Ex. No : 9 **Date :**	**Demonstration of Intrusion Detection System(IDS)**

AIM:

To demonstrate Intrusion Detection System (IDS) using Snort software tool.

STEPS ON CONFIGURING AND INTRUSION DETECTION:

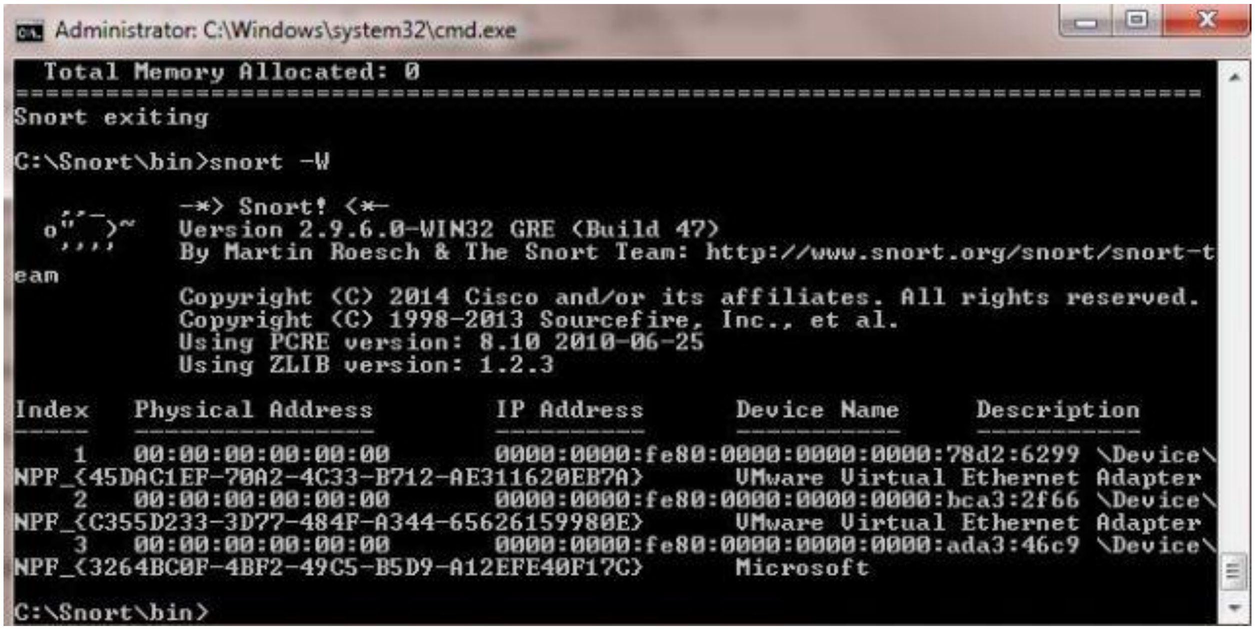
1. Download Snort from the Snort.org website. (http://www.snort.org/snort-downloads)
2. Download Rules(https://www.snort.org/snort-rules). You must register to get the rules. (You should download these often)
3. Double click on the .exe to install snort. This will install snort in the “C:\Snort” folder.It is important to have WinPcap (https://www.winpcap.org/install/) installed
4. Extract the Rules file. You will need WinRAR for the .gz file.
5. Copy all files from the “rules” folder of the extracted folder. Now paste the rules into *“C:\Snort\rules”* folder.
6. Copy “snort.conf” file from the “etc” folder of the extracted folder. You must paste it into “C:\Snort\etc” folder. Overwrite any existing file. Remember if you modify your snort.conf file and download a new file, you must modify it for Snort to work.
7. Open a command prompt (cmd.exe) and navigate to folder “C:\Snort\bin” folder. (at the Prompt, type cd\snort\bin)
8. To start (execute) snort in sniffer mode use following command:

```
snort -dev -i 3
```

-i indicates the interface number. You must pick the correct interface number. In my case, it is 3.
-dev is used to run snort to capture packets on your network.

To check the interface list, use following command:

```
snort   -W
```



```
  Total Memory Allocated: 0
===============================================================================
Snort exiting

C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.6.0-WIN32 GRE (Build 47)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Index   Physical Address        IP Address       Device Name     Description
-----   ----------------        ----------       -----------     -----------
    1   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:78d2:6299 \Device\
NPF_{45DAC1EF-70A2-4C33-B712-AE311620EB7A}       VMware Virtual Ethernet Adapter
    2   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:bca3:2f66 \Device\
NPF_{C355D233-3D77-484F-A344-65626159980E}       VMware Virtual Ethernet Adapter
    3   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:ada3:46c9 \Device\
NPF_{3264BC0F-4BF2-49C5-B5D9-A12EFE40F17C}       Microsoft

C:\Snort\bin>
```

Finding an interface

You can tell which interface to use by looking at the Index number and finding Microsoft. As you can see in the above example, the other interfaces are for VMWare. My interface is 3.

9. To run snort in IDS mode, you will need to configure the file “snort.conf” according to your network environment.
10. To specify the network address that you want to protect in snort.conf file, look for the following line.
var HOME_NET 192.168.1.0/24 (You will normally see any here)
11. You may also want to set the addresses of DNS_SERVERS, if you have some on your network.

Example:

example snort
12. Change the RULE_PATH variable to the path of rules folder.
var RULE_PATH c:\snort\rules

path to rules

13. Change the path of all library files with the name and path on your system. and you must change the path of snort_dynamicpreprocessorvariable.
C:\Snort\lib\snort_dynamiccpreprocessor
You need to do this to all library files in the “C:\Snort\lib” folder. The old path might be: “/usr/local/lib/…”.you will need to replace that path with your system path. Using C:\Snort\lib
14. Change the path of the “dynamicengine” variable value in the “snort.conf” file..
Example:
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

15 Add the paths for “include classification.config” and “include reference.config” files.
include c:\snort\etc\classification.config
include c:\snort\etc\reference.config
16. Remove the comment (#) on the line to allow ICMP rules, if it is commented with a #.
include $RULE_PATH/icmp.rules
17. You can also remove the comment of ICMP-info rules comment, if it is commented.
include $RULE_PATH/icmp-info.rules
18. To add log files to store alerts generated by snort, search for the “output log” test in snort.conf and add the following line:
outputalert_fast: snort-alerts.ids
19. Comment (add a #) the whitelist $WHITE_LIST_PATH/white_list.rules and the blacklist

Change the nested_ipinner , \ to nested_ip inner #, \
20. Comment out (#) following lines:
#preprocessor normalize_ip4
#preprocessor normalize_tcp: ipsecn stream
#preprocessor normalize_icmp4
#preprocessor normalize_ip6
#preprocessor normalize_icmp6

21. Save the “snort.conf” file.
22. To start snort in IDS mode, run the following command:

```
snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3
```

(Note: 3 is used for my interface card)

If a log is created, select the appropriate program to open it. You can use WordPard or NotePad++ to read the file.

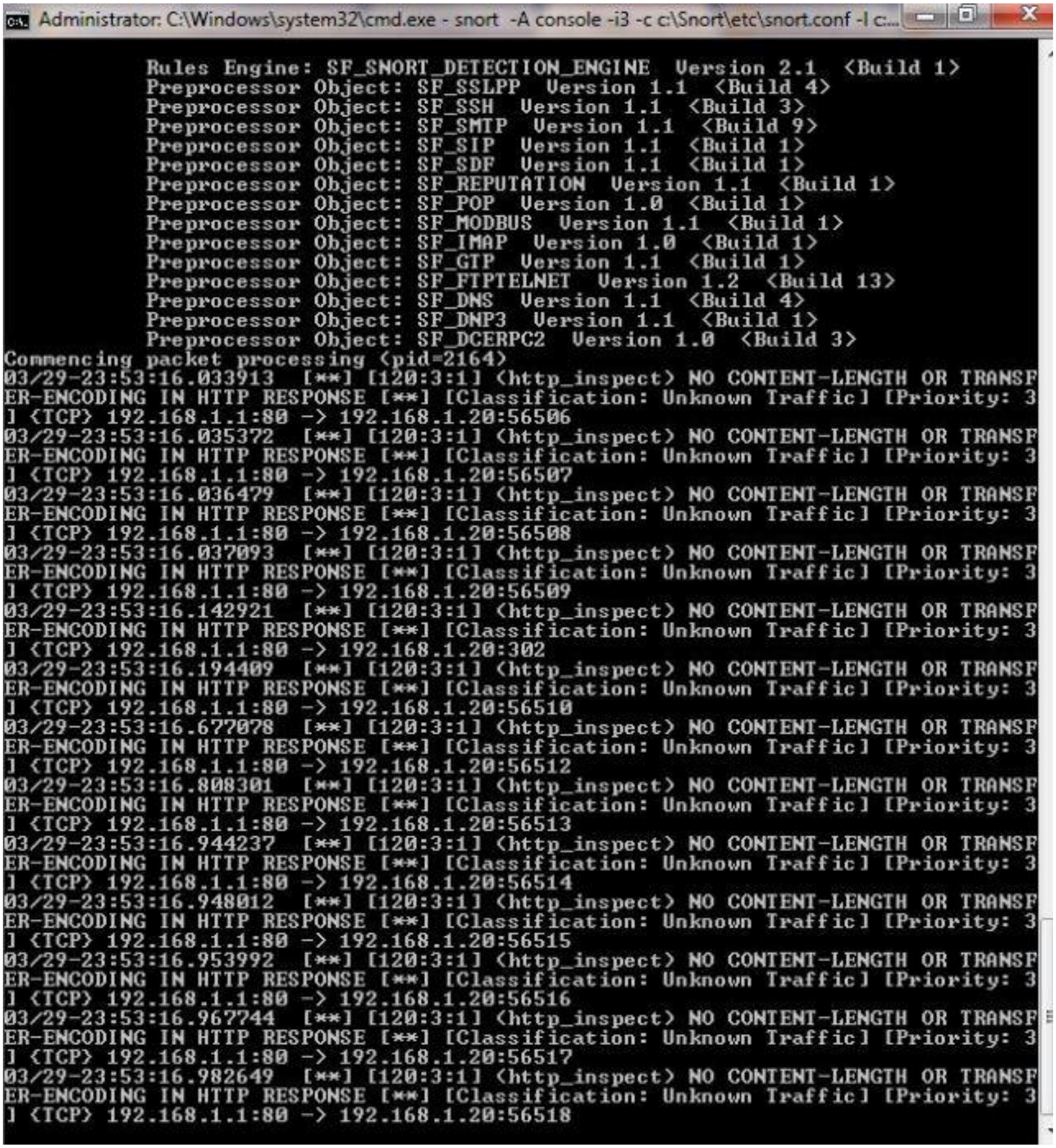
To generate Log files in ASCII mode, you can use following command while running snort in IDS mode:

```
snort -A console -i3 -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii
```

23. Scan the computer that is running snort from another computer by using PING or NMap (ZenMap).

After scanning or during the scan you can check the snort-alerts.ids file in the log folder to insure it is logging properly. You will see IP address folders appear.

Snort monitoring traffic –



```
Administrator: C:\Windows\system32\cmd.exe - snort  -A console -i3 -c c:\Snort\etc\snort.conf -l c...
```

```
           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=2164)
03/29-23:53:16.033913  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56506
03/29-23:53:16.035372  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56507
03/29-23:53:16.036479  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56508
03/29-23:53:16.037093  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56509
03/29-23:53:16.142921  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:302
03/29-23:53:16.194409  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56510
03/29-23:53:16.677078  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56512
03/29-23:53:16.808301  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56513
03/29-23:53:16.944237  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56514
03/29-23:53:16.948012  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56515
03/29-23:53:16.953992  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56516
03/29-23:53:16.967744  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56517
03/29-23:53:16.982649  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56518
```

RESULT:

Thus the Intrusion Detection System(IDS) has been demonstrated by using the Open Source Snort Intrusion Detection Tool.

Ex. No : 10 **Date :**	**Exploring N-Stalker, a Vulnerability Assessment Tool**

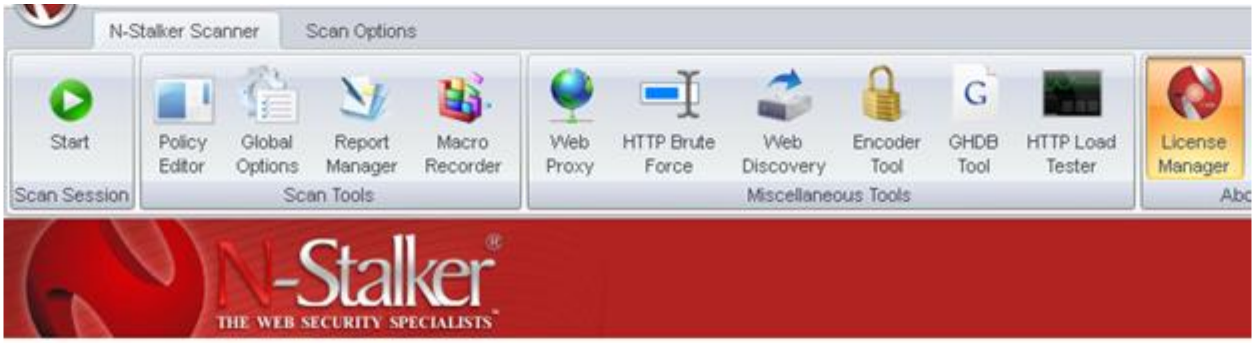
AIM:

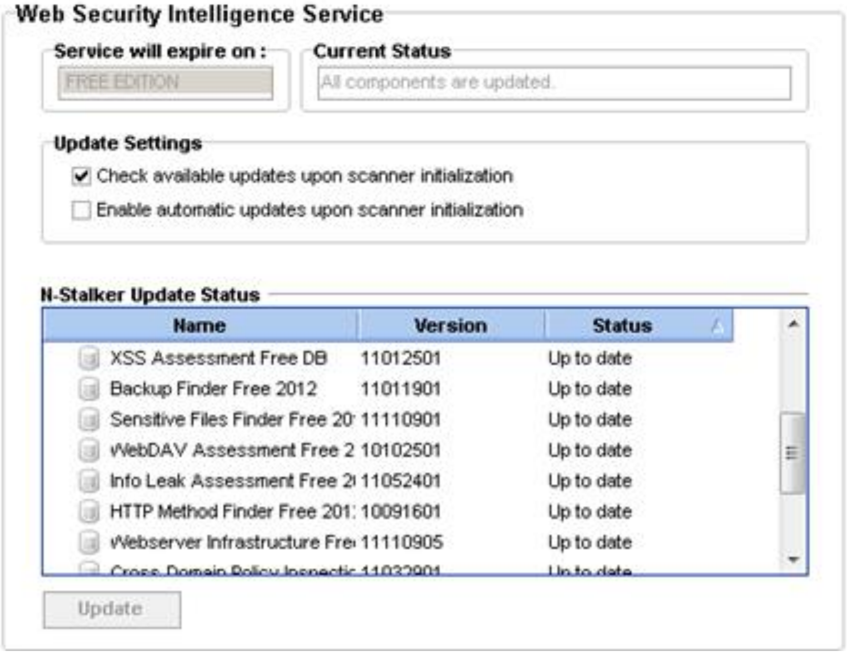
To download the N-Stalker Vulnerability Assessment Tool and exploring the features.

EXPLORING N-STALKER:

- N-Stalker Web Application Security Scanner is a Web security assessment tool.
- It incorporates with a well-known N-Stealth HTTP Security Scanner and 35,000 Web attack signature database.
- This tool also comes in both free and paid version.
- Before scanning the target, go to “License Manager” tab, perform the update.
- Once update, you will note the status as up to date.
- You need to download and install N-Stalker from www.nstalker.com.

1. Start N-Stalker from a Windows computer. The program is installedunder Start ➪ Programs ➪ N-Stalker ➪ N-Stalker Free Edition.
2. Enter a host address or a range of addresses to scan.
3. Click Start Scan.
4. After the scan completes, the N-Stalker Report Manager will prompt
5. you to select a format for the resulting report as choose Generate HTML.
6. Review the HTML report for vulnerabilities.




Web Security Intelligence Service

Service will expire on : FREE EDITION

Current Status: All components are updated.

Update Settings

☑ Check available updates upon scanner initialization

☐ Enable automatic updates upon scanner initialization

N-Stalker Update Status

Name	Version	Status
XSS Assessment Free DB	11012501	Up to date
Backup Finder Free 2012	11011901	Up to date
Sensitive Files Finder Free 20	11110901	Up to date
WebDAV Assessment Free 2	10102501	Up to date
Info Leak Assessment Free 2	11052401	Up to date
HTTP Method Finder Free 201	10091601	Up to date
Webserver Infrastructure Fre	11110905	Up to date
Cross Domain Policy Inspectio	11032901	Up to date

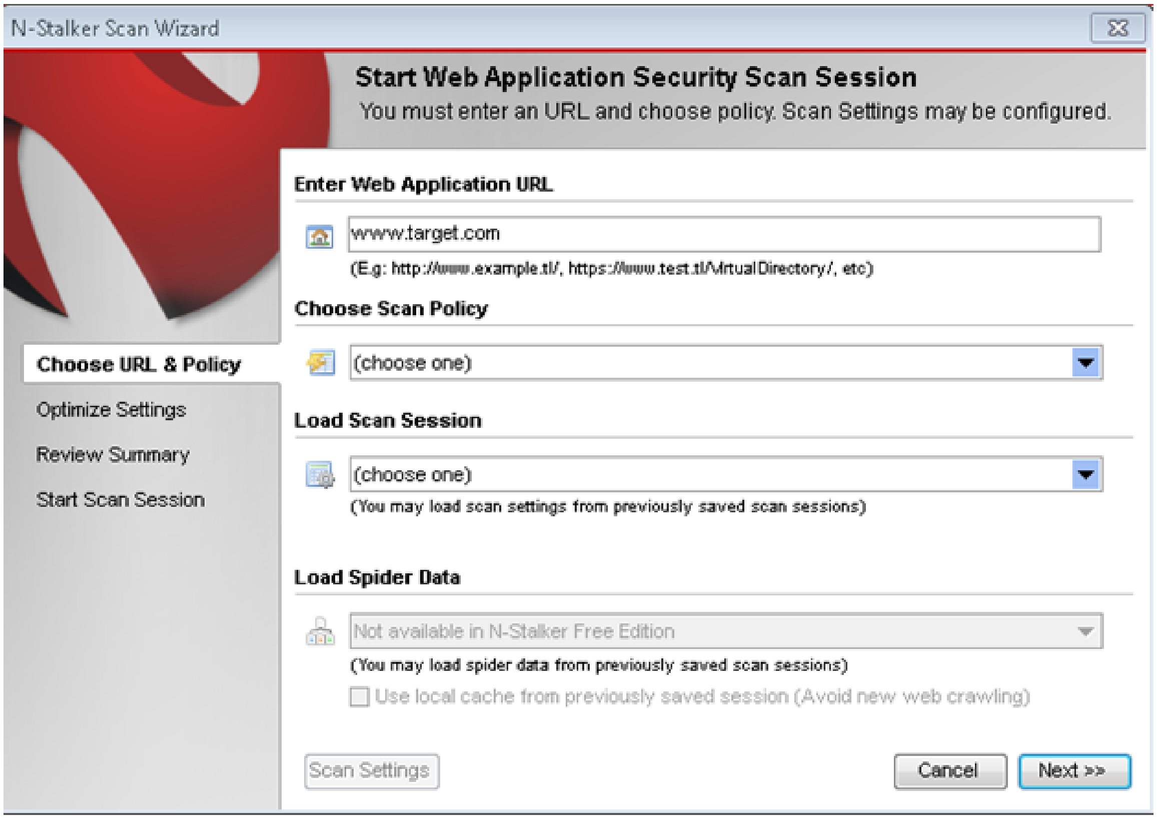
Now goto “Scan Session”, enter the target URL.

In scan policy, you can select from the four options,

- Manual test which will crawl the website and will be waiting for manual attacks.
- full xss assessment
- owasp policy
- Web server infrastructure analysis.

Once, the option has been selected, next step is “Optimize settings” which will crawl the whole website for further analysis.

In review option, you can get all the information like host information, technologies used, policy name, etc.



Start Web Application Security Scan Session

You must enter an URL and choose policy. Scan Settings may be configured.

Enter Web Application URL

www.target.com

(E.g: http://www.example.tl/, https://www.test.tl/VirtualDirectory/, etc)

Choose Scan Policy

(choose one)

Load Scan Session

(choose one)

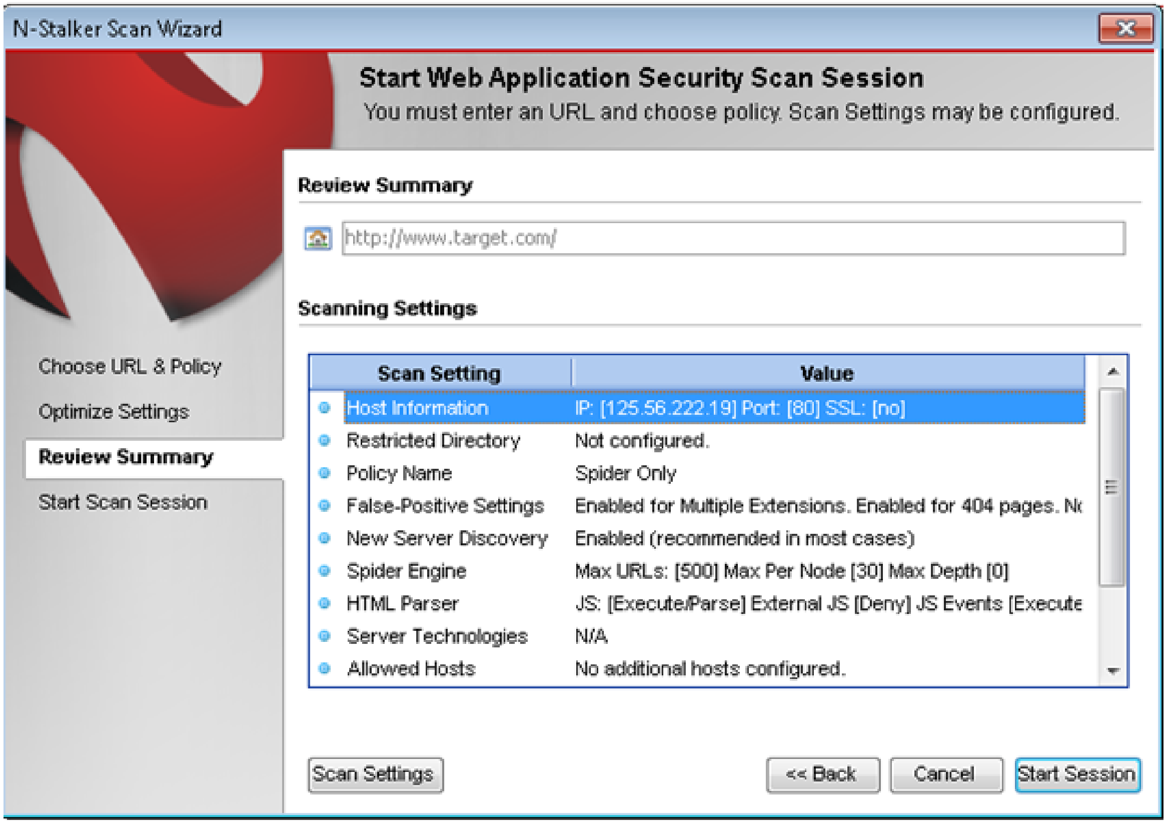
(You may load scan settings from previously saved scan sessions)

Load Spider Data

Not available in N-Stalker Free Edition

(You may load spider data from previously saved scan sessions)

□ Use local cache from previously saved session (Avoid new web crawling)



Start Web Application Security Scan Session

You must enter an URL and choose policy. Scan Settings may be configured.

Review Summary

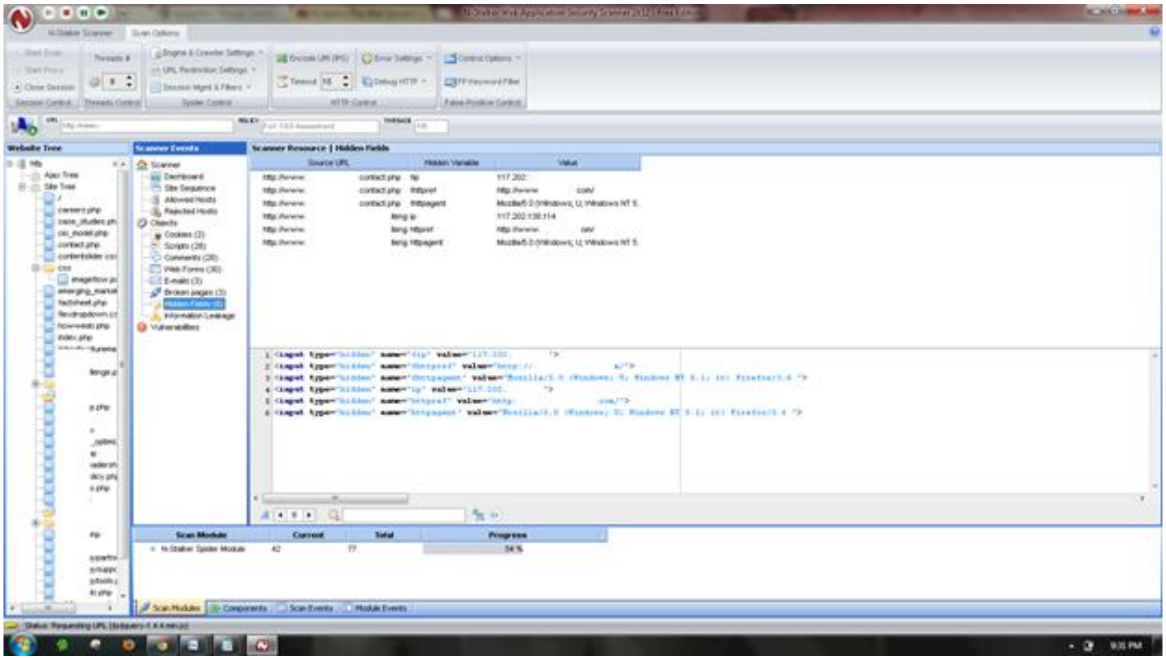
http://www.target.com/

Scanning Settings

Scan Setting	Value
Host Information	IP: [125.56.222.19] Port: [80] SSL: [no]
Restricted Directory	Not configured.
Policy Name	Spider Only
False-Positive Settings	Enabled for Multiple Extensions. Enabled for 404 pages. No
New Server Discovery	Enabled (recommended in most cases)
Spider Engine	Max URLs: [500] Max Per Node [30] Max Depth [0]
HTML Parser	JS: [Execute/Parse] External JS [Deny] JS Events [Execute
Server Technologies	N/A
Allowed Hosts	No additional hosts configured.

Once done, start the session and start the scan.

The scanner will crawl the whole website and will show the scripts, broken pages, hidden fields, information leakage, web forms related information which helps to analyze further.



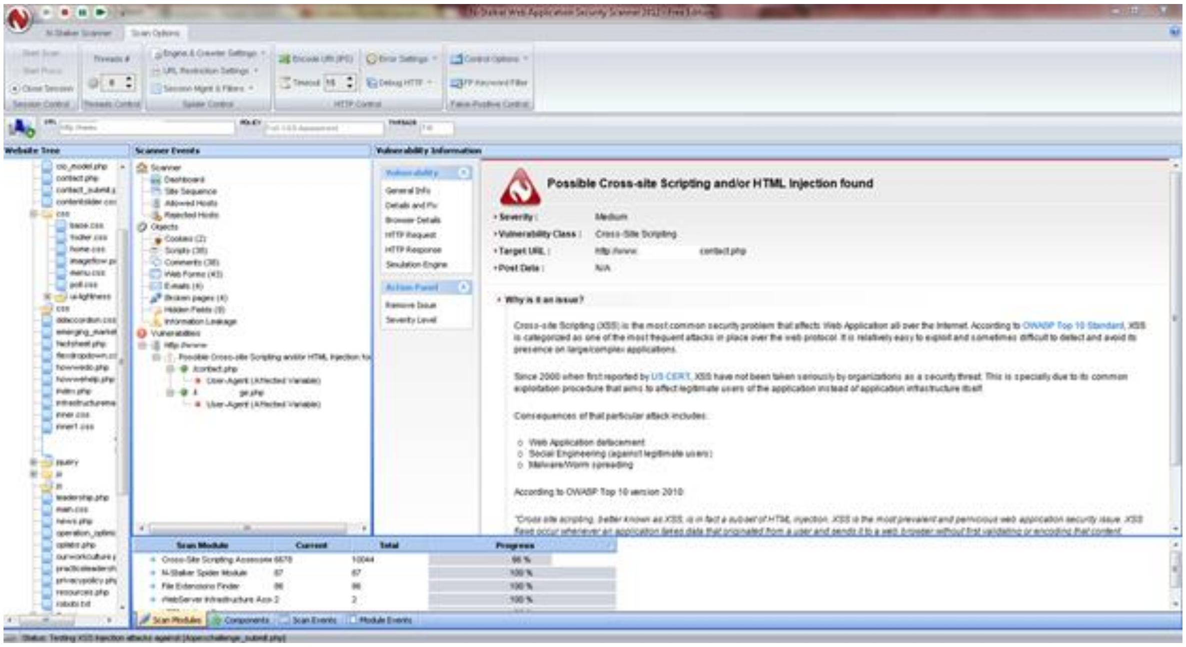
Scanner Resource | Hidden Fields

Source URL	Hidden Variable	Value
http://www. contact.php	fip	117.202.
http://www. contact.php	fhttpref	http://www. .com/
http://www. contact.php	fhttpagent	Mozilla/5.0 (Windows; U; Windows NT 5.
http://www. tieng	ip	117.202.138.114
http://www. tieng	httpref	http://www. .com/
http://www. tieng	httpagent	Mozilla/5.0 (Windows; U; Windows NT 5.

```
<input type="hidden" name="fip" value="117.202.        ">
<input type="hidden" name="fhttpref" value="http://                a/">
<input type="hidden" name="fhttpagent" value="Mozilla/5.0 (Windows; U; Windows NT 5.1; in; Firefox/3.6 ">
<input type="hidden" name="ip" value="117.202.        ">
<input type="hidden" name="httpref" value="http:                 .com/">
<input type="hidden" name="httpagent" value="Mozilla/5.0 (Windows; U; Windows NT 5.1; in; Firefox/3.6 ">
```

Scan Module	Current	Total	Progress
N-Stalker Spider Module	42	77	54 %

Once the scan is completed, the NStalker scanner will show details like severity level, vulnerability class, why is it an issue, the fix for the issue and the URL which is vulnerable to the particular vulnerability?



Possible Cross-site Scripting and/or HTML Injection found

- **Severity :** Medium
- **Vulnerability Class :** Cross-Site Scripting
- **Target URL :** http://www. contact.php
- **Post Data :** N/A

Why is it an issue?

Cross-site Scripting (XSS) is the most common security problem that affects Web Application all over the Internet. According to OWASP Top 10 Standard, XSS is categorized as one of the most frequent attacks in place over the web protocol. It is relatively easy to exploit and sometimes difficult to detect and avoid its presence on large/complex applications.

Since 2000 when first reported by US CERT, XSS have not been taken seriously by organizations as a security threat. This is specially due to its common exploitation procedure that aims to affect legitimate users of the application instead of application infrastructure itself.

Consequences of that particular attack includes:

- Web Application defacement
- Social Engineering (against legitimate users)
- Malware/Worm spreading

According to OWASP Top 10 version 2010:

"Cross site scripting, better known as XSS, is in fact a subset of HTML injection. XSS is the most prevalent and pernicious web application security issue. XSS flaws occur whenever an application takes data that originated from a user and sends it to a web browser without first validating or encoding that content.

Scan Module	Current	Total	Progress
Cross-Site Scripting Assessme	6878	10044	98 %
N-Stalker Spider Module	67	67	100 %
File Extensions Finder	86	86	100 %
WebServer Infrastructure Ass	2	2	100 %

Status: Testing XSS Injection attacks against [/open/challenge_submit.php]

RESULT:

Thus the N-Stalker Vulnerability Assessment tool has been downloaded, installed and the features has been explored by using a vulnerable website.

Ex. No : 11(a) **Date :**	**Defeating Malware - Building Trojans**

AIM:

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

PROCEDURE:

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,ortrojan, 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*.

CODE:

Trojan.bat

```
@echo off
:x
startmspaint
start notepad
startcmd
start explorer
start control
startcalc
goto x
```

OUTPUT

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

RESULT:

Thus a trojan has been built and the harmness of the trojan viruses has been explored.

Ex. No : 11(b) **Date :**	**Defeating Malware - Rootkit hunter**

AIM:

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

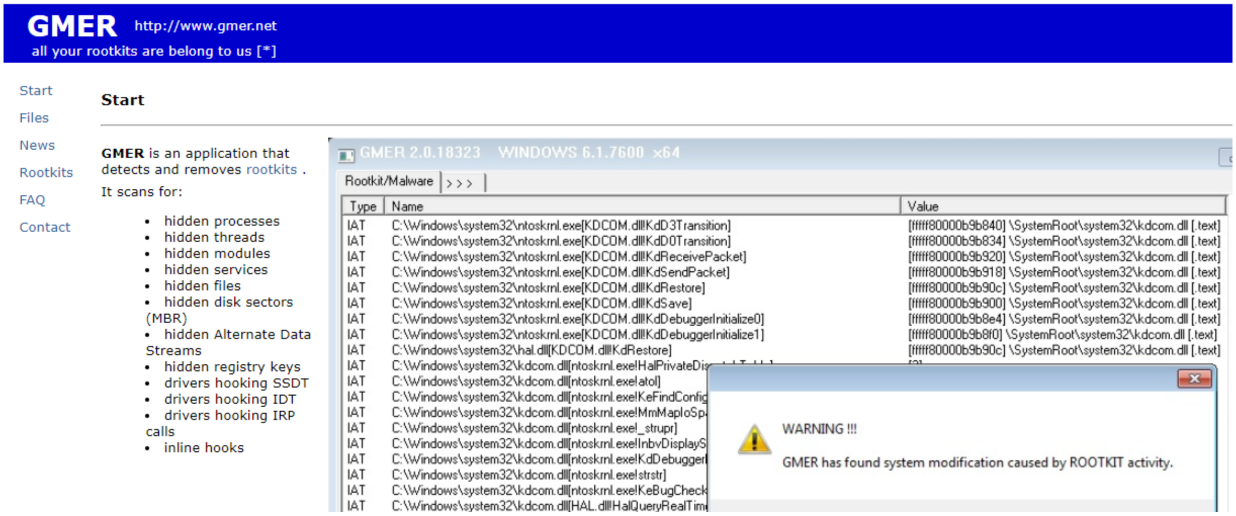
ROOTKIT HUNTER:

- rkhunter (Rootkit Hunter) is a Unix-based tool that scans for rootkits, backdoors and possible 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 almost all UNIX-derived systems.

GMER ROOTKIT TOOL:

- GMER is a software tool written by a Polish researcher PrzemysławGmerek, for detecting 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



GMER is an application that detects and removes rootkits .

It scans for:

- hidden processes
- hidden threads
- hidden modules
- hidden services
- hidden files
- hidden disk sectors (MBR)
- hidden Alternate Data Streams
- hidden registry keys
- drivers hooking SSDT
- drivers hooking IDT
- drivers hooking IRP calls
- inline hooks

```
Type  Name                                                          Value
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdD3Transition]      [fffff80000b9b840] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdD0Transition]      [fffff80000b9b834] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdReceivePacket]     [fffff80000b9b920] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdSendPacket]        [fffff80000b9b918] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdRestore]           [fffff80000b9b90c] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdSave]              [fffff80000b9b900] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdDebuggerInitialize0]  [fffff80000b9b8e4] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdDebuggerInitialize1]  [fffff80000b9b8f0] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\hal.dll[KDCOM.dll!KdRestore]                [fffff80000b9b90c] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!HalPrivateDis
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!atol]
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!KeFindConfig
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!MmMapIoSp
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!_strupr]
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!InbvDisplayS
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!KdDebugger
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!strstr]
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!KeBugCheck
IAT   C:\Windows\system32\kdcom.dll[HAL.dll!HalQueryRealTim
```

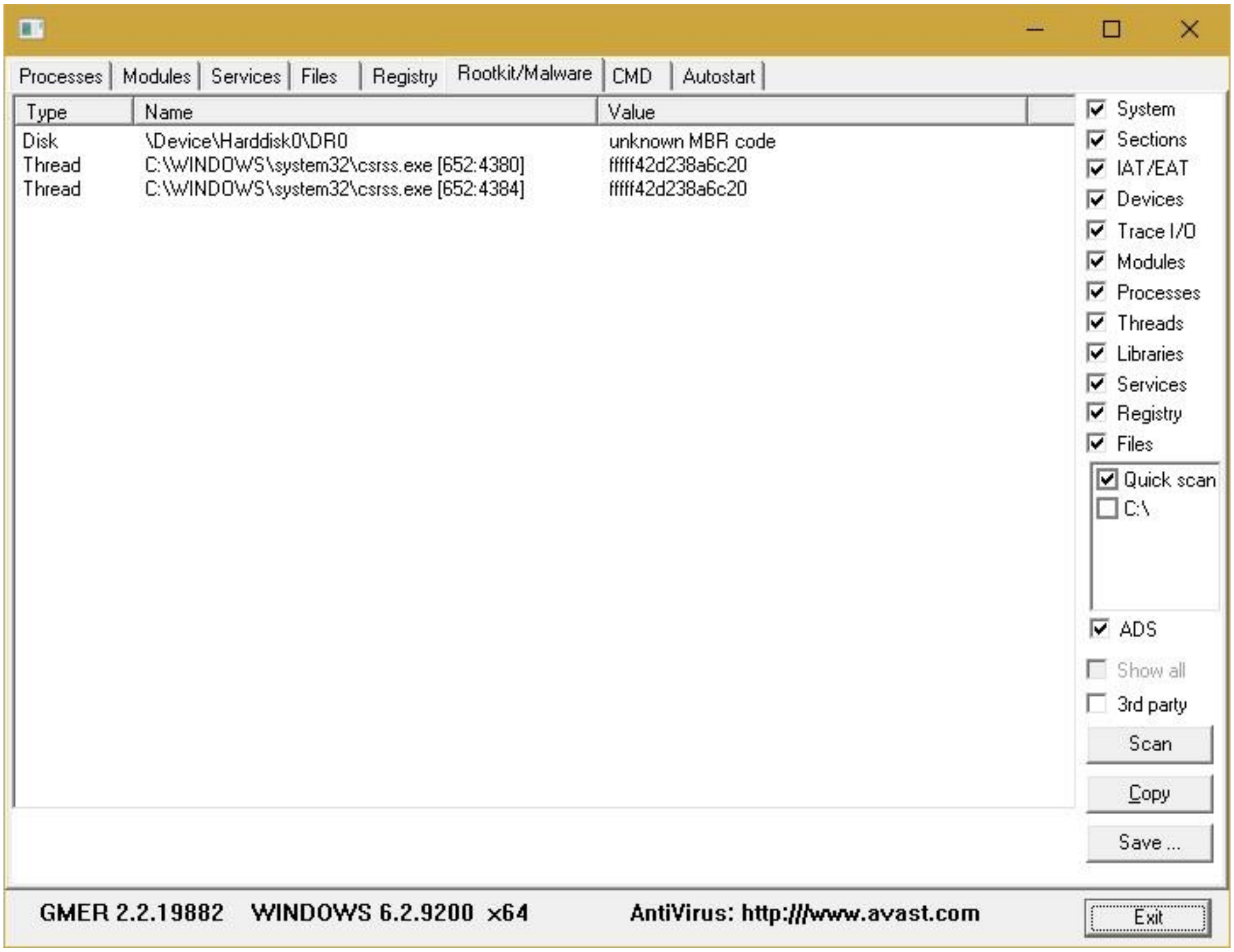
WARNING !!!

GMER has found system modification caused by ROOTKIT activity.

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, as some rootkits will close “gmer.exe” before you can open it.

Step 2



```
Type     Name                                         Value
Disk     \Device\Harddisk0\DR0                        unknown MBR code
Thread   C:\WINDOWS\system32\csrss.exe [652:4380]     fffff42d238a6c20
Thread   C:\WINDOWS\system32\csrss.exe [652:4384]     fffff42d238a6c20
```

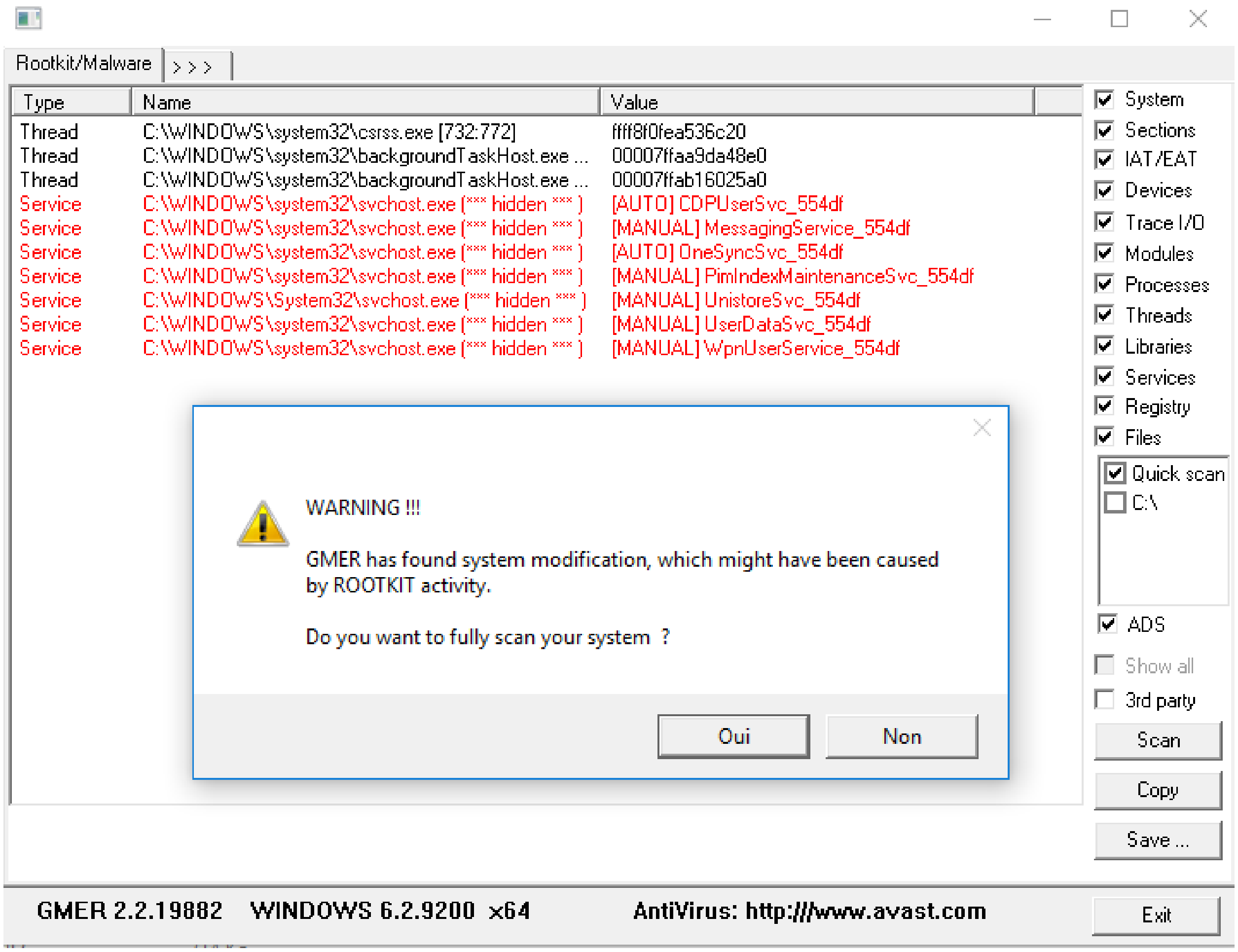
☑ System
☑ Sections
☑ IAT/EAT
☑ Devices
☑ Trace I/O
☑ Modules
☑ Processes
☑ Threads
☑ Libraries
☑ Services
☑ Registry
☑ Files
☑ Quick scan
□ C:\
☑ ADS
□ Show all
□ 3rd party

GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http://www.avast.com

Double-click the icon for the program.

Click the "Scan" button in the lower-right corner of the dialog box. Allow the program to scan your entire hard drive.

Step 3



Type	Name	Value
Thread	C:\WINDOWS\system32\csrss.exe [732:772]	ffff8f0fea536c20
Thread	C:\WINDOWS\system32\backgroundTaskHost.exe ...	00007ffaa9da48e0
Thread	C:\WINDOWS\system32\backgroundTaskHost.exe ...	00007ffab16025a0
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[AUTO] CDPUserSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] MessagingService_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[AUTO] OneSyncSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] PimIndexMaintenanceSvc_554df
Service	C:\WINDOWS\System32\svchost.exe (*** hidden ***)	[MANUAL] UnistoreSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] UserDataSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] WpnUserService_554df

WARNING !!!

GMER has found system modification, which might have been caused by ROOTKIT activity.

Do you want to fully scan your system ?

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

GMER 2.2.19882   WINDOWS 6.2.9200 x64   AntiVirus: http://www.avast.com

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 service is detected.

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

RESULT:

In this experiment a rootkit hunter software tool has been installed and the rootkits have been detected.