Correct Answer: B

QUESTION 343

A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

A. Information reporting
B. Vulnerability assessment
C. Active information gathering
D. Passive information gathering

Correct Answer: D

QUESTION 344

Which of the following is an application that requires a host application for replication?

A. Micro
B. Worm
C. Trojan
D. Virus

Correct Answer: D

QUESTION 345

Which of the following is a characteristic of Public Key Infrastructure (PKI)?

A. Public-key cryptosystems are faster than symmetric-key cryptosystems.
B. Public-key cryptosystems distribute public-keys within digital signatures.
C. Public-key cryptosystems do not require a secure key distribution channel.
D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

Correct Answer: B

QUESTION 346

What statement is true regarding LM hashes?

A. LM hashes consist in 48 hexadecimal characters.
B. LM hashes are based on AES128 cryptographic standard.

C. Uppercase characters in the password are converted to lowercase.
D. LM hashes are not generated when the password length exceeds 15 characters.

Correct Answer: D

QUESTION 347
What is a successful method for protecting a router from potential smurf attacks?

A. Placing the router in broadcast mode.
B. Enabling port forwarding on the router.
C. Installing the router outside of the network's firewall.
D. Disabling the router from accepting broadcast ping messages.

Correct Answer: D

QUESTION 348
Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?

A. NMAP
B. Metasploit
C. Nessus
D. BeEF

Correct Answer: C

QUESTION 349
The use of technologies like IPSec can help guarantee the following, authenticity, integrity, confidentiality and

A. non-repudiation
B. operability
C. security
D. usability

Correct Answer: A

QUESTION 350

A security administrator notices that the log file of the company`s webserver contains suspicious entries:

```
\[20/Mar/2011:10:49:07\] "GET /login.php?user=test'+oR+3>2%20-- HTTP/1.1" 200 9958
\[20/Mar/2011:10:51:02\] "GET /login.php?user=admin';%20-- HTTP/1.1" 200 9978
```

The administrator decides to further investigate and analyze the source code of login.php file:

```
php
include('../../config/db_connect.php');
$user = $_GET['user'];
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND password = '$pass'";
$result = mysql_query($sql) or die ("couldn't execute query");

if (mysql_num_rows($result) != 0 ) echo 'Authentication granted!';
else echo 'Authentication failed!';
?>
```

Based on source code analysis, the analyst concludes that the login.php script is vulnerable to

A. command injection
B. SQL injection
C. directory traversal
D. LDAP injection

Correct Answer: B

QUESTION 351

Which of the following is a detective control?

A. Smart card authentication
B. Security policy
C. Audit trail
D. Continuity of operations plan

Correct Answer: C

QUESTION 352

A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?

A. Spoofing an IP address
B. Tunneling scan over SSH
C. Tunneling over high port numbers
D. Scanning using fragmented IP packets

Correct Answer: B

QUESTION 353
A circuit level gateway works at which of the following layers of the OSI Model?

A. Layer 5 - Application
B. Layer 4 - TCP
C. Layer 3 - Internet protocol
D. Layer 2 - Data link

Correct Answer: B

QUESTION 354
Which of the following lists are valid data-gathering activities associated with a risk assessment?

A. Threat identification, vulnerability identification, control analysis.
B. Threat identification, response identification, mitigation identification.
C. Attack profile, defense profile, loss profile.
D. System profile, vulnerability identification, security determination.

Correct Answer: A

QUESTION 355
A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

A. Implementing server-side PKI certificates for all connections.
B. Mandating only client-side PKI certificates for all connections.
C. Requiring client and server PKI certificates for all connections.
D. Requiring strong authentication for all DNS queries.

Correct Answer: C

QUESTION 356
Which command line switch would be used in NMAP to perform operating system detection?

A. -OS
B. -sO
C. -sP
D. -O

Correct Answer: D

QUESTION 357
Bluetooth uses which digital modulation technique to exchange information between paired devices?

A. PSK (phase-shift keying)
B. FSK (frequency-shift keying)
C. ASK (amplitude-shift keying)
D. QAM (quadrature amplitude modulation)

Correct Answer: A

QUESTION 358
A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

A. Forensic attack
B. ARP spoofing attack
C. Social engineering attack
D. Scanning attack

Correct Answer: C

QUESTION 359
A security policy will be more accepted by employees if it is consistent and has the support of

A. coworkers
B. executive management
C. the security officer
D. a supervisor