Cyber Forensics

Exam Information

Exam number
830

Items
30

Points
35

Prerequisites
Digital Literacy

Recommended course length
One semester

National Career Cluster
Information Technology

Performance standards
Included (Optional)

Certificate available
Yes

Description

Cyber Forensics is a course that introduces students to the principles and techniques of computer hacking forensic investigation. Students will learn how to detect, analyze, and document hacking attacks, as well as how to collect and preserve evidence for legal and ethical purposes. Students will also learn how to conduct audits and implement security measures to prevent future attacks. This course will help students develop critical thinking, problem-solving, and communication skills in the context of cybercrime and cybersecurity.

Exam Blueprint

Standard	Percentage of exam
1. Forensic Basics	17%
2. Network Forensics	20%
3. Anti Forensic Techniques	27%
4. Collecting Forensic Evidence	27%
5. Incident Response	10%

Standard 1

Forensic Basics

Objective 1 Understand how to analyze forensic images

1. Apply basic forensic analysis using NIST accepted forensic techniques.
2. Outcomes include:
3. Understand how to use a forensic tool to analyze an image.
4. Identifying actors, authenticity verification (integrity), violation of company policy.
5. Being able to compare side by side analysis of reference image and current image - spotting differences.
6. Ensure following a defined procedure and documenting.

Standard 1 Performance Evaluation included below (Optional)

Test Name

Performance assessments may be completed and evaluated at any time during the course. The following performance skills are to be used in connection with the associated standards and exam. To pass the performance standard the student must attain a performance standard average of 8 or higher on the rating scale. Students may be encouraged to repeat the objectives until they average 8 or higher.

Student's Name: ____

Class: ____

Objective 2 Outline the process for creating a forensically sound image

1. Understand that when a device is found leave it in the same state to preserve the integrity of the data.
2. Isolate the image and create a hash to ensure data integrity.
3. Write blocking to prevent modifying or writing over the data.

Objective 3 Understand Metadata

1. Understand what is metadata and why it is important including: metadata found in email, images, webfiles, files, GPS.
2. Analyze metadata to identify anomalies and outliers to find an incident.
3. Alter metadata to find and hide a secret message.

Standard 2

Network Forensics

Objective 1 Network Basics

1. Understand network protocols including UDP, TCP/IP model, ICMP.
2. Understand the difference between connection and connectionless transmission.
3. Understand 6 most common ports used including: FTP/21, SSH/22, SMTP/25, DNS/53, HTTP/80,

HTTPS/443.

4. Understand the purpose and use of port forwarding.
5. Understand the purpose behind subnet masks and be able to read slash notation. 10.10.10.0/8.
6. Understand how to set up and configure an Intrusion Detection System (IDS) on a network.

Objective 2 Understand how to analyze network data

1. Understand the purpose and use of packet capture software.
2. Apply the principles of packet captures to a message between two computers.
3. Analyze the packets captured to find a hidden message.
4. Identify the ports, protocol, source and destination IP's of a network capture.

Standard 3

Anti Forensic Techniques

Objective 1 Understand Steganography

1. Understand the principles behind steganography and why a threat actor would use it.
2. Apply principles of steganography to hide information inside a text and image file.
3. Apply principles of steganography to find information inside a text and image file.

Objective 2 Understand Trail Obfuscation techniques

1. Understand the principles behind trail obfuscation techniques and why a threat actor would use them including - altering or deleting logs, spoofing, timestamp alteration, data sanitization and disk destruction.
2. Apply the principles of trail obfuscation to hide information using data sanitization (as a minimum).
3. Apply the principles of trail obfuscation to find altered information from an altered log and timestamp alteration (as a minimum).
4. Apply one of the above techniques to a different Operating System.

Standard 4

Collecting Forensic Evidence.

Objective 1 Determine and report logon/logoff times for a specific use

1. Outcomes -
2. Students should be able to find a user breaking the company's AUP assigned time

Objective 2 Understand how to use hashes

1. Understand the basics of hash algorithms and their uses.
2. Outcomes -
3. Students know how to create a hash output for a file.
4. Students compare hash values to verify file integrity.

Objective 3 Summarize the proper handling of evidence

1. Understand the purpose of evidence logs.
2. Understand how to implement a chain of evidence policy.

3. Understand the purpose and value of a chain of custody.
4. Discriminate between a live acquisition and static acquisition.
5. Document the incident by taking photos of the scene before removing evidence.

Objective 4 Determine the important content of event logs in forensics.

1. Understand the purpose of event logs.
2. Outcomes -
3. Students will be able to read event logs and find suspicious activity.

Standard 5

Incident Response

Objective 1 Incident Response Team

1. Understand the purpose of an incident response team.
2. Identify the members of an incident response team including: team leader, team communicator, team members, share and stakeholders.
3. Identify the process of how a general user will report an incident to the team.

Objective 2 Identify the emergency contact list for incident response

1. Identify who should be on the list, including position, responsibilities.
2. Identify who needs to be contacted and availability.
3. Create a process for keeping the list updated regularly

Objective 3 Create an incident report process

1. How to insure the integrity of the documents
2. What is the standard information needed for each incident
3. How are the reports maintained and backed up
4. Understand the parts of the incident report- Summary, Timeline of events, description of events, analysis of root cause and impact.
5. Communicate the results of an investigation to an internal team.

Objective 4 Create a post incident response process

1. Configuration changes - firewall rules and device management setup, etc.
2. Update loss prevention policies.
3. Update certificates.
4. Update incident response processes as needed.

Performance standards rating scale

0	Limited skills	2	→	4	Moderate skills	6	→	8	High skills	10

Standard 1 – Forensic Basics

Score:

- Understand how to analyze forensic images

Standard 2 – Network Forensics

- Network Basics
- Understand how to analyze network data

Standard 3 – Anti Forensic Techniques

- Understand Steganography
- Understand Trail Obfuscation techniques

Standard 4 – Collecting Forensic Evidence

- Determine and report logon/logoff times for a specific use
- Understand how to use hashes
- Summarize the proper handling of evidence
- Determine the important content of event logs in forensics.

Standard 5 – Incident Response

- Incident Response Team
- Identify the emergency contact list for incident response
- Create an incident report process
- Create a post incident response process

Score: (move to the right)

Performance standard average score:

Evaluator Name: ____

Evaluator Title: ____

Evaluator Signature: ____

Date: ____