IT8761 – Security Laboratory

Reshma Ramesh Babu

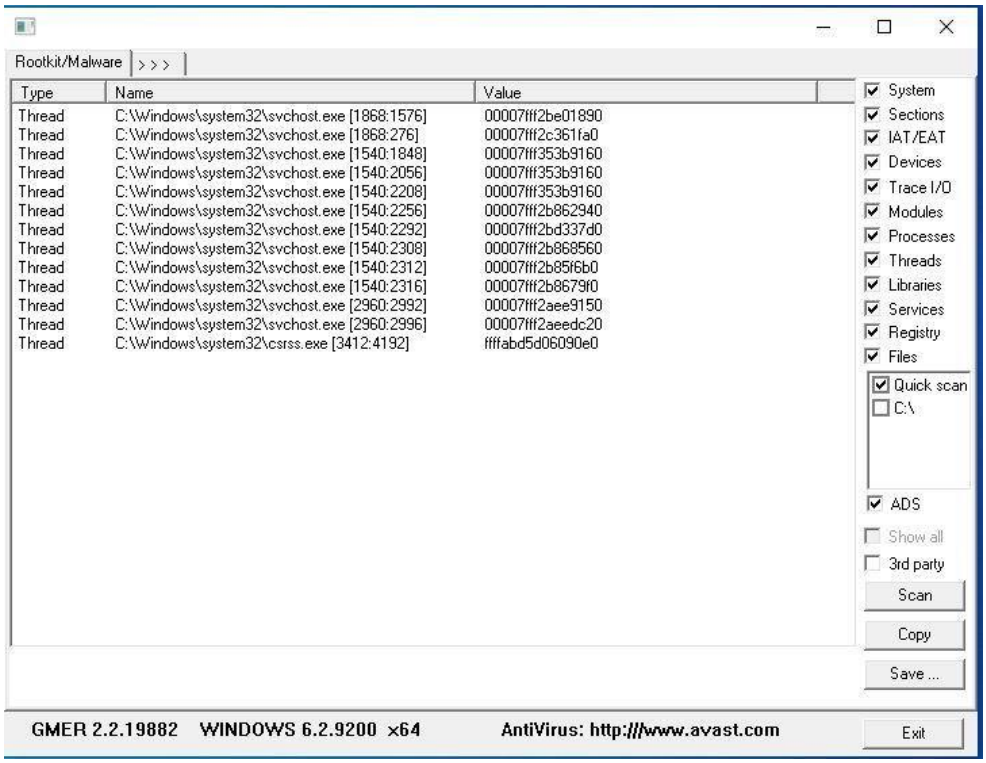
312217104129

Exercise 12 b

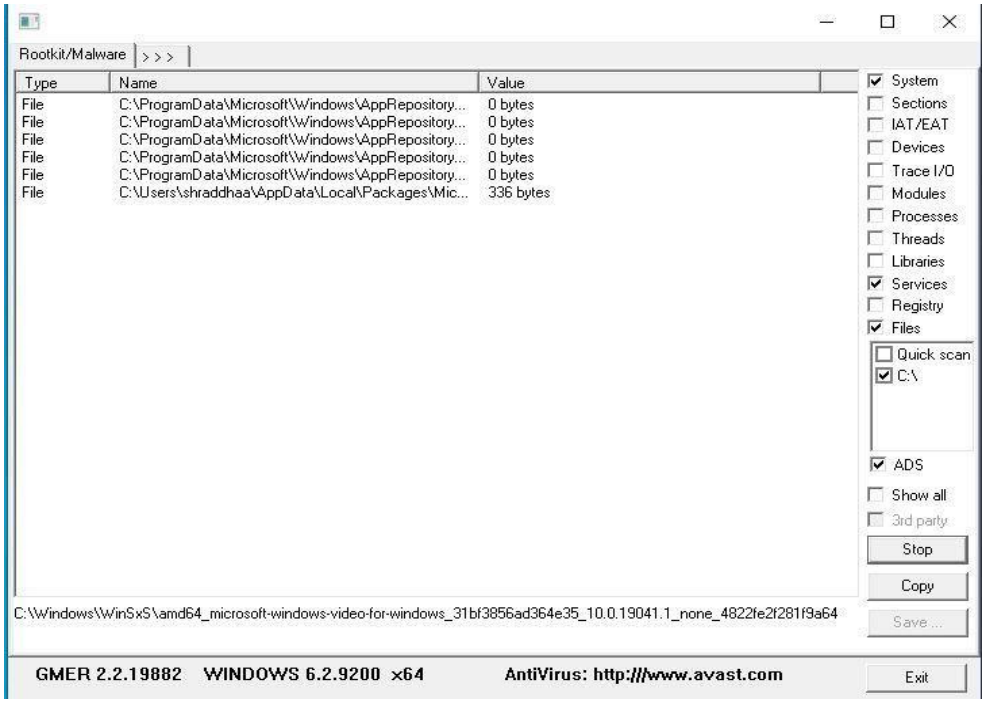
Aim: To install rootkit and to study about the variety of options

Output:

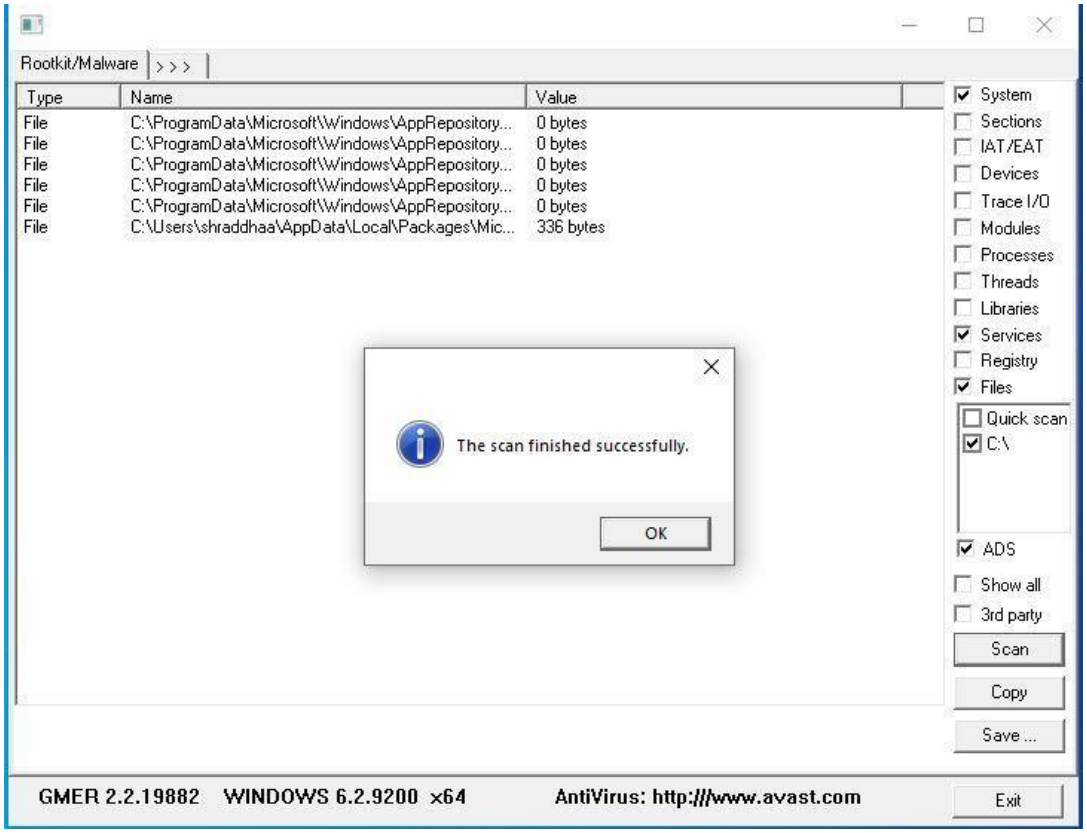
1. Download and install the Rootkit Tool from GMER website. www.gmer.net
2. Now the rootkit screen will be displayed



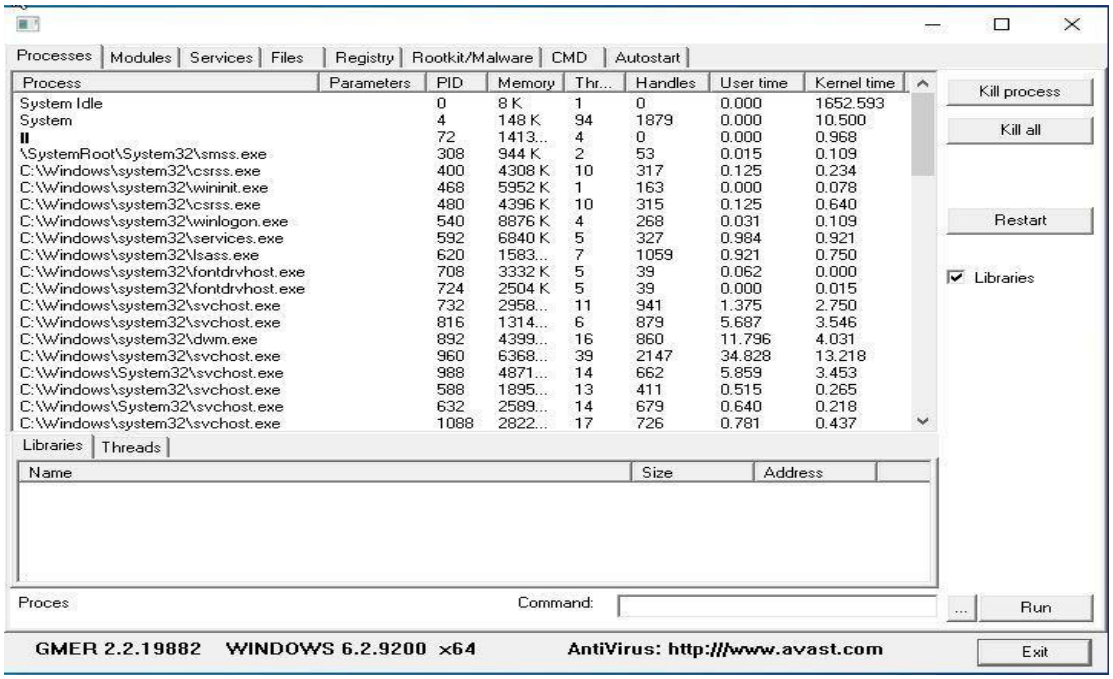
3. Select anyone of the drive which is shown at right side of the screen. After selecting the drive click on scan button.



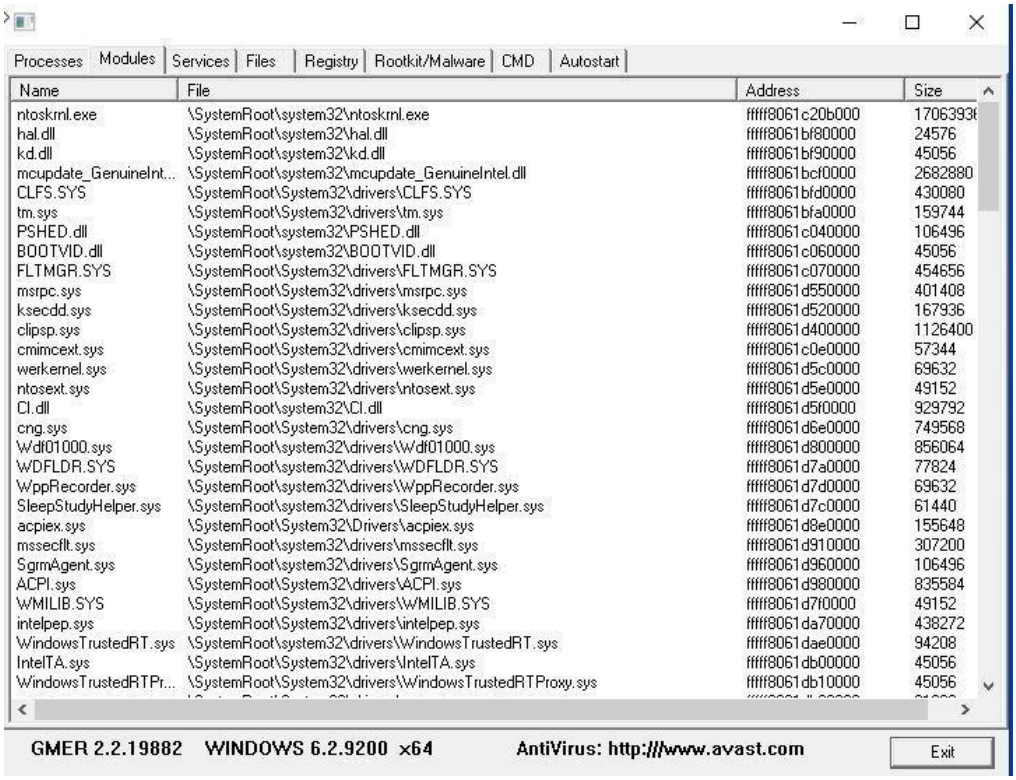
4. Wait for the scan to finish



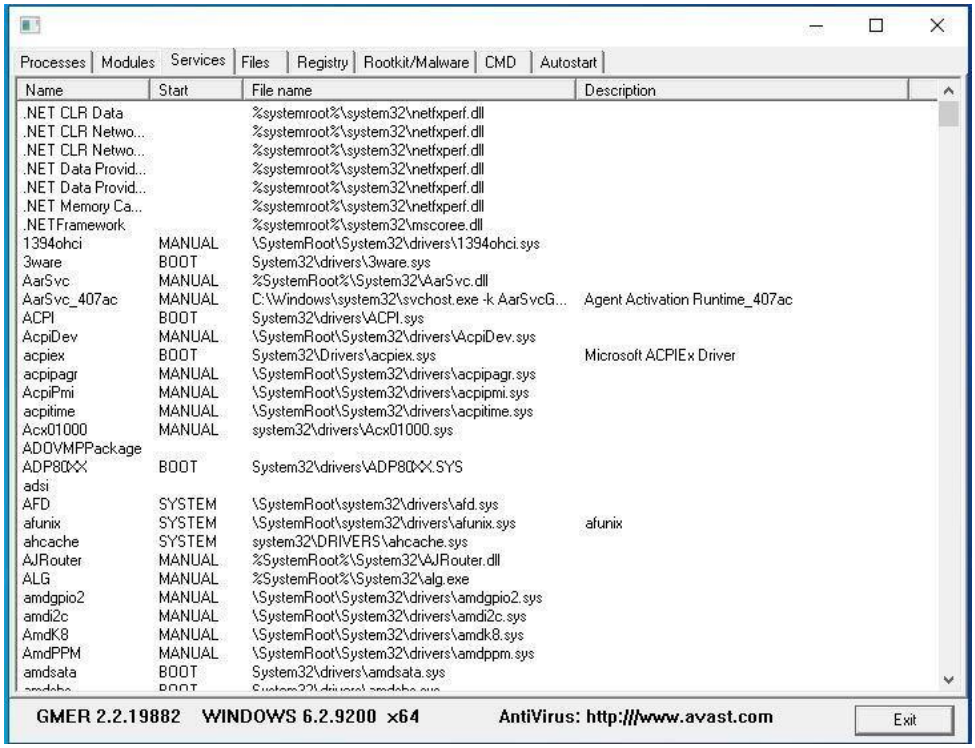
5. Click on the options. This displays the Processes, Modules, Services, Files, Registry, RootKit/Malwares, Autostart, CMD of local host. Select Processes menu and kill any unwanted process if any. (Read the details listed, Malware affected processes, services if any will be shown in red. Before selecting the kill option, care must be taken, since the Rootkit tool's suspects may be systems core services.)



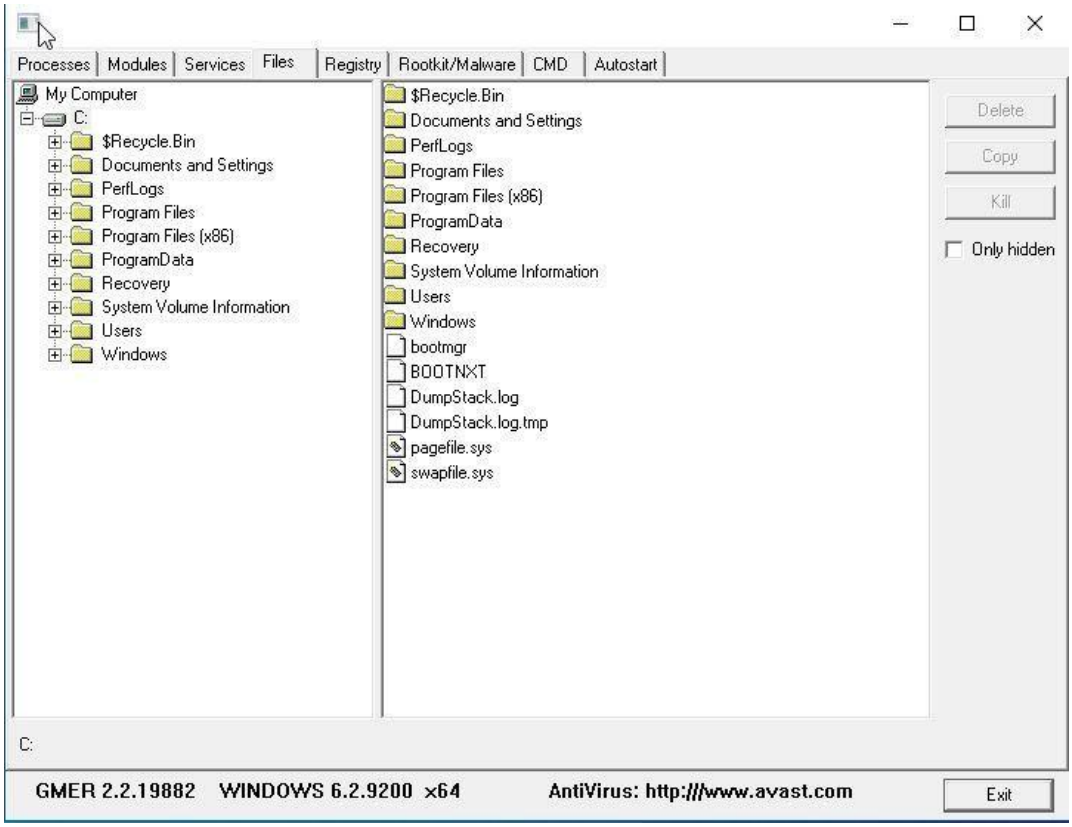
6. Modules menu displays the various system files like .sys, .dll



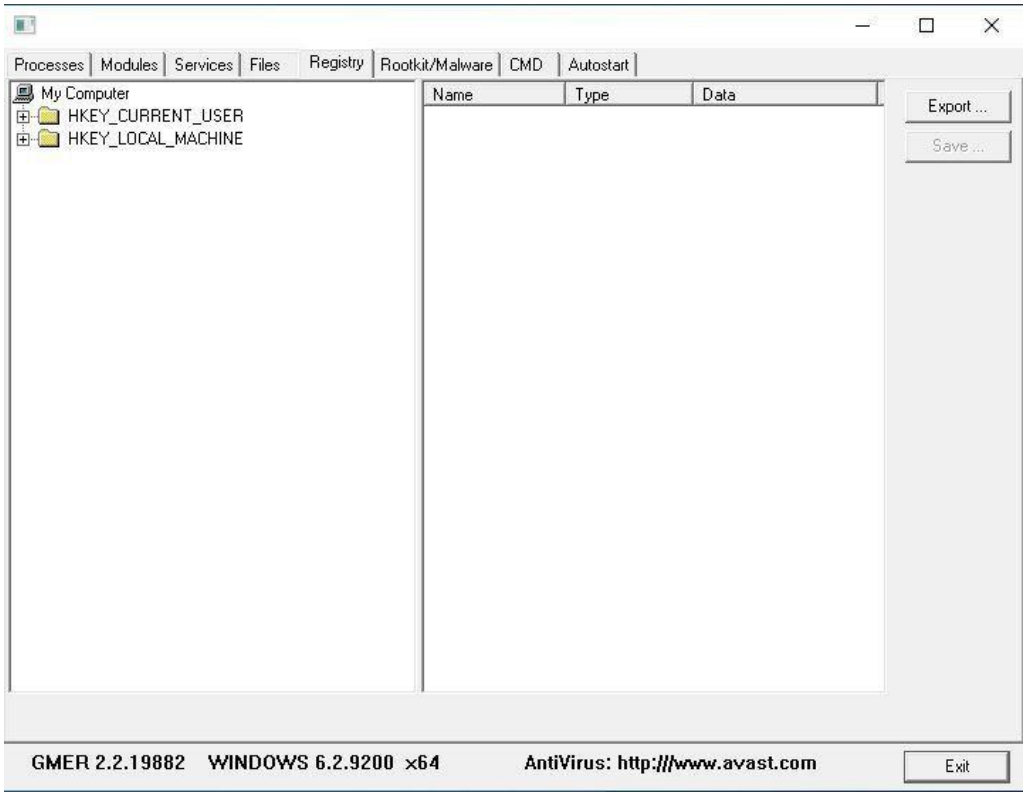
7. Services menu displays the complete services running with Autostart, Enable, Disable, System, Boot.



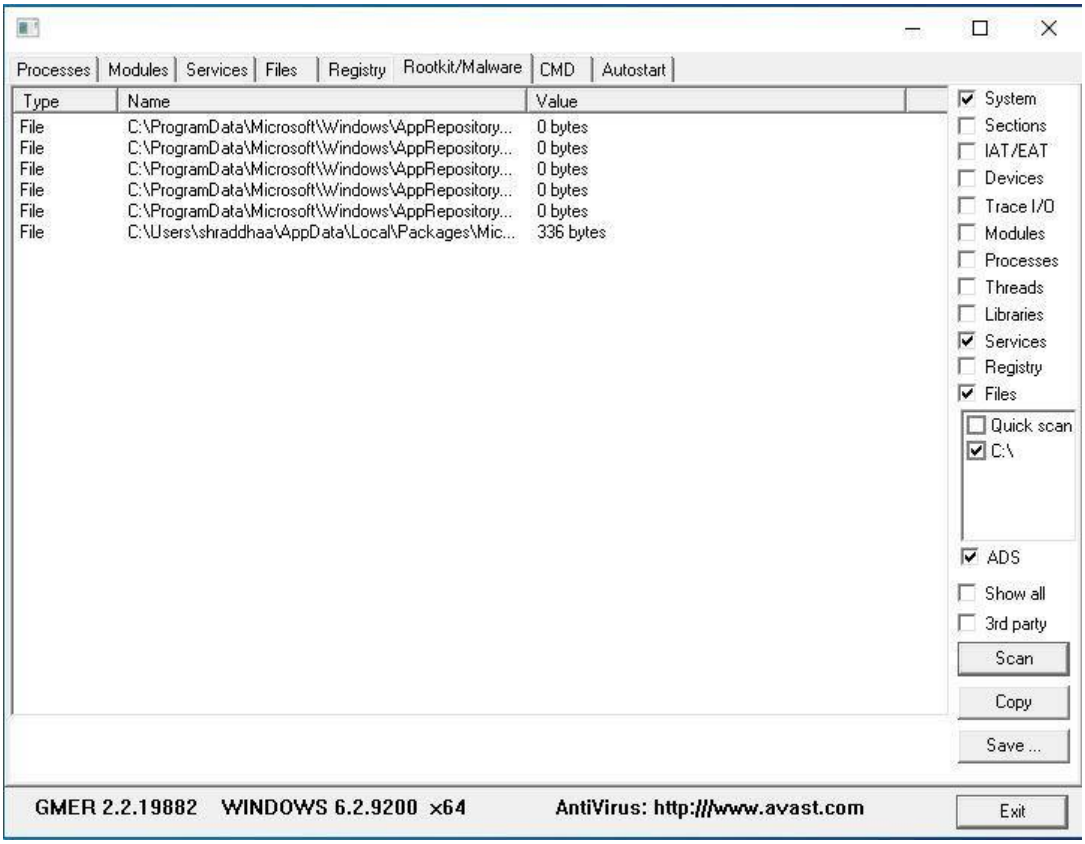
8. Files menu displays full files on Hard-Disk volumes.



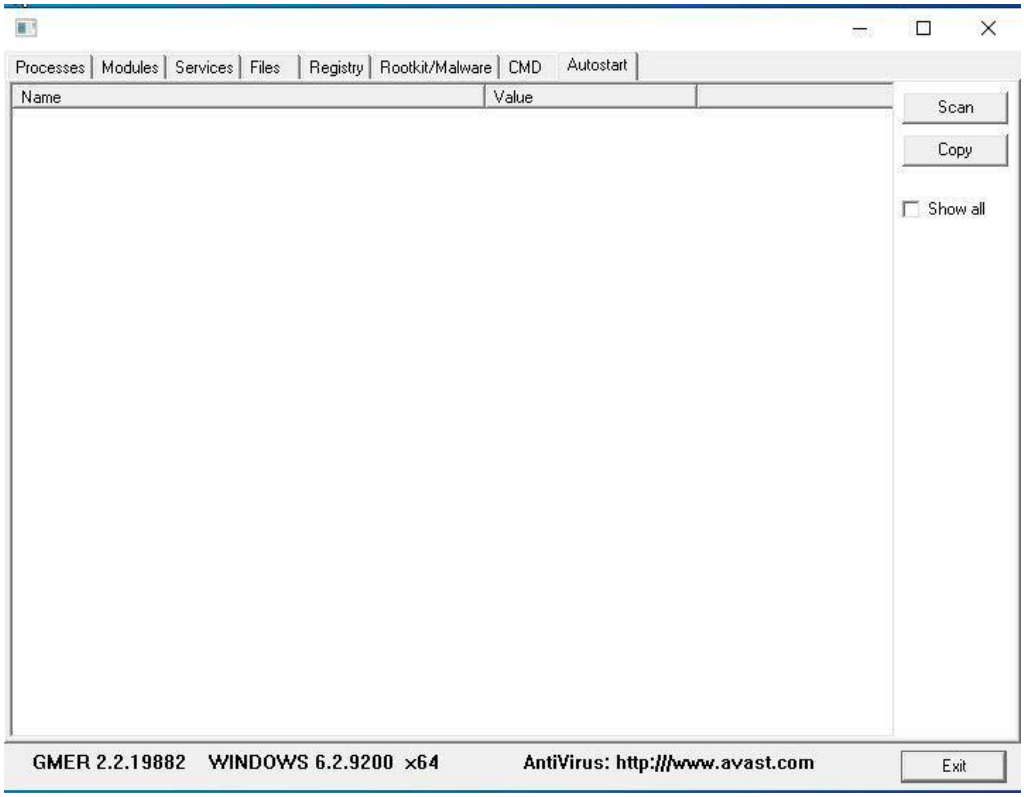
9. Registry displays Hkey_Current_user and Hkey_Local_Machine.



10. Rootkits/Malawares scans the local drives selected.



11. Autostart displays the registry base Autostart applications.



12. CMD allows the user to interact with command line utilities or Registry