# Troika Cyber Security Analyst

# Introduction

Cyber breaches are increasing world over and india too is one of the major targets of cyber attacks, as per report by PWC Cybersecurity breaches incidents spurt 117% in India. Organizations in INDIA are looking towards innovative security solutions to mitigate new range of attacks. Security professionals with Vulnerability assessment, penetration testing and malware analysis skills can be 1st line of defence to organizations layered security architecture. This course is designed for students who are new cyber security domain with more emphasis on hand's on lab (80% lab and 20% theory) .

TCSA has been designed by industry skilled professionals and covers comprehensive attack vectors, with Troika iLab's professionals can master their learning by exploiting various vulnerabilities and analysing attack behaviour

**Who should attend:** Information security staff, Network security administrators, System admins and others requiring in depth understanding of cyber security

**Prerequisites:** General knowledge of computer and operating system fundamentals is required. Some exposure to software development and experience in assembly and C programming languages is recommended.

**Take away**: After completion of this course students will attain understanding of various attack vectors and hands-on learning of vulnerabilities exploitation

- Understanding of cyber security and why its important in today's world
- Overview of various attack vectors & attack life-cycle
- Exploring KALI Linux and programming essentials
- Information gathering - Scanning the network
    - Active reconnaissance
    - Passive reconnaissance
- Understanding and exploringmetasploit framework
    - Type of shell's
        - Reverse TCP shell
        - Bind TCP shell
    - Attacking your first machine
    - Post exploitation using meterpreter.
- Overview of shell code and crafting your shell code
- Buffer overflows
    - Assembly language basics

    - Understanding various registers
- OWASP & Web application security
    - Understanding OPWASP top vulnerabilities
    - Browser exploitation
    - Local & remote file inclusion
    - SQL injection & XSS attacks
- Overview of mobile hacking & smartphone pentest framework
- Tracing malware in your lab environment
    - Static analysis
    - Dynamic analysis

# Course content

## Module 0 – Introduction to Ethical Hacking

- Cyber security overview
- Top information security attack vectors
    - Understanding threat vectors
        - Operating systems attacks
        - Application oriented attacks
        - Network level threats
    - Attack lifecycle and phases of attacks
    - Attackers motives
    - Essential terminologies

## Module 1 – Introduction to Kali Linux

- Setup virtual environment for Kali Linux and target virtual machines
- Overview of Linux command line
    - Directory structure
    - File permissions
    - User privileges
    - Process and services
- Install new packages on Kali Linux
- Managing packages

- Netcat - The Swiss Army Knife of TCP/IP Connections

## Module 2 – Programming refresher

- Overview of bash scripting & Python
    - A sample bash script
    - Adding functionality with "if" statement
    - Bash script with "for" statement
- Writing and compiling the program
- Streamlining the results

## Module 3 – Before the snap: Scanning the network

- Information gathering
- Identifying the Target – Passive Reconnaissance
    - Open source intelligence gathering
        - Netcraft
        - Whois Lookups
        - DNS Reconnaissance
        - Maltego
        - Harvester
    - Port scanning
        - Manual port scanning
        - Port scan with NMAP
- Identifying the Target – Active Reconnaissance
    - Finding vulnerabilities with Nessus and Nmap
    - Nmap NSE scripts for advance scanning
    - Web application scanning

## Module 4 – Exploitation using Metasploit -1

- Understanding Metasploit framework
- Essential Metasploit terminology
    - Exploit, payload, shell code
    - Module, listener, handler
- Understanding Metasploit interface and utilities
    - MSFconsole, MSFcli, Armitage
    - MSFpayload, Nasm shell

- Exploiting your first machine with Metasploit
- Types of shell
    - Bind shell, reverse shell
- Understanding meterpreter framework – post exploitation
    - Basic meterpreter commands
    - Capturing keystrokes
    - Dumping username and password
    - Privilege escalation using meterpreter
    - Token impersonation
- Avoiding detection – creating standalone binaries with MSFpayload
- Evading antivirus detection
    - Encoding with MSFpayload
    - Multi-encoding
    - Understanding  packers

## Module 5 – Exploitation using Metasploit -2

- Exploitation using client side attacks
    - How browser based attacks works
    - Looking at NOP's
    - File format exploits
- Understating Metasploit auxiliary modules
- Anatomy of an auxiliary module
- Creating Standalone Payloads with Msfvenom
    - Choosing a Payload
    - Using the Multi/Handler Module
- Creating your own exploits
    - Art of fuzzing
    - Remote code execution

## Module 6 – password attacks

- Password management
- Online password attacks
    - Wordlists
    - Guessing Usernames and Passwords with Hydra
- Offline Password Attacks

    - Recovering Password Hashes from a Windows SAM File
    - Dumping Password Hashes with Physical Access
    - LM vs. NTLM Hashing Algorithms
    - John the Ripper
    - Cracking Linux Passwords
    - Rainbow Tables
- Online Password-Cracking Services
- Dumping Plaintext Passwords from Memory with Windows Credential Editor

## Module7 – OWASP & Web application security

- Understanding OWASP top 10 vulnerabilities
- Understating browser exploitation framework
- SQL injection
    - Testing for SQL Injection Vulnerabilities
    - Exploiting SQL Injection Vulnerabilities
    - Using SQLMap
- Local File Inclusion
- Remote File Inclusion
- Command Execution
- Cross-Site Scripting
    - Checking for a Reflected XSS Vulnerability
    - Leveraging XSS with the Browser Exploitation Framework
- Cross-Site Request Forgery
- Web Application Scanning with w3af
- Policy based forwarding, Static and dynamic routing protocols
- Web attack tools
    - Using Burp Proxy
    - OWASP ZAP
    - SET password harvesting
    - Fimap
- Attacking session management
    - Clickjacking
- Web session tools
    - Firefox plugins: cookie injector, cookie manager, etc.

- Cookie cadger

## Module 8 – Social engineering

- The Social-Engineer Toolkit
- Spear-Phishing Attacks
  - Choosing a Payload
  - Setting Options
  - Naming Your File, Single or Mass Email
  - Creating the Template, Setting the Target
  - Setting Up a Listener
- Multipronged attacks

## Module 9 – Buffer overflow

- Understanding memory Theory
- Overview of buffer overflow attacks
  - Understanding vulnerable program
  - Causing a crash
  - Running GDB
  - Crashing program in GDB
  - Controlling EIP
  - Hijacking execution
- Searching known vulnerability in any known application
  - Causing a crash
  - Locating EIP
  - Hijacking execution
  - Getting a shell

## Module 10– Mobile hacking

- Using smartphone pentest framework
- Understanding mobile attack vectors
  - Text messages
  - Near Field Communication
  - QR Codes

- The Smartphone Pentest Framework
    - Setting Up SPF
    - Android Emulators
    - Attaching a Mobile Modem
- Remote Attacks
    - Default iPhone SSH Login
- Client-Side Attacks
    - Client-Side Shell
    - USSD Remote Control
- Malicious Apps
    - Creating Malicious SPF Agents
- Mobile Post Exploitation
    - Information Gathering
    - Remote Control
    - Pivoting Through Mobile Devices
    - Privilege Escalation

## Module 11 – Malware analysis -1

- What Is Malware Analysis?
- How to create a safe malware analysis environment
- The malware analysis and reporting process
- Malware Analysis Techniques
- Basic static analysis techniques
    - Antivirus Scanning: A Useful First Step
        - Hashing: A Fingerprint for Malware
        - Finding Strings
    - Packed and Obfuscated Malware
        - Packing Files
        - Detecting Packers with PEiD
        - Portable Executable File Format
        - Static, Runtime, and Dynamic Linking
            - Exploring Dynamically Linked Functions with Dependency Walker
            - Imported Functions
            - Exported Functions

    - Static Analysis in Practice
        - PotentialKeylogger.exe: An Unpacked Executable
        - PackedProgram.exe: A Dead End
    - The PE File Headers and Sections
        - Examining PE Files with PEview
        - Viewing the Resource Section with Resource Hacker
- Malware analysis in virtual machine
- Creating your malware analysis machine
- Simulating malware in virtual environment

## Module 12 – Malware analysis-2

- Basic dynamic analysis techniques
- Using a Malware Sandbox
- Running Malware
- Monitoring with Process Monitor
    - The Procmon Display
    - Filtering in Procmon
- Viewing Processes with Process Explorer
    - Using Dependency Walker
    - Analyzing Malicious Documents
- Comparing Registry Snapshots with Regshot
- Faking a Network
    - Using ApateDNS
    - Monitoring with Netcat
- Packet Sniffing with Wireshark
- Using INetSim
- Basic Dynamic Tools in Practice
- Malware behavior
- Backdoors
    - Reverse Shell, RAT's
    - Botnets
- Privilege Escalation

# Stay Ahead of the curve