Type d'attaquants
- Script kiddy: Jouent avec des outils
- Pirates défi: Attirés par le defi
- Pirates vengeurs: Comme Sony (Par vengeance)
- Pirates par conviction: A but « politique »
- Pirates étatiques: Cyber-guerre / Cyber-espionnage

Motivations des attaquants
S'amuser, Curiosité, Prise de contrôle (ego), Acquérir des connaissances techniques, Idéologiques (politique), Ressources gratuites, Argent (escroqueries), Terrorisme, espionnage

Intentions des attaquants
- Constructives: Test pénétration (pentest)
- Neutres: zone grise
- Destructives: Pirate Malveillances

Principe CIA
Préservation de la confidentialité, intégrité et disponibilité de l'information.

Condifentialité (Confidentiality)
- s'assurer que l'information est accessible seulement à ceux qui sont autorisés à y avoir accès

Intégrité (Integrity)
- protéger l'exactitude et la complétude de l'information et des méthodes de traitement

Disponibilité (Availability)
s'assurer que les utilisateurs autorisés ont accès à l'information et aux ressources associées au moment et au lieu exigés

SSI (Sécurité du système d'information)

Cycle de vie
- une prévention (via une protection) contre les incidents de sécurité
- la détection (via une surveillance) de ces dernières
- la réaction (analyse, confinement)
- la récupération (reprise, sanctions éventuelles), puis analyse «post mortem» suite aux dommages survenus

5 couches de sécurité
Souvent décrite comme une sécurité sous forme d'onion car composé de plusieurs couche.
1. Physique :
   - sécurité physique
2. Réseau :
   - architecture et éléments réseau, adressage IP.
3. Protocoles :
   - Protocoles de communication, middleware.
4. Hosts :
   - systèmes d'exploitation et applications hosts.
5. Applications :
   - langages de programmation, applications spécifiques/dédiées, données spécifiques.

Contrôle d'accès (AAA)
- Authentication
  - S'assurer que la personne est bien celle qu'elle prétend être
  - Déterminer son identité et éventuellement sonrôle
- Authorization
  - Détermine en fonction de l'identité (ou rôle), que cela soit une personne ou système, si l'accès (ou le traitement) est autorisé
- Accounting/Auditing
  - S'assurer qu'il soit possible de suivre les accès/traitement qui ont été effectués
- Logging

5 principes fondamentaux
1. La sécurité globale est aussi forte que le maillon
le plus faible
2. La sécurité parfaite n'existe pas
3. La sécurité est un processus, pas un produit
4. La sécurité est inversement proportionnelle à la complexité
5. Participation des utilisateurs

Types de menaces
- Accidentelles: mauvaises manips, suppression
- Environnementales: naturelle ou industrielle
- Délibérées: origine criminelle

Vulnérabilités
- Matériel: disque saturés / morts
- Logiciel: oubli / incompétence (WEF)
- Réseau: trafic non protégé
- Personnel: manque de formation
- Site (physique): alim instable
- Organisation: enregistrement d'utilisateurs

Attack Kill Chain
Malicious and ethical hackers use the same steps
1. Reconnaissance
2. Exploit
3. Post Exploit

Etapes:
1. Collecte d'informations
2. Scanning
3. Enumérations
4. Intrusions
5. Escalade de privilèges
6. Pillage
7. Nettoyage des traces
8. Backdoors, rootkits

Cassage de mots de passe
Hachage: procédé cryptographique à sens unique
En ligne: requêtes vers site web, serveur,...
Hors ligne: tout en local

Etapes
1. Obtenir les empreintes (hash)
2. Attaque
   - Force brute: toutes les combinaisons
   - Dictionnaire: liste générique/ thématique
   - Heuristique: variations des éléments des dictionnaires
   - Pré-génération d'empreintes

Méthode Hellman
Hasher le MDP, réduire le hash, hasher la réduction, ...

Rainbow tables
Méthode de Hellman mais avec une réduction différente à chaque étape
La réduction donne une chaine de lettres (plaintext)
- Evite les collisions
- Réduit l'espace nécessaire
- Réduit le temps de calcul

Empreinte salées
Ajoute une string aléatoire au mot de passe avant de le hasher. (i.e. le même mot de passe produira des hashs différents)
- Impossible de calculer à l'avance les tables de "crackage"

Windows
Security Accounts Manager
`c:\Windows\system32\config\SAM`

Hashage
- Win 98/ME: LM (LAN Manager)
- Win NT/2k/XP/2003: NTLM et LM
- Win Vista/7/8/10/11: NTLM

LAN Manager Hash
Hash séparamment les deux parties du MDP, max 14 char (128b)

NT LAN Manager Hash
Hash tout d'un coup, max 256 char (128b)

Linux
`/etc/shadow`

Identifiants
- vide: DES, sans sel
- 1: MD5 (vieux linux & BSD)
- 2a/2b/2x/2y: Blowfish (OpenBSD)
- 5/6: SHA-256/SHA-512 (Linux/FreeBSD)
- y: yescrypt (Linux & glibc récente)

Comparaison des méthodes de cassage

Méthode	Temps préparation	Temps cassage	Taille mémoire	Probabilité succès	Sel
Dictionnaire	0	?	Faible	?	Idem
Heuristique	0	?	Faible	?	Idem
Force brute	0	O(N)	0	100%	Idem
Pré-calcultaion complète	O(N)	0	O(N)	100%	Plus Dur
Hellman	Long	Faible	Variable	50-95%	Plus Dur
Rainbow tables	Long	Faible	Variable	50-95%	Plus Dur

Authentification des emails
- SPF: vérifie que l'expéditeur est autorisé
- DKIM: vérifie signature authentique

Protection
- Utiliser TLS (Transport Layer Security protocol)
- Utiliser l'authentification
- Utiliser la messagerie sécurisée
  - chiffrement
  - signature électronique

Malware

Types
- Virus
  - Code executable
  - Se reproduit automatiquement
  - S'attache à d'autres programmes / fichiers
  - Besoin des utilisateurs pour se propager

- Ver
  - Code executable
  - Se reproduit automatiquement
  - Se propage via les réseaux
  - Autonome (pas besoin d'utilisateurs)
- Spyware, Canular, Adware
- Gov-ware, Cyber War

Antivirus

Protection sur 4 niveaux recommandé
- Tous les postes clients
- Serveurs de fichiers
- Serveurs de messagerie
- Proxies internet