Hi, I'm Mike Chapple and this is the audio review of the exam essentials for chapter 12 of the official CISSP study guide. Here are the top things you need to know for the exam from this chapter on secure communications and network attacks.

Understand PPP. The point-to-point protocol PPP is an encapsulation protocol designed to support the transmission of IP traffic over dial up or point-to-point links. The original PPP options for authentication were PAP, CHAP and EAP. Define PAP, CHAP and EAP. The password authentication protocol PAP transmits usernames and passwords in clear text. The challenge handshake authentication protocol CHAP performs authentication using a challenge response dialogue that cannot be replayed. The extensible authentication protocol EAP allows customized authentication security solutions.

Understand IEEE 802.1X. IEEE 802.1X defines the use of encapsulated EAP to support a wide range of authentication options for land connections. The IEEE 802.1X standard is formerly named port-based network access control. Know about port security. Port security can mean the physical control of all connection points such as RJ45 wall jacks or device ports. Port security is the management of TCP and UDP ports. Port security can also refer to the need to authenticate to a port before being allowed to communicate through or across the port.

Understand voice communication security. Voice communications are vulnerable to many attacks, especially as voice communications become an important part of network services. You can obtain confidentiality by using encrypted communications. Countermeasures must be deployed to protect against interception, eavesdropping, tapping and other types of exploitation.

Know the threats associated with PBX systems and the countermeasures to PBX fraud. Countermeasures to PBX fraud and abuse include many of the same precautions you would employ to protect a typical computer network. Logical or technical controls, administrative controls and physical controls.

Recognize what freaking is. Freaking is a specific type of attack in which various types of technology are used to circumvent the telephone system to make free long distance calls, to alter the function of the telephone service, to steal specialized services or to cause service disruptions. A freaker is an attacker who performs freaking.

Understand the issues of remote access security management. Remote access security management requires that security system designers address the hardware and software components of an implementation along with issues related to policy, work tasks and encryption. Know various issues related to remote access security. Be familiar with remote access, dial up connections, screen scrapers, virtual applications in desktops and general telecommuting security concerns.

Understand multimedia collaboration. Multimedia collaboration is the use of various multimedia supporting communication solutions to enhance distance collaboration and communications. Know the purpose of load balancers. The purpose of load balancing is to obtain more optimal infrastructure utilization, minimize response time, maximize throughput, reduce overloading and eliminate bottlenecks. A load balancer is used to spread or distribute network traffic load across several network links or network devices.

Understand active-active. An active-active system is a form of load balancing that uses all available pathways or systems during normal operations, but has reduced capacity in adverse conditions.

Understand active-passive. An active-passive system is a form of load balancing that keeps some pathways or systems in an unused dormant state during normal operations. It's able to maintain consistent capacity during abnormal conditions.

Understand virtualized networks. A virtualized network or network virtualization is the combination of hardware and software networking components into a single integrated entity. Examples include software-defined networks, VLANs, VPNs, virtual switches, virtual SANs, guest operating systems, port isolation and NAT. Define tunneling. Tunneling is the encapsulation of a protocol deliverable message within a second protocol. The second protocol often performs encryption to protect the message contents.

Understand VPNs. VPNs are based on encrypted tunneling. They can offer authentication and data protection as a point-to-point solution. Common VPN protocols are PPTP, L2TP, SSH, TLS and IPSec.

Understand split tunnel versus full tunnel. A split tunnel is a VPN configuration that allows a VPN connected client system to access both the organizational network over the VPN and the internet directly at the same time. A full tunnel is a VPN configuration in which all of the clients traffic is sent to the organizational network over the VPN link and then any internet Destin traffic is routed out of the organizational network's proxy or firewall interface to the internet. Be able to explain NAT. NAT protects the addressing scheme of a private network, allows the use of private IP addresses and enables multiple internal clients to obtain internet access through a few public IP addresses. NAT is supported by many security border devices such as firewalls, routers, gateways, WAPS and proxies. Know about third-party connectivity. Most organizations interact with outside third-party providers. Most of these external entities do not need to interact directly with an organization's IT or IS department. However, for the few that do, it's important to consider the risks and ramifications. This includes partnerships, cloud services and remote workers.

Understand the difference between packet switching and circuit switching. In circuit switching, a dedicated physical pathway is created between the two communicating parties. Packet switching occurs when the message or communication is broken up into small segments and sent across the intermediary networks to the destination. Within packet switching systems are two types of communication path or virtual circuits, permanent virtual circuits PVCs and switched virtual circuits SVCs.

Understand the various network attacks and countermeasures associated with communication security. Communication systems are vulnerable to many attacks, including distributed denial of service, eavesdropping, impersonation, replay, modification, spoofing and ARP and DNS attacks, be able to supply effective countermeasures for each. Those are the exam essentials that you'll need to know for Chapter 12, secure communications and network attacks.

From:
https://trident365.com/ - **三叉戟**

Permanent link:
https://trident365.com/doku.php?id=projects:cissp:chapter12

Last update: **2025/05/18 17:16**