NETWORK SECURITY PRACTICES – ATTACK AND DEFENSE

Reconnaissance

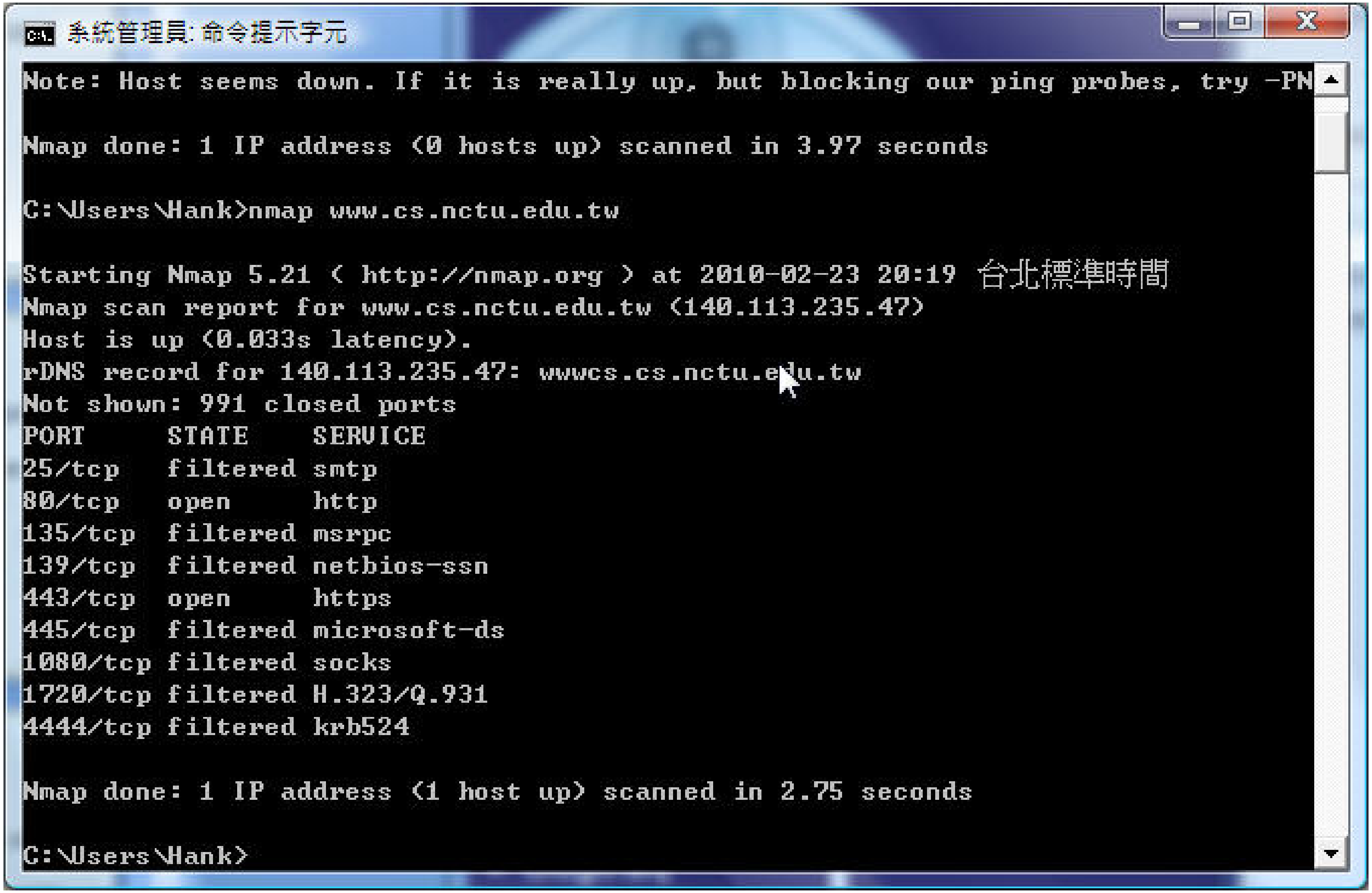
Reconnaissance

- Systematic and methodical understanding of a system’s security posture
  - Domain names, IP addresses, routers, servers,…
- Network Scanning
- Vulnerability Scanning
- LAN Reconnaissance
- Wireless Reconnaissance
- Custom Packet Generation

Network Scanning

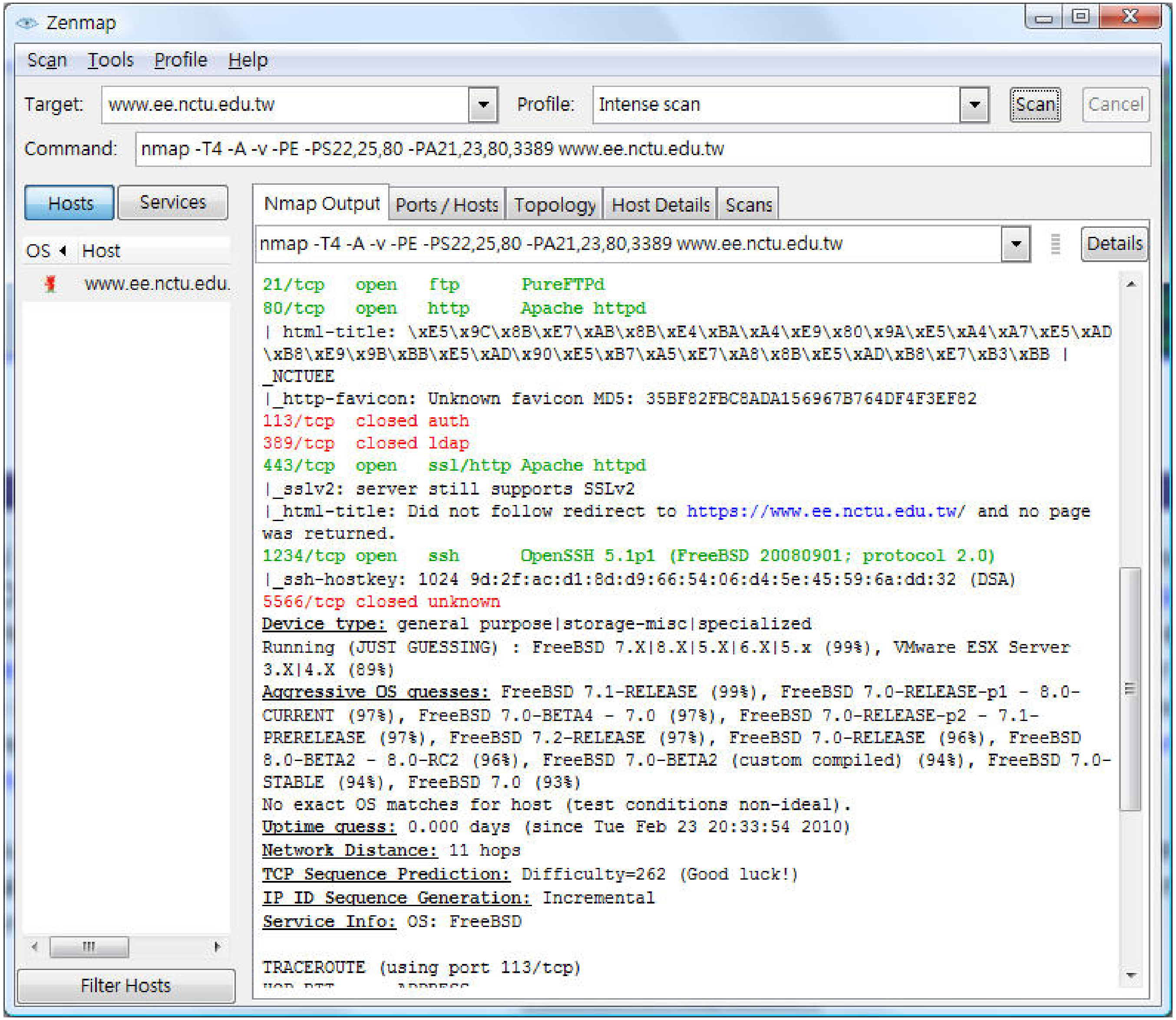
- Identify network-facing services
  - Web Server (80/443), SMTP (25), DNS (53)…
  - Tens to thousands of machines
  - Each machine has 65,536 distinct TCP or UDP ports
  - The port bindings are not fixed (use of non-standard port numbers).
  - Firewall / PortSentry can block scan
- Scanrand, Nmap, Zenmap, Unicornscan,…

Network Scanning



```
Note: Host seems down. If it is really up, but blocking our ping probes, try -PN

Nmap done: 1 IP address (0 hosts up) scanned in 3.97 seconds

C:\Users\Hank>nmap www.cs.nctu.edu.tw

Starting Nmap 5.21 ( http://nmap.org ) at 2010-02-23 20:19 台北標準時間
Nmap scan report for www.cs.nctu.edu.tw (140.113.235.47)
Host is up (0.033s latency).
rDNS record for 140.113.235.47: wwwcs.cs.nctu.edu.tw
Not shown: 991 closed ports
PORT      STATE    SERVICE
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open     https
445/tcp   filtered microsoft-ds
1080/tcp  filtered socks
1720/tcp  filtered H.323/Q.931
4444/tcp  filtered krb524

Nmap done: 1 IP address (1 host up) scanned in 2.75 seconds

C:\Users\Hank>
```

Network Scanning



Target: www.ee.nctu.edu.tw

Profile: Intense scan

Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 www.ee.nctu.edu.tw

```
nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 www.ee.nctu.edu.tw
```

```
21/tcp   open   ftp      PureFTPd
80/tcp   open   http     Apache httpd
| html-title: \xE5\x9C\x8B\xE7\xAB\x8B\xE4\xBA\xA4\xE9\x80\x9A\xE5\xA4\xA7\xE5\xAD
\xB8\xE9\x9B\xBB\xE5\xAD\x90\xE5\xB7\xA5\xE7\xA8\x8B\xE5\xAD\xB8\xE7\xB3\xBB |
_NCTUEE
|_http-favicon: Unknown favicon MD5: 35BF82FBC8ADA156967B764DF4F3EF82
113/tcp  closed auth
389/tcp  closed ldap
443/tcp  open   ssl/http Apache httpd
|_sslv2: server still supports SSLv2
|_html-title: Did not follow redirect to https://www.ee.nctu.edu.tw/ and no page
was returned.
1234/tcp open   ssh      OpenSSH 5.1p1 (FreeBSD 20080901; protocol 2.0)
|_ssh-hostkey: 1024 9d:2f:ac:d1:8d:d9:66:54:06:d4:5e:45:59:6a:dd:32 (DSA)
5566/tcp closed unknown
Device type: general purpose|storage-misc|specialized
Running (JUST GUESSING) : FreeBSD 7.X|8.X|5.X|6.X|5.x (99%), VMware ESX Server
3.X|4.X (89%)
Aggressive OS guesses: FreeBSD 7.1-RELEASE (99%), FreeBSD 7.0-RELEASE-p1 - 8.0-
CURRENT (97%), FreeBSD 7.0-BETA4 - 7.0 (97%), FreeBSD 7.0-RELEASE-p2 - 7.1-
PRERELEASE (97%), FreeBSD 7.2-RELEASE (97%), FreeBSD 7.0-RELEASE (96%), FreeBSD
8.0-BETA2 - 8.0-RC2 (96%), FreeBSD 7.0-BETA2 (custom compiled) (94%), FreeBSD 7.0-
STABLE (94%), FreeBSD 7.0 (93%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.000 days (since Tue Feb 23 20:33:54 2010)
Network Distance: 11 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: FreeBSD

TRACEROUTE (using port 113/tcp)
HOP RTT      ADDRESS
```

How Scanners Work

- TCP Scanning
  - Open a connection to a destination port
    - Successful connection => the service is present
  - Scanner sends SYN packet
    - If SYN/ACK is returned, then port is open
    - If RST is returned, then port is closed
    - If no response after timeout, the port is either filtered or the host is not up
  - Some scanners (e.g. Nmap) will attempt to communicate with the service over the established connection
    - To verify its guess or even identify the version of the service

How Scanners Work

- UDP Scanning
  - There is no three-way handshakes like TCP
    - The very first packet sent goes directly to the application (not just the TCP/IP stack)
  - UDP applications usually discard packets they can’t parse. Scanner might never see a response if the application is present.
    - Consider the port as open or filtered
  - However, if UDP is sent to a closed port, the IP stack returns ICMP port unreachable
- The inability to distinguish between open and filtered ports is a weakness of simple UDP scanners
  - Many people abandon UDP scanning entirely
  - Some scanners (e.g. Unicornscan) improves the limitation by speaking the most common UDP protocols

Superuser Privileges

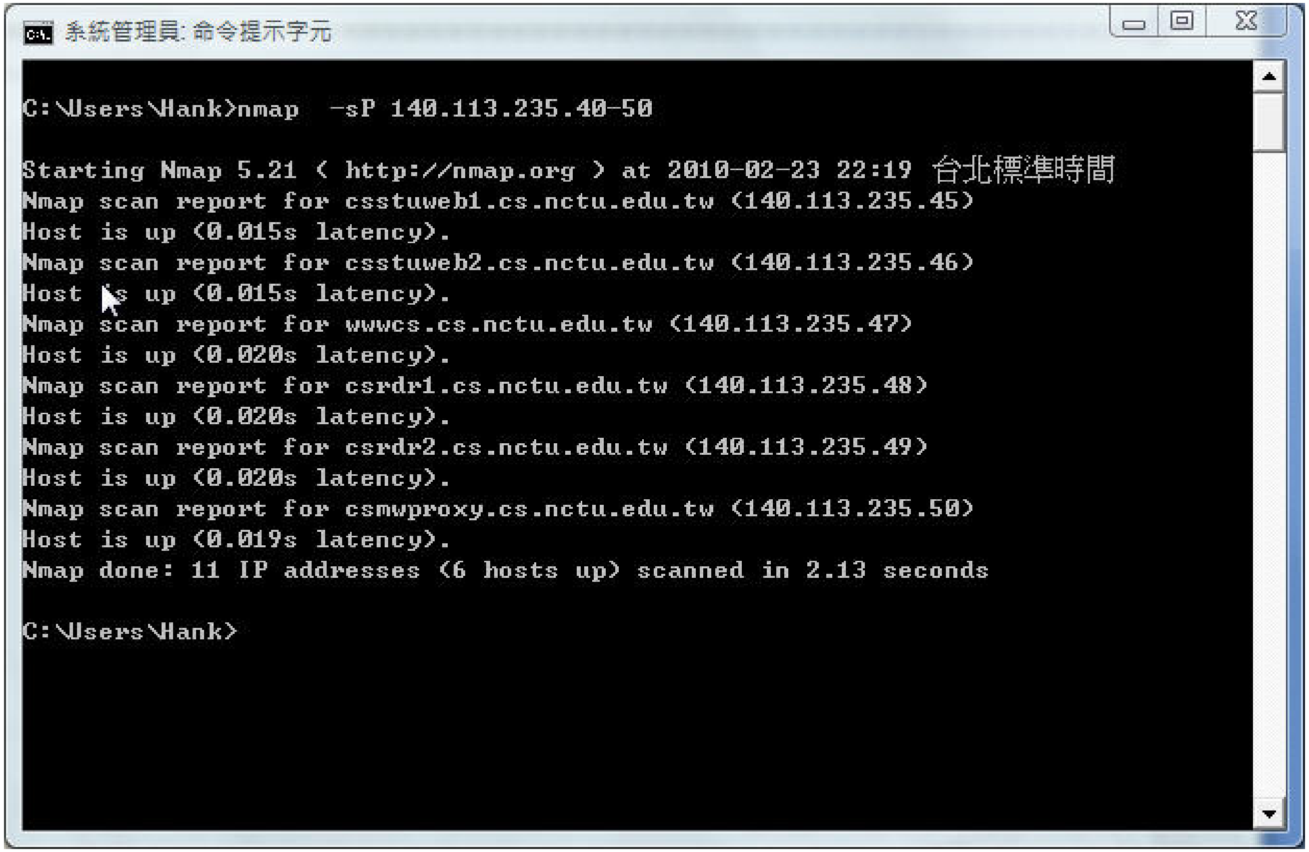
- Most scanners require root privileges on Unix-like system (e.g. Linux or Mac OS X) for their *advanced* scanning modes
  - Need to send packets with very special parameters (raw packets)
- The basic connect scan (establish a full connection) mode can be run with user privilege
- Nmap works fine on Windows with an unprivileged user account
- Why would someone limit the use of raw packets to superuser only?

Three Network Scanners to Consider

- Nmap (http://nmap.org/)
  - Oldest, most popular, and most feature-rich
- Unicornscan (http://www.unicornscan.org/)
  - Designed with speed and scalability in mind
- Scanrand (http://www.sans.org/security-resources/idfaq/scanrand.php)
  - Encoding information in the headers of TCP SYN packets
  - Very fast stateless canning of a large set of addresses and ports

Host Discovery

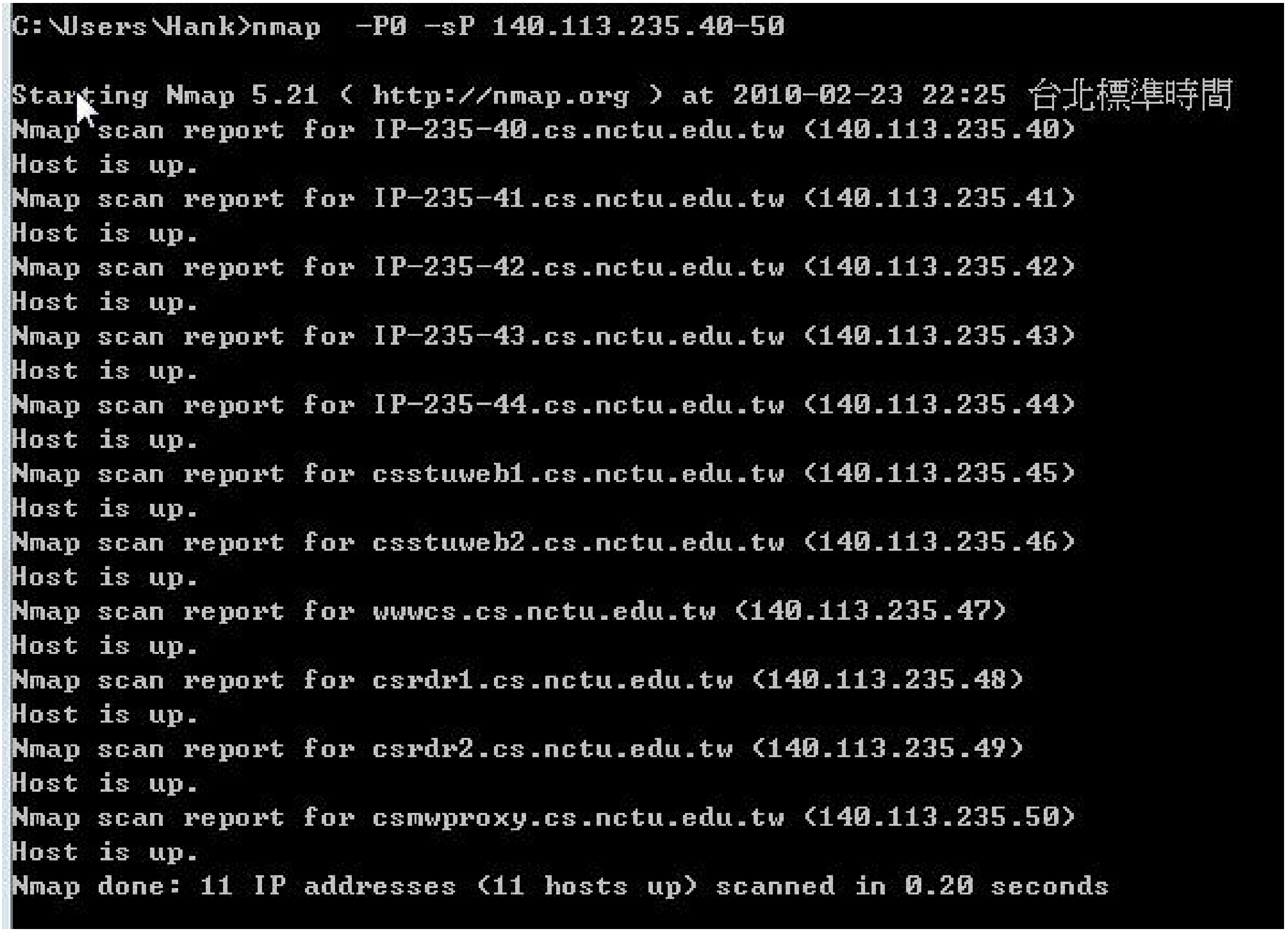
- -sP option with Nmap for host scan
  - Send ICMP echo request (ping) + TCP SYN packet to port 80



```
C:\Users\Hank>nmap  -sP 140.113.235.40-50

Starting Nmap 5.21 ( http://nmap.org ) at 2010-02-23 22:19 台北標準時間
Nmap scan report for csstuweb1.cs.nctu.edu.tw (140.113.235.45)
Host is up (0.015s latency).
Nmap scan report for csstuweb2.cs.nctu.edu.tw (140.113.235.46)
Host is up (0.015s latency).
Nmap scan report for wwwcs.cs.nctu.edu.tw (140.113.235.47)
Host is up (0.020s latency).
Nmap scan report for csrdr1.cs.nctu.edu.tw (140.113.235.48)
Host is up (0.020s latency).
Nmap scan report for csrdr2.cs.nctu.edu.tw (140.113.235.49)
Host is up (0.020s latency).
Nmap scan report for csmwproxy.cs.nctu.edu.tw (140.113.235.50)
Host is up (0.019s latency).
Nmap done: 11 IP addresses (6 hosts up) scanned in 2.13 seconds

C:\Users\Hank>
```

Host Discovery

- -P0 option to connect to every port even if the host seems down (ICMP echo + TCP SYN on port 80)



```
C:\Users\Hank>nmap  -P0 -sP 140.113.235.40-50

Starting Nmap 5.21 ( http://nmap.org ) at 2010-02-23 22:25 台北標準時間
Nmap scan report for IP-235-40.cs.nctu.edu.tw (140.113.235.40)
Host is up.
Nmap scan report for IP-235-41.cs.nctu.edu.tw (140.113.235.41)
Host is up.
Nmap scan report for IP-235-42.cs.nctu.edu.tw (140.113.235.42)
Host is up.
Nmap scan report for IP-235-43.cs.nctu.edu.tw (140.113.235.43)
Host is up.
Nmap scan report for IP-235-44.cs.nctu.edu.tw (140.113.235.44)
Host is up.
Nmap scan report for csstuweb1.cs.nctu.edu.tw (140.113.235.45)
Host is up.
Nmap scan report for csstuweb2.cs.nctu.edu.tw (140.113.235.46)
Host is up.
Nmap scan report for wwwcs.cs.nctu.edu.tw (140.113.235.47)
Host is up.
Nmap scan report for csrdr1.cs.nctu.edu.tw (140.113.235.48)
Host is up.
Nmap scan report for csrdr2.cs.nctu.edu.tw (140.113.235.49)
Host is up.
Nmap scan report for csmwproxy.cs.nctu.edu.tw (140.113.235.50)
Host is up.
Nmap done: 11 IP addresses (11 hosts up) scanned in 0.20 seconds
```

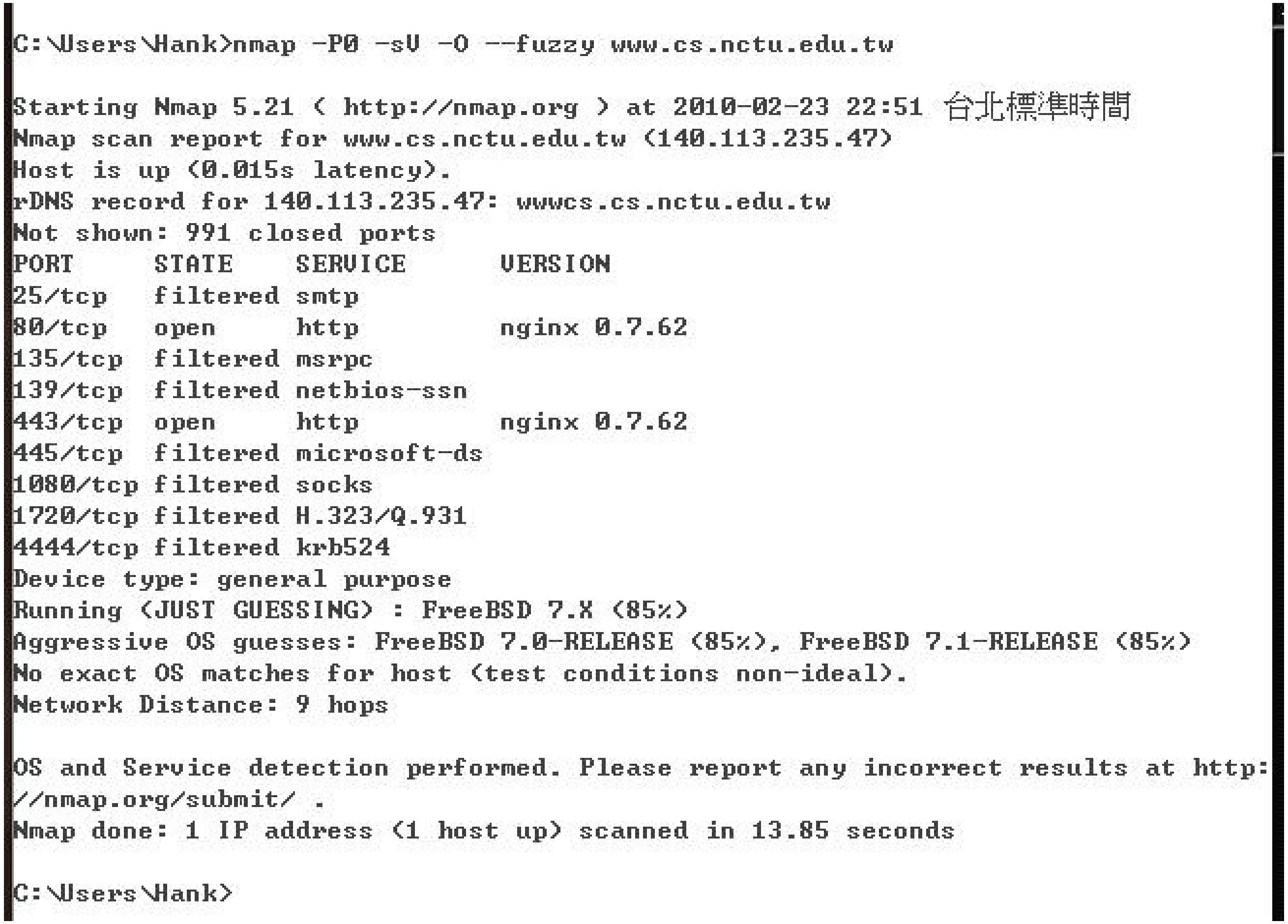
Different Scan Types

- UDP Scan
  - nmap –sU *target*
- TCP Scan
  - nmap –scanflags SYNRST *target*

Nmap: Application Fingerprinting and OS Detection

- Nmap can probe the application types / versions
  - Applications have different footprints (replies, banners, …)
  - http://nmap.org/book/vscan-technique.html
- Contribute footprints
  - http://nmap.org/book/vscan-community.html

Nmap: Application Fingerprinting and OS Detection



```
C:\Users\Hank>nmap -P0 -sV -O --fuzzy www.cs.nctu.edu.tw

Starting Nmap 5.21 ( http://nmap.org ) at 2010-02-23 22:51 台北標準時間
Nmap scan report for www.cs.nctu.edu.tw (140.113.235.47)
Host is up (0.015s latency).
rDNS record for 140.113.235.47: wwwcs.cs.nctu.edu.tw
Not shown: 991 closed ports
PORT     STATE    SERVICE      VERSION
25/tcp   filtered smtp
80/tcp   open     http         nginx 0.7.62
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
443/tcp  open     http         nginx 0.7.62
445/tcp  filtered microsoft-ds
1080/tcp filtered socks
1720/tcp filtered H.323/Q.931
4444/tcp filtered krb524
Device type: general purpose
Running (JUST GUESSING) : FreeBSD 7.X (85%)
Aggressive OS guesses: FreeBSD 7.0-RELEASE (85%), FreeBSD 7.1-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 9 hops

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.85 seconds

C:\Users\Hank>
```

Scanning can still do harm

- Fast scans can exhaust the resource on stateful network devices
  - E.g. firewalls and NATing routers
  - Nmap –t5 option
- Most IDS/IPS detect scanning
- Top 30 Nmap command examples
  - http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/