**Trainer Azhar Abbas (professional Information Security Analyst)**

**Course Title: Cyber Security (Cybersecurity Fundamentals with a Focus on SOC Operations)**

**Objective of Course:** To prepare the trainees to work as Information Security Professional in a wide variety of computer-related industries and has a strong emphasis on Network related problems.

**Duration 5 Months**

**LEARNING OUTCOMES**

As a result of the course, participants will acquire:

* Knowledge of computer security elements fundamentals
* Knowledge of computer access control
* Knowledge of security architecture
* Knowledge of technical measures for network and host security
* Knowledge of network management best practices
* Knowledge of physical protection role in computer security.
* Knowledge of securing networks, systems, servers and operating Systems with troubleshooting.
* Knowledge of the web attacks in modern day servers

|  |  |  |  |
| --- | --- | --- | --- |
| **Course Execution Plan:** 3 hours per week   |  | | --- | | **Total contact Hours :** 66 hrs. | | **Total Weeks :** 22 | | **Class Day :** Sunday | |

**TRAINING COURSE CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| Schedule week | Module Title | Learning Units | Remarks |
| 1st Week | Introduction | • Motivational Lecture  • Course Introduction  • Job market  • Institute/work ethics  • Introduction to Cybersecurity  • Objectives  • Roles  • What is Cyber security? | Assignment |
| 2nd Week | Basic Fundamental 1 | • Differences between Information security and cybersecurity.  • Why is Cyber Security Important?  • Prerequisites of Cyber security  • Lab Setup  • Virtualization and OS installations | Assignment |
| 3rd Week | Basic Fundamental 2 | • About Kali Linux  • Different flavor of Linux for Hacking and pen testing  • Current Security Landscape  • Common Security Principles | Assignment |
| 4th Week | Network & Security Layers | • TCP /IP Layers  • Security level Layers, Multilevel Security Layers  • Security Zones | Assignment |
| 5th Week | Network Security Parameters | • Network devices & Services  • Firewall  • VPN  • E-mail Analysis | Assignment |
| 6th Week | Basic Terminologies | • CIA Triad  • Common types of attacks | Assignment |
| 7th Week | SOC Fundamentals | • Introduction SOC Environment  • SOC Types and Roles  • SOC analyst responsibilities | Assignment |
| 8th Week | SOC Part 2 | • SIEM and Analyst relationship  • Log Management | Assignment |
| 9th Week | SOC Part 3 | • Windows Geology  • Windows Attack  • Active Directory | Assignment |
| 10th Week | SOC Part 4 | • DNS Flow  • Proxy Flow  • Phishing Email Analysis | Assignment |
| 11th Week | SOC Part 5 | • SIEM Introduction  • SIEM Architecture  • EPP vs EDR vs XDR | Assignment |
| 12th Week | SOC Part 6 | • Tools Knowledge (Waf, NDR, Defender, FireEye, Carbon black ,Crowd strike etc.) | Assignment |
| 13thWeek | SOC Part 7 | • Malware Analysis  • Sandboxing tools (VT, MX-tool) | Assignment |
| 14th Week | SOC Part 8 | • Mitre and Tactics frame work  • Web Attacks  • Investigate web Attacks | Assignment |
| 15th Week | SOC Part 9 | • Windows Events ID  • Firewall event ID  • Kerberos vs NTLM Authentication | Assignment |
| 16th Week | SOC Part 10 | • Common Ports  • Secure and Insecure ports | Assignment |
| 17th Week | SOC Part 11 | • Cyber Kill chain  • Escalation of incident/Investigation and process | Assignment |
| 18th Week | SOC Part 12 | • Audit & Governed  • IS framework | Assignment |
| 19th Week | SOC Part 13 | • Symmetric & Asymmetric Encryption  • Social Engineering attacks | Assignment |
| 20th Week | SOC Part 14 | • Workflow of incident  • Incident Reporting tools | Assignment |
| 21st Week | Interview | Preparation |  |
| 22nd Week |  | Mock Interview  Question & Answers or Quires (Exam) |  |