210-255

Implementing Cisco Cybersecurity Operations

NWExam.com

SUCCESS GUIDE TO CISCO CERTIFICATION

Exam Summary – Syllabus – Questions

Table of Contents

Introduction to 210-255 Exam on Implementing Cisco Cybersecurity Operations

A great way to start the Cisco Certified Network Associate Cyber Ops (SECOPS) preparation is to begin by properly appreciating the role that syllabus and study guide play in the Cisco 210-255 certification exam. This study guide is an instrument to get you on the same page with Cisco and understand the nature of the Cisco CCNA Cyber Ops exam.

Our team of experts has composed this Cisco 210-255 exam preparation guide to provide the overview about Cisco Implementing Cisco Cybersecurity Operations exam, study material, sample questions, practice exam and ways to interpret the exam objectives to help you assess your readiness for the Cisco SECOPS exam by identifying prerequisite areas of knowledge. We recommend you to refer the simulation questions and practice test listed in this guide to determine what type of questions will be asked and the level of difficulty that could be tested in the Cisco CCNA Cyber Ops certification exam.

Cisco 210-255 Certification Details:

Exam Name	Implementing Cisco Cybersecurity Operations
Exam Number	210-255 SECOPS
Exam Price	$300 USD
Duration	90 minutes
Number of Questions	50-60
Passing Score	Variable (750-850 / 1000 Approx.)
Recommended Training	Implementing Cisco Cybersecurity Operations (SECOPS)
Exam Registration	PEARSON VUE
Sample Questions	Cisco 210-255 Sample Questions
Practice Exam	**Cisco Certified Network Associate Cyber Ops Practice Test**

Cisco 210-255 Exam Syllabus:

Section	Weight	Objectives
Network Concepts	12%	1 Describe the function of the network layers as specified by the OSI and the TCP/IP network models 2 Describe the operation of the following a) IP b) TCP c) UDP d) ICMP 3 Describe the operation of these network services a) ARP b) DNS c) DHCP 4 Describe the basic operation of these network device types a) Router b) Switch c) Hub d) Bridge e) Wireless access point (WAP) f) Wireless LAN controller (WLC) 5 Describe the functions of these network security systems as deployed on the host, network, or the cloud: a) Firewall b) Cisco Intrusion Prevention System (IPS) c) Cisco Advanced Malware Protection (AMP) d) Web Security Appliance (WSA) / Cisco Cloud Web Security (CWS) e) Email Security Appliance (ESA) / Cisco Cloud Email Security (CES) 6 Describe IP subnets and communication within an IP subnet and between IP subnets 7 Describe the relationship between VLANs and data visibility 8 Describe the operation of ACLs applied as packet filters on the interfaces of network devices 9 Compare and contrast deep packet inspection with packet filtering and stateful firewall operation

Section	Weight	Objectives
		10 Compare and contrast inline traffic interrogation and taps or traffic mirroring 11 Compare and contrast the characteristics of data obtained from taps or traffic mirroring and NetFlow in the analysis of network traffic 12 Identify potential data loss from provided traffic profiles
Security Concepts	17%	1 Describe the principles of the defense in depth strategy 2 Compare and contrast these concepts a) Risk b) Threat c) Vulnerability d) Exploit 3 Describe these terms a) Threat actor b) Run book automation (RBA) c) Chain of custody (evidentiary) d) Reverse engineering e) Sliding window anomaly detection f) PII g) PHI 4 Describe these security terms a) Principle of least privilege b) Risk scoring/risk weighting c) Risk reduction d) Risk assessment 5 Compare and contrast these access control models a) Discretionary access control b) Mandatory access control c) Nondiscretionary access control 6 Compare and contrast these terms a) Network and host antivirus b) Agentless and agent-based protections c) SIEM and log collection 7 Describe these concepts a) Asset management b) Configuration management c) Mobile device management d) Patch management

Section	Weight	Objectives
		e) Vulnerability management
Cryptography	12%	1 Describe the uses of a hash algorithm 2 Describe the uses of encryption algorithms 3 Compare and contrast symmetric and asymmetric encryption algorithms 4 Describe the processes of digital signature creation and verification 5 Describe the operation of a PKI 6 Describe the security impact of these commonly used hash algorithms a) MD5 b) SHA-1 c) SHA-256 d) SHA-512 7 Describe the security impact of these commonly used encryption algorithms and secure communications protocols a) DES b) 3DES c) AES d) AES256-CTR e) RSA f) DSA g) SSH h) SSL/TLS 8 Describe how the success or failure of a cryptographic exchange impacts security investigation 9 Describe these items in regards to SSL/TLS a) Cipher-suite b) X.509 certificates c) Key exchange d) Protocol version e) PKCS
Host-Based Analysis	19%	1 Define these terms as they pertain to Microsoft Windows a) Processes b) Threads c) Memory allocation d) Windows Registry e) WMI

Section	Weight	Objectives
		f) Handles g) Services 2 Define these terms as they pertain to Linux a) Processes b) Forks c) Permissions d) Symlinks e) Daemon 3 Describe the functionality of these endpoint technologies in regards to security monitoring a) Host-based intrusion detection b) Antimalware and antivirus c) Host-based firewall d) Application-level whitelisting/blacklisting e) Systems-based sandboxing (such as Chrome, Java, Adobe reader) 4 Interpret these operating system log data to identify an event a) Windows security event logs b) Unix-based syslog c) Apache access logs d) IIS access logs
Security Monitoring	19%	1 Identify the types of data provided by these technologies a) TCP Dump b) NetFlow c) Next-Gen firewall d) Traditional stateful firewall e) Application visibility and control f) Web content filtering g) Email content filtering 2 Describe these types of data used in security monitoring a) Full packet capture b) Session data c) Transaction data d) Statistical data f) Extracted content g) Alert data 3 Describe these concepts as they relate to security monitoring a) Access control list b) NAT/PAT c) Tunneling

Section	Weight	Objectives
		d) TOR e) Encryption f) P2P g) Encapsulation h) Load balancing 4 Describe these NextGen IPS event types a) Connection event b) Intrusion event c) Host or endpoint event d) Network discovery event e) NetFlow event 5 Describe the function of these protocols in the context of security monitoring a) DNS b) NTP c) SMTP/POP/IMAP d) HTTP/HTTPS
Attack Methods	21%	1 Compare and contrast an attack surface and vulnerability 2 Describe these network attacks a) Denial of service b) Distributed denial of service c) Man-in-the-middle 3 Describe these web application attacks a) SQL injection b) Command injections c) Cross-site scripting 4 Describe these attacks a) Social engineering b) Phishing c) Evasion methods 5 Describe these endpoint-based attacks a) Buffer overflows b) Command and control (C2) c) Malware d) Rootkit e) Port scanning f) Host profiling 6 Describe these evasion methods a) Encryption and tunneling b) Resource exhaustion c) Traffic fragmentation

Section	Weight	Objectives
		d) Protocol-level misinterpretation e) Traffic substitution and insertion f) Pivot 7 Define privilege escalation 8 Compare and contrast remote exploit and a local exploit

210-255 Sample Questions:

01. Which option allows a file to be extracted from a TCP stream within Wireshark?
a) File > Export Objects
b) Analyze> Extract
c) Tools > Export > TCP
d) View > Extract

02. From a security perspective, why is it important to employ a clock synchronization protocol on a network?
a) so that everyone knows the local time
b) to ensure employees adhere to work schedule
c) to construct an accurate timeline of events when responding to an incident
d) to guarantee that updates are pushed out according to schedule

03. Which component of the NIST SP800-61 r2 incident handling strategy reviews data?
a) preparation
b) detection and analysis
c) containment, eradication, and recovery
d) post-incident analysis

04. Which statement about threat actors is true?
a) They are any company assets that are threatened.
b) They are any assets that are threatened.
c) They are perpetrators of attacks.
d) They are victims of attacks.

05. Which regular expression matches "color" and "colour"?
a) col[0-9]+our
b) colo?ur
c) colou?r
d)]a-z]{7}

06. Which data type is protected under the PCI compliance framework?
a) credit card type
b) primary account number
c) health conditions
d) provision of individual care

07. Which element is included in an incident response plan?
a) organization mission
b) junior analyst approval
c) day-to-day firefighting
d) siloed approach to communications

08. Which identifies both the source and destination location?
a) IP address
b) URL
c) ports
d) MAC address

09. Which two components are included in a 5-tuple?
(Choose two.)
a) port number
b) destination IP address
c) data packet
d) user name
e) host logs

10. Which type of analysis allows you to see how likely an exploit could affect your network?
a) descriptive
b) casual
c) probabilistic
d) inferential

Answers to 210-255Exam Questions:

Question: 01 Answer: a	Question: 02 Answer: c	Question: 03 Answer: d	Question: 04 Answer: c	Question: 05 Answer: c
Question: 06 Answer: a	Question: 07 Answer: a	Question: 08 Answer: c	Question: 09 Answer: a, b	Question: 10 Answer: c

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@nwexam.com