98-367$^{\text{Q\&As}}$

Security Fundamentals

Pass Microsoft 98-367 Exam with 100% Guarantee

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

Which of the following viruses cannot be detected by signature-based antivirus?

A. Macro virus

B. Boot sector virus

C. MBR virus

D. Polymorphic virus

Correct Answer: D

A polymorphic virus has the ability to change its own signature at the time of infection. This virus is very complicated and hard to detect. When the user runs the infected file in the disk, it loads the virus into the RAM. The new virus starts making its own copies and infects other files of the operating system. The mutation engine of the polymorphic virus generates a new encrypted code, thus changing the signature of the virus. Therefore, polymorphic viruses cannot be detected by signature-based antivirus. Answer: A is incorrect. A macro virus is a virus that consists of a macro code which infects the system. A Macro virus can infect a system rapidly. Since this virus has VB event handlers, it is dynamic in nature and displays random activation. The victim has only to open a file having a macro virus in order to infect the system with the virus. DMV, Nuclear, and Word Concept are some good examples of macro viruses. Answer: C is incorrect. A Master boot record (MBR) virus replaces the boot sector data with its own malicious code. Every time when the computer starts up, the boot sector virus executes. It can then generate activity that is either annoying (system will play sounds at certain times) or destructive (erase the hard drive of the system). Because the code in the Master Boot Record executes before any operating system is started, no operating system can detect or recover from corruption of the Master Boot Record. Answer: B is incorrect. A boot sector virus infects the master boot files of the hard disk or floppy disk. Boot record programs are responsible for booting the operating system and the boot sector virus copies these programs into another part of the hard disk or overwrites these files. Therefore, when the floppy or the hard disk boots, the virus infects the computer.

QUESTION 2

Creating MD5 hash for files is an example of ensuring what?

A. Confidentiality

B. Availability

C. Least privilege

D. Integrity

Correct Answer: D

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

QUESTION 3

Which of the following is an authentication protocol?

A. Kerberos

B. LDAP

C. TLS

D. PPTP

Correct Answer: A

Kerberos is an industry standard authentication protocol used to verify user or host identity. Kerberos v5 authentication protocol is the default authentication service for Windows 2000. It is integrated into the administrative and security model,

and provides secure communication between Windows 2000 Server domains and clients.

Answer: C is incorrect. Transport Layer Security (TLS) is an application layer protocol that uses a combination of public and symmetric key processing to encrypt data.

Answer: B is incorrect. Lightweight Directory Access Protocol (LDAP) is a protocol used to query and modify information stored within directory services. Answer: D is incorrect. Point-to-Point Tunneling Protocol (PPTP) is a method for

implementing virtual private networks. PPTP does not provide confidentiality or encryption. It relies on the protocol being tunneled to provide privacy. It is used to provide secure, low-cost remote access to corporate networks through public

networks such as the Internet. Using PPTP, remote users can use PPP- enabled client computers to dial a local ISP and connect securely to the corporate network through the Internet. PPTP has been made obsolete by Layer 2 Tunneling

Protocol (L2TP) and IPSec.

QUESTION 4

You are trying to connect to an FTP server on the Internet from a computer in a school lab. You cannot get a connection. You try on another computer with the same results. The computers in the lab are able to browse the Internet.

You are able to connect to this FTP server from home.

What could be blocking the connection to the server?

A. A layer-2 switch

B. A wireless access point

C. A firewall

D. A layer-2 hub

Correct Answer: C

QUESTION 5

Malicious software designed to collect personally identifiable information is referred to as :

A. spyware

B. a cookie

C. a network sniffer

D. freeware

Correct Answer: A