| Training | Course Overview | Who Should Attend | Course Outline | Event Info |
| --- | --- | --- | --- | --- |
| Penetration testing training | ACIC’s Penetration Testing training teaches the methodologies, techniques, and tactical tools of modern adversaries. This course is uniquely designed to meet local use cases such as ATM attacks, Mobile attack and starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, web app manipulation, and attacking the Windows domain, with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the best penetration testers to help you do your job safely, efficiently...and with great skill. | * ICT teams * System Admins * Database Administrators * Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities * Penetration testers * Defenders who want to better understand offensive methodologies, tools, and techniques * Auditors who need to build deeper technical skills. * Red Team members * Blue Team members * Forensics specialists who want to better understand offensive tactics | See below | **Title of the Course:**  Penetration Testing  **Training Duration:**  5 Days  **Training Timing:**  8:30 AM to 4:30 PM  March, Kenya (18 - 22nd)    May, Nigeria (18-22nd) |
| Certified Ethical Hacking (C|EH v10) | **C|EH** is the world’s most advanced ethical hacking course covering 20 of the most  important security domains any individual will need when they are planning  to beef-up the information security posture of their organization. The course  provides hacking techniques and tools used by hackers and information security  Professionals.  **Why this course?**  • Over 140 labs that mimic real scenarios  • Over 2,200 commonly used hacking tools to immerse you in the hacker world  • Over 1,685 graphically rich, specially designed slides to help you grasp complex security concepts in depth | * ICT teams * Infrastructure * System Admins * Database Administrators * Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities * Penetration testers * Defenders who want to better understand offensive methodologies, tools, and techniques * Auditors who need to build deeper technical skills. * Red Team members * Blue Team members   Forensics specialists who want to better understand offensive tactics | **Day 1**   1. Introduction to Ethical Hacking 2. Foot printing and Reconnaissance 3. Scanning Networks 4. Enumeration   **Day 2**   1. Vulnerability Analysis 2. System Hacking 3. Malware Threats 4. Sniffing 5. Social Engineering   **Day 3**   1. Denial-of-Service 2. Session Hijacking 3. Evading IDS, Firewalls, and Honeypots 4. Hacking Web Servers   **Day 4**   1. Hacking Web Applications 2. SQL Injection 3. Hacking Wireless Networks 4. Hacking Mobile Platforms   **Day 5**   1. IoT Hacking 2. Cloud Computing 3. Cryptography | **Title of the Course:**  Certified Ethical Hacking and Countermeasures  Version:  10  **Training Duration:**  5 Days  **Training Timing:**  8:30 AM to 4:30 PM  Location and Dates:  February, 24th-28th- Nairobi Kenya  June, 25th - 29th- Nairobi Kenya  September, 24th – 28th- Nairobi Kenya |
| Cyber Defense and Network Security | This training is focused on improving the blue-teaming capabilities of the attendees to allow them detect and respond to network attacks in a timely manner. Candidates will be required to perform practical blue-teaming exercises to successfully complete the course. Successful candidates will be provisioned with their certificate and will gain Cyber Immersion Club membership. | * ICT teams * Infrastructure * System Admins * Database Administrators * Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities * Penetration testers * Defenders who want to better understand offensive methodologies, tools, and techniques * Auditors who need to build deeper technical skills. * Red Team members * Blue Team members   Forensics specialists who want to better understand offensive tactics | **Day 1**  Network Packet Analysis  **Day 2:**  Malware Analysis  **Day 3:**  Log Monitoring and Analysis  **Day 4:**  Red team/Blue Team  **Day 5:**  Forensic Analysis | **Title of the Course:**  Cyber Defense and Network Security  **Training Duration:**  5 Days  **Training Timing:**  8:30 AM to 4:30 PM  **Location and Dates:**  August, 17th-21st, Mauritius |
| Risk Quantification and Exposure Analysis | Course Summary  Are you struggling to measure and communicate your current cybersecurity risk posture in monetary terms? This workshop will enable ICT, Audit, Operations and Risk Management professionals to provide ExCo, the Board and regulators with objective, quantifiable and observable cyber security metrics to enable key stakeholders to make strategic decisions.  Serianu Limited is pleased to invite you to a 5-day workshop that will guide you on measuring and quantifying cybersecurity risks.  Objectives   1. Understand how to define, develop, maintain and communicate an effective risk profile and appetite statement to ExCo and Board members. 2. Discuss new holistic, risk-based, business-driven approach to measure, benchmark and track maturity of your cybersecurity program. 3. Understand how to develop cyber risk metrics that are quantifiable, observable, and objective data supporting metrics. This will involve the use of metrics to facilitate decision making and improve performance and accountability. 4. Discuss how to determine an organization’s cyber risk tolerance level using the organizations current risk investments and potential exposure or losses. | ICT and Information Security Professionals  Risk Management and Audit Officers  Legal and Compliance Officers  Finance and Strategy Managers | See Below | **Title of the Course:**  Cyber Risk Quantification and Exposure Analysis  **Training Duration:**  5 Days  **Training Timing:**  8:30 AM to 4:30 PM  **Location and Dates:**  March, 23rd-27th, Botswana  April, 6th -10th, Kenya  May, 11-15th, Tanzania  June, 22-25th, Ethiopia  July, 6th-10th, Nigeria  September,21 -25th Tanzania  October 12th-16th, Botswana  November,9th -13th, Kenya |
| Operating and managing SIEM |  | Security Analyst  Security Architects  Senior Security Engineers  Technical Security Managers  SOC Analysts  SOC Engineers  SOC Managers  CND Analysts  Security Monitoring  System Administrators  Cyber Threat Investigators  Individuals working to implement Continuous Security Monitoring or Network  Individuals working in a hunt team capacity | **Day 1:**   * SIEM Introduction: Log types and collection * SIEM Correlation: Normalization and Parsing of events   Day 2   * Incident Review: Incident Notification and Correlation   Day 3   * Reporting and Dashboards * Breach Scenario  and Use cases | **Title of the Course:**  SIEM Training  **Training Duration:**  3 Days  **Training Timing:**  8:30 AM to 4:30 PM  **Location and Dates:**  April, 15-17th, Kenya  October, 7th- 9th, Kenya |
| Business Managers Masterclass | This is a 2-day in class course that prepares non-technical business managers to understand, assess and take a proactive posture in cyber security. Along the way, attendees investigate risk assessment and management frameworks that help mitigate the risks, as well as identify potential security gaps that could prove a liability. This course enables non-technical business managers to address and handle the threats from emerging cyber security advances that can decimate an organization. | Human Resource Managers  Procurement Managers  Operations Managers  Legal Teams  Finance teams | **Day 1:**  Cybersecurity Risk and Trends facing organisations  How to work with millennials to get the most productivity and efficiency out of them  Legal ins & outs of human resource  **Day 2:**  Fraud:  Bridging the Gap - Employing Fraud Risk Assessment to Guide Investments in Fraud Mitigation  Integrating anti-fraud controls with internal frameworks  **Day 3:**  Contract and Procurement Fraud  Fraud schemes pre, during and post procurement  Frauds relating to contracting and contract management  Role of internal audit in preventing and detecting procurement fraud  Third-Party Relationships and the Associated Frauds | **Title of the Course:**  Masterclass for Business Managers  **Training Duration:**  3 Days  **Training Timing:**  8:30 AM to 4:30 PM  **Location and Dates:**  April, 8th-10th, Kenya  July, 1st-3rd, Nigeria |
| Exco/Board Training | The objective of this course is to provide Senior Executives and Board members with a thorough and operational knowledge of information security so that this critical area is recognized as a management issue and not an IT issue. In this workshop, CEOs and Board Directors will get first-hand information on how companies are managing their information security risk and building secure organizations in the face of more sophisticated attacks. The course will be undertaken using a moderated roundtable format with panel discussions and structured breakouts. | Executives  Board Members | At the end of this course, participants will be able to:   1. Understand information security and emerging threats. 2. Identify governing bodies and legislative drivers for protecting information security. 3. Understand an executive’s role and responsibilities in the areas of information security and privacy. 4. Get an understanding of the changing Risk Landscape 5. Explain the role of Senior management in information risk management 6. Understand your organization’s Information risk management maturity level. | On demand |
| End User Training | The EndUser Training Content Series is the latest in cyber security training for employees.  Equipped with a variety of brand-new Training Content Styles and fresh updates to our existing computer-based training styles, we evoke engagement of every employee, regardless of their comprehension level through dynamic, effective training content, teaching best-in-class security behaviors.  The expertly created, comprehensive suite of cyber security awareness training for employees will help you build a powerful program that embodies your organization’s needs and learning levels.  We’ve taken the guesswork out of building a program to suit your organization’s specific culture.**Training can be crafted into a custom mix of training to cover the relevant awareness topics and can be hosted on nearly any platform.** | All Employees | 1. You are a Target 2. Password Security 3. Physical Security 4. Business Email Compromise 5. Social Engineering Attacks Identification and Countermeasures 6. Cyber Vigilance | **Title of the Course:**  End user Training  **Location: Onsite, Online**  **Time:** On demand |

Penetration Testing Course Outline

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DAY 1 | DAY 2 |  | DAY 3 | DAY 4 | Day 5 |
| NETWORK PENETRATION TESTING (RECONNAISANCE) | NETWORK PENETRATION TESTING  (WIRELESS AND PASSWORD ATTACKS) |  | APPLICATION PENETRATION TESTING (MOBILE/WEB/APIs) | MOBILE APPLICATION ASSESSMENT | CLASS WRAP UP,  PRESENTATION OF CERTIFICATES AND  LOCAL TOURISM |
| Understanding your target: Penetration Testing Planning   * The Mindset of the Professional Pen Tester * Building an Effective Cost Efficient Pen Test Infrastructure | Understanding secure network design and architecture   * Designing secure networks with a defense in depth approach |  | Understanding secure application architecture   * Most common web technologies and related inherent risks that they bring to web applications * API Security and Testing | Understanding secure application architecture with a focus on most common attack vectors.  - Client software running on the mobile device  - Communications channel  - Server side infrastructure |
| Understanding your target: A focus on Reconnaissance   * Detailed Recon Using the Latest Tools * Mining Search Engine Results * Document Metadata Extraction and Analysis | Wireless and Password Attacks   * An introduction to John the Ripper and Cain * Wireless Attacks * Password cracking and sniffing attacks. |  | Identifying Web Application Vulnerabilities with Nikto and other web assessment tools  Web application pen testing, covering the most common web application attack techniques. | Preparing The Test Environment.  Assessing Mobile application using state-of-the-art techniques. |  |
| Cyber-Range Exercises   1. Hands-on labs covering data analysis to enable us obtain sensitive information about a target environment 2. Using Recon-ng to plunder a target's DNS infrastructure and online presence. | Cyber-Range Exercises   1. Cracking passwords and sniffed Windows authentication messages. 2. Rainbow Table Attacks with Ophcrack 3. Pass-the-hash attacks. |  | Cyber-Range Exercises   1. Leveraging Command Injection Flaws 2. Exploiting SQL Injection Flaws to Gain Shell Access of Web Targets | A Focus on Understanding Cyber Measurements and  Metrics |  |

Risk Quantification Content

**Lesson 1: Cybersecurity Trends, Risk Profiling and Appetite**

Introduction

* Emerging Trends
* Threat Actors and their Motives
* Top Risks
* Cause and Effect Matrix
* Top Priorities for African Organizations

Cyber Risk Profiling

* The Inherent Risk Profile
* Categories of the Inherent Risk Profile
* Measuring the Risk
* Measuring Overall Inherent Risk Profile

Cyber Risk Exposure Analysis

* Governance and Processes around Cyber Risk Appetite
* Preparing, Reviewing and Reporting the Cyber Risk Appetite Statement
* Risk Appetite Framework Metrics

Introduction to Cyber Visibility and Exposure Quantification (CVEQ)

**Lesson2: Cybersecurity Benchmarking and Maturity Assessments**

Introduction

* Cybersecurity Frameworks
* Cyber Visibility & Exposure Quantification (CVEQ)
* Benchmarking using CVEQ
* Weighted Score
* Maturity Assessment using CVEQ
* Calculating Cybersecurity Maturity
* Meeting compliance needs with CVEQ Framework
* Domain 1: Cybersecurity Risk Management
* Domain 2: Cybersecurity Asset Management
* Domain 3: Cyber User Management
* Domain 4: Cyber Incident Management
* Domain 5: Cyber Continuity Management

**Lesson3: Visibility and Exposure Analysis**

Introduction

* Visibility Controls
* Testing of Controls – Existence, Completeness, Timeliness, Reporting

Exposure Analysis

**Lesson 4: Monitoring and Analysis**

Introduction

* Introduction to Incident Monitoring and Analysis (Static and Dynamic)
* Static Analysis in the SOC
* Dynamic Analysis in the SOC

**Lesson 5: Risk Tolerance and Prioritization**

Introduction

* Using Exposure to Calculate Risk Tolerance
* Mapping and Weighting of Exposures to CVEQ Visibility Controls
* Calculating Cyber Risk Tolerance

**Lesson 6: Reporting to the Board and Exco**

Introduction

* Introduction to stakeholder reporting
* Reporting to the Board and Exe. Comm (Exco)

Cybersecurity Scorecard

* Inherent Risk Profile Statement
* Risk Appetite Statement
* Benchmarking and Maturity Statement
* Visibility Statement
* Deficiency Statement
* Breach Exposure Statement
* Incident Trending Statement