Les techniques d'attaques

Les techniques d'attaques

❑Attaques de mot de passe

Une attaque de mot de passe ou le cassage de mot de passe est une stratégie d'attaque informatique ayant pour but de prendre connaissance des mots de passe des utilisateurs des outils informatiques (un serveur, un site internet ou d'une application..)

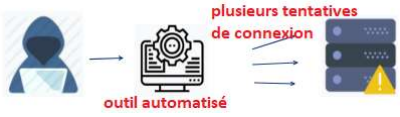
Il est possible de distinguer différentes attaques de mots de passe tels que:

✓**Attaque par force brute (brute force attack)**

C'est une stratégie d'attaque qui se base sur le test de chaque combinaison possible d'un mot de passe ou d'une clé pour un identifiant, afin de se connecter au service ciblé.

En fonction de la longueur et de la complexité du mot de passe, le craquage peut prendre entre quelques secondes et plusieurs années.

En réalité, que certains pirates ciblent les mêmes systèmes chaque jour pendant des mois et parfois même des années.



Les techniques d'attaques

les outils

La découverte du mot de passe peut durer longtemps. Par conséquent, les attaquants ont mis au point des outils pour faire le travail plus rapidement.

➢**Les dictionnaires** sont les outils les plus basiques. Certains pirates parcourent des dictionnaires en intégralité et complètent les mots avec des caractères spéciaux et des chiffres, ou utilisent des dictionnaires de mots spécifiques. Toutefois, ce type d'attaque séquentielle est fastidieux.

➢**Des outils automatisés comme :** Medusa, THC Hydra, Ncrack, John the Ripper et Aircrack-ng peuvent aider à trouver un mot de passe en quelques secondes

Remarque

Ces outils servent aux administrateurs système à éprouver la solidité des mots de passe de leurs utilisateurs mais leur usage est détourné par les attaquants pour s'introduire dans les systèmes informatiques

Les techniques d'attaques

Le processeur accélère l'attaque par force brute

Ajouter des processeurs graphiques accélère la puissance des machines, afin de permettre au système de gérer plusieurs tâches simultanément. En effet ajouter un seul processeur peut minimiser le temps nécessaire pour craquer un mot par 250 fois .

Exemple

le nombre de combinaisons possibles pour un mot de passe à six caractères comprenant des chiffres est d'environ 2 milliards. Le craquer à l'aide d'une unité centrale puissante qui essaie 30 mots de passe par seconde dure plus de deux ans. Ajouter un processeur puissant permet au même ordinateur de tester 7 100 mots de passe par seconde et de deviner le mot de passe en 3,5 jours.

https://www.kaspersky.fr/resource-center/definitions/brute-force-attack

Les techniques d'attaques

Mesures de protection

✓**Pour les informaticiens**

Pour qu'il soit plus compliqué de mener à bien des attaques par force brute, les administrateurs système doivent s'assurer que les mots de passe de leur système sont chiffrés en utilisant les taux de chiffrement les plus élevés possible, comme le chiffrement à 256 bits.

✓**Pour les utilisateurs**

les utilisateurs doivent choisir des mots de passe à 10 caractères contenant des symboles ou des chiffres. Ainsi, le nombre de possibilités s'élève à 171,3 trillions ($1{,}71 \times 10^{20}$). En utilisant un processeur graphique qui essaie 10,3 milliards de hachages par seconde, craquer le mot de passe prendrait normalement environ 526 ans, même si un superordinateur pourrait le craquer en quelques semaines.

Les techniques d'attaques

Attaque par dictionnaire

Une stratégie d'attaque qui consiste à essayer de trouver un mot de passe en essayant une liste de mots tirés d'un dictionnaire.

Elle est considérée comme plus efficace qu'une attaque par force brute, car certains utilisateurs utilisent des mots de fréquents du dictionnaire pour obtenir un mot de passe facile à retenir. Les noms d'animaux domestiques, les noms de parents, la couleur préférée ou les équipes de football sont parmi les options les plus couramment utilisées.

Quelle est la différence entre une attaque par force brute et par dictionnaire ?

✓Dans une attaque par dictionnaire, l'attaquant utilise une liste de mots dans l'espoir que le mot de passe de l'utilisateur soit un mot couramment utilisé ou un mot de passe vu sur des sites précédents. Les attaques par dictionnaire sont optimales pour les mots de passe basés sur un seul mot

✓Dans une attaque par force brute, l'attaquant peut utiliser un outil pour essayer toutes les combinaisons de lettres et de chiffres, en espérant finalement deviner le mot de passe.. Tout mot de passe, aussi fort soit-il, est vulnérable à cette attaque, mais cette méthode prendra un certain temps.

Les techniques d'attaques

Attaque par dictionnaire(suite)

Pour effectuer une attaque de mot de passe par dictionnaire, on peut encore compter sur un des nombreux outils fourni par Kali Linux tel que: **crunch**.


```
crunch <minLength> <maxLength> <Charset> <Options>
```

L'objectif est de demander au programme de composer des mots de passé d'une longueur minimum et de longueur maximum, utilisant un jeu de caractères passé en paramètre. Le résultat peut alors être redirigé vers un fichier en sortie :

```
crunch 8 10 ABCDEFGHIJKLMNabcdefghijklmn0123456789 –o /root/Desktop/Dictionary.txt
```

Les techniques d'attaques

L'utilisation du calcul distribué

Le calcul distribué consiste à répartir le traitement mathématique de données sur plusieurs ordinateurs. Jusqu'ici, cette manière d'utiliser les ordinateurs en réseau était réservée au monde scientifique qui a parfois besoin de capacités de calcul très importantes

les attaquants se sont approprié cette technologie car le décodage de mots de passe fait justement parti des opérations qui demandent un très grand nombre de calculs.

Les vitesses atteintes sont de l'ordre de 1 000 000 000 mots de passe traités par seconde pour un système distribué de moyenne ou de grande ampleur (c'est ce que l'on peut obtenir avec un supercalculateur d'une université par exemple).

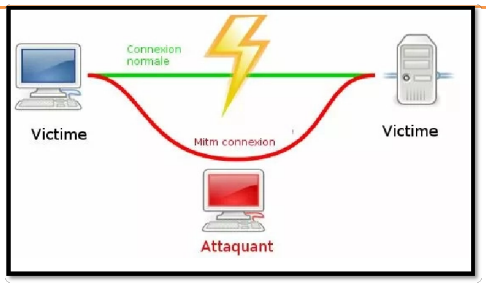
Les systèmes de cloud computing (ex : Amazon EC2) qui proposent des solutions de calculs distribués peuvent tout à fait servir de base pour ce genre d'opération

Les techniques d'attaques

Attaque de l'homme du milieu « man in the middle »

Principe

se placer entre deux acteurs, souvent un client et un serveur, en se faisant passer pour un des acteurs. L'intérêt est de lire les données échangées et éventuellement les modifier.



la plus courante implique qu'un attaquant utilise un routeur Wi-Fi afin d'intercepter les communications des utilisateurs. Ceci peut être effectué de différentes manières :

❖En installant un routeur malveillant qui apparaît être légitime

Exemple

L'attaquant peut configurer son ordinateur portable ou un autre appareil sans fil afin qu'il agisse comme une borne Wi-Fi et lui donner un nom souvent utilisé dans les lieux publics comme les aéroports ou les cafés.

Les techniques d'attaques

✓En exploitant un défaut dans l'installation d'un routeur légitime dans le but d'intercepter les sessions de l'utilisateurs sur le routeur.

Exemple

L'attaquant identifie une vulnérabilité dans la configuration ou dans le système de chiffrement d'un routeur **Wi-Fi** légitime afin de l'exploiter et d'espionner les communications entre les utilisateurs et le routeur.

Une méthode plus récente d'attaque HDM est connu sous le nom d'attaque « man-in-the-browser ». Dans ce scénario, l'attaquant utilise une des nombreuses méthodes pour introduire un code malveillant au sein du navigateur.

Ce malware enregistre en silence les données envoyées entre le navigateur et les différents sites ciblés que l'attaquant a codé en dur dans le malware.

Fameuses attaques de type HDM

✓Attaque par rejeu

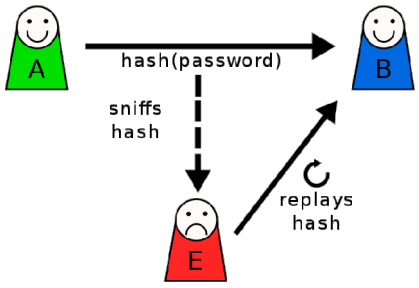
✓Détournement de flux

Les techniques d'attaques

Attaque par rejeu

Une **attaque par rejeu** (en anglais, *replay attack* ou *playback attack*) est une forme d'attaque réseau dans laquelle une transmission est malicieusement répétée par un attaquant qui a intercepté la transmission. Il s'agit d'un type **d'usurpation d'identité**.

Appelée également attaque par relecture, elle permet à une entité malveillante d'intercepter puis de rejouer une transmission de données valides sans avoir à la déchiffrer.



Les techniques d'attaques

Détournement de flux

des techniques permettant de rediriger le flux réseau vers un client, vers un serveur, ou vers une autre machine.

Exemple de méthodes :

- ✓ARP-Poisoning/ARP-spoofing
- ✓Détournement du session TCP/UDP Hijacking

Rappel :

les protocoles ARP (Address Resolution Protocol) permet de faire correspondre une adresse MAC à une adresse IP donnée et RARP (Reverse Address Resolution Protocol)permet l'inverse

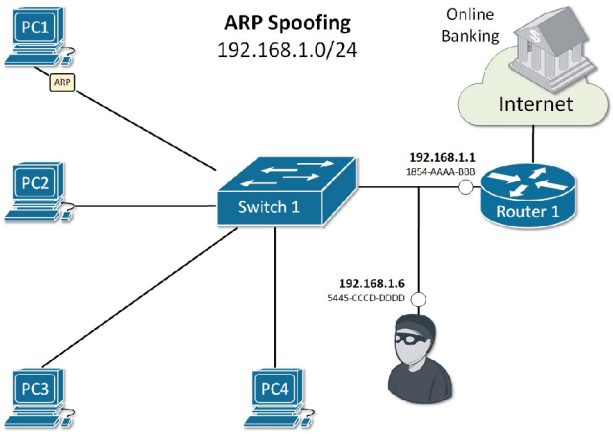
- ✓Le protocole ARP émet un datagramme particulier par diffusion à toutes les stations du réseau et qui contient entre autre l'adresse IP à convertir.
- ✓La station qui se reconnaît retourne un message (réponse ARP) à l'émetteur avec son adresse MAC.
- ✓L'émetteur dispose alors de l'adresse physique du destinataire et ainsi la couche liaison de données peut émettre les trames directement vers cette adresse physique.
- ✓Les adresses résolues sont placées dans un cache ce qui évite de déclencher plusieurs requêtes lorsque plusieurs datagramme doivent être envoyés.

Les techniques d'attaques

Détournement de flux (ARP-Poisoning/ARP-Spoofing)

Principe

Rediriger le trafic réseau d'une ou plusieurs machines vers la machine de l'attaquant, en corrompant le cache ARP



Les techniques d'attaques

Détournement de flux: TCP Hijacking

Principe:

L'attaquant va prendre le contrôle d'une session de communication TCP entre deux machines.

En effet, un attaquant peut avoir accès à une communication en interceptant la session TCP sans problème, dans la mesure où l'authentification se fait uniquement à l'ouverture de la session.

✓Cette attaque fonctionne en devinant les numéros de séquences

✓Les technique utilisée pour les détournements de session TCP (TCP Hijacking) :

❑**Attaque à l'aveugle** : consiste à envoyer des paquets à l'aveugle (blind attack), sans recevoir de réponse, en essayant de prédire les numéros de séquence.

❑**Ecoute passive** : permet une fois que le pirate intercepte l'entête TCP , il peut connaître le numéro de séquence attendu par le serveur, le nombre accusé de réception, les ports et les protocoles utilisés. Ainsi, le pirate peut forger le paquet et l'envoyer au serveur avant que le client.

Exemple d'attaque

- IP spoofing
- injection du code

Les techniques d'attaques

Détournement de flux: UDP Hijacking

✓UDP n'utilise pas les numéros de séquence des paquets pour la synchronisation : il est plus facile de détourner la session UDP que TCP.

User Datagram Protocol, abrégé en UDP, est un protocole permettant l'**envoi sans connexion de datagrammes** dans des réseaux basés sur le protocole IP.

✓L'attaquant peut simplement forger une réponse à une requête UDP d'un client UDP avant la réponse du serveur.

Les techniques d'attaques:Les failles web

UDP Flooding

✓L'attaquant envoie des paquets de données inutiles au système cible de façon très rapprochée. L'objectif est de saturer la cible jusqu'à ce qu'elle ne soit plus en mesure de répondre aux requêtes légitimes. Une fois cet état atteint, le service est alors interrompu.

Dans le cas d'une attaque UDP flood, les choses se passent de la façon suivante :

1. L'attaquant utilise une adresse IP d'expéditeur usurpée pour envoyer des paquets UDP à des ports aléatoires du système cible.
2. du côté du système cible, le processus suivant doit être répété pour chaque paquet entrant:
   - ✓Vérifier si une application écoute sur le port indiqué dans le paquet UDP ; comme le port est choisi au hasard, ce n'est généralement pas le cas.
   - ✓Envoyer un paquet ICMP « Destination Unreachable » à l'expéditeur présumé ; comme l'adresse IP a été usurpée, ces paquets sont généralement reçus par un tiers

Les techniques d'attaques:Les failles web

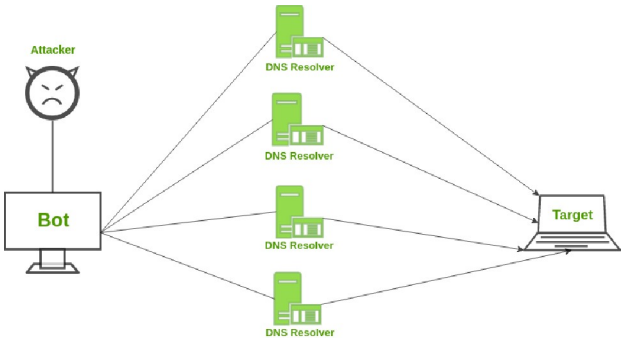
Déni de service (Dos)/ Deni de service distribué (DDos) SYN flooding / Inondation de SYN

Principe :

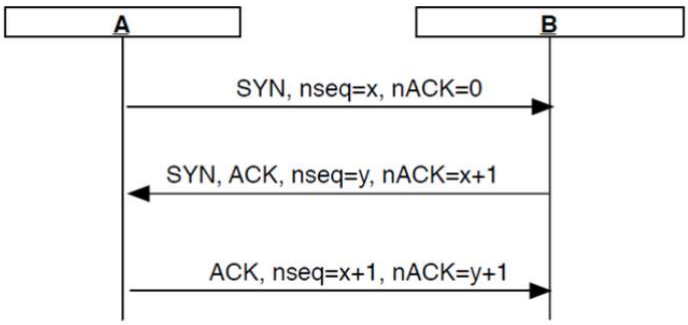
✓envoyer massivement des demandes de connexion (flag SYN à 1) vers la machine cible avec des adresses source aléatoire.

✓La machine cible renvoie les SYN-ACK en réponse à chaque SYN reçu Aucun ACK c'est renvoyé pour établir la connexion : ces connexions semi-ouvertes consomment des ressources mémoire

✓Au bout d'un moment, la machine cible est saturée et ne peut plus accepter de connexions



Les techniques d'attaques:Les failles web



✓Les numéros de séquence initiaux x et y sont choisis "aléatoirement".

✓Un timer est déclenché après l'envoi d'un SYN

✓ Si une réponse tarde trop à arriver (>75s), la connexion est abandonnée.

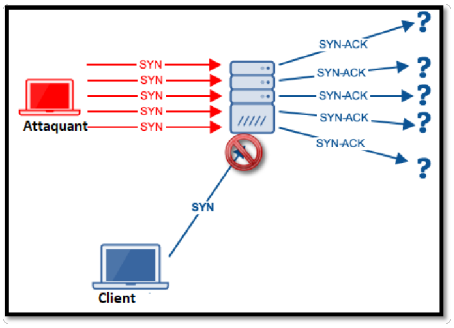
Les techniques d'attaques:Les failles web

Exemple de méthodes :

✓**SYN Flooding**

✓L'inondation TCP SYN (alias SYN flood) est un type d'attaque par déni de service distribué (DDoS) qui exploite une partie de la poignée de main tripartite TCP normale pour consommer les ressources du serveur ciblé et le rendre insensible.

✓Essentiellement, avec SYN flood DDoS, le délinquant envoie des demandes de connexion TCP plus rapidement que la machine ciblée ne peut les traiter, ce qui provoque une saturation du réseau.



Les techniques d'attaques:Les failles web

Déni de service (Dos)

Il existe plusieurs outils de Kali Linux qui peuvent être utilisés pour tester une attaque DoS (Denial of Service). Voici quelques exemples :

Hping : Cet outil de test réseau peut être utilisé pour générer des paquets de données malveillants pour saturer une cible avec un trafic réseau excessif, provoquant ainsi une interruption de service

LOIC (Low Orbit Ion Cannon) : C'est un outil de test de stress qui utilise l'attaque par déni de service distribué (DDoS) pour surcharger une cible avec un trafic réseau massif provenant de plusieurs ordinateurs

Slowloris : Cet outil crée une attaque DoS en envoyant de multiples requêtes HTTP incomplètes et en les maintenant ouvertes pour éviter que la cible puisse répondre aux autres demandes.

Les techniques d'attaques:Les failles web

Ping of death

Le ping of death (ping de la mort) est une attaque historique de réseau. Elle entraîne un **arrêt immédiat des systèmes vulnérables**. Heureusement, ce type d'attaque ne fonctionne plus sur la plupart des systèmes depuis 1998.

L'attaque ping of death, utilise le protocole ICMP (Internet Control Message Protocol). En principe, d'autres protocoles basés sur l'IP peuvent également être utilisés. Les **systèmes modernes sont sécurisés contre le ping of death**.

Fonctionnement du ping of death

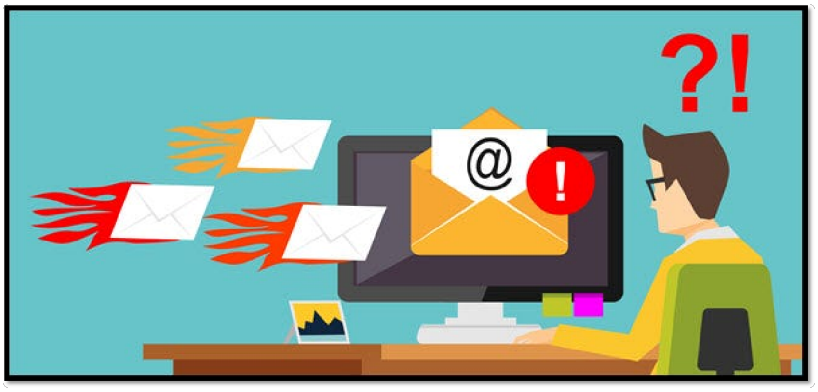
Pour effectuer une attaque par ping of death, l'attaquant crée un paquet I**CMP qui dépasse la taille autorisée**. Lors du transfert le paquet est divisé en plusieurs petits éléments. Lors du réassemblage dans le système cible, le dernier fragment fait dépasser la taille autorisée. Sur les systèmes non protégés, cela provoque un débordement de la mémoire tampon.

→ le système se bloque ou s'arrête complètement, ce qui entraîne un **effet de déni de service**.

Les techniques d'attaques:Les failles web

Bombe e-mail

Une bombe par e-mail est une forme d'abus d'Internet perpétrée par l'envoi d'énormes volumes d'e-mails à une adresse e-mail spécifique dans le but de déborder de la boîte aux lettres et de submerger le serveur de messagerie hébergeant l'adresse, ce qui en fait une forme de déni de service. attaque.



Les techniques d'attaques:Les failles web

Bombe e-mail

des outils utiles pour tester un système contre les attaques par e-mail sont :

MailSniper - un outil qui permet de tester les faiblesses de sécurité des serveurs de messagerie Exchange

Metasploit Framework - un outil complet de test de pénétration qui peut être utilisé pour tester les vulnérabilités des systèmes de messagerie

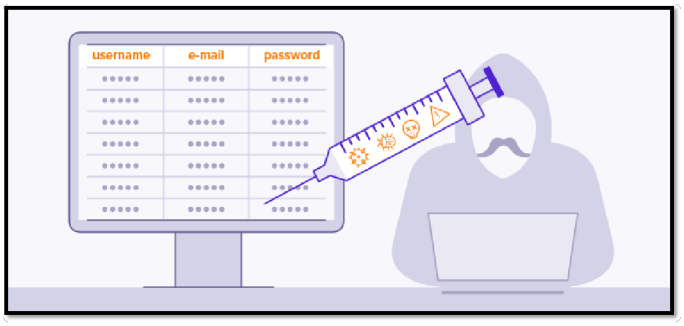
Social-Engineer Toolkit - un ensemble d'outils qui peut être utilisé pour tester les vulnérabilités de sécurité des utilisateurs en utilisant des techniques de manipulation sociale, y compris les attaques par e-mail.

Les techniques d'attaques:Les failles web

Attaques par injection

Une attaque par injection SQL permet à un pirate de voir des données dont il n'est pas au courant ou sur lesquelles il ne peut pas mettre la main. Les données sont sensibles car il peut s'agir de données appartenant à des utilisateurs ou de données auxquelles l'application peut accéder.

Généralement, le pirate supprimera les données de l'application Web ou les modifiera complètement pour causer des problèmes et modifier le comportement.



Les techniques d'attaques:Les failles web

Exemple

On considère le lien suivant:
https://universite.com/students?name=StudentX

SELECT * FROM students WHERE name = 'StudentX' AND released = 1

Cette requête SQL demande à la base de données de renvoyer :

✓tous les détails (*)de la table des étudiants où le nom est StuduentX .

released = 1 : est utilisée pour masquer les noms des étudiants qui ne sont pas demandés. (released = 0).

SELECT * FROM students WHERE name = 'StudentX'--' AND released = 1

L'élément clé ici est que la séquence à double tiret -- est un indicateur de commentaire en SQL, et signifie que le reste de la requête est interprété comme un commentaire. Cela supprime effectivement le reste de la requête, de sorte qu'elle n'inclut plus AND release = 1. Cela signifie que tous les noms sont affichés, y compris les noms inédits.

Les techniques d'attaques:Les failles web

En allant plus loin, un attaquant peut faire en sorte que l'application affiche tous les produits de n'importe quel nom, y compris des noms qu'il ne connaît pas.

https://universite.com/students?name=StudentX'+OR+1=1--

Cela se traduit par la requête SQL :

SELECT * FROM products WHERE name = 'StudentX' OR 1=1--' AND released = 1

La requête modifiée renverra tous les éléments dont 'name' est 'StudentX' ou 1 est égal à 1. Puisque 1=1 est toujours vrai, la requête renverra tous les éléments.

Les techniques d'attaques:Les failles web

des outils utiles pour tester un système contre les attaques par e-mail sont:

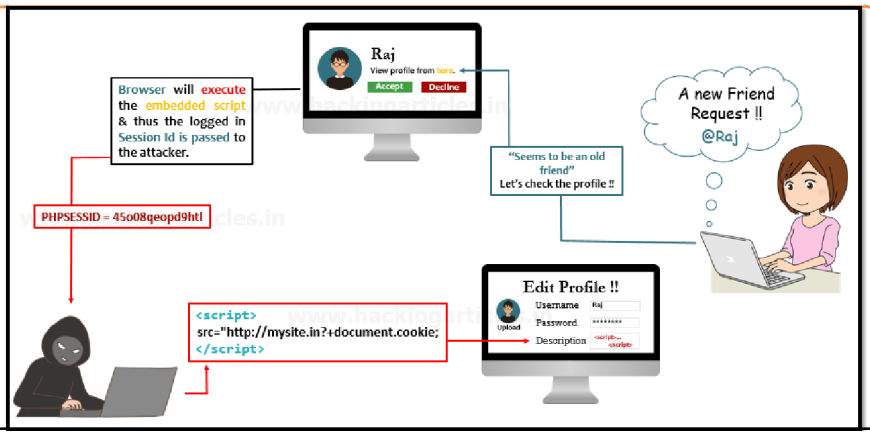
sqlmap est un outil open source qui permet de déterminer si vos serveurs de base de données peuvent être pénétrés par des attaques par injection SQL. Il recherche les vulnérabilités dans une suite complète de bases de données SQL et Nosql, notamment Oracle, MySql, SAP, Microsoft Access, IBM DB2, etc

Sqlninja Contrairement à sqlmap, qui cible toutes les bases de données SQL et NoSQL, sqlninja est utilisé pour pénétrer les applications basées sur Microsoft SQL Server. Le test de pénétration concerne principalement les systèmes Web

Les techniques d'attaques:Les failles web

Cross-site scripting (XSS)

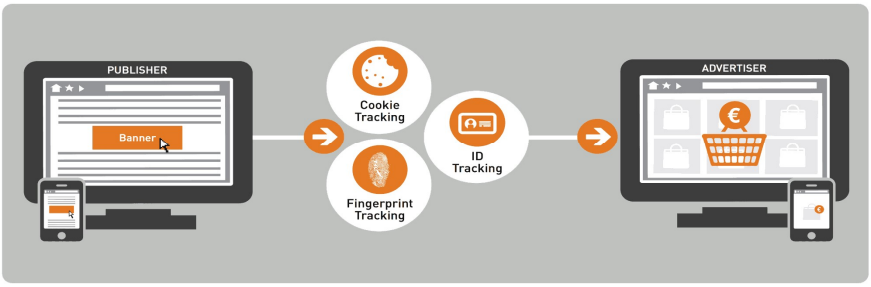
Le cross-site scripting (XSS) est une type de vulnérabilité de site web qui permet aux attaquants de placer des scripts malveillants dans des pages web par ailleurs dignes de confiance qui installent ensuite des logiciels malveillants dans les navigateurs web des utilisateurs. Avec le cross-site scripting, les attaquants ne ciblent ou ne redirigent pas les utilisateurs directement mais diffusent plutôt leurs logiciels malveillants à de nombreuses personnes.



Types de failles :Les failles web

Utilisation des cookies

Les cookies sont des petits fichiers que nous envoient les sites afin de mémoriser des informations sur notre profil, ou l'historique de notre navigation.



Les techniques d'attaques: Attaque par faille matérielle

- ✓**Attaque sur le matériel réseau**
- ✓**Attaques sur Périphérique et composant de l'ordinateur**
- ✓**Les attaques biométriques**

Les techniques d'attaques: Attaque par faille matérielle

Attaque sur le matériel réseau

Une attaque informatique sur le matériel réseau peut prendre différentes formes, mais cela implique généralement une intrusion malveillante visant à compromettre le matériel de réseau, tel que des routeurs, des commutateurs ou des pare-feu.

Exemples

✓Attaques par déni de service (DDoS) : ces attaques consistent à surcharger un équipement réseau en envoyant un grand nombre de demandes simultanées, ce qui rend le matériel indisponible pour les utilisateurs légitimes.

✓Exploitation de vulnérabilités : les attaquants peuvent exploiter des vulnérabilités connues ou inconnues dans le logiciel du matériel pour prendre le contrôle de celui-ci ou en extraire des informations sensibles.

Les techniques d'attaques: Attaque par faille matérielle

Attaques sur les périphériques et les composants de l'ordinateur

Les attaques sur les périphériques et les composants de l'ordinateur sont une forme de cyber-attaque qui cible spécifiquement les composants matériels d'un système informatique plutôt que le logiciel.

Exemples

✓Attaques par enregistreur de frappe (keylogger) : ces attaques sont conçues pour intercepter les frappes au clavier, souvent en se connectant à un périphérique de saisie de données tel qu'un clavier ou une souris.

✓Attaques par canal latéral (side-channel) : ces attaques exploitent des informations fuitées par un périphérique ou un composant lorsqu'il effectue une opération, comme la consommation d'énergie ou le temps de réponse, pour déduire des informations confidentielles

✓Attaques par attaque physique : ces attaques impliquent l'accès physique à un périphérique ou à un composant, tel que l'installation d'un dispositif d'enregistrement caché ou la modification de circuits électroniques pour effectuer des tâches malveillantes.

Les techniques d'attaques: Attaque par faille matérielle

Les attaques biométriques

Les attaques biométriques sont des attaques qui visent à exploiter les failles des systèmes de sécurité basés sur la biométrie. La biométrie est une méthode d'identification qui se base sur des caractéristiques physiques ou comportementales uniques de chaque individu, telles que les empreintes digitales, la reconnaissance faciale, la reconnaissance de la voix, la reconnaissance de l'iris, etc.

Exemples

- ✓Attaques par force brute : Les attaquants peuvent tenter de contourner les systèmes biométriques en utilisant des techniques de force brute pour trouver une correspondance entre les données biométriques stockées et les données de test. Les attaquants peuvent également utiliser des techniques d'usurpation d'identité en imitant les caractéristiques biométriques d'une autre personne.
- ✓Attaques de falsification : Les attaquants peuvent également utiliser des techniques de falsification pour tromper les systèmes biométriques, par exemple en utilisant des images ou des enregistrements audio ou vidéo truqués pour duper les capteurs biométriques
- ✓Attaques de reconnaissance de modèle : Les attaquants peuvent tenter d'analyser le modèle de reconnaissance biométrique utilisé par le système de sécurité pour trouver des failles et des vulnérabilités.

Les techniques d'attaques: Attaque par ingénierie sociale

Définition: Une attaque par ingénierie sociale est une technique utilisée par des pirates informatiques pour manipuler et tromper des personnes afin d'obtenir des informations confidentielles ou d'accéder à des systèmes informatiques. L'objectif est de convaincre la victime de divulguer des informations telles que des identifiants de connexion, des mots de passe ou des numéros de carte de crédit, ou de réaliser une action qui permettrait à l'attaquant d'accéder à des informations ou des systèmes

Les attaques par ingénierie sociale peuvent prendre de nombreuses formes tels que:

- ✓e-mails de phishing
- ✓des appels téléphoniques frauduleux
- ✓des messages textes malveillants,
- ✓des messages sur les réseaux sociaux
- ✓des manipulations en personne