Achievable

CCNA DUMP SHEET

Security concepts

Core terms, with the lock analogy

- **Vulnerability:** exploitable weakness in design, implementation, or configuration: a default password. *Faulty lock*
- **Exploit:** method or tool that takes advantage of one. *Lock pick*
- **Threat:** potential danger: an actor could use an exploit to harm an asset. *Burglar with the pick*
- **Mitigation:** technical (firewalls, IDS, encryption, patches) or procedural (policies, training). *New lock, alarm, guard*
- **CIA triad:** Confidentiality (authorized access only), Integrity (data unaltered), Availability (up when needed; DoS targets it)

Network attacks

Attack	How it works
MITM	Secretly intercepts and relays traffic
ARP poisoning	Forged ARP: attacker's MAC, gateway's IP
DoS	One source overwhelms a target
TCP SYN flood	Spoofed SYNs leave half-open connections
DDoS	Many bots under a botmaster, one target
MAC spoofing	Fake MAC poisons MAC tables, ARP caches
IP spoofing	Forged source IP hides the attacker
DHCP spoofing	Rogue server: attacker as gateway or DNS
DHCP starvation	Spoofed DHCP requests drain the pool
Buffer overflow	Past a buffer: crash or injected code

- **Counters:** SSH (MITM), DAI (ARP), DHCP snooping (rogues)

Malware and social engineering

Name	What it is
Virus	Attaches to a file, needs user action
Worm	Spreads by itself through vulnerabilities
Trojan	Poses as useful software, doesn't replicate
Phishing	Fake email: malicious link or attachment
Vishing	Phone call, such as fake IT support
Smishing	SMS text message
Spear phishing	Targeted phishing, after reconnaissance
Whaling	Spear phishing at a VP or CEO

- **Social engineering:** targets people, not systems

Security program elements

- **User awareness:** protect data and credentials, spot phishing, report incidents
- **User training:** periodic, required sessions that reinforce policy
- **Physical access control:** lock wiring closets (IDFs) and data centers. Key cards log who entered and when

Passwords and alternatives

- **Attacks:** guessing, dictionary, brute force (all combinations)
- **Policy:** complexity (long, mixed characters), regular changes, account lockout after failed logins
- **MFA:** two or more factors from different categories: something you know (password, PIN), have (token, smart card, phone code), or are (fingerprint, face)
- **Certificate:** proves ownership of a public key. Signed by a certificate authority (CA), revoked through a CRL. Expires, so clocks need NTP
- **Biometrics:** hard to steal, but masks can fool them, and injury or aging changes them

AAA, pronounced triple A

	Asks	For example
Authentication	Who is the user?	Username and password
Authorization	What may they do?	Which modes, commands
Accounting	What did they do?	Logins, commands, usage

- **Server:** central AAA server, such as Cisco ISE
- **Protocols:** TACACS+, RADIUS, on the device security sheet

Firewalls and IPS

Type	What sets it apart
Stateful	Rules plus state, by 5-tuple: IPs, ports, protocol. Replies pass, unsolicited packets drop
Zone-based	Zone to zone denied unless a rule allows: usually Inside to Outside only. DMZ for public servers
NGFW	Adds IPS, deep packet inspection, URL filtering
Proxy	Older: a gateway for specific applications
Host-based	Software in the OS, protects one host

- **IDS:** only alerts. **IPS:** blocks in real time

IPsec VPNs

	Site-to-site	Remote access
Links	Networks, LAN-to-LAN	One device to a network
For	HQ to branch offices	Teleworkers, contractors
Ends	Router or firewall per site	VPN client to concentrator or firewall
Client	None on end hosts	Runs on each device
Tunnel	Kept up automatically	Started by the user

- **IKE (IKEv1, IKEv2):** negotiates SAs, exchanges keys
- **IPsec:** encryption, authentication, integrity at Layer 3
- **Posture assessment:** remote access can check patches first