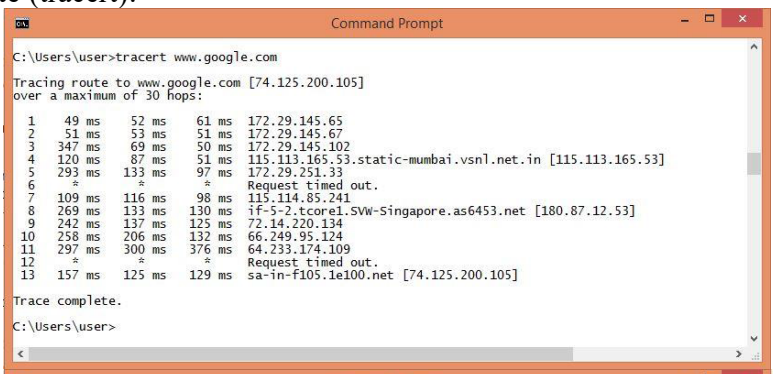
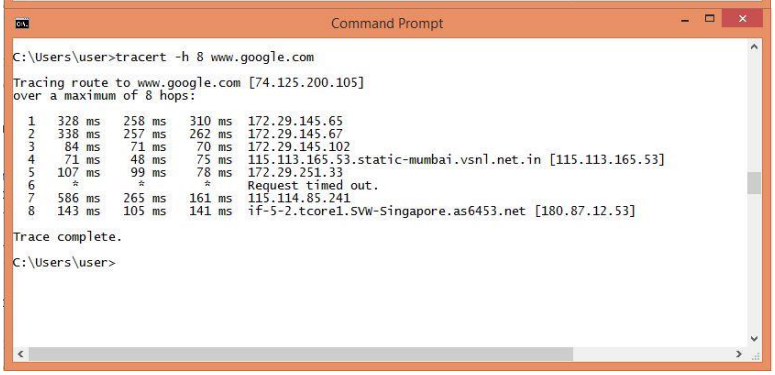
| | | | |
|---|---|---|---|
| A. | Use the following tools to perform footprinting and reconnaissance | 82 | |
| 1) | Recon-ng (Using Kali Linux) | 82 | |
| 2) | Metasploit (for information gathering) | 83 | |

# PRACTICAL 1

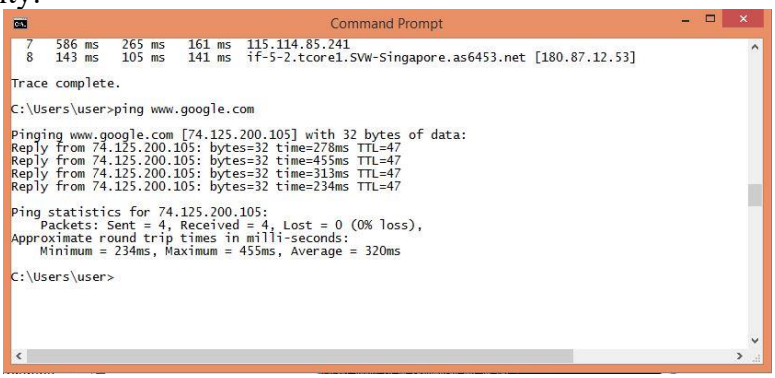
## A. Using the tools for whois, traceroute, email tracking, google hacking.

1) Traceroute (tracert):

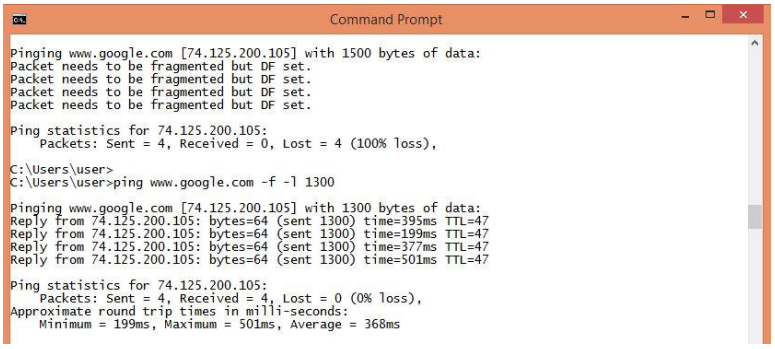


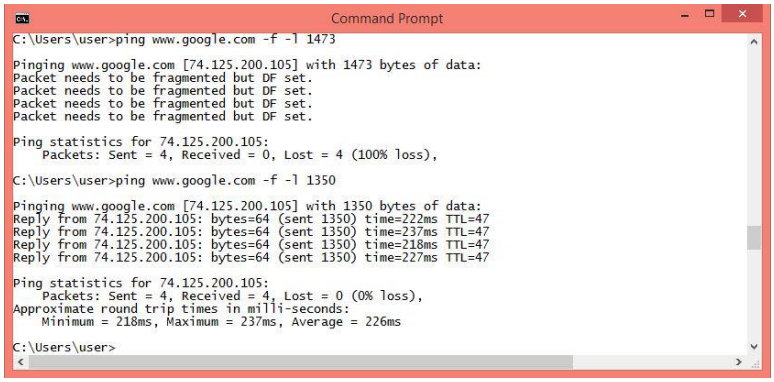

2) Ping Utility:



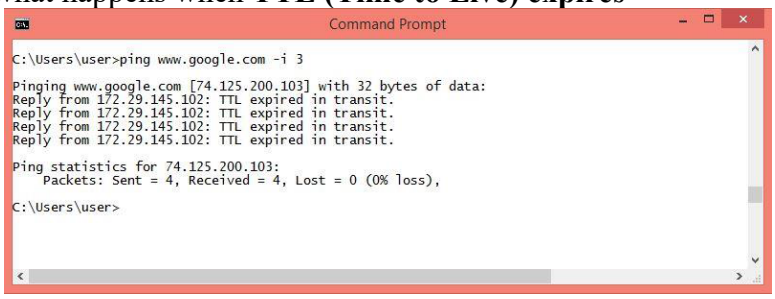

Finding out the maximum frame size on the network



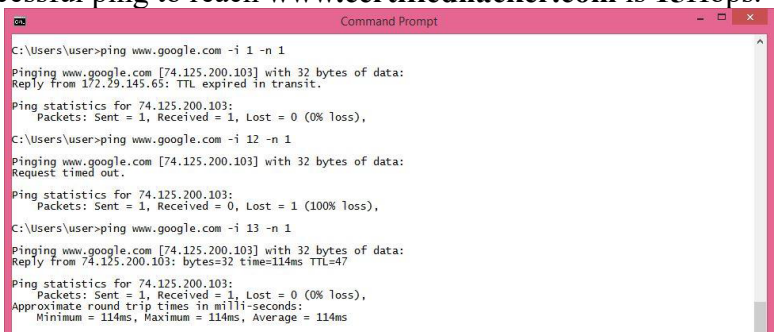

Trying different values until you find the maximum frame size.




Finding out what happens when **TTL (Time to Live) expires**



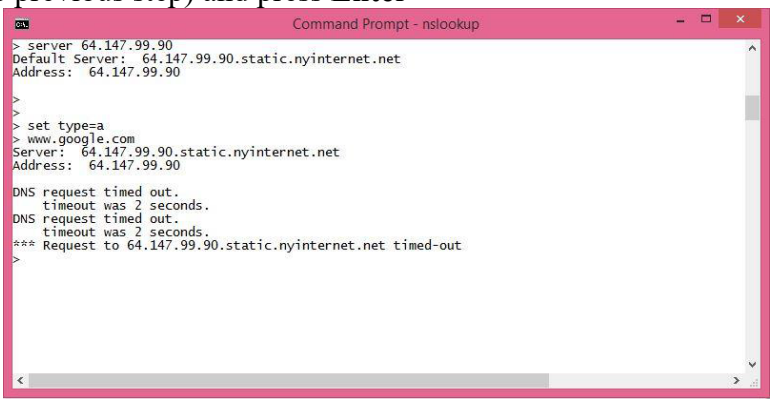

Command ping www.certifiedhacker.com –I 1-n 1. Repeat the steps until you reach the IP Address for www.certifiedhacker.com (111 this case, 202.75.54.101)
Here the successful ping to reach **www.certifiedhacker.com** is **15**Hops.



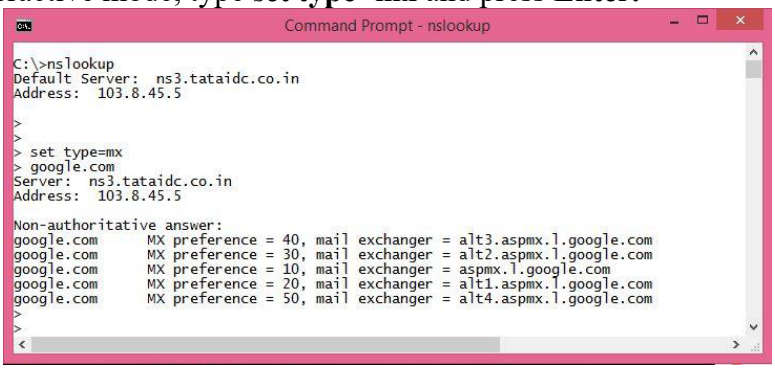

3) nslookup:


nslookup interactive mode, type **set type=cname** and press **Enter**


nslookup interactive mode, type **server 64.147.99.90** (or any other IP Address you receive in the previous step) and press **Enter**



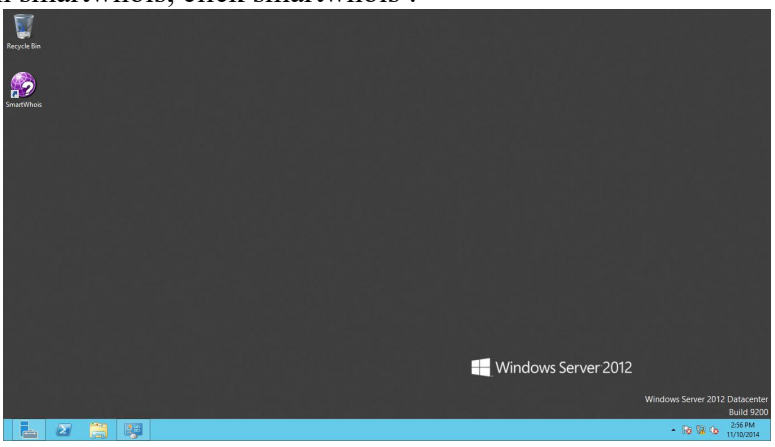

nslookup interactive mode, type **set type=mx** and press **Enter.**



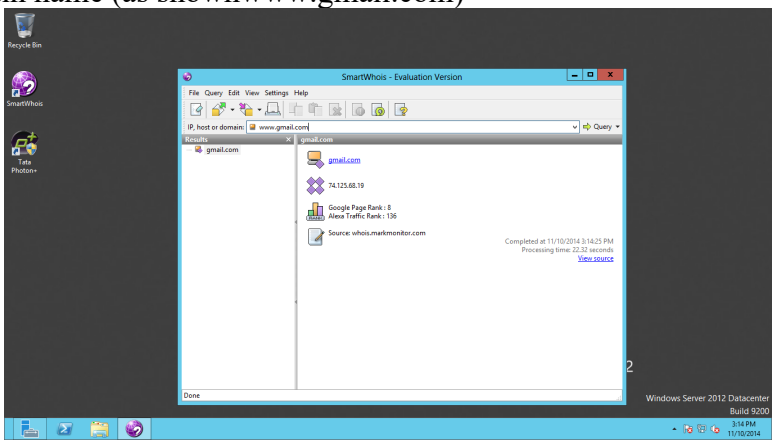

4) SmartWhois

Follow the wizard driven installation steps and install smartwhois :

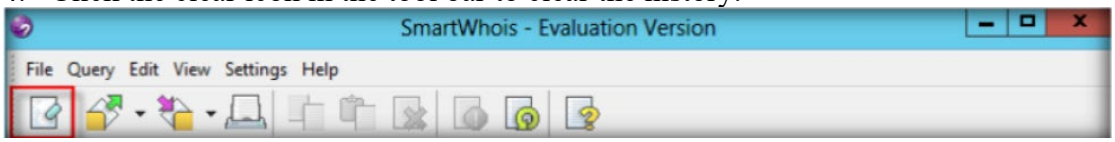
1. To launch smartwhois, click smartwhois :



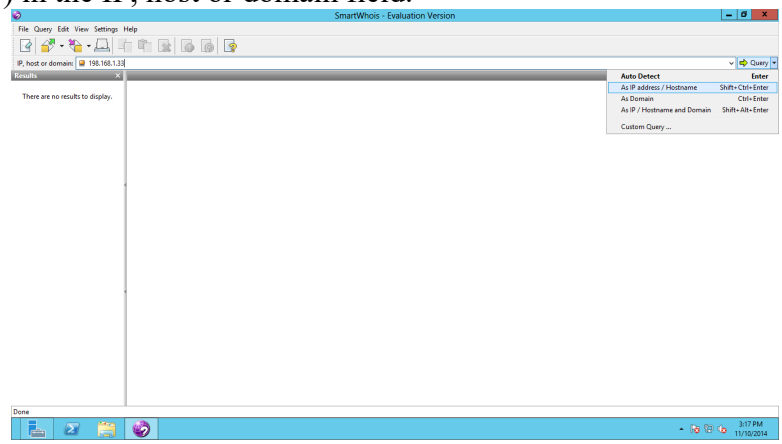
2. The smartwhoisin main window appears .
3. Type an IP Address, hostname or domain name in the tab field .An example of the domain name (as shownwww.gmail.com)



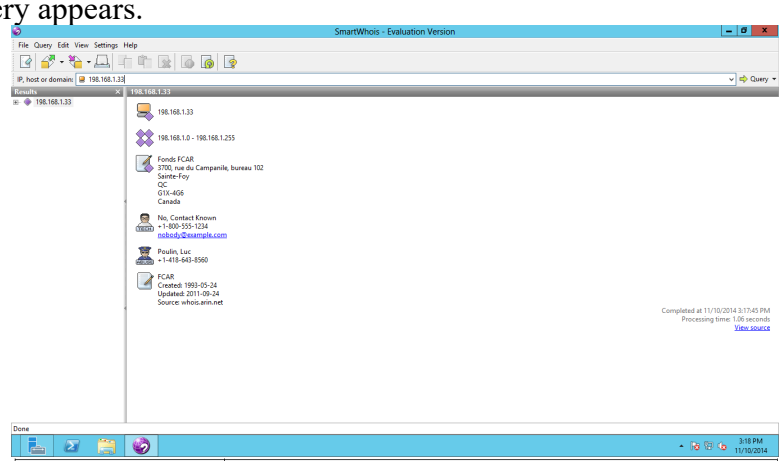

4. Click the clear icon in the tool bar to clear the history.




5. To perform a sample IP Address query type the IP Address (windows 8 IP Address ) in the IP, host or domain field.



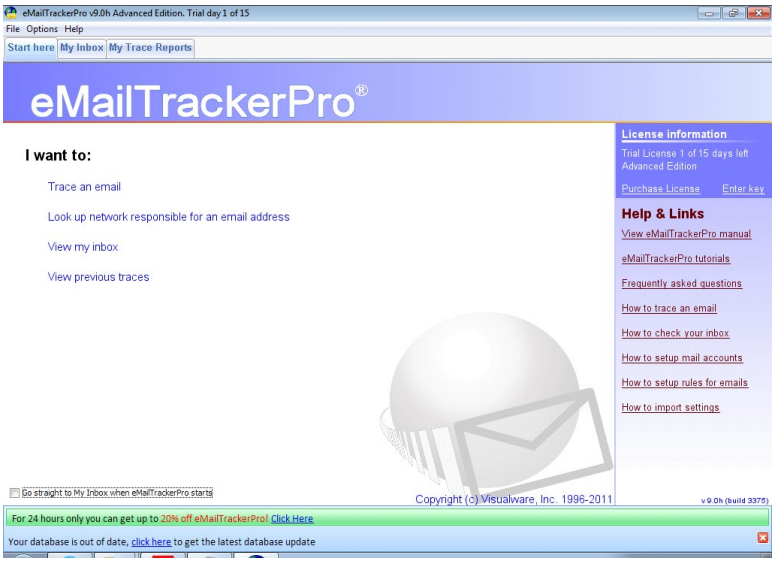

6. In the left pane of the window the result appears and in the right pane result of your query appears.



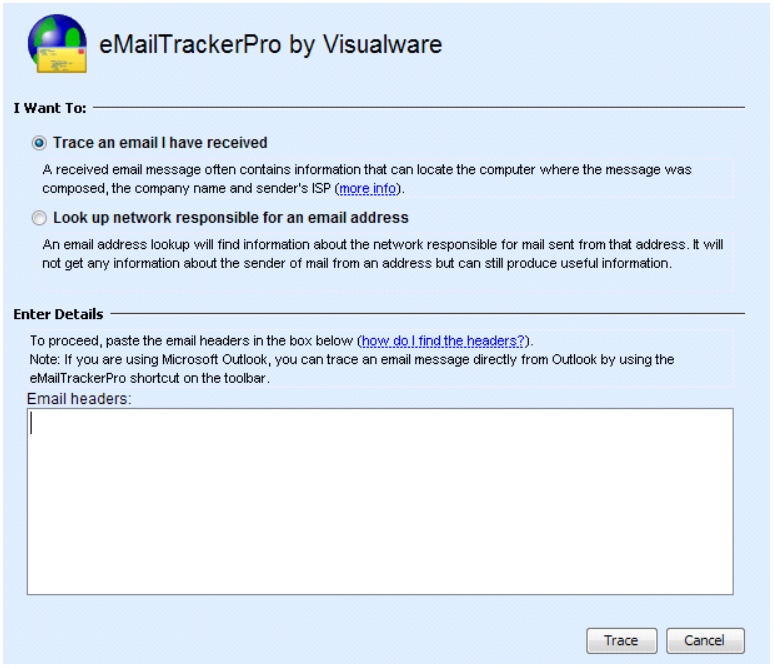

| Tool/Utility | Information collected /objectives achived |
|---|---|
| **SmartWhois** | **Domain name query results**: Owner of the website |
| | **Host name query results**: geographical location of the hosted website |
| | **Ip address query results**: owner of the ip address block |

5) eMailTracker Pro

Run eMailTrackerPro

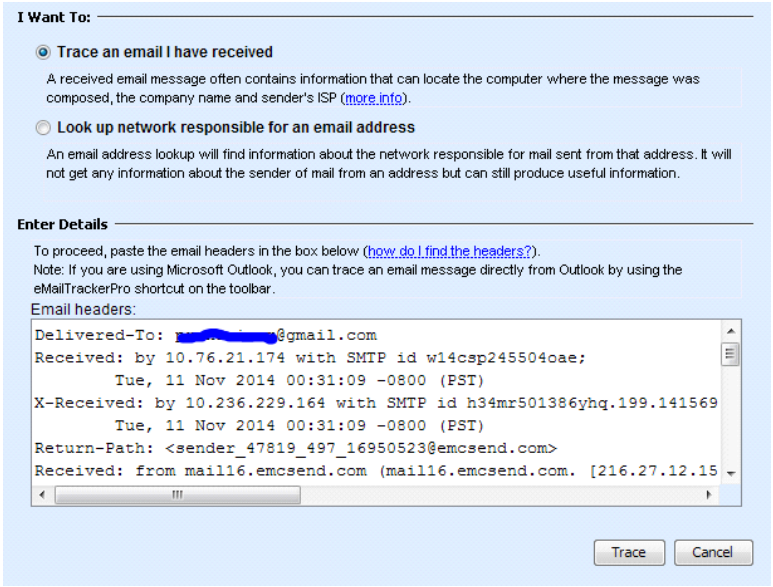



Select 1st option - Trace an email

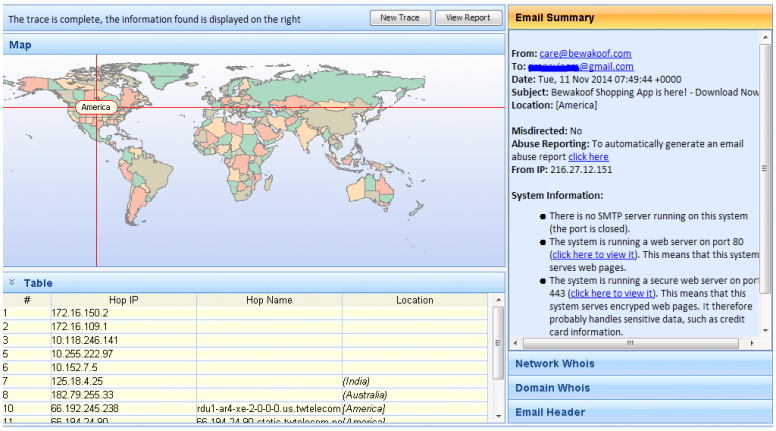



Trace an email I have received

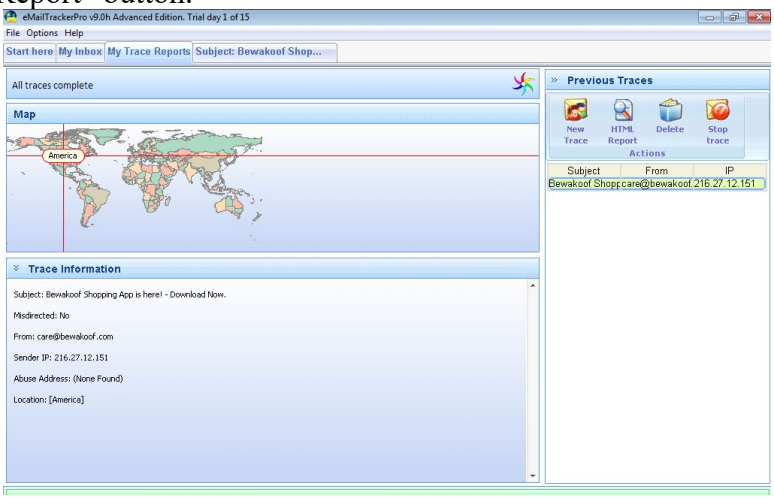
Insert the email header in the Given box 'Enter Details'




Click on Trace




The result shows a location map, the Trace Route below and the Whois/Network/Email summary in the right columns
To view the HTML Report of it, go to the “My Trace Reports” tab and then click on the “HTML Report” button.

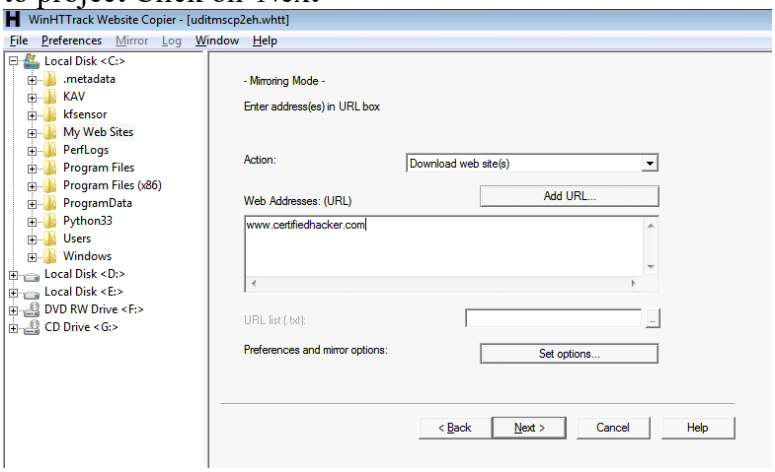


6) HTTrack Website Copier

Start > Programs > HTTrack Website Copier

Click on 'Next' to create Project

Give a name to project Click on 'Next'

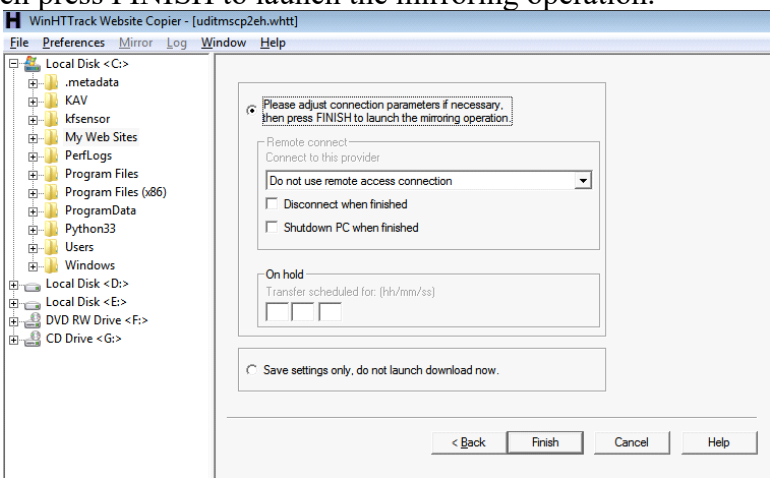



Click on ‘Add URL’ and give the URL of the site to mirror from.

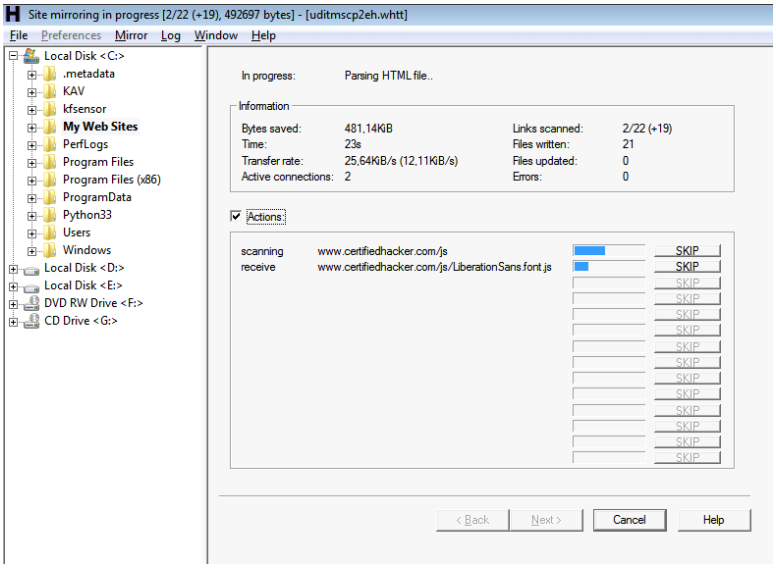
Any additional options that need to be set, can be set from the ‘Set Options’ menu

Then click 'Next'

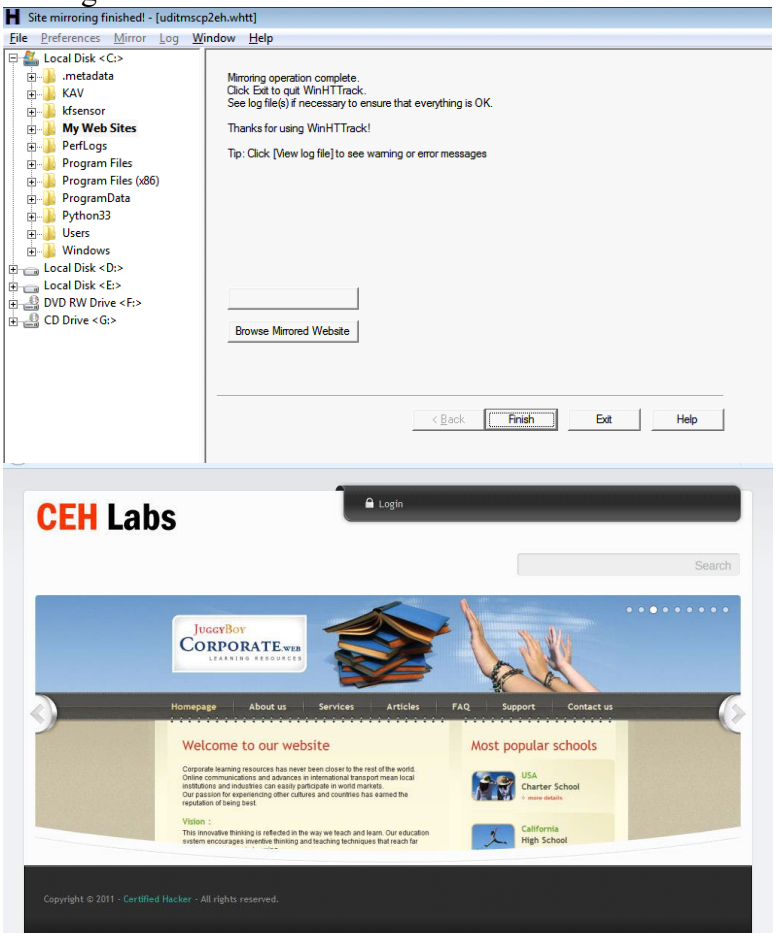
By default, the radio button will be selected for Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.




The mirroring of the site now begins. The site will be downloaded and be saved in the C:\My Web Sites\<Project Name>




Process of mirroring the website



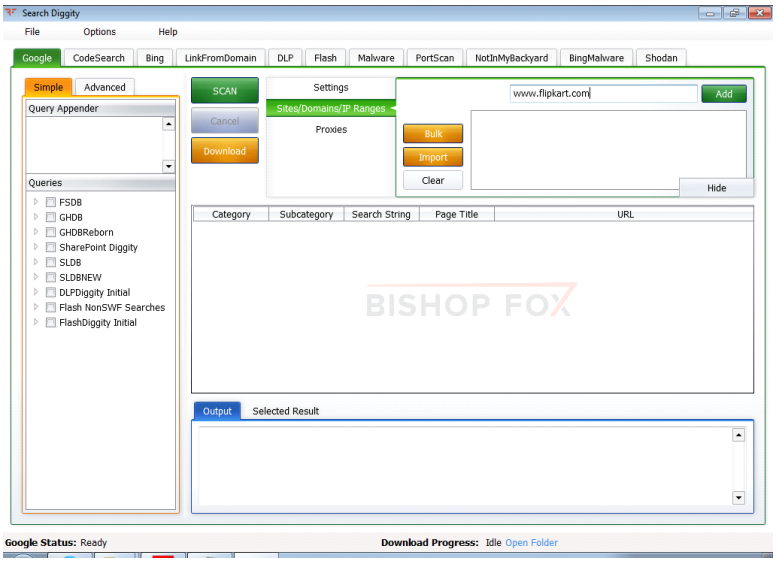

7) Search Diggity

It is used to **I**dentity vulnerabilities and information disclosures in websites using Search Engine Hacks/Keywords

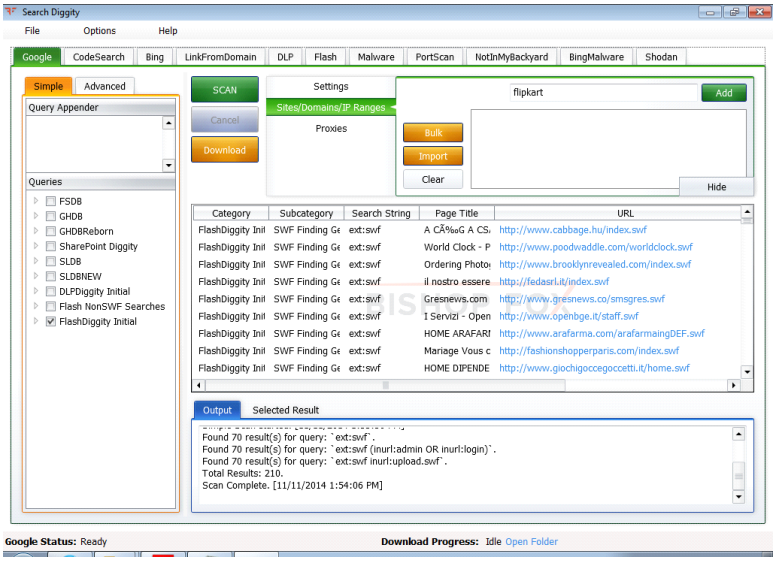
Start > Programs > SearchDiggity

The Search Diggity main window appears with Google as the default search engine

Select “Sites/Domains/IP Ranges. Type a URL to perform Google Hacking against and then click on the Add button.




Select the vulnerability database to use from the left and then select the search queries you would like to search for

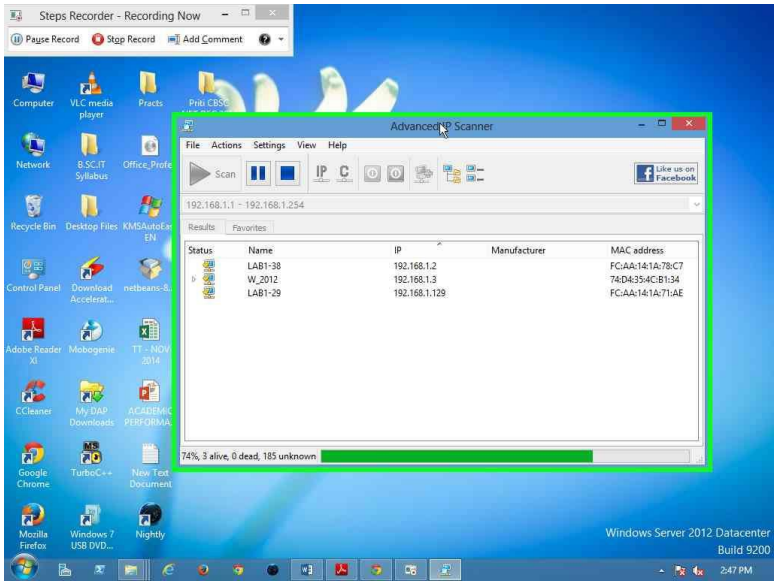


# PRACTICAL 2

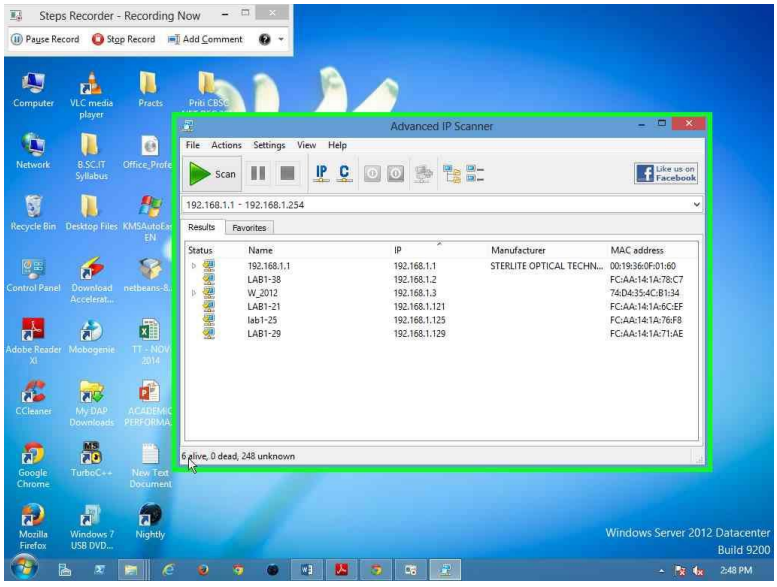
**A. Using the tools for scanning network, IP fragmentation, war dialing countermeasures, SSL Proxy, Censorship circumvention.**

1) Advanced IP Scanner

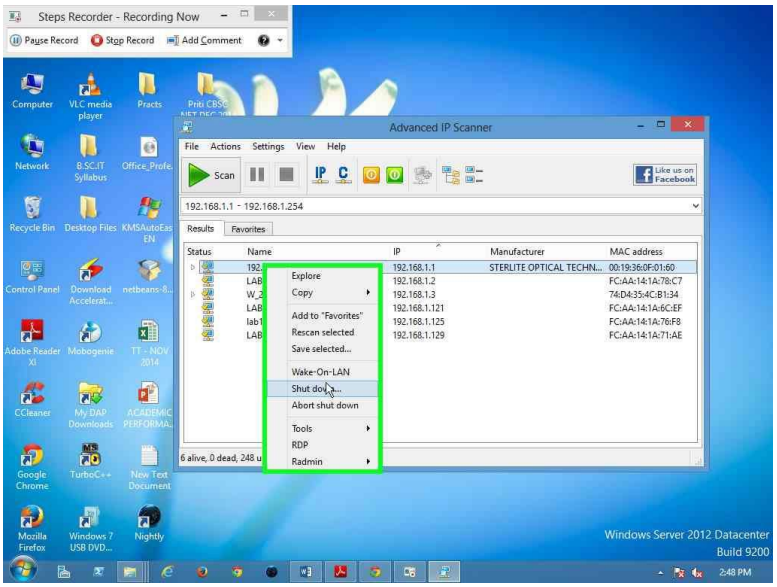
1. After successful installation of the software, launch the tool.
2. click on scan:



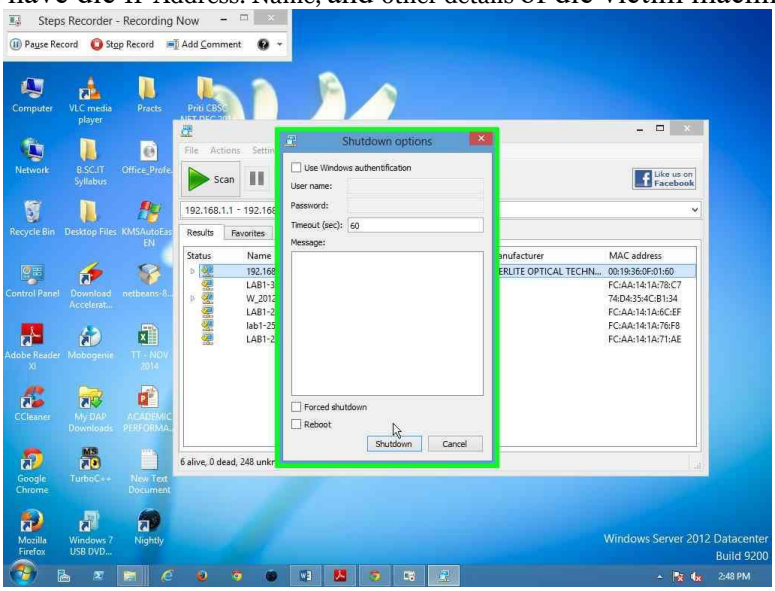

3. The tool will scan the network for IP Addresses



4. Right-click any of die detected IP Addresses. It will list Wake-On-LAN.Shut down, and Abort Shut down.

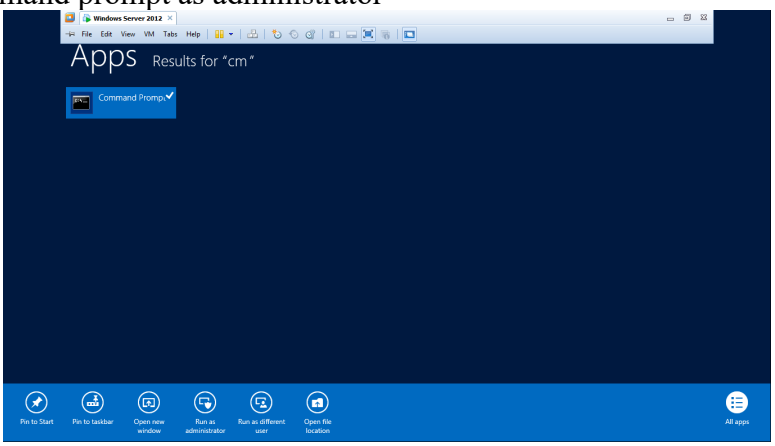


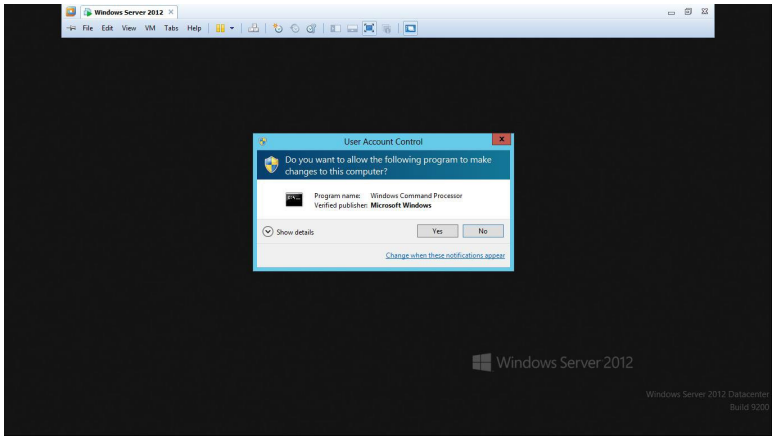

5. Now you have die IP Address. Name, and other details of die victim machine



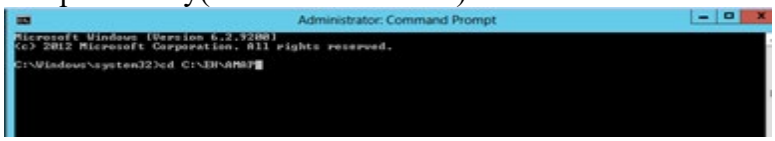

2) Amap

1. Run command prompt as administrator

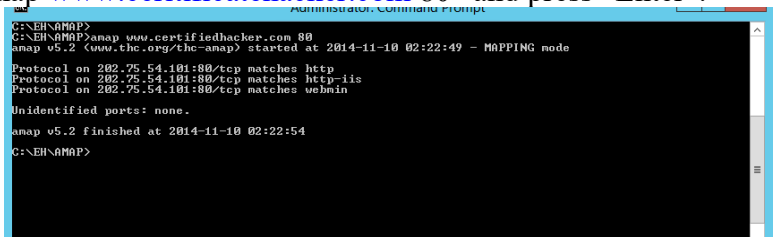




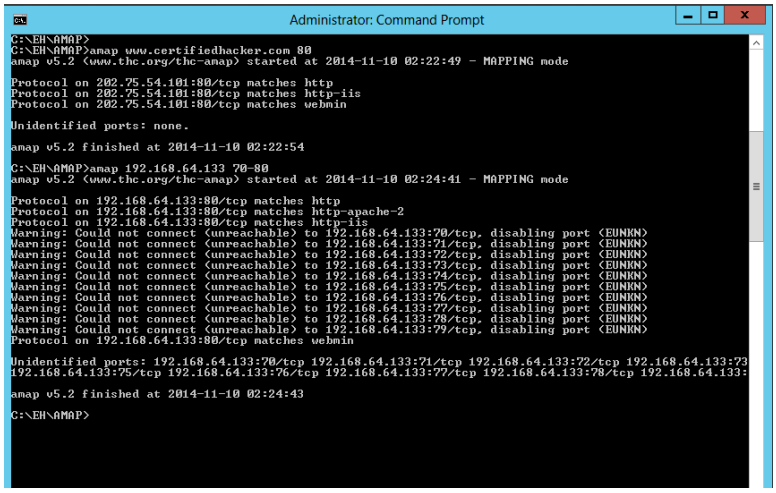

2. Navigate amap directory(here C:\EH\AMAP)




3. Type “amap www.ceritificatehacker.com 80” and press “Enter”.




4. You can see the specific application protocols running on the entered host name and port 80
5. Use the IP Address to check the application running on a particular host.
6. In command prompt type the IP Address of your windows server 2012(here 192.168.64.133) as “amap 192.168.64.133 70-80” and press Enter
7. Try scanning different websites using different switches like “amap www.certifiedhacker.com 70-80”.

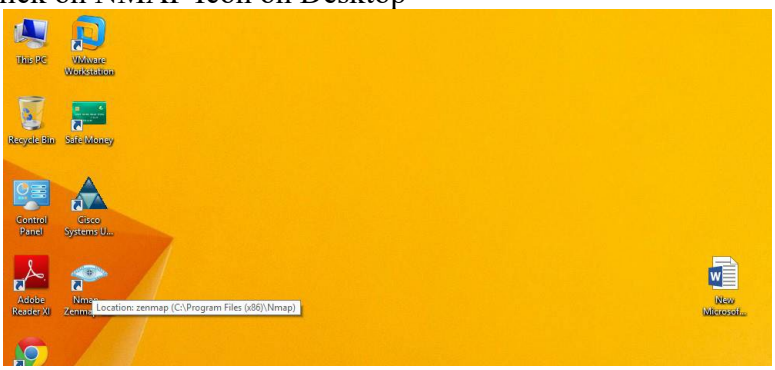



Identified open port : 80
Web servers:
http
http-apache-2
http-iis
webmin

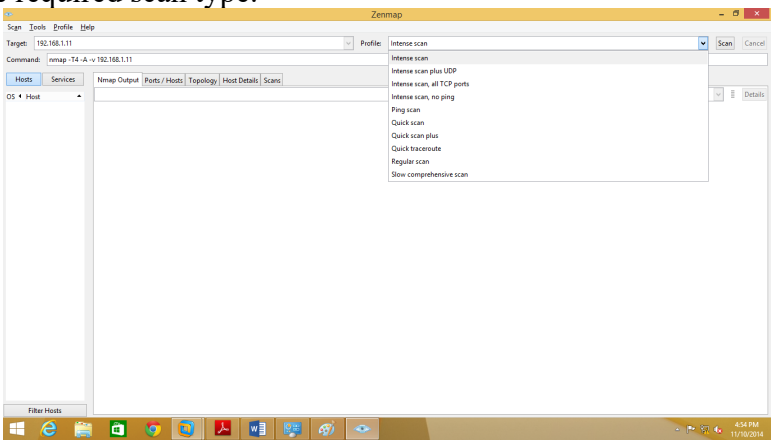
Unidentified ports:
192.168.64.133:70/tcp
192.168.64.133:71/tcp
192.168.64.133:72/tcp
192.168.64.133:73/tcp
192.168.64.133:74/tcp
192.168.64.133:75/tcp
192.168.64.133:76/tcp
192.168.64.133:77/tcp
192.168.64.133:78/tcp
192.168.64.133:79/tcp (total 10).

3) Nmap

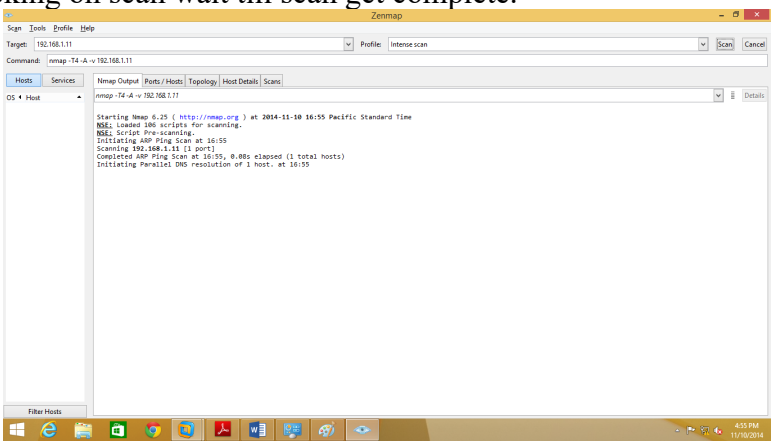
1. Select the NMAP icon
2. Double click on NMAP Icon on Desktop



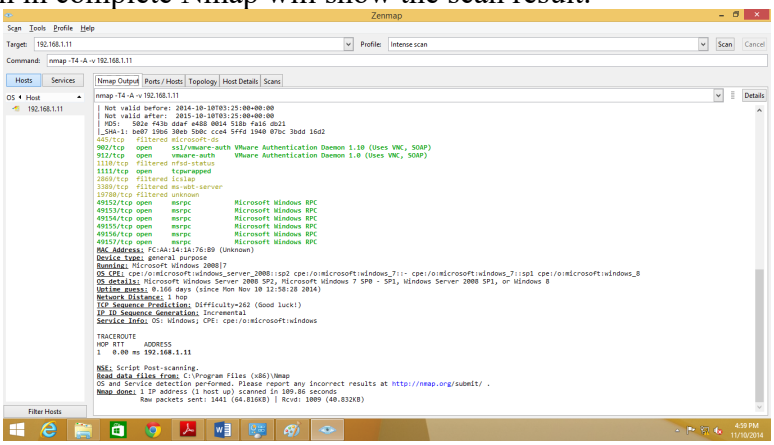

3. Put the IP-Address for scanning
4. Select the required scan type.



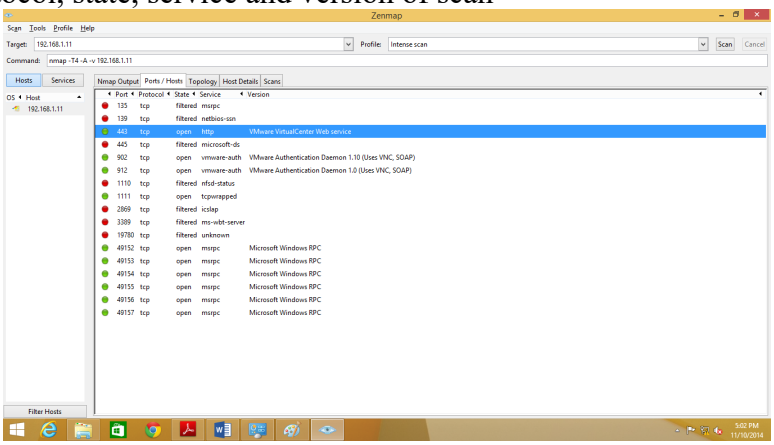
5. After selecting scan type click on scan button.
6. After clicking on scan wait till scan get complete.



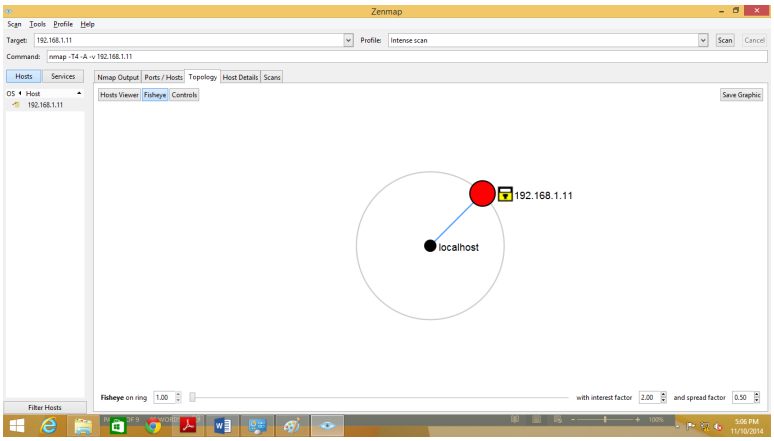

7. After scan in complete Nmap will show the scan result.



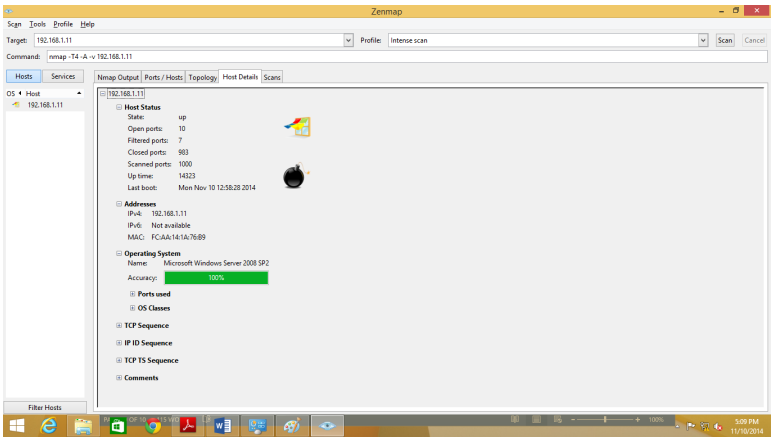

8. Click port /host tab for display more information about scan; NMAP also display port, protocol, state, service and version of scan



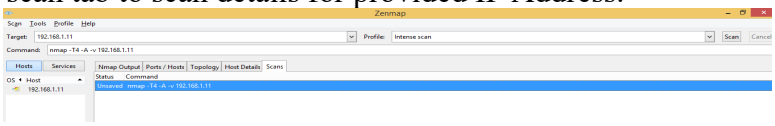
9. Click on topology tab to view Nmap's topology for the provided IP Address in the intense scan



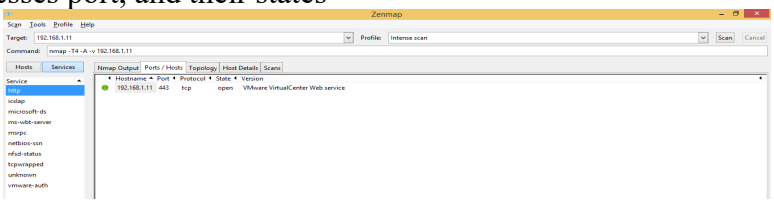

10. Click the host details tab to see the details of all host discovered during scan.



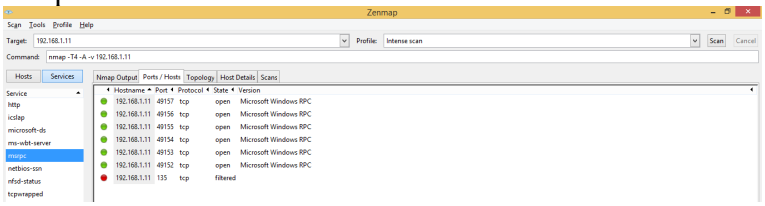

11. Click the scan tab to scan details for provided IP Address.



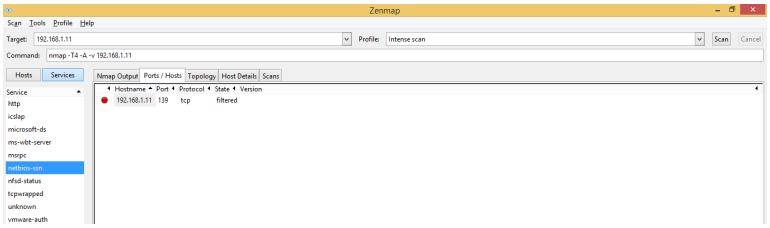

12. Now click on the service tab located in the right pane of the windows, this will display the list of services. Now click the http service to list all the http hostname /IP Addresses port, and their states



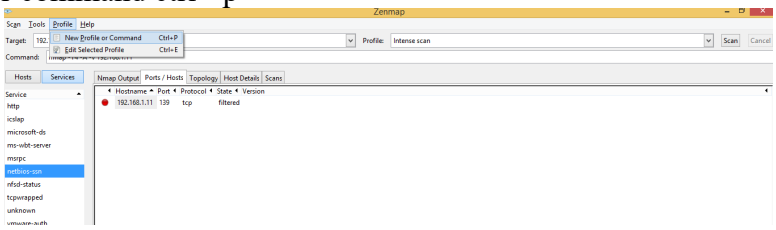

13. Click the msrpc service to list all the Microsoft windows RPC



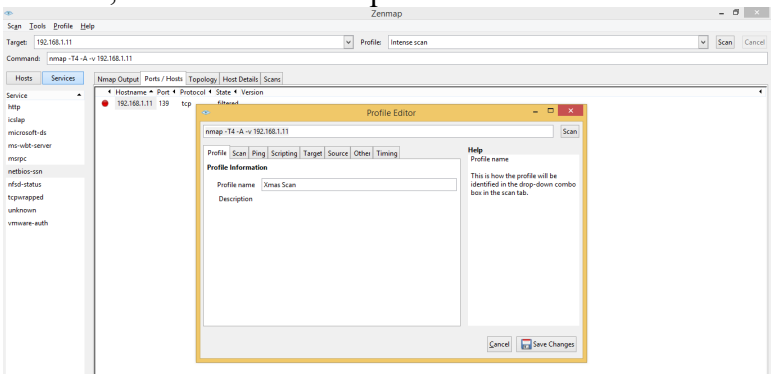
14. Click the netbios-ssn service to list all NetBIOS hostnames.



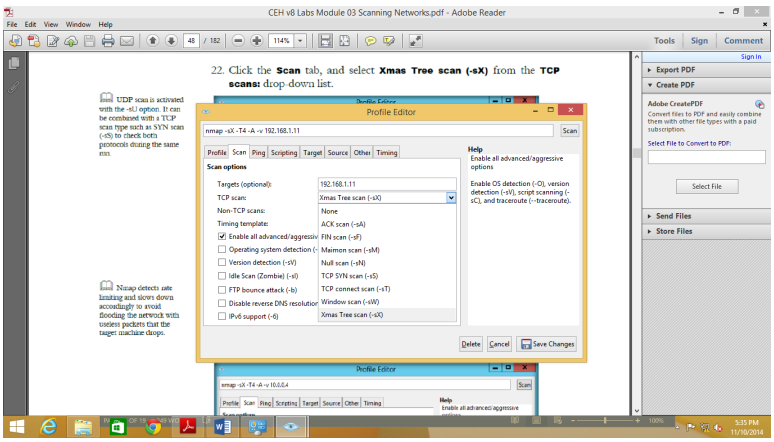

15. Xmas scan sends a TCP frame to a remote device with URG, ACK,RST,SYN and FIN flag set. FIN scans only with OS TCP/IP Developed according to RFC 793Now perform xmasscan,you need to create a new profile. Click profile ->New Profile Or command ctrl +p



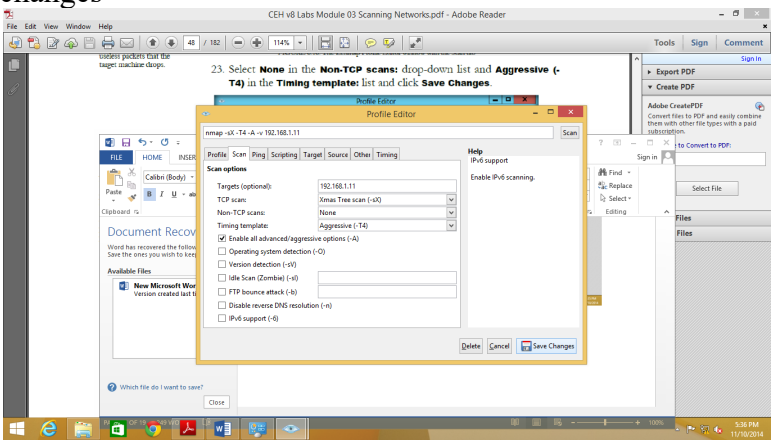

16. On the profile tab, enters scan ion the profile name text field.



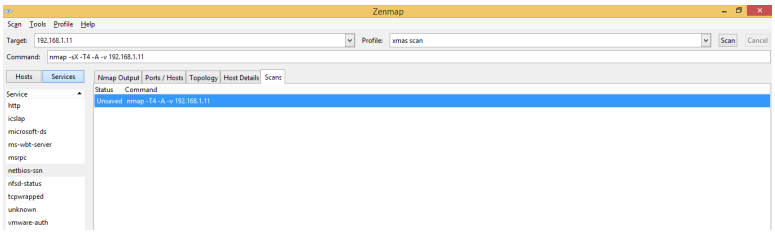

17. Click the scan tab and select Xmas tree Scan (-sx) from the TCP Scans:Drop Down



18. Save the changes



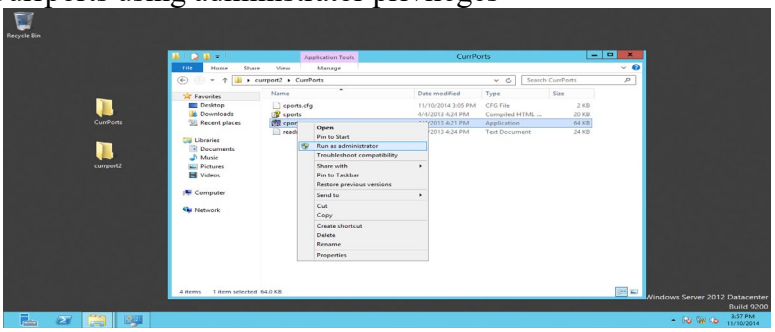

19. Now perform the same steps from 3 to 5 but select the xmas scan in profile drop down that we have created now.

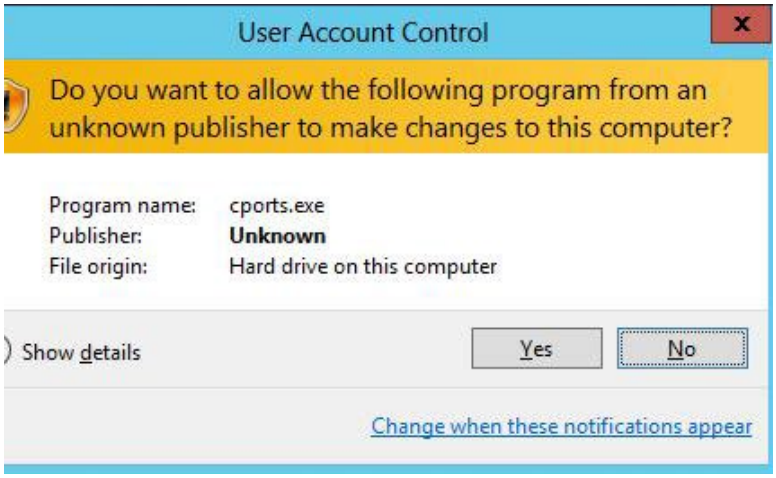



To create different scan profile perform the steps 15 to 17

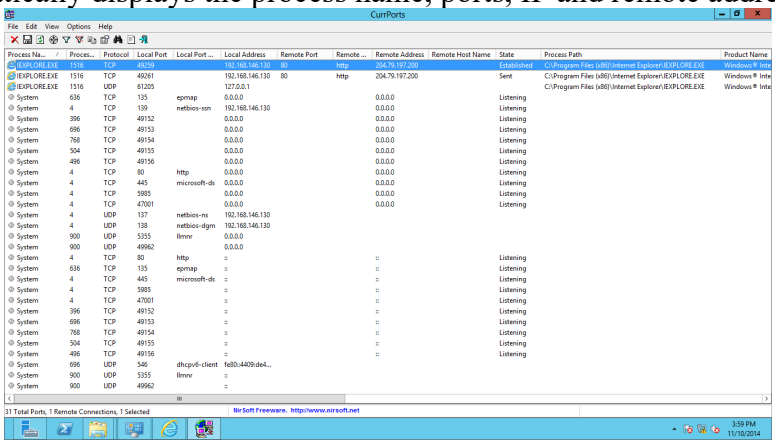
4) CurrPorts Tool

1. Launch Currports using administrator privileges

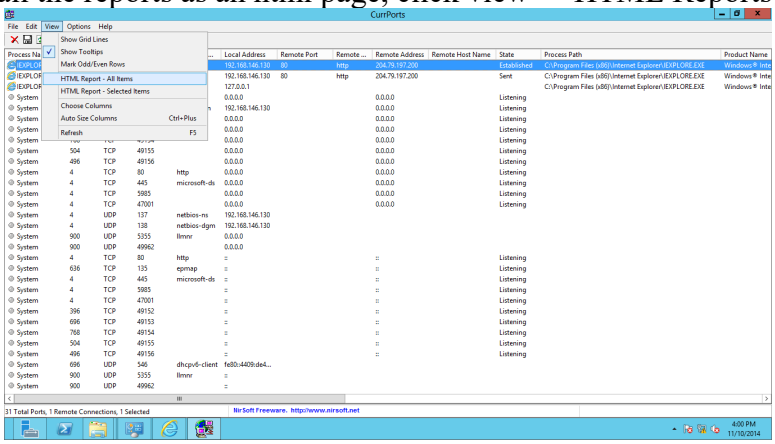




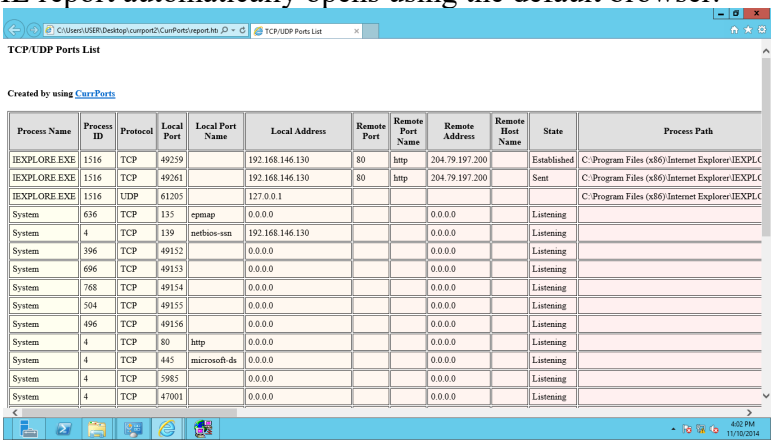

2. it automatically displays the process name, ports, IP and remote address and states



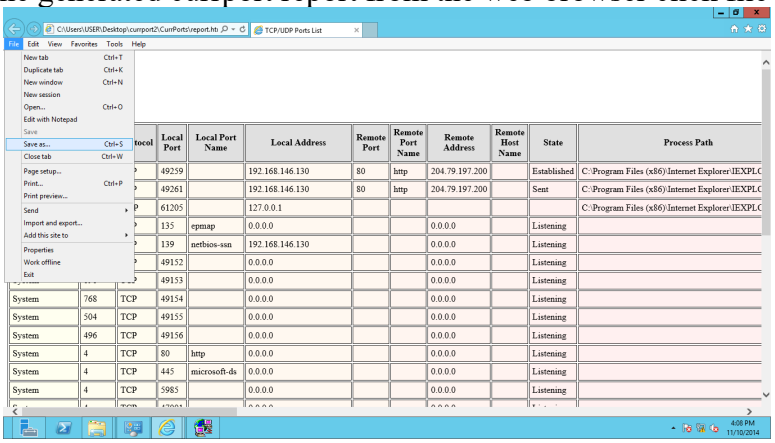

3. Currports lists all the processes and there ids protocols used local and remote IP Address, local and remote ports and remote host names
4. To view all the reports as an html page, click view -> HTML Reports –All Items



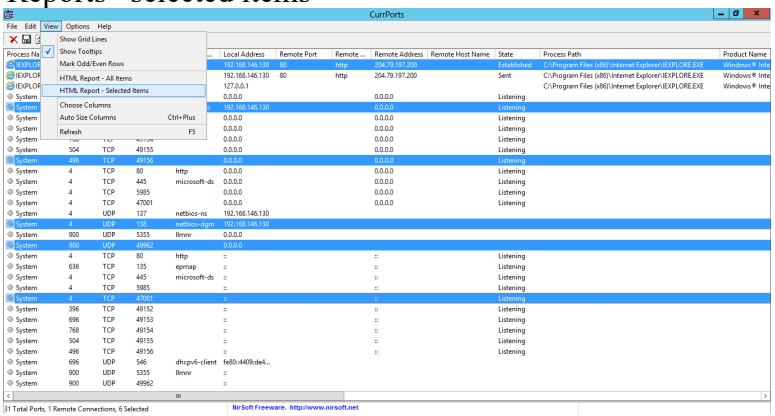
5. The HTML report automatically opens using the default browser.



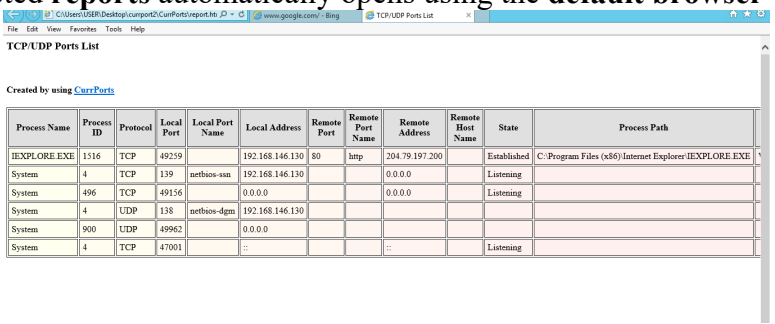

6. To save the generated currport report from the web browser click file -> save as..



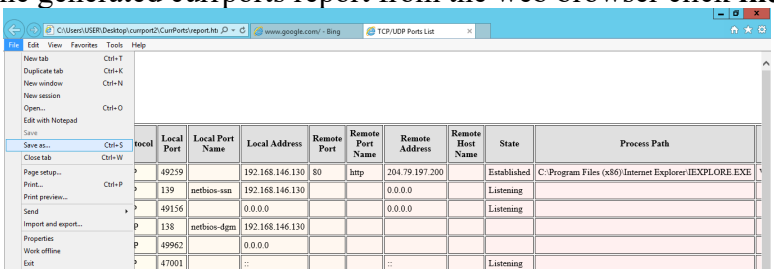

7. To view only the selected report as an HTML page select reports and click View -> HTML Reports –selected items



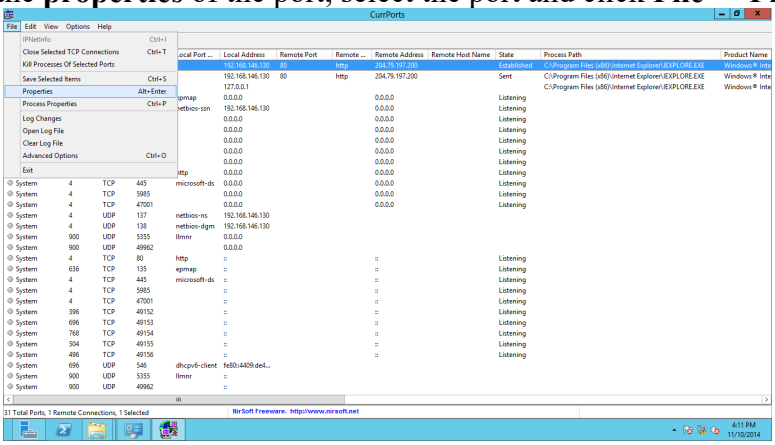

8. The selected **reports** automatically opens using the **default browser**



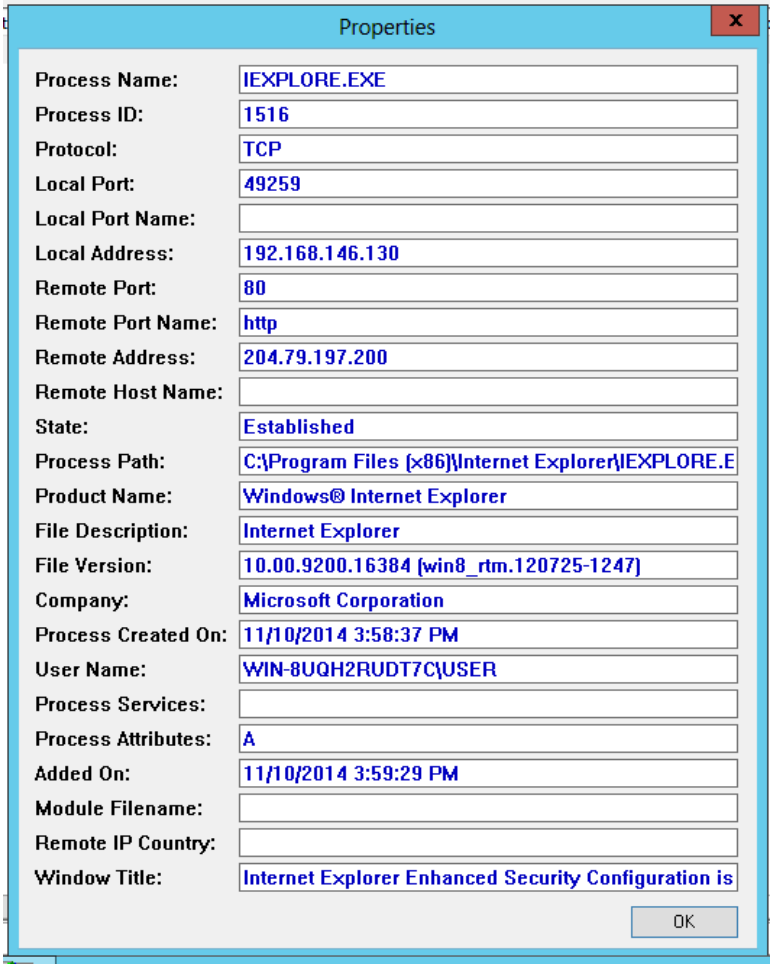
9. To save the generated currports report from the web browser click **file -> save as..**



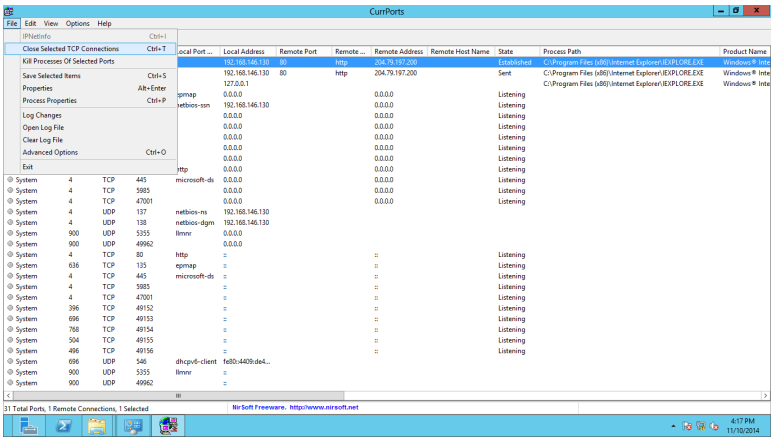
10. To view the **properties** of the port, select the port and click **File -> Properties**



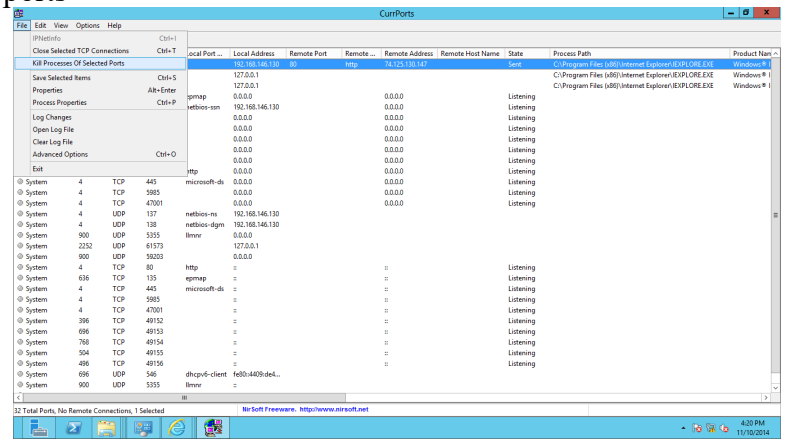
11. The properties window appears and displays all the properties for the selected port



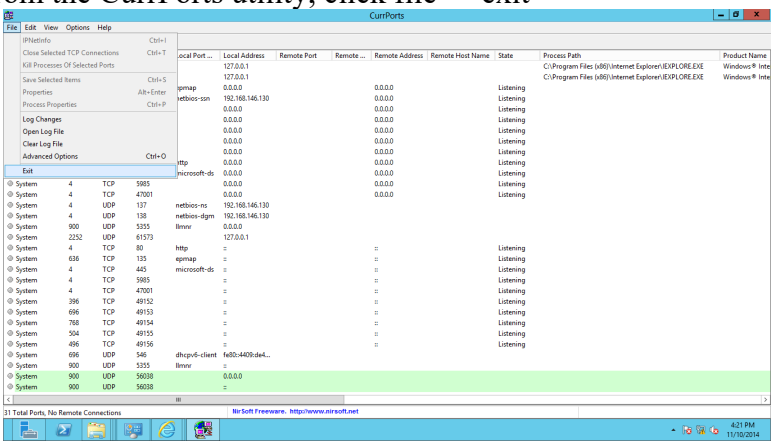
12. To close a TCP connection you think, select the process and click File -> Close Selected TCP Connections




13. To kill the process of a port, select the port and click file -> Kill process of selected ports

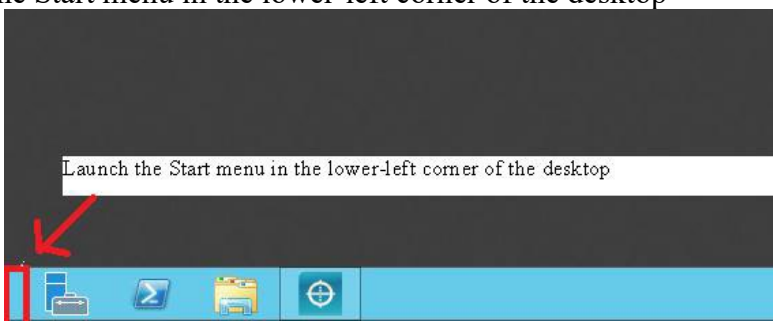



14. To exit from the CurrPorts utility, click file -> exit

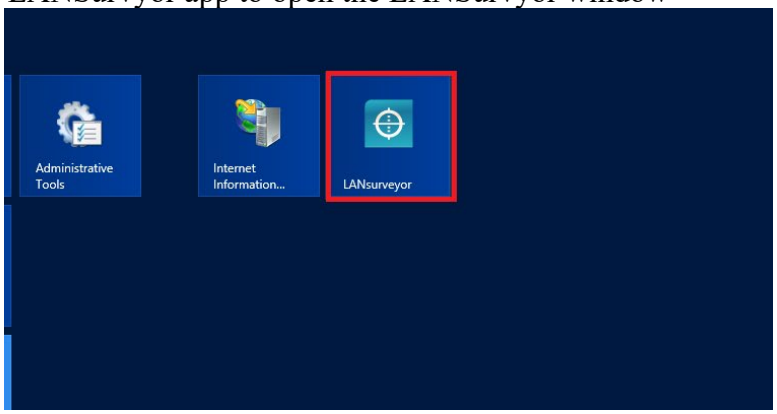


5) LANSurveyor

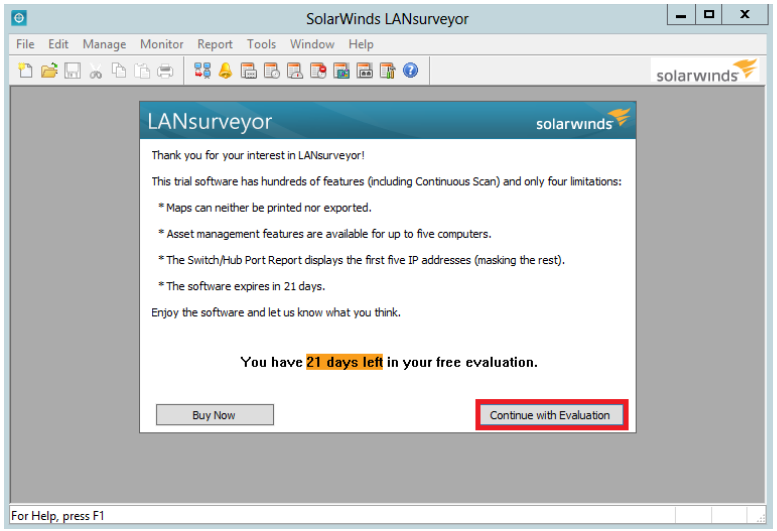
1. Launch the Start menu in the lower-left corner of the desktop



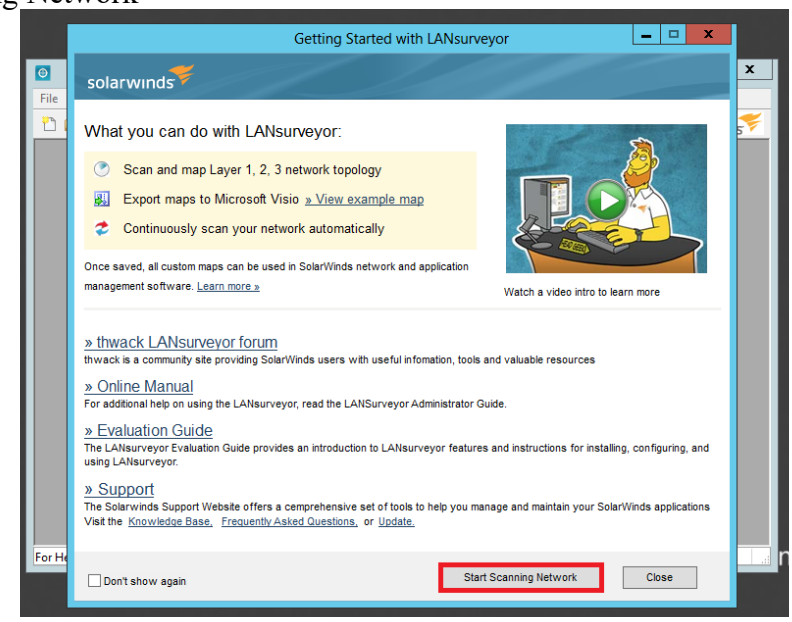

2. Click the LANSurvyor app to open the LANSurvyor window



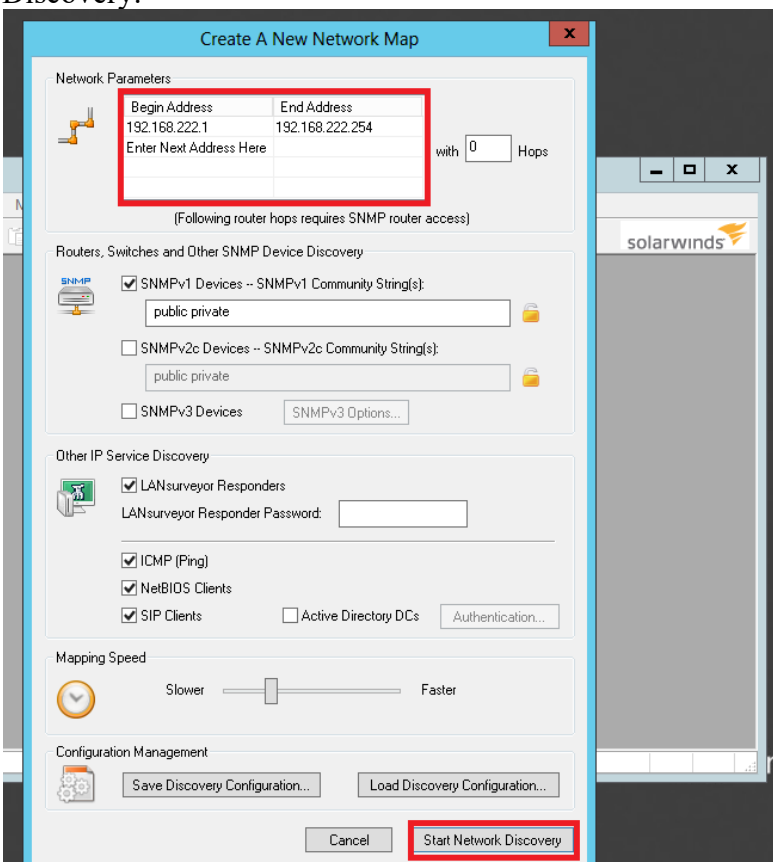

3. click Continue with Evaluation to continue the evaluation



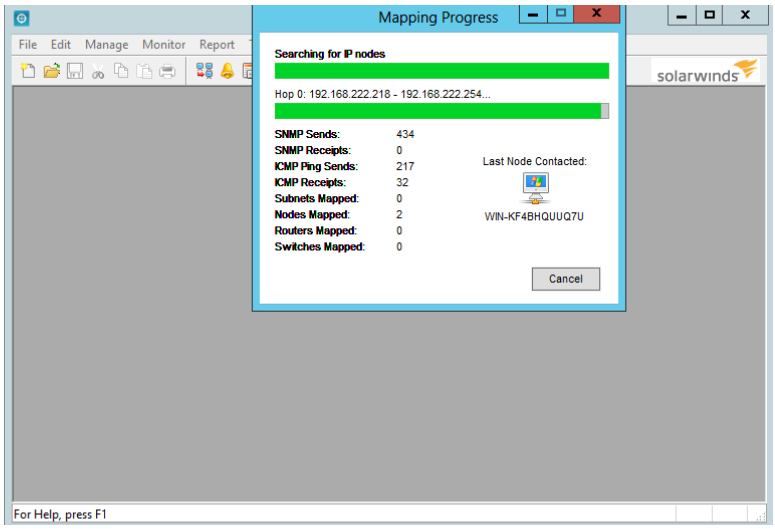
4. The Getting Started with LANsurveyor dialog box is displayed. Click Start Scanning Network



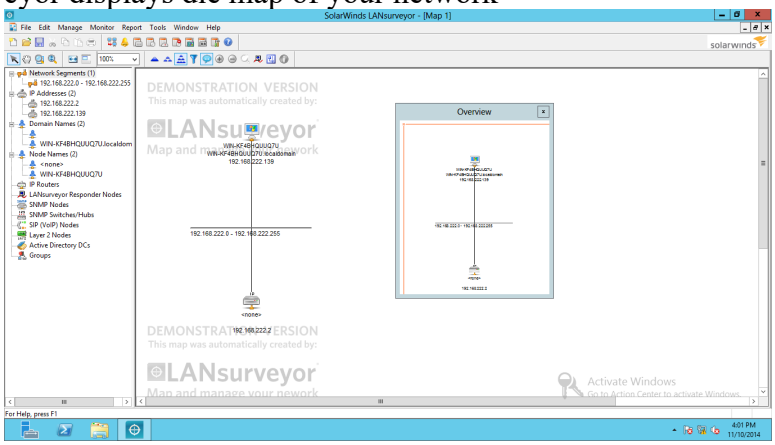

5. The Create A Network Map window will appears; in order to draw a network diagram enter the IP Address in Begin Address and End Address, and click Start Network Discovery.



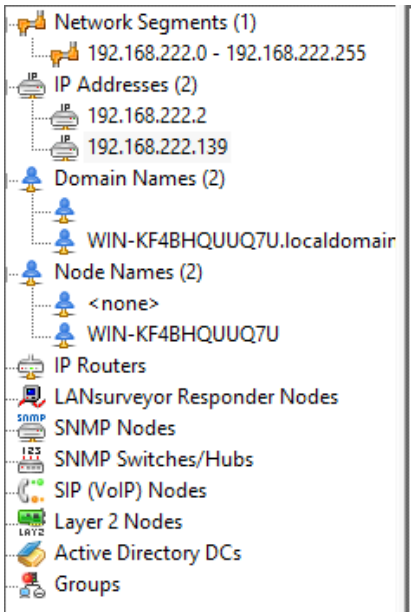
6. The entered IP Address mapping process will display as shown in the following figure




7. LANsurveyor displays die map of your network




8. Document all die IP Addresses, domain names, node names, and SNMPnodes



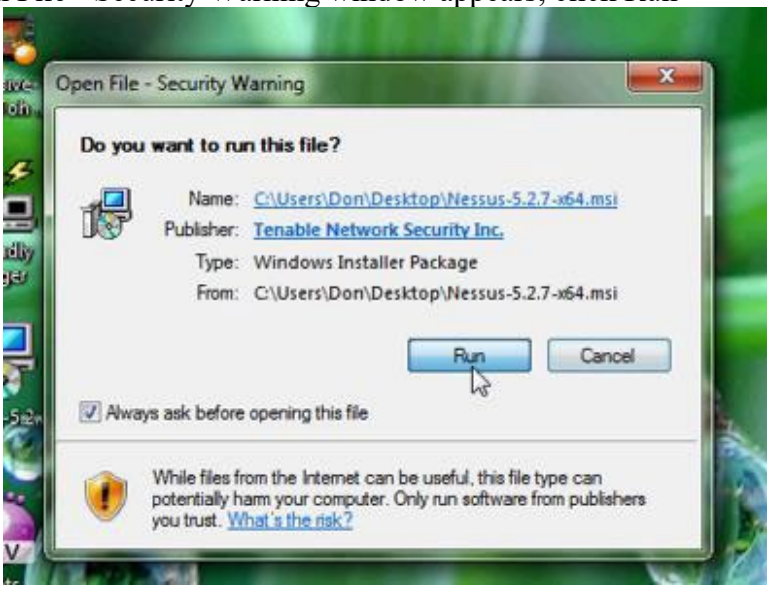

Report:-
IP Address : 192.168.222.0-192.168.222.254
IP Nodes Details :

SNMP send - 496
ICMP Ping Send - 248
ICMP ReceIPts - 4
Nodes Mapped - 4

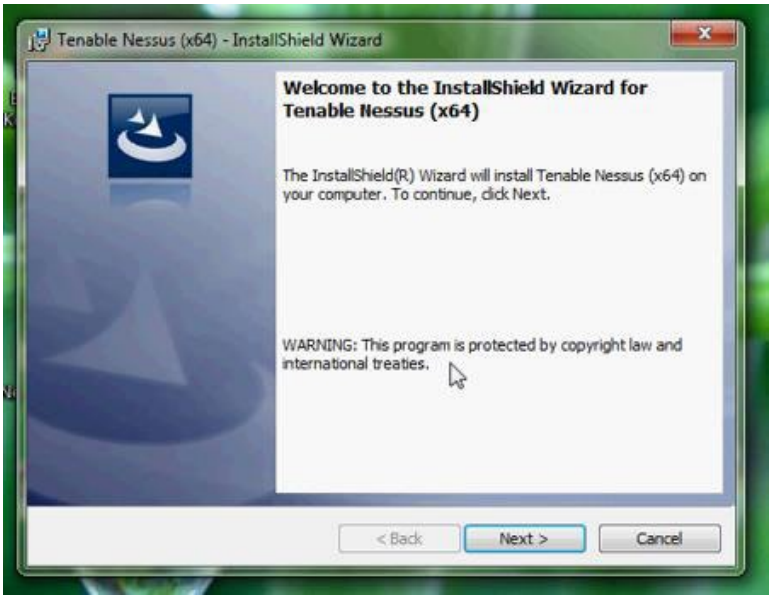
Network Segment Details :
IP Address - 2
Domain name - 2
Node Names – 2

6) Nessus

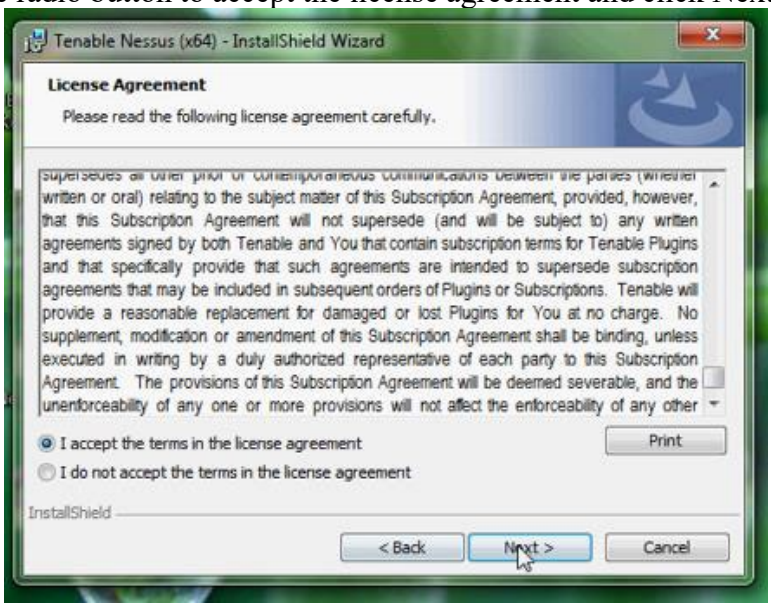
1. Double-click the Nessus-5.0.1-x86_64.msi file.
2. The Open File - Security Warning window appears; click Run



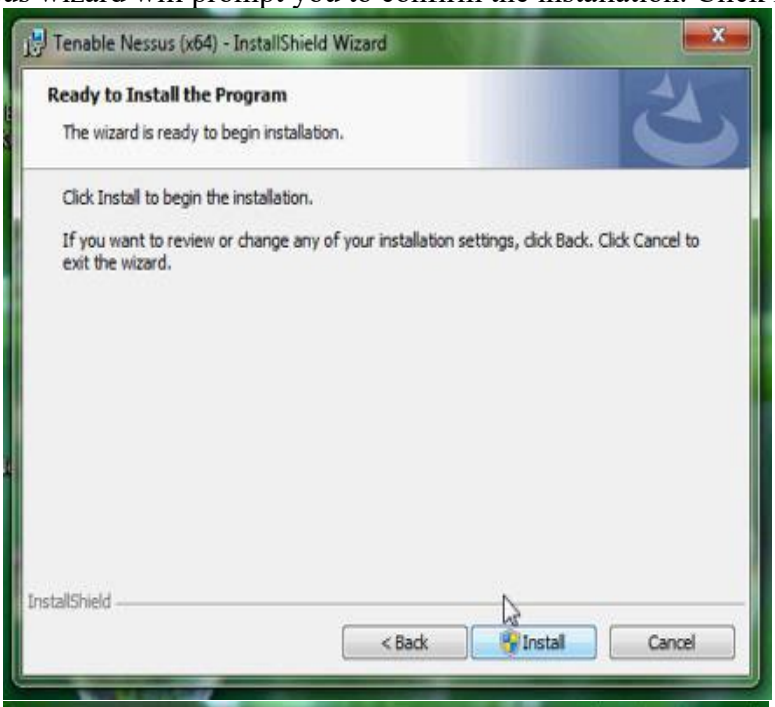

3. The Nessus – Install Shield Wizard appears. Dining the installation process, the wizard prompts you for some basic information. Follow die instructions. Click Next.

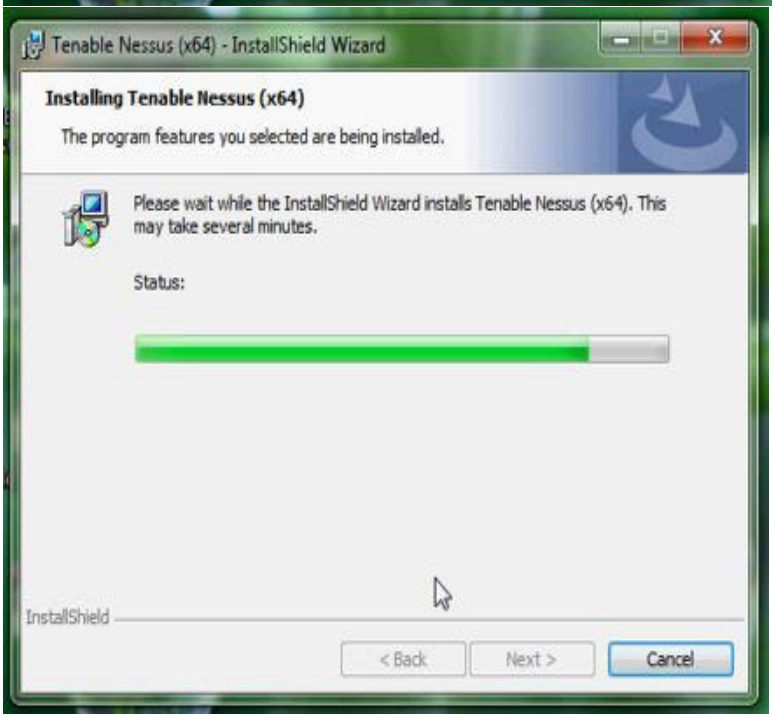


4. Before you begin installation, you must agree to the license agreement as shown in the following figure.
5. Select the radio button to accept the license agreement and click Next.

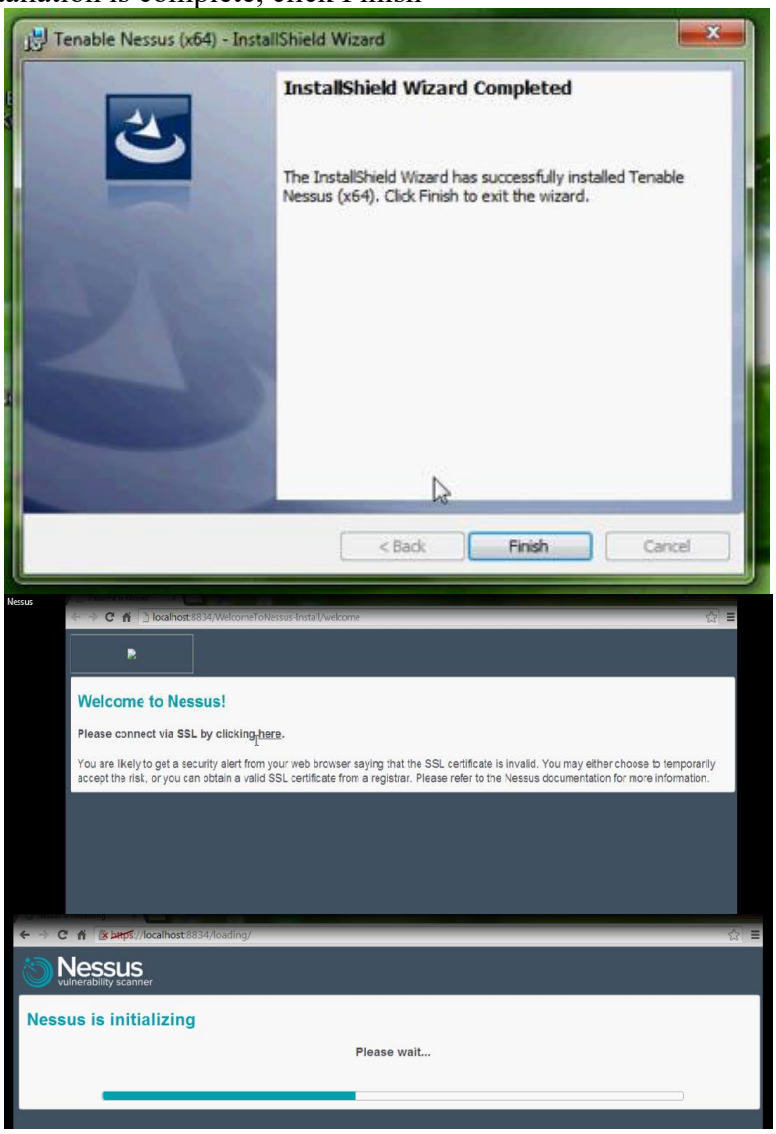


6. The Nessus wizard will prompt you to confirm the installation. Click Install.

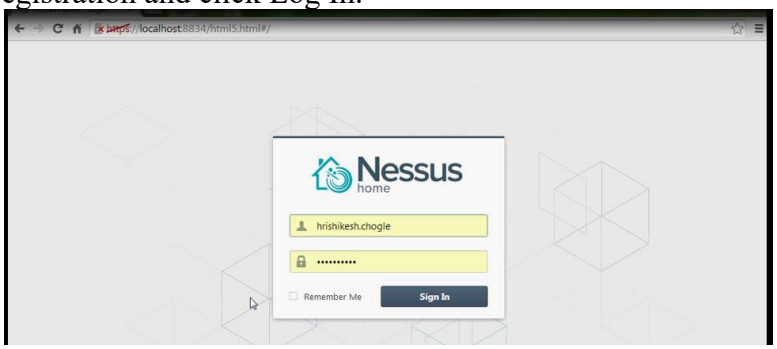


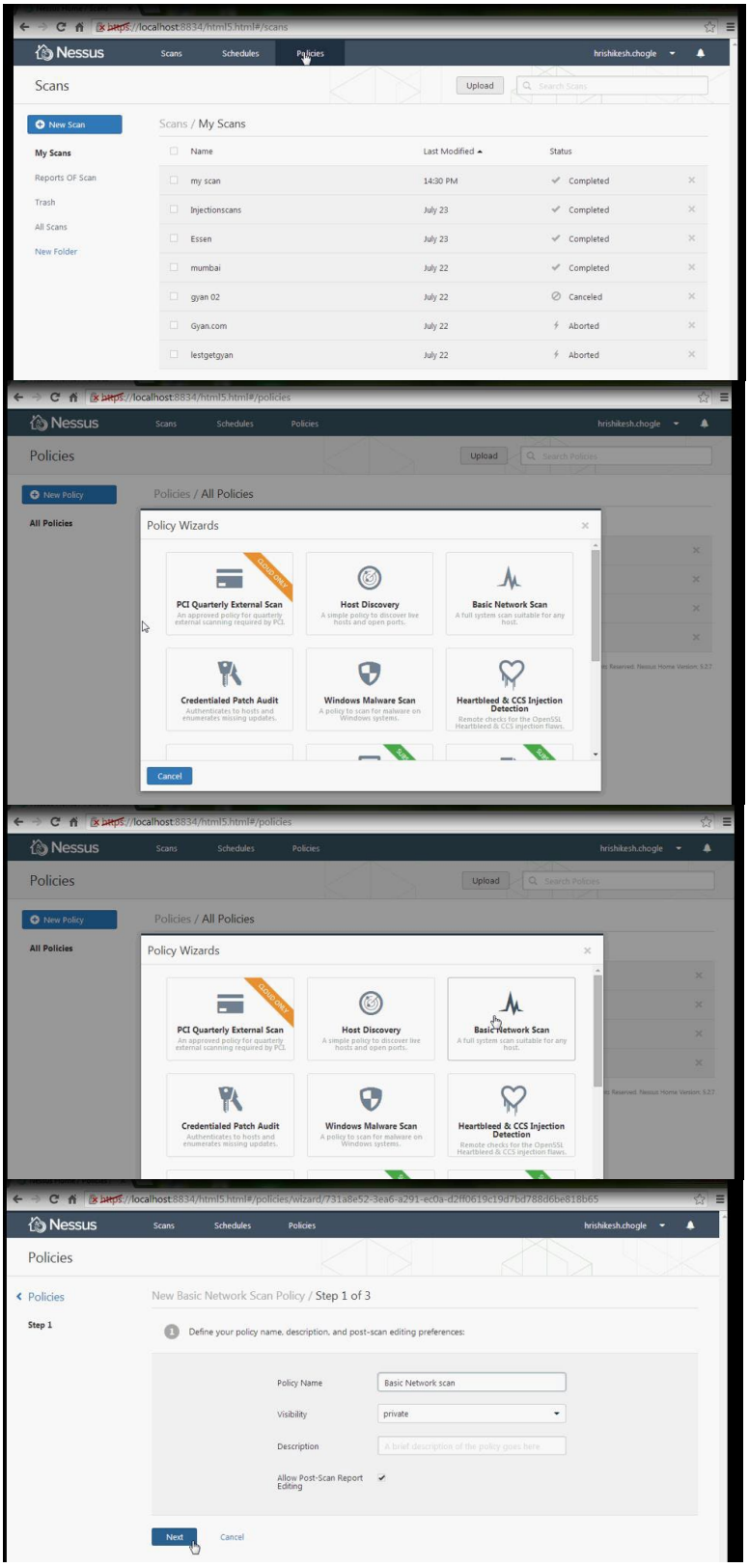
7. Once installation is complete, click Finish

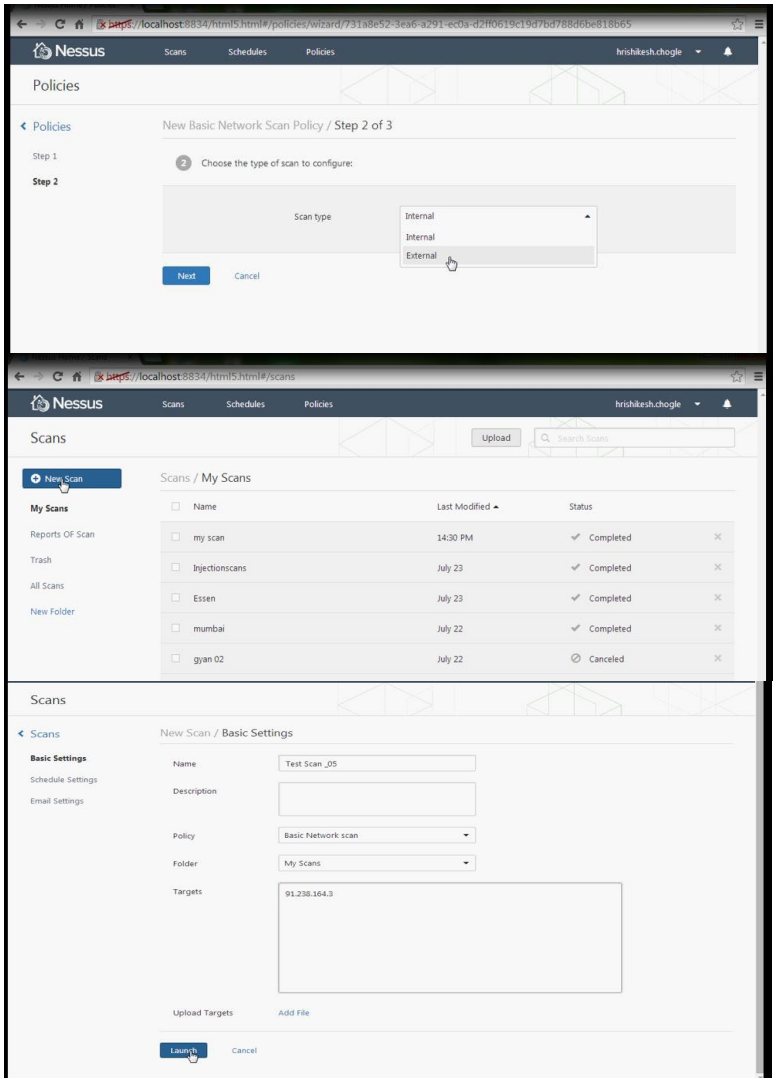



8. The Nessus Log In page appears. Enter the Username and Password given at the time o f registration and click Log In.

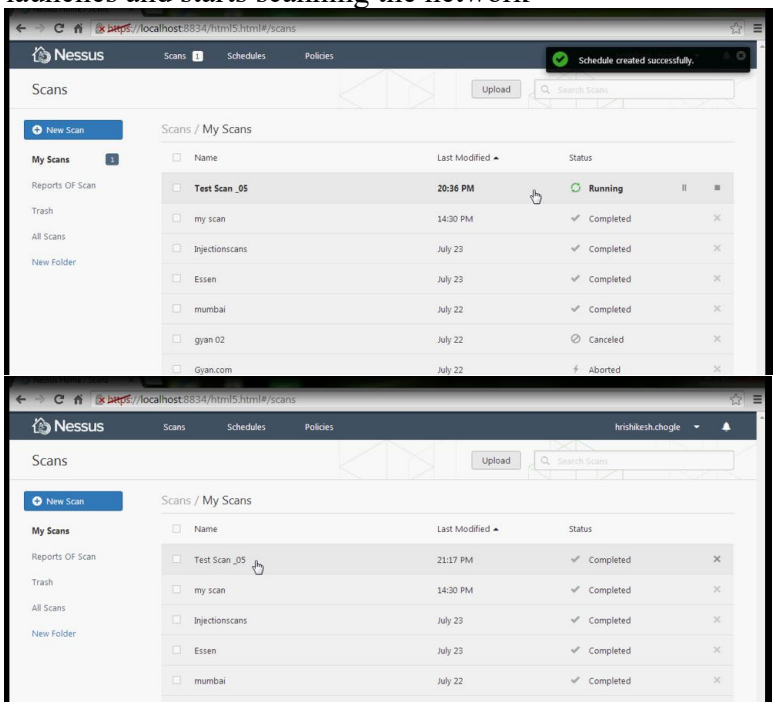


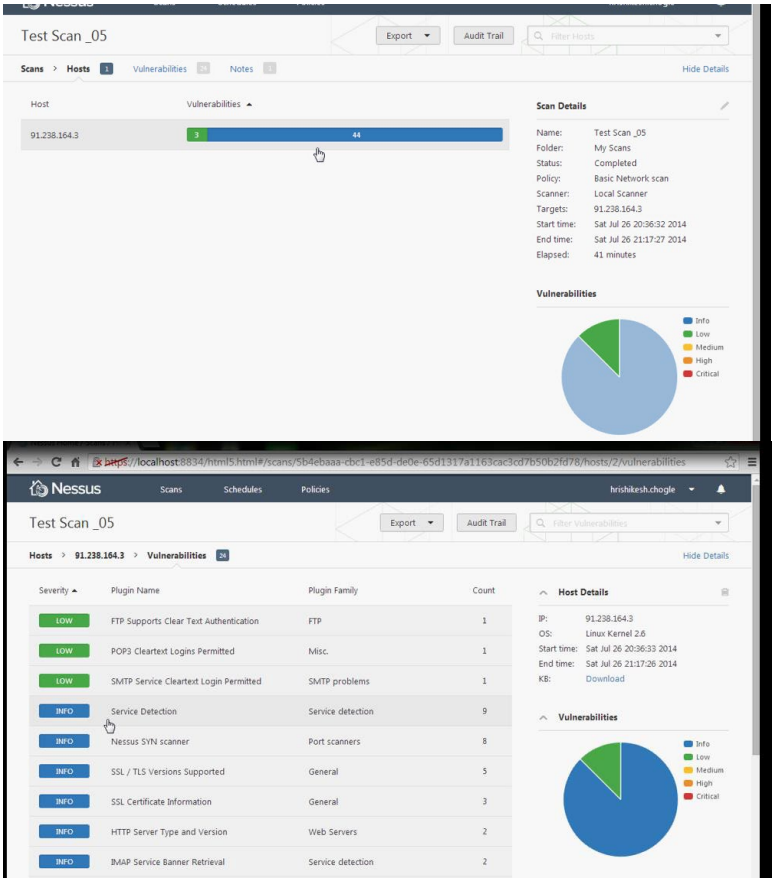
9. To add a new policy, click Policies -> Add Policy. Fill in the General policy sections, namely, Basic, Scan, Network Congestion, Port Scanners, Port Scan Options, and Performance.





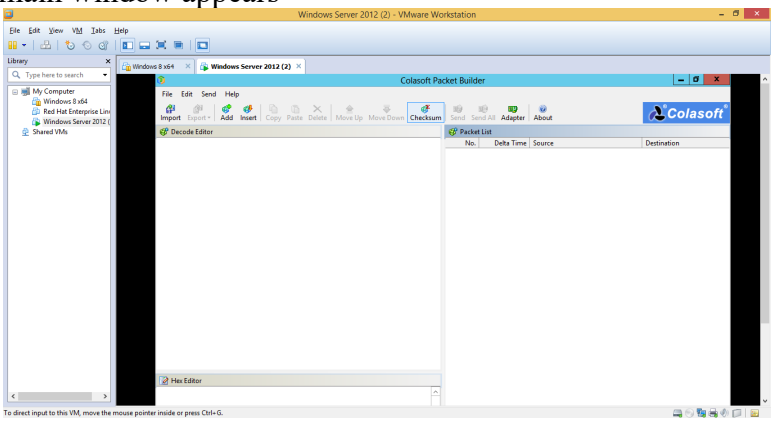

10. The scan launches and starts scanning the network



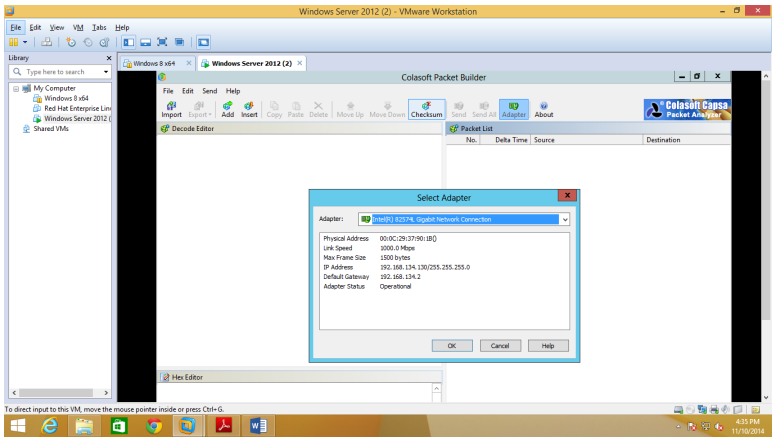



7) Colasoft Packet Builder

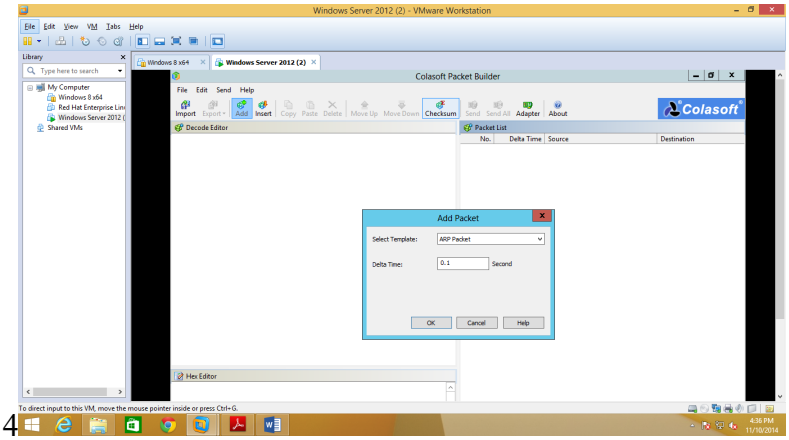
1. Install and Launch the Colasoft Packet Builder.
2. Colasoft main window appears



3. Before starting your task check that Adapter stings are set to Default and then click OK.

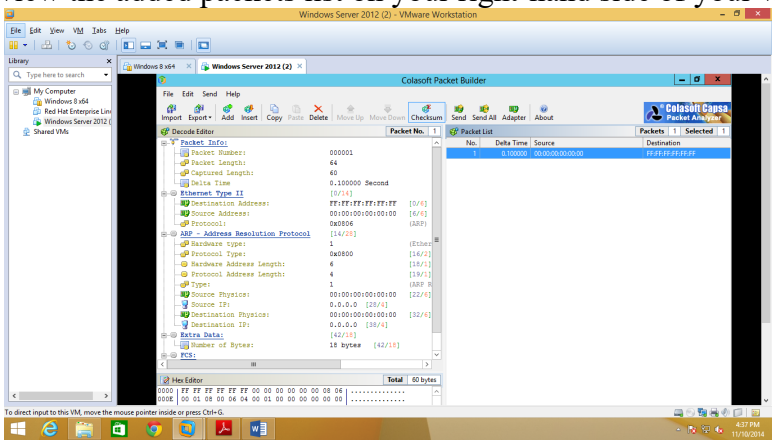



4. To add or create the packet, Click Add in the menu section.
5. When an Add Packet dialog box pops IP, you need to select the template and click OK.

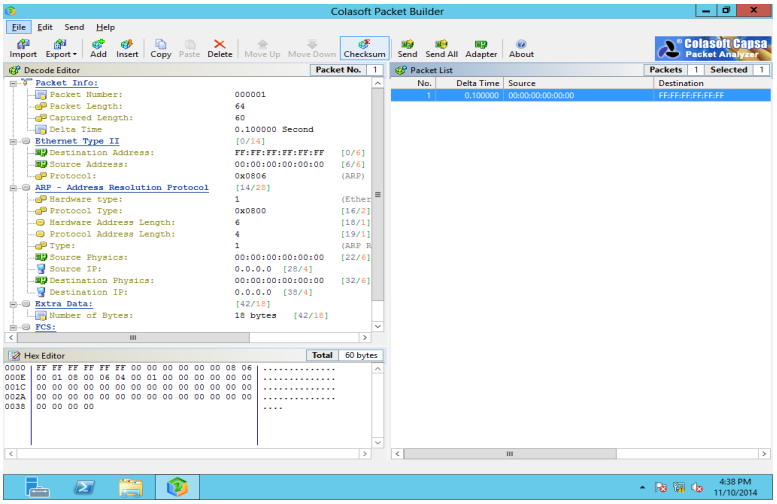



4

6. You can view the added packets list on your right-hand side of your window.

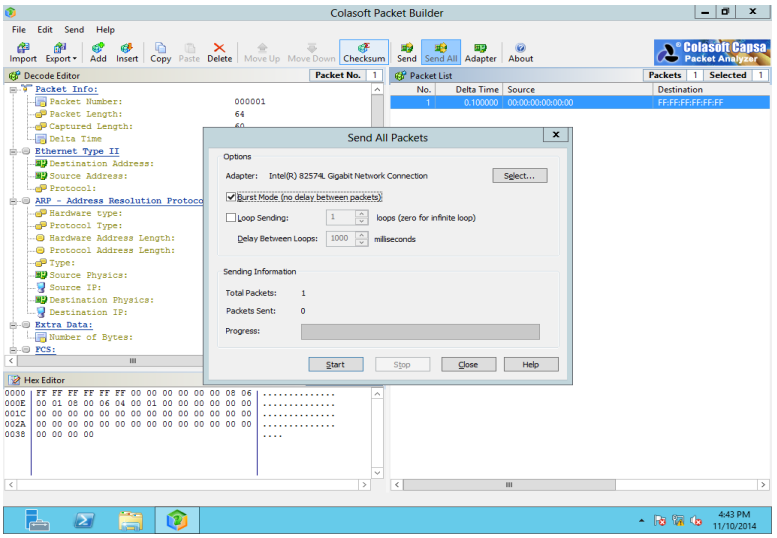



7. Colasoft Packet Builder allows you to edit the decoding information in the two editors: Decode Editor and Hex Editor.

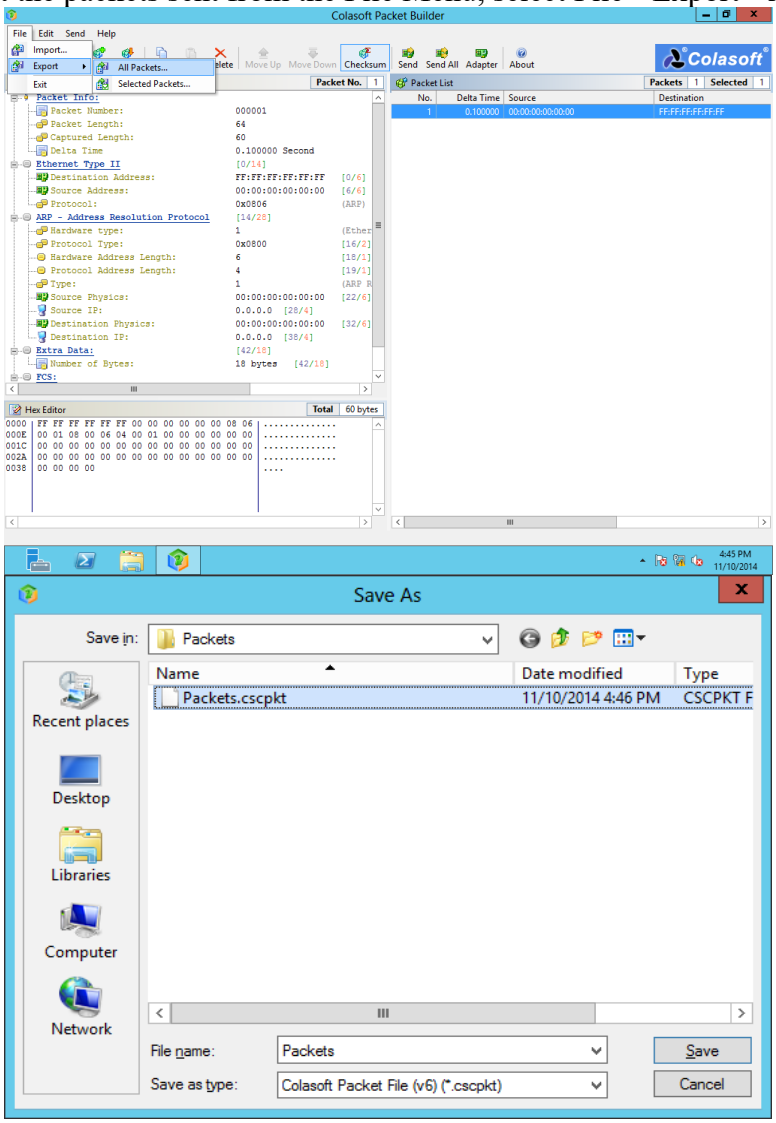



8. To send all packets at one time, click Send all from the menu bar.


9. Check the Burst Mode option in the Send All Packets dialog window, and then click Start

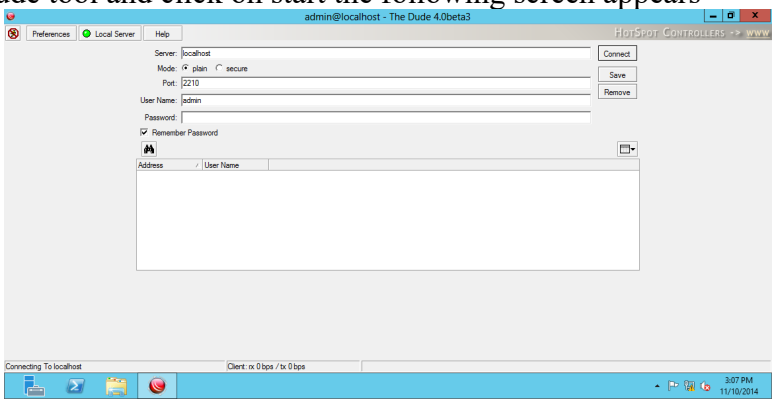


10. Click Start.
11. To export the packets sent from the File Menu, select File->Export->All Packets

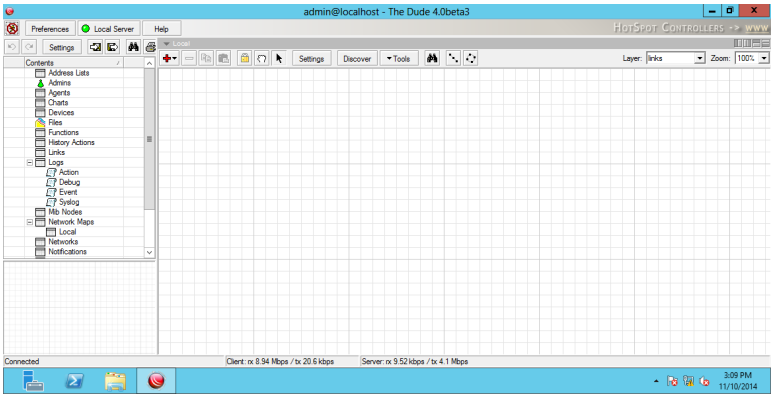



8) The Dude

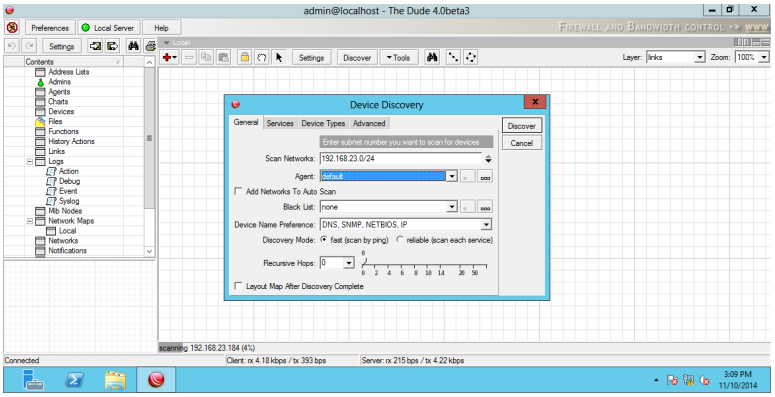
1. Install Dude tool and click on start the following screen appears



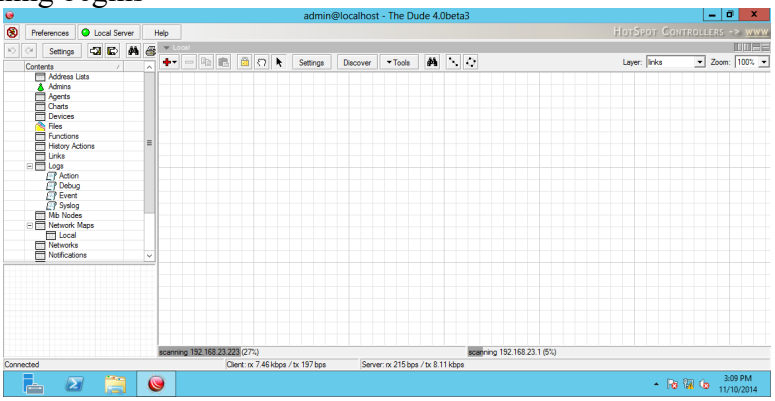
2. Click connect



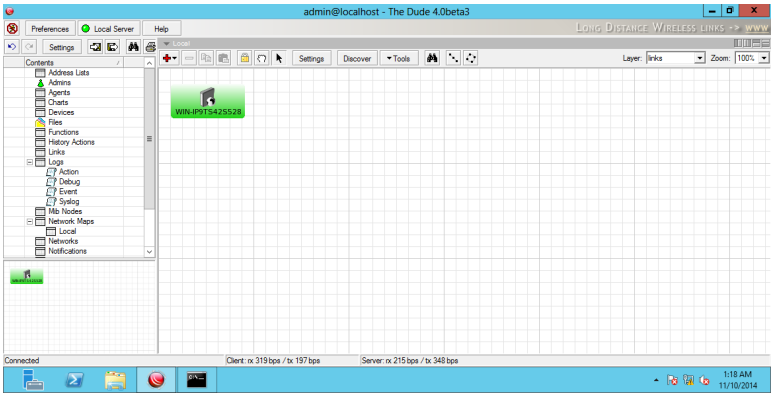

3. Click discover



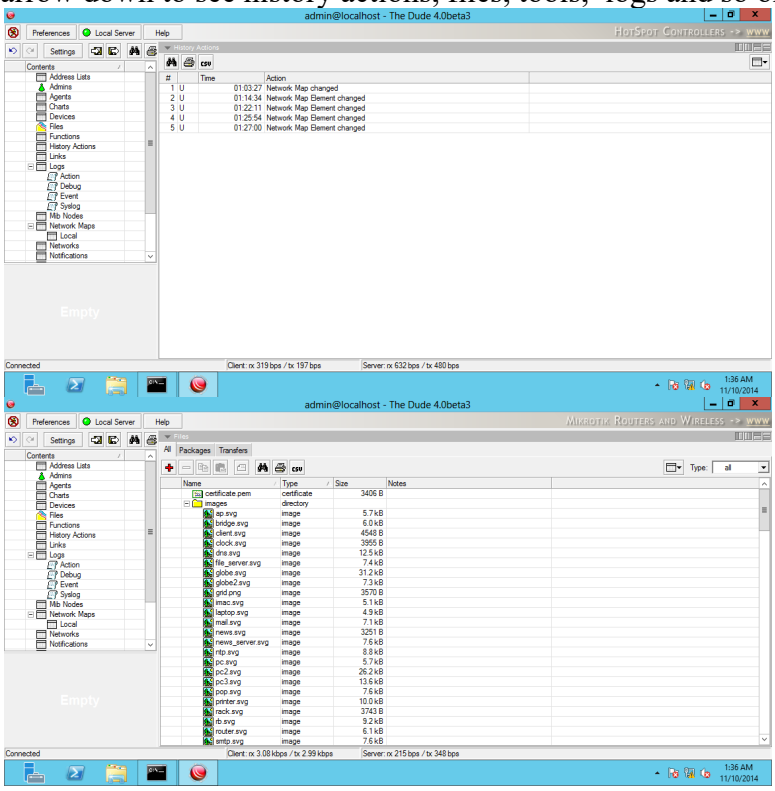

4. The scanning begins




5. Then it shows the network connection



6. Click on arrow down to see history actions, files, tools, logs and so on



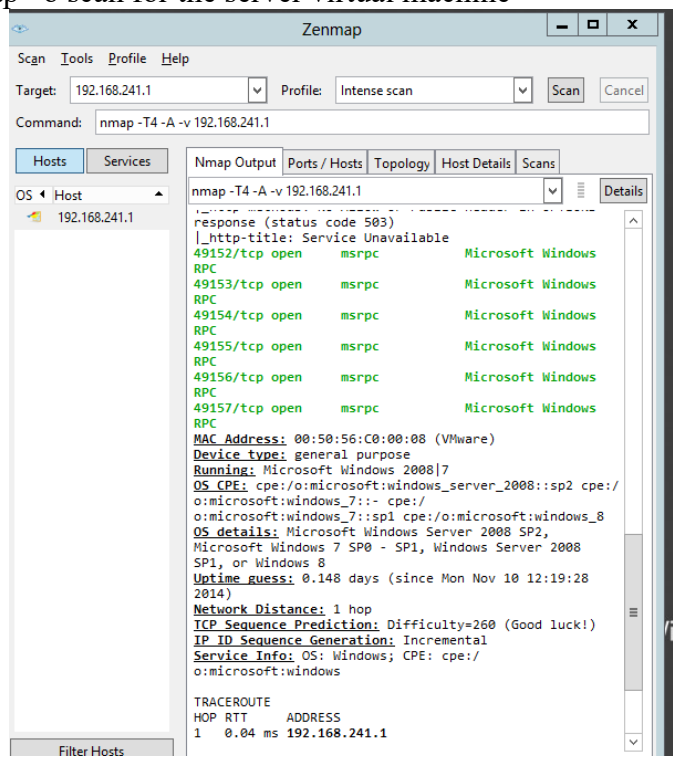

7. Once scanning is complete click “Disconnect button” to disconnect

# PRACTICAL 3

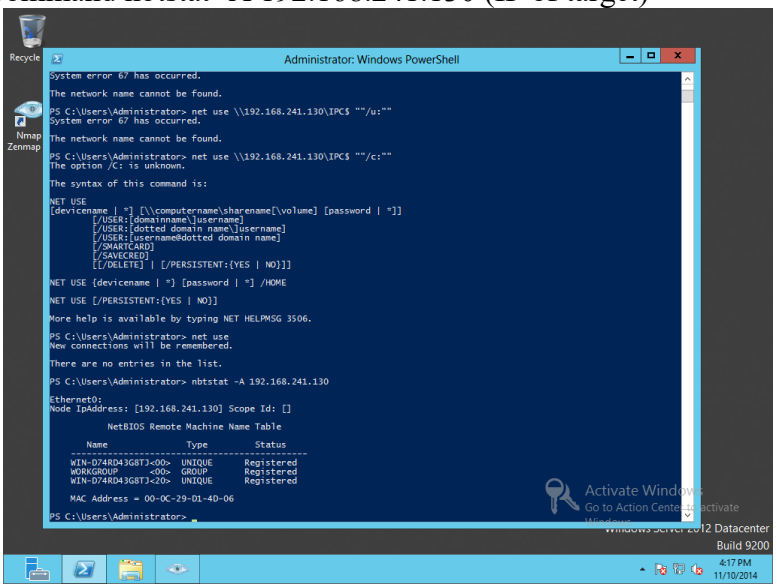
**A. Using NETBIOS Enumeration tool, SNMP Enumeration tool, LINUX/UNIX. enumeration tools, NTP Enumeration tool, DNS analyzing and enumeration tool.**

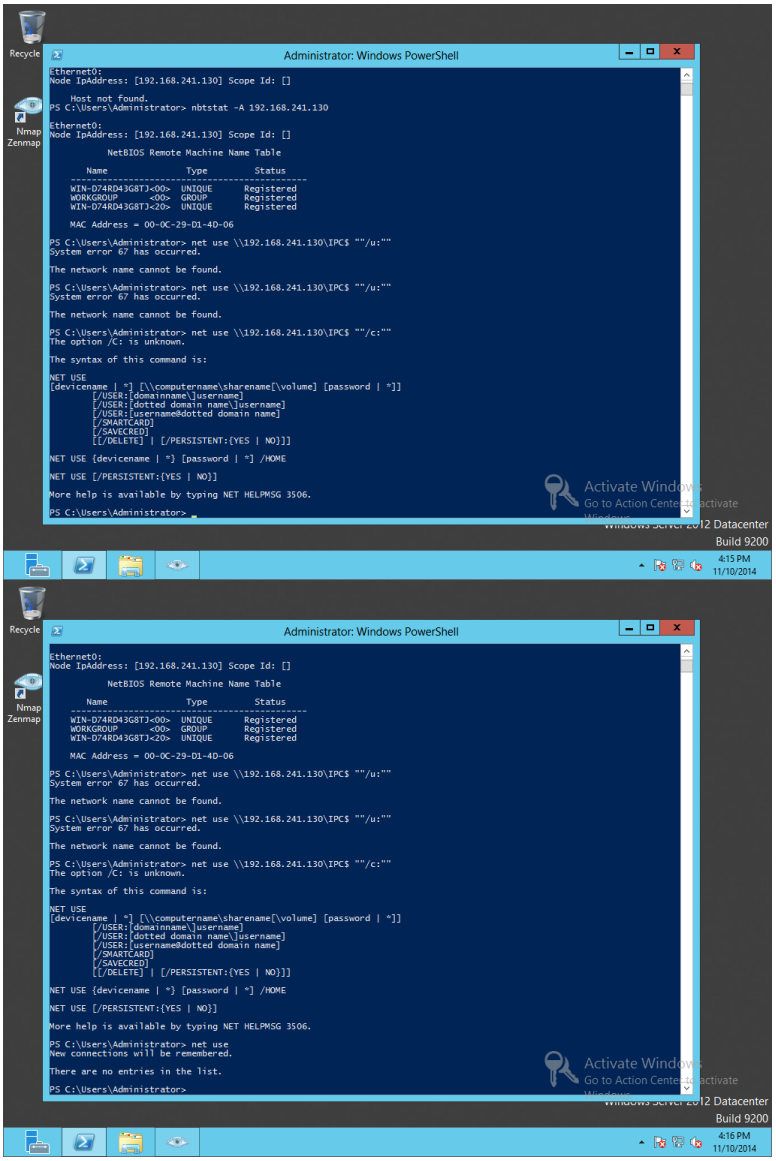
1) Nmap

1. Perform nmap –o scan for the server virtual machine



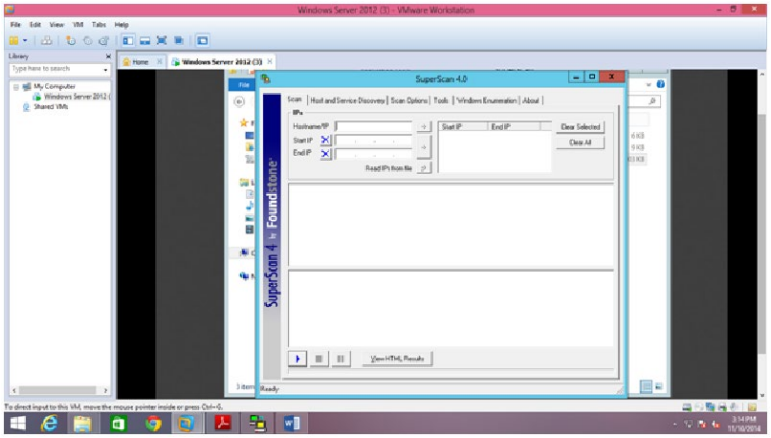

2. Now launch the command prompt in of virtual machine and perform nbtstat on port of target machine
3. Run the command nbtstat -A 192.168.241.130 (IP of target)



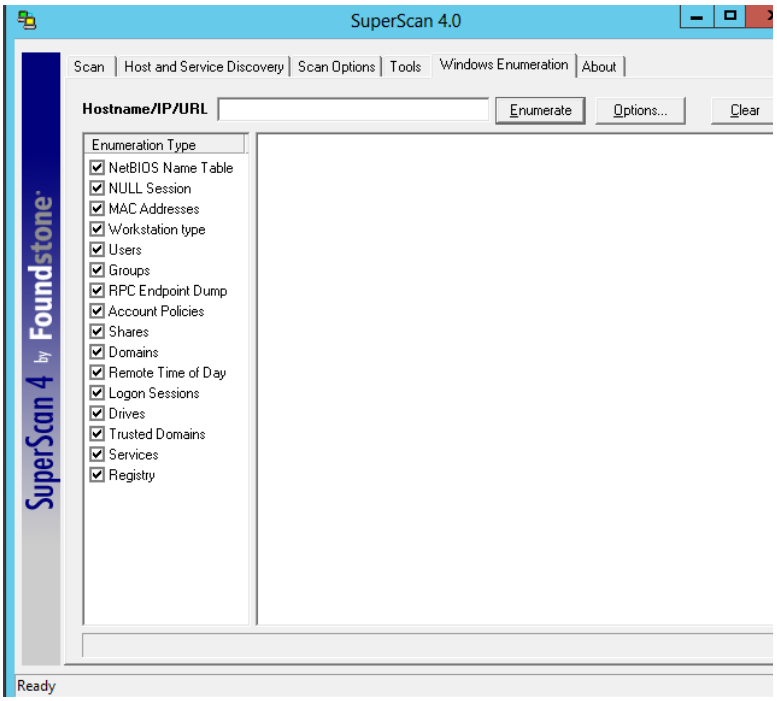



2) SuperScan

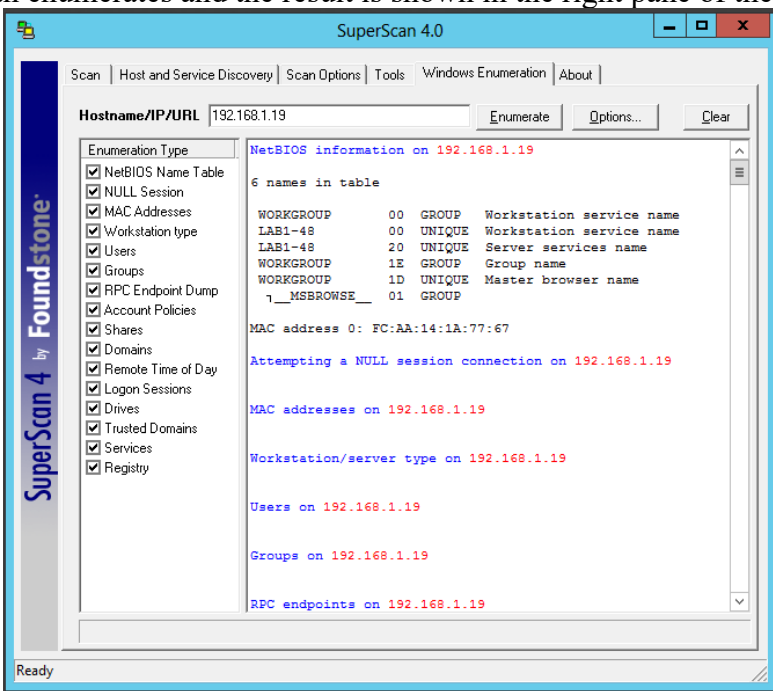
1. Launch SuperScan
2. Click on windows Enumeration tab located on top menu



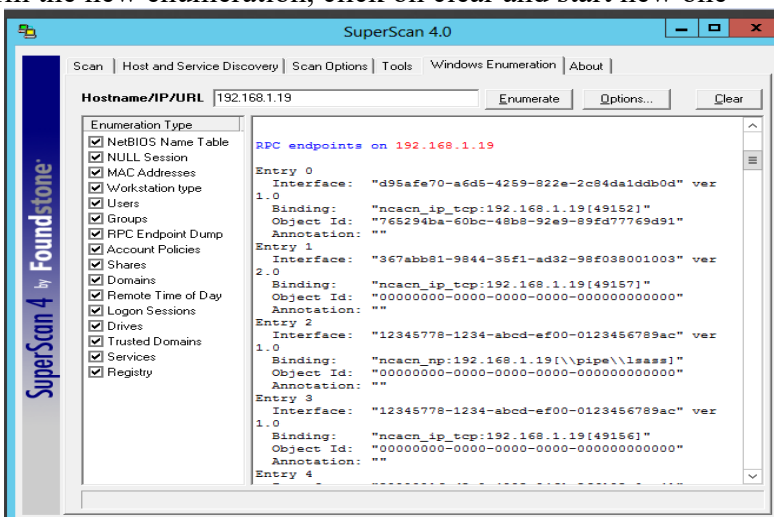
3. Enter host name IP Address of target machine, check the type of enumeration, and click on enumerate

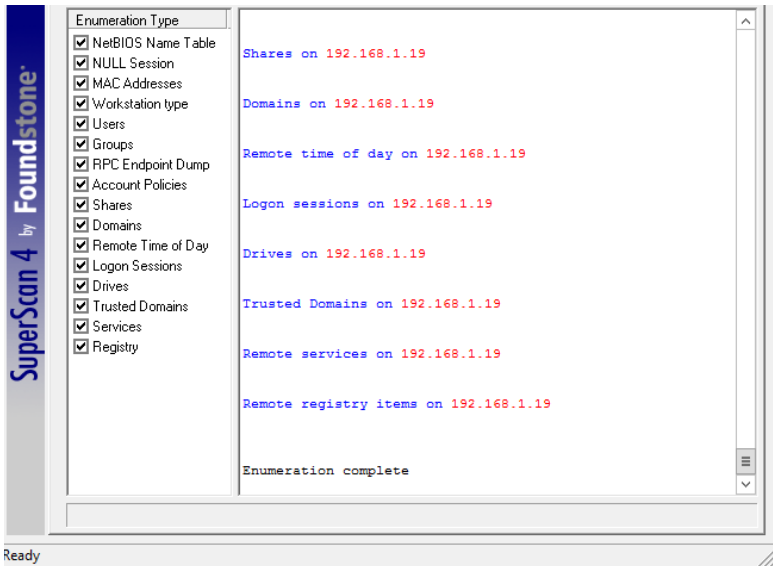



4. SuperScan enumerates and the result is shown in the right pane of the window



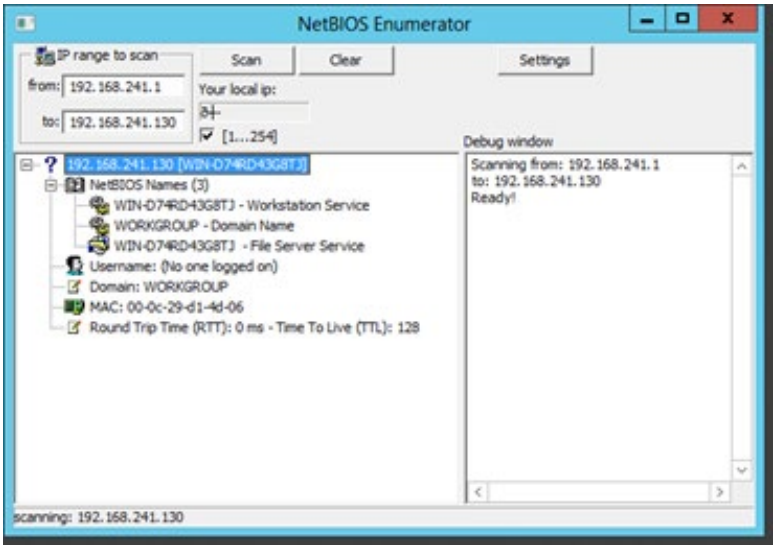
5. To perform the new enumeration, click on clear and start new one



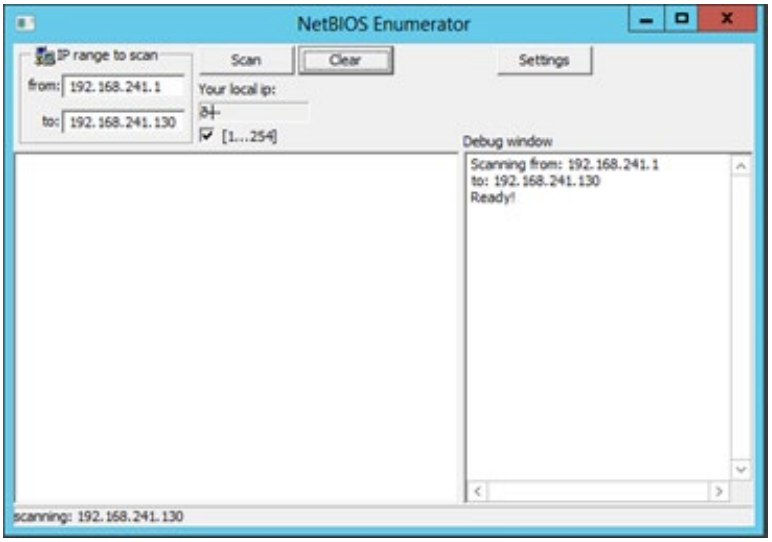




3) NetBIOS Enumerator Tool

1. Launch NetBIOS enumerator
2. In the IP range to scan enter the IP range
3. Click scan

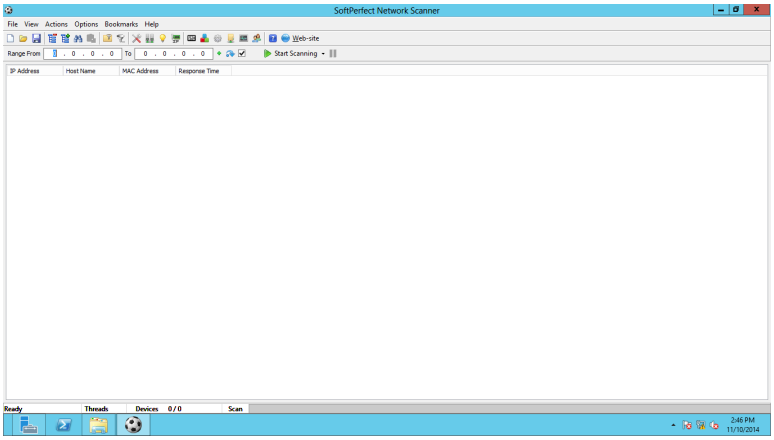


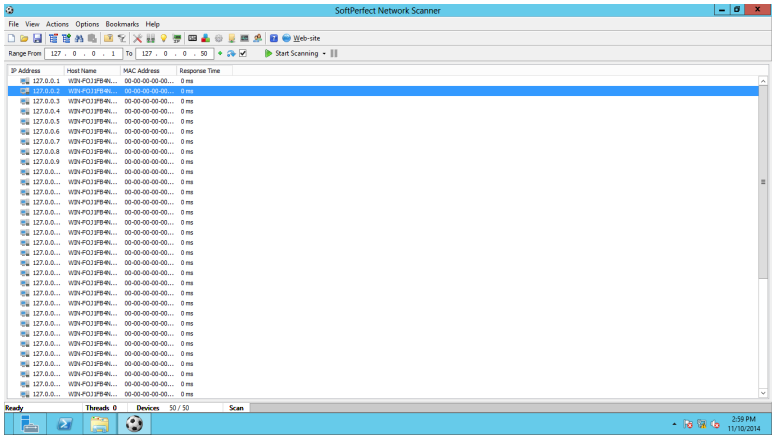

4. To perform the new scan click clear



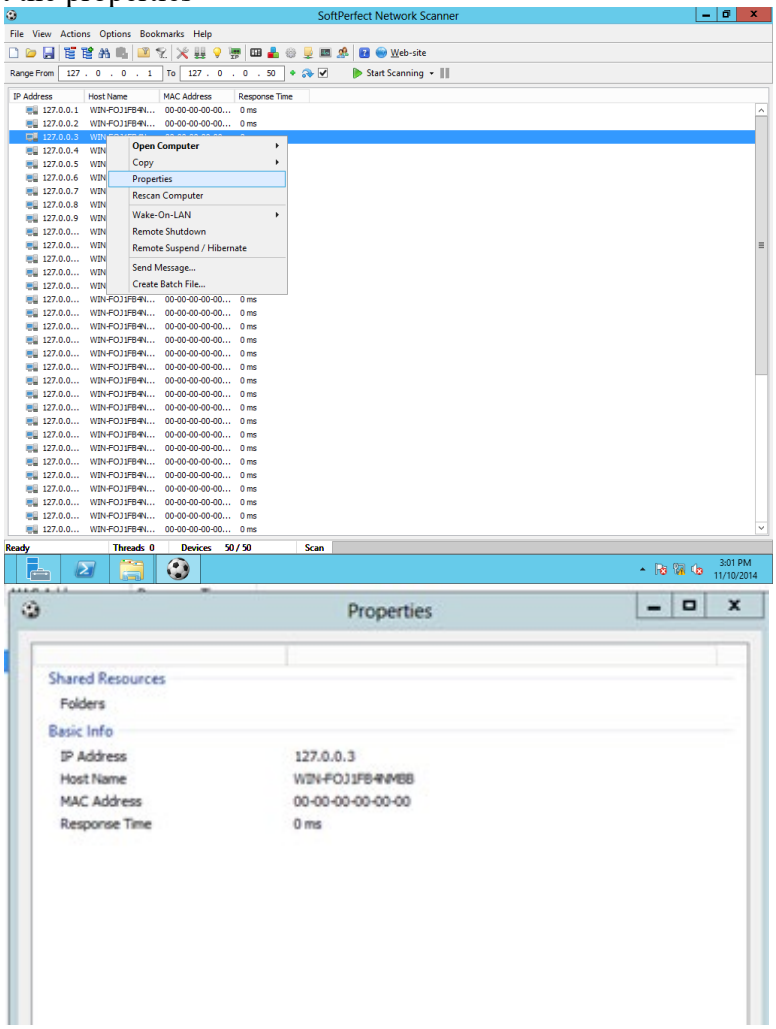

4) SoftPerfect Network Scanner

1. Launch SoftPerfect Network Scanner by double clicking on netScan.exe
2. To start scanning network enter the IP range and start scanning



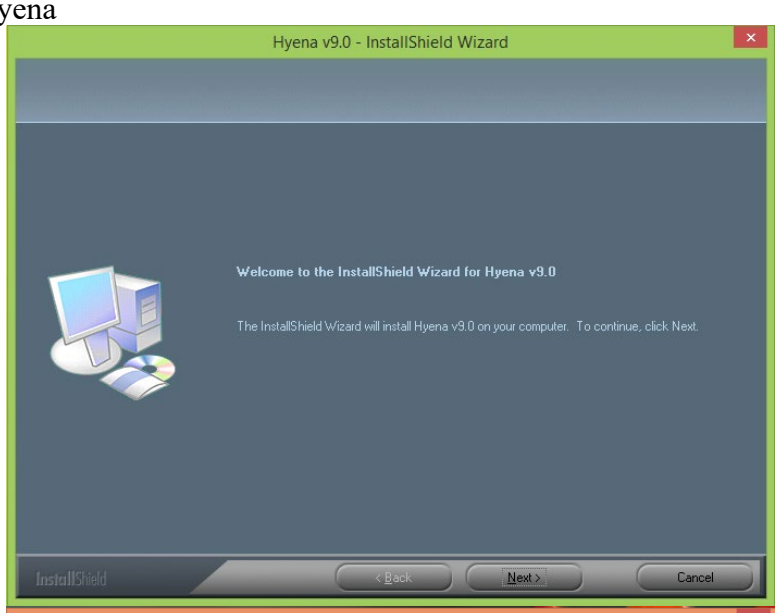


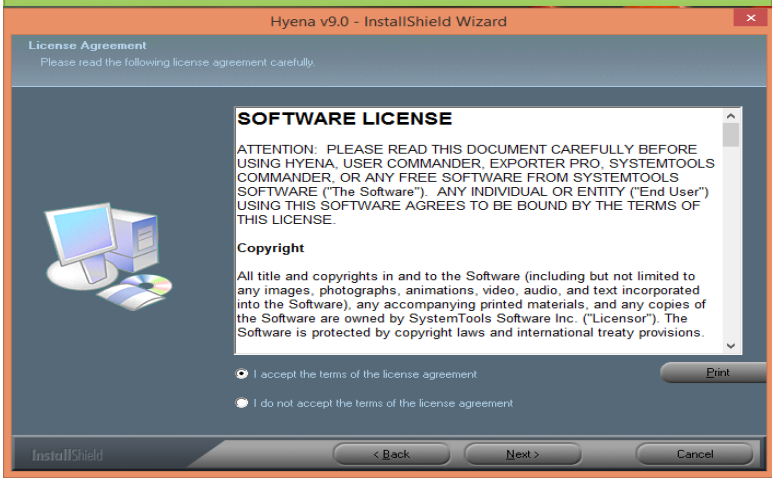

3. To view the properties of the individual IP Address, right click that IP Address and select the properties

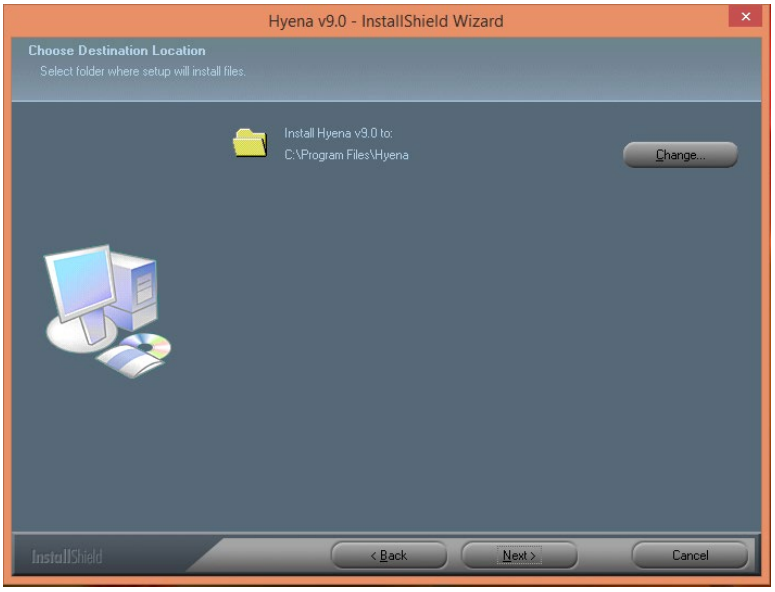


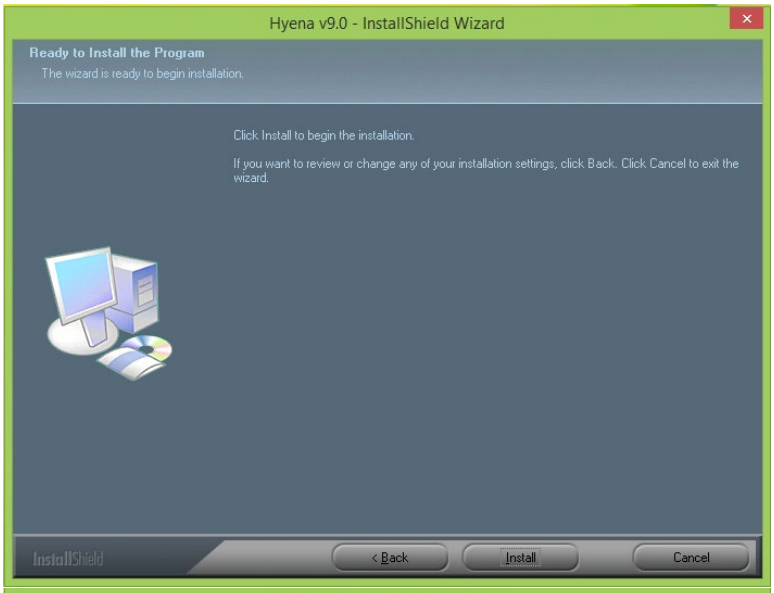
5) Hyena

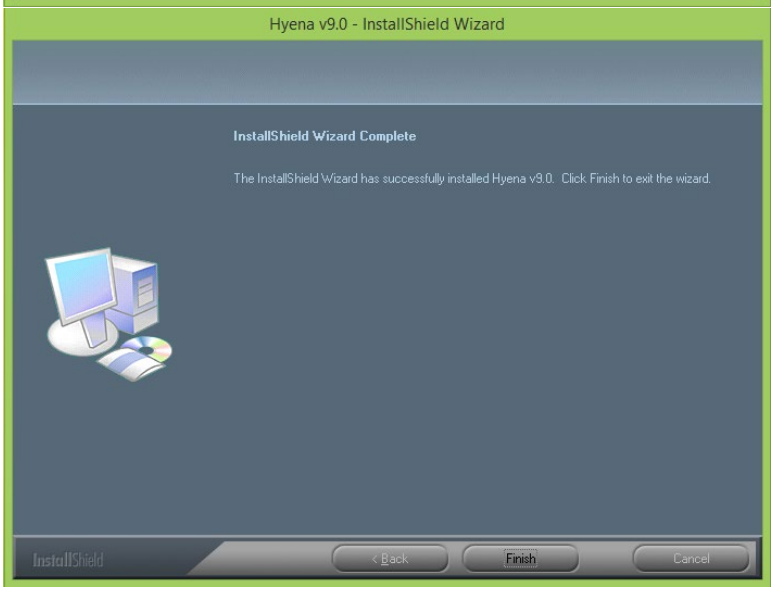
1. Install Hyena

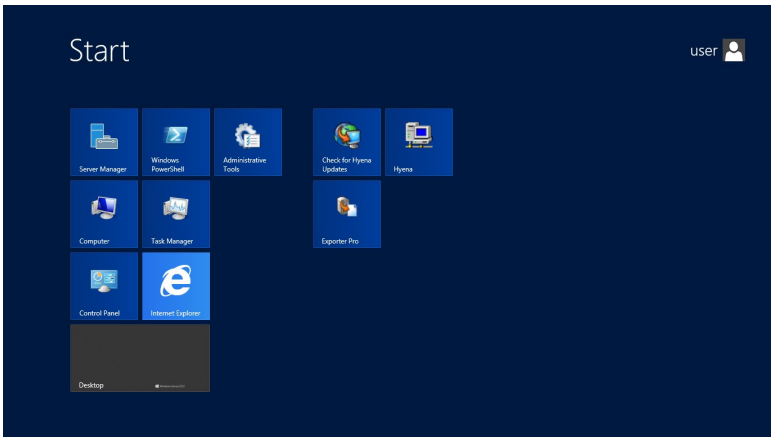


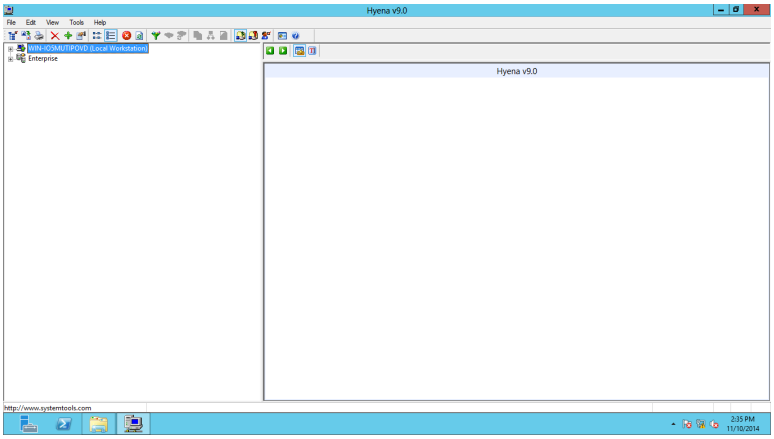





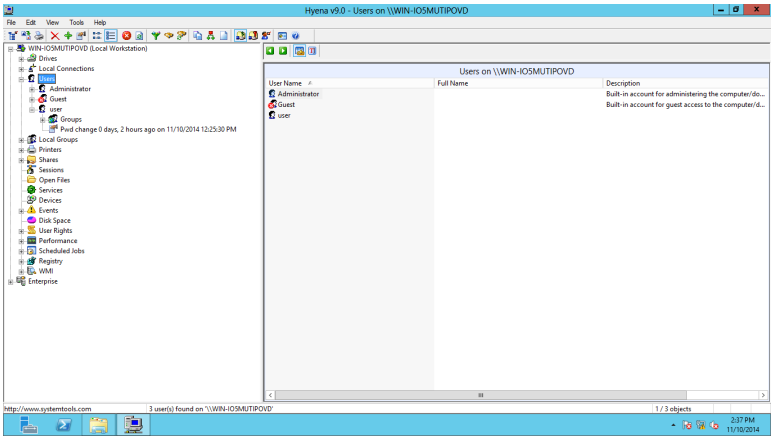



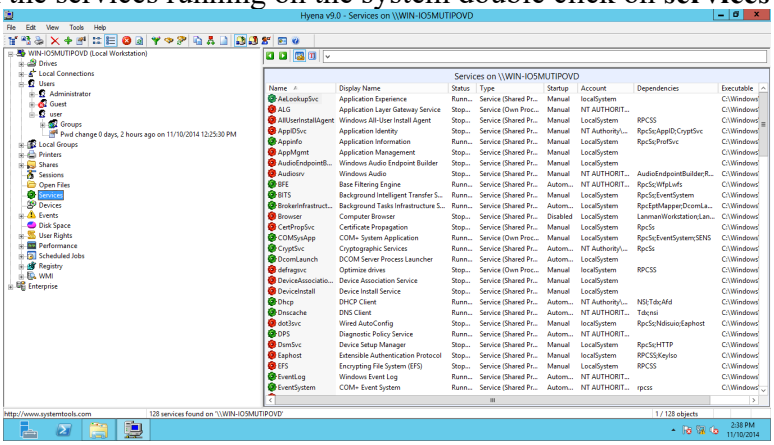

2. The registration window will appear, click ok to continue
3. The main window of hyena is shown below



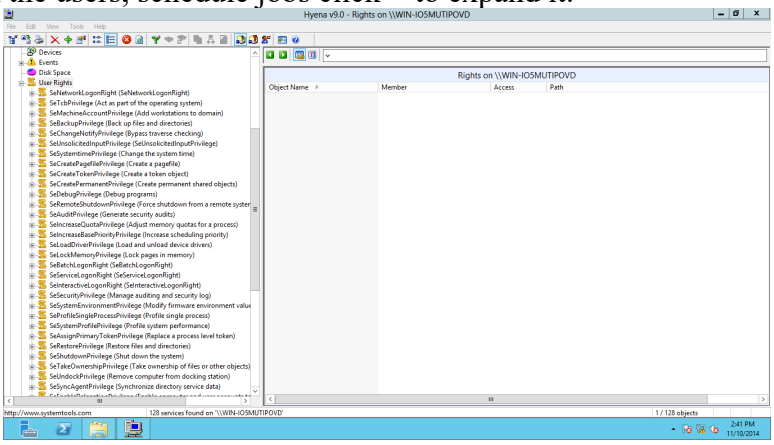

4. Click + to expand the local work station and click Users.




5. To check the services running on the system double click on **services**



6. To check the users, schedule jobs click + to expand it.



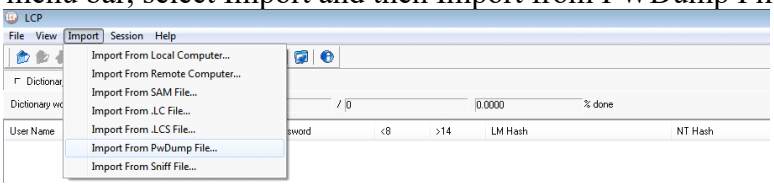
# PRACTICAL 4

## A. Study of System Hacking tool

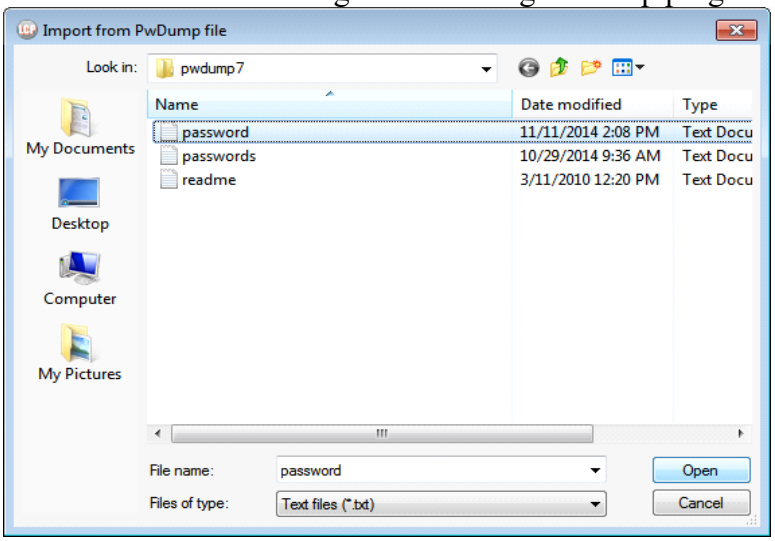
1) LCP

1. Extract the SAM Hashes by using PwDump7 program
2. Pwdump7.exe > password.txt

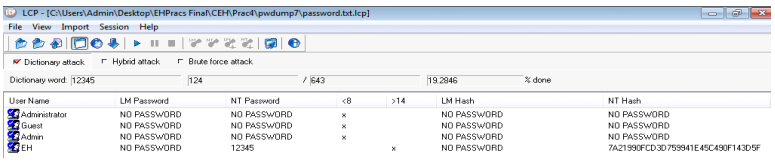

3. This PWDump file will be used for many programs in this practical
4. From the menu bar, select Import and then Import from PWDump File.




5. Select password.txt file which was generated using Pwdump program

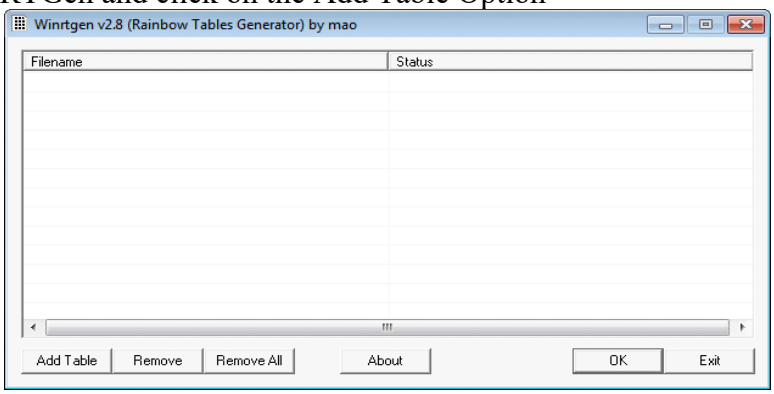



6. After opening the file, hit the play button in LCP window to start cracking the SAM Hashes

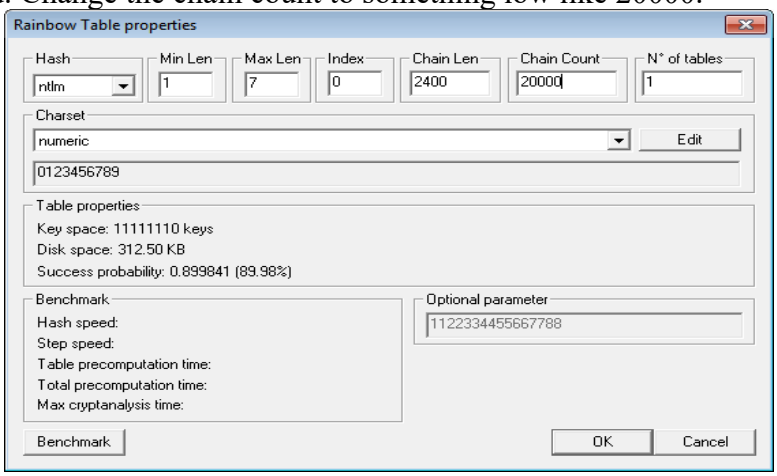


2) RainbowCrack and WinRTGen

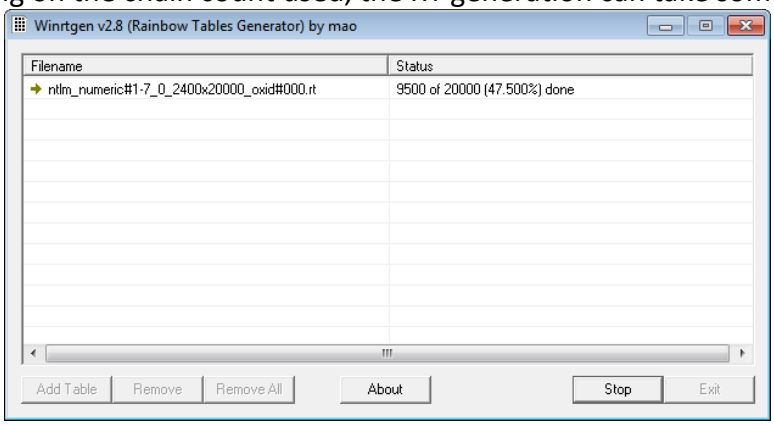
1. Run WinRTGen and click on the Add Table Option



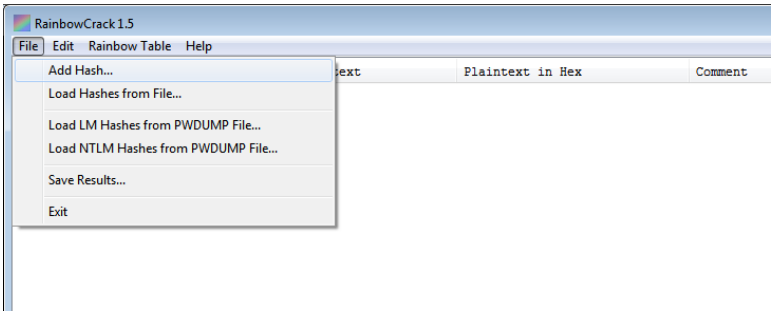

2. Select the Hash to target, the minimum and maximum length of the guessed password. Change the chain count to something low like 20000.



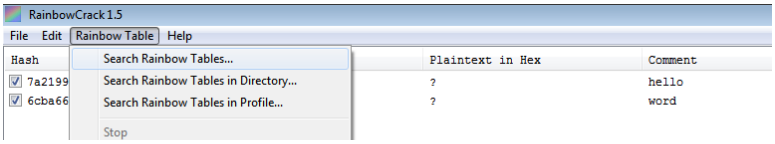

3. You can choose the charset to use. Numeric will only generate a RT of numeric passwords.
4. Click on OK and click on OK at the next screen to start generating the RT. Depending on the chain count used, the RT generation can take some time.

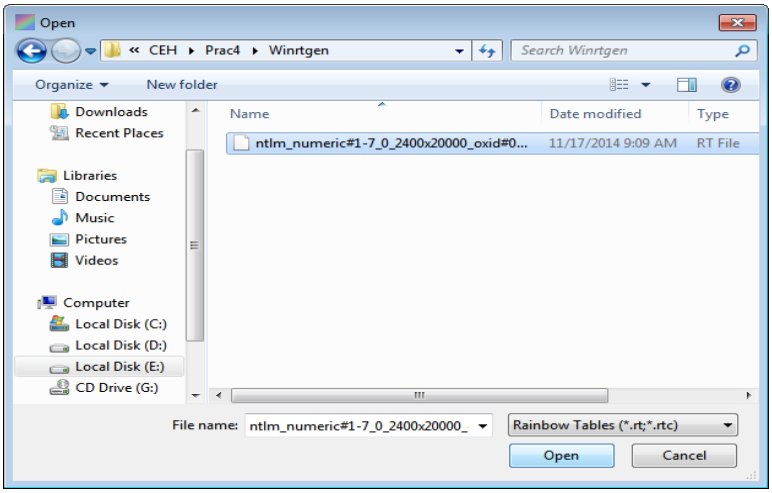



5. Run rgrack_gui.exe to run RainbowCrack
6. Go to File -> Load Hashes from PWdump file

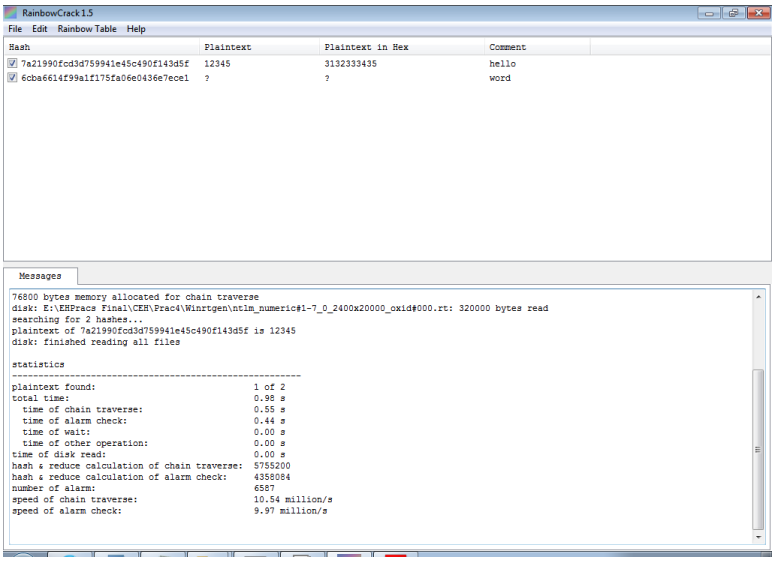



7. Once they are loaded, they will show the accounts in the window.
8. Go to Rainbow Table -> Search Rainbow Tables, and select the RT generated by WinRTGen



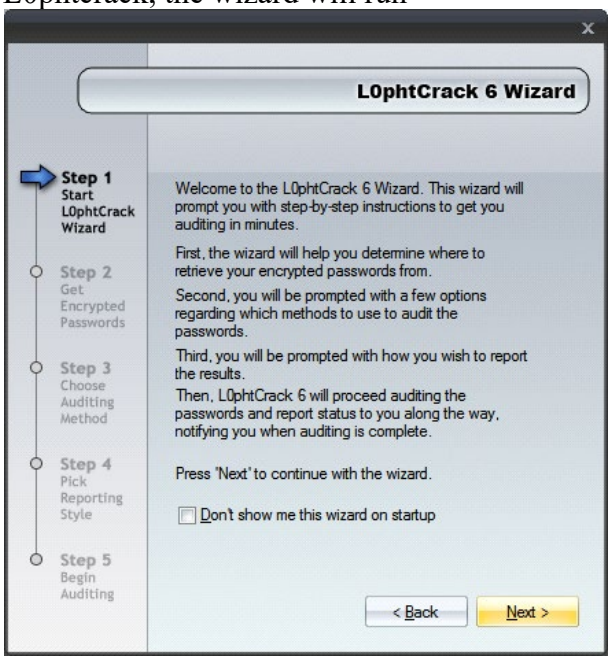




9. It will then crack the password using the Rainbow Table and show the passwords in plaintext



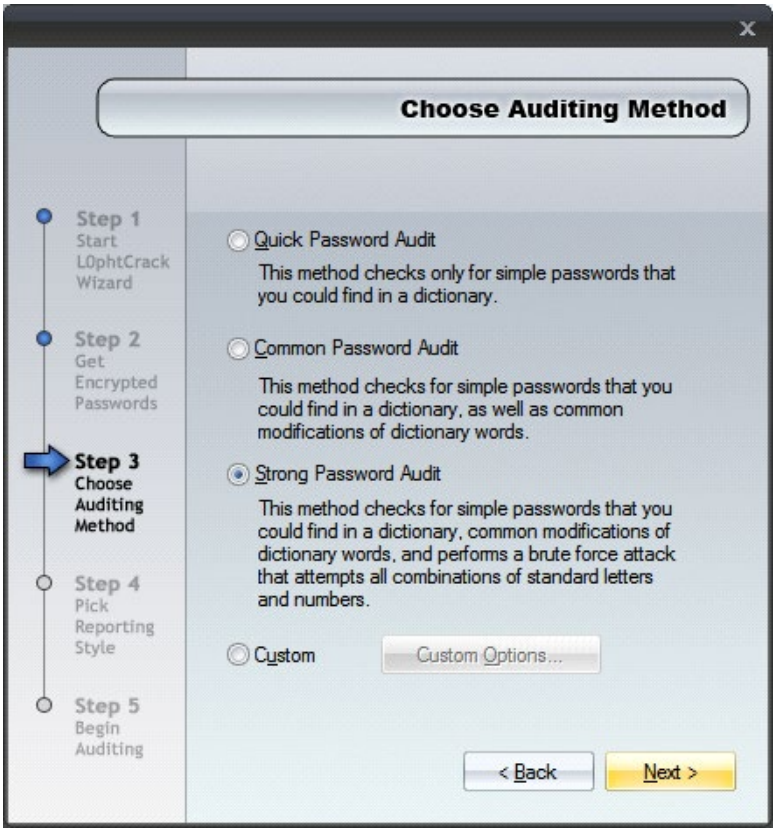
3) L0pthCrack

1. When you start L0phtcrack, the wizard will run

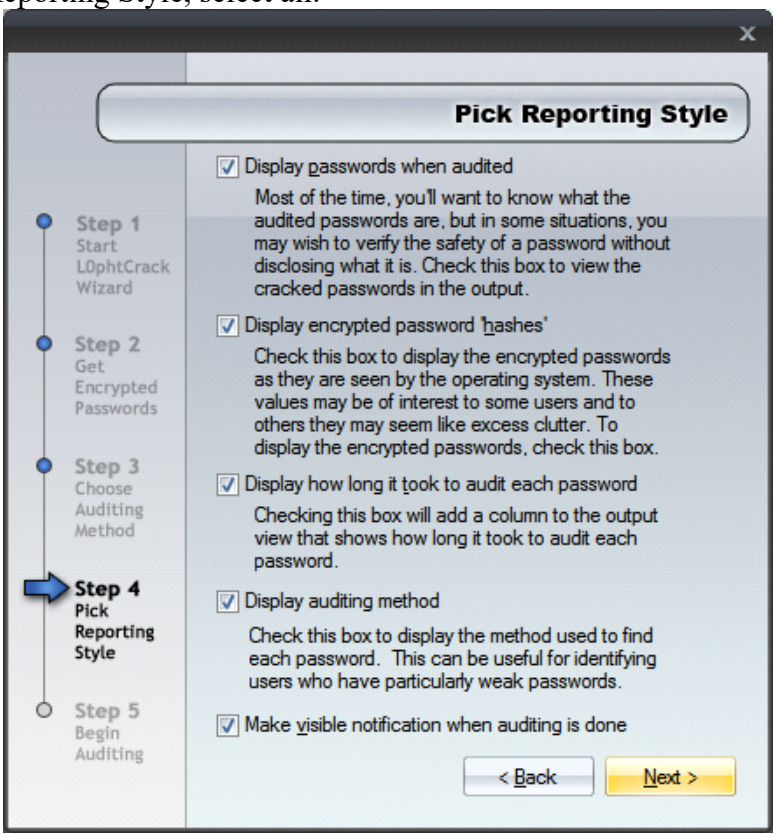



2. Choose Retrieve from the local machine in the Get Encrypted Passwords wizard and click Next

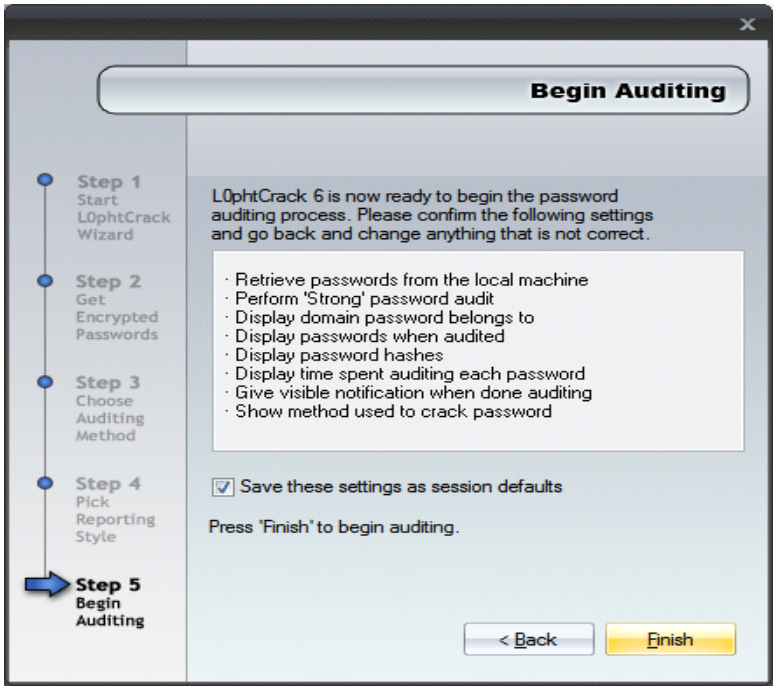

3. Choose Strong Password Audit from the Choose Auditing Method wizard and click Next



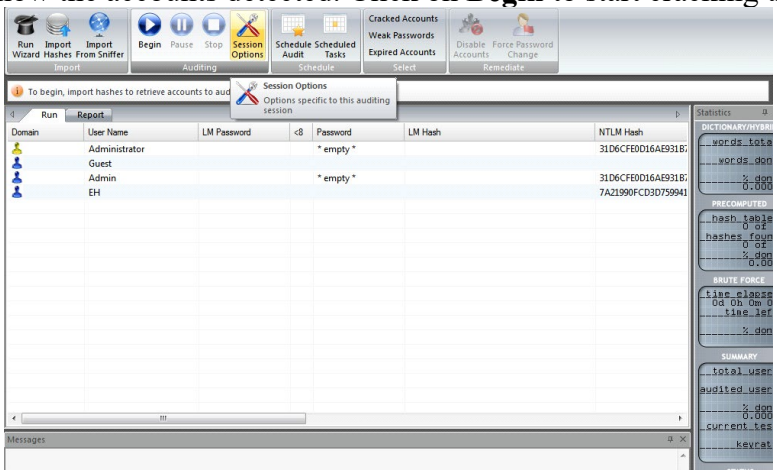

4. In Pick Reporting Style, select all.



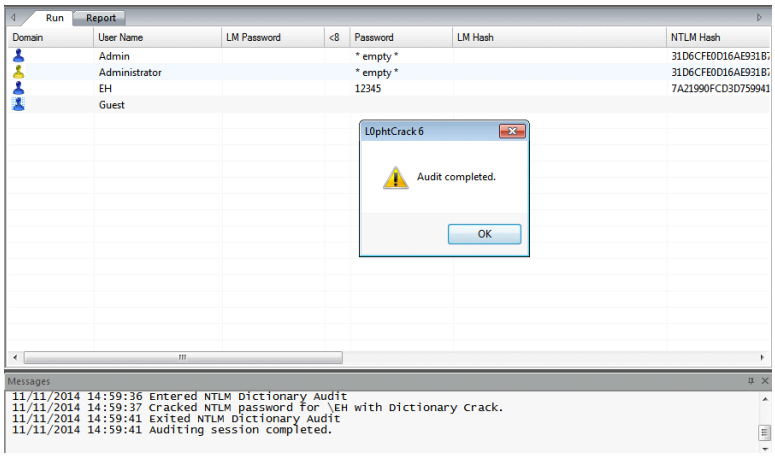

5. Click Finish




It will then show the accounts detected. Click on **Begin** to start cracking the password

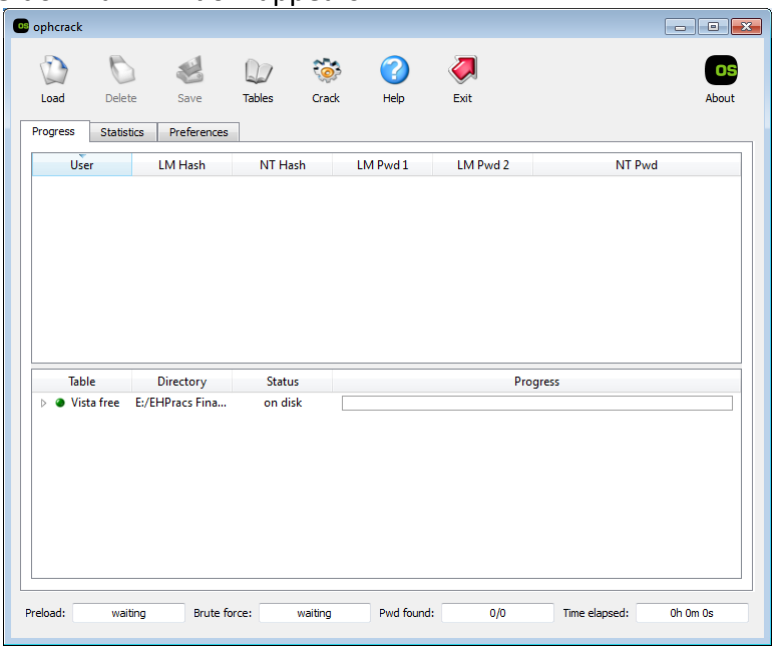



6. A report is then generated and shows the cracked passwords

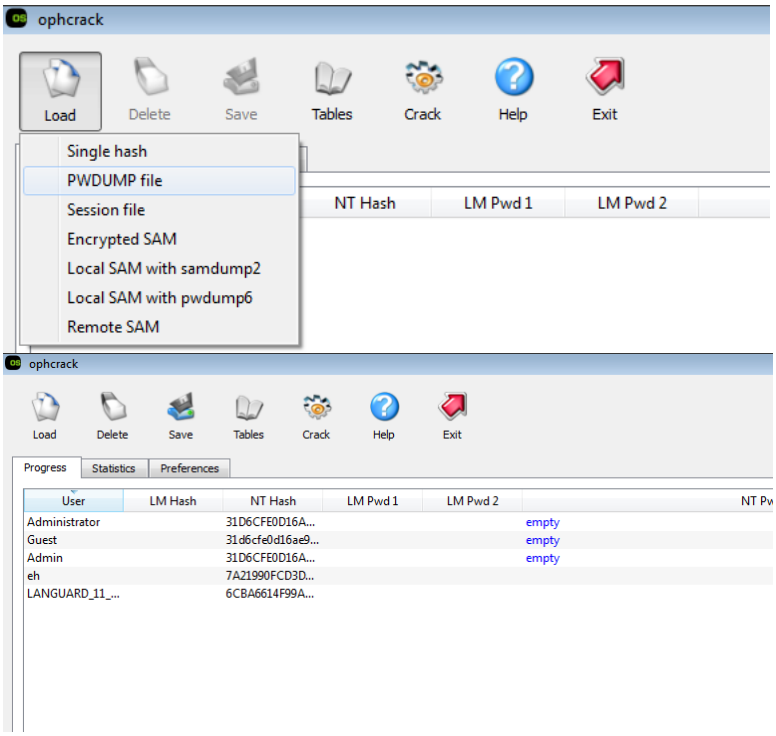


4) Ophcrack

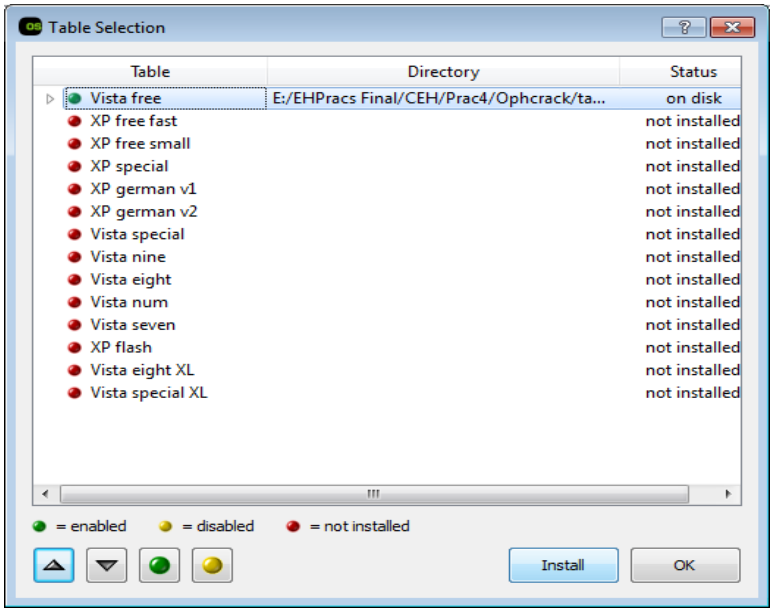
1. Open OphCrack.
2. The **OphCrack** main window appears.



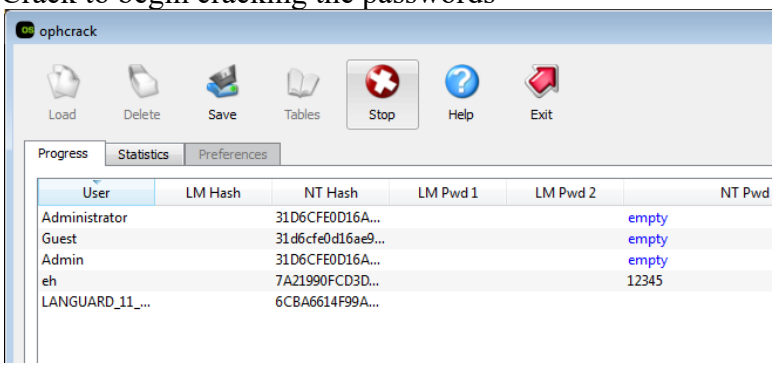

3. Click Load, and then click PWDUMP file. Browse to the location where the extracted PWDump passwords file is and select it. Upon selection, it will load the hashes into the window.




4. Click Table. The Table Selection window will appear as shown in the following figure.
5. Select the appropriate version depending on the system from where the PWdump file was generated.

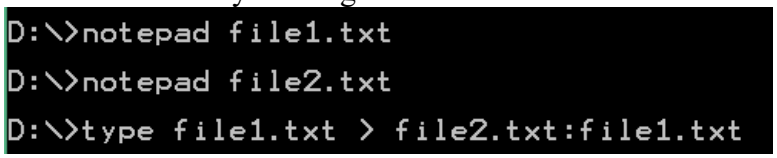



6. The Browse for Folder window appears; select the folder that has downloaded and extracted tables_<OS>_free and click Install.
7. When the tables have been installed properly, they will turn green. Click on OK
8. Click on Crack to begin cracking the passwords

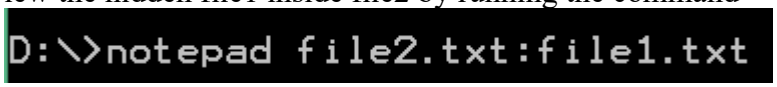


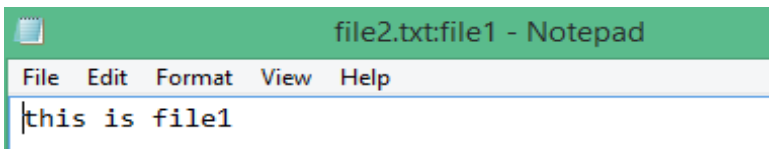

5) NTFS ADS

1. Create two files, file1.txt and file2.txt and let them both have some data. Note down each files file size.
2. We hide file1 inside file2 by running the command



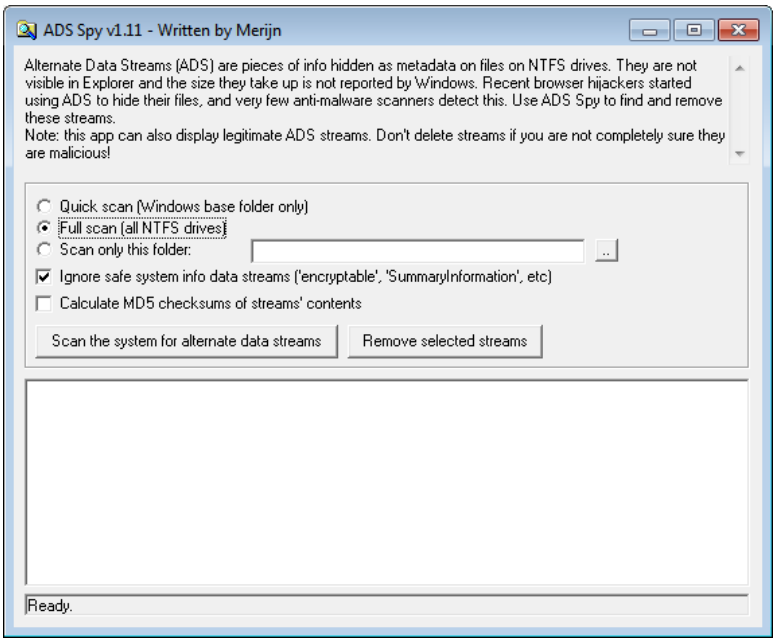

3. We can view the hidden file1 inside file2 by running the command



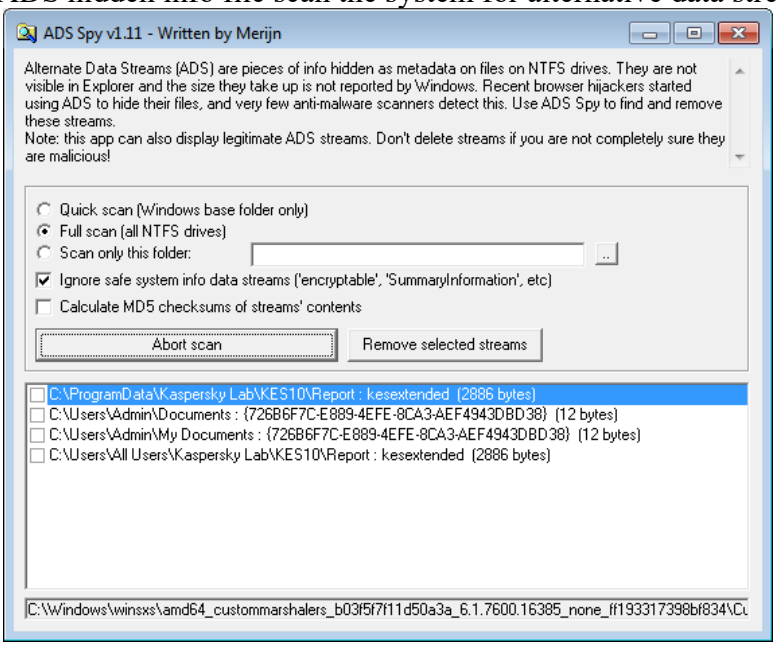



6) ADS Spy

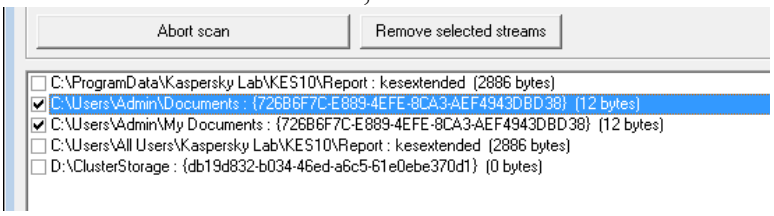
1. Launch ADS Spy.
2. Select a folder to scan by choosing Scan only this folder and click scan the system for alternate data streams.




3. Find the ADS hidden info file scan the system for alternative data streams.

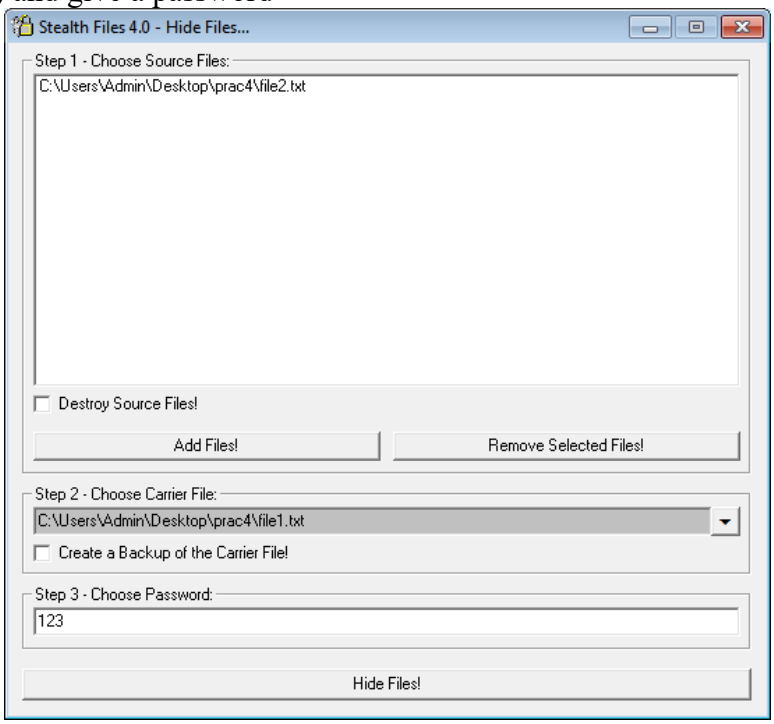



4. To remove the Alternate Data Stream, click Remove selected streams. Click Yes

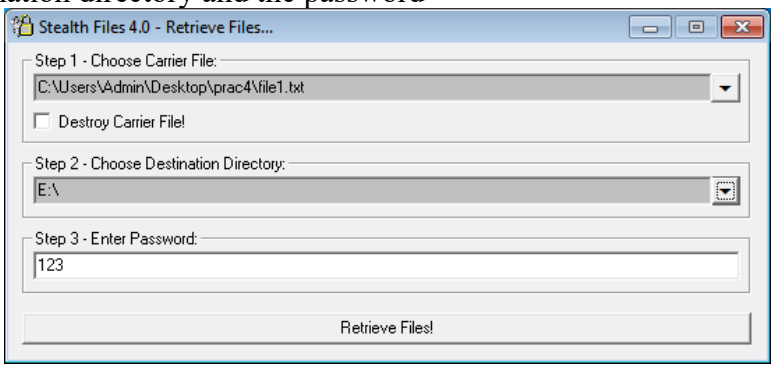


7) Stealth Files Tool

1. Create a file named file1.txt and let it have some data.
2. Run Stealth Files Tool, and click on the Hide Files button
3. Choose the source file (file1.txt) and choose the carrier file (File to hide file1 inside of) and give a password



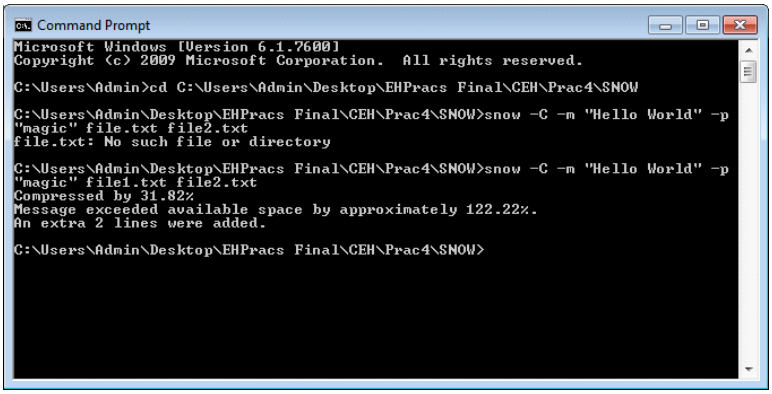

4. When you click Hide Files, it will hide the source file inside of the carrier file.
5. To retrieve the hidden file, click on Retrieve files button. Choose the Carrier File, the destination directory and the password



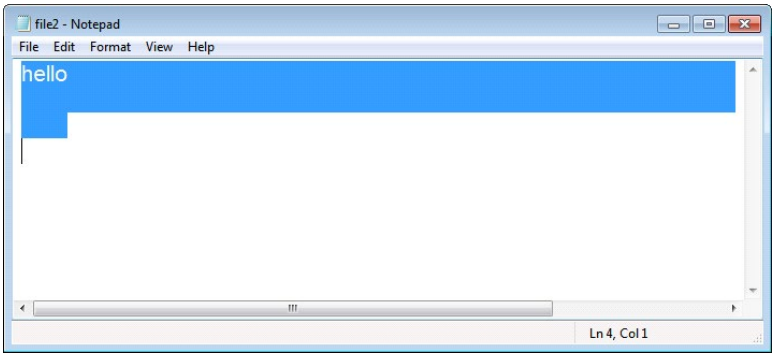

The hidden file will be extracted from the carrier file and outputted to the destination directory

8) Snow

1. Create a file named file1.txt (with data)
2. snow -C -m "Hello World" -p "magic" file1.txt file2.txt
3. Above command will use SNOW to hide the message "Hello World" inside file1.txt white spaces and output it to a new file file2.txt. The password used is magic
4. snow -C -p "magic" file2.txt
5. Above command will then use SNOW to extract the hidden message in file2.txt using the password magic

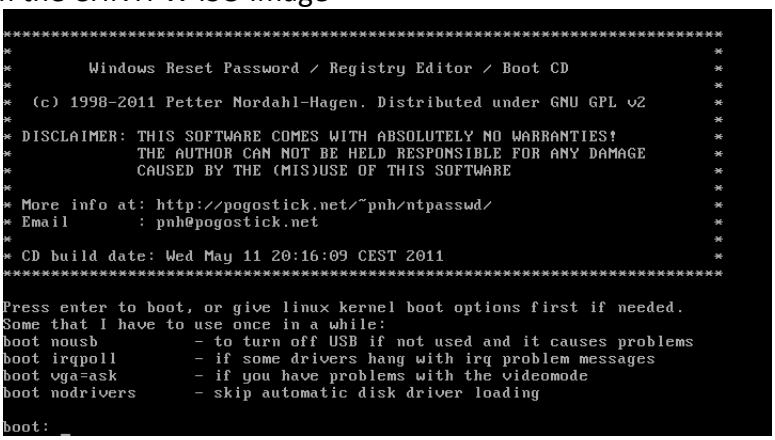



6. Because data is hidden in white spaces in the file2.txt file, doing a Ctrl+A will select spaces and text together

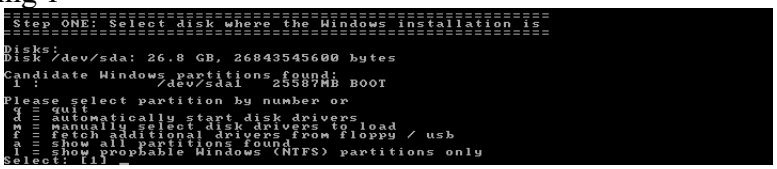



9) CHNTPW.ISO

1. Boot from the CHNTPW ISO Image

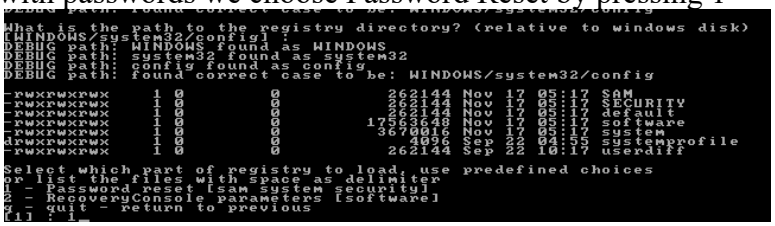


2. Press Enter to boot
3. In STEP ONE, select the Windows Partition by using the numeric keys. Here we are pressing 1

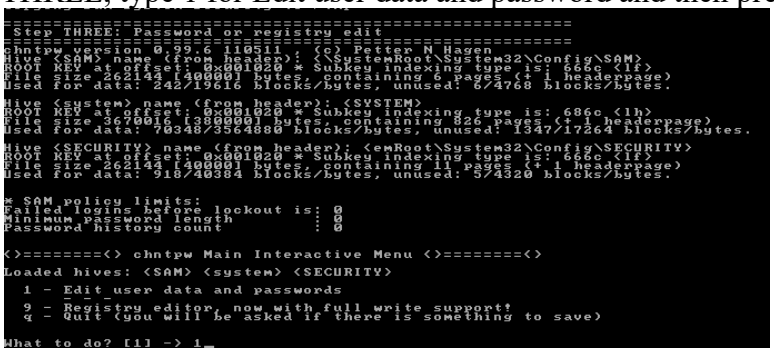



4. In STEP TWO we are letting the system automatically detect the windows folders. Press Enter

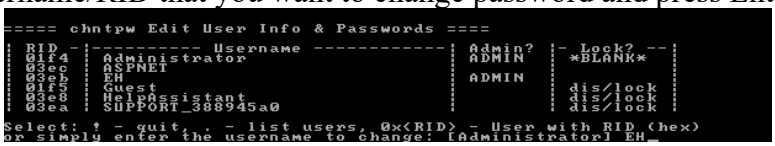

5. In the next part, we need to select the part of the registry to load. Since we are working with passwords we choose Password Reset by pressing 1



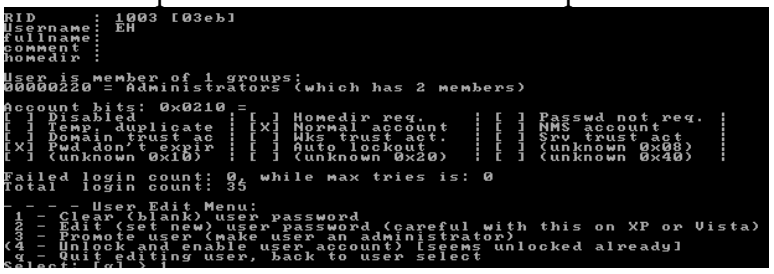

6. In STEP THREE, type 1 for Edit user data and password and then press Enter.



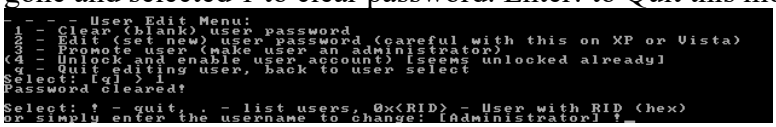

7. Type Username/RID that you want to change password and press Enter



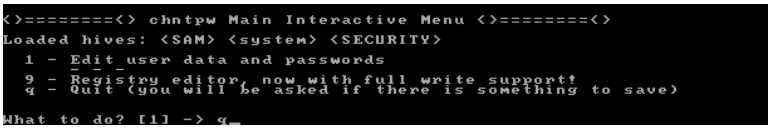

8. Enter 1 to Clear user password or 2 to set a new user password



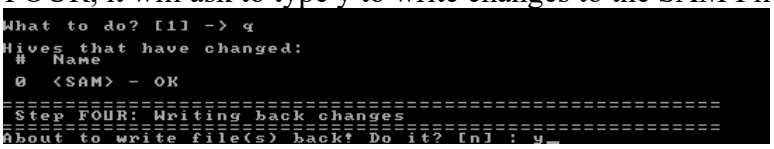

9. We have gone and selected 1 to clear password. Enter! to Quit this mode




10. type q to Quit the edit mode




11. At STEP FOUR, it will ask to type y to write changes to the SAM File.

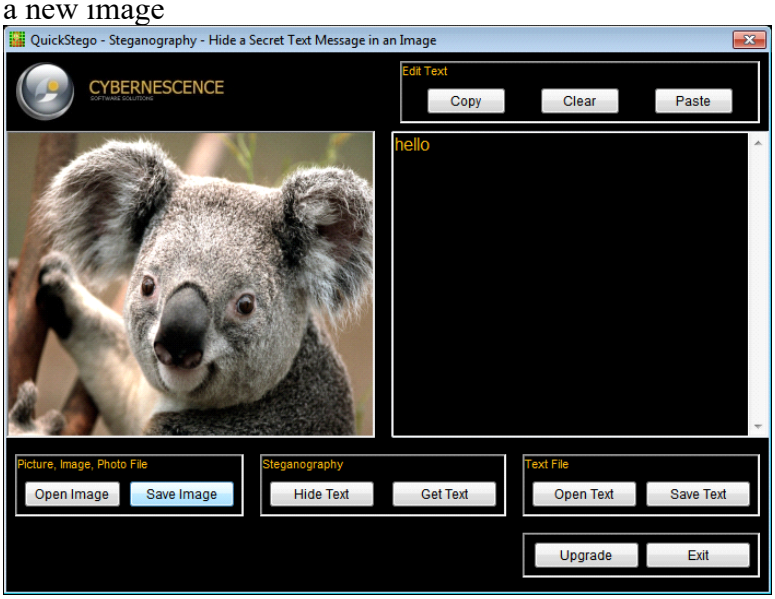



12. Type y to perform it again or n to exit


13. Reboot the machine and then load windows directly. You will see that it is not asking for password now.

10) Quick Stego

1. Used to perform image based Steganography
2. To Hide Text inside the image
3. Type the text in the textbox and then click on Open Image to browse and select the image to store the text inside of. The image opens in the left image box. To hide text, click on the Hide Text button and do a Save Image to save the stego image as a new image

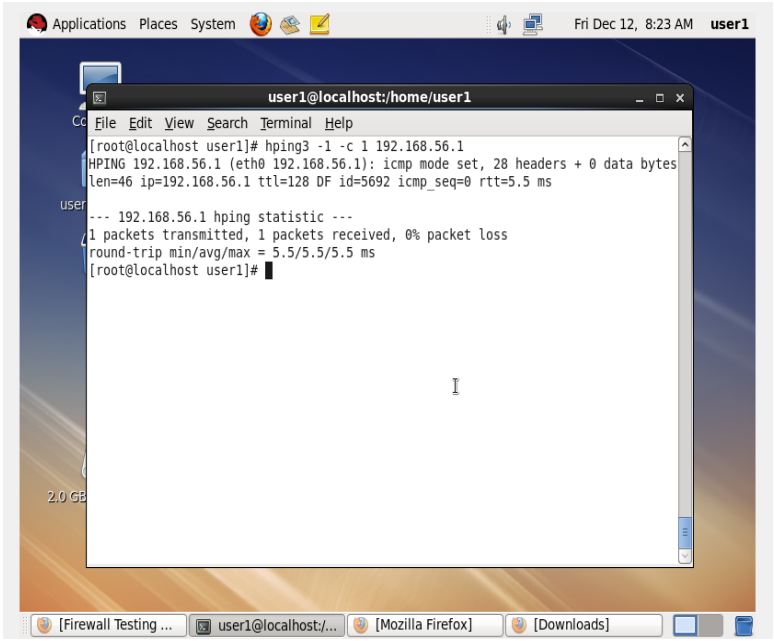



4. To see the text hidden inside of an image
5. Open the image using **Open Image** and Quick Stego will directly show the hidden text from inside the image

# PRACTICAL 5

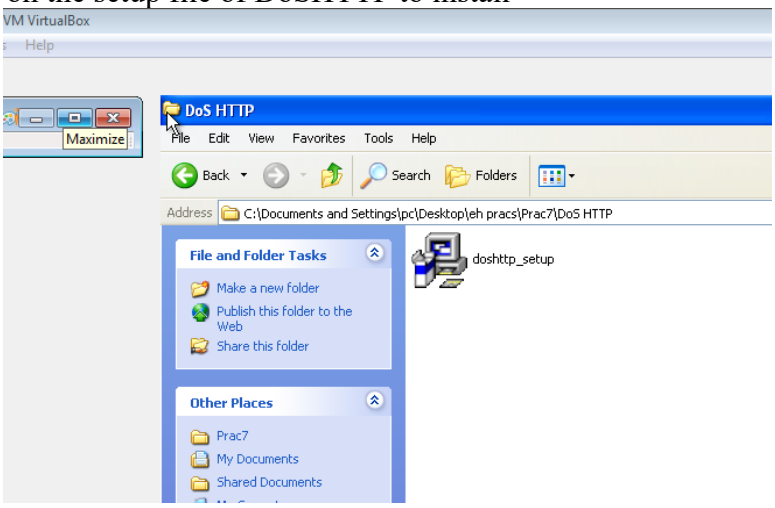
## A. Study of Denial of Service attack tools.

1) hping3

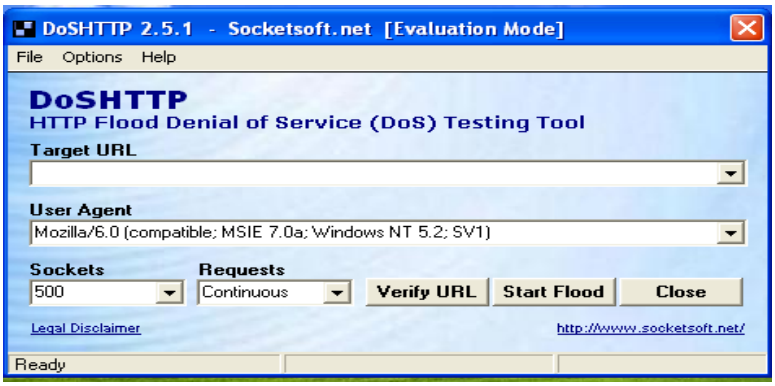



2) DoSHTTP

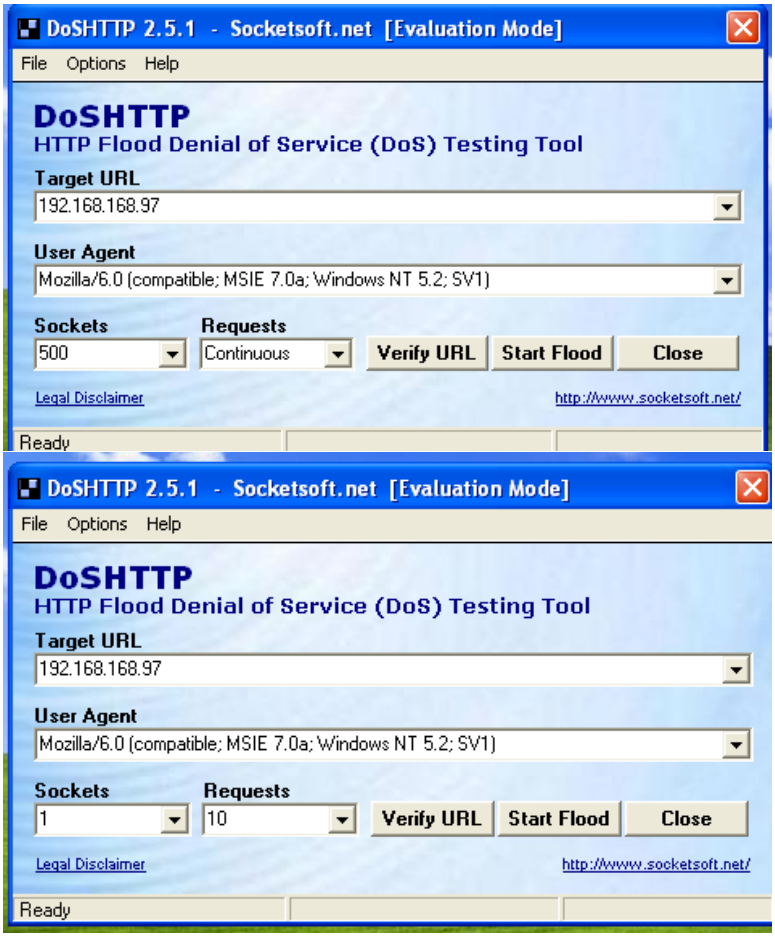
Double click on the setup file of DoSHTTP to install




this shows the interface of the DoSHTTP




Enter IP Address or the target url, user agent using for flood and sockets and the request type and click on "Start Flood"


DoSHTTP 2.5.1 - Socketsoft.net [Evaluation Mode]
File Options Help
DoSHTTP
HTTP Flood Denial of Service (DoS) Testing Tool
Target URL
192.168.168.97
User Agent
Mozilla/6.0 (compatible; MSIE 7.0a; Windows NT 5.2; SV1)
Sockets
500
Requests
Continuous
Verify URL
Start Flood
Close
Legal Disclaimer
http://www.socketsoft.net/
Ready
DoSHTTP 2.5.1 - Socketsoft.net [Evaluation Mode]
File Options Help
DoSHTTP
HTTP Flood Denial of Service (DoS) Testing Tool
Target URL
192.168.168.97
User Agent
Mozilla/6.0 (compatible; MSIE 7.0a; Windows NT 5.2; SV1)
Sockets
1
Requests
10
Verify URL
Start Flood
Close
Legal Disclaimer
http://www.socketsoft.net/
Ready

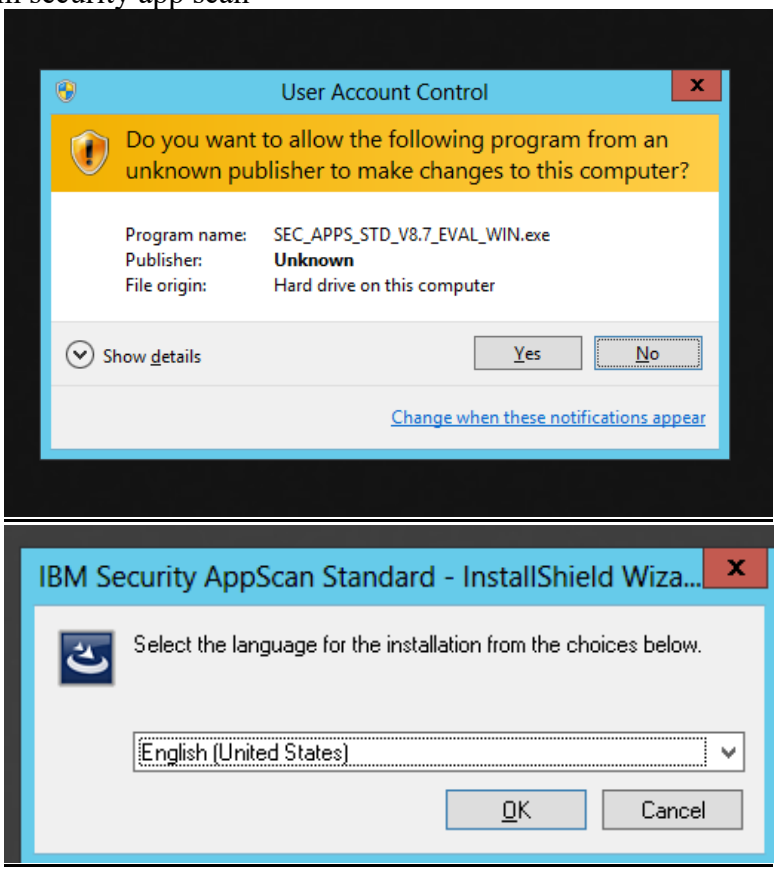
# PRACTICAL 6

## A. Study of Web server Attack tools

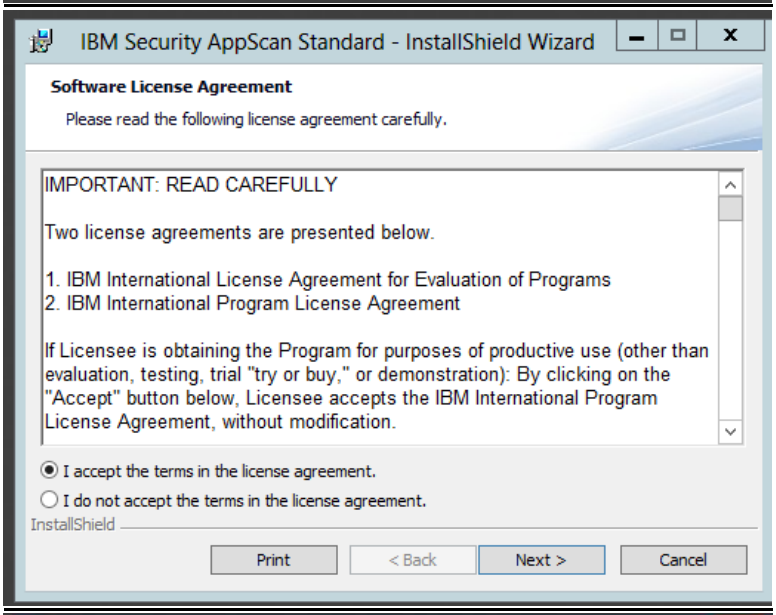
1) IBM Security AppScan

Solution:

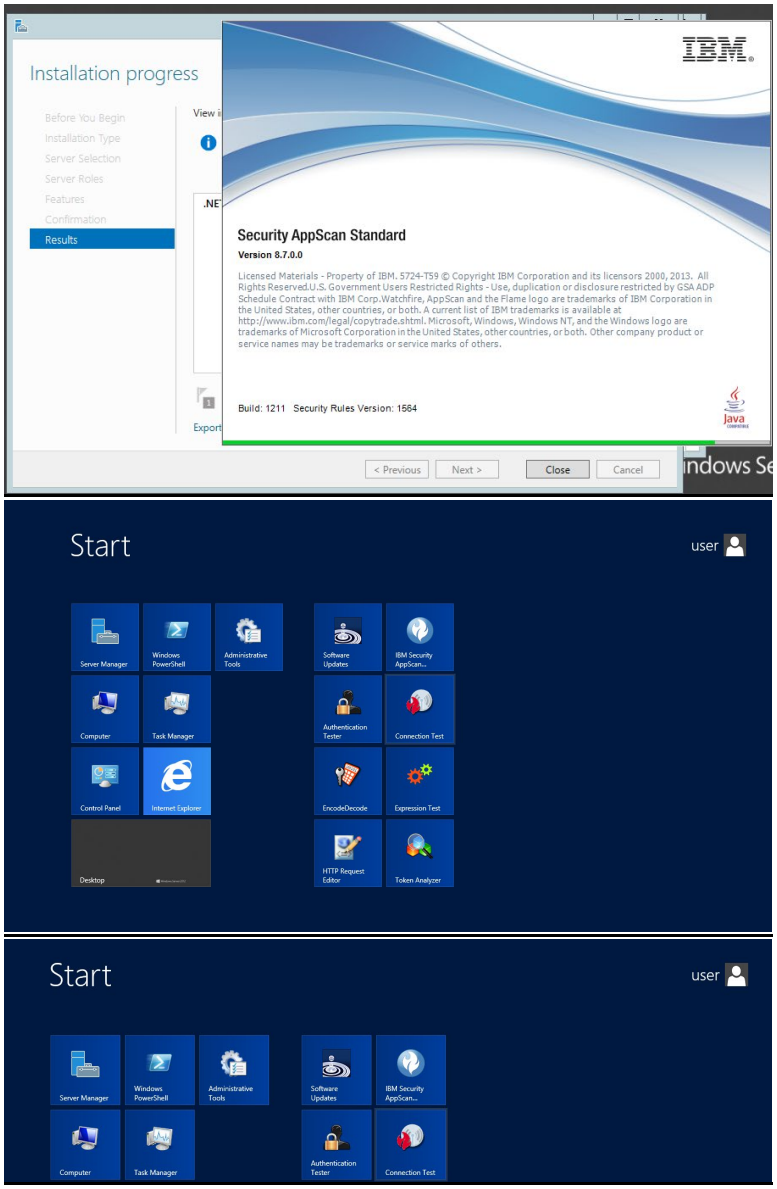
1. Install ibm security app scan




IBM Security AppScan Standard - InstallShield Wizard
Preparing to Install...
IBM Security AppScan Standard Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
Extracting: IBM Security AppScan Standard.msi
Cancel


IBM Security AppScan Standard - InstallShield Wizard
Software License Agreement
Please read the following license agreement carefully.
IMPORTANT: READ CAREFULLY
Two license agreements are presented below.
1. IBM International License Agreement for Evaluation of Programs
2. IBM International Program License Agreement
If Licensee is obtaining the Program for purposes of productive use (other than evaluation, testing, trial "try or buy," or demonstration): By clicking on the "Accept" button below, Licensee accepts the IBM International Program License Agreement, without modification.
I accept the terms in the license agreement.
I do not accept the terms in the license agreement.
InstallShield
Print
< Back
Next >
Cancel


IBM Security AppScan Standard - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install IBM Security AppScan Standard to:
C:\Program Files (x86)\IBM\AppScan Standard\
Change...
InstallShield
< Back
Install
Cancel

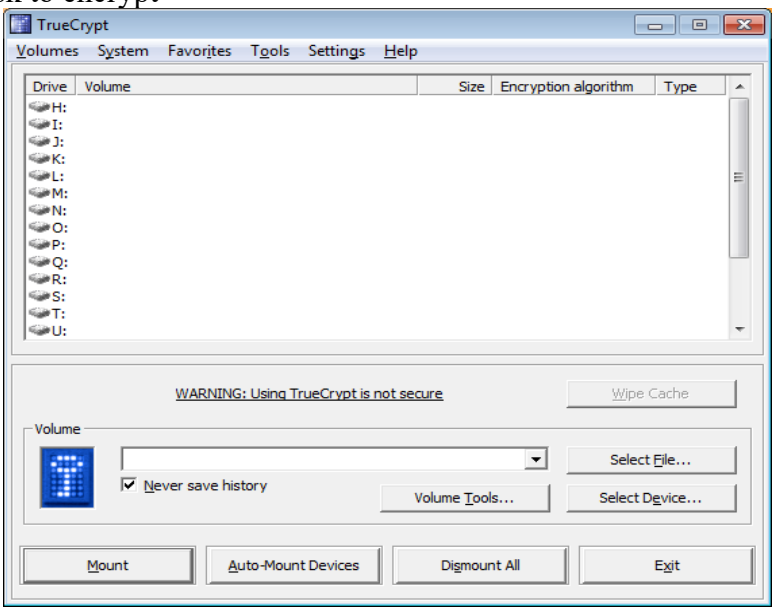

Installation progress
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
IBM
Security AppScan Standard
Version 8.7.0.0
Licensed Materials - Property of IBM. 5724-T59 © Copyright IBM Corporation and its licensors 2000, 2013. All Rights Reserved.U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.Watchfire, AppScan and the Flame logo are trademarks of IBM Corporation in the United States, other countries, or both. A current list of IBM trademarks is available at http://www.ibm.com/legal/copytrade.shtml. Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. Other company product or service names may be trademarks or service marks of others.
Build: 1211 Security Rules Version: 1564
Java
< Previous
Next >
Close
Cancel
Start
user
Server Manager
Windows PowerShell
Administrative Tools
Software Updates
IBM Security AppScan...
Computer
Task Manager
Authentication Tester
Connection Test
Control Panel
Internet Explorer
EncodeDecode
Expression Test
Desktop
HTTP Request Editor
Token Analyzer
Start
user
Server Manager
Windows PowerShell
Administrative Tools
Software Updates
IBM Security AppScan...
Computer
Task Manager
Authentication Tester
Connection Test

# PRACTICAL 7

## A. Using Cryptanalysis Tools

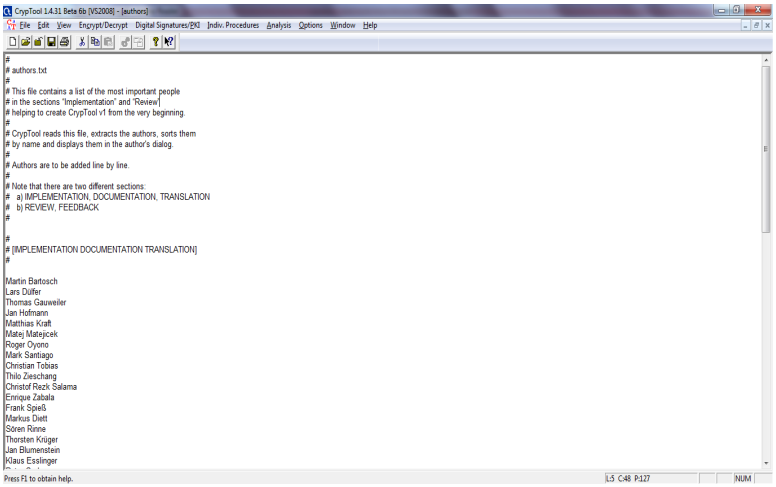
1) TrueCrypt

1. Open the TrueCrypt software
2. Select disk to encrypt

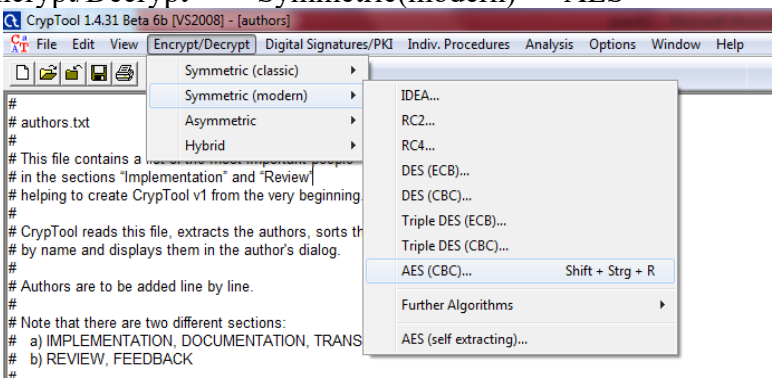



2) Cryptool

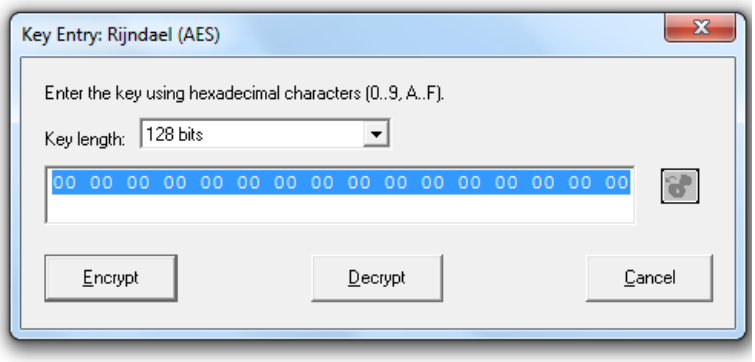
1. Open the software

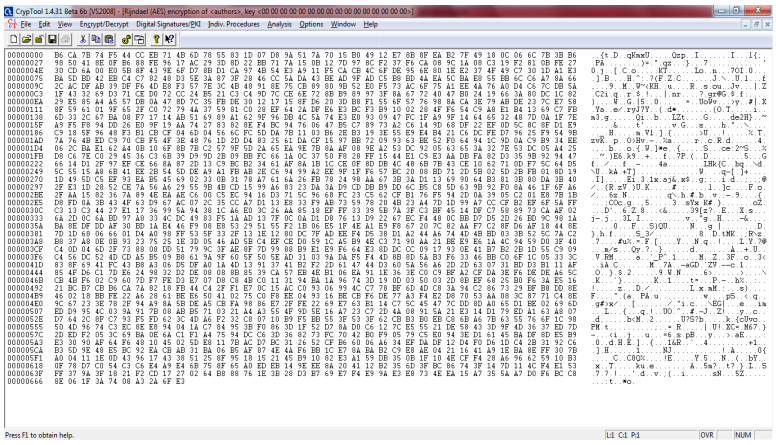


2. Go to "Encrypt/Decrypt" --> Symmetric(modern) -->AES

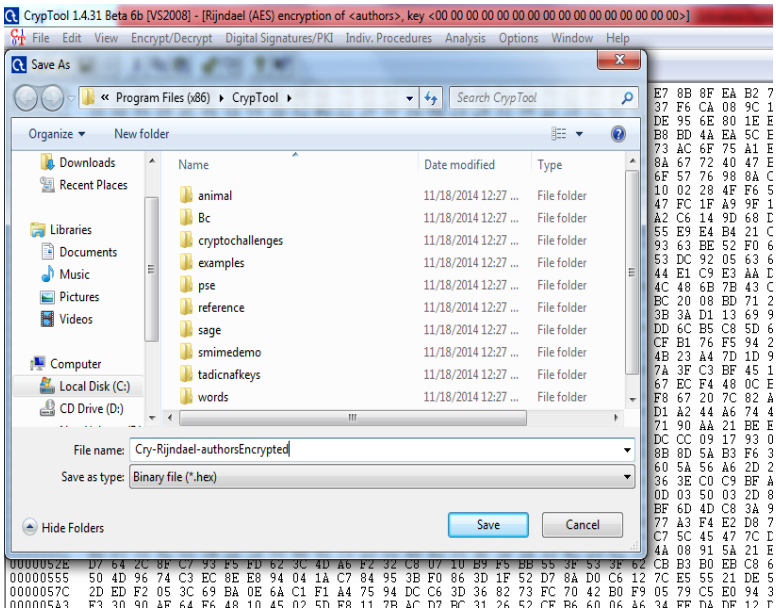


3. Click on "Encrypt"



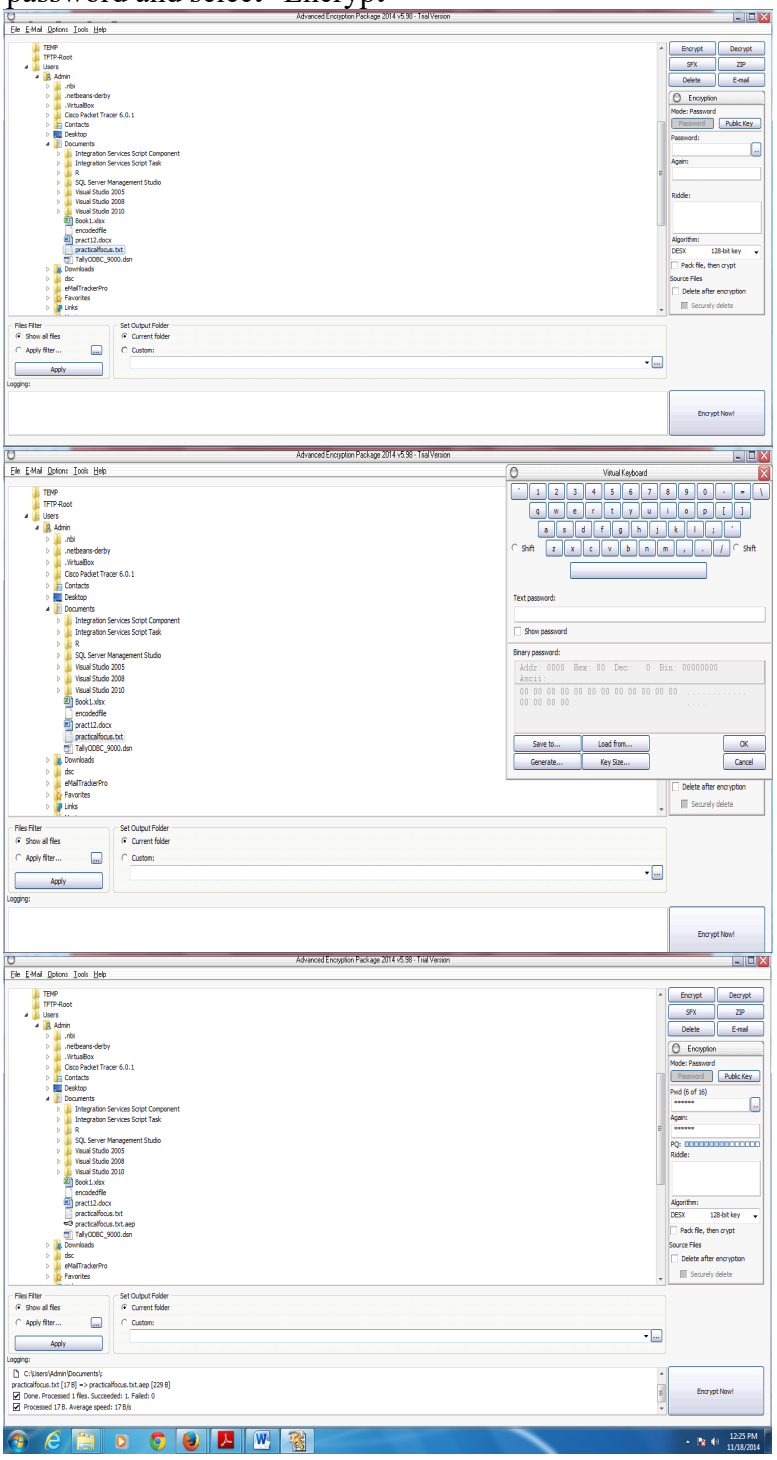



4. Save the file in a location



3) Advanced Encryption Package

1. Open the software
2. Browse any file to decrypt e.g. "abc.txt"
3. Enter the password and select "Encrypt"

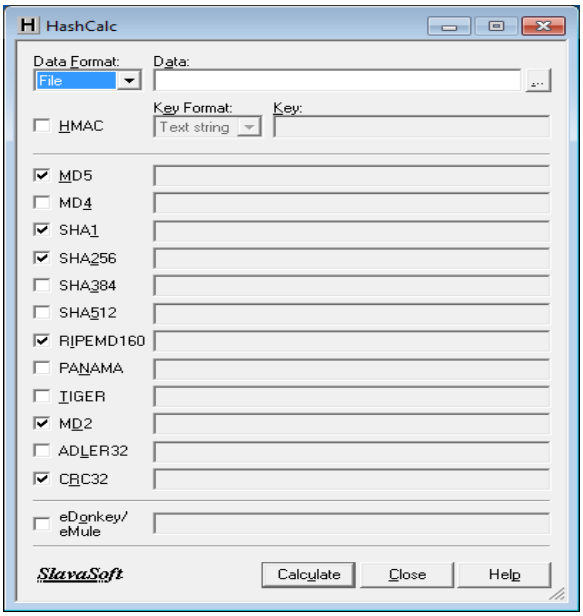


# PRACTICAL 8

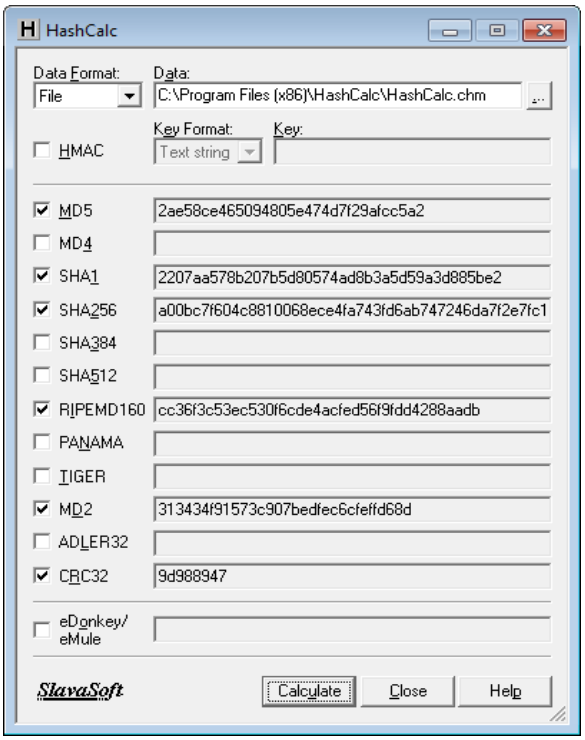
## A. Using HashCalc Tools

1) HashCalc

1. Open HashCalc software




2. Browse the "HashCalc.chm" file

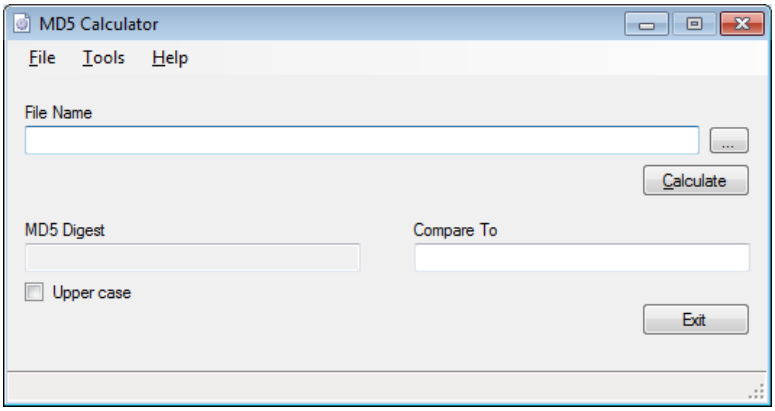


# PRACTICAL 9

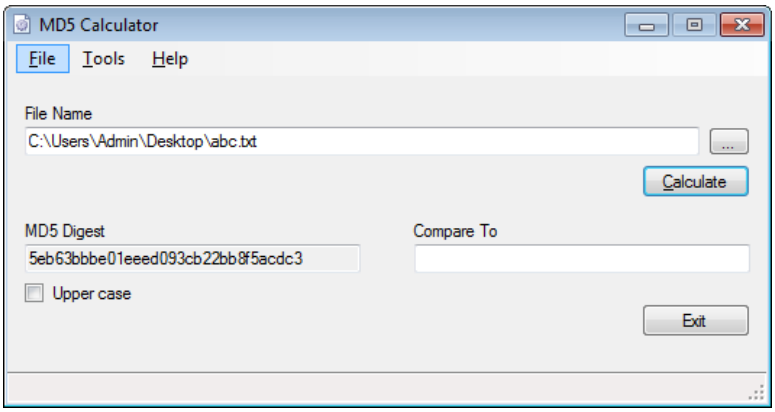
## A. Using MD5 Calculator Tools

1) MD5 Calculator

1. Open MD5 Calculator




2. Select "File"
3. Browse any file to decrypt e.g. "abc.txt"
4. Select Calculate

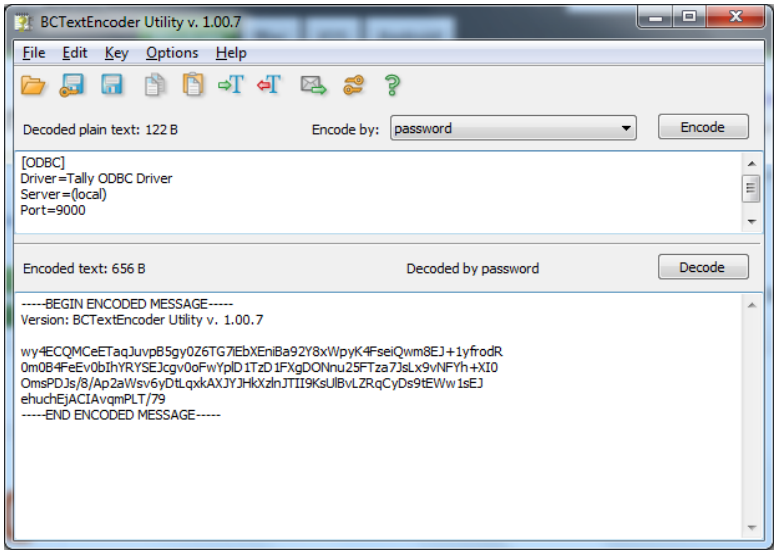


# PRACTICAL 10

## A. Using BCTextEncoder Tools

1) BCTextEncoder

1. Open the file --> Encode

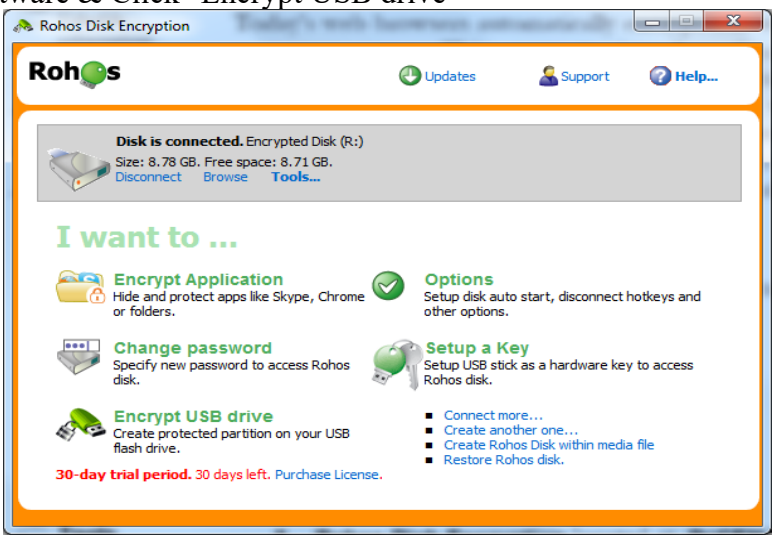


# PRACTICAL 11

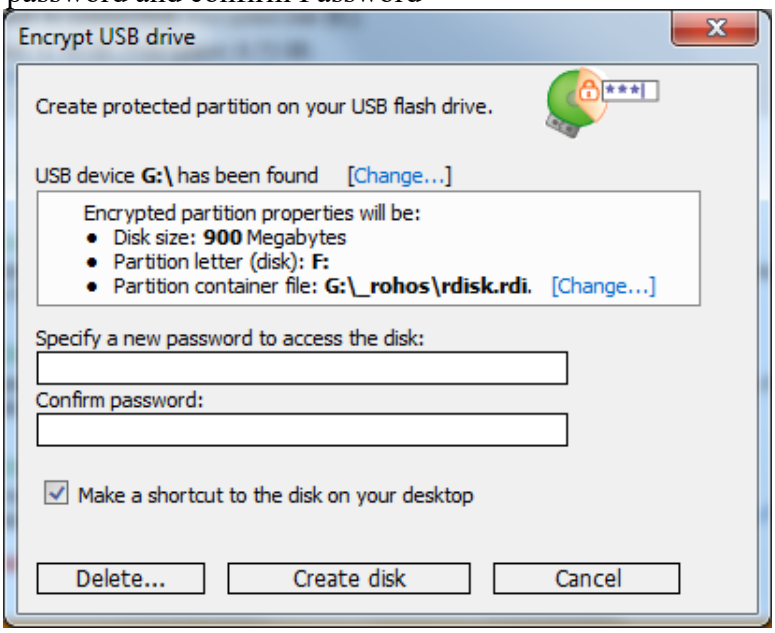
## A. Using Rohos Disk Encryption Tools

1) Rohos Disk Encryption

1. Open software & Click "Encrypt USB drive"

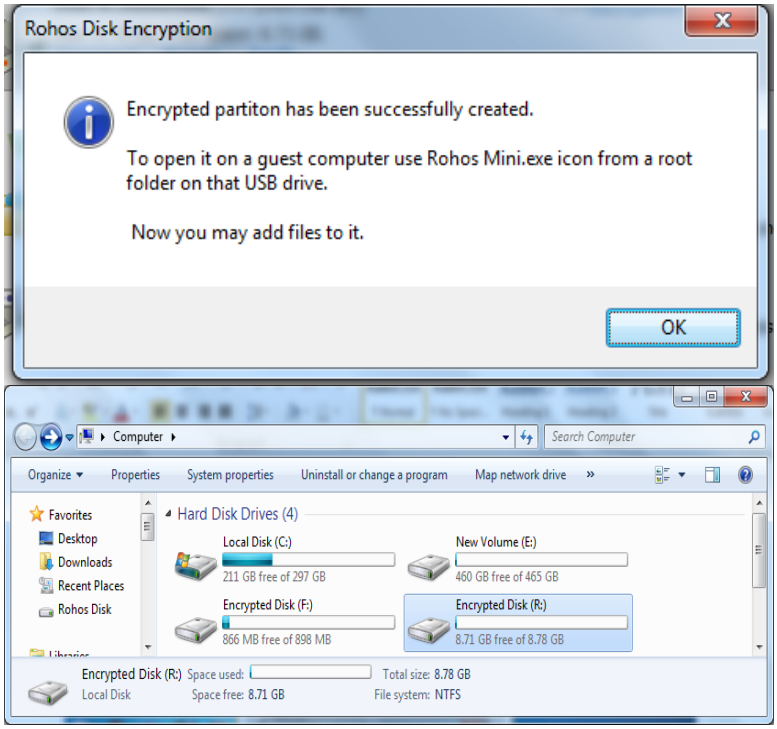



2. Enter the password and confirm Password




3. Create Disk

4. Click "OK"


Rohos Disk Encryption
Encrypted partiton has been successfully created.
To open it on a guest computer use Rohos Mini.exe icon from a root folder on that USB drive.
Now you may add files to it.
OK
Computer
Search Computer
Organize
Properties
System properties
Uninstall or change a program
Map network drive
Favorites
Desktop
Downloads
Recent Places
Rohos Disk
Hard Disk Drives (4)
Local Disk (C:)
211 GB free of 297 GB
New Volume (E:)
460 GB free of 465 GB
Encrypted Disk (F:)
866 MB free of 898 MB
Encrypted Disk (R:)
8.71 GB free of 8.78 GB
Encrypted Disk (R:) Space used:
Total size: 8.78 GB
Local Disk
Space free: 8.71 GB
File system: NTFS

# PRACTICAL 12

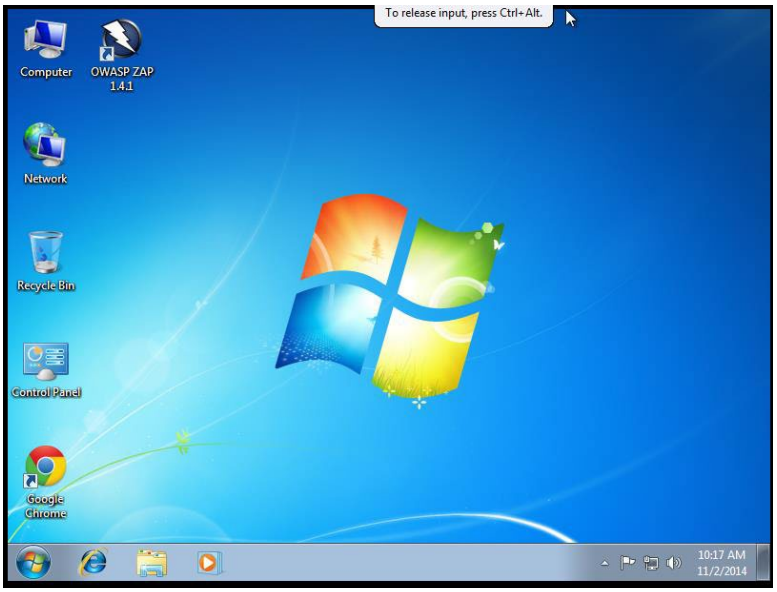
## A. Study of Session Hijacking tools

1) ZAP

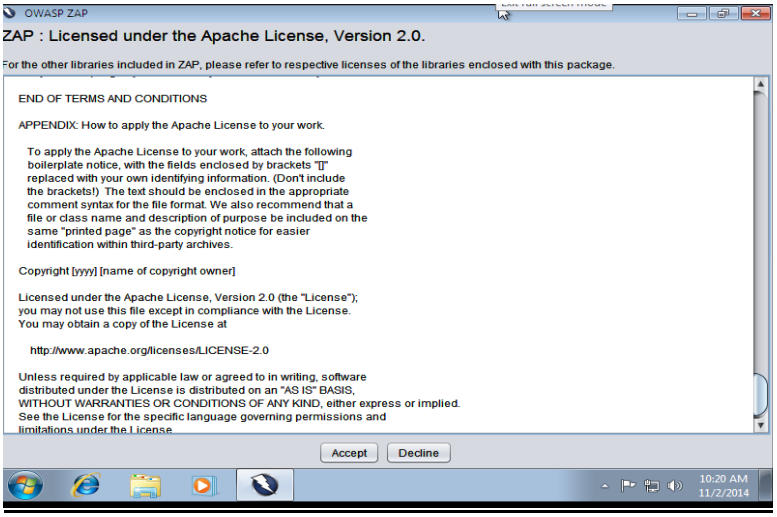
Solution:

Lab Task:

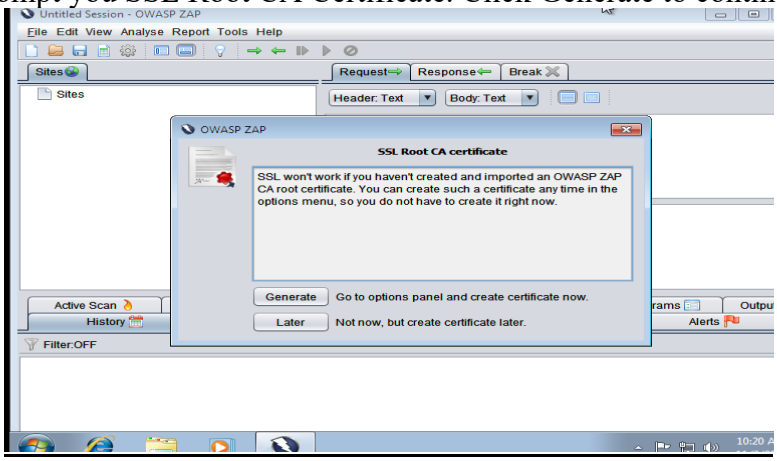
1. Launch windows 8 or windows 7 in virtual machine.



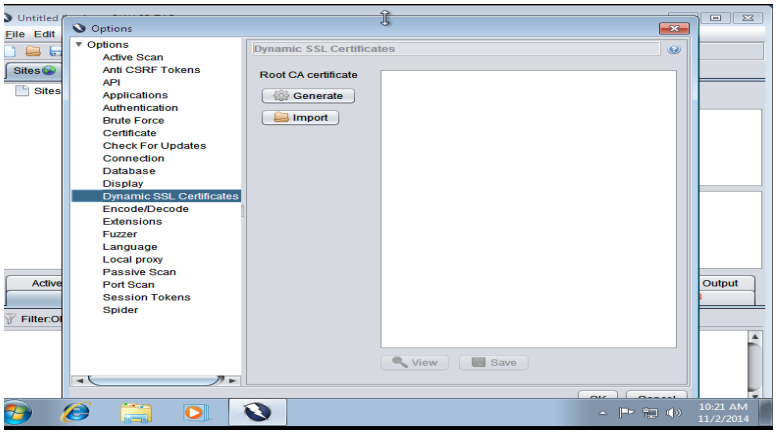

2. Install ZAP Tool. And Launch it.
3. Accept license.



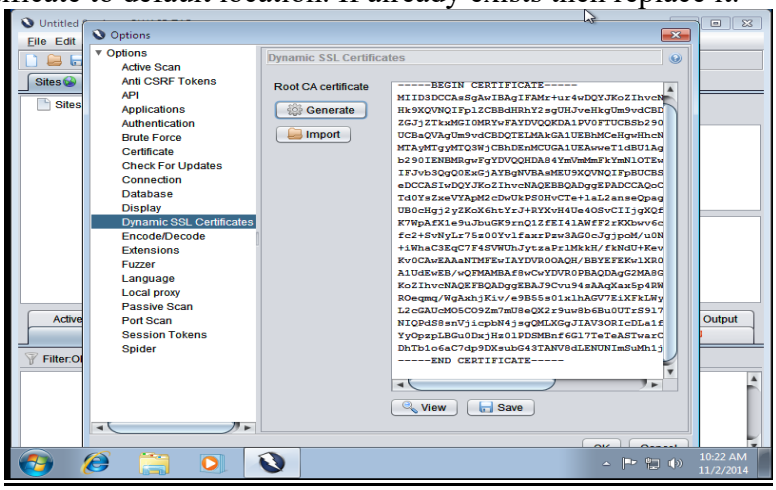
4. It will prompt you SSL Root CA Certificate. Click Generate to continue.

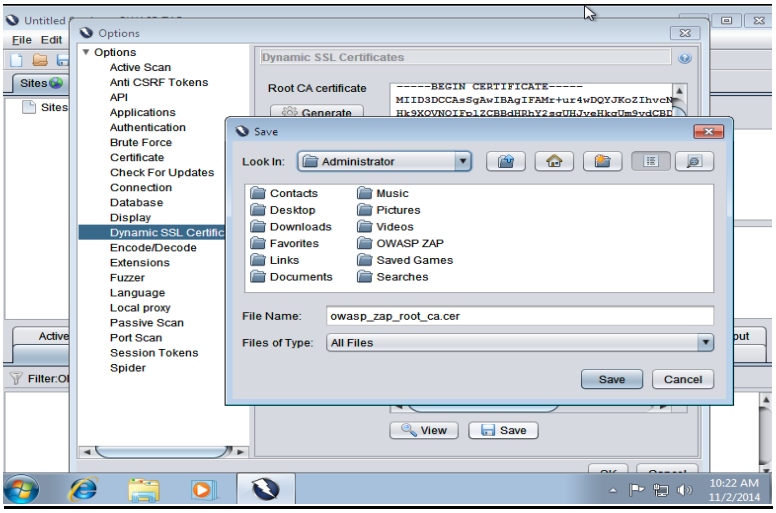



5. In the options window, select Dynamic SSL Certificates and click Generate to generate certificate. Then Save it.

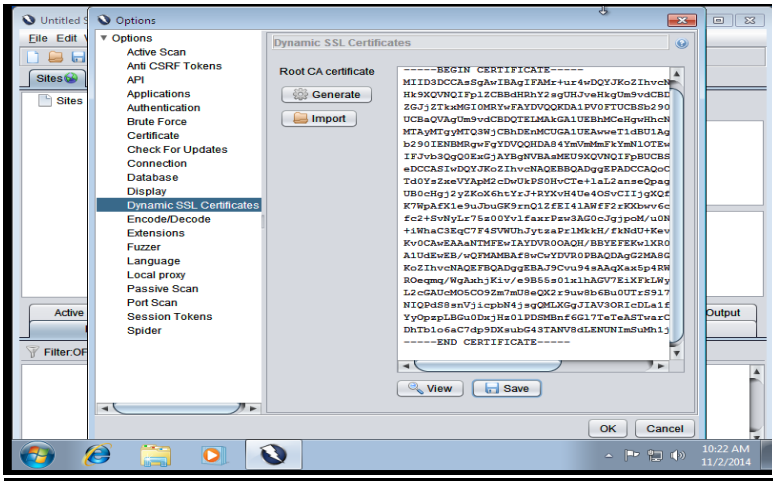



6. Save certificate to default location. If already exists then replace it.

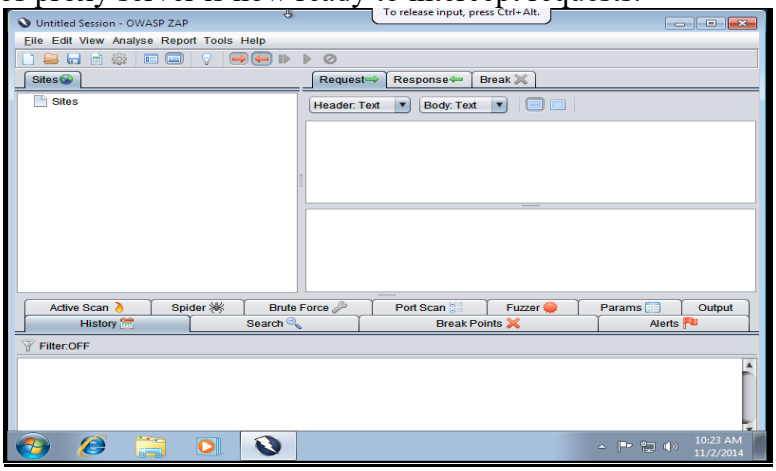




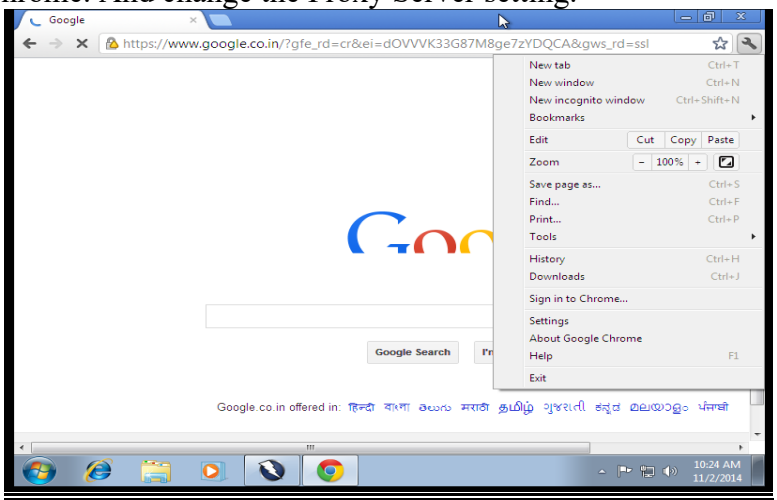

7. Click OK.

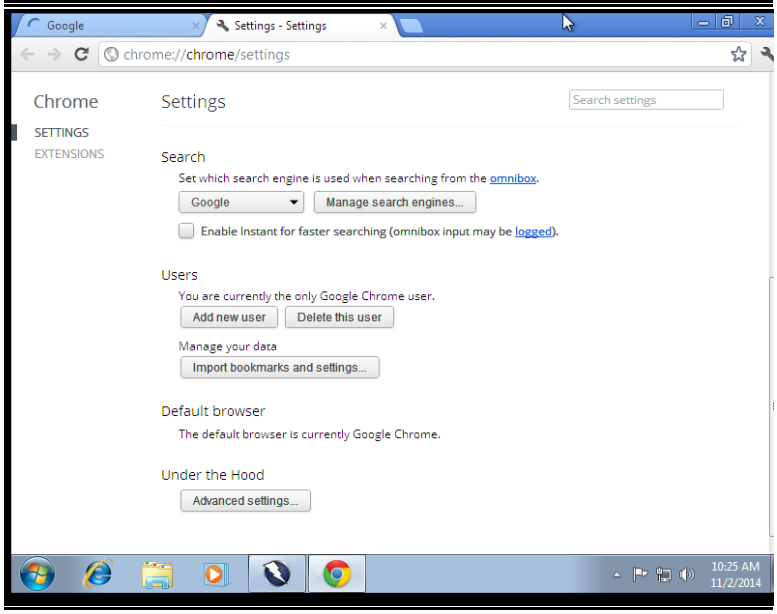


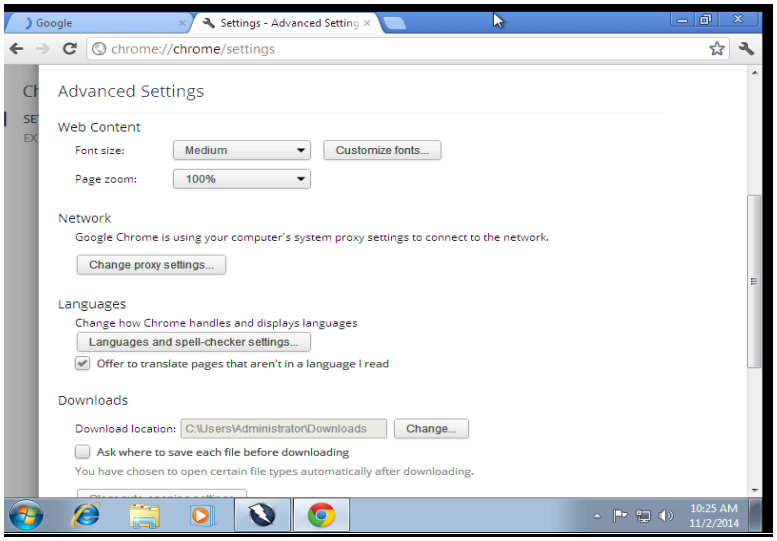

8. Your Paros proxy server is now ready to intercept requests.

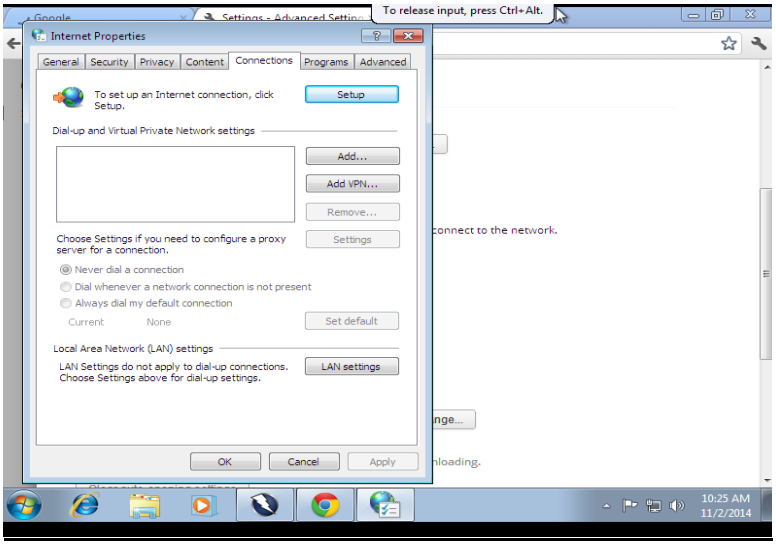


9. Launch chrome. And change the Proxy Server setting.

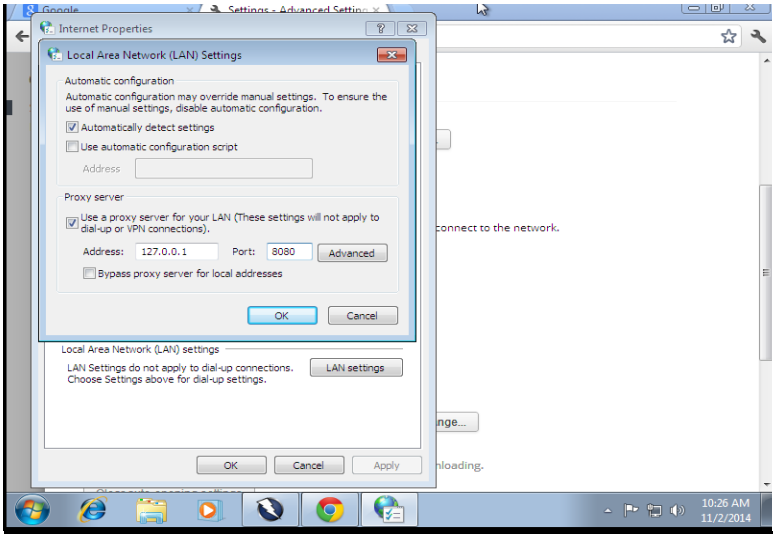


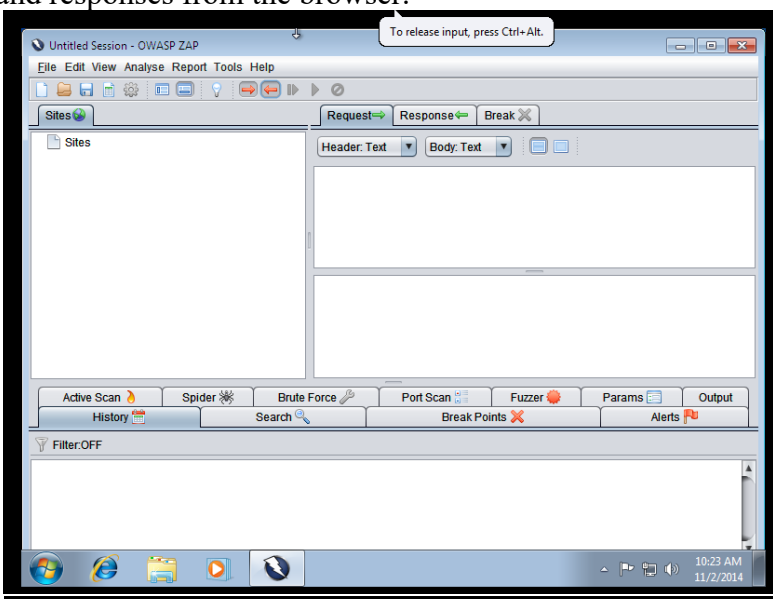





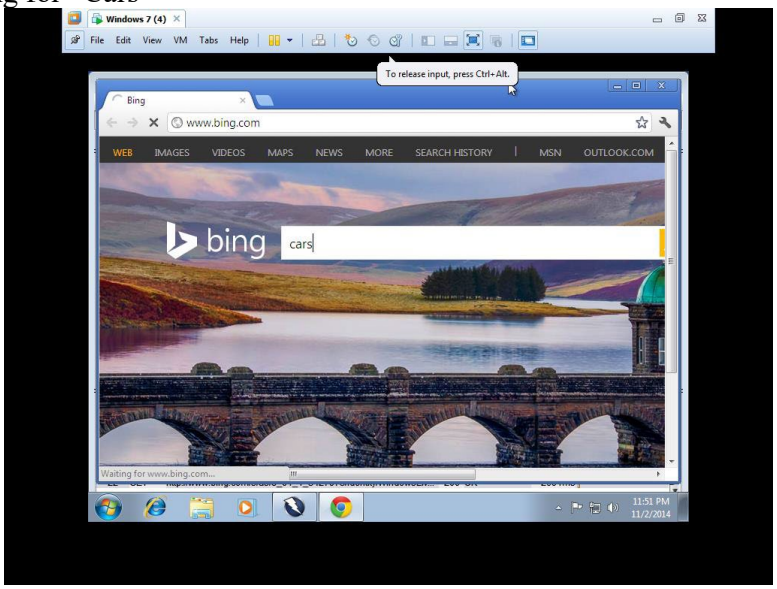

10. Check Use proxy server for your LAN. And type 127.0.0.1 as address and 8080 as a port number.



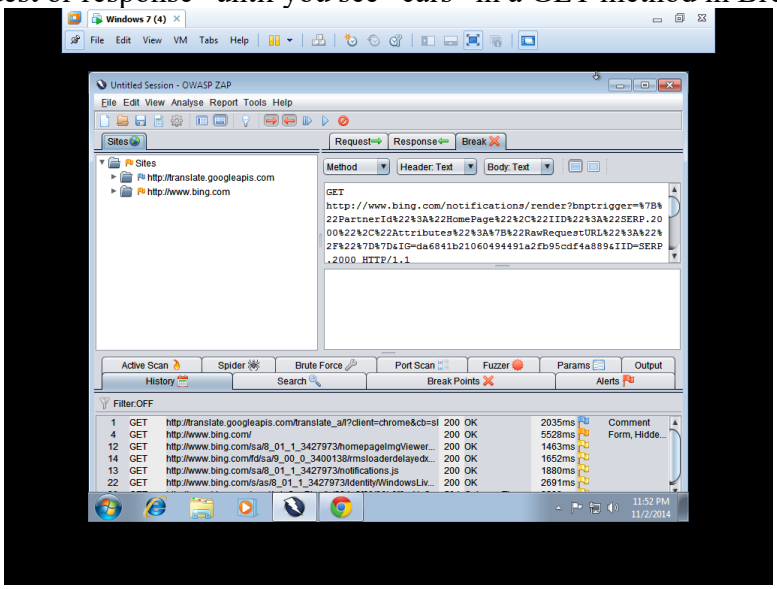

11. Click “Set break on all requests” and “Set break on all responses” to trap all requests and responses from the browser.

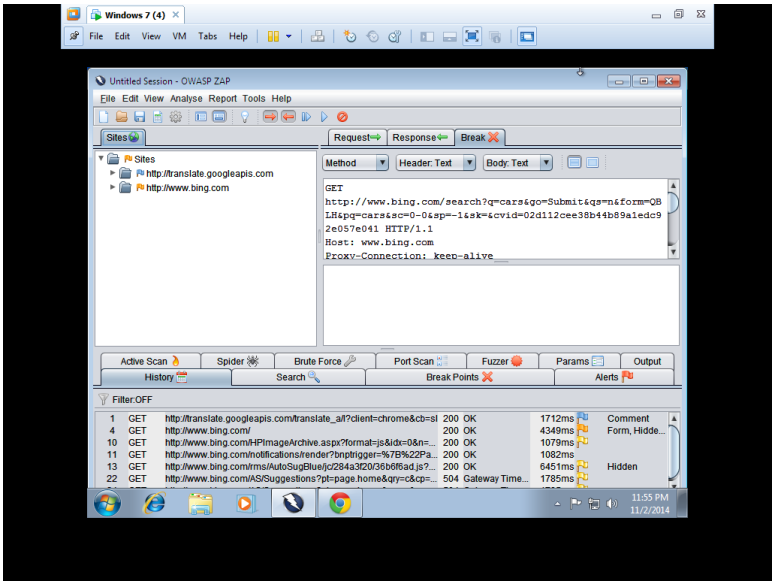


12. Now navigate to chrome browser and open www.bing.com
Start searching for “Cars”

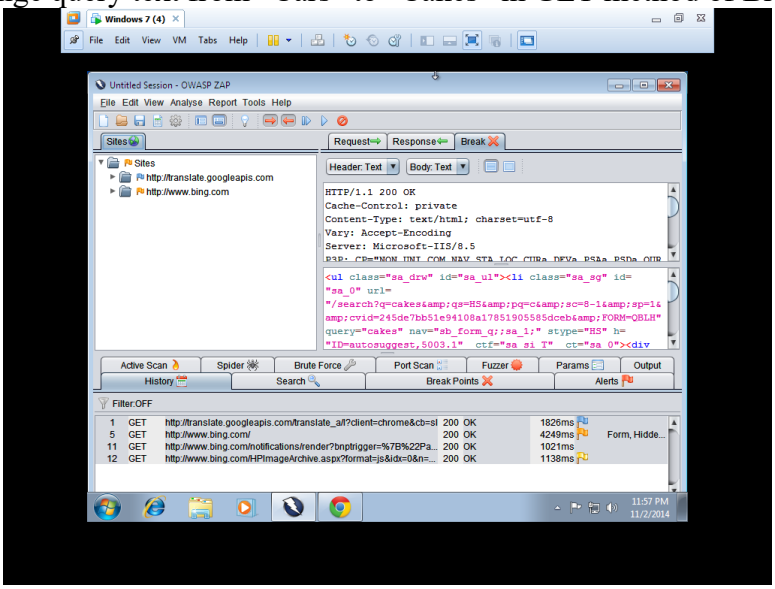



13. Open ZAP and observe trapped traffic.
14. Observe first few lines of trapped traffic and keep clicking “Submit” and step to next request or response” until you see “cars” in a GET method in Break tab.

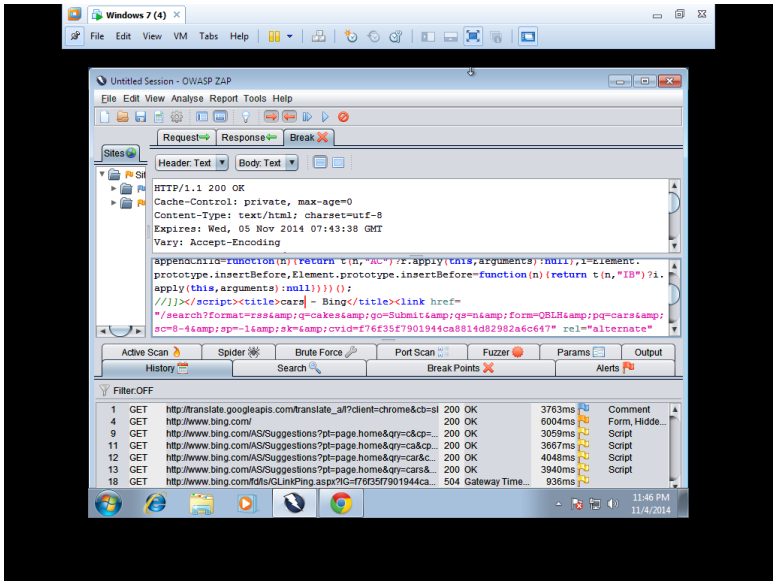


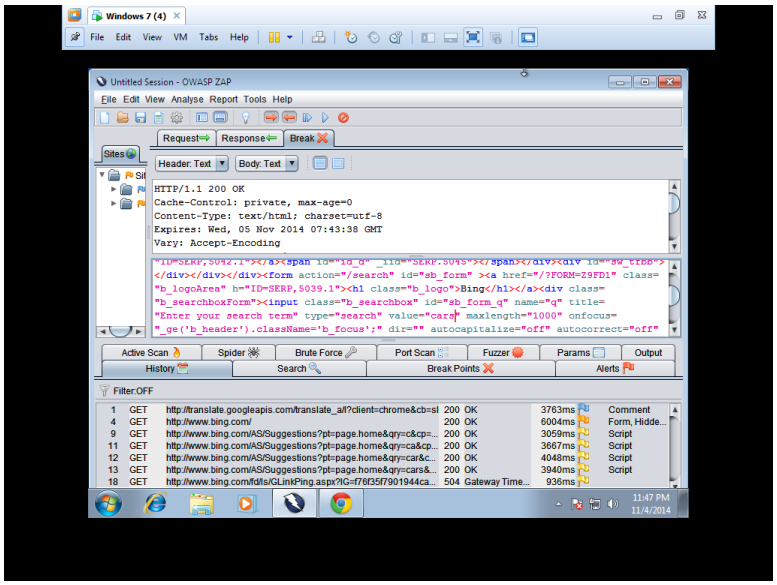


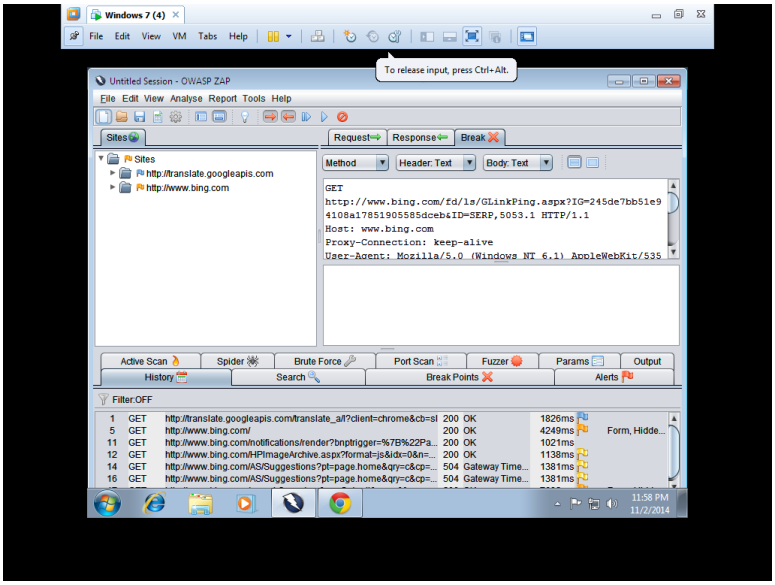

15. Now change query text from “Cars” to “Cakes” in GET method of Break tab.



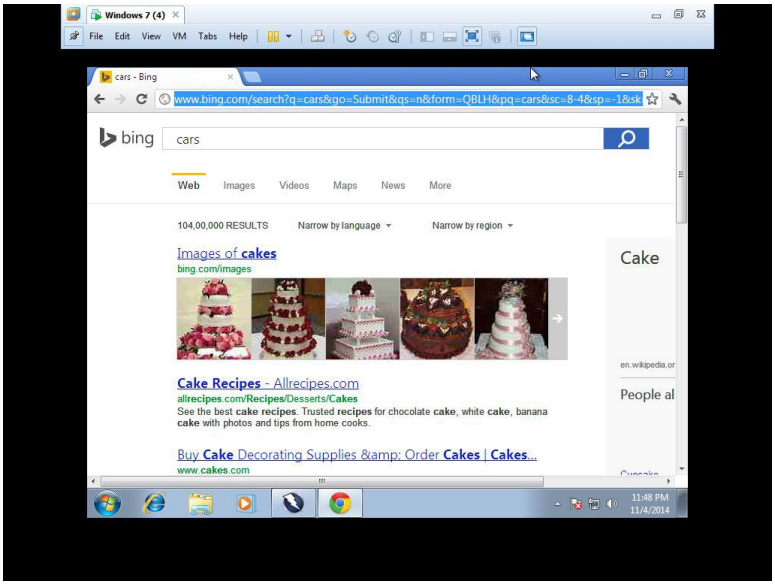
16. In the same response pane, replace “cakes” with “cars” as shown in following screenshots. And continue clicking “Submit and step to next request or response”.






17. Now open the browser. Observe URL and the result.



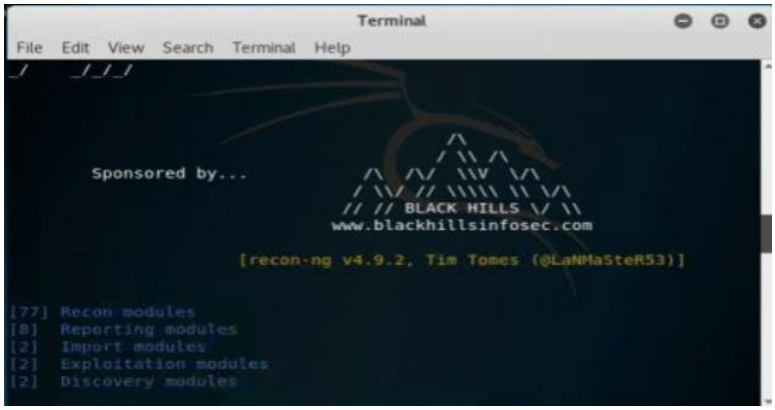
# PRACTICAL 13

**A. Use the following tools to perform footprinting and reconnaissance**

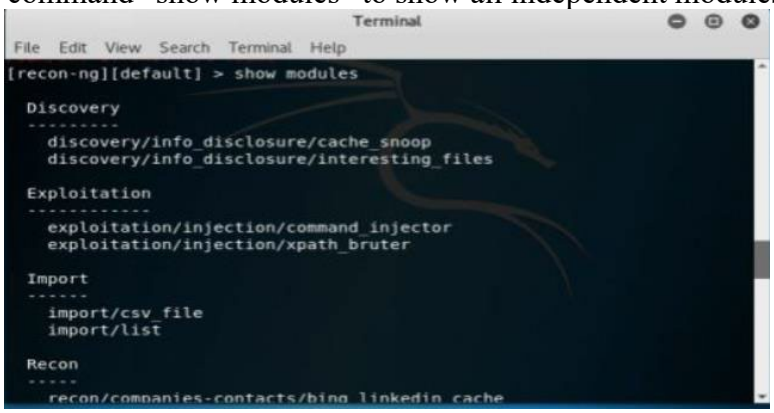
1) Recon-ng (Using Kali Linux)

Recong0-ng is a full feature Web Reconnaissance framework used for information gathering purpose as well as network detection. This tool is written in python, having independent modules, database interaction and other features. You can download the software from www.bitbucket.org. This Open Source Web Reconnaissance tool requires kali Linux Operating system.

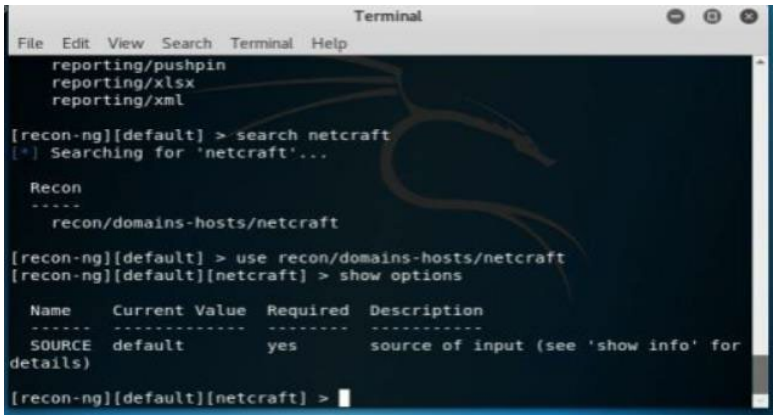
1. Run the Application Recon-ng or open the terminal of Kali-Linux and type recon-ng and hit enter.



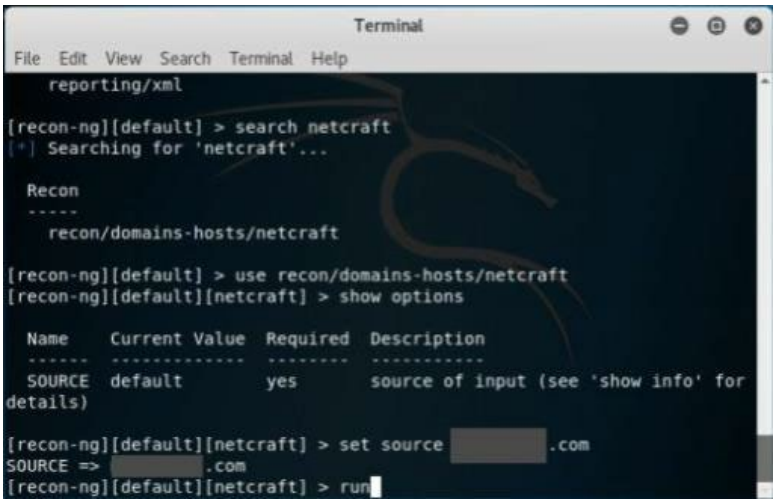

2. Enter the command “show modules” to show all independent modules available.



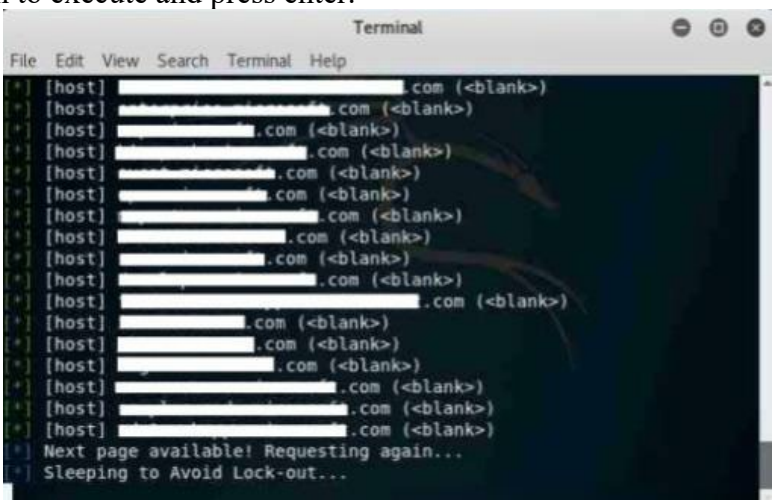

3. You can search for any entity within a module. For example, in above figure, the command “Search Netcraft” is used.



4. To use the Netcraft module, use the command syntax “use recon/domain-hosts/Netcraft” and hit enter.




5. Set the source by the command “set source [domain].” Press enter to continue. Type Run to execute and press enter.



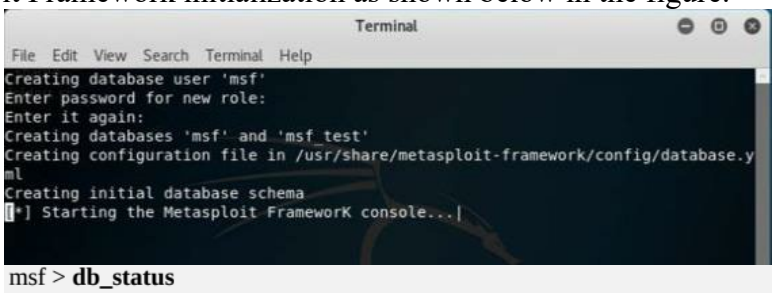

2) Metasploit (for information gathering)

In this lab, we are using Metasploit Framework, default application in Kali Linux for gathering more information about the host in a network. A Metasploit Framework is a powerful tool, popularly used for scanning & gathering information in the hacking environment. Metasploit Pro enables you to automate the process of discovery and exploitation and provides you with the necessary tools to perform the manual testing phase of a penetration test. You can use Metasploit Pro to scan for open ports and services, exploit vulnerabilities, pivot further into a network, collect evidence, and create a report of the test results.

Topology Information: In this lab, we are running Metasploit Framework on a private network 10.10.50.0/24 where different hosts are live including Windows 7, Kali Linux, Windows Server 2016 and others.

1. Open Kali Linux and Run Metasploit Framework.


2. Metasploit Framework initialization as shown below in the figure.




msf > **db_status**
[*] postgresql connected to msf

// If your database is not connected, it means your database is not initiated. You will need to exit msfconsole & restart the postgresql service.

// Performing nmap Scan for ping sweep on the subnet 10.10.50.0/24

msf > **nmap -Pn -sS -A -oX Test 10.10.50.0/24**
[*] exec: nmap -Pn -sS -A -oX Test 10.10.50.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-26 01:49 EDT
Stats: 0:04:31 elapsed; 247 hosts completed (8 up), 8 undergoing Script Scan
NSE Timing: About 99.77% done; ETC: 01:53 (0:00:00 remaining)
Stats: 0:05:04 elapsed; 247 hosts completed (8 up), 8 undergoing Script Scan
NSE Timing: About 99.79% done; ETC: 01:54 (0:00:00 remaining)
Stats: 0:06:21 elapsed; 247 hosts completed (8 up), 8 undergoing Script Scan
NSE Timing: About 99.93% done; ETC: 01:55 (0:00:00 remaining)
Nmap scan report for 10.10.50.1
Host is up (0.0012s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION

```
22/tcp   open  ssh       Cisco SSH 1.25 (protocol 1.5)
| ssh-hostkey:
|_  512 ca:9c:c7:d2:d4:b0:78:82:3e:34:8f:cf:00:9d:75:db (RSA1)
|_sshv1: Server supports SSHv1
23/tcp   open  telnet    Cisco router telnetd
5060/tcp open  sip-proxy  Cisco SIP Gateway (IOS 15.2.4.M4)
|_sip-methods: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER,
SUBSCRIBE, NOTIFY, INFO, REGISTER
5061/tcp open  tcpwrapped
MAC Address: C0:67:AF:C7:D9:80 (Cisco Systems)
OS details: Cisco 836, 890, 1751, 1841, 2800, or 2900 router (IOS 12.4 - 15.1), Cisco Aironet 1141N
(IOS 12.4) or 3602I (IOS 15.3) WAP, Cisco Aironet 2600-series WAP (IOS 15.2(2))
Network Distance: 1 hop
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT     ADDRESS
1   1.15 ms 10.10.50.1

Nmap scan report for 10.10.50.10
Host is up (0.00030s latency).
Not shown: 990 filtered ports
PORT     STATE  SERVICE        VERSION
22/tcp   open   ssh            OpenSSH 5.6 (protocol 2.0)
| ssh-hostkey:
|   1024 e3:93:64:12:9c:c0:70:72:35:e1:ac:61:af:cc:49:ec (DSA)
|_  2048 2a:0b:42:38:f4:ca:d6:07:95:aa:87:ed:52:de:d1:14 (RSA)
80/tcp   open   http           VMware ESXi Server httpd
|_http-title: Did not follow redirect to https://10.10.50.10/
427/tcp  open   svrloc?
443/tcp  open   ssl/http       VMware ESXi Server httpd
|_http-title: " + ID_EESX_Welcome + "
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2014-01-15T03:42:31
|_Not valid after:  2025-07-16T03:42:31
|_ssl-date: 2018-04-25T19:58:24+00:00; -9h53m36s from scanner time.
| vmware-version:
|   Server version: VMware ESXi 5.1.0
|   Build: 1065491
|   Locale version: INTL 000
|   OS type: vmnix-x86
|_  Product Line ID: embeddedEsx
902/tcp  open   ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
5988/tcp closed wbem-http
5989/tcp open   ssl/wbem       SBLIM Small Footprint CIM Broker
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2014-01-15T03:42:31
|_Not valid after:  2025-07-16T03:42:31
|_ssl-date: 2018-04-25T19:58:23+00:00; -9h53m36s from scanner time.
8000/tcp open   http-alt?
8100/tcp open   tcpwrapped
8300/tcp closed tmi
MAC Address: F8:72:EA:A4:A1:CC (Cisco Systems)
Aggressive OS guesses: VMware ESXi 5.0 - 5.5 (96%), VMware ESXi 5.5 (96%), VMware ESXi
4.1 (95%), VMware ESXi 6.0.0 (93%), FreeBSD 7.0-RELEASE-p1 - 10.0-CURRENT (93%),
VMware ESXi 4.1.0 (93%), VMware ESX Server 4.0.1 (91%), FreeBSD 5.2.1-RELEASE (91%),
FreeBSD 8.0-BETA2 - 10.1-RELEASE (90%), FreeBSD 5.3 - 5.5 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: localhost.localdomain; CPE: cpe:/o:vmware:esxi, cpe:/o:vmware:ESXi:5.1.0

Host script results:
|_clock-skew: mean: -9h53m36s, deviation: 0s, median: -9h53m36s

TRACEROUTE
HOP RTT     ADDRESS
1   0.30 ms 10.10.50.10

Nmap scan report for 10.10.50.11
Host is up (0.00058s latency).
Not shown: 990 filtered ports
PORT     STATE  SERVICE        VERSION
22/tcp   open   ssh            OpenSSH 5.6 (protocol 2.0)
| ssh-hostkey:
|   1024 6f:d3:3d:cb:54:0b:83:3e:bd:25:1c:da:67:b6:92:fb (DSA)
|_  2048 f9:bc:20:c5:6e:db:6a:86:ea:f5:24:06:57:c6:d9:6f (RSA)
80/tcp   open   http           VMware ESXi Server httpd
|_http-title: Did not follow redirect to https://10.10.50.11/
427/tcp  open   svrloc?
443/tcp  open   ssl/http       VMware ESXi Server httpd
|_http-title: " + ID_EESX_Welcome + "
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2014-01-18T05:33:03
|_Not valid after:  2025-07-19T05:33:03
|_ssl-date: 2018-04-25T19:50:12+00:00; -10h01m33s from scanner time.
| vmware-version:
|   Server version: VMware ESXi 5.1.0
|   Build: 1065491
|   Locale version: INTL 000
|   OS type: vmnix-x86
|_  Product Line ID: embeddedEsx
902/tcp  open   ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
5988/tcp closed wbem-http
5989/tcp open   ssl/wbem       SBLIM Small Footprint CIM Broker
```

```
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2014-01-18T05:33:03
|_Not valid after:  2025-07-19T05:33:03
|_ssl-date: 2018-04-25T19:50:25+00:00; -10h01m35s from scanner time.
8000/tcp open   http-alt?
8100/tcp open   tcpwrapped
8300/tcp closed tmi
MAC Address: F8:72:EA:A4:A1:2C (Cisco Systems)
Device type: specialized
Running: VMware ESXi 5.X
OS CPE: cpe:/o:vmware:esxi:5
OS details: VMware ESXi 5.0 - 5.5
Network Distance: 1 hop
Service Info: Host: localhost.localdomain; CPE: cpe:/o:vmware:esxi, cpe:/o:vmware:ESXi:5.1.0

Host script results:
|_clock-skew: mean: -10h01m34s, deviation: 1s, median: -10h01m35s

TRACEROUTE
HOP RTT     ADDRESS
1   0.58 ms 10.10.50.11

Nmap scan report for vc.ooredoocloud.qa (10.10.50.20)
Host is up (0.00065s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8d:b4:b0:01:63:84:eb:c7:bf:cf:f7:b0:c3:12:0e:13 (RSA)
|   256 02:31:3e:d3:75:97:f2:10:88:30:6a:c1:ca:a4:82:bf (ECDSA)
|_  256 c5:21:3a:a7:81:f5:a6:00:ee:5e:76:94:88:68:03:1d (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:72:4A:C1 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.65 ms 10.10.50.20

Nmap scan report for 10.10.50.100
Host is up (0.00078s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE         VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp   open  ssl/http        VMware VirtualCenter Web service
|_http-title: Site doesn't have a title (text; charset=plain).
| ssl-cert: Subject: commonName=VMware/countryName=US
| Not valid before: 2017-12-19T17:36:01
|_Not valid after:  2018-12-19T17:36:01
|_ssl-date: TLS randomness does not represent time
| vmware-version:
|   Server version: VMware Workstation 12.5.6
|   Build: 5528349
|   Locale version: INTL
|   OS type: win32-x86
|_  Product Line ID: ws
445/tcp   open  microsoft-ds    Windows 7 Professional 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
554/tcp   open  rtsp?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1025/tcp  open  msrpc           Microsoft Windows RPC
1026/tcp  open  msrpc           Microsoft Windows RPC
1027/tcp  open  msrpc           Microsoft Windows RPC
1028/tcp  open  msrpc           Microsoft Windows RPC
1030/tcp  open  msrpc           Microsoft Windows RPC
1031/tcp  open  msrpc           Microsoft Windows RPC
2869/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server   Microsoft Terminal Service
| ssl-cert: Subject: commonName=Win7-PC
| Not valid before: 2017-12-12T19:55:25
|_Not valid after:  2018-06-13T19:55:25
|_ssl-date: 2018-04-26T05:47:49+00:00; -3m54s from scanner time.
5357/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
MAC Address: 00:0C:29:95:04:33 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN7-PC; OS: Windows; CPE: cpe:/o:microsoft:windows,
cpe:/o:vmware:Workstation:12.5.6
```

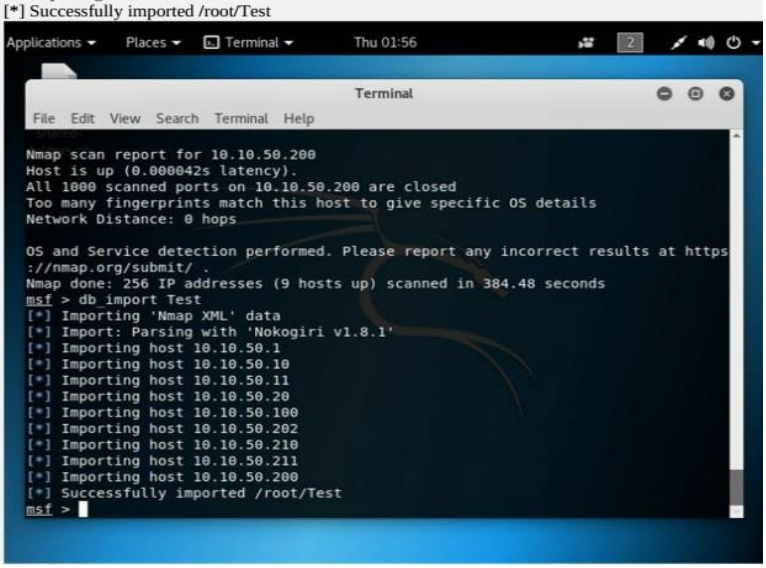
```
Host script results:
|_clock-skew: mean: -3m54s, deviation: 0s, median: -3m54s
|_nbstat: NetBIOS name: WIN7-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:95:04:33
(VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Win7-PC
|   NetBIOS computer name: WIN7-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2018-04-26T10:47:56+05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2018-04-26 01:48:04
|_  start_date: 2018-03-27 07:26:43

TRACEROUTE
HOP RTT     ADDRESS
1   0.78 ms 10.10.50.100

Nmap scan report for 10.10.50.202
Host is up (0.00096s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup:
WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=Win7-1-PC
| Not valid before: 2018-03-05T06:10:47
|_Not valid after:  2018-09-04T06:10:47
|_ssl-date: 2018-04-26T05:51:38+00:00; -28s from scanner time.
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
49160/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:20:C4:A9 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN7-1-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -28s, deviation: 0s, median: -28s
|_nbstat: NetBIOS name: WIN7-1-PC, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:20:c4:a9 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Win7-1-PC
|   NetBIOS computer name: WIN7-1-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2018-04-25T22:51:33-07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2018-04-26 01:51:33
|_  start_date: 2018-03-29 05:57:42

TRACEROUTE
HOP RTT     ADDRESS
1   0.96 ms 10.10.50.202

Nmap scan report for 10.10.50.210
Host is up (0.00065s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3c:9c:fb:cb:58:35:f9:d7:d7:32:6f:ad:6a:f8:c7:9b (RSA)
```

```
|   256 70:e7:d9:a2:6a:54:92:e6:07:c9:89:58:b5:99:7d:0d (ECDSA)
|_  256 b1:be:a6:62:96:69:76:64:aa:23:bb:ad:54:cc:c0:db (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:EA:BD:DF (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.65 ms 10.10.50.210

Nmap scan report for 10.10.50.211
Host is up (0.00037s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-2HMGPM3UAD7
| Not valid before: 2018-03-28T12:23:16
|_Not valid after:  2018-09-27T12:23:16
|_ssl-date: 2018-04-26T05:51:41+00:00; -5s from scanner time.
MAC Address: 00:0C:29:BA:AC:AA (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 6.X (85%)
OS CPE: cpe:/o:FreeBSD:FreeBSD:6.2
Aggressive OS guesses: FreeBSD 6.2-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:Microsoft:windows

Host script results:
|_clock-skew: mean: -5s, deviation: 0s, median: -5s

TRACEROUTE
HOP RTT     ADDRESS
1   0.37 ms 10.10.50.211

Nmap scan report for 10.10.50.200
Host is up (0.000042s latency).
All 1000 scanned ports on 10.10.50.200 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (9 hosts up) scanned in 384.48 seconds
```

//Importing Nmap XML file

msf > **db_import Test**

```
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.8.1'
[*] Importing host 10.10.50.1
[*] Importing host 10.10.50.10
[*] Importing host 10.10.50.11
[*] Importing host 10.10.50.20
[*] Importing host 10.10.50.100
[*] Importing host 10.10.50.202
[*] Importing host 10.10.50.210
[*] Importing host 10.10.50.211
[*] Importing host 10.10.50.200
[*] Successfully imported /root/Test
```




msf > hosts

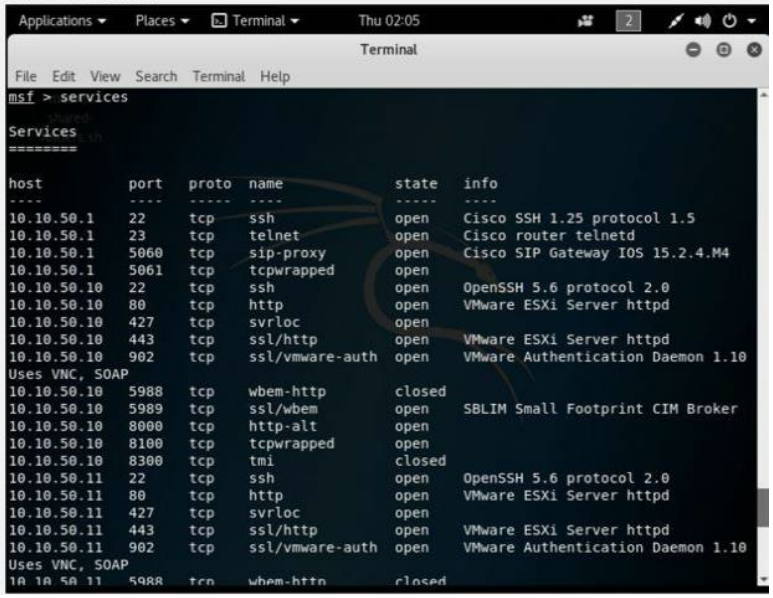
```
Hosts
=====

Address         mac            name       os_name   os_flavor os_sp purpose info comments
-------         ---            ----       -------   --------- ----- ------- ---- --------
10.10.50.1      c0:67:af:c7:d9:80            IOS                 12.X  device
10.10.50.10     f8:72:ea:a4:a1:cc            ESXi                5.X   device
10.10.50.11     f8:72:ea:a4:a1:2c            ESXi                5.X   device
10.10.50.20     00:0c:29:72:4a:c1            Linux               3.X   server
10.10.50.100    00:0c:29:95:04:33            Windows 7                 client
10.10.50.200    Unknown                 device
10.10.50.202    00:0c:29:20:c4:a9            Windows 7                 client
10.10.50.210    00:0c:29:ea:bd:df            Linux               3.X   server
10.10.50.211    00:0c:29:ba:ac:aa            FreeBSD             6.X   device
```

//Performing Services scan

msf > **db_nmap -sS -A 10.10.50.211**

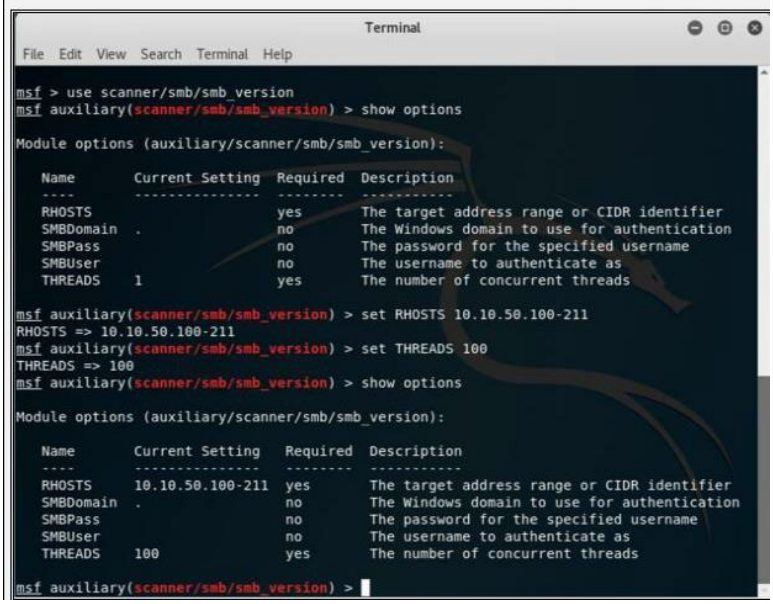

Observe the scan result showing different services, open and closed port information of live hosts.

msf > **services**

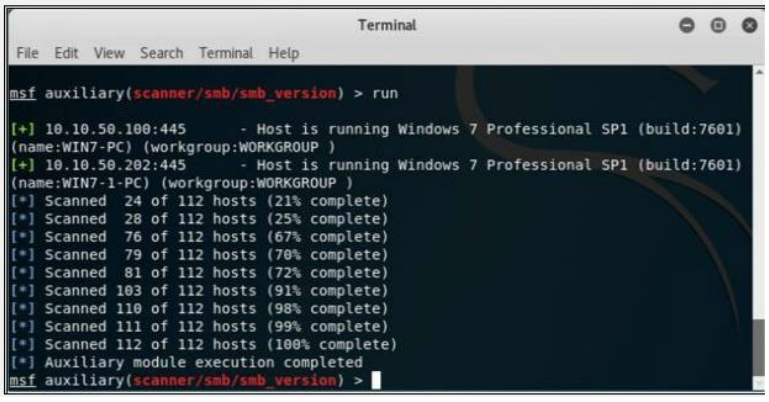


```
msf > use scanner/smb/smb_version
msf auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   SMBDomain.                  no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads
```

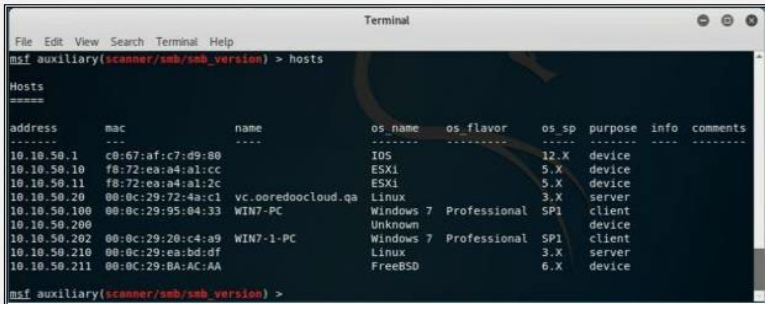
```
msf auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.50.100-211
RHOSTS => 10.10.50.100-211

msf auxiliary(scanner/smb/smb_version) > set THREADS 100
THREADS => 100

msf auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS     10.10.50.100-211 yes       The target address range or CIDR identifier
   SMBDomain.                  no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    100              yes       The number of concurrent threads
```




```
msf auxiliary(scanner/smb/smb_version) > run
```



msf auxiliary(scanner/smb/smb_version) > **hosts**




Observe the OS_Flavor field. SMB scanning scans for Operating System Flavor for the RHOST range configured.