Full Backup - All data are backed up. The archive bit is cleared, which means that it is set to 0.
Differential Backup - Backup the files that have been modified since the last Full Backup. The archive bit does not change. Take more time while the backup phase is performed and take less time to restore.

Reference(s) used for this question:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

QUESTION 506
Which of the following backup methods makes a complete backup of every file on the server every time it is run?

A. full backup method.
B. incremental backup method.
C. differential backup method.
D. tape backup method.

Correct Answer: A
Explanation:
The Full Backup Method makes a complete backup of every file on the server every time it is run.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

QUESTION 507
A Business Continuity Plan should be tested:

A. Once a month.
B. At least twice a year.
C. At least once a year.
D. At least once every two years.

Correct Answer: C
Explanation:
It is recommended that testing does not exceed established frequency limits. For a plan to be effective, all components of the BCP should be tested at least once a year. Also, if there is a major change in the operations of the organization, the plan should be revised and tested not more than three months after the change becomes operational.
Source: BARNES, James C.& ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 165).

QUESTION 508
A weakness or lack of a safeguard, which may be exploited by a threat, causing harm to the information systems or networks is called a ?

A. Vulnerability
B. Risk
C. Threat
D. Overflow

Correct Answer: A
Explanation:

The Correct Answer: Vulnerability; Vulnerability is a weakness or lack of a safeguard, which may be exploited by a threat, causing harm to the information systems or networks.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

QUESTION 509
Which of the following is NOT a part of a risk analysis?

A. Identify risks
B. Quantify the impact of potential threats
C. Provide an economic balance between the impact of the risk and the cost of the associated countermeasure
D. Choose the best countermeasure

Correct Answer: D
Explanation:
This step is not a part of RISK ANALYSIS. A risk analysis has three main goals: identify risks, quantify the impact of potential threats, and provide an economic balance between the impact of the risk and the cost of the associated countermeasure. Choosing the best countermeasure is not part of the risk analysis.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 3: Security Management Practices (page 73). HARRIS, Shon, Mike Meyers' CISSP(R) Certification Passport, 2002, McGraw-Hill, page 12.

QUESTION 510
In the course of responding to and handling an incident, you work on determining the root cause of the incident. In which step are you in?

A. Recovery
B. Containment
C. Triage
D. Analysis and tracking

Correct Answer: D
Explanation:
In this step, your main objective is to examine and analyze what has occurred and focus on determining the root cause of the incident.
Recovery is incorrect as recovery is about resuming operations or bringing affected systems back into production
Containment is incorrect as containment is about reducing the potential impact of an incident.
Triage is incorrect as triage is about determining the seriousness of the incident and filtering out false positives

Reference:
Official Guide to the CISSP CBK, pages 700-704

QUESTION 511
Prior to a live disaster test also called a Full Interruption test, which of the following is most important?

A. Restore all files in preparation for the test.
B. Document expected findings.

C. Arrange physical security for the test site.
D. Conduct of a successful Parallel Test

Correct Answer: D
Explanation:
A live disaster test or Full interruption test is an actual simulation of the Disaster Recovery Plan. All operations are shut down and brought back online at the alternate site. This test poses the biggest threat to an organization and should not be performed until a successful Parallell Test has been conducted.

1. A Checklist test would be conducted where each of the key players will get a copy of the plan and they read it to make sure it has been properly developed for the specific needs of their departments.

2. A Structure Walk Through would be conducted next. This is when all key players meet together in a room and they walk through the test together to identify shortcoming and dependencies between department.

3. A simulation test would be next. In this case you go through a disaster scenario up to the point where you would move to the alternate site. You do not move to the alternate site and you learn from your mistakes and you improve the plan. It is the right time to find shortcomings.

4. A Parallell Test would be done. You go through a disaster scenario. You move to the alternate site and you process from both sites simultaneously.

5. A full interruption test would be conducted. You move to the alternate site and you resume processing at the alternate site.

The following answers are incorrect:

Restore all files in preparation for the test. Is incorrect because you would restore the files at the alternate site as part of the test not in preparation for the test.

Document expected findings. Is incorrect because it is not the best answer. Documenting the expected findings won't help if you have not performed tests prior to a Full interruption test or live disaster test.

Arrange physical security for the test site. Is incorrect because it is not the best answer. why physical security for the test site is important if you have not performed a successful structured walk-through prior to performing a Full interruption test or live disaster test you might have some unexpected and disasterous results.

QUESTION 512
Which of the following is an example of an active attack?

A. Traffic analysis
B. Scanning
C. Eavesdropping
D. Wiretapping

Correct Answer: B
Explanation:
Scanning is definitively a very active attack. The attacker will make use of a scanner to perform the attack, the scanner will send a very large quantity of packets to the target in order to illicit

responses that allows the attacker to find information about the operating system, vulnerabilities, misconfiguration and more. The packets being sent are sometimes attempting to identify if a known vulnerability exist on the remote hosts.

A passive attack is usually done in the footprinting phase of an attack. While doing your passive reconnaissance you never send a single packet to the destination target. You gather information from public databases such as the DNS servers, public information through search engines, financial information from finance web sites, and technical infomation from mailing list archive or job posting for example.

An attack can be active or passive.
An "active attack" attempts to alter system resources or affect their operation.

A "passive attack" attempts to learn or make use of information from the system but does not affect system resources. (E.g., see: wiretapping.)

The following are all incorrect answers because they are all passive attacks:

Traffic Analysis - Is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security.

Eavesdropping - Eavesdropping is another security risk posed to networks. Because of the way some networks are built, anything that gets sent out is broadcast to everyone. Under normal circumstances, only the computer that the data was meant for will process that information. However, hackers can set up programs on their computers called "sniffers" that capture all data being broadcast over the network. By carefully examining the data, hackers can often reconstruct real data that was never meant for them. Some of the most damaging things that get sniffed include passwords and credit card information.

In the cryptographic context, Eavesdropping and sniffing data as it passes over a network are considered passive attacks because the attacker is not affecting the protocol, algorithm, key, message, or any parts of the encryption system. Passive attacks are hard to detect, so in most cases methods are put in place to try to prevent them rather than to detect and stop them. Altering messages, modifying system files, and masquerading as another individual are acts that are considered active attacks because the attacker is actually doing something instead of sitting back and gathering data. Passive attacks are usually used to gain information prior to carrying out an active attack."

Wiretapping - Wiretapping refers to listening in on electronic communications on telephones, computers, and other devices. Many governments use it as a law enforcement tool, and it is also used in fields like corporate espionage to gain access to privileged information. Depending on where in the world one is, wiretapping may be tightly controlled with laws that are designed to protect privacy rights, or it may be a widely accepted practice with little or no protections for citizens. Several advocacy organizations have been established to help civilians understand these laws in their areas, and to fight illegal wiretapping.

Reference(s) used for this question:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 6th Edition, Cryptography, Page 865
http://en.wikipedia.org/wiki/Attack_%28computing%29
http://www.wisegeek.com/what-is-wiretapping.htm

https://pangea.stanford.edu/computing/resources/network/security/risks.php
http://en.wikipedia.org/wiki/Traffic_analysis

QUESTION 513
Which of the following would BEST be defined as an absence or weakness of safeguard that could be exploited?

A. A threat
B. A vulnerability
C. A risk
D. An exposure

Correct Answer: B
Explanation:
It is a software , hardware or procedural weakness that may provide an attacker the open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment. A vulnerability characterizes the absence or weakness of a safeguard that could be exploited. This vulnerability may be a service running on a server, unpatched applications or operating system software etc.

The following answers are incorrect because:
Threat: A threat is defined as a potential danger to information or systems. The threat is someone or something will identify a specific vulnerability and use it against the company or individual. The entity that takes advantage of a vulnerability is referred to as a 'Threat Agent'. A threat agent could be an intruder accessing the network through a port on the firewall , a process accessing data that violates the security policy.
Risk: A risk is the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact. If a firewall has several ports open , there is a higher likelihood that an intruder will use one to access the network in an unauthorized method.

Exposure: An exposure is an instance of being exposed to losses from a threat agent.

References:
SHON HARRIS, ALL IN ONE THIRD EDITION: Chapter 3 : Security Management Practices, Pages: 57-59

QUESTION 514
Which of the following statements pertaining to disk mirroring is incorrect?

A. Mirroring offers better performance in read operations but writing hinders system performance.
B. Mirroring is a hardware-based solution only.
C. Mirroring offers a higher fault tolerance than parity.
D. Mirroring is usually the less cost-effective solution.

Correct Answer: B
Explanation:
With mirroring, the system writes the data simultaneously to separate drives or arrays.
The advantage of mirroring are minimal downtime, simple data recovery, and increased performance in reading from the disk.
The disadvantage of mirroring is that both drives or disk arrays are processing in the writing to disks function, which can hinder system performance.
Mirroring has a high fault tolerance and can be implemented either through a hardware RAID controller or through the operating system. Since it requires twice the disk space than actual data,