Cisco.Premium.210-250.by.VCEplus.120q

Number: 210-250 VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 5.9

Exam Code: 210-250
Exam Name:Understanding Cisco Cybersecurity Fundamentals
Certification Provider: Cisco
Corresponding Certification: CCNA Cyber Ops
Website: www.vceplus.com
Free Exam: https://vceplus.com/ccna-exam-210-250-secfnd/
Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in 210-250 exam products and you get latest questions. We strive to deliver the best 210-250 exam product for top grades in your first attempt.

VCE to PDF Converter : https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus
Google+ : https://plus.google.com/+Vcepluscom
LinkedIn : https://www.linkedin.com/company/vceplus

Exam A

QUESTION 1
Which definition of a process in Windows is true?

A. running program
B. unit of execution that must be manually scheduled by the application
C. database that stores low-level settings for the OS and for certain applications
D. basic unit to which the operating system allocates processor time

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which definition of permissions in Linux is true?

A. rules that allow network traffic to go in and out
B. table maintenance program
C. written affidavit that you have to sign before using the system
D. attributes of ownership and control of an object

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which hashing algorithm is the least secure?

A. MD5
B. RC4
C. SHA-3
D. SHA-2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which definition of a daemon on Linux is true?

A. error check right after the call to fork a process
B. new process created by duplicating the calling process
C. program that runs unobtrusively in the background
D. set of basic CPU instructions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6

Which definition of vulnerability is true?

A. an exploitable unpatched and unmitigated weakness in software
B. an incompatible piece of software
C. software that does not have the most current patch applied
D. software that was not approved for installation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which option is an advantage to using network-based anti-virus versus host-based anti- virus?

A. Network-based has the ability to protect unmanaged devices and unsupported operating systems.
B. There are no advantages compared to host-based antivirus.
C. Host-based antivirus does not have the ability to collect newly created signatures.
D. Network-based can protect against infection from malicious files at rest.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which evasion method involves performing actions slower than normal to prevent detection?

A. traffic fragmentation
B. tunneling
C. timing attack
D. resource exhaustion

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which event occurs when a signature-based IDS encounters network traffic that triggers an alert?

A. connection event
B. endpoint event
C. NetFlow event
D. intrusion event

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which data can be obtained using NetFlow?

A. session data
B. application logs
C. network downtime
D. report full packet capture

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

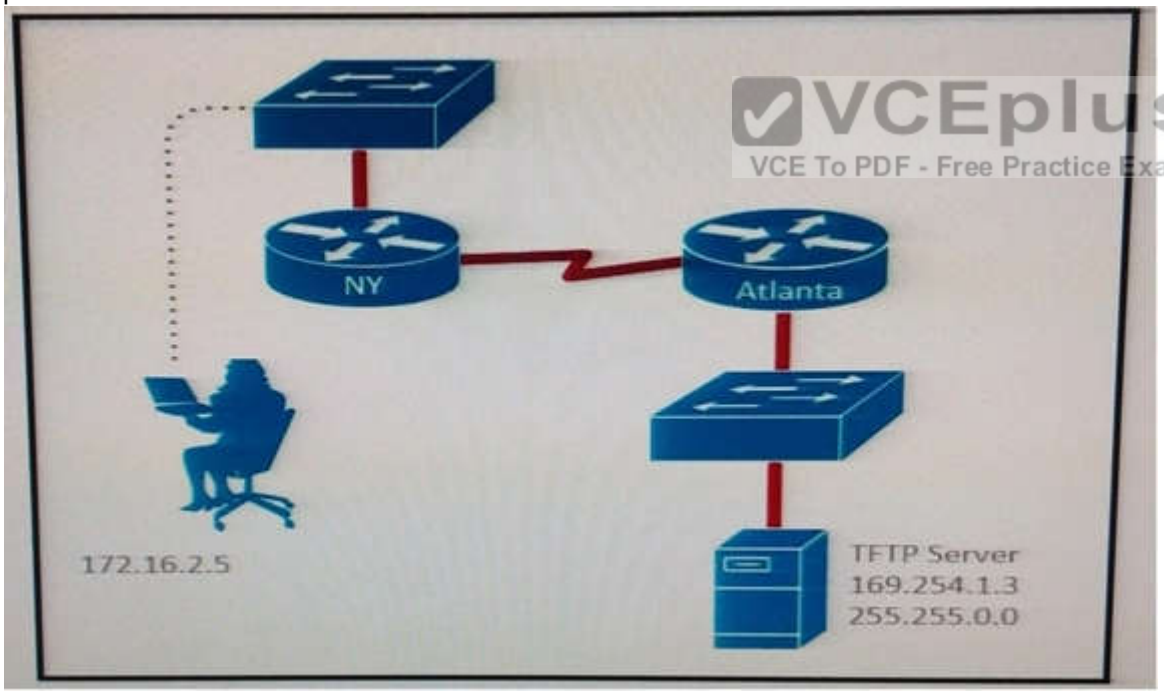
QUESTION 11
Which term describes the act of a user, without authority or permission, obtaining rights on a system, beyond what were assigned?

A. authentication tunneling
B. administrative abuse
C. rights exploitation
D. privilege escalation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Refer to the exhibit. A TFTP server has recently been installed in the Atlanta office. The network administrator is located in the NY office and has attempted to make a connection to the TFTP server. They are unable to backup the configuration file and Cisco IOS of the NY router to the TFTP server Which cause of this problem is true?



A. The TFTP server cannot obtain an address from a DHCP Server.
B. The TFTP server has an incorrect IP address.
C. The network administrator computer has an incorrect IP address
D. The TFTP server has an incorrect subnet mask.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
If a host cannot obtain an IP address from a DHCP server, it automatically assigns itself an Automatic Private IP Addressing (APIPA) IP address until a DHCP server becomes available. The IP address range is 169.254.0.1 through 169.254.255.254.

QUESTION 13
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: C
Section: (none)
Explanation

Explanation/Reference:
A threat is any potential danger to assets. An exploit is a method of leveraging a vulnerability to do harm.

QUESTION 14
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
Section: (none)

Explanation

Explanation/Reference:

QUESTION 15
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
In computer security, which information is the term PHI used to describe?

A. private host information
B. protected health information
C. personal health information
D. protected host information

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which security monitoring data type requires the most storage space?

A. full packet capture

B. transaction data
C. statistical data
D. session data

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which type of exploit normally requires the culprit to have prior access to the target system?

A. local exploit
B. denial of service
C. system vulnerability
D. remote exploit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which identifier is used to describe the application or process that submitted a log message?

A. action
B. selector
C. priority
D. facility

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which concern is important when monitoring NTP servers for abnormal levels of traffic?

A. Being the cause of a distributed reflection denial of service attack.
B. Users changing the time settings on their systems.
C. A critical server may not have the correct time synchronized.
D. Watching for rogue devices that have been added to the network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which protocol is primarily supported by the third layer of the Open Systems Interconnection reference model?

A. HTTP/TLS
B. IPv4/IPv6
C. TCP/UDP
D. ATM/ MPLS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A firewall requires deep packet inspection to evaluate which layer?

A. application
B. Internet
C. link
D. transport

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which two protocols are used for email (Choose two)

A. NTP
B. DNS
C. HTTP
D. IMAP
E. SMTP

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which two options are recognized forms of phishing? (Choose two)

A. spear
B. whaling
C. mailbomb
D. hooking
E. mailnet

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
While viewing packet capture data, you notice that one IP is sending and receiving traffic for multiple devices by modifying the IP header, Which option is making this behavior possible?

A. TOR
B. NAT
C. encapsulation
D. tunneling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which definition of an antivirus program is true?

A. program used to detect and remove unwanted malicious software from the system
B. program that provides real time analysis of security alerts generated by network hardware and application
C. program that scans a running application for vulnerabilities
D. rules that allow network traffic to go in and out

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IPS phones?

A. replay
B. man-in-the-middle
C. dictionary
D. known-plaintext

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
An intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources. Which evasion technique does this attempt indicate?

A. traffic fragmentation
B. resource exhaustion
C. timing attack
D. tunneling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which type of attack occurs when an attacker utilizes a botnet to reflect requests off an NTP server to overwhelm their target?

A. man in the middle
B. denial of service
C. distributed denial of service
D. replay

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
In NetFlow records, which flags indicate that an HTTP connection was stopped by a security appliance, like a firewall, before it could be built fully?

A. ACK
B. SYN ACK
C. RST
D. PSH, ACK

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
When a connection is stopped by a security appliance it will send an RST flag.

QUESTION 31
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
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: BC
Section: (none)
Explanation

Explanation/Reference:
The purpose of PKI is the secure distribution of public keys. It helps answer three (3) questions to authenticate a certificate. Is it valid, is it signed and is it revoked.

QUESTION 33
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which network device is used to separate broadcast domains?

A. router
B. repeater
C. switch
D. bridge

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: