https://www.geekcert.com/200-201.html
Geekcert.com

200-201^{Q&As}

200-201^{Q&As}

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/200-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

💠 **Instant Download** After Purchase

💠 **100% Money Back** Guarantee

💠 **365 Days** Free Update

💠 **800,000+** Satisfied Customers

QUESTION 1
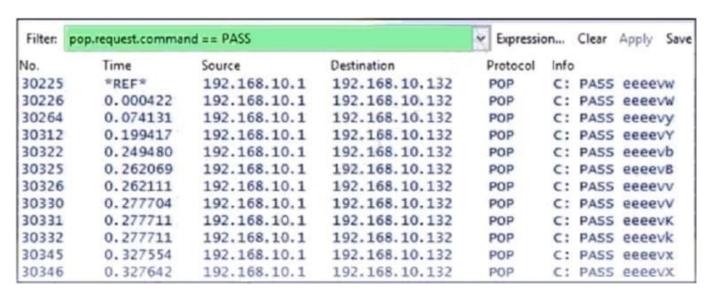
Which CVSS metric group identifies other components that are affected by a successful security attack?

A. scope

B. privileges required

C. integrity

D. attack vendor

Correct Answer: A

QUESTION 2

Refer to the exhibit.

Filter:	pop.request.command == PASS			Expression...	Clear	Apply	Save

No.	Time	Source	Destination	Protocol	Info		
30225	*REF*	192.168.10.1	192.168.10.132	POP	C: PASS eeeevw		
30226	0.000422	192.168.10.1	192.168.10.132	POP	C: PASS eeeevw		
30264	0.074131	192.168.10.1	192.168.10.132	POP	C: PASS eeeevy		
30312	0.199417	192.168.10.1	192.168.10.132	POP	C: PASS eeeevY		
30322	0.249480	192.168.10.1	192.168.10.132	POP	C: PASS eeeevb		
30325	0.262069	192.168.10.1	192.168.10.132	POP	C: PASS eeeevB		
30326	0.262111	192.168.10.1	192.168.10.132	POP	C: PASS eeeevv		
30330	0.277704	192.168.10.1	192.168.10.132	POP	C: PASS eeeevV		
30331	0.277711	192.168.10.1	192.168.10.132	POP	C: PASS eeeevK		
30332	0.277711	192.168.10.1	192.168.10.132	POP	C: PASS eeeevk		
30345	0.327554	192.168.10.1	192.168.10.132	POP	C: PASS eeeevx		
30346	0.327642	192.168.10.1	192.168.10.132	POP	C: PASS eeeevX		

Which alert is identified from this packet capture?

A. man-in-the-middle attack

B. brute-force attack

C. ARP poisoning

D. SQL injection

Correct Answer: B

QUESTION 3

Refer to the exhibit.

```
192.168.10.10 – – [01/Dec/2020:11:12:22 -0200] "GET /icons/powered_by_rh.png HTT
P/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-U
S; 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 2
88 "-" "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

Correct Answer: A

Reference: https://www.tutorialspoint.com/http/http_requests.htm
https://github.com/gwroblew/detectXSSlib/blob/master/test/attacks.txt

QUESTION 4

Which type of verification consists of using tools to compute the message digest of the original and copied data, then comparing the similarity of the digests?

A. evidence collection order

B. data integrity

C. data preservation

D. volatile data collection

Correct Answer: B

QUESTION 5

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

Correct Answer: AB

200-201 PDF Dumps   200-201 Exam Questions   200-201 Braindumps