Chapter 1: The Concepts of Data Security

Data vs. Info

Data: Raw and unprocessed.

Information: Data that has been processed and organized.

Cybercrime

Any illegal activity using a computer, Internet, or network.

- **Monetary:** Stealing money.
- **Non-monetary:** Non-financial harm.

Threat Origins

- **Internal threats:** Come from employees, service providers, or insiders.
- **External threats:** Come from outside attackers or force majeure (acts of God).

Protection Motives

- **Personal:** Preventing identity theft.
- **Commercial:** Client privacy is a top priority.

The Hacking Spectrum & The CIA Triad

The Hacking Spectrum

Hacking: Unauthorized access without intent to harm.

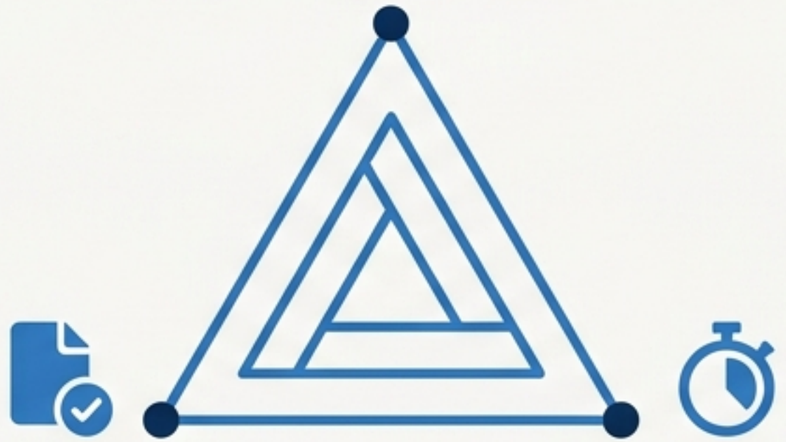
Cracking: Unauthorized access designed to cause damage.

Ethical hacking: Companies hire people to find system vulnerabilities before real attackers do.

Exam Tip: Hacking lacks harm intent; Cracking causes damage.

Confidentiality

Only authorized users access data.



Integrity

Data stays accurate and unaltered.

Availability

Data is reliable and accessible when needed.

Unauthorized access is prevented using usernames, passwords, and encryption.

Human Vulnerabilities

Identity Theft Methods

Information Diving: Dumpster diving (searching trash), social media exploitation, mail theft.

Skimming: Hardware stealing card info.

Pretexting: Fake identity/story to extract info.

Social Engineering (Manipulating human psychology to extract confidential data)

Vishing: Via phone.

Phishing: Via fraudulent emails.

Shoulder surfing: Physically watching someone enter a password.

Passwords should protect any document with sensitive information.

Key Takeaway

Human psychology is as vulnerable as digital systems; the CIA Triad is the foundation of protecting it.

Chapter 2: Malware & Concealment

Malware is malicious software that infiltrates, damages, or controls a device without permission.

Concealment Methods

Trojans: Hide as legitimate files.

Rootkits: Activate before the OS and are very hard to detect.

Backdoors: Let developers bypass security for permanent remote access.

Infectious vs. Surveillance Malware

Infectious Malware

Virus

Attaches to .exe files, spreads via shared files and email. Doesn't need human action to spread, but needs a host file.

Worm

A self-replicating virus subclass that spreads across connected systems without human action.

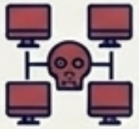
⚠ **Exam Tip:** Worms travel alone; Viruses need a host file!

Other Malware Types

Adware: Forces ads in free software and can be malicious.

Spyware: Silently monitors user activity (when adware becomes malicious).

Keystroke logging: Records every keyboard tap (used legitimately for corporate monitoring or maliciously for stealing passwords).



Botnets: Turn computers into zombies forming an army for coordinated attacks.

Dialers: Modify modems to secretly make long-distance calls (old-fashioned today).

The Antivirus Scan Flow

Step 1: Two Checks

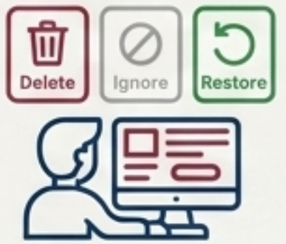
- **Dictionary check:** Matches files against known threats that must be updated weekly.
- **Behavioral check:** Detects suspicious activity.

Step 2: Isolation

Known threats go to quarantine, where infected files are isolated.

Step 3: Resolution

The user decides to delete, ignore, or restore. The antivirus software delegates the final decision to you.



Key Takeaway: Malware hides and spreads in different ways; antivirus relies on a two-step verification process to quarantine threats, delegating the final choice to the user.

Chapter 3: Network Security & Scale

WAN (Wide Area Network): Countries (e.g., the Internet is the ultimate WAN).

LAN (Local Area Network): Building/home (e.g., school printer sharing).

MAN (Metropolitan Area Network): City/campus (e.g., city libraries connected).

WAN (Wide Area Network): Countries (e.g., the Internet is the ultimate WAN).

Network: 2+ devices connected wirelessly or via cables to share resources.

Network Administrator: Maintains and updates these systems.

Firewall: Hardware or software that blocks unauthorized users and unwanted traffic before it enters your network.

Wireless Defenses & Access Control

Wireless Vulnerabilities & Protocols

Unsecured/open networks let eavesdroppers intercept everything (messages, browsing history).

WEP
WEAK

WEP (Wired Equivalent Privacy): **Older, weaker.**

WPA/WPA2
STRONG

WPA/WPA2 (Wi-Fi Protected Access): **Stronger, modern.**

MAC
DEVICE IDENTITY

MAC (Media Access Control): Controls access by recognizing a device's **unique hardware identity.**

MAC ADDRESS

Access Control

Systems require a username and password to verify identity.

The 6 Password Rules

- ☑ Long
- ☑ Mixed characters
- ☑ Never shared
- ☑ Not a dictionary word
- ☑ Not easy to guess
- ☑ Changed regularly

Identity Verification via Biometrics

Biometrics verify identity using unique body traits.

Fingerprint scan

Retina scan (scanning the back of the eye)

Hand geometry

Face recognition

⚠️ **Exam Tip:** Unlike passwords, biological traits can’t be stolen, shared, or forgotten.

Key Takeaway

Networks scale from personal to global, requiring layered digital locks (encryption protocols) and biological verification (biometrics) to secure access.

Chapter 4: Secure Data Management

Physical Security

The strongest firewall is useless if someone can walk in and take a laptop.

1. Equipment logs: Recording who has which device.

2. Cable locks: Tethering devices to fixed objects like desks.

3. Access control: Locking server room doors.

Backing Up Data

Scheduling frequent copies of files.

Method 1:
External drive / USB

Method 2:
Cloud backup service

Incremental Backup

A time-saving method that only copies files modified since the last full backup.

Deleting vs. Destroying Data

Deleting data	Destroying data
Moves it to the recycle bin to free up memory or remove sensitive info. Accidentally deleted files can be restored. It is only permanently removed once the bin is emptied.	Ensures files can never be recovered (irretrievable).

⚠ **Exam Tip:** Even emptied recycle bin files can be recovered by hackers. Only true data destruction guarantees safety.

Destruction Methods

Shredding
(paper/CDs)

Degaussing
(using powerful magnets to erase magnetic drives)

Drive destruction
(physically crushing a hard drive)

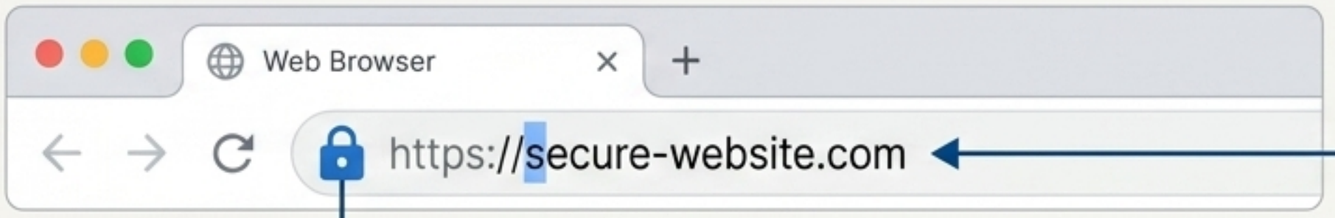
Data destruction utilities
(software that permanently overwrites files)

Key Takeaway: Digital firewalls cannot stop physical theft; data is only truly gone when physically or cryptographically destroyed.

Chapter 5: Secure Web Use

Web Verification

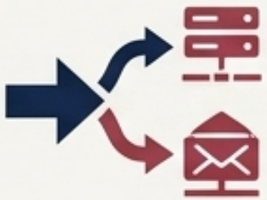
Secure websites stop unauthorized people from seeing data.



Look for the S in HTTPS + Lock Icon: Signs that SSL/TLS encryption is protecting you.

Digital Certificates: Electronic ID cards that prove a website is real and belongs to who it says it does.

The Pharming Threat



Attack

Malicious code sends you to a fake website even when you type the correct URL.

Defense

One-Time Passwords (OTP).
Passwords that work only once and expire quickly.
Sent as an extra layer via SMS or email (does not replace login).
A hacker would need access to two separate devices to break in.

Tracking & Blocking

Cookies

Small messages a server sends to your browser to remember who you are, save preferences, keep you logged in, and track browsing habits.

Session cookies: Disappear when you close the browser.

Permanent cookies: Stay until they expire or you delete them yourself.

Content Control Software (Censorware)

Limits what content can be seen and how long a device is used.

Internet filtering: Blocks certain websites.

Parental controls: Manage screen time, programs, and file access based on user needs.

Key Takeaway: Cookies track to personalize your experience, while censorware blocks harmful content to protect you; always look for the visual identifiers of SSL/TLS encryption.

Chapter 7: Protocols for Secure Communications

The 4 Pillars of Network Security

1. **Confidentiality:** Encryption stops unauthorized reading.
2. **Authentication:** Verifying identity.
3. **Message Integrity:** Detecting changes in data.
4. **Access & Availability:** Verified users can reach services when needed.

Cryptographic Web Protocols

(Security rules added on top of existing apps)

1.	**SSL**	Uses public key encryption to protect a whole session as a secure channel. Provides confidentiality, integrity, authentication. Offers an API with C and Java libraries. (TLS is the newer version of SSL).
2.	**S-HTTP / HTTPS**	Encrypts single messages between browser and server.
3.	**SET**	MasterCard & VISA (1997). Uses DES for card info and RSA for key exchange (works online/in-store).
4.	**SSH-2**	Works alongside protocols to secure web browsers and e-commerce.

Exam Tip: S-HTTP = single messages; SSL = whole channel!

The Secure Email Flow (Alice & Bob)

Step 1 (Secrecy):

Alice encrypts her message with a random symmetric key (Ks).

Step 2 (Key Delivery):

Alice encrypts Ks with Bob's public key.

Step 3 (Authentication & Integrity):

Alice sends the message in the clear with a digital signature (a hash encrypted with her private key).

Step 4 (Verification):

Bob verifies with Alice's public key and re-hashes the message.

Total Security = 3 Keys. (Alice's private, Bob's public, and a temporary symmetric key working together for secrecy, authentication, and integrity).

Email, Network, & Wireless Standards

Email Standards

S/MIME: Adds signatures and encryption.

PEM: Uses 3DES.

PGP: (Phil Zimmermann, 1991). Unofficial email standard. Uses IDEA Cipher (128-bit key, 64-bit blocks) + RSA for both key exchange and digital signatures. Provides 6 services: authentication, encryption, compression, compatibility, segmentation, key management.

Network

IPSec: Secures data at the IP packet level using AH (identity) and ESP (encryption). Combines Diffie-Hellman, public key cryptography, bulk encryption algorithms, and CA-signed certs.

Wireless Evolution

WEP failed early -> WPA/WPA2 fixed it -> Next gen is RSN with AES Counter Mode and AES Offset Codebook. Bluetooth is vulnerable within 30 feet.

SSL/TLS Lifecycle Flow

Handshake -> Key derivation -> Data transfer -> Connection closure.

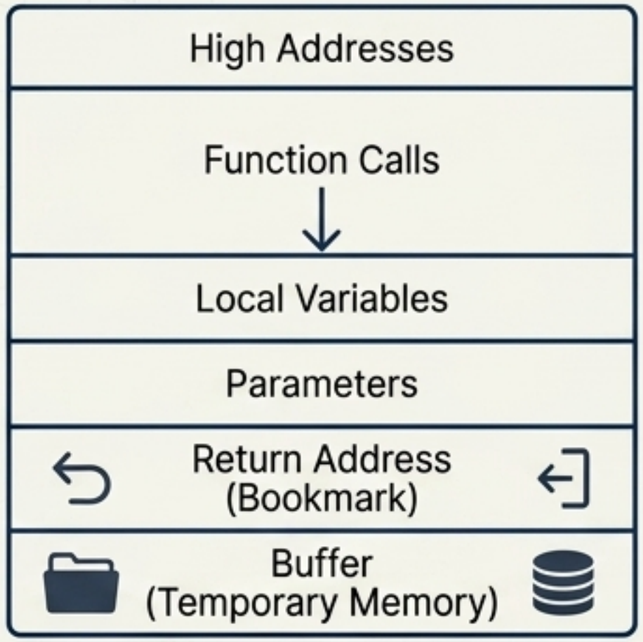
Key Takeaway

Symmetric keys = speed; Public/Private keys = secure delivery + authentication; Hashing = integrity.

Chapter 8: Software Security & Buffer Overflow

Core Rule: All user input is evil — never trust it.

The Stack



Memory organized in frames, high to low addresses. Manages function calls and stores: local variables, parameters, and the return address (bookmark for where to return). A buffer is temporary memory for a set amount of data.

Buffer Overflow Attack

The Flaw:
Not checking input length (e.g., a 12-byte buffer uses gets()).

The Attack:
Attacker types 50 characters, spilling into other memory and overwriting the return address.

The Payload: Deploys ShellCode (creates a shell for arbitrary commands) running with host program or OS root privileges.

Mitigation Principle: Least privilege principle (give programs only the minimum permissions needed).

Attack Variations & The Two Layers of Defense

Buffer Attack Variations

- 🔗 **Return-to-libc**: Redirects to existing library functions.
- 🧱 **Heap overflows**: Target dynamic memory (**malloc()/free()**), overwriting function pointers.
- 💔 **Heartbleed**: Over-read bug leaking passwords and encryption keys.

Code-level (Developer)

- Use **safe languages** (Java, C++, Python) with strong typing, automatic bounds checking, and automatic memory management (Trade-off: performance degradation).
- **Unsafe languages (C)**: Treat input as evil, use safer functions with bounds checking, deploy analysis tools like OWASP.
- **Note**: Hard to eliminate all overflows.

System-level (OS/Hardware)

- 🐦‍⬛ **Stack canaries**: Random value before return address, compared with a copy in a register. Mismatch = program halted.
- 🔀 **ASLR**: Randomizes stack/heap/libc locations each run.
- 🛑 **Non-executable stack**: Refuses to run code placed on the stack.

⚠️ **Exam Tip:** Code-level relies on developers; System-level relies on OS/Hardware randomizations.

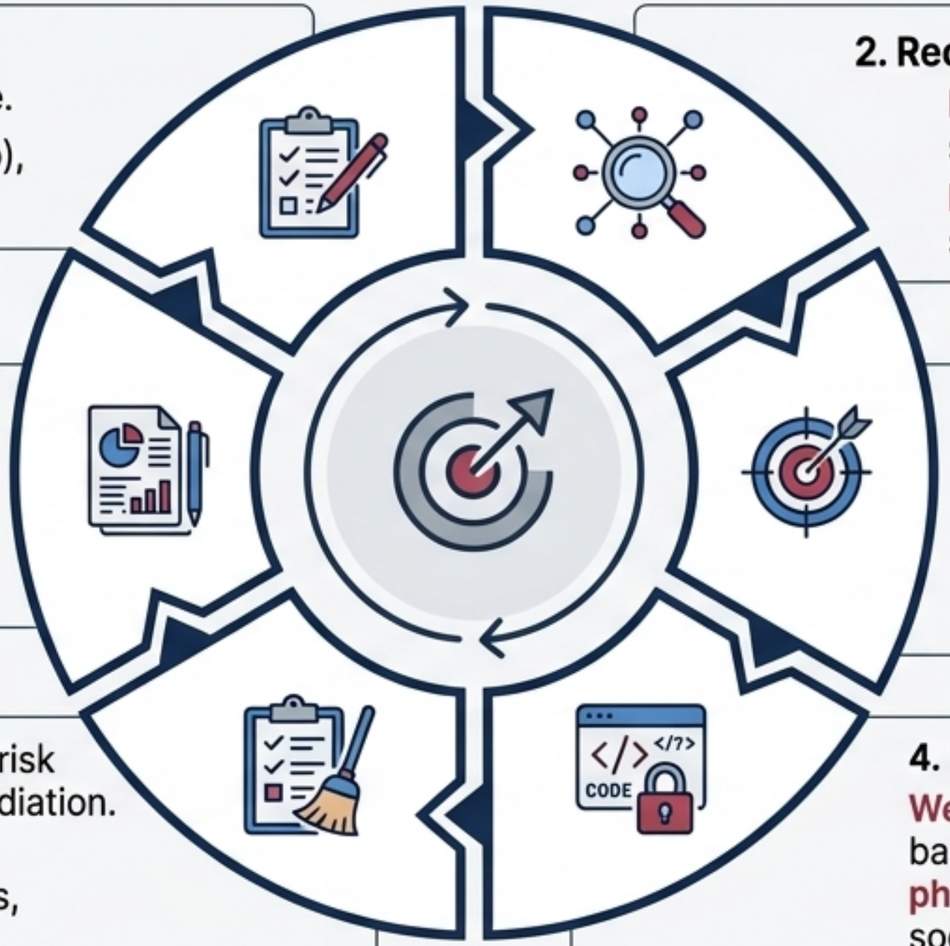
Key Takeaway:
Never trust user input; mitigating buffer overflows requires proactive developer coding and reactive system-level hardware traps.

Chapter 9: The 6 Phases of Penetration Testing

Penetration testing: An authorized ethical hacker legally tests systems for vulnerabilities to provide verifiable proof of security (must be regular, not one-time).

1. Pre-Engagement: Define rules, legal, budget, timeline, objectives, risks, culture.

Choose: **White Box** (full), **Black Box** (zero), **Gray Box** (partial).



2. Reconnaissance/OSINT: Public intelligence.

Internet footprinting (search, WHOIS, scraping, social engineering/sales calls).

Internal footprinting (ping sweeps, port scanning, reverse DNS, packet sniffing).

3. Threat Modeling: Map attack vectors by value. Categorize **internal threats** (management/vendors) and **external threats** (open ports/web apps).
Use a **vulnerability scanner**, then manually **validate**.

4. Exploitation: Test limits.

Web app attacks, network attacks, memory-based attacks, **zero-day exploits**, and **physical & edge attacks** (Wi-Fi, breaches, social engineering).

5. Post-Exploitation: Document, conduct risk analysis (financial value), actionable remediation.

Cleanup: eliminate rootkits/backdoors, remove scripts/temp files, delete accounts, reconfigure to pre-test state.

6. Reporting: Written recommendations, security risk score, and strategic remediation roadmap on a prioritized timeline (**OS hardening, patching, policy, training, monitoring**).

The 6 Types of Pen Testing

Network

- Port scans, packet sniffing, host discovery, password cracking, buffer overruns, spoofing.

Web App

- Logic flaws, session management, cookie manipulation, brute-force, poor server config, file upload/download attacks, HTML/SQL injection, manual testing.

Mobile

- Protect data on device and in transit, secure credentials/session management, backend API security, third-party integration, user consent, prevent access to paid resources, secure provisioning.

Wireless

- Rogue access points, vendor defaults, eavesdropping, no monitoring, misconfigured firewalls, WEP weaknesses, MITM, DoS.

API

- Excessive data exposure, injection flaws, lack of rate limiting, improper assets management, insufficient logging.

Continuous

Standard tests are just snapshots; a single update can destabilize security — continuous testing fills the gaps.

Vendor Selection Checklist & Final Takeaway

Selecting a Penetration Testing Vendor

	**1.** Define project scope.
	**2.** Verify specialized skills for your industry.
	**3.** Demand credentials (PTES, OSSTM, OWASP).
	**4.** Check actual client references.
	**5.** Review sanitized sample reports (clear, no jargon).

	**6.** Agree on data security (accessed, handled, stored, disposed of).
	**7.** Verify liability insurance.
	**8.** Set rules of engagement (scope, limitations, availability).
	**9.** Define expectations.
	**10.** Determine frequency: one-time, follow-ups, ongoing, or on-demand.

Final Takeaway

Security must be verified, not trusted; thorough pen testing requires clear rules of engagement, exhaustive exploitation, and meticulous post-test cleanup. Data is your most valuable asset—protect it accordingly.