

Le RAT

Pré-Requis

Deux machines virtuelles Debian9 :

- Une qui jouera le rôle de l'attaquant et l'autre le rôle de la victime

Avoir des connaissances de base dans l'utilisation du langage Python.

- Il ne s'agit pas d'un cours de Python !

Ce programme n'est qu'une base de travail que vous pourrez par la suite enrichir à votre convenance.

Il est interdit d'utiliser ce type de programme sur un système dont vous n'êtes pas propriétaire ou pour lequel vous n'avez pas reçu les autorisations.

Qu'est-ce qu'un RAT ?

RAT signifie Remote Access Tool.

On peut également retrouver les dénominations suivantes :

- Remote Administration Tool
- Remote Admin Tool
- Remote Admin Tools

Il s'agit d'un programme permettant la prise de contrôle totale, à distance, d'un équipement depuis un autre équipement.

Composition d'un RAT

Le RAT est généralement constitué de deux parties : le « Client » et le « Serveur ».

Le Client est installé sur l'ordinateur de l'attaquant et le serveur est installé sur l'équipement à contrôler.

Notre code

Le code que nous allons créer va nous permettre d'exécuter toutes les commandes disponibles au niveau du terminal depuis notre ordinateur à destination de l'équipement attaqué.

Nous pourrions ainsi par exemple capturer le contenu du fichier `/etc/shadow` afin de cracker les mots de passe qui y sont stockés.

Utilisation de Socket

Dans notre code nous allons utiliser ce qu'on appelle des **Sockets**.

On peut le traduire par « Connecteur Réseau » ou « Interface de Connexion ».

Il s'agit d'une interface logicielle avec les services du système d'exploitation, grâce à laquelle le développeur peut utiliser les services d'un protocole Réseau.

- On peut ainsi aisément y établir une session TCP, puis recevoir et envoyer des données grâce à elle.