

# Forum:[Hack Forums](#)

Thread: [Monitor all activity on operating system](#)

**BlvckGod** - December 28, 2016, 8:30 pm

How would I check the activity of an operating system?

For example, if I moved a mouse, or if I opened an application. Does the computer keep track of all these things? If so how do I access it?

**Malum™** - December 28, 2016, 8:36 pm

You would have to individually monitor everything. The easier one to start with would probably be [FileSystemWatcher](#). Then moving on to [detecting mouse and key input](#). You could run a loop checking with the [Process Library](#) for new processes and windows. The lists goes on from there. Best of luck! There might be better ways (I guarantee it) but these are the only ones I know to get you started.

**BlvckGod** - December 28, 2016, 8:46 pm

(Dec 28, 2016 09:36 PM)Malum™ Wrote: [\[CITE\]](#) You would have to individually monitor everything. The easier one to start with would probably be [FileSystemWatcher](#). Then moving on to [detecting mouse and key input](#). You could run a loop checking with the [Process Library](#) for new processes and windows. The lists goes on from there. Best of luck! There might be better ways (I guarantee it) but these are the only ones I know to get you started.

Does CMD provide this sort of thing? Like a live feed of computer activity

**Malum™** - December 28, 2016, 8:56 pm

(Dec 28, 2016 09:46 PM)BlvckGod Wrote: [\[CITE\]](#) Does CMD provide this sort of thing? Like a live feed of computer activity

Not to my knowledge. All CMD does is:

"Command Prompt is used to execute entered commands. Most of those commands are used to automate tasks via scripts and batch files, perform advanced administrative functions, and troubleshoot and solve certain kinds of Windows issues."

- [Source](#)

**hfTP54** - January 1, 2017, 8:34 pm

The event log can be partially helpful. You will still have to hook keyboard and mouse but you can pull a lot from the elog like errors, info, logs etc.

**Malum™** - January 1, 2017, 10:09 pm

(Jan 1, 2017 09:34 PM)hfTP54 Wrote: [\[CITE\]](#) The event log can be partially helpful. You will still have to hook keyboard and mouse but you can pull a lot from the elog like errors, info, logs etc.

Just learned about [EventLogs](#). They can be pretty useful. Good luck OP!

**Wh1t3\_Tr4sH\_G0D** - January 1, 2017, 10:11 pm

I know that in the metasploit meterpreter shell, the 'clearev' commands clears evidence. Hey... Thats pretty good!

**Malum™** - January 1, 2017, 10:13 pm

(Jan 1, 2017 11:11 PM)Wh1t3\_Tr4sH\_G0D Wrote: [\[CITE\]](#) I know that in the metasploit meterpreter shell, the 'clearev' commands clears evidence. Hey... Thats pretty good!

[https://msdn.microsoft.com/en-us/library/system.diagnostics.eventlog.clear\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/system.diagnostics.eventlog.clear(v=vs.110).aspx)  
<https://support.microsoft.com/en-us/kb/814564>

You don't even need metasploit :P