QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

Microsoft

98-367

Security Fundamentals

Answer: A

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

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.

Answer: C

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
D. Active Directory Administrative Center

Answer: B

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

Answer: D

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

Answer: C

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)

Answer: A

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

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

Answer: D

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

Answer: C

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

Answer: A

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.

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.