https://www.leads4pass.com/200-201.html
Vendor: Cisco
Exam Code: 200-201
Exam Name: Understanding Cisco Cybersecurity Operations Fundamentals
Certification: CCNA Cybersecurity
Total Questions: 491 Q&A (View Details)
Updated on: Mar 09, 2026

Question 1:
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

Correct Answer: C

Reference: https://www.brinqa.com/vulnerability-management-primer-part-2-challenges/

Vulnerability management is the "cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating" software vulnerabilities.[1] Vulnerability management is integral to computer security and network security, and must not be confused with Vulnerability assessment" source: https://en.wikipedia.org/wiki/Vulnerability_management

---

Question 2:
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

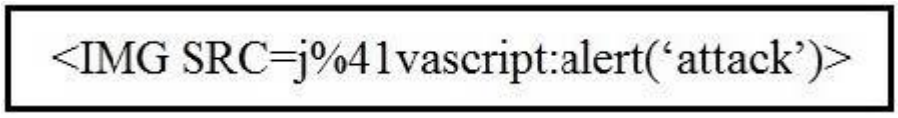
C. ip.src=10.11.0.0/16 and ip.dst=10.11.0.0/16

D. src==10.11.0.0/16 and dst==10.11.0.0/16

Correct Answer: B

Question 3:

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

Correct Answer: A

Question 4:
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

Correct Answer: AB

Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

---

Question 5:
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

Correct Answer: C

Question 6:
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

Correct Answer: B

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

Correct Answer: D

Question 8:
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$

Correct Answer: A

Question 9:
What is a benefit of using asymmetric cryptography?

A. decrypts data with one key

B. fast data transfer

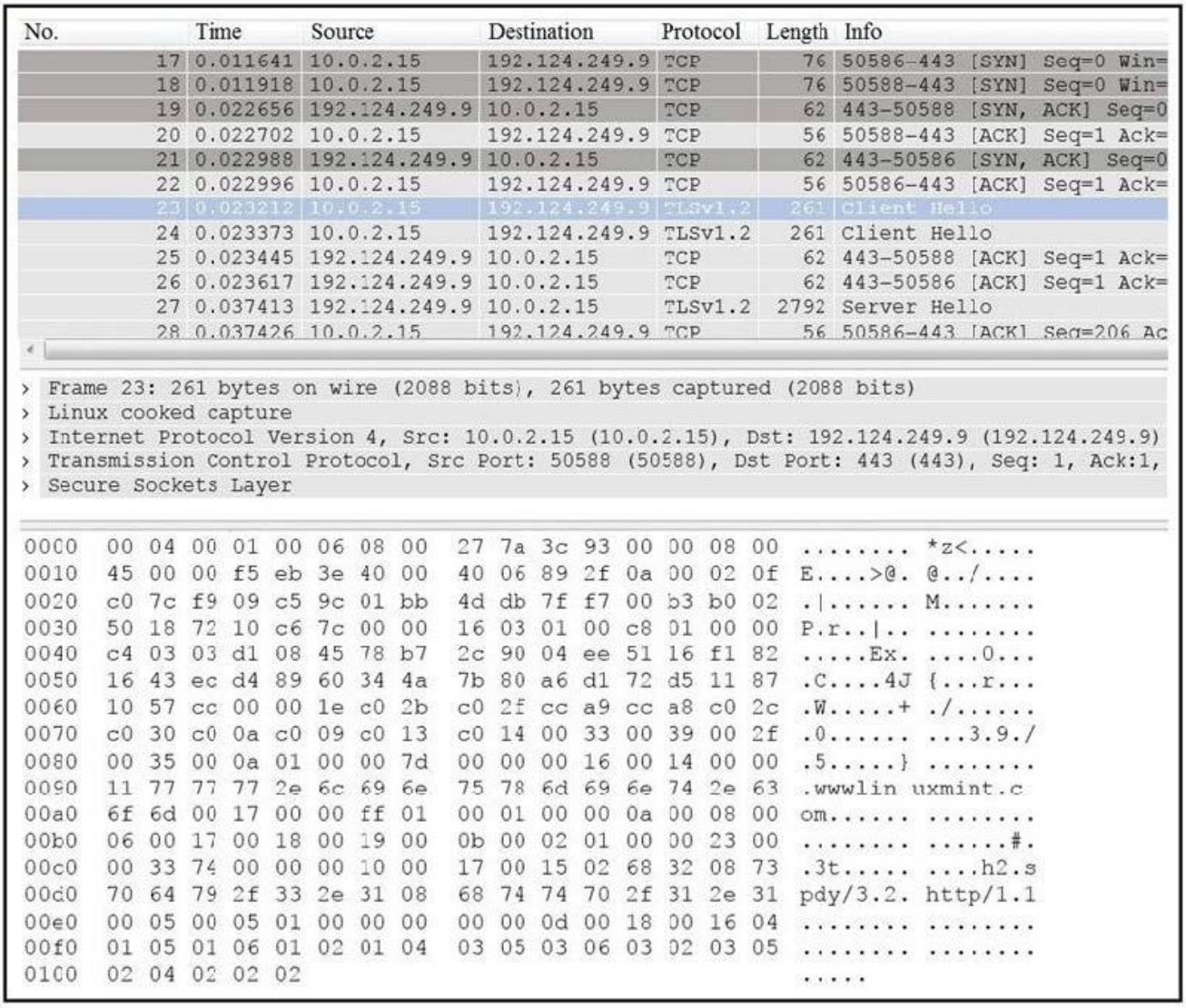
C. secure data transfer

D. encrypts data with one key

Correct Answer: C

Question 10:
DRAG DROP

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.

Select and Place:

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

Correct Answer:

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

Question 11:
A company plans to implement network segmentations and use IP address inventory management best practices. Servers and end-user devices are using the same VLANs and IP subnets with manual address assignment. What are the first two steps the engineers must take to meet these requirements? (Choose two.)

A. Configure packet captures to perform deep packet inspection for further traffic analysis and implementation of access rules.

B. Implement deep network traffic analysis using NetFlow v5 from routers and switches.

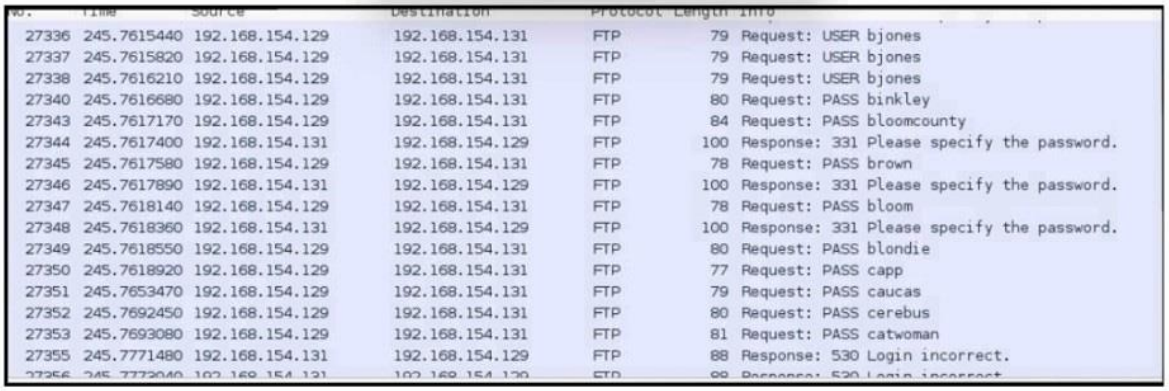
C. Deploy an Active Directory server and add all assets to the created domain for better visibility.

D. Assign separate hard-coded IP address spaces for critical assets, according to their role and functions.

E. Create IP address inventory database and deploy separate role-based IP subnetting for users using centralized DHCP server.

Correct Answer: DE

Question 12:
Refer to the exhibit.



No.	Time	Source	Destination	Protocol	Length	Info
27336	245.7615440	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27337	245.7615820	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27338	245.7616210	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27340	245.7616680	192.168.154.129	192.168.154.131	FTP	80	Request: PASS binkley
27343	245.7617170	192.168.154.129	192.168.154.131	FTP	84	Request: PASS bloomcounty
27344	245.7617400	192.168.154.131	192.168.154.129	FTP	100	Response: 331 Please specify the password.
27345	245.7617580	192.168.154.129	192.168.154.131	FTP	78	Request: PASS brown
27346	245.7617890	192.168.154.131	192.168.154.129	FTP	100	Response: 331 Please specify the password.
27347	245.7618140	192.168.154.129	192.168.154.131	FTP	78	Request: PASS bloom
27348	245.7618360	192.168.154.131	192.168.154.129	FTP	100	Response: 331 Please specify the password.
27349	245.7618550	192.168.154.129	192.168.154.131	FTP	80	Request: PASS blondie
27350	245.7618920	192.168.154.129	192.168.154.131	FTP	77	Request: PASS capp
27351	245.7653470	192.168.154.129	192.168.154.131	FTP	79	Request: PASS caucas
27352	245.7692450	192.168.154.129	192.168.154.131	FTP	80	Request: PASS cerebus
27353	245.7693080	192.168.154.129	192.168.154.131	FTP	81	Request: PASS catwoman
27355	245.7771480	192.168.154.131	192.168.154.129	FTP	88	Response: 530 Login incorrect.

An analyst was given a PCAP file, which is associated with a recent intrusion event in the company FTP server Which display filters should the analyst use to filter the FTP traffic?

A. dstport == FTP

B. tcp.port==21

C. tcpport = FTP

D. dstport = 21

Correct Answer: B

Question 13:

A user received a targeted spear-phishing email and identified it as suspicious before opening the content. To which category of the Cyber Kill Chain model does to this type of event belong?

A. weaponization

B. delivery

C. exploitation

D. reconnaissance

Correct Answer: B

Question 14:
Which vulnerability type is used to read, write, or erase information from a database?

A. cross-site scripting

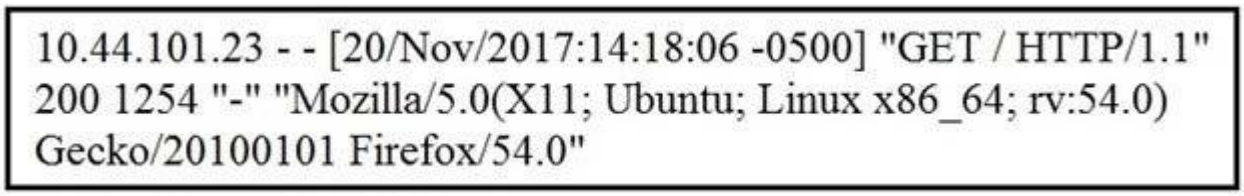
B. cross-site request forgery

C. buffer overflow

D. SQL injection

Correct Answer: D

Question 15:
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

Correct Answer: C