Nmap Experiment

Outline

- Introduction
- Function
- Pros & Cons
- NMAP Install
  - Install of under Windows
  - Install of under Linux
- NMAP Experiment
- Conclusions

Nmap - Network Mapper

- What is Nmap?
  - Utility for network discovery and security auditing
  - Useful for network inventory, managing service upgrade schedules, and monitoring host or service uptime
- What Nmap suite includes?
  - Zenmap
    - A advanced Graphical User Interface (GUI) and results viewer
  - Ncat
    - A flexible data transfer, redirection, and debugging tool
  - Ndiff
    - A utility for comparing scan results
  - Nping
    - A packet generation and response analysis tool

NMAP port scanning

- Know remote host executive services
- Guess remote host's Operation System & Version
- Scan subnet
  - To detect the subnet on which hosts and each of detection of its services
  - E.g. $nmap 192.168.0.1/13

Function

- Host Discovery
  - ICMP
    - Send an ICMP echo request with Nmap
  - E.g. $nmap –PE –sn 192.168.0.16
- Port Scanning
  - Status
    - open, closed, filtered, unfiltered, open|filtered and closed|filtered
  - E.g. $ time nmap -T4 -sT -p T:1-65535 192.168.0.1
- Version Detection
  - -sV flags
    - -sV: Version detection
  - E.g. $nmap -sV 192.168.5.102

Function

- OS detection
  - E.g. version scan to detect the OS:
    $nmap -sV -O -v 192.168.0.1
- Firewall/IDS(Intrusion detection system) evasion
  - E.g. Split of a probe into several smaller packets(Frames):
    $nmap -f 192.168.0.1
- Nmap Scripting Engine
  - E.g. Allows users to write (and share) simple scripts to automate a wide variety of networking tasks
    $nmap --script "not intrusive"

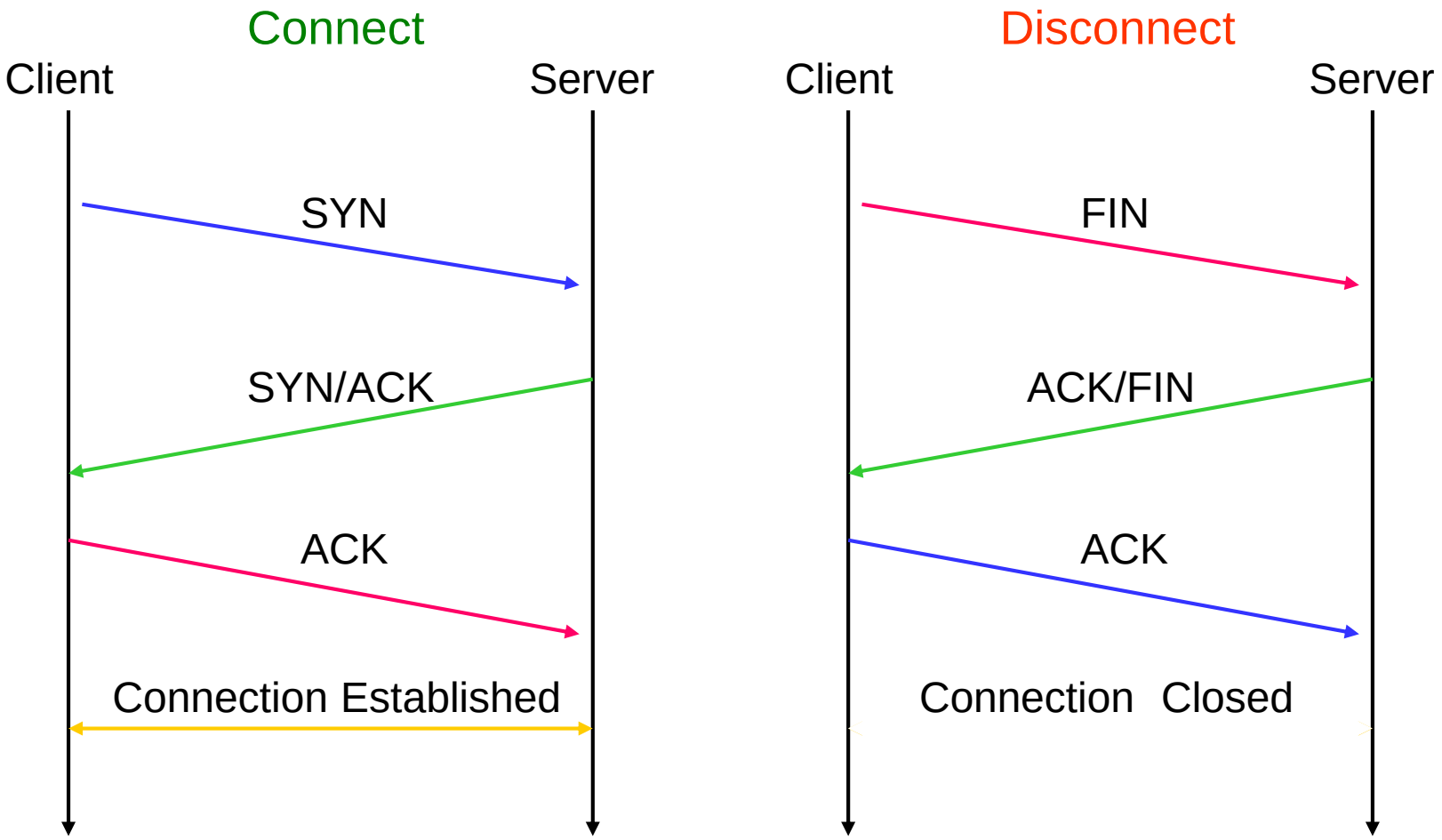
Pros & Cons

- Advantages
  - Flexible
    - Support scanning of variety protocols
    - Operate interface simply
  - Powerful
    - Scan huge networks of literally hundreds of thousands of machines
  - Portable
    - Support most of existing system
  - Easy
    - Offer powerful functions with simple instructions
  - Free
    - Offer for free
- Disadvantages
  - Obscure
    - Nmap Scripting Engine (NSE) scripts are written in lua

TCP Flag Definition

Flag	
SYN	The beginning of a connection
ACK	Acknowledge receipt of a previous packet or transmission
FIN	Close a TCP connection
RST	Abort a TCP connection

Three-way handshake



Nmap Install

Windows

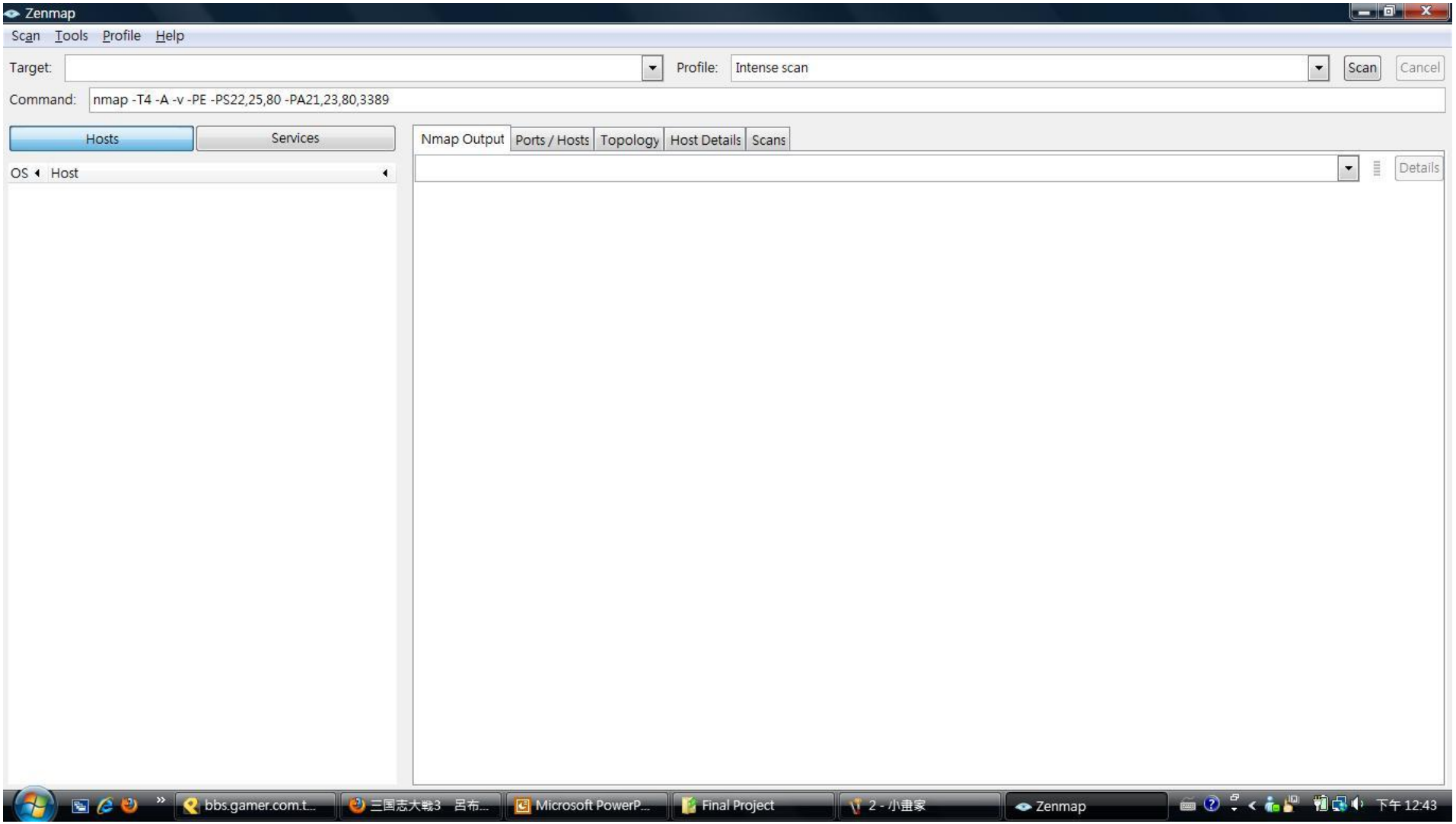
- Official website
  - http://insecure.org

Linux

- Fedora : (Root Permission) yum install Nmap

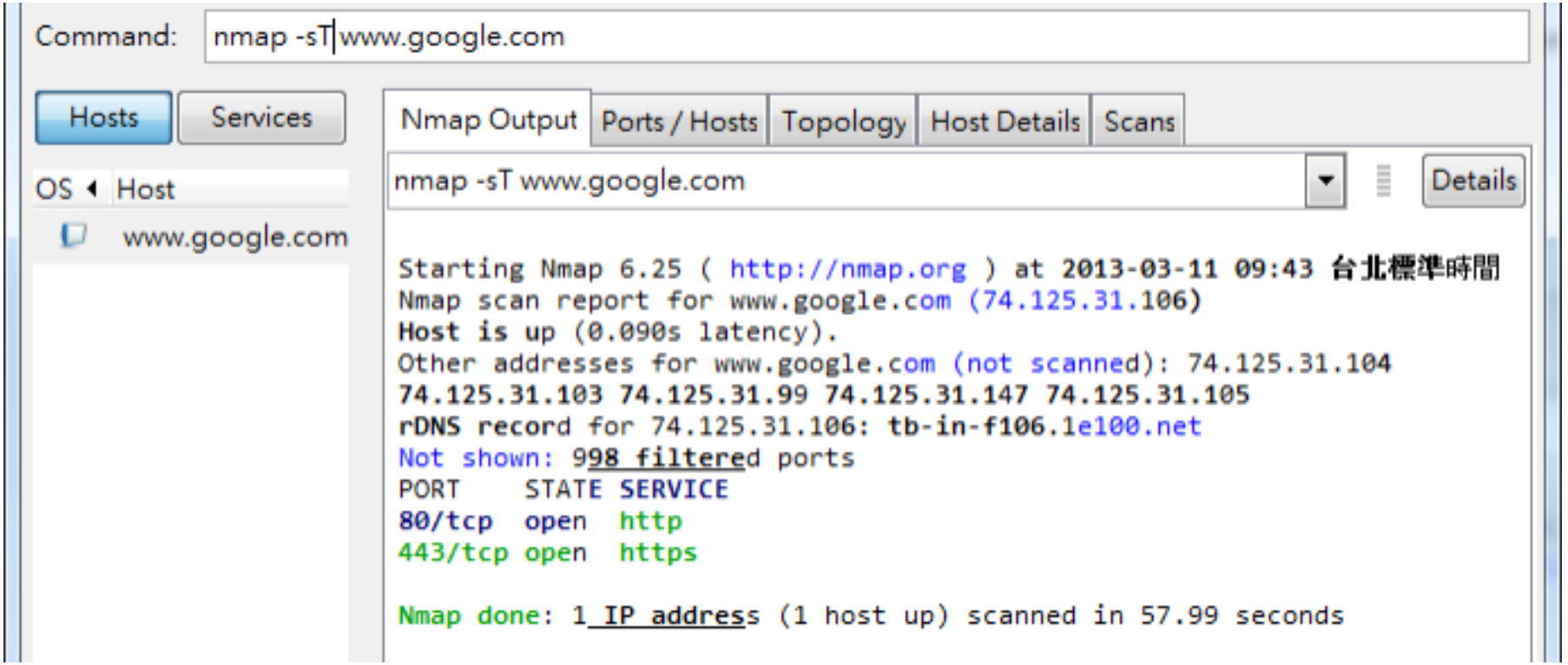
  or wget http://~~/nmap-5.00-1.i386.rpm
- Ubuntu : sudo apt-get install Nmap

Nmap


Zenmap
Scan Tools Profile Help
Target:
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
bbs.gamer.com.t...
三国志大戦3 呂布...
Microsoft PowerP...
Final Project
2 - 小畫家
Zenmap
下午 12:43

Scanning for TCP Ports

- Instruction： nmap –sT Target host



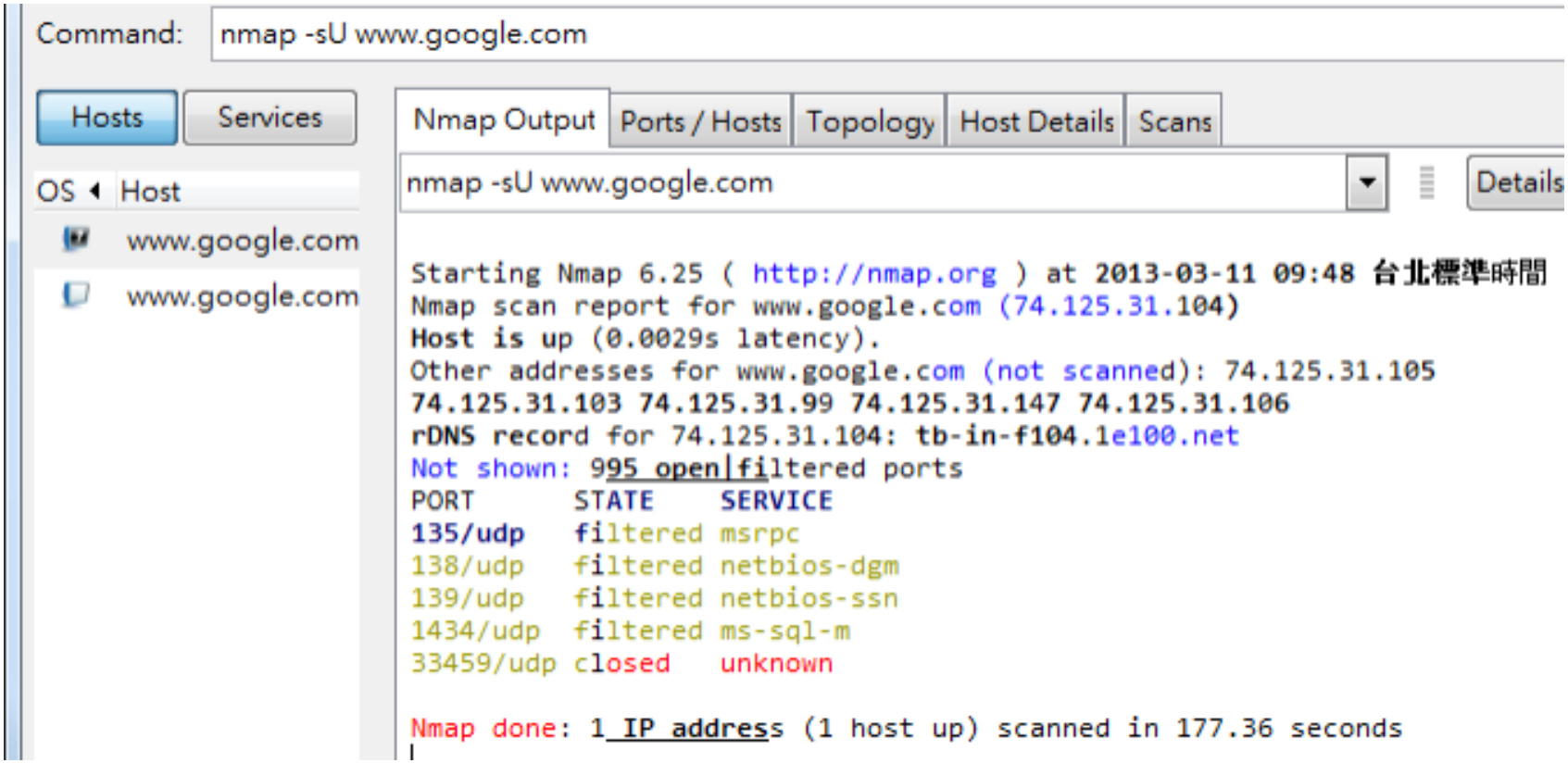
SYN Scan

Instruction : nmap –sS Target host

Nmap sends to Host Port	Nmap receives from Host Port	Nmap Assumes
SYN	SYN/ACK	**Port is open** **Host is up**
SYN	RST	**Port is closed** **Host is up**
SYN	Nothing	**Port is blocked by firewall** **Or Host is down**

Scanning UDP Port

- Instruction : nmap –sU archive.ubuntu.com

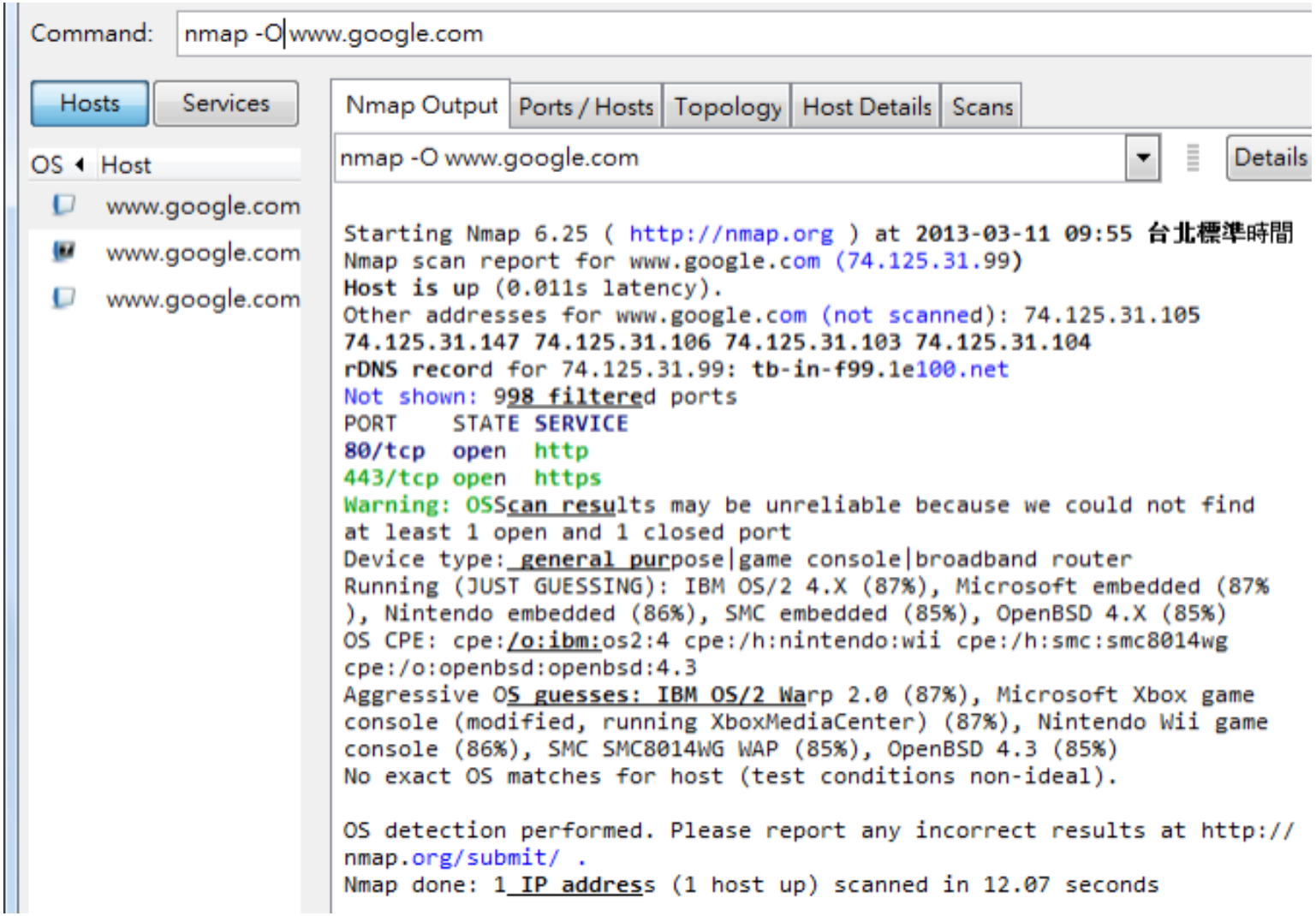


OS detection

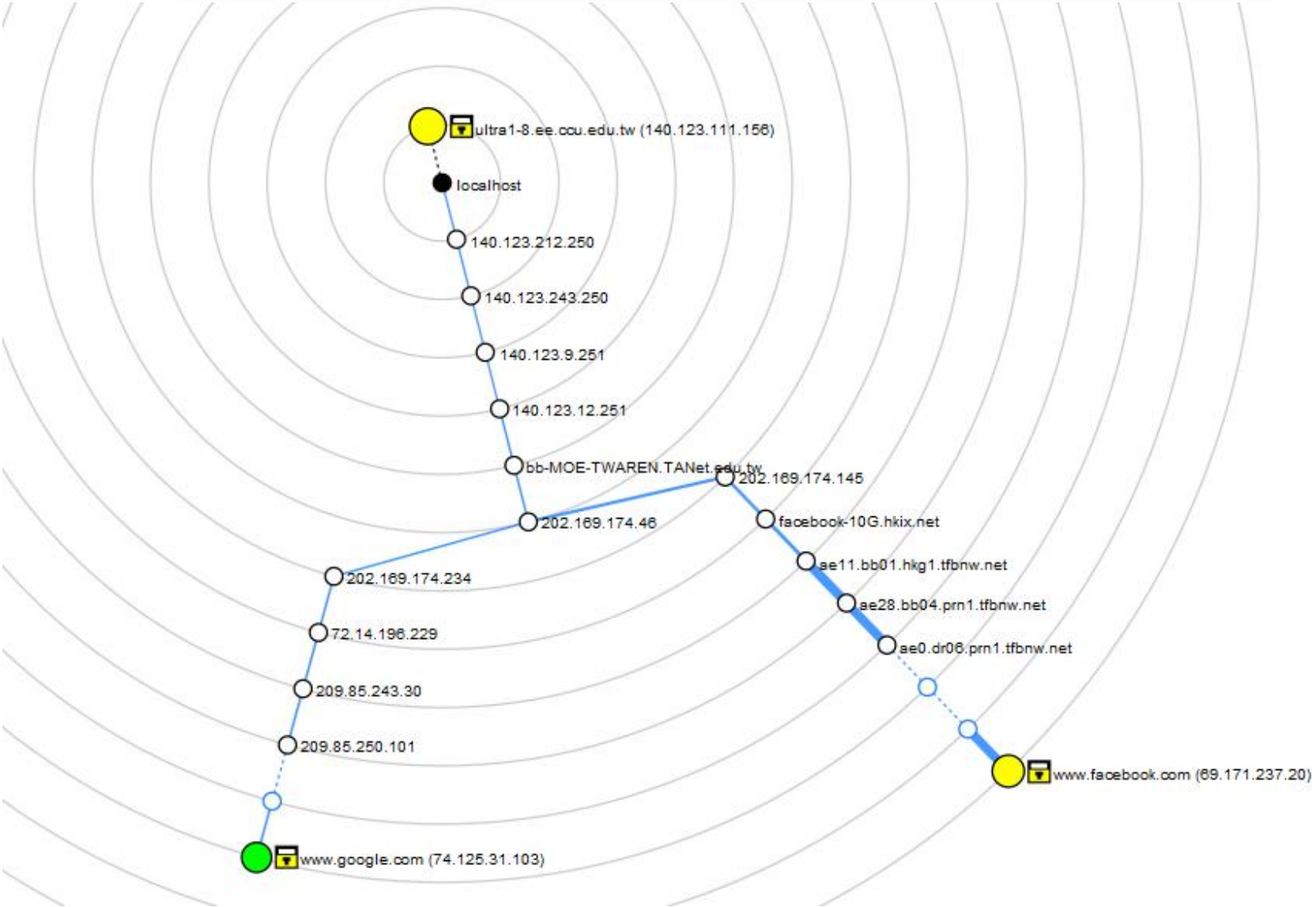
- Using TCP/IP stack fingerprinting
- Send a series of TCP and UDP packets to the remote host
- Examine practically every bit in the responses

OS detection

- Command : nmap –O Target host



Topology


ultra1-8.ee.ccu.edu.tw (140.123.111.156)
localhost
140.123.212.250
140.123.243.250
140.123.9.251
140.123.12.251
bb-MOE-TWAREN.TANet.edu.tw
202.169.174.145
202.169.174.46
facebook-10G.hkix.net
ae11.bb01.hkg1.tfbnw.net
ae28.bb04.prn1.tfbnw.net
ae0.dr06.prn1.tfbnw.net
202.169.174.234
72.14.196.229
209.85.243.30
209.85.250.101
www.facebook.com (69.171.237.20)
www.google.com (74.125.31.103)

Conclusions

- Nmap is a useful and free security detective tool

- Through Nmap provide detailed information that can understand host deeply and also avoid unexpected security vulnerabilities

- Other scanning tools
  - Netscantools
  - Superscan
  - IPEYE
  - WUPS

Exercise

- 1. Topology of
  - 140.123.111.163
  - www.facebook.com

- 2. 請找一台目標主機(自己的、同學的、虛擬機...)，並掃描有哪些port是open的?
  - 並探測作業系統與狀態為open所對應之服務。

Homework

- 1. Scan an IP address (IPv4)

  - multiple IP address

  - a range of IP address

- 2. Read list of hosts from a file
- 3. Use TCP SYN , TCP connect , UDP protocol scan
- 4. Find out if a host open firewall
- 5. Scan a network to find out which servers are up and running