Liste Menace

La première menace identifié est l'empoisonnement ARP :

Dans un réseau local, les machines utilisent les adresses MAC pour envoyer des paquets. Pour faire le lien entre une IP et une MAC les systèmes utilisent le protocole ARP.

Principe de l'attaque

Après avoir eu accès au réseau, l'attaquant envoie un paquet réponse ARP (reply) falsifié à la victime avec l'adresse IP source du routeur et sa propre adresse MAC, et un autre paquet réponse ARP falsifié au routeur avec l'adresse IP source de la victime et sa propre adresse MAC. :

Victime : IP routeur correspond à MAC de l'attaquant

Routeur : IP Victime correspond à MAC de l'attaquant

ARP étant un vieux protocole (années 80) il a était initialement conçu pour fonctionner sur des réseaux sécurisé, et donc il n'y a aucune authentification, aucune vérification que le paquet ARP a était demandé et aucune protection contre les faux paquets et donc la table ARP se met à jour automatiquement avec une réponse ARP :

Request : Une machine demande "Qui à l'adresse IP 192.168.x.x ? Donne moi ton adresse MAC."

Reply : Une machine répond "Moi, L'IP 192.168.x.x correspond a la MAC AA:BB:CC:DD:EE:FF."

Pour des questions de réduction des délais de communication, d'avoir une table ARP toujours à jour sans avoir à lancer toujours une requête pour remplir la table.

L'attaquant envoi donc des reply ARP aux machines du réseau avec en IP source le routeur pour la victime et la victime pour le routeur avec sa propre MAC (celle du pirate)

Conséquence

Le traffic destiné au routeur est redirigé vers l'attaquant, qui peut alors :

Intercepter les données échangées, les modifier, ou simplement les relayer au routeur afin de les espionner sans attirer l'attention.

La deuxième menace identifier est l'empoisonnement DNS :

Le DNS est comme un annuaire qui fait la relation entre nom de domaine d'un site web et adresse IP.

Principe de l'attaque

L'attaquant intercepte la requête DNS de la victime et envoie une réponse DNS falsifié avant que le vrai serveur DNS ne le fasse. La victime est alors redirigé vers l'IP du site que l'attaquant a fait correspondre au nom de domaine dans la requête de la victime.

L'attaquant intercepte la requête DNS de la victime, garde en tête quelque informations et en falsifie tel que :

- l'ID de la requête initiale envoyer par la victime,
- le nom de domaine demandés,
- l'enregistrement A (IPv4), en le faisant pointer vers l'IP du site frauduleux,
- l'IP source du paquet (mise à l'adresse IP du vrai serveur DNS),
- l'IP de destination (IP de la victime)

l'attaquant lui répond alors avec une fausse réponse contenant ces informations, et le système de la victime croit recevoir une réponse légitime de la part du serveur DNS requêter.

Conséquence

La victime croit se connecter à un site légitime (comme sa banque), mais elle se retrouve sur un site frauduleux (phishing, infection par malware, ...)