

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

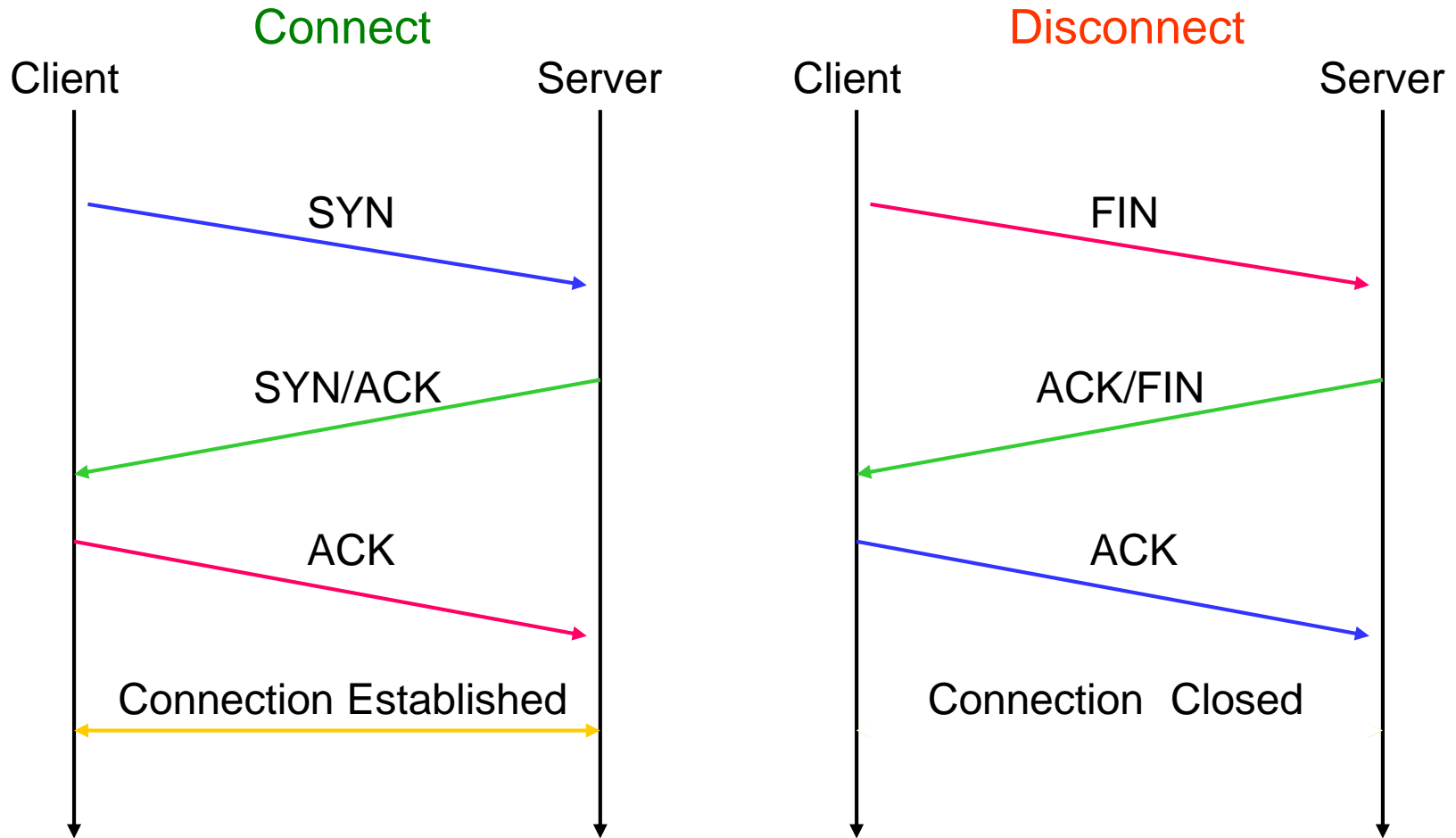
FIN

Close a TCP connection

RST

Abort a TCP connection

Three-way handshake



Nmap Install



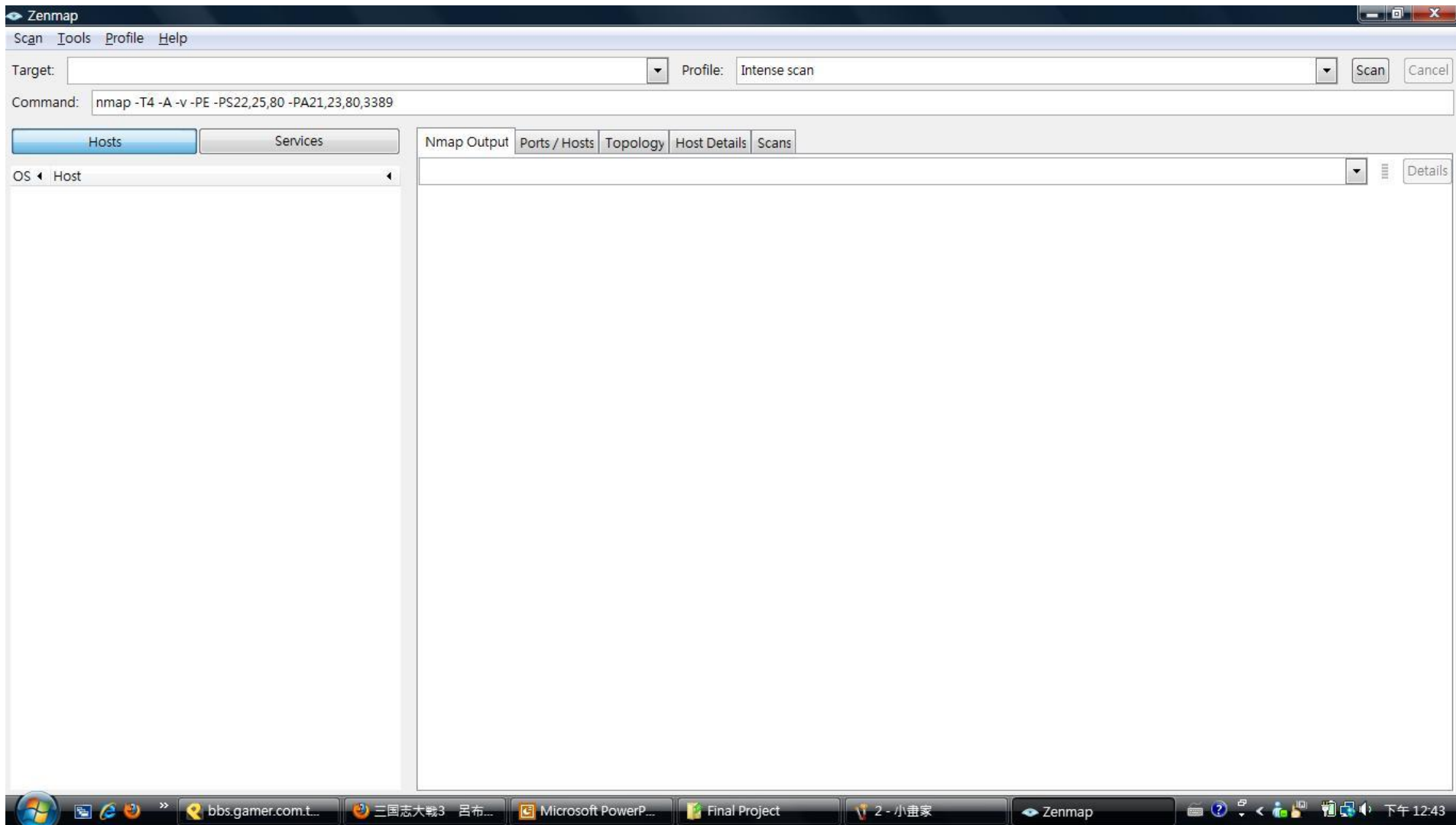
Windows

- 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



Scanning for TCP Ports

- Instruction : `nmap -sT` Target host

The screenshot shows the Nmap GUI interface. At the top, the 'Command' field contains `nmap -sT www.google.com`. Below this, there are tabs for 'Hosts' and 'Services'. The 'Hosts' tab is active, showing a list of hosts with 'www.google.com' selected. To the right, there are tabs for 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Nmap Output' tab is active, displaying the scan results for `nmap -sT www.google.com`. The output text is as follows:

```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-03-11 09:43 台北標準時間
Nmap scan report for www.google.com (74.125.31.106)
Host is up (0.090s latency).
Other addresses for www.google.com (not scanned): 74.125.31.104
74.125.31.103 74.125.31.99 74.125.31.147 74.125.31.105
rDNS record for 74.125.31.106: tb-in-f106.1e100.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 57.99 seconds
```

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 Target host`

The screenshot shows the Nmap GUI interface. At the top, the command `nmap -sU www.google.com` is entered. Below the command bar, there are tabs for 'Hosts' and 'Services'. The 'Hosts' tab is active, showing a list of hosts with `www.google.com` selected. To the right, there are tabs for 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Nmap Output' tab is active, displaying the scan results for `www.google.com`. The output text is as follows:

```
nmap -sU www.google.com

Starting Nmap 6.25 ( http://nmap.org ) at 2013-03-11 09:48 台北標準時間
Nmap scan report for www.google.com (74.125.31.104)
Host is up (0.0029s latency).
Other addresses for www.google.com (not scanned): 74.125.31.105
74.125.31.103 74.125.31.99 74.125.31.147 74.125.31.106
rDNS record for 74.125.31.104: tb-in-f104.1e100.net
Not shown: 995 open|filtered ports
PORT      STATE      SERVICE
135/udp    filtered   msrpc
138/udp    filtered   netbios-dgm
139/udp    filtered   netbios-ssn
1434/udp   filtered   ms-sql-m
33459/udp  closed     unknown

Nmap done: 1 IP address (1 host up) scanned in 177.36 seconds
```


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

- Instruction: `nmap -O` Target host

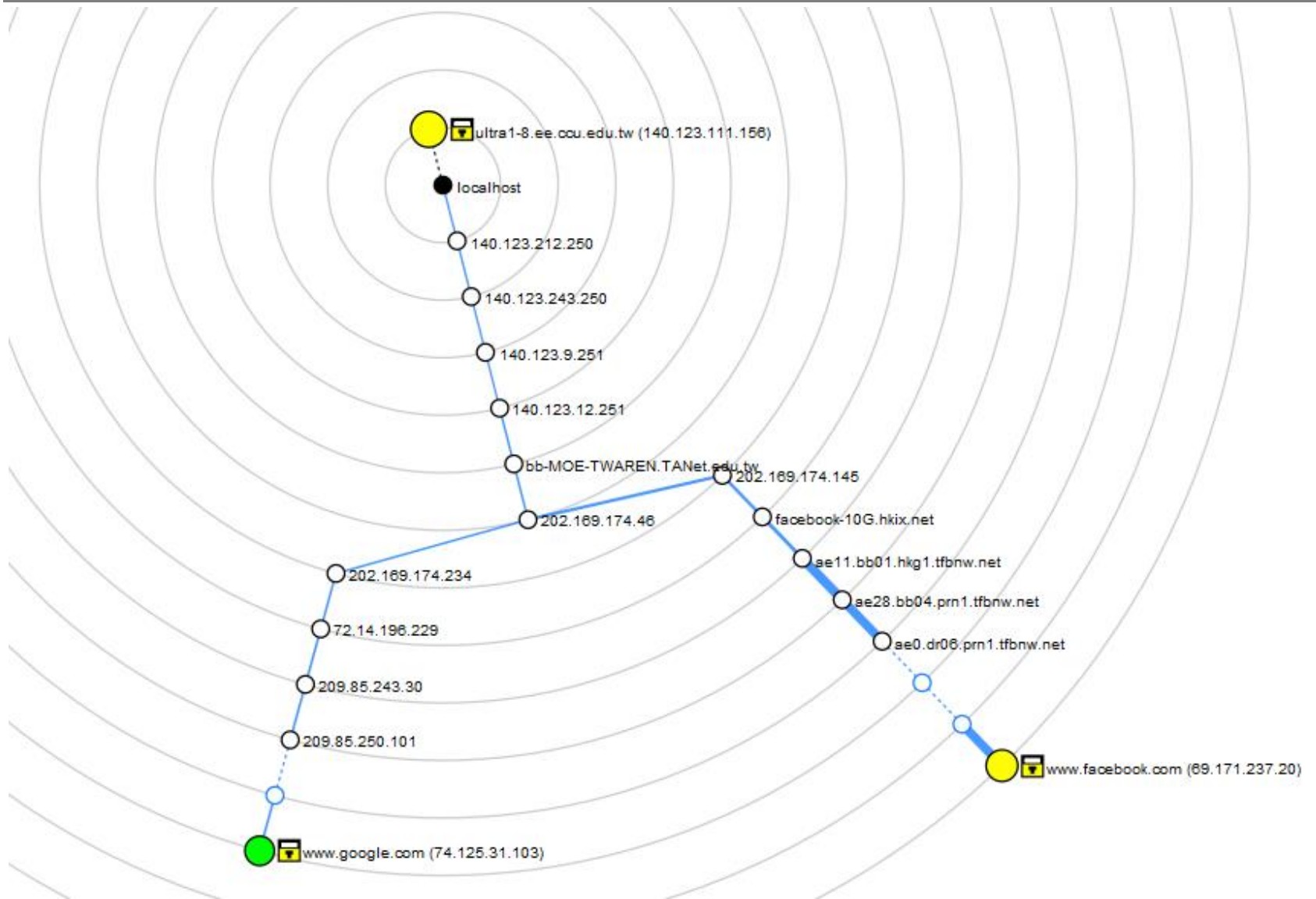
The screenshot shows the Nmap GUI interface. At the top, the command `nmap -O www.google.com` is entered. The left sidebar shows a list of hosts under the 'Hosts' tab, with `www.google.com` selected. The main panel displays the 'Nmap Output' for the selected host. The output text is as follows:

```
nmap -O www.google.com

Starting Nmap 6.25 ( http://nmap.org ) at 2013-03-11 09:55 台北標準時間
Nmap scan report for www.google.com (74.125.31.99)
Host is up (0.011s latency).
Other addresses for www.google.com (not scanned): 74.125.31.105
74.125.31.147 74.125.31.106 74.125.31.103 74.125.31.104
rDNS record for 74.125.31.99: tb-in-f99.1e100.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
Device type: general purpose|game console|broadband router
Running (JUST GUESSING): IBM OS/2 4.X (87%), Microsoft embedded (87%)
, Nintendo embedded (86%), SMC embedded (85%), OpenBSD 4.X (85%)
OS CPE: cpe:/o:ibm:os2:4 cpe:/h:nintendo:wii cpe:/h:smc:smc8014wg
cpe:/o:openbsd:openbsd:4.3
Aggressive OS guesses: IBM OS/2 Warp 2.0 (87%), Microsoft Xbox game
console (modified, running XboxMediaCenter) (87%), Nintendo Wii game
console (86%), SMC SMC8014WG WAP (85%), OpenBSD 4.3 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.07 seconds
```

Topology



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
 - Nmap
 - 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