Cyber Security Risk & Incident Management

Course Code: BECCS2C023
Course Title: Cyber Security Risk & Incident Management
Semester: IV
Credits: 4 (03 Theory and 01 Lab)

Rationale

To learn the concepts and strategies to deal with cyber security risks and incidents. This includes the understanding of fundamental concepts of cyber security, risk management methodology covering risk identification, risk analysis, and risk evaluation. Also, emphasis will be on the methodology for dealing with cyber incidents which includes preparation, detection, analysis, containment, eradication, recovery, and post incident management.

Course Outlines

Contents	**No. of Lectures**
Unit I Conceptual Introduction: Cyber Systems, Cyber Security, Risk, Risk Management: Communication and Consultation, Risk Assessment, Monitoring and Review Cyber Risk, Cyber Events and Incidents, Cyber Risk Management: Cyber Risk, Communicating and Consulting Cyber Risk, Cyber Risk Assessment: (Context Establishment for Cyber-risk, Identification of Malicious Cyber-risk, Identification of Non-malicious Cyber-risk, Analysis of Cyber-risk, Evaluation of Cyber-risk, Treatment of Cyber-risk), Monitoring and Review: (Monitoring and Review of Cyber-risk, Monitoring and Review of Cyber-risk Management)	10
Unit II Risk Identification: Risk Identification Techniques, Malicious Risks (Threat Source Identification, Threat Identification, Vulnerability Identification, Incident Identification), Non-malicious Risks (Incident Identification, Vulnerability Identification, Threat Identification, Threat Source Identification)	10
Unit III Risk Analysis: Threat Analysis, Vulnerability Analysis, Likelihood of Incidents, Consequence of Incidents Risk Evaluation: Consolidation of Risk Analysis Results, Evaluation of Risk Level, Risk Aggregation, Risk Grouping Risk Treatment: Risk Treatment Identification, Risk Acceptance	10
Unit IV Cyber Security Incident Management: Incident Management Preparation, Incident Detection and Analysis, Incident Containment, Incident Eradication and Clean-up, Recovery, Post Incident Management. Communication During a Cyber Security Incident: Incident Reporting, Incident Reporting Tools, Incident-Specific Communication Plan	10
Unit V Introduction to Cyber Security Frameworks and Standards: NIST Cybersecurity Framework, HIPAA, FISMA, ISO 27000 series	10

NIST Cyber Security Framework (CSF): CSF Primary Components, Key Framework Attributes, CSF Core: Identify, Protect, Detect, Respond, and Recover, Framework Implementation Tiers, Risk Management Perspective	

List of Lab Practical's

1	Conduct network and host scanning and fingerprinting using NMap
2	Capture network packets using Wireshark to analyse sensitive information disclosure
3	Capture network packets using Scapy to analyse sensitive information disclosure
4	Craft different types of packets using Scapy
5	Create a dynamic webpage for simulating XSS and SQL injection attacks
6	Execute XSS attacks on a dummy webpage on localhost
7	Execute SQL Injection attacks on a dummy website database hosted on localhost
8	Utilize Burp Suite for packet interception and execution of Replay attacks
9	Simulate the use of Dictionary attack to crack weak passwords
10	Introduction to Metasploit framework for vulnerability assessment and penetration testing
11	Utilize Metasploit framework for network scanning
12	Understand the usage of Metasploit MSF venom for vulnerability exploitation
13	Use Snort Intrusion Detection System (IDS) and modify its default configuration rules

Course Outcomes

After completion of the course, the student should be able to

- Understand basic terms related to cyber security
- Identify cyber security requirements
- Describe cyber security risk management and incident management
- Apply cyber security risk management methodology
- Apply cyber security incident management methodology

Text Books

1. Refsdal, A., Solhaug, B., Stølen, K., Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk management. Springer International Publishing. ISBN 978-3-319-23569-1.
2. Clark, C. A. (2020). Cybersecurity Incident Management Masters Guide: Volume 1 - Preparation, Threat Response, & Post-Incident Activity (Cybersecurity Masters Guides)
3. Brumfield, C. (2021). Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework. John Wiley & Sons.

Reference Books

1. Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. Risk Management and Insurance Review, 24(1), 93-125.
2. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology. NIST Special Publication, 800(61r2). doi:10.6028/NIST.SP.800-61r2
3. Strupczewski, G. (2021). Defining cyber risk. Safety science, 135, 105143.
4. The Institute of Risk Management. (2014) Cyber Risk: Resources for Practitioners. https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf
5. Calder, A. (2018). *NIST Cybersecurity Framework: A pocket guide*. IT Governance Publishing Ltd.