ETHICAL HACKING

Module

- Introduction to Cyber World
- Cyber Definition
- www - Tim Burners Lee
- Journey from Main Frame System to Smart Phone
- Facts and Figures of Computer, Internet, Mobile Users
- Operating Systems and the founders/ key role players like Linus torvald
- Famous old hacks and some recent major/world famous incidents
- Wikileaks Story
- Edward Snowden Story
- Cyber Warfare -- China officially announced they have cyber army
- Information Security and its need
- Stats (Forbs story about cyber security 2nd most paid job) etc..
- Some general terms used in Cyber World
- Some Formal Strategies (phases) in Penetration Testing

Networking Fundamentals

- Introduction of Network/Networking
- Definition of Network
- Origin of Intranet
- Types of Network
- Network Devices
- Medium Access Control (MAC) Address

- Need of Networking
- TCP V/s UDP connections
- Introduction to IP addresses (v4,v6,v5)
- IPv4 Types, Classes
- Dynamic Host Control Protocol (DHCP)
- Ports
- Net Cat (Demonstration)
- Router & Accessing Routers
- Domain Name System (/etc/host)
- Working of DNS
- DNS settings in windows/Linux/routers
- Introduction to Servers (Web Server/Mail Server/DB server)

Malware

- Introduction of Malwares
- types
- Virus & worms (practical)
- Rootkits
- Trojan | win/nix
- RAT | win/nix
- Key logger (offline vs online)
- Binders
- Extension Spoofing (charmap)
- Anti-Keylogging concepts
- History
- Recent Attacks
- Anti-Virus Concepts

Web Application Penetration Testing

- Introduction Web Application
- Server/Client Side Scripting
- RDBMS concepts
- Introduction to SQL/PgSQL/MySQL/MsSQL
- Basic Working with MySQL
- Installing and working for Local Server (xampp/apache2)
- Working of HTTP
- HTTP Request & Response Examples
- Different HTTP Codes (200,302,404,400,500 etc)
- Using HTTP Interceptor
- Functional Testing V/s Security Testing
- Brute Forcing passwords
- Introduction of Captcha
- Introduction to WASC/OWASP
- Google Hacking Database (GHDB)

XSS Cross Site Scripting

- Introduction
- Reflected XSS
- Stored XSS
- Dom Based XSS
- Temporary Defacement
- Insecure Redirect via XSS
- Cookie Grabbing
- Broken Authentication and Session Management

- Authentication Bypass (SQLi Basics)
- SQL Injection
- WAF Bypass (Limited Edition)
- Using tools (Sqlmap, Havij)
- Cross Site Request Forgery

Information Gathering

- Introduction Of Information Gathering
- Who is and Domain tools
- Email Harvesting
- Social Networking Sites
- Working of Search Engines
- Concept of Robots.txt
- Concept of Sitemap.xml
- Concept of Web Crawling
- Mirroring Web Applications
- Wayback Machine
- Social Engineering Techniques
- Demonstration
- Introduction of Phishing
- Remote Phishing
- Desktop Phishing
- Fake Mailers
- Email Tracing

Case Studies Along With Investigation Methods