GIAC

Exam GSNA

GIAC Systems and Network Auditor

Version: 3.0

[Total Questions: 368]

Topic 3, Volume C

Question No : 1 - (Topic 3)

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He executes the following command in the terminal: echo $USER, $UID Which of the following will be displayed as the correct output of the above command?

A. John, 0
B. root, 0
C. root, 500
D. John, 502

Answer: B

Explanation: According to the scenario, John is a root user. Hence, the value of the environmental variables $USER and $UID will be root and 0, respectively.

Topic 4, Volume D

Question No : 2 - (Topic 4)

Mike works as a Network Engineer for XYZ CORP. The company has a multi-platform network. Recently, the company faced lots of blended threat issues that lead to several drastic attacks. Mike has been assigned a project to manage the resources and services of the company through both Intranet and Internet to protect the company from these attacks. Mike needs a system that provides auto-discovering and network topology building features to allow him to keep an intuitive view of the IT infrastructure. What will Mike use to meet the requirement of the project?

A. eBox
B. dopplerVUe
C. David system
D. EM7

Answer: C

Explanation: David system is a network management system that allows a user to

manage the resources and services through both Intranet and Internet. It provides auto-discovering and network topology building features to facilitate in keeping an intuitive view of the IT infrastructure. The resources, real-time monitoring, and accessibility of historical data facilitate reaction to failures. Configured interfaces for monitored devices permit a user to focus on the most important aspects of their work. Answer: B is incorrect. dopplerVUe is a network management tool that facilitates network discovery, mapping, alerts and alarm management, and bandwidth management system. It enables monitoring of Ping, SNMP, syslog, and WMI performance metrics. It can also be used to monitor IPv6 devices, as well as services such as DNS, http, and email. Answer: A is incorrect. eBox is an open source distribution and web development framework. This framework is used to manage server application configuration. It is based on Ubuntu Linux. It is projected to manage services in a computer network. The modular design of eBox allows a user to pick and choose the services. Answer: D is incorrect. EM7 is a network monitoring system that is used to measure IT infrastructure health and performance. It is an NMS integrated system. It is designed to help in optimizing the performance and availability of the networks, systems, and applications. It facilitates trouble-ticketing, event management, reporting, IP management, DNS, and monitoring.

Topic 1, Volume A

Question No : 3 - (Topic 1)

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to set some terminal characteristics and environment variables. Which of the following Unix configuration files can you use to accomplish the task?

A. /etc/sysconfig/routed
B. /proc/net
C. /etc/sysconfig/network-scripts/ifcfg-interface
D. /etc/sysconfig/init

Answer: D

Explanation: In Unix, the /etc/sysconfig/init file is used to set terminal characteristics and environment variables. Answer: B is incorrect. In Unix, the /proc/net file contains status information about the network protocols. Answer: C is incorrect. In Unix, the /etc/sysconfig/network-scripts/ifcfg-interface file is the configuration file used to define a network interface. Answer: A is incorrect. In Unix, the /etc/sysconfig/routed file is used to

set up the dynamic routing policies.

Question No : 4 - (Topic 1)

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to see the list of the filesystems mounted automatically at startup by the mount -a command in the /etc/rc startup file. Which of the following Unix configuration files can you use to accomplish the task?

A. /etc/named.conf
B. /etc/groups
C. /etc/mtab
D. /etc/fstab

Answer: D

Explanation: In Unix, the /etc/fstab file is used by system administrators to list the filesystems that are mounted automatically at startup by the mount –a command (in /etc/rc or its equivalent startup file). Answer: C is incorrect. In Unix, the /etc/mtab file contains a list of the currently mounted file systems. This is set up by the boot scripts and updated by the mount command. Answer: A is incorrect. In Unix, the /etc/named.conf file is used for domain name servers. Answer: B is incorrect. In Unix, the /etc/groups file contains passwords to let a user join a group.

Question No : 5 - (Topic 1)

Which of the following statements about a screened host is true?

A. It facilitates a more efficient use of the Internet connection bandwidth and hides the real IP addresses of computers located behind the proxy.
B. It is a small network that lies in between the Internet and a private network.
C. It provides added security by using Internet access to deny or permit certain traffic from the Bastion Host.
D. It provides a physical connection between computers within a network.

Answer: C

Explanation: A screened host provides added security by using Internet access to deny or permit certain traffic from the Bastion Host. Answer: D is incorrect. A network interface card provides a physical connection between computers within a network.
Answer: B is incorrect. 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. Answer: A is incorrect. A proxy server facilitates a more efficient use of the Internet connection bandwidth and hides the real IP addresses of computers located behind the proxy.

Question No : 6 - (Topic 1)

You work as a Network Administrator for ABC Inc. The company uses a secure wireless network. John complains to you that his computer is not working properly. What type of security audit do you need to conduct to resolve the problem?

A. Non-operational audit
B. Dependent audit
C. Independent audit
D. Operational audit

Answer: C

Explanation: An independent audit is an audit that is usually conducted by external or outside resources. It is the process of reviewing detailed audit logs for the following purposes: To examine the system activities and access logs To assess the adequacy of system methods To assess the adequacy of system controls To examine compliance with established enterprise network system policies To examine compliance with established enterprise network system procedures To examine effectiveness of enabling, support, and core processes Answer: B is incorrect. It is not a valid type of security audit. Answer: D is incorrect. It is done to examine the operational and ongoing activities within a network. Answer: B is incorrect. It is not a valid type of security audit. Answer: D is incorrect. It is done to examine the operational and ongoing activities within a network. Answer: A is incorrect. It is not a valid type of security audit.

Question No : 7 - (Topic 4)

You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?

A. Implement WPA
B. Implement WEP
C. Don't broadcast SSID
D. Implement MAC filtering

Answer: C

Explanation: By not broadcasting your SSID some simple war driving tools won't detect your network. However you should be aware that there are tools that will still detect networks that are not broadcasting their SSID across your network. Answer: D is incorrect. While MAC filtering may help prevent a hacker from accessing your network, it won't keep him or her from finding your network.

Question No : 8 - (Topic 1)

You work as a Java Programmer for JavaSkills Inc. You are working with the Linux operating system. Nowadays, when you start your computer, you notice that your OS is taking more time to boot than usual. You discuss this with your Network Administrator. He suggests that you mail him your Linux bootup report. Which of the following commands will you use to create the Linux bootup report?

A. touch bootup_report.txt
B. dmesg > bootup_report.txt
C. dmesg | wc
D. man touch

Answer: B

Explanation: According to the scenario, you can use dmesg > bootup_report.txt to create the bootup file. With this command, the bootup messages will be displayed and will be redirected towards bootup_report.txt using the > command.

Question No : 9 - (Topic 1)

Which of the following tools is used to make fake authentication certificates?

A. Obiwan
B. Netcat
C. WinSSLMiM
D. Brutus

Answer: C

Explanation:

WinSSLMiM is an HTTPS Man in the Middle attacking tool. It includes FakeCert, a tool used to make fake certificates. It can be used to exploit the Certificate Chain vulnerability in Internet Explorer. The tool works under Windows 9x/2000. For example, Generate fake certificate: fc -s www.we-are-secure.com -f fakeCert.crt Launch WinSSLMiM: wsm -f fakeCert.crt Answer: D is incorrect. Brutus is a password cracking tool that performs both dictionary and brute force attacks in which passwords are randomly generated from given characters. Brute forcing can be performed on the following authentications: HTTP (Basic Authentication) HTTP (HTML Form/CGI) POP3 (Post Office Protocol v3) FTP (File Transfer Protocol) SMB (Server Message Block) Telnet Answer: A is incorrect. Obiwan is a Web password cracking tool that is used to perform brute force and hybrid attacks. It is effective against HTTP connections for Web servers that allow unlimited failed login attempts by the user. Obiwan uses wordlists as well as alphanumeric characters as possible passwords. Answer: B is incorrect. Netcat is a freely available networking utility that reads and writes data across network connections by using the TCP/IP protocol. Netcat has the following features: It provides outbound and inbound connections for TCP and UDP ports. It provides special tunneling such as UDP to TCP, with the possibility of specifying all network parameters. It is a good port scanner. It contains advanced usage options, such as buffered send-mode (one line every N seconds), and hexdump (to stderr or to a specified file) of transmitted and received data. It is an optional RFC854 telnet code parser and responder.

Question No : 10 - (Topic 3)

Sarah works as a Web Developer for XYZ CORP. She develops a Web site for the company. She uses tables in the Web site. Sarah embeds three tables within a table. What is the technique of embedding tables within a table known as?

A. Nesting tables
B. Stacking tables
C. CSS tables
D. Horned tables

Answer: A

Explanation: In general, nesting means embedding a construct inside another. Nesting tables is a technique in which one or more tables are embedded within a table. Answer: B, C, D are incorrect. There are no techniques such as stacking tables, horned tables, or CSS tables.

Topic 2, Volume B

Question No : 11 - (Topic 2)

Which of the following firewalls inspects the actual contents of packets?

A. Circuit-level firewall
B. Stateful inspection firewall
C. Packet filtering firewall
D. Application-level firewall

Answer: D

Explanation: The application level firewall inspects the contents of packets, rather than the source/destination or connection between the two. An Application level firewall operates at the application layer of the OSI model. Answer: A is incorrect. The circuit-level firewall regulates traffic based on whether or not a trusted connection has been established. It operates at the session layer of the OSI model. Answer: C is incorrect. The packet filtering firewall filters traffic based on the headers. It operates at the network layer of the OSI model. Answer: B is incorrect. The stateful inspection firewall assures the connection between the two parties is valid and inspects packets from this connection to assure the packets are not malicious.

Question No : 12 - (Topic 2)

You want to record auditing information in the SYS.AUD$ table, and also want to record SQL bind variables as well as the SQL text in the audit trail. Which of the following statements will accomplish this task?

A. ALTER SYSTEM SET AUDIT_TRAIL = DB, XML SCOPE=SPFILE;
B. ALTER SYSTEM SET AUDIT_TRAIL = 'DB, EXTENDED' SCOPE=SPFILE;
C. ALTER SYSTEM SET AUDIT_TRAIL = 'DB','EXTENDED' SCOPE=SPFILE;
D. ALTER SYSTEM SET AUDIT_TRAIL = DB, EXTENDED SCOPE=SPFILE;
E. ALTER SYSTEM SET AUDIT_FILE_DEST = 'DB, EXTENDED' SCOPE=SPFILE;
F. ALTER SYSTEM SET AUDIT_TRAIL = DB, EXTENDED SCOPE=BOTH;

Answer: C,D

Explanation: The initialization parameter AUDIT_TRAIL is used to specify the kind of auditing that needs to be performed, as well as the destination where it will be performed. There are three basic values for auditing that are DB, OS, and XML. Specifying DB sends all audit rows to the table SYS.AUD$, OS sends the audit rows to an operating system file, and XML sends the audit rows to an operating system file in the XML format. The location for external audit rows is specified by the AUDIT_FILE_DEST parameter. By adding the EXTENDED parameter for either DB or XML auditing, all SQL bind variables and the text of all SQL commands are included in the audit row. EXTENDED cannot be specified for OS auditing. In addition, NONE can be specified as the value for AUDIT_TRAIL, which will disable all auditing. Answer: B is incorrect. DB, EXTENDED in single quotes cannot be specified when setting the AUDIT_TRAIL parameter. Answer: E is incorrect. AUDIT_TRAIL must be set to specify the type of auditing. AUDIT_FILE_DEST is used to specify the operating system location for either OS or XML auditing. Answer: A is incorrect. DB and XML auditing cannot be specified at the same time and the database must be restarted for the auditing change to go into effect.

Question No : 13 - (Topic 2)

Sam works as a Network Administrator for Blue Well Inc. All client computers in the company run the Windows Vista operating. Sam creates a new user account. He wants to create a temporary password for the new user such that the user is forced to change his

password when he logs on for the first time. Which of the following options will he choose to accomplish the task?

A. User cannot change password
B. Delete temporary password at next logon
C. User must change password at next logon
D. Password never expires

Answer: C

Explanation: Enabling the user must change password at next logon option will make the given password a temporary password. Enabling this option forces a user to change his existing password at next logon. Answer: B is incorrect. There is no such option in Windows Vista. Answer: D is incorrect. This option sets the password to never expire. Answer: A is incorrect. This option sets the existing password as a permanent password for the user. Only administrators can change the password of the user.

Question No : 14 - (Topic 1)

You work as a Network Administrator for XYZ CORP. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest network. You configure a new Windows Server 2008 server in the network. The new server is not yet linked to Active Directory. You are required to accomplish the following tasks: Add a new group named "Sales". Copy the "Returns" group from the older server to the new one. Rename the "Returns" group to "Revenue". View all group members, including for multiple groups/entire domain. You use Hyena to simplify and centralize all of these tasks. Which of the assigned tasks will you be able to accomplish?

A. Copy the "Returns" group to the new server.
B. Rename the "Returns" group to "Revenue".
C. Add the new group named "Sales".
D. View and manage all group members, including for multiple groups/entire domain.

Answer: A,B,C

Explanation: Hyena supports the following group management functions: Full group administration such as add, modify, delete, and copy Rename groups Copy groups from one computer to another View both direct and indirect (nested) group members for one or more groups [only for Active Directory] View all group members, including for multiple groups/entire domain [only for Active Directory] Answer: D is incorrect. All group members