

Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals



NEW QUESTION 1

Refer to the exhibit.



Which component is identifiable in this exhibit?

- A. Trusted Root Certificate store on the local machine
- B. Windows PowerShell verb
- C. Windows Registry hive
- D. local service in the Windows Services Manager

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives>

https://ldapwiki.com/wiki/HKEY_LOCAL_MACHINE#:~:text=HKEY_LOCAL_MACHINE%20Windows%2

NEW QUESTION 2

What causes events on a Windows system to show Event Code 4625 in the log messages?

- A. The system detected an XSS attack
- B. Someone is trying a brute force attack on the network
- C. Another device is gaining root access to the system
- D. A privileged user successfully logged into the system

Answer: B

NEW QUESTION 3

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 4

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

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 5

What is the difference between deep packet inspection and stateful inspection?

- A. Stateful inspection verifies contents at Layer 4. and deep packet inspection verifies connection at Layer 7.
- B. Stateful inspection is more secure than deep packet inspection on Layer 7.
- C. Deep packet inspection is more secure than stateful inspection on Layer 4.
- D. Deep packet inspection allows visibility on Layer 7, and stateful inspection allows visibility on Layer 4.

Answer: D

NEW QUESTION 6

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
17	0.011641	10.0.2.15	192.124.249.9	TCP	76	50586-443 [SYN] Seq=0 Win=
18	0.011918	10.0.2.15	192.124.249.9	TCP	76	50588-443 [SYN] Seq=0 Win=
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443-50588 [SYN, ACK] Seq=0
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588-443 [ACK] Seq=1 Ack=
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443-50586 [SYN, ACK] Seq=0
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=1 Ack=
23	0.023212	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
24	0.023373	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443-50588 [ACK] Seq=1 Ack=
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443-50586 [ACK] Seq=1 Ack=
27	0.037413	192.124.249.9	10.0.2.15	TLSv1.2	2792	Server Hello
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=206 Ac

> Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
 > Linux cooked capture
 > Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)
 > Transmission Control Protocol, Src Port: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack:1,
 > Secure Sockets Layer

```

0000 00 04 00 01 00 06 08 00 27 7a 3c 93 00 00 08 00 ..... *z<.....
0010 45 00 00 f5 eb 3e 40 00 40 06 89 2f 0a 00 02 0f E....>@. @../....
0020 c0 7c f9 09 c5 9c 01 bb 4d db 7f f7 00 b3 b0 02 .|..... M.....
0030 50 18 72 10 c6 7c 00 00 16 03 01 00 c8 01 00 00 P.r..|.. .....
0040 c4 03 03 d1 08 45 78 b7 2c 90 04 ee 51 16 f1 82 .....Ex. ....0...
0050 16 43 ec d4 89 60 34 4a 7b 80 a6 d1 72 d5 11 87 .C....4J {...r...
0060 10 57 cc 00 00 1e c0 2b c0 2f cc a9 cc a8 c0 2c .W.....+ ./.....
0070 c0 30 c0 0a c0 09 c0 13 c0 14 00 33 00 39 00 2f .0..... ...3.9./
0080 00 35 00 0a 01 00 00 7d 00 00 00 16 00 14 00 00 .5.....} .....
0090 11 77 77 77 2e 6c 69 6e 75 78 6d 69 6e 74 2e 63 .wwwlin uxmint.c
00a0 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 08 00 om..... .....
00b0 06 00 17 00 18 00 19 00 0b 00 02 01 00 00 23 00 ..... .....#.
00c0 00 33 74 00 00 00 10 00 17 00 15 02 68 32 08 73 .3t..... ...h2.s
00d0 70 64 79 2f 33 2e 31 08 68 74 74 70 2f 31 2e 31 pdy/3.2. http/1.1
00e0 00 05 00 05 01 00 00 00 00 00 0d 00 18 00 16 04 ..... .....
00f0 01 05 01 06 01 02 01 04 03 05 03 06 03 02 03 05 ..... .....
0100 02 04 02 02 02 .....
    
```

Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

source address	source address
destination address	source port
source port	destination port
destination port	destination address
Network Protocol	Transport Protocol
Transport Protocol	Network Protocol
Application Protocol	Application Protocol

NEW QUESTION 7

A network engineer discovers that a foreign government hacked one of the defense contractors in their home country and stole intellectual property. What is the threat agent in this situation?

- A. the intellectual property that was stolen
- B. the defense contractor who stored the intellectual property
- C. the method used to conduct the attack
- D. the foreign government that conducted the attack

Answer: D

NEW QUESTION 8

A user received an email attachment named "Hr405-report2609-empl094.exe" but did not run it. Which category of the cyber kill chain should be assigned to this type of event?

- A. installation
- B. reconnaissance
- C. weaponization
- D. delivery

Answer: D

NEW QUESTION 9

An analyst is using the SIEM platform and must extract a custom property from a Cisco device and capture the phrase, "File: Clean." Which regex must the analyst import?

- A. File: Clean
- B. ^Parent File Clean\$
- C. File: Clean (.*)
- D. ^File: Clean\$

Answer: A

NEW QUESTION 10

Refer to the exhibit.

```
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63064 135 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.14 63065 49156 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63066 65386 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63067 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.14 62292 389 0 - - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63068 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63069 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.13 62293 389 0 - - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63070 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63071 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63072 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63073 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63074 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63075 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63076 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 55053 53 0 - - - - - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 50845 53 0 - - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP fe80::29ea:1a3c:24d6:fb49 ff02::1:3 57333 5355 0 - - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP 10.40.4.252 224.0.0.252 59629 5355 0 - - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 58846 5355 0 - - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP 10.40.4.182 224.0.0.252 58846 5355 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 137 137 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 63504 5355 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 63504 5355 0 - - - - - - - SEND
```

An engineer received an event log file to review. Which technology generated the log?

- A. NetFlow
- B. proxy
- C. firewall
- D. IDS/IPS

Answer: C

NEW QUESTION 10

What is the difference between discretionary access control (DAC) and role-based access control (RBAC)?

- A. DAC requires explicit authorization for a given user on a given object, and RBAC requires specific conditions.
- B. RBAC access is granted when a user meets specific conditions, and in DAC, permissions are applied on user and group levels.
- C. RBAC is an extended version of DAC where you can add an extra level of authorization based on time.
- D. DAC administrators pass privileges to users and groups, and in RBAC, permissions are applied to specific groups

Answer: A

NEW QUESTION 14

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: D

NEW QUESTION 18

What is the difference between deep packet inspection and stateful inspection?

- A. Deep packet inspection gives insights up to Layer 7, and stateful inspection gives insights only up to Layer 4.
- B. Deep packet inspection is more secure due to its complex signatures, and stateful inspection requires less human intervention.
- C. Stateful inspection is more secure due to its complex signatures, and deep packet inspection requires less human intervention.
- D. Stateful inspection verifies data at the transport layer and deep packet inspection verifies data at the application layer

Answer: B

NEW QUESTION 21

Which evasion technique is indicated when an intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources?

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

Answer: A

Explanation:

Resource exhaustion is a type of denial-of-service attack; however, it can also be used to evade detection by security defenses. A simple definition of resource exhaustion is “consuming the resources necessary to perform an action.” Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW QUESTION 26

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 30

Refer to the exhibit.

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 (DCLOUD-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 (DCLOUD-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 (DCLOUD-SOC LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp

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 32

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 35

Which two components reduce the attack surface on an endpoint? (Choose two.)

- A. secure boot
- B. load balancing
- C. increased audit log levels
- D. restricting USB ports
- E. full packet captures at the endpoint

Answer: AD

NEW QUESTION 38

Which information must an organization use to understand the threats currently targeting the organization?

- A. threat intelligence
- B. risk scores
- C. vendor suggestions
- D. vulnerability exposure

Answer: A

NEW QUESTION 41

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 43

Which security principle is violated by running all processes as root or administrator?

- A. principle of least privilege
- B. role-based access control
- C. separation of duties
- D. trusted computing base

Answer: A

NEW QUESTION 44

Which evasion technique is a function of ransomware?

- A. extended sleep calls
- B. encryption
- C. resource exhaustion
- D. encoding

Answer: B

NEW QUESTION 47

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 51

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 53

Which type of access control depends on the job function of the user?

- A. discretionary access control
- B. nondiscretionary access control
- C. role-based access control
- D. rule-based access control

Answer: C

NEW QUESTION 57

An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?

- A. sequence numbers
- B. IP identifier
- C. 5-tuple
- D. timestamps

Answer: C

NEW QUESTION 60

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 61

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 63

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

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

Answer: AB

NEW QUESTION 68

What are two categories of DDoS attacks? (Choose two.)

- A. split brain
- B. scanning
- C. phishing
- D. reflected
- E. direct

Answer: DE

NEW QUESTION 70

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 75

How does an attacker observe network traffic exchanged between two users?

- A. port scanning
- B. man-in-the-middle
- C. command injection
- D. denial of service

Answer: B

NEW QUESTION 79

Refer to the exhibit.

```
GET /item.php?id=34' or sleep(10)
```

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: D

NEW QUESTION 81

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 85

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 88

Which technology on a host is used to isolate a running application from other applications?

- A. sandbox
- B. application allow list
- C. application block list
- D. host-based firewall

Answer: A

NEW QUESTION 89

What should an engineer use to aid the trusted exchange of public keys between user tom0411976943 and dan1968754032?

- A. central key management server
- B. web of trust
- C. trusted certificate authorities
- D. registration authority data

Answer: C

NEW QUESTION 90

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 95

How does TOR alter data content during transit?

- A. It spoofs the destination and source information protecting both sides.
- B. It encrypts content and destination information over multiple layers.
- C. It redirects destination traffic through multiple sources avoiding traceability.
- D. It traverses source traffic through multiple destinations before reaching the receiver

Answer: B

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

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

Explanation:

A false negative occurs when the security system (usually a WAF) fails to identify a threat. It produces a "negative" outcome (meaning that no threat has been observed), even though a threat exists.

NEW QUESTION 103

Which metric is used to capture the level of access needed to launch a successful attack?

- A. privileges required
- B. user interaction
- C. attack complexity
- D. attack vector

Answer: D

Explanation:

Attack Vector (AV) represents the level of access an attacker needs to have to exploit a vulnerability. It can assume four values: Network, Adjacent, Local and Physical. Source: Official cert Guide Cisco CyberOps Associate CBROPS 200-201 Chapter7: Introduction to Security Operations Management.

NEW QUESTION 107

What is the difference between a threat and a risk?

- A. Threat represents a potential danger that could take advantage of a weakness in a system
- B. Risk represents the known and identified loss or danger in the system
- C. Risk represents the nonintentional interaction with uncertainty in the system
- D. Threat represents a state of being exposed to an attack or a compromise, either physically or logically.

Answer: A

Explanation:

A threat is any potential danger to an asset. If a vulnerability exists but has not yet been exploited—or, more importantly, it is not yet publicly known—the threat is latent and not yet realized.

NEW QUESTION 108

Refer to the exhibit.

```

443/tcp closed https
'nap done: 1. IP address (1 host up) scanned in 0.19 seconds
Ps C:\Program Files (x86)\Nmap> nmap --top-ports 10 172.31.45.240
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 22:05 Coordinated Universal Time
'nap scan report for ip-172-31-45-240.us-west-2.compute.internal (172.31.45.240)
Host is up (0.00s latency).

PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    closed http
110/tcp   closed pop3
139/tcp   open  netbios-ssn
443/tcp   closed https
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

'map done: 1 IP address (1 host up) scanned in 0.19 seconds PS
C:\Program Files (x86)\Nmap>

```

What does this output indicate?

- A. HTTPS ports are open on the server.
- B. SMB ports are closed on the server.
- C. FTP ports are open on the server.
- D. Email ports are closed on the server.

Answer: D

NEW QUESTION 112

Which utility blocks a host portscan?

- A. HIDS
- B. sandboxing
- C. host-based firewall
- D. antimalware

Answer: C

NEW QUESTION 113

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
18	0.011318	10.0.2.15	192.124.249.9	TCP	78	50588-443 [FIN] Seq=1
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443-50588 [SYN, ACK]
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588-443 [ACK] Seq=1
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443-50586 [SYN, ACK]
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=1
23	0.023212	10.0.2.15	192.124.249.9	TCP	261	50588-443 [PSH, ACK]
24	0.023373	10.0.2.15	192.124.249.9	TCP	261	50586-443 [PSH, ACK]
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443-50588 [ACK] Seq=1
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443-50586 [ACK] Seq=1
27	0.037413	192.124.249.9	10.0.2.15	TCP	2792	443-50586 [PSH, ACK]
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=2

> Frame 24: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
 > Linux cooked capture
 > Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)
 > Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, A
 > Data [205 bytes]
 Data: 16030100c8010000c403030e06ead078d17676c13ab46ebf...
 [Length: 205]

```

0000  00 04 00 01 00 06 08 00 27 7a 3c 93 00 00 08 00  ..... *z<.....
0010  45 00 00 f5 48 7b 40 00 40 06 2b f3 0a 00 02 0f  E...H{@. @.+.....
0020  c0 7c f9 09 c5 9a 01 bb 0e 1f dc b4 00 b4 aa 02  .|.....
0030  50 18 72 10 c6 7c 00 00 16 03 01 00 c8 01 00 00  P.r..|..
0040  c4 03 03 0e 06 ea d0 78 d1 76 76 c1 3a b4 6e bf  .....x .vv.:n..
0050  e6 b8 b8 b2 ba 08 d6 6d 0d 38 fb 91 45 de fc ee  .....m .8..E...
0060  8b 6e f8 00 00 1e c0 2b c0 2f cc a9 cc a8 c0 2c  .n.....+ ./.....
0070  c0 30 c0 0a c0 09 c0 13 c0 14 00 33 00 39 00 2f  .0..... ...3.9./
0080  00 35 00 0a 01 00 00 7d 00 00 00 16 00 14 00 00  .5.....} .....
0090  11 77 77 77 2e 6c 69 6e 75 78 6d 69 6e 74 2e 63  .wwwlin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 08 00  om.....
00b0  06 00 17 00 18 00 19 00 0b 00 02 01 00 00 23 00  .....
00c0  00 33 74 00 00 00 10 00 17 00 15 02 68 32 08 73  .3t..... .h2.s
00d0  70 64 79 2f 33 2e 31 08 68 74 74 70 2f 31 2e 31  pdy/3.1. http/1.1
00e0  00 05 00 05 01 00 00 00 00 00 0d 00 18 00 16 04  .....
00f0  01 05 01 06 01 02 01 04 03 05 03 06 03 02 03 05  .....
0100  02 04 02 02 02  .....
  
```

Which application protocol is in this PCAP file?

- A. SSH
- B. TCP
- C. TLS
- D. HTTP

Answer: D

NEW QUESTION 115

An analyst is exploring the functionality of different operating systems.

What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?

- A. queries Linux devices that have Microsoft Services for Linux installed
- B. deploys Windows Operating Systems in an automated fashion
- C. is an efficient tool for working with Active Directory
- D. has a Common Information Model, which describes installed hardware and software

Answer: D

NEW QUESTION 120

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.003987	10.128.0.2	10.0.0.2	TCP	58	88 - 3222 [SYN, ACK] Seq=0 Ack=1 Win=29288 Len=0 NSS=1468
3	0.005514	10.128.0.2	10.0.0.2	TCP	58	88 - 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
4	0.008429	10.0.0.2	10.128.0.2	TCP	54	3342 - 80 [SYN] Seq=0 Win=512 Len=0
5	0.010233	10.128.0.2	10.0.0.2	TCP	58	88 - 3220 [SYN, ACK] Seq=0 Ack=1 Win=2988 Len=0 NSS=1468
6	0.014072	10.128.0.2	10.0.0.2	TCP	58	80 - 3342 [SYN, ACK] Seq=0 Ack=1 Win=2900 Len=0 NSS=1460
7	0.016830	10.0.0.2	10.128.0.2	TCP	54	3343 - 88 [SYN] Seq=0 Win=512 Len=0
8	0.022220	10.128.0.2	10.0.0.2	TCP	58	89 - 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
9	0.023496	10.128.0.2	10.0.0.2	TCP	58	89 - 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
10	0.025243	10.0.0.2	10.128.0.2	TCP	54	3344 - 88 [SYN] Seq=0 Win=512 Len=0
11	0.026672	10.128.0.2	10.0.0.2	TCP	58	89 - 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
12	0.028038	10.128.0.2	10.0.0.2	TCP	58	80 - 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
13	0.030523	10.128.0.2	10.0.0.2	TCP	58	88 - 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460


```

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)
Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.128.0.2
Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 3341
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  [Next sequence number: 0 (relative sequence number)]
  * Acknowledgement number: 1023350884
  0101 ... = Header Length: 20 bytes (5)
  * Flags: 0x002 (SYN)
  Windows Size Value: 512
  [Calculated window size: 512]
  Checksum: 0x8d5a [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  * [Timestamps]
    
```

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. High rate of ACK packets being sent from a single source IP towards multiple destination IPs.
- C. Flood of ACK packets coming from a single source IP to multiple destination IPs.
- D. Flood of SYN packets coming from a single source IP to a single destination IP.

Answer: D

NEW QUESTION 123

Refer to the exhibit.

```
Aug 24 2020 09:02:37: %ASA-4-106023: Deny tcp src outside:209.165.200.228/51585 dst
inside:192.168.150.77/22 by access-group "OUTSIDE" [0x5063b82f, 0x0]
```

An analyst received this alert from the Cisco ASA device, and numerous activity logs were produced. How should this type of evidence be categorized?

- A. indirect
- B. circumstantial
- C. corroborative
- D. best

Answer: C

Explanation:

Indirect=circumstantial so there is no possibility to match A or B (only one answer is needed in this question). For user it's not a BEST evidence - this FW data inform only of DROPPED traffic. If smth happend inside network, presented evidence could be used to support other evidences or make our narreation stronger but alone it's mean nothing.

NEW QUESTION 126

A security incident occurred with the potential of impacting business services. Who performs the attack?

- A. malware author
- B. threat actor
- C. bug bounty hunter
- D. direct competitor

Answer: B

NEW QUESTION 131

An offline audit log contains the source IP address of a session suspected to have exploited a vulnerability resulting in system compromise. Which kind of evidence is this IP address?

- A. best evidence
- B. corroborative evidence
- C. indirect evidence
- D. forensic evidence

Answer: B

NEW QUESTION 135

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 139

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 142

What is an incident response plan?

- A. an organizational approach to events that could lead to asset loss or disruption of operations
- B. an organizational approach to security management to ensure a service lifecycle and continuous improvements
- C. an organizational approach to disaster recovery and timely restoration of operational services
- D. an organizational approach to system backup and data archiving aligned to regulations

Answer: C

NEW QUESTION 143

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 146

What is a description of a social engineering attack?

- A. fake offer for free music download to trick the user into providing sensitive data
- B. package deliberately sent to the wrong receiver to advertise a new product
- C. mistakenly received valuable order destined for another person and hidden on purpose
- D. email offering last-minute deals on various vacations around the world with a due date and a counter

Answer: D

NEW QUESTION 147

How does a certificate authority impact security?

- A. It validates client identity when communicating with the server.
- B. It authenticates client identity when requesting an SSL certificate.
- C. It authenticates domain identity when requesting an SSL certificate.
- D. It validates the domain identity of the SSL certificate.

Answer: D

Explanation:

A certificate authority is a computer or entity that creates and issues digital certificates. CA do not "authenticate" it validates. "D" is wrong because The digital certificate validate a user. CA --> DC --> user, server or whatever.

NEW QUESTION 149

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 151

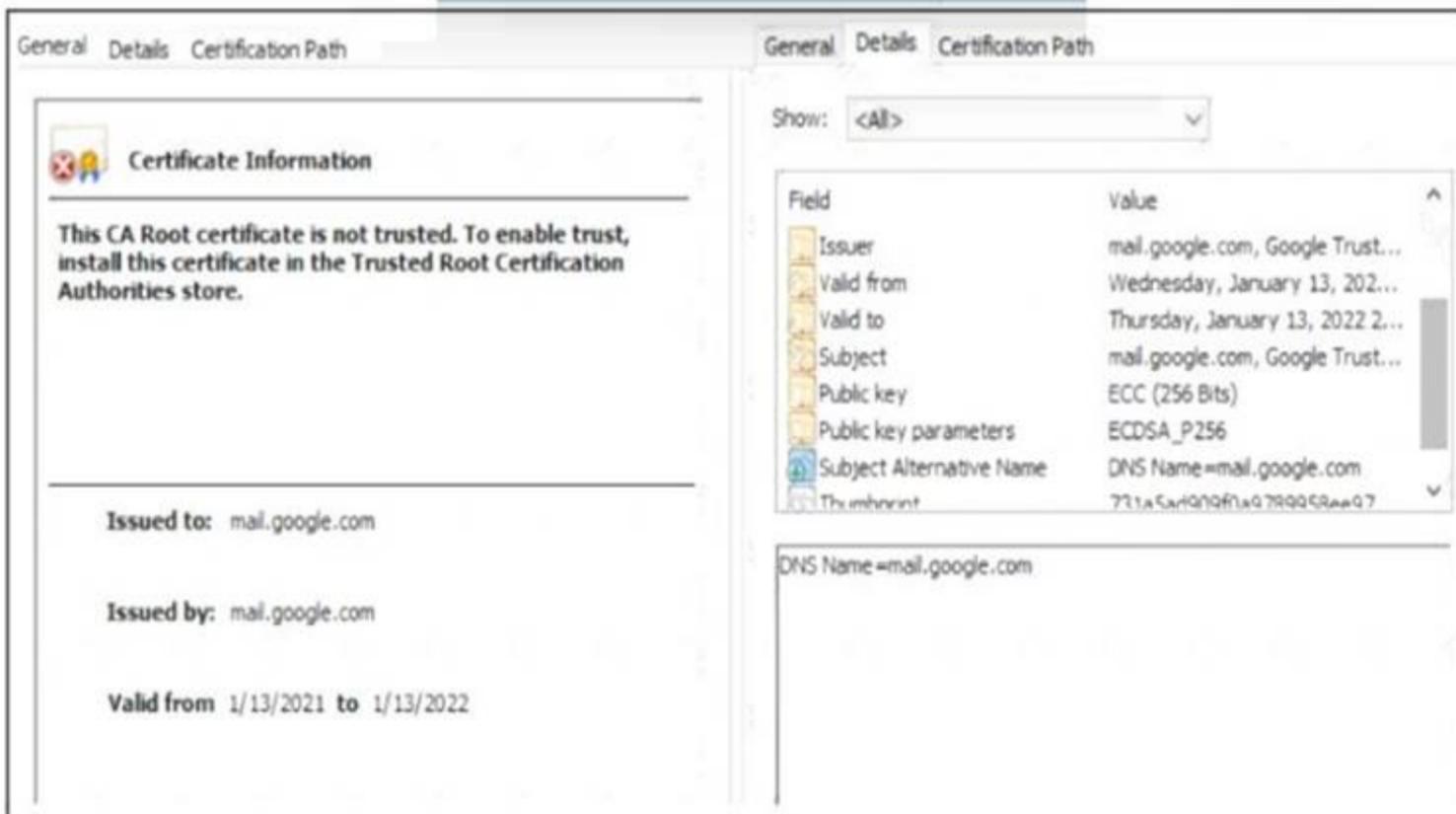
A user received a malicious attachment but did not run it. Which category classifies the intrusion?

- A. weaponization
- B. reconnaissance
- C. installation
- D. delivery

Answer: D

NEW QUESTION 153

Refer to the exhibit.



A company employee is connecting to mail.google.com from an endpoint device. The website is loaded but with an error. What is occurring?

- A. DNS hijacking attack
- B. Endpoint local time is invalid.
- C. Certificate is not in trusted roots.
- D. man-in-the-middle attack

Answer: C

NEW QUESTION 157

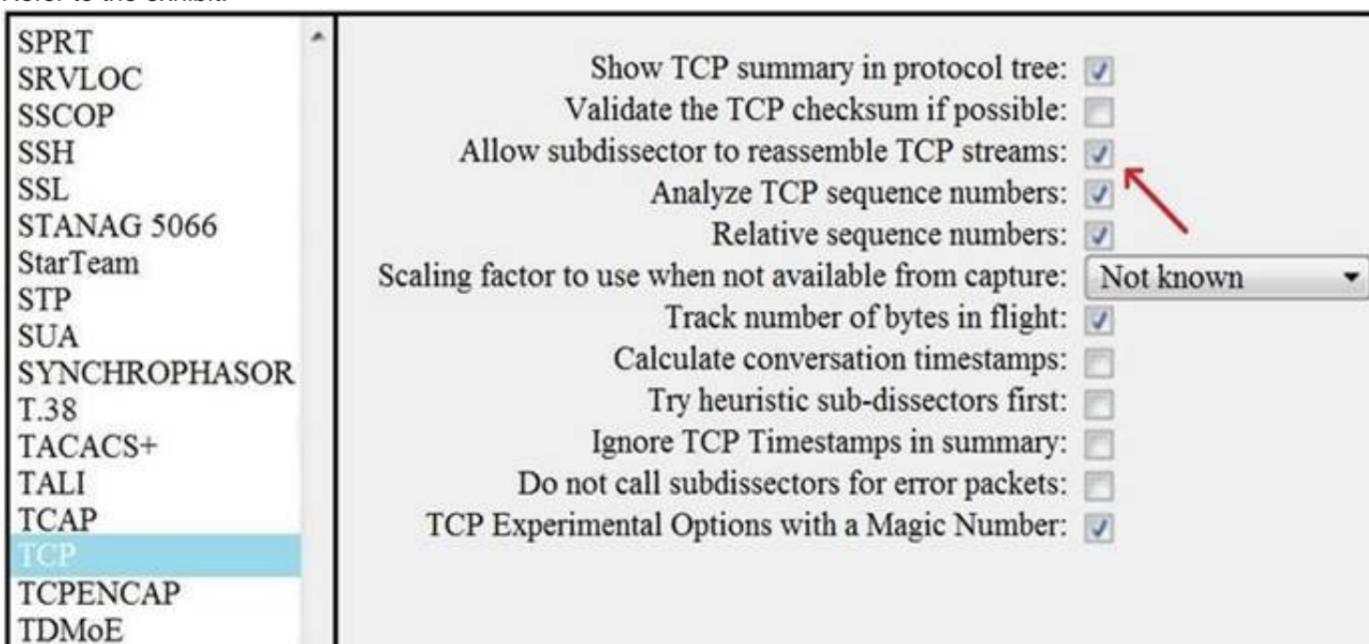
Which attack represents the evasion technique of resource exhaustion?

- A. SQL injection
- B. man-in-the-middle
- C. bluesnarfing
- D. denial-of-service

Answer: D

NEW QUESTION 158

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. extract a file from a packet capture
- C. disable TCP streams
- D. unfragment TCP

Answer: D

NEW QUESTION 163

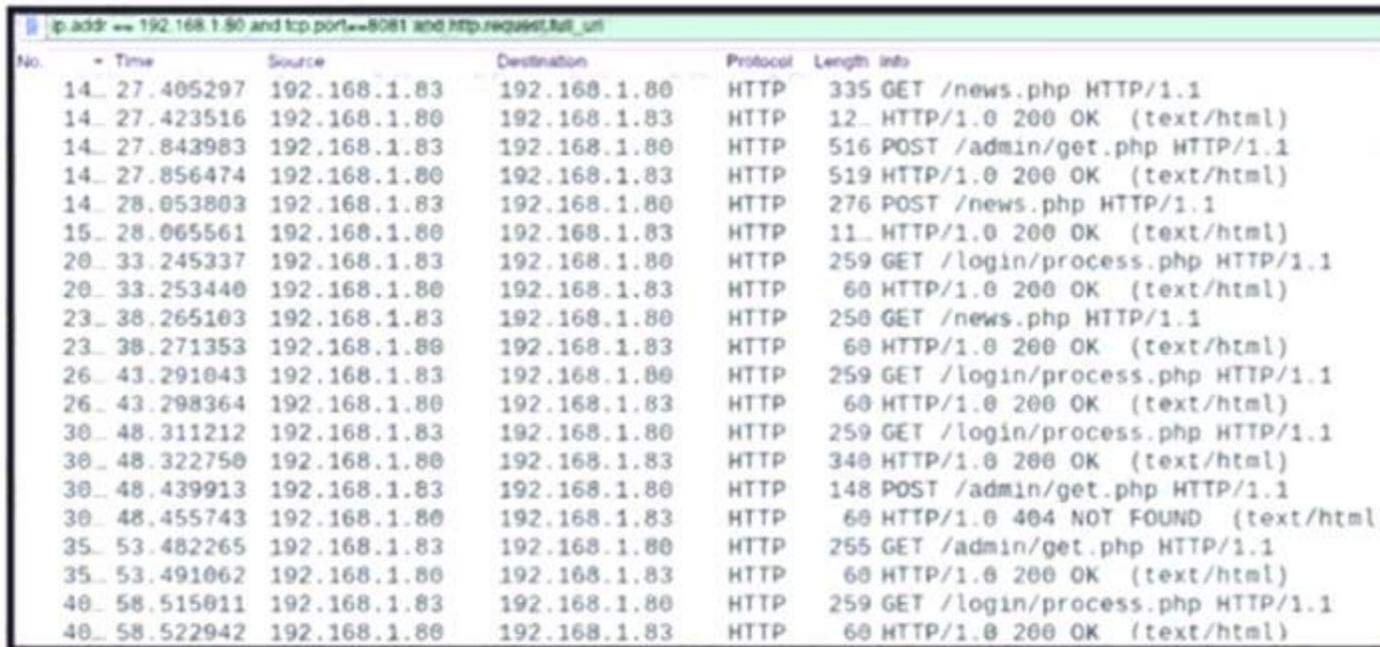
What is indicated by an increase in IPv4 traffic carrying protocol 41 ?

- A. additional PPTP traffic due to Windows clients
- B. unauthorized peer-to-peer traffic
- C. deployment of a GRE network on top of an existing Layer 3 network
- D. attempts to tunnel IPv6 traffic through an IPv4 network

Answer: D

NEW QUESTION 165

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 168

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 171

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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 First Try
- * 200-201 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 200-201 Practice Test Here](#)