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 incident response handling process.

CO2 :: discuss the methodology of detecting an incident and responding to it in case of a security breach

CO3 :: examine the process of live data collection and forensic duplication during forensic investigations

CO4 :: outline the network and host-based evidence collection during the evidence handling process

CO5 :: classify various data analysis techniques for network and system evidence data

CO6 :: evaluate the process of extracting critical data from windows systems and routers

Unit I

Introduction to Incident Response : What is computer security incident?, What are goals of incident response?, Who is involved in incident response process?, Incident response methodology, Formulate a response strategy, Investigate the incident, Reporting, Resolution, The incident response framework, CSIRT, Incident response plan, Incident classification, Incident response playbook, Escalation procedures, Maintaining incident response capability

Unit II

Preparing for Incident Response : Overview of incident response preparation, Identifying risks, Preparing individual hosts, Preparing a network, Establishing appropriate policies and procedures, Creating a response toolkit, Establishing an incident response team

After detecting an Incident : Overview of initial response phase, Establishing an incident notification procedure, Recording details after initial detection, Incident declaration, Assembling the CSIRT, Performing traditional investigative steps, Conducting interviews, Formulating a response strategy.

Unit III

Live data collection : Creating a response toolkit, Storing information obtained during initial response, Obtaining volatile data, Performing in-depth live response, Is forensic duplication necessary?

Forensic duplication : Forensic duplicates as admissible evidence, Forensic duplication tool requirement, Creating a forensic duplicate of a hard drive, Creating a qualified forensic duplicate of hard drive.

Unit IV

Collecting network based Evidence : What is network based evidence?, Goals of network monitoring, Types of network monitoring, Setting up a network monitoring system, Performing a trap and trace, Using TCPDUMP for full-context monitoring, Collecting network based log files

Acquiring host-based Evidence : Preparation, Evidence volatility, Evidence acquisition, Evidence collection procedures, Memory acquisition, Local acquisition, Remote acquisition, Virtual machines, Non-volatile data

Evidence handling : What is evidence?, Challenges of evidence handling, Overview of evidence handling procedures

Unit V

Data analysis techniques : Preparation for forensic analysis, Restoring a forensic duplicate, Restoring a qualified forensic duplicate of a hard disk, Reviewing image files with forensic suites, Converting a qualified forensic duplicate to a forensic duplicate, Recovering deleted files on windows systems, Recovering unallocated space, Free space and slack space, Generating files list, Preparing a drive for string searches

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

Network evidence analysis : Analyzing packet captures, Command line tools, Wireshark, Xplico and CapAnalysis, Analyzing network log files, DNS blacklists, SIEM, ELK stack

Unit VI

Investigating windows systems : Where evidence resides on windows systems, Conducting a windows investigation, Identifying unauthorized user accounts or groups, File auditing and theft of information, Handle the departing employee

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
- RawCap and Wireshark.

Acquiring Host Based Evidence

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

Understanding Forensic Imaging

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

Network-Evidence Analysis

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

Network Log Analysis

- Analyzing network log files with help of DNS Blacklists and ELK Stacks.

Analyzing System Memory

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

Volatility

- Performing the analysis of memory images with the help of opensource advanced memoryforensics framework.

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.

Text Books:

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

References:

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