

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:

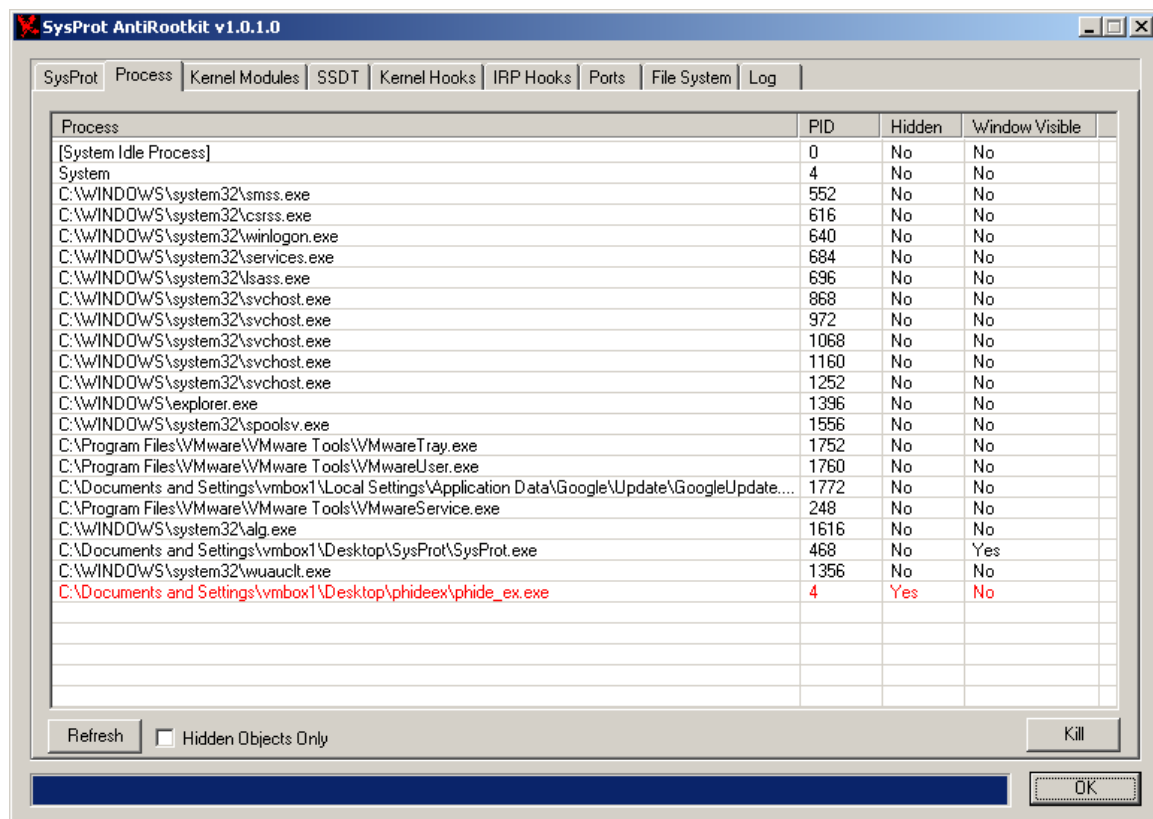
- Hidden process detection and removal
- Hidden driver detection and removal
- SSDT hooks detection and removal
- Kernel inline hooks detection and removal
- Sysenter hook detection
- TCP/UDP ports information
- Hidden/locked files detection and removal

Usage:

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

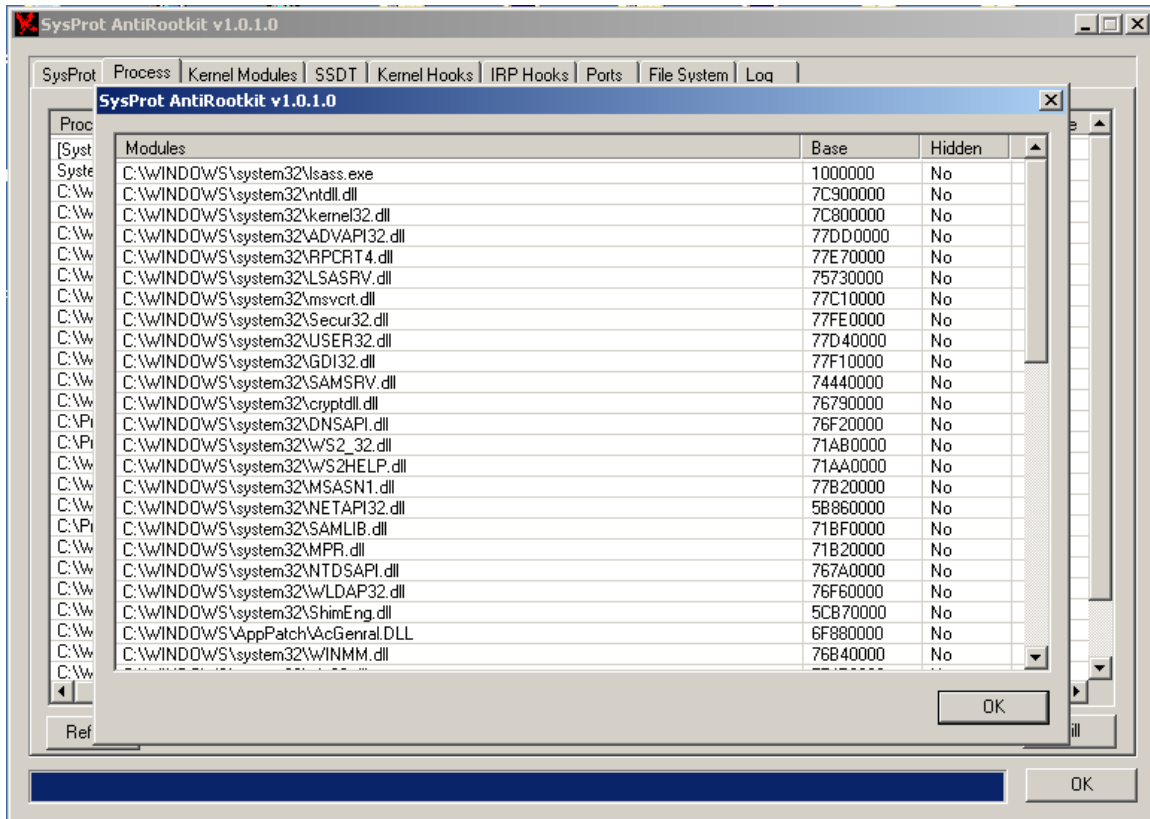
Process:

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.



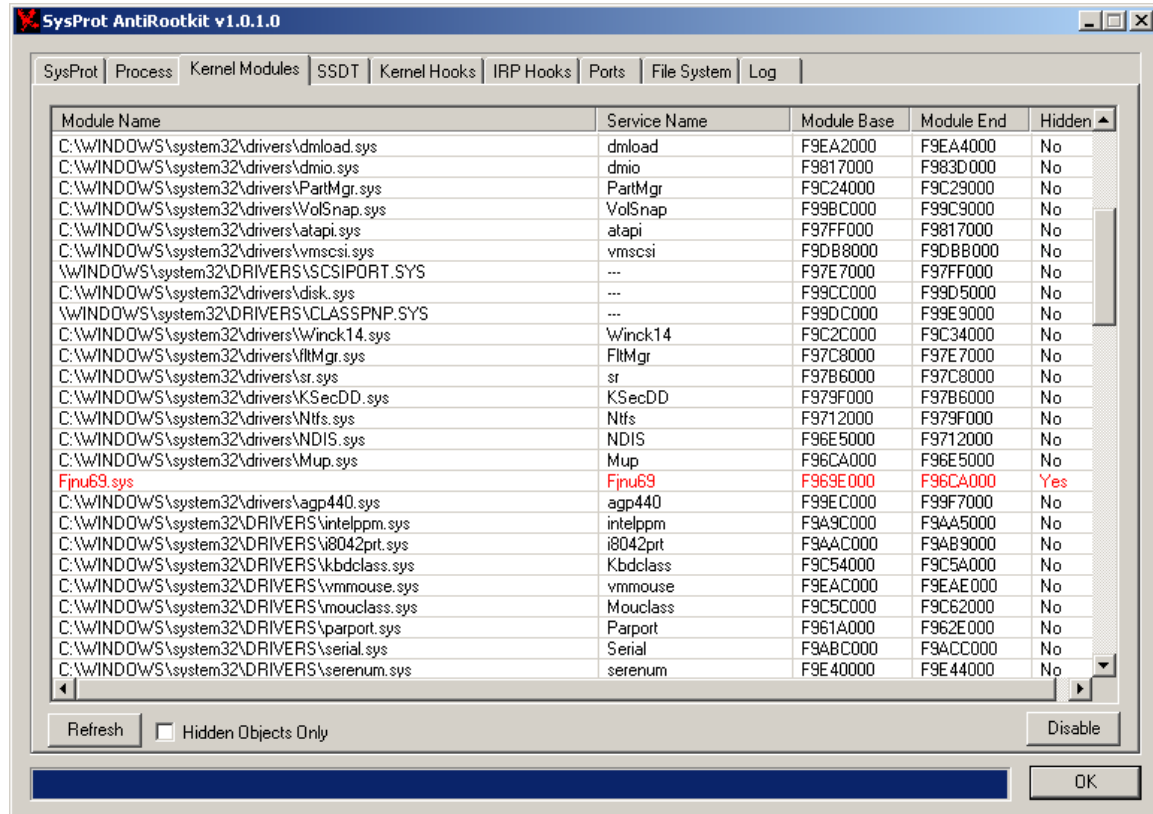
Modules:

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.



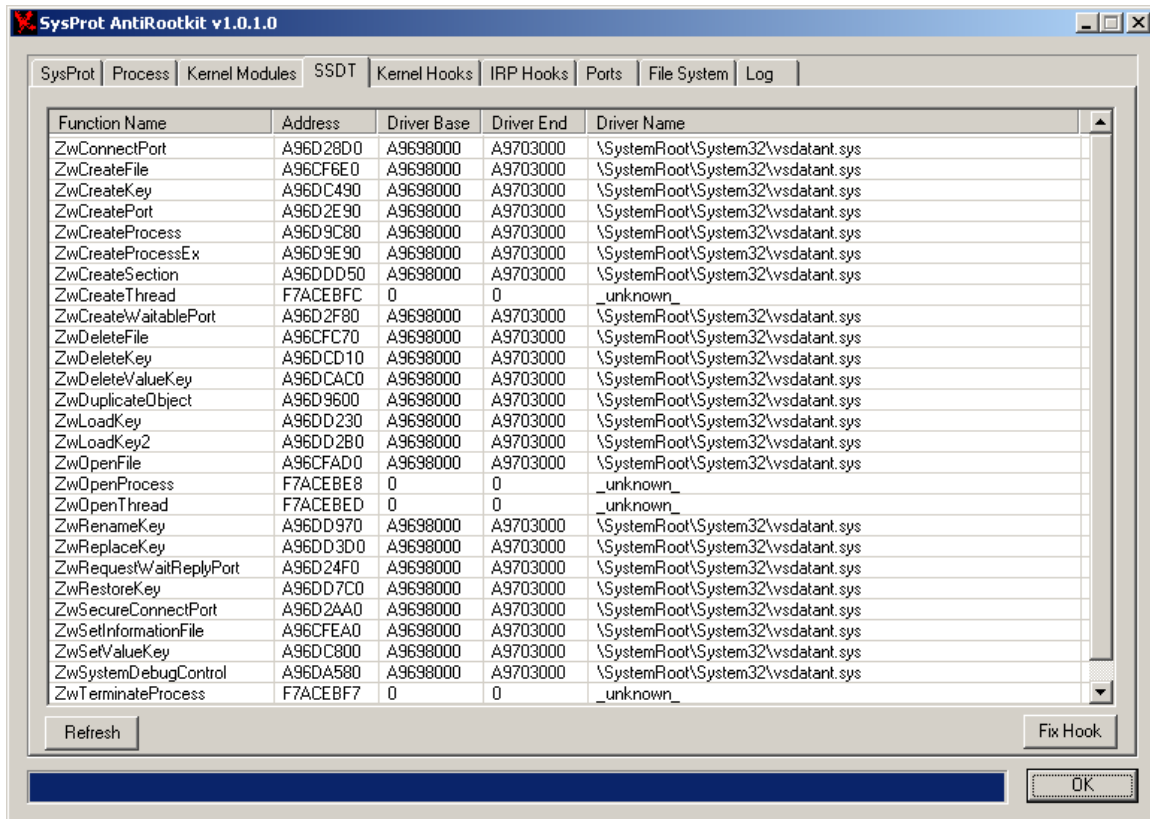
Module Name	Service Name	Module Base	Module End	Hidden
C:\WINDOWS\system32\drivers\dmload.sys	dmload	F9EA2000	F9EA4000	No
C:\WINDOWS\system32\drivers\dmio.sys	dmio	F9817000	F983D000	No
C:\WINDOWS\system32\drivers\PartMgr.sys	PartMgr	F9C24000	F9C29000	No
C:\WINDOWS\system32\drivers\VolSnap.sys	VolSnap	F99B0000	F99C9000	No
C:\WINDOWS\system32\drivers\atapi.sys	atapi	F97FF000	F9817000	No
C:\WINDOWS\system32\drivers\vm SCSI.sys	vm SCSI	F9DB8000	F9DBB000	No
C:\WINDOWS\system32\DRIVERS\SCSI\PORT.SYS	---	F97E7000	F97FF000	No
C:\WINDOWS\system32\drivers\disk.sys	---	F99CC000	F99D5000	No
C:\WINDOWS\system32\DRIVERS\CLASSPNP.SYS	---	F99DC000	F99E9000	No
C:\WINDOWS\system32\drivers\Winck14.sys	Winck14	F9C2C000	F9C34000	No
C:\WINDOWS\system32\drivers\FltMgr.sys	FltMgr	F97C8000	F97E7000	No
C:\WINDOWS\system32\drivers\sr.sys	sr	F97B6000	F97C8000	No
C:\WINDOWS\system32\drivers\KSecDD.sys	KSecDD	F979F000	F97B6000	No
C:\WINDOWS\system32\drivers\Ntfs.sys	Ntfs	F9712000	F979F000	No
C:\WINDOWS\system32\drivers\NDIS.sys	NDIS	F96E5000	F9712000	No
C:\WINDOWS\system32\drivers\Mup.sys	Mup	F96CA000	F96E5000	No
Fjnu69.sys	Fjnu69	F969E000	F96CA000	Yes
C:\WINDOWS\system32\drivers\agp440.sys	agp440	F99EC000	F99F7000	No
C:\WINDOWS\system32\DRIVERS\intelppm.sys	intelppm	F9A9C000	F9AA5000	No
C:\WINDOWS\system32\DRIVERS\i8042prt.sys	i8042prt	F9AAC000	F9AB9000	No
C:\WINDOWS\system32\DRIVERS\kbdclass.sys	Kbdclass	F9C54000	F9C5A000	No
C:\WINDOWS\system32\DRIVERS\vmouse.sys	vmouse	F9EAC000	F9EAE000	No
C:\WINDOWS\system32\DRIVERS\mouclass.sys	Mouclass	F9C5C000	F9C62000	No
C:\WINDOWS\system32\DRIVERS\parport.sys	Parport	F961A000	F962E000	No
C:\WINDOWS\system32\DRIVERS\serial.sys	Serial	F9ABC000	F9ACC000	No
C:\WINDOWS\system32\DRIVERS\serenum.sys	serenum	F9E40000	F9E44000	No

Refresh ☐ Hidden Objects Only Disable OK

Note: SysProt AntiRootkit may show few drivers such as dump_atapi.sys, dump_wmlib.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.

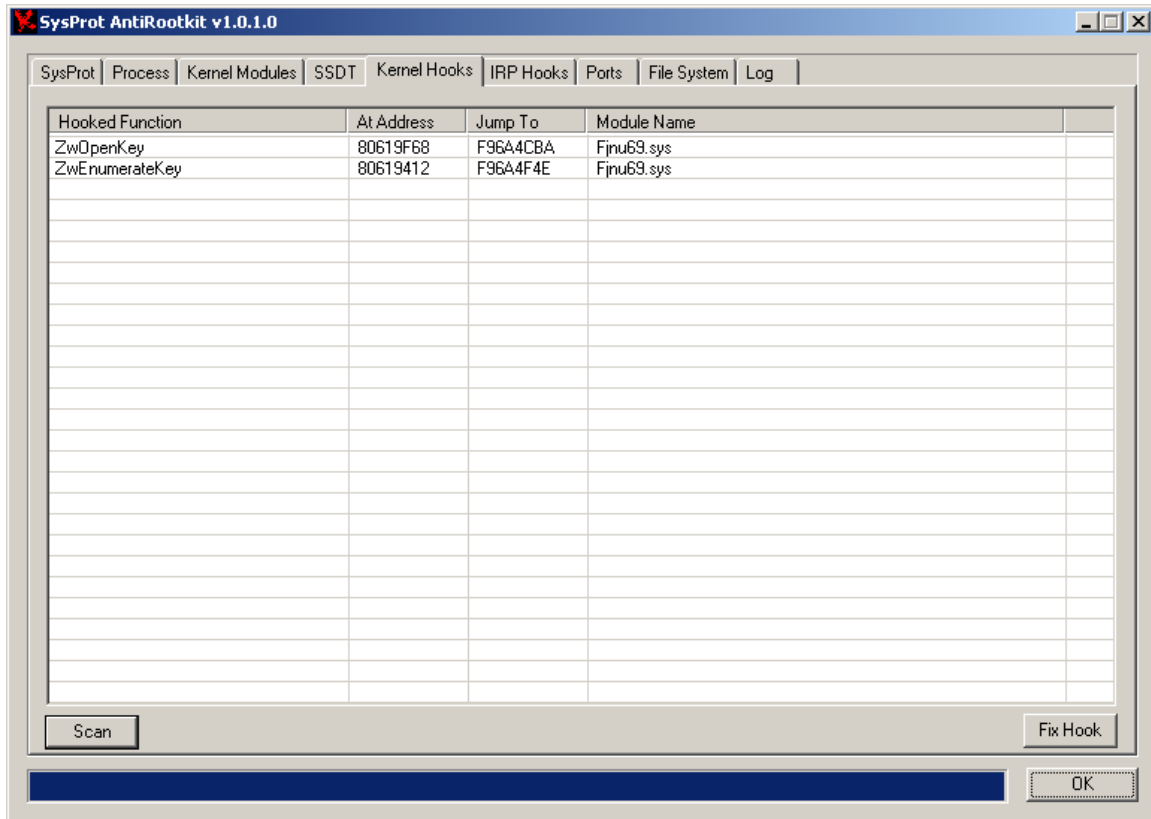
SSDT:

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.



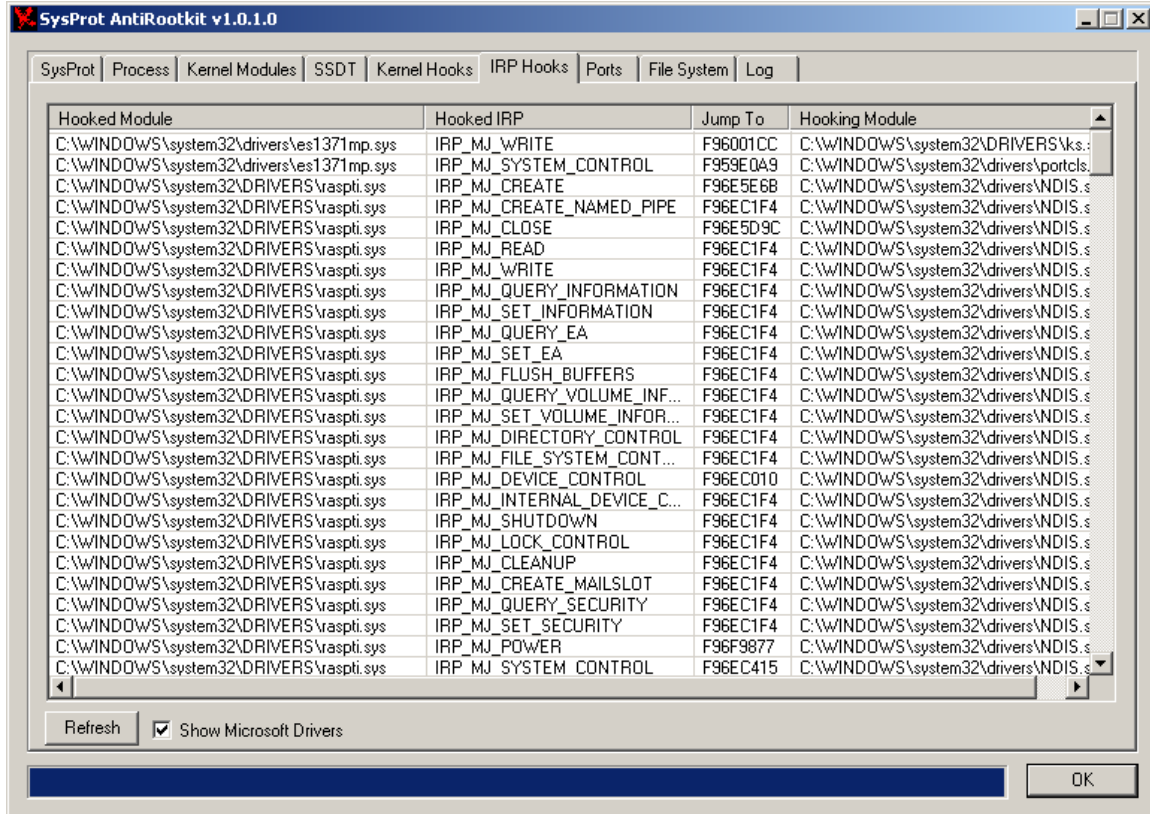
Kernel Hooks:

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:

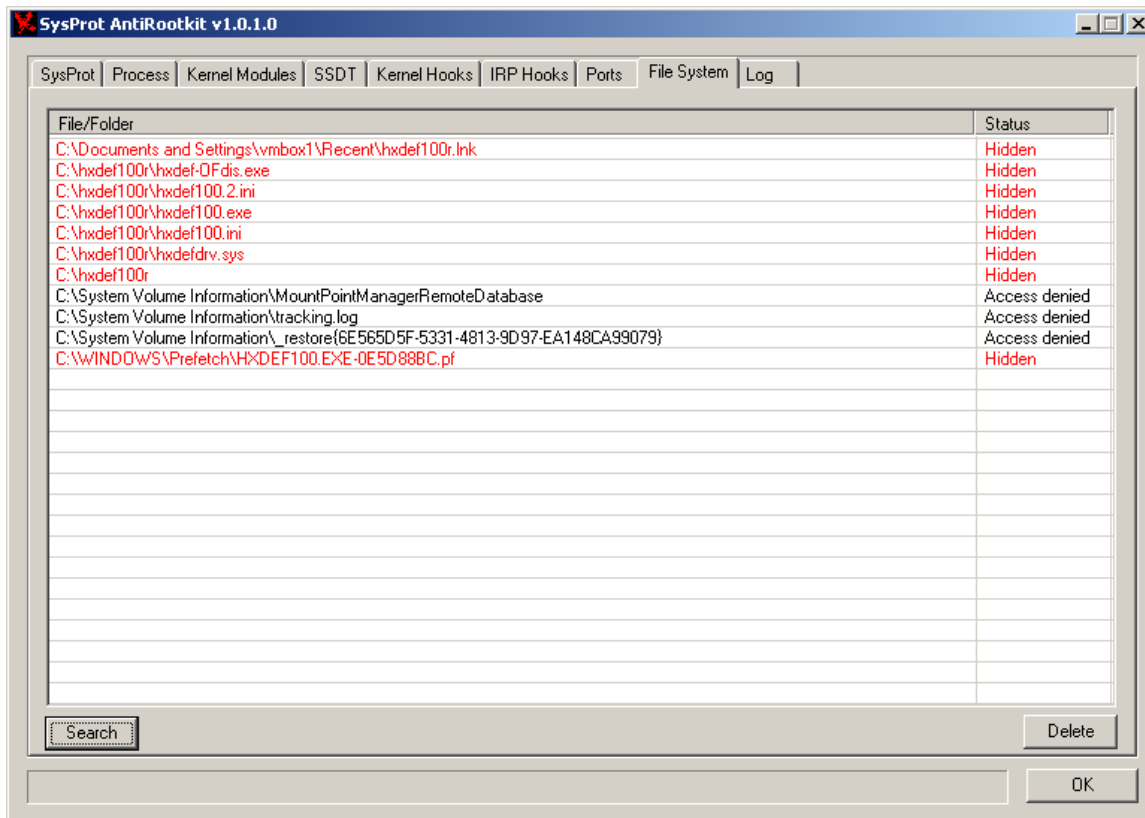
The "Ports" tab displays all TCP and UDP ports/endpoints that are opened by various processes. Sometimes ports scan takes longer duration; hence SysProt AntiRootkit does not automatically start scanning when this tab is selected. Scanning can be started by clicking "Scan" button.

The screenshot shows the SysProt AntiRootkit v1.0.1.0 application window. The 'Ports' tab is selected in the top navigation bar. The main area displays a table of network connections. Below the table is a 'Scan' button and an 'OK' button.

Local Address	Remote Address	Type	Process	State
VMBOX.LOCALDOMAIN:2678	MAIL7.HSPHERE.CC:SMTP	TCP	C:\WINDOWS\system32\svchost.exe	SYN_SENT
VMBOX.LOCALDOMAIN:2675	HS.2-104.ZLKON.LV:HTTP	TCP	C:\WINDOWS\system32\spoolsv.exe	SYN_SENT
VMBOX.LOCALDOMAIN:2639	MAILSECURE.GBC.NET:SMTP	TCP	C:\WINDOWS\system32\svchost.exe	SYN_SENT
VMBOX.LOCALDOMAIN:2580	91.207.4.122:HTTP	TCP	[System Idle Process]	TIME_W...
VMBOX.LOCALDOMAIN:2561	SPF13.US4.OUTBLAZE.COM...	TCP	[System Idle Process]	TIME_W...
VMBOX.LOCALDOMAIN:2549	SMTP1.GOOGLE.COM:SMTP	TCP	[System Idle Process]	TIME_W...
VMBOX.LOCALDOMAIN:2532	94.100.176.20:SMTP	TCP	[System Idle Process]	TIME_W...
VMBOX.LOCALDOMAIN:2531	MAILSECURE.GBC.NET:SMTP	TCP	[System Idle Process]	TIME_W...
VMBOX.LOCALDOMAIN:2454	MAILSECURE.GBC.NET:SMTP	TCP	[System Idle Process]	TIME_W...
VMBOX.LOCALDOMAIN:2346	MAILSECURE.GBC.NET:SMTP	TCP	[System Idle Process]	TIME_W...
VMBOX.LOCALDOMAIN:1030	DEB17.ELANINET.COM:1929	TCP	C:\WINDOWS\system32\svchost.exe	ESTABL...
VMBOX.LOCALDOMAIN:NETB...	0.0.0.0	TCP	System	LISTENING
VMBOX:49123	0.0.0.0	TCP	C:\WINDOWS\system32\cssrss.exe	LISTENING
VMBOX:42485	0.0.0.0	TCP	C:\WINDOWS\system32\cssrss.exe	LISTENING
VMBOX:40702	0.0.0.0	TCP	C:\WINDOWS\system32\cssrss.exe	LISTENING
VMBOX:16786	0.0.0.0	TCP	C:\WINDOWS\system32\cssrss.exe	LISTENING
VMBOX:MICROSOFT-DS	0.0.0.0	TCP	System	LISTENING
VMBOX:EPMAP	0.0.0.0	TCP	C:\WINDOWS\system32\svchost.exe	LISTENING
VMBOX.LOCALDOMAIN:1900	NA	UDP	C:\WINDOWS\system32\svchost.exe	NA
VMBOX.LOCALDOMAIN:138	NA	UDP	System	NA
VMBOX.LOCALDOMAIN:NETB...	NA	UDP	System	NA
VMBOX.LOCALDOMAIN:123	NA	UDP	C:\WINDOWS\system32\svchost.exe	NA
VMBOX:1900	NA	UDP	C:\WINDOWS\system32\svchost.exe	NA
VMBOX:123	NA	UDP	C:\WINDOWS\system32\svchost.exe	NA
VMBOX:4500	NA	UDP	C:\WINDOWS\system32\lsass.exe	NA
VMBOX:2682	NA	UDP	C:\WINDOWS\system32\svchost.exe	NA
VMBOX:2681	NA	UDP	C:\WINDOWS\system32\svchost.exe	NA

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/sysprotantirookit/>

<http://swatrant.blogspot.com/>