


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



Server

Hostname: ws01  
Domain: comptia.org  
IPv4: 10.1.9.50  
IPv4: 10.2.10.50  
Root: home.aspx  
DNS CNAME: homesite

### Extensions

commonName	policyIdentifier
extendedKeyUsage	subjAltName

### Values

ws01.comptia.org
DNS Name=*.comptia.org
serverAuth
clientAuth
DNS Name=homesite.comptia.org
OCSP:URI:http://ocsp.pki.comptia.org
URL=http://homesite.comptia.org/home.aspx

### Certificate Signing Request

Extension	Value
commonName	ws01.comptia.org
extendedKeyUsage	OCSP:URI:http://ocsp.pki.comptia.org
policyIdentifier	URL=http://homesite.comptia.org/home.aspx
subjAltName	DNS Name=*.comptia.org



### QUESTION 326

An application owner reports suspicious activity on an internal financial application from various internal users within the past 14 days. A security analyst notices the following:

- Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.
- Internal users in question were changing their passwords frequently during that time period.
- A jump box that several domain administrator users use to connect to remote devices was recently compromised.
- The authentication method used in the environment is NTLM.

Which of the following types of attacks is MOST likely being used to gain unauthorized access?

- A. Pass-the-hash
- B. Brute-force
- C. Directory traversal
- D. Replay

**Correct Answer: A**

### QUESTION 327

An attacker was easily able to log in to a company's security camera by performing a basic online search for a setup guide for that particular camera brand and model. Which of the following BEST

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

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

describes the configurations the attacker exploited?

- A. Weak encryption
- B. Unsecure protocols
- C. Default settings
- D. Open permissions

**Correct Answer: C**

**QUESTION 328**

An organization recently recovered from a data breach. During the root cause analysis, the organization determined the source of the breach to be a personal cell phone that had been reported lost. Which of the following solutions should the organization implement to reduce the likelihood of future data breaches?

- A. MDM
- B. MAM
- C. VDI
- D. DLP

**Correct Answer: C**

**QUESTION 329**

An organization wants to implement a biometric system with the highest likelihood that an unauthorized user will be denied access. Which of the following should the organization use to compare biometric solutions?

- A. FRR
- B. Difficulty of use
- C. Cost
- D. FAR
- E. CER

**Correct Answer: A**

**QUESTION 330**

A financial analyst has been accused of violating the company's AUP and there is forensic evidence to substantiate the allegation. Which of the following would dispute the analyst's claim of innocence?

- A. Legal hold
- B. Order of volatility
- C. Non-repudiation
- D. Chain of custody

**Correct Answer: D**

**QUESTION 331**

A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?

- A. Evil twin
- B. Jamming
- C. DNS poisoning
- D. Bluesnarfing
- E. DDoS

**Correct Answer:** E

**QUESTION 332**

An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan the analyst identifies that a server has some insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Select THREE)

- A. SFTP FTPS
- B. SNMPv2 SNMPv3
- C. HTTP, HTTPS
- D. TFTP FTP
- E. SNMPv1, SNMPv2
- F. Telnet SSH
- G. TLS, SSL
- H. POP, IMAP
- I. Login, rlogin

**Correct Answer:** BCF

**QUESTION 333**

The security team received a report of copyright infringement from the IP space of live corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted file. The analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again. Which of the following is MOST capable of accomplishing both tasks?

- A. HIDS
- B. Allow list
- C. TPM
- D. NGFW

**Correct Answer:** D

**QUESTION 334**

A security analyst generated a file named host1.pcap and shared it with a team member who is going to use it for further incident analysis. Which of the following tools will the other team member MOST likely use to open this file?

- A. Autopsy
- B. Memdump
- C. FTK imager
- D. Wireshark

**Correct Answer:** D

**Explanation:**

Some common applications that can open .pcap files are Wireshark, WinDump, tcpdump, Packet Square - Capedit and Ethereal.

**QUESTION 335**

Which of the following is the MOST relevant security check to be performed before embedding third-party libraries in developed code?

- A. Check to see if the third party has resources to create dedicated development and staging environments.
- B. Verify the number of companies that downloaded the third-party code and the number of contributions on the code repository.
- C. Assess existing vulnerabilities affecting the third-party code and the remediation efficiency of the libraries' developers.
- D. Read multiple penetration-testing reports for environments running software that reused the library.

**Correct Answer:** D

**QUESTION 336**

As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

- A. TAXII
- B. TLP
- C. TTP
- D. STIX

**Correct Answer:** C

**Explanation:**

TTPs Within Cyber Threat Intelligence:

- Tactics, techniques and procedures (TTPs) are the "patterns of activities or methods associated with a specific threat actor or group of threat actors."
- Analysis of TTPs aids in counterintelligence and security operations by describing how threat actors perform attacks.
- Top threats facing an organization should be given priority for TTP maturation. Smaller organizations may benefit strategically by outsourcing research and response.

One acronym everyone working on a cybersecurity team should be familiar with is TTPs - tactics, techniques and procedures - but not everyone understands how to use them properly within a cyber threat intelligence solution. TTPs describe how threat actors (the bad guys) orchestrate, execute and manage their operations attacks. ("Tactics" is also sometimes called "tools" in the acronym.) Specifically, TTPs are defined as the "patterns of activities or methods associated with a specific threat actor or group of threat actors," according to the Definitive Guide to Cyber Threat Intelligence.

**QUESTION 337**

Which of the following holds staff accountable while escorting unauthorized personnel?

- A. Locks
- B. Badges
- C. Cameras
- D. Visitor logs

**Correct Answer: B**

**QUESTION 338**

A security analyst wants to fingerprint a web server. Which of the following tools will the security analyst MOST likely use to accomplish this task?

- A. nmap -p1-65535 192.168.0.10
- B. dig 192.168.0.10
- C. curl --head http://192.168.0.10
- D. ping 192.168.0.10

**Correct Answer: C**

**Explanation:**

curl - Identify remote web server

Type the command as follows:\$

```
curl -I http://www.remote-server.com/
```

```
$
```

```
curl -I http://vivekgite.com/
```

Output:

```
HTTP/1.1 200 OK
```

```
Content-type: text/html
```

```
Content-Length: 0
```

```
Date: Mon, 28 Jan 2008 08:53:54 GMT
```

```
Server: lighttpd
```

**QUESTION 339**

A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

- A. IP restrictions
- B. Multifactor authentication
- C. A banned password list