Introduction:

SysProt AntiRootkit is a free tool to detect and remove rootkits. Currently, SysProt AntiRootkit supports Windows **2000/XP/2003/Vista 32-bit** operating systems. Some of the key features of the tool are:

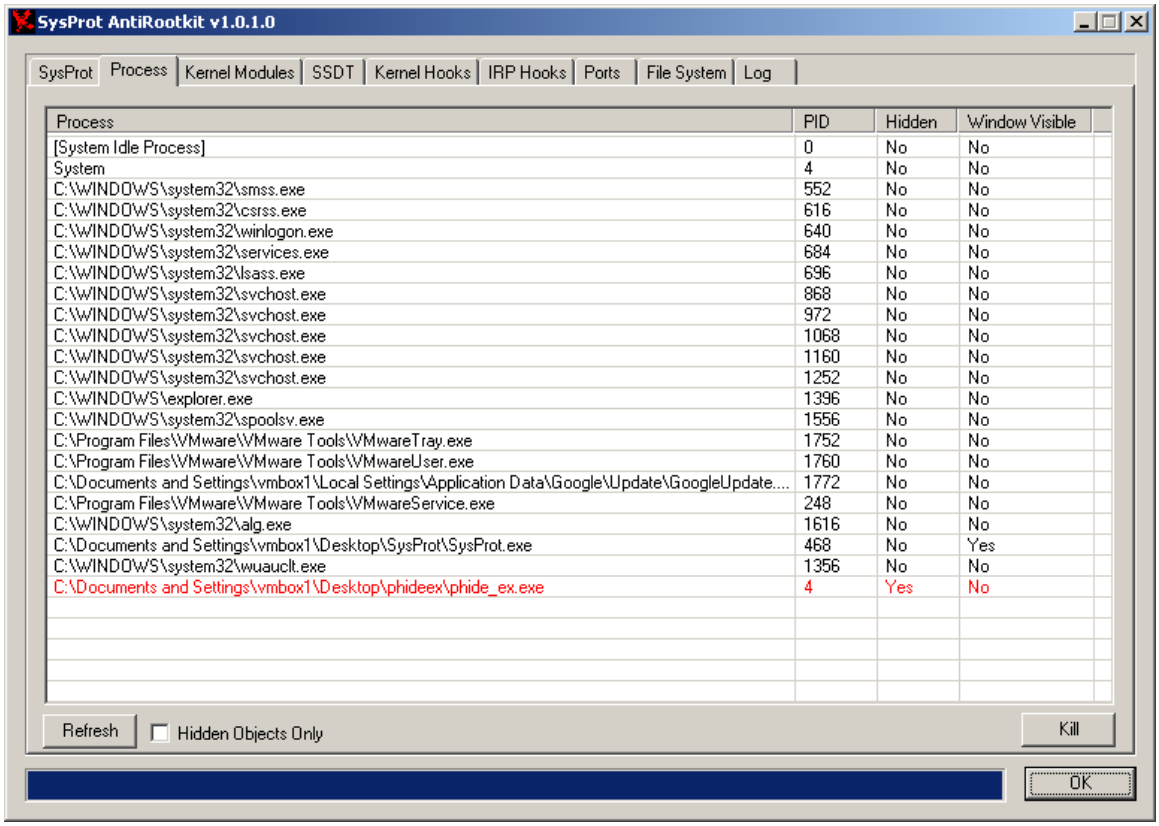
- Hidden process detection and removal
- Hidden driver detection and removal
- SSDT hooks detection and removal
- Kernel inline hooks detection and removal
- Sysenter hook detection
- TCP/UDP ports information
- Hidden/locked files detection and removal

Usage:

SysProt AntiRootkit requires Admin privileges to run. The various tabs present in SysProt AntiRootkit and their usage are as follows:

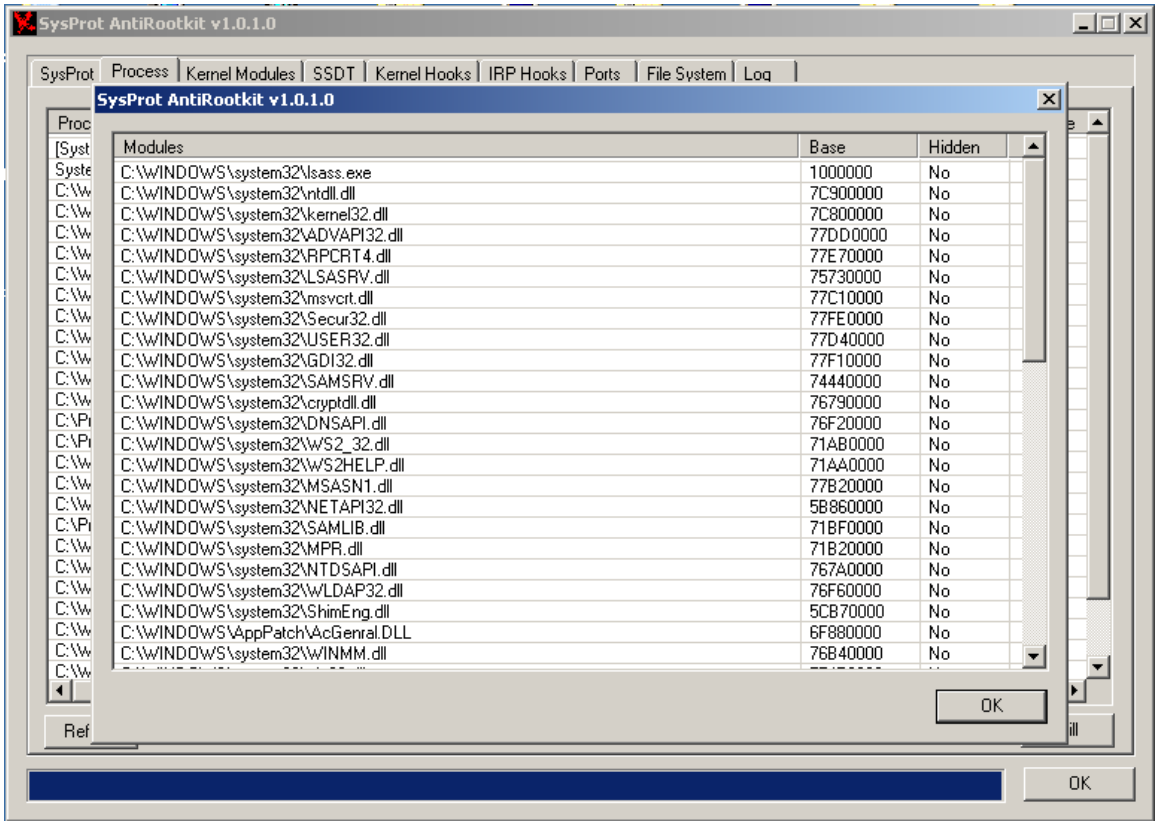
Process:

The “Process” tab displays all running processes in the system. Hidden (rooted) processes are shown in red color. Select the “Hidden Objects Only” checkbox to display only hidden processes. To kill a process, click and select that particular process and then click “Kill” button.



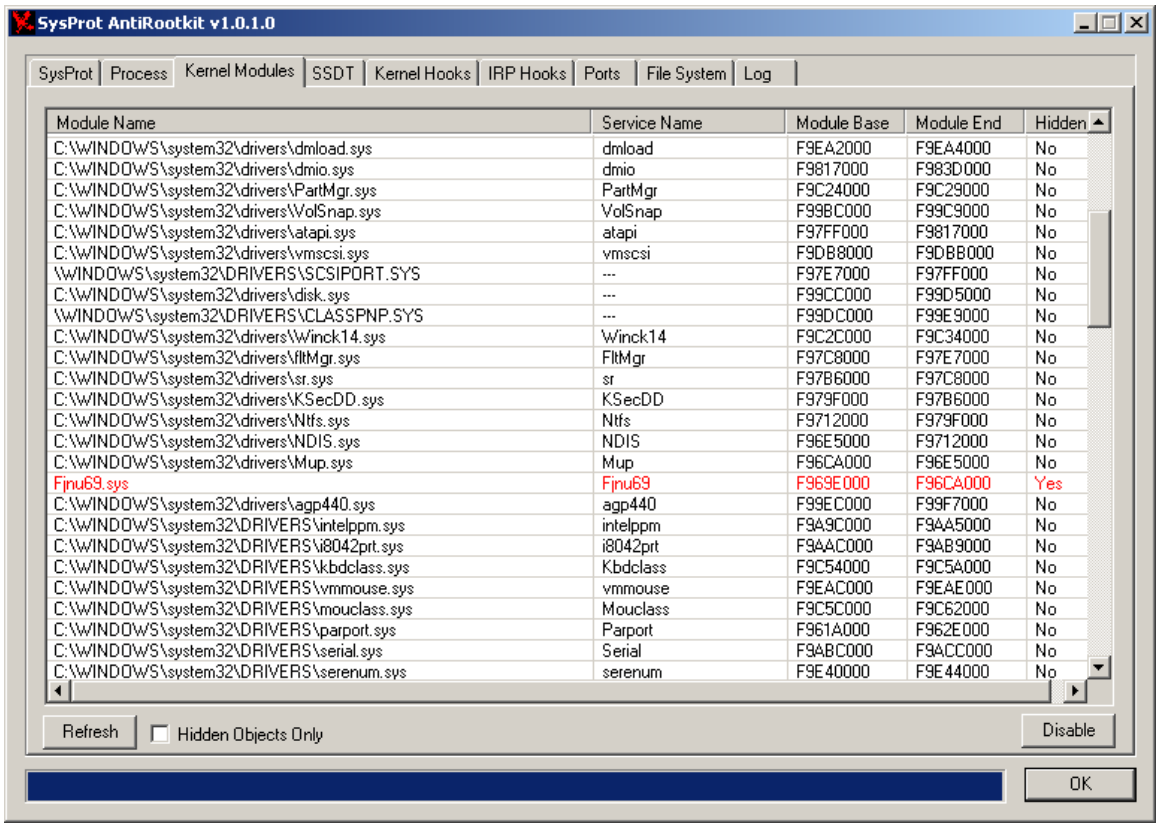
Modules:

Double-clicking on a process in “Process” tab will bring another window that shows DLLs loaded by that process. Again, a hidden DLL is shown in red color.



Kernel Modules:

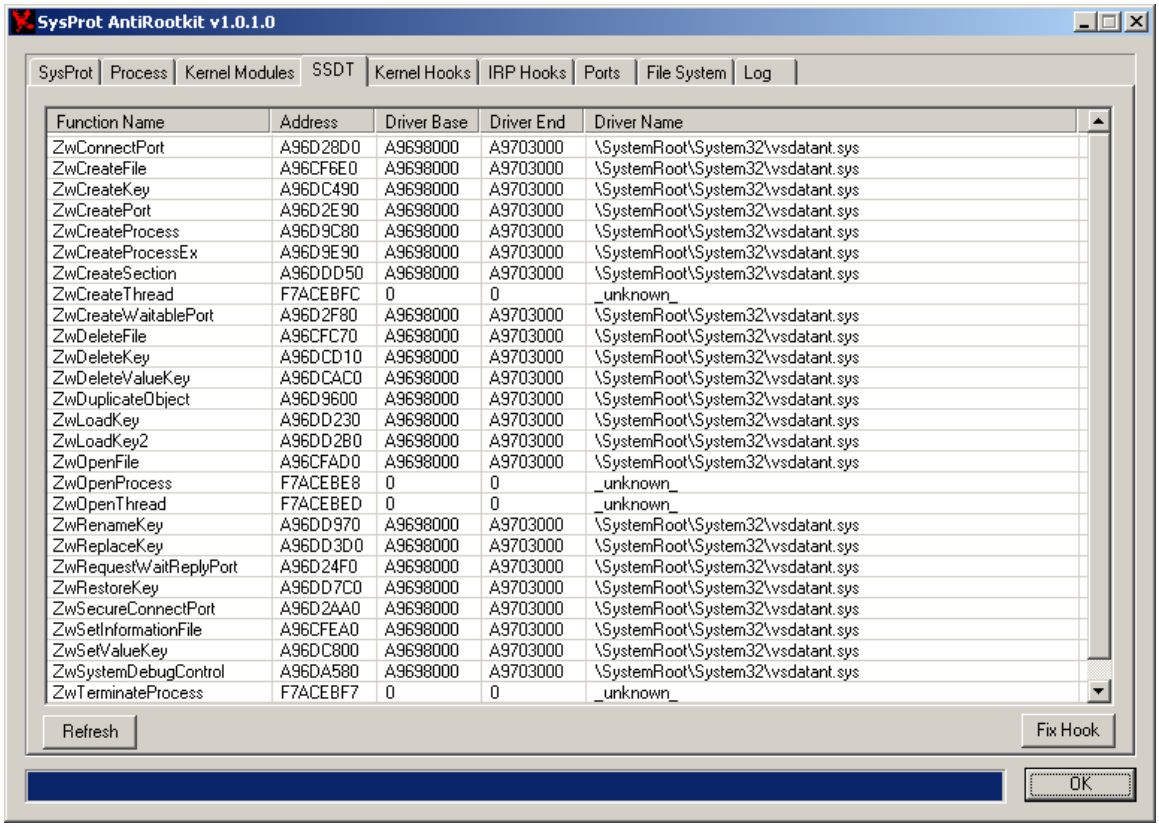
The “Kernel Modules” tab displays all device drivers loaded in memory. Hidden drivers are shown in red color. Select the “Hidden Objects Only” checkbox to display only hidden drivers. To disable a driver, select that particular driver and click “Disable” button. The system needs to be restarted to make the changes take effect.



Note: SysProt AntiRootkit may show few drivers such as dump_atapi.sys, dump_wmilib.sys and dump_iaStor.sys in red color. These are false positives. These drivers are not malicious and do not belong to any rootkit component. SysProt AntiRootkit is showing them as “hidden” because those drivers are not present on disk. They are present only in memory.

SSDT:

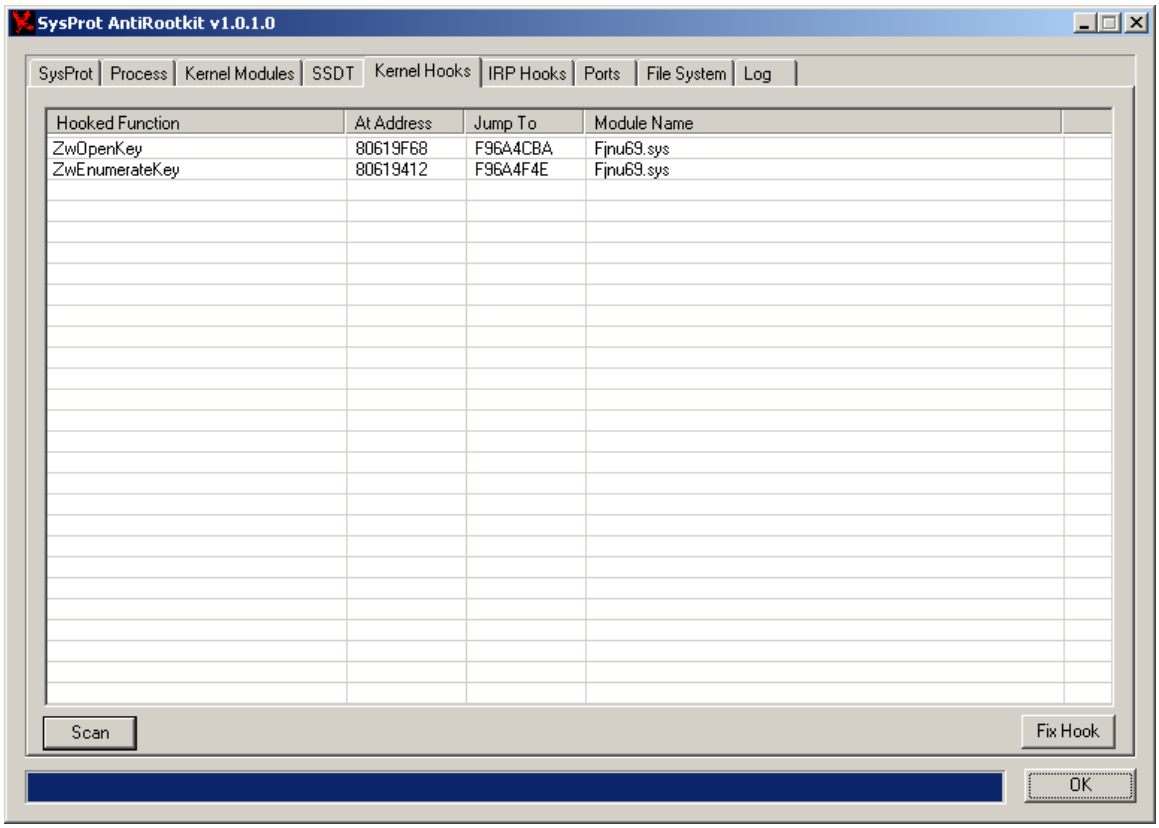
The “SSDT” tab shows the SSDT hooks installed by various drivers. If there are no SSDT hooks, then this list will be empty. To remove a hook, select that hook and click “Fix Hook” button.



Function Name	Address	Driver Base	Driver End	Driver Name
ZwConnectPort	A96D28D0	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwCreateFile	A96CF6E0	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwCreateKey	A96DC490	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwCreatePort	A96D2E90	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwCreateProcess	A96D9C80	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwCreateProcessEx	A96D9E90	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwCreateSection	A96DDD50	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwCreateThread	F7ACEBFC	0	0	_unknown_
ZwCreateWaitablePort	A96D2F80	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwDeleteFile	A96CFC70	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwDeleteKey	A96DCD10	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwDeleteValueKey	A96DCAC0	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwDuplicateObject	A96D9600	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwLoadKey	A96DD230	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwLoadKey2	A96DD2B0	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwOpenFile	A96CFAD0	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwOpenProcess	F7ACEBE8	0	0	_unknown_
ZwOpenThread	F7ACEBED	0	0	_unknown_
ZwRenameKey	A96DD970	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwReplaceKey	A96DD3D0	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwRequestWaitReplyPort	A96D24F0	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwRestoreKey	A96DD7C0	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwSecureConnectPort	A96D2AA0	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwSetInformationFile	A96CFEA0	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwSetValueKey	A96DC800	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwSystemDebugControl	A96DA580	A9698000	A9703000	\SystemRoot\System32\vsdatant.sys
ZwTerminateProcess	F7ACEBF7	0	0	_unknown_

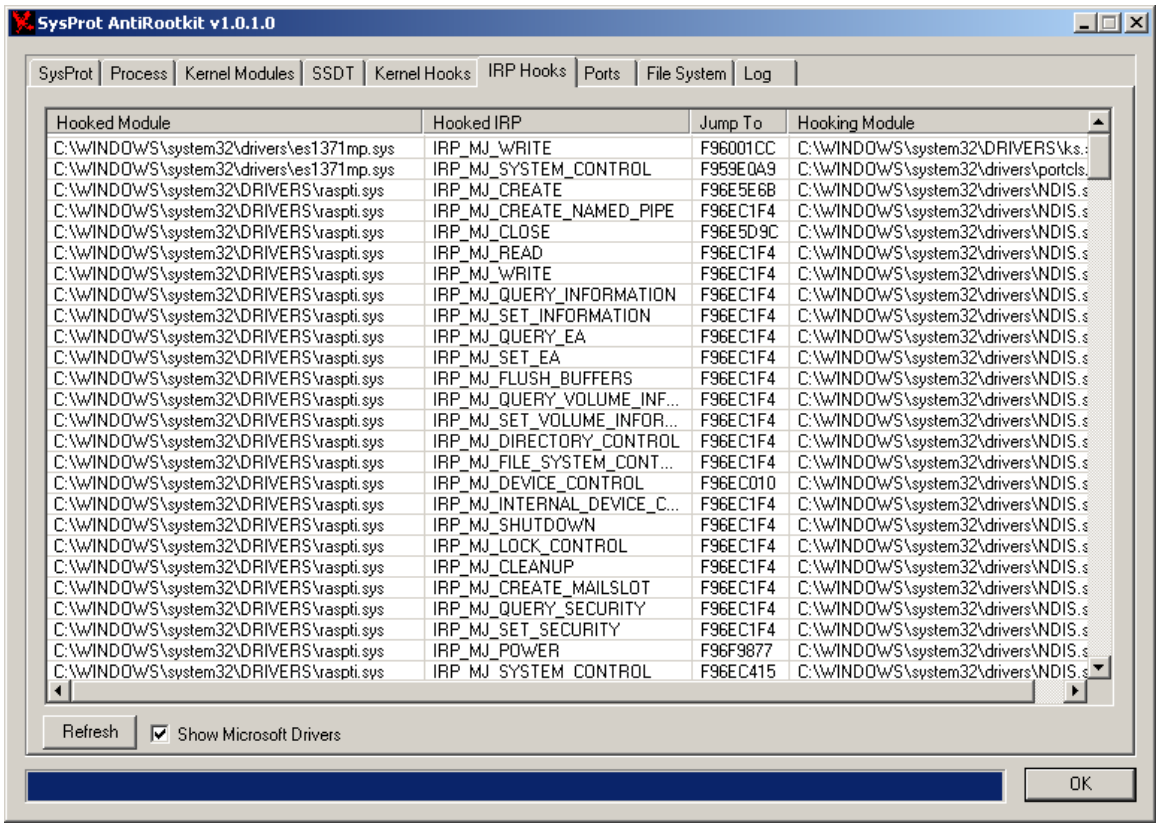
Kernel Hooks:

The “Kernel Hooks” tab shows inline hooks that may be present in NT kernel and also the Sysenter hook. Since this scan takes slightly longer duration, SysProt AntiRootkit does not automatically start scanning when this tab is clicked. Scanning can be started by clicking on “Scan” button. If there are no kernel-inline hooks or Sysenter hook, then this list will be empty. To remove a kernel inline hook, select that hook and click “Fix Hook” button.



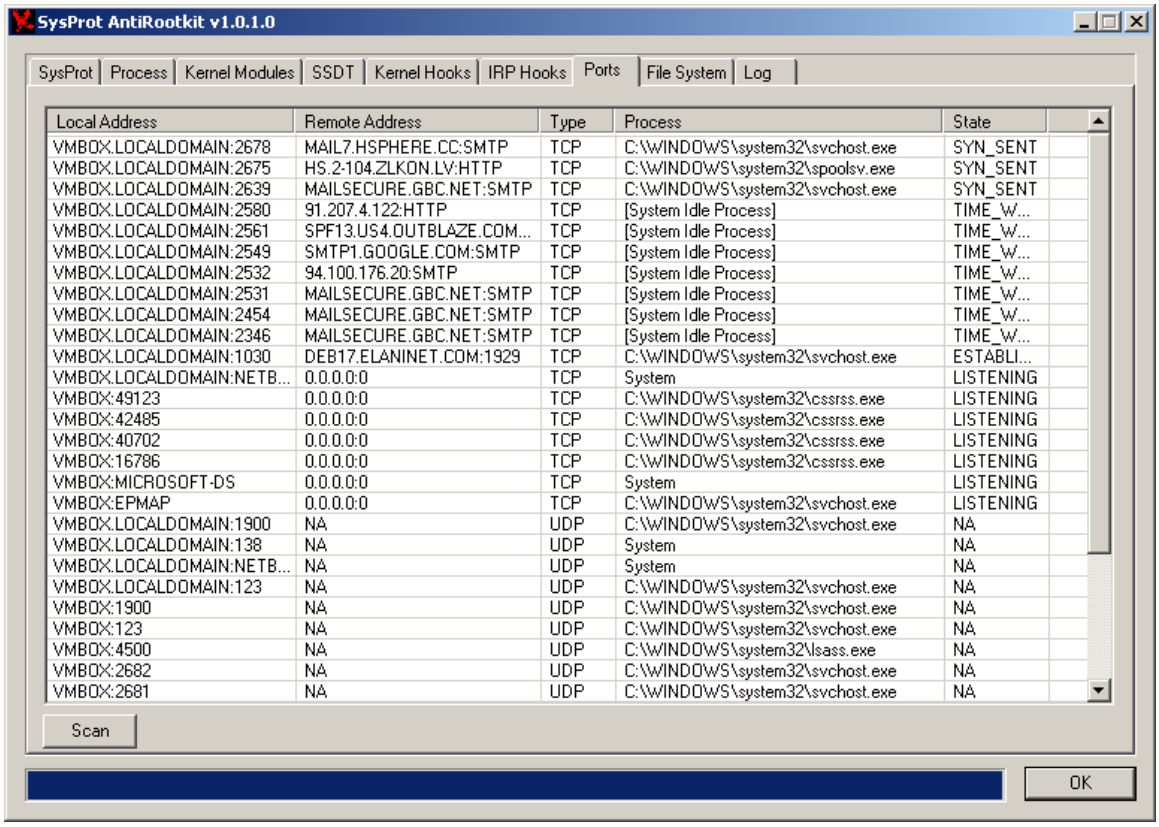
IRP Hooks:

The “IRP Hooks” tab shows hooked IRP major functions. Since many legitimate Microsoft Windows files install IRP hooks, only hooks installed by non-Microsoft files are shown. All hooks (even the ones installed by Microsoft files) can be seen by selecting “Show Microsoft Drivers” checkbox. If there are no IRP hooks, then this list will be empty.



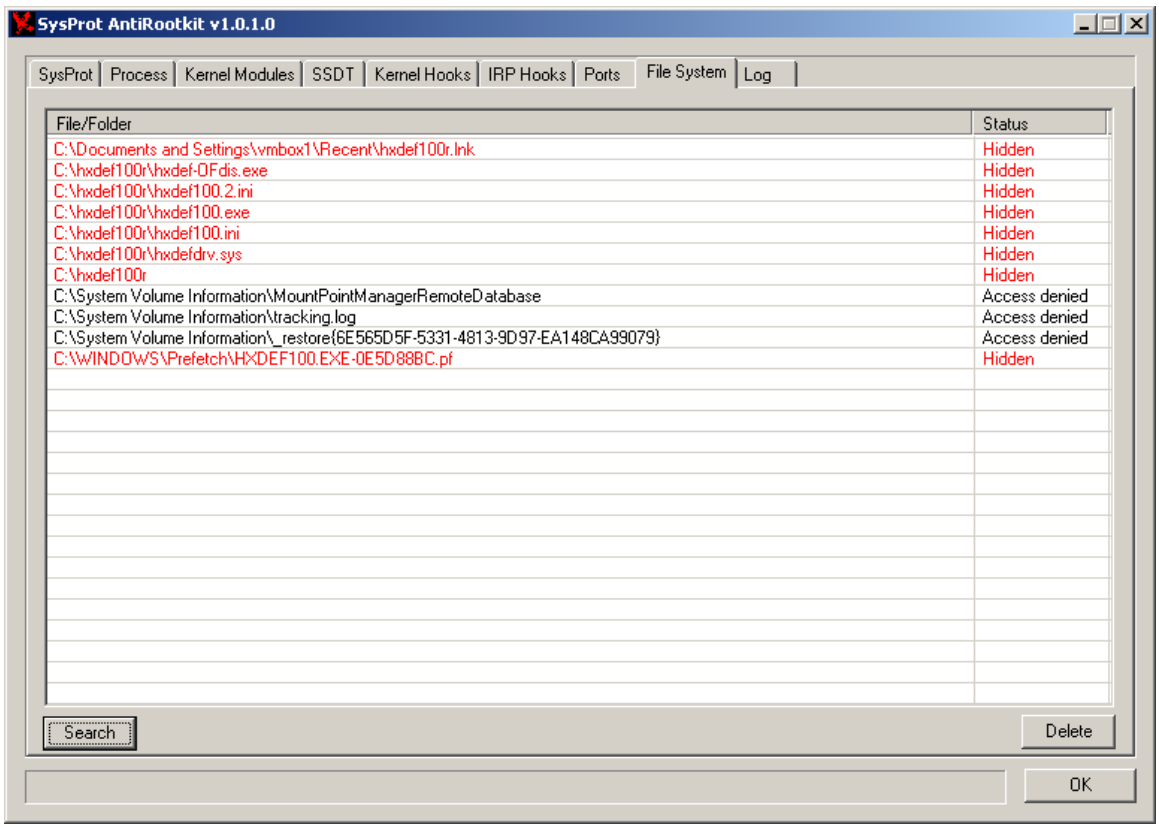
Ports:

The “Ports” tab displays all TCP and UDP ports/endpoints that are opened by various processes. Sometimes ports scan takes longer duration; hence SysProt AntiRootkit does not automatically start scanning when this tab is selected. Scanning can be started by clicking “Scan” button.



File System:

The “File System” tab searches for hidden files and folders in the system. Scanning can be started by clicking “Search” button. All the hidden and locked files are displayed when the scan completes. A file or folder can be deleted by selecting its entry and clicking “Delete” button.



Log:

The “Log” tab aggregates the information from all of tabs listed above, and writes it to a file. The log file is created in the same directory where SysProt AntiRootkit executable is located.

Operating Systems:

SysProt AntiRootkit has been tested on following 32-bit operating systems:
Windows 2000 Service Pack 4
Windows XP Service Pack 1, Service Pack 2 and Service Pack 3
Windows 2003 Service Pack 1 and Service Pack 2
Windows 2003 R2 Service Pack 1 and Service Pack 2
Windows Vista Service Pack 1

Download:

The latest version, **SysProt AntiRootkit v1.0.1.0**, can be downloaded from the following website:
http://sites.google.com/site/sysprotantirootkit/
http://swatrant.blogspot.com/