B. C#
C. Python
D. ASP.NET

Correct Answer: C

QUESTION 427
While performing data validation of web content, a security technician is required to restrict malicious input. Which of the following processes is an efficient way of restricting malicious input?

A. Validate web content input for query strings.
B. Validate web content input with scanning tools.
C. Validate web content input for type, length, and range.
D. Validate web content input for extraneous queries.

Correct Answer: C

QUESTION 428
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

A. The gateway is not routing to a public IP address.
B. The computer is using an invalid IP address.
C. The gateway and the computer are not on the same network.
D. The computer is not using a private IP address.

Correct Answer: A

QUESTION 429
A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location. During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis. Which of the following is an issue with the situation?

A. Segregation of duties.
B. Undue influence.
C. Lack of experience.
D. Inadequate disaster recovery plan.

Correct Answer: A

QUESTION 430
In the OSI model, where does PPTP encryption take place?

A. Transport layer
B. Application layer
C. Data link layer
D. Network layer

Correct Answer: C

QUESTION 431
What is the main advantage that a network-based IDS/IPS system has over a host-based solution?

A. They do not use host system resources.
B. They are placed at the boundary, allowing them to inspect all traffic.
C. They are easier to install and configure.
D. They will not interfere with user interfaces.

Correct Answer: A

QUESTION 432
An NMAP scan of a server shows port 25 is open. What risk could this pose?

A. Open printer sharing
B. Web portal data leak
C. Clear text authentication
D. Active mail relay

Correct Answer: D

QUESTION 433
Which of the following are variants of mandatory access control mechanisms? (Choose two.)

A. Two factor authentication
B. Acceptable use policy
C. Username / password
D. User education program
E. Sign in register

Correct Answer: AC

QUESTION 434
An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?

A. Classified
B. Overt
C. Encrypted
D. Covert

Correct Answer: D

QUESTION 435
An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?

A. Classified
B. Overt
C. Encrypted
D. Covert

Correct Answer: D

QUESTION 436
What is the primary drawback to using advanced encryption standard (AES) algorithm with a 256 bit key to share sensitive data?

A. Due to the key size, the time it will take to encrypt and decrypt the message hinders efficient communication.
B. To get messaging programs to function with this algorithm requires complex configurations.
C. It has been proven to be a weak cipher; therefore, should not be trusted to protect sensitive data.
D. It is a symmetric key algorithm, meaning each recipient must receive the key through a

different channel than the message.

Correct Answer: D

QUESTION 437

Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?

A. Cain
B. John the Ripper
C. Nikto
D. Hping

Correct Answer: A

QUESTION 438

Information gathered from social networking websites such as Facebook, Twitter and LinkedIn can be used to launch which of the following types of attacks? (Choose two.)

A. Smurf attack
B. Social engineering attack
C. SQL injection attack
D. Phishing attack
E. Fraggle attack
F. Distributed denial of service attack

Correct Answer: BD

QUESTION 439

Which of the following examples best represents a logical or technical control?

A. Security tokens
B. Heating and air conditioning
C. Smoke and fire alarms
D. Corporate security policy

Correct Answer: A

QUESTION 440

Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

A. Metasploit scripting engine
B. Nessus scripting engine
C. NMAP scripting engine
D. SAINT scripting engine

Correct Answer: C

QUESTION 441
A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

A. white box
B. grey box
C. red box
D. black box

Correct Answer: D

QUESTION 442
How can a policy help improve an employee's security awareness?

A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security.
B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees.
C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line.
D. By decreasing an employee's vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths.

Correct Answer: A

QUESTION 443
Which statement is TRUE regarding network firewalls preventing Web Application attacks?

A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.
B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.
C. Network firewalls can prevent attacks if they are properly configured.
D. Network firewalls cannot prevent attacks because they are too complex to configure.