Cisco.210-255.v2018-06-05.q62

Exam Code:	210-255
Exam Name:	Implementing Cisco Cybersecurity Operations
Certification Provider:	Cisco
Free Question Number:	62
Version:	v2018-06-05
# of views:	1597
# of Questions views:	45717
https://www.freecram.net/torrent/Cisco.210-255.v2018-06-05.q62.html	

NEW QUESTION: 1
Which two options can be used by a threat actor to determine the role of a server? (Choose two.)
A. PCAP
B. tracert
C. running processes
D. hard drive configuration
E. applications
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 2
Which type of analysis assigns values to scenarios to see what the outcome might be in each scenario?
A. deterministic
B. exploratory
C. probabilistic
D. descriptive
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 3
Refer to the exhibit. What can be determined from this ping result?
A. The public IP address of cisco.com is 2001:420:1101:1::a.
B. The Cisco.com website is down.
C. The Cisco.com website is responding with an internal IP.

D. The public IP address of cisco.com is an IPv4 address.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 4
Which element is included in an incident response plan?
A. organization mission
B. junior analyst approval
C. day-to-day firefighting
D. siloed approach to communications
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 5
Which option is generated when a file is run through an algorithm and generates a string specific to the contents of that file?
A. URL
B. hash
C. IP address
D. destination port
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 6
In the context of incident handling phases, which two activities fall under scoping? (Choose two.)
A. determining the number of attackers that are associated with a security incident
B. ascertaining the number and types of vulnerabilities on your network
C. identifying the extent that a security incident is impacting protected resources on the network
D. determining what and how much data may have been affected
E. identifying the attackers that are associated with a security incident
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 7
From a security perspective, why is it important to employ a clock synchronization protocol on a network?
A. so that everyone knows the local time

B. to ensure employees adhere to work schedule
C. to construct an accurate timeline of events when responding to an incident
D. to guarantee that updates are pushed out according to schedule
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 8
A user on your network receives an email in their mailbox that contains a malicious attachment. There is no indication that the file was run. Which category as defined in the Diamond Model of Intrusion does this activity fall under?
A. reconnaissance
B. weaponization
C. delivery
D. installation
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The methodology meta-feature allows an analyst to describe the general class of activity, for example:
spear-phish email, content-delivery attack, syn flood, port scan, etc. As with other feature types, this also allows more than one definition as necessary. For instance, a malicious spear-phishing email with malware attached may be categorized as both a "spear-phish email" and a "content-delivery attack".

NEW QUESTION: 9
DRAG DROP
Drag and drop the elements of incident handling from the left into the correct order on the right.
Select and Place:
Answer:
Explanation/Reference:
Reference: https://countuponsecurity.com/2012/12/21/computer-security-incident-handling-6-steps/

NEW QUESTION: 10
Which option can be addressed when using retrospective security techniques?
A. if the affected host needs a software update
B. how the malware entered our network
C. why the malware is still in our network
D. if the affected system needs replacement
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:

NEW QUESTION: 11
Refer to the exhibit. Which application protocol is in this PCAP file?
A. TCP
B. SSH
C. HTTP
D. SSL
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 12
Which information must be left out of a final incident report?
A. server hardware configurations
B. exploit or vulnerability used
C. impact and/or the financial loss
D. how the incident was detected
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 13
Which description of a retrospective malware detection is true?
A. You use Wireshark to identify the malware source.
B. You use historical information from one or more sources to identify the affected host or file.
C. You use information from a network analyzer to identify the malware source.
D. You use Wireshark to identify the affected host or file.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 14
What information from HTTP logs can be used to find a threat actor?
A. referer
B. IP address
C. user-agent
D. URL
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 15
During which phase of the forensic process are tools and techniques used to extract the relevant information from the collective data?
A. examination
B. reporting
C. collection
D. investigation
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference:http://resources.infosecinstitute.com/computer-forensics-investigation-case-study/#gref

NEW QUESTION: 16
Which two components are included in a 5-tuple? (Choose two.)
A. port number
B. destination IP address
C. data packet
D. user name
E. host logs
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A 5-tuple refers to a set of five different values that comprise a Transmission Control Protocol/Internet Protocol (TCP/IP) connection. It includes a source IP address/port number, destination IP address/port number and the protocol in use.

NEW QUESTION: 17
Which CVSSv3 metric value increases when the attacker is able to modify all files protected by the vulnerable component?
A. confidentiality
B. integrity

C. availability
D. complexity
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
There is a total loss of integrity, or a complete loss of protection. For example, the attacker is able to modify any/all files protected by the impacted component. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.

NEW QUESTION: 18
What is accomplished in the identification phase of incident handling?
A. determining the responsible user
B. identifying source and destination IP addresses
C. defining the limits of your authority related to a security event
D. determining that a security even has occurred
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
In the identification phase you need to work out whether you are dealing with an event or an incident. This is where understanding your environment is critical as it means looking for significant deviations from
"normal" traffic baselines or other methods.

NEW QUESTION: 19
Which option filters a LibPCAP capture that used a host as a gateway?
A. [tcp|udp] [src|dst] port <port>
B. [src|dst] net <net> [{mask <mask>}|{len <len>}]
C. ether [src|dst] host <ehost>
D. gateway host <host>
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference:https://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html

NEW QUESTION: 20
Which source provides reports of vulnerabilities in software and hardware to a Security Operations Center?

A. Analysis Center
B. National CSIRT
C. Internal CSIRT

D. Physical Security
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Some general categories of CSIRTs include, but are not limited to, the following:
Internal CSIRTs provide incident handling services to their parent organization. This could be a CSIRT
for a bank, a manufacturing company, a university, or a federal agency.
National CSIRTs provide incident handling services to a country. Examples include: the Japan CERT Coordination Center (JPCERT/CC) or the Singapore Computer Emergency Response Team (SingCERT).
Coordination Centers coordinate and facilitate the handling of incidents across various CSIRTs. Examples include the CERT Coordination Center or the United States Computer Emergency Readiness Team (US-CERT).
Analysis Centers focus on synthesizing data from various sources to determine trends and patterns in
incident activity. This information can be used to help predict future activity or to provide early warning when the activity matches a set of previously determined characteristics.
Vendor Teams handle reports of vulnerabilities in their software or hardware products. They may work
within the organization to determine if their products are vulnerable and to develop remediation and mitigation strategies. A vendor team may also be the internal CSIRT for a vendor organization.
Incident Response Providers offer incident handling services as a for-fee service to other organizations.

NEW QUESTION: 21
Which identifies both the source and destination location?
A. IP address
B. URL
C. ports
D. MAC address
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 22
Refer to the exhibit. You notice that the email volume history has been abnormally high. Which potential result is true?
A. Email sent from your domain might be filtered by the recipient.
B. Messages sent to your domain may be queued up until traffic dies down.

C. Several hosts in your network may be compromised.
D. Packets may be dropped due to network congestion.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 23
Which option creates a display filter on Wireshark on a host IP address or name?
A. ip.address == <address> or ip.network == <network>
B. [tcp|udp] ip.[src|dst] port <port>
C. ip.addr == <addr> or ip.name == <name>
D. ip.addr == <addr> or ip.host == <host>
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 24
Which two HTTP header fields relate to intrusion analysis? (Choose two.)
A. user-agent
B. host
C. connection
D. language
E. handshake type
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 25
An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group. Which term defines the initial event in the NIST SP800-61 r2?
A. instigator
B. precursor
C. online assault
D. trigger
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Signs of an incident fall into one of two categories: precursors and indicators. A precursor is a sign that an incident may occur in the future. An indicator is a sign that an incident may have occurred or may be occurring now.
Reference: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NEW QUESTION: 26
What mechanism does the Linux operating system provide to control access to files?
A. privileges required
B. user interaction
C. file permissions
D. access complexity
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 27
Which regular expression matches "color" and "colour"?
A. col[0-9]+our
B. colo?ur
C. colou?r
D. [a-z]{7}
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference:http://www.regular-expressions.info/quickstart.html

NEW QUESTION: 28
Which process is being utilized when IPS events are removed to improve data integrity?
A. data normalization
B. data availability
C. data protection
D. data signature
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 29
Which CVSSv3 Attack Vector metric value requires the attacker to physically touch or manipulate the vulnerable component?
A. local
B. physical
C. network
D. adjacent
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:

NEW QUESTION: 30

Which element can be used by a threat actor to discover a possible opening into a target network and can also be used by an analyst to determine the protocol of the malicious traffic?

A. TTLs
B. ports
C. SMTP replies
D. IP addresses
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 31

You see confidential data being exfiltrated to an IP address that is attributed to a known Advanced Persistent Threat group. Assume that this is part of a real attack and not a network misconfiguration. Which category does this event fall under as defined in the Diamond Model of Intrusion?

A. reconnaissance
B. weaponization
C. delivery
D. action on objectives
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 32

Refer to the exhibit. We have performed a malware detection on the Cisco website. Which statement about the result is true?

A. The website has been marked benign on all 68 checks.
B. The threat detection needs to run again.
C. The website has 68 open threats.
D. The website has been marked benign on 0 checks.

Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Example:https://www.virustotal.com/en/url/
df05d8e27bd760c33dc709951a5840cc6578d78d544d869890b7b94ea21e46b0/analysis/1368183553/

NEW QUESTION: 33
In Microsoft Windows, as files are deleted the space they were allocated eventually is considered available for use by other files. This creates alternating used and unused areas of various sizes. What is this called?
A. network file storing
B. free space fragmentation
C. alternate data streaming
D. defragmentation
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 34
Which stakeholder group is responsible for containment, eradication, and recovery in incident handling?
A. facilitators
B. practitioners
C. leaders and managers
D. decision makers
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NEW QUESTION: 35
DRAG DROP
Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.
Select and Place:
Answer:

NEW QUESTION: 36
Which network device creates and sends the initial packet of a session?
A. source
B. origination

C. destination
D. network
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 37
DRAG DROP
Drag and drop the type of evidence from the left onto the correct description(s) of that evidence on the right.
Select and Place:
Answer:

NEW QUESTION: 38
You have run a suspicious file in a sandbox analysis tool to see what the file does. The analysis report shows that outbound callouts were made post infection. Which two pieces of information from the analysis report are needed or required to investigate the callouts? (Choose two.)
A. file size
B. domain names
C. dropped files
D. signatures
E. host IP addresses
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference:https://digital-forensics.sans.org/blog/2012/07/26/four-focus-areas-of-malware-analysis

NEW QUESTION: 39
You see 100 HTTP GET and POST requests for various pages on one of your webservers. The user agent in the requests contain php code that, if executed, creates and writes to a new php file on the webserver.
Which category does this event fall under as defined in the Diamond Model of Intrusion?
A. delivery
B. reconnaissance
C. action on objectives
D. installation
E. exploitation
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 40
DRAG DROP
Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the NetFlow v5r record from a security event on the right.
Select and Place:
Answer:

NEW QUESTION: 41
During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?
A. collection
B. examination
C. reporting
D. investigation
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The basic phases of the forensic process are: collection, examination, analysis, and reporting. During collection, data related to a specific event is identified, labeled, recorded, and collected, and its integrity is preserved. In the second phase, examination, forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity. Examination may use a combination of automated tools and manual processes. The next phase, analysis, involves analyzing the results of the examination to derive useful information that addresses the questions that were the impetus for performing the collection and examination. The final phase involves reporting the results of the analysis, which may include describing the actions performed, determining what other actions need to be performed, and recommending improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process.
Reference:http://itlaw.wikia.com/wiki/Forensic_process

NEW QUESTION: 42
Which type of analysis allows you to see how likely an exploit could affect your network?
A. descriptive
B. casual
C. probabilistic
D. inferential
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference:https://www.owasp.org/index.php/Application_Threat_Modeling#Threat_Analysis

NEW QUESTION: 43

Which option has a drastic impact on network traffic because it can cause legitimate traffic to be blocked?

A. true positive

B. true negative

C. false positive

D. false negative

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

A false positive is basically when a legitimate user generates the protection system and in response that visitor appears as an attacker. In this situation, the legitimate user is restricted to visit the website which would eventually lead towards losing the customers or clients.

NEW QUESTION: 44

Which data element must be protected with regards to PCI?

A. past health condition

B. geographic location

C. full name

D. recent payment amount

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 45

Which feature is used to find possible vulnerable services running on a server?

A. CPU utilization

B. security policy

C. temporary internet files

D. listening ports

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

A vulnerability that occurs because under certain circumstances Internet Explorer does not correctly check the component that the OBJECT tag calls. This could allow an attacker to obtain the name of the Temporary Internet Files folder on the user's local machine. The vulnerability would not allow an attacker to read or modify any files on the user's local system, since the Temporary Internet Files folder resides in the Internet security zone. Knowledge of the name of the Temporary Internet Files folder could allow an attacker to identify the username of the logged-on user and read other information in the Temporary Internet Files folder such as cookies.

NEW QUESTION: 46

Refer to the exhibit. A customer reports that they cannot access your organization's website. Which option is a possible reason that the customer cannot access the website?
A. The server at 10.33.1.5 is using up too much bandwidth causing a denial-of-service.
B. The server at 10.67.10.5 has a virus.
C. A vulnerability scanner has shown that 10.67.10.5 has been compromised.
D. Web traffic sent from 10.67.10.5 has been identified as malicious by Internet sensors.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Every firewall has its own database where it maintains the website reputation on terms of security, ease of access, performance etc and below certain score (generally 7 in case of Cisco), firewalls block access to the sites. For example, you can visit www.senderbase.org and enter name of any website and you will see the reputation of that website.

NEW QUESTION: 47
Which data type is protected under the PCI compliance framework?
A. credit card type
B. primary account number
C. health conditions
D. provision of individual care
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The goal of the PCI Data Security Standard (PCI DSS) is to protect cardholder data wherever it is processed, stored or transmitted. The security controls and processes required byPCI DSS are vitalfor protecting cardholder account data, including the PAN - the primary account number printed on the front of a payment card.
Reference:https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

NEW QUESTION: 48
Which CVSSv3 metric captures the level of access that is required for a successful attack?

A. attack vector
B. attack complexity
C. privileges required
D. user interaction
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The new metric, Privileges Required, replaces the Authentication metric of v2.0. Instead of measuring thenumber of timesan attacker must separately authenticate to a system, Privileges Requiredcaptures thelevel of accessrequired for a successful attack. Specifically, the metric values High, Low, and None reflect the privileges required by an attacker in order to exploit the vulnerability.
Reference:https://www.first.org/cvss/cvss-v30-user_guide_v1.4.pdf

NEW QUESTION: 49
Which option is a misuse variety per VERIS enumerations?
A. snooping
B. hacking
C. theft
D. assault
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 50
When performing threat hunting against a DNS server, which traffic toward the affected domain is considered a starting point?

A. HTTPS traffic
B. TCP traffic
C. HTTP traffic
D. UDP traffic
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 51
Which element is part of an incident response plan?
A. organizational approach to incident response
B. organizational approach to security
C. disaster recovery
D. backups
Answer: (SHOW ANSWER)

Explanation/Reference:
Explanation:

NEW QUESTION: 52
Which statement about threat actors is true?
A. They are any company assets that are threatened.
B. They are any assets that are threatened.
C. They are perpetrators of attacks.
D. They are victims of attacks.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 53
Which CVSSv3 metric value increases when attacks consume network bandwidth, processor cycles, or disk space?
A. confidentiality
B. integrity
C. availability
D. complexity
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 54
A CMS plugin creates two filters that are accessible from the Internet: myplugin.html and exploitable.php. A newly discovered exploit takes advantage of an injection vulnerability in exploitable.php. To exploit the vulnerability, one must send an HTTP POST with specific variables to exploitable.php. You see traffic to your webserver that consists of only HTTP GET requests to myplugin.html. Which category best describes this activity?
A. weaponization
B. exploitation
C. installation
D. reconnaissance
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 55
Which option allows a file to be extracted from a TCP stream within Wireshark?
A. File > Export Objects

B. Analyze > Extract
C. Tools > Export > TCP
D. View > Extract
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 56
Refer to the exhibit. Which type of log is this an example of?
A. syslog
B. NetFlow log
C. proxy log
D. IDS log
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 57
You receive an alert for malicious code that exploits Internet Explorer and runs arbitrary code on the site visitor machine. The malicious code is on an external site that is being visited by hosts on your network.
Which user agent in the HTTP headers in the requests from your internal hosts warrants further investigation?
A. Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Trident 6.0)
B. Mozilla/5.0 (XII; Linux i686; rv: 1.9.2.20) Gecko/20110805
C. Mozilla/5.0 (Windows NT 6.1; WOW64; rv:400) Gecko/20100101
D. Opera/9.80 (XII; Linux i686; Ubuntu/14.10) Presto/2.12.388 Version/12.16
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 58
In VERIS, an incident is viewed as a series of events that adversely affects the information assets of an organization. Which option contains the elements that every event is comprised of according to VERIS incident model?
A. victim demographics, incident description, incident details, discovery & response
B. victim demographics, incident details, indicators of compromise, impact assessment
C. actors, attributes, impact, remediation
D. actors, actions, assets, attributes
Answer: (SHOW ANSWER)
Explanation/Reference:

Reference: https://github.com/vz-risk/veris/wiki/VERIS-Overview

NEW QUESTION: 59
Refer to the exhibit. Which type of log is this an example of?
A. IDS log
B. proxy log
C. NetFlow log
D. syslog
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference:http://stackoverflow.com/questions/14591741/timestamps-on-netflow

NEW QUESTION: 60
Which component of the NIST SP800-61 r2 incident handling strategy reviews data?
A. preparation
B. detection and analysis
C. containment, eradication, and recovery
D. post-incident analysis
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference:http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NEW QUESTION: 61
Refer to the exhibit. Which packet contains a file that is extractable within Wireshark?
A. 1986
B. 2318
C. 2542
D. 2317
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 62
Which goal of data normalization is true?
A. Reduce data redundancy.
B. Increase data redundancy.
C. Reduce data availability.
D. Increase data availability.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
normalization, is the process of organizing the columns (attributes) and tables (relations) of a relational database to reduce dataredundancy and improve data integrity.