Free Questions for CPEH-001 by ebraindumps

Shared by Roy on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The Slammer Worm exploits a stack-based overflow that occurs in a DLL implementing the Resolution Service. Which of the following Database Server was targeted by the slammer worm?

Options:

A- Oracle

B- MSSQL

C- MySQL

D- Sybase

E- DB2

Answer:

B

Explanation:

W32.Slammer is a memory resident worm that propagates via UDP Port 1434 and exploits a vulnerability in SQL Server 2000 systems and systems with MSDE 2000 that have not applied the patch released by Microsoft Security Bulletin MS02-039.

Question 2

Question Type: MultipleChoice

Melissa is a virus that attacks Microsoft Windows platforms.

To which category does this virus belong?

Options:

A- Polymorphic

B- Boot Sector infector

C- System

D- Macro

Answer:

D

Explanation:

The Melissa macro virus propagates in the form of an email message containing an infected Word document as an attachment.

Question 3

Question Type: MultipleChoice

What is the best means of prevention against viruses?

Options:

A- Assign read only permission to all files on your system.

B- Remove any external devices such as floppy and USB connectors.

C- Install a rootkit detection tool.

D- Install and update anti-virus scanner.

Answer:

D

Explanation:

Although virus scanners only can find already known viruses this is still the best defense, together with users that are informed about risks with the internet.

Question 4

Question Type: MultipleChoice

What are the main drawbacks for anti-virus software?

Options:

A- AV software is difficult to keep up to the current revisions.

B- AV software can detect viruses but can take no action.

C- AV software is signature driven so new exploits are not detected.

D- It's relatively easy for an attacker to change the anatomy of an attack to bypass AV systems

E- AV software isn't available on all major operating systems platforms.

F- AV software is very machine (hardware) dependent.

Answer:

C

Explanation:

Although there are functions like heuristic scanning and sandbox technology, the Antivirus program is still mainly depending of signature databases and can only find already known viruses.

Question 5

Question Type: **MultipleChoice**

Virus Scrubbers and other malware detection program can only detect items that they are aware of. Which of the following tools would allow you to detect unauthorized changes or modifications of binary files on your system by unknown malware?

Options:

A- System integrity verification tools

B- Anti-Virus Software

C- A properly configured gateway

D- There is no way of finding out until a new updated signature file is released

Answer:

A

Explanation:

Programs like Tripwire aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.

Question 6

Question Type: **MultipleChoice**

Joe Hacker is going wardriving. He is going to use PrismStumbler and wants it to go to a GPS mapping software application. What is the recommended and well-known GPS mapping package that would interface with PrismStumbler?

Select the best answer.

Options:

A- GPSDrive

B- GPSMap

C- WinPcap

D- Microsoft Mappoint

Explanations:

GPSDrive is a Linux GPS mapping package. It recommended to be used to send PrismStumbler data to so that it can be mapped. GPSMap is a generic term and not a real software package. WinPcap is a packet capture library for Windows. It is used to capture packets and deliver them to other programs for analysis. As it is for Windows, it isn't going to do what Joe Hacker is wanting to do. Microsoft Mappoint is a Windows application. PrismStumbler is a Linux application. Thus, these two are not going to work well together.

Answer:

A

Question 7

Question Type: MultipleChoice

Sally is a network admin for a small company. She was asked to install wireless accesspoints in the building. In looking at the specifications for the access-points, she sees that all of them offer WEP. Which of these are true about WEP? Select the best answer.

Options:

A- Stands for Wireless Encryption Protocol

B- It makes a WLAN as secure as a LAN

C- Stands for Wired Equivalent Privacy

D- It offers end to end security

Explanations:

WEP is intended to make a WLAN as secure as a LAN but because a WLAN is not constrained by wired, this makes access much easier. Also, WEP has flaws that make it less secure than was once thought.WEP does not offer end-to-end security. It only attempts to protect the wireless portion of the network.

Answer:

C

Question 8

Question Type: **MultipleChoice**

Why do you need to capture five to ten million packets in order to crack WEP with AirSnort?

Options:

A- All IVs are vulnerable to attack

B- Air Snort uses a cache of packets

C- Air Snort implements the FMS attack and only encrypted packets are counted

D- A majority of weak IVs transmitted by access points and wireless cards are not filtered by contemporary wireless manufacturers

Answer:

C

Explanation:

Since the summer of 2001, WEP cracking has been a trivial but time consuming process. A few tools, AirSnort perhaps the most famous, that implement the Fluhrer-Mantin-Shamir (FMS) attack were released to the security community -- who until then were aware of the problems with WEP but did not have practical penetration testing tools. Although simple to use, these tools require a very large number of packets to be gathered before being able to crack a WEP key. The AirSnort web site estimates the total number of packets at five to ten million, but the number actually required may be higher than you think.

To Get Premium Files for CPEH-001 Visit

https://www.p2pexams.com/products/cpeh-001

For More Free Questions Visit

https://www.p2pexams.com/gaqm/pdf/cpeh-001

20%
DISCOUNT