Cyber Security Training Programs

The IOED is offering a unique range of hands on training programs in the area of Cyber Security. it would assist the participants embark on a journey to become Cyber Warriors, who would possess the **requisite skills to Prevent, Detect and Respond** to the current, highly sophisticated and potent attack vectors.

These Cyber warriors would be a great asset to the governmental and private organisations to assist in keeping the critical IT assets safe and secure. These courses are being organized with Industry partners to ensure that the skills attained can be directly applied in their own organizations' current setups. The Cyber Range adds a lot of value to the course conduct as it presents hyper real network environments with real world attacks which participants detect and respond repeatedly. This helps them develop the requisite skill in addition to the knowledge and understanding and validate their existing processes. Given below is a broad overview of the three levels of Cyber Security Courses.

Cyber Security Courses

Training	Pre Requisite	Target Audience	Terminal Objective	Duration
Basic	This is an entry level course	Anyone/ End User/ Company Employee Basic Computer User	Understanding of the technical concepts and importance of proper detection mechanisms and prevention for Cyber security. Desktop security	05 Working Days / 01 Week
Intermediate	Basic Networking understanding	Information System Owners /Analysts/ Cyber Security Managers/ IT Engineer	Participants will be able to establish an industry acceptable hardening and pen testing concepts.	05 Working Days / 01 Week
Advanced	Sound knowledge of TCP/IP, Computer hardware knowledge	IS Security Officers Cyber Security Managers/Admins / IT Engineer	Confidently able to assess security loopholes. Visualize various cyber threats and select the correct response mechanism. Confident in configuration of various security appliances.	10 Working Days / 02 Weeks

Cyber Security Basic Level Program

The basic level course is suitable for individuals who handle sensitive data in any vertical of an organization. These may be managers or equivalent personnel and may or may not be from IT / security background. However, it is essential these days that these individuals have basic knowledge as well as the requisite skills to implement standard cyber security controls to combat the modern day attacks.

On completion, the participants would acquire the skills to harden their windows based machines right from the operating system level to the commonly used applications being used. They will gain visibility into the various attack vectors in a LAN environment and would be made aware of techniques to remain secure while surfing the web. An overview of Wi-Fi and mobile security including an understanding of the IT act is also a part of the curriculum to ensure that the participants get an overall understanding of the security domain.

Course Outline

Module 1 – Cyber Security Overview
Module 2 – Windows Hardening
Module 3 - Vulnerabilities and Threats
Module 4 - Application hardening and Security
Module 5 - Network Security
Module 6 - Social Engineering
Module 7 - Wireless Security
Module 8 - Mobile Security
Module 9 - IT Act
Module 10 – Audit, Compliance and Standards

Note:

- These would be conducted in a batch size of 25 to 30 participants.
- **The cost of the basic course is Rs 15000/- (Rs Fifteen thousand only) per participant exclusive of all taxes**.
- It is a hands on course and all participants are expected to get their personal laptops with a min specs with CPU: i3 and above, RAM: 4 GB and above.

Security Cyber Intermediate Level Program

As **Offense is the best form of Defence**, this Course helps the participants in imbibing the skills of an ethical hacker. These skills are essential as only after learning the techniques being employed by the real hackers, can one effectively assess their organization's own security posture.

The intermediate level Cyber Security course is well suited for individuals who handle sensitive IT networks and have a couple of years of IT / cyber security experience. They must have basic knowledge of networking protocols and security fundamentals. While undergoing this training program the participants would be given ample hands on exercises on simulated network environments and access to latest hacking tools to practice all the steps of the ethical hacking cycle from Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks. The course is modeled using a cyber-range thereby helping the participants acquire the skills in addition to the knowledge and understanding of the security domain.

Course Outline

Module 1 – Security Fundamentals	Module 9 - Hacking UNIX/Linux
Module 2 - Information Gathering	Module 10 - Exploitation Techniques
Module 3 - Detecting Live Systems	Module 11 – Pen Testing Wireless Networks
Module 4 – Enumeration	Module 12 - Networks, Sniffing, and IDS
Module 5 - Exploitation Techniques	Module 13 - Injecting the Database
Module 6 - Vulnerability Assessments	Module 14 - Attacking Web Technologies
Module 7 - Malware Goes Undercover	Module 15 - Project Documentation
Module 8 - Windows hacking	Module 16 - Pen Testing w/Power shell

Note:

- The training program would be conducted in a batch size of 20 to 30 participants
- **The cost of the intermediate level course is Rs 50,000/- (Rs Fifty thousand only) per participant exclusive of all taxes**.
- It is a hand on course and all participants are expected to get their personal laptops with min specs of i3 processor and 4 GB of RAM.
- The course can be conducted on campus as a residential course. The boarding and lodging expenses on actual would be extra in that case.

Cyber Security Advance Level Program

The advance level course is suitable for individuals who handle sensitive IT networks data centers, server farms security operational centers etc. It is understood that they have adequate experience in handling security incidents. They must have good knowledge of networking and security protocols and have basic knowledge of ethical hacking methodology.

This course helps the participants acquire the finer points of being a master penetration tester thereby being able to respond to vicious modern day attacks like DDOS, APT, ransom ware etc. They will be able to practice on complex simulated networked environments alive with high volume of business traffic and the standard perimeter security framework all of which would be created on a state of the art cyber-range. This hyper real environment would be attacked by using advanced Kali Linux tools, Metaspolit framework and other custom techniques and tools. The course would also include modules on web application attacks, bypassing firewalls and anti-virus applications.

This would give a thorough understanding of the pen test technique enabling the participants to acquire the skill of an offensive security professional and confidently fine tune their organisations security posture.

Course Outline

Module 1: Penetration Testing Fundamentals	Module 9: Buffer Overflow in Linux
Module 2: Deep Dive into Kali Linux	Module 10: Privilege Escalation
Module 3: My basic Tool Kit	Module 11: Client Side Attacks
Module 4: Passive snooping	Module 12: Web Application Attacks
Module 5: Active snooping	Module 13: Port Redirection and Tunneling
Module 6: Fine tune the VA process	Module 14: Understanding the Metasploit Framework
Module 7: Start with Exploits	Module 15: Bypassing Firewalls and Antivirus
Module 8: Buffer Overflows	Module 16: Final Reporting and Compliance
Module 17: Let's get Real: Hackathon	

Note:

- These would be conducted in a batch size of 15 to 20 participants
- **The cost of the advance course is Rs 75,000/- (Rs Seventy-Five thousand only) per participant exclusive of all taxes**.
- It is a hand on course and all participants are expected to get their personal laptops with min specs of an i3 processor with a min of 4 GB of RAM.
- The course can be conducted on campus as a residential course. The boarding and lodging expenses on actual would be extra in that case.