

Network Scanner

Network Scanner User Guild

Version 1.05

Ireul Lin

目錄：

一	概述.....	3
二	掃描方式.....	3
	ICMP scan.....	3
	SYN scan	3
	SYN/ACK scan	3
	FIN scan	4
三	開發語言.....	4
四	使用的函式庫.....	4
五	開發環境.....	4
六	編譯及安裝.....	5
	編譯.....	5
	安裝.....	5
	若有需要調整安裝的流程，請自行修改 makefile.....	5
七	設定檔 /etc/ntscan.conf.....	5
	port.....	5
	keep_status	5
	log_path	5
八	使用導覽.....	6
	啟動程式.....	6
	操控介面.....	6
	控制面板說明.....	7
	頁籤說明.....	8
	掃描到的主機資訊說明.....	9

一 概述

Network Scanner 是一支在 linux 上運作的程式，他提供了掃描其他網路上主機是否運作以及某些特定 port 是否開放的功能，並且藉由 http 協定可以由瀏覽器操控該程式的行為

二 掃描方式

ICMP scan

ICMP 全名為 Internet Control Message Protocol (網際網路訊息控制協定)，ICMP 基本上是一個錯誤偵測與回報的機制，通常是用來檢驗網路的連線狀態與連線的正確性，可藉由此來得知遠端的主機是否存在

SYN scan

基於 TCP/IP 的協定，對一個埠送出 SYN 封包，如果該埠是開啟的狀態下的話，會回應一個 SYN/ACK，若是關閉狀態則回應 RST

SYN/ACK scan

基於 TCP/IP 的協定，對一個埠送出 SYN/ACK 封包，如果該埠是關閉的狀態下的話，某些主機會回應一個 RST，若是開啟狀態則該封包會被丟棄不回

應

FIN scan

基於 TCP/IP 的協定，對一個埠送出 FIN 封包，如果該埠是關閉的狀態下的話，某些主機會回應一個 RST，若是開啟狀態則該封包會被丟棄不回應

三 開發語言

C++98

四 使用的函式庫

Standard Template Library (STL)

Realtime Extensions library (rt)

Pthread

五 開發環境

Ubuntu 12.10 server 32-bit

gcc version 4.7.2

六 編譯及安裝

編譯

請先確認系統是否已安裝編譯器

將安裝包解壓縮到作業系統中之後，執行 `make` 即可開始編譯

安裝

請執行 `make install`

若有需要調整安裝的流程，請自行修改 `makefile`

七 設定檔 `/etc/ntscan.conf`

`port`

程式啟動後，瀏覽器的連接埠

`keep_status`

是否持續更新系統運作狀況，或是保留歷史資料

`log_path`

Log 寫入的目錄

八 使用導覽

啟動程式

請直接輸入 ntscan

```
root@UbuntuServer:/etc# cd /  
root@UbuntuServer:/# ntscan
```

啟動完成後會看到以下畫面代表啟動完成

```
please connect to  
http://192.168.20.119:18000  
  
press ctrl-c to exit  
  
queue      sent      result    buffer  
=====
```

0	0	0	0
---	---	---	---

操控介面

請使用瀏覽器連接到上述網址即可看到操控介面

Network Scanner

192.168.20.119:18000

MyWeb JazzInfo 網路電話 BullEIP Evernote Google Raison D'etre The C++ Resources HTML5 軟體 Yahoo! 奇摩 Yahoo! 奇摩字典 YouTube 其他書籤

Network Scanner

IP range: /

port range: ~

scan type: ☒ ICMP ☐ SYN ☐ FIN ☐ SYN/ACK

source port:

timeout:

Waiting Sent Received

Prepare to send

ip	port	type
192.168.20.192		ICMP
192.168.20.193		ICMP
192.168.20.194		ICMP
192.168.20.195		ICMP

Copyright is owned by Ireul Lin (ireulin@gmail.com)

Version 1.05 was built at 2013/05/17 11:13:10.000

控制面板說明

IP range: /

port range: ~

scan type: ☒ ICMP ☐ SYN ☐ FIN ☐ SYN/ACK

source port:

timeout:

IP range

輸入要掃描的網段與遮罩

port range

輸入要掃描主機的埠範圍，ICMP 的掃描方式不需要指定

scan type

選擇要使用的掃描類型

source port

本地端 (指執行 nmap 的機器) 要使用的掃描埠

timeout

多久沒收到回應判斷為逾時

clear history on server

清除目前 nmap 上記錄的掃描結果

scan

根據控制面板上面的設定值開始進行掃描

頁籤說明



Waiting

等待掃描的主機資料

Sent

已經送出掃描封包，但還沒回應的資訊

Received

已收到回應或是判定為逾時的主機資訊

掃描到的主機資訊說明

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		
							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) Ulrix(V4.2-4.5)
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) Ulrix(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) Ulrix(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

封包送出的時間

received time

收到回應或是判斷為逾時的時間

ip

被掃描的主機 ip

port

被掃描的主機埠

type

掃描的類型，目前有 ICMP SYN SYN/ACK FIN

status

掃描的結果，分為 EXISTED (該主機存在，僅限 ICMP 掃描) · OPENED (該埠開放，僅限 SYN 掃描) · CLOSED (該埠關閉) 與 TIMEOUT (被掃描的主機沒有回應)

ttl

該台主機回應的 ttl 值，此 ttl 值有可能因為封包經過 router 而衰減

os

猜測該主機的 OS 類型