Information Security – CS439

Eng. Abdo Saeed

65880042

Introduction to Information Security

1. What is Information Security?

Information Security is the practice of **protecting information** against threats like **unauthorized access, disclosure, alteration, or destruction**, while maintaining:

- **Confidentiality** – only authorized people can access it.
- **Integrity** – data remains accurate and unchanged unless properly authorized.
- **Availability** – information is accessible to authorized users when needed.

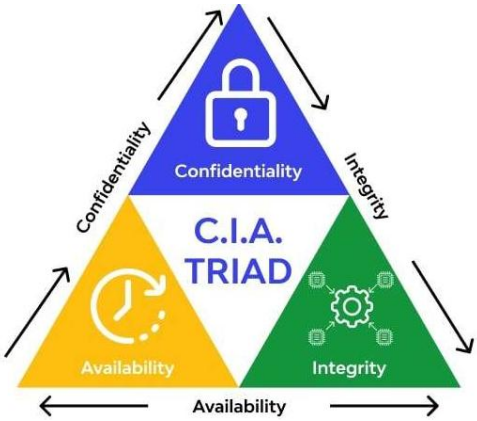
Achieved through:

- Policies
- Awareness programs
- Training & Education
- Technology

Main goals:

- **Prevention**: Stop attackers from exploiting systems.
- **Detection**: Identify when exploitation is happening.
- **Recovery**: Continue functioning correctly even if compromised.

CIA Triangle



- **Confidentiality** – prevents unauthorized access.
- **Integrity** – prevents unauthorized changes.
- **Availability** – ensures resources remain usable to authorized users.

Vulnerabilities

A **vulnerability** = a weakness in systems, processes, or designs that attackers can exploit.

Types of vulnerabilities:

1. **External** – Internet-facing weaknesses (e.g., exposed servers).
2. **Internal** – Weaknesses inside the organization.
3. **Application & Database** – Bugs in apps or databases.
4. **Physical** – Risks from physical access or damage.
5. **Network & Wireless** – Weaknesses in wired/wireless setups.
6. **Social Engineering** – Human mistakes via manipulation.

Attacks

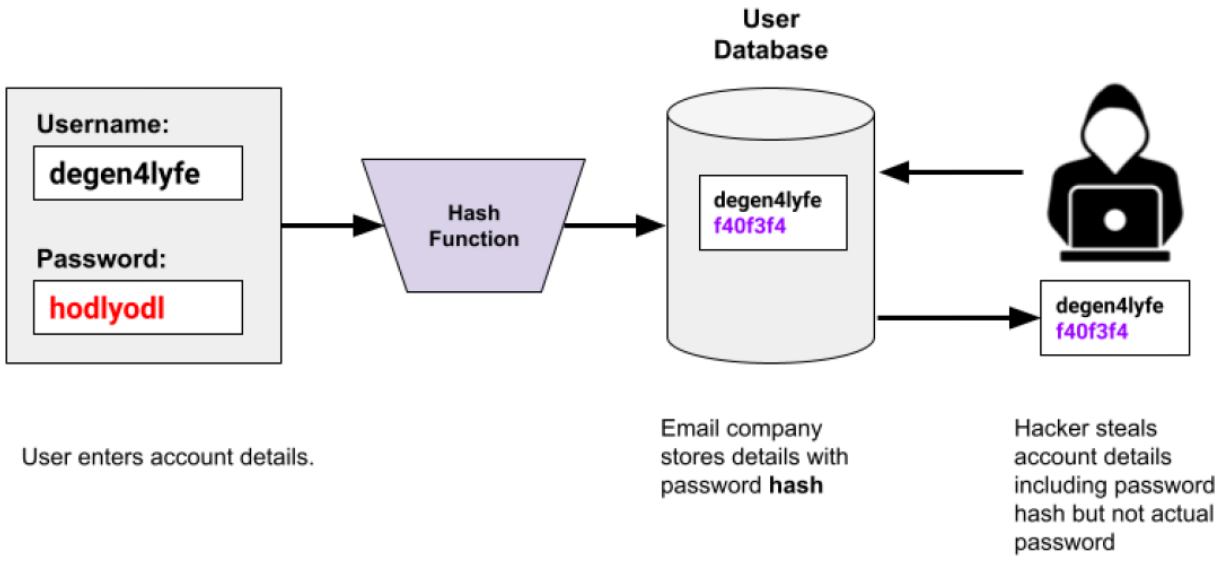
An **attack** = exploiting a vulnerability to damage or steal data.

- **Passive attacks**: spying/eavesdropping.
- **Active attacks**: password guessing, Denial of Service (DoS).

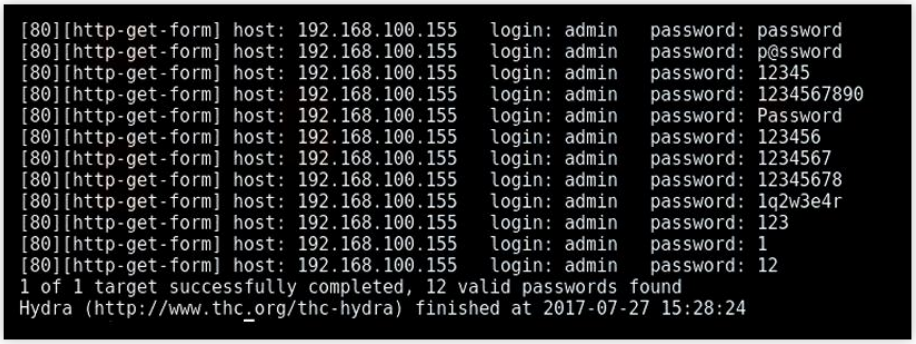
Types of attackers: Hackers, criminals, insiders, nation-states.

Password Attacks

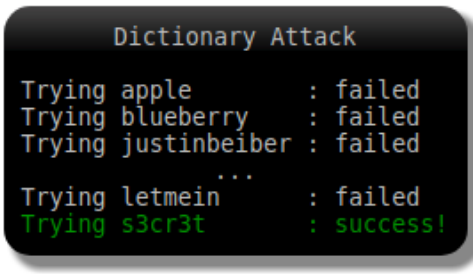
Password Cracking: Trying to reverse-calculate a password.



Brute Force Attack: Trying all possible password combinations.

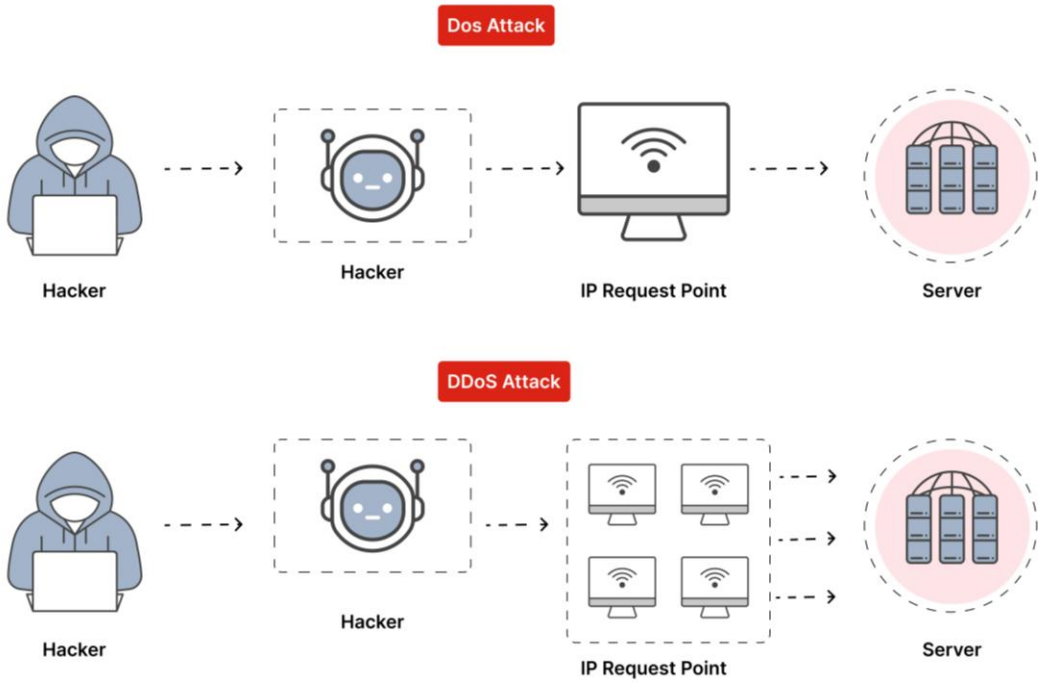


Dictionary Attack: Trying common passwords from a “dictionary.”



DoS vs DDoS

- **DoS (Denial of Service)**: Overloads a system to make it unavailable.
- **DDoS (Distributed DoS)**: Same attack, but from multiple devices simultaneously.



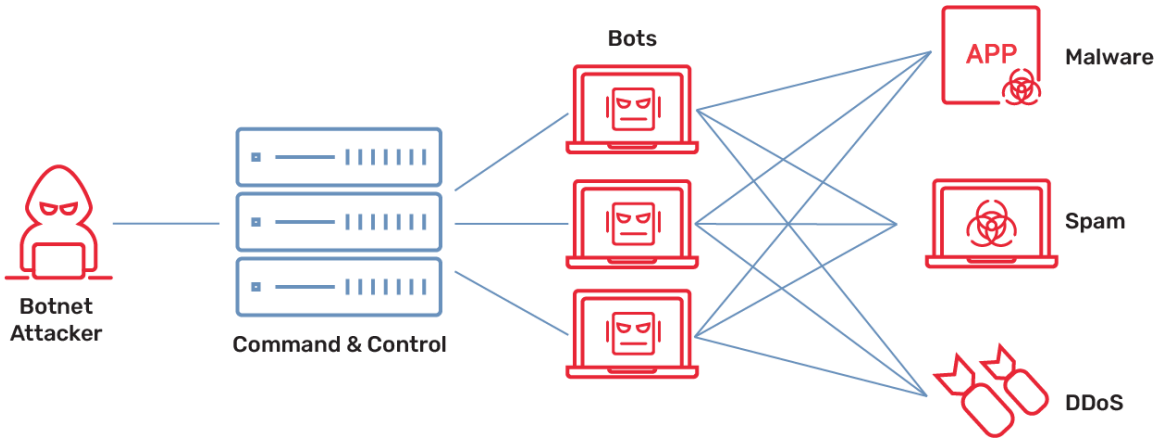
Parameter	DOS	DDOS
Full Form	Denial Of Service	Distributed Denial Of Service
Source of attack	DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource	DDoS attack uses multiple computers and Internet connections to flood the targeted resource.
Protection	System can be stopped/protected easily	Difficult to protect system against DDOS attack
Threat Level	Low threat level	Medium to high threat level, as these can be used to do some serious damage to networks and end systems.
Malware involvement	No malware involved	A botnet is usually made up of thousands of infected pc's.
Cost and management	Easier to operate and manage	Not easy to manage and operate

WWW.IPWITHEASE.COM

Botnets

A **Botnet** = network of malware-infected devices controlled remotely.

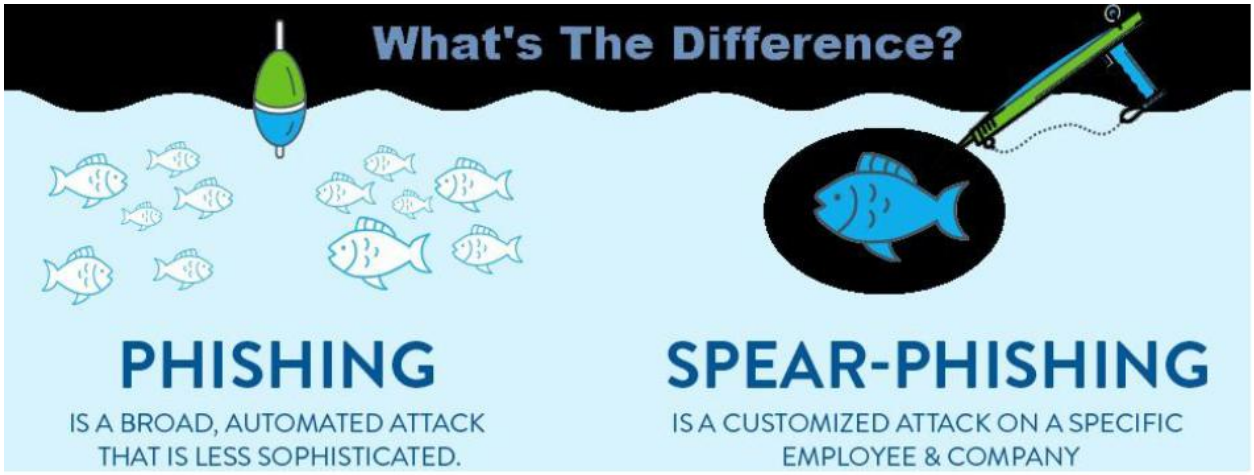
- Used for spam, DDoS, or data theft.
- Controlled via **Command & Control (C&C) servers**.



Social Engineering

Social Engineering is manipulating people to **reveal sensitive information**

- Examples: phishing



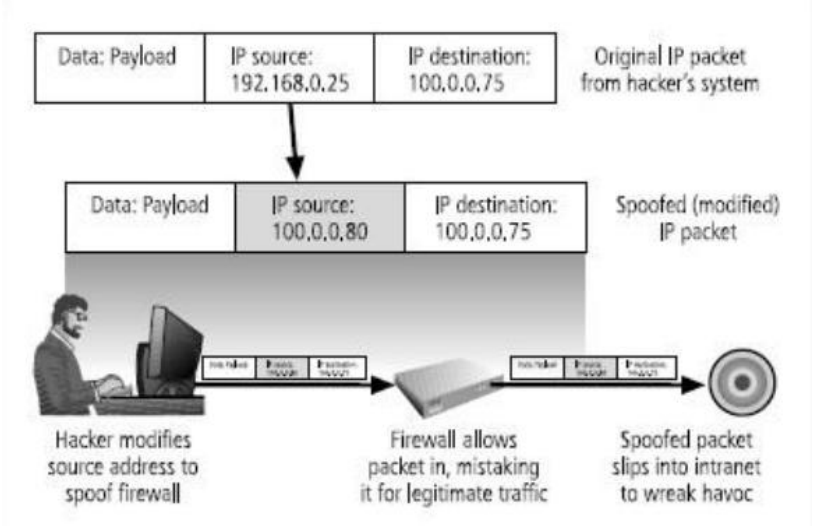
Spoofing Attacks

Spoofing means tricking systems or users by falsifying identity.



Types of Spoofing

IP Spoofing – Fake IPs to gain access.



- **Face Spoofing** – Fooling biometric systems with photos/videos.



Hong Kong arrests eight over disguised air passenger

Chinese man, believed to be in his 20s, donned Hollywood-style 'old man' mask to board flight to Canada

▲ A young man boarded an Air Canada flight in Hong Kong while elaborately disguised as an elderly man.
Photograph: Canada Border Services Agency/AP

- **Link Spoofing** – Malicious URLs made to look genuine (e.g., kcst-edu.kw vs kcst.edu.kw).

https://www.kcst-edu.kw

Vs.

https://www.kcst.edu.kw

- **Email Spoofing** – Fake "trusted" sender to trick victims.

From: ceo@kcst.edu.kw
To: FinancialManger@kcst.edu.kw
Subject: Urgent Request

Please transfer 50,000 KW to this account immediately. (attacker account)
- CEO

- **SMS Spoofing** – Fake text messages.



- **Caller ID Spoofing** – Fake numbers to scam.



- **Location Spoofing** – Faking GPS/social media location.



RANSOMWARE

Ransomware – type of malware designed to **block access to a computer system or data** until a ransom is paid



- **Scams** – Fraud to steal money/data.
- **Types:**
    - Telemarketing scams
    - Fake shopping sites
    - Phishing emails
    - Fake job offers
    - Identity theft
    - Fake donations
    - Catfishing

Recommendations to Avoid Cyber Attacks

- Report scams immediately.
- Check emails for spelling/grammar errors.
- Verify URLs (look for HTTPS padlock).
- Don’t click suspicious links.
- Enable **two-factor authentication**.
- Keep systems updated & patched.
- Use firewalls & anti-spoofing tools.
- Train employees on cyber hygiene.
- Make file extensions visible.
- Use penetration testing to find vulnerabilities.