

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

<https://www.2passeasy.com/dumps/200-201/>



NEW QUESTION 1

When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification. Which information is available on the server certificate?

- A. server name, trusted subordinate CA, and private key
- B. trusted subordinate CA, public key, and cipher suites
- C. trusted CA name, cipher suites, and private key
- D. server name, trusted CA, and public key

Answer: D

NEW QUESTION 2

An engineer must compare NIST vs ISO frameworks The engineer decided to compare as readable documentation and also to watch a comparison video review. Using Windows 10 OS. the engineer started a browser and searched for a NIST document and then opened a new tab in the same browser and searched for an ISO document for comparison

The engineer tried to watch the video, but there 'was an audio problem with OS so the engineer had to troubleshoot it At first the engineer started CMD and looked for a driver path then looked for a corresponding registry in the registry editor The engineer enabled "Audiosrv" in task manager and put it on auto start and the problem was solved Which two components of the OS did the engineer touch? (Choose two)

- A. permissions
- B. PowerShell logs
- C. service
- D. MBR
- E. process and thread

Answer: AC

NEW QUESTION 3

What is an advantage of symmetric over asymmetric encryption?

- A. A key is generated on demand according to data type.
- B. A one-time encryption key is generated for data transmission
- C. It is suited for transmitting large amounts of data.
- D. It is a faster encryption mechanism for sessions

Answer: D

NEW QUESTION 4

Drag and drop the type of evidence from the left onto the description of that evidence on the right.

direct evidence	log that shows a command and control check-in from verified malware
corroborative evidence	firewall log showing successful communication and threat intelligence stating an IP is known to host malware
indirect evidence	NetFlow-based spike in DNS traffic

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 5

An engineer needs to configure network systems to detect command and control communications by decrypting ingress and egress perimeter traffic and allowing network security devices to detect malicious outbound communications. Which technology should be used to accomplish the task?

- A. digital certificates
- B. static IP addresses
- C. signatures
- D. cipher suite

Answer: A

NEW QUESTION 6

Refer to the exhibit.

Flow Search Results (1,166)

05/06/2020 06:00 AM - 05/06/2020 1:20 PM (Time Ra) 2,000 (Max Records)

Subject: 10.201.3.149 Client

Connection: All (Flow Direction)

Peer: Outside Hosts

START	DURATION	SUBJECT IP AD...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDRE...
May 6, 2020 6:46:42 AM (9hr 14min 19s ago)	15min 13s	10.201.3.149	52599/UDP	End User Devices, Desktops, Atlanta, Sales and Marketing	6.42 M	Undefined UDP	132.53 M	152.46.6.91

General

View URL Data

Subject	Totals	Peer
Packets: 60.06 K	Packets: 165.87 K	Packets: 105.81 K
Packet Rate: 65.78 pps	Packet Rate: 181.67 pps	Packet Rate: 115.89 pps
Bytes: 6.42 MB	Bytes: 132.53 MB	Bytes: 126.11 MB
Byte Rate: 7.37 Kbps	Byte Rate: 152.2 Kbps	Byte Rate: 144.83 Kbps
Percent Transfer: 4.64%	Subject Byte Ratio: 4.84%	Percent Transfer: 95.16%
Host Groups: End User Devices, Desktops, Atlanta, Sales and Marketing	RTT: --	Host Groups: United States
Payload: --	SRT: --	Payload: --

May 6, 2020 9:44:05 AM (6hr 16min 56s ago) 55 min 56s 10.201.3.149 52599/UDP End User Devices, Desktops, Atlanta, Sales and Marketing 4.13 M Undefined UDP 96.26 M 152.46.6.91

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: D

NEW QUESTION 7

Which action should be taken if the system is overwhelmed with alerts when false positives and false negatives are compared?

- A. Modify the settings of the intrusion detection system.
- B. Design criteria for reviewing alerts.
- C. Redefine signature rules.
- D. Adjust the alerts schedule.

Answer: A

Explanation:

Traditional intrusion detection system (IDS) and intrusion prevention system (IPS) devices need to be tuned to avoid false positives and false negatives. Next-generation IPSs do not need the same level of tuning compared to traditional IPSs. Also, you can obtain much deeper reports and functionality, including advanced malware protection and retrospective analysis to see what happened after an attack took place. Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW QUESTION 8

An investigator is examining a copy of an ISO file that is stored in CDFS format. What type of evidence is this file?

- A. data from a CD copied using Mac-based system
- B. data from a CD copied using Linux system
- C. data from a DVD copied using Windows system
- D. data from a CD copied using Windows

Answer: B

Explanation:

CDfs is a virtual file system for Unix-like operating systems; it provides access to data and audio tracks on Compact Discs. When the CDfs driver mounts a Compact Disc, it represents each track as a file. This is consistent with the Unix convention "everything is a file". Source: <https://en.wikipedia.org/wiki/CDfs>

NEW QUESTION 9

Refer to the exhibit.

Overview Analysis Policies Devices Objects Health System Hel

Content Explorer Connections > Security Intelligence Events Intrusions Files Hosts Users Vulnerabilities Correlation Custom Search

Security Intelligence Events (switch workflow) 2018-03-07 07:20:20 - 2018-03-07 13:47:20

Security Intelligence with Application Details > Table View of Security Intelligence Events

Search Constraints (Edit Search Serve Search) Expanding Disabled Columns

Jump to...

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port/ICMP Type
2018-03-07 13:42:01		Sinkhole DNS Block		10.0.10.75		JERI LABORDE (D\CLOUD-SOC LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
2018-03-07 13:42:01		Sinkhole DNS Block		10.0.0.100		AMPARO GIVENS (D\CLOUD-SOC LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
2018-03-07 13:42:01		Sinkhole DNS Block		10.112.10.158		VERNETTA DONNEL (D\CLOUD-SOC LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp

<< Page 1 of 1 >> Displaying rows 1-3 of 3 rows

View Delete View All Delete All

Which two elements in the table are parts of the 5-tuple? (Choose two.)

- A. First Packet
- B. Initiator User
- C. Ingress Security Zone
- D. Source Port
- E. Initiator IP

Answer: DE

NEW QUESTION 10

What is the impact of false positive alerts on business compared to true positive?

- A. True positives affect security as no alarm is raised when an attack has taken place, while false positives are alerts raised appropriately to detect and further mitigate them.
- B. True-positive alerts are blocked by mistake as potential attacks, while False-positives are actual attacks Identified as harmless.
- C. False-positive alerts are detected by confusion as potential attacks, while true positives are attack attempts identified appropriately.
- D. False positives alerts are manually ignored signatures to avoid warnings that are already acknowledged, while true positives are warnings that are not yet acknowledged.

Answer: C

NEW QUESTION 10

Refer to the exhibit.

File name: VAC-Bypass-Loader.exe

Full analysis: <https://app.any.run/tasks/b6c8538c-0b3d-4e57-8900-863115142a98>

Verdict: Malicious activity

Threats: njRAT

njRAT is a remote access Trojan. It is one of the most widely accessible RATs on the market that features an abundance of educational information. Interested attackers can even find tutorials on YouTube. This allows it to become one of the most popular RATs in the world.

Malware Trends Tracker More details

Analysis date: 12/13/2020, 19:21:33

OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)

Tags: trojan rat agent stealer

Indicators: [Icons]

MIME: application/x-dosexec

File info: PE32 executable (GUI) Intel 80386, for MS Windows

MDS: 112E1B83R07106EE6146D6600209AT...

Where is the executable file?

- A. info
- B. tags
- C. MIME
- D. name

Answer: C

NEW QUESTION 15

A company encountered a breach on its web servers using IIS 7.5. During the investigation, an engineer discovered that an attacker read and altered the data on a secure communication using TLS 1.2 and intercepted sensitive information by downgrading a connection to export-grade cryptography. The engineer must mitigate similar incidents in the future and ensure that clients and servers always negotiate with the most secure protocol versions and cryptographic parameters. Which action does the engineer recommend?

- A. Upgrade to TLS v1.3.
- B. Install the latest IIS version.
- C. Downgrade to TLS 1.1.
- D. Deploy an intrusion detection system

Answer: B

NEW QUESTION 18

Which event is user interaction?

- A. gaining root access
- B. executing remote code
- C. reading and writing file permission
- D. opening a malicious file

Answer: D

NEW QUESTION 21

During which phase of the forensic process are tools and techniques used to extract information from the collected data?

- A. investigation
- B. examination
- C. reporting
- D. collection

Answer: D

NEW QUESTION 26

An engineer is investigating a case of the unauthorized usage of the "Tcpdump" tool. The analysis revealed that a malicious insider attempted to sniff traffic on a specific interface. What type of information did the malicious insider attempt to obtain?

- A. tagged protocols being used on the network
- B. all firewall alerts and resulting mitigations
- C. tagged ports being used on the network
- D. all information and data within the datagram

Answer: C

NEW QUESTION 28

Which step in the incident response process researches an attacking host through logs in a SIEM?

- A. detection and analysis
- B. preparation
- C. eradication
- D. containment

Answer: A

Explanation:

Preparation --> Detection and Analysis --> Containment, Erradicaion and Recovery --> Post-Incident Activity Detection and Analysis --> Profile networks and systems, Understand normal behaviors, Create a log retention policy, Perform event correlation. Maintain and use a knowledge base of information. Use Internet search engines for research. Run packet sniffers to collect additional data. Filter the data. Seek assistance from others. Keep all host clocks synchronized. Know the different types of attacks and attack vectors. Develop processes and procedures to recognize the signs of an incident. Understand the sources of precursors and indicators. Create appropriate incident documentation capabilities and processes. Create processes to effectively prioritize security incidents. Create processes to effectively communicate incident information (internal and external communications).

Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW QUESTION 32

What is rule-based detection when compared to statistical detection?

- A. proof of a user's identity
- B. proof of a user's action
- C. likelihood of user's action
- D. falsification of a user's identity

Answer: B

NEW QUESTION 33

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. signatures
- B. host IP addresses
- C. file size
- D. dropped files
- E. domain names

Answer: BE

NEW QUESTION 36

Which technology prevents end-device to end-device IP traceability?

- A. encryption
- B. load balancing
- C. NAT/PAT
- D. tunneling

Answer: C

NEW QUESTION 37

An engineer is working with the compliance teams to identify the data passing through the network. During analysis, the engineer informs the compliance team that external penmeter data flows contain records, writings, and artwork Internal segregated network flows contain the customer choices by gender, addresses, and product preferences by age. The engineer must identify protected data. Which two types of data must be identified? (Choose two.)

- A. SOX
- B. PII
- C. PHI
- D. PCI
- E. copyright

Answer: BC

NEW QUESTION 40

An analyst received an alert on their desktop computer showing that an attack was successful on the host. After investigating, the analyst discovered that no mitigation action occurred during the attack. What is the reason for this discrepancy?

- A. The computer has a HIPS installed on it.
- B. The computer has a NIPS installed on it.
- C. The computer has a HIDS installed on it.
- D. The computer has a NIDS installed on it.

Answer: C

NEW QUESTION 44

Refer to the exhibit.

```
- Internet Protocol version 4, Src: 192.168.122.100 (192.168.122.100), Dst:
81.179.179.69 (81.179.179.69)
  Version: 4
  Header Length: 20 bytes
+ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT
(Not ECN-Capable Transport))
  Total Length: 538
  Identification: 0x6bse (27534)
+ Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
+ Header checksum: 0x000 [Validation disabled]
  Source: 192.168.122.100 (192.168.122.100)
  Destination: 81.179.179.69 (81.179.179.69)
  [Source GeoIP: Unknown]

+ Transmission control protocol. src port: 50272 (50272) Dst Port: 80 (80).
Seq: 419451624. Ack: 970444123. Len: 490
```

What should be interpreted from this packet capture?

- A. 81.179.179.69 is sending a packet from port 80 to port 50272 of IP address 192.168.122.100 using UDP protocol.
- B. 192.168.122.100 is sending a packet from port 50272 to port 80 of IP address 81.179.179.69 using TCP protocol.
- C. 192.168.122.100 is sending a packet from port 80 to port 50272 of IP address 81.179.179.69 using UDP protocol.
- D. 81.179.179.69 is sending a packet from port 50272 to port 80 of IP address 192.168.122.100 using TCP UDP protocol.

Answer: B

NEW QUESTION 45

Which data type is necessary to get information about source/destination ports?

- A. statistical data
- B. session data
- C. connectivity data
- D. alert data

Answer: B

Explanation:

Session data provides information about the five tuples; source IP address/port number, destination IP address/port number and the protocol
What is Connectivity Data? According to IBM - Connectivity data defines how entities are connected in the network. It includes connections between different

devices, and VLAN-related connections within the same device <https://www.ibm.com/docs/en/networkmanager/4.2.0?topic=relationships-connectivity-data>

NEW QUESTION 47

Which category relates to improper use or disclosure of PII data?

- A. legal
- B. compliance
- C. regulated
- D. contractual

Answer: C

NEW QUESTION 48

Refer to the exhibit.

Interface: 192.168.1.29 --- 0x11		
Internet Address	Physical Address	Type
192.168.1.10	d8-a7-56-d7-19-ea	dynamic
192.168.1.67	d8-a7-56-d7-19-ea	dynamic
192.168.1.1	01-00-5e-00-00-16	static

What is occurring in this network?

- A. ARP cache poisoning
- B. DNS cache poisoning
- C. MAC address table overflow
- D. MAC flooding attack

Answer: A

NEW QUESTION 52

Which metric should be used when evaluating the effectiveness and scope of a Security Operations Center?

- A. The average time the SOC takes to register and assign the incident.
- B. The total incident escalations per week.
- C. The average time the SOC takes to detect and resolve the incident.
- D. The total incident escalations per month.

Answer: C

NEW QUESTION 56

At which layer is deep packet inspection investigated on a firewall?

- A. internet
- B. transport
- C. application
- D. data link

Answer: C

Explanation:

Deep packet inspection is a form of packet filtering usually carried out as a function of your firewall. It is applied at the Open Systems Interconnection's application layer. Deep packet inspection evaluates the contents of a packet that is going through a checkpoint.

NEW QUESTION 58

Which system monitors local system operation and local network access for violations of a security policy?

- A. host-based intrusion detection
- B. systems-based sandboxing
- C. host-based firewall
- D. antivirus

Answer: A

Explanation:

HIDS is capable of monitoring the internals of a computing system as well as the network packets on its network interfaces. Host-based firewall is a piece of software running on a single Host that can restrict incoming and outgoing Network activity for that host only.

NEW QUESTION 63

A company receptionist received a threatening call referencing stealing assets and did not take any action assuming it was a social engineering attempt. Within 48 hours, multiple assets were breached, affecting the confidentiality of sensitive information. What is the threat actor in this incident?

- A. company assets that are threatened
- B. customer assets that are threatened
- C. perpetrators of the attack
- D. victims of the attack

Answer: C

NEW QUESTION 66

What is a difference between tampered and untampered disk images?

- A. Tampered images have the same stored and computed hash.
- B. Tampered images are used as evidence.
- C. Untampered images are used for forensic investigations.
- D. Untampered images are deliberately altered to preserve as evidence

Answer: D

NEW QUESTION 69

Refer to the exhibit.

```
192.168.10.10 -- [01/Dec/2020:11:12:22 -0200] "GET /icons/powered_by_rh.png HTTP/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 -- [01/Dec/2020:11:13:15 -0200] "GET /favicon.ico HTTP/1.1" 404 288 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 -- [01/Dec/2020:11:14:22 -0200] "GET /%27%27;!-%22%3CXSS%3E=&{} HTTP/1.1" 404 310 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
```

What is occurring within the exhibit?

- A. regular GET requests
- B. XML External Entities attack
- C. insecure deserialization
- D. cross-site scripting attack

Answer: A

NEW QUESTION 71

A security engineer notices confidential data being exfiltrated to a domain "Ranso4134-mware31-895" address that is attributed to a known advanced persistent threat group. The engineer discovers that the activity is part of a real attack and not a network misconfiguration. Which category does this event fall under as defined in the Cyber Kill Chain?

- A. reconnaissance
- B. delivery
- C. action on objectives
- D. weaponization

Answer: C

NEW QUESTION 75

Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

- A. NetScout
- B. tcpdump
- C. SolarWinds
- D. netsh

Answer: B

NEW QUESTION 80

What are two social engineering techniques? (Choose two.)

- A. privilege escalation
- B. DDoS attack
- C. phishing
- D. man-in-the-middle
- E. pharming

Answer: CE

NEW QUESTION 83

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 --top-ports 192.168.1.0/24
- B. nmap -sP 192.168.1.0/24
- C. nmap -sL 192.168.1.0/24

D. nmap -sV 192.168.1.0/24

Answer: B

Explanation:

<https://explainshell.com/explain?cmd=nmap+-sP>

NEW QUESTION 85

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 link 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

NEW QUESTION 88

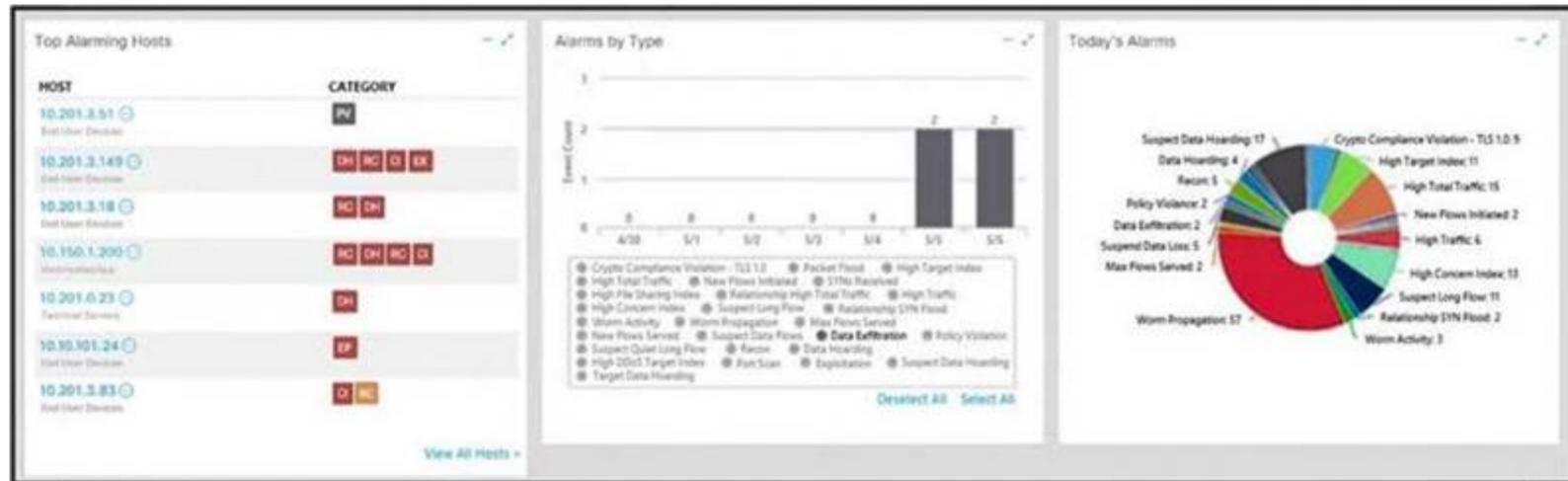
Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

- A. syslog messages
- B. full packet capture
- C. NetFlow
- D. firewall event logs

Answer: C

NEW QUESTION 91

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: C

NEW QUESTION 94

Refer to the exhibit.

```
10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1"
200 1254 "-" "Mozilla/5.0(X11; Ubuntu; Linux x86_64; rv:54.0)
Gecko/20100101 Firefox/54.0"
```

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

NEW QUESTION 97

What is the practice of giving an employee access to only the resources needed to accomplish their job?

- A. principle of least privilege
- B. organizational separation

- C. separation of duties
- D. need to know principle

Answer: A

NEW QUESTION 98

What is obtained using NetFlow?

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

Answer: A

NEW QUESTION 99

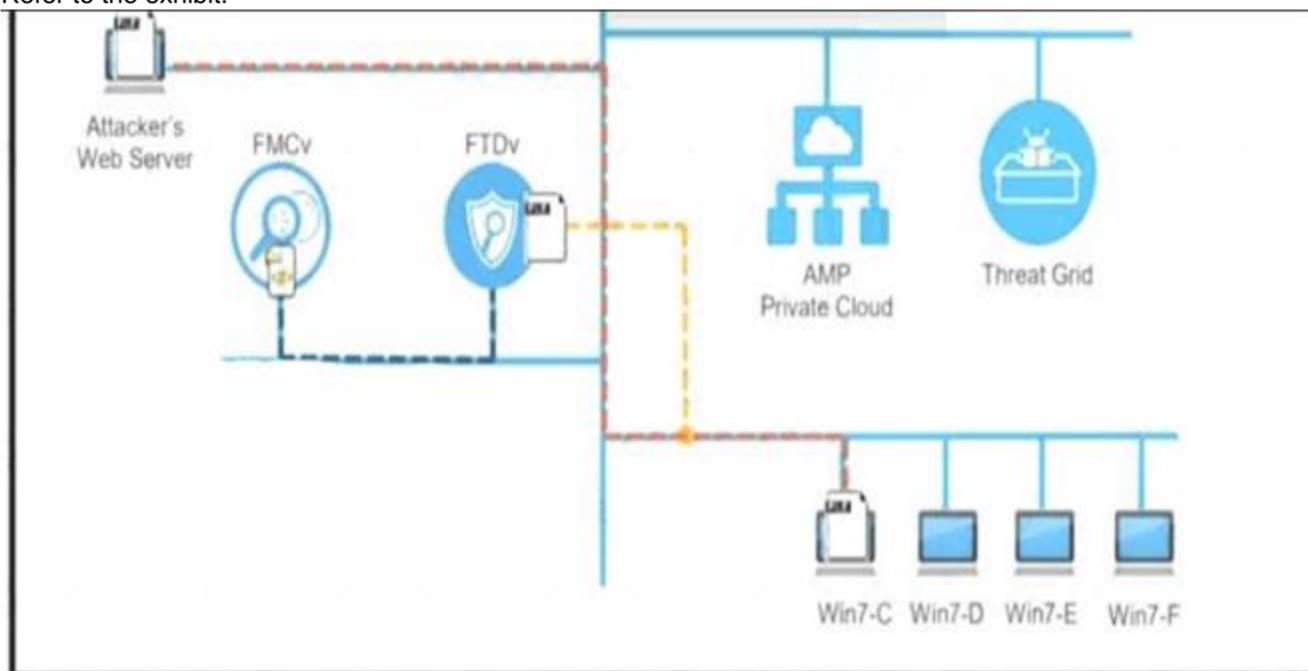
Which regular expression matches "color" and "colour"?

- A. colo?ur
- B. col[08]+our
- C. colou?r
- D. col[09]+our

Answer: C

NEW QUESTION 101

Refer to the exhibit.



A workstation downloads a malicious docx file from the Internet and a copy is sent to FTDv. The FTDv sends the file hash to FMC and the file event is recorded. What would have occurred with stronger data visibility?

- A. The traffic would have been monitored at any segment in the network.
- B. Malicious traffic would have been blocked on multiple devices
- C. An extra level of security would have been in place
- D. Detailed information about the data in real time would have been provided

Answer: B

NEW QUESTION 106

What are the two differences between stateful and deep packet inspection? (Choose two)

- A. Stateful inspection is capable of TCP state tracking, and deep packet filtering checks only TCP source and destination ports
- B. Deep packet inspection is capable of malware blocking, and stateful inspection is not
- C. Deep packet inspection operates on Layer 3 and 4. and stateful inspection operates on Layer 3 of the OSI model
- D. Deep packet inspection is capable of TCP state monitoring only, and stateful inspection can inspect TCP and UDP.
- E. Stateful inspection is capable of packet data inspections, and deep packet inspection is not

Answer: AB

NEW QUESTION 110

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

NEW QUESTION 111

Refer to the exhibit.

Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Details
5585	43.600368	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142352 TSecr=17155
5586	43.604379	192.168.56.101	192.168.56.1	22	SSHv2	146 Server: Encrypted packet (len=80)
5587	43.604402	192.168.56.1	192.168.56.101	22	SSHv2	146 Client: Encrypted packet (len=80)
5588	43.604497	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142357 TSecr=17155
5589	43.611441	192.168.56.101	192.168.56.1	22	SSHv2	130 Server: Encrypted packet (len=64)
5590	43.611542	192.168.56.1	192.168.56.101	22	SSHv2	146 Client: Encrypted packet (len=80)
5591	43.611898	192.168.56.101	192.168.56.1	22	SSHv2	538 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=192)
5592	43.612193	192.168.56.1	192.168.56.101	22	SSHv2	82 Client: New Keys
5593	43.612287	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142364 TSecr=17155
5594	43.612608	192.168.56.1	192.168.56.101	22	SSHv2	130 Client: Encrypted packet (len=64)
5595	43.612697	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142365 TSecr=17155
5596	43.615355	192.168.56.101	192.168.56.1	22	SSHv2	130 Server: Protocol (SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u1)
5597	43.615375	192.168.56.1	192.168.56.101	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142366 TSecr=17155
5598	43.615717	192.168.56.101	192.168.56.1	22	SSHv2	738 Client: Key Exchange Init
5599	43.619098	192.168.56.101	192.168.56.1	22	SSHv2	130 Server: Encrypted packet (len=64)
5600	43.619184	192.168.56.101	192.168.56.101	22	SSHv2	146 Client: Encrypted packet (len=80)
5601	43.624638	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142377 TSecr=17155
5602	43.624751	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142377 TSecr=17155
5603	43.624867	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142377 TSecr=17155
5604	43.625019	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142377 TSecr=17155
5605	43.625111	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142377 TSecr=17155
5606	43.625272	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142378 TSecr=17155
5607	43.625835	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142378 TSecr=17155
5608	43.625985	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142378 TSecr=17155
5609	43.626094	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142378 TSecr=17155
5610	43.628193	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142378 TSecr=17155
5611	43.628283	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142378 TSecr=17155
5612	43.628718	192.168.56.101	192.168.56.1	22	SSHv2	538 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=192)
5613	43.627975	192.168.56.1	192.168.56.101	22	SSHv2	82 Client: New Keys
5614	43.627621	192.168.56.101	192.168.56.1	22	TCP	66.22.48922 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142388 TSecr=17155

An engineer is analyzing a PCAP file after a recent breach. An engineer identified that the attacker used an aggressive ARP scan to scan the hosts and found web and SSH servers. Further analysis showed several SSH Server Banner and Key Exchange Initiations. The engineer cannot see the exact data being transmitted over an encrypted channel and cannot identify how the attacker gained access. How did the attacker gain access?

- A. by using the buffer overflow in the URL catcher feature for SSH
- B. by using an SSH Tectia Server vulnerability to enable host-based authentication
- C. by using an SSH vulnerability to silently redirect connections to the local host
- D. by using brute force on the SSH service to gain access

Answer: C

NEW QUESTION 112

Which two pieces of information are collected from the IPv4 protocol header? (Choose two.)

- A. UDP port to which the traffic is destined
- B. TCP port from which the traffic was sourced
- C. source IP address of the packet
- D. destination IP address of the packet
- E. UDP port from which the traffic is sourced

Answer: CD

NEW QUESTION 114

At a company party a guest asks questions about the company's user account format and password complexity. How is this type of conversation classified?

- A. Phishing attack
- B. Password Revelation Strategy
- C. Piggybacking
- D. Social Engineering

Answer: D

NEW QUESTION 115

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 three active data exfiltration alerts.

D. A policy violation is active for host 10.201.3.149.

Answer: C

Explanation:

"EX" = exfiltration And there are three.

Also the "suspect long flow" and "suspect data heading" suggest, for example, DNS exfiltration

[https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6 page 177](https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6_page_177).

NEW QUESTION 118

What is the difference between an attack vector and attack surface?

- A. An attack surface identifies vulnerabilities that require user input or validation; and an attack vector identifies vulnerabilities that are independent of user actions.
- B. An attack vector identifies components that can be exploited, and an attack surface identifies the potential path an attack can take to penetrate the network.
- C. An attack surface recognizes which network parts are vulnerable to an attack; and an attack vector identifies which attacks are possible with these vulnerabilities.
- D. An attack vector identifies the potential outcomes of an attack; and an attack surface launches an attack using several methods against the identified vulnerabilities.

Answer: C

NEW QUESTION 121

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group.

What is the initial event called in the NIST SP800-61?

- A. online assault
- B. precursor
- C. trigger
- D. instigator

Answer: B

Explanation:

A precursor is a sign that a cyber-attack is about to occur on a system or network. An indicator is the actual alerts that are generated as an attack is happening.

Therefore, as a security professional, it's important to know where you can find both precursor and indicator sources of information.

The following are common sources of precursor and indicator information:

- > Security Information and Event Management (SIEM)
- > Anti-virus and anti-spam software
- > File integrity checking applications/software
- > Logs from various sources (operating systems, devices, and applications)
- > People who report a security incident <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

NEW QUESTION 124

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. src=10.11.0.0/16 and dst=10.11.0.0/16
- B. ip.src==10.11.0.0/16 and ip.dst==10.11.0.0/16
- C. ip.src=10.11.0.0/16 and ip.dst=10.11.0.0/16
- D. src==10.11.0.0/16 and dst==10.11.0.0/16

Answer: B

NEW QUESTION 129

What is the difference between statistical detection and rule-based detection models?

- A. Rule-based detection involves the collection of data in relation to the behavior of legitimate users over a period of time
- 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. Statistical detection involves the evaluation of an object on its intended actions before it executes that behavior
- D. Rule-based detection defines legitimate data of users over a period of time and statistical detection defines it on an IF/THEN basis

Answer: B

NEW QUESTION 132

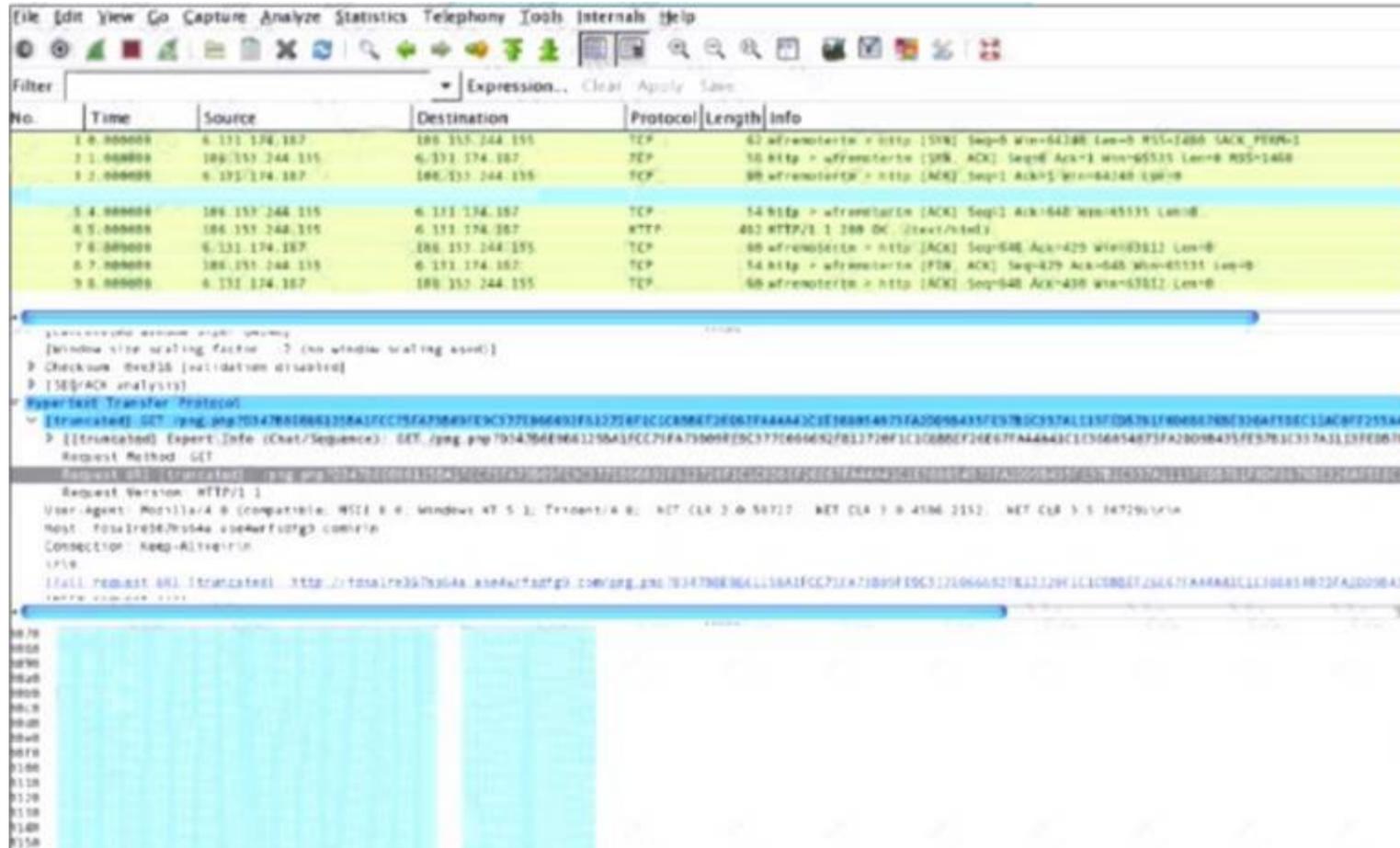
Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)

- A. detection and analysis
- B. post-incident activity
- C. vulnerability management
- D. risk assessment
- E. vulnerability scoring

Answer: AB

NEW QUESTION 137

Refer to the exhibit.



What is shown in this PCAP file?

- A. Timestamps are indicated with error.
- B. The protocol is TCP.
- C. The User-Agent is Mozilla/5.0.
- D. The HTTP GET is encoded.

Answer: D

NEW QUESTION 138

Which vulnerability type is used to read, write, or erase information from a database?

- A. cross-site scripting
- B. cross-site request forgery
- C. buffer overflow
- D. SQL injection

Answer: D

NEW QUESTION 141

Which security model assumes an attacker within and outside of the network and enforces strict verification before connecting to any system or resource within the organization?

- A. Biba
- B. Object-capability
- C. Take-Grant
- D. Zero Trust

Answer: D

Explanation:

Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

NEW QUESTION 143

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
14	27.405297	192.168.1.83	192.168.1.80	HTTP	335	GET /news.php HTTP/1.1
14	27.423516	192.168.1.80	192.168.1.83	HTTP	12	HTTP/1.0 200 OK (text/html)
14	27.843983	192.168.1.83	192.168.1.80	HTTP	516	POST /admin/get.php HTTP/1.1
14	27.856474	192.168.1.80	192.168.1.83	HTTP	519	HTTP/1.0 200 OK (text/html)
14	28.053803	192.168.1.83	192.168.1.80	HTTP	276	POST /news.php HTTP/1.1
15	28.065561	192.168.1.80	192.168.1.83	HTTP	11	HTTP/1.0 200 OK (text/html)
20	33.245337	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
20	33.253440	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
23	38.265103	192.168.1.83	192.168.1.80	HTTP	250	GET /news.php HTTP/1.1
23	38.271353	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
26	43.291043	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
26	43.298364	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
30	48.311212	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
30	48.322750	192.168.1.80	192.168.1.83	HTTP	340	HTTP/1.0 200 OK (text/html)
30	48.439913	192.168.1.83	192.168.1.80	HTTP	148	POST /admin/get.php HTTP/1.1
30	48.455743	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 404 NOT FOUND (text/html)
35	53.482265	192.168.1.83	192.168.1.80	HTTP	255	GET /admin/get.php HTTP/1.1
35	53.491062	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
40	58.515011	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
40	58.522942	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)

A network administrator is investigating suspicious network activity by analyzing captured traffic. An engineer notices abnormal behavior and discovers that the default user agent is present in the headers of requests and data being transmitted. What is occurring?

- A. indicators of denial-of-service attack due to the frequency of requests
- B. garbage flood attack: attacker is sending garbage binary data to open ports
- C. indicators of data exfiltration: HTTP requests must be plain text
- D. cache bypassing attack: attacker is sending requests for noncacheable content

Answer: D

NEW QUESTION 146

An engineer received a flood of phishing emails from HR with the source address HRjacobm@companycom. What is the threat actor in this scenario?

- A. phishing email
- B. sender
- C. HR
- D. receiver

Answer: B

NEW QUESTION 148

What are two denial-of-service (DoS) attacks? (Choose two)

- A. port scan
- B. SYN flood
- C. man-in-the-middle
- D. phishing
- E. teardrop

Answer: BC

NEW QUESTION 149

What is the difference between the rule-based detection when compared to behavioral detection?

- A. Rule-Based detection is searching for patterns linked to specific types of attacks, while behavioral is identifying per signature.
- B. Rule-Based systems have established patterns that do not change with new data, while behavioral changes.
- C. Behavioral systems are predefined patterns from hundreds of users, while Rule-Based only flags potentially abnormal patterns using signatures.
- D. Behavioral systems find sequences that match a particular attack signature, while Rule-Based identifies potential attacks.

Answer: D

NEW QUESTION 154

Refer to the exhibit.

```
# nmap -sV 172.18.104.139

Starting Nmap 7.01 ( https://nmap.org ) at 2020-03-07 11:36 EST
Nmap scan report for 172.18.104.139
Host is up (0.000018s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp     Postfix smtpd
110/tcp   open  pop3     Dovecot pop3d
143/tcp   open  imap     Dovecot imapd
Service Info: Host: 172.18.108.139; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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 port of an FTP server
- C. open ports of an email server
- D. running processes of the server

Answer: C

NEW QUESTION 159

What is a difference between SIEM and SOAR?

- A. SOAR predicts and prevents security alerts, while SIEM checks attack patterns and applies the mitigation.
- B. SIEM's primary function is to collect and detect anomalies, while SOAR is more focused on security operations automation and response.
- C. SIEM predicts and prevents security alerts, while SOAR checks attack patterns and applies the mitigation.
- D. SOAR's primary function is to collect and detect anomalies, while SIEM is more focused on security operations automation and response.

Answer: B

NEW QUESTION 161

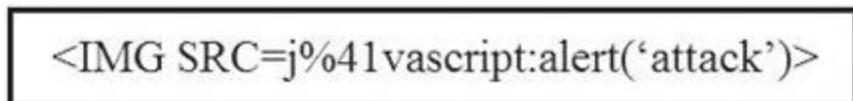
What is vulnerability management?

- A. A security practice focused on clarifying and narrowing intrusion points.
- B. A security practice of performing actions rather than acknowledging the threats.
- C. A process to identify and remediate existing weaknesses.
- D. A process to recover from service interruptions and restore business-critical applications

Answer: C

NEW QUESTION 165

Refer to the exhibit.



Which kind of attack method is depicted in this string?

- A. cross-site scripting
- B. man-in-the-middle
- C. SQL injection
- D. denial of service

Answer: A

NEW QUESTION 168

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 200-201 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 200-201 Product From:

<https://www.2passeasy.com/dumps/200-201/>

Money Back Guarantee

200-201 Practice Exam Features:

- * 200-201 Questions and Answers Updated Frequently
- * 200-201 Practice Questions Verified by Expert Senior Certified Staff
- * 200-201 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 200-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year