EX.NO:5 **SETUP A HONEY POT AND MONITOR THE HONEY POT**
DATE: **ON NETWORK (KF SENSOR)**

AIM:

To Setup a honey pot and monitor the honey pot on the network using KF Sensor tool.

INTRODUCTION:

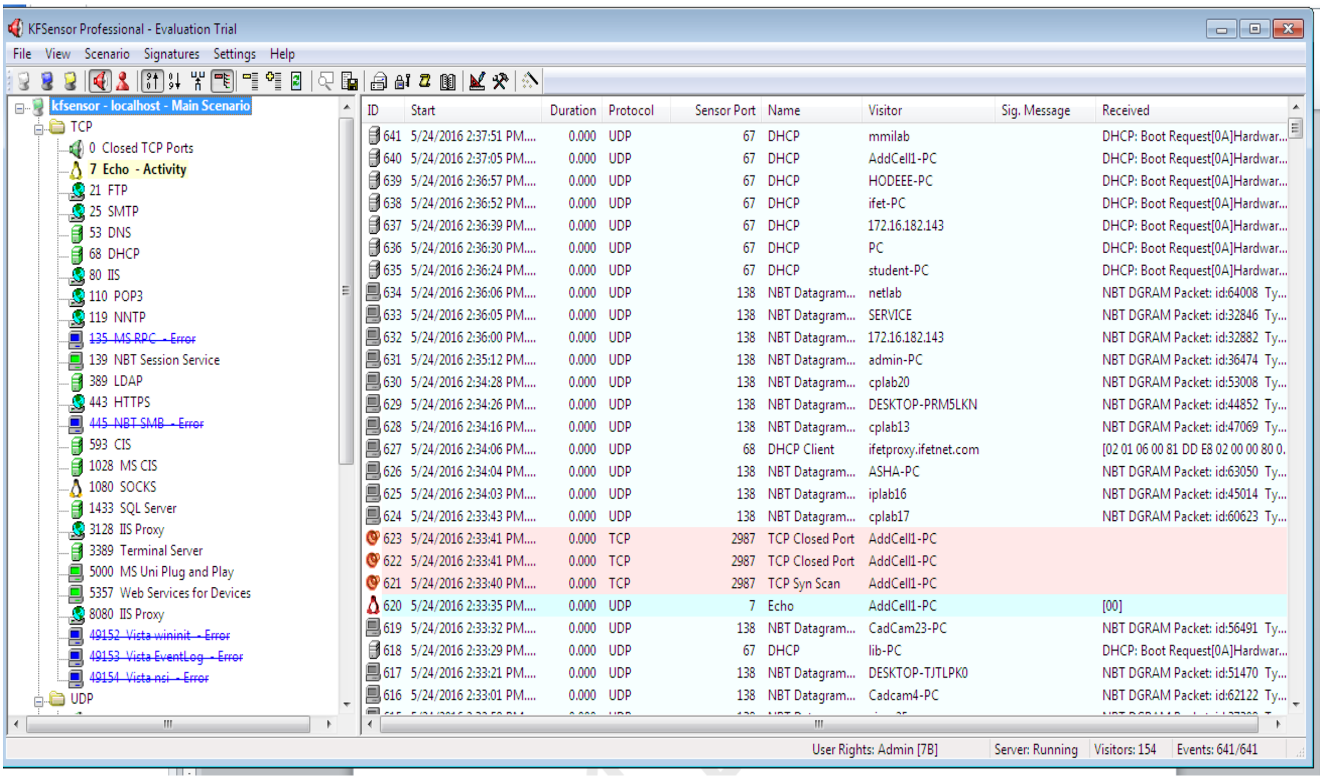
Honey Pot is a device placed on Computer Network specifically designed to capture malicious network traffic. KF Sensor is the tool to setup as honeypot when KF Sensor is running it places a siren icon in the windows system tray in the bottom right of the screen. If there are no alerts then green icon is displayed.

PROCEDURE:

- Install KF Sensor and set appropriate directory path.
- Reboot the Computer now.
- The KF Sensor automatically starts during windows boot.
- Click Next to setup wizard.
- Select all port classes to include and Click Next.
- Send the email and Send from email enter the ID and Click Next.
- Select the options such as Denial of Service[DOS], Port Activity, Proxy Emulsion, Network Port Analyzer,
- Click Next.
- Select Install as System service and Click Next.
- Click finish.
- Click on the ports icon to view the local host with TCP and UDP
- Click on the visitor’s icon to view the visitors in the network and to know the recent activities done by them.

OUTPUT:

LOCAL HOST:



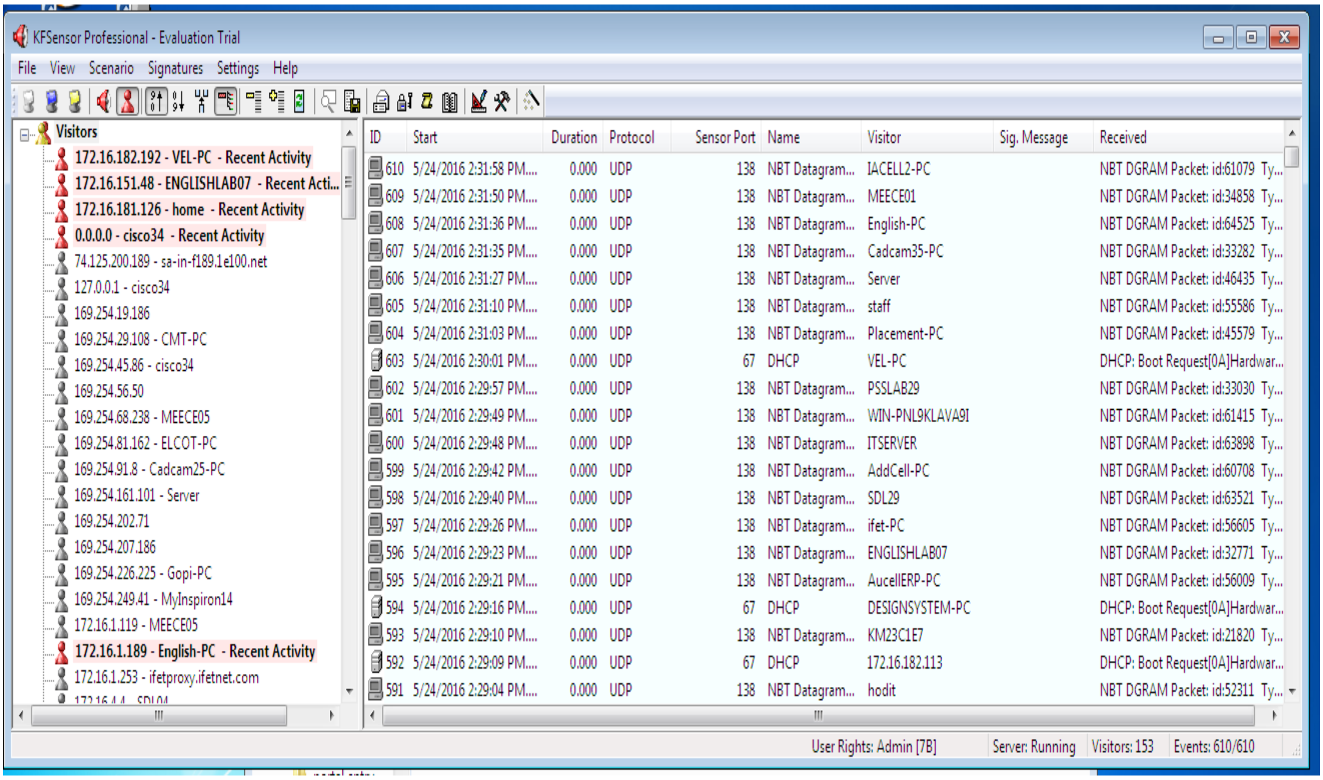
KFSensor Professional - Evaluation Trial

- kfsensor - localhost - Main Scenario
  - TCP
    - 0 Closed TCP Ports
    - 7 Echo - Activity
    - 21 FTP
    - 25 SMTP
    - 53 DNS
    - 68 DHCP
    - 80 IIS
    - 110 POP3
    - 119 NNTP
    - ~~135 MS RPC - Error~~
    - 139 NBT Session Service
    - 389 LDAP
    - 443 HTTPS
    - ~~445 NBT SMB - Error~~
    - 593 CIS
    - 1028 MS CIS
    - 1080 SOCKS
    - 1433 SQL Server
    - 3128 IIS Proxy
    - 3389 Terminal Server
    - 5000 MS Uni Plug and Play
    - 5357 Web Services for Devices
    - 8080 IIS Proxy
    - ~~49152 Vista wininit - Error~~
    - ~~49153 Vista EventLog - Error~~
    - ~~49154 Vista nsi - Error~~
  - UDP

ID	Start	Duration	Protocol	Sensor Port	Name	Visitor	Sig. Message	Received
641	5/24/2016 2:37:51 PM....	0.000	UDP	67	DHCP	mmilab		DHCP: Boot Request[0A]Hardwar...
640	5/24/2016 2:37:05 PM....	0.000	UDP	67	DHCP	AddCell1-PC		DHCP: Boot Request[0A]Hardwar...
639	5/24/2016 2:36:57 PM....	0.000	UDP	67	DHCP	HODEEE-PC		DHCP: Boot Request[0A]Hardwar...
638	5/24/2016 2:36:52 PM....	0.000	UDP	67	DHCP	ifet-PC		DHCP: Boot Request[0A]Hardwar...
637	5/24/2016 2:36:39 PM....	0.000	UDP	67	DHCP	172.16.182.143		DHCP: Boot Request[0A]Hardwar...
636	5/24/2016 2:36:30 PM....	0.000	UDP	67	DHCP	PC		DHCP: Boot Request[0A]Hardwar...
635	5/24/2016 2:36:24 PM....	0.000	UDP	67	DHCP	student-PC		DHCP: Boot Request[0A]Hardwar...
634	5/24/2016 2:36:06 PM....	0.000	UDP	138	NBT Datagram...	netlab		NBT DGRAM Packet: id:64008 Ty...
633	5/24/2016 2:36:05 PM....	0.000	UDP	138	NBT Datagram...	SERVICE		NBT DGRAM Packet: id:32846 Ty...
632	5/24/2016 2:36:00 PM....	0.000	UDP	138	NBT Datagram...	172.16.182.143		NBT DGRAM Packet: id:32882 Ty...
631	5/24/2016 2:35:12 PM....	0.000	UDP	138	NBT Datagram...	admin-PC		NBT DGRAM Packet: id:36474 Ty...
630	5/24/2016 2:34:28 PM....	0.000	UDP	138	NBT Datagram...	cplab20		NBT DGRAM Packet: id:53008 Ty...
629	5/24/2016 2:34:26 PM....	0.000	UDP	138	NBT Datagram...	DESKTOP-PRM5LKN		NBT DGRAM Packet: id:44852 Ty...
628	5/24/2016 2:34:16 PM....	0.000	UDP	138	NBT Datagram...	cplab13		NBT DGRAM Packet: id:47069 Ty...
627	5/24/2016 2:34:06 PM....	0.000	UDP	68	DHCP Client	ifetproxy.ifetnet.com		[02 01 06 00 81 DD E8 02 00 00 80 0.
626	5/24/2016 2:34:04 PM....	0.000	UDP	138	NBT Datagram...	ASHA-PC		NBT DGRAM Packet: id:63050 Ty...
625	5/24/2016 2:34:03 PM....	0.000	UDP	138	NBT Datagram...	iplab16		NBT DGRAM Packet: id:45014 Ty...
624	5/24/2016 2:33:43 PM....	0.000	UDP	138	NBT Datagram...	cplab17		NBT DGRAM Packet: id:60623 Ty...
623	5/24/2016 2:33:41 PM....	0.000	TCP	2987	TCP Closed Port	AddCell1-PC		
622	5/24/2016 2:33:41 PM....	0.000	TCP	2987	TCP Closed Port	AddCell1-PC		
621	5/24/2016 2:33:40 PM....	0.000	TCP	2987	TCP Syn Scan	AddCell1-PC		
620	5/24/2016 2:33:35 PM....	0.000	UDP	7	Echo	AddCell1-PC		[00]
619	5/24/2016 2:33:32 PM....	0.000	UDP	138	NBT Datagram...	CadCam23-PC		NBT DGRAM Packet: id:56491 Ty...
618	5/24/2016 2:33:29 PM....	0.000	UDP	67	DHCP	lib-PC		DHCP: Boot Request[0A]Hardwar...
617	5/24/2016 2:33:21 PM....	0.000	UDP	138	NBT Datagram...	DESKTOP-TJTLPK0		NBT DGRAM Packet: id:51470 Ty...
616	5/24/2016 2:33:01 PM....	0.000	UDP	138	NBT Datagram...	Cadcam4-PC		NBT DGRAM Packet: id:62122 Ty...

User Rights: Admin [7B] | Server: Running | Visitors: 154 | Events: 641/641

VISITORS IN THE NETWORK:



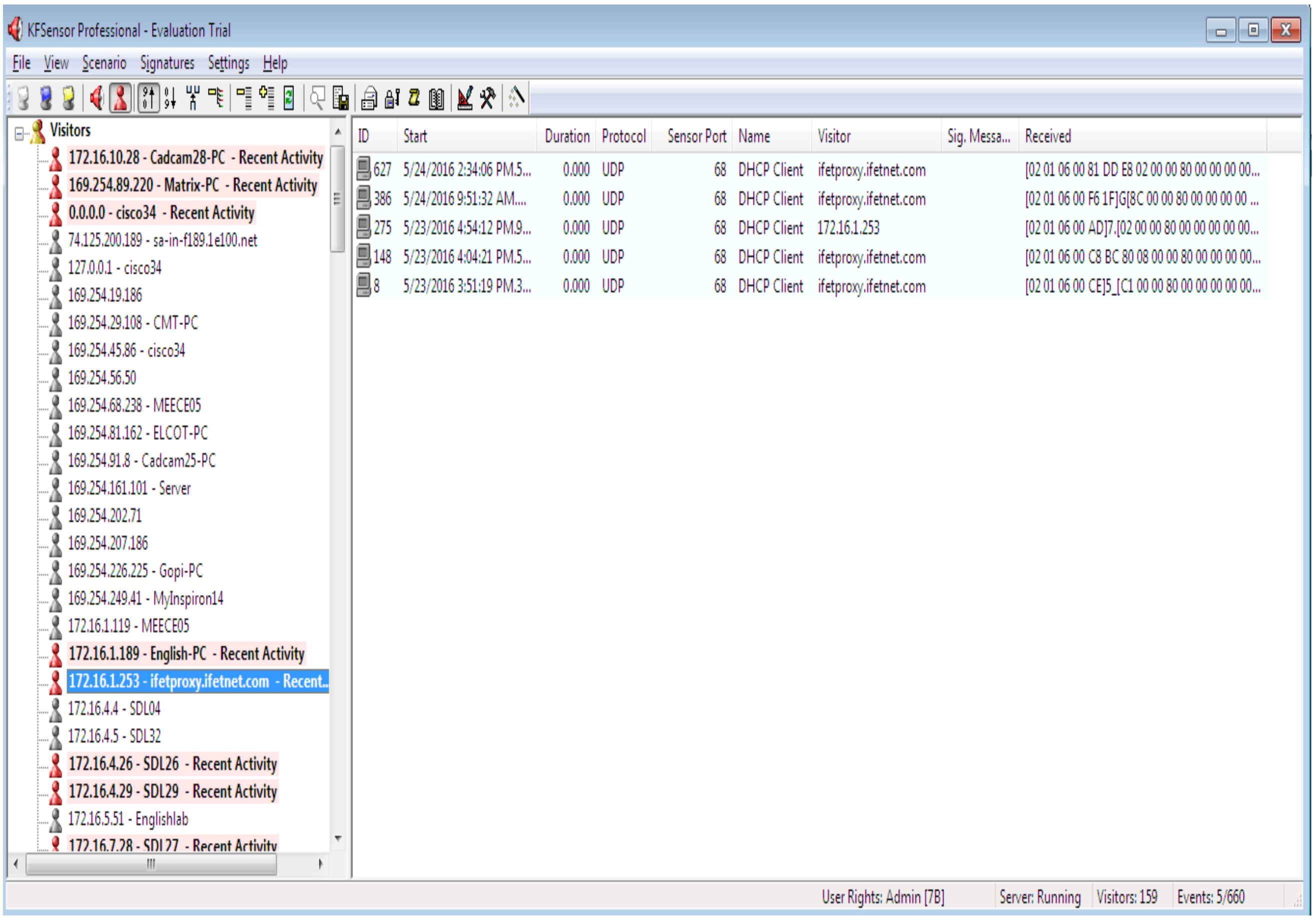
KFSensor Professional - Evaluation Trial

- Visitors
  - 172.16.182.192 - VEL-PC - Recent Activity
  - 172.16.151.48 - ENGLISHLAB07 - Recent Acti...
  - 172.16.181.126 - home - Recent Activity
  - 0.0.0.0 - cisco34 - Recent Activity
  - 74.125.200.189 - sa-in-f189.1e100.net
  - 127.0.0.1 - cisco34
  - 169.254.19.186
  - 169.254.29.108 - CMT-PC
  - 169.254.45.86 - cisco34
  - 169.254.56.50
  - 169.254.68.238 - MEECE05
  - 169.254.81.162 - ELCOT-PC
  - 169.254.91.8 - Cadcam25-PC
  - 169.254.161.101 - Server
  - 169.254.202.71
  - 169.254.207.186
  - 169.254.226.225 - Gopi-PC
  - 169.254.249.41 - MyInspiron14
  - 172.16.1.119 - MEECE05
  - 172.16.1.189 - English-PC - Recent Activity
  - 172.16.1.253 - ifetproxy.ifetnet.com

ID	Start	Duration	Protocol	Sensor Port	Name	Visitor	Sig. Message	Received
610	5/24/2016 2:31:58 PM....	0.000	UDP	138	NBT Datagram...	IACELL2-PC		NBT DGRAM Packet: id:61079 Ty...
609	5/24/2016 2:31:50 PM....	0.000	UDP	138	NBT Datagram...	MEECE01		NBT DGRAM Packet: id:34858 Ty...
608	5/24/2016 2:31:36 PM....	0.000	UDP	138	NBT Datagram...	English-PC		NBT DGRAM Packet: id:64525 Ty...
607	5/24/2016 2:31:35 PM....	0.000	UDP	138	NBT Datagram...	Cadcam35-PC		NBT DGRAM Packet: id:33282 Ty...
606	5/24/2016 2:31:27 PM....	0.000	UDP	138	NBT Datagram...	Server		NBT DGRAM Packet: id:46435 Ty...
605	5/24/2016 2:31:10 PM....	0.000	UDP	138	NBT Datagram...	staff		NBT DGRAM Packet: id:55586 Ty...
604	5/24/2016 2:31:03 PM....	0.000	UDP	138	NBT Datagram...	Placement-PC		NBT DGRAM Packet: id:45579 Ty...
603	5/24/2016 2:30:01 PM....	0.000	UDP	67	DHCP	VEL-PC		DHCP: Boot Request[0A]Hardwar...
602	5/24/2016 2:29:57 PM....	0.000	UDP	138	NBT Datagram...	PSSLAB29		NBT DGRAM Packet: id:33030 Ty...
601	5/24/2016 2:29:49 PM....	0.000	UDP	138	NBT Datagram...	WIN-PNL9KLAVA9I		NBT DGRAM Packet: id:61415 Ty...
600	5/24/2016 2:29:48 PM....	0.000	UDP	138	NBT Datagram...	ITSERVER		NBT DGRAM Packet: id:63898 Ty...
599	5/24/2016 2:29:42 PM....	0.000	UDP	138	NBT Datagram...	AddCell-PC		NBT DGRAM Packet: id:60708 Ty...
598	5/24/2016 2:29:40 PM....	0.000	UDP	138	NBT Datagram...	SDL29		NBT DGRAM Packet: id:63521 Ty...
597	5/24/2016 2:29:26 PM....	0.000	UDP	138	NBT Datagram...	ifet-PC		NBT DGRAM Packet: id:56605 Ty...
596	5/24/2016 2:29:23 PM....	0.000	UDP	138	NBT Datagram...	ENGLISHLAB07		NBT DGRAM Packet: id:32771 Ty...
595	5/24/2016 2:29:21 PM....	0.000	UDP	138	NBT Datagram...	AucellERP-PC		NBT DGRAM Packet: id:56009 Ty...
594	5/24/2016 2:29:16 PM....	0.000	UDP	67	DHCP	DESIGNSYSTEM-PC		DHCP: Boot Request[0A]Hardwar...
593	5/24/2016 2:29:10 PM....	0.000	UDP	138	NBT Datagram...	KM23C1E7		NBT DGRAM Packet: id:21820 Ty...
592	5/24/2016 2:29:09 PM....	0.000	UDP	67	DHCP	172.16.182.113		DHCP: Boot Request[0A]Hardwar...
591	5/24/2016 2:29:04 PM....	0.000	UDP	138	NBT Datagram...	hodit		NBT DGRAM Packet: id:52311 Ty...

User Rights: Admin [7B] | Server: Running | Visitors: 153 | Events: 610/610

CLICK ON THE SPECIFIC VISITOR TO SHOW THE SYSTEM ACTIVITIES:



Visitors
- 172.16.10.28 - Cadcam28-PC - Recent Activity
- 169.254.89.220 - Matrix-PC - Recent Activity
- 0.0.0.0 - cisco34 - Recent Activity
- 74.125.200.189 - sa-in-f189.1e100.net
- 127.0.0.1 - cisco34
- 169.254.19.186
- 169.254.29.108 - CMT-PC
- 169.254.45.86 - cisco34
- 169.254.56.50
- 169.254.68.238 - MEECE05
- 169.254.81.162 - ELCOT-PC
- 169.254.91.8 - Cadcam25-PC
- 169.254.161.101 - Server
- 169.254.202.71
- 169.254.207.186
- 169.254.226.225 - Gopi-PC
- 169.254.249.41 - MyInspiron14
- 172.16.1.119 - MEECE05
- 172.16.1.189 - English-PC - Recent Activity
- 172.16.1.253 - ifetproxy.ifetnet.com - Recent...
- 172.16.4.4 - SDL04
- 172.16.4.5 - SDL32
- 172.16.4.26 - SDL26 - Recent Activity
- 172.16.4.29 - SDL29 - Recent Activity
- 172.16.5.51 - Englishlab
- 172.16.7.28 - SDL27 - Recent Activity

ID	Start	Duration	Protocol	Sensor Port	Name	Visitor	Sig. Messa...	Received
627	5/24/2016 2:34:06 PM.5...	0.000	UDP	68	DHCP Client	ifetproxy.ifetnet.com		[02 01 06 00 81 DD E8 02 00 00 80 00 00 00 00...
386	5/24/2016 9:51:32 AM....	0.000	UDP	68	DHCP Client	ifetproxy.ifetnet.com		[02 01 06 00 F6 1F]G[8C 00 00 80 00 00 00 00 ...
275	5/23/2016 4:54:12 PM.9...	0.000	UDP	68	DHCP Client	172.16.1.253		[02 01 06 00 AD]7.[02 00 00 80 00 00 00 00 00...
148	5/23/2016 4:04:21 PM.5...	0.000	UDP	68	DHCP Client	ifetproxy.ifetnet.com		[02 01 06 00 C8 BC 80 08 00 00 80 00 00 00 00...
8	5/23/2016 3:51:19 PM.3...	0.000	UDP	68	DHCP Client	ifetproxy.ifetnet.com		[02 01 06 00 CE]5_[C1 00 00 80 00 00 00 00 00...

User Rights: Admin [7B] Server: Running Visitors: 159 Events: 5/660

RESULT:

Thus, the implementation of Setting a honey pot and monitoring the honey pot on the network using KF Sensor tool was executed and verified successfully.

EX.NO:6 **INSTALLATION OF ROOTKITS AND STUDY ABOUT THE VARIETY OF OPTIONS**

DATE:

AIM:

To install the rootkits and study about the variety of options using rootkit tool.

INTRODUCTION:

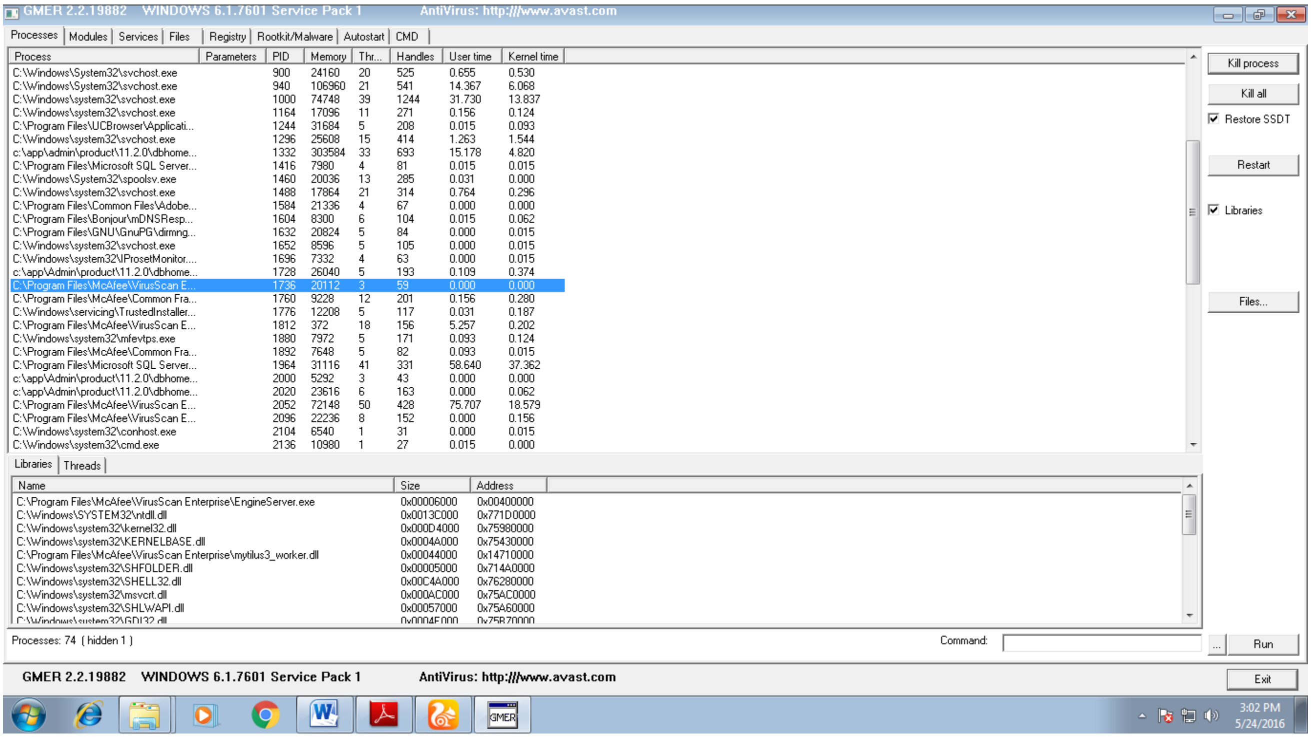
Root kit is a stealth type of malicious software designed to hide the existence of certain process from normal methods of detection and enables continued privileged access to a computer.

PROCEDURE:

- Download and install Rootkit Tool GMER.
- 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.
- Modules menu displays the various system files like .sys, .dll
- Services menu displays the complete services running with Autostart, Enable, Disable, System, Boot.
- Files menu displays full files on Hard-Disk volumes.
- Registry displays Hkey_Current_user and Hkey_Local_Machine.
- Rootkits/Malwares scans the local drives selected.
- Autostart displays the registry base Autostart applications.
- CMD allows the user to interact with command line utilities or Registry.

OUTPUT:

Choose a process to kill:

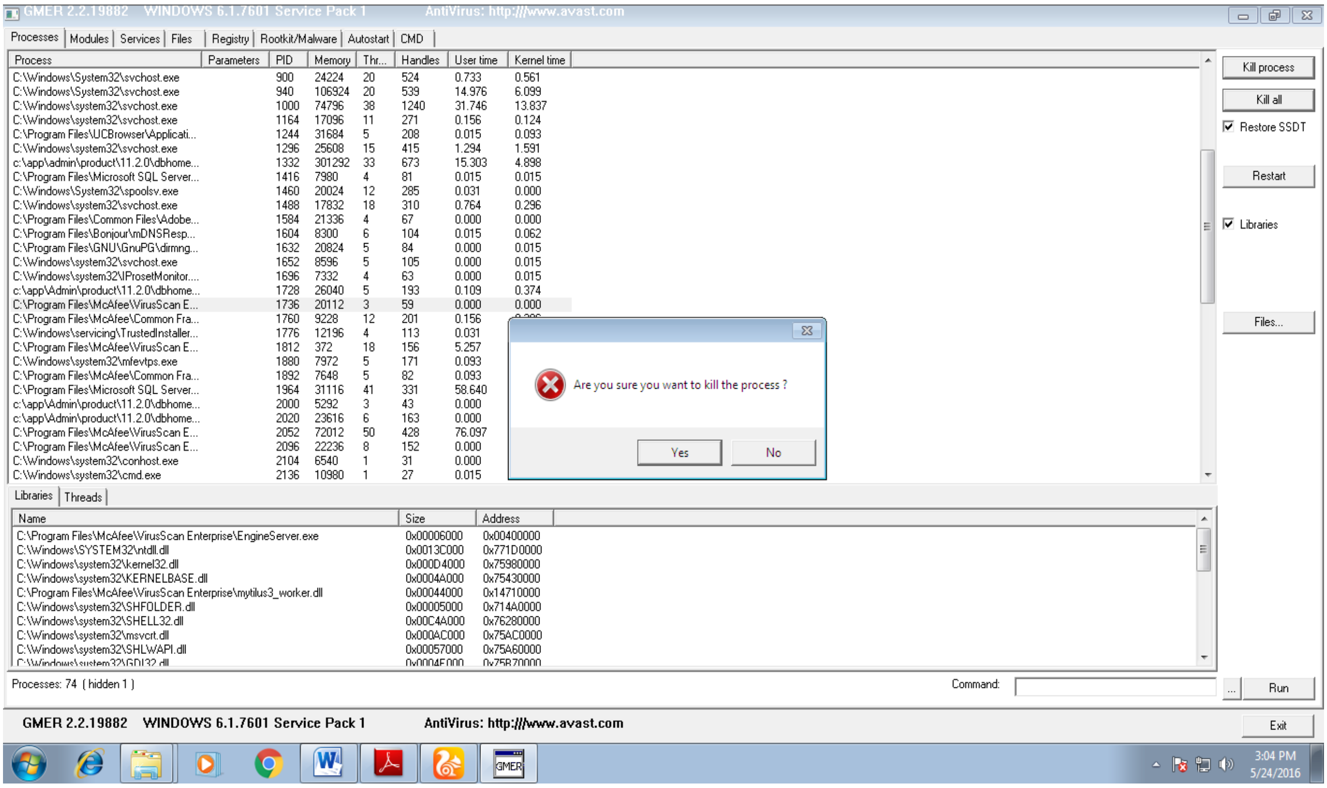


Process	Parameters	PID	Memory	Thr...	Handles	User time	Kernel time
C:\Windows\System32\svchost.exe		900	24160	20	525	0.655	0.530
C:\Windows\System32\svchost.exe		940	106960	21	541	14.367	6.068
C:\Windows\system32\svchost.exe		1000	74748	39	1244	31.730	13.837
C:\Windows\system32\svchost.exe		1164	17096	11	271	0.156	0.124
C:\Program Files\UCBrowser\Applicati...		1244	31684	5	208	0.015	0.093
C:\Windows\system32\svchost.exe		1296	25608	15	414	1.263	1.544
c:\app\admin\product\11.2.0\dbhome...		1332	303584	33	693	15.178	4.820
C:\Program Files\Microsoft SQL Server...		1416	7980	4	81	0.015	0.015
C:\Windows\System32\spoolsv.exe		1460	20036	13	285	0.031	0.000
C:\Windows\system32\svchost.exe		1488	17864	21	314	0.764	0.296
C:\Program Files\Common Files\Adobe...		1584	21336	4	67	0.000	0.000
C:\Program Files\Bonjour\mDNSResp...		1604	8300	6	104	0.015	0.062
C:\Program Files\GNU\GnuPG\dirmng...		1632	20824	5	84	0.000	0.015
C:\Windows\system32\svchost.exe		1652	8596	5	105	0.000	0.015
C:\Windows\system32\IProsetMonitor....		1696	7332	4	63	0.000	0.015
c:\app\Admin\product\11.2.0\dbhome...		1728	26040	5	193	0.109	0.374
C:\Program Files\McAfee\VirusScan E...		1736	20112	3	59	0.000	0.000
C:\Program Files\McAfee\Common Fra...		1760	9228	12	201	0.156	0.280
C:\Windows\servicing\TrustedInstaller...		1776	12208	5	117	0.031	0.187
C:\Program Files\McAfee\VirusScan E...		1812	372	18	156	5.257	0.202
C:\Windows\system32\mfevtps.exe		1880	7972	5	171	0.093	0.124
C:\Program Files\McAfee\Common Fra...		1892	7648	5	82	0.093	0.015
C:\Program Files\Microsoft SQL Server...		1964	31116	41	331	58.640	37.362
c:\app\Admin\product\11.2.0\dbhome...		2000	5292	3	43	0.000	0.000
c:\app\Admin\product\11.2.0\dbhome...		2020	23616	6	163	0.000	0.062
C:\Program Files\McAfee\VirusScan E...		2052	72148	50	428	75.707	18.579
C:\Program Files\McAfee\VirusScan E...		2096	22236	8	152	0.000	0.156
C:\Windows\system32\conhost.exe		2104	6540	1	31	0.000	0.015
C:\Windows\system32\cmd.exe		2136	10980	1	27	0.015	0.000

Name	Size	Address
C:\Program Files\McAfee\VirusScan Enterprise\EngineServer.exe	0x00006000	0x00400000
C:\Windows\SYSTEM32\ntdll.dll	0x0013C000	0x771D0000
C:\Windows\system32\kernel32.dll	0x000D4000	0x75980000
C:\Windows\system32\KERNELBASE.dll	0x0004A000	0x75430000
C:\Program Files\McAfee\VirusScan Enterprise\mytilus3_worker.dll	0x00044000	0x14710000
C:\Windows\system32\SHFOLDER.dll	0x00005000	0x714A0000
C:\Windows\system32\SHELL32.dll	0x00C4A000	0x76280000
C:\Windows\system32\msvcrt.dll	0x000AC000	0x75AC0000
C:\Windows\system32\SHLWAPI.dll	0x00057000	0x75A60000
C:\Windows\system32\GDI32.dll	0x0004F000	0x75B70000

Processes: 74 (hidden 1)

Choose kill process button:



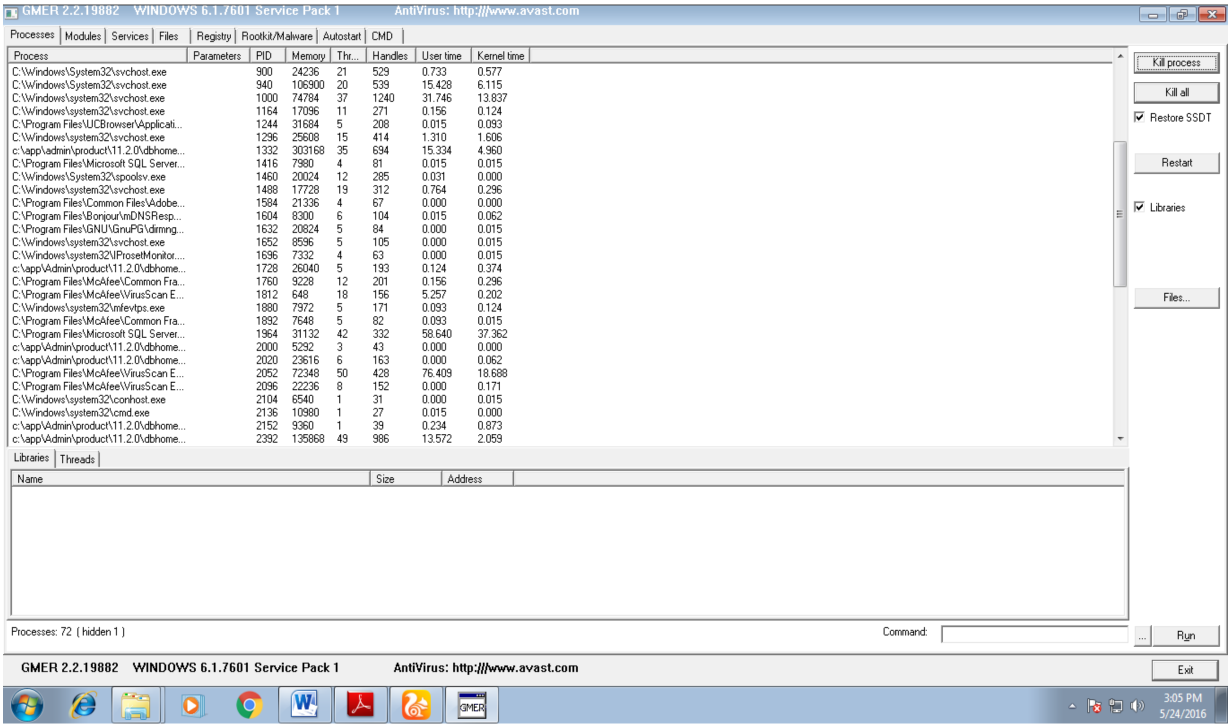
Are you sure you want to kill the process ?

Process	Parameters	PID	Memory	Thr...	Handles	User time	Kernel time
C:\Windows\System32\svchost.exe		900	24224	20	524	0.733	0.561
C:\Windows\System32\svchost.exe		940	106924	20	539	14.976	6.099
C:\Windows\system32\svchost.exe		1000	74796	38	1240	31.746	13.837
C:\Windows\system32\svchost.exe		1164	17096	11	271	0.156	0.124
C:\Program Files\UCBrowser\Applicati...		1244	31684	5	208	0.015	0.093
C:\Windows\system32\svchost.exe		1296	25608	15	415	1.294	1.591
c:\app\admin\product\11.2.0\dbhome...		1332	301292	33	673	15.303	4.898
C:\Program Files\Microsoft SQL Server...		1416	7980	4	81	0.015	0.015
C:\Windows\System32\spoolsv.exe		1460	20024	12	285	0.031	0.000
C:\Windows\system32\svchost.exe		1488	17832	18	310	0.764	0.296
C:\Program Files\Common Files\Adobe...		1584	21336	4	67	0.000	0.000
C:\Program Files\Bonjour\mDNSResp...		1604	8300	6	104	0.015	0.062
C:\Program Files\GNU\GnuPG\dirmng...		1632	20824	5	84	0.000	0.015
C:\Windows\system32\svchost.exe		1652	8596	5	105	0.000	0.015
C:\Windows\system32\IProsetMonitor....		1696	7332	4	63	0.000	0.015
c:\app\Admin\product\11.2.0\dbhome...		1728	26040	5	193	0.109	0.374
C:\Program Files\McAfee\VirusScan E...		1736	20112	3	59	0.000	0.000
C:\Program Files\McAfee\Common Fra...		1760	9228	12	201	0.156	
C:\Windows\servicing\TrustedInstaller...		1776	12196	4	113	0.031	
C:\Program Files\McAfee\VirusScan E...		1812	372	18	156	5.257	
C:\Windows\system32\mfevtps.exe		1880	7972	5	171	0.093	
C:\Program Files\McAfee\Common Fra...		1892	7648	5	82	0.093	
C:\Program Files\Microsoft SQL Server...		1964	31116	41	331	58.640	
c:\app\Admin\product\11.2.0\dbhome...		2000	5292	3	43	0.000	
c:\app\Admin\product\11.2.0\dbhome...		2020	23616	6	163	0.000	
C:\Program Files\McAfee\VirusScan E...		2052	72012	50	428	76.097	
C:\Program Files\McAfee\VirusScan E...		2096	22236	8	152	0.000	
C:\Windows\system32\conhost.exe		2104	6540	1	31	0.000	
C:\Windows\system32\cmd.exe		2136	10980	1	27	0.015	

Name	Size	Address
C:\Program Files\McAfee\VirusScan Enterprise\EngineServer.exe	0x00006000	0x00400000
C:\Windows\SYSTEM32\ntdll.dll	0x0013C000	0x771D0000
C:\Windows\system32\kernel32.dll	0x000D4000	0x75980000
C:\Windows\system32\KERNELBASE.dll	0x0004A000	0x75430000
C:\Program Files\McAfee\VirusScan Enterprise\mytilus3_worker.dll	0x00044000	0x14710000
C:\Windows\system32\SHFOLDER.dll	0x00005000	0x714A0000
C:\Windows\system32\SHELL32.dll	0x00C4A000	0x76280000
C:\Windows\system32\msvcrt.dll	0x000AC000	0x75AC0000
C:\Windows\system32\SHLWAPI.dll	0x00057000	0x75A60000
C:\Windows\system32\GDI32.dll	0x0004F000	0x75B70000

Processes: 74 (hidden 1)

After killing the unwanted processes:



GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 AntiVirus: http:///www.avast.com

Process	Parameters	PID	Memory	Thr...	Handles	User time	Kernel time
C:\Windows\System32\svchost.exe		900	24236	21	529	0.733	0.577
C:\Windows\System32\svchost.exe		940	106900	20	539	15.428	6.115
C:\Windows\system32\svchost.exe		1000	74784	37	1240	31.746	13.837
C:\Windows\system32\svchost.exe		1164	17096	11	271	0.156	0.124
C:\Program Files\UCBrowser\Applicati...		1244	31684	5	208	0.015	0.093
C:\Windows\system32\svchost.exe		1296	25608	15	414	1.310	1.606
c:\app\admin\product\11.2.0\dbhome...		1332	303168	35	694	15.334	4.960
C:\Program Files\Microsoft SQL Server...		1416	7980	4	81	0.015	0.015
C:\Windows\System32\spoolsv.exe		1460	20024	12	285	0.031	0.000
C:\Windows\system32\svchost.exe		1488	17728	19	312	0.764	0.296
C:\Program Files\Common Files\Adobe...		1584	21336	4	67	0.000	0.000
C:\Program Files\Bonjour\mDNSResp...		1604	8300	6	104	0.015	0.062
C:\Program Files\GNU\GnuPG\dirmng...		1632	20824	5	84	0.000	0.015
C:\Windows\system32\svchost.exe		1652	8596	5	105	0.000	0.015
C:\Windows\system32\IProsetMonitor....		1696	7332	4	63	0.000	0.015
c:\app\Admin\product\11.2.0\dbhome...		1728	26040	5	193	0.124	0.374
C:\Program Files\McAfee\Common Fra...		1760	9228	12	201	0.156	0.296
C:\Program Files\McAfee\VirusScan E...		1812	648	18	156	5.257	0.202
C:\Windows\system32\mfevtps.exe		1880	7972	5	171	0.093	0.124
C:\Program Files\McAfee\Common Fra...		1892	7648	5	82	0.093	0.015
C:\Program Files\Microsoft SQL Server...		1964	31132	42	332	58.640	37.362
c:\app\Admin\product\11.2.0\dbhome...		2000	5292	3	43	0.000	0.000
c:\app\Admin\product\11.2.0\dbhome...		2020	23616	6	163	0.000	0.062
C:\Program Files\McAfee\VirusScan E...		2052	72348	50	428	76.409	18.688
C:\Program Files\McAfee\VirusScan E...		2096	22236	8	152	0.000	0.171
C:\Windows\system32\conhost.exe		2104	6540	1	31	0.000	0.015
C:\Windows\system32\cmd.exe		2136	10980	1	27	0.015	0.000
c:\app\Admin\product\11.2.0\dbhome...		2152	9360	1	39	0.234	0.873
c:\app\Admin\product\11.2.0\dbhome...		2392	135868	49	986	13.572	2.059

☑ Restore SSDT

☑ Libraries

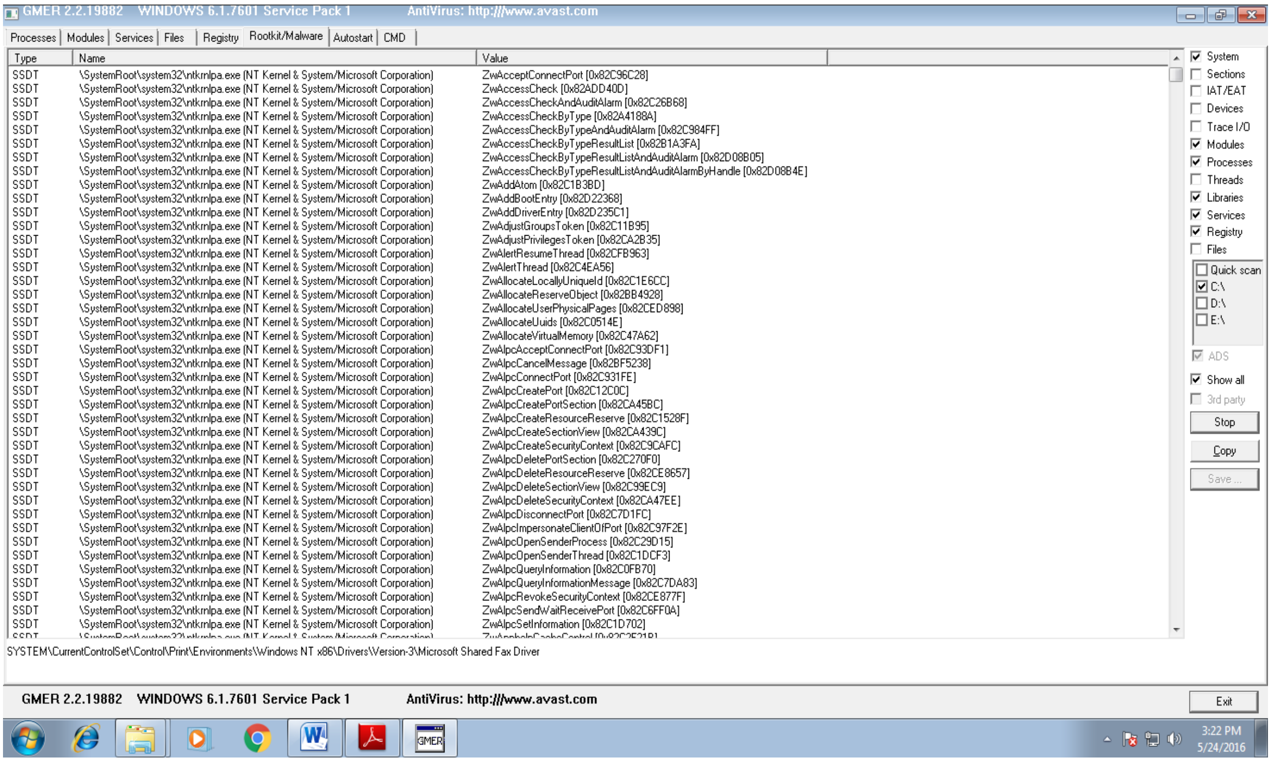
Name	Size	Address

Processes: 72 (hidden 1)

Command:

GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 AntiVirus: http:///www.avast.com

Click rootkit / malware tab to scan the local drives selected



GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 AntiVirus: http:///www.avast.com

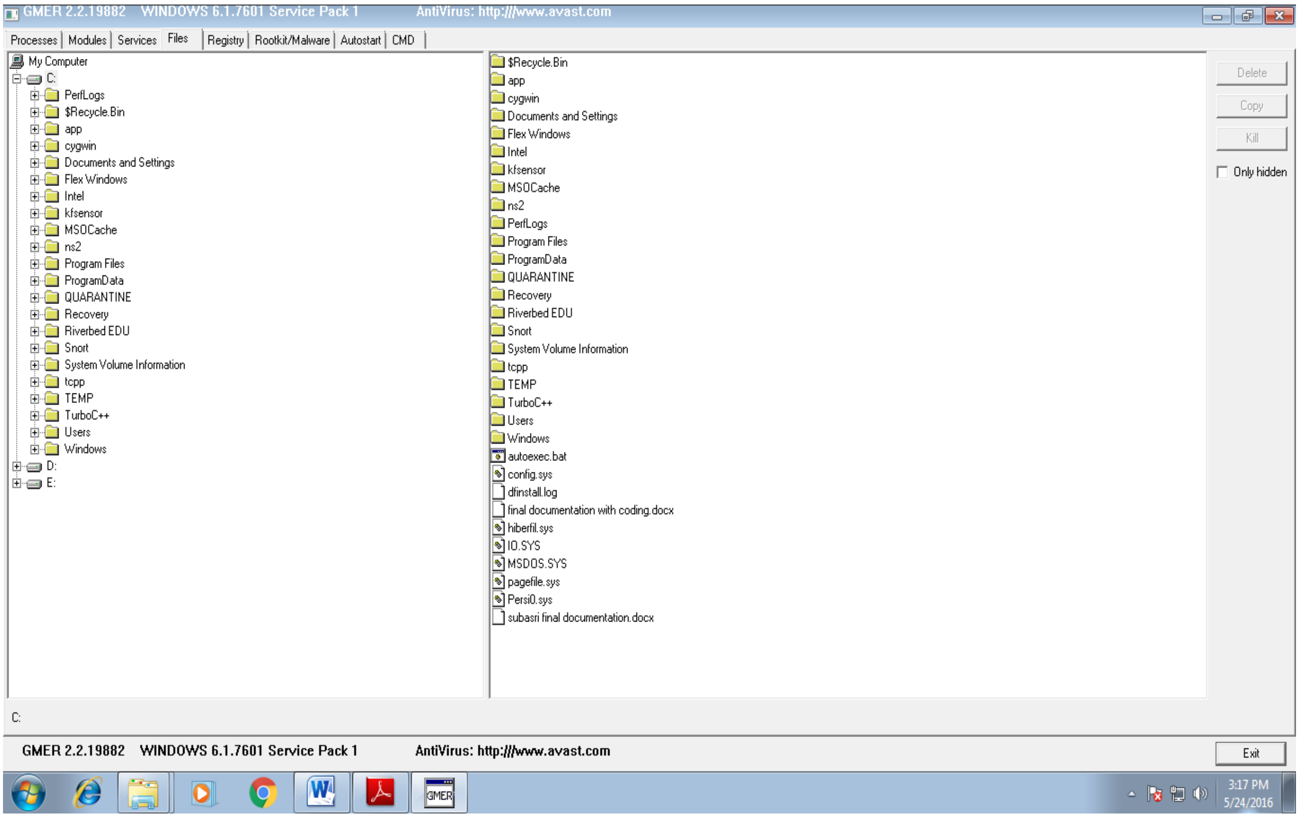
Type	Name	Value
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAcceptConnectPort [0x82C96C28]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAccessCheck [0x82ADD40D]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAccessCheckAndAuditAlarm [0x82C26B68]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAccessCheckByType [0x82A4188A]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAccessCheckByTypeAndAuditAlarm [0x82C984FF]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAccessCheckByTypeResultList [0x82B1A3FA]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAccessCheckByTypeResultListAndAuditAlarm [0x82D08B05]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAccessCheckByTypeResultListAndAuditAlarmByHandle [0x82D08B4E]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAddAtom [0x82C1B3BD]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAddBootEntry [0x82D22368]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAddDriverEntry [0x82D235C1]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAdjustGroupsToken [0x82C11B95]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAdjustPrivilegesToken [0x82CA2B35]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlertResumeThread [0x82CFB963]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlertThread [0x82C4EA56]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAllocateLocallyUniqueId [0x82C1E6CC]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAllocateReserveObject [0x82BB4928]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAllocateUserPhysicalPages [0x82CED898]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAllocateUuids [0x82C0514E]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAllocateVirtualMemory [0x82C47A62]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcAcceptConnectPort [0x82C93DF1]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcCancelMessage [0x82BF5238]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcConnectPort [0x82C931FE]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcCreatePort [0x82C12C0C]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcCreatePortSection [0x82CA45BC]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcCreateResourceReserve [0x82C1528F]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcCreateSectionView [0x82CA439C]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcCreateSecurityContext [0x82C9CAFC]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcDeletePortSection [0x82C270F0]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcDeleteResourceReserve [0x82CE8657]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcDeleteSectionView [0x82C99EC9]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcDeleteSecurityContext [0x82CA47EE]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcDisconnectPort [0x82C7D1FC]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcImpersonateClientOfPort [0x82C97F2E]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcOpenSenderProcess [0x82C29D15]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcOpenSenderThread [0x82C1DCF3]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcQueryInformation [0x82C0FB70]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcQueryInformationMessage [0x82C7DA83]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcRevokeSecurityContext [0x82CE877F]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcSendWaitReceivePort [0x82C6FF0A]
SSDT	\SystemRoot\system32\ntkrnlpa.exe (NT Kernel & System/Microsoft Corporation)	ZwAlpcSetInformation [0x82C1D702]

☑ System
□ Sections
□ IAT/EAT
□ Devices
□ Trace I/O
☑ Modules
☑ Processes
□ Threads
☑ Libraries
☑ Services
☑ Registry
□ Files
□ Quick scan
☑ C:\
□ D:\
□ E:\
☑ ADS
☑ Show all
□ 3rd party

SYSTEM\CurrentControlSet\Control\Print\Environments\Windows NT x86\Drivers\Version-3\Microsoft Shared Fax Driver

GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 AntiVirus: http:///www.avast.com

Click on the files tab to view all the files including hidden files:



GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 AntiVirus: http://www.avast.com

```
My Computer
  C:
    PerfLogs
    $Recycle.Bin
    app
    cygwin
    Documents and Settings
    Flex Windows
    Intel
    kfsensor
    MSOCache
    ns2
    Program Files
    ProgramData
    QUARANTINE
    Recovery
    Riverbed EDU
    Snort
    System Volume Information
    tcpp
    TEMP
    TurboC++
    Users
    Windows
  D:
  E:
```

```
$Recycle.Bin
app
cygwin
Documents and Settings
Flex Windows
Intel
kfsensor
MSOCache
ns2
PerfLogs
Program Files
ProgramData
QUARANTINE
Recovery
Riverbed EDU
Snort
System Volume Information
tcpp
TEMP
TurboC++
Users
Windows
autoexec.bat
config.sys
dfinstall.log
final documentation with coding.docx
hiberfil.sys
IO.SYS
MSDOS.SYS
pagefile.sys
Persi0.sys
subasri final documentation.docx
```

C:

GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 AntiVirus: http://www.avast.com

RESULT:

Thus, the installation of rootkits and study about the variety of options using rootkit tool was executed and verified successfully.