Vendor:EC-COUNCIL

Exam Code:312-50V8

Exam Name: Certified Ethical Hacker v8

Version: Demo

QUESTION 1

Windows LAN Manager (LM) hashes are known to be weak.

Which of the following are known weaknesses of LM? (Choose three)

A. Converts passwords to uppercase.

B. Hashes are sent in clear text over the network.

C. Makes use of only 32 bit encryption.

D. Effective length is 7 characters.

Correct Answer: ABD

QUESTION 2

Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?

A. Fast processor to help with network traffic analysis

B. They must be dual-homed

C. Similar RAM requirements

D. Fast network interface cards

Correct Answer: B

QUESTION 3

Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

A. Cross-site scripting

B. SQL injection

C. VPath injection

D. XML denial of service issues

Correct Answer: D

QUESTION 4

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs.

Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

A. Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus

B. Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus

C. No. June can\\'t use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program

D. No. June can\\'t use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus

Correct Answer: C

QUESTION 5

Which of the following is assured by the use of a hash?

A. Availability

B. Confidentiality

C. Authentication

D. Integrity

Correct Answer: D

QUESTION 6

_____ will let you assume a users identity at a dynamically generated web page or site.

A. SQL attack

B. Injection attack

C. Cross site scripting

D. The shell attack

E. Winzapper

Correct Answer: C

QUESTION 7

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 8

Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

A. Kismet

B. Netstumbler

C. Abel

D. Nessus

Correct Answer: A

QUESTION 9

Which of the following buffer overflow exploits are related to Microsoft IIS web server? (Choose three)

A. Internet Printing Protocol (IPP) buffer overflow

B. Code Red Worm

C. Indexing services ISAPI extension buffer overflow

D. NeXT buffer overflow

Correct Answer: ABC

QUESTION 10

Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2e%2f%2e%2e%2f = ../../../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

A. Configure the Web Server to deny requests involving "hex encoded" characters

B. Create rules in IDS to alert on strange Unicode requests

C. Use SSL authentication on Web Servers

D. Enable Active Scripts Detection at the firewall and routers

Correct Answer: B

QUESTION 11

Which of the following tools are used for footprinting? (Choose four)

A. Sam Spade

B. NSLookup

C. Traceroute

D. Neotrace

E. Cheops

Correct Answer: ABCD

QUESTION 12

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