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 Contents	2
Table of Figures and Tables	3
Disclaimer	5
Abstract	6
Introduction	7
Common Uses	7
Assumptions	8
Product Description	9
Implementation	10
How to Use	16
Identify IP Hosts on the Network	18
Designed for Efficiency and Performance	20
Scan for TCP Ports	22
Saving the Scan Results	23
Hacking with Angry IP	25
Command Line Usage	26
Product Extensibility	26
Network Defenses	27
Product Technical Support	28
Product Financial Contributions	28
Conclusion	29
Glossary	30
Bibliography	32

# Table of Figures and Tables

Name	Description	Page Number
Table No. 1	Minimum Skills and Level of Experience Required to use the Angry IP Tool	8
Table No. 2	Angry IP Product Facts	9
Figure No. 1	The Angry IP Scanner website	10
Figure No. 2	The Angry IP Scanner download area.	11
Figure No. 3	The Angry IP Scanner download area in greater detail.	12
Figure No. 4	Saving Angry IP Scanner into a local directory.	13
Figure No. 5	Using Windows Explorer to initially launch the Angry IP application.	14
Figure No. 6	The Angry IP application, initiating the formal installation process.	15
Figure No. 7	The Angry IP application, completing installation process.	15
Figure No. 8	The Angry IP application at initial start-up.	16
Figure No. 9	Entering a Class C IP Address range for scanning.	17
Figure No. 10	The Natural order of IP Addresses, starting with the beginning of the IP address range.	18
Figure No. 11	The small announcement dialog box Angry IP in scan completion mode.	19
Figure No. 12	IP Addresses Sorted by Live Hosts	20
Figure No. 13	Windows Task Manager shows Angry IP in Full Scan Mode has up to 65 Threads!	21
Figure No. 14	Windows Task Manager shows Angry IP in scan completion mode with only two threads!	21

Name	Description	Page Number
Figure No. 15	Port Range Selection Dialog Box from the Options menu	22
Figure No. 16	Angry IP allows the scan data on selected host names to be exported and saved to a text file.	23
Figure No. 17	The IP host selection data gets saved in this text format for later reuse.	24
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.	25
Figure No. 19	Angry IP can show "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.	28

### 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.

C:\Slater\00_Anti_Hacker_Tool_	Kit\Tools\AngryIP				<u>_                                    </u>
<u>File Edit View Favorites To</u>	ols <u>H</u> elp				<b>1</b>
🕒 Back 👻 🕗 🖌 🏂 🔎 Sea	rch 🔀 Folders	▶			
Address C:\Slater\00_Anti_Hacker_T	ool_Kit\Tools\AngryIP			•	🔁 Go
Folders	Name 🔺	Size	Туре	Date Modified	
Pesktop	aliases_src.zip	16 KB	WinRAR ZIP archive	7/2/2007 9:09 PM	
+ Documents	ARPMAC_column_src.zip	8 KB	WinRAR ZIP archive	7/2/2007 9:08 PM	
D 00 Anti Hacker Tool Kit	ftp_detect_src.zip	8 KB	WinRAR ZIP archive	7/2/2007 9:09 PM	
	hello_column_src.zip	7 KB	WinRAR ZIP archive	7/2/2007 9:08 PM	
	🗣 ipscan. exe	109 KB	Application	7/2/2007 9:07 PM	
	ipscan.zip	104 KB	WinRAR ZIP archive	7/2/2007 9:06 PM	
Back Oriffice	shares_src.zip	6 KB	WinRAR ZIP archive	7/2/2007 9:08 PM	
	web_detect_src.zip	8 KB	WinRAR ZIP archive	7/2/2007 9:08 PM	
Coroper's Toolkit					
	그				
8 objects			262 KB	😼 My Computer	/_

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.

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

🔄 C:\Slater\00_Anti_Hacker_Tool_Kit\Tools\AngryIP					
<u>File Edit View Favorites Too</u>	ls <u>H</u> elp				
🕞 Back 👻 🕥 🗸 🏂 🔎 Seard	h 🔀 Folders 🚯 🏂 🗙	<b>19</b>			
Address C:\Slater\00_Anti_Hacker_Too	ol_Kit\Tools\AngryIP			🔽 🔁 Go	,
Folders X	Name 🔺	Size	Type	Date Modified	_
Pagkton	Caliasses		File Folder	7/2/2007 9:46 PM	_
E My Deciments	web_detect		File Folder	7/11/2003 6:38 PM	
E C 00 Apti Hacker Tool Kit	aliases_src.zip	16 KB	WinRAR ZIP archive	7/2/2007 9:09 PM	
	ARPMAC_column.cpp	4 KB	C++ Source	11/23/2004 12:19 PM	
	ARPMAC_column.opt	48 KB	OPT File	1/31/2003 3:06 PM	
	ARPMAC_column.sln	1 KB	Microsoft Visual Stu	11/24/2004 11:43 AM	
Back Oriffice	ARPMAC_column.vcproj	4 KB	VC++ Project	11/24/2004 11:41 AM	
	ARPMAC_column_src.zip	8 KB	WinRAR ZIP archive	7/2/2007 9:08 PM	
	🖬 Defs.pas	7 KB	PAS File	11/14/2003 10:45 AM	
	FTP Detect.sln	1 KB	Microsoft Visual Stu	8/8/2004 2:17 PM	
	FTP Detect.suo	8 KB	Visual Studio Solutio	8/8/2004 2:35 PM	
	FTP Detect.vcproj	4 KB	VC++Project	8/8/2004 2:35 PM	
D1 Java Decompiler	🕶 ftp_detect.cpp	7 KB	C++ Source	8/10/2004 5:01 PM	
	ftp_detect_src.zip	8 KB	WinRAR ZIP archive	7/2/2007 9:09 PM	
C Ethereal	🖬 Funcs.pas	3 KB	PAS File	11/17/2003 2:37 PM	
	Hello_column.cpp	3 KB	C++ Source	2/19/2003 6:14 PM	
	🚰 hello_column.dsp	5 KB	VC++6 Project	1/23/2003 1:05 PM	
	hello_column.dsw	1 KB	VC++6 Workspace	1/23/2003 12:05 PM	
ETK Imager	🖬 hello_column.opt	48 KB	OPT File	1/31/2003 3:06 PM	
	hello_column_src.zip	7 KB	WinRAR ZIP archive	7/2/2007 9:08 PM	
GNU binutils	🗣 ipscan.exe	109 KB	Application	7/2/2007 9:07 PM	
GNU netcat	ipscan.zip	104 KB	WinRAR ZIP archive	7/2/2007 9:06 PM	
🔁 HexEdit	b plugin. Description: Angry IP sc	anner 6 KB	C/C++ Header	7/25/2003 12:42 PM	
D hping	ShareLi Company: Angryziber So	oftware 3 KB	PAS File	11/17/2003 2:35 PM	
	Shares File Version: 0.0.0.0	2 KB	DOF File	11/17/2003 2:55 PM	
isic	Shares Size: 108 KB	1KB	DPR File	11/17/2003 2:40 PM	
John the Ripper	shares_srcvzip	6 KB	WinRAR ZIP archive	7/2/2007 9:08 PM	
Libpst	web_detect_src.zip	8 KB	WinRAR ZIP archive	7/2/2007 9:08 PM	
📩 libwhisker					
🗖 Loki 🚽					
Description: Angry IP scanner Company: An	gryziber Software File Version: 0.0.0.0	Date Created: 7/2	/2007 9:07 108 KB	😼 My Computer	1.

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.

Angry IP Scanner 2.21		
<u>F</u> ile <u>G</u> o to <u>C</u> ommands	Favorites Options Utils Help	
IP range: 192 . 168 . 0	1 to 192 . Delete from list	
Hostname: ClaudeShannon	IP& B Show last scan ir	I ▶ Install the program Info Remove settings from registry
IP <b>® 1</b> Ping	● 1 Hostname ● 1	
Ready		

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

🚣 Angry IP Scanner 2.21
<u>File Goto Commands Favorites Options Utils Help</u>
IP range: 192 . 168 . 0 . 1 to 192 . 168 . 0 . 254 🥥 Start
Hostname: ClaudeShannon
IP oi Installation X
The list is empty. S Copy program to this location: C:\tools\Angry_IP\ Create group in Start Menu Create desktop shortcut Install Cancel
Ready

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:

🛱 Angry IP Scanner 2.21 📃 🗵
<u>File Goto Commands Favorites Options Utils H</u> elp
IPrange: 🚺 . 0 . 0 . 0 to 0 . 0 . 0 . 0 . 🥥 Start 🖕
Hostname: ClaudeShannon
IP 💿 î Ping 💿 î Hostname 💿 î
The list is empty. Set the re-range and click Start to start set
Ready

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.

🖏 Angry IP Scanner 2.21
<u>File Go to Commands Favorites Options Utils Help</u>
IP range: 192 . 168 . 0 . 1 to 192 . 168 . 0 . 254 Gestart
Hostname: ClaudeShannon
IP 💿 î Ping 💿 î Hostname 💿 î
scanning.
Ready

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.

🐥 Angry IP Scan	ner 2.21		<u> </u>	
<u>F</u> ile <u>G</u> o to <u>C</u> or	mmands <u>F</u> avorit	es <u>O</u> ptions <u>U</u> tils	ls <u>H</u> elp	
IP range: 192 .	168.0.1	to 192 . 168 .	. 0 . 254 🧉 Start 👳	
Hostname: ClaudeSl	hannon	IPt 🔂 👻	Threads 0	
IP oì	Ping 🛛 💿 🗎	Hostname 🛛 💿 🛍		
9 192.168.0.201	<b>0 ms</b> Open ports: 515	ANDREAS		
0 192.168.0.101	<b>0 ms</b> Open ports: N/A	ClaudeShannon		
0 192.168.0.17	<b>0 ms</b> Open ports: 42,139,	JULIE 162		
0 192.168.0.235	<b>0 ms</b> Open ports: 1027	WIESIEK		
0 192.168.0.1	<b>0 ms</b> Open ports: N/A	N/A		
9 192.168.0.254	Dead Open ports: N/S	N/S		
• 192.168.0.253	Dead Open ports: N/S	N/S		
• 192.168.0.252	Dead Open ports: N/S	N/S		
9 192.168.0.251	Dead Open ports: N/S	N/S		▼
Ready				

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.

Options View	Sh <u>u</u> t Down	<u>H</u> elp								
plications Processes	Performance	Networking								
Image Name	PID	User Name	CPU	CPU Time	Mem Usage	Page Faults	VM Size	Base Pri	Threads	
hpwuSchd.exe	3100	Slater	00	0:00:00	2,076 K	576	648 K	Normal	1	
HWAPI.exe	1068	SYSTEM	00	0:00:02	5,788 K	16,247	9,820 K	Normal	9	
iexplore.exe	5112	Slater	00	0:14:31	43,800 K	338,570	140,948 K	Normal	29	
iexplore.exe	6592	Slater	00	0:00:37	72,488 K	49,099	57,248 K	Normal	20	
iFrmewrk.exe	3012	Slater	00	0:00:00	12,068 K	6,632	6,068 K	Normal	4	
igfxpers.exe	2872	Slater	00	0:00:00	2,752 K	737	748 K	Normal	3	
igfxsrvc.exe	2940	Slater	00	0:00:02	3,156 K	849	1,288 K	Normal	3	
inetinfo.exe	1036	SYSTEM	00	0:00:25	7,884 K	2,182	4,088 K	Normal	14	
ipscan.exe	4500	Slater	00	0:00:16	9,132 K	5,216	4,784 K	Normal	65	
java.exe	1508	SYSTEM	00	0:00:14	49,648 K	20,002	51,496 K	Normal	32	-
jusched.exe	2964	Slater	00	0:00:00	2,336 K	633	784 K	Normal	1	
lsass.exe	1176	SYSTEM	00	0:00:07	1,576 K	39,467	4,820 K	Normal	19	
LVCOMSX.EXE	3156	Slater	00	0:00:00	4,484 K	1,285	2,420 K	Normal	9	
LVPrcSrv.exe	136	SYSTEM	00	0:00:00	2,116 K	3,975	772 K	Normal	12	
mcagent.exe	2652	Slater	00	0:00:00	2,012 K	5,350	3,784 K	Normal	4	
mcmscsvc.exe	1296	SYSTEM	00	0:00:02	2,056 K	10,984	3,584 K	Normal	8	
McNASvc.exe	1952	SYSTEM	00	0:00:19	8,724 K	129,111	4,556 K	Normal	12	
mcods.exe	240	SYSTEM	00	0:00:00	216 K	7,809	2,500 K	Normal	8	
mcpromgr.exe	364	SYSTEM	00	0:00:11	3,012 K	96,624	7,144 K	Normal	13	
mcrdsvc.exe	4108	LOCAL SERVICE	00	0:00:00	2,964 K	769	824 K	Normal	5	
Mcshield.exe	460	SYSTEM	00	0:03:05	19,676 K	675,464	28,256 K	High	31	
Show processes fro	m all users								End Pr	ocess

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

	arformance	Networking								
	entormance	Networking								
Image Name	PID	User Name	CPU	CPU Time	Mem Usage	Page Faults	VM Size	Base Pri	Threads	
hpwuSchd.exe	3100	Slater	00	0:00:00	2,076 K	576	648 K	Normal	1	
HWAPI.exe	1068	SYSTEM	00	0:00:03	5,880 K	17,072	9,908 K	Normal	8	
iexplore.exe	5112	Slater	00	0:14:44	50,040 K	341,088	139,640 K	Normal	29	
iexplore.exe	6592	Slater	00	0:00:39	6,668 K	50,884	57,112 K	Normal	21	
iFrmewrk.exe	3012	Slater	00	0:00:00	12,068 K	6,632	6,068 K	Normal	4	
igfxpers.exe	2872	Slater	00	0:00:00	2,752 K	737	748 K	Normal	3	
igfxsrvc.exe	2940	Slater	00	0:00:02	3,156 K	849	1,288 K	Normal	3	
inetinfo.exe	1036	SYSTEM	00	0:00:25	7,884 K	2,182	4,088 K	Normal	14	
ipscan.exe	4500	Slater	00	0:00:21	8,520 K	5,695	3,912 K	Normal	2	
java.exe	1508	SYSTEM	00	0:00:14	49,776 K	20,050	51,676 K	Normal	36	
jusched.exe	2964	Slater	00	0:00:00	2,336 K	633	784 K	Normal	1	
lsass.exe	1176	SYSTEM	00	0:00:07	560 K	39,895	4,788 K	Normal	18	
LVCOMSX.EXE	3156	Slater	00	0:00:00	4,484 K	1,285	2,420 K	Normal	9	
LVPrcSrv.exe	136	SYSTEM	00	0:00:00	2,116 K	3,975	772 K	Normal	12	
mcagent.exe	2652	Slater	00	0:00:00	2,012 K	5,350	3,784 K	Normal	4	
mcmscsvc.exe	1296	SYSTEM	00	0:00:02	2,056 K	10,984	3,584 K	Normal	8	
McNASvc.exe	1952	SYSTEM	00	0:00:20	8,724 K	130,531	4,556 K	Normal	12	
mcods.exe	240	SYSTEM	00	0:00:00	216 K	7,809	2,500 K	Normal	8	
mcpromgr.exe	364	SYSTEM	00	0:00:11	3,012 K	96,624	7,144 K	Normal	13	
mcrdsvc.exe	4108	LOCAL SERVICE	00	0:00:00	2,964 K	769	824 K	Normal	5	
Mcshield.exe	460	SYSTEM	00	0:03:05	19,652 K	675,867	28,256 K	High	31	
Show processes from a	all users								End Pre	ncess
									Endrit	10035

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.

😤 Angry IP S	canner 2.21		
<u>F</u> ile <u>G</u> o to	<u>C</u> ommands	<u>Favorites</u> Options Util	ls <u>H</u> elp
IP range: 19	2.168.0	🗆 . 1 🛛 to 🛛 192 . 168 .	. 0 . 254 🧉 Start
Hostname: Clau	deShannon	IP& 🔂 🖱	Threads 0
IP 🔹	🛛 🛍 Ping	💿 🕯 Hostname 🛛 🔍 🕯	<u> </u>
9192.168.0.1	0 ms	N/A	
9192.168.0.2	Dead	N/S	Select ports X
9 192.168.0.3	Dead	N/S	
9192.168.0.4	Dead	N/S	Enter ports to scan (or use helpers below)
9192.168.0.5	Dead	N/S	Ports: 1-2000
9192.168.0.6	Dead	N/S	
9192.168.0.7	Dead	N/S	Single port
9192.168.0.8	Dead	N/S	Port: Add
9 192.168.0.9	Dead	N/S	
9192.168.0.1	0 Dead	N/S	Port range
9192.168.0.1	1 Dead	N/S	From: to Add
9192.168.0.1	2 Dead	N/S	
9192.168.0.1	3 Dead	N/S	Note: please be patient when scanning ports. It may
9192.168.0.1	4 Dead	N/S	take long if you want to scan too many ports.
9192.168.0.1	5 Dead	N/S	OK Cancel
A 192 168 N 1	6 Dead	N/S	
Ready			

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.

👫 Angry IP Scan	ner 2.21		
<u>File Goto Co</u> r	mmands	Eavorites Options Utils	Help
IP range: 192 .	168.0	. 1 to 192 . 168 . I	Save As ? X
Hostname: ClaudeS	hannon	IP& 🔂 👑	Save in: 🔁 Week_09 💽 🖛 🗈 📸 🎫
IP 💿 ì	Ping	oî Hostna… ∆oî	~\$_Scan_Range_Using_Angry_IP_2007_0715txt
9192.168.0.201	0 ms	ANDREAS	IP_Scan_Range_Using_Angry_IP_2007_0715txt
9192.168.0.101	0 ms	ClaudeShannon	IT_Security_Class_HW_2_Notes.txt
9192.168.0.17	0 ms	JULIE	
9192.168.0.235	0 ms	WIESIEK	
9192.168.0.1	0 ms	NZA	
9 192.168.0.2	Dead	N/S	
9192.168.0.3	Dead	N/S	
9 192.168.0.4	Dead	N/S	
9 192.168.0.5	Dead	N/S	rile tiame. JIP_Scan_Range_Using_Angry_IP_2007_0715Save
9192.168.0.6	Dead	N/S	Save as type: Text files (* tyt)
9192.168.0.7	Dead	N/S	
9 192.168.0.8	Dead	N/S	
A 107 100 N 0	Dead	M /C	f.com/ for the latest vers
Ready			

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



### 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."

🐥 A	Angry IP Scanner 2.21						
<u>F</u> ile	<u>G</u> o to <u>C</u> o	mmands <u>F</u> avorite	s <u>O</u> ptions <u>U</u> tils <u>H</u>	elp			
IP rar	nge: 206 .	126 . 230 . 1	to 206 . 126 . 230	. 254 🧭 Start			
Hostr	name: ClaudeS	hannon	IPA 🔂 😁 😋	Threads 0			
IP		💿 讠 Ping	💿 🛍 Hostname	0ì	<u> </u>		
2	206.126.230.1	Dead	N/S				
2	206.126.230.2	Dead	N/S				
2	206.126.230.3	Dead	N/S				
2	206.126.230.4	Dead	N/S				
2	06.126.230.5	Dead	N/S				
2	206.126.230.6	Dead	N/S				
2	06.126.230.7	Dead	N/S				
2	06.126.230.8	Dead	N/S				
2	206.126.230.9	Dead	N/S				
2	206.126.230.10	Dead	N/S				
2	206.126.230.11	Dead	N/S				
2	06.126.230.12	Dead	N/S				
2	206.126.230.13	Dead	N/S				
2	206.126.230.14	Dead	N/S				
2	06.126.230.15	Dead	N/S				
2	06 126 230 16	Dead	N7S		<u> </u>		
Read	у						

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.
ТСР	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.