210-250

Understanding Cisco Cybersecurity Fundamentals

NWExam.com

SUCCESS GUIDE TO CISCO CERTIFICATION

Exam Summary – Syllabus – Questions

Table of Contents

Introduction to 210-250 Exam on Understanding Cisco Cybersecurity Fundamentals

A great way to start the Cisco Certified Network Associate Cyber Ops (SECFND) preparation is to begin by properly appreciating the role that syllabus and study guide play in the Cisco 210-250 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 210-250 exam preparation guide to provide the overview about Cisco Understanding Cisco Cybersecurity Fundamentals exam, study material, sample questions, practice exam and ways to interpret the exam objectives to help you assess your readiness for the Cisco SECFND 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 210-250 Certification Details:

Exam Name	Understanding Cisco Cybersecurity Fundamentals
Exam Number	210-250 SECFND
Exam Price	$300 USD
Duration	90 minutes
Number of Questions	60-70
Passing Score	Variable (750-850 / 1000 Approx.)
Recommended Training	Understanding Cisco Cybersecurity Fundamentals (SECFND)
Exam Registration	PEARSON VUE
Sample Questions	Cisco 210-250 Sample Questions
Practice Exam	**Cisco Certified Network Associate Cyber Ops Practice Test**

Cisco 210-250 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 10 Compare and contrast inline traffic interrogation and taps or traffic mirroring

Section	Weight	Objectives
		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 e) Vulnerability management
Cryptography	12%	1 Describe the uses of a hash algorithm 2 Describe the uses of encryption algorithms

Section	Weight	Objectives
		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 f) Handles g) Services 2 Define these terms as they pertain to Linux a) Processes b) Forks c) Permissions

Section	Weight	Objectives
		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 d) TOR e) Encryption f) P2P g) Encapsulation h) Load balancing 4 Describe these NextGen IPS event types a) Connection event b) Intrusion event

Section	Weight	Objectives
		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 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

210-250 Sample Questions:

01. Which statement about digitally signing a document is true?
a) The document is hashed and then the document is encrypted with the private key.
b) The document is hashed and then the hash is encrypted with the private key.
c) The document is encrypted and then the document is hashed with the public key
d) The document is hashed and then the document is encrypted with the public key.

02. A firewall requires deep packet inspection to evaluate which layer?
a) application
b) Internet
c) link
d) transport

03. Which option is a purpose of port scanning?
a) Identify the Internet Protocol of the target system.
b) Determine if the network is up or down
c) Identify which ports and services are open on the target host.
d) Identify legitimate users of a system.

04. Where is a host-based intrusion detection system located?
a) on a particular end-point as an agent or a desktop application
b) on a dedicated proxy server monitoring egress traffic
c) on a span switch port
d) on a tap switch port

05. Which definition of vulnerability is true?
a) an exploitable unpatched and unmitigated weakness in software
b) an incompatible piece of software
c) software that does not have the most current patch applied
d) software that was not approved for installation

06. Which hashing algorithm is the least secure?
a) MD5
b) RC4
c) SHA-3
d) SHA-2

07. Which two actions are valid uses of public key infrastructure?
(Choose two)
a) ensuring the privacy of a certificate
b) revoking the validation of a certificate
c) validating the authenticity of a certificate
d) creating duplicate copies of a certificate
e) changing ownership of a certificate

08. Which data can be obtained using Net Flow?
a) session data
b) application logs
c) network downtime
d) report full packet capture

09. For which reason can HTTPS traffic make security monitoring difficult?
a) encryption
b) large packet headers
c) Signature detection takes longer.
d) SSL interception

10. Which security monitoring data type requires the most storage space?
a) full packet capture
b) transaction data
c) statistical data
d) session data

Answers to 210-250 Exam Questions:

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

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