

**Understanding Cisco Cybersecurity Fundamentals (210-250)**

**Exam Description:** The Understanding Cisco Cybersecurity Fundamentals (SECFND) exam (210-250) is a 90-minute, 60−70 question assessment that is associated with the Cisco CCNA Cyber Ops certification. Candidates can prepare for this exam by taking the Understanding Cisco Cybersecurity Fundamentals (SECFND) v1.0 course. This exam tests a candidate's understanding of cybersecurity basic principles, foundational knowledge, and core skills needed to grasp the more associate-level materials in the second required exam, Implementing Cisco Cybersecurity Operations (SECOPS).

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

# 12% 1.0 Network Concepts

* 1. Describe the function of the network layers as specified by the OSI and the TCP/IP network models
     + - The purpose of the network layer in the OSI and TCP/IP models is to forward information between logical networks.
  2. Describe the operation of the following
     1. IP
        + Stands for Internet Protocol, provides end-to-end delivery of packets through an internetwork.
     2. TCP
        + Layer 4 protocol responsible for providing reliable, full-duplex, communications by use of a three-way handshake to begin communications (syn, syn-ack, ack). TCP uses packet sequence numbers to ensure full data delivery. Error recovery is provided. Uses 5-tupple metadata for ensuring session management.
     3. UDP
        + IP protocol 17. Layer 4 protocol that provides connectionless communications for real-time applications such as live voice and video conferencing. Simplified header and best-effort network delivery ensures fast communications. Responsibility of higher-layer to provide error checking and recovery.
     4. ICMP
        + Internet Control Message Protocol – Provides method to communicate that an error occurred during the routing of packets.
  3. Describe the operation of these network services
     1. ARP
        + Service used to request the Layer 2 MAC of a host using its IP address. ARP requests are started by the device sending a broadcast query. The intended device will respond to the ARP request with an ARP reply containing its MAC address.
     2. DNS
        + System to resolve human readable domain names to its IP address equivalent. Primarily uses UDP port 53 but may also use TCP port 53.
     3. DHCP
        + Provides dynamic network configuration information to the requesting host, primarily an IP address. A four-step process for requests: Discovery, Offer, Request, and ACK. Both Discovery and Request are broadcast messages intended for the subnets DHCP server. May also contain additional information such as the default gateway, DNS servers, and NTP servers. Uses UDP port 67 for the DHCP server, and UDP port 68 for the DHCP client.
  4. Describe the basic operation of these network device types
     1. Router
        + Layer 3 device that delivers packets between two networks. Breaks up broadcast and collision domains. Works by creating a routing table consisting of connected interfaces, static routes, dynamic routes, and default routes. Interior routing protocols are divided into two main categories: distance vector (routers advertise all connected routers and their distance, RIP and EIGRP) and link state (the router learns the complete topology of the network, OSPF and IS-IS). There is a single Exterior Gateway Protocol in use today, BGP.
     2. Switch
        + A layer 2 device used to forward frames and separates each interface into its own collision domain. Switches can be separated into two major categories, layer 2 and layer 3 switches. Layer 3 switches add the capability of providing routing functionality through the use of VLANs.
     3. Hub
        + Layer 1 device that regenerates the outbound signal across all ports except sender. Half-duplex communications and uses CSMA/CD to mitigate collisions. All interfaces part of same collision and broadcast domain.
     4. Bridge
        + A bridge is a layer 2 device with functionally similar to a switch. The network bridge predates switches. Bridges separate interfaces into their own collision domains.
     5. Wireless access point (WAP)
        + Defined by 802.11, half-duplex communications using CSMA/CA to avoid collisions. Standalone. CSMA/CA can use a physical carrier sense to ensure the medium is clear or a virtual carrier sense to predict how long the medium will be busy based on the estimated time the current frame will take to transmit based on a value in the 802.11 frame. Frames must be acknowledged by the receiver on a WLAN unlike an Ethernet LAN.
     6. Wireless LAN controller (WLC)
        + A WLAN controller provide management functions to control Lightweight Access Points. WLC’s provide the ability to monitor and provide real-time signal shaping to ensure maximum coverage. Some benefits of using a WLC include Dynamic channel assignment, transmit power optimization, self-healing wireless coverage, flexible client roaming, dynamic client load balancing, security management, and wireless intrusion protection system
  5. Describe the functions of these network security systems as deployed on the host, network, or the cloud:
     1. Firewall
        + Protects the trusted, inside network and the untrusted outside network. Firewalls connected to the Internet are often called Internet Edge Firewalls. May also provide Network Address Translation services, filtering, and application inspection. Perimeter security is accomplished by simple packet-filtering techniques, application proxies, NAT, stateful inspection, and next-gen context aware firewalls.
     2. Cisco Intrusion Prevention System (IPS)
        + An IPS can both detect and eliminate network threats. They can be deployed inline with network traffic to actively stop attacks. Intrusion Prevention Systems can network-based or host-based. The different detection methodologies include: pattern matching and stateful pattern matching, protocol analysis, heuristics, anomaly, and global threat correlation.
     3. Cisco Advanced Malware Protection (AMP)
        + Next-generation protection using telemetry from big data, continuous analysis, and advanced. Protection monitors possible attacks while they are in progress to provide alerts during all stages of system compromise. Connectors are created for networks, endpoints, and content security appliances to provide greater monitoring and system remediation.
     4. Web Security Appliance (WSA) / Cisco Cloud Web Security (CWS)
        + WSA is a Cisco device used to protect an organization during the attack continuum. Uses website reputation and zero-day threat intel. Can be deployed in transparent or explicit proxy mode.
        + CWS is a Cisco technology that provides worldwide threat intelligence and defense as well as roaming user protection. CWS uses proxies in the Cisco cloud that scan traffic for malware and policy.
     5. Email Security Appliance (ESA) / Cisco Cloud Email Security (CES)
        + An ESA is a Cisco product running the AsyncOS used to mitigate email-based threats. ESA’s use the following features: access control, anti-spam, network antivirus, AMP, DLP, email encryption, email authentication, outbreak filters. Acts as the email gateway for your organization handling email connections, accepting messages, and relaying messages.
        + CES allows companies to outsource the management of their email security. A hybrid approach with ESAs provide maximum protection. CES helps to ensure DLP and retention compliance.

|  |  |  |
| --- | --- | --- |
|  | 1.6 | Describe IP subnets and communication within an IP subnet and between IP subnets   * An Ethernet broadcast domain defines a subnet. Communications between subnets is accomplished by using a router. The requesting computer examines the requested IP address and subnet to determine if the IP address resides on the local network, if so an ARP request is processed and the data is transferred using Ethernet frames. If the IP address is not found to be in the local scope the packet is sent to the gateway router for forwarding. The packet source address, destination address, and source MAC are set as expected, however the destination address will be set to the gateway router. This process is repeated until the packet is forwarded to the correct network and then the data is sent using Ethernet frames to the desired host. |
| 1.7 | Describe the relationship between VLANs and data visibility   * VLANs are used to segregate data for security by creating layer 2 network separation and to provide smaller, less congested broadcast domains as well as providing fault isolation that prevents misconfigurations from propagating to the rest of the network. Typically, VLANs are used to segregate data by user type, geographically, or device types such as printers, servers, and PCs. A routing device must be used to provide inter-VLAN routing. |
| 1.8 | Describe the operation of ACLs applied as packet filters on the interfaces of network devices   * ACLs can be used to filter traffic based on origin, destination, port, and rudimentary state information. |
| 1.9 | Compare and contrast deep packet inspection with packet filtering and stateful firewall operation   * DPI looks into layer 7 payloads to protect against threats by examining IP addressing information as well as dynamically assigned ports. Stateful firewall operations work by ensuring packets are part of valid, established connections. This done by examining packet header information as well as layer 7 information in the payload. |
| 1.10 | Compare and contrast inline traffic interrogation and taps or traffic mirroring   * An inline tool passes live traffic directly through a tool to process the live traffic before it is forwarded on to its final destination. A network TAP is a simple device that connects directly to the cabling infrastructure to split or copy packets for use in analysis, security, or general network management. SPAN, or Switch Port ANalyzer, is a software function of a switch or router that duplicates traffic from incoming or outgoing ports and forwards the copied traffic to a special SPAN port which is also known as a mirror port. |
| 1.11 | Compare and contrast the characteristics of data obtained from taps or traffic mirroring and NetFlow in the analysis of network traffic |
| 1.12 | Identify potential data loss from provided traffic profiles   * Several different methods of data analysis can reveal sources of data loss. An abnormal volume of protocol-specific data may suggest a specific attack vector (a large amount of SMTP packets may indicate a compromised email server). Comparing data destination against an established baseline can indicate an attack source or, at least, an attacker’s distributed network architecture. Monitoring file share access can indicate internal threats. |
| **17%** | **2.0** | **Security Concepts** |
|  | 2.1 | Describe the principles of the defense in depth strategy |
|  | 2.2 | Compare and contrast these concepts |

* + 1. Risk
* Likelihood of a given threat-source's exercising a particular potential vulnerability
* Risk = Threats x Vulnerabilities x Impact
  + 1. Threat
* Potential danger to assets
  + 1. Vulnerability
* The weakness of a system or design that makes it vulnerable to a threat
  + 1. Exploit
* Method to leverage vulnerability of attack
  1. Describe these terms
     1. Threat actor
     2. Run book automation (RBA)
     3. Chain of custody (evidentiary)
     4. Reverse engineering
     5. Sliding window anomaly detection
     6. PII
* Personally Identifiable Information
* information that can be used on its own, or with other information, to identify, contact, or locate a single person, or to identify an individual in context.
* Examples include name, SSN, biometrics, date and place of birth, mother’s maiden name, credit card numbers, bank account numbers, driver’s license number, address information such as email addresses or street addresses, and telephone numbers
* Does not include certain work information
  + 1. PHI
* Protected Health Information
* Protects name, dates (birth, death, discharge, and administration), telephone numbers, email and street addresses, medical record numbers, health plan beneficiary
  1. Describe these security terms
     1. Principle of least privilege
* The concept of providing employees the least amount of system access to accomplish their job. This could include limiting the number of systems or limiting the amount of time to access systems to mitigate data exfiltration and other malicious activity.
  + 1. Risk scoring/risk weighting
    2. Risk reduction
    3. Risk assessment
  1. Compare and contrast these access control models
     1. Discretionary access control
* Data owner assigns ACLs to allow access.
* File share permissions is a good example.
* Simplest model to implement but the security policy lacks central control.
  + 1. Mandatory access control
* Assigning classification and category labels to data and personnel. The individual accessing the data/system must match or exceed its classification and category label.
* Often used in high security environments like military and governments.
* This model maintains strict control, over information flow but is complex to manage.
  + 1. Nondiscretionary access control
       - This model allows the administrator to assign roles to the data users. Access to data is controlled by the roles assigned to each user.
       - This model scales well but results in an increase of role definition.
  1. Compare and contrast these terms
     1. Network and host antivirus
     2. Agentless and agent-based protections
     3. SIEM and log collection
  2. Describe these concepts
     1. Asset management
     2. Configuration management
     3. Mobile device management
     4. Patch management
     5. Vulnerability management

|  |  |  |
| --- | --- | --- |
| **12%** | **3.0** | **Cryptography** |
|  | 3.1 | Describe the uses of a hash algorithm   * Hashing is used to ensure data integrity. Algorithm turns input data into a unique fingerprint of the data. Algorithms must be one way and be able to resist cryptanalysis. A good algorithm will produce a low probability of a collision. |
|  | 3.2 | Describe the uses of encryption algorithms   * Encryption is used to hide data to ensure confidentiality. Takes plain text and converts cipher text using an encryption key, or keys. |
|  | 3.3 | Compare and contrast symmetric and asymmetric encryption algorithms |
|  | 3.4 | * Symmetric key encryption uses the same key for both encryption and decryption. Asymmetric encryption uses different keys for each task.   Describe the processes of digital signature creation and verification |
|  | 3.5 | * Uses private key of sender, read with public key. Provides authenticity, integrity and non-repudiation. Takes a hash of the email’s data and encrypts the hash using sender’s private key. The receiver must have the users public key to decrypt the hash. The receiver then performs their own has and compares their results with the decrypted hash that was attached to the message.   Describe the operation of a PKI   * Public key Infrastructure is a collection of technologies used to create trust in communications. When a user wants to communicate over a secure channel with a server the user’s computer will forward a request to a protected resource like a checkout page. The |
|  | 3.6 | Describe the security impact of these commonly used hash algorithms   * Used for downloading software * Cisco Products * Authentication Digital Certs * Public Key transfers * Public Key Encryption (PKE) * Cisco AMP – Host-based IDS Malware * VPN * Digital forensics * Incidence response   Find length and application of each algorithm (47:00 into replay) |

* + 1. MD5
* MD5 was designed by Ron Rivest as a secure hashing algorithm. It was once thought to be resilient against collisions but has been since found to be vulnerable. A one-way function that produces a fixed value called a message digest, or just digest
  + 1. SHA-1
* Developed by NIST in 1994 as a secure revision to SHA, was used to hash messages up to 264 bits long and produced a 160-bit message digest. The SHA-1 algorithm was slightly slower than MD5 but produced a digest more resistive to collisions. SHA-1 was optionally replaced in 2006 and mandatorily replaced in2010 by the SHA-2 family of hashing algorithms.
* Prone to collisions
  + 1. SHA-256
* Part of the SHA-2 family of hashing algorithms which replaced SHA-1. Capable of hashing data up to 264 bits in length.
* SHA-2: 224-512 bit (224, 256, 384, 512)
* Collision-resistant
  + 1. SHA-512
* Part of the SHA-2 family of hashing algorithms which replaced SHA-1. Capable of hashing data up to 2128 bits in length. Faster to implement in 64-bit systems than SHA-256.
* Collision-resistant
  1. Describe the security impact of these commonly used encryption algorithms and secure communications protocols
     1. DES
* Symmetric algorithm typically operating in block mode. A fixed 56 bit key is used to encrypt, another 8 bits is used for parity. Considered week because of a lower comparable key size to today’s encryption algorithms.
  + 1. 3DES
* Uses three rounds of DES to perform encryption. K1 encrypts message, K2 decrypts message, K3 encrypts message. This results in an effective key length of 168 bits. If K1 and K3 are the same key, 112 bits.
  + 1. AES
* Based on the Rijndael cipher, became the official US standard on May 26, 2002 by the US Secretary of Commerce. Uses key lengths of 128, 192, or 256 bits. Runs faster than DES on comparable hardware. AES is used a block cipher.
  + 1. AES256-CTR
* CTR mode typically uses a one-time unpredictable value called a nonce that is concatenated with a counter to provide randomness to the message encryption process. CBC, or cypher block chain, xor’s the previous block of encrypted data to provide randomness to the message encryption process. The first block uses an initialization vector as the xor value.
  + 1. RSA
* RSA stands for Rivest–Shamir–Adleman and is named after the cryptosystem’s co-founders. Uses asymmetric public key encryption. Considered
  + 1. DSA
       - DSA stands for Digital Signature Algorithm and is an asymmetric algorithm that is primarily used for digital signatures.
    2. SSH
       - Stands for Secure Shell and allows users access to a remote command line for configuring and using a \*NIX environment. Uses TCP port 22 for communications and can be configured to authenticate with passwords or certificates.
    3. SSL/TLS
       - The standard that is responsible for secure website communications. SSL is the predecessor of TLS. The web server and host use ephemeral parameters along with private keys to produce a shared secret that can be used to protect traffic.
  1. Describe how the success or failure of a cryptographic exchange impacts security investigation
     + - If the cryptographic exchange fails and the data is not properly encrypted it may no longer be possible to authenticate the message’s origin or verify the message’s confidentiality. This would impact the security investigation because it would be impossible to determine when or who accessed the data in question.
  2. Describe these items in regards to SSL/TLS
     1. Cipher-suite
        + A cipher suite is a named combination of authentication and encryption algorithms used to negotiate the security settings for a network connection that uses the Transport Layer Security (TLS) / Secure Sockets Layer (SSL) network protocols
     2. X.509 certificates
        + X.509v3 is a standard for implementing digital certificates with directory services.
     3. Key exchange
        + Key exchange is handled by the Diffie-Hellman protocol which is an asymmetric algorithm that produces a symmetric key that can be used to protect data using an cryptographic algorithm such as 3DES and AES.
     4. Protocol version
        + SSLv1 was never released, SSLv2 was the first publically available implementation of SSL, SSLv3 was renamed to TLS 1.0 and replaced SSLv2. Subsequently, TLS 1.1 and 1.2 have been released and TLS 1.3 is currently in draft
     5. PKCS
        + PKCS stands for Public Key Cryptography Standards and is a collection of specifications that are used to control the format and use of digital certificates.

# 19% 4.0 Host-Based Analysis

* 1. Define these terms as they pertain to Microsoft Windows
     1. Processes
     2. Threads
     3. Memory allocation
     4. Windows Registry
     5. WMI
     6. Handles
     7. Services
  2. Define these terms as they pertain to Linux
     1. Processes
     2. Forks
     3. Permissions
     4. Symlinks
     5. Daemon
  3. Describe the functionality of these endpoint technologies in regards to security monitoring
     1. Host-based intrusion detection
     2. Antimalware and antivirus
     3. Host-based firewall
     4. Application-level whitelisting/blacklisting
     5. Systems-based sandboxing (such as Chrome, Java, Adobe reader)
  4. Interpret these operating system log data to identify an event
     1. Windows security event logs
     2. Unix-based syslog
     3. Apache access logs
     4. IIS access logs

# 19% 5.0 Security Monitoring

* 1. Identify the types of data provided by these technologies
     1. TCP Dump
     2. NetFlow
     3. Next-Gen firewall
     4. Traditional stateful firewall
     5. Application visibility and control
     6. Web content filtering
     7. Email content filtering
  2. Describe these types of data used in security monitoring
     1. Full packet capture
     2. Session data
     3. Transaction data
     4. Statistical data
     5. Extracted content
     6. Alert data
  3. Describe these concepts as they relate to security monitoring
     1. Access control list
     2. NAT/PAT
     3. Tunneling
     4. TOR
     5. Encryption
     6. P2P
     7. Encapsulation
     8. Load balancing
  4. Describe these NextGen IPS event types
     1. Connection event
     2. Intrusion event
     3. Host or endpoint event
     4. Network discovery event
     5. NetFlow event
  5. Describe the function of these protocols in the context of security monitoring
     1. DNS
     2. NTP
     3. SMTP/POP/IMAP
     4. HTTP/HTTPS

# 21% 6.0 Attack Methods

* 1. Compare and contrast an attack surface and vulnerability
  2. Describe these network attacks
     1. Denial of service
     2. Distributed denial of service
     3. Man-in-the-middle
  3. Describe these web application attacks
     1. SQL injection
     2. Command injections
     3. Cross-site scripting
  4. Describe these attacks
     1. Social engineering
     2. Phishing
     3. Evasion methods
  5. Describe these endpoint-based attacks
     1. Buffer overflows
     2. Command and control (C2)
     3. Malware
     4. Rootkit
     5. Port scanning
     6. Host profiling
  6. Describe these evasion methods
     1. Encryption and tunneling
     2. Resource exhaustion
     3. Traffic fragmentation
     4. Protocol-level misinterpretation
     5. Traffic substitution and insertion
     6. Pivot
  7. Define privilege escalation
  8. Compare and contrast remote exploit and a local exploit