Correct Answer: C

QUESTION 257

On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

A. nessus +
B. nessus *s
C. nessus &
D. nessus -d

Correct Answer: C

QUESTION 258

Least privilege is a security concept that requires that a user is

A. limited to those functions required to do the job
B. given root or administrative privileges
C. trusted to keep all data and access to that data under their sole control
D. given privileges equal to everyone else in the department

Correct Answer: A

QUESTION 259

A covert channel is a channel that

A. transfers information over, within a computer system, or network that is outside of the security policy
B. transfers information over, within a computer system, or network that is within the security policy
C. transfers information via a communication path within a computer system, or network for transfer of data
D. transfers information over, within a computer system, or network that is encrypted

Correct Answer: A

QUESTION 260

SOAP services use which technology to format information?

A. SATA

B. PCI
C. XML
D. ISDN

Correct Answer: C

QUESTION 261
A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command.

NMAP –n –sS –P0 –p 80 ***.***.**.**

What type of scan is this?

A. Quick scan
B. Intense scan
C. Stealth scan
D. Comprehensive scan

Correct Answer: C

QUESTION 262
Which of the following is a hashing algorithm?

A. MD5
B. PGP
C. DES
D. ROT13

Correct Answer: A

QUESTION 263
Which of the following identifies the three modes in which Snort can be configured to run?

A. Sniffer, Packet Logger, and Network Intrusion Detection System.
B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System.
C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System.
D. Sniffer, Packet Logger, and Host Intrusion Prevention System.

Correct Answer: A

QUESTION 264
Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

A. Cross-site scripting
B. SQL injection
C. VPath injection
D. XML denial of service issues

Correct Answer: D

QUESTION 265
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?

A. NMAP -P 192.168.1-5.
B. NMAP -P 192.168.0.0/16
C. NMAP -P 192.168.1.0, 2.0, 3.0, 4.0, 5.0
D. NMAP -P 192.168.1/17

Correct Answer: A

QUESTION 266
When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

A. Vulnerability scanning
B. Social engineering
C. Application security testing
D. Network sniffing

Correct Answer: B

QUESTION 267
What is the broadcast address for the subnet 190.86.168.0/22?

A. 190.86.168.255
B. 190.86.255.255
C. 190.86.171.255
D. 190.86.169.255

Correct Answer: C

QUESTION 268
Which of the following are valid types of rootkits? (Choose three.)

A. Hypervisor level
B. Network level
C. Kernel level
D. Application level
E. Physical level
F. Data access level

Correct Answer: ACD

QUESTION 269
John the Ripper is a technical assessment tool used to test the weakness of which of the following?

A. Usernames
B. File permissions
C. Firewall rule sets
D. Passwords

Correct Answer: D

QUESTION 270
A company has made the decision to host their own email and basic web services. The administrator needs to set up the external firewall to limit what protocols should be allowed to get to the public part of the company's network. Which ports should the administrator open? (Choose three.)

A. Port 22
B. Port 23
C. Port 25
D. Port 53
E. Port 80
F. Port 139
G. Port 445

Correct Answer: CDE

QUESTION 271
Which type of scan measures a person's external features through a digital video camera?

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

Correct Answer: C

QUESTION 272
In order to show improvement of security over time, what must be developed?

A. Reports
B. Testing tools
C. Metrics
D. Taxonomy of vulnerabilities

Correct Answer: C

QUESTION 273
In the software security development life cycle process, threat modeling occurs in which phase?

A. Design
B. Requirements
C. Verification
D. Implementation

Correct Answer: A

QUESTION 274
Which of the following items of a computer system will an anti-virus program scan for viruses?

A. Boot Sector
B. Deleted Files
C. Windows Process List
D. Password Protected Files

Correct Answer: A