أكاديمية الأمن السيبراني
Cyber Academy

www.CyberAcademy.ly

Linux+ Network+ Security+ CySA+ PenTest+ CASP+

Security+

اعداد وتقديم :

By: Eng Taher Boujrida
م. الطاهر أبوجريدة
Information Security Consultant
خبير أمن المعلومات
CTO@Openvision.ly
المدير الفني/ شركة الرؤية المفتوحة

PECB
Certified ISO/IEC 27001
Lead Implementer

C)ISSO mile2 Cyber Security Certifications
C)PTE mile2 Cyber Security Certifications
Astaro Security Gateway Certified Administrator (ACA)

OPEN VISION
الرؤية المفتوحة لتقنية وأمن المعلومات

www.openvision.ly

24/7/2023 طرابلس/ليبيا

أكاديمية الأمن السيبراني
Cyber Academy

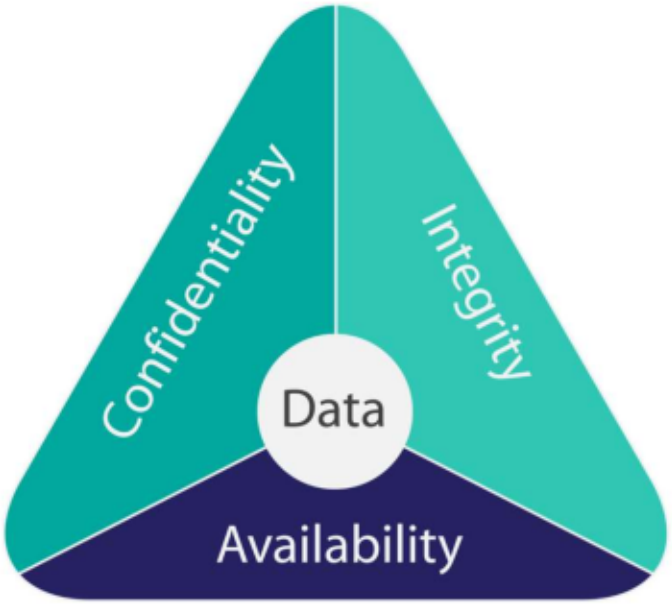
www.CyberAcademy.ly

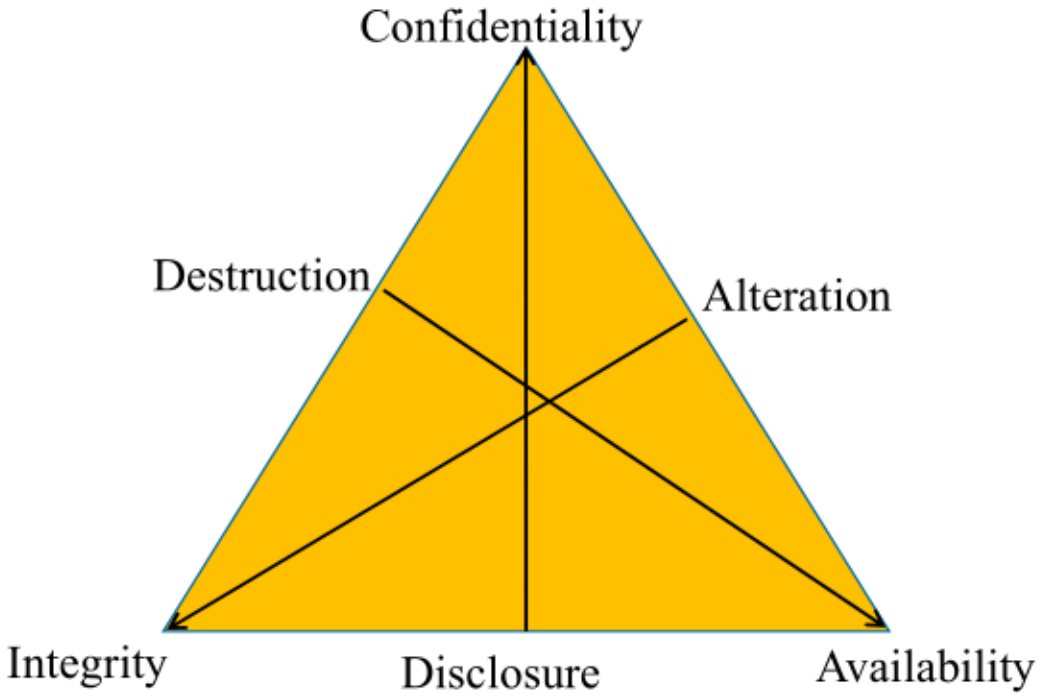
Security+ 601

Introduction, CIA, Threats, Threat Actors, Common Attacks of Malicious Software and Social engineering

Introduction المقدمة

CIA Triad / Disclosure / Alteration / Destruction





Risk, Vulnerability,Threat, Impact

- ***Risk*** **is the likelihood that a threat will exploit a vulnerability.**
- **A vulnerability is a weakness, and a threat is a potential danger.**
- **The result is a negative impact on the organization.**
- **Impact refers to the magnitude of harm that can be caused if a threat exercises a vulnerability**

Vulnerability الثغرة/نقطة الضعف

- A vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions) within a computer system.
- Vulnerabilities are classified according to the asset class they are related to:-
  - Hardware:- Susceptibility to humidity/dust ; Unprotected storage; Over-heating.
  - Software:- Insufficient testing; insecure coding; lack of audit trail; Design flaw.
  - Network:- Unprotected communication lines; Insecure network architecture.
  - Configuration network devices and servers
  - Personnel:- Inadequate recruiting process; Inadequate security awareness; insider threat
  - Physical site:- Area subject to natural disasters (e.g. flood, earthquake); interruption to power source
  - Organizational:- Lack of regular audits; lack of continuity plans;

Vulnerabilities الثغرات/نقاط الضعف

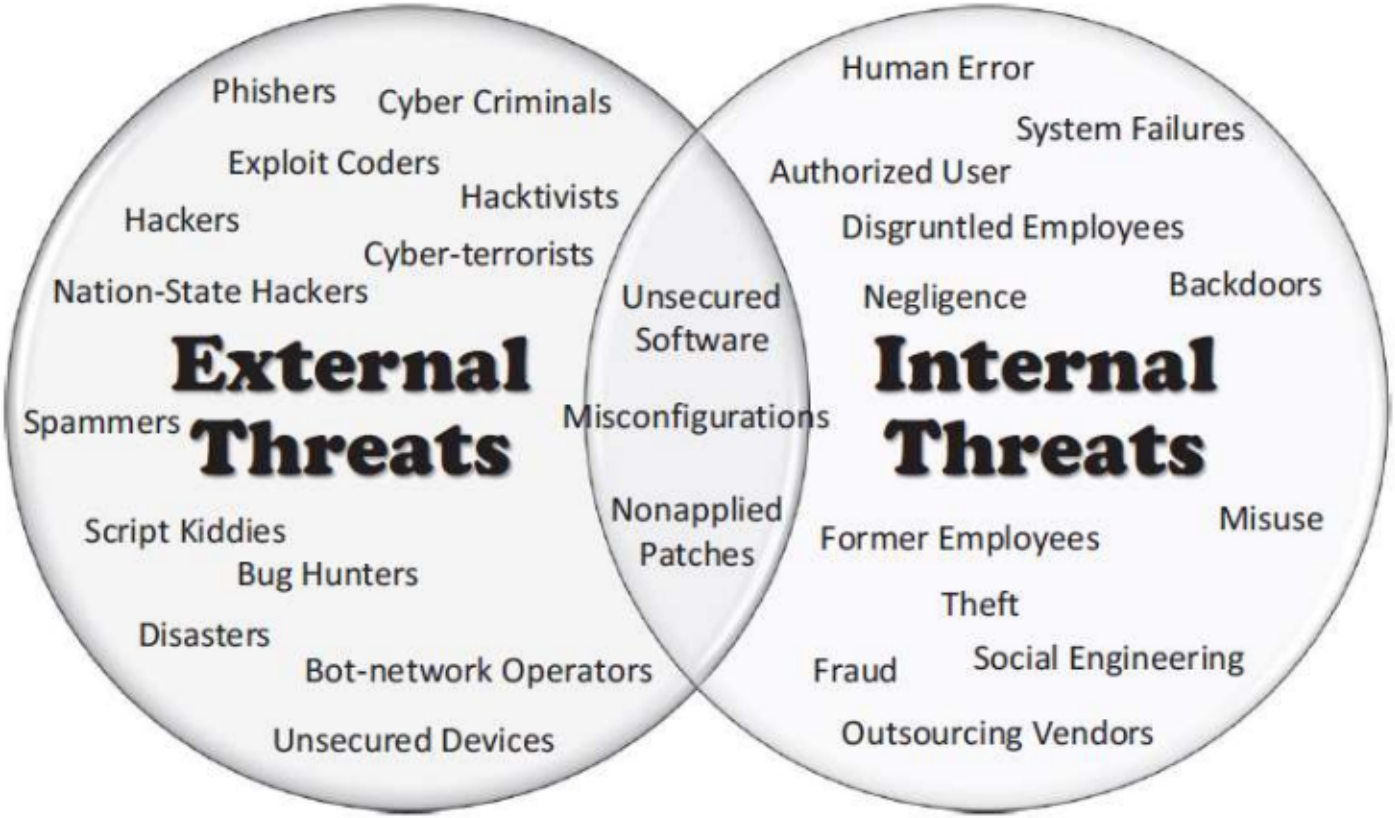
- A *vulnerability* is a flaw or weakness in software or hardware, or a weakness in a process that a threat could exploit, resulting in a security breach.
- Examples of vulnerabilities include:
  - • Lack of updates. If systems aren't kept up to date with patches, hotfixes, and service packs, they are vulnerable to bugs and flaws in the software.
  - • Default configurations. Hardening a system includes changing systems from their default hardware and software configurations, including changing default usernames and passwords. If systems aren't hardened, they are more susceptible to attacks.
  - Lack of malware protection or updated definitions. Antivirus and anti-spyware methods protect systems from malware, but if they aren't used and kept up to date, systems are vulnerable to malware attacks
  - • Lack of firewalls. If personal and network firewalls aren't enabled or configured properly, systems are more vulnerable to network and Internet-based attacks.
  - • Lack of organizational policies. If job separation, mandatory vacations, and job rotation policies aren't implemented, an organization may be more susceptible to fraud and collusion from employees.

Threat ما هو التهديد؟

- A threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.
- *Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.*
- A countermeasure is any step you take to ward off a threat to protect user, data, or computer from harm.
- Various Security threats:-
  - Users:- Identity Theft; Loss of Privacy; Exposure to Spam; Physical Injuries.
  - Hardware:- Power-related problems; theft; vandalism; and natural disasters.
  - Data:- Malwares; Hacking; Cybercrime; and Cyber-terrorism.

Threats التهديدات الداخلية والخارجية

Identify, Protect, Detect, Respond, Recover



Threat vector جبهات التهديدات

- Threat vectors are paths through which an attacker can exploit to penetrate a system component or bypass defenses to attack a target.
- Method used by an attacker to gain access to a victim's machine in order to infect it with malware

Threat Actors مصادر التهديدات

1) Script kiddie
2) Hacktivist
3) Insider
4) Competitors
5) Organized crime
6) Nation state entity (state - sponsored)
7) Corporate espionage groups

Threat Actors: Script kiddies

- A script kiddie is an attacker who uses existing computer scripts or code to launch attacks.
- Script kiddies typically have very little expertise or sophistication, and very little funding.
- Many people joke about the bored teenager as the script kiddie, attacking sites or organizations for the fun of it.
- However, there isn't any age limit for a script kiddie.
- More important, they can still get their hands on powerful scripts and launch dangerous attacks.
- Their motivations vary, but they are typically launching attacks out of boredom, or just to see what they can do.

Threat Actors: Hacktivist

- A hacktivist launches attacks as part of an activist movement or to further a cause. Hacktivists typically aren't launching these attacks for their own benefit, but instead to increase awareness about a cause.
- As an example, Deric Lostutter (known online as KYAnonymous) was upset about the rape of a Steubenville, Ohio, high school girl, and what he perceived as a lack of justice. He later admitted to participating in several efforts to raise awareness of the case, including targeting a web site ran by one of the high school's football players.
- Eventually, two high school football players were convicted of the rape. One was sentenced to a year in juvenile detention and served about 10 months. The other one was sentenced to two years and served about 20 months. Lostutter was ultimately sentenced to two years in federal prison.

Threat Actors: Insider

- An insider is anyone who has legitimate access to an organization's internal resources.
- Common security issues caused by insider threats include loss of confidentiality, integrity, and availability of the organization's assets.
- The extent of the threat depends on how much access the insider has. For example, an administrator would have access to many more IT systems than a regular user.
- Malicious insiders have a diverse set of motivations. For example,
  1) some malicious insiders are driven by greed and simply want to enhance their finances,
  2) while others want to exact revenge on the organization. They may steal files that include valuable data, install or run malicious scripts, or redirect funds to their personal accounts

Threat Actors: Competitors

- Competitors can also engage in attacks. Their motivation is typically to gain proprietary information about another company.
  - Although it's legal to gather information using open- source intelligence, greed sometimes causes competitors to cross the line into illegal activity.
- This can be as simple as rummaging through a competitor's trash bin, which is known as dumpster diving.
- In some cases, competitors hire employees from other companies and then get these new employees to provide proprietary information about their previous employer.

Threat Actors: Organized crime

- **Organized crime** is an enterprise that employs a group of individuals working together in criminal activities. This group is organized with a hierarchy with a leader and workers, like a normal business. Depending on how large the enterprise is, it can have several layers of management.
- **The primary motivation of criminals in organized crime is money.** Almost all their efforts can be traced back to greed with the goal of getting more money, regardless of how they get it.
- Unlike a legitimate business, these enterprises are focused on criminal activity.
- As an example, Symantec reported on Butterfly, a group of well organized and highly capable attackers who steal market-sensitive information on companies and sell that information to the highest bidder.
  - They have compromised some large U.S. companies, including Apple, Microsoft, and Facebook. Additionally, they have steadily increased their targets to include pharmaceutical and commodities-based organizations.

Threat Actors: APT

Nation state entity (state–sponsored)

- advanced persistent threat (*APT*) attackers are organized and sponsored by a nation-state or government.
- APT attacks are typically launched by a group that has both the capability and intent to launch sophisticated and targeted attacks.
- APT often have a significant amount of resources and funding.
- Individuals within an APT group typically have very specific targets, such as a specific company, organization, or government agency.
- Successful attacks from APT often allow unauthorized access for long periods of time, allowing attacks to exfiltrate a significant amount of data.
- As an example, Mandiant concluded that the group they named APT1
- operates as Unit 61398 of the People's Liberation Army (PLA) inside China. Mandiant estimates that APT1 includes over 1,000 servers and between dozens and hundreds of individual operators.

Threat Actors:

APT Nation state entity: APT1 in China

- **APT1 in China as advanced persistent threat (*APT*)**
  - **Released at least 40 different families of malware**
  - **Stolen hundreds of terabytes of data from at least 141 organizations**
  - **Maintained access to some victim networks for over four years before being detected**
  - **Established footholds within many networks after email recipients opened malicious files that installed backdoors, allowing attackers remote access**
  - **Chinese officials have denied these claims.**
- **Nation state entity: APT28 in Russia**
- **Fancy Bear (APT 28) and Cozy Bear (APT 29) (Russian)**
- **GRIZZLY STEPPE also indicates these two APTs compromised and exploited networks associated with the 2016 U.S. presidential election.**

Corporate espionage groups

- **"Corporate Espionage" - the theft of trade secrets for economic gain**
- **"Trade Secret" - property right which has value by providing an advantage in business over competitors who do not know the secret**
- **International Trade Commission estimates current annual losses to U.S. industries due to corporate espionage to be over $70 billion**

Who do it:

1. Employees
2. Professional industrial spies
3. Members of the Society for Competitive Intelligence Professionals
4. Business consultants

Symptoms of Infection

- Your computer might have been infected if it begins to act strangely

1) ▪ Hard drives, files, or applications are not accessible anymore
2) ▪ Strange noises occur
3) ▪ Unusual error messages
4) ▪ Display looks strange
5) ▪ Jumbled printouts
6) ▪ Double file extensions are being displayed, such as textfile.txt.exe
7) ▪ New files and folders have been created or files and folders are missing/corrupted
8) ▪ System Restore will not function

ACTIONS: TOP EIGHT CYBER SAFETY ACTIONS


Protect Passwords


Prevent Identity Theft


Beware of Phishing

Avoid Malware


Run Antivirus Software


Install Updates


Back Up Important Files


Turn On Firewalls

Consequences of attacks

Job Difficulties

- Loss of access to organization computing network
- Inability to access files and do work

Data Loss

- Loss of confidentiality and integrity
- Loss of valuable organization info or research
- Compromised personal data

Disciplinary Actions

- Lawsuits دعاوى قضائية
- Loss of public trust
- Loss of grant opportunities
- Prosecution الملاحقة القضائية
- Internal disciplinary action
- Termination of employment

أكاديمية الأمن السيبراني
Cyber Academy

www.CyberAcademy.ly

Linux+ Network+ Security+ CySA+ PenTest+ CASP+

THANK YOU Q&A شكرا

م. الطاهر أبوجريدة

Phone:

0923030202 0914316

Email:

info@cyberacademy.ly

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.
Maecenas porttitor congue massa