Angry IP – An IP Scanner Tool

A Product Analysis and User Tutorial

William F. Slater, III, PMP, CISSP, SSCP

IDCP Internet Security

Marist College

Week 9 – Homework Assignment No. 2

Robert Cannistra, M.S. - Instructor

July 16, 2007

Table of Contents

Table of Figures and Tables

Disclaimer

The author states that the description of the Angry IP tool and its uses described in this document are strictly for use in an academic test network environment or in an isolated network environment that is strictly controlled, such as an isolated network segment. The author does not advocate the use of Angry IP in any production network environment and assumes no responsibilities for any uses of the Angry IP tool on any network and/or on any machine, nor does he assume any consequences resulting from the use of this tool.

Abstract

The Angry IP tool is a freeware IP scanner tool that can used to identify networked devices on an IP-based network segment and give detailed descriptions about their IP configurations, as well as their names. This document is both a product analysis and a brief user tutorial about the uses of Angry IP and how it works.

Introduction

The Angry IP scanner is a very fast, easy to use IP scanner and port scanner tool. It can scan IP addresses and ports in any specified IP address range. Compared to other IP scanner tools, its file size is very small. When it is used to perform IP scanning, Angry IP scanner simply and automatically pings each IP address in the specified IP address range to see if it is alive. Then, according to its product's configuration settings, it resolves the hostname, determines the MAC address, scans ports, etc. Data can be exported to a file in any of several formats, and the amount of gathered data collected about each host can be extended with the available plug-ins.

Common Uses

This program is mostly useful for network administrators to monitor and manage their networks. But it can also be used by the following: 1) students for learning networks; 2) researchers for security and networking projects; 3) auditors for analyzing networks; and 4) hackers for discovering information about network topologies and hosts they intend to break into.

Assumptions

This document assumes the person who uses the Angry IP tool, will have the following minimum levels of skills and experience:

Skill or Experience	Level of Experience
Basic computer experience	6 months to 1 year
Windows or Linux	6 months to 1 year
Understanding of how to use a browser to navigate to a website URL	1 month
Application software installation and execution	6 months to 1 year
TCP/IP Understanding	1 year
Understanding of IP address ranges and networks	1 year
Understanding of basic network security and computer security.	1 year
Understanding of files, file management and file management tools, such as Windows Explorer	6 months to 1 year
Understanding of how to unzip a file that is in WinZip format.	1 month

Table No. 1 – Minimum Skills and Level of Experience Required to use the Angry IP Tool

Product Description

Angry IP has been around for several years and is considered to be number 51 in the greatest hacker tools of all time. Basically, it is a very simple tool that operates in both Windows environments and Linux environments, to allow someone to easily and quickly scan an IP-based network IP address range that represents a network segment. Attributes and details about the version of the Angry IP product described in this document are shown in the Table No. 2 below:

Attribute	Detail
Name	Angry IP
Version:	2.21
Author:	Angryziber
URL Source:	http://www.angryziber.com/ipscan/
Pricing:	FREE
Platform(s):	Windows 2000 / Windows XP / Windows Vista / Windows Server 2003 / Linux
Version Image Date for the Windows Executable:	April 7, 2004
File Name:	ipscan.zip
Download File Format for the Windows Executable:	Windows Zip format
Download File Size for the Windows Executable:	106,149 bytes
Executable File Format for the Windows Executable::	Windows .EXE file
Executable File Size for the Windows Executable::	111,104 bytes
Modes:	GUI and command line

Table No. 2 – Angry IP Product Facts

Implementation

To implement Angry IP, go to the website at http://www.angryziber.com/ipscan/ and go to the Angry IP Scanner link shown in the figure below to click and start the download process:

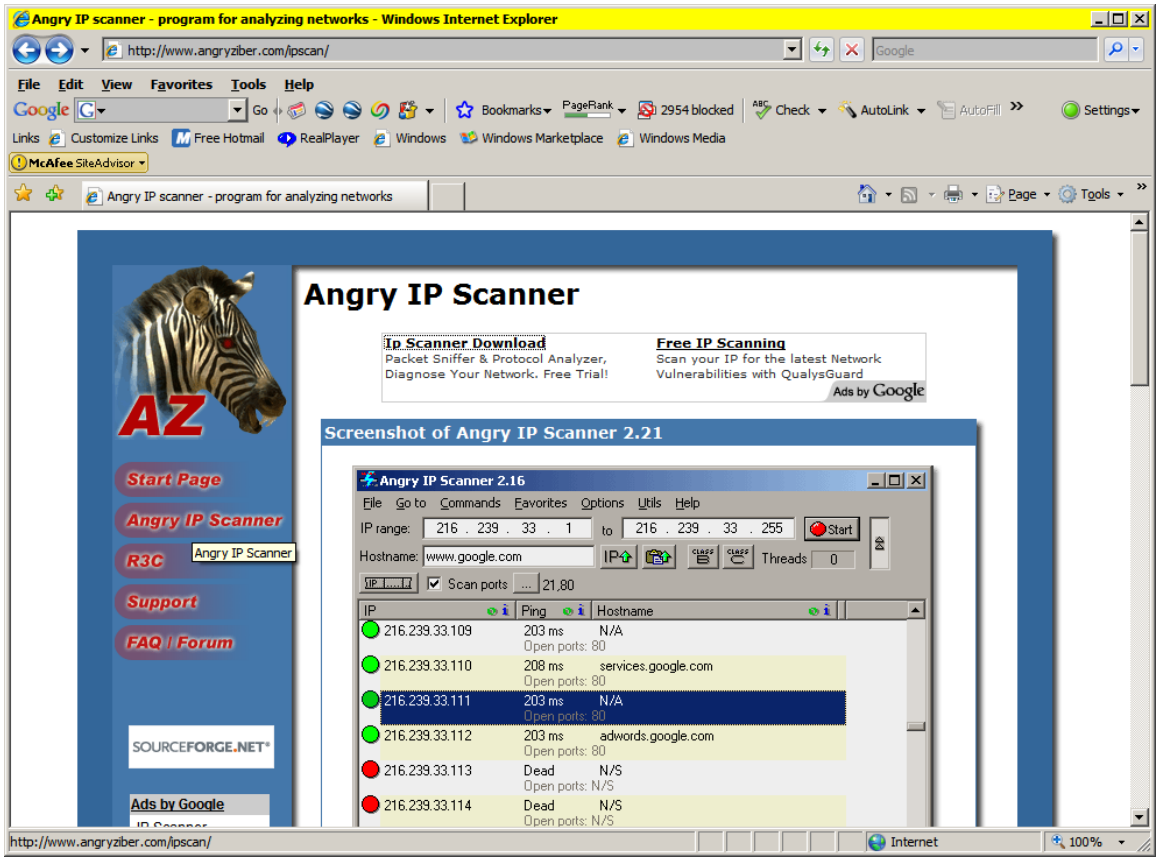


Figure No. 1 - The Angry IP Scanner website

Scroll down to the bottom of the page and click on the link named download page.

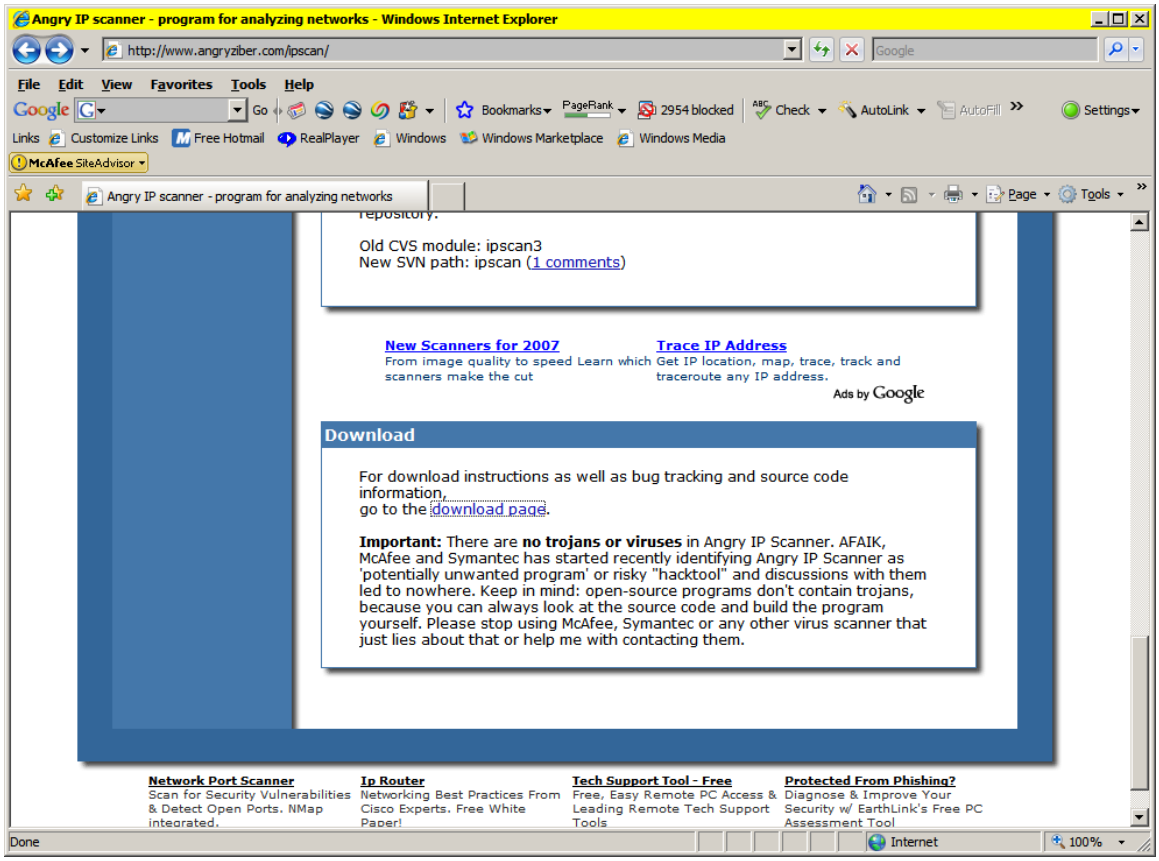


Figure No. 2 - The Angry IP Scanner download area.

To begin the program download, click on the link named ipscan.zip.

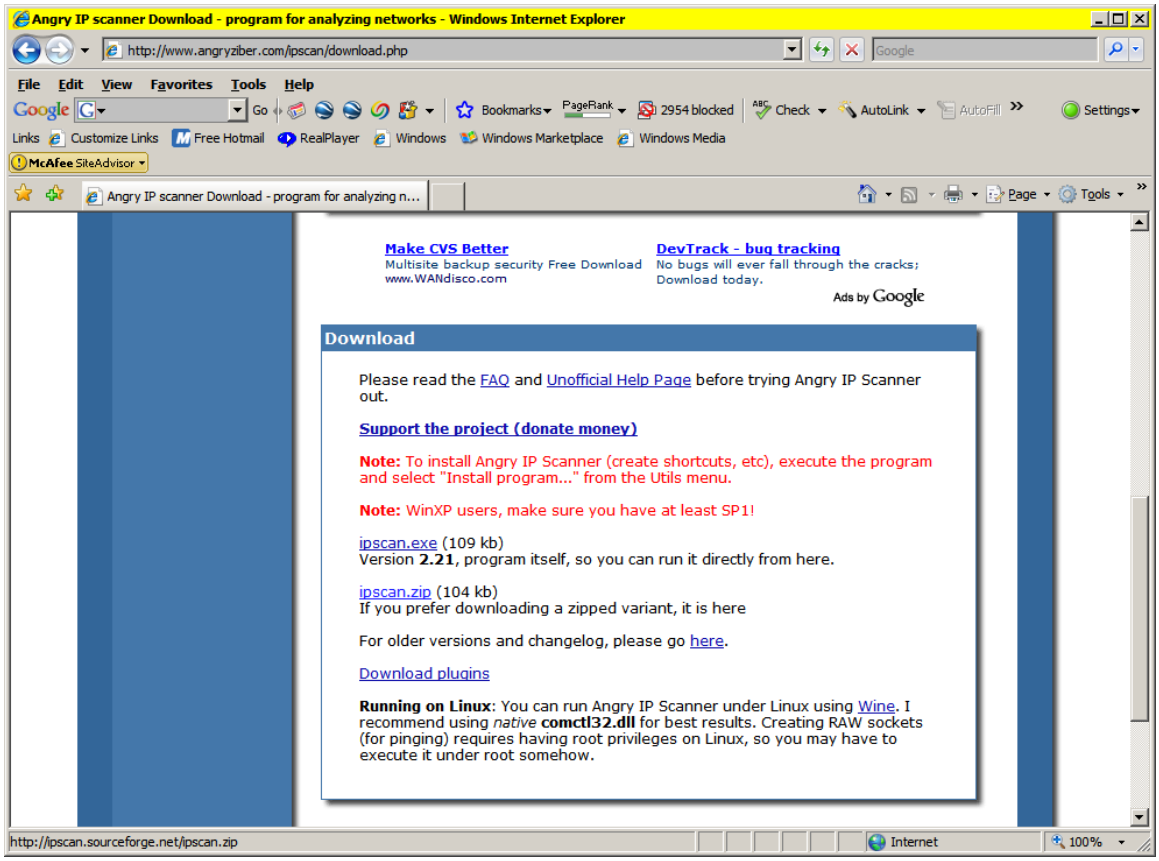


Figure No. 3 - The Angry IP Scanner download area in greater detail.

Save the downloaded file into a directory with a logical sounding name. I used c:\slater\00_Anti_Hacker_Tool_Kit_Angry_IP.

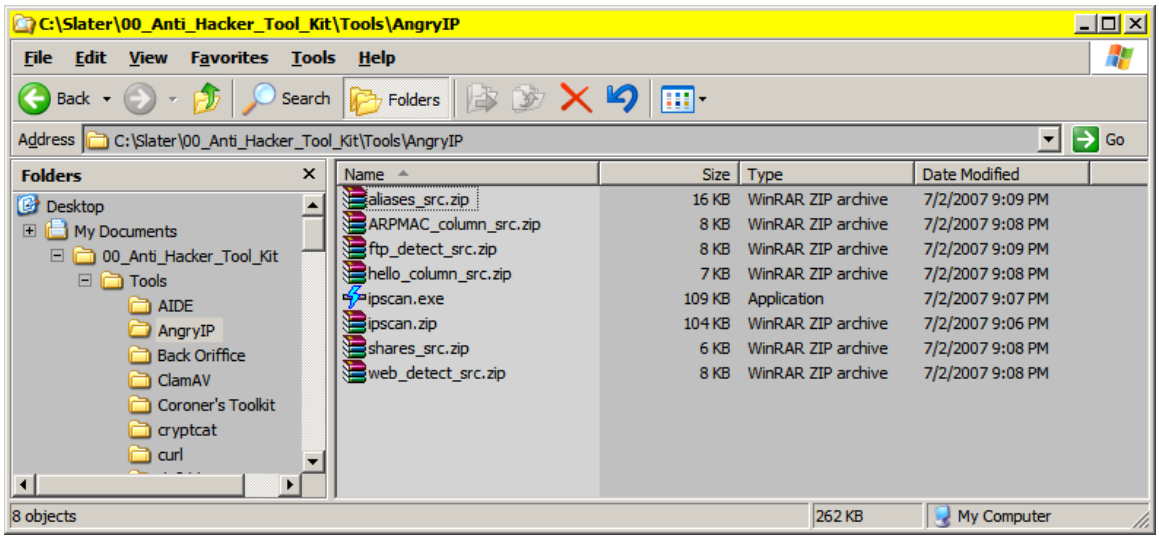


Figure No. 4 - Saving Angry IP Scanner into a local directory.

When the product has been downloaded, the file name will be ipscan.zip. It should be unzipped, revealing the file name ipscan.exe. Using Windows Explorer, the ipscan.exe should be copied to a meaningful directory name, such as c:\tools\angry_ip\. There are then two was to operate the program.

1) Using Windows Explorer, double-click the executable file, ipscan.exe. The figure below shows how to do this.

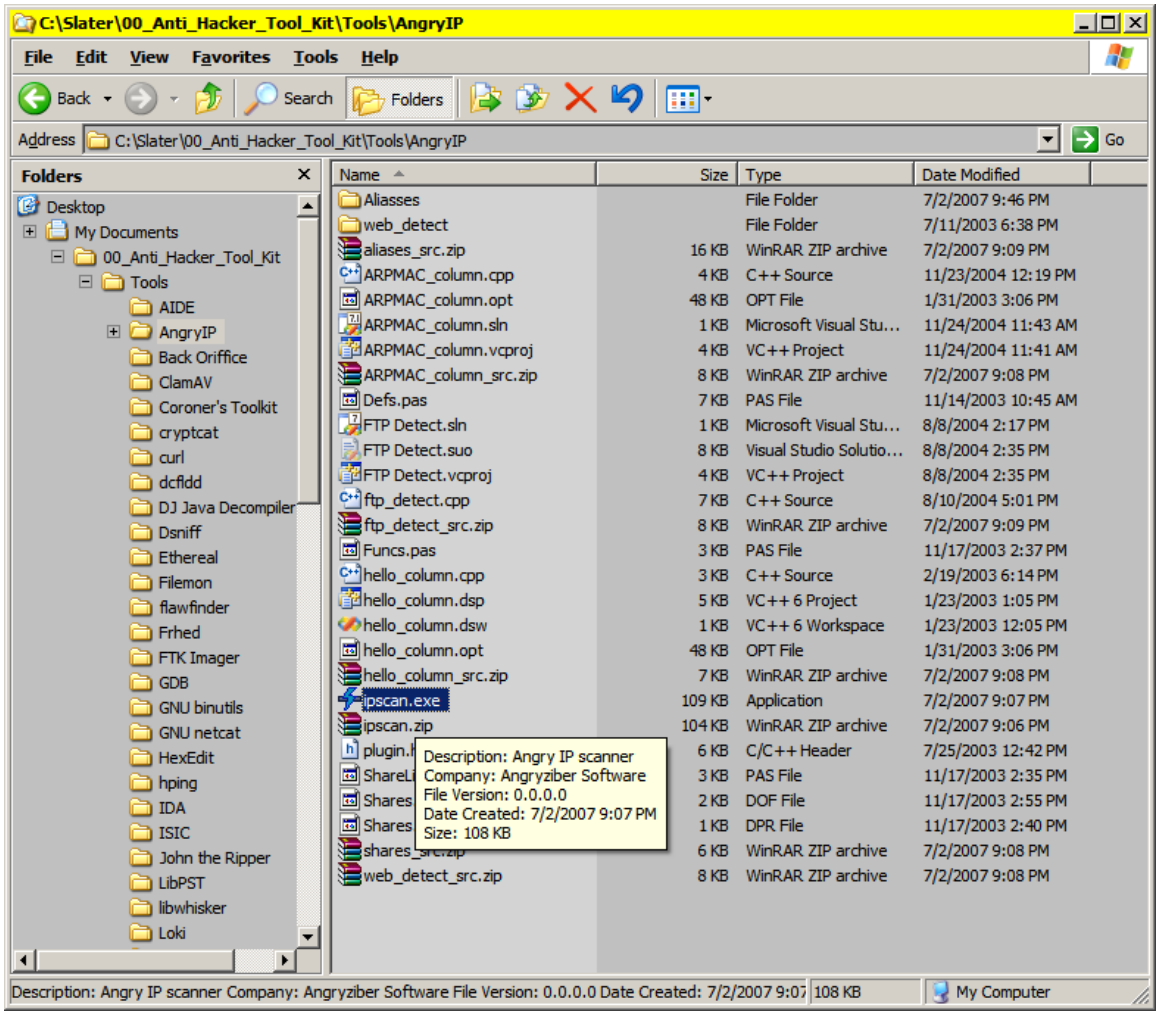


Figure No. 5 - Using Windows Explorer to initially launch the Angry IP application.

2) After launching Angry IP, you can execute the program as shown in the section below, or you can click on the Utilities menu option and go through a formal installation process, during which Angry IP application settings are written into the Windows Registry. This is a simple, safe process and the figure below show the initiation of this process. The chief advantage of a formal installation process is that the installation will create a program group

for Angry IP, as well as a short cut link for the Desktop, so you can easily start the application.

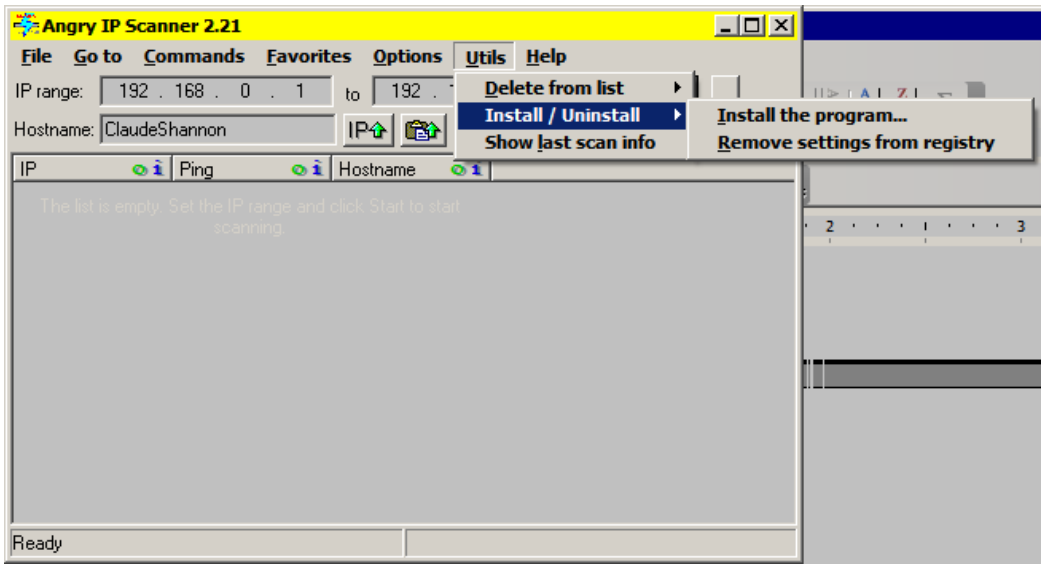


Figure No. 6 - The Angry IP application, initiating the formal installation process.

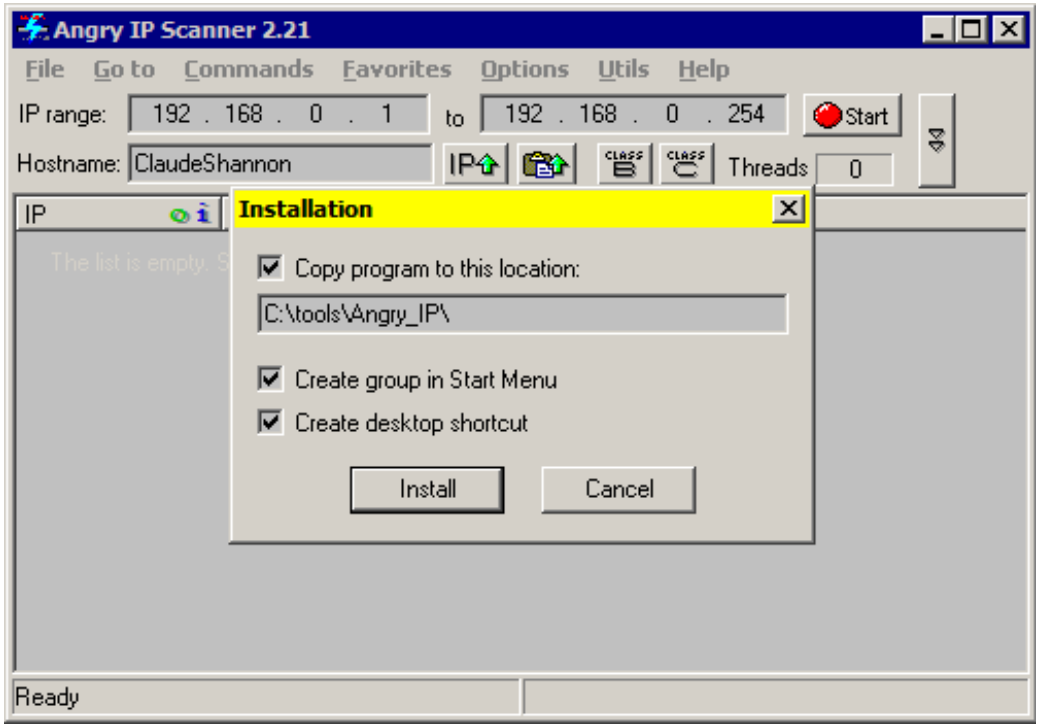


Figure No. 7- The Angry IP application, completing installation process.

How to Use

Once it is properly installed, Angry IP can be invoked using either shortcut placed on the Desktop of the computer where it was installed, or by clicking on Start | Programs |Angryziber | Angry IP Scanner. When the program launches, you get the image shown in Figure No. 8 below:

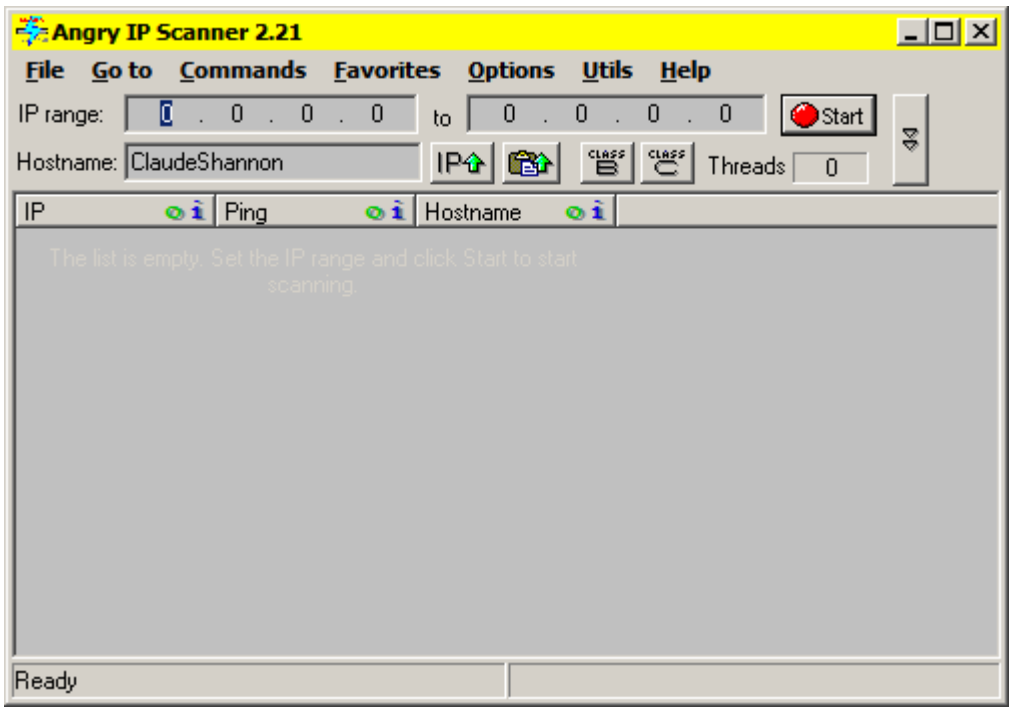


Figure No. 8 - The Angry IP application at initial start-up.

You should the IP address range of the network you want to scan. Angry IP automatically fills in the completed octets of the first address in the space for the second part of the range. Figure 9 below shows a completed IP address range for a Class C IP network.

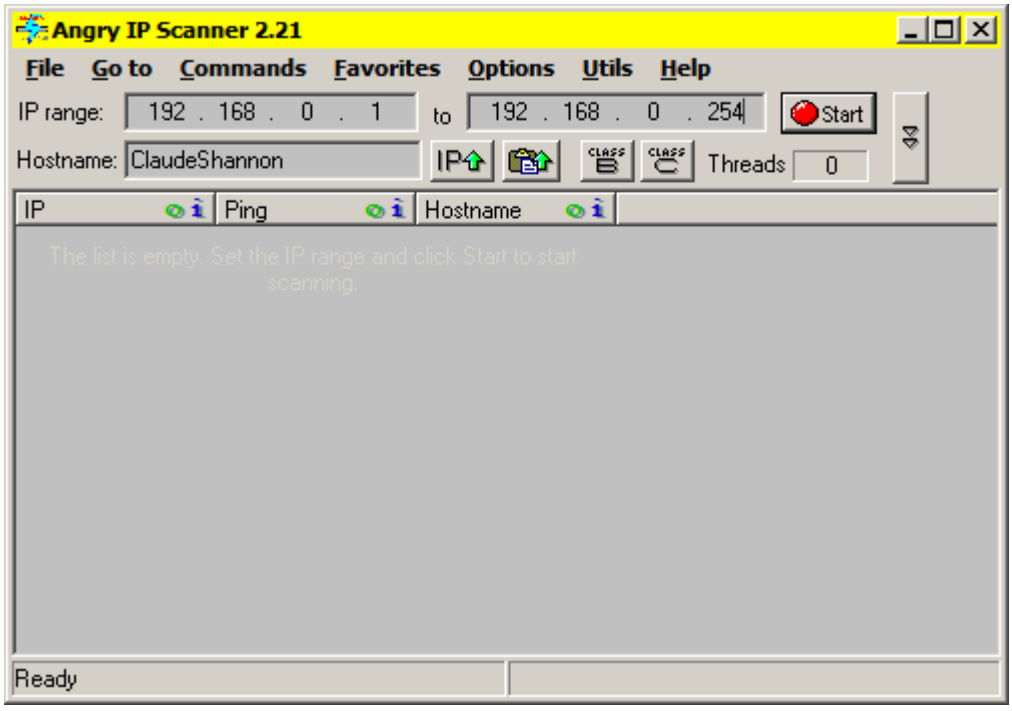


Figure No. 9 - Entering a Class C IP Address range for scanning.

Click the Start button to start the IP scanning of this address range you configured in the previous step.

Identify IP Hosts on the Network

Angry IP will automatically use the ping utility to ping every possible IP address given in the range that you input prior to starting the scan process. Figure 10 below show how the scanning looks when it is in process.

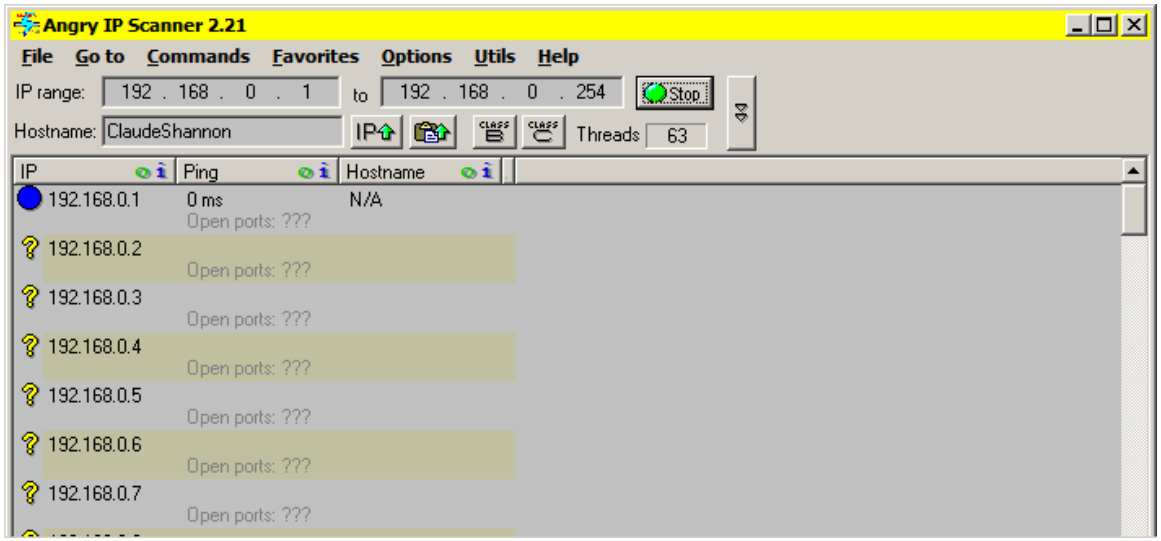


Figure No. 10 - The Natural order of IP Addresses, starting with the beginning of the IP address range.

When the scanning is completed, Angry IP proudly displays a system modal informational dialog box indicating how many IP hosts were scanned, how many live IP hosts were found, and how many had open ports.

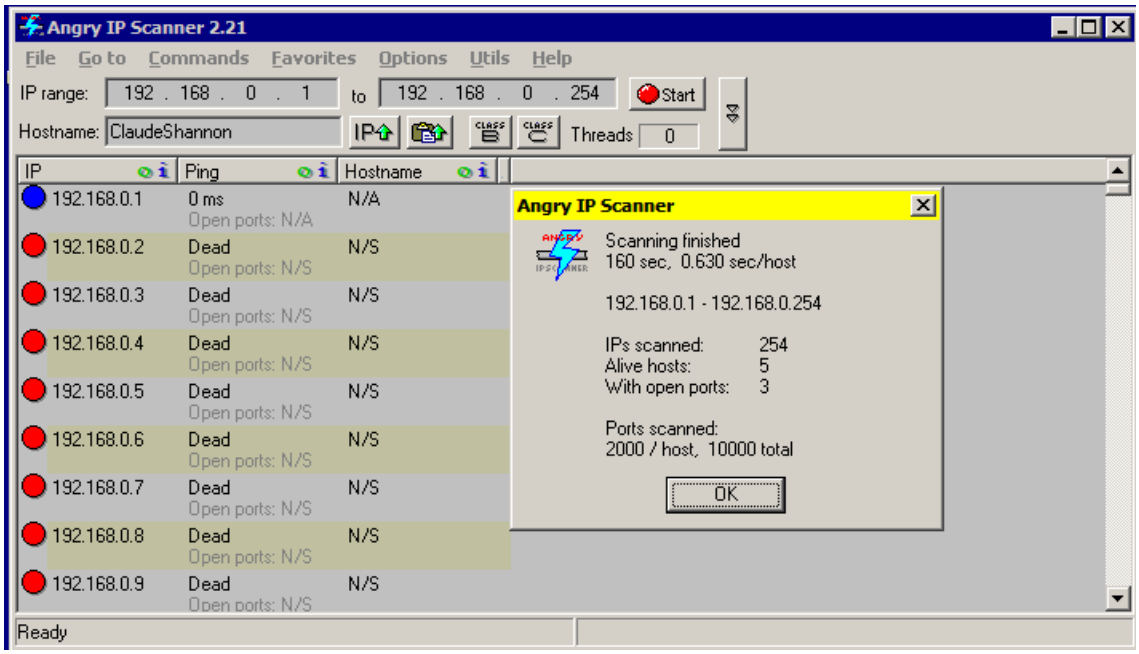


Figure No. 11 - The small announcement dialog box Angry IP in scan completion mode.

To see the hosts in a more meaningful display, click on the term Hostname in the column title bar. That will cause Angry IP to sort its list of IP hosts by Hostname. The result is a quick display of the live IP hosts all together.

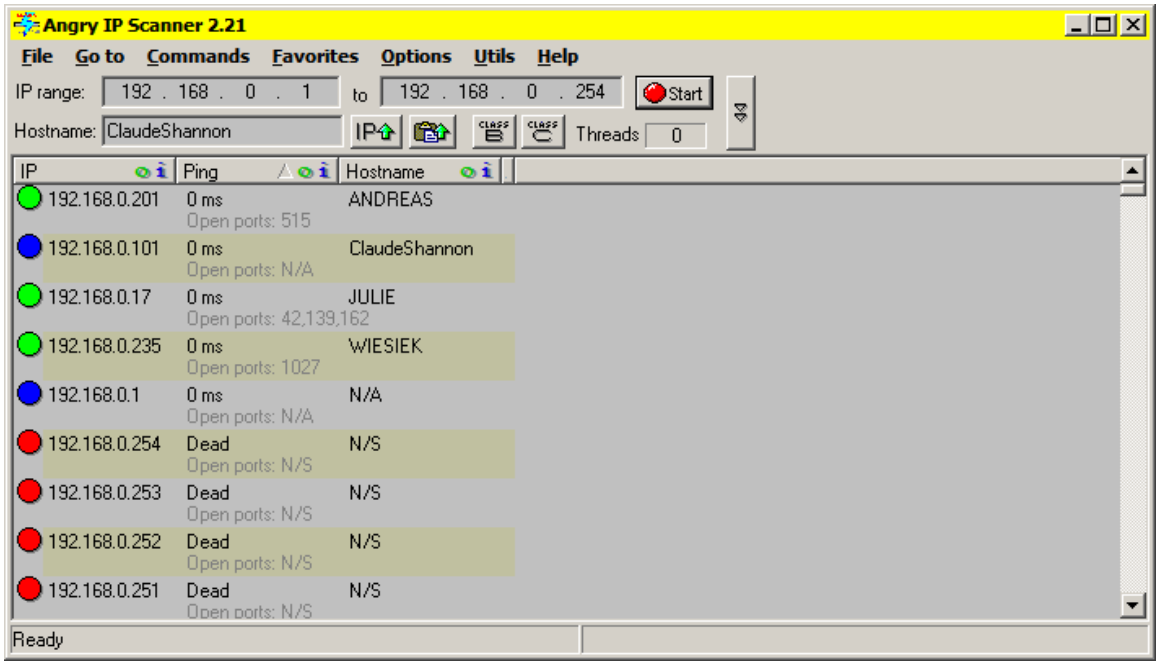


Figure No. 12 - IP Addresses Sorted by Live Hosts

To discover specific details about a live host, click on the host to select it and then use menu options to gather additional details about that host.

Designed for Efficiency and Performance

In order to increase scanning speed, Angry IP is designed to efficiently operate using a multithreaded approach: in standard operation with a large IP address range, the program creates several threads, up to a limit of 65 threads, to increase the speed of pinging, data collection and display. Review Figures 13 and 14 to see the difference between in the ipscan.exe process when a full scan is underway and when the tool is in a quiet state. In Figure 14, ipscan.exe is only using two threads compared to 65 in Figure 13 when a full scan is in operation.

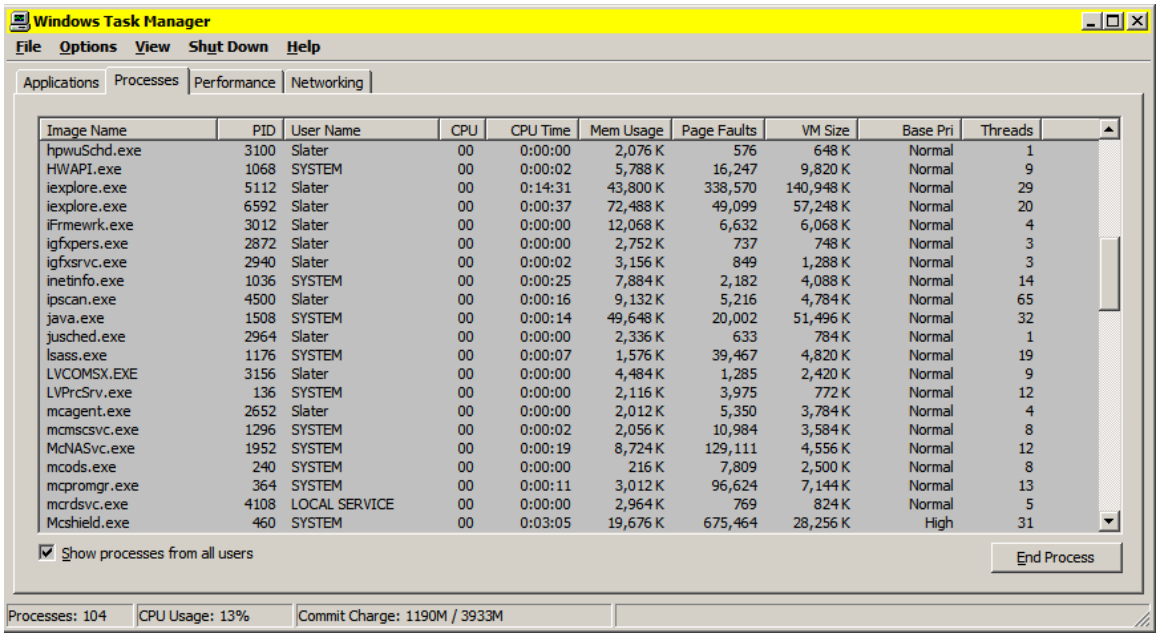


Figure No. 13 - Windows Task Manager shows Angry IP in Full Scan Mode has up to 65 Threads!

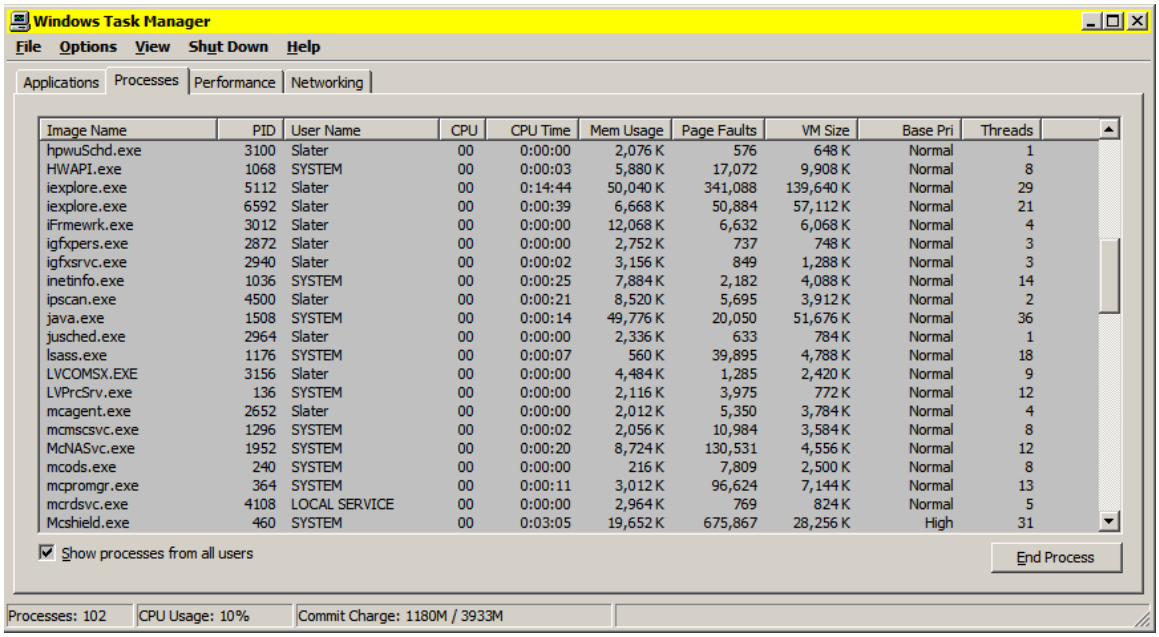


Figure No. 14 - Windows Task Manager shows Angry IP in scan completion mode with only two threads!

Scan for TCP Ports

One main reason for IP scanning is to get into the details involving ports that are available for various IP hosts. Using the Options menu item, you can go to a dialog box that will allow you to Select specific ports. It is quickest to use port ranges rather than search on specific port numbers, but this will also add time to your scanning, because it will require that every port number in that range you specify is probed for every IP host address in the IP scanning range. If there are 2000 port numbers per computer to scan, that port scanning effort could be significant in a large network segment. Figure 15 below shows how to set a port range in preparation for port scanning.

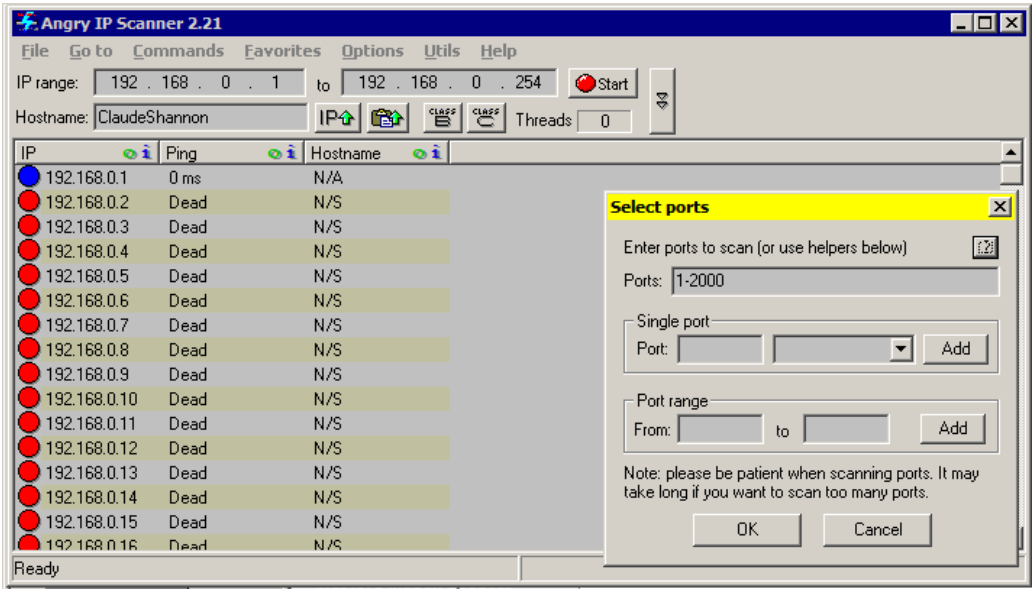


Figure No. 15 - Port Range Selection Dialog Box from the Options menu

Saving the Scan Results

Angry IP allows you to save the results of your scan. This can be useful for conducting an audit and using this data for the audit report. After the scan has completed, click on the File option on the menu and you can export the entire range results, or only the IP addresses that are selected. Figure 16 below shows how to save your IP scanning results. Note that you need to select the IP hosts whose information will be saved.

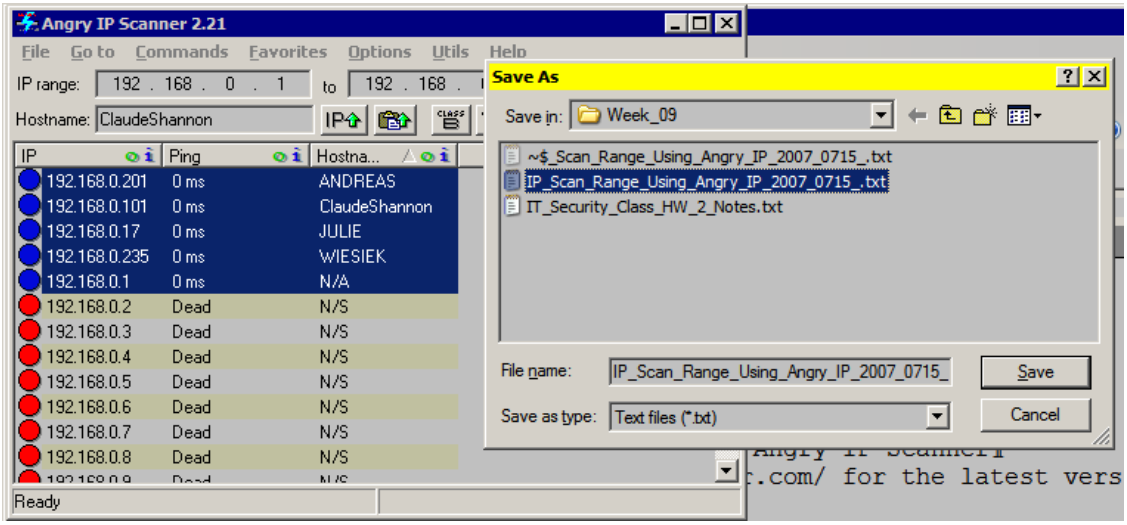
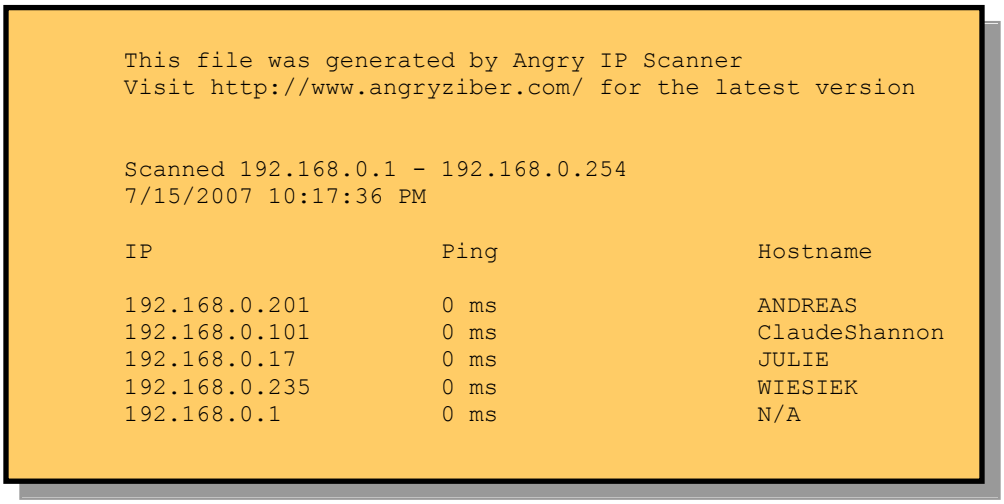


Figure No. 16 - Angry IP allows the scan data on selected host names to be exported and saved to a text file.

The information in Figure 17 below is what was written to the text file to which the IP scan data was exported:



```
This file was generated by Angry IP Scanner
Visit http://www.angryziber.com/ for the latest version


Scanned 192.168.0.1 - 192.168.0.254
7/15/2007 10:17:36 PM

IP                      Ping                    Hostname

192.168.0.201           0 ms                    ANDREAS
192.168.0.101           0 ms                    ClaudeShannon
192.168.0.17            0 ms                    JULIE
192.168.0.235           0 ms                    WIESIEK
192.168.0.1             0 ms                    N/A
```

Figure No. 17 -The IP host selection data gets saved in this text format for later reuse.

Hacking with Angry IP

Under the Commands menu option, Angry IP can be used to invoke a probing "attack" on any of the live IP hosts it identifies in a scanning range. Shown below, is the use of Windows Explorer to connect to a selected IP host through a connection showing the shares at 192,168.0.101. In the hands of an evil person who could obtain use names and passwords, this could be an extremely dangerous capability. Figure 18 shows how a hacker could use some of Angry IP's capabilities on the Commands menu in order to enter a live host machine in the IP address range via an IP connection.

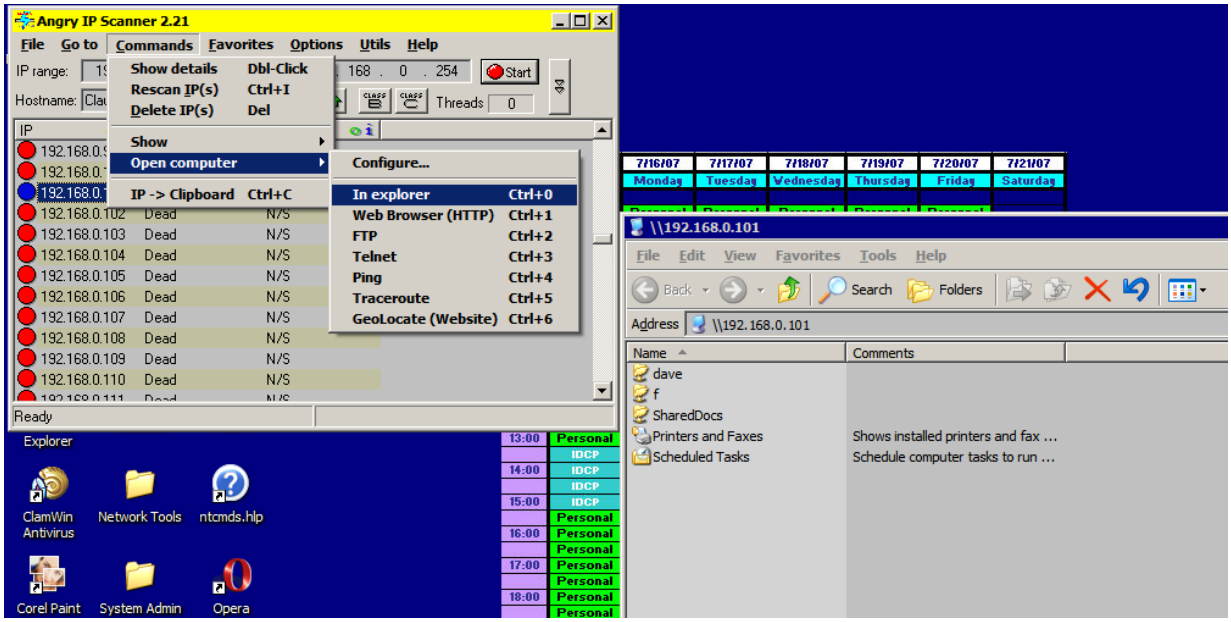


Figure No. 18 - Angry IP can be used on selected IP hosts to hack into the machine, using tools over the network. In this case, Windows Explorer was used to enumerate the shares across the network and Angry IP invoked this instance of Windows Explorer locally using a remote network connection.

Command Line Usage

Angry IP can be invoked also using the command line at the Windows Command Prompt. However, this tutorial will not cover that option.

Product Extensibility

Through the use of "plug-ins," Angry IP's functions can be extended so that the product can display even greater details about the IP hosts on a given IP address range. However, this document will not cover those extensible capabilities of the product.

Network Defenses

While finishing this assignment, I used Angry IP to scan the IP address range at my ISP (SPEEDSITE.com) where my website, BILLSLATER.com, is hosted. That range is 206.126.230.1 – 206.126.230.254. On the second attempt, I noticed it was taking longer, so I stopped it and turned off the port scanning option. On the third attempt, when I restarted the IP scan without port scanning, I noticed all IP hosts came up listed as "dead" when the scanning was completed. This means that the network defenses at my ISP must have recognized my scanning exercise with Angry IP as a public, external IP scanning attack from my SBCGLOBAL.NET IP address of 75.3.131.111, and on the third attempt they were ready for me and just shut down scanning attempts from this IP address. Note that these three attempts were my first and only attempts at scanning public, external IP address ranges. (Maybe I better call my ISP in the morning and send them a copy of this report so they won't think I was up to something with evil intent!) See Figure 19 for a picture of all the IP hosts in the specified address range at my ISP. All reported as "dead," though I am certain they were not. This is because a defense mechanism made Angry IP believe that all IP hosts in that address range were "dead."

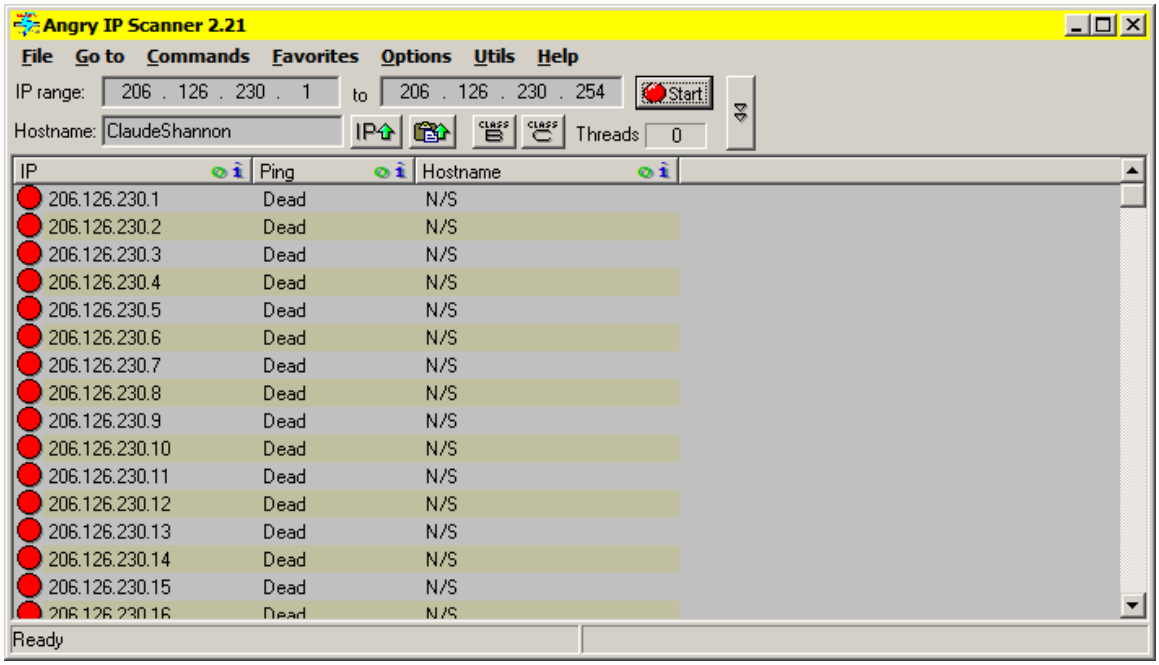


Figure No. 19 -Angry IP can showing "dead IP hosts" after network defenses were applied after the third remote IP host scan attempt on the range from 206.126.230.1 – 206.126.230.254.

Product Technical Support

As a free product, Angry IP doesn't come with a lot of fancy technical support such as a 1-800 Technical Support Help Line number. But the website where you download Angry IP does provide a Frequently Asked Questions file, as well as a Forum for posting questions.

Product Financial Contributions

Due to the technical excellence of this product and its standing in the hacker community, it can be said that the quality of such a free and use product is a feat as well as a generous contribution to the technical networking world. The team that developed

this product does accept financial contributions when people feel led to donate money for their efforts, and details of how to contribute financially are on the Angry IP website.

Conclusion

Angry IP is a great, free, legal "hacker tool" with which to learn about TCP/IP, IP scanning, and port scanning. Its strengths are its ease of use and its high performance capability because of the advance multi-threading technique and capability it uses to perform its scanning and collect the data it has discovered during scanning. But as with any network-based hacker-like tool, it must be used with care, or else it could get the user into big trouble, either on the job, with law enforcement authorities, or both.

Glossary

Terminology	Definition
External IP Address	The unique public IP address that is either static or dynamically assigned to a router's external interface. Note DSL Routers and Cable Modem Routers typically have dynamically assigned IP addresses which are assigned by an ISP's DHCP server.
Internal IP Address	The unique public IP or address that is both static and assigned to a router's external interface.
IP	The Internet Protocol, which functions at the Network Layer, to provide a way to encapsulate segments from the Transport Layer into a packet that has a header with the Source and Destination IP address. On a given private network, all IP hosts must have unique IP addresses, and on the big Internet, and public IP addresses must be unique.
LAN	LAN stands for Local Area Network, which is a network configuration that is typically found at one site of a company. LANs typically have high-speed transmission capacities in the realm of 10/100/1000 Mbs.
PING	PING is an IP host-based, network troubleshooting software tool that allows a user to send test messages to another IP host. PING can be executed using a host IP address, or if a DNS server is available to resolve host names, PING can be executed using the host name. Normally, with a Microsoft default PING, four test messages are sent to a host. The reply time in milliseconds for each ECHO REPLY is displayed if the PING was successful. PING is valuable because it tells a user that Layers 1 – 4 of his or her IP host are working properly and also that the Layers 1 – 4 of the target IP host are working properly. PING is based on the ICMP Protocol, which is part of the TCP/IP protocol suite defined in the RFCs.
TCP	The Transmission Control Protocol, which works at the Transport Layer, to control TCP connections, place data into segments in preparation to be placed into an IP packet at Layer 3, and also resend data based on the non-receipt of an ACK message.

Terminology	Definition
TCP Port	From a network engineer perspective, a TCP port is an endpoint connection between two IP hosts. From an OS perspective, a TCP port is a special communication location associated with an IP address, and it is designated by a number using this kind of notation with an IPv4 address: 206.126.230.92:80. TCP ports are used by Layer 4, the Transport Layer (and other upper layers) in TCP communications, to establish and maintain connection-oriented network communications between two IP hosts that are each talking TCP. Similarly, UDP (User Datagram Protocol) ports are used by Layer 4, the Transport Layer (and other upper layers), in UDP communications, to utilize connectionless network communications between two IP hosts that are each talking UDP. There are at least two types of numbers associated with TCP Ports and UDP Ports. 1) Well-known Ports that are established by the Internet Engineering Task Force (IETF), assigned by the Internet Assign Numbers Authority (IANA), and documented in the RFCs; and dynamically assigned ports, which are especially used by IP clients attempting to connection to an IP host running a server that has an IP address and which is listening for communications on a well-known port.

Bibliography

Casey, E. (2001). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press: London, England.

Cisco Systems, Inc. (2003). Cisco Academy Program CCNA 1 and 2 Companion Guide, third edition. Cisco Press: Indianapolis, IN.

Farmer, D. and Wietse, V. (2005). Forensic Discovery. Addison-Wesley: Upper Saddle River, NJ.

Middleton, B. (2005). Cyber Crime Investigator's Field Guide, second edition. Auerbach Publications: Boca Raton, FL.

Pfleeger, C. P. and Pfleeger, S. L. (2003). Security in Computing, third edition. Prentice Hall: Upper Saddle River, NJ.

Shema, M., et al. (2006). Anti-Hacker Tool Kit, third edition. Osborn-McGraw Hill: Emeryville, CA.

Vacca, J. R. (2002). Computer Forensics: Computer Crime Scene Investigation. Charles River Media: Hingham, MA.