GIAC

GSEC Exam

GIAC Security Essentials

Thank you for Downloading GSEC exam PDF Demo

You can Buy Latest GSEC Full Version Download

https://www.certkillers.net/Exam/GSEC

Question: 1

Which of the following is NOT the feature of SELinux in the Red Hat enterprise Linux?

A. SELinux does not provide Kernel-level security.
B. All process and files have a context.
C. SELinux implements Mandatory Access Control (MAC) security in Red Hat Enterprise Linux.
D. SELinux applies to all users, including root.

Answer: A

Explanation:
SELinux is an operating system based on Linux which includes Mandatory Access Control. The SELinux provides Kernel-level security for Red Hat Enterprise Linux.
Answer options C, B, and D are incorrect. These are the features of SELinux.

Question: 2

You have been hired by the company to upgrade its existing Windows NT 4.0 network to a Windows 2000 based network. In the past, the company's support group has faced difficult time because users changed the configuration of their workstations. Which of the following features of the Active Directory would best justify the move to the Windows 2000 network?

A. Dynamic domain name system (DDNS)
B. Organizational unit (OU)
C. Dynamic host configuration protocol (DHCP)
D. Group policy object (GPO)

Answer: D

Explanation:
Group policy object (GPO) is used to restrict users from changing the setting of their workstations in the network.
Group policy object (GPO) is a collection of group policy settings. It can be created using a Windows utility known as the Group Policy snap-in.
GPO affects the user and computer accounts located in sites, domains, and organizational units (OUs). The Windows operating system
supports two types of GPOs, i.e., local and non-local (Active Directory-based) GPOs.
Dynamic Domain Name System (DDNS) enables clients with dynamically assigned address to register directly with a server running the DNS
Service and update the DNS table dynamically.
Dynamic Host Configuration Protocol (DHCP) is a TCP/IP standard used to dynamically assign IP addresses to computers, so that they can communicate with other network services. It reduces the complexity of managing network client IP address configuration. A DHCP server configures DHCP-

CertKillers.net

enabled client computers on the network. It runs on servers only. It also provides integration with the Active Directory directory service.
An organizational unit (OU) is a type of Active Directory object (or container) in which user accounts, groups, computers, printers, applications,
file shares, and other organizational units within a single domain can be placed. It allows administrators to logically organize and store Active
Directory objects in a domain. OUs are used to contain and assign specific permissions to groups of objects, such as users and printers.
Reference: Microsoft TechNet Technical Information CD "Chapter 9 - Designing Active Directory Structure"

Question: 3

Which of the following devices connects two segments of the same local area network (LAN) but keeps traffic separate on the two segments?

A. Hub
B. Modem
C. Bridge
D. Switch

Answer: C

Explanation:
A bridge connects two segments of the same LAN but keeps traffic separate on the two segments.
A bridge is an interconnectivity device that connects two local area networks (LANs) or two segments of the same LAN using the same
communication protocols, and provides address filtering between them. Users can use this device to divide busy networks into segments and
reduce network traffic. A bridge broadcasts data packets to all the possible destinations within a specific segment. Bridges operate at the
data-link layer of the OSI model.
Answer option B is incorrect. Modem stands for Modulator-Demodulator. It is a device that enables a computer to transmit information over standard telephone lines. Since a computer stores information digitally and a telephone line is analog, a modem converts digital signals to analog and vice versa. The conversion of a digital signal to analog is known as modulation and that of an analog signal to digital is known as demodulation.
Answer option D is incorrect. A switch is a network connectivity device that brings media segments together in a central location. It reads the
destination's MAC address or hardware address from each incoming data packet and forwards the data packet to its destination. This reduces
the network traffic. Switches operate at the data-link layer of the OSI model.
Answer option A is incorrect. A hub is a device used to link computers in a network. It connects computers that have a common architecture,
such as Ethernet, ARCnet, FDDI, or Token Ring. All hub-computer connections for a particular network use the same type of cable, which can
be twisted-pair, coaxial, or fiber-optic. Hubs are generally used in star topology networks. Token Ring hubs are also known as Multistation

CertKillers.net

Access Units (MSAUs). A hub works on the physical layer of the OSI model.

Question: 4

You work as a Network Administrator for McRoberts Inc. The company has a Linux-based network. You have created a script named lf.cgi. You want to provide the following permissions on it:
rwsr-sr--
Which of the following commands will you execute?

A. chmod 2754
B. chmod 6754
C. chmod 7754
D. chmod 4754

Answer: B

Explanation:
According to the question, the permission set requires setting SID with the owner and the group. Moreover, the Read, Write, and Execute permissions on the script file are required for the owner, Read and Execute permissions for the group, and Read permission for others.
The chmod command is used to change the permissions. The last three digits, i.e., 754 will provide the required permissions to the owner,
group, and others. The digit 7 will provide the Read, Write, and Execute permissions to the owner. The digit 5 will provide the Read and
Execute permissions to the group. The digit 4 will provide the Read permission to others.
According to the question, you have to set SID for the owner and users. For the owner (SUID), you will have to add 4 as a prefix to the
permission number. For the group (SGID), you will have to add 2 as a prefix to it. For setting both the SIDs (SUID and SGID), you will have to
add 6 as a prefix to the permission set. Hence, in order to accomplish the task, you will have to run the following command:
chmod 6754
This will set the SID for the owner and group on the permission set of the lf.cgi script file. When SID is set, the Execute permission symbol x is replaced with s.

Question: 5

Which of the following records is the first entry in a DNS database file?

A. SOA
B. SRV
C. CNAME
D. MX

Answer: A

Explanation:

Start of Authority (SOA) record is the first record in any DNS database file. The SOA resource record includes the following fields: owner, TTL,
class, type, authoritative server, refresh, minimum TTL, etc.
Answer option C is incorrect. Canonical Name (CNAME) is a resource record that creates an alias for the specified Fully Qualified Domain Name
(FQDN). It hides the implementation details of a network from the clients that are connected to the network.
Answer option D is incorrect. MX is a mail exchange resource record in the database file of a DNS server. It specifies a mail exchange server for
a DNS domain name.
Answer option B is incorrect. SRV resource record is a DNS record that enables users to specify the location of servers for a specific service,
protocol, and DNS domain. For example, if there are two servers in a domain, creating SRV records specifies which hosts serve as Web
servers, and resolvers can then retrieve all the SRV resource records for the Web servers.

Question: 6

Which of the following terms describes software technologies that improve portability, manageability and compatibility of applications by encapsulating them from the underlying operating system on which they are executed?

A. Application virtualization
B. Encapsulation
C. System hardening
D. Failover

Answer: A

Explanation:
Application virtualization is an umbrella term that describes software technologies that improve portability, manageability and compatibility of
applications by encapsulating them from the underlying operating system on which they are executed. A fully virtualized application is not
installed in the traditional sense, although it is still executed as if it is. The application is fooled at runtime into believing that it is directly
interfacing with the original operating system and all the resources are managed by it, when in reality it is not. Application virtualization differs
from operating system virtualization in that in the latter case, the whole operating system is virtualized rather than only specific applications.
Answer option C is incorrect. 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 option B is incorrect. Encapsulation is an object-oriented programming term used to define the ability to contain and hide information
about an object, such as internal data structures and code. Encapsulation isolates the internal complexity of an object's operation from the

CertKillers.net

rest of the application. For example, when you set the width property on a command button, you do not need to know how the value is
stored and how the command button is resized.
Answer option D is incorrect. Failover is a term associated with cluster services. It refers to the ability of a server to immediately start servicing
the requests if a primary server fails. If the application services in a cluster-node fail, the Cluster Service generally tries to restart them on the
same node. If the services do not start, then it moves the services to another node in the cluster and restarts them on that node.

Question: 7

Which of the following frequencies are used by wireless standard 802.11n to operate?
Each correct answer represents a complete solution. Choose two.

A. 1 Ghz
B. 2 Ghz
C. 2.4 Ghz
D. 5 Ghz

Answer: CD

Explanation:
The wireless standard 802.11n operates at 2.4 Ghz and 5 Ghz frequencies.
IEEE 802.11n is an upcoming improvement to the IEEE 802.11-2007 wireless networking standard to improve network throughput over
previous standards, such as 802.11b and 802.11g. The IEEE 802.11n standard offers data rates from 54 Mbps to a maximum of 600 Mbps.
The current state of the art supports a physical rate of 450 Mbps, with the use of 3 spatial streams at a channel width of 40 MHz. Depending
on the environment, this may translate into a user throughput of 110 Mbps.

Question: 8

What is the maximum cable segment length supported by a 10BaseT network?

A. 100 meters
B. 300 meters
C. 250 meters
D. 500 meters
E. 150 meters

Answer: A

Explanation:
The most widely used Ethernet networks are 10BASE-T, 100BASE-TX, and 1000BASE-T (Gigabit Ethernet), running at 10 Mbit/s, 100 Mbit/s,

and 1000 Mbit/s (1 Gbit/s) respectively. These three standards all use the same connectors. Higher speed implementations nearly always
support the lower speeds as well, so that in most cases different generations of equipment can be freely mixed. They use 8 position modular
connectors, usually called RJ45 in the context of Ethernet over twisted pair. The cables usually used are four-pair or above twisted pair cable.
Each of the three standards support both full-duplex and half-duplex communication. According to the standards, they all operate over
distances of 'up to 100 meters'.

Question: 9

Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2003 domain-based network. The company has two offices in different cities. The offices are connected through the Internet. Both offices have a Windows 2003 server named SERV1 and SERV2 respectively. Mark is required to create a secure connection between both offices. He configures a VPN connection between the offices using the two servers. He uses L2TP for VPN and also configures an IPSec tunnel. Which of the following will he achieve with this configuration?
Each correct answer represents a part of the solution. Choose two.

A. Encryption for the local files stored on the two servers
B. Highest possible encryption for traffic between the offices
C. Mutual authentication between the two servers
D. Extra bandwidth on the Internet connection

Answer: BC

Explanation:
Configuration of an L2TP VPN connection and an IPSec tunnel between the offices, will provide the highest possible encryption for traffic between the offices as well as mutual authentication between the two servers.
L2TP uses IPSec for data encryption. This will ensure the highest possible level of encryption for traffic between the two offices, as well as mutual authentication without any additional hardware or software.

Question: 10

You have a customer who wants to put wireless internet in his remote cabin. The cabin is many miles from any other building with internet connectivity or access points. What should you recommend?

A. DSL
B. FIOS connection
C. Satellite internet
D. Microwave connection

Answer: C

CertKillers.net

Explanation:
Much like Satellite TV, Satellite internet does not require any physical connectivity and is available almost anywhere on the planet, since it uses orbiting satellites for connectivity. Speeds are not as fast as DSL, and the connectivity can be expensive.
Answer option D is incorrect. Microwave connections are very expensive and not available for residential internet use.
Answer options B and A are both incorrect. Both require local, physical connections and would not be available in a remote rural area.

Question: 11

Which of the following terms refers to manual assignment of IP addresses to computers and devices?

A. Static IP addressing
B. Spoofing
C. APIPA
D. Dynamic IP addressing

Answer: A

Explanation:
The Static IP addressing is the term used for manual assignment of IP addresses to computers and devices.
Answer option C is incorrect. Automatic Private IP Addressing (APIPA) is a Windows feature, which allows household users and small business
users to create a functional single subnet TCP/IP network without manually configuring the TCP/IP protocol or setting up a DHCP server.
Answer option D is incorrect. Dynamic IP addressing is used when IP addresses are assigned to computers and devices automatically by the
DHCP service or APIPA.
Answer option 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.

Question: 12

Which of the following statements regarding Secure Sockets Layer (SSL) are true?
Each correct answer represents a complete solution. Choose all that apply.

A. SSL provides message integrity to prevent alteration to the message.
B. During SSL session, information is encrypted to prevent unauthorized disclosure.
C. SSL can process credit cards.
D. SSL can support 128-bit encryption.

CertKillers.net

Answer: BAD

Explanation:
Secure Sockets Layer (SSL) is a protocol used to transmit private documents via the Internet. SSL uses a combination of public key and symmetric encryption to provide communication privacy, authentication, and message integrity. Using the SSL protocol, clients and servers can
communicate in a way that prevents eavesdropping and tampering of data on the Internet. Many Web sites use the SSL protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:. By default, SSL uses port 443 for secured communication.
Answer option C is incorrect. SSL can only secure the communication transport. Processing of credit cards cannot be done by SSL.

Question: 13

Which of the following protocols multicasts messages and information among all member devices in an IP multicast group?

A. IGMP
B. TCP
C. ARP
D. ICMP

Answer: A

Explanation:
Internet Group Management Protocol (IGMP) is a communication protocol that multicasts messages and information among all member devices in an IP multicast group. However, multicast traffic is sent to a single MAC address but is processed by multiple hosts. It can be effectively
used for gaming and showing online videos. IGMP is vulnerable to network attacks.
Answer option D is incorrect. Internet Control Message Protocol (ICMP) is an integral part of IP. It is used to report an error in datagram
processing. The Internet Protocol (IP) is used for host-to-host datagram service in a network. The network is configured with connecting
devices called gateways. When an error occurs in datagram processing, gateways or destination hosts report the error to the source hosts
through the ICMP protocol. The ICMP messages are sent in various situations, such as when a datagram cannot reach its destination, when
the gateway cannot direct the host to send traffic on a shorter route, when the gateway does not have the buffering capacity, etc.
Answer option C is incorrect. Address Resolution Protocol (ARP) is a network maintenance protocol of the TCP/IP protocol suite. It is
responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC). The ARP cache is
used to maintain a correlation between a MAC address and its corresponding IP address. ARP provides the protocol rules for making this

CertKillers.net

correlation and providing address conversion in both directions. ARP is limited to physical network systems that support broadcast packets.
Answer option B is incorrect. Transmission Control Protocol (TCP) is a reliable, connection-oriented protocol operating at the transport layer of
the OSI model. It provides a reliable packet delivery service encapsulated within the Internet Protocol (IP). TCP guarantees the delivery of
packets, ensures proper sequencing of data, and provides a checksum feature that validates both the packet header and its data for
accuracy. If the network corrupts or loses a TCP packet during transmission, TCP is responsible for retransmitting the faulty packet. It can
transmit large amounts of data. Application-layer protocols, such as HTTP and FTP, utilize the services of TCP to transfer files between clients and servers.

Question: 14

Which of the following is not an encryption technology?

A. Blowfish
B. KILL
C. 3DES
D. MD5

Answer: B

Explanation:
KILL is a command used to terminate a specified process.
Answer options A, C, and D are incorrect. Blowfish, 3DES, and MD5 are encryption technologies used to secure the communication between computers on the network.

Question: 15

Which of the following statements about the availability concept of Information security management is true?

A. It ensures reliable and timely access to resources.
B. It determines actions and behaviors of a single individual within a system.
C. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.
D. It ensures that modifications are not made to data by unauthorized personnel or processes.

Answer: A

Explanation:
The concept of availability ensures reliable and timely access to data or resources. In other words, availability ensures that the systems are up and running when needed. The availability concept also ensures that the security services are in working order.
Answer options D and C are incorrect. The concept of integrity ensures that modifications are not

CertKillers.net

made to data by unauthorized personnel or
processes. It also ensures that unauthorized modifications are not made to data by authorized personnel or processes.
Answer option B is incorrect. Accountability determines the actions and behaviors of an individual within a system, and identifies that particular individual. Audit trails and logs support accountability.

Question: 16

You work as a Network Administrator for Perfect World Inc. You are configuring a network that will include 1000BaseT network interface cards in servers and client computers. What is the maximum segment length that a 1000BaseT network supports?

A. 100 meters
B. 480 meters
C. 1000 meters
D. 10 meters

Answer: A

Explanation:
The maximum segment length that a 1000BaseT network supports is 100 meters. Type 1000BaseT network uses 5-level encoding and Cat 5 UTP media. It can provide data transmission speeds of up to 1000 megabits per second.

Question: 17

The /cat/etc/passwd file on a client computer contains the following entry:
Martha:x:::::bin/false
Which of the following is true for Martha?

A. Martha's password is x.
B. Martha has full access on the computer.
C. Martha has limited access on the computer.
D. Martha has been denied access on the computer.

Answer: D

Explanation:
In order to deny access to a user account, an invalid shell such as /bin/false should be assigned for the user account in the /etc/passwd file. When an invalid shell is assigned to a user account, a user cannot use the computer. You can take the following steps to deny access for a user to the computer:
1.Edit the /etc/passwd file and make the appropriate changes.
2.Use the -s switch with the USERMOD command.
3.Use CHSH -s /bin/false <user name> command.
Alternatively, you can use the USERMOD -l <user name> command at the command prompt to lock the user account.

CertKillers.net

Question: 18

Which of the following terms is synonymous with the willful destruction of another person's property?

A. Spoofing
B. Hacking
C. Phishing
D. Vandalism

Answer: D

Explanation:
Vandalism is the term synonymous with the willful destruction of another person's property.
Answer option B 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 the network.
Answer option A 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 option C is incorrect. Phishing is a type of scam that entices a user to disclose personal information, such as social security number,
bank account details, or credit card number. An example of phishing attack is a fraudulent e-mail that appears to come from a user's bank asking to change his online banking password. When the user clicks the link available on the e-mail, it directs him to a phishing site that
replicates the original bank site. The phishing site lures the user to provide his personal information.

Question: 19

Which of the following is used to implement a procedure to control inbound and outbound traffic on a network?

A. Cookies
B. Sam Spade
C. NIDS
D. ACL

Answer: D

Explanation:
Access Control List (ACL) is the most commonly method used to implement a procedure to control inbound and outbound traffic on the network.
It filters traffic packets by controlling whether or not inbound and outbound packets are forwarded or blocked at the router's interfaces.
According to the criteria specified within the access lists, router determines whether the packets are

CertKillers.net

to be forwarded or dropped. Access
control list criteria could be the source or destination address of the traffic or other information.
Answer option A 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. A Web server cannot access cookies created by other Web servers.
Answer option B is incorrect. Sam Spade is a penetration-testing tool that is used in the discovery phase. It provides GUI graphics and a lot of
functionalities. It can perform mainly whois queries, ping requests, DNS requests, tracerouting, OS finger-printing, zone transferring, SMTP mail
relay checking, and Web site crawling and mirroring. Sam Spade runs on Windows operating systems.
Answer option C is incorrect. A Network-based Detection System (NIDS) analyzes data packets flowing through a network. It can detect
malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules. It is responsible for detecting anomalous or
inappropriate data that may be considered 'unauthorized' on a network. An NIDS captures and inspects all data traffic, regardless of whether
or not it is permitted for checking.

Question: 20

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

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.

CertKillers.net

Thank You for trying GSEC PDF Demo

To Buy Latest GSEC Full Version Download visit link below

https://www.certkillers.net/Exam/GSEC

Start Your GSEC Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your GSEC preparation with actual exam questions.

CertKillers.net