Miami Dade College

Course Description

CIS4388 | Advanced Computer Forensics | 4.00 credits

This upper division course is a continuation of Computer Forensics. The course examines forensics techniques necessary to investigate and analyze network traffic. The course covers packet capture and analysis, log file analysis, and flow analysis. Other topics include mobile forensics, cloud forensics, malware forensics, database forensics, and investigating email crimes and web attacks. Prerequisite: CIS4366.

Course Competencies:

Competency 1: The student will be able to collect and analyze log files by:

1. Using log files as evidence
2. Evaluating log file accuracy and authenticity
3. Explaining the importance of audit logs
4. Describing Syslog
5. Configuring Windows logging
6. Describing NTP
7. Describing Linux process accounting

Competency 2: The student will be able to capture and analyze packets by:

1. Describing the physical and data link layers of the OSI model
2. Describing the network and transport layers of the OSI model
3. Comparing types of network attacks
4. Performing evidence gathering via sniffing
5. Using tools to investigate network traffic, including wireless traffic
6. Documenting the evidence gathered on a network

Competency 3: The student will be able to demonstrate an understanding of router forensics by:

1. Describing router architecture
2. Explaining the use of Routing Information Protocol (RIP)
3. Listing the different types of router attacks
4. Differentiating router forensics from traditional forensics
5. Listing the steps for investigating router attacks
6. Conducting an incident response
7. Reading router logs
8. Listing various router auditing tools

Competency 4: The student will be able to demonstrate an understanding of Network Intrusion Detection and Prevention Systems (NIDS/NIPS) by:

1. Describing NIDS/NIPS
2. Analyzing NIDS logs
3. Gathering evidence from an IDS

Competency 5: The student will be able to investigate DoS attacks by:

1. Describing DoS attacks
2. Recognizing the indications of a DoS/DDoS attack
3. Listing the different types of DoS attacks
4. Explaining DDoS attacks
5. Examining the working of a DDoS attack

6. Classifying DDoS attacks
7. Detecting DoS attacks using Cisco NetFlow
8. Investigating DoS attacks
9. Discussing the challenges in investigating DoS attacks

Competency 6: The student will be able to investigate email crimes by:

1. Understanding Email Systems, Email Clients, and Email Servers, along with their characteristics
2. Understanding the importance of electronic records management
3. Listing the email crimes and discussing the crimes committed via chat room
4. Describing the components of an email message
5. Listing Common Headers and X-Headers
6. Reviewing the steps to investigate email crimes and violations
7. Describing email forensics tools
8. Discussing U.S. law against email crime: CAN- SPAM Act and its characteristics

Course Competency 7: The student will be able to investigate web attacks by:

1. Interpreting the steps to investigate web attacks
2. Performing web attacks investigation on Windows-based servers
3. Illustrating IIS web server architecture and performing IIS logs investigation
4. Illustrating Apache web server architecture and performing Apache logs investigation
5. Investigating various attacks on web applications

Course Competency 8: The student will be able to demonstrate an understanding of database forensics by:

1. Performing MSSQL forensics. 2. Determining the database evidence repositories and collecting the evidence files
2. Examining evidence files using SQL Server Management Studio and ApexSQL DBA
3. Performing MySQL forensics
4. Understanding the architecture of MySQL and determining the structure of the data directory
5. Listing MySQL utilities for performing forensic analysis
6. Using database forensics tools

Learning Outcomes:

- Solve problems using critical and creative thinking and scientific reasoning
- Use computer and emerging technologies effectively