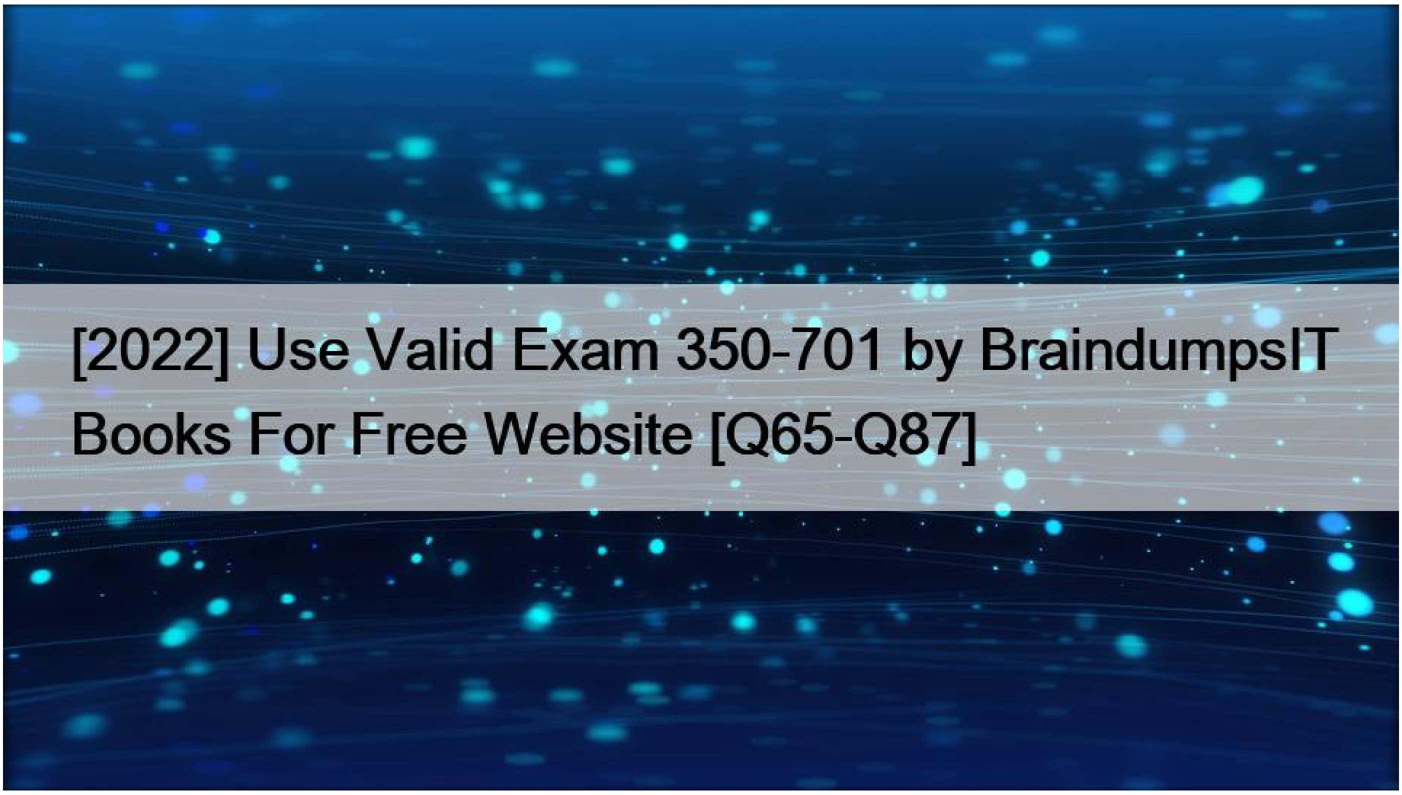
[2022 Use Valid Exam 350-701 by BraindumpsIT Books For Free Website [Q65-Q87



[2022] Use Valid Exam 350-701 by BraindumpsIT Books For Free Website
Free CCNP Security 350-701 Official Cert Guide PDF Download

QUESTION 65

In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?
* Smurf
* distributed denial of service
* cross-site scripting
* rootkit exploit
Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message.

Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on.

For example the code below is written in hex: <a

href=javascript:alert&#

x28&#8217;XSS&#8217;)>Click Here</a>

is equivalent to:

<a href=javascript:alert(&#8216;XSS&#8217;)>Click Here</a>

Note: In the format &#8220;&#xhhhh&#8221;, hhhh is the code point in hexadecimal form.

QUESTION 66

An organization has a Cisco ESA set up with policies and would like to customize the action assigned for violations. The organization wants a copy of the message to be delivered with a message added to flag it as a DLP violation. Which actions must be performed in order to provide this capability?
* deliver and send copies to other recipients
* quarantine and send a DLP violation notification
* quarantine and alter the subject header with a DLP violation
* deliver and add disclaimer text
You specify primary and secondary actions that the appliance will take when it detects a possible DLP violation in an outgoing message. Different actions can be assigned for different violation types and severities. Primary actions include: &#8211; Deliver &#8211; Drop &#8211; Quarantine Secondary actions include: &#8211; Sending a copy to a policy quarantine if you choose to deliver the message. The copy is a perfect clone of the original, including the Message ID. Quarantining a copy allows you to test the DLP system before deployment in addition to providing another way to monitor DLP violations. When you release the copy from the quarantine, the appliance delivers the copy to the recipient, who will have already received the original message. &#8211; Encrypting messages. The appliance only encrypts the message body. It does not encrypt the message headers. &#8211; Altering the subject header of messages containing a DLP violation. &#8211; Adding disclaimer text to messages. &#8211; Sending messages to an alternate destination mailhost. &#8211; Sending copies (bcc) of messages to other recipients. (For example, you could copy messages with critical DLP violations to a compliance officer&#8217;s mailbox for examination.) &#8211; Sending a DLP violation notification message to the sender or other contacts, such as a manager or DLP compliance officer. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html in an outgoing message. Different actions can be assigned for different violation types and severities.

Primary actions include:

&#8211; Deliver

&#8211; Drop

&#8211; Quarantine

Secondary actions include:

&#8211; Sending a copy to a policy quarantine if you choose to deliver the message. The copy is a perfect clone of the original, including the Message ID. Quarantining a copy allows you to test the DLP system before deployment in addition to providing another way to monitor DLP violations. When you release the copy from the quarantine, the appliance delivers the copy to the recipient, who will have already received the original message.

&#8211; Encrypting messages. The appliance only encrypts the message body. It does not encrypt the message headers.

&#8211; Altering the subject header of messages containing a DLP violation.

&#8211; Adding disclaimer text to messages.

&#8211; Sending messages to an alternate destination mailhost.

&#8211; Sending copies (bcc) of messages to other recipients. (For example, you could copy messages with critical DLP violations to a compliance officer&#8217;s mailbox for examination.)

&#8211; Sending a DLP violation notification message to the sender or other contacts, such as a manager or DLP compliance officer.

Reference:

You specify primary and secondary actions that the appliance will take when it detects a possible DLP violation in an outgoing message. Different actions can be assigned for different violation types and severities. Primary actions include: &#8211; Deliver &#8211; Drop &#8211; Quarantine Secondary actions include: &#8211; Sending a copy to a policy quarantine if you choose to deliver the message. The copy is a perfect clone of the original, including the Message ID. Quarantining a copy allows you to test the DLP system before deployment in addition to providing another way to monitor DLP violations. When you release the copy from the quarantine, the appliance delivers the copy to the recipient, who will have already received the original message. &#8211; Encrypting messages. The appliance only encrypts the message body. It does not encrypt the message headers. &#8211; Altering the subject header of messages containing a DLP violation. &#8211; Adding disclaimer text to messages. &#8211; Sending messages to an alternate destination mailhost. &#8211; Sending copies (bcc) of messages to other recipients. (For example, you could copy messages with critical DLP violations to a compliance officer&#8217;s mailbox for examination.) &#8211; Sending a DLP violation notification message to the sender or other contacts, such as a manager or DLP compliance officer. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html

QUESTION 67

Which algorithm provides asymmetric encryption?

- RC4
- RSA
- AES
- 3DES

Reference:

https://securityboulevard.com/2020/05/types-of-encryption-5-encryption-algorithms-how-to-choose-the-right-one/#:~:text=Standard%20asymmetric%20encryption%20algorithms%20include,%2C%20El%20Gamal%2C%20and%20DSA.

QUESTION 68

Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?

- Correlation
- Intrusion
- Access Control
- Network Discovery

The Firepower System uses network discovery and identity policies to collect host, application, and user data for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible. You can configure your network discovery policy to perform host and application detection. Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introduction_to_network_discovery_and_identity.html for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible.

You can configure your network discovery policy to perform host and application detection.

The Firepower System uses network discovery and identity policies to collect host, application, and user data for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible. You can configure your network discovery policy to perform host and application detection. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introduction_to_network_discovery_and_identity.html

QUESTION 69

Which compliance status is shown when a configured posture policy requirement is not met?
* unknown
* authorized
* compliant
* noncompliant

QUESTION 70

What are two DDoS attack categories? (Choose two.)
* sequential
* protocol
* database
* volume-based
* scree-based

Explanation

https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html

QUESTION 71

Which public cloud provider supports the Cisco Next Generation Firewall Virtual?
* Google Cloud Platform
* Red Hat Enterprise Visualization
* VMware ESXi
* Amazon Web Services

Explanation Explanation Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco&#8217;s Firepower next generation firewall. The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure. In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet. In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions. Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/ white-paper-c11-740505.html Explanation Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco&#8217;s Firepower next generation firewall.

The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure.

In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet.

In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions.

Explanation Explanation Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco&#8217;s Firepower next generation firewall. The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure. In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet. In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions. Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/ white-paper-c11-740505.html

QUESTION 72

What are two rootkit types? (Choose two)
* registry
* bootloader
* buffer mode
* user mode
* virtual

QUESTION 73

When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, which name is used?
* Common Vulnerabilities and Exposures
* Common Exploits and Vulnerabilities
* Common Security Exploits
* Common Vulnerabilities, Exploits and Threats
Explanation

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cve/174/cve-addressed-1741.html

QUESTION 74

Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two)
* packet decoder
* SIP
* modbus
* inline normalization
* SSL
Application layer protocols can represent the same data in a variety of ways. The Firepower System provides application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing

application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Application_Layer_Preprocessors.html#ID-2244-0000080c FirePower uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results.

Reference:

Application layer protocols can represent the same data in a variety of ways. The Firepower System provides application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Application_Layer_Preprocessors.html#ID-2244-0000080c FirePower uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

QUESTION 75

Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect from phishing attacks? (Choose two.)
* blocks malicious websites and adds them to a block list
* does a real-time user web browsing behavior analysis
* provides a defense for on-premises email deployments
* uses a static algorithm to determine malicious
* determines if the email messages are malicious

QUESTION 76

Which two fields are defined in the NetFlow flow? (Choose two)
* type of service byte
* class of service bits
* Layer 4 protocol type
* destination port
* output logical interface
Explanation

Explanation

Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share seven values which define a unique key for the flow:

+ Ingress interface (SNMP ifIndex)

+ Source IP address

+ Destination IP address

+ IP protocol

+ Source port for UDP or TCP, 0 for other protocols

+ Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols

+ IP Type of Service

Note: A flow is a unidirectional series of packets between a given source and destination.

QUESTION 77

Which algorithm provides encryption and authentication for data plane communication?
* AES-GCM
* SHA-96
* AES-256
* SHA-384
Explanation The data plane of any network is responsible for handling data packets that are transported across the network. (The data plane is also sometimes called the forwarding plane.) Maybe this Qwants to ask about the encryption and authentication in the data plane of a SD-WAN network (but SD-WAN is not a topic of the SCOR 350-701 exam?). In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetrickey algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates. Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html The data plane of any network is responsible for handling data packets that are transported across the network.

(The data plane is also sometimes called the forwarding plane.)

Maybe this Qwants to ask about the encryption and authentication in the data plane of a SD-WAN network (but SD-WAN is not a topic of the SCOR 350-701 exam?).

In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetrickey algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates.

Explanation The data plane of any network is responsible for handling data packets that are transported across the network. (The data plane is also sometimes called the forwarding plane.) Maybe this Qwants to ask about the encryption and authentication in the data plane of a SD-WAN network (but SD-WAN is not a topic of the SCOR 350-701 exam?). In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetrickey algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates. Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html

QUESTION 78

A network engineer is configuring DMVPN and entered the crypto is akmp key cisc0380739941 address

0.0.0.0 command on host A The tunnel is not being established to host B.

What action is needed to authenticate the VPN?
* Enter the same command on host B.
* Enter the command with a different password on host B.
* Change isakmp to ikev2 in the command on host A.
* Change the password on host A to the default password.

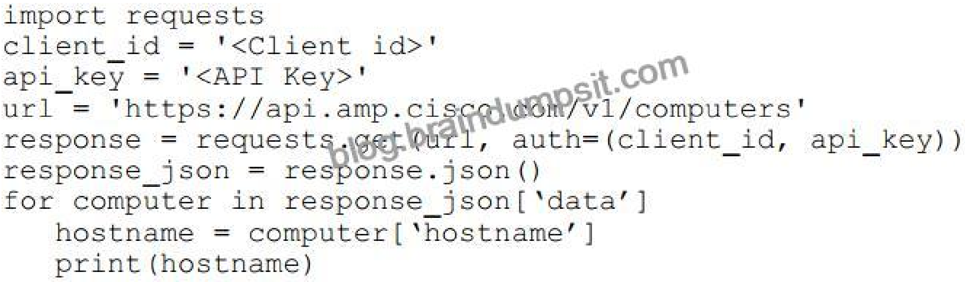
QUESTION 79

An engineer is configuring web filtering for a network using Cisco Umbrella Secure Internet Gateway.

The requirement is that all traffic needs to be filtered. Using the SSL decryption feature, which type of certificate should be presented to the end-user to accomplish this goal?
* third-party
* self-signed
* organization owned root
* SubCA

QUESTION 80

Refer to the exhibit.



```
import requests
client_id = '<Client id>'
api_key = '<API Key>'
url = 'https://api.amp.cisco.com/v1/computers'
response = requests.get(url, auth=(client_id, api_key))
response_json = response.json()
for computer in response_json[‘data’]
   hostname = computer[‘hostname’]
   print(hostname)
```

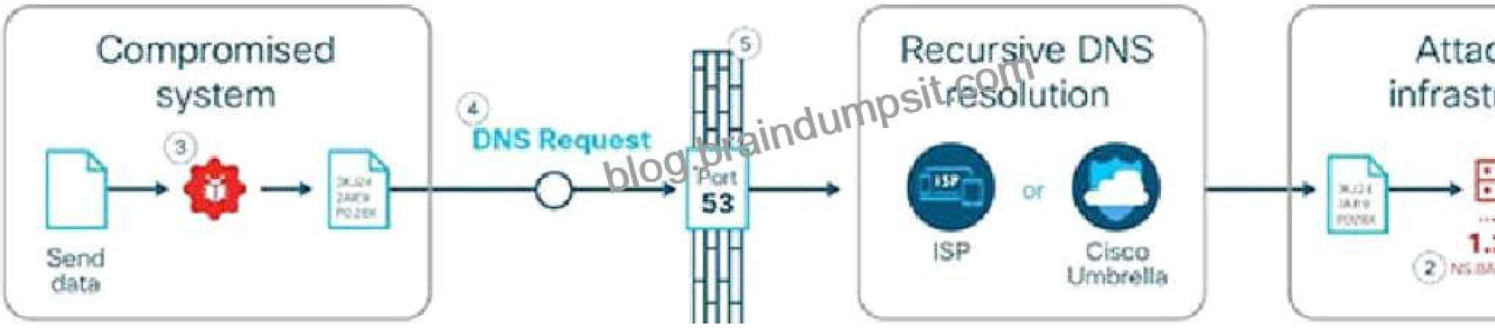
What will happen when the Python script is executed?
* The hostname will be translated to an IP address and printed.
* The hostname will be printed for the client in the client ID field.
* The script will pull all computer hostnames and print them.
* The script will translate the IP address to FODN and print it

QUESTION 81

How is DNS tunneling used to exfiltrate data out of a corporate network?
* It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.
* It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data.
* It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network.
* It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.
Explanation

Domain name system (DNS) is the protocol that translates human-friendly URLs, such as securitytut.com, into IP addresses, such as 183.33.24.13. Because DNS messages are only used as the beginning of each communication and they are not intended for data transfer, many organizations do not monitor their DNS traffic for malicious activity. As a result, DNS-based attacks can be effective if launched against their networks. DNS tunneling is one such attack.

An example of DNS Tunneling is shown below:



The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNS nameserver (NS) and malicious payload.

2. An IP address (e.g. 1.2.3.4) is allocated from the attacker&#8217;s infrastructure and a domain name (e.g. attackerdomain.com) is registered or reused. The registrar informs the top-level domain (.com) nameservers to refer requests for attackerdomain.com to ns.attackerdomain.com, which has a DNS record mapped to 1.2.3.4

3. The attacker compromises a system with the malicious payload. Once the desired data is obtained, the payload encodes the data as a series of 32 characters (0-9, A-Z) broken into short strings (3KJ242AIE9, P028X977W,&#8230;).

4. The payload initiates thousands of unique DNS record requests to the attacker&#8217;s domain with each string as a part of the domain name (e.g. 3KJ242AIE9.attackerdomain.com). Depending on the attacker&#8217;s patience and stealth, requests can be spaced out over days or months to avoid suspicious network activity. 5. The requests are forwarded to a recursive DNS resolver. During resolution, the requests are sent to the attacker&#8217;s authoritative DNS nameserver, 6. The tunneling kit parses the encoded strings and rebuilds the exfiltrated data. Reference: https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0

5. The requests are forwarded to a recursive DNS resolver. During resolution, the requests are sent to the attacker&#8217;s authoritative DNS nameserver,

6. The tunneling kit parses the encoded strings and rebuilds the exfiltrated data.

a part of the domain name (e.g. 3KJ242AIE9.attackerdomain.com). Depending on the attacker&#8217;s patience and stealth, requests can be spaced out over days or months to avoid suspicious network activity. 5. The requests are forwarded to a recursive DNS resolver. During resolution, the requests are sent to the attacker&#8217;s authoritative DNS nameserver, 6. The tunneling kit parses the encoded strings and rebuilds the exfiltrated data. Reference: https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0

QUESTION 82

Which threat involves software being used to gain unauthorized access to a computer system?
* ping of death

* NTP amplification
* HTTP flood
* virus

QUESTION 83

What is the benefit of integrating cisco ISE with a MDM solution?
* It provides the ability to update other applications on the mobile device
* It provides compliance checks for access to the network
* It provides the ability to add applications to the mobile device through Cisco ISE
* It provides network device administration access

QUESTION 84

Under which two circumstances is a CoA issued? (Choose two.)
* A new authentication rule was added to the policy on the Policy Service node.
* An endpoint is deleted on the Identity Service Engine server.
* A new Identity Source Sequence is created and referenced in the authentication policy.
* An endpoint is profiled for the first time.
* A new Identity Service Engine server is added to the deployment with the Administration persona.
Explanation/Reference: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

QUESTION 85

Which two request of REST API are valid on the Cisco ASA Platform? (Choose two.)
* Put
* Option
* Get
* Push
* Connect

QUESTION 86

An organization wants to secure users, data, and applications in the cloud. The solution must be API-based and operate as a cloud-native CASB. Which solution must be used for this implementation?
* Cisco Cloudlock
* Cisco Cloud Email Security
* Cisco Firepower Next-Generation Firewall
* Cisco Umbrella
Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform.

Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform.

Reference:

738565.pdf

Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and

cloud cybersecurity platform.

738565.pdf

QUESTION 87

Which benefit does DMVPN provide over GETVPN?
* DMVPN supports QoS, multicast, and routing, and GETVPN supports only QoS.
* DMVPN is a tunnel-less VPN, and GETVPN is tunnel-based.
* DMVPN supports non-IP protocols, and GETVPN supports only IP protocols.
* DMVPN can be used over the public Internet, and GETVPN requires a private network.