RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université des sciences et de la technologie Houari Boumediene Faculté d'Informatique

Rapport de projet

Filière : Sécurité des systèmes informatiques

Thème

Sécurisation du réseau d'une entreprise

Les membres :

- Aloui Ikram
- Bentaleb Ikram
- Issaadi Kaouther Ismahane
- Djennane Lyna
- Abdeddaim Rania Farah
- Djehaiche Maroua Fella
- Bouali Habiba
- Kechid Yasmine
- Brahimi Nesrine
- Asmani Lyna

Table des matières

Attaque de VLAN Hopping

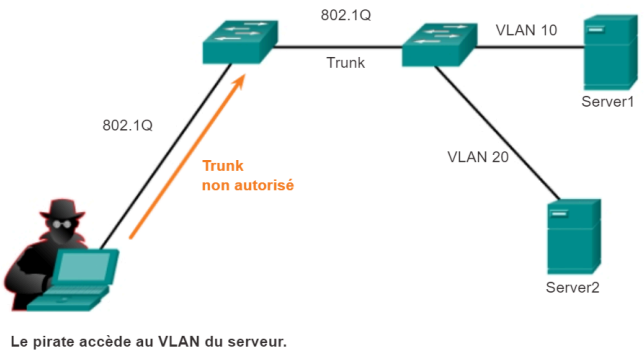
L'attaque VLAN Hopping est une méthode d'attaque des ressources réseau du VLAN en envoyant des paquets à un port qui n'est généralement pas accessible à partir d'un système final. L'objectif principal de cette forme d'attaque est d'accéder à d'autres VLAN sur le même réseau.
Dans le cas du saut de VLAN, un acteur malveillant doit d'abord pénétrer dans au moins un VLAN sur le réseau. Cela permet aux cybercriminels de créer une base d'opérations pour attaquer d'autres VLAN connectés au réseau.

Par double marquage

Les attaques par double marquage VLAN exploitent la manipulation des balises sur les trames Ethernet pour envoyer des paquets à travers n'importe quel VLAN en tant que VLAN natif non balisé sur la jonction. L'attaquant envoie une trame Ethernet avec deux étiquettes VLAN : une externe autorisée et une interne non autorisée. Les commutateurs ne suppriment que la balise externe avant de transférer la trame vers tous les ports VLAN natifs, permettant à l'attaquant d'accéder à d'autres VLAN.
En utilisant cette technique, l'attaquant peut tromper les commutateurs pour accéder à des VLAN auxquels il n'est normalement pas autorisé.

Usurpation d'identité

L'usurpation de commutateur se produit lorsque l'attaquant envoie des paquets DTP (Dynamic Trunking Protocol) de Cisco pour négocier une jonction avec un commutateur. Cela n'est possible que lors de l'utilisation des modes de commutation par défaut automatique dynamique ou dynamique souhaitable. Une fois qu'un trunk est connecté à l'ordinateur, l'attaquant accède à tous les VLAN.



Le pirate accède au VLAN du serveur.

solution:

-Utilisez des ACL VLAN pour filtrer le trafic non autorisé et empêcher le saut de VLAN.

-Utilisez des protocoles de troncage VLAN comme 802.1Q ou ISL pour vous assurer que les étiquettes VLAN sont correctement propagées entre les commutateurs.

-Utilisez des protocoles de sécurité tels que le VLAN Trunking Protocol (VTP) version 3

-désactivez la fonction d'agrégation automatique (DTP désactivée) sur tous les commutateurs qui n'ont pas besoin d'être agrégés.

ARP poisoning

ARP:

le protocole ARP est utilisé pour mapper les adresses IP (couche réseau) aux adresses MAC (couche liaison de données) sur un réseau local. Lorsqu'un appareil souhaite communiquer avec une autre machine sur le réseau, il envoie une requête ARP pour trouver l'adresse MAC associée à une adresse IP cible.

Empoisonnement ARP:

L'empoisonnement ARP est un type d'attaque de l'homme du milieu (MitM) qui permet aux pirates d'espionner les communications entre deux parties sur un réseau local (LAN). Le protocole ARP a été principalement conçu pour l'efficacité et non pour la sécurité. Les concepteurs du protocole n'ont pas inclus de système d'authentification pour valider les messages ARP. En conséquence, tout appareil sur le même réseau peut répondre à une requête ARP, même si le message original ne lui est pas destiné.
L'attaquant envoie des réponses ARP falsifiées aux appareils sur le réseau, associant son adresse MAC à l'adresse IP d'une autre machine (comme la passerelle par défaut).

Comment prévenir l'empoisonnement ARP?

- Utiliser un réseau privé virtuel (VPN) : Utiliser un VPN est le moyen le plus simple et le plus efficace pour prévenir l'empoisonnement ARP. Il permet à votre appareil de se connecter à Internet via un tunnel chiffré, rendant impossible pour un attaquant d'usurper ARP.
- Utiliser ARP statique : Le protocole ARP vous permet de créer une entrée ARP statique pour une adresse IP. Cela empêche les appareils d'écouter les réponses ARP pour cette adresse.

Comment identifier une attaque d'empoisonnement du cache ARP ?
Si le cache ARP d'un appareil spécifique a été empoisonné, la manière la plus simple de l'identifier est d'utiliser la ligne de commande :

- La commande suivante affiche la table ARP:

arp -a

- Cependant, si la table montre deux adresses IP différentes ayant la même adresse MAC, cela signifie que vous êtes victime d'une attaque d'empoisonnement ARP.

De plus, si on souhaite découvrir l'empoisonnement ARP dans un grand réseau et obtenir plus d'informations sur le type de communication que l'attaquant effectue, on utiliser Wireshark.

Effectuer attaque de spoofing ARP

Nous utiliserons une machine Kali fonctionnant sur une machine virtuelle en tant qu'attaquant.

Sur la cible, on ouvre CMD et utilisez la commande ***arp -a*** pour afficher la table de cache ARP. On allume la machine Kali et activez le port forwarding dessus. On ouvre deux terminaux différents sur Kali et exécutez la commande suivante dans le premier terminal :

arpspoof –i [interface] –t [IP de la cible] [IP du routeur]

et exécuter :

arpspoof –i [interface] –t [IP du routeur] [IP de la cible]

dans le second terminal.

En exécutant ces 2 commandes, des paquets ARP falsifiés seront envoyés à la fois à la machine cible et à la passerelle par défaut. Pour vérifier l'exécution de l'attaque, on utilise **arp -a** sur la machine cible et on constatera que la table de cache a été manipulée avec une fausse entrée de l'adresse MAC de la machine Kali correspondant à l'IP de la passerelle par défaut.

Une attaque de spoofing ARP réussie peut ouvrir la porte à des attaques plus graves comme l'homme du milieu (MitM), le déni de service (DoS) et le détournement de session.

DHCP starving

Le protocole DHCP:

Le protocole DHCP (Dynamic Host Configuration Protocol) est utilisé pour attribuer automatiquement des adresses IP aux machines d'un réseau. Il est également connu sous le nom de protocole zeroconf, car les administrateurs de réseau n'ont pas besoin d'attribuer manuellement des adresses IP aux machines. Pour attribuer les adresses IP, le DHCP utilise des paquets DORA, qui signifient respectivement Discover message (message de découverte), offer message (message d'offre), Request message (message de demande) et acknowledgegment message (message d'accusé de réception).

Attaque DHCP starving:

Une attaque de famine DHCP peut entraîner une attaque de déni de service (DoS) ou une attaque de l'homme du milieu (MitM). L'attaquant envoie de nombreux messages DHCP Discover avec des adresses MAC source falsifiées. Le serveur DHCP essaie de répondre à tous ces messages, épuisant ainsi le pool d'adresses IP du serveur. Un utilisateur légitime ne peut donc pas obtenir une adresse IP via DHCP. L'attaquant peut ensuite configurer un serveur DHCP malveillant pour attribuer des adresses IP aux utilisateurs légitimes, routant tout le trafic réseau via la machine de l'attaquant.

Prévention des attaques de famine DHCP:

- implémenter la sécurité des ports, en configurant un switch pour limiter le nombre d'adresses MAC apprises par port. Cela empêcherait les paquets falsifiés d'atteindre le serveur DHCP.

implementation de l'attaque:

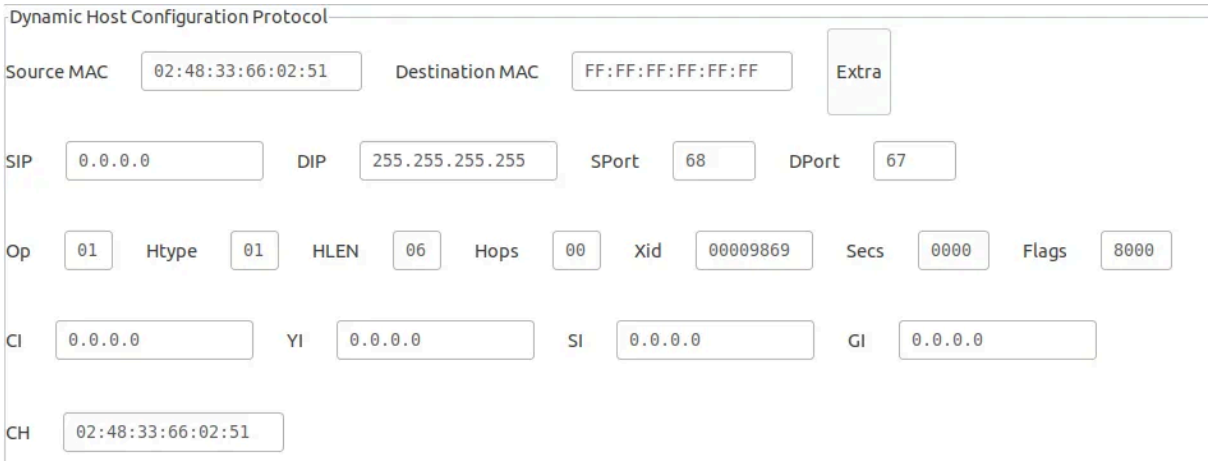
nous utilisons l'outils Yersinia un outil permettant de réaliser des attaques de couche 2. Il exploite les faiblesses des protocoles existants pour lancer une variété d'attaques.

Étape 1 : installer Yersinia de https://github.com/tomac/yersinia

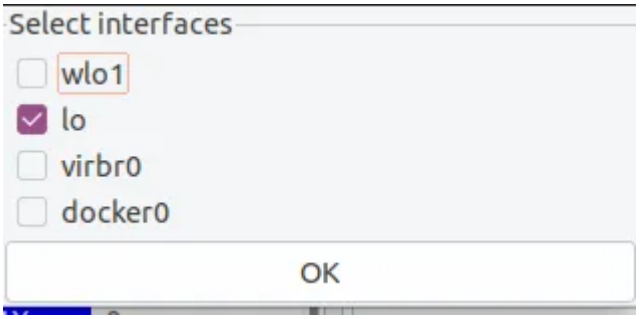
Étape 2 : Exécuter la commande suivante pour ouvrir Yersinia en mode GUI :

yersinia -G

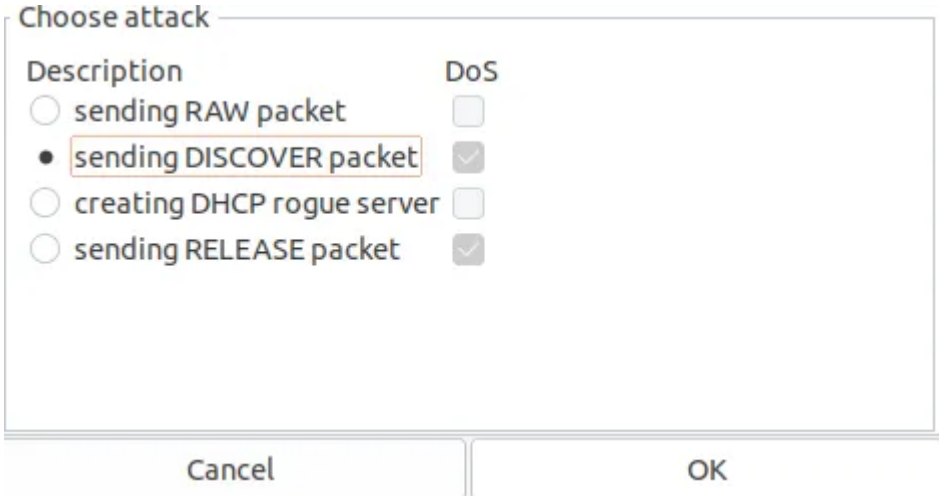
L'image montre les paramètres par défaut pour DHCP dans Yersinia. L'adresse IP source est définie sur 0.0.0.0 car les nouveaux utilisateurs envoient des paquets en utilisant cette adresse IP avant qu'ils ne reçoivent une adresse IP du serveur DHCP et l'adresse IP de destination est définie sur 255.255.255.255 car le paquet de découverte DHCP est diffusé sur tout le réseau.



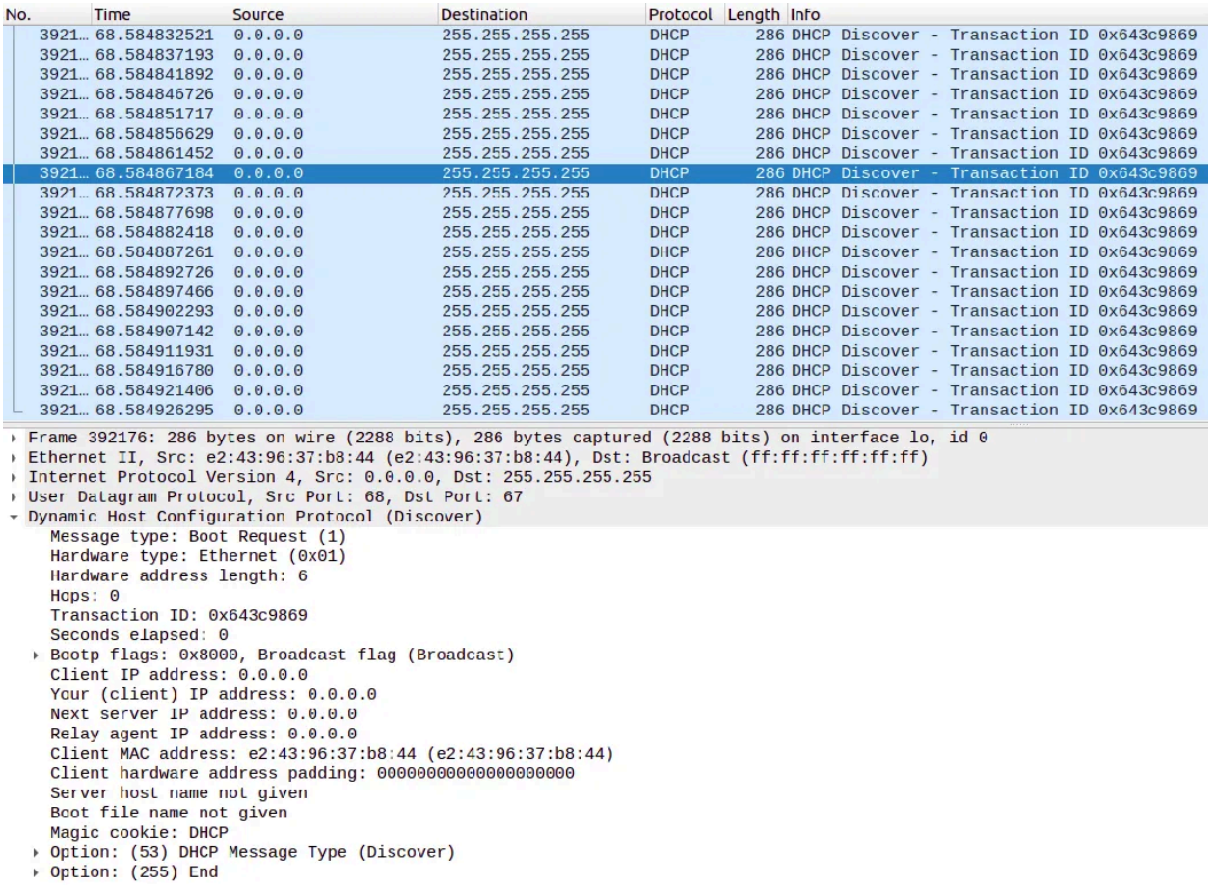
Étape 3 : Ensuite, nous devons sélectionner l'interface appropriée. À des fins de simulation, l'interface lo, c'est-à-dire l'interface de bouclage, a été sélectionnée. Ce paramètre enverra les paquets de découverte DHCP à l'adresse de bouclage.



Étape 4 : Ensuite, nous devons sélectionner le type d'attaque, c'est-à-dire "envoyer un paquet de découverte".



Étape 5 : Après avoir lancé l'attaque, de nombreux paquets de découverte DHCP ont été capturés à l'aide de Wireshark sur l'interface de bouclage. Nous pouvons voir un des paquets dans l'image ci-dessous. Nous pouvons également voir l'adresse MAC source fictive. Tous ces paquets ont des adresses MAC source différentes.

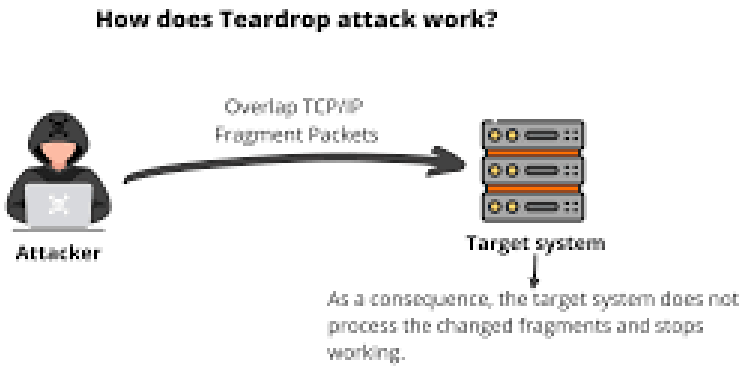


L'attaque Teardrop

L'attaque Teardrop, une forme de déni de service (DoS), vise à rendre des dispositifs ou des réseaux inaccessibles en les inondant de paquets de données surdimensionnés qui exploitent des vulnérabilités du processus TCP/IP et des codes de fragmentation.

Fonctionnement :

Les systèmes fragmentent les grandes données en petits morceaux, chacun ayant un numéro spécifique dans le champ de décalage de fragment. Lors d'une attaque, un acteur malveillant injecte une faille dans ce champ, perturbant ainsi l'ordre des fragments et entraînant l'accumulation de champs de décalage corrompus, ce qui provoque le plantage du système.



Stratégies d'atténuation :

- Pare-feu : Utiliser un pare-feu pour bloquer le trafic provenant de sources malveillantes connues.
- Déchargement de la fragmentation : Activer cette fonctionnalité pour permettre au système de réassembler les paquets fragmentés plus efficacement.
- Mises à jour : Maintenir le système et les logiciels de sécurité à jour pour corriger les vulnérabilités et détecter les nouvelles formes d'attaques.
- Systèmes de détection et de prévention des intrusions : Mettre en place ces systèmes pour identifier et bloquer le trafic malveillant.
- Éducation des utilisateurs : Former les utilisateurs et les administrateurs sur les risques des attaques Teardrop et les bonnes pratiques de sécurité (mots de passe forts, prudence avec les pièces jointes et liens).

Scan de Ports et Reconnaissance

Un attaquant, utilisant des outils comme Nmap, commence par effectuer une reconnaissance sur le réseau de l'entreprise pour identifier les dispositifs actifs et les services en cours d'exécution. Cette étape permet à l'attaquant de cartographier le réseau et de découvrir les points d'entrée potentiels. Par exemple, en scannant les plages d'adresses IP de l'entreprise, il peut identifier les serveurs critiques, les routeurs, et autres équipements réseau. Une fois ces dispositifs identifiés, l'attaquant procède à un scan des ports pour déterminer quels services (comme SSH, HTTP, etc.) sont disponibles sur ces dispositifs. Ces informations permettent à l'attaquant de planifier des attaques plus ciblées, exploitant les vulnérabilités des services identifiés.

Mesures de Sécurité :

- Utiliser des firewalls pour filtrer le trafic entrant.
- Désactiver les services et ports inutilisés.
- Mettre en place des systèmes de détection d'intrusion (IDS) pour surveiller et alerter sur les scans de ports.

Exploitation de Vulnérabilités

Après avoir identifié les services actifs, l'attaquant cherche des vulnérabilités connues associées à ces services. Par exemple, si un serveur web exécutant une version obsolète de WordPress est découvert, l'attaquant peut utiliser une vulnérabilité connue pour prendre le contrôle de ce serveur. Il recherche des exploits dans des bases de données de vulnérabilités comme CVE et utilise des outils comme Metasploit pour automatiser l'attaque. En réussissant à exploiter la vulnérabilité, l'attaquant obtient un accès non autorisé au serveur, ce qui lui permet d'exécuter des commandes à distance, de voler des données sensibles ou d'installer des logiciels malveillants.

Mesures de Sécurité :

- Mettre à jour régulièrement les systèmes et les applications avec les derniers correctifs de sécurité.
- Utiliser des solutions de sécurité applicative comme un Web Application Firewall (WAF).
- Effectuer des audits de sécurité réguliers et des tests de pénétration.

Attaque Man-in-the-Middle (MITM)

Dans une attaque Man-in-the-Middle, l'attaquant intercepte les communications entre deux dispositifs sans que ceux-ci ne s'en rendent compte. Cela peut être réalisé en utilisant des techniques d'ARP spoofing pour rediriger le trafic réseau via la machine de l'attaquant. Par exemple, dans un réseau interne où des dispositifs communiquent entre eux, l'attaquant envoie de fausses réponses ARP pour associer sa propre adresse MAC à l'adresse IP de la passerelle réseau. Une fois positionné entre les communications, l'attaquant peut capturer des informations sensibles telles que les identifiants de connexion, modifier les données transmises, ou rediriger les utilisateurs vers des sites malveillants.

Mesures de Sécurité :

- Activer Dynamic ARP Inspection (DAI) et DHCP Snooping sur les switches.
- Utiliser des protocoles sécurisés pour les communications (comme HTTPS et SSH).
- Mettre en place des systèmes de détection des intrusions pour détecter les attaques MITM.

Attaque par Déni de Service (DoS)

Un attaquant externe peut lancer une attaque par déni de service (DoS) pour rendre les services web de l'entreprise inaccessibles. En inondant le serveur cible avec un flux massif de requêtes, le serveur devient saturé et incapable de répondre aux requêtes légitimes des utilisateurs. Cette interruption de service peut entraîner des pertes financières et de réputation pour l'entreprise. Les attaques DoS peuvent être particulièrement dévastatrices si elles ciblent des services critiques comme des serveurs web ou des applications financières.

Mesures de Sécurité :

- Utiliser des services de protection contre les attaques DDoS (comme ceux fournis par Cloudflare ou Akamai).
- Mettre en place des solutions de surveillance pour détecter les attaques DDoS en temps réel.
- Configurer des règles de rate limiting pour limiter le nombre de requêtes par IP.

Intrusion dans le Réseau via la DMZ

La DMZ (zone démilitarisée) est souvent la cible des attaquants car elle contient des services accessibles depuis l'extérieur. Par exemple, si un serveur web dans la DMZ est compromis, l'attaquant peut tenter d'utiliser cette position pour pénétrer plus profondément dans le réseau interne. En exploitant des vulnérabilités dans le serveur web ou en utilisant des techniques de pivoting, l'attaquant peut essayer d'accéder aux bases de données ou à d'autres ressources internes protégées. La compromission de la DMZ peut servir de point de départ pour des attaques plus sophistiquées et persistantes.

Mesures de Sécurité :

- Isoler strictement la DMZ du réseau interne avec des firewalls.
- Utiliser des solutions de détection et de prévention des intrusions (IPS).
- Configurer des contrôles d'accès stricts pour les ressources critiques.

Attaque par Rejeu

Les attaques par rejeu impliquent la capture et la réutilisation de communications légitimes entre deux parties pour réaliser une action malveillante. Par exemple, un attaquant pourrait intercepter une session de connexion et rejouer les informations d'authentification pour accéder à un compte utilisateur sans en connaître le mot de

passe. Ces attaques exploitent souvent des failles dans les protocoles de communication qui ne sécurisent pas correctement les sessions.

Mesures de Sécurité :

- Utiliser des protocoles sécurisés avec chiffrement (comme TLS) pour les communications.
- Mettre en place des mécanismes de validation des sessions pour détecter et empêcher les tentatives de rejeu.
- Configurer des délais d'expiration pour les sessions afin de limiter la fenêtre d'opportunité pour les attaques par rejeu.

Exploitation des Protocole de Routage (OSPF)

Les attaquants peuvent exploiter les vulnérabilités des protocoles de routage, comme l'OSPF, pour injecter des routes malveillantes ou provoquer des recalculs fréquents des routes. Cela peut entraîner une instabilité du réseau, des boucles de routage, ou la redirection du trafic vers des destinations contrôlées par l'attaquant.

Mesures de Sécurité :

- Activer l'authentification sur les protocoles de routage (comme MD5 pour OSPF).
- Surveiller et journaliser les événements liés au routage.
- Utiliser des systèmes de détection des anomalies pour identifier les comportements suspects dans les annonces de routage.
- Manipulation des ports

Attaque DDoS

Les attaques DDoS visent à submerger un réseau ou un service en ligne avec un trafic massif provenant de multiples sources. Ces attaques peuvent rendre les services web inaccessibles et causer des interruptions de service significatives. Les attaquants peuvent utiliser des botnets pour orchestrer ces attaques à grande échelle.

Mesures de Sécurité :

- Collaborer avec des fournisseurs de protection DDoS pour bénéficier de capacités de mitigation en amont.

- Concevoir une architecture réseau redondante pour absorber et disperser le trafic de l'attaque.
- Utiliser des systèmes de détection d'anomalies pour identifier et filtrer le trafic malveillant en temps réel.
-

Vulnérabilités des Protocoles VRRP

Sans mécanisme d'authentification, un attaquant pourrait se faire passer pour un routeur virtuel légitime et influencer le processus d'élection pour devenir le routeur maître dans un réseau VRRP. Cela pourrait entraîner un détournement du trafic réseau et des interruptions de service.

Mesures de Sécurité :

- Activer l'authentification VRRP pour sécuriser les échanges de messages entre les routeurs virtuels.
- Utiliser des méthodes d'authentification comme MD5 pour VRRP.
- Surveiller les annonces VRRP pour détecter les comportements suspects.

Vulnérabilités Logicielles et Systèmes

Les vulnérabilités logicielles, comme celles présentes dans les systèmes Cisco vIOS et Arista EOS, peuvent être exploitées pour causer des dénis de service ou exécuter du code arbitraire. Par exemple, la CVE-2022-20661 permet à un attaquant d'exécuter du code persistant au démarrage ou de rendre le dispositif inopérant, tandis que la CVE-2023-20033 permet de provoquer un redémarrage intempestif du dispositif.

Mesures de Sécurité :

- Mettre à jour régulièrement les logiciels et les systèmes avec les derniers correctifs.
- Utiliser des solutions de surveillance et de gestion des vulnérabilités pour identifier et remédier rapidement aux failles.
- Configurer des mesures de sécurité supplémentaires comme BPDU Guard, IP Source Guard, et Dynamic ARP Inspection (DAI) pour renforcer la protection réseau.

En intégrant ces mesures de sécurité et en adoptant une approche proactive de surveillance et de gestion des vulnérabilités, l'entreprise peut renforcer

significativement sa posture de sécurité et se protéger contre une large gamme d'attaques.

Vulnérabilités server ubuntu

CVE-2017-16995 est une vulnérabilité d'escalade de privilèges locale (LPE) dans le noyau Linux qui affecte les systèmes Ubuntu 16.04.3 LTS exécutant le noyau 4.4.0-92-generic. Elle permet à un attaquant local d'exécuter du code arbitraire avec des privilèges élevés, compromettant ainsi le système.

Mesures de Sécurité:

-Mettez à jour le noyau Linux sudo apt-get update | sudo apt-get dist-upgrade |sudo reboot
-Installez les dernières mises à jour de sécurité: sudo apt-get update |sudo apt-get upgrade |sudo apt-get install unattended-upgrades
-Vérifiez la version du noyau: uname -r et assure que la version du noyau est supérieure à 4.4.0-116.

Vulnérabilité d'Escalade de Privilèges dans OpenSSH

elle affecte OpenSSH dans certaines configurations personnalisées où les groupes supplémentaires ne sont pas correctement initialisés Les commandes `AuthorizedKeysCommand` et `AuthorizedPrincipalsCommand`, conçues pour autoriser les clés et les principaux, peuvent être configurées pour s'exécuter en tant qu'utilisateur différent. Cependant, lorsque ces commandes sont utilisées avec cette configuration spécifique, les groupes supplémentaires du processus `sshd` ne sont pas réinitialisés comme prévu. Cela permet aux programmes auxiliaires de hériter des privilèges associés aux groupes du processus `sshd` plutôt que de l'utilisateur spécifié, entraînant une élévation de privilèges inattendue. Un attaquant qui contrôle ou influence ces commandes peut exploiter cette vulnérabilité pour exécuter du code avec des privilèges plus élevés que prévu.

Mesures de Sécurité:

-Mettre à jour OpenSSH vers la version 8.8 ou ultérieure où cette vulnérabilité est corrigée
-Limitez les permissions et les accès aux scripts utilisés par ces commandes.
-Ajoutez des vérifications et des mesures de sécurité dans les scripts pour s'assurer qu'ils ne s'exécutent qu'avec les groupes appropriés.

Partie Accès:
Le matériel de cette partie est très vulnérable, on a découvert plusieurs CVE et ces dernières sont encore découvertes jusqu'à ce jour, ce qui rend impossible de les lister . Donc en pratiquant de bonnes pratiques, on implémente dans notre infrastructure un logiciel qui surveille et effectue des mises à jour chaque période spécifique (15 jours par exemple).