Cell-cyber

Upskill your cyber security workforce today to overcome the challenges of tomorrow

We help organisations enhance their cultures of cyber safety by providing access to cutting-edge, live-fire simulated training.

Capability Statement

Cell-cyber

Document Control

This document has been prepared by Cell Cyber Security Pty Ltd.

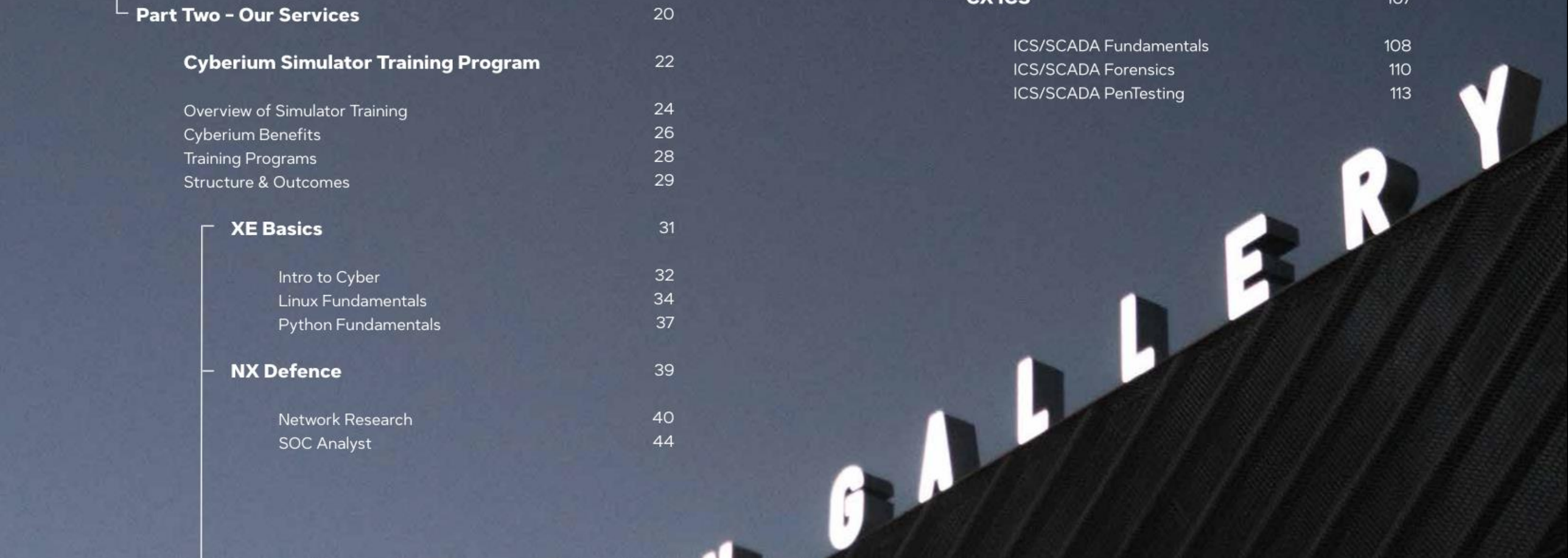
Version: Issue 1
Approved by: Uzy Samorali
Date: 08/07/2021

Contact

Uzy Samorali
Co-Founder / Managing Director

Cell-cyber

Contents



Executive Summary

Thank you for your interest in us . We are pleased to introduce you to our team, products and capabilities in this document and are grateful for this opportunity to collaborate with you and your organisation.
Ioti is a specialist Australian cybersecurity training and software provider helping digitally enabled organisation's to effectively reduce IT RTO, build strong cybersecurity safety cultures and improve resiliency to defend against emerging threats.

Offering a comprehensive suite of cybersecurity products, courses, content and simulated training programs, our learning pathways are designed for both technical and non-technical participants, delivered digitally and on-demand.

We're proud to be the only cybersecurity training provider in Australia delivering mission-critical, cutting- edge and Israeli-led simulator-based training designed to upskill personnel against the latest, rapidly evolving threats.

Unlike traditional Universities and Registered Training Organisation's in Australia, our training isn't delivered by academics; it's led by highly experienced Israeli domain experts on the frontline of Israel's cybersecurity threat defence.

Our specialism is your strength. Our unique suite of products and services offer clients a comprehensive and cutting-edge set of tools, training and capability required to secure their business.

We're driven by a services-first ideology focused on people, process and disruptive technology to deliver value and confidence for our clients. Our difference goes deeper than 'what we do'. It's a belief system around which we identify and deliver innovative capabilities and disruptive emerging technologies in order to effectively defend against new and improved cyber-attacks. We're looking forward to collaborating with you and your team to enhance cyber hygiene and build a sustainable culture of safety within your organisation.

Kind Regards,

Uzy Samorali
Director

PART

01

OUR COMPANY

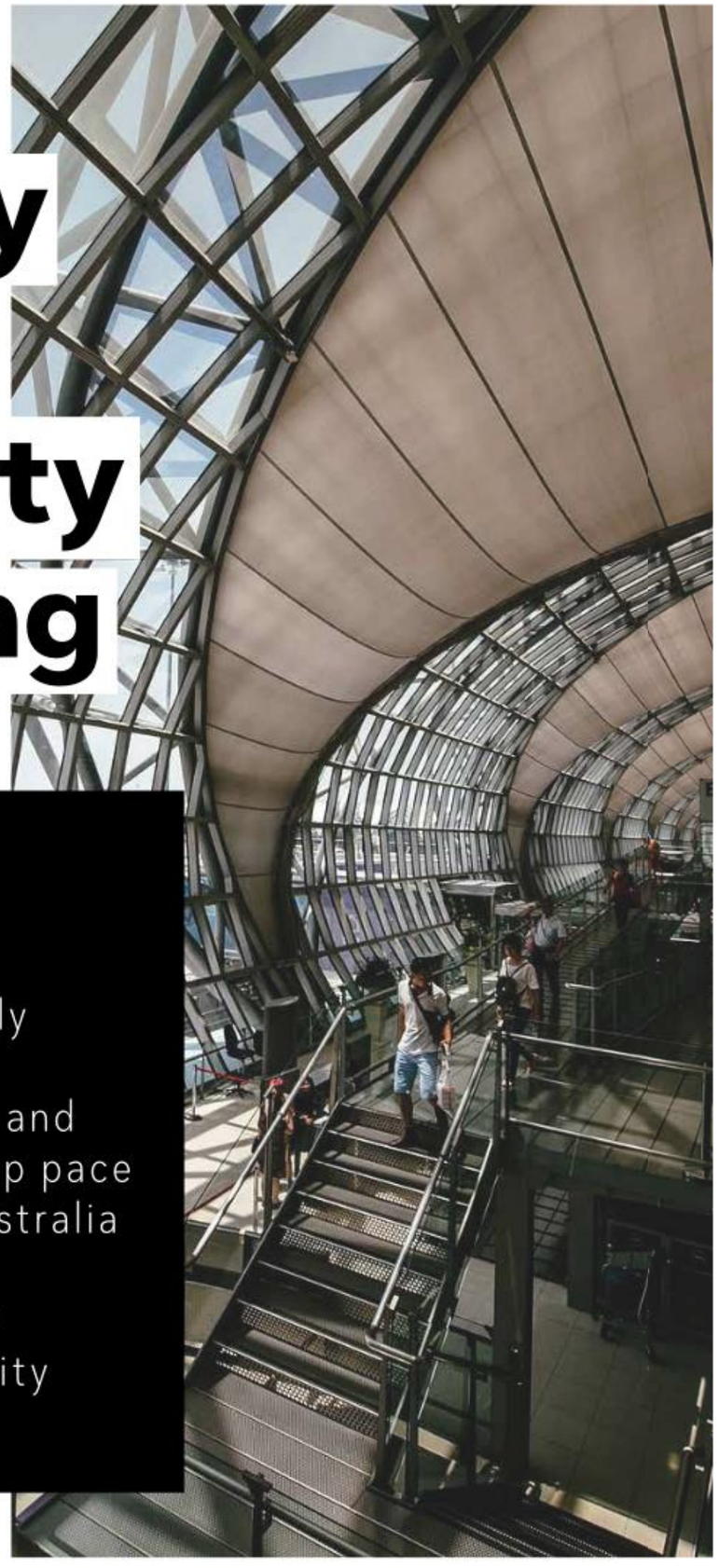
Our Mission

We're on a mission to help organisation's enhance their culture of safety by improving access to cutting edge cybersecurity training.

Covid-19 accelerated adoption of new technology to mitigate and manage the impact of the pandemic. This shift created opportunities and unearthed new cybersecurity threats. Business continuity will increasingly depend upon an embedded safety culture that has a capability to identify and address evolving and dynamic cybersecurity threats.

In Dire Need of

Quality Cyber Security Training



Cyber threats are becoming more sophisticated and evolving too rapidly for traditional training providers and universities to keep pace at a time when Australia is facing a critical shortage of highly skilled cybersecurity professionals.

Recent studies estimate that the average financial impact of a data breach is about $3.8 million, and enterprise level companies can be between 10x - 100x that sum. COVID-19 and the subsequent acceleration of digital transformation has only exacerbated cyber risk for organisation's while also increasing the number of potential attack vectors being exploited by cybercriminals to target organisations.

$30 - 300m

The average financial impact for enterprise resulting form data breach.

$3.8m

The average financial impact for SME's resulting from data breach.

Top #3 threats

Malware, Web-based attakcs and Phishing attacks are becoming more common.

Covid-19

Accelerated tech adoption and significantly increased the risk of cyber attack.

Who Is CellCyber Security?

We offer on-demand access to leading Israeli cybersecurity specialists deployed to provide first-hand, cutting-edge and simulator-based training to rapidly upskill organisations' existing

cyber security personnel against the very latest, rapidly evolving cybersecurity threats.

We are the only cybersecurity education provider in Australia delivering mission-critical and cutting edge training and professional development led by highly-trained career specialists who are actively engaged in Israel's cybersecurity threat defence.

We're different from traditional Universities and Registered Training Organisations (RTO's) in Australia. Our training isn't delivered by academics; it's led by leading Israeli domain experts experienced on the frontline of Israel's cybersecurity threat defence.

Tailored Courses

Non-generic course content. Our trainers tailor material by industri and organisational need.

Safety Culture

Training quality is about building a culture of safety, not simply focusing on the latest technology.

Israeli Trainers

Learn first-hand from leading specialists engaged in Israeli's cyberwarfare threath defence.

Cutting Edge Material

Threat risk and reliable countermeasures are evolving in real time. Our content is relevant and mission critical.

Why Our Capability is Israeli-led

As a nation living under constant threat of cyberwarfare, Israel recognises that the most critical ingredient in an effective cybersecurity threat defence capability is its people and they have invested extensively in world leading research and education, beginning in middle school and culminating in six university research centres dedicated solely to cybersecurity.

Extremely adverse geo-political circumstances have forced Israel into becoming a cybersecurity powerhouse; boasting the world's leading training institutions and dedicated universities, high-growth cyber security start-ups and the battle-tested domain experts.

Home Grown Capability Building

Australia's cybersecurity skills shortage is most critical within crucial senior and specialist levels needed to build the nation's future capability.

Australia is facing a critical shortage of highly skilled cybersecurity professionals, with an additional 17,000 personnel expected to be needed by 2026.

we provide access to a pool of the leading cybersecurity professionals in Israel to enable organisations to invest in upskilling their workforce, build sustainable cultures of safety and mount a credible threat defence.

Australian cybersecurity personnel and capability is growing. Our academic institutions are producing new cybersecurity graduates each year, however, we're critically lacking highly experienced cybersecurity specialists, in senior roles, who can lead and develop our nation's future technical talent. At Cell cybersecurity our objective is to play a critical role in levelling up Australia's cybersecurity capability, promote the development of home grown technical talent and build a sustainable community for cybersecurity personnel in Australia.

Connective Tissue
How we're Building Capability

By providing access to a pool of senior cybersecurity professionals in Israel, Ioti is aiming to accelerate the development of cybersecurity action plans and the development of safety cultures within organisations as they undertake expansive digital transformation post-COVID-19.

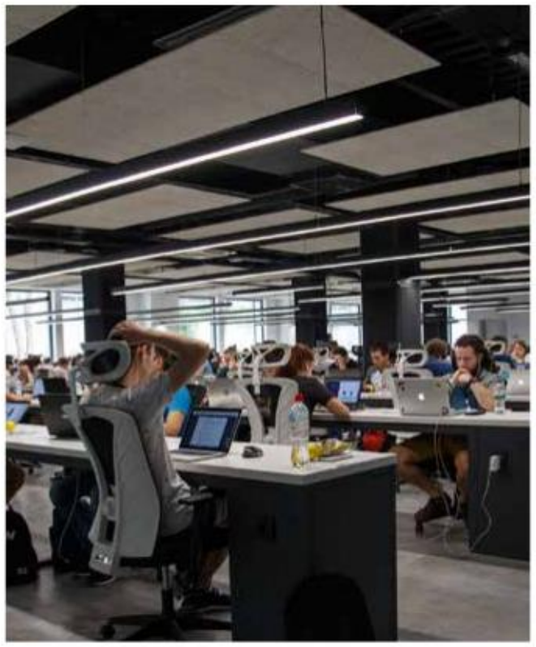
Skills Development
How we're Building Capability

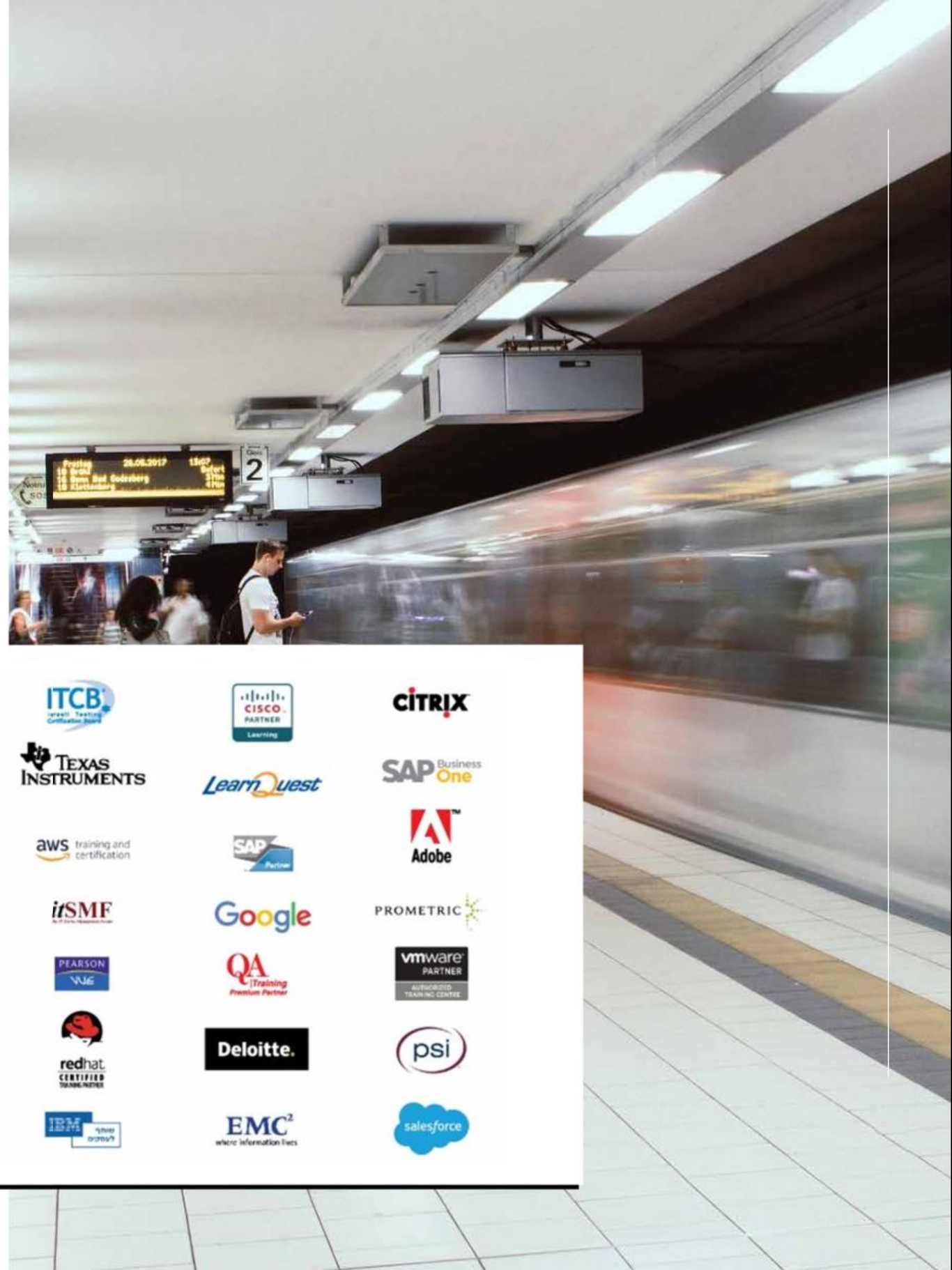
By accelerating growth and development of cybersecurity within organisations, we will play a leading role in developing the next generation of home grown professionals leading the next wave of our national threat defence and turn Australia into a cybersecurity powerhouse.

Track Record

Our cohorts of Israeli experts are already training the world's leading brands to improve cyber hygiene and build sustainable cultures of safety.

our cohort of Israeli trainers are working with many of the world's leading companies to develop and enhance internal cybersecurity capabilities and support the development of enduring cultures of safety within the organisation.





PART

02

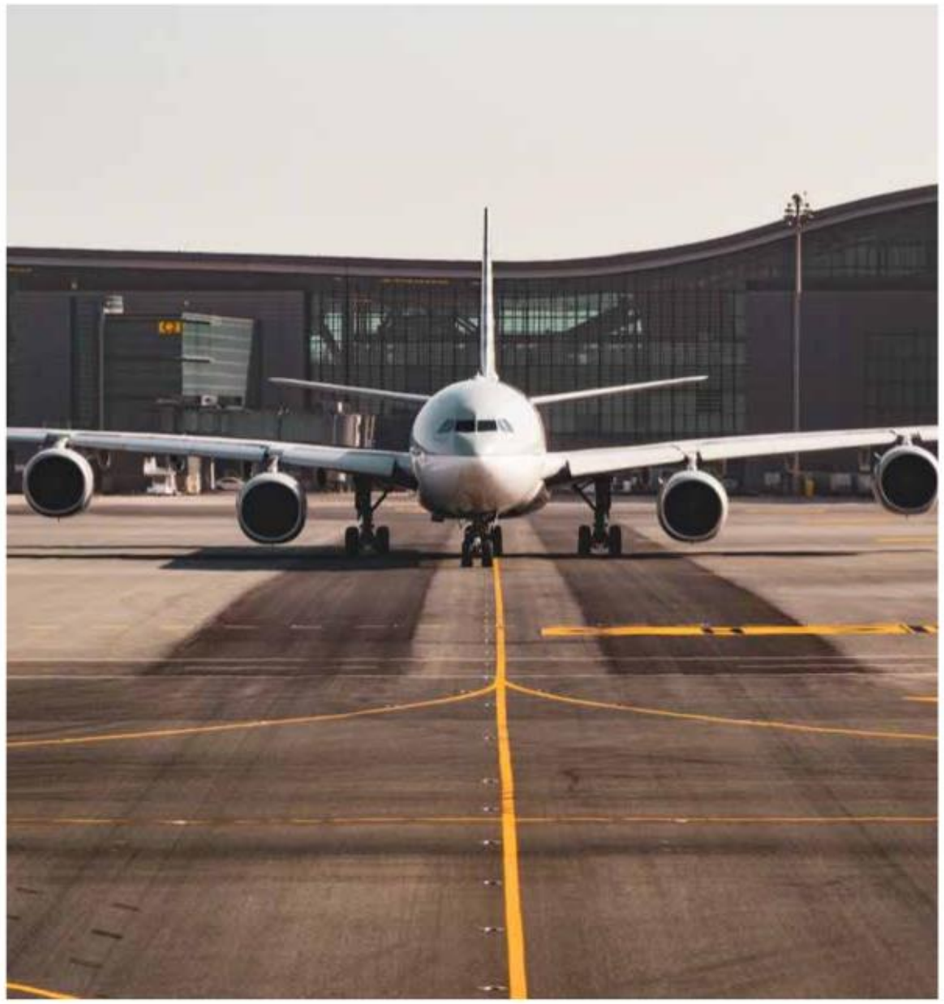
OUR SERVICES

Training & Professional Development

Offering a comprehensive suite of cybersecurity courses, content and simulated training programs with learning pathways designed for both technical and non-technical participants, delivered digitally and on-demand.

Our trainers have extensive civil and military cybersecurity operational experience and offer unparalleled insight and understanding of cutting-edge tools, technologies and strategies to design, implement and manage an effective threat defence for your organisation.

Our clients benefit from on-demand access to a pool of world-class, highly trained cybersecurity experts to complement and cover technical training capability not currently met by local providers.



Cyberium Simulator Training Program

Training within Cyberium enables students to develop high-level cybersecurity expertise.

Overview

Cyberium is a high-end cybersecurity simulator which trains students in the use of a wide variety of online tools for identifying the nature of a cyber-attack and responding quickly and appropriately to prevent damage and disable the attacker.

Students also learn how to identify potential vulnerabilities in their organisation's network, so they can be addressed before an attacker has a chance to exploit them.

Once students have familiarized themselves with these tools and their use they move on to simulated "real-life" attacks, many of them based on actual incidents. The challenge is to thwart an attack in its earliest stages before it has done any significant damage to the organisation's network.

Training within Cyberium enables students to develop high-level cybersecurity expertise and to maintain their edge via regularly updating and sharpening their knowledge and skills in this ever-changing field via training scenarios that are designed to reflect the most current cybersecurity challenges.

Benefits

Cyberium is a high-end cybersecurity simulator focused on cybersecurity training. The simulator offers a diverse series of live-fire scenarios where students can learn, train and enhance their skills and capabilities. Each training course has full scenarios with a set of problems and issues they will face in the real world including labs and class materials implemented within the simulator.

Students will learn the components and architecture, the latest

threat information, and how to penetrate the ICS/SCADA system. Actual field devices and ICS/SCADA simulations will be utilized to teach zero-day vulnerabilities found on ICS/SCADA related products and how to find zero-day vulnerabilities.

What Makes the Simulator Unique?

The simulator does not have the visual flash of a computer game. We are not training participants to be gamers. Our approach is serious and purpose-driven. We are developing skills and teaching techniques in order to produce cybersecurity professionals who can cope with rapidly emerging challenges.

The simulator is focused on cyber issues of operations technology and cyber risks. It is through these scenarios that participants are trained. Each scenario has a set of problems, featuring various servers and networks to expose participants to the variety of issues they will face in the real world.

Real-life scenarios provide participants with actual past or possible situations from cybersecurity or cyberterrorism to solve.

Unlimited Parallel Classes

Cyberium cutting-edge technology allows unlimited use of labs and scenarios.

Smart Record

Saves individual student progress.

Scenario Creator

Create additional scenarios and give your team unlimited scenario permutations.

Traffic Generator

Network traffic is being generated according to the scenario.

On-site or Cloud-based

Supports both on-site and cloud-based operations.

IT & OT Simulator

The unique advantage is custom -designed ICS/SCADA models that mirror a company's working environment.

Dynamic Systems

Systems are being generated automatically, allowing the trainer to set a different environment for the trainees.

Training Programs

The simulator offers a 360 degree solution, including labs, books, reports, projects, and international certifications preparation. Cyberium is a high-end simulator focused on cybersecurity training issues such as cyber-attacks and operations technology; through these scenarios, participants can learn within a dynamic, live-fire environment.

Structure & Outcomes

Coursebooks

The coursebooks accompany the lecturers and students alike in cybersecurity studies. The books have been adapted to the learning processes and allow the student additional help during and after the training and are accessed via the simulator.

Labs

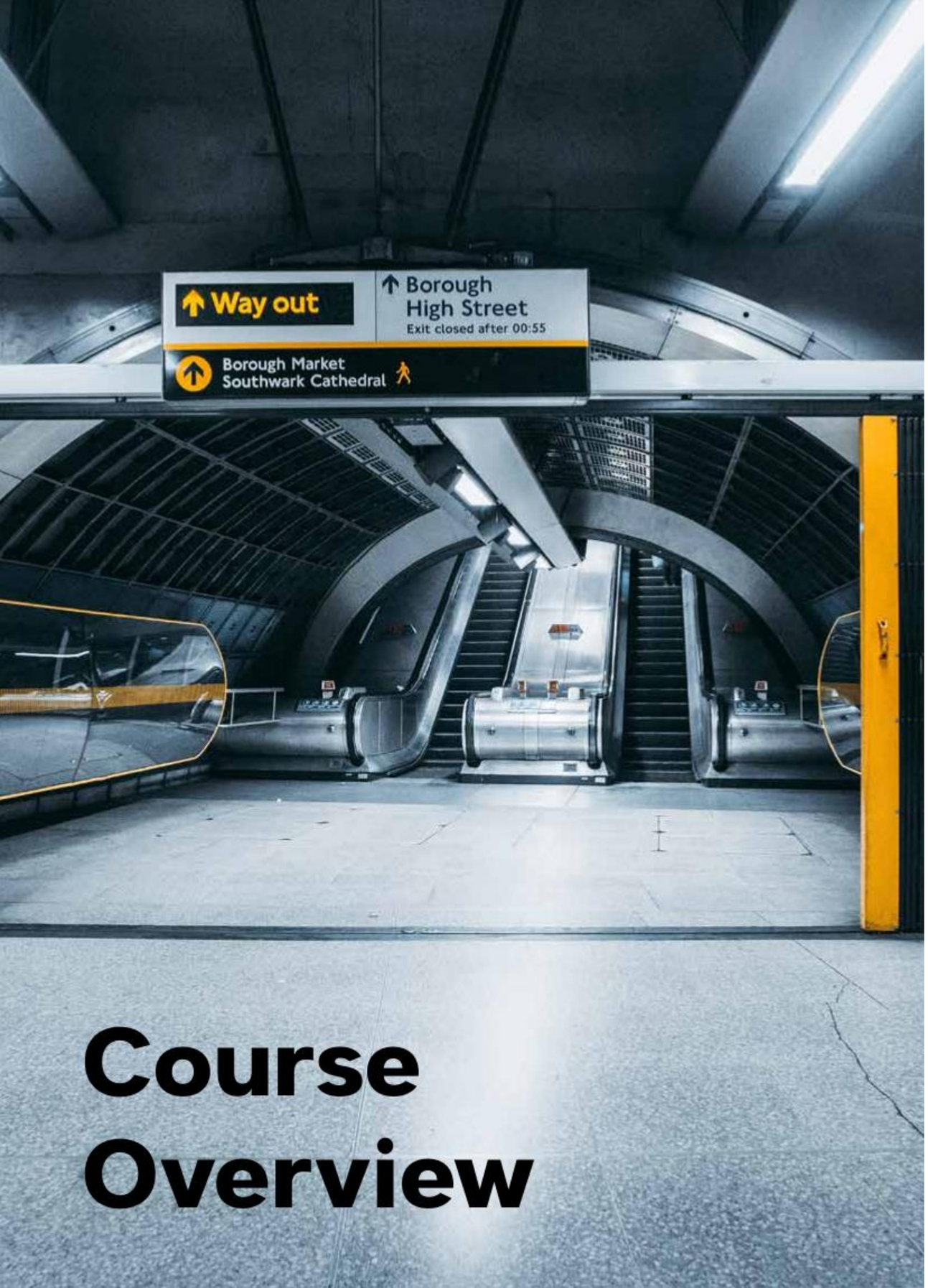
The labs hold questions and tasks to support the training, and students can track their progress and results at any time. The labs are controlled by the trainer and allow students to perform defense and attack assignments and become more professional.

Scenarios

Provide participants with actual past or possible situations from cybersecurity or cyberterrorism to solve. An example of a real-life scenario would be: The police computer system has been attacked. The mission is to identify the attacker, repair the damage, and secure the system against future attacks.

Projects

Trainees must complete a built-in project, which reflects the knowledge they've acquired and their ability to produce defense and assault tools.



Course Overview

XE Basics

3 Courses

36 Built-in Labs

48 Hours of Training

Overview

XE Basics offers an entry-level training program focusing on basic Cyber, Linux and Python fundamentals.

Intro to Cyber

Introduction to Cyber is an essential course covering main topics from the cyber world and allows the participants to quickly view the complex world of digital crimes.

This training covers the core concepts of defence and understanding in the practical world using the Cyberium simulator.

Target Audience

The course targets participants with basic computer knowledge and managers wanting to understand the world of cyber security.

Course Objectives

- Acquiring the knowledge and tools to understand the corporate network.
- Understanding cyber-attacks for security awareness.
- Being able to make better decisions in the corporate world.

Students will learn about different domain structures and security technology products.

Module 1: Introduction to Tier 1

During this module, students will study the fundamental concepts of the world of cyber security.

Fundamental Concepts

Definitions
Key Players
History and the Future
Security Awareness
Cyber Job Roles
Basic Networking
Remote Access
Steganography and Ciphers
Hash Functions and Encodings

Module 2: Cyber Security

In this module, students will embrace the attacker state of mind to recognise the necessary defence mechanisms.

Cyber Concepts

OSI Model
DNS and DHCP - From an attacker perspective
Security Products Explained
Anonymity on the Network
Concepts of Wi-Fi Security

Cyber Attacks Demos

MiTM Attacks
Brute Force
Phishing
Trojans

Linux Fundamentals

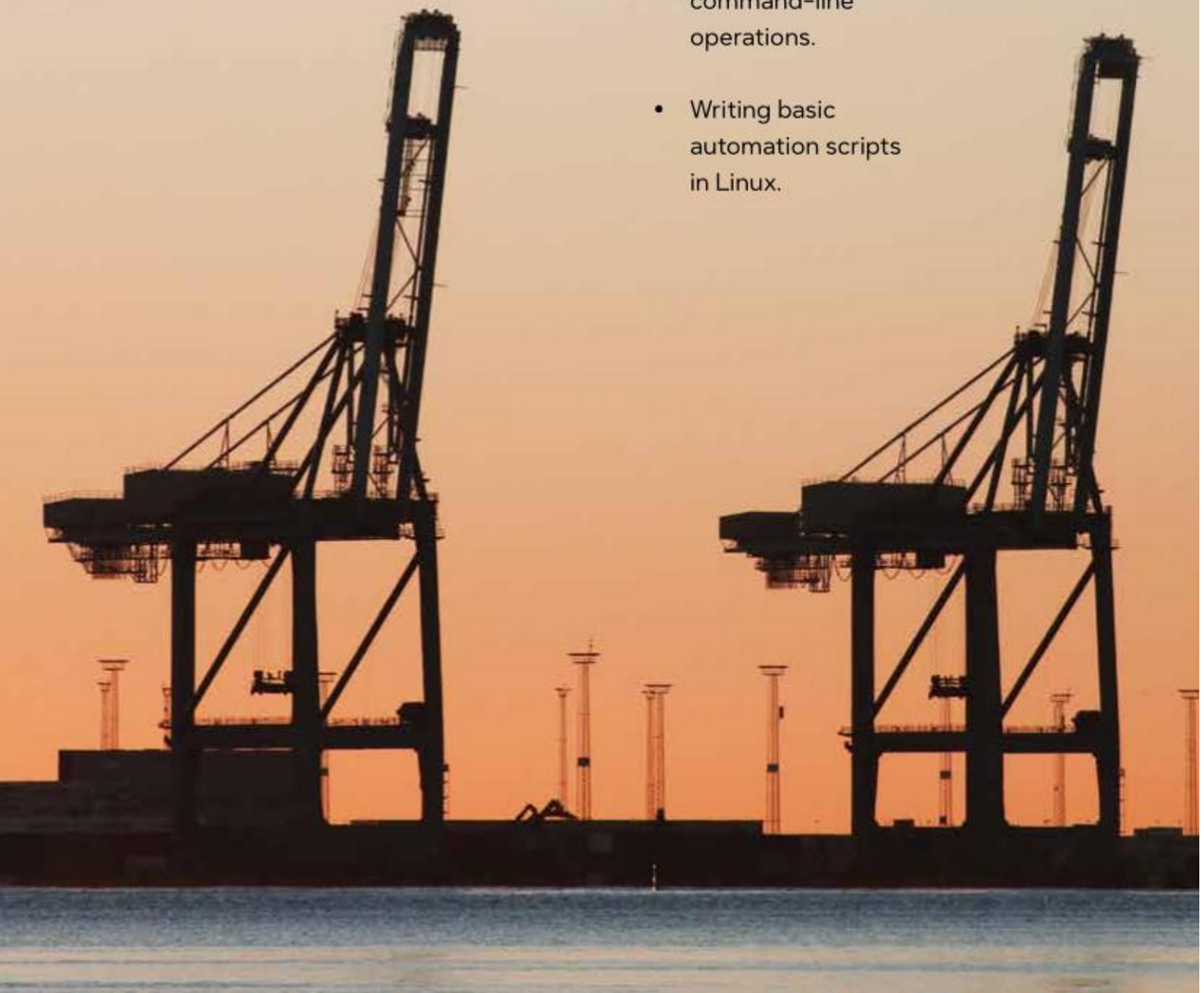
This training covers basic use in the Linux environment. Linux Fundamentals is a course designed for non-technical users, helping them become comfortable with Linux and basic automation scripting capabilities.

Target Audience

The course targets students with basic computer knowledge.

Course Objectives

- Using Linux command-line operations.
- Writing basic automation scripts in Linux.



Module 1: Command-Line

During this model, students will explore the advanced features of the Linux Command Line and text manipulation.

Introduction

History of Linux
Exploring Distributions

The Terminal

Basic Commands
Permissions
Text Manipulation Commands
Writing Scripts
Working with Archives

Module 2: Bash Scripting

In this module, students will learn how to write basic scripts and start creating different automation.

Bash Scripting

Introduction to Programming
Writing Bash Scripts
Getting User Input
Performing Math
Logic Statements
Global vs Local Environment Variables

Module 3: Networking

This module will teach the students to gain full control of the Linux Environment. The students will learn to administer their system and manage software and services.

Network Troubleshooting

Network Configuring
Basic Network Troubleshooting

Package Management

Installing Deb Packages
Using APT

Python Fundamentals

Any person wanting to automate stages and create cyber-tools must learn to program. Python is an easy language used by many to build tools in different fields, including cyber.

This training will provide the student with a stepping stone on understanding programming logic and creating basic scripts to take skills to the next level.

Target Audience

The course targets participants with basic computer knowledge wanting to get into the programming world.

Course Objectives

- Getting to know Python variables.
- Building basic Python code.

Module 1: Introduction to Python

During this module, students will be introduced to the world of Python. Students will learn to install Python and its additional modules.

Introduction

Installing Python
Variables and Booleans
Dictionaries and Tuples

Module 2: Conditions and Functions

Students will learn to work with conditions during this module and create a dynamic code that will operate accordingly.

Conditions

Conditional Statements
While and For Loops
Scoping and Subroutines

Functions

Working with Functions
External Functions
Exceptions

Module 3: Files I/O

Using files, using both reading and writing is an important capability in any programming language.

Python Scripting

Reading Files
Extracting Data
Writing into Files

NX Defence

11 Courses

55 Built-in Scenarios

128 Built-in Labs

440 Hours of Training

Overview

NX Defence offers a suite of training programs designed to train the Blue Team in defence best practice.

Network Research

Large and small companies face a critical stage; cyber-attacks have transformed dramatically over the past few years. Unfortunately, organisations are still being breached too often and are under more pressure than ever to secure their systems.

The Network Security course aims to address cyber challenges experienced on the network level. The course covers various attack techniques and how to defend against them.

The course sets the groundwork for later specialisation in cyber forensics, advanced cyber defence and penetration testing.

The course helps prepare for the certification exams Linux + (CompTIA) and LPIC-2 (LPI).

Target Audience

The course targets students with basic IT or networking knowledge who wish to understand corporate cyber security and cyber defence from a technical perspective.

Course Objectives

- Becoming familiar with the cyber threat landscapes.
- Acquiring the knowledge and tools to recognise threats in the network.
- Understanding cyber-attacks.
- Becoming familiar with a variety of available tools for performing security related tasks.

Module 1: Introduction to Linux

Students will study the Linux OS fundamentals. This module uses Linux commands, manipulating text and command outputs, understanding terminal emulators, permissions and other security concepts.

Virtualisation

Introduction to Virtualisation
About Linux Distro
Installing Linux
Working with VMWare
Bridged vs NAT

Working with Linux

Linux Directories
Linux Users
Packages
File Manipulation Commands
Text and File Manipulation Techniques
Writing Linux Scripts

Module 2: Networking

During the module, participants will study network infrastructures, common network types, network layers, communication between protocols, communication between network devices from different layers and network anonymity methods.

Protocols and Services

TCP/IP and OSI Model
Network Routing Basics
DNS
DHCP
ARP
Remote Connection Protocols

Wireshark – Diving into Packets

Non-Secure and Secure Packets
Filtering and Parsing
Extracting Objects and Files from PCAP Files

Module 3: Introduction to Network Forensics

Large organisations these days suffer greatly from network attacks and malicious intrusions. Those who manage the organisation's network have an immense impact on ensuring its safety. This module will introduce participants to Network Forensics and learn how to locate and better understand various attacks.

Windows Tools

Network Miner
Advanced Wireshark
OS-Fingerprinting
Detecting Suspicious Traffic
Sysinternals

Linux Tools

TShark - Network Analyzing Automation
Capture Packet Data from Live Network
Filter Packets from Live Network
Filter Packet from PCAP File
Traffic Statistics
File-Carving
Parsing Traffic Logs
CAPInfo

Module 4: Cybersecurity

This module's primary goal is to teach participants to embrace the attacker's state of mind to recognise the necessary defence mechanisms. Participants will deal with several types of attacks. Students will learn about hash functions; furthermore, they will learn how wireless networks are attacked and how they are vulnerable to those attacks. Social engineering and honeypot techniques will also be demonstrated.

Cybersecurity Vectors

Anti-viruses
DoS and DDos
CNC Services and Botnets
Steganography

Network Attacks

Scanning Methods
MiTM
ARP Poisoning
DHCP Starvation
LLMNR Attacks
Offline Password Brute-Force
Working with Responder

Cyber Attack Practice

Payloads: Reverse vs Blind
Privilege Escalation

SOC Analyst

The Security Operations Centre (SOC) should have everything it needs to mount a confident defence against constantly changing attacks. The SOC includes a vast array of sophisticated detection and prevention technologies, cyber intelligence reporting, and access to a rapidly expanding workforce and talented professionals.

This SOC Analyst course is designed for SOC organisations to implement a SOC solution and provide full guidance on the necessary skills and procedures to operate it. The training will provide participants with all aspects of an SOC team.

This course helps prepare for the certification exams CISM (ISACA), GSEC (SANS) and GMON (SANS).

Target Audience

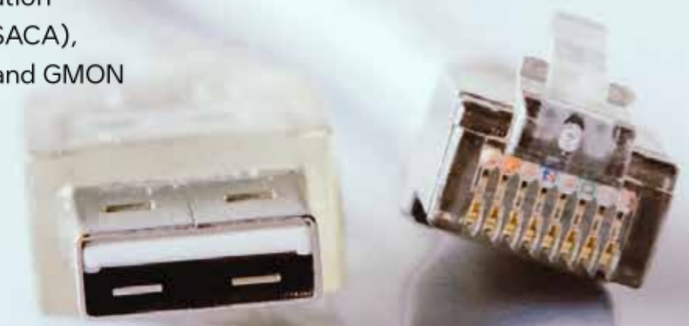
The course targets participants with foundational knowledge in computer networking.

Prerequisites

Linux

Course Objectives

- Provide participants with a solid understanding of the SOC environment, it's roles, and functionalities.
- Provide participants with the ability to gain practical capabilities of working inside a SOC.
- Practice the acquired knowledge in real-time through the simulation environment.



Module 1: Intrusion Detection

During this module, participants will further explore data packets and study on a deeper level, learn to identify network anomalies, and understand system alerts.

Students will master the use of well-known command-line-interface (CLI) and graphic user interface (GUI) tools to further specialise in the field. Students will learn methodologies to approach investigations of incidents.

Networking

Network Protocols
The OSI Model
Analyzing Packets

Basic Intrusion Detection Tools and Methods

Wireshark
GeoIP Integration
TShark
Sysmon

Module 2: Setting Up the SOC Environment

Companies regularly deploy various security technologies designed to prevent and detect threats and strengthen and protect assets. During this module, we will detail SOC environments and how they work.

The student will learn to build and properly configure their SOC environment and correlate it with other security products and assets. Having a SOC allows you to have a dynamic security apparatus that acts as a real bastion of analysis, monitoring, prevention, and remediation.

Preparing the Framework

Introduction to ELK
Deploying Beats
Identifying Threats
Aggregating Data
Real-Time Monitoring

Hands-on PfSense

Setting and Configuring Rules
Passing Traffic using the NAT Feature
Configuring Firewall Rules
Managing Network Security
Snort

Module 3: Using the SIEM

In this module, students will learn about Security Information and Event Management (SIEM), the primary system used by SOC analysts for monitoring the network.

Participants will install a freely available open source SIEM platform and simulate different scenarios through a pre-prepared virtual environment, mimicking an organisation.

Building SIEM Environment

Configuring your Domain
Setting up an Open Source SIEM
Deploying Security Onion
Network and Host DLP Monitoring and Logging

Monitoring using the Virtual Environment

Firewall Monitoring and Management
Email and Spam Gateway and Web Gateway Filtering
Vulnerability Assessment and Monitoring
Setting you Rules for Cyber Threats

Module 4: Windows Management Instrumentation (WMI)

In this module, students will learn to use the Windows Management Instrumentation.

Students will learn how the core management process is accomplished and use WMI to manage both local and remote computers on the LAN network to consolidate the acquired knowledge into building tools skills in PowerShell scripts and regular WMI usage.

WMI Architecture

Using WMI Methods
Working with Remote Computers
Access to the Registry
Information Gathering
Storage Information
Command Execution
Common Events
Detection with WMI

Target Audience

This course targets participants with basic knowledge who wish to understand cyber investigators.

Course Objectives

- Understanding the Windows files structure.
- Accessing concealed files on the system.
- Extracting sensitive information.
- Mastering the steps of incident response.

Windows Forensics

Windows Forensics is an essential skill in the cybersecurity world. This course covers a broad spectrum of aspects of the forensic investigation process performed on Windows OS. Participants will learn how different computer components work and how to investigate after a cyber incident. This training will focus on developing hands-on capabilities of forensics teams of individual practitioners.

The course helps prepare for the certification exams CHFI (EC|Council) and GCIH (SANS).

Module 1: Computer Hardware

This module will cover different components of computer hardware. Students will learn the main components of storage disks, the Windows OS structure and install virtual forensics stations.

Drivers and Disks

Data Representation
Volumes and Partitions
Disk Partitioning and the Disk Management Tool
Solid State Drive (SSD) Features

Understanding Windows OS Structure

NTFS Structure
Master File Table
Windows System Files

Data and Files Structure

Hex Editors
File Structure

Module 2: Forensic Fundamentals

In this module, students will learn the Windows OS' internal components and the forensics investigation process.

Understanding Hashes and Encodings

The Use of Hash for Forensics
Base Encodings

Windows Artifacts

Startup Files
Jump List
Thumbnail Cache
Shadow Copy
Prefetch and Temp Directories
RecentApps
Registry Hives
Embedded Metadata

Module 3: Collecting Evidence

Students will master techniques for collecting evidence, accessing and retrieving volatile and non-volatile information.

Forensic Data Carving

Manual Carving
Automatic Tools

Collecting Information

Event Viewer
Detecting Hidden Files
Collecting Network Information
Sysinternals
Extracting Credentials

Module 4: Analysing Forensic Findings

In this module, students will understand how to uncover hidden information, detect tampered files, work with memory and analyse the RAM.

Drive Data Acquisition

Creating an Image
Analyzing Prefetch Files

Working with Volatile-Memory

Extracting Data from RAM
Identifying Network Connecting
Dumping Processes from Memory

Registry Analysis

Viewing Registry Dumps
Using Dat Files
Forensics Findings in the Registry

Anti-Forensics Techniques

Wiping Drives
Artifact Removal

Network Forensics

Network forensics training is about the analysis of network traffic to identify intrusion or anomalous activity. Compared to computer forensics evidence which is usually preserved on disk, network data is more volatile and unpredictable and requires a different approach.

This course sets the groundwork for understanding networks and the investigation process on them.

Students or master the fundamentals of conducting forensic analysis in a network environment. This course will incorporate demonstrations and lab exercises to reinforce hands-on capabilities.

Target Audience

This course addresses those with basic knowledge in networks and Linux.

Prerequisites

Linux
Networking

Course Objectives

- Detecting various types of computer & network incidence.
- Analysing network artefacts left on a compromised system.
- Performing network traffic monitoring and analysing logs.
- Learning to work with different network analysis tools.

Module 1: Intrusion Detection

During this module, participants will further explore data packets and study on a deeper level, learn to identify network anomalies, and understand system alerts.

Students will master the use of well-known command line interface (CLI) and graphical user interface (GUI) tools to further specialise in the field. Students will learn methodologies to approach investigations of incidents.

Networking

Network Protocols
The OSI model
Analysing packets

Basic intrusion detection tools and methods

Wireshark
TShark
GeoIP Integration

Using the Scapy Module

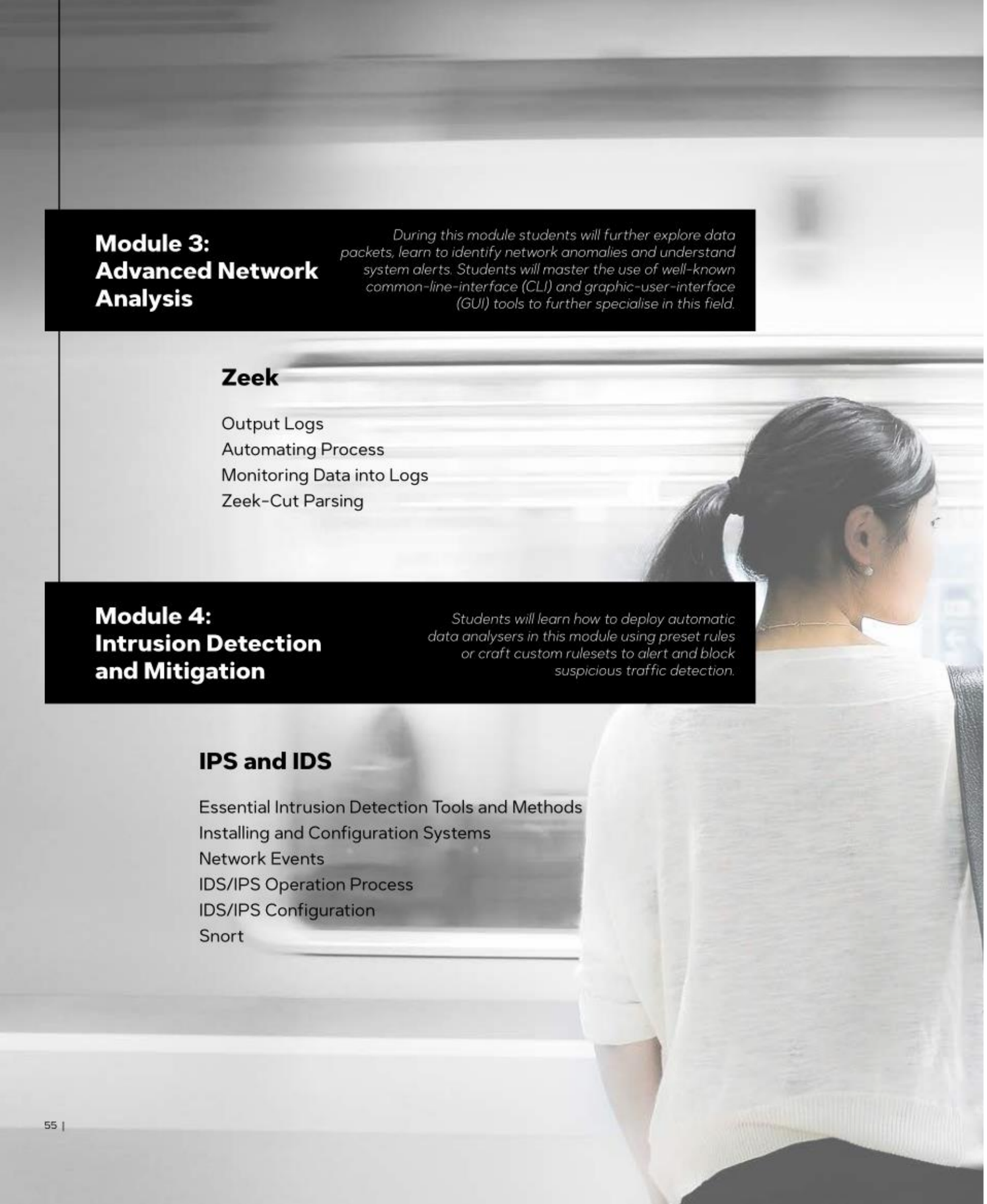
Crafting and Analysing Packets
Working with PCAP files
Replaying Packets for Investigation

Module 2: Case Investigation

During this module, students will understand the challenges of investigating network-based cases. Students will practice using various tools and investigation methodologies to correlate data and collect evidence.

Investigation Process

MiTM Attack
Find Network Anomalies
Flow Analysis
Network File Carving
NetworkMiner
File Carvers



Module 3: Advanced Network Analysis

During this module students will further explore data packets, learn to identify network anomalies and understand system alerts. Students will master the use of well-known common-line-interface (CLI) and graphic-user-interface (GUI) tools to further specialise in this field.

Zeek

Output Logs
Automating Process
Monitoring Data into Logs
Zeek-Cut Parsing

Module 4: Intrusion Detection and Mitigation

Students will learn how to deploy automatic data analysers in this module using preset rules or craft custom rulesets to alert and block suspicious traffic detection.

IPS and IDS

Essential Intrusion Detection Tools and Methods
Installing and Configuration Systems
Network Events
IDS/IPS Operation Process
IDS/IPS Configuration
Snort

OSINT

Open-source intelligence (OSINT) covers the techniques and procedures practiced retrieving targeted information from open-source networks containing immense amounts of data.

This course teaches participants how to collect and analyze information using every data source available. Students will be further exposed to collecting information from the Darknet, social networks and other sources.

This course helps students prepare for the certification exams GOSI (SANS) and C|OSINT (McAfee).

Target Audience

This course targets mostly law-enforcement wanting to master the art of finding data around the internet.

Course Objectives

- Providing students with an all-source methodology of employing open-source intelligence gathering.
- Discovering techniques and technologies needed to generate highly relevant intelligence.
- Understanding how to collect information from various social networks.
- Exploring the Darknet for information bases.

Module 1: Introduction to the Internet

In this module, participants will learn the fundamentals of the internet. Students will also learn to gather information regarding domains in different parts of the world.

Networking

The Internet Structure
The OSI Model
The TCP/IP Model
Network Devices
Network Protocols
Proxy Layer
Virtual Private Network (VPN)
DNS Leakage Testing

Domains and Organisations

Extracting Details
Collecting Information
Reconnaissance of an Organisation

Module 2: OSINT Tools and Search Engines

In this module, students will learn to use the a Students will get to know practical tools and search engines they will handle to collect data throughout this module.

They will deepen their understanding of various information sources and will focus on gathering data from social networks.

Introduction to OSINT

Building OSINT Plan
Categorizing and Cataloging
Information
Organising and Formatting Data

OSINT Tools

Online Tools and Frameworks
Introduction to Basic Bash Scripting
and Automation
Extracting Information from Major
Social Networks

Searching for OSINT Information

Dive into Metadata
Common Files Metadata
Web Sites Metadata
People Search Engines
Types of OSINT Sources
Reverse Image Search

Module 3: Advanced OSINT Search Engines

Students will become familiar with a wider and more advanced array of OSINT tools and search engines in this module.

They will understand how to use metadata and maximise the use of different filtering and customisation options for searching. Students will gain the capability to identify further information that may not be disclosed in a standard Google search.

Mastering Google Search Engine

Google Search Engine Advanced Search
Geographic Information Gathering
Searching in Different Languages
Building a Google Custom Search Engine
Reverse Image Search
Passive Target Scanners

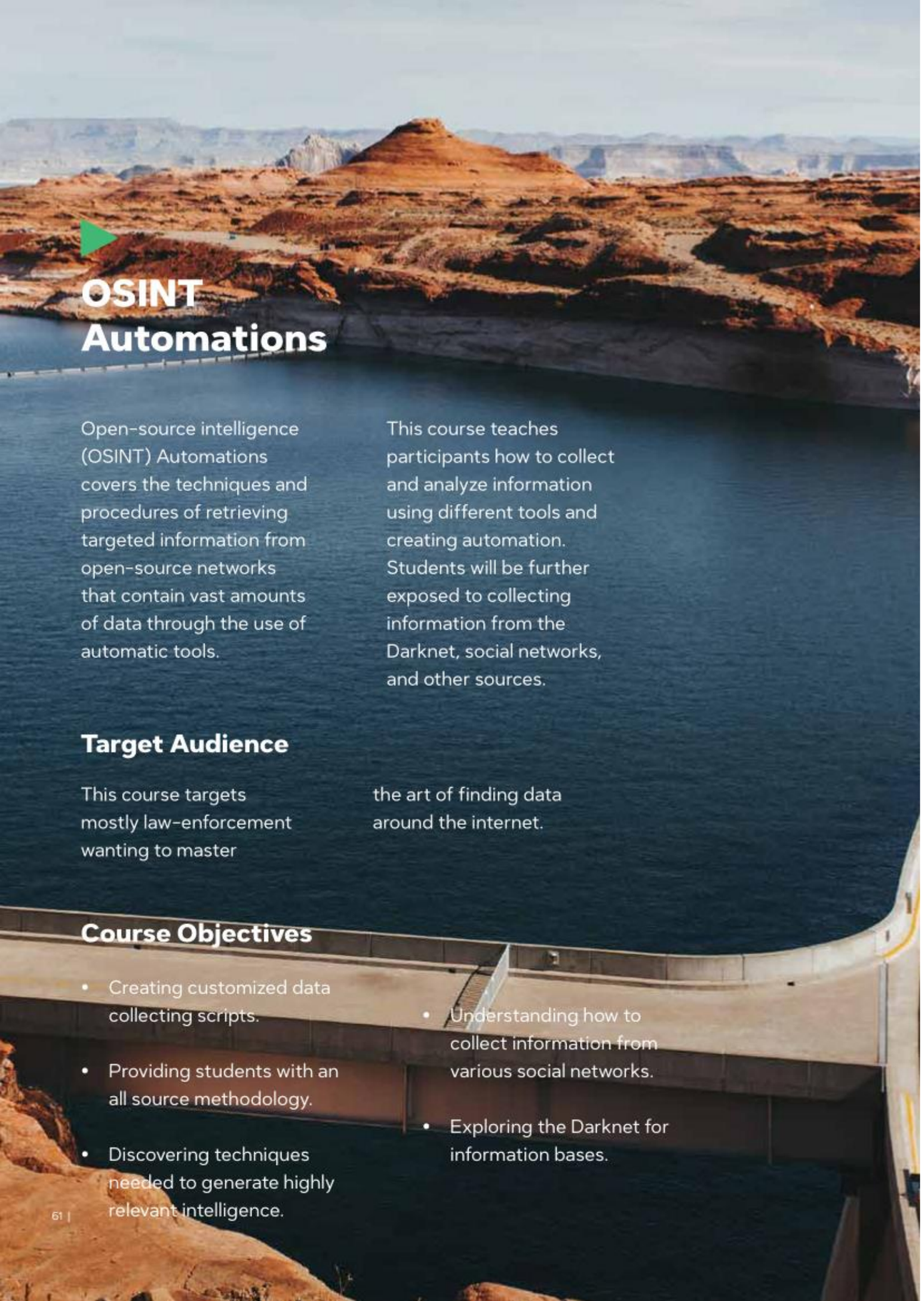
Module 4: The Darknet

The Darknet is considered the most prominent source of vast amounts of relevant information that is not accessible through the usual network.

During this module, participants will learn to use the Darknet, pinpoint the information they are looking for, collect it, use avatars, purchase databases with sensitive information and activate different automated tools for browsing and extracting information from the Darknet.

Darknet Overview

Understanding Global Internet Layers
Surface Web and Deep Web
Installing and Configuration of the Tor Browser
Darknet Search Engines
Installation and Security Concerns
The Tor UI
Onion System
Find Hidden Services
Understanding Cryptocurrency Marketing
Analysing Databases from the Darknet
Validating Leaked Password Databases



OSINT Automations

Open-source intelligence (OSINT) Automations covers the techniques and procedures of retrieving targeted information from open-source networks that contain vast amounts of data through the use of automatic tools.

This course teaches participants how to collect and analyze information using different tools and creating automation. Students will be further exposed to collecting information from the Darknet, social networks, and other sources.

Target Audience

This course targets mostly law-enforcement wanting to master the art of finding data around the internet.

Course Objectives

- Creating customized data collecting scripts.
- Providing students with an all source methodology.
- Discovering techniques needed to generate highly relevant intelligence.
- Understanding how to collect information from various social networks.
- Exploring the Darknet for information bases.

Module 1: Collecting with Linux

In this module, participants will learn to use Linux for collecting data from different sources. Students will also learn to gather information regarding domains in different parts of the world.

Linux Scripting

Open-Source Intelligence
Becoming Anonymous
Building your Lab
Virtual Private Networks (VPN)
Proxy Layer
Working with VPS
DNS Leakage Testing
Reconnaissance of an Organisation

Basic Intrusion Detection Tools and Methods

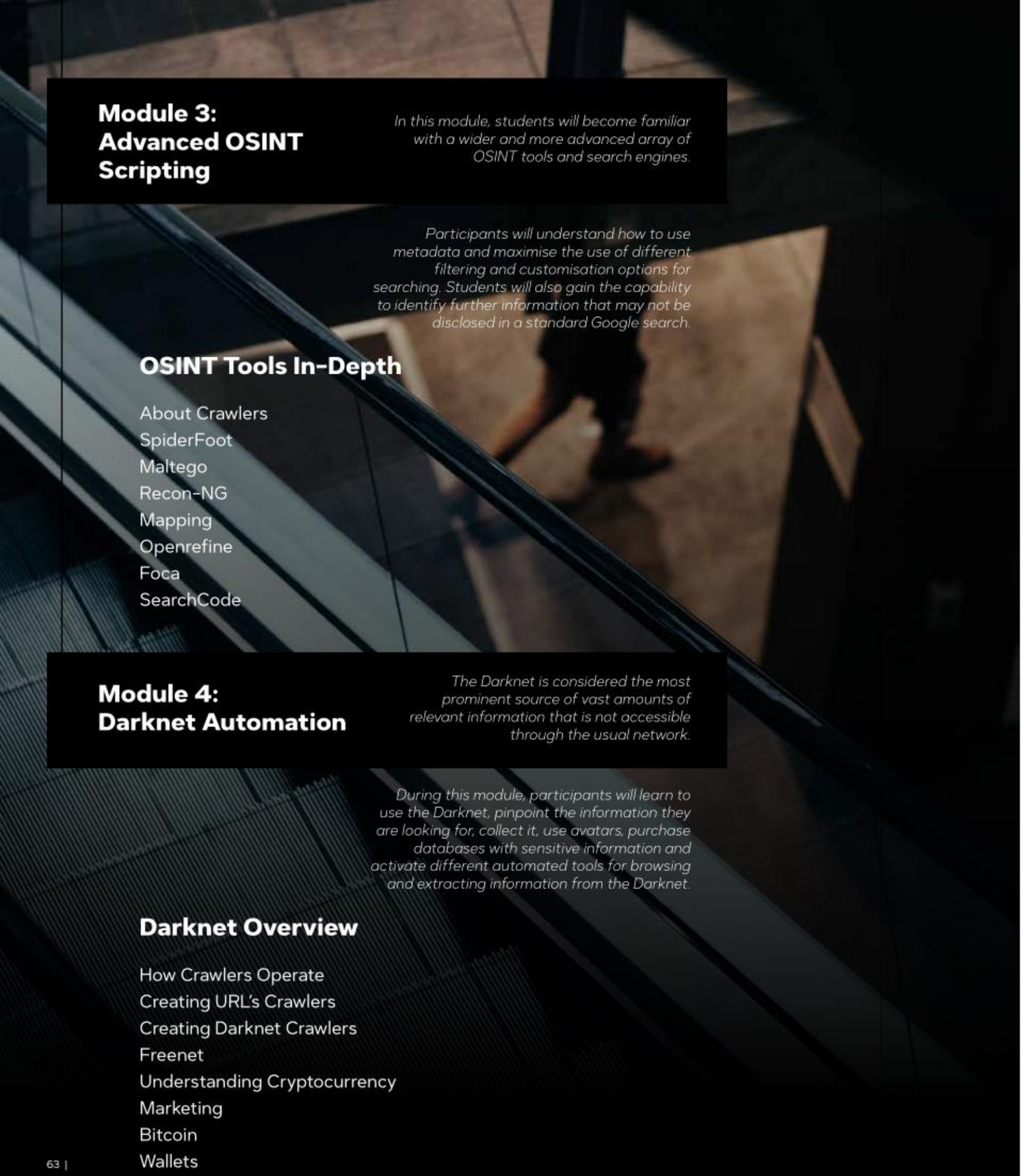
Wireshark
GeoIP Integration
TShark
Sysmon

Module 2: OSINT Tools and Search Engines

Students will get to know practical tools and search engines they will handle to collect data throughout this module. They will deepen their understanding of various information sources and will focus on gathering data from social networks.

OSINT Tools

Online Tools and Frameworks
Introduction to Basic Bash Scripting and Automation
Extracting Information from Major Social Networks
Extracting Metadata and Geolocation



Module 3: Advanced OSINT Scripting

In this module, students will become familiar with a wider and more advanced array of OSINT tools and search engines.

Participants will understand how to use metadata and maximise the use of different filtering and customisation options for searching. Students will also gain the capability to identify further information that may not be disclosed in a standard Google search.

OSINT Tools In-Depth

About Crawlers
SpiderFoot
Maltego
Recon-NG
Mapping
Openrefine
Foca
SearchCode

Module 4: Darknet Automation

The Darknet is considered the most prominent source of vast amounts of relevant information that is not accessible through the usual network.

During this module, participants will learn to use the Darknet, pinpoint the information they are looking for, collect it, use avatars, purchase databases with sensitive information and activate different automated tools for browsing and extracting information from the Darknet.

Darknet Overview

How Crawlers Operate
Creating URL's Crawlers
Creating Darknet Crawlers
Freenet
Understanding Cryptocurrency
Marketing
Bitcoin
Wallets

Penetration Testing

Penetration Testers face a combination of intrusion detection systems, host-based protection, hardened systems, and analysts that pour over data collected by their security information management system.

Penetration tests help find flaws in the system to take appropriate security measures to protect the data and maintain functionality. This training will provide the student with a foundation to run penetration testing in practice and take on the complex task of effective targeting and planning and penetration attack on a traditionally secured environment.

Target Audience

This course targets people from an IT background that want to upgrade their career and master the art of penetration testing.

Prerequisites

Linus
Networking

Course Objectives

- Bypass security and attack the network.
- Becoming familiar with penetration.
- Testing existing security weaknesses.

Module 1: Planning and Collecting Information

Before the penetration testing team can analyse and conduct a series of tests and attacks, the team needs to gather data to construct a better action plan. In this module, the student will go through the basics of information gathering and reconnaissance.

Passive Information Gathering

The OSINT Framework
Monitoring Personal and Corporate Blogs
Collecting Employees Personal Information
Harvesting Organisation Emails

Active Information Gathering

NMAP Scanning
Services Versions
DNS Enumeration

Identifying Vulnerability and Exploits

NSE Scripting
Vulnerabilities Detection Methods
Shodan Search Engine
Finding Exploits
Automating the Scanning

Module 2: Gaining Access and Post-Exploitation

In this module, the students will learn to use their knowledge in the first two phases to gain access, either using an existing exploit or brute-forcing them into the network.

After gaining control of the target, the students will learn to abuse existing services to elevate their permissions.

Finding a Way In

Social Engineering
Brute-Forcing Services
Metasploit

Gaining Access through Wi-Fi

Wi-Fi Basics
Management and Monitor Modes
Gaining Access to the Network

Post Exploitation and Evidence Gathering

Basic Privilege Escalation
Using the Meterpreter Modules
Windows and Linux Privesc Basics
Network Pivoting

Module 3: Inside Threats

Finding vulnerabilities on the network using different sniffing techniques is very important and can reveal the organisations vulnerabilities.

Sniffing Attacks

MAC Attacks
DHCP Attacks
ARP Poisoning
Spoofing Attacks
DNS Poisoning
Sniffing Tools
Sniffing Detection Techniques
Kerberos Attacks
Silver Tickets for Persistence
Domain Mapping and Exploitation
Effective Domain Privilege Escalation
SMB Exploits
SNMP Exploits
SMTP Exploits
FTP Exploits
Pass-The-Hash

Module 4: Intro to Web Application Security

In this module, students will learn the importance of web application security analysis. Many organisations were hacked using vulnerabilities in the application layer.

Hacking Web Servers

SQL Injection
File Upload Vulner
Local File Inclusion
Remote File Inclusion
XSS
BeEF
Password Attacks

Threat Hunting

In today's cybersecurity landscape, it isn't possible to prevent every attack. Threat hunting is the proactive technique that focuses on pursuing attacks and the evidence that attackers leave behind when they patrol an attack using malware or expose sensitive data.

Target Audience

This course targets people with networking knowledge who want to acquire threat hunting capabilities to protect their organisation.

Prerequisites

Linus
Networking

Course Objectives

- Identify and create intelligence requirements through practices.
- Generate threat intelligence to detect and respond.
- Learn the different sources to collect adversary data.
- Create indicators of Compromise (IOCs)

Module 1: Introduction to Threat Intelligence

In this module, students will learn about techniques and procedures necessary to effectively hunt, detect and contain various adversaries and minimise incidents.

Passive Information Gathering

Phases of Threat Intelligence
Phases of Intrusion Kill Chain
Understanding MITRE ATT&CK
Identifying Intrusions in Logs
Creating Automation For Notification of Malicious Activity
Analysing Network-Based tTools logs
Analysing host based tools logs
Linking Intrusions

Memory Forensics

Process Injection
Thread Injection
Malware Analysis
Malicious Document Analysis

Module 2: Data Collection

Students will use practical tools to collect data throughout this module. Students will deepen their understanding of various information sources.

Hunting

Parsing Relevant Data Techniques
VirusTotal
OSINT
Dynamic Indicators
Tracking Network Traffic
Passive DNS
Ransomware Traffic

Sources

Malware Analysis Databases
Intrusion Key Indicators
Domain Data Collection
Open SOurce Intelligence Tools
C2 Samples

Module 3: Threat Intelligence Automation

During this module, students will be creating tool automation to take threat intelligence to a higher level. Students will understand how to use their knowledge and maximise the use of different filtering and customisation options for searching.

Automation

YARA Examples
Working with YARA
Automating Malware Analysis
Configuring Honeypots
Extracting and Analysing Honeypots Logs

Domain Automation

Running Campaigns
Checking Key Indicators Inside Domains
Resting Your Indicators
Tactical intelligence Tools
Operation Intelligence Tools

Darknet

Relevant Leaks
Hacking Forums

Network Security

Network Security is a broad term that covers multiple technologies, devices, and processes. Every organisation, regardless of size, industry, or infrastructure, requires a network security expert in place to protect it from the ever-growing landscape of cyber threats today.

After this course, students will discover security vulnerabilities across the entire network using network hacking techniques and vulnerability scanning. Students will understand the various types of firewalls available and master both Windows and Linux servers' hardening.

Target Audience

This course targets participants with IT or networking knowledge who wish to understand corporate cybersecurity and cyber defense from a technical perspective.

Prerequisites

Linux
SOC or
Penetration Testing

Course Objectives

- Learning the cyber threat landscape that modern organisations face.
- Acquiring the necessary knowledge and tools to defend the corporate network.
- Identifying when attacks are happening on the network.
- Becoming familiar with available tools for performing security related tasks.

Module 1: Cyber Security In Networks

In this module, students will dive deeper into the world of cybersecurity, the primary goal being to teach participants to embrace the attacker state of mind to recognise the necessary defense mechanisms.

Network Security Fundamentals

Principles of Network Security
Security Components
Security Policies
Physical Security
Securing Devices

Network Attacks

Lab Setup: Creating your Organisation Domain
Identifying Application Attacks
Analyzing C&C Communications
Reversing Malware Network Behaviour

Module 2: Advanced Network Awareness

Organisations suffer greatly from network attacks and malicious intrusions. Those who manage the organisation's network have an immense impact on ensuring its safety.

This module will teach students to embrace the role of the network security administrator. Students will learn to inspect the network and find targets and possible security issues before the attackers can use them.

Analysing the Network

Automations Using NMAP
Detecting Service Changes Using Shodan CLI
Launching NSE to Detect Possible Vulnerabilities
Capturing Fake MAC and IP Addresses
Spying on the Local Network
Hunting for Rootkits with Windbg
Using the Sysinternals Suite to Identify Unusual Ports

Module 3: Cryptography in Theory

In this module, students will discuss cryptography and understand different types of algorithms.

Introduction to Cryptography

Ciphers in General
Encodings

Usage of Cryptography in the Cyber World

The Theory of Cryptography in Cybersecurity
Hash-based Password Verification
VPN and SSL Based VPNs
IPsec and Tunnelling
Poor Cryptography Threats
Algorithm Problems
Collision Attacks
Random Number Generation
Key Management Problems

Module 4: Practical Cryptography

In this module, students will learn how to implement famous techniques practically. Students will cover private key cryptosystems such as Caesar cipher, Vigenere cipher, Data Encryption Standard (DES), and Advanced Encryption Standard (AES).

Key Based Encryptions

Ciphers in General
Symmetric-Key
Asymmetric-Key
Block Ciphers
Attacks on Block Ciphers

Practical Ciphering

Classical Encryption Types
Mechanical - Enigma and Lorenz
Encryption in Application

Module 5: Hardening the Network

In this module, students will learn a wide range of IT security concepts and tools including step-by-step hardening measures, exploration of security weaknesses of the Linux operating system and protections against those weaknesses.

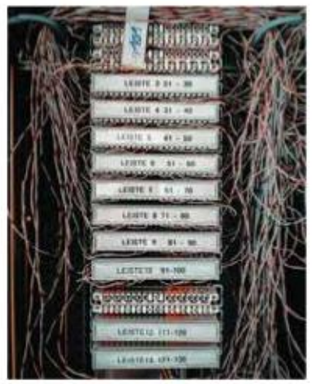
Routing and Network Components Hardening

Iptables vs. UFW
Monitoring the FW using Tshark
Mitigating DoS Techniques
Static ARP and DHCP Entry to Prevent Poisoning

Students will also learn how to secure the various account types on a Linux system, enforce strong passwords, and configure the firewall.

IPv6 Security

IPv6 Protocols
Protecting Against Rogue DHCPv6 Servers
Mitigate Ipv6 Attacks
DDos in IPv6



Counter-Measuring Attacks

Host vs. Network-Based IDS
Snorts as IDS and IPS
Constructing Honeypots
Identifying Log Tampering

Malware Analysis

Malware Analysis is the study and close examination of malware to understand its origins, purpose and potential impact on the system. Malware analysts accomplish their tasks by using various tools and expert level knowledge to understand what a piece of malware can do and how it does it. This course provides participants with the practical skills and knowledge to analyse malware and exposes them to a critical set of tools required for their tasks.

Target Audience

The course targets participants with a strong foundation in the forensics world who wish to upgrade their skill sets and become malware analysts.

Prerequisites

Linux
Forensics

Course Objectives

- Malware analysis using both dynamic and static analysis methods.
- Learning the Assembly Language to examine malware.
- Understanding malware using various tools.

Module 1: Introduction to Malware Analysis

In this module, students will study different types of malware to discover how they operate, understand how the antivirus works and eventually to develop an understanding of how to approach a malicious file and where to find it.

Introduction to Malware Analysis

Types of Malware
Memory Analysis
Security Mechanisms
Understanding the PE Format
Windows Libraries and Processes
Windows API's

Setting Up a Safe Environment for Inspecting Malware

Building and Configuring Virtual Machine
Malware Analysis Tools

Extracting Malware from Data Segments

Network PCAP Files
Volatile Memory
Malicious Activity Research

Module 2: Basic Analysis

Basic static analysis and basic dynamic analysis allow malware research to inspect malware influences on the system while it is in static and dynamic modes. This phase is critical for collecting information about the malware for more advanced stages of the research.

Basic Static Analysis

PE File Sections
Information Gathering from PE
Analysing Program Dependency Libraries
Resources Section Anomaly
Database of Files Hashes

Basic Dynamic Analysis

Identifying Virtual Machines
Searching for Ports
Testing Network Traffic
Snapshot System
Analysing Processes
Registry Analysis
DNS Monitoring
Simulating Internet Services
Analysing Findings

Module 3: Advanced Dynamic Analysis

Advanced dynamic analysis is the stage to inspect and analyse malware at a higher level. Students will learn to use debugging tools and analyse the malware.

Advanced Analysis

Understanding Debuggers
Running Malware in OllyDbg
Running Malware in Windbg

Module 4: Advanced Static Analysis

This module will introduce students to Assembly Language basics. Familiarity with Assembly will allow students to gain a closer understanding of what lies at the base of the malware's code and how it was meant to operate when activated and is an entry ticket into the world of reverse engineering.

Assembly Language Basics

X86 Processor Architecture
Understanding Buses and Data Traffic
Syscalls Table
Number and Character
Representation
Basic Assembly x86 Programming

Disassembler

Using IDA
IDA Features
Analysing Malware with IDA Pro

Reverse Engineering

Reverse Engineering is a technique used to analyse software to identify and understand its components and its flows. It is a process of understanding code infringement and processes and analysing software weaknesses. Reverse engineers analyse systems to create system representations in another form of abstraction.

Target Audience

This course targets cybersecurity practitioners with experience in malware analysis, Windows forensics, and exploit development capabilities.

Course Objectives

- Analyse various file formats to uncover the hidden codes within them.
- Identify control flows.
- Understand Assembly.
- Exploiting server, database and application software.

Prerequisites

Linux
Forensics
Malware Analysis

Module 1: Methods of Counting & Representing Information on a Computer

This module aims to cover necessary theories and concepts which reverse engineering is based on, starting from the base structure of files and their source.

Calculation of Bases

Hexadecimal Base
Binary Base
Transition Between Bases
Transition Between Hexadecimal to Binary and vice versa
Numerical Actions on Numbers in Different Representations
Negative Numbers

Module 2: Computer Systems Structure - Assembly Language

During this module, students will practice an in-depth analysis of the program codes using Assembly principles. Students will be able to recognise the effect of software and codes before their initial execution.

Assembly

Registries
Processor Architecture
Portable Executable

Installing a Workspace

Linux syscall Table
File Descriptor
The Connection to Files
Start of Program Construction
Debugging Process
IDA

Module 3: Exploitation

Students will learn about memory management and control code flows in this module while utilizing it to develop exploits.

Professionalization of GDB

Jumps & Conditions
Manipulation on a Processor
Loops
Activating Number-Detonation on the Processor
Ordering Bytes
Maintaining Flags Mode using a Stack
STack
Calling Conventions
Build printf functions using Assembly
Call to Functions

Buffer

Protostar
Buffer Overflow

Writing Exploits to Bypass Protections

Processes in Computer Science
Pseudo-terminal
Race Condition
Apport Service
How Debugger Works
Anti-Reversing
Return Oriented Programming (ROP)

Memory Management Policy

W^X
NX bit
DEP
Ret2libc
Format String
Overcoming the ASLR Mechanism through the Format String Attack
The Process of Adding the Addresses to a Written Code

Memory Management

How a Process Gets Memory from the System
Heap Overflow

Preparing a Windows Workspace

Visual Studio
OllyDbg

Exploitation Over the Internet

Buffer Overflow Over the Internet
Tracer Browser Detection
Fuzzing
SPIKE
Debug Using OllyDbg to Restore Crash
Shellcode
Manually Create Shellcode
Create Shellcode Using Metasploit

Bad Characters

Encoding
From Python to Metasploit
Mixins
SLmail
Immunity Debugger
Mona.py

ZX Offence

7 Courses

35 Built-in Scenarios

82 Built-in Labs

280 Hours of Training

Overview

ZX Offence offers a suite of training programs designed to provide best practice offensive training to the Red Team.

Cyber Warfare

This training is an advanced course that covers topics in the Red-Team cyber warfare methodologies. Students will get an in-depth look into the mind of a Black-Hat hacker and take a deep dive into its practical world using both IT and IoT devices. Students will learn the different information gathering tools and security bypassing products that can be leveraged to attack against every defense layer.

Target Audience

This course targets penetration testers that would like to embrace Red-Team's capabilities.

Prerequisites

Networking
Penetration Testing
Web Application Hacking

Course Objectives

- Acquiring the knowledge and tools to become a Red-Team member.
- Working with tools for security-related tasks.
- Becoming familiar with a variety of attack scenarios.
- Understanding different attack possibilities.
- Using automation as a Red-Team member.
- Becoming familiar with IoT
- Acquiring the necessary techniques and tools for Iot exploitation.
- Firmware exploitation and analysis.

Module 1: Introduction to IoT Security

Students will learn about IoT and smart devices, IoT device architecture analysis, and breaking it down to individual components, techniques, and tools during this module. Students will learn to find vulnerabilities all around the internet using smart queries.

Fundamental concepts

Understanding Firmwares
Retrieving Firmwares

Mapping the Internet

Mapping Attack Surface of an IoT Device
Setting up Debian-OS for IoT
Penetration Testing
Nmap Basics
Banner Grabbing Techniques
IoT Mapping with Shodan

Module 2: Embedded IoT Operating Systems

In this module, students will become familiar with Linux and network-based exploitation and use their IoT environments skills.

Introduction to Embedded OS

Working with Squash FS
Using Binwalk
Detecting Default Password
Analysing System Files
Firmware Analysis - Identifying Hardcoded Secrets

Emulating Firmware Binary

Working with QEMU
Deploying Firmadyne
Automating the Deployments
Weaponizing Firmwares

Web Application Security for IoT

Installing BurpSuite and Setting Proxy
Interruption
BurpSuite Components
Exploitation with Command Injection
Online Brute Force Basics

Module 3: Red-Team Domain Techniques

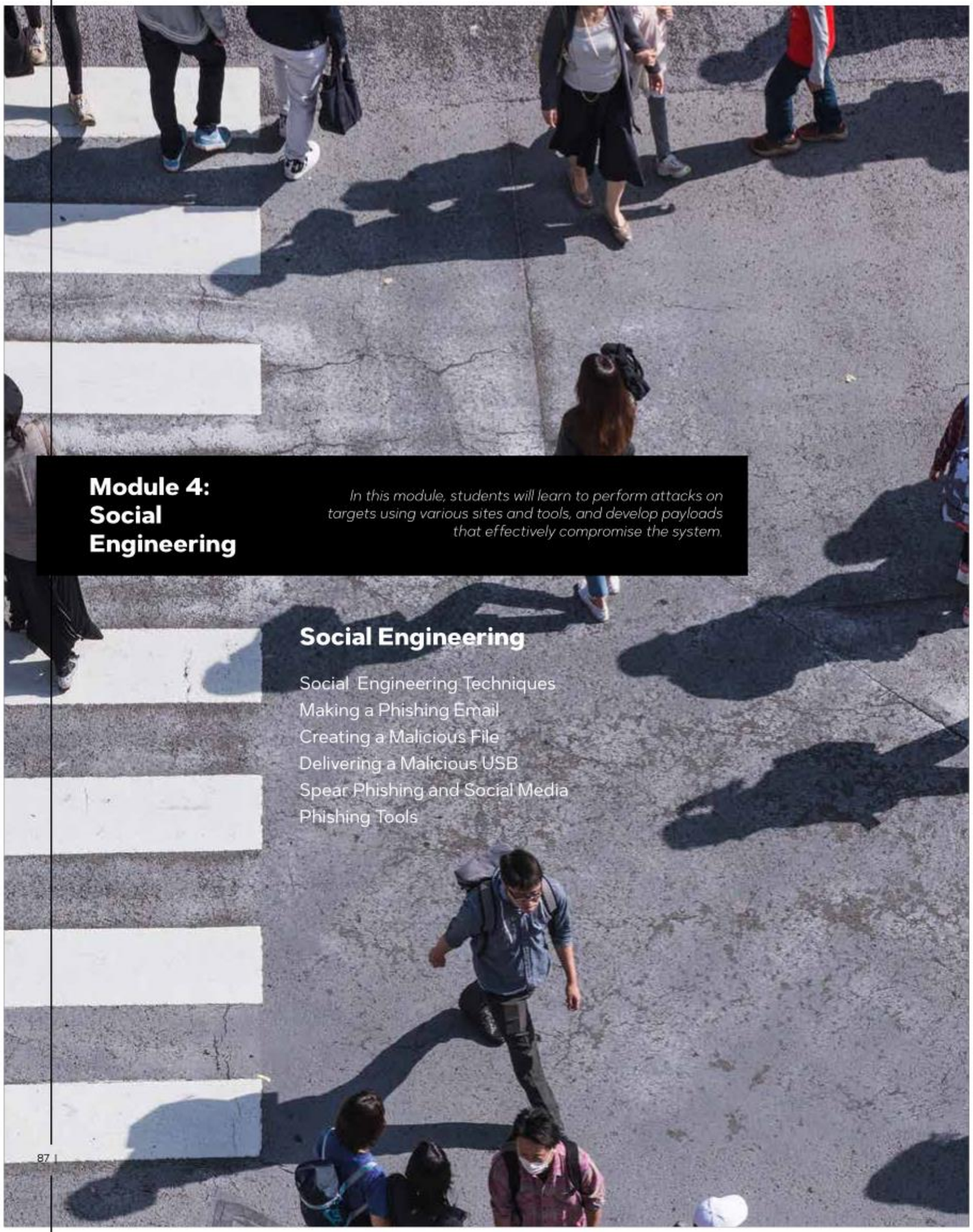
In this module, students will learn to act as the Red Team while attempting to gain information about the target using different techniques.

Mastering Domain Techniques

Setting Up Your Lab
Passive Scanning
Host Enumeration
Domain Enumeration
Port Forwarding and Exfiltration
Privilege Escalation
Lateral Movement
Persistence Techniques - Domain and Local
Detection and Defences

Red Team Tools

C2 Framework
Password Extractors
Persistence
Configuring your Metasploit Payloads
Post Exploitation
Process Injection



Module 4: Social Engineering

In this module, students will learn to perform attacks on targets using various sites and tools, and develop payloads that effectively compromise the system.

Social Engineering

Social Engineering Techniques
Making a Phishing Email
Creating a Malicious File
Delivering a Malicious USB
Spear Phishing and Social Media
Phishing Tools

Web Application

This Web Application course will help participants understand web application languages and their exploitation. Students will learn a proven process for locating these flaws consistently. This training program's primary goal is to help security specialists understand web application risks in their organisation and learn how to conduct web application security assessments.

Target Audience

This course targets cyber experts who wish to learn web application languages and people who wish to learn web application security fundamentals.

Prerequisites

Networking

Course Objectives

- Discovering and mitigating website vulnerabilities.
- Using tools to automate your tasks.
- Securing web servers from attacks.

Module 1: Introduction to IoT Security

Students will learn web application security, techniques, and web app developers' methods in this module.

WebApp Concepts

Web Application Architecture
Clients
Fingerprinting Websites
Robots.txt Structure
Securing the Admin Interface
Parameter Tampering
HTTPS Encryption

WebApp Basics

HTML
PHP
Combining HTML and PHP
HTTP Response Codes

Module 2: JavaScript

In this module, students will learn how to work with Javascript, including for penetration testing purposes.

Javascript

Modifying HTML
Hijacking Forms
Keylogger
Social Engineering
HTML Parsing
JSON Parsing
XML Parsing

Module 3: SQL Databases

Students will learn the basics of SQL databases, using and conducting tests on web applications to detect security holes either by brute-force or by exploiting a vulnerability during this module.

SQL Database

SQL Explained
Creating Databases
Understanding SQL Injection
Testing for SQL Injection
Exploiting SQL Injection
Blind SQL Injection

Module 4: Introduction to Web Application Vulnerabilities

During this module, students will learn about common vulnerabilities in web applications, how they can be exploited, and what impact they could pose.

Exploitation

Burpsuite Fundamentals
Brute Force
Command Injection
User Enumeration
Local File Inclusion
Reflected XSS
Stored XSS
DOM Based XSS

Web Application Hacking

During this training, students will gain knowledge and skills used by penetration testers, and their procedures, to detect security vulnerabilities in web applications using a combination of manual and automated techniques and methods. Testing web application security is not intuitive and to be useful you need an understanding of web application design, HTTP, JavaScript, browser behaviour, and other technologies.

Target Audience

This course targets cyber experts who wish to learn web application penetration testing and people who wish to learn web application advanced security methods and techniques to find security holes.

Prerequisites

Networking
Penetration Testing

Course Objectives

- Learning different vulnerabilities.
- Being able to perform web application penetration testing.
- Discovering security holes in web application.
- Using tools to automate your tasks.

Module 1: Advanced Penetration Testing Skills

In this module, students will learn advanced techniques to understand penetration testing on the web app. Working correctly in a local proxy environment without using a browser can block us from partnering and not reveal all sites information

Advanced Information Gathering

Website Spidering and Crawling
Revealing Website History
Web Page Snapshots
Data Extraction and Scrapping

Advanced Discovery

Understanding Advanced Methodologies
Crafting Discovery PowerShell Scripts
Weaponizing Curl and Wget in Discovery Scripts
Using Metasploit Framework Web Modules
Nmap NSE Scripts

Module 2: Web Ethical Hacking

In this module, students will learn how to perform hacking and testing capabilities of the web application. Students will handle the various results received and learn to gain remote control of the system with common web attacks

Advanced Offensive Techniques

RCE in Various Environments
Understanding SQL Injection Techniques Manually
Format String Vulnerabilities
Cross-Site Scripting (XSS)
Wordpress Application Testing
Understanding Steganography and Encryption
Error Messages
Common HTTP Feature
Information Control

Module 3: Web Ethical Hacking Part B

In this module, students will learn how to perform advanced hacking and testing web application capabilities.

Attacks In-Depth

Cross-Site Scripting
Persistent
Stored
Command Injection
Brute Force
User Enumeration
XML
Privilege Escalation
Directory Traversal
Local File Inclusion (LFI)
Remote File Inclusion (RFI)
File Upload Vulnerability
File Inclusion to Reverse Shell Techniques
Blind SQL Injection
The SQL Query to Reverse Shell Techniques

Module 4: Mitigations

In this module, students will learn how to protect web application vulnerabilities.

Mitigations

Injection
Broken Authentication
Sensitive Data Exposure
XML External Entities
Broken Access Control
Security Misconfiguration
Cross-Site Scripting
Insecure Deserialisation
Insufficient Logging

Windows Exploitation

Microsoft Windows is one of the most popular operating systems ever used. This operating system can be found on any device, such as computers, phones, banking systems, and many more. In this course, students will learn about the Windows operating system's advanced hacking techniques. students will also experience both offensive and defensive methods; students will learn the latest hacking methodologies.

Target Audience

This course targets penetration testers and security experts interested in upgrading their cyber knowledge and capabilities in the Windows OS environment.

Prerequisites

Linux
Penetration Testing

Course Objectives

- Learning advanced attack methods.
- Using Windows API.
- Using PowerShell.

Module 1: Windows Management Instrumentation (WMI)

This module will explain and expand on the use of windows management instrumentation. Students will learn how the core management process is accomplished and use WMI to manage both local and remote computers on the LAN network.

WMI Architecture

Using WMI Methods
Working with Remote Computers
Information Gathering
Active Directory Enumeration
Lateral Movement
Storage Information
Command Execution
WMI Common Events
Detection with WMI

Module 2: Offensive Powershell

PowerShell is a built-in shell, available on every supported version of Microsoft Windows, and provides incredible flexibility and functionality to manage the system.

Introduction to PowerShell Scripting

About PowerShell
Using ISE, Help System, cmdlets, and syntax of PowerShell
Scripting Basics
Working with Pipeline, Files, Functions, Objects, Jobs, and Modules
Improving Performances
Executing Policies with Scripts
Command Injection

In this module, students will learn various techniques to use PowerShell as a Red Team tool in the Windows environment and understand and leverage the PowerShell platforms capability to maintain access.

PowerShell as Offensive Tool

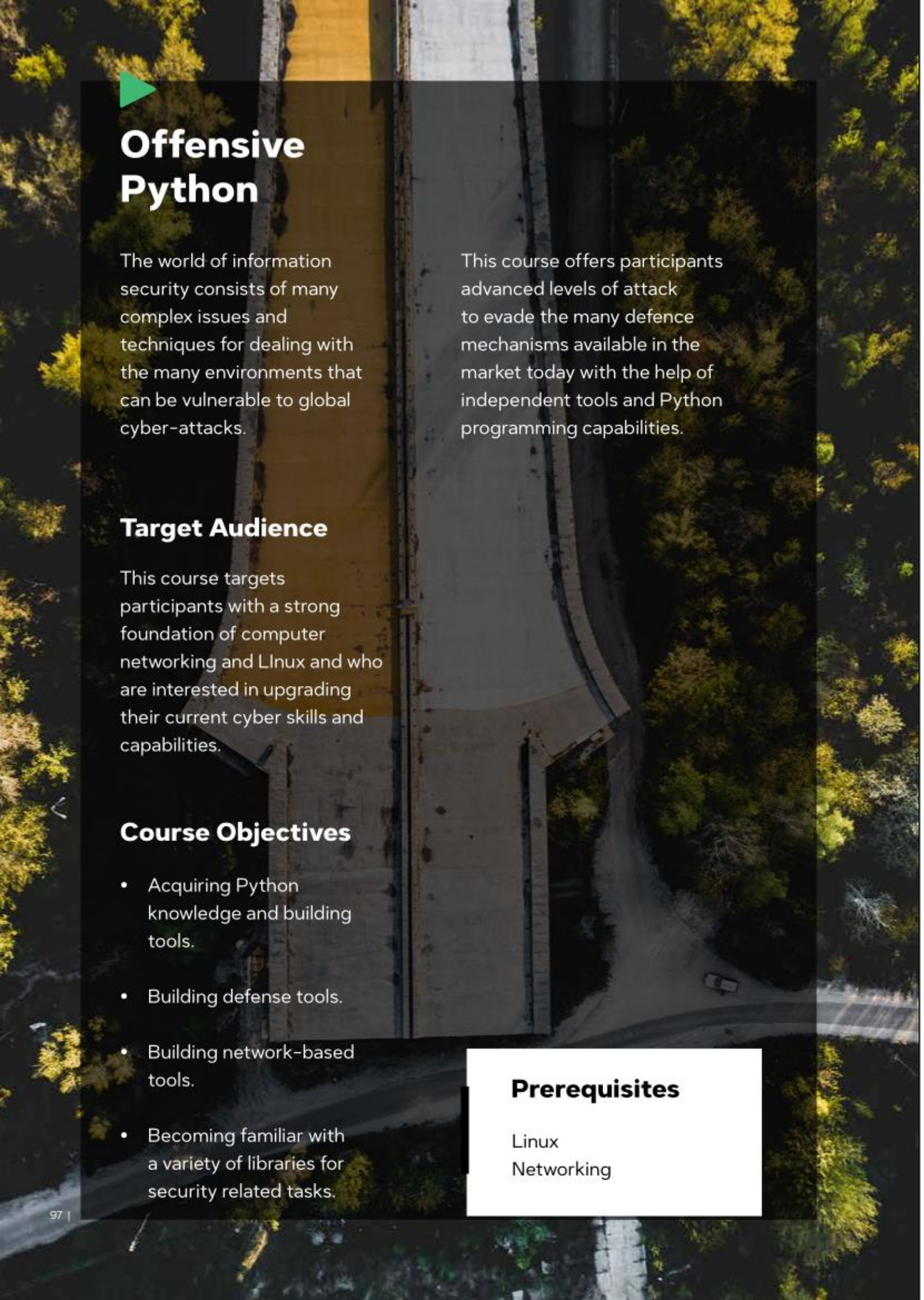
Gathering Information about the Network
Vulnerability Scanning and Analysis
Avoiding Detection
Tools Written/Integrated with PowerShell
Brute Forcing
Client-Side Attacks
Using Existing Exploitation Techniques
Porting Exploits to PowerShell - When & How
Human Interface Device
Getting a Foothold on the System
Use Management Tools to Attack Systems
Writing Shells in PowerShell
Pivoting to other Machines Using PowerShell

Module 3: Windows Application Programming Interface (API)

API is a set of functions that allows applications to access data and interact with external software components, operating systems, or microservices. This module will focus on Windows API attack capabilities.

Windows API Overview

Windows Internals
Drivers
Memory
Threads
Process Listing
Syscall
System Activity in Windows Kernel
Dumping DLL
Detect Remote Thread Injection
Enumerating the Structure
Tokens and Privileges
Reading Process Memory



Offensive Python

The world of information security consists of many complex issues and techniques for dealing with the many environments that can be vulnerable to global cyber-attacks.

This course offers participants advanced levels of attack to evade the many defence mechanisms available in the market today with the help of independent tools and Python programming capabilities.

Target Audience

This course targets participants with a strong foundation of computer networking and LInux and who are interested in upgrading their current cyber skills and capabilities.

Course Objectives

- Acquiring Python knowledge and building tools.
- Building defense tools.
- Building network-based tools.
- Becoming familiar with a variety of libraries for security related tasks.

Prerequisites

Linux
Networking

Module 1: Working with Python

This module will teach students how to use the python programming language and how to use Python to automate the network analysis script on various information security fields.

Python Networking

Introduction to Sockets
Connecting with TCP & UDP
Banner Grabbing
Port Scanner

Useful Libraries for Security

Cymruwhois
Faker

Password Cracking

Brute Force Attacks
Brute Force Zip Attacks
FTP Cracker

Module 2: Packet Crafting with Python

This module will teach students to handle the network traffic and various ethical hacking techniques to write automation processes to that procedure.

Scapy

Sniffing with Scapy
Researching Pcap Files
Crafting Packets
Sending Packets
Automation with Scapy
Port Scanners
MiTM Attack
Creating Security Tools

Module 3: Scanners

In this module, students will learn to generate custom scans and use automation to achieve cyber procedures.

Scanning with Python

Nmap
Shodan

Automation with Python

Paramiko
Pexpect

Module 4: WebApp Security with Python

The web application security module is an important part of our training. Students will learn how to use their knowledge of the web, extract sensitive data, and create web servers for Red Team tasks.

HTTP Programming

Simple Web Server
Urllib
BeautifulSoup
Requests

Web Application Security

Setting the User Agent
Setting Cookies
Using Web Proxy
Spidering

Module 5: Replicate Metasploit Features

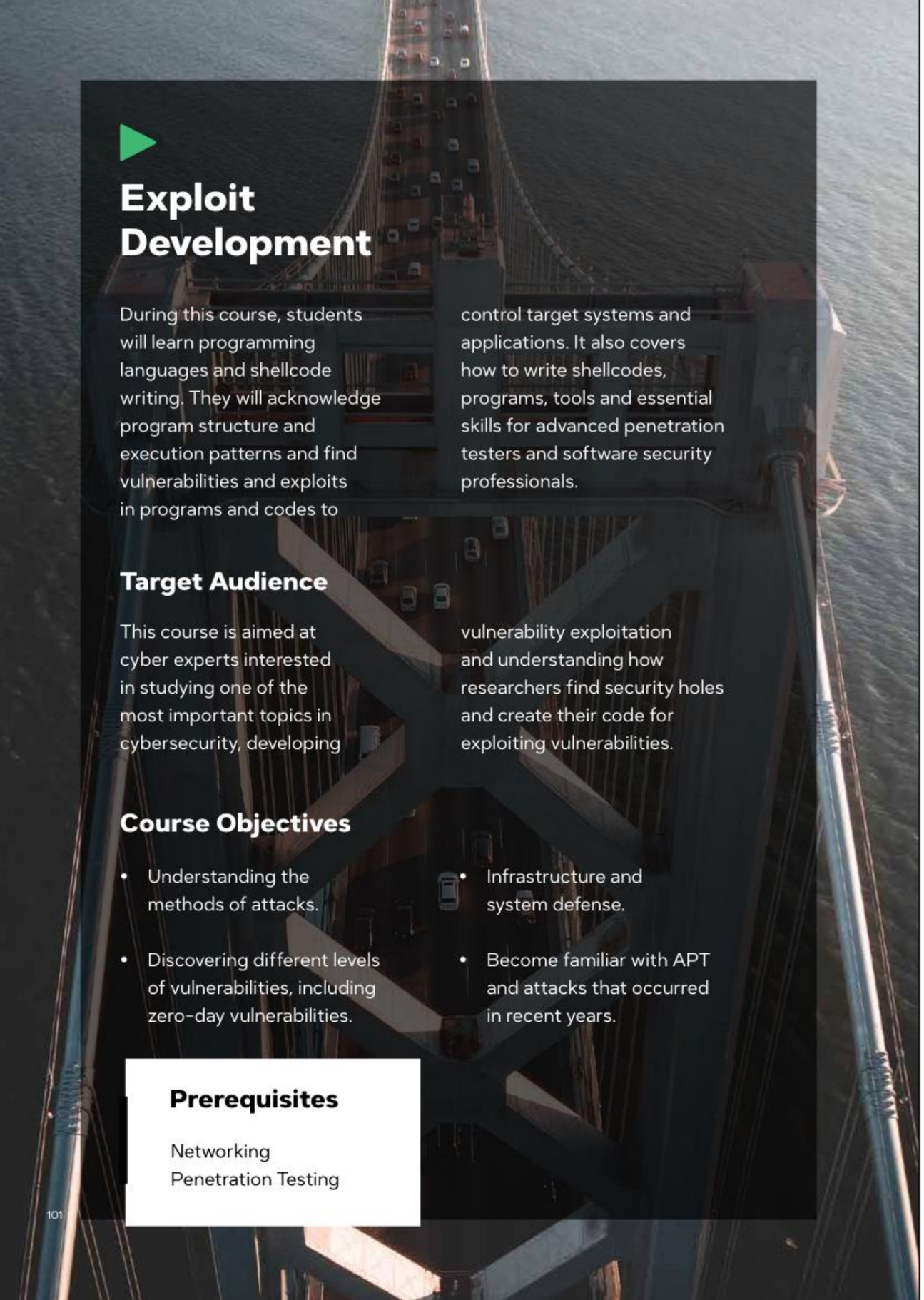
In this module, students will learn how to automate Metasploit script using Python and other useful techniques for ethical hacking.

Working with Payloads

MSFVenom
The Python Payload
TCP Reverse Shell Explained
HTTP Reverse Shell Explained
Persistence Explained
Upgrading your Shell
DDNS Reverse Shell

Local Attacks

DNS Poison
Extracting Passwords from Chrome
Keylogger



Exploit Development

During this course, students will learn programming languages and shellcode writing. They will acknowledge program structure and execution patterns and find vulnerabilities and exploits in programs and codes to control target systems and applications. It also covers how to write shellcodes, programs, tools and essential skills for advanced penetration testers and software security professionals.

Target Audience

This course is aimed at cyber experts interested in studying one of the most important topics in cybersecurity, developing vulnerability exploitation and understanding how researchers find security holes and create their code for exploiting vulnerabilities.

Course Objectives

- Understanding the methods of attacks.
- Discovering different levels of vulnerabilities, including zero-day vulnerabilities.
- Infrastructure and system defense.
- Become familiar with APT and attacks that occurred in recent years.

Prerequisites

Networking
Penetration Testing

Module 1: C Programming Crash Course

In this module, students will learn a course that will speed up their C-language programming capabilities in order to acquire the necessary writing shellcode skills.

C Programming Fundamentals

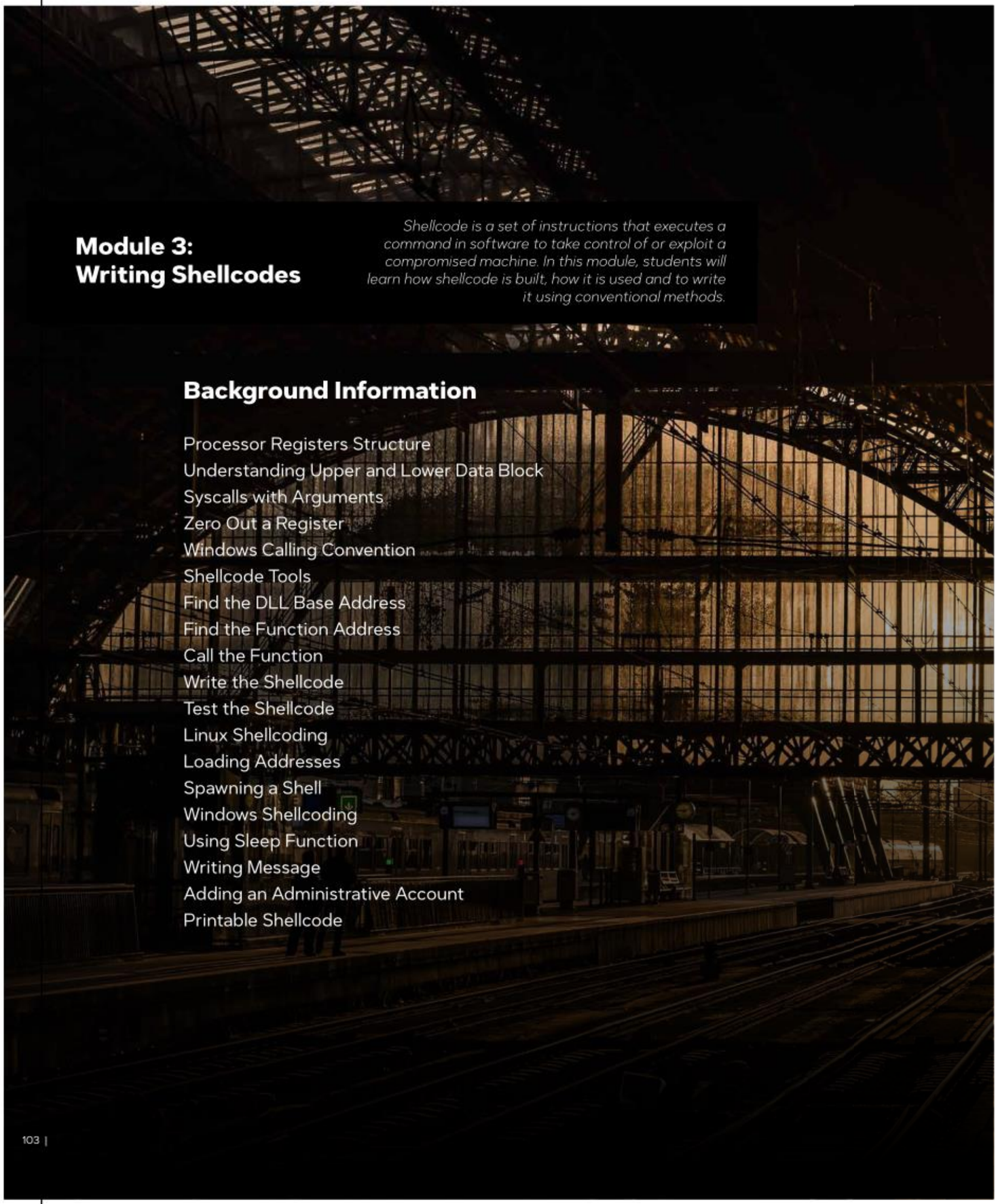
Variables
Input and Output
Keywords and Operators
Expressions and Statements
Control Flow
The C Preprocessor
Functions
Pointers
Code Structures
Using C Libraries
Memory Allocation

Module 2: Assembly x86

Students will acquire the machine language assembly experience in this module to become familiar with shellcodes and write one by themselves.

x86 Processor Architecture

Understanding Buses and Data Traffic
Syscalls Table
Number and Character Representation
Basic Assembly x86 Programming
Standard Output
Registers
Variables and Reserves
Strings in Assembly
Working with Numbers
Jumps and Flags



Module 3: Writing Shellcodes

Shellcode is a set of instructions that executes a command in software to take control of or exploit a compromised machine. In this module, students will learn how shellcode is built, how it is used and to write it using conventional methods.

Background Information

Processor Registers Structure
Understanding Upper and Lower Data Block
Syscalls with Arguments
Zero Out a Register
Windows Calling Convention
Shellcode Tools
Find the DLL Base Address
Find the Function Address
Call the Function
Write the Shellcode
Test the Shellcode
Linux Shellcoding
Loading Addresses
Spawning a Shell
Windows Shellcoding
Using Sleep Function
Writing Message
Adding an Administrative Account
Printable Shellcode

Exploit Development Advanced

In this course, students will deepen their knowledge and understanding of exploit research and development. This comprehensive course is designed to turn students into high-level security experts. Students will learn how to find critical vulnerabilities everywhere in the platforms and exploit them.

Target Audience

This course is aimed at cyber experts interested in studying one of the most important topics in cybersecurity, developing vulnerability exploitation and understanding how researchers find security holes and create their code for exploiting vulnerabilities.

Course Objectives

- Discovering different levels of vulnerabilities, including zero-day vulnerabilities.
- Understanding the methods of attacks.
- Infrastructure and system defense.
- Become familiar with APT and attacks.
- Understanding modern security mechanisms.

Prerequisites

Networking
Penetration Testing
C
Assembly

Module 1: Buffer Overflow Attacks

This module will introduce students to the world of exploit development, explain the basic rules, what needs to be focused on, and create a neat and professional work process. This module will show the basic techniques of binary exploitation.

Anatomy of a Program in Memory

Process Memory Organisation
Memory Stack
Buffer Overflow Concepts and Definitions
Brief on Assembly Registers and Data Organization

Stack Overflow

The Stack Variables
Environment Variables
Overwriting Function Pointers Stored on the Stack
Segmentation Fault Error
Understand Pointers
System Instructions and OPCodes
Executing '\xcc' Instruction
Find Executable Crash-Address
Crashing Executables with Programming
Allocate Buffer Size
Allocate Shellcode Size
Stack Common Defence Mechanisms
Working with NOP
Find JMP Instructions in the Memory
Writing POC Code

Format Strings Vulnerability

Strings Leakage
Modify the Execution Flow of Programs
Modify Arbitrary Memory Locations
Specific Values Assignments
Writing Larger Data to the Process
Redirecting Execution in a Process

Module 2: Advanced Buffer Overflow Attacks

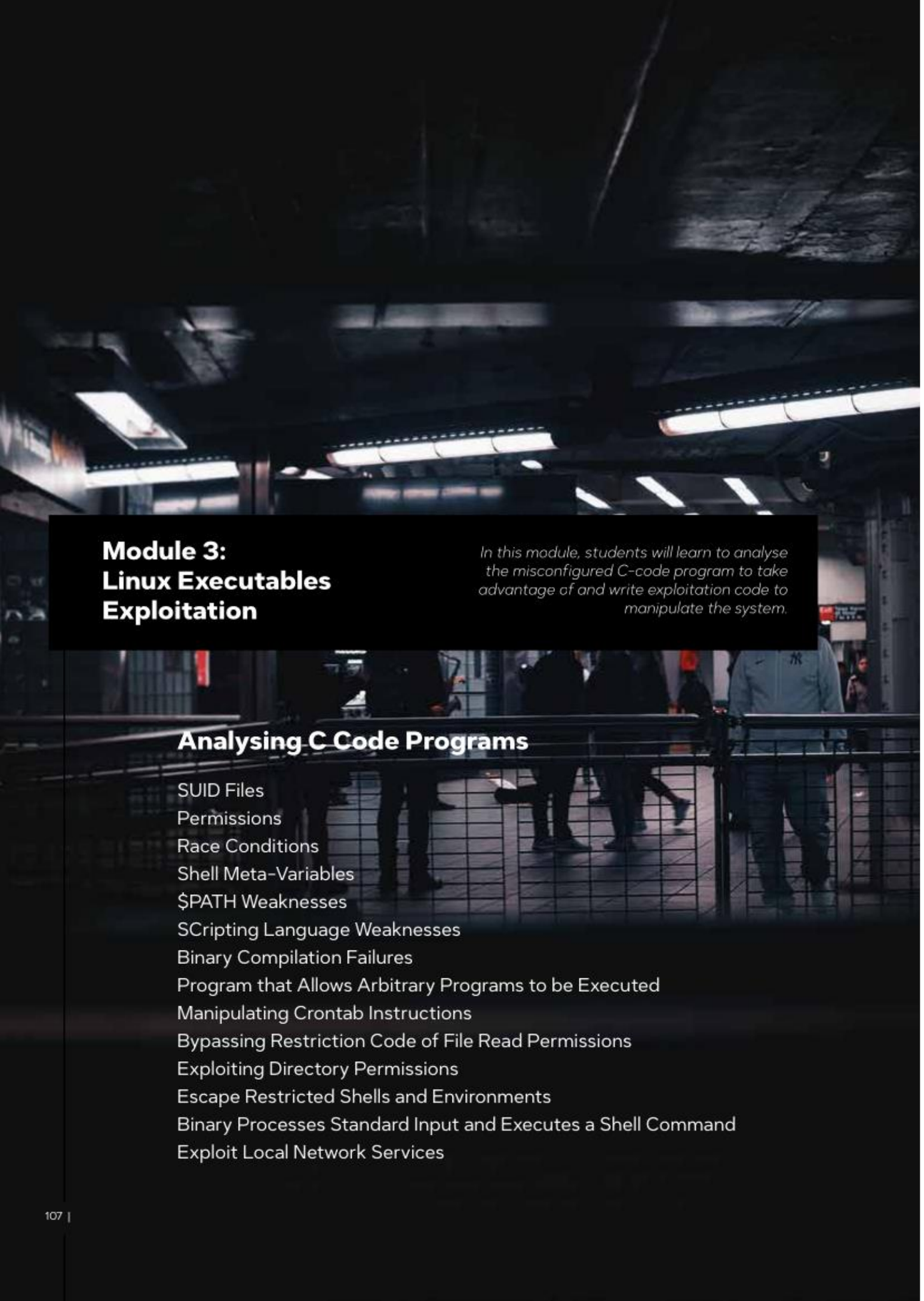
In this module, students will learn about buffer overflow capabilities and present advanced and widely accepted techniques in the world of binary exploitation.

Heap Overflow

Heap Memory Section
Heap Structure and Functionality
Influence the Code Flow
Hijacking the Data Overwrite
Heap Pointers
Heap Metadata
'Dlmalloc' to Change Program Execution

Advanced Overflow Techniques

Converting Strings to Little Endian Integers
Convert Binary Integers to ASCII Representation
Working with 32-bit Unsigned Integers
Remote Blind Format String
Remote Heap Overflow Attack
Heap Overflows using VEH
Heap Overflows using the UEF



Module 3: Linux Executables Exploitation

In this module, students will learn to analyse the misconfigured C-code program to take advantage of and write exploitation code to manipulate the system.

Analysing C Code Programs

- SUID Files
- Permissions
- Race Conditions
- Shell Meta-Variables
- $PATH Weaknesses
- SCripting Language Weaknesses
- Binary Compilation Failures
- Program that Allows Arbitrary Programs to be Executed
- Manipulating Crontab Instructions
- Bypassing Restriction Code of File Read Permissions
- Exploiting Directory Permissions
- Escape Restricted Shells and Environments
- Binary Processes Standard Input and Executes a Shell Command
- Exploit Local Network Services

CX ICS

3 Courses

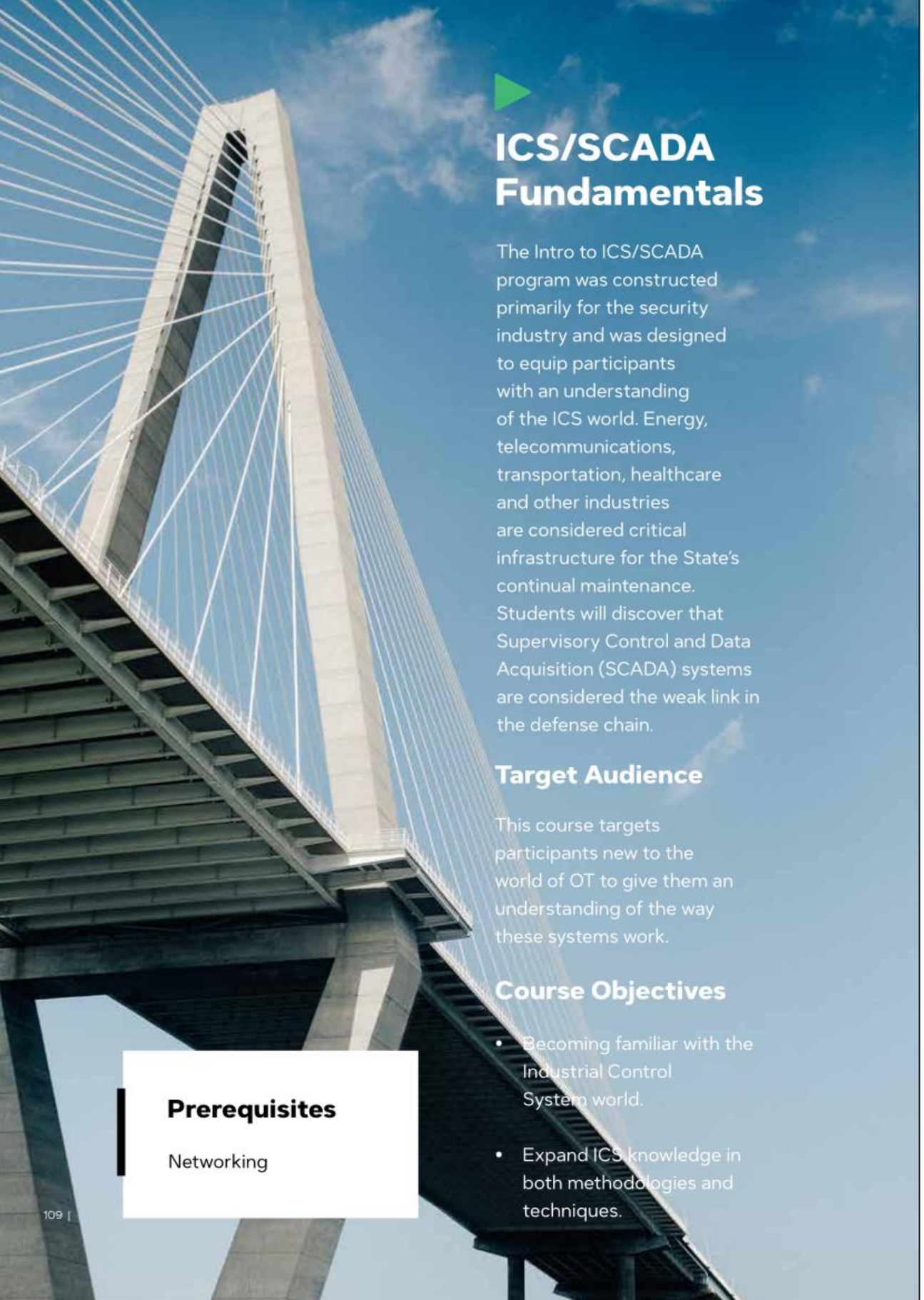
10 Built-in Scenarios

30 Built-in Labs

100 Hours of Training

Overview

The CX ICS suite is a training package designed to train ICS/SCADA teams.



ICS/SCADA Fundamentals

The Intro to ICS/SCADA program was constructed primarily for the security industry and was designed to equip participants with an understanding of the ICS world. Energy, telecommunications, transportation, healthcare and other industries are considered critical infrastructure for the State's continual maintenance. Students will discover that Supervisory Control and Data Acquisition (SCADA) systems are considered the weak link in the defense chain.

Target Audience

This course targets participants new to the world of OT to give them an understanding of the way these systems work.

Course Objectives

- Becoming familiar with the Industrial Control System world.
- Expand ICS knowledge in both methodologies and techniques.

Prerequisites

Networking

Module 1: ICS Overview

Students will get an overview of the ICS/SCADA and learn the basics and structure of Industrial Control Systems during this module.

IT vs. OT

Types of ICS Systems
DCS vs. SCADA

SCADA Components

Human Machine Interface (HMI)
Supervisory System
Remote Terminal Units (RTU's)
Programmable Logic Controllers (PLCs)

ICS Security Overview

Basic Security Concepts
Physical Security
Digital Security
ICS Lifecycle Challenges

Module 2: ICS Protocols

Students will get an overview of the general ICS/SCADA protocols of Industrial Control Systems during this module and learn how they work.

ICS Network

Known ICS Protocols
Modbus
DNP3
How to Approach Protocols Research
ICS Protocol Fuzzing

ICS/SCADA Forensics

Organisations, both civilian and government, are trying to build security teams to protect the ICS/SCADA environment. This program was designed comprehensively to impart the skills and knowledge required to integrate into the information security world's key positions, both in an offensive and defensive capability.

Students will learn about the security threats that are unique to ICS/SCADA systems and the inherent weaknesses and vulnerabilities in Programmable Logic Controllers (PLC's) and Remote Term Units (RTU's) through the use of real-world examples, the frameworks and standards available to help develop an effective ICS/SCADA cybersecurity strategies.

Target Audience

This course targets participants with cybersecurity knowledge and who want to master the forensics knowledge within critical infrastructure.

Course Objectives

- Understand ICS networks on a deep level.
- Monitor user and system activities on the ICS network to recognise patterns of typical attacks.
- Analyse abnormal activity patterns.
- Using tools for intrusion detection.
- Analyse log files and log data.

Prerequisites

Linux
Forensics

Module 1: ICS Risk Assessment

During this module, students will learn how a control system can be attacked from the internet and perform hands on practice sessions on network discovery techniques.

ICS Network

Known ICS Protocols
Modbus
DNP3
How to Approach Protocols Research
ICS Protocol Fuzzing
Host Configuration Overview
Wireless Access Overview
Remote Access Overview
Cybersecurity for ICS
Passive Discovery
ActiveDiscovery
Passive Enumeration
Using CSET
Ladder Logic Overflow
Using Metasploit Framework
Web Hacking Techniques

Module 2: Security Methods and Products

This module will present students with ways to plan, design and implement an effective program to protect SCADA systems. Students will understand common Industrial Control Systems (ICS) threats, vulnerabilities, and risks.

ICS Protection Concepts

Endpoint Defenses
Passive Solutions
Agents
Update and Patching
Hardening Configuration
Auditing Log Management

Network Fundamentals

TCP/IP Protocol Suite
ICS Protocols over TCP/IP
Firewalls
Building an ICS/SCADA Honeypot

Module 3: ICS Network Analysis

ICS Network Analysis revolves around the extraction, analysis and identification of a users online activities.

The findings include artifacts such as logs and history files, cookies, cached content and any remnants of the information left in the computer's volatile memory. During this module, students will identify different user behavior patterns. Upon completion, students will perform a detailed forensic analysis of the network traffic.

Wireshark Analysis

Wireshark Tool Inspection
Using Display Filters
Advanced Usage
Extracting Files from PCAP Files
Reading Encrypted Data with Wireshark
Attack Analysis

Identifying Attacks

Dump Memory from Devices
Network Scanning
MiTM
Brute Force
Injections
Web Server Attacks
Extracting Network Traffic from Memory
Firewall Findings

ICS/SCADA PenTesting

This course covers possible attack methods by hostile entities and the security challenges that naturally follow.

Cyber warfare is one of the most challenging and advanced disciplines in the cybersecurity environment.

Target Audience

This course targets participants with cybersecurity knowledge and who want to master the penetration knowledge within critical infrastructure.

Course Objectives

- Hands on with critical infrastructure protocols and vulnerabilities.
- Various aspects of cyber warfare on the defensive side.
- Expand ICS knowledge in both methodologies and required techniques.

Prerequisites

Linux
Penetration

Module 1: ICS Overview

During this module, students will learn cybersecurity in the context of Industrial Control Systems (ICS). Students will learn how a control system can be attacked from the internet and perform hands on practice sessions on network discovery techniques.

ICS Network

Types of ICS Systems
Human Machine Interface (HMI)
Supervisory System
Remote Terminal Units (RTU's)
Programmable Logic Controllers (PLC's)
Basic Security Concepts
Physical Security
Digital Security
ICS Lifecycle Challenges
ICS Network Architecture
Known ICS Protocols
ICS Protocol Fuzzing

Module 2: ICS Attacks and Vulnerabilities

In this module, we will cover the ways to attack the SCADA environment. Students will be trained on network discovery using Metasploit and practice hands-on Red Team exercises.

Security in ICS

Encryption
Firewalls with ICS
DMZ Approach
Access Control
Intrusion Detection (IDS)
Web Application Attacks

Students will also develop a broader understanding of where these specific attack vectors exist and the tools used to discover vulnerabilities.

Metasploit

ICS Exploitation using Metasploit
Metasploit modules for SCADA
Exploit with Metasploit
Control with Metasploit
ICS Attack Tools
ICS Scanning Tools
Denial of Service (DoS)
Wi-Fi Security Issues
Attacks on HMI

Module 3: ICS Penetration Testing

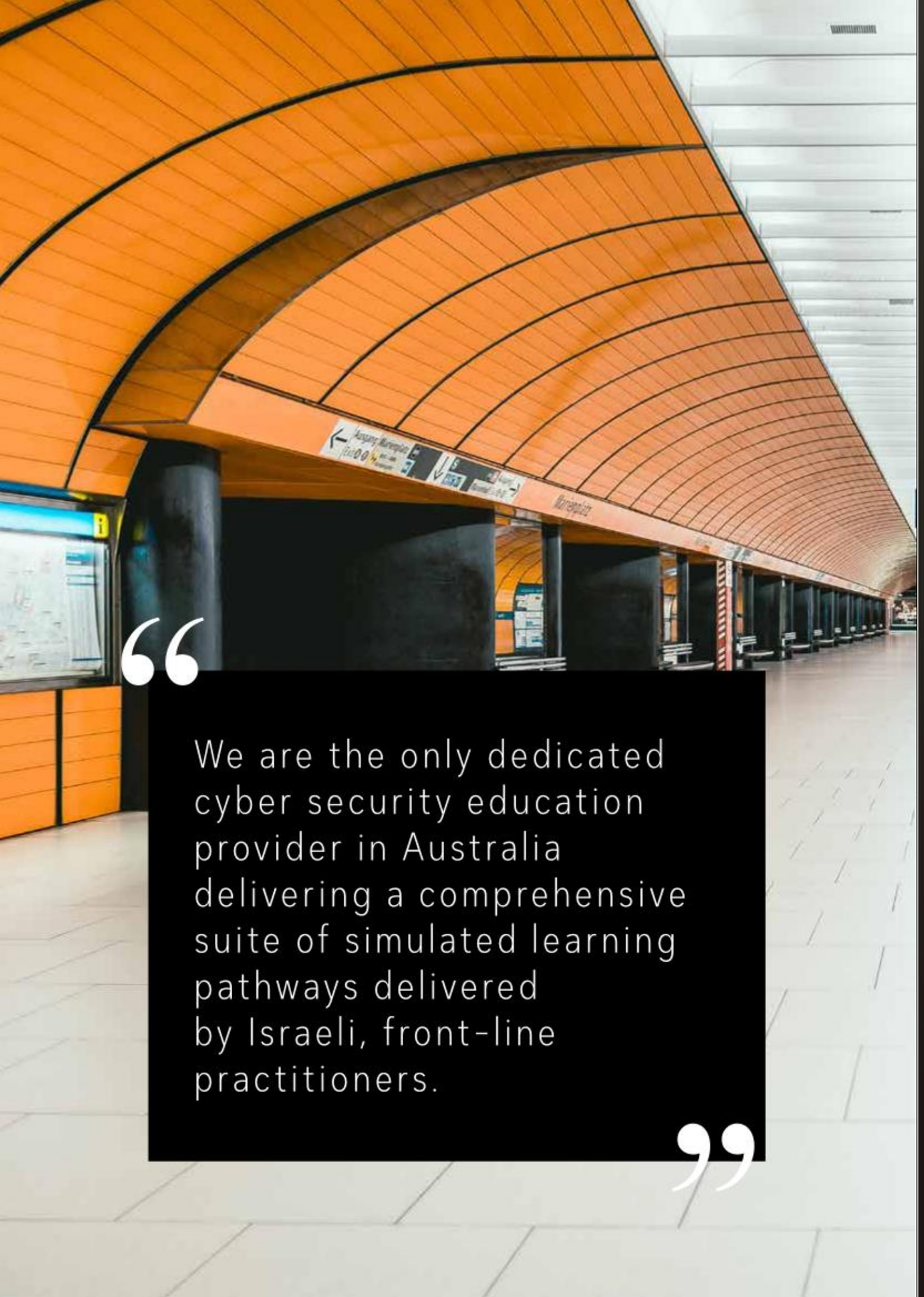
In this module, students will become familiar with ways to plan, design and implement an effective program to protect SCADA systems using Penetration Testing methods. Students will gain knowledge of conducting these tests in the "Test Environment" using advanced techniques.

Preparing for Penetration Testing

Setting up a Virtual Machine for Penetration Testing
Creation your VM Network
Architectures Overview
Testing your Network
Gathering Information PAssively
Port Scanning
System Fingerprinting

Vulnerabilities

Checking for Vulnerabilities
Analysing Services and Ports
Analysing Communications
Testing for Vulnerabilities on User Interfaces
Searching for Web Applications Vulnerabilities
Testing for Vulnerabilities on Network Protocols
Protocol Analysis
Using Network Based Signatures
Sniffing Network Traffic
Testing for Vulnerabilities in Embedded Devices
Firmware Fuzzing
Analysing the Firmware
Exploiting Firmware Vulnerabilities
Security Assessment.



“We are the only dedicated cyber security education provider in Australia delivering a comprehensive suite of simulated learning pathways delivered by Israeli, front-line practitioners.”

cellcyber.com.au

Cell-cyber