Cisco.210-255.v2019-11-01.q55

Exam Code:	210-255
Exam Name:	Implementing Cisco Cybersecurity Operations
Certification Provider:	Cisco
Free Question Number:	55
Version:	v2019-11-01
# of views:	779
# of Questions views:	15164
https://www.freecram.net/torrent/Cisco.210-255.v2019-11-01.q55.html	

NEW QUESTION: 1
Which of the following are not components of the 5-tuple of a flow in NetFlow? (Select all that apply.)
A. Gateway
B. Source port
C. Destination port
D. Flow record ID
E. Source IP address
Answer: (SHOW ANSWER)

NEW QUESTION: 2
What is Data mapping used for? (Choose two)
A. data accuracy (integrity)
B. data normalization
C. data visualisation
D. data confidentiality
E. data availability
Answer: (SHOW ANSWER)

NEW QUESTION: 3
When performing threat hunting against a DNS server, which traffic toward the affected domain is considered a starting point?
A. HTTP traffic
B. HTTPS traffic
C. UDP traffic
D. TCP traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 4
In addition to cybercrime and attacks, evidence found on a system or network may be presented in a court of law to support accusations of crime or civil action, including which of the following?
A. All of the above
B. Drug-related crime
C. Fraud, money laundering, and theft
D. Murder and acts of violence
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which regular expression matches "color" and "colour"?
A. col[0-9]+our
B.]a-z]{7}
C. colo?ur
D. colou?r
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Which option is the process of remediating the network and systems and/or reconstructing the attack so that the responsible threat actor can be revealed?
A. data analytics
B. evidence collection
C. threat actor attribution
D. asset attribution
Answer: (SHOW ANSWER)

NEW QUESTION: 7
What is the difference between deterministic and probabilistic assessment method?
A. At deterministic method we know the facts beforehand and at probabilistic method we make assumptions
B. At probabilistic method we know the facts beforehand and at deterministic method we make assumptions
C. Probabilistic method has an absolute nature
D. Determinist method has an absolute nature
Answer: (SHOW ANSWER)

NEW QUESTION: 8
Which string matches the regular expression r(ege)+x?
A. r(ege)x
B. regeegex

C. rege+x

D. rx

Answer: (SHOW ANSWER)

NEW QUESTION: 9

Which data element must be protected with regards to PCI?

A. full name

B. geographic location

C. recent payment amount

D. past health condition

Answer: A (LEAVE A REPLY)

NEW QUESTION: 10

Refer to the exhibit. Which packet contains a file that is extractable within Wireshark?

No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14404 ACK=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522-80 [ACK] Seq=2987 ACK=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/1/ntpagetag.gif?js=1&ts=1476292607552.2866tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14593 ACK=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14593 ACK=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14593 ACK=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522-80 [ACK] Seq=6871 ACK=14979 Win=62480 Len=0

A. 2317

B. 1986

C. 2318

D. 2542

Answer: (SHOW ANSWER)

NEW QUESTION: 11

What is the common artifact that is used to uniquely identify a detected file?

A. Timestamp

B. Hash

C. File size

Answer: (SHOW ANSWER)

NEW QUESTION: 12

Which statement about collecting data evidence when performing digital forensics is true?

A. Not allowing items of evidence to be physically touch

B. Allowing unrestricted access to impacted devices

C. Powering off the device after collecting the data

D. It must be preserved and integrity checked

Answer: D (LEAVE A REPLY)

NEW QUESTION: 13

Which type of analysis allows you to see how likely an exploit could affect your network?

A. probabilistic

B. inferential

C. casual

D. descriptive

Answer: (SHOW ANSWER)

NEW QUESTION: 14

Which expression creates a filter on a host IP address or name?

A. gateway host <host>

B. [src|dst] host <host host >

C. [tcp|udp] [src|dst] port<port>

D. ether [src|dst] host<ehost>

Answer: (SHOW ANSWER)

NEW QUESTION: 15

What is the process of remediation the network and systems and/or reconstructing so the responsible threat actor can be revealed?

A. Threat actor distribution

B. Data analysis

C. Assets distribution

D. Evidence collection

Answer: (SHOW ANSWER)

NEW QUESTION: 16

Which type of analysis allows you to see how likely an exploit could affect your network?

A. probabilistic

B. casual

C. descriptive

D. inferential

Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which information must be left out of a final incident report?
A. exploit or vulnerability used
B. server hardware configurations
C. impact and/or the financial loss
D. how the incident was detected
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which description of deterministic analysis is true?
A. lack of proof of a user's identity
B. definitive proof of a user's identity
C. probable proof of a user's identity
D. false proof of a user's identity
Answer: (SHOW ANSWER)

NEW QUESTION: 19
What is accomplished in the identification phase of incident handling?
A. identifying source and destination IP addresses
B. determining the responsible user
C. determining that a security event has occurred
D. defining the limits of your authority related to a security event
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which of the following is not a metadata feature of the Diamond Model?
A. Devices
B. Result
C. Resources
D. Direction
Answer: (SHOW ANSWER)

NEW QUESTION: 21

Which of the following are examples of Linux boot loaders?
A. GRUB
B. ILOS
C. LILO
D. Ubuntu BootPro
Answer: (SHOW ANSWER)

NEW QUESTION: 22
Which process is being utilized when IPS events are removed to improve data integrity?
A. data availability
B. data signature
C. data normalization
D. data protection
Answer: (SHOW ANSWER)

NEW QUESTION: 23
How is confidentiality defined in the CVSS v3.0 framework?
A. confidentiality of the information resource managed by a person due to a successfully vulnerability
B. confidentiality of the information resource managed by person due to an unsuccessfully exploited vulnerability
C. confidentiality of the information resource managed by a software component due to an unsuccessfully exploited vulnerability
D. confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24
Which of the following is one of the main goals of the CSIRT?
A. To configure the organization's firewalls
B. To monitor the organization's IPS devices
C. To minimize and control the damage associated with incidents, provide guidance for mitigation, and work to prevent future incidents
D. To hire security professionals who will be part of the InfoSec team of the organization.
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which CVSS metric describes the conditions that are beyond the attacker's control that must be exist to exploit the vulnerability?
A. privileges required
B. user interaction

C. attack vector
D. attack complexity
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Which concept is used to understand instances of the same cybersecurity event occurring over the course of a few weeks that could be linked together through multiple illustrations and then linked back to the same adversary?
A. threat model
B. diamond model of intrusion
C. intrusion threat intelligence model
D. compliance and Intrusion model
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Drag and Drop Question

sIP	dIP	sPort	dPort	pro	packets	bytes	flags	sTime	duration		eTime
10.232.38.20	208.100.26.233	80	39613	6	60	3120	A	2016/10/09T00:09:43.112	1774.708	2016/10/09T00:39:17.820	

Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the NetFlow v5 record from a security event on the right.

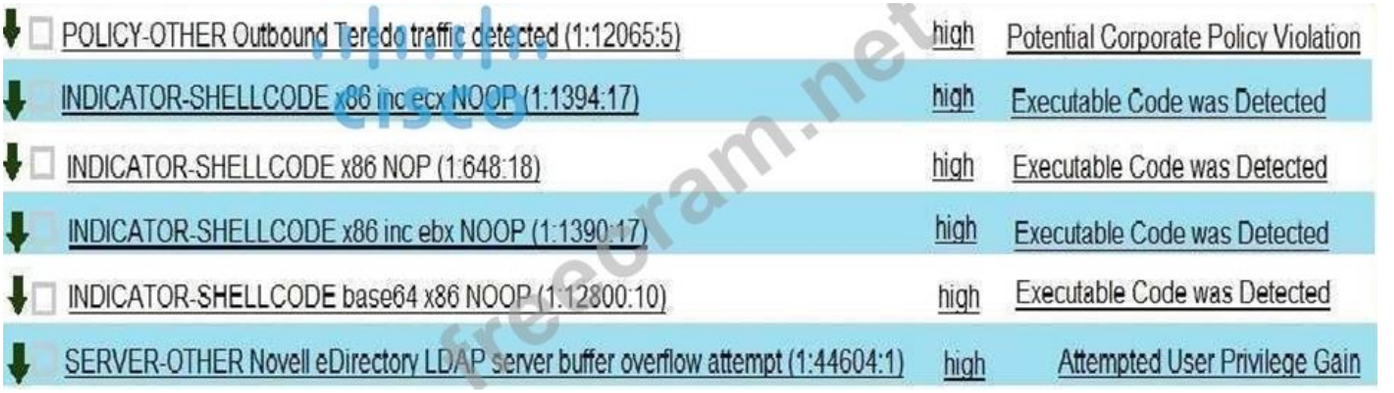
Answer:

NEW QUESTION: 28
Which description of a retrospective malware detection is true?
A. You use historical information from one or more sources to identify the affected host or file.
B. You use information from a network analyzer to identify the malware source.
C. You use Wireshark to identify the affected host or file.
D. You use Wireshark to identify the malware source.
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Which option is unnecessary for determining the appropriate containment strategy according to NIST.SP800-61 r2?
A. effectiveness of the strategy
B. need for evidence preservation
C. time and resource needed to implement the strategy
D. attack vector used to compromise the system
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Which type of intrusion event is an attacker retrieving the robots. txt file from target site?
A. exploitation
B. weaponization
C. scanning
D. reconnaissance
Answer: D (LEAVE A REPLY)

NEW QUESTION: 31
Refer to exhibit. Which option is the logical source device for these events?



A. proxy server
B. NetFlow collector
C. web server
D. IDS/IPS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 32
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. trigger
C. precursor
D. online assault
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which two components are included in a 5-tuple? (Choose two.)
A. host logs
B. destination IP address
C. data packet
D. port number
E. user name
Answer: (SHOW ANSWER)

NEW QUESTION: 34
Filtering ports in wireshark?
A. tcp.port 80
B. tcp.port == 80
C. port 80
D. tcp port equals 80
Answer: B (LEAVE A REPLY)

NEW QUESTION: 35
What are the metric values for confidentiality impact in the CVSS v3.0 framework?
A. open, closed, obsolete
B. high, medium, none
C. high, low
D. high, low, none
Answer: D (LEAVE A REPLY)

NEW QUESTION: 36
You have a video of a suspect entering a data center that was captured on the same that files in the same data center were transferred to a computer. Which type of is this?
A. indirect evidence
B. prima faice evidence
C. Physical evidence
D. best evidence
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which analyzing technique describe the outcome as well as how likely each outcome is?
A. probabilistic
B. exploratory
C. deterministic
D. descriptive
Answer: (SHOW ANSWER)

NEW QUESTION: 38
The united State CERT provides cybersecurity protection to Federal, civilian, and executive branch agencies through intrusion detection and prevention capabilities. Which type of incident response team is this an example of?
A. National CSIRT
B. National PSIRT
C. Federal PSIRT
D. Federal CSIRT

Answer: (SHOW ANSWER)

NEW QUESTION: 39
Which option is a misuse variety per VERIS enumerations?
A. assault
B. hacking
C. theft
D. snooping
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which of the following is true about journaling?
A. The journal is the most used part of the disk, making the blocks that form part of it less prone to hardware failure.
B. The journal is the least used part of the disk, making the blocks that form part of it less prone to hardware failure.
C. The journal is the least used part of the disk, making the blocks that form part of it more prone to hardware failure.
D. The journal is the most used part of the disk, making the blocks that form part of it more prone to hardware failure.
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which identifies both the source and destination location?
A. ports
B. IP address
C. MAC address
D. URL
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Which of the following are core responsibilities of a national CSIRT and CERT?
A. Provide solutions for bug bounties
B. Provide vulnerability brokering to vendors within a country
C. Create regulations around cybersecurity within the country
D. Protect their citizens by providing security vulnerability information, security awareness training, best practices, and other information
Answer: (SHOW ANSWER)

NEW QUESTION: 43
Which of the following is not an example of weaponization?

A. Wrapping software with a RAT
B. Developing an automated script to inject commands on a USB device
C. Creating a backdoor in an application
D. Connecting to a command and control server
Answer: (SHOW ANSWER)

NEW QUESTION: 44
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. identifying the extent that a security incident is impacting protected resources on the network
C. determining what and how much data may have been affected
D. ascertaining the number and types of vulnerabilities on your network
E. identifying the attackers that are associated with a security incident
Answer: (SHOW ANSWER)

NEW QUESTION: 45
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 68 open threats.
B. The website has been marked benign on 0 checks.
C. The threat detection needs to run again.
D. The website has been marked benign on all 68 checks.
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Which feature is used to find possible vulnerable services running on a server?
A. security policy
B. temporary internet files
C. listening ports
D. CPU utilization
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Which CVSS Attach Vector metric value means that the vulnerable component is not bound to the network stack and the path of the attacker is via read/write/execute capabilities?
A. local
B. adjacent
C. physical
D. network
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Which CVSS Attach Vector metric value means that the vulnerable component is not bound to the network stack and the path of the attacker is via read/write/execute capabilities?
A. adjacent
B. physical
C. network
D. local
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which command can be used to find open ports on a system?
A. netstat-g
B. netstat -r
C. netstat -l
D. netstat -v
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Which option is missing a malware variety per VERIS enumerations?
A. packet sniffer, password dumper, scan network
B. abuse of functionality, cache poisoning, remote file inclusion
C. adware, brute force, client-side attack
D. backdoor, command and control, denial or service attack

Answer: (SHOW ANSWER)

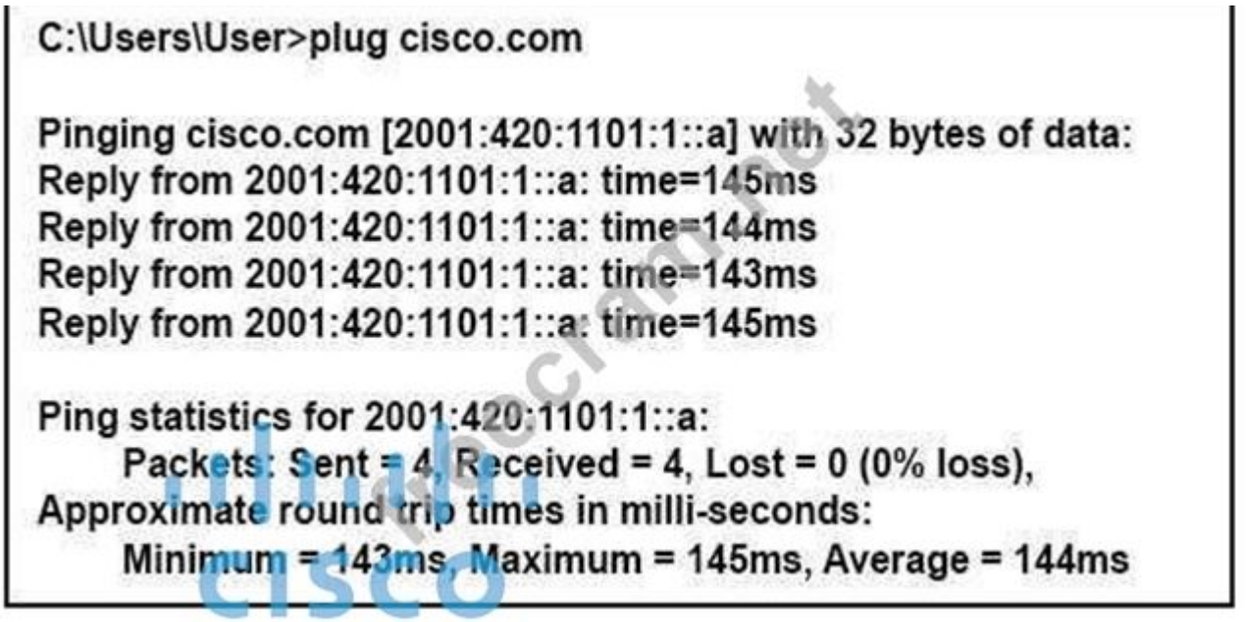
NEW QUESTION: 51
Which option creates a display filter on Wireshark on a host IP address or name?
A. ip.addr == <addr> or ip.host == <host>
B. ip.address == <address> or ip.network == <network>
C. ip.addr == <addr> or ip.name == <name>
D. [tcp|udp] ip.[src|dst] port <port>
Answer: (SHOW ANSWER)

NEW QUESTION: 52
How do you verify that one of your hosts is potentially compromised based on their communication destinations?
A. Search the communication destinations of the host in the Talos IP & Domain Reputation Center.
B. Check the Firepower appliance to see if malicious files were downloaded.
C. Analyze how much traffic the host sent and received from each IP address or domain.
D. See if any Stealthwatch alarms were triggered for the host communicating with internal hosts.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 53
Which filter shows only SMTP and ICMP traffic on Wireshark?
A. tcp.eq 25 or icmp
B. tcp.port eq 25 or icmp
C. tcp.port eq 25 also icmp
D. port eq 25 and icmp
Answer: (SHOW ANSWER)

NEW QUESTION: 54
What information from HTTP logs can be used to find a threat actor?
A. referer
B. user-agent
C. URL
D. IP address
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Refer to the exhibit. What can be determined from this ping result?



A. The public IP address of cisco.com is an IPv4 address.

B. The Cisco.com website is down.

C. The public IP address of cisco.com is 2001:420:1101:1::a.

D. The Cisco.com website is responding with an internal IP.

Answer: (SHOW ANSWER)