application.

D. The vulnerable application does not display errors with information about the injection results to the attacker.

Correct Answer: D

QUESTION 326

Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

A. Regulatory compliance
B. Peer review
C. Change management
D. Penetration testing

Correct Answer: C

QUESTION 327

Data hiding analysis can be useful in

A. determining the level of encryption used to encrypt the data.
B. detecting and recovering data that may indicate knowledge, ownership or intent.
C. identifying the amount of central processing unit (cpu) usage over time to process the data.
D. preventing a denial of service attack on a set of enterprise servers to prevent users from accessing the data.

Correct Answer: B

QUESTION 328

Smart cards use which protocol to transfer the certificate in a secure manner?

A. Extensible Authentication Protocol (EAP)
B. Point to Point Protocol (PPP)
C. Point to Point Tunneling Protocol (PPTP)
D. Layer 2 Tunneling Protocol (L2TP)

Correct Answer: A

QUESTION 329

A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:

- Untrust (Internet) – (Remote network = 217.77.88.0/24)
- DMZ (DMZ) – (11.12.13.0/24)
- Trust (Intranet) – (192.168.0.0/24)

The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?

A. Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389
B. Permit 217.77.88.12 11.12.13.50 RDP 3389
C. Permit 217.77.88.12 11.12.13.0/24 RDP 3389
D. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

Correct Answer: B

QUESTION 330

When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is

A. OWASP is for web applications and OSSTMM does not include web applications.
B. OSSTMM is gray box testing and OWASP is black box testing.
C. OWASP addresses controls and OSSTMM does not.
D. OSSTMM addresses controls and OWASP does not.

Correct Answer: D

QUESTION 331

Which of the following is a protocol that is prone to a man-in-the-middle (MITM) attack and maps a 32-bit address to a 48-bit address?

A. ICPM
B. ARP
C. RARP
D. ICMP

Correct Answer: B

QUESTION 332

Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS?

A. Timing options to slow the speed that the port scan is conducted.
B. Fingerprinting to identify which operating systems are running on the network.
C. ICMP ping sweep to determine which hosts on the network are not available.
D. Traceroute to control the path of the packets sent during the scan.

Correct Answer: A

QUESTION 333

Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?

A. Cross-site scripting
B. SQL injection
C. Missing patches
D. CRLF injection

Correct Answer: C

QUESTION 334

Which type of access control is used on a router or firewall to limit network activity?

A. Mandatory
B. Discretionary
C. Rule-based
D. Role-based

Correct Answer: C

QUESTION 335

Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?

A. NMAP -PN -A -O -sS 192.168.2.0/24
B. NMAP -P0 -A -O -p1-65535 192.168.0/24
C. NMAP -P0 -A -sT -p0-65535 192.168.0/16
D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

Correct Answer: B

QUESTION 336
Which types of detection methods are employed by Network Intrusion Detection Systems (NIDS)? (Choose two.)

A. Signature
B. Anomaly
C. Passive
D. Reactive

Correct Answer: AB

QUESTION 337
The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

A. Multiple keys for non-repudiation of bulk data.
B. Different keys on both ends of the transport medium.
C. Bulk encryption for data transmission over fiber.
D. The same key on each end of the transmission medium.

Correct Answer: D

QUESTION 338
Which command lets a tester enumerate alive systems in a class C network via ICMP using native Windows tools?

A. ping 192.168.2.
B. ping 192.168.2.255
C. for %V in (1 1 255) do PING 192.168.2.%V
D. for /L %V in (1 1 254) do PING -n 1 192.168.2.%V | FIND /I "Reply"

Correct Answer: D

QUESTION 339
How can telnet be used to fingerprint a web server?

A. telnet webserverAddress 80

HEAD / HTTP/1.0

B. telnet webserverAddress 80
PUT / HTTP/1.0

C. telnet webserverAddress 80
HEAD / HTTP/2.0

D. telnet webserverAddress 80
PUT / HTTP/2.0

Correct Answer: A

QUESTION 340
Which of the following problems can be solved by using Wireshark?

A. Tracking version changes of source code.
B. Checking creation dates on all webpages on a server.
C. Resetting the administrator password on multiple systems.
D. Troubleshooting communication resets between two systems.

Correct Answer: D

QUESTION 341
Which of the following is an example of an asymmetric encryption implementation?

A. SHA1
B. PGP
C. 3DES
D. MD5

Correct Answer: B

QUESTION 342
What is the purpose of conducting security assessments on network resources?

A. Documentation
B. Validation
C. Implementation
D. Management