Information Gathering Automation

(misc.)

X-MAS CTF 2019

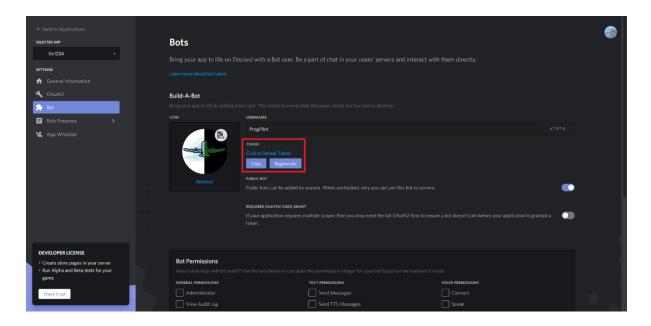
Written by Tom Pain (0x5444) for ProgPilot

Information Gathering Automation was a challenge which was part of the 2019 X-MAS CTF, organised by HTsP. The description was as follows:

"Our agency wants to collect information related to the next line-up of entertainment objects that are currently being built by Santa's gnome team. We noticed that the factory only trusts Discord bots to enter, so we need you to create an Information Gathering Automation in order to collect the factory's secrets."

It sounded interesting and right up my street, so I thought I'd give it a shot.

The brief specified we'll have to make our own Discord bot, so I set about doing that first. It's fairly simple to setup your own Discord bot - head to the My Applications section of the Discord Developer Portal, hit new application, give it a name, enable the bot feature, and you're set. Note down the token.



To get your bot in the factory server, you have to make up an invite URL for it (see https://discordapp.com/developers/docs/topics/oauth2#bot-authorization-flow) and send that URL to the challenge author.

Once this has been done, you can begin writing your bot code. I used <u>Discord.Py</u> for this, but you could use <u>Discord.JS</u> if you wanted.

The code I wrote was simple - the bot would connect, check if it was a member of the target guild (in this case "Toy Factory") and if it was, iterate over every channel and retrieve the last 200 messages. If a message that had "X-MAS" in it was found, that would be highlighted.

```
None -
None - (@207598855666139137) Nope :)
None - i kindof feel like sending a message in every server im in on start to trigger an on message send event to get t server info was not the most efficient way to do this :joy:
X-MAS{this-isnt-the-flag-but-i-hope-it-tripped-up-your-bot}
None - X-MAS{this-isnt-the-flag-but-i-hope-it-tripped-up-your-bot}
None - yo what's up
None - angery
None - i kindof feel like sending a message in every server im in on start to trigger an on message send event to get server info was not the most efficient way to do this :joy:
None -
None -
None -
None -
None -
None - behave yourselves
```

Nice try

```
C:\Python37\python.exe
                                                                                                                                                                                                                                                                                                            П
 ogged in as ProgPilot#7474 - bot is a member of the folling guilds
<Guild id=592045028679876621 name='dfkjgh' shard_id=None chunked=True member_count=3>, <Guild id=616408544090128395 nam
:='Toy Factory' shard_id=None chunked=True member_count=17>]
The bot is a member of the target guild.
Indexing messages
 Channel '{channel.name}' '{channel.topic}'
None - Nice, gj
None - thanks :)
None - this was a super cool challenge!
                     - yo
- yo whats up guys
        None -
None -
None -
None -
None -
None -
                     - D DD
- thanks for the challenge!
         None -
Totally Not An Information Gathe -
         None - our handy little automaton
None - Welcome, MOL3
                      - welcome!
                           swiggity swoggity
   nannel '{channel.name}' '{channel.topic}'
        nnel '{channel.name}' '{channel.topic}'
None - henlo
None - hey
nnel '{channel.name}' '{channel.topic}'
None - I can say 'Hot'.
None - pretty close, yes
None - am I close to the flag?
None - bring it
 None - bring it
None - yes
None - yes
None - wanna play hot or cold?
channel '{channel.name}' '{channel.topic}'
None - all good!
None - whatsup fellow elves
channel '{channel.name}' '{channel.topic}'
None - @everyone Elves will start their normal working schedule tomorrow.
channel '{channel.name}' '{channel.topic}'
None - @veryone Elves will start their normal working schedule tomorrow.
        None - lol
None - I heard reindeers go like NEEEEEEigh
nnel '{channel.name}' '{channel.topic}'
None - haha
        None - haha
None - and yes, indeed it's `hotter`
None - how do `YOU' know?
None - hotter
None - how close am I now?
nnel '{channel.name}' '{channel.topic}'
None - nice work
None - Sweet! `NOW` I got it!
X-MAS(Blind As A mel3 scouring through
```

Actual output (yes, I did forget an f string)

You can see the code I wrote for this challenge here.

Challenge description

Information Gathering Automaton 496 Points Our agency wants to collect information related to the next line-up of entertainment objects that are currently being built by Santa's gnome team. We noticed that the factory only trusts Discord bots to enter, so we need you to create an Information Gathering Automaton in order to collect the factory's secrets. You can PM Milkdrop your Discord bot invite token so that he adds it to the factory server. Author: Milkdrop