DUMPSBOSS.

Understanding Cisco Cybersecurity Fundamentals

Cisco 210-250

Version Demo

Total Demo Questions: 20

Total Premium Questions: 1138

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

What is the main difference between a Layer 2 switch and a multi layer switch?

A. A multilayer switch includes Layer 3 functionality.

B. A multilayer switch can be deployed on multiple racks.

C. A Layer 2 switch is faster.

D. A Layer 2 switch uses a MAC table whereas a multilayer switch uses an ARP table.

ANSWER: A

QUESTION NO: 2

In addition to discretionary, non-discretionary, and mandatory access control, which two should be part of an organization's access security plan? (Choose two.)

A. separation of duties

B. account lock-outs

C. physical security locks

D. principle of least privilege

E. photo identification

ANSWER: A D

QUESTION NO: 3 - (DRAG DROP)

DRAG DROP

Match the following characteristics with the appropriate threat model.

Select and Place:

Originally introduced by Lockheed Martin, it has seven stages, and the attackers do not necessarily need to follow the exact steps and sequences of the framework	APT
Originally introduced in the Mandiant Report, it maintains access to victim networks for a long time, and some of the most formidable threats are based in the intelligence services of foreign governments.	diamond model
Developed by Caltagirone, Pendergast, and Betzis, the four nodes in the model are: adversary, capability, infrastructure, and victim. An event that is described as an adversary deploys a capability over some infrastructure against a victim.	cyber kill chain

ANSWER:

	Originally introduced in the Mandiant Report, it maintains access to victim networks for a long time, and some of the most formidable threats are based in the intelligence services of foreign governments.
	Developed by Caltagirone, Pendergast, and Betzis, the four nodes in the model are: adversary, capability, infrastructure, and victim. An event that is described as an adversary deploys a capability over some infrastructure against a victim.
	Originally introduced by Lockheed Martin, it has seven stages, and the attackers do not necessarily need to follow the exact steps and sequences of the framework

QUESTION NO: 4

Which of the following are metrics that can measure the effectiveness of a runbook?

A. Mean time to repair (MTTR)

B. Mean time between failures (MTBF)

C. Mean time to discover a security incident

D. All of the above

ANSWER: D

QUESTION NO: 5

In which context is it inappropriate to use a hash algorithm?

A. SSH logins

B. verifying file integrity

C. Telnet logins

D. digital signature verification

ANSWER: C

QUESTION NO: 6

If the date and time are not synchronized among network and security devices, logs can become almost impossible to correlate. What protocol is recommended as a best practice to deploy to mitigate this issue?

A. Network address translation

B. Port address translation

C. Network Time Protocol (NTP)

D. Native Time Protocol (NTP)

ANSWER: C

QUESTION NO: 7

Chain of custody is the way you document and preserve evidence from the time you started the cyber forensics investigation to the time the evidence is

A. Documentation about how and when the evidence was collected

B. Documentation about how evidence was transported

C. Documentation about who had access to the evidence and how it was accessed

D. Documentation about the CVSS score of a given CVE

ANSWER: A B C

QUESTION NO: 8

What are two controls that the Cisco WSA can use to validate web requests? (Choose two.)

A. basic URL filtering that leverages pre-defined, category-based web usage controls

B. AMP for isolating reputable exploits and malware samples to its local disk for further investigation

C. a reputation database that is used to analyze web requests as part of a security control procedure

D. IPS-based signatures that are loaded in the Cisco WSA to prevent intrusions and alert system administrators

E. a reputation database within the Cisco WSA that uses Snort-like rule sets to combat RootKit intrusions

ANSWER: A C

QUESTION NO: 9

Which of the following are part of a security label used in the mandatory access control model? (Choose all that apply.)

A. Classification

B. Category

C. Role

D. Location

ANSWER: A B

QUESTION NO: 10

Which of the following is not a true statement about TACACS+?

A. It offers command-level authorization.

B. It is proprietary to Cisco.

C. It encrypts the TACACS+ header.

D. It works over TCP.

ANSWER: C

QUESTION NO: 11

What are three characteristics of an advanced persistent threat (APT)? (Choose three.)

A. one time or drive-by file dropper

B. pursues its objectives repeatedly over an extended period

C. easily identified by common antivirus tools

D. adapts to defenders' efforts to detect it

E. maintains a level of interactions with the attacker's command and control infrastructure to execute its objectives

F. usually injected via email attachment

G. does not exhibit any signs of polymorphic behavior

ANSWER: B D E

QUESTION NO: 12

Which two statements are true about malvertisements? (Choose two.)

A. Malvertisements are sometimes set up to affect all visitors to a site only during a specific period of time.

B. Malvertisements' malicious code remains forever.

C. Malvertisements affect both trustworthy and untrustworthy sites.

D. Infection only occurs when the victim clicks a malvertisement.

ANSWER: A C

QUESTION NO: 13

Which three are important distinctions of HTTP? (Choose three.)

A. Cookie information is sent in the URL.

B. Cookie information is sent in the URI.

C. Cookie information is sent in the response header.

D. Cookie information is sent in the request header.

E. Cookie information is sent in the request body.

F. Cookie information is sent in the response body.

G. Cookie information is sent via the response codes.

H. Cookie information is always private and encrypted.

I. Cookie information is stored on the client's browser.

Answer: CDI

Explanation:

ANSWER: C D I

QUESTION NO: 14

How is malware that is not on the whitelist able to execute?

A. by executing it in memory and injecting malicious code into a legitimate process that is currently running

B. by changing the register setting

C. by packing (encrypting or compressing) the file

D. by executing it using the safe mode

ANSWER: A

QUESTION NO: 15

The Cisco CWS service uses web proxies in the Cisco cloud environment that scan traffic for malware and policy enforcement. Cisco customers can connect to the Cisco CWS service directly by using a proxy auto-configuration (PAC) file in the user endpoint or through connectors integrated into which of the following Cisco products?

A. Cisco ISR G2 routers

B. Cisco ASA

C. Cisco WSA

D. Cisco AnyConnect Secure Mobility Client

ANSWER: A B C D

QUESTION NO: 16

What protocol uses TCP port 143?

A. SMTP

B. POP

C. LDAP

D. IMAP

ANSWER: D

QUESTION NO: 17

ARP messages are sent using which Ethertype designation in the frame header?

A. 0x2100

B. 0x0800

C. 0x8100

D. 0x0806

ANSWER: D

QUESTION NO: 18

If a client connected to a server using SSHv1 previously, how should the client be able to authenticate the server?

A. The same encryption algorithm will be used each time and will be in the client cache.

B. The server will autofill the stored password for the client upon connection.

C. The client will receive the same public key that it had stored for the server.

D. The server will not use any asymmetric encryption, and jump right to symmetric encryption.

ANSWER: C

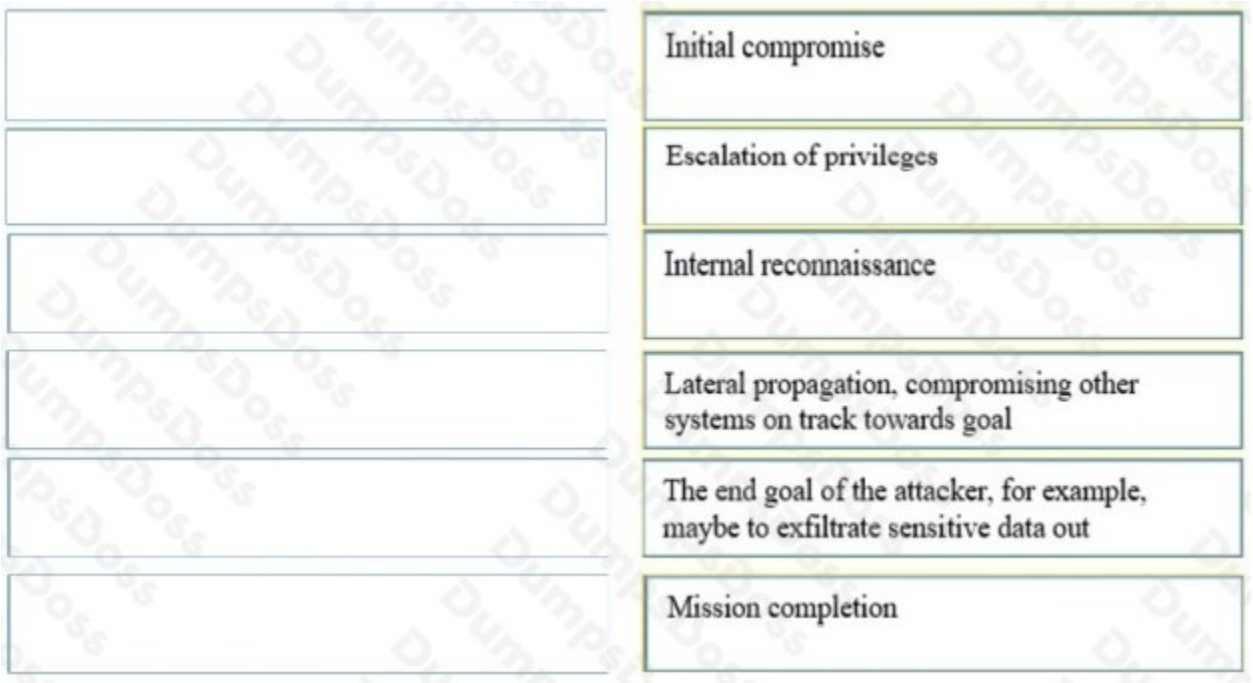
QUESTION NO: 19 - (DRAG DROP)

DRAG DROP

The structure of an APT attack does not follow a blueprint, but there is a common methodology to the attack. Match the attack steps to their description:

Select and Place:

ANSWER:



QUESTION NO: 20

Which of the following are examples of application file and folder attributes that can help with application whitelisting?

A. Application store

B. File path

C. Filename

D. File size

ANSWER: B C D