Vendor:EC-COUNCIL

Exam Code:312-50V10

Exam Name: Certified Ethical Hacker Exam (C|EH v10)

Version: Demo

QUESTION 1

The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?

A. An extensible security framework named COBIT

B. A list of flaws and how to fix them

C. Web application patches

D. A security certification for hardened web applications

Correct Answer: B

QUESTION 2

Company XYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of Company XYZ. The employee of Company XYZ is aware of your test.

Your email message looks like this:

From: jim_miller@companyxyz.com

To: michelle_saunders@companyxyz.com

Subject: Test message

Date: 4/3/2017 14:37

The employee of Company XYZ receives your email message. This proves that Company XYZ\\'s email gateway doesn\\'t prevent what?

A. Email Phishing

B. Email Masquerading

C. Email Spoofing

D. Email Harvesting

Correct Answer: C

QUESTION 3

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 4

The practical realities facing organizations today make risk response strategies essential. Which of the following is NOT one of the five basic responses to risk?

A. Accept

B. Mitigate

C. Delegate

D. Avoid

Correct Answer: C

QUESTION 5

Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?

A. SHA-2

B. SHA-3

C. SHA-1

D. SHA-0

Correct Answer: C

QUESTION 6

What is the role of test automation in security testing?

A. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

B. It is an option but it tends to be very expensive.

C. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.

D. Test automation is not usable in security due to the complexity of the tests.

Correct Answer: A

QUESTION 7

Why should the security analyst disable/remove unnecessary ISAPI filters?

A. To defend against social engineering attacks

B. To defend against webserver attacks

C. To defend against jailbreaking

D. To defend against wireless attacks

Correct Answer: B

QUESTION 8

Study the following log extract and identify the attack.

```
12/26-07:0622:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13   TTL:50 TOS:0x0 IP:53476 DFF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E C0 AF 2E  GET /msadc/.....
2E 2F 2E 2E C0 AF 2E 2E 2F 2E 2E C0 AF 2E 2E 2F  ./....../....../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63  winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A  md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65  \ HTTP/1.1..Acce
70 74 3A 20 69 6D 61 67 65 2F 67 69 66 2C 20 69  pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20  mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67  image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61  e/pjpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65  tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D  l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69  sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70  on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70  oint, */*..Accep
74 2D 4C 61 6C 61 2F 34 2E 30 20 28 63 6F 6D 70  ozilla/age: en-v
73 0D 0A 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30  atible;pt-Encod2
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A  ng:Windows 95)..
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D  e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70  ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30  atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A  1; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72  Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69  ip.org..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A  on: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49  Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F  ONIDGQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E  HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46  IFIFB....APNIFIF
42 0D 0A 0D 0A 42 2E 2E 2E 2E                     B....
```

A. Hexcode Attack

B. Cross Site Scripting

C. Multiple Domain Traversal Attack

D. Unicode Directory Traversal Attack

Correct Answer: D

QUESTION 9

Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

A. The root CA is the recovery agent used to encrypt data when a user\\'s certificate is lost.

B. The root CA stores the user\\'s hash value for safekeeping.

C. The CA is the trusted root that issues certificates.

D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

Correct Answer: C

QUESTION 10

SOAP services use which technology to format information?

A. SATA

B. PCI

C. XML

D. ISDN

Correct Answer: C

QUESTION 11

When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

A. A bottom-up approach

B. A top-down approach

C. A senior creation approach

D. An IT assurance approach

Correct Answer: B

QUESTION 12

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

C. g++ -i hackersExploit.pl -o calc.exe

D. g++ --compile ? hackersExploit.cpp -o calc.exe

Correct Answer: A