

## Commandes du système de fichiers

- **cat** - Lire et diffuser le contenu d'un fichier
- **cd** - Modifier le répertoire sur la victime
- **del** - Supprimer un fichier sur la victime
- **download** - Téléchargez un fichier du système de la victime vers le système de l'attaquant
- **edit** - Éditer un fichier avec vim
- **getlwd** – Affiche le répertoire local
- **getwd** – Affiche le répertoire de travail
- **lcd** – Changer le répertoire local
- **lpwd** – Affiche le répertoire local
- **ls** - Liste des fichiers dans le répertoire actuel
- **mkdir** - Créer un répertoire sur le système de la victime
- **pwd** – Affiche le répertoire de travail
- **rm** – Effacer un fichier
- **rmdir** - Supprimer le répertoire sur le système de la victime
- **upload** - Télécharger un fichier du hacker vers la victime

## Commandes réseau

- **ipconfig** - Affiche les interfaces réseaux avec des informations clés, y compris l'adresse IP, etc.
- **portfwd** - Transféré un port sur le système de la victime vers un service distant
- **route** - Afficher ou modifier la table de routage de la victime

## System Commands

- **clearav** - Efface les journaux d'événements sur l'ordinateur de la victime
- **drop\_token** - Dépose un jeton volé
- **execute** – Exécuter une commande
- **getpid** - Obtient l'ID de processus actuel (PID)
- **getprivs** - Obtient autant de privilèges que possible
- **getuid** – Obtient l'utilisateur que le serveur est exécuté de
- **kill** - Mettre fin au processus désigné par le PID
- **ps** - Liste des processus en cours
- **reboot** - Redémarre l'ordinateur victime
- **reg** - Interagir avec le registre de la victime
- **rev2self** - Appelle RevertToSelf () sur la machine victime
- **shell** - Ouvre un shell de commande sur la machine victime
- **shutdown** - Arrête l'ordinateur de la victime
- **steal\_token** - Tente de voler le jeton d'un processus spécifié (PID)

- **sysinfo** - Obtient les détails sur l'ordinateur victime tel que le système d'exploitation et son nom

### **User Interface Commands**

- **enumdesktops** – Affiche tous les ordinateurs de bureau accessibles
- **getdesktop** – Obtenir le poste de travail meterpreter actuel
- **idletime** - Vérifie depuis combien de temps que le système victime est inactif
- **keyscan\_dump** – Obtenir le contenu du keylogger
- **keyscan\_start** - Démarre le keylogger lorsqu'il est associé à un processus tel que Word ou un navigateur
- **keyscan\_stop** – Arrêt du keylogger
- **screenshot** – Saisit une capture d'écran du bureau de l'ordinateur victime
- **uictl** - Permet de contrôler certains des composants de l'interface utilisateur