

CYBER SCHEME FOUNDATION LEVEL - Training Course Syllabus 2023

The Cyber Scheme has developed the CSFL assessment to measure the competence of a junior and/or graduate cyber security professional looking for an entry level role.

To support the assessment, The Cyber Scheme has developed a comprehensive training course which will highlight and enhance the skills and knowledge required in order to be successful in the exam.

See below the topics which will be covered in our training course. Please note we offer small class, face-to-face training with opportunities to identify and address specific knowledge gaps directly with our trainers.

The Laws and Ethics Associated with Security Testing

- Understands and can apply the Computer Misuse Act to stay within a scope
- Has knowledge of how the PJA / RIPA laws affect security testing
- Is aware of how the GDPR and the DPA affects security testing
- Understands how the HRA has to be applied as part of a security test
- Has an understanding of ACPO (Formerly known as) and where it applies
- Understands what should be in a scope and keeping to scope
- Understands the risks associated with any form of security testing.

Building and Maintaining a Security Testing Device

- Can recommend and implement full disk encryption
- Understands the fundamentals of using virtualised and non-virtualised distros for security testing
- Can demonstrate how to install and maintain a security testing distro
- Can justify the use of administrative and non-administrative accounts for security testing
- Can customise a security testing distro to complete an engagement based on a scoping document.

Fundamental Linux CLI for the Purpose of Security Testing

- Understands the folder structure and standards used on device with a Linux operating system
- Can demonstrate how to list a range of files and can explain the displayed output
- Can demonstrate how to manipulate a range of files using a range of applications
- Understands how to copy, move and delete files on a Linux file system
- Can manipulate and navigate the directory structure of a Linux File system
- Can demonstrate setting up file permissions and can justify the choices made
- Understands the use of escalation techniques to prevent overuse of the superuser in a Linux environment
- Can demonstrate the use of search tools, filters and pipes
- Can competently make use of foreground and background processes

- Can demonstrate the use of the tools available in a Linux environment to trouble shoot networking issues
- Understands a range of administrative protocols used to administer a Linux system
- Understands the use remote file systems both for enumeration and configuration purposes
- Can demonstrate how to administer user accounts and understand the fundamental technologies in use
- Understands the file compression techniques available in a Linux environment
- Can use local resources for tool and utility advice and guidance
- Can demonstrate the configuration and enumeration of timed events to administer a Linux system.

Fundamental Linux scripting for the Purposes of Security Testing

- Understands the fundamentals of using a Shebang
- Can input and output data to the various streams
- Understands the use of arguments when writing scripts and utilities
- Can demonstrate the use of Arrays and complex data structures
- Can use the correct operators to achieve a set objective
- Can use code-based decision making
- Understands the importance of iteration in program code and scripting
- Can demonstrate the use of meta characters and how to escape them
- Can redirect output and input streams
- Can justify the use of Functions and Returns for structured code practices.

Fundamental Python coding for Ethical Hackers

- Understands the layout, principles, and construction of python code
- Understands the use of variables, types and data structures
- Can demonstrate the use of the List data type
- Can select the correct operators to fulfil an objective
- Can construct and manipulate string data types using the python language
- Can use conditions and code-based decision making
- Can construct iteration code to apply secure coding principles
- Can use functions to apply the "DRY" coding principle
- Understands the use of classes and objects in the python language.

Fundamental Windows Operating System commands

- Understands how to manipulate files and folders including hidden files in a Windows environment
- Can demonstrate how to traverse and manipulate the directory structure
- Understands how to enumerate and manipulate a Windows system for users, shares and policies using the command line interface (CLI)

- Understands the difference between the domain controller (DC), workstations and non-domain joined devices
- Understands how to read and write to the file system using various techniques
- Understands user privileges and the security models available in Windows environments
- Can demonstrate the use of network trouble shooting tools and utilities to solve commonly found issues
- Can demonstrate basic PowerShell commands and understands the security model in place
- Understands the fundamental principles of the remote desktop protocol, virtual network computing and secure shell in a Windows Environment
- Understands the networking configuration and how to enumerate it in a Windows operating system
- Understands the concept of password hashing, brute forcing and using MFA.

Computer Networking Fundamentals

- Understands the use of DNS, and the DNS record types
- Understands the ARP protocol and its uses
- Understands the use of gateway devices to divide subnets
- Understands the 7 layer OSI model and the 4 layer DoD model
- Has a fundamental grip on the TCP/IP suite of protocols including UDP
- Understands a range of management protocols on a computer network.

Packet capturing for security testing and ethical hacking

- Can demonstrate the configuration of packet capturing software
- Can capture and analyse the various network packets on a TCP network
- Understands how to apply filters to packet capturing tools
- Can demonstrate the capturing of TCP streams and interpret the data.

Web application Fundamentals

- Understands the send and receive HTTP model
- Understands the concept of session tokens to identify user sessions
- Can demonstrate how to run scripts embedded in HTML pages.
- Understands security headers and can recommend improvements based on a scenario
- Understands the response and error codes associated with the HTTP(s) protocol.

Vulnerability Analysis Fundamentals

- Can demonstrate the installation and configuration of VA software and tools
- Can demonstrate the configuration of a scan to achieve a set goal
- Can check for false positives and understands the VA tool output

- Understands how to configure VA software to complete a credentialed security test
- Understands how to configure VA software to complete a CIS benchmark security test
- Understands the basics of using The Common Vulnerability Scoring System (CVSS)
- Understands the basics of port scanning.

Testing Mobile Devices Fundamentals

- Understands the function of mobile device management (MDM)
- Can determine if a device is jailbroken
- Can check and recommend patching and software levels
- Understands mobile technical controls
- Understands the file types associated with mobile applications

An Introduction to Testing in the Cloud

- Understands the basics of Cloud security testing.
- Understands the basics principles of testing within Azure
- Understands the basics principles of testing within AWS.