KL (DEEMED TO BE UNIVERSITY)

CRYPT ANALYSIS & CYBER DEFENCE

22CSB3101A

III YEAR ,I SEMESTER
Academic Year: 2024-2025
KONERU LAKSHMAIAH EDUCATION FOUNDATION

CRYPT ANALYSIS & CYBER DEFENCE

(22CSB3101A, 22CSB3101R &22CSB3101P)

Mode: A

SKILL WORKBOOK

STUDENT ID:

ACADEMIC YEAR: 2024-25

STUDENT NAME

KLEF (Deemed to be University), Vaddeswaram

UNIVERSITY VISION AND MISSION

Vision

To be a Globally Renowned University

Mission

To impart quality higher education and to undertake research and extension with emphasis on application and innovation that cater to the emerging societal needs through all-round development of the students of all sections, enabling them to be globally competitive and socially responsible citizens with intrinsic values.

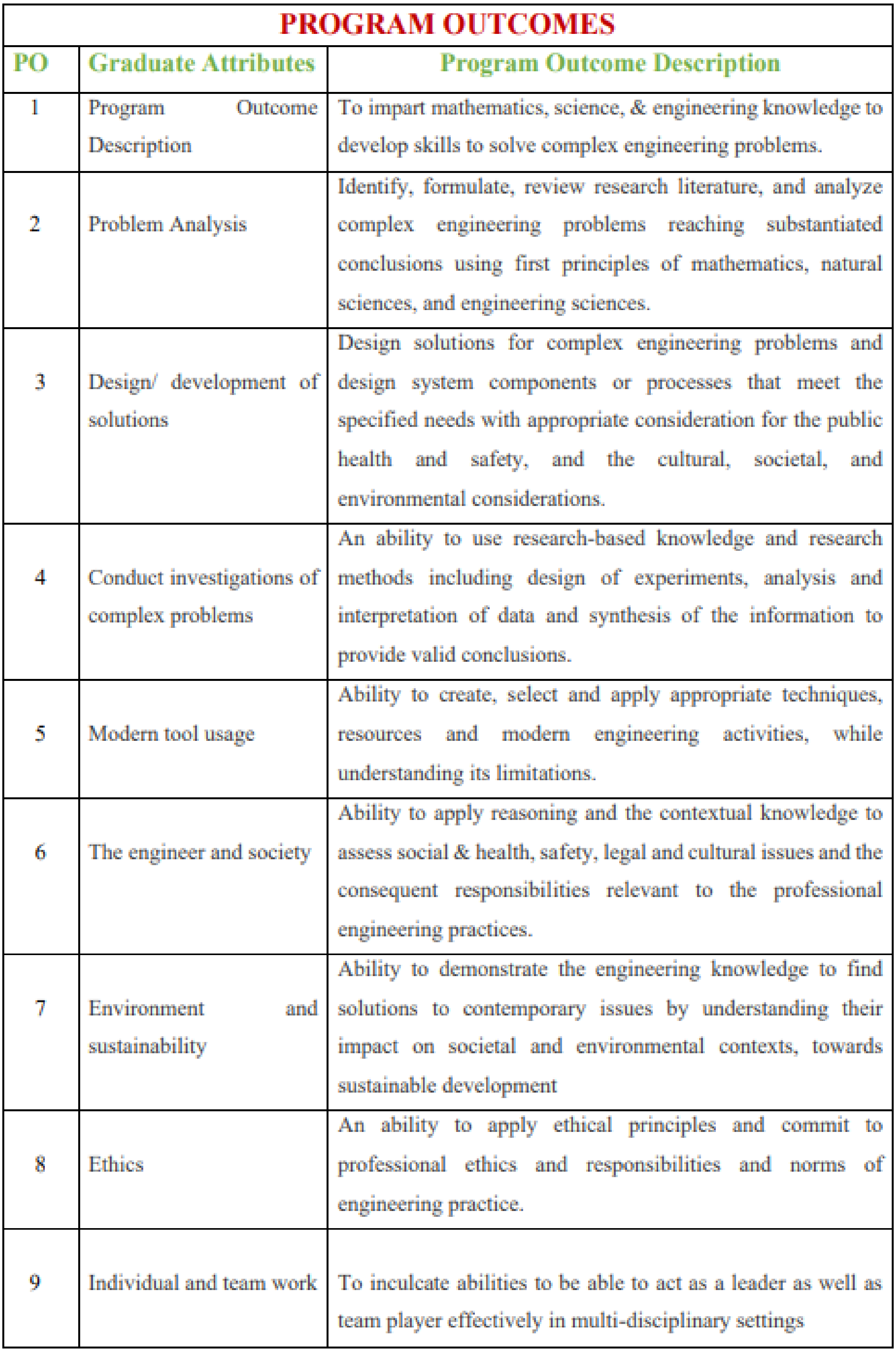
Weblink: **https://www.kluniversity.in/Mission.aspx**

Department of Computer Science and Engineering

Program Educational Objectives

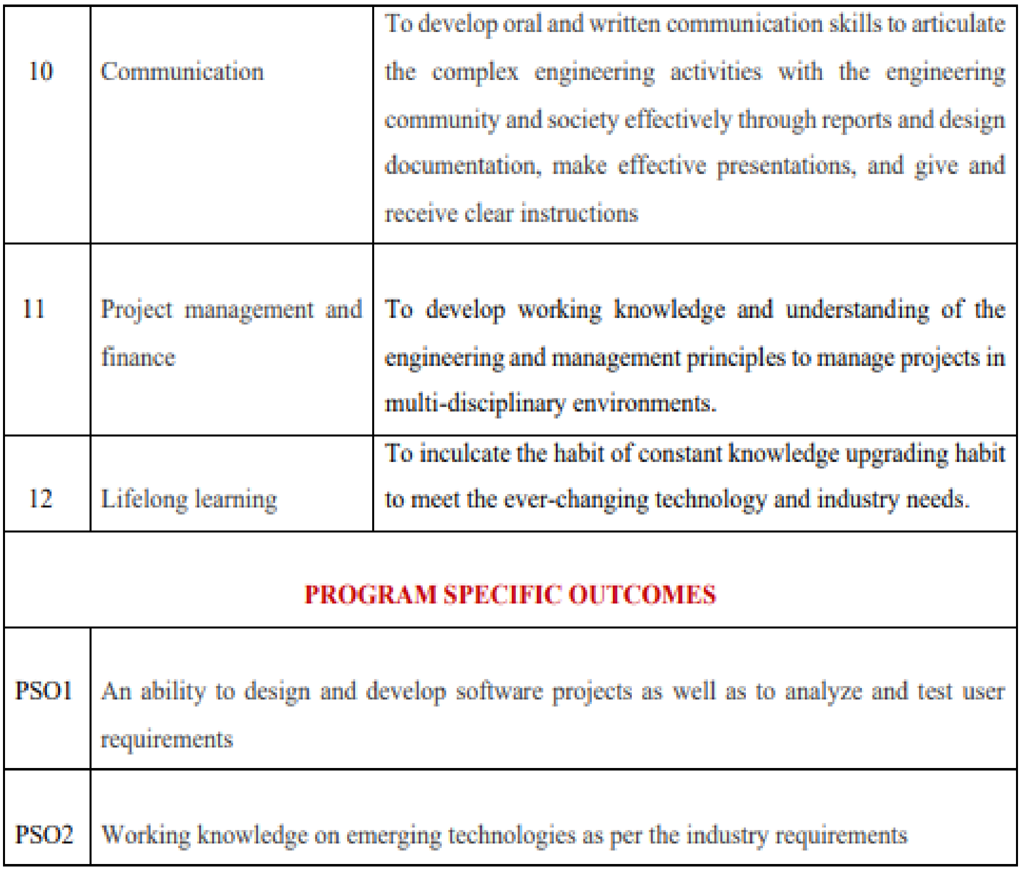
1. **Practice engineering in a broad range of industrial, societal and real-world applications.**
2. **Pursue advanced education, research and development, by adapting creative and innovative practices in their professional careers.**
3. **Conduct themselves in a responsible, professional, and ethical manner.**
4. **Participate as leaders in their fields of expertise and in activities that support service and economic development throughout the world.**

Web link: https://www.kluniversity.in/cse1/vission.aspx



PROGRAM OUTCOMES

PO	Graduate Attributes	Program Outcome Description
1	Program Outcome Description	To impart mathematics, science, & engineering knowledge to develop skills to solve complex engineering problems.
2	Problem Analysis	Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3	Design/ development of solutions	Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4	Conduct investigations of complex problems	An ability to use research-based knowledge and research methods including design of experiments, analysis and interpretation of data and synthesis of the information to provide valid conclusions.
5	Modern tool usage	Ability to create, select and apply appropriate techniques, resources and modern engineering activities, while understanding its limitations.
6	The engineer and society	Ability to apply reasoning and the contextual knowledge to assess social & health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practices.
7	Environment and sustainability	Ability to demonstrate the engineering knowledge to find solutions to contemporary issues by understanding their impact on societal and environmental contexts, towards sustainable development
8	Ethics	An ability to apply ethical principles and commit to professional ethics and responsibilities and norms of engineering practice.
9	Individual and team work	To inculcate abilities to be able to act as a leader as well as team player effectively in multi-disciplinary settings



10	Communication	To develop oral and written communication skills to articulate the complex engineering activities with the engineering community and society effectively through reports and design documentation, make effective presentations, and give and receive clear instructions
11	Project management and finance	To develop working knowledge and understanding of the engineering and management principles to manage projects in multi-disciplinary environments.
12	Lifelong learning	To inculcate the habit of constant knowledge upgrading habit to meet the ever-changing technology and industry needs.
PROGRAM SPECIFIC OUTCOMES		
PSO1	An ability to design and develop software projects as well as to analyze and test user requirements	
PSO2	Working knowledge on emerging technologies as per the industry requirements	

Table of Contents

A.Y. 2024-25 SKILL CONTINUOUS EVALUATION

S.No	Date	Experiment Name	Pre-Skill (10M)	In-Skill (25M)			Post-Skill (10M)	Viva Voce (5M)	Total (50M)	Faculty Signature
				Program/Procedure (5M)	Data and Results(10M)	Analysis & Inference(10M)				
1		Installing Virtual Box and Creating a Virtual install of Kali Linux								
2.		Analyse Packet Capturing Using Airodump-ng								
3.		Implementation of Social Engineering Using King Phisher								
4.		Implementation of Social Engineering Using Maltego								
5.		Implementation of Password Cracking Using John the Ripper								
6.		Implementation of Wi-Fi Hacking Using Reaver								
7.		Implementation of NMAP Scanning Technique								
8.		Implementation of Man in the Middle Attack using (Ettercap Tool)								
9.		Analyse Mobile Security Using APK Tool								
10.		Implementation of Web Application Security Using Burp Suite								

S.No	Date	Experiment Name	Pre-Skill (10M)	In-Skill (25M)			Post-Skill (10M)	Viva Voce (5M)	Total (50M)	Faculty Signature
				Program/Procedure (5M)	Data and Results(10M)	Analysis & Inference(10M)				
11		Implementation of SQL Injection Using SQL Map								
12.		Implementation of Cross Site Scripting Attack								
13.		Analyse Windows Exploit using Metasploit								
14.		Analyse Vulnerability Analysis Using Wireshark								
15.		Implementation of Web Application Security (Paros)								
16.		Analyse Processing Crime and Incident Scenes								
17.		Implementation to find Last Connected USB on your system (USB Forensics)								
18.		Implementation to View Last Activity of Your PC								
19.		Implementation of Working with Windows and CLI Systems								
20.		Implementation of Live Forensics Case Investigation using Autopsy								
21.		Implementation of Recovering Deleted Files								

S.No	Date	Experiment Name	Pre-Skill (10M)	In-Skill (25M)			Post-Skill (10M)	Viva Voce (5M)	Total (50M)	Faculty Signature
				Program/Procedure (5M)	Data and Results(10M)	Analysis & Inference(10M)				
		using Forensics Tools								
22		Implementation to Extract Browser Artifacts								
23		Implementation of Comparing two Files for forensics investigation by Compare IT software								
24		Implementation of Collecting Email Evidence in Victim PC								

Experiment #		Student ID	
Date		Student Name	

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

1. Installing Virtual Box and Creating a Virtual install of Kali Linux

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective: The learning objective of this task is to understand the process of installing Virtual Box and setting up Kali Linux as a virtual machine.

Description: In this task, you will learn how to install Oracle VirtualBox, a virtualization software, and create a virtual machine to install Kali Linux, a popular penetration testing and security auditing Linux distribution. This setup allows you to run Kali Linux as a virtual operating system within your existing operating system, providing a safe and isolated environment for security testing and experimentation.

Pre-Requisites:

1. Oracle VirtualBox: You will need to download and install the latest version of VirtualBox from the official Oracle website. Ensure that you choose the appropriate version for your operating system (Windows, macOS, or Linux).

2. Kali Linux ISO: Download the latest Kali Linux ISO image from the official Kali Linux website. Select the appropriate ISO file based on your system architecture (32-bit or 64-bit).

Steps to Install VirtualBox and Set Up Kali Linux:

1. Download and Install VirtualBox:

- Go to the Oracle VirtualBox website (https://www.virtualbox.org) and download the installer for your operating system.
- Run the installer and follow the on-screen instructions to install VirtualBox on your computer.

2. Prepare the Kali Linux Virtual Machine:

- Launch VirtualBox.
- Click on "New" to create a new virtual machine.
- Provide a name for the virtual machine (e.g., "Kali Linux") and select the operating system type as "Linux" and version as "Other Linux (64-bit)" or "Other Linux (32-bit)" depending on your ISO file.
- Allocate the desired amount of RAM for the virtual machine (at least 2GB is recommended).
- Choose the option to create a virtual hard disk now.
- Select the hard disk file type as "VDI" (VirtualBox Disk Image).
- Choose "Dynamically allocated" for the storage on physical hard disk.
- Specify the size of the virtual hard disk (20GB or more is recommended).
- Click "Create" to create the virtual machine.

3. Configure the Kali Linux Virtual Machine:

- In the VirtualBox Manager, select the newly created virtual machine and click on "Settings."
- In the settings window, navigate to the "Storage" tab.
- Under "Controller: IDE," click on the disk icon next to "Empty" and choose the Kali Linux ISO file you downloaded.
- Click "OK" to save the settings.

4. Install Kali Linux:

- Start the Kali Linux virtual machine by selecting it in the VirtualBox Manager and clicking on the "Start" button.
- The Kali Linux installation process will begin. Follow the on-screen instructions to install Kali Linux within the virtual machine.
- After the installation is complete, restart the virtual machine.

5. Set Up Kali Linux:

- Log in to Kali Linux using the credentials you created during the installation process.
- Configure the network settings, update the system, and install any desired tools or packages within Kali Linux.

By following these steps, you will have successfully installed VirtualBox and set up Kali Linux as a virtual machine.

Note: It's important to ensure you have sufficient system resources (CPU, RAM, disk space) to run Virtual Box and the virtual machine smoothly.

Pre-Skill Task:

1. What is VirtualBox, and what is its purpose in the context of virtualization?

2. Explain the benefits of using virtualization for running operating systems.

3. Can you provide a step-by-step guide on how to install VirtualBox on a specific operating system?

4. What are the minimum system requirements for running VirtualBox effectively?

5. How do you create a new virtual machine in VirtualBox? Explain the necessary steps.

In-Skill Task:

Harsha a technology evangelist has just started learning about OS virtualization and interestedin learning ethical hacking as Harsha a newbie in this you are requested by Harsha to help himto install Kali Linux in his computer using Virtual Box

Viva questions:

1. Describe the process of downloading the Kali Linux ISO image and selecting the appropriate version.

2. What are the recommended settings for a virtual machine running Kali Linux in terms of memory allocation, CPU, and storage?

3. What is the significance of enabling virtualization features in the computer's BIOS settings?

4. Explain the network configuration options available in VirtualBox and their implications for a virtual machine running Kali Linux.

5. How do you mount the Kali Linux ISO image to the virtual machine and initiate the installation process?

Post Lab Task:

1. Why Kali Linux is newbie friendly for cyberSecurity enthusiast?

2. What are different types of Linux Distro’s available?

3. List some security focused Linux Distro’s available.

(For Evaluator’s use only)

Comment of the Evaluator (if Any)	Evaluator’s Observation Marks Secured:________out of __________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation:

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

2. Analyse Packet Capturing Using Airodump-ng

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of analysing packet capturing using Airodump-ng is to gain an understanding of wireless network traffic and perform advanced analysis on captured packets. This involves identifying nearby wireless networks, monitoring network activity, and extracting valuable information from captured packets.

Description:

Airodump-ng is a powerful command-line tool used for capturing and analyzing wireless network packets. It is part of the Aircrack-ng suite and is primarily used for monitoring and analysing Wi-Fi networks. Airodump-ng captures raw wireless packets from nearby networks, allowing users to analyze network traffic, discover connected devices, and gather information about the network's security.

Pre-Requisites:

To complete the analysis of packet capturing using Airodump-ng, you will need the following software:

1. Aircrack-ng Suite: Airodump-ng is part of the Aircrack-ng suite, which includes other tools for wireless network analysis and security testing. You can download the Aircrack-ng suite from the official website (https://www.aircrack-ng.org/) and follow the installation instructions specific to your operating system.

2. Terminal or Command Prompt: Airodump-ng is a command-line tool, so you will need a terminal or command prompt to execute the Airodump-ng commands. Most operating systems provide built-in terminals or command prompts.

3. Compatible Wireless Network Adapter: Airodump-ng requires a wireless network adapter that supports monitor mode for capturing packets. Make sure you have a compatible Wi-Fi adapter installed on your system. You can check the Aircrack-ng website for a list of supported adapters (https://www.aircrack-ng.org/doku.php?id=compatible_cards).

Experiment #		Student ID	
Date		Student Name	

Pre-Skill Task:

1.What is packet capturing, and why is it important in network analysis and security?

2. Can you explain the purpose and functionality of Airodump-ng?

3. What are the prerequisites and system requirements for using Airodump-ng effectively?

4. How does Airodump-ng capture packets from wireless networks? Explain the underlying mechanism.

5. What are the different types of information that can be obtained by analysing captured packets with Airodump-ng?

In-Skill Task:

1.Ramesh wants to perform “CRACKING WEP KEYS” By using Monitor mode which was available in kali Linux. So, he wants to perform following operations:

1.Monitor mode using wifi-adapter

2. Capturing packets

3.Capturing ARP requests

Help him by doing those operations Successfully (If Possible, include screenshots of those outputs)

Solution:

Viva Questions:

1. How can Airodump-ng help in analysing wireless network security vulnerabilities, such as identifying rogue access points or detecting unauthorized clients?

2. What are the different filtering options available in Airodump-ng, and how can they be used to focus on specific network or device information?

3. Explain the significance of different fields displayed in the Airodump-ng output, such as BSSID, ESSID, Power, Channel, and Encryption.

4. How can you interpret and analyse the collected data in Airodump-ng, such as identifying patterns, trends, or potential security issues?

5 Are there any limitations or challenges associated with using Airodump-ng for packet capturing and analysis? How can these limitations be mitigated or overcome?

Post-Skill-Task:

1) write the steps of analyzing packet capturing using Airodump-ng,

Sol)

Experiment #		Student ID	
Date		Student Name	

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT CODE: 22CSB3101A,
CRYPTANALYSIS AND CYBER DEFENSE WORKBOOK

3. Implementation of Social Engineering Using King Phisher

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of implementing social engineering using King Phisher is to understand the techniques and tools used in social engineering attacks and gain practical experience in conducting such attacks in a controlled environment.

Description:

Social engineering is a method of manipulating individuals to disclose sensitive information or perform certain actions by exploiting their trust, curiosity, or ignorance. King Phisher is an open-source software tool that helps simulate and test social engineering attacks, allowing organizations to assess their vulnerability to such attacks and develop countermeasures. This project involves implementing social engineering attacks using King Phisher to understand the various attack vectors, analyse their effectiveness, and explore ways to mitigate the associated risks.

Pre-Requisites:

1. King Phisher: An open-source phishing campaign toolkit.

2. Virtual Machine or Sandbox Environment: To set up a controlled environment for testing and executing social engineering attacks.

3. Operating System: Linux distribution (recommended) or Windows with a virtualization platform like VirtualBox or VMware.

Pre-Skill:

1. What is social engineering, and why is it considered a significant threat to organizations?

2. Explain the concept of phishing and how it is used in social engineering attacks.

3. What is King Phisher, and what functionalities does it offer for conducting social engineering attacks?

4. Describe the process of setting up a virtual machine or sandbox environment for implementing social engineering using King Phisher.

5. How can King Phisher be used to create and customize phishing campaigns?

In-Skill Task:

1) Siddharth is a Computer Science Student, and he is Naughty. He wants to fool his friend Siva by sending a Fake Mail by King Phisher tool. But he doesn’t know that how that tool Works.

a. He want to learn How the Tool (King Phisher) Works

So, Help Siddharth to understand how the Tool Work in a step-by-step process.

Viva Questions:

- What are the different types of social engineering attacks that can be simulated using King Phisher?
- What are the potential risks and ethical considerations involved in implementing social engineering attacks using King Phisher?
- How can organizations defend against social engineering attacks, and how can the insights gained from using King Phisher be utilized to improve security measures?
- Discuss the legal and regulatory implications of conducting social engineering attacks for educational or testing purposes.
- How can user awareness training and education be effective in mitigating social engineering attacks, and how does King Phisher contribute to this process?

Post Lab Task:

1. What is Ghost Phisher?

-

2.Name the dependencies that are required in the proper running of Ghost Phisher.

- *(For Evaluator's use only)*

Comment of the Evaluator (if Any)	Evaluator's Observation
	Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

Experiment #		Student ID	
Date		Student Name	

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

4. Implementation of Social Engineering Using Maltego

Date of the Session: ___/___/___ **Time of the Session: _____to______**

Learning Objective:

The learning objective of implementing social engineering using Maltego is to understand the techniques and tools involved in conducting social engineering attacks and to utilize Maltego software for gathering and analysing relevant information to facilitate the attacks.

Description:

Social engineering is a technique used by malicious actors to manipulate individuals and exploit their vulnerabilities to gain unauthorized access to systems or sensitive information. Maltego is a powerful data mining and visualization tool that can be used for information gathering and analysis. In this project, the goal is to explore the use of Maltego in conducting social engineering attacks by utilizing its features to collect and analyse data about the target, identify potential attack vectors, and develop persuasive techniques to deceive individuals.

Pre-Requisites:

1. Maltego: A licensed version of Maltego software needs to be installed. Maltego provides different editions, such as Maltego Classic, XL, or CE (Community Edition). The choice of edition depends on the project requirements and access to various features.

Pre-Skill Task:

1. What is social engineering and why is it considered a threat to security?

2. How does Maltego assist in the implementation of social engineering attacks?

3. What are the primary steps involved in conducting a social engineering attack using Maltego?

4. How does Maltego facilitate data gathering and analysis during a social engineering attack?

5. Can you explain the process of identifying potential attack vectors using Maltego?

In-Skill Task:

Kavya heard about the sales in Myntra. She wants to find out the name servers of 'myntra.com'. She is also keen to know what other domains use these name servers. Help her in finding out the above mentioned using Maltego. Also help her get the email addresses thesedomains use and verify whether these mails exist or not.

Viva Questions :

- What are some persuasive techniques commonly employed in social engineering attacks?
- How can Maltego be used to simulate and validate social engineering attacks without causing harm?
- What are the ethical considerations and legal implications of implementing social engineering using Maltego?
- How can organizations protect themselves against social engineering attacks conducted through tools like Maltego?
- Can you discuss any real-world examples of social engineering attacks and the role of Maltego in their execution?

Post-Skill-Task:

1.Write a detailed report on the methodology and techniques used in the social engineering experiment.

2. Discuss the effectiveness of different social engineering tactics employed.

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 22CSB3101A,
CRYPTANALYSIS AND CYBER DEFENSE WORKBOOK

5. Implementation of Password Cracking Using John the Ripper

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of implementing password cracking using John the Ripper is to understand the principles and techniques of password cracking and gain hands-on experience with the John the Ripper software.

Description:

This project involves implementing password cracking using John the Ripper, a popular open-source password cracking tool. The project aims to explore different password cracking techniques, such as dictionary attacks, brute-force attacks, and hybrid attacks, and understand their strengths and limitations. By using John the Ripper, you will gain practical knowledge of configuring and utilizing the tool to crack passwords from various sources, such as password hashes obtained from system files or password-protected files.

Pre-Requisites:

1. John the Ripper: The primary Pre-Requisites for this project is John the Ripper, which is an open-source password cracking tool. It is available for various operating systems, including Windows, Linux, and macOS.

Pre-Skill:

1. What is password cracking, and why is it important from a security perspective?

2. Explain the working principle of John the Ripper.

3. What are the different types of password cracking techniques supported by John the Ripper?

4. How does a dictionary attack work, and what are its limitations?

5. Describe the process of configuring John the Ripper for password cracking.

In-Skill Task:

1.Two best friends started doing a project at last they made the project into a zip file with a password. Unfortunately, by the presentation day they both forgot the password, so help them out by cracking the password using John the Ripper

Viva Questions

- What are the commonly used password hash formats supported by John the Ripper?
- How does John the Ripper handle salted password hashes?
- What is the difference between a brute-force attack and a dictionary attack?
- Explain the concept of a hybrid attack and its advantages over other cracking techniques.
- What are the countermeasures that can be taken to defend against password cracking?

Post Lab:

Perform the following Tasks by using John the Ripper Tool

1. Security Auditing

2. Penetration Testing

3. Password Recovery

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

6. Implementation of Wi-Fi Hacking Using Reaver

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of implementing Wi-Fi hacking using Reaver is to understand the vulnerabilities in Wi-Fi networks and gain practical knowledge of exploiting these vulnerabilities to gain unauthorized access to protected networks. Additionally, the objective is to familiarize oneself with the Reaver tool and its functionalities for conducting Wi-Fi hacking.

Description:

The implementation of Wi-Fi hacking using Reaver involves using the Reaver tool, which is an open-source software designed to exploit vulnerabilities in WPS (Wi-Fi Protected Setup) enabled routers. Reaver utilizes a brute-force attack against the WPS PIN to recover the Wi-Fi passphrase or key. This implementation aims to demonstrate the security weaknesses of WPS and educate users about the importance of securing their Wi-Fi networks.

Pre-Requisites:

1. Reaver: It is an open-source command-line tool available for Linux and other Unix-based operating systems. It can be downloaded and installed from the official Reaver website or via package managers like apt-get or yum.

Pre-Skill:

1. What is the objective of implementing Wi-Fi hacking using Reaver?

2. Explain the purpose of Reaver in Wi-Fi hacking.

3. What is WPS and how does it contribute to Wi-Fi vulnerability?

4. Describe the process followed by Reaver to exploit WPS vulnerabilities.

5. What precautions should be taken before conducting Wi-Fi hacking using Reaver?

In-Skill-Task:

1. Dheeraj is learning Reaver. As a beginner he wants to know the use of following commands in Reaver:-

i) Wash

ii) Reaver

2. Karun forgot his Wi-Fi password. He wants to know the password. Karun approached you for help. Help Karun by hacking the Wi-Fi using Reaver.

Write down the wireless interface names, monitor mode, ESSID, Channel, BSSID of the target and paste the screen shots of execution and the outputs.

Note:- Perform this experiment on your native Wi-fi, your home Wi-Fi preferably.

Viva Questions:

- Are there any legal implications associated with Wi-Fi hacking using Reaver? Explain.
- What are some countermeasures that can be implemented to protect against Reaver attacks?
- Can you suggest alternative tools or techniques for Wi-Fi penetration testing apart from Reaver?
- How does the implementation of Wi-Fi hacking using Reaver help raise awareness about Wi-Fi security?
- In what scenarios can the knowledge gained from implementing Wi-Fi hacking using Reaver be useful from a security perspective?

Post-Skill- Task:

- Key Generation Techniques:
- Strength of AES Keys:
- Key Management and Storage:
- Key Generation Performance:

Experiment #		Student ID	
Date		Student Name	

(For Evaluators Use Only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

7. Implementation of NMAP Scanning Technique

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of implementing the NMAP scanning technique is to understand and gain practical experience with network scanning using the NMAP tool. By the end of this project, students should be able to effectively utilize NMAP to discover hosts, services, and vulnerabilities on a network.

Description:

The implementation of the NMAP scanning technique involves using the NMAP tool to perform network scans and gather information about hosts and services. Students will learn how to configure and execute different types of scans, interpret the results, and understand the implications of the findings. They will also gain knowledge about common scanning techniques, such as TCP SYN, UDP, and comprehensive scanning.

Pre-Requisites:

1. NMAP: It is an open-source network scanning tool available for Windows, Linux, and macOS. Students should have NMAP installed on their machines to perform the scans.

Pre-Skill:

1. What is NMAP, and why is it used for network scanning?

2. Describe the different types of scanning techniques supported by NMAP.

3. How can you perform a TCP SYN scan using NMAP? Explain the steps involved.

4. What is the purpose of performing a UDP scan? How can you execute it using NMAP?

5. What is a comprehensive scan? How is it different from other scanning techniques?

In-Skill Task:

1. Vicky came to know that NMAP (Network Mapper) is a very versatile tool for Linux system/network administrators and is used for exploring networks, perform security scans, network audit and finding open ports on remote machine, Live hosts and Operating systems. So, he decided to work on the tool. Help him in performing the following scans:

   a. Ping sweep

   b. Port scan

   c. TCP full open scan

   d. TCP SYN scan

   e. UDP scan

   f. Version detection scan

   g. OS detection scan and

   h. Aggressive scan.

Viva Questions:

- Explain the concept of stealth scanning and how it can be achieved with NMAP.
- How does NMAP identify the operating system of a target host? Discuss the techniques used.
- What is banner grabbing, and why is it useful during a network scan? How can NMAP accomplish banner grabbing?
- What are some common options and flags used in NMAP? Provide examples and explain their significance.
- . How can NMAP be used for vulnerability scanning? Discuss the process and the benefits of integrating vulnerability scanning with network scanning.

Post -Skill-Task:

1. Billy is trying to understand how "–v" option is used in NMAP scanning technique. Explain him the use of the option "-v" by working on it.

Experiment #		Student ID	
Date		Student Name	

(For Evaluator’s use only)

Comment of the Evaluator (if Any)	Evaluator’s Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

Experiment #		Student ID	
Date		Student Name	

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

8. Implementation of Man in the Middle Attack using (Ettercap Tool)

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of implementing a Man-in-the-Middle (MITM) attack using the Ettercap tool is to understand the concepts and techniques involved in intercepting and manipulating network communications for malicious purposes, and to gain practical experience in executing such an attack.

Description:

In this project, you will learn how to use the Ettercap tool to perform a Man-in-the-Middle attack. A Man-in-the-Middle attack involves intercepting and altering communication between two parties without their knowledge. Ettercap is a widely used tool for executing MITM attacks, and it provides various features for sniffing and manipulating network traffic. By implementing this attack, you will gain insights into the vulnerabilities that exist in network communications and the potential risks associated with them. You will learn how an attacker can eavesdrop on sensitive information, inject malicious content, or impersonate legitimate entities to deceive users.

Pre-Requisites:

To implement the Man-in-the-Middle attack using the Ettercap tool, you will need the following software and tools:

1. Ettercap: The Ettercap tool is an open-source network security tool available for various operating systems. It can be downloaded from the official Ettercap website (https://www.ettercap-project.org).

Pre-Skill:

1. What is a Man-in-the-Middle attack, and how does it work?

2. What are the potential risks and consequences of a successful Man-in-the-Middle attack?

3. Explain the role of Ettercap in executing a Man-in-the-Middle attack.

4. What are the steps involved in setting up and configuring Ettercap for the attack?

5. How does Ettercap intercept network traffic, and what techniques does it use for packet sniffing?

In-Skill Task

1. Monica and Jessica are exploring possible man in the middle attacks in cyber security in that process they learnt about ARP poisoning/spoofing. To demonstrate this they wanted to work with Ettercap, what could be the process or steps involved in this experiment, Demonstrate.

Viva Questions:

- How can an attacker leverage a Man-in-the-Middle attack to obtain sensitive information from network communications?
- What countermeasures can be taken to prevent or mitigate Man-in-the-Middle attacks?
- Discuss the ethical implications and legal consequences of performing a Man-in-the-Middle attack without proper authorization.
- Can you explain any real-world examples or case studies where Man-in-the-Middle attacks have been employed?
- How can network administrators detect and defend against Man-in-the-Middle attacks in their systems?

Post -Skill-Task:

1. Explain the four modules in the Ettercap?

2. Is Ettercap a sniffing tool?

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 22CSB3101
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

9. Analyse Mobile Security Using APK Tool.

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The objective of this analysis is to understand and evaluate the mobile security of Android applications using APK Tool, a popular tool for reverse engineering and analysing APK files.

Description: This analysis focuses on utilizing APK Tool to assess the security aspects of mobile applications. APK Tool allows the extraction of the source code, resources, and other components of an APK file, enabling a deeper understanding of the application's inner workings. By analysing the extracted information, various security vulnerabilities can be identified, such as insecure data storage, weak encryption, improper permissions, and potential code vulnerabilities.

Pre-Requisites:

1. APK Tool: This is the main Pre-Requisites for reverse engineering and analysing APK files. It can be downloaded from the official website or obtained through package managers like Homebrew or Chocolatey.

2. Java Development Kit (JDK): APK Tool requires the JDK to be installed on the system, as it relies on Java for its functionality.

3. Decompile/Disassembler: While not mandatory, having a decompile or disassembler tool like JADX, JD-GUI, or JADX-GUI can enhance the analysis process by providing a more readable representation of the decompiled code.

Pre-Skill:

1. What is the purpose of APK Tool in mobile security analysis?

2. How does APK Tool help in understanding the inner workings of an Android application?

3. What are the steps involved in using APK Tool to analyse mobile security?

4. Can you explain the process of extracting the source code and resources from an APK file using APK Tool?

5. What are some common security vulnerabilities that can be identified through APK Tool analysis?

In-Skill Task:

1. MOBILE SECURITY USING APK TOOL. Explore the following steps.
Task1: Installing process of APK tool? Task2: Working of APK tool
Task 3: What is the conclusion of Working of APK tool?

Viva Questions:

- How can APK Tool help in identifying improper permissions or excessive privileges in an application?
- Are there any limitations or challenges in using APK Tool for mobile security analysis?
- How can the use of a decompile or disassembler tool complement the analysis process with APK Tool?
- Can you provide examples of real-world cases where APK Tool analysis has revealed significant security vulnerabilities?
- What are the best practices for using APK Tool and ensuring the security of the analysis environment?

Post -Skill- Task:

Perform the following things by using APK Tools

1. Vulnerability Assessment
2. Malware Analysis
3. Penetration Testing
4. Code Auditing

(For Evaluator’s use only)

Comment of the Evaluator (if Any)	Evaluator’s Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

10.Implementation of Web Application Security Using Burp Suite.

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of implementing web application security using Burp Suite is to understand the fundamentals of web application security testing and learn how to utilize Burp Suite, a popular web application security testing tool, to identify vulnerabilities and secure web applications.

Description:

This project involves the practical implementation of web application security using Burp Suite. Burp Suite is an integrated platform for performing security testing of web applications. It combines various tools and functionalities to identify vulnerabilities, such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and more. By utilizing Burp Suite, you will learn how to perform manual and automated security testing, analyse and intercept web traffic, manipulate requests and responses, and identify and exploit vulnerabilities in web applications.

Pre-Requisites:

1. Burp Suite: It is essential to have Burp Suite installed on your machine. Burp Suite Community Edition can be downloaded for free from the Port Swigger website (https://portswigger.net/burp/communitydownload).

Pre-Skill:

1. What is the purpose of web application security testing?

2. Explain the role of Burp Suite in web application security testing.

3. What are the different modules/tools available in Burp Suite?

4. How can you configure your browser to work with Burp Suite for intercepting web traffic?

5. Walk me through the process of manually testing a web application using Burp Suite.

Experiment #		Student ID	
Date		Student Name	

In-Skill Task:

1. Find out all the requests sent to server when we access a particular URL(any URL)? And list those requests here.

2.Open the given URL, change the details entered by the user in that page (first name, last name, user name) using parameter pampering.

Viva Questions:

- What is the difference between active and passive scanning in Burp Suite?
- How can you use Burp Intruder to automate the process of identifying vulnerabilities?
- What are some common web application vulnerabilities that can be identified using Burp Suite?
- How does Burp Suite help in identifying and exploiting SQL injection vulnerabilities?
- Explain the steps involved in securing a web application using Burp Suite's recommendations.

Post -Skill- Task:

1. Perform the following things
2. Security Configuration Assessment
3. Session Management Testing
4. API Security Testing
5. Web Application Firewall (WAF

Experiment #		Student ID	
Date		Student Name	

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

11. Implementation of SQL Injection Using SQL Map

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of implementing SQL Injection using SQLMap is to understand the concept of SQL Injection, learn how to use the SQLMap tool to automate the process, and gain practical experience in identifying and exploiting SQL Injection vulnerabilities in web applications.

Description:

SQL Injection is a common web application vulnerability that allows attackers to manipulate database queries through user input. SQLMap is a powerful open-source penetration testing tool that automates the process of identifying and exploiting SQL Injection vulnerabilities. This exercise focuses on learning how to utilize SQLMap to detect and exploit SQL Injection vulnerabilities in a controlled environment.

Pre-Requisites:

1. SQLMap: SQLMap is a command-line tool written in Python and is used for automating the process of detecting and exploiting SQL Injection vulnerabilities.

2. Web Application: You will need a vulnerable web application that can be used for testing and practicing SQL Injection attacks. This can be a locally hosted application or a deliberately vulnerable web application like Damn Vulnerable Web Application (DVWA) or WebGoat.

Pre-Skill:

1. What is SQL Injection and why is it a significant security vulnerability?

2. Explain the working principle of SQLMap.

3. How do you install and set up SQLMap?

4. What are the different detection techniques employed by SQLMap to identify SQL Injection vulnerabilities?

5. How does SQLMap automate the process of exploiting SQL Injection vulnerabilities?

In-Skill Task:

1. Given below is a testing and demo website for sqlmap practice. http://testphp.vulweb.com/listproducts.php?cat=1

a) Find out the backend DBMS used in the mentioned website. Also list the databases present in it.

b) Now pick any database from the output and list the tables in it.

c) Search for the user name and passwords from those tables and try to login.

Viva Questions:

- Describe the steps involved in conducting a SQL Injection attack using SQLMap.
- What are the potential risks and consequences of SQL Injection attacks?
- How can developers prevent SQL Injection vulnerabilities in their web applications?
- Are there any limitations or challenges associated with using SQLMap for SQL Injection testing?
- Can you explain the difference between blind SQL Injection and error-based SQL Injection, and how SQLMap can handle each type?

Post -Skill- Task:

1. SUBTASK OF PREVIOUS WEBSITE:

a) Dump the artist names available in the database you found out.

b) In the previous question the vulnerable website was already given to you, instead, list one of the various ways through which we can identify vulnerable websites to access their databases and information.

Experiment #		Student ID	
Date		Student Name	

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

12. Implementation of Cross Site Scripting Attack.

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of implementing a Cross-Site Scripting (XSS) attack is to understand the techniques and vulnerabilities associated with XSS attacks, as well as the potential impact they can have on web applications. By gaining hands-on experience with implementing an XSS attack, learners can better understand the importance of secure coding practices and the countermeasures that can be employed to mitigate XSS vulnerabilities.

Description:

The implementation of a Cross-Site Scripting (XSS) attack involves injecting malicious scripts into a vulnerable web application to exploit the trust that a user has for the website. This allows an attacker to execute arbitrary code within the victim's browser, potentially leading to session hijacking, data theft, or defacement of the targeted website. The attack typically occurs when user-supplied input is not properly validated or sanitized by the application.

Pre-Requisites:

1. Web server (e.g., Apache, Nginx)

2. Web application vulnerable to XSS attacks (e.g., Damn Vulnerable Web Application, OWASP Juice Shop)

3. Web browser (e.g., Google Chrome, Mozilla Firefox)

4. Text editor or Integrated Development Environment (IDE) for modifying web application source code (e.g., Sublime Text, Visual Studio Code)

Pre-Skill:

1. What is Cross-Site Scripting (XSS), and how does it differ from other web application vulnerabilities?

2. Explain the three main types of XSS attacks: Stored XSS, Reflected XSS, and DOM-based XSS.

3. Why is input validation and output encoding important in preventing XSS attacks?

4. Describe the steps involved in implementing a simple stored XSS attack.

5. How can an attacker leverage an XSS vulnerability to perform session hijacking?

In-Skill Task:

1. Implement Cross Site Scripting for the following tasks in the given link below. And write the steps you have used for applying XSS:

Link : http://www.xss-game.appspot.com/

Task 1:

Mission Description

This level demonstrates a common cause of cross-site scripting where user input is directly included in the page without proper escaping.

Interact with the vulnerable application window below and find a way to make it execute JavaScript of your choosing. You can take actions inside the vulnerable window or directly edit its URL bar.

Mission Objective

Inject a script to pop up a JavaScript alert() in the frame below. Link: http://www.xss-game.appspot.com/level1

Viva Questions:

- Discuss the potential impact of an XSS attack on a web application and its users.
- What are some techniques or countermeasures that can be used to prevent XSS vulnerabilities?
- How can Content Security Policy (CSP) help mitigate the risk of XSS attacks?
- Explain the difference between server-side XSS filtering and client-side XSS filtering.
- What are the ethical and legal implications of conducting an XSS attack?

Post -Skill- Task:

Mission Description

Web applications often keep user data in server-side and, increasingly, client-side databases and later display it to users. No matter where such user-controlled data comes from, it should be handled carefully.

This level shows how easily XSS bugs can be introduced in complex apps. Mission Objective Inject a script to pop up an alert() in the context of the application.

Note: the application saves your posts so if you sneak in code to execute the alert, this level will be solved every time you reload it.

Link : http://www.xss-game.appspot.com/level2

Experiment #		Student ID	
Date		Student Name	

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

Experiment #		Student ID	
Date		Student Name	

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

13. Analyse Windows Exploit using Metasploit

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of analysing a Windows exploit using Metasploit is to understand the process of identifying, analysing, and exploiting vulnerabilities in Windows operating systems using the Metasploit Framework. This involves gaining practical knowledge of exploit analysis, vulnerability assessment, and penetration testing techniques.

Description:

In this exercise, you will learn how to analyse a Windows exploit using the Metasploit Framework. Metasploit is a powerful open-source penetration testing framework that provides a range of tools and exploits to assess the security of computer systems. You will analyse a specific Windows exploit, understand its underlying vulnerabilities, and exploit them using Metasploit.

Pre-Requisites:

1. Metasploit Framework: Metasploit is an open-source framework available for multiple platforms. You will need to install Metasploit on your system to perform the exploit analysis.

Pre-Skill:

1. What is the purpose of analysing Windows exploits using Metasploit?

2. How does Metasploit help in identifying vulnerabilities in Windows operating systems?

3. Explain the process of analysing a Windows exploit using Metasploit.

4. What are some common vulnerabilities that can be exploited in Windows systems?

5. How does Metasploit assist in exploiting vulnerabilities in Windows?

In-Skill Task:

1. Being a cyber security aspirant you want to join in KL University in cyber security and block chain specialization in order to confirm your seat you should clear basic entrance exam conducted by the University. Your problem statement is to exploit windows xp. All the best Happy Hacking!!

(Hint: You can use smb vulnerability)

Viva Questions:

- What is the MD5 algorithm used for?
- What are the key properties of the MD5 algorithm?
- How does the MD5 algorithm generate a hash value?
- Can you explain the concept of collision resistance in the MD5 algorithm?
- What are the limitations or vulnerabilities of the MD5 algorithm?

Post-Skill-Task:

Perform the following

1. Exploit Development
2. Incident Response:
3. Patch Management
4. Security Awareness and Training

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

14. Analyse Vulnerability Analysis Using Wireshark

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of analysing vulnerability analysis using Wireshark is to understand how to identify and analyse network vulnerabilities using the Wireshark network protocol analyser. Participants will learn how to capture network traffic, interpret packet data, and identify potential security vulnerabilities in network communications.

Description:

This training session focuses on the practical application of Wireshark for vulnerability analysis. Participants will be introduced to the fundamentals of network protocols and packet analysis. They will learn how to capture network traffic using Wireshark, analyse captured packets, and identify common vulnerabilities such as unencrypted credentials, malicious traffic patterns, and potential attack vectors. Additionally, participants will gain insights into different techniques and methodologies for vulnerability analysis using Wireshark.

Pre request:

1. Wireshark: The latest version of Wireshark should be installed on the participants' machines.
2. A network environment: Participants should have access to a network environment, either physical or virtual, to capture network traffic for analysis.

Pre-Skill Task:

1. What is the purpose of Wireshark in vulnerability analysis?

2. How does Wireshark capture network traffic? Explain the different capture methods.

3. What are the common security vulnerabilities that can be identified using Wireshark?

4. Describe the process of analysing captured packets in Wireshark.

5. What are some key features or functionalities of Wireshark that are useful for vulnerability analysis?

In-Skill Task:

1. How to capture the data packets using the Wireshark tool? Mention the step-by-step process.

2. Analyse any packets that you capture and write down their information i.e., their source, destination along with its IP Address and to which protocol they belong to?

Viva Questions:

- How can Wireshark be used to identify potential attack vectors in a network?
- What are the steps involved in conducting vulnerability analysis using Wireshark?
- Can you explain any specific techniques or methodologies for vulnerability analysis using Wireshark?
- What are some challenges or limitations of using Wireshark for vulnerability analysis?
- How can the findings from Wireshark analysis be used to improve network security?

Post -skill- Task:

1.Document the steps followed to capture network traffic using Wireshark.

Experiment #		Student ID	
Date		Student Name	

\

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

15. Implementation of Web Application Security (Paros)

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of implementing Web Application Security using Paros is to understand and apply security measures to identify and mitigate common vulnerabilities in web applications.

Description:

The implementation of Web Application Security using Paros involves using the Paros Proxy tool to intercept and analyse web application traffic, identify potential security vulnerabilities, and suggest remedial actions. Paros is an open-source web proxy that allows security testers to analyse and modify HTTP and HTTPS traffic between a web browser and a target application.

Pre request:

1. Paros Proxy: It can be downloaded and installed from the official Paros website or other trusted sources.

2. Web browser: Any modern web browser such as Google Chrome, Mozilla Firefox, or Microsoft Edge.

3. Target web application: A web application with known or simulated security vulnerabilities for testing purposes.

Pre Skill:

1. What is the purpose of implementing web application security using Paros?

2. How does Paros Proxy work and what is its role in web application security?

3. What are the key features and functionalities of Paros Proxy?

4. How can Paros Proxy be used to intercept and analyse web application traffic?

5. What are the common security vulnerabilities that can be identified using Paros?

In Lab:

1. Why is it important for penetration testing tools on web applications. and how do you use Paros to validate vulnerabilities reports?

2. Write steps to implement Paros in your Kali Linux?

Viva Questions:

- Explain the process of configuring Paros Proxy to work with a target web application.
- What are some common security measures or actions that can be taken based on the findings from Paros Proxy analysis?
- Can Paros Proxy analyse both HTTP and HTTPS traffic? If yes, how?
- Are there any limitations or challenges in using Paros Proxy for web application security testing?
- How can the results obtained from Paros Proxy be documented and communicated to stakeholders effectively?

Post Skill Task:

1- Describe the process of setting up and configuring Paros for web application security testing.

2- Conduct a comprehensive security assessment of a web application using Paros.

(For Evaluator’s use only)

Comment of the Evaluator (if Any)	Evaluator’s Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

16. Analyse Processing Crime and Incident Scenes

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of this analysis is to develop a comprehensive understanding of the process involved in analysing crime and incident scenes. This includes gaining knowledge of the techniques, methodologies, and Pre request in processing crime scenes to gather evidence and support investigations.

Description:

This analysis focuses on the systematic approach used in processing crime and incident scenes. It covers various aspects such as scene assessment, documentation, evidence collection, and preservation. Additionally, it explores the use of software tools that aid in crime scene analysis and reconstruction. By studying these processes, learners will be equipped with the knowledge and skills necessary to effectively analyse and interpret evidence obtained from crime and incident scenes.

Pre-Requuisites:

1. Crime Scene Management Software: Examples include Crime Scene Investigator (CSI) Tools, iWitnessPRO, or CrimePad.

2. Photogrammetry Software: Examples include Agisoft Metashape, Pix4D, or Autodesk ReCap.

3. Forensic Imaging and Enhancement Software: Examples include Adobe Photoshop, Amped FIVE, or Forensic Image Clarification Suite.

4. 3D Modelling and Reconstruction Software: Examples include FARO Zone 3D, Autodesk 3ds Max, or SketchUp Pro.

5. Evidence Management Software: Examples include EVIDENCEonQ, Tracker Products, or iJustice.

Pre-Skill

1. What are the key steps involved in processing a crime or incident scene?

2. How would you assess and document a crime scene? What are the crucial elements to consider?

3. Describe the importance of evidence collection and preservation at a crime scene.

4. What software tools are commonly used in crime scene analysis, and what are their specific functions?

5. How does photogrammetry software contribute to crime scene analysis and reconstruction?

In-Skill Task

- Study and analyse the steps involved in processing crime and incident scenes.

- Familiarize yourself with the tools and techniques used in evidence collection, preservation, and documentation.

- Participate in mock crime scene simulations to gain hands-on experience in processing different types of scenes.

- Learn about the chain of custody and proper handling of evidence.

Viva Questions

1. Explain the role of forensic imaging and enhancement software in analysing visual evidence.
2. How can 3D modelling and reconstruction software assist in understanding complex crime scenes?
3. What are the challenges associated with using crime scene management software, and how can they be overcome?
4. Discuss the significance of evidence management software in the overall crime scene analysis process.
5. In your opinion, what are the emerging trends or advancements in processing crime and incident scenes, and how might they impact future investigations?

Post-Skill-tasks:

- Prepare a detailed report outlining the various stages of crime and incident scene processing.

- Reflect on the challenges faced during the mock simulations and propose improvements or alternative approaches.

- Discuss the importance of maintaining the integrity of evidence and the potential impact of mishandling it.

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

17. Find Last Connected USB on your system (USB Forensics)

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of studying USB forensics, specifically identifying the last connected USB device on a system, aims to equip students with the skills to extract and analyze digital artifacts such as registry entries, system logs, and event histories to determine recent USB activity. This knowledge enables forensic investigators to reconstruct timelines accurately, understand device interactions, and present findings ethically and legally in digital forensic investigations.

Description:

In USB forensics, the process of identifying the last connected USB device on a system involves examining digital artifacts such as registry entries, system logs, and event logs. These artifacts contain timestamps and details that help forensic analysts reconstruct the sequence of USB device connections, enabling them to establish when and which devices were plugged into or removed from the system. This analysis is crucial for understanding user activity, potential data transfers, and can provide valuable evidence in digital forensic investigations.

Pre request:

In USB forensics, several tools are instrumental for analyzing and extracting information related to USB devices connected to a system. USBDeview from NirSoft is commonly used to list connected USB devices along with their properties and connection timestamps. RegRipper is essential for parsing Windows registry hives to extract USB-related information, such as device connections and historical data. Autopsy, an open-source digital forensics platform, includes modules for analyzing USB artifacts stored in system logs and registry entries. Forensic Toolkit (FTK) offers tools for comprehensive analysis of USB-related artifacts, aiding in identifying device connections and activities.

Pre-Skill:

1. Explain the significance of USB forensics in digital investigations.

2. What types of information can be retrieved from USB artifacts on a system?

3. Describe the steps involved in locating the last connected USB device on a Windows system.

4. How does the registry play a role in USB forensics?

5. Discuss the challenges faced in recovering USB-related artifacts from a system

Experiment #		Student ID	
Date		Student Name	

In-Skill:

1. Implementation to find Last Connected USB on your system (USB Forensics)

Viva Questions

1. What are the potential evidentiary uses of USB forensics in a criminal investigation?
2. Compare and contrast the differences in USB artifact recovery between Windows and macOS systems.
3. Explain the concept of timeline analysis in USB forensics.
4. What tools and techniques are commonly used to extract USB-related data from a system?
5. How can you verify the reliability and accuracy of USB forensic findings in a digital investigation?

Experiment #		Student ID	
Date		Student Name	

Post-Skill-tasks:

1. Modify the Windows Registry to prevent data from being written to a USB storage device.

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

18. View Last Activity of Your PC

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective: The learning objective of viewing the last activity of a PC in digital forensics aims to equip investigators with the skills to reconstruct and analyse the recent actions and events on a computer system. This includes understanding how to examine system logs, event histories, and timestamped artifacts to determine the sequence and nature of user interactions, file accesses, application usage, and network connections. By achieving these objectives, forensic analysts can effectively establish timelines of activities, identify potential security breaches, and gather evidence crucial for investigative purposes.

Description:

In digital forensics, analysing the last activity of a PC involves examining various digital artifacts to reconstruct recent user actions and system events. This includes scrutinizing system logs, event logs, registry entries, and filesystem metadata to pinpoint the timing and nature of activities such as file access, application usage, internet browsing, and device connections. By correlating timestamps and data from these artifacts, forensic analysts can establish a timeline of events leading up to a specific point in time, uncovering crucial information about user behaviour, potential security incidents, or unauthorized access. This process is essential for investigating incidents, identifying relevant evidence, and providing a comprehensive understanding of the digital footprint left on the system.

Prerequisites:

In digital forensics, several tools are essential for analyzing the last activity of a PC, providing capabilities to examine various digital artifacts and reconstruct timelines of events. Tools such as Autopsy, a comprehensive open-source forensic platform, facilitate the analysis of system logs, event logs, and filesystem metadata to identify recent user activities and interactions. The Sleuth Kit, another open-source toolkit, offers utilities like mactime and timeline analysis tools to correlate timestamps and reconstruct chronological sequences of events on the system. Commercial tools like FTK (Forensic Toolkit) provide advanced capabilities for analyzing registry entries, web browsing histories, and application usage logs to uncover detailed insights into the activities performed on the PC. Additionally, tools such as Windows Event Viewer, RegRipper,

Pre-Skill:

1. Explain the importance of analysing the last activity of a PC in digital forensics.

2. What types of digital artifacts are typically examined to determine the last activity on a PC?

3. Describe the steps involved in analysing system logs to identify the last user login and logout times.

4. How can timestamps from filesystem metadata be used to reconstruct a timeline of events on a PC?

5. Discuss the significance of event log analysis in uncovering user actions and system events leading up to a specific incident.

In-Skill tasks:

1. Implementation to View Last Activity of Your PC

Viva Questions

1. Compare and contrast the differences in analysing the last activity of a PC between Windows and macOS systems.
2. What challenges might forensic analysts face when reconstructing timelines of events from disparate digital artifacts?
3. Explain the role of timeline analysis tools, such as mactime, in digital forensics when investigating the last activity of a PC.
4. How can you differentiate between legitimate user activities and suspicious behaviour during the analysis of the last activity on a PC?
5. What are the legal and ethical considerations when presenting findings related to the last activity of a PC in a digital forensic investigation?

Post-Skill-tasks:

1. Mounting a Forensic Image and Scanning It with Anti-virus Software.

Experiment #		Student ID	
Date		Student Name	

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

Experiment #		Student ID	
Date		Student Name	

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

19. Working with Windows and CLI Systems

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective: The learning objective of working with Windows and Command-Line Interface (CLI) systems in digital forensics aims to equip forensic analysts with the skills to effectively navigate and analyse these environments. This includes understanding the structure of Windows filesystems, registry hives, and event logs, as well as proficiency in using CLI commands to gather, analyse, and interpret digital evidence. By achieving these objectives, analysts can conduct thorough investigations, recover critical information, and present findings that adhere to forensic standards and are admissible in legal proceedings.

Description:

In digital forensics, proficiency in working with Windows and Command-Line Interface (CLI) systems is crucial for conducting thorough investigations and extracting valuable evidence. Analysts must navigate Windows filesystems, examining directories, files, and metadata to uncover artifacts relevant to the investigation. Understanding Windows registry structures and utilizing CLI commands enables the extraction of configuration settings, user activities, and system logs crucial for reconstructing timelines of events. This expertise allows forensic analysts to identify malicious activities, unauthorized access, or data breaches, and to present findings accurately in a format suitable for legal proceedings. By mastering these skills, analysts ensure comprehensive analysis of digital evidence, supporting effective resolution of forensic investigations.

Prerequisites

In digital forensics, several tools are essential for working with Windows and Command-Line Interface (CLI) systems to analyze and extract evidence effectively. Forensic tools such as Autopsy and The Sleuth Kit provide GUI and command-line interfaces for examining Windows filesystems, registry hives, and event logs, allowing forensic analysts to recover deleted files, analyze timestamps, and identify user activities. CLI utilities like PowerShell enable scripted analysis and automation of forensic tasks, facilitating bulk data extraction and analysis across Windows systems. Commercial forensic suites such as EnCase and FTK offer comprehensive capabilities for acquiring disk images, parsing filesystem metadata, and analyzing Windows-specific artifacts, ensuring thorough investigation and documentation of digital evidence. These tools collectively enable forensic analysts to navigate Windows environments, uncover critical information, and present findings that are forensically sound and admissible in legal proceedings.

Pre-Skill:

1. Explain the importance of understanding Windows filesystems and registry structures in digital forensics.

2. Describe the process of using CLI commands to gather digital evidence from a Windows system. Provide examples of useful CLI commands for forensic analysis.

3. Compare and contrast the advantages and limitations of GUI-based forensic tools like Autopsy with CLI-based tools such as The Sleuth Kit in digital forensic investigations.

4. How can PowerShell scripts be utilized in digital forensics to automate tasks such as data extraction or analysis of Windows event logs?

5. Discuss the significance of timestamp analysis in Windows forensics. How do timestamps from filesystems and registry entries contribute to establishing timelines of user activities?

In-Skill tasks:

1. Using DART to Export Windows Registry.
2. Examining the SAM Hive

Experiment #		Student ID	
Date		Student Name	

Viva Questions

1. What are the potential challenges faced when conducting digital forensic investigations on Windows systems, and how can these challenges be mitigated?
2. Explain the role of Windows event logs in digital forensics. How can event log analysis assist in reconstructing user actions and system events?
3. Provide examples of Windows-specific artifacts that forensic analysts commonly examine during investigations. How do these artifacts contribute to understanding user behaviour and system interactions?
4. What are the legal considerations when collecting and analysing digital evidence from Windows systems using CLI tools or forensic software?
5. How do forensic analysts ensure the integrity and reliability of findings obtained from Windows systems during a digital forensic investigation?

Post-Skill

1. Examining the SYSTEM Hive

2. Examining the ntuser.dat Registry File

Experiment #		Student ID	
Date		Student Name	

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

20. Live Forensics Case Investigation using Autopsy

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of Live Forensics Case Investigation using Autopsy is to equip participants with the practical skills and theoretical knowledge necessary to effectively conduct live forensic investigations using the Autopsy digital forensics tool. Participants will learn how to respond to real-time incidents, gather volatile data, and analyze live systems while adhering to forensic best practices and legal guidelines. Through hands-on exercises and case studies, participants will develop proficiency in acquiring and preserving evidence, analyzing system memory, and generating comprehensive reports that can withstand legal scrutiny. Ultimately, the course aims to empower participants with the expertise needed to conduct thorough and reliable forensic investigations in dynamic and time-sensitive environments using Autopsy.

Description:

Live Forensics Case Investigation using Autopsy in digital forensics involves the real-time examination and analysis of digital systems and networks to gather volatile data and uncover evidence of security breaches, cybercrimes, or policy violations. Utilizing Autopsy, participants learn to perform live acquisitions of data from running systems, conduct memory analysis to identify active processes and malware, and apply forensic techniques to preserve the integrity of digital evidence. The course emphasizes the importance of maintaining chain of custody, adhering to legal standards, and preparing detailed forensic reports that can be used in legal proceedings. Through hands-on exercises and simulated case scenarios, participants gain practical experience in responding swiftly to incidents, mitigating further risks, and effectively documenting findings for investigative and evidentiary purposes in the field of digital forensics.

Prerequisites

Prerequisites for Live Forensics Case Investigation using Autopsy in digital forensics typically include foundational knowledge in computer operating systems (Windows, Linux, and macOS), networking principles, and basic understanding of digital forensics concepts such as evidence handling, data acquisition methods, and forensic analysis techniques. Participants should have familiarity with file systems, data storage formats, and common types of digital evidence encountered in forensic investigations. Proficiency in using forensic tools and software, including but not limited to Autopsy, is advantageous. Additionally, a solid understanding of legal considerations and chain of custody procedures relevant to digital evidence is essential to ensure compliance with investigative standards and protocols.

Pre-Skill:

1. What is live forensics, and how does it differ from traditional forensic analysis?

2. Describe the process of acquiring volatile data from a live system using Autopsy. What types of information can be gathered in this manner?

3. Explain the significance of conducting memory forensics during a live investigation. How does Autopsy facilitate memory analysis?

4. What are the challenges and considerations involved in conducting live forensics using Autopsy, particularly in terms of preserving evidence integrity and maintaining chain of custody?

5. How does Autopsy assist in analysing network artifacts and connections during a live forensics investigation?

In-Skill tasks:

1. Implementation of Live Forensics Case Investigation using Autopsy

Viva Questions

1. Discuss the role of timestamps and metadata in digital forensics investigations. How does Autopsy handle and utilize this information?
2. What steps should a forensic investigator take when encountering encrypted files or data during a live investigation with Autopsy?
3. Compare the advantages and limitations of using Autopsy for live forensics investigations versus other digital forensic tools available in the market.
4. n what scenarios would live forensics using Autopsy be particularly advantageous compared to traditional post-mortem forensic analysis? Provide examples.
5. How does Autopsy generate and present forensic reports? What elements are typically included in these reports, and how are they used in legal proceedings?

Post-Skill

1. Using Autopsy to search an Image of a Hard Drive
2. Using Autopsy to process a Mac OS X Image

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

21. Implementation of Recovering Deleted files Using Forensic Tools

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of recovering deleted files using forensic tools in digital forensics is to equip participants with the knowledge and skills necessary to retrieve and reconstruct data that has been intentionally or accidentally deleted from storage media. Participants will learn various techniques and methodologies employed by forensic tools to locate and recover deleted files, understand the importance of maintaining data integrity throughout the recovery process, and apply best practices for documenting findings in a forensic report suitable for legal and investigative purposes

Description:

Recovering deleted files using forensic tools in digital forensics involves the systematic retrieval and reconstruction of data that has been intentionally or inadvertently erased from storage devices. This process is crucial in investigations where deleted information may hold critical evidence related to cybercrimes, data breaches, or legal disputes. Forensic tools employ advanced techniques such as file carving, metadata analysis, and disk imaging to locate remnants of deleted files, reconstruct them to their original state, and verify their integrity. Throughout this procedure, stringent adherence to forensic principles ensures that recovered data remains admissible in court, preserving the chain of custody and maintaining the evidentiary value of findings. This capability not only aids in uncovering valuable evidence but also supports the comprehensive analysis and documentation necessary for thorough forensic examinations in digital environments.

Pre request:

Prerequisites for recovering deleted files using forensic tools in digital forensics typically include a solid foundation in computer operating systems such as Windows, Linux, and macOS, as well as knowledge of file systems and data storage principles. Participants should be familiar with basic concepts of digital forensics, including evidence handling procedures, data acquisition methods, and forensic analysis techniques. Proficiency in using forensic tools and software specifically designed for file recovery, such as EnCase, FTK (Forensic Toolkit), or Sleuth Kit/Autopsy, is essential. Additionally, a thorough understanding of legal considerations related to digital evidence, chain of custody protocols, and the ability to interpret metadata and file structures are critical to ensuring the integrity and admissibility of recovered data in legal proceedings.

Pre-Skill:

1. What is file carving and how is it used in recovering deleted files?

2. Explain the difference between logical and physical data recovery methods in digital forensics.

3. How do forensic tools handle fragmented file recovery?

4. What role does metadata play in the recovery of deleted files?

5. How can forensic investigators ensure the integrity of recovered files for legal purposes?

In-Skill tasks:

1. Implementation of Recovering Deleted files Using Forensic Tools

Viva Questions:

1. Compare EnCase, FTK, and Sleuth Kit/Autopsy in recovering deleted files.
2. How do file system journaling and transaction logs impact file recovery?
3. What challenges does file encryption pose to recovering deleted files, and how can they be addressed?
4. Describe the structure and content of a forensic report after recovering deleted files.

5. Discuss the importance of chain of custody in recovering and presenting deleted files as evidence.

Experiment #		Student ID	
Date		Student Name	

Post-Skill-tasks:

1. Recovering Files from Forensic Images with EnCase.

Experiment #		Student ID	
Date		Student Name	

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

22. Extract Browser Artifacts

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of extracting browser artifacts in digital forensics is to equip participants with the knowledge and skills necessary to identify, collect, and analyze digital evidence left behind by web browsers. Participants will learn techniques to extract artifacts such as browsing history, cached files, cookies, and saved passwords from various browsers. Understanding these artifacts aids in reconstructing user activities, determining internet usage patterns, and gathering crucial evidence for investigative and legal purposes in digital forensic examinations.

Description:

Extracting browser artifacts in digital forensics involves the systematic retrieval and analysis of digital evidence left behind by web browsers on computing devices. This process includes identifying and extracting a variety of artifacts such as browsing history, cached files, cookies, download records, autofill data, and bookmarks. These artifacts provide insights into user activities, websites visited, interactions with online services, and potentially malicious activities. Forensic investigators utilize specialized tools and techniques to extract these artifacts while preserving their integrity and ensuring admissibility in legal proceedings. The analysis of browser artifacts is crucial for reconstructing timelines of internet activity, establishing user intent, and uncovering digital footprints that can support investigations into cybercrimes, unauthorized access, and other digital security incidents.

Pre request:

Prerequisites for effectively extracting browser artifacts in digital forensics include a solid understanding of computer operating systems such as Windows, macOS, and Linux, as well as familiarity with various web browsers including Chrome, Firefox, Safari, and Edge. Participants should possess foundational knowledge of digital forensics principles, including data acquisition methods, evidence handling procedures, and forensic analysis techniques specific to browser artifacts. Proficiency in using forensic tools designed for browser artifact extraction, such as Internet Evidence Finder (IEF), Forensic Toolkit (FTK), or Oxygen Forensic Detective, is essential. Additionally, a comprehensive understanding of legal considerations pertaining to digital evidence, including chain of custody and data privacy laws, is crucial to ensure the admissibility of findings in legal proceedings.

Pre-Skill:

1. How do you extract browsing history from different web browsers in digital forensics?

2. Explain the importance of extracting cookies and cache files from web browsers in forensic investigations.

3. What tools are commonly used to extract browser artifacts like bookmarks and download history?

4. How can extracted browser artifacts contribute to reconstructing user activities in digital forensic analysis?

5. Describe the steps involved in preserving the integrity of extracted browser artifacts for legal purposes.

In-Skill tasks:

1. Implementation to Extract Browser Artifacts

Viva Questions:

1. What challenges might forensic investigators face when extracting browser artifacts from encrypted or protected browsing sessions?
2. Compare the extraction methods of browser artifacts between Chrome, Firefox, Safari, and Edge in digital forensics.
3. What do you mean by history available in system and explain its importance
4. What do you mean by cache and explain its uses.
5. What do you mean by cookies and explain its importance

Post-Skill-tasks:

1. Display the browsing history of Web browsers in one table (Analysis of Browser History).

Experiment #		Student ID	
Date		Student Name	

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

Experiment #		Student ID	
Date		Student Name	

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

23. Comparing two Files for forensics investigation by Compare IT software

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of comparing two files using Compare IT software in digital forensics is to identify differences and similarities between files to aid in forensic investigations. This process helps forensic analysts determine if files have been altered, identify specific changes, or confirm authenticity by comparing attributes such as timestamps, file size, and content variations. It enhances the ability to reconstruct events and understand the sequence of actions related to digital evidence.

Description:

In digital forensics, comparing two files using Compare IT software serves as a crucial method to analyse differences and similarities between digital artifacts. This process involves examining various attributes such as file content, metadata, timestamps, and file size to detect alterations or similarities. By highlighting discrepancies or matches between files, Compare IT software enables forensic analysts to reconstruct events, determine if data has been tampered with or modified, and establish the integrity and authenticity of digital evidence. This methodical comparison aids in piecing together timelines, understanding the sequence of actions, and uncovering crucial details necessary for investigative purposes in both criminal and civil cases.

Pre-Requisites:

Before comparing two files using Compare IT software in digital forensics, several prerequisites are essential to ensure accurate and effective analysis. Firstly, a clear understanding of the investigation's scope and objectives is crucial to determine which files need to be compared and why. It's also important to ensure that both files are preserved in their original state to maintain integrity and avoid contamination. Knowledge of the file types and formats involved is necessary to interpret the results correctly, as different formats may require specific handling or considerations during comparison. Additionally, having a working knowledge of Compare IT software itself, including its features, capabilities, and limitations, ensures that forensic analysts can leverage its tools effectively to identify discrepancies, similarities, and other relevant forensic artifacts within the files being examined. These prerequisites collectively support a thorough and reliable comparison process that contributes to the overall investigative integrity in digital forensics.

Pre-Skill:

1. How does Compare IT software help in identifying file alterations during forensic investigations?

2. What are the key attributes Compare IT software compares between two files for digital forensic analysis?

3. Can Compare IT software detect similarities between files of different formats in digital forensics?

4. What precautions should be taken when using Compare IT software for file comparison in forensic investigations?

5. How does Compare IT software contribute to reconstructing timelines in digital forensic investigations?

In-Skill tasks:

1. Implementation of Comparing two Files for forensics investigation by Compare IT software.

Viva Questions:

1. What are the steps involved in using Compare IT software to compare two files for forensic purposes?
2. What are the limitations or challenges of using Compare IT software for file comparison in digital forensics?
3. How can Compare IT software help in reconstructing the sequence of events based on file changes?
4. What are the criteria for selecting files for comparison using Compare IT software in a forensic investigation?
5. What role does Compare IT software play in detecting hidden or embedded data within files during forensic analysis?

Experiment #		Student ID	
Date		Student Name	

Post-Skill-tasks:

1. Creating a Mini-Win FE Boot CD

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT CODE: 22CSB3101A
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

24. Collecting Email Evidence in Victim PC

Date of the Session: ___/___/___ Time of the Session: _____to______

Learning Objective:

The learning objective of collecting email evidence from a victim's PC in digital forensics is to teach investigators how to identify, preserve, and analyze emails and associated metadata effectively. This includes understanding the legal and ethical considerations, maintaining chain of custody, and utilizing specialized tools to extract and interpret email data crucial to investigations and potential legal proceedings.

Description:

Collecting email evidence from a victim's PC in digital forensics involves systematically identifying, acquiring, and analyzing emails and their associated metadata. Investigators follow strict protocols to ensure the integrity and admissibility of evidence, starting with securing the victim's computer to prevent alteration or contamination of data. Using specialized forensic tools, they extract email artifacts, including headers, content, attachments, and timestamps, which are crucial for reconstructing communication timelines and identifying relevant parties involved. Detailed documentation and adherence to legal guidelines are essential throughout the process to support the investigation's findings and potential legal proceedings.

Pre-Requisites:

Prerequisites for collecting email evidence from a victim's PC in digital forensics include a solid understanding of computer systems and networks, proficiency in forensic acquisition techniques to preserve evidence integrity, and knowledge of email protocols and storage formats (e.g., PST, OST, EML). Investigators must be trained in using forensic software tools for acquiring and analyzing email artifacts while adhering to legal and procedural guidelines for evidence handling and chain of custody. Additionally, familiarity with privacy laws and ethical considerations is crucial to ensure compliance and maintain the reliability of collected evidence in investigative and judicial contexts.

Pre-Skill:

1. Discuss in detail about email header.

2. Discuss in detail about prefetch files.

3. What techniques are used to recover deleted emails in digital forensics?

4. What is mobile phone cloning?

5. What are the roles of mobile phones, smartphones, and PDAs in crime

In-Skill tasks:

1. Implementation of Collecting Email Evidence in Victim PC.

Experiment #		Student ID	
Date		Student Name	

Viva Questions:

1. How do you identify and collect email evidence from a suspect's device in digital forensics?
2. What steps are involved in analysing email headers and metadata for investigative purposes?
3. Explain the significance of preserving chain of custody when handling email evidence in digital forensics.
4. How do you differentiate between legitimate and forged email communications during forensic analysis?
5. What legal considerations must be taken into account when presenting email evidence in court?

Post-Skill:

Using OS Forensics to search for Email Messages and Mailboxes

Experiment #		Student ID	
Date		Student Name	

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation
	Marks Secured: ________out of _________ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

SKILL WORKBOOK

(DEEMED TO BE UNIVERSITY)

KONERU LAKSHMAIAH EDUCATION FOUNDATION,
GREEN FIELDS, VADDESWARAM,
GUNTUR-522502

www.kluniversity.in

CATEGORY 1 UNIVERSITY
BY MHRD, Govt. of India

KL ACCREDITED BY NAAC WITH A++ GRADE

nirf 2023 NATIONAL INSTITUTIONAL RANKING FRAMEWORK RANKED 28 AMONG ALL UNIVERSITIES

43 YEARS OF EDUCATIONAL LEADERSHIP