www.CertBus.com

CERTBUS

210-250^{Q&As}

210-250 $^{Q\&As}$

Understanding Cisco Cybersecurity Fundamentals

Pass Cisco 210-250 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/210-250.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which term represents the likely hood of potential danger that could take advantage of a weakness in a system?

A. vulnerability

B. risk

C. threat

D. exploit

Correct Answer: B

QUESTION 2

Which term represents a potential danger that could take advantage of a weakness in a system?

A. vulnerability

B. risk

C. threat

D. exploit

Correct Answer: D

QUESTION 3

How many broadcast domains are created if three hosts are connected to a Layer 2 switch in full-duplex mode?

A. 4

B. 3

C. None

D. 1

Correct Answer: D

QUESTION 4

Which definition of a Linux daemon is true?

A. Process that is causing harm to the system by either using up system resources or causing a critical crash.

B. Long ?running process that is the child at the init process

C. process that has no parent process

D. process that is starved at the CPU.

Correct Answer: B

QUESTION 5

You must create a vulnerability management framework. Which main purpose of this framework is true?

A. Conduct vulnerability scans on the network.

B. Manage a list of reported vulnerabilities.

C. Identify, remove and mitigate system vulnerabilities.

D. Detect and remove vulnerabilities in source code.

Correct Answer: C

QUESTION 6

Which two features must a next generation firewall include? (Choose two.)

A. data mining

B. host-based antivirus

C. application visibility and control

D. Security Information and Event Management

E. intrusion detection system

Correct Answer: CE

QUESTION 7

You get an alert on your desktop computer showing that an attack was successful on the host but up on investigation you see that occurred duration the attack. Which reason is true?

A. The computer has HIDS installed on it

B. The computer has NIDS installed on it

C. The computer has HIPS installed on it

D. The computer has NIPS installed on it

Correct Answer: A

QUESTION 8

Which two terms are types of cross site scripting attacks? (Choose two)

A. directed

B. encoded

C. stored

D. reflected

E. cascaded

Correct Answer: CD

QUESTION 9

Based on which statement does the discretionary access control security model grant or restrict access?

A. discretion of the system administrator

B. security policy defined by the owner of an object

C. security policy defined by the system administrator

D. role of a user within an organization

Correct Answer: B

QUESTION 10

If a web server accepts input from the user and passes it to a bash shell, to which attack method is it vulnerable?

A. input validation

B. hash collision

C. command injection

D. integer overflow

Correct Answer: C

QUESTION 11

Which definition of the IIS Log Parser tool is true?

A. a logging module for IIS that allows you to log to a database

B. a data source control to connect to your data source

C. a powerful, versatile tool that makes it possible to run SQL-like queries against log flies

D. a powerful versatile tool that verifies the integrity of the log files

Correct Answer: C

QUESTION 12

Which term describes reasonable effort that must be made to obtain relevant information to facilitate appropriate courses of action?

A. Due diligence

B. ethical behavior

C. decision making

D. data mining.

Correct Answer: A

QUESTION 13

which security principle is violated by running all processes as root/admin

A. RBAC

B. Principle of least privilege C. Segregation of duty

Correct Answer: B

QUESTION 14

As per RFC 1035 which transport layer protocol is used for DNS zone transfer?

A. HTTP

B. RDP

C. UDP

D. TCP

Correct Answer: D

QUESTION 15

For which purpose can Windows management instrumentation be used?

A. Remote viewing of a computer

B. Remote blocking of malware on a computer

C. Remote reboot of a computer

D. Remote start of a computer

Correct Answer: A

QUESTION 16

According to the attribute-based access control (ABAC) model, what is the subject location considered?

A. Part of the environmental attributes

B. Part of the object attributes

C. Part of the access control attributes

D. None of the above

Correct Answer: A

QUESTION 17

An attacker installs a rogue switch that sends superior BPDUs on your network.

What is a possible result of this activity?

A. The switch could offer fake DHCP addresses.

B. The switch could become the root bridge.

C. The switch could be allowed to join the VTP domain

D. The switch could become a transparent bridge.

Correct Answer: B

QUESTION 18

Which two actions are valid uses of public key infrastructure? (Choose two)

A. ensuring the privacy of a certificate

B. revoking the validation of a certificate

C. validating the authenticity of a certificate

D. creating duplicate copies of a certificate

E. changing ownership of a certificate

Correct Answer: AC

QUESTION 19

Which definition of a fork in Linux is true?

A. daemon to execute scheduled commands

B. parent directory name of a file pathname

C. macros for manipulating CPU sets

D. new process created by a parent process

Correct Answer: D

QUESTION 20

Which term represents the practice of giving employees only those permissions necessary to perform their specific role within an organization?

A. integrity validation

B. due diligence

C. need to know

D. least privilege

Correct Answer: D

QUESTION 21

If a router has four interfaces and each interface is connected to four switches, how many broadcast domains are present on the router?

A. 1

B. 2

C. 4

D. 8

Correct Answer: C

QUESTION 22

Which option is true when using the traffic mirror feature in a switch?

A. Full packet captures are possible

B. Packets are automatically decrypted

C. Ethernet header ate modified before capture

D. Packet payloads are lost

Correct Answer: A

QUESTION 23

Stateful and traditional firewalls can analyze packets and judge them against a set of predetermined rules called access control lists (ACLs). They inspect which of the following elements within a packet? (Choose Two)

A. Session headers

B. NetFlow flow information

C. Source and destination ports and source and destination IP addresses

D. Protocol information

Correct Answer: CD

QUESTION 24

Which Linux terminal command can be used to display all the processes?

A. ps –ef

B. ps –u

C. ps –d

D. ps –m

Correct Answer: A

QUESTION 25

Which definition describes the purpose of a Security Information and Event Management?

A. a database that collects and categorizes indicators of compromise to evaluate and search for potential security threats

B. a monitoring interface that manages firewall access control lists for duplicate firewall filtering

C. a relay server or device that collects then forwards event logs to another log collection device

D. a security product that collects, normalizes, and correlates event log data to provide holistic views of the security posture

Correct Answer: D

QUESTION 26

Which security principle states that more than one person is required to perform a critical task?

A. due diligence

B. separation of duties

C. need to know

D. least privilege

Correct Answer: B

QUESTION 27

Which protocol is expected to have NTP a user agent, host, and referrer headers in a packet capture?

A. NTP

B. HTTP

C. DNS

D. SSH

Correct Answer: B

QUESTION 28

Which statement about the difference between a denial-of-service attack and a distributed denial-of service attack is true?

A. dos attacks only use flooding to compromise a network, and DDOS attacks m=only use other methods?

B. Dos attacks are launched from one host, and DDOS attacks are lunched from multiple hosts.

C. Dos attacks are lunched from one host, and DDOS attacks are lunched from multiple hosts

D. DDos attacks are lunched from one host, and DOS attacks are lunched from multiple hosts

E. Dos attacks and DDOS attacks have no differences?

Correct Answer: B

QUESTION 29

Which evasion method servers as an important functionality of ransomware?

A. Encoding

B. Encryption

C. Resource exhaustion

D. Extended sleep calls

Correct Answer: B

QUESTION 30

Which encryption algorithm is the strongest?

A. AES

B. CES

C. DES

D. 3DES

Correct Answer: A

210-250 PDF Dumps   210-250 Exam Questions   210-250 Braindumps

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

One Year Free Update
Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee
To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy
We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.