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
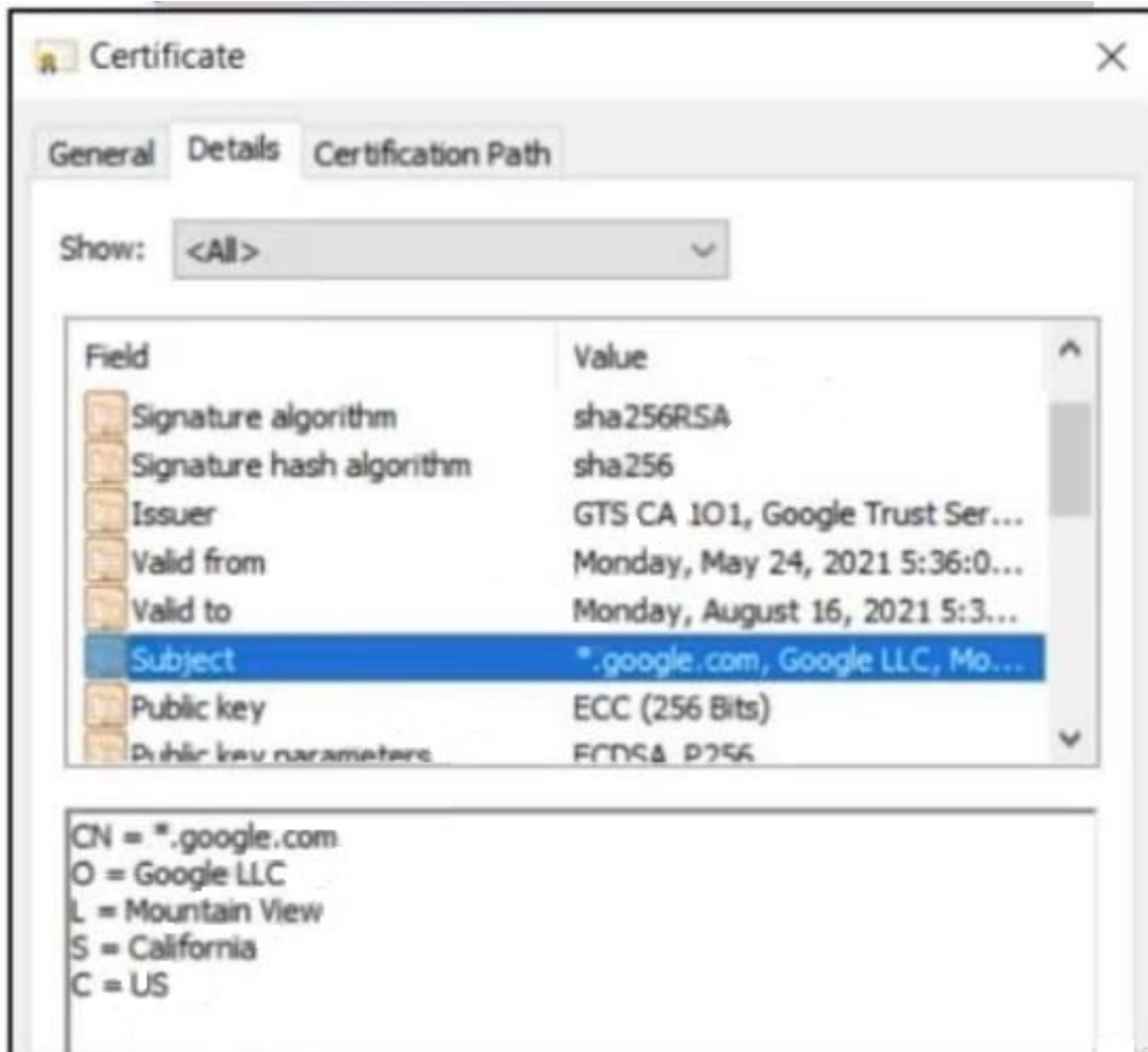
100% Passing Guarantee
100% Money Back Assurance

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

Refer to the exhibit.

An engineer needs to identify certificate information on server1234567890. What does the exhibit indicate?

A. Elliptic-curve cryptography is used for the public keys.

B. Key exchange is not secure as the SHA256 hashing algorithm is used.

C. The certificate is signed by GTS CA on May 24 and is invalid.

D. Asymmetric cryptography is used for key exchange.

Correct Answer: A

QUESTION 2

Refer to the exhibit.

Summary		⬇ Download ⟳ Resubmit sample
Size	28.5KB	
Type	PE32 executable (console) Intel 80386, for MS Windows	
MD5	1f4c06b2e4dd2943934e05348b17f974	
SHA1	aa5fbc5a4e98cbeb359caf34a6cd3a721a3bf9d9	
SHA256	b232641eb80eb1a050630de7aac1ac4805c84559ec03103a4677eccdd7ad1ee6	
SHA512	Show SHA512	
CRC32	AABE8BB6	
ssdeep	None	
PDB Path	\\vmware-host\Shared Folders\Documents\121file\crackme-121-3\Debug\crackme-121-3.pdb	
Yara	• vmdetect • anti_dbg	

An engineer is reviewing a Cuckoo report of a file. What must the engineer interpret from the report?

A. The file will appear legitimate by evading signature-based detection.

B. The file will not execute its behavior in a sandbox environment to avoid detection.

C. The file will insert itself into an application and execute when the application is run.

D. The file will monitor user activity and send the information to an outside source.

Correct Answer: B

QUESTION 3

What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?

A. MAC is controlled by the discretion of the owner and DAC is controlled by an administrator

B. MAC is the strictest of all levels of control and DAC is object-based access

C. DAC is controlled by the operating system and MAC is controlled by an administrator

D. DAC is the strictest of all levels of control and MAC is object-based access

Correct Answer: B

QUESTION 4

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

Correct Answer: A

QUESTION 5

Refer to the exhibit.

```
Nov 30 17:48:38 ip-172-31-27-153 sshd[22997]: Invalid user password from 218.26.11.11
Nov 30 17:48:39 ip-172-31-27-153 sshd[22997]: Invalid user password from 218.26.11.11
Nov 30 17:48:41 ip-172-31-27-153 sshd[22999]: Invalid user password from 218.26.11.11
Nov 30 17:48:41 ip-172-31-27-153 sshd[22999]: Invalid user password from 218.26.11.11
Nov 30 17:48:41 ip-172-31-27-153 sshd[22999]: Invalid user password from 218.26.11.11
Nov 30 17:48:41 ip-172-31-27-153 sshd[22999]: Invalid user password from 218.26.11.11
Nov 30 17:48:43 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:43 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:43 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:49 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
Nov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
```

A security analyst is investigating unusual activity from an unknown IP address Which type of evidence is this file1?

A. indirect evidence

B. best evidence

C. corroborative evidence

D. direct evidence

Correct Answer: D

200-201 PDF Dumps   200-201 Practice Test   200-201 Exam Questions