

No.	Name	Page No.	Sign
	<b>PRACTICAL 1</b>	<b>1</b>	
A.	Using the tools for whois, traceroute, email tracking, google hacking.	1	
1)	Traceroute (tracert):	1	
2)	Ping Utility:	1	
3)	nslookup:	2	
4)	SmartWhois	3	
5)	eMailTracker Pro	5	
6)	HTTrack Website Copier	7	
7)	Search Diggity	8	
	<b>PRACTICAL 2</b>	<b>10</b>	
A.	Using the tools for scanning network, IP fragmentation, war dialing countermeasures, SSL Proxy, Censorship circumvention.	10	
1)	Advanced IP Scanner	10	
2)	Amap	11	
3)	Nmap	13	
4)	CurrPorts Tool	17	
5)	LANSurveyor	22	
6)	Nessus	25	
7)	Colasoft Packet Builder	31	
8)	The Dude	34	
	<b>PRACTICAL 3</b>	<b>37</b>	
A.	Using NETBIOS Enumeration tool, SNMP Enumeration tool, LINUX/UNIX. enumeration tools, NTP Enumeration tool, DNS analyzing and	37	

	enumeration tool.		
1)	Nmap	37	
2)	SuperScan	38	
3)	NetBIOS Enumerator Tool	40	
4)	SoftPerfect Network Scanner	41	
5)	Hyena	43	
<b>PRACTICAL 4</b>		<b>47</b>	
A.	Study of System Hacking tool	47	
1)	LCP	47	
2)	RainbowCrack and WinRTGen	48	
3)	L0pthCrack	50	
4)	Ophcrack	53	
5)	NTFS ADS	54	
6)	ADS Spy	55	
7)	Stealth Files Tool	56	
8)	Snow	57	
9)	CHNTPW.ISO	57	
10)	Quick Stego	59	
<b>PRACTICAL 5</b>		<b>60</b>	
A.	Study of Denial of Service attack tools.	60	
1)	hping3	60	
2)	DoSHTTP	60	
<b>PRACTICAL 6</b>		<b>62</b>	

A.	Study of Web server Attack tools	62	
1)	IBM Security AppScan	62	
<b>PRACTICAL 7</b>		<b>65</b>	
A.	Using Cryptanalysis Tools	65	
1)	TrueCrypt	65	
2)	Cryptool	65	
3)	Advanced Encryption Package	67	
<b>PRACTICAL 8</b>		<b>68</b>	
A.	Using HashCalc Tools	68	
1)	HashCalc	68	
<b>PRACTICAL 9</b>		<b>69</b>	
A.	Using MD5 Calculator Tools	69	
1)	MD5 Calculator	69	
<b>PRACTICAL 10</b>		<b>70</b>	
A.	Using BCTextEncoder Tools	70	
1)	BCTextEncoder	70	
<b>PRACTICAL 11</b>		<b>71</b>	
A.	Using Rohos Disk Encryption Tools	71	
1)	Rohos Disk Encryption	71	
<b>PRACTICAL 12</b>		<b>73</b>	
A.	Study of Session Hijacking tools	73	
1)	ZAP	73	
<b>PRACTICAL 13</b>		<b>82</b>	

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):

```
C:\Users\user>tracert www.google.com
Tracing route to www.google.com [74.125.200.105]
over a maximum of 30 hops:
1  49 ms   52 ms   61 ms  172.29.145.65
2  51 ms   53 ms   51 ms  172.29.145.67
3  347 ms  69 ms   50 ms  172.29.145.102
4  120 ms  87 ms   51 ms  115.113.165.53.static-mumbai.vsnl.net.in [115.113.165.53]
5  293 ms  133 ms  97 ms  172.29.251.33
6  *         *         * Request timed out.
7  109 ms  116 ms  98 ms  115.114.85.241
8  269 ms  133 ms  130 ms  if-5-2.tcore1.SVW-Singapore.as6453.net [180.87.12.53]
9  242 ms  137 ms  125 ms  72.14.220.134
10  258 ms  206 ms  132 ms  66.249.95.14
11  297 ms  303 ms  376 ms  64.233.174.109
12  *         *         * Request timed out.
13  157 ms  125 ms  129 ms  sa-in-F105.ie100.net [74.125.200.105]

Trace complete.

C:\Users\user>
```

```
C:\Users\user>tracert -h 8 www.google.com
Tracing route to www.google.com [74.125.200.105]
over a maximum of 8 hops:
1  328 ms  258 ms  310 ms  172.29.145.65
2  338 ms  257 ms  262 ms  172.29.145.67
3  84 ms   71 ms   70 ms   172.29.145.102
4  71 ms   48 ms   75 ms   115.113.165.53.static-mumbai.vsnl.net.in [115.113.165.53]
5  107 ms  99 ms   78 ms   172.29.251.33
6  *         *         * Request timed out.
7  586 ms  265 ms  161 ms  115.114.85.241
8  143 ms  105 ms  141 ms  if-5-2.tcore1.SVW-Singapore.as6453.net [180.87.12.53]

Trace complete.

C:\Users\user>
```

### 2) Ping Utility:

```
C:\Users\user>ping www.google.com
Pinging www.google.com [74.125.200.105] with 32 bytes of data:
Reply from 74.125.200.105: bytes=32 time=278ms TTL=47
Reply from 74.125.200.105: bytes=32 time=455ms TTL=47
Reply from 74.125.200.105: bytes=32 time=313ms TTL=47
Reply from 74.125.200.105: bytes=32 time=234ms TTL=47

Ping statistics for 74.125.200.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 234ms, Maximum = 455ms, Average = 320ms

C:\Users\user>
```

Finding out the maximum frame size on the network

```
C:\Users\user>ping www.google.com -f -l 1500
Pinging www.google.com [74.125.200.105] with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 74.125.200.105:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user>ping www.google.com -f -l 1300
Pinging www.google.com [74.125.200.105] with 1300 bytes of data:
Reply from 74.125.200.105: bytes=64 (sent 1300) time=395ms TTL=47
Reply from 74.125.200.105: bytes=64 (sent 1300) time=199ms TTL=47
Reply from 74.125.200.105: bytes=64 (sent 1300) time=377ms TTL=47
Reply from 74.125.200.105: bytes=64 (sent 1300) time=501ms TTL=47

Ping statistics for 74.125.200.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 199ms, Maximum = 501ms, Average = 368ms
```

Trying different values until you find the maximum frame size.

```
C:\Users\user>ping www.google.com -f -l 1473
C:\Users\user>ping www.google.com -f -l 1350
```

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

```
C:\Users\user>ping www.google.com -i 3
C:\Users\user>
```

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 15Hops.

```
C:\Users\user>ping www.google.com -i 1 -n 1
C:\Users\user>ping www.google.com -i 12 -n 1
C:\Users\user>ping www.google.com -i 13 -n 1
C:\Users\user>
```

### 3) nslookup:

```
C:\>nslookup
Server: ns3.tataidc.co.in
Address: 103.8.45.5

> set type= cname
> www.google.com
Server: ns3.tataidc.co.in
Address: 103.8.45.5

Non-authoritative answer:
Name: www.google.com
Addresses: 74.125.130.106
74.125.130.105
74.125.130.99
74.125.130.104
74.125.130.103
74.125.130.147
```

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

```
C:\>nslookup
Default Server: ns3.tataidc.co.in
Address: 103.8.45.5

> set type=cname
> google.com
Server: ns3.tataidc.co.in
Address: 103.8.45.5

google.com
    primary name server = ns1.google.com
    responsible mail addr = dns-admin.google.com
    serial = 1572902
    refresh = 7200 (2 hours)
    retry = 1800 (30 mins)
    expire = 1209600 (14 days)
    default TTL = 300 (5 mins)
```

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

```
> server 64.147.99.90
Default Server: 64.147.99.90.static.nyinternet.net
Address: 64.147.99.90

>
>
> set type=a
> www.google.com
Server: 64.147.99.90.static.nyinternet.net
Address: 64.147.99.90

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to 64.147.99.90.static.nyinternet.net timed-out
>
```

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

```
C:\>nslookup
Default Server: ns3.tataidc.co.in
Address: 103.8.45.5

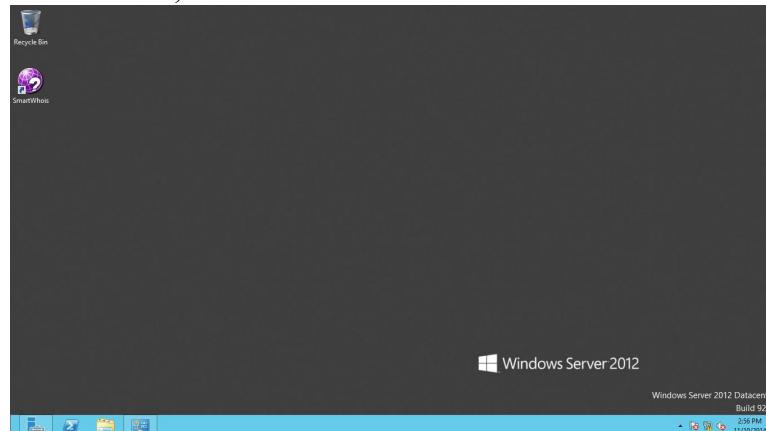
>
>
> set type=mx
> google.com
Server: ns3.tataidc.co.in
Address: 103.8.45.5

Non-authoritative answer:
google.com    MX preference = 40, mail exchanger = alt3.aspmx.l.google.com
google.com    MX preference = 30, mail exchanger = alt2.aspmx.l.google.com
google.com    MX preference = 10, mail exchanger = aspmx.l.google.com
google.com    MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
google.com    MX preference = 50, mail exchanger = alt4.aspmx.l.google.com
```

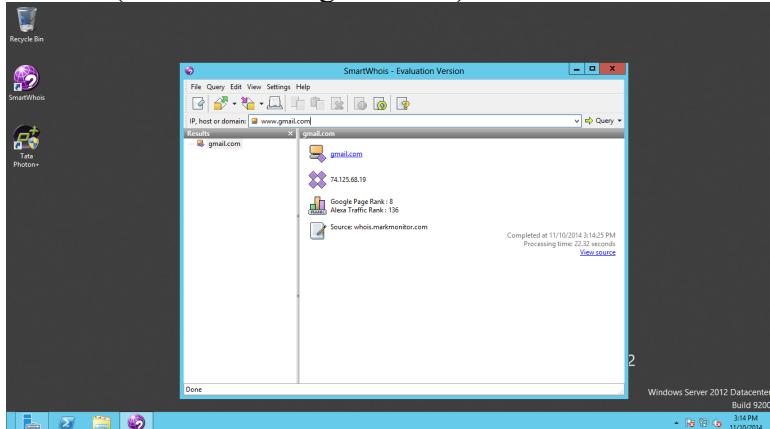
#### 4) SmartWhois

Follow the wizard driven installation steps and install smartwhois :

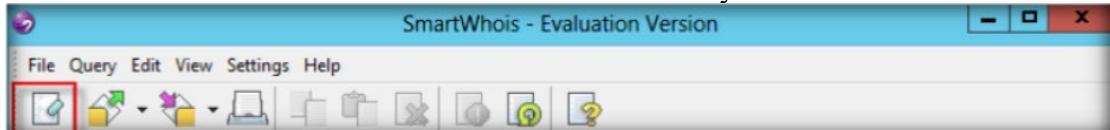
1. To launch smartwhois, click smartwhois :



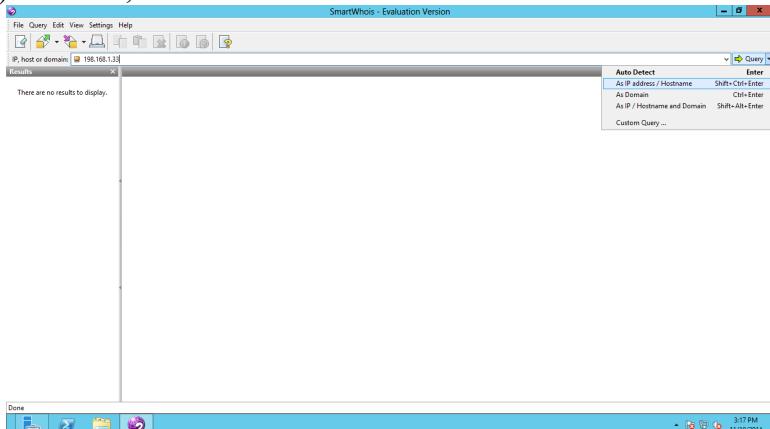
2. The smartwhois main window appears .
3. Type an IP Address, hostname or domain name in the tab field .An example of the domain name (as shownwww.gmail.com)



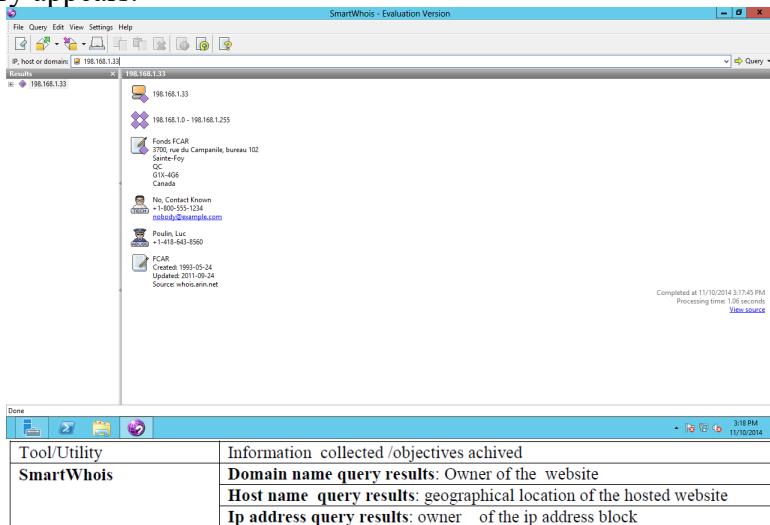
4. Click the clear icon in the tool bar to clear the history.



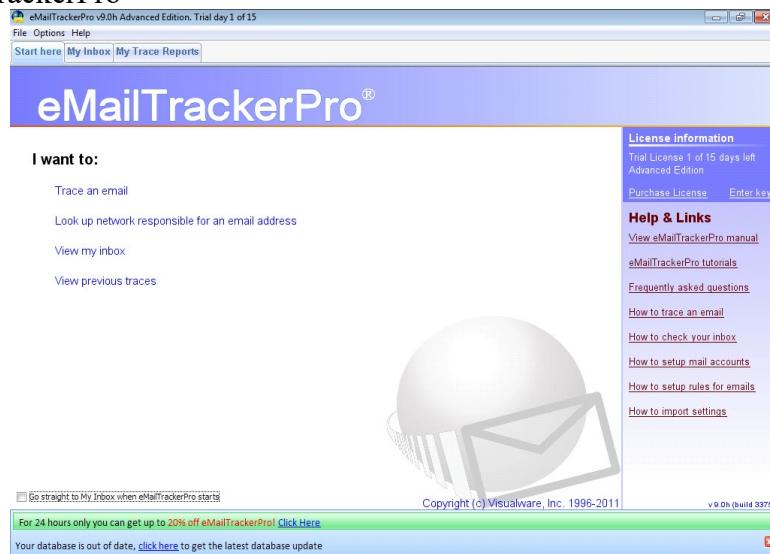
5. To perform a sample IP Address query type the IP Address (windows 8 IP Address ) in the IP, host or domain field.



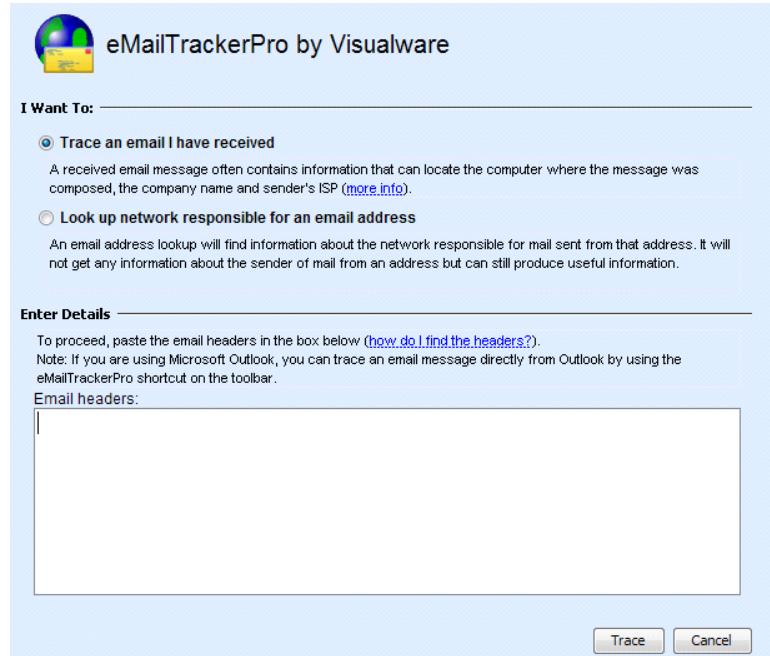
6. In the left pane of the window the result appears and in the right pane result of your query appears.



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'

# Security Breaches and Countermeasures

2314041

**I Want To:**

Trace an email I have received  
A received email message often contains information that can locate the computer where the message was composed, the company name and sender's ISP ([more info](#)).

Look up network responsible for an email address  
An email address lookup will find information about the network responsible for mail sent from that address. It will not get any information about the sender of mail from an address but can still produce useful information.

**Enter Details**

To proceed, paste the email headers in the box below ([how do I find the headers?](#)).  
Note: If you are using Microsoft Outlook, you can trace an email message directly from Outlook by using the eMailTrackerPro shortcut on the toolbar.

Email headers:

```
Delivered-To: [REDACTED]@gmail.com
Received: by 10.76.21.174 with SMTP id w14csp245504oae;
Tue, 11 Nov 2014 00:31:09 -0800 (PST)
X-Received: by 10.236.229.164 with SMTP id h34mr501386yhq.199.141569
Tue, 11 Nov 2014 00:31:09 -0800 (PST)
Return-Path: <sender_47819_497_16950523@emcsend.com>
Received: from mail116.emcsend.com (mail116.emcsend.com. [216.27.12.15]
<[REDACTED]>
```

**Trace**    **Cancel**

## Click on Trace

The trace is complete, the information found is displayed on the right

**Map**

**Table**

#	Hop IP	Hop Name	Location
1	172.16.150.2		
2	172.16.109.1		
3	10.118.246.141		
5	10.255.222.97		
6	10.152.7.5		
7	125.18.4.25		(India)
8	182.79.255.33		(Australia)
10	66.192.245.238	rdt1-ar4-xe-2-0-0-0.us.twftelecom[America]	
11	66.192.24.90	66.192.24.90.static.twftelecom[America]	

**Email Summary**

From: care@bewakoof.com  
To: [REDACTED]@gmail.com  
Date: Tue, 11 Nov 2014 07:49:44 +0000  
Subject: Bewakoof Shopping App is here! - Download Now  
Location: [America]

Misdirected: No  
Abuse Reporting: To automatically generate an email abuse report [click here](#)  
From IP: 216.27.12.151

System Information:

- There is no SMTP server running on this system (the port is closed).
- The system is running a web server on port 80 ([click here to view it](#)). This means that this system serves web pages.
- The system is running a service web server on port 443 ([click here to view it](#)). This means that this system serves encrypted web pages. It therefore probably handles sensitive data, such as credit card information.

**Network Whois**  
**Domain Whois**  
**Email Header**

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.

eMailTrackerPro 9.0h Advanced Edition. Trial day 1 of 15

File Options Help

Start here My Inbox My Trace Reports Subject: Bewakoof Shop...

All traces complete

**Map**

**Trace Information**

Subject: Bewakoof Shopping App is here! - Download Now.  
Misdirected: No  
From: care@bewakoof.com  
Sender IP: 216.27.12.151  
Abuse Address: (None Found)  
Location: [America]

**Previous Traces**

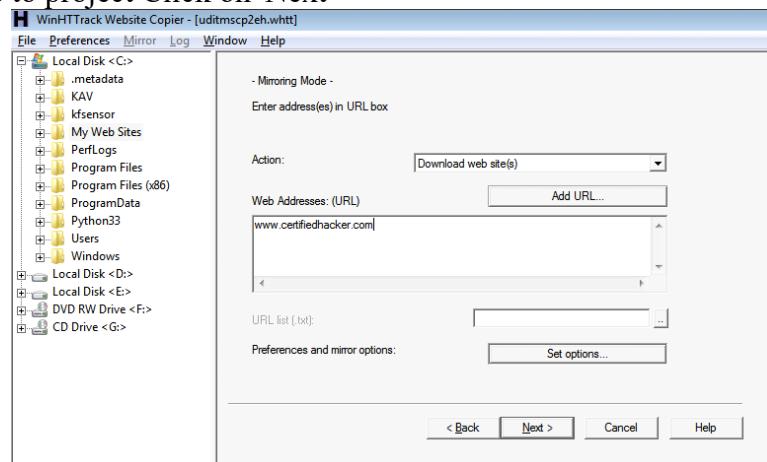
Actions	Subject	From	IP
New Trace	Bewakoof Shop	care@bewakoof	216.27.12.151

## 6) HTTrack Website Copier

Start > Programs > HTTrack Website Copier

Click on 'Next' to create Project

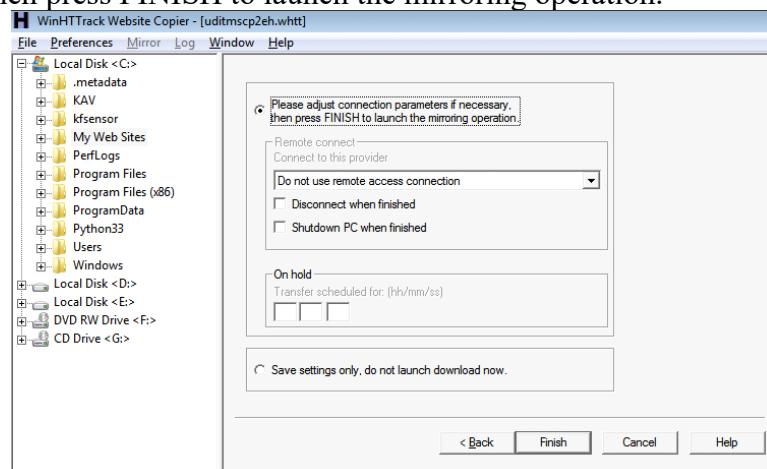
Give a name to project Click on 'Next'



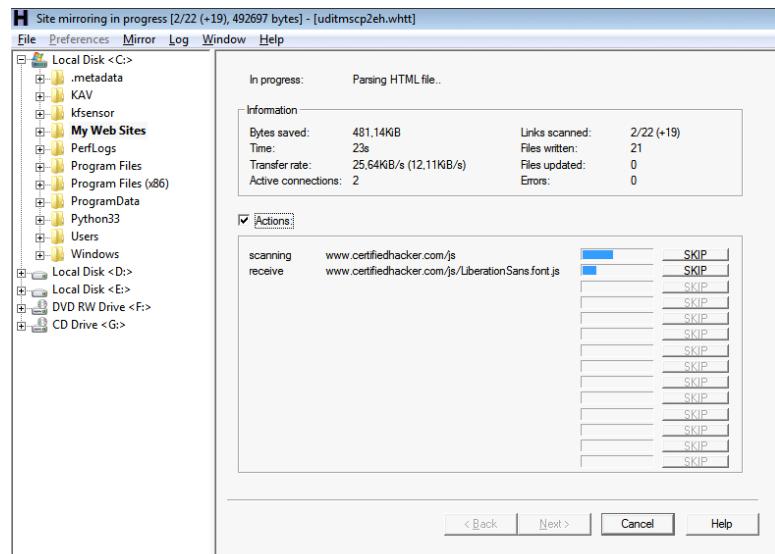
Click on 'Add URL' and give the URL of the site to mirror from.

Any additional options that need to be set, can be set from the 'Set Options' menu  
Then click 'Next'

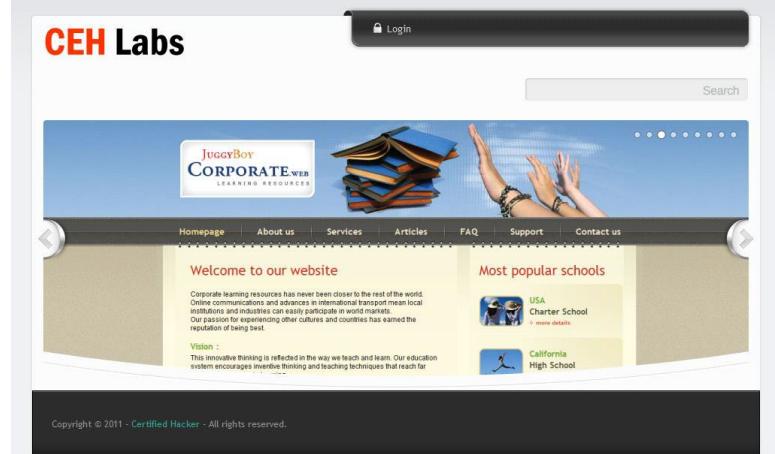
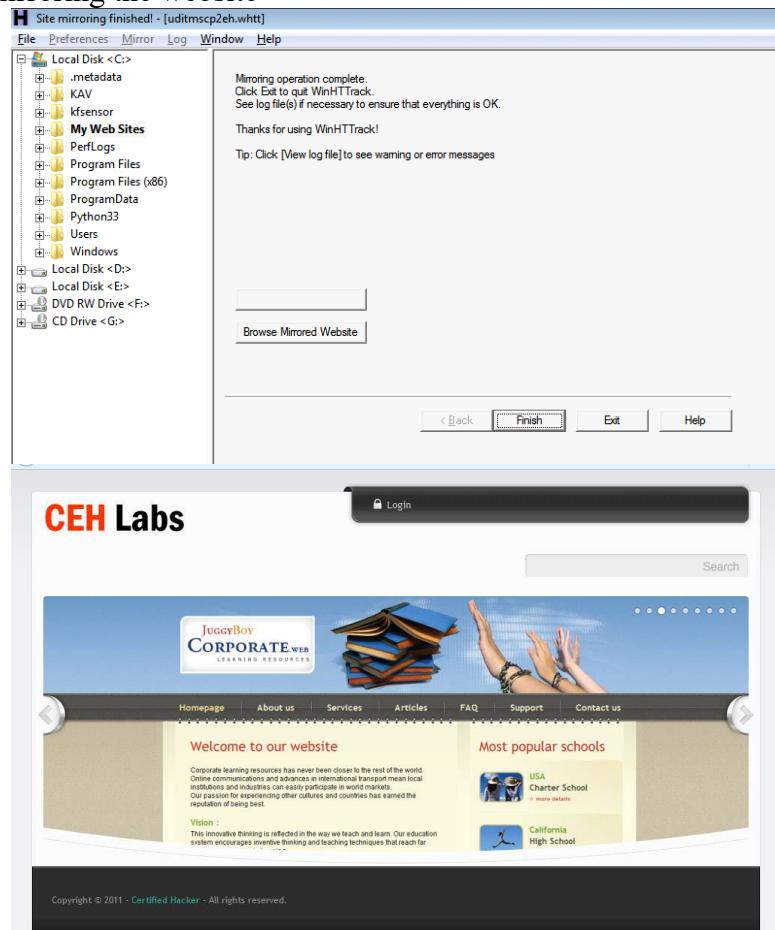
By default, the radio button will be selected for Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.



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



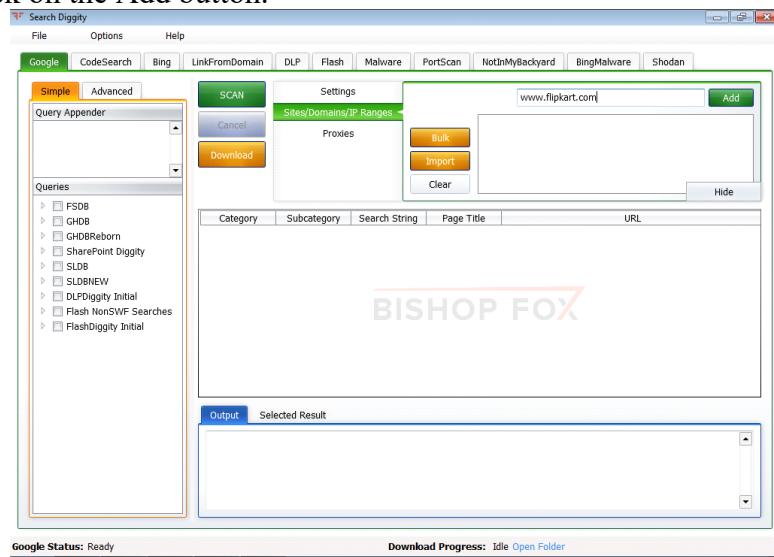
### 7) Search Diggity

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

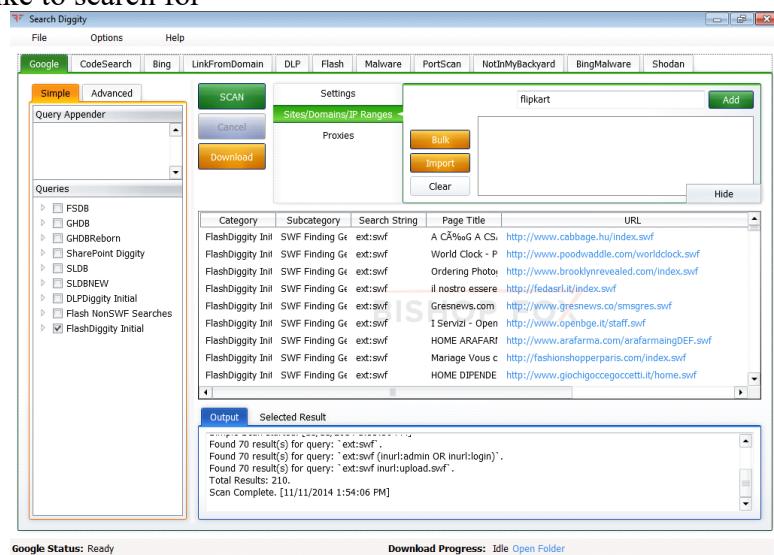
Start > Programs > SearchDiggity

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

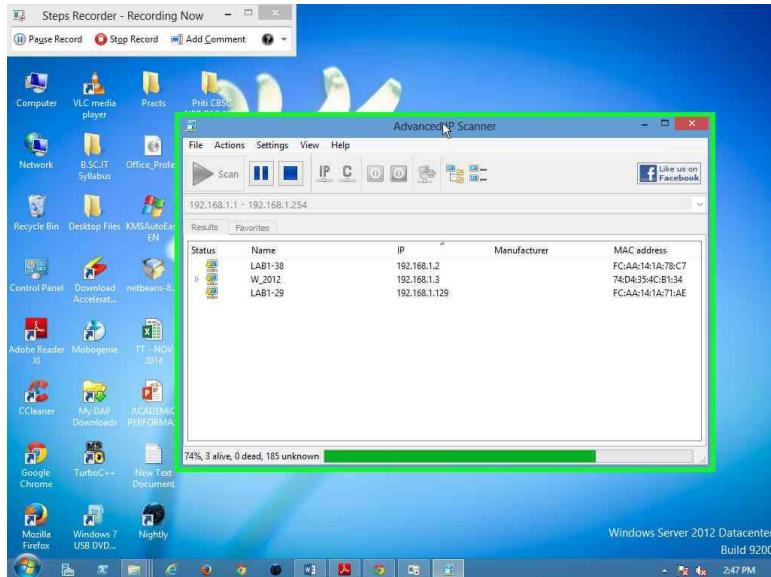


## PRACTICAL 2

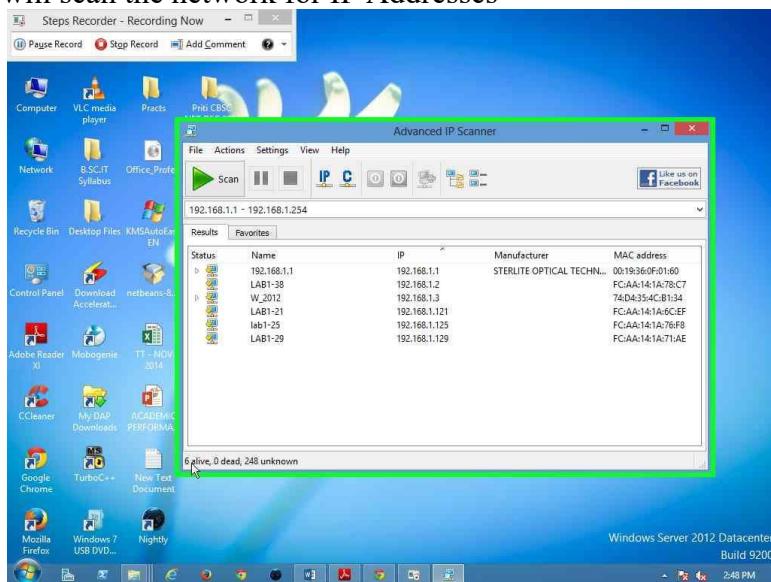
### A. Using the tools for scanning network, IP fragmentation, war dialing countermeasures, SSL Proxy, Censorship circumvention.

#### 1) Advanced IP Scanner

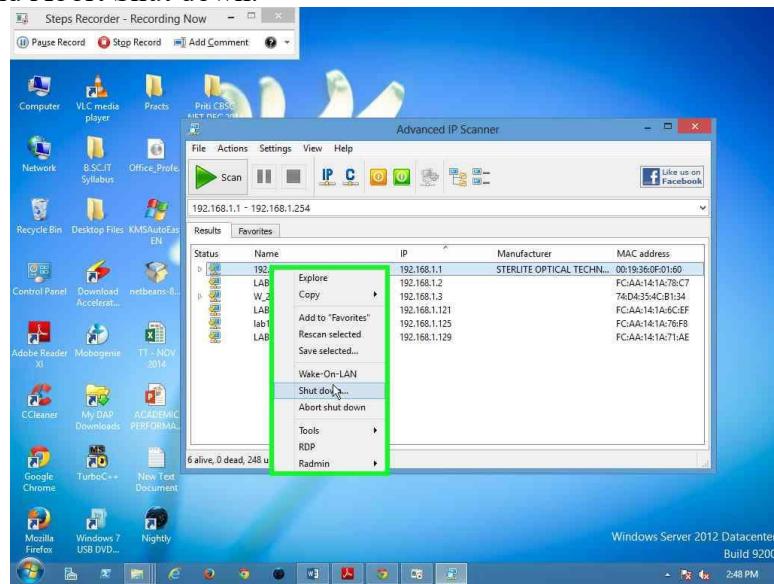
1. After successful installation of the software, launch the tool.
2. click on scan:



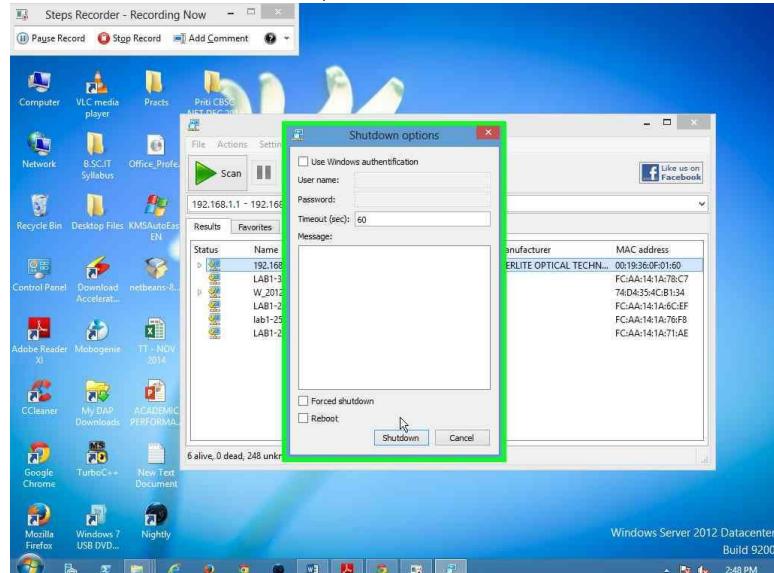
3. The tool will scan the network for IP Addresses



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

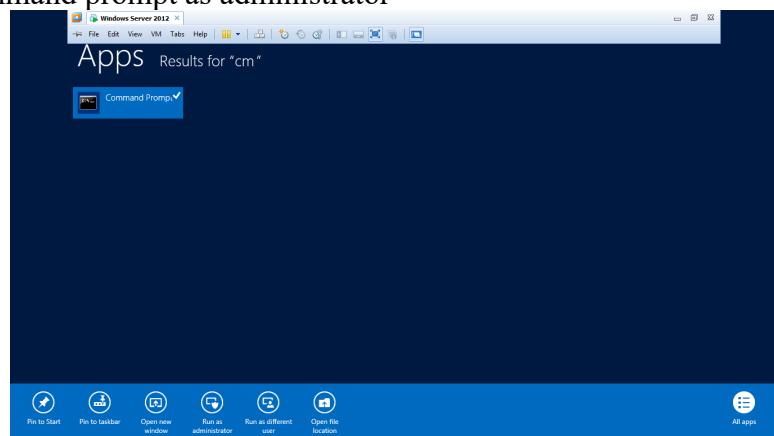


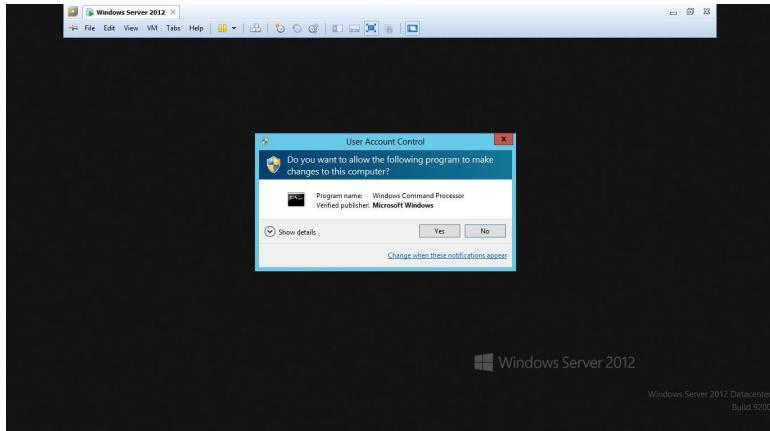
5. Now you have die IP Address, Name, and other details of die victim machine



2) Amap

1. Run command prompt as administrator

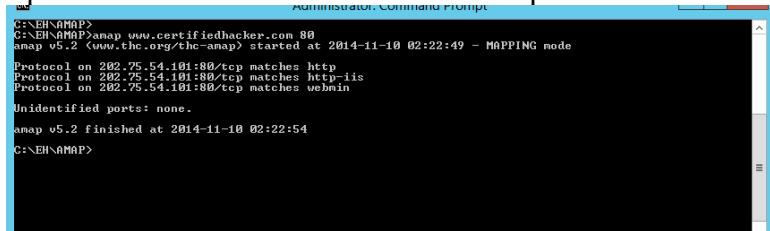




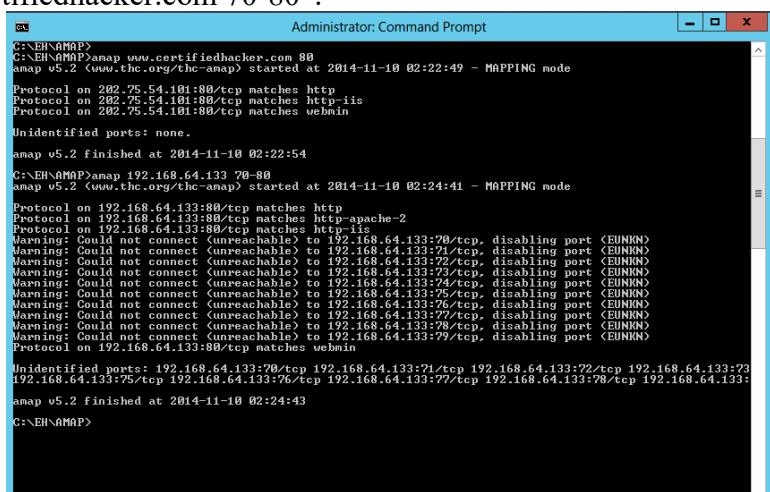
2. Navigate amap directory(here C:\EH\AMAP)



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.ceritificatehacker.com 70-80".



Identified open port : 80

Web servers:

http  
http-apache-2  
http-iis  
webmin

Unidentified ports:

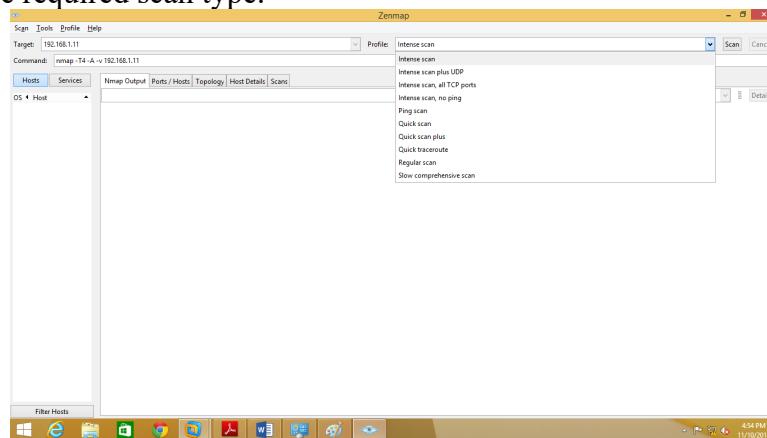
192.168.64.133:70/tcp  
192.168.64.133:71/tcp  
192.168.64.133:72/tcp  
192.168.64.133:73/tcp  
192.168.64.133:74/tcp  
192.168.64.133:75/tcp  
192.168.64.133:76/tcp  
192.168.64.133:77/tcp  
192.168.64.133:78/tcp  
192.168.64.133:79/tcp (total 10).

3) Nmap

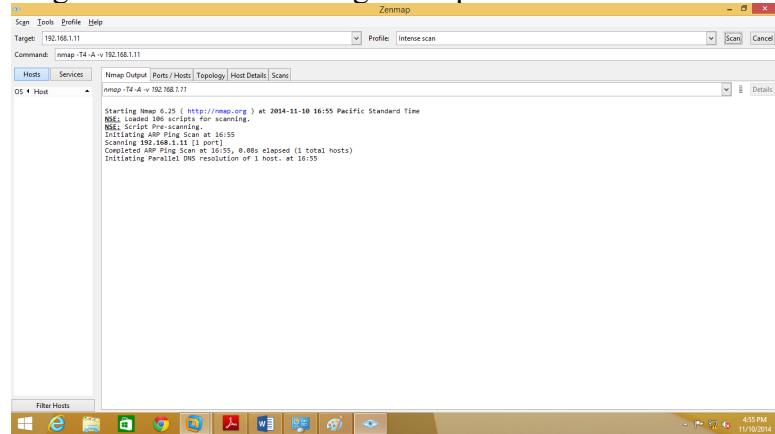
1. Select the NMAP icon
2. Double click on NMAP Icon on Desktop



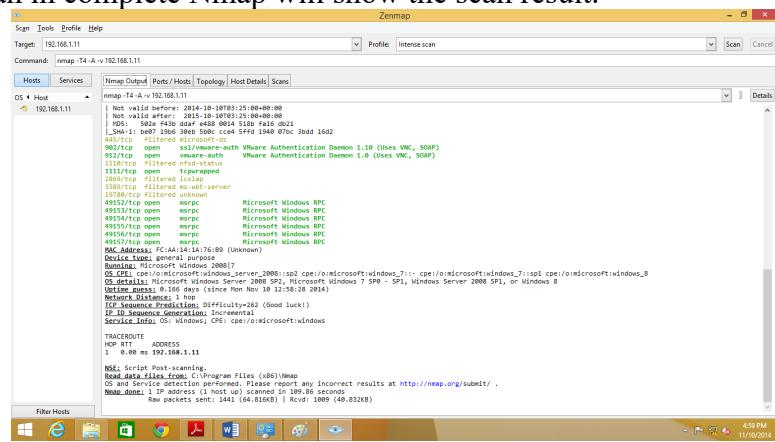
3. Put the IP-Address for scanning
4. Select the required scan type.



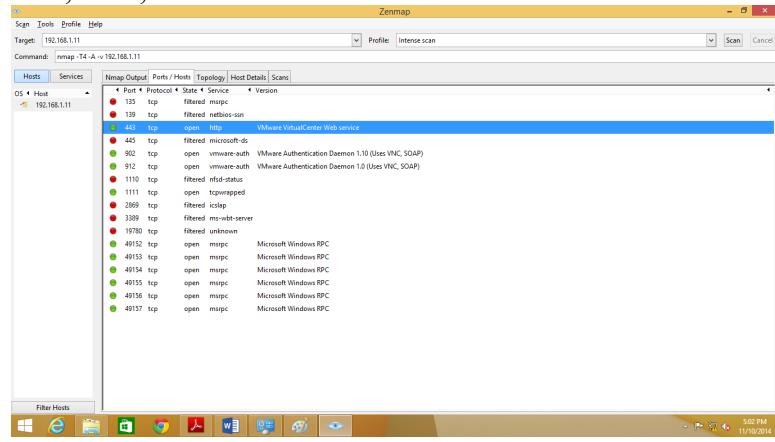
5. After selecting scan type click on scan button.
6. After clicking on scan wait till scan get complete.



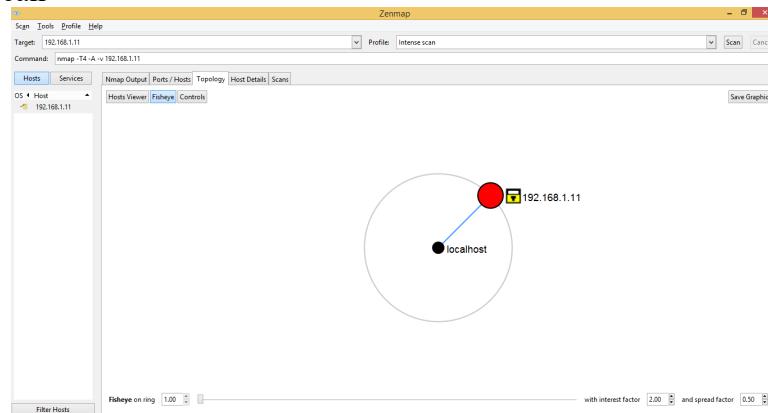
7. After scan in complete Nmap will show the scan result.



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.

Host Status	State	OS
Ports	Open ports: 10 Filtered ports: 7 Closed ports: 983 Scanned ports: 1000 Up time: 14123 Last boot: Mon Nov 10 12:58:28 2014	Microsoft Windows Server 2008 SP2

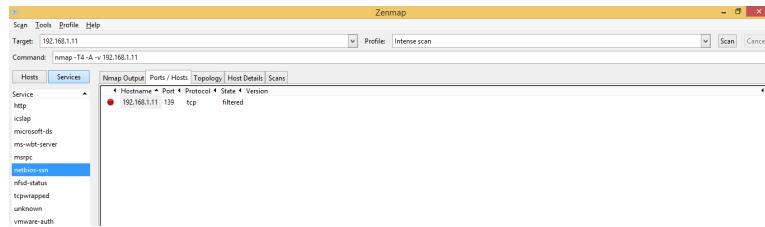
11. Click the scan tab to scan details for provided IP Address.

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

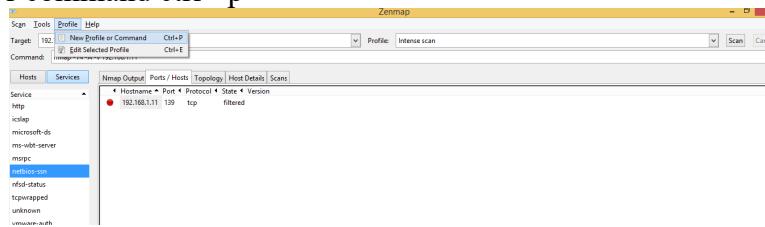
13. Click the msrpc service to list all the Microsoft windows RPC

Service	Port	Protocol	State	Version
http	49157	tcp	open	VMware VirtualCenter Web service
icqdp	49156	tcp	open	Microsoft Windows RPC
msrpc	49155	tcp	open	Microsoft Windows RPC
ms-wbt-server	49154	tcp	open	Microsoft Windows RPC
netbios-ssn	49153	tcp	open	Microsoft Windows RPC
netbios-status	49152	tcp	open	Microsoft Windows RPC
rdpwrapped	135	tcp	filtered	

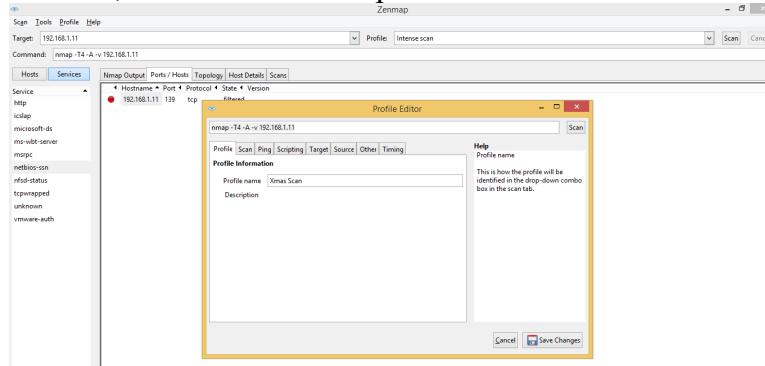
14. Click the netbios-ssn service to list all NetBIOS hostnames.



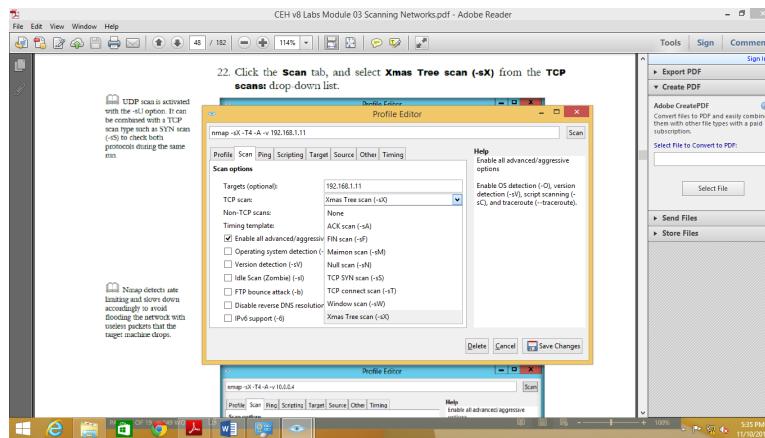
15. Xmas scan sends a TCP frame to a remote device with URG, ACK,RST,SYN and FIN flag set. FIN scans only with OS TCP/IP Developed according to RFC 793Now perform xmasscan,you need to create a new profile. Click profile ->New Profile Or command ctrl +p



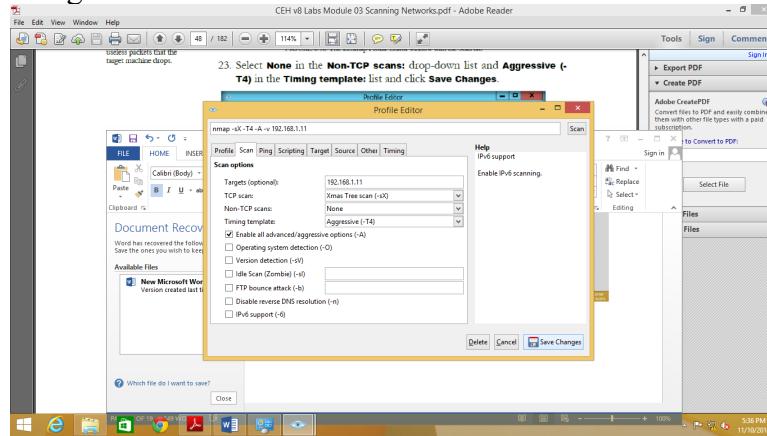
16. On the profile tab, enters scan ion the profile name text field.



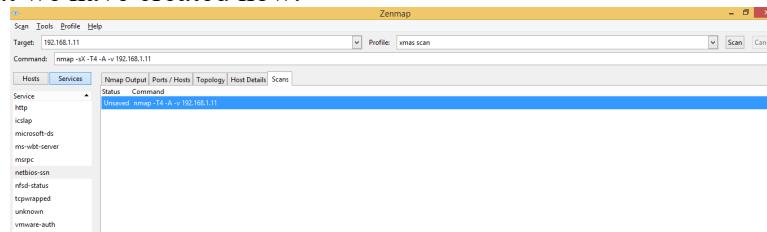
17. Click the scan tab and select Xmas tree Scan (-sx) from the TCP Scans:Drop Down



## 18. Save the changes



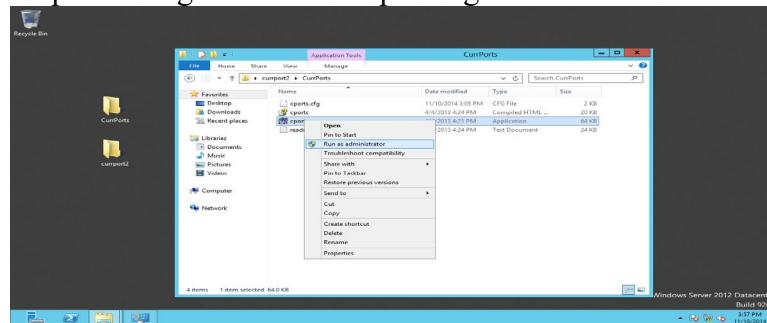
19. Now perform the same steps from 3 to 5 but select the xmas scan in profile drop down that we have created now.



To create different scan profile perform the steps 15 to 17

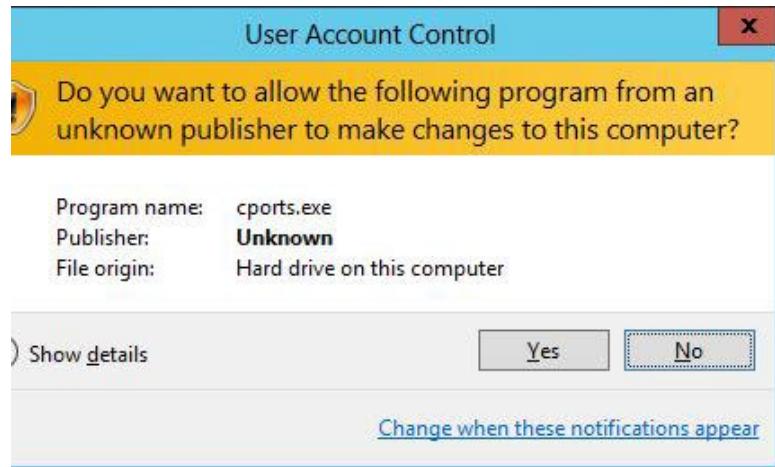
### 4) CurrPorts Tool

1. Launch Currports using administrator privileges



## Security Breaches and Countermeasures

2314041



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

Process Name	Process ID	Protocol	Local Port	Local Port Range	Local Address	Remote Port	Remote Port Range	Remote Address	Remote Host Name	State	Process Path	Product Name
EXPLORE.EXE	1516	TCP	40361		192.168.146.130	80		http	204.79.197.200	Established	C:\Program Files (x86)\Internet Explorer\EXPLORE.EXE	Windows® Internet Explorer
EXPLORE.EXE	610	UDP	61205			127.0.0.1				Listening	C:\Program Files (x86)\Internet Explorer\EXPLORE.EXE	Windows® Internet Explorer
System	636	TCP	135		epmap	0.0.0.1				Listening	C:\Program Files (x86)\Windows Resource Manager\epmap.exe	Windows®
System	4	TCP	139		netbios-ssn	0.0.0.1				Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	396	TCP	49152			0.0.0.0				Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	696	TCP	49153			0.0.0.0				Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	768	TCP	49154			0.0.0.0				Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	504	TCP	49155			0.0.0.0				Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	496	TCP	49156			0.0.0.0				Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	4	TCP	80		http	0.0.0.0				Listening	C:\Windows\system32\services\HTTP.dll	Windows®
System	4	TCP	443		microsoft-ds	0.0.0.0				Listening	C:\Windows\system32\services\HTTP.dll	Windows®
System	4	TCP	5005			0.0.0.0				Listening	C:\Windows\system32\services\HTTP.dll	Windows®
System	4	TCP	47001			0.0.0.0				Listening	C:\Windows\system32\services\HTTP.dll	Windows®
System	4	UDP	137		netbios-ns	192.168.146.130				Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	4	UDP	138		netbios-dgm	192.168.146.130				Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	900	UDP	5005			0.0.0.0				Listening	C:\Windows\system32\services\HTTP.dll	Windows®
System	900	UDP	49962			0.0.0.0				Listening	C:\Windows\system32\services\HTTP.dll	Windows®
System	4	TCP	80		http	=	=	=	=	Listening	C:\Windows\system32\services\HTTP.dll	Windows®
System	636	TCP	135		epmap	=	=	=	=	Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	4	TCP	443		microsoft-ds	=	=	=	=	Listening	C:\Windows\system32\services\HTTP.dll	Windows®
System	4	TCP	5005			=	=	=	=	Listening	C:\Windows\system32\services\HTTP.dll	Windows®
System	4	TCP	47001			=	=	=	=	Listening	C:\Windows\system32\services\HTTP.dll	Windows®
System	396	TCP	49152			=	=	=	=	Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	696	TCP	49153			=	=	=	=	Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	768	TCP	49154			=	=	=	=	Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	504	TCP	49155			=	=	=	=	Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	496	TCP	49156			=	=	=	=	Listening	C:\Windows\system32\services\NETLOGON.dll	Windows®
System	696	UDP	544		dhcpv4-client	f60:4409:d4...				Listening	C:\Windows\system32\services\DHCPV4.dll	Windows®
System	900	UDP	5355			0.0.0.0				Listening	C:\Windows\system32\services\DHCPV4.dll	Windows®
System	900	UDP	49962			=	=	=	=	Listening	C:\Windows\system32\services\HTTP.dll	Windows®

3. Curports lists all the processes and their 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.

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address	Remote Host Name	State	Process Path
IEXPLORE.EXE	1516	TCP	49259		192.168.146.130	80	http	204.79.197.200	Established	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	
IEXPLORE.EXE	1516	TCP	49261		192.168.146.130	80	http	204.79.197.200	Sent	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	
IEXPLORE.EXE	1516	UDP	61205		127.0.0.1					Listening	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
System	636	TCP	135	epmap	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	139	netbios-ssn	192.168.146.130			0.0.0.0		Listening	
System	396	TCP	49152		0.0.0.0			0.0.0.0		Listening	
System	696	TCP	49153		0.0.0.0			0.0.0.0		Listening	
System	768	TCP	49154		0.0.0.0			0.0.0.0		Listening	
System	504	TCP	49155		0.0.0.0			0.0.0.0		Listening	
System	496	TCP	49156		0.0.0.0			0.0.0.0		Listening	
System	4	TCP	80	http	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	445	microsoft-ds	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	5985		0.0.0.0			0.0.0.0		Listening	
System	4	TCP	47001		0.0.0.0			0.0.0.0		Listening	

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

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address	Remote Host Name	State	Process Path
IEXPLORE.EXE	1516	TCP	49259		192.168.146.130	80	http	204.79.197.200	Established	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	
IEXPLORE.EXE	1516	TCP	49261		192.168.146.130	80	http	204.79.197.200	Sent	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	
IEXPLORE.EXE	1516	UDP	61205		127.0.0.1					Listening	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
System	636	TCP	135	epmap	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	139	netbios-ssn	192.168.146.130			0.0.0.0		Listening	
System	396	TCP	49152		0.0.0.0			0.0.0.0		Listening	
System	696	TCP	49153		0.0.0.0			0.0.0.0		Listening	
System	768	TCP	49154		0.0.0.0			0.0.0.0		Listening	
System	504	TCP	49155		0.0.0.0			0.0.0.0		Listening	
System	496	TCP	49156		0.0.0.0			0.0.0.0		Listening	
System	4	TCP	80	http	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	445	microsoft-ds	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	5985		0.0.0.0			0.0.0.0		Listening	
System	4	TCP	47001		0.0.0.0			0.0.0.0		Listening	

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

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address	Remote Host Name	State	Process Path
IEXPLORE	1516	TCP	49259		192.168.146.130	80	http	204.79.197.200	Established	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	
IEXPLORE	1516	TCP	49261		192.168.146.130	80	http	204.79.197.200	Sent	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	
IEXPLORE	1516	UDP	61205		127.0.0.1					Listening	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
System	636	TCP	135	epmap	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	139	netbios-ssn	192.168.146.130			0.0.0.0		Listening	
System	396	TCP	49152		0.0.0.0			0.0.0.0		Listening	
System	696	TCP	49153		0.0.0.0			0.0.0.0		Listening	
System	768	TCP	49154		0.0.0.0			0.0.0.0		Listening	
System	504	TCP	49155		0.0.0.0			0.0.0.0		Listening	
System	496	TCP	49156		0.0.0.0			0.0.0.0		Listening	
System	4	TCP	80	http	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	445	microsoft-ds	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	5985		0.0.0.0			0.0.0.0		Listening	
System	4	TCP	47001		0.0.0.0			0.0.0.0		Listening	
System	4	UDP	137	netbios-ssn	192.168.146.130						
System	900	UDP	5355	linsec	0.0.0.0						
System	900	UDP	49962		0.0.0.0						
System	4	TCP	80	http	=	=	=	=	=	Listening	
System	4	TCP	138	epmap	=	=	=	=	=	Listening	
System	4	TCP	445	microsoft-ds	=	=	=	=	=	Listening	
System	4	TCP	5985		=	=	=	=	=	Listening	
System	4	TCP	47001		=	=	=	=	=	Listening	
System	4	UDP	137	netbios-ssn	192.168.146.130						
System	900	UDP	5355	linsec	=	=	=	=	=	Listening	
System	900	UDP	49962		=	=	=	=	=	Listening	

8. The selected reports automatically opens using the default browser

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address	Remote Host Name	State	Process Path
IEXPLORE.EXE	1516	TCP	49259		192.168.146.130	80	http	204.79.197.200	Established	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	
System	4	TCP	139	netbios-ssn	192.168.146.130			0.0.0.0		Listening	
System	496	TCP	49156		0.0.0.0			0.0.0.0		Listening	
System	4	UDP	138	netbios-dgm	192.168.146.130						
System	900	UDP	49962		0.0.0.0						
System	4	TCP	47001		=	=	=	=	=	Listening	

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

Local Port	Local Address	Remote Port	Remote Address	State	Process Path
49259	192.168.146.130	80	http	204.79.197.200	Established C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
139	netbios-ssn	192.168.146.130		0.0.0.0	Listening
49156		0.0.0.0		0.0.0.0	Listening
138	netbios-dgm	192.168.146.130		0.0.0.0	Listening
49962		0.0.0.0		0.0.0.0	Listening
47001		0.0.0.0		0.0.0.0	Listening

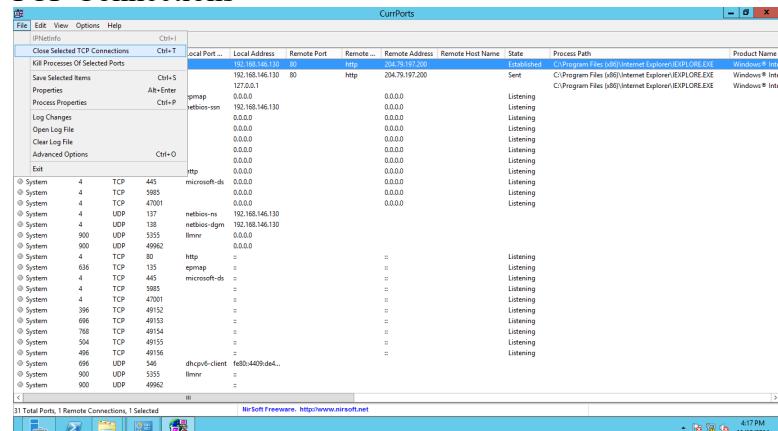
10. To view the properties of the port, select the port and click File -> Properties

Local Port	Local Address	Remote Port	Remote Address	Remote Host Name	State	Process Path	Product Name
49259	192.168.146.130	80	http	204.79.197.200	Sent	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	Windows® Internet Explorer
139	netbios-ssn	192.168.146.130		0.0.0.0	Listening	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	Windows® Internet Explorer
49156		0.0.0.0		0.0.0.0	Listening	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	Windows® Internet Explorer
138	netbios-dgm	192.168.146.130		0.0.0.0	Listening		
49962		0.0.0.0		0.0.0.0	Listening		
47001		0.0.0.0		0.0.0.0	Listening		

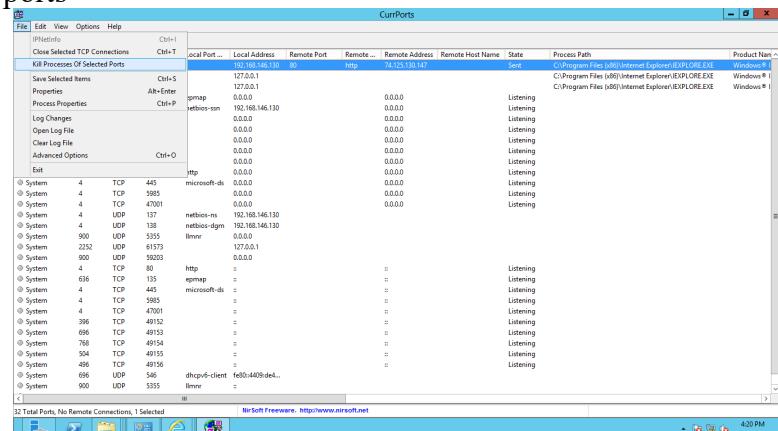
11. The properties window appears and displays all the properties for the selected port

<b>Process Name:</b>	IEXPLORE.EXE
<b>Process ID:</b>	1516
<b>Protocol:</b>	TCP
<b>Local Port:</b>	49259
<b>Local Port Name:</b>	
<b>Local Address:</b>	192.168.146.130
<b>Remote Port:</b>	80
<b>Remote Port Name:</b>	http
<b>Remote Address:</b>	204.79.197.200
<b>Remote Host Name:</b>	
<b>State:</b>	Established
<b>Process Path:</b>	C:\Program Files (x86)\Internet Explorer\IEXPLORE.E
<b>Product Name:</b>	Windows® Internet Explorer
<b>File Description:</b>	Internet Explorer
<b>File Version:</b>	10.00.9200.16384 (win8_rtm.120725-1247)
<b>Company:</b>	Microsoft Corporation
<b>Process Created On:</b>	11/10/2014 3:58:37 PM
<b>User Name:</b>	WIN-8UQH2RUDT7C\USER
<b>Process Services:</b>	
<b>Process Attributes:</b>	A
<b>Added On:</b>	11/10/2014 3:59:29 PM
<b>Module Filename:</b>	
<b>Remote IP Country:</b>	
<b>Window Title:</b>	Internet Explorer Enhanced Security Configuration is

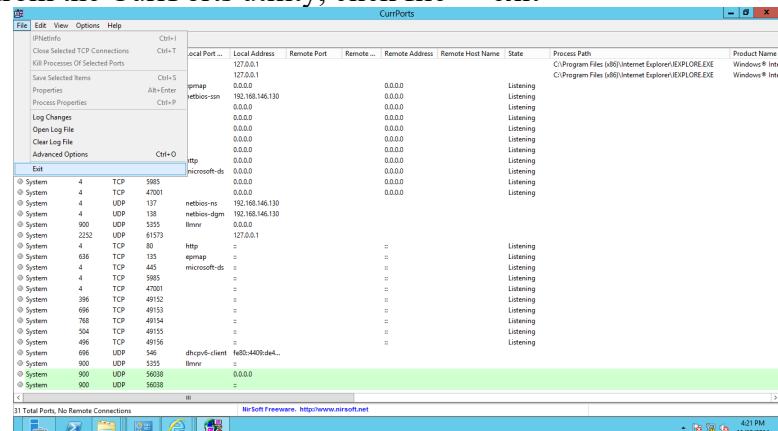
12. To close a TCP connection you think, select the process and click File -> Close Selected TCP Connections



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

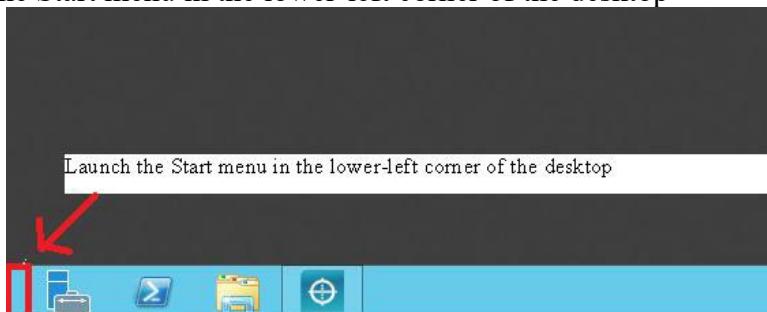


14. To exit from the CurrPorts utility, click file -> exit

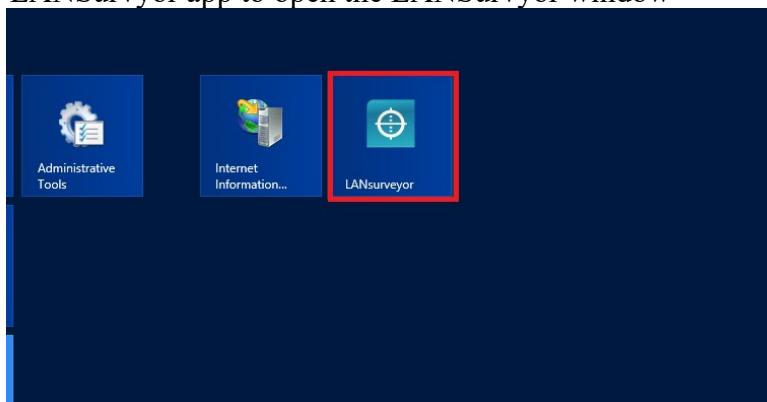


5) LANSurveyor

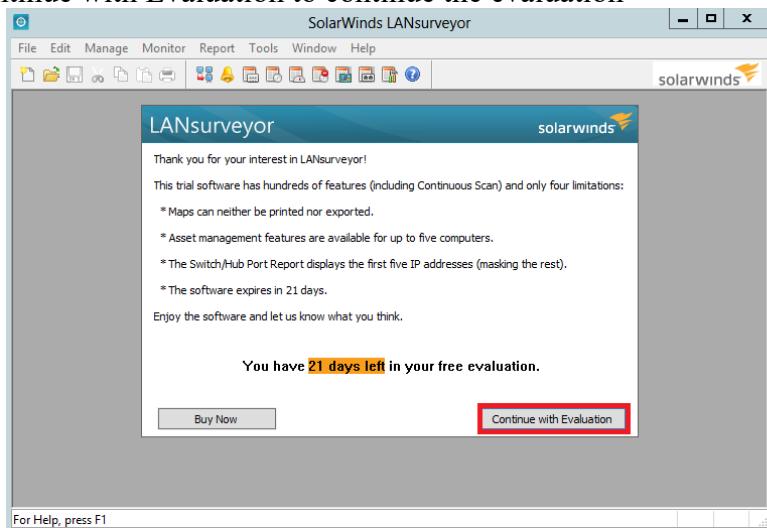
1. Launch the Start menu in the lower-left corner of the desktop



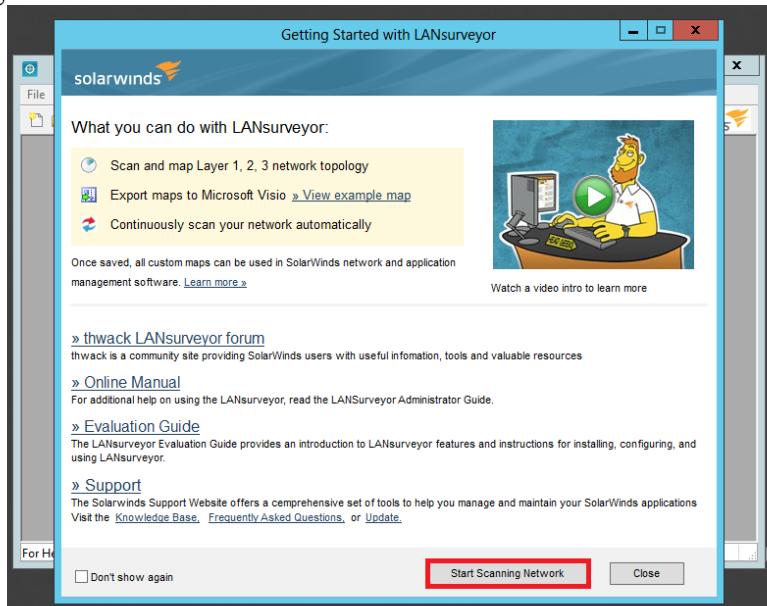
2. Click the LANSurveyor app to open the LANSurveyor window



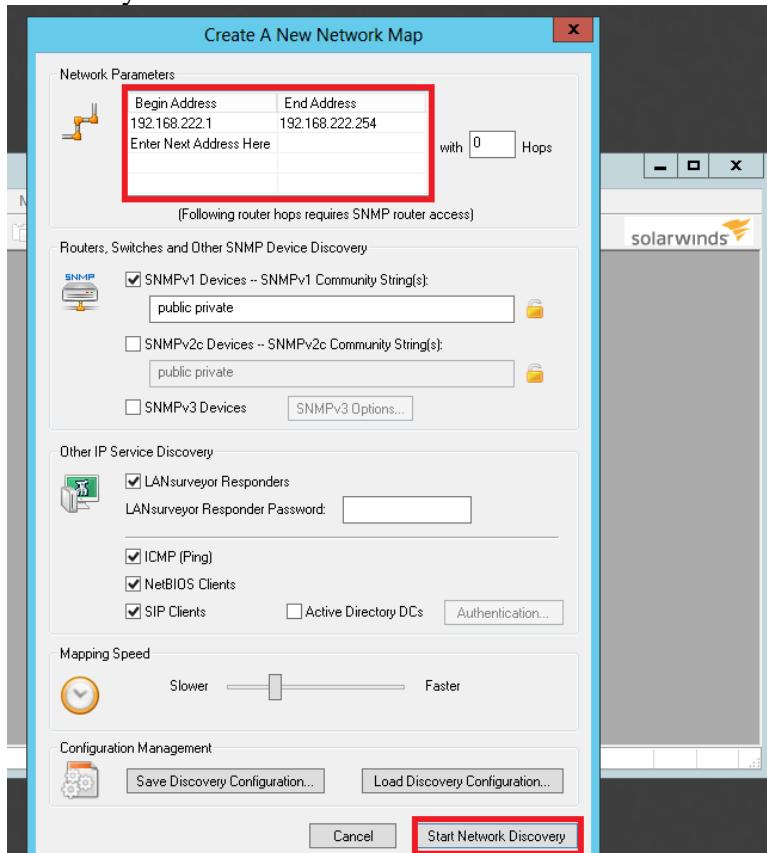
3. click Continue with Evaluation to continue the evaluation



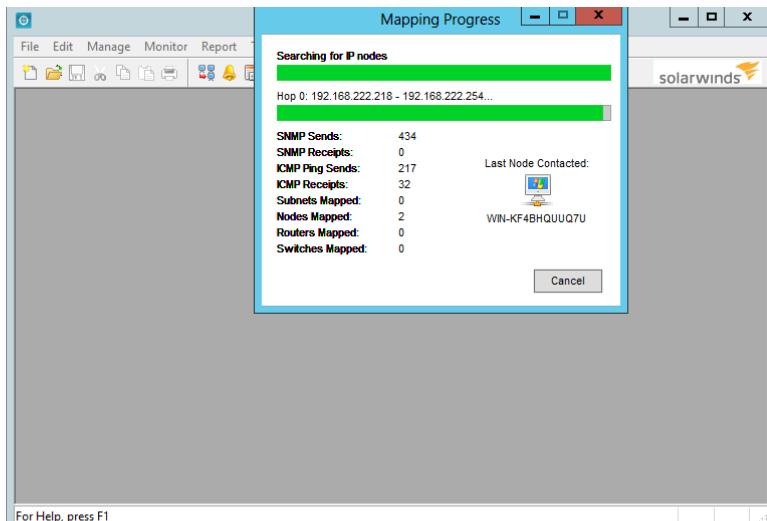
4. The Getting Started with LANsurveyor dialog box is displayed. Click Start Scanning Network



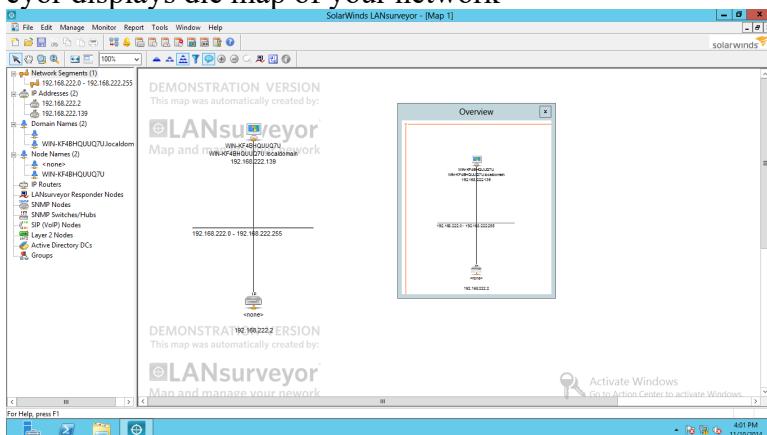
5. The Create A Network Map window will appear; in order to draw a network diagram enter the IP Address in Begin Address and End Address, and click Start Network Discovery.



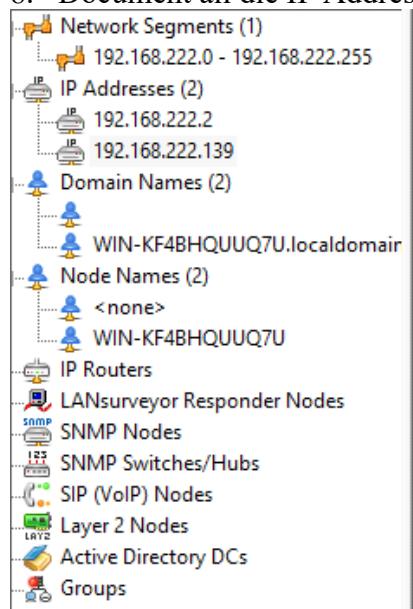
6. The entered IP Address mapping process will display as shown in the following figure



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

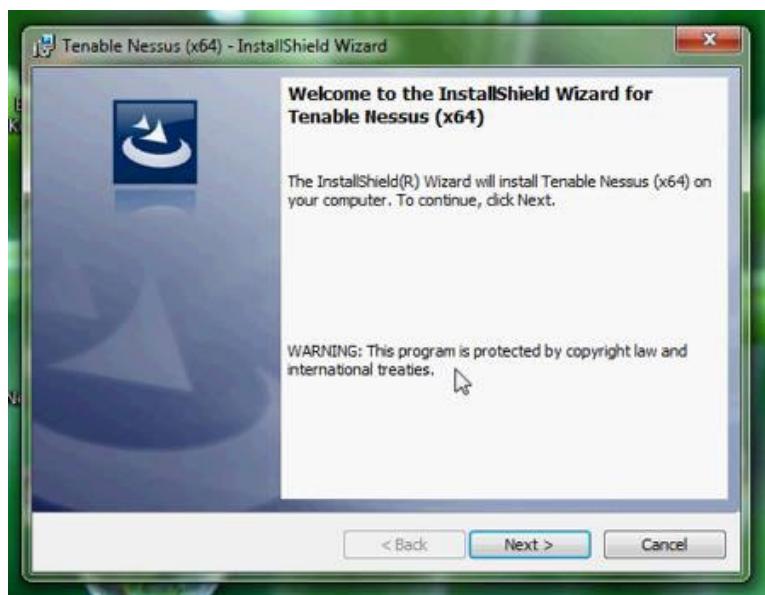
Node	Names	-	2
------	-------	---	---

6) Nessus

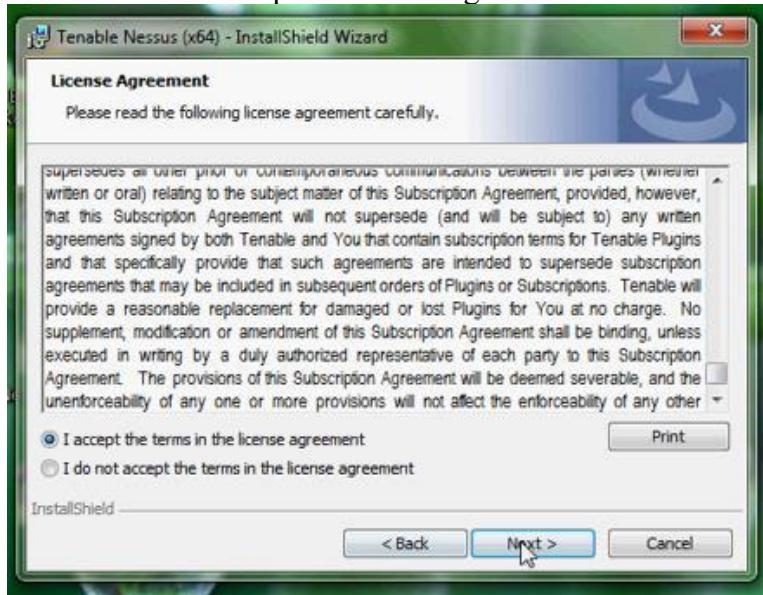
1. Double-click the Nessus-5.0.1-x86\_64.msi file.
2. The Open File - Security Warning window appears; click Run



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



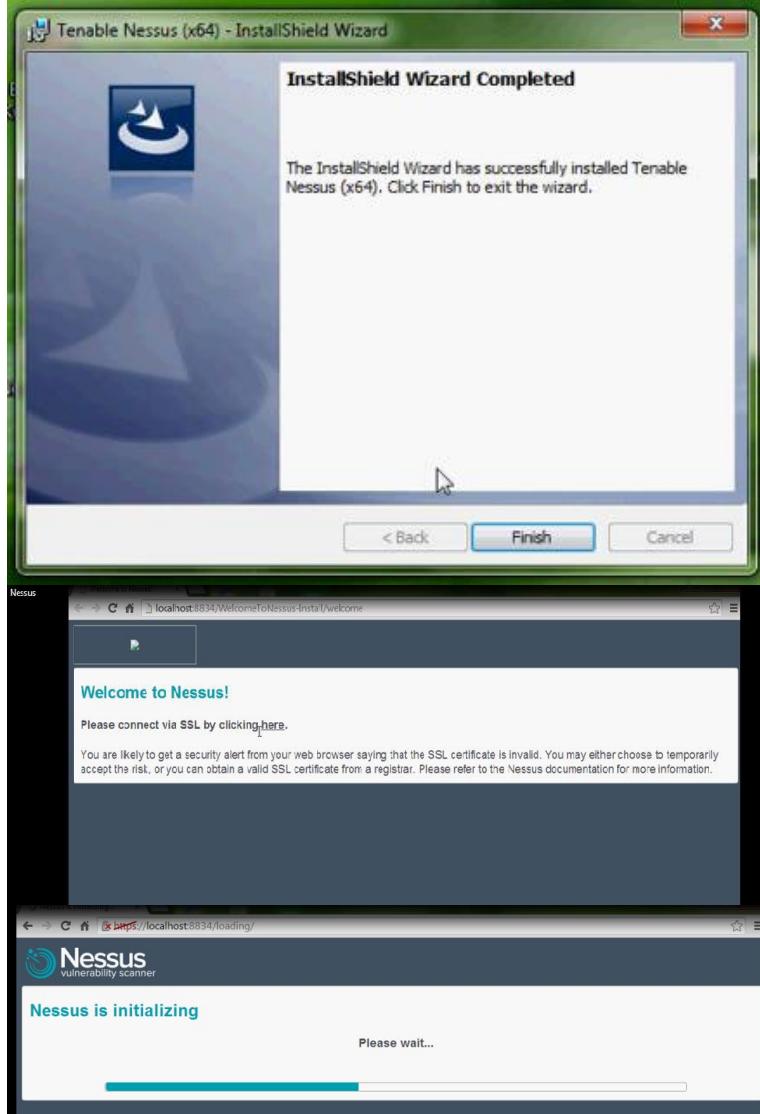
4. Before you begin installation, you must agree to the license agreement as shown in the following figure.
5. Select the radio button to accept the license agreement and click Next.



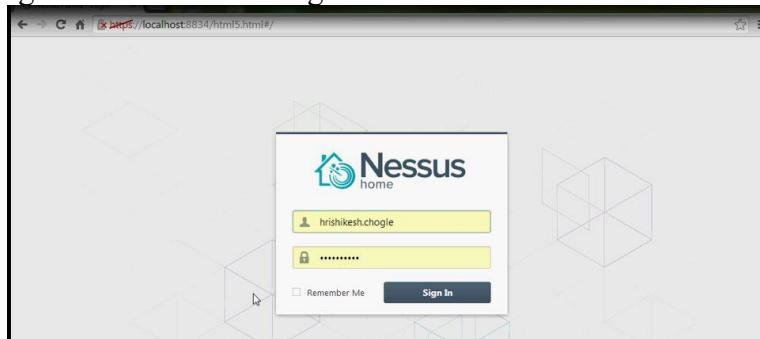
6. The Nessus wizard will prompt you to confirm the installation. Click Install.



7. Once installation is complete, click Finish



8. The Nessus Log In page appears. Enter the Username and Password given at the time of 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.

The image consists of three vertically stacked screenshots of the Nessus web interface, showing the steps to create a new policy:

- Screenshot 1:** Shows the 'Scans' page with a list of completed scans: 'my scan', 'Injectionscans', 'Essen', 'mumbai', 'gyan\_02', 'Gyan.com', and 'lestgetgyan'. A 'New Scan' button is visible on the left.
- Screenshot 2:** Shows the 'Policies' page with a 'Policy Wizards' modal open. It displays six policy templates: 'PCI Quarterly External Scan' (marked as 'Approved'), 'Host Discovery', 'Basic Network Scan', 'Credentialed Patch Audit', 'Windows Malware Scan', and 'Heartbleed & CCS Injection Detection'. A 'New Policy' button is visible on the left.
- Screenshot 3:** Shows the 'Policies / All Policies' page with the 'Policy Wizards' modal still open. The same six policy templates are shown. A 'New Policy' button is visible on the left.
- Screenshot 4:** Shows the 'Policies' page with the 'New Basic Network Scan Policy / Step 1 of 3' dialog open. The dialog title is 'Step 1 Define your policy name, description, and post-scan editing preferences'. It contains fields for 'Policy Name' (set to 'Basic Network scan'), 'Visibility' (set to 'private'), 'Description' (a placeholder text area), and 'Allow Post-Scan Report Editing' (checkbox checked). A 'Next' button is at the bottom.

# Security Breaches and Countermeasures

2314041

The screenshot shows two overlapping Nessus web interface windows.

The top window is titled "Policies" and shows "Step 2" of creating a "New Basic Network Scan Policy". It asks to choose the type of scan to configure, with "Scan type" set to "External". Below this are "Next" and "Cancel" buttons.

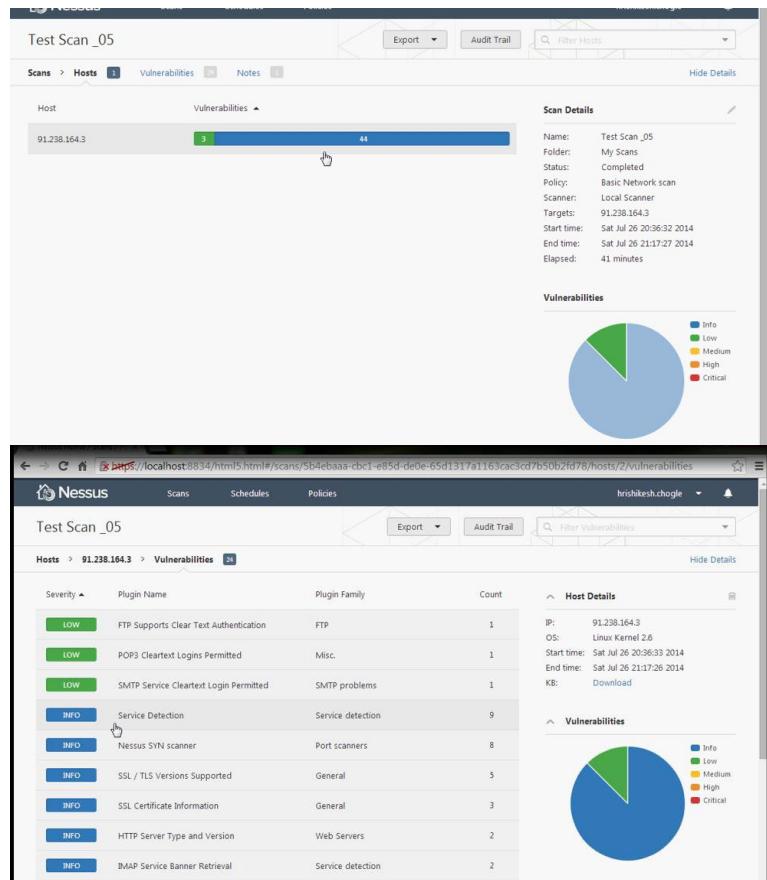
The bottom window is titled "Scans" and shows the "Scans / My Scans" list. It lists several completed scans: "my scan" (Completed), "Injectionscans" (Completed), "Essen" (Completed), "mumbai" (Completed), and "gyan 02" (Canceled). A new scan named "Test Scan \_05" is being configured in the "Basic Settings" section. The "Targets" field contains the IP address "91.238.164.3". Below the form are "Upload Targets" and "Add File" buttons, and "Launch" and "Cancel" buttons at the bottom.

10. The scan launches and starts scanning the network

The screenshot shows two overlapping Nessus web interface windows.

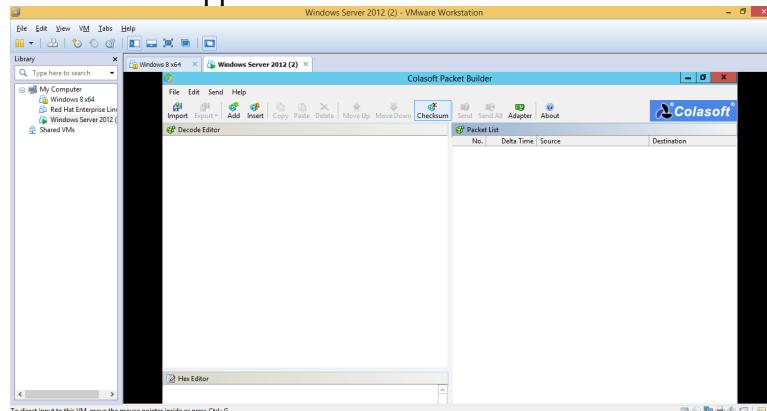
The top window is titled "Scans" and shows the "Scans / My Scans" list. It lists several scans: "Test Scan \_05" (Running), "my scan" (Completed), "Injectionscans" (Completed), "Essen" (Completed), "mumbai" (Completed), and "Gyan.com" (Aborted).

The bottom window is titled "Scans" and shows the "Scans / My Scans" list. It lists several completed scans: "Test Scan \_05" (Completed), "my scan" (Completed), "Injectionscans" (Completed), "Essen" (Completed), and "mumbai" (Completed).

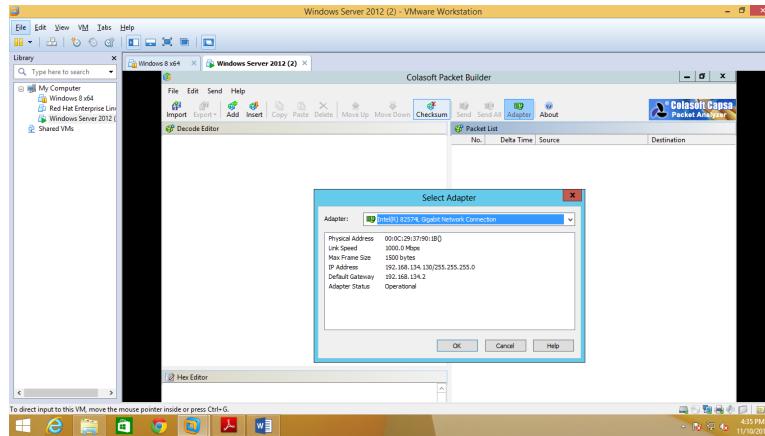


## 7) Colasoft Packet Builder

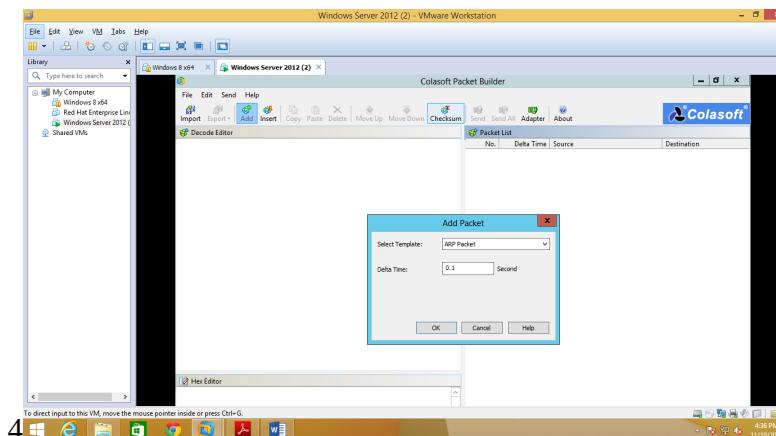
1. Install and Launch the Colasoft Packet Builder.
2. Colasoft main window appears



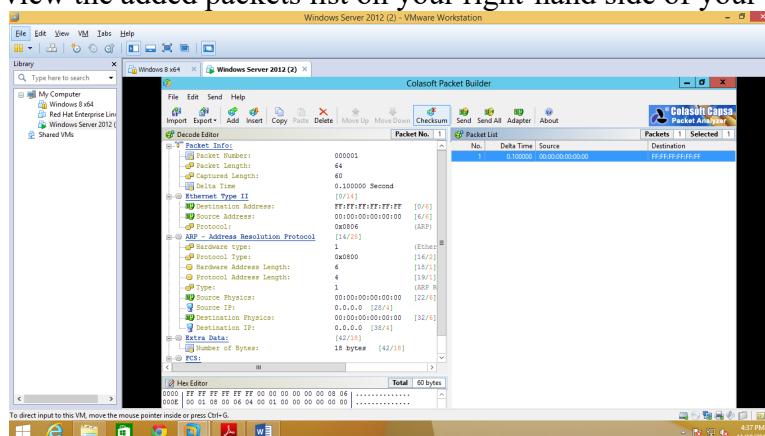
3. Before starting your task check that Adapter stings are set to Default and then click OK.



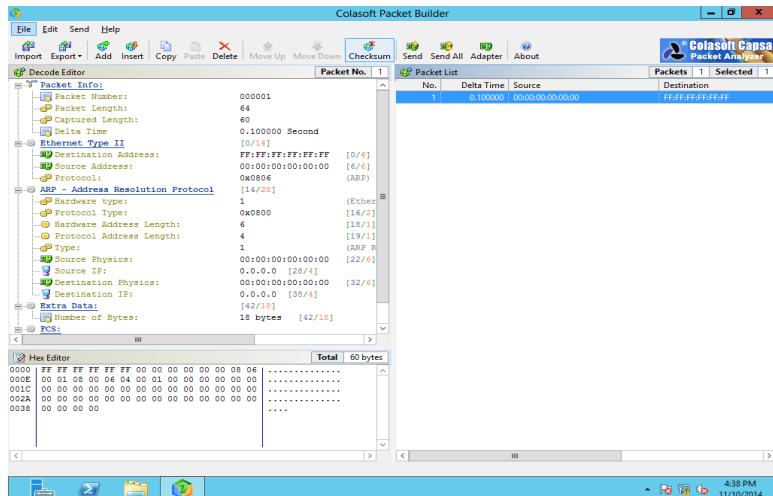
4. To add or create the packet, Click Add in the menu section.
5. When an Add Packet dialog box pops up, you need to select the template and click OK.



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



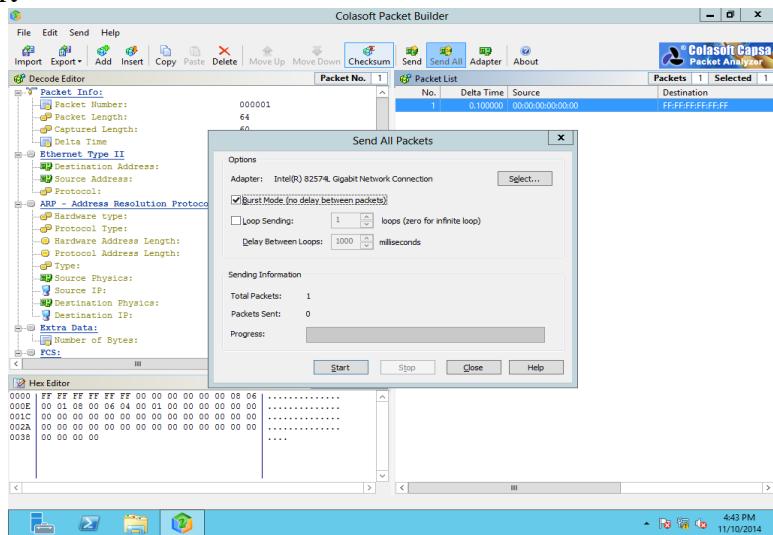
7. Colasoft Packet Builder allows you to edit the decoding information in the two editors: Decode Editor and Hex Editor.



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

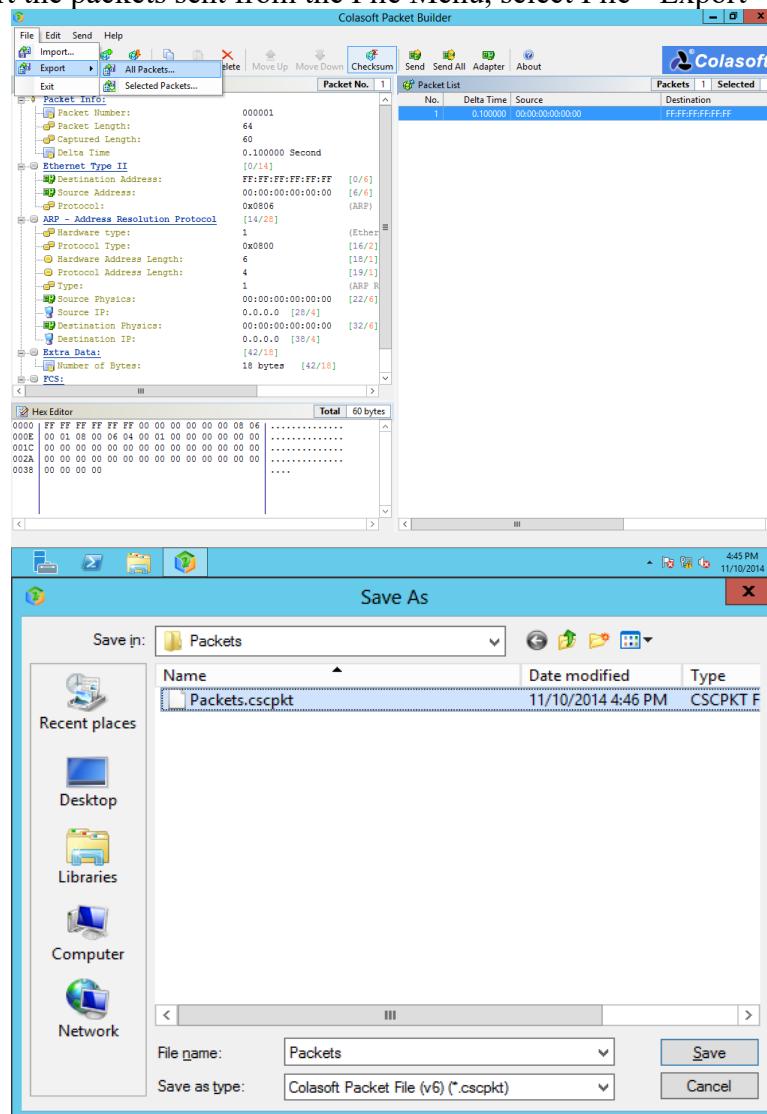


9. Check the Burst Mode option in the Send All Packets dialog window, and then click Start



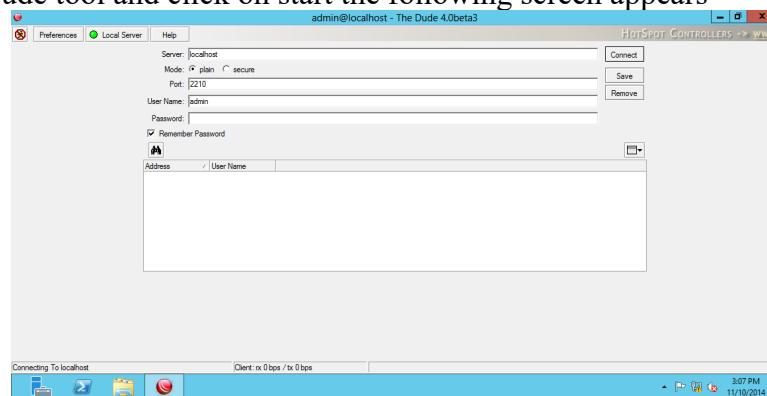
10. Click Start.

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

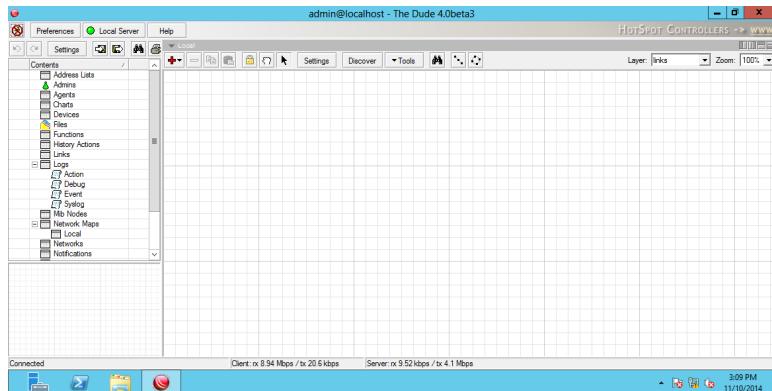


8) The Dude

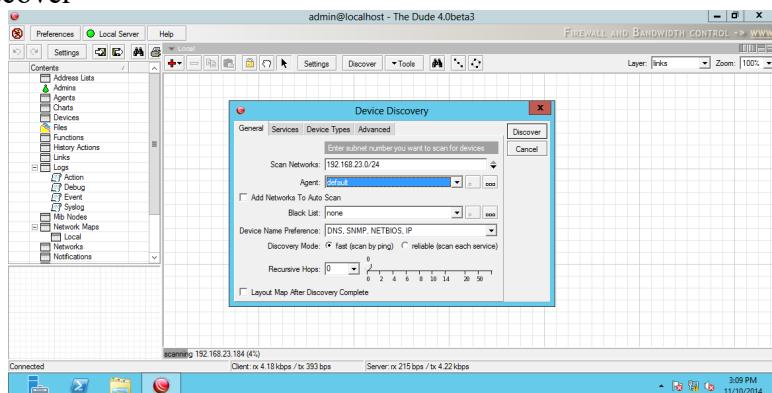
1. Install Dude tool and click on start the following screen appears



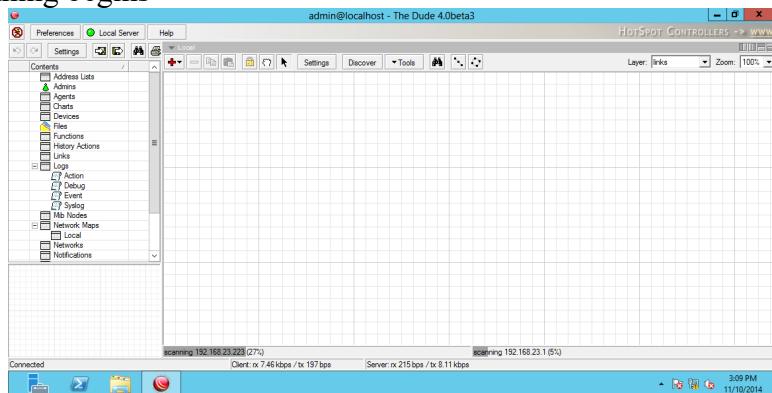
## 2. Click connect



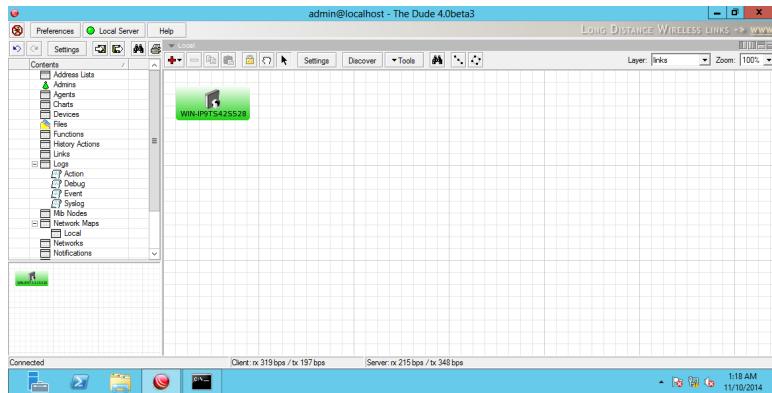
## 3. Click discover



## 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

The screenshot shows two windows of The Dude 4.0beta3 interface. The top window displays the 'History Actions' section, which lists five actions with their times and descriptions:

#	User	Action	Time
1	U	Network Map changed	01/03/27
2	U	Network Map Element changed	01/14/34
3	U	Network Map Element changed	01/22/11
4	U	Network Map Element changed	01/25/20
5	U	Network Map Element changed	01/27/00

The bottom window shows the 'File Manager' section, listing various files under the 'images' directory:

Name	Type	Size	Notes
certificate.pem	certificate	3406 B	
ap.svg	image	5.7 kB	
apple.svg	image	6.0 kB	
client.svg	image	4548 B	
clock.svg	image	3955 B	
file.svg	image	12.4 kB	
file_server.svg	image	7.4 kB	
globe.svg	image	31.2 kB	
globe2.svg	image	7.3 kB	
laptop.svg	image	3570 B	
mac.svg	image	5.1 kB	
laptop2.svg	image	4.9 kB	
news.svg	image	7.1 kB	
news.svg	image	3251 B	
news_server.svg	image	7.6 kB	
pc.svg	image	8.4 kB	
pc2.svg	image	5.7 kB	
pc2.svg	image	26.2 kB	
pc3.svg	image	13.1 kB	
printer.svg	image	7.5 kB	
printer2.svg	image	10.0 kB	
rack.svg	image	3743 B	
server.svg	image	9.2 kB	
router.svg	image	6.1 kB	
umb.svg	image	7.6 kB	

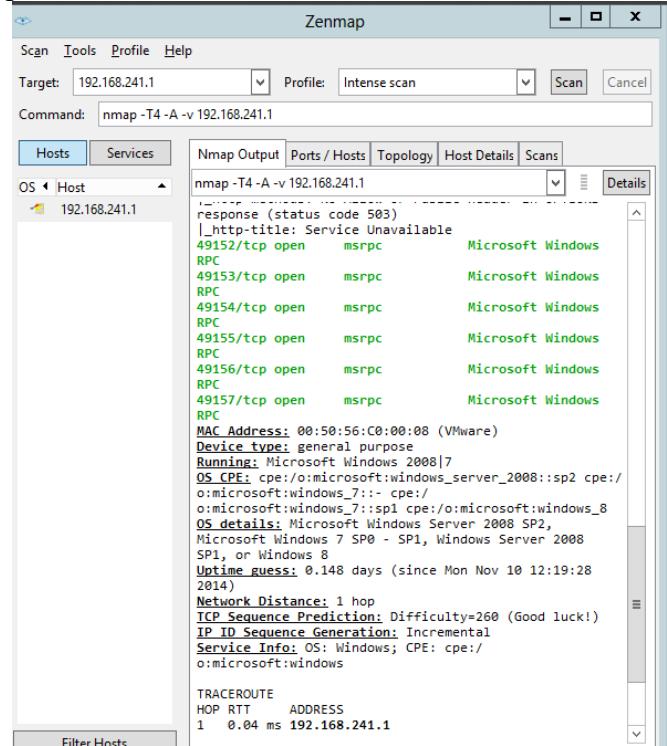
7. Once scanning is complete click “Disconnect button” to disconnect

## 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)

```

Administrator: Windows PowerShell
System error 67 has occurred.
The network name cannot be found.
PS C:\Users\Administrator> net use \\192.168.241.130\IPC$ ""/u:""
System error 67 has occurred.
The network name cannot be found.
PS C:\Users\Administrator> net use \\192.168.241.130\IPC$ ""/c:""
The option '/C:' is unknown.
The syntax of this command is:
NET USE
[devicename | *] [\\computername\sharename[\\volume] [password | *]]
[\\computername\sharename]
[\\computername\sharename\username]
[\\computername\username@domain name]
[\\computername\username@domain name]
[-SAVECREDS]
[-DELETE] [-PERSISTENT:{YES | NO}]
NET USE {devicename | *} [password | *] /HOME
NET USE [/PERSISTENT:{YES | NO}]
More help is available by typing NET HELPMSG 3506.
PS C:\Users\Administrator> nbtstat -A 192.168.241.130
New connections will be remembered.
There are no entries in the list.
PS C:\Users\Administrator> nbtstat -A 192.168.241.130
Ethernet0:
Node IpAddress: [192.168.241.130] Scope Id: []
NetBIOS Remote Machine Name Table
Name Type Status
WIN-D74RD43GBT<0> UNIQUE Registered
WIN-D74RD43GBT<2> UNIQUE Registered
WIN-D74RD43GBT<2> UNIQUE Registered
MAC Address = 00-0C-29-01-40-06
PS C:\Users\Administrator>

```

# Security Breaches and Countermeasures

2314041

Administrator: Windows PowerShell

```
[Ethernet0:  
Node IpAddress: [192.168.241.130] Scope Id: []  
          Host not found.  
PS C:\Users\Administrator> nbtstat -A 192.168.241.130  
  
Ethernet0:  
Node IpAddress: [192.168.241.130] Scope Id: []  
          NetBIOS Remote Machine Name Table  
  
          Name           Type            Status  
WIN-D74RD43G8T<0>  UNIQUE          Registered  
WORKGROUP<0>          GROUP          Registered  
WIN-D74RD43G8T<2>  UNIQUE          Registered  
  
MAC Address = 00-0C-29-D1-4D-06  
  
PS C:\Users\Administrator> net use \\192.168.241.130\IPC$ ""/u:""  
System error 67 has occurred.  
The network name cannot be found.  
PS C:\Users\Administrator> net use \\192.168.241.130\IPC$ ""/u:""  
System error 67 has occurred.  
The network name cannot be found.  
PS C:\Users\Administrator> net use \\192.168.241.130\IPC$ ""/c:""  
The option '/c' is unknown.  
The syntax of this command is:  
  
NET USE  
[deviceName | +] [\computerName\shareName[\volume] [password | *]]  
[PERSISTENT:{YES | NO}]  
[USER:{dotNetUserName} |  
[USER:{username}@dotNetDomainName} |  
[USER:{username}@dotNetDomainName} |  
[SMARTCARD] |  
[SAVCRED])  
[DELETE] | [/PERSISTENT:{YES | NO}]]  
  
NET USE [deviceName | +] [password | *] /HOME  
NET USE [/PERSISTENT:{YES | NO}]  
More help is available by typing NET HELPMSG 3506.  
PS C:\Users\Administrator>  
  
Activate Windows  
Go to Action Center to activate  
Windows  
Windows Server 2012 Datacenter  
Build 9200  
  
Recycle      D      F      E      S      R      C      L      W      X  
4:15 PM 11/10/2014  
  
Administrator: Windows PowerShell

```
Ethernet0:  
Node IpAddress: [192.168.241.130] Scope Id: []  
          NetBIOS Remote Machine Name Table  
  
          Name           Type            Status  
WIN-D74RD43G8T<0>  UNIQUE          Registered  
WORKGROUP<0>          GROUP          Registered  
WIN-D74RD43G8T<2>  UNIQUE          Registered  
  
MAC Address = 00-0C-29-D1-4D-06  
  
PS C:\Users\Administrator> net use \\192.168.241.130\IPC$ ""/u:""  
System error 67 has occurred.  
The network name cannot be found.  
PS C:\Users\Administrator> net use \\192.168.241.130\IPC$ ""/u:""  
System error 67 has occurred.  
The network name cannot be found.  
PS C:\Users\Administrator> net use \\192.168.241.130\IPC$ ""/c:""  
The option '/c' is unknown.  
The syntax of this command is:  
  
NET USE  
[deviceName | +] [\computerName\shareName[\volume] [password | *]]  
[PERSISTENT:{YES | NO}]  
[USER:{dotNetUserName} |  
[USER:{username}@dotNetDomainName} |  
[USER:{username}@dotNetDomainName} |  
[SMARTCARD] |  
[SAVCRED])  
[DELETE] | [/PERSISTENT:{YES | NO}]]  
  
NET USE [deviceName | +] [password | *] /HOME  
NET USE [/PERSISTENT:{YES | NO}]  
More help is available by typing NET HELPMSG 3506.  
PS C:\Users\Administrator> net use  
New connections will be remembered.  
There are no entries in the list.  
PS C:\Users\Administrator>
```

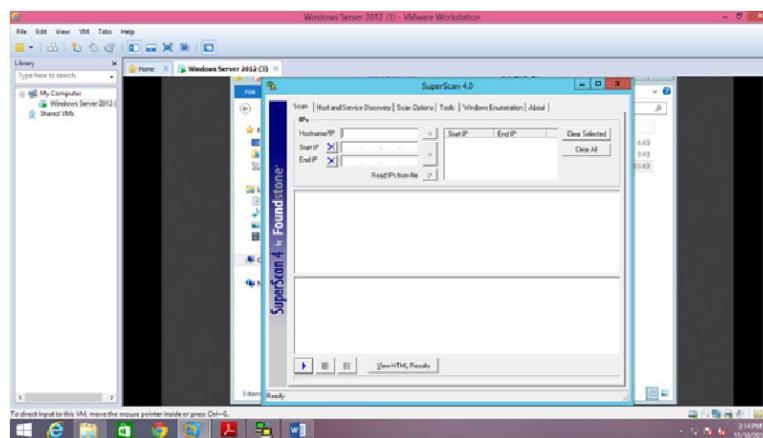


Activate Windows  
Go to Action Center to activate  
Windows  
Windows Server 2012 Datacenter  
Build 9200  
4:16 PM 11/10/2014

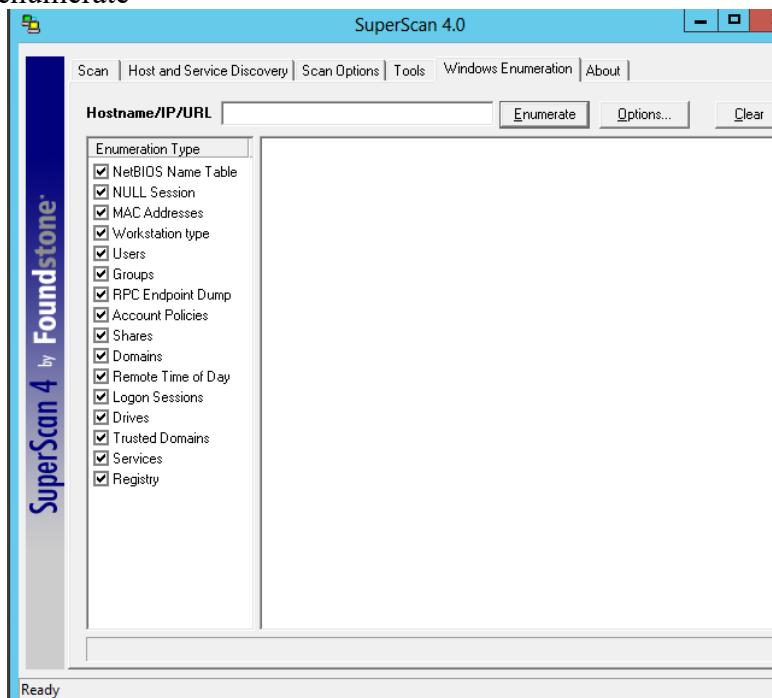

```

## 2) SuperScan

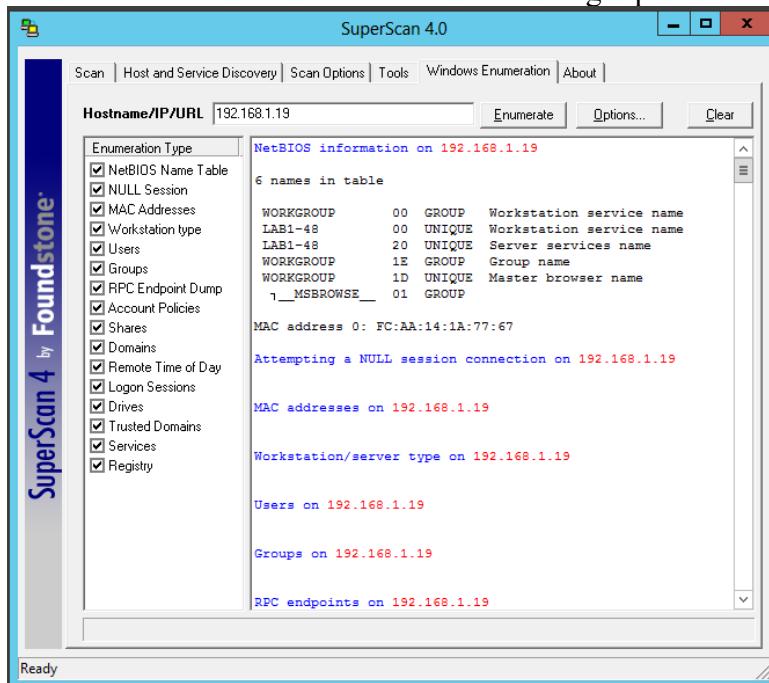
1. Launch SuperScan
  2. Click on windows Enumeration tab located on top menu



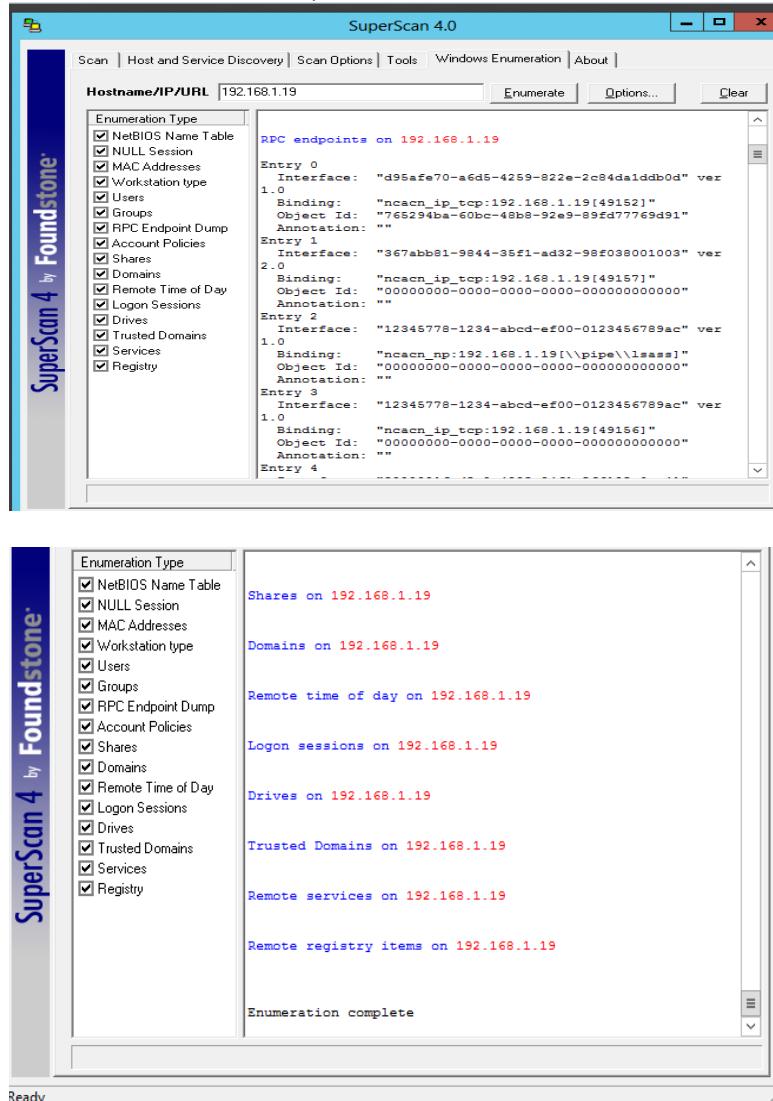
3. Enter host name IP Address of target machine, check the type of enumeration, and click on enumerate



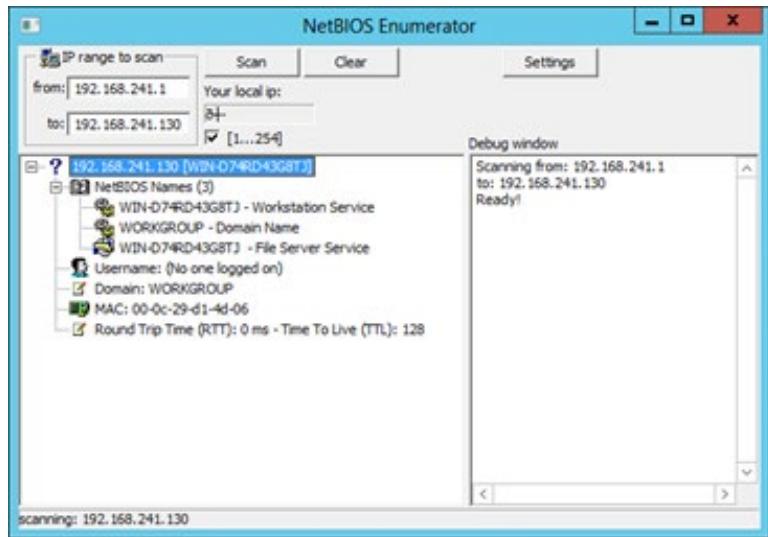
4. SuperScan enumerates and the result is shown in the right pane of the window



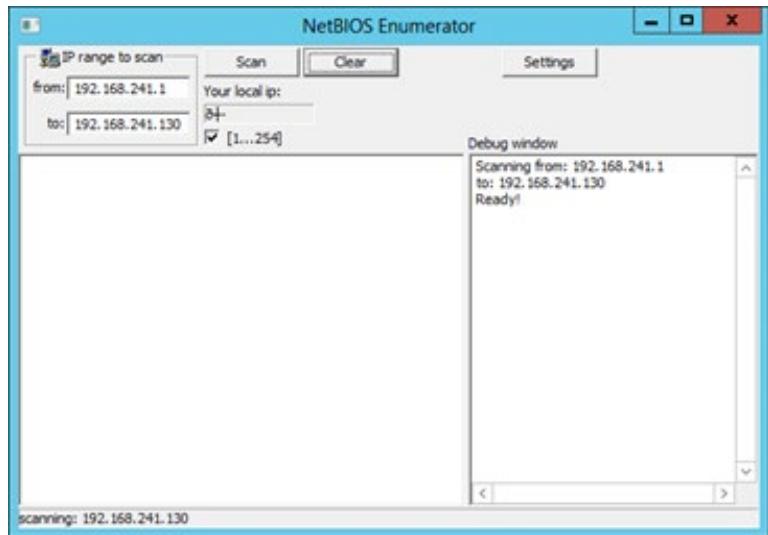
5. To perform the new enumeration, click on clear and start new one



- 3) NetBIOS Enumerator Tool
  1. Launch NetBIOS enumerator
  2. In the IP range to scan enter the IP range
  3. Click scan

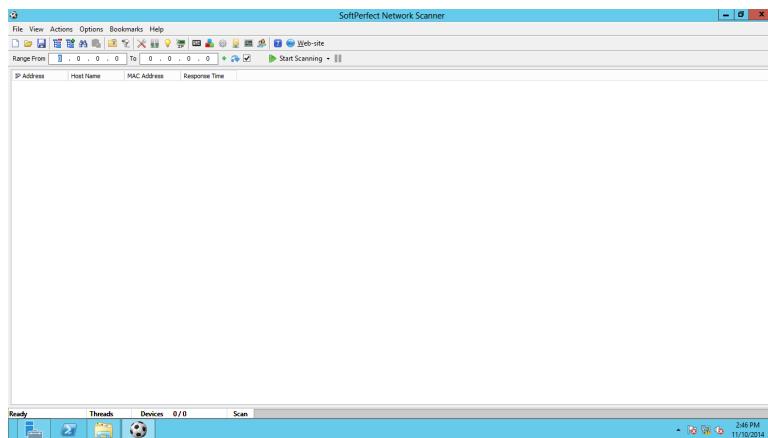


4. To perform the new scan click clear



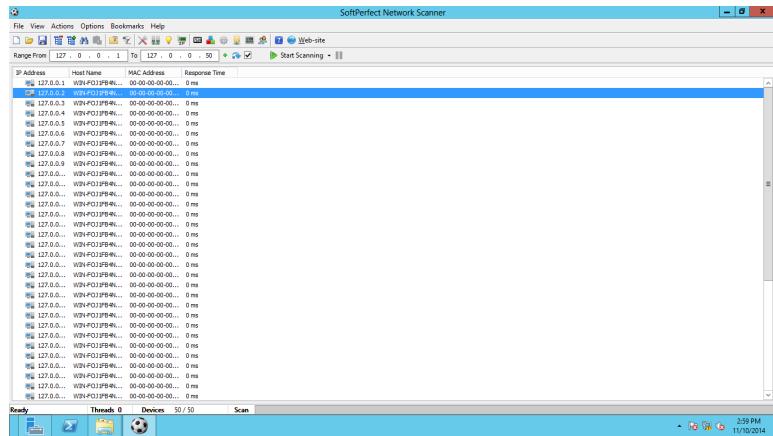
4) SoftPerfect Network Scanner

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



## Security Breaches and Countermeasures

2314041



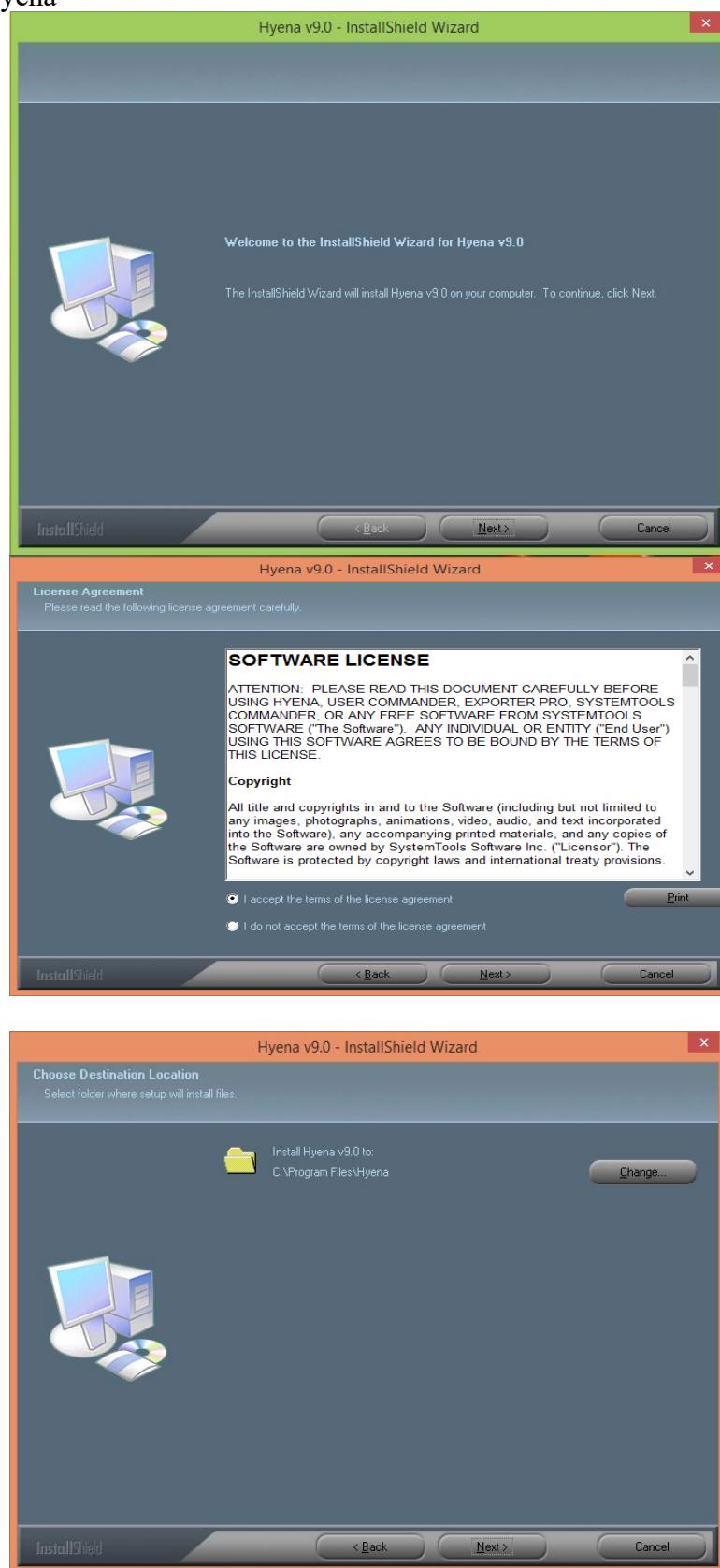
3. To view the properties of the individual IP Address, right click that IP Address and select the properties

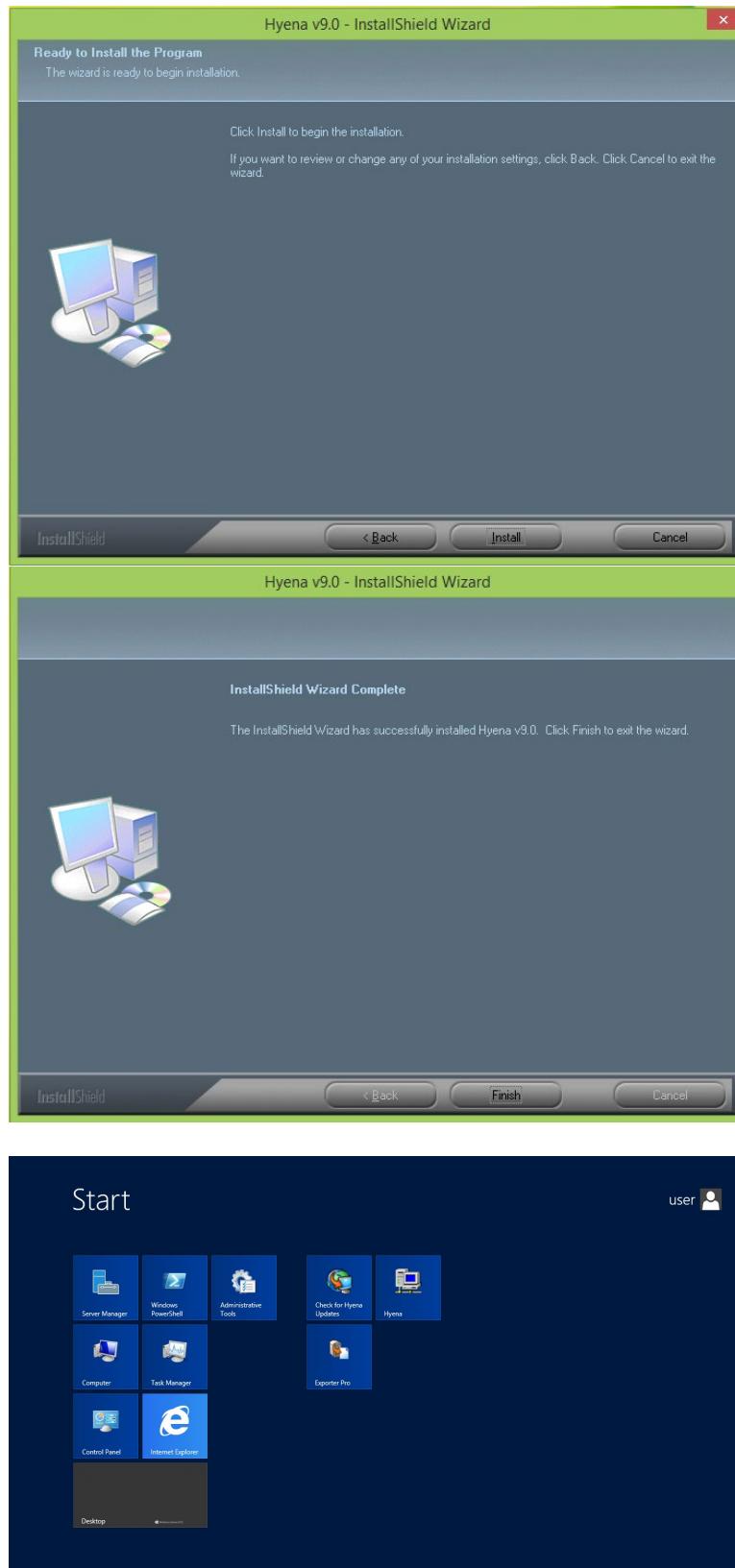
The 'Properties' dialog box displays the following information:

Basic Info	Value
IP Address	127.0.0.3
Host Name	WIN-FOJ1FB4NMB
MAC Address	00-00-00-00-00-00
Response Time	0 ms

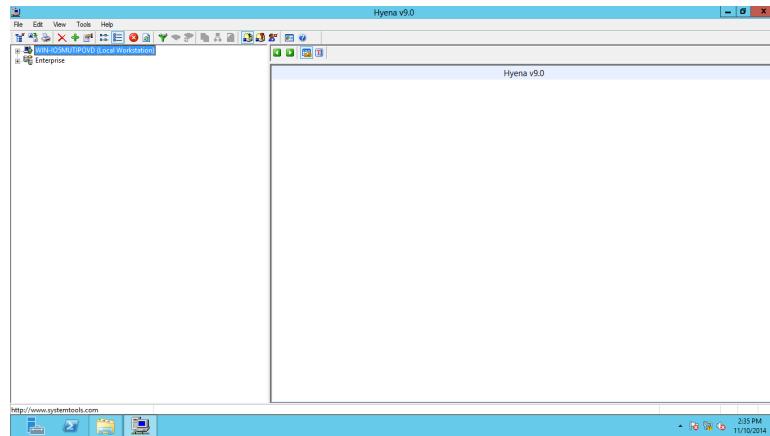
## 5) Hyena

## 1. Install Hyena

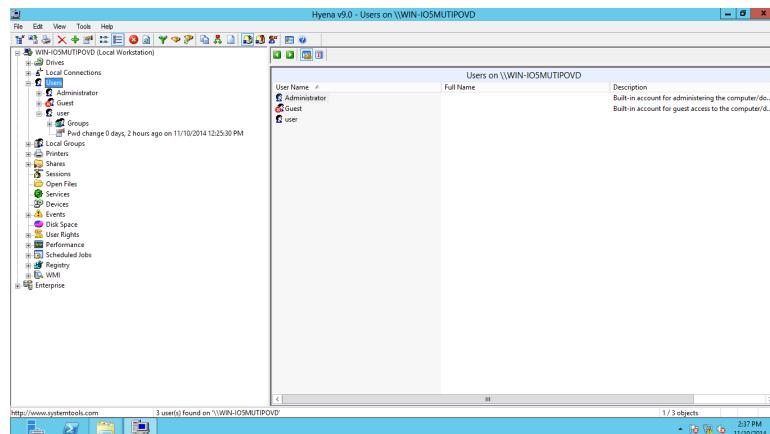




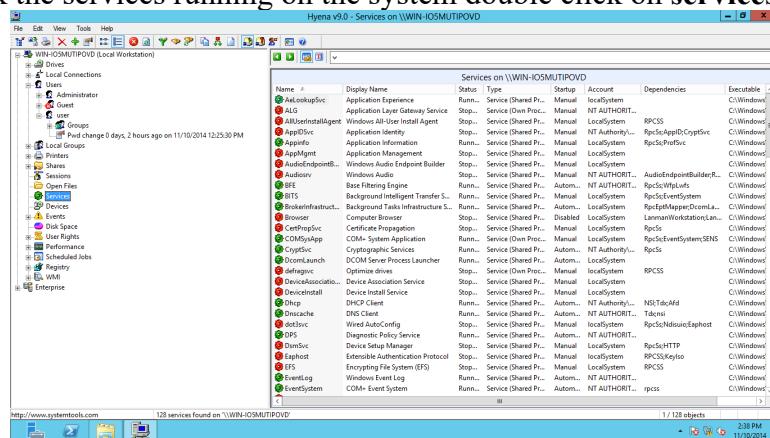
2. The registration window will appear, click ok to continue
3. The main window of hyena is shown below



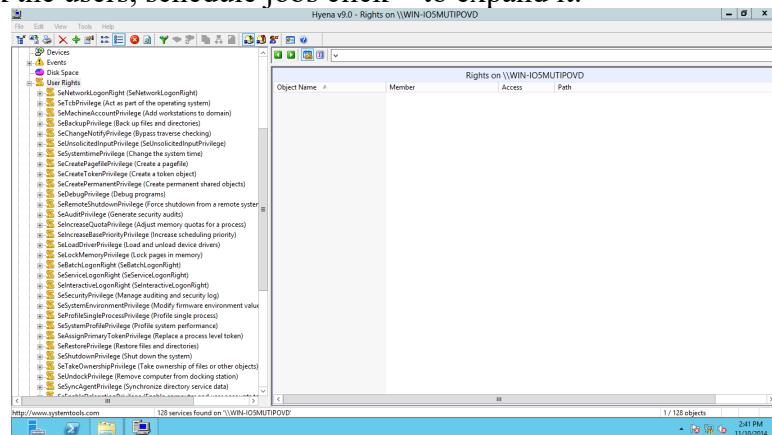
4. Click + to expand the local work station and click Users.



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

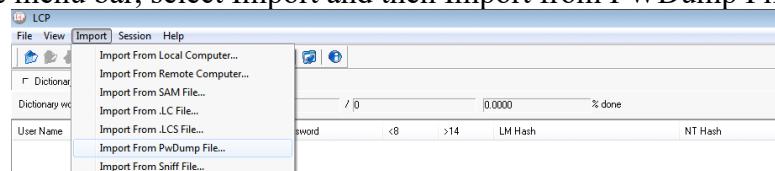
1. Extract the SAM Hashes by using PwDump7 program
2. Pwdump7.exe > password.txt

```
C:\Users\Admin\Desktop\EHPracs_Final\CEH\Prac4\pwdump7>pwdump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

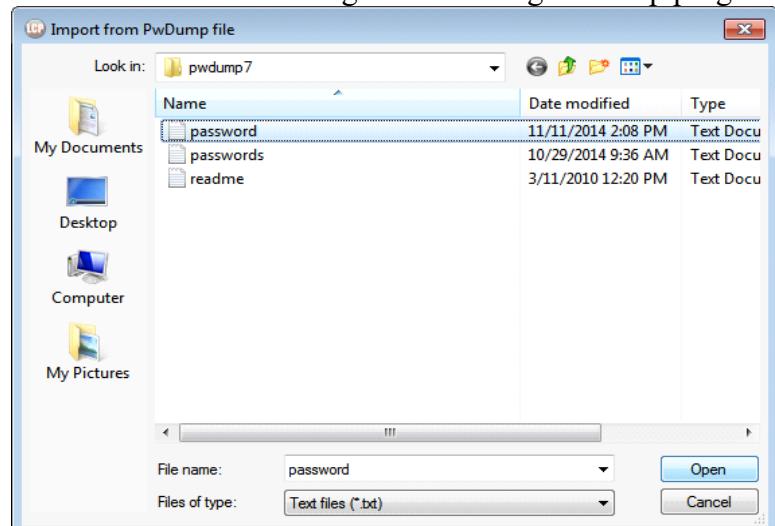
Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C08
PC0:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::
Admin:1000:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::
EH:1004:NO PASSWORD*****:2A21990FC0D3D759941E45C490F143D5F:::

C:\Users\Admin\Desktop\EHPracs_Final\CEH\Prac4\pwdump7>pwdump7.exe>password.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es
```

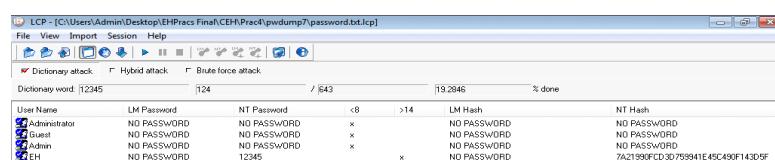
3. This PWDump file will be used for many programs in this practical
4. From the menu bar, select Import and then Import from PWDump File.



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

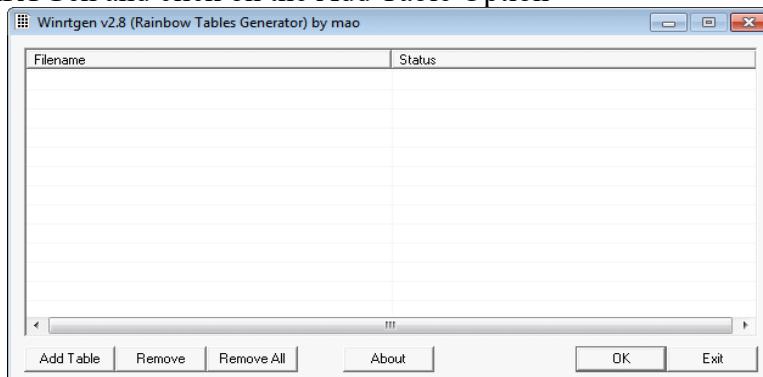


6. After opening the file, hit the play button in LCP window to start cracking the SAM Hashes

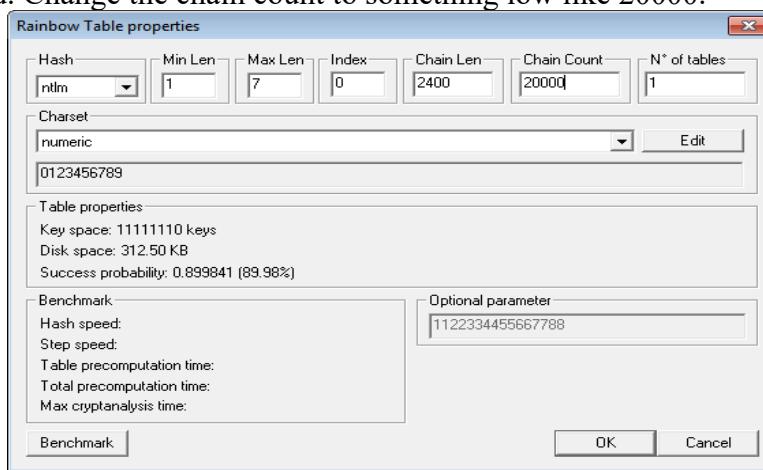


2) RainbowCrack and WinRTGen

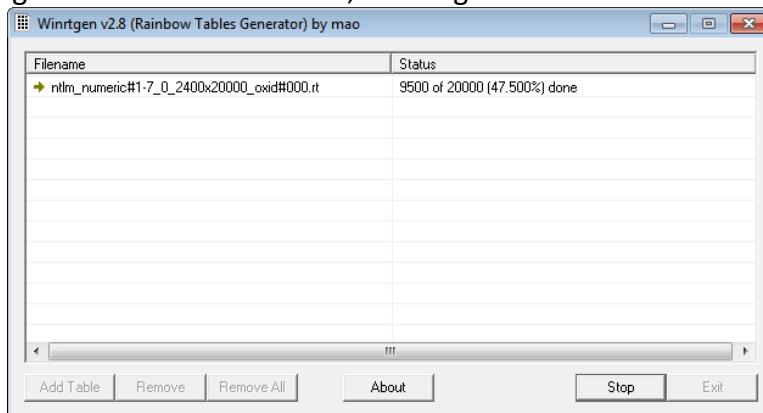
1. Run WinRTGen and click on the Add Table Option



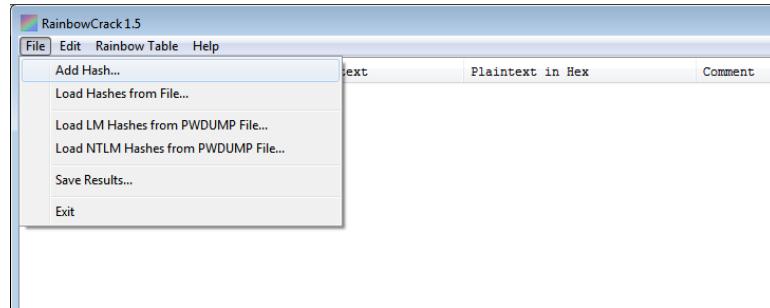
2. Select the Hash to target, the minimum and maximum length of the guessed password. Change the chain count to something low like 20000.



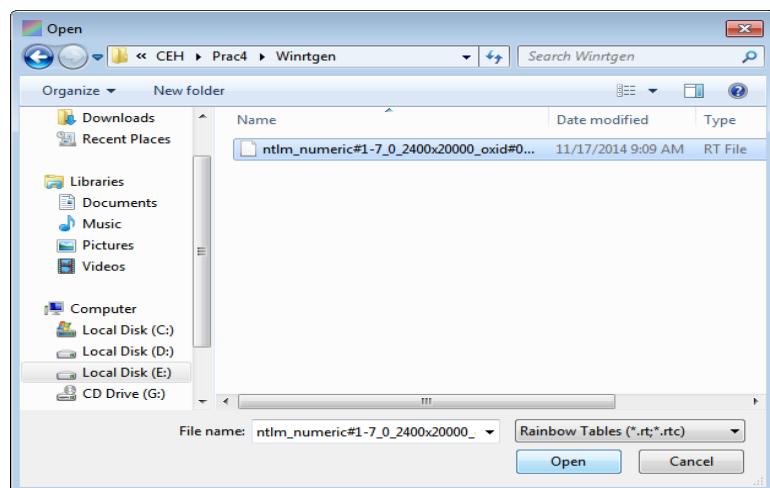
3. You can choose the charset to use. Numeric will only generate a RT of numeric passwords.  
4. Click on OK and click on OK at the next screen to start generating the RT. Depending on the chain count used, the RT generation can take some time.



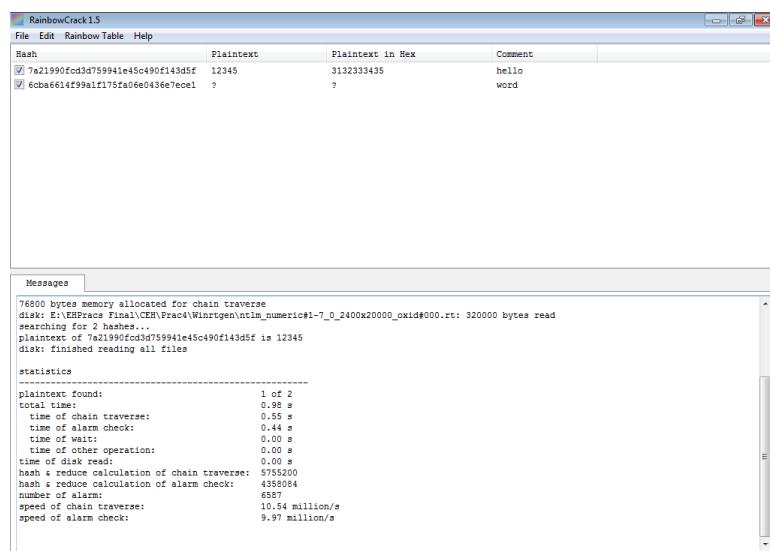
5. Run rcrack\_gui.exe to run RainbowCrack  
6. Go to File -> Load Hashes from PWdump file



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

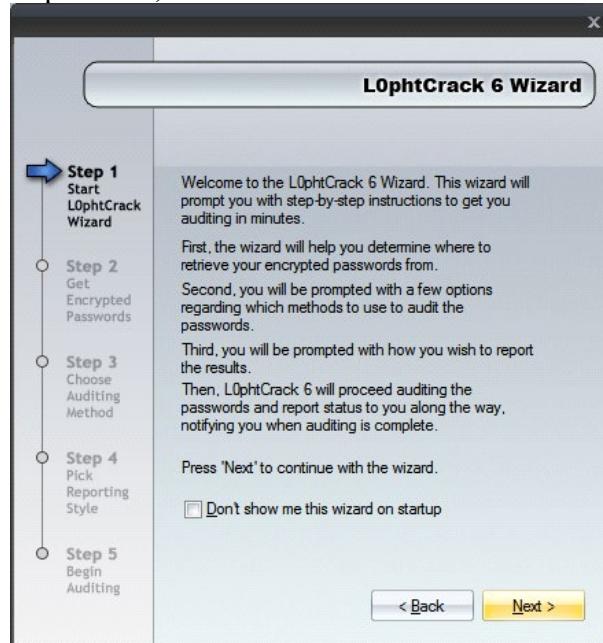


9. It will then crack the password using the Rainbow Table and show the passwords in plaintext

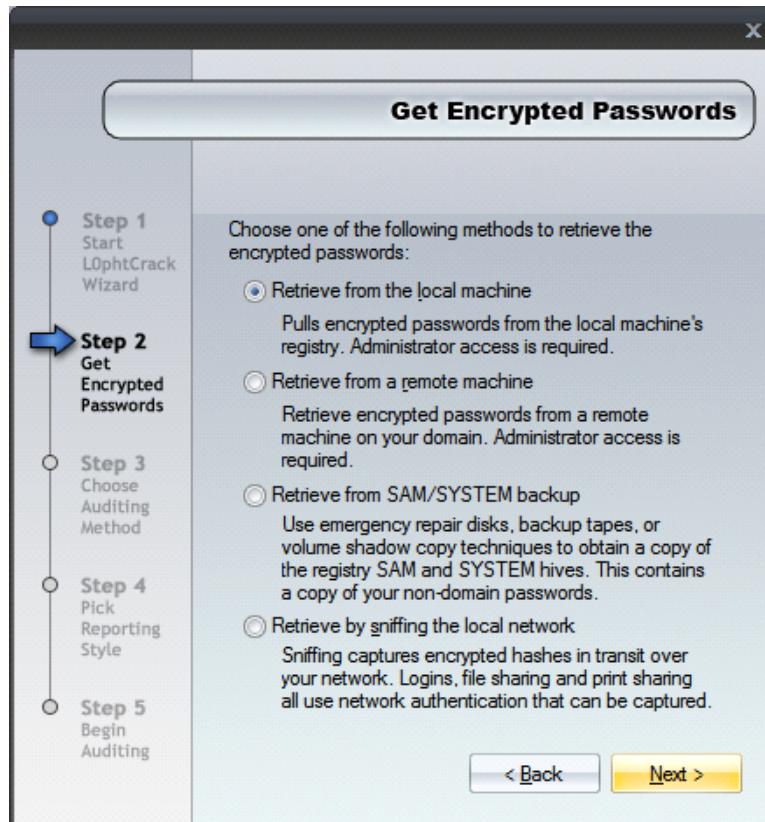


3) L0pthCrack

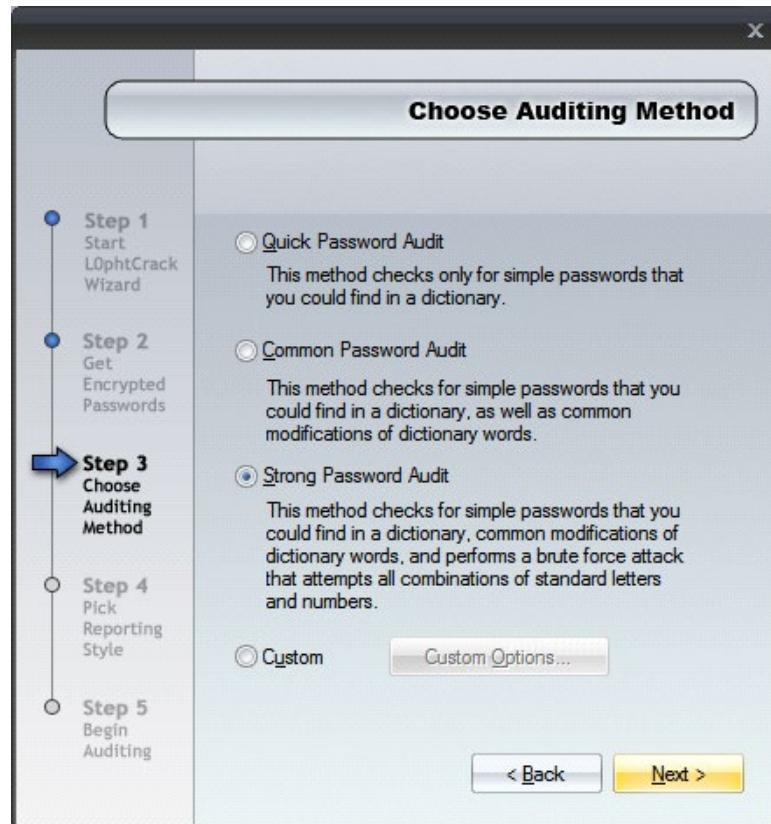
- When you start L0phcrack, the wizard will run



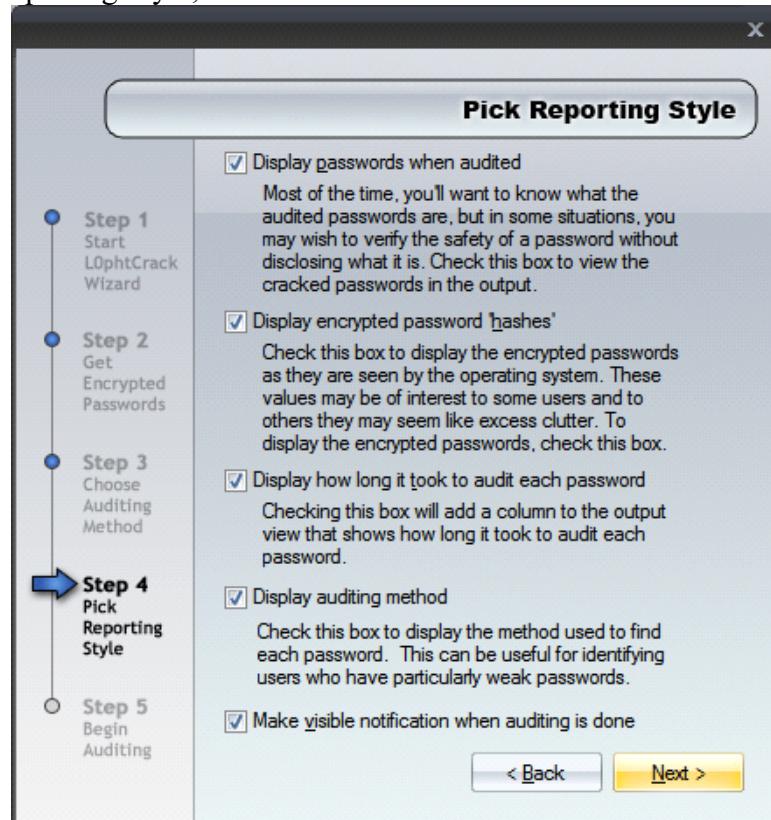
- Choose Retrieve from the local machine in the Get Encrypted Passwords wizard and click Next



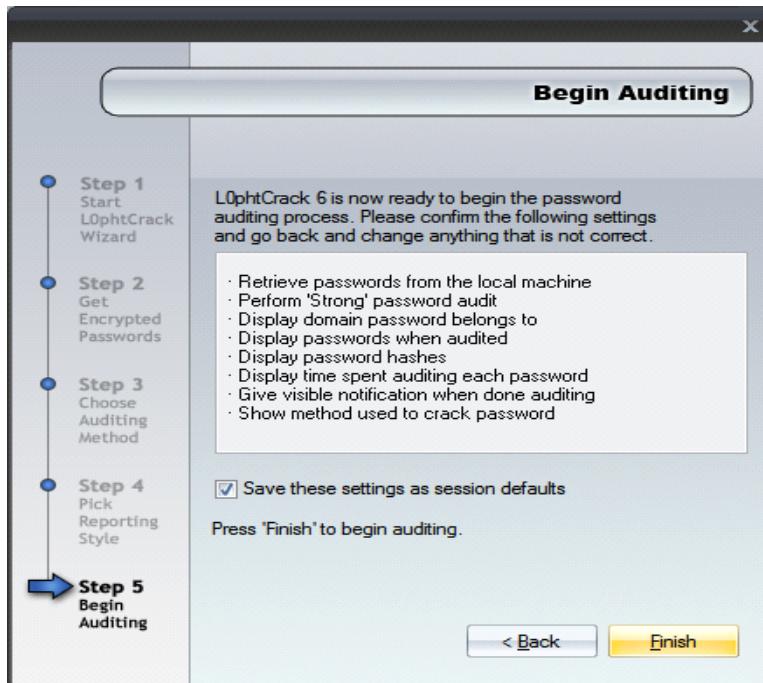
- Choose Strong Password Audit from the Choose Auditing Method wizard and click Next



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

Domain	User Name	LM Password	c8	Password	LM Hash	NTLM Hash
	Administrator			* empty *		31D6CFED016AE931B
	Guest			* empty *		31D6CFED016AE931B
	Admin					7A21990FC03D759941
	EH					

To begin, import hashes to retrieve accounts to audit.

Session Options

Statistics

DIGEST/HYBRID

PRECOMPUTED

BRUTE FORCE

SUMMARY

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

Domain	User Name	LM Password	c8	Password	LM Hash	NTLM Hash
	Admin			* empty *		31D6CFED016AE931B
	Administrator			* empty *		31D6CFED016AE931B
	EH			12345		7A21990FC03D759941
	Guest					

L0phtCrack 6

Audit completed.

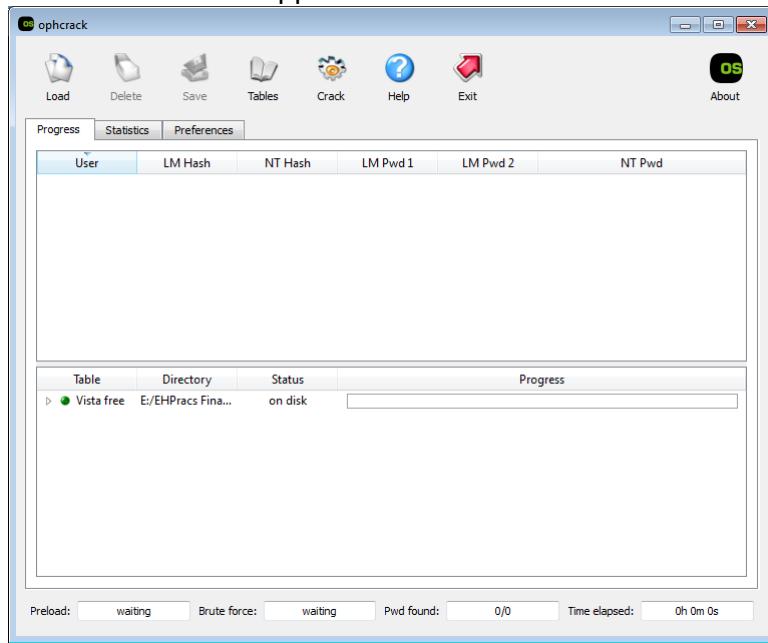
OK

Messages

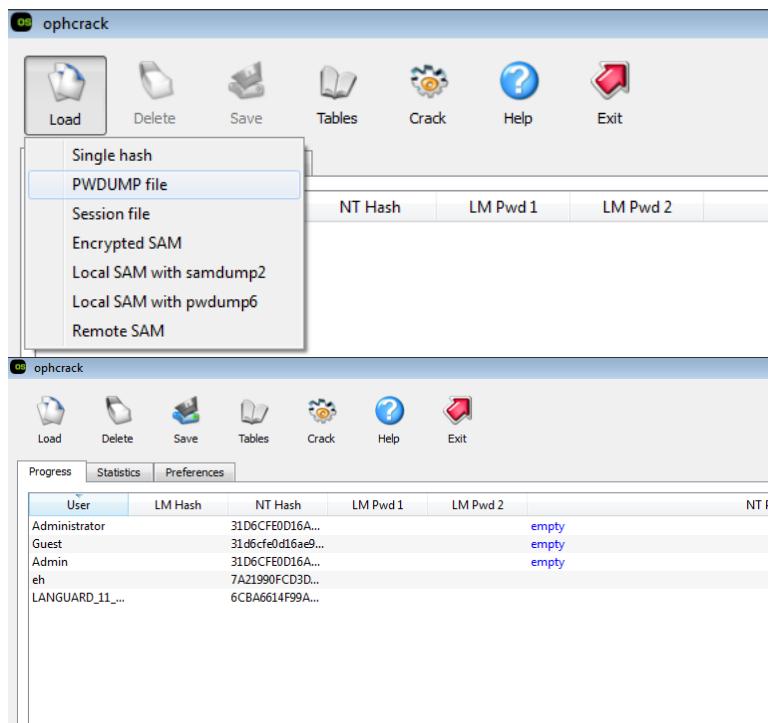
11/11/2014 14:59:36 Entered NTLM Dictionary Audit  
11/11/2014 14:59:37 Cracked NTLM password for '\EH with Dictionary Crack.  
11/11/2014 14:59:41 Exited NTLM Dictionary Audit  
11/11/2014 14:59:41 Auditing session completed.

## 4) Ophcrack

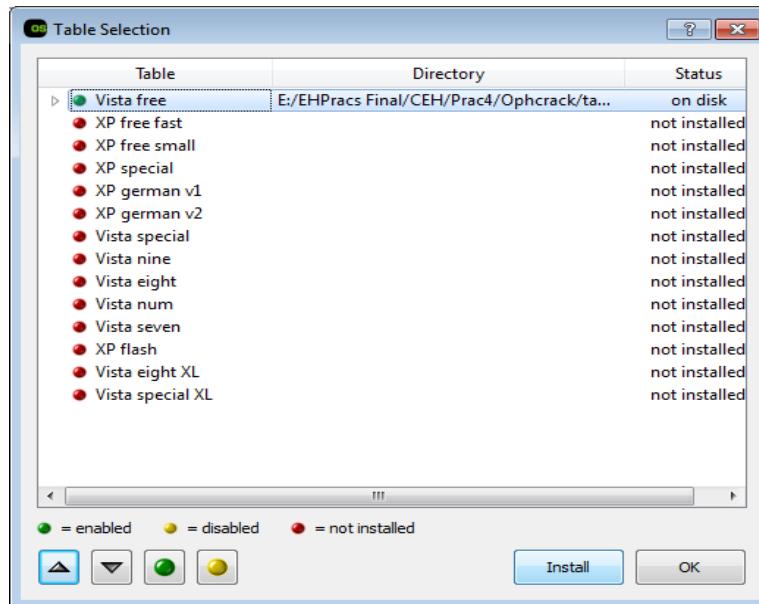
1. Open OphCrack.
2. The **OphCrack** main window appears.



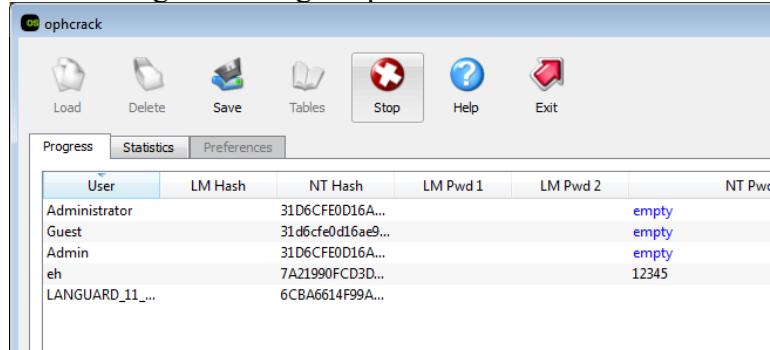
3. Click Load, and then click PWDUMP file. Browse to the location where the extracted PWDump passwords file is and select it. Upon selection, it will load the hashes into the window.



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



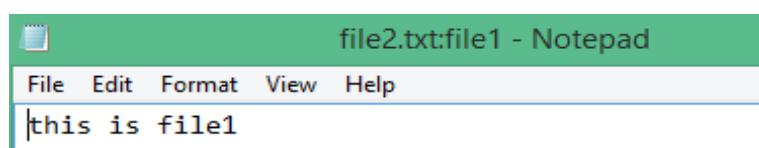
##### 5) NTFS ADS

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

```
D:\>notepad file1.txt
D:\>notepad file2.txt
D:\>type file1.txt > file2.txt:file1.txt
```

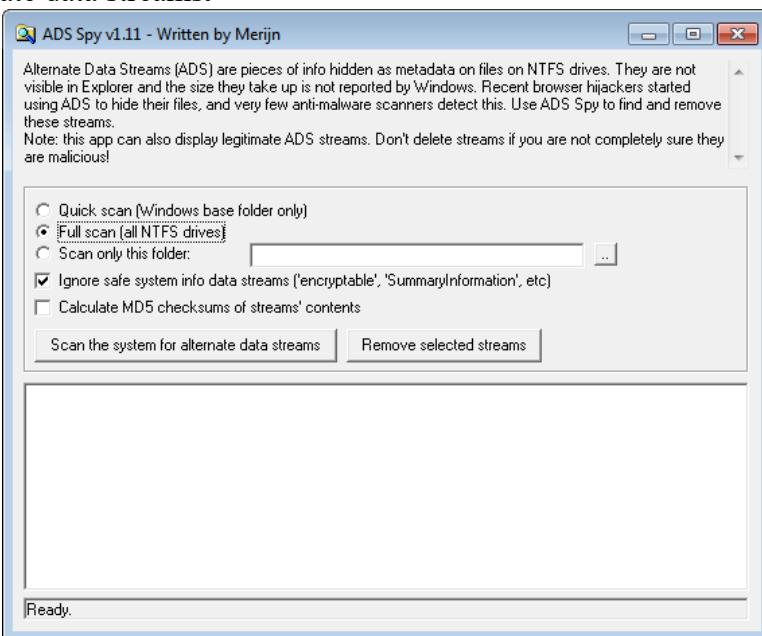
3. We can view the hidden file1 inside file2 by running the command

```
D:\>notepad file2.txt:file1.txt
```

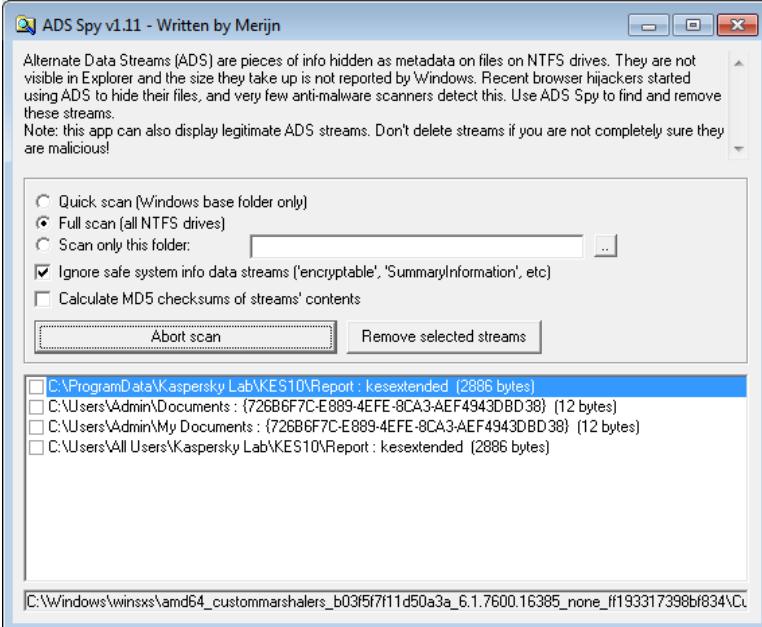


## 6) ADS Spy

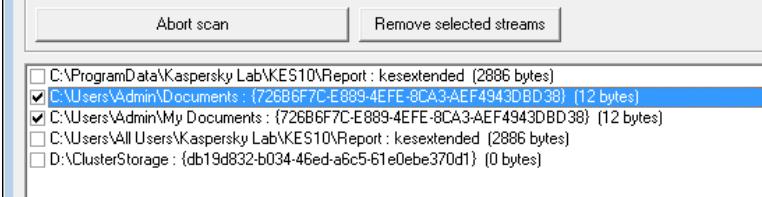
1. Launch ADS Spy.
2. Select a folder to scan by choosing Scan only this folder and click scan the system for alternate data streams.



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

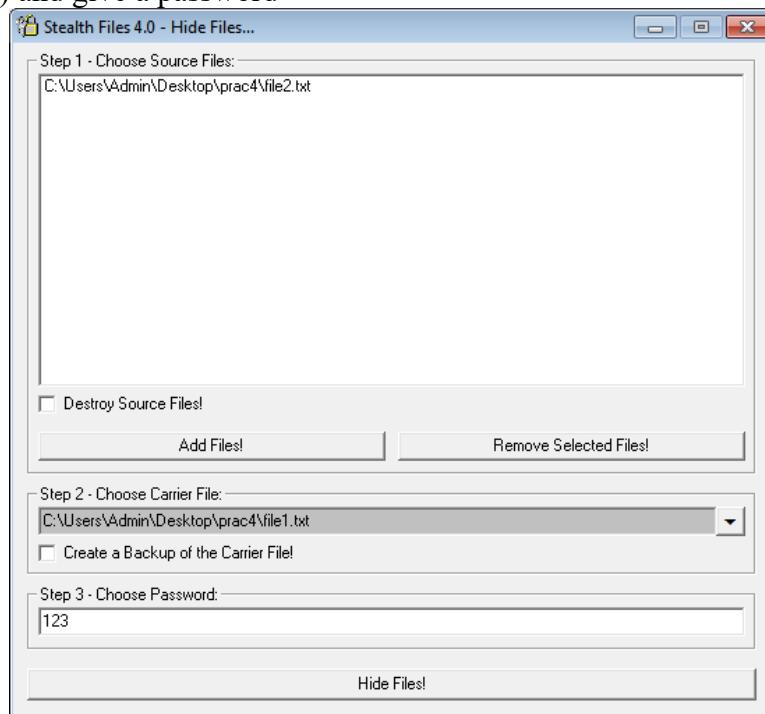


4. To remove the Alternate Data Stream, click Remove selected streams. Click Yes

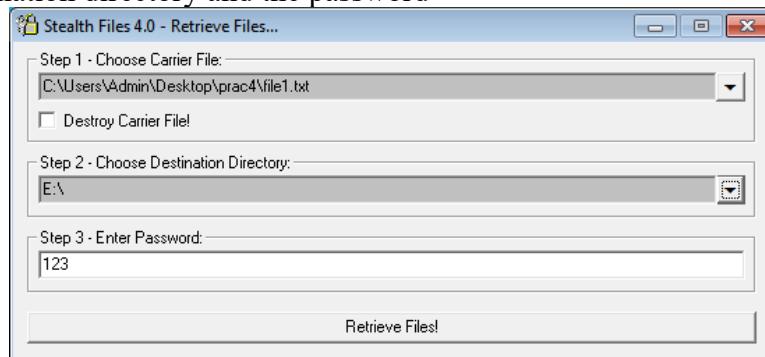


7) Stealth Files Tool

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

```

C:\ Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

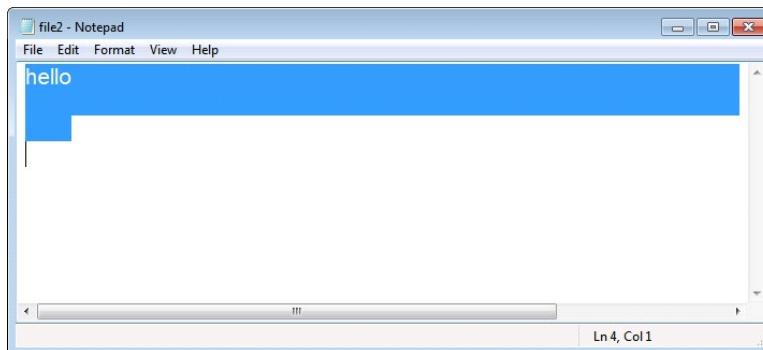
C:\Users\Admin>cd C:\Users\Admin\Desktop\CEHPacs Final\CEH\Prac4\SNOW
C:\Users\Admin\Desktop\CEHPacs Final\CEH\Prac4\SNOW>snow -C -m "Hello World" -p
"magic" file1.txt file2.txt
file.txt: No such file or directory

C:\Users\Admin\Desktop\CEHPacs Final\CEH\Prac4\SNOW>snow -C -m "Hello World" -p
"magic" file1.txt file2.txt
Compressed by 31.82%
Message exceeded available space by approximately 122.22%.
An extra 2 lines were added.

C:\Users\Admin\Desktop\CEHPacs Final\CEH\Prac4\SNOW>

```

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

```

*****
*          Windows Reset Password / Registry Editor / Boot CD
*
*  (c) 1998-2011 Petter Nordahl-Hagen. Distributed under GNU GPL v2
*
* DISCLAIMER: THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTIES!
*              THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR ANY DAMAGE
*              CAUSED BY THE (MIS)USE OF THIS SOFTWARE
*
* More info at: http://pogostick.net/~pnh/ntpasswd/
* Email       : pnh@pogostick.net
*
* CD build date: Wed May 11 20:16:09 CEST 2011
*****
Press enter to boot, or give linux kernel boot options first if needed.
Some that I have to use once in a while:
boot nosusb      - to turn off USB if not used and it causes problems
boot irqpoll     - if some drivers hang with irq problem messages
boot vga=ask      - if you have problems with the videomode
boot nodrivers   - skip automatic disk driver loading
boot:

```

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

```
==== Step ONE: Select disk where the Windows installation is ====
Disks:
Disk /dev/sda: 26.8 GB, 26843545600 bytes
Candidate Windows partitions found:
1. /dev/sda1 23587MB BOOT
Please select partition by number or
q - quit automatically start disk drivers
n - new partition
f - fetch additional drivers from floppy / usb
a - show all possible Windows (NTFS) partitions only
Select: 1
```

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

```
==== Step TWO: Select PATH and registry files =====
DEBUG path: windows found as WINDOWS
DEBUG path: system32 found as system32
DEBUG path: config found as config
DEBUG path: found correct case to be: WINDOWS/system32/config
What is the path to the registry directory? (relative to windows disk)
\WINDOWS\system32\config
```

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

```
What is the path to the registry directory? (relative to windows disk)
DEBUG path: \WINDOWS\system32\config found as WINDOWS
DEBUG path: system32 found as system32
DEBUG path: config found as config
DEBUG path: found correct case to be: WINDOWS/system32/config
-pxwxxrwxrwx 1 0 0 2622144 Nov 17 09:17 SECURITY
-pxwxxrwxrwx 1 0 0 2622144 Nov 17 09:17 default
-pxwxxrwxrwx 1 0 0 17563648 Nov 17 09:17 software
-pxwxxrwxrwx 1 0 0 367096 Nov 17 09:17 systemprofile
-dwxwrxrwxrwx 1 0 0 4096 Sep 22 04:55 systemprofile
-pxwxxrwxrwx 1 0 0 2622144 Sep 22 10:17 userdiff

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password Reset (recommended)
2 - RecoveryConsole Parameters (software)
3 - quit - Return to previous
[1]: 1
```

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

```
==== Step THREE: Password or registry edit =====
chntpw version 0.99.6-110511-1c Patterns N Hgenes
drive <SAM> name <from header>: <\SystemRoot\System32\Config\SAM>
File size 2621440 bytes. Subkey indexing type is: 666c <1h>
File offset 2621440 bytes. Subkey containing offset is: 1 (0x1) <page>
Used for data: 24219616 blocks/bytes; unused: 674768 blocks/bytes.

Hive <SYSTEM> name <from header>: <SYSTEM>
ROOT KEY at offset 0x00000200 *Subkey indexing type is: 666c <1h>
File size 2621440 bytes. Subkey containing offset is: 1 (0x1) <page>
Used for data: 7034873564800 blocks/bytes; unused: 1347/17264 blocks/bytes.

Hive <SECURITY> name <from header>: <\SystemRoot\System32\Config\SECURITY>
ROOT KEY at offset 0x001020 *Subkey indexing type is: 666c <1f>
File size 2621440 bytes. Subkey containing offset is: 1 (0x1) <page>
Used for data: 21800384 blocks/bytes; unused: 274320 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Account lockout duration: 0
Password history count: 0

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
1 - Edit user data and passwords
2 - Registry editor now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> 1
```

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

```
==== chntpw Edit User Info & Passwords ====
RID - Username ----- Admin? | Lock? --
0xf4 - Administrator | ADMIN | *BLANK*
0x1 - ANONYMOUS | ADMIN | *
0x3eb - EH | ADMIN | *
0x1f5 - Guest | dis/lock |
0x3e8 - HelpAssistant | dis/lock |
0xea - SILENT_388945a0 | dis/lock |

Select: f - quit - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] EH
```

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

```
RID : 1003 [0x3eb]
Username: EH
Full name:
Comment:
homedir:

User is member of 1 groups:
00000220 = Administrators (which has 2 members)

Account bits: 0x0210 =
[ ] Disabled [ ] Homedir req. [ ] Passwd not req.
[ ] Temp. duplicate [X] Normal account [ ] NMS account
[ ] Don't trust acc [ ] No type act. [ ] Srv. trust act.
[X] Don't logon [ ] Auto lockout [ ] Unknown 0x088
[ ] (unknown 0x10) [ ] (unknown 0x20) [ ] (unknown 0x40)

Failed login count: 0 while max tries is: 0
Total login count: 35

User Edit Menu:
1 -- Clear (blank) user password
2 -- Edit (set new) user password (careful with this on XP or Vista)
3 -- Promote user (make user an administrator)
4 -- Unlock and enable user account (seems unlocked already)
q -- Quit editing user, back to user select
Select: [q] q

Select: f - quit - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] EH
```

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

```
-- User Edit Menu:
1 -- Clear (blank) user password
2 -- Edit (set new) user password (careful with this on XP or Vista)
3 -- Promote user (make user an administrator)
4 -- Unlock and enable user account (seems unlocked already)
q -- Quit editing user, back to user select
Select: [q] q

Select: f - quit - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] EH
```

10. type q to Quit the edit mode

```
<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
1 - Edit user data and passwords
2 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> q
```

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

```
What to do? [1] -> q
Hives that have changed:
# Name
0 <SAM> - OK
=====
Step FOUR: Writing back changes
About to write file(s) back? Do it? [n]: y
```

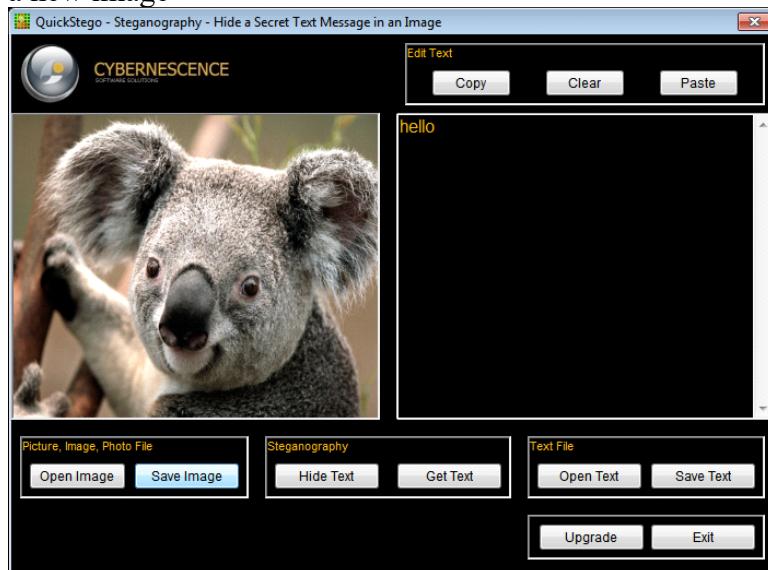
12. Type y to perform it again or n to exit

```
***** EDIT COMPLETE *****
You can try again if it somehow failed, or you selected wrong
New run? [y] n
```

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

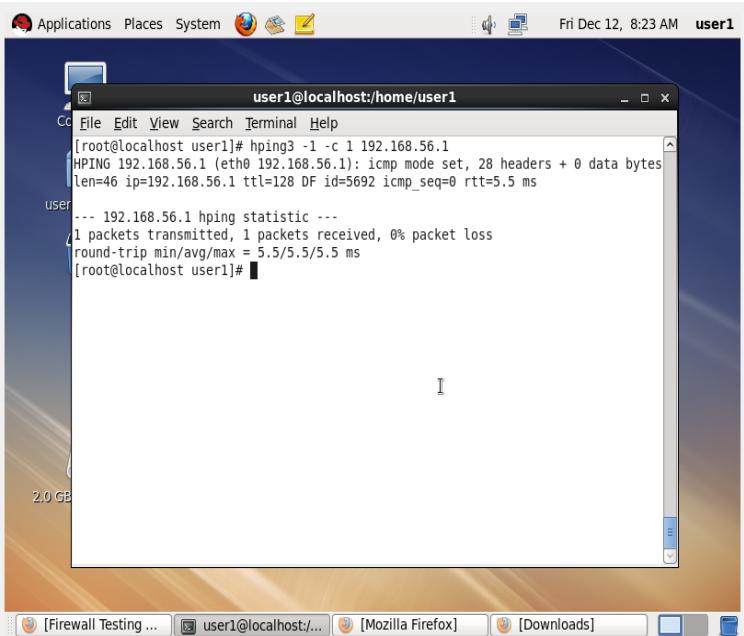


4. To see the text hidden inside of an image
5. Open the image using **Open Image** and Quick Stego will directly show the hidden text from inside the image

## PRACTICAL 5

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

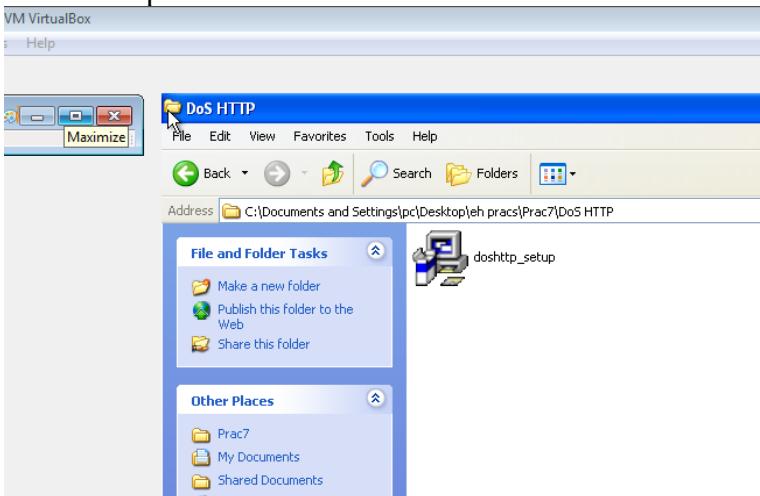
#### 1) hping3



```
user1@localhost:~$ hping3 -1 -c 1 192.168.56.1
HPING 192.168.56.1 (eth0 192.168.56.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.56.1 ttl=128 DF id=5692 icmp_seq=0 rtt=5.5 ms
user1--- 192.168.56.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 5.5/5.5/5.5 ms
user1@localhost:~$
```

#### 2) DoSHTTP

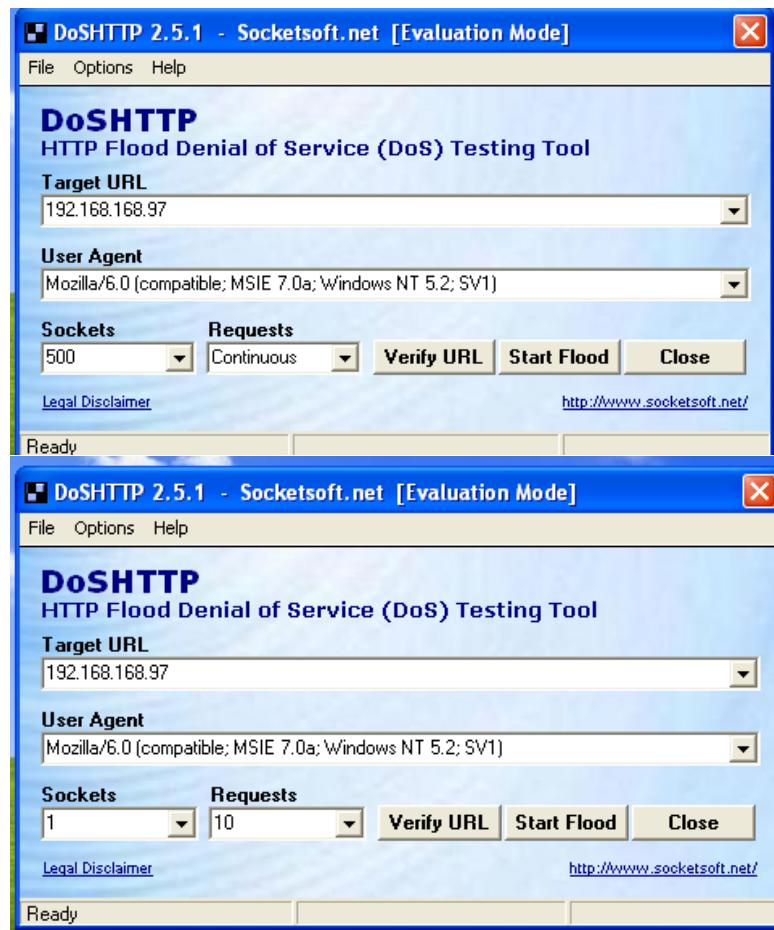
Double click on the setup file of DoSHTTP to install



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"



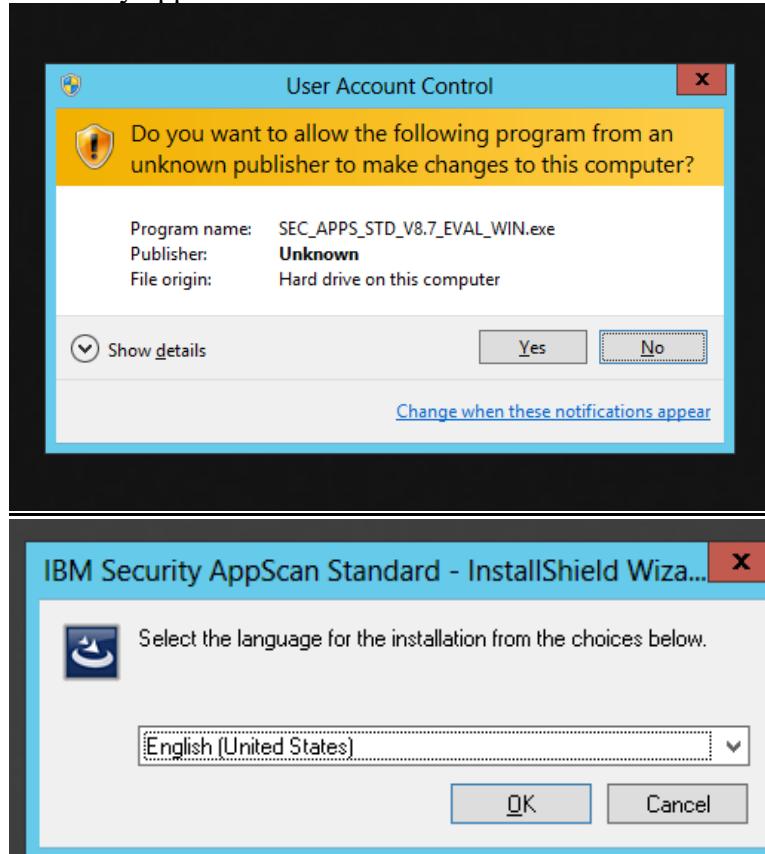
## PRACTICAL 6

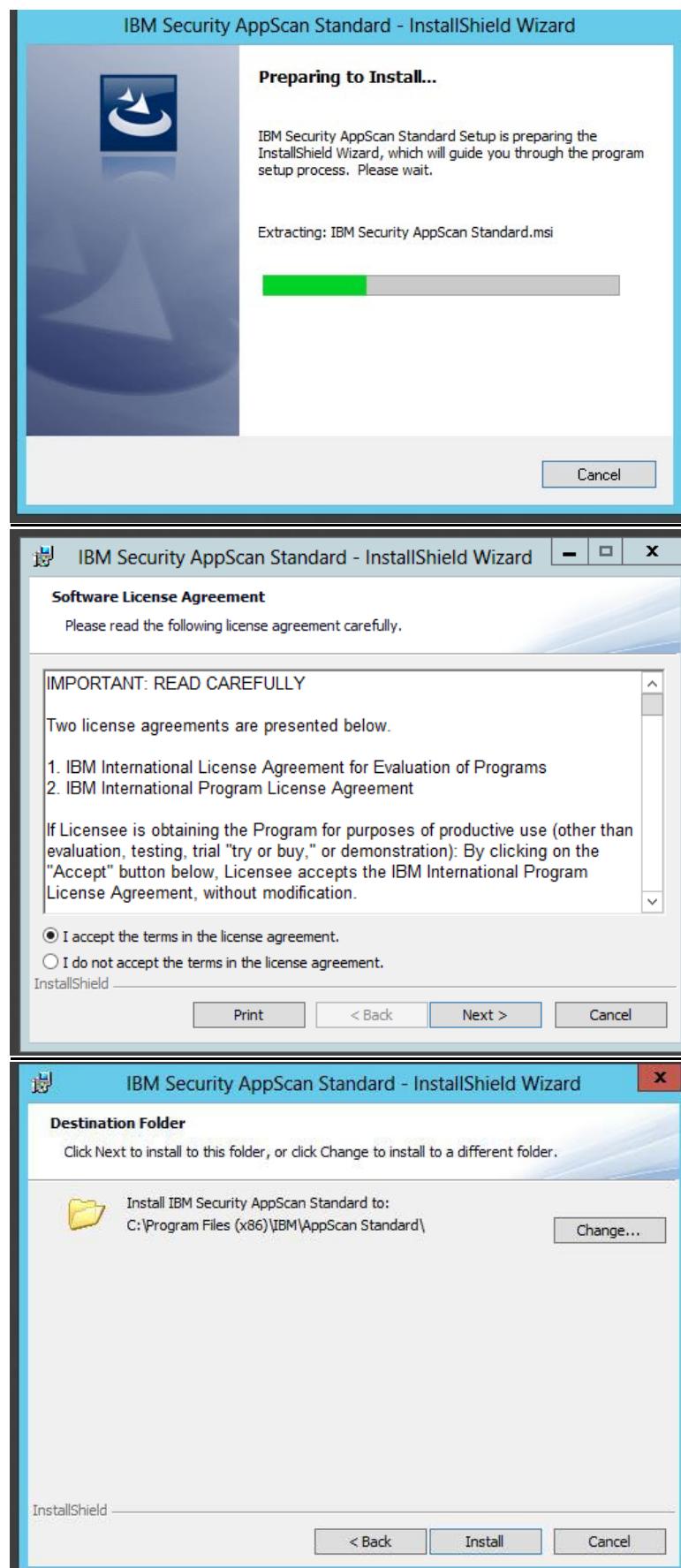
### A. Study of Web server Attack tools

#### 1) IBM Security AppScan

Solution:

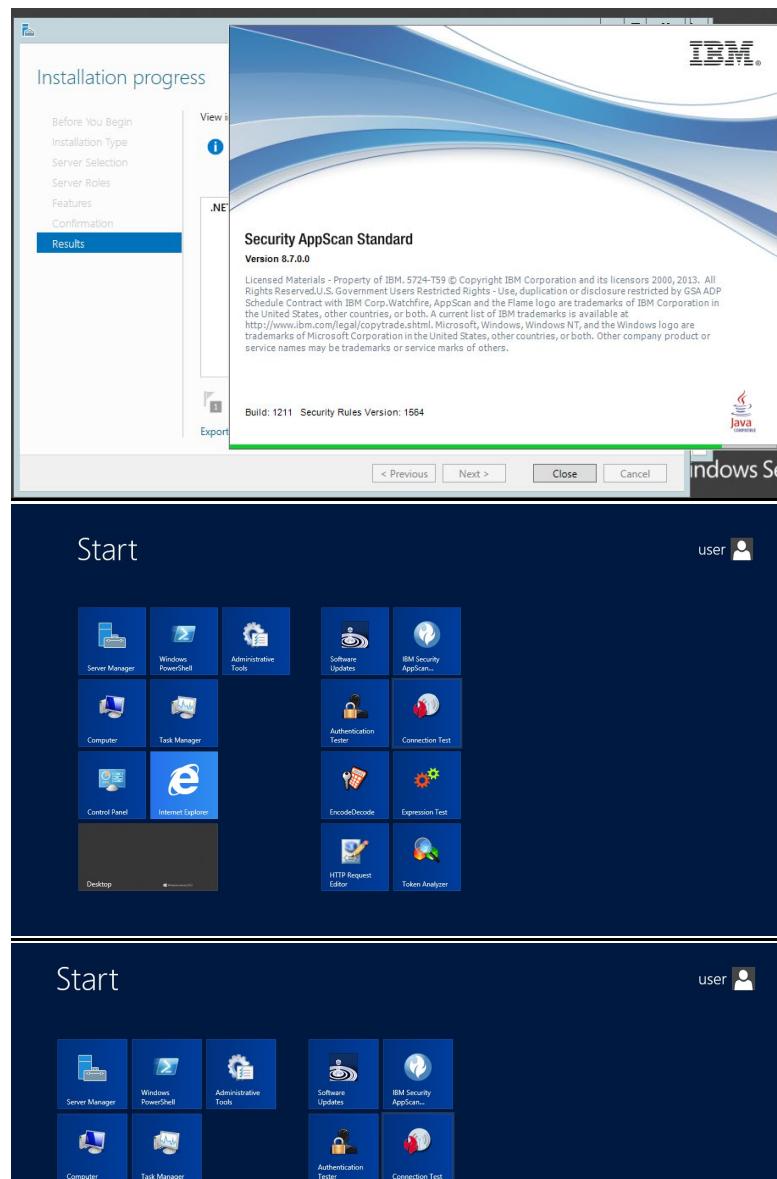
1. Install ibm security app scan





## Security Breaches and Countermeasures

2314041

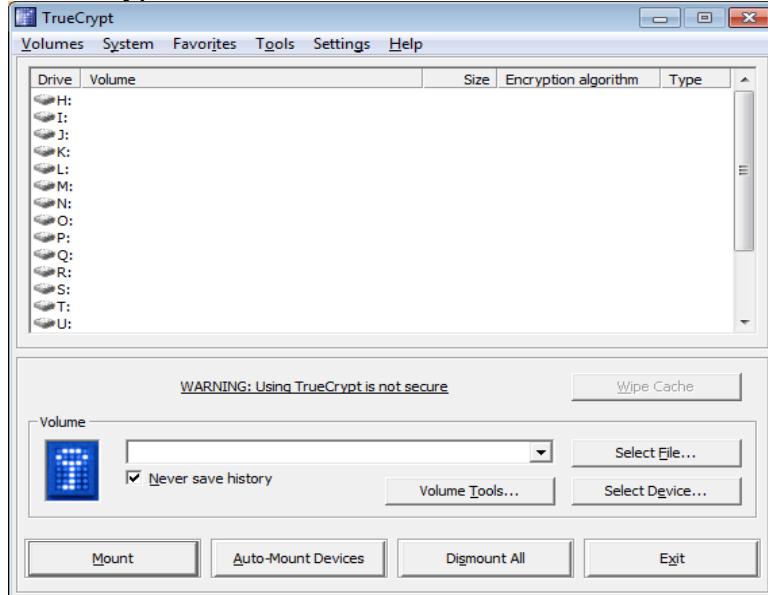


# PRACTICAL 7

## A. Using Cryptanalysis Tools

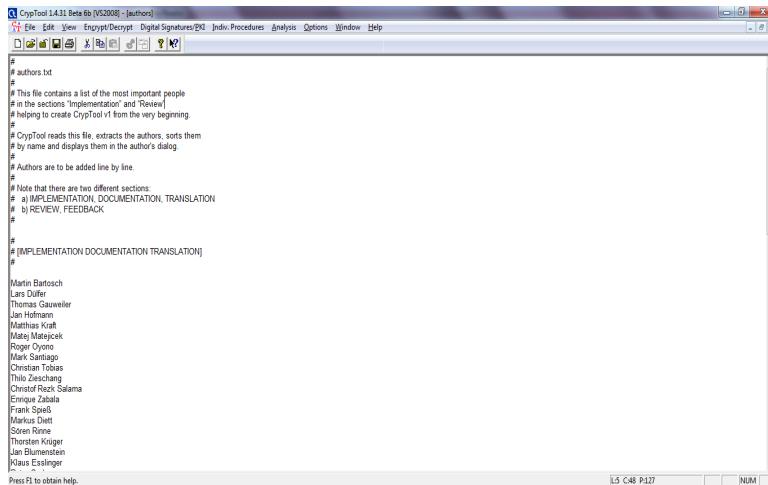
### 1) TrueCrypt

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

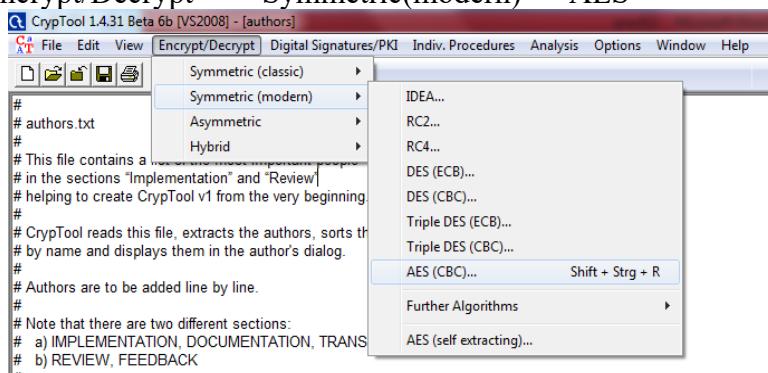


### 2) Cryptool

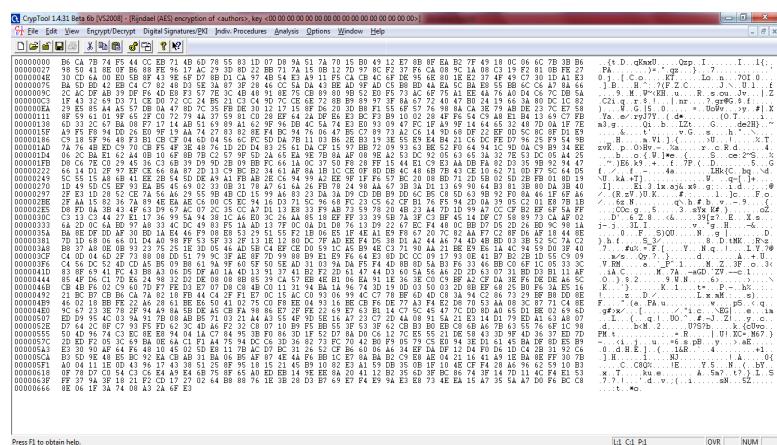
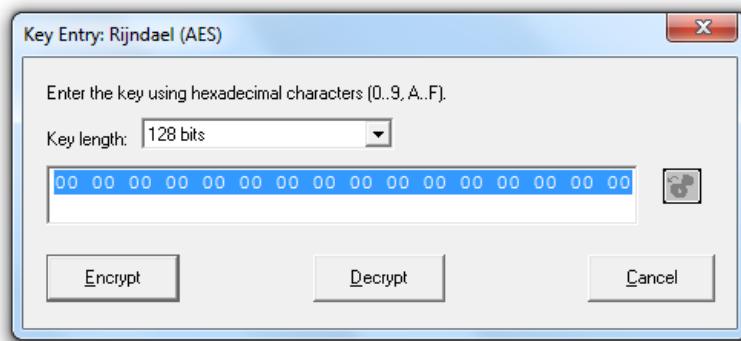
1. Open the software



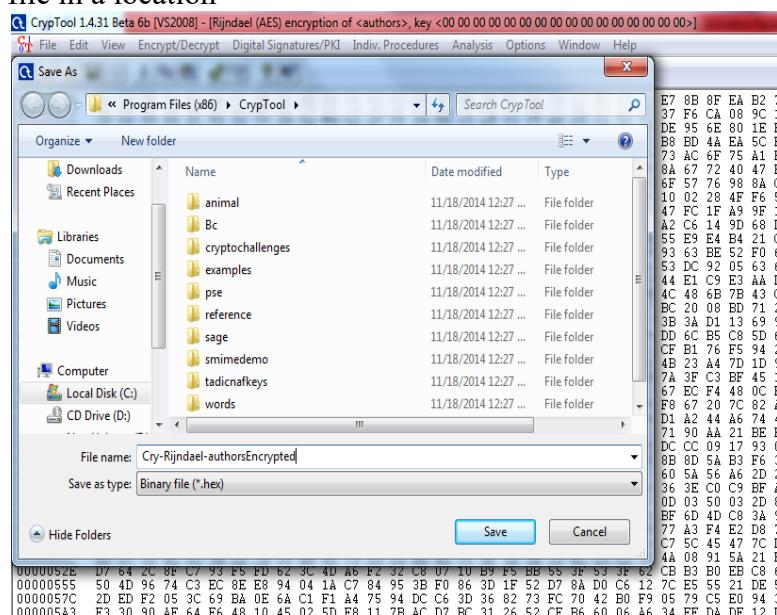
2. Go to "Encrypt/Decrypt" --> Symmetric(modern) -->AES



### 3. Click on "Encrypt"

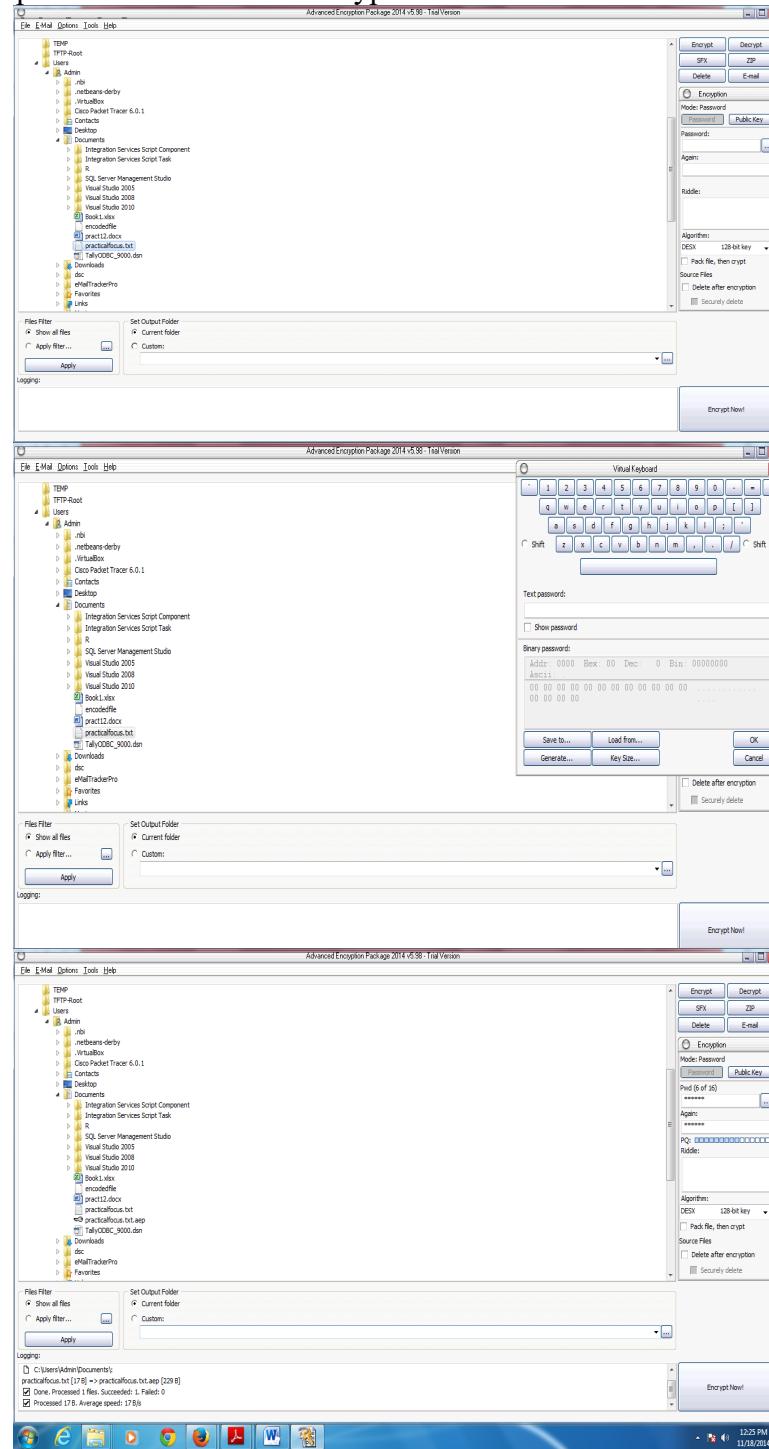


### 4. Save the file in a location



### 3) Advanced Encryption Package

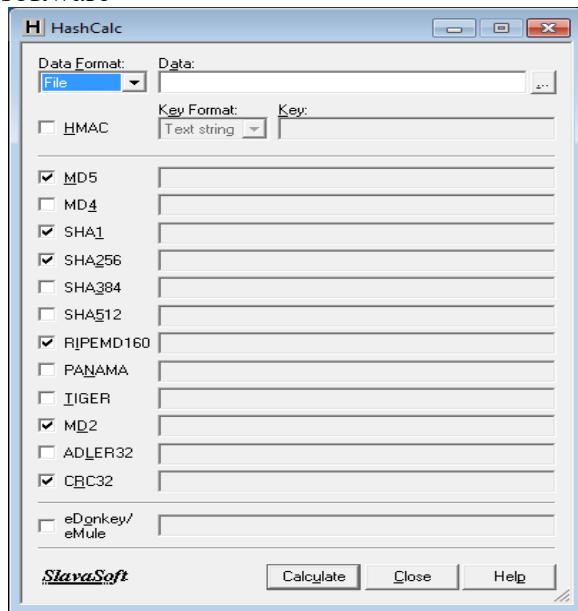
1. Open the software
2. Browse any file to decrypt e.g. "abc.txt"
3. Enter the password and select "Encrypt"



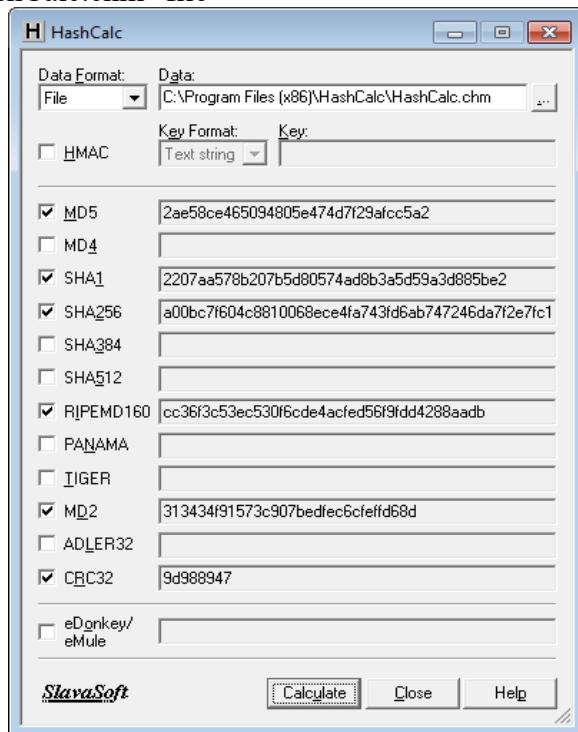
## PRACTICAL 8

### A. Using HashCalc Tools

- 1) HashCalc
1. Open HashCalc software



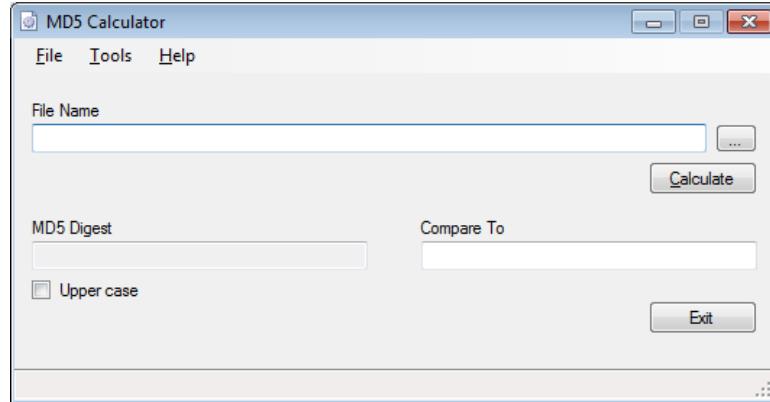
2. Browse the "HashCalc.chm" file



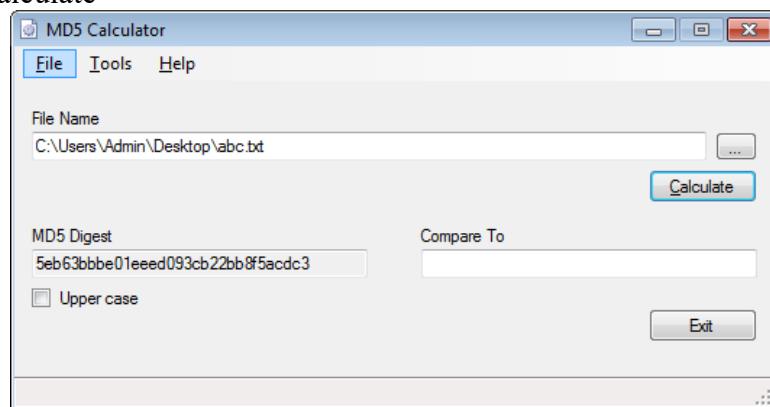
# PRACTICAL 9

## A. Using MD5 Calculator Tools

- 1) MD5 Calculator
1. Open MD5 Calculator



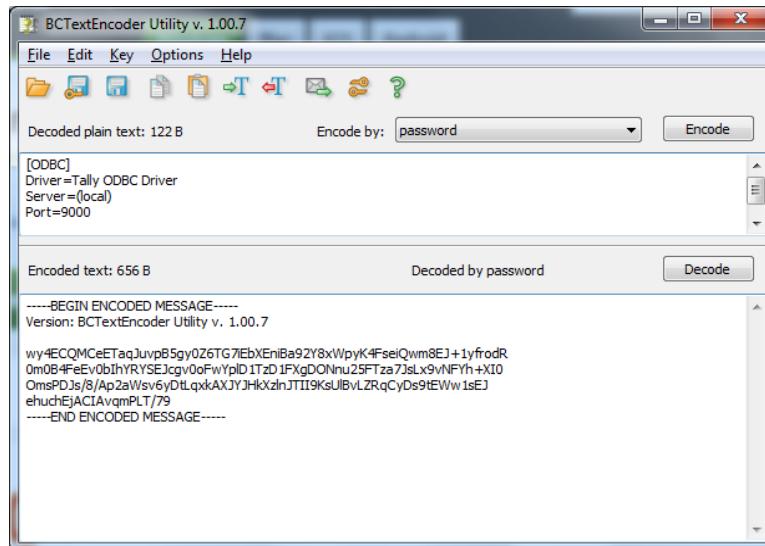
2. Select "File"
3. Browse any file to decrypt e.g. "abc.txt"
4. Select Calculate



## PRACTICAL 10

### A. Using BCTextEncoder Tools

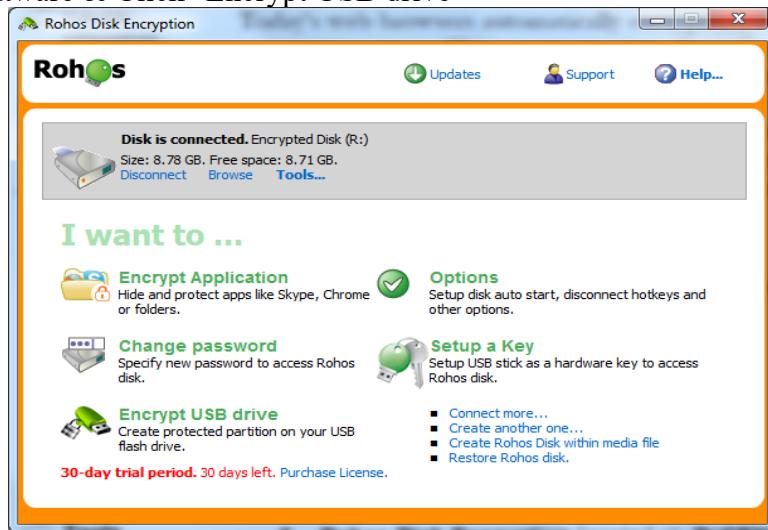
- 1) BCTextEncoder
1. Open the file --> Encode



## PRACTICAL 11

### A. Using Rohos Disk Encryption Tools

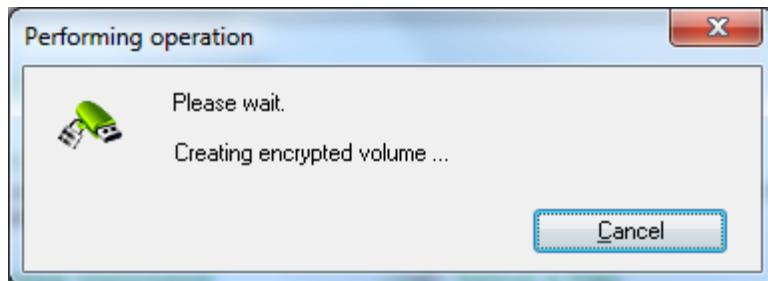
- 1) Rohos Disk Encryption
1. Open software & Click "Encrypt USB drive"



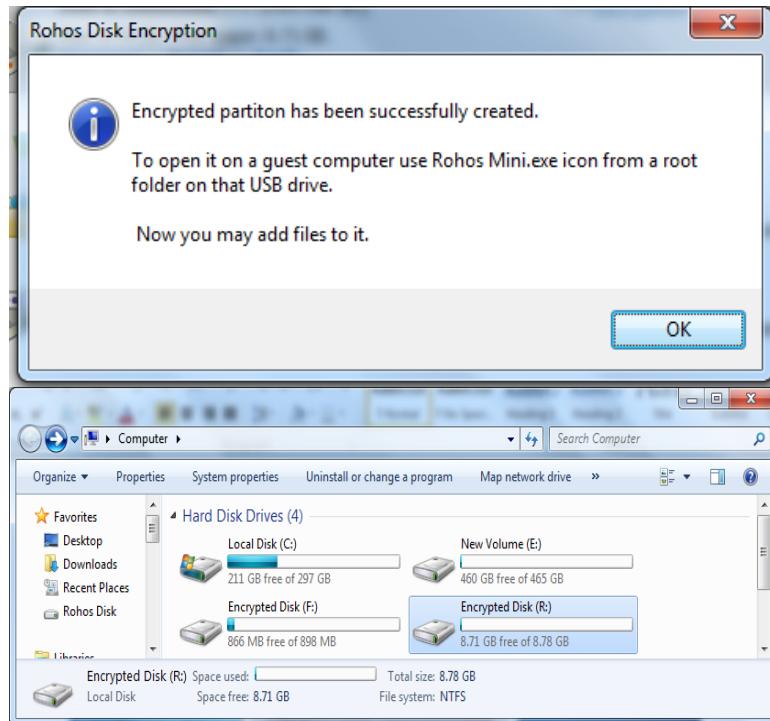
2. Enter the password and confirm Password



3. Create Disk



4. Click "OK"



## PRACTICAL 12

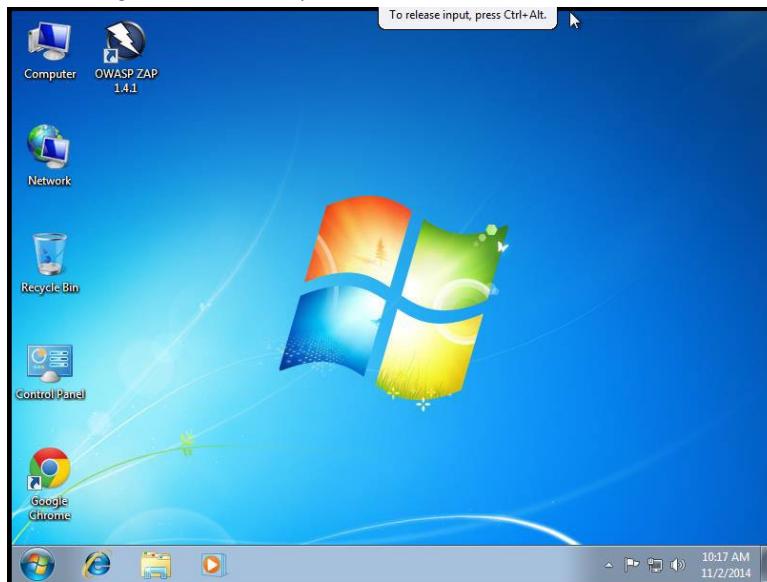
### A. Study of Session Hijacking tools

1) ZAP

Solution:

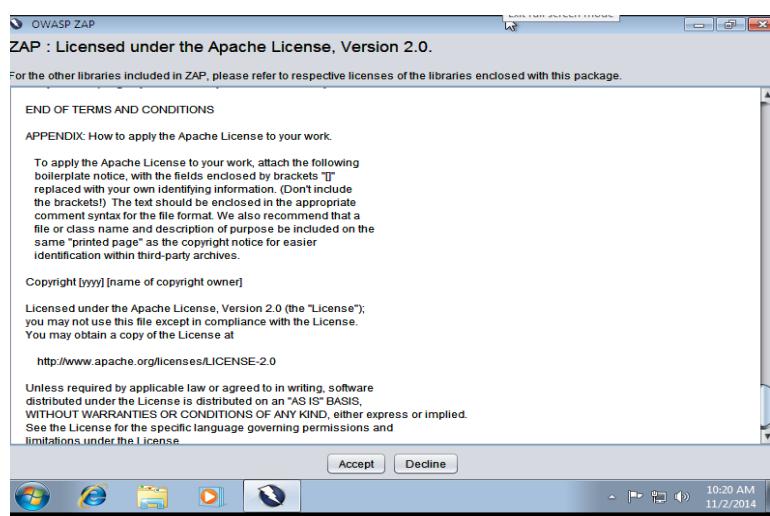
Lab Task:

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

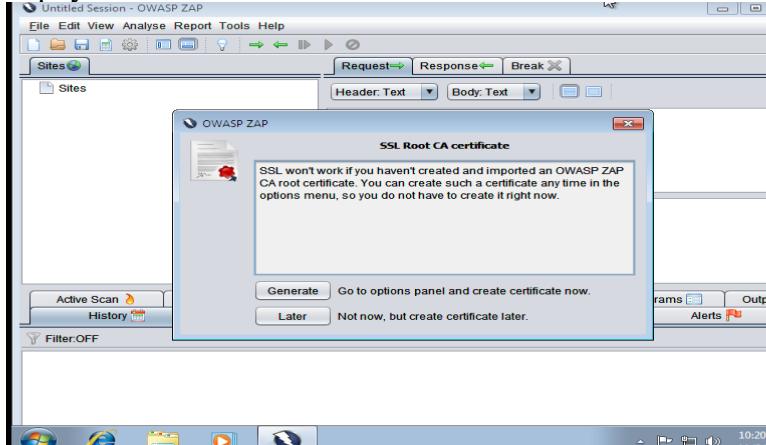


2. Install ZAP Tool. And Launch it.

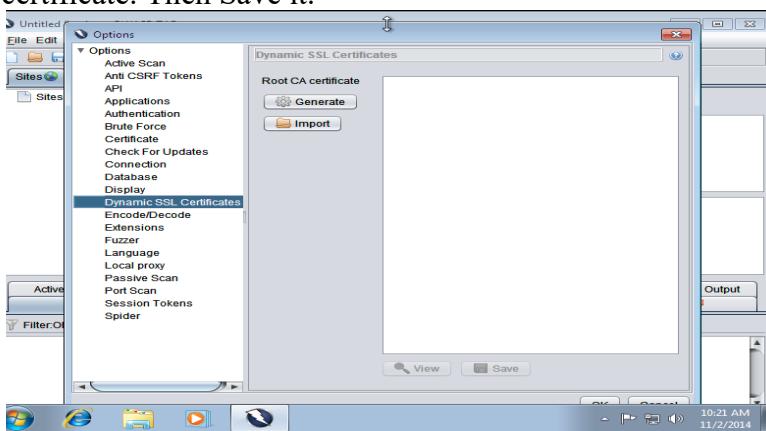
3. Accept license.



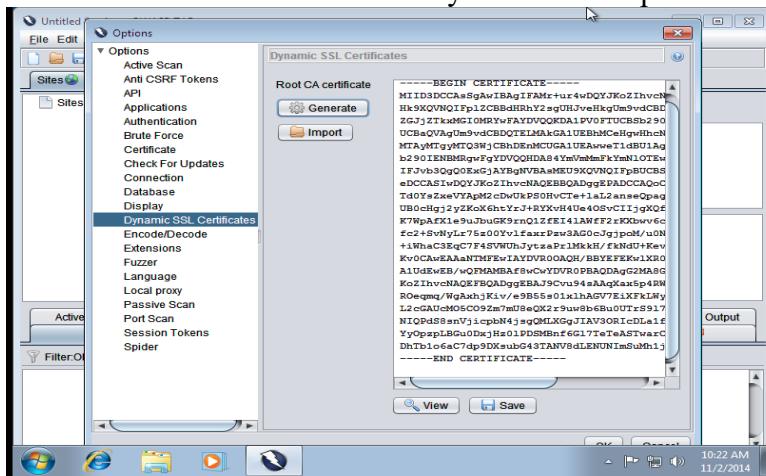
4. It will prompt you SSL Root CA Certificate. Click Generate to continue.

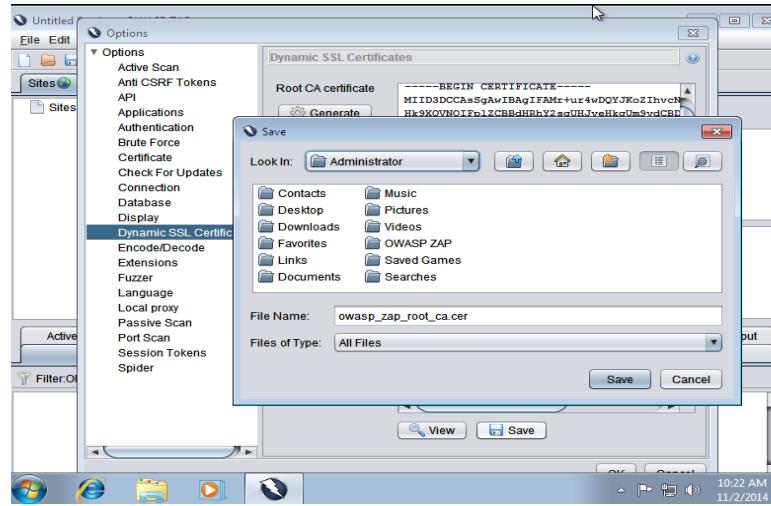


5. In the options window, select Dynamic SSL Certificates and click Generate to generate certificate. Then Save it.

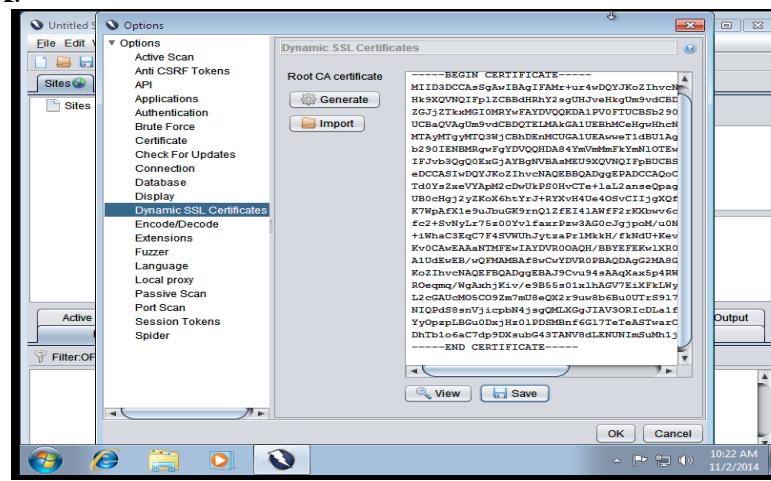


6. Save certificate to default location. If already exists then replace it.

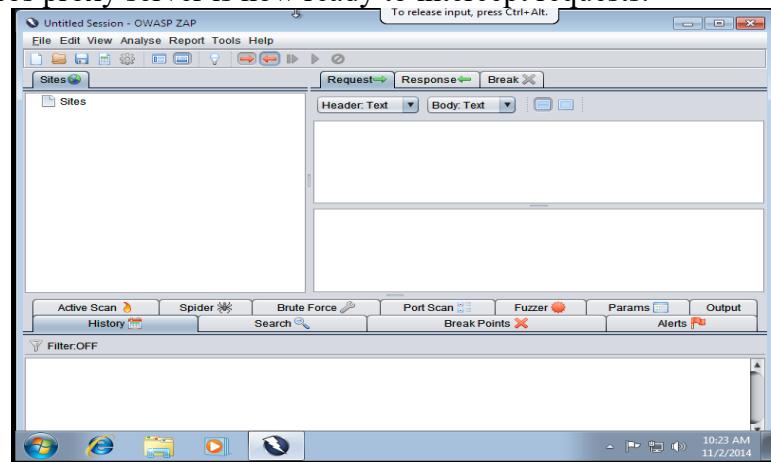




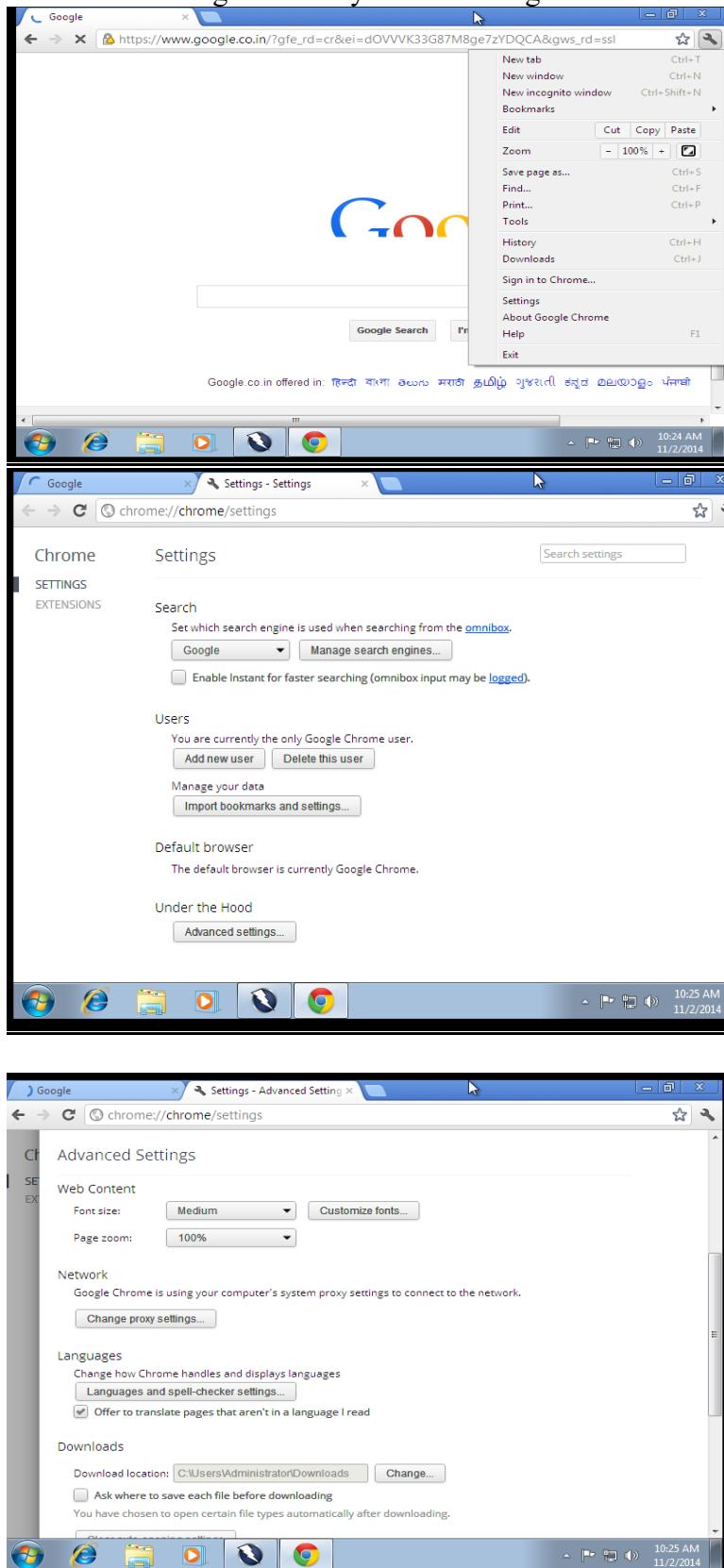
7. Click OK.

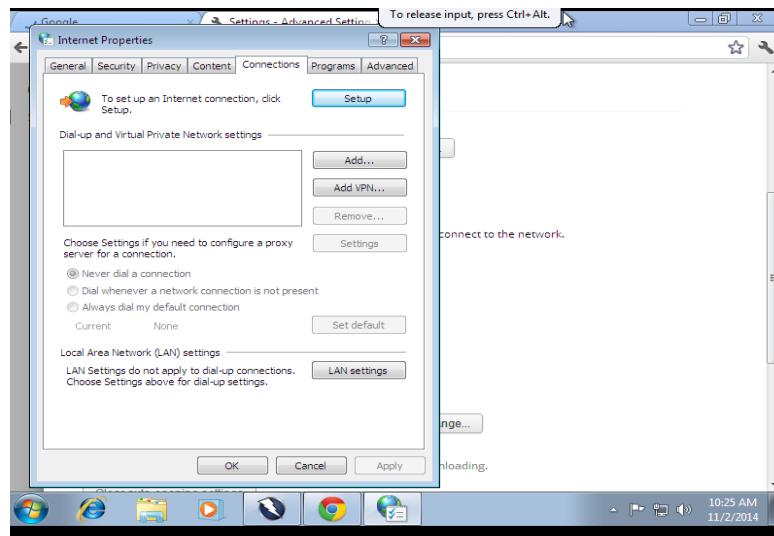


8. Your Paros proxy server is now ready to intercept requests.

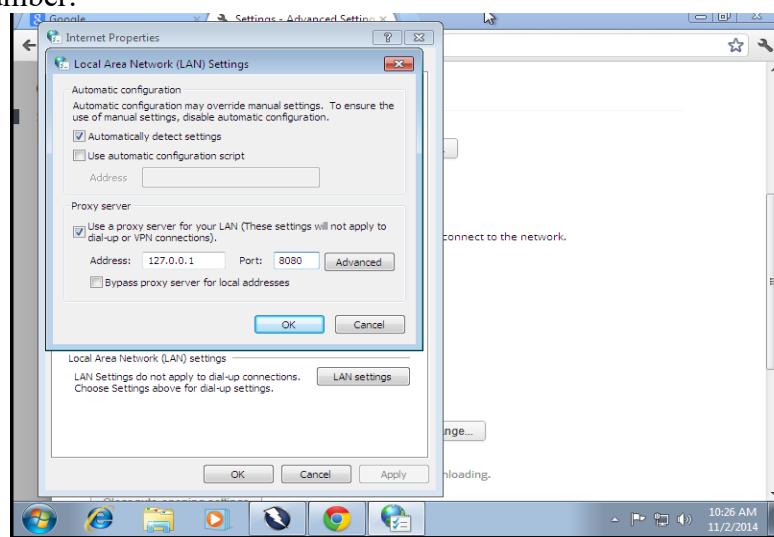


9. Launch chrome. And change the Proxy Server setting.

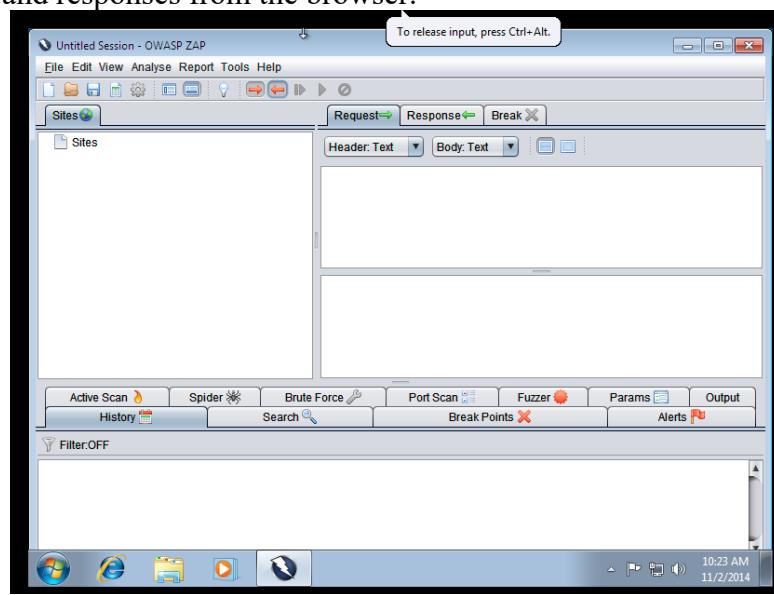




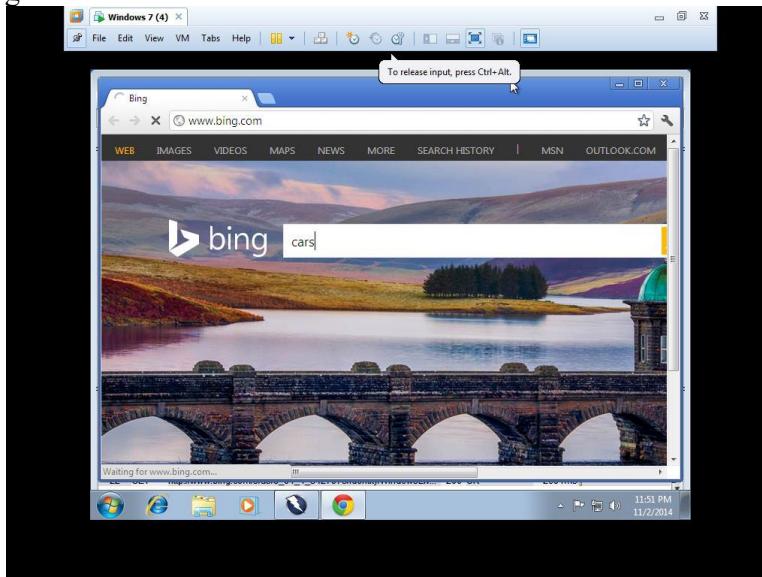
10. Check Use proxy server for your LAN. And type 127.0.0.1 as address and 8080 as a port number.



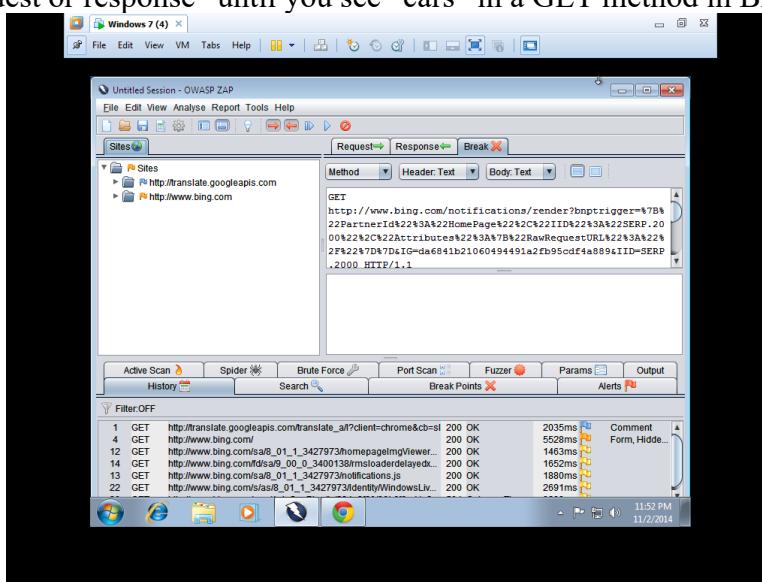
11. Click “Set break on all requests” and “Set break on all responses” to trap all requests and responses from the browser.

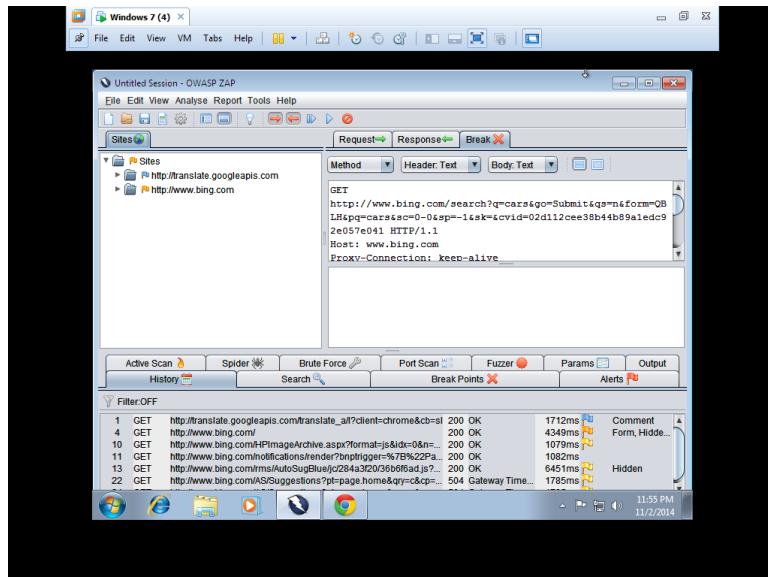


12. Now navigate to chrome browser and open www.bing.com  
Start searching for “Cars”

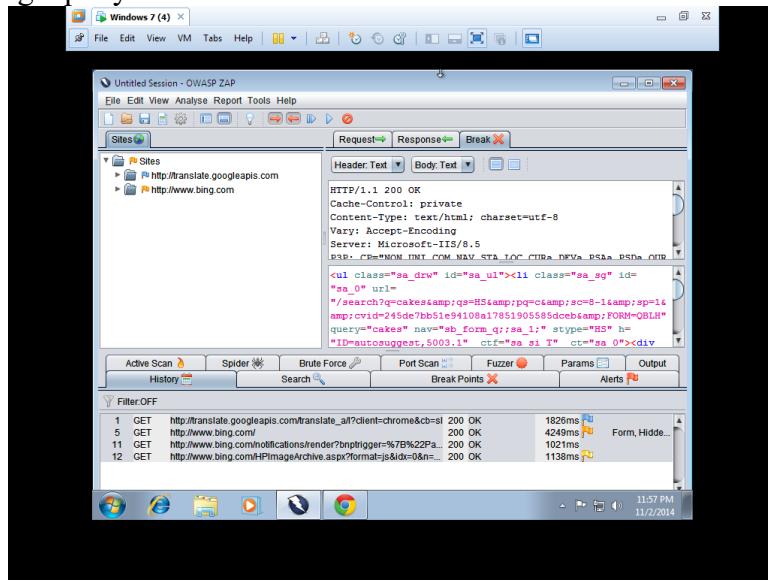


13. Open ZAP and observe trapped traffic.  
14. Observe first few lines of trapped traffic and keep clicking “Submit” and step to next request or response” until you see “cars” in a GET method in Break tab.





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”.

The screenshot shows the OWASP ZAP interface with the 'Response' tab selected. The 'Header.Text' and 'Body.Text' dropdowns are open. The 'Body.Text' dropdown contains the following modified JavaScript code:

```

HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Type: text/html; charset=utf-8
Expires: Wed, 05 Nov 2014 07:43:38 GMT
Vary: Accept-Encoding

[...] //script><title>car</title><link href="/search?format=css&amp;q=cakes&amp;go=Submit&amp;qs=&amp;form=QSL&amp;pg=cars&amp;sc=8&amp;sp=1&amp;sk=1&amp;cvid=f76f35f7901944ca8814d82982a6c647" rel="alternate"

```

The 'History' tab at the bottom shows a list of requests and responses, with the last entry being a 504 Gateway Timeout.

The screenshot shows the OWASP ZAP interface with the 'Response' tab selected. The 'Header.Text' and 'Body.Text' dropdowns are open. The 'Body.Text' dropdown contains the original JavaScript code:

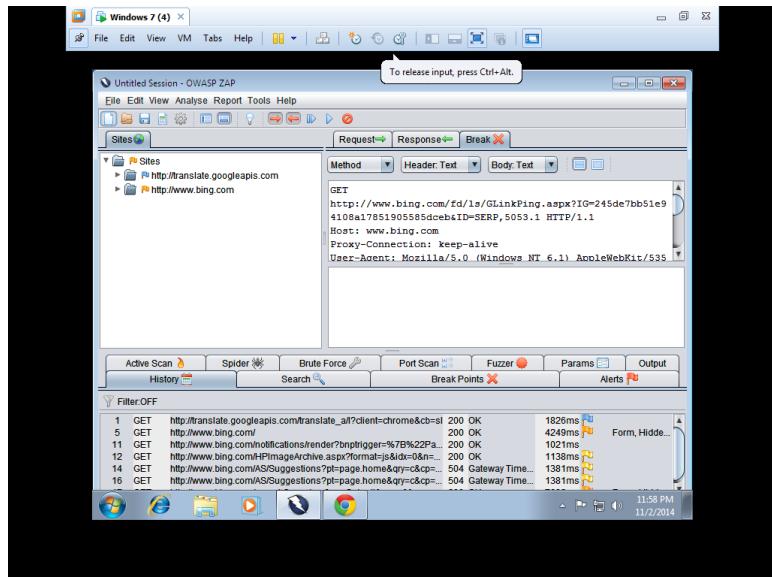
```

HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Type: text/html; charset=utf-8
Expires: Wed, 05 Nov 2014 07:43:38 GMT
Vary: Accept-Encoding

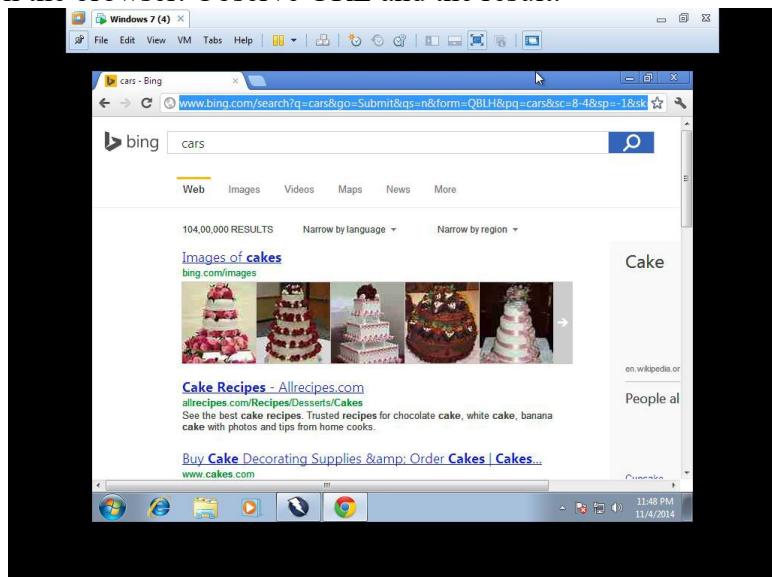
[...] //script><title>cake</title><link href="/search?format=css&amp;q=cakes&amp;go=Submit&amp;qs=&amp;form=QSL&amp;pg=cars&amp;sc=8&amp;sp=1&amp;sk=1&amp;cvid=f76f35f7901944ca8814d82982a6c647" rel="alternate"

```

The 'History' tab at the bottom shows a list of requests and responses, with the last entry being a 504 Gateway Timeout.



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](http://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.

```
Terminal
File Edit View Search Terminal Help
Sponsored by...
BLACK HILLS www.blackhillsinfosec.com
[recon-ng v4.9.2, Tim Tomes (@LaNNMaSteR53)] 

[77] Recon modules
[8] Reporting modules
[2] Import modules
[2] Exploitation modules
[2] Discovery modules
```

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

```
Terminal
File Edit View Search Terminal Help
[recon-ng][default] > show modules

Discovery
-----
discovery/info_disclosure/cache_snoop
discovery/info_disclosure/interesting_files

Exploitation
-----
exploitation/injection/command_injector
exploitation/injection/xpath_bruter

Import
-----
import/csv_file
import/list

Recon
-----
recon/companies-contacts/bing_linkedin_cache
```

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

```
Terminal
File Edit View Search Terminal Help
reporting/pushpin
reporting/xlsx
reporting/xml

[recon-ng][default] > search netcraft
[*] Searching for 'netcraft'...

Recon
-----
recon/domains-hosts/netcraft

[recon-ng][default] > use recon/domains-hosts/netcraft
[recon-ng][netcraft] > show options

Name Current Value Required Description
----- ----- ----- -----
SOURCE default yes source of input (see 'show info' for
details)

[recon-ng][default][netcraft] >
```

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

```
[recon-ng][default] > search netcraft
[*] Searching for 'netcraft'...

Recon
-----
  recon/domains-hosts/netcraft

[recon-ng][default] > use recon/domains-hosts/netcraft
[recon-ng][default][netcraft] > show options

  Name      Current Value  Required  Description
  -----  -----
  SOURCE    default        yes       source of input (see 'show info' for
details)

[recon-ng][default][netcraft] > set source [REDACTED].com
SOURCE => [REDACTED].com
[recon-ng][default][netcraft] > run
```

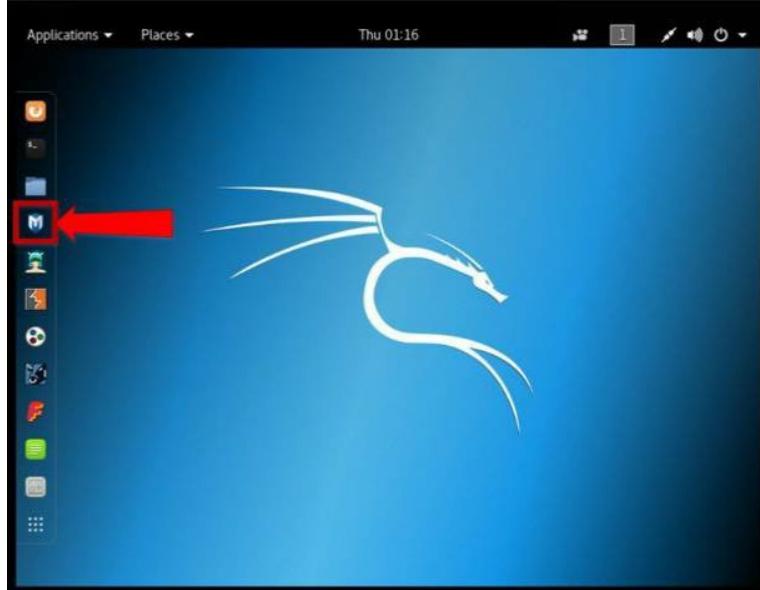
5. Set the source by the command “set source [domain].” Press enter to continue. Type Run to execute and press enter.

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.

```
File Edit View Search Terminal Help
Creating database user 'msf'
Enter password for new role:
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/metasploit-framework/config/database.yml
[*] Starting the Metasploit Framework console...|
```

```
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 36021 (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:e0:70:72:35: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 6fd3:3d:cb:54:0b:83:3e:bd:25:1c:da:67:b6:92:fb (DSA)
|_ 2048 f9:bc:20:c5:6e:db: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?
8100/tcp open tcpwrapped
8300/tcp closed tm1
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:1: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)

```

## Security Breaches and Countermeasures

2314041

```
| 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'
[*] Import: 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

Applications ▾ Places ▾ Terminal ▾ Thu 01:56
Terminal
File Edit View Search Terminal Help
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
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 >
```

msf > hosts

Hosts	Address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
<hr/>									
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
```

```
Applications ▾ Places ▾ Terminal ▾ Thu 02:02
File Edit View Search Terminal Help

msf > db nmap -SS -A 10.10.50.211
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-26 02:01 EDT
[*] Nmap: Nmap scan report for 10.10.50.211
[*] Nmap: Host is up (0.00032s latency).
[*] Nmap: Not shown: 999 filtered ports
[*] Nmap: PORT      STATE SERVICE          VERSION
[*] Nmap: 3389/tcp open  ms-wbt-server Microsoft Terminal Services
[*] Nmap: | ssl-cert: Subject: commonName=WIN-2HMGPM3UAD7
[*] Nmap: |_ Not valid before: 2018-03-28T12:23:16
[*] Nmap: |_ Not valid after: 2018-09-27T12:23:16
[*] Nmap: |_ ssl-date: 2018-04-26T06:01:58+00:00; -4s from scanner time.
[*] Nmap: MAC Address: 00:0C:29:BA:AC:AA (VMware)
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
[*] Nmap: Device type: general purpose
[*] Nmap: Running (JUST GUESSING): FreeBSD 6.X (85%)
[*] Nmap: OS CPE: cpe:/o:freebsd:freebsd:6.2
[*] Nmap: Aggressive OS guesses: FreeBSD 6.2-RELEASE (85%)
[*] Nmap: No exact OS matches found for host (test conditions non-ideal).
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Host script results:
[*] Nmap: |_ clock-skew: mean: -4s, deviation: 0s, median: -4s
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT      ADDRESS
[*] Nmap: 1  0.31 ms 10.10.50.211
[*] Nmap: OS and Service detection performed. Please report any incorrect results at h
```

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

msf > services

```
Applications ▾ Places ▾ Terminal ▾ Thu 02:05
Terminal

File Edit View Search Terminal Help
msf > services
[shared]
Services
=====
host      port    proto   name          state   info
---       ---     ---     ---           ---     ---
10.10.50.1  22     tcp     ssh           open    Cisco SSH 1.25 protocol 1.5
10.10.50.1  23     tcp     telnet        open    Cisco router telnetd
10.10.50.1  5060   tcp     sip-proxy     open    Cisco SIP Gateway IOS 15.2.4.M4
10.10.50.1  5061   tcp     tcpwrapped   open
10.10.50.10 22     tcp     ssh           open    OpenSSH 5.6 protocol 2.0
10.10.50.10 80     tcp     http          open    VMware ESXi Server httpd
10.10.50.10 427    tcp     svrloc        open
10.10.50.10 443    tcp     ssl/http      open    VMware ESXi Server httpd
10.10.50.10 902    tcp     ssl/vmware-auth open    VMware Authentication Daemon 1.10
Uses VNC, SOAP
10.10.50.10 5988   tcp     wbem-ssh     closed
10.10.50.10 5989   tcp     ssl/wbem      open    SBLIM Small Footprint CIM Broker
10.10.50.10 8000   tcp     http-alt      open
10.10.50.10 8100   tcp     tcpwrapped   open
10.10.50.10 8300   tcp     tmi           closed
10.10.50.11 22     tcp     ssh           open    OpenSSH 5.6 protocol 2.0
10.10.50.11 80     tcp     http          open    VMware ESXi Server httpd
10.10.50.11 427    tcp     svrloc        open
10.10.50.11 443    tcp     ssl/http      open    VMware ESXi Server httpd
10.10.50.11 902    tcp     ssl/vmware-auth open    VMware Authentication Daemon 1.10
Uses VNC, SOAP
10.10.50.11 5988   tcp     wbem-ssh     closed
```

```
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	no	The password for the specified username
SMBUser	no	no	The username to authenticate as
THREADS	100	yes	The number of concurrent threads

```
Terminal
File Edit View Search Terminal Help

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         no        The password for the specified username
SMBUser     no         no        The username to authenticate as
THREADS    100        yes        The number of concurrent threads

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

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

```
Terminal
File Edit View Search Terminal Help

msf auxiliary(scanner/smb/smb_version) > run

[+] 10.10.50.100:445 - Host is running Windows 7 Professional SPI (build:7601)
(name:WIN7-PC) (workgroup:WORKGROUP)
[+] 10.10.50.202:445 - Host is running Windows 7 Professional SPI (build:7601)
(name:WIN7-1-PC) (workgroup:WORKGROUP)
[*] Scanned 24 of 112 hosts (21% complete)
[*] Scanned 28 of 112 hosts (25% complete)
[*] Scanned 76 of 112 hosts (67% complete)
[*] Scanned 79 of 112 hosts (70% complete)
[*] Scanned 81 of 112 hosts (72% complete)
[*] Scanned 103 of 112 hosts (91% complete)
[*] Scanned 110 of 112 hosts (98% complete)
[*] Scanned 111 of 112 hosts (99% complete)
[*] Scanned 112 of 112 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) >
```

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

Hosts							
address	mac	name	os_name	os_flavor	os_sp	purpose	info comments
10.10.50.1	c0:67:af:c7:d9:88		10S	52.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:29:72:4d:c1	vc.coreddoocloud.qa	Linux	5.X		server	
10.10.50.100	00:0c:29:95:04:33	WIN7-PC	Windows 7	Professional	SP1	client	
10.10.50.200			Unknown			device	
10.10.50.202	00:0c:29:20:c4:a9	WIN7-1-PC	Windows 7	Professional	SP1	client	
10.10.50.210	00:0c:29:ea:bd:df		Linux	5.X		server	
10.10.50.211	00:0c:29:BA:AC:AA		FreeBSD	6.X		device	

Observe the OS\_Flavor field. SMB scanning scans for Operating System Flavor for the RHOST range configured.