THE CSTM (CYBER SCHEME TEAM MEMBER):

TECHNICAL INTERVIEW QUESTIONS

CSTM TECHNICAL QUESTIONS

To reduce the likelihood of an over-reliance on AI undermining the validity of the CSTM assessment, and protect its quality and integrity, we are adjusting the technical interview component.

This change is aligned to our ongoing commitment to ISO 27001, which requires us to maintain robust, secure, and reliable assessment processes and ensure that our certification methods remain resilient against emerging technological risks.

From 1 March 2026, the technical interview will become closed book, with all questions available in this document and on our website. This approach allows us to maintain transparency (a core ISO 27001 principle), while reducing the likelihood of AI-driven automation undermining the validity of the assessment.

The practical CSTM element will remain open book.

Questions fall into the following categories:

Current Technology

Older Technology

Networking

Protocols

Mitigation

Scope/Laws/Risk

Please note the questions outlined in this document are subject to change as needed.

1. CURRENT TECHNOLOGY

What is Root Squashing?

Explain how run0 and the polkit can be used as a more secure alternative to sudo on Linux platforms.

What is DMARC (Domain-based Message Authentication, Reporting, and Conformance)?

What is the purpose of the Sender Policy Framework (SPF)?

What is the purpose of DomainKeys Identified Mail (DKIM)?

What are the security issues with the FTP protocol?

What is Kerberos?

Explain directory traversal exploitation

What are the four types of Application Programming Interface (API)?

How would you fingerprint a database server?

Explain symmetrical and asymmetrical cryptography

What is the difference between SQL and no SQL database vulnerabilities?

What is the Open Vulnerability and Assessment Language (OVAL)?

Explain the difference between Phishing, Smishing and Vishing and what risks do they pose?

What tools could you use to enumerate Domain Name System (DNS) for ZONE transfer vulnerabilities?

Explain what a Security identifier (SID) is and the different parts of a SID.

What are the two IPsec encoding methods and what are the pros and cons of each?

In key signing do you use the private or public key for signing?

What ports need to be open on a domain controller (DC)?

Explain the Simple Network Management Protocol (SNMP) protocol and any weaknesses in the protocol

What are the trade-offs between symmetrical and asymmetrical cryptography?

Explain some vulnerabilities in SSL (Secure Sockets Layer) and TLS (Transport Layer Security)?

Explain the purpose of a Remote Authentication Dial-In User Service (RADUIS) server

Where are passwords stored on server devices?

Explain Structured Query Language injection (SQLi)

1. CURRENT TECHNOLOGY

If password hashes cannot be cracked can the hashes be used in any way and how would you do this?

Explain how a Cross-Site Request Forgery (CSRF) exploit works

Explain session hijacking (with respect to web application testing)

What is Internet Information Service (IIS)?

Explain baseboard management controller (BMC) Hacking and the Intelligent Platform Management Interface (IPMI)

What are the pros and cons of using the cloud vs on prem (in terms of cyber security)?

What technical controls are available in the cloud to help with cyber security?

What are the most popular containerization solutions?

What's the difference between virtual machines and containerization?

What are the signs a mobile device has been jail broken?

What file types are associated with android apps?

What file types are associated with apple apps?

Explain the use case for Datagram Transport Layer Security (DTLS).

What are the built-in user accounts on a Windows server?

Name some protocols in the Industrial control system (ICS) / Operational Technology (OT) space?

2. OLDER TECHNOLOGY

Name some security models and what is the purpose of security models?

What are the issues with the Wired Equivalent Privacy (WEP) protocol?

What are the security issues associated with Lanman (LM) passwords?

Explain the purpose of the phpMyAdmin application.

How would you find and download files from a File Transfer Protocol (FTP) server or a Trivial File Transfer Protocol (TFTP) server?

What enumeration can the Simple Mail Transfer Protocol (SMTP) service be used for?

What is steganography?

What is a relative identifier (RID) Master?

Explain Hashing functions ie MD5 and SHA1

Explain with examples some protocols used for Wide Area Networks (WAN)

What is a One-Time-Pad?

What is a Schema Master?

Explain null sessions and restrict anonymous settings

What vulnerability might be present if Server Message Block (SMB) version 1 was enabled on a Windows device?

3. NETWORKING

Explain the Open Systems Interconnection (OSI) model

Explain the Department of Defense (DoD) networking model

Explain how Dynamic Host Configuration Protocol (DHCP) works

What is a Start of Authority (SOA) record - with respect to Domain Name System (DNS)?

Explain what Domain Name System (DNS) is and explain how DNS works.

Explain the IP protocol and explain IP addresses.

Explain Classless Inter-Domain Routing (CIDR)

Explain how Machine-in-the-Middle (MITM) techniques work with the Address Resolution Protocol (ARP).

What is the function of Port Address Translation (PAT)?

What is the Lightweight Directory Access Protocol (LDAP)?

Name and explain two distance vector routing protocols

Explain Medium Access Control (MAC) addresses and explain what an Organizationally Unique Identifier (OUI) is?

What is firewalking (with respect to network security)?

Explain the Wi-Fi Protected Access (WPA) protocol

Explain IPSec

Where would you find the hosts file and what is its purpose of this file?

Explain how Virtual Local Area Networks (VLANS) work

Explain the purpose of a Terminal Access Controller Access Control System (TACACS)

Why are CLOSED ports a cause for concern?

How would you set a source port in nmap and why would you use this feature?

4. PROTOCOLS

Explain the Address Resolution Protocol (ARP) protocol

Explain the Internet Control Message Protocol (ICMP) protocol

Explain the User Datagram Protocol (UDP) protocol

What are the response codes for the Hypertext Transfer Protocol (http) protocol?

Explain IPV6 and why its not widely adopted

What are the two IPSec Modes

What is the Intermediate System to Intermediate System (IS-IS) protocol?

Explain the Network File System (NFS) protocol

Explain the Internet Key Exchange (IKE) Protocol

What protocols are associated with Virtual Private Network (VPN)?

What protocols are associated with Voice over Internet Protocol (VOIP)?

Name and explain a Kerberos exploit?

What is a Pre-Shared Key (PSK) used for and what are the issues with its use?

How many versions of the Network File System (NFS) protocol are there and what is the compatibility between the versions?

5. MITIGATION

How do you mitigate Server Message Block (SMB) issues?

How do you mitigate an external facing Remote Desktop Protocol (RDP) server with an expired Transport Layer Security (TLS) certificate?

How do you mitigate machine in the middle (MITM) attacks?

How do you mitigate Structured Query Language injection (SQLi)?

How do you mitigate socially engineered staff?

How do you mitigate a Cross-Site Scripting (XSS) vulnerability?

What is the mitigation for a ransomware attack where files have been locked?

6. SCOPE/LAWS/RISK

What should be in a scope document for a security test?

What laws affect security testing?

What risk mitigation can you put in place before conducting a security test?

What is the Common Vulnerability Scoring System (CVSS) and Common vulnerabilities and Exposures (CVE)?

What are the testing regulations regarding CHECK level testing?

What part of the Human Rights Act 1998 affects pen testers?

What is the Regulation of Investigatory Powers Act 2000 (RIPA) and does it affect security testing?

What is the General Data Protection Regulation (GDPR) and how does it affect security testing?

Name and explain three security standards

What are the risks of enumerating and vulnerability assessing a multifunction printing device?

What are the risks of enumerating and vulnerability assessing an ICS device?

What is the Police and Justice Act 2006 (PJA) and how does it affect security testing?

Explain how to keep to scope during a security test.