Question 1:

'Which of the following styles of fuzzer is more likely to explore paths covering every line of code in the following program?', A. 'Generational', B. 'Blackbox', C. 'Whitebox', D. 'Mutation-based'

===========================

Answer Option 1:

Final Answer: C

***************************

Answer Option 2:

Final Answer: C

***************************

Answer Option 3:

Final Answer: C

***************************

Answer Option 4:

Final Answer: C

***************************

Answer Option 5:

Final Answer: C

***************************

Answer Option 6:

Final Answer: C

***************************

Answer Option 7:

Final Answer: C

***************************

Answer Option 8:

Final Answer: C

***************************

Answer Option 9:

Final Answer: C

***************************

Question 2:

'Assume that a TLS connection has been established successfully between a client and a server. Establishing the session included checking the server certificate and executing a DiffieHelmann exchange, but the client did not provide a client certificate. Further, assume that the client and server are honest, that the client and server don’t leak their keys, and that the cryptography is good. Which of the following attacks does TLS protect against?

1. An attacker replaying bytes that a client sent earlier.

2. An attacker impersonating the server.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

==========================

Answer Option 1:

Final Answer: A

***************************

Answer Option 2:

Final Answer: A

***************************

Answer Option 3:

Final Answer: A

***************************

Answer Option 4:

Final Answer: A

***************************

Answer Option 5:

Final Answer: A

***************************

Answer Option 6:

Final Answer: A

***************************

Answer Option 7:

Final Answer: A

***************************

Answer Option 8:

Final Answer: A

***************************

Answer Option 9:

Final Answer: A

***************************

Question 3:

'MIT's Kerberos KDC server has a maximum ticket lifetime of 24 hours (for most user principals). What ensures that an expired Kerberos ticket can no longer be used?', A. 'The Kerberos server (KDC) refuses to establish new connections between clients and servers for expired tickets.', B. 'When a client connects to a server, the server sets a 24-hour timer to terminate the connection, which ensures a client cannot remain connected past the ticket's maximum lifetime.', C. 'When a client connects to a server, the server compares the ticket's expiration time to the server's current clock, and refuses to authenticate the user if the ticket expiration time is in the past.', D. 'When a client connects to a server, the server sends a query to the KDC to check if the ticket is still valid with respect to the KDC's clock, and refuses to authenticate the user if the KDC reports that the ticket is expired.'

=========================

Answer Option 1:

Final Answer: C

***************************

Answer Option 2:

Final Answer: C

***************************

Answer Option 3:

Final Answer: C

***************************

Answer Option 4:

Final Answer: C

***************************

Answer Option 5:

Final Answer: C

***************************

Answer Option 6:

Final Answer: C

***************************

Answer Option 7:

Final Answer: C

***************************

Answer Option 8:

Final Answer: C

***************************

Answer Option 9:

Final Answer: C

***************************

Question 4:

'In Message Condentiality, the transmitted message must make sense to only intended', A. 'Receiver', B. 'Sender', C. 'Modulor', D. 'Translator'

==========================

Answer Option 1:

Final Answer: A

***************************

Answer Option 2:

Final Answer: A

***************************

Answer Option 3:

Final Answer: A

***************************

Answer Option 4:

Final Answer: A

***************************

Answer Option 5:

Final Answer: A

***************************

Answer Option 6:

Final Answer: A

***************************

Answer Option 7:

Final Answer: A

***************************

Answer Option 8:

Final Answer: A

***************************

Answer Option 9:

Final Answer: A

***************************

Question 5:

'Which of the following is a remote Trojan?', A. 'Troya', B. 'DaCryptic', C. 'BankerA', D. 'Game-Troj'

==========================

Answer Option 1:

Final Answer: B

***************************

Answer Option 2:

Final Answer: B

***************************

Answer Option 3:

Final Answer: B

***************************

Answer Option 4:

Final Answer: B

***************************

Answer Option 5:

Final Answer: B

***************************

Answer Option 6:

Final Answer: B

***************************

Answer Option 7:

Final Answer: B

***************************

Answer Option 8:

Final Answer: B

***************************

Answer Option 9:

Final Answer: B

***************************

Question 6:

'______________ is a widespread app’s coding mistake made by developers which could be exploited by an attacker for gaining access or malfunctioning your system.', A. 'Memory leakage', B. 'Buffer-overrun', C. 'Less processing power', D. 'Inefficient programming'

==========================

Answer Option 1:

Final Answer: B

***************************

Answer Option 2:

Final Answer: B

***************************

Answer Option 3:

Final Answer: B

***************************

Answer Option 4:

Final Answer: B

***************************

Answer Option 5:

Final Answer: B

***************************

Answer Option 6:

Final Answer: B

***************************

Answer Option 7:

Final Answer: B

***************************

Answer Option 8:

Final Answer: B

***************************

Answer Option 9:

Final Answer: B

***************************

Question 7:

'Consider the paper Native Client: A Sandbox for Portable, Untrusted x86 Native Code by Yee et al. Ben Bitdiddle notes that NaCl uses Intel x86 segmentation to ensure that the sandboxed module does not read or write memory outside its own data area, and does not execute instructions outside its own code. Ben thinks that with these restrictions alone, executing the sandboxed module must be safe; that is, he thinks validation is not needed. Ben is wrong. Circle the types of x86 machine instructions that the validator always forbids in sandboxed code. Please ignore trampoline and springboard code.', A. 'all instructions that modify segment state', B. 'all loads or stores to addresses that are not 0 mod 32', C. 'all indirect loads or stores (via an address in a register or variable)', D. 'all indirect jumps (via an address in a register or variable)'

==========================

Answer Option 1:

Final Answer: A

***************************

Answer Option 2:

Final Answer: A

***************************

Answer Option 3:

Final Answer: A

***************************

Answer Option 4:

Final Answer: A

***************************

Answer Option 5:

Final Answer: A

***************************

Answer Option 6:

Final Answer: A

***************************

Answer Option 7:

Final Answer: A

***************************

Answer Option 8:

Final Answer: A

***************************

Answer Option 9:

Final Answer: A

***************************

Question 8:

'____________ is also a part of darknet that is employed for transferring files anonymously.', A. 'Freenet', B. 'ARPANET', C. 'Stuxnet', D. 'Internet'

==========================

Answer Option 1:

Final Answer: A

***************************

Answer Option 2:

Final Answer: A

***************************

Answer Option 3:

Final Answer: A

***************************

Answer Option 4:

Final Answer: A

***************************

Answer Option 5:

Final Answer: A

***************************

Answer Option 6:

Final Answer: A

***************************

Answer Option 7:

Final Answer: A

***************************

Answer Option 8:

Final Answer: A

***************************

Answer Option 9:

Final Answer: A

***************************

Question 9:

'Why apps developed in languages like C, C++ is prone to Buffer-overflow?', A. 'No string boundary checks in predefined functions', B. 'No storage check in the external memory', C. 'No processing power check', D. 'No database check'

==========================

Answer Option 1:

Final Answer: A

**************************

Answer Option 2:

Final Answer: A

**************************

Answer Option 3:

Final Answer: A

**************************

Answer Option 4:

Final Answer: A

**************************

Answer Option 5:

Final Answer: A

**************************

Answer Option 6:

Final Answer: A

**************************

Answer Option 7:

Final Answer: A

**************************

Answer Option 8:

Final Answer: A

**************************

Answer Option 9:

Final Answer: A

**************************

Question 10:

'Man in the middle attack can endanger the security of Diffie Hellman method if two parties are not', A. 'Joined', B. 'Authenticated', C. 'Submitted', D. 'Shared'

===========================

Answer Option 1:

Final Answer: B

***************************

Answer Option 2:

Final Answer: B

***************************

Answer Option 3:

Final Answer: B

***************************

Answer Option 4:

Final Answer: B

***************************

Answer Option 5:

Final Answer: B

***************************

Answer Option 6:

Final Answer: B

***************************

Answer Option 7:

Final Answer: B

***************************

Answer Option 8:

Final Answer: B

***************************

Answer Option 9:

Final Answer: B

***************************

Question 11:

'An integer overflow occurs when', A. 'an integer expression's result "wraps around"; instead of creating a very large number, a very small (or negative) number ends up getting created', B. 'an integer is used as if it was a pointer', C. 'an integer is used to access a buffer outside of the buffer's bounds', D. 'there is no more space to hold integers in the program'

==========================

Answer Option 1:

Final Answer: A

***************************

Answer Option 2:

Final Answer: A

***************************

Answer Option 3:

Final Answer: A

***************************

Answer Option 4:

Final Answer: A

***************************

Answer Option 5:

Final Answer: A

***************************

Answer Option 6:

Final Answer: A

***************************

Answer Option 7:

Final Answer: A

***************************

Answer Option 8:

Final Answer: A

***************************

Answer Option 9:

Final Answer: A

***************************

Question 12:

'Let HH be a Merkle-Damgard hash function is H:X^{\leq L} \to TH:X^≤L →T. Construct a MAC from this HH as follows: \ \ S(k,m) = H(k \| m) S(k,m)=H(k■m). This mac is insecure because:', A. 'Given H(k \| m)H(k■m) anyone can compute H(w \| k \| m \| \text{PB})H(w■k■m■PB) for any ww', B. 'Given H(k \| m)H(k■m) anyone can compute H(k \| m \| w)H(k■m■w) for any ww', C. 'Given H(k \| m)H(k■m) anyone can compute H(k \| m \| \text{PB} \| w)H(k■m■PB■w) for any ww', D. 'Anyone can compute H( k \| m )H(k■m) for any mm'

==========================

Answer Option 1:

Final Answer: B

***************************

Answer Option 2:

Final Answer: B

***************************

Answer Option 3:

Final Answer: B

***************************

Answer Option 4:

Final Answer: B

***************************

Answer Option 5:

Final Answer: B

***************************

Answer Option 6:

Final Answer: B

***************************

Answer Option 7:

Final Answer: B

***************************

Answer Option 8:

Final Answer: B

***************************

Answer Option 9:

Final Answer: B

***************************

Question 13:

'Suppose that Alice and Bob sent confidential text messages to one another last month through an encrypted messaging system. Alice and Bob are worried that an adversary might compromise one of their computers today, while they are taking the 6.858 final exam, and would then be able to decrypt those messages. Which of the following security properties can address Alice and Bob's concern?', A. 'Authentication.', B. 'Deniability.', C. 'Forward secrecy', D. 'Backward secrecy.'

=========================

Answer Option 1:

Final Answer: C

***************************

Answer Option 2:

Final Answer: C

***************************

Answer Option 3:

Final Answer: C

***************************

Answer Option 4:

Final Answer: C

***************************

Answer Option 5:

Final Answer: C

***************************

Answer Option 6:

Final Answer: C

***************************

Answer Option 7:

Final Answer: C

***************************

Answer Option 8:

Final Answer: C

***************************

Answer Option 9:

Final Answer: C

***************************

Question 14:

'The AH Protocol provides source authentication and data integrity, but not', A. 'Integrity', B. 'Privacy', C. 'Nonrepudiation', D. 'Both A & C'

==========================

Answer Option 1:

Final Answer: B

**************************

Answer Option 2:

Final Answer: B

**************************

Answer Option 3:

Final Answer: B

**************************

Answer Option 4:

Final Answer: B

**************************

Answer Option 5:

Final Answer: B

**************************

Answer Option 6:

Final Answer: B

**************************

Answer Option 7:

Final Answer: B

**************************

Answer Option 8:

Final Answer: B

**************************

Answer Option 9:

Final Answer: B

**************************

Question 15:

'Which of the following is not a security exploit?', A. 'Eavesdropping', B. 'Cross-site scripting', C. 'Authentication', D. 'SQL Injection'

==========================

Answer Option 1:

Final Answer: C

***************************

Answer Option 2:

Final Answer: C

***************************

Answer Option 3:

Final Answer: C

***************************

Answer Option 4:

Final Answer: C

***************************

Answer Option 5:

Final Answer: C

***************************

Answer Option 6:

Final Answer: C

***************************

Answer Option 7:

Final Answer: C

***************************

Answer Option 8:

Final Answer: C

***************************

Answer Option 9:

Final Answer: C

***************************

Question 16:

'_______________ is the central node of 802.11 wireless operations.', A. 'WPA', B. 'Access Point', C. 'WAP', D. 'Access Port'

==========================

Answer Option 1:

Final Answer: B

***************************

Answer Option 2:

Final Answer: B

***************************

Answer Option 3:

Final Answer: B

***************************

Answer Option 4:

Final Answer: B

***************************

Answer Option 5:

Final Answer: B

***************************

Answer Option 6:

Final Answer: B

***************************

Answer Option 7:

Final Answer: B

***************************

Answer Option 8:

Final Answer: B

***************************

Answer Option 9:

Final Answer: B

***************************

Question 17:

'In MD-5 the length of the message digest is', A. '160', B. '128', C. '64', D. '54'

=========================

Answer Option 1:

Final Answer: B

**************************

Answer Option 2:

Final Answer: B

**************************

Answer Option 3:

Final Answer: B

**************************

Answer Option 4:

Final Answer: B

**************************

Answer Option 5:

Final Answer: B

**************************

Answer Option 6:

Final Answer: B

**************************

Answer Option 7:

Final Answer: B

**************************

Answer Option 8:

Final Answer: B

**************************

Answer Option 9:

Final Answer: B

**************************

Question 18:

'What is Nmap?', A. 'It is a scanner which works by injecting packets to a range of addresses, and inferring what hosts and services might be at those addresses, based on the responses', B. 'It is a network fuzz testing tool', C. 'It is a map of the Internet', D. 'It is a suite of tools for scripting attacks: probe, construct, encode, inject, wait for response'

==========================

Answer Option 1:

Final Answer: A

**************************

Answer Option 2:

Final Answer: A

**************************

Answer Option 3:

Final Answer: A

**************************

Answer Option 4:

Final Answer: A

**************************

Answer Option 5:

Final Answer: A

**************************

Answer Option 6:

Final Answer: A

**************************

Answer Option 7:

Final Answer: A

**************************

Answer Option 8:

Final Answer: A

**************************

Answer Option 9:

Final Answer: A

**************************

Question 19:

'How do you prevent SQL injection?', A. 'Escape queries', B. 'Interrupt requests', C. 'Merge tables', D. 'All of the above'

==========================

Answer Option 1:

Final Answer: A

***************************

Answer Option 2:

Final Answer: A

***************************

Answer Option 3:

Final Answer: A

***************************

Answer Option 4:

Final Answer: A

***************************

Answer Option 5:

Final Answer: A

***************************

Answer Option 6:

Final Answer: A

***************************

Answer Option 7:

Final Answer: A

***************************

Answer Option 8:

Final Answer: A

***************************

Answer Option 9:

Final Answer: A

***************************

Question 20:

'What does it mean to "be stealthy" during a penetration test?', A. 'Performing the tests from an undisclosed location', B. 'Using encryption during tests to make the source of attacks impossible to determine', C. 'Performing penetration testing without the target organization knowing', D. 'Taking care to avoid activities during a penetration test that might attract attention, e.g., by operators or IDS services'

==========================

Answer Option 1:

Final Answer: D

***************************

Answer Option 2:

Final Answer: D

***************************

Answer Option 3:

Final Answer: D

***************************

Answer Option 4:

Final Answer: D

***************************

Answer Option 5:

Final Answer: D

***************************

Answer Option 6:

Final Answer: D

***************************

Answer Option 7:

Final Answer: D

***************************

Answer Option 8:

Final Answer: D

***************************

Answer Option 9:

Final Answer: D

***************************

Question 21:

'Which of the following is not a transport layer vulnerability?', A. 'Mishandling of undefined, poorly defined variables', B. 'The Vulnerability that allows “fingerprinting” & other enumeration of host information', C. 'Overloading of transport-layer mechanisms', D. 'Unauthorized network access'

==========================

Answer Option 1:

Final Answer: A

***************************

Answer Option 2:

Final Answer: A

***************************

Answer Option 3:

Final Answer: A

***************************

Answer Option 4:

Final Answer: D

***************************

Answer Option 5:

Final Answer: D

***************************

Answer Option 6:

Final Answer: D

***************************

Answer Option 7:

Final Answer: D

***************************

Answer Option 8:

Final Answer: A

***************************

Answer Option 9:

Final Answer: D

***************************

Question 22:

'In Brumley and Boneh's paper on side-channel attacks, why does blinding prevent the timing attack from working?', A. 'Blinding prevents the server from using the CRT optimization, which is essential to the timing attack.', B. 'Blinding changes the p and q primes that are used, so an adversary cannot learn the server's true p and q values.', C. 'Blinding randomizes the ciphertext being decrypted, thus obscuring the correlation between an adversary’s input and the timing differences.', D. 'Blinding adds a random amount of time to the decryption due to the multiplication and division by the blinding random value r, which obscures the timing differences used in the attack.'

==========================

Answer Option 1:

Final Answer: C

***************************

Answer Option 2:

Final Answer: C

***************************

Answer Option 3:

Final Answer: C

***************************

Answer Option 4:

Final Answer: C

***************************

Answer Option 5:

Final Answer: C

***************************

Answer Option 6:

Final Answer: C

***************************

Answer Option 7:

Final Answer: C

***************************

Answer Option 8:

Final Answer: C

***************************

Answer Option 9:

Final Answer: C

***************************

Question 23:

'The openSSL implementation described in “Remote Timing Attacks are Practical” (by Brumley and Boneh) uses the following performance optimizations: Chinese Remainder (CR), Montgomery Representation (MR), Karatsuba Multiplication (KM), and Repeated squaring and Sliding windows (RS). Which of the following options would close the timing channel attack described in the paper if you turned the listed optimizations off?

1. RS and KM

2. RS and MR', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=========================

Answer Option 1:

Final Answer: C

***************************

Answer Option 2:

Final Answer: D

***************************

Answer Option 3:

Final Answer: D

***************************

Answer Option 4:

Final Answer: B

***************************

Answer Option 5:

Final Answer: B

***************************

Answer Option 6:

Final Answer: B

***************************

Answer Option 7:

Final Answer: C

***************************

Answer Option 8:

Final Answer: C

***************************

Answer Option 9:

Final Answer: A

***************************

Question 24:

'Public key encryption is advantageous over Symmetric key Cryptography because of', A. 'Speed', B. 'Space', C. 'Key exchange', D. 'Key length'

==========================

Answer Option 1:

Final Answer: C

***************************

Answer Option 2:

Final Answer: C

***************************

Answer Option 3:

Final Answer: C

***************************

Answer Option 4:

Final Answer: C

***************************

Answer Option 5:

Final Answer: C

***************************

Answer Option 6:

Final Answer: C

***************************

Answer Option 7:

Final Answer: C

***************************

Answer Option 8:

Final Answer: C

***************************

Answer Option 9:

Final Answer: C

***************************

Question 25:

'The __________ was a huge marketplace of Dark Web specifically famous for selling of illegal drugs & narcotics as well as you can find a wide range of other goods for sale.', A. 'Silk Road', B. 'Cotton Road', C. 'Dark Road', D. 'Drug Road'

==========================

Answer Option 1:

Final Answer: A

***************************

Answer Option 2:

Final Answer: A

***************************

Answer Option 3:

Final Answer: A

***************************

Answer Option 4:

Final Answer: A

***************************

Answer Option 5:

Final Answer: A

***************************

Answer Option 6:

Final Answer: A

***************************

Answer Option 7:

Final Answer: A

***************************

Answer Option 8:

Final Answer: A

***************************

Answer Option 9:

Final Answer: A

***************************

Question 26:

'The ______________ is categorized as an unknown segment of the Deep Web which has been purposely kept hidden & is inaccessible using standard web browsers.', A. 'Haunted web', B. 'World Wide Web', C. 'Dark web', D. 'Surface web'

==========================

Answer Option 1:

Final Answer: C

***************************

Answer Option 2:

Final Answer: C

***************************

Answer Option 3:

Final Answer: C

***************************

Answer Option 4:

Final Answer: C

***************************

Answer Option 5:

Final Answer: C

***************************

Answer Option 6:

Final Answer: C

***************************

Answer Option 7:

Final Answer: C

***************************

Answer Option 8:

Final Answer: C

***************************

Answer Option 9:

Final Answer: C

***************************

Question 27:

'What does EXE do when the STP solver times out on a constraint query for a particular path?', A. 'Assume that the query is satisfiable and continue executing the path.', B. 'Assume that the query is not satisfiable and stop executing the path', C. 'Restart STP and retry the query, up to a limited number of retries.', D. 'Remove a subset of the constraints and retry the query.'

==========================

Answer Option 1:

Final Answer: A

**************************

Answer Option 2:

Final Answer: A

**************************

Answer Option 3:

Final Answer: A

**************************

Answer Option 4:

Final Answer: A

**************************

Answer Option 5:

Final Answer: A

**************************

Answer Option 6:

Final Answer: A

**************************

Answer Option 7:

Final Answer: A

**************************

Answer Option 8:

Final Answer: B

**************************

Answer Option 9:

Final Answer: A

**************************

Question 28:

'To verify a digital signature we need the', A. 'Sender's Private key', B. 'Sender's Public key', C. 'Receiver's Private key', D. 'Receiver's Public key'

==========================

Answer Option 1:

Final Answer: B

***************************

Answer Option 2:

Final Answer: B

***************************

Answer Option 3:

Final Answer: B

***************************

Answer Option 4:

Final Answer: B

***************************

Answer Option 5:

Final Answer: B

***************************

Answer Option 6:

Final Answer: B

***************************

Answer Option 7:

Final Answer: B

***************************

Answer Option 8:

Final Answer: B

***************************

Answer Option 9:

Final Answer: B

***************************

Question 29:

'Suppose you want to use fuzzing on a program to try to find memory errors; which of the following statements is true?', A. 'You should not use a grammar-based fuzzer, because its adherence to the grammar means it will not find memory errors', B. 'Compiling the program with address sanitizer (ASAN) will make errors harder to reproduce', C. 'Compiling the program with address sanitizer (ASAN) will make the source of a memory error easier to find', D. 'Fuzzing doesn't find memory errors, it finds crashes and hangs'

==========================

Answer Option 1:

Final Answer: C

***************************

Answer Option 2:

Final Answer: C

***************************

Answer Option 3:

Final Answer: C

***************************

Answer Option 4:

Final Answer: C

***************************

Answer Option 5:

Final Answer: C

***************************

Answer Option 6:

Final Answer: C

***************************

Answer Option 7:

Final Answer: C

***************************

Answer Option 8:

Final Answer: C

***************************

Answer Option 9:

Final Answer: C

***************************

Question 30:

'Based on the paper “SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificates trust model enhancements”, which of the following statements are false?', A. 'Valid DV certificates provide more confidence to a user that she is connecting to the intended party than valid EV certificates.', B. 'OCSP stapling allows a server to prove to a browser that its certificate hasn't been revoked.', C. 'DANE makes it difficult for an adversary to launch a SSL stripping attack.', D. 'Server key-pinning makes it harder for an adversary to convince a CA to mint a certificate for a site and launch an MITM attack on that site.'

==========================

Answer Option 1:

Final Answer: A

***************************

Answer Option 2:

Final Answer: A

***************************

Answer Option 3:

Final Answer: A

***************************

Answer Option 4:

Final Answer: A

***************************

Answer Option 5:

Final Answer: A

***************************

Answer Option 6:

Final Answer: A

***************************

Answer Option 7:

Final Answer: A

***************************

Answer Option 8:

Final Answer: A

***************************

Answer Option 9:

Final Answer: A

***************************

Question 31:

'What tool can be used to perform SNMP enumeration?', A. 'DNSlookup', B. 'Whois', C. 'Nslookup', D. 'IP Network Browser'

==========================

Answer Option 1:

Final Answer: D

**************************

Answer Option 2:

Final Answer: D

**************************

Answer Option 3:

Final Answer: D

**************************

Answer Option 4:

Final Answer: D

**************************

Answer Option 5:

Final Answer: D

**************************

Answer Option 6:

Final Answer: D

**************************

Answer Option 7:

Final Answer: D

**************************

Answer Option 8:

Final Answer: D

**************************

Answer Option 9:

Final Answer: D

**************************

Question 32:

'Which among them has the strongest wireless security?', A. 'WEP', B. 'WPA', C. 'WPA2', D. 'WPA3'

==========================

Answer Option 1:

Final Answer: D

***************************

Answer Option 2:

Final Answer: D

***************************

Answer Option 3:

Final Answer: D

***************************

Answer Option 4:

Final Answer: D

***************************

Answer Option 5:

Final Answer: D

***************************

Answer Option 6:

Final Answer: D

***************************

Answer Option 7:

Final Answer: D

***************************

Answer Option 8:

Final Answer: D

***************************

Answer Option 9:

Final Answer: D

***************************

Question 33:

'Suppose Unix did not provide a way of passing file descriptors between processes, but still allowed inheriting file descriptors from a parent on fork and exec. What aspects of the OKWS design would break without file descriptor passing?

1. It would be impossible for services to get a TCP connection to the client web browser.

2. It would be impossible for okd to run as a non-root user.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

==========================

Answer Option 1:

Final Answer: D

***************************

Answer Option 2:

Final Answer: D

***************************

Answer Option 3:

Final Answer: D

***************************

Answer Option 4:

Final Answer: D

***************************

Answer Option 5:

Final Answer: D

***************************

Answer Option 6:

Final Answer: D

***************************

Answer Option 7:

Final Answer: D

***************************

Answer Option 8:

Final Answer: D

***************************

Answer Option 9:

Final Answer: D

***************************

Question 34:

'Failed sessions allow brute-force attacks on access credentials. This type of attacks are done in which layer of the OSI model?', A. 'Physical layer', B. 'Data-link Layer', C. 'Session layer', D. 'Presentation layer'

==========================

Answer Option 1:

Final Answer: C

**************************

Answer Option 2:

Final Answer: C

**************************

Answer Option 3:

Final Answer: C

**************************

Answer Option 4:

Final Answer: C

**************************

Answer Option 5:

Final Answer: C

**************************

Answer Option 6:

Final Answer: C

**************************

Answer Option 7:

Final Answer: C

**************************

Answer Option 8:

Final Answer: C

**************************

Answer Option 9:

Final Answer: C

**************************

Question 35:

'Which of the following is an authentication method?', A. 'Secret question', B. 'Biometric', C. 'SMS code', D. 'All of the above'

==========================

Answer Option 1:

Final Answer: D

***************************

Answer Option 2:

Final Answer: D

***************************

Answer Option 3:

Final Answer: D

***************************

Answer Option 4:

Final Answer: D

***************************

Answer Option 5:

Final Answer: D

***************************

Answer Option 6:

Final Answer: D

***************************

Answer Option 7:

Final Answer: D

***************************

Answer Option 8:

Final Answer: D

***************************

Answer Option 9:

Final Answer: D

***************************

Question 36:

'When does a buffer overflow occur, generally speaking?', A. 'when writing to a pointer that has been freed', B. 'when copying a buffer from the stack to the heap', C. 'when a pointer is used to access memory not allocated to it', D. 'when the program notices a buffer has filled up, and so starts to reject requests'

==========================

Answer Option 1:

Final Answer: C

**************************

Answer Option 2:

Final Answer: C

**************************

Answer Option 3:

Final Answer: C

**************************

Answer Option 4:

Final Answer: C

**************************

Answer Option 5:

Final Answer: C

**************************

Answer Option 6:

Final Answer: C

**************************

Answer Option 7:

Final Answer: C

**************************

Answer Option 8:

Final Answer: C

**************************

Answer Option 9:

Final Answer: C

**************************

Question 37:

'A digital signature needs a', A. 'Private-key system', B. 'Shared-key system', C. 'Public-key system', D. 'All of them'

==========================

Answer Option 1:

Final Answer: A

***************************

Answer Option 2:

Final Answer: C

***************************

Answer Option 3:

Final Answer: C

***************************

Answer Option 4:

Final Answer: A

***************************

Answer Option 5:

Final Answer: C

***************************

Answer Option 6:

Final Answer: C

***************************

Answer Option 7:

Final Answer: C

***************************

Answer Option 8:

Final Answer: C

***************************

Answer Option 9:

Final Answer: C

***************************

Question 38:

'A packet filter firewall filters at the', A. 'Application or transport', B. 'Data link layer', C. 'Physical Layer', D. 'Network or transport layer'

===========================

Answer Option 1:

Final Answer: D

***************************

Answer Option 2:

Final Answer: D

***************************

Answer Option 3:

Final Answer: D

***************************

Answer Option 4:

Final Answer: D

***************************

Answer Option 5:

Final Answer: D

***************************

Answer Option 6:

Final Answer: D

***************************

Answer Option 7:

Final Answer: D

***************************

Answer Option 8:

Final Answer: D

***************************

Answer Option 9:

Final Answer: D

***************************

Question 39:

'Let I = (S,V)I=(S,V) be a MAC. Suppose S(k,m)S(k,m) is always 5 bits long. Can this MAC be secure?', A. 'No, an attacker can simply guess the tag for messages', B. 'It depends on the details of the MAC', C. 'Yes, the attacker cannot generate a valid tag for any message', D. 'Yes, the PRG is pseudorandom'

==========================

Answer Option 1:

Final Answer: A

***************************

Answer Option 2:

Final Answer: A

***************************

Answer Option 3:

Final Answer: A

***************************

Answer Option 4:

Final Answer: A

***************************

Answer Option 5:

Final Answer: A

***************************

Answer Option 6:

Final Answer: A

***************************

Answer Option 7:

Final Answer: A

***************************

Answer Option 8:

Final Answer: A

***************************

Answer Option 9:

Final Answer: A

***************************

Question 40:

'Which of the following deals with network intrusion detection and real-time traffic analysis?', A. 'John the Ripper', B. 'L0phtCrack', C. 'Snort', D. 'Nessus'

==========================

Answer Option 1:

Final Answer: C

**************************

Answer Option 2:

Final Answer: C

**************************

Answer Option 3:

Final Answer: C

**************************

Answer Option 4:

Final Answer: C

**************************

Answer Option 5:

Final Answer: C

**************************

Answer Option 6:

Final Answer: C

**************************

Answer Option 7:

Final Answer: C

**************************

Answer Option 8:

Final Answer: C

**************************

Answer Option 9:

Final Answer: C

**************************

Question 41:

'The Message condentiality or privacy means that the sender and the receiver expect', A. 'Integrity', B. 'Condentiality', C. 'Authentication', D. 'Nonrepudiation'

==========================

Answer Option 1:

Final Answer: B

**************************

Answer Option 2:

Final Answer: B

**************************

Answer Option 3:

Final Answer: B

**************************

Answer Option 4:

Final Answer: B

**************************

Answer Option 5:

Final Answer: B

**************************

Answer Option 6:

Final Answer: B

**************************

Answer Option 7:

Final Answer: B

**************************

Answer Option 8:

Final Answer: B

**************************

Answer Option 9:

Final Answer: B

**************************

Question 42:

'When a wireless user authenticates to any AP, both of them go in the course of four-step authentication progression which is called _____________', A. 'AP-handshaking', B. '4-way handshake', C. '4-way connection', D. 'wireless handshaking'

==========================

Answer Option 1:

Final Answer: B

***************************

Answer Option 2:

Final Answer: B

***************************

Answer Option 3:

Final Answer: B

***************************

Answer Option 4:

Final Answer: B

***************************

Answer Option 5:

Final Answer: B

***************************

Answer Option 6:

Final Answer: B

***************************

Answer Option 7:

Final Answer: B

***************************

Answer Option 8:

Final Answer: B

***************************

Answer Option 9:

Final Answer: B

***************************

Question 43:

'Message authentication is a service beyond', A. 'Message Condentiality', B. 'Message Integrity', C. 'Message Splashing', D. 'Message Sending'

==========================

Answer Option 1:

Final Answer: B

***************************

Answer Option 2:

Final Answer: B

***************************

Answer Option 3:

Final Answer: B

***************************

Answer Option 4:

Final Answer: B

***************************

Answer Option 5:

Final Answer: B

***************************

Answer Option 6:

Final Answer: B

***************************

Answer Option 7:

Final Answer: B

***************************

Answer Option 8:

Final Answer: B

***************************

Answer Option 9:

Final Answer: B

***************************

Question 44:

'Which of the following are most vulnerable to injection attacks?', A. 'Session IDs', B. 'Registry keys', C. 'Network communications', D. 'SQL queries based on user input'

==========================

Answer Option 1:

Final Answer: D

***************************

Answer Option 2:

Final Answer: D

***************************

Answer Option 3:

Final Answer: D

***************************

Answer Option 4:

Final Answer: D

***************************

Answer Option 5:

Final Answer: D

***************************

Answer Option 6:

Final Answer: D

***************************

Answer Option 7:

Final Answer: D

***************************

Answer Option 8:

Final Answer: D

***************************

Answer Option 9:

Final Answer: D

***************************

Question 45:

'Assume that a TLS connection has been established successfully between a client and a server. Establishing the session included checking the server certificate and executing a DiffieHelmann exchange, but the client did not provide a client certificate. Further, assume that the client and server are honest, that the client and server don’t leak their keys, and that the cryptography is good. Which of the following attacks does TLS protect against?

1. An attacker replacing bytes sent by a client with bytes of the attacker’s own choosing.

2. An attacker reading the plaintext bytes sent by a client.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

==========================

Answer Option 1:

Final Answer: A

***************************

Answer Option 2:

Final Answer: A

***************************

Answer Option 3:

Final Answer: A

***************************

Answer Option 4:

Final Answer: A

***************************

Answer Option 5:

Final Answer: A

***************************

Answer Option 6:

Final Answer: A

***************************

Answer Option 7:

Final Answer: A

***************************

Answer Option 8:

Final Answer: A

***************************

Answer Option 9:

Final Answer: A

***************************

Question 46:

'Which of the following is a Wireless traffic Sniffing tool?', A. 'Maltego', B. 'BurpSuit', C. 'Nessus', D. 'Wireshark'

==========================

Answer Option 1:

Final Answer: D

***************************

Answer Option 2:

Final Answer: D

***************************

Answer Option 3:

Final Answer: D

***************************

Answer Option 4:

Final Answer: D

***************************

Answer Option 5:

Final Answer: D

***************************

Answer Option 6:

Final Answer: D

***************************

Answer Option 7:

Final Answer: D

***************************

Answer Option 8:

Final Answer: D

***************************

Answer Option 9:

Final Answer: D

***************************

Question 47:

'A ___________ is a method in which a computer security mechanism is bypassed untraceable for accessing the computer or its information.', A. 'front-door', B. 'backdoor', C. 'clickjacking', D. 'key-logging'

==========================

Answer Option 1:

Final Answer: B

***************************

Answer Option 2:

Final Answer: B

***************************

Answer Option 3:

Final Answer: B

***************************

Answer Option 4:

Final Answer: B

***************************

Answer Option 5:

Final Answer: B

***************************

Answer Option 6:

Final Answer: B

***************************

Answer Option 7:

Final Answer: B

***************************

Answer Option 8:

Final Answer: B

***************************

Answer Option 9:

Final Answer: B

***************************

Question 48:

'Which of the following is not a block cipher operating mode?', A. 'ECB', B. 'CFB', C. 'CBF', D. 'CBC'

==========================

Answer Option 1:

Final Answer: C

***************************

Answer Option 2:

Final Answer: C

***************************

Answer Option 3:

Final Answer: C

***************************

Answer Option 4:

Final Answer: C

***************************

Answer Option 5:

Final Answer: C

***************************

Answer Option 6:

Final Answer: C

***************************

Answer Option 7:

Final Answer: C

***************************

Answer Option 8:

Final Answer: C

***************************

Answer Option 9:

Final Answer: C

***************************

Question 49:

'What is a web proxy?', A. 'A piece of software that intercepts and possibly modifies requests (and responses) between a web browser and web server', B. 'An agent that makes decisions on the client's behalf when interacting with web applications', C. 'A piece of software that makes a web application look like a standalone application, making it easier to test', D. 'A simulator for the web, for use when off-line'

==========================

Answer Option 1:

Final Answer: A

**************************

Answer Option 2:

Final Answer: A

**************************

Answer Option 3:

Final Answer: A

**************************

Answer Option 4:

Final Answer: A

**************************

Answer Option 5:

Final Answer: A

**************************

Answer Option 6:

Final Answer: A

**************************

Answer Option 7:

Final Answer: A

**************************

Answer Option 8:

Final Answer: A

**************************

Answer Option 9:

Final Answer: A

**************************

Question 50:

'Buffer-overflow may remain as a bug in apps if __________ are not done fully.', A. 'boundary hacks', B. 'memory checks', C. 'boundary checks', D. 'buffer checks'

==========================

Answer Option 1:

Final Answer: C

***************************

Answer Option 2:

Final Answer: C

***************************

Answer Option 3:

Final Answer: C

***************************

Answer Option 4:

Final Answer: C

***************************

Answer Option 5:

Final Answer: C

***************************

Answer Option 6:

Final Answer: C

***************************

Answer Option 7:

Final Answer: C

***************************

Answer Option 8:

Final Answer: C

***************************

Answer Option 9:

Final Answer: C

***************************