350-701$^{Q\&As}$

Implementing and Operating Cisco Security Core Technologies (SCOR)

Pass Cisco 350-701 Exam with 100% Guarantee

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

How does DNS Tunneling exfiltrate data?

A. An attacker registers a domain that a client connects to based on DNS records and sends malware through that connection.

B. An attacker opens a reverse DNS shell to get into the client\\'s system and install malware on it.

C. An attacker uses a non-standard DNS port to gain access to the organization\\'s DNS servers in order to poison the resolutions.

D. An attacker sends an email to the target with hidden DNS resolvers in it to redirect them to a malicious domain.

Correct Answer: A

The attacker registers a domain, such as badsite.com. The domain\\'s name server points to the attacker\\'s server, where a tunneling malware program is installed.

The attacker infects a computer, which often sits behind a company\\'s firewall, with malware. Because DNS requests are always allowed to move in and out of the firewall, the infected computer is allowed to send a query to the DNS resolver.

The DNS resolver is a server that relays requests for IP addresses to root and top-level domain servers.

The DNS resolver routes the query to the attacker\\'s command-and-control server, where the tunneling program is installed. A connection is now established between the victim and the attacker through the DNS resolver. This tunnel can be

used to exfiltrate data or for other malicious purposes. Because there is no direct connection between the attacker and victim, it is more difficult to trace the attacker\\'s computer.

QUESTION 2

Which two actions does the Cisco identity Services Engine posture module provide that ensures endpoint security?(Choose two.)

A. The latest antivirus updates are applied before access is allowed.

B. Assignments to endpoint groups are made dynamically, based on endpoint attributes.

C. Patch management remediation is performed.

D. A centralized management solution is deployed.

E. Endpoint supplicant configuration is deployed.

Correct Answer: AC

ISE posture assessment includes a set of rules in a security policy that define a series of checks before an endpoint is granted access to the network. Posture assessment checks include the installation of OS patches, host based firewall, antivirus and anti-malware software, disk encryption and more

QUESTION 3

Which two parameters are used for device compliance checks? (Choose two.)

A. endpoint protection software version

B. Windows registry values

C. DHCP snooping checks

D. DNS integrity checks

E. device operating system version

Correct Answer: BE

QUESTION 4

Which two capabilities does TAXII support? (Choose two)

A. Exchange

B. Pull messaging

C. Binding

D. Correlation

E. Mitigating

Correct Answer: AB

https://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part1-overview.html

"There are three Capabilities that the current version of TAXII supports: push messaging, pull messaging, and discovery." "Discovery does, however, allow for the automated exchange of information..."

QUESTION 5

What features does Cisco FTDv provide over Cisco ASAv?

A. Cisco FTDv runs on VMWare while ASAv does not

B. Cisco FTDv provides 1GB of firewall throughput while Cisco ASAv does not

C. Cisco FTDv runs on AWS while ASAv does not

D. Cisco FTDv supports URL filtering while ASAv does not

Correct Answer: D