

# Technical Workshop Report: Cyber Security and Ethical Hacking

**Date:** 16th and 17th October 2023

**Venue:** DBMS Lab, Department of Computer Science and Engineering, AIET

**Resource Person:** Mr. Samarth Bhaskar Bhat, Reverse Engineering Infosec, Bengaluru

**Collaboration:** IEEE Student Chapter, AIET

The Technical Workshop on Cyber Security and Ethical Hacking, organized by "C maniax" Department of Computer Science and Engineering, AIET, in collaboration with the IEEE Student Chapter, was successfully conducted on 16th and 17th October 2023. The workshop was held in the DBMS Lab.

The event commenced with an inaugural ceremony where the Head of Department, Dr. Manjunath Kothari, delivered a presidential address. Chief Guest, Mr. Samarth Bhaskar Bhat from Reverse Engineering Infosec, Bengaluru, addressed the gathering. Dr. Aslam B Nandyal, Forum Coordinator of "C maniax," expressed gratitude through the vote of thanks. The inauguration ceremony also witnessed the presence of members from the IEEE Student Chapter.





During the workshop, Mr. Samarth Bhaskar Bhat covered various essential topics related to ethical hacking, including the usage of Kali Linux and other related tools. Participants gained valuable insights into the world of cyber security and explored the techniques and practices of ethical hacking. The workshop was a great success, providing students with practical knowledge and hands-on experience in the field of cyber security. The collaborative effort of "C maniax" Department of Computer Science and Engineering and the IEEE Student Chapter enhanced the overall learning experience. We extend our sincere thanks to Mr. Samarth Bhaskar Bhat for



sharing his expertise and making the event a memorable one.

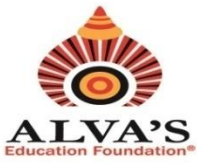
The Session wise content details have been provided below.

<ul style="list-style-type: none"><li>- Introduction to Cyber Security &amp; Ethical hacking</li><li>- Misconceptions of Hacking</li><li>- Reason why everything can be hacked?</li><li>- Why is Cyber Security Essential?</li></ul>	2 Hours
<ul style="list-style-type: none"><li>- What are the skills required for cyber security profession?</li><li>- Top industrial Certifications</li><li>- How to bridge the gap between campus and company placements?</li><li>- How to start with Cyber security?</li><li>- What is a CTF competition?</li><li>- Applications of cyber security</li></ul>	2 Hours

<ul style="list-style-type: none"><li>- What is Vulnerability Assessment?</li><li>- How can we find vulnerabilities?</li><li>- VAPT Approach</li><li>- Internal / External Tests</li></ul>	2 Hours
--	---------




<ul style="list-style-type: none"><li>- Hands on session on solving various basic CTF challenges.</li><li>- Machine 1 – sunset</li><li>- Machine 2 – dina</li><li>- Machine 3 – Mhz</li></ul>	2 Hours
<ul style="list-style-type: none"><li>- Machine 4 – lazysysadmin</li><li>- Machine 5 – covefefe</li><li>- Machine 6 – basic pentesting</li></ul>	2 Hours
<ul style="list-style-type: none"><li>- What is Digital Forensics?</li><li>- Need for Digital forensics</li><li>- Forensics Categorization</li></ul>	2 Hours



**Alva's Institute of Engineering & Technology**  
**Shobhavana Campus, Mijar, Moodbidri, D.K – 574225**  
**Phone: 08258-262725, Fax: 08258-262726**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**  
**(Accredited by NBA, New Delhi 2019-2022)**

This workshop was a stepping stone towards enriching the participants' understanding of the growing field of cyber security. We express our gratitude to all the participants and look forward to organizing similar events in the future to continue fostering knowledge and skills in this domain.

  
**Head of the Department**  
**Dept. of Computer Science & Engineering**  
**Alva's Institute of Engineering and Technology**  
**Mijar, Moodubidri - 574 225, D.K. Karnataka, India**

## **STUDENT INTERACTION, SESSION ON CYBER SECURITY, AWS SECURITY AND PLACEMENT GUIDANCE IN CISO OF RAZORPAY**

**Resource person: Mr Hilal Ahmad Lone, Chief Information Security Officer**

**Date:09/03/2024**

**Time:10:00AM-1:00PM**

In a third week of training there was a interactive session with chief information security officer,CISO of Razorpay.

This report provides session covered by chief information security officer, CISO of Razorpay on 09/03/2024 at 10:00am-1:00pm in DBMS Lab .They explained about

- Overview on cybersecurity
- Cybersecurity path and how to enter into Cybersecurity
- Cloud security
- Cybersecurity aspects in AWS
- Question and answer session
- Feedback and interaction with students regarding CSFS curriculum



Sir explained about cyber security path start by understanding the fundamentals of cyber security, including basic networking concepts, operating systems, and security principles. Pursue formal education or certifications such as CompTIA Security+, Certified Information Systems Security Professional (CISSP), or Certified Ethical Hacker (CEH) depending on your interest and career goals. Cyber security is a vast field. Choose a specialization based on your interests such as network security, cloud security, application security, etc. Consider pursuing advanced certifications such as Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), or Offensive Security Certified Professional (OSCP) as you progress in your career.





Familiarize yourself with the various services offered by AWS and their respective security implications. This includes compute, storage, networking, and database services. Understand the shared responsibility model of AWS, where AWS is responsible for the security of the cloud infrastructure, while customers are responsible for securing their data and applications in the cloud. Implement encryption mechanisms for data at rest and in transit using AWS Key Management Service (KMS), AWS Certificate Manager (ACM), and other encryption features provided by AWS. Utilize AWS CloudTrail for logging API activity and AWS CloudWatch for monitoring and alerting on AWS resources. Implement AWS Config to assess and audit the configuration of AWS resources.



In AWS, cybersecurity encompasses a wide range of aspects to ensure the protection of data, applications, and infrastructure hosted on the AWS platform. Here are some key cybersecurity aspects in AWS:

- **Identity and Access Management (IAM):** IAM enables you to manage user identities, roles, and permissions within your AWS environment.
- **Data Encryption:** AWS offers various encryption services to protect data both at rest and in transit. Amazon S3 provides server-side encryption to encrypt data stored in S3 buckets, while AWS Key Management Service (KMS) allows you to manage encryption keys securely.
- **Network Security:** AWS provides tools to secure your network infrastructure, such as security groups and network access control lists (NACLs) to control inbound and outbound traffic. AWS Virtual Private Cloud (VPC) enables you to create isolated network environments with customizable routing, subnets, and access controls.
- **Logging and Monitoring:** AWS CloudTrail records API activity within your AWS account, providing visibility into actions taken by users, applications, and services. AWS CloudWatch allows you to monitor metrics, set alarms, and collect logs for AWS resources, helping you detect and respond to security incidents in real-time.

- **Compliance and Governance:** AWS adheres to various compliance standards and provides services to help customers achieve compliance with regulations such as HIPAA, GDPR, PCI DSS, etc. AWS Config enables continuous monitoring and assessment of resource configurations for compliance purposes.
- **Incident Response:** AWS provides services like AWS Shield for DDoS protection and AWS WAF (Web Application Firewall) to protect against common web exploits. Additionally, AWS offers incident response services and resources to help customers effectively respond to security incidents.
- **Security Best Practices:** Following security best practices recommended by AWS is essential for maintaining a secure environment. This includes regularly applying security patches, using multi-factor authentication (MFA), implementing strong password policies, and regularly auditing and monitoring your AWS environment.
- **Security Automation:** AWS offers services like AWS Security Hub and AWS GuardDuty, which use machine learning algorithms to analyze logs and detect security threats automatically. These services help in identifying potential security issues and streamline incident response processes.

By focusing on these cybersecurity aspects and leveraging the security features and services provided by AWS, organizations can build and maintain a robust security posture in their AWS environments.





As a token of love Dr.Manjunath Kotari,Hod of computer science and engineering AIET, Moodabidri gave memento to our resource person.

The session ended up with the interaction of 50 participants of cyber security finishing school.

*A. K. L.*

Club coordinator

*H. O. D.*

HOD H.O.D.  
Dept. Of Computer Science & Engineering  
Alva's Institute of Engrg. & Technology  
Mijar, MOODABIDRI - 574 225



## Report on Cyber Security Finishing School (CSFS)

Alva's Institute of Engineering and Technology, Moodbidri and CySecK(Cyber Security Karnataka), Govt. of Karnataka, in association with Trishaka Foundations, Chennai organized a "Cyber Security Finishing School (CSFS)"- a pilot program on CSFS training for B.E Final year students of all the Engineering students of Karnataka. A 35 days of training program is held between 19<sup>th</sup> February to 22<sup>nd</sup> March,2024 at Alva's Institute of Engineering & Technology, Moodbidri Campus.

The inauguration of CSFS training program was held on 19<sup>th</sup> February, 2024 Mr. Praveen Castelino, Co-Founder & CTO, Code Craft Technologies, Mangalore was the Chief Guest of the program. After lighting the lamp Mr. Praveen Castelino said that " Now a days people are not aware about the importance of severity of cyber-attacks happed to them. Majority of them use to hide the incidents due to the reputation & most them will end their life due the cyber attack incidents because which is attacked to their personal. He added that, people need to take care while keep posting pictures in the Social Media."

After the Inauguration **CySecK Centre Head, Mr. Karthik Rao R** said that " We are started with a pilot program of Finishing School and he told that scale this program to bigger level in the future. He acknowledge the AIET for the taking this initiation"

In the presidential address Mr.Vivek Alva said that "Most of the Social Media accounts are fake and keep posting wrong informations. People use to pass these informations to the others and finally wrong thing will become the truth of the life. So He told that, always keep verify the contents before forwarding anything to others. Most of the cyber attackers are less sensitive about life and reputations of the people."

Dr.Manjunath Kotari, Professor & Head-CSE, Alva's Institute of Engineering & Technology, "Gave the statistics of the Cyber Attacks in the India & World. He also highlighted about the 35 days of CSFS Training program".

Cyber Security Club Coordinator of AIET, Moodbidri Mrs.Deepika Kamath welcome the gathering. Mrs Deeksha M & Mrs. Vidya introduced the guests to the audience. Ms. Bhagshree proposed the vote of thanks.

Program Director of Trishakha Foundation Mr.Mohan Ram, Principal AIET, Dr.Peter Fernandes, Cyber Security Engineers Mr Vineeth Shetty and Mr.Kaushik, CySecK , Banaglore also present.

## Cyber Security Finishing School (CSFS) has the following features:

- 1) The CSFS training program focusing on following major areas of cyber security
  - a. Foundations of Cyber Security
  - b. Cloud Security
  - c. Cyber Threat Intelligence
  - d. Malware Analysis
  - e. Secure System Operations
- 2) The CSFS is a **full-time residential specialized training programme** aimed at improving the Cyber Security skills and employability of Engineering (B.E./B.Tech.) graduates who are about to enter the job market.
- 3) Only full-time final-year B.E./B.Tech. students who are interested in pursuing a career in Cyber Security are considered for enrolment with no restrictions on their branch of study.
- 4) Since it is a pilot program for CSFS, the troop size was limited to 50 participants.
- 5) The CSFS is structured as a **five-week long training programme (19<sup>th</sup> Feb to 22<sup>nd</sup> March)** covering 40 hours of training per week on each of the above-mentioned sub-domains of Cyber Security, giving a **total of 200 hours of training spread over the five weeks**.
- 6) Every weekend there will be a assessment by senior information security officer(SISO) of various organizations.

Out of 50 participants, the students from following colleges got selected for the CSFS training.

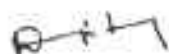
- Acharya Institute of Technology, Bangalore -7 students
- Sharanabasva University, Kalburgi-4 students
- Govt. Sri Krishnarajendra Silver Jubilee Technological Institute, Bangalore(Govt SKSJT)-3 students
- IIIT Raichur-2 students
- Appa Institute of Engineering and Technology, Gulbarga -2 students
- Reva University, Bangalore-1 student
- M S Ramaiah Institute of Technology, Bangalore -1 student
- Amrita School of Engineering, Bangalore -1 student
- Bangalore Institute of Technology, Bangalore -1 student
- Dayananda Sagar College of Engineering, , Bangalore -1 student
- Jain Institute of Technology, Davangere -1 student
- Sambhram Institute of Technology, Bangalore-1 student
- Alva's Institute of Engineering & Technology, Moodbidri -25 students







The session ended up with the interaction of 50 participants of cyber security finishing school.



Club coordinator



HOD, O. D.

Dept. Of Computer Science & Engineering  
Alva's Institute of Engn. & Technology  
Mijar, MOODBIDRI - 574 225



# **ALVA'S INSTITUTE OF ENGINEERING & TECHNOLOGY**

(A Unit of Alva's Education Foundation(R), Moodubidire)

Affiliated to Visvesvaraya Technological University, Belagavi,

Approved by AICTE, New Delhi, Recognized by Govt. of Karnataka.

**Accredited by NAAC with A+ & NBA (ECE & CSE)**

Shobhavana Campus, MIJAR-574225, Moodubidire, D. K., Karnataka



## **CYBERSECURITY CLUB**

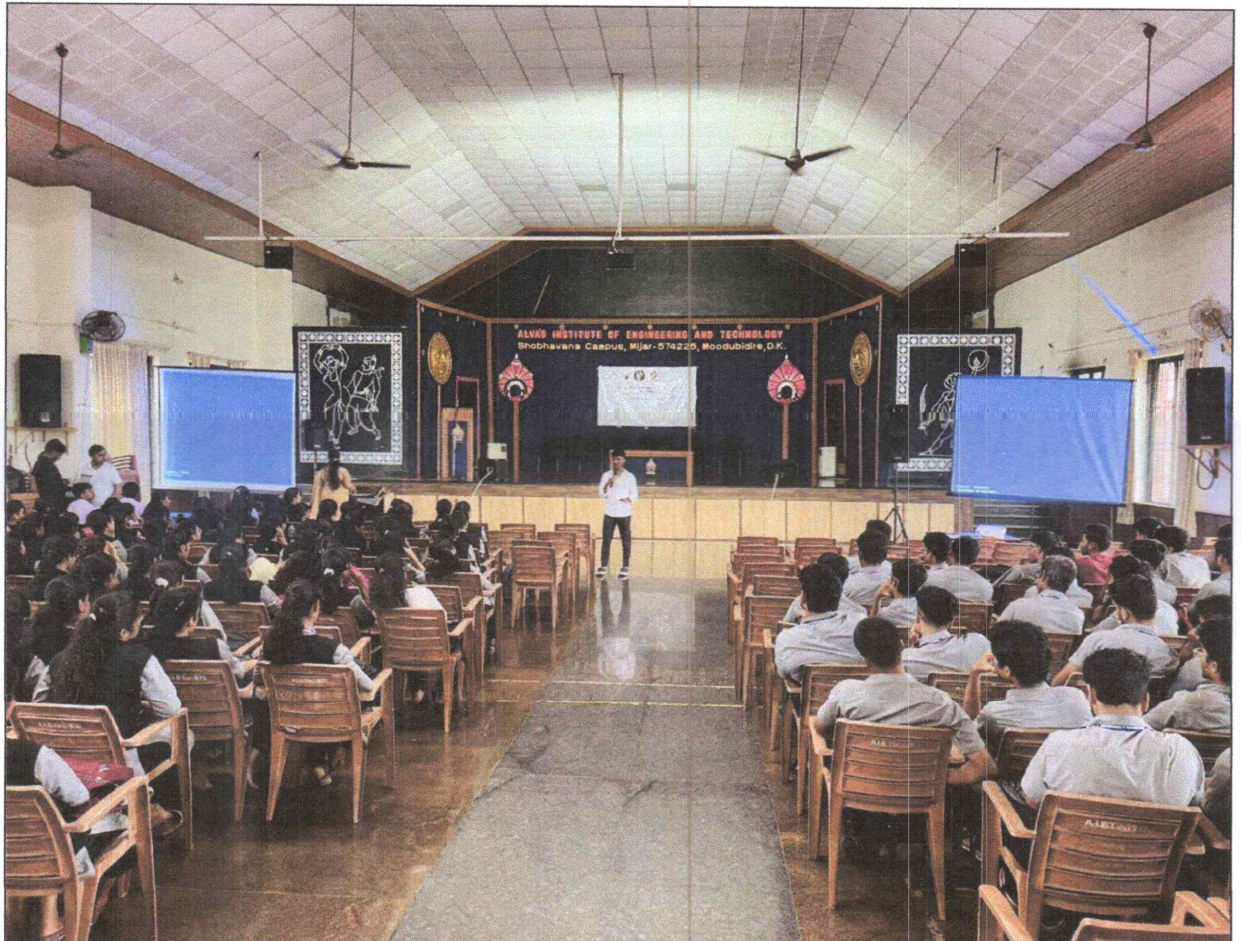
**REPORT ON:**

**“Cyber Awareness and Internet Safety”**



## 1. Introduction

On 4<sup>th</sup> July, 2024, the members of cybersecurity club conducted a comprehensive session on "Cyber Awareness and Internet Safety." The session aimed to educate participants on the importance of cyber awareness, the potential threats in the digital world, and practical steps to ensure internet safety. The event was part of our ongoing initiative to empower individuals with the knowledge and skills necessary to navigate the cyber landscape securely.



## 2. Objectives

The primary objectives of the session were:

1. To raise awareness about common cyber threats and vulnerabilities.
2. To educate participants on best practices for online safety.
3. To provide practical tips for securing personal and professional data.
4. To promote responsible digital behaviour.



### 3. Key Topics Covered

#### 1. Introduction to Cybersecurity

- Overview of cybersecurity and its significance in today's digital age.
- Explanation of common cyber threats such as phishing, malware, and ransom ware.

#### 2. Understanding Cyber Threats

- Detailed discussion on various types of cyber threats.
- Real-life examples and case studies to illustrate the impact of cyber-attacks.

#### 3. Best Practices for Internet Safety

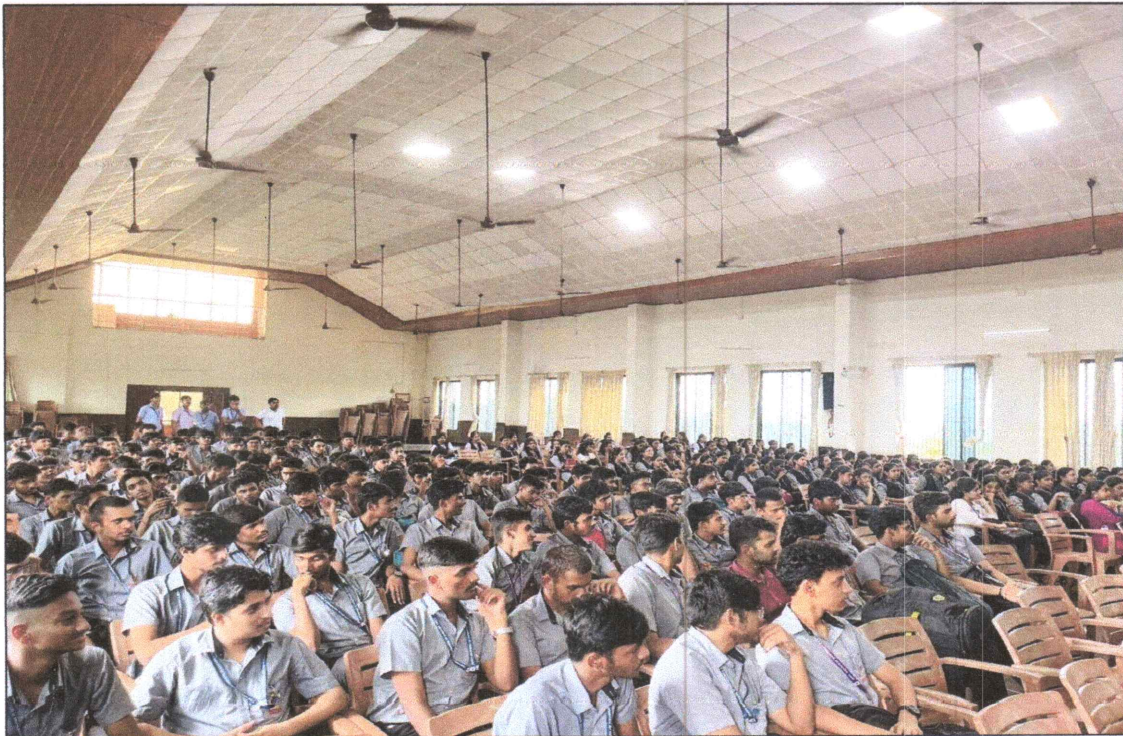
- Tips for creating strong passwords and using password managers.
- Importance of keeping software and systems updated.
- Guidelines for safe browsing and recognizing suspicious links.

#### 4. Protecting Personal Information

- Strategies for safeguarding personal information online.
- Importance of privacy settings on social media platforms.
- Tips for secure online transactions.

#### 5. Responding to Cyber Incidents

- Steps to take if you suspect a cyber-attack.
- Importance of reporting incidents to relevant authorities.
- Basic incident response plan for individuals and organizations.





## 4. Interactive Activities

To ensure active participation and better understanding, the session included several interactive activities:

- **Quiz on Cybersecurity Basics:** A quick quiz to test participants' knowledge and reinforce key concepts.
- **Phishing Simulation:** A demonstration on identifying phishing emails and avoiding scams.
- **Password Strength Workshop:** A hands-on activity to create and test strong passwords using tools like password managers.



## 5. Feedback and Evaluation

The session received positive feedback from participants. Many expressed that they found the information valuable and applicable to their daily online activities. Key points of feedback included:

- Appreciation for the real-life examples and practical tips.
- Interest in more advanced topics and in-depth workshops on specific cybersecurity areas.
- Requests for follow-up sessions and resources for further learning.



## 6. Conclusion

The "Cyber Awareness and Internet Safety" session was a significant step in our mission to empower individuals with cybersecurity knowledge. The enthusiastic participation and positive feedback from attendees highlight the importance and relevance of such initiatives. Moving forward, we plan to conduct more in-depth workshops and create additional resources to support our community's journey towards a safer digital experience.



## 7. Future Plans

Based on the feedback received, our future plans include:

- Organizing advanced cybersecurity workshops.
- Developing online resources and tutorials.
- Collaborating with schools, colleges, and organizations to expand our outreach.

By Sujay Adoor

Student Coordinator, Cyber Security Club

A handwritten signature in black ink, appearing to be 'Sujay Adoor'.

Club Coordinator

A handwritten signature in black ink, appearing to be 'Sujay Adoor'.

Head of the Department  
Dept. of Computer Science & Engineering  
Alva's Institute of Engineering and Technology  
Mijar, Moodubidire - 574 225, D.K. K. Prataka, India

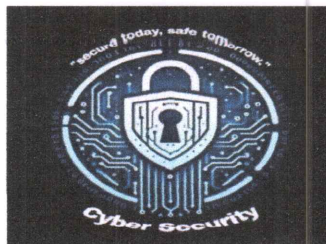
**ALVA'S INSTITUTE OF ENGINEERING & TECHNOLOGY**  
(A Unit of Alva's Education Foundation(R), Moodubidire) Affiliated to Visvesvaraya  
Technological University, Belagavi,  
Approved by AICTE, New Delhi, Recognized by Govt. of Karnataka.  
Accredited by NAAC with A+ & NBA (ECE & CSE)  
Shobhavana Campus, MIJAR-574225, Moodubidire, D. K., Karnataka



## **CYBER SECURITY CLUB**

**REPORT ON:**

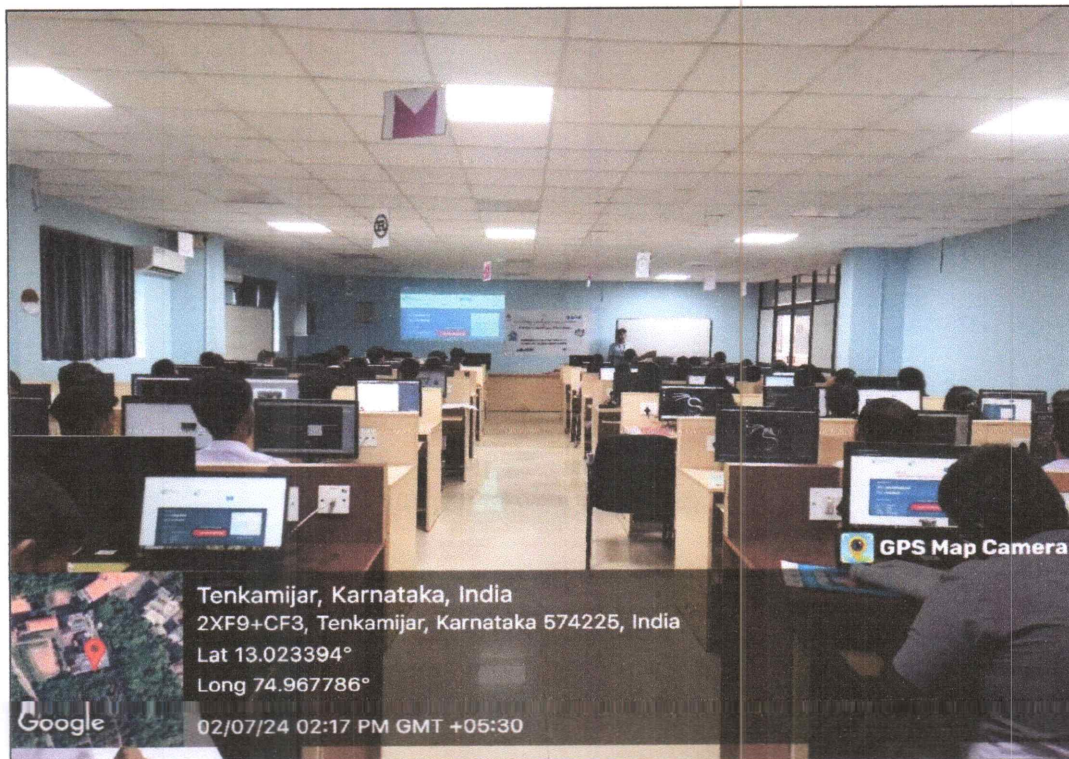
**“HANDS ON SESSION FOR 2<sup>nd</sup> YEAR IOT STUDENTS”**





## Introduction

Cybersecurity is a critical field in today's digital age, encompassing measures to protect systems, networks, and data from malicious attacks. Practical exercises are essential for cybersecurity professionals to develop skills in identifying vulnerabilities, assessing risks, and implementing effective defenses. This report aims to explore various cybersecurity tools and techniques using Kali Linux, a widely used distribution for penetration testing and security auditing.



## Installation and Basic Linux Commands

### Installation of Kali Linux

Installing Kali Linux involves several steps to set up a virtual machine or install it directly on hardware. The process typically includes downloading the ISO image, creating a bootable USB drive or DVD, and following installation prompts to configure the operating system.

### Basic Linux Commands

Understanding basic Linux commands is crucial for navigating the operating system and performing tasks efficiently. Commands such as `ls` (list directory contents), `cd` (change directory), `mkdir` (make directory), `rm` (remove files or directories), `cp` (copy files), `mv` (move files), and `grep` (search for patterns within files) are fundamental for day-to-day operations and cybersecurity tasks.





## Network Scanning with Nmap (Zenmap)

### Methodology

Nmap, a powerful network scanning tool, and Zenmap, its graphical interface, are used to conduct network reconnaissance. Techniques such as ping scanning, port scanning (TCP SYN scan, UDP scan), OS detection, and service version detection are employed to gather information about active hosts, open ports, running services, and potentially vulnerable systems.

### Findings

The results of network scans provide insights into the network's topology, the services exposed to the internet, and potential security vulnerabilities. Identifying outdated services or open ports can help prioritize security patches and configurations to reduce attack surfaces.

### Conclusion

Network scanning is a foundational step in cybersecurity assessments, aiding in identifying potential entry points for attackers and guiding defensive strategies such as firewall configurations and network segmentation.



## **Phishing Simulations**

### **Tools Used**

Google's G Suite, LUCY, and GoPhish are commonly used tools for creating and executing phishing simulations. These tools allow cybersecurity professionals to craft convincing phishing emails and track user interactions without causing harm.

### **Methodology**

Phishing simulations involve designing email templates that mimic legitimate communications, configuring landing pages to capture credentials or other sensitive information, and analyzing user responses to gauge susceptibility to phishing attacks.

### **Outcome**

Analysis of phishing simulation results provides insights into organizational susceptibility to social engineering attacks. Metrics such as click-through rates, submission of credentials on phishing pages, and employee awareness levels are evaluated to tailor cybersecurity awareness training and enhance defenses.

### **Conclusion**

Phishing remains a prevalent threat vector, emphasizing the need for continuous training and awareness programs to educate users about identifying and mitigating phishing attempts.

## **Packet Analysis using Wireshark**

### **Installation**

Wireshark, a popular packet analysis tool, is installed on Kali Linux to capture and analyze network traffic. Configuration settings for capturing packets from specific interfaces or applying filters to focus on relevant traffic are configured.

### **Methodology**

Capturing packets involves monitoring network traffic in real-time or analyzing saved packet captures. Protocols such as TCP and UDP are dissected to examine packet headers, payloads, and interactions between network nodes.

**Findings**

Packet analysis reveals valuable insights into network behavior, including data transfers, protocol anomalies, and potential security threats such as unauthorized access attempts or data exfiltration.

**Conclusion**

Wireshark facilitates proactive network monitoring and troubleshooting, enabling cybersecurity professionals to detect and respond to network anomalies and security incidents effectively.

**Ransomware Tabletop Exercise****Scenario**

Designing a tabletop exercise involves creating a hypothetical ransomware attack scenario initiated by an insider threat. Participants simulate their roles and responses to the ransomware incident, focusing on containment, eradication, and recovery strategies.

**Methodology**

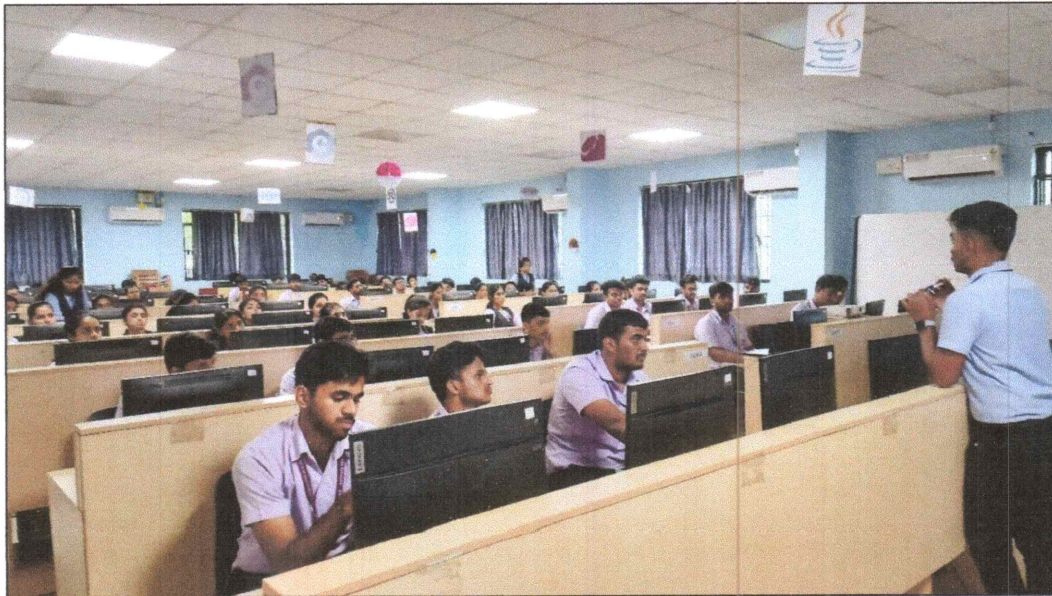
The tabletop exercise unfolds through scenario-based discussions, decision-making processes, and coordination among stakeholders. Response plans and incident response procedures are evaluated for effectiveness and adaptability in mitigating ransomware attacks.

**Outcome**

Lessons learned from the tabletop exercise inform improvements in incident response capabilities, including updating backup strategies, enhancing endpoint security controls, and refining communication protocols during ransomware incidents.

**Conclusion**

Tabletop exercises are invaluable for rehearsing incident response plans and fostering collaboration across organizational departments to mitigate the impact of ransomware attacks effectively.



## **SQL Injection with BurpSuite**

### **Methodology**

BurpSuite, an integrated platform for web application security testing, is used to simulate SQL injection attacks against vulnerable web applications. Techniques such as SQL payload injection, error-based SQL injection, and blind SQL injection are employed to exploit database vulnerabilities.

### **Findings**

Identifying vulnerable SQL injection points and exploiting them to extract sensitive information or modify database entries highlights the critical importance of secure coding practices and robust input validation mechanisms.

### **Conclusion**

SQL injection vulnerabilities pose significant risks to web application security, underscoring the need for comprehensive security testing and proactive vulnerability management strategies.

## **Packet Analysis with Wireshark and Tcpdump**

### **Installation and Setup**

Wireshark and Tcpdump are installed and configured on Kali Linux to capture and analyze UDP/TCP datagrams exchanged in client-server communications. Packet filters and display filters are utilized to focus on specific protocols or network interactions.



## Methodology

Capturing and analyzing UDP/TCP datagrams involve inspecting packet headers, payloads, and sequence numbers to understand data flows, identify communication patterns, and detect anomalies indicative of potential security threats.

## Findings

Observations from packet analysis provide insights into network performance, protocol compliance, and security posture. Identifying suspicious activities or unauthorized data transfers helps strengthen network defenses and mitigate risks.

## Conclusion

Wireshark and Tcpcdump serve as indispensable tools for network administrators and cybersecurity professionals, facilitating comprehensive packet analysis and effective incident response capabilities.




## Conclusion

In conclusion, the practical exercises conducted using Kali Linux and various cybersecurity tools demonstrate the importance of hands-on training in developing technical skills and enhancing cybersecurity awareness. Each exercise contributes valuable insights into network reconnaissance, social engineering defenses, packet analysis techniques, and web application security practices. Recommendations for ongoing training, threat intelligence integration, and incident response preparedness are essential for maintaining robust cybersecurity defenses in today's evolving threat landscape.



**Students:**

- |                       |            |
|-----------------------|------------|
| 1. Sujaykumar B Adoor | 4AL21CG057 |
| 2. Manoj M            | 4AL21CG036 |
| 3. Sharvari M S       | 4AL21CG049 |
| 4. Chandana N M       | 4AL21IS064 |
| 5. Vinith Kalikar     | 4AL21CG062 |

  
**Club Coordinator**  
**HOD**  
**Head of the Department**  
**Dept. of Computer Science & Engineering**  
**Alva's Institute of Engineering and Technology**  
Mijar, Moodubidire - 574 225, D.K. Karnataka, India