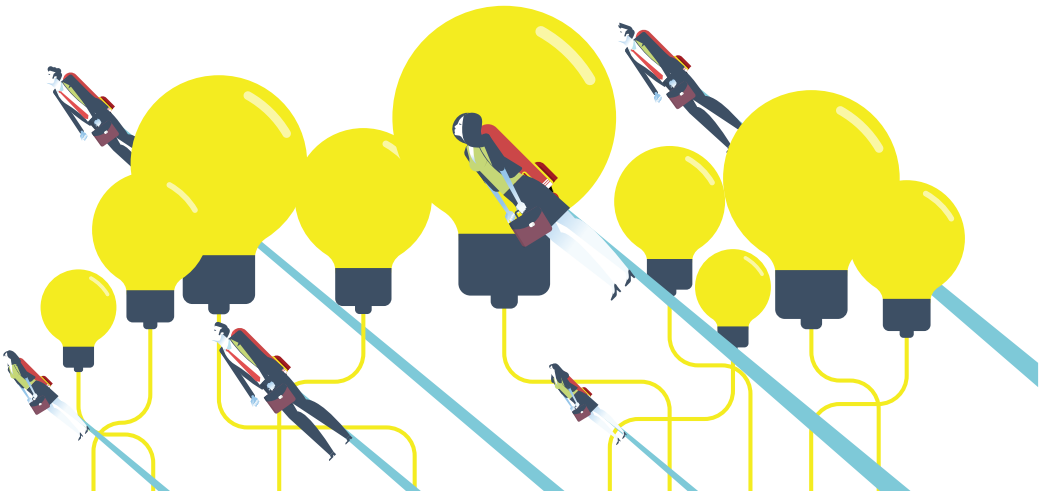
THE CSFL
(CYBER SCHEME FOUNDATION LEVEL).

TRAINING AND ASSESSMENT
TO MEASURE AND RECOGNISE THE COMPETENCE
OF JUNIOR TECHNICAL CONSULTANTS.



ABOUT THE TRAINING AND EXAM

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.

CSFL provides a technical introduction into cyber security in general; it will highlight and enhance the skills and knowledge required at this beginner level, whilst measuring competence.

Practical skills, technical knowledge and a pathway to Professional Registration

The CSFL is currently being mapped to CyBOK and SFIA. This assessment also provides access to the Associate Level Professional Title, allowing individuals to begin their professional career with a recognised pathway endorsed by the UK Government. It is expected that anyone successfully completing the assessment will be awarded the Associate Level Professional Title from the UK Cyber Security Council.

Training

Live training – the sure route to success. Available anywhere worldwide with our remote learning course.

As soon as candidates begin the course they will be immersed in the world of cyber security with practical hands-on exercises and expert tuition from a Cyber Scheme Instructor. They will learn about Linux systems, Windows systems, how to script in bash and in python. Also taught are the fundamentals of computer networking, web application technologies and vulnerability scanning, as well as the laws and ethics associated with security testing. This training will give candidates the essential skills of an ethical hacker at junior level.

The Assessment

The assessment will combine practical skills with a demonstration of knowledge and understanding, delivered through a presentation and a technical interview.

The assessment is open book; however, candidates will need to showcase their technical ability rather than rely solely on resources. The assessment will not be a long or arduous process and will adopt a more sample-based approach to evaluating candidates.

Presentation and resource preparation: 60 minutes

Technical showcase: 15 minutes

Interview: 15 minutes

KNOWLEDGE DOMAINS

- The Laws and Ethics Associated with Security Testing
- Building and Maintaining a Security Testing Device
- Fundamental Linux CLI for the Purpose of Security Testing
- Fundamental Linux scripting for the Purposes of Security Testing
- Fundamental Python coding for Ethical Hackers
- Fundamental Windows Operating System commands
- Computer Networking Fundamentals
- Packet capturing for security testing and ethical hacking
- Web application Fundamentals
- Vulnerability Analysis Fundamentals
- Testing Mobile Devices Fundamentals
- An Introduction to Testing in the Cloud

Please note the knowledge domains and topics outlined in this document are for guidance only and subject to change.

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 Linux scripting

Understands the importance of iteration in program code and scripting

Can justify the use of Functions and Returns for structured code practices

Can read and evaluate scripts

Can reuse and modify scripts

Can use AI to vibe code for hacking purposes.

FUNDAMENTAL PYTHON CODING FOR ETHICAL HACKERS

Understands the layout, principles, and construction of python code

Can construct iteration code to apply secure coding principles

Can use functions to apply the “DRY” coding principle

Understands the fundamentals of Python code

Can read and evaluate Python code

Can reuse and modify Python code

Can use AI to vibe code for hacking purposes.

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.