# GIAC.GSEC.v2022-10-06.q104

| | |
|---|---|
| **Exam Code:** | GSEC |
| **Exam Name:** | GIAC Security Essentials Certification |
| **Certification Provider:** | GIAC |
| **Free Question Number:** | 104 |
| **Version:** | v2022-10-06 |
| **# of views:** | 1457 |
| **# of Questions views:** | 1040 |
| https://www.dumpsdb.com/dumps/GIAC/GSEC/GIAC.GSEC.v2022-10-06.q104 | |

**NEW QUESTION: 1**
Which of the following commands is used to change file access permissions in Linux?
**A.** chgrp
**B.** chown
**C.** chperm
**D.** chmod
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 2**
Which of the following is an advantage of private circuits versus VPNs?
**A.** Cost
**B.** Flexibility
**C.** Time required to implement
**D.** Performance guarantees
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 3**
Which common firewall feature can be utilized to generate a forensic trail of evidence and to identify attack trends against your network?
**A.** State Table
**B.** Logging
**C.** Content filtering
**D.** NAT
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 4**
Which of the following tools is used to configure, control, and query the TCP/IP network interface parameters?
**A.** IPCONFIG
**B.** IFCONFIG
**C.** NSLOOKUP
**D.** ARP
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 5**
You ask your system administrator to verify user compliance with the corporate policies on password strength, namely that all passwords will have at least one numeral, at least one letter, at least one special character and be 15 characters long. He comes to you with a set of compliance tests for use with an offline password cracker. They are designed to examine the following parameters of the password:
*they contain only numerals
*they contain only letters
*they contain only special characters
*they contain only letters and numerals
" they contain only letters and special characters
*they contain only numerals and special characters
Of the following, what is the benefit to using this set of tests?
**A.** They are focused on cracking passwords that use characters prohibited by the password policy
**B.** They find non-compliant passwords without cracking compliant passwords.
**C.** They crack compliant and non-compliant passwords to determine whether the current policy is strong enough
**D.** They are focused on cracking passwords that meet minimum complexity requirements
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 6**
Which of the following terms refers to manual assignment of IP addresses to computers and devices?
**A.** APIPA
**B.** Static IP addressing
**C.** Dynamic IP addressing
**D.** Spoofing
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 7**

Which of the following statements about Microsoft's VPN client software is FALSE?
**A.** The VPN client software is built into the Windows operating system.
**B.** The VPN interface can be figured into the route table.
**C.** The VPN interface has the same IP address as the interface to the network it's been specified to protect.
**D.** The VPN tunnel appears as simply another adapter.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 8**
Which of the following statements about DMZ are true? Each correct answer represents a complete solution. Choose two.
**A.** It is the boundary between the Internet and a private network.
**B.** It is an anti-virus software that scans the incoming traffic on an internal network.
**C.** It contains company resources that are available on the Internet, such as Web servers and FTP servers.
**D.** It contains an access control list (ACL).
**Answer: A,C (LEAVE A REPLY)**

**NEW QUESTION: 9**
At what point in the Incident Handling process should an organization determine its approach to notifying law enforcement?
**A.** When reacting to an incident
**B.** When preparing policy
**C.** When performing analysis
**D.** When recovering from the incident
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 10**
Which of the following are the types of access controls?
Each correct answer represents a complete solution. Choose three.
**A.** Physical
**B.** Administrative
**C.** Automatic
**D.** Technical
**Answer: A,B,D (LEAVE A REPLY)**

**NEW QUESTION: 11**
At what point in the Incident Handling process should an organization determine its approach to notifying law enforcement?
**A.** When preparing policy
**B.** When recovering from the incident

**C.** When performing analysis
**D.** When reacting to an incident
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 12**
Which of the following statements about Hypertext Transfer Protocol Secure (HTTPS) are true? Each correct answer represents a complete solution. Choose two.
**A.** It uses TCP port 80 as the default port.
**B.** It uses TCP port 443 as the default port.
**C.** It is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure site.
**D.** It is a protocol used to provide security for a database server in an internal network.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 13**
Which of the following heights of fence deters only casual trespassers?
**A.** 3 to 4 feet
**B.** 8 feet
**C.** 2 to 2.5 feet
**D.** 6 to 7 feet
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 14**
Which of the following is used to implement a procedure to control inbound and outbound traffic on a network?
**A.** NIDS
**B.** Sam Spade
**C.** ACL
**D.** Cookies
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 15**
Which of the following is a private, RFC 1918 compliant IP address that would be assigned to a DHCP scope on a private LAN?
**A.** 10.254.1.50
**B.** 127.0.0.100
**C.** 169.254.1.50
**D.** 172.35.1.100
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 16**

Which of the following TCP dump output lines indicates the first step in the TCP 3-way handshake?
**A.** 07:09:43.368615 download.net 39904 > ftp.com.21: S 733381829:733381829(0) win 8760 <mss 1460> (DF)
**B.** 07:09:43.370302 ftp.com.21 > download.net.39904: S 1192930639:1192930639(0} ack 733381830 win 1024 <mss 1460> (DF)
**C.** 09:09:22.346383 ftp.com.21 > download.net.39904: , rst 1 win 2440(DF)
**D.** 07:09:43.370355 download.net.39904 > ftp.com.21: , ack 1 win 8760 (DF)
**Answer: (SHOW ANSWER)**
Explanation



**NEW QUESTION: 17**
You work as a Network Administrator for NetTech Inc. The company wants to encrypt its e-mails. Which of the following will you use to accomplish this?
**A.** IPSec
**B.** PPTP
**C.** PGP
**D.** NTFS
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 18**
When using Pretty Good Privacy (PGP) to digitally sign a message, the signature is created in a two-step process. First, the message to be signed is submitted to PGP's cryptographic hash algorithm. What is one of the hash algorithms used by PGP for this process?
**A.** Cast
**B.** DES
**C.** SHA-I
**D.** Blowfish

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 19**
Which of the following monitors program activities and modifies malicious activities on a system?
**A.** RADIUS
**B.** NIDS
**C.** HIDS
**D.** Back door
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 20**
Which of the following protocols multicasts messages and information among all member devices in an IP multicast group?
**A.** IGMP
**B.** ARP
**C.** TCP
**D.** ICMP
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 21**
What is the main problem with relying solely on firewalls to protect your company's sensitive data?
**A.** Their value is limited because operating systems are now automatically patched.
**B.** Their value is limited unless a full-featured Intrusion Detection System is used.
**C.** Their value is limited because they can be bypassed by technical and non-technical means.
**D.** Their value is limited because they cannot be changed once they are configured.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 22**
You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network.
You are required to search for the error messages in the /var/log/messages log file. Which of the following commands will you use to accomplish this?
**A.** ps /var/log/messages
**B.** cat /var/log/messages | look error
**C.** cat /var/log/messages | grep error
**D.** cat /var/log/messages
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 23**
The following three steps belong to the chain of custody for federal rules of evidence. What additional step is recommended between steps 2 and 3?
STEP 1 - Take notes: who, what, where, when and record serial numbers of machine(s) in question.
STEP 2 - Do a binary backup if data is being collected.
STEP 3 - Deliver collected evidence to law enforcement officials.
**A.** Take photographs of all persons who have had access to the computer.
**B.** Conduct a forensic analysis of all evidence collected BEFORE starting the chain of custody.
**C.** Rebuild the original hard drive from scratch, and sign and seal the good backup in a plastic bag.
**D.** Check the backup integrity using a checksum utility like MD5, and sign and seal each piece of collected evidence in a plastic bag.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 24**
You have reason to believe someone with a domain user account has been accessing and modifying sensitive spreadsheets on one of your application servers. You decide to enable auditing for the files to see who is accessing and changing them. You enable the Audit Object Access policy on the files via Group Policy. Two weeks later, when you check on the audit logs, you see they are empty. What is the most likely reason this has happened?
**A.** You did not save the change to the policy
**B.** You did not enable auditing on the files
**C.** You cannot enable auditing on files, just folders
**D.** The person modifying the files turned off auditing
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 25**
An IT security manager is trying to quickly assess the risks associated with not implementing a corporate firewall system. What sort of risk assessment is most appropriate?
**A.** Quantitative risk assessment
**B.** Qualitative risk assessment
**C.** Annualized Risk Assessment
**D.** Iterative Risk Assessment
**E.** Technical Risk Assessment
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 26**

You work as a Network Administrator for Tech2tech Inc. You have configured a network-based IDS for your company. You have physically installed sensors at all key positions throughout the network such that they all report to the command console.
What will be the key functions of the sensors in such a physical layout?
Each correct answer represents a complete solution. Choose all that apply.
**A.** To collect data from operating system logs
**B.** To collect data from Web servers
**C.** To analyze for known signatures
**D.** To notify the console with an alert if any intrusion is detected
**Answer: C,D (LEAVE A REPLY)**

**NEW QUESTION: 27**
You work as a Network Administrator for Secure World Inc. The company has a Linux-based network. You want to run a command with the changed root directory. Which of the following commands will you use?
**A.** chdir
**B.** chroot
**C.** route
**D.** ls
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 28**
Which of the following is TRUE regarding Ethernet?
**A.** Ethernet is shared media.
**B.** Several stations are allowed to be transmitting at any given time within a single collision domain.
**C.** Stations are not required to monitor their transmission to check for collisions.
**D.** Stations are not required to listen before they transmit.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 29**
A Host-based Intrusion Prevention System (HIPS) software vendor records how the Firefox Web browser interacts with the operating system and other applications, and identifies all areas of Firefox functionality. After collecting all the data about how Firefox should work, a database is created with this information, and it is fed into the HIPS software. The HIPS then monitors Firefox whenever it's in use. What feature of HIPS is being described in this scenario?
**A.** Signature Matching
**B.** Application Behavior Monitoring
**C.** Host Based Sniffing
**D.** Application Action Modeling

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 30**
Which of the following tools is used to query the DNS servers to get detailed information about IP addresses, MX records, and NS servers?
**A.** NSLOOKUP
**B.** NETSTAT
**C.** PING
**D.** NBTSTAT
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 31**
How often is session information sent to the web server from the browser once the session information has been established?
**A.** With any hidden form element data
**B.** With any change in session data
**C.** With every subsequent request
**D.** With the initial request to register the session
**Answer: B (LEAVE A REPLY)**



**NEW QUESTION: 32**
Against policy, employees have installed Peer-to-Peer applications on their workstations and they are using them over TCP port 80 to download files via the company network from other Peer-to-Peer users on the Internet. Which of the following describes this threat?
**A.** Phishing attempt
**B.** Firewall subversion
**C.** Backdoor installation
**D.** Malicious software infection
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 33**
Which of the following statements about a bastion host is true?

**A.** It is a computer that is accessible from the Internet to collect information about internal networks.
**B.** It is a computer that must be made secure because it is accessible from the Internet and hence is more vulnerable to attacks.
**C.** It is a computer that is used to resolve the NetBIOS name to an IP address.
**D.** It is a computer that is used to resolve the host name to an IP address.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 34**
You have a home user as a customer. You need to configure her computer to use the appropriate IP address from her ISP. Which is the most likely way you will do this?
**A.** Get the IP from the ISP tech support and put it in as a dynamic IP.
**B.** Get the IP from the ISP tech support and put it in as a static IP.
**C.** Set the computer up for dynamic IP addresses using the ISP's preferred DHCP server.
**D.** Set the computer for dynamic IP addresses using a DHCP server in the customers home.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 35**
Which of the following statements would describe the term "incident" when used in the branch of security known as Incident Handling?
**A.** A and C
**B.** A, B, and C
**C.** Harm to systems
**D.** B and C
**E.** Any observable network event
**F.** Significant threat of harm to systems
**G.** A and B
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 36**
What would the following IP tables command do?
IP tables -I INPUT -s 99.23.45.1/32 -j DROP
**A.** Drop all packets to the specified address
**B.** Input all packers to the source address
**C.** Drop all packets from the source address
**D.** Log all packets to or from the specified address
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 37**

An employee is currently logged into the corporate web server, without permission. You log into the web server as 'admin" and look for the employee's username: "dmaul" using the "who" command. This is what you get back:

```
[user@localhost ~]$ who
admin :0 2010-09-11 06:49
dvader pts/3 2010-09-11 08:07 (localhost.localdomain)
hsolo pts/4 2010-09-11 08:14 (192.168.54.3)
cdooku pts/4 2010-09-11 08:14 (192.168.54.5)
```

**A.** The contents of the utmp file has been altered
**B.** The contents of the /var/log/messages file has been altered
**C.** The contents of the bash history file has been altered
**D.** The contents of the http logs have been altered
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 38**
Victor wants to send an encrypted message to his friend. He is using certain steganography technique to accomplish this task. He takes a cover object and changes it accordingly to hide information. This secret information is recovered only when the algorithm compares the changed cover with the original cover. Which of the following Steganography methods is Victor using to accomplish the task?
**A.** The cover generation technique
**B.** The substitution technique
**C.** The spread spectrum technique
**D.** The distortion technique
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 39**
When a host on a remote network performs a DNS lookup of www.google.com, which of the following is likely to provide an Authoritative reply?
**A.** The top-level DNS server for .com
**B.** The root DNS server
**C.** The DNS server for google.com
**D.** The local DNS server
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 40**
In preparation to do a vulnerability scan against your company's systems. You've taken the steps below:
You've notified users that there will be a system test.
You've priontized and selected your targets and subnets.
You've configured the system to do a deep scan.
You have a member of your team on call to answer questions.

Which of the following is a necessary step to take prior to starting the scan?
**A.** Placing the incident response team on call.
**B.** Getting permission to run the scan.
**C.** Scheduling the scan to run before OS updates.
**D.** Clear relevant system log files.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 41**
What type of malware is a self-contained program that has the ability to copy itself without parasitically infecting other host code?
**A.** Trojans
**B.** Viruses
**C.** Worms
**D.** Boot infectors
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 42**
Which of the following statements regarding the Secure Sockets Layer (SSL) security model are true?
Each correct answer represents a complete solution. Choose two.
**A.** The client can optionally authenticate the server.
**B.** The server can optionally authenticate the client.
**C.** The client always authenticates the server.
**D.** The server always authenticates the client.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 43**
You work as a Network Administrator for Net World Inc. The company has a Linux-based network.
You want to mount an SMBFS share from a Linux workstation. Which of the following commands can you
use to accomplish the task?
Each correct answer represents a complete solution. Choose two.
**A.** smbfsmount
**B.** mount smb
**C.** mount -t smbfs
**D.** smbmount
**Answer: C,D (LEAVE A REPLY)**

**NEW QUESTION: 44**
A folder D:\Files\Marketing has the following NTFS permissions:

* Administrators: Full Control
* Marketing: Change and Authenticated
* Users: Read
It has been shared on the server as "MARKETING", with the following share permissions:
* Full Control share permissions for the Marketing group
Which of the following effective permissions apply if a user from the Sales group accesses the \\FILESERVER
\MARKETING shared folder?
**A.** No access
**B.** Full Control
**C.** Read
**D.** Change
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 45**
You work as a Network Administrator for NetTech Inc. The company wants to encrypt its e-mails. Which of the following will you use to accomplish this?
**A.** PPTP
**B.** NTFS
**C.** IPSec
**D.** PGP
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 46**
Why would someone use port 80 for deployment of unauthorized services?
**A.** Google will detect the service listing on port 80 and post a link, so that people all over the world will surf to the rogue service.
**B.** If someone were to randomly browse to the rogue port 80 service they could be compromised.
**C.** This is a technique commonly used to perform a denial of service on the local web server.
**D.** HTTP traffic is usually allowed outbound to port 80 through the firewall in most environments.
**Answer: (SHOW ANSWER)**
Explanation/Reference:

**NEW QUESTION: 47**
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of
www.we-are-secure.com
. He traceroutes the We-are-secure server and gets the following result: Considering the above traceroute result, which of the following statements can be true? Each correct answer represents a complete solution. Choose all that apply.
**A.** While tracerouting, John's network connection has become slow.
**B.** The We-are-secure server is using a packet filtering firewall.
**C.** Some router along the path is down.
**D.** The IP address of the We-are-secure server is not valid.
**Answer: A,B,C (LEAVE A REPLY)**

**NEW QUESTION: 48**
Which Host-based IDS (HIDS) method of log monitoring utilizes a list of keywords or phrases that define the events of interest for the analyst, then takes a list of keywords to watch for and generates alerts when it sees matches in log file activity?
**A.** Passive analysis
**B.** Exclusive analysis
**C.** Inclusive analysis
**D.** Retroactive analysis
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 49**
Which of the following statements about Microsoft's VPN client software is FALSE?
**A.** The VPN interface has the same IP address as the interface to the network it's been specified to protect.
**B.** The VPN tunnel appears as simply another adapter.
**C.** The VPN client software is built into the Windows operating system.
**D.** The VPN interface can be figured into the route table.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 50**
You have just taken over network support for a small company. They are currently using MAC filtering to secure their wireless network. Is this adequate or not and why or why not?
**A.** Yes, in fact MAC filtering is the most security you can have.
**B.** No, you should have WEP or WPA encryption as well.
**C.** No, MAC filtering is not secure at all.

**D.** Yes, MAC filtering includes encryption.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 51**
While building multiple virtual machines on a single host operating system, you have determined that each virtual machine needs to work on the network as a separate entity with its own unique IP address on the same logical subnet. You also need to limit each guest operating system to how much system resources it has access to. Which of the following correctly identifies steps that must be taken towards setting up these virtual environments?
**A.** The virtual machine software must define a separate virtual network Interface to each virtual machine and then define which unique logical hard drive partition should be available to the guest operating system.
**B.** The virtual machine software must define a separate virtual network interface to each virtual machine as well as how much RAM should be available to each virtual machine.
**C.** The virtual machine software establishes the existence of the guest operating systems and the physical system resources to be used by that system will be configured from within the guest operating system.
**D.** The virtual machine software must define a separate physical network interface to each virtual machine so that the guest operating systems can have unique IP addresses and then define how much of the systems RAM is available to the guest operating system.
**E.** The virtual machine software must define a separate virtual network interface since each system needs to have an IP address on the same logical subnet requiring they use the same physical interface on the host operating system.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 52**
What would the file permission example "rwsr-sr-x" translate to in absolute mode?
**A.** 1644
**B.** 1755
**C.** 6755
**D.** 6645
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 53**
Which of the following is a remote access protocol that supports encryption?
**A.** PPP
**B.** SLIP
**C.** UDP
**D.** SNMP
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 54**
Which of the following would be a valid reason to use a Windows workgroup?
**A.** Lower initial cost
**B.** Simplicity of single sign-on
**C.** Consistent permissions and rights
**D.** Centralized control
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 55**
Regarding the UDP header below, what is the length in bytes of the UDP datagrarn?
04 1a 00 a1 00 55 db 51
**A.** 219
**B.** 85
**C.** 81
**D.** 161
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 56**
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 wants to change the modified date and time of the file private.txt to 11 Nov 2009 02:59:58 am. Which of the following commands will John use to accomplish his task? Each correct answer represents a complete solution. Choose all that apply.
**A.** touch -t 200911110259.58 private.txt
**B.** rm private.txt #11 Nov 2009 02:59:58 am
**C.** touch private.txt #11 Nov 2009 02:59:58 am
**D.** touch -d "11 Nov 2009 02:59:58 am" private.txt
**Answer: A,D (LEAVE A REPLY)**

**NEW QUESTION: 57**
Which of the following ports is the default port for Layer 2 Tunneling Protocol (L2TP) ?
**A.** TCP port 110
**B.** TCP port 443
**C.** UDP port 161
**D.** UDP port 1701
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 58**

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.** 1000 meters

**C.** 480 meters

**D.** 10 meters

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 59**

What file instructs programs like Web spiders NOT to search certain areas of a site?

**A.** Search.txt

**B.** Spider.txt

**C.** Restricted.txt

**D.** Robots.txt

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 60**

Which of the following utilities provides an efficient way to give specific users permission to use specific system commands at the root level of a Linux operating system?

**A.** SSH

**B.** SUDO

**C.** Snort

**D.** Apache

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 61**

Which of the following statements about policy is FALSE?

**A.** Policy protects people who are trying to do the right thing.

**B.** A well-written policy contains definitions relating to "what" to do.

**C.** Security policy establishes what must be done to protect information stored on computers.

**D.** A well-written policy states the specifics of "how" to do something.

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 62**
You are responsible for the wireless network of your company. You have been asked to create SSID's for wireless routers. What are the limits on an SSID?
Each correct answer represents a complete solution. Choose two.
**A.** It is not case sensitive.
**B.** It must be 32 or fewer characters long.
**C.** It must be 64 or fewer characters long.
**D.** It can only contain letters, not numbers.
**E.** It is case sensitive.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 63**
You work as a Network Administrator for McNeil Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest domain-based network. The company's management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks:
The wireless network communication should be secured.
The laptop users should be able to use smart cards for getting authenticated. In order to accomplish the tasks, you take the following steps:
Configure 802.1x and WEP for the wireless connections. Configure the PEAP-MS-CHAP v2 protocol for authentication. What will happen after you have taken these steps?
**A.** None of the tasks will be accomplished.
**B.** Both tasks will be accomplished.
**C.** The wireless network communication will be secured.
**D.** The laptop users will be able to use smart cards for getting authenticated.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 64**
Your organization has broken its network into several sections/segments, which are separated by firewalls, ACLs and VLANs. The purpose is to defend segments of the network from potential attacks that originate in a different segment or that attempt to spread across segments.
This style of defense-in-depth protection is best described as which of the following?
**A.** Uniform protection
**B.** Vector-oriented
**C.** Information-centric

**D.** Protected enclaves
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 65**
Which choice best describes the line below?
alert tcp any any -> 192.168.1.0/24 80 (content: /cgi-bin/test.cgi"; msg: "Attempted CGI-BIN Access!!";)
**A.** Snort rule
**B.** Wire shark filter
**C.** IP tables rule
**D.** Tcpdump filter
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 66**
You work as a Network Administrator for Tech Perfect Inc. The company has a Linux-based network. You want to kill a process running on a Linux server. Which of the following commands will you use to know the process identification number (PID) of the process?
**A.** killall
**B.** getpid
**C.** kill
**D.** ps
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 67**
Which of the following commands is used to change file access permissions in Linux?
**A.** chown
**B.** chgrp
**C.** chperm
**D.** chmod
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 68**
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 wants to change the modified date and time of the file private.txt to 11 Nov 2009 02:59:58 am. Which of the following commands will John use to accomplish his task?
Each correct answer represents a complete solution. Choose all that apply.
**A.** rm private.txt #11 Nov 2009 02:59:58 am
**B.** touch -t 200911110259.58 private.txt
**C.** touch -d "11 Nov 2009 02:59:58 am" private.txt
**D.** touch private.txt #11 Nov 2009 02:59:58 am

**Answer: B,C (LEAVE A REPLY)**

**NEW QUESTION: 69**
A sensor that uses a light beam and a detecting plate to alarm if the light beam is obstructed is most commonly used to identify which of the following threats?
**A.** Smoke
**B.** Toxins
**C.** Power
**D.** Water
**E.** Natural Gas
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 70**
With regard to defense-in-depth, which of the following statements about network design principles is correct?
**A.** A secure network design will seek to separate resources by providing a security boundary between systems that have different network security requirements.
**B.** A secure network design will seek to provide an effective administrative structure by providing a single choke-point for the network from which all security controls and restrictions will be enforced.
**C.** A secure network design requires that networks utilize VLAN (Virtual LAN) implementations to insure that private and semi-public systems are unable to reach each other without going through a firewall.
**D.** A secure network design requires that systems that have access to the Internet should not be accessible from the Internet and that systems accessible from the Internet should not have access to the Internet.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 71**
You have set up a local area network for your company. Your firewall separates your network into several sections: a DMZ with semi-public servers (web, dns, email) and an intranet with private servers. A penetration tester gains access to both sections and installs sniffers in each. He is able to capture network traffic for all the devices in the private section but only for one device (the device with the sniffer) in the DMZ. What can be inferred about the design of the system?
**A.** You installed a switch in the private section and a router in the DMZ
**B.** You installed a switch in the private section and a hub in the DMZ
**C.** You installed a router in the private section and a switch in the DMZ
**D.** You installed a hub in the private section and a switch in the DMZ
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 72**
Which of the following is an advantage of a Host Intrusion Detection System (HIDS) versus a Network Intrusion Detection System (NIDS)?
**A.** Ability to detect malicious traffic after it has been decrypted by the host
**B.** Ability to detect malicious traffic before it has been decrypted
**C.** Ability to listen to network traffic at the perimeter
**D.** Ability to decrypt network traffic
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 73**
Which of the following enables an inventor to legally enforce his right to exclude others from using his invention?
**A.** Spam
**B.** Patent
**C.** Artistic license
**D.** Phishing
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 74**
Which of the following TCP packet flags indicates that host should IMMEDIATELY terminate the connection containing the packet?
**A.** FIN
**B.** URG
**C.** SYN
**D.** RST
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 75**
What is the maximum passphrase length in Windows 2000/XP/2003?
**A.** 63 characters
**B.** 255 characters
**C.** 127 characters
**D.** 95 characters
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 76**
You are reviewing a packet capture file from your network intrusion detection system. In the packet stream, you come across a long series of "no operation" (NOP) commands. In addition to the NOP commands, there appears to be a malicious payload. Of the following, which is the most appropriate preventative measure for this type of attack?
**A.** Boundary checks on program inputs

**B.** Controls against time of check/time of use attacks
**C.** Limits on the number of failed logins
**D.** Restrictions on file permissions
**Answer: B (LEAVE A REPLY)**



**NEW QUESTION: 77**
Which of the following is an advantage of a Host Intrusion Detection System (HIDS) versus a Network Intrusion Detection System (NIDS)?
**A.** Ability to detect malicious traffic after it has been decrypted by the host
**B.** Ability to decrypt network traffic
**C.** Ability to listen to network traffic at the perimeter
**D.** Ability to detect malicious traffic before it has been decrypted
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 78**
Which of the following protocols describes the operation of security In H.323?
**A.** H.235
**B.** H.239
**C.** H.225
**D.** H.245
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 79**
A folder D:\Files\Marketing has the following NTFS permissions:
Administrators: Full Control
Marketing: Change and Authenticated
Users: Read
It has been shared on the server as "MARKETING", with the following share permissions:
Full Control share permissions for the Marketing group
Which of the following effective permissions apply if a user from the Sales group accesses the \\FILESERVER\MARKETING shared folder?
**A.** No access
**B.** Change

**C.** Read
**D.** Full Control
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 80**
You have implemented a firewall on the company's network for blocking unauthorized network connections. Which of the following types of security control is implemented in this case?
**A.** Detective
**B.** Directive
**C.** Preventive
**D.** Corrective
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 81**
While building multiple virtual machines on a single host operating system, you have determined that each virtual machine needs to work on the network as a separate entity with its own unique IP address on the same logical subnet. You also need to limit each guest operating system to how much system resources it has access to. Which of the following correctly identifies steps that must be taken towards setting up these virtual environments?
**A.** The virtual machine software must define a separate virtual network interface to each virtual machine as well as how much RAM should be available to each virtual machine.
**B.** The virtual machine software must define a separate virtual network interface since each system needs to have an IP address on the same logical subnet requiring they use the same physical interface on the host operating system.
**C.** The virtual machine software establishes the existence of the guest operating systems and the physical system resources to be used by that system will be configured from within the guest operating system.
**D.** The virtual machine software must define a separate physical network interface to each virtual machine so that the guest operating systems can have unique IP addresses and then define how much of the systems RAM is available to the guest operating system.
**E.** The virtual machine software must define a separate virtual network Interface to each virtual machine and then define which unique logical hard drive partition should be available to the guest operating system.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 82**
When Net Stumbler is initially launched, it sends wireless frames to which of the following addresses?
**A.** Subnet address

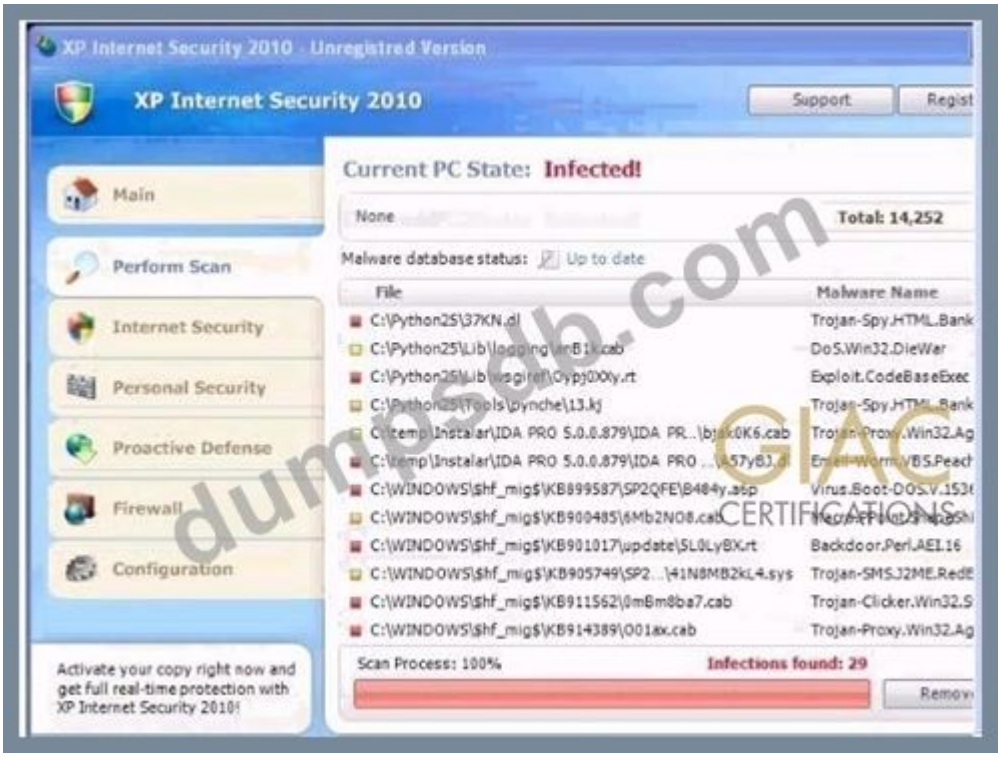
**B.** Broadcast address
**C.** Default gateway address
**D.** Network address
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 83**
What is the following sequence of packets demonstrating?
**A.** telnet.com.telnet > client.com.38060: F 4289:4289(0) ack 92 win 1024
**B.** telnet.com.telnet > client.com.38060: .ack 93 win 1024
**C.** client.com.38060 > telnet.com.telnet: .ack 4290 win 8760 (DF)
**D.** client.com.38060 > telnet.com.telnet: F 92:92(0) ack 4290 win 8760 (DF)
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 84**
An attacker gained physical access to an internal computer to access company proprietary data. The facility is protected by a fingerprint biometric system that records both failed and successful entry attempts.
No failures were logged during the time periods of the recent breach. The account used when the attacker entered the facility shortly before each incident belongs to an employee who was out of the area. With respect to the biometric entry system, which of the following actions will help mitigate unauthorized physical access to the facility?
**A.** Try to lower the False Accept Rate (FAR)
**B.** Try to set a lower False Reject Rate (FRR)
**C.** Try setting the Equal Error Rate (EER) to zero
**D.** Try raising the Crossover Error Rate (CER)
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 85**
Which of the following tools is also capable of static packet filtering?
**A.** netstat.exe
**B.** ipsecpol.exe
**C.** ipconfig.exe
**D.** net.exe
**Answer: B (LEAVE A REPLY)**
Explanation/Reference:

**NEW QUESTION: 86**
Analyze the screenshot below. What is the purpose of this message?




**A.** To get the user to download malicious software
**B.** To gather non-specific vulnerability information
**C.** To test the browser plugins for compatibility
**D.** To alert the user to infected software on the computer.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 87**
Drag and drop the appropriate protocols in front of their descriptions.
**Answer:**
Answer: A

**NEW QUESTION: 88**
What is the term for a game in which for every win there must be an equivalent loss?
**A.** Untenable
**B.** Zero-sum
**C.** Gain-oriented
**D.** Asymmetric
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 89**
For most organizations, which of the following should be the highest priority when it comes to physical security concerns?
**A.** Controlling access to servers
**B.** Controlling access to workstations
**C.** Protecting physical assets

**D.** Controlling ingress and egress
**E.** Ensuring employee safety
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 90**
Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2003 domain- based network. The network contains ten Windows 2003 member servers, 150 Windows XP Professional client computers. According to the company's security policy, Mark needs to check whether all the computers in the network have all available security updates and shared folders. He also needs to check the file system type on each computer's hard disk. Mark installs and runs MBSACLI.EXE with the appropriate switches on a server.
Which of the following tasks will he accomplish?
**A.** None of the tasks will be accomplished.
**B.** He will be able to check the file system type on each computer's hard disk.
**C.** He will be able to accomplish all the tasks.
**D.** He will be able to check all available security updates and shared folders.
**Answer: C (LEAVE A REPLY)**
Explanation

**NEW QUESTION: 91**
What is the name of the registry key that is used to manage remote registry share permissions for the whole registry?
**A.** rrsreg
**B.** regkey
**C.** winreg
**D.** regmng
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 92**
What is the unnoticed theft of sensitive data from a laptop owned by an organization's CEO an example of in information warfare?
**A.** Zero-sum game

**B.** Win-win situation
**C.** Symmetric warfare
**D.** Non-zero sum game
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 93**
What will be displayed as the output by using the following command?
TAIL /var/log/messages
**A.** The first ten lines of the /var/log/messages log file.
**B.** An error message because of insufficient parameters.
**C.** The last ten lines of the /var/log/messages log file.
**D.** All lines of the /var/log/messages log file.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 94**
What type of attack can be performed against a wireless network using the tool Kismet?
**A.** Eavesdropping
**B.** Denial of Service
**C.** Masquerading
**D.** IP spoofing
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 95**
In order to capture traffic for analysis, Network Intrusion Detection Systems (NIDS) operate with network cards in what mode?
**A.** Reporting
**B.** Promiscuous
**C.** Discrete
**D.** Alert
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 96**
What protocol is a WAN technology?
**A.** Frame Relay
**B.** Ethernet
**C.** 802.11
**D.** 802.3
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 97**
Where is the source address located in an IPv4 header?

**A.** At an offset of 12 bytes
**B.** At an offset of 20 bytes
**C.** At an offset of 8 bytes
**D.** At an offset of 16 bytes
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 98**
You work as a Linux Technician for Tech Perfect Inc. The company has a Linux-based network. You have configured a database server in the network. Users complain that the server has become remarkably slow. However, the previous day, the server was performing well. You know that some of the processes may be the cause of the issue. You run the PS command on the server. In the result set, which information will you look at that suggests the problematic process?
**A.** A high process ID
**B.** A high load average
**C.** A low CPU time
**D.** A low load average
**E.** A high CPU time
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 99**
You work as a Network Administrator for Tech Perfect Inc. The company has a Linux-based network. You have configured a VPN server for remote users to connect to the company's network. Which of the following encryption types will Linux use?
**A.** MSCHAP
**B.** 3DES
**C.** CHAP
**D.** RC2
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 100**
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
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 101**

Which of the following is a required component for successful 802.lx network authentication?
**A.** Ticket Granting Server (TGS)
**B.** Supplicant
**C.** IPSec
**D.** 3rd-party Certificate Authority
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 102**
Which choice best describes the line below?
alert tcp any any -> 192.168.1.0/24 80 (content: /cgi-bin/test.cgi"; msg: "Attempted CGI-BIN Access!!";)
**A.** Wire shark filter
**B.** IP tables rule
**C.** Tcpdump filter
**D.** Snort rule
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 103**
You have implemented a firewall on the company's network for blocking unauthorized network connections.
Which of the following types of security control is implemented in this case?
**A.** Directive
**B.** Preventive
**C.** Corrective
**D.** Detective
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 104**
If a DNS client wants to look up the IP address for good.news.com and does not receive an authoritative reply from its local DNS server, which name server is most likely to provide an authoritative reply?
**A.** The .com (top-level) domain name server
**B.** The .(root-level) domain name server
**C.** The .gov (top-level) domain name server
**D.** The news.com domain name server
**Answer: (SHOW ANSWER)**