Network Scanner

Network Scanner User Guild

Version 1.05

Ireul Lin

Catalog

1. Introduction

Network Scanner is a program which based on linux. It provides functions to explore other hosts on the domain were working or listening which ports. You can command it with your browser.

2. Types of scan

ICMP scan

ICMP full name is “Internet Control Message Protocol”. It is a protocol to assist you finding and checking exactitude of network. Sometime you can get which hosts were existing on the network with ICMP.

SYN scan

In situation of TCP/IP, You shell receive a package of SYN/ACK if you sent a SYN to a port and the port is working. But, if it is not working, you may receive RST.

SYN/ACK scan

In situation of TCP/IP, You may receive a package of RST if you sent a SYN/ACK to a port and the port is not working. But, if it is working, the host will throw it

FIN scan

In situation of TCP/IP, You may receive a package of RST if you sent a FIN to a port and the port is not working. But, if it is working, the host will throw it

3. Language

C++98

4. Libraries

Standard Template Library (STL)

Realtime Extensions library (rt)

Pthread

5. Operating System and Compiler

Ubuntu 12.10 server 32-bit

gcc version 4.7.2

6. Compile and installation

How to compile.

Please ensure your compiler is ready.

Decompress the package, and enter “make” to compile.

How to install.

Enter “make install” after compile.

If you have some custom installation, please modify the

makefile kindly.

7. Setting file /etc/ntscan.conf

port

A connecting port of your browser.

keep_status

Weather keep information on the screen.

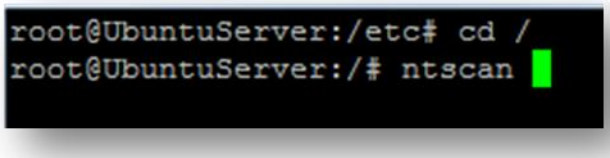
log_path

The path which log will write to.

8. User guild

How to start up

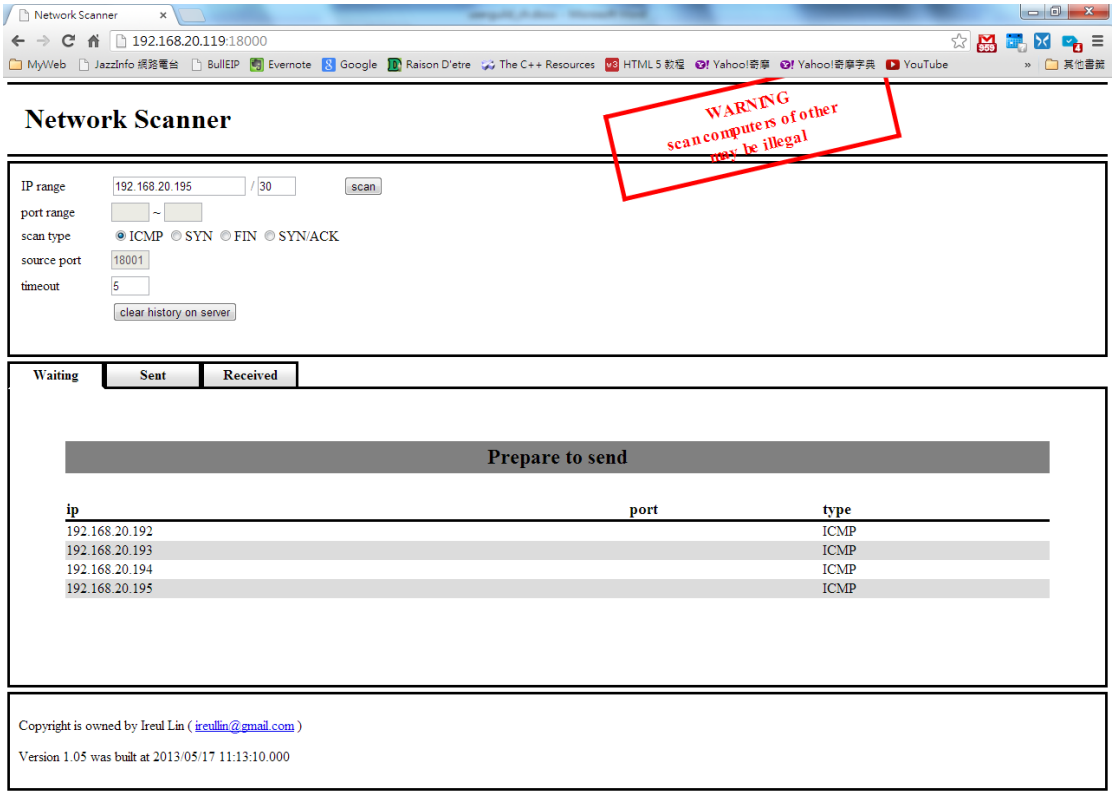
Please enter “ntscan”



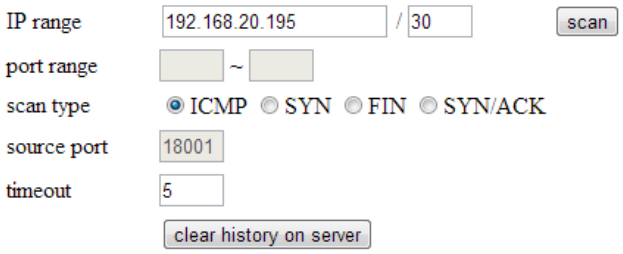
You will see this screen if the program has been started up.

Controller UI on the browser

Please connect to URL as above.



UI’s description



IP range

Enter domain and mask which you will scan.

port range

Enter ranges of port which you will scan. In ICMP situation, you don’ t need to assign them.

scan type

Chose a type you will scan.

source port

The local port which used by ntscan.

timeout

How long to determine timeout if you don’ t receive acknowledgement character.

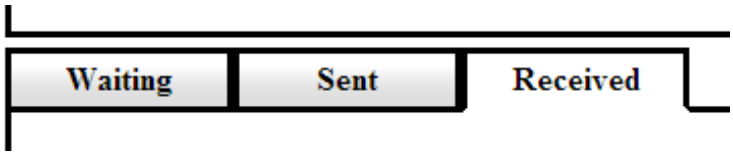
clear history on server

Clear results of scan on server.

scan

Starting scan by setting value.

Page tab description



Waiting

Server data which are waiting to scan.

Sent

The scan package which has sent without received acknowledgement character.

Received

The package which has received acknowledgement character or has determined timeout.

Description of received tab

Received list

sent time	received time	ip	port	type	status	ttl	os
2013/05/17 15:08:06.700	2013/05/17 15:08:12.203	192.168.20.193		ICMP	TIMEOUT		
2013/05/17 15:08:06.700	2013/05/17 15:08:12.203	192.168.20.192		ICMP	TIMEOUT		
2013/05/17 15:08:06.700	2013/05/17 15:08:06.702	192.168.20.194		ICMP	EXISTED	255	AIX(3.2, 4.1) BSDI(BSD/OS 3.1 and 4.) FreeBSD(3.4, 4.0) HP-UX(10.2) HP-UX(11) Irix(6.5.3, 6.5.8) Linux(2.2.14 kernel) Linux(2.4 kernel) NetBSD OpenBSD(2.6 & 2.7) OpenVMS(07.01.2002) Solaris(2.5.1, 2.6, 2.7,) Stratus(TCP_OS) SunOS(5.7) Ultrix(V4.2-4.5)
2013/05/17 15:08:06.700	2013/05/17 15:08:06.702	192.168.20.195		ICMP	EXISTED	255	AIX(3.2, 4.1) BSDI(BSD/OS 3.1 and 4.) FreeBSD(3.4, 4.0) HP-UX(10.2) HP-UX(11) Irix(6.5.3, 6.5.8) Linux(2.2.14 kernel) Linux(2.4 kernel) NetBSD OpenBSD(2.6 & 2.7) OpenVMS(07.01.2002) Solaris(2.5.1, 2.6, 2.7,) Stratus(TCP_OS) SunOS(5.7) Ultrix(V4.2-4.5)
2013/05/17 15:07:57.198	2013/05/17 15:08:03.201	192.168.20.193		ICMP	TIMEOUT		
2013/05/17 15:07:57.198	2013/05/17 15:08:03.201	192.168.20.192		ICMP	TIMEOUT		

sent time

The time which package sent

received time

The time which package received or determined timeout.

ip

IP of servers which be scanned.

port

Port of servers which be scanned.

type

Scan types, you can chose ICMP SYN SYN/ACK and FIN

status

Results of scanned, here are EXSTED(The host is existing, only for ICMP), OPENED(The port is opening, only for SYN), CLOSED(The port has be closed) and TIMEOUT(Don’ t received acknowledgement character)

ttl

TTL is which the host responsed, it may be attenuated by router.

os

Guess the OS type.