INTRO TO SYSINTERNALS

Author: IaintShootinMis
Twitter | GitHub

WHAT IS SYSINTERNALS

- Created in 1996 by Mark Russinovich, CTO for Azure

- Purchased by Microsoft in 2006

- Technical resources to manage, diagnose, troubleshoot, & monitor Windows environments

- Many useful tools, 5 you should know, 2 we’ll discuss in depth

WHAT IS SYSINTERNALS

- PS Exec

- ProcDump

- ProcExplorer

- Sysmon

- ProcMon

WGET SYSINTERNALS

Two ways to use

- Download the SysInternals Suite (great for a jumpdrive)
    - Offers full suite of 32/64 bit exes

- Run from live.sysinternals.com (great for attackers)
    - Allows you to download individual files

- Don’t host it on an open fileshare, monitor the DNS and alert on the program execution using Sysmon, block the execution using AppLocker

PSExec

- Originally a Telnet replacement

- Allowed a user to execute commands on a remote system using NTLM credentials

- NTLM Credentials are cached and can be stolen from Security Account Manager (SAM) database

- DON’T DO THIS

- Deprecated, use Powershell Remote

Source: [MSDocs | PSRemoting]

ProcDump

- Used to create memory dumps and monitor CPU spikes

- Allows a user to dump memory to disk

- Monitor for procdump usage in your environment

- Used by attackers to steal passwords in memory along with LSASS

Source: [MITRE ATT&CK | OS Credential Dumping]

ProcExplorer

- Shows file locks, open directory’s, parent processes, and memory handles

- Powerful search features

- Make a part of your troubleshooting arsenal

- Two modes: DLL mode and Handle mode

Source: [MS Docs | ProcExplorer]

SYSMON

- Persistent forensic logging software

- Can monitor 25 unique event types using multiple categories, including parent.exe, file location, commandline, dns query, etc…

- Easy to install, difficult to configure

- Live Life on Easy Mode, Prebuilt configs
Source: [GitHub | IAintShootinMis]

Exercise #1: SYSMON Installation

1) Download sysmon64.exe and sysmon-config.xml

2) Open an admin powershell prompt

3) Navigate to the sysmon64.exe file location

4) Run `.\sysmon64.exe -accepteula -i .\PathTo\sysmon-config.xml`

5) Run `eventvwr.exe`

6) Navigate to `Application and Services > Microsoft > Windows > Sysmon > Operational`

7) Congrats! You installed Sysmon! Now do it again for all your computers!

ProcMon

- Real-time Logging of File System access, registry activity, process/thread activity, network,

- Overwhelming and immediate insight into kernel level system calls

- Non-destructive filtering allows you to filter on any number of event properties

- Can be used for forensics, troubleshooting, etc…

Source: [AdamTheAutomator | ProcMon]

ProcMon Gotchas

- Launching ProcMon immediately starts the event logger with no filters.
  - This can quickly overwhelm a system.

- Launch from command line with the `/NoConnect` flag to prevent capturing on launch or press `CTRL+E`

- Missing events? Clear the filter
  - Press `CTRL+L` and remove any filters you've added

Exercise #2: ProcMon Capture

- Launch from command line with the /NoConnect flag
- Begin capturing by pressing CTRL+E
- Count to 5
- Stop capturing by pressing CTRL+E
- Look through the Operations available

  All these can be filtered on!
- Note the sheer volume of logs collected

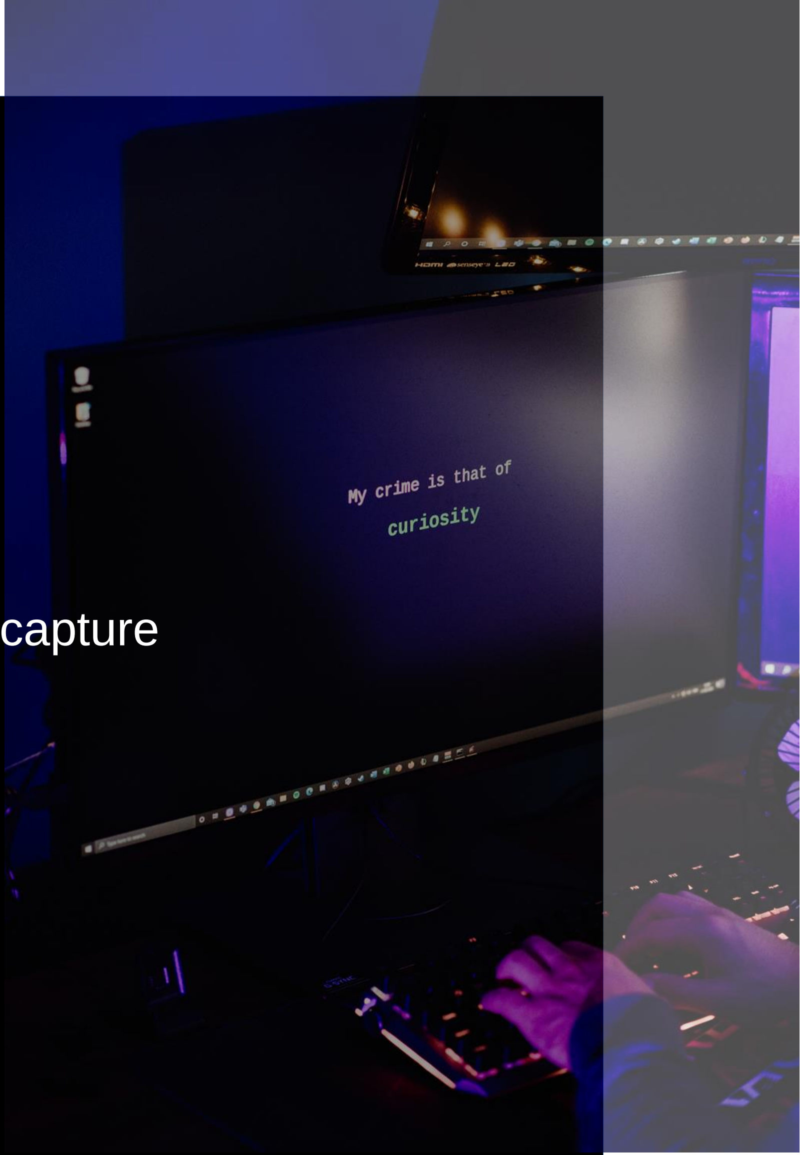
  These are all held in memory

  Move them by selecting File > Backing Files

Missing events? Clear the filter

- Press CTRL+L and remove any filters you've added

Exercise #3: ProcMon Filtering



- Press CTRL+L and create a filter of Operation is LockFile
- Click Add and Apply
- We now have a list of all files that were locked during our capture

Why might this be helpful information?

Missing events? Clear the filter

- Press CTRL+L and remove any filters you've added

Exercise #4: ProcMon Configurations

- Press FILE and select Export Configuration
- Name the file and click save
- We now have a list of all filters we’ve used on our capture

Note: We can import the same way!

Why might this be helpful?
- We now have a fast and easy way to share Indicators of Compromise and other common troubleshooting identifiers

Exercise #5: ProcMon Export

Three ways to Export Events
- All Events (Perfect for forensics, establishing admissible evidence), pairs well with an exported filter
- Selected Events (Great for sharing with peers/others where chain of evidence isn’t necessary)
- Highlighted Events (only the selected events, can ctrl click)

Three file types
- PML – Native ProcMon format, can be opened with ProcMon
- CSV – Comma Separated Values, can be opened with everything
- XML – Extensible Markup Lang, can transport additional information

Exercise #5: ProcMon Export

- Press FILE and select Save
- Choose which events and file type to save
- We now have a list of all events we’ve captured and filtered!

Note: We can import these files, share them with others, and import the configs we used!

Exercise #6: ProcMon Filtered Capture

- Apply any desired filters before capturing
- Click FILTER and select DROP FILTERED EVENTS
- Start capture as normal

- Only *destructive* filtering option, events immediately purged from memory, irrecoverable
- Great for long running captures when we know exactly what we're looking for
- This isn't recommended for troubleshooting, forensics, or evidence collection

Sources:

Shout out to AdamTheAutomator for his wonderful Sysmon walkthrough

https://adamtheautomator.com/procmon/

Check out the section of his post. Pay special attention to the section titled “Real-World Examples” as well as his guide to more advanced features.

Twitter: @Adbertram
And @SwiftOnSecurity for the maintenance of a beautiful sysmon configuration

Photo credit to Anete Lusina on Pexels