



98-367

MTA Security Fundamentals

Document version: 1 .04 .11

Important Note About 98-367 PDF

techeXams' **98-367 PDF** is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this exam questions. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. It's our guarantee.

Copyright

techeXams holds the copyright of this material. techeXams grants you a limited license to view and study this material, either for personal or commercial use. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

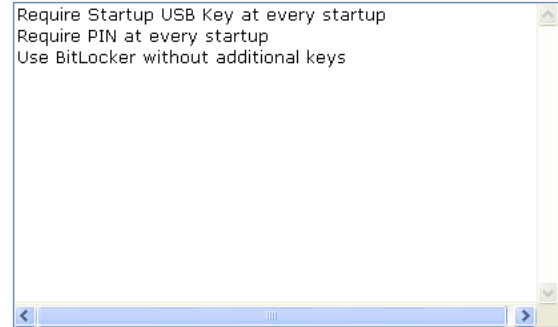
Question: 1

You have bought a Windows Vista Enterprise Edition computer. You want to enable BitLocker encryption through the Control Panel. In the Startup Preference dialog box, choose the startup options that can be selected if the computer has a built-in TPM chip.

Startup options that support TPM

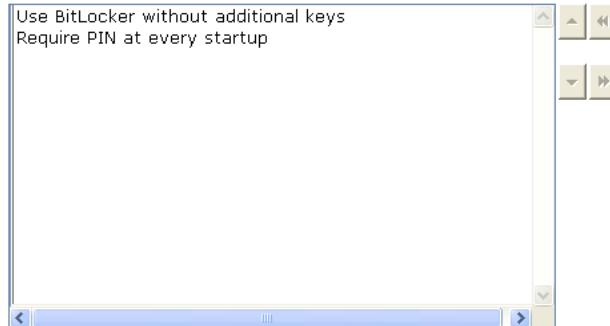


Startup options in BitLocker



Answer:

Startup options that support TPM



Startup options in BitLocker



Explanation:

You can select either the Use BitLocker Without Additional Keys or Require PIN at Every Startup option to enable BitLocker encryption. The Use BitLocker without additional keys option uses the TPM to verify the integrity of the operating system at every startup. If you choose this option, the user will not be prompted during startup. It provides complete transparent protection. The Require PIN at every startup option also uses TPM to verify the integrity of the operating system at every startup and requires a user to enter a PIN to verify the user's identity. This option provides additional protection, as it also verifies the user.

Question: 2

Which of the following is a process in which data is changed before or while it is entered into a computer system?

- A. Data diddling
- B. Authentication
- C. Domain kiting
- D. Packet sniffing

Answer: A

Explanation:

Data diddling is a process in which data is changed before or while it is entered into a computer system. A malicious code or virus can perform data diddling. For example, a virus can be written to intercept keyboard input. The virus displays the appropriate characters on the computer screen so that the user does not know the actual problem. Answer: C is incorrect. Domain kiting is a process whereby a user registers a domain (usually one with a prominent sounding name likely to attract significant traffic), and on that domain, he puts up a page with a lot of click through ads (the ads that pay the owner of the Web site for all clicks). During this process, the user who registered the domain cancels it before the normal grace period is over and then re-registers it again. This process is repeated any number of times with the end result of having the domain registered without ever actually paying for it. Answer: B is incorrect. Authentication is a process of verifying the identity of a person, network host, or system process. The authentication process compares the provided credentials with the credentials stored in the database of an authentication server. Answer: D is incorrect. Packet sniffing is a process of monitoring data packets that travel across a network. The software used for packet sniffing is known as sniffers. There are many packet-sniffing programs that are available on the Internet. Some of these are unauthorized, which can be harmful for a network's security.

Question: 3

Which of the following contains a tree of domain names?

- A. Domain name space
- B. Domain name formulation
- C. Domain Name System
- D. Authoritative name server

Answer: A

Explanation:

Domain name space consists of a tree of domain names. Each node or leaf in the tree has zero or more resource records, which hold information associated with the domain name. The tree subdivides into zones starting at the root zone. Answer: B is incorrect. The definitive descriptions of the rules for forming domain names appear in RFC 1035, RFC 1123, and RFC 2181. A domain name consists of one or more parts, technically called labels that are conventionally concatenated, and delimited by dots.

Answer: C is incorrect. Domain Name System (DNS) is a distributed hierarchical naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participants. Answer: D is incorrect. An authoritative name server is a name server that gives answers that have been configured by an original source, for example, the domain administrator or by dynamic DNS methods, in contrast to the answers that were obtained via a regular DNS query to one more name server. An authoritative-only name server only returns answers to the queries about domain names that have been specifically configured by the administrator.

Question: 4

Mark works as a Systems Administrator for TechMart Incl. The company has Windows-based network. Mark has been assigned a project to track who tries to log into the system and the time of the day at which the attempts occur. He is also required to create a system to track when confidential files are opened and who is trying to open it. Now, Mark logs when someone is not able to make a successful attempt to log into the system as Administrator but he also wants to log when the user is successful to log into the system as Administrator. Which of the following is the reason of logging by Mark when a user is successfully logged into the system as well as when he is failed?

- A. To determine if and when someone is authenticating successfully with high privilege.
- B. To make sure that user is not using the Administrator account.
- C. To determine if and when someone is authenticating successfully with high privilege.
- D. To make sure that user is not facing any problem.

Answer: C**Explanation:**

In the above scenario, Mark is required to determine if and when someone is able to be authenticated successfully with high privilege as well as the hacker activity. If any user was failed for

a number of times and was then successful any attempt, it can be a hacker activity. That's why Mark logs when a user is successfully logged into the system as well as when he is failed.

Question: 5

Mark works as a Systems Administrator for TechMart Inc. The company has a Windows-based network. The company is adding an open, high-speed, wireless access for their customers and secured wireless for employees at all 37 branches. He wants to check the various security concerns for ensuring that business traffic is secured. He is also in under pressure to make this new feature a winning strategy for a company. Mark wants the employees to be free to troubleshoot their own wireless connections before contacting him. Which of the following is the basic troubleshooting step that he can ask them to do?

- A. To power cycle the wireless access points and then reboot the systems.
- B. To configure the network to use only Extensible Authentication Protocol (EAP).
- C. To reboot the computers they are using and then use the MAC filtering.
- D. To right-click the network icon in the system tray and then select Troubleshoot Problems.

Answer: D**Explanation:**

The basic troubleshooting step that Mark can ask his employees is to right-click the network icon in the system tray and then select Troubleshoot Problems. Answer: B is incorrect. Extensible Authentication Protocol (EAP) is defined as an authentication framework providing for the transport and usage of keying material and parameters that are generated by EAP methods. EAP is not a wire protocol and it defines only message formats.

Question: 6

Which of the following protects against unauthorized access to confidential information via encryption and works at the network layer?

- A. Firewall
- B. NAT
- C. IPSec
- D. MAC address

Answer: C

Explanation:

Internet Protocol security (IPSec) protects against data manipulation and unauthorized access to confidential information via encryption and works at the network layer. IPSec provides machine-level authentication as well as data encryption. It is used for VPN connections that use the L2TP protocol. It secures both data and password. Answer: B is incorrect. NAT also works at the network layer, but it does not provide encryption for data.

Question: 7

You want to standardize security throughout your network. You primarily use Microsoft operating systems for servers and workstations. What is the best way to have standardized security (i.e. same password policies, lockout policies, etc.) throughout the network on clients and servers?

- A. Publish the desired policies to all employees directing them to implement according to policy.
- B. Configure each computer to adhere to the standard policies.
- C. When installing new workstations or servers, image a machine that has proper security settings and install the new machine with that image.
- D. Utilize Windows Security Templates for all computers.

Answer: D

Explanation:

Windows templates are a method for setting security policies in a template, then applying that template to multiple computers. Answer: C is incorrect. This would only work for new computers and will not help you with existing computers on your network. Answer: A is incorrect. Asking employees to implement security policies will usually result in an uneven application of the policies. Some employees will get them properly implemented, some won't. Answer: B is incorrect. While this would work, it would be very labor intensive and is not the recommended method.

Question: 8

Mark works as a Network Administrator for Blue Well Inc. The company has a Windows-based network. Mark is facing a series of problems with email spam and identifying theft via phishing scams. He wants to implement the various security measures and to provide some education because it is related to the best practices while using email. Which of the following will Mark ask to employees of his company to do when they receive an email from a company they know with a request to click the link to "verify their account information"?

- A. Provide the required information
- B. Hide the email
- C. Use Read-only Domain Controller
- D. Delete the email

Answer: D

Explanation:

In the above scenario, Mark will ask his employees to delete the email whenever he receives an email from a company that they know with to click the link to "verify their account information", because companies do not ask for account information via email now a days. Answer: C is incorrect. Read-only Domain Controller (RODC) is a domain controller that hosts the read-only partition of the Active Directory database. RODC was developed by Microsoft typically to be deployed in a branch office environment. RODC is a good option to enhance security by placing it in a location where physical security is poor. RODC can also be placed at locations having relatively few users and a poor network bandwidth to the main site. As only the read-only partition of the Active Directory database is hosted by RODC, a little local IT knowledge is required to maintain it.

Question: 9

Which of the following infects the computer and then hides itself from detection by antivirus software?

- A. EICAR virus
- B. Boot-sector virus
- C. Macro virus
- D. Stealth virus

Answer: D

Explanation:

A stealth virus is a file virus. It infects the computer and then hides itself from detection by antivirus software. It uses various mechanisms to avoid detection by antivirus software. It hides itself in computer memory after infecting the computer. It also masks itself from applications or utilities. It uses various tricks to appear that the computer has not lost any memory and the file size has not been changed. The virus may save a copy of original and uninfected data. When the anti-virus program tries to check the files that have been affected, the virus shows only the uninfected data. This virus generally infects .COM and .EXE files. 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. Answer: C 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: A is incorrect. The EICAR (EICAR Standard Anti-Virus Test File) virus is a file that is used to test the response of computer antivirus (AV) programs. The rationale behind it is to allow people, companies, and antivirus programmers to test their software without having to use a real computer virus that could cause actual damage should the antivirus not respond correctly. The file is simply a text file of either 68 or 70 bytes that is a legitimate executable file called a COM file that can be run by Microsoft operating systems and some work-alikes (except for 64-bit due to 16-bit limitations), including OS/2. When executed, it will print "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!" and then stop. The string used in the EICAR virus is as follows:

Question: 10

Which of the following states that a user should never be given more privileges than are required to carry out a task?

- A. Security through obscurity
- B. Segregation of duties
- C. Principle of least privilege
- D. Role-based security

Answer: C**Explanation:**

The principle of least privilege states that a user should never be given more privileges than are required to carry out a task. The user should not be logged on as an administrator, if the user is not

doing administrative work on a computer. The administrator account should be used for performing tasks, such as changing system time, installing software, or creating standard accounts. Answer: D is incorrect. Role-based security provided by the .NET Framework allows, grants, or denies access to resources based on a Windows user's identity. It is built on the principle that the user is authenticated and can be authorized or assigned roles and permissions. Answer: B is incorrect. Segregation of duties is used to determine whether decision-making, executive tasks, or control tasks are carried out by a person to avoid unauthorized or unintended changes or the misuse of the organization's assets. Whether the person needs access to information can also be determined. The risk of information being intentionally or unintentionally used, altered, or destroyed is increased by unnecessary access. It is called the 'need to know' principle. Answer: A is incorrect. Security through obscurity is a principle in security engineering, which attempts to use secrecy (of design, implementation, etc.) to provide security. A system relying on security through obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe that the flaws are not known, and that attackers are unlikely to find them.

Question: 11

Which of the following are the major components of the IPsec protocol? Each correct answer represents a complete solution. Choose all that apply.

- A. Encapsulating Security Payload (ESP)
- B. Authentication Header (AH)
- C. Internet Encryption Key (IEK)
- D. Internet Key Exchange (IKE)

Answer: B, A, and D**Explanation:**

The IPsec protocol has three major components: 1.Authentication Header (AH) 2.Encapsulating Security Payload (ESP) 3.Internet Key Exchange (IKE) Answer: C is incorrect. There is no such component of the IPsec protocol as Internet Encryption Key.

Question: 12

Which of following is required to be configured to ensure that the BitLocker storage can be reclaimed?

- A. BitLocker to use data recovery agents

- B. BitLocker to use the password screen saver
- C. BitLocker to use the Secret Retrieval Agent
- D. BitLocker to use the Artificial Intelligence recovery option.

Answer: A

Explanation:

BitLocker to use data recovery agents is created and properly stored to ensure that the secured data can be reclaimed when the Bitlocker protected storage is shifted to another computer.

Question: 13

The stronger password is a critical element in the security plan. Which of the following are the characteristics used to make up a strong password?

- A. It contains more than seven hundred characters and does not contain the user name, real name, or any name that can be guessed by the attacker easily.
- B. It contains more than seven characters and does not contain the user name, real name, or anyname that can be guessed by the attacker easily.
- C. It contains the user name, real name, or any name that can be remembered easily and does not contain more than seven characters.
- D. It contains more than seven characters and the user name, real name, or any name.

Answer: B

Explanation:

A strong password contains more than seven characters and does not contain the user name, real name, or any name that can be guessed by the attacker easily.

Question: 14

Which of the following can be installed and configured to prevent suspicious emails from entering the user's network?

- A. Kerberos
- B. Single sign-on (SSO)

- C. TCP/IP protocol
- D. Microsoft Forefront and Threat Management Gateway

Answer: D

Explanation:

To prevent suspicious emails from entering the network, it is required to install Microsoft Forefront and Threat Management Gateway and configure it so that it can block any malicious emails. Exchange server has many spam filtering tools but Forefront and TMG are additional security measures used for enhancing the protection of the system. Answer: B is incorrect. Single sign-on (SSO) is defined as a mechanism in which a single action of user authentication and authorization is used to allow a user to access all computers and systems where he got a access permission, without entering passwords for multiple times. Answer: A is incorrect. Kerberos is defined as a secure method used for authenticating a request for a service in a computer network. Answer: C is incorrect. TCP/IP protocol is used to define the rule computers are required to follow for communicating with each other over the internet.

Question: 15

Which of the following are types of password policies of Windows 7? Each correct answer represents a complete solution. Choose all that apply.

- A. Store Password Using Reversible Encryption
- B. Minimum Password Length
- C. User Name Length
- D. Password Must Meet Complexity Requirements

Answer: B, A, and D

Explanation:

Password policies are account policies that are related to user accounts. These policies increase the effectiveness of users' passwords by enforcing different types of controls on their usage. In Windows 7, there are following six types of password policies that can be configured by administrators:

Enforce Password History

Maximum Password Age Minimum Password Age Minimum Password Length Password Must Meet Complexity Requirements Store Password Using Reversible Encryption These options are disabled by default. However, an administrator can enable any option in the Local Security Settings tool, which

can be accessed from the Administrative tools window found under Control Panel. Answer: C is incorrect. User name length does not come under password policies.

Question: 16

Which of the following is a technique used to attack an Ethernet wired or wireless network?

- A. ARP poisoning
- B. DNS poisoning
- C. Mail bombing
- D. Keystroke logging

Answer: A**Explanation:**

Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The attack can only be used on networks that actually make use of ARP and not another method of address resolution. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN. Generally, the aim is to associate the attacker's MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly sent to the attacker instead. The attacker could then choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it. ARP spoofing attacks can be run from a compromised host, or from an attacker's machine that is connected directly to the target Ethernet segment. Answer: C is incorrect. Mail bombing is an attack that is used to overwhelm mail servers and clients by sending a large number of unwanted e-mails. The aim of this type of attack is to completely fill the recipient's hard disk with immense, useless files, causing at best irritation, and at worst total computer failure. E-mail filtering and properly configuring email relay functionality on mail servers can be helpful for protection against this type of attack. Answer: B is incorrect. DNS poisoning is the process in which a DNS server may return an incorrect IP address, diverting traffic to another computer. Answer: D is incorrect. Keystroke logging is a method of logging and recording user keystrokes. It can be performed with software or hardware devices. Keystroke logging devices can record everything a person types using his keyboard, such as to measure employee's productivity on certain clerical tasks. These types of devices can also be used to get usernames, passwords, etc.

Question: 17

You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. You want to configure Network Access Protection (NAP) on your network. You want that the clients connecting to the network must contain certain configurations. Which of the following Windows components ensure that only clients having certain health benchmarks access the network resources? Each correct answer represents a part of the solution. Choose two.

- A. Windows Firewall
- B. System Health Agents (SHA)
- C. Terminal Service
- D. System Health Validators (SHV)
- E. TS Gateway

Answer: B and D

Explanation:

The System Health Agents (SHA) and System Health Validators (SHV) are the components of Windows Server 2008 to validate a computer's health against a configured set of security benchmarks. These components are parts of Network Access Protection deployed on a network. The SHV component specifies which benchmarks the client must meet. The SHA component specifies configuration against those benchmarks that are being tested. They ensure that computers accessing resources on the network meet certain client health benchmarks. Answer: A is incorrect. Windows firewall is used to prevent network from unauthorized access. It can be one of the benchmarks configured for health checkup. Answer: E and C are incorrect. TS Gateway and Terminal Service are not used to enforce configurations specified in the

Question: 18

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows 2008 Active Directory-based network. All client computers on the network run Windows Vista Ultimate. You have configured a Dynamic DNS (DDNS) on the network. There are a lot of mobile users who often connect to and disconnect from the network. Users on the network complain of slow network responses. You suspect that the stale records on the DNS server may be the cause of the issue. You want to remove the stale records. Which of the following technologies will you use to accomplish the task?

- A. RODC

- B. Aging
- C. Scavenging
- D. Forwarding

Answer: C

Get Full Version of Exam 98-367 PDF Q&A

techeXams presents authentic, genuine and valid study material, which promise 100% success in very first attempt. To take optimal results for 98-367 exam, you need to buy full version of 98-367 question and answer. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. So come join us and quench your thirst for knowledge.

Get complete 98-367 questions and answers by visiting URL

["http://www.techexams.ws/exams/98-367.do"](http://www.techexams.ws/exams/98-367.do)