Pyimplant

Pyimplant

Writeup by: GoProSlowYo
Team: OnlyFeet
Link: https://infosecstream.github.io/

We're given python source and a "modified" compiled pyc file. We're told one has been modified and to find the difference.

Initial Research

First we decided to look at a few tools that decompile python `.pyc` files into roughly their original source code:

```
$ docker run -it -v $PWD:/chal python bash
root@737f35ee8f80:/# pip install uncompyle6 decompyle3 && cd /chal
root@737f35ee8f80:chal/# decompyle3 manipulated_tictactoe.cpython-36.pyc
Error: decompyle3 requires Python 3.7-3.8
root@737f35ee8f80:/chal# uncompyle6 manipulated_tictactoe.cpython-36.pyc >
decomp.py
root@737f35ee8f80:/chal# diff -y tictactoe.py decomp.py
root@737f35ee8f80:/chal# exit
$
```

Version Mismatches

Here you can see decompyle3 complains that it want's us to use a specific version of python and decompyle6 output decompiled code that is exactly similar to the source code provided except some `#` comments missing.

We need to do a little more research and found that first we should be using the correct version of python that the `pyc` was created with. That appears to be version 3.6. Unfortunately running that `latest` docker container gave us python 3.9 which is a bit too new.

```
$ docker run -it -v $PWD:/chal python:3.6 bash
root@be34237eefad:/# pip install uncompyle6 decompyle3 && cd /chal
root@be34237eefad:/chal# uncompyle6 manipulated_tictactoe.cpython-36.pyc >
decomp.py
root@be34237eefad:/chal# diff -y tictactoe.py decomp.py
```

Ancient History or Stegosarus Time && Victory

And again, we found no differences so time to do more research. A little googling brought us to a great resource and in it we found mention of a tool called Stegosaurus.

Stegosarus gave us the flag pretty easily:

```
root@be34237eefad:/chal# git clone
https://bitbucket.org/jherron/stegosaurus.git
Cloning into 'stegosaurus'...
Unpacking objects: 100% (18/18), 8.18 KiB | 2.73 MiB/s, done.
root@be34237eefad:/chal# python stegosaurus/stegosaurus.py -x
manipulated_tictactoe.cpython-36.pyc
Extracted payload: ALLES!{py7h0n_byt3cod3_s3cr3ts}
```

ALLES!{py7h0n_byt3cod3_s3cr3ts}