|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| D:\UAAR\UIIT\courseOutlineCommittee\CourseContents_Final_V02\New folder\logo4.png | **PMAS Arid Agriculture University Rawalpindi**  **University Institute of Information Technology** | | | |
| CS-597 Cyber Security | | | | | |
| **Credit Hours:** | | **3(3-0)** | **Prerequisites:** | **None** | |
| **Teacher:** | | Shakeel Ahmad | **Contact:** | shakeelalvi@gmail.com | |

|  |
| --- |
| **Course Description:** |
| Basic security concepts, Information security terminology, Malware classifications, Types of malware. Server side web applications attacks. Cross-site scripting, SQL Injection, Cross-site request forgery, Planning and policy, Network protocols and service models. Transport layer security, Network layer security, Wireless security. |
| **Course Objective:** |
| * To equip and familiarize the students with the knowledge to defend against cyber threats. * To focus attention on security, creating sensitivity to the threats and vulnerabilities of computer systems and recognition of the need to protect data, information and systems. |
| **Teaching Methodology:** |
| Lectures, Assignments, Presentations, etc. Major component of the course should be covered using conventional lectures. |
| **Courses Assessment:** |
| Exams, Assignments, Quizzes. Course will be assessed using a combination of written examinations. |
| **Reference Materials:** |
| * Security+ Guide to Network Security Fundamentals by Mark Ciampa, 4th Edition * Corporate Computer Society by Randall J.Boyle, 3rd Edition * Certified Information Systems Security Professional Official Study Guide 9th Edition by James Michael Stewart, Mike Chapple,Darril Gibson |

|  |  |  |
| --- | --- | --- |
| **Course Learning Outcomes (CLOs):** |  |  |
| At the end of the course the students will be able to: | **Domain** | **BT Level\*** |
| 1. Analyze and resolve security issues in networks and computer systems to secure an IT infrastructure. | C | 2 |
| 1. Develop policies and procedures to manage enterprise security risks. | C | 2 |
| 1. Evaluate and communicate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities and training. | C | 3 |
| 1. Design, develop, test and evaluate secure software. | C | 4 |
| \* BT= Bloom’s Taxonomy, C=Cognitive domain, P=Psychomotor domain, A= Affective domain | | |

|  |  |
| --- | --- |
| **Week** | **Theory** |
| **Week 1** | * **Motivational Lecture** * **Course Introduction** * **Success stories** * **Job market** * **Course Applications** * **Institute/work ethics** * Introduction to Cybersecurity * Objectives * Roles * Differences between Information security and cybersecurity. * What is Cyberspace? * What is Cyber security? * Why is Cyber security Important? * What is a Hacker? * Malicious Code and Application Attacks * Malicious Code * Password Attacks * Application Attacks * Web Application Security * Reconnaissance Attacks * Masquerading Attacks |
| **Week 2** | * Security Governance Through Principles and Policies * Understand and Apply Concepts of Confidentiality, Integrity, and Availability * Apply Security Governance Principles * Develop and Implement Documented Security Policy, Standards, Procedures, * and Guidelines * Understand and Apply Threat Modeling * Integrate Security Risk Considerations into Acquisition Strategy and Practice |
| **Week 3** | * Personnel Security and Risk Management Concepts * Contribute to Personnel Security Policies * Security Governance * Understand and Apply Risk Management Concepts * Establish and Manage Information Security Education, Training, and Awareness * Manage the Security Function |
| **Week 4** | * Protecting Security of Assets * Classifying and Labeling Assets * Identifying Data Roles * Protecting Privacy |
| **Week 5** | * Cryptography and Symmetric Key Algorithms * Historical Milestones in Cryptography * Cryptographic Basics |
| **Week 6** | * Modern Cryptography * Symmetric Cryptography * Cryptographic Life Cycle |
| **Week 7** | * PKI and Cryptographic Applications * Asymmetric Cryptography * Hash Functions * Digital Signatures |
| **Week 8** | * Public Key Infrastructure * Asymmetric Key Management * Applied Cryptography * Cryptographic Attacks |
| **Mid Exam** | |
| **Week 9** | * Principles of Security Models, Design, and Capabilities * Implement and Manage Engineering Processes Using Secure Design Principles * Understand the Fundamental Concepts of Security Models * Select Controls and Countermeasures Based on Systems Security Evaluation * Models * Understand Security Capabilities of Information Systems |
| **Week 10** | * Security Vulnerabilities, Threats, and Countermeasures * Assess and Mitigate Security Vulnerabilities * Client-Based * Server-Based * Database Security * Distributed Systems * Industrial Control Systems |
| **Week 11** | * Assess and Mitigate Vulnerabilities in Web-Based Systems * Assess and Mitigate Vulnerabilities in Mobile Systems * Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical * Systems * Essential Security Protection Mechanisms * Common Architecture Flaws and Security Issues |
| **Week 12** | * Physical Security Requirements * Apply Secure Principles to Site and Facility Design * Design and Implement Physical Security * Implement and Manage Physical Security |
| **Week 13** | * Secure Network Architecture and Securing Network Components * OSI Model * TCP/IP Model * Converged Protocols * Wireless Networks * General Wi-Fi Security Procedure * Cabling, Wireless, Topology, and Communications Technology |
| **Week 14** | * Secure Communications and Network Attacks * Network and Protocol Security Mechanisms * Secure Voice Communications * Multimedia Collaboration * Manage Email Security * Remote Access Security Management * Virtual Private Network * Virtualization * Network Address Translation * Switching Technologies * WAN Technologies * Miscellaneous Security Control Characteristics * Security Boundaries * Prevent or Mitigate Network Attacks |
| **Week 15** | * Managing Identity and Authentication * Controlling Access to Assets * Comparing Identification and Authentication * Implementing Identity Management * Managing the Identity and Access Provisioning Life Cycle * Controlling and Monitoring Access * Comparing Access Control Models * Understanding Access Control Attacks |
| **Week 16** | * Software Development Security * Introducing Systems Development Controls * Establishing Databases and Data Warehousing * Storing Data and Information * Understanding Knowledge-Based Systems |
| **Final Exam** | |