Allsafe
Cybersecurity

12/2023

AMÉLIORATION DE LA SÉCURITÉ INFORMATIQUE

PROJET CYBERSECURITE ALLSAFE

Documentation

Imad CHAMKHI

SOMMAIRE

INTRODUCTION

ALLSAFE CYBERSECURITY, une entreprise spécialisée dans la fourniture de solutions de cybersécurité pour les professionnels, évolue dans des secteurs variés tels que les banques, les assurances et les grandes enseignes d'alimentation générale. Sous la direction de Monsieur Gideon GODDARD, l'infrastructure actuelle comprend une centaine de postes de travail et plusieurs serveurs virtualisés dans un datacenter local, avec un Plan de Reprise d'Activité (PRA) dans un cloud hybride.

Suite à des incidents internes liés à l'intégration de stagiaires, des pentests ont été commandés par Monsieur GODDARD pour évaluer la sécurité du réseau local. Lors d'un récent pentest réalisé par Mr. ALDERSON Elliot en utilisant une approche "ethical hacking" de type "gray hat", des attaques de type Man-In-The-Middle (MITM) ont été exécutées sans être détectées par l'équipe IT. Ces attaques ont exploité des faux messages ARP, permettant à l'attaquant de détourner les communications entre deux machines, ouvrant la porte à diverses menaces telles que le reniflage de paquets, le piratage de session, l'écoute d'appels VoIP, la manipulation des données, et d'autres.

ANALYSE DES BESOINS

Sécurité des laptops

- Mettre en place des contre-mesures pour prévenir les attaques MITM (Man-In-The-Middle) sur la flotte de 100 laptops équipés de Windows 10 Enterprise.
- Développer des mécanismes de détection avancée des faux messages ARP afin d'assurer l'intégrité des communications.

Sécurité des serveurs et commutateurs

- Proposer des solutions robustes contre l'ARP SPOOFING pour sécuriser les serveurs Windows 2019 GUI et GNU/Linux DEBIAN 10.
- Renforcer la sécurité des commutateurs CISCO 2960 en identifiant et en prévenant les attaques d'usurpation d'adresse ARP.

Évaluation du routeur/pare-feu

- Réévaluer le routeur/pare-feu "fait maison" fonctionnant sous GNU/LINUX DEBIAN 10.
- Revoir les règles de filtrage du côté LAN pour garantir une configuration optimale et minimiser les risques potentiels.

Développement de la Sécurité des Systèmes d'Informations (SSI)

- Mettre en place des programmes de sensibilisation et de formation du personnel pour réduire les risques liés aux attaques MITM et à l'empoisonnement ARP.
- S'assurer que les pratiques de sécurité sont intégrées dans tous les aspects du système d'information.

SOLUTION PROPOSÉE DANS LE CAHIER DE CHARGE.

- **AMÉLIORATION DE LA SÉCURITÉ RÉSEAU DES LAPTOPS**

Utiliser des sites sécurisés

- Les connexions HTTP ne sont pas sécurisées, le trafic et les identifiants de connexion passent en clair. Les sites HTTPS offrent un meilleur niveau de sécurité avec un chiffrement des données et une vérification de l'identité du site.
- Les sites HTTP peuvent être plus facilement falsifiés et redirigés par des attaquants, ce qui n'est pas possible avec HTTPS.

Utiliser un VPN

- Un VPN masque l'adresse IP de l'utilisateur, rendant plus difficile pour un attaquant de le cibler.
- La connexion entre le laptop et le serveur VPN est sécurisée dans un tunnel chiffré.

Chiffrer les données

- Le chiffrement symétrique et asymétrique des données empêche les tiers de récupérer les informations en cas de capture du trafic.
- HTTPS utilise des algorithmes de chiffrement pour protéger les identifiants de connexion.
- L'authentification à deux facteurs ajoute une couche de sécurité supplémentaire.

Sécuriser les connexions à des réseaux publics

- Il est recommandé de ne pas entrer d'identifiants de connexion sur des réseaux publics non sécurisés.
- Il faut également éviter d'effectuer des paiements en ligne sur ces réseaux.

Utiliser des outils de sécurité

- Sur Windows, NetCut Defender peut protéger contre l'empoisonnement ARP.
- Sur Linux, EtherWall peut détecter les attaques de type Man-in-the-Middle et FirewallD peut bloquer les ports pour éviter les reniflages.

- **AMÉLIORATION DE LA SÉCURITÉ DES SERVEURS WINDOWS ET GNU/LINUX**

Utiliser des entrées ARP statiques

- Sur Windows, on peut utiliser la commande arp -s pour configurer des entrées ARP statiques et empêcher la manipulation des caches ARP.

Segmenter le réseau en couches commutées

- En divisant le réseau en plusieurs segments commutés, les demandes de broadcast ARP ne touchent que les systèmes du même segment.
- Les commutateurs peuvent alors vérifier les requêtes ARP entre les segments et détecter les incohérences.

Utiliser des outils de surveillance ARP

- Des programmes comme Arpwatch, ARP-Guard ou XArp peuvent être utilisés pour surveiller le trafic ARP et détecter les activités suspectes.

Autres solutions pour se protéger de l'empoisonnement ARP

- Utiliser des tables ARP statiques sur un segment réseau séparé pour protéger les informations les plus sensibles.
- Appliquer une sécurité au niveau des ports des commutateurs pour n'autoriser qu'une seule adresse MAC par port.
- Chiffrer les identifiants de connexion avec SSL/TLS.

- **SOLUTIONS TECHNIQUES ET LOGICIELLES ET JUSTIFICATION DES CHOIX**

Port Security

- Le port security sur les commutateurs Cisco permet de limiter le nombre d'adresses MAC autorisées sur chaque port.
- Cela empêche les utilisateurs non autorisés de se connecter au réseau en restreignant l'accès aux ports du commutateur.
- Cela aide à prévenir les attaques par usurpation d'identité MAC et les accès non autorisés au réseau.

VLANs

- L'utilisation de VLANs permet de segmenter le réseau en différents réseaux logiques isolés.
- Cela permet d'isoler le trafic entre les différents groupes d'utilisateurs ou de périphériques (postes de travail, serveurs, etc.).
- Cela réduit le trafic inutile à travers l'ensemble du réseau et améliore la sécurité en cloisonnant les différents segments.

DHCP Snooping

- Le DHCP Snooping protège contre les attaques d'empoisonnement DHCP.
- Il s'assure que seuls les serveurs DHCP autorisés peuvent fournir des adresses IP aux clients.
- Cela empêche les attaquants de se faire passer pour un serveur DHCP légitime et de distribuer de fausses informations.

Dynamic ARP Inspection (DAI)

- Le DAI vérifie la correspondance entre les adresses IP et MAC dans les messages ARP.
- Cela permet de détecter et de bloquer les attaques par usurpation d'identité ARP.

• PRÉSENTATION DES MATÉRIELS, LOGICIELS ET DESCRIPTIFS DE FONCTIONNEMENTS.

Les commutateurs Cisco 2960 seront configurés avec les fonctionnalités de sécurité suivantes : Port Security, VLANs, DHCP Snooping et Dynamic ARP Inspection.

Les routeurs Cisco seront configurés pour surveiller le trafic ARP.

Les serveurs Windows 2019 et Debian 10 auront des adresses IP statiques pour prévenir l'ARP Spoofing.

Les laptops équipés de Windows 10 Enterprise auront le pare-feu Windows Defender activé avec des règles personnalisées.

Les outils de détection d'ARP Spoofing, tels que Colasoft Capsa pour Windows et ARPWatch pour Linux, seront utilisés de manière proactive pour détecter et réagir rapidement en cas d'attaques.

SOLUTION MISE EN PLACE POUR L'AMÉLIORATION DE LA SÉCURITÉ RÉSEAU DES LAPTOPS.

J'ai choisi XArp, un outil essentiel pour la détection et la prévention des attaques Man-In-The-Middle (MITM) basées sur le protocole ARP (Address Resolution Protocol).

INSTALLATION DE XARP

- **Configuration Système Requise**

Avant d'installer XArp, j'ai vérifié que mon système satisfait les conditions suivantes :

- Système d'exploitation : Windows (XP, 7, 8, 10)
- Espace Disque : 50 Mo disponible
- Mémoire RAM : 512 Mo ou plus
- Connexion Internet (pour les mises à jour)

- **Téléchargement et Installation**

1. J'ai consulté le site officiel de XArp (https://www.xarp.net/).
2. J'ai téléchargé la version compatible avec mon système d'exploitation.
3. J'ai exécuté le programme d'installation.
4. J'ai suivi les instructions à l'écran pour terminer l'installation.

- **Configuration Initiale**

Lors du premier lancement, XArp a effectué une configuration initiale minimale. J'ai suivi ces étapes :

1. J'ai ouvert XArp depuis le menu Démarrer.
2. J'ai sélectionné la langue de mon choix.
3. J'ai cliqué sur "Next" pour accepter les paramètres par défaut.
4. J'ai choisi si je souhaitais participer au programme d'amélioration.
5. J'ai cliqué sur "Finish" pour terminer.

CONFIGURATION DE XARP

- **Paramètres Généraux**

1. J'ai ouvert l'onglet "Settings" dans l'interface utilisateur.
2. J'ai configuré les options de démarrage automatique selon mes préférences.
3. J'ai choisi la langue préférée dans la section "Language".
4. J'ai cliqué sur "Apply" pour enregistrer les modifications.

- **Alertes et Notifications**

1. J'ai accédé à l'onglet "Alerts" pour définir le niveau de sensibilité des alertes.
2. J'ai configuré les notifications par courriel si nécessaire.
3. J'ai activé ou désactivé les alertes sonores en fonction de mes besoins.
4. J'ai sauvegardé les modifications en cliquant sur "Apply".

- **Gestion des Adresses IP et MAC**

1. Dans l'onglet "IP/MAC Addresses", j'ai géré les adresses IP et MAC de confiance.
2. J'ai ajouté les adresses qui doivent être exclues des alertes.
3. J'ai supprimé les entrées obsolètes.
4. J'ai cliqué sur "Apply" pour valider les changements.

- **Exclusion d'Adresses Confiance**

1. Accédez à l'onglet "Exclusions" pour exclure des plages d'adresses spécifiques.
2. J'ai ajouté des règles pour ignorer certains sous-réseaux.
3. J'ai cliqué sur "Apply" pour enregistrer les exclusions.

UTILISATION DE XARP

- **Interface Utilisateur**

J'ai la liste des adresses IP et MAC surveillées

J'ai les alertes en temps réel

J'ai les options de filtrage et de tri

- **Analyse en Temps Réel**

1. J'ai surveillé l'activité en temps réel dans l'onglet "Realtime"
2. J'ai identifié les alertes et les activités suspectes
3. J'ai utilisé les filtres pour affiner les résultats

- **Rapports et Journaux**

1. J'ai consulté les rapports dans l'onglet "Reports"
2. J'ai analysé les journaux pour une période spécifique
3. J'ai exporté les rapports si nécessaire

- **Réponses aux Alertes**

1. En cas d'alerte, j'ai identifié l'origine et la nature de l'attaque
2. J'ai pris des mesures appropriées pour sécuriser le réseau
3. J'ai utilisé les journaux pour l'analyse post-incident

SOLUTION MISE EN PLACE POUR L'AMÉLIORATION DE LA SÉCURITÉ DES SERVEURS WINDOWS ET GNU/LINUX

UTILISATION D'IDS/IPS POUR LA DÉTECTION D'ARP POISONING

- **Installation de Colasoft Capsa (Windows)**

Colasoft Capsa est un outil d'IDS/IPS permettant de détecter les activités ARP suspectes sur les serveurs Windows. Voici les étapes à suivre pour son installation :

1. J'ai téléchargé Colasoft Capsa depuis le site officiel.
2. J'ai exécuté le programme d'installation.
3. J'ai suivi les instructions à l'écran pour installer le logiciel.

- **Configuration des Règles d'IDS/IPS**

Une fois Colasoft Capsa installé, j'ai configuré les règles pour détecter les attaques ARP Poisoning :

1. J'ai lancé Colasoft Capsa.
2. J'ai accédé à l'onglet "Rules" ou "Règles" selon la version.
3. J'ai ajouté une règle pour détecter les anomalies ARP.
4. J'ai spécifié les actions à entreprendre en cas de détection (par exemple, alerter l'administrateur).

En suivant ces étapes, j'ai pu installer et configurer Colasoft Capsa pour surveiller mon réseau et détecter les attaques ARP Poisoning.

SURVEILLANCE DU TRAFIC ARP AVEC ARPWATCH (LINUX)

- **Installation d'ARPWatch**

ARPWatch est un outil de surveillance du trafic ARP sur les serveurs Linux. Voici les étapes pour l'installer :

1. J'ai ouvert le terminal sur le serveur Linux.
2. J'ai exécuté la commande : `**sudo apt-get install arpwatch**`.
3. J'ai édité le fichier **`sudo nano /etc/default/arpwatch`** pour configurer les interfaces à surveiller.
4. J'ai redémarré ARPWatch avec la commande **`sudo systemctl restart arpwatch`**.

- **Configuration d'ARPWatch**

Pour configurer ARPWatch pour surveiller le trafic ARP :

1. J'ai édité le fichier de configuration d'ARPWatch.
2. J'ai spécifié les actions à entreprendre en cas de détection d'activités ARP suspectes.
3. J'ai redémarré ARPWatch pour appliquer les modifications.

- **Configuration sur les Serveurs Linux**

Sur les serveurs Linux, j'ai utilisé la commande `arp` pour configurer une adresse ARP fixe :

1. J'ai ouvert le terminal.
2. J'ai exécuté la commande : `sudo arp -s [adresse IP] [adresse MAC]`.
3. J'ai répété cette opération pour chaque adresse IP du serveur.

- **Configuration sur les Serveurs Linux**

Sur les serveurs Linux, j'ai utilisé la commande `arp` pour configurer une adresse ARP fixe :

1. J'ai ouvert le terminal.
2. J'ai exécuté la commande : `sudo arp -s [adresse IP] [adresse MAC]`.
3. J'ai répété cette opération pour chaque adresse IP du serveur.

- **Mettre en place des règles de pare-feu sur Linux**

J'ai utilisé `iptables` pour configurer des règles de pare-feu sur les serveurs Linux, limitant le trafic ARP aux adresses MAC légitimes.

- **Utiliser des VPNs sur Linux**

J'ai installé et configuré OpenVPN, un serveur VPN populaire sur Linux, pour sécuriser le trafic réseau.

" **bashCopy code sudo apt-get install openvpn "**

SOLUTION MISE EN PLACE POUR L'AMÉLIORATION DE LA SÉCURITÉ AU NIVEAU DES COMMUTATEURS CISCO

- **Connexion au Commutateur**

1. J'utilise un navigateur Web compatible avec l'interface de gestion des commutateurs Cisco Google Chrome.
2. J'entre l'adresse IP du commutateur dans la barre d'adresse .
3. Je me connecte en utilisant mes informations d'identification.

- **Configuration de Port Security**

Je configure le Port Security sur chaque port des commutateurs pour limiter le nombre d'adresses MAC autorisées.

`switchport port-security`

`switchport port-security maximum 1`

`switchport port-security violation restrict`

- **Configuration des VLANs**

J'utilise les VLANs pour segmenter le réseau et isoler les postes de travail, les serveurs et autres dispositifs.

- `vlan 10`

- `name Postes_Travail`

- `vlan 20`

- `name Serveurs`

- **Activation du DHCP Snooping**

J'active le DHCP Snooping pour protéger contre les attaques d'empoisonnement DHCP.

`ip dhcp snooping`

`ip dhcp snooping vlan 10,20`

- **Activation de Dynamic ARP Inspection (DAI)**

Je configure le Dynamic ARP Inspection pour valider les associations entre les adresses IP et les adresses MAC.

- `ip arp inspection vlan 10,20`

- **Configuration de la surveillance du trafic ARP**

Je configure certains routeurs Cisco pour surveiller le trafic ARP et détecter les activités suspectes.

- `interface FastEthernet0/0`

- `ip verify unicast source reachable-via rx`

- **Bonnes Pratiques de Sécurité**

Je change régulièrement les mots de passe d'administration.

Je surveille les journaux d'événements pour détecter toute activité suspecte.

Je mets à jour régulièrement le firmware des commutateurs.

COMPÉTENS ACQUIS

Expertise en cybersécurité :

- Compréhension approfondie des concepts de cybersécurité et des techniques de protection contre les attaques MITM et ARP Spoofing.

Gestion des équipements réseau :

- Capacité à configurer et gérer efficacement les commutateurs Cisco, les routeurs et autres équipements réseau.

Connaissance des protocoles de sécurité réseau :

- Maîtrise des protocoles de sécurité tels que Port Security, VLANs, DHCP Snooping et Dynamic ARP Inspection.

Utilisation d'outils de sécurité :

- Aptitude à utiliser des outils de détection d'attaques ARP et de surveillance du trafic réseau, comme XArp, Colasoft Capsa et ARPWatch.

Sécurisation des systèmes d'exploitation :

- Compétences en configuration et sécurisation des systèmes Windows et GNU/Linux, y compris la gestion des adresses ARP statiques.

Mise en place de bonnes pratiques de sécurité :

- Capacité à mettre en place des procédures de surveillance régulière des journaux d'événements et de mise à jour du firmware des équipements.

Communication et sensibilisation :

- Compétences en communication et en conception de programmes de formation du personnel sur les risques liés aux attaques MITM et ARP Spoofing.

CONCLUSION

Nous avons conçu ce projet en réponse aux incidents internes et aux tests d'intrusion réalisés chez ALLSAFE CYBERSECURITY. À la suite d'une analyse approfondie des besoins et des objectifs de l'entreprise, nous avons proposé et mis en œuvre des solutions pour prévenir les attaques Man-In-The-Middle (MITM), renforcer la sécurité des serveurs et des commutateurs, évaluer et améliorer le routeur/pare-feu, et développer la sensibilisation du personnel.

Les principaux axes du projet ont été définis pour répondre spécifiquement aux besoins de l'entreprise. Nous avons mis en place des contre-mesures telles que la configuration de Port Security, l'utilisation de VLANs, l'activation du DHCP Snooping et de Dynamic ARP Inspection, ainsi que la surveillance du trafic ARP.

Nous avons soigneusement sélectionné les solutions techniques et logicielles pour répondre aux exigences de sécurité tout en tenant compte de la compatibilité avec l'infrastructure existante. Des outils comme XArp, Colasoft Capsa et ARPWatch ont été intégrés pour la détection proactive des attaques ARP et la réaction rapide en cas d'incident.

Grâce à ce projet, notre équipe a renforcé la posture de sécurité des systèmes d'information d'ALLSAFE CYBERSECURITY, réduit les vulnérabilités et les risques associés aux attaques MITM et ARP Spoofing, et assuré la continuité des opérations dans un environnement de cybersécurité de plus en plus complexe et menaçant.