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

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

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

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:

- 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

You can also download Advanced IP Scanner from 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

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

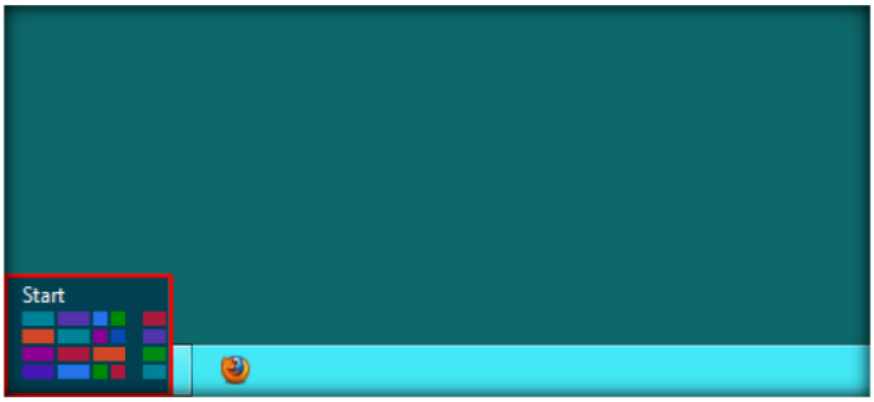


FIGURE 1.1: Windows 8 – Desktop view

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

FIGURE 1.2: Windows 8 – Apps

With Advanced IP Scanner, you can scan hundreds of IP addresses simultaneously.

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

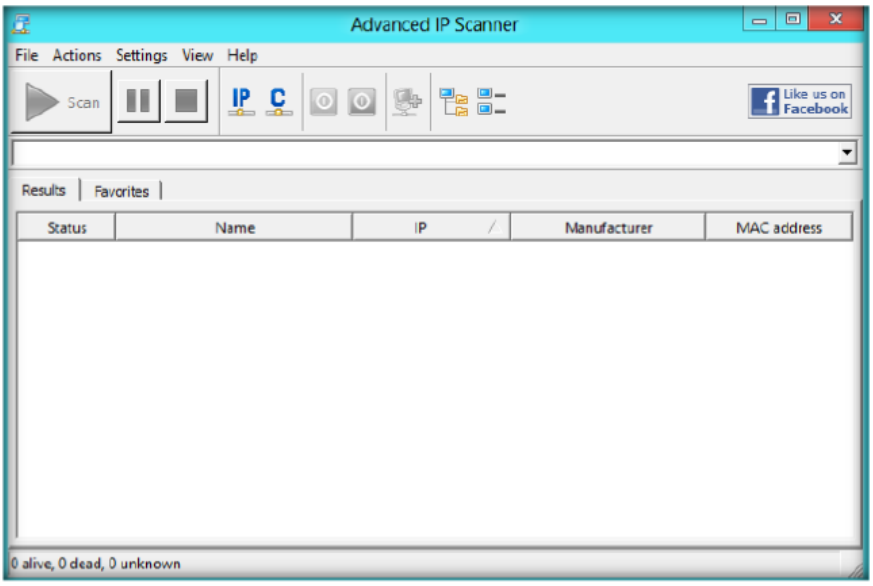


FIGURE 1.3: The Advanced IP Scanner main window

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

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

You have to guess a range of IP address of victim machine.

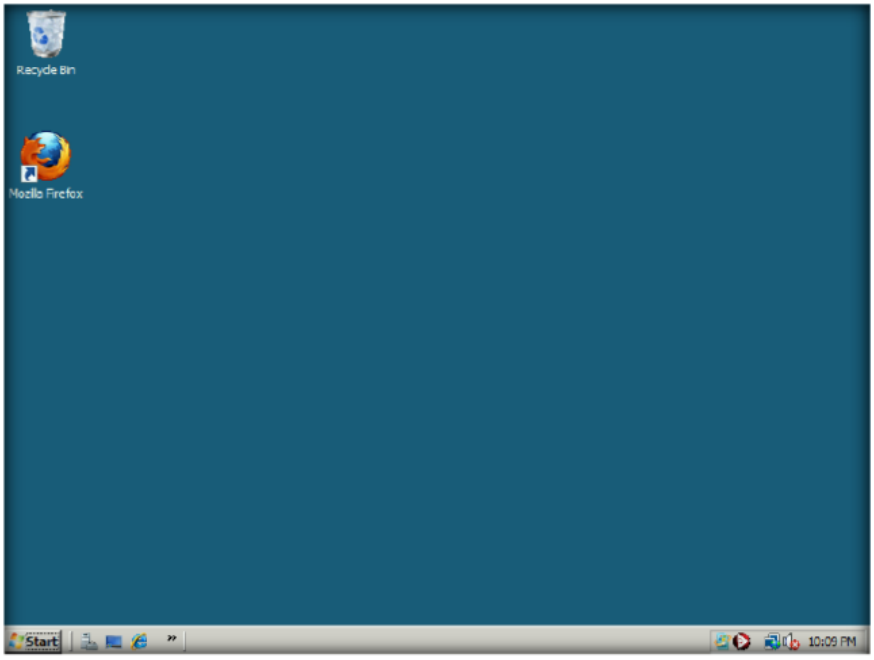


FIGURE 1.4: The victim machine Windows server 2008

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.

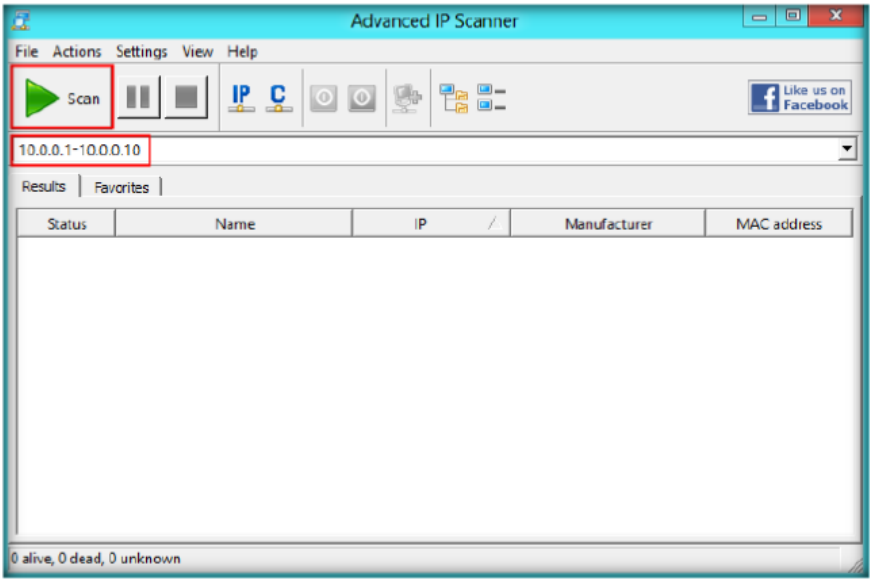


FIGURE 1.5: The Advanced IP Scanner main window with IP address range

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

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.

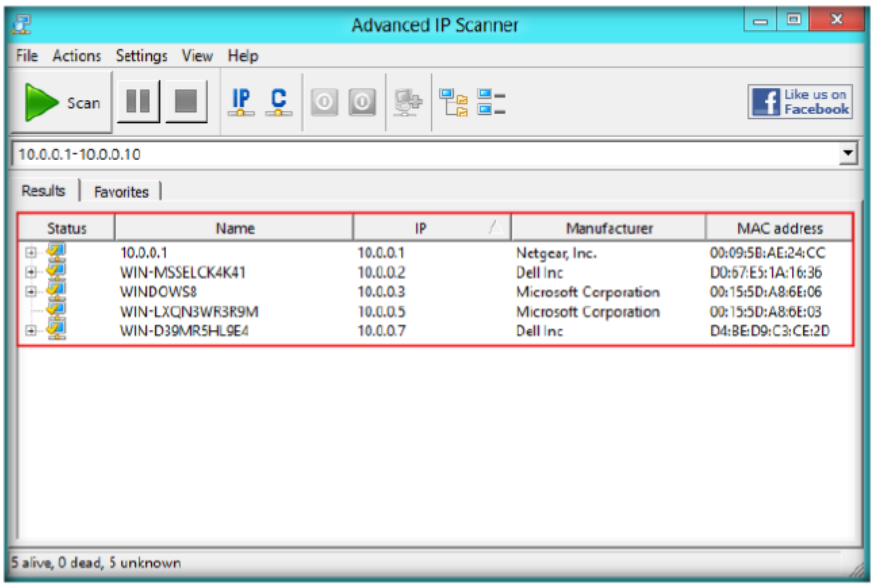


FIGURE 1.6: The Advanced IP Scanner main window after scanning

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.

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**, **Shut down**, and **Abort Shut down**

TASK 2

Extract Victim's IP Address Info

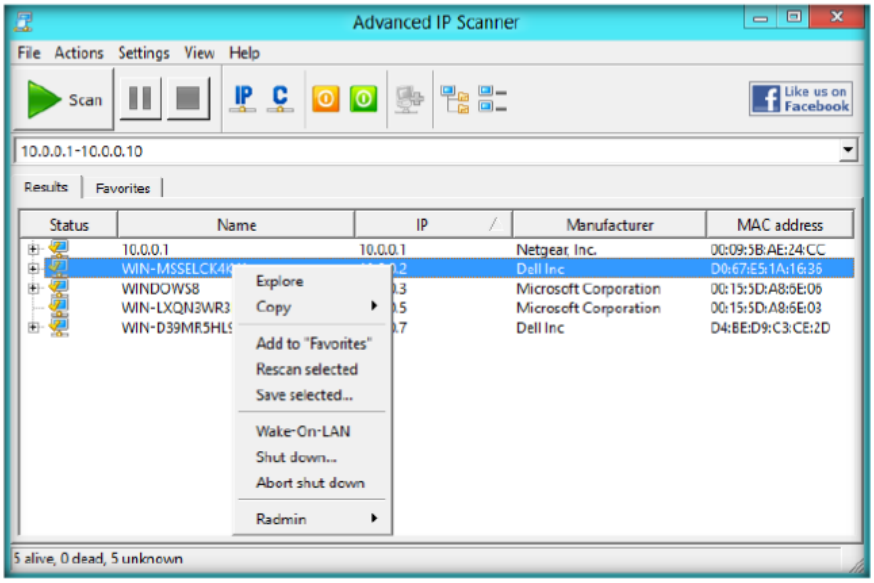


FIGURE 1.7: The Advanced IP Scanner main window with Alive Host list

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

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

Winfingerprint Input Options:

- IP Range (Netmask and Inverted Netmask supported) IP ListSingle Host Neighborhood

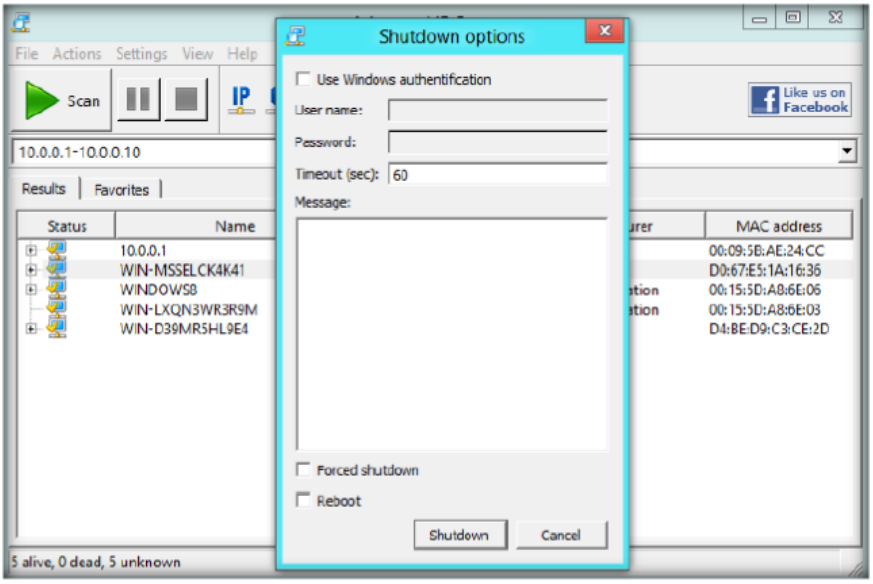


FIGURE 1.8: The Advanced IP Scanner Computer properties window

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	**Scan Information:** ▪ 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	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

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:

- Identify the domain IP address
- Identify the domain information

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

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

TASK 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 **Sever Query** tab

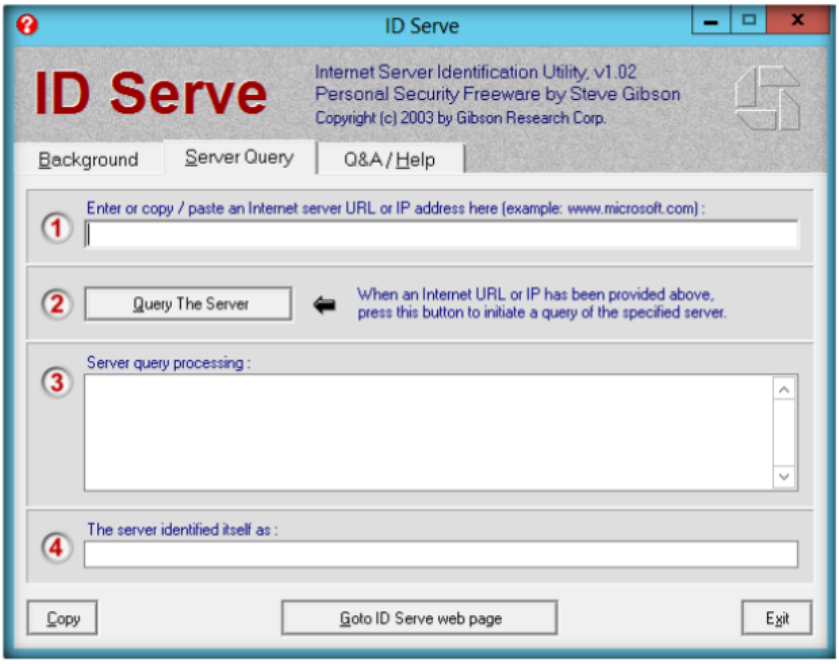


FIGURE 2.1: Main window of ID Serve

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

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

ID Serve can accept the URL or IP as a command-line parameter

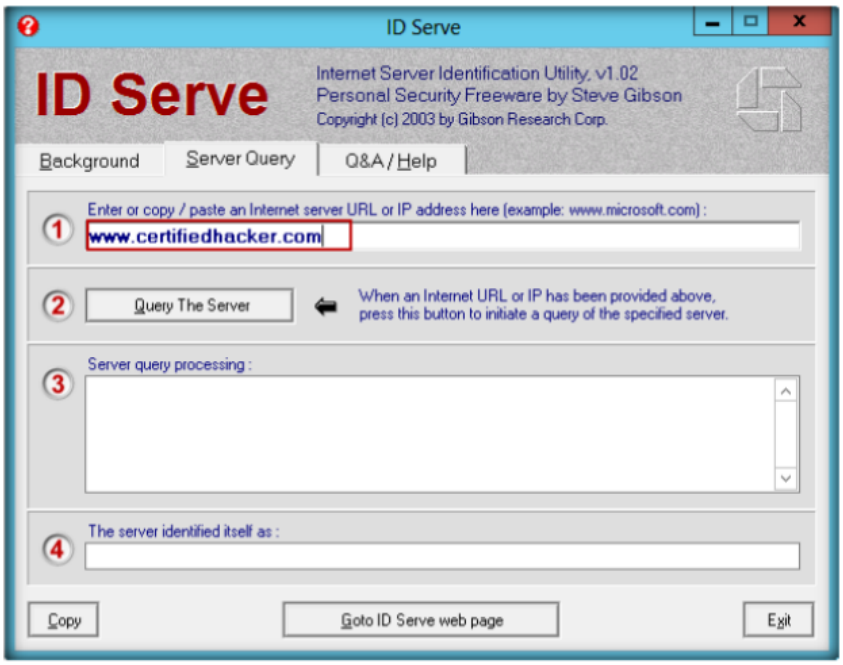


FIGURE 2.2: Entering the URL for query

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

ID Serve can also connect with non-web servers to receive and report that server's greeting message. This generally reveals the server's make, model, version, and other potentially useful information.

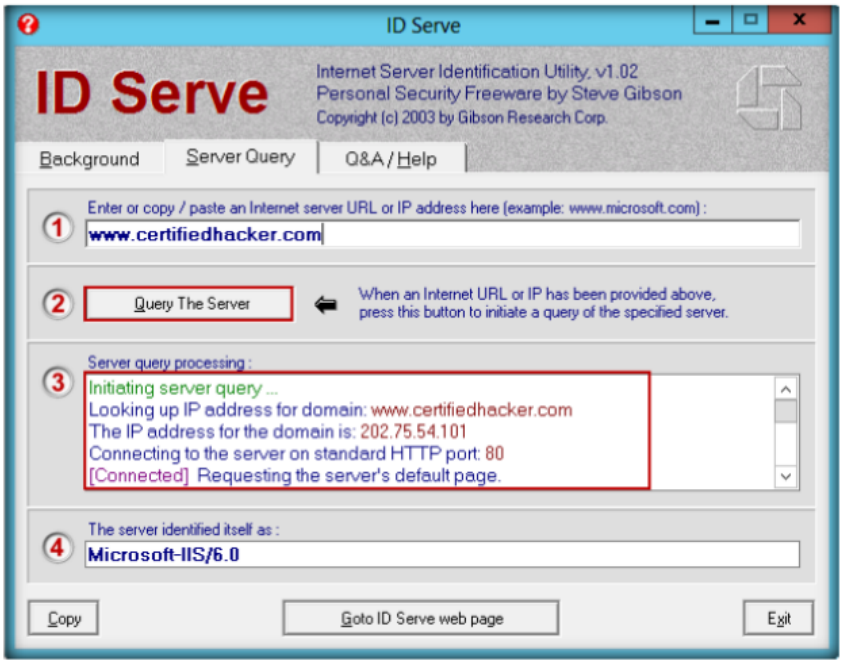


FIGURE 2.3: Server processed information

Lab Analysis

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

Tool/Utility	Information Collected/Objectives Achieved
ID Serve	**IP address:** 202.75.54.101
	Server Connection: Standard HTTP port: 80
	Response headers returned from server: ▪ 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	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 3

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.

Lab Tasks

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**.

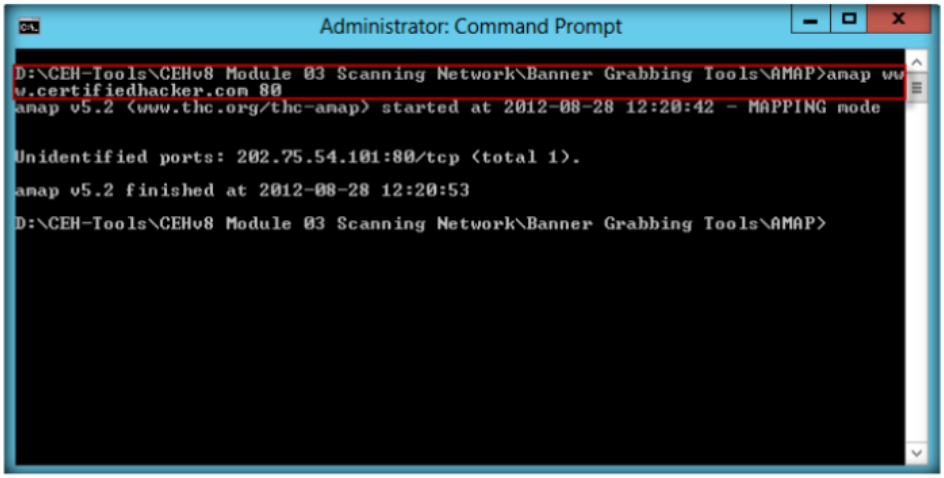


FIGURE 3.1: Amap with host name www.certifiedhacker.com with Port 80

Syntax: amap [-A|-B|-P|-W] [-1buSRHUdqv] [[-m] -o <file>]

[-D <file>] [-t/-T sec] [-c cons] [-C retries]

[-p proto] [-i <file>] [target port [port] ...]

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

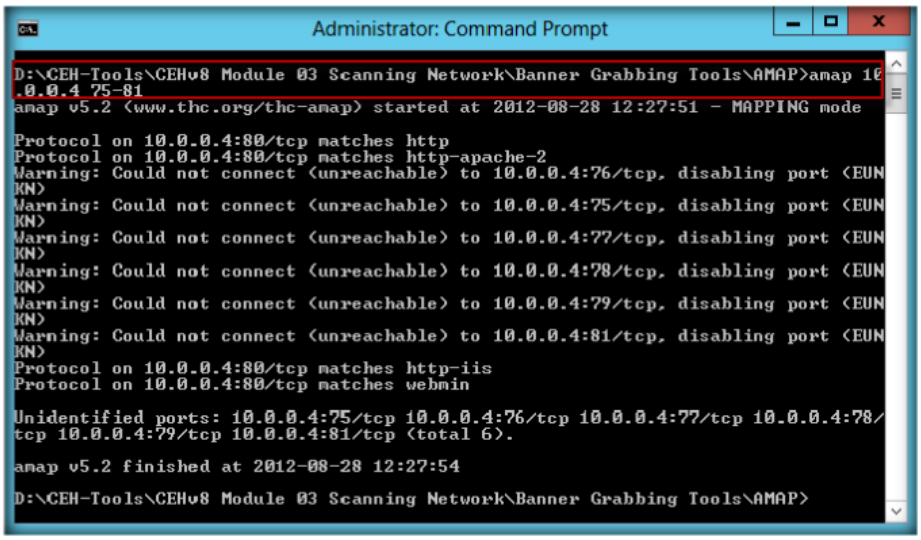


FIGURE 3.2: Amap with IP address and with range of switches 75-81

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
Amap	**Identified open port:** 80
	WebServers: ▪ http-apache-2 ▪ http-iis ▪ 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

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	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ 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 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

1. Launch **Currports**. It **automatically displays** the process name, ports, IP and remote addresses, and their states.

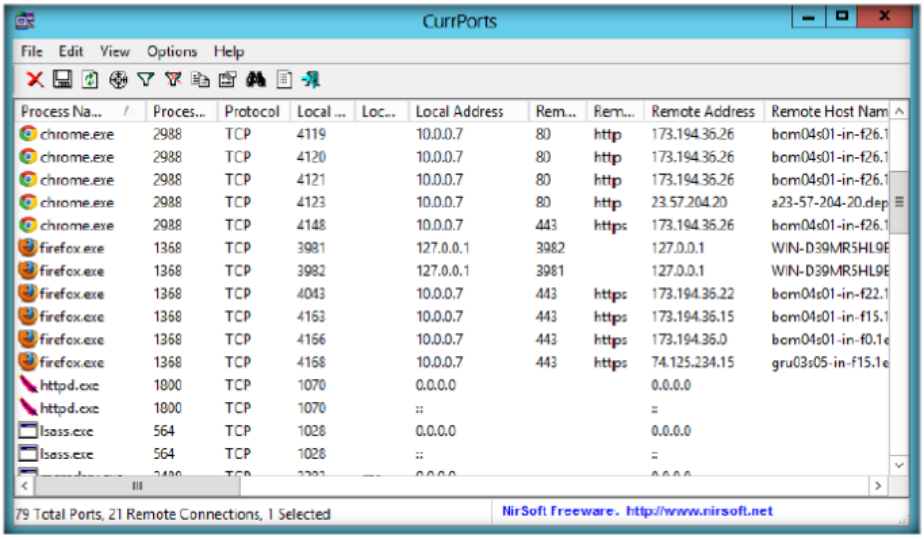


FIGURE 4.1: The CurrPorts main window with all processes, ports, and IP addresses

2. CurrPorts lists all the **processes** and their IDs, protocols used, **local and remote IP address**, local and remote ports, and **remote host names**.

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

3. To view all the reports as an HTML page, click **View → HTML Reports - All Items**.

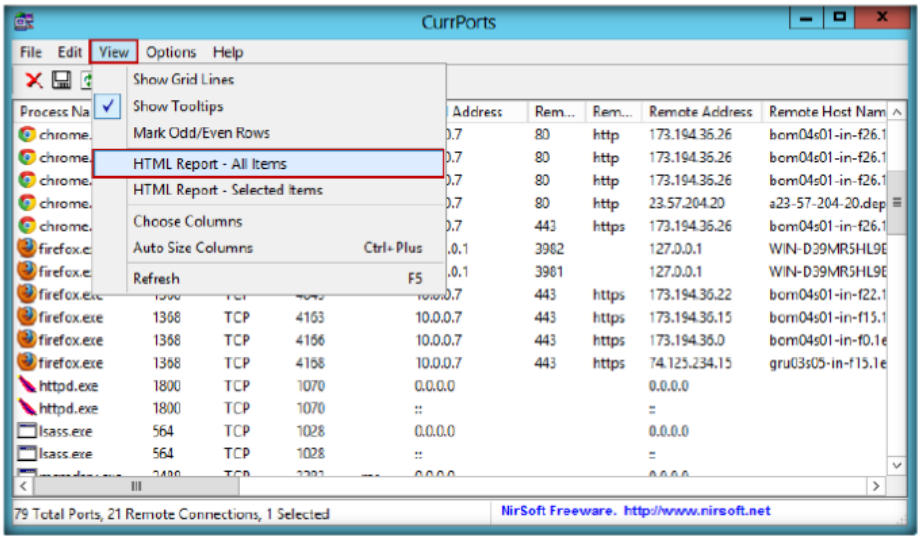
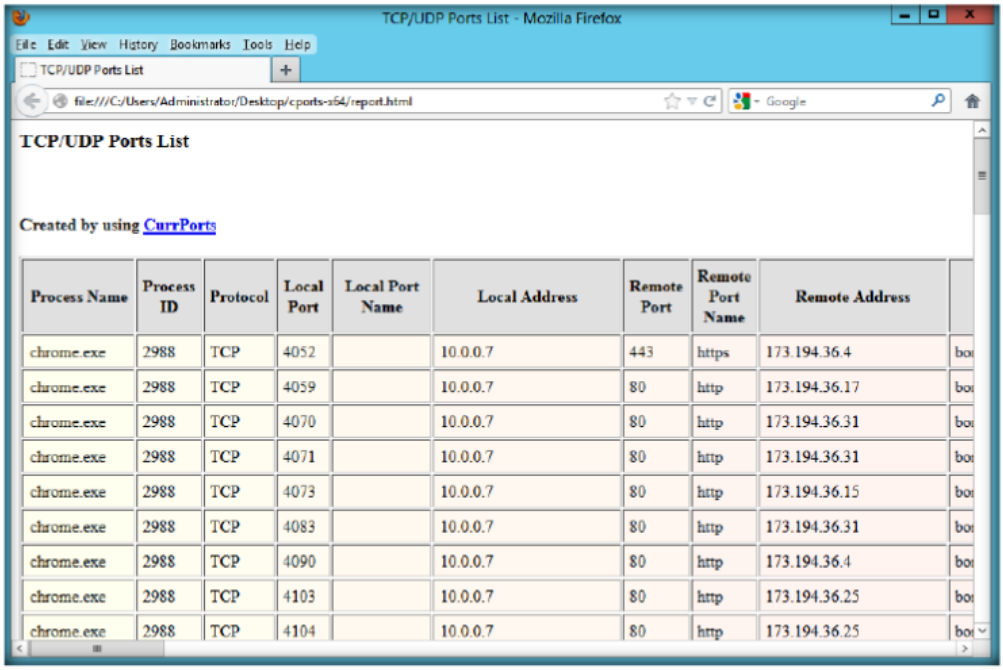


FIGURE 4.2: The CurrPorts with HTML Report – All Items

In the bottom left of the CurrPorts window, the status of total ports and remote connections displays.

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



Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address
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

To check the countries of the remote IP addresses, you have to download the latest IP to Country file. You have to put the 'IpToCountry.csv' file in the same folder as cports.exe.

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.

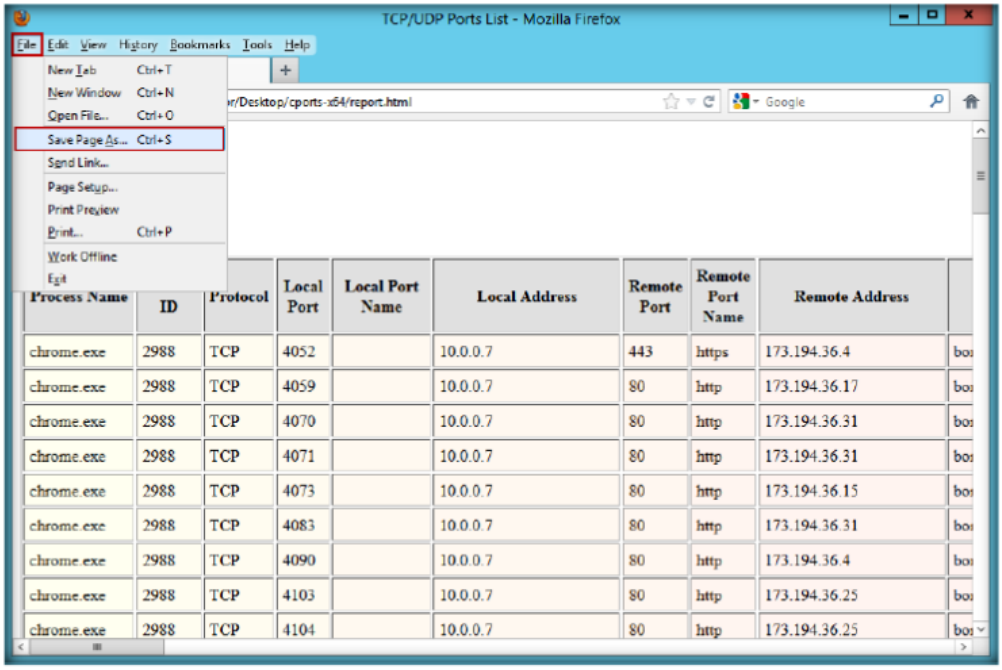


FIGURE 4.4: The Web browser to Save CurrPorts Report – All Items

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

Be aware! The log file is updated only when you refresh the ports list manually, or when the Auto Refresh option is turned on.

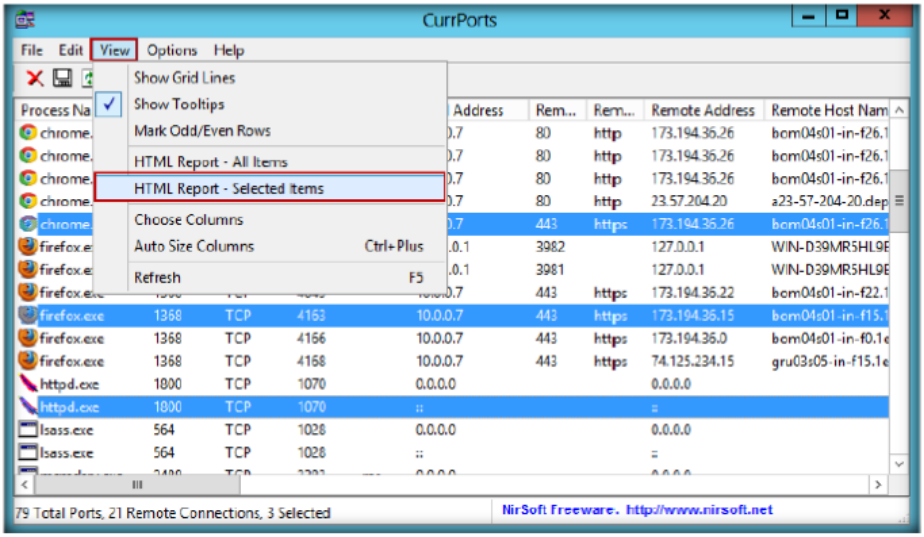


FIGURE 4.5: CurrPorts with HTML Report – Selected Items

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

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

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

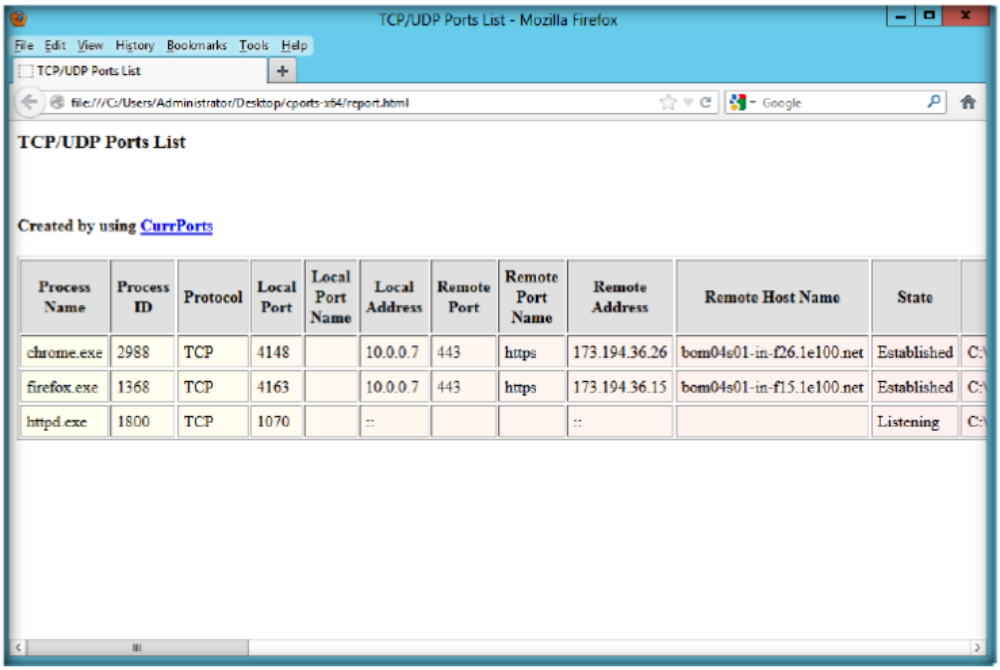


FIGURE 4.6: The Web browser displaying CurrPorts with HTML Report – Selected Items

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**.

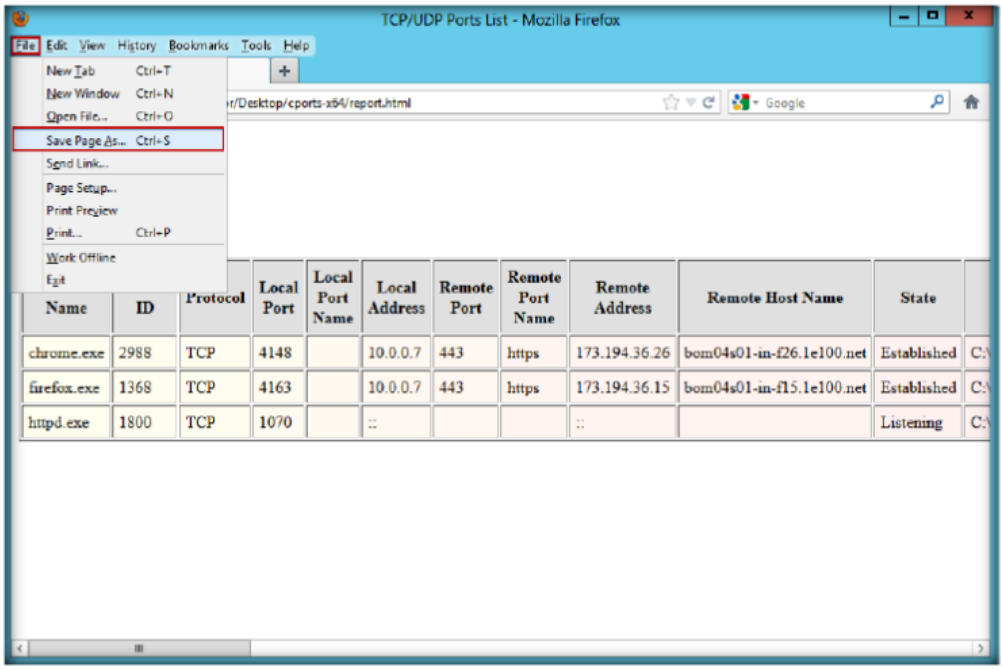


FIGURE 4.7: The Web browser to Save CurrPorts with HTML Report – Selected Items

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**.

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

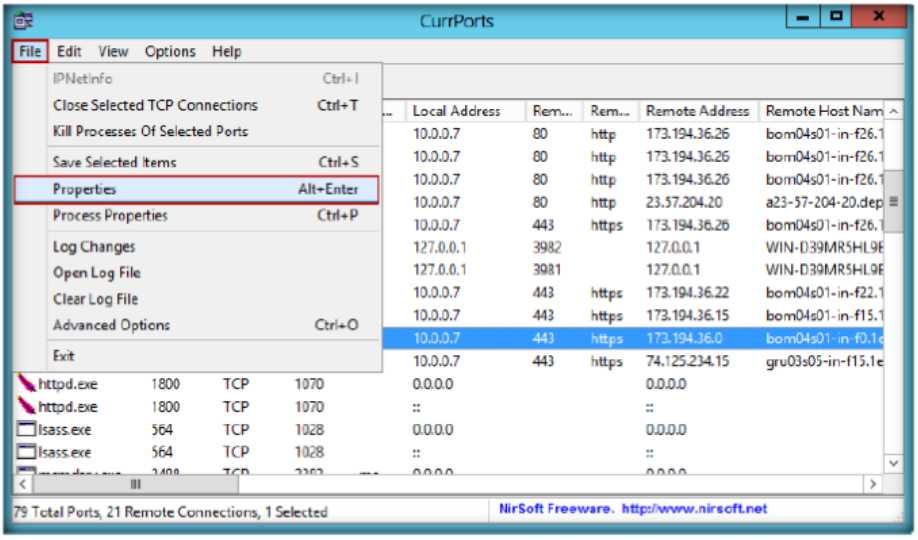


FIGURE 4.8: CurrPorts to view properties for a selected port

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: /shtml <Filename> means save the list of all opened TCP/UDP ports into an HTML file (Horizontal).

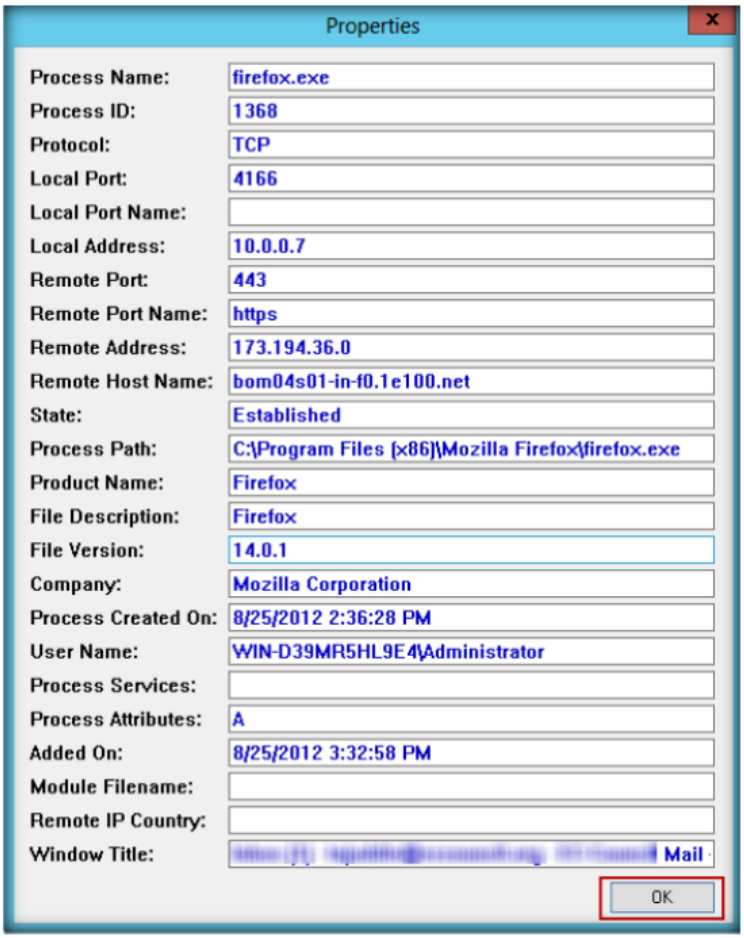


FIGURE 4.9: The CurrPorts Properties window for the selected port

TASK 2

Close TCP Connection

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

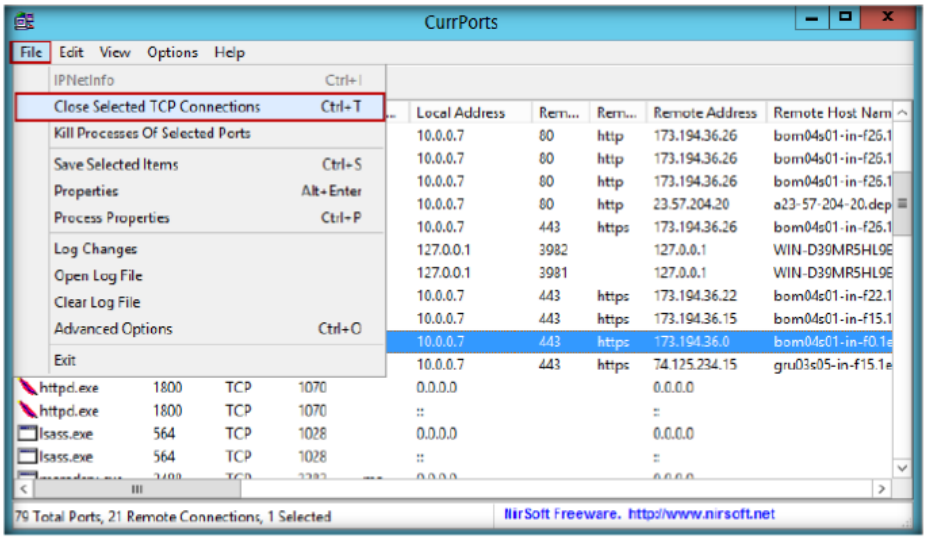


FIGURE 4.10: The CurrPorts Close Selected TCP Connections option window

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

TASK 3

Kill Process

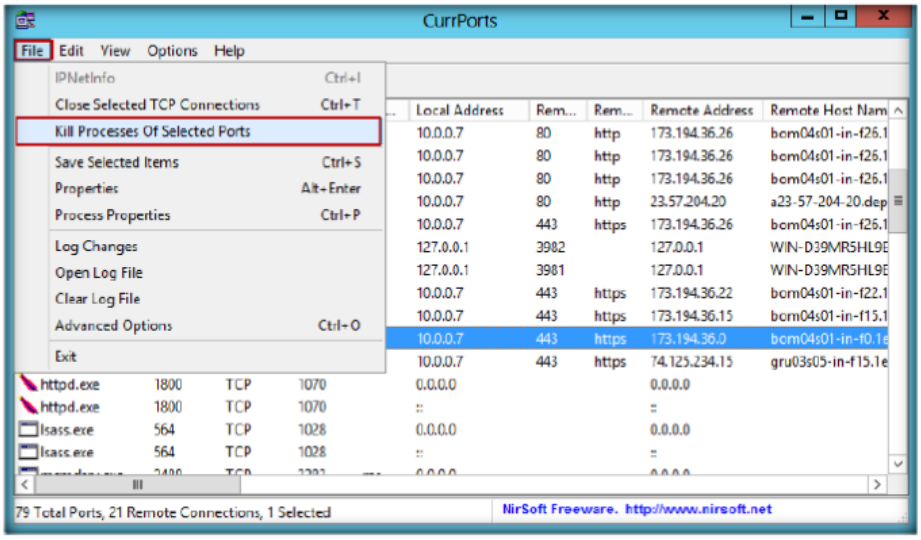


FIGURE 4.11: The CurrPorts Kill Processes of Selected Ports Option Window

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

Command-line option: /sverhtml <Filename> Save the list of all opened TCP/UDP ports into HTML file (Vertical).

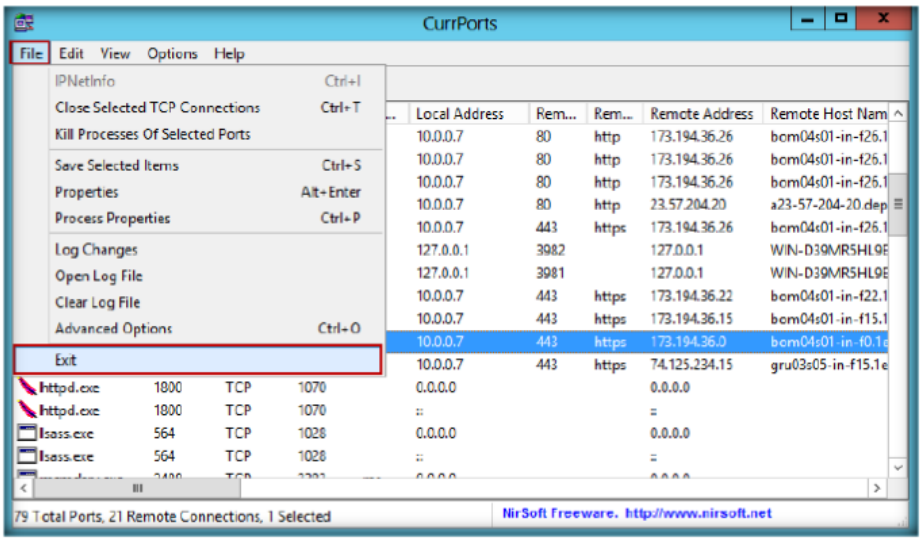


FIGURE 4.12: The CurrPorts Exit option window

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	**Profile Details:** Network scan for open ports
	Scanned Report: ▪ 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

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.

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

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 compatibly 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.

TASK 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

1. Navigate to **Windows Server 2012** and launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

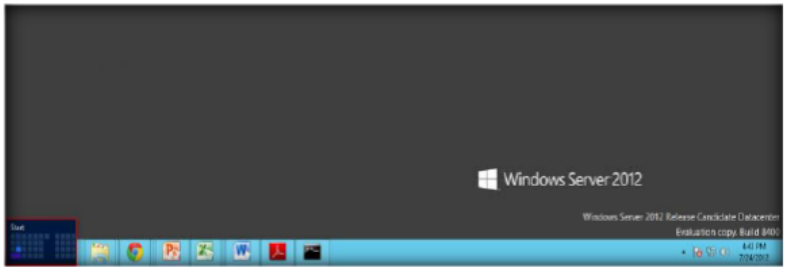


FIGURE 5.1: Windows Server 2012 – Desktop view

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

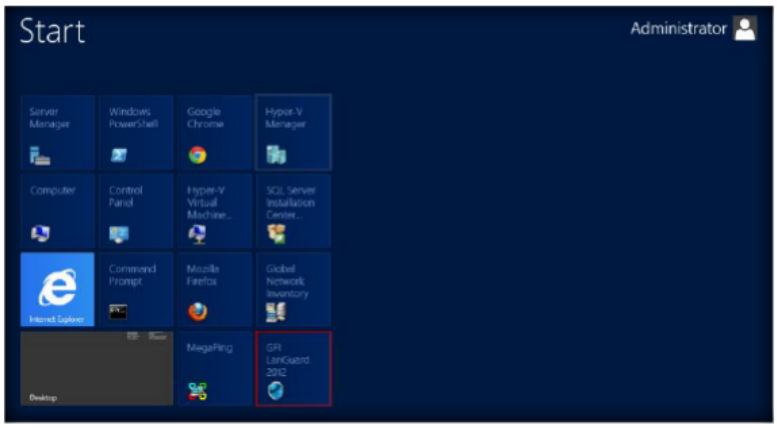


FIGURE 5.2: Windows Server 2012 – Apps

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.

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

FIGURE 5.3: The GFI LANguard main window

Custom scans are recommended:

- When performing a onetime scan with particular scanning parameters/profiles
- When performing a scan for particular network threats and/or system information
- To perform a target computer scan using a specific scan profile

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**.

For large network environments, a Microsoft SQL Server/MSDE database backend is recommended instead of the Microsoft Access database.

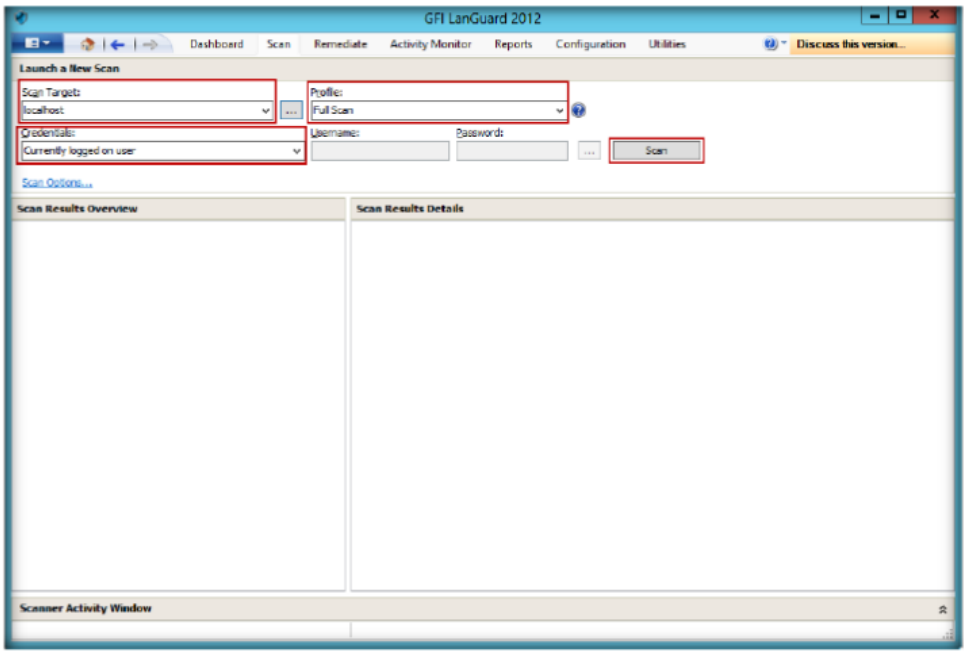


FIGURE 5.5: Selecting an option for network scanning

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

Quick scans have relatively short scan duration times compared to full scans, mainly because quick scans perform vulnerability checks of only a subset of the entire database. It is recommended to run a quick scan at least once a week.

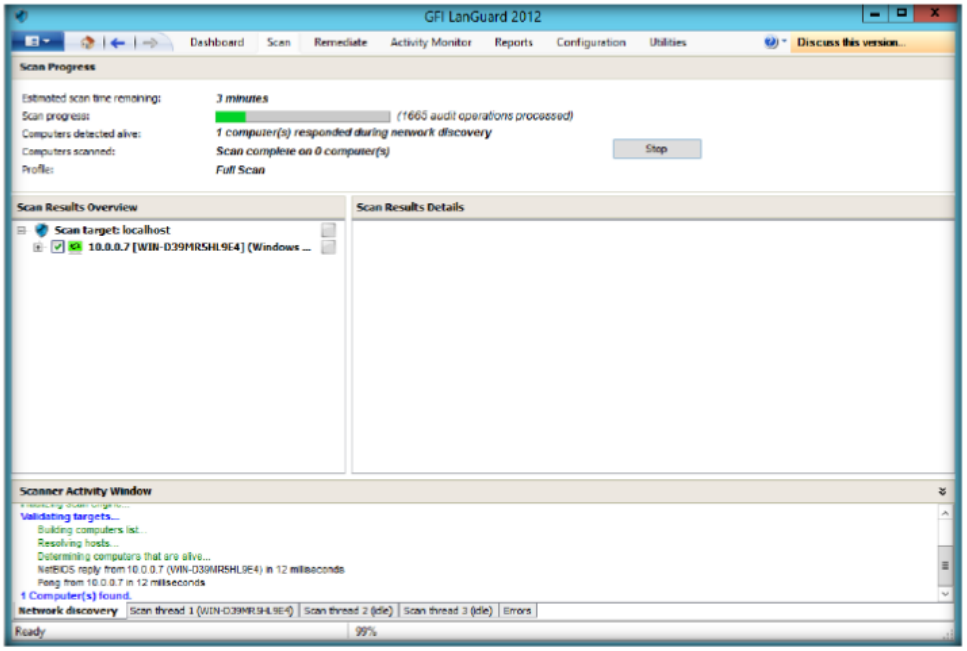


FIGURE 5.6: The GFI LanGuard scanning a network

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

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.

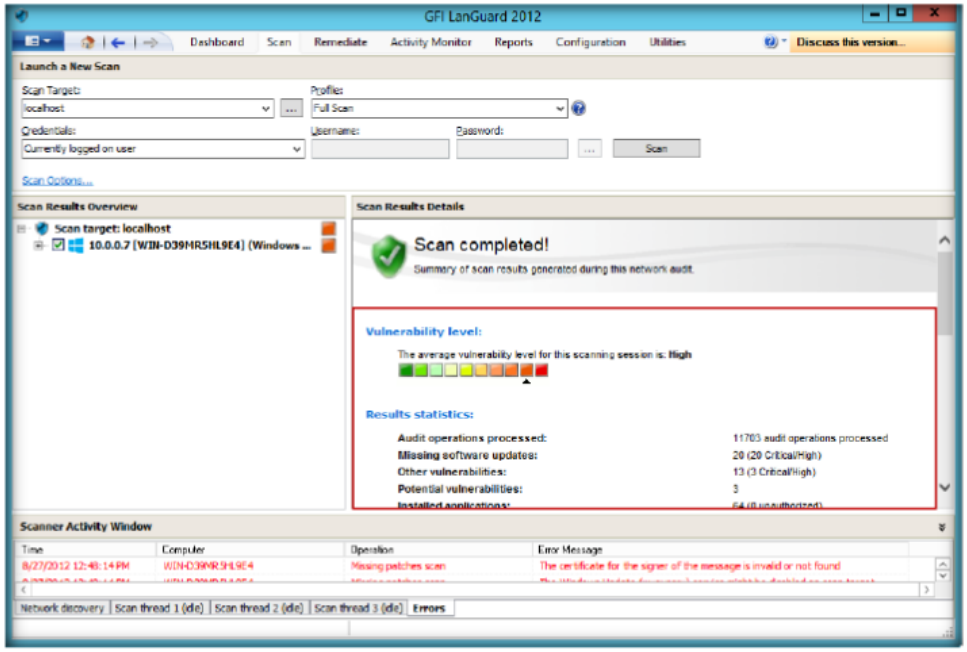


FIGURE 5.7: The GFI LanGuard Custom scan wizard

9. To check the Scan Result Overview, click **IP address** of the machinein the right panel
10. It shows the **Vulnerability Assessment and Network & Software Audit**; click **Vulnerability Assessment**

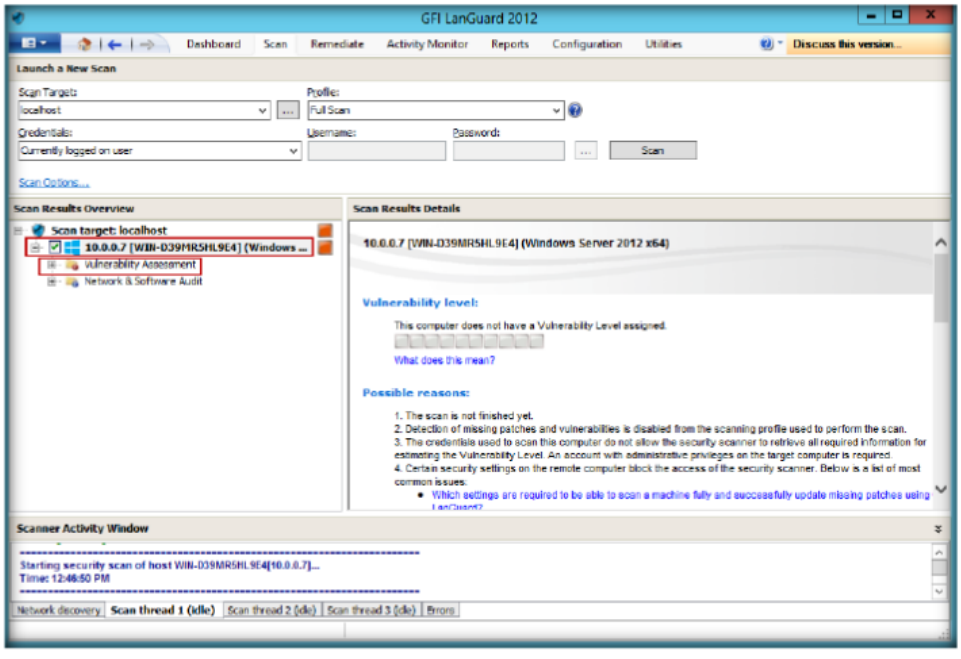


FIGURE 5.8: Selecting Vulnerability Assessment option

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

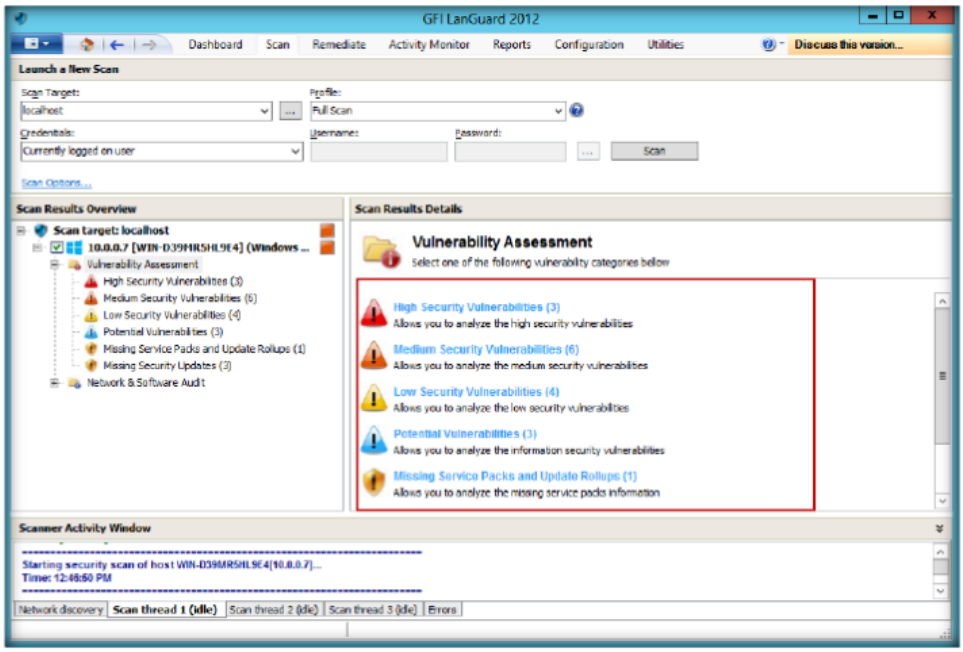


FIGURE 5.9: List of Vulnerability Assessment categories

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.

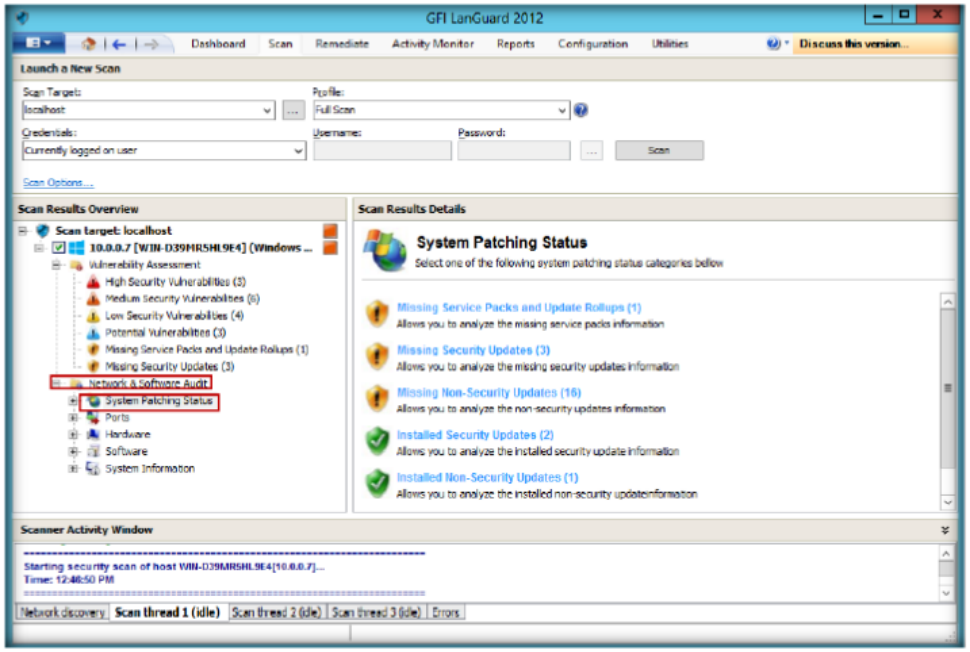


FIGURE 5.10: System patching status report

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

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

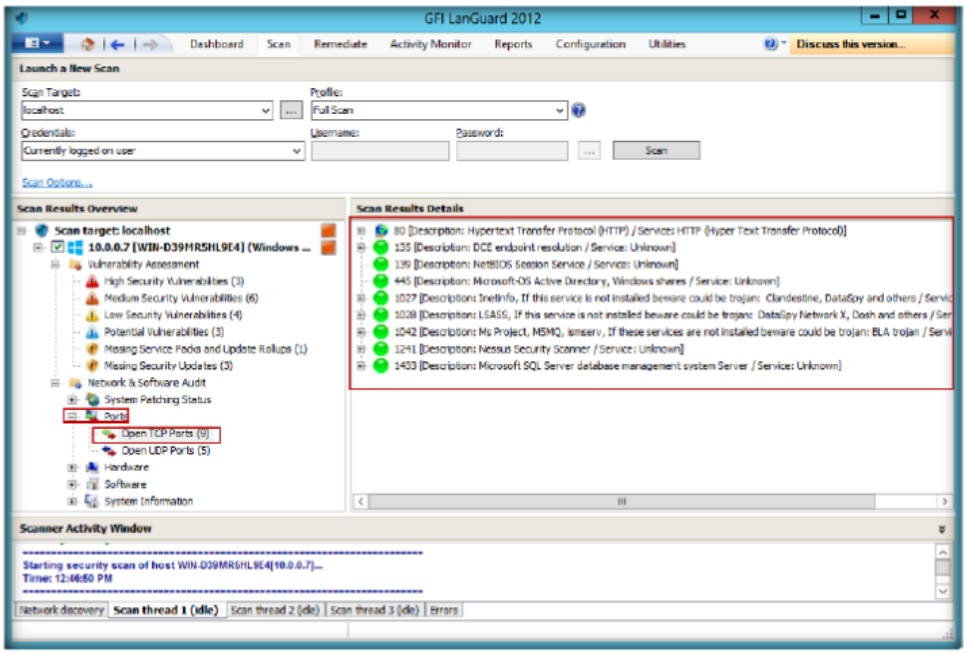


FIGURE 5.11: TCP/UDP Ports result

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

The next job after a network security scan is to identify which areas and systems require your immediate attention. Do this by analyzing and correctly interpreting the information collected and generated during a network security scan.

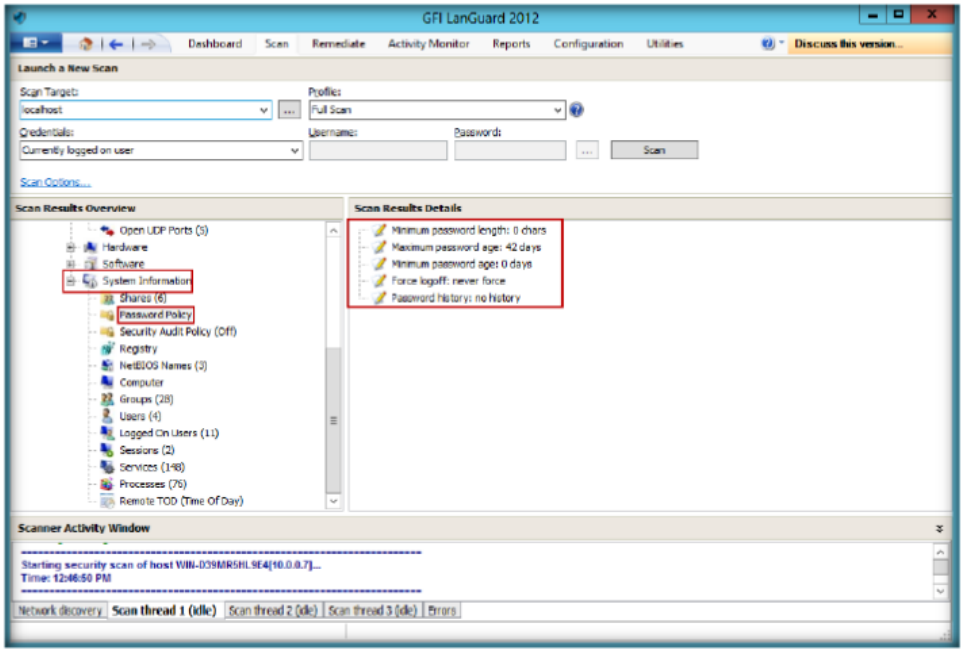


FIGURE 5.12: Information of Password Policy

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

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.

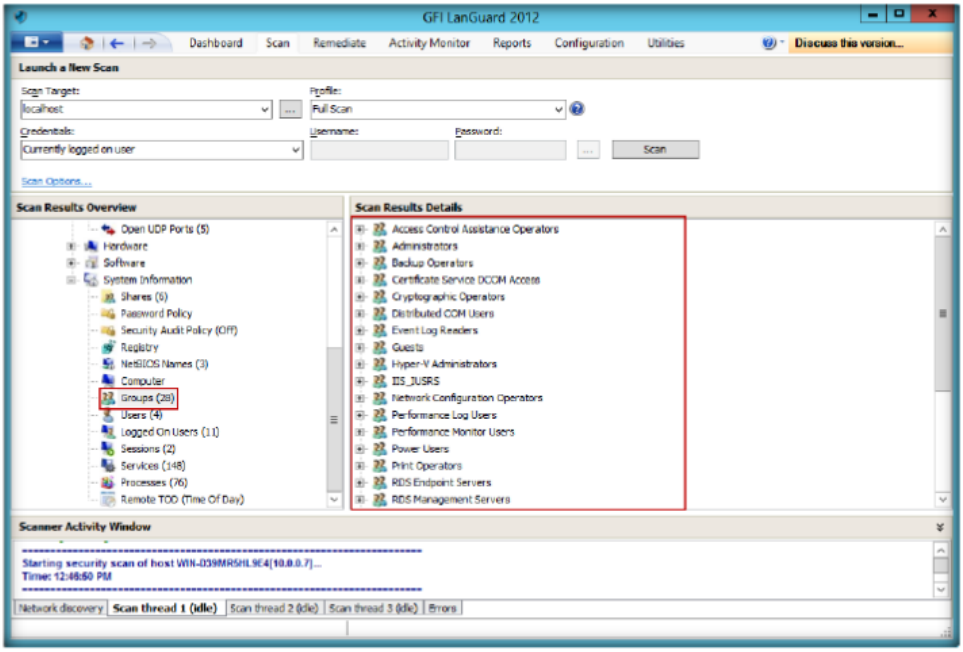


FIGURE 5.13: Information of Groups

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

It is recommended to use scheduled scans:

- To perform periodical/regular network vulnerability scans automatically and using the same scanning profiles and parameters
- To trigger scans automatically after office hours and to generate alerts and auto-distribution of scan results via email
- To automatically trigger auto-remediation options, (e.g., Auto download and deploy missing updates)

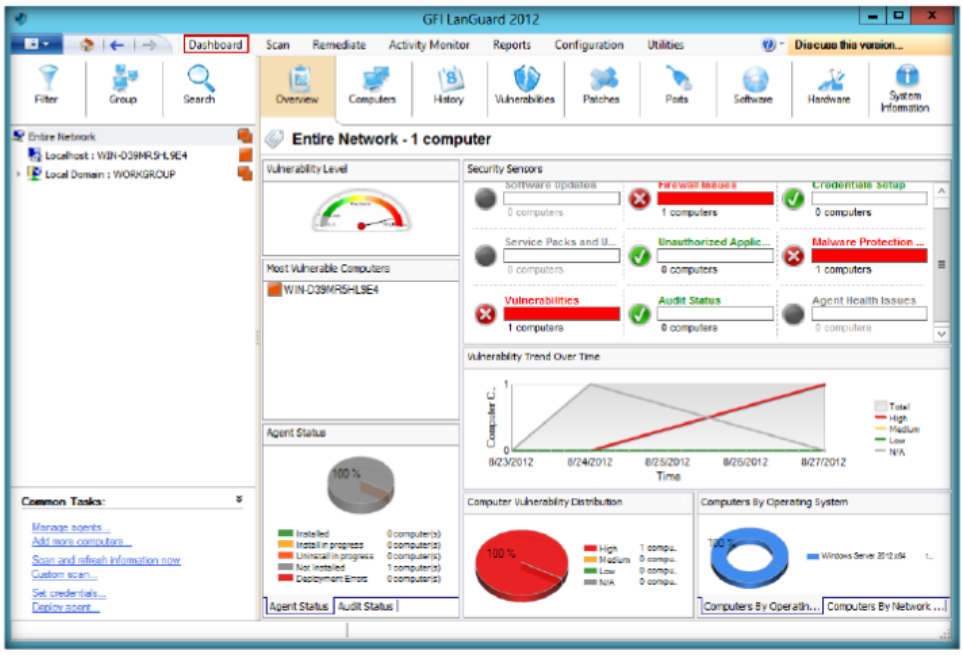


FIGURE 5.14: scanned report of the network

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 ▪ 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	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 6

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

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

- 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

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

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

Lab Tasks

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

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

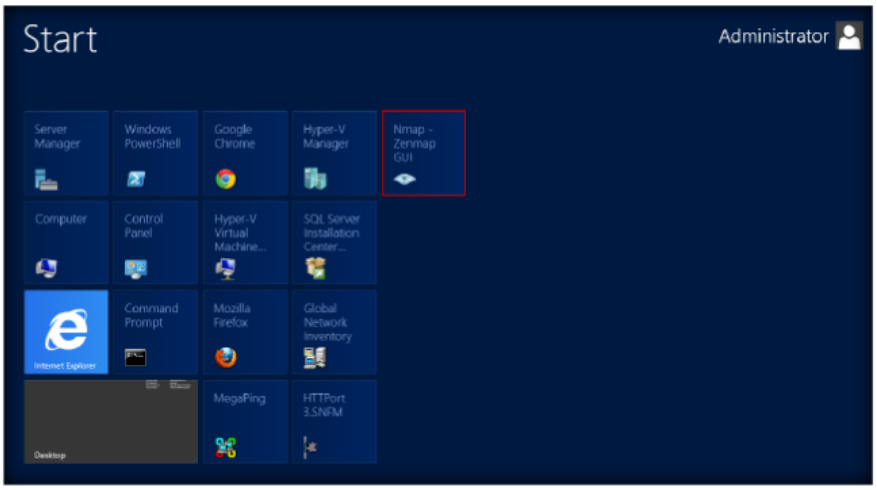


FIGURE 6.2: Windows Server 2012 – Apps

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

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

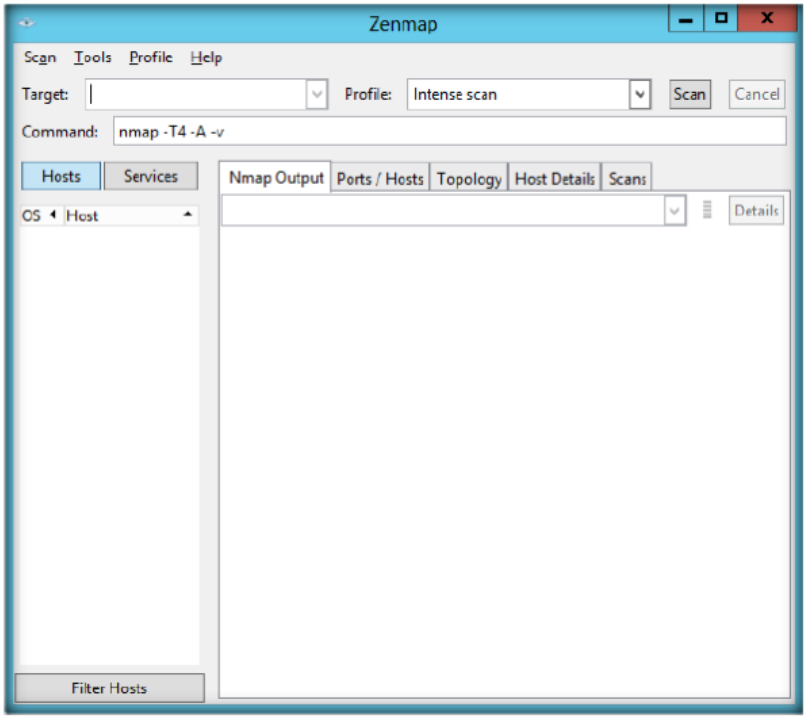


FIGURE 6.3: The Zenmap main window

Nmap Syntax: nmap [Scan Type(s)] [Options] {target specification}

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.

4. 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.
5. In this lab, the IP address would be **10.0.0.4**; it will be different from your lab environment
6. 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**.

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

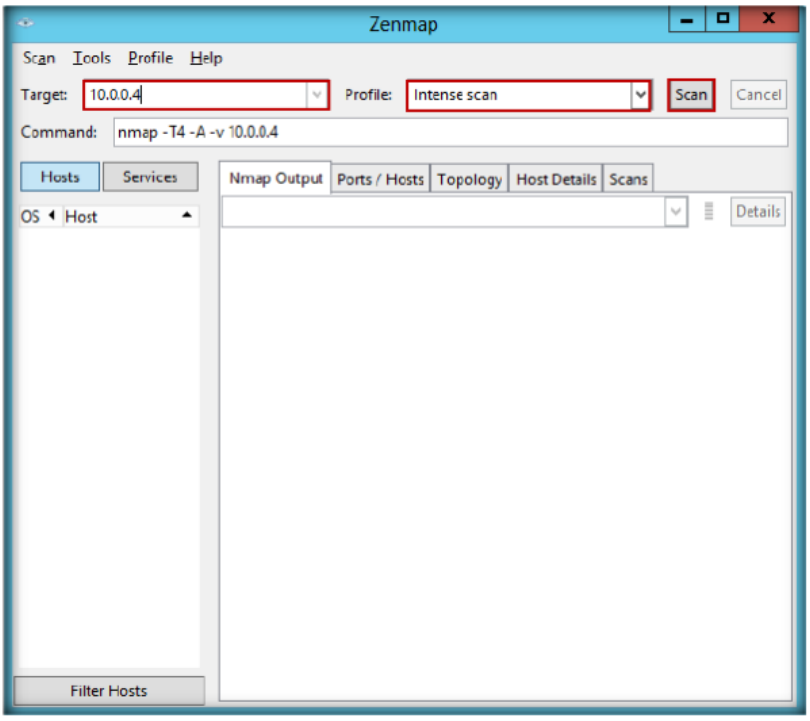


FIGURE 6.4: The Zenmap main window with Target and Profile entered

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.

The six port states recognized by Nmap:

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

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

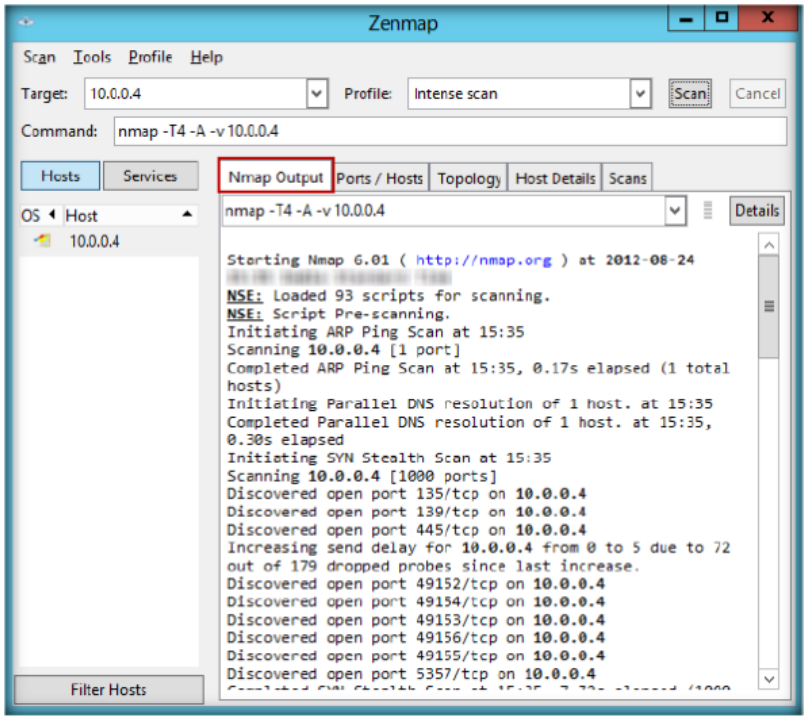


FIGURE 6.5: The Zenmap main window with the Nmap Output tab for Intense Scan

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

9. 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)

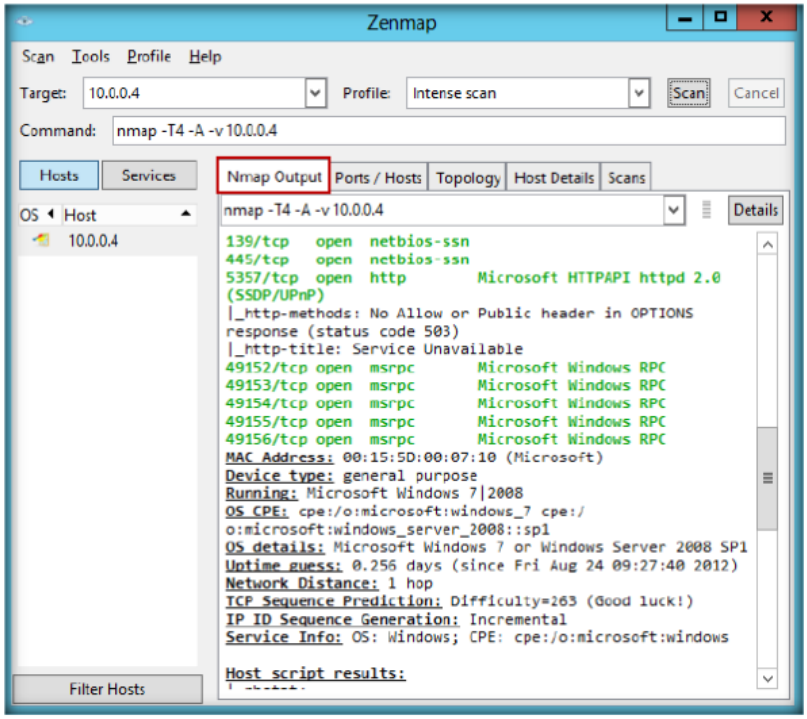


FIGURE 6.6: The Zenmap main window with the Nmap Output tab for Intense Scan

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.

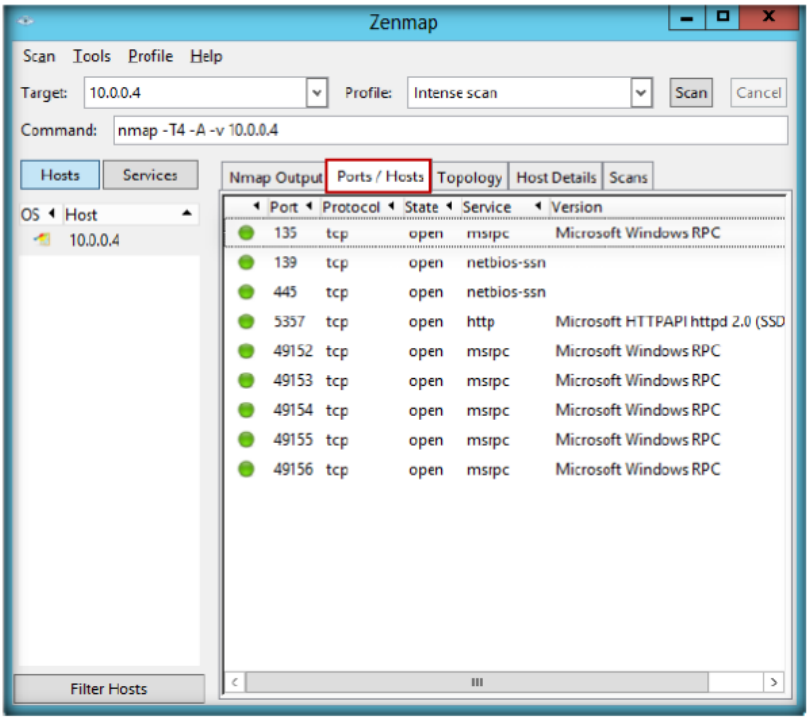


FIGURE 6.7: The Zenmap main window with the Ports/Hosts tab for Intense Scan

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

By default, Nmap performs a host discovery and then a port scan against each host it determines to be on line.

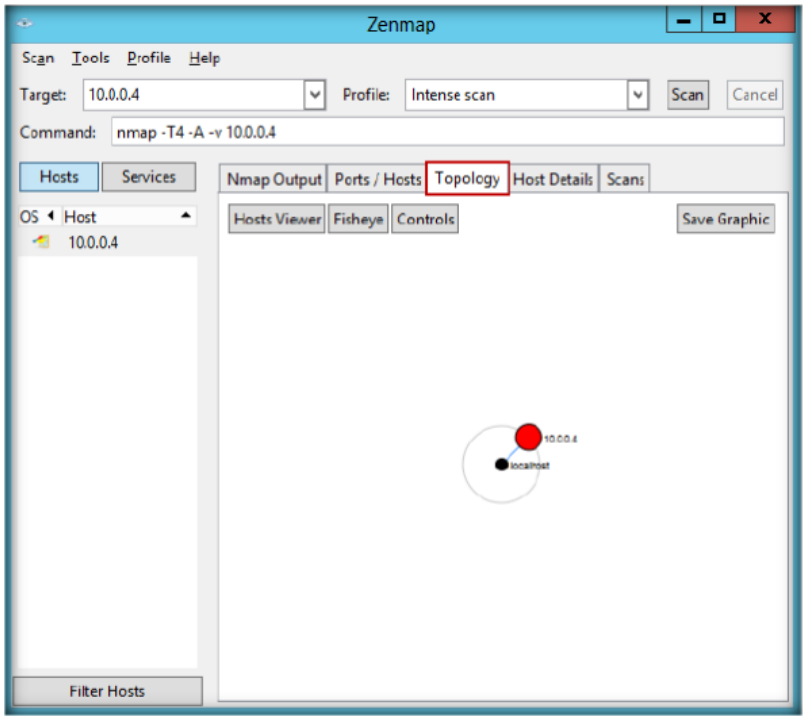


FIGURE 6.8: The Zenmap main window with Topology tab for Intense Scan

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

By default, Nmap determines your DNS servers (for rDNS resolution) from your resolv.conf file (UNIX) or the Registry (Win32).

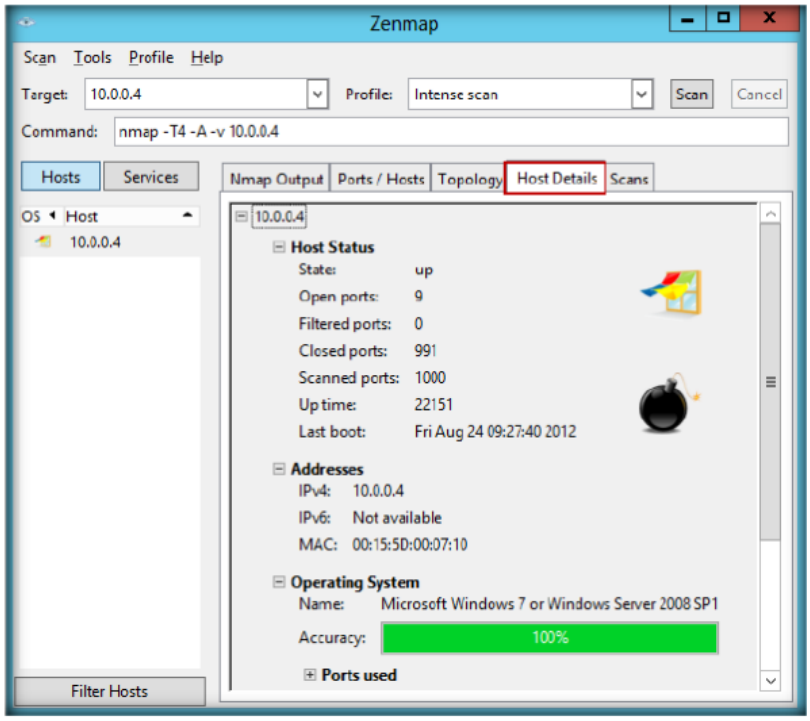


FIGURE 6.9: The Zenmap main window with Host Details tab for Intense Scan

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

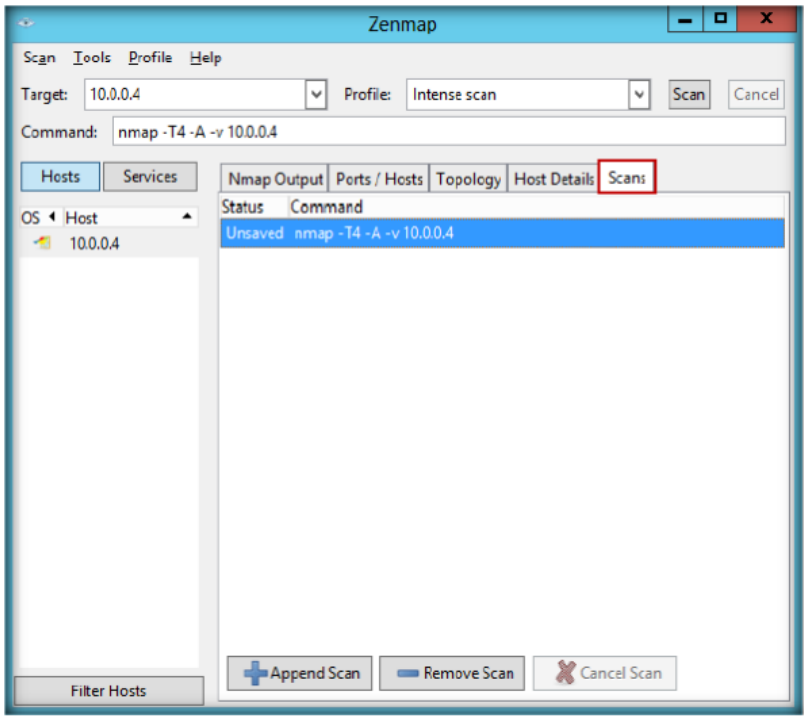


FIGURE 6.10: The Zenmap main window with Scan tab for Intense Scan

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

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

15. Now, click the **Services** tab located in the right pane of the window. This tab displays the **list** of services.

16. Click the **http** service to list all the HTTP Hostnames/**IP addresses**, Ports, and their **states** (Open/Closed).

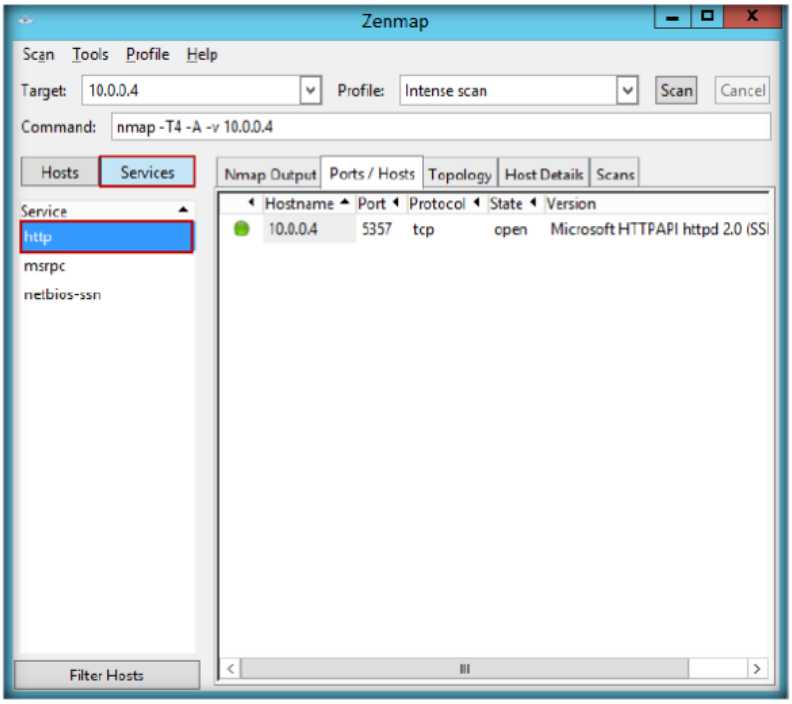


FIGURE 6.11: The Zenmap main window with Services option for Intense Scan

In Nmap, option -F means fast (limited port) 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

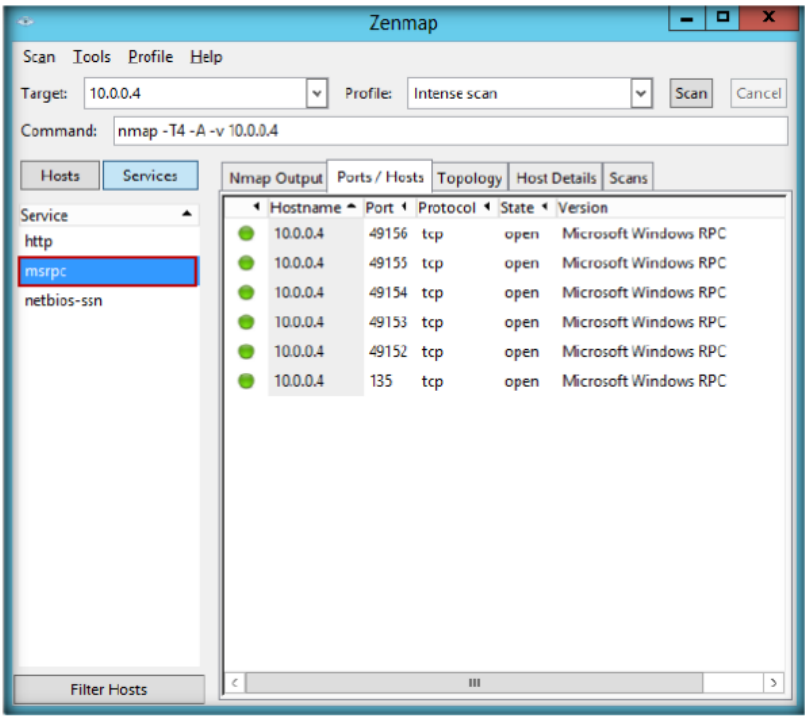


FIGURE 6.12: The Zenmap main window with msrpc Service for Intense Scan

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

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

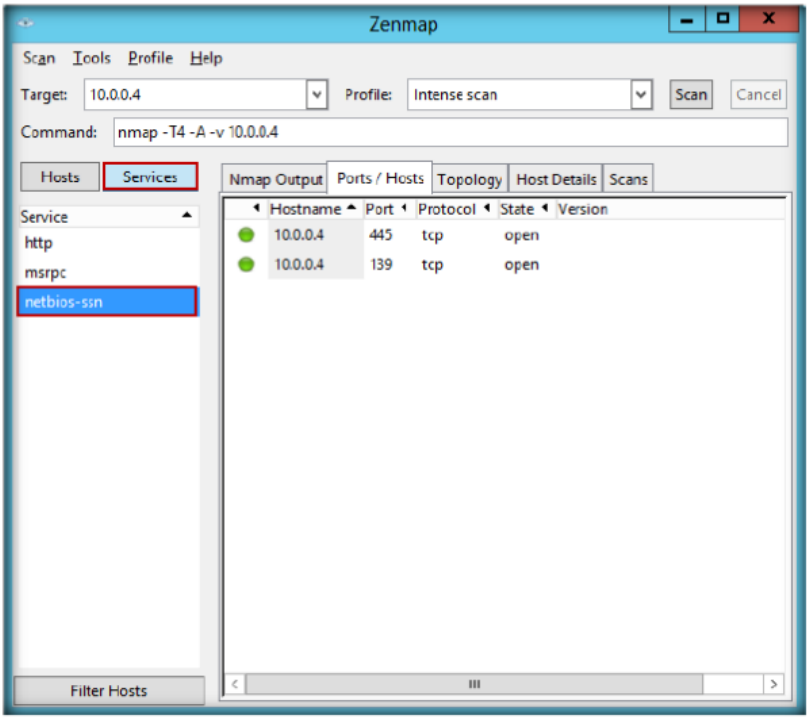


FIGURE 6.13: The Zenmap main window with netbios-ssn Service for Intense Scan

TASK 2

Xmas 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

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.

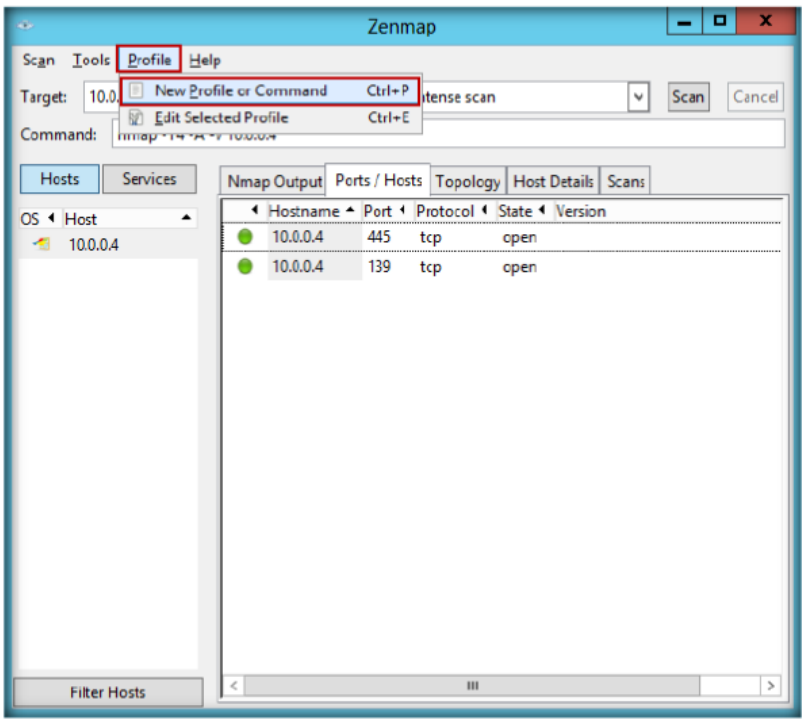


FIGURE 6.14: The Zenmap main window with New Profile or Command menu option

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

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

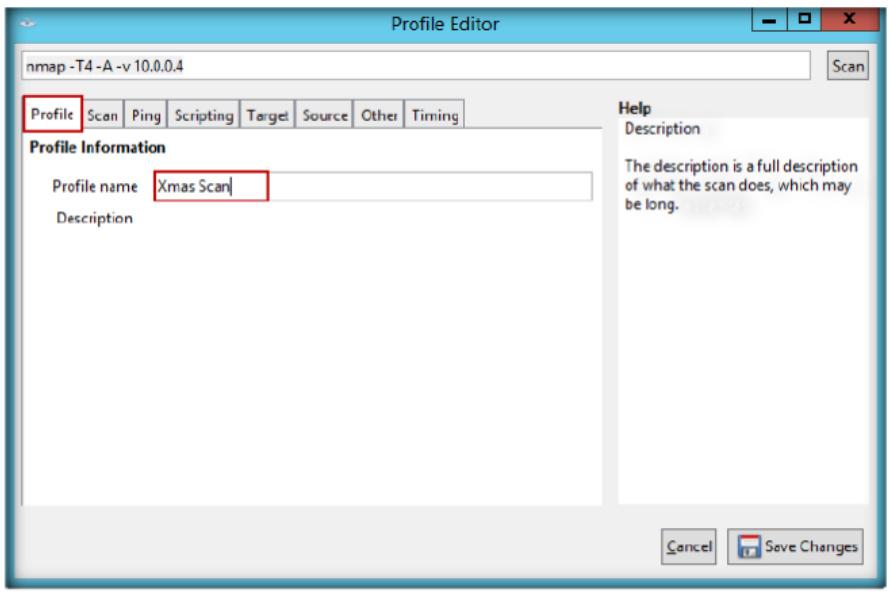


FIGURE 6.15: The Zenmap Profile Editor window with the Profile tab

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

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.

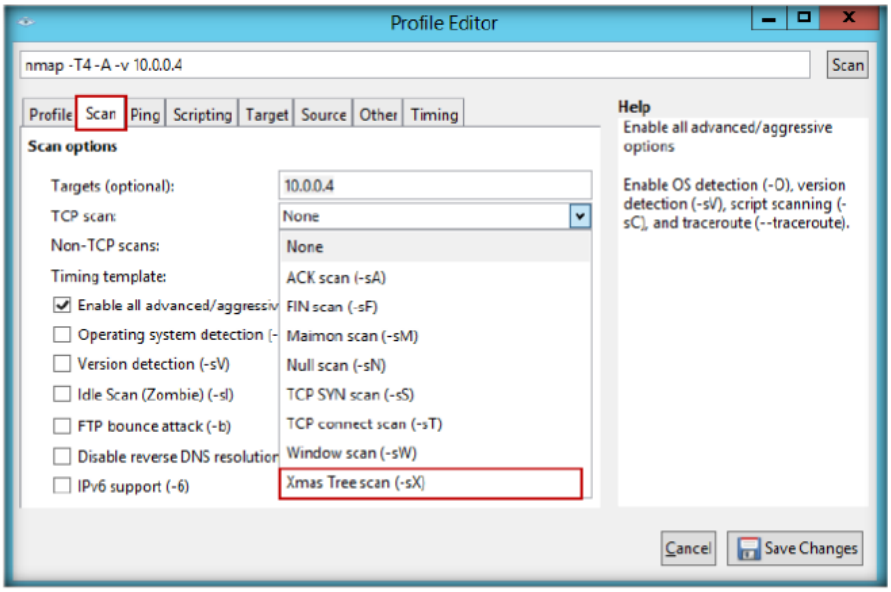


FIGURE 6.16: The Zenmap Profile Editor window with the Scan tab

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

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

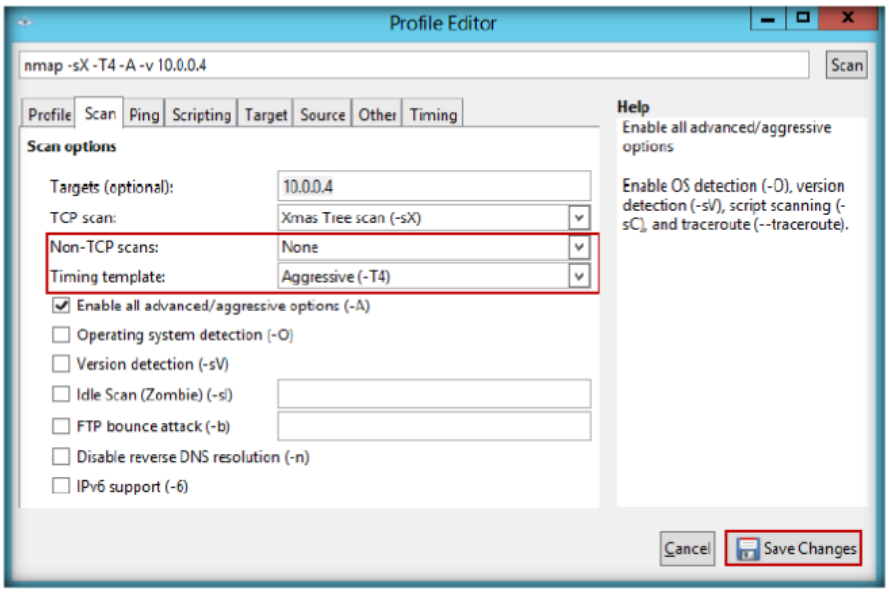


FIGURE 6.17: The Zenmap Profile Editor window with the Scan tab

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.

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

In Nmap, option -sY (SCTP INIT scan) is often referred to as half-open scanning, because you don't open a full SCTP association. You send an INIT chunk, as if you were going to open a real association and then wait for a response.

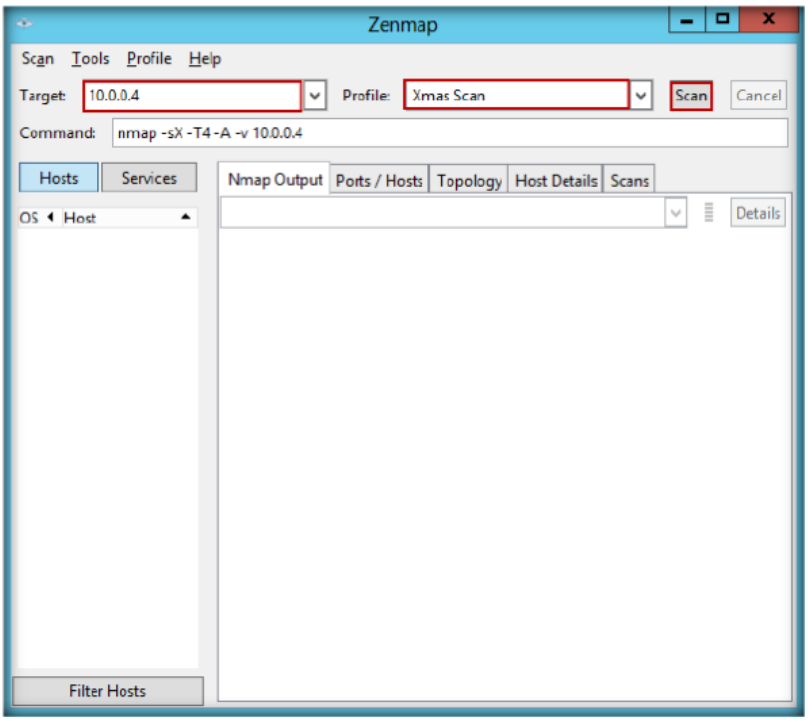


FIGURE 6.18: The Zenmap main window with Target and Profile entered

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.

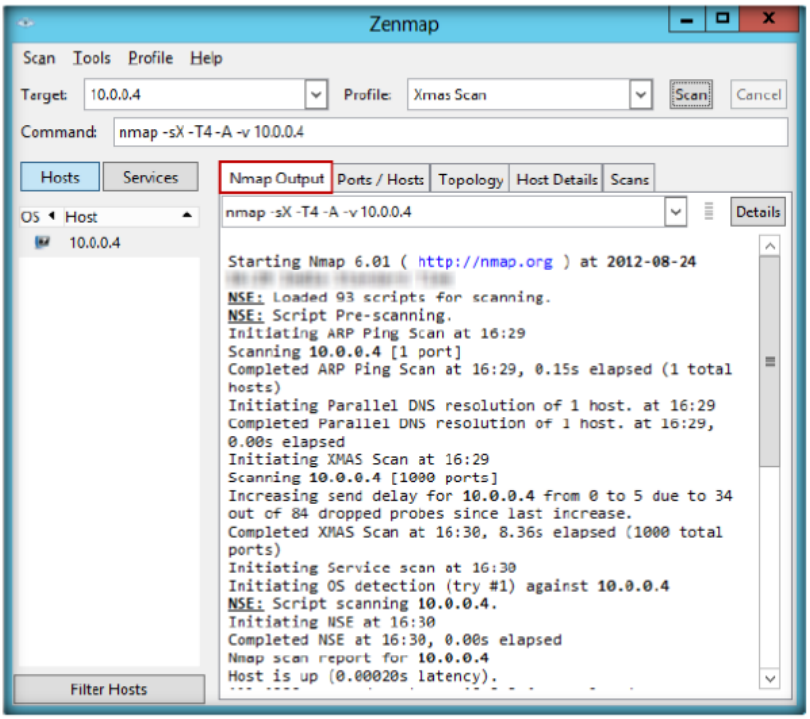


FIGURE 6.19: The Zenmap main window with the Nmap Output tab

The option, -sA (TCP ACK scan) is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

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

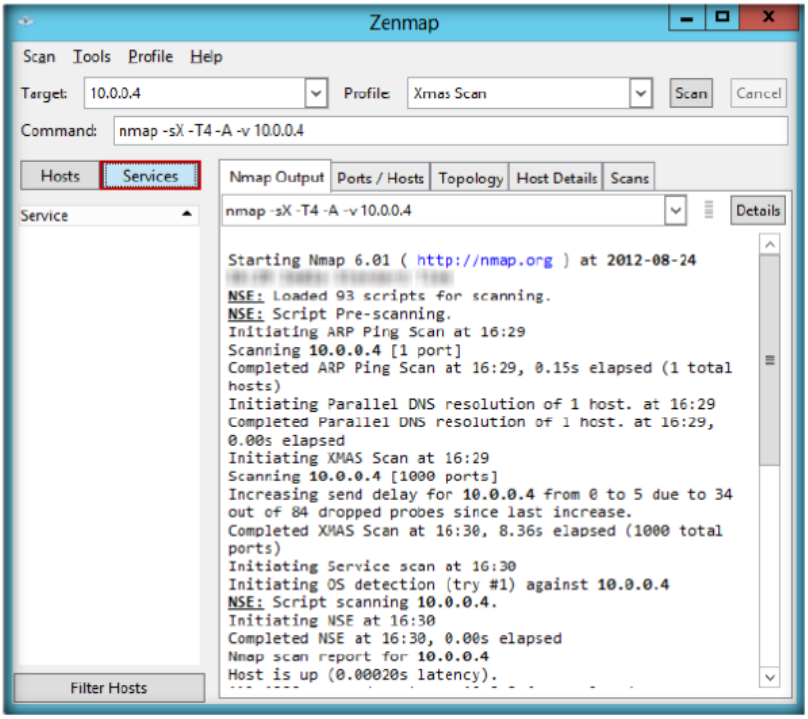


FIGURE 6.20: Zenmap Main window with Services Tab

TASK 3

Null Scan

27. **Null scan** works only if the operating system's TCP/IP implementation is developed according to RFC 793. In a null scan, attackers send a TCP frame to a remote host with NO Flags.

28. To perform a null scan for a target IP address, create a new profile. Click **Profile → New Profile or Command Ctrl+P**.

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

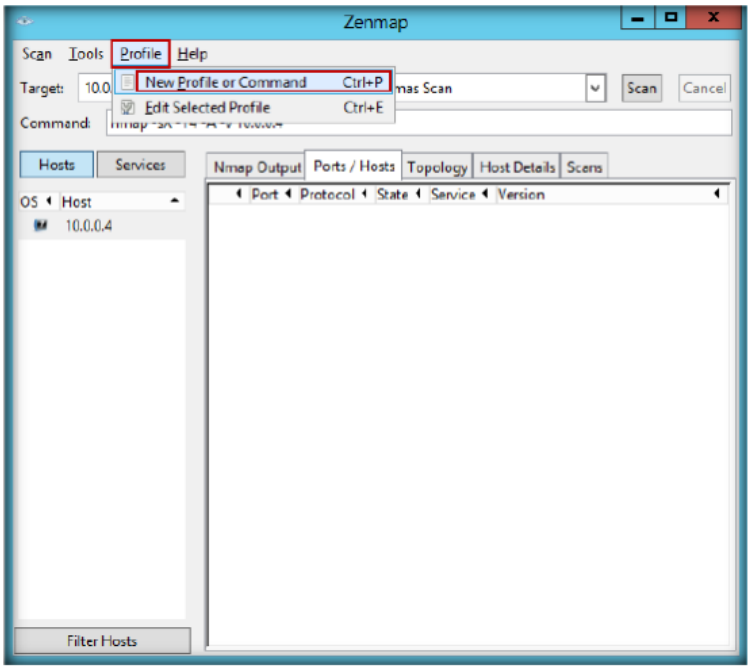


FIGURE 6.21: The Zenmap main window with the New Profile or Command option

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.

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

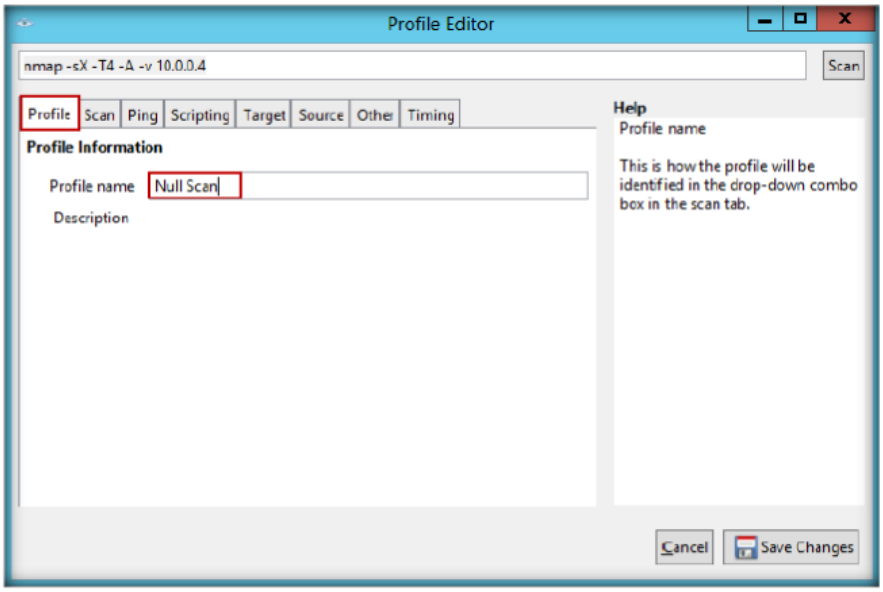


FIGURE 6.22: The Zenmap Profile Editor with the Profile tab

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.

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

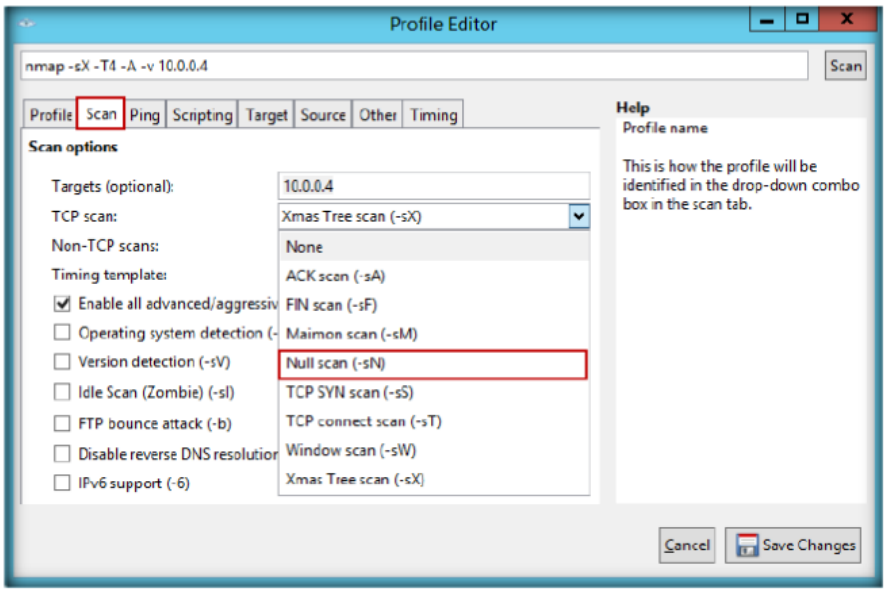


FIGURE 6.23: The Zenmap Profile Editor with the Scan tab

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.

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, -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.

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.

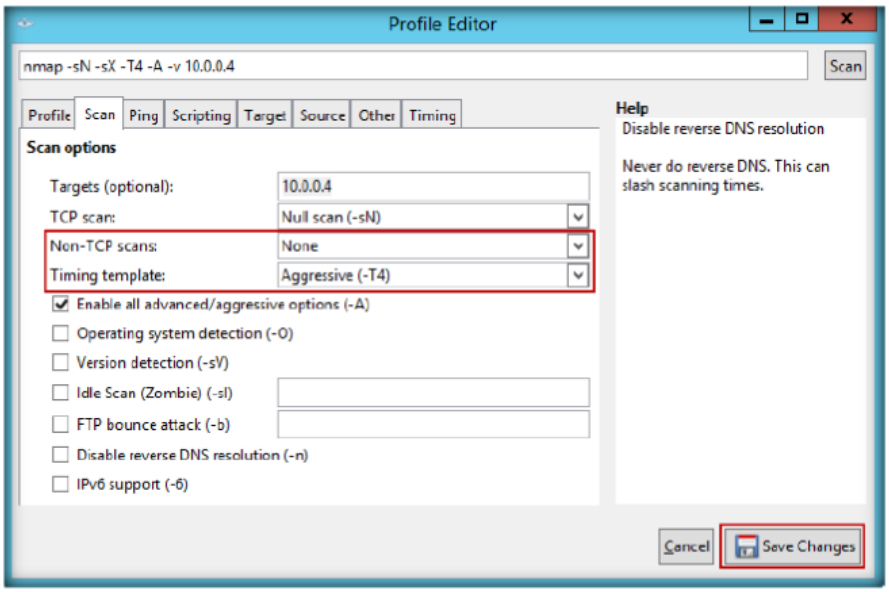


FIGURE 6.24: The Zenmap Profile Editor with the Scan tab

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

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**.

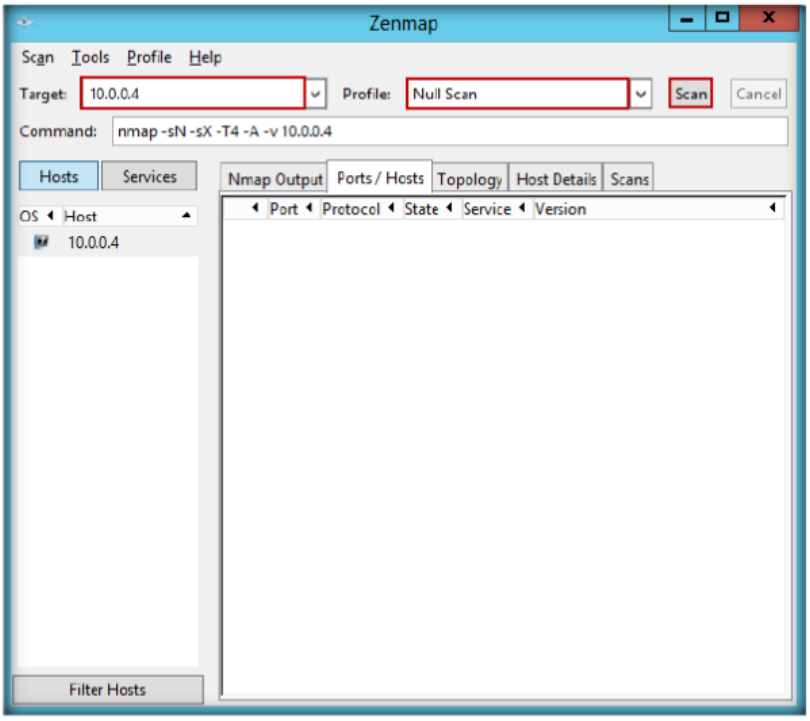


FIGURE 6.25: The Zenmap main window with Target and Profile entered

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.

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

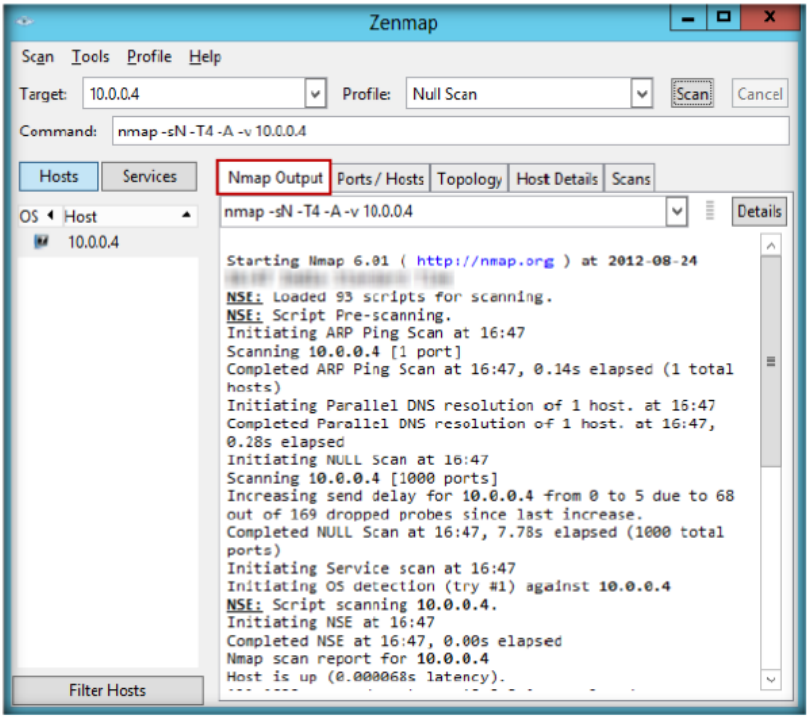


FIGURE 6.26: The Zenmap main window with the Nmap Output tab

The option --version-trace (Trace version scan activity) causes Nmap to print out extensive debugging info about what version scanning is doing. It is a subset of what you get with --packet-trace,

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

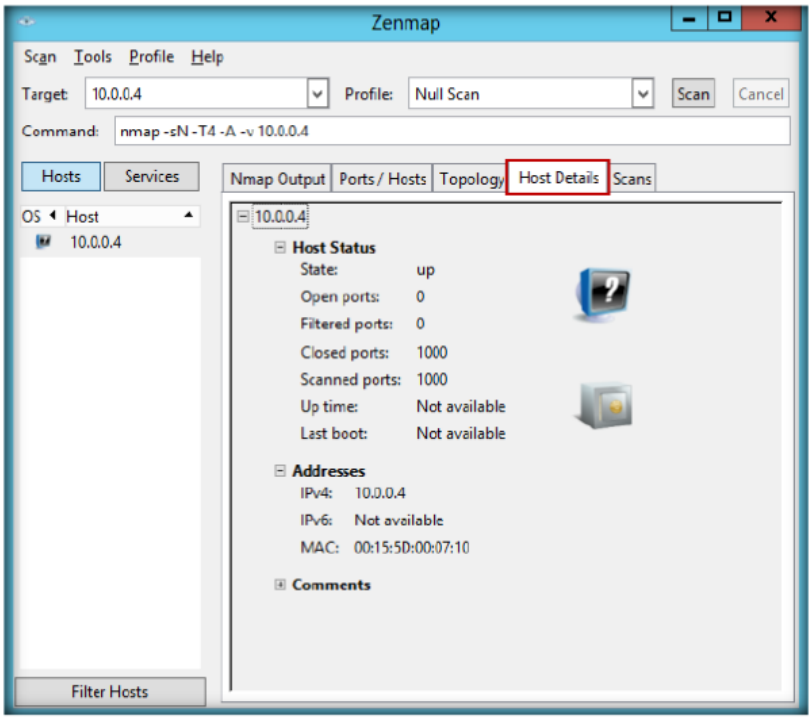


FIGURE 6.27: The Zenmap main window with the Host Details tab

TASK 4

ACK Flag Scan

36. 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**.

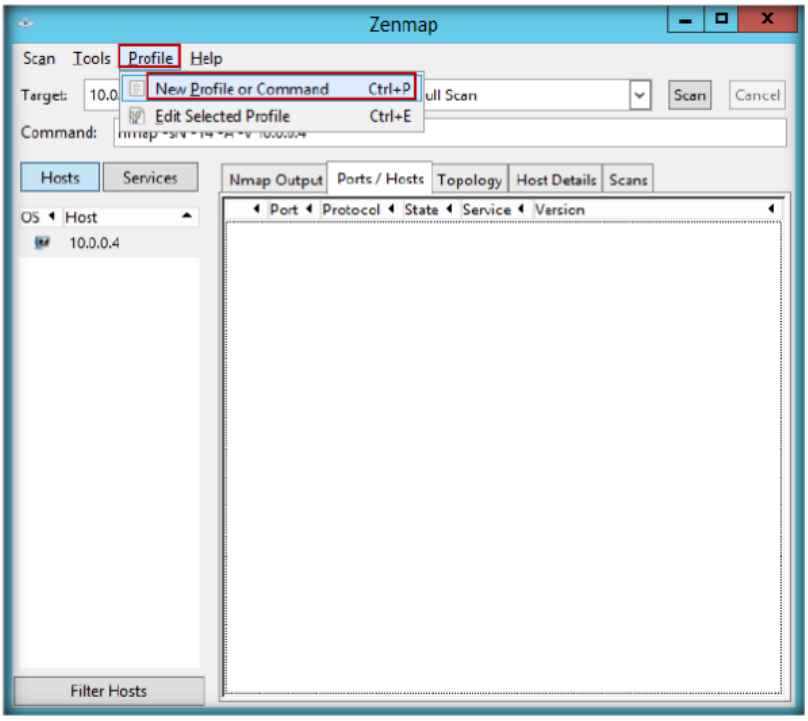


FIGURE 6.28: The Zenmap main window with the New Profile or Command option

The script: --script-updatedb option updates the script database found in scripts/script.db, which is used by Nmap to determine the available default scripts and categories. It is necessary to update the database only if you have added or removed NSE scripts from the default scripts directory or if you have changed the categories of any script. This option is generally used by itself: nmap --script-updatedb.

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

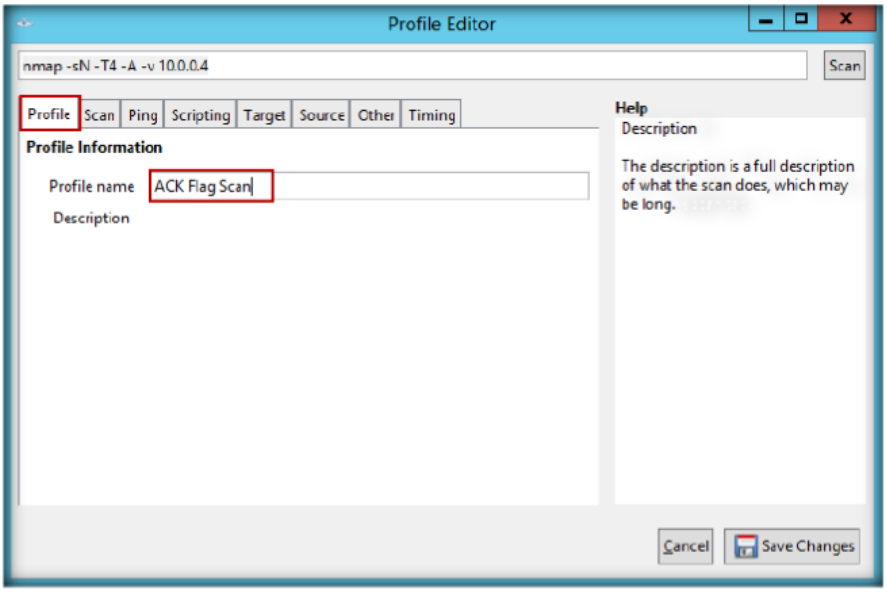


FIGURE 6.29: The Zenmap Profile Editor Window with the Profile tab

The options: --min-parallelism <numprobes>; --max-parallelism <numprobes> (Adjust probe parallelization) control the total number of probes that may be outstanding for a host group. They are used for port scanning and host discovery. By default, Nmap calculates an ever-changing ideal parallelism based on network performance.

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.

The option: --min-rtt-timeout <time>, --max-rtt-timeout <time>, --initial-rtt-timeout <time> (Adjust probe timeouts). Nmap maintains a running timeout value for determining how long it waits for a probe response before giving up or retransmitting the probe. This is calculated based on the response times of previous probes.

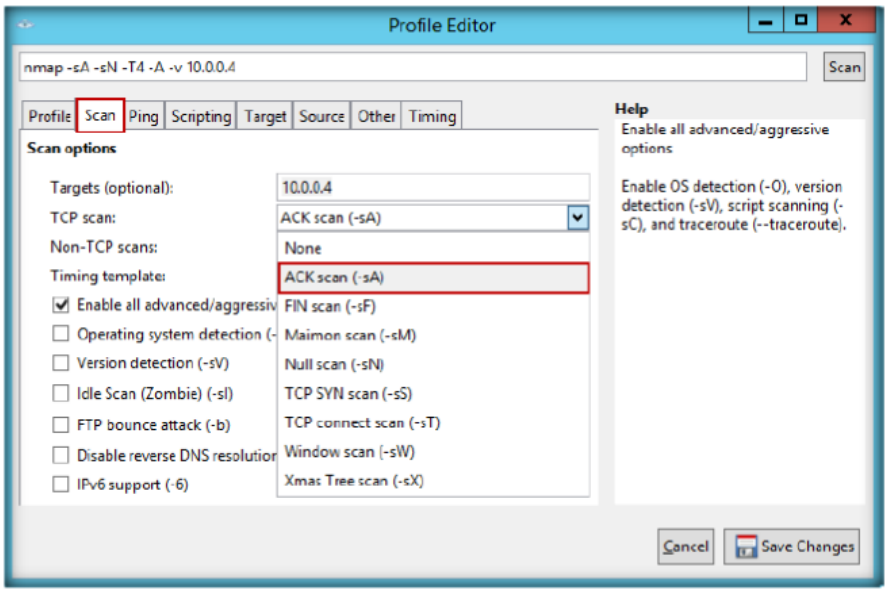


FIGURE 6.30: The Zenmap Profile Editor window with the Scan tab

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

The Option: --max-retries <numtries> (Specify the maximum number of port scan probe retransmissions). When Nmap receives no response to a port scan probe, it can mean the port is filtered. Or maybe the probe or response was simply lost on the network.

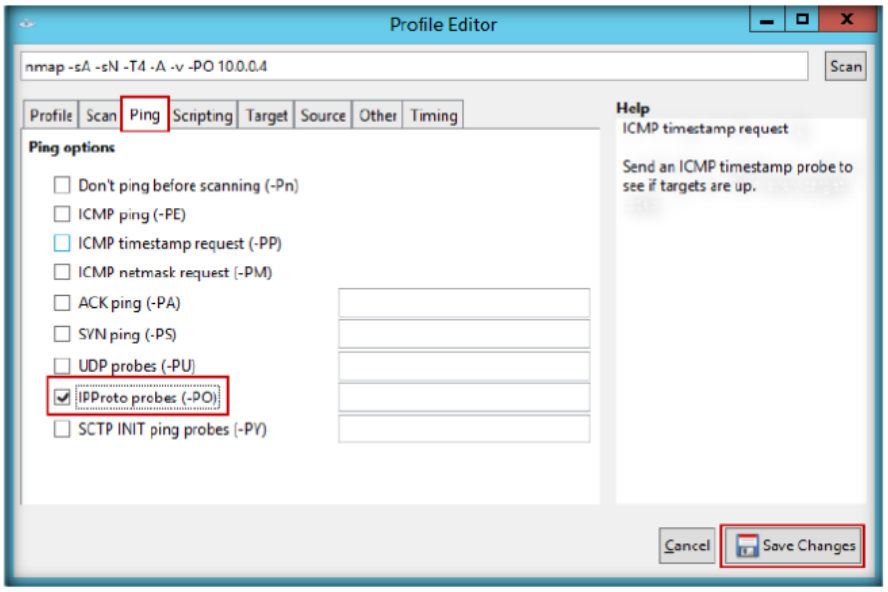


FIGURE 6.31: The Zenmap Profile Editor window with the Ping tab

41. 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**.

The option: --host-timeout <time> (Give up on slow target hosts). Some hosts simply take a long time to scan. This may be due to poorly performing or unreliable networking hardware or software, packet rate limiting, or a restrictive firewall. The slowest few percent of the scanned hosts can eat up a majority of the scan time.

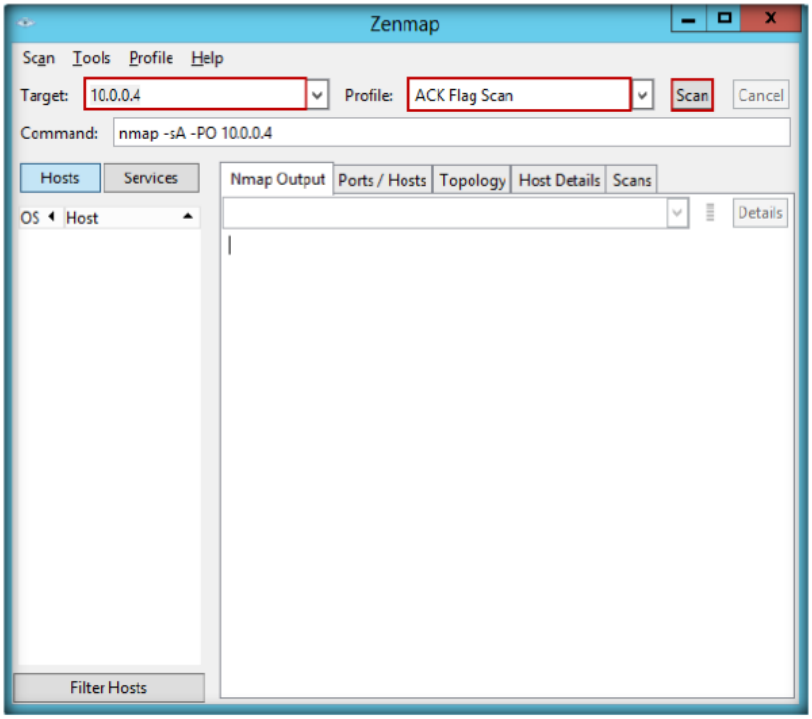


FIGURE 6.32: The Zenmap main window with the Target and Profile entered

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

The option: --scan-delay <time>; --max-scan-delay <time> (Adjust delay between probes).This option causes Nmap to wait at least the given amount of time between each probe it sends to a given host. This is particularly useful in the case of rate limiting.

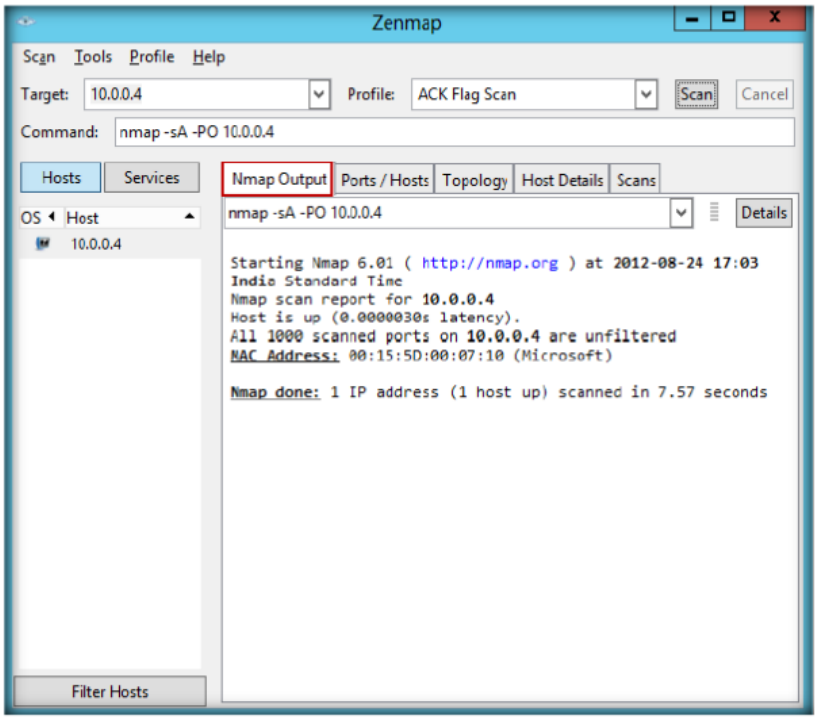


FIGURE 6.33: The Zenmap main window with the Nmap Output tab

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

The option: --min-rate <number>; --max-rate <number> (Directly control the scanning rate). Nmap's dynamic timing does a good job of finding an appropriate speed at which to scan. Sometimes, however, you may happen to know an appropriate scanning rate for a network, or you may have to guarantee that a scan finishes by a certain time.

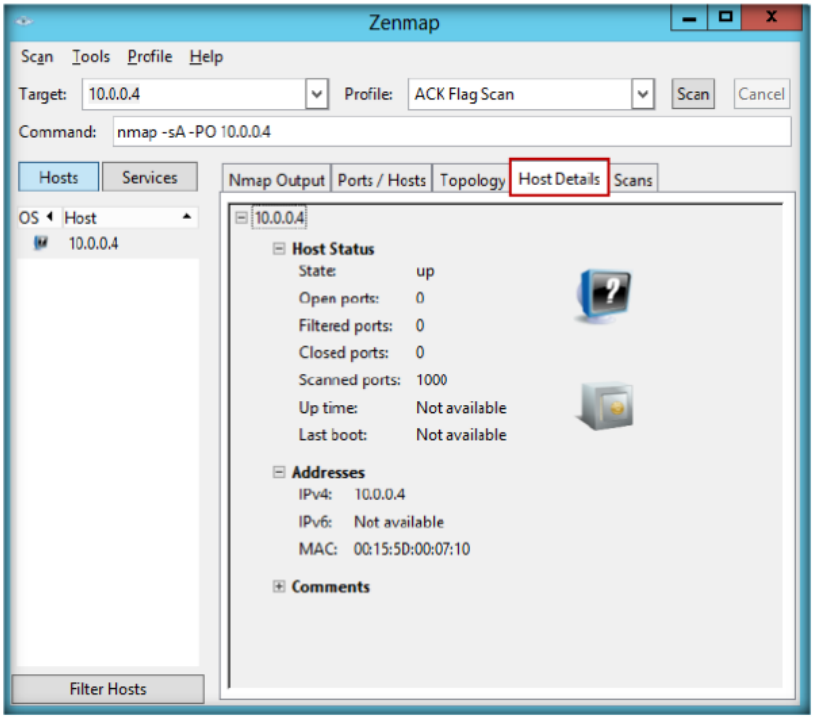


FIGURE 6.34: The Zenmap main window with the Host Details tab

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	**Types of Scan used:** ▪ Intense scan ▪ Xmas scan ▪ Null scan ▪ ACK Flag scan
	Intense Scan – Nmap Output ▪ ARP Ping Scan – 1 host ▪ Parallel DNS resolution of 1 host ▪ SYN Stealth Scan • Discovered open port on 10.0.0.4 o 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	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 7

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

Lab Tasks

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

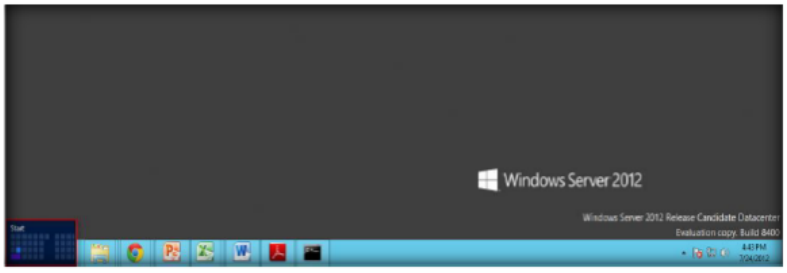


FIGURE 7.1: Windows Server 2012 – Desktop view

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

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..

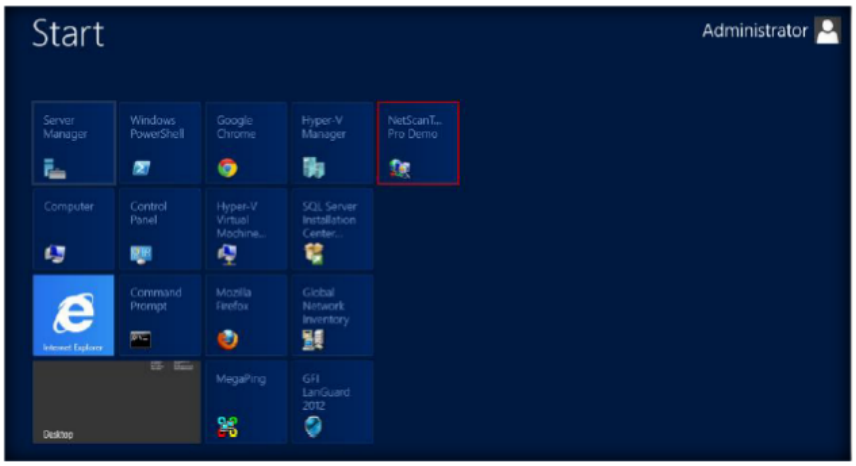
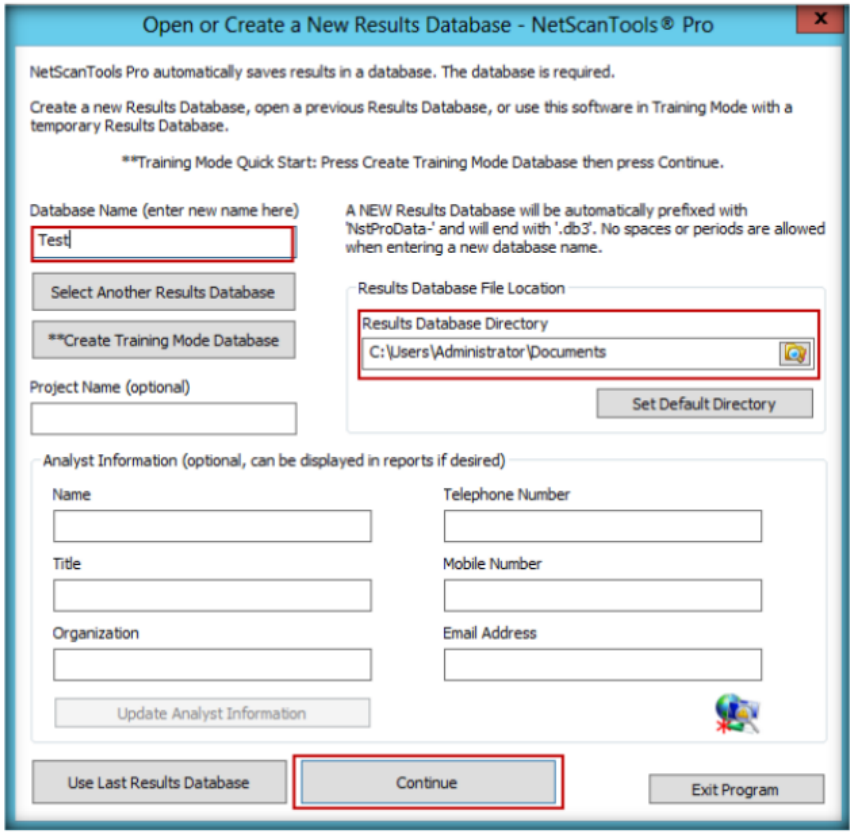


FIGURE 7.2: Windows Server 2012 – Apps

3. If you are using the Demo version of NetScan Tools Pro, then click **Start the DEMO**

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

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

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`

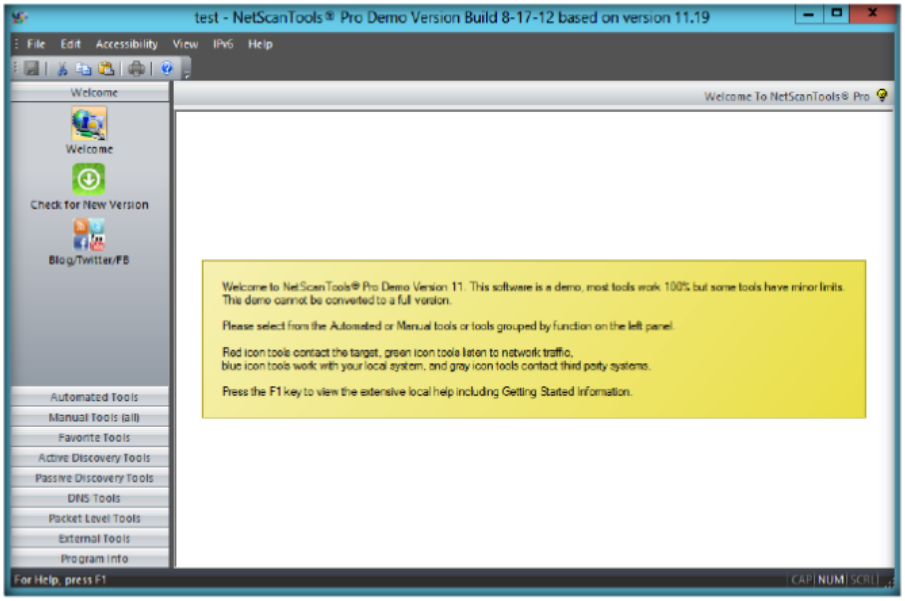


FIGURE 7.4: Main window of NetScan Tools Pro

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

Arp 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

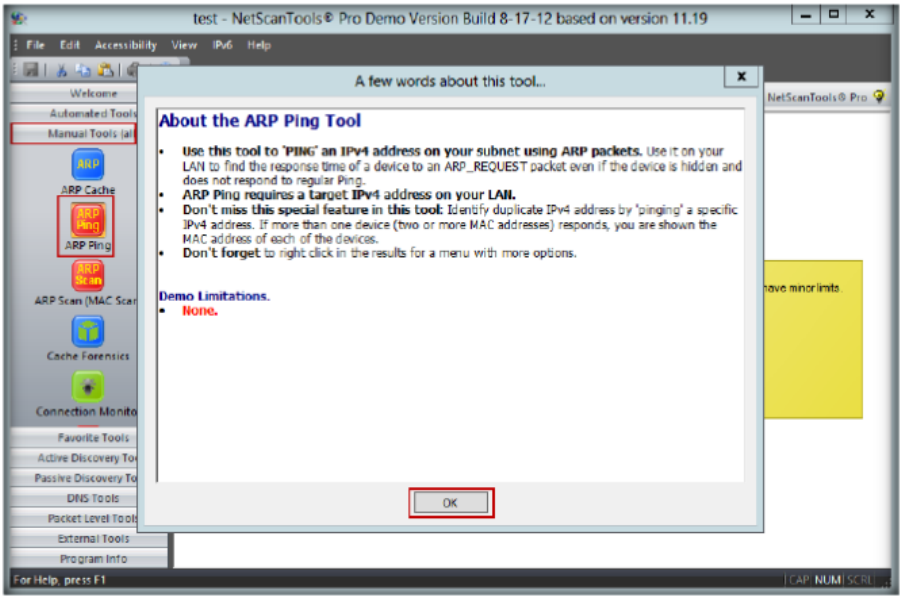
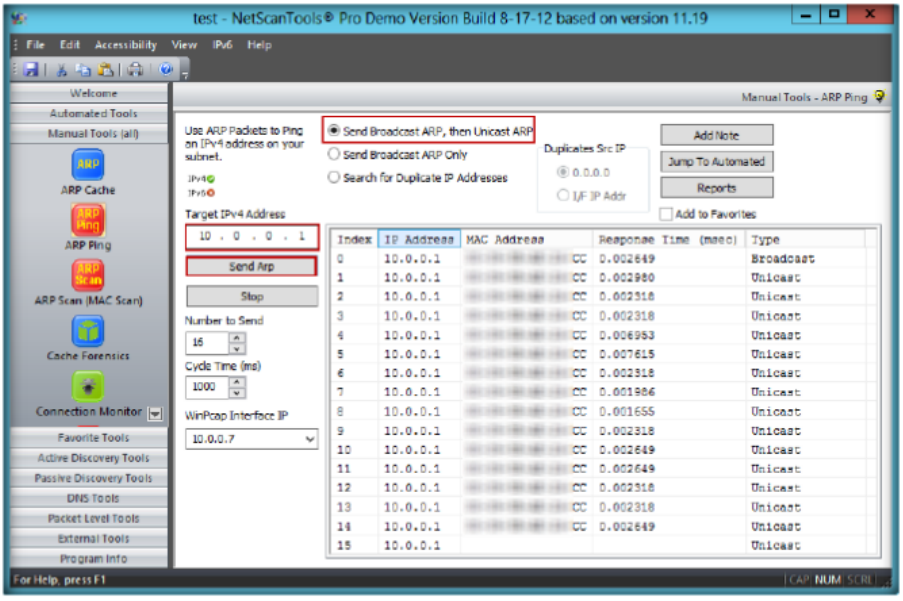


FIGURE 7.5: Selecting manual tools option

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

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



FPinger 7.6: Result of ARP Ping

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

ARP Scan (sometimes called a MAC Scan) sends ARP packets to the range of IPv4 addresses specified by the Start and End IP Address entry boxes. The purpose of this tool is to rapidly sweep your subnet for IPv4 connected devices.

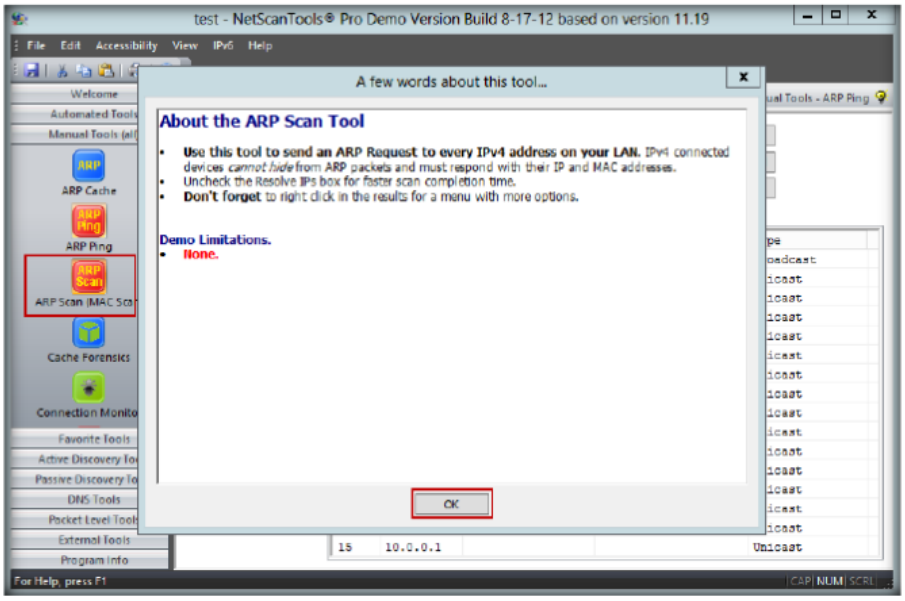


FIGURE 7.7: Selecting ARP Scan (MAC Scan) option

11. Enter the range of IPv4 address in **Starting IPv4 Address** and **Ending IPv4 Address** text boxes

12. Click **Do Arp Scan**

☞ 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.

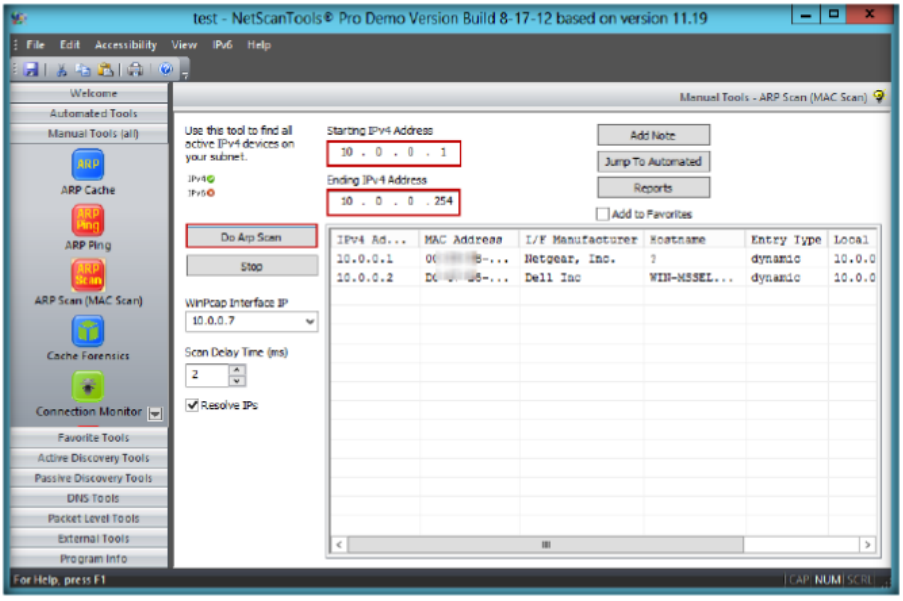


FIGURE 7.8 Result of ARP Scan (MAC Scan)

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

🕮 DHCP is a method of dynamically assigning IP addresses and other network parameter information to network clients from DHCP serv.

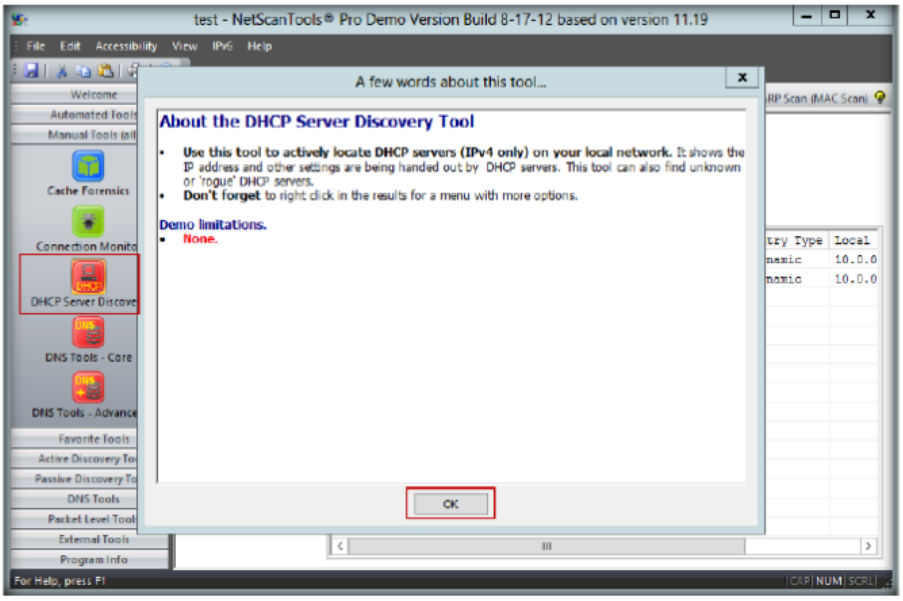


FIGURE 7.9: Selecting DHCP Server Discovery Tool Option

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

📖 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

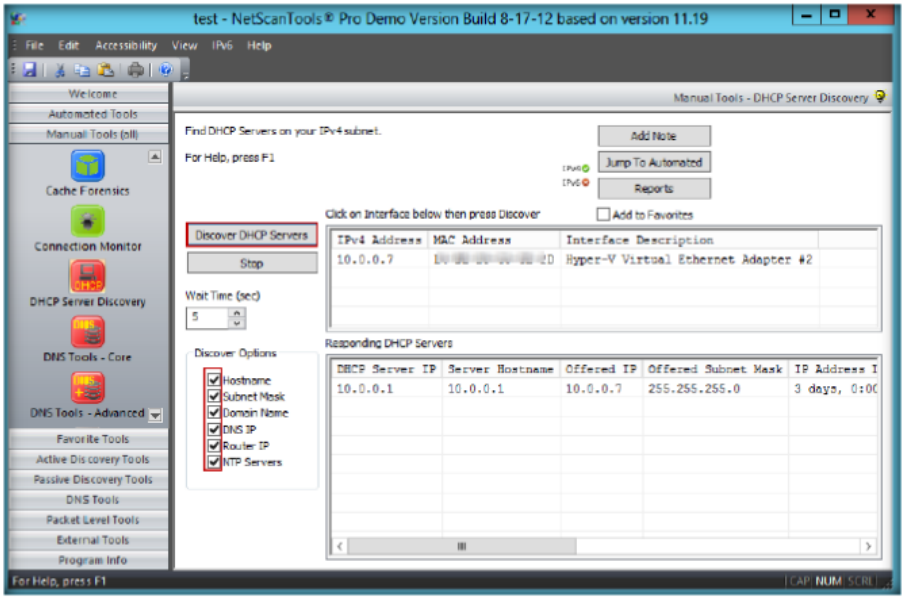


FIGURE 7.10: Result of DHCP Server Discovery

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

📖 Port Scanner is a tool designed to determine which ports on a target computer are active i.e. being used by services or daemons.

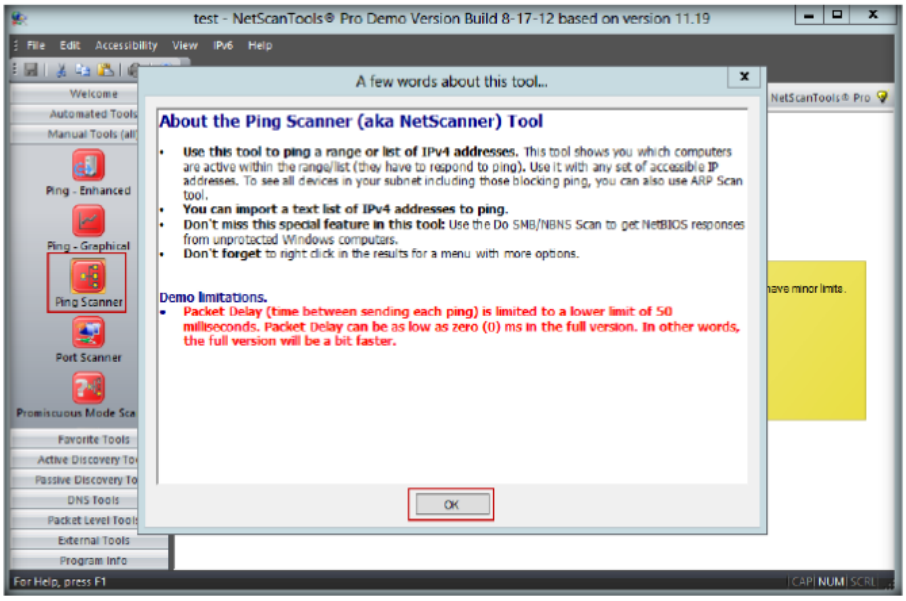


FIGURE 7.11: selecting Ping scanner Option

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

🕮 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.

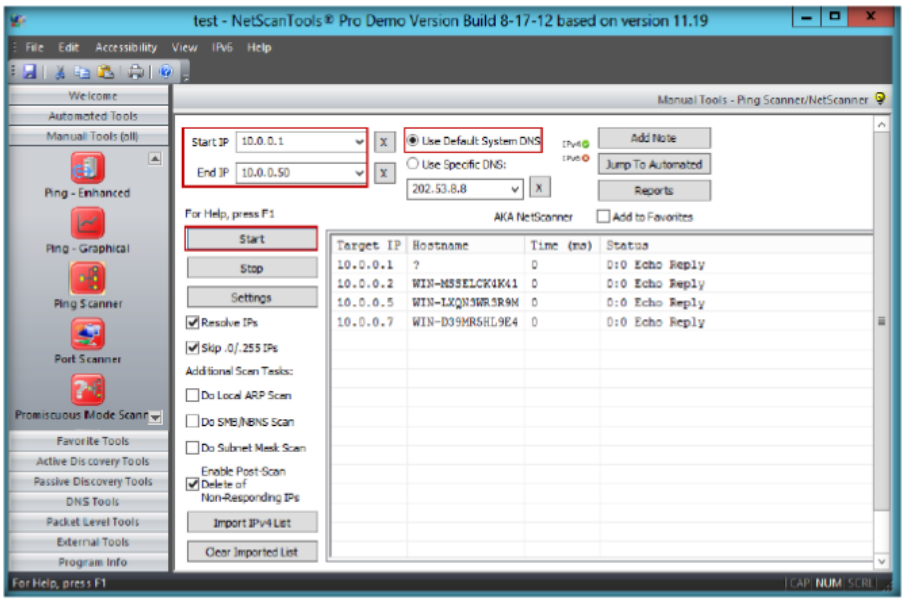


FIGURE 7.12: Result of san IP address

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

🕮 Whois is a client utility that acts as an interface to a remote whois server database. This database may contain domain, IP address or AS Number registries that you can access given the correct query

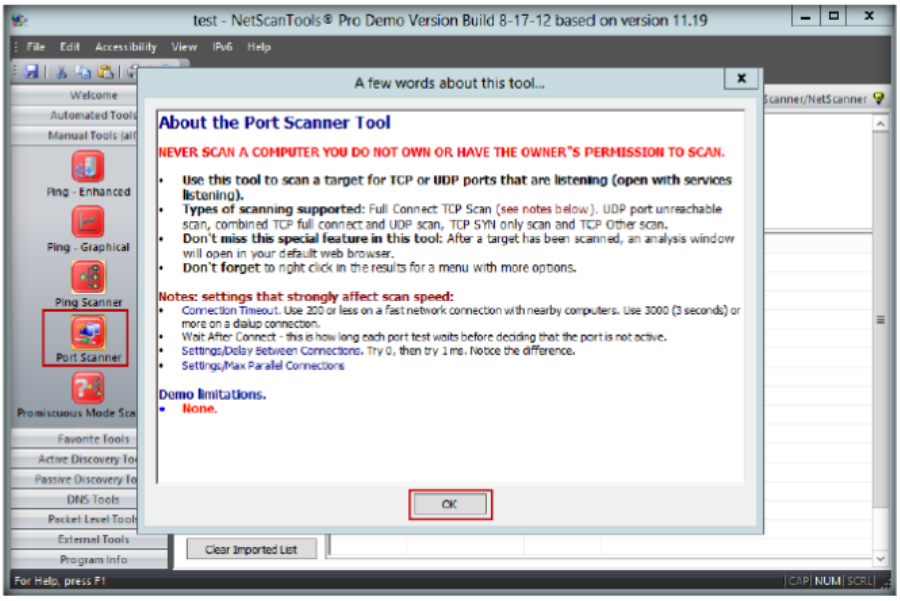


FIGURE 7.13: selecting Port scanner option

19. Enter the IP Address in the **Target Hostname or IP Address** field and select the **TCP Ports only** radio button

20. Click **Scan Range of Ports**

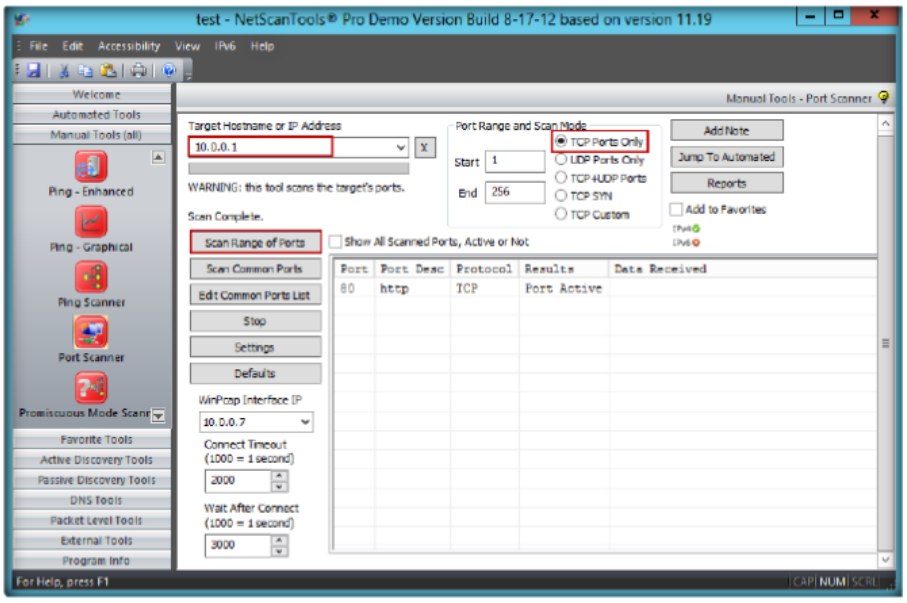


FIGURE 7.14: Result of Port scanner

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	**ARP Scan Results:** ▪ IPv4 Address ▪ MAC Address ▪ I/F Manufacturer ▪ Hostname ▪ Entry Type ▪ Local Address
	Information for Discovered DHCP Servers: ▪ **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	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 8

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

Lab Tasks

Install LANSurveyor on your **Windows Server 2012**

Follow the wizard-driven installation steps and install LANSurvyor.

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

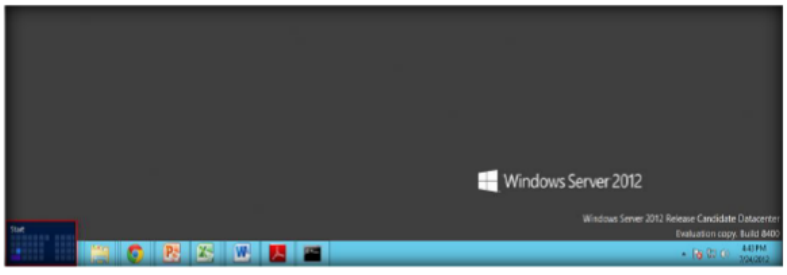


FIGURE 8.1: Windows Server 2012 – Desktop view

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

📖 LANsurveyor's Responder client Manage remote Windows, Linux, and Mac OS nodes from the LANsurveyor map, including starting and stopping applications and distributing files

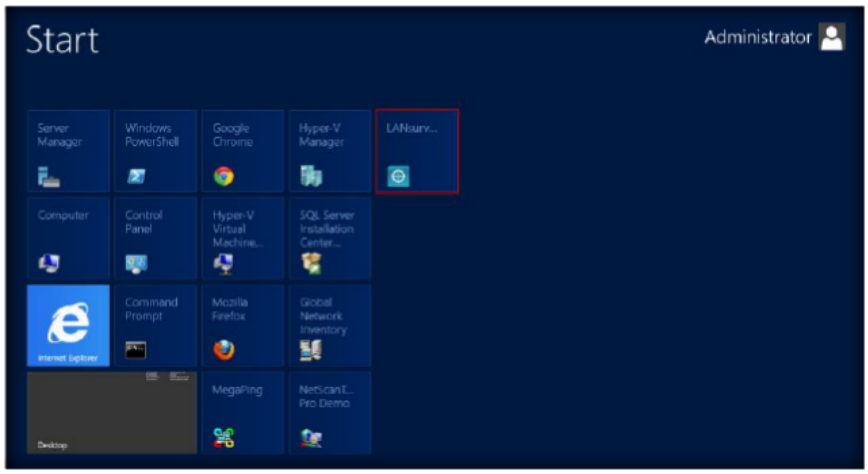


FIGURE 8.2: Windows Server 2012 – Apps

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

🗁 LANsurveyor uses an almost immeasurable amount of network bandwidth. For each type of discovery method (ICMP Ping, NetBIOS, SIP, etc.)

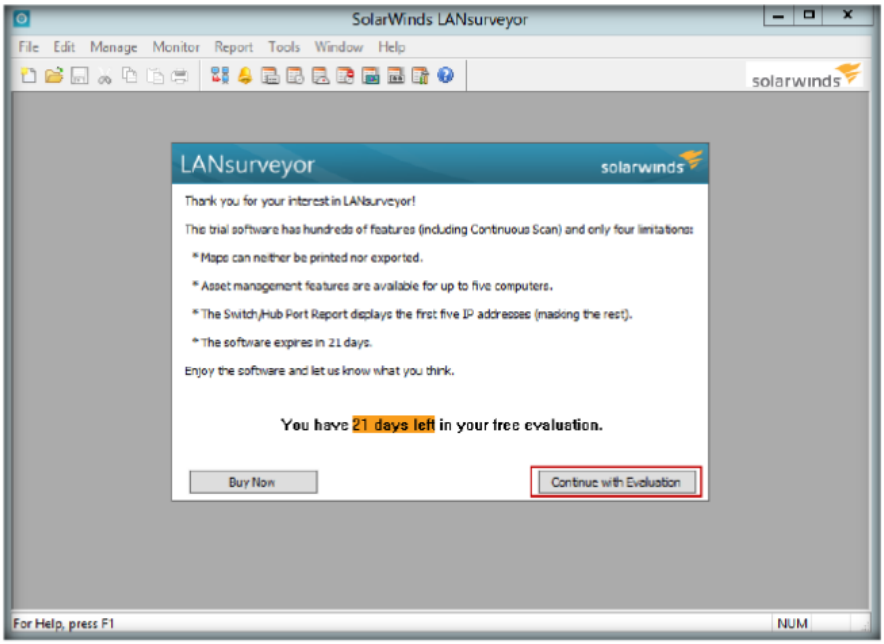


FIGURE 8.3: LANSurveyor evaluation window

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

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.

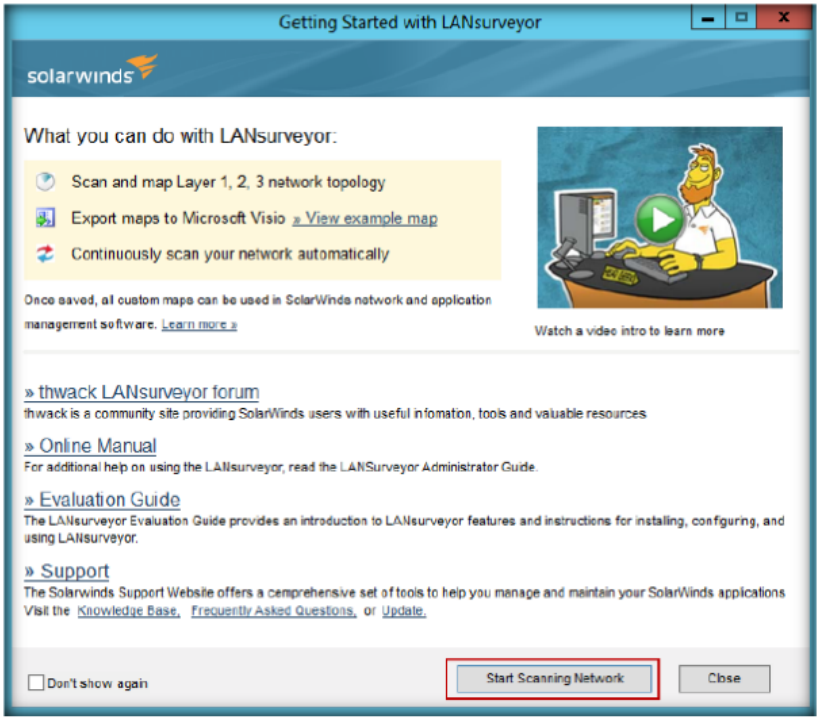


FIGURE 8.4: Getting Started with LANSurveyor Wizard

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

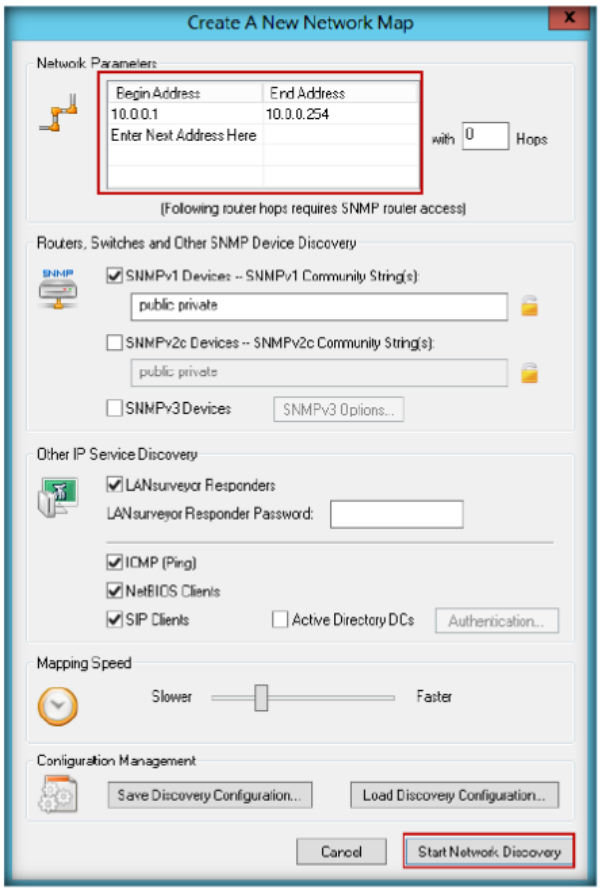


FIGURE 8.5: New Network Map window

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

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

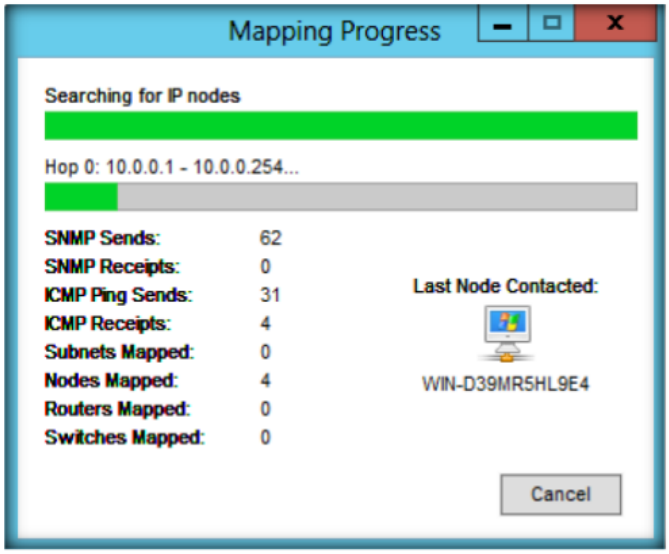


FIGURE 8.6: Mapping progress window

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

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.

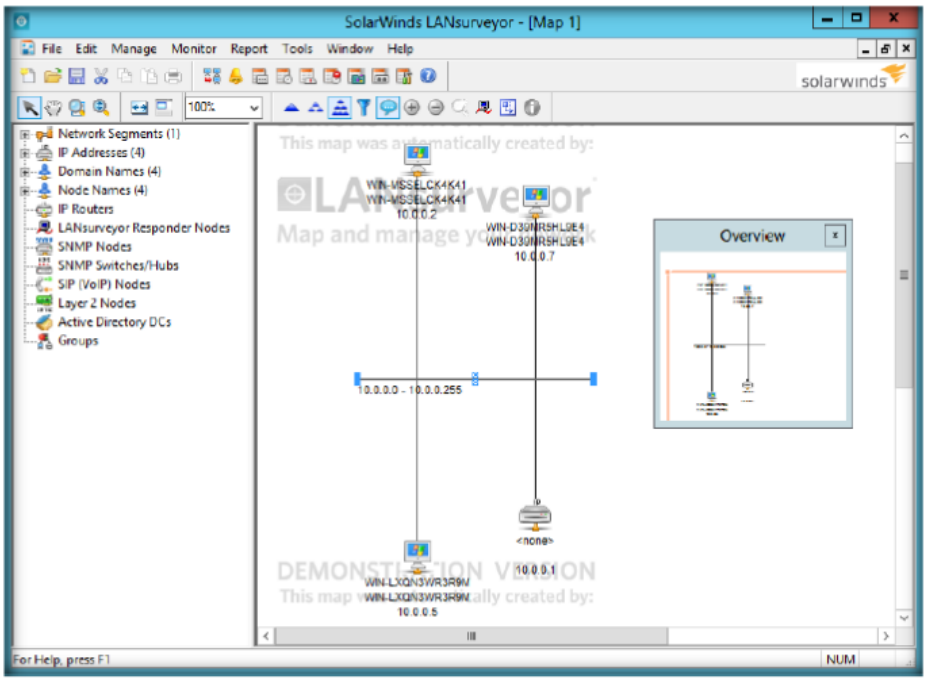


FIGURE 8.7: Resulted network diagram

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	**IP address:** 10.0.0.1 -10.0.0.254
	IP Nodes Details: ▪ SNMP Send - 62 ▪ ICMP Ping Send - 31 ▪ ICMP Receipts - 4 ▪ Nodes Mapped - 4
	Network segment Details: ▪ 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

TASK 1

Draw Network Map

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

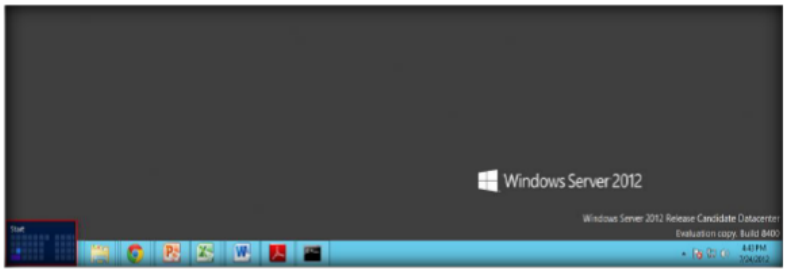


FIGURE 9.1: Windows Server 2012 – Desktop view

4. Click the **Friendly Pinger** app to open the **Friendly Pinger** window

You are alerted when nodes become unresponsive (or become responsive again) via a variety of notification methods.

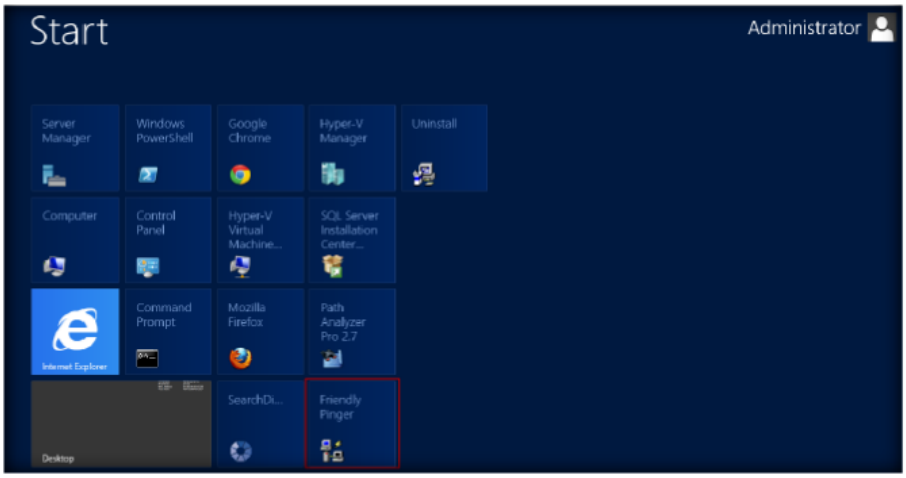


FIGURE 9.2: Windows Server 2012 – Apps

Friendly Pinger will display IP-address of your computer and will offer an exemplary range of IP-addresses for scanning

5. The **Friendly Pinger** window appears, and Friendly Pinger prompts you to watch an online demonstration.

6. Click **No**

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

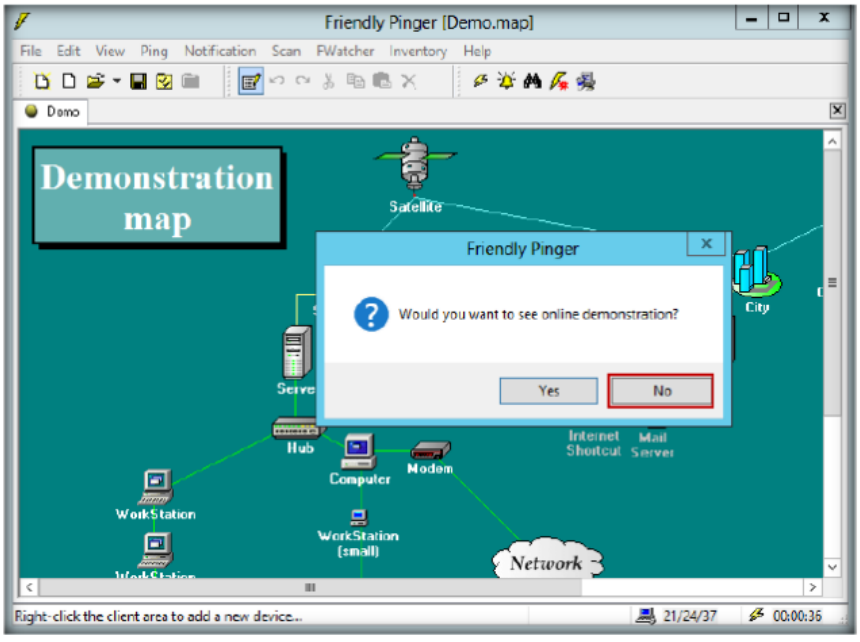


FIGURE 9.3: FPinger Main Window

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

7. Select **File** from the menu bar and select the **Wizard** option

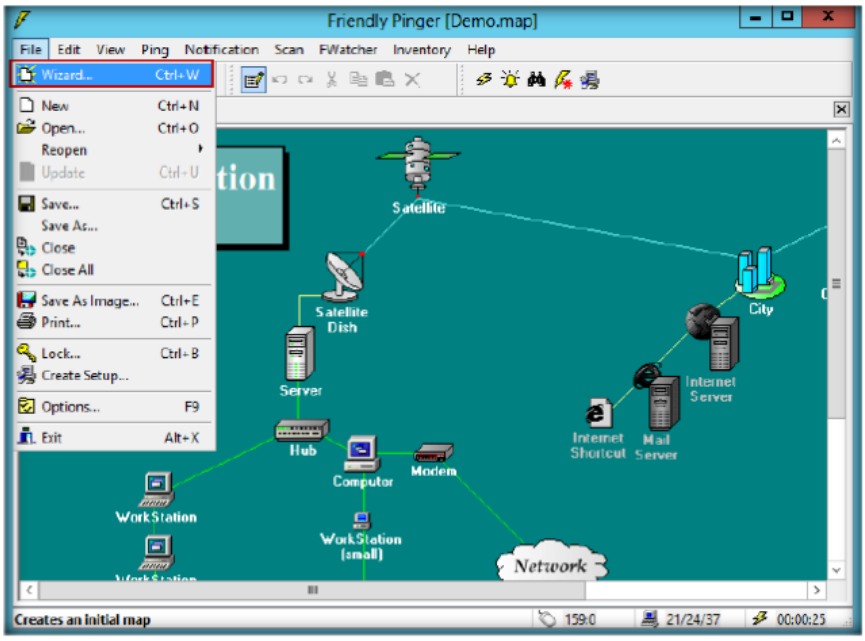


FIGURE 9.4: FPinger Starting Wizard

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

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**

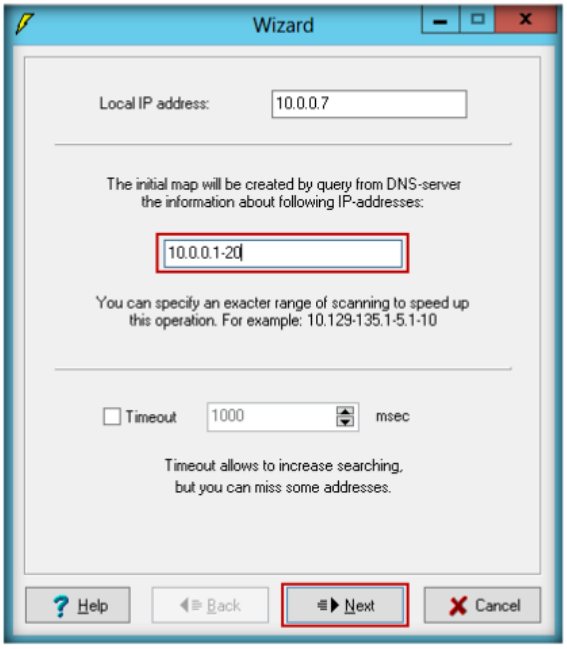
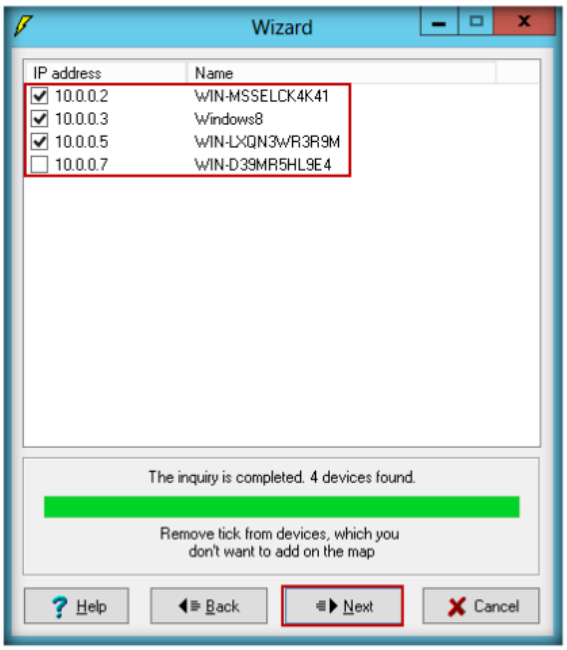


FIGURE 9.5: FPinger Intializing IP address range

The device is displayed as an animated picture, if it is pinged, and as a black and white picture if it is not pinged

9. Then the wizard will start scanning of **IP addresses** in the network, and list them.
10. Click **Next**



FPinger 9.6: FPinger Scanning of Address completed

Press CTRL+I to get more information about the created map. You will see you name as the map author in the appeared dialog window

11. Set the default options in the **Wizard** selection windows and click **Next**

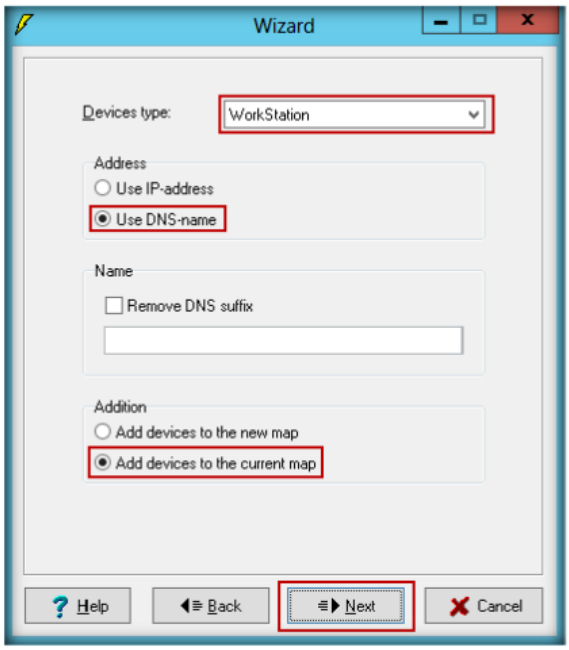


FIGURE 9.7: FPinger selecting the Devices type

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.

12. Then the client area will displays 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.

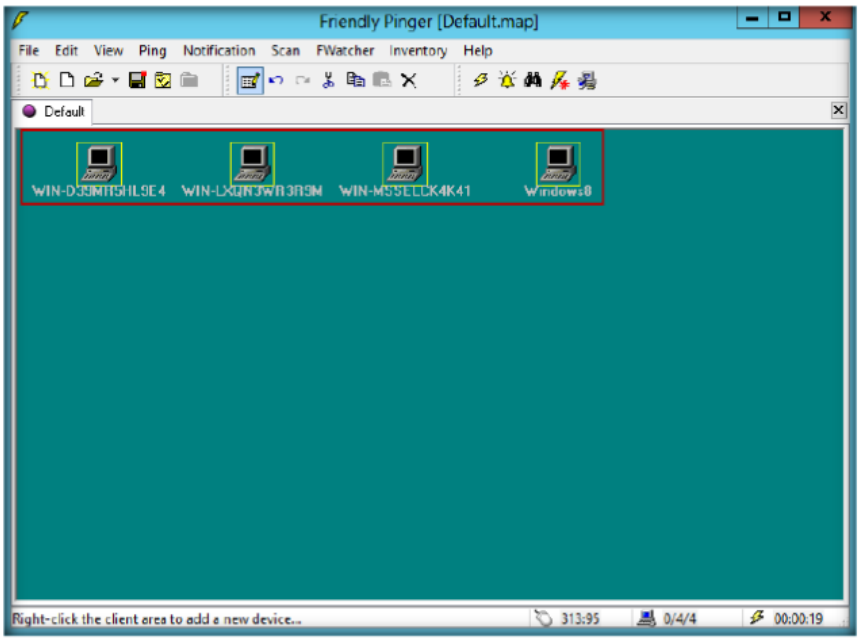


FIGURE 9.8 FPinger Client area with Network architecture

13. 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.

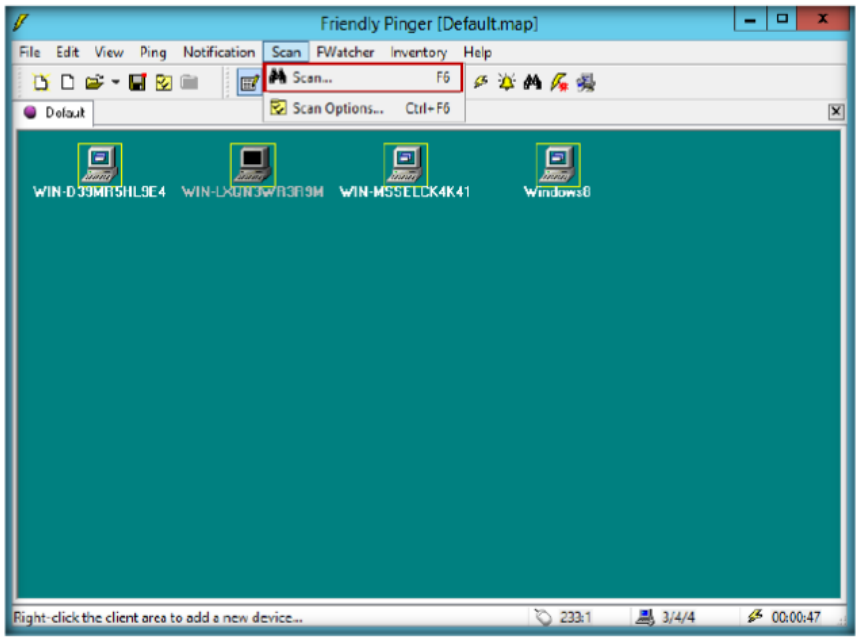


FIGURE 9.9: FPinger Scanning the computers in the Network

Select "File | Options..." and configure **Friendly Pinger** to your taste.

14. It displays **scanned details** in the **Scanning** wizard

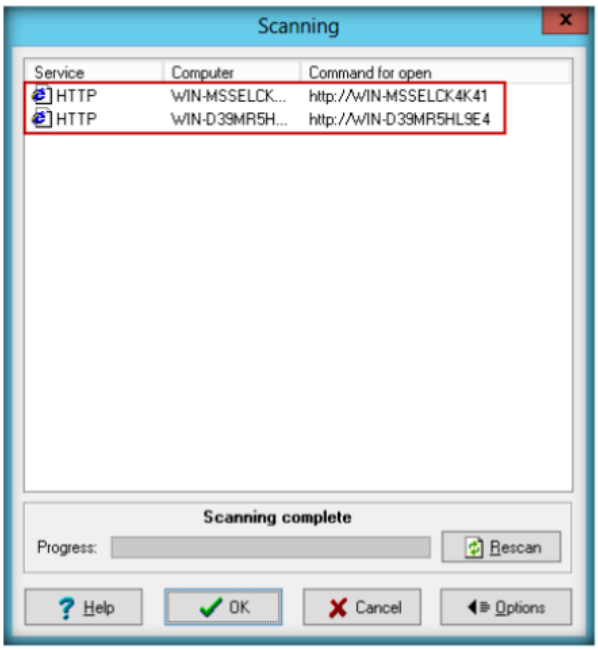


FIGURE 9.10: FPinger Scanned results

Double-click the device to open it in Explorer.

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

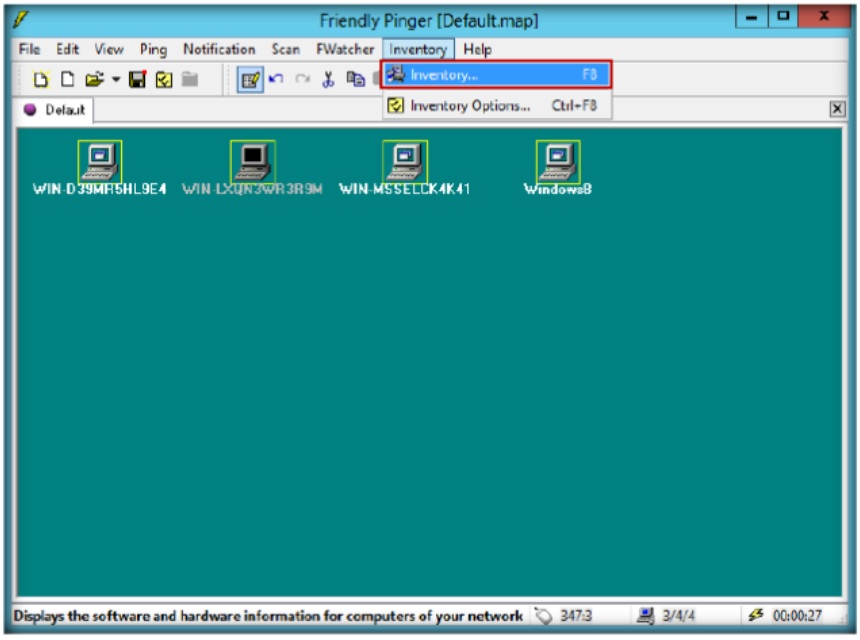


FIGURE 9.11: FPinger Inventory tab

Tracking user access and files opened on your computer via the network

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

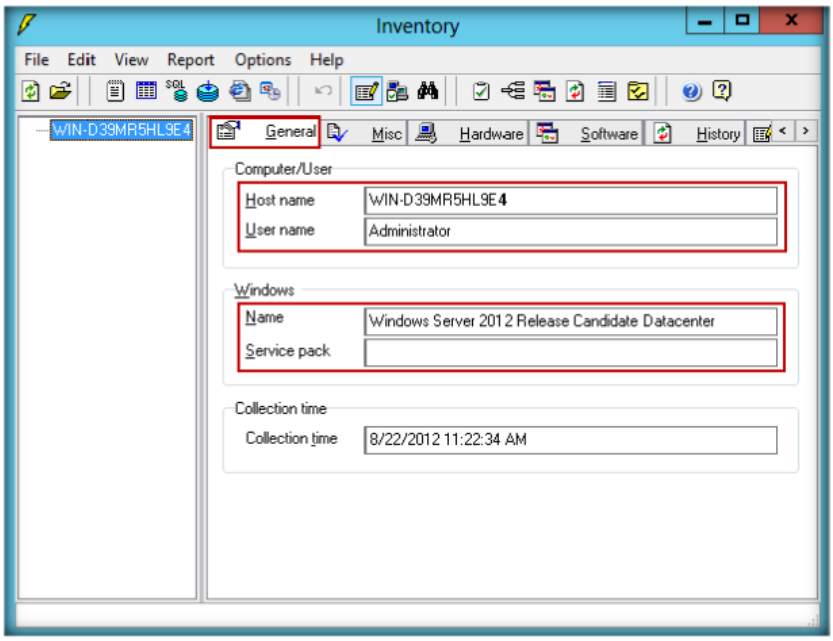
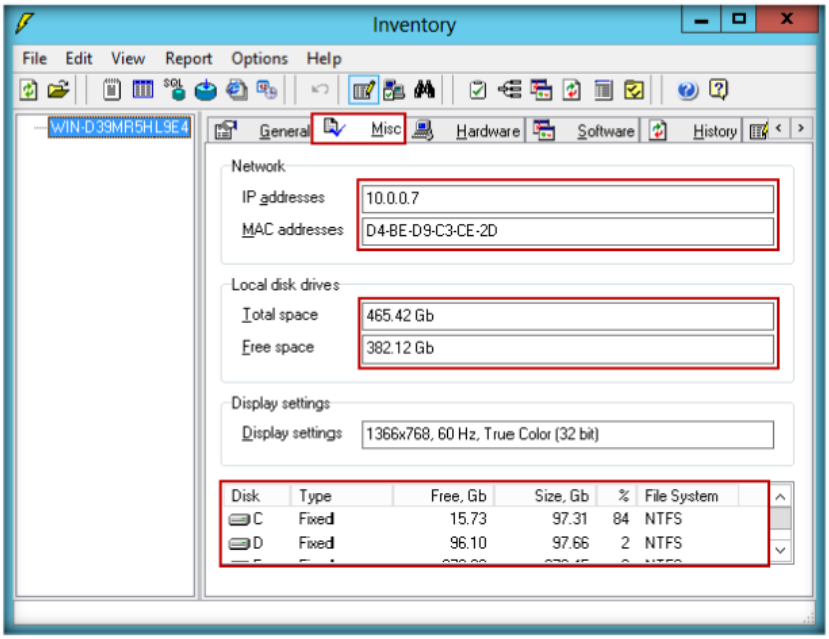


FIGURE 9.12: FPinger Inventory wizard General tab

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

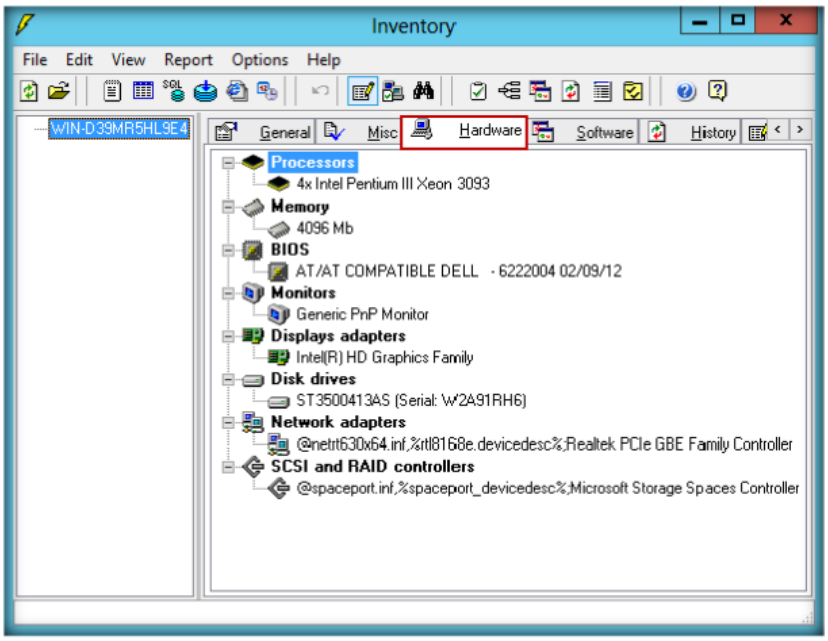


FIGURE 9.14: FPinger Inventory wizard Hardware tab

19. The **Software** tab shows the installed software on the computers

🕮 Visualization of your computer network as a beautiful animated screen

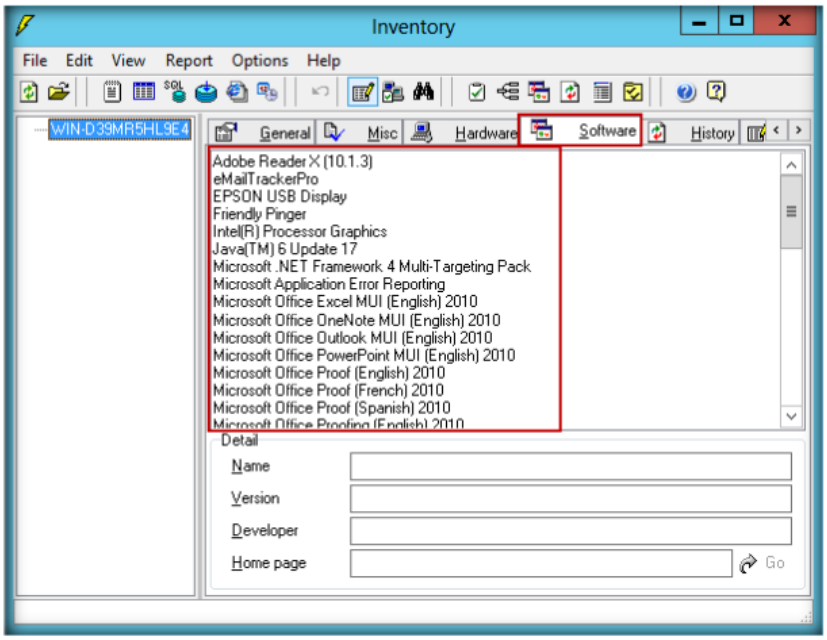


FIGURE 9.15: FPinger Inventory wizard Software tab

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
FriendlyPinger	**IP address:** 10.0.0.1 -10.0.0.20
	Found IP address: ▪ 10.0.0.2 ▪ 10.0.0.3 ▪ 10.0.0.5 ▪ 10.0.0.7
	Details Result of 10.0.0.7: ▪ 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

Overview of Nessus Tool

Nessus is public Domain software related under the GPL.

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**

Nessus is designed to automate the testing and discovery of known security problems.

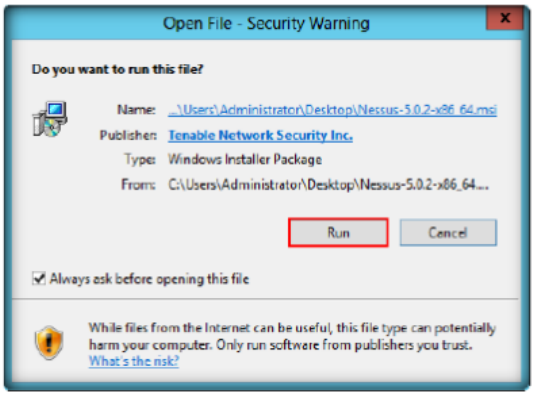


FIGURE 10.1: Open File - Security Warning

4. The **Nessus - InstallShield Wizard** appears. During the installation process, the wizard prompts you for some basic information. Follow the instructions. Click **Next**.

The updated Nessus security checks database is can be retrieved with commands nessus-updated-plugins.

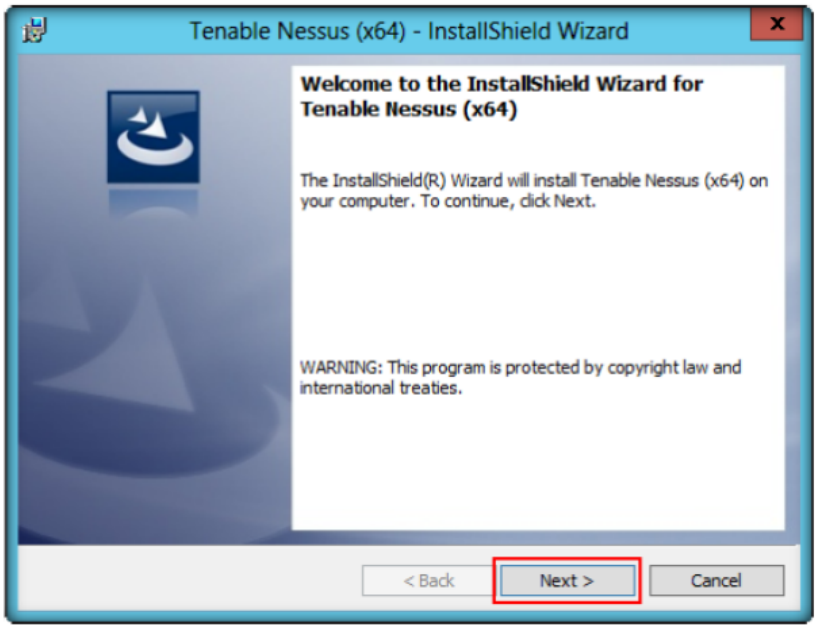


FIGURE 10.2: The Nessus installation window

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

Nessus has the ability to test SSLized services such as http, smtps, imaps and more.

Nessus security scanner includes NASL (Nessus Attack Scripting Language).

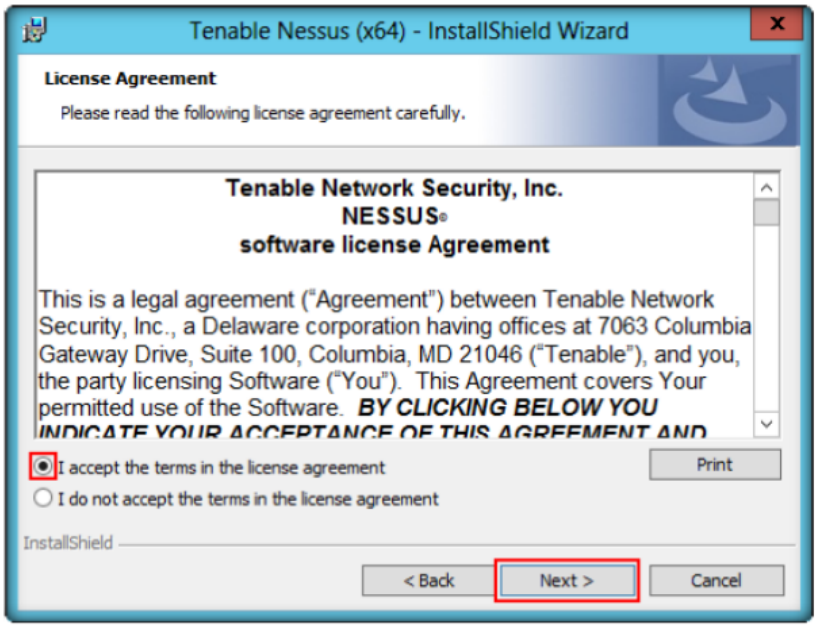


FIGURE 10.3: The Nessus Install Shield Wizard

7. Select a destination folder and click **Next**.

Nessus gives you the choice for performing regular nondestructive security audit on a routinely basis.

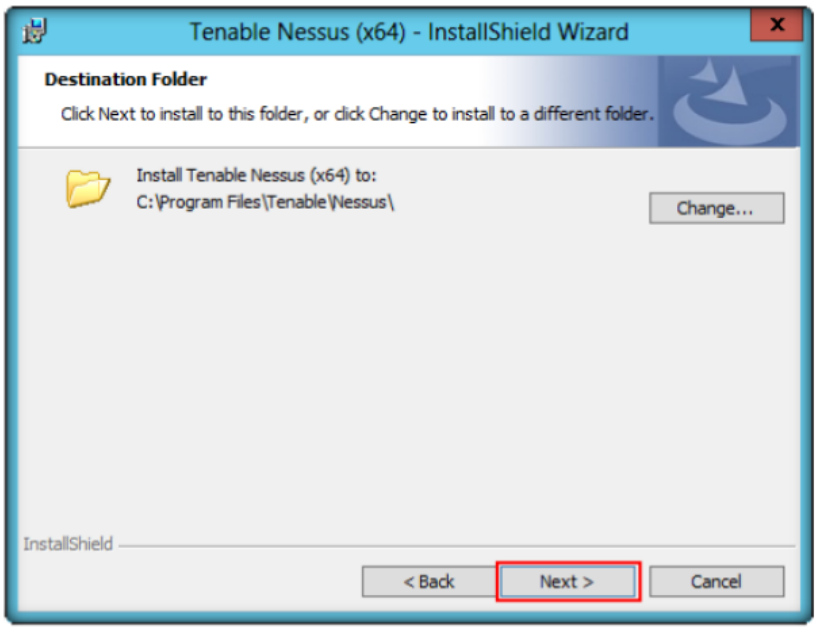


FIGURE 10.4: The Nessus Install Shield Wizard

8. The wizard prompts for **Setup Type**. With the **Complete** option, all program features will be installed. Check **Complete** and click **Next**.

Nessus probes a range of addresses on a network to determine which hosts are alive.

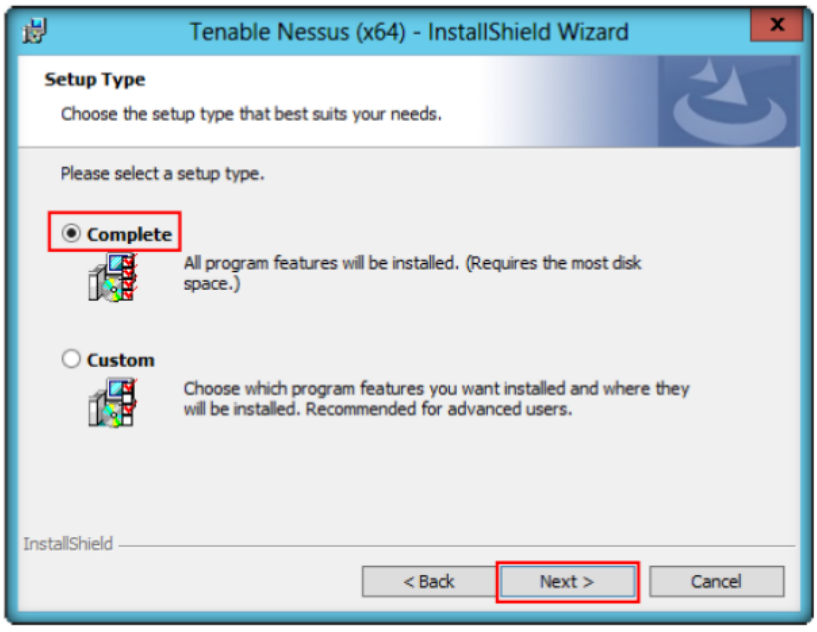


FIGURE 10.5: The Nessus Install Shield Wizard for Setup Type

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

Nessus probes network services on each host to obtain banners that contain software and OS version information.

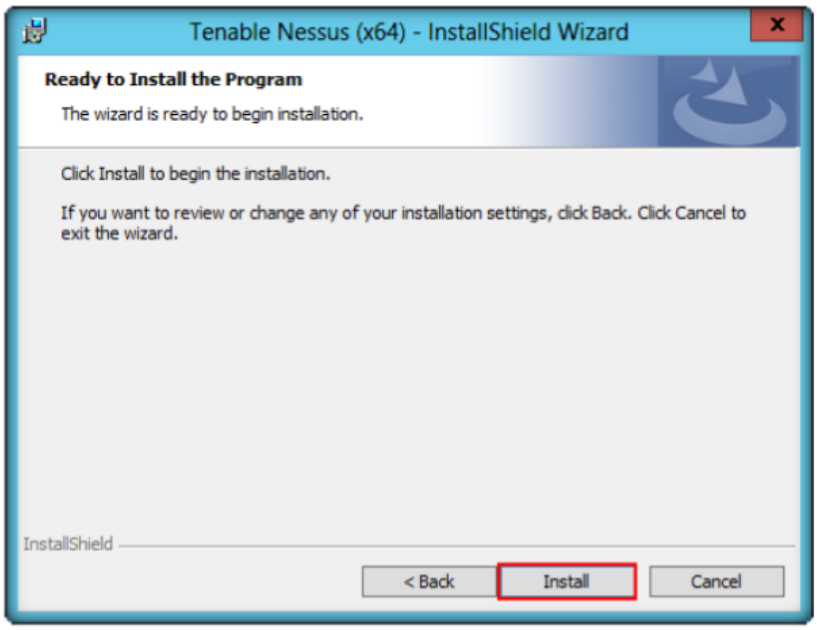


FIGURE 10.6: Nessus InstallShield Wizard

10. Once installation is complete, click **Finish.**

Path of Nessus home directory for windows \programfiles\tanable\nessus

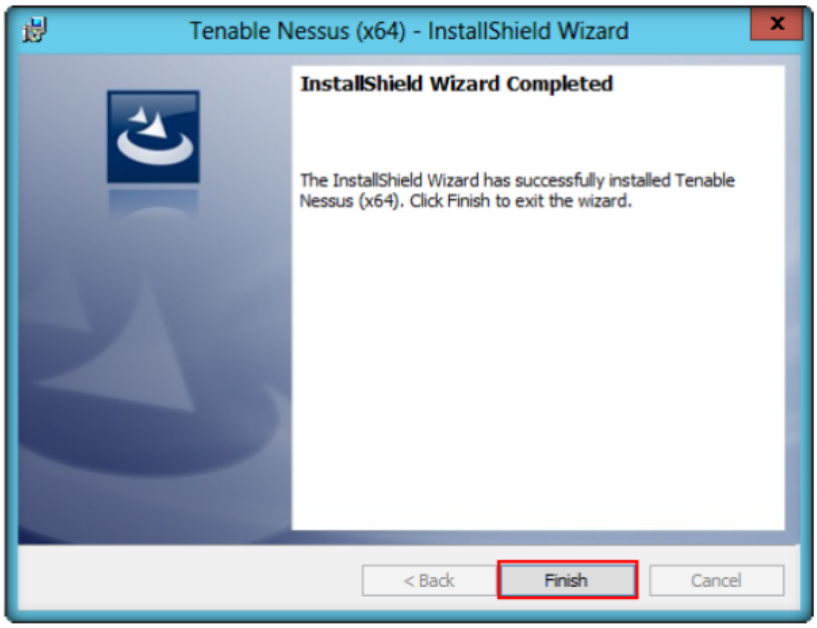


FIGURE 10.7: Nessus Install Shield wizard

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**

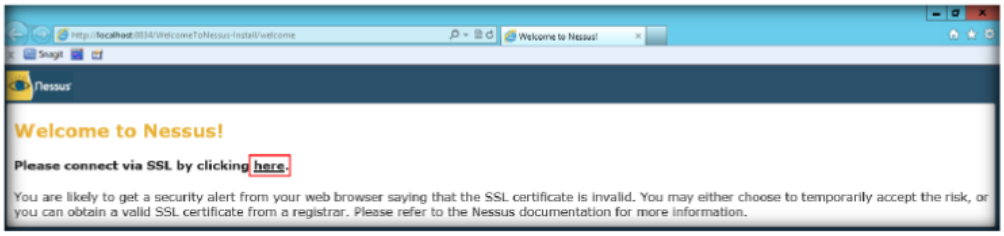


FIGURE 10.8: Nessus SSL certification

13. Click **OK** in the **Security Alert** pop-up, if it appears

The Nessus Server Manager used in Nessus 4 has been deprecated

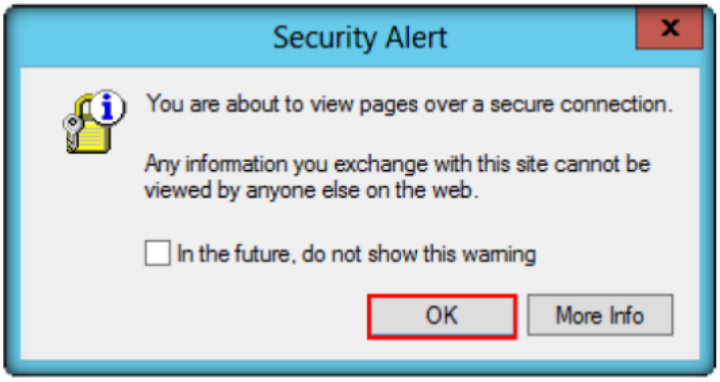


FIGURE 10.9: Internet Explorer Security Alert

14. Click the **Continue to this website (not recommended)** link to continue

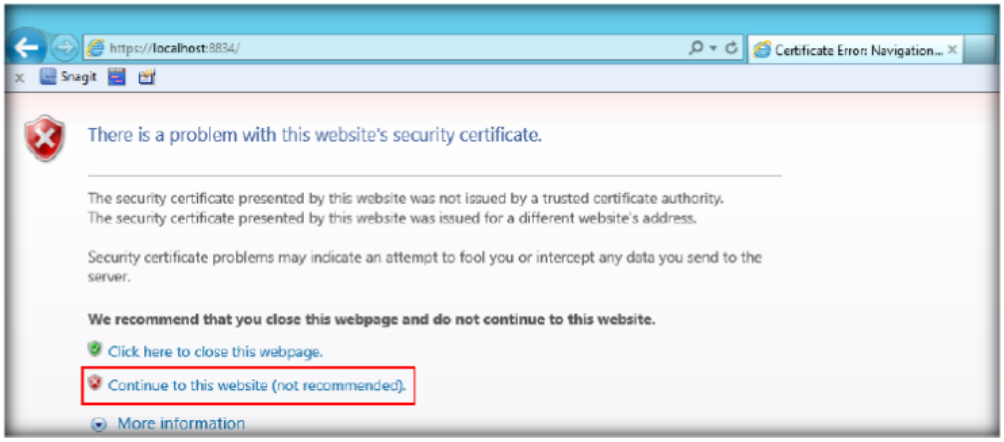


FIGURE 10.10: Internet Explorer website's security certificate

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

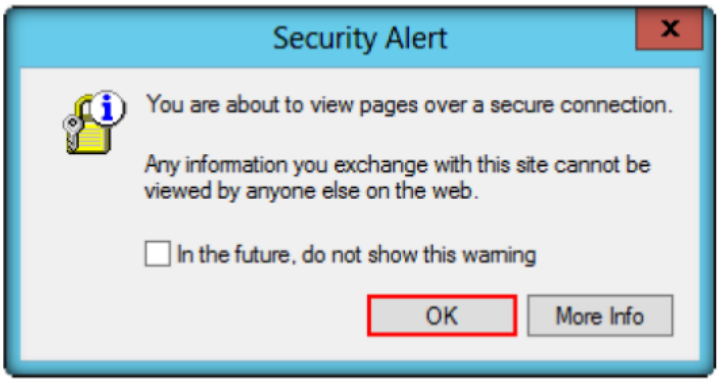


FIGURE 10.11: Internet Explorer Security Alert

16. The **Thank you for installing Nessus** screen appears. Click the **Get Started >** button.

warning, a custom certificate to your organization must be used

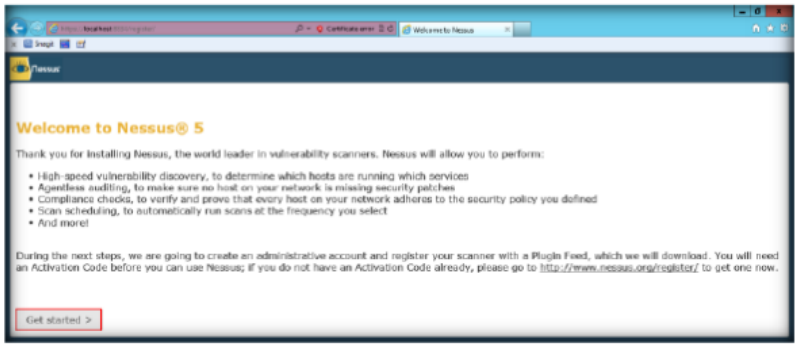


FIGURE 10.11: Nessus Getting Started

17. In **Initial Account Setup** enter the credentials given at the time of registration and click **Next >**.

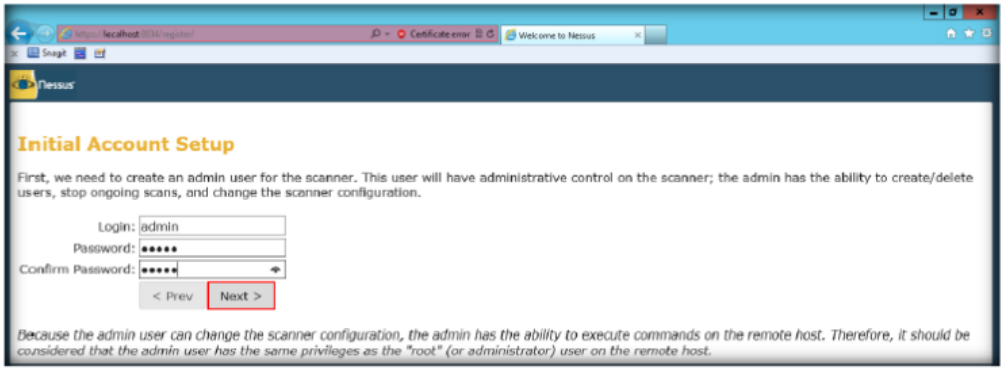


FIGURE 10.12: Nessus Initial Account Setup

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.

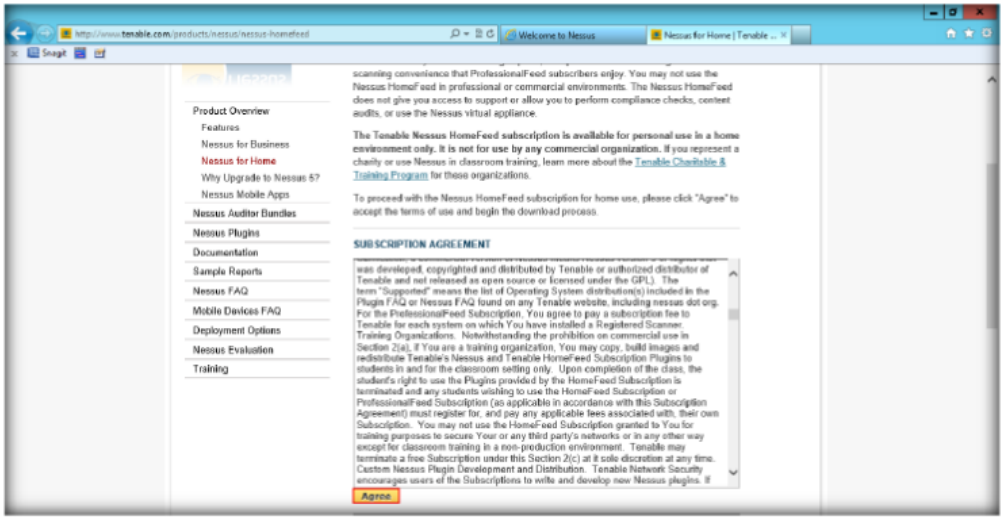


FIGURE 10.14: Nessus Subscription Agreement

21. Fill in the **Register a HomeFeed** section to obtain an activation code and click **Register**.

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.

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 plugins-customers.nessus.org

23. Now log in to your email for the activation code provided at the time of registration as shown in the following figure.

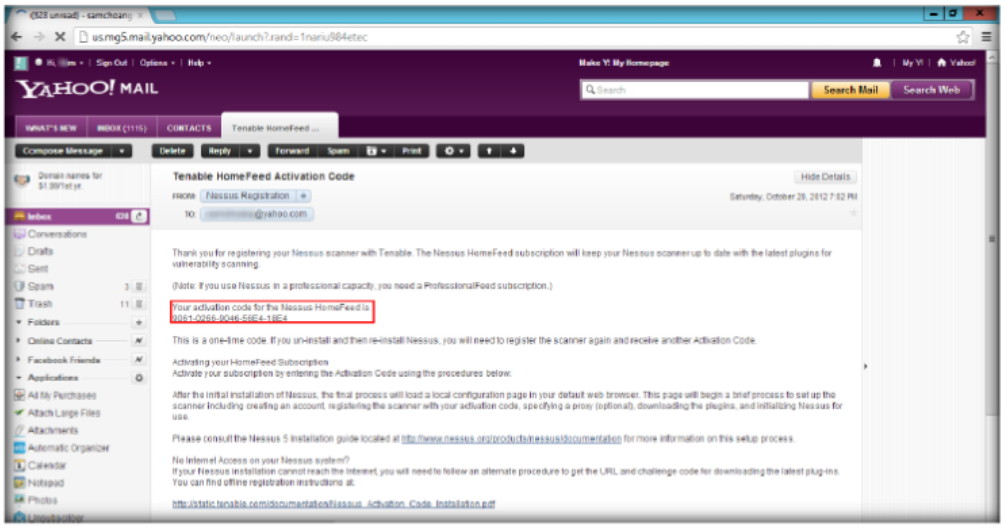


FIGURE 10.17: Nessus Registration mail

24. 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

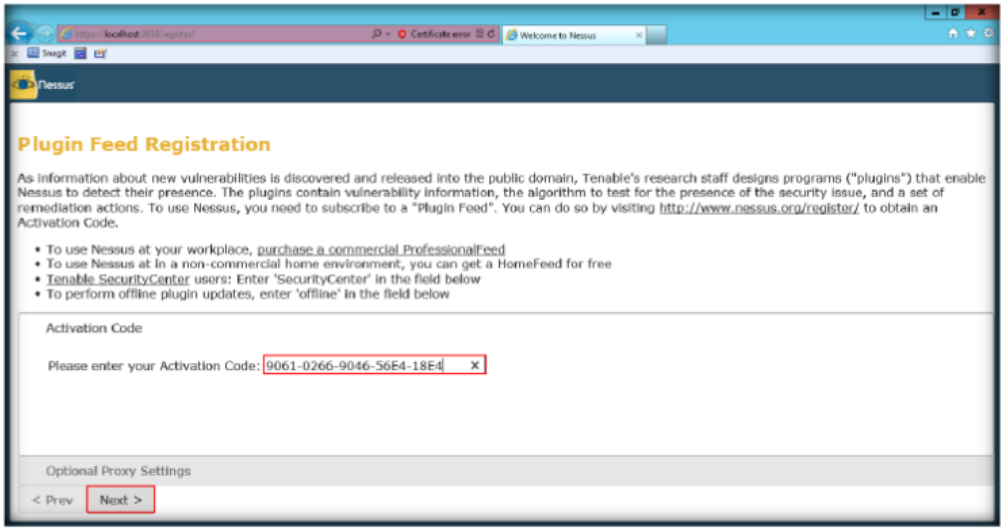


FIGURE 10.18: Nessus Applying Activation Code

25. The **Registering** window appears as shown in the following screenshot.

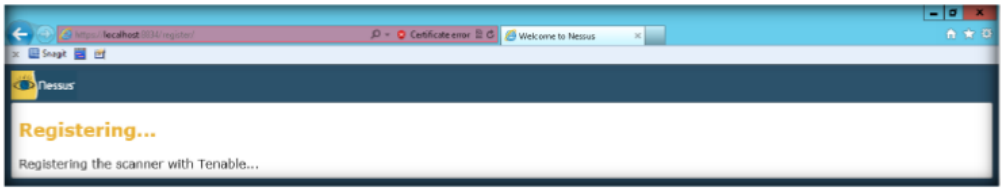


FIGURE 10.19: Nessus Registering Activation Code

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

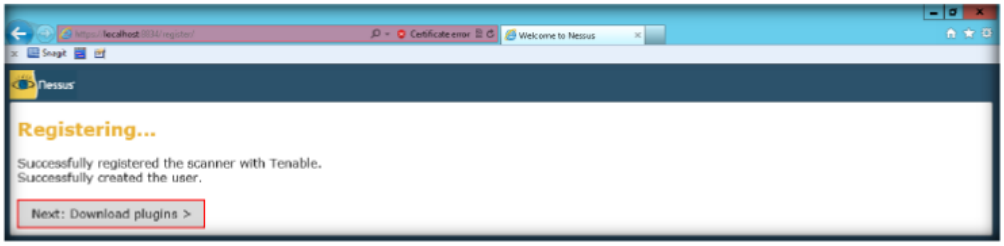


FIGURE 10.20: Nessus Downloading Plugins

27. Nessus will start fetching the plugins and it will install them, it will take time to install plugins and initialization

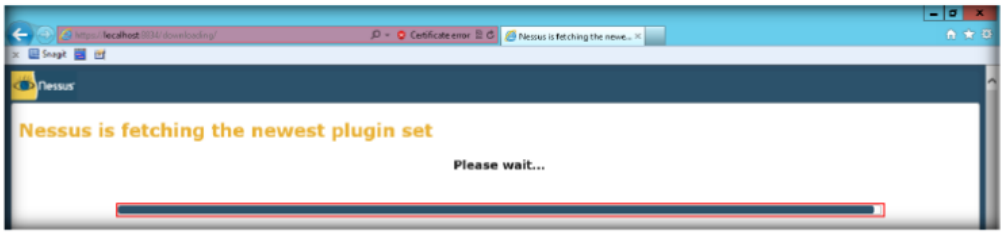


FIGURE 10.21: Nessus fetching the newest plugin set

28. The **Nessus Log In** page appears. Enter the **Username** and **Password** given at the time of registration and click **Log In**.

TASK 2

Network Scan Vulnerabilities

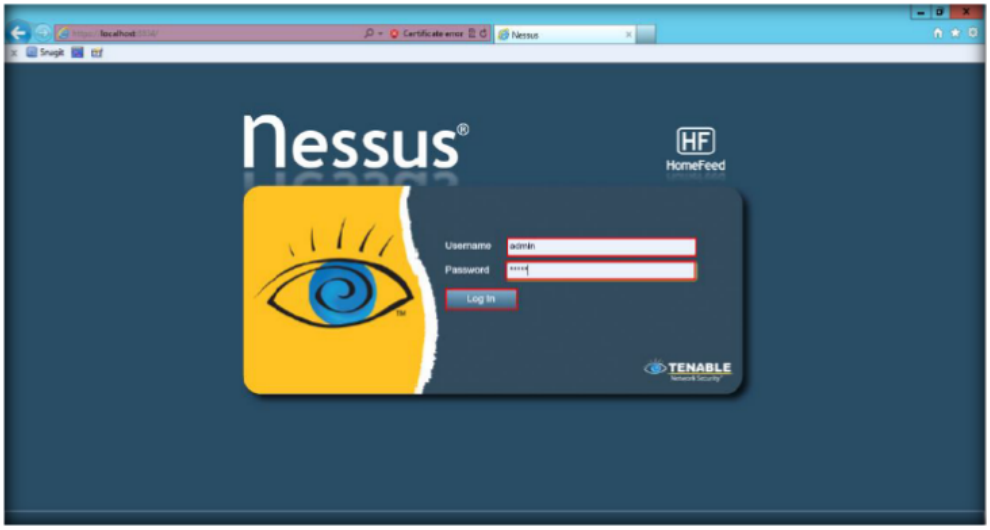


FIGURE 10.22: The Nessus Log In screen

For the item SSH user name, enter the name of the account that is dedicated to Nessus on each of the scan target systems.

29. The **Nessus HomeFeed** window appears. Click **OK**.

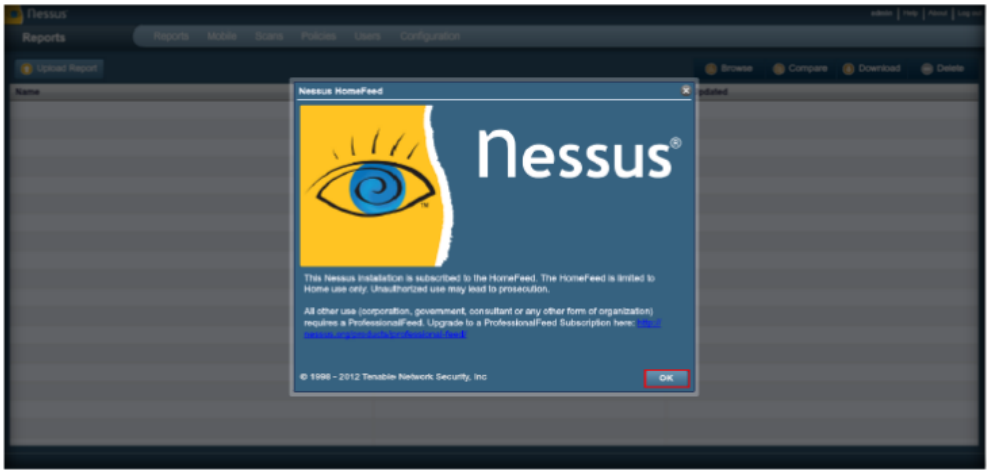


FIGURE 10.23: Nessus HomeFeed subscription

30. After you successfully log in, the **Nessus Daemon** window appears as shown in the following screenshot.

To add a new policy, click Policies → Add Policy.

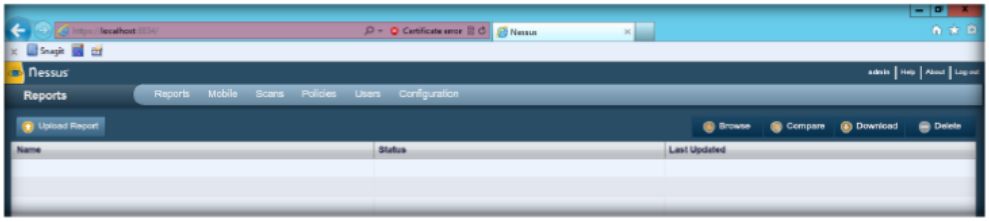


FIGURE 10.24: The Nessus main screen

31. If you have an **Administrator Role**, you can see the **Users** tab, which lists all **Users**, their **Roles**, and their **Last Logins**.

New policies are configured using the Credentials tab.

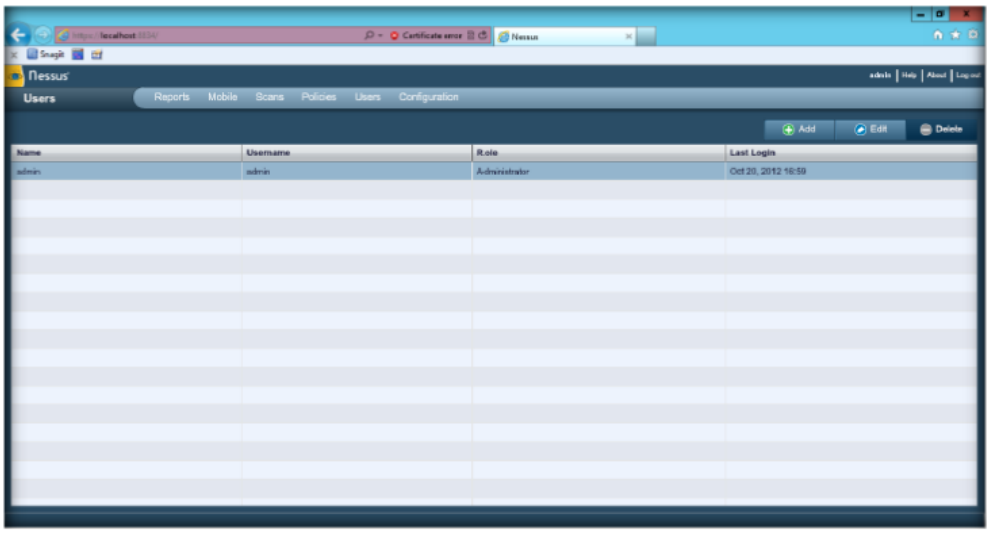


FIGURE 10.25: The Nessus administrator view

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**.

WARNING: Any changes to the Nessus scanner configuration will affect ALL Nessus users. Edit these options carefully

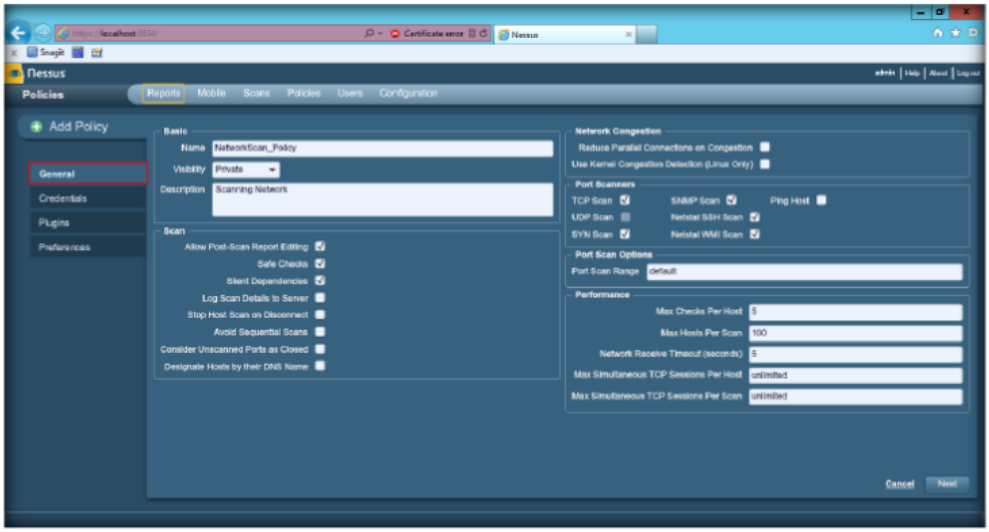


FIGURE 10.26: Adding Policies

33. To configure the credentials of new policy, click the **Credentials** tab shown in the left pane of **Add Policy**.

The most effective credentials scans are those for which the supplied credentials have root privileges.

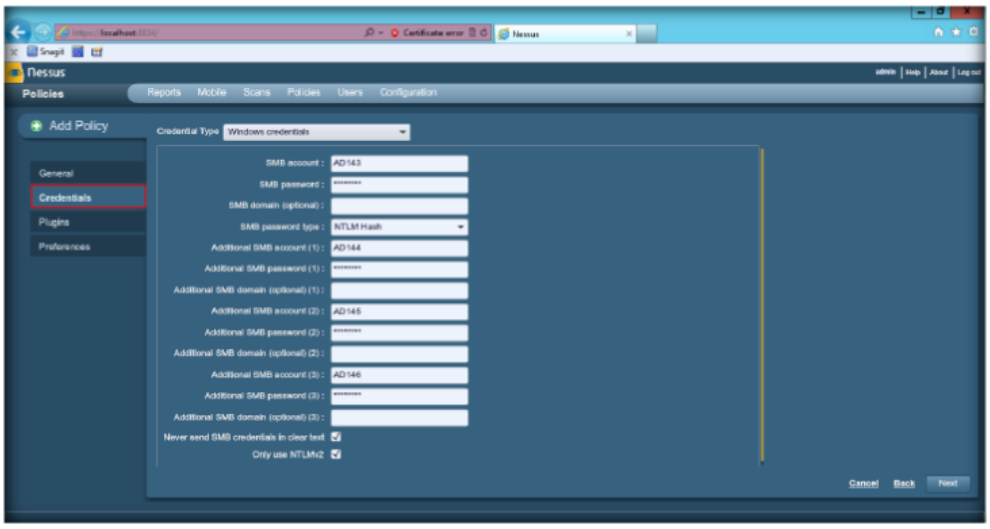


FIGURE 10.27: Adding Policies and setting Credentials

34. To select the required plugins, click the **Plugins** tab in the left pane of **Add Policy**.

If you are using Kerberos, you must configure a Nessus scanner to authenticate a KDC.

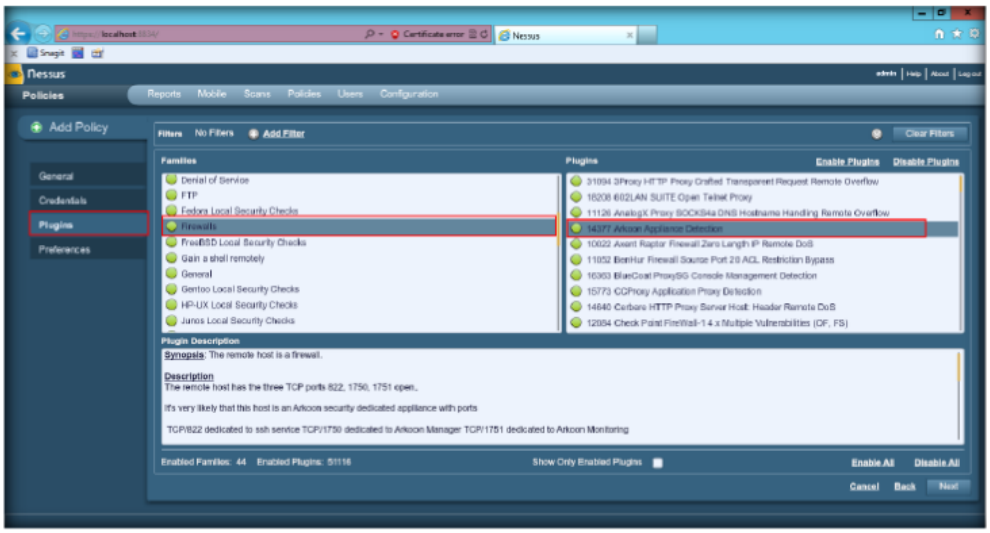


FIGURE 10.28: Adding Policies and selecting Plugins

35. To configure preferences, click the **Preferences** tab in the left pane of **Add Policy**.
36. In the **Plugin** field, select **Database settings** from the drop-down list.

If the policy is successfully added, then the Nessus server displays the massage.

37. Enter the **Login** details given at the time of registration.
38. Give the Database SID: **4587**, Database port to use: **124**, and select Oracle auth type: **SYSDBA**.
39. Click **Submit**.

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

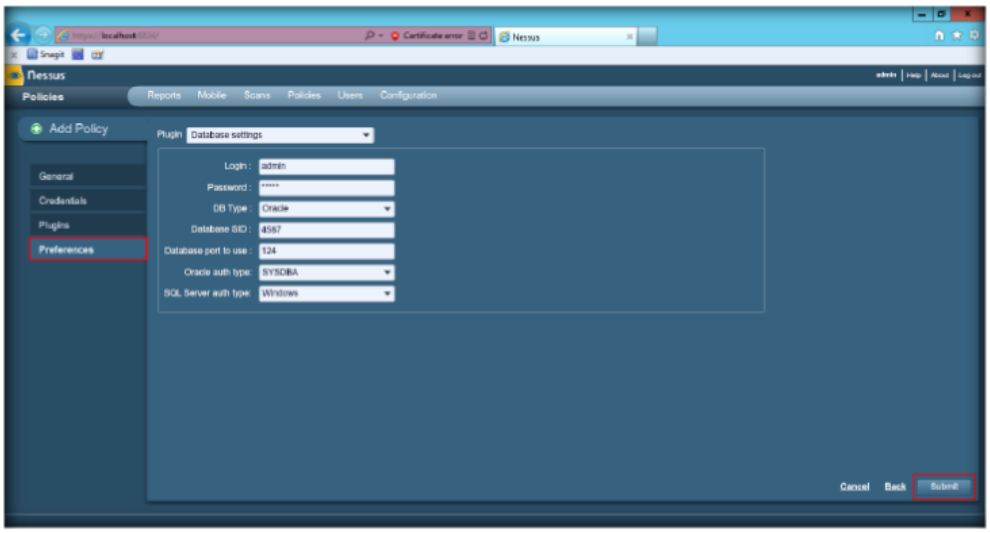


FIGURE 10.29: Adding Policies and setting Preferences

40. A message **Policy "NetworkScan_Policy" was successfully added** displays as shown as follows.

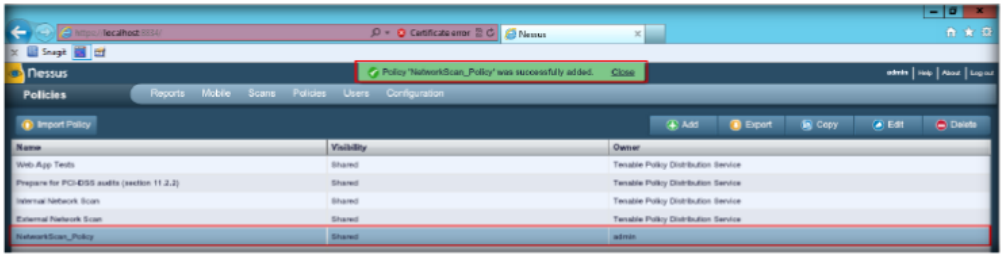


FIGURE 10.30: The NetworkScan Policy

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

Nessus has the ability to save configured scan policies, network targets, and reports as a .nessus file.

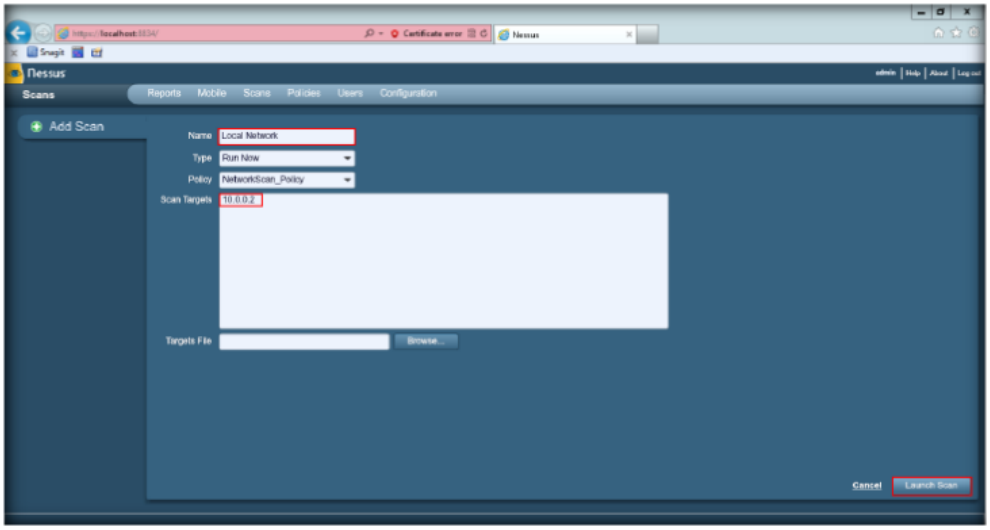


FIGURE 10.31: Add Scan

45. The scan launches and **starts scanning** the network.

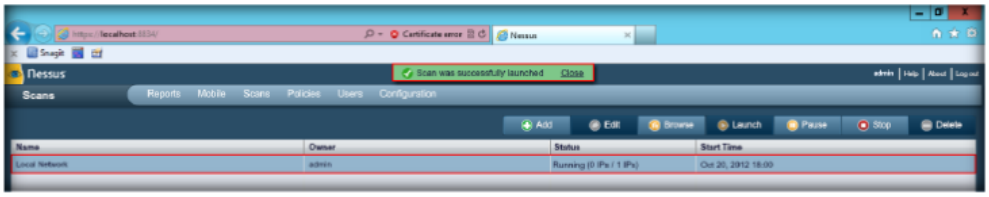


FIGURE 10.32: Scanning in progress

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.

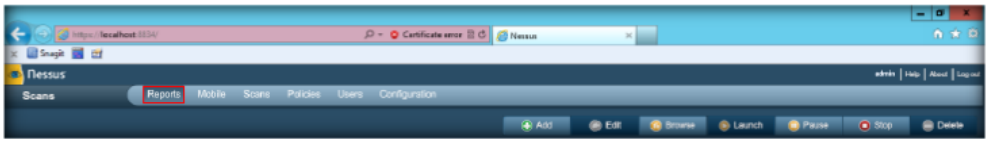


FIGURE 10.33: Nessus Reports tab

47. Double-click **Local Network** to view the detailed scan report.

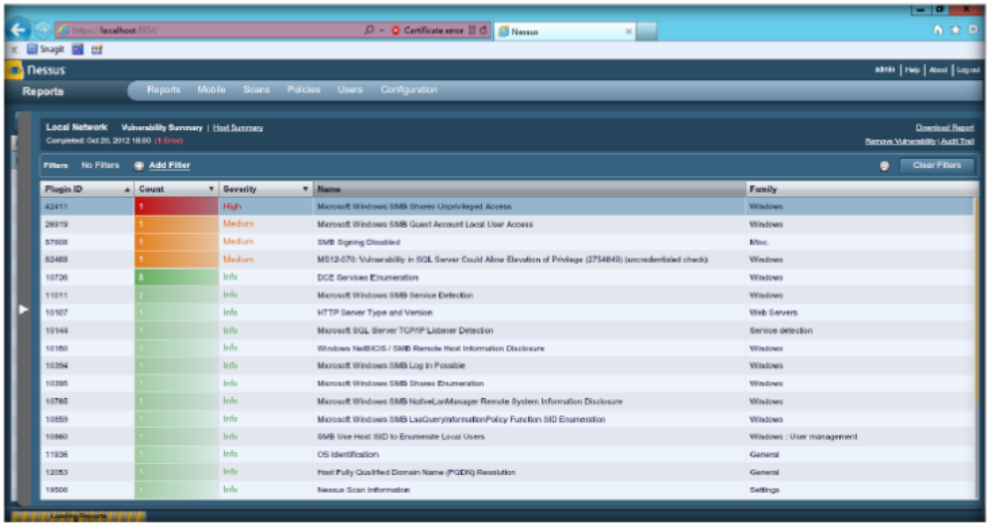
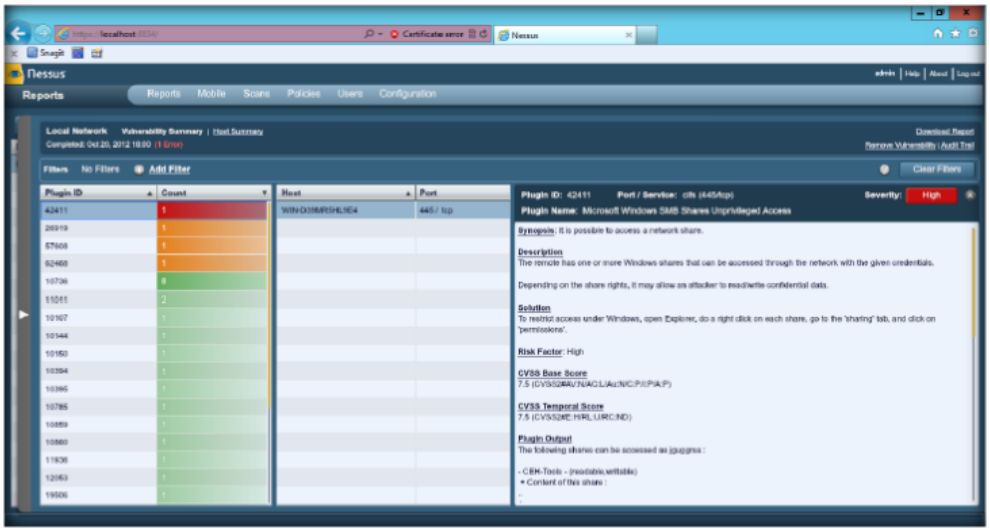


FIGURE 10.34: Report of the scanned target

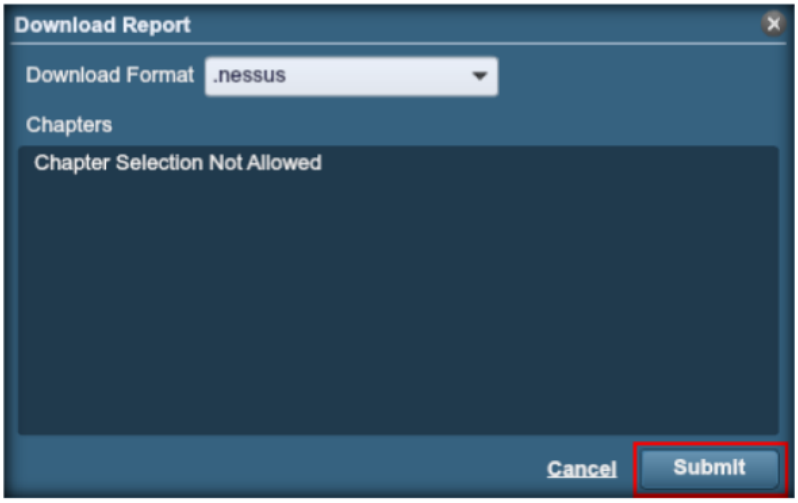
48. Double-click any **result** to display a more detailed synopsis, description, security level, and solution.



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

49. Click the **Download Report** button in the left pane.
50. 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

51. Now, click **Log out**.
52. 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	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ 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 (IDSes) 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

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.

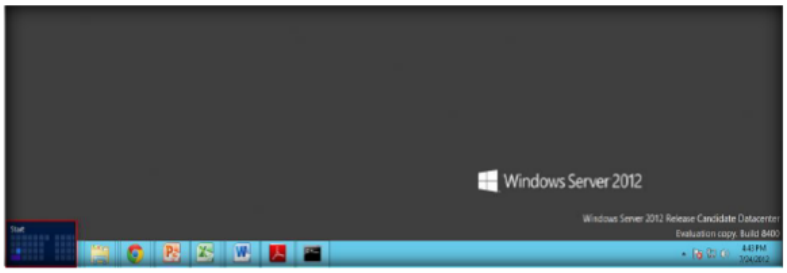


FIGURE 11.1: Windows Server 2012 – Desktop view

2. Click the **Global Network Inventory** app to open the **Global Network Inventory** window.

📖 Scan computers by IP range, by domain, single computers, or computers, defined by the Global Network Inventory host file

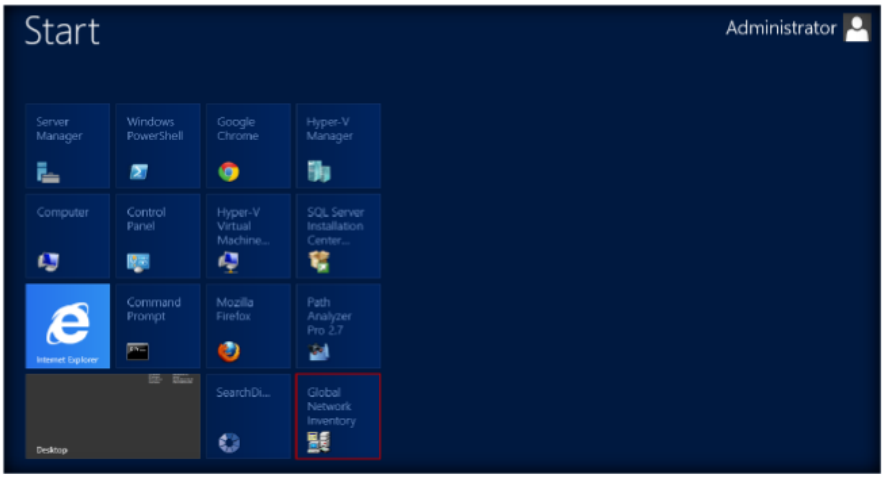


FIGURE 11.2: Windows Server 2012 – Apps

3. The **Global Network Inventory** Main window appears as shown in the following figure.
4. The **Tip of Day** window also appears; click **Close**.

🗁**Scan only items that you need by customizing scan elements**

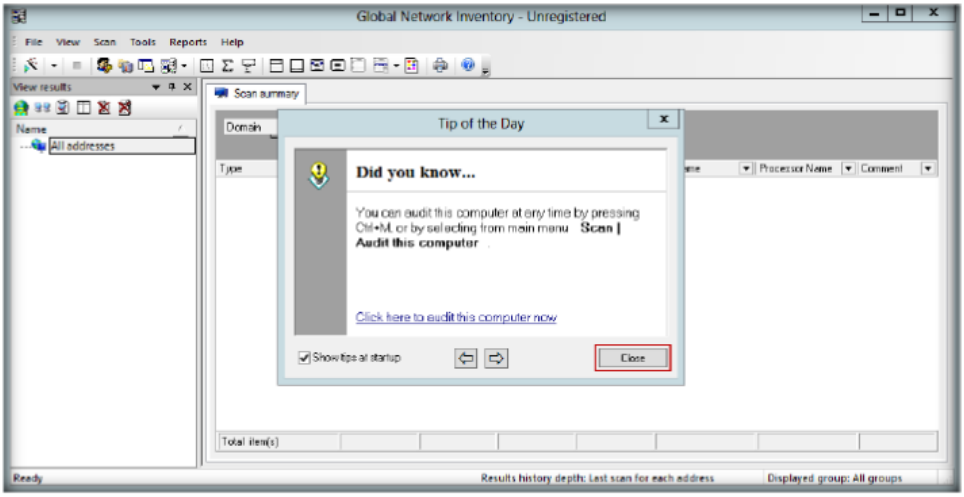


FIGURE 11.3: Global Network Inventory Main Window

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

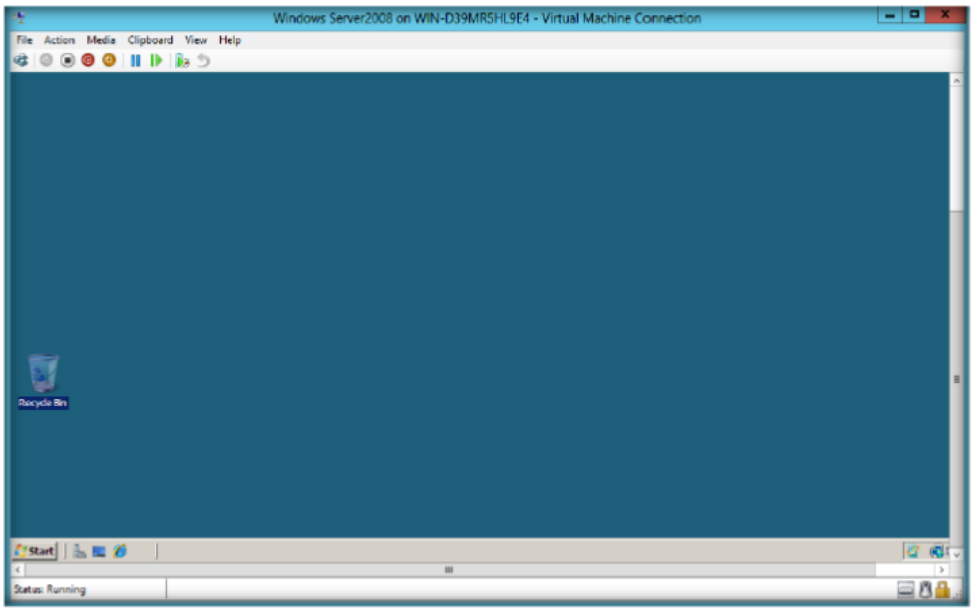


FIGURE 11.4: Windows 2008 Virtual Machine

6. 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)**.

FIGURE 11.5: Global Network Inventory new audit wizard

7. Select **IP range** scan and then click **Next** in the **Audit Scan Mode** wizard.

VIEWS SCAN RESULTS, INCLUDING HISTORIC RESULTS FOR ALL SCANS, INDIVIDUAL MACHINES, OR SELECTED NUMBER OF ADDRESSES

Fully customizable layouts and color schemes on all views and reports

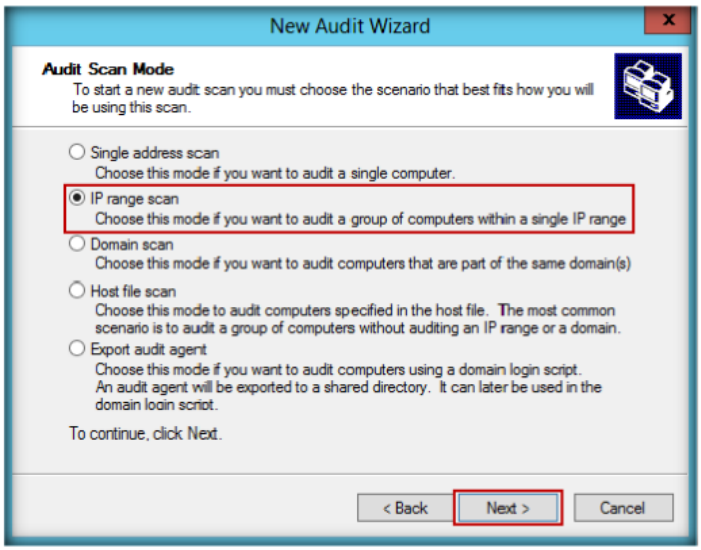


FIGURE 11.6: Global Network Inventory Audit Scan Mode

8. Set an **IP range** scanand then click **Next** in the **IP Range Scan** wizard.

Export data to HTML, XML, Microsoft Excel, and text formats

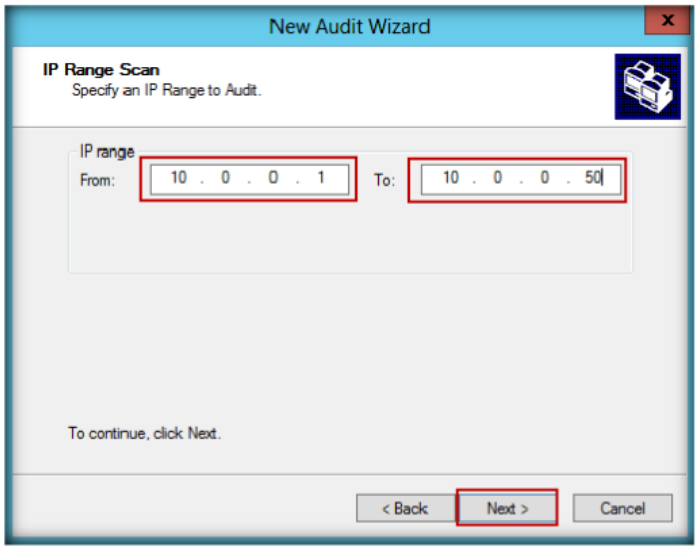


FIGURE 11.7: Global Network Inventory setting an IP range to scan

Licenses are network-based rather than user-based. In addition, extra licenses to cover additional addresses can be purchased at any time if required

9. 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

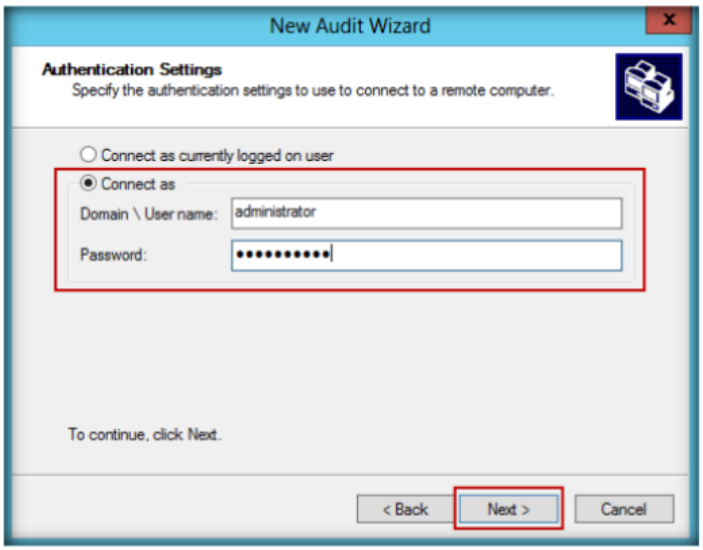


FIGURE 11.8 Global Network Inventory Authentication settings

10. Live 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 a 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.

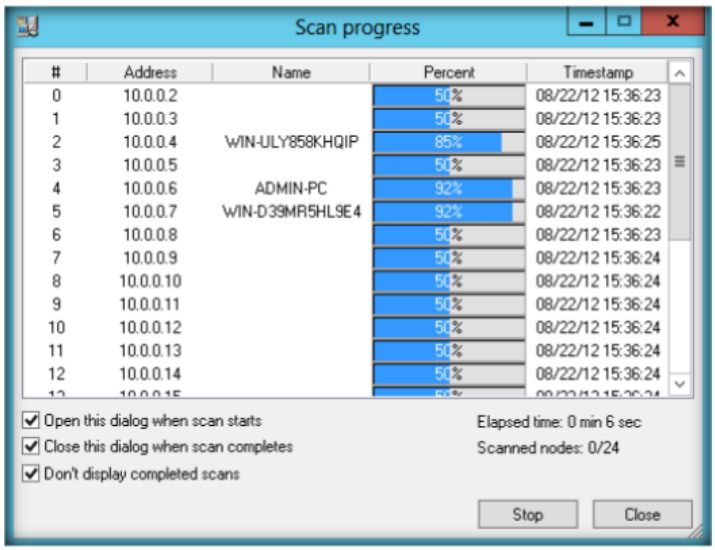


FIGURE 11.10: Global Network Inventory Scanning Progress

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)

12. After completion, **scanning results** can be viewed as shown in the following figure.

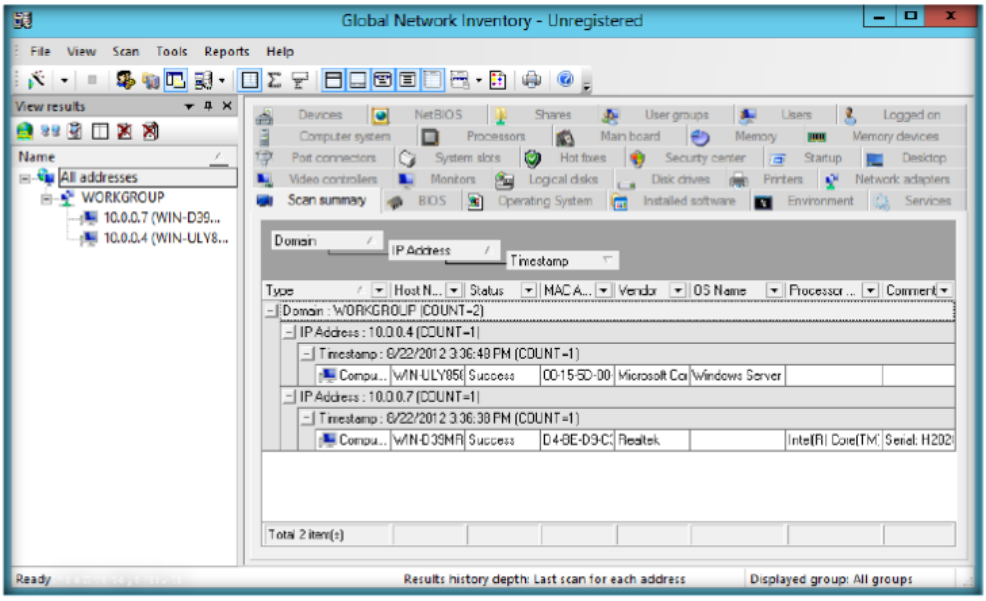


FIGURE 11.11: Global Network Inventory result window

Global Network Inventory lets you change grid layout simply by dragging column headers using the mouse. Dropping a header onto the Grouping pane groups data according to the values stored within the "grouped" column

13. Now select **Windows Server 2008** machine from view results to view individual results.

Global Network Inventory grid color scheme is completely customizable.
You can change Global Network Inventory colors by selecting **Tools | Grid colors** from main menu and changing colors

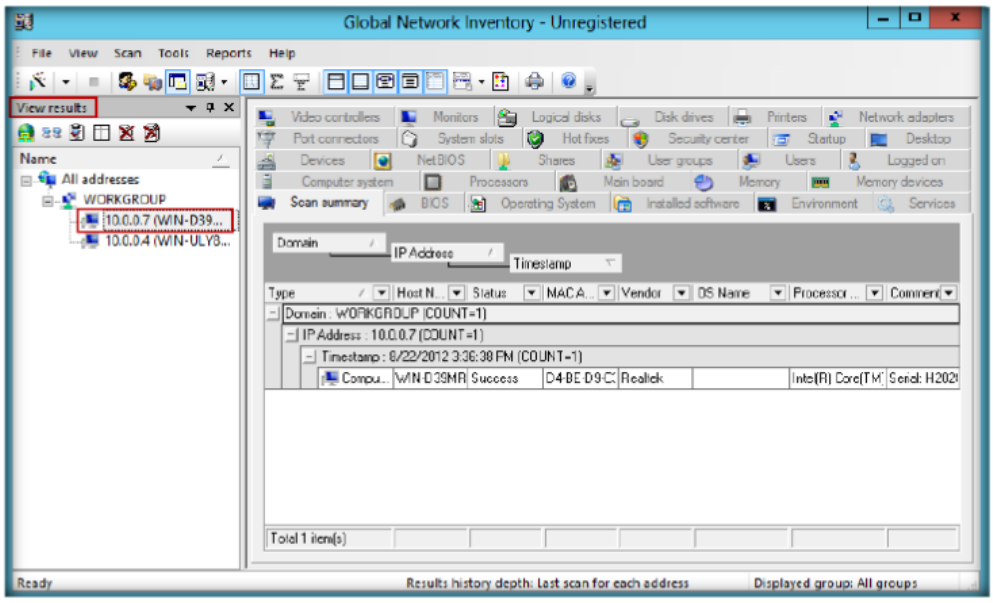


FIGURE 11.12: Global Network Inventory Individual machine results

14. The **Scan Summary** section gives you a brief summary of the machines that have been scanned.

To configure results history level choose Scan | Results history level from the main menu and set the desired history level

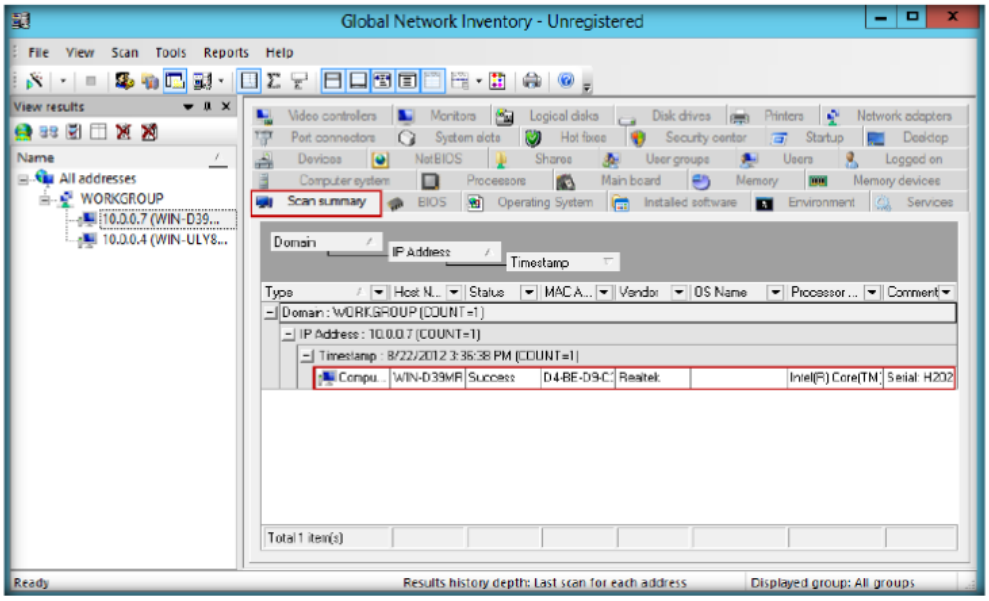


FIGURE 11.13: Global Inventory Scan Summary tab

15. The **Bios** section gives details of Bios settings.

Scan only items that you need by customizing scan elements

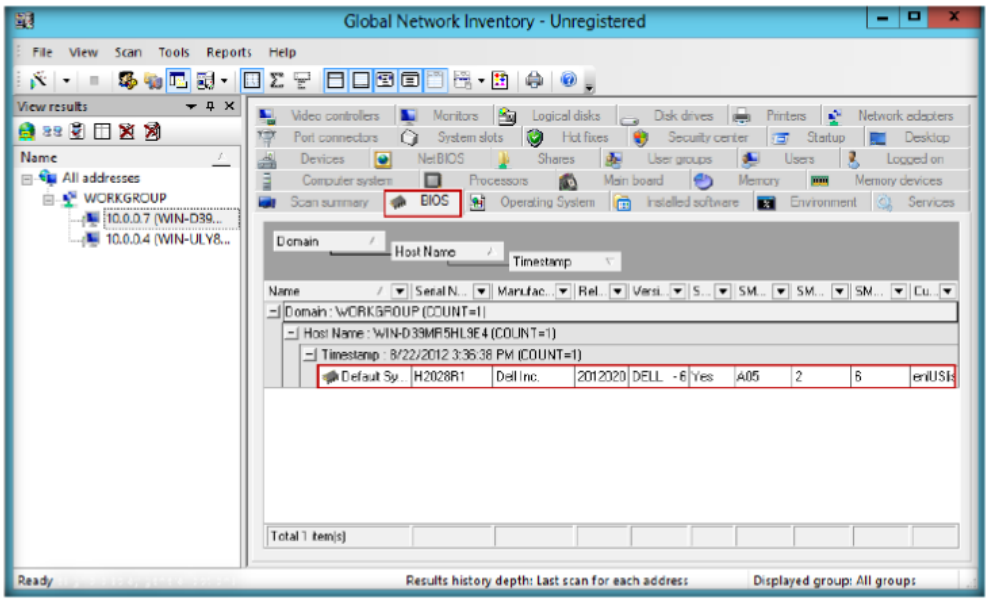


FIGURE 11.14: Global Network Inventory Bios summary tab

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

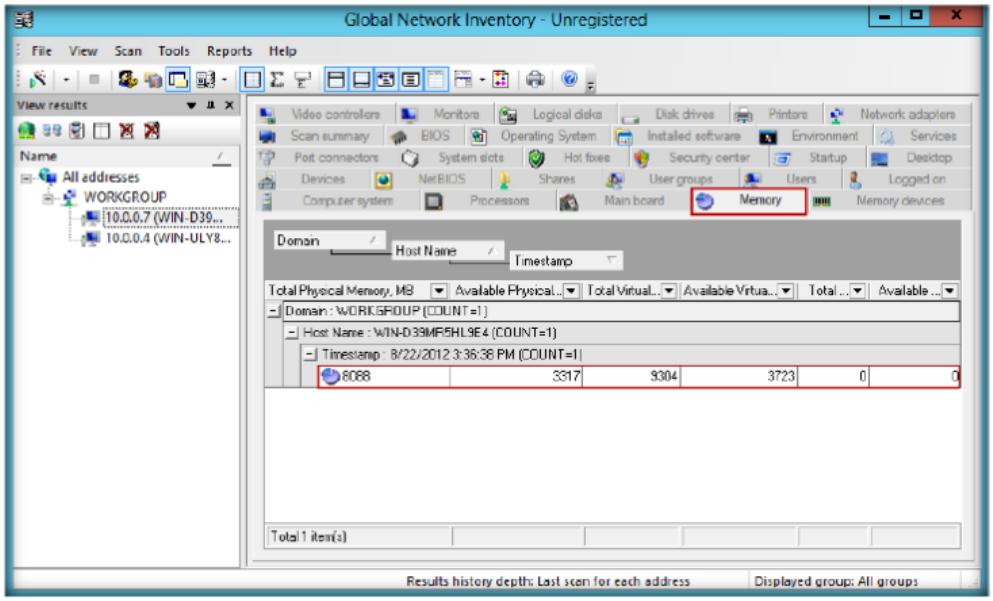


FIGURE 11.15: Global Network Inventory Memory tab

17. In the **NetBIOS** section, complete details can be viewed.

Message subject - Type the Subject of your message. Global Network Inventory cannot post a message that does not contain a subject

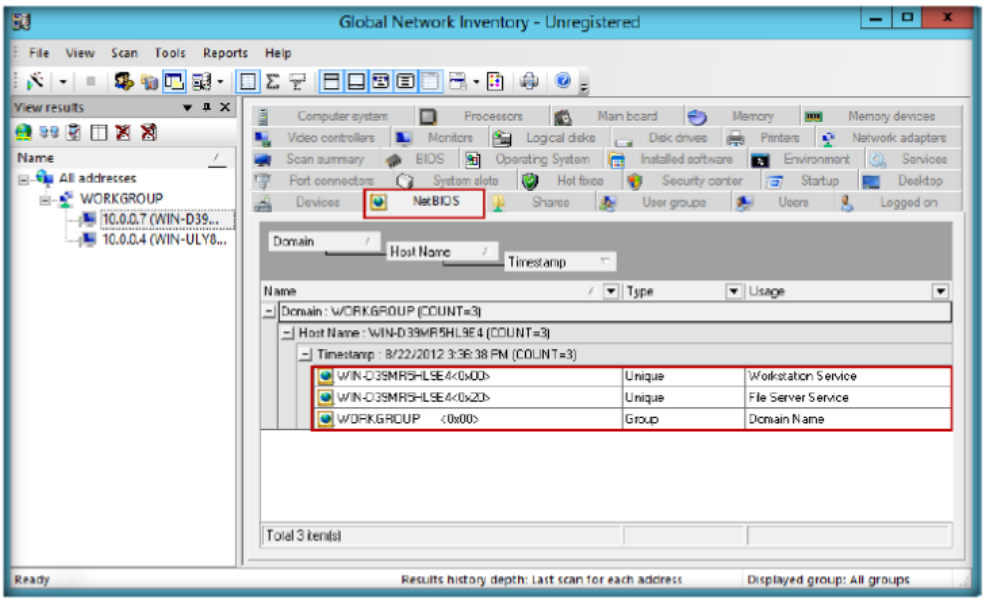


FIGURE 11.16: Global Network Inventory NetBIOS tab

18. The **User Groups** tab shows user account details with the work group.

Name - Specifies the friendly name associated with your e-mail address. When you send messages, this name appears in the From box of your outgoing messages

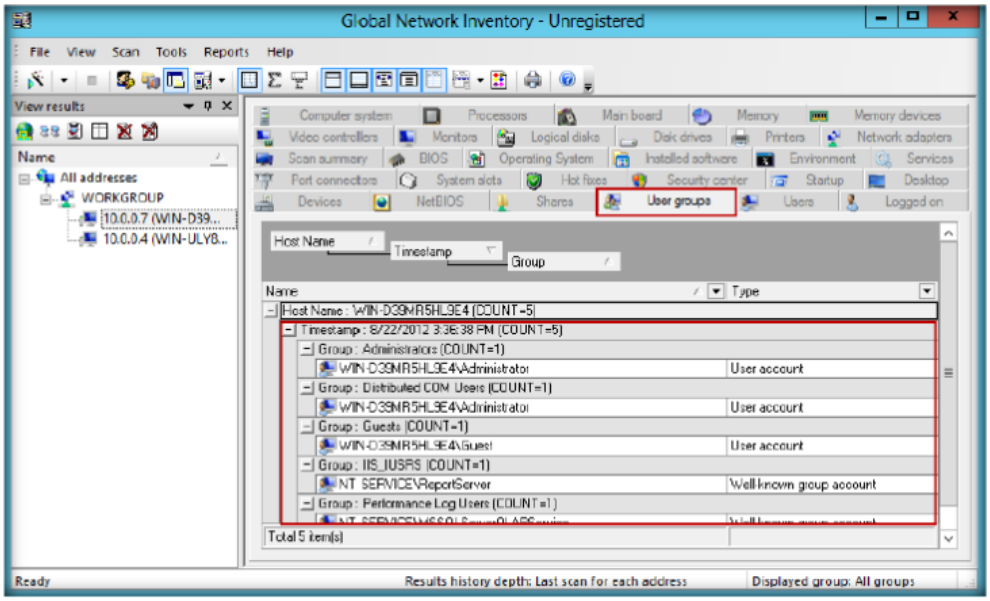


FIGURE 11.17: Global Network Inventory User groups section

19. The **Logged on** tab shows detailed logged on details of the machine.

Port - Specifies the port number you connect to on your outgoing e-mail (SMTP) server. This port number is usually 25.

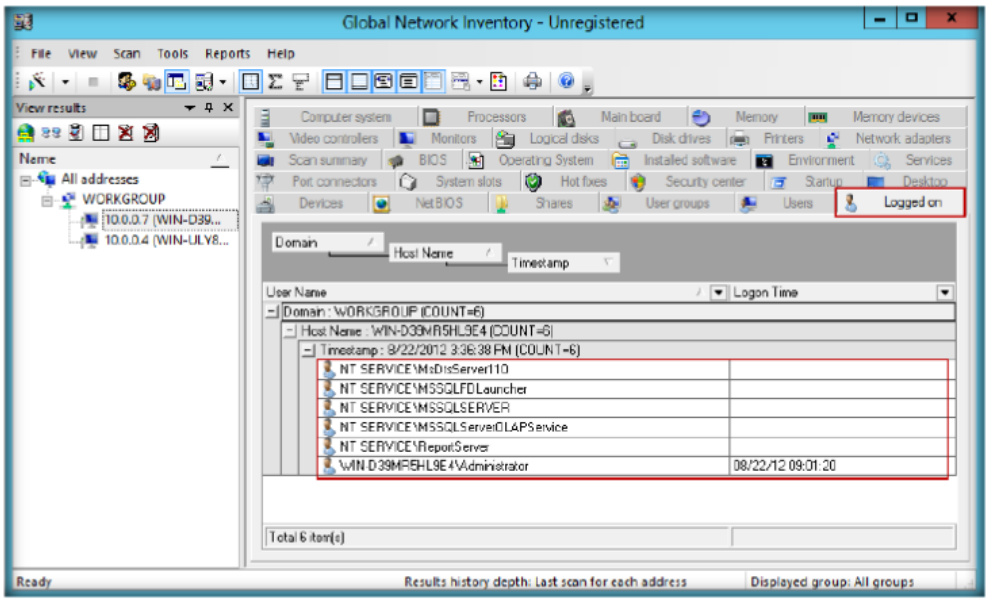


FIGURE 11.18: Global Network Inventory Logged on Section

20. The **Port connectors** section shows ports connected in the network.

Outgoing mail (SMTP) - Specifies your Simple Mail Transfer Protocol (SMTP) server for outgoing messages

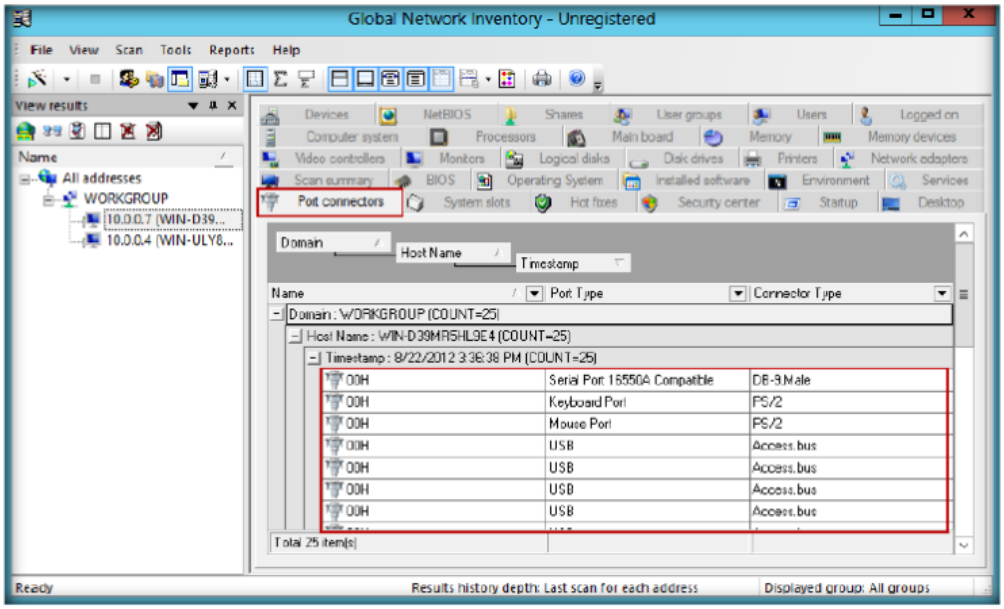


FIGURE 11.19: Global Network Inventory Port connectors tab

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

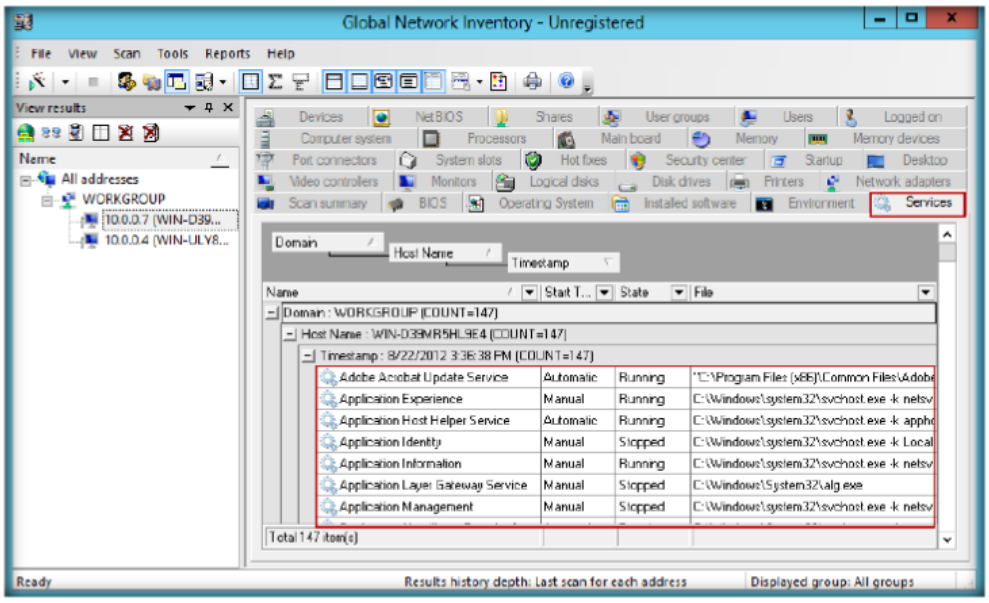


FIGURE 11.20: Global Network Inventory Services Section

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

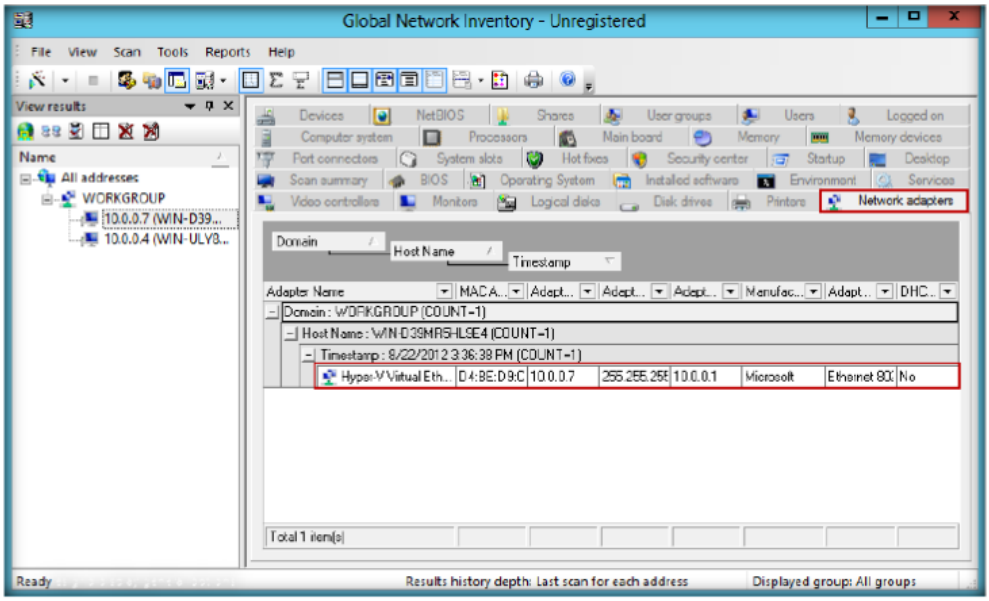


FIGURE 11.21: Global Network Inventory Network Adapter tab

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	**IP Scan Range:** 10.0.0.1 – 10.0.0.50
	Scanned IP Address: 10.0.0.7,10.0.0.4
	Result: ▪ 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	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ 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:

- 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

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

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

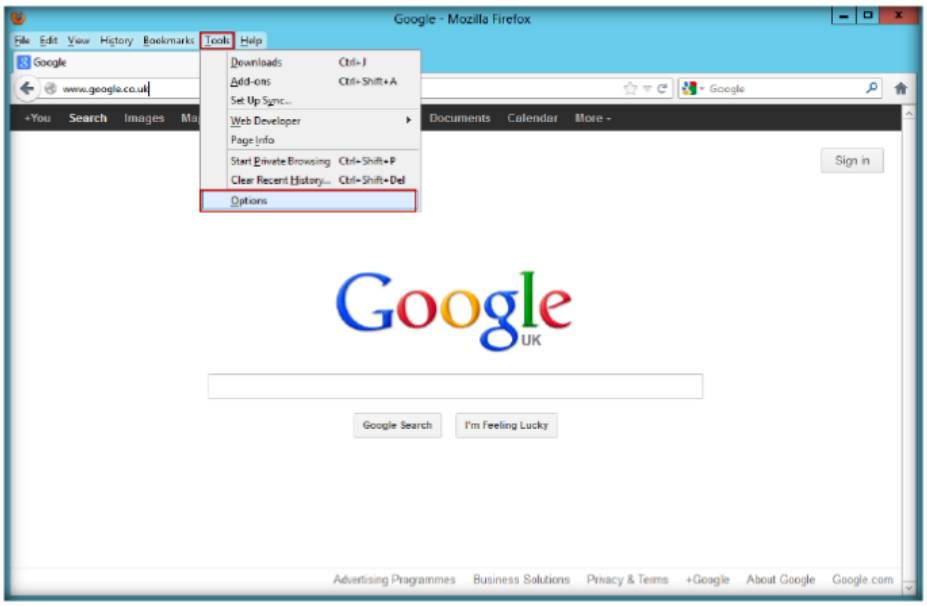


FIGURE 12.1: Firefox options tab

6. Go to the **Advanced** profile in the **Options** wizard of Firefox, and select **Network** tab, and then click **Settings**.

Proxy Switcher fully compatible with Internet Explorer, Firefox, Opera and other programs

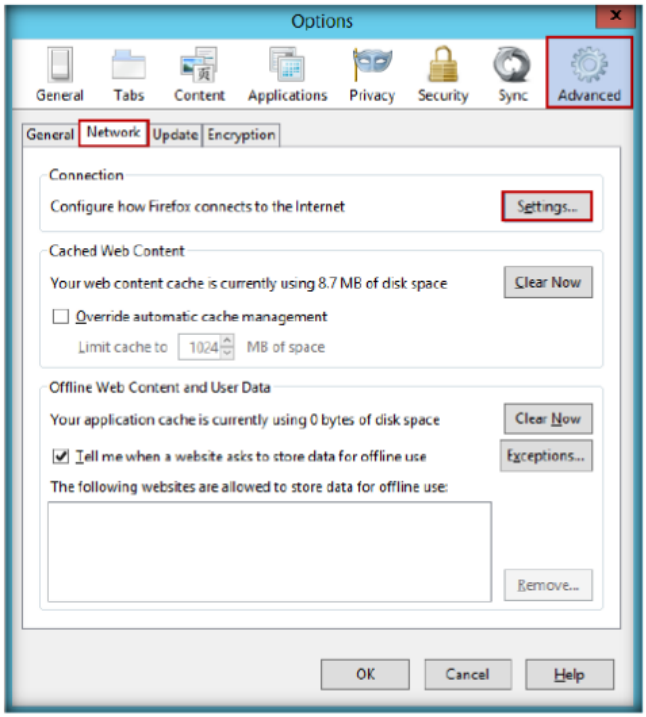


FIGURE 12.2: Firefox Network Settings

7. Select the **Use System proxy settings** radio button, and click **OK**.

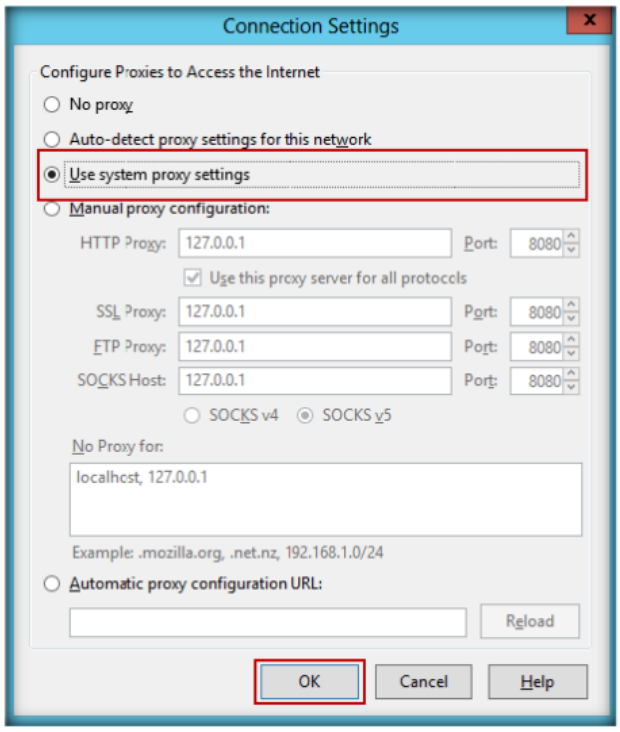


FIGURE 12.3: Firefox Connection Settings

proxy switcher supports following command line options:

-d: Activate direct connection

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.

TASK 1

Proxy Servers Downloading

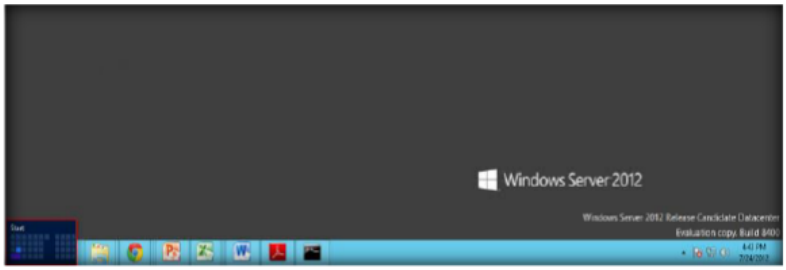


FIGURE 12.4: Windows Server 2012 – Desktop view

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

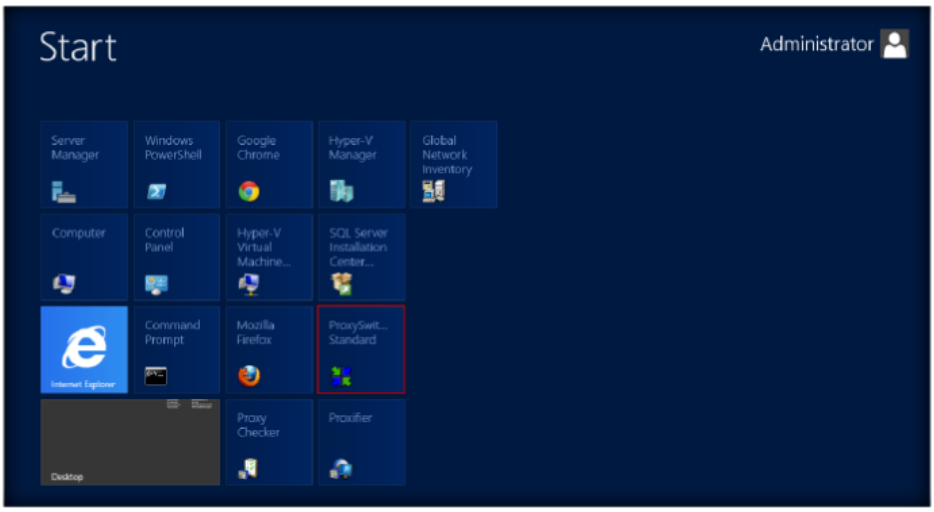


FIGURE 12.5: Windows Server 2012 – Apps

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.

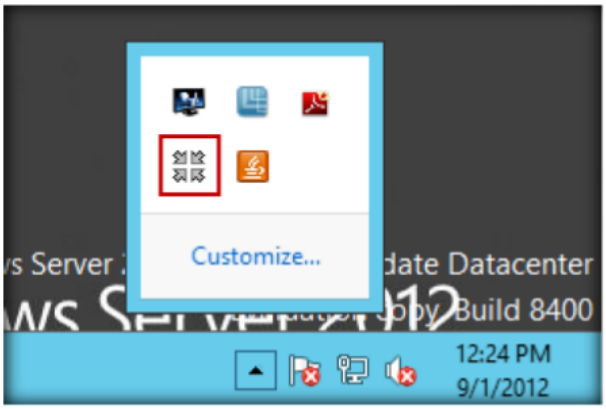


FIGURE 12.6: Select Proxy Switcher

11. The **Proxy List Wizard** will appear as shown in the following figure; click **Next**.

🗁 **Proxy Switcher ssupports for LAN, dialup, VPN and other RAS connections**

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).**

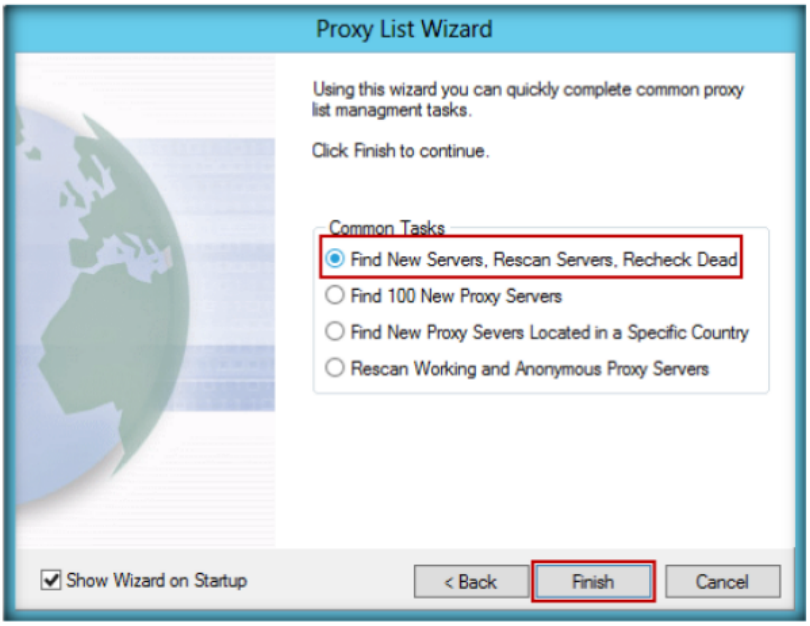


FIGURE 12.8: Select common tasks

13. A list of **downloaded proxy servers** will show in the left panel.

When Proxy Switcher is running in *Keep-Alive* mode it tries to maintain working proxy server connection by switching to different proxy server if current dies

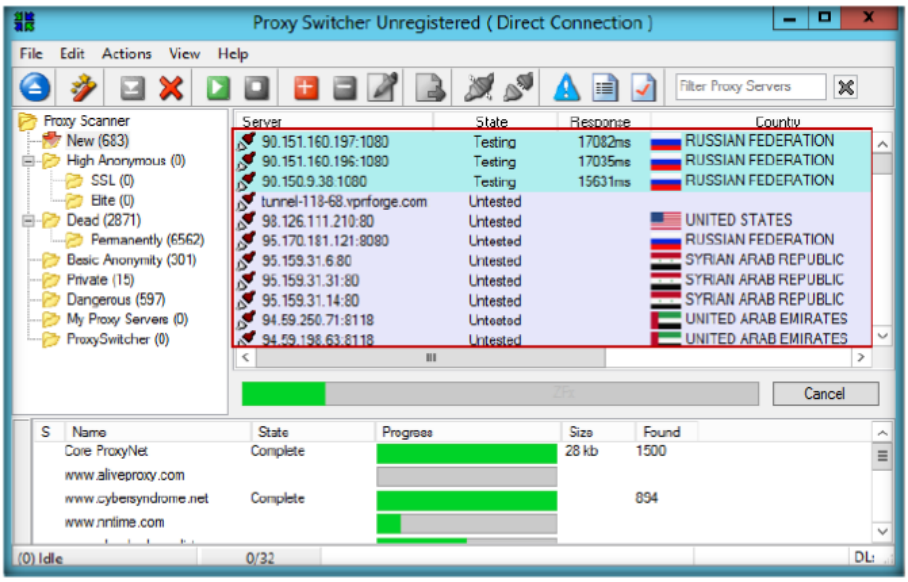


FIGURE 12.9: List of downloadeed Proxy Server

14. To **stop** downloading the proxy server click  .

When active proxy server becomes inaccessible Proxy Switcher will pick different server from **ProxySwitcher category**. If the active proxy server is currently *alive* the background will be green

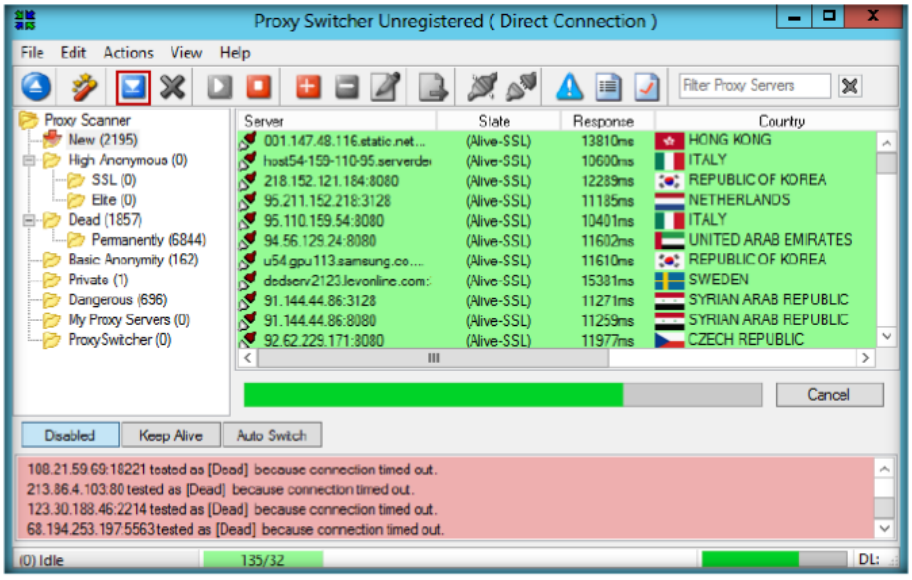


FIGURE 12.10: Click on Start button

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

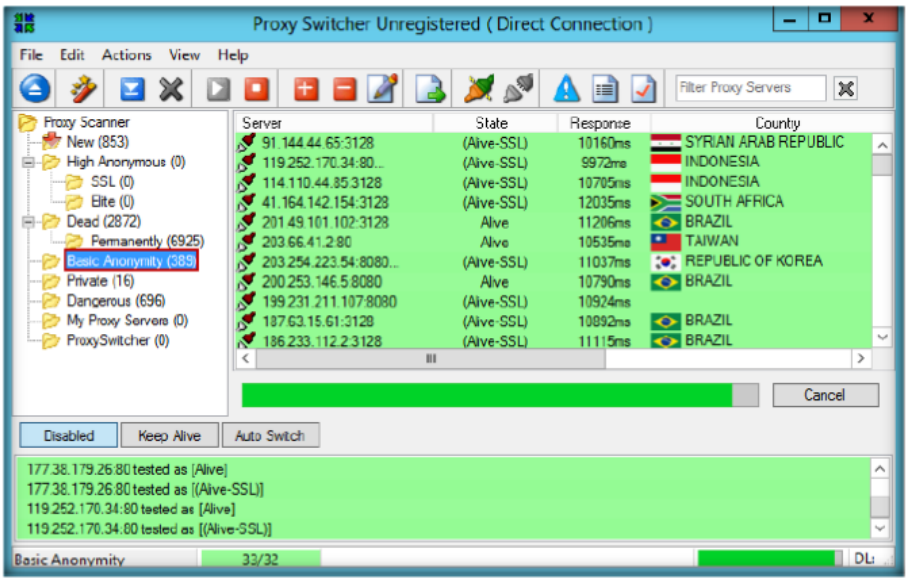


FIGURE 12.11: Selecting downloaded Proxy server from Basic Anonymity

16. Select one **Proxy server IP address** from right panel to swich the selected proxy server, and click the  icon.

In addition to standard add/remove/edit functions proxy manager contains functions useful for anonymous surfing and proxy availability testing

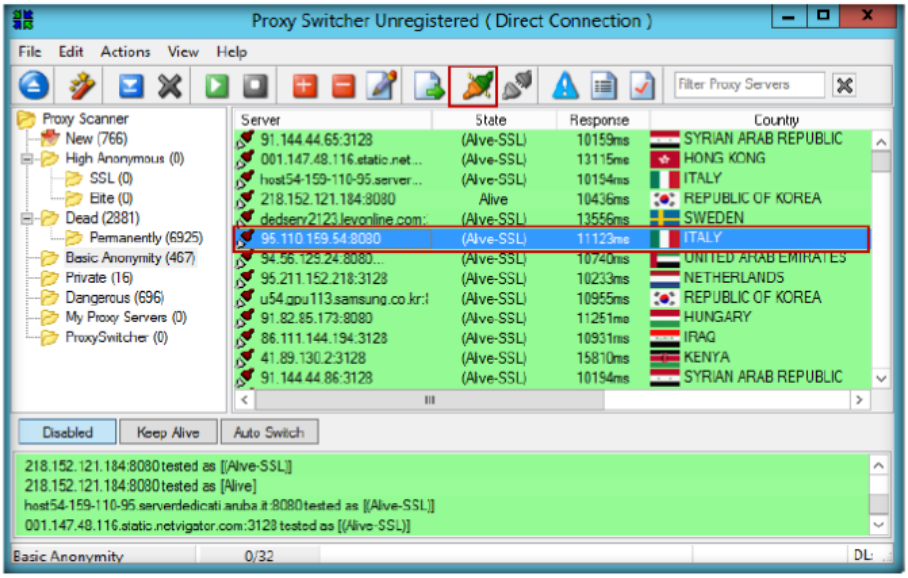


FIGURE 12.12: Selecting the proxy server

17. The selected **proxy server** will connect, and it will show the following connection icon.

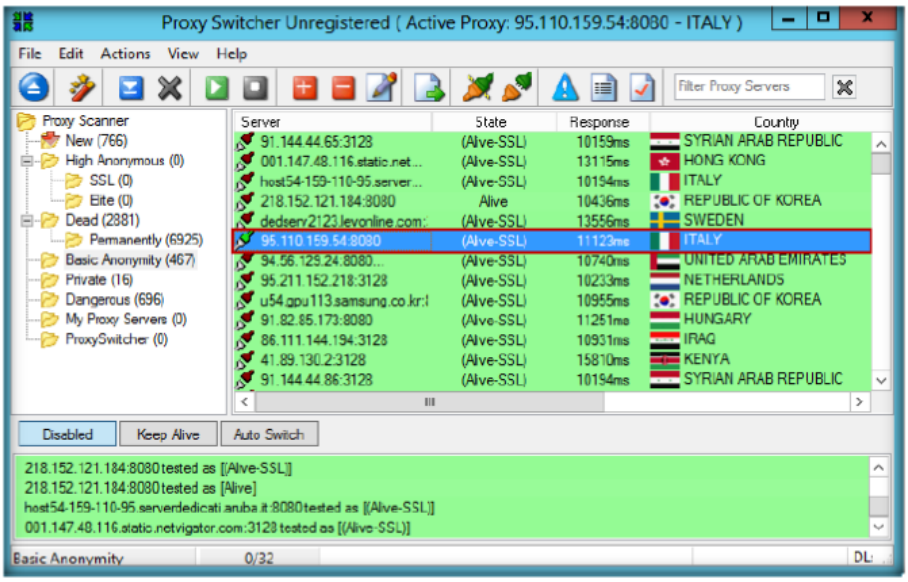


FIGURE 12.13: Succesful connection of selected proxy

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 connetivity; if it is successfully conncted, then it shows the following figure.

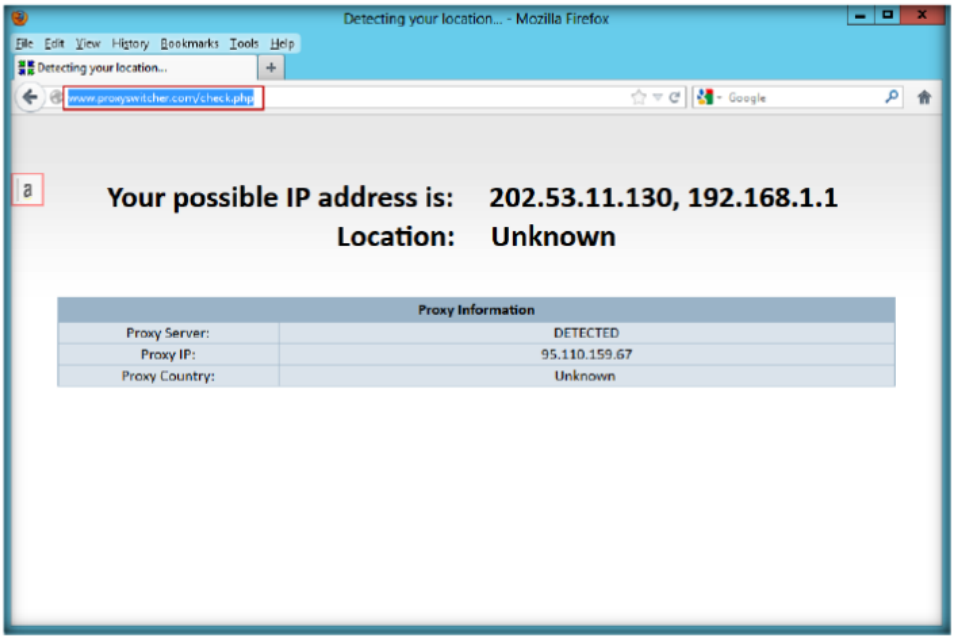


FIGURE 12.14: Detected Proxy server

19. Open another tab in the **web browser**, and surf anonymosly using this proxy.

After the anonymous proxy servers have become available for switching you can activate any one to become invisible for the sites you visit.

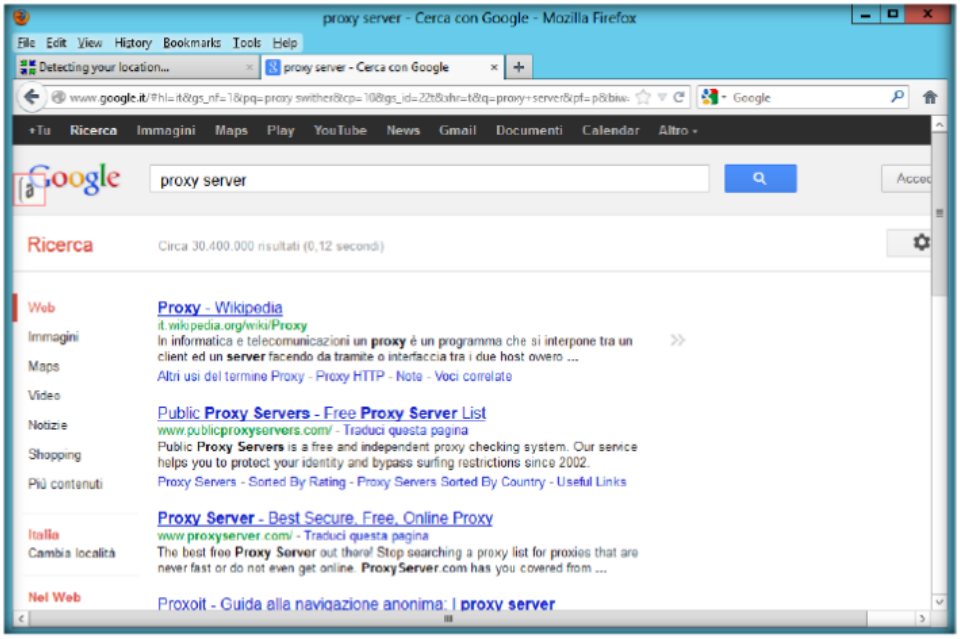


FIGURE 12.14: Surf using Proxy server

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**

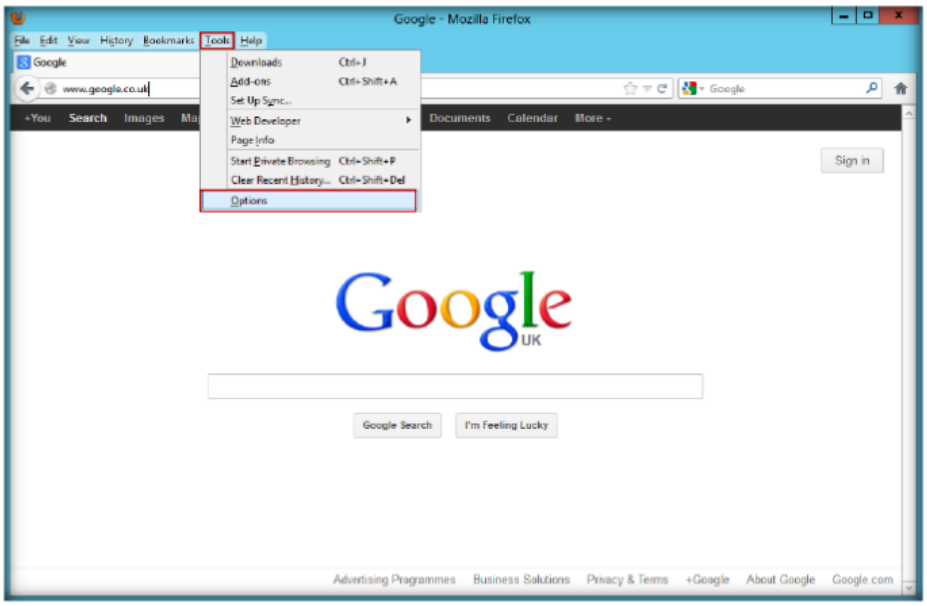


FIGURE 13.1: Firefox options tab

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

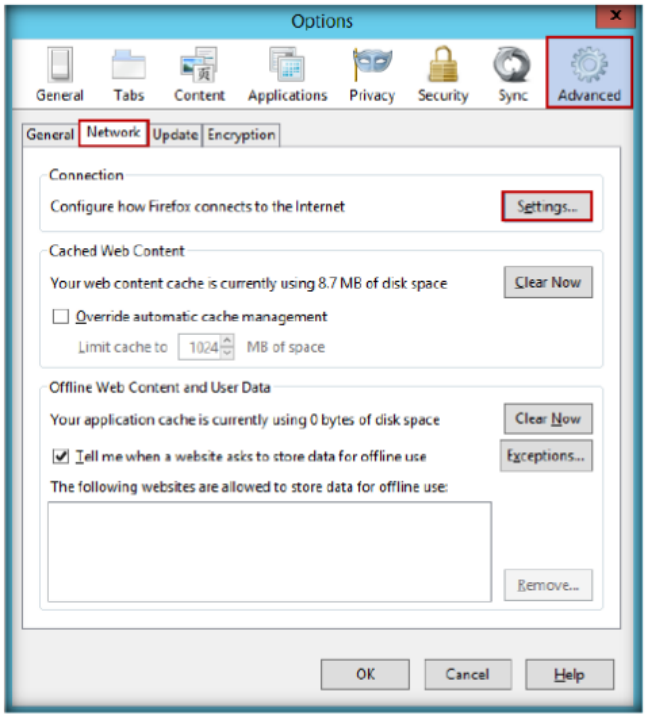


FIGURE 13.2: Firefox Network Settings

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**.

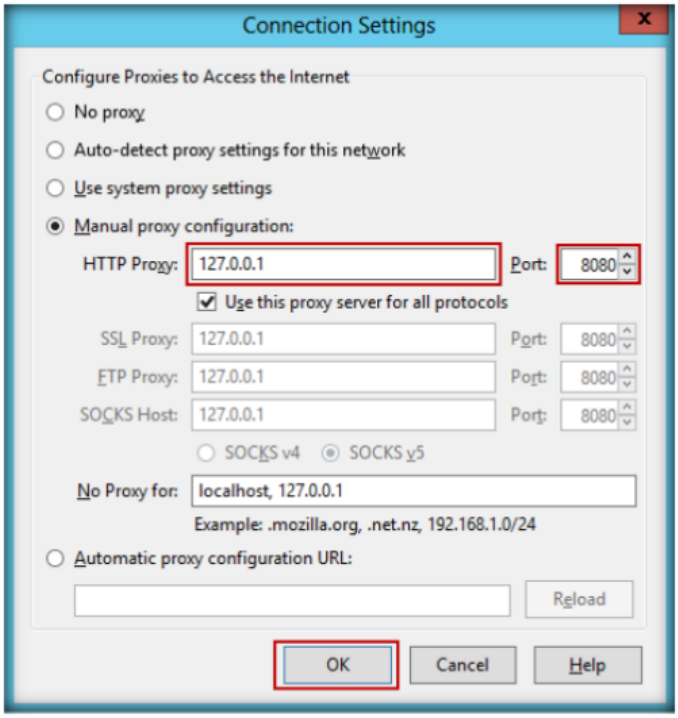


FIGURE 13.3: Firefox Connection Settings

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.

Scan computers by IP range, by domain, single computers, or computers, defined by the Global Network Inventory host file

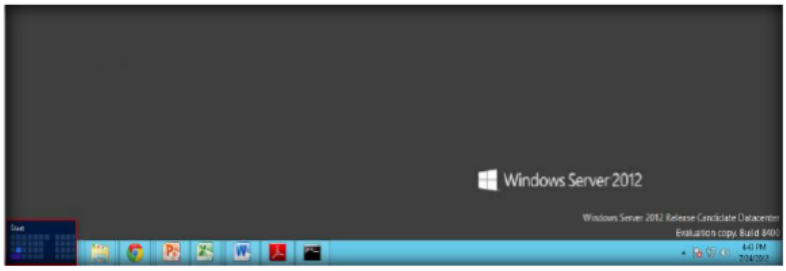


FIGURE 13.4: Windows Server 2012 – Desktop view

12. Click the **Proxy Workbench** app to open the **Proxy Workbench** window.

The events panel displays the total number of events that Proxy Workbench has in memory. By clearing the data (**File->Clear All Data**) this will decrease to zero if there are no connections that are Alive

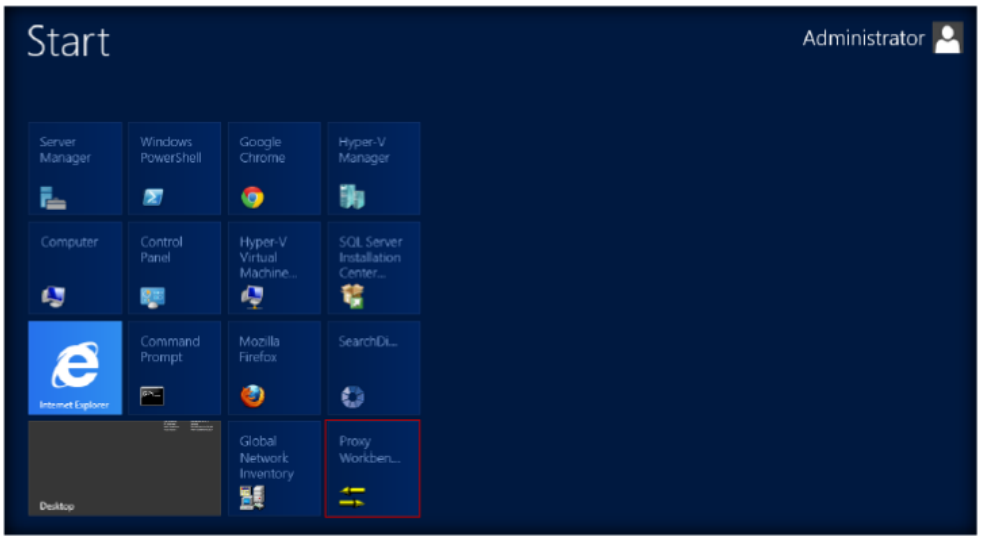


FIGURE 13.5: Windows Server 2012 – Apps

13. The **Proxy Workbench** main window appears as shown in the following figure.

The last panel displays the current time as reported by your operating system

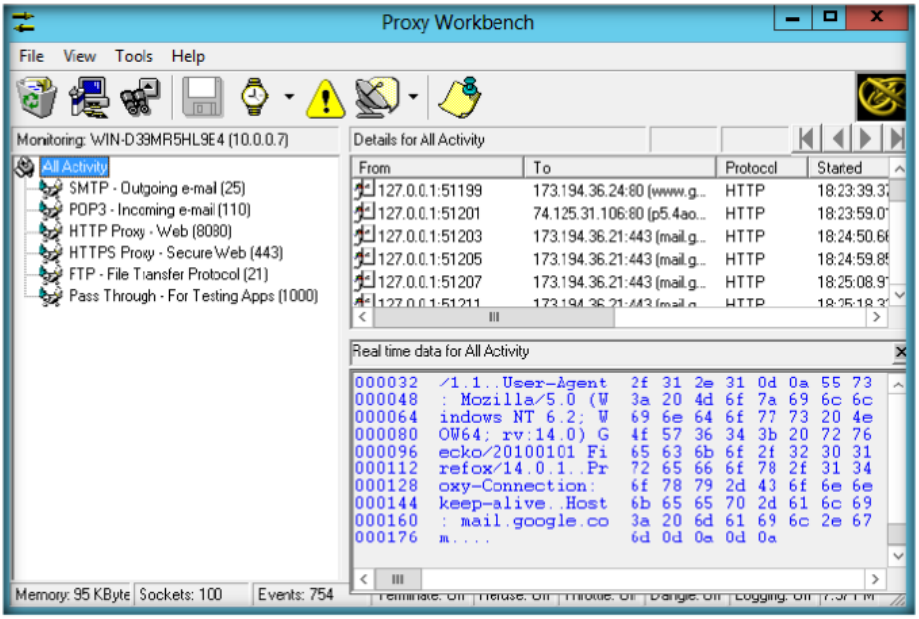


FIGURE 13.6: Proxy Workbench main window

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

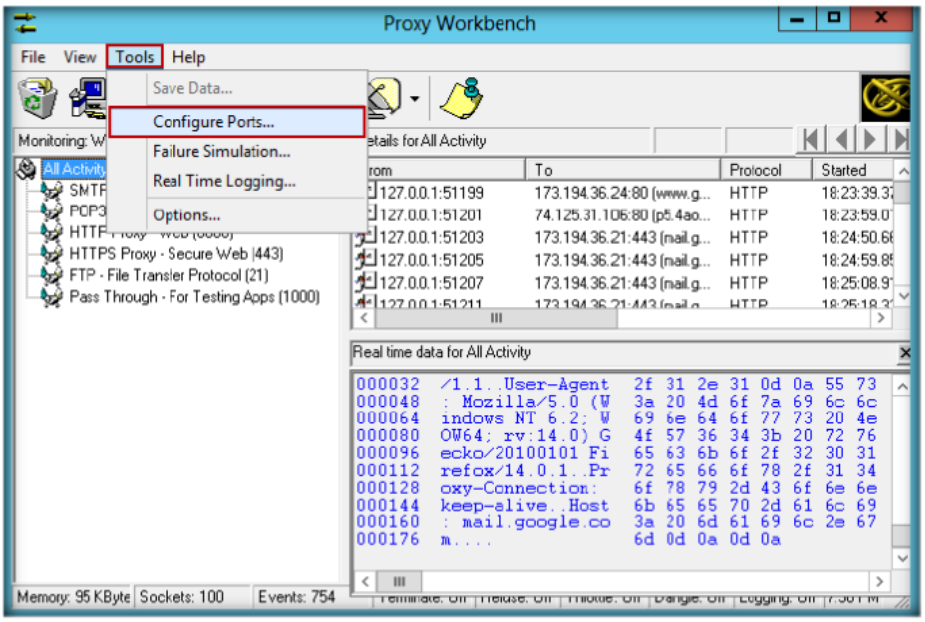


FIGURE 13.7: Proxy Workbench ConFIGURE Ports option

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.

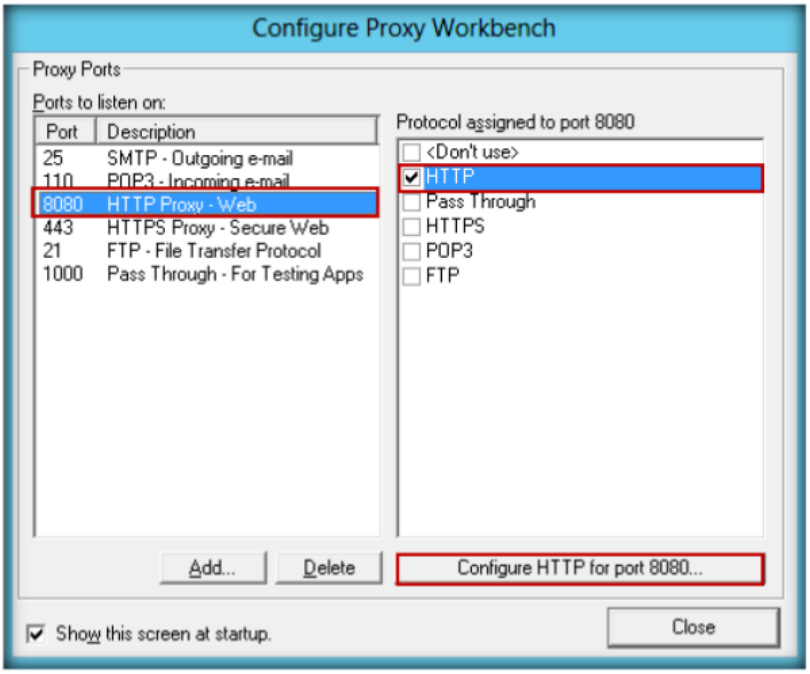


FIGURE 13.8: Proxy Workbench Configuring HTTP for Port 8080

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**

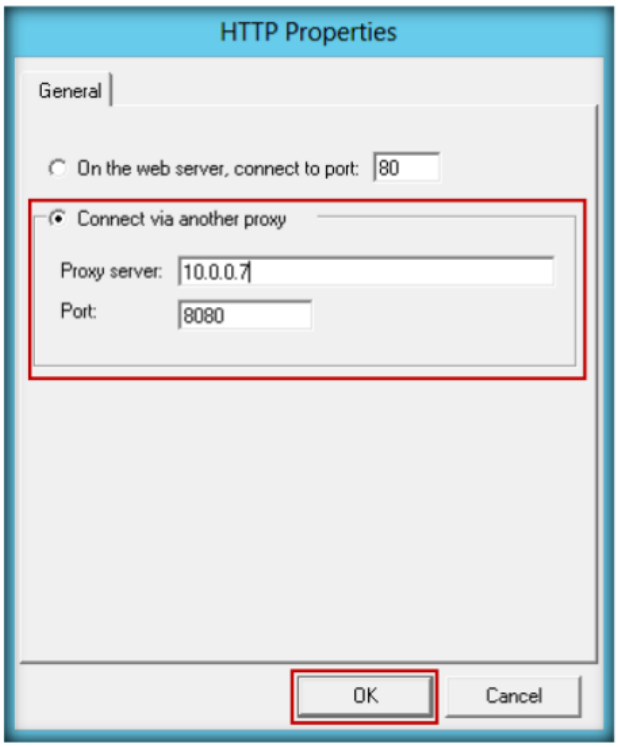


FIGURE 13.9: Proxy Workbench HTTP for Port 8080

Many people understand sockets much better then 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.altaviata.com" with port number 80

18. Click **Close** in the **Configure Proxy Workbench** wizard after completing the **configuration settings**

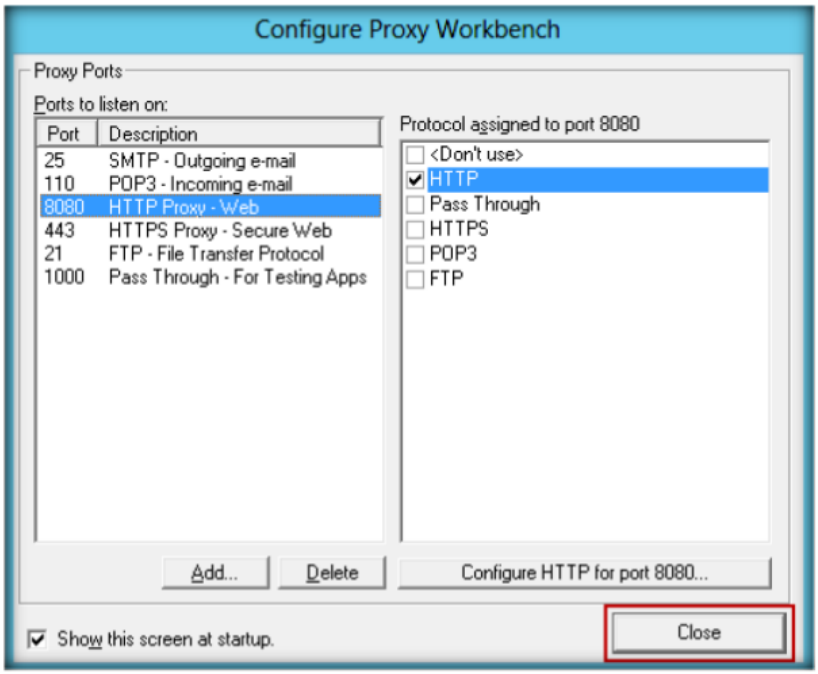


FIGURE 13.10: Proxy Workbench Configured proxy

The real time logging allows you to record everything Proxy Workbench does to a text file. This allows the information to be readily imported in a spreadsheet or database so that the most advanced analysis can be performed on the data

19. Repeat the configuration steps of Proxy Workbench from **Step 11 to Step 15** in Windows Server 2008 Virtual Machines.

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).

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

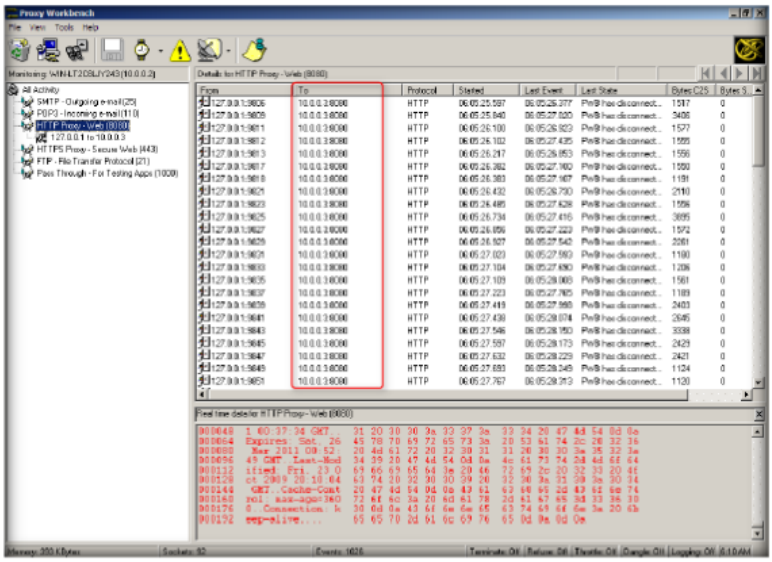


FIGURE 13.11: Proxy Workbench Generated Traffic in Windows Server 2012 Host Machine

24. Now log in 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).

And now, Proxy Workbench includes connection failure simulation strategies. What this means is that you can simulate a poor network, a slow Internet or unresponsive server. This is makes it the definitive TCP application tester

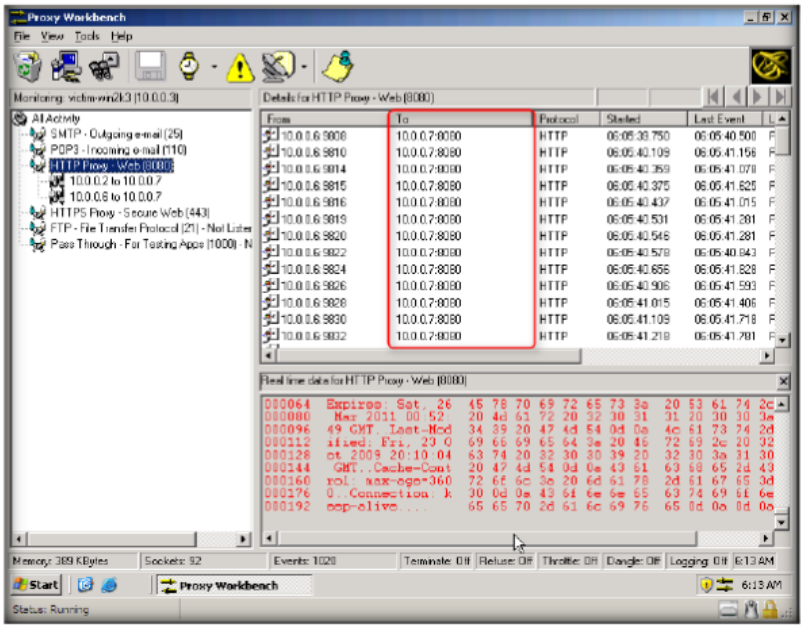


FIGURE 13.12: Proxy Workbench Generated Traffic in Windows Server 2003 Virtual Machine

25. Select On the web server, connect to **port 80** in **Windows 7** virtual machine, and click **OK**

FIGURE 13.13: Configuring HTTP properties in Windows 7

🗀 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

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**.

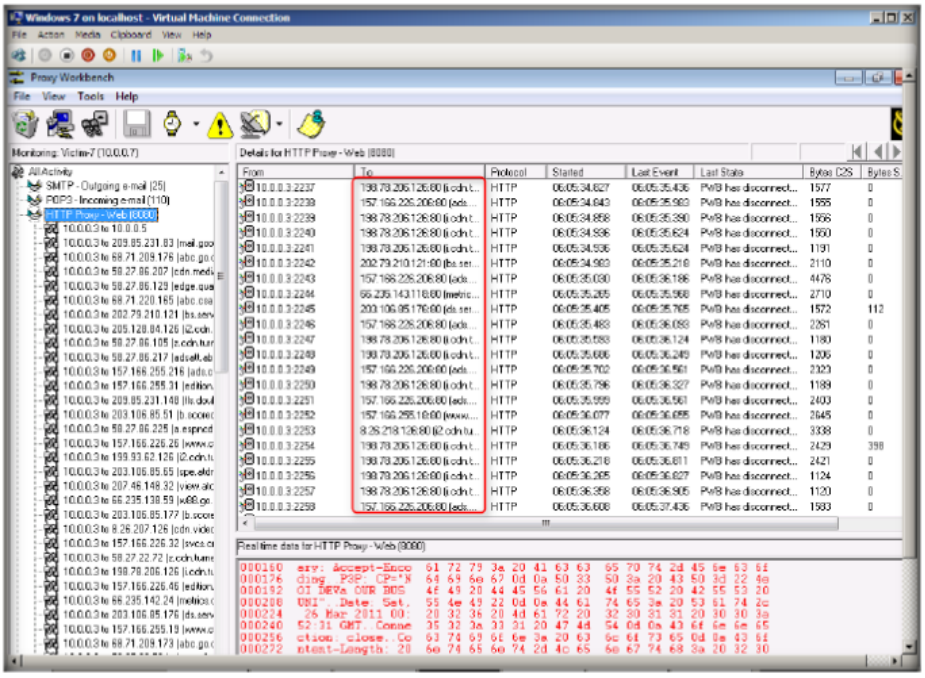


FIGURE 13.14: Proxy Workbench Generated Traffic in Windows 7 Virtual Machine

🕮 **In the Connection Tree, if a protocol or a client/server pair is selected, the Details Pane displays the summary information of all of the socket connections that are in progress for the selected item on the Connection Tree.**

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	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Lab 14

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.

- 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

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

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**.

Lab Tasks

TASK 1

Stopping IIS Services

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.

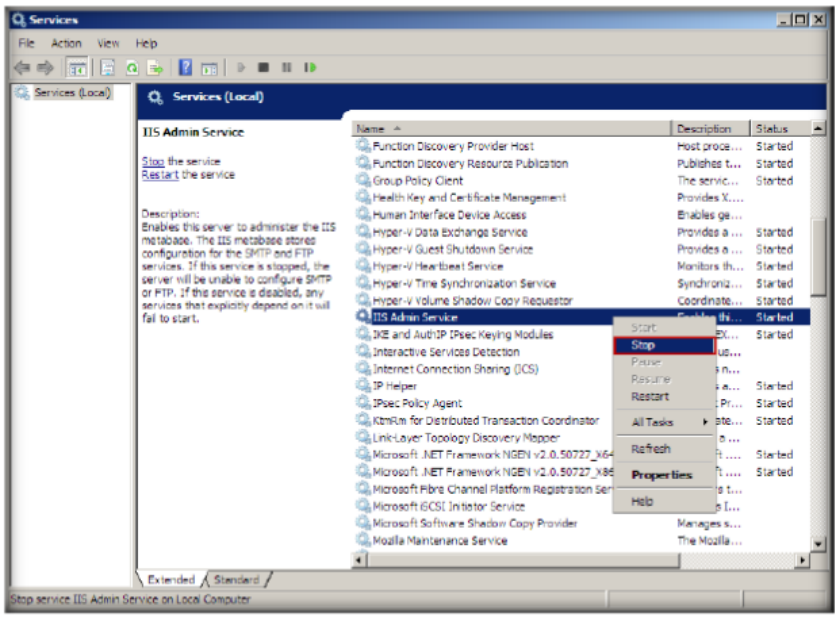


FIGURE 14.1: Stopping IIS Admin Service in Windows Server 2008

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.

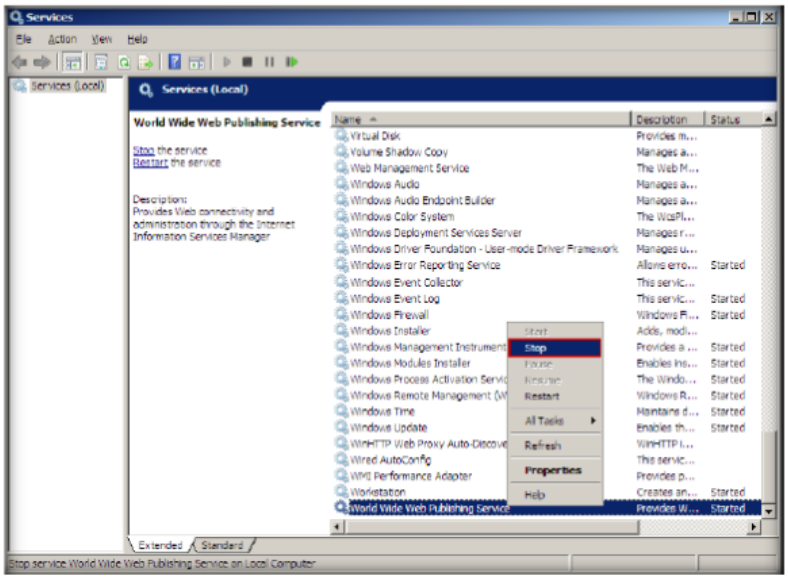


FIGURE 14.2: Stopping World Wide Web Services in Windows Server 2008

🕮 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**.

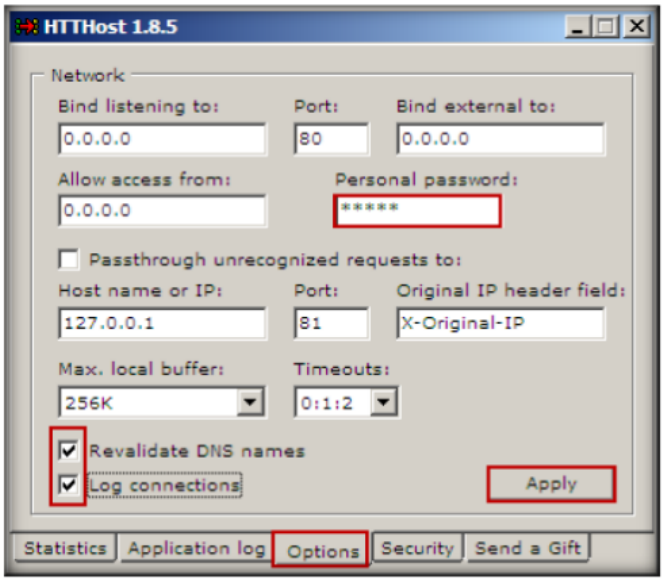


FIGURE 14.3: HTTHost Options tab

To set up HTTPort need to point your browser to 127.0.0.1

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 **httport3snfm.exe**.

HTTPort goes with the predefined mapping "External HTTP proxy" of local port

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

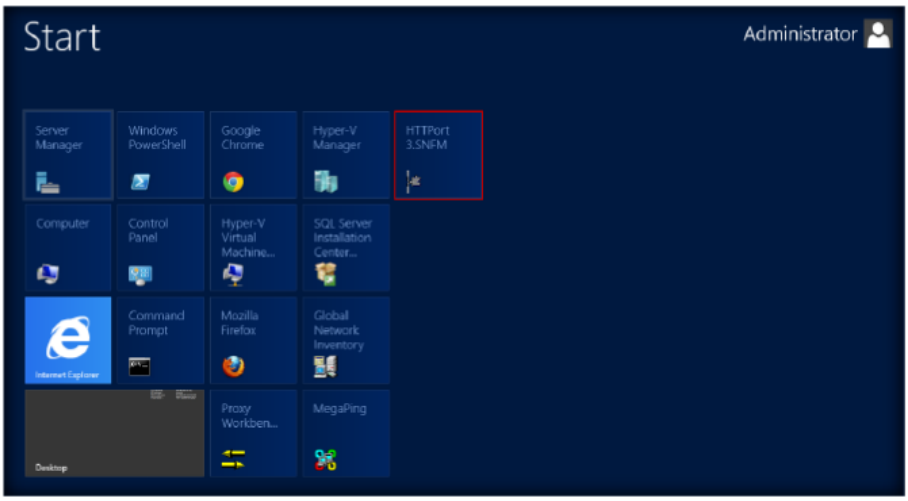


FIGURE 14.5: Windows Server 2012 – Apps

14. The **HTTPort 3.SNFM** window appears as shown in the figure that follows.

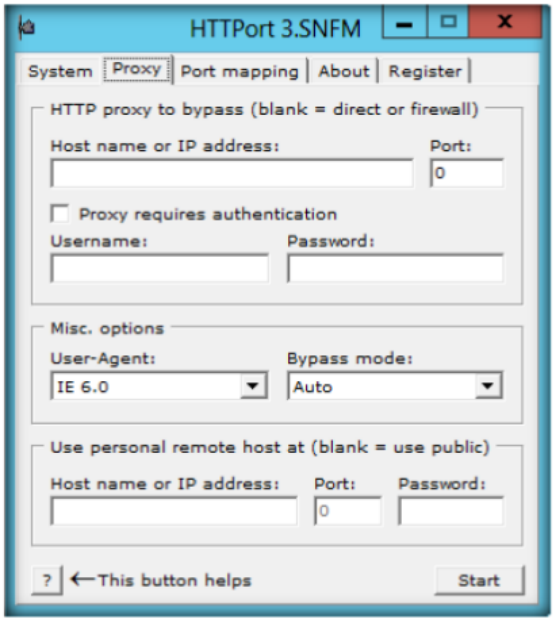


FIGURE 14.6: HTTPort Main Window

For each software to create custom, given all the addresses from which it operates. For applications that are dynamically changing the ports there Socks4-proxy mode, in which the software will create a local server Socks (127.0.0.1)

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.

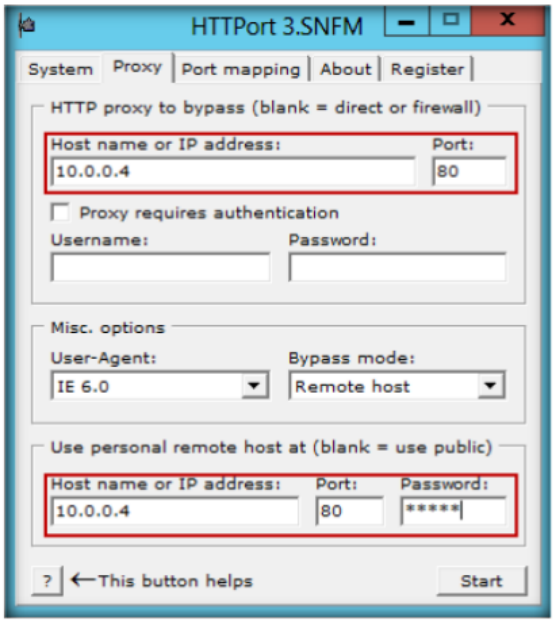


FIGURE 14.7: HTTPort Proxy settings window

20. Select the **Port Mapping** tab and click **Add** to create **New Mapping**

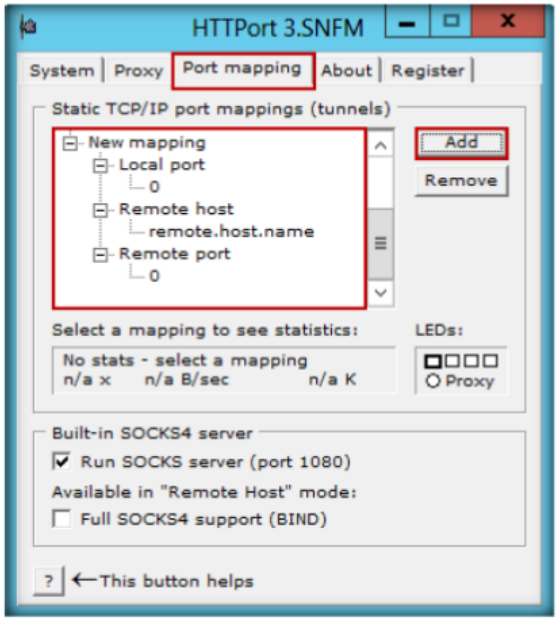


FIGURE 14.8: HTTPort creating a New Mapping

21. Select **New Mapping Node**, and right-click **New Mapping**, and click **Edit**

📖 HTTHost supports the registration, but it is free and password-free - you will be issued a unique ID, which you can contact the support team and ask your questions.

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

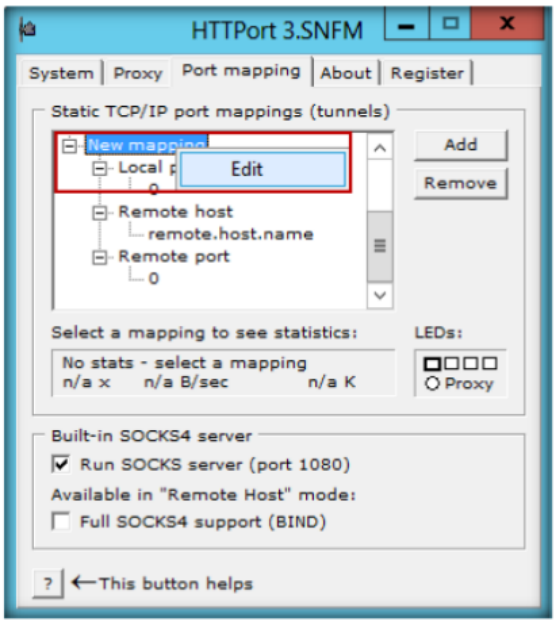


FIGURE 14.9: HTTPort Editing to assign a mapping

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**

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.

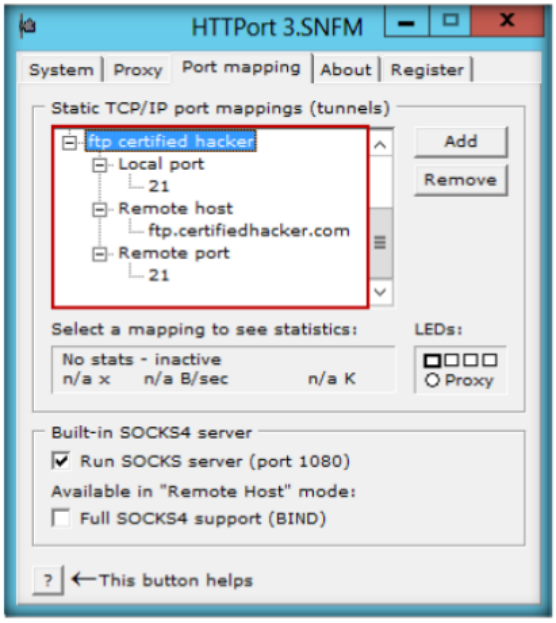


FIGURE 14.10: HTTPort Static TCP/IP port mapping

25. Click **Start** on the **Proxy** tab of HTTPort to run the HTTP tunneling.

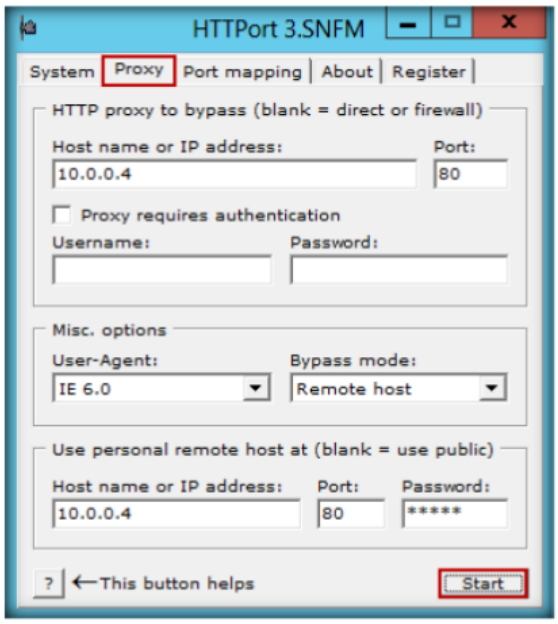
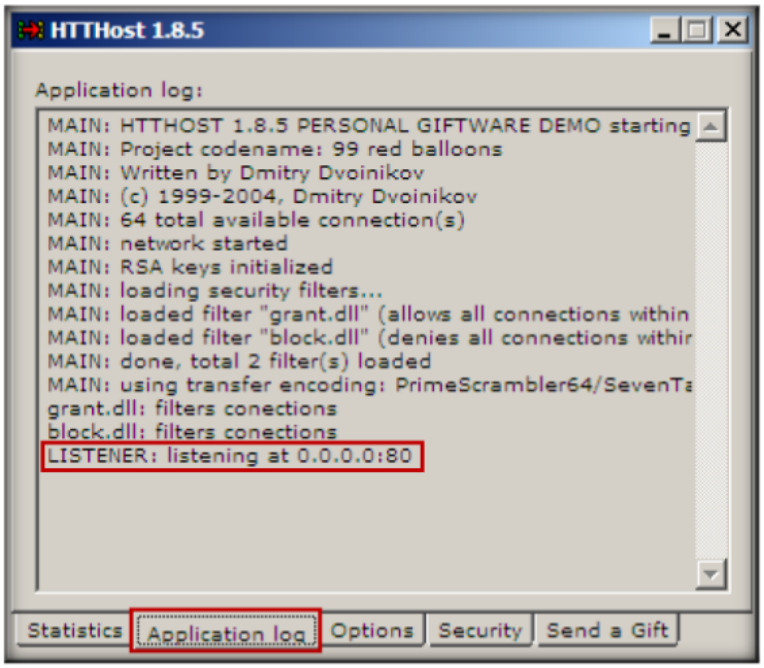


FIGURE 14.11: HTTPort to start tunneling

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.



To make a data tunnel through the password protected proxy, so we can map external website to local port, and federate the search result.

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.

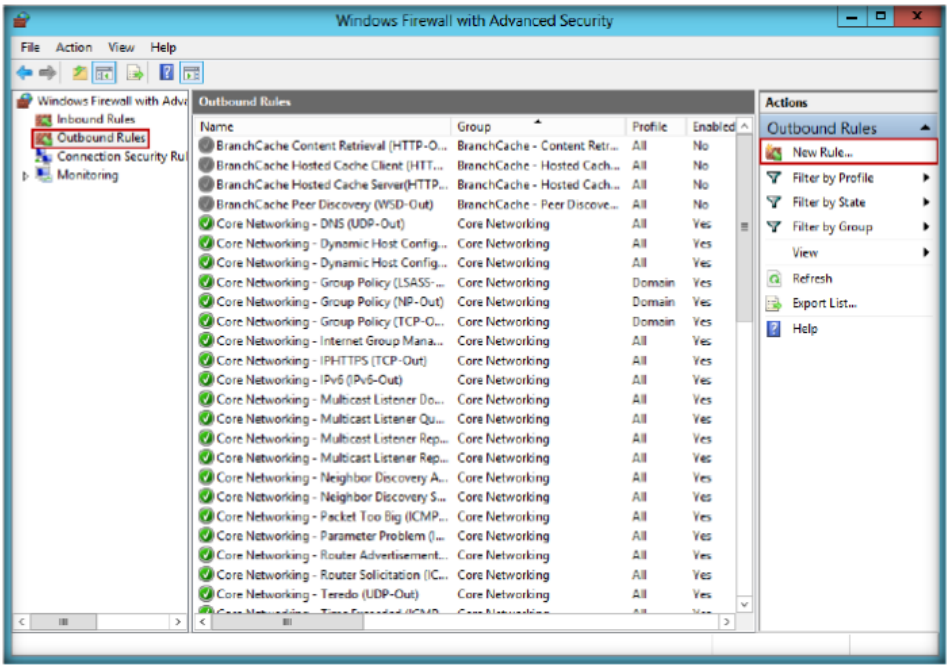


FIGURE 14.13: Windows Firewall with Advanced Security window in Windows Server 2008

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

31. In the **New Outbound Rule Wizard**, select the **Port** option in the **Rule Type** section and click **Next**

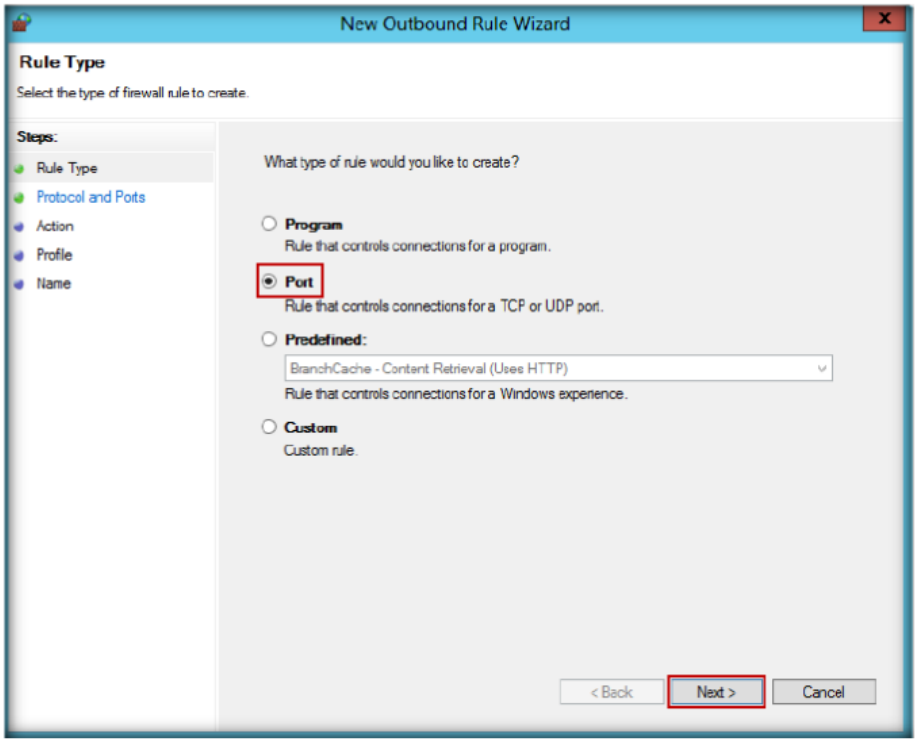


FIGURE 14.14: Windows Firewall selecting a Rule Type

Tools demonstrated in this lab are available in Z:\ Mapped Network Drive in Virtual Machines

32. Now select **All remote ports** in the **Protocol and Ports** section, and click **Next**

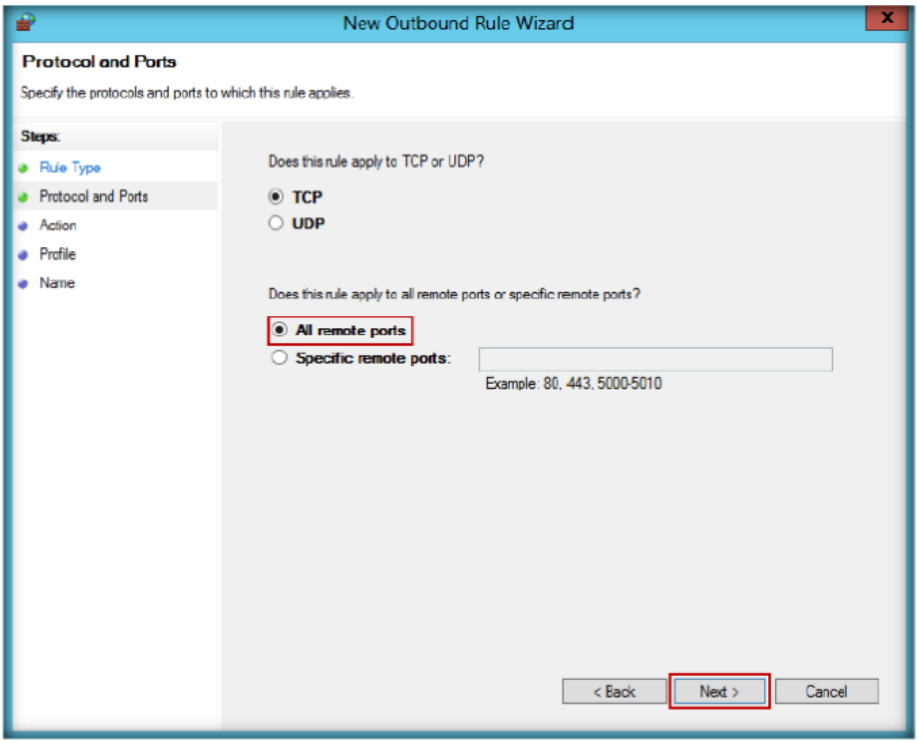
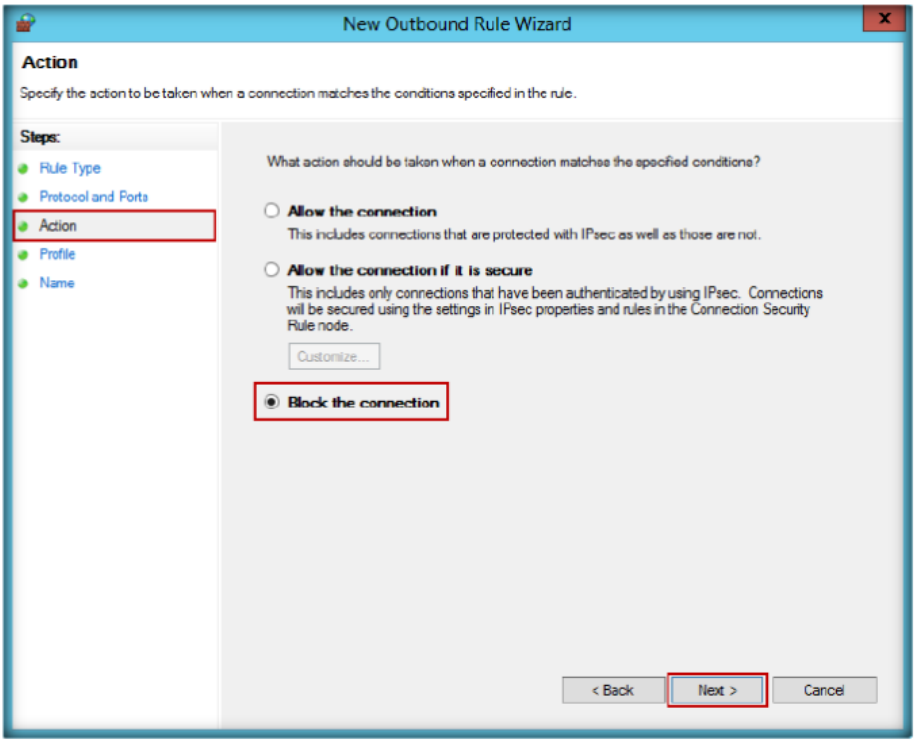


FIGURE 14.15: Windows Firewall assigning Protocols and Ports

HTTPort doesn't really care for the proxy as such, it works perfectly with firewalls, transparent accelerators, NATs and basically anything that lets HTTP protocol through.

33. In the **Action** section, select the **Block the connection**" option and click **Next**



You need to install htthost on a PC, who is generally accessible on the Internet - typically your "home" PC. This means that if you started a webserver on the home PC, everyone else must be able to connect to it. There are two showstoppers for htthost on home PCs

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.

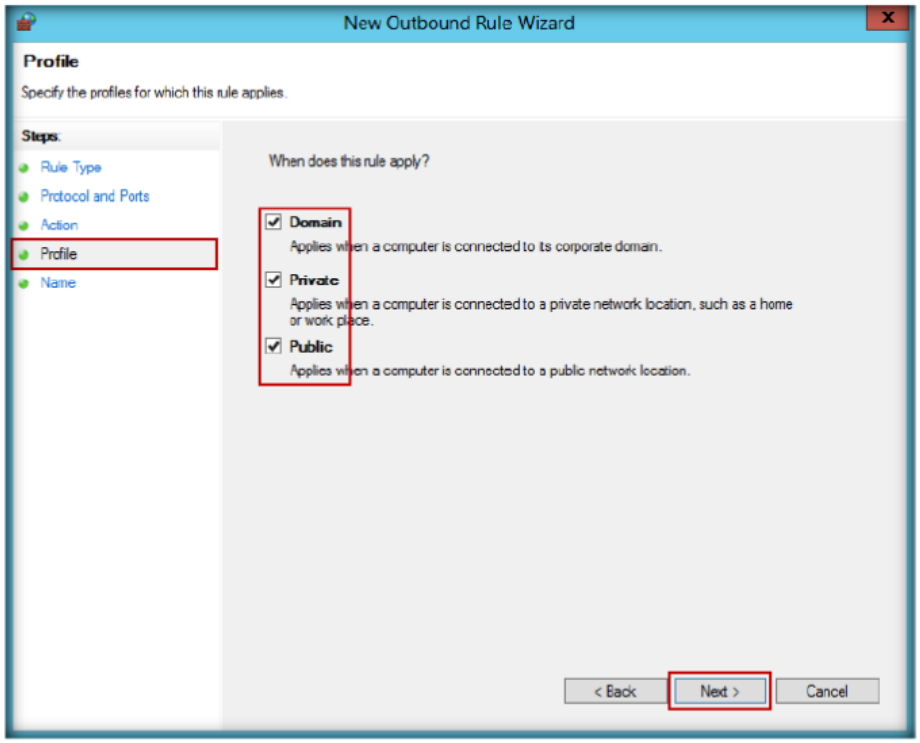
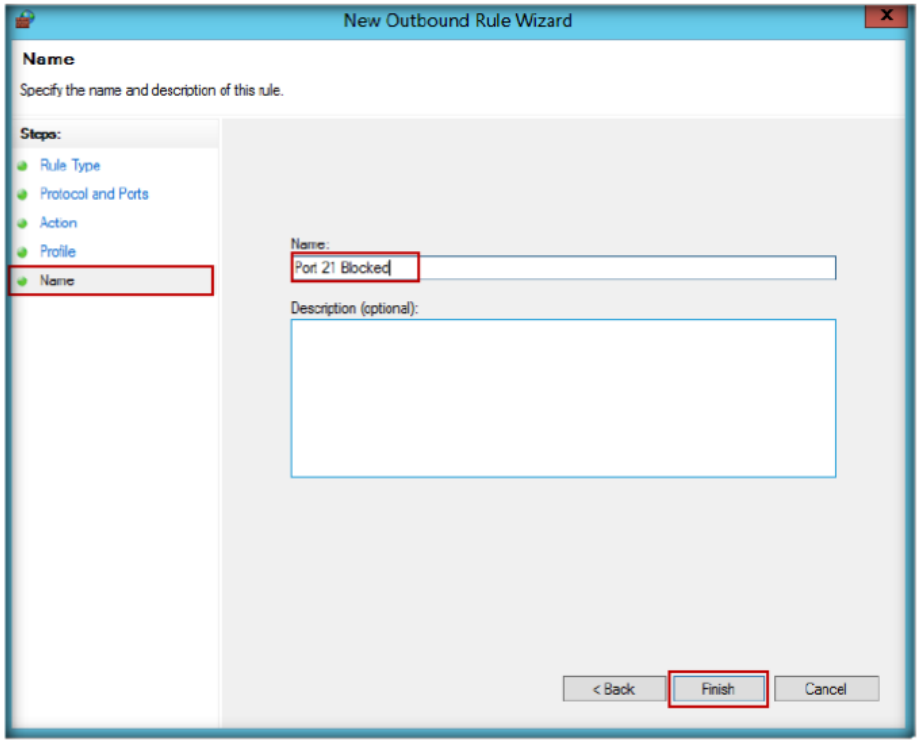


FIGURE 14.17: Windows Firewall Profile settings

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

35. Type **Port 21 Blocked** in the **Name** field, and click **Finish**



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 connection issues.

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.

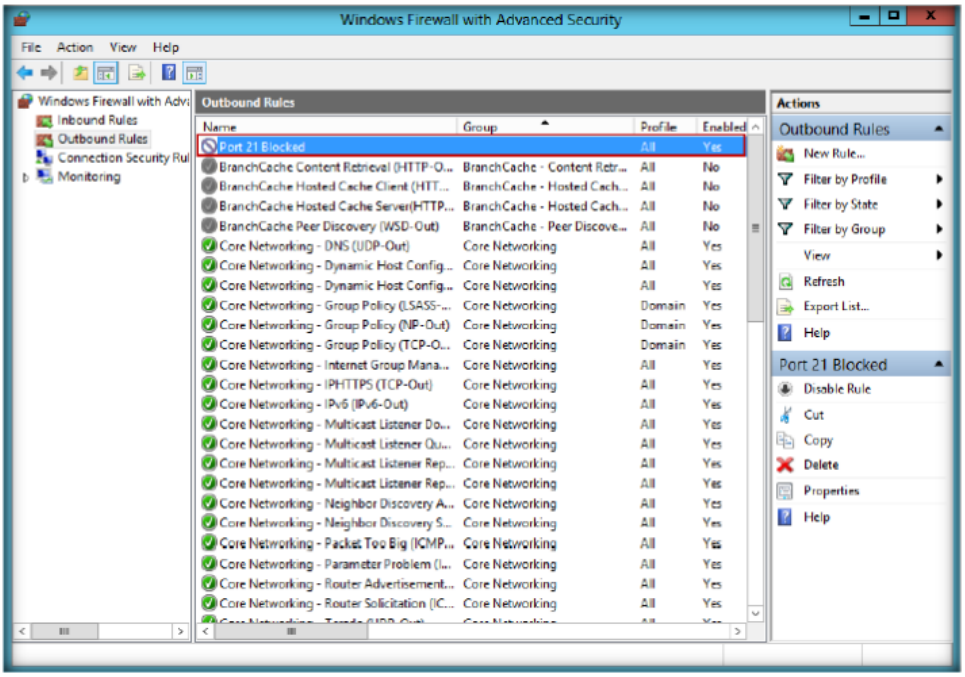


FIGURE 14.19: Windows Firewall New rule

37. Right-click the newly created rule and select **Properties**

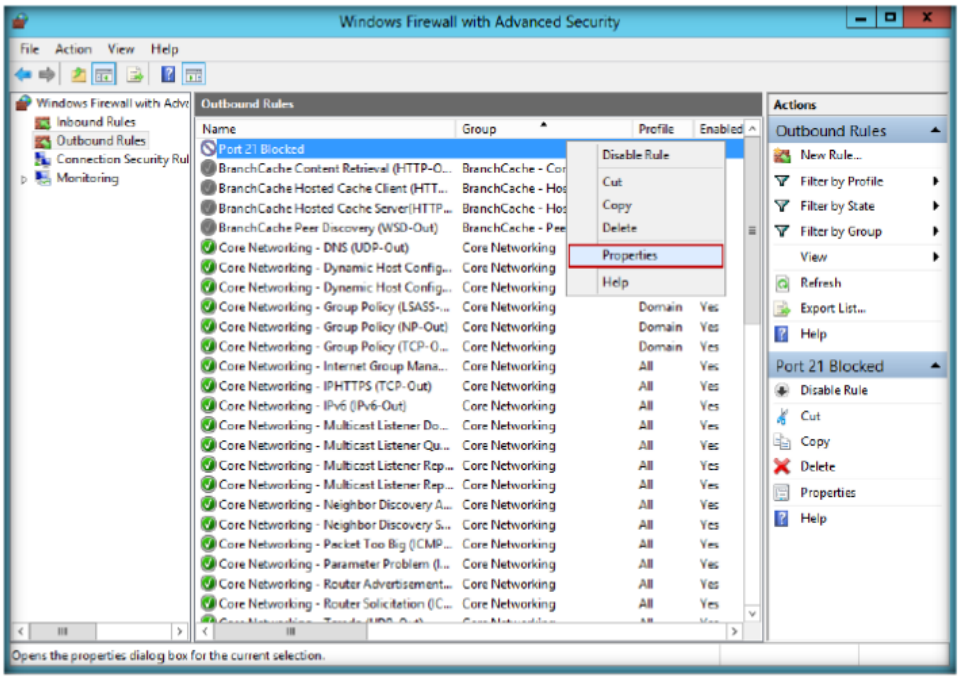


FIGURE 14.20: Windows Firewall new rule properties

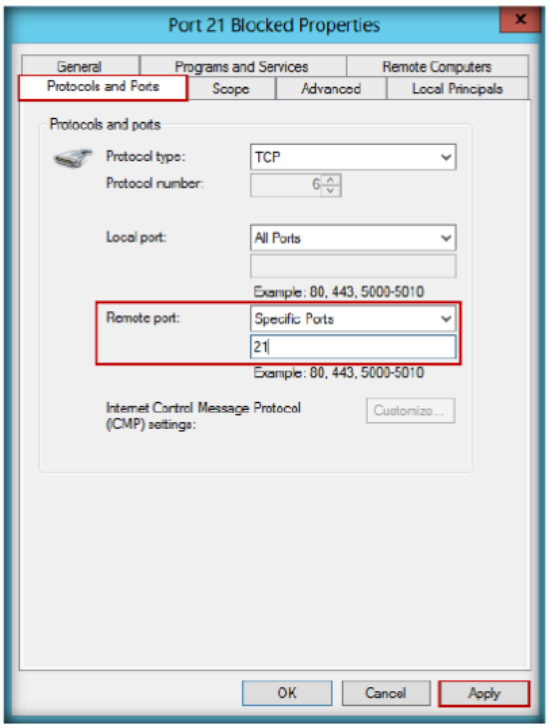
38. Select the **Protocols and Ports** tab. Change the **Remote Port** option to **Specific Ports** and enter the **Port number** as **21**

39. Leave the other settings as their defaults and click **Apply** then click **OK**.

HTTPort doesn't really care for the proxy as such: it works perfectly with firewalls, transparent accelerators, NATs and basically anything that lets the HTTP protocol through.

HTTPort then intercepts that connection and runs it through a tunnel through the proxy.

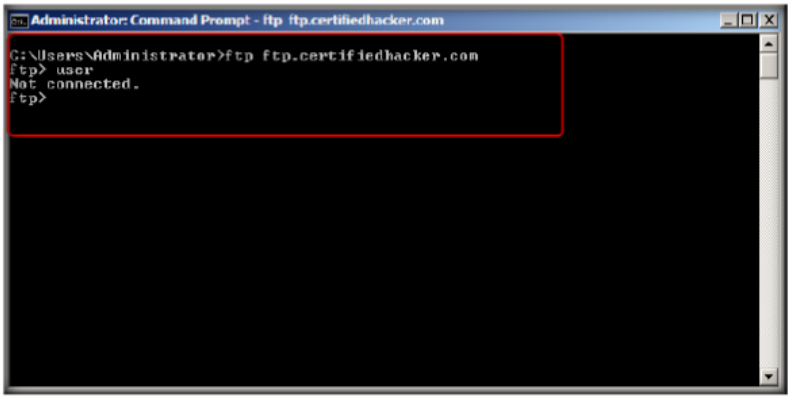
Enables you to bypass your HTTP proxy in case it blocks you from the Internet



With HTTPort, you can use various Internet software from behind the proxy, e.g., e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC etc. The basic idea is that you set up your Internet software

FIGURE 14.21: Firewall Port 21 Blocked Properties

40. Type **ftp ftp.certifiedhacker.com** in the command prompt and press **Enter**. The connection is blocked in **Windows Server 2008 by firewall**



HTTPort does neither freeze nor hang. What you are experiencing is known as "blocking operations"

FIGURE 14.22: ftp connection is blocked

41. 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".

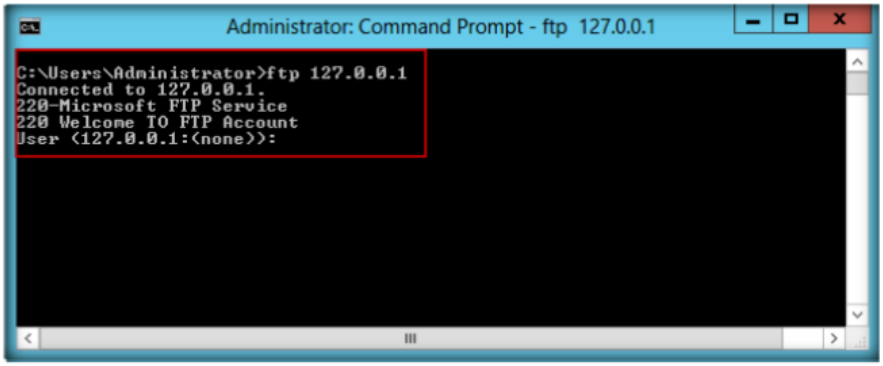


FIGURE 14.23: Executing ftp command

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
HTTPort	**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

1. How do you set up an HTTPort to use an email client (Outlook, Messenger, etc.)?
2. Examine if software does not allow editing the address to connect to.

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ 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

- 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**

PING stands for Packet Internet Groper.

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

TASK 1

IP Scanning

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

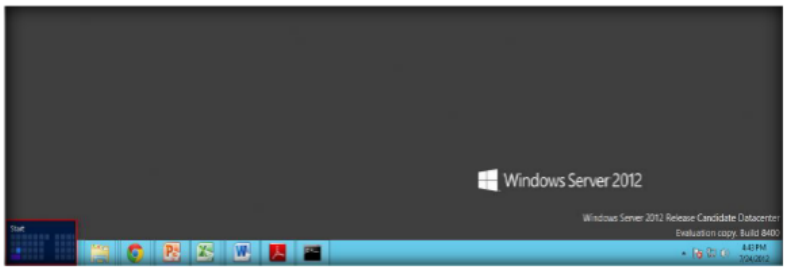


FIGURE 15.1: Windows Server 2012 – Desktop view

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

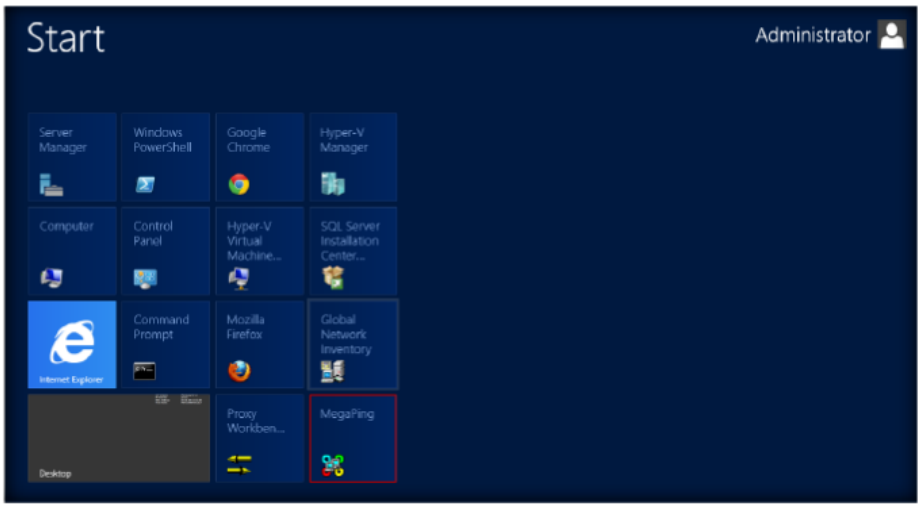


FIGURE 15.2: Windows Server 2012 – Apps

3. The **MegaPing** main window, as shown in the following figure.

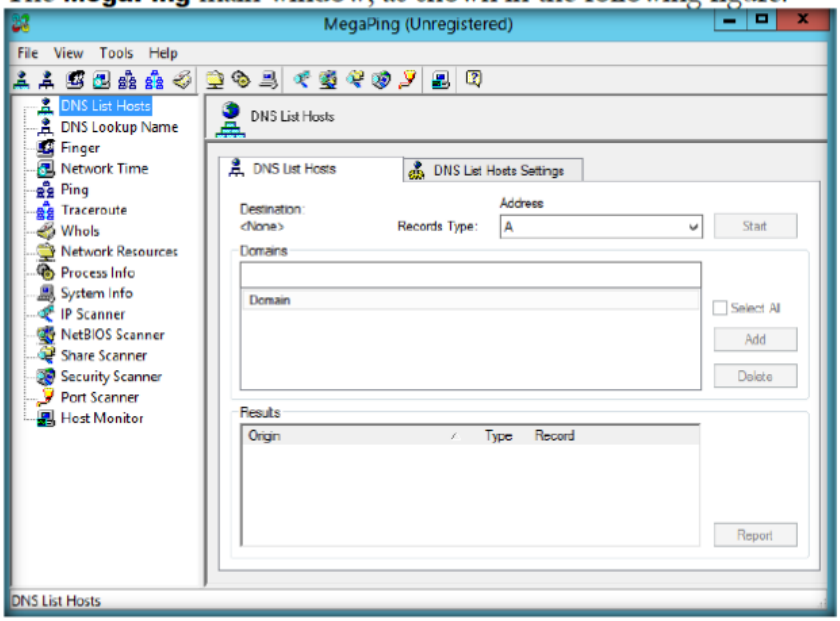


Figure15.3: MegaPing main windows

4. Select any one of the **options** from the left pane of the window.
5. 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**
6. 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

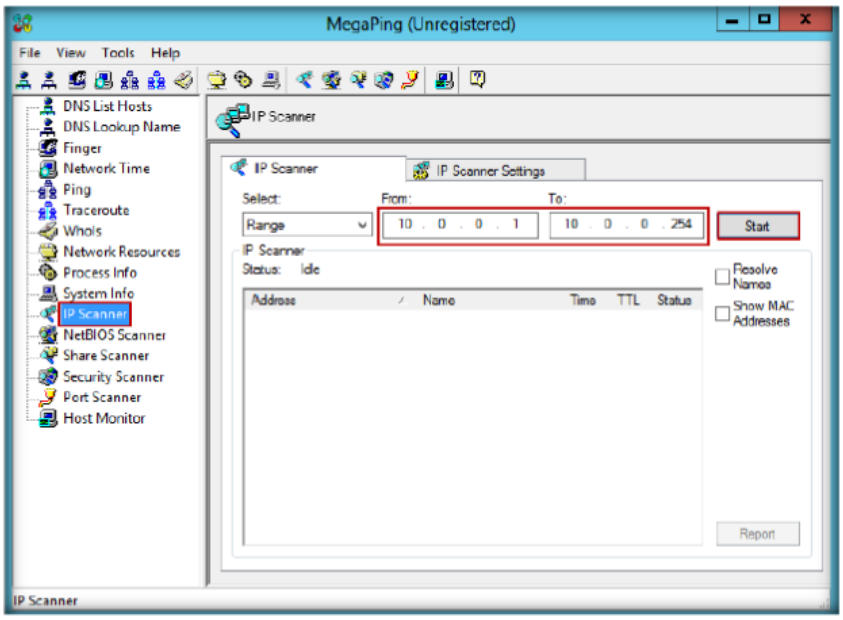


FIGURE 15.4: MegaPing IP Scanning

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.

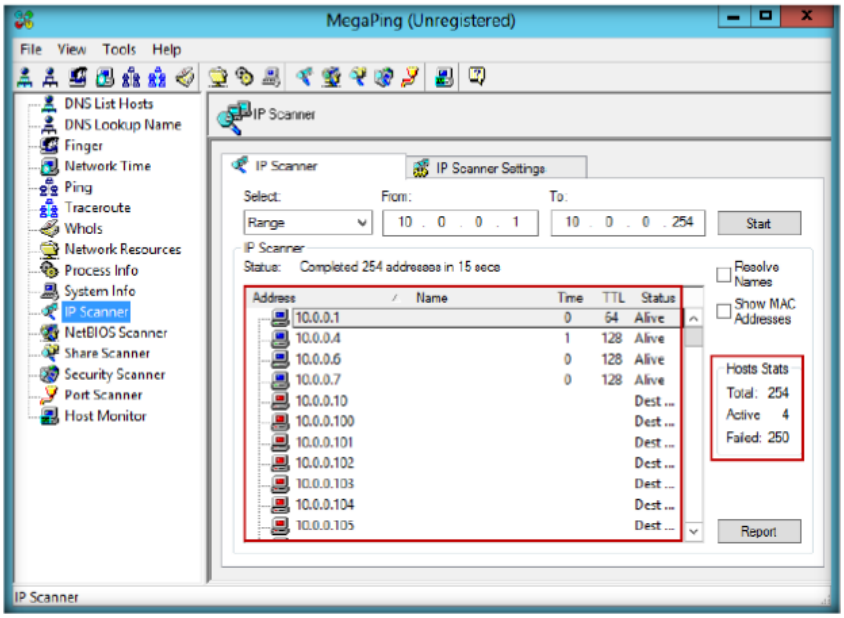


FIGURE 15.5: MegaPing IP Scanning Report

🗀 **Network utilities:** DNS list host, DNS lookup name, Network Time Synchronizer, Ping, Traceroute, Whois, and Finger.

TASK 2

NetBIOS Scanning

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**

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.

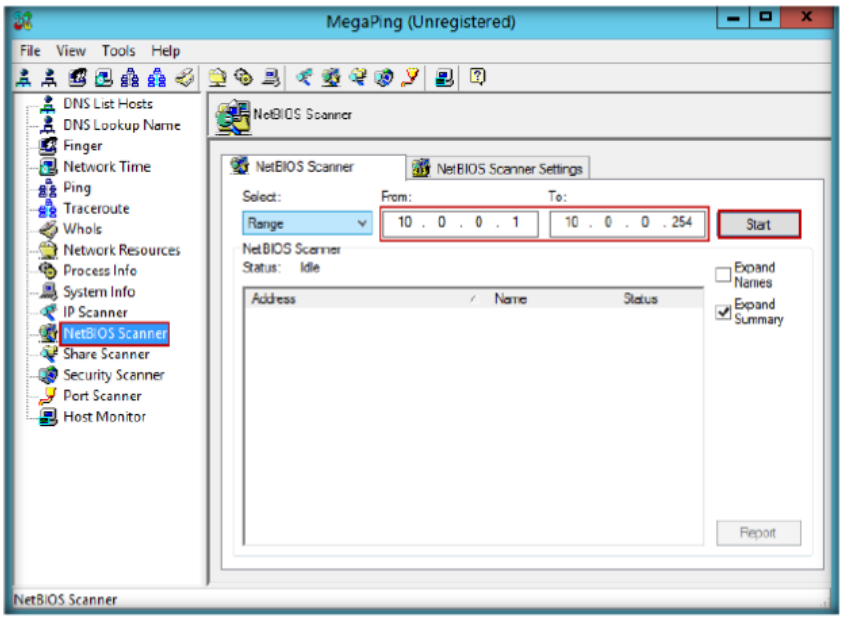


FIGURE 15.6: MegaPing NetBIOS Scanning

9. The **NetBIOS** scan will list all the hosts with their **NetBIOS name**s and **adapter addresses**

Scan results can be saved in HTML or TXT reports, which can be used to secure your network - for example, by shutting down unnecessary ports, closing shares, etc.

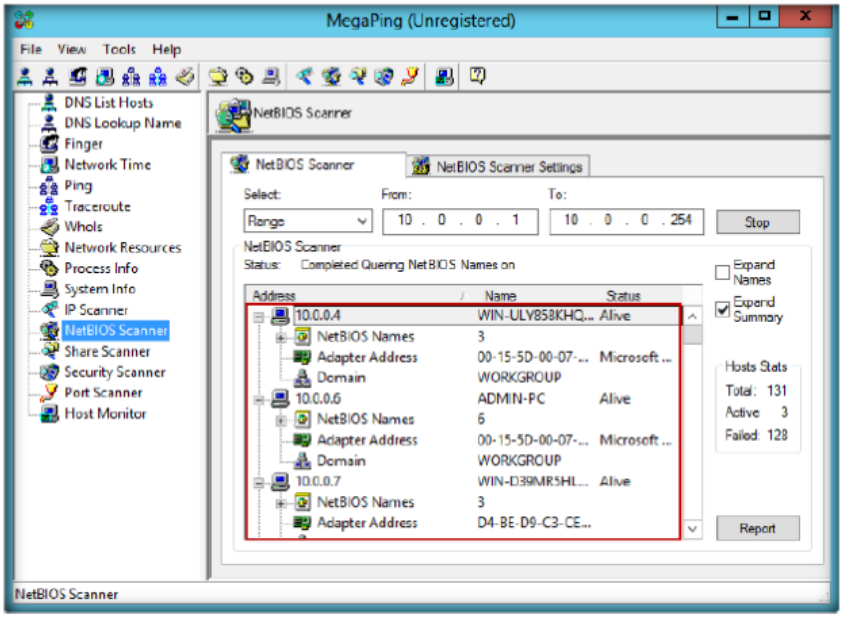


FIGURE 15.7: MegaPing NetBIOS Scanning Report

10. Right-click the IP address. In this lab, the selected IP is 10.0.0.4; it will be different in your network.
11. Then, right-click and select the **Traceroute** option.

TASK 3

Traceroute

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

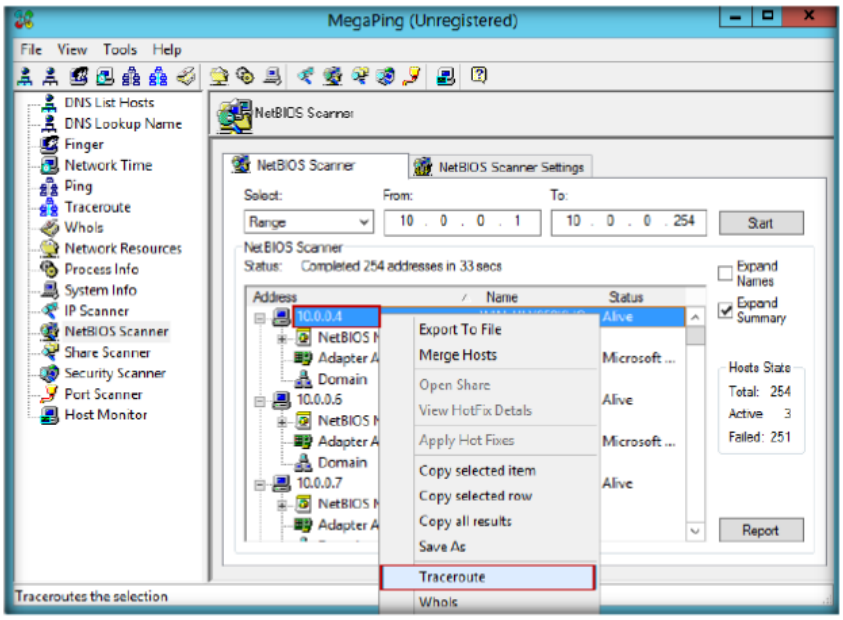


FIGURE 15.8: MegaPing Traceroute

12. It will open the **Traceroute** window, and will trace the IP address selected.

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

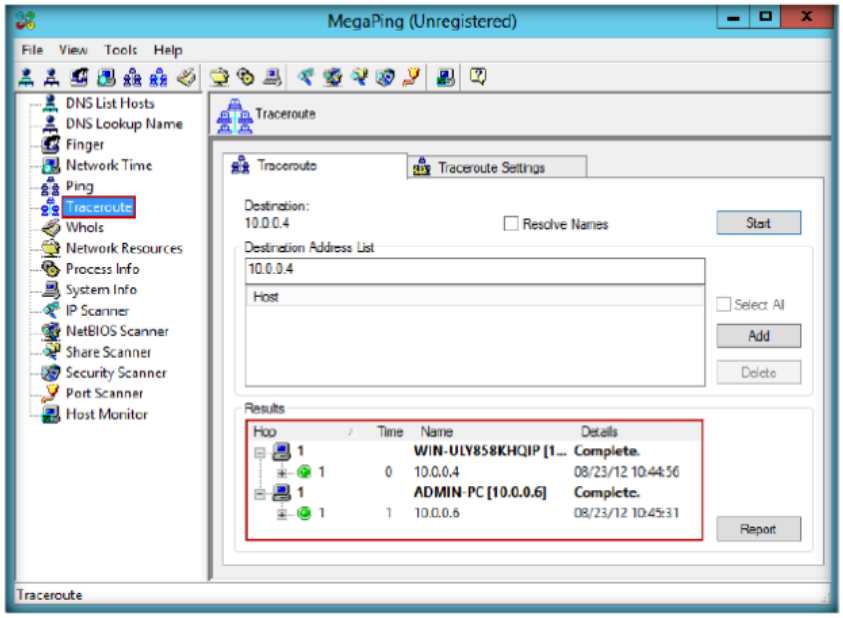


FIGURE 15.9: MegaPing Traceroute Report

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

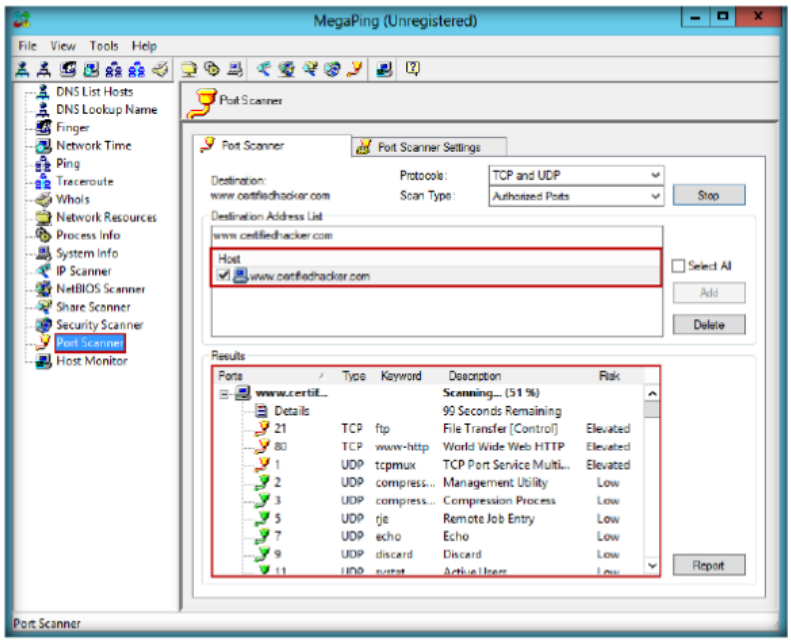


FIGURE 15.10: MegaPing Port Scanning Report

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	**IP Scan Range:** 10.0.0.1 – 10.0.0.254
	Performed Actions: ▪ IP Scanning ▪ NetBIOS Scanning ▪ Traceroute ▪ Port Scanning
	Result: ▪ 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

TASK 1

Detect & Delete Google Cookies

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

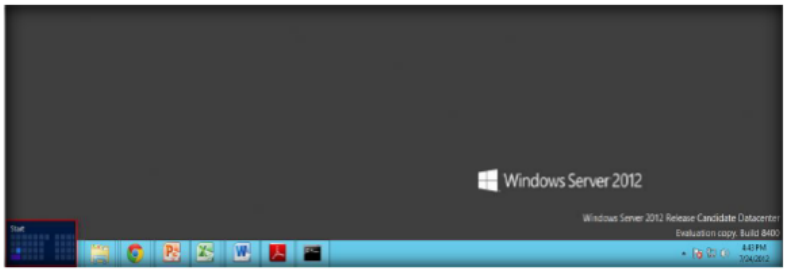


FIGURE 16.1: Windows Server 2012 – Desktop view

2. Click the **G-Zapper** app to open the **G-Zapper** window.

G-Zapper is compatible with Windows 95, 98, ME, NT, 2000, XP, Vista, Windows 7.

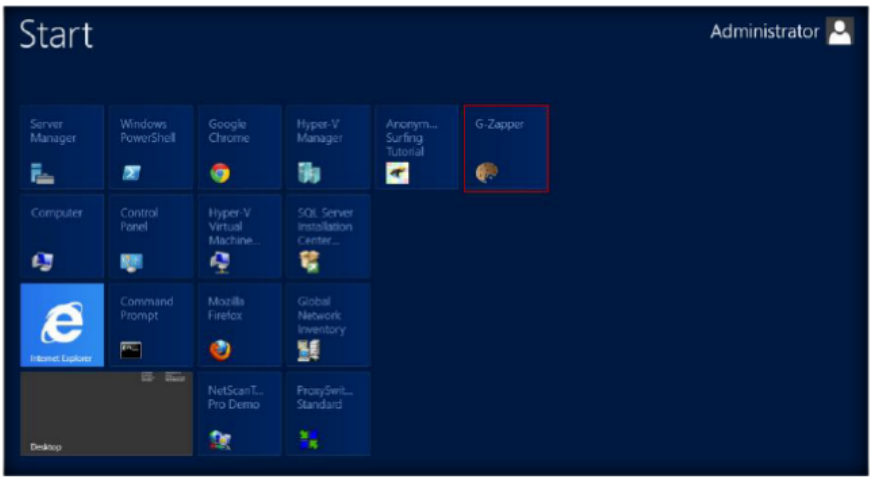


FIGURE 16.2: Windows Server 2012 – Apps

3. The **G-Zapper** main window will appear as shown in the following screenshot.

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

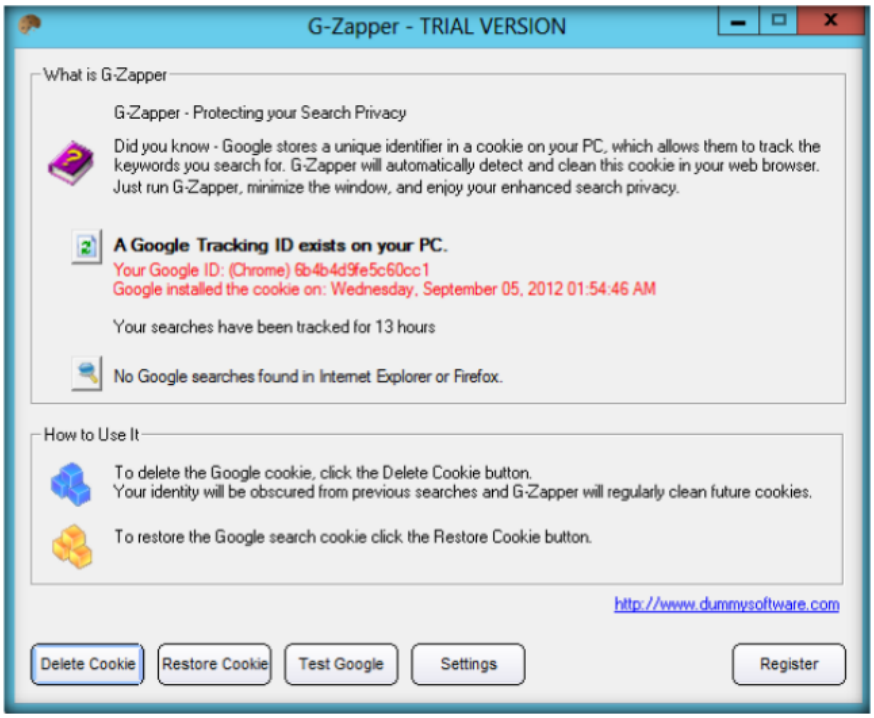


FIGURE 16.3: G-Zapper main windows

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.

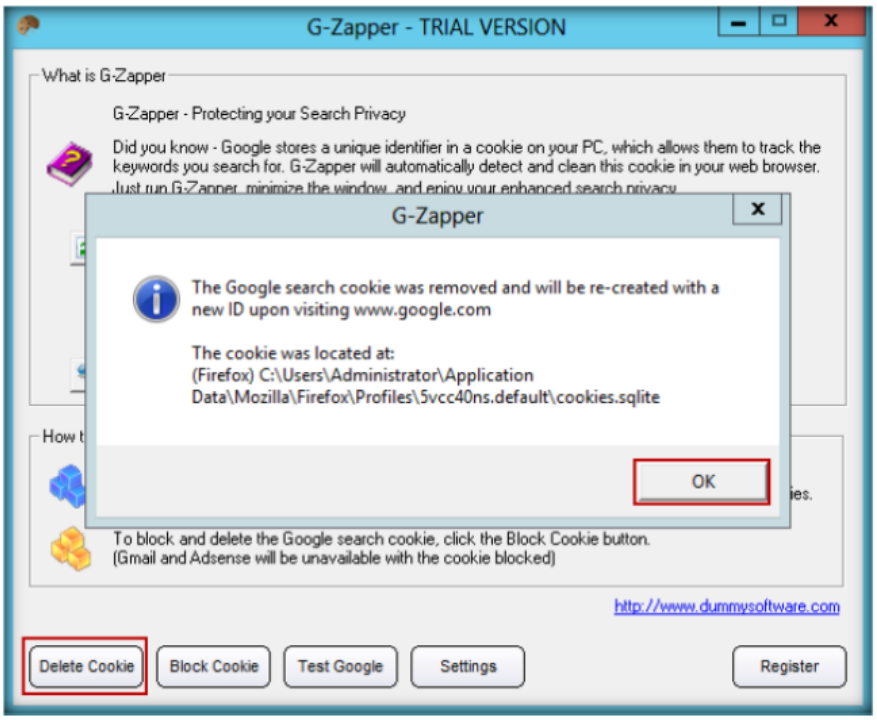


FIGURE 16.4: Deleting search cookies

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.**

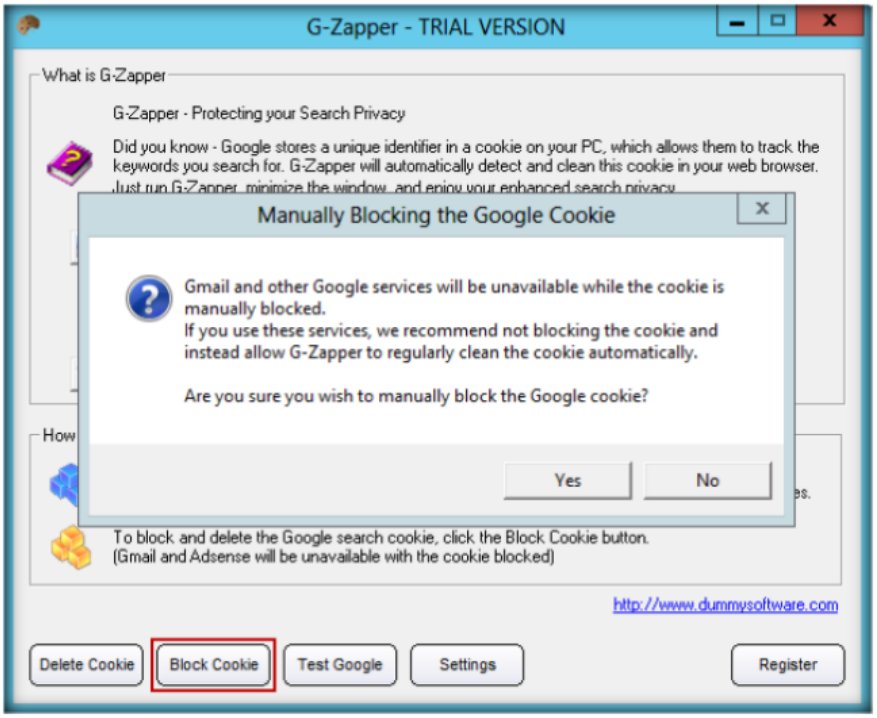


FIGURE 16.5: Block Google cookie

6. It will show a message that the Google cookie has been blocked. To verify, click **OK**

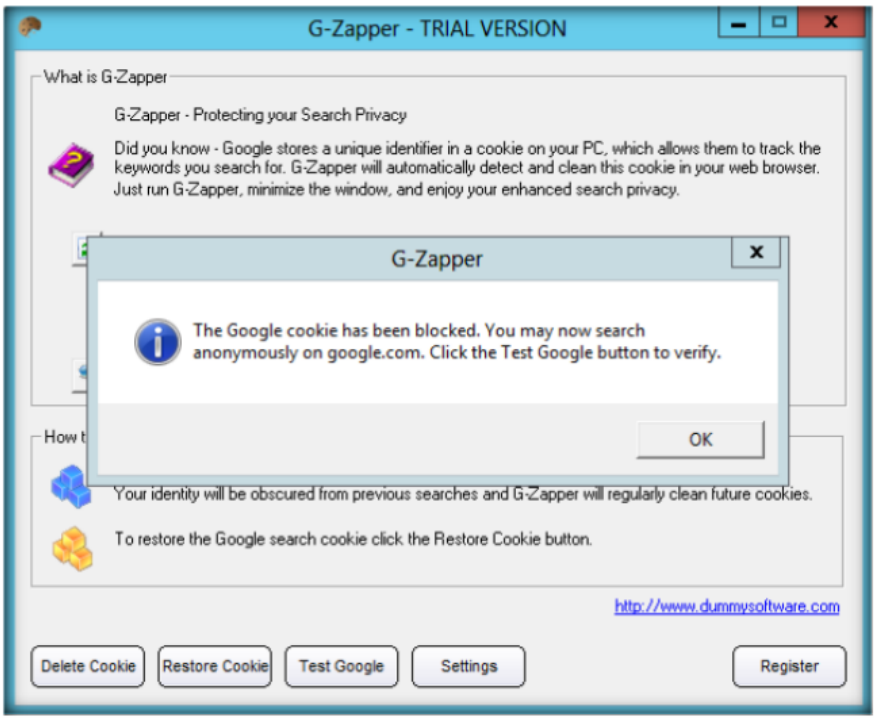


FIGURE 16.6: Block Google cookie (2)

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.

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**.

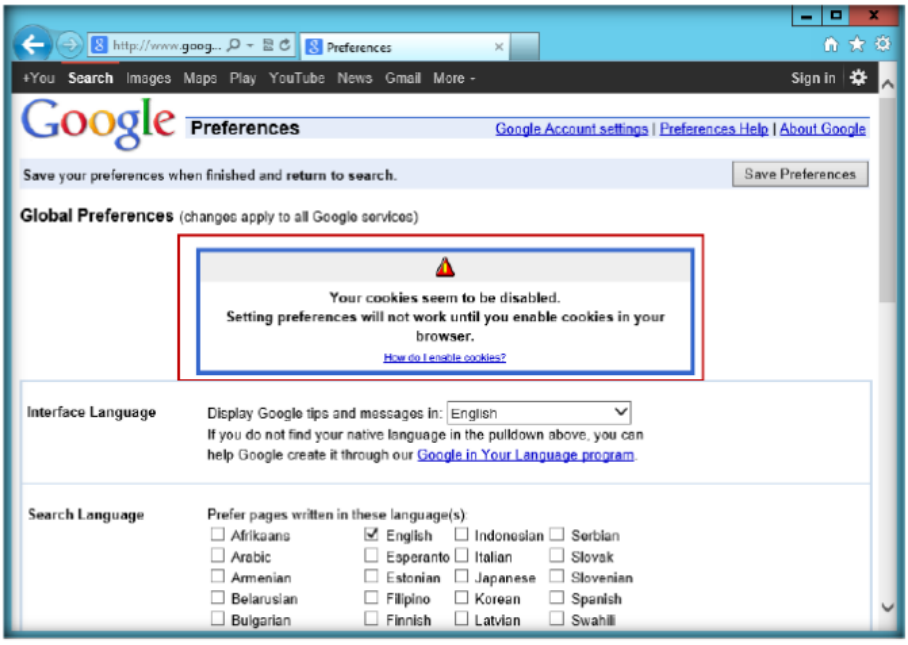


FIGURE 16.7: Cookies disabled massage

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

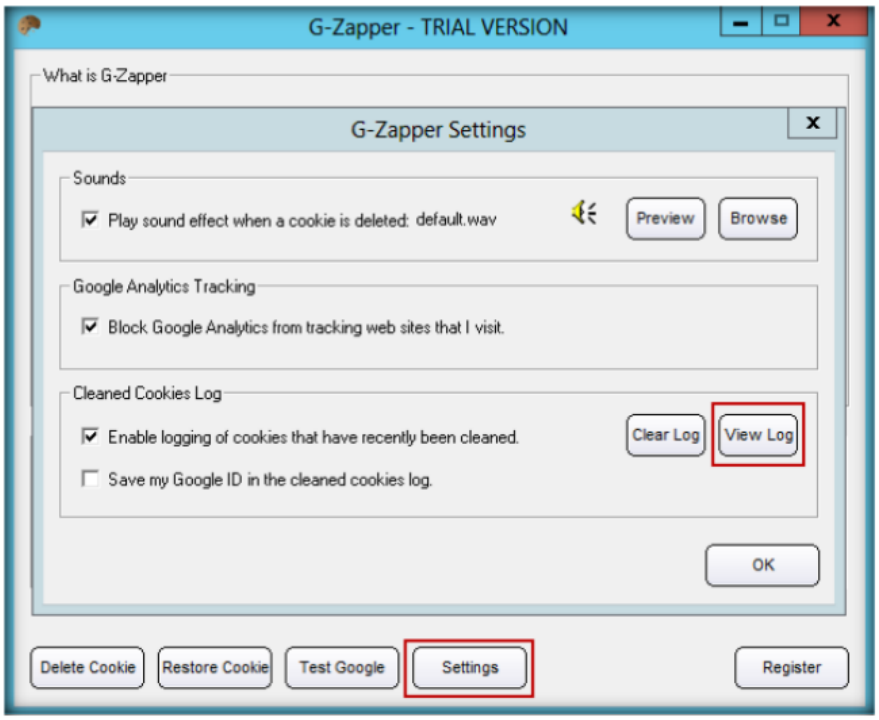


FIGURE 16.8: Viewing the deleted logs

10. The deleted cookies information opens in Notepad.

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

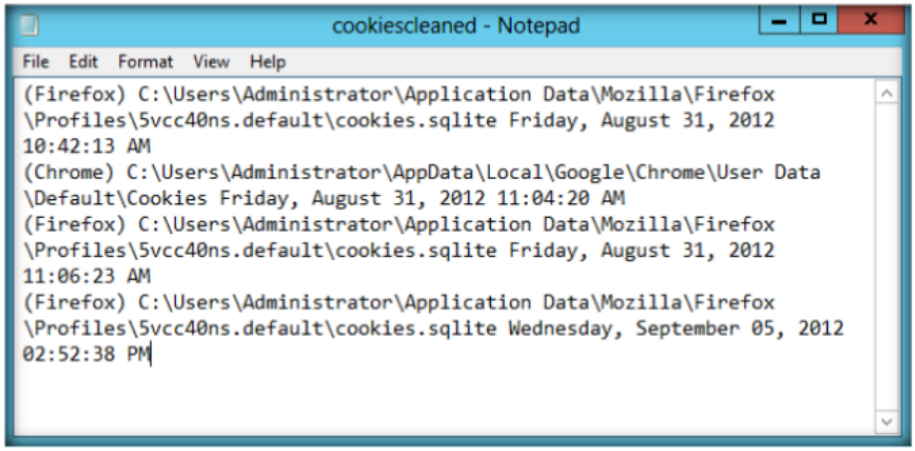


FIGURE 16.9: Deleted logs Report

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	**Action Performed:** ▪ Detect the cookies ▪ Delete the cookies ▪ Block the cookies
	Result: Deleted cookies are stored in C:\Users\Administrator\Application Data

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	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ 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 be learn about sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning.

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 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.

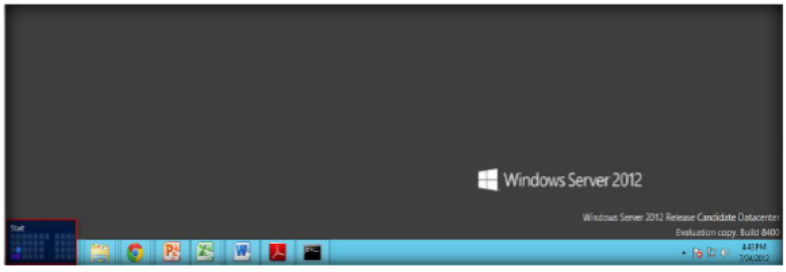


FIGURE 17.1: Windows Server 2012 – Desktop view

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.

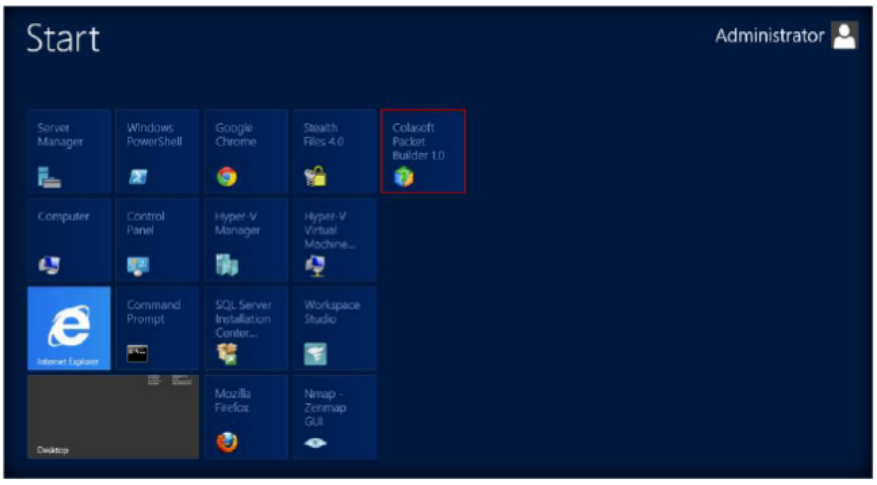


FIGURE 17.2: Windows Server 2012 – Apps

4. The Colasoft Packet Builder main window appears.

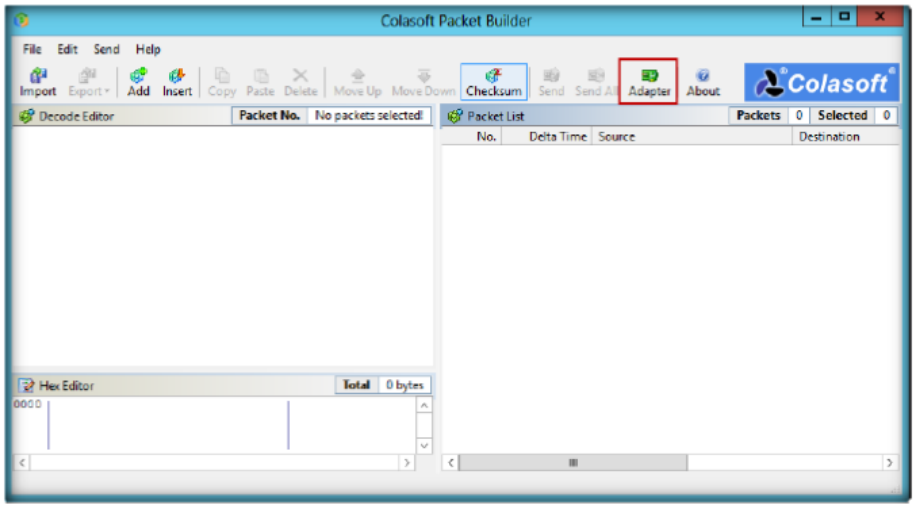


FIGURE 17.3: Colasoft Packet Builder main screen

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**.

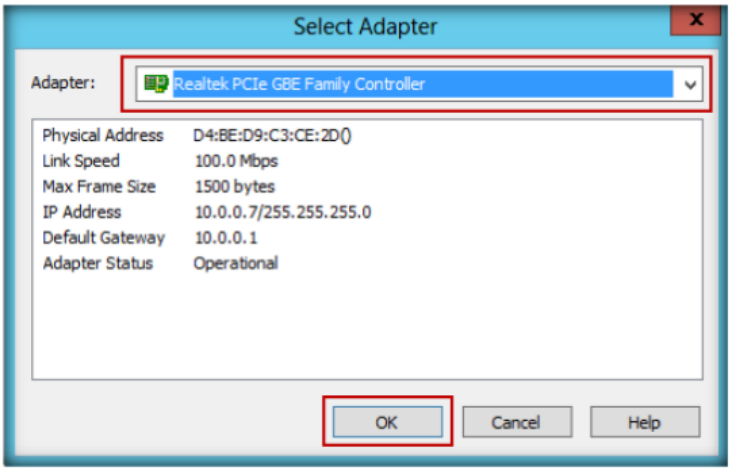


FIGURE 17.4: Colasoft Packet Builder Adapter settings

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.

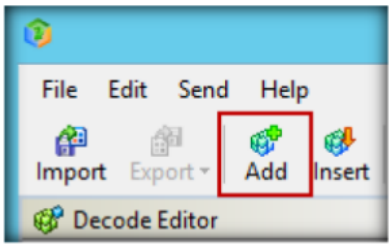


FIGURE 17.5: Colasoft Packet Builder creating the packet

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).

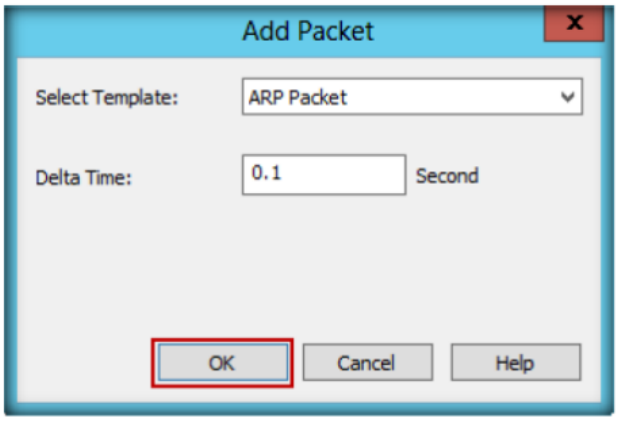


FIGURE 17.6: Colasoft Packet Builder Add Packet dialog box

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

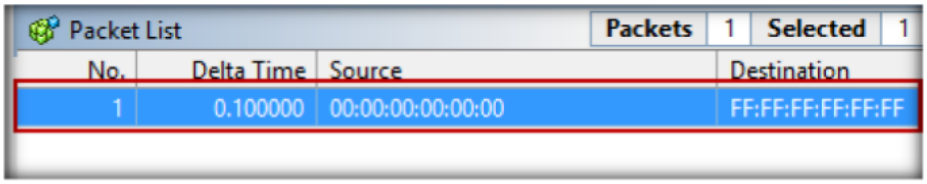


FIGURE 17.7: Colasoft Packet Builder Packet List

TASK 2

Decode Editor

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

Bust 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.

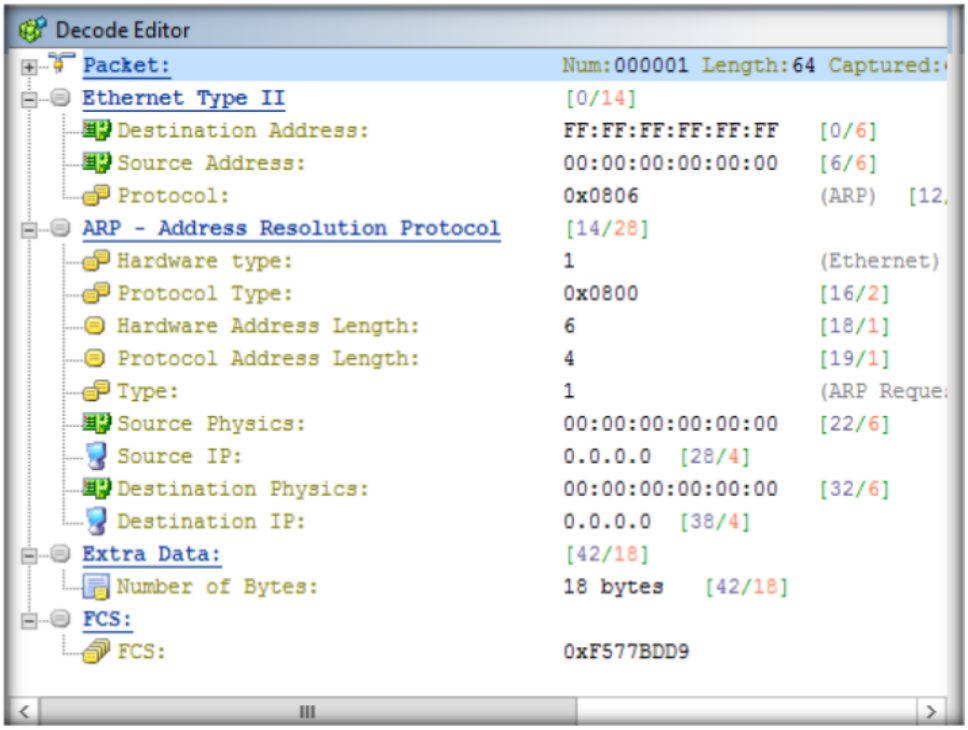


FIGURE 17.8: Colasoft Packet Builder Decode Editor

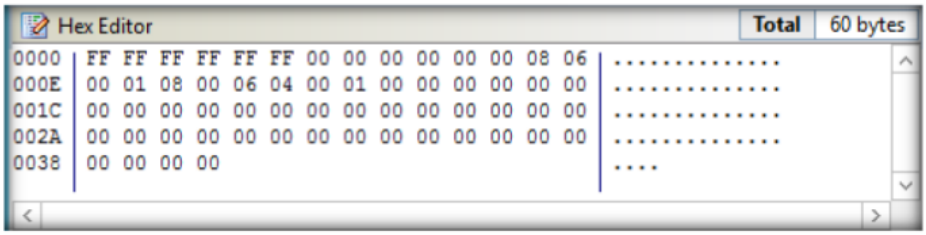


FIGURE 17.9: Colasoft Packet Builder Hex Editor

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

Select a packet from the packet listing to activate Send All button

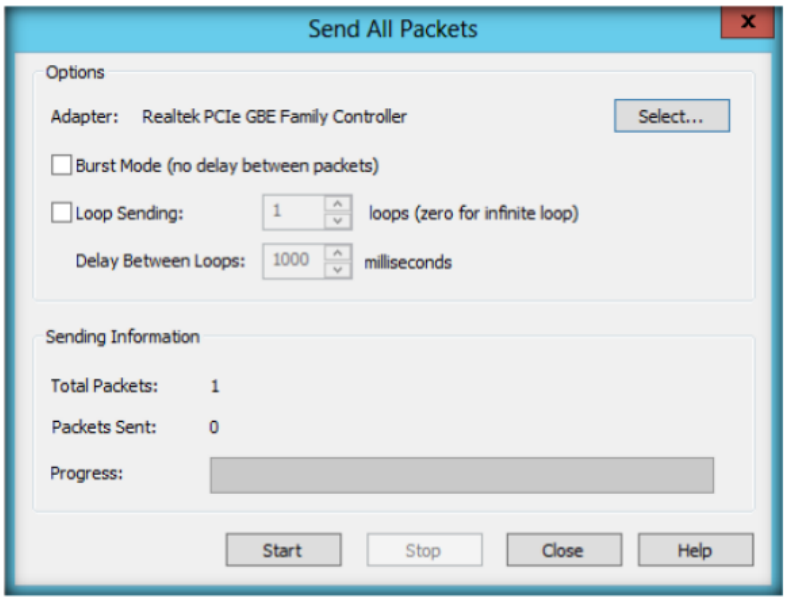


FIGURE 17.11: Colasoft Packet Builder Send All Packets

12. Click **Start**

The progress bar presents an overview of the sending process you are engaged in at the moment.

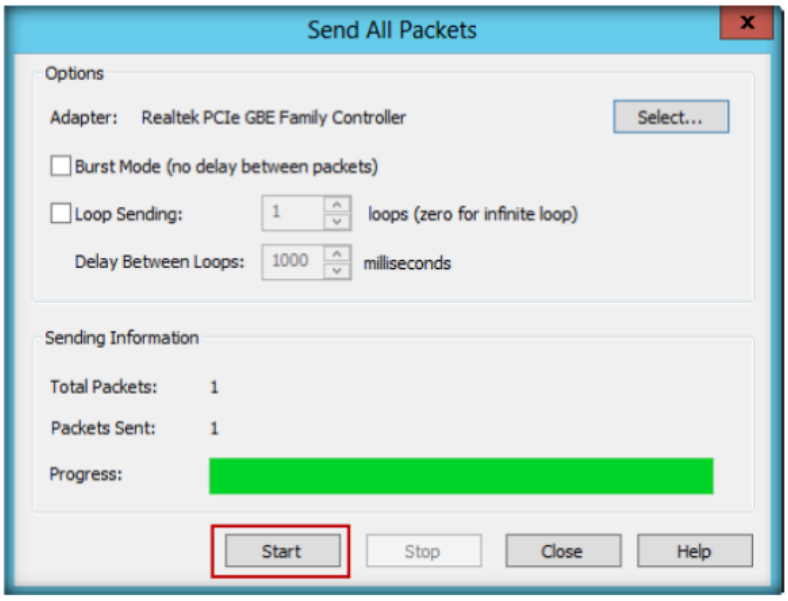


FIGURE 17.12: Colasoft Packet Builder Send All Packets

13. To **export** the packets sent from the File menu, select **File→Export→All Packets**.

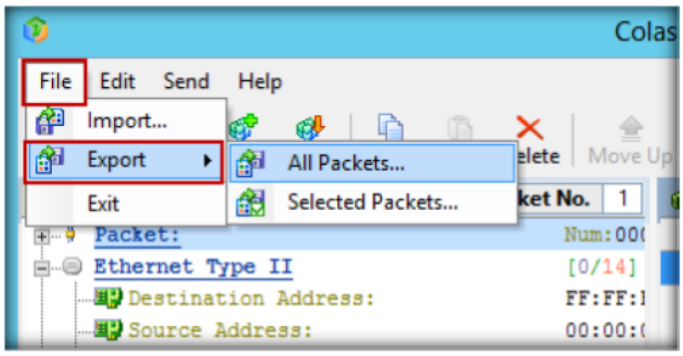


FIGURE 17.13: Export All Packets potion

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.

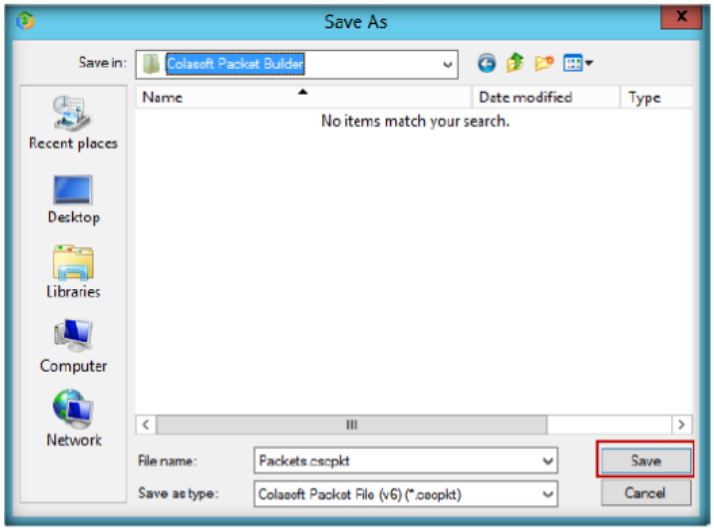


FIGURE 17.14: Select a location to save the exported file

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	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

18

Scanning Devices in a Network Using The Dude

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

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.

Lab Scenario

In the previous lab you learned how packets can be captured using Colasoft Packet Builder. Attackers too can sniff can 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.

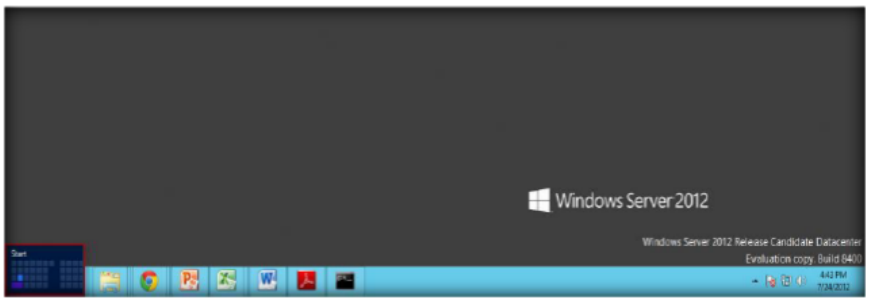


FIGURE 18.1: Windows Server 2012 – Desktop view

TASK 1

Launch The Dude

2. In the **Start** menu, to launch **The Dude**, click **The Dude** icon.

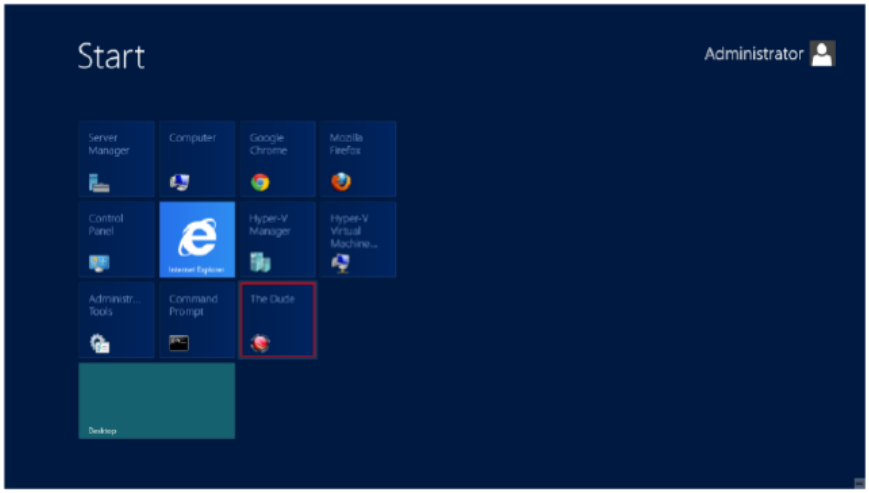


FIGURE 18.2: Windows Server 2012 – Start menu

3. The main window of **The Dude** will appear.

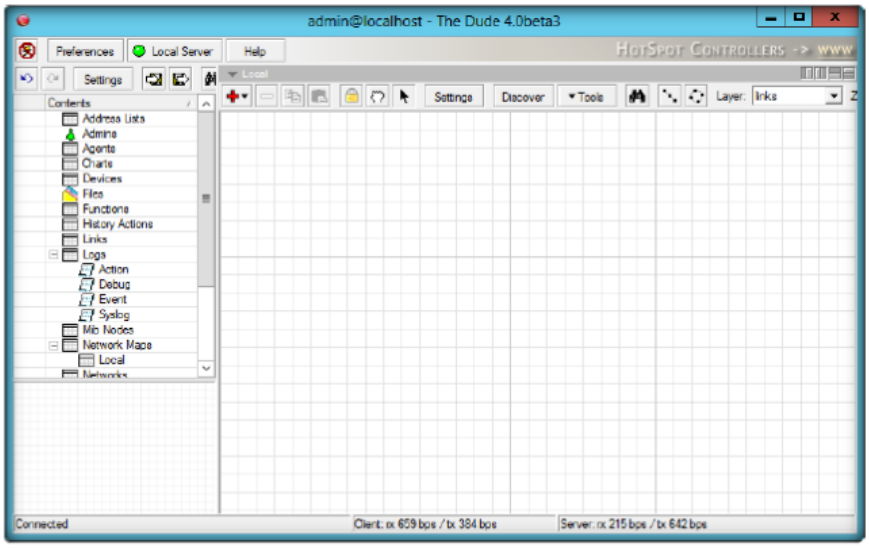


FIGURE 18.3: Main window of The Dude

4. Click the **Discover** button on the toolbar of the main window.

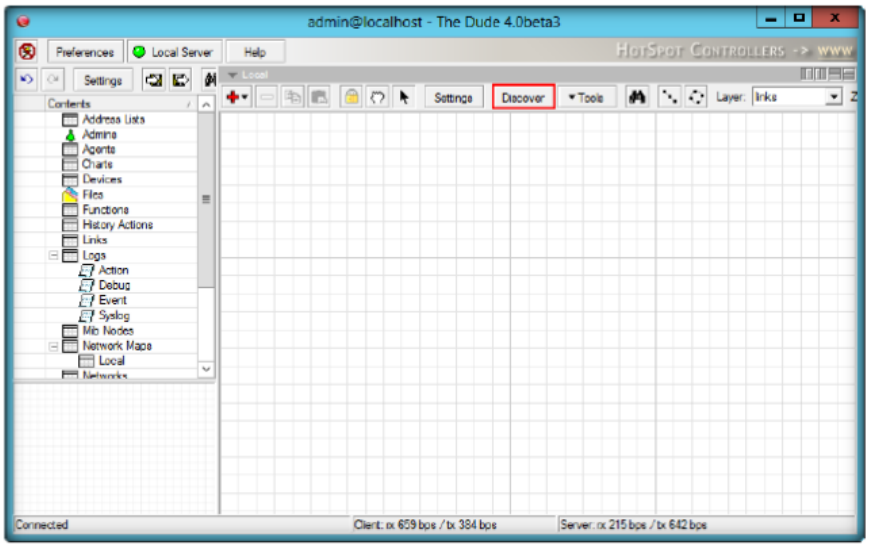


FIGURE 18.4: Select discover button

5. The **Device Discovery** window appears.

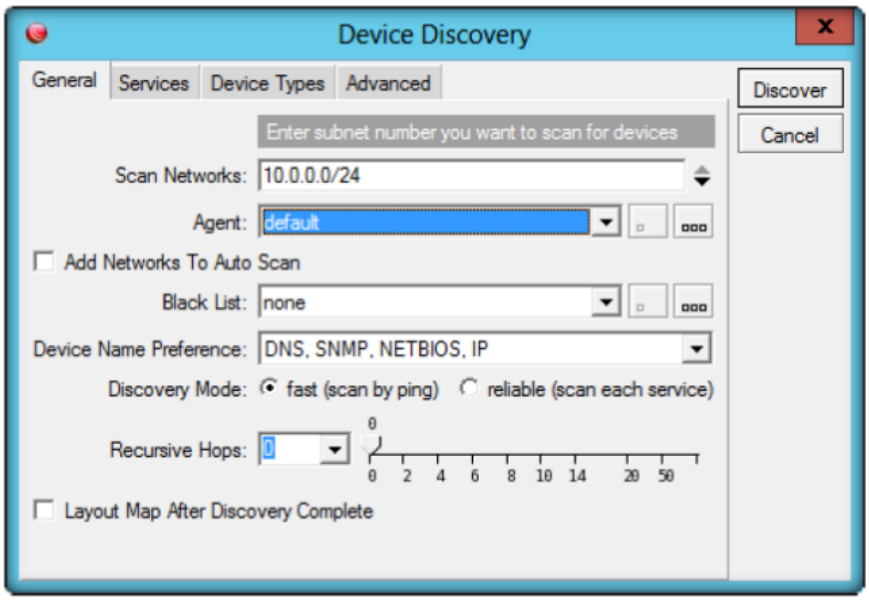


FIGURE 18.6: Device discovery window

6. 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**.

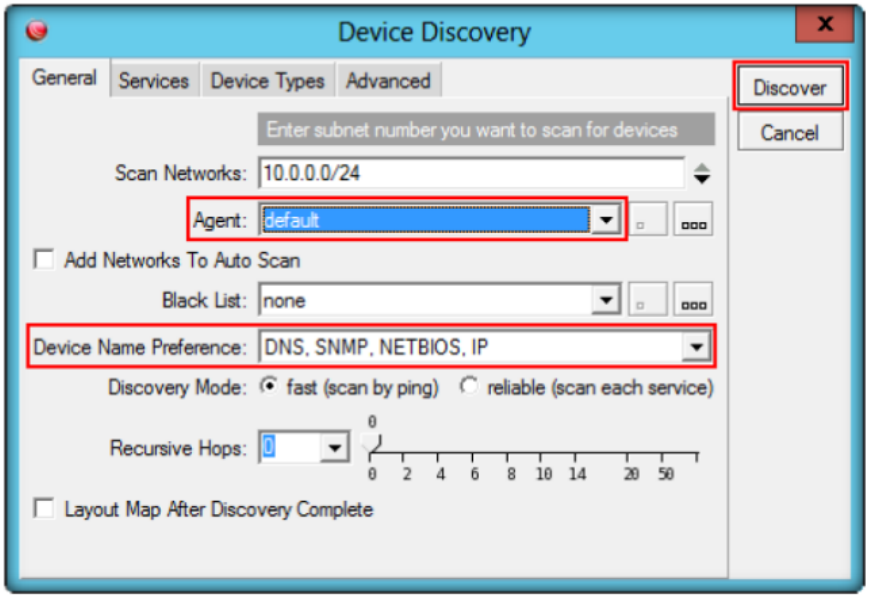


FIGURE 18.7: Selecting device name preference

7. Once the scan is complete, all the devices connected to a particular network will be displayed.

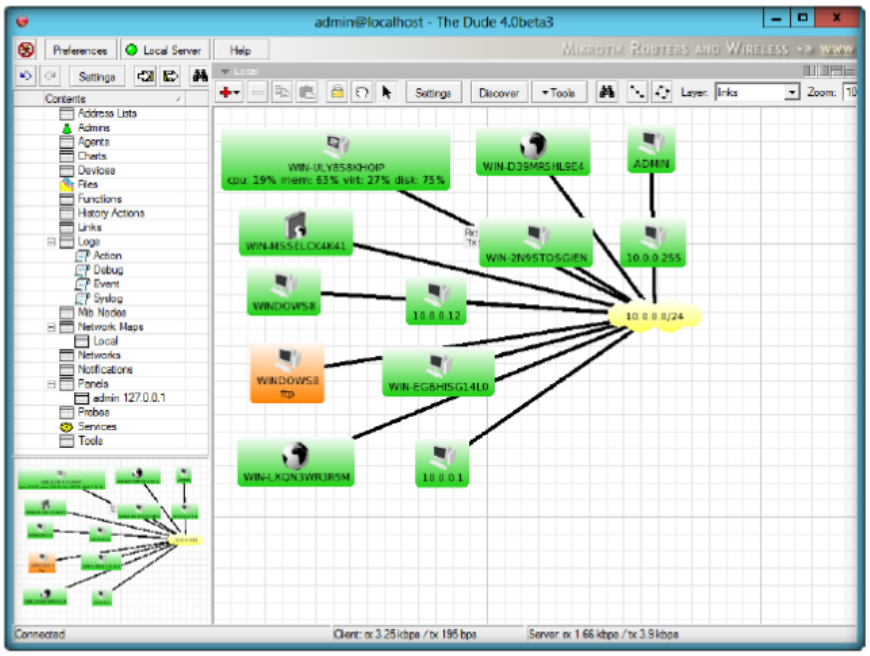


FIGURE 18.8: Overview of network connection

8. Select a device and place the mouse cursor on it to display the detailed information about that device.

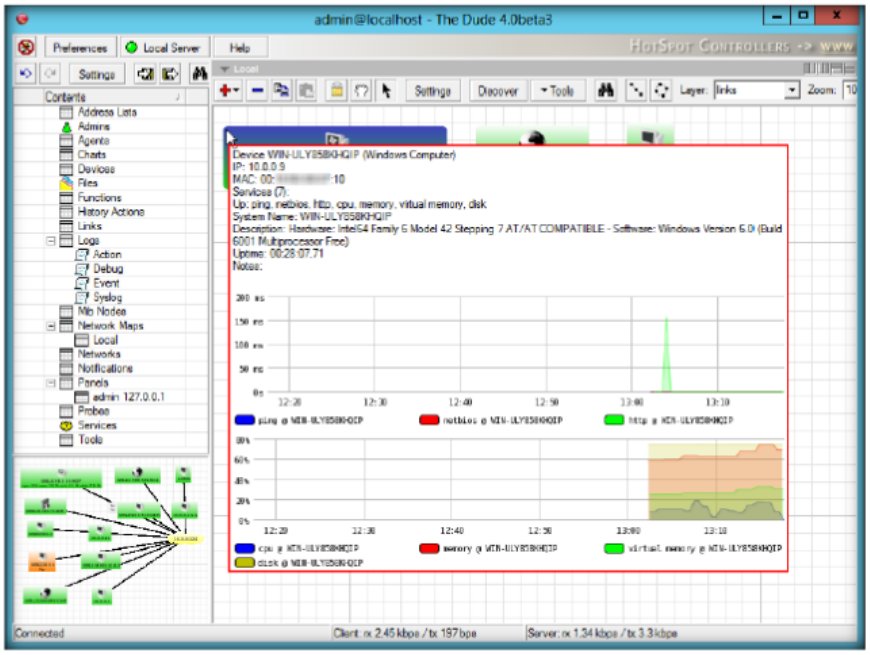


FIGURE 18.9: Detailed information of the device

9. Now, click the down arrow for the **Local** drop-down list to see information on **History Actions**, **Tools**, **Files**, **Logs**, and so on.

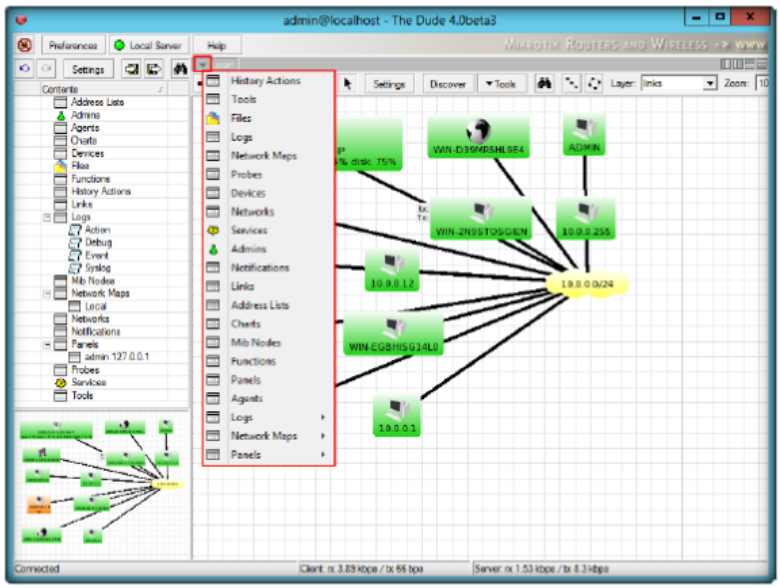


FIGURE 18.10: Selecting Local information

10. Select options from the drop-down list to view complete information.

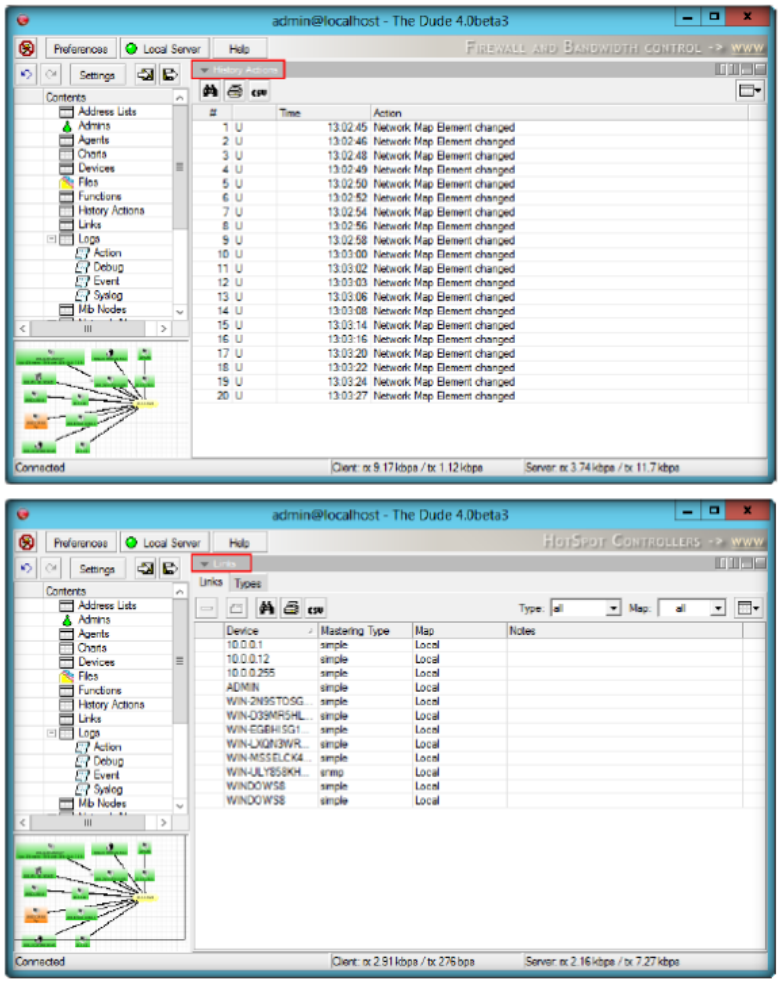


FIGURE 18.11: Scanned network complete information

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.

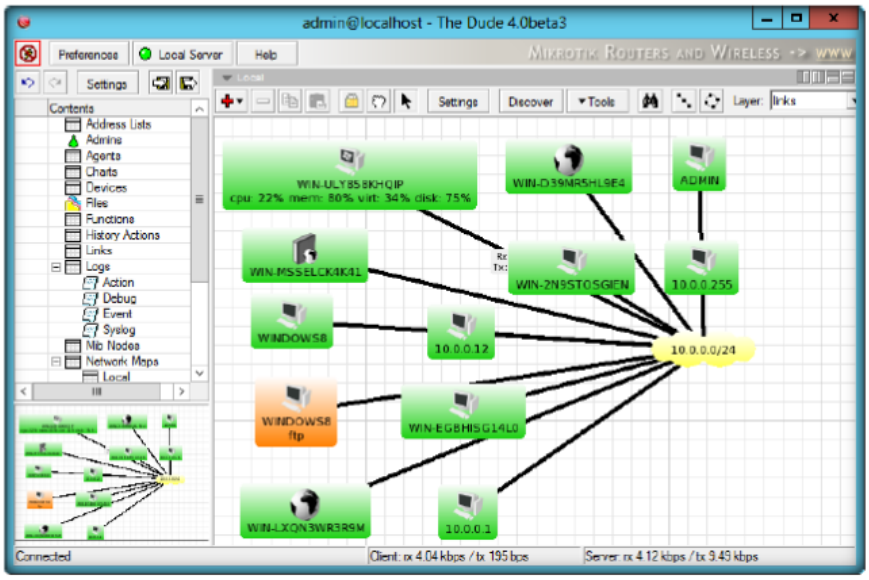


FIGURE 18.12: Connection of systems in network

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