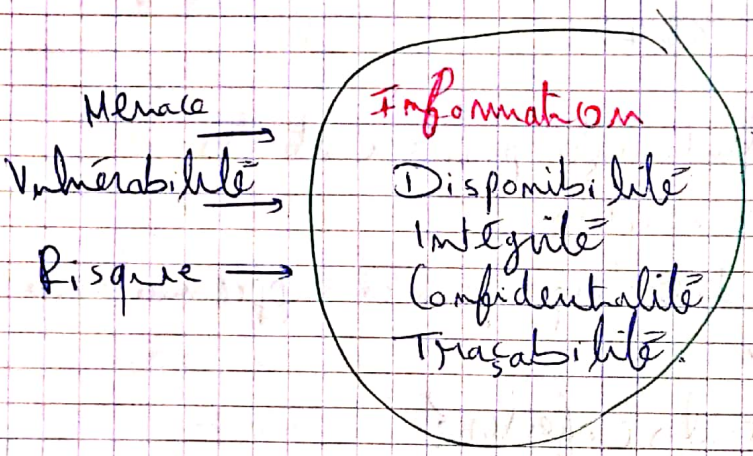
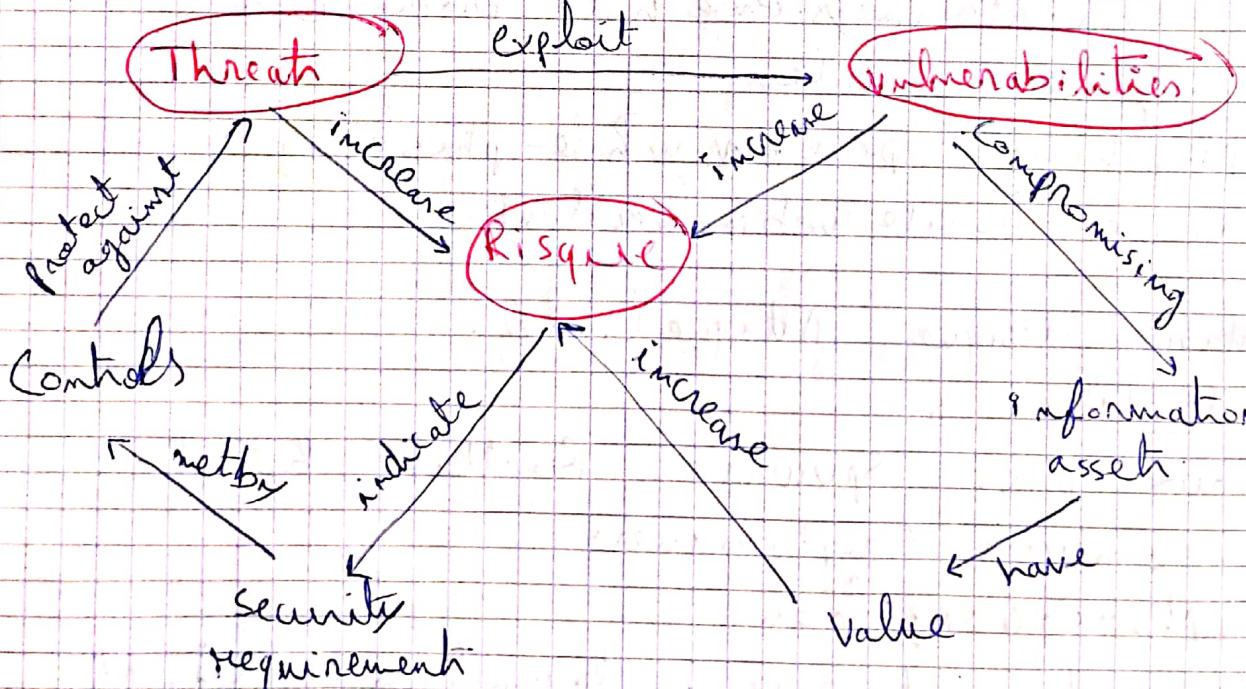
④ WISDOM : Knowledge of what is true and right
③ KNOWLEDGE : information analyzed.
② Information : Data elements with context.
① Data : individual element used to create information.

- Système d'information : un ensemble intégré de composants utilisés pour la collecte, le stockage et le traitement des données et pour la diffusion de l'information et des connaissances.





- If you know the enemy and know yourself, you need not fear the result of a hundred battles... if you know yourself but not the enemy, for every victory gained you

will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

the art of war - Sun Zhu

- Répartition régionale de la cybercriminalité

① North America ② Europe and Central Asia
③ East Asia & Pacific

- Top des pays et territoires où des objets malveillants ont été bloqués

① Algeria 69,4 % ② Bolivia 68,5 % ③ Vietnam 68,4 %

Malware : Un code malveillant conçu pour s'installer secrètement sur un système cible.
"Détruire des données, installer des programmes supplémentaires & filtrer des données"

Comment les systèmes sont-ils infectés ?
- Accès direct à un système hôte "Disque, USB ...
- ingénierie sociale.
- Phishing "spear ou whale-phishing
- Visite d'un site web malveillant.

- Attaque classique Attaque Ciblée.

Ex de Malwares
Virus . Vers . Spyware . Rootkit . Botnet
Ransomware Cryptominer

Symptômes d'infection
. Comportement bizzare sur la machine (old school)
. La souris qui bouge toute seule.
. ouverture de fenêtres en permanence.
. Ralentissement du système (cryptomineurs)

- Utilisation de beaucoup de ressources.
- Processeur qui chauffe en continu
- changement de mot de passe de vos comptes.
- transactions depuis votre compte bancaire.

• Vecteur d'attaque Distant Locaux Humains

① - Distant Drive by Download. click-jacking
- Phishing Email
- Pièces jointes aux courriels
- hyperliens intégrés
- Websites / Downloads
- Drive-by infections.
- Exploit Kits (EK) sont des outils utilisés par les criminels qui sont conçus pour identifier les vulnérabilités de votre machine et les exploiter.
- Common Exploit Kits "Angler, Nuclear, Rig, Magnitude".

② Locaux
- Accès Physique
- Supports amovibles infectés "USB"
- Partages réseaux Intranet "Man In The Middle"

③ Humains
- Phishing / Hameçonage - Réseaux sociaux

Les phases d'infections : La reconnaissance, Extension de périmètre, L'intrusion, La compromission

Les APT

APT : advanced Persistant Threat / Furtivité. Exfiltration de données, Malwares assez sophistiqués. Et des Hacktivistes.

Les APT : Reconnaissance → Distribution - Opération
Collecte de données → Exfiltration

- China APT 10 - Corea APT 38

APT Logbook

- Analyse Statique
  - Fingerprinting - Detection des packers - Extraction des string
  - Analyse Header PE - Désassemblage
  >> analyse fichier binaire : sur windows "virustotal. pestudio" et sur kali "malwin".
  pip3 install -r requirements.txt.
- L'analyse dynamique
  Sandbox

Les Ransomwares
- DDoS : Distributed Denial of Service Ransom.
- Data Breach Ransom.
- Denial of Service Ransom.

>> Les hôpitaux sont une cible de premier choix "La vie et la mort"

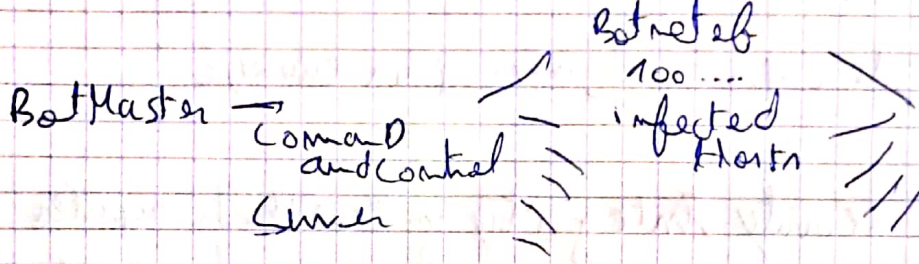
DoS
- Attaque par déni de service - Envoi grand nbr de requêtes
- Restreindre ou Réduire l'accès à une ressource

DDoS
Même concept que le DoS, use d'une multitude de systèmes
- Botnets — Zombies.

Catégories DoS / DDoS
- Abus de version - Volumétrie - Les protocoles.
- Couche applicative.

Bots: Programme automatisant des tâches sur le net.

Botnets: Large réseau de machines compromises à des fins malicieuses. entre autre des attaques DDoS



Quiz

1) Il s'agit de tout logiciel conçu pour endommager ou perturber un système: • (Malicious software) malware

2) - fait peur à l'user en lui faisant croire qu'il a beaucoup de virus. • Scareware

3) Crypte tous les fichiers sur l'appareil. L'attaquant exige de grosses sommes d'argent pour décrypter les fichiers:
• Ransomware

4) surveille secrètement les actions des users (par ex: les boutons enfoncés) - les informations sont envoyées à un pirate
• Spyware

5) Les users propagent ces fichiers en les copiant et activent les virus en ouvrant les fichiers infectés • virus.

6) - s'auto-répliquer, signifie se propager très rapidement
• worm

7) - Déguisé en logiciel légitime. Les users les installent sans se rendre compte qu'ils ont un but caché
• trojan

8) - Malware is another name for computer viruses.
Faux

9) Comment s'appelle le logiciel qui empêche le code malveillant d'entrer sur le réseau Firewall

10) WAN Wan Area Network

11) packet "décomposées données pour envoyé"

*) In computer security integrity means that computer system assets can be modified only by authorized parties.

*) In C.... Confidentiality means that the information in a computer system only be accessible for reading by authorized parities.

2) IPsec encypte use Both SHA and MD5

3) IPsec AH; ESP

*) . organizations is primarily concerned with military encryption systems. NSA