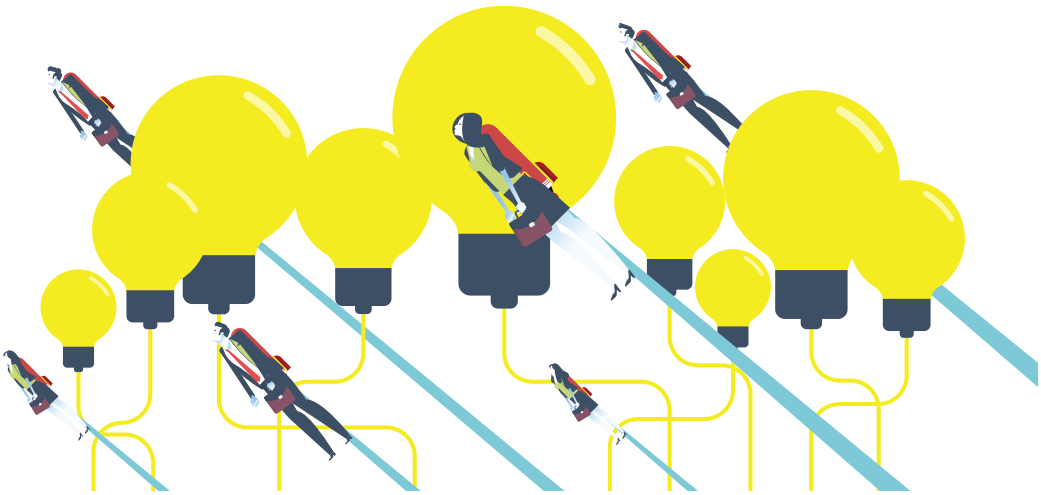
THE CSFL
(CYBER SCHEME FOUNDATION LEVEL).

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

1. The Laws and Ethics Associated with Security Testing
2. Building and Maintaining a Security Testing Device
3. Fundamental Linux CLI for the Purpose of Security Testing
4. Fundamental Linux scripting for the Purposes of Security Testing
5. Fundamental Python coding for Ethical Hackers
6. Fundamental Windows Operating System commands
7. Computer Networking Fundamentals
8. Packet capturing for security testing and ethical hacking
9. Web application Fundamentals
10. Vulnerability Analysis Fundamentals
11. Testing Mobile Devices Fundamentals
12. 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.

1. THE LAWS AND ETHICS ASSOCIATED WITH SECURITY TESTING

1.1 Understands and can apply the Computer Misuse Act to stay within a scope

1.2 Has knowledge of how the PJA / RIPA laws affect security testing

1.3 Is aware of how the GDPR and the DPA affects security testing

1.4 Understands how the HRA has to be applied as part of a security test

1.5 Has an understanding of ACPO (Formerly known as) and where it applies

1.6 Understands what should be in a scope and keeping to scope

1.7 Understands the risks associated with any form of security testing.

2. BUILDING AND MAINTAINING A SECURITY TESTING DEVICE

2.1 Can recommend and implement full disk encryption

2.2 Understands the fundamentals of using virtualised and non-virtualised distros for security testing

2.3 Can demonstrate how to install and maintain a security testing distro

2.4 Can justify the use of administrative and non-administrative accounts for security testing

2.5 Can customise a security testing distro to complete an engagement based on a scoping document.

3. FUNDAMENTAL LINUX CLI FOR THE PURPOSE OF SECURITY TESTING

3.1 Understands the folder structure and standards used on device with a Linux operating system

3.2 Can demonstrate how to list a range of files and can explain the displayed output

3.3 Can demonstrate how to manipulate a range of files using a range of applications

3.4 Understands how to copy, move and delete files on a Linux file system

3.5 Can manipulate and navigate the directory structure of a Linux File system

3.6 Can demonstrate setting up file permissions and can justify the choices made

3.7 Understands the use of escalation techniques to prevent overuse of the superuser in a Linux environment

3.8 Can demonstrate the use of search tools, filters and pipes

3.9 Can competently make use of foreground and background processes

3.10 Can demonstrate the use of the tools available in a Linux environment to trouble shoot networking issues

3.11 Understands a range of administrative protocols used to administer a Linux system

3.12 Understands the use remote file systems both for enumeration and configuration purposes

3.13 Can demonstrate how to administer user accounts and understand the fundamental technologies in use

3.14 Understands the file compression techniques available in a Linux environment

3.15 Can use local resources for tool and utility advice and guidance

3.16 Can demonstrate the configuration and enumeration of timed events to administer a Linux system.

4. FUNDAMENTAL LINUX SCRIPTING FOR THE PURPOSES OF SECURITY TESTING

4.1 Understands the fundamentals of Linux scripting

4.2 Understands the importance of iteration in program code and scripting

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

4.4 Can read and evaluate scripts

4.5 Can reuse and modify scripts

4.6 Can use AI to vibe code for hacking purposes.

5. FUNDAMENTAL PYTHON CODING FOR ETHICAL HACKERS

5.1 Understands the layout, principles, and construction of python code

5.2 Can construct iteration code to apply secure coding principles

5.3 Can use functions to apply the “DRY” coding principle

5.4 Understands the fundamentals of Python code

5.5 Can read and evaluate Python code

5.6 Can reuse and modify Python code

5.7 Can use AI to vibe code for hacking purposes.

6. FUNDAMENTAL WINDOWS OPERATING SYSTEM COMMANDS

6.1 Understands how to manipulate files and folders including hidden files in a Windows environment

6.2 Can demonstrate how to traverse and manipulate the directory structure

6.3 Understands how to enumerate and manipulate a Windows system for users, shares and policies using the command line interface (CLI)

6.4 Understands the difference between the domain controller (DC), workstations and non-domain joined devices

6.5 Understands how to read and write to the file system using various techniques

6.6 Understands user privileges and the security models available in Windows environments

6.7 Can demonstrate the use of network trouble shooting tools and utilities to solve commonly found issues

6.8 Can demonstrate basic PowerShell commands and understands the security model in place

6.9 Understands the fundamental principles of the remote desktop protocol, virtual network computing and secure shell in a Windows Environment

6.10 Understands the networking configuration and how to enumerate it in a Windows operating system

6.11 Understands the concept of password hashing, brute forcing and using MFA.

7. COMPUTER NETWORKING FUNDAMENTALS

7.1 Understands the use of DNS, and the DNS record types

7.2 Understands the ARP protocol and its uses

7.3 Understands the use of gateway devices to divide subnets

7.4 Understands the 7 layer OSI model and the 4 layer DoD model

7.5 Has a fundamental grip on the TCP/IP suite of protocols including UDP

7.6 Understands a range of management protocols on a computer network.

8. PACKET CAPTURING FOR SECURITY TESTING AND ETHICAL HACKING

8.1 Can demonstrate the configuration of packet capturing software

8.2 Can capture and analyse the various network packets on a TCP network

8.3 Understands how to apply filters to packet capturing tools

8.4 Can demonstrate the capturing of TCP streams and interpret the data.

9. WEB APPLICATION FUNDAMENTALS

9.1 Understands the send and receive HTTP model

9.2 Understands the concept of session tokens to identify user sessions

9.3 Can demonstrate how to run scripts embedded in HTML pages.

9.4 Understands security headers and can recommend improvements based on a scenario

9.5 Understands the response and error codes associated with the HTTP(s) protocol.

10. VULNERABILITY ANALYSIS FUNDAMENTALS

10.1 Can demonstrate the installation and configuration of VA software and tools

10.2 Can demonstrate the configuration of a scan to achieve a set goal

10.3 Can check for false positives and understands the VA tool output

10.4 Understands how to configure VA software to complete a credentialed security test

10.5 Understands how to configure VA software to complete a CIS benchmark security test

10.6 Understands the basics of using The Common Vulnerability Scoring System (CVSS)

10.7 Understands the basics of port scanning.

11. TESTING MOBILE DEVICES FUNDAMENTALS

11.1 Understands the function of mobile device management (MDM)

11.2 Can determine if a device is jailbroken

11.3 Can check and recommend patching and software levels

11.4 Understands mobile technical controls

11.5 Understands the file types associated with mobile applications.

12. AN INTRODUCTION TO TESTING IN THE CLOUD

12.1 Understands the basics of Cloud security testing

12.2 Understands the basics principles of testing within Azure

12.3 Understands the basics principles of testing within AWS.