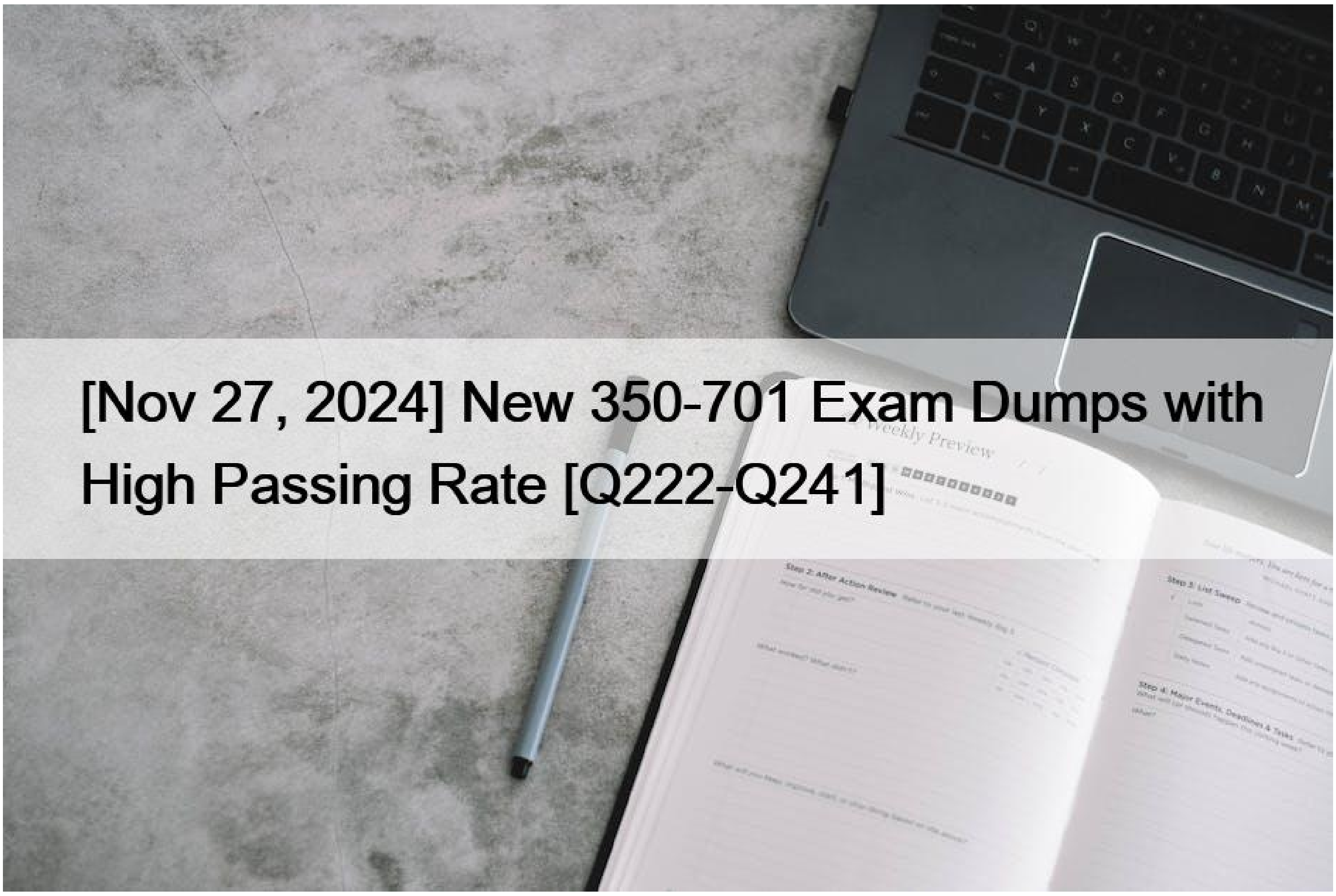
[Nov 27, 2024 New 350-701 Exam Dumps with High Passing Rate [Q222-Q241



[Nov 27, 2024] New 350-701 Exam Dumps with High Passing Rate
Get 350-701 Braindumps & 350-701 Real Exam Questions

Conclusion

With a Cisco certification, you are better equipped for instant success in the modern IT environments. And with the new CCNP Security designation, you are well-prepared to take on more complex security roles at the professional level. All it takes is passing the Cisco 350-701 exam. Develop the right mindset, review the exam topics, and explore all the study materials to guarantee your career growth today.

Cisco 350-701 certification exam is a valuable credential for IT professionals who want to demonstrate their skills and knowledge in implementing and operating Cisco Security Core Technologies. Implementing and Operating Cisco Security Core Technologies certification exam covers various topics related to network security and is suitable for network engineers, administrators, and security analysts. Implementing and Operating Cisco Security Core Technologies certification is recognized globally and requires extensive study and hands-on experience in network security technologies. With the certification, IT professionals are equipped to secure their organization's networks and protect against threats and attacks.

Cisco 350-701 (Implementing and Operating Cisco Security Core Technologies) Exam is designed for network security professionals who are responsible for implementing and operating core security technologies for their organization. 350-701 exam focuses on the latest security technologies and solutions that are necessary to implement a comprehensive security strategy. 350-701 exam validates the knowledge and skills of the candidates in areas such as network security, cloud security, content security, endpoint protection and detection, secure network access, visibility, and enforcement.

QUESTION 222

Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?
* It allows the endpoint to authenticate with 802.1x or MAB.
* It verifies that the endpoint has the latest Microsoft security patches installed.
* It adds endpoints to identity groups dynamically.
* It allows CoA to be applied if the endpoint status is compliant.

Posture is a service in Cisco ISE that checks the compliance of endpoints with corporate security policies before allowing them to connect to the network. Posture policies define the requirements that endpoints must meet to be compliant, such as having antivirus software installed and updated, or having a specific registry key value. If an endpoint is compliant, Cisco ISE can apply a Change of Authorization (CoA) to grant it access to the network resources. CoA is a mechanism that allows Cisco ISE to dynamically change the authorization attributes of an existing session, such as VLAN, dACL, or SGT, without requiring the user to reauthenticate.

CoA can be triggered by various events, such as posture assessment results, profiling changes, or manual actions by the administrator. CoA can also be used to quarantine or disconnect non-compliant endpoints.

Therefore, ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE provides the benefit of allowing CoA to be applied if the endpoint status is compliant. References :=

* Cisco Identity Services Engine Administrator Guide, Release 2.2 &#8211; Configure Client Posture Policies

* Cisco Identity Services Engine Administrator Guide, Release 2.2 &#8211; Change of Authorization

QUESTION 223

What is a benefit of using Cisco FMC over Cisco ASDM?
* Cisco FMC uses Java while Cisco ASDM uses HTML5.
* Cisco FMC provides centralized management while Cisco ASDM does not.
* Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.
* Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices

https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html

QUESTION 224

What is the purpose of the Cisco Endpoint IoC feature?
* It is an incident response tool.
* It provides stealth threat prevention.
* It is a signature-based engine.
* It provides precompromise detection.

The Cisco Endpoint IoC feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers. Endpoint IoCs are imported through the console from OpenIOC-based files written to trigger on file properties such as name, size, hash, and other attributes and system properties such as process information, running services, and Windows Registry entries. The IoC syntax can be used by incident responders to find specific artifacts or use logic to create sophisticated, correlated detections for families of malware. Endpoint IoCs have the advantage of being portable to share within your organization or in industry vertical forums and mailing lists. The Endpoint IoC scanner is available in AMP for Endpoints Windows Connector versions 4 and higher. Running Endpoint IoC scans may require up to 1 GB of free drive space. The Endpoint IoC feature is based on the openioc.com framework, which is an open standard for sharing threat intelligence. References:

* Cisco Endpoint IOC Attributes, User Guide

* What Are Indicators of Compromise (IOC)? &#8211; Cisco, Security Indicators of Compromise

* General questions about AMP &#8211; Cisco Community, Post by Cisco Employee Reference: https://docs.amp.cisco.com/Cisco%20Endpoint%20IOC%20Attributes.pdf The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers.

QUESTION 225

Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?
* RADIUS-based REAP
* fingerprinting
* Dynamic ARP Inspection
* multifactor authentication

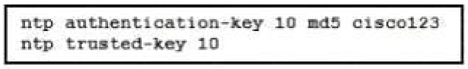
QUESTION 226

Which Cisco ISE feature helps to detect missing patches and helps with remediation?
* posture assessment
* profiling policy
* authentication policy
* enabling probes

Posture assessment is a feature of Cisco ISE that allows you to check the compliance of endpoints with corporate security policies before allowing them to access the network1. Posture assessment can detect missing patches on endpoints and help with remediation by applying the appropriate posture policy and requirement2. Posture assessment can also check for the presence and status of security software, such as antivirus, antispyware, firewall, and so on3. Posture assessment is one of the core security technologies covered in the Implementing and Operating Cisco Security Core Technologies (SCOR) course4, which prepares you for the Cisco CCNP Security and CCIE Security certifications and for senior-level security roles. References: 1: Posture Service 2: Configure Posture Policies 3: Posture Conditions 4: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

QUESTION 227

Refer to the exhibit.



```
ntp authentication-key 10 md5 cisco123
ntp trusted-key 10
```

A network engineer is testing NTP authentication and realizes that any device synchronizes time with this router and that NTP authentication is not enforced What is the cause of this issue?
* The key was configured in plain text.

* NTP authentication is not enabled.
* The hashing algorithm that was used was MD5. which is unsupported.
* The router was not rebooted after the NTP configuration updated.

QUESTION 228

Which API method and required attribute are used to add a device into Cisco DNA Center with the native API?
* GET and serialNumber
* userSudiSerlalNos and deviceInfo
* POST and name
* lastSyncTime and pid

QUESTION 229

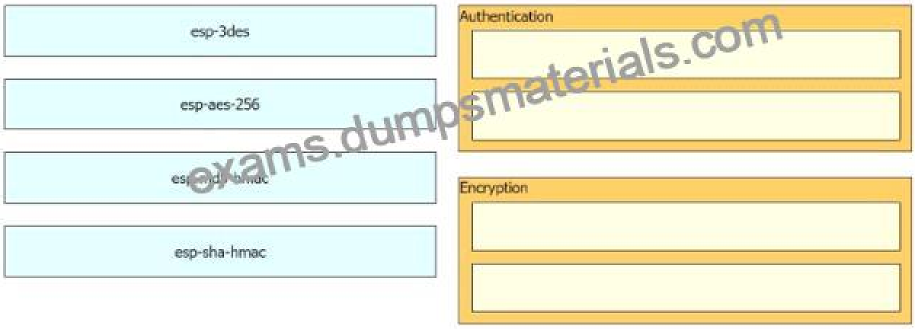
Which exfiltration method does an attacker use to hide and encode data inside DNS requests and queries?
* DNS tunneling
* DNSCrypt
* DNS security
* DNSSEC
Explanation/Reference: https://learn-umbrella.cisco.com/cloud-security/dns-tunneling

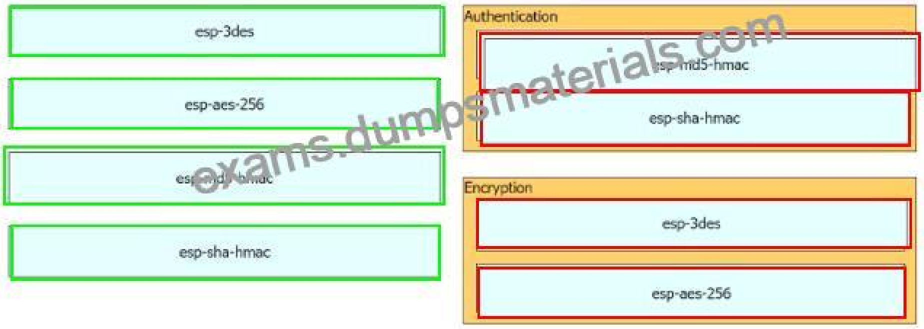
QUESTION 230

What do tools like Jenkins, Octopus Deploy, and Azure DevOps provide in terms of application and infrastructure automation?
* continuous integration and continuous deployment
* cloud application security broker
* compile-time instrumentation
* container orchestration

QUESTION 231

Drag and drop the cryptographic algorithms for IPsec from the left onto the cryptographic processes on the right.





QUESTION 232

Which risk is created when using an Internet browser to access cloud-based service?
* misconfiguration of infrastructure, which allows unauthorized access
* intermittent connection to the cloud connectors
* vulnerabilities within protocol
* insecure implementation of API

QUESTION 233

What is the benefit of integrating Cisco ISE with a MDM solution?
* It provides compliance checks for access to the network
* It provides the ability to update other applications on the mobile device
* It provides the ability to add applications to the mobile device through Cisco ISE
* It provides network device administration access
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_interoperab

QUESTION 234

In which two ways does Easy Connect help control network access when used with Cisco TrustSec? (Choose two)
* It allows multiple security products to share information and work together to enhance security posture in the network.
* It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.
* It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.
* It integrates with third-party products to provide better visibility throughout the network.
* It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).
Explanation Explanation Easy Connect simplifies network access control and segmentation by allowing the assignment of Security Group Tags to endpoints without requiring 802.1X on those endpoints, whether using wired or wireless connectivity. Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec-witheasy-connect-configuration-guide.pdf Explanation Easy Connect simplifies network access control and segmentation by allowing the assignment of Security Group Tags to endpoints without requiring 802.1X on those endpoints, whether using wired or wireless connectivity.

Explanation Explanation Easy Connect simplifies network access control and segmentation by allowing the assignment of Security Group Tags to endpoints without requiring 802.1X on those endpoints, whether using wired or wireless connectivity. Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec-witheasy-connect-configuration-guide.pdf

QUESTION 235

Which attack is preventable by Cisco ESA but not by the Cisco WSA?
* buffer overflow
* DoS
* SQL injection
* phishing
The following are the benefits of deploying Cisco Advanced Phishing Protection on the Cisco Email Security Gateway:

Prevents the following:

+ Attacks that use compromised accounts and social engineering.

+ Phishing, ransomware, zero-day attacks and spoofing.

+ BEC with no malicious payload or URL.

The following are the benefits of deploying Cisco Advanced Phishing Protection on the Cisco Email Security Gateway:

Prevents the following:

+ Attacks that use compromised accounts and social engineering.

+ Phishing, ransomware, zero-day attacks and spoofing.

+ BEC with no malicious payload or URL.

The following are the benefits of deploying Cisco Advanced Phishing Protection on the Cisco Email Security Gateway:

Prevents the following:

+ Attacks that use compromised accounts and social engineering.

+ Phishing, ransomware, zero-day attacks and spoofing.

+ BEC with no malicious payload or URL.

Reference:

5/m_advanced_phishing_protection.html

5/m_advanced_phishing_protection.html

QUESTION 236

Which Cisco security solution determines if an endpoint has the latest OS updates and patches installed on the system?
* Cisco Endpoint Security Analytics
* Cisco AMP for Endpoints
* Endpoint Compliance Scanner
* Security Posture Assessment Service

QUESTION 237

How does Cisco Stealthwatch Cloud provide security for cloud environments?
* It delivers visibility and threat detection.
* It prevents exfiltration of sensitive data.
* It assigns Internet-based DNS protection for clients and servers.
* It facilitates secure connectivity between public and private networks.
Explanation

Cisco Stealthwatch Cloud: Available as an SaaS product offer to provide visibility and threat detection within public cloud infrastructures such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

QUESTION 238

Which solution allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard?
* Cisco Umbrella
* Cisco AMP for Endpoints
* Cisco ISE
* Cisco Stealthwatch

QUESTION 239

A switch with Dynamic ARP Inspection enabled has received a spoofed ARP response on a trusted interface.

How does the switch behave in this situation?
* It forwards the packet after validation by using the MAC Binding Table.
* It drops the packet after validation by using the IP & MAC Binding Table.
* It forwards the packet without validation.
* It drops the packet without validation.
Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets on untrusted interfaces by comparing the MAC address to IP address bindings in the DHCP snooping database or an ARP access-list. If the ARP packet contains invalid or spoofed information, it is dropped and logged. DAI also inspects ARP packets on trusted interfaces, but it does not drop them if they are invalid. Instead, it forwards them to the destination without validation. This allows the switch to support devices that use static IP addresses or have legitimate reasons to send ARP packets with different MAC address to IP address bindings. However, this also means that if a spoofed ARP packet is received on a trusted interface, it will bypass the DAI validation and be forwarded to the destination. This could allow an attacker to poison the ARP cache of other devices and perform a man-in-the-middle attack. Therefore, the correct answer is option B. The switch drops the packet after validation by using the IP & MAC Binding Table.
References:

* Understanding and Configuring Dynamic ARP Inspection

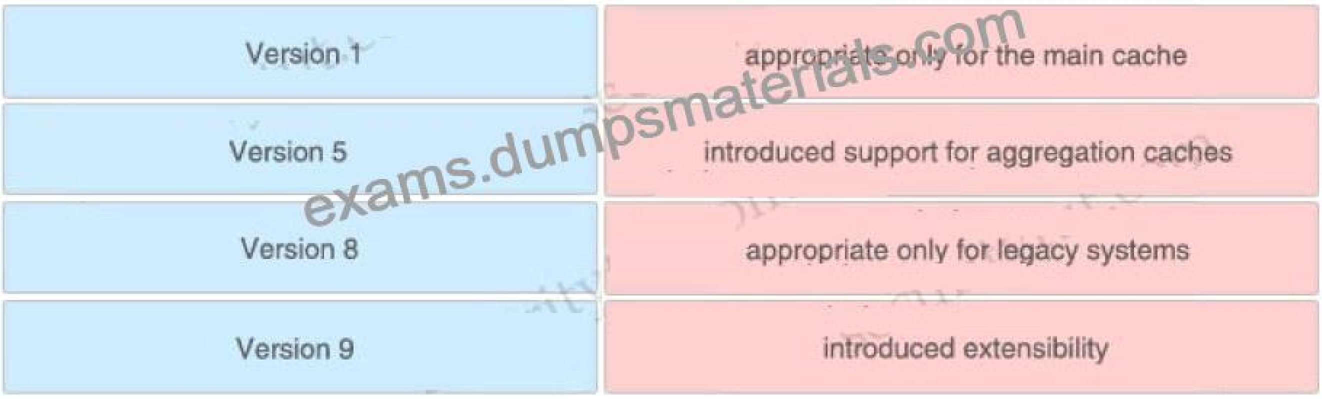
* DAI (Dynamic ARP Inspection)

* Dynamic ARP Inspection (DAI) Explanation & Configuration

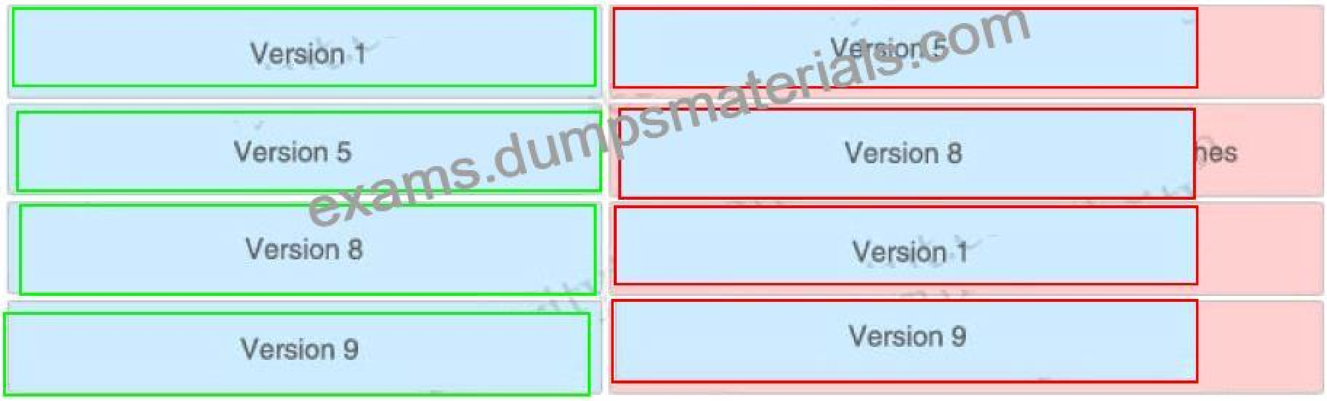
* Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

QUESTION 240

Drag and drop the NetFlow export formats from the left onto the descriptions on the right.



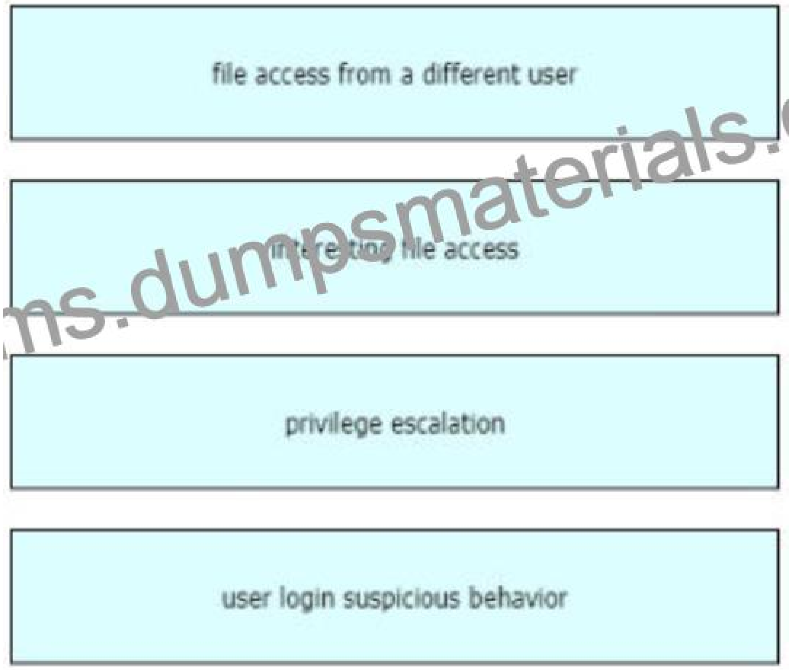
Version 1	appropriate only for the main cache
Version 5	introduced support for aggregation caches
Version 8	appropriate only for legacy systems
Version 9	introduced extensibility



Version 1	Version 5
Version 5	Version 8 hes
Version 8	Version 1
Version 9	Version 9

QUESTION 241

Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.



file access from a different user

interesting file access

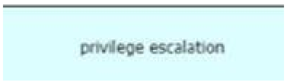
privilege escalation

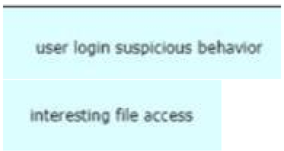
user login suspicious behavior

see the answer below.

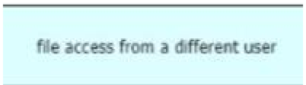
Explanation

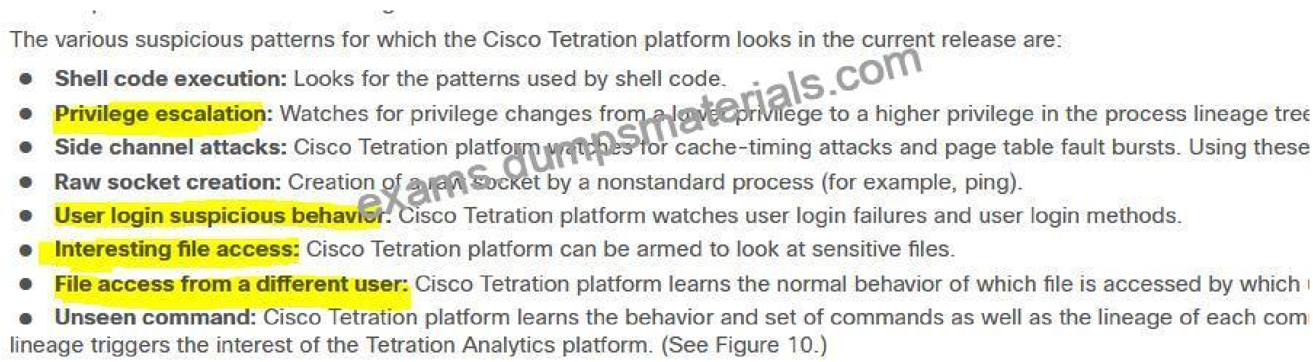
Answer options


privilege escalation


user login suspicious behavior

interesting file access


file access from a different user


The various suspicious patterns for which the Cisco Tetration platform looks in the current release are:

- **Shell code execution:** Looks for the patterns used by shell code.
- **Privilege escalation:** Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree
- **Side channel attacks:** Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these
- **Raw socket creation:** Creation of a raw socket by a nonstandard process (for example, ping).
- **User login suspicious behavior:** Cisco Tetration platform watches user login failures and user login methods.
- **Interesting file access:** Cisco Tetration platform can be armed to look at sensitive files.
- **File access from a different user:** Cisco Tetration platform learns the normal behavior of which file is accessed by which
- **Unseen command:** Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each com

lineage triggers the interest of the Tetration Analytics platform. (See Figure 10.)

https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-7403

350-701 Dumps To Pass Cisco Exam in 24 Hours - DumpsMaterials:
https://www.dumpsmaterials.com/350-701-real-torrent.html]