FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

Course outline

Module 1: Introduction to Digital Forensics

Module 1: Introduction to Digital Forensics is an introductory module for the FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics course. It provides an overview of the digital forensics process, including the fundamentals of digital evidence, the importance of chain of custody, and the use of digital forensics tools. It also covers the basics of digital forensics investigations, such as data acquisition, analysis, and reporting.

Lessons

- Overview of Digital Forensics
- Digital Forensics Processes and Methodologies
- Digital Evidence Collection and Preservation
- Digital Evidence Analysis and Reporting
- Digital Forensics Tools and Techniques
- Network Forensics
- Mobile Device Forensics
- Cloud Forensics
- Malware Forensics
- File System Forensics
- Memory Forensics
- Database Forensics
- Steganography and Cryptography
- Legal and Ethical Considerations in Digital Forensics

After completing this module, students will be able to:

- Understand the fundamentals of digital forensics and its role in incident response.
- Identify and analyze digital artifacts associated with malicious activity.
- Utilize digital forensics tools to investigate and analyze digital evidence.
- Develop a comprehensive incident response plan to respond to digital forensic incidents.

Module 2: Network Forensics

Module 2 of the FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics course covers the fundamentals of network forensics. It provides an overview of the tools and techniques used to

investigate network-based incidents, including packet capture and analysis, log analysis, and malware analysis. It also covers the use of open source and commercial tools to analyze network traffic and identify malicious activity.

Lessons

- Network Traffic Analysis
- Network Protocol Analysis
- Network Intrusion Detection
- Network Packet Capture and Analysis
- Network Log Analysis
- Network Forensics Tools
- Network Forensics Investigations
- Network Forensics Reporting
- Network Forensics Best Practices
- Network Forensics Case Studies

After completing this module, students will be able to:

- Understand the fundamentals of network forensics and its role in incident response.
- Utilize network forensics tools to capture, analyze, and report on network traffic.
- Identify malicious network activity and develop strategies to mitigate it.
- Develop an understanding of the legal implications of network forensics.

Module 3: Memory Forensics

Module 3 of the FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics course covers Memory Forensics. This module provides an in-depth look at the techniques and tools used to analyze volatile memory for evidence of malicious activity. Students will learn how to identify and analyze malicious artifacts in memory, as well as how to use memory forensics to detect and respond to advanced threats.

Lessons

- Introduction to Memory Forensics
- Memory Acquisition and Analysis
- Memory Forensics Tools
- Investigating Malware with Memory Forensics
- Investigating Rootkits with Memory Forensics
- Investigating Web Browser Activity with Memory Forensics
- Investigating Network Activity with Memory Forensics
- Investigating Windows Logon Activity with Memory Forensics
- Investigating Windows Registry Activity with Memory Forensics
- Investigating Windows File System Activity with Memory Forensics
- Investigating Windows Process Activity with Memory Forensics
- Investigating Windows Services with Memory Forensics
- Investigating Windows Security with Memory Forensics
- Investigating Linux Memory Forensics

- Investigating Mac Memory Forensics

After completing this module, students will be able to:

- Understand the fundamentals of memory forensics and its role in incident response and digital forensics.
- Utilize memory forensics tools to analyze and interpret memory dumps.
- Identify malicious artifacts in memory dumps and use them to identify malicious activity.
- Develop strategies for responding to incidents involving memory forensics.

Module 4: Malware Analysis

Module 4 of the FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics course covers the fundamentals of malware analysis. Students will learn how to identify malicious code, analyze the behavior of malware, and develop strategies for responding to and mitigating malware threats. The module also covers the use of various tools and techniques for malware analysis, such as static and dynamic analysis, memory forensics, and sandboxing.

Lessons

- Introduction to Malware Analysis
- Reverse Engineering Malware
- Malware Analysis Tools and Techniques
- Malware Obfuscation and Anti-Analysis Techniques
- Malware Network Analysis
- Malware Memory Analysis
- Malware Forensics
- Malware Detection and Prevention
- Malware Incident Response
- Malware Hunting and Investigation

After completing this module, students will be able to:

- Identify and analyze malicious code and malware
- Utilize reverse engineering techniques to analyze malware
- Develop strategies to detect and respond to malware incidents
- Utilize memory forensics to detect and analyze malicious activity

Module 5: Incident Response Process

Module 5 of the FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics course covers the incident response process. It provides an overview of the incident response process, including the steps to take when responding to an incident, the roles and responsibilities of the incident response team, and the tools and techniques used to investigate and contain the incident. It also covers the importance of documenting the incident response process and the need for post-incident analysis.

Lessons

- Establishing an Incident Response Team
- Developing an Incident Response Plan
- Identifying and Collecting Evidence
- Analyzing Evidence
- Containing and Remediating the Incident
- Reporting and Documenting the Incident
- Post-Incident Review and Improvement
- Legal Considerations for Incident Response
- Incident Response in the Cloud
- Automating Incident Response Processes

After completing this module, students will be able to:

- Understand the fundamentals of incident response and the incident response process.
- Develop an incident response plan and the necessary procedures to respond to a security incident.
- Utilize digital forensics and threat hunting techniques to identify, contain, and remediate security incidents.
- Analyze and interpret evidence from various sources to determine the root cause of a security incident.

Module 6: Advanced Incident Response Techniques

Module 6 of the FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics course covers advanced incident response techniques. It provides an in-depth look at the various tools and techniques used to identify, contain, and remediate malicious activity. Topics include memory forensics, network forensics, malware analysis, and more. Students will gain a comprehensive understanding of the incident response process and how to effectively respond to security incidents.

Lessons

- Advanced Network Forensics
- Advanced Memory Forensics
- Advanced Malware Analysis
- Advanced Log Analysis
- Advanced File System Forensics
- Advanced Mobile Forensics
- Advanced Cloud Forensics
- Advanced Network Packet Analysis
- Advanced Network Intrusion Detection
- Advanced Host-Based Intrusion Detection
- Advanced Incident Response Methodologies
- Advanced Incident Response Automation
- Advanced Threat Hunting Techniques
- Advanced Digital Forensics Investigations
- Advanced Incident Response Reporting

After completing this module, students will be able to:

- Utilize advanced incident response techniques to identify, contain, and eradicate malicious activity.
- Analyze and interpret system and network logs to identify malicious activity.
- Develop and implement threat hunting strategies to detect and respond to advanced persistent threats.
- Utilize digital forensics techniques to investigate and analyze digital evidence.

Module 7: Threat Hunting

Module 7 of the FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics course focuses on the process of threat hunting. It covers the fundamentals of threat hunting, including the use of threat intelligence, data analysis, and investigative techniques to identify malicious activity. It also covers the use of various tools and techniques to detect and respond to threats.

Lessons

- Introduction to Threat Hunting
- Identifying Indicators of Compromise
- Analyzing Network Traffic for Malicious Activity
- Analyzing Host Logs for Malicious Activity
- Analyzing Memory for Malicious Activity
- Analyzing Malware for Indicators of Compromise
- Analyzing the Attacker’s Tactics, Techniques, and Procedures
- Developing and Implementing a Threat Hunting Plan
- Automating Threat Hunting
- Advanced Threat Hunting Techniques
- Incident Response and Remediation
- Reporting and Documentation

After completing this module, students will be able to:

- Identify and analyze malicious activity on a network.
- Utilize threat hunting techniques to detect and respond to advanced persistent threats.
- Develop and implement a threat hunting program.
- Utilize digital forensics tools to investigate and analyze malicious activity.

Module 8: Advanced Threat Hunting Techniques

Module 8 of the FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics course covers advanced threat hunting techniques. It provides an in-depth look at the various methods and tools used to detect and investigate malicious activity on a network. Topics include advanced hunting techniques, threat intelligence, and the use of open source intelligence. The module also covers the use of advanced analytics and machine learning to detect and respond to threats.

Lessons

- Analyzing Network Traffic for Indicators of Compromise
- Exploring Malware Behavior and Techniques
- Investigating Advanced Persistent Threats
- Utilizing Machine Learning for Threat Hunting
- Leveraging Open Source Intelligence for Threat Hunting
- Developing Custom YARA Rules for Malware Detection
- Utilizing Endpoint Detection and Response Tools
- Investigating Memory Forensics for Malware Detection
- Analyzing Logs for Indicators of Compromise
- Investigating Cloud-Based Infrastructure for Threat Hunting

After completing this module, students will be able to:

- Identify and analyze malicious activity in a network environment.
- Utilize advanced threat hunting techniques to detect and respond to threats.
- Develop and implement strategies to mitigate threats.
- Utilize digital forensics tools to investigate and analyze malicious activity.

Module 9: Advanced Digital Forensics

Module 9 of the FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics course covers advanced digital forensics topics such as memory forensics, malware analysis, and network forensics. Students will learn how to use various tools and techniques to analyze digital evidence and uncover malicious activity. The module also covers topics such as data carving, timeline analysis, and the use of open source intelligence.

Lessons

- Advanced Digital Forensics Techniques
- Investigating Network Intrusions
- Investigating Malware
- Investigating Mobile Devices
- Investigating Cloud Computing
- Investigating Social Media
- Investigating Encrypted Data
- Investigating Web Applications
- Investigating Internet of Things (IoT)
- Investigating Big Data
- Investigating Artificial Intelligence (AI)
- Investigating Blockchain
- Investigating Cryptocurrency
- Investigating Insider Threats
- Investigating Insider Abuse
- Investigating Insider Fraud
- Investigating Insider Misuse
- Investigating Insider Data Leaks
- Investigating Insider Data Theft
- Investigating Insider Data Manipulation

After completing this module, students will be able to:

- Understand the principles of digital forensics and how to apply them to incident response and threat hunting.
- Utilize advanced digital forensics techniques to identify and analyze malicious activity.
- Develop and implement a comprehensive digital forensics strategy for an organization.
- Identify and analyze evidence from various sources, including memory, network traffic, and disk images.

Module 10: Data Analysis and Visualization

Module 10 of the FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics course covers the fundamentals of data analysis and visualization. Students will learn how to use various tools and techniques to analyze and visualize data from digital forensic investigations. They will also learn how to create meaningful visualizations to help identify patterns and trends in the data.

Lessons

- Exploring Data Analysis and Visualization Tools
- Analyzing Network Traffic with Visualization
- Visualizing Malware Analysis Results
- Visualizing Host-Based Forensics
- Visualizing Log Analysis
- Visualizing Memory Forensics
- Visualizing Threat Hunting Results
- Visualizing Incident Response Results
- Exploring Data Visualization Techniques
- Creating Custom Visualizations with Python

After completing this module, students will be able to:

- Understand the fundamentals of data analysis and visualization techniques.
- Utilize data analysis and visualization tools to identify patterns and trends in digital forensic data.
- Develop strategies for analyzing and visualizing digital forensic data.
- Interpret and communicate the results of data analysis and visualization to stakeholders.

Module 11: Legal and Ethical Considerations

Module 11 of the FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics course covers the legal and ethical considerations of digital forensics. It provides an overview of the legal and ethical issues that arise when conducting digital forensics investigations, including the use of evidence in court, the handling of confidential information, and the ethical implications of digital forensics. It also covers the legal and ethical considerations of threat hunting and incident response.

Lessons

- Understanding the Legal and Ethical Implications of Digital Forensics
- Investigating Cybercrime in a Legal and Ethically Responsible Manner
- Analyzing the Legal and Ethical Implications of Data Collection and Analysis
- Understanding the Legal and Ethical Implications of Cybersecurity
- Investigating Cybercrime in a Manner that Respects Privacy Rights
- Analyzing the Legal and Ethical Implications of Digital Evidence
- Understanding the Legal and Ethical Implications of Cybersecurity Investigations
- Investigating Cybercrime in a Manner that Respects Human Rights
- Analyzing the Legal and Ethical Implications of Cybersecurity Policies
- Understanding the Legal and Ethical Implications of Cybersecurity Regulations

After completing this module, students will be able to:

- Understand the legal implications of digital forensics investigations and the ethical considerations of conducting such investigations.
- Identify the legal requirements for collecting, preserving, and analyzing digital evidence.
- Recognize the importance of adhering to the chain of custody and other legal requirements when conducting digital forensics investigations.
- Develop an understanding of the ethical considerations of conducting digital forensics investigations and the potential consequences of not following ethical guidelines.

Module 12: Reporting and Documentation

Module 12 of the FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics course covers the fundamentals of reporting and documentation. It provides an overview of the different types of reports and documents that are used in incident response and digital forensics, as well as best practices for creating and maintaining them. It also covers the importance of evidence preservation and chain of custody.

Lessons

- Understanding the Role of Documentation in Incident Response
- Developing an Incident Response Plan
- Writing an Incident Report
- Documenting Digital Evidence
- Creating a Chain of Custody
- Documenting Digital Forensics Investigations
- Documenting Threat Hunting Activities
- Writing a Post-Incident Report
- Developing a Digital Forensics Report
- Understanding the Role of Legal Considerations in Reporting and Documentation

After completing this module, students will be able to:

- Understand the importance of reporting and documentation in digital forensics and incident response.
- Develop comprehensive reports that accurately document the incident response process.

- Utilize various tools and techniques to create detailed reports and documentation.
- Identify and document evidence and artifacts related to digital forensics investigations.