A. Input validation flaw
B. HTTP header injection vulnerability
C. 0-day vulnerability
D. Time-to-check to time-to-use flaw

Correct Answer: C

QUESTION 477

What are the three types of authentication?

A. Something you: know, remember, prove.
B. Something you: have, know, are.
C. Something you: show, prove, are.
D. Something you: show, have, prove.

Correct Answer: B

QUESTION 478

What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

A. Legal, performance, audit.
B. Audit, standards based, regulatory.
C. Contractual, regulatory, industry.
D. Legislative, contractual, standards based.

Correct Answer: D

QUESTION 479

While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?

A. 10.10.10.10
B. 127.0.0.1
C. 192.168.1.1
D. 192.168.168.168

Correct Answer: B

QUESTION 480

Which of the following business challenges could be solved by using a vulnerability scanner?

A. Auditors want to discover if all systems are following a standard naming convention.

B. A web server was compromised and management needs to know if any further systems were compromised.

C. There is an emergency need to remove administrator access from multiple machines for an employee that quit.

D. There is a monthly requirement to test corporate compliance with host application usage and security policies.

Correct Answer: D

QUESTION 481

Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?

A. Fast processor to help with network traffic analysis.

B. They must be dual-homed.

C. Similar RAM requirements.

D. Fast network interface cards.

Correct Answer: B

QUESTION 482

If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?

A. SDLC process

B. Honey pot

C. SQL injection

D. Trap door

Correct Answer: D

QUESTION 483

A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

A. Public key
B. Private key
C. Modulus length
D. Email server certificate

Correct Answer: B

QUESTION 484

Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS
B. IANA
C. CAPTCHA
D. IETF

Correct Answer: A

QUESTION 485

Which set of access control solutions implements two-factor authentication?

A. USB token and PIN
B. Fingerprint scanner and retina scanner
C. Password and PIN
D. Account and password

Correct Answer: A

QUESTION 486

What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

A. Blue Book

B. ISO 26029
C. Common Criteria
D. The Wassenaar Agreement

Correct Answer: C

QUESTION 487

Advanced encryption standard is an algorithm used for which of the following?

A. Data integrity
B. Key discovery
C. Bulk data encryption
D. Key recovery

Correct Answer: C

QUESTION 488

Which statement best describes a server type under an N-tier architecture?

A. A group of servers at a specific layer.
B. A single server with a specific role.
C. A group of servers with a unique role.
D. A single server at a specific layer.

Correct Answer: C

QUESTION 489

During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?

A. The web application does not have the secure flag set.
B. The session cookies do not have the HttpOnly flag set.
C. The victim user should not have an endpoint security solution.
D. The victim's browser must have ActiveX technology enabled.

Correct Answer: B

QUESTION 490

Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

A. UDP 123
B. UDP 541
C. UDP 514
D. UDP 415

Correct Answer: C

QUESTION 491

A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

A. Say no; the friend is not the owner of the account.
B. Say yes; the friend needs help to gather evidence.
C. Say yes; do the job for free.
D. Say no; make sure that the friend knows the risk she's asking the CEH to take.

Correct Answer: A

QUESTION 492

A hacker is attempting to see which ports have been left open on a network. Which NMAP switch would the hacker use?

A. -sO
B. -sP
C. -sS
D. -sU

Correct Answer: A

QUESTION 493

The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

A. Asymmetric
B. Confidential
C. Symmetric
D. Non-confidential