Bert Van Itterbeeck

Bert.vanitterbeeck@student.be

Ethical Hacking

Python Eindopdracht

Contents

[Modules: 2](#_Toc123578782)

[Keylogger: 2](#_Toc123578783)

[Monitor: 2](#_Toc123578784)

[Gitpyhton: 2](#_Toc123578785)

[OSDetect 2](#_Toc123578786)

[Screenshot: 2](#_Toc123578787)

[sshKeys: 3](#_Toc123578788)

[Data ophalen 3](#_Toc123578789)

[Github repository: 3](#_Toc123578790)

# Modules:

## Keylogger:

De keylogger heb ik gehaal van thepythoncode.com. Deze kan eventueel ook de keylogs versturen naar een email adres. Ik heb verschillende dingen geprobeert om deze zijn info naar github te laten zenden maar ik ben hier niet in geslaagd.

def run(\*\*args):

    keylogger = Keylogger(interval=SEND\_REPORT\_EVERY, report\_method="file")

    keylogger.start()

    time.sleep(120)

    return keylogger.\_\_str\_\_

is de code zoals ze nu gedraaid wordt. Omdat ik dacht dat een return niet uitgevoerd wordt omdat de keylogger niet afsluit. Heb ik getracht te werken met threading.

def run(\*\*args):

    keylogger = Keylogger(interval=SEND\_REPORT\_EVERY, report\_method="file")

    def returnValue(keylogger):

        print("function return started" + keylogger.\_\_str\_\_)

        return keylogger.\_\_str\_\_

    Thread(target = keylogger.start()).start()

    return Thread(target = returnValue(keylogger)).start()

Dit gaf echter ook niet het gewenste effect.

Eerdere pogingen heb ik ondernomen door gebruik te proberen te maken van variabelen, maar ook hier heb ik gefaald.

## Monitor:

De basis voor deze code heb ik gehaald van thepythoncorner.com. Ik ben hier op gestuit omdat ik een andere manier zocht om de keylog files van de vorige module door te sturen naar github. Ik stuite hier echter op dezelfde problemen als bij de keylogger. De module werkt maar enkel lokaal.

## Gitpyhton:

Mijn zeer onderhande manier om de info toch op github te krijgen. Na 90 seconden stuurt dit script de hele repo op naar git via force push! Ik besef dat dit niet echt de bedoeling is maar het werkt!

## OSDetect

Doormiddel van de python libary platform is het mogelijk om gegevens over het systeem te verkrijgen. Deze module werkt via de github-client en ook via git python. Omdat gitpython door de force push alles overschrijft heb ik gezorgd dat hier ook een file wordt aangemaakt.

## Screenshot:

Ik heb gebruik gemaakt van mss. Image wordt opgeslagen lokaal en doorgestuurd.

## sshKeys:

Kijkt op verschillende locaties of ssh sleutels gevonden kunnen worde, geeft anders terug dat dit niet het geval is.

# Data ophalen

Het script getData.py werkt wanneer de module gitpython niet gebruikt wordt. Omdat deze module alles niet geëncrypteerd doorstuurt, en het getdata script uitgaat van base64.

# Github repository:

Github link = https://github.com/vitterb/ehtroj