
MANUEL D'UTILISATION

Installation

Pour simplifier l'installation du pare-feu, 2 scripts ont été prévu : le premier pour installer Python et le deuxième pour installer les librairies complémentaires.

1^{ère} étape : setup.bat

1. Au lancement de setup.bat, une interface pour l'installation de python s'ouvre.
2. Cochez la case **Add Python 3.6 to PATH**
3. Cliquez sur **Install now**
4. Une fois l'installation terminée, sélectionnez **Disable path lenght limit**
5. L'installation étant terminée, cliquez sur **Close**

En cas de difficultés, vous pouvez télécharger Python depuis python.org, et reprendre l'installation à partir de l'étape 1.2

2^{ème} étape : setup-dependencies.bat

1. Pour cette étape, aucune action n'est nécessaire. Il vous suffit de lancer le script

En cas de difficultés, vérifiez que Python a bien été ajouté au variables d'environnement de votre ordinateur. Ce problème peut survenir si Python était déjà installé. Vous pouvez également télécharger les librairies vous-même.

Un raccourcis a été ajouter sur votre bureau. Il ne vous reste plus qu'à l'exécuter en administrateur pour lancer l'invite de commande du pare-feu.

Invite de commande

Après le lancement du programme, une invite de commande se présente, vous pouvez entrer les premières commandes.

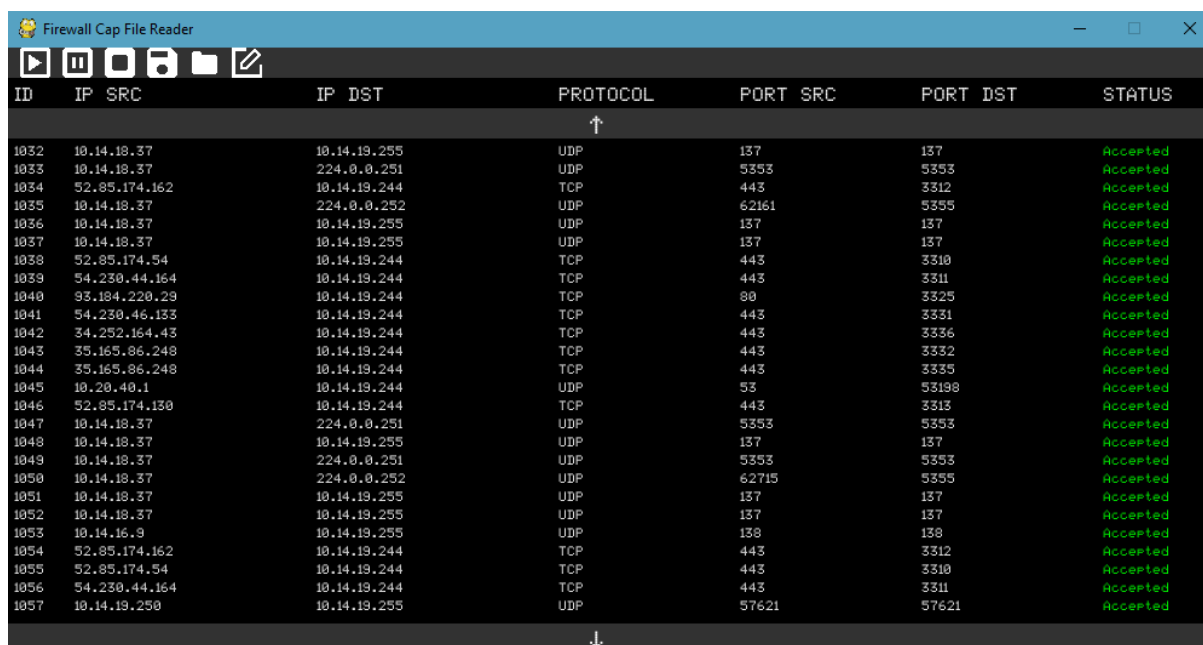
Pour commencer, utilisez la commande « man ». Elle va lister une série de commandes utiles.

ATTENTION : l'invite doit être **obligatoirement** être lancé en tant qu'administrateur.

Commandes

- **man** : affiche la liste des commandes disponibles.
- **start firewall** : lance le pare feu et l'analyse des paquets.
- **stop firewall** : interrompt le pare-feu et son processus d'analyse.
- **start interface** : affiche l'interface graphique.
- **stop interface** : masque l'interface graphique.
- **ban <host name>** : bloque l'accès à une adresse IP d'après son host name.
Ex : *ban rennes-atalante.fr*
- **unban <host name>** : révoque une interdiction d'accès. Ex : *unban rennes-atalante.fr*
- **add rule <rules>** : ajoute une règle et ses propriétés. Ex : *add rule protocol: TCP, portdest: 80*
- **delete rule <index>** : supprime une règle selon son index. Ex : *delete rule 27*
- **read file <path>** : permet de lire un fichier .cap. Ex : *read file C:\Users\user\desktop\mycapfile.cap*
- **show rules** : affiche une liste des règles mises en place.
- **show status** : affiche le statut du pare-feu et de l'interface (ON/OFF).
- **show packets** : affiche les paquets selon un schéma. (*ID, IP source, IP de destination, protocole, port source, port de destination*)
- **exit** : quitte l'invite de commande.

Interface graphique



ID	IP SRC	IP DST	PROTOCOL	PORT SRC	PORT DST	STATUS
1032	10.14.18.37	10.14.19.255	UDP	137	137	Accepted
1033	10.14.18.37	224.0.0.251	UDP	5353	5353	Accepted
1034	52.85.174.162	10.14.19.244	TCP	443	3312	Accepted
1035	10.14.18.37	224.0.0.252	UDP	62161	5355	Accepted
1036	10.14.18.37	10.14.19.255	UDP	137	137	Accepted
1037	10.14.18.37	10.14.19.255	UDP	137	137	Accepted
1038	52.85.174.54	10.14.19.244	TCP	443	3310	Accepted
1039	54.230.44.164	10.14.19.244	TCP	443	3311	Accepted
1040	93.184.220.29	10.14.19.244	TCP	80	3325	Accepted
1041	54.230.46.133	10.14.19.244	TCP	443	3331	Accepted
1042	34.252.164.43	10.14.19.244	TCP	443	3336	Accepted
1043	35.165.86.248	10.14.19.244	TCP	443	3332	Accepted
1044	35.165.86.248	10.14.19.244	TCP	443	3335	Accepted
1045	10.20.40.1	10.14.19.244	UDP	53	53198	Accepted
1046	52.85.174.130	10.14.19.244	TCP	443	3313	Accepted
1047	10.14.18.37	224.0.0.251	UDP	5353	5353	Accepted
1048	10.14.18.37	10.14.19.255	UDP	137	137	Accepted
1049	10.14.18.37	224.0.0.251	UDP	5353	5353	Accepted
1050	10.14.18.37	224.0.0.252	UDP	62715	5355	Accepted
1051	10.14.18.37	10.14.19.255	UDP	137	137	Accepted
1052	10.14.18.37	10.14.19.255	UDP	137	137	Accepted
1053	10.14.16.9	10.14.19.255	UDP	138	138	Accepted
1054	52.85.174.162	10.14.19.244	TCP	443	3312	Accepted
1055	52.85.174.54	10.14.19.244	TCP	443	3310	Accepted
1056	54.230.44.164	10.14.19.244	TCP	443	3311	Accepted
1057	10.14.19.250	10.14.19.255	UDP	57621	57621	Accepted

Affichage :

ID : Numéro du paquet

IP SRC : Adresse IP source

IP DST : Adresse IP de destination


PROTOCOL : Protocole réseau utilisé


PORT SRC : Port source

PORT DST : Port de destination


STATUS : Statut du paquet traité


Fonctionnalités :

 : Permet la vision en direct des paquets une fois analysés.

 : Met en pause le flux de paquets.

 : Interrompt et masque le flux de paquets.

 : Créé un fichier de capture avec les paquets actuels ou sauvegarde les dernières règles ajoutées via l'interface (selon l'endroit dans lequel on se trouve dans l'interface : vue du flux ou gestionnaire de règles).

 : Permet d'ouvrir et de lire un fichier .pcap (uniquement).

 : Ouvre le gestionnaire de règles.