200-201$^{\text{Q\&As}}$

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

QUESTION 1

What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

A. least privilege

B. need to know

C. integrity validation

D. due diligence

Correct Answer: A

QUESTION 2

What is the impact of false positive alerts on business compared to true positive?

A. True positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.

B. True positive alerts are blocked by mistake as potential attacks affecting application availability.

C. False positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.

D. False positive alerts are blocked by mistake as potential attacks affecting application availability.

Correct Answer: C

QUESTION 3

What is an advantage of symmetric over asymmetric encryption?

A. A key is generated on demand according to data type.

B. A one-time encryption key is generated for data transmission

C. It is suited for transmitting large amounts of data.

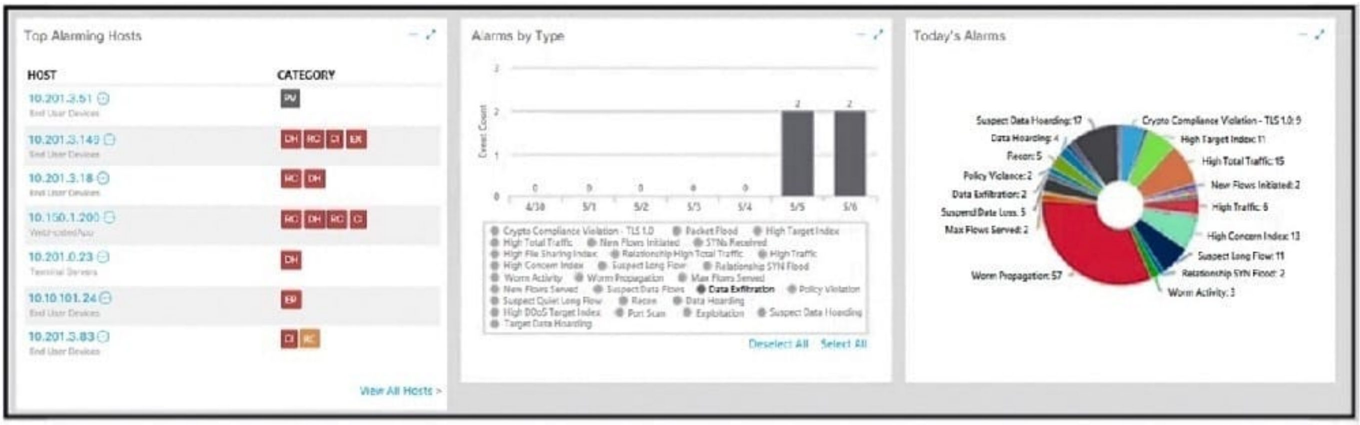
D. It is a faster encryption mechanism for sessions

Correct Answer: D

Symmetric Encryption is generally faster than asymmetric encryption, as it requires less computational power, making it suitable for encrypting large amounts of data

QUESTION 4

Refer to the exhibit.



Top Alarming Hosts

HOST	CATEGORY
10.201.3.51 End User Devices	PV
10.201.3.149 End User Devices	DH RC CI EX
10.201.3.18 End User Devices	RC DH
10.150.1.200 Web Hosted Apps	RC DH RC CI
10.201.0.23 Terminal Servers	DH
10.10.101.24 End User Devices	EP
10.201.3.83 End User Devices	CI RC

View All Hosts >
Alarms by Type
Event Count
0
1
2
3
0
0
0
0
0
2
2
4/30
5/1
5/2
5/3
5/4
5/5
5/6
● Crypto Compliance Violation - TLS 1.0 ● Packet Flood ● High Target Index
● High Total Traffic ● New Flows Initiated ● SYNs Received
● High File Sharing Index ● Relationship High Total Traffic ● High Traffic
● High Concern Index ● Suspect Long Flow ● Relationship SYN Flood
● Worm Activity ● Worm Propagation ● Max Flows Served
● New Flows Served ● Suspect Data Flows ● Data Exfiltration ● Policy Violation
● Suspect Quiet Long Flow ● Recon ● Data Hoarding
● High DDoS Target Index ● Port Scan ● Exploitation ● Suspect Data Hoarding
● Target Data Hoarding
Deselect All
Select All
Today's Alarms
Suspect Data Hoarding: 17
Data Hoarding: 4
Recon: 5
Policy Violance: 2
Data Exfiltration: 2
Suspend Date Loss: 5
Max Flows Served: 2
Worm Propagation: 57
Crypto Compliance Violation - TLS 1.0: 9
High Target Index: 11
High Total Traffic: 15
New Flows Initiated: 2
High Traffic: 6
High Concern Index: 13
Suspect Long Flow: 11
Relationship SYN Flood: 2
Worm Activity: 3

What is the potential threat identified in this Stealthwatch dashboard?

A. A policy violation is active for host 10.10.101.24.

B. A host on the network is sending a DDoS attack to another inside host.

C. There are two active data exfiltration alerts.

D. A policy violation is active for host 10.201.3.149.

Correct Answer: C

QUESTION 5

Which process is used when IPS events are removed to improve data integrity?

A. data availability

B. data normalization

C. data signature

D. data protection

Correct Answer: B

QUESTION 6

A developer is working on a project using a Linux tool that enables writing processes to obtain these required results:

If the process is unsuccessful, a negative value is returned. If the process is successful, 0 value is returned to the child process, and the process ID is sent to the parent process.

Which component results from this operation?

A. parent directory name of a file pathname

B. process spawn scheduled

C. macros for managing CPU sets

D. new process created by parent process

Correct Answer: D

There are two tasks with specially distinguished process IDs: swapper or sched has process ID 0 and is responsible for paging, and is actually part of the kernel rather than a normal user-mode process. Process ID 1 is usually the init process primarily responsible for starting and shutting down the system. Originally, process ID 1 was not specifically reserved for init by any technical measures: it simply had this ID as a natural consequence of being the first process invoked by the kernel. More recent Unix systems typically have additional kernel components visible as \\'processes\\', in which case PID 1 is actively reserved for the init process to maintain consistency with older systems

QUESTION 7

Which attack method intercepts traffic on a switched network?

A. denial of service

B. ARP cache poisoning

C. DHCP snooping

D. command and control

Correct Answer: B

An ARP-based MITM attack is achieved when an attacker poisons the ARP cache of two devices with the MAC address of the attacker\\'s network interface card (NIC). Once the ARP caches have been successfully poisoned, each victim device sends all its packets to the attacker when communicating to the other device and puts the attacker in the middle of the communications path between the two victim devices. It allows an attacker to easily monitor all communication between victim devices. The intent is to intercept and view the information being passed between the two victim devices and potentially introduce sessions and traffic between the two victim devices

QUESTION 8

Which type of data collection requires the largest amount of storage space?

A. alert data

B. transaction data

C. session data

D. full packet capture

Correct Answer: D

QUESTION 9

What is the difference between vulnerability and risk?

A. A vulnerability is a sum of possible malicious entry points, and a risk represents the possibility of the unauthorized entry itself.

B. A risk is a potential threat that an exploit applies to, and a vulnerability represents the threat itself

C. A vulnerability represents a flaw in a security that can be exploited, and the risk is the potential damage it might cause.

D. A risk is potential threat that adversaries use to infiltrate the network, and a vulnerability is an exploit

Correct Answer: C

QUESTION 10

What is a difference between tampered and untampered disk images?

A. Tampered images have the same stored and computed hash.

B. Tampered images are used as evidence.

C. Untampered images are used for forensic investigations.

D. Untampered images are deliberately altered to preserve as evidence

Correct Answer: B

QUESTION 11

Which of these describes volatile evidence?

A. logs

B. registers and cache

C. disk and removable drives

D. usernames

Correct Answer: B

Caches and Registers- Data in memory is the most volatile. This includes data in centralprocessor unit (CPU) registers, caches, and system random access memory(RAM).- The data in cache and CPU registers is the most volatile,

mostlybecause the storage space is so small.

https://blogs.getcertifiedgetahead.com/cfr-and-order-of-volatility/#:~:text=Caches%20and%20Registers,storage%20space%20is%20so%20small.

QUESTION 12

Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?

A. ClientStart, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

B. ClientStart, TLS versions it supports, cipher-suites it supports, and suggested compression methods

C. ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods

D. ClientHello, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

Correct Answer: C

QUESTION 13

What is the difference between deep packet inspection and stateful inspection?

A. Deep packet inspection gives insights up to Layer 7, and stateful inspection gives insights only up to Layer 4.

B. Deep packet inspection is more secure due to its complex signatures, and stateful inspection requires less human intervention.

C. Stateful inspection is more secure due to its complex signatures, and deep packet inspection requires less human intervention.

D. Stateful inspection verifies data at the transport layer and deep packet inspection verifies data at the application layer

Correct Answer: A

QUESTION 14

A user received a malicious email attachment named "DS045-report1122345.exe" and executed it. In which step of the Cyber Kill Chain is this event?

A. reconnaissance

B. delivery

C. weaponization

D. installation

Correct Answer: B

QUESTION 15

Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

A. availability

B. confidentiality

C. scope

D. integrity

Correct Answer: D