EXPERIMENT NO. 09

AIM :- Installation of rootkits

SOFTWARE USED :- GERM WEBSITE

INTRODUCTION:-

Rootkit is a stealth type of malicious software designed to hide the existence of certain process from normal methods of detection and enables continued privileged access to a computer.

Breaking the term rootkit into the two component words, root and kit, is a useful way to define it. Root is a UNIX/Linux term that's the equivalent ofAdministrator in Windows. The word kit denotes programs that allow someone to obtain root/admin-level access to the computer by executing the programs in the kit — all of which is done without end-user consent or knowledge.

A rootkit is a type of malicious software that is activated each time your system boots up. Rootkits are difficult to detect because they are activated before your system's Operating System has completely booted up. A rootkit often allows the installation of hidden files, processes, hidden user accounts, and more in the systems OS. Rootkits are able to intercept data from terminals,network connections, and the keyboard.

Rootkits have two primary functions: remote command/control (back door) and software eavesdropping. Rootkits allow someone, legitimate or otherwise, to administratively control a computer. This means executing files, accessing logs, monitoring user activity, and even changing the computer's configuration. Therefore, in the strictest sense, even versions of VNC are rootkits. This surprises most people, as they consider rootkits to be solely malware, but in of themselves they aren't malicious at all.

The presence of a rootkit on a network was first documented in the early 1990s. At that time, Sun and Linux operating systems were the primary targets for a hacker looking to install a rootkit. Today, rootkits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network.

PROCEDURE:

STEP-1: Download Rootkit Tool from GMER website www.gmer.net.

STEP-2: This displays the Processes, Modules, Services, Files, Registry, RootKit / Malwares, Autostart, CMD of local host.

STEP-3: Select Processes menu and kill any unwanted process if any.

STEP-4: Modules menu displays the various system files like .sys, .dll

STEP-5: Services menu displays the complete services running with Autostart, Enable, Di

System, Boot.

STEP-6: Files menu displays full files on Hard-Disk volumes.

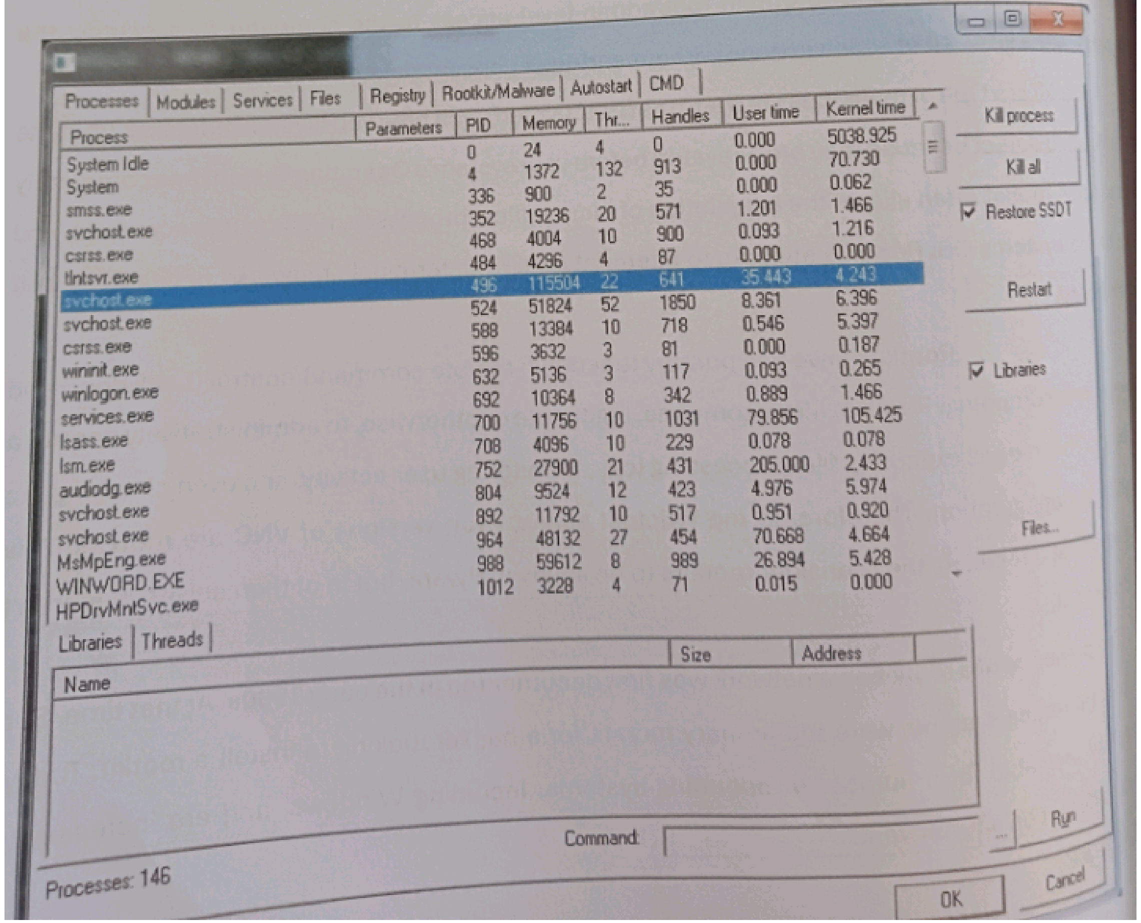
STEP-7: Registry displays Hkey_Current_user and Hkey_Local_Machine.

STEP-8: Rootkits / Malwares scans the local drives selected.

STEP-9: Autostart displays the registry base Autostart applications.

STEP-10:CMD allows the user to interact with command line utilities or Registry

SCREENSHOTS:



Process	Parameters	PID	Memory	Thr...	Handles	User time	Kernel time
System Idle		0	24	4	0	0.000	5038.925
System		4	1372	132	913	0.000	70.730
smss.exe		336	900	2	35	0.000	0.062
svchost.exe		352	19236	20	571	1.201	1.466
csrss.exe		468	4004	10	900	0.093	1.216
tlntsvr.exe		484	4296	4	87	0.000	0.000
svchost.exe		496	115504	22	641	35.443	4.243
svchost.exe		524	51824	52	1850	8.361	6.396
csrss.exe		588	13384	10	718	0.546	5.397
wininit.exe		596	3632	3	81	0.000	0.187
winlogon.exe		632	5136	3	117	0.093	0.265
services.exe		692	10364	8	342	0.889	1.466
lsass.exe		700	11756	10	1031	79.856	105.425
lsm.exe		708	4096	10	229	0.078	0.078
audiodg.exe		752	27900	21	431	205.000	2.433
svchost.exe		804	9524	12	423	4.976	5.974
svchost.exe		892	11792	10	517	0.951	0.920
MsMpEng.exe		964	48132	27	454	70.668	4.664
WINWORD.EXE		988	59612	8	989	26.894	5.428
HPDrvMntSvc.exe		1012	3228	4	71	0.015	0.000

Processes: 146