Which of the following is an example of what the engineer performed?

A. Cross-site scripting
B. Banner grabbing
C. SQL injection
D. Whois database query

Correct Answer: B

QUESTION 377
To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

A. Harvesting
B. Windowing
C. Hardening
D. Stealthing

Correct Answer: C

QUESTION 378
While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model. Which type of firewall is the tester trying to traverse?

A. Packet filtering firewall
B. Application-level firewall
C. Circuit-level gateway firewall
D. Stateful multilayer inspection firewall

Correct Answer: C

QUESTION 379
Which type of scan is used on the eye to measure the layer of blood vessels?

A. Facial recognition scan
B. Retinal scan
C. Iris scan
D. Signature kinetics scan

Correct Answer: B

QUESTION 380

A security analyst in an insurance company is assigned to test a new web application that will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application's search form and introduces the following code in the search input field.

IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC" originalPath="vbscript:msgbox("Vulnerable");>"

When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable". Which web applications vulnerability did the analyst discover?

A. Cross-site request forgery
B. Command injection
C. Cross-site scripting
D. SQL injection

Correct Answer: C

QUESTION 381

While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site.

<script>alert(" Testing Testing Testing ")</script>

Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

A. Buffer overflow
B. Cross-site request forgery
C. Distributed denial of service
D. Cross-site scripting

Correct Answer: D

QUESTION 382
A hacker was able to sniff packets on a company's wireless network. The following information was discovered.

- The Key 10110010 01001011
- The Cyphertext 01100101 01011010

Using the Exclusive OR, what was the original message?

A. 00101000 11101110
B. 11010111 00010001
C. 00001101 10100100
D. 11110010 01011011

Correct Answer: B

QUESTION 383
International Organization for Standardization (ISO) standard 27002 provides guidance for compliance by outlining

A. guidelines and practices for security controls
B. financial soundness and business viability metrics
C. standard best practice for configuration management
D. contract agreement writing standards

Correct Answer: A

QUESTION 384
Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions?

A. Firewall
B. Honeypot
C. Core server
D. Layer 4 switch

Correct Answer: B

QUESTION 385
A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21. During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?

A. True negatives
B. False negatives
C. True positives
D. False positives

Correct Answer: D

QUESTION 386
The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:

Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

What type of activity has been logged?

A. Port scan targeting 192.168.1.103.
B. Teardrop attack targeting 192.168.1.106.
C. Denial of service attack targeting 192.168.1.103.
D. Port scan targeting 192.168.1.106.

Correct Answer: D

QUESTION 387
Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

A. Detective
B. Passive

C. Intuitive
D. Reactive

Correct Answer: B

QUESTION 388
Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?

A. Netstat WMI Scan
B. Silent Dependencies
C. Consider unscanned ports as closed
D. Reduce parallel connections on congestion

Correct Answer: D

QUESTION 389
Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

A. 768 bit key
B. 1025 bit key
C. 1536 bit key
D. 2048 bit key

Correct Answer: C

QUESTION 390
Which results will be returned with the following Google search query?

site:target.com -site:Marketing.target.com accounting

A. Results matching all words in the query
B. Results matching "accounting" in domain target.com but not on the site Marketing.target.com
C. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
D. Results for matches on target.com and Marketing.target.com that include the word "accounting"

Correct Answer: B