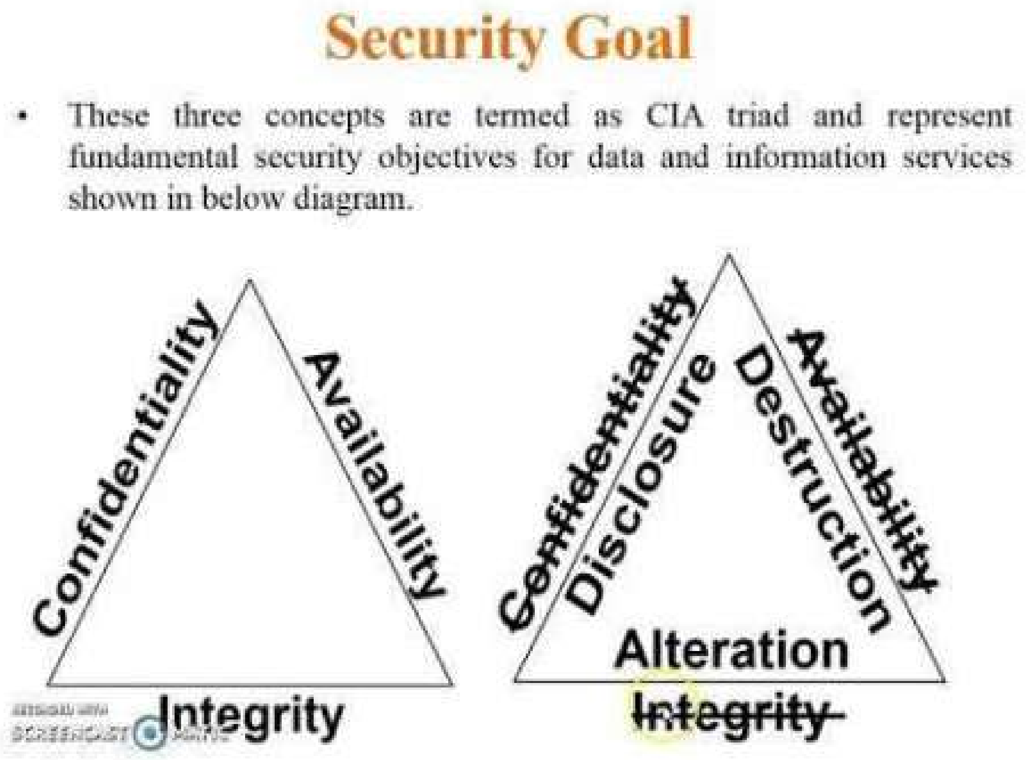
0. Introduction

Fundamental Security Concepts

The whole principle is to avoid **Theft, Tampering and Disruption** of the systems through **CIA Triad** (Confidentiality, Integrity and Availability).



Security Goal

- These three concepts are termed as CIA triad and represent fundamental security objectives for data and information services shown in below diagram.

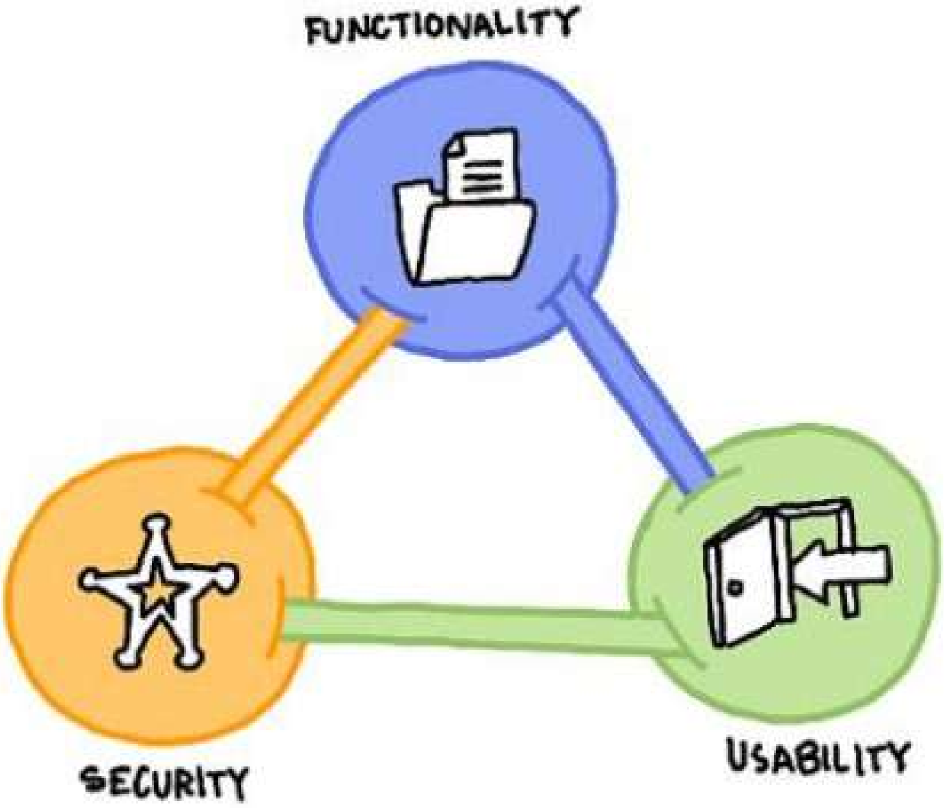
- **Confidentiality** Keeping systems and data from being accessed, seen, read to anyone who is not authorized to do so.
- **Integrity** Protect the data from modification or deletion by unauthorized parties, and ensuring that when authorized people make changes that shouldn't have been made the damage can be undone.
- **Availability** Systems, access channels, and authentication mechanisms must all be working properly for the information they provide and protect to be available when needed.

Note: *In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. (ISO/IEC 27000:2009)*

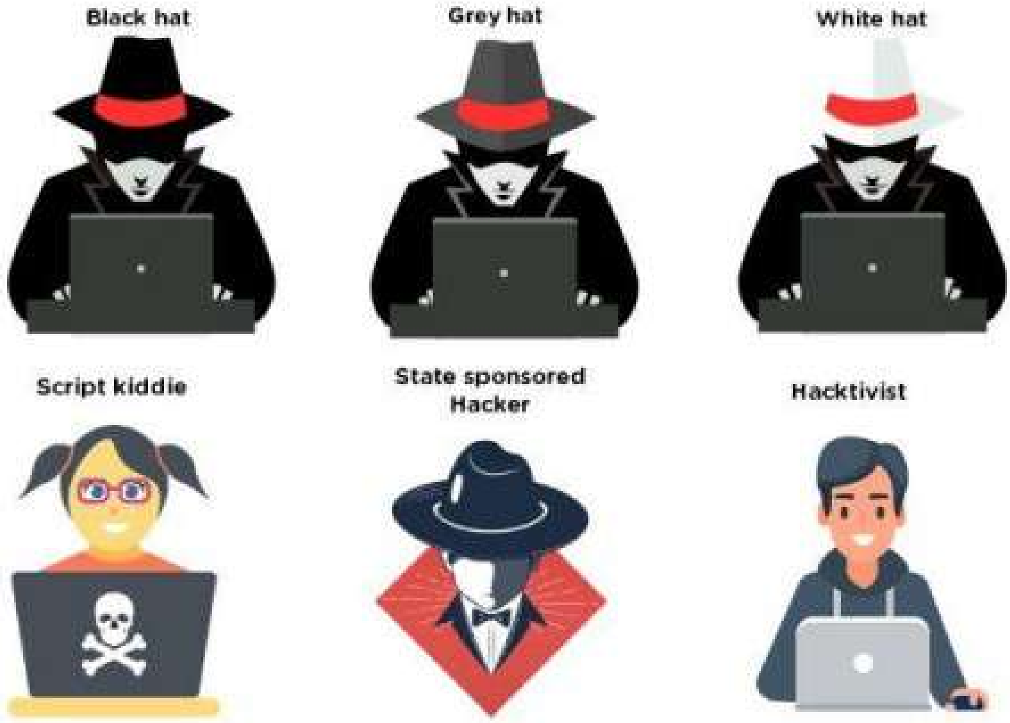
- **Auditing & Accountability** Basically keep tracking of everthing, like, who's been logging in when are they loggin in whose access this data.
- **Non-Repudiation** Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

Security, Functionality and Usability balance

There is an inter dependency between these three attributes. When **security goes up, usability and functionality come down**. Any organization should balance between these three qualities to arrive at a balanced information system.



Types of Hackers



- **Black Hat** - Hackers that seek to perform malicious activities.
- **Gray Hat** - Hackers that perform good or bad activities but do not have the permission of the organization they are hacking against.
- **White Hat** - Ethical hackers; They use their skills to improve security by exposing vulnerabilities before malicious hackers.

Script Kiddie / Skiddies - Unskilled individual who uses malicious scripts or programs, such as a web shell, developed by others to attack computer systems and networks and deface websites.

State-Sponsored Hacker - Hacker that is hired by a government or entity related.

Hacktivist - Someone who hacks for a cause; political agenda.

Suicide Hackers - Are hackers that are not afraid of going jail or facing any sort of punishment; hack to get the job done.

Cyberterrorist - Motivated by religious or political beliefs to create fear or disruption.

Hacking Vocabulary

- **Hack value** - Perceived value or worth of a target as seen by the attacker.
- **Vulnerability** - A system flaw, weakness on the system (on design, implementation etc).

- **Threat** - Exploits a vulnerability.
- **Exploit** - Exploits are a way of gaining access to a system through a security flaw and taking advantage of the flaw for their benefit.
- **Payload** - Component of an attack; is the part of the private user text which could also contain malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.
- **Zero-day attack** - Attack that occurs before a vendor knows or is able to patch a flaw.
- **Daisy Chaining / Pivotting** - It involves gaining access to a network and /or computer and then using the same information to gain access to multiple networks and computers that contains desirable information.
- **Doxxing** - Publishing PII about an individual usually with a malicious intent.
- **Enterprise Information Security Architecture** (EISA) - determines the structure and behavior of organization's information systems through processes, requirements, principles and models.

Threat Categories

- **Network Threats**
    - Information gathering
    - Sniffing and eavesdropping
    - DNS/ARP Poisoning
    - MITM (Man-in-the-Middle Attack)
    - DoS/DDoS
    - Password-based attacks
    - Firewall and IDS attack
    - Session Hijacking
- **Host Threats**
    - Password cracking
    - Malware attacks
    - Footprinting
    - Profiling
    - Arbitrary code execution
    - Backdoor access
    - Privilege Escalation
    - Code Execution

- **Application Threats**
  - Injection Attacks
  - Improper data/input validation
  - Improper error handling and exeception management
  - Hidden-field manipulation
  - Broken session management
  - Cryptography issues
  - SQL injection
  - Phishing
  - Buffer Overflow
  - Information disclosure
  - Security Misconfigurations

Attack Vectors

Path by which a hacker can gain access to a host in order to deliver a payload or malicious outcome

- **APT - Advanced Persistent Threats**
  - An advanced persistent threat is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period; Typically uses zero day attacks.
- **Cloud computing / Cloud based technologies**
  - Flaw in one client's application cloud allow attacker to access other client's data
- **Viruses, worms, and malware**
  - Viruses and worms are the most prevalent networking threat that are capable of infecting a network within seconds.
- **Ransomware**
  - Restricts access to the computer system's files and folders and demands an online ransom payment to the attacker in order to remove the restrictions.
- **Mobile Device threats**

- **Botnets**
  - Huge network of compromised systems used by an intruder to perform various network attacks
- **Insider attacks**
  - Disgruntled employee can damage assets from inside.
  - Huge network of compromised hosts. (used for DDoS).
- **Phishing attacks**
- **Web Application Threats**
  - Attacks like SQL injection, XSS (Cross-site scripting)...
- **IoT Threats**

Attack Types

1. Operating System

Attacks targeting OS flaws or security issues inside such as guest accounts or default passwords.

- **Vectors**: Buffer overflows, Protocol Implementations, software defects, patch levels, authentication schemes

2. Application Level

Attacks on programming code and software logic.

- **Vectors**: Buffer overflows, Bugs, XSS, DoS, SQL Injection, MitM

3. Misconfiguration

Attack takes advantage of systems that are misconfigured due to improper configuration or default configuration.

- **Examples**: Improper permissions of SQL users; Access-list permit all

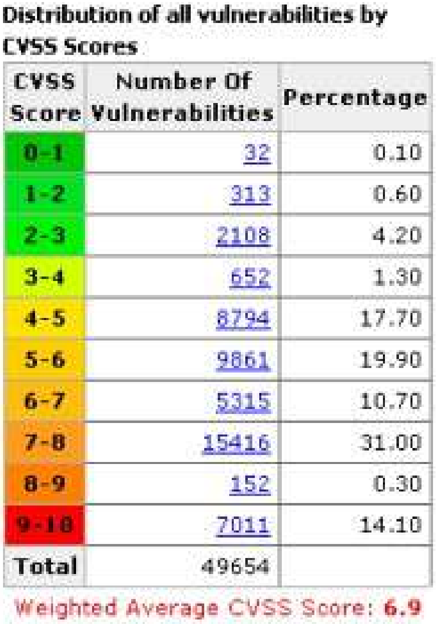
4. Shrink-Wrap Code

Act of exploiting holes in unpatched or poorly-configured software.

- **Examples**: Software defect in version 1.0; DEfect in example CGI scripts; Default passwords

Vulnerabilities

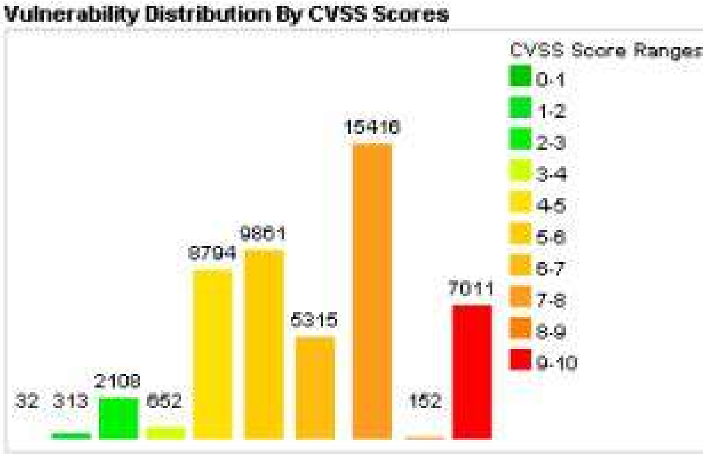
- **CVSS - Common Vulnerability Scoring System** [+]
    - Places numerical score based on severity



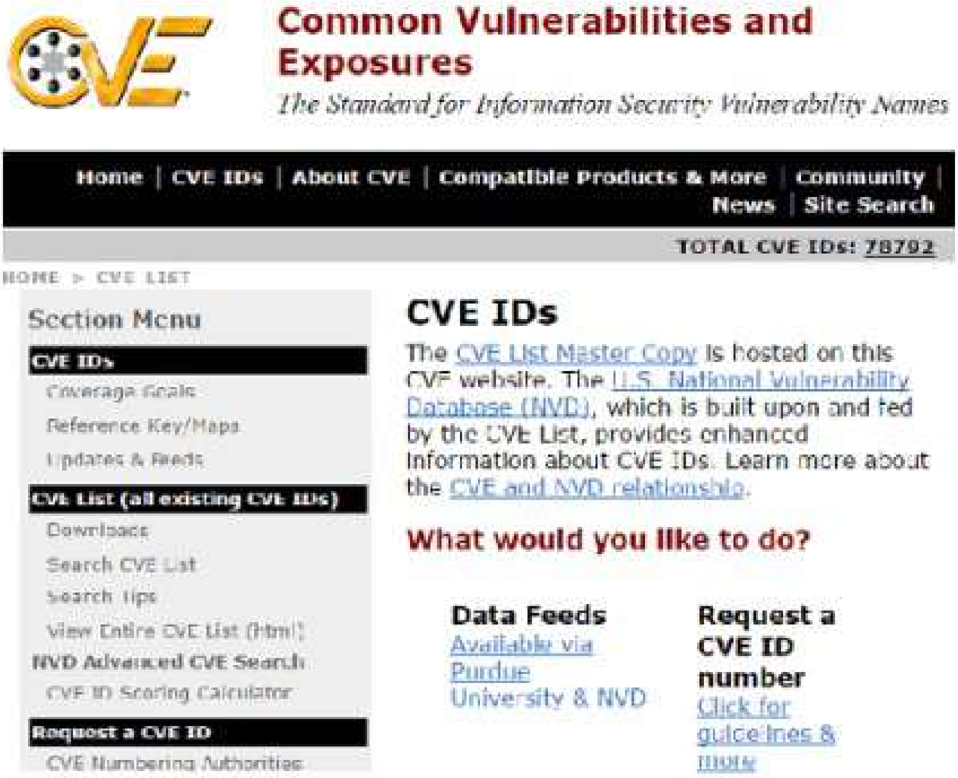
Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	32	0.10
1-2	313	0.60
2-3	2108	4.20
3-4	652	1.30
4-5	8794	17.70
5-6	9861	19.90
6-7	5315	10.70
7-8	15416	31.00
8-9	152	0.30
9-10	7011	14.10
Total	49654	

Weighted Average CVSS Score: **6.9**



- **CVE – Common Vulnerabilities and Exposures** [+]
    - Is a list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE.



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Home | CVE IDs | About CVE | Compatible Products & More | Community | News | Site Search

TOTAL CVE IDs: 78792

HOME > CVE LIST

Section Menu

CVE IDs

Coverage Goals

Reference Key/Maps

Updates & Feeds

CVE List (all existing CVE IDs)

Downloads

Search CVE List

Search Tips

View Entire CVE List (Html)

NVD Advanced CVE Search

CVE ID Scoring Calculator

Request a CVE ID

CVE Numbering Authorities

CVE IDs

The CVE List Master Copy is hosted on this CVE website. The U.S. National Vulnerability Database (NVD), which is built upon and fed by the CVE List, provides enhanced information about CVE IDs. Learn more about the CVE and NVD relationship.

What would you like to do?

Data Feeds
Available via Purdue University & NVD

Request a CVE ID number
Click for guidelines & more

- **NVD - National Vulnerability Database** [+]
  - is a database, maintained by NIST, that is fully synchronized with the MITRE CVE list; US Gov. vulnerabilities repository.

Vulnerability Categories

- **Misconfiguration** - improperly configuring a service or application
- **Default installation** - failure to change settings in an application that come by default
- **Buffer overflow** - code execution flaw
- **Missing patches** - systems that have not been patched
- **Design flaws** - flaws inherent to system design such as encryption and data validation
- **Operating System Flaws** - flaws specific to each OS
- **Default passwords** - leaving default passwords that come with system/application

Pen Test Phases (CEH)

1. **Pre-Attack Phase** - Reconnaissance and data-gathering.
2. **Attack Phase** - Attempts to penetrate the network and execute attacks.

3. **Post-Attack Phase** - Cleanup to return a system to the pre-attack condition and deliver reports.

⚠ For the exam, EC-Council brings his own methodology and that's all you need for the exam; you can check another pentesting methodologies here if you are interested; In case you are studying to become a professional pentester besides certification content, I recommend the OSSTMM (Open Source Security Testing Methodology Manual).

The Five Stages of Ethical Hacking

1. Reconnaissance

Gathering evidence about targets; There are two types of Recon:

- **Passive Reconnaissance**: Gain information about targeted computers and networks **without direct interaction with the systems**.
    - e.g: Google Search, Public records, New releases, Social Media, Wardrive scanning networks around.
- **Active Reconnaissance**: Envolves direct interaction with the target.
    - e.g: Make a phone call to the target, Job interview; tools like Nmap, Nessus, OpenVAS, Nikto and Metasploit can be considered as Active Recon.

2. Scanning & Enumeration

Obtaining more in-depth information about targets.

- e.g: Network Scanning, Port Scanning, Which versions of services are running.

3. Gaining Access

Attacks are leveled in order to gain access to a system.

- e.g: Can be done locally (offline), over a LAN or over the internet.
    - e.g(2): Spoofing to exploit the system by pretending to be a legitimate user or different systems, they can send a data packet containing a bug to the target system in order to exploit a vulnerability.
    - Can be done using many techniques like command injection, buffer overflow, DoS, brute forcing credentials, social engineering, misconfigurations etc.

4. Maintaining Access

Items put in place to ensure future access.

- e.g: Rookit, Trojan, Backdoor can be used.

5. Covering Tracks

Steps taken to conceal success and intrusion; Not be noticed.

- e.g: Clear the logs; Obfuscate trojans or malicious backdoors programs.