EX.NO:	DEFEATING MALWARE - BUILDING TROJANS

Aim:

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

Algorithm:

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

TROJAN:

- In computing, a Trojan horse,or Trojan, is any malware which misleads users of itstrue 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 bankinginformation, passwords, or personal identity.
- ***Example:*** *Ransomware* attacks are often carried out using a *trojan*.

Setting Up a Safe Environment

1. Create a Virtual Machine

1. **Download and Install VirtualBox or VMware**: These are popular VM managers.
2. **Create a New Virtual Machine**: Install a Windows operating system on it.

2. Prepare the Virtual Environment

1. **Isolate the VM**: Ensure the VM network settings are set to "Host-only" or disconnected to prevent any potential spread.
2. **Take a Snapshot**: Before starting, take a snapshot of your VM. This allows you to revert to a clean state if needed.

Creating and Running the Batch Script

1. **Open Notepad in the VM**:
    - Press Win + R, type notepad, and press Enter.
2. **Create the Batch Script**:
    - Copy and paste the following code into Notepad:

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

3. **Save the Script**:
    - Save the file with a .bat extension, for example, Trojan.bat.
4. **Execute the Script**:
    - Double-click the Trojan.bat file to execute it.

Observing the Behavior

- **Open Task Manager**:
    - Press Ctrl + Shift + Esc to open Task Manager and observe the running processes.
- **Monitor System Performance**:
    - Check CPU and memory usage to see the impact of the script.

Stopping the Script

1. **Open Task Manager**:
   - Press Ctrl + Shift + Esc to open Task Manager.
2. **End the Batch Script Process**:
   - Find the running cmd.exe processes related to the batch script and end them.
3. **Close the Applications**:
   - Manually close any opened applications (MS Paint, Notepad, CMD, Explorer, Control Panel, Calculator).

Clean Up and Restore

1. **Delete the Batch Script**:
   - Delete the Trojan.bat file to prevent accidental re-execution.
2. **Revert the VM**:
   - Revert to the snapshot taken before running the script to ensure the VM is clean.

Program:

Trojan.bat

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

Output:

(MS-Paint, Notepad, Command Prompt, Explorer will open infinitely)

Result:

EX.NO:	DEFEATING MALWARE - ROOTKIT HUNTER

Aim:

To install a rootkit hunter and find the malwares in a computer.

Algorithm:

ROOTKIT HUNTER:

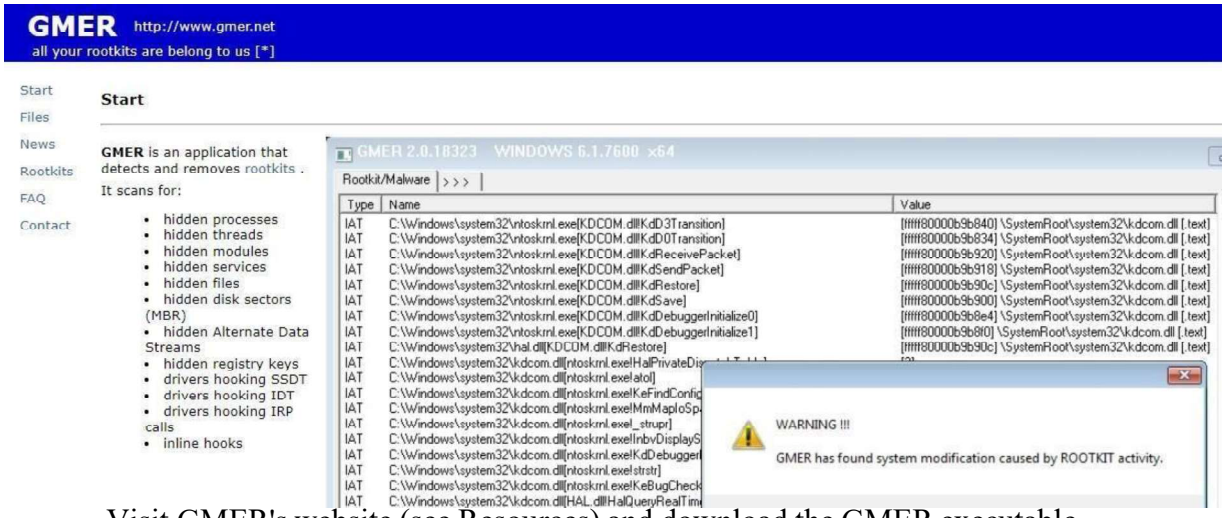
- rkhunter (Rootkit Hunter) is a Unix-based tool that scans for rootkits, backdoors andpossible local exploits.
- It does this by comparing SHA-1 hashes of important files with known good ones in online databases, searching for default directories (of rootkits), wrong permissions, hidden files, suspicious strings in kernel modules, and special tests for Linux and FreeBSD.
- rkhunter is notable due to its inclusion in popular operating systems (Fedora, Debian,etc.)
- The tool has been written in Bourne shell, to allow for portability. It can run on almostall UNIX-derived systems.

GMER ROOTKIT TOOL:

- GMER is a software tool written by a Polish researcher Przemysław Gmerek, fordetecting and removing rootkits.
- It runs on Microsoft Windows and has support for Windows NT, 2000, XP, Vista, 7, 8

and 10. With version 2.0.18327 full support for Windows x64 is added

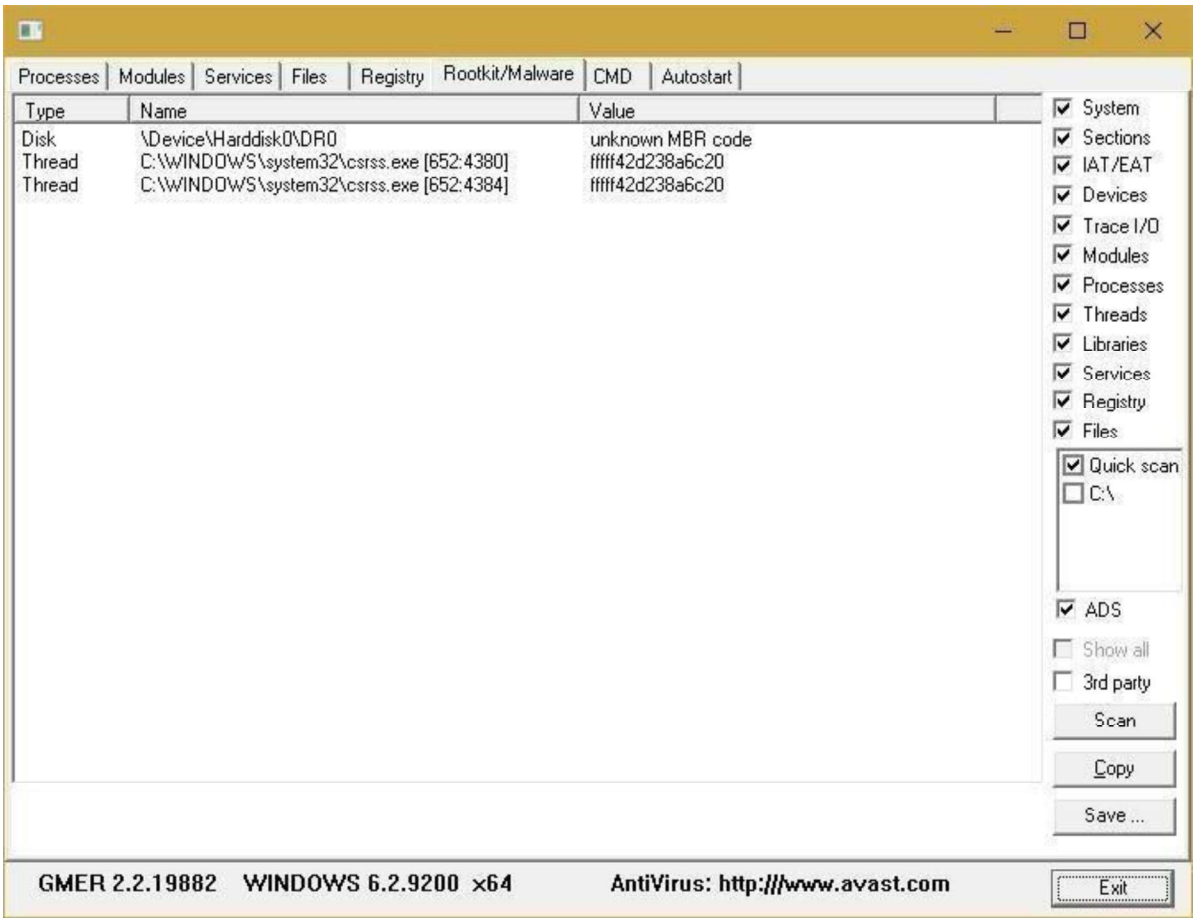
Step 1



Visit GMER's website (see Resources) and download the GMER executable.

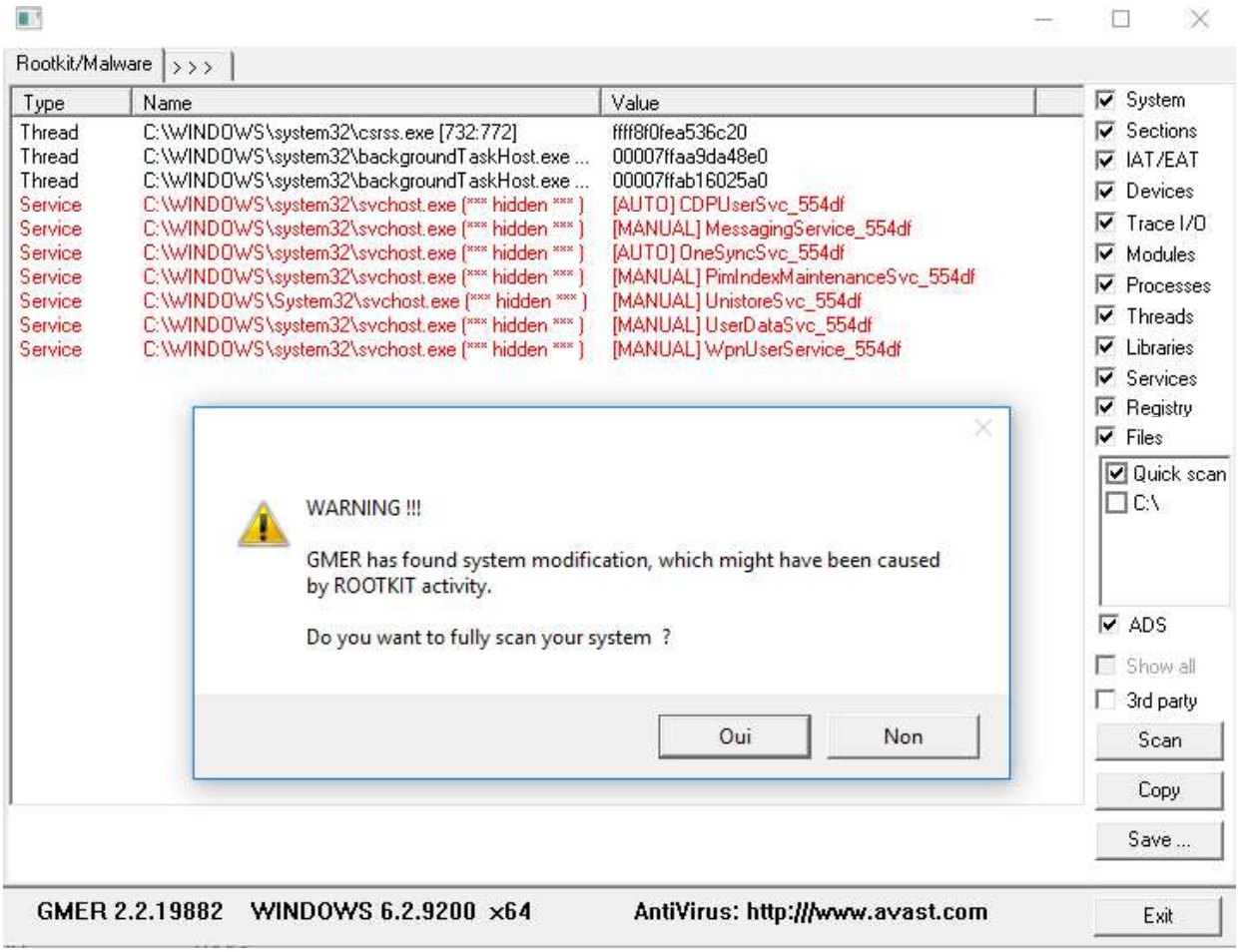
Click the "Download EXE" button to download the program with a random file name, assome rootkits will close “gmer.exe” before you can open it.

Step 2



Double-click the icon for the program.
Click the "Scan" button in the lower-right corner ofthe dialog box. Allow the program toscan your entire hard drive.

Step 3



When the program completes its scan, select any program or file listed in red. Right-click it and select "Delete."

If the red item is a service, it may be protected. Right-click the service and select "Disable." Reboot your computer and run the scan again, this time selecting "Delete" when that serviceis detected.

When your computer is free of Rootkits, close the program and restart your PC.

RESULT:

A rootkit hunter software tool *gmer* has been installed and the rootkits have beendetected.