**Syllabus**:

|  |  |  |
| --- | --- | --- |
| **Course Code** | **Course Name** | **Credits** |
| **ITC702** | **Infrastructure Security** | **04** |

|  |  |  |
| --- | --- | --- |
| **Module** | **Detailed Contents** | **Hrs** |
| **01** | Cyber-attacks, Vulnerabilities, Defense Strategies and Techniques, Authentication Methods- Password, Token and Biometric, Access Control Policies and Models (DAC,MAC, RBAC, ABAC, BIBA, Bell La Padula), Authentication and Access Control Services- RADIUS, TACACS, and TACACS+ | **06** |
| **02** | **Software Vulnerabilities:** Buffer overflow, Format String, Cross-Site Scripting, SQL Injection, Malware: Viruses, Worms, Trojans, Logic Bomb, Bots, Rootkits  **Operating System Security**: Memory and Address Protection, File Protection Mechanism, User Authentication. Linux and Windows: Vulnerabilities, File System Security  **Database Security:** Database Security Requirements, Reliability and Integrity, Sensitive Data, Inference Attacks, Multilevel Database Security | **12** |
| **03** | Mobile Device Security- Security Threats, Device Security, GSM, UMTS and 4G Security, IEEE 802.11xWireless LAN Security, VPN Security, Wireless Intrusion Detection System (WIDS) | **09** |
| **04** | Cloud Security Risks and Countermeasures, Data Protection in Cloud, Cloud Application Security, Cloud Identity and Access Management, Cloud Security as a Service, SAML, OAuth | **08** |
| **05** | Web Security Considerations, User Authentication and Session Management, Cookies, SSL, HTTPS, SSH, Privacy on Web, Web Browser Attacks, Account Harvesting, Web Bugs, Clickjacking, CrossSite Request Forgery, Session Hijacking and Management, Phishing and Pharming Techniques, DNS Attacks, Web Service Security, Secure Electronic Transaction, Email Attacks, Web Server Security as per OWASP, Firewalls, Penetration Testing | **12** |
| **06** | Security Policies, Business Continuity Plan, Risk Analysis, Incident Management, Legal System and Cybercrime, Ethical Issues in Security Management. | **05** |

**Text Books:**

1. Computer Security Principles and Practice, William Stallings, Sixth Edition, Pearson Education

2. Security in Computing, Charles P. Pfleeger, Fifth Edition, Pearson Education

3. Network Security and Cryptography, Bernard Menezes, Cengage Learning

4. Network Security Bible, Eric Cole, Second Edition, Wiley

**Reference Books:**

1. Web Application Hackers Handbook by Wiley.

2. Computer Security, Dieter Gollman, Third Edition, Wiley

3. CCNA Security Study Guide, Tim Boyle, Wiley

4. Introduction to Computer Security, Matt Bishop, Pearson.

5. Cloud Security and Privacy, Tim Mather, Subra Kumaraswamy, Shahed Latif, O’Riely

**Assessment:**

**Internal Assessment for 20 marks:**

Consisting of **Two Compulsory Class Tests**

Approximately 40% to 50% of syllabus content must be covered in First test and remaining 40% to 50% of syllabus contents must be covered in second test.

**End Semester Examination:** Some guidelines for setting the question papers are as:

* Weightage of each module in end semester examination is expected to be/will be proportional to number of respective lecture hours mentioned in the syllabus.
* Question paper will comprise of total **six questions**, **each carrying 20 marks.**
* **Q.1** will be **compulsory** and should **cover maximum contents of the syllabus**.
* **Remaining question will be mixed in nature** (for example if Q.2 has part (a) from module 3 then part (b) will be from any other module. (Randomly selected from all the modules.)
* Total **four questions** need to be solved.

**Outcomes:**

|  |  |
| --- | --- |
| **CO1** | Understand the concept of vulnerabilities, attacks and protection mechanisms. |
| **CO2** | Analyze and evaluate software vulnerabilities and attacks on databases and operating systems |
| **CO3** | Explain the need for security protocols in the context of wireless communication |
| **CO4** | Understand and explain various security solutions for Web and Cloud infrastructure |
| **CO5** | Understand, and evaluate different attacks on Open Web Applications and Web services |
| **CO6** | Design appropriate security policies to protect infrastructure components |

**Lecture Plan:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No of classes Planned:** | 49 | **No of Classes taken:** |  | |
|  |  |  |  | |
| **Sr. No.** | **Topic Planned** | **Planned Date** | **Actual Date** | **Delivery Mechanisms** |
|  | Introduction to Course and syllabus discussion | 02/07/2019 |  | Board + PPT |
|  | Cyber-attacks and Vulnerabilities | 03/07/2019 |  | Board + PPT |
|  | Defense Strategies and Techniques | 04/07/2019 |  | Board + PPT |
|  | Authentication Methods: Password-based, Token-based, Biometric-based and other authentication methods | 05/07/2019 |  | Board + PPT |
|  | Access Control Policies and Models:Access Control Elements, Access Control Requirements, Access matrix data structures, DAC, An Access Control Model | 09/07/2019 |  | Board + PPT |
|  | Access Control Policies and Models: MAC, Security Levels, RBAC, General RBAC, Variations | 10/07/2019 |  | Board + PPT |
|  | Access Control Policies and Models: ABAC, Sample ABAC scenario, ACL vs ABAC trust relationships, Identity, Credential, and Access Management (ICAM) | 11/07/2019 |  | Board + PPT |
|  | Access Control Policies and Models: Case study: RBAC system for a bank, BIBA Model | 12/07/2019 |  | Board + PPT |
|  | Access Control Policies and Models: BIBA Model cont., Bell Bell La Padula | 16/07/2019 |  | Board + PPT |
|  | Authentication and Access Control Services: RADIUS | 17/07/2019 |  | Board + PPT |
|  | Authentication and Access Control Services: TACACS and TACACS+ | 18/07/2019 |  | Board + PPT |
|  | Software Vulnerabilities: Buffer Overflow-I | 19/07/2019 |  | Board + PPT |
|  | Software Vulnerabilities: Buffer Overflow-II | 23/07/2019 |  | Board + PPT |
|  | Software Vulnerabilities: Format String, Cross-Site Scripting | 24/07/2019 |  | Board + PPT |
|  | Software Vulnerabilities: SQL Injection | 25/07/2019 |  | Board + PPT |
|  | Software Vulnerabilities: Viruses, Worms, Trojans, Logic Bomb | 26/07/2019 |  | Board + PPT |
|  | Software Vulnerabilities: Bots and Botnets, Rootkits | 30/07/2019 |  | Board + PPT |
|  | Operating System Security: Memory and Address Protection-I | 31/07/2019 |  | Board + PPT |
|  | Operating System Security: Memory and Address Protection-II | 01/08/2019 |  | Board + PPT |
|  | Operating System Security: File Protection Mechanism, User Authentication. | 02/08/2019 |  | Board + PPT |
|  | Operating System Security: Linux and Windows: Vulnerabilities, File System Security | 06/08/2019 |  | Board + PPT |
|  | Database Security: Database Security Requirements, Reliability and Integrity | 07/08/2019 |  | Board + PPT |
|  | Database Security: Protecting Sensitive Data, Inference Attacks-I, Multilevel Database Security | 08/08/2019 |  | Board + PPT |
|  | Wireless Security: Wireless Security Overview, Wireless Network Modes, Wireless Networking Components (Facilitating points of attack) | 09/08/2019 |  | Board + PPT |
|  | Wireless Security: Wireless Network Threats, Mobile Device Security- Security Threats, Wireless Security Measures | 20/08/2019 |  | Board + PPT |
|  | Wireless Security: Mobile Device Security Challenges, Mobile Device Security Threats, | 21/08/2019 |  | Board + PPT |
|  | Wireless Security: Mobile Device Security Strategy, Mobile Device Security Elements | 22/08/2019 |  | Board + PPT |
|  | Wireless Security: IEEE 802.11 Wireless LAN, IEEE 802.11 Protocol Stack, IEEE 802.11# Wireless Security, | 23/08/2019 |  | Board + PPT |
|  | Wireless Security: WEP - Wired Equivalent Privacy, Attacks on WEP, WEP Cracking Example, WPA - WI-FI Protected Access, WPA2 - WI-FI Protected Access 2, WEP vs WPA vs WPA2, | 27/08/2019 |  | Board + PPT |
|  | Wireless Security: Procedures to Improve Wireless Security, Securing Wireless Transmission, Securing Wireless Networks | 28/08/2019 |  | Board + PPT |
|  | Wireless Security: IEEE 802 Protocol Architecture, Wireless LAN Security Protocols, | 29/08/2019 |  | Board + PPT |
|  | Wireless Security: Elements of IEEE 802.11i, IEEE 802.11i Phases of Operation | 30/08/2019 |  | Board + PPT |
|  | Wireless Security: IEEE 802.1x Access Control, IEEE 802.11i Keys for Data Confidentiality and Integrity Protocols | 11/09/2019 |  | Board + PPT |
|  | Cloud Security: Cloud Service Models, Cloud Deployment Models, NIST Cloud Architecture | 12/09/2019 |  | Board + PPT |
|  | Cloud Security: NIST Cloud Security Guidelines, Security Issues for Cloud Computing, Control Functions and Classes, | 13/09/2019 |  | Board + PPT |
|  | Cloud Security: Risks and Countermeasures, Data Protection in the Cloud | 17/09/2019 |  | Board + PPT |
|  | Cloud Security: Cloud Application Security, Cloud Identity and Access Management | 18/09/2019 |  | Board + PPT |
|  | Cloud Security: Cloud Identity and Access Management | 19/09/2019 |  | Board + PPT |
|  | Cloud Security: Cloud Security as a Service, SAML, OAuth | 20/09/2019 |  | Board + PPT |
|  | Web Security: Web Security Considerations, User Authentication and Session Management, Cookies, SSL, | 24/09/2019 |  | Board + PPT |
|  | Web Security: HTTPS, SSH, Privacy on Web | 25/09/2019 |  |  |
|  | Web Security: Web Browser Attacks, Account Harvesting, Web Bugs, | 26/09/2019 |  |  |
|  | Web Security: Clickjacking, CrossSite Request Forgery, Session Hijacking and Management, | 27/09/2019 |  |  |
|  | Web Security: Phishing and Pharming Techniques, DNS Attacks, | 01/10/2019 |  |  |
|  | Web Security: Web Service Security, Secure Electronic Transaction, Email Attacks, | 03/10/2019 |  |  |
|  | Web Security: Web Server Security as per OWASP, Firewalls, Penetration Testing | 04/10/2019 |  |  |
|  | Information Security and Risk Management: Security Policies, Business Continuity Plan, | 09/10/2019 |  |  |
|  | Information Security and Risk Management: Risk Analysis, Incident Management, | 10/10/2019 |  |  |
|  | Information Security and Risk Management: Legal System and Cybercrime, Ethical Issues in Security Management. | 11/10/2019 |  |  |