Certificate Course on "Cyber Security and Ethical Hacking" at Pune Institute of Computer Technology,(P.I.C.T) Pune.

Objectives and Outcomes	**Objectives:** 1) To learn foundations of Cyber Security and Ethical Hacking analysis using programming languages like python. 2) To learn various types of algorithms and its applications of Cyber Security and Ethical Hacking using forensic detection 3) To learn python toolkit for required for programming Cyber Security, Ethical Hacking concepts. 4) To understand the concepts of Cyber Security, Ethical HackingForensic detection image processing ,pattern recognition, and natural language processing. 5) To identify insights on how to apply Cyber Security, Ethical Hacking to solve a interdisciplinary problems. 6) To acquire the hands-on skills and the knowledge required for job competency. **Outcomes:** **On completion of the course, student will be able to** 1) Understand, appreciate, employ, design and implement appropriate security technologies and policies to protect computers and digital information. 2) Identify & Evaluate Information Security threats and vulnerabilities in Information Systems and apply security measures to real time scenarios 3) Identify common trade-offs and compromises that are made in the design and development process of Information Systems 4) Demonstrate the use of standards and cyber laws to enhance information security in the development process and infrastructure protection.
Scope	This course aims at providing the attendee with a broad introduction to the profound concepts in Cyber Security and Ethical Hacking using forensic detection by exposing them to practical scenarios in order to make them industry ready. It's definitely beneficial to professionals looking for change/ advancement in their career as well as Budding Engineers to start their career as Ethical Hacking Data Scientist, Cyber Security Engineer, Anti Cyber Terrorism Scientist, etc. The emphasis will be more on intuition and practical examples

	rather than theoretical aspects.
Target Participants	Any working professionals holding BCA/MCA/BE/ B.Tech/M.Tech. or equivalent degree, Candidates holding B. Sc./M.Sc. in Mathematics or Statistics. **Eligibility:** The candidate must have 50% in the qualifying degree. The candidate must have awareness of programming concept. **Selection Criteria :** Admission to these programmes is done through a Aptitude and Screening test. **Batch Size :**40 participants
Course Contents	Module-wise Break Up Module I : Foundations of Cyber Security Concepts (10H) Module II : Cryptography and Cryptanalysis (20H) Module III : Infrastructure and Network Security (40H) Module IV : Cyber Security Vulnerabilities& Safe Guards (40H) Module V : Malware (20) Module VI : Security in Evolving Technology (10H) Module VII : Cyber Laws and Forensics (60H) Module VIII: Introduction to Ethical Hacking (10H) Module IX : Server Hacking and Security Techniques (20H) Module X : Computer Forensic Detection and Incident Management(30H) Module XI : Project and Internship (40H) (Detail Syllabus is provided at the end)
Facilities Available	Classrooms with LCD, Laboratories equipped with high end PCs with latest Configuration, Library with lot of e journals, Books, conference proceedings, etc.
Course Details	**PG Diploma in Cyber S**ecurity and **Ethical Hacking** • Duration : 06 Months • Number of Hours : **Aprx. 300 Hrs.** • Type: **Weekend Course** • **Day and Timings :** **Friday:02pm – 05pm ; Saturday and Sunday :09am-01pm** • **Course Fees : 50,000/-** excluding GST (Fee waiver scheme is available *) * First Topper/ Economically Poor Student / Category • Start Date (Tentative) : July 2020

Syllabus

Cyber Security and Ethical Hacking

Total Modules:11

Total Duration & Hours:Six months and 300 hours

Contents
Module-I: Foundations of. Cyber Security Concepts(10H)
Essential Terminologies: CIA, Risks, Breaches, Threats, Attacks, Exploits. Information Gathering (Social Engineering, Foot Printing & Scanning).Open Source/ Free/ Trial Tools: nmap, zenmap, Port Scanners, Network scanners
Module – II: Cryptography and Cryptanalysis(20H)
Introduction to Cryptography, Symmetric key Cryptography, Asymmetric key Cryptography,Message Authentication, Digital Signatures, Applications of Cryptography. Overview of Firewalls- Types of Firewalls, User Management, VPN Security, Security Protocols: - security at the Application Layer-PGP and S/MIME, Security at Transport Layer- SSL and TLS, Security at Network Layer-IPSec.
Module – III Infrastructure and Network Security.(40H)
Python programming environment Overview. Introduction to System Security, Server Security, OS Security, Physical Security, Introduction to Networks, Network packet Sniffing, Network Design Simulation. DOS/ DDOS attacks. Asset Management and Audits, Vulnerabilities and Attacks. Intrusion detection and Prevention Techniques, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation.
Module – IV Cyber Security Vulnerabilities& Safe Guards(40H)
Internet Security, Cloud Computing &Security, Social Network sites security, Cyber Security Vulnerabilities-Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Authorization, Unprotected Broadband communications, Poor Cyber Security Awareness. Cyber Security Safeguards- Overview, Access control, IT Audit, Authentication. Open Web Application Security Project (OWASP), Web Site Audit and Vulnerabilities assessment.Open Source/ Free/ Trial Tools: WinAudit, Zap proxy (OWASP), burp suite, DVWA kit. Hands on project and mini project
Module – V Malware (20H)
Explanation of Malware, Types of Malware: Virus, Worms, Trojans, Rootkits, Robots, Adware's, Spywares, Ransom wares, Zombies etc., OS Hardening (Process Management, Memory Management, Task Management, Windows Registry/ services another configuration), Malware Analysis.Open Source/ Free/ Trial Tools: Antivirus Protection, Anti Spywares, System tuning tools, Anti Phishing.

Hands on Cyber security and Framework
Module – VI Security in Evolving Technology(10H)
Biometrics, Mobile Computing and Hardening on android and ios, IOT Security, Web server configuration and Security. Introduction, Basic security for HTTP Applications and Services, Basic Security for Web Services like SOAP, REST etc., Identity Management and Web Services, Authorization Patterns, Security Considerations, Challenges. Open Source/ Free/ Trial Tools: adb for android, xcode for ios, Implementation of REST/ SOAP web services and Security implementations Reviews and Conclusion
Module – VII Cyber Laws and Forensics(60H)
Introduction, Cyber Security Regulations, Roles of International Law, the state and Private Sector in Cyberspace, Cyber Security Standards. The INDIAN Cyberspace, National Cyber Security Policy 2013. Introduction to Cyber Forensics, Need of Cyber Forensics, Cyber Evidence, Documentation and Management of Crime Sense, Image Capturing and its importance, Partial Volume Image, Web Attack Investigations, Denial of Service Investigations, Internet Crime Investigations, Internet Forensics, Steps for Investigating Internet Crime, Email Crime Investigations.
Module -VIII Introduction to Ethical Hacking (10H) LINUX and Networking,Doxing,Website/ IP information Gathering,Network Mapping Google Hacking, Discovering IP Range and Open Port, Identifying Target Operating System and Services,Secure Bypassing Firewalls while Scanning,Understanding Wireless Networks, Deauthentication attack, Fragmentation Attacks, Chop Chop attack, Fake authentication Evil Twin Attack, Cafe-latte attack,Reveal Hidden SSID's, WPA and WPA2 wireless password,hacking techniques,Cracking Wireless Passwords using Rainbow tables, Brute force techniques. Wordpress-scan , Drupal scan, Joomscan, cms-explorer for CMS Hacking and Pentesing,Websploit, SET, Fast-Track SQL Pwnage, Winautopwn for various System
Module -IX Server Hacking and Security Techniques(20H) Learning Various Methods to Use Proxies, Hiding yourself behind VPN, Using Proxies and VPN for Hacking Tools i.e Scanning, Configuring TOR with Backtrack and Nmap for Invisible Scanning, Using Tunneling methods for IP hide, Types of Email Addresses, Security measures for Phishing, Security measures for Password Guessing, Security measures for Mobile Phone., Hacking Windows Passwords using various methods & Security, Cracking SAM file, Protecting SAM file from hack, Privilege Escalation in windows and Linux,, Using Stealers, Key loggers and Remote Administrations Tools (RATs), Creating Undetectable Viruses using Crypters, Binders and Assembly Codes.,, Protection against Trojans , Worms and Malwares, Advance SQL Injection, Cross Site Scripting, Router Hacking, Sniffing Data and Passwords, ARP , DNS, DHCP Spoofing attacks. DNS poising , DOS attack against

an IP address Flood the LAN with random MAC addresses .Packet Injection

Module -X Computer Forensic Detection and Incident Management(30H)

Computer Investigation Process and Collecting Digital Evidences. Cyber Crime Investigation and Understanding various trace back Techniques. Acquiring data, duplicating data and Recovering deleted Files. Understanding Boot Process and Important System Files Investigating Network Traffic, Cyber Crimes and Laws Understanding Various Corporate Threats .Case Studies. Setup lab with bWAPPSet up Burp Suite -Configure Firefox and add certificateMapping and scoping websiteSpideringActive and passive scanningScanner options and demo Introduction to password securityIntruder. Intruder attack typesPayload settings,Intruder settings.

Module – XI Project and Internship (40H)

LIST OF PRACTICALS

1. Implementation to gather information from any PC's connected to the LAN using whois, port scanners, network scanning, Angry IP scanners etc.
2. Implementation of Symmetric and Asymmetric cryptography.
3. Implementation of Steganography.
4. Implementation of MITM- attack using wireshark/ network sniffers
5. Implementation of Windows security using firewall and other tools
6. Implementation to identify web vulnerabilities, using OWASP project
7. Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report.
8. Implementation of OS hardening and RAM dump analysis to collect the Artifacts and other information's.
9. Implementation of Mobile Audit and generate the report of the existing Artiacts.
10. Implementation of Cyber Forensics tools for Disk Imaging, Data acquisition, Data extraction and Data Analysis and recovery.

LIST OF SUGGESTED BOOKS

1. William Stallings, “Cryptography and Network Security”, Pearson Education/PHI, 2006.

2. V.K. Jain, “Cryptography and Network Security”, Khanna Publishing House.

3. Gupta Sarika, “Information and Cyber Security”, Khanna Publishing House, Delhi.

4. Atul Kahate, “Cryptography and Network Security”, McGraw Hill.

5. V.K. Pachghare, “Cryptography and Information Security”, PHI Learning

6. Nina Godbole, “Information System Security”, Wiley

7. Bothra Harsh, “Hacking”, Khanna Publishing House, Delhi

8..The basic of Hacking and Penetration testing ,second edition on ethical hacking and penetration by Patrick Engebretson

9.The web application hackers handbook and LAB manual by Wiley

Reference Websites :

http://www.ignou.ac.in/upload/Announcement/programmedetails.pdf