Microsoft.Test-inside.98-367.v2014-02-11.by.Elsy.160q

Number: 98-367
Passing Score: 700
Time Limit: 60 min
File Version: 12.5

Exam Code:98-367

Exam Name:Security Fundamentals

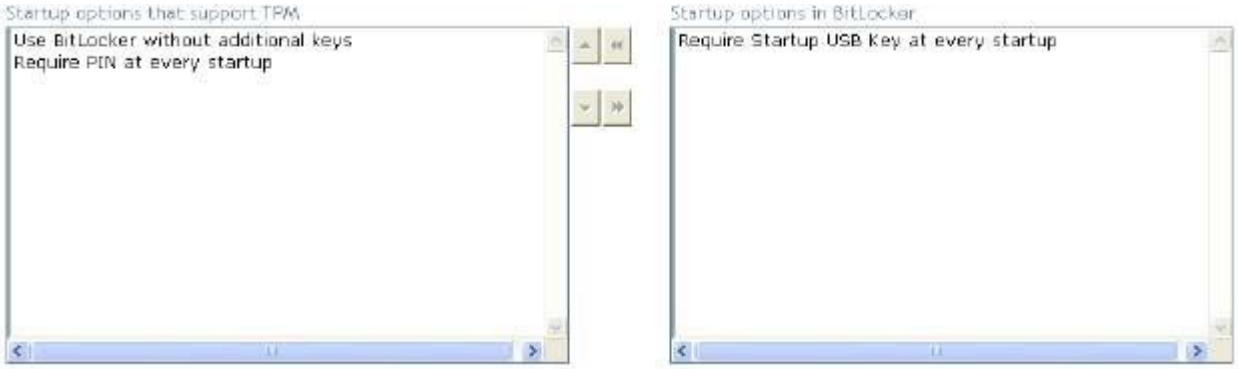
Exam A

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.

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:



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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A stealth virus is a file virus. It infects the computer and then hides itself from detection by antivirus software. It uses various mechanisms to avoid detection by antivirus software. It hides itself in computer memory after infecting the computer. It also masks itself from applications or utilities. It uses various tricks to appear that the computer has not lost any memory and the file size has not been changed. The virus may save a copy of original and uninfected data. When the anti-virus program tries to check the files that have been affected, the virus shows only the uninfected data. This virus generally infects .COM and .EXE files. Answer: B is incorrect. A boot sector virus infects the master boot files of the hard disk or floppy disk. Boot record programs are responsible for booting the operating system and the boot sector virus copies these programs into another part of the hard disk or overwrites these files. Therefore, when the floppy or the hard disk boots, the virus infects the computer.
Answer: C is incorrect. A macro virus is a virus that consists of a macro code which infects the system. A Macro virus can infect a system rapidly. Since this virus has VB event handlers, it is dynamic in nature and displays random activation. The victim has only to open a file having a macro virus in order

to infect the system with the virus. DMV, Nuclear, and Word Concept are some good examples of macro viruses.

Answer: A is incorrect. The EICAR (EICAR Standard Anti-Virus Test File) virus is a file that is used to test the response of computer antivirus (AV) programs. The rationale behind it is to allow people, companies, and antivirus programmers to test their software without having to use a real computer virus that could cause actual damage should the antivirus not respond correctly. The file is simply a text file of either 68 or 70 bytes that is a legitimate executable file called a COM file that can be run by Microsoft operating systems and some work-alikes (except for 64-bit due to 16-bit limitations), including OS/2. When executed, it will print "EICAR- STANDARD-ANTIVIRUS-TEST-FILE!" and then stop. The string used in the EICAR virus is as follows:

QUESTION 10
Which of the following states that a user should never be given more privileges than are required to carry out a task?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The principle of least privilege states that a user should never be given more privileges than are required to carry out a task. The user should not be logged on as an administrator, if the user is not doing administrative work on a computer. The administrator account should be used for performing tasks, such as changing system time, installing software, or creating standard accounts. Answer: D is incorrect. Role-based security provided by the .NET Framework allows, grants, or denies access to resources based on a Windows user's identity. It is built on the principle that the user is authenticated and can be authorized or assigned roles and permissions.
Answer: B is incorrect. Segregation of duties is used to determine whether decision-making, executive tasks, or control tasks are carried out by a person to avoid unauthorized or unintended changes or the misuse of the organization's assets. Whether the person needs access to information can also be determined. The risk of information being intentionally or unintentionally used, altered, or destroyed is increased by unnecessary access. It is called the 'need to know' principle. Answer: A is incorrect. Security through obscurity is a principle in security engineering, which attempts to use secrecy (of design, implementation, etc.) to provide security. A system relying on security through obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe that the flaws are not known, and that attackers are unlikely to find them.

QUESTION 11
Which of the following are the major components of the IPsec protocol? Each correct answer represents a complete solution. Choose all that apply.

A. Encapsulating Security Payload (ESP)
B. Authentication Header (AH)

C. Internet Encryption Key (IEK)
D. Internet Key Exchange (IKE)

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Answer: B, A, and D

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

QUESTION 12
Which of following is required to be configured to ensure that the Bitlocker storage can be reclaimed?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 13
The stronger password is a critical element in the security plan. Which of the following are the characteristics used to make up a strong password?

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

C. It contains the user name, real name, or any name that can be remembered easily and does not contain more than seven characters.
D. It contains more than seven characters and the user name, real name, or any name.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 14
Which of the following can be installed and configured to prevent suspicious emails from entering the user's network?

A. Kerberos
B. Single sign-on (SSO)
C. TCP/IP protocol
D. Microsoft Forefront and Threat Management Gateway

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 15
Which of the following are types of password policies of Windows 7? Each correct answer represents a complete solution. Choose all that apply.

A. Store Password Using Reversible Encryption
B. Minimum Password Length
C. User Name Length

D. Password Must Meet Complexity Requirements

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Answer: B, A, and D

Explanation:
Password policies are account policies that are related to user accounts. These policies increase the effectiveness of users' passwords by enforcing different types of controls on their usage. In Windows
7, there are following six types of password policies that can be configured by administrators: Enforce Password History
Maximum Password Age Minimum Password Age Minimum Password Length Password Must Meet Complexity Requirements
Store Password Using Reversible Encryption
These options are disabled by default. However, an administrator can enable any option in the Local Security Settings tool, which can be accessed from the Administrative tools window found under Control Panel. Answer: C is incorrect. User name length does not come under password policies.

QUESTION 16
Which of the following is a technique used to attack an Ethernet wired or wireless network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing
(APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The attack can only be used on networks that actually make use of ARP and not another method of address resolution. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN. Generally, the aim is to associate the attacker's MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly sent to the attacker instead. The attacker could then

choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it. ARP spoofing attacks can be run from a compromised host, or from an attacker's machine that is connected directly to the target Ethernet segment.

Answer: C is incorrect. Mail bombing is an attack that is used to overwhelm mail servers and clients by sending a large number of unwanted e-mails. The aim of this type of attack is to completely fill the recipient's hard disk with immense, useless files, causing at best irritation, and at worst total computer failure. E-mail filtering and properly configuring email relay functionality on mail servers can be helpful for protection against this type of attack. Answer: B is incorrect. DNS poisoning is the process in which a DNS server may return an incorrect IP address, diverting traffic to another computer. Answer: D is incorrect. Keystroke logging is a method of logging and recording user keystrokes. It can be performed with software or hardware devices. Keystroke logging devices can record everything a person types using his keyboard, such as to measure employee's productivity on certain clerical tasks. These types of devices can also be used to get usernames, passwords, etc.

QUESTION 17
You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. You want to configure Network Access Protection (NAP) on your network. You want that the clients connecting to the network must contain certain configurations. Which of the following Windows components ensure that only clients having certain health benchmarks access the network resources? Each correct answer represents a part of the solution. Choose two.

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Answer: B and D

Explanation:
The System Health Agents (SHA) and System Health Validators (SHV) are the components of Windows Server 2008 to validate a computer's health against a configured set of security benchmarks. These components are parts of Network Access Protection deployed on a network. The SHV component specifies which benchmarks the client must meet. The SHA component specifies configuration against those benchmarks that are being tested. They ensure that computers accessing resources on the network meet certain client health benchmarks.

Answer: A is incorrect. Windows firewall is used to prevent network from unauthorized access. It can be one of the benchmarks configured for health checkup. Answer: E and C are incorrect. TS Gateway and Terminal Service are not used to enforce configurations specified in the

QUESTION 18
You work as a Network Administrator for Tech Perfect Inc. The company has a Windows 2008 Active Directory-based network. All client computers on the network run Windows Vista Ultimate. You have configured a Dynamic DNS (DDNS) on the network. There are a lot of mobile users who often connect to and disconnect from the network. Users on the network complain of slow network responses. You suspect that the stale records on the DNS server may be the cause of the issue. You want to remove the stale records. Which of the following technologies will you use to accomplish the task?

A. RODC
B. Aging
C. Scavenging
D. Forwarding

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In DNS, with dynamic updates enabled, resource records (RRs) are automatically added to zones when computers start on the network or connect to the network. In some cases, these records are not automatically removed when computers leave the network. These stale records fill up the DNS zone and adversely affect the performance of the DNS server. Scavenging is the process of removing these stale records from the DNS zone.
Answer: B is incorrect. Aging is a process in which resource records (RRs) in a DNS zone get aged according to their time stamp and DNS settings. These aged (stale) records get deleted during the scavenging of the DNS zone. Manually added records on the DNS zone do not get aged by default.
Answer: A 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.
Answer: D is incorrect. Forwarding is a technique in which DNS servers on the network are configured to send DNS queries to a particular DNS server.

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:
Explanation:
Eavesdropping is the process of listening to private conversations. It also includes attackers listening the network traffic. For example, it can be done over telephone lines (wiretapping), email, instant messaging, and any other method of communication considered private.
Answer: C is incorrect. Sanitization is the process of removing sensitive information from a document or other medium so that it may be distributed to a

broader audience. When dealing with classified information, sanitization attempts to reduce the document's classification level, possibly yielding an unclassified document. Originally, the term sanitization was applied to printed documents; it has since been extended to apply to computer media and the problem of data remanence as well.
Answer: D is incorrect. Hacking is a process by which a person acquires illegal access to a computer or network through a security break or by implanting a virus on the computer or network.
Answer: B is incorrect. Subnetting is a process through which an IP address network is divided into smaller networks. It is a hierarchical partitioning of the network address space of an organization into several subnets. Subnetting creates smaller broadcast domains. It helps in the better utilization of the bits in the Host ID.

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:
Explanation:

Domain isolation is a Windows configuration option that enables administrators to restrict communication among domain members only. Domain isolation enforces a policy that restricts domain member computers to only accept incoming communication requests from the members of the same domain. When domain isolation is implemented, domain members can initiate communication with hosts outside the domain. However, hosts from outside the network cannot initiate communication with domain members.
Answer: B is incorrect. Server isolation is a Windows Server 2008 configuration option to isolate a specific set of servers in a domain. These set of computers are prevented from being accessed by any computer outside the domain. When server isolation is implemented, only computer those are members of the domain are able to communicate with the isolated servers. Server isolation is usually implemented by placing a set of servers in a specific organizational unit (OU) and applying connection security rule to the OU through a group policy object (GPO). Answer: D 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: A is incorrect. The Demilitarized zone (DMZ) or perimeter network is a small network that lies in between the Internet and a private network. It is the boundary between the Internet and an internal network, usually a combination of firewalls and bastion hosts that are gateways between inside networks and outside networks. DMZ provides a large enterprise network or corporate network the ability to use the Internet while still maintaining its security.

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:
Answer: C and A

Explanation:
It is required to enable User Account Control on all Windows 7 computers and to configure software restriction policies to prevent the users from downloading and installing software from the Internet.

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:
Explanation:
The Windows firewall has an exception list of applications and ports that are allowed to pass through the firewall. Find this port and remove it from the exception list.

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:
Explanation:
Group Policy is a feature of the Microsoft Windows NT family of operating systems. It is a set of rules, which control the working environment of user accounts and computer accounts. Group Policy provides the centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. Group Policy is often used to restrict certain actions that may pose potential security risks. For example, block access to the Task Manager, restrict access to certain folders, disable the downloading of executable files, and so on. As part of Microsoft's IntelliMirror technologies, Group Policy aims to reduce the cost of supporting users. IntelliMirror technologies relate to the management of disconnected machines or roaming users and include roaming user profiles, folde redirection, and offline files.

Answer: A is incorrect. Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as "secret", he cannot grant permission to other users to see this object unless they have the appropriate permission.
Answer: D is incorrect. An Intrusion detection system (IDS) is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet. It can detect several types of attacks and malicious behaviors that can compromise the security of a network and computers. This includes network attacks against vulnerable services, unauthorized logins, and access to sensitive data, and malware (e.g. viruses, worms, etc.). An IDS also detects attacks that originate from within a system. In most cases, an IDS has three main components: Sensors, Console, and Engine. Sensors generate security events. A console is used to alert and control sensors and to monitor events. An engine is used to record events and to generate security alerts based on received security events. In many IDS implementations, these three components are combined into a single device. Basically, the following two types of IDS are used:
Network-based IDS Host-based IDS
Answer: B is incorrect. Access control list (ACL) is a rule list containing access control entries. It is used to allow or deny access to network resources. ACL can be implemented on network users and network devices such as routers and firewalls. Routers and firewalls use ACL to determine which packets should be forwarded or dropped.

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:
Explanation:
The default security level of the Local intranet zone is Medium-Low. Internet Explorer (IE) allows configuring different levels of security for different types of Web sites by segmenting them into the following security zone:
Local Intranet: IE can be configured to detect intranet sites automatically. Users can add Web sites to this zone through Local Intranet sites dialog box. Protected Mode is not enabled for sites in this zone. The default security level of this zone is Medium- Low.
Trusted Sites: Putting sites in the Trusted Sites zone often provide elevated privileges. The default security level for this zone is Medium. Restricted Sites: Potentially malicious sites are put in this zone. The default security level for this zone is High. Protected Mode is enabled by default for sites in this zone. Internet: The sites that are not contained in other zones are automatically hosted in this zone. Sites in this zone are blocked from viewing private data from other Web sites. The default security level of this zone is Medium-High. Protected Mode is enabled by default for sites in this zone.
The three default security levels are Medium, Medium-High, and High.

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:

Explanation:
To be sure that the team members are on a secure site, they are required to look for a padlock in the lower right corner of the browser and https:// in the address bar. It will not guarantee that the site is secure but can be used. Answer: D is incorrect. The Internet zone feature in IE 8 can be configured and users are enabled to easily browse the local intranet without disturbing the security levels by using the following steps:
1.Go into the Internet Options and select the Security. 2.Add the intranet site to the list of Local Intranet Site. Answer: C is incorrect. Social engineering can be defined as any type of behavior used to inadvertently or deliberately aid an attacker in gaining access to an authorized user's password or other sensitive information. Social engineering is the art of convincing people and making them disclose useful information such as account names and passwords. This information is further exploited by hackers to gain access to a user's computer or network. This method involves mental ability of people to trick someone rather than their technical skills. A user should always distrust people who ask him for his account name, password, computer name, IP address, employee ID, or other information that can be misused. Answer: B While stressing the Con?dentiality, Integrity, and Availability triangle in the training of users, the process of providing availability is related to security training to ensure the protection against a Distributed Denial of Services attack.

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:
Explanation:
The group policies are used to disable the use of floppy drives or USB drives to ensure physical security of desktop computers. Several computers are able to use the mechanism of attaching a locking device to the desktops, but disabling USB and floppy drives can disable a larger set of threats. Answer: D is incorrect. While stressing the Con?dentiality, Integrity, and Availability triangle in the training of users, the process of providing availability is related to security training to ensure the protection against a Distributed Denial of Services attack.

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:
Explanation:
Network Access Protection (NAP) is a set of operating system components included with the Windows Server 2008 and Windows Vista/7 operating systems. It ensures that the client computers on a private network meet administrator-defined requirements for system health. NAP policies define the required configuration and update status for a client computer's operating system and critical software. For example, an administrator can set policies that computers might be required to have antivirus software with the latest virus definition installed and current operating system updates. Using NAP, a network administrator can enforce compliance with health requirements for the client computers connection to the network. NAP helps network administrators to reduce the risk caused by improperly configured client computers that might be exposed to viruses and other malicious software. It is required to define exceptions in NAP for those devices that are not compatible with NAP.

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:
Explanation:
A group is a collection or list of user accounts or computer accounts. Groups can be used to simplify administration, especially when assigning rights and permissions. Answer: B is incorrect. Active Directory is a centralized and standardized system that is available with the Windows Server 2008 platform. Active Directory stores information in a central database and allows users to have a single user account called "domain user account" for the network. Active Directory helps to automate network management of user data, security, and distributed resources, thereby enabling interoperation with other directories. Active Directory is Microsoft's trademarked directory service, an integral part of the Windows architecture. This directory is especially designed for distributed networking environments. Answer: C is incorrect. In the Windows environment, a domain is a set of network resources that are part of a network and share a common directory database. A domain is administered as a unit with common rules and procedures. Each domain has a

unique name. Users just have to log on to a domain to access the network resources within it.
Answer: D is incorrect. A public folder is a storage area on public information store. It is used to collect, organize, and share information among users in an organization. It provides a permanent storage place. Moreover, it can be used to post information on an electronic bulletin board and store sharable items, i.e., calendars and contacts, etc. A public folder can be created and configured in an Exchange organization by administrators and other users who have sufficient access permissions.

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:
Explanation:

The protected mode feature of IE 7+ prevents a computer from saving the files or programs of a Web site. The Protected mode makes it more difficult for malware to be installed. In case such a program is installed, it makes it difficult for the program to damage a user's file and the other operating system files. Protected mode is enabled by default for Internet, local intranet, and restricted sites. However, it is not enabled for the trusted sites.
Answer: B is incorrect. The Phishing filter of IE 7+ provides protection from online phishing attacks, frauds, and spoofed Web sites. The filter helps determine whether a Web site is a legitimate site or a phishing site. The filter blocks the Web sites and cautions the users about both reported and suspected phishing Web sites. Answer: D is incorrect. A pop-up blocker allows users to block most pop-ups while surfing the Internet on their computers. Users can select the level of blocking; hey can either block all pop-up windows, or allow pop-ups that they want to see.
Answer: A is incorrect. IE 7+ provides a user the facility of configuring security through the security zones. It allows a user or systems administrator to categorize Web sites that a user visits into several groups with a suitable security level.

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:
Explanation:
A polymorphic virus has the ability to change its own signature at the time of infection. This virus is very complicated and hard to detect. When the user runs the infected file in the disk, it loads the virus into the RAM. The new virus starts making its own copies and infects other files of the operating system. The mutation engine of the polymorphic virus generates a new encrypted code, thus changing the signature of the virus. Therefore, polymorphic viruses cannot be detected by signature-based antivirus. Answer: A is incorrect. A macro virus is a virus that consists of a macro code which infects the system. A Macro virus can infect a system rapidly. Since this virus has VB event handlers, it is dynamic in nature and displays random activation. The victim has only to open a file having a macro virus in order to infect the system with the virus. DMV, Nuclear, and Word Concept are some good examples of macro viruses. Answer: C is incorrect. A Master boot record (MBR) virus replaces the boot sector data with its own malicious code. Every time when the computer starts up, the boot sector virus executes. It can then generate activity that is either annoying (system will play sounds at certain times) or destructive

(erase the hard drive of the system). Because the code in the Master Boot Record executes before
any operating system is started, no operating system can detect or recover from corruption of the Master Boot Record.
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.

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:
Explanation:
A personal identification number (PIN) is a secret numeric password shared between a user and a system for authenticating the user to the system.
Answer: A is incorrect. Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.
Answer: C is incorrect. In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages.

Answer: B is incorrect. A Public Key is known commonly to everybody. It is used to encrypt data. Only specific users can decrypt it. Data encryption is used to encrypt data so that it can only be decrypted with the corresponding private key owned by the public key owner. The public key is also used to verify digital signatures. This signature is created by the associated private key.

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:
Explanation:
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. Answer: C is incorrect. Windows Server Update Services (WSUS) is an add- on component of Windows Server 2008. It provides functionality to a server to run as a Windows Update server in a Windows network environment. Administrators can configure a WSUS server as the only server to download updates from Windows site, and configure other computers on the network to use the server as the source of update files. This will save lots of bandwidth as each computer will not download updates individually. WSUS 3.0 SP1 is the only version of WSUS that can be installed on Windows Server 2008. Earlier versions of WSUS cannot be installed on a server running Windows Server 2008.
Answer: D is incorrect. DNS dynamic update is used to enable DNS client computers for registering and dynamically updating their resource records with a DNS server whenever any modification or change has been taken place. It is used to update the DNS client computers with the reflecting changes. Answer: B is incorrect. Microsoft Baseline Security Analyzer (MBSA) is a software tool of Microsoft to determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server, and Microsoft Office macro settings. Microsoft Baseline Security Analyzer (MBSA) includes a graphical and command line interface that can perform local or remote scans of Windows systems.

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:
Explanation:
User Account Control (UAC) is used to prevent unauthorized changes to computers on the domain
Answer: B is incorrect. Kerberos is defined as a secure method used for authenticating a request for a service in a computer network. Answer: D is incorrect. The Lightweight Directory Access Protocol (LDAP) is defined as a directory service protocol that is used to provide a mechanism used to connect to, search, and modify Internet directories. Answer: A is incorrect. TCP/IP protocol is used to define the rule computers are required to follow for communicating with each other over the internet.

QUESTION 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:
Explanation:
A public certificate is defined as a digitally signed statement used to authenticate and to secure information on open networks
Answer: C is incorrect. Single sign-on (SSO) is defined as a mechanism in which a single action of user authentication and authorization is used to allow a user to access all computers and systems where he got a access permission, without entering passwords for multiple times.
Answer: A is incorrect. Kerberos is defined as a secure method used for authenticating a request for a service in a computer network. Answer: D is incorrect. SEAL is an alternative encryption algorithm to software- based DES, 3DES, and AES. It uses a 160-bit encryption key. SEAL provides less impact to the CPU than other software- based encryption algorithms. In Cisco IOS IPSec implementations, SEAL supports the SEAL algorithm. It can be configured

through the command-line interface using the crypto ipsec transform-set command and the esp-seal transform option.

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:
Explanation:
The network layer defines the mechanisms that allow data to be passed from one network to another.
Answer: B is incorrect. The session layer is responsible for data synchronization between the applications on the sending device and the receiving device. Answer: C is incorrect. The physical layer is the lowest layer of the OSI model. The physical layer is responsible for packaging and transmitting data over physical media. This layer controls the way in which data is sent and received over a physical medium.
Answer: D is incorrect. The data-link layer is responsible for error free transfer of data frames.

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:
Answer: B and D

Explanation:
For security, you will have to rename the Administrator account and disable the Guest account. Renaming the Administrator account will ensure that hackers do not break

into the network or computer by guessing the password of the Administrator account. You can also create a fake Administrator account that has no privileges and audit its use to detect attacks. Disabling the Guest account will prevent users who do not have a domain or local user account from illegally accessing the network or computer. By default, the Guest account is disabled on systems running Windows 2000 Server. If the Guest account is enabled, you will have to disable it.

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:
Explanation:
Identity spoofing (IP address spoofing) will occur when the attacker wants to use an IP address of a network, computer, or network component without being authorized for this task. It allows the unprivileged code to use someone else's identity, and use their security credentials
Answer: B is incorrect. A honey pot is a computer that is used to attract potential intruders or attackers. It is for this reason that a honey pot has low security permissions. A honey pot is used to gain information about the intruders and their attack strategies.
Answer: C is incorrect. RIP and SAP are used to broadcast network information in a regular way regardless of no changes in the routing or service tables. RIP/SAP spoofing method is used to intercept the SAP and RIP broadcasts by using a spoofing modem/router, and then re-broadcast network information via its own routing table or service table.
Answer: A is incorrect. In the distributed denial of service (DDOS) attack, an attacker uses multiple computers throughout the network that it has previously infected. Such computers act as zombies and work together to send out bogus messages, thereby increasing the amount of phony traffic. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down. TFN, TRIN00, etc. are tools used for the DDoS attack.

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:
Explanation:
Configuring the settings on the Web browser will enable a computer to ask for confirmation before installing an ActiveX component. This will enable users to prevent the download of potentially unsafe controls onto the computer. ActiveX controls are software components that can be integrated into Web pages and applications, within a computer or among computers in a network, to reuse the functionality. Reusability of controls reduces development time of applications and improves program interfaces.
They enhance the Web pages with formatting features and animation. ActiveX controls can be used in applications written in different programming languages that recognize Microsoft's Component Object Model (COM). These controls always run in a container. ActiveX controls simplify and automate the authoring tasks, display data, and add functionality to Web pages.
Answer: A and D are incorrect. Configuring a firewall or DMZ will not help in accomplishing the task.

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:
Answer: D and B

Explanation:
A biometric device is used for uniquely recognizing humans based upon one or more intrinsic, physical, or behavioral traits. Biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.
Biometric characteristics can be divided into two main classes:

1.Physiological: These devices are related to the shape of the body. These are not limited to the fingerprint, face recognition, DNA, hand and palm geometry, and iris recognition, which has largely replaced the retina and odor/scent. 2.Behavioral: These are related to the behavior of a person. They are not limited to the typing rhythm, gait, and voice.
Answer: A and C are incorrect. These are not the classes of biometric characteristics.

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:
Explanation:
The advantage of using Hyper-V on Windows Server 2008 is that a user can use many of the services offered with the Windows Server 2008 environment. One such service is the Network Access Protection (NAP) feature, which allows you to quarantine machines that do not meet specific network or corporate policies. The noncompliant machines will not be allowed to access the network utility unless and until they comply with the organization's policies.

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:
Explanation:
Port 143 is used by the IMAP4 protocol.
Answer: A is incorrect. Port 443 is used by the HTTPS protocol.

Answer: B is incorrect. Port 53 is used by DNS. Answer: D is incorrect. Port 110 is used by the POP3 protocol.

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:
Explanation:
The level of security set for the restricted sites is applied to the sites that might potentially damage your computer, or your information. Answer: D is incorrect. The level of security set for an Internet zone is applied to all the Websites by default.
Answer: B is incorrect. The level of security set for trusted sites is applied to the sites that you have specifically indicated as the ones that you trust.
Answer: C is incorrect. The level of security set for the local intranet zone is applied to the Websites and content that are stored on a corporate or business network.

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:
Explanation:
In order to prevent users from accessing the graphical user interface (GUI) on the computers in the network, you will have to implement a group policy. A group policy that is created by an administrator affects all users on a computer or all users on a domain. Group policies can be used for defining, customizing, and controlling the functioning of network resources, computers, and operating systems. They can be set for a single computer with multiple users, for users in workgroups, or for computers in a domain. Administrators can configure group

policy settings for users as well as for computers in many ways. Group policies can be used to allow or restrict the access of a particular program by a particular user. It can also be used to configure the desktop, the Start menu, the taskbar, the Control Panel, security settings, among other things. In Windows XP, group policies can be configured by using the Group Policy Console dialog box, which can be opened by running the GPEDIT.MSC command from the Start menu. Answer: D is incorrect. An account policy controls the password expiration policy, the lockout policy, and other password features. Answer: A is incorrect. A remote access policy specifies how remote users can connect to the network and the requirements for each of their systems before they are allowed to connect. It defines the methods users can use to connect remotely such as dial up or VPN. This policy is used to prevent damage to the organizational network or computer systems and to prevent compromise or loss of data. Answer: C is incorrect. Applying NTFS permission will not help in accomplishing the task.

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:
Explanation:
A logic bomb is malware that executes its malicious activity when a certain condition is met, often when a certain date/time is reached. In this case it waited for the Web server to pass a certain threshold.

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:
Explanation:
Auditing is the process of keeping track of a user's activity while accessing network resources. Auditing is used to track user accounts for file and object access, logon attempts, system shutdown, etc. This enhances the security of the network. Answer: A 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: C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.
Answer: D is incorrect. Biometrics is a method of authentication that uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user. Nowadays, the usage of biometric devices such as hand scanners and retinal scanners is becoming more common in the business environment.

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:
Explanation:
In a NAP infrastructure, authentication is handled using the Extensible Authentication Protocol
(EAP). Extensible Authentication Protocol (EAP) is an authentication protocol that provides support for a wide range of authentication methods, such as smart cards, certificates, one-time passwords, public keys, etc. It is an extension to Point-to-Point Protocol (PPP), which allows the application of arbitrary authentication mechanisms for the validation of a PPP connection.

Answer: C, D, and B are incorrect. The use of PAP, SPAP, and CHAP is not recommended unless it is required. Microsoft recommends using only the strongest authentication protocols required for your configuration.

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:
Explanation:
A honey pot is a device specifically designed to emulate a high value target such as a database server or entire sub section of your network. It is designed to attract the hacker's attention.

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:
Explanation:
The Web browser's Security setting controls the way in which a Web browser receives information and downloads content from Web sites. In Internet Explorer, users can access the Security setting from Tools menu > Internet Options > Security tab page.
Answer: C is incorrect. A cookie is a small bit of text that accompanies requests and pages as they move between Web servers and browsers. It contains information that is read by a Web application, whenever a user visits a site. Cookies are stored in the

memory or hard disk of client computers. A Web site stores information, such as user preferences and settings in a cookie. This information helps in providing customized services to users. There is absolutely no way a Web server can access any private information about a user or his computer through cookies, unless a user provides the information. The Web server cannot access cookies created by other Web servers. Answer: D is incorrect. Proxy server setting is used to connect to the Internet through a proxy server.

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:
Explanation:
To prevent normal users from logging onto the systems, it is required to create a group policy that can be applied to the servers to Deny Log on Locally for all non- administrative users. It will create a problem for the people who are in the data center with physical access. However, normal users should not have the ability to log on locally.
Answer: C While stressing the Con?dentiality, Integrity, and Availability triangle in the training of users, the process of providing availability is related to security training to ensure the protection against a Distributed Denial of Services attack.

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:
Explanation:
An armored virus is designed to stop antivirus researchers from examining its code by using various methods to make tracing and disassembling difficult. This type of virus also protects itself from antivirus programs, making it more difficult to trace. Answer: D is incorrect. A macro virus is a virus

that consists of a macro code which infects the system. A Macro virus can infect a system rapidly. Since this virus has VB event handlers, it is dynamic in nature and displays random activation. The victim has only to open a file having a macro virus in order to infect the system with the virus. DMV, Nuclear, and Word Concept are some good examples of macro viruses. Answer: C 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. The boot sector virus copies these programs into another part of the hard disk or overwrites these files.
Answer: B is incorrect. A Master boot record (MBR) virus replaces the boot sector data with its own malicious code. Every time when the computer starts up, the boot sector virus executes.

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:
Explanation:
A network perimeter 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. In an efficient enterprise security design, the network perimeter offers a great opportunity for enhancing the security position of a network. The network perimeter consists of a Border Network and a Perimeter Network; each assumes an enforcement point within the network perimeter with each having a exclusive responsibility in the perimeter security model.

Answer: C is incorrect. An intranet is a private network that is contained within an enterprise. Intranet is used to share company information and computing resources among employees. It is also used to facilitate working in groups and for teleconferencing. An intranet uses TCP/IP, HTTP, and other Internet protocols. Answer: D is incorrect. A VLAN is a broadcast domain created by a switch. Each broadcast domain connected to interfaces of the switch is known as a separate VLAN. A VLAN should be configured when a LAN has lots of traffic or more than 200 devices. It is also required when groups of users need more security or when a group of users has the same type of work and needs to be on the same broadcast domain. Answer: A is incorrect. Internet is a global network of computers, connected to each other using the TCP/IP protocol. Internet sites are available to all users. The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers). It was conceived by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first known as the ARPANET.
Today, the Internet is a public, cooperative, and self-sustaining facility accessible to hundreds of millions of people worldwide. Physically, the Internet uses a portion of the total resources of the currently existing public telecommunication networks. Technically, what distinguishes the Internet is its use of a set of protocols called TCP/IP (for Transmission Control Protocol/Internet Protocol).

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:
Explanation:

In the above scenario, it is required to implement a VPN server to permit the travel agents remote access without compromising the security because VPN can be used to use several methods of encryption.
Answer: C, and B are incorrect. Wireless Security Options are used to decrease the risk of data interception by a third party in Wireless Networking. Data can be protected by using encryption technologies. In Wireless Networking Connection, various methods are used to increase security as follows:
Using Wired Equivalent Privacy: The goal is to allow only authorized users to connect to the wireless network. While initially configuring routers and network adapters, users create a WEP key. The level of security depends on the length of the key measured in bits. Another step is to share WEP keys to authorized users. Specifically, it is possible for unauthorized users to determine the mathematical value of a WEP key by monitoring a sufficient amount of networking traffic. WEP is an additional security, but it does not completely address all potential vulnerabilities. Using Wi-Fi Protected Access: The Wi-Fi Protected Access protocol is used to provide higher security over the WEP standard. It is considered as a replacement for the less secured WEP protocol. WPA security is configured on a wireless router or an access point.
Using Service Set Identifiers: Service Set Identifiers are used to assist users to find and connect to a wireless network. Whenever a wireless network adapter is available on a computer, Windows Vista automatically identifies the available networks based on their SSID.
Answer: A is incorrect. The principle of least privilege gives a user only those privileges that are essential to do his/her work. In information security, computer science, and other fields, the principle of least privilege, is also known as the principle of minimal privilege or least privilege. It define that in a particular abstraction layer of a computing environment, every module has to be able to access only the information and resources that are essential for its legitimate purpose. It needs that each subject in a system be granted the most restrictive set of privileges required for the authorized tasks.

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:
Answer: D, A, and B

Explanation:
The following practices should be followed to keep passwords secure: Never write down a password.

Change the passwords whenever there is suspicion that they may have been compromised. A password should be alpha-numeric. Never use the same password for more than one account. Never tell a password to anyone, including people who claim to be from customer service or security.
Never communicate a password by telephone, e-mail, or instant messaging. Ensure that an operating system password and application passwords are different. Make passwords completely random but easy for you to remember.

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

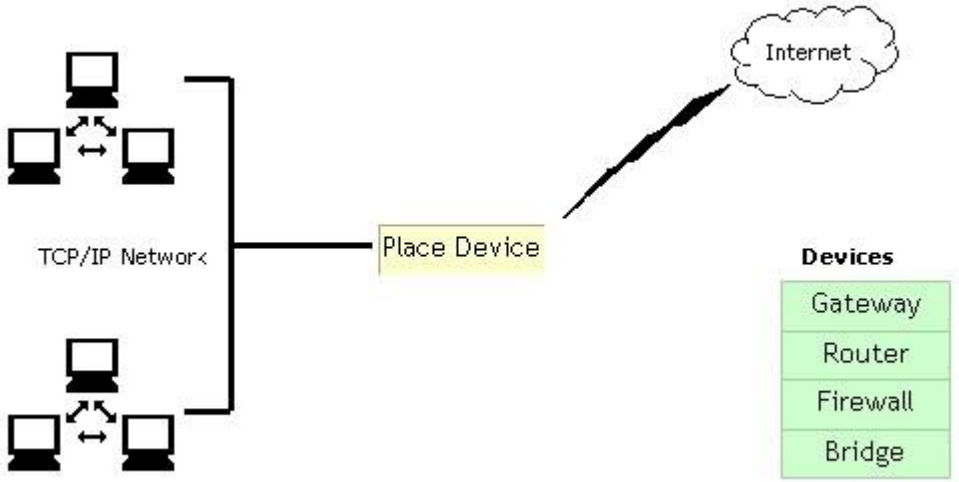
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Spambot is a software program that collects email addresses of users and creates a mailing list. Spam will be sent to the email addresses stored in the mailing list. Answer:
B is incorrect. A cookie is a small piece of text stored on a user's computer by a web browser. A cookie consists of one or more name-value pairs containing bits of information.
The cookie is sent as an HTTP header by a web server to a web browser and then sent back unchanged by the browser each time it accesses that server. A cookie can be used for authentication, session tracking (state maintenance), storing site preferences, shopping cart contents, the identifier for a server-based session, or anything else that can be accomplished through storing textual data. Answer: A is incorrect. A browser is an application that enables a user to view Hypertext Markup Language (HTML) documents on the World Wide Web, on another network, or on his computer. Internet Explorer is an example of a browser application. A browser is also known as a Web browser. Answer: D is incorrect. A perimeter network, also known as a demilitarized zone or DMZ, is positioned between the Internet and the intranet. It protects the network from unauthorized traffic. Servers, routers,

and switches that maintain security by preventing the internal network from being exposed on the Internet are placed in the perimeter network. A firewall is used to protect the perimeter network.

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

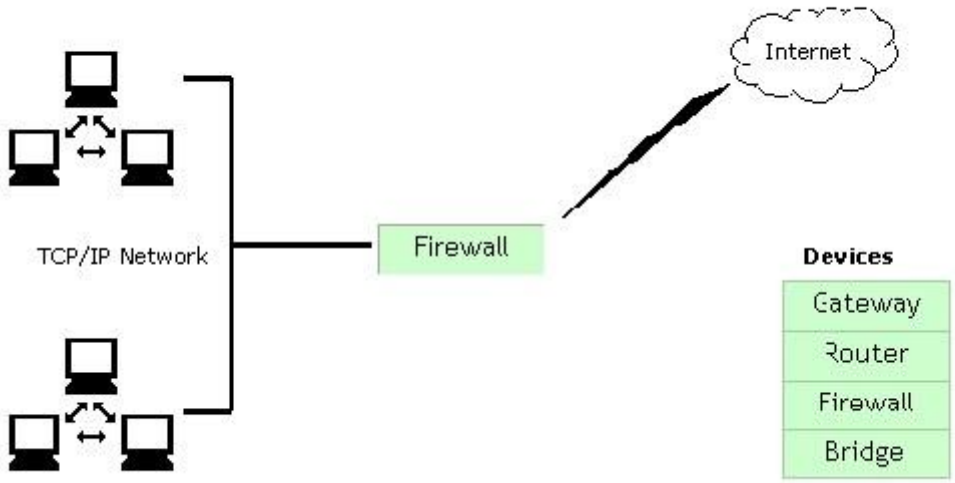
external access and misuse. Which device will you install between your LAN and the Internet to accomplish this?



A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:



Explanation:
You should install a firewall between the LAN and the Internet to protect your LAN against external access and misuse.

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:
Explanation:
The various enabled file auditing events are documented and written in the security event log
Answer: A is incorrect. A filesystem ACL is deifned as a data structure (usually a table) that contains entries specifying individual user or group rights to specific system objects like programs, processes, or files. These entries are known as access control entries (ACEs) in the Microsoft Windows NT,

OpenVMS, Unix-like, and Mac OS X operating systems and each of the accessible object contains an identifier to its ACL. The permissions are used to find the particular access rights, such as whether a user is able to read from, write to, or execute an object. Answer: C is incorrect. Network Access Control List is defined as a set of rules applied to port numbers or network daemon names that are available on a host or other layer 3, and attached with a list of hosts and networks permitted to use the various defined service. The individual servers and routers can have network ACLs. It is used to control both inbound and outbound traffic as firewall does. Answer: B is incorrect. A biometric device is used for uniquely recognizing humans based upon one or more intrinsic, physical, or behavioral traits. Biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance. Biometric characteristics can be divided into two main classes:
1.Physiological: These devices are related to the shape of the body. These are not limited to the fingerprint, face recognition, DNA, hand and palm geometry, and iris recognition, which has largely replaced the retina and odor/scent. 2.Behavioral: These are related to the behavior of a person. They are not limited to the typing rhythm, gait, and voice.

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:
Explanation:
The Phishing filter of IE 7+ provides protection from online phishing attacks, frauds, and spoofed Web sites. The filter helps determine whether a Web site is a legitimate

site or a phishing site. The filter blocks the Web sites and cautions the users about both reported and suspected phishing Web sites. Answer: B is incorrect. A Pop-up blocker allows users to block most pop-ups while surfing the Internet on their computers. The users can select the level of blocking; they can either block all pop- up windows or allow pop-ups that they want to see. Answer: A is incorrect. The protected mode feature of IE 7+ prevents a computer from saving the files or programs of a Web site. The protected mode makes it more difficult for malware to be installed. In case such a program is installed, it makes it difficult for the program to damage a user's file and the other operating system files. Protected mode is enabled by default for Internet, local intranet, and restricted sites. However, it is not enabled for the trusted sites. Answer: C is incorrect. IE 7+ provides a user the facility of configuring security through the security zones. It allows a user or systems administrator to categorize Web sites that a user visits into several groups with a suitable security level.

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:
Explanation:
Sender Policy Framework (SPF) is an e-mail validation system designed to prevent e- mail spam by tackling source address spoofing. SPF allows administrators to specify which hosts are allowed to send e-mail from a given domain by creating a specific SPF record (or TXT record) in the public Domain Name System (DNS). Mail exchangers then use the DNS to check whether that mail from the given domain is being sent by a host sanctioned by that domain's administrators. Answer: A, D, and C are incorrect. These records do not help prevent domain names from being exploited by hackers.

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:
Explanation:
Answer: B is incorrect. SEAL is an alternative encryption algorithm to software- based DES, 3DES, and AES. It uses a 160-bit encryption key. SEAL provides less impact to the CPU than other software- based encryption algorithms. In Cisco IOS IPSec implementations, SEAL supports the SEAL algorithm. It can be configured through the command-line interface using the crypto ipsec transform-set command and the esp-seal transform option.
Answer: A is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. It helps an attacker not only to execute a malicious code on the target system but also to install backdoors on the target system for further attacks. All buffer overflow attacks are due to only sloppy programming or poor memory management by the application developers. The main types of buffer overflows are:
Stack overflow
Format string overflow
Heap overflow
Integer overflow
Answer: D is incorrect. A bot is defined as a program that is used to perform some task on a network especially a task that is repetitive or time-

consuming such as spybot or tracking software that uses other forms of deceptive software and programs conducting some activities on a computer without getting appropriate consent from the users.

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:
Explanation:
A logic bomb is a malicious program that executes when a predetermined event occurs. For example, a logic bomb can execute when a user logs on to a computer or

presses certain keys on the keyboard. It can also execute on a particular date or time specified by developers.
Answer: D is incorrect. Trojan horse is a malicious software program code that masquerades itself as a normal program. When a Trojan horse program is run, its hidden code runs to destroy or scramble data on the hard disk. An example of a Trojan horse is a program that masquerades as a computer logon to retrieve user names and password information. The developer of a Trojan horse can use this information later to gain unauthorized access to computers. Trojan horses are normally spread by e-mail attachments. Unlike viruses, Trojan horses do not replicate themselves but only destroy information on hard disks. Answer: A is incorrect. A keylogger is a software tool that traces all or specific activities of a user on a computer. Once a keylogger is installed on a victim's computer, it can be used for recording all keystrokes on the victim's computer in a predefined log file. An attacker can configure a log file in such a manner that it can be sent automatically to a predefined e-mail address. Some of the main features of a keylogger are as follows:
It can record all keystrokes.
It can capture all screenshots.
It can record all instant messenger conversations. It can be remotely installed.
It can be delivered via FTP or e-mail.
Answer: C is incorrect. Spyware is a computer program that collects all the information on the computer user and sends it to another computer or destination. It is used for monetary gain. It may have several ways of making money by using the information obtained. It tries to violate the privacy of the computer without causing damage to the computer or the software installed on it.

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:
Explanation:
The biometric identification is defined as a use of physical characteristics and traits for identifying individuals. The various methods of biometric identification included fingerprint, handwriting, iris/eye scan, face scan, voice print, and hand print. Some organizations cannot afford it because it requires expensive instruments.

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:
Explanation:
Inheritance is defined as the concept of permissions that are propagated to an object from a parent object. It is found in both file system permissions and Active Directory permissions and does not work with share permissions. It is used to reassign permissions without assigning permissions to every parent and child folder Answer: B is incorrect. Kerberos is defined as a secure method used for authenticating a request for a service in a computer network. Answer: D is incorrect. User Account Control (UAC) is used to prevent unauthorized changes to computers on the domain. Answer: C is incorrect. TCP/IP protocol is used to define the rule computers are required to follow for communicating with each other over the internet.

QUESTION 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:
Explanation:
SHA is a Federal government algorithm created to generate a secure message digest. The Secure Hash Algorithm (SHA) is a cryptographic hash algorithm. It generates a fixed-length digital representation (message digest) of an input data

sequence of any length. The SHA algorithm is very secure, as it is computationally very difficult to find a message that corresponds to a given message digest. In this algorithm, any change to a message will result in a completely different message digest. There are five SHA algorithms: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.
Answer: A is incorrect. Digital Signature Algorithm (DSA) is a United States Federal Government standard or FIPS for digital signatures. DSA is a public key algorithm; the secret key operates on the message hash generated by SHA-1; to verify a signature, one recomputes the hash of the message, uses the public key to decrypt the signature and then compares the results. The key size is variable from 512 to 1024 bits, which is adequate for the current computing capabilities as long as a user uses more than 768 bits.
Answer: B is incorrect. RSA stands for Rivest, Shamir, and Adleman. It is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. Answer: C is incorrect. Triple DES is the common name for the Triple Data Encryption Algorithm
(TDEA). It is so named because it applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The Data Encryption Standard (DES) is a block cipher (a form of shared secret encryption), which is based on a symmetric-key algorithm that uses a 56-bit key. The algorithm was initially controversial with classified design elements, a relatively short key length, and suspicions about a National Security Agency (NSA) backdoor. Triple DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm.

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:
Explanation:
It is required to implement Windows Software Update Services for controlling all Microsoft updates for operating systems and Microsoft product that are currently in use to ensure that the computers have the latest security updates.

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:
Answer: D, A, and C

Explanation:
Following are the types of group scopes:
1.Domain local
2.Global
3.Universal

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 802.1x 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:
Explanation:
In order to accomplish the task, Mark will have to configure all access points as RADIUS clients to Network Policy Server (NPS). Network Access Protection (NAP) is a set of operating system components included with the Windows Server 2008 and Windows Vista/7 operating systems. It ensures that the client computers on a private network meet administrator-defined requirements for system health. NAP policies define the required configuration and update status for a client computer's operating system and critical software. For example, an administrator can set policies that computers might be required to have antivirus software with the latest virus definition installed and current operating system updates. Using NAP, a network

administrator can enforce compliance with health requirements for the client computers connection to the network. NAP helps network administrators to reduce the risk caused by improperly configured client computers that might be exposed to viruses and other malicious software.
Network Policy Server (NPS) is a Remote Authentication Dial-In User Service (RADIUS) server and proxy in Windows Server 2008. It allows administrator to create and enforce network access policies for client health, connection request authentication, and connection request authorization. It can be used to centrally manage network access through a variety of network access servers, including wireless access points, VPN servers, dial-up servers, and 802.1X authenticating switches. NPS can also be used to deploy secure password authentication with Protected Extensible Authentication Protocol (PEAP)-MS-CHAP v2 for wireless connections.
Answer B is incorrect. Distributed file system (Dfs) is a network server component:
that makes it easier for users to find files and resources on distributed enterprise networks. It permits the linking of servers and shares into a simpler, more meaningful name space. Dfs provides improved load sharing and data availability. Answer: A is incorrect. IPSec has nothing to do with the solution. Answer: C is incorrect. Configuring Link-local Multicast Name Resolution (LLMNR) on the network has nothing to do with the solution.

QUESTION 67
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:
Explanation:
Two-factor authentication offers an extra security mechanism above that offered by passwords alone. It is frequently used by mobile users who want to

establish connectivity to a corporate network.

QUESTION 68
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:
The DMZ is an IP network segment that contains resources available to Internet users such as Web servers, FTP servers, e-mail servers, and DNS servers. DMZ provides a large enterprise network or corporate network the ability to use the Internet while still maintaining its security.
Answer: D is incorrect. Virtual local area network (VLAN) is a virtual subnet that is created by switches and supported routers that are VLAN enabled. VLAN is created by tagging the data frames that a switch receives from hosts. Each port on the switch behaves in the same way as an IP subnet and might require routing to communicate with hosts on other VLANs. VLANs can be used to isolate hosts and segments and to control broadcast traffic.
Answer: A is incorrect. VPN stands for virtual private network. It allows users to use the Internet as a secure pipeline to their corporate local area networks (LANs). Remote users can dial-in to any local Internet Service Provider (ISP) and initiate a VPN session to connect to their corporate LAN over the Internet. Companies using VPNs significantly reduce long-distance dial-up charges. VPNs also provide remote employees with an inexpensive way of remaining connected to their company's LAN for extended periods.Answer: B is incorrect. There is no area of a network such as MMZ.

QUESTION 69
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:

Explanation:
To enable DNS dynamic updates in the DHCP server, open the DHCP console, and then, open the Properties dialog box for the DHCP server. Select the Enable dynamic update of the DNS client information check box in the Dynamic DNS tab. Then,

select the Update, according to client request option, to allow the DHCP client computer to update A (host) resource record, and the DHCP server to update the PTR (pointer) resource record.If you want to allow the DHCP server to update both A (host) and PTR (pointer) resource records regardless of the DHCP client computer's request, select Always update forward and reverse lookups option.

QUESTION 70
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:
Answer: C, B, and A

Explanation:
The various features of security level in the Restricted Sites zone are as follows:
1.The default security level is high.
2.Most of the features are disabled.
3.The maximum safeguards are used.
4.The protection against harmful content is provided.

QUESTION 71
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:
Explanation:
A personal identification number (PIN) is a secret numeric password shared between a user and a system for authenticating the user to the system.
Answer: C is incorrect. Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications,

or governments, who may wish to be able to view the contents of encrypted communications.
Answer: B is incorrect. In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages.
Answer: D is incorrect. A Public Key is known commonly to everybody. It is used to encrypt data. Only specific users can decrypt it. Data encryption is used to encrypt data so that it can only be decrypted with the corresponding private key owned by the public key owner. The public key is also used to verify digital signatures. This signature is created by the associated private key.

QUESTION 72
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:
Explanation:
In the above scenario, Mark will create a perimeter network to isolate the servers from the internal network because Internet-exposed servers and devices should not be located in an internal network. They have to be segmented or isolated into a protected part of the network.

QUESTION 73
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:
Explanation:
Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.
Answer: C is incorrect. Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality. Answer: A is incorrect. A honey pot is a computer that is used to attract potential intruders or attackers. It is for this reason that a honey pot has low security permissions. A honey pot is used to gain information about the intruders and their attack strategies.
Answer: D is incorrect. Protocol spoofing is used in data communications for enhancing the performance in situations where an currently working protocol is inadequate. In a computer security context, it refers to several forms of falsification of technically unrelated data.

QUESTION 74
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:
Explanation:
Kerberos is defined as a secure method used for authenticating a request for a service in a computer network.
Answer: D is incorrect. The Lightweight Directory Access Protocol (LDAP) is defined as a directory service protocol that is used to provide a mechanism used to connect to, search, and modify Internet directories. Answer: A is incorrect. TCP/IP protocol is used to define the rule computers are required to follow for communicating with each other over the internet.

Answer: B is incorrect. This is an invalid Answer: .

QUESTION 75
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:
Explanation:
When any of the team members receives a suspicious email containing an embedded hyperlink, Mark suggests them to delete the email and then contact Mark and the customer contact to verify that the email that is sent to him is sent by the authorized customer and never forward this type of email to other team members.

QUESTION 76
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:

Explanation:
The Network Access Protection (NAP) health policies are combination of the following settings:
1.Connection request policies
2.Network policies
3.Health policies
4.Network Access Protection settings Connection request policies are sets of rules that allow the NPS service to determine whether an incoming connection request should be processed locally or forwarded to another RADIUS server. The network policies are sets of rules that specify the circumstances under which connection attempts corresponding to incoming request messages are either authorized or rejected. Health policies are used to specify health requirements in terms of the installed system health validators (SHVs). The Network Access Protection (NAP) settings consist of the configuration of the SHVs installed on the NAP health policy server for health requirements and error conditions, and remediation server groups.

QUESTION 77
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:
Explanation:
The Melissa virus infects Word 97 documents and the NORMAL.DOT file of Word 97 and Word 2000. This macro virus resides in word documents containing one macro named as "Melissa". The Melissa virus has the ability to spread itself very fast by using an e-mail. When the document infected by the Melissa virus is opened for

the first time, the virus checks whether or not the user has installed Outlook on the computer. If it finds the Outlook, it sends e-mail to 50 addresses from the address book of the Outlook. This virus can spread only by using the Outlook. This virus is also known as W97M/Melissa, Kwyjibo, and Word97.Melissa. Answer: C is incorrect. The EICAR (EICAR Standard Anti-Virus Test File) virus is a file that is used to test the response of computer antivirus (AV) programs. The rationale behind it is to allow people, companies, and antivirus programmers to test their software without having to use a real computer virus that could cause actual damage should the antivirus not respond correctly. The file is simply a text file of either 68 or 70 bytes that is a legitimate executable file called a COM file that can be run by Microsoft operating systems and some work-alikes (except for 64-bit due to 16-bit limitations), including OS/2. When executed, it will print "EICAR- STANDARD-ANTIVIRUS-TEST-FILE!" and then stop. The string used in the EICAR virus is as follows:
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST- FILE!$H+H*
Answer: A is incorrect. The Chernobyl (CIH) virus is a good example of a dual payload virus. Since the first payload of the virus changes the first megabyte of a computer's hard drive to zero, the contents of the partition tables are deleted, resulting in the computer hanging. The second payload of CIH replaces the code of the flash BIOS with garbage values so that the flash BIOS is unable to give a warning, the end result being that the user is incapable of changing the BIOS settings. CIH spreads under the Portable Executable file format under Windows 95, Windows 98, and Windows ME.
Answer: B is incorrect. Brain, the first computer virus, was written in January 1986. It was written by two Pakistani brothers (Basit and Amjad Farooq Alvi) to protect their medical software from piracy. It infects the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system. The virus is also known as Lahore, Pakistani, Pakistani Brain, Brain-A, and UIUC. Brain affects the computer by replacing the boot sector of a floppy disk with a copy of the virus. The real boot sector is moved to another sector and marked as bad. Infected disks usually have five kilobytes of bad sectors.

QUESTION 78
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 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:
Explanation:
The principle of least privilege gives a user only those privileges that are essential to do his/her work. In information security, computer science, and other fields, the principle of least privilege, is also known as the principle of minimal privilege or least privilege. It define that in a particular abstraction layer of a computing environment, every module has to be able to access only the information and resources that are essential for its legitimate purpose. It needs that each subject in a system be granted the most restrictive set of privileges required for the authorized tasks.

QUESTION 79
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:
Explanation:
Microsoft Windows Malicious Software Removal Tool is used to remove the malware.
Answer: D is incorrect. A bot is defined as a program that is used to perform repetitive or time- consuming task on a network. Answer: A is incorrect. Rootkit is used to gain unauthorized remote access to a computer and launch additional attacks.
Answer: B is incorrect. A worm can automatically distribute itself from one computer to another via network connections.

QUESTION 80
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:
Explanation:
The attack surface is a software environment where codes can be run by unauthenticated users. By improving information security, the attack surface of a system or software can be reduced. Although attack surface reduction helps prevent security failures; it does not mitigate the amount of damage an attacker could inflict once a vulnerability is found.
Answer: B is incorrect. A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers make DoS attacks by sending a large number of protocol packets to a network. The problems caused by a DoS attack are as follows: Saturate network resources.
Disrupt connections between two computers, thereby preventing communications between services.
Disrupt services to a specific computer.
Answer: D is incorrect. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e-mail and other private communications. Sometimes, organizations also snoop their employees legitimately to monitor their use of organizations' computers and track Internet usage.
Answer: A is incorrect. Social engineering is the art of convincing people and making them disclose useful information such as account names and passwords. This information is further exploited by hackers to gain access to a user's computer or network. This method involves mental ability of people to trick someone rather than their technical skills. A user should always distrust people who ask him for his account name, password, computer name, IP address, employee ID, or other information that can be misused.

QUESTION 81
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: B, C, and A

Explanation:
It is very hard to detect a keylogger's activity. Hence, a Network Administrator should take the following steps as countermeasures against software keyloggers:
Actively monitor the programs running on the server. Monitor the network whenever an application attempts to make a network connection. Use commercially available anti-keyloggers, such as PrivacyKeyboard.
Update one's antivirus regularly.
Use on-screen keyboards and speech-to-text conversion software which can also be useful against keyloggers, as there are no typing or mouse movements involved. Keyloggers are programs that run in the background and record each and every keystroke. Keyloggers record computer keystrokes either through hardware or software.
Answer: D is incorrect. This step should not be taken by an administrator as countermeasures against software keyloggers.

QUESTION 82
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:
Explanation:
A sniffer is a software tool that is used to capture any network traffic. Since a sniffer changes the NIC of the LAN card into promiscuous mode, the NIC begins to record incoming and outgoing data traffic across the network. A sniffer attack is a passive attack because the attacker does not directly connect with the target host. This attack is most often used to grab logins and passwords from network traffic. Tools such as Ethereal, Snort, Windump, EtherPeek, Dsniff are some good examples of sniffers. These tools provide many facilities to users such as graphical user interface, traffic statistics graph, multiple sessions tracking, etc. Answer: D is incorrect. A protocol analyzer for particular types of networks is a computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the protocol analyzer captures each packet and, if needed, decodes and analyzes its content according to the appropriate RFC or other specifications.

Answer: A is incorrect. A keylogger is a software tool that traces all or specific activities of a user on a computer. Once a keylogger is installed on a victim's computer, it can be used for recording all keystrokes on the victim's computer in a predefined log file. An attacker can configure a log file in such a manner that it can be sent automatically to a predefined e-mail address. Some of the main features of a keylogger are as follows:
It can record all keystrokes.
It can capture all screenshots.
It can record all instant messenger conversations. It can be remotely installed.
It can be delivered via FTP or e-mail.

Answer: C is incorrect. Key fobs are security devices used by telecommuters to provide one part of a three way match for a user to log on to a secured network.

These are display-only devices that algorithmically generate security codes as part of a challenge/response authentication system. This code usually changes very quickly and is used with the PIN for authentication.

QUESTION 83
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:
Explanation:
A Heuristic antivirus protection solution uses certain behaviors to identify a file as a virus, even if it is not on any known antivirus list.

QUESTION 84
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:
Explanation:
Single sign-on (SSO) is defined as a mechanism in which a single action of user authentication and authorization is used to allow a user to access all computers and systems where he got a access permission, without entering passwords for multiple times.
Answer: C is incorrect. Kerberos is defined as a secure method used for authenticating a request for a service in a computer network. Answer: A is incorrect. TCP/IP protocol is used to define the rule computers are required to follow for communicating with each other over the internet. Answer: B is incorrect. This is an invalid Answer:

QUESTION 85
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:
Explanation:
A polymorphic virus has the ability to change its own signature at the time of infection. This virus is very complicated and hard to detect. When the user runs the infected file in the disk, it loads the virus into the RAM. The new virus starts making its own copies and infects other files of the operating system. The mutation engine of the polymorphic virus generates a new encrypted code, thus changing the signature of the virus. Therefore, polymorphic viruses cannot be detected by signature-based antivirus. Answer: B is incorrect. A Master boot record (MBR) virus replaces the boot sector data with its own malicious code. Every time when the computer starts up, the boot sector virus executes. It can then generate activity that is either annoying (system will play sounds at certain times) or destructive
(erase the hard drive of the system). Because the code in the Master Boot Record executes before any operating system is started, no operating system can detect or recover from corruption of the Master Boot Record.

Answer: D is incorrect. A macro virus is a virus that consists of a macro code which infects the system. A Macro virus can infect a system rapidly. Since this virus has VB event handlers, it is dynamic in nature and displays random activation. The victim has only to open a file having a macro virus in order to infect the system with the virus. DMV, Nuclear, and Word Concept are some good examples of macro viruses. Answer: C 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.

QUESTION 86
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:
Explanation:
Dynamic Network Address Translation (NAT) uses a pool of public IP addresses. Dynamic NAT is a technique that maps an unregistered IP address to a registered IP address from a group of registered IP addresses. It also establishes a one-to-one mapping between unregistered (private) and registered (public) IP addresses, but the mapping varies depending on the registered address available in the IP address pool at the time of connection. Answer: A is incorrect. Static NAT performs a manual translation of one IP address to a different one. Static NAT is typically used to translate the destination IP address in packets that reach to the translation device (such as a router) for LAN. In static translation type, a manual translation is performed between two addresses and possibly port numbers.
Answer: B is incorrect. Port Address Translation (PAT) is also a type of NAT. This type of NAT is used in home networks that are using DSL or cable modems. It is designed to provide Internet access to many internal users through one external address.
Answer: D is incorrect. There is no such type of NAT as Cache NAT.

QUESTION 87
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:
Explanation:
Denial of service (DOS) attack is an attack that is used to poison a network or computer to the point where the system is turned into a unusable state.
Answer A is incorrect. Mail bombing is an attack that is used to overwhelm mail:

servers and clients by sending a large number of unwanted e-mails. The aim of this type of attack is to completely fill the recipient's hard disk with immense, useless files, causing at best irritation, and at worst total computer failure. E-mail filtering and properly configuring email relay functionality on mail servers can be helpful for protection against this type of attack.
Answer: B is incorrect. Pharming is a hacker's attack aiming to redirect a Web site's traffic to another Web site. Pharming can be conducted either by changing the hosts files on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their IP addresses. Incorrect entries in a computer's hosts files are a popular target for malware.
Answer: C is incorrect. Protocol spoofing is used in data communications for enhancing the performance in situations where an currently working protocol is inadequate. In a computer security context, it refers to several forms of falsification of technically unrelated data.

QUESTION 88
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:
Explanation:
A VLAN is a broadcast domain created by a switch. Each broadcast domain connected to interfaces of the switch is known as a separate VLAN. A VLAN should be configured when a LAN has lots of traffic or more than 200 devices. It is also required when groups of users need more security or when a group of users has the

same type of work and needs to be on the same broadcast domain. Answer: D is incorrect. A Virtual Private Network (VPN) is a computer network that is implemented in an additional software layer (overlay) on top of an existing larger network for the purpose of creating a private scope of computer communications or providing a secure extension of a private network into an insecure network such as the Internet.
The links between nodes of a Virtual Private Network are formed over logical connections or virtual circuits between hosts of the larger network. The Link Layer protocols of the virtual network are said to be tunneled through the underlying transport network.
Answer: C is incorrect. A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.
Answer: B is incorrect. Metropolitan Area Network (MAN) represents a network that connects two or more LANs in the same geographic area. A network connecting two different buildings or offices in the same city is an example of a MAN. The LANs involved in a MAN are connected to one another through high-speed connections such as T1, SONET, SDH, etc. A MAN is a hybrid of a LAN and a WAN. A WAN provides low to medium

speed access, whereas a MAN provides high-speed access.

QUESTION 89
Which of the following is an authentication protocol?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Kerberos is an industry standard authentication protocol used to verify user or host identity. Kerberos v5 authentication protocol is the default authentication service for Windows 2000. It is integrated into the administrative and security model, and provides secure communication between Windows 2000 Server domains and clients.

Answer: C is incorrect. Transport Layer Security (TLS) is an application layer protocol that uses a combination of public and symmetric key processing to encrypt data.
Answer: B is incorrect. Lightweight Directory Access Protocol (LDAP) is a protocol used to query and modify information stored within directory services.
Answer: D is incorrect. Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP does not provide confidentiality or encryption. It relies on the protocol being tunneled to provide privacy. It is used to provide secure, low-cost remote access to corporate networks through public networks such as the Internet. Using PPTP, remote users can use PPP- enabled client computers to dial a local ISP and connect securely to the corporate network through the Internet. PPTP has been made obsolete by Layer 2 Tunneling Protocol (L2TP) and IPSec.

QUESTION 90
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: A, B, and C

Explanation:
A keylogger is a software tool that traces all or specific activities of a user on a computer. Once a keylogger is installed on a victim's computer, it can be used for recording all keystrokes on the victim's computer in a predefined log file. An attacker can configure a log file in such a manner that it can be sent automatically to a predefined e-mail address. Some of the main features of a keylogger are as follows:
It can record all keystrokes.
It can capture all screenshots.
It can record all instant messenger conversations. It can be remotely installed.
It can be delivered via FTP or e-mail.
Answer: D is incorrect. It cannot detect viruses.

QUESTION 91
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:
Explanation:
In order to accomplish the task, Mark will have to use IPSec NAP policy between the client computer and the company's network. Using the IPSec NAP policy between client computer and the company's network will provide the strongest security for data transmission. IPSec enforcement provides the strongest form of NAP enforcement. Because this enforcement method uses IPsec, the administrator can define requirements for protected communications on a per-IP address or per- TCP/UDP port number basis.
Answer: A is incorrect. Encrypting File System (Efs) cannot work on the network. Answer: C is incorrect. According to the Question ensure that the data transmission between the client computer and the company's network is as secure as possible. Hence, this solution will not fulfill the requirement.
Answer: D is incorrect. Using DHCP enforcement, DHCP servers and Network Policy Server (NPS) can enforce health policy when a computer attempts to lease or renew an IP version 4 (IPv4) address.

QUESTION 92
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:

Explanation:
In the above scenario, a potential risk is a viruses and malware attack because a VPN does not prevent potential viruses and malware attack on the home computer from being infecting the entire network. Mark can use the Direct Access that is a new feature with Windows 7 and Windows Server 2008 R2, to help in mitigating the potential risks. Answer: C is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. It helps an attacker not only to execute a malicious code on the target system but also to install backdoors on the target system for further attacks. All buffer overflow attacks are due to only sloppy programming or poor memory management by the application developers. The main types of buffer overflows are:
Stack overflow
Format string overflow
Heap overflow
Integer overflow

QUESTION 93
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:
Explanation:
To prevent the use of key loggers in the organization, user is required to ensure that the terminals are locked and to perform a regular inspection of the ports on the systems.
Answer: A While stressing the Con? dentiality, Integrity, and Availability triangle in the training of users, the process of providing availability is related to security training to ensure the protection against a Distributed Denial of Services attack.

QUESTION 94
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:
Explanation:
Microsoft Baseline Security Analyzer is a tool that can be used to evaluate the servers having vulnerabilities that are related to the operating system and installed software Microsoft Baseline Security Analyzer (MBSA) is a software tool of Microsoft to determine security state by assessing missing security updates and less- secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server, and Microsoft Office macro settings. Microsoft Baseline Security Analyzer (MBSA) includes a graphical and command line interface that can perform local or remote scans of Windows systems.
Answer: B is incorrect. Windows Server Update Services (WSUS) is an add- on component of Windows Server 2008. It provides functionality to a server to run as a Windows Update server in a Windows network environment. Administrators can configure a WSUS server as the only server to download updates from Windows site, and configure other computers on the network to use the server as the source of update files. This will save lots of bandwidth as each computer will not download updates individually. WSUS 3.0 SP1 is the only version of WSUS that can be installed on Windows Server 2008. Earlier versions of WSUS cannot be installed on a server running Windows Server 2008.
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.
Answer: A is incorrect. DNS dynamic update is used to enable DNS client computers for registering and dynamically updating their resource records with a DNS server whenever any modification or change has been taken place. It is used to update the DNS client computers with the reflecting

changes.

QUESTION 95

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:
Explanation:
Port 3389 is used by the Remote Desktop Protocol. Answer: B is incorrect. Port 23 is used by the TELNET protocol. Answer: A is incorrect. Port 80 is used by the HTTP protocol. Answer: D is incorrect. Port 110 is used by the POP3 protocol.

QUESTION 96
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:
Explanation:
The Active Directory Sites and Services MMC snap-in console is used to administer the replication of directory data among all sites in an Active Directory Domain Services (AD DS) forest.
Answer: A is incorrect. The Active Directory Domains and Trusts console is used to administer domain trusts, domain and forest functional levels, and user principal name (UPN) suffixes.
Answer: B is incorrect. Active Directory Administrative Center is used to administer and publish information in the directory, including managing users, groups, computers, etc.

Answer: C is incorrect. Group Policy Management Console (GPMC) is used to provide a single administrative tool for managing Group Policy across the enterprise.

QUESTION 97

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)
C. Kerberos

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Virtual Private Network (VPN) is used to create a secured connection over an unsecured network.
Answer: C is incorrect. Single sign-on (SSO) is defined as a mechanism in which a single action of user authentication and authorization is used to allow a user to access all computers and systems where he got a access permission, without entering passwords for multiple times.
Answer: D is incorrect. Kerberos is defined as a secure method used for authenticating a request for a service in a computer network. Answer: A is incorrect. TCP/IP protocol is used to define the rule computers are required to follow for communicating with each other over the internet.

QUESTION 98
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: C, A, and B

Explanation:
Following are the Internet Explorer security zones: Local intranet Trusted sites Internet Restricted sites
Answer: D is incorrect. There is no such Internet Explorer security zone as extranet.

QUESTION 99
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:
Explanation:
The registry is a central, secure database in which Windows stores all hardware configuration information, software configuration information, and system security policies.
The registry is the central storage for all configuration data. It stores Windows operating system configuration, computer hardware configuration, configuration information about Win32-based applications, and user preferences in a hierarchical database file.
Answer: B, C, and D are incorrect. The Program files folder, DLL file, or Configuration file is not a central, secure database in which Windows stores all hardware configuration information, software configuration information, and system security policies.

QUESTION 100
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:
Explanation:
Virtualized Internet browser can protect your operating system from Malware installation from unknown Web sites. It protects the operating system and other

applications from poorly written or buggy code by isolating applications from the operating system.

QUESTION 101
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: B and C

Explanation:
To ensure proper DHCP-DNS integration, Mark must enable dynamic DNS support on the DNS server as well as on the DHCP server. In the Windows 2000 Server, the DHCP service provides support to register and update information for legacy DHCP clients in DNS zones. Legacy clients typically include other Microsoft TCP/IP client computers that were released prior to Windows 2000 like Windows 9x, Windows NT. The DNS-DHCP integration, provided in the Windows 2000 Server, enables a DHCP client that is unable to dynamically update DNS resource records directly to have this information updated in the DNS forward, and reverse lookup zones by the DHCP server. Note: Dynamic integration with the DHCP service is available only with Windows 2000 Server. DNS-DHCP integration is not supported by DHCP servers running under Windows NT Server 4.0 and earlier versions.

QUESTION 102
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: A and D

Explanation:
Network address translation (NAT) is a technique that allows multiple computers to share one or more IP addresses. NAT is configured at the server between a private network and the Internet. It allows the computers in a private network to share a global, ISP assigned address. It reduces the need for globally unique IP addresses. NAT modifies the headers of packets traversing the server. For packets outbound to the Internet, it translates the source addresses from private to public, whereas for packets inbound from the Internet, it translates the destination addresses from public to private.
Answer: B is incorrect. Screened host provides added security by using Internet access to deny or permit certain traffic from the Bastion Host. Answer: C is incorrect. Bastion host allows external network clients access to internal services.

QUESTION 103
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:
Explanation:
To minimize the amount of spam that is hitting the Microsoft Exchange server, it is required to enable reverse DNS lookup on the SMTP virtual server. It forces a system to crosscheck the domain name with a PTR record (IP address associated with the domain name) and if the IP address is not matched the record associated with that domain name, it will not delivered.
Answer: C is incorrect. SPF is used to permit the administrator to configure the server to establish who is acceptable to send email from their domain.
Answer: D is incorrect. User Account Control (UAC) is a technology and security infrastructure introduced with Microsoft's Windows Vista and Windows Server 2008 operating systems, with a more relaxed version also present in Windows 7 and Windows Server 2008 R2. It aims to improve the security of Microsoft Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation.

Answer: B 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 104
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:
Explanation:
An open relay is the most common method for an attacker to spoof email. An open relay is an SMTP mail server configured in such a way that it allows anyone on the Internet to send e-mail through it. By processing mail that is neither for nor from a local user, an open relay makes it possible for a spammer to route large volumes of spam.
Answer: C is incorrect. Man-in-the-middle attacks occur when an attacker successfully inserts an intermediary software or program between two communicating hosts. The intermediary software or program allows attackers to listen to and modify the communication packets passing between the two hosts. The software intercepts the communication packets and then sends the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client.
Answer: A is incorrect. A backdoor is a program or account that allows access to a system by skipping the security checks. Many vendors and developers implement backdoors to save time and effort by skipping the security checks while troubleshooting. A backdoor is considered to be a security threat and should be kept with the highest security. If a backdoor becomes known to attackers and malicious users, they can use it to exploit the system.
Answer: B is incorrect. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet.

QUESTION 105
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:
Explanation:
WIPS is used to detect the DOS attack in order to enhance the security of the network. Wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence ofunauthorized access points (intrusion detection), and can automaticallytake countermeasures (intrusion prevention). The primary purpose of a WIPS is to prevent unauthorized network access to local area networks and other information assets by wireless devices. Answer:
C is incorrect. A wireless LAN controller is a device that is used in combination with Lightweight Access Point Protocol (LWAPP) to manage light weight access points in large quantities by the network administrator or NOC. The wireless LAN controller is a part of the Data Plane within the Cisco Wireless Model. The WLAN controller automatically handles the configuration of anywhere from 6 to 300 wireless access-points, depending on the model.
Answer: D is incorrect. A spectrum analyzer, or spectral analyzer, is a device that is used to examine the spectral composition of some electrical, acoustic, or optical waveform. It may also measure the power spectrum. The analog and digital spectrum analyzers are as follows:
1.An analog spectrum analyzer uses either a variable band-pass filter whose mid- frequency is automatically tuned (shifted, swept) through the range of frequencies of which the spectrum is to be measured.
2.A digital spectrum analyzer computes the discrete Fourier transform (DFT), a mathematical process that transforms a waveform into the components of its frequency spectrum.
Answer: A is incorrect. A protocol analyzer is a network diagnostic utility for viewing the current contents of a packet traveling on the network. Protocol analyzers are mainly used for performance measurement and troubleshooting. These devices connect to the network to calculate key performance indicators (KPI) to monitor the network and speed up troubleshooting activities.

QUESTION 106
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:
Explanation:
The level of security set for an Internet zone is applied to all the Websites by default. Answer: C is incorrect. The level of security set for the restricted sites is applied to the sites that might potentially damage your computer, or your information.

Answer: D is incorrect. The level of security set for the local intranet zone is applied to the Websites and content that are stored on a corporate or

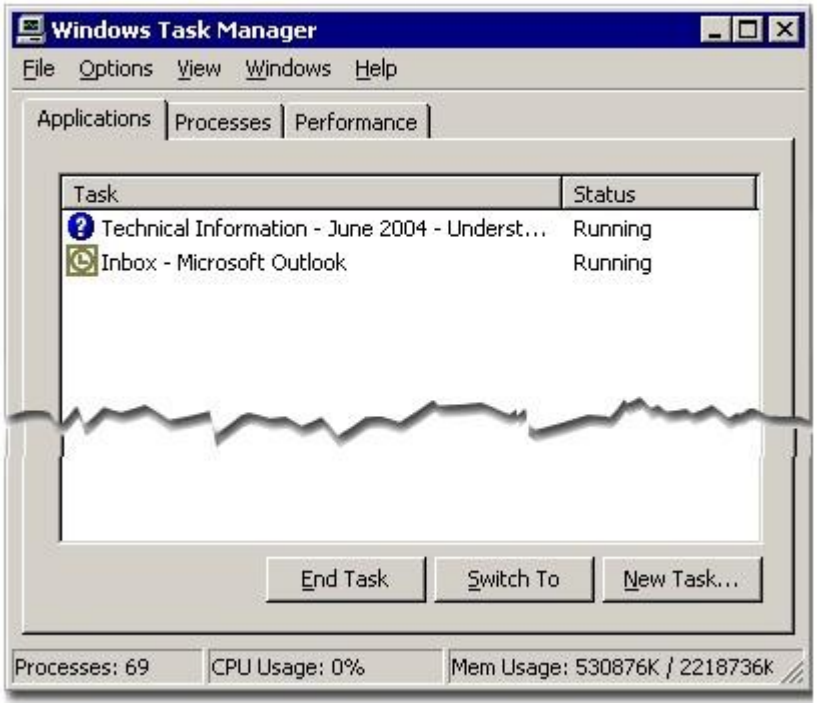
business network. Answer:
A is incorrect. The level of security set for the trusted sites is applied to sites that you have specifically indicated as the ones that you trust.

QUESTION 107
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:
Explanation:
A keylogger is a software tool that traces all or specific activities of a user on a computer. Once a keylogger is installed on a victim's computer, it can be used for recording all keystrokes on the victim's computer in a predefined log file. An attacker can configure a log file in such a manner that it can be sent automatically to a predefined e-mail address. Some of the main features of a keylogger are as follows:
It can record all keystrokes.
It can capture all screenshots.
It can record all instant messenger conversations. It can be remotely installed.
It can be delivered via FTP or e-mail.
Answer: A is incorrect. Task Manager is a utility that is used for managing applications, processes, and the general system performance and also for viewing the networking and user statistics. The Task Manager utility is used to run or end programs or applications. Administrators use this tool to quickly identify and terminate a rogue application.



This utility can be run by invoking a Windows Security menu by using the Ctrl+Alt+Delkey combination and then clicking the Task Manager button or by right- clicking the task bar and then clicking the Task Managermenu option. Answer: B is incorrect. Event Viewer is an administrative utility that displays the event log of a computer running Windows NT. Event Viewer displays the following categories of events:
Error: These events show significant problems, such as loss of data or loss of functionality. Warning: These events are not necessarily significant but indicate possible problems. Information: These events describe the successful operation of an application, driver, or service. Success Audit: These events show successful audited security access attempts.
Failure Audit: These events show failed audited security access attempts. Answer: C is incorrect. Network Monitor (Netmon) is a protocol analyzer. It is used to analyze the network traffic. It is installed by default during the installation of the operating system. It can be installed by using Windows Components Wizard in the Add or Remove Programs tool in Control Panel. Network Monitor is used to perform the following tasks:
1.Capture frames directly from the network.
2.Display and filter captured frames immediately after capture or a later time. 3.Edit captured frames and transmit them on the network.
4.Capture frames from a remote computer.

QUESTION 108
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:
Explanation:
RADIUS is a mechanism that allows authentication of dial-in and other network connections.
RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The Remote Access Server, the Virtual Private Network server, the Network switch with port-based authentication, and the Network Access Server are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server. The RADIUS server is usually a background process running on a UNIX or Windows NT machine.
RADIUS serves three functions:
To authenticate users or devices before granting them access to a network To authorize those users or devices for certain network services To account for usage of those services
Answer: D is incorrect. Single Sign-On is an approach which involves a server that acts as an online certificate authority within a single sign-on system. A single sign-on server will issue digital certificates into the client system, but never stores them. Users can execute programs, etc. with the temporary certificate. It is common to find this solution variety with x.509-based certificates. Answer: B is incorrect. NTFS is a high-performance file system proprietary to Microsoft. NTFS supports file-level security, compression, and auditing. It also supports large volumes and powerful storage solution such as RAID. The latest feature of NTFS is its ability to encrypt files and folders to protect sensitive data. Answer: A is incorrect. A virtual private network (VPN) is a form of wide area network (WAN) that supplies network connectivity over a possibly long physical distance. A virtual private network is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.
A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a tunnel that cannot be entered by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

QUESTION 109

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

B. Reaction based packet inspection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In the above scenario, Mark will use stateful packet inspection because this method is used to inspect the packets as they pass through the connection.

QUESTION 110
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: C and B

Explanation:
Two-factor authentication is defined as a security process that is used to confirm user identities by using two individual factors as follows:
Something they have such as token, smart cards, etc Something they know such as password.

QUESTION 111
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: B and C

Explanation:
In such a situation, when John receives an error message revealing that Kernel32.exe is encountering a problem, he needs to come to the conclusion that his antivirus program needs to be updated, because Kernel32.exe is not a Microsoft file (It is a Kernel32.DLL file.).
Although such viruses normally run on stealth mode, he should examine the process viewer (Task Manager) to see whether any new process is running on the computer or not. If any new process (malicious) is running on the server, he should exterminate that process.
Answer: A and D are incorrect. Since kernel.exe is not a real kernel file of Windows, there is no need to repair or download any patch for Windows Server 2003 from the Microsoft site to repair the kernel.
Note: Such error messages can be received if the computer is infected with malware, such as Worm_Badtrans.b, Backdoor.G_Door, Glacier Backdoor, Win32.Badtrans.29020, etc.

QUESTION 112
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:
Explanation:
MAC address is a physical address stored in the Network Interface card on your system or any other device residing on your network. A Media Access Control (MAC) address is a numerical identifier that is unique for each network interface card (NIC). MAC addresses are 48-bit values expressed as twelve hexadecimal digits, usually divided into hyphen-separated pairs, for example, FF-00-F8-32-13-

19. The MAC address consists of two parts. The first three pairs are collectively known as the Organizationally Unique Identifier (OUI). The remaining part is known as the device ID. The OUI is administered by IEEE. MAC addresses are also referred to as hardware addresses, Ethernet addresses, and universally administered addresses (UAAs).
Answer: D is incorrect. Broadcast address is a special kind of IP address that is used to send packets to all the devices on a same segment of a network. For IP broadcasts, broadcast address is the address in which the host portion of the IP address consists of either all 0's or all 255's. For MAC broadcasts, all of the bet positions in the address are enabled, making the address FFFF.FFFF.FFFF in hexadecimal. Answer: A is incorrect. An IP

address is a four-byte number that uniquely identifies a computer on a TCP/IP network. It is made up of 32 bits of information. These bits are divided into four sections, each section containing one byte (8 bits), also known as an octet. Each node on the TCP/IP network must be assigned a unique IP address. There are two types of IP addresses, i.e., Private and Public. Answer: B is incorrect. I/O address is a communication port between a device and the CPU. The CPU needs a memory address, known as Input/Output (I/O) address, to communicate with any peripheral device. I/O address is a hexadecimal number that the CPU uses to identify a device. I/O address allows the CPU to send instructions to devices installed on the bus slot of a computer. Resources such as I/O addresses, IRQs, and DMAs are configurable aspects of communication between devices inside a PC. Whenever a component, such as a sound card or internal modem is installed in a PC, its I/O address, IRQ, and DMA channels must be correctly configured.

QUESTION 113
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:
Explanation:
Network Access Protection (NAP) is a set of operating system components included with the Windows Server 2008 and Windows Vista/7 operating systems. It ensures that the client computers on a private network meet administrator-defined requirements for system health. NAP policies define the required configuration and update status for a client computer's operating system and critical software. For

example, an administrator can set policies that computers might be required to have antivirus software with the latest virus definition installed and current operating system updates. Using NAP, a network administrator can enforce compliance with health requirements for the client computers connection to the network. NAP helps network administrators to reduce the risk caused by improperly configured client computers that might be exposed to viruses and other malicious software. Answer: C is incorrect. Single sign-on (SSO) is defined as a mechanism in which a single action of user authentication and authorization is used to allow a user to access all computers and systems where he got a access permission, without entering passwords for multiple times.
Answer: B is incorrect. Kerberos is defined as a secure method used for authenticating a request for a service in a computer network. Answer: A is incorrect. TCP/IP protocol is used to define the rule computers are required to follow for communicating with each other over the internet.

QUESTION 114
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:
Explanation:
Social engineering can be defined as any type of behavior used to inadvertently or deliberately aid an attacker in gaining access to an authorized user's password or other sensitive information. Social engineering is the art of convincing people and making them disclose useful information such as account names and passwords. This information is further exploited by hackers to gain access to a user's computer or network. This method involves mental ability of people to trick someone rather than their technical skills. A user should always distrust people who ask him for his account name, password, computer name, IP address, employee ID, or other information that can be misused.

Answer: B is incorrect. The group policies are used to disable the use of floppy drives or USB drives to ensure physical security of desktop computers. Several computers are able to use the mechanism of attaching a locking device to the desktops, but disabling USB and floppy drives can disable a larger set of threats. Answer: D is incorrect. While stressing the Con? dentiality, Integrity, and Availability triangle in the training of users, the process of providing availability is related to security training to ensure the protection against a Distributed Denial of Services attack.

QUESTION 115
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:
Explanation:
The reason of properly securing an audit log is used to ensure that potential hackers becomes unable to delete the event logs for covering their tracks.

QUESTION 116
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:
Explanation:
The policy of maximum password age defines a time duration before a password is required to be changed.

QUESTION 117

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:
Explanation:
UDP is often used for one-to-many communications, using broadcast or multicast IP datagrams. User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths. UDP is sometimes called the Universal Datagram Protocol. Answer: D is incorrect. Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. E-mailing systems use this protocol to send mails over the Internet. SMTP works on the application layer of the TCP/IP or OSI reference model. The SMTP client typically initiates a Transmission Control Protocol (TCP) connection to the SMTP server on the well-known port designated for SMTP, port number 25. However, e-mail clients require POP or IMAP to retrieve mails from e-mail servers.
Answer: B is incorrect. File Transfer Protocol (FTP) is a standard network protocol used to copy a file from one host to another over a TCP/IP-based

network, such as the Internet. FTP is built on a client- server architecture and utilizes separate control and data connections between the client and server applications, which solves the problem of different end host configurations (i.e., Operating System, file names). FTP is used with user-based password authentication or with anonymous user access. Answer: C is incorrect. The Hyper Text Transfer protocol is a standard application-level protocol used to request and transmit files, especially web pages and webpage components, on the World Wide Web. HTTP runs on top of the TCP/IP protocol. Web browsers are HTTP clients that send file requests to Web Servers, which in turn handle the requests via an HTTP service.

QUESTION 118
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:
Explanation:
BitLocker is used to protect all files stored on the drive on which Windows is installed. It encrypts the entire system drive and helps block hackers from accessing the system files they rely on to discover user passwords. BitLocker also prevents hackers from accessing the hard disk by removing it from a computer, and installing it on a different computer. BitLocker does not work for USB Flash Drives. Answer:
A is incorrect. SocketShield provides a protection shield to a computer system against malware, viruses, spyware, and various types of keyloggers. SocketShield provides protection at the following two levels:
1.Blocking: In this level, SocketShield uses a list of IP addresses that are known as purveyor of exploits. All http requests for any page in these domains are simply blocked.
2.Shielding: In this level, SocketShield blocks all the current and past IP addresses that are the cause of unauthorized access.
Answer: B is incorrect. A firewall is a system that helps in preventing access to a system from unauthorized internet or network users. A firewall can be hardware as well as software. A firewall is implemented on systems that are connected to the internet and are vulnerable to hackers, viruses, worms, and other harmful intrusions. Answer: D is incorrect. Hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users' keystrokes, including sensitive passwords. They can be implemented via BIOS-level firmware, or alternatively, via a device plugged inline between a computer keyboard and a computer. They log all keyboard activities to their internal memory.

QUESTION 119
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:

Explanation:
WPA2 (Wi-Fi Protected Access 2) is used to provide network administrators with a high level of assurance that only authorized users are able to access the network. It provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm. Wireless Security Options are used to decrease the risk of data interception by a third party in Wireless Networking. Data can be protected by using encryption technologies. In Wireless Networking Connection, various methods are used to increase security as follows:
Using Wired Equivalent Privacy: The goal is to allow only authorized users to connect to the wireless network. While initially configuring routers and network adapters, users create a WEP key. The level of security depends on the length of the key measured in bits. Another step is to share WEP keys to authorized users. Specifically, it is possible for unauthorized users to determine the mathematical value of a WEP key by monitoring a sufficient amount of networking traffic. WEP is an additional security, but it does not completely address all potential vulnerabilities. Using Wi-Fi Protected Access: The Wi-Fi Protected Access protocol is used to provide higher security over the WEP standard. It is considered as a replacement for the less secured WEP protocol. WPA security is configured on a wireless router or an access point.
Using Service Set Identifiers: Service Set Identifiers are used to assist users to find and connect to a wireless network. Whenever a wireless network adapter is available on a computer, Windows Vista automatically identifies the available networks based on their SSID.
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 120
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:
Explanation:
Service Set Identifier, or SSID, is a name that identifies a particular 802.11 wireless LAN. A client device receives broadcast messages from all access

points within range, advertising their SSIDs. The client device can then either manually or automatically, based on configuration, select the network and can associate itself. The SSID can be up to 32 characters long. As the SSID displays to users, it normally

consists of human-readable characters. The SSID is defined as a sequence of 1-32 octets, each of which may take any value.
Answer: B is incorrect. IBSS (Independent Basic Service Set) is an ad-hoc network of client devices that does not require a central control access point. In IBSS, the SSID is chosen by the client device that starts the communication. The broadcasting of the SSID is performed in a pseudo-random order by all devices that are members of the network.
Answer: C is incorrect. Mandatory access control (MAC) refers to a type of access control by which the operating system constrains the ability of a subject or initiator to access or generally perform some sort of operation on an object or target. In practice, a subject is usually a process or thread; objects are constructs such as files, directories, TCP/UDP ports, shared memory segments, etc. Subjects and objects each have a set of security attributes. Whenever a subject attempts to access an object, an authorization rule enforced by the operating system kernel examines these security attributes and decides whether the access can take place. Any operation by any subject on any object will be tested against the set of authorization rules to determine if the operation is allowed.
Answer: A is incorrect. Microsoft Baseline Security Analyzer (MBSA) is a software tool of Microsoft to determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server, and Microsoft Office macro settings. Microsoft Baseline Security Analyzer (MBSA) includes a graphical and command line interface that can perform local or remote scans of Windows systems.

QUESTION 121
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:
Explanation:
Password Authentication Protocol (PAP) is the least sophisticated authentication protocol, used mostly when a client calls a server running an operating system other than Windows. PAP has a number of security vulnerabilities because it transmits user credentials as plaintext.
Answer: A is incorrect. Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol that uses a secure form of encrypted authentication. Using CHAP, network dial-up connections are able to securely connect to almost all PPP servers.

Answer: B is incorrect. Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) is the new version of MS-CHAP. MS-CHAP v2 provides the highest level of security and encryption for dial-up connection in the environment consisting of both Windows NT and Windows 2000/XP dial-up clients. It provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving data.

Answer: D is incorrect. Microsoft created the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) to authenticate remote Windows workstations. It is designed especially for Windows 95, Windows 98, Windows NT, and Windows 2000 networking products. This protocol provides data encryption along with password encryption.

QUESTION 122
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:
Explanation:
Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, Web servers, etc. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The Remote Access Server, the Virtual Private Network server, the Network switch with port-based authentication, and the Network Access Server, are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server. The RADIUS server is usually a background process running on a UNIX or Windows NT machine. RADIUS serves three functions:
To authenticate users or devices before granting them access to a network To authorize those users or devices for certain network services To account for usage of those services
Answer: D is incorrect. Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) is the new version of MS-CHAP.

MS-CHAP v2 provides the highest level of security and encryption for dial-up connection in the environment consisting of both Windows NT and Windows 2000/XP dial-up clients. It provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving data.
Answer: A is incorrect. PEAP (Protected Extensible Authentication Protocol) is a method to securely transmit authentication information over wired or wireless networks. It was jointly developed by Cisco Systems, Microsoft, and RSA Security. PEAP is not an encryption protocol; as with other EAP protocols, it only authenticates a client into a network.
PEAP uses server-side public key certificates to authenticate the server. It creates an encrypted SSL/TLS (Secure sockets layer/Transport layer security) tunnel between the client and the authentication server. In most configurations, the keys for this encryption are transported using the server's public key. The resultant exchange of authentication information inside the tunnel to authenticate the client is then encrypted and the user

credentials are thus safe and secure. Answer: C is incorrect. Kerberos is a computer network authentication protocol that allows individuals communicating over a non- secure network to prove their identity to one another in a secure manner. Kerberos builds on symmetric key cryptography and requires a trusted third party. Kerberos uses as its basis the Needham-Schroeder protocol. It makes use of a trusted third party, termed a key distribution center (KDC), which consists of two logically separate parts:
Authentication Server (AS)
Ticket Granting Server (TGS)
Kerberos works on the basis of tickets, which serve to prove the identity of users. The KDC maintains a database of secret keys; each entity on the network, whether a client or a server, shares a secret key known only to itself and to the KDC. Knowledge of this key serves to prove an entity's identity. For communication between two entities, the KDC generates a session key, which they can use to secure their interactions.

QUESTION 123
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:
Explanation:
Zone rule is method that can be used to identify Internet software in Software Restriction Policies.
Answer: C, B, and A are incorrect. These are invalid Answer: .

QUESTION 124
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:
Explanation:
Hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users' keystrokes, including sensitive passwords. They can be implemented via BIOS-level firmware, or alternatively, via a device plugged inline between a computer keyboard and a computer. They log all keyboard activities to their internal memory. Answer: D is incorrect. Anti-Virus software is used to prevent, detect, and remove malware, including computer viruses, worms, and trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware.
Anti-Virus software is a class of program that searches your hard drive, floppy drive, and pen drive for any known or potential viruses. The market for this kind of program has expanded because of Internet growth and the increasing use of the Internet by businesses concerned about protecting their computer assets. Popular Anti-Virus packages are as follows: Bit Defender Anti-Virus McAfee Virus Scan Kaspersky Anti-Virus F-Secure Anti-Virus Symantec Norton Anti-Virus Panda Titanium Anti-Virus Avira Anti-Virus Avast Anti-Virus Trend Micro Anti-Virus Grisoft AVG Anti-Virus ESET Nod32 Anti-Virus Webroot Anti-Virus Quick Heal Anti-Virus eTrust EZ Anti-Virus ZoneAlarm Anti-Virus
Answer: B is incorrect. Alchemy Remote Executor is a system management tool that allows Network Administrators to execute programs on remote network computers without leaving their workplace. From the hacker's point of view, it can be useful for installing keyloggers, spyware, Trojans, Windows rootkits and such. One necessary condition for using the Alchemy Remote Executor is that the user/attacker must have the administrative passwords of the remote computers on which the malware is to be installed.

Answer: C is incorrect. SocketShield provides a protection shield to a computer system against malware, viruses, spyware, and various types of keyloggers. SocketShield provides protection at the following two levels:
1.Blocking: In this level, SocketShield uses a list of IP addresses that are known as purveyor of exploits. All http requests for any page in these domains are simply blocked.
2.Shielding: In this level, SocketShield blocks all the current and past IP addresses that are the cause of unauthorized access.

QUESTION 125
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: B, D, and C and correct.

Explanation:
The following operating systems have Security Health Agent (SHA) on computers and report their status to the Security Health Validator (SHV):

QUESTION 126
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:
Explanation:

Secondary Logon (Run As) is defined as a starting programs and tools in local administrative context. Windows secondary logon is used to permit administrators to log on with a non-administrative account and be able to perform the several administrative tasks without logging off by using trusted administrative programs in administrative contexts. Answer: B is incorrect. The security log is generated by a firewall or other security device. It is used to define list of events that could affect the security of data or infrastructure, such as access attempts or commands, and the names of the users participating in this illegal process.
Answer: C is incorrect. Hardware firewall is defined as the important part of the system and network set-up on a broadband connection. It can be effective with small or no configuration, and is used to protect every machine on a local network. The hardware firewalls will have at least four network ports for connecting to other computers. This type of firewall uses packet filtering for checking the header of a packet in order to check its source and destination. The information obtained in this manner is compared to a set of predefined or user-created rules and then the packet is forwarded or dropped.

QUESTION 127
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:

Section: (none)
Explanation

Explanation/Reference:
Answer: B and A

Explanation:
Network Access Protection (NAP) is a set of operating system components included with the Windows Server 2008 and Windows Vista/7 operating systems. It ensures that the client computers on a private network meet administrator-defined requirements for system health. NAP policies define the required configuration and update status for a client computer's operating system and critical software. For example, an administrator can set policies that computers might be required to have antivirus software with the latest virus definition installed and current operating system updates. Using NAP, a network administrator can enforce compliance with health requirements for the client computers connection to the network. NAP helps network administrators to reduce the risk caused by improperly configured client computers that might be exposed to viruses and other malicious software. It is used to verify the complete integrity of the device by testing that it has the most current software updates or configuration modifications because the systems that are not able to receive the updates can be as problematic as they seem to be infected by malware.

Answer: C is incorrect. Single sign-on (SSO) is defined as a mechanism in which a single action of user authentication and authorization is used to allow a user to access all computers and systems where he got a access permission, without entering passwords for multiple times.
Answer: D is incorrect. Kerberos is defined as a secure method used for authenticating a request for a service in a computer network.

QUESTION 128
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: C and B

Explanation:
IPSec is an interoperable standard developed by Internet Engineering Task Force to secure the data sent between two computers on an IP network. It protects the data by providing the following two services:
Data Authentication: IPSec can be configured to ensure that each IP packet received from a trusted party is exactly originated from that party. It can be configured to ensure that data is not altered in between (from source to destination). It can also be configured to ensure that no packet is duplicated in the transit. Encryption: IPSec is used to encrypt data so that it can't be read if captured during transmission.

Answer: D and A are incorrect. These services are not provided by IPSec.

QUESTION 129
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: A, B, D, and C

Explanation:
A firewall is a combination of software and hardware that prevents data packets from coming in or going out of a specified network or computer. It is used to separate an internal network from the Internet. It analyzes all the traffic between a network and the Internet, and provides centralized access control on how users should use the network. A firewall can also perform the following functions:
Block unwanted traffic.
Direct the incoming traffic to more trustworthy internal computers. Hide vulnerable computers that are exposed to the Internet.
Log traffic to and from the private network.
Hide information, such as computer names, network topology, network device types, and internal user IDs from external users.

QUESTION 130
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:
Explanation:
While stressing the Con?dentiality, Integrity, and Availability triangle in the training of users, the process of providing availability is related to security training to ensure the protection against a Distributed Denial of Services attack.

QUESTION 131
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: C, A, and D

Explanation:
A virus is a program that can do the same things as other programs. The only major difference is that it attaches itself to other programs. It executes secretly when the host program is run. A computer virus can corrupt or delete data on a computer. Even it can delete all content of a hard disk and can move to another computer through any media such as pen drives, floppy drives, e-mail attachments, etc. Some indications of a virus attack are as follows:
The computer runs slower than usual and stops responding. The applications installed on the computer system do not work properly and the computer restarts on its own.
Disk drives cannot be accessed.
An antivirus program is not able to run, and unusual error messages are displayed. An attachment is opened having double extension, such as .jpg, .vbs, .gif, or .exe. Although the computer has sufficient memory, an out-of-memory error message is displayed. Task Manager or Command Prompt cannot be started. The computer virus can reformat the disk and change the file settings.

QUESTION 132
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:
Explanation:
DNSLint is an utility used to identify anomalies of records in the targeted DNS zone. The examples of some of the items tested are as follows:
1.Recursive lookup of DNS zone from the Internet 2.Configuration of the SOA record

3.MX records present and resolution tested
4.Active Directory replication issues
Answer: C is incorrect. DNSCMD.exe is a command-line tool that performs the same task as the
DNSMGMT.msc MMC performs.
Answer: A is incorrect. Nslookup.exe is a troubleshooting utility used to identify name resolution issues for all record types created within a DNS zone.
Answer: B is incorrect. IPCONFIG is a command-line utility that displays the current TCP/IP configuration, such as the IP address, subnet mask, default gateway, etc. of a networked computer. It refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Users can run IPCONFIG from the command prompt whenever they need to know the status of a computer's TCP/IP configuration.

QUESTION 133
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:
Explanation:
The level of security set for the local intranet zone is applied to the Websites and content that are stored on a corporate, or business network. Answer: D is incorrect. The level of security set for an Internet zone is applied to all the Websites by default.
Answer: A is incorrect. The level of security set for the restricted sites is applied to the sites that might potentially damage your computer, or your information. Answer: C is incorrect. The level of security set for the trusted sites is applied to sites that you have specifically indicated as the ones that

you trust.

QUESTION 134
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:
Explanation:
The presentation layer is the layer in which encryption and decryption of data takes place.
Answer: B is incorrect. The session layer is responsible for data synchronization between the applications on the sending device and the receiving device. Answer: C is incorrect. The physical layer is the lowest layer of the OSI model. The physical layer is responsible for packaging and transmitting data over physical media. This layer controls the way in which data is sent and received over a physical medium.
Answer: D is incorrect. The data-link layer is responsible for error free transfer of data frames.

QUESTION 135
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:
Explanation:
The HKEY_CLASSES_ROOT root key stores information about registered applications such as file association data that tells which default program opens files with a certain extension.
Answer: D is incorrect. The HKEY_CURRENT_USER root key stores settings that are specific to the currently logged-in user. When a user logs off, the HKEY- CURRENT-USER is saved to HKEY-USERS.
Answer: A is incorrect. The HKEY_USERS root key contains subkeys corresponding to the HKEY_CURRENT_USER keys for each user profile actively

loaded on the machine.
Answer: C is incorrect. The HKEY_CURRENT_CONFIG root key contains information gathered at run time.

QUESTION 136
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:
Explanation:
International Computer Security Association (ICSA) is an independent organization that defines standards for anti-virus software and shares critical security information with security product manufacturers, developers, security experts, and corporations. Answer: D is incorrect. Institute of Electrical and Electronics Engineers (IEEE) is an organization of engineers and electronics professionals who develop standards for hardware and software. Answer: B is incorrect. Internet Engineering Task Force (IETF) is an open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and coordination of the operation and management of the Internet. It works towards introducing procedures for new technologies on the Internet. IETF specifications are released in Requests for Comments (RFCs). Answer: C is incorrect. Internet Information Service (IIS) is a software service that comes with Window NT Server and Windows 2000 Server operating systems. It supports Web site creation, configuration, and management.

QUESTION 137
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:
Section: (none)

Explanation

Explanation/Reference:
Answer: C and A

Explanation:

Mark can add another level of security after implanting encryption techniques for the business wireless traffic by implementing the access point isolation and hiding the Service Set Identifier (SSID). It is a simple security measure that can be used.

QUESTION 138
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:
Explanation:
To minimize the amount of spam that is hitting the Microsoft Exchange server, it is required to enable reverse DNS lookup on the SMTP virtual server. It forces a system to crosscheck the domain name with a PTR record (IP address associated with the domain name) and if the IP address is not matched the record associated with that domain name, it will not delivered. SPF is used to permit the administrator to configure the server to establish who is acceptable to send email from their domain. Answer: D is incorrect. Windows Server Update Services (WSUS) is an add- on component of Windows Server 2008. It provides functionality to a server to run as a Windows Update server in a Windows network environment. Administrators can configure a WSUS server as the only server to download updates from Windows site, and configure other computers on the network to use the server as the source of update files. This will save lots of bandwidth as each computer will not download updates individually. WSUS 3.0 SP1 is the only version of WSUS that can be installed on Windows Server 2008. Earlier versions of WSUS cannot be installed on a server running Windows Server 2008.
Answer: A is incorrect. User Account Control (UAC) is a technology and security infrastructure introduced with Microsoft's Windows Vista and Windows Server 2008 operating systems, with a more relaxed version also present in Windows 7 and Windows Server 2008 R2. It aims to improve the security of Microsoft Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation.
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 139
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:
Explanation:
BitLocker Drive Encryption is an operating system technology that can be used to encrypt an entire hard drive. It cannot be used to just encrypt a database. It is capable of encrypting an entire hard drive, but not individual files. Answer: C is incorrect. Kerberos is defined as a secure method used for authenticating a request for a service in a computer network. Answer: D is incorrect. Encrypting file system (EFS) is defined as a feature of Windows that permits a user to store information on the hard disk in an encrypted format that is obtained by encryption. Encryption is the process of encoding data for preventing unauthorized access during transmission. Answer: B is incorrect. This is an invalid Answer: .

QUESTION 140
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:

Explanation:
L2TP is more secure than PPTP because PTP uses MPPE for security that is less secure than L2TP that uses IPsec as a encryption method for security.

QUESTION 141
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:
Explanation:
Windows Server Update Services (WSUS) is an add-on component of Windows Server 2008. It provides functionality to a server to run as a Windows Update server in a Windows network environment. Administrators can configure a WSUS server as the only server to download updates from Windows site, and configure other computers on the network to use the server as the source of update files. This will save lots of bandwidth as each computer will not download updates individually. WSUS 3.0 SP1 is the only version of WSUS that can be installed on Windows Server 2008. Earlier versions of WSUS cannot be installed on a server running Windows Server 2008.
Answer: B 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.
Answer: D is incorrect. DNS dynamic update is used to enable DNS client computers for registering and dynamically updating their resource records with a DNS server whenever any modification or change has been taken place. It is used to update the DNS client computers with the reflecting changes. Answer: C is incorrect. Microsoft Baseline Security Analyzer (MBSA) is a software tool of Microsoft to determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server, and Microsoft Office macro settings. Microsoft Baseline Security Analyzer (MBSA) includes a graphical and command line interface that can perform local or remote scans of Windows systems.

QUESTION 142
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:
Explanation:
Stateless inspection is used to add flexibility and scalability to network configuration. It is used to inspect network information on the basis of source and destination address. In this inspecxtion method, packets are inspected up to Layer 3 of the OSI model that is the network layer. It is able to inspect source and destination IP addresses, and protocol source and destination ports. Answer: D and B are incorrect. These are invalid Answer: . Answer: C is incorrect. Stateful packet inspection firewall is a type of hardware firewall used to track information about the applications sending the packets, contents of the packet and state of the connection. This process permits the firewall to make decisions about packets based on context and administrator defined rules.

QUESTION 143
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:
Explanation:
In the above scenario, to attract the attackers for understating their strategy, Mark can create a honeypot outside the perimeter network that is a erroneous program that can try to be like a VPN or service.

QUESTION 144

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:
Explanation:
The Internet zone feature in IE 8 can be configured and users are enabled to easily browse the local intranet without disturbing the security levels by using the following steps:
1.Go into the Internet Options and select the Security. 2.Add the intranet site to the list of Local Intranet Site.
Answer:
C While stressing the Con?dentiality, Integrity, and Availability triangle in the training of users, the process of providing availability is related to security training to ensure the protection against a Distributed Denial of Services attack.

QUESTION 145
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:
Explanation:
In order to provide stateful packet inspection (SPI) to your mobile users, you need to purchase a third party firewall solution for your mobile users. Windows firewalls are all simple packet filtering firewalls. There is no support for advanced features such as stateful packet inspection.

QUESTION 146
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:
Explanation:
Share permissions can be configured to allow or deny access on shared folders for users. Share permission has three types of permissions:
1.Read: It allows users to only view the folders, files, and data. It also allows users to run programs.
2.Change: With Change permissions, users can create folders, files, change data in files, add data in files, delete folders and files, change file attributes. Users will also be able to perform actions permitted by Read permissions. 3.Full Control: It allows users full control on the shared resources. Users get Read and Change permissions as well as the ability to change share permissions.

QUESTION 147
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:
Explanation:
Encrypting File System (EFS) works by encrypting a file with a bulk symmetric key, also known as the File Encryption Key (FEK). It uses a symmetric encryption algorithm that takes a lesser amount of time to encrypt or decrypt large amounts of data. Files encrypted by EFS cannot be compressed with NTFS compression. Answer: A is incorrect. BitLocker Drive Encryption (BitLocker) is used to protect all files stored on the drive on which Windows is installed. It encrypts the entire system drive and helps block hackers from accessing the system files they rely on to discover user passwords. BitLocker also prevents hackers from accessing the hard disk by removing it from a computer, and installing it on a different computer. BitLocker does not work for USB Flash Drives.
Answer: B is incorrect. Service Set Identifier, or SSID, is a name that identifies a particular 802.11 wireless LAN. A client device receives broadcast messages from all access points within range, advertising their SSIDs. The client device can then either manually or automatically, based on configuration, select the network and can associate itself. The SSID can be up to 32 characters long. As the SSID displays to users, it normally consists of human-readable characters. The SSID is defined as a sequence of 1-32 octets, each of which may take any value. Answer: C is incorrect. BitLocker To Go is an extension of BitLocker Drive Encryption. BitLocker To Go prevents from disclosure of data made available through physical loss of removable storage devices such as USB Flash Drives, USB Portable Hard Drives, etc. BitLocker To Go gives administrators control over how removable storage devices can be utilized within their environment and the strength of protection that they require. BitLocker To Go is a separate feature than the traditional BitLocker feature and it can be utilized on its own, without requiring the system partition to be protected with the traditional BitLocker feature.

QUESTION 148
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:
Explanation:
Piggybacking is a term used to refer to 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. It is a legally and ethically controversial practice, with laws that vary in jurisdictions around the world.
Answer: A is incorrect. Samhain is an open source multi-platform application that is used for checking the integrity of centralized files and for detecting host-based intrusion on POSIX systems
(Unix, Linux, Cygwin/Windows). Although it can be used to monitor a single host, it is designed to monitor multiple hosts with potentially different operating systems from a central location. Samhain can therefore be configured as a client/server application to monitor many hosts on a network from a single central location. Answer:

D is incorrect. A vampire tap is a cable connection that is made with a unit that clamps onto and bites into the cable. Vampire taps are often used to attach thick Ethernet transceivers to the coaxial cable. Without a vampire tap, the cable has to be cut and connectors have to be attached to both ends.
Answer: B is incorrect. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e-mail and other private communications. Sometimes, organizations also snoop their employees legitimately to monitor their use of organizations' computers and track Internet usage.

QUESTION 149
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:
Explanation:
The system will remember the last 10 passwords and will not permit the user to reuse any of those passwords when a user sets the value of Enforce Password History to 10.

QUESTION 150
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: B and A

Explanation:
Fingerprinting is the easiest way to detect the Operating System (OS) of a remote system. OS detection is important because, after knowing the target system's OS, it becomes easier to hack into the system. The comparison of data packets that are sent by the target system is done by fingerprinting. The analysis of data packets gives the attacker a hint as to which operating system is being used by the remote system. There are two types of fingerprinting techniques as follows:
1.Active fingerprinting
2.Passive fingerprinting
In active fingerprinting ICMP messages are sent to the target system and the response message of the target system shows which OS is being used by the remote system. In passive fingerprinting the number of hops reveals the OS of the remote system. Answer: C and D are incorrect. There are no such types of OS fingerprinting.

QUESTION 151
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:
Explanation:
A gateway filter checks spam at the network gateway before it even reaches the email server. This gives you a common network wide solution that is easy to manage, and it does not utilize the resources of the email server. Answer: D is incorrect. This solution will utilize mail server resources and hinder the performance of the email server.
Answer: A is incorrect. Client side solutions would not be common to the entire network. Even if all the clients are similarly configured, over time some will mark items that others will not as spam. This will not be easy to administer.

QUESTION 152
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
B. Active Directory Administrative Center

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Active Directory Domains and Trusts MMC snap-in console is used to administer domain and forest functional levels and user principal name (UPN) suffixes. Answer: C is incorrect. The Active Directory Sites and Services MMC snap-in is used to administer the replication of directory data among all sites in an Active Directory Domain Services (AD DS) forest.
Answer: A is incorrect. Group Policy Management Console (GPMC) is used to provide a single administrative tool for managing Group Policy across the enterprise. Answer: D is incorrect. Active Directory Administrative Center is used to administer and publish information in the directory, including managing users, groups, computers, domains, domain controllers, and organizational units.

QUESTION 153
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:
Explanation:
In computer networking, MAC filtering (or EUI filtering, or layer 2 address filtering) 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. MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists.
Answer: A is incorrect. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e-mail and other private communications. Sometimes, organizations also snoop their employees legitimately to monitor their use of organizations' computers and track Internet usage.
Answer: B is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.
Answer: C is incorrect. The term encapsulation refers to the process where headers and trailers are added around some data. A TCP/IP host sends data by performing a process in which four layers encapsulate data (adds headers and trailers) before physically transmitting it.

QUESTION 154
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:

Explanation:
The Security zones in Internet Explorer are security-related zones containing a particular group of Web sites. Different levels of permissions are assigned through these groups. These zones are included in the configuration settings. The security settings for each zone can be configured by the user. Following are the types of Security zones:
Internet: This is the default zone for all Web sites, including all public Internet Web sites. By default, the security level is Medium-High. Local Intranet: This zone is for the Web sites on the local network. These sites are considered relatively trustworthy. The default security level for this zone is Medium-Low.
Trusted Sites: This zone is for the trusted Web sites specified by the user. The default security level for this zone is Medium.
Restricted Sites: This zone is for the Web sites that the user does not trust. These sites are considered risky by the user. The default security level for this zone is High.

QUESTION 155
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:
Explanation:
Network address translation (NAT) works at the network layer and hides the local area network IP address and topology. Network address translation

(NAT) is a technique that allows multiple computers to share one or more IP addresses. It is configured at a server between a private network and the Internet. It allows the computers in the private network to share a global, ISP assigned address. It modifies the headers of packets traversing the server. For the packets outbound to the Internet, it translates the source addresses from private to public, whereas for the packets inbound from the Internet, it translates the destination addresses from public to private.
Answer: B and D are incorrect. The MAC address and the network interface card (NIC) work at the data link layer.
Answer: C is incorrect. A hub works at the physical layer.

QUESTION 156

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:
Section: (none)
Explanation

Explanation/Reference:
Answer: A and B

Explanation:
In order to prevent malicious code from being downloaded from the Internet onto a computer, you will have to disable unauthorized ActiveX Controls and Active Scripting on the Web browser. Disabling Active Scripting and ActiveX controls makes browsers safer for browsing the Web.

QUESTION 157
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:
Explanation:
A token-based authentication system is a two-factor authentication system. Two factor authentication is based on two types of information: First, a piece of information that a user knows, such as the password; Second, an external device such as a credit card or a key fob a user can carry with them. Each device has a unique serial number. In addition to hardware tokens, some vendors offer software-based tokens that are capable of running on mobile devices. The token-based authentication is a strong form of authentication. Answer: C is incorrect. The certificate-based authentication uses a digital certificate to verify an identity. In addition to the user name and password, other credentials are

also provided to prove the identity of the user who is trying to access the mailbox resources stored on the Exchange 2010 server. A digital certificate consists of two components: the private key that is stored on the device and the public key that is installed on the server.
If Exchange 2010 is configured to require certificate-based authentication for Exchange ActiveSync, only devices that meet the following criteria can synchronize with Exchange 2010:
1.The device has a valid client certificate installed that was created for the user authentication.
2.The device has a trusted root certificate for the server to which the user is connecting to establish the SSL connection.
Answer: B is incorrect. The basic authentication is the simplest form of authentication. In basic authentication, the client submits a user name and a password to the server. The user name and password are sent to the server in clear text over the Internet. The server verifies whether the user name and password are valid and grants or denies access to the client accordingly. The basic authentication is enabled for Exchange ActiveSync by default. However, it is recommended that basic authentication should be disabled unless SSL is also deployed. When basic authentication is used over SSL, the user name and password are still sent in plain text, but the communication channel is encrypted. Answer: A is incorrect. There is no such authentication method as device-based authentication.

QUESTION 158
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:
Explanation:
Spyware is software that gathers information about a user without his knowledge. Spyware can get into a computer when the user downloads software from the Internet. Spyware can search the contents of a hard disk, address book of an e-mail, or any information about the computer, and transmits the information to the advertisers or other interested parties.

Answer: B is incorrect. Firmware is a term often used to denote the fixed, usually rather small, programs and data structures that internally control various electronic devices. Firmware sits on the reader and controls its function. It reads only one type of tag either active or passive.

Answer: A is incorrect. Malware or malicious software is a threat that attempts to break into a computer or damage it without the consent of the owner of the system. There are a number of types of malware depending upon their threat level and functions. Some malware are conditionally executed while others are unconditional. Answer: D is incorrect. Adware is software that automatically downloads and display advertisements in the Web browser without user permission. When a user visits a site or downloads software, sometimes a hidden adware software is also downloaded to display advertisement automatically. This can be quite irritating to user. Some adware can also be spyware.

QUESTION 159
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:
Explanation:
Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.
Answer: B is incorrect. Man-in-the-middle attacks occur when an attacker successfully inserts an intermediary software or program between two communicating hosts. The intermediary software or program allows attackers to listen to and modify the communication packets passing between the two hosts. The software intercepts the communication packets and then sends the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client.
Answer: C is incorrect. A CookieMonster attack is a man-in-the-middle exploit where a third party can gain HTTPS cookie data when the 'Encrypted Sessions Only' property is not properly set. This could allow access to sites with sensitive personal or financial information. Users of the World Wide Web can reduce their exposure to

CookieMonster attacks by avoiding websites that are vulnerable to these attacks. Certain web browsers make it possible for the user to establish which sites these are. For example, users of the Firefox browser can go to the Privacy tab in the Preferences window, and click on 'Show Cookies.' For a given site, inspecting the individual cookies for the top level name of the site, and any subdomain names, will reveal if 'Send For: Encrypted connections

only,' has been set. If it has, the user can test for the site's vulnerability to CookieMonster attacks by deleting these cookies and visiting the site again. If the site still allows the user in, the site is vulnerable to CookieMonster attacks.
Answer: D is incorrect. Phreaking is a process used to crack the phone system. The main aim of phreaking is to avoid paying for long-distance calls. As telephone networks have become computerized, phreaking has become closely linked with computer hacking. This is sometimes called the H/P culture (with H standing for Hacking and P standing for Phreaking).

QUESTION 160
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:
Section: (none)
Explanation

Explanation/Reference:
Answer: D and C

Explanation:
The following steps will help in system or host hardening: Disabling unnecessary services from the host.
Installing or applying a patch on the host provided by the operating system manufacturer.
System hardening is a term used for securing an operating system. It can be achieved by installing the latest service packs, removing unused protocols and services, and limiting the number of users with administrative privileges. Answer: A and B are incorrect. Installing updated device drivers on the computer or adding users to the administrators group will not help in system or host hardening. Adding users to the administrators group will give users unnecessary permission to the computer. This will be a security issue.