C.   Anti-virus software is usable to remove the viral code.

D.   These viruses almost exclusively affect the operating system.

Correct Answer: D

QUESTION 516

What is the term used to describe a virus that can infect both program files and boot sectors?

A.   Polymorphic

B.   Multipartite

C.   Stealth

D.   Multiple encrypting

Correct Answer: B

QUESTION 517

Why are macro viruses easy to write?

A.   Active contents controls can make direct system calls

B.   The underlying language is simple and intuitive to apply.

C.   Only a few assembler instructions are needed to do damage.

D.   Office templates are fully API compliant.

Correct Answer: B

QUESTION 518

Which one of the following traits allows macro viruses to spread more effectively than other types?

A.   They infect macro systems as well as micro computers.

B.   They attach to executable and batch applications.

C.   They can be transported between different operating systems.

D.   They spread in distributed systems without detection.

Correct Answer: C

QUESTION 519

In what way could Java applets pose a security threat?

A. Their transport can interrupt the secure distribution of World Wide Web pages over the Internet by removing SSL and S-HTTP.
B. Java interpreters do not provide the ability to limit system access that an applet could have on a client system.
C. Executables from the Internet may attempt an intentional attack when they are downloaded on a client system.
D. Java does not check the bytecode at runtime or provide other safety mechanisms for program isolation from the client system.

Correct Answer: C

QUESTION 520

What setup should an administrator use for regularly testing the strength of user passwords?

A. A networked workstation so that the live password database can easily be accessed by the cracking program
B. A networked workstation so the password database can easily be copied locally and processed by the cracking program
C. A standalone workstation on which the password database is copied and processed by the cracking program
D. A password-cracking program is unethical; therefore it should not be used.

Correct Answer: C

QUESTION 521

On UNIX systems, passwords shall be kept:

A. In any location on behalf of root.
B. In a shadow password file.
C. In the /etc/passwd file.
D. In root.

Correct Answer: B

QUESTION 522

Which of the following would constitute the best example of a password to use for access to a system by a network administrator?

A. holiday
B. Christmas12
C. Jenny&30
D. TrZc&45g

Correct Answer: D

QUESTION 523

Which of the following is not a media viability control used to protect the viability of data storage media?

A. clearing
B. marking
C. handling
D. storage

Correct Answer: A

QUESTION 524

Which of the following refers to the data left on the media after the media has been erased?

A. remanence
B. recovery
C. sticky bits
D. semi-hidden

Correct Answer: A

QUESTION 525

What is the main issue with media reuse?

A. Degaussing
B. Data remanence
C. Media destruction
D. Purging

Correct Answer: B

QUESTION 526

What should a company do first when disposing of personal computers that once were used to store confidential data?

A. Overwrite all data on the hard disk with zeroes.
B. Delete all data contained on the hard disk.
C. Demagnetize the hard disk.
D. Low level format the hard disk.

Correct Answer: C

QUESTION 527

Which of the following is not a critical security aspect of Operations Controls?

A. Controls over hardware
B. data media used
C. Operations using resources
D. Environment controls

Correct Answer: D

QUESTION 528

What tool is being used to determine whether attackers have altered system files of executables?

A. File Integrity Checker
B. Vulnerability Analysis Systems
C. Honey Pots
D. Padded Cells

Correct Answer: A

QUESTION 529

A system file that has been patched numerous times becomes infected with a virus. The anti-virus software warns that disinfecting the file can damage it. What course of action should be taken?

A. Replace the file with the original version from master media.
B. Proceed with automated disinfection.
C. Research the virus to see if it is benign.
D. Restore an uninfected version of the patched file from backup media.

Correct Answer: A

QUESTION 530

In an on-line transaction processing system, which of the following actions should be taken when erroneous or invalid transactions are detected?

A. The transactions should be dropped from processing.
B. The transactions should be processed after the program makes adjustments.
C. The transactions should be written to a report and reviewed.
D. The transactions should be corrected and reprocessed.

Correct Answer: C

QUESTION 531

Which of the following is a reasonable response from the intrusion detection system when it detects Internet Protocol (IP) packets where the IP source address is the same as the IP destination address?

A. Allow the packet to be processed by the network and record the event.
B. Record selected information about the item and delete the packet.
C. Resolve the destination address and process the packet.
D. Translate the source address and resend the packet.

Correct Answer: B

QUESTION 532

Which of the following is not a good response to a detected intrusion?

A. Collect additional information about the suspected attack.
B. Inject TCP reset packets into the attacker's connection to the victim system.
C. Reconfigure routers and firewalls to block packets from the attacker's apparent connection.
D. Launch attacks or attempt to actively gain information about the attacker's host.

Correct Answer: D

QUESTION 533

Once an intrusion into your organizations information system has been detected, which of the following actions should be performed first?

A. Eliminate all means of intruder access.