THROUGHSEC

Digital Forensics Course Syllabus

Course Overview:

This is an introductory yet in-depth course on the major aspects of digital forensics, within a Windows environment. This course will cover the skills required for an investigator to analyse digital evidence across several forensic disciplines. Hands-on training in natural situations through practical labs and case studies will equip the pupil to tackle different searching tasks.

Module 1: Introduction to Digital Forensics

This is an overview module that will give students the basic concepts and principles of digital forensics before taking a deeper look into specialty forensic field areas. This course provides an overview of the role of digital forensics in Cybersecurity.

- Definition and Scope: Understanding digital forensics and its importance.
- Key Principles: The chain of custody, evidence handling, and legal considerations.
- Types of Digital Forensics: Disk, memory, email, network, and more.
- Forensic Tools Overview: Popular tools and their use cases (e.g., FTK, Autopsy).

Module 2: Setting Up the Environment

This module guides students through configuring a specialized forensic environment, focusing on tools and techniques needed for a complete digital forensic workspace. Using environments like FLARE VM and other virtualized platforms, students will set up and configure their tools to streamline and secure forensic analysis

- Forensic Workstation Requirements: Hardware and software needs.
- Installing and Configuring Forensic Tools: Step-by-step setup of forensic tools.
- Isolated Environment Setup: Using virtual machines or isolated networks.
- Understanding File Systems: NTFS, FAT32, and other structures.

Module 3: Email Forensics: Investigating Authentication Failures and Malicious Indicators

- Email Basics: Understanding headers, metadata, and protocols (SMTP, IMAP, POP).
- Investigating Authentication Failures: Analyzing login attempts, phishing, and social engineering attacks.
- Malicious Indicators: Identifying malicious attachments, links, and spoofing.

Module 4: Evidence Collection: Disk and Memory Forensics in Windows Systems

- Disk Imaging Basics: Importance of bit-by-bit imaging and tools (e.g., dd, FTK Imager).
- Memory Dump Collection: Using tools like Volatility, DumpIt, and RAM capture.
- Understanding Artifacts: Registry analysis, event logs, and application artifacts.
- Maintaining Integrity: Hashing evidence and preventing contamination.

Module 5: Windows Disk Image Forensics: Evidence Collection and Analysis

- Analyzing Disk Images: Techniques for searching files, metadata, and hidden partitions.
- Recovering Deleted Data: Identifying and recovering deleted files and folders.
- Registry Forensics: Investigating user activities and installed software.
- File Carving: Extracting files from raw data without metadata.

Module 6: Windows Memory Forensics: Evidence Collection and Analysis

- Understanding Memory Structures: Processes, threads, and DLLs.
- Volatility Framework: Extracting and analyzing memory dumps.
- Analyzing Malware: Detecting suspicious processes and injected code.
- Incident Analysis: Tracing back actions to determine the timeline of events.

Module 7: Incident Response: Investigating and Mitigating Security Breaches

- Incident Handling Process: Preparation, detection, containment, eradication, recovery, and lessons learned.
- Root Cause Analysis: Identifying the cause and scope of the breach.
- Log Analysis: Parsing Windows Event Logs and other log sources for anomalies.
- Reporting and Documentation: Writing effective forensic and incident reports.

Module 7: Network Forensics: Investigating and Analyzing Network-Based Security Incidents

- Network Traffic Basics: Understanding protocols (TCP, UDP, HTTP, DNS, etc.).
- Packet Capture and Analysis: Using tools like Wireshark and Tcpdump.
- Intrusion Detection: Leveraging IDS/IPS logs and network monitoring tools.
- Investigating Security Incidents: Tracing malicious activities, such as DDoS, MITM, or exfiltration attempts.

The **Digital Forensics & Incident Response Course** is designed for individuals seeking to develop defensive cybersecurity skills. Here are some key groups who would benefit from this course:

1. **Aspiring Cybersecurity Professionals**: Those new to the field of cybersecurity who want to specialize in defensive security roles such as SOC Analyst, Incident Responder, or Security Engineer.
2. **IT Professionals**: Individuals already working in IT roles like system administrators, network engineers, or IT support, looking to shift to a cybersecurity-focused role with an emphasis on defending systems and networks.
3. **Students in Cybersecurity**: College students pursuing a degree in cybersecurity, IT, or related fields who want to gain practical, hands-on experience in blue team operations.
4. **Incident Responders and SOC Analysts**: Those aiming to specialize in responding to security incidents, analyzing system logs, detecting anomalies, and maintaining the security of IT infrastructures.
5. **Network and System Security Engineers**: IT professionals who want to deepen their understanding of defensive security, particularly focusing on network defense mechanisms, endpoint protection, and incident response.
6. **Cybersecurity Consultants**: Freelancers or consultants who wish to add defensive security strategies to their toolkit, offering security assessments and incident response planning to organizations.