

- 001.** The four birthday problems are used to analyze the _____ D
 A MAC B HMAC
 C MDC D Random Oracle Model
- 002.** _____ are used to analyze the collision attack. 1. First Birthday Problem2. Second Birthday Problem3. Third Birthday Problem 4. Fourth Birthday Problem C
 A Only 1 B 1 and 2
 C 3 and 4 D Only 4
- 003.** MD5 creates digest of _____ bits B
 A 64 B 128
 C 160 D 512
- 004.** In RSA digital signature scheme, d, e and n are _____ C
 A d- Public , e-Public and n-Public B d- Public , e- Private and n-Public
 C d-Private , e-Public and n-Public D d- Public , e-Public and n- Private
- 005.** In Message Integrity, message digest needs to be kept1. Secret.2. Low.3. High.4. Down. A
 A 1 only B 1 and 3
 C 2 and 3 D 1 and 4
- 006.** The generalized version of pigeonhole principal is that if n pigeonholes are occupied by k pigeons, then at least one pigeonhole is occupied by _____ pigeons. B
 A $K+2$ B $K+1$
 C Two D $N+1$
- 007.** One way to preserve integrity of a document is through use of a B
 A Thumb Impression. B Finger Print.
 C Biometric. D X-Rays.
- 008.** Message digest needs to be_1. public.2. private.3. kept secret4. safe from change B
 A 1 and 2 B 3 and 4
 C 1 and 4 D 2 and 3
- 009.** _____ are used to analyze the preimage attack. 1. First Birthday Problem2. Second Birthday Problem3. Third Birthday Problem 4. Fourth Birthday Problem A
 A Only 1 B Only 2
 C 1 and 2 D 3 and 4
- 010.** SHA-1 creates a digest of _____ bits C
 A 64 B 128
 C 160 D 512
- 011.** A cryptographic hash function creates a _____ out of a message A
 A message digest B Document
 C Key D Value
- 012.** The diffie-Hellman key exchange is suscepble to _ attack 1. Meet- in- the middle attack C
 2. Man-in- the middle attack 3. Discrete- logarithm attack 4. Bucket bridge attack
 A 1 and 2 B 1 and 3
 C 2,3 and 4 D 1,2,3 and 4
- 013.** To ensure the integrity of a message_____ is needed. 1. Message 2. Document B
 3. Message digest 4. Fingerprint
 A 1 and 2 B 1 and 3
 C 2 and 3 D 2 and 4
- 014.** NIST has issued a standard(FIPS 198) for a nested MAC that is often referred to as A
 A HMAC B MAC
 C CMAC D CBCMAC
- 015.** A _____ can be used to ensure the integrity of a document or a message. 1. fingerprint2. A message digest 3. MAC 4. HMAC
 A 1 or 2 B 2 and 3
 C 1 and 4 D 2 or 4
- 016.** To ensure the integrity of a document_____ is needed. C
 A Document B Fingerprint

- C Both Document and fingerprint D Neither document nor fingerprint
- 017.** A digital signature needs a public key system. The signer signs with her ___ key and verifier verifies with the signers ___ key. **C**
- | | |
|-------------------|--------------------|
| A Public, Public | B Public, Private |
| C Private, Public | D Private, Private |
- 018.** In which of the following, to make the scheme stronger against the attack, the plaintext, **C** the cipher key and the ciphertext are all exclusive-ored together.
- | | |
|----------------------------|-----------------------------|
| A Davies-Meyer scheme | B Matyas-Meyer-Oseas scheme |
| C Miyaguchi-Preneel scheme | D Merkle-Damgård scheme |
- 019.** NIST has issued a standard(FIPS 198) for a nested MAC that is often referred to as 1. **D** HMAC 2. MAC 3. CMAC4. CBCMAC
- | | |
|----------|----------|
| A 1 only | B 3 only |
| C 1 or 2 | D 3 or 4 |
- 020.** The ___ is an ideal mathematical model for a hash function. **A**
- | | |
|------------------------|-------|
| A Random Oracle Model, | B MAC |
| C HMAC | D MDC |
- 021.** Which of the following are TRUE? 1. In a cryptosystems, we use the private and public keys of the sender. 2. For digital signature, we use the private and public keys of the receiver. **D**
- | | |
|-----------------------|------------------------|
| A 1- True and 2-True | B 1- False and 2-True |
| C 1- True and 2-False | D 1- False and 2-False |
- 022.** A digital signature needs ___ systems. **C**
- | | |
|------------------|-----------------|
| A Asymmetric key | B Symmetric key |
| C Public key | D Private key |
- 023.** The symmetric (shared) key in Diffie-Hellman method is $K=$ ___. **A**
- | | |
|------------------------|-------------------|
| A $K=g^{xy} \bmod p$. | B $K=g^y \bmod p$ |
| C $K=g^x \bmod p$ | D $K=g^2 \bmod p$ |
- 024.** Security of Station-to-Station protocol prevent ___ attack **B**
- | | |
|-----------------------------|----------------------------|
| A Meet-in-the-middle attack | B Man-in-the-middle attack |
| C Discrete-logarithm attack | D Birthday attack |
- 025.** PHP is integrated with a number of popular databases. like ___ 1. MySQL 2. PostgreSQL 3. Oracle 4. Sybase **D**
- | | |
|-----------|---------------|
| A 1 and 2 | B 2 and 3 |
| C 3 and 4 | D 1,2,3 and 4 |
- 026.** PHP supports ___ protocols. **B**
- | | |
|------------|------------------------|
| A TCP/IP | B POP3, MAP, and LDAP. |
| C ICMP,IPX | D ATM, POP3 |
- 027.** What are the characteristics of PHP? **A**
- | | |
|---|---|
| A Simplicity, Efficiency, Security, Flexibility and Familiarity | B Efficiency, Security, Flexibility and Familiarity |
| C Simplicity, Security, Flexibility and Familiarity | D Efficiency, Security and Flexibility |
- 028.** Which of the following are uses of PHP? 1. You add, delete, modify elements within your database through PHP. 2. Access cookies variables and set cookies. 3. It can encrypt data. 4. Using PHP, you can restrict users to access some pages of your website. **D**
- | | |
|-------------|---------------|
| A 1 and 2 | B 3 and 4 |
| C 1,2 and 4 | D 1,2,3 and 4 |
- 029.** Which of the following statements are true about PHP? 1. Server scripting language 2. Client scripting language 3. Dynamic programming 4. Interactive programming **D**
- | | |
|---------------------|----------------------|
| A 1 and 3 is True | B 2 and 4 is True |
| C 1,2 and 3 is True | D 1, 3 and 4 is True |
- 030.** PHP is used to manage _____. 1. Dynamic content 2. Databases 3. Session tracking 4. **C**

Build entire e-commerce sites.

- | | |
|------------------|-------------|
| A 4 only | B 3,4 |
| C 1,2,3 and 4 | D 1 only |

031. ___ are used to analyze the second prime attack. 1. First Birthday Problem
2. Second Birthday Problem 3. Third Birthday Problem 4. Fourth Birthday Problem

- A Only 1 B Only 2
C 3 and 4 D Only 4

032. What are the cryptographic hash function criterion properties? 1. Preimage resistance C

033. _____ is same as the Rabin scheme except it uses forward feed to protect against meet-in-middle attack.

- | | | | |
|---|--------------------------|---|---------------------------|
| A | Davies-Meyer scheme | B | Matyas-Meyer-Oseas scheme |
| C | Miyaguchi-preneel scheme | D | Merkle-Damgaard scheme |

034. Which of the following are the cryptographic hash function criterian properties? 1. Preimage resistance 2. Second preimage resistance 3. Third preimage resistance 4. Collision resistance

035. One of the promising cryptographic hash function is SHA-512. Its message digest based on _____ scheme?

- A Davies-Meyer scheme B Matyas-Meyer-Oseas scheme
C Miyaguchi-Preneel scheme D Merkle-Damgard scheme

036. What is the block size for SHA-384?

- A 128 B 512
C 1024 D 2048

037. Whirlpool is an iterated cryptographic hash function, based on

- A Davies-Meyer scheme B Matyas-Meyer-Oseas scheme
C Miyaguchi-Preneel scheme D Merkle-Damgard scheme

038- Myalgia... protein concern... D. MORRIS BANISTER, DOCTOR
is expected to be resistant to all attacks, including collision attacks.

039. In order to develop and run PHP Web pages what are the vital components need to be installed on your computer system? **A**

- A Web server, Database and PHP parser B Web server and PHP parser

C Database and PHP parser D FTP Server, Database and PHP parser

040. Which of the following scheme can be used if the datablock and the cipher key are the same size? **B**

- A Davies-Meyer scheme B Matyas-Meyer-Oseas scheme
 C Miyaguchi-Preneel scheme D Merkle-Damgard scheme

041. _____ servers include in Kerberos protocol ? 1. An authentication server 2. Ticket granting server 3. A real (data) server

042. Public key Infrastructure (PKI) is a model for ____ based on the X.509 1. Creating certificate 2. Distributing certificate 3. Revoking certificate

- A 1 only B 2 only
C 3 only D 1,2 and 3

043. PKI defines trust models 1. Hierarchical 2. Mesh 3. Web of trust

- 044.** How many pages are occupied by a message of 2^{128} bits? D
 A 2^6 pages B 2^{18} pages
 C 2^{32} pages D 2^{110} pages
- 045.** In symmetric key cryptography, if N people need to communicate with each other, ____ A keys are needed. A
 A $N(N-1)/2$ B $(2N-1)/2$
 C $N^2-1/2$ D $N(1-N)/2$
- 046.** Which of the following sentence is true? 1. Kerberos is an authentication protocol. 2. Kerberos is a key distribution center. A
 A 1-True and 2-True B 1-False and 2-True
 C 1-True and 2- False D 1- False and 2- False
- 047.** SHA-512 creates a 512-bit message digest out of a message less than B
 A 2^{124} B 2^{128}
 C 2^{256} D 2^{512}
- 048.** In the schnorr digital signature scheme, Alices public keys ____ C
 A e and n B e1,e2 and p
 C e1,e2,p and q D d only
- 049.** S/MIME is abbreviated as ____ D
 A Secure/Multimedia Internet Mailing Extensions B Secure/Multipurpose Internet Mailing Extensions
 C Secure/Multimedia Internet Mail Extensions D Secure/Multipurpose Internet Mail Extensions
- 050.** PGP use code conversion. For that it convert code in to ____ code. C
 A EBCDIC B Hexa
 C Radix-64 D BCD-8
- 051.** In the architecture of email system, the MAA client program is called as ____ program . C
 A Send B Receive
 C Pull D Push
- 052.** In the architecture of email system, the MTA client program is called as ____ program . D
 A Send B Receive
 C Pull D Push
- 053.** Like IpSec, in e-mail there is no____ C
 A Sender B Data
 C Session D Message
- 054.** In e-mail security, the sender of the message needs to include the _____ used in the message. A
 A identifiers of the algorithms B identifiers of the sender
 C identifiers of the message D identifiers of the receiver
- 055.** In e-mail security, the encryption/decryption is done using a _____ algorithm. B
 A Public-key B symmetric-key
 C Asymmetric-key D Private-key
- 056.** The key management in S/MIME is ____ 1. key management used by X.509 2. key management used by PGP C
 A 1 only B 2 only
 C a combination of 1 and 2 D neither 1 nor 2
- 057.** Pretty good privacy (PGP) is used in 1. browser security 2. email security 3. FTP security B
 A 1 only B 2 only
 C 3 only D 1,2 and 3
- 058.** The entire operations of PGP depends on ____ 1. Introducer trust 2. Certificate trust 3. D
 A 1 only B 2 only
 C 3 only D 1,2 and 3

Legitimacy of the public key

- | | |
|----------|-------------|
| A 1 only | B 2 only |
| C 3 only | D 1,2 and 3 |

059. Protocol that uses X.509 certificate depends on the _____. 1. Hierarchical structure of the trust 2. Mesh structure of the trust 3. Web of trust

- | | |
|-------------|-----------|
| A 1 only | B 1 and 2 |
| C 1,2 and 3 | D 3 only |

060. In _____, there is a single path from the fully trusted authority to any certificate. 1. PGP 2. X.509 3. S/MIME

- | | |
|-----------|-----------|
| A 1 only | B 2 only |
| C 1 and 3 | D 2 and 3 |

061. PGP makes a web of trust between_____

- | | |
|-----------------------|-----------------------|
| A Sender and receiver | B Alice and Bob |
| C A group of people | D Receiver and sender |

062. Weighted trusts are used in which of the following? 1. Introducer trust 2. Certificate trust 3. Legitimacy of the public key

- | | |
|----------|-------------|
| A 1 only | B 2 only |
| C 3 only | D 1,2 and 3 |

063. In SSL, what is used for authenticating a message?

- | | |
|-------------------------------------|-------------------------------------|
| A MAC (Message Access Code) | B MAC (Message Authentication Code) |
| C MAC (Machine Authentication Code) | D MAC (Machine Access Code) |

064. SSL divides the data into blocks of _____ bytes or less.

- | | |
|------------|------------|
| A 2^{12} | B 2^{14} |
| C 2^{16} | D 2^{24} |

065. Pretty good privacy (PGP) security system uses 1. Public key cryptosystem 2. Private key cryptosystem

- | | |
|----------------|-------------------|
| A 1 only | B 2 only |
| C Both 1 and 2 | D Neither 1 nor 2 |

066. The cryptography algorithms used in S/MIME are _____.

- | | |
|--------------|--------|
| A IDEA. | B RC4. |
| C RSA,DES-3. | D RC5. |

067. PGP can be used for _____. 1. email 2. file storage application

- | | |
|----------------|-------------------|
| A 1 only | B 2 only |
| C Both 1 and 2 | D Neither 1 nor 2 |

068. In PGP, a hash code of a message is created using _____. 1. SHA-12. IDEA3. 3DES

- | | |
|-----------|-------------|
| A 1 only | B 2 and 3 |
| C 1 and 3 | D 1,2 and 3 |

069. The use of S/MIME _____. 1. commercial 2. organization

- | | |
|-----------|-------------------|
| A 1 only | B 2 only |
| C 1 and 2 | D Neither 1 nor 2 |

070. PGP provides e-mail with 1. Authentication 2. Integrity 3. Privacy

- | | |
|----------------|-------------|
| A 1 only | B 2 only |
| C 2 and 3 only | D 1,2 and 3 |

071. Which of the following statements are true? 1. In PGP, there is no need of CAs. 2. In PGP, there is no hierarchy of trust.

- | | |
|-----------------------|------------------------|
| A 1- True and 2-True | B 1- False and 2-True |
| C 1- True and 2-False | D 1- False and 2-False |

072. In e-mail security, the secret key to decrypt the message is encrypted with the _____ key of the _____ and is sent with the message.

- | | |
|--------------------|---------------------|
| A Public, Sender | B Private, Sender |
| C Public, Receiver | D Private, Receiver |

073. Which one of the following is not a higher layer SSL protocol?

- | | |
|------------------|-------------------------------|
| A Alert Protocol | B Handshake Protocol |
| C Alarm Protocol | D Change Cipher Spec Protocol |

- 074.** The full form of SSL is _____ B
 A Serial Session Layer B Secure Socket Layer
 C Session Secure Layer D Series Socket Layer
- 075.** To exchange authenticated and confidential messages, the client need ___ and the server need ___ cryptographic secrets A
 A 6 and 6 B 4 and 2
 C 4 and 6 D 2 and 4
- 076.** Number of phases in the handshaking protocol? C
 A 2 B 3
 C 4 D 5
- 077.** Which protocol consists of only 1 bit? D
 A Alert Protocol B Handshake Protocol
 C Upper-Layer Protocol D Change Cipher Spec Protocol
- 078.** The client_key_exchange message uses a pre master key of size A
 A 48 bytes B 56 bytes
 C 64 bytes D 32 bytes
- 079.** What is the size of the RSA signature hash after the MD5 and SHA-1 processing? C
 A 42 bytes B 32 bytes
 C 36 bytes D 48 bytes
- 080.** After the encryption stage in SSL, the maximum length of each fragment is B
 A $2^{14}+1028$ B $2^{14}+2048$
 C $2^{16}+1028$ D $2^{16}+2048$
- 081.** What is the key size allowed in PGP? C
 A 1024-1056 B 1024-4056
 C 1024-4096 D 1024-2048
- 082.** SSL primarily focuses on _____ A
 A integrity and authenticity B integrity and non-repudiation
 C authenticity and privacy D confidentiality and integrity
- 083.** Which is the key exchange algorithm used in CipherSuite parameter? 1. RSA 2. Fixed Diffie-Hellman 3. Ephemeral Diffie-Hellman D
 A 1 only B 2 only
 C 3 only D 1,2 and 3
- 084.** Which of the message we have in PGP? 1. Encrypted message 2. Signed message 3. Decrypted messages 4. Certificate message C
 A 1 and 2 B 1, 2 and 3
 C 1,2 and 4 D 1,2,3 and 4
- 085.** In the alert protocol the first byte takes the value 1 or 2 which corresponds to _____ and _____ respectively. D
 A Select, Alarm B Alert, Alarm
 C Warning, Alarm D Warning, Fatal
- 086.** Which of the following are possible sizes of MACs? 1. 12 Bytes 2. 16 Bytes 3. 20 Bytes 4. 24 Bytes C
 A 1 and 3 B 2 only
 C 2 and 3 D 2, 3 and 4
- 087.** Which protocol is used for the purpose of copying the pending state into the current state? D
 A Alert Protocol B Handshake Protocol
 C Upper-Layer Protocol D Change Cipher Spec Protocol
- 088.** Which protocol is used to convey SSL related alerts to the peer entity? A
 A Alert Protocol B Handshake Protocol
 C Upper-Layer Protocol D Change Cipher Spec Protocol
- 089.** In _____, there can be multiple paths from the fully or partially trusted authority to any certificate. 1. PGP 2. X.509 3. S/MIME A
 A 1 only B 2 only

- | | | | |
|-------------|---|----|---|
| C | 1 and 3 | D | 2 and 3 |
| 090. | None, partial and full trust levels are used in which of the following? 1. Introducer trust
2. Certificate trust 3. Legitimacy of the public key | A | 1 only |
| | | B | 1 and 2 |
| | | C | 2 and 3 |
| | | D | 1,2 and 3 |
| 091. | In the SSL record protocol operation pad_1 is | A | is the byte 0x36 repeated 40 times for MD5 |
| | | B | is the byte 0x5C repeated 40 times for MD5 |
| | | C | is the byte 0x5C repeated 48 times for SHA-1 |
| | | D | is the byte 0x36 repeated 48 times for MD5 |
| 092. | In the SSL record protocol operation pad_2 is | A | is the byte 0x36 repeated 40 times for MD5 |
| | | B | is the byte 0x5C repeated 48 times for MD5 |
| | | C | is the byte 0x5C repeated 48 times for SHA-1 |
| | | D | is the byte 0x36 repeated 48 times for MD5 |
| 093. | The DSS signature uses which hash algorithm? | 1. | MD5 |
| | | 2. | SHA-2 |
| | | 3. | SHA-1 |
| | | A | 1 only |
| | | B | 2 and 3 |
| | | C | 3 only |
| | | D | 1,2 and 3 |
| 094. | In the Handshake protocol action, which is the last step of the Phase 2 : Server Authentication and Key Exchange? | A | serverHelloDone |
| | | B | ClientHello |
| | | C | certificateVerify |
| | | D | HelloRequest |
| 095. | Which protocol in SSL is used to report error and abnormal conditions? | A | Alert Protocol |
| | | B | Handshake Protocol |
| | | C | Upper-Layer Protocol |
| | | D | Change Cipher Spec Protocol |
| 096. | Which of the following statements are True? | 1. | Record protocol use HMAC for signing the message. |
| | | 2. | SSL and TLS use MAC |
| | | A | 1- True and 2-True |
| | | B | 1- False and 2-True |
| | | C | 1- True and 2- False |
| | | D | 1- False and 2- False |
| 097. | The certificate message is required for any agreed-on key exchange method except | A | Ephemeral Diffie-Hellman |
| | | B | Anonymous Diffie-Hellman |
| | | C | Fixed Diffie-Hellman |
| | | D | RSA |
| 098. | In ____ mode , IPsec layer comes between transport layer and network layer | A | Tunnel mode |
| | | B | Transport mode |
| | | C | Communication mode |
| | | D | User mode |
| 099. | IPSec support__ | 1. | IPv4 |
| | | 2. | IPv6 |
| | | A | 1 only |
| | | B | 2 only |
| | | C | 1 and 2 |
| | | D | Neither 1 nor 2 |
| 100. | Which of the following is True about IPSec? | 1. | It can enhance security for emails |
| | | 2. | It can not enhance security for client/server program which use HTTP. |
| | | A | 1- True and 2 True |
| | | B | 1- False and 2 True |
| | | C | 1- True and 2 False |
| | | D | 1- False and 2 False |
| 101. | IPsec is designed to provide security at the ____ layer | A | Application |
| | | B | Transport |
| | | C | Network |
| | | D | Datalink |
| 102. | In tunnel mode IPsec protects the | 1. | Entire IP packet |
| | | 2. | only IP header |
| | | 3. | Only IP payload |
| | | A | 1 only |
| | | B | 2 and 3 |
| | | C | 1 and 3 |
| | | D | 1,2 and 3 |
| 103. | Which component is included in IP security? | A | Authentication Header (AH) |
| | | B | Encapsulating Security Payload (ESP) |
| | | C | Internet key Exchange (IKE) |
| | | D | AH, ESP and IKE |

- 104.** IPSEC in Transport mode protect____ 1. IP header 2. IP payload 3. Information coming from transport layer
A 1 only B 2 only
C 3 only D 1,2 and 3

105. IPSce indirectly provide access control using a ____
A SPD B SAD
C ESP D IKE

106. Which of the following are called third generation firewalls?
A packet firewalls B circuit level firewalls
C application layer firewalls D dynamic packet filter firewalls

107. Expand ESP?
A Encapsulating Service Payload B Encapsulating Security Payload
C Encapsulating Security Protocol D Exchange Security Payload

108. Which of the following service not provided by AH
A Access control B Message integrity
C Confidentiality D Replay attack protection

109. IPSec require a Security Association between ____
A Two hosts B Two routers
C Two gateways D One host and one router

110. The Outbound SPD, the out put cases are ____ 1. Drop 2. Discard 3. Bypass 4. Apply
A 1 and 2 B 1, 3 and 4
C 2 and 3 D 2,3 and 4

111. To protect against ____ attack, IKE uses cookies.
A Clogging attack B Replay attack
C Man- in the middle attack D Bucket bridge attack

112. Possible threat to any information cannot be _____
A Reduced B Protected
C Ignored D Transferred

113. Lack of access control policy is a _____
A Bug B threat
C attack D vulnerability

114. Intruders are classified as____ 1. Masquerader 2. Misfeasor 3. Clandestine user
A 1 and 2 B 2 and 3
C 1 and 3 D 1,2 and 3

115. In CSPARC and MIPS processors, the stack grows____
A From lower memory address to B From higher memory address to
higher memory address. lower memory address.
C With in few set of memory address. D In a specific memory locations.

116. To protect against ____ attack, IKE uses nonces.
A Clogging attack B Replay attack
C Man- in the middle attack D Bucket bridge attack

117. Expand SAD?
A Service Association Database B Service Assistant Database
C Security Access Database D Security Association Database

118. Expand IDS?
A Information detection system B Intrusion detection system
C Intrusion detection software D Intrusion deleting software

119. ____ will detect and warn about the security violation.
A Information detection system B Intrusion detection system
C Intrusion detection software D Intrusion deleting software

120. ____ may not detect the security violation byt block the attack.
A Gateway B Switch
C Firewall D router

121. Which of the following is True about IPSEC? 1. It provide security for those client/server A

programs that do not use security service provided at transport layer. 2. It enhance security for those client/server programs that use security service provided at transport layer.

- A 1- True and 2 True B 1- False and 2 True
C 1- True and 2 False D 1- False and 2 False
122. When integrity is lacking in a security system, _____ occurs. C
A database hacking B data deletion
C data tampering D data leaking
123. To protect against ____ attack, IKE each party need a secret. C
A Clogging attack B Replay attack
C Man-in-the-middle attack D Bucket bridge attack
124. The Inbound SPD, the out put cases are __ 1. Drop 2. Discard 3. Bypass 4. Apply C
A 1 and 3 B 2 and 3
C 2,3 and 4 D 1,3 and 4
125. In ____ mode, the flow is from Network layer to IPsec layer then back to network layer. A
A Tunnel mode B Transport mode
C Communication mode D User mode
126. Which of the following will have payload and trigger are the two parts of it A
A Logic bombs B Trojans
C Spywares D adwares.
127. ____ can not run independently C
A Malicious programs B Warms programs
C Virus programs D Spyware
128. The intel ____ and ____ instructions are provided to perform the prolog and epilog procedures efficiently D
A INPUT , LEAVE B ENTER , OUTPUT
C INPUT , OUTPUT D ENTER , LEAVE
129. ____ cannot perform security checks on higher level protocols B
A Packet firewalls B Circuit level firewalls
C Application layer firewalls D Dynamic packet filter firewalls
130. The 8-bit next header field of AH define the ____ type of payload carried by the IP datagram. 1. TCP 2. UDP 3. ICMP 4. OSPF D
A 1 and 2 B 3 and 4
C 1,2 and 3 D 1,2, 3 and 4
131. ____ run independently B
A Malicious programs B Warms programs
C Virus programs D Spyware
132. In intel machines the stack pointer is being denoted as ____ and the frame pointer is denoted as ____ C
A SP and EBP B ESP and Fp
C ESP and EBP D SP and Fp
133. The 8-bit next header field of ESP define the ____ type of payload carried by the IP datagram. 1. TCP 2. UDP 3. ICMP 4. OSPF A
A 1,2 only B 3,4 only
C 1,3 only D 2,4 only
134. ____ are malicious programs. 1. Logic bombs 2. Trojans 3. Spywares 4. Adwares D
A 1,2 only B 2,3 only
C 1,2 and 3 D 1,2, 3 and 4
135. A ____ is single point defense between two networks A
A Firewall B Gateway
C Router D Switch
136. Drive by download is a phenomenon, comes in ____ C
A Logic bombs B Trojans
C Spywares D adwares.

