Cisco CCNA Certification 210-250 Exam

- **Vendor: Cisco**
- **Exam Code: 210-250**
- **Exam Name: Understanding Cisco Cybersecurity Fundamentals (SECFND)**

QUESTION 1
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.

Answer: A

QUESTION 2
Which definition of the virtual address space for a Windows process is true?

A. actual physical location of an object in memory
B. set of virtual memory addresses that it can use
C. set of pages that are currently resident in physical memory
D. system-level memory protection feature that is built into the operating system

Answer: A

QUESTION 3
Which information security property is supported by encryption?

A. sustainability
B. integrity
C. confidentiality
D. availability

Answer: A

QUESTION 4
Which situation indicates application-level white listing?

A. Allow everything and deny specific executable files.
B. Allow specific executable files and deny specific executable files.
C. Writing current application attacks on a whiteboard daily.
D. Allow specific files and deny everything else.

Answer: C

QUESTION 5
If a web server accepts input from the user and passes it to a bash shell, to which attack method is it vulnerable?

A. input validation
B. hash collision
C. command injection
D. integer overflow

Answer: B

QUESTION 6

Which definition of a process in Windows is true?

A. running program
B. unit of execution that must be manually scheduled by the application
C. database that stores low-level settings for the OS and for certain applications
D. basic unit to which the operating system allocates processor time

Answer: C

QUESTION 7
Which definition of permissions in Linux is true?

A. rules that allow network traffic to go in and out
B. table maintenance program
C. written affidavit that you have to sign before using the system
D. attributes of ownership and control of an object

Answer: A

QUESTION 8
Which hashing algorithm is the least secure?

A. MD5
B. RC4
C. SHA-3
D. SHA-2

Answer: D

QUESTION 9
Which protocol is expected to have NTP a user agent, host, and referrer headers in a packet capture?

A. NTP
B. HTTP
C. DNS
D. SSH

Answer: C

QUESTION 10
What is PHI?

A. Protected HIPAA information
B. Protected health information
C. Personal health information
D. Personal human information

Answer: B

QUESTION 11
Which of the following are Cisco cloud security solutions?

A. CloudDLP
B. OpenDNS
C. CloudLock
D. CloudSLS

Answer: BC

QUESTION 12
What is a trunk link used for?

A. To pass multiple virtual LANs
B. To connect more than two switches
C. To enable Spanning Tree Protocol
D. To encapsulate Layer 2 frames

Answer: A

QUESTION 13
At which OSI layer does a router typically operate?

A. Transport
B. Network
C. Data link
D. Application

Answer: B

QUESTION 14
Cisco pxGrid has a unified framework with an open API designed in a hub-and-spoke architecture. pxGrid is used to enable the sharing of contextual-based information from which devices?

A. From a Cisco ASA to the Cisco OpenDNS service
B. From a Cisco ASA to the Cisco WSA
C. From a Cisco ASA to the Cisco FMC
D. From a Cisco ISE session directory to other policy network systems, such as Cisco IOS devices and the Cisco ASA

Answer: D

QUESTION 15
What are the advantages of a full-duplex transmission mode compared to half-duplex mode? (Select all that apply.)

A. Each station can transmit and receive at the same time.
B. It avoids collisions.
C. It makes use of backoff time.
D. It uses a collision avoidance algorithm to transmit.

Answer: AB

QUESTION 16

Stateful and traditional firewalls can analyze packets and judge them against a set of predetermined rules called access control lists (ACLs). They inspect which of the following elements within a packet? (Choose two.)

A. Session headers
B. NetFlow flow information
C. Source and destination ports and source and destination IP addresses
D. Protocol information

Answer: CD

QUESTION 17
In which case should an employee return his laptop to the organization?

A. When moving to a different role
B. Upon termination of the employment
C. As described in the asset return policy
D. When the laptop is end of lease

Answer: C

QUESTION 18
.....

QUESTION 91
The FMC can share HTML, PDF and CSV data type that relate to a specific event type data. Which specific event type data?

A. Connection
B. Host
C. Netflow
D. Intrusion

Answer: D
Explanation:
The Firepower System has features that you can use to gather intrusion data in standard formats such as HTML, PDF, and CSV (comma-separated values) so that you can easily share intrusion data with others.
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/incidents.html

QUESTION 92
For which purpose can Windows management instrumentation be used?

A. Remote viewing of a computer
B. Remote blocking of malware on a computer
C. Remote reboot of a computer
D. Remote start of a computer

Answer: A
Explanation:
The purpose of WMI is to define a proprietary set of environment-independent specifications which allow management information to be shared between management applications. WMI allows

scripting languages to locally and remotely manage Microsoft Windows computers and services. The following list provides examples of what WMI can be used for:
-- Providing information about the status of local or remote computer systems
-- Configuring security settings
-- Modifying system properties
-- Changing permissions for authorized users and user groups
-- Assigning and changing drive labels
-- Scheduling times for processes to run
-- Backing up the object repository
-- Enabling or disabling error logging

QUESTION 93
Which international standard is for general risk management, including the principles and guideline for managing risk?

A. ISO 31000
B. ISO 27001
C. ISO 27005
D. ISO 27002

Answer: A
Explanation:
ISO 31000:2018, Risk management -- Guidelines, provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.
https://www.iso.org/iso-31000-risk-management.html

QUESTION 94
Which statement about the difference between a denial-of-service attack and a distributed denial of service attack is true?

A. Dos attack are launched from one host, and DDoS attack are launched from multiple host.
B. DoS attack and DDoS attack have no differences.
C. DDoS attacks are launched from one host, and DoS attacks are launched from multiple host.
D. Dos attack only use flooding to compromise a network, and DDoS attacks only use other methods.

Answer: A
Explanation:
DDoS refers to a "distributed denial of service" attack. With this attack a hacker will use multiple servers to attack another target server i.e. the attack is distributed across multiple servers. Traffic associated with a single DDoS attack may originate from hundreds or thousands of compromised servers or PCs. Whereas a "denial of service" (DoS) attack is when a single server is used to attack another targeted server.
https://hetzner.co.za/help-centre/website/what-is-the-difference-between-a-dos-and-ddos-attack/

QUESTION 95
You discover that a foreign government hacked one of the defense contractors in your country and stole intellectual property. In this situation, which option is considered the threat agent?

A. method in which the hack occurred
B. defense contractor that stored the intellectual property

C. intellectual property that was stolen
D. foreign government that conducted the attack

Answer: A

QUESTION 96
After a large influx of network traffic to externally facing devices, you begin investigating what appear to be a denial of service attack. When you review packets capture data, you notice that the traffic is a single SYN packet to each port. Which kind of attack is this?

A. SYN flood.
B. Host profiling.
C. Traffic fragmentation.
D. Port scanning.

Answer: D

QUESTION 97
Which definition of common event format is terms of a security information and event management solution is true?

A. A type of event log used to identify a successful user login.
B. A TCP network media protocol.
C. Event log analysis certificate that stands for certified event forensics.
D. A standard log event format that is used for log collection.

Answer: D

QUESTION 98
Which definition of a Linux daemon is true?

A. Process that is causing harm to the system by either using up system resources or causing a critical crash.
B. Long - running process that is the child at the init process.
C. Process that has no parent process.
D. Process that is starved at the CPU.

Answer: B
Explanation:
A daemon is a type of program on Unix-like operating systems that runs unobtrusively in the background, rather than under the direct control of a user, waiting to be activated by the occurance of a specific event or condition. Unix-like systems typically run numerous daemons, mainly to accommodate requests for services from other computers on a network, but also to respond to other programs and to hardware activity.
...
Daemons are recognized by the system as any processes whose parent process has a PID of one, which always represents the process init. init is always the first process that is started when a Linux computer is booted up (i.e., started), and it remains on the system until the computer is turned off. init adopts any process whose parent process dies (i.e., terminates) without waiting for the child process's status. Thus, the common method for launching a daemon involves forking (i.e., dividing) once or twice, and making the parent (and grandparent) processes die while the child (or grandchild) process begins performing its normal function.
http://www.linfo.org/daemon.html

QUESTION 99

Which term describes reasonable effort that must be made to obtain relevant information to facilitate appropriate courses of action?

A. Due diligence.
B. Ethical behavior.
C. Decision making.
D. Data mining.

Answer: A

QUESTION 100
According to the common vulnerability scoring system, which term is associated with scoring multiple vulnerabilities that are exploit in the course of a single attack?

A. chained score
B. risk analysis
C. vulnerability chaining
D. confidentiality

Answer: C
Explanation:
CVSS is designed to classify and rate individual vulnerabilities. However, it is important to support the needs of the vulnerability analysis community by accommodating situations where multiple vulnerabilities are exploited in the course of a single attack to compromise a host or application. The scoring of multiple vulnerabilities in this manner is termed Vulnerability Chaining. Note that this is not a formal metric, but is included as guidance for analysts when scoring these kinds of attacks. https://www.first.org/cvss/cvss-v30-user_guide_v1.1.pdf (page 10 -- Vulnerability Chaining)

QUESTION 101
……