QUESTION 391
One advantage of an application-level firewall is the ability to

A. filter packets at the network level
B. filter specific commands, such as http:post
C. retain state information for each packet
D. monitor tcp handshaking

Correct Answer: B

QUESTION 392
Which type of security document is written with specific step-by-step details?

A. Process
B. Procedure
C. Policy
D. Paradigm

Correct Answer: B

QUESTION 393
A certified ethical hacker (CEH) completed a penetration test of the main headquarters of a company almost two months ago, but has yet to get paid. The customer is suffering from financial problems, and the CEH is worried that the company will go out of business and end up not paying. What actions should the CEH take?

A. Threaten to publish the penetration test results if not paid.
B. Follow proper legal procedures against the company to request payment.
C. Tell other customers of the financial problems with payments from this company.
D. Exploit some of the vulnerabilities found on the company webserver to deface it.

Correct Answer: B

QUESTION 394
If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

A. Hping

B. Traceroute
C. TCP ping
D. Broadcast ping

Correct Answer: A

QUESTION 395
How can rainbow tables be defeated?

A. Password salting.
B. Use of non-dictionary words.
C. All uppercase character passwords.
D. Lockout accounts under brute force password cracking attempts.

Correct Answer: A

QUESTION 396
Which of the following is an advantage of utilizing security testing methodologies to conduct a security audit?

A. They provide a repeatable framework.
B. Anyone can run the command line scripts.
C. They are available at low cost.
D. They are subject to government regulation.

Correct Answer: A

QUESTION 397
A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

A. if (billingAddress = 50) {update field} else exit
B. if (billingAddress != 50) {update field} else exit
C. if (billingAddress >= 50) {update field} else exit
D. if (billingAddress <= 50) {update field} else exit

Correct Answer: D

QUESTION 398
If the final set of security controls does not eliminate all risk in a system, what could be done next?

A. Continue to apply controls until there is zero risk.
B. Ignore any remaining risk.
C. If the residual risk is low enough, it can be accepted.
D. Remove current controls since they are not completely effective.

Correct Answer: C

QUESTION 399
In keeping with the best practices of layered security, where are the best places to place intrusion detection/intrusion prevention systems? (Choose two.)

A. HID/HIP (Host-based Intrusion Detection/Host-based Intrusion Prevention)
B. NID/NIP (Node-based Intrusion Detection/Node-based Intrusion Prevention)
C. NID/NIP (Network-based Intrusion Detection/Network-based Intrusion Prevention)
D. CID/CIP (Computer-based Intrusion Detection/Computer-based Intrusion Prevention)

Correct Answer: AC

QUESTION 400
What is one thing a tester can do to ensure that the software is trusted and is not changing or tampering with critical data on the back end of a system it is loaded on?

A. Proper testing
B. Secure coding principles
C. Systems security and architecture review
D. Analysis of interrupts within the software

Correct Answer: D

QUESTION 401
Which of the following algorithms provides better protection against brute force attacks by using a 160-bit message digest?

A. MD5
B. SHA-1

C. RC4
D. MD4

Correct Answer: B

QUESTION 402

Company A and Company B have just merged and each has its own Public Key Infrastructure (PKI). What must the Certificate Authorities (CAs) establish so that the private PKIs for Company A and Company B trust one another and each private PKI can validate digital certificates from the other company?

A. Poly key exchange
B. Cross certification
C. Poly key reference
D. Cross-site exchange

Correct Answer: B

QUESTION 403

What is the best defense against privilege escalation vulnerability?

A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.
B. Run administrator and applications on least privileges and use a content registry for tracking.
C. Run services with least privileged accounts and implement multi-factor authentication and authorization.
D. Review user roles and administrator privileges for maximum utilization of automation services.

Correct Answer: C

QUESTION 404

Fingerprinting VPN firewalls is possible with which of the following tools?

A. Angry IP
B. Nikto
C. Ike-scan
D. Arp-scan

Correct Answer: C

QUESTION 405
A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?

A. Reject all invalid email received via SMTP.
B. Allow full DNS zone transfers.
C. Remove A records for internal hosts.
D. Enable null session pipes.

Correct Answer: C

QUESTION 406
Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.
B. CSIRT provides a computer security surveillance service to supply a government with important intelligence information on individuals travelling abroad.
C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multi-national corporations.
D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

Correct Answer: A

QUESTION 407
Which of the following is a client-server tool utilized to evade firewall inspection?

A. tcp-over-dns
B. kismet
C. nikto
D. hping

Correct Answer: A

QUESTION 408
Which of the following is a symmetric cryptographic standard?