1. What type of authentication system requests a username, a password and requires the user to type the code displayed on a disconnected token generator?

A Message.

B Double.

C Complex.

D Two-factor.

1. Why is it good practice for an organisation to place a shredder next to a network printer?

A To encourage employees to securely destroy all unwanted prints.

B So that misprints can be easily disposed of by employees.

C To encourage employees to recycle unwanted copies.

D To keep the print room tidy and safe from slip hazards.

1. Which of the following describes a Zero-day software vulnerability?

A It is considered as a low priority business risk by developers and vendors.

B It is known to the vendor as an auxiliary non-critical information.

C It is not known to the vendor until it is exploited by hackers.

D It is exploitable by the tech savvy employees working for the vendor.

1. What is the importance of patching-up security issues of antivirus software?

A To prevent vulnerabilities from being exploited.

B To comply with company maintenance schedule.

C To ensure all software code is unaffected.

D To comply with licencing agreements.

1. Which of the following methods is likely to produce the LEAST problems in password management by employees?

A Enforcing password changes every month.

B Allowing staff to choose their own passwords.

C Issuing centrally-assigned passwords.

D Training staff to use mnemonic-based passwords.

1. Which risk mitigation technique is used to counter the threat of repudiation?

A Installing load balancers.

B Using a strong encryption.

C Prompt system patching.

D Enabling system auditing.

1. What term is applied to a physical or logical subnetwork that exposes an organisation’s external facing servers to an untrusted network, such as the Internet?

A Corporate Server Zone (CSZ).

B Reverse Proxy Zone (RPZ).

C Unrestricted Zone (URZ

D Demilitarised Zone (DMZ).

1. An organisation would use a demilitarised zone (DMZ) to avoid exposure of which of the following?

A Its computers to the internet.

B Its computers to the firewall.

C Its firewall to the Internet.

D The Internet to its business processes.

1. Which of the following responses accurately describes Payment Card Industry Data Security Standard (PCI DSS) compliance?

A An organisation can guarantee that credit card and financial data will never be lost.

B An organisation has followed the rules set forth in the PCI DSS standard and can offer proof in the form of documentation.

C An organisation is not liable if credit card or other personal data is lost or stolen.

D An organisation does not store PAN or CVV data under any circumstances.

1. Which of the following is NOT a benefit of implementing Virtual LANs (VLAN) within a network?

A Reduced broadcast traffic.

B Greater network segregation.

C Enhanced security policy enforcement.

D Lower administrative overhead.

1. During a network DDoS attack, implementation of which of the following controls is MOST LIKELY to support network availability?

A IP address blacklisting.

B Hardware based load balancers.

C IP address whitelisting.

D Web Application Firewall (WAF).

1. Which of the following provides the BEST increase in integrity when implementing a Full Disk Encryption (FDE) solution for an end-user laptop?

A Trusted Platform Module (TPM).

B Hardware Security Module (HSM).

C Public Key Infrastrcuture (PKI).

D Advanced Encryption Standard (AES).

1. Which of the following is GENERALLY considered as the MOST secure identification technology?

A Biometrics.

B Barcode cards.

C Personal Identification Numbers (PINs).

D One-time passwords.

1. Which type of proxy server retrieves resources on behalf of a client from one or more servers?

A Open.

B Reverse.

CTrans.

DSOCKS.

1. Parameterised queries in SQL are used to protect databases against which type of attack?

A Operating system vulnerabilities.

B Unauthorised privilege elevation.

C Privilege abuse.

D SQL injection.

1. What type of access control is implemented where a database administrator can grant UPDATE privileges in a database to specific users or groups?

A Supplemental.

B Discretionary.

C Mandatory.

D System.

1. According to the SANS Top 20 Critical Security Controls for Effective Cyber Defence, which of the following is NOT a critical security control?

A Physical protection.

B Data protection.

C Boundary defence.

D Malware defence.

1. What is the purpose of DMZ?

A To act as an additional security level for a switch.

B To act as an additional security level for a router.

C To allow two trusted networks to operate securely without a firewall.

D To add an additional layer of security to a local area network (LAN).

1. Which type of penetration testing provides the MOST realistic assessment of a real-world attack by an external threat actor?

A Black box.

B Orange box.

C White box.

D Grey box.

1. When designing a secure login portal for a website, which of the following control combinations provides the BEST confidentiality, integrity and availability?

A Single-factor authentication, HTTP and stateful firewall.

B Multi-factor authentication, HTTPS and Web Application Firewall (WAF).

C Single-factor authentication, HTTPS and layer 2 firewall.

D Multi-factor authentication, HTTPS and stateful firewall.