EX0-107 V8.02_formatted

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

http://www.gratisexam.com/

Exam : EX0-107

Title : SCNP Strategic

Infrastructure Security

Version : V8.02

Exam A

QUESTION 1
In the process of public key cryptography, which of the following is true?

A. Only the public key is used to encrypt and decrypt
B. Only the private key can encrypt and only the public key can decrypt
C. Only the public key can encrypt and only the private key can decrypt
D. The private key is used to encrypt and decrypt
E. If the public key encrypts, then only the private key can decrypt

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
As per the guidelines in the ISO Security Policy standard, what is the purpose of the section on Physical and Environmental Security?

A. The objectives of this section are to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements, and to ensure compliance of systems with organizational security policies and standards.
B. The objectives of this section are to prevent unauthorized access, damage and interference to business premises and information; to prevent loss, damage or compromise of assets and interruption to business activities; to prevent compromise or theft of information and information processing facilities.
C. The objectives of this section are to provide management direction and support for information security.
D. The objectives of this section are to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.
E. The objectives of this section are to control access to information, to prevent unauthorized access to information systems, to ensure the protection of networked services, and to prevent unauthorized computer access.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
During a one week investigation into the security of your network you work on identifying the information that is leaked to the Internet, either directly or indirectly. One thing you decide to evaluate is the information stored in the Whois lookup of your organizational website. Of the following, what pieces of information can be identified via this method?

A. Registrar
B. Mailing Address
C. Contact Name
D. Record Update
E. Network Addresses (Private)

Correct Answer: ABCD

Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
You are aware of the significance and security risk that Social Engineering plays on your company. Of the following Scenarios, select those that, just as described, represent potentially dangerous Social Engineering:

A. A writer from a local college newspapers calls and speaks to a network administrator. On the call the writer requests an interview about the current trends in technology and offers to invite the administrator to speak at a seminar.
B. An anonymous caller calls and wishes to speak with the receptionist. On the call the caller asks the receptionist the normal business hours that the organization is open to the public.
C. An anonymous caller calls and wishes to speak with the purchaser of IT hardware and software. On the call the caller lists several new products that the purchaser may be interested in evaluating. The caller asks for a time to come and visit to demonstrate the new products.
D. An email, sent by the Vice President of Sales and Marketing, is received by the Help Desk asking to reset the password of the VP of Sales and Marketing.
E. An email is received by the Chief Security Officer (CSO) about a possible upgrade coming from the ISP to a different brand of router. The CSO is asked for the current network's configuration data and the emailer discusses the method, plan, and expected dates for the rollover to the new equipment.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
During the review of the security logs you notice some unusual traffic. It seems that a user has connected to your Web site ten times in the last week, and each time has visited every single page on the site. You are concerned this may be leading up to some sort of attack.
What is this user most likely getting ready to do?

A. Mirror the entire web site.
B. Download entire DNS entries.
C. Scan all ports on a web server.
D. Perform a Distributed Denial of Service attack through the Web server.
E. Allow users to log on to the Internet without an ISP.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
What type of cipher is used by an algorithm that encrypts data one bit at a time?

A. 64-bit encryption Cipher
B. Block Cipher
C. Stream Cipher
D. Diffuse Cipher
E. Split Cipher

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
You have just become the senior security professional in your office. After you have taken a complete inventory of the network and resources, you begin to work on planning for a successful security implementation in the network. You are aware of the many tools provided for securing Windows 2003 machines in your network.
What is the function of Secedit.exe?

A. This tool is used to set the NTFS security permissions on objects in the domain.
B. This tool is used to create an initial security database for the domain.
C. This tool is used to analyze a large number of computers in a domain-based infrastructure.
D. This tool provides an analysis of the local system NTFS security.
E. This tool provides a single point of management where security options can be applied to a local computer or can be imported to a GPO.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

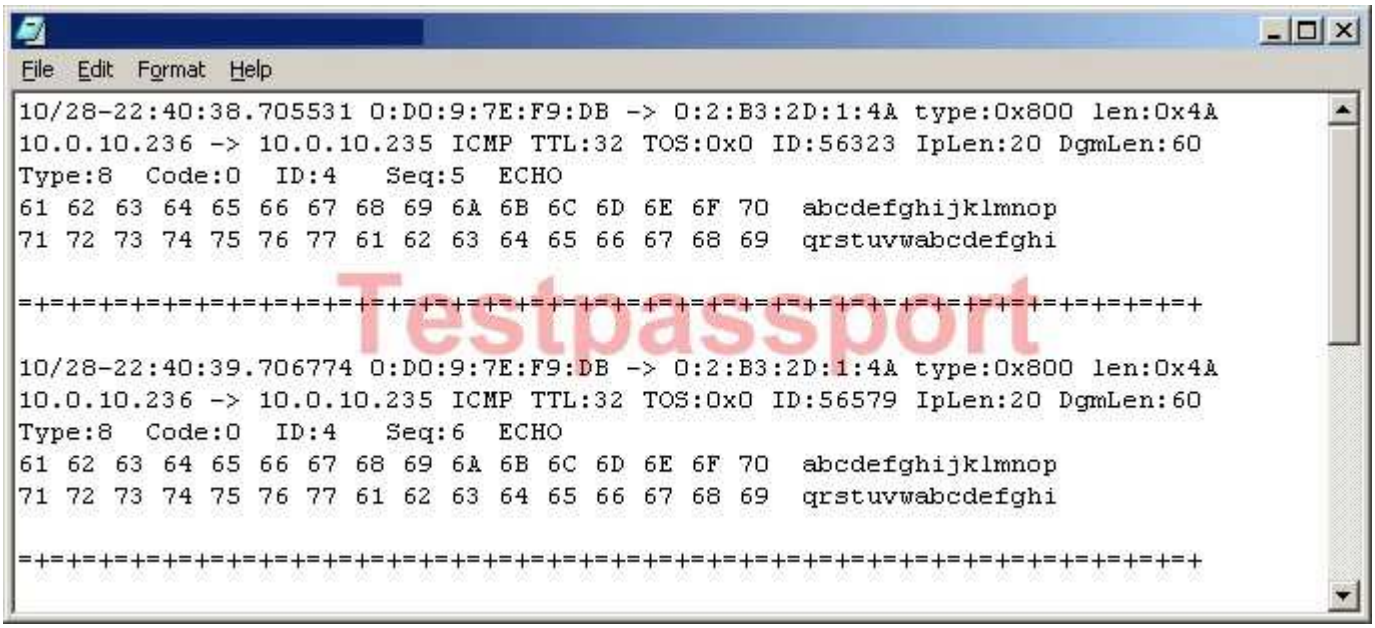
QUESTION 8
To increase the security of your network and systems, it has been decided that EFS will be implemented in the appropriate situations. Two users are working on a common file, and often email this file back and forth between each other.
Is this a situation where the use of EFS will create effective security, and why (or why not)?

A. No, the security will remain the same since both users will share the same key for encryption.
B. Yes, since the file will be using two keys for encryption the security will increase.
C. No, the security will remain the same since both users will share the same key for decryption.
D. Yes, since the file will be using two keys for decryption the security will increase.
E. No, EFS cannot be used for files that are shared between users.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?



A. Windows 2000 Ping Request
B. Windows NT 4.0 Ping Request
C. Linux Ping Request
D. Linux Ping Response
E. Windows NT 4.0 Ping Response

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
In order for your newly written security policy to have any weight, it must be implemented. Which of the following are the three components of a successful Security Policy Implementation in an organization?

A. Policy Monitoring
B. Policy Design
C. Policy Committee
D. Policy Enforcement
E. Policy Documentation

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Attackers have the ability to use programs that are able to reveal local passwords by placing some kind of a pointer/cursor over the asterisks in a program's password field. The reason that such tools can uncover passwords in some Operating Systems is because:

A. the passwords are simply masked with asterisks
B. the etc/passwd file is on a FAT32 partition
C. the passwords are decrypted on screen
D. the password text is stored in ASCII format
E. the etc/passwd file is on a FAT16 partition

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
You have become the lead security professional for a mid-sized organization. You are currently studying DNS issues, and configuration options. You come across the concepts of DNS Spoofing, and investigate more. What is DNS Spoofing?

A. DNS Spoofing is when the DNS client submits a false DNS request to the DNS server, and the DNS server responds with correct data.
B. DNS Spoofing is the DNS client submits a DNS request to the DNS server using a bogus IP address, and the DNS server responds to the incorrect host.
C. DNS Spoofing is when a DNS Server responds to an unauthorized DNS client, providing that client with name resolution.
D. DNS Spoofing is when a DNS client is forced to make a DNS query to an imposter DNS server, which send the client to an imposter resource.
E. DNS spoofing is when a DNS server provides name resolution to clients that are located in a different IP subnet than the server itself.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
What is a problem with symmetric key cryptography?

A. It is slower than asymmetric key cryptography
B. Secure distribution of the public key
C. There is a lack of encryption protocols that can use symmetric key cryptography
D. Secure distribution of a secret key
E. Symmetric key cryptography is reserved for the NSA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
What is the name of the informational page that is relevant to a particular command in Linux?

A. Readme Page
B. Lnx_nfo Page
C. Man Page
D. X_Win Page
E. Cmd_Doc Page

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
You have just downloaded a new file, called scnpfile.tar.gz. You are going to verify the file prior to un-archiving the file.
Which command do you need to type to un-compress the file, prior to un-archiving?

A. tar xvf scnpfile.tar.gz
B. tar -zxvf scnpfile.tar.gz
C. gunzip scnpfile.tar.gz
D. gunzip -xvf scnpfile.tar.gz
E. gunzip -zxvf scnpfile.tar.gz

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
You are configuring the lines that control access to exported objects on your server running NFS. If you have a directory called /Tech and you wish to export this directory to network 192.168.20.0/24, allowing root access, and the permissions of read and write, which of the following lines will accomplish this?

A. (RW) no_root_squash /Tech 192.168.20.0/24
B. /Tech 192.168.20.0/24 (rw) no_root_squash
C. (RW) no_root_squash 192.168.20.0/24 /Tech
D. (RW)no_root_squash:/Tech 192.168.20.0/24
E. /Tech 192.168.20.0/24(rw) no_root_squash

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
You are working on the authentication systems in your network, and are concerned with your legacy systems. In Windows NT 4.0, before Service Pack 4 (SP4), there were only two supported methods of authentication. What were those two methods?

A. NetBIOS
B. LM
C. NTLM
D. NTLMv2
E. Kerberos

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

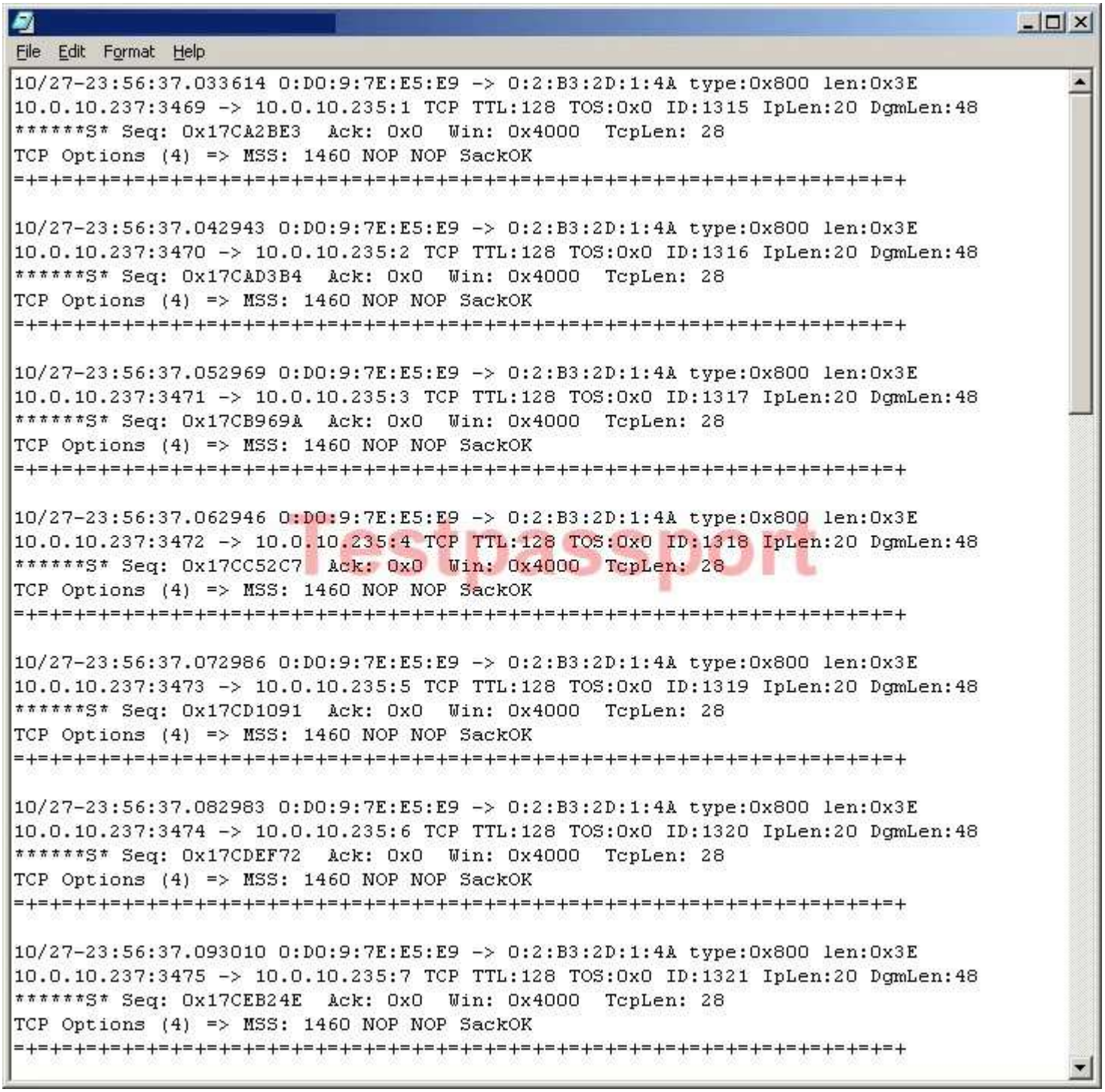
QUESTION 19
If you encrypt or decrypt files and folders located on a remote computer that has been enabled for remote encryption; the data that is transmitted over the network by this process is not encrypted. In order to keep data encrypted as it is transmitted over the network, which of the following must you do?

A. You must implement EFS.
B. You must implement B2 security for Windows.
C. You must use IPSec.
D. You must use a recovery agent.
E. You must transmit the entire folder, not individual files.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?



A. NetBus Scan
B. Trojan Scan
C. Ping Sweep
D. Port Scan

E. Ping Sweep

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
As per the guidelines in the ISO Security Policy standard, what is the purpose of the section on Business Continuity Planning?

A. The objectives of this section are to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.
B. The objectives of this section are to provide management direction and support for information security.
C. The objectives of this section are to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.
D. The objectives of this section are to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements, and to ensure compliance of systems with organizational security policies and standards.
E. The objectives of this section are to control access to information, to prevent unauthorized access to information systems, to ensure the protection of networked services, and to prevent unauthorized computer access.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
On Monday, during a routine check of a users Windows workstation, you find the following program, called regedit.bat on the users local hard drive:
Net localgroup administrators local /all
Start regedit.exe
Exit
What is this program capable of doing on this computer?

A. Nothing, the first line is coded wrong.
B. It will add the administrators to the local group
C. It will add the local user to all local groups
D. It will add the administrators to all local groups
E. It will add the local user to the administrators group

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Often times attackers will run scans against the network to identify different network and operating systems, and resources that are available.

If an attacker runs scans on the network, and you are logging the connections, which of the following represent the legitimate combination of packets that will be sent between the attacker and target?

A. Attacker PSH-FIN Scan, Target RST-FIN Response
B. Attacker ACK Scan, Target NULL Response
C. Attacker NULL Scan, Target RST Response
D. Attacker SYN Scan, Target NULL Response
E. Attacker FIN Scan, Target RST Response

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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 Internets 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.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
When using the 3DES encryption (C = EK1[DK2[EK1[P]]]), what is the function of C?

A. C is the text before encryption
B. C is the first encryption key
C. C is the second encryption key
D. C is the decryption key
E. C is the text after encryption

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following are symmetric encryption algorithms?

A. MD5

B. RSA
C. Diffie-Hellman
D. 3DES
E. AES

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
During the configuration of your Linux system, you are working with the available drives in the computer. What syntax defines the First (Primary) IDE hard disk drive?

A. /dev/sda
B. /dev/fda
C. /dev/hd1
D. /dev/hda
E. /dev/fd1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
You are configuring the permissions to a file, called file1, on your Linux file server. You wish to change the permissions to remove the execute permission from the others and group.
Which of the following commands will complete this task?

A. umask x-og file1
B. umask og-x file1
C. chmod xog- file1
D. chmod x-og file1
E. chmod og-x file1

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
In the past it was, at times, difficult to locate current information on security vulnerabilities. What is the name of the security communitys effort to create a comprehensive database of multiple vulnerabilities and security tools?

A. Common Vulnerabilities and Exploits
B. Cataloged Venerations and Exposures
C. Common Vulnerabilities and Exposures

D. Cataloged Vulnerabilities and Exposures
E. Cataloged Vulnerabilities and Exploits

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following answers is the word SECURITY after having been encrypted using the following Polybius Cipher shown in the figure?

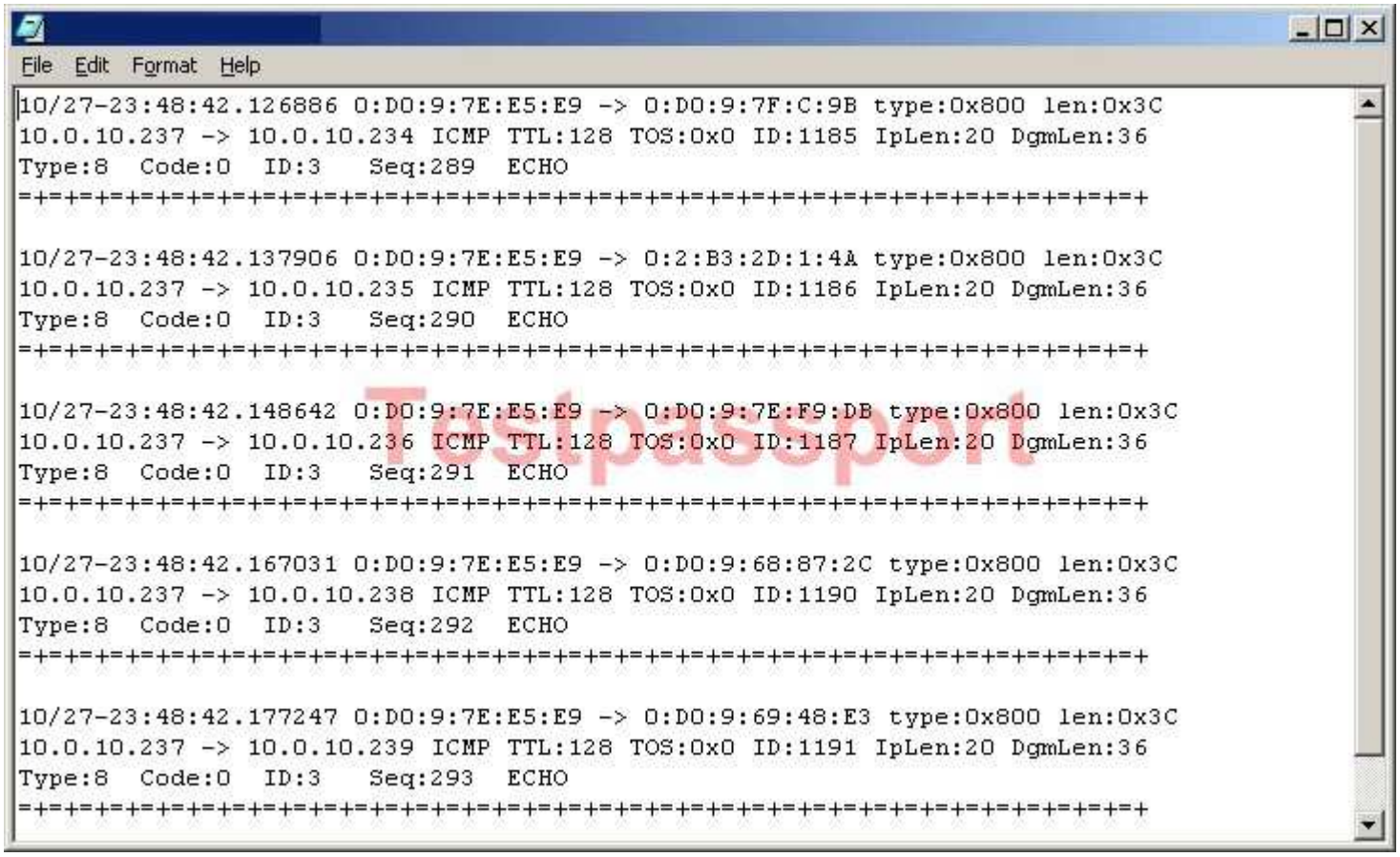
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

A. 280
B. 34 51 31 54 24 42 44 45
C. 7 6 8 9 6 6 8 9
D. 43 15 13 45 42 24 44 54
E. 4315 4224 1345 4454

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

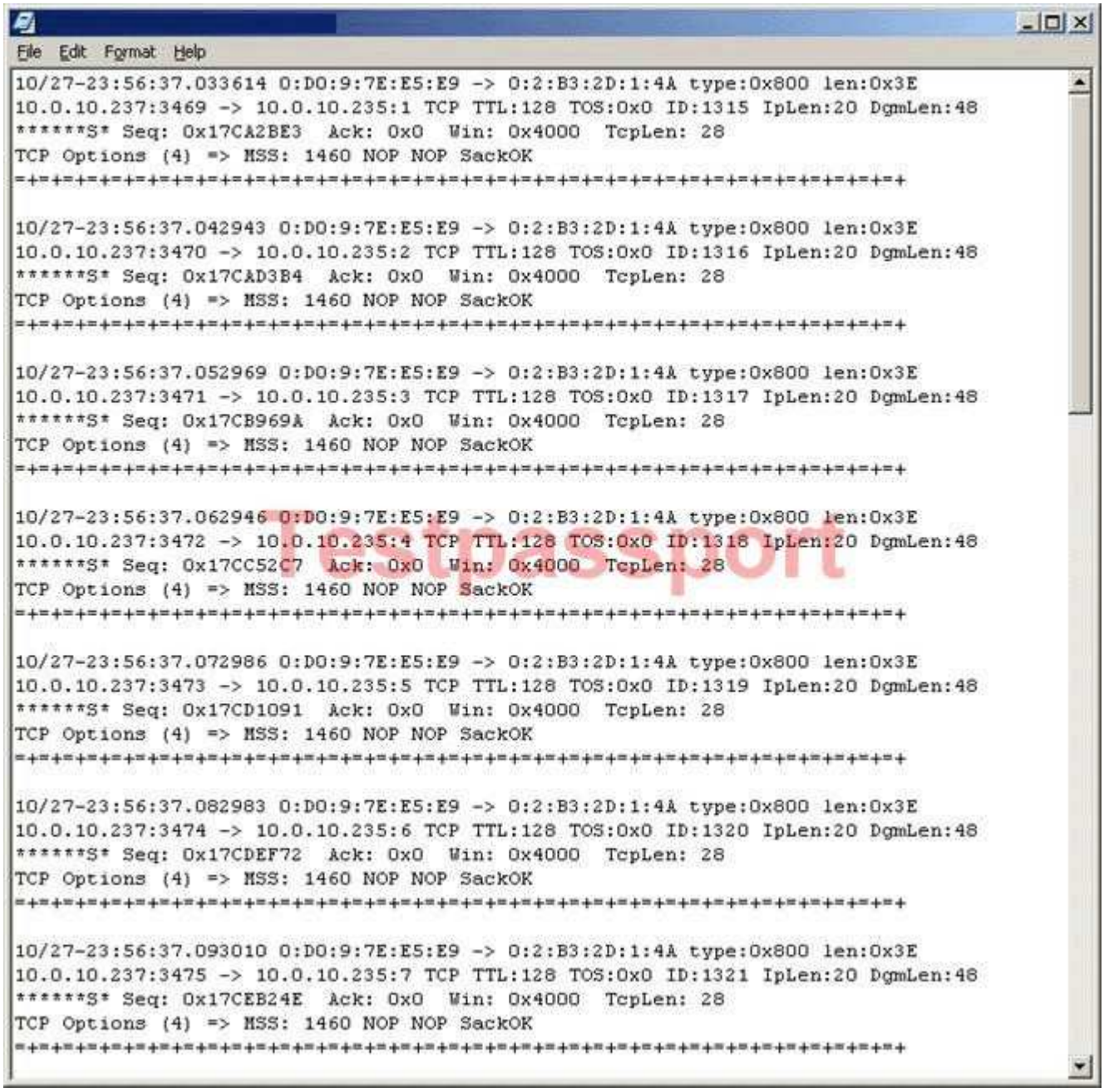


A. Nmap Scan
B. Port Scan
C. Trojan Scan
D. Ping Request
E. Ping Sweep

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?



A. NetBus Scan
B. Trojan Scan
C. Ping Sweep
D. Port Scan
E. Ping Sweep

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

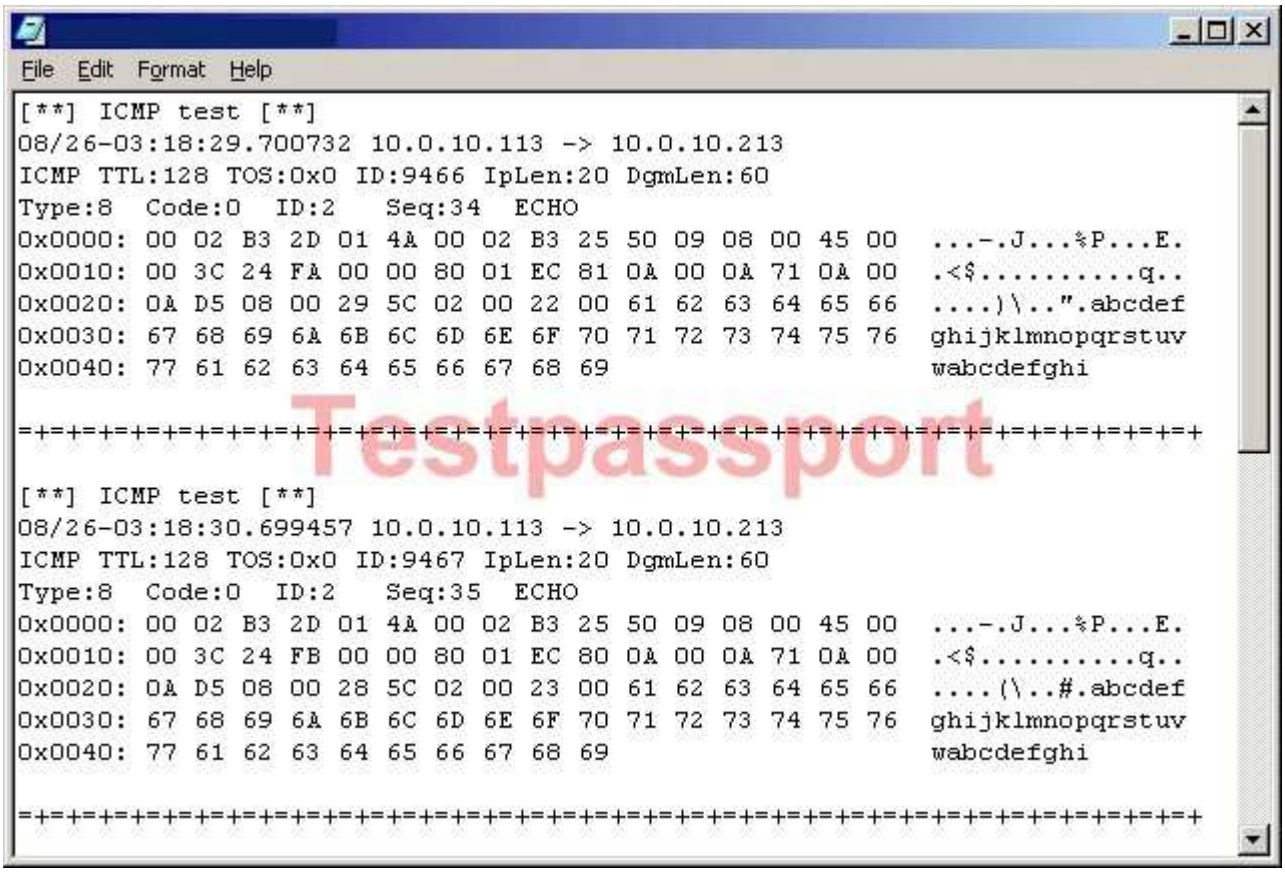
QUESTION 33
If you wish to change the permissions of a parent directory in your Linux system, and want the permissions to be changed on the files and subdirectories in the parent directory to be the same, what switch must you use?

A. -G
B. -R
C. -P
D. -S
E. -F

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?



A. Linux Ping Reply
B. Windows 2000 Ping Reply
C. Windows NT 4.0 Ping Request
D. Linux Ping Request
E. Windows 2000 Ping Request

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
It has come to your attention that some machine has tried to send a packet to your DNS server containing both a DNS query and an answer that is false.
What type of attack was used against your network?

A. DNS overflow
B. DNS poisoning through sequence prediction
C. Statd overflow
D. DNS cache poisoning
E. DNS parse corruption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
What type of an attack would someone be using if they sent a packet to their target with identical source and destination IP address and port (which is the address of the target machine) which can cause a system to go into an infinite loop trying to complete a connection?

A. SYN loop
B. WinNuke
C. SYN flood
D. Ping of death
E. Land attack

Correct Answer: E
Section: (none)
Explanation

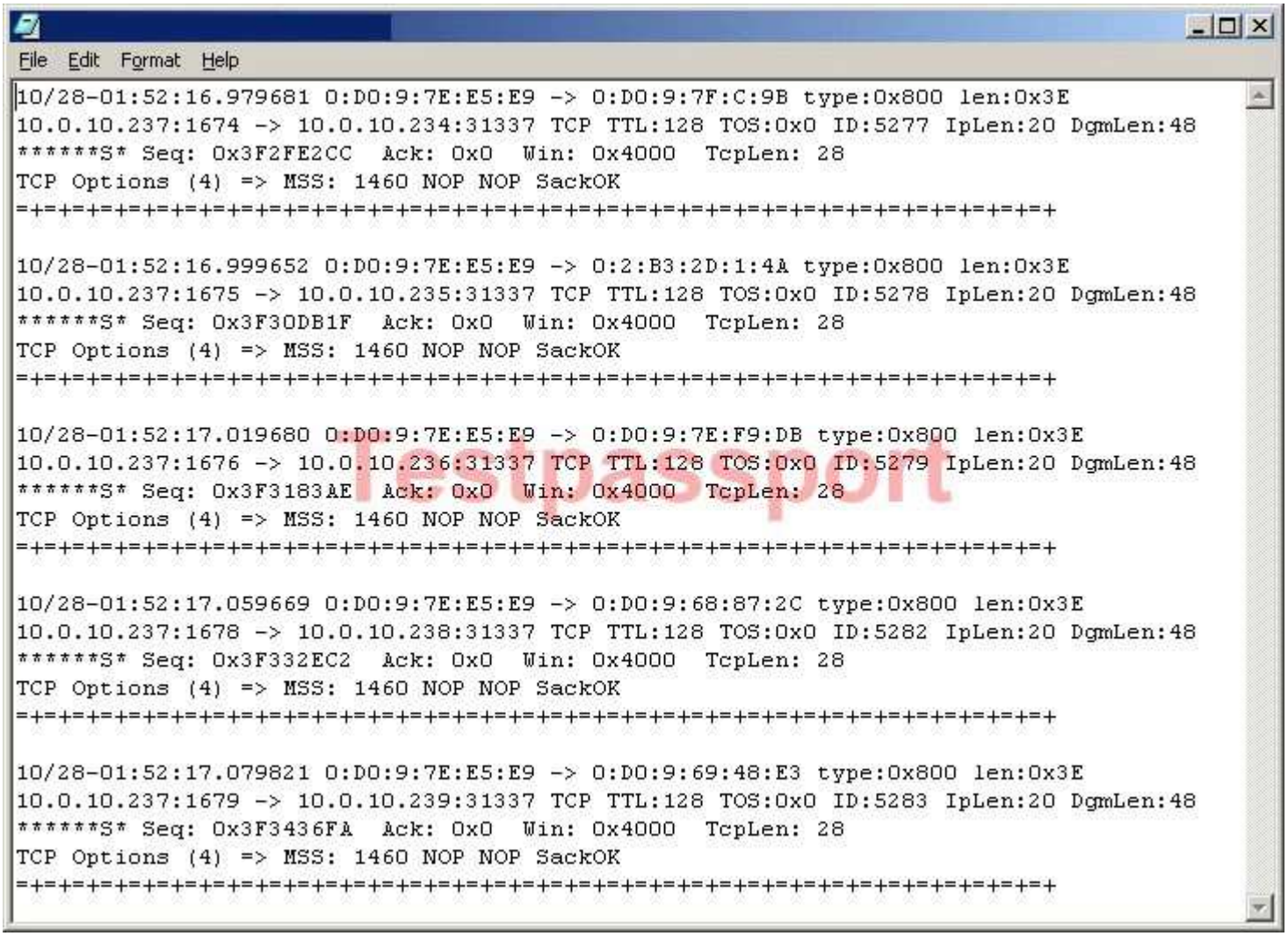
Explanation/Reference:

QUESTION 37
You are examining a packet from an unknown host that was trying to ping one of your protected servers and notice that the packets it sent had an IPLen of 20 byes and DgmLen set to 60 bytes. What type of operating system should you believe this packet came from?

A. Linux
B. SCO
C. Windows
D. Mac OSX
E. Netware

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
38 Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?



A. Trojan Horse Scan
B. Back Orifice Scan
C. NetBus Scan
D. Port Scan
E. Ping Sweep
Answer: B

QUESTION 38
Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

A. Linux Ping Response
B. Linux Ping Request
C. Windows 2000 Ping Request
D. Windows 2000 Ping Response
E. Windows NT 4.0 Ping Request

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

A. Nmap SYN/FIN Scan
B. Nmap ACK Scan
C. Nmap NULL Scan
D. Nmap XMAS Scan
E. Nmap SYN Scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

A. Nmap SYN/FIN Scan
B. Nmap NULL Scan
C. Nmap ACK Scan
D. Nmap SYN Scan
E. Nmap XMAS Scan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

A. Nmap XMAS Scan
B. Nmap NULL Scan
C. Nmap SYN Scan
D. Nmap ACK Scan
E. Nmap SYN/FIN Scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Recently you have had meetings with an organization to design their security policy. There has been some resistance on their board concerning the need for a security policy. To help remove the resistance, you describe the many benefits to having a security policy. Which of the following are the benefits of a security policy?

A. Help to prevent misuse of resources
B. Help to decrease the legal liability
C. Help to protect proprietary information
D. Help to lower bandwidth usage
E. Help protect data from unauthorized access

Correct Answer: ABCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
You are forming the security policy for your organization. You have identified those in the organization who will participate in the creation of the policy. Several of the people you have contacted wish to know what will be on the agenda during the first meeting.
During the very first policy design meeting, which of the following issues will you tell those in the policy committee to discuss?

A. Identification of the critical business resources
B. Identification of the infrastructure architecture
C. Determination of the type of policy to create
D. Identification of the critical business policies
E. Determination of the critical policies of key connected business partners

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
You are creating the User Account section of your organizational security policy. From the following options, select the questions to use for the formation of this section?

A. Are users allowed to make copies of any operating system files (including, but not limited to /etc/passwd or the SAM)?
B. Who in the organization has the right to approve the request for new user accounts?
C. Are users allowed to have multiple accounts on a computer?
D. Are users allowed to share their user account with coworkers?
E. Are users required to use password-protected screensavers?
F. Are users allowed to modify files they do not own, but have write abilities?

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
You have been given the task of writing your organizations 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

Correct Answer: AD

Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
From the following list, chose the primary reason for splitting a Security Policy into multiple smaller policies?

A. Smaller policies are cheaper to produce
B. Smaller policies are simpler to manage
C. Smaller policies are simpler to produce
D. Smaller policies are more legally binding
E. Smaller policies provide better security control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
You are creating the Remote Access section of your organizational security policy. From the following options, select the questions to use for the formation of this section?

A. What methods of remote access are allowed (cable modem, DSL, and so on)?
B. How are partner VPNs to be configured (to firewall or host)?
C. Which users are authorized to install networking devices into computers?
D. What is the process for becoming authorized for remote access?
E. Is the entire network accessible remotely?

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Recently at your organization you have been requested to lead the team in performing a new Risk Analysis of the organization. During the first team meeting you identify to your team the three areas of Risk Analysis. What are those three areas?

A. Verifying Risk, Minimizing Risk, Removing Risk
B. Qualifying Risk, Mitigating Risk, Removing Risk
C. Predicating Risk, Qualifying Risk, Minimizing Risk
D. Predicting Risk, Quantifying Risk, Mitigating Risk
E. Quantifying Risk, Mitigating Risk, Removing Risk

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Your organization assigns an Annual Loss Expectancy to assets during a risk analysis meeting. You have a server which if down for a day will lose the company $25,000, and has a serious root access attack against it once per month.
What is the ALE for this attack against this server?

A. $25,000
B. $300,000
C. $120,000
D. $2,083
E. $2,500

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which two of the following are factors that must be considered in determining the likelihood of occurrence during a risk analysis review?

A. What are the methods available to attack this asset?
B. What are the costs associated with protecting this asset?
C. Does the threat have sufficient capability to exercise the attack?
D. Does the threat have the motivation or incentive to exercise the attack?
E. Are any of the assets worthy of an attack?

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
After a security meeting, IT leaders decided that the organization will perform a completely new risk analysis, as the previous one was done over five years ago. The methods that will be used is FRAP. Which of the following best describes the FRAP method of risk analysis?

A. FRAP involves assigning team members to identify specific vulnerabilities. Once the vulnerabilities have been identified, a level of risk is assigned, as a factor of times per year this vulnerability may be exploited. Finally, a dollar value in lost revenue is assigned to each asset that can be compromised by this vulnerability.
B. FRAP is a team method. Individuals from different aspects of an organization form a committee. Once together, they discuss the areas of risk, the likelihood of a threat, the impact of the threat, and the methods that should be used to minimize the threat.
C. FRAP involves assigning dollar values to assets, and calculating how often a threat to the asset will occur. Once determined an approximate dollar value to each asset and threat combination is calculated.
D. FRAP is the process of determining the likelihood of a threat as medium, high, or low. Once the likelihood is determined the cost is identified, again as medium, high, or low. Finally, based on cost, a response to the threat is determined.
E. FRAP is the process of determining the likelihood of a threat as medium, high, or low. Once the likelihood is

determined, the level of damage is identified, again as high, medium, or low. Finally, the response to the threat is determined.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Your organization assigns an Annual Loss Expectancy to assets during a risk analysis meeting. You have a server which if down for a day will lose the company $35,000, and has a serious root access attack against it once per month.
What is the ALE for this attack against this server?

A. $35,000
B. $120,000
C. $2,916
D. $3,500
E. $420,000

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following best describes the Repair Model?

A. The model makes use of preventive measures and regular service as well as updates such as Service Packs, maintenance updates, and patches. Preventive measures can also improve the chances of the repair model working better than if the system had no preventive measures ever taken.
B. The repair model is the transference of risk to an insurance company that covers the costs of replacing the critical assets within your network. The drawbacks are increase in premiums after making a claim, high premiums anyway, down time while the insurance company is processing the claim, and claim may not pay what replacement costs are today.
C. Assets will typically cost much more than the original capital outlay that it took to purchase it long ago. Repair costs can be very high and a decision to exercise this model should not be made in haste. There are also depreciation issues to deal with as well. In any case, this model should be the last resort because of cost and may be the most time consuming.
D. The repair model makes use of the acknowledged skills and abilities of the existing personnel. Knowing that assets have very specific dollar values assigned to them, the choice on how to manage the asset is based on the experience of the personnel.
E. Before incurring the cost for repair of an inoperative asset, check for maintenance agreements that may include the cost of repair or the actual repair itself. Nevertheless, the repair model should focus on the restoration of the downed asset to its working status within the network infrastructure. Keep in mind that after hardware costs, costs for the reloading or replacement of software can be a large cost factor as well.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
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
F. b, d, c, e, a
G. a, b, d, c, e
H. d, b, c, a, e
I. a, b, c, d, e
J. d, b, a, c, e

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
You have just recently finished a complete Risk Analysis of your organization. During your presentation you present the controls you feel must be implemented.
Which is considered to be the major factor in determining a specific control system to implement?

A. Control system documentation
B. Return on investment
C. Current system availability
D. Familiarity with the system
E. Staffs previous use of system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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.

Correct Answer: E
Section: (none)

Explanation

Explanation/Reference:

QUESTION 57
To manage the risk analysis of your organization you must first identify the method of analysis to use. Which of the following organizations defines the current standards of risk analysis methodologies?

A. NIST
B. CERT
C. F-ICRC
D. NBS
E. NSA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
You are running a Linux machine as a dedicated file server for your network. You are trying to use Nmap to perform some security tests.
On your Linux machine, in order to run TCP SYN scans from a host using Nmap or NmapFE you must have which of the following?

A. telnet access
B. root privileges
C. access to tcpdump
D. login access to a router
E. login access to the target

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
One of your users calls to state the their computer is acting unusual. You go to investigate and find there is an unauthorized program installed on this computer. You examine the network and find that this program has replicated itself to other machines in the network, without the input of the user.
What type of program is in the network?

A. The program is a Worm.
B. The program is a Virus.
C. The program is a Bug.
D. The program is a Trojan Horse.
E. The program is a Macro.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 60
If an attacker uses a program that sends thousands of email messages to every user of the network, some of them with over 50MB attachments.
What are the possible consequences to the email server in the network?

A. Server hard disk can fill to capacity
B. Client hard disks can fill to capacity
C. Server can completely crash
D. Network bandwidth can be used up
E. Clients cannot receive new email messages

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Your network has been hit by a virus that is infecting the MBR on many of the systems in the network. You are working to repair the damage this virus has done. After two days of non-stop work on the problem, you get things under control.
What type of virus was in your network?

A. Macro Virus
B. Scripting Virus
C. Boot Sector Virus
D. Multi-part Virus
E. File Infection Virus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Your network has been hit by a very bad virus recently. As you tracked the virus through the network, it was changing from system, to system. Each time it went to infect a system; it had evolved slightly to have a different file size, or different file structure. After extensive work, you and your team were able to isolate and remove the virus from the network.
Which of the following best identifies the type of virus that was in your network?

A. Boot Sector Virus
B. Macro Virus
C. Stealth Virus
D. Multi-part Virus
E. Polymorphic Virus

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
You are running some tests in your network, to see if you can remotely identify the operating system of nodes in the network.
Using the nmap tool, which of the following commands will identify the operating system of the computer using IP address 192.168.10.1?

A. nmap -ident 192.168.10.1 -sS
B. nmap -sS 192.168.10.1 -O
C. nmap -Id 192.168.10.1 -sS
D. nmap -a -u -x -Id 192.168.10.1
E. nmap -Id 192.168.10.1 -aux -sS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
You are running Nessus in your organization to perform vulnerability assessments. If you wish to write your own plugin, to scan for a custom vulnerability, what will you use to write the plugin?

A. Nessus Plugin Scripting (NPS)
B. Nessus Custom Scripting (NCS)
C. Nessus C++ Scripting (NC+S)
D. Nessus Attack Scripting Language (NASL)
E. Nessus Java Scripting Language (NJSL)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
You have recently started using Nessus to perform vulnerability scans on the systems in your network. You now wish to perform further testing, to ensure that passwords are the proper length in the network. What feature of Nessus allows you to perform this type of custom scanning?

A. Nessus Plugins
B. Nessus cannot perform this type of scan, it is restricted to vulnerability scanning
C. Nessus Advanced Scripting
D. Nessus Password Scanning Module
E. Nessus Policies

Correct Answer: E

Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
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 -s 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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
You have just finished running vulnerability test, using Nessus, on a remote host in your network. You are reading the report Nessus generated, and are looking for those items you must address right away. In a Nessus report, how are items marked that require your immediate attention?

A. With a Yellow Exclamation Point
B. With a Red X
C. With a Black check
D. With a Yellow check
E. With a bulls-eye target

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
In order to run some tests on your system, you have decided to use the netcat utility. You want to be able to access the command prompt on a Windows system from your Linux system. What is the proper command on the Windows system to allow for you to gain remote access?

A. netcat -p 2020 -l cmd.exe
B. netcat -p 2020 -cmd.exe
C. nc -l -p 2020 -e cmd.exe
D. nc -p 2020 -l run/cmd.exe
E. netcat -p 2020 -l -run cmd.exe

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 69
In order to check on the passwords in your organization, you have been given the authority to run a password checking tool. You are going to use the tool LCP to check the passwords. What are the three main options available to you to configure LCP to attack and check passwords?

A. Reverse Attack
B. Dictionary Attack
C. Hybrid Attack
D. Brute Force Attack
E. Cryptographic Attack

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
To increase the security of your corporate website, you are running some basic checks on leaked information. You view the source code for a web page and see the following:
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252"> <meta name="GENERATOR" content="FrontPage 4.0">
<meta name="ProgId" content="Editor.Document">
<title>Security Certifications for the IT Pro</title>
<style type="text/css">
<!--
P, TD, LI, TH { font-size: 10pt; font-family: Arial, Verdana, Helvetica } .eight { font-size: 8pt }
-->
</style>
</head>
From this code, which of the following would an attacker most likely assume is the operating system that was used to create this web site?

A. OpenBSD
B. FreeBSD
C. Linux 5.0
D. Linux 6.0
E. Windows NT

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
In your network, you have built a single domain of only Windows computers. There are 55 XP machines and 10 Windows Server 2003 machines. You are concerned about the security of your SAM files on the Servers. Windows Server 2003 is the only Operating System on the computers, and the hard drives are all formatted with NTFS.
Which of the following are issues you must be sure to address when securing the SAM file?

A. You must be sure that no user while locally logged in to the Server can delete the SAM file.
B. You must be sure that no user while logged in to the Server remotely can delete the SAM file.
C. You must be sure that no user can boot to DOS and delete the SAM file from there.
D. You must be sure that no user can install a parallel Operating System and delete the SAM file from there.
E. You must be sure to encrypt the Operating System files using the built-in EFS, so that no user may delete the SAM file from anywhere.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
You are working with some new RPM files on your Linux system. You know there are several options when dealing with RPM files.
Which of the following answers lists proper RPM commands, with the correct description of the command?

A. rpm -q <package name> This command performs software verification.
B. rpm -e <package name> This command removes the software.
C. rpm -v <package name> This command performs software verification.
D. rpm -r <package name> This command removes the software.
E. rpm -i <package name> This command installs the software.
F. rpm -in <package name> This command installs the software.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
One of your users calls to state that their computer is acting unusual. You go to investigate and find there is an unauthorized program installed on this computer. You examine the network and find that this program is now on other machines in the network. It seems to be unable to move through the network on its own, and is getting sent as an email attachment.
What type of program is in the network?

A. The program is a Worm.
B. The program is a Virus.
C. The program is a Port scanner.
D. The program is a Trojan Horse.
E. The program is a Macro.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
In order to obtain public IP addresses, Internet Service Providers (ISPs) contact their upstream registry or their appropriate regional registry (an IANA subsidiary) at which of the following?

A. APNIC
B. ARIN
C. RIPE NCC
D. IETF
E. IESG

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
You have a series of new Windows Server 2003 systems, including 3 new web servers running IIS 6.0. You are concerned about the overall security of your servers, and are checking with Microsoft for any patches or updates that you might need to apply to your systems. Which of the following would you apply if you need to implement an update based on a critical Microsoft Security Bulletin?

A. Critical Update
B. Security Update
C. Feature Pack
D. Update Rollup
E. MSB Update

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
You have a series of new Windows Server 2003 systems, including 3 new web servers running IIS 6.0. You are concerned about the overall security of your servers, and are checking with Microsoft for any patches or updates that you might need to apply to your systems. Which of the following would you apply if you need to implement an update to fix a specific problem that addresses a critical, non-security-related bug?

A. Critical Update
B. Security Update
C. Feature Pack
D. Update Rollup
E. MSB Update

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
You have a series of new Windows Server 2003 systems, including 3 new web servers running IIS 6.0. You are concerned about the overall security of your servers, and are checking with Microsoft for any patches or updates that you might need to apply to your systems. Which of the following would you apply if you need to implement a single update, which contains a single cumulative package that includes multiple files that are used to address a problem in your IIS Servers?

A. Critical Update
B. Security Update
C. Feature Pack
D. Update Rollup
E. MSB Update

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
You have recently installed a new Linux machine, running Apache as your web server. You are running Novell SuSe Linux, and are going to use YaST to disable some unneeded modules. In the left-hand options of YaST, which section would you choose in order to disable modules for your Apache web server?

A. Network Services
B. Software
C. System
D. Software Management
E. Miscellaneous

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
You have recently installed an Apache Web server on a SuSe Linux machine. When you return from lunch, you find that a colleague has made a few configuration changes. One thing you notice is a .htpasswd file.
What is the function of this file?

A. It is a copy of the /etc/passwd file for Web access
B. It is a copy of the etc/shadow file for Web access
C. It is a listing of all anonymous users to the Web server
D. It is a listing of http users and passwords for authentication
E. It is a database file that can be pulled remotely via a web interface to identify currently logged in users.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Recently you found out that there has been a flood of bogus network traffic hitting your Email server. Because of this flood, authorized users have not been able to consistently send or receive email. What is happening to your Email server?

A. A Denial of Service Attack
B. A Virus Attack
C. A Worm Attack
D. A Macro Attack
E. A Trojan Attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
You are conducting a security awareness session for some of the employees in your organization. The discussion moves to the use if the web browser, which is Internet Explorer 7.0 for all employees. What are the four Zones that are available in Internet Explorer 7.0?

A. Internet
B. Local intranet
C. Trusted sites
D. Restricted sites
E. Unrestricted sites

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
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 are available 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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
You just installed a new SuSe Linux web server, running Apache, and are in the process of hardening the server. The server will perform basic web services, static web pages to internal clients only. Which of the following would you not perform to harden this system?

A. Disable server-side includes
B. Disable CGI execution
C. Disable httpd.conf
D. Disable directory browsing
E. Disable unnecessary modules

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
One of the major benefits to the design of the Internet is the redundancy that is built-in. To provide a measure of fault tolerance for DNS on the Internet, the designers of the Domain Name System distributed the root servers in various countries around the world. If an attacker were to attempt to disable DNS, they would have to gain administrative access on all the root servers. How many DNS servers would have to be compromised to have complete control of the Internet DNS?

A. 4
B. 8
C. 10
D. 12
E. 13

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following is the name of the Active X authentication system Microsoft has included to prevent Active X controls from being altered or corrupted by attackers wanting to perform unwarranted operations?

A. Driver Signing
B. Authenticode
C. Certificate services
D. NTLM
E. Kerberos

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
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 and other DNS attacks. If an attacker is able to take advantage of a BIND vulnerability to gain root access, this is which type of DNS Attack?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
In your organization, the majority of employees use Microsoft Outlook Express as their email client. You are configuring these systems so that applications on the employee systems cannot send email, posing as the user of the system.
Under the Security tab, which option will you select to achieve this goal?

A. Do not allow other applications to send mail as me.
B. Disable application mail delivery.
C. Prompt me prior to application mail delivery.
D. Warn me when other applications try to send mail as me.
E. Do not allow applications that could potentially transmit a virus to send mail as me.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
The Root-Level DNS servers have come under many attacks over the years. Due to attacks, such as the DDoS attack on the Root-Level DNS servers in October of 2002, which of the following systems was implemented to increase the security of the DNS servers for the Internet?

A. Multicasting
B. Unicasting
C. Anycasting
D. Broadcasting
E. X-Casting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
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"> <input type=hidden name="price" value="39.95">
<input type=hidden name="item_no" value="WIDGET9">
QUANTITY: <input type=text name="quantity" size=2 maxlength=2 value=1> </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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
You have been hired to work in the security division of a global Tier One ISP. You have been given a staff of 25 people all new to network security. You wish to bring them all up to speed on the components of the Internet and how they interact.
Which one of the following is not a major component of the Internet?

A. The Backbone
B. NAPs (Network Access Points)
C. ISPs (Internet Service Providers)
D. NICs (Network Information Centers)
E. DNS (Domain Name Service)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
You are discussing the design and infrastructure of the Internet with several colleagues when a disagreement begins over the actual function of the Tier System in the Internets design. What is the function of the Tier System in the physical structure of the Internet?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
After a year as a senior network administrator, you have been promoted to work in the security department of a large global Tier One ISP. You are to spend one month in training on security issues, concepts, and procedures. The third day in your new position, the ISP is hit with a DDoS attack from over 100,000 computers on the Internet. While the department works to manage the attack, you monitor the impact on the network. What is the impact to the ISP when hit with a DDoS such as this?

A. The attack compromises internal IP addresses of clients.
B. The attack denies legitimate users the ability to access legitimate resources.
C. The attack compromises internal email addresses of clients in the network.
D. The attack creates a loop of data, where requests for resources are routed to a different location.
E. The attack will cause (due to the large number of computers involved) the IDS to crash and no longer log network activity.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
During a routine security inspection of the clients in your network, you find a program called cgiscan.c on one of the computers. You investigate the file, reading part of the contents. Using the portion of the program shown below, identify the function of the program.
Temp[1] = "GET /cgi-bin/phf HTTP/1.0\n\n";
Temp[2] = "GET /cgi-bin/Count.cgi HTTP/1.0\n\n";
Temp[3] = "GET /cgi-bin/test-cgi HTTP/1.0\n\n";
Temp[4] = "GET /cgi-bin/php.cgi HTTP/1.0\n\n";
Temp[5] = "GET /cgi-bin/handler HTTP/1.0\n\n";
Temp[6] = "GET /cgi-bin/webgais HTTP/1.0\n\n";

Temp[7] = "GET /cgi-bin/websendmail HTTP/1.0\n\n";

A. The program is designed to launch the users email program.
B. The program is designed to manage the counters on a target web server.
C. The program is simply old temp files, and nothing of interest.
D. The program is designed to test the functionality of the cgi email scripts that are installed on the server.
E. The program is a vulnerability scanner

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
You are monitoring the DNS traffic on your network to see what kind of zone transfer data is currently being exchanged. You wish to monitor the incremental zone transfers. You run a packet capture to gather network traffic for this project.
Which kind of transfer traffic are you looking for?

A. HOST
B. MX
C. CNAME
D. IXFR
E. PTR

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
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. You have a few older machines that define the storage of Resource Records (RR) based on the TTL of name mapping information. If an attacker sends fake mapping information to the DNS Server, with a high TTL, which type of DNS Spoofing is this?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
When using the 3DES encryption (C = EK1[DK2[EK1[P]]]) , what is the function of P?

A. P is the text before encryption
B. P is the first encryption key
C. P is the second encryption key
D. P is the decryption key
E. P is the text after encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Public Key Cryptography systems use which two of the following keys?

A. Symmetric Key
B. Public Key
C. Hash Key
D. Asymmetric Key
E. Private Key

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
When a computer requires an input value to begin the cryptographic process, what is this value called?

A. F^1 Value
B. Entropic Value
C. RNG Value
D. PRNG Value
E. Seed Value

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103

Which of the following are asymmetric encryption algorithms?

A. MD5
B. RSA
C. Diffie-Hellman
D. 3DES
E. AES

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
If you wanted to use Public Key cryptography to encrypt data transmissions, which of the following ciphers could you use?

A. Triple-DES
B. DES
C. Blowfish
D. IDEA
E. RSA

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
If you had a cipher that used a unique key every time you encoded text, what would you be using?

A. A block cipher
B. A One-time pad
C. A stream cipher
D. An asymmetric cipher
E. A symmetric cipher

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
What can be used to remove any of the frequency and statistical relationship between unencrypted and encrypted text? (Choose two)

A. Exponentialism
B. Differentialism
C. Supposition

D. Confusion
E. Diffusion

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which of the following is a block cipher?

A. DES
B. 3DES
C. AES
D. RC4
E. GLOC

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
When using DH, what keys will Bob use to send an encrypted message to Alice?

A. Alices Public Key
B. Alices Private Key
C. The Session Key
D. Bobs Public Key
E. Bobs Private Key

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
What type of encryption converts data from a variable-length to a fixed length piece of data?

A. Asymmetric
B. Symmetric
C. Hash
D. IPSec
E. S/MIME

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Default DES implementations use a key length that is how long?

A. 1024 bits
B. 72 bits
C. 56 bits
D. 256 bits
E. 512 bits

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
When using the 3DES encryption (C = EK1[DK2[EK1[P]]]), what is the function of D?

A. D is the text before encryption
B. D is the first encryption key
C. D is the second encryption key
D. D is the decryption key
E. D is the text after encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Which of the following are hash algorithms?

A. MD5
B. SHA
C. RSA
D. 3DES
E. AES

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Which three of the following are examples of the reason that Message Authentication is needed?

A. Packet Loss

B. Content Modification
C. Masquerading
D. Public Key Registration
E. Sequence Modification

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

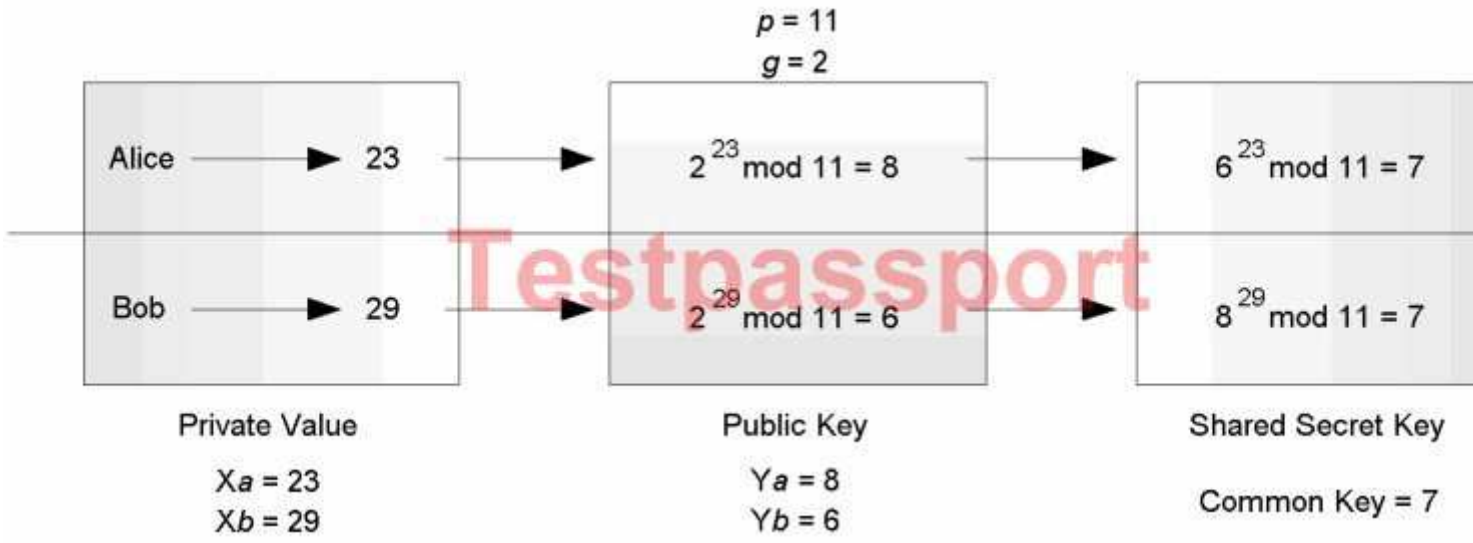
QUESTION 114
What type of cipher is used by an algorithm that encrypts data in chunks of data, 64 bits at a time?

A. 64-bit encryption Cipher
B. Block Cipher
C. Stream Cipher
D. Diffuse Cipher
E. Split Cipher

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
The image shows an example of what algorithm?



A. DES
B. Triple-DES
C. Blowfish
D. DH
E. IDEA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Which of the following types of attack is a vulnerability of DH?

A. Man-in-the-middle
B. IP Spoofing
C. IP Sequencing
D. Impersonation
E. Masquerading

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
When a cryptanalyst is using linguistic patterns to decrypt ciphertext, what is the analyst doing?

A. Analyzing the frequency of letters
B. Analyzing the degree of the letters
C. Analyzing the Caesar Shift
D. Analyzing the Transposition Cipher
E. Analyzing the Substitution Cipher

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
In the English language, what is the most frequently used letter?

A. A
B. E
C. T
D. R
E. S

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
When performing cryptanalysis, often the analyst will use linguistic patterns. What is a digram?

A. A two-letter word
B. Two letters that are next to each other in alphabetic order
C. A two-letter combination
D. Two letters whose letter place in the alphabet add up to an even value
E. A three-letter combination

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

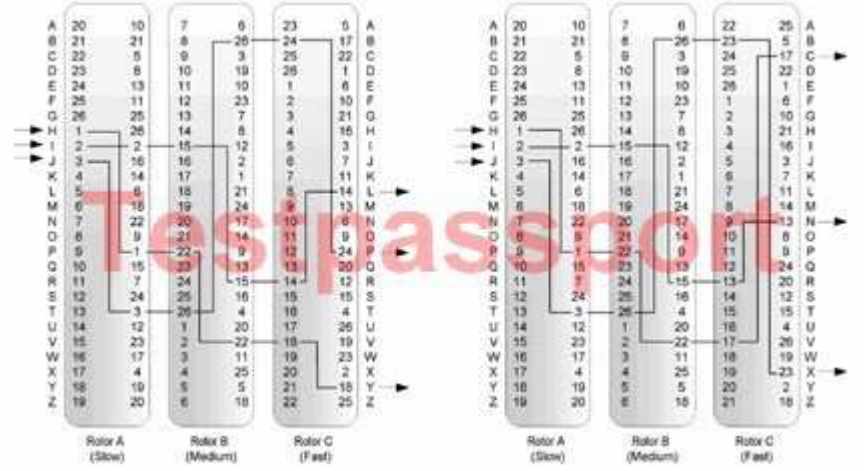
QUESTION 120
What are the four different modes of implementation of DES?

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

Correct Answer: BCDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
What type of cryptographic system is represented in this image?



A. Caesar
B. Vingre
C. Polybius

D. Purple
E. Enigma

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
Which of the following equation pairs show examples of an Inverse Function?

A. 20+3=23 and 23-3=20
B. 10*2=20 and 20/2=10
C. 20*2=40 and 40*0.5=20
D. 40/2=20 and 20/0.5=40
E. 30+10=40 and 40-10=30
F. 10*2=20 and 20*0.5=10

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

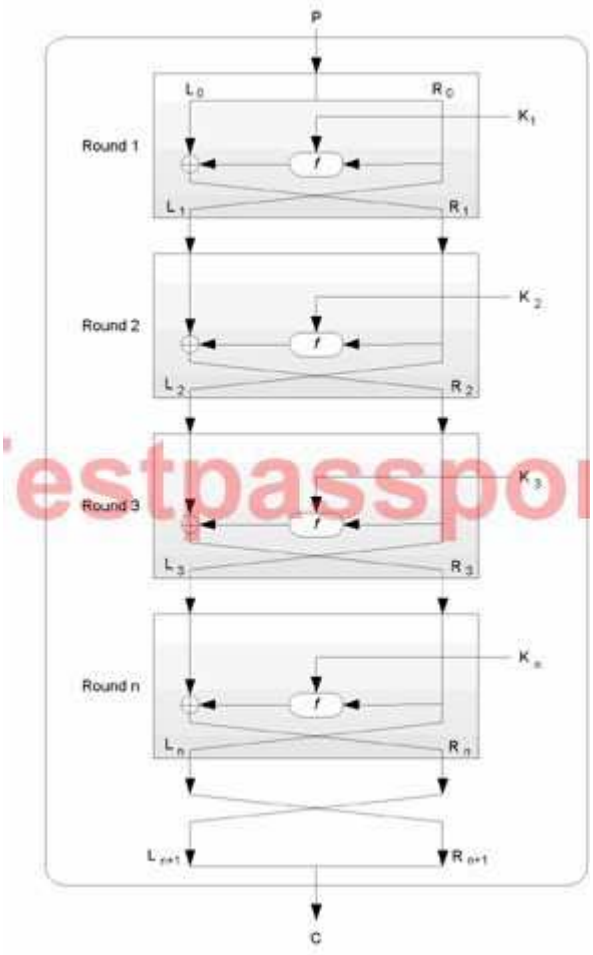
QUESTION 123
From the answers listed, select the one that does not represent a correct XOR (exclusive OR) operation:

A. 0 XOR 0 = 0
B. 0 XOR 1 = 1
C. 1 XOR 0 = 1
D. 1 XOR 1 = 0
E. 1 XOR 1 = 1

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
What classic cipher is shown in this image?



A. Feistel Cipher
B. Caesar Cipher
C. Vingre Cipher
D. Polybius Cipher
E. Enigma Cipher

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Which one of the following is an incorrect mod equation?

A. 9 mod 3 = 0
B. 40 mod 10 = 0
C. 40 mod 9 = 4
D. (6-1) mod 3 = 0
E. (2+4) mod 5 = 1

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Which of the following answers is the word SECURITY after having been encrypted using a Transposition Cipher?

A. S3CUR1+Y
B. TYSECURI
C. 57153497848
D. 5648135709
E. S1E2C3U4R5I6T7Y8

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
DES is often defined as no longer "secure enough" to handle high security requirements. Why is this?

A. DES is more vulnerable to dictionary attacks than other algorithms
B. DES is more vulnerable to brute-force attacks than other algorithms
C. DES uses a 32-bit key length, which can be cracked easily
D. DES uses a 64-bit key, which can be cracked easily
E. The DES key can be cracked in a short time

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
Which cryptographic process took advantage of a physical machine using rotors?

A. Rijndael
B. Feistel
C. Enigma
D. Vingre
E. Polybius

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
When using multiple alphabets, what type of cipher is being used?

A. Polyalphabetic Cipher
B. Multiple Cipher
C. Multialphabetic Cipher
D. Confusion Cipher
E. Diffusion Cipher

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
The computer you are currently using is running Linux, and you are logged into the system with your normal user account. An application you wish to run requires root access to execute. Which of the following can you do to have the application execute, and not have the security of the system lowered?

A. Log out as your user account, and log in as root
B. You cannot run an application as a user other than the one you are logged in as
C. Use the sw ID 0 command
D. Install the Switch User application, restart the computer, log in as root, then switch to your current user account and run the application
E. Use the su root command

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
You have decided to alter the default permissions of files on your SuSe Linux system. To do so, you are going to change the umask settings.
Where is the umask setting located?

A. /etc/profile
B. /etc/umask
C. /var/profile
D. /var/umask
E. /dev/null

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
Which of the following pieces of information are found in the Inode, on a Linux system?

A. Directory Location
B. File ownership information
C. File size in Bytes
D. Filename
E. File access time

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
You fear an unauthorized program has taken control of your CPU in your Linux system. What command will you run to see the CPU percentage per application in real-time?

A. top
B. netmon
C. ps
D. cpu_id
E. ps aux

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
You are setting the permissions on a new file in Linux.
What will be the level of permission given to the user if you assign an Octal value of 7?

A. rw-
B. r-x
C. ---

D. r--
E. rwx

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
You are setting the permissions on a new file in Linux.
What will be the level of permission given to the user if you assign an octal value of 6?

A. rwx
B. rw-
C. r--
D. r-x
E. ---

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
After installing a new application on your SuSe Linux server, you need to read through the log files. When you open the files, you notice they are very long, and you only wish to check the newest entries to the file.
What command do you use to perform this action?

A. currentlog
B. newest
C. /var/last
D. lastlog
E. trail

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
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 and Write for the Group: and Read for the Others.
What command will allow you to achieve this?

A. chmod 700 test_file.tar.gz
B. chmod 600 test_file.tar.gz
C. chmod 774 test_file.tar.gz
D. chmod 644 test_file.tar.gz
E. chmod 674 test_file.tar.gz

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
When a new user account is created in Linux, what values are assigned to the user account?

A. Shell_GID
B. SetGID
C. SetUID
D. UID
E. GID

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
As you configure your SuSe Linux computer, you make sure to modify TCP Wrappers as required by the security policy.
What are two benefits that TCP Wrappers provides you with in controlling the security of the system?

A. Connection Logging
B. Password Encryption
C. Network Encryption
D. Network Access Control
E. Secure Packet Encapsulation

Correct Answer: AD
Section: (none)

Explanation

Explanation/Reference:

QUESTION 142
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 and Write for the User; Read and Write for the Group: and Read for the others.
What command will allow you to achieve this?

A. chmod 660 test_file.tar.gz
B. chmod 760 test_file.tar.gz
C. chmod 604 test_file.tar.gz
D. chmod 704 test_file.tar.gz
E. chmod 664 test_file.tar.gz

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
The test.doc file on your Linux system that needs the ownership changed. You wish to have the new owner of the file to be vp_finance.
Which of the following is the command to change ownership to the vp_finance user account?

A. ch_own vp_finance test_doc
B. chown vp_finance test.doc
C. chown test/doc vp_finance
D. chown vp_finance test/doc
E. ch_own vp_finance test.doc

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
If you have enabled the Shadow Password file on your Linux system, what will be visible as the password for a user account in the /etc/passwd file?

A. An X for every character of the real password
B. An X for every character of the encrypted password
C. A single -
D. A single X
E. A single E

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
Which of the following fields are found in a user account's line in the /etc/passwd file?

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

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
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

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
When the first new user is created in Linux, what is the starting value for the assignment of a User Identifier?

A. 0
B. 1
C. 100
D. 500
E. 5000

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
You are configuring TCP Wrappers on your Linux system. What are the two configuration files that are used by TCP Wrappers to provide control?

A. /etc/hosts.allow
B. /etc/hosts.deny
C. /etc/tcpwrappers/inbound/conf.d
D. /etc/tcpwrappers/outbound/conf.d
E. /etc/hosts/allow
F. /etc/hosts/deny

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
After you have configured your new Linux file server, a colleague wishes to check the permission settings on some files.
You run the command to view the permissions, and the onscreen result is:
-rwx-rw-rw- 1 ps_admin root 2345 10:23 file1
Which of the following are true based on this output?

A. The owner has read, write, and execute permissions
B. The group has read, write, and execute permissions
C. The others have read, write, and execute permissions
D. ps_admin is the owner
E. root is the group

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
You are viewing the /etc/passwd file on your SuSe Linux computer, and you see the following entry:
root:23rs5:0:0:root:/root:/bin/bash
In this entry, what does the 23rs5 mean?

A. It is the code for the time when the root account was created
B. It is the group that the root account belongs to
C. It is the unencrypted password of the root account
D. It is the login name that the root account is to use
E. It is the encrypted password of the root account

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
While configuring TCP Wrappers on your Linux system, you desire to create a line that will effect every local computer's access to the ftp service.

Which of the following lines will achieve this desired result?

A. NETWORK(LOCAL): in.ftpd
B. in.ftpd: LOCAL
C. in.ftpd: NETWORK
D. in.ftpd: NETWORK(LOCAL)
E. LOCAL_NET: in.ftpd

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
While configuring TCP Wrappers on your Linux system, you desire to create a line that will effect the single host 10.20.23.45 accessing the telnet service.
Which of the following lines will achieve this desired result?

A. 10.20.23.45_HOST: in.telnetd
B. HOST(10.20.23.45): in.telnetd
C. in.telnetd: HOST_10.20.23.45
D. in.telnetd: ONLY_10.20.23.45/32
E. in.telnetd: 10.20.23.45

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
You are reviewing the lines used in the configuration of TCP Wrappers on your Linux system. When placed in the denial file, what is the function of the following line? in.telnetd: 192.168.23.: spawn (/bin/echo %c >> /var/log/telnet.log)

A. This line will initiate a Telnet connection to the 192.168.23.0/24 network.
B. This line will write a log line to the /bin/echo directory when a host tries to use Telnet to connect to the 192.168.23.0/24 network.
C. This line will initiate an ICMP echo request when a host from the 192.168.23.0/24 network uses Telnet.
D. This line will write a log line that contains client information when a host from the 192.168.23.0/24 network attempts to use Telnet.
E. This line will write a log line to the /var/log directory when a host tries to use Telnet to connect to the 192.168.23.0/24 network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154

To increase the security of your SuSe Linux system you have decided to implement control of the services running with Xinetd.
What is the name of the file that manages Xinetd?

A. /etc/system32/xinetd.d
B. /etc/xinetd.d
C. /etc/xinetd.conf
D. /xinetd/config.conf
E. /xinetd/conf.d

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
You are configuring the security of a service using Xinetd. You wish to add a line to the configuration of the service that grants access during the hours of 6AM to 7PM. Which of the following lines will you need to add to the configuration to achieve this result?

A. access_from = 6:00 - 19:00
B. access_times = 6AM:7PM
C. access_from = 6AM:7PM
D. access_times = 6:00<->19:00
E. access_times = 6:00 - 19:00

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
You are configuring the security of a service using Xinetd. You wish to add a line to the configuration of the service that limits the number of simultaneous connections to a service at 5, and defines the wait for new connections at 45 seconds.
Which of the following lines will you need to add to the configuration to achieve this result?

A. cps = 5 45
B. conn_5; time_45
C. conn=5; time=45
D. cps = 5:cps = 45
E. time=>45: conn=>5

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157

On your Linux computer you are examining the contents of various files to ensure they are secured and contain the designated information.
Entries in the /etc/hosts file consist of which of the following?

A. The IP address, the host-name and aliases (if any)
B. The IP address, subnet mask, the host-name (if any)
C. The IP address, subnet mask, the host-name and aliases (if any)
D. The IP address, subnet mask, default gateway and the host-name
E. The IP address, subnet mask, default gateway, the host-name and aliases (if any)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
You are using Samba on your SuSe Linux system to share files with a Windows network. What is the command to access the shared directory Finance on Windows machine Mktg_01 with user account User_01 from your Linux machine?

A. net use //Mktg_01/Finance -U User_01
B. net use -U User_01 //Mtkg_01/Finance
C. smbclient \Mtkg_01\Finance -U User_01
D. smbclient \\Mtkg_01\\Finance -U User_01
E. smbclient //Mktg_01/Finance -U User_01

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
You have just installed a new SuSe Linux machine, and you are working on managing the processes running

on the system.
What command will you need to issue in order to see the running processes, with the screen being updated every 10 seconds?

A. ps -aux -10
B. ps d 10 -aux
C. top d 10
D. ps d 10
E. top -aux -10

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
After installing a new SuSe Linux system, you wish to enhance the security of this computer. You type in the following commands (with actions in parenthesis):
grub (press Enter)
md5crypt
qwerty
(copy the result of this command)
quit
gedit /boot/grub/menu.1st &
password -md5 (Paste what you copied earlier)
(Save and close gedit)
What is the effect of following these commands and actions?

A. You have encrypted the grub menu with an MD5 hash.
B. You have added an MD5 hash of the word qwerty to the 1st time the grub menu is run.
C. You have added an MD5 password to the gedit process.
D. You have added an MD5 hash to the grub process.
E. You have added an MD5 hash of the word qwerty to the boot process.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
During a test of your SuSe Linux machine, you have noticed a specific process that is no longer working as desired.
What is the proper command to restart a process?

A. kill -restart <pid>
B. kill -HUP <pid>
C. kill <pid> -reset
D. kill <pid> -HUP
E. term-HUP <pid>

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 163
You are showing a colleague some of the commands available in Linux, and you type telinit 6 what is the result of typing this command?

A. This runs the telnet service with a priority level of 6.
B. This configures the system to use single-user mode.
C. This halts the system.
D. This restarts the system.
E. This interrupts the telnet service on socket 6.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
What of the following user accounts are given the correct default User Identifier and Group Identifier, assuming the system is running Red Hat Linux?

A. ftp: User Identifier 21, Group Identifier 21
B. root: User Identifier 0, Group Identifier 0
C. bin: User Identifier 1, Group Identifier 1
D. adm: User Identifier 3, Group Identifier 3
E. mail: User Identifier 25, Group Identifier 25

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
You wish to add a new user to your Linux system. The user account is called Lnx_1,the password is QW3RTY, and the group is Users.
What is the correct command to add this user account?

A. useradd -g Users Lnx_1
B. useradd Lnx_1 +grp Users
C. useradd Lnx_1 +g Users
D. adduser g/Users u/Lnx_1
E. adduser g/Users -act Lnx_1

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
You wish to add a new group to your Linux system. The group is called SCNP_Admins, and is to be given a Group Identifier of 1024.
What is the correct command to add this new group?

A. addgroup SCNP_Admins -id 1024
B. groupadd -g 1024 SCNP_Admins
C. addgroup SCNP_Admins id/1024
D. groupadd id/1024 g/SCNP_Admins
E. groupadd g/1024 SCNP_Admins

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
At the root@linuxbox$ prompt on a Linux machine you type ls -l b.doc and the output reads:
-rw-rw-r--1 simonusers31337Oct 5 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 the simon trojan
D. Nobody can read this file
E. Everyone can read this file

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
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 computers 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 in inetd.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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
In Windows Server 2003, there are four methods of implementing IPSec. They are:
1 - Require Security
2 - Request Security
3 - Respond Only
4 - No IPSec Policy
Your network hosts many servers, and different security policies are in place in different locations in the network.
The Clients and Servers in your network are configured as follows:
-You have servers numbered 1-9, which have a policy stating they require no network traffic security. -You have servers numbered 10-19, which have a policy stating they are not required to be secure, but will encrypt network traffic if the client is able to receive it. -You have servers numbered 20-29, which have a policy stating they are required to be secure and all network traffic they deliver must be secured.
-You have clients numbered 60-79 that are required to access secure servers 20-29. -You have clients numbered 80-99 that are not required to access secure servers 20-29, but are required to access servers 1-9 and 10-19.
Based on the Client and Server configuration provided above, which of the following computers will implement IPSec method 4?

A. Computers numbered 1-9
B. Computers numbered 10-19
C. Computers numbered 20-29
D. Computers numbered 60-79
E. Computers numbered 80-99

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
In your Windows 2003 Active Directory enabled network it has been decided that Dynamic DNS will be implemented. Once implemented this should help to minimize IP address to name mapping issues. One of your assistants wonders if using DDNS will present a single point of failure for the network. Which of the following is the reason that this is not the case?

A. Each client builds a DNS table that can be shared if need be.
B. Each client is configured with an Internet DNS server address in addition to the internal server.
C. All the Windows 2003 servers maintain a copy of the DDNS database.
D. All the Windows NT domain controllers maintain a copy of the DDNS database.
E. All the Windows 2003 domain controllers maintain a copy of the DDNS database.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
You are configuring a complex set of policies in your Windows 2003 Active Directory network. You have parent and child GPOs.
If you do not want the child GPO to inherit policy from the parent GPO, you would do which of the following?

A. Check the Block Policy Inheritance checkbox.
B. Uncheck the Disallow Inheritable Permissions to Traverse from Parent to Child Object box.
C. Uncheck the Reset Permissions on All Child Objects and Enable Propagation of Inheritable Permissions.
D. Check the Disallow Inheritable Permissions to Traverse from Parent to Child Object box.
E. You cannot block policy inheritance from parent to child GPOs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
You are in the process of securing several new machine on your Windows 2003 network. To help with the process Microsoft has defined a set of Security Templates to use in various situations. Which of the following best describes the Secure Security Templates (SECURE*.INF)?

A. This template is provided as a way to reverse the implementation of different Windows 2000 security settings, except for user rights.
B. This template is provided so that Local Users have ideal security settings, while Power Users have settings that are compatible with NT 4 Users.
C. This template is provided to implement suggested security settings for all security areas, except for the following: files, folders, and Registry keys.
D. This template is provided to create the maximum level of security for network traffic between Windows 2000 clients.
E. This template is provided to allow for an administrator to run legacy applications on a DC.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
You run an enterprise network for a large company. There are a few isolated branches in the company, which do not connect to the main network. You wish to increase the security of those branches by implementing NTLMv2.
Since, those branches are in areas of the world where United States Export Restrictions are not met, what mode will NTLMv2 be installed in?

A. 512-bit mode
B. 256-bit mode
C. 128-bit mode
D. 64-bit mode
E. 56-bit mode

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
You are working on the configuration of the authentication systems used in your network, and are considering several different authentication methods for your computer systems. What do LM, NTLM, and NTLMv2 use as their Authentication method?

A. Challenge/Response
B. Public Key Cryptography
C. Private Key Cryptography
D. Private Certificates
E. Public Certificates

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
You are creating a new Auditing and Logging policy for your network. On a Windows 2003 system, if you wish to audit events like access to a file, folder, or printer, which of the following options would you use?

A. Audit Account Logon Events
B. Audit Account Management
C. Audit Logon Events
D. Audit Object Access
E. Audit System Events

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
You are creating a new Auditing and Logging policy for your network. On a Windows 2003 system, if you wish to audit events like the computer restarting, which of the following options would you use?

A. Audit Account Logon Events
B. Audit Account Management
C. Audit Logon Events
D. Audit Object Access
E. Audit System Events

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
You are examining the Event IDs in your Windows 2003 network. There have been a large number of failed

attempts at logon in the network.
What is the Event ID for a failed attempt at Logon due to an unknown username or bad password?

A. 412
B. 529
C. 675
D. 749
E. 855

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
You have a Windows Server 2003 that you have been told must be reached by the Internet. Although you recommend against it, you are instructed to provide Telnet service to authorized users through this server. In order to increase security by restricting access to the Telnet server, you choose to restrict access to a single group of users.
Which of the following techniques will allow you to restrict Telnet access as you are required?

A. Creating a TelnetClients group and include within this group those users you wish to grant access to the Telnet server.
B. Configuring the properties of the Telnet Service to allow only a list of users to access the service.
C. Configuring the properties of the RPC Service (as Telnet Service is dependent on RPC) to allow only a group of users to access the service.
D. Configuring the properties of the RPC Locator Service (as Telnet Service is dependent on RPC) to allow only a group of users to access the service.
E. Creating a hardware profile and configuring the Telnet Service to start only when this hardware profile is chosen upon login.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
You are examining the Event IDs in your Windows 2003 network. There have been a large number of failed attempts at logon in the network.
What is the Event ID for a failed attempt at Logon due to an account being disabled?

A. 107
B. 230
C. 374
D. 413
E. 531

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
You are examining the Event IDs in your Windows 2003 network. There have been a large number of failed attempts at logon in the network.
What is the Event ID for a failed attempt at Logon due to an account having expired?

A. 231
B. 375
C. 414
D. 532
E. 676

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
You are examining the Authentication Logs on your Windows 2003 server. Specifically, you are looking for types of logon that were successful.
Which of the following correctly match the Logon Type with its numerical value?

A. Logon Type 0 - Interactive with Smart Card
B. Logon Type 1 - Network with Smart Card
C. Logon Type 2 - Interactive
D. Logon Type 3 - Network
E. Logon Type 7 - Unlock the Workstation

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
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. TCPAllowedConnections
D. TCPMaxHalfOpenRetried
E. TCPAllowedSessions

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
On your Windows 2003 system, you want to control inbound access to various ports.
What feature of Windows 2003 will allow you to do this?

A. Datagram Filtering
B. IPSec
C. EFS
D. TCP/IP Filtering
E. Session Management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
You are running a computer that boots to multiple operating systems on multiple partitions and wish to use Windows 2003 data encryption to protect your files. Which of the following options will Windows 2003's EFS perform?

A. Allows you to encrypt a file as well as the file name, so no one other than you or the recovery agent can see the existence of the file.
B. Allows you to encrypt a folder as well as the folder name, so no one other than you or the recovery agent can see the existence of the folder.
C. Allows you to encrypt a file only if the folder it is in allows encryption.
D. Allows you to encrypt a folder but not the folder name; however, the folder itself is not encrypted. Only the files within the folder are encrypted.
E. Allows you to encrypt a file but not the file name; users with access to the folder that the file is in are not prohibited from viewing the existence of a file.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
Logging is critical when you want to determine whether or not your server is being attacked. You must enable logging on your Web servers. To help prevent malicious users from deleting files to cover their tracks, you should make sure the ACLs on the IIS-generated log files (%systemroot%\system32\LogFiles) are set to Administrators (Full Control) and System (Full Control). The ACL for the Everyone group should not be greater than which of the following?

A. Full Control
B. Modify
C. Read & Execute
D. List Folder
E. Read

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
One of your assistants has configured a Windows 2003 Server to use EFS. This server is only accessed from internal network clients over a 100BaseT infrastructure. You tell your assistant that the security offered by EFS in this situation will not increase the security of the data transferred.
Why is your statement correct?

A. Each user would have to log in directly to the server to decrypt their files.
B. There is no way to securely share the key that the server will use to perform the encryption.
C. The files cannot be encrypted remotely by users at client computers.
D. The files will be decrypted remotely, and then sent to the clients in clear text.
E. The network cannot be configured to receive encrypted data without modifying the switches for such traffic.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
You have recently hired an assistant to help you with managing the security of your network. You are currently running an all Windows environment, and are describing NTFS permission issues. You are using some demonstration files to help with your discussion. You have two NTFS partitions, C:\ and D:\ There is a test file, C:\DIR1\test.txt that is currently set so that only Administrators have Full Control. If you move this file to the C:\DIR2 folder, what will the permissions be for this file?

A. The file will have the same permissions as D:\DIR2
B. The file permissions will remain the same
C. The file permissions will be lost
D. The file permissions will convert to Everyone - Full Control
E. The permissions will be set to whatever the CREATOR OWNER permissions are for the D:\ partition

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
You have just become the senior security professional in your office. After you have taken a complete inventory of the network and resources, you begin to work on planning for a successful security implementation in the network. You are aware of the many tools provided for securing Windows 2003 machines in your network.
What is the function of The Security Configuration and Analysis snap-in?

A. This tool is used to manage the NTFS security permissions on objects in the domain.
B. This tool is used to create an initial security database for the domain.
C. This tool is used to analyze a large number of computers in a domain-based infrastructure.
D. This tool provides an analysis of the local system security configuration.
E. This tool provides a single point of management where security options can be applied to a local computer or can be imported to a GPO.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
Windows 2003 Server can utilize many different forms of authentication, from standard passwords to Smart Cards.
What are the advantages of using NTLM Authentication over LM Authentication in Windows?

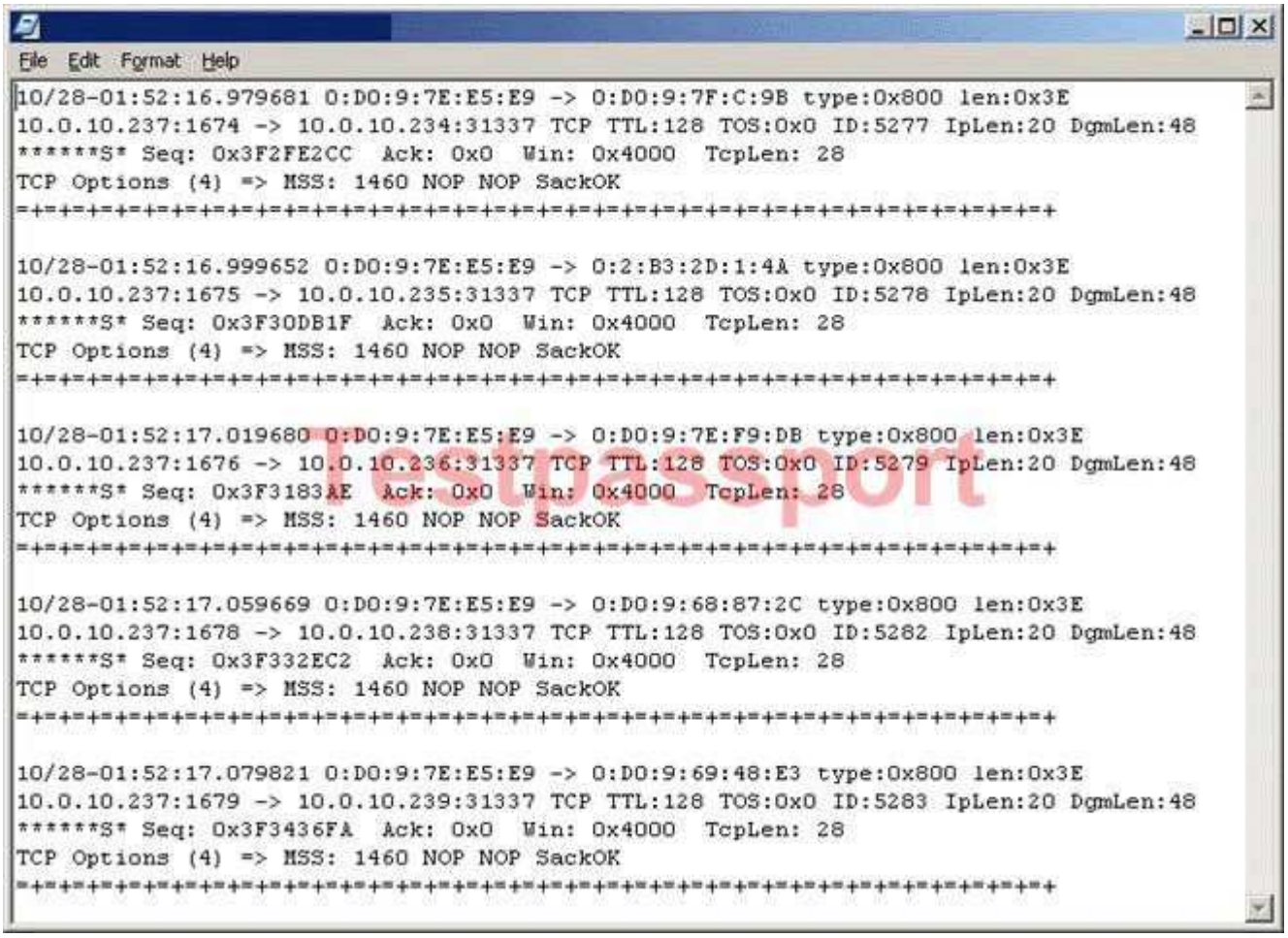
A. Creates 128-bit hash with MD4
B. Creates 64-bit hash with DES
C. Single string of 14 characters
D. Uses 16-bit Unicode characters
E. Uses standard character set

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
In Windows 2003, there are four methods of implementing IPSec. They are:
1 - Require Security
2 - Request Security
3 - Respond Only
4 - No IPSec Policy
Your network hosts many servers, and different security policies are in place in different locations in the network.
The Clients and Servers in your network are configured as follows:
-You have servers numbered 1-9, which have a policy stating they require no network traffic security. -You have servers numbered 10-19, which have a policy stating they are not required to be secure, but will encrypt network traffic if the client is able to receive it. -You have servers numbered 20-29, which have a policy stating

they are required to be secure and all network traffic they deliver must be secured.
-You have clients numbered 60-79 that are required to access secure servers 20-29. -You have clients numbered 80-99 that are not required to access secure servers 20-29, but are required to access servers 1-9 and 10-19.
Based on the Client and Server configuration provided above, which of the following computers must implement IPSec method 3?



A. Computers numbered 1-9
B. Computers numbered 10-19
C. Computers numbered 20-29
D. Computers numbered 60-79
E. Computers numbered 80-90

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
You are the main person responsible for the security of a mid-sized company. To have control over all the aspects of the security of the network, you study and analyze each component thoroughly. Your network is running all Windows 2003 servers, and you are studying the logon process. You know there are many components of the process, and are now at the point where you are analyzing the Security Accounts Manager

(SAM).
What is the SAM?

A. The SAM is a listing of users or group SIDS
B. The SAM is an authentication protocol used by Windows to authenticate clients
C. The SAM is used to check user permissions in order to access an object
D. The SAM is used to store user account information
E. The SAM is used to generate access tokens, and manages authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
You have recently introduced the users of your Windows 2003 Domain network to EFS, and the company policy indicates that several users must take advantage of EFS for certain files. Since it is new, you are concerned with EFS being implemented in ways not defined in the policy. Which user account is, by default, the Recovery Agent, that can decrypt data if need be?

A. The user who created the file
B. Domain Administrator
C. The user who encrypted the file
D. Any PowerUser
E. The Backup Operator

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
It has been decided that the network you manage will implement new Windows 2003 Servers, using Active Directory. You are configuring several of the Active Directory objects in your Windows 2003 network.
What is used as the default security for these objects?

A. Public Keys
B. EFS
C. NTFS
D. ACLs
E. Private Keys

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
You are going to use EFS to increase the security of the files and folders on your Windows Server 2003 systems in your network. You wish to have complete knowledge of the process of EFS, so that you may manage any situations or problems that may arise.
What is file data encrypted with when using EFS?

A. DES (Data Encryption Standard)
B. FEK (File Encryption Key)
C. DDF (Data Decryption Field)
D. DRF (Data Recovery Field)
E. RSA (Rivest Shamir Adelman)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
The security policy of your organization defines what data is to be locally encrypted and what is not to be. You are running Windows Server 2003, which allows for local encryption, and you have data that has been secured. Which of the following is the correct command for decrypting a subfolder named "March" under a folder named "Financials"?

A. decrypt Financials/March
B. cipher /d Financials/March
C. cipher /d Financials\March
D. decrypt Financials\March
E. cipher /d %sysroot%/Financials\March

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
You are making changes to your Windows Server 2003 file server, to increase security. You are aware from your auditing that attackers have been trying to map your network and perform reconnaissance. You wish to stop attackers from enumerating share names.
What can you do to stop this?

A. Disable the NULL Session under Local Policies, Security Options
B. Be sure that the ADMIN$ share has been removed
C. Be sure the %sysroot% is not accessible remotely
D. Disable the Traverse Folders option from the %sysroot% directory
E. Share Enumeration cannot be stopped. Enable Object Access logging to watch for this type of traffic pattern.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
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 and folders, 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. Change file permissions and take ownership of files

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

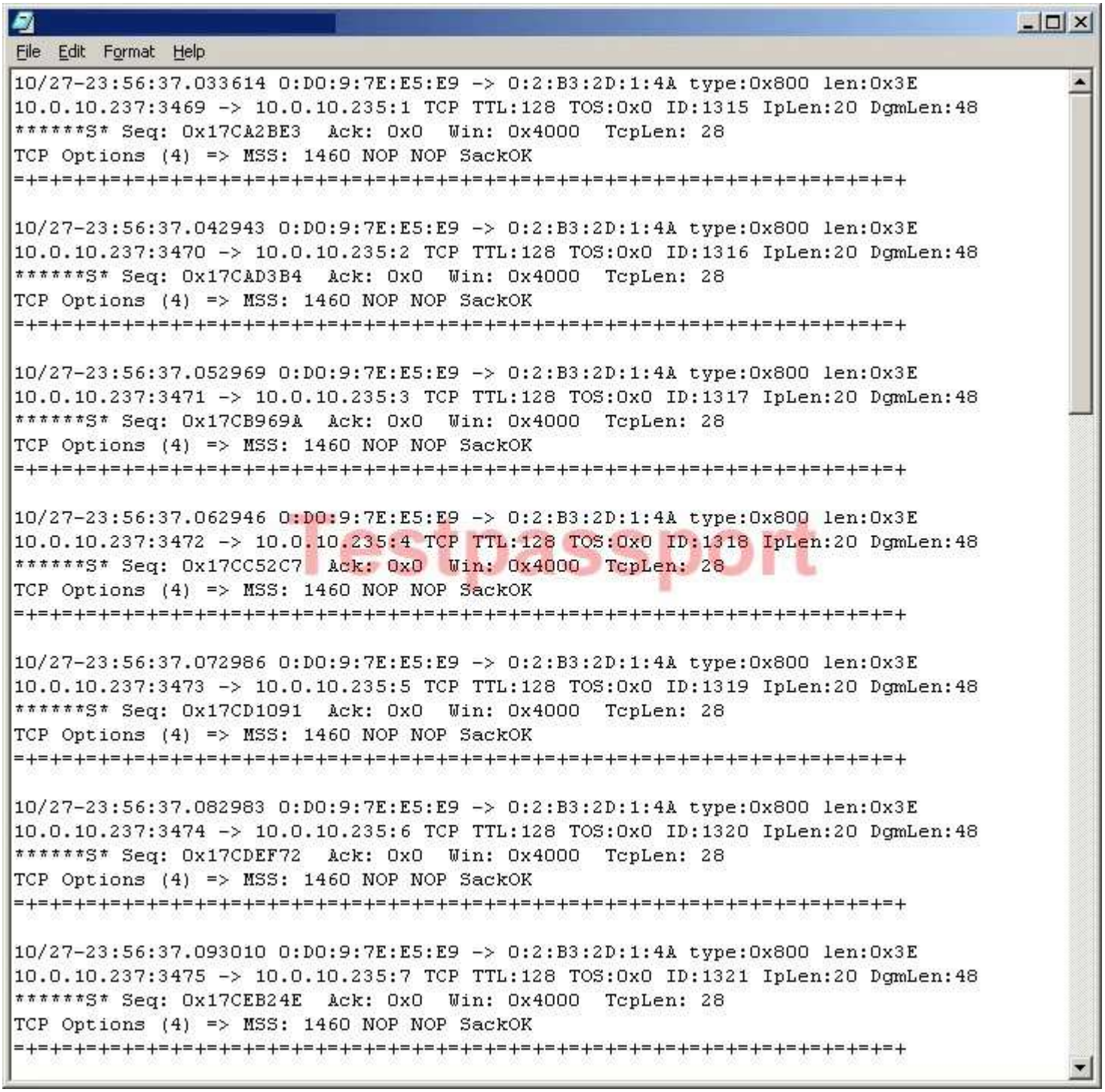
QUESTION 201
What encryption algorithm was selected to replace DES?

A. RC5
B. IDEA
C. AES
D. Blowfish
E. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?



A. NetBus Scan
B. Trojan Scan
C. Ping Sweep
D. Port Scan
E. Ping Sweep

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

A. Port Scan
B. Trojan Scan
C. Back Orifice Scan
D. NetBus Scan
E. Ping Sweep

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: