Latest 300-215 Exam Test | 300-215 Study Group

P.S. Free 2026 Cisco 300-215 dumps are available on Google Drive shared by Itexamguide: https://drive.google.com/open?id=12Ivsl3vMIOiINzFNI6w8JrRcTivg2hUg

If you want to be familiar with the real test and grasp the rhythm in the real test, you can choose our 300-215 exam test engine to practice. Both our soft test engine and app test engine provide the exam scene simulation functions. You set timed 300-215 test and practice again and again. Besides, 300-215 exam test engine cover most valid test questions so that it can guide you and help you have a proficient & valid preparation process.

Prerequisites

The Cisco 300-215 CBRFIR exam does not have any formal requirements. However, it is recommended that the candidates have between three and five years of practical experience in implementing different enterprise networking solutions. It is also pretty important to be familiar with the content of the test.

Cisco 300-215 certification exam is designed to validate the knowledge and skills of professionals in conducting forensic analysis and incident response using Cisco technologies for CyberOps. Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps certification exam is ideal for security professionals, incident responders, and forensic analysts who want to advance their careers in cybersecurity.

>> Latest 300-215 Exam Test <<

Free PDF Cisco - 300-215 - Professional Latest Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps Exam Test

It doesn't matter if it's your first time to attend 300-215 practice test or if you are freshman in the IT certification test, our latest 300-215 dumps guide will boost you confidence to face the challenge. Our dumps collection will save you much time and ensure you get high mark in 300-215 Actual Test with less effort. Come and check the free demo in our website you won't regret it.

Cisco 300-215 Certification Exam is designed to measure the competency of professionals in conducting forensic analysis and incident response using Cisco technologies for CyberOps. Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps certification exam is suitable for security analysts, network security engineers, cybersecurity operations center (SOC) analysts, and incident response teams.

Cisco Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps Sample Questions (Q39-Q44):

NEW QUESTION # 39
A scanner detected a malware-infected file on an endpoint that is attempting to beacon to an external site. An analyst has reviewed the IPS and SIEM logs but is unable to identify the file's behavior. Which logs should be reviewed next to evaluate this file further?

- A. email security appliance
- B. network device
- C. Antivirus solution
- D. DNS server

Answer: C

Explanation:
If IPS and SIEM logs do not give enough insight into a file's behavior, the next logical step is to review the Antivirus solutionlogs.
These logs often provide detailed behavior analytics such as:
* File actions and access patterns
* Registry modifications
* File execution history
The Cisco CyberOps guide emphasizes AV logs as critical forensic artifacts for understanding endpoint-based infections, especially when beaconing or suspicious activity is suspected.

NEW QUESTION # 40
What is the steganography anti-forensics technique?

- A. sending malicious files over a public network by encapsulation
- B. concealing malicious files in ordinary or unsuspecting places
- C. changing the file header of a malicious file to another file type
- D. hiding a section of a malicious file in unused areas of a file

Answer: B

Explanation:
Steganography is the anti-forensics technique of hiding malicious content within seemingly innocent files, such as image, audio, or video files. The goal is to conceal data or code in a way that avoids suspicion and detection, thereby making traditional security inspection tools ineffective unless they are explicitly designed to detect hidden data within media files.
Steganography differs from encryption because it does not simply make data unreadable; it hides the existence of the data itself. It is commonly used in cyber operations to hide command-and-control instructions or to exfiltrate sensitive information in covert ways.
Reference:CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Evasion and Obfuscation Techniques, Anti-Forensics, Steganography Section.

NEW QUESTION # 41
Refer to the exhibit.

```
New-Item -Path HKCU:\Software\Classes -Name Folder -Force;
New-Item -Path HKCU:\Software\Classes\Folder -Name shell -Force;
New-Item -Path HKCU:\Software\Classes\Folder\shell -Name open -Force;
New-Item -Path HKCU:\Software\Classes\Folder\shell\open -Name command -Force;
Set-ItemProperty -Path "HKCU:\Software\Classes\Folder\shell\open\command" -Name "(Default)"
Set-ItemProperty -Path "HKCU:\Software\Classes\Folder\shell\open\command" -Name "DelegateExecute" -Force
```

What does the exhibit indicate?

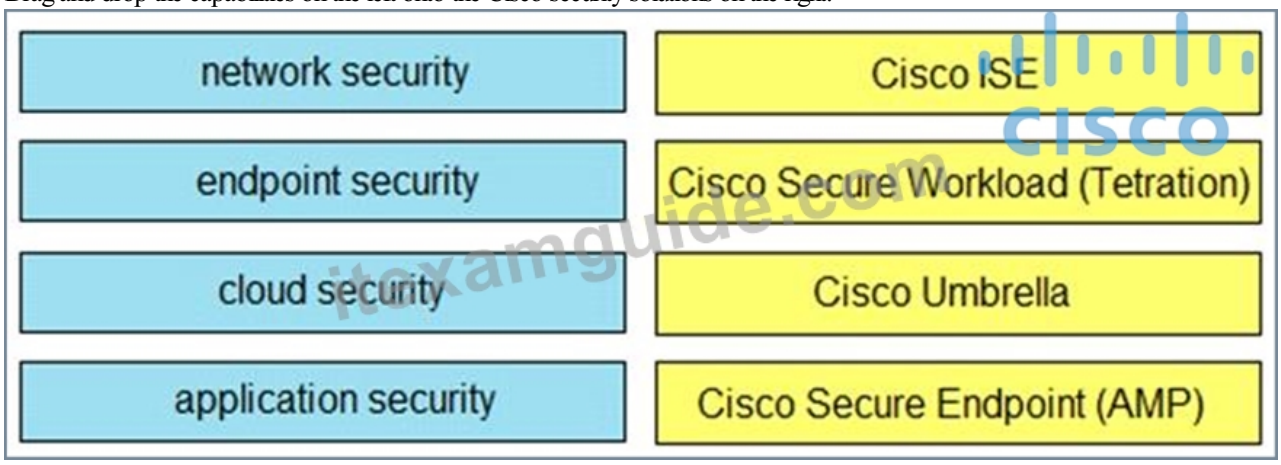
- A. A UAC bypass is created by modifying user-accessible registry settings.
- B. A scheduled task named "DelegateExecute" is created.
- C. The new file is created under the Software\Classes disk folder.
- D. The shell software is modified via PowerShell.

Answer: A

Explanation:
The exhibit shows a PowerShell script that modifies registry keys under:
* HKCU:\Software\Classes\Folder\shell\open\command
This technique is commonly associated with a UAC (User Account Control) bypass. Specifically:
* It creates a new custom shell command path for opening folders.
* The key registry property "DelegateExecute" is set, which is a known bypass method. If set without a value, it may cause Windows to run commands with elevated privileges without showing the UAC prompt.
The use of HKCU (HKEY_CURRENT_USER) rather than HKLM (HKEY_LOCAL_MACHINE) allows the attacker to bypass

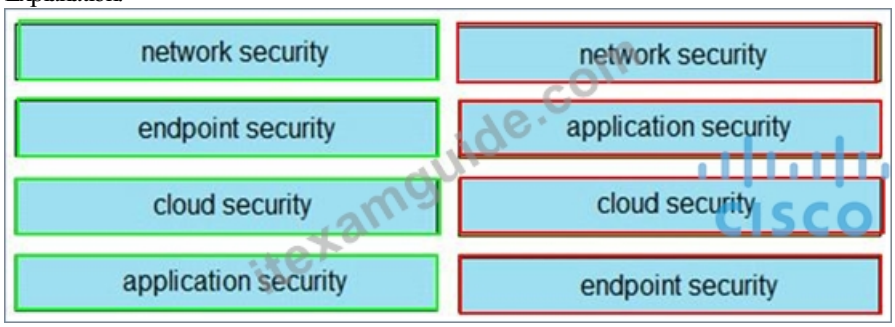
permissions since HKCU is writable by the current user. This registry hijack can be leveraged by a malicious actor to execute arbitrary commands with elevated rights.
This is identified in the Cisco CyberOps study material under "UAC bypass techniques," which describes:
"Attackers often create or modify registry keys like DelegateExecute to hijack the default behavior of applications and elevate privileges".
Thus, option B is correct: the exhibit demonstrates a UAC bypass using user-accessible registry modification.

NEW QUESTION # 42
Drag and drop the capabilities on the left onto the Cisco security solutions on the right.

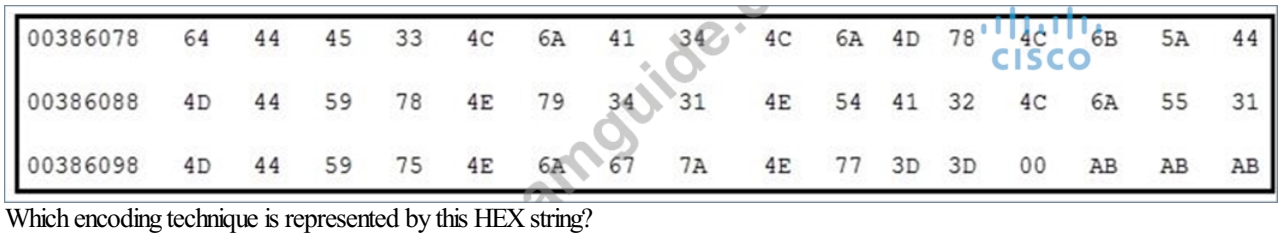


Answer:

Explanation:



NEW QUESTION # 43
Refer to the exhibit.



00386078	64	44	45	33	4C	6A	41	34	4C	6A	4D	78	4C	6B	5A	44
00386088	4D	44	59	78	4E	79	34	31	4E	54	41	32	4C	6A	55	31
00386098	4D	44	59	75	4E	6A	67	7A	4E	77	3D	3D	00	AB	AB	AB

Which encoding technique is represented by this HEX string?

- A. Base64
- B. Unicode
- C. Charcode
- D. Binary

Answer: C

Explanation:
The hexadecimal representation in the exhibit does not match the Base64 encoding format, which uses ASCII characters (A-Z, a-z, 0-9, +, /) and often includes padding with=. This string is clearly hex and is more aligned withCharcode, where hexadecimal values represent individual characters based on ASCII values.

The Cisco CyberOps Associate guide refers to such encodings during forensic analysis and emphasizes identifying patterns in memory dumps, payloads, or logs. "Security professionals often decode hexadecimal strings to reveal ASCII representations, particularly when inspecting encoded payloads or character obfuscation techniques used in malware".

NEW QUESTION # 44

.....