CISCO 300-215 CBRFIR STUDY GUIDE PDF

Cisco CyberOps Professional Certification Questions & Answers

Details of the Exam-Syllabus-Questions

300-215

Cisco Certified CyberOps Specialist - CyberOps Forensic Analysis and Incident Response

55-65 Questions Exam – Variable (750-850 / 1000 Approx.) Cut Score – Duration of 90 minutes

Table of Contents:

Get an Overview of the 300-215 CBRFIR Certification: 2

Why Should You Earn the Cisco 300-215 Certification? 2

What Is the Cisco 300-215 CyberOps Professional Certification Exam Structure? 2

Enhance Knowledge with 300-215 Sample Questions: 3

What Study Guide Works Best in Acing the Cisco 300-215 CyberOps Professional Certification? 6

Explore the Syllabus Topics and Learn from the Core: 6

Make Your Schedule: 7

Get Expert Advice from the Training: 7

Get Access to the PDF Sample Questions: 7

Avoid Dumps and Utilize the Cisco 300-215 Practice Test: 7

Get an Overview of the 300-215 CBRFIR Certification:

Who should take the **300-215 exam**? This is the first question that comes to a candidate's mind when preparing for the CyberOps Professional certification. The 300-215 certification is suitable for candidates who are keen to earn knowledge on the CyberOps and grab their Cisco Certified CyberOps Specialist - CyberOps Forensic Analysis and Incident Response. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But 300-215 CBRFIR study guide PDF is here to solve the problem. 300-215 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the Cisco 300-215 Certification?

There are several reasons why one should grab the 300-215 certification.

- The CyberOps Professional certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the **Cisco Certified CyberOps Specialist - CyberOps Forensic Analysis and Incident Response** is a powerful qualification for a prosperous career.

What Is the Cisco 300-215 CyberOps Professional Certification Exam Structure?

Exam Name	Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps
Exam Number	300-215 CBRFIR
Exam Price	$300 USD
Duration	90 minutes

Number of Questions	55-65
Passing Score	Variable (750-850 / 1000 Approx.)
Recommended Training	**Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)**
Exam Registration	**PEARSON VUE**
Sample Questions	**Cisco 300-215 Sample Questions**
Practice Exam	**Cisco Certified CyberOps Specialist - CyberOps Forensic Analysis and Incident Response Practice Test**

Enhance Knowledge with 300-215 Sample Questions:

Question: 1

Over the last year, an organization's HR department has accessed data from its legal department on the last day of each month to create a monthly activity report.

An engineer is analyzing suspicious activity alerted by a threat intelligence platform that an authorized user in the HR department has accessed legal data daily for the last week.

The engineer pulled the network data from the legal department's shared folders and discovered above average-size data dumps. Which threat actor is implied from these artifacts?

a) privilege escalation
b) internal user errors
c) malicious insider
d) external exfiltration

Answer: c

Question: 2

Which technique is used to evade detection from security products by executing arbitrary code in the address space of a separate live operation?

a) process injection
b) privilege escalation
c) GPO modification
d) token manipulation

Answer: a

Question: 3

Which information is provided bout the object file by the “-h” option in the objdump line command objdump –b oasys –m vax –h fu.o?

a) bfdname
b) debugging
c) headers
d) help

Answer: c

Question: 4

A security team receives reports of multiple files causing suspicious activity on users’ workstations. The file attempted to access highly confidential information in a centralized file server.

Which two actions should be taken by a security analyst to evaluate the file in a sandbox?

(Choose two.)

a) Inspect registry entries
b) Inspect processes.
c) Inspect file hash.
d) Inspect file type.
e) Inspect PE header.

Answer: b, c

Question: 5

A security team detected an above-average amount of inbound tcp/135 connection attempts from unidentified senders. The security team is responding based on their incident response playbook.

Which two elements are part of the eradication phase for this incident? (Choose two.)

a) anti-malware software
b) data and workload isolation
c) centralized user management
d) intrusion prevention system
e) enterprise block listing solution

Answer: c, d

Question: 6

What is the steganography anti-forensics technique?

a) hiding a section of a malicious file in unused areas of a file
b) changing the file header of a malicious file to another file type
c) sending malicious files over a public network by encapsulation
d) concealing malicious files in ordinary or unsuspecting places

Answer: d

Question: 7

What is a concern for gathering forensics evidence in public cloud environments?

a) High Cost: Cloud service providers typically charge high fees for allowing cloud forensics.
b) Configuration: Implementing security zones and proper network segmentation.
c) Timeliness: Gathering forensics evidence from cloud service providers typically requires substantial time.
d) Multitenancy: Evidence gathering must avoid exposure of data from other tenants.

Answer: d

Question: 8

A security team received an alert of suspicious activity on a user's Internet browser. The user's anti-virus software indicated that the file attempted to create a fake recycle bin folder and connect to an external IP address.

Which two actions should be taken by the security analyst with the executable file for further analysis?

(Choose two.)

a) Evaluate the process activity in Cisco Umbrella.
b) Analyze the TCP/IP Streams in Cisco Secure Malware Analytics (Threat Grid).
c) Evaluate the behavioral indicators in Cisco Secure Malware Analytics (Threat Grid).
d) Analyze the Magic File type in Cisco Umbrella.
e) Network Exit Localization in Cisco Secure Malware Analytics (Threat Grid).

Answer: b, c

Question: 9

What is the function of a disassembler?

a) aids performing static malware analysis
b) aids viewing and changing the running state
c) aids transforming symbolic language into machine code
d) aids defining breakpoints in program execution

Answer: a

Question: 10

An engineer received a call to assist with an ongoing DDoS attack. The Apache server is being targeted, and availability is compromised. Which step should be taken to identify the origin of the threat?

a) An engineer should check the list of usernames currently logged in by running the command $ who | cut – d' ' -f1| sort | uniq
b) An engineer should check the last hundred entries of a web server with the command sudo tail -100 /var/ log/apache2/access.log.
c) An engineer should check the services on the machine by running the command service -status-all.
d) An engineer should check the server's processes by running commands ps -aux and sudo ps -a.

Answer: b

What Study Guide Works Best in Acing the Cisco 300-215 CyberOps Professional Certification?

The 300-215 CBRFIR study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the CyberOps Professional exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus

sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the Cisco 300-215 training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and Utilize the Cisco 300-215 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, 300-215 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven 300-215 Practice Test for Success!!!

Do you want to pass the 300-215 exam on your first attempt? Stop worrying; we, NWExam.com are here to provide you the best experience during your Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **300-215 practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.