Publications

Red Team Tactics: Advanced process monitoring techniques in offensive operations

Cornelis de Plaa | March 11, 2020

In this blog post we are going to explore the power of well-known process monitoring utilities and demonstrate how the technology behind these tools can be used by Red Teams within offensive operations.

Having a good technical understanding of the systems we land on during an engagement is a key condition for deciding what is going to be the next step within an operation. Collecting and analysing data of running processes from compromised systems gives us a wealth of information and helps us to better understand how the IT landscape from a target organisation is setup. Moreover, periodically polling process data allows us to react on changes within the environment or provide triggers when an investigation is taking place.

To be able to collect detailed process data from compromised end-points we wrote a collection of process tools which brings the power of these advanced process utilities to C2 frameworks (such as Cobalt Strike).

The tools (including source) can be found here:

https://github.com/outflanknl/Ps-Tools

Windows internals system utilities

We will first explore which utilities are available for harvesting process information from a Windows computer. We can then learn how these utilities collect such information, so that we can subsequently leverage these techniques in our red teaming tools.

The Windows Operating System is equipped with many out-of-the-box utilities to administer the system. Although most of these tools would fit the purpose of basic system administration, some lack the functionality we need for more advanced troubleshooting and monitoring. The Windows task manager for example, provides us basic information about all the processes running within the system, but what if we need more detailed information like the object handles, network connections or loaded modules within a particular process?

To collect detailed information, there is more advanced tooling available. For example the system utilities within the Sysinternals suite. As a Red Team operator with a long background in network and system administration I have always been a big fan of the Sysinternals tools.

When troubleshooting a slow performing server system or a possibly infected client computer, most times I started initial troubleshooting with tools like Process Explorer or Procmon.

From a digital forensics perspective these tools are also very useful for basic dynamic analysis of malware samples and searching for artefacts on infected systems. So why are these tools so popular among system administrators as well as security professionals? Let's explore this by showing some interesting process information we can gather using the Process Explorer tool.

Using Process Explorer