

- A. MAC Flooding
- B. DNS poisoning
- C. MAC cloning
- D. ARP poisoning

**Correct Answer:** A

**QUESTION 203**

An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?

- A. TLS
- B. PFS
- C. ESP
- D. AH

**Correct Answer:** A

**QUESTION 204**

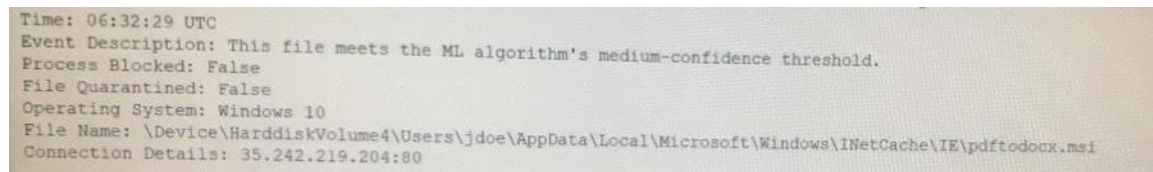
Which of the following types of controls is a CCTV camera that is not being monitored?

- A. Detective
- B. Deterrent
- C. Physical
- D. Preventive

**Correct Answer:** B

**QUESTION 205**

An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:



```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows\INetCache\IE\pdfdocx.msi
Connection Details: 35.242.219.204:80
```

Which of the following is the MOST likely cause of the issue?

- A. The end user purchased and installed a PUP from a web browser
- B. A bot on the computer is brute forcing passwords against a website
- C. A hacker is attempting to exfiltrate sensitive data
- D. Ransomware is communicating with a command-and-control server.

**Correct Answer:** A

**QUESTION 206**

A nuclear plant was the victim of a recent attack, and all the networks were air gapped. A subsequent investigation revealed a worm as the source of the issue. Which of the following BEST explains what happened?

- A. A malicious USB was introduced by an unsuspecting employee.
- B. The ICS firmware was outdated
- C. A local machine has a RAT installed.
- D. The HVAC was connected to the maintenance vendor.

**Correct Answer: A**

**QUESTION 207**

A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial opinion article in a national newspaper, which may result in new cyberattacks. Which of the following would be BEST for the security manager to use in a threat mode?

- A. Hacktivists
- B. White-hat hackers
- C. Script kiddies
- D. Insider threats

**Correct Answer: A**

**Explanation:**

Hacktivists - "a person who gains unauthorized access to computer files or networks in order to further social or political ends."

**QUESTION 208**

A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat against the organization's network. Which of the following will the analyst MOST likely use to accomplish the objective?

- A. A table exercise
- B. NST CSF
- C. MTRE ATT\$CK
- D. OWASP

**Correct Answer: C**

**QUESTION 209**

A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an item, the password for the wireless network is printed on the receipt so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?

- A. WPA-EAP
- B. WEP-TKIP
- C. WPA-PSK

D. WPS-PIN

**Correct Answer: A**

**QUESTION 210**

Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

- A. The data protection officer
- B. The data processor
- C. The data owner
- D. The data controller

**Correct Answer: C**

**QUESTION 211**

A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen. Which of the following would BEST meet these requirements? (Select TWO).

- A. Full-device encryption
- B. Network usage rules
- C. Geofencing
- D. Containerization
- E. Application whitelisting
- F. Remote control

**Correct Answer: AB**

**QUESTION 212**

Given the following logs:

```
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "password"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "access"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "allow"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "please"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "ftp"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "letmein"
[21][ftp] host: 192.168.50.1 login:admin password:letmein
1 of 1 target successfully completed, 1 valid password found
```

Which of the following BEST describes the type of attack that is occurring?

- A. Rainbow table
- B. Dictionary
- C. Password spraying
- D. Pass-the-hash

**Correct Answer: C**

**QUESTION 213**

An organization routes all of its traffic through a VPN. Most users are remote and connect into a corporate datacenter that houses confidential information. There is a firewall at the Internet border.

## [Download Full Version JK0-022 Exam Dumps\(Updated in Feb/2023\)](#)

followed by a DLP appliance, the VPN server and the datacenter itself. Which of the following is the WEAKEST design element?

- A. The DLP appliance should be integrated into a NGFW.
- B. Split-tunnel connections can negatively impact the DLP appliance's performance
- C. Encrypted VPN traffic will not be inspected when entering or leaving the network
- D. Adding two hops in the VPN tunnel may slow down remote connections

**Correct Answer: C**

### **QUESTION 214**

A security analyst is running a vulnerability scan to check for missing patches during a suspected security incident. During which of the following phases of the response process is this activity MOST likely occurring?

- A. Containment
- B. Identification
- C. Recovery
- D. Preparation

**Correct Answer: B**

### **QUESTION 215**

A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office. Priority must be given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?

- A. Nmap
- B. Heat maps
- C. Network diagrams
- D. Wireshark

**Correct Answer: B**

#### **Explanation:**

Engineer needs to create a plan for upgrading the wireless infrastructure in a large office. Priority must be given to areas that are currently.

Site surveys and heat maps provide the following benefits: Identify trouble areas to help eliminate slow speeds and poor performance

### **QUESTION 216**

A symmetric encryption algorithm is BEST suited for:

- A. key-exchange scalability.
- B. protecting large amounts of data.
- C. providing hashing capabilities,
- D. implementing non-repudiation.

**Correct Answer: D**

[JK0-022 Exam Dumps](#) [JK0-022 PDF Dumps](#) [JK0-022 VCE Dumps](#) [JK0-022 Q&As](#)

<https://www.ensurepass.com/JK0-022.html>

**QUESTION 217**

A university is opening a facility in a location where there is an elevated risk of theft. The university wants to protect the desktops in its classrooms and labs. Which of the following should the university use to BEST protect these assets deployed in the facility?

- A. Visitor logs
- B. Cable locks
- C. Guards
- D. Disk encryption
- E. Motion detection

**Correct Answer: B**

**QUESTION 218**

An organization blocks user access to command-line interpreters but hackers still managed to invoke the interpreters using native administrative tools. Which of the following should the security team do to prevent this from happening in the future?

- A. Implement HIPS to block inbound and outbound SMB ports 139 and 445.
- B. Trigger a SIEM alert whenever the native OS tools are executed by the user.
- C. Disable the built-in OS utilities as long as they are not needed for functionality.
- D. Configure the AV to quarantine the native OS tools whenever they are executed.

**Correct Answer: C**

**QUESTION 219**

Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

- A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.
- B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.
- C. Malware trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox.
- D. Routing tables have been compromised, and an attacker is rerouting traffic to malicious websites.

**Correct Answer: D**

**QUESTION 220**

Which of the following organizational policies are MOST likely to detect fraud that is being conducted by existing employees? (Select TWO).

- A. Offboarding
- B. Mandatory vacation
- C. Job rotation
- D. Background checks
- E. Separation of duties
- F. Acceptable use

**Correct Answer: BC**