

- A. COPE
- B. VDI
- C. GPS
- D. TOTP
- E. RFID
- F. BYOD

Correct Answer: BE

QUESTION 132

Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

- A. Unsecure protocols
- B. Use of penetration-testing utilities
- C. Weak passwords
- D. Included third-party libraries
- E. Vendors/supply chain
- F. Outdated anti-malware software

Correct Answer: DE

QUESTION 133

Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

- A. DNSSEC and DMARC
- B. DNS query logging
- C. Exact mail exchanger records in the DNS
- D. The addition of DNS conditional forwarders

Correct Answer: C

QUESTION 134

A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

- A. SDP
- B. AAA
- C. IaaS
- D. MSSP
- E. Microservices

Correct Answer: D

QUESTION 135

A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

- A. CVE
- B. SIEM
- C. SOAR

D. CVSS

Correct Answer: D

Explanation:

The Common Vulnerability Scoring System (CVSS) is a system widely used in vulnerability management programs. CVSS indicates the severity of an information security vulnerability, and is an integral component of many vulnerability scanning tools.

QUESTION 136

An organization just experienced a major cyberattack modem. The attack was well coordinated sophisticated and highly skilled. Which of the following targeted the organization?

- A. Shadow IT
- B. An insider threat
- C. A hacktivist
- D. An advanced persistent threat

Correct Answer: D

Explanation:

<https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/>
https://csrc.nist.gov/glossary/term/advanced_persistent_threat

QUESTION 137

A security analyst needs to be proactive in understand the types of attacks that could potentially target the company's execute. Which of the following intelligence sources should to security analyst review?

- A. Vulnerability feeds
- B. Trusted automated exchange of indicator information
- C. Structured threat information expression
- D. Industry information-sharing and collaboration groups

Correct Answer: D

QUESTION 138

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

- A. Nmap
- B. Wireshark
- C. Autopsy
- D. DNSEnum

Correct Answer: A

Explanation:

<https://nmap.org/book/man-version-detection.html>

NMAP scans running services and can tell you what services are running

QUESTION 139

A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator

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

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

configure?

- A. A captive portal
- B. PSK
- C. 802.1X
- D. WPS

Correct Answer: C

QUESTION 140

A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

- A. DDoS attack
- B. Memory leak
- C. Buffer overflow
- D. Resource exhaustion

Correct Answer: D

QUESTION 141

Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and It has continues to evade detection. Which of the following should administrator implement to protect the environment from this malware?

- A. Install a definition-based antivirus.
- B. Implement an IDS/IPS
- C. Implement a heuristic behavior-detection solution.
- D. Implement CASB to protect the network shares.

Correct Answer: C

Explanation:

Heuristic analysis is also one of the few methods capable of combating polymorphic viruses -- the term for malicious code that constantly changes and adapts. Heuristic analysis is incorporated into advanced security solutions offered by companies like Kaspersky Labs to detect new threats before they cause harm, without the need for a specific signature.

<https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis>

QUESTION 142

Which of the following will provide the BEST physical security countermeasures to stop intruders? (Select TWO.)

- A. Alarms
- B. Signage

- C. Lighting
- D. Mantraps
- E. Fencing
- F. Sensors

Correct Answer: DE

QUESTION 143

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis, However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern? (Select TWO.)

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens
- E. Geotagging
- F. Role-based access controls

Correct Answer: AE

QUESTION 144

Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

- A. Integer overflow
- B. Zero-day
- C. End of life
- D. Race condition

Correct Answer: B

QUESTION 145

A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control. Which of the following BEST describes this process?

- A. Continuous delivery
- B. Continuous integration
- C. Continuous validation
- D. Continuous monitoring

Correct Answer: B

QUESTION 146

A user contacts the help desk to report the following:

- Two days ago, a pop-up browser window prompted the user for a name and password after

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

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

connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.

- The user was able to access the Internet but had trouble accessing the department share until the next day.
- The user is now getting notifications from the bank about unauthorized transactions.

Which of the following attack vectors was MOST likely used in this scenario?

- A. Rogue access point
- B. Evil twin
- C. DNS poisoning
- D. ARP poisoning

Correct Answer: A

QUESTION 147

In which of the following common use cases would steganography be employed?

- A. Obfuscation
- B. Integrity
- C. Non-repudiation
- D. Blockchain

Correct Answer: A

QUESTION 148

After a ransomware attack a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. Which of the following will the company MOST likely review to trace this transaction?

- A. The public ledger
- B. The NetFlow data
- C. A checksum
- D. The event log

Correct Answer: A

QUESTION 149

When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

- A. Tokenization
- B. Data masking
- C. Normalization
- D. Obfuscation

Correct Answer: C

QUESTION 150

A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use. Which of the following would add another factor of authentication?