ISC2

Domain 4 Key Takeaways

Security professionals reviewing CISSP Domain 4 must understand the principles of communication and network security and the different tools and techniques used to protect information as it is transmitted over networks. This includes securing network protocols and services, using network security devices, implementing secure transmission protocols, securing wireless networks, and mitigating internet-related security risks. Additionally, special security considerations are required for real-time communication technologies.

1. Communication and network security involves protecting the confidentiality, integrity, and availability of information as it is transmitted over networks.

2. Network protocols and services, such as TCP/IP, DNS, and DHCP, are fundamental to network communication and must be secured to prevent attacks.

3. Network security devices, such as firewalls and intrusion detection/prevention systems, can be used to protect networks from unauthorized access and attacks.

4. Secure transmission protocols, such as SSL/TLS and VPNs, can be used to protect information as it is transmitted over networks.

5. Wireless networks present unique security challenges, including the need to secure access points and encrypt data transmissions.

6. The internet presents significant security risks, including malware, phishing attacks, and denial-of-service attacks. Network security measures must be implemented to mitigate these risks.

7. Voice over IP (VoIP) and other real-time communication technologies require special security considerations, such as ensuring the confidentiality of conversations and protecting against eavesdropping.

Secure Design in Network Architectures

- Applying a security architecture to a technical design often involves compromises for both system performance and security capabilities. Legacy methods, immature technology, and improper implementation can all create vulnerabilities subject to exploitation. The security professional should be able to explain the risk implications of the tradeoffs that so a proper risk decision can be made.

- Security professionals need to be familiar with both the TCP/IP and OSI 7-Layer Models to make many security analyses, engineering, and assurance activities more straightforward. At a practical level, it is important to recognize that many products and services use terminology and ideas from both protocol stacks. Neither model is a theoretical expression of ideas; both have real forms that show up in elements of the hardware, firmware, software, and virtualized services that make the internet and the World Wide Web what they are today.

- Early internet protocols, such as file transfer protocol (FTP), Telnet, the finger command, and others, often had limited authentication controls, lacked cryptographic protections, or were subject to manipulation of the packet forms. Over time, many of the protocols became more robust, but the existence of the legacy protocols, with their weaknesses, continues to plague poorly implemented environments.

- While general communications infrastructures rely heavily on the TCP/IP suite, many protocols exist to meet the demands of specific environments or are proprietary to an organization. This opens the possibility that the combination of protocols may create a larger attack surface, or that the TCP/IP suite will not offer the QoS needed by an application. Other protocols, in such areas as telecommunications and healthcare, present similar challenges to providing secure connectivity between devices.

- Software-defined networking (SDN) is rapidly changing how networks are constructed and implemented, particularly in virtualized and cloud environments. SDN is repurposing existing infrastructure from being device- and hardware-centric to virtual- and data-centric. The aim is to deliver services rather than technology. A caution is warranted here: software-defined can apply to many things besides networking. Security, for example, can be established by using an integrated application to model, plan, direct, and monitor security operations.

- Content distribution networks continue to evolve their provision of specialized services, including security, content optimization, and CDN federation, to reduce the impact of traffic on the internet backbone.

- In Trust but Verify, system elements rely upon other core processes to authenticate and authorize users, processes, or devices to be connected to the network. Once connected, the trustworthiness of these identities and their claims of privileges can be validated by individual systems elements if their security needs dictate. Zero trust is a design approach that recognizes even the most robust access control systems have their weaknesses. In the extreme, it insists that every process or action a user attempts must be authenticated and authorized; the window of trust (the time-to-live of a token, so to speak) becomes vanishingly small.

Secure Network Components

- The complex interrelationship between hardware and software is the starting point for the operation of secure systems.

- An application cannot operate securely if the operating system is compromised. Similarly, an OS cannot be trusted if the underlying hardware is untrustworthy. The concept of the Root of Trust (RoT) relies on an immutable (unchangeable) trusted hardware component—a trust anchor—that subsequent actions can rely upon to ensure they are starting from a secure system state.

- The network access control (NAC) device will provide the network visibility needed for access security and may later be used for incident response. Aside from identifying connections, it should also be able to ensure that all devices wishing to join the network do so only when they comply with the requirements laid out in policy. This visibility will encompass regular users, temporary users, and any devices they may bring with them into the organization. The NAC device(s) should also provide bidirectional integration, allowing full integration with all security and network solutions that are, or will be, deployed within the corporate network.

- Security analysts and systems vendors have focused increased attention on how to harden endpoint devices of all types. This includes mobile and fixed devices on wired or wireless connections, and from high-performance workstations down to the simplest IoT devices. This has given rise to many products and services for endpoint device management, which are continually evolving.

- There are several vendors and consortiums working on developing standards for interoperability for NAC devices and solutions, with perhaps the biggest three being Cisco's CNAC (Cisco network access control) architecture, Microsoft's NAP (network access protection) initiative, and the Trusted Computing Group's (TNC) standard.

- Before deploying NAC devices, remote access policies should be written or evaluated. This policy should clearly identify the scope of network access that the organization wishes to allow and will include both the corporate users and the range of devices. The policy should detail what controls these users or devices need to adhere to such as encryption, screen locking, antivirus (AV), and firewall settings. Once the policy requirements are fully understood, then examine the options presented by the various NAC vendors and choose the solution that best fits with the policy.

Secure Communication Channels

- Security professionals should study and evaluate the communications infrastructure their organization relies upon so that it meets the organization's business goals and risk tolerances.

- VoIP and multimedia collaboration platforms can offer many methods of encryption, call logging, recording, and conferencing capabilities that go far beyond what the plain old telephone system (POTS) could ever provide. From a security perspective, this is both good news and bad.

    - *The good news.* Security policies can enforce meeting or call security, limit access, and protect proprietary or sensitive content. Automated recordkeeping provides a basis for audit and investigation if required.

  - *The bad news.* Some of these products and services may involve encryption solutions that have been compromised or cracked by various national governments or other parties.

- Wireless networks face the same vulnerabilities, threats, and risks as any cabled network, but they also have additional security considerations that complicate establishing and maintaining effective device-level NAC. Many wireless devices, once connected to your networks, can then act as access points and as routers, allowing other devices to connect first to them, and then through them to your networks. Done improperly, this can provide unauthorized devices (and users) access to your systems.

- Remote access has taken on new meaning and importance as organizations have moved to highly mobile end users among their workforce, customers, suppliers, and other stakeholders. Remote users employ VPNs to access their organization's network securely. Depending on the VPN's implementation, they may have most of the same resources available to them as if they were physically at the office. Strong VPN connections between the teleworker and the organization need to be established, and full device encryption should be the norm for protecting sensitive information.

- It is worth recognizing that all multimedia collaboration by end users is done via applications programs, which may each use a wide variety of technologies and protocols. These products change rapidly, as the threat landscape keeps changing and user needs become more demanding.

- Distinctions between circuit-switched networks and packet-switched networks are becoming increasingly blurred as telecommunications carriers move their infrastructures to packet-switched technology at the core while maintaining circuit-switched infrastructure to the endpoint.

- The modern virtualization of networks and the associated technology is called network function virtualization or alternately referred to as virtual network function or virtualized networks. The objective of NFV is to decouple functions away from specific hardware implementation into software solutions.

- To achieve efficiencies in business operations, organizations often rely on third parties to provide connectivity services or enable third parties to directly connect to their infrastructure. Good management practices for these relationships include the following:

    - Found an organizational policy for establishing, onboarding, monitoring, managing, and offboarding third-party connectivity relationships.

    - Inventory existing third-party relationships, evaluating the relationship against the policy to identify relationships that pose greater risk to the organization.

    - Apply monitoring and auditing practices, consistent with contractual relationships, to third-party relationships.