assessment Report
Change Information:
Consultation with all departments affected by this course is required.
Course description
Pre-requisite, co-requisite, or enrollment restrictions
Outcomes/Assessment
Objectives/Evaluation
Rationale: Update existing course description to reflect recent industry tools.
Proposed Start Semester: Winter 2024
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 the analysis of network packet capture files. Network topologies examined include enterprise, local area network (LAN), wide-area network (WAN) and wireless configurations, and the use of forensics tools for end-point analysis. Students will perform configuration, monitoring and troubleshooting of various network services and after-event analysis of network intrusions.

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 a LAN, and analyze traffic packet capture files from that network.
   Assessment 1
   Assessment Tool: Outcome-related practical in-class assignment
   Assessment Date: Fall 2025
   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: Student achievement checklist
   Standard of success to be used for this assessment: 70% of the students will score 75% or higher on the checklist.
   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: Outcome-related practical in-class assignment
   Assessment Date: Fall 2025
   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: Student achievement checklist
   Standard of success to be used for this assessment: 70% of the students will score 75% or higher on the checklist.
   Who will score and analyze the data: Departmental faculty

3. Analyze captured network traffic files from LAN, WAN and enterprise network environments using network forensic analysis tools.
   Assessment 1
   Assessment Tool: Outcome-related practical final exam questions
   Assessment Date: Fall 2025
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All
   Number students to be assessed: All
   How the assessment will be scored: Answer key
   Standard of success to be used for this assessment: 70% of students will score 75% or higher on the outcome-related questions.

Who will score and analyze the data: Departmental faculty

Course Objectives

1. Use packet analyzer, network maintenance and analysis tools to determine the most efficient configuration for a given topology.
2. Demonstrate how to baseline network performance to determine the most efficient configuration for a given topology.
3. Recognize and monitor network events such as an attack.
4. Perform after-event analysis of a network attack using open source tools such as Autopsy, monitoring scripts and examining event logs.
5. Use open source network monitoring tools to determine the source or origination of a network attack.
6. Create incident responses to detected events in a practice network.
7. Identify an attack in progress.
8. Identify layer three devices in a network
9. Create a network attack graph based on vulnerability analysis and performance monitoring.
10. Identify specific source and destination addresses from a captured .pcap traffic file.
11. Analyze and describe the portion of a captured .pcap traffic file that contains a malicious payload.
12. Demonstrate how to use appropriate protocol analysis and network forensic analysis tools (NFATs) to analyze a captured .pcap traffic file.

New Resources for Course

Course Textbooks/Resources

Textbooks

CDTS. *Network Forensics*, 4th ed. CDTS, 2023

Manuals

Periodicals

Software

Equipment/Facilities

Level III classroom

Computer workstations/lab

Data projector/computer

Other: Computer networking classroom and lab, preferably Cisco lab.

Reviewer	Action	Date
Faculty Preparer:		
James Lewis	*Faculty Preparer*	*Apr 27, 2023*
Department Chair/Area Director:		
Scott Shaper	*Recommend Approval*	*May 05, 2023*
Dean:		
Eva Samulski	*Recommend Approval*	*May 12, 2023*
Curriculum Committee Chair:		
Randy Van Wagnen	*Recommend Approval*	*Nov 14, 2023*
Assessment Committee Chair:		
Jessica Hale	*Recommend Approval*	*Nov 15, 2023*
Vice President for Instruction:		
Brandon Tucker	*Approve*	*Nov 17, 2023*

Washtenaw Community College Comprehensive Report

CNT 290 Network Forensics
Effective Term: Winter 2021

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: Three Year Review / Assessment Report
Change Information:
Consultation with all departments affected by this course is required.
Course description
Pre-requisite, co-requisite, or enrollment restrictions
Outcomes/Assessment
Rationale: This course has never been offered but has been revised to be included in the Cisco networking academy program as a capstone course.
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, and the use of forensics tools for end-point analysis. Students will perform configuration, monitoring and troubleshooting of various network services and after-event analysis of network intrusions.

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: Outcome-related questions on the 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: Outcome-related 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: Outcome-related questions on the 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: Outcome-related 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

3. Perform image analysis of a suspected compromised system, and identify the method of entry and the level of intrusion into the system.

Assessment 1

Assessment Tool: Outcome-related 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

Assessment 2

Assessment Tool: Outcome-related questions on the 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

Course Objectives

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

New Resources for Course

Course Textbooks/Resources

Textbooks

CDTS. *Introduction to Network Forensics*, 3rd ed. CDTS, 2020

Manuals
Periodicals
Software

Equipment/Facilities

Level III classroom
Computer workstations/lab
Data projector/computer
Other: Computer networking classroom and lab, preferably Cisco lab.

Reviewer	Action	Date
Faculty Preparer:		
James Lewis	*Faculty Preparer*	*Jul 28, 2020*
Department Chair/Area Director:		
Cyndi Millns	*Recommend Approval*	*Jul 29, 2020*
Dean:		
Eva Samulski	*Recommend Approval*	*Jul 30, 2020*
Curriculum Committee Chair:		
Lisa Veasey	*Recommend Approval*	*Sep 16, 2020*
Assessment Committee Chair:		
Shawn Deron	*Recommend Approval*	*Sep 21, 2020*
Vice President for Instruction:		
Kimberly Hurns	*Approve*	*Sep 21, 2020*