QUESTION 943
Which of the following could an attacker use to overwrite instruction pointers in order to execute malicious code?

A. Memory leak
B. SQL injection
C. Resource exhaustion
D. Buffer overflow

Answer: D

QUESTION 944
An administrator is beginning an authorized penetration test of a corporate network. Which of the following tools would BEST assist in identifying potential attacks?

A. Netstat
B. Honeypot
C. Company directory
D. Nmap

Answer: D

QUESTION 945
A security administrator is implementing a SIEM and needs to ensure events can be compared against each other based on when the events occurred and were collected. Which of the following does the administrator need to implement to ensure this can be accomplished?

A. TOTP
B. TKIP
C. NTP
D. HOTP

Answer: B

QUESTION 946
A company is deploying NAFDs in its office to improve employee productivity when dealing with paperwork. Which of the following concerns is MOST likely to be raised as a possible security issue in relation to these devices?

A. Sensitive scanned materials being saved on the local hard drive
B. Faulty printer drivers causing PC performance degradation

C. Improperly configured NIC settings interfering with network security
D. Excessive disk space consumption due to storing large documents

Answer: D

QUESTION 947
Which of the following BEST describes how a MITM attack differs from a spear phishing attack?

A. A MITM attack uses spyware to log user activity, while a spear phishing attack installs a rootkit on the client to forge the identity of the user.
B. A MITM attack compromises routers in an effort to intercept passwords. while a spear phishing attack targets end-user devices.
C. A MITM attack requires root or administrator permission. while a spear phishing attack may use accounts with less powerful permissions.
D. A MITM attack intercepts credentials, while a spear phishing attack might attempt to get the user to provide those credentials directly.

Answer: A

QUESTION 948
During a risk assessment, results show that a fire in one of the company's datacenters could cost up to $20 million in equipment damages and lost revenue. As a result. the company insures the datacenter for up to S20 million in damages for the cost of $30.000 a year. Which of the following risk response techniques has the company chosen?

A. Transference
B. Avoidance
C. Mitigation
D. Acceptance

Answer: A

QUESTION 949
Which of the following concepts ensure ACL rules on a directory are functioning as expected? (Select TWO).

A. Accounting
B. Authentication
C. Auditing
D. Authorization
E. Non-repudiation

Answer: AC

QUESTION 950
Staff members from a call center frequently use a conference room for meetings in the secured SOC. While walking through the soc, the start members can view sensitive materials displayed for monitoring purposes. The call center staff was emailed the PIN needed to open the SOC door by human resources. Which of the following access controls would prevent this situation from occurring? (Select TWO).

A. Change the entry system to one that uses proximity cards assigned to individual security staff members.
B. Create a security awareness program that educates all staff members on the risks involved with sharing the PIN for the SOC!
C. Install screen filters on all devices within the SOC and position monitors so they are not facing shared walkways.
D. Implement time-of-day restrictions that prevent access to the SOC using the shared PIN after

hours.

E. Install CCTV monitors and a visitor log to control who is entering the SOC

Answer: AC

QUESTION 951
Given the information below:
MD5 HASH document.doc 049eab40 fd36caad1fab10b3cdf4a883
MD5 HASH image. jpg 049eab40fd36caad1fab0b3cdf4a883
Which of the following concepts are described above? (Select TWO)

A. Salting
B. Collision
C. Steganography
D. Hashing
E. Key stretching

Answer: BD

QUESTION 952
Some call center representatives' workstations were recently updated by a contractor, who was able to collect customer information from the call center workstations. Which of the following types of malware was installed on the call center users' systems?

A. Adware
B. Logic bomb
C. Trojan
D. Spyware

Answer: C

QUESTION 953
During the incident handling process, an analyst ran the following command:

```
PS c:\>get-filehash c:\windows\system32\cmd.exe
SHA1 cmd.exe cda52a0faca4ac7df32cfb6c8fa09acf42ad5cb7
```

The original file hash for cmd.exe was:
ab5d7c8faca 4ac7d32cfb6c8fa09acf42ad5f12
Which of the following is MOST associated with this indicator of compromise?

A. Virus
B. Rootkit
C. Backdoor
D. Keylogger

Answer: A

QUESTION 954
A service provider recently upgraded one of the storage clusters that houses non-confidential data for clients. The storage provider wants the hard drives back in working condition. Which of the following is the BEST method for sanitizing the data given the circumstances?

A. Hashing
B. Wiping

C. Purging
D. Degaussing

Answer: B

QUESTION 955
Which of the following attacks is used to capture the WPA2 handshake?

A. Replay
B. IV
C. Evil twin
D. Disassociation

Answer: A