

**SSN College of Engineering,
Department of Computer Science and Engineering
IT8761 Security Laboratory**

Exercise 12a:

To build a Trojan and know the harmness of the trojan malwares in a computer system.

Output: Upload the snapshot of the programs opened

Introduction:

TROJAN:

- In computing, a Trojan horse or trojan, is any malware which misleads users of its true intent.
- Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an email attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else.
- Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer.
- Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity.
- Example: Ransomware attacks are often carried out using a trojan

Assignment Hints:

- 1. Create a simple trojan by using Windows Batch File (.bat)**
- 2. Type these below code in notepad and save it as Trojan.bat**

```
@echo off
:x
start mspaint
start notepad
start cmd
start explorer
start control
start calc
goto x
```

- 3. Double click on Trojan.bat file.**
- 4. When the trojan code executes, it will open MS-Paint, Notepad, Command Prompt, Explorer, etc., infinitely.**
- 5. Restart the computer to stop the execution of this trojan.**

**SSN College of Engineering,
Department of Computer Science and Engineering
IT8791 Security Laboratory**

Exercise 12b:

To install rootkit and to study about the variety of options.

Output: Upload the capture snapshots of every tab in its UI

Introduction :

- A rootkit is a stealthy type of malicious software (malware) designed to hide the existence of certain processes or programs from normal methods of detection and enables continued privileged access to a computer.
- The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implement the tool).
- A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network.
- Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password.
- Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.
- A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection

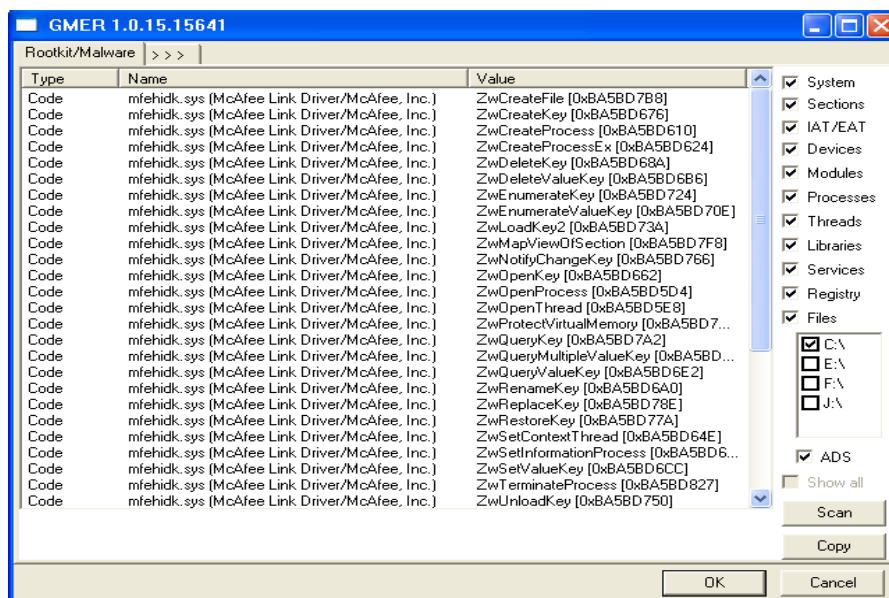
GMER :

- GMER is a free rootkit detector developed by Przemyslaw Gmerek, a Polish security researcher.
- Some of the features that GMER provides include detection of hidden processes, threads, services, files. It also provides removal and restoration options if a rootkit is detected.

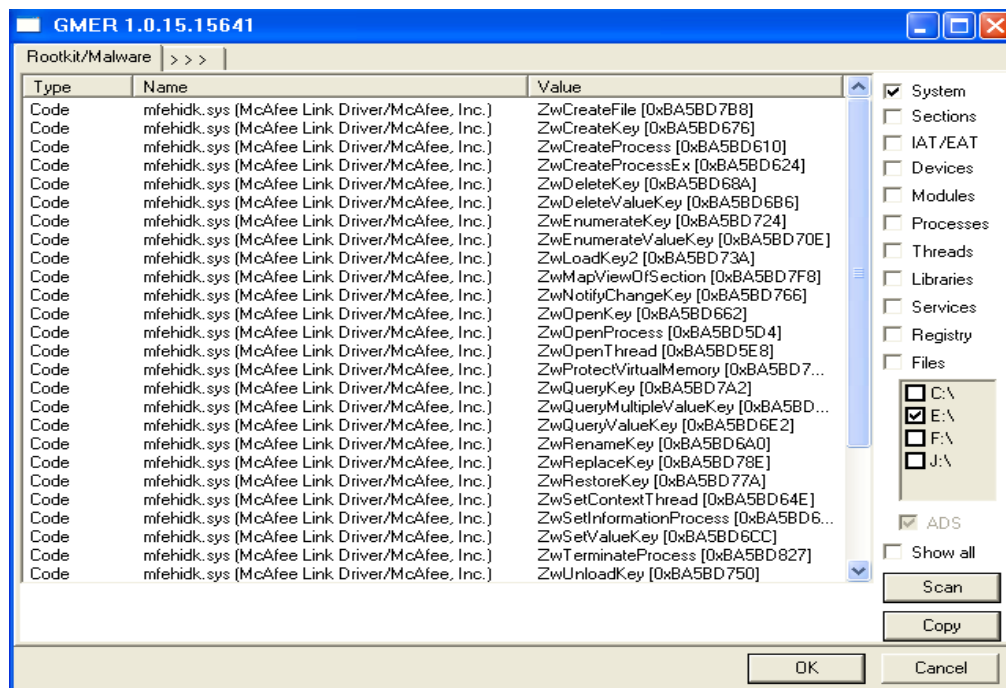
- GMER has built-in protection by hooking various Windows OS services to prevent malware from interfering with its operation.
- Additionally, GMER randomly changes the name of its running process as another method of self-protection.
- GMER has the ability to scan and display all currently loaded drivers and tell you whether they are hidden and whether the drivers file is visible on disk.
- It scans for hidden, locked or falsified files on the system
- It scans and displays the currently running processes (similar to Process Explorer) but shows if the process is hidden or locked.
- It scans for Stealth objects which looks for rootkit symptoms in general.
- It scans for Hidden services and displays them.
- Once you have found something malicious, you can right click on the driver/file/service and either copy, wipe or force delete it.

Installation of GMER:

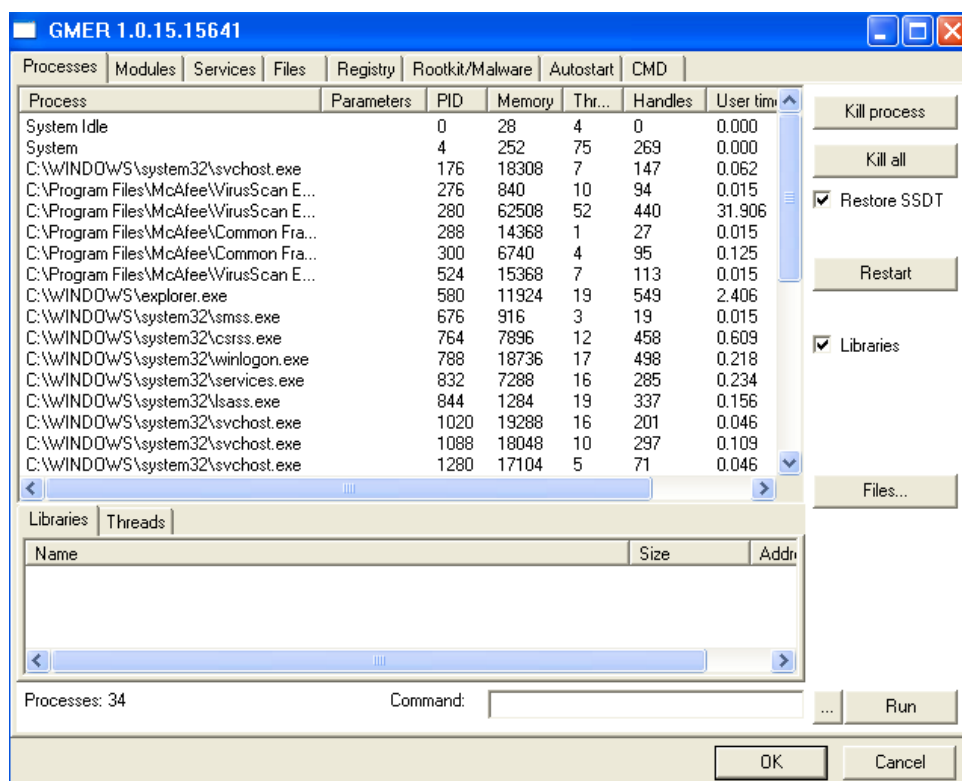
1. Download and install the Rootkit Tool from GMER website. www.gmer.net
2. Now the rootkit screen will be displayed



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



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.)

8. Modules menu displays the various system files like .sys, .dll
9. Services menu displays the complete services running with Autostart, Enable, Disable, System, Boot.
10. Files menu displays full files on Hard-Disk volumes.
11. Registry displays Hkey_Current_user and Hkey_Local_Machine.
12. Rootkits/Malawares scans the local drives selected.
13. Autostart displays the registry base Autostart applications.
14. CMD allows the user to interact with command line utilities or Registry