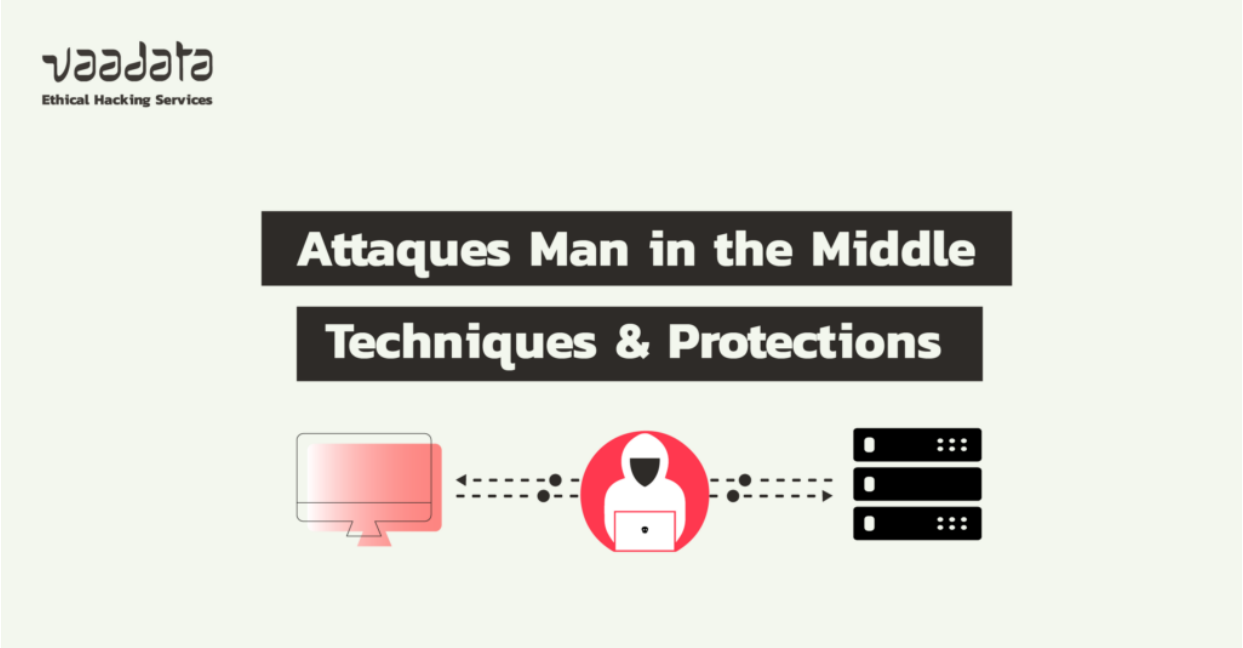
Attaques Man in the Middle (MitM) : Types et Protections

5 NOVEMBRE 2024



Les attaques Man in the Middle (MitM) exploitent des failles de configuration réseau et l'absence de mécanismes de sécurité robustes pour garantir l'intégrité et la confidentialité des données échangées.

Ces attaques consistent à intercepter et manipuler les communications entre deux parties, généralement un client et un serveur, sans que ces dernières en aient connaissance.

Dans cet article, nous examinerons en détail le principe des attaques MitM et les différentes techniques. Nous passerons également en revue les mesures de sécurité et protections à implémenter pour contrer ces attaques.

Guide complet sur les attaques Man in the Middle (MitM)

Qu’est-ce qu’une attaque Man in the Middle (MitM) ?

Une attaque Man in the Middle (MitM) survient lorsqu’un attaquant s’introduit dans une communication entre deux parties sans que celles-ci en soient conscientes.
Ainsi, une fois positionné en Man in the Middle, généralement entre un client et un serveur, l’attaquant peut :

- **Intercepter les données en transit** : Il devient un point de passage pour toutes les données échangées ; et peut potentiellement intercepter des informations sensibles, telles que des identifiants de connexion, des communications privées, des fichiers, etc.
- **Modifier les données en transit** : Il peut altérer les messages échangés et manipuler le contenu de la communication ; ce qui ouvre la porte à de nombreuses exploitations malveillantes.
- **Injecter du code malveillant** : Depuis sa position, l’attaquant peut insérer du contenu malveillant dans le flux de données. Par exemple, il pourrait injecter des malwares, des scripts ou des pages web falsifiées dans la communication. Cette technique peut être employée dans des contextes variés, comme des attaques de phishing notamment.

Quels sont les principaux types d’attaques Man in the Middle et comment se protéger ?

Il existe plusieurs techniques pour réaliser des attaques MitM. Dans cette section, nous verrons les principaux types d’attaques ainsi que les bonnes pratiques sécurité associées.

ARP Poisoning (Empoisonnement ARP)

L'ARP Poisoning, aussi appelé ARP Spoofing, est une méthode couramment utilisée dans les attaques MitM pour intercepter les communications sur les réseaux locaux (LAN).

Cette technique exploite le fonctionnement du protocole ARP (Address Resolution Protocol).

Rôle et fonctionnement du protocole ARP

Le protocole ARP est essentiel dans les réseaux locaux, car il permet de résoudre les adresses IP en adresses MAC (Media Access Control), indispensables pour que les paquets de données puissent être acheminés correctement.

Le rôle de l'ARP est d'associer dynamiquement une adresse IP (niveau réseau) à une adresse MAC (niveau matériel) afin que les machines puissent communiquer directement entre elles sur le réseau.

Voici le processus de base du protocole ARP :

- Lorsqu'une machine souhaite envoyer des données à une adresse IP spécifique, elle diffuse une demande ARP pour trouver l'adresse MAC correspondant à cette adresse IP.
- La machine détenant cette adresse IP répond avec son adresse MAC.
- Les deux périphériques conservent ces informations dans une table ARP, ou cache ARP, pour ne pas devoir répéter la demande à chaque transmission de données.

En quoi consiste l'ARP Poisoning ?

L'ARP Poisoning consiste à exploiter ce processus pour induire en erreur les dispositifs réseau.

Dans une attaque d'ARP Spoofing, l'attaquant envoie de fausses réponses ARP aux machines sur le réseau, liant son adresse MAC à l'adresse IP d'un autre dispositif (généralement un routeur ou une passerelle).

Cela conduit les autres machines à rediriger leur trafic vers l'attaquant, croyant qu'il est le destinataire légitime.

En effet, l'ARP Poisoning exploite la principale vulnérabilité du protocole ARP à savoir sa caractéristique « stateless » (sans état), qui fait que toutes les machines connectées au réseau recevront une réponse ARP même s'ils n'ont pas envoyé de requête. Cela signifie qu'ils mettront à jour leurs caches ARP chaque fois qu'il y aura une réponse ARP.

Le fonctionnement, étape par étape, est le suivant :

- L'attaquant commence par envoyer des paquets ARP falsifiés sur le réseau local. Ces paquets contiennent de fausses informations, indiquant que son adresse MAC correspond à l'adresse IP d'un autre périphérique sur le réseau.
- Ces informations sont ensuite mises en cache par d'autres périphériques du réseau.
- Une fois que les informations ARP falsifiées sont en cache sur d'autres périphériques, le trafic destiné à l'adresse IP légitime est redirigé vers l'adresse MAC de l'attaquant. Cela permet à l'attaquant d'intercepter, d'altérer ou de simplement observer le trafic entre les deux parties légitimes sans leur consentement.
- L'attaquant peut alors agir en tant qu'intermédiaire entre les deux parties, facilitant la capture de données sensibles, l'injection de paquets malveillants ou d'autres attaques.

Les conséquences de l'ARP Poisoning peuvent être graves, car elle compromet l'intégrité et la confidentialité des communications sur le réseau. Les attaques de ce type peuvent être utilisées pour voler des informations sensibles telles que des identifiants de connexion, des données financières, ou même pour mener d'autres attaques plus avancées.

Comment prévenir l'ARP Poisoning ?

Il existe plusieurs mesures pour se protéger ou limiter l'impact de l'ARP Poisoning :

- Utiliser des tables ARP statiques pour configurer manuellement les adresses IP et MAC, notamment pour les dispositifs critiques, comme les routeurs et les serveurs. Cela rend plus difficile l'injection de fausses réponses ARP.

- Implémenter des systèmes d'intrusion (IDS) pour surveiller les requêtes ARP anormales ou les modifications suspectes du cache ARP et alerter les administrateurs réseau en cas d'activité suspecte.
- Chiffrer les données pour protéger le contenu des communications contre la lecture par un attaquant, même si celui-ci intercepte les données.
- Segmenter le réseau en VLANs (Virtual Local Area Networks) pour réduire la portée des attaques ARP Spoofing.

DNS Spoofing (Empoisonnement DNS)

Le DNS Spoofing est une technique permettant à un attaquant de rediriger le trafic réseau vers des sites malveillants en compromettant le système de résolution de noms de domaine (DNS).

Cette méthode est largement utilisée dans les attaques Man in the Middle pour intercepter les communications entre un utilisateur et un site légitime.

Comment fonctionne le protocole DNS ?

Le protocole DNS (Domain Name System) est essentiel pour la navigation sur Internet.

Il agit comme un annuaire qui associe des noms de domaine à des adresses IP, nécessaires pour que les dispositifs puissent se connecter aux serveurs hébergeant les sites web.

Le DNS fonctionne de la manière suivante :

- Lorsqu'un utilisateur tente d'accéder à un site, sa machine envoie une requête DNS pour obtenir l'adresse IP du domaine.
- La requête est acheminée vers un serveur DNS, qui résout le nom de domaine en adresse IP et la renvoie au dispositif de l'utilisateur.
- Cette réponse DNS est ensuite stockée temporairement dans un cache DNS sur le dispositif pour accélérer les accès futurs au même site.

Principes du DNS Spoofing

Le DNS Spoofing vise à insérer de fausses informations dans le cache DNS des serveurs pour rediriger les utilisateurs vers des sites frauduleux.

Pour ce faire, un attaquant modifie l'adresse IP associée à un nom de domaine dans le cache DNS d'un serveur. Les utilisateurs qui accèdent ensuite à ce domaine sont redirigés vers un site contrôlé par l'attaquant, bien que l'URL saisie dans le navigateur semble être correcte.

Un exemple typique de DNS Spoofing se produit lorsqu'un attaquant associe l'adresse IP d'un site légitime à l'adresse IP d'un faux site.

Les utilisateurs pensent alors se connecter au site officiel, mais en réalité, ils transmettent leurs identifiants et autres informations sensibles à l'attaquant.

Prévenir le DNS Spoofing

Plusieurs mesures peuvent être adoptées pour prévenir les attaques de DNS Spoofing :

- Implémenter DNSSEC (Domain Name System Security Extensions) pour ajouter des signatures cryptographiques aux réponses DNS, afin de garantir leur authenticité. Cela permet aux serveurs DNS de vérifier que les réponses DNS n'ont pas été modifiées et de rejeter celles qui semblent corrompues ou malveillantes.
- Mettre en place des outils de détection et d'analyse réseau pour surveiller les activités DNS suspectes et alerter les administrateurs en cas de tentatives d'empoisonnement.

DHCP Spoofing (Empoisonnement DHCP)

Le DHCP Spoofing est une technique d'attaque permettant à un attaquant de se placer dans une position privilégiée au sein d'un réseau local en détournant le processus de distribution des adresses IP.

Quel est le rôle et le fonctionnement du protocole DHCP ?

Le protocole DHCP (Dynamic Host Configuration Protocol) est utilisé pour attribuer automatiquement des adresses IP et d'autres paramètres réseau aux périphériques connectés à un réseau.

Cela simplifie grandement la gestion des adresses IP, car les périphériques n'ont pas besoin d'une configuration manuelle pour accéder au réseau.

Le fonctionnement de base du DHCP est le suivant :

- Lorsqu'un dispositif se connecte au réseau, il envoie une demande DHCP pour obtenir une adresse IP.
- Un serveur DHCP légitime répond avec une adresse IP disponible et d'autres configurations nécessaires pour la connexion.
- Le dispositif accepte l'offre du serveur DHCP, ce qui lui permet de se connecter au réseau en utilisant les paramètres fournis.

En quoi consiste le DHCP Spoofing ?

Dans une attaque de DHCP Spoofing, un attaquant configure un dispositif malveillant pour se faire passer pour un serveur DHCP légitime.

Lorsque des dispositifs sur le réseau envoient des demandes DHCP, l'attaquant répond rapidement en fournissant des informations configurées pour intercepter le trafic.

Ainsi, il peut grâce au DHCP Spoofing :

- **Détourner la passerelle par défaut** : En indiquant son propre dispositif comme passerelle par défaut, l'attaquant redirige tout le trafic du réseau à travers lui, interceptant ainsi toutes les communications.
- **Modifier les serveurs DNS** : En remplaçant l'adresse IP des serveurs DNS légitimes par une adresse de son choix, l'attaquant peut rediriger les utilisateurs vers des sites malveillants en exécutant une attaque de DNS Spoofing en parallèle.
- **Contrôler la configuration IP des dispositifs** : En fournissant des adresses IP et des configurations de masque de sous-réseau incorrectes, l'attaquant peut également désactiver la connectivité réseau, créant ainsi une perturbation temporaire.

Se prémunir du DHCP Spoofing

Plusieurs mesures peuvent être prises pour prévenir les attaques de DHCP Spoofing :

- **Activer les protections de port DHCP sur les switches (DHCP Snooping)** : Les équipements réseau, comme les switches gérés, disposent souvent de fonctionnalités de sécurité, telles que le DHCP Snooping. Cette fonctionnalité limite les réponses DHCP aux seuls ports autorisés (généralement ceux connectés au serveur DHCP légitime) et bloque les réponses provenant de dispositifs non approuvés.
- **Segmenter le réseau avec VLANs (Virtual Local Area Networks)** : En utilisant des VLANs, les administrateurs peuvent isoler les dispositifs en fonction de leur rôle ou de leur niveau de sécurité, limitant ainsi la portée de l'attaque. L'attaquant se retrouve confiné dans son VLAN sans pouvoir influencer les autres segments du réseau.
- **Superviser les activités DHCP** : Des systèmes de surveillance réseau peuvent détecter les activités suspectes, comme la présence de multiples réponses DHCP provenant de différents dispositifs. Une détection rapide permet aux administrateurs de prendre des mesures avant qu'une attaque n'aboutisse.
- **Configurer les règles de pare-feu et les ACLs (Access Control Lists)** : Des règles de pare-feu et des ACLs peuvent être configurées pour limiter les réponses DHCP provenant de sources non autorisées. En contrôlant quels dispositifs peuvent répondre aux requêtes DHCP, le risque d'attaque est réduit.

Chiffrer les communications avec TLS pour prévenir les attaques Man in the Middle

Le chiffrement des communications est l'une des mesures les plus efficaces pour protéger les échanges de données contre les attaques Man in the Middle (MitM).

Le protocole TLS (Transport Layer Security) est aujourd'hui la norme pour assurer la confidentialité, l'intégrité et l'authenticité des communications.

En effet, TLS crée un canal sécurisé entre un client et un serveur, protégeant les informations contre l'interception et la manipulation. Ce chiffrement repose sur l'utilisation de certificats numériques qui authentifient le serveur et garantissent l'identité de la source des données.

Par ailleurs, bien que TLS renforce considérablement la sécurité, certaines configurations sont essentielles pour maximiser sa fiabilité :

- Les certificats TLS doivent être émis par des autorités de certification (CA) reconnues et renouvelés régulièrement. Les certificats expirés ou autosignés peuvent exposer à des risques de sécurité.
- Activer HTTP Strict Transport Security (HSTS) pour obliger les navigateurs à utiliser uniquement des connexions sécurisées avec le serveur.

Réaliser un test d'intrusion interne pour évaluer les risques d'attaques Man in the Middle

Un test d'intrusion interne est une évaluation de sécurité visant à identifier et corriger les failles présentes dans un réseau.
Dans le contexte des attaques Man in the Middle, un test d'intrusion interne permet de simuler des tentatives d'interception de communications sensibles en utilisant les attaques que nous avons détaillées.

Auteur : Amin TRAORÉ – CMO – @Vaadata