**DAILY DIARY NIKHIL RANA 2302727**

**Industrial Training on Cyber Security**

## WEEK 1: INTRODUCTION TO CYBERSECURITY & SOCIAL ENGINEERING

### Day 1

The first day of industrial training began with an orientation session where the objectives, duration, and expected outcomes of the training were explained. An overview of cybersecurity was provided, highlighting its importance in protecting data, systems, and networks. The concept of ethical hacking and the responsibility of cybersecurity professionals were discussed to ensure legal and ethical compliance throughout the training.

### Day 2

This day focused on the fundamentals of cybersecurity. Topics such as confidentiality, integrity, and availability (CIA Triad) were explained in detail. Real-world examples of cyberattacks were discussed to understand how security breaches impact individuals and organizations. The increasing role of cybersecurity in today's digital world was emphasized.

### Day 3

An introduction to social engineering was given. Various manipulation techniques used by attackers to exploit human behavior were explained. The session covered phishing, vishing, smishing, baiting, and impersonation attacks. The psychological aspects behind these attacks, such as trust and urgency, were also discussed.

### Day 4

The social engineering attack lifecycle was studied in detail. Steps such as information gathering, building trust, exploiting vulnerabilities, and disengagement were explained. The importance of understanding human behavior in preventing social engineering attacks was highlighted through case studies.

### Day 5

The week concluded with a discussion on defensive strategies against social engineering attacks. User awareness, strong password policies, and multi-factor authentication were explained. Ethical considerations and the importance of user consent during cybersecurity testing were also reinforced.

## WEEK 2: LINUX & ENVIRONMENT SETUP

### Day 6

The basics of the Linux operating system were introduced. The role of Linux in cybersecurity and ethical hacking was discussed. Students learned about different Linux distributions and why Kali Linux is widely used for penetration testing.

**Day 7**

Hands-on practice with Linux commands was conducted. Commands related to file handling, directory navigation, permissions, and system monitoring were practiced. This session helped build confidence in working with the Linux terminal.

**Day 8**

Kali Linux installation using Oracle VirtualBox was performed. System requirements, virtual machine configuration, and network settings were discussed. The importance of using virtual machines for safe and isolated testing was emphasized.

**Day 9**

Post-installation configuration of Kali Linux was carried out. System updates and upgrades were performed to ensure compatibility with cybersecurity tools. The importance of keeping systems updated to avoid vulnerabilities was explained.

**Day 10**

Essential tools such as Git, Python, PHP, Ngrok, and ADB were installed. Their roles in phishing simulations and device testing were discussed. The week ended with a review of environment setup and troubleshooting common issues.

**WEEK 3: CAMPHISH TOOL PRACTICAL**

**Day 11**

The Camphish tool was introduced. Its purpose in simulating camera-based phishing attacks was explained. The ethical use of Camphish for awareness and training purposes was emphasized.

**Day 12**

Camphish was installed by cloning the repository from GitHub. Required permissions were granted, and dependencies were verified. The internal structure of the tool was explored to understand its working.

**Day 13**

Ngrok and Cloudflare tunneling options were studied. The role of tunneling in generating public URLs for phishing simulations was explained. Differences between Ngrok and Cloudflare were analyzed.

**Day 14**

Festival Wishing phishing template was executed. The simulation demonstrated how attackers trick users into granting camera permissions. Captured information such as IP address and device details was analyzed.

**Day 15**

Live YouTube TV phishing template was tested. User behavior during permission requests was observed. Defensive insights were discussed, highlighting the importance of verifying links before granting permissions.

**WEEK 4: ADVANCED CAMPHISH & RUBIKPHISH**

**Day 16**

The Online Meeting phishing template in Camphish was explored. The simulation showed how attackers exploit remote work culture. Preventive measures against such attacks were discussed.

**Day 17**

A detailed analysis of Camphish results was conducted. Ethical boundaries of phishing simulations were reinforced. The importance of cybersecurity awareness training was emphasized.

**Day 18**

Introduction to Rubikphish tool was provided. Its role in simulating credential harvesting attacks was explained. Various phishing templates available in Rubikphish were explored.

**Day 19**

Rubikphish installation and setup were performed. Permissions and dependencies were configured properly. The interface of Rubikphish was studied in detail.

**Day 20**

Facebook phishing template was selected and executed. Credential capture process was observed in real time. Defensive strategies such as URL verification and MFA were discussed.

**WEEK 5: PHONESPLOIT & DEVICE SECURITY**

**Day 21**

Introduction to PhoneSploit tool and Android exploitation concepts was given. The role of ADB in device communication was explained.

**Day 22**

ADB was installed and PhoneSploit-Pro repository was cloned. Test Android devices were prepared by enabling developer options and USB debugging.

**Day 23**

PhoneSploit was executed to retrieve device information. Screenshots and system details were captured for analysis. The risks of unsecured Android devices were discussed.

**Day 24**

Device shell access and command execution were tested in a controlled environment. The importance of disabling USB debugging after use was emphasized.

**Day 25**

Ethical considerations related to device exploitation were discussed. All testing was reviewed to ensure it followed legal and ethical guidelines.

**WEEK 6: EVALUATION, CONCLUSION & DOCUMENTATION**

**Day 26**

Evaluation of training activities was conducted. The effectiveness of phishing tools and simulations was analyzed.

**Day 27**

Results obtained during training were discussed. The role of user awareness in preventing cyberattacks was emphasized.

**Day 28**

Mitigation techniques such as security policies, incident response planning, and awareness programs were studied.

**Day 29**

Documentation work for the training report and daily diary was completed. Formatting and structuring as per university guidelines were reviewed.

**Day 30**

The training concluded with a summary of learnings. Practical exposure to social engineering, phishing simulations, and ethical hacking strengthened understanding of real-world cybersecurity challenges and future career opportunities.