بررسی ساختار دامنه چهارم CISSP

ذهنیت سازی امنیت ارتباطات و شبکه

دامنه چهارم

Communication and Network Security

4

بررسی جامع دامنه ۴ مدرک CISSP: امنیت ارتباطات و شبکه

(Communication and Network Security)

مقدمه:

در دنیای فناوری‌محور امروز، ارتباطات امن در بستر شبکه نقشی حیاتی در محافظت از دارایی‌های اطلاعاتی سازمان‌ها دارد. دامنه چهارم مدرک CISSP با عنوان "امنیت ارتباطات و شبکه"، مفاهیم و فناوری‌هایی را بررسی می‌کند که برای تضمین محرمانگی، یکپارچگی، و دسترس‌پذیری اطلاعات در حین انتقال طراحی شده‌اند. در این مقاله به بررسی ساختار مفهومی، ابزارها، تهدیدها و راهکارهای دفاعی این دامنه می‌پردازیم.

بخش ۱: مدل OSI - ستون فقرات درک مفاهیم شبکه

مدل OSI (Open Systems Interconnection) از ۷ لایه تشکیل شده است:

1. لایه فیزیکی (Physical)
2. لایه پیوند داده (Data Link)
3. لایه شبکه (Network)
4. لایه انتقال (Transport)
5. لایه جلسه (Session)
6. لایه نمایش (Presentation)
7. لایه کاربرد (Application)

درک این لایه‌ها برای تحلیل مسیر داده‌ها، محل وقوع حملات، و انتخاب ابزارهای دفاعی الزامی است.

بخش ۲: توپولوژی‌ها و رسانه‌های انتقال

توپولوژی‌ها:

- Bus
- Tree
- Star
- Ring
- Mesh

رسانه‌ها:

- سیمی: Twisted Pair، Coaxial، Fiber Optic
- بی‌سیم: امواج رادیویی، مادون قرمز، مایکروویو، Wi-Fi، WiMAX، GSM، CDMA

بخش ۳: پروتکل‌ها، دستگاه‌ها و ابزارهای پایه شبکه

- CSMA/CDو CSMA/CA برای مدیریت برخورد داده‌ها
- دستگاه‌هاHubs :، Switches، Routers، Firewalls، Application Firewalls
- پروتکل‌هاARP :، IP، ICMP، IGMP، PPTP، PPP، PAP، CHAP، EAP، TCP/UDP، SSL/TLS، BGP، HTTP/S، DNS، DHCP، LDAP

بخش ۴: حملات رایج در سطح شبکه

- Eavesdropping
- IP Spoofing
- SYN Flooding
- DoS / DDoS
- Man-in-the-Middle
- ARP Poisoning

بخش ۵: دفاع در عمق – ابزارهای امنیتی

- فایروال‌ها(Packet Filtering, Stateful, Circuit Proxy, Application Firewall)
- NAT / PAT
- IDS/IPS
- Segmentation، DMZ، Bastion Host
- Honeypot / Honeynet
- لیست‌های سفید/سیاه

بخش ۶: امنیت ارتباطات راه دور

- VPN: IPSec، PPTP، L2TP، GRE
- حالت‌ها: Transport Mode، Tunnel Mode
- احراز هویت دوطرفه، IKE، SA

- SOCKS ،SSH ،SSL/TLS
- پروتکل‌های مدیریت RADIUS :، TACACS+، Diameter، SNMP، Telnet

بخش ۷: احراز هویت در سطح شبکه

- PAP، CHAP، EAP، PEAP
- Mutual Authentication

بخش ۸: مفاهیم پیشرفته SDN و مجازی‌سازی

- VLAN
- SDN با API های Northbound/Southbound
- نقش Virtualization در جداسازی منابع

بخش ۹: دستورات پایه برای تحلیل شبکه

- ipconfig
- ping
- traceroute
- whois
- dig

بخش ۱۰: منابع آموزشی پیشنهادی برای یادگیری دامنه چهارم

1. کتاب رسمی $(ISC)^2$ CISSP CBK
2. دوره‌های ویدیویی Cybrary ،INE ،Pluralsight
3. سایت‌های آموزشی: InfoSec Institute ،SANS ،YouTube (مثل GRC و CBT Nuggets)
4. آزمایشگاه‌های عملی: TryHackMe (Network Security Labs) ،HackTheBox ،Cisco Packet Tracer
5. کتاب «CISSP All-in-One» نوشته Shon Harris