Exambible 98-367V8.02_formatted

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

98-367:

MTA Security Fundamentals

Practice Test

Version:

V8.02
About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study

materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+,

Network+ certification practice exams and so on. We guarantee that the candidates will not only pass

any IT exam at the first attempt but also get profound understanding about the certificates they have

got.

There are so many alike companies in this industry, however, Exambible has its unique

advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

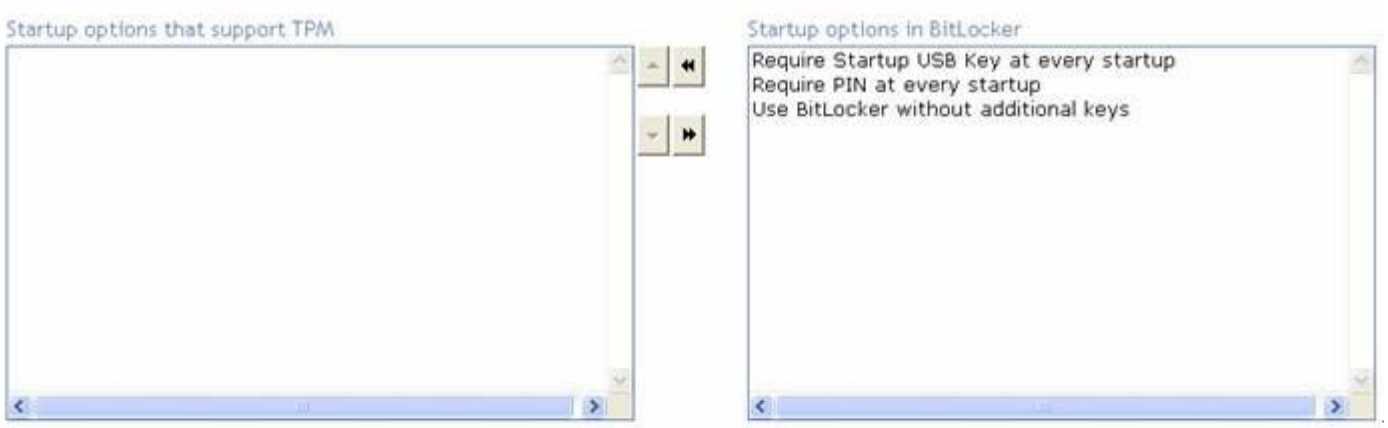
* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you,

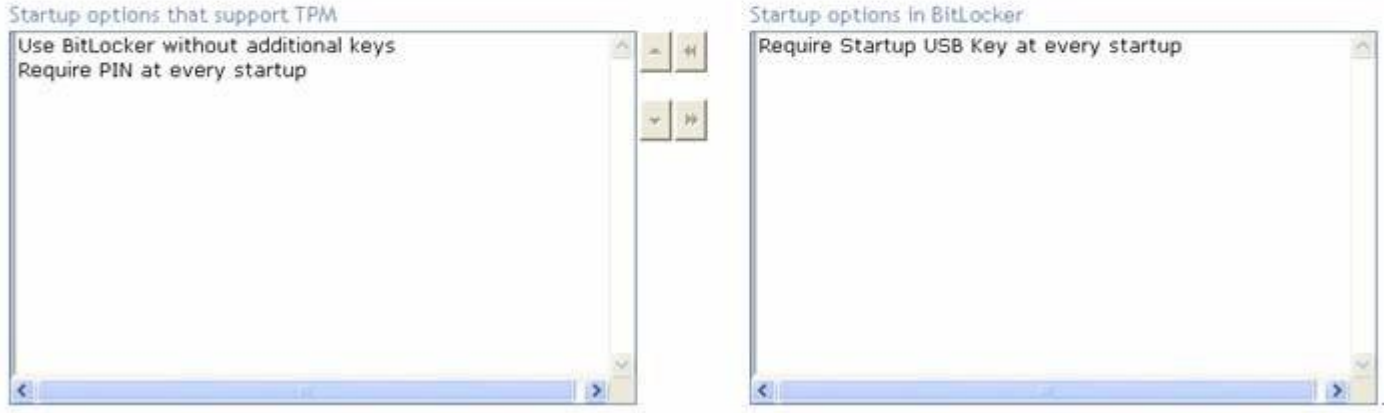
but also provide you another exam of your claim, ABSOLUTELY FREE!

Exam A

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:



A.

B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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)

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following is the process used by attackers for listening to the network traffic?

A. Eavesdropping
B. Subnetting
C. Sanitization
D. Hacking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following is a Windows configuration option that enables administrators to restrict

communication among domain members only?

A. Demilitarized zone
B. Server isolation
C. Domain isolation
D. Domain kiting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21

Which of the following are required to enable for preventing the users from downloading and installing

software from the Internet? Each correct answer represents a complete solution. Choose all that apply.

A. Software restriction policies
B. PTR record
C. User Account Control
D. Anti-Virus software

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
You check the logs on several clients and find that there is traffic coming in on an odd port (port 1872).

All clients have the Windows XP firewall turned on. What should you do to block this unwanted traffic?

A. Perform a virus scan to find the virus responsible for this traffic.
B. Check the exceptions in the firewall and unselect that port exception.
C. Trace back that traffic and find its origin.
D. Shut down the service that connects to that port.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following is a set of rules that control the working environment of user accounts and computer accounts?

A. Mandatory Access Control
B. Access control list
C. Group Policy
D. Intrusion detection system

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
By default, what level of security is set for the Local intranet zone?

A. High-Medium
B. Medium-Low
C. High
D. Low

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Mark works as a Desktop Administrator for TechMart Inc. The company has a Windows-based network.

He has bees assigned a project to upgrade the browsers to Internet Explorer (IE) 8 for working with the

latest Internet technologies Mark wants to ensure that the company uses a number of the security features

built into the browser while maintaining functionality within the company's intranet. Mark is also educating

his users to be good Internet citizens and use the safe web sur?ng. Mark asked his team to be assured that

they are on a secured website. What they will do?

A. Take a look for a padlock in the lower right corner of the browser and https:// in the address bar.
B. Provide protection against a Distributed Denial of Services attack.
C. Call a team member while behaving to be someone else for gaining access to sensitive information.
D. Go into the Internet Options, select the Security, and add the intranet site to the list of Local Intranet Site.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Mark works as a Security Officer for TechMart Inc. The company has a Windows-based network. He

has bees assigned a project for ensuring the safety of the customer's money and information, not to

mention the company's reputation. The company has gone through a security audit to ensure that it is in

compliance with industry regulations and standards. Mark understands the request and has to do his due diligence for providing any information the regulators require as they are targeting potential security holes.

In this situation, his major concern is the physical security of his company's system. Which of the following

actions will Mark take to ensure the physical security of the company's desktop computers?

A. Call a team member while behaving to be someone else for gaining access to sensitive information.
B. Develop a social awareness of security threats within an organization.
C. Use group policies to disable the use of floppy drives or USB drives.
D. Provide protection against a Distributed Denial of Services attack.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Mark works as a Network Administrator for TechMart Inc. The company has a Windows-based network.

Mark wants to implement a method to ensure that the mobile devices are in a good state of security health

when they are trying to access the corporate network. For this purpose, Mark is using NAP. Which of the

following will he do for those computers in the network that are not compatible with NAP?

A. Define exceptions in NAP for computers that are not compatible with NAP.
B. Hide those computers that are not compatible with NAP.
C. Remove those computers that are not compatible with NAP.
D. Do not use the NAP, if any of the computers is showing incompatibility in the entire network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which of the following is a collection or list of user accounts or computer accounts?

A. Group
B. Active Directory
C. Domain
D. Public folder

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following security features of IE 7+ makes it more difficult for malware to be installed?

A. Security zones
B. Phishing filter
C. Protected mode
D. Pop-up blocker

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following is a secret numeric password shared between a user and a system for

authenticating the user to the system?

A. Key escrow
B. Public key
C. Private key
D. PIN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following can be installed for ensuring that the domain is secure in the remote locations?

A. Read-Only domain controller (RODC)
B. Microsoft Baseline Security Analyzer
C. Windows Software Update Services

D. DNS dynamic update

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
You work as a Network Administrator for TechMart Inc. The company has a Windows-based network.

After completing a security audit of the company's Microsoft Windows Server 2008 R2 file servers, you

have determined that folder and share security requires a revision on the basis of corporate reorganization.

You have noticed that some shares on the file system are not secured. Which of the following will you use to

prevent unauthorized changes to computers on the domain?

A. TCP/IP protocol
B. Kerberos
C. User Account Control (UAC)
D. Lightweight Directory Access Protocol

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following is defined as a digitally signed statement used to authenticate and to secure

information on open networks?

A. Kerberos
B. Public certificate
C. Single sign-on (SSO)
D. SEAL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following layers defines the mechanisms that allow data to be passed from one network to another?

A. Network layer
B. Session layer
C. Physical layer
D. Data-link layer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
You work as a Network Administrator for NetTech Inc. Your computer has the Windows 2000 Server operating system. You want to harden the security of the server. Which of the following changes are required to accomplish this? Each correct answer represents a complete solution. Choose two.

A. Enable the Guest account.
B. Rename the Administrator account.
C. Remove the Administrator account.
D. Disable the Guest account.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following types of attack is used to configure a computer to behave as another computer

on a trusted network by using the IP address or the physical address?

A. Distributed denial of service (DDOS) attack
B. Honeypot
C. RIP/SAP Spoofing
D. Identity spoofing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following actions should be taken so that the computer requires confirmation before

installing an ActiveX component?

A. Configuring a firewall on the network
B. Configuring the settings on the Web Browser
C. Installing an anti-virus software
D. Configuring DMZ on the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
What are the main classes of biometric characteristics? Each correct answer represents a complete

solution. Choose two.

A. Psychological
B. Behavioral
C. Fundamental
D. Physiological

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
You work as a network administrator for an insurance company called InZed Inc. The company has

developed a corporate policy that requires all machines to use the IPSec security protocol. If the computer

they are logging in from does not follow this corporate policy, they will be denied access to the network.

Which of the following can you set up to help enforce the corporate policy?

A. Server Access Protection
B. System Center Data Protection Manager (DPM)
C. Microsoft Assessment and Planning (MAP) Toolkit
D. Network Access Protection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following ports is used by the IMAP4 protocol?

A. 443
B. 53
C. 143

D. 110

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
On which of the following is the level of security set for the restricted sites applied?

A. To the sites that might potentially damage your computer, or your information.
B. To the sites that you have specifically indicated as the ones that you trust.
C. To the Websites and content that are stored on a corporate or business network.
D. To all the Websites by default.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
You work as a Network Administrator for NetTech Inc. You want to prevent users from accessing the

graphical user interface (GUI) on the computers in the network. What will you do to accomplish this task?

A. Implement a remote access policy
B. Implement a group policy
C. Apply NTFS permission
D. Implement an account policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Your Web server crashes at exactly the point where it reaches 1 million total visits. You discover the

cause of the server crash is malicious code. Which description best fits this code?

A. Virus
B. Worm
C. Polymorphic Virus
D. Logic Bomb

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following is the process of keeping track of a user's activity while accessing network

resources?

A. Authentication
B. Auditing
C. Spoofing
D. Biometrics

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Mark works as a Network Administrator for NetTech Inc. The company has a Windows Server 2008

domain-based network. The network has a Windows Server 2008 member server that works as a Routing

and Remote Access Server (RRAS). Mark implements Network Access Protection (NAP) for the network.

Mark wants to configure Point-to-Point Protocol (PPP) authentication on the RRAS server. Which of the following authentication methods should Mark use to accomplish this task?

A. EAP
B. CHAP
C. SPAP
D. PAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
You are taking over the security of an existing network. You discover a machine that is not being used as such, but has software on it that emulates the activity of a sensitive database server. What is this?

A. A Polymorphic Virus
B. A Honey Pot
C. A reactive IDS.
D. A Virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Sam works as a Web Developer for McRobert Inc. He wants to control the way in which a Web browser receives information and downloads content from Web sites. Which of the following browser settings will Sam use to accomplish this?

A. Security

B. Certificate
C. Cookies
D. Proxy server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Mark works as a Security Officer for TechMart Inc. The company has a Windows-based network. He has bees assigned a project for ensuring the safety of the customer's money and information, not to mention the company's reputation. The company has gone through a security audit to ensure that it is in compliance with industry regulations and standards. Mark understands the request and has to do his due diligence for providing any information the regulators require as they are targeting potential security holes. In this situation, his major concern is the physical security of his company's system. He has a concern that people are authenticated to the servers in the data center. Which of the following actions will Mark take to prevent normal users from logging onto the systems?

A. Call a team member while behaving to be someone else for gaining access to sensitive information.
B. Use group policies to disable the use of floppy drives or USB drives.
C. Provide protection against a Distributed Denial of Services attack.
D. Develop a social awareness of security threats within an organization.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following types of viruses protects itself from antivirus programs and is more difficult to

trace?

A. Armored virus
B. MBR virus
C. Boot sector virus
D. Macro virus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which of the following is the edge between the private and locally managed-and-owned side of a

network and the public side that is commonly managed by a service provider?

A. Internet
B. Network perimeter
C. Intranet
D. VLAN

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Mark work as a System Administrator for TechMart Inc. The company has a Windows-based network.

Mark wants to allow the remote travel agents to be able to access the corporate network so that they are

free to check email and post appointments that are booked for the particular day. Mark has decided to

permit the travel agents to use their home computers but he is required to be assured that the information is

not compromised by anyone because the security of client information is on the top priority for him. Which

of the following will Mark use to accomplish the task?

A. Implement the principle of least privilege that permits the travel agents for remote access.
B. Implement a Wi-Fi Protected Access that permits the travel agents for remote access.
C. Implement a Wired Equivalent Privacy that permits the travel agents for remote access.
D. Implement a VPN server that permits the travel agents for remote access.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following practices should be followed to keep passwords secure? Each correct answer

represents a complete solution. Choose three.

A. Change the passwords whenever there is suspicion that they may have been compromised.
B. A password should be alpha-numeric.
C. A password should not be more than five words.
D. Never write down a password.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following collects email addresses of users and creates a mailing list?

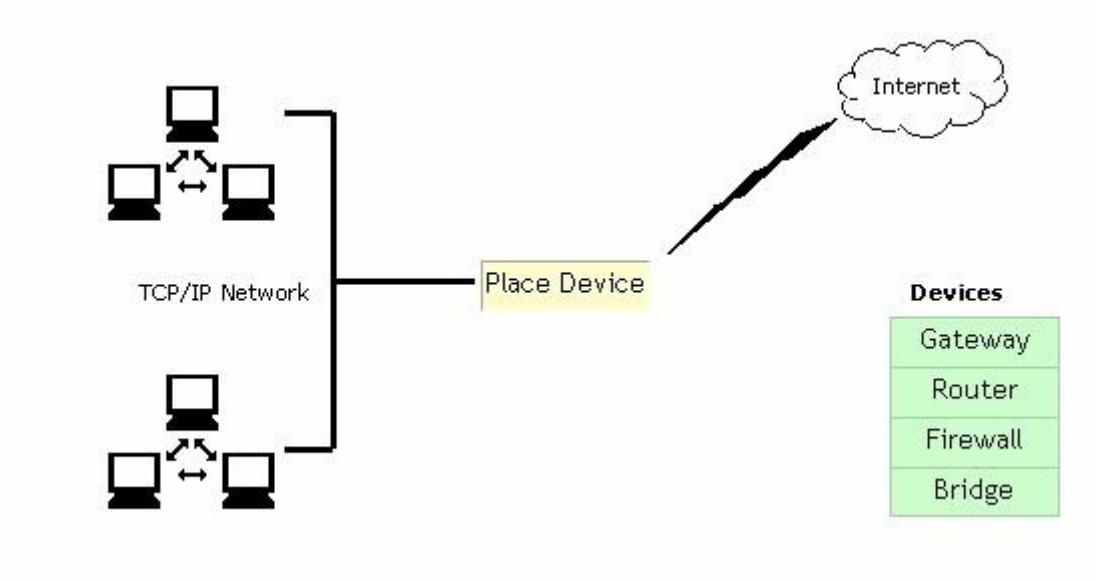
A. Browser
B. Cookie
C. Spambot
D. Perimeter network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
You work as a Network Administrator for McRobert Inc. Your company has a TCP/IP-based network.

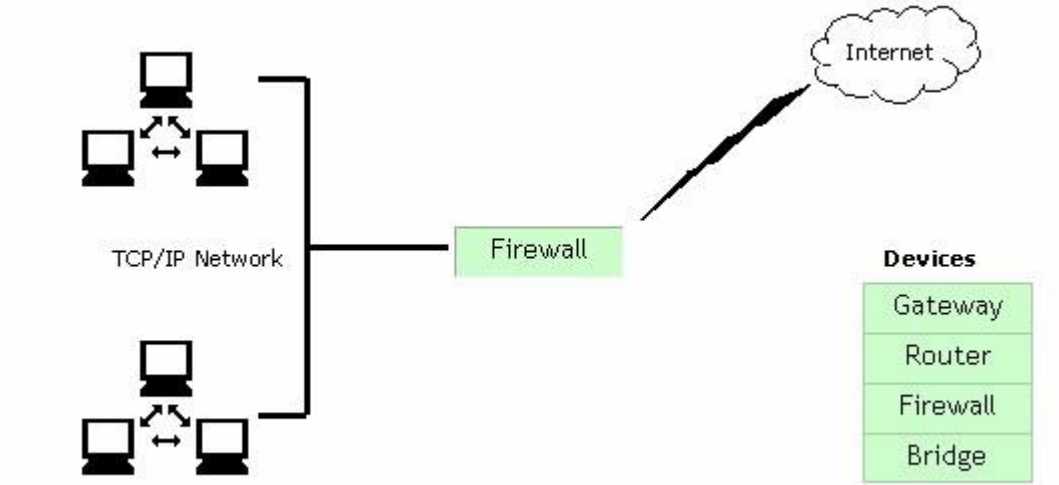
You plan to connect your company's LAN to the Internet. You are concerned about the security of your network and want to protect it against external access and misuse. Which device will you install between your LAN and the Internet to accomplish this?



A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:



QUESTION 56
In which of the following is the file audit events are written when auditing is enabled?

A. File system ACL
B. Biometric device
C. Network Access Control List
D. Security event log

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following security features of IE 7+ helps determine whether a Web site is a legitimate

site?

A. Protected mode
B. Pop-up blocker
C. Security zones
D. Phishing filter

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Ron owns the domain TechPerfect.net. He often receives bounces about messages he didn't send.

After looking at all such mails, he is sure that someone is spamming e-mails and using his domain name.

What will Ron do to ensure that his domain name is not exploited?

A. Publish the MX record for the domain.
B. Publish the SPF record for the domain.
C. Publish the AAAA record for the domain.
D. Publish the A record for the domain.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following points has to be considered for using the BitLocker?

A. The deployment of antivirus because BitLocker needs a a removal of buffer overflow.
B. The deployment of SEAL because BitLocker needs an alternative encryption algorithm to software-based DES, 3DES, and AES. .
C. The deployment of hardware because BitLocker needs a system reserved partition.
D. The deployment of hard disk because BitLocker needs a bot.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following is a program that runs at a specific date and time to cause unwanted and

unauthorized functions?

A. Keylogger
B. Logic bomb
C. Spyware
D. Trojan horse

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following is a disadvantage of using biometric identification?

A. It breaks the several firewall security rules.
B. It needs a new network configuration of the entire infrastructure.
C. It can be faked and will not be trusted by several organizations.
D. It is expensive and cannot be afforded by several organizations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62

You work as a Network Administrator for TechMart Inc. The company has a Windows-based network.

After completing a security audit of the company's Microsoft Windows Server 2008 R2 file servers, you

have determined that folder and share security requires a revision on the basis of corporate reorganization. You have noticed that some shares on the file system are not secured. Which of the following is a feature

that you will use to reassign permissions without assigning permissions to every parent and child folder?

A. Inheritance
B. Kerberos
C. TCP/IP protocol
D. User Account Control (UAC)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following is a US Federal government algorithm created to generate a secure message

digest?

A. DSA
B. RSA
C. Triple DES
D. SHA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Which of the following can be implemented to ensure that the computers are using latest security

updates?

A. Hardening
B. Windows Software Update Services
C. Microsoft Baseline Security Analyzer
D. Domain Name System

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following are the types of group scopes? Each correct answer represents a complete

solution. Choose all that apply.

A. Global
B. Domain Users
C. Universal
D. Domain local

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Mark works as a Network Administrator for NetTech Inc. The company has a Windows Server 2008

domain-based network. Mark configures Network Access Protection (NAP) on the network. He then

configures secure wireless access to the network from all access points on the network. He also configures

A.
B.

C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
1x authentication for accessing the network. Mark wants to ensure that all computers connecting to the network are checked by NAP for the required configuration and update status. What will Mark do to accomplish the task?

A. Configure all computers connecting to the network with IPSec.
B. Configure all access points as RADIUS clients to Distributed File System.
C. Configure Link-local Multicast Name Resolution (LLMNR) on the network.
D. Configure all access points as RADIUS clients to Network Policy Server (NPS).

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
You work as a security manager for Company Inc. An individual is connecting to your corporate internal network over the Internet. You have to ensure that he is not an intruder masquerading as an authorized user. Which of the following technologies will you use to accomplish the task?

A. Two-factor authentication
B. IP address packet filtering
C. Intrusion detection system (IDS)
D. Embedded digital signature

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which of the following areas of a network contains DNS servers and Web servers for Internet users?

A. VPN
B. MMZ
C. DMZ
D. VLAN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
All your domain controllers are configured for DHCP. Each time the system is booted, it gets a new IP address from the DHCP server. You had also configured the Active Directory on the domain controllers. You want to configure your DNS settings so that it will dynamically update DNS data whenever the IP address of a domain controller changes. How will you configure for dynamic updates?

A. Configure the DNS server for dynamic updates.
B. Configure the DHCP server for DNS dynamic updates.
C. Configure each domain controller for Dynamic update.
D. Configure the Active directory for dynamic updates.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following are the features of security level in the Restricted Sites zone

A. The protection against harmful content is provided.
B. The maximum safeguards are used.
C. Most of the features are disabled.
D. The default security level is low.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following is a secret numeric password shared between a user and a system for

authenticating the user to the system?

A. PIN
B. Private key
C. Key escrow
D. Public key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Mark works as a Network Administrator for BlueWell Inc. The company has a Windows-based network.

Mark has retained his services to perform a security assessment of the company's network that has various

servers exposed to the Internet. So, it may be vulnerable to an attack. Mark is using a single

perimeter ?rewall, but he does not know if that is enough. He wants to review the situation and make some

reliable recommendations so that he can protect the data over company's network. Which of the following will Mark do to accomplish the task?

A. Outsource the related services.
B. Encrypt the data and than start transmission.
C. Locate the Internet-exposed servers and devices in an internal network.
D. Create a perimeter network to isolate the servers from the internal network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following is a security protocol that is used to protect data from being modified, corrupted,

or accessed without authorization?

A. Honeypot
B. IP Security (IPsec)
C. DNSSEC
D. Protocol spoofing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following protocols is used to secure workstation and computer authentication across the

network?

A. TCP/IP
B. Network Directory Access Protocol

C. Kerberos
D. Lightweight Directory Access Protocol

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Mark works as a Systems Administrator for TechMart Inc. The company has a Windows-based network.

The company had a many outbreaks of viruses on the network that are propagated via email. Mark wants to

educate his team about malicious software and email. Which of the following will he suggest his team

members to do when a suspicious email that contains an embedded hyperlink is received from a customer?

A. To delete the email and then contact Mark and the customer.
B. To forward the email to other team members for warning them that the email is not legitimate.
C. To click the hyperlink for checking the result.
D. To resend the email to the customer from which it seems to be sent.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
You work as a Network Administrator for NetTech Inc. The company has a Windows Server 2008

domain-based network. The network contains 4 Windows Server 2008 member server and 120 Windows

Vista client computers. Your assistant wants to know about the settings that make up Network Access

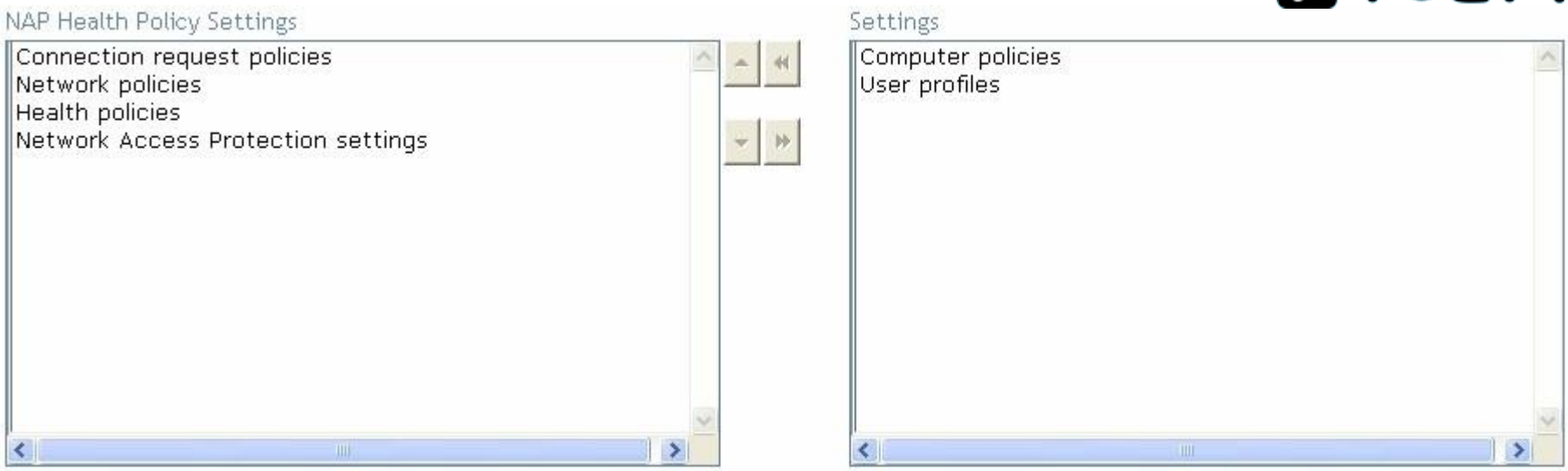
Protection (NAP) health policies. Choose the settings that are the part of Network Access Protection (NAP)

health policies.

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:



QUESTION 78
Which of the following viruses infects Word 97 documents and the NORMAL.DOT file of Word 97 and

Word 2000?

A. Chernobyl
B. Brain
C. EICAR
D. Melissa

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Mark works as a Security Administrator for TechMart Inc. The company has a Windows-based network.

Mark has gone through a security audit for ensuring that the technical system is secure and protected.

While this audit, he identified many areas that need improvement. He wants to minimize the risk for

potential security threats by educating team members in the area of social engineering, and providing basic security principle knowledge and he also wants to stress the Con?dentiality, Integrity, and Availability triangle in his training. For this purpose, he plans to implement the principle of least privilege. In which of the following way, it will affect his team members?

A. They are required to ask administrator every time when they want to access resources.
B. They are granted with a smallest set of privileges to the resources
C. They are required to log on as administrator to have access to their resources
D. The current resource access of team members will not change.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following is a use of Microsoft Windows Malicious Software Removal Tool?

A. To gain unauthorized remote access to a computer and launch additional attacks.
B. To distribute itself automatically from one computer to another via network connections.
C. To remove the malware.
D. To perform repetitive or time-consuming task on a network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which of the following helps prevent security failures?

A. Social engineering
B. Denial-of-Service attack

C. Attack surface reduction
D. Snooping

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following steps can be taken by an administrator as countermeasures against software

keyloggers? Each correct answer represents a part of the solution. Choose all that apply.

A. Use commercially available anti-keyloggers.
B. Actively monitor the programs running on the server.
C. Update antivirus regularly.
D. Always check hard disk space on the server.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following applications captures network packets as they traverse a network and displays

them to the attacker?

A. Keylogger
B. Sniffer
C. Key fob
D. Protocol analyzer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
You are responsible for virus protection for a large college campus. You are very concerned that your

antivirus solution must be able to capture the latest virus threats. What sort of virus protection should you

implement?

A. Network Based
B. Host based
C. Dictionary
D. Heuristic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following can be implemented to decrease the number of times a user is required to be

authenticated for access a particular resource?

A. TCP/IP protocol
B. Network Directory Access Protocol
C. Kerberos
D. Single Sign-on (SSO)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86

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

A. Polymorphic
B. MBR virus
C. Boot sector
D. Macro

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following types of Network Address Translation (NAT) uses a pool of public IP addresses?

A. Static NAT
B. Port Address Translation (PAT)
C. Dynamic NAT
D. Cache NAT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following is a attack type that is used to poison a network or computer to the point where

the system is turned into unusable state?

A. Mail bombing
B. Pharming
C. Protocol spoofing
D. Denial of service (DOS)

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following is a broadcast domain created by a switch?

A. VLAN
B. MAN
C. DMZ
D. VPN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following is an authentication protocol?

A. Kerberos
B. LDAP
C. TLS
D. PPTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following are the main features of a key logger? Each correct answer represents a

complete solution. Choose all that apply.

A. It can be delivered via FTP or e-mail.
B. It can record all keystrokes.
C. It can capture all screenshots.
D. It can detect viruses on the computer.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Mark works as a Network Administrator for NetTech Inc. The company has a Windows Server 2008 domain-based network. The network uses Network Access Protection (NAP). The company's employees at the remote locations are connecting to the company's network from their Windows Vista clients. Mark wants to ensure that the data transmission between a client computer and the company's network is as secure as possible. What will Mark do to accomplish the task?

A. Use Encrypting File System (Efs) between the client computer and the company's network.
B. Use IPSec NAP policy between client computer and the company's network.
C. Use VPN connection with MS-CHAP v2 between the client computer and the company's network.
D. Use NAP enforcement for DHCP.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Mark work as a System Administrator for TechMart Inc. The company has a Windows-based network. Mark wants to allow the remote travel agents to be able to access the corporate network so that they are free to check email and post appointments that are booked for the particular day.

Mark has decided to permit the travel agents to use their home computers but he is required to be assured

that the information is not compromised by anyone because the security of client information is on the top priority for him. Which of the following is a potential risk if the travel agents will use their home computers for

VPN access?

A. VPN handles everything and encrypts the data.
B. VPN does not allow the travel agents to use their home computers.
C. VPN cannot prevent buffer overflow on the home computer from infecting the network.
D. VPN cannot prevent potential viruses and malware on the home computer from infecting the network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Mark works as a Security Officer for TechMart Inc. The company has a Windows-based network. He

has bees assigned a project for ensuring the safety of the customer's money and information, not to

mention the company's reputation. The company has gone through a security audit to ensure that it is in

compliance with industry regulations and standards. Mark understands the request and has to do his due

diligence for providing any information the regulators require as they are targeting potential security holes.

In this situation, his major concern is the physical security of his company's system. Which of the following

actions will Mark take to prevent the use of key loggers in the company?

A. Provide protection against a Distributed Denial of Services attack.
B. Call a team member while behaving to be someone else for gaining access to sensitive information.
C. Ensure that the terminals are locked and perform a regular inspection of the ports on the systems.
D. Develop a social awareness of security threats within an organization.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Which of the following is a tool that can be used to evaluate the servers having vulnerabilities that are

related to the operating system and installed software?

A. DNS dynamic update
B. Windows Software Update Services
C. Read-Only domain controller (RODC)
D. Microsoft Baseline Security Analyzer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following ports is used by the Remote Desktop Protocol?

A. 80
B. 23
C. 3389
D. 110

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which of the following MMC snap-in consoles is used to administer the replication of directory data

among all sites in an Active Directory Domain Services (AD DS) forest?

A. Active Directory Domains and Trusts
B. Active Directory Administrative Center
C. Group Policy Management Console
D. Active Directory Sites and Services

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following is used to create a secured connection over an unsecured network?

A. TCP/IP protocol
B. Virtual Private Network (VPN)
C. Single Sign-on (SSO)
D. Kerberos

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following are the Internet Explorer security zones? Each correct answer represents a

complete solution. Choose three.

A. Trusted sites
B. Internet
C. Local intranet
D. Extranet

Correct Answer: ABC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following is a central, secure database in which Windows stores all hardware configuration information, software configuration information, and system security policies?

A. Registry
B. Program files folder
C. DLL file
D. Configuration file

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
You have configured a virtualized Internet browser on your Windows XP professional computer. Using

the virtualized Internet browser, you can protect your operating system from which of the following?

A. Brute force attack
B. Distributed denial of service (DDOS) attack
C. Mail bombing
D. Malware installation from unknown Web sites

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Mark works as the Network Administrator of a Windows 2000 based network. In order to reduce the

administrative burden and to optimize the network performance, he implements the DHCP and the DNS

servers on the network. What will he do integrate the working between the DHCP and the DNS servers?

Each correct answer represents a part of the solution. Choose two.

A. Configure the clients to use the DHCP server.
B. Enable DNS updates on the DHCP server.
C. Enable dynamic update on the DNS server.
D. Use the TCP/IP protocol on the network.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Which of the following statements about Network Address Translation (NAT) are true? Each correct

answer represents a complete solution. Choose two.

A. It allows the computers in a private network to share a global, ISP assigned address to connect to the Internet.
B. It provides added security by using Internet access to deny or permit certain traffic from the Bastion Host.
C. It allows external network clients access to internal services.
D. It reduces the need for globally unique IP addresses.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
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 can Mark use to minimize the spam amount that is hitting the Microsoft Exchange server of the company?

A. Enable reverse DNS lookup
B. Use Read-only Domain Controller
C. Add Sender Policy Framework
D. Permit User Account Control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Which of the following is the most common method for an attacker to spoof email?

A. Back door
B. Replay attack
C. Man-in-the-middle attack
D. Open relay

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Which of the following security methods can be used to detect the DoS attack in order to enhance the security of the network?

A. Protocol analyzer
B. WIPS

C. WLAN controller
D. Spectrum analyzer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
On which of the following is the level of security set for an Internet zone applied?

A. To the sites that you have specifically indicated as the ones that you trust.
B. To all the Websites by default.
C. To the sites that might potentially damage your computer, or your information.
D. To the Websites and content that are stored on a corporate or business network.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
Which of the following tools traces all or specific activities of a user on a computer?

A. Task Manager
B. Event Viewer
C. Network Monitor
D. Keylogger

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Which of the following is a mechanism that allows authentication of dial-in and other network

connections?

A. VPN
B. NTFS
C. RADIUS
D. Single Sign-On

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Mark works as a Network Administrator for BlueWell Inc. The company has a Windows-based network.

Mark has retained his services to perform a security assessment of the company's network that has various

servers exposed to the Internet. So, it may be vulnerable to an attack. Mark is using a single

perimeter ?rewall, but he does not know if that is enough. He wants to review the situation and make some

reliable recommendations so that he can protect the data over company's network. Which of the following

will Mark use to provide better security?

A. Tricky packet inspection
B. Stateful packet inspection
C. Stateless packet inspection
D. Reaction based packet inspection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Which of the following can be used to implement two-factor authentications? Each correct answer

represents a complete solution. Choose all that apply.

A. Firewall security rule
B. Password
C. Smart card
D. Encrypted network configuration

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
John works as a Network Administrator for We-are-secure Inc. The We-are-secure server is based on

Windows Server 2003. One day, while analyzing the network security, he receives an error message that

Kernel32.exe is encountering a problem. Which of the following steps should John take as a

countermeasure to this situation? Each correct answer represents a complete solution. Choose all that

apply.

A. He should restore his Windows settings.
B. He should upgrade his antivirus program.
C. He should observe the process viewer (Task Manager) to see whether any new process is running on the computer or not. If any new malicious process is running, he should kill that process.
D. He should download the latest patches for Windows Server 2003 from the Microsoft site, so that he can repair the kernel.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Which of the following is a physical address stored in the Network Interface card on your system or any

other device residing on your network?

A. IP address
B. I/O address
C. MAC Address
D. Broadcast address

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
Mark works as a Network Administrator for TechMart Inc. The company has a Windows-based network.

Mark wants to implement a method to ensure that the mobile devices are in a good state of security health

when they are trying to access the corporate network. Which of the following is a control or strategy that

Mark will implement to assure the security health?

A. TCP/IP protocol
B. Kerberos
C. Single Sign On
D. Network Access Protection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Mark works as a Security Administrator for TechMart Inc. The company has a a Windows-based

network. Mark has gone through a security audit for ensuring that the technical system is secure and protected. While this audit, he identified many areas that need improvement. He wants to minimize the risk for potential security threats by educating team members in the area of social engineering, and providing basic security principle knowledge while stressing the Con?dentiality, Integrity, and Availability triangle in the training of his team members . Which of the following ways will Mark use for educating his team members on the social engineering process?

A. He will call a team member while behaving to be someone else for gaining access to sensitive information.
B. He will use group policies to disable the use of floppy drives or USB drives.
C. He will develop a social awareness of security threats within an organization.
D. He will protect against a Distributed Denial of Services attack.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Which of the following is the reason of properly securing an audit log?

A. To ensure that only authorized person can check the log file.
B. To ensure that no one can remove it as there is no back up is provided for this log.
C. To ensure that potential hackers becomes unable to delete the event logs for covering their tracks.
D. To ensure that potential hackers can be tracked easily without changing the network configuration.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117

Which of the following is used to describe the policy of maximum password age?

A. It is used to determine how old the user has to create a password.
B. It is a time duration before a password is required to be public.
C. It is a time duration before a password is required to be changed.
D. It determines how old the password must be before the user is permitted to change it.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following is often used for one-to-many communications using broadcast or multicast IP

datagrams?

A. UDP
B. FTP
C. HTTP
D. SMTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
Which of the following is used to protect all files stored on the drive on which Windows is installed?

A. SocketShield
B. Firewall
C. Bitlocker
D. Hardware keylogger

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
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 under pressure to make this new feature a winning strategy for a company. Which of the following is the most secure protocol that Mark can implement to ensure that the

business-related traffic is encrypted?

A. WiFi Protected Access (WPA) 2
B. Extensible Authentication Protocol (EAP)
C. Wired Equivalent Privacy (WEP)
D. Service Set Identifiers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
Which of the following is a name that identifies a particular 802.11 wireless LAN?

A. MBSA
B. IBSS
C. MAC
D. SSID

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
Which of the following protocols transmits user credentials as plaintext?

A. CHAP
B. MS-CHAP v2
C. PAP
D. MS-CHAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Which of the following is a networking protocol that provides centralized Authentication, Authorization,

and Accounting management for computers to connect and use a network service?

A. PEAP
B. RADIUS
C. Kerberos
D. MS-CHAP v2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
Which of the following is method that can be used to identify Internet software in Software Restriction

Policies?

A. Restriction rule
B. Identification rule
C. Internet rule
D. Zone rule

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Which of the following is a method of capturing and recording computer users' keystrokes including

sensitive passwords?

A. Using hardware keyloggers
B. Using Alchemy Remote Executor
C. Using SocketShield
D. Using Anti-virus software

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Which of the following operating systems have Windows Security Health Agent (SHA) on computers

and report their status to the Security Health Validator (SHV)? Each correct answer represents a complete

solution. Choose three.

A. Windows 2000 Professional
B. Windows Vista Business
C. Windows XP Service Pack 3
D. Windows 7 Professional

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Mark works as a Network Administrator for TechMart Inc. The company has a Windows-based network.

Mark wants to implement stronger authentication measures for the customers, as well as eliminate IT staff

from logging on with high privileges. Mark has various options, but he is required to keep the processes

easy for the helpdesk staff. Which of the following is a service can the staff uses as an alternative of signing

in with elevate privileges?

A. Secondary Logon-Run As
B. Security log
C. Hardware firewall
D. Encrypted network configuration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
Which of the following are the uses of Network Access Protection (NAP)?

Each correct answer represents a complete solution. Choose all that apply.

A. It is used to protect against virus.
B. It is used to verify the complete integrity of each device.
C. It permits a user to access all computers and systems where he got a access permission, without entering passwords for multiple times
D. It is used to authenticate a request for a service in a computer network.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
Which of the following services does IPSec provide for protecting data? Each correct answer

represents a complete solution. Choose two.

A. Network authentication
B. Encryption
C. Data authentication
D. Compression

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
Which of the following functions are performed by a firewall? Each correct answer represents a

complete solution. Choose all that apply.

A. It blocks unwanted traffic.
B. It hides vulnerable computers that are exposed to the Internet.
C. It enhances security through various methods, including packet filtering, circuit-level filtering, and application filtering.
D. It logs traffic to and from the private network.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
Mark works as a Security Administrator for TechMart Inc. The company has a a Windows-based network. Mark has gone through a security audit for ensuring that the technical system is secure and protected. While this audit, he identified many areas that need improvement. He wants to minimize the risk for potential security threats by educating team members in the area of social engineering, and providing basic security principle knowledge while stressing the Con?dentiality, Integrity, and Availability triangle in the training of his team members. In which of the following ways, the security training is related to providing availability?

A. Providing protection against a Distributed Denial of Services attack.
B. Developing a social awareness of security threats within an organization.
C. Calling a team member while behaving to be someone else for gaining access to sensitive information.
D. Using group policies to disable the use of floppy drives or USB drives.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
Which of the following are indications of a virus attack on a computer? Each correct answer represents a complete solution. Choose three.

A. Although the computer has sufficient memory, an out-of-memory error message is displayed.
B. The applications installed on the computer system work properly.
C. An antivirus program is not able to run.
D. The computer runs slower than usual and stops responding.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
You work as an Exchange Administrator for UniCom Inc. The company has a Windows 2003 Active

Directory-based network. The network contains an Exchange Server 2007 organization. You have deployed

a DNS server in your messaging organization. The DNS server hosting the DNS zone data for the

Exchange Server is not capable of processing dynamic DNS updates. You decide to troubleshoot DNS.

Which of the following utilities will you use to identify anomalies of records in the targeted DNS zone?

A. Nslookup.exe
B. IPCONFIG
C. DNSCMD.exe
D. DNSLint

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
On which of the following is the level of security set for the local intranet zone applied?

A. To the sites that might potentially damage your computer, or your information.
B. To the Websites and content that are stored on a corporate, or business network.
C. To the sites that you have specifically indicated as the ones that you trust.
D. To all the Websites by default.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
Which of the following is the layer in which encryption and decryption of data takes place?

A. Presentation layer
B. Session layer
C. Physical layer
D. Data-link layer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
Which of the following root keys stores information about registered applications?

A. HKEY_USERS
B. HKEY_CLASSES_ROOT
C. HKEY_CURRENT_CONFIG
D. HKEY_CURRENT_USER

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Which of the following is an organization that defines standards for anti-virus software?

A. ICSA
B. IETF
C. IIS
D. IEEE

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 138
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 under pressure to make this new feature a winning strategy for a company.

In which of the following ways can Mark add another level of security after implanting encryption techniques for the business wireless traffic? Each correct answer represents a complete solution. Choose all that apply.

A. Hide the Service Set Identifier (SSID)
B. Configure the network to use only Extensible Authentication Protocol (EAP)
C. Implement access point isolation and
D. Use MAC filtering

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
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 can Mark do after enabling reverse DNS lookups to minimize the amount of spam?

A. Permit User Account Control
B. Add Sender Policy Framework
C. Use Read-only Domain Controller
D. Windows Server Update Services

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Mark works as a Network Administrator for TechMart Inc. The company has a Windows-based network

He has been assigned a project to take care of the sensitive data that can be hacked if any of the laptop

computers would be misplaced. Mark is required to ensure the con? dentiality of data on the mobile stations,

all of which are running Windows 7 Enterprise. Which of the following will Mark use to accomplish the task?

A. BitLocker
B. Confidential File System
C. Kerberos
D. Encrypting File System (EFS)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Which of the following is more secure protocol between Point to Point Tunneling Protocol (PPTP) and

Layer 2 Tunneling Protocol (L2TP)?

A. PPTP and L2TP, both of them define the same security standard.
B. PPTP is more secure than L2TP.

C. PPTP and L2TP , both of them are used to provide the database connection.
D. L2TP is more secure than PPTP.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
Which of the following is a service can be enabled to ensure that the servers are able to receive all

essential software updates?

A. Windows Software Update Services
B. Read-Only domain controller (RODC)
C. Microsoft Baseline Security Analyzer
D. DNS dynamic update

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Mark works as a Network Administrator for BlueWell Inc. The company has a Windows-based network.

Mark has retained his services to perform a security assessment of the company's network that has various

servers exposed to the Internet. So, it may be vulnerable to an attack. Mark is using a single

perimeter ?rewall, but he does not know if that is enough. He wants to review the situation and make some

reliable recommendations so that he can protect the data over company's network. Which of the following

will Mark use to inspect network information on the basis of source and destination address?

A. Stateless packet inspection

B. Tricky packet inspection
C. Stateful packet inspection
D. Reaction based packet inspection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
Mark work as a System Administrator for TechMart Inc. The company has a Windows-based network.

Mark wants to allow the remote travel agents to be able to access the corporate network so that they are free to check email and post appointments that are booked for the particular day.

Mark has decided to permit the travel agents to use their home computers but he is required to be assured that the information is not compromised by anyone because the security of client information is on the top priority for him. Mark is concerned about probable attackers will be able to penetrate the VPN. Which of the following will Mark use to attract the attackers for understanding their methods?

A. CIA Triangle
B. Attack surface
C. Honeypot
D. Social engineering

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
Mark works as a Desktop Administrator for TechMart Inc. The company has a Windows-based network.

He has bees assigned a project to upgrade the browsers to Internet Explorer (IE) 8 for working with the

latest Internet technologies Mark wants to ensure that the company uses a number of the security features built into the browser while maintaining functionality within the company's intranet. Mark is also educating his users to be good Internet citizens and use the safe web sur?ng. Which of the following actions will Mark take to configure Internet zone feature in IE 8 and to enable users to easily browse the local intranet without disturbing the security levels?

A. Develop a social awareness of security threats within an organization.
B. Call a team member while behaving to be someone else for gaining access to sensitive information.
C. Provide protection against a Distributed Denial of Services attack.
D. Go into the Internet Options, select the Security, and add the intranet site to the list of Local Intranet Site.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
The workstations on your network utilize Windows XP (service pack 2 or later). Many users take their laptops on the road. You are very concerned about the security and want to have a robust firewall solution for mobile users. You have decided that all your firewalls to use the Stateful Packet Inspection (SPI) method.

What must you do to provide SPI to your mobile users?

A. You must purchase a third party firewall solution for your mobile users.
B. Do nothing. Windows XP service pack 2 has a firewall turned on by default.
C. Configure the Windows XP firewall to use SPI.
D. Download the SPI template from Microsoft.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
You work as a Network Administrator for TechMart Inc. The company has a Windows-based network.

After completing a security audit of the company's Microsoft Windows Server 2008 R2 file servers, you

have determined that folder and share security requires a revision on the basis of corporate reorganization.

You have noticed that some shares on the file system are not secured. Which of the following is the default

permission setting that you have used when a share is created?

A. Everyone with Change permission
B. Administrators with the Full Control permission
C. Administrators with the Change permission
D. Everyone with Read permission

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
Which of the following uses a symmetric encryption algorithm that takes a lesser amount of time to

encrypt or decrypt large amounts of data.

A. BitLocker
B. SSID
C. BitLocker To Go
D. EFS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
Which of the following terms refers to the access of a wireless Internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the

subscriber's explicit permission or knowledge?

A. Samhain
B. Snooping
C. Piggybacking
D. Vampire tap

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
Which of the following is the result of setting the value of Enforce Password History to 10?

A. The system will remember the last 10 passwords and will not permit the user to reuse any of those passwords.
B. The user is granted with a permission of 10 attempts to validate the password
C. The password can be changed only after 10 days of its creation.
D. The system will automatically generate the new 10 passwords that can be used by the user.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
Which of the following are the types of OS fingerprinting techniques? Each correct answer represents

a complete solution. Choose two.

A. Passive fingerprinting

B. Active fingerprinting
C. Laser fingerprinting
D. Unidirectional fingerprinting

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
You work as a Network Administrator for a medium sized business. Spam has become a significant

problem for your company. You want to have a common network wide solution. You want a solution that is

easy to administer. However, you do not want your solution to hinder the performance of your email server.

What is the best solution for you to implement?

A. Utilize a client side anti-spam solution.
B. Use a combination of mail server engine and client side.
C. Utilize a gateway filter anti-spam solution.
D. Utilize a mail server engine anti-spam solution.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
Which of the following MMC snap-in consoles is used to administer domain and forest functional levels

and user principal name (UPN) suffixes?

A. Group Policy Management Console
B. Active Directory Domains and Trusts
C. Active Directory Sites and Services

D. Active Directory Administrative Center

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
Which of the following refers to a security access control methodology whereby the 48-bit address is

assigned to each network card which is used to determine access to the network?

A. Snooping
B. Spoofing
C. Encapsulation
D. MAC filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
Which of the following security zones is used for Web sites that the user does not trust?

A. Internet zone
B. Trusted zone
C. Restricted zone
D. Local Intranet zone

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
Which of the following works at the network layer and hides the local area network IP address and

topology?

A. Network address translation (NAT)
B. MAC address
C. Hub
D. Network interface card (NIC)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
A user has opened a Web site that automatically starts downloading malicious code onto his computer.

What should he do to prevent this? Each correct answer represents a complete solution. Choose two.

A. Disable ActiveX Controls
B. Disable Active Scripting
C. Implement File Integrity Auditing
D. Configure Security Logs

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
You work as an Exchange Administrator for TechWorld Inc. The company has a Windows 2008 Active

Directory-based network. The network contains an Exchange Server 2010 organization. You are in the

process of choosing an authentication method for Exchange ActiveSync. You need an authentication

method that requires both, a password and an external device. Which of the following authentication

methods will you choose for Exchange ActiveSync?

A. Device-based authentication
B. Basic authentication
C. Certificate-based authentication
D. Token-based authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
Which of the following can search contents of a hard disk, address book of an e-mail, or any

information about the computer, and transmit the information to the advertisers or other interested parties

without user knowledge?

A. Malware
B. Firmware
C. Spyware
D. Adware

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
You work as a Network Administrator for SpyNet Inc. The company has a Windows-based network.

You have been assigned the task of auditing the scheduled network security. After a regular audition, you

suspect that the company is under attack by an intruder trying to gain access to the company's network

resources. While analyzing the log files, you find that the IP address of the intruder belongs to a trusted partner company. Assuming this situation, which of the following attacks is the company being subjected to?

A. Spoofing
B. Man-in-the-middle
C. CookieMonster
D. Phreaking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
Which of the following steps will help in system or host hardening? Each correct answer represents a complete solution. Choose two.

A. Installing updated device drivers.
B. Adding users to the administrators group.
C. Installing or applying a patch on the host provided by the operating system manufacturer.
D. Disabling unnecessary services from the host.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Contact us by emails

Please allow up to 24 hours for us to respond

problems about sales and so on problems about payment,installation, acitvation and so on

Sales Email sales@exambible.comSupport Email support@exambible.com

Please Note: Please accept mail from an official, do not believe any of the other E-mail