SolveMyQues
Test your skills online

Sample Questions with Answers

Cybersecurity - Penetration Testing

Generated on June 17, 2026 at 12:35 PM

Cybersecurity

[NOTE] Important Note: This PDF contains sample questions with complete answers and explanations. **Visit SolveMyQues.com** for our complete question bank, interactive tests, and detailed performance tracking!

Question 1:

What is a computer virus?

[ANSWER] Answer & Explanation:

A computer virus is a software program that has been intentionally created to cause a user grief, spread to other computers, or destroy data on an individual's computer. To help prevent a computer from becoming infected by a virus, software developers have developed antivirus programs that stay active on the computer helping to protect it. It is important to realize that many computers do not come pre-loaded with these already installed and that if computers do come with these programs, the programs may expire within 90 days.

Question 2:

Information on Excel/Laroux virus.

[ANSWER] Answer & Explanation:

Excel Macro/Laroux consists of two macros, auto_open and check_files.The auto_open macro executes whenever an infected Spreadsheet is opened, followed by the check_files macro that determines the startup path of Excel. If there is no file named PERSONAL.XLS in the startup path, the virus creates one. This file contains a module called "Laroux."PERSONAL.XLS is the default filename for any macros recorded under Excel. Thus, you might have PERSONAL.XLS on your system even though you are not infected by this virus. The startup path is by default set as \MSOffice\EXCEL\XLSTART, but it can be changed from Excel's Tools/Options/General/Alternate Startup File menu option.If an infected workbook resides on a write-protected floppy, an error will occur when Excel tries to open it and the virus will not be able to replicate. Excel Macro/Laroux is not intentionally destructive and contains no payload; it just replicates, so most likely will not harm Office97.

Question 3:

Information on the Alive.3400 virus.

[ANSWER] Answer & Explanation:

We unfortunately have not heard of this virus; however, it could be a different version of a previous version of alive, alive.2340, which is a Polymorphic memory virus. A Polymorphic virus has a capability of being hundreds of different viruses by modifying its own code to prevent it from being detected, and this could be what the alive.3400 could be. It is recommended that you get the latest version of a Virus protection program to protect you and hopefully clean your computer.

Question 4:

Information about the Stoned Empire monkey virus.

[ANSWER] Answer & Explanation:

About Stoned Empire Monkey virusThe Monkey virus was first discovered in Edmonton, Canada, in the year 1991. The virus spread quickly to USA, Australia and UK and is now one of the most common boot sector viruses.As the name indicates, Monkey is a distant relative of Stoned. Its technical properties make it quite a remarkable virus, however the virus infects the Master Boot Records of hard disks and the DOS boot records of diskettes, just like Stoned. Monkey spreads only through diskettes.Monkey does not let the original partition table remain in its proper place in the Master Boot Record, as Stoned does. Instead it moves the whole Master Boot Record to the hard disk's third sector, and replaces it with its own code. The hard disk is inaccessible after a diskette boot, since the operating system cannot find valid partition data in the Master Boot Record - attempts to use the hard disk result in the DOS error message Invalid drive specification.When the computer is booted from the hard disk, the virus is executed first, and the hard disk can thereafter be used normally. The virus is not, therefore, easily noticeable, unless the computer is booted from a diskette.The fact that Monkey encrypts the Master Boot Record besides relocating it on the disk makes the virus still more difficult to remove. The changes to the Master Boot Record cannot be detected while the virus is active, since it reroutes the BIOS-level disk calls through its own code. Upon inspection, the hard disk seems to be in its original shape.Detecting the virusIt is difficult to spot the virus, since it does not activate in any way. A one-kilobyte reduction in DOS memory is the only obvious sign of its presence. The memory can be checked MS- DOS's CHKDSK and MEM programs. However, even if MEM reports that the computer has 639 kilobytes of basic memory instead of the more common 640 kilobytes, it does not necessarily mean that the computer is infected. In many computers, the BIOS allocates one kilobyte of basic memory for its own use.The Monkey virus is quite compatible with different diskette types. It carries a table containing data for the most common diskettes. Using this table, the virus is able to move a diskette's original boot record and a part of its own code to a safe area on the diskette. Monkey does not recognize 2.88 megabyte ED diskettes; however, and partly overwrites their File Allocation Tables. Some revisions can be spotted by running fdisk and displaying the partition information; if you see % # or any other strange characters as the partition, label, etc, it's a good possibility that you may have the virus.Information about removalThe relocation and encryption of the partition table render two often-used methods of removing a MBR Virus unviable. One of these is the MS-DOS command FDISK /MBR, capable of removing most viruses that infect Master Boot Records. The other is using a disk editor to restore the Master Boot Record back on the zero track. Although both of these procedures destroy the actual virus code, the computer cannot be booted from the hard disk afterwards.There are six different ways to remove the Monkey virus: Purchase a Virus protection utility and have it clean the Virus. While not all virus protection programs are capable of removing this virus, additional add-ons can be installed allowing the virus protection utility to remove the virus. The original Master Boot Record and partition table can be restored from a backup taken before the infection. Such a backup can be made by using, for example, the MIRROR /PARTN command of MS-DOS The hard disk can be repartitioned by using the FDISK program and then the logical disks must be formatted. All data on the hard disk will consequently be lost, however. The virus code can be overwritten by using FDISK /MBR, and the partition table restored manually. In this case, the partition values of the hard disk must be calculated and inserted in the partition table with the help of a disk editor. The method requires expert knowledge of the disk structure, and its success is doubtful. Usually, this causes the current partitions to double, causing more havoc. It is possible to exploit Monkey's stealth capabilities by taking a copy of the zero track while the virus is active. Since the virus hides the changes it has made, this copy will contain the original Master Boot Record. This method is not recommended, because the diskettes used in the copying may well get infected. The original zero track can be located, decrypted and moved back to its proper place. As a result, the hard disk is restored to its exact original state. Some virus scanners have this capability, and can successfully remove the virus.

Question 5:

Information on the E-Morph virus.

[ANSWER] Answer & Explanation:

The E-morph virus that is labeled as E-Morph, E-Morph-1696 and E-Morph 1696, infects MS-DOS .COM files, and currently is not known to be a widely spread virus.The virus is 1696 bytes long and is memory resident. The virus is not capable of infecting floppy disks nor is it able to infect the hard drive boot record, and it is not encrypted in any way. E-Morph is not a destructive virus and can usually be removed by major virus scanners.