Usurpation d’adresse IP

1. **Objectifs**

- Connaitre les techniques d'usurpation d’adresse IP
- Être capable de se protéger de l'usurpation d'adresse IP

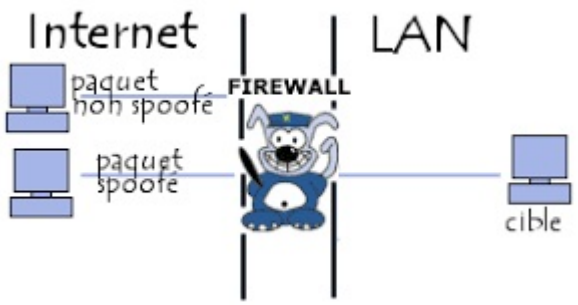
- **Présentation**



- L'usurpation d'adresse IP (en anglais : IP spoofing ou IP address spoofing) est une technique de piratage informatique utilisée en informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet.
- Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès.
- L’usurpation d’adresse IP (également appelé mystification ou spoofing IP) est une technique consistant à remplacer l’adresse IP de l’expéditeur d’un paquet IP par l’adresse IP d’une autre machine.
- L'usurpation d’adresse IP est la création de paquets IP (Internet Protocol) contenant une adresse source modifiée afin de cacher l'identité de l'expéditeur ou pour se faire passer pour un autre système informatique, ou les deux. C'est une technique souvent utilisée par les acteurs malveillants pour réaliser des attaques DDoS contre un appareil ciblé ou

l’infrastructure environnante.

La technique de l'usurpation d'adresse IP



- Cette technique permet ainsi à un pirate d’envoyer des paquets anonymement.
- Il ne s’agit pas pour autant d’un changement d’adresse IP, mais d’une mascarade de l’adresse IP au niveau des paquets émis.
- La technique de l’usurpation d’adresse IP peut permettre à un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage de paquets (pare-feu).
- En effet, un système pare-feu (firewall) fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines internes au réseau.
- Ainsi, un paquet spoofé avec l’adresse IP d’une machine interne semblera provenir du réseau interne et sera relayé à la machine cible, tandis qu’un paquet contenant une adresse IP externe sera automatiquement rejeté par le pare-feu.
- Cependant, le protocole TCP (protocole assurant principalement le transport fiable de données sur Internet) repose sur des liens d’authentification et d’approbation entre les machines d’un réseau, ce qui signifie que pour accepter le paquet, le destinataire doit auparavant accuser réception auprès de l’émetteur, ce dernier devant à nouveau accuser réception de l’accusé de réception.

Comment fonctionne l'usurpation d’identité ?

- Le spoofing peut s’appliquer à différents modes de communication et fait appel à divers niveaux de savoir-faire technique. Il peut être utilisé pour réaliser des attaques de phishing, une escroquerie visant à obtenir les informations confidentielles des particuliers et des entreprises.

apcpedagogie.com

- **Usurpation du numéro de téléphone**
    - Le spoofing téléphonique consiste à usurper l'identité de l'appelant. Cela donne l'impression au destinataire que les appels proviennent d'un numéro connu et/ou de confiance ou encore d'un numéro qui indique un emplacement géographique spécifique.
    - Les pirates peuvent alors utiliser le social engineering – souvent en se faisant passer pour l'employé d'une banque ou d'un service clientèle – pour convaincre leurs cibles de fournir, par téléphone, des informations sensibles telles que des mots de passe, des informations de compte, des numéros de sécurité sociale, etc.

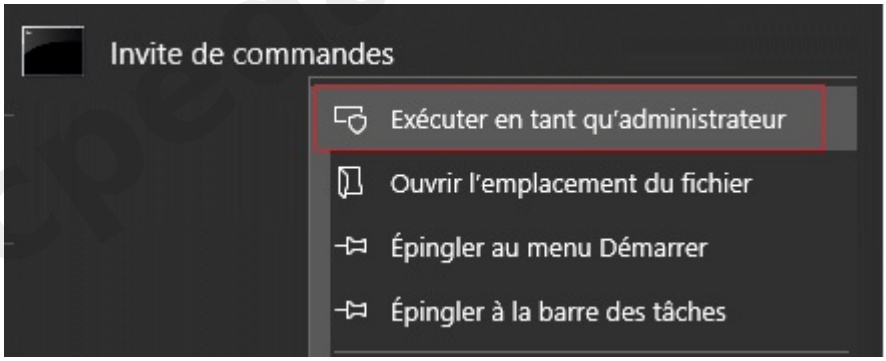
- **Usurpation de site Web**
    - L'usurpation (spoofing) de site Web se produit lorsqu'un escroc essaie de faire en sorte qu'un site Web dangereux ressemble à un site Web sûr, en utilisant des polices, des couleurs et des logos légitimes et réalistes.
    - Le spoofing de site web fait référence au cas où un site web est conçu pour imiter un site existant connu et/ou auquel l'utilisateur fait confiance. Les pirates utilisent ces sites pour obtenir des informations de connexion et d'autres informations personnelles des utilisateurs.
    - Cela se fait en répliquant un site de confiance avec l'intention de diriger les utilisateurs vers un site de phishing ou malveillant.
    - Ces sites copiés auront généralement une adresse de site Web similaire à celle du site d'origine et semblent être réels à première vue. Cependant, ils sont généralement créés pour obtenir les informations personnelles du visiteur.

- **Usurpation d'adresse IP**
    - Les attaquants peuvent utiliser l'usurpation d'adresse IP (protocole Internet) pour dissimuler l'adresse IP d'un ordinateur. Ils peuvent ainsi cacher l'identité de l'expéditeur ou se faire passer pour un autre système informatique. Un des buts de ce type de spoofing est d'accéder à un réseau qui authentifie les utilisateurs sur la base des adresses IP.
    - Le plus souvent, cependant, les pirates utilisent l'adresse IP d'une cible dans une attaque par déni de service pour submerger la victime de trafic entrant. L'attaquant envoie des paquets à plusieurs destinataires du réseau. Lorsque ceux-ci transmettent une réponse, ils sont acheminés vers l'adresse IP frauduleuse de l'expéditeur cible.

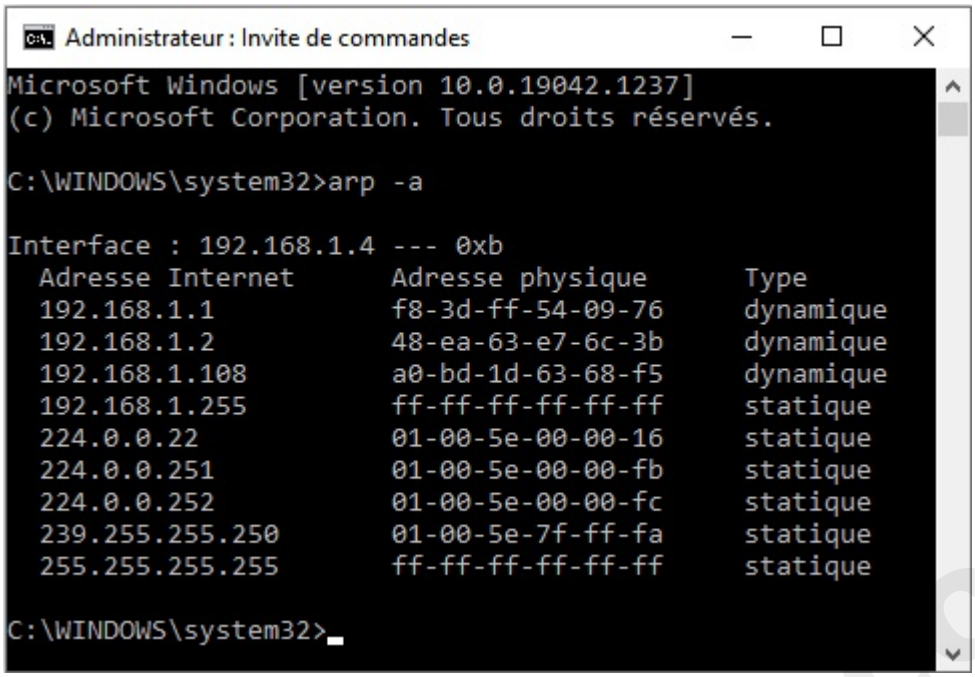
- **ARP Spoofing**

apcpedagogie.com

- Pour bien comprendre ce qu'est l'usurpation d'ARP et son fonctionnement, nous devons d'abord savoir ce qu'est l'ARP lui-même.
- Il signifie Address Resolution Protocol, et sa fonction principale est de résoudre les adresses de couche Internet en adresses de couche de liaison. Une autre façon de penser à ARP est qu'il traduit les adresses MAC en adresses de protocole Internet (et vice-versa).
- L'ARP (**A**ddress **R**esolution **P**rotocol) est un protocole qui convertit les adresses IP en adresses MAC (Media Access Control) pour la transmission des données.
- L'usurpation d’identité ARP est utilisée pour lier le MAC d’un pirate à une adresse IP d’un réseau légitime. L’attaquant peut ainsi recevoir des données destinées au propriétaire associé avec cette adresse IP.
- L’usurpation d’identité ARP est couramment utilisée pour voler ou modifier des données, mais elle peut également être utilisée dans les attaques par déni de service, les attaques man in the middle ou dans le détournement de session.
- **Comment détecter l'usurpation d'ARP ?**
- Vous préférez ne pas installer un programme externe supplémentaire ? Alors vous pouvez également utiliser la fonctionnalité intégrée de votre système d'exploitation pour détecter l'usurpation d'ARP.
    - Cette méthode utilise la ligne de commande, nous commençons donc par ouvrir un shell du système d'exploitation en tant qu'administrateur. Sous Windows 10, cela ressemblera à ceci :



    - Saisissez la commande suivante pour afficher la table ARP :**`arp -a`**



- Ensuite, vous voudrez vérifier s'il existe plusieurs adresses IP avec la même adresse MAC (appelée « adresse physique » ci-dessus). C'est ce qui indique qu'une attaque d'usurpation d'identité ARP est en cours.

- **L'usurpation de serveur DNS**
  - L’usurpation DNS (**D**omain **N**ame **S**ystem), également appelée empoisonnement du cache, est utilisée pour rediriger le trafic vers différentes adresses IP. Cela conduira les visiteurs vers des sites Web malveillants. Cela se fait en remplaçant les adresses IP stockées sur le serveur DNS par celles que l’escroc souhaite utiliser.
  - Les serveurs DNS convertissent les URL et les adresses e-mail en adresses IP correspondantes. L’usurpation d’identité DNS permet aux attaquants de détourner le trafic vers une adresse IP différente, conduisant les victimes vers des sites qui propagent des logiciels malveillants.

- **L'usurpation d'e-mails**
  - L'usurpation d'e-mails se produit lorsqu’un fraudeur envoie des e-mails contenant de fausses adresses d’expéditeurs dans le but d’infecter votre ordinateur avec des logiciels malveillants, de demander de l’argent ou de voler des informations. Ces fausses adresses d’expéditeurs sont créées pour donner l’impression qu’elles proviennent d’une personne que vous connaissez, comme un collègue ou un ami.
    Ces adresses peuvent être créées en utilisant des chiffres ou des lettres alternatifs pour avoir un aspect légèrement différent de l’original, ou en déguisant le champ « de » pour

être l’adresse e-mail exacte d’un membre de votre réseau.
- L'usurpation d'identité par e-mail a lieu lorsqu’un pirate utilise un message électronique pour faire croire à un destinataire qu’il provient d’une source connue et/ou fiable.
- Ces mails peuvent contenir des liens menant à des sites web nuisibles ou des pièces jointes infectées par des malwares. Ils peuvent également utiliser le social engineering pour convaincre leur destinataire de divulguer librement des informations sensibles.
- Les données des expéditeurs se piratent relativement facilement de deux façons :
  - En imitant une adresse e-mail ou un domaine de confiance à l’aide de lettres ou de chiffres alternatifs qui ne diffèrent que légèrement de l'original.
  - En faisant passer le champ "De" pour l’adresse e-mail exacte d’une source connue et/ou de confiance.

Comment se protéger de l'usurpation d'adresse IP ?

- Pour éviter ce genre d'attaques, il est recommandé de ne pas utiliser de service se basant sur l'adresse IP pour identifier les clients mais d'employer des solutions de niveau plus sécurisé avec authentification par exemple.
- Des algorithmes cryptologiques peuvent être utilisés pour authentifier le correspondant, comme c'est le cas par exemple dans IPsec, SSL, SSH. Il est aussi possible de faire appel à un tunnel VPN.
- Bien que l'usurpation d'adresse IP ne puisse être empêchée, des mesures peuvent être prises pour empêcher les paquets falsifiés d'infiltrer un réseau.
- Le filtrage d'entrée est une forme de filtrage de paquets généralement implémentée sur un périphérique de périphérie du réseau qui examine les paquets IP entrants et examine leurs en-têtes source. Si les en-têtes source de ces paquets ne correspondent pas à leur origine ou s'ils semblent louches, les paquets sont rejetés.
- Certains réseaux mettront également en œuvre un filtrage de sortie, qui examine les paquets IP sortant du réseau, garantissant que ces paquets ont des en-têtes source légitimes pour empêcher quelqu'un au sein du réseau de lancer une attaque malveillante sortante en utilisant l'usurpation d'adresse IP.

Exercices d'application

[h5p id="54"]

Sommaire du cours Administration et sécurité des sites web

apcpedagogie.com

Source : https://apcpedagogie.com/usurpation-dadresse-ip · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com