INT250:DIGITAL EVIDENCE ANALYSIS

L:2 T:0 P:2 Credits:3

Course Outcomes: Through this course students should be able to

CO1 :: describe the fundamentals of computer forensics and incident response handling process.

CO2 :: discuss data acquisition fundamentals, methodology and file system

CO3 :: examine the evidence handling procedure and window forensics

CO4 :: impart the knowledge of linux tools and network forensics

CO5 :: analyze system memory and explore email crime investigation

CO6 :: practice forensic report writing and investigating routers

Unit I

Understanding Computer Forensics : What is computer security incident? Understand the Fundamentals of Computer Forensics, Understand Cybercrimes and their Investigation Procedures, Understand Digital Evidence, Understand Forensic Readiness, Incident Response, and the Role of SOC (Security Operations Center) in Computer Forensics, Identify the Roles and Responsibilities of a Forensic Investigator

Computer Forensics Investigation Process : Understand the Forensic Investigation Process and Its Importance, Understand the Pre-investigation Phase, Understand First Response, Understand the Investigation Phase.

Unit II

Understanding Hard Disks and File Systems : Describe Different Types of Disk Drives, Explain the Logical Structure of a Disk, Understand Booting Process of Windows and Linux, Understand Various File Systems of Windows and Linux, Examine File System Using Autopsy, Understand Storage Systems, Understand Encoding Standards and Hex Editors

Data Acquisition and Duplication : Understand Data Acquisition Fundamentals, Understand Data Acquisition Methodology, Prepare an Image for Examination

Unit III

Evidence handling : What is evidence? Challenges of evidence handling, Evidence collection procedures and handling procedures.

Windows Forensics : Collect Volatile and Non-volatile Information, Perform Windows Memory and Registry Analysis, Examine the Cache, Cookie and History Recorded in Web Browsers, Examine Windows Files and Metadata, Understand Text- based Logs and Windows Event Logs

Unit IV

Linux : Understand Volatile and Non-volatile Data in Linux, Analyze File system Image, Demonstrate Memory Forensics.

Network Forensics : Understand Network Forensics, Explain Logging Fundamentals and Network Forensic Readiness, Summarize Event Correlation Concepts, Identify Indicators of Compromise (IoCs) from Network Logs, Investigate Network Traffic.

Unit V

Analysing system memory : Memory evidence overview, Memory analysis, Tools

Dark Web Forensics : Understand the Dark Web

Investigating Email Crimes : Understand Email Basics, Understand Email Crime Investigation and its Steps.

Unit VI

Investigating routers : Obtaining volatile data prior to powering down, Finding the proof, Using routers as response tools

Writing computer forensic reports : What is a computer forensic report?, Report writing guidelines, A template for computer forensic reports

List of Practicals / Experiments:

Network Evidence Collection

- Network evidence collection and analysis of captured packet with the help of tcpdump

- nmap
- wireshark

Understanding Forensic Imaging

- Demonstration of Dead Imaging and Live Imaging with help of FTK Imager .

Network-Evidence Analysis

- Analysis of packet information and gaining overall sense of traffic contained within a packet capture with the help of Wireshark

Network Log Analysis

- Analyzing network log files with help of DNS Blacklists

Analyzing System Memory

- Reviewing the images of memory with the help of Mandiant Redline.

Analyzing System Storage

- Demonstration of timeline analysis
- keyword searching
- and web and email artifacts and to filter results on known bad file hashes using Autopsy.

Integrity Check

- MD5 Sum Utility
- Simple Hasher Tool

Acquiring Host Based Evidences

- Local volatile and non-volatile acquisition and memory acquisition with the help FTK imager

Window Investigation

- Demonstration of window investigation using OS Forensics

References:

1. DIGITAL FORENSICS AND INCIDENT RESPONSE by GERARD JOHANSEN, PACKT PUBLISHING

2. INCIDENT RESPONSE & COMPUTER FORENSICS by JASON LUTTGENS, MATTHEW PEPE AND KEVIN MANDIA, Mc Graw Hill Education