http://www.ipass4sure.com

98-367

Microsoft

Security Fundamentals

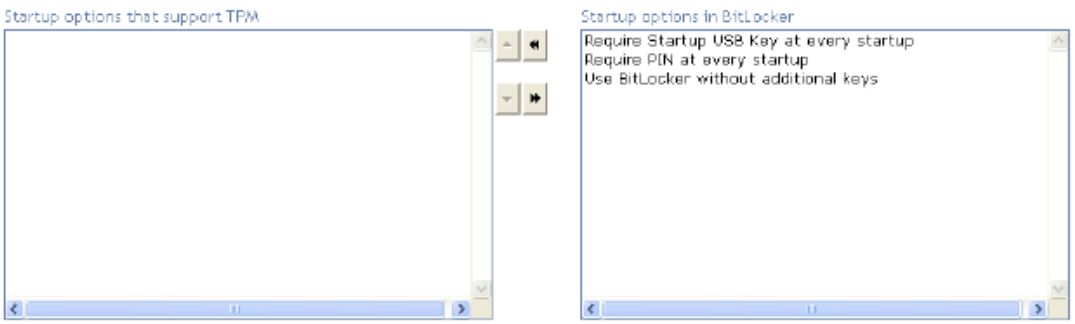
The 98-367 practice exam is written and formatted by Certified Senior IT Professionals working in today's prospering companies and data centers all over the world! The 98-367 Practice Test covers all the exam topics and objectives and will prepare you for success quickly and efficiently.
The 98-367 exam is very challenging, but with our 98-367 questions and answers practice exam, you can feel confident in obtaining your success on the 98-367 exam on your FIRST TRY!

Microsoft 98-367 Exam Features

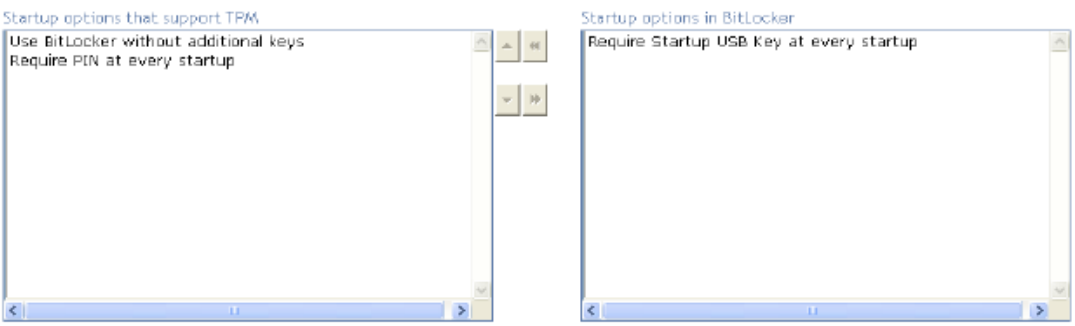
- Detailed questions and answers for 98-367 exam
- Try a demo before buying any Microsoft exam
- 98-367 questions and answers, updated regularly
- Verified 98-367 answers by Experts and bear almost 100% accuracy
- 98-367 tested and verified before publishing
- 98-367 exam questions with exhibits
- 98-367 same questions as real exam with multiple choice options

Acquiring Microsoft certifications are becoming a huge task in the field of I.T. More over these exams like 98-367 exam are now continuously updating and accepting this challenge is itself a task. This 98-367 test is an important part of Microsoft certifications. We have the resources to prepare you for this. The 98-367 exam is essential and core part of Microsoft certifications and once you clear the exam you will be able to solve the real life problems yourself.Want to take advantage of the Real 98-367 Test and save time and money while developing your skills to pass your Microsoft 98-367 Exam? Let us help you climb that ladder of success and pass your 98-367 now!

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.



Answer:



Explanation:
You can select either the Use BitLocker Without Additional Keysor 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 sub- divides 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 fot 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.

Pass4sure Certification Exam Features;

- Pass4sure offers over **2500** Certification exams for professionals.
- More than **98,800** Satisfied Customers Worldwide.
- Average **99.8%** Success Rate.
- Over **120** Global Certification Vendors Covered.
- Services of Professional & Certified Experts available via support.
- Free 90 days updates to match real exam scenarios.
- Instant Download Access! No Setup required.
- Price as low as $19, which is 80% more cost effective than others.
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions / Answers are downloadable in **PDF** format.
- Mobile Device Supported (Android, iPhone, iPod, iPad)
- **No authorization** code required to open exam.
- **Portable** anywhere.
- ***Guaranteed Success***.
- **Fast**, helpful support 24x7.

View list of All certification exams offered;
http://www.ipass4sure.com/allexams.asp

View list of All Study Guides (SG);
http://www.ipass4sure.com/study-guides.asp

View list of All Audio Exams (AE);
http://www.ipass4sure.com/audio-exams.asp

Download Any Certication Exam DEMO.
http://www.ipass4sure.com/samples.asp

To purchase Full version of exam click below;
http://www.ipass4sure.com/allexams.asp

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google	

and many others.. See complete list Here