ITINS Exam Note - 2108121 - May 2026

Introduction

Threat: potential for violation of security; *vulnerability:* way by which loss can happen; *attack:* assault on security system.
Low impact: limited effects, degradation in functions, minor harm; *moderate impact:* serious effect, significant degradation in functions, significant harm; *high impact:* catastrophic effect, severe degradation, inability to perform 1 primary function, catastrophic harm to individuals, death.
White hat: ethical, legal; *grey hat:* commit crimes, unethical, not for personal gain; *black hat:* unethical, criminals, for personal gain.
Policy enforcement: *Secure:* reachable entirely in secure states with buffer; *precise:* reachable entirely in secure, no buffer; *board:* some reachable in secure, some not.

Threats, Risk Assessment & Trust

Trust: assumption system is secure; *Assurance:* degree of confidence that a system or service meets requirements.
Risk likelihood something bad happens & causes harm. *Ass. Steps:* 1. identify risks; 2. analyse likelihood; 3. formulate solutions for reducing; 4. continuously monitor. *Risk accepted:* low value, low frequency, low impact.
Single Loss Expectancy = Assets Value × Exposure Factor. SLE × Annual Rate Occurrence = Annual Loss Expectancy.
TCSEC (Orange Book): D minimal protection (fail / off the shelf); C1 discretionary protection (identification & authen. deployed & access control); C2 controlled access protection (object reuse & auditing configured); B1 labelled security protection (access control on limited objects, informal model of sec. pol.); B2 structured protections (trusted path for login, principl. least priv., formal sec. pol. model, config mgmt.); B3 security domains (full validation mechanism at arch. level, constraints on code devel., documentation & testing); A1 verified protection (formal methods analysis & verification, trusted distribution).
ITSEC E1 informal architecture, security target defined & tested; E2 informal descr. design, config control; E3 correspondence between code & sec. target; E4 formal model sec. pol. structured design, vulnerability analysis; E5 code matches design, code vuln. analysis; E6 formal architecture, formal design map to sec. pol., executable maps to source.

Firewalls

Types (in sec order): Basic Packet Filter, Circuit Level Proxy, Stateful PF, Application Level Proxy, Personal.
Ports: 20, 21 FTP; 22 SSH; 23 Telnet; 25 SMTP (send email); 52 DNS; 80 HTTP; 110 POP3 (col. email); 143 IMAP (col. email); 443 HTTPS. >1024 dynamically assigned. <1024 statically assigned to appl. Max no. 16383.
Routed mode: border between 2 networks, L3 NAT boundary; *Transparent mode:* between two existing routers, no NAT boundary, no IP altering.
Cisco Scenarios: *Small Branch:* 2 VLANS inside & outside; *Small Business:* 3 VLANS inside, outside, DMZ; *Enterprise:* corp hq, 2 remote wrks. IPsec VPN, ASA fw at boundaries of 3x network.

Intrusion {Detection/Prevention} Service

Network Intrusion: 1. reconnaissance; 2. access; 3. elevate; 4. root kit; 5. utilise.
IDS: out-of-band; passive inspection only; triggers logs / alerts after detection. Invented first.
IPS: physically in-line with core traffic flow path; active mitigation; drops packets; can introduce slight delay for pkt. inspection. IDS deploy where traffic go from one layer to another. IPS deploy in-line at border between diff. networks. IDS & IPS not mutex. Detection rules = signatures, like AV signatures. *Atomic* 1 packet; *composite* many packets. High accuracy for known exploits, blind to zero-days exploits. *Anomaly Based:* uses baseline of normal network behaviour patterns over time, flags metrics outside this, can identify zero-days, notorious for high false-positive rates
Cisco IPS Actions: Drop, alert, reset TCP connection, isolate

Authentication, Authorisation and Accounting

Methods: What you know, are, have. PWs, PINs, Biom. Alts: Graphical, Elec. Tattoos, Chip filled pills, SecurID.
Kerberos: User contacts Auth. Server (within Key Distribution Centre). AS responds with encrypted Ticket Granting Service Ticket. User sends TGT to TGS. TGS returns encrypted service ticket to user. User uses service ticket to access network service.
Kerberos v5: separate subkey for each session; authen. uses subkeys; authen. fwd. (ie print server can access email server on users behalf etc); realm hierarchies; multiple encryption schemes.
Administrative Domains: X.500 series of standards; X.511 defines standard operations
LDAP is simplified X.500; LDAP uses TCP

IPsec

Components: Security Protocol (Authentication Header or Encapsulating Security Payload); key management (Internet Key Exchange); Cryptographic Algorithms.
Packets: Header, Payload, Trailer.
AH: hashed message and message transmitted in plain sight; hash recomputed on receiving end to validate authenticity.
ESP encrypted message transmitted; authenticity optional using MD5 or SHA to hash message. Encryption always performed first.
Modes: *Transport:* security for transport layer and above; protect payload; original IP in plaintext; ESP used between hosts where encrypted TCP session forms. *Tunnel:* security for entire original IP packet; encrypted orig. packet and encapsulated in another; ESP tunnel formed in site-to-site between secure gateways.
authenticated, {encrypted}

Orig packet: IP header, TCP header, data

AH, Tra: IP header, AH header, TCP header, data

AH, Tun: New IP header, AH header, IP header, TCP header, data

ESP, Tra: IP header, ESP header, {TCP header, Data, ESP trailer}, ESP auth

ESP, Tun: New IP header, ESP header, {IP header, TCP header, Data, ESP trailer}, ESP auth

Security Associations: one-way sender-receiver relationship; defines protocol, mode, encryption or hashing, keys & key lifetimes,

SA lifetime.
IKE: R1 & R2 negotiate IKE phase 1 session: ISAKMP policy, DH key exchange, verify peer identity; R1 & R2 negotiate IKE phase 2 session: IPsec policy; information exchanged via tunnel; tunnel terminated.

Transport Layer Security & Virtual Private Network

TLS: C: ClientHello; S: ServerHello; S: Certificate, ServerHelloDone; C: ChangeCipherSpec, Finished; S: ChangeCipherSpec, Finished.
VPN: Remote access: IPsec or SSL, user initiated, from client to server. Site-to-Site: VPN gateway encapsulates all outgoing traffic, and decrypted on receiving site, IPsec.

MPLS

Between layer 2 and 3 of OSI. Maps IP addresses to fixed-length labels. Interfaces with RSVP and OSPF.
Shim: between link layer header & network layer header. Generic format: 20 bits label; 3 experimental bits (used as class of service); 1 bottom of stack; 8 TTL.
Components: Label Edge Router (edge of MPLS, assign and remove labels); Label Switching Router (high speed router in core of MPLS network); Forward Equivalence Class (representation of group of packets sharing same requirements, pkts assigned to FEC once when they enter network); Label Switched Path (path is representation of FEC, established before routing starts. Ether hop-by-hop (LSR independently selects next hop) or ingress LSR specifies nodes).
Operation: label creation and distribution; table creation at each router (making entries in label information base); label-switched path creation (done in reverse direction to entries in LIBs); label insertion / table lookup; packet forwarding.
Adv.: improves packet fwd. performance,; supports QoS & CoS; scalable; intergrates IP & ATM; interoperable. *Disadv.:* additional complexity for router & additional layer in packet.
MPLS VPN: Customer Edge Router, Provider Edge Router, Provider Router, AS Border Router

Auditing

Types: Process, Product, System
Syslog 0 emergency; 1 alert; 2 critical; 3 errors; 4 warnings; 5 notifications; 6 informative; 7 debug.
SNMP: v1: connectionless, community facility (authentication, access policy, proxy); v2 connection-oriented; v3 defines security to be used with v1 or v2 through user-based security model. Data secured using view-based access control model (defines access control policy)

Wi-Fi

802.11: a 54M@5G; b 11M@2.4G; g 45M@2.4G; n(4) 600M@2.4,5G; ac(5) 6.933G@5G; ax(6) 9.6078G@2.4,5G; d regulatory domains; e QoS; f IAPP; g DSS & TPC; i security; j Japan 5GHz; k measurements
Challenges: interference (unlicensed spectrum, blame baby monitors, mobile phones, microwaves); health issues.
Attacks: Reconnaissance; Rogue AP; WEP bit flipping; DoS; WLAN Jack
Authen. & Assoc.: Probe, Authentication, Association. S1: Unauth. & Unassoc.; S2: Auth. & Unassoc.; S3: Auth. & Assoc.
Open Auth.: On success, client & AP: Auth Algorithm No: 0; Authn Trans. Seq. No.: 1; AP only: Status Code: 0
Hierarchy: 802.11i (WPA2 Full std.) >WPA2 >WPA >WEP.
WEP: Static key, short 24-bit Initialisation Vector with RC4 cipher. Weak IVs repeat quickly, allows packet capture and decrypt root key.
WPA: Stopgap for WEP. Same hardware as WEP but needs firmware update. Replaces RC4 with TKIP and adds per-packet key hashing.
WPA2: Robust. Advanced CCMP (counter mode cipher block chaining message authentication code protocol), uses AES.
WPA vs. 802.11i: Common: OPeration within BSS, cipher & authentication negotiation during initial association, dynamic keys (temp. session keys), key hierarchy (pairwise master key produces pairwise transient key). Different: WPA no pre-authentication (802.11i has it which means client complete 802.1X auth. to new ap before disconnecting from current) *EAP Process:* EAP supplicant associates with AP; AP blocks all requests to LAN; client provides login credentials, sent to RADIUS; client auth. RADIUS server; RADIUS server auth. client; RADIUS server & client derive unicast WEP keys; RADIUS server delivers unicast WEP key to AP; AP delivers broadcast WEP key encrypted with unicast WEP key to client; client and AP activate WEP and use keys for transmission.
WLC Topology: Central switching: WLC switches all WLC traffic; Central vs. Local switching: branch site switch does local switching, all other traffic sent over WAN link to HQ for WLC switching. APs have to contact WLC over Layer 3.