JSPM's Rajarshi Shahu College of Engineering
An Empowered Autonomous Institute Affiliated to Savitribai Phule Pune University, Approved by AICTE,
Accredited by NBA (UG Programs), Accredited by NAAC With "A" Grade
MHRD-NIRF Rank:151-200

Cybersecurity Workshop Report

Organized By

Microsoft CyberShikshaa

Institution: JSPM's Rajarshi Shahu College of Engineering

Trainer: Pranay Kadam

Workshop Duration: 10 Days (70 Hours)

10th Dec to 20th Dec 2024

9 am to 5 pm

Students Count:76

Workshop Report on Cybersecurity Training (Stage 3)

1. Introduction The cybersecurity training workshop (Stage 3) was conducted as part of the Microsoft Cyber Shikshaa initiative at JSPMS Rajarshi Shahu College of Engineering. This workshop aimed to provide in-depth knowledge and hands-on experience in various cybersecurity concepts, techniques, and tools. The training was structured into multiple sessions, each covering critical aspects of cybersecurity, such as network security threats, firewalls, and countermeasures.

2. Objectives of the Workshop The primary objectives of this workshop were:

- To familiarize participants with various cybersecurity threats and vulnerabilities.
- To introduce network security measures, including different types of firewalls.
- To enhance participants' skills in implementing cybersecurity practices through hands-on exercises.
- To provide insights into best practices for securing information systems.

3. Workshop Structure and Methodology The workshop was designed to provide a mix of theoretical concepts and practical exposure. The following methodologies were employed:

- **Lectures:** Detailed explanations of cybersecurity concepts.
- **Demonstrations:** Live demonstrations of security tools and techniques.
- **Hands-on Sessions:** Practical exercises to reinforce learning.
- **Case Studies:** Real-world examples to highlight best practices.
- **Interactive Discussions:** Q&A sessions to address participants' queries.

4. Session Breakdown The workshop was divided into multiple sessions, each focusing on specific cybersecurity topics. Some key sessions included:

- **Session 1: Network Security Threats and Countermeasures**
    - **Overview of Network Threats:** Understanding different types of cyber threats, such as malware, phishing, denial-of-service attacks, and man-in-the-middle attacks.
    - **Classification and Analysis of Cyberattacks:** Exploring various attack techniques, their impact, and real-world examples.
    - **Mitigation Strategies:** Implementing best practices, security policies, and countermeasures to secure network infrastructure.
- **Session 2: Firewall Technologies**
    - **Introduction to Firewalls:** Understanding the purpose and functionality of firewalls in network security.

    - **Types of Firewalls:** Packet-filtering firewalls, stateful inspection firewalls, proxy firewalls, and next-generation firewalls.
    - **Hands-on Firewall Configuration:** Practical exercises on configuring and managing firewall rules, policies, and access control lists.
- **Session 3: Intrusion Detection and Prevention Systems (IDPS)**
    - **Understanding IDPS:** Differentiating between intrusion detection systems (IDS) and intrusion prevention systems (IPS).
    - **Comparison Between IDS and IPS:** Discussing their functionalities, strengths, and weaknesses.
    - **Implementation of IDPS:** Setting up and configuring IDPS in real-world network environments.
- **Session 4: Secure Network Protocols**
    - **Overview of Secure Communication Protocols:** Understanding SSL/TLS, IPsec, SSH, and their role in securing data transmission.
    - **Importance of Encryption:** Exploring encryption techniques and their significance in cybersecurity.
    - **Practical Implementation:** Configuring secure connections and encrypting data for enhanced network security.

The above sessions are covered as below in the day wise.

Day 1: Introduction to Network Security Threats and Countermeasures

The session covered an introduction to network security, including various types of threats and the importance of firewalls. Different firewall configurations and their applications were demonstrated.

Day 2: Types of Firewalls

Participants learned about packet filtering, proxy-based, and stateful firewalls, along with practical demonstrations of firewall configurations.

Day 3: Intrusion Detection and Prevention Systems (IDS & IPS)

This session introduced IDS and IPS concepts, including hands-on exercises to detect and prevent cyber intrusions.

Day 4: Web Security and Common Attacks

Topics such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) were explored with hands-on exercises.

Day 5: Secure Coding Practices

Participants were introduced to secure coding techniques and best practices to protect web applications from vulnerabilities.

Day 6: Ethical Hacking – Foot-printing and Scanning

A deep dive into reconnaissance techniques and network scanning methodologies was conducted through hands-on labs.

Day 7: Ethical Hacking - System Hacking

Topics included password cracking, privilege escalation, and ethical hacking techniques to test system security.

Day 8: Cyber Défense and Incident Response

This session focused on cybersecurity incident management, including real-world case studies and response strategies.

Day 9: Security Operations and SIEM

Participants learned about security operations, monitoring systems, and Security Information and Event Management (SIEM) tools.

Day 10: Final Assessment and Certification Exam

A comprehensive assessment was conducted to evaluate participants' knowledge and practical skills gained during the workshop.

5. Key Takeaways Participants gained significant knowledge and skills, including:

- Identifying and mitigating network security threats and countermeasures
- Hands-on experience with firewalls, IDS, and IPS.
- Practical knowledge of ethical hacking techniques.
- Configuring and managing firewalls.
- Implementing intrusion detection and prevention mechanisms.
- Secure web development practices to prevent cyber attacks
- Incident response and cybersecurity operations management.
- Applying secure network protocols to enhance communication security.

6. Challenges Faced Some challenges encountered during the workshop included:

- Participants' varying levels of prior knowledge in cybersecurity.
- Technical difficulties in hands-on exercises due to software compatibility issues.
- Limited time to cover advanced topics in detail.

7. Feedback and Suggestions Feedback from participants was generally positive. Some suggested improvements include:

- Increasing the duration of hands-on sessions for better practical exposure.
- Providing additional resources for self-study.

- Organizing follow-up sessions for advanced cybersecurity topics.

8. Conclusion The cybersecurity training workshop (Stage 3) successfully equipped participants with essential cybersecurity skills and knowledge. By blending theoretical instruction with practical exercises, the workshop enhanced participants' ability to secure networks and mitigate cyber threats. Future sessions could focus on deeper engagement with emerging cybersecurity trends and advanced security measures.

9. Acknowledgments We extend our gratitude to Microsoft CyberShikshaa, JSPMS Rajarshi Shahu College of Engineering, trainers, and participants for their contributions to the success of this workshop.

Photo’s

Training Coordinator	SPOC	HOD E&TC	Director of RSCOE
Prof.D.V.Chhatrikar	Prof.A.S.Baviskar	Dr.S.C.Wagaj	Dr.S.P.Bhosle

JSPM's Rajarshi Shahu College of Engineering (An Autonomous Institute) Pune University I.D. No PU/PN/Engg/173/(2001) Tathawade, Pune - 33.

Jayawant Shikshan Prasarak Mandal's
Rajarshi Shahu College of Engineering
(An Autonomous Institute)
Tathawade, Pune - 411 033, M.S. (India)