System Services and Activity Monitoring with Python

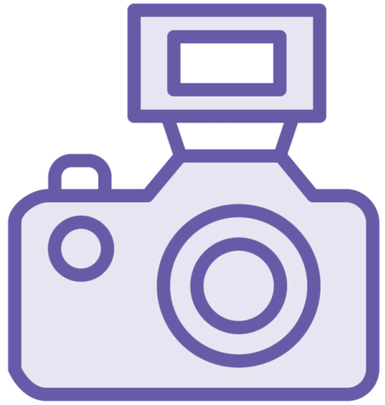
Acquiring Server Information with Python

Sean Wilkins
Network Engineer & Author

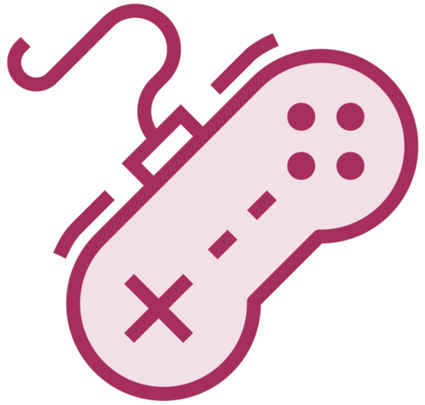
swilkins@infodispersion.com www.infodispersion.com

Course and Module Overview

Move on from Network Centric topics



This module focuses on collecting server information



Help engineers know their environment

Overview

- Setting the Stage
- Creating a Learning Environment
- Collecting Local Server Information
- Concepts Demonstration - Local Collection
- Collecting Remote Server Information
- Concepts Demonstration - Remote Collection

Globomantics

Let's set the conditions of our course's scenario

Globomantics is hiring you as one of their network security engineers

You are bringing new ideas and direction

- **Includes several Python modules**

This course focuses on common use cases

Including:

- Real environment demonstrations
  - Modules that collect information
  - Interact with MySQL and DNS servers
  - Track IP address locations
  - Monitor for abnormal behavior

Module Coverage Includes

Focus on collecting system information

Python modules: platform, psutil, and wmi

Hardware/Software versions
Processes
Utilization
Network

Once collected, can focus on potential attacks

Collecting system information allows the vulnerabilities of the system be determined

We will be using Microsoft Windows 10 Professional, Python v3.10.8, and Microsoft Visual Studio code

Windows is the main focus

Python modules and functions can be run on other OSs with modifications

Windows isn't free

Can be used in limited mode without a license

Tasks to Perform

Install Python: python.org

v3.10.8

Install Visual Studio Code

code.visualstudio.com

Mirrors common Windows install process

Need to install the Python modules once the environment is setup and installed

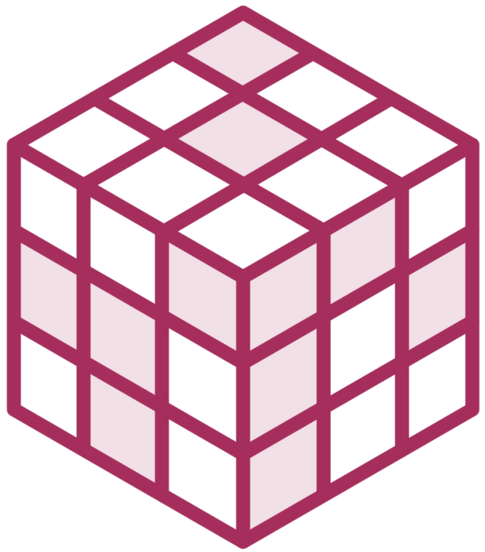
Begin at a command prompt

python –m pip install command for each module

ie: use python –m pip install platform command to install the platform module

Let’s investigate the different modules available to gather information from the local device

Python Modules



Common Python modules

Includes:

- **platform**
- **psutil**
- **Wmi**
- **winapps**

Other modules are available

Use the python pip utility to install

Platform Module

Used to access target platforms

Includes multiple data points

Systems architecture, platform, platform version/edition, python version/implementation

psutil Module

More expansive

Collects and monitors information

Displays overall and process utilization

wmi module allows the management of a device locally and remotely

Winapps module works with Windows installed applications

Security

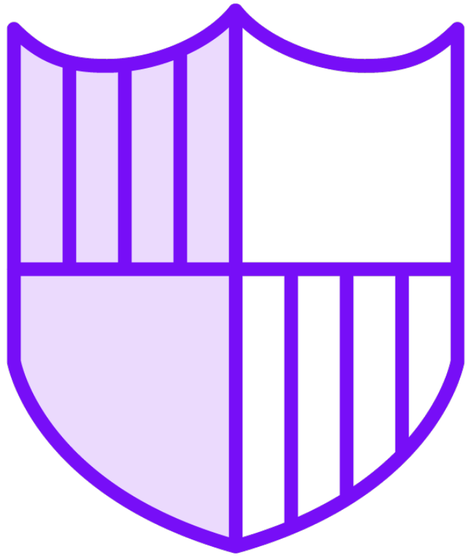
Determine what is running

Who spawned them

Resource use

Attackers can use this information to further their attack of the system

Security



Responsible for the system's security

Penetration tasks are important to maintain security

Demo

- Show *platform* module in use
- Show *psutil* module being used for processes display
- Show *psutil* module being used for utilization display
- Show *WMI* module being used
- Show *Winapps* module collecting application information

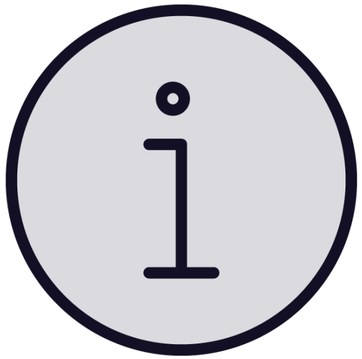
Remote Collection

Utilize Python WMI module

Connect to a remote device

Target machine must be configured to allow WMI communications

WMI



Not all systems are configured with WMI

Goal is to collect as much information as possible remotely

If enabled, helps manage the infrastructures

If not, need to gain enough access to enable

Demo

Show *WMI* module being used

Summary

- Setting the Stage
- Creating a Learning Environment
- Collecting Local Server Information
- Concepts Demonstration - Local Collection
- Collecting Remote Server Information
- Concepts Demonstration - Remote Collection