CSCO 513 : Ethical Hacking and Digital Forensics

Course Objectives:

1. To make the student aware of the need to ethically hack one's own systems and network to know the loopholes.
2. To make the student aware of the forensics which need to performed to produce digital trails of crimes in the modern world

Course Outcomes:

1. Student gets the skills and the knowledge of the tools required for performing ethical hacking and the digital forensics
2. Student gets the legal architecture of the nation which needs to be observed while performing ethical hacking and digital forensic

UNIT I (12 Hours)

HACKING WINDOWS : Network Hacking, Web Hacking, Common Network Hacking Techniques, Password hacking, Cracking Passwords, Input Validation Attacks, SQL Injection Attacks, Buffer overflow attacks, Privacy Attacks**,**

TCP / IP AND FIREWALLS : TCP/IPChecksum, TCP / IP and Firewalls, IP Spoofing, Services Vulnerable to IP Spoofing, Port Scanning, DNS Spoofing, DNS ID Spoofing, DOS Attack, Application Level Attacks, Distributed Denial-of-Service Attacks (DDoS), DDoS Tools, UDP Flooding, Firewalls, Packet Filtering Firewall, Filtering on IP Header Criteria, Application Proxy Firewalls, Firewall's security policy, Batch File Programming

UNIT II (12 Hours)

COMPUTER FRAUD: Insider Threat Concepts, Insider Threat Study, Methodology for the Optimization of Resources in the Detection of Computer Fraud, Managing the Insider Threat, The Insider Threat Strategic Planning Process, Cyber-Security Risk Governance Processes for Web-Based Application Protection (Understanding the External Risks and Internal Information Security Risks), The Risk Management Process, The Tailored Risk Integrated Process (TRIP), Security Controls in Application Systems Controls (ISO 27001, The Strategic Planning Process for Reducing the Insider Threat, The Threat Assessment Matrix, Application and Code Review, Strategic, Legal/Regulatory, and Operational Risk Ratings, The Information Security Scorecard, Develop Security Patterns for Applications/ Systems Software Engineering (Process and Product Improvements), Implemented Software Engineering InfoSec Process and Product Improvements

UNIT III **(12 Hours)**

ARCHITECTURE STRATEGIES: Architecture strategies for computer fraud prevention, Architectural Strategies to Prevent and Detect ICF, Intrusion Detection Systems, NIDSNetwork Intrusion Detection Systems, Host-Based Intrusion Detection Systems (HIDS), The Penetration Testing Process, Web Services-Reducing Transaction risks, Extensible Mark-up Language (XML), XML and Security, Simple Object Access Protocol (SOAP), Problems with Web Services Security**, FRAUD SELECTION & DETECTION**: Key Fraud Indicator selection process, Macro Computer Fraud Taxonomy, Key fraud signature selection process, Accounting Forensics, Computer Forensics, Journaling and its requirements, The National Industrial Security Program Operating Manual (NISPOM), Journaling Risk/Controls Matrix, Standardised Logging Criteria for Forensic Photo Frames, Neural networks – Misuse detection and Novelty detection.

Textbooks :

Textbooks :

1. Kenneth C.Brancik, Insider Computer Fraud, Auerbach Publications Taylor & Francis, Group 2008.
2. Ankit Fadia, Ethical Hacking, Second Edition Macmillan India Ltd, 2006.

3. https://healholistic.files.wordpress.com/2013/08/batch-file-programming-ankitfadia.pdf.

4. https://www.princeton.edu/~rblee/ELE572F02presentations/DDoS.pp Permission to reproduce extracts from BS ISO/IEC/2700: 2005 is granted by BSI.British Standards can be obtained in PDF format from the BSI Online Shop: http://www.BS l-Global.com/en/shop

5. GTAG (Global Technology Audit Guide), Application Based Controls. The Institute of Internal Auditors, 2005.

6. The FFIEC Information Security Booklet, 2006.

7. Komanosky, Sasha. Enterprise Security Patterns, June 2004. The original source for the security pattern was the 3/03I SSA Password/Journal Enterprise Security Patterns

8. Caudill, Maureen and Butler, Charles, Naturally Intelligent Systems, MIT Press, Cambridge, MA, 1992.

9. Hawkins, Jeff, On Intelligence, Times Books, Henry Holt, New York, 2004.

10. Saffron Technologies, Technical White Paper, Morrisville, NC, 2004 (www.saffrontech.com).

11. Nigrini, Mark, Fraud Detection—I've Got Your Number. Journal of Accountancy, May, 79–83, 1999.