EX. NO: 06

INSTALLATION OF ROOTKITS

AIM:

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.

INTRODUCTION:

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, Disable, System, Boot.

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

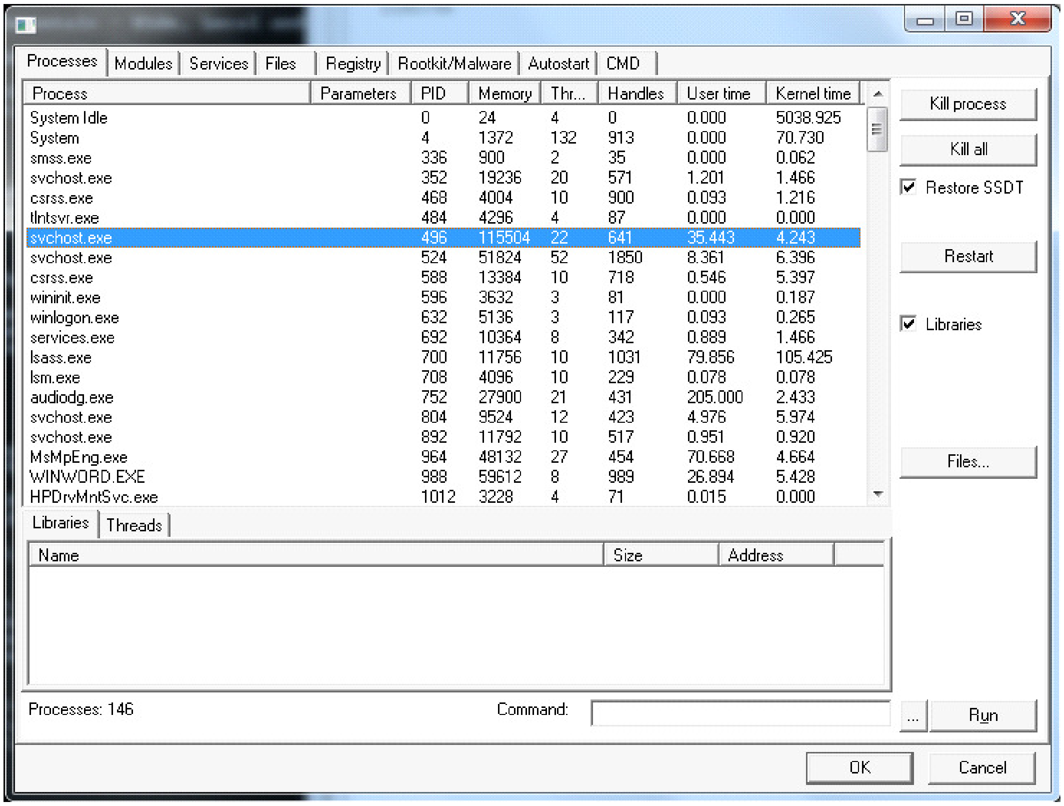
STEP-7: Registry displays Hkey_Current_user and Hkey_Local_Machine.

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

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

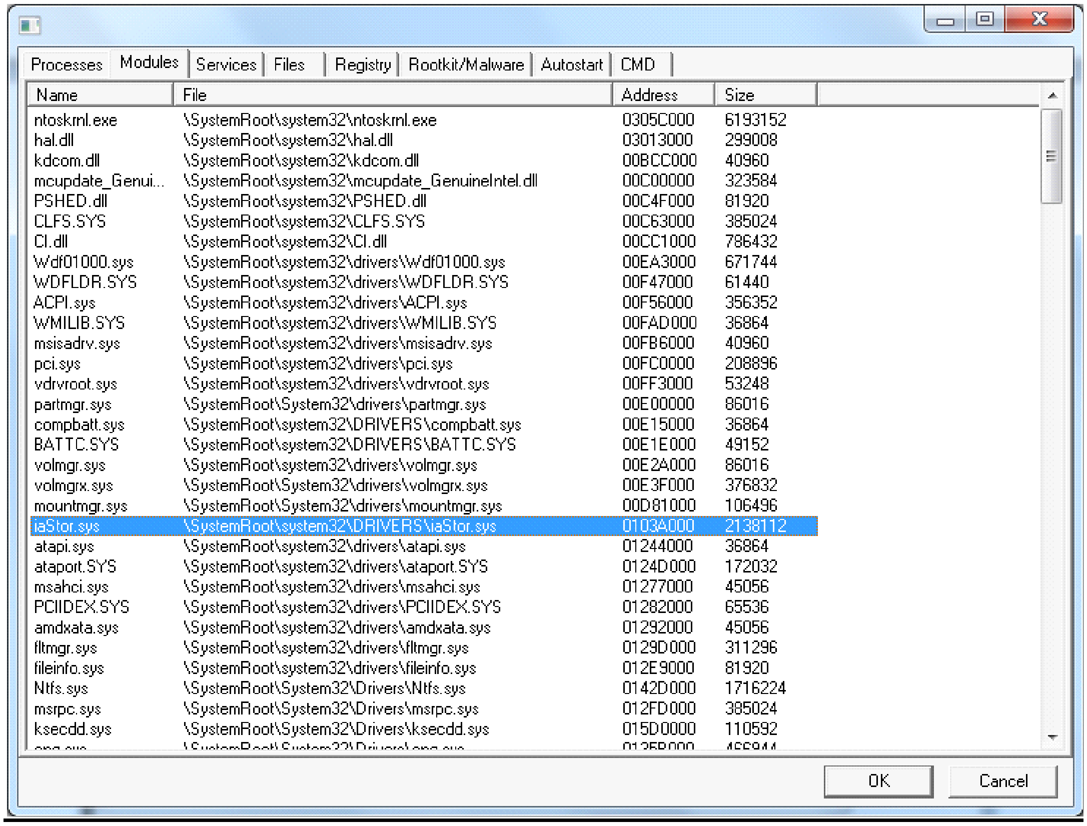
STEP-10:CMD allows the user to interact with command line utilities or Registry

SCREENSHOTS:

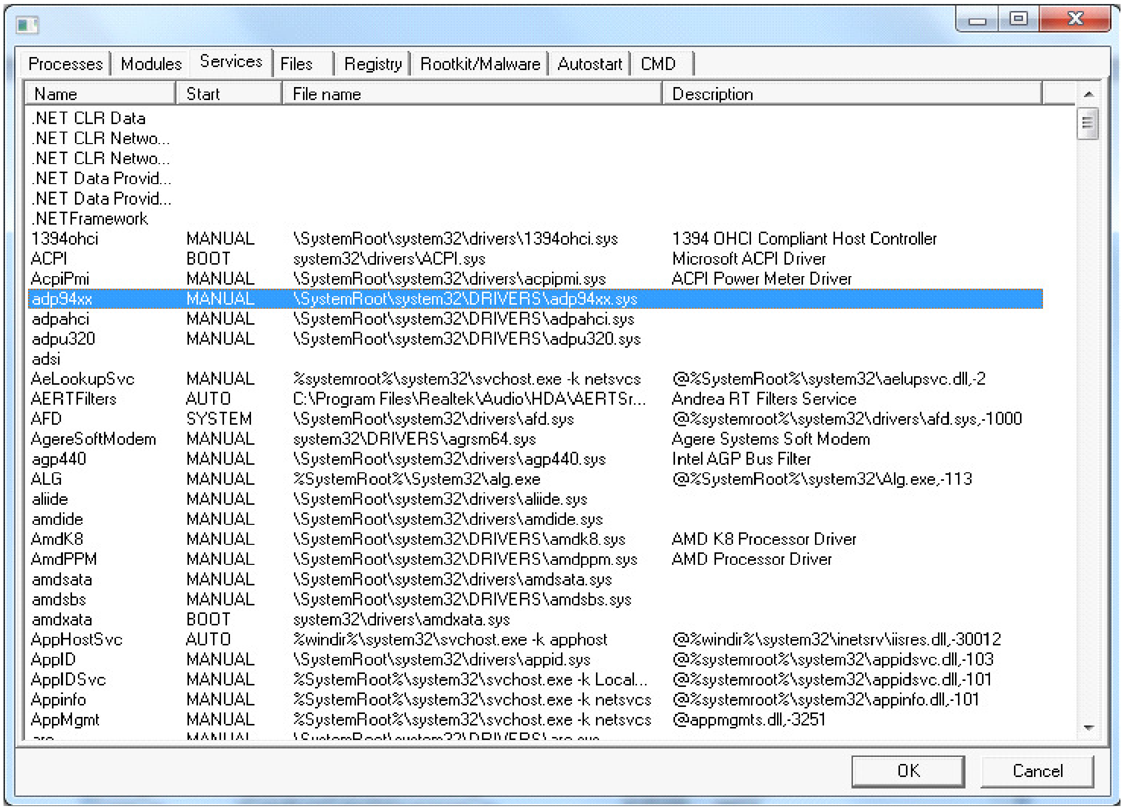


Process	Parameters	PID	Memory	Thr...	Handles	User time	Kernel time
System Idle		0	24	4	0	0.000	5038.925
System		4	1372	132	913	0.000	70.730
smss.exe		336	900	2	35	0.000	0.062
svchost.exe		352	19236	20	571	1.201	1.466
csrss.exe		468	4004	10	900	0.093	1.216
tlntsvr.exe		484	4296	4	87	0.000	0.000
svchost.exe		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

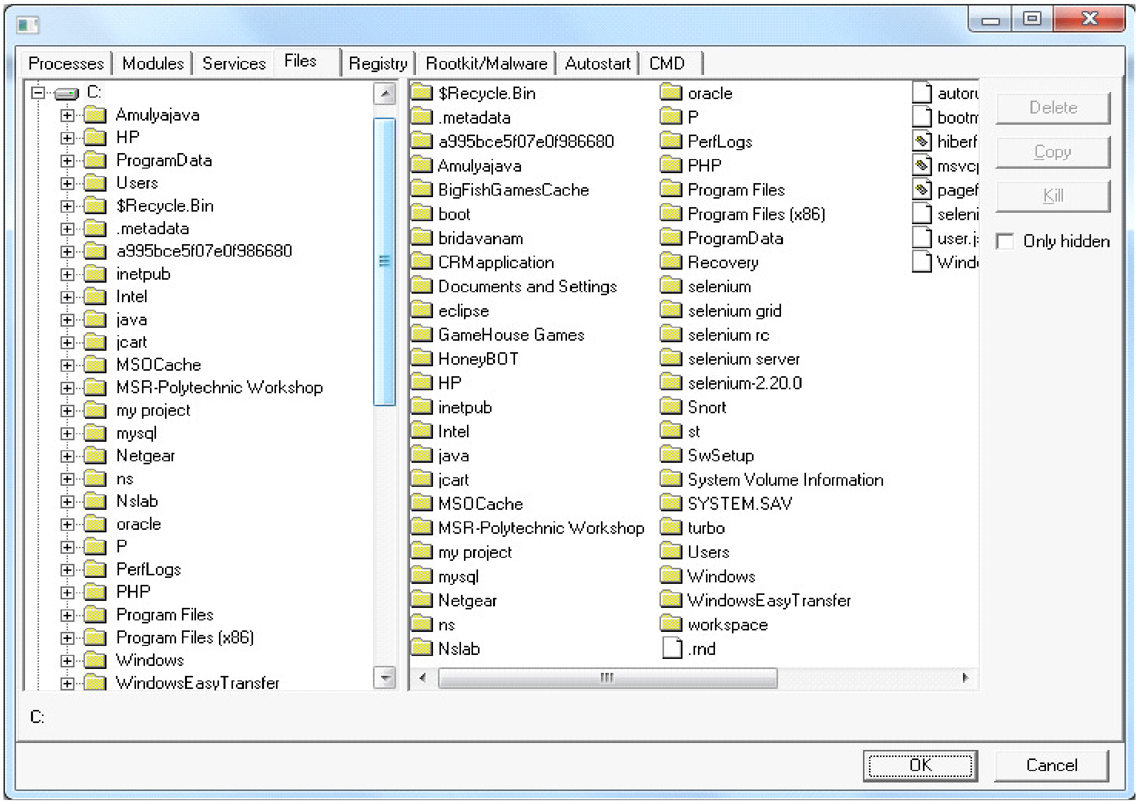
Processes: 146



Name	File	Address	Size
ntoskrnl.exe	\SystemRoot\system32\ntoskrnl.exe	0305C000	6193152
hal.dll	\SystemRoot\system32\hal.dll	03013000	299008
kdcom.dll	\SystemRoot\system32\kdcom.dll	00BCC000	40960
mcupdate_Genui...	\SystemRoot\system32\mcupdate_GenuineIntel.dll	00C00000	323584
PSHED.dll	\SystemRoot\system32\PSHED.dll	00C4F000	81920
CLFS.SYS	\SystemRoot\system32\CLFS.SYS	00C63000	385024
CI.dll	\SystemRoot\system32\CI.dll	00CC1000	786432
Wdf01000.sys	\SystemRoot\system32\drivers\Wdf01000.sys	00EA3000	671744
WDFLDR.SYS	\SystemRoot\system32\drivers\WDFLDR.SYS	00F47000	61440
ACPI.sys	\SystemRoot\system32\drivers\ACPI.sys	00F56000	356352
WMILIB.SYS	\SystemRoot\system32\drivers\WMILIB.SYS	00FAD000	36864
msisadrv.sys	\SystemRoot\system32\drivers\msisadrv.sys	00FB6000	40960
pci.sys	\SystemRoot\system32\drivers\pci.sys	00FC0000	208896
vdrvroot.sys	\SystemRoot\system32\drivers\vdrvroot.sys	00FF3000	53248
partmgr.sys	\SystemRoot\System32\drivers\partmgr.sys	00E00000	86016
compbatt.sys	\SystemRoot\system32\DRIVERS\compbatt.sys	00E15000	36864
BATTC.SYS	\SystemRoot\system32\DRIVERS\BATTC.SYS	00E1E000	49152
volmgr.sys	\SystemRoot\system32\drivers\volmgr.sys	00E2A000	86016
volmgrx.sys	\SystemRoot\System32\drivers\volmgrx.sys	00E3F000	376832
mountmgr.sys	\SystemRoot\System32\drivers\mountmgr.sys	00D81000	106496
iaStor.sys	\SystemRoot\system32\DRIVERS\iaStor.sys	0103A000	2138112
atapi.sys	\SystemRoot\system32\drivers\atapi.sys	01244000	36864
ataport.SYS	\SystemRoot\system32\drivers\ataport.SYS	0124D000	172032
msahci.sys	\SystemRoot\system32\drivers\msahci.sys	01277000	45056
PCIIDEX.SYS	\SystemRoot\system32\drivers\PCIIDEX.SYS	01282000	65536
amdxata.sys	\SystemRoot\system32\drivers\amdxata.sys	01292000	45056
fltmgr.sys	\SystemRoot\system32\drivers\fltmgr.sys	0129D000	311296
fileinfo.sys	\SystemRoot\system32\drivers\fileinfo.sys	012E9000	81920
Ntfs.sys	\SystemRoot\System32\Drivers\Ntfs.sys	0142D000	1716224
msrpc.sys	\SystemRoot\System32\Drivers\msrpc.sys	012FD000	385024
ksecdd.sys	\SystemRoot\System32\Drivers\ksecdd.sys	015D0000	110592



Name	Start	File name	Description
.NET CLR Data			
.NET CLR Netwo...			
.NET CLR Netwo...			
.NET Data Provid...			
.NET Data Provid...			
.NETFramework			
1394ohci	MANUAL	\SystemRoot\system32\drivers\1394ohci.sys	1394 OHCI Compliant Host Controller
ACPI	BOOT	system32\drivers\ACPI.sys	Microsoft ACPI Driver
AcpiPmi	MANUAL	\SystemRoot\system32\drivers\acpipmi.sys	ACPI Power Meter Driver
adp94xx	MANUAL	\SystemRoot\system32\DRIVERS\adp94xx.sys	
adpahci	MANUAL	\SystemRoot\system32\DRIVERS\adpahci.sys	
adpu320	MANUAL	\SystemRoot\system32\DRIVERS\adpu320.sys	
adsi			
AeLookupSvc	MANUAL	%systemroot%\system32\svchost.exe -k netsvcs	@%SystemRoot%\system32\aelupsvc.dll,-2
AERTFilters	AUTO	C:\Program Files\Realtek\Audio\HDA\AERTSr...	Andrea RT Filters Service
AFD	SYSTEM	\SystemRoot\system32\drivers\afd.sys	@%systemroot%\system32\drivers\afd.sys,-1000
AgereSoftModem	MANUAL	system32\DRIVERS\agrsm64.sys	Agere Systems Soft Modem
agp440	MANUAL	\SystemRoot\system32\drivers\agp440.sys	Intel AGP Bus Filter
ALG	MANUAL	%SystemRoot%\System32\alg.exe	@%SystemRoot%\system32\Alg.exe,-113
aliide	MANUAL	\SystemRoot\system32\drivers\aliide.sys	
amdide	MANUAL	\SystemRoot\system32\drivers\amdide.sys	
AmdK8	MANUAL	\SystemRoot\system32\DRIVERS\amdk8.sys	AMD K8 Processor Driver
AmdPPM	MANUAL	\SystemRoot\system32\DRIVERS\amdppm.sys	AMD Processor Driver
amdsata	MANUAL	\SystemRoot\system32\drivers\amdsata.sys	
amdsbs	MANUAL	\SystemRoot\system32\DRIVERS\amdsbs.sys	
amdxata	BOOT	system32\drivers\amdxata.sys	
AppHostSvc	AUTO	%windir%\system32\svchost.exe -k apphost	@%windir%\system32\inetsrv\iisres.dll,-30012
AppID	MANUAL	\SystemRoot\system32\drivers\appid.sys	@%systemroot%\system32\appidsvc.dll,-103
AppIDSvc	MANUAL	%SystemRoot%\system32\svchost.exe -k Local...	@%systemroot%\system32\appidsvc.dll,-101
Appinfo	MANUAL	%SystemRoot%\system32\svchost.exe -k netsvcs	@%systemroot%\system32\appinfo.dll,-101
AppMgmt	MANUAL	%SystemRoot%\system32\svchost.exe -k netsvcs	@appmgmts.dll,-3251



```
C:
  Amulyajava
  HP
  ProgramData
  Users
  $Recycle.Bin
  .metadata
  a995bce5f07e0f986680
  inetpub
  Intel
  java
  jcart
  MSOCache
  MSR-Polytechnic Workshop
  my project
  mysql
  Netgear
  ns
  Nslab
  oracle
  P
  PerfLogs
  PHP
  Program Files
  Program Files (x86)
  Windows
  WindowsEasyTransfer
```

```
$Recycle.Bin              oracle                     autoru
.metadata                 P                          bootm
a995bce5f07e0f986680      PerfLogs                   hiberf
Amulyajava                PHP                        msvc
BigFishGamesCache         Program Files              pagef
boot                      Program Files (x86)        seleni
bridavanam                ProgramData                user.j
CRMapplication            Recovery                   Wind
Documents and Settings    selenium
eclipse                   selenium grid
GameHouse Games           selenium rc
HoneyBOT                  selenium server
HP                        selenium-2.20.0
inetpub                   Snort
Intel                     st
java                      SwSetup
jcart                     System Volume Information
MSOCache                  SYSTEM.SAV
MSR-Polytechnic Workshop  turbo
my project                Users
mysql                     Windows
Netgear                   WindowsEasyTransfer
ns                        workspace
Nslab                     .rnd
```

C:

RESULT:

Thus the study of installation of Rootkit software and its variety of options were developed successfully.

EX. NO: 08

WORKING WITH SNORT TOOL TO DEMONSTRATE INTRUSION DETECTION SYSTEM

AIM:

Snort is an open source network intrusion detection system (NIDS) and it is a packet sniffer that monitors network traffic in real time.

INTRODUCTION:

INTRUSION DETECTION SYSTEM :

Intrusion detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level. Intrusion detection systems fall into two basic categories:

- ✓ Signature-based intrusion detection systems
- ✓ Anomaly detection systems.

Intruders have signatures, like computer viruses, that can be detected using software. You try to find data packets that contain any known intrusion-related signatures or anomalies related to Internet protocols. Based upon a set of signatures and rules, the detection system is able to find and log suspicious activity and generate alerts.

Anomaly-based intrusion detection usually depends on packet anomalies present in protocol header parts. In some cases these methods produce better results compared to signature-based IDS. Usually an intrusion detection system captures data from the network and applies its rules to that data or detects anomalies in it. Snort is primarily a rule-based IDS, however input plug-ins are present to detect anomalies in protocol headers.

SNORT TOOL:

Snort is based on libpcap (for library packet capture), a tool that is widely used in TCP/IPtraffic sniffers and analyzers. Through protocolanalysis and content searching and matching, Snort detects attack methods, including denial of service, buffer overflow, CGI attacks, stealthport scans, and SMB probes. When suspicious behavior is detected, Snort sends a real-time alert to syslog, a separate 'alerts' file, or to apop-up window.

Snort is currently the most popular free network intrusion detection software. The advantages of Snort are numerous. According to the snort web site, “It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflow, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more" (Caswell).

One of the advantages of Snort is its ease of configuration. Rules are very flexible, easily written, and easily inserted into the rule base. If a new exploit or attack is found a rule for the attack can be added to the rule base in a matter of seconds. Another advantage of snort is that it allows for raw packet data analysis.

SNORT can be configured to run in three modes:

1. Sniffer mode
2. Packet Logger mode
3. Network Intrusion Detection System mode

1. **Sniffer mode**
   - ✓ **Snort –v** Print out the TCP/IP packets header on the screen
   - ✓ **Snort –vd** show the TCP/IP ICMP header with application data in transmit
2. **Packet Logger mode**
   - ✓ **snort –dev –l c:\log** [create this directory in the C drive] and snort will automatically know to go into packet logger mode, it collects every packet it sees and places it in log directory.
   - ✓ **snort –dev –l c:\log –h ipaddress/24**:This rule tells snort that you want to print out the data link and TCP/IP headers as well as application data into the log directory. snort –l c:\log –b This is binary mode logs everything into a single file.
3. **Network Intrusion Detection System mode**
   - ✓ **snort –d c:\log –h ipaddress/24 –c snort.conf** This is a configuration file applies rule to each packet to decide it an action based upon the rule type in the file.
   - ✓ **Snort –d –h ipaddress/24 –l c:\log –c snort.conf** This will cnfigure snort to run in its most basic NIDS form, logging packets that trigger rules specifies in the snort.conf.

PROCEDURE:

STEP-1: Sniffer mode→ snort –v → Print out the TCP/IP packets header on the screen.

STEP-2: Snort –vd → Show the TCP/IP ICMP header with application data in transit.

STEP-3: Packet Logger mode → snort –dev –l c:\log [create this directory in the C drive] and snort will automatically know to go into packet logger mode, it collects every packet it sees and places it in log directory.

STEP-4: snort –dev –l c:\log –h ipaddress/24 → This rule tells snort that you want to print out the data link and TCP/IP headers as well as application data into the log directory.

STEP-5: snort –l c:\log –b → this binary mode logs everything into a single file.

STEP-6: Network Intrusion Detection System mode → snort –d c:\log –h ipaddress/24 –c snort.conf → This is a configuration file that applies rule to each packet to decide it an action based upon the rule type in the file.

STEP-7: snort –d –h ip address/24 –l c:\log –c snort.conf → This will configure snort to run in its most basic NIDS form, logging packets that trigger rules specifies in the snort.conf.

STEP-8: Download SNORT from snort.org. Install snort with or without database support.

STEP-9: Select all the components and Click Next. Install and Close.

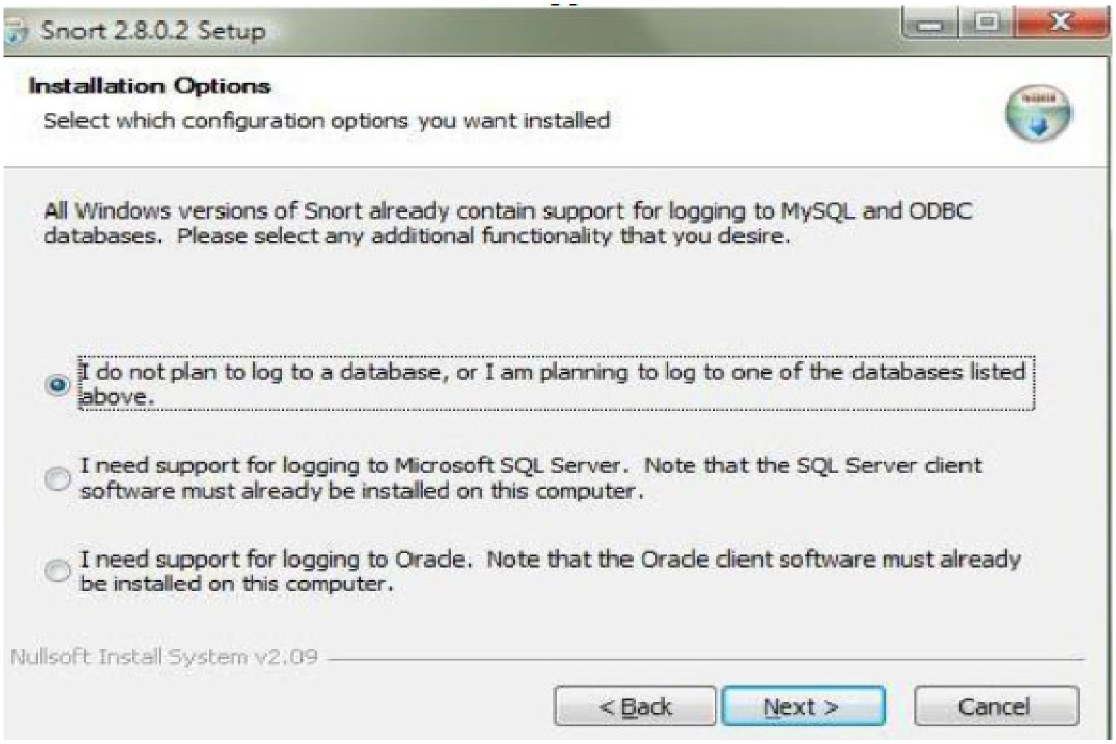
STEP-10: Skip the WinPcap driver installation.

STEP-11: Add the path variable in windows environment variable by selecting new classpath.

STEP-12: Create a path variable and point it at snort.exe variable name → path and variable value → c:\snort\bin.

STEP-13: Click OK button and then close all dialog boxes. Open command prompt and type the following commands:

INSTALLATION PROCESS :



Snort 2.8.0.2 Setup

Installation Options

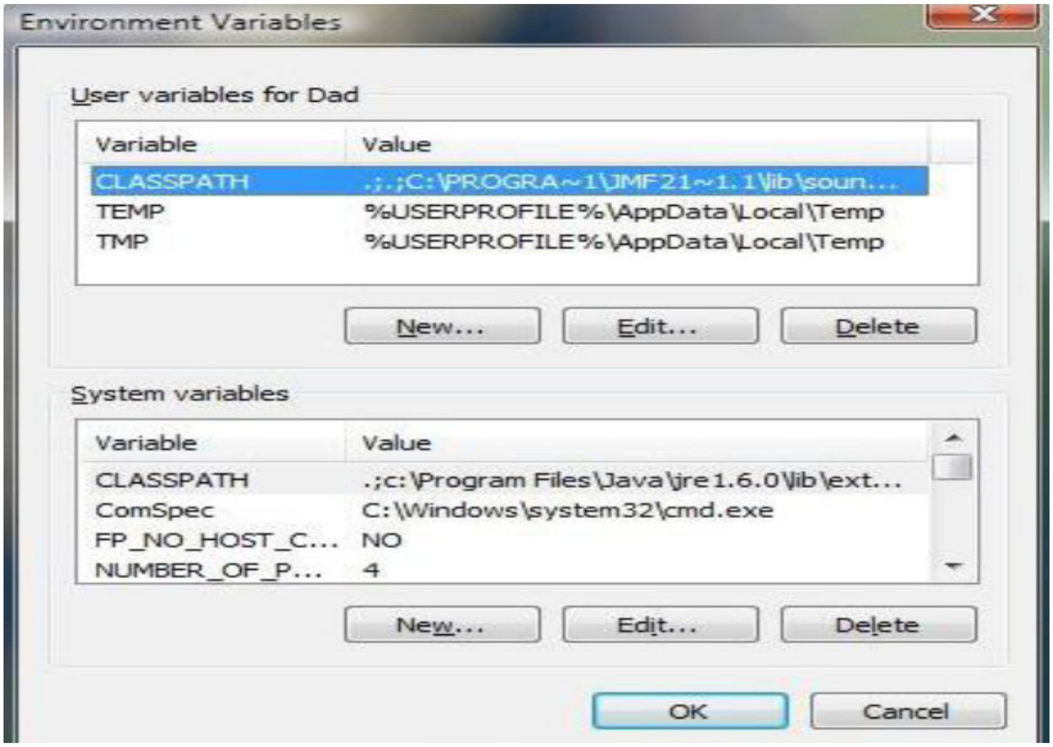
Select which configuration options you want installed

All Windows versions of Snort already contain support for logging to MySQL and ODBC databases. Please select any additional functionality that you desire.

● I do not plan to log to a database, or I am planning to log to one of the databases listed above.

○ I need support for logging to Microsoft SQL Server. Note that the SQL Server client software must already be installed on this computer.

○ I need support for logging to Oracle. Note that the Oracle client software must already be installed on this computer.



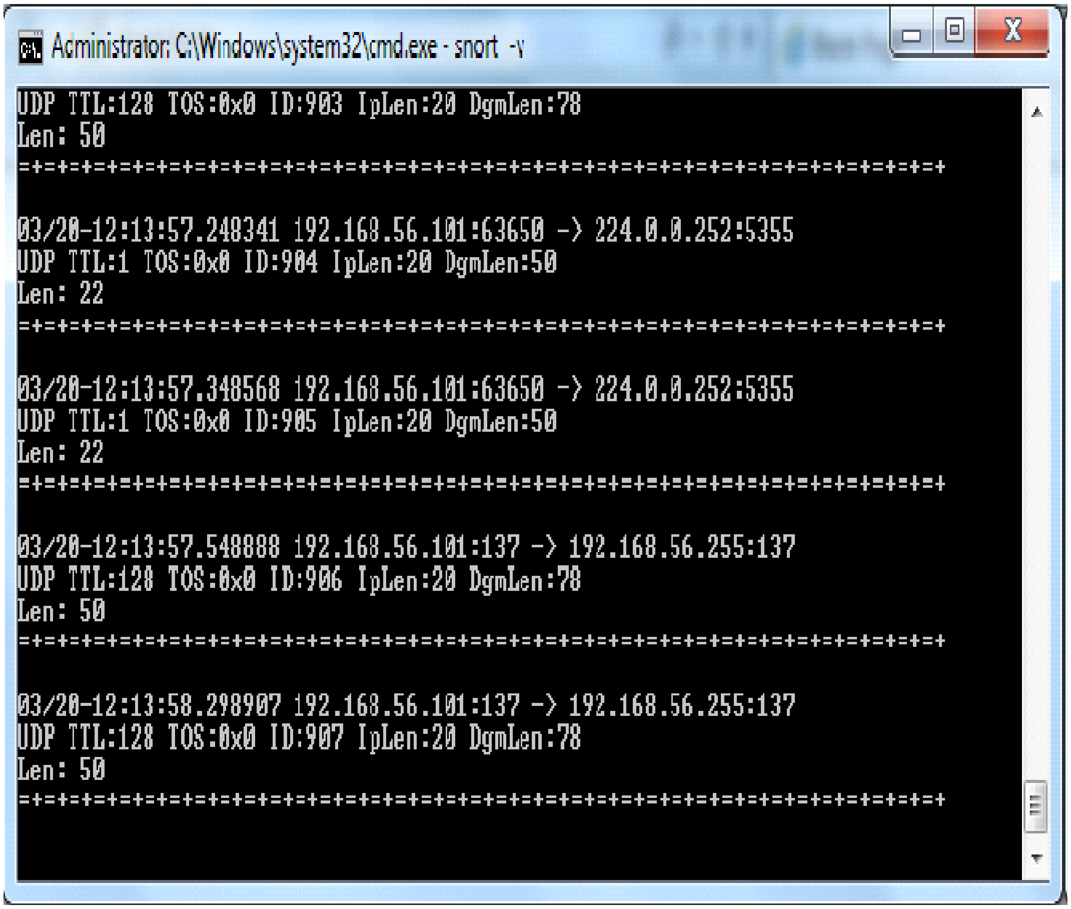
Environment Variables

User variables for Dad

Variable	Value
CLASSPATH	.;.;C:\PROGRA~1\JMF21~1.1\lib\soun...
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
CLASSPATH	.;c:\Program Files\Java\jre1.6.0\lib\ext...
ComSpec	C:\Windows\system32\cmd.exe
FP_NO_HOST_C...	NO
NUMBER_OF_P...	4



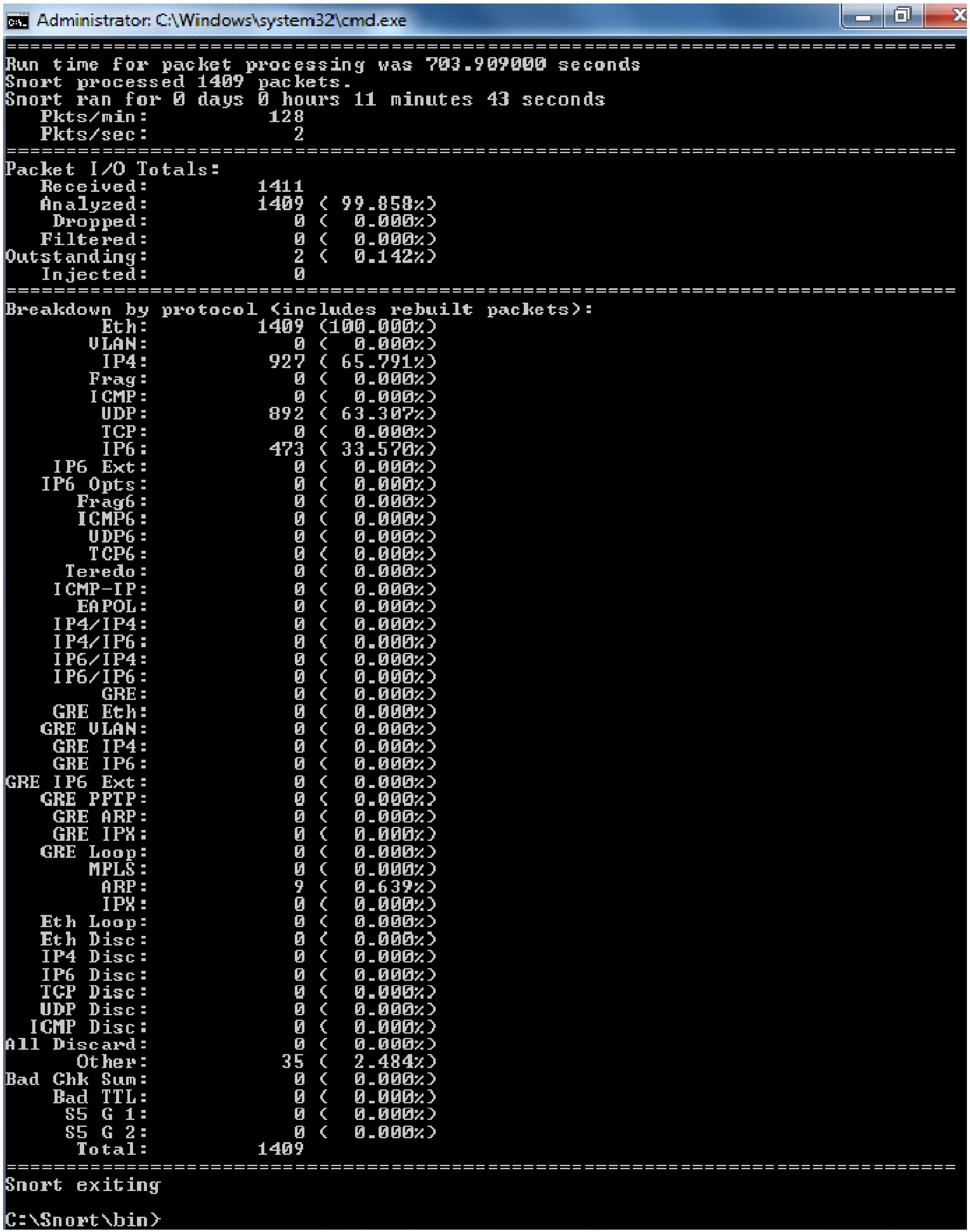
```
UDP TTL:128 TOS:0x0 ID:903 IpLen:20 DgmLen:78
Len: 50
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/20-12:13:57.248341 192.168.56.101:63650 -> 224.0.0.252:5355
UDP TTL:1 TOS:0x0 ID:904 IpLen:20 DgmLen:50
Len: 22
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/20-12:13:57.348568 192.168.56.101:63650 -> 224.0.0.252:5355
UDP TTL:1 TOS:0x0 ID:905 IpLen:20 DgmLen:50
Len: 22
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/20-12:13:57.548888 192.168.56.101:137 -> 192.168.56.255:137
UDP TTL:128 TOS:0x0 ID:906 IpLen:20 DgmLen:78
Len: 50
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/20-12:13:58.298907 192.168.56.101:137 -> 192.168.56.255:137
UDP TTL:128 TOS:0x0 ID:907 IpLen:20 DgmLen:78
Len: 50
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```



```
===============================================================================
Run time for packet processing was 703.909000 seconds
Snort processed 1409 packets.
Snort ran for 0 days 0 hours 11 minutes 43 seconds
   Pkts/min:          128
   Pkts/sec:            2
===============================================================================
Packet I/O Totals:
   Received:         1411
   Analyzed:         1409 ( 99.858%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            2 (  0.142%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:         1409 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          927 ( 65.791%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:          892 ( 63.307%)
        TCP:            0 (  0.000%)
        IP6:          473 ( 33.570%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            9 (  0.639%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:           35 (  2.484%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:         1409
===============================================================================
Snort exiting

C:\Snort\bin>
```

RESULT:

Thus the demonstration of the instruction detection using Snort tool was done successfully.