CERTYBOX™
SKILLS FOR TOMORROW

CYBER SECURITY

COURSE CURRICULUM

Module 1 – Understanding Security Threats

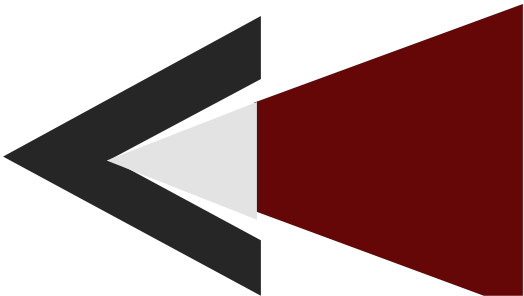
- Capture FTP and HTTP Traffic
- Lessons Learnt
- Understanding the Attack Surface
- Network Hardening Explained
- Demilitarized Layer
- Threats vs Vulnerabilities vs Risks
- Top Security Threats
- Types of Attacks
- Physical Security
- Social Engineering
- The Importance of the Corporate Security Policy
- Password Protection Policies
- Why Never to Ask an Admin for Favors
- Practical Exercise

Module 2 – Protecting your Information

- Security on the Road
- E-mail Security
- How to Handle Sensitive Data
- When and What to Share
- BYOD and IoT
- Wireless Networking Challenges
- Posting on Social Media
- Importance of Security Programs
- Employee Training, Awareness, and Advocacy
- Balancing Up-Front Costs vs Downtime in the Future
- Convenience vs Security
- Practical Exercise

Module 3 – Session & Risk Management

- Assets,Threats and Vulnerabilities
- Risk Management
- Map Risks to Risk Treatments
- Deploy User Account Security Settings
- User Account Management
- HTTP Session Management
- Configure SSL and TLS Settings
- Mobile Device Access Control
- Data Confidentiality



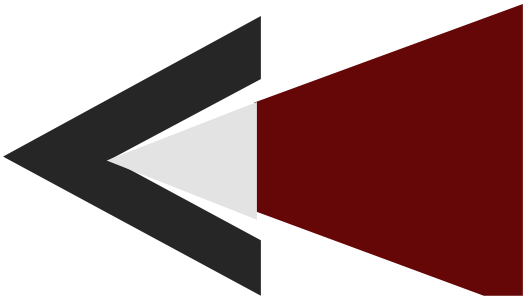
- Implement Encryption for Data in Motion
- Implement Encryption for Data at Rest
- Practical Exercise

Module 4 – Auditing & Incident Response

- Security Auditing and Accountability
- Enable Windows File System Auditing
- Conduct a Vulnerability Assessment Using Windows
- Conduct a Vulnerability Assessment Using Linux
- Mobile Device Access Control
- Configure Mobile Device Hardening Policies
- Enable a Smartphone as a Virtual MFA Device
- Securing Applications
- Implement File Hashing
- Incident Response Planning
- Examine Network Traffic for Security Incidents
- Practical Exercise

Module 5 – Network Architecture and Reconnaissance

- OSI Model
- Network Hardware
- IPv4
- IPv6
- TCP and UDP
- Use common Windows TCP/IP utilities
- Use common Linux TCP/IP utilities
- Network Services
- Configure and Scan for Open Ports
- Wired and Wireless Networks
- Use Common Wireless Tools
- Internal and External Networks
- Topology, Service Discovery, and OS Fingerprinting
- Packet Capturing
- Network Infrastructure Discovery
- E-mail and DNS Harvesting
- Social Engineering and Phishing
- Cloud Concepts
- Cloud Service Models
- Virtualization
- Cloud Security Options
- Acceptable Use Policy
- Data Ownership and Retention Policy



- Data Classification Policy
- Password Policy
- Practical Exercise

Module 6 – Threat Identification

- Threat Overview
- Threat Classification
- Personally Identifiable Information
- Payment Card Information
- Intellectual Property
- Data Loss Prevention
- Prevent Data Storage on Unencrypted Media
- Scope of Impact
- Stakeholders
- Role-based Responsibilities
- Incident Communication
- Host Symptoms and Response Actions
- Network Symptoms and Response Actions
- Application Symptoms and Response Actions
- Incident Containment
- Incident Eradication
- OEM Documentation
- Network Documentation
- Incident Response Plan/call list
- Incident Documentation
- Chain of Custody Form
- Change Control Processes
- Types of Reports
- Service Level Agreement
- Memorandum of Understanding
- Asset Inventory
- Practical Exercise

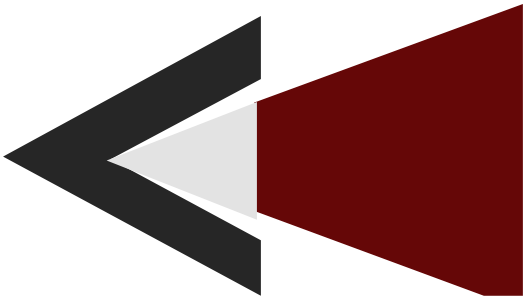
Module 7 – Threat Mitigation

- SDLC Phases
- Secure Coding
- Security Testing
- Host Hardening
- Patching Overview
- Use SCCM to Deploy Patches
- File System Permissions
- Network Access Control

- VLAN
- Determining Resource Access
- Honeypots
- Jump Box
- IT Security Governance
- Regulatory Compliance
- Standards and Technology
- International standards for organisation
- ITIL
- TOGAF
- Logical Controls
- Physical Controls
- Configure Router ACL Rules
- Administrative Controls
- Compensating Controls
- Continuous Monitoring of Controls
- Hardware Trust
- Penetration Testing
- Practical Exercise

Module 8 – Reducing Vulnerabilities

- Cryptography Primer
- Symmetric Cryptography
- Asymmetric Cryptography
- Public Key Infrastructure
- Request a PKI Certificate from a Windows CA
- Use Windows EFS File Encryption
- Fingerprinting and Hashing
- File Hashing in Linux
- File Hashing in Windows
- Authentication
- Configure Multifactor Authentication for VPN Clients
- Authorization
- RADIUS, TACACS+
- User Provisioning and Deprovisioning
- Identity Federation
- Server Vulnerabilities
- Endpoint Vulnerabilities
- Network Vulnerabilities
- Mobile Device Vulnerabilities
- Vulnerability Scanning Overview
- Vulnerability Scanning Settings



- SCAP
- Scan for Vulnerabilities using Nessus
- Common Vulnerability Scanning Tools
- Scan for Vulnerabilities using Microsoft Baseline Security Analyzer
- Review Vulnerability Scan Results
- Vulnerability Remediation
- Practical Exercise

Module 9 – Investigate Security Incidents

- Firewalls
- Detecting Intrusions
- Malware
- Digital Forensics
- Practical Exercise

Module 10 – Monitoring for Security Issues

- Hiring and Background Checks
- User Onboarding and Offboarding
- Personnel Management Best Practices
- Threats, Vulnerabilities, and Exploits
- Spoofing
- Packet Forgery using Kali Linux
- Impersonation
- Cross-site Scripting
- Root Kits
- Privilege Escalation
- Common Exploit Tools
- Exploring the Metasploit Suite of Tools
- Exploring the Kali Linux Suite of Tools
- Password Cracking
- Common Monitoring Tools
- Linux OS Monitoring Tools
- Windows OS Monitoring Tools
- Windows Event Log Forwarding
- SIEM
- SCADA and ICS
- Monitoring Network Bandwidth
- Analyzing Reconnaissance Results
- Practical Exercise