# Free Questions for CFR-210 by ebraindumps

## Shared by Heath on 20-10-2022

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

Which of the following technologies is used as mitigation to XSS attacks?

## Options:

**A-** Intrusion prevention

**B-** Proxy filtering

**C-** Web application firewall

**D-** Intrusion detection

## Answer:

C

# Question 2

**Question Type:** MultipleChoice

A logfile generated from a Windows server was moved to a Linux system for further analysis. A system administrator is now making edits to the file with vi and notices the file contains numerous instances of Ctrl-M (^M) characters. Which of the following command line tools is the administrator MOST likely to use to remove these characters from the logfile? (Choose two.)

### Options:

**A-** tr

**B-** cut

**C-** cat

**D-** unix2dos

**E-** awk

### Answer:

A, C

## Question 3

**Question Type:** **MultipleChoice**

While reviewing some audit logs, an analyst has identified consistent modification of the sshd_config file for an organization's server. The analyst would like to investigate and compare contents of the current file with archived versions of files that are saved weekly. Which of the following tools will be MOST effective during the investigation?

### Options:

**A-** cat <beginning of filename>* | cut --d ',' --f 2,5,7

**B-** more <beginning of filename>* | grep <string of characters>

**C-** diff <filename> <filename 2>

**D-** sort <beginning of filename>*

### Answer:

B

# Question 4

**Question Type:** **MultipleChoice**

Which of the following logs should be checked to determine if an internal user connected to a potentially malicious website? (Choose two.)

### Options:

**A-** FTP logs

**B-** Email logs

**C-** Firewall logs

**D-** Proxy logs

**E-** HTTP logs

### Answer:

D, E

## Question 5

**Question Type:** **MultipleChoice**

During an investigation on Windows 10 system, a system administrator needs to analyze Windows event logs related to CD/DVD-burning activities. In which of the following paths will the system administrator find these logs?

### Options:

**A-** \Windows\Systems32\winevt\logs\System.evt

**B-** \Windows\System32\winevt\Logs\System.evtx

**C-** \Windows\Systems\winevt\Evtlogs\System.evtx

**D-** \Windows\System\winevt\Logs\System.evt

### Answer:

B

## Question 6

**Question Type:** MultipleChoice

The incident response team needs to track which user last connected to a specific Windows domain controller. Which of the following is the BEST way to identify that specific user?

### Options:

**A-** Check Systems Event Log on the user's computer

**B-** Check Systems Event Log on the domain controller

**C-** Check Security Log on the user's computer

**D-** Check SecurityLog on the domain controller

### Answer:

D

# Question 7

**Question Type:** **MultipleChoice**

An organization performs regular updates to its network devices to alert and prevent access to streaming media sites by the employees. Each device will send logs and alerts to a centralized server for storage, archive, and analysis. Which of the following BEST describes the system that is correlating the data found in all alerts and logs?

### Options:

**A-** SIEM

**B-** NIDS

**C-** HIPS

**D-** WIPS

## Answer:

A