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: C

****

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: A

****

Answer Option 7:

Final Answer: C

****

Answer Option 8:

Final Answer: C

****

Answer Option 9:

Final Answer: C

****

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: A

****

Answer Option 2:

Final Answer: C

****

Answer Option 3:

Final Answer: B

****

Answer Option 4:

Final Answer: C

****

Answer Option 5:

Final Answer: B

****

Answer Option 6:

Final Answer: C

****

Answer Option 7:

Final Answer: C

****

Answer Option 8:

Final Answer: B

****

Answer Option 9:

Final Answer: C

****

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: C, D

****

Answer Option 2:

Final Answer: C, D

****

Answer Option 3:

Final Answer: C, D

****

Answer Option 4:

Final Answer: A, C, D

****

Answer Option 5:

Final Answer: A, C, D

****

Answer Option 6:

Final Answer: C, D

****

Answer Option 7:

Final Answer: C and D

****

Answer Option 8:

Final Answer: A, B, C, D

****

Answer Option 9:

Final Answer: C, D

****

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 $H:X^{\leq L} \to T$ H: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: A

****

Answer Option 2:

Final Answer: B

****

Answer Option 3:

Final Answer: B

****

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: B

****

Answer Option 9:

Final Answer: C

****

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: D

****

Answer Option 3:

Final Answer: C

****

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 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: C

****

Answer Option 3:

Final Answer: D

****

Answer Option 4:

Final Answer: C

****

Answer Option 5:

Final Answer: D

****

Answer Option 6:

Final Answer: D

****

Answer Option 7:

Final Answer: C

****

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: 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 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: 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 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: D

****

Answer Option 2:

Final Answer: D

****

Answer Option 3:

Final Answer: C

****

Answer Option 4:

Final Answer: A

****

Answer Option 5:

Final Answer: D

****

Answer Option 6:

Final Answer: C

****

Answer Option 7:

Final Answer: C

****

Answer Option 8:

Final Answer: A

****

Answer Option 9:

Final Answer: D

****

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: C

****

Answer Option 2:

Final Answer: C

****

Answer Option 3:

Final Answer: B

****

Answer Option 4:

Final Answer: A

****

Answer Option 5:

Final Answer: B

****

Answer Option 6:

Final Answer: C

****

Answer Option 7:

Final Answer: B

****

Answer Option 8:

Final Answer: C

****

Answer Option 9:

Final Answer: B

****

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: 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: B

****

Answer Option 9:

Final Answer: D

****

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: B

****

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: C

****

Answer Option 4:

Final Answer: A

****

Answer Option 5:

Final Answer: A

****

Answer Option 6:

Final Answer: C

****

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: 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 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: 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 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: C

****

Answer Option 2:

Final Answer: B

****

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: B

****

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: 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 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

****

Question 51:

'Applications developed by programming languages like _____ and _____ have this common buffer-overflow error.', A. 'C, Ruby', B. 'Python, Ruby', C. 'C, C++', D. 'Tcl, C#'

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

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 52:

'Encryption and decryption provide secrecy, or condentiality, but not', A. 'Authentication', B. 'Integrity', C. 'Privacy', D. 'All of the above'

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

Answer Option 1:

Final Answer: D

****

Answer Option 2:

Final Answer: B

****

Answer Option 3:

Final Answer: B

****

Answer Option 4:

Final Answer: B

****

Answer Option 5:

Final Answer: D

****

Answer Option 6:

Final Answer: D

****

Answer Option 7:

Final Answer: D

****

Answer Option 8:

Final Answer: B

****

Answer Option 9:

Final Answer: D

****

Question 53:

'A/an _____ is a program that steals your logins & passwords for instant messaging applications.', A. 'IM – Trojans', B. 'Backdoor Trojans', C. 'Trojan-Downloader', D. 'Ransom Trojan'

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

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 54:

'The sub key length at each round of DES is_____', A. '32', B. '56', C. '48', D. '64'

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

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 55:

'Which of the following is true of mutation-based fuzzing?', A. 'It generates each different input by modifying a prior input', B. 'It works by making small mutations to the target program to induce faults', C. 'Each input is mutation that follows a given grammar', D. 'It only makes sense for file-based fuzzing, not network-based fuzzing'

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

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 56:

'What are the types of scanning?', A. 'Port, network, and services', B. 'Network, vulnerability, and port ', C. 'Passive, active, and interactive', D. 'Server, client, and network'

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

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: B

****

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 57:

'A sender must not be able to deny sending a message that was sent, is known as', A. 'Message Nonrepudiation', B. 'Message Integrity', C. 'Message Condentiality', D. 'Message Sending'

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

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 58:

'A proxy rewall lters at the', A. 'Physical layer', B. 'Application layer', C. 'Data link layer', D. 'Network layer'

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

Answer Option 1:

Final Answer: B

****

Answer Option 2:

Final Answer: D

****

Answer Option 3:

Final Answer: B

****

Answer Option 4:

Final Answer: D

****

Answer Option 5:

Final Answer: D

****

Answer Option 6:

Final Answer: B

****

Answer Option 7:

Final Answer: B

****

Answer Option 8:

Final Answer: D

****

Answer Option 9:

Final Answer: D

****

Question 59:

'Encapsulating Security Payload (ESP) belongs to which Internet Security Protocol?', A. 'Secure Socket Layer Protocol', B. 'Secure IP Protocol', C. 'Secure Http Protocol', D. 'Transport Layer Security

Protocol'

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

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 60:

'A special tool is necessary for entering the network which is _____ that helps the anonymous internet users to access into the Tor's network and use various Tor services.', A. 'Opera browser', B.

'Firefox', C. 'Chrome', D. 'Tor 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 61:

'How does a buffer overflow on the stack facilitate running attacker-injected code?', A. 'By overwriting the return address to point to the location of that code', B. 'By writing directly to the instruction pointer

register the address of the code', C. 'By writing directly to %eax the address of the code', D. 'By changing the name of the running executable, stored on the stack'

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

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 62:

'The digest created by a hash function is normally called a', A. 'Modication detection code (MDC)', B. 'Modify authentication connection', C. 'Message authentication control', D. 'Message authentication cipher'

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

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 63:

'Let F: K \times R \to MF:K×R→M be a secure PRF. For m \in Mm∈M define E(k,m) = \big[r \gets R,\ \text{output } \big(r,\ F(k,r) \oplus m\big)\ \big]E(k,m)=[r←R, output (r, F(k,r)⊕m)] Is EE symantically secure under CPA?', A. 'Yes, whenever F is a secure PRF', B. 'No, there is always a CPA attack on this system', C. 'Yes, but only if R is large enough so r never repeats (w.h.p)', D. 'It depends on what F is used'

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

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 64:

'Old operating systems like _____ and NT-based systems have buffer-overflow attack a common vulnerability.', A. 'Windows 7', B. 'Chrome', C. 'IOS12', D. 'UNIX'

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

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 65:

'What is a replay attack?', A. 'When the attacker replies to a message sent to it by the system', B. 'An attack that continuously repeats, probing for a weakness', C. 'An attack that uses the system's own messages and so cannot be defended against', D. 'The attacker resends a captured message, and the site accept its and responds in the attacker's favor'

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

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 66:

'Statement 1| A U2F USB dongle prevents malware on the user's computer from stealing the user's second factor to authenticate as that user even when the user's computer is turned off. Statement 2| A

server using U2F can reliably determine that the user who is attempting to login is indeed behind the computer that sent the login request.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

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

Answer Option 1:

Final Answer: C

****

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 67:

'_____ is the anticipation of unauthorized access or break to computers or data by means of wireless networks.', A. 'Wireless access', B. 'Wireless security', C. 'Wired Security', D. 'Wired device apps'

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

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 68:

'Which of the following are benefits of penetration testing?', A. 'Results are often reproducible', B. 'Full evidence of security: a clean test means a secure system', C. 'Compositionality of security properties

means tested components are secure even if others change', D. 'Makes an adversarial neural network converge more quickly'

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

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 69:

'1. _____ framework made cracking of vulnerabilities easy like point and click.', A. '.Net', B. 'Metasploit', C. 'Zeus', D. 'Ettercap'

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

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 70:

'You are given a message (m) and its OTP encryption (c). Can you compute the OTP key from m and c ?', A. 'No, I cannot compute the key.', B. 'Yes, the key is k = m xor c.', C. 'I can only compute half the

bits of the key.', D. 'Yes, the key is k = m xor m.'

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

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 71:

'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. CR and MR

2. CR', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

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

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: D

****

Answer Option 9:

Final Answer: C

****

Question 72:

'When the data must arrive at the receiver exactly as they were sent, its called', 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 73:

'What is the difference between a direct leak and a side channel?', A. 'A direct leak creates a denial of service by failing to free memory, while a channel frees memory as a side effect', B. 'A direct leak is one that is intentional, rather than by unintentional', C. 'A direct leak comes via the software system's intended interaction mechanism, where as a side channel leak comes from measurements of other system features, like timing, power usage, or space usage', D. 'There is no difference'

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

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 74:

'A session symmetric key between two parties is used', A. 'Only once', B. 'Twice', C. 'Multiple times', D. 'Conditions dependant'

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

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 75:

'What is a nop sled', A. 'It is an anonymous version of a mop sled', B. 'It is a sequence of nops preceding injected shellcode, useful when the return address is unknown', C. 'It is a method of removing zero

bytes from shellcode', D. 'It is another name for a branch instruction at the end of sequence of nops'

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

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 76:

'Which Nmap scan is does not completely open a TCP connection?', A. 'SYN stealth scan', B. 'TCP connect', C. 'XMAS tree scan', D. 'ACK scan'

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

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 77:

'Based on the paper "Click Trajectories: End-to-End Analysis of the Spam Value Chain", which of the following statements are true? "Spammers" here refer to operators of various parts of the "spam value chain.", A. 'Spammers run their spam-advertised web sites on compromised user machines that are part of a botnet.', B. 'Spammers need to register domain names in order for their spam-based advertisements to be effective.', C. 'There is a high cost for spammers to switch acquiring banks.', D. 'B and C'

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

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 78:

'In a _____ attack, the extra data that holds some specific instructions in the memory for actions is projected by a cyber-criminal or penetration tester to crack the system.', A. 'Phishing', B. 'MiTM', C. 'Buffer-overflow', D. 'Clickjacking'

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

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 79:

'_____ is a popular tool used for network analysis in multiprotocol diverse network.', A. 'Snort', B. 'SuperScan', C. 'Burp Suit', D. 'EtterPeak'

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

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 80:

'_____ is alike as that of Access Point (AP) from 802.11, & the mobile operators uses it for offering signal coverage.', A. 'Base Signal Station', B. 'Base Transmitter Station', C. 'Base Transceiver Station', D. 'Transceiver Station'

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

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 81:

'A _____ is a sequential segment of the memory location that is allocated for containing some data such as a character string or an array of integers.', A. 'stack', B. 'queue', C. 'external storage', D.

'buffer'

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

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 82:

'Which form of encryption does WPA use?', A. 'Shared key', B. 'LEAP', C. 'TKIP', D. 'AES'

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

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 83:

'Let suppose a search box of an application can take at most 200 words, and you've inserted more than that and pressed the search button; the system crashes. Usually this is because of limited

_____', A. 'buffer', B. 'external storage', C. 'processing power', D. 'local storage'

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

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 84:

'_____ began to show up few years back on wireless access points as a new way of adding or connecting new devices.', A. 'WPA2', B. 'WPA', C. 'WPS', D. 'WEP'

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

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 85:

'What are the port states determined by Nmap?', A. 'Active, inactive, standby', B. 'Open, half-open, closed ', C. 'Open, filtered, unfiltered', D. 'Active, closed, unused'

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

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 86:

'Which among the following is the least strong security encryption standard?', A. 'WEP', B. 'WPA', C. 'WPA2', D. 'WPA3'

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

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 87:

'Why is it that the compiler does not know the absolute address of a local variable?', A. 'Programs are not allowed to reference memory using absolute addresses', B. 'The size of the address depends on the architecture the program will run on', C. 'As a stack-allocated variable, it could have different addresses depending on when its containing function is called', D. 'Compiler writers are not very good at that sort of thing'

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

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 88:

'The stack is memory for storing', A. 'Local variables', B. 'Program code', C. 'Dynamically linked libraries', D. 'Global variables'

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

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 89:

'Can a stream cipher have perfect secrecy?', A. 'Yes, if the PRG is really "secure"', B. 'No, there are no ciphers with perfect secrecy', C. 'Yes, every cipher has perfect secrecy', D. 'No, since the key is shorter

than the message'

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

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: B

****

Answer Option 8:

Final Answer: A

****

Answer Option 9:

Final Answer: A

****

Question 90:

'Which of the following does authorization aim to accomplish?', A. 'Restrict what operations/data the user can access', B. 'Determine if the user is an attacker', C. 'Flag the user if he/she misbehaves', D.

'Determine who the user is'

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

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 91:

'The message must be encrypted at the sender site and decrypted at the', A. 'Sender Site', B. 'Site', C. 'Receiver site', D. 'Conferencing'

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

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 92:

'A _____ may be a hidden part of a program, a separate infected program a Trojan in disguise of an executable or code in the firmware of any system's hardware.', A. 'crypter', B. 'virus', C.

'backdoor', D. 'key-logger'

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

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 93:

'How is IP address spoofing detected?', A. 'Installing and configuring a IDS that can read the IP header', B. 'Comparing the TTL values of the actual and spoofed addresses', C. 'Implementing a firewall to the network', D. 'Identify all TCP sessions that are initiated but does not complete successfully'

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

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 94:

'Which of the following is not an example of presentation layer issues?', A. 'Poor handling of unexpected input can lead to the execution of arbitrary instructions', B. 'Unintentional or ill-directed use of superficially supplied input', C. 'Cryptographic flaws in the system may get exploited to evade privacy', D. 'Weak or non-existent authentication mechanisms'

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

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 95:

'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 send messages to oklogd.

2. It would be impossible for services to get a TCP connection to a database proxy.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

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

Answer Option 1:

Final Answer: C

****

Answer Option 2:

Final Answer: C

****

Answer Option 3:

Final Answer: D

****

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 96:

'Why would a ping sweep be used?', A. 'To identify live systems', B. 'To locate live systems', C. 'To identify open ports', D. 'To locate firewalls'

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

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 97:

'The four Primary Security Principles related to messages are', A. 'Confidentiality, Integrity, Non repudiation and Authentication', B. 'Confidentiality, Access Control, Integrity, Non repudiation', C. 'Authentication, Authorization, Availability, Integrity', D. 'Availability, Authorization, Confidentiality, Integrity'

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

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 98:

'What was the first buffer overflow attack?', A. 'Love Bug', B. 'SQL Slammer', C. 'Morris Worm', D. 'Code Red'

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

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 99:

'The _____ can cost you money, by sending text messages from your mobile phone numbers.', A. 'IM – Trojans', B. 'Backdoor Trojans', C. 'SMS Trojan', D. 'Ransom Trojan'

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

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 100:

'Three of the following are classic security properties; which one is not?', A. 'Confidentiality', B. 'Availability', C. 'Correctness', D. 'Integrity'

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

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

****