Cyber Security with VAPT, CISA, CISSP

Objective: Working with Fundamentals of Cyber Security and its Tools

Pre-requisites: To Learn Cyber Security, we need to familiarize with some basic networking concepts, some linux concepts and commands execution in linux environment

Session 1 (Basic Networking Concepts)

- What is Network?
- What is IP Address and Types?
- Networking Models (OSI and TCP/IP Models)
- Internetworking
- Domain Name
- OS, Severs, Ports and Types of Ports
- Introduction to Web Browser
- Security of Web Browser

Session 2 (Ethical Hacking and Cyber Security and Overview)

- Cybercrime scenario in India and worldwide
- Short Description about hacking vs Ethical Hacking
- Skill Profile of a Hacker
- Some Famous Hackers and Groups
- Cyber World
- Advantage and Disadvantage of Cyber World
- Types of Hackers
- Classes of Hacker
- Who is a Hacker?
- Security Challenges
- Skills Required for an Ethical Hacker

Session 3 (Overview of Cyber Law)

- Introduction to Cyber Law
- Indian Cyber Laws
- Technical Aspect of Indian Cyber Law
- IT ACT 2000 and 2008
- Internet Crimes And Frauds
- Cyber Law Cases in India

- Study of IT-Act
- Advantages of Cyber Laws

Session 4 (Computer Virtualization Technology and LAB Setup)

- Concept of Virtualization Technology
- Need and Advantage of Virtualization
- Requirements for Virtualization
- Creating Virtual Machines and Optimization Performance
- Installing OS (Windows and Linux) On Virtual Machines
- Virtual Networking What and Why?

Session 5 (Information Gathering – Foot Printing)

- What is Information Gathering & Why Hackers Need This?
- Types of Information Gathering
- Information Gathering Using Websites
- Information Gathering using Software's
- Search Engines – Smart Way of Information Gathering
- Ping, Location Find-out
- Web Data, Who-is Lookup
- People Search, DNS Lookup
- Benefits of Foot Printing
- Many more methods of Information Gathering

Session 6 (Windows, Linux Password Hacking and Security)

- Introduction Windows Security
- User Accounts Security, Attacks and Countermeasure
- Hacking Into System by Changing Passwords
- Getting Access to System By Elevating Privileges
- Finding Out the Passwords Of Windows
- Bypassing the Windows and Linux Security
- Live Demo All Password Bypass
- Study of Password Security

Session 7 (Some Other Concepts for Cyber Security)

- Data Recovery & Data Hide
- Steganography
- Cryptography

- VAPT (Vulnerability Assessment & Penetration Testing)
- Scanning
- Bug Bounty

Session 8 (Mobile Phone Hacking)

- Use of Mobile In Hacking
- Hidden Function of Mobile
- Backdoor Attack
- Fake Calling and SMS

Session 9 (Denial of Service Attack – DOS Attack)

- What is Denial of Service Attack?
- What is Distributed Denial of Service Attacks?
- DOS Attack Techniques
- Detail Study of DOS Attack Tools

Session 10 (Hacking by Viruses, Trojans, Keyloggers & Backdoor)

- What is Viruses?
- What is Trojan?
- Trojans/Viruses Attack
- Different way a Trojan Can Get Into A System
- How Attacker Bypass Your Antivirus By Trojans

Session 11 (Proxy Server & Virtual Private Network – VPN Technology)

- Proxy and Types of Proxies
- Why Hackers Use Proxy?
- How to Hide IP Address While Chatting
- How to Open Block Website in College/Companies
- Advantage and Disadvantage of Proxy
- How Proxy Hack Your Password Etc
- What is VPN?
- Why We Use VPN?
- Advantage and Disadvantage of VPN
- Free VPN

Session 12 (Google Hacking and Google Hacking Database)

- Introduction and Working of Search Engines
- List of Common Search Engines on Web

- Comparing and Choosing Best Search Engine
- Google for Hacking Search Engines
- Finding Admin Pages and Weakness In Site
- Security Against Search Engine Hacking

Session 13 (Social Sites Hacking & Security Issues)

- Cookies Stealing (Session Hijacking) of All Big Mail Servers
- Phishing Attacks (Normal & Advanced)
- Analyzing Fake & Real Profiles & Email Accounts
- Facebook phishing Attacks
- Facebook Account Security with Email and SMS Notifications

Session 14 (Email Hacking and Tracing)

- Fake Mailing Attack
- Email and Fake Profile Tracing
- Email Security

Session 15 (SQL Injection)

- What is SQL Injection?
- SQL Injection Attacks
- How Web Applications Work?
- SQL Injection Detection
- Types of SQL Injection
- How to Defend Against SQL Injection Attacks?

Session 16 (Linux Training)

- How to Bootable OS
- Live Run and Fully Install
- What is Linux and how to operate this OS
- Use of Linux, Set Terminal
- Advance Information Gathering
- Session Hijacking
- Site Cloning and Advance phishing Attack
- Network Find and Scanning
- Wireshark, Armitage
- NMAP, Terminal Function

Session 17 (Wireless Hacking)

- Wireless Standards
- Common Vulnerabilities in Wireless Devices
- Encryption Standards Used in Wi-Fi
- WEP Cracking
- WPA/WPA2 Cracking
- Wi-Fi Jammer
- Solve Security Challenges

Session 18 (Security)

- Facebook/Mail Account Security
- Whatsup Security
- How to secure your data
- Android Phone Security

Session 19 (Cyber Crime Investigation – Case Study)

- Introduction to Cyber Crime Investigation
- Types of Cyber Crimes
- Report Cyber Crimes
- Investing Emails (Email Tracing)
- Online Email Header Analysis
- Investing Phishing Cases
- Investing Data Theft Cases
- Investing Facebook Profile Impersonation Cases

Session 20 (Security and Risk Management)

- Understand and apply concepts of Confidentiality, Integrity and Availability
- Develop and Implement Documented Security Policy, Standards, Procedures and Guidelines
- Understand Business Continuity Requirements
- Contribute to Personnel Security Policies
- Understand and Apply Risk Management Concepts

Session 21 (Security Architecture Engineering)

- The Engineering Life Cycle Using Security Design Principles
- Fundamental Concepts of Security Models
- The Engineering Life Cycle Using Security Design Principles
- Fundamental Concepts of Security Models

- Assess and mitigate the vulnerabilities in Web-based systems
- Assess and mitigate the vulnerabilities in Mobile Systems
- Assess and mitigate the vulnerabilities in Embedded Devices
- Apply Cryptography
- Implement facility Security Controls, Wiring Closets/Intermediate distribution facility

Session 22 (Communication and Network Security)

- Apply Secure Design Principles in Network Architecture
- Implications of Multi-Layer Protocols
- Converged Protocols
- Securing Network Components
- Implement Secure Communication Channels according to design

Session 23 (Identity and Access Management – IAM)

- Physical and Logical Access to Assets
- Manage Identification and Authentication of People, Devices and Services
- Federated Identity Management
- Integrate Identity as a third-party service
- Attribute Based Access Controls
- Implement and Manage Authorization Mechanisms
- Identity and Access Provisioning Life Cycle

Session 24 (Project Work)