Firstly, I ensured the VM could pick up ip addresses for both interfaces

A computer screen shot of a black screen

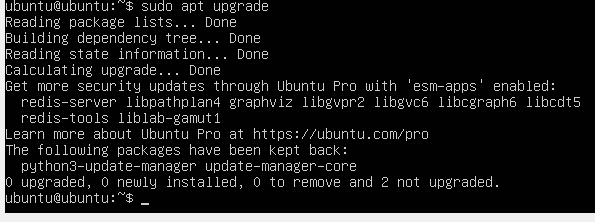
Description automatically generated

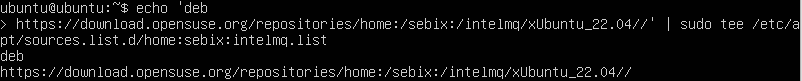
A screenshot of a computer program

Description automatically generated

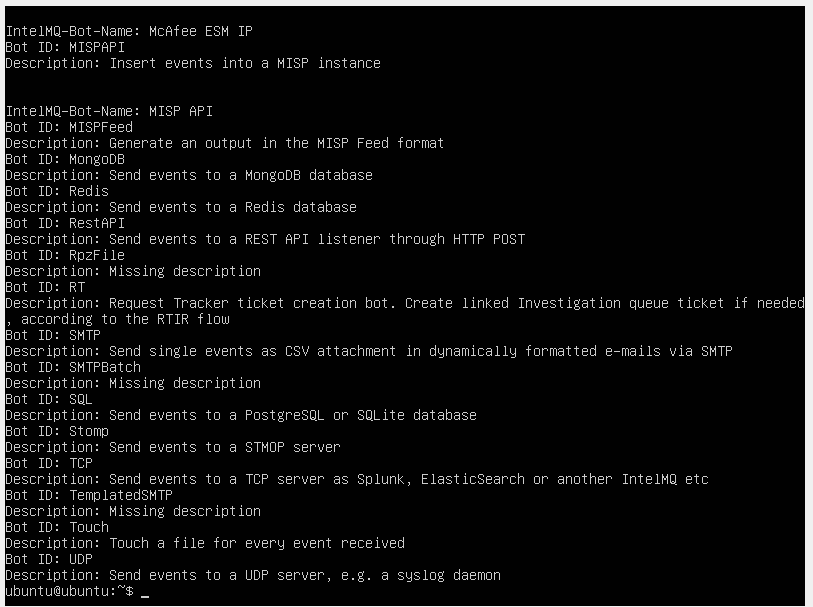
A screenshot of a computer

Description automatically generated





Next, I had to ensure IntelMQ was updated and installed properly

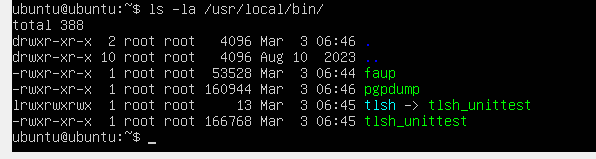


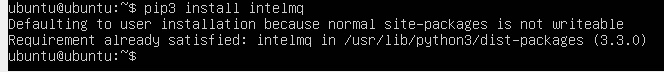
I then checked what bots were configured on intelmq

A computer screen with white text

Description automatically generated







Pip3 is not integrated with intelmq so we can begin searching for the data sources using “pip search”

A screenshot of a computer screen

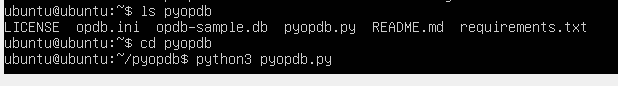
Description automatically generated

Next, I had to install GIT, Python and PHP SSH

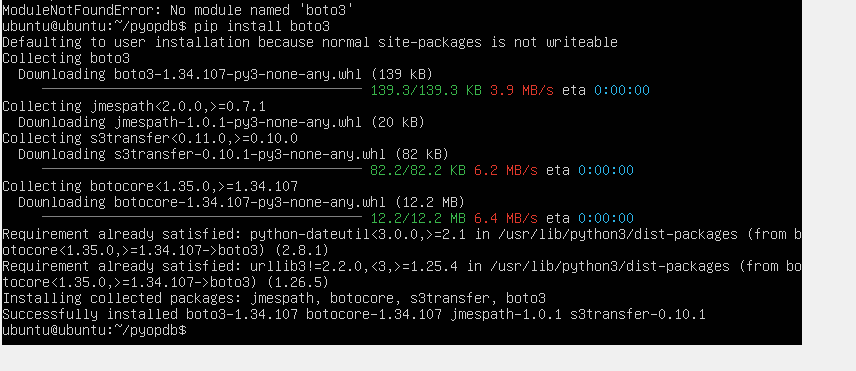
A screenshot of a computer

Description automatically generated

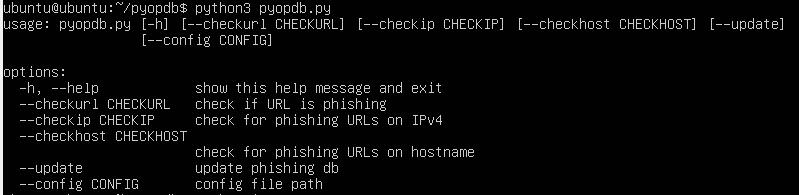
Next I cloned the GITHUB repository for Openphish (one of the data sources found from Deakin Threat Mirror research in T3 2023).



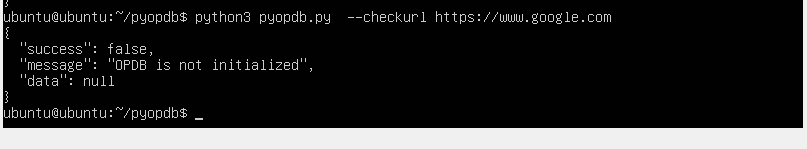
Next, I changed directory to the Openphish folder (pyopdb) and ran the program using python3



I received an error as Intelmq did not have boto3, which was required to run Openphish



Now, Openphish is running on the IntelMQ VM.



I could now use Openphish to complete tasks such as check URLs, however the application requires a key from the developers which is currently unavailable.

A screenshot of a chat

Description automatically generated

If Deakin Threat Mirror could obtain the key from the Openphish developers, it would allow for us to check the following:

Checking if a URL is a known phishing URL

Checking if an IPv4 address hosts any phishing URL

Checking if a hostname is associated with any phishing URLs