QUESTION 292
Which of the following processes evaluates the adherence of an organization to its stated security policy?

A. Vulnerability assessment
B. Penetration testing
C. Risk assessment
D. Security auditing

Correct Answer: D

QUESTION 293
Which of the following statements are true regarding N-tier architecture? (Choose two.)

A. Each layer must be able to exist on a physically independent system.
B. The N-tier architecture must have at least one logical layer.
C. Each layer should exchange information only with the layers above and below it.
D. When a layer is changed or updated, the other layers must also be recompiled or modified.

Correct Answer: AC

QUESTION 294
Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.
C. Hashing is faster compared to more traditional encryption algorithms.
D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

Correct Answer: D

QUESTION 295
What is the main disadvantage of the scripting languages as opposed to compiled programming languages?

A. Scripting languages are hard to learn.
B. Scripting languages are not object-oriented.

C. Scripting languages cannot be used to create graphical user interfaces.
D. Scripting languages are slower because they require an interpreter to run the code.

Correct Answer: D

QUESTION 296
Which of the following are password cracking tools? (Choose three.)

A. BTCrack
B. John the Ripper
C. KerbCrack
D. Nikto
E. Cain and Abel
F. Havij

Correct Answer: BCE

QUESTION 297
Which of the following techniques can be used to mitigate the risk of an on-site attacker from connecting to an unused network port and gaining full access to the network? (Choose three.)

A. Port Security
B. IPSec Encryption
C. Network Admission Control (NAC)
D. 802.1q Port Based Authentication
E. 802.1x Port Based Authentication
F. Intrusion Detection System (IDS)

Correct Answer: ACE

QUESTION 298
When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

A. At least once a year and after any significant upgrade or modification.
B. At least once every three years or after any significant upgrade or modification.
C. At least twice a year or after any significant upgrade or modification.
D. At least once every two years and after any significant upgrade or modification.

Correct Answer: A

QUESTION 299
Which type of antenna is used in wireless communication?

A. Omnidirectional
B. Parabolic
C. Uni-directional
D. Bi-directional

Correct Answer: A

QUESTION 300
Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?

A. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.
B. Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.
C. Configure the firewall to allow traffic on TCP port 53.
D. Configure the firewall to allow traffic on TCP port 8080.

Correct Answer: A

QUESTION 301
Which initial procedure should an ethical hacker perform after being brought into an organization?

A. Begin security testing.
B. Turn over deliverables.
C. Sign a formal contract with non-disclosure.
D. Assess what the organization is trying to protect.

Correct Answer: C

QUESTION 302
Which of the following guidelines or standards is associated with the credit card industry?

A. Control Objectives for Information and Related Technology (COBIT)
B. Sarbanes-Oxley Act (SOX)
C. Health Insurance Portability and Accountability Act (HIPAA)

D. Payment Card Industry Data Security Standards (PCI DSS)

Correct Answer: D

QUESTION 303
An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

A. Timing attack
B. Replay attack
C. Memory trade-off attack
D. Chosen plain-text attack

Correct Answer: D

QUESTION 304
Which tool can be used to silently copy files from USB devices?

A. USB Grabber
B. USB Dumper
C. USB Sniffer
D. USB Snoopy

Correct Answer: B

QUESTION 305
How can a rootkit bypass Windows 7 operating system’s kernel mode, code signing policy?

A. Defeating the scanner from detecting any code change at the kernel.
B. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions.
C. Performing common services for the application process and replacing real applications with fake ones.
D. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options.

Correct Answer: D

QUESTION 306

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system.
B. Determine the impact of enabling the audit feature.
C. Perform a cost/benefit analysis of the audit feature.
D. Allocate funds for staffing of audit log review.

Correct Answer: B

QUESTION 307

A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer. What is the consultant's obligation to the financial organization?

A. Say nothing and continue with the security testing.
B. Stop work immediately and contact the authorities.
C. Delete the pornography, say nothing, and continue security testing.
D. Bring the discovery to the financial organization's human resource department.

Correct Answer: B

QUESTION 308

How is sniffing broadly categorized?

A. Active and passive.
B. Broadcast and unicast.
C. Unmanaged and managed.
D. Filtered and unfiltered.

Correct Answer: A

QUESTION 309

An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

A. g++ hackersExploit.cpp -o calc.exe
B. g++ hackersExploit.py -o calc.exe