Cisco.200-201.v2022-01-19.q100

Exam Code:	200-201
Exam Name:	Understanding Cisco Cybersecurity Operations Fundamentals
Certification Provider:	Cisco
Free Question Number:	100
Version:	v2022-01-19
# of views:	2364
# of Questions views:	1000
https://www.freepdfdumps.com/Cisco.200-201.v2022-01-19.q100.html	

NEW QUESTION: 1
Refer to the exhibit.
What is the potential threat identified in this Stealthwatch dashboard?
A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.
B. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.
C. Host 152.46.6.91 is being identified as a watchlist country for data transfer.
D. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which event is user interaction?
A. reading and writing file permission
B. executing remote code
C. gaining root access
D. opening a malicious file
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?
A. Tapping interrogations detect and block malicious traffic
B. Tapping interrogation replicates signals to a separate port for analyzing traffic
C. Inline interrogation detects malicious traffic but does not block the traffic
D. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
What is the difference between statistical detection and rule-based detection models?
A. Statistical detection involves the evaluation of an object on its intended actions before it executes that behavior
B. Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis
C. Rule-based detection defines legitimate data of users over a period of time and statistical detection defines it on an IF/THEN basis
D. Rule-based detection involves the collection of data in relation to the behavior of legitimate users over a period of time
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
Which attack method intercepts traffic on a switched network?
A. denial of service
B. DHCP snooping
C. command and control
D. ARP cache poisoning
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
Refer to the exhibit.
Which type of log is displayed?
A. IDS
B. proxy
C. NetFlow
D. sys
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
An analyst discovers that a legitimate security alert has been dismissed. Which signature caused this impact on network traffic?
A. true negative
B. false negative
C. true positive
D. false positive
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8
Which security technology allows only a set of pre-approved applications to run on a system?

A. application-level blacklisting
B. antivirus
C. host-based IPS
D. application-level whitelisting
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which attack method intercepts traffic on a switched network?
A. denial of service
B. ARP cache poisoning
C. DHCP snooping
D. command and control
Answer: B (LEAVE A REPLY)
Explanation
An ARP-based MITM attack is achieved when an attacker poisons the ARP cache of two devices with the MAC address of the attacker's network interface card (NIC). Once the ARP caches have been successfully poisoned, each victim device sends all its packets to the attacker when communicating to the other device and puts the attacker in the middle of the communications path between the two victim devices. It allows an attacker to easily monitor all communication between victim devices. The intent is to intercept and view the information being passed between the two victim devices and potentially introduce sessions and traffic between the two victim devices

NEW QUESTION: 10
What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?
A. DAC is the strictest of all levels of control and MAC is object-based access
B. MAC is the strictest of all levels of control and DAC is object-based access
C. DAC is controlled by the operating system and MAC is controlled by an administrator
D. MAC is controlled by the discretion of the owner and DAC is controlled by an administrator
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
What is rule-based detection when compared to statistical detection?
A. likelihood of user's action
B. falsification of a user's identity
C. proof of a user's identity
D. proof of a user's action
Answer: D (LEAVE A REPLY)

NEW QUESTION: 12

While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header.
Which technology makes this behavior possible?
A. NAT
B. encapsulation
C. TOR
D. tunneling
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which event artifact is used to identity HTTP GET requests for a specific file?
A. HTTP status code
B. destination IP address
C. TCP ACK
D. URI
Answer: D (LEAVE A REPLY)

NEW QUESTION: 14
What are the two characteristics of the full packet captures? (Choose two.)
A. Identifying network loops and collision domains.
B. Troubleshooting the cause of security and performance issues.
C. Reassembling fragmented traffic from raw data.
D. Detecting common hardware faults and identify faulty assets.
E. Providing a historical record of a network transaction.
Answer: C,E (LEAVE A REPLY)
Section: Security Monitoring

NEW QUESTION: 15
Refer to the exhibit. This request was sent to a web application server driven by a database.
Which type of web server attack is represented?
A. parameter manipulation
B. heap memory corruption
C. command injection
D. blind SQL injection
Answer: (SHOW ANSWER)
Section: Host-Based Analysis

NEW QUESTION: 16
What is a difference between SOAR and SIEM?
A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not

B. SIEM receives information from a single platform and delivers it to a SOAR
C. SIEM applications are used for threat and vulnerability management, but SOAR platforms are not
D. SOAR receives information from a single platform and delivers it to a SIEM
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Refer to the exhibit.
What is occurring in this network traffic?
A. High rate of SYN packets being sent from a multiple source towards a single destination IP.
B. Flood of SYN packets coming from a single source IP to a single destination IP.
C. Flood of ACK packets coming from a single source IP to multiple destination IPs.
D. High rate of ACK packets being sent from a single source IP towards multiple destination IPs.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
In a SOC environment, what is a vulnerability management metric?
A. code signing enforcement
B. full assets scan
C. internet exposed devices
D. single factor authentication
Answer: (SHOW ANSWER)
Section: Security Policies and Procedures

NEW QUESTION: 19
Why is encryption challenging to security monitoring?
A. Encryption analysis is used by attackers to monitor VPN tunnels.
B. Encryption is used by threat actors as a method of evasion and obfuscation.
C. Encryption introduces additional processing requirements by the CPU.
D. Encryption introduces larger packet sizes to analyze and store.
Answer: (SHOW ANSWER)
Section: Security Concepts

NEW QUESTION: 20
What does cyber attribution identity in an investigation?
A. cause of an attack
B. exploit of an attack
C. vulnerabilities exploited
D. threat actors of an attack
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 21
What does an attacker use to determine which network ports are listening on a potential target device?
A. man-in-the-middle
B. port scanning
C. SQL injection
D. ping sweep
Answer: B (LEAVE A REPLY)
Section: Security Concepts

NEW QUESTION: 22
What is the difference between deep packet inspection and stateful inspection?
A. Stateful inspection is more secure than deep packet inspection on Layer 7
B. Deep packet inspection is more secure than stateful inspection on Layer 4
C. Stateful inspection verifies contents at Layer 4 and deep packet inspection verifies connection at Layer 7
D. Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer 4
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
Refer to the exhibit.
What is the expected result when the "Allow subdissector to reassemble TCP streams" feature is enabled?
A. insert TCP subdissectors
B. disable TCP streams
C. extract a file from a packet capture
D. unfragment TCP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24

An engineer needs to have visibility on TCP bandwidth usage, response time, and latency, combined with deep packet inspection to identify unknown software by its network traffic flow. Which two features of Cisco Application Visibility and Control should the engineer use to accomplish this goal? (Choose two.)

A. traffic filtering
B. metrics collection and exporting
C. adaptive AVC
D. management and reporting
E. application recognition
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 25
A malicious file has been identified in a sandbox analysis tool.
Which piece of information is needed to search for additional downloads of this file by other hosts?

A. file type
B. file size
C. file hash value
D. file name
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

A. availability
B. confidentiality
C. scope
D. integrity
Answer: D (LEAVE A REPLY)

NEW QUESTION: 27
Which security monitoring data type requires the largest storage space?

A. statistical data
B. session data
C. transaction data
D. full packet capture
Answer: (SHOW ANSWER)

NEW QUESTION: 28
An engineer runs a suspicious file in a sandbox analysis tool to see the outcome. The analysis report shows that outbound callouts were made post infection.

Which two pieces of information from the analysis report are needed to investigate the callouts? (Choose two.)
A. dropped files
B. domain names
C. signatures
D. file size
E. host IP addresses
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 29
Refer to the exhibit. Which type of log is displayed?
A. proxy
B. NetFlow
C. sys
D. IDS
Answer: (SHOW ANSWER)

NEW QUESTION: 30
The target web application server is running as the root user and is vulnerable to command injection. Which result of a successful attack is true?
A. buffer overflow
B. cross-site scripting request forgery
C. cross-site scripting
D. privilege escalation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
What is a difference between inline traffic interrogation and traffic mirroring?
A. Inline inspection acts on the original traffic data flow
B. Traffic mirroring passes live traffic to a tool for blocking
C. Traffic mirroring inspects live traffic for analysis and mitigation
D. Inline traffic copies packets for analysis and security
Answer: B (LEAVE A REPLY)
Section: Network Intrusion Analysis

NEW QUESTION: 32
Refer to the exhibit.
What is the expected result when the "Allow subdissector to reassemble TCP streams" feature is enabled?
A. disable TCP streams
B. extract a file from a packet capture
C. insert TCP subdissectors
D. unfragment TCP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 33
How does an SSL certificate impact security between the client and the server?
A. by enabling an authenticated channel between the client and the server
B. by creating an integrated channel between the client and the server
C. by enabling an authorized channel between the client and the server
D. by creating an encrypted channel between the client and the server
Answer: D (LEAVE A REPLY)
Section: Security Monitoring

NEW QUESTION: 34
Refer to the exhibit.
Which type of log is displayed?
A. NetFlow
B. proxy
C. IDS
D. sys
Answer: A (LEAVE A REPLY)

NEW QUESTION: 35
Refer to the exhibit. What is the potential threat identified in this Stealthwatch dashboard?
A. A policy violation is active for host 10.10.101.24.
B. A host on the network is sending a DDoS attack to another inside host.
C. There are two active data exfiltration alerts.
D. A policy violation is active for host 10.201.3.149.
Answer: (SHOW ANSWER)
Section: Host-Based Analysis

NEW QUESTION: 36

What is the virtual address space for a Windows process?
A. physical location of an object in memory
B. set of pages that reside in the physical memory
C. system-level memory protection feature built into the operating system
D. set of virtual memory addresses that can be used
Answer: D (LEAVE A REPLY)

NEW QUESTION: 37
An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email.
When the fink launched, it infected machines and the intruder was able to access the corporate network.
Which testing method did the intruder use?
A. eavesdropping
B. piggybacking
C. social engineering
D. tailgating
Answer: C (LEAVE A REPLY)

NEW QUESTION: 38
When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?
A. fragmentation
B. pivoting
C. encryption
D. stenography
Answer: C (LEAVE A REPLY)
Explanation
https://techdifferences.com/difference-between-steganography-and-cryptography.html#:~:text=The%20steganog

NEW QUESTION: 39
Which two elements are used for profiling a network? (Choose two.)
A. listening ports
B. total throughout
C. OS fingerprint
D. session duration
E. running processes
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 40
Refer to the exhibit.
Which two elements in the table are parts of the 5-tuple? (Choose two.)
A. Ingress Security Zone
B. Initiator IP
C. Source Port
D. First Packet
E. Initiator User
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 41
What specific type of analysis is assigning values to the scenario to see expected outcomes?
A. exploratory
B. descriptive
C. probabilistic
D. deterministic
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Refer to the exhibit.
An engineer is analyzing this Cuckoo Sandbox report for a PDF file that has been downloaded from an email.
What is the state of this file?
A. The file was matched by PEiD threat signatures but no suspicious features are identified since the signature list is up to date.
B. The file has an embedded Windows 32 executable and the Yara field lists suspicious features for further analysis.
C. The file has an embedded executable and was matched by PEiD threat signatures for further analysis.
D. The file has an embedded non-Windows executable but no suspicious features are identified.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
Drag and drop the technology on the left onto the data type the technology provides on the right.
Answer:

NEW QUESTION: 44
Which type of data consists of connection level, application-specific records generated from network traffic?
A. transaction data
B. location data

C. statistical data
D. alert data
Answer: A (LEAVE A REPLY)
Section: Security Monitoring
Explanation/Reference:

NEW QUESTION: 45
Which two elements are assets in the role of attribution in an investigation? (Choose two.)
A. context
B. session
C. laptop
D. firewall logs
E. threat actor
Answer: A,E (LEAVE A REPLY)
Section: Security Policies and Procedures

NEW QUESTION: 46
Drag and drop the technology on the left onto the data type the technology provides on the right.
Answer:

NEW QUESTION: 47
What causes events on a Windows system to show Event Code 4625 in the log messages?
A. A privileged user successfully logged into the system
B. Another device is gaining root access to the system
C. Someone is trying a brute force attack on the network
D. The system detected an XSS attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
What is a benefit of agent-based protection when compared to agentless protection?
A. It lowers maintenance costs
B. It provides a centralized platform

C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously
Answer: B (LEAVE A REPLY)
Section: Security Concepts

NEW QUESTION: 49
How is attacking a vulnerability categorized?
A. exploitation
B. installation
C. delivery
D. action on objectives
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50
What is a sandbox interprocess communication service?
A. A collection of host services that allow for communication between sandboxes.
B. A collection of rules within the sandbox that prevent the communication between sandboxes.
C. A collection of interfaces that allow for coordination of activities among processes.
D. A collection of network services that are activated on an interface, allowing for inter-port communication.
Answer: (SHOW ANSWER)

NEW QUESTION: 51
Which signature impacts network traffic by causing legitimate traffic to be blocked?
A. true negative
B. false negative
C. false positive
D. true positive
Answer: C (LEAVE A REPLY)

NEW QUESTION: 52
DRAG DROP
Drag and drop the technology on the left onto the data type the technology provides on the right.
Select and Place:
Answer:

NEW QUESTION: 53
Which type of evidence supports a theory or an assumption that results from initial evidence?
A. best
B. indirect
C. corroborative

D. probabilistic
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54
Refer to the exhibit.
Which type of log is displayed?
A. NetFlow
B. sys
C. IDS
D. proxy
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?
A. tcpdump
B. NetScout
C. SolarWinds
D. netsh
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
What is a difference between inline traffic interrogation and traffic mirroring?
A. Inline inspection acts on the original traffic data flow
B. Traffic mirroring passes live traffic to a tool for blocking
C. Traffic mirroring inspects live traffic for analysis and mitigation
D. Inline traffic copies packets for analysis and security
Answer: A (LEAVE A REPLY)
Explanation
Inline traffic interrogation analyzes traffic in real time and has the ability to prevent certain traffic from being forwarded Traffic mirroring doesn't pass the live traffic instead it copies traffic from one or more source ports and sends the copied traffic to one or more destinations for analysis by a network analyzer or other monitoring device

NEW QUESTION: 57
What is the function of a command and control server?
A. It enumerates open ports on a network device
B. It sends instruction to a compromised system
C. It drops secondary payload into malware
D. It is used to regain control of the network after a compromise
Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
Refer to the exhibit.
What does the output indicate about the server with the IP address 172.18.104.139?
A. running processes of the server
B. open ports of an email server
C. open port of an FTP server
D. open ports of a web server
Answer: B (LEAVE A REPLY)

NEW QUESTION: 59
One of the objectives of information security is to protect the CIA of information and systems.
What does CIA mean in this context?
A. confidentiality, identity, and authorization
B. confidentiality, integrity, and authorization
C. confidentiality, identity, and availability
D. confidentiality, integrity, and availability
Answer: (SHOW ANSWER)
Section: Security Concepts

NEW QUESTION: 60
Which utility blocks a host portscan?
A. antimalware
B. sandboxing
C. host-based firewall
D. HIDS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 61
When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?
A. stenography
B. pivoting
C. fragmentation
D. encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 62
Drag and drop the definition from the left onto the phase on the right to classify intrusion events according to the Cyber Kill Chain model.
Answer:

NEW QUESTION: 63
How is NetFlow different from traffic mirroring?
A. NetFlow collects metadata and traffic mirroring clones data.
B. Traffic mirroring impacts switch performance and NetFlow does not.
C. Traffic mirroring costs less to operate than NetFlow.
D. NetFlow generates more data than traffic mirroring.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64
What do the Security Intelligence Events within the FMC allow an administrator to do?
A. See if a host is connecting to a known-bad domain.
B. Verify host-to-host traffic within your network.
C. View any malicious files that a host has downloaded.
D. Check for host-to-server traffic within your network.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 65
Refer to the exhibit. Which packet contains a file that is extractable within Wireshark?
A. 2317
B. 1986
C. 2318
D. 2542
Answer: D (LEAVE A REPLY)
Explanation

NEW QUESTION: 66
What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?
A. least privilege
B. need to know
C. integrity validation

D. due diligence
Answer: A (LEAVE A REPLY)
Section: Security Concepts

NEW QUESTION: 67
A user received a malicious attachment but did not run it. Which category classifies the intrusion?
A. reconnaissance
B. weaponization
C. installation
D. delivery
Answer: (SHOW ANSWER)

NEW QUESTION: 68
What is personally identifiable information that must be safeguarded from unauthorized access?
A. date of birth
B. gender
C. driver's license number
D. zip code
Answer: C (LEAVE A REPLY)

NEW QUESTION: 69
An analyst discovers that a legitimate security alert has been dismissed.
Which signature caused this impact on network traffic?
A. true negative
B. false negative
C. false positive
D. true positive
Answer: B (LEAVE A REPLY)
Section: Network Intrusion Analysis

NEW QUESTION: 70
What are two differences in how tampered and untampered disk images affect a security incident? (Choose two.)
A. Untampered images are used in the security investigation process
B. Tampered images are used in the security investigation process
C. The image is tampered if the stored hash and the computed hash match
D. Tampered images are used in the incident recovery process
E. The image is untampered if the stored hash and the computed hash match
Answer: B,E (LEAVE A REPLY)
Section: Host-Based Analysis

NEW QUESTION: 71
One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?
A. confidentiality, integrity, and availability
B. confidentiality, integrity, and authorization
C. confidentiality, identity, and authorization
D. confidentiality, identity, and availability
Answer: A (LEAVE A REPLY)

NEW QUESTION: 72
At a company party a guest asks question:s about the company's user account format and password complexity. How is this type of conversation classified?
A. Password Revelation Strategy
B. Piggybacking
C. Phishing attack
D. Social Engineering
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Refer to the exhibit.
Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.
Answer:

NEW QUESTION: 74
Which security principle requires more than one person is required to perform a critical task?
A. separation of duties
B. least privilege
C. due diligence
D. need to know
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
DRAG DROP
Drag and drop the access control models from the left onto the correct descriptions on the right.
Select and Place:
Answer:

NEW QUESTION: 76
Which two pieces of information are collected from the IPv4 protocol header? (Choose two.)
A. UDP port to which the traffic is destined
B. UDP port from which the traffic is sourced

C. source IP address of the packet
D. TCP port from which the traffic was sourced
E. destination IP address of the packet
Answer: (SHOW ANSWER)

NEW QUESTION: 77
When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?
A. fragmentation
B. pivoting
C. encryption
D. stenography
Answer: D (LEAVE A REPLY)
Section: Security Concepts

NEW QUESTION: 78
Refer to the exhibit.
Which event is occurring?
A. A binary on VM cuckoo1 is being submitted for evaluation
B. A binary is being submitted to run on VM cuckoo1
C. A URL is being evaluated to see if it has a malicious binary
D. A binary named "submit" is running on VM cuckoo1.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 79
Drag and drop the elements from the left into the correct order for incident handling on the right.
Answer:

NEW QUESTION: 80
Refer to the exhibit. What information is depicted?
A. IIS data
B. NetFlow data

C. network discovery event
D. IPS event data
Answer: B (LEAVE A REPLY)
Section: Security Monitoring

NEW QUESTION: 81
Which filter allows an engineer to filter traffic in Wireshark to further analyze the PCAP file by only showing the traffic for LAN 10.11.x.x, between workstations and servers without the Internet?
A. ip.src=10.11.0.0/16 and ip.dst=10.11.0.0/16
B. src=10.11.0.0/16 and dst=10.11.0.0/16
C. src==10.11.0.0/16 and dst==10.11.0.0/16
D. ip.src==10.11.0.0/16 and ip.dst==10.11.0.0/16
Answer: D (LEAVE A REPLY)

NEW QUESTION: 82
What is the principle of defense-in-depth?
A. Access control models are involved.
B. Agentless and agent-based protection for security are used.
C. Several distinct protective layers are involved.
D. Authentication, authorization, and accounting mechanisms are used.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 83
Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?
A. decision making
B. rapid response
C. data mining
D. due diligence
Answer: (SHOW ANSWER)

NEW QUESTION: 84
Which two elements are used for profiling a network? (Choose two.)
A. session duration
B. total throughput
C. running processes
D. listening ports
E. OS fingerprint
Answer: D,E (LEAVE A REPLY)
Section: Security Policies and Procedures
Explanation

NEW QUESTION: 85
Refer to the exhibit.
What does the message indicate?
A. an access attempt was made from the Mosaic web browser
B. a successful access attempt was made to retrieve the password file
C. a successful access attempt was made to retrieve the root of the website
D. a denied access attempt was made to retrieve the password file
Answer: C (LEAVE A REPLY)

NEW QUESTION: 86
At which layer is deep packet inspection investigated on a firewall?
A. data link
B. transport
C. application
D. internet
Answer: (SHOW ANSWER)

NEW QUESTION: 87
A company is using several network applications that require high availability and responsiveness, such that milliseconds of latency on network traffic is not acceptable. An engineer needs to analyze the network and identify ways to improve traffic movement to minimize delays. Which information must the engineer obtain for this analysis?
A. total throughput on the interface of the router and NetFlow records
B. output of routing protocol authentication failures and ports used
C. running processes on the applications and their total network usage
D. deep packet captures of each application flow and duration
Answer: (SHOW ANSWER)

NEW QUESTION: 88
An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?
A. nmap -sL 192.168.1.0/24
B. nmap -sP 192.168.1.0/24
C. nmap --top-ports 192.168.1.0/24
D. nmap -sV 192.168.1.0/24
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89

An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the fink launched, it infected machines and the intruder was able to access the corporate network.
Which testing method did the intruder use?
A. social engineering
B. eavesdropping
C. piggybacking
D. tailgating
Answer: A (LEAVE A REPLY)
Section: Security Monitoring

NEW QUESTION: 90
What is the relationship between a vulnerability and a threat?
A. A vulnerability exploits a threat
B. A vulnerability is a calculation of the potential loss caused by a threat
C. A threat is a calculation of the potential loss caused by a vulnerability
D. A threat exploits a vulnerability
Answer: D (LEAVE A REPLY)

NEW QUESTION: 91
Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key?
A. forgery attack
B. plaintext-only attack
C. ciphertext-only attack
D. meet-in-the-middle attack
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 92
Refer to the exhibit.

What does the output indicate about the server with the IP address 172.18.104.139?

A. open ports of a web server

B. open ports of an email server

C. running processes of the server

D. open port of an FTP server

Answer: (SHOW ANSWER)

NEW QUESTION: 93

Which security technology allows only a set of pre-approved applications to run on a system?

A. application-level blacklisting

B. host-based IPS

C. application-level whitelisting

D. antivirus

Answer: C (LEAVE A REPLY)

Section: Host-Based Analysis

NEW QUESTION: 94

Refer to the exhibit.

Which application protocol is in this PCAP file?

A. SSH

B. TLS

C. TCP

D. HTTP

Answer: D (LEAVE A REPLY)

NEW QUESTION: 95

Which regex matches only on all lowercase letters?

A. [a−z]+

B. [^a−z]+

C. a−z+

D. a*z+

Answer: (SHOW ANSWER)

Section: Network Intrusion Analysis

NEW QUESTION: 96

What is an attack surface as compared to a vulnerability?

A. any potential danger to an asset

B. the sum of all paths for data into and out of the application

C. an exploitable weakness in a system or its design

D. the individuals who perform an attack

Answer: B (LEAVE A REPLY)

Section: Security Monitoring

NEW QUESTION: 97
An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture the analyst cannot determine the technique and payload used for the communication.
Which obfuscation technique is the attacker using?
A. transport layer security encryption
B. Base64 encoding
C. SHA-256 hashing
D. ROT13 encryption
Answer: A (LEAVE A REPLY)

NEW QUESTION: 98
Refer to the exhibit.
This request was sent to a web application server driven by a database. Which type of web server attack is represented?
A. blind SQL injection
B. command injection
C. parameter manipulation
D. heap memory corruption
Answer: A (LEAVE A REPLY)

NEW QUESTION: 99
Refer to the exhibit.
Which packet contains a file that is extractable within Wireshark?
A. 2318
B. 2317
C. 1986
D. 2542
Answer: D (LEAVE A REPLY)

NEW QUESTION: 100
Refer to the exhibit. What is the potential threat identified in this Stealthwatch dashboard?
A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.
B. Host 152.46.6.91 is being identified as a watchlist country for data transfer.
C. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.
D. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.
Answer: (SHOW ANSWER)
Section: Host-Based Analysis