Hi, I'm Mike Chapple and this is the audio review of the exam essentials for chapter 11 of the official CISSP study guide. Here are the top things you need to know for the exam from this chapter on secure network architecture and components.

Know the OSI model layers. The OSI layers are application, presentation, session, transport, network, data link and physical. Know the network container names. The network containers are OSI layer seven to five, protocol data unit PDU, layer four is a segment for TCP or a datagram for UDP, layer three is a packet, layer two is a frame and layer one are bits.

Understand the MAC address. Media access control or a MAC address is a 6-byte 48-bit binary address written in a hexadecimal notation. It's also known as the hardware address, the physical address, the nick address and the ethernet address. The first three bytes, 24 bits of the address is the organizationally unique identifier, OUI, which denotes the vendor or manufacturer.

Understand the TCP/IP model, also known as the DARPA or DoD model, the TCP/IP model has four layers. Application also known as process, transport also known as host to host, internet sometimes known as internetworking and link, although the terms network interface and sometimes network access are used for that last layer.

Understand DNS. The domain name system DNS is the hierarchical naming scheme used in both public and private networks. DNS links human friendly, fully qualified domain names and IP addresses together. DNSEC and DoH are DNS security features. Understand DNS poisoning. DNS poisoning is the act of falsifying DNS information used by a client to reach a desired system. It can be accomplished through a rogue DNS server, farming, altering a host file, corrupting IP configurations, DNS query spoofing and proxy falsification.

Know about ARP. The address resolution protocol ARP is essential to the interoperability of logical and physical addressing schemes. ARP is used to resolve IP addresses into Mac addresses. Also know about ARP poisoning, know about microsegmentation. Microsegmentation is dividing up an internal network into numerous sub zones, potentially as small as a single device, such as a high-value server or even a client or endpoint device. Each zone is separated from the others by internal segmentation firewalls, subnets or VLANs.

Know about edge networks. An edge network is a carefully designed data architecture that strategically allocates computing resources to edge devices within a network. This design helps distribute processing power demands away from central servers, empowering the devices to handle a significant portion of the processing workload.

Understand the various wireless technologies. Cell phones, bluetooth and Wi-Fi wireless networking are all wireless technologies, even though they all operate differently. Be aware of their differences, strengths and weaknesses.

Understand the basics of securing 802.11 networks. Know about RFID, NFC, satellite, narrowband and Zigbee. Understand site surveys. A site survey is a formal assessment of wireless signal strength, quality and interference using an RF signal detector. A site survey is performed by placing a wireless base station in a desired location and then collecting signal measurements from throughout the area.

Understand WPS attacks. Wi-Fi protected setup WPS is intended to simplify the effort involved in adding new clients to a secured wireless network. It operates by automatically connecting the first new wireless client to seek the network once WPS is triggered.

Understand captive portals. A captive portal is an authentication technique that redirects a newly

connected client to a web-based portal access control page. Know wireless attacks. Wireless attacks include war driving, wireless scanners and crackers, rogue access points, evil twins, disassociation, jamming, IV abuse and replay. Be familiar with CDNs. A content distribution network or content delivery network CDN is a collection of resource services deployed in numerous data centers across the internet to provide low latency, high performance and high availability of the hosted content.

Understand NAC. Network access control or NAC is the concept of controlling access to an environment through strict adherence to an enforcement of security policy. Know about 8021x pre-admission, post admission, agent-based and agentless NAC.

Understand the various types of firewalls. There are several types of firewalls. Static packet filtering, application level, circuit level, stateful inspection, NGFW and ISFW. Also know about virtual firewalls, filters, rules, [UNCLEAR], bastion hosts, ingress and egress, stateless versus stateful, WAF, secure web gateways, TCP wrappers, DPI and content and URL filtering. Know about proxies. A proxy server is used to mediate between clients and servers. Proxies are most often used in the context of providing clients on a private network with internet access while protecting the identity of the clients. Know about forward, reverse, transparent and non-transparent proxies.

Understand endpoint security. Endpoint security is the concept that each individual device must maintain local security, whether or not it's network or telecommunications channels also provide security. Endpoint detection and response is a combination of firewall, intrusion detection system, and anti-malware. Managed detection and response combines EDR with security information and event management, network traffic analysis and network IDS. Endpoint protection platform is an intrusion prevention system variant of EDR. Extended detection and response XDR is the combination of EDR, MDR and EPP often with cloud-based remote monitoring and analysis.

Be familiar with the common LAN technologies. The most common LAN technology is ethernet. Also be familiar with analog versus digital communications, synchronous versus asynchronous communications, duplexing, baseband versus broadband communications, broadcast, multicast, unicast, anycast and geocast communications. Know about CSMA, CSMA CD, and CSMA CA as well as token passing and polling. Those are the study essentials that you need to know for Chapter 11, secure network architecture and components.

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

Permanent link:
https://trident365.com/doku.php?id=projects:cissp:chapter11

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