SCP SC0-471

SC0-471 Strategic Infrastructure Security

Practice Test

Version 1.3

QUESTION NO: 1

You wish to increase the security of your Windows 2003 system by modifying TCP/IP in the Registry. To alter how Windows reacts to SYN Attacks, which three values are adjusted?

A. TCPMaxPortsExhausted
B. TCPMaxHalfOpen
C. TCPAIIowedConnections
D. TCPMaxHalfOpenRetried
E. TCPAIIowedSessions

Answer: A,B,D

QUESTION NO: 2

Most companies that do business via the Web offer a shopping cart so you can specify all the items you want before placing the order. Poor shopping cart design, however, can allow a different kind of hack. Take a look at the HTML code sample presented here and determine the line that presents the vulnerability:

<FORM ACTION="http://10.0.10.236/cgi-bin/orders.pl" method="post">
<inputtype=hidden name="price" value="39.95">
<inputtype=hidden name="item_no" value="WIDGET9">
QUANTITY: <input type=text name="quantity" size=2 maxlength=2 value=l>
</FORM>

A. The line specifying the Perl script orders.pl
B. The line specifying input type for price
C. The line specifying input type for item number
D. The line specifying input type for quantity
E. The line specifying input type for item number and quantity

Answer: B

QUESTION NO: 3

You have recently hired an assistant to help you with managing the security of your network. You are currently running an all Windows Server 2003 environment, and are describing the issues associated with sharing folders. You describe different shared folder permissions. Which of the following describes the maximum abilities of the Read permission?

A. Display folder names, filenames and data, and execute files

B. Rename files andfolders, delete files and folders
C. Create folders, add files to folders, change or delete flies in folders
D. Rename files and folders, and execute files
E. Changefile permissions and take ownership of files

Answer: A

QUESTION NO: 4

You read on a security website that hackers are reading Newsgroup messages to try to identify potential targets and target details. You had previously not closed the port for the Newsgroup service on your firewall. After you close that port, you do an Internet newsgroup search for your domain name. You do find several messages from users in your organization. What type of information may be found by examining these messages?

A. Email Address
B. Internal Server Names
C. Corporate Public IP Address
D. Client Newsreader Program
E. Client Email Program

Answer: A,C,D

QUESTION NO: 5

You suspect that your root account has been compromised. What command can you run on your Linux system, in the /var/log directory to see you the recent login activity of the root account?

A. root_access -R
B. -R root
C. last -U/acct:root
D. last -a -d root
E. last -R/acct:root

Answer: D

QUESTION NO: 6

There are several clients of your network that require the ability to connect remotely. You are using Internet Authentication Services (IAS) in Windows Server 2003 for security. What is IAS the Windows implementation of?

A. MD5
B. DES
C. RSA
D. PKI
E. RADIUS

Answer: E

QUESTION NO: 7

You have been given the task of writing your organization's security policy. During your research you find that there are several established standards for security policy design. Which of the following are accepted standards?

A. ISO 17799
B. BS 197
C. ISO 979
D. BS 7799
E. ISO 179

Answer: A,D

QUESTION NO: 8

You wish to manage your Linux system remotely, using a web browser. Which of the following tools will allow you to accomplish your task?

A. Snort
B. Bastille
C. Tripwire
D. Webmin
E. SSH

Answer: D

QUESTION NO: 9

You are concerned that email messages sent to your Outlook clients could contain customized and dangerous scripting. What can you do to minimize the threat that this specific type of email presents?

A. Install and Update Anti-Virus software
B. Update the Security Settings for the clients at the SMTP Server
C. Disable the Preview Pane
D. Be sure that all forms of scripting are disabled on all clients
E. Minimize the number of contacts allowed in an address book

Answer: C

QUESTION NO: 10

Which of the following has the stages of Risk Analysis in order, from a to e?

A. Management
b. Threat Assessment
C. Control Evaluation
D. Inventory
E. Monitoring
B. b, d, c, e, a
C. a, b, d, c, e
D. d, b, c, a, e
E. a, b, c, d, e
F. d, b, a, c, e

Answer: C

QUESTION NO: 11

Microsoft has developed several security tools to help you with the security and configuration of the systems in your network. One of these tools is the Microsoft Security Baseline Analyzer (MBSA). In the command line options of the MBSA is the HFNetChk tool. What is the function of the HFNetChk tool, available with MBSA?

A. To check for the current Hotfixes that areavailable from Microsoft
B. It is an upgrade to the Windows Update tool for checking on all updates
C. It is the tool that must be run prior to installing IIS 6.0
D. It is the tool that checks the network configuration of all web servers
E. To record what Hotfixes and service packs are running on the Windows machine

Answer: E

QUESTION NO: 12

You are studying the current attack methods and find that one of your servers is vulnerable to a Buffer Overflow attack. Which of the following do Buffer Overflows exploit?

A. Ramdrives
B. A program that does not do bounds checking
C. Memory leaks in the hardware
D. A program allowing itself to be copied
E. Paging of memory to a disk

Answer: B

QUESTION NO: 13

At the root@linuxbox$ prompt on a Linux machine you type Is -I b.doc and the output reads:

-tw-tw-r--1 simonusers313370ct5 11:21 b.doc

According to this output, which of the following is true?

A. b.doc is a word document
B. Nobody but the owner can execute this file
C. This file is infected by thesimon trojan
D. Nobody can read this file
E. Everyone can read this file

Answer: E

QUESTION NO: 14

You suspect that your root account has been compromised. What command can you run on your Linux system, in the /var/log directory to see you the recent login activity of the root account?

A. root_access -R
B. -R root
C. last -U/acct:root
D. last -a -d root
E. last -R/acct:root

Answer: D

QUESTION NO: 15

You are running a Linux Server for your organization. You realize after a security scan that the Telnet service is accepting connections, which you do not want. In order to disable the computer's ability to accept incoming Telnet sessions, the easiest method for you to choose is which of the following?

A. Remove the Telnet service from the server
B. Comment out the Telnet line ininetd.conf
C. Stop the Telnet service on the server
D. Pause the Telnet service on the server
E. Configure the firewall to block Telnet requests

Answer: B

QUESTION NO: 16

You have a file on your Linux system, and you need to modify the file's permissions. The permissions you wish to apply are: Read, Write, and Execute for the User; Read for the Group: and Read for the Others. What command will allow you to achieve this?

A. chmod 744 test_file.tar.gz
B. chmod 644 test_file.tar.gz
C. chmod 700 test_file.tar.gz
D. chmod 774 test_file.tar.gz
E. chmod 600 test_file.tar.gz

Answer: A

QUESTION NO: 17

You are discussing the design and infrastructure of the Internet with several colleagues when a disagreement begins over the actual function of the NAP in the Internet design. What is the function of a NAP in the physical structure of the Internet?

A. The NAP provides for a layered connection system of ISPs connecting to the backbone.
B. The NAP provides the actual connection point between a local user and the Internet.
C. The NAP provides the physical network with communication channels for the Internet and voice/data applications.
D. The NAP provides a national interconnection of systems, called peering centers, to the NSPs.
E. The NAP provides for a connection point between an ISP and the backbone of the Internet.

Answer: E

QUESTION NO: 18

You work for a medium sized ISP and there have been several attacks of the DNS configuration recently. You are particularly concerned with DNS Spoofing attacks. If an attacker is able to send out false data to a DNS client before the response from the DNS server arrives, this is which type of DNS Spoofing?

A. DNS Server Compromise
B. DNS Cache Poisoning
C. Spoofing the DNS Response
D. DNS Source-Router Spoof
E. IXFR Source-Spoof

Answer: C

QUESTION NO: 19

During a discussion of asset classification and protection with a coworker, you realize that your coworker does not know the basic concepts of asset protection. You are asked to describe the types of asset protection. Which of the following describes the concept of feasible protection of an asset?

A. The cost to replace the asset is greater than the cost of recovery of the asset.
B. The cost to replace the asset is less than the cost of protect the asset.
C. The cost to protect the asset is greater than the cost of recovery of the asset.
D. The cost to replace the asset is less than the cost of recovery of the asset.
E. The cost to protect the asset is less than the cost of recovery of the asset.

Answer: E

QUESTION NO: 20

What are the four different modes of implementation of DES?

A. Stream Cycle Chaining (SCC)
B. Electronic Codebook (ECB)
C. Output Feedback (OFB)
D. Cipher Feedback (CFB)
E. Cipher Block Chaining (CBC)

Answer: B,C,D,E

QUESTION NO: 21

You are studying the current attack methods and find that one of your servers is vulnerable to a Buffer Overflow attack. Which of the following do Buffer Overflows exploit?

A. Ramdrives
B. A program that does not do bounds checking
C. Memory leaks in the hardware
D. A program allowing itself to be copied
E. Paging of memory to a disk

Answer: B

QUESTION NO: 22

Which of the following fields are found in a user account's line in the /etc/shadow file?

A. The User Identifier assigned to the user account
B. The home directory used by the user account
C. The hashed version of the user account's password
D. The number of days since the user account password was changed
E. The number of days until the user account's password must change

Answer: C,D,E

QUESTION NO: 23

In the English language, what is the most frequently used letter?

A. A
B. E
C. T
d. r
e. s

Answer: B

QUESTION NO: 24

You have just finished installing new servers and clients in your office network. All the new client machines are running Windows 2000 Professional, and the servers are running Windows Server 2003. You are now working on securing all user authentication related areas of the systems. Where is user account information stored, both for the Domain and the local machine?

A. Domain user account information is stored in the Active Directory.
B. Local user account information is stored in the SAM.
C. Local user account information is stored in the Active Directory.
D. Domain user account information is stored in the SAM.
E. Domain user account information is stored in the Metabase

Answer: A,B

QUESTION NO: 25

You wish to install a new Windows 2003 Server in your network, and are deciding which of the server roles will best suit your environment. From the following answers, select the option that is not a Windows 2003 Server Role.

A. SQL Server
B. DNS Server
C. DHCP Server
D. Print Server
E. SharePoint Services Server

Answer: A

QUESTION NO: 26

To maintain the security of your network you routinely run several checks of the network and computers. Often you use the built-in tools, such as netstat. If you run the following command:

netstat -e

Which of the following will be the result?

A. Displays all connections and listening ports
B. Displays Ethernet statistics
C. Displays addresses and port numbers in numerical form
D. Shows connections for the protocol specified
E. Displays per-protocol statistics