1. Which of the following statements is TRUE for the process of mutual authentication?

A Two remote systems authenticate each other at the same time.

B Two remote systems authenticate each other in sequence.

C Three or more remote systems authenticate each other at the same time.

D Three or more remote systems authenticate each other in sequence.

1. Which of the following is a feature of symmetric encryption?

A Only the recipient must know the secret key.

B The keys can safely be published online.

C Two keys exist, one to encrypt the message, the other to decrypt the message.

D The same key is used to decrypt and encrypt.

1. Which of the following is LEAST LIKELY to be placed in a corporate DMZ?

A Web servers.

B FTP servers.

C Database servers.

D Mail servers.

1. Security SHOULD first become involved in which stage of the application development life cycle?

A Prior to the implementation of the application.

B Prior to user acceptance testing.

C During unit testing.

D During requirements development.

1. What is the BEST practice when installing anti-virus updates?

A Update as soon as possible.

B Wait to get feedback first about the update.

C It is working fine as it is, update in the future.

D Wait 3 months to make sure that there are no bugs.

1. Which of the following is an example of social engineering?

A Sending an email with a malicious link attached requesting information to be added.

B Sending an email and offering to pay for an organisations data.

C Sending an email demanding your personal details be removed from a data list.

D Sending an email to return sensitive information you have been sent.

1. An application fails to error check input between data or code. Which OWASP Top 10 vulnerability is MOST LIKELY to occur in the application?

A Injection Attack.

B Insecure direct object references.

C Failure to restrict URL access.

D Insufficient transport layer protection.

1. A security administrator is evaluating various firewalls to find the best solution for an office environment with an email server. Which of the following is an undesirable feature of a firewall in this environment?

A Only specified traffic can be allowed to pass through.

B The firewall itself should be immune to penetration.

C It should allow for configuration changes by authorised users.

D It must only allow network traffic to travel from inside the network to the Internet.

1. Which one of the following is GENERALLY a poor practice for managing passwords?

A Passwords should be changed once in 5 years.

B Users must change their passwords at their first login.

C It contains upper and lower-case characters.

D It contains numbers and special characters.

1. What term is used where an organisation selectively defines the path that certain packets take through their network?

A Dynamic routing.

B Static routing.

C Policy-based routing.

D Snapshot routing.

1. Which three of the following SHOULD the security administrator implement to limit web traffic based on country of origin?

a) Spam Filter. b) Load Balancer. c) Antivirus. d) Proxies. e) Firewall.

f) NIDS. g) URL Filtering.

Aa, b and g only.

B d, e and f only.

Cc, f and g only.

Da, b and e only.

1. Which of the following are suitable for a secure transfer of data?

A SSL and TELNET.

B SSH and SFTP.

C SFTP and TELNET.

D None of these.

1. Biometric authentication, electromagnetic shielding and advanced locking mechanisms are TYPICALLY used as security in which OSI Layer?

A Network.

B Physical.

C Transport.

D Presentation.

1. An example of a system that is able to control access to network resources, enforce policies and supply the information necessary to bill for services is?

A An intrusion detection system.

B A state ful firewall.

C A RADIUS server.

D An intrusion protection system.

1. What is the purpose of a hash function in a secure exchange of messages over open networks?

A It secures data from an attack by an eavesdropper.

B It allows a user to check if the original data has been tampered with.

C It encrypts the data to prevent reading by unauthorised users.

D It creates a secure digital envelope for data.

1. A system having INCORRECT permissions set on files, folders, and symbolic links has which of the following?

A Vulnerabilities.

B Threats.

C Risks.

D Exploits.

1. You are setting up a single sign-on authentication system for a large enterprise LAN containing 5000 users. Which of the following authentication protocols would be MOSTappropriate?

A SAML.

B XACML.

C SASL.

D Kerberos.

1. Select the MOST significant concern to an organisation when storing data across a cloud provider’s network which is geographically distributed?

A It has data sovereignty concerns for the stored data across geo-political locations.

B Network latency between sites may increase.

C Confidentiality of the stored data is an increased security concern.

D Data recovery becomes harder due to accessibility issues across multiple gro-political locations.

1. Which of the following accreditation bodies in the UK run an accreditation process for organisations providing penetration testing?

A CREST (The Council for Registered Ethical Security Testers).

B EC Council.

C ISC2 (International Information System Security Certification Consortium).

D ISACA (Information Systems Audit and Control Association).

1. Which of the following is a characteristic of a RADIUS system?

A It is a hardened file access system.

B It operates at the Transport layer to identify duplicate network segments.

C It provides centralised Triple A management for users who connect and use a network service.

D It provides centralised encryption for network traffic and alerts the network administrator of unauthorised eavesdropping.