NMAP

Ms. SMITA BANSOD
Asst. Prof., SAKEC

Contents

- Nmap Introduction
- How it works
- Basic Nmap Scan
- Scanning for Host & Port
- OS Detection
- Mapping Networks

NMAP Introduction

Original author(s)	Gordon Lyon
Initial release	September 1997
Repository	github.com/nmap/nmap
Development status	Active
Written in	C, C++, Python, Lua
Operating system	Cross-platform
Available in	English
Type	computer security, network management
License	GPL v2
Website	nmap.org

Features

- Host discovery
- Port scan
- Version detection
- OS detection
- Scriptable interaction with the target

Uses of NMAP

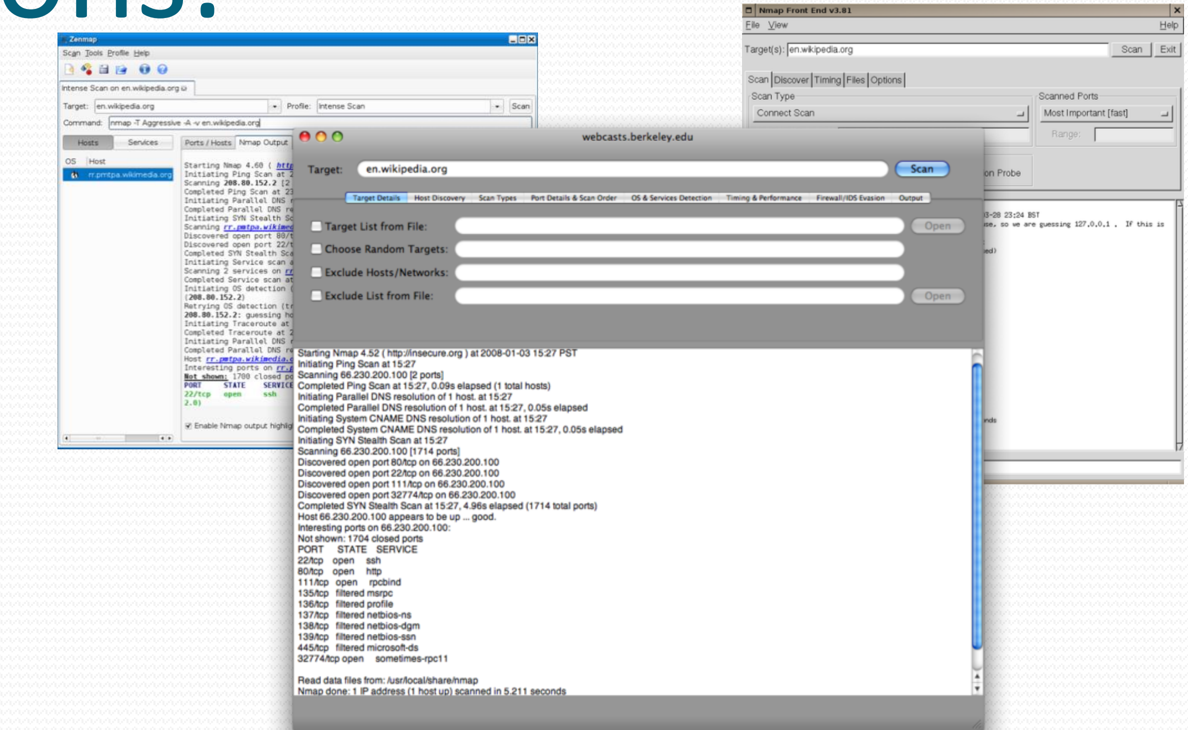
- Identifying open ports
- Network Mapping
- Auditing security

Tool Environment

- Runs on Linux, Windows, Mac OS X and other smaller operating systems

GUI options:

- Zenmap
- XNMap
- NmapFE



Target: en.wikipedia.org

Profile: Intense Scan

Command: nmap -T Aggressive -A -v en.wikipedia.org

Target(s): en.wikipedia.org

Scan Type: Connect Scan

Scanned Ports: Most Important [fast]

Target: en.wikipedia.org

```
Starting Nmap 4.52 ( http://insecure.org ) at 2008-01-03 15:27 PST
Initiating Ping Scan at 15:27
Scanning 66.230.200.100 [2 ports]
Completed Ping Scan at 15:27, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:27
Completed Parallel DNS resolution of 1 host. at 15:27, 0.05s elapsed
Initiating System CNAME DNS resolution of 1 host. at 15:27
Completed System CNAME DNS resolution of 1 host. at 15:27, 0.05s elapsed
Initiating SYN Stealth Scan at 15:27
Scanning 66.230.200.100 [1714 ports]
Discovered open port 80/tcp on 66.230.200.100
Discovered open port 22/tcp on 66.230.200.100
Discovered open port 111/tcp on 66.230.200.100
Discovered open port 32774/tcp on 66.230.200.100
Completed SYN Stealth Scan at 15:27, 4.96s elapsed (1714 total ports)
Host 66.230.200.100 appears to be up ... good.
Interesting ports on 66.230.200.100:
Not shown: 1704 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
111/tcp   open     rpcbind
135/tcp   filtered msrpc
136/tcp   filtered profile
137/tcp   filtered netbios-ns
138/tcp   filtered netbios-dgm
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
32774/tcp open     sometimes-rpc11

Read data files from: /usr/local/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.211 seconds
```

How It Works

- DNS lookup- matches name with IP
- NMap pings the remote target with 0 byte packets to each port
- Sends different packets with different timing to determine status, version, etc.

* Firewalls can interfere with this process

Basic NMAP scans

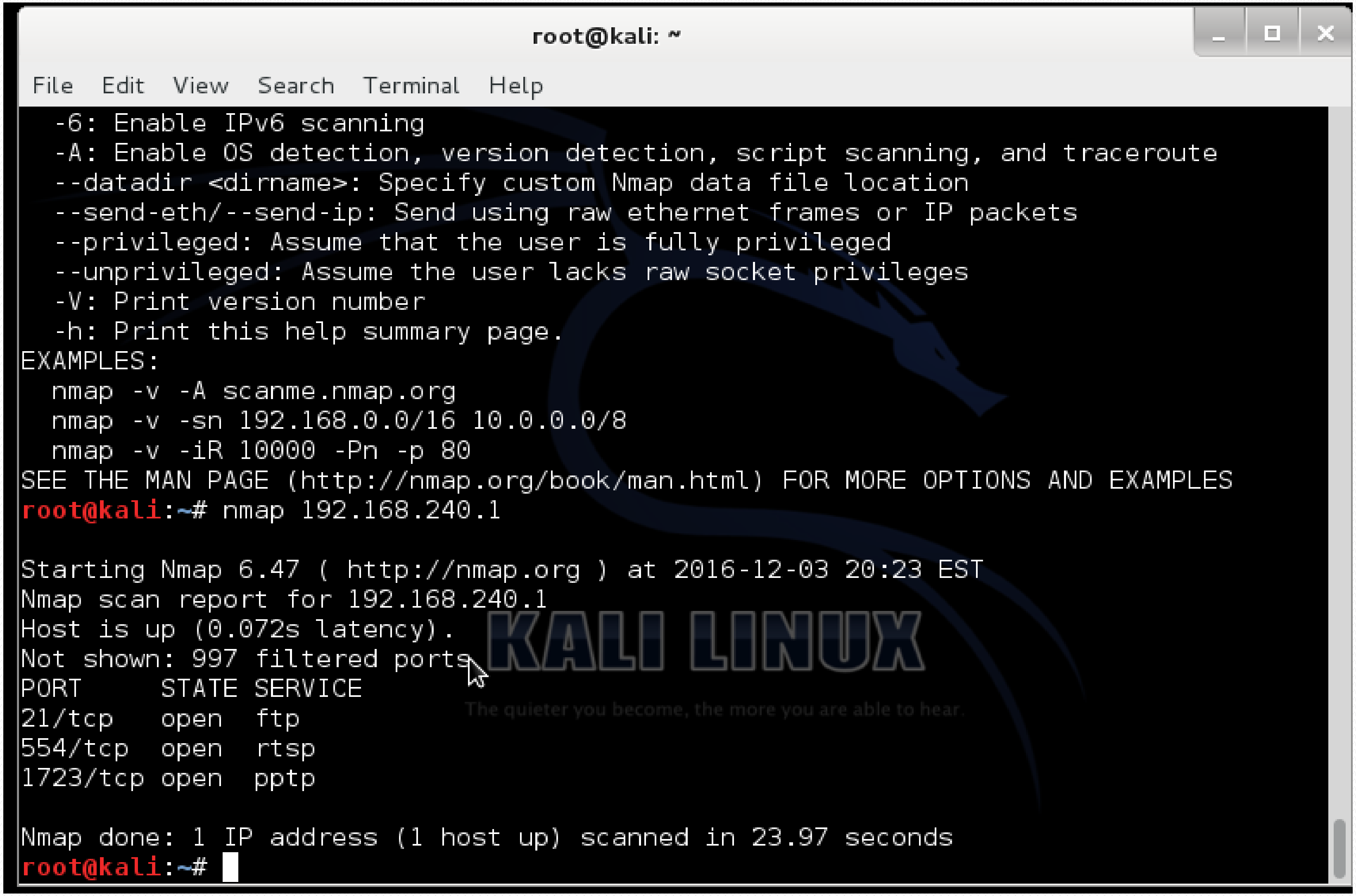
- When run through command prompt or terminal, entry fields are:
  - Program
  - Constraints on run
  - Target

  Syntax:

  >nmap [scan type(s)][Option] {Target Specification}

- Ex.   > nmap –sS scanme.nmap.org

Output from NMAP



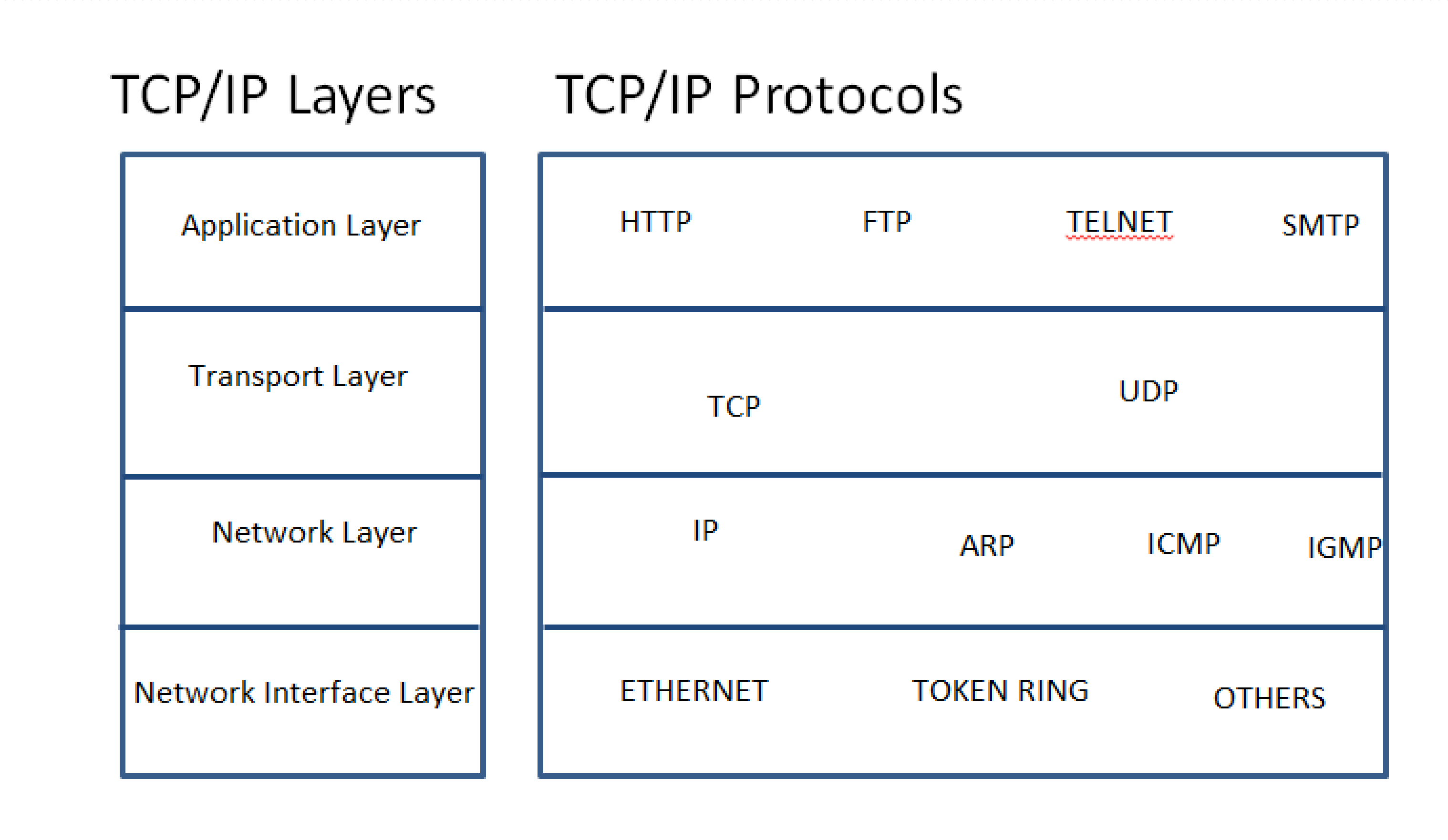
```
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap 192.168.240.1

Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-03 20:23 EST
Nmap scan report for 192.168.240.1
Host is up (0.072s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
554/tcp  open  rtsp
1723/tcp open  pptp

Nmap done: 1 IP address (1 host up) scanned in 23.97 seconds
root@kali:~#
```

Ethical Issues

- Can be used for hacking- to discover vulnerable ports
- System admin can use it to check that system meets security standards
- Unauthorized use of Nmap on a system could be illegal. Make sure you have permission before using this tool.

Basic Concepts

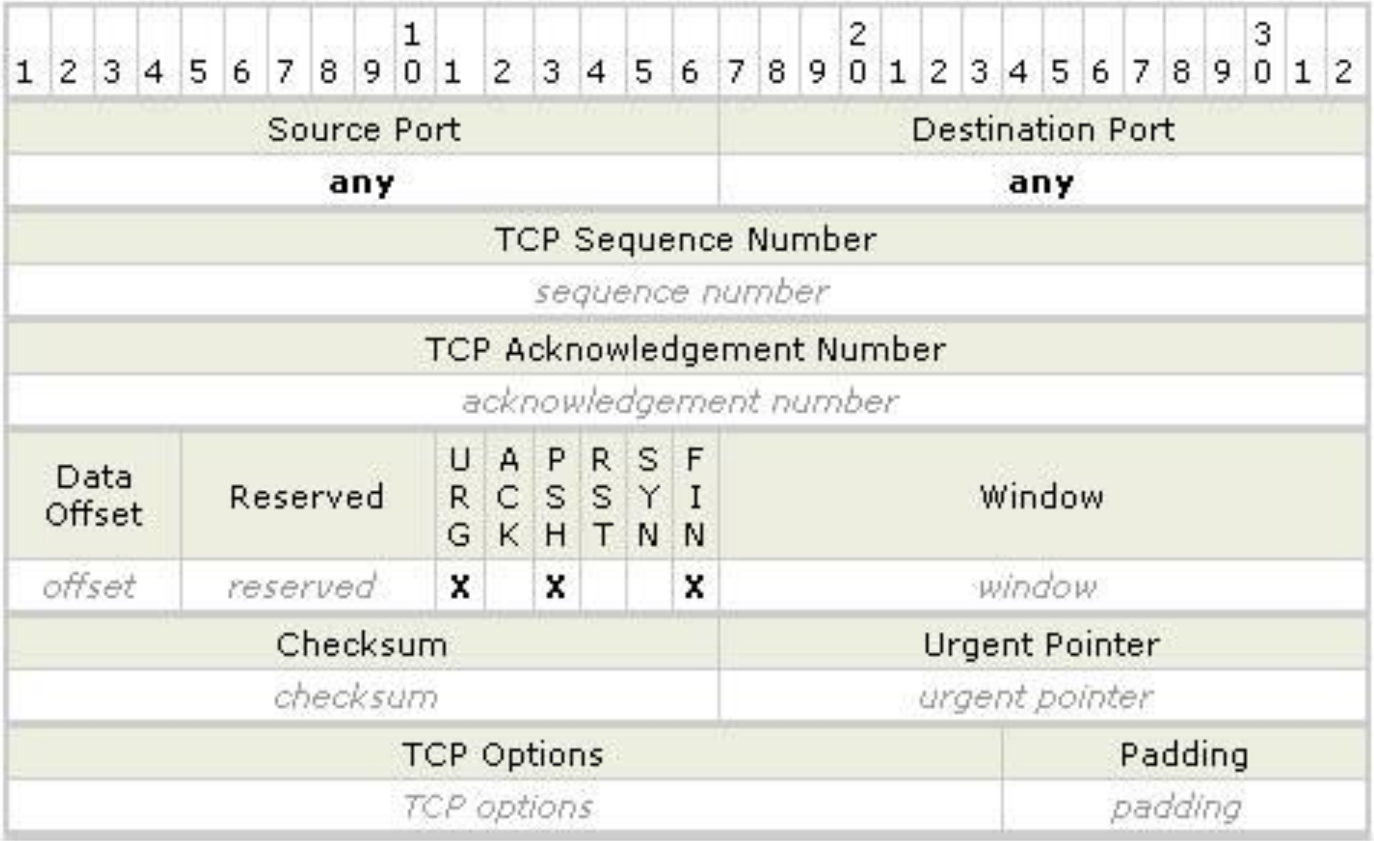
- Layered Architecture



TCP/IP Layers	TCP/IP Protocols			
Application Layer	HTTP	FTP	TELNET	SMTP
Transport Layer	TCP	UDP		
Network Layer	IP	ARP	ICMP	IGMP
Network Interface Layer	ETHERNET	TOKEN RING	OTHERS	

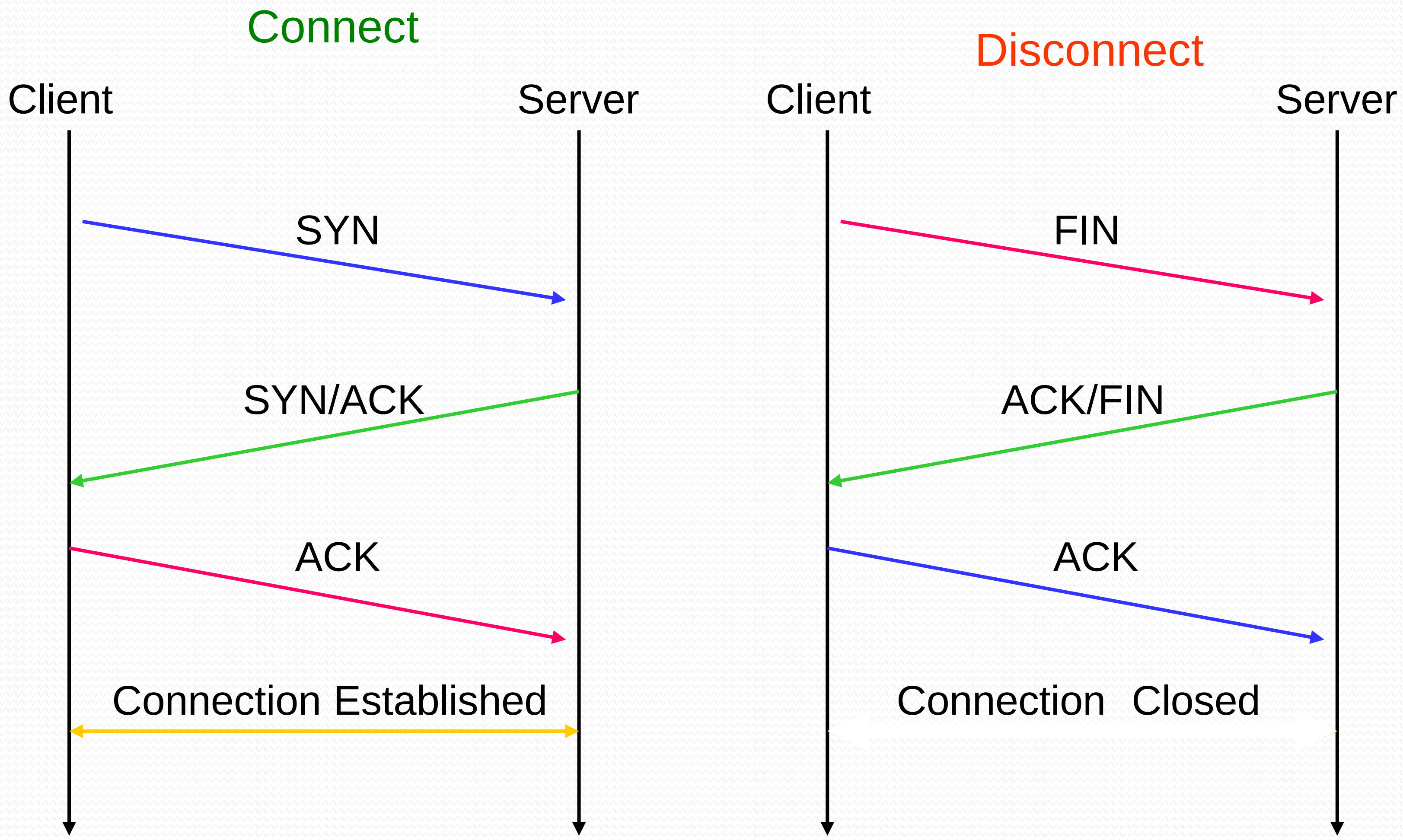
Basic Concepts…

- TCP Packet Header



<table>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>3</td><td></td><td></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td></tr>
<tr><td colspan="16">Source Port</td><td colspan="16">Destination Port</td></tr>
<tr><td colspan="16">**any**</td><td colspan="16">**any**</td></tr>
<tr><td colspan="32">TCP Sequence Number</td></tr>
<tr><td colspan="32">*sequence number*</td></tr>
<tr><td colspan="32">TCP Acknowledgement Number</td></tr>
<tr><td colspan="32">*acknowledgement number*</td></tr>
<tr><td colspan="4">Data Offset</td><td colspan="6">Reserved</td><td>U
R
G</td><td>A
C
K</td><td>P
S
H</td><td>R
S
T</td><td>S
Y
N</td><td>F
I
N</td><td colspan="16">Window</td></tr>
<tr><td colspan="4">*offset*</td><td colspan="6">*reserved*</td><td>**X**</td><td></td><td>**X**</td><td></td><td></td><td>**X**</td><td colspan="16">*window*</td></tr>
<tr><td colspan="16">Checksum</td><td colspan="16">Urgent Pointer</td></tr>
<tr><td colspan="16">*checksum*</td><td colspan="16">*urgent pointer*</td></tr>
<tr><td colspan="23">TCP Options</td><td colspan="9">Padding</td></tr>
<tr><td colspan="23">*TCP options*</td><td colspan="9">*padding*</td></tr>
</table>

TCP conversation



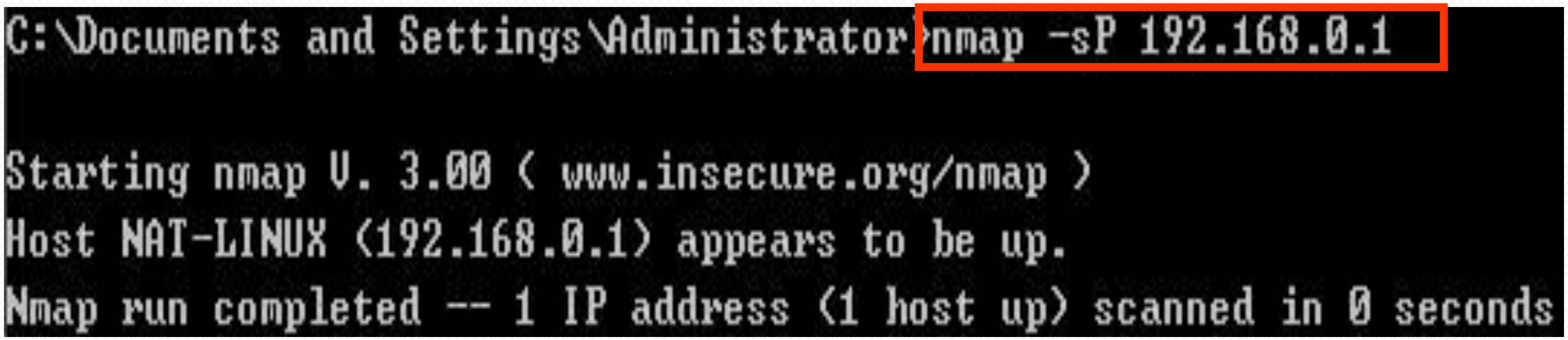
Three-way handshake

TCP Flag Definitions

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

Scanning for Hosts

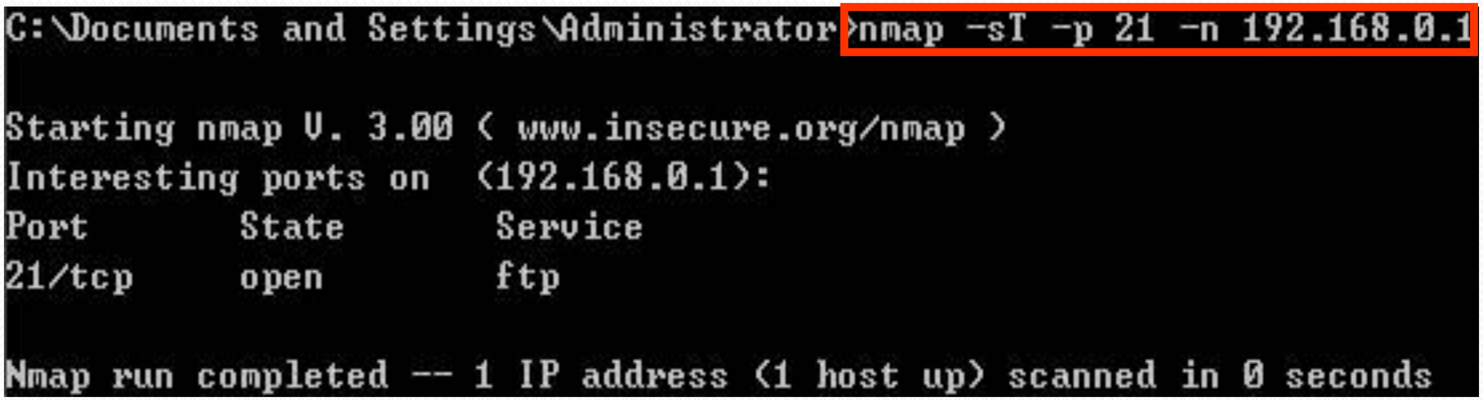
- Is the host alive ?
  - Ping Scan (Ping Sweep)
    - nmap –sP 192.168.0.1



```
C:\Documents and Settings\Administrator>nmap -sP 192.168.0.1

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host NAT-LINUX (192.168.0.1) appears to be up.
Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
```

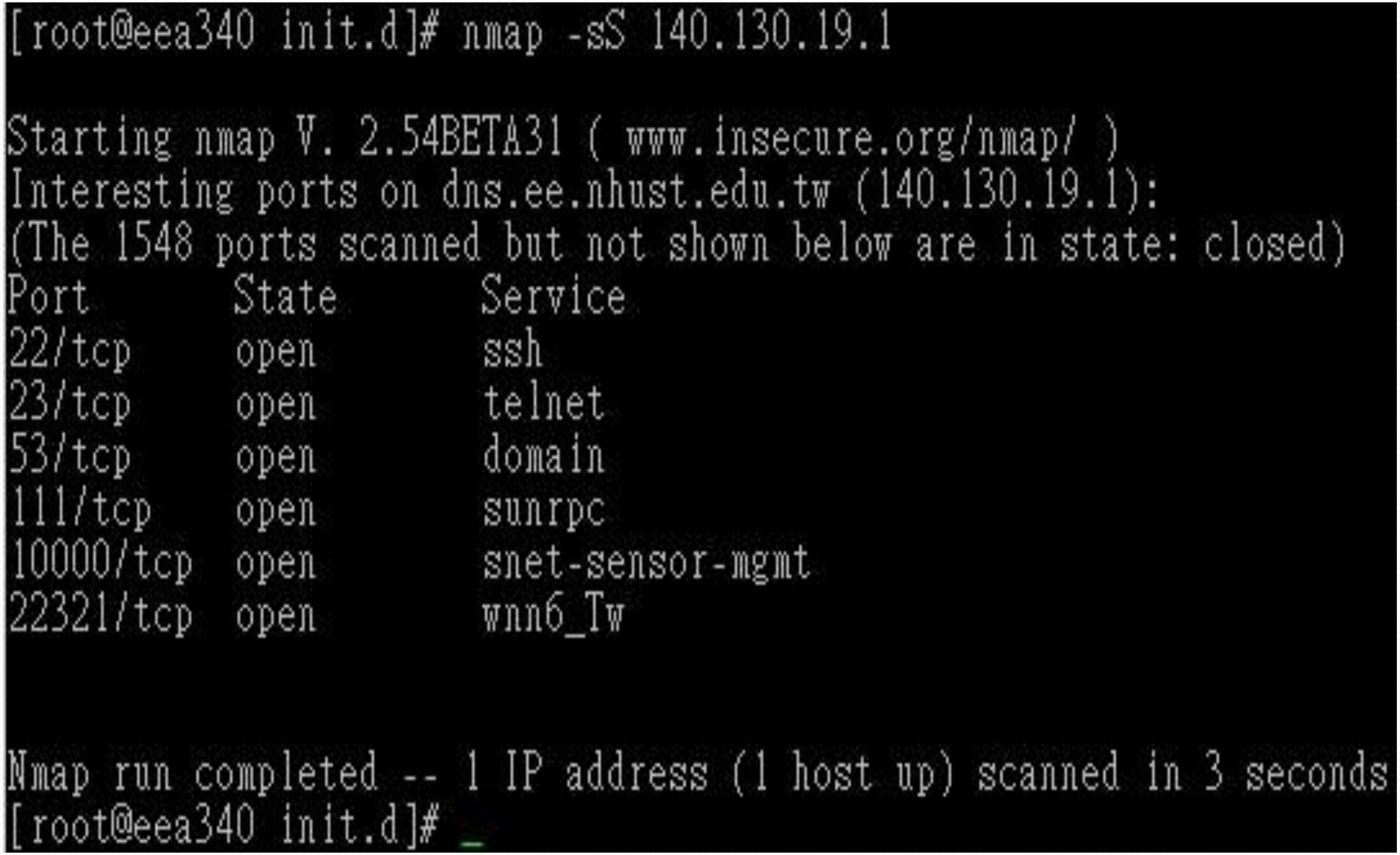
Scanning for TCP Ports

- TCP connect
  - nmap –sT 192.168.0.1



```
C:\Documents and Settings\Administrator>nmap -sT -p 21 -n 192.168.0.1

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on  (192.168.0.1):
Port        State       Service
21/tcp      open        ftp

Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
```

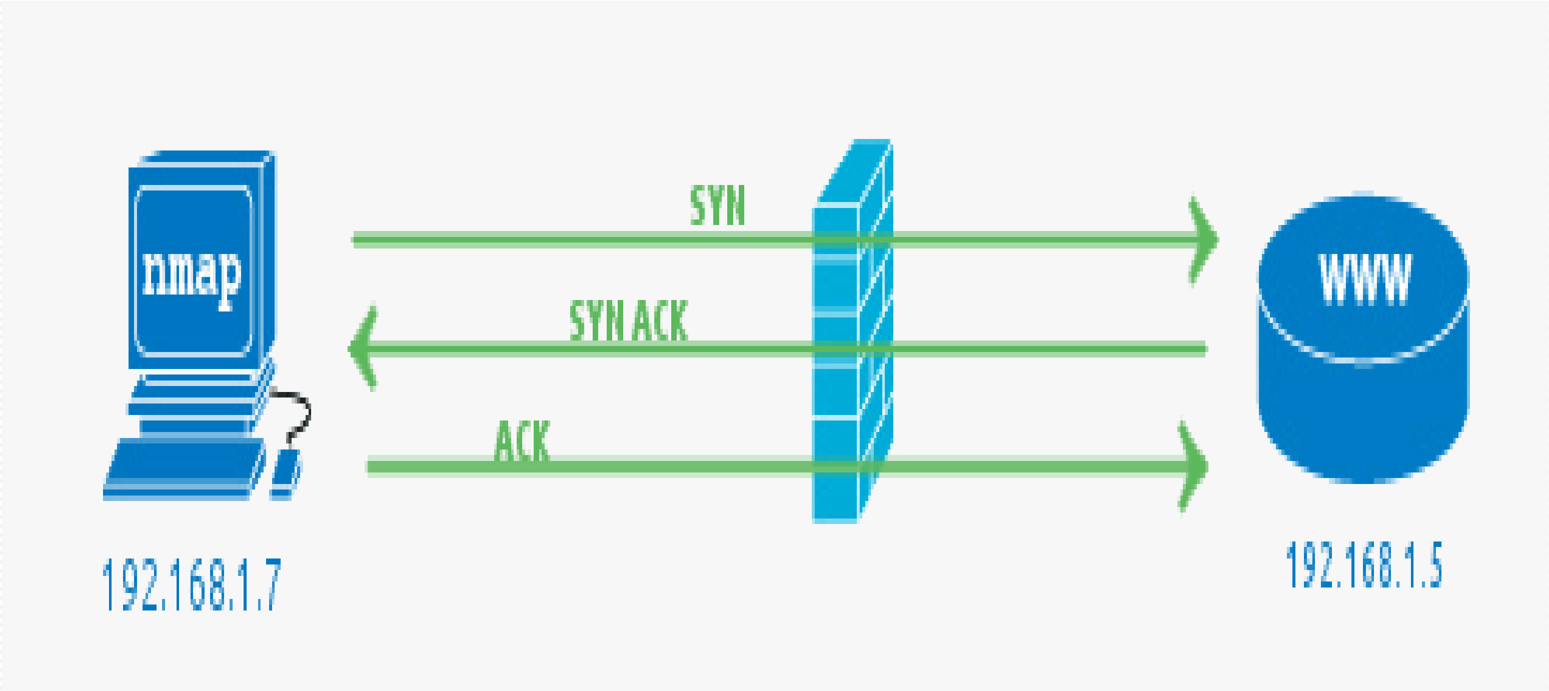
SYN Scan



```
[root@eea340 init.d]# nmap -sS 140.130.19.1

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on dns.ee.nhust.edu.tw (140.130.19.1):
(The 1548 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
23/tcp     open        telnet
53/tcp     open        domain
111/tcp    open        sunrpc
10000/tcp  open        snet-sensor-mgmt
22321/tcp  open        wnn6_Tw


Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
[root@eea340 init.d]# _
```

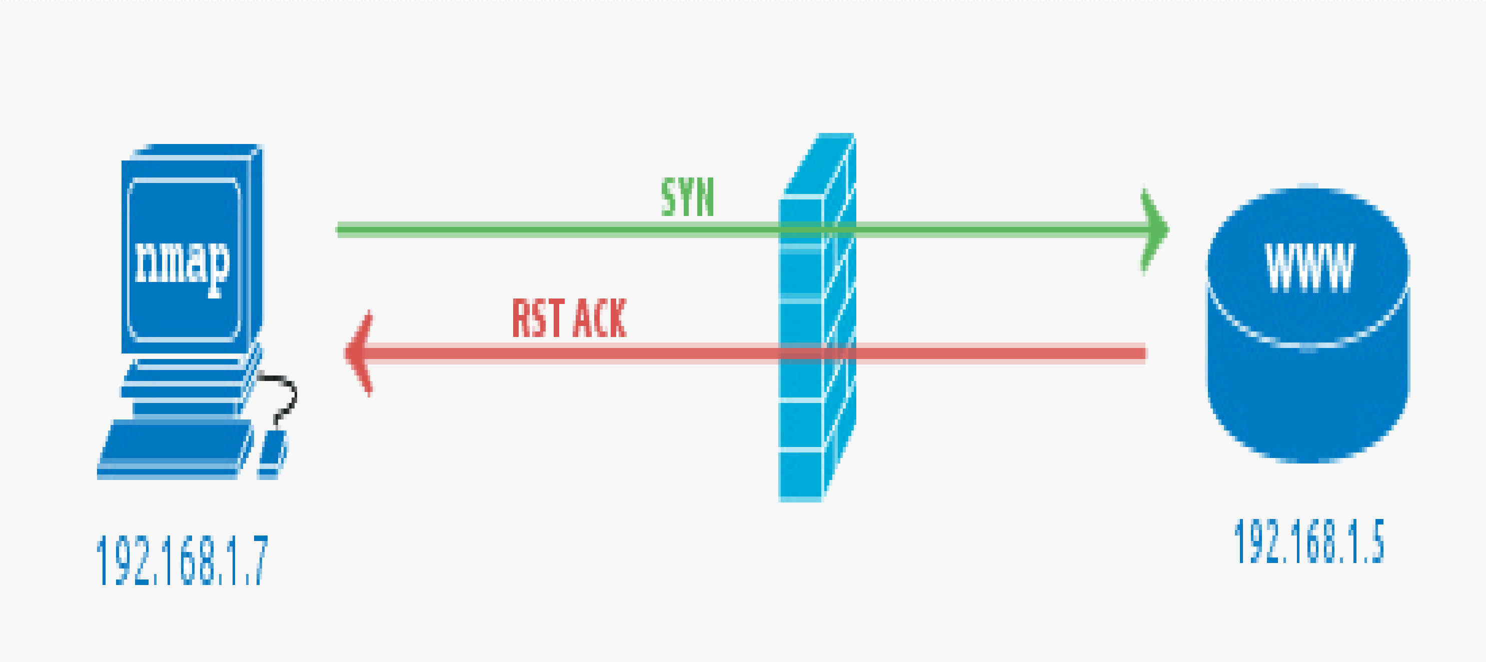
Port Status

OPEN: The 3 way TCP handshake



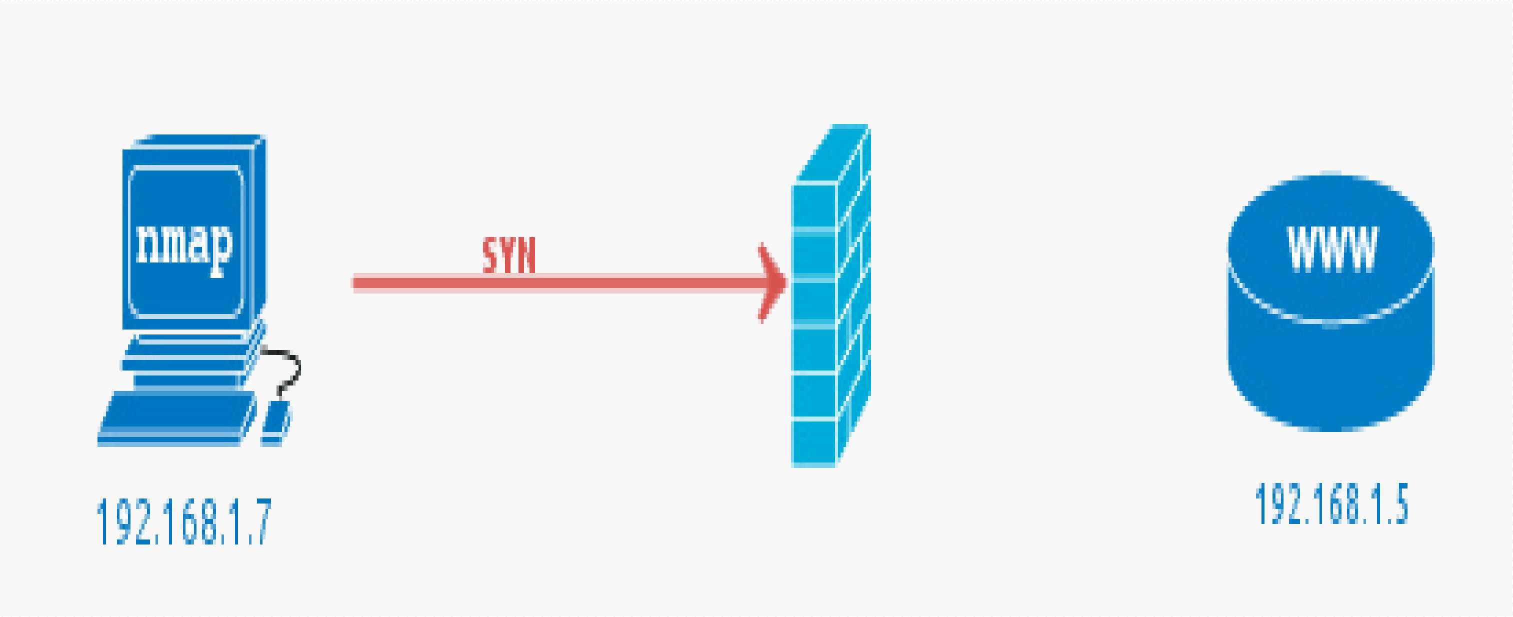
Port Status…

CLOSED ports or when the Firewall fails



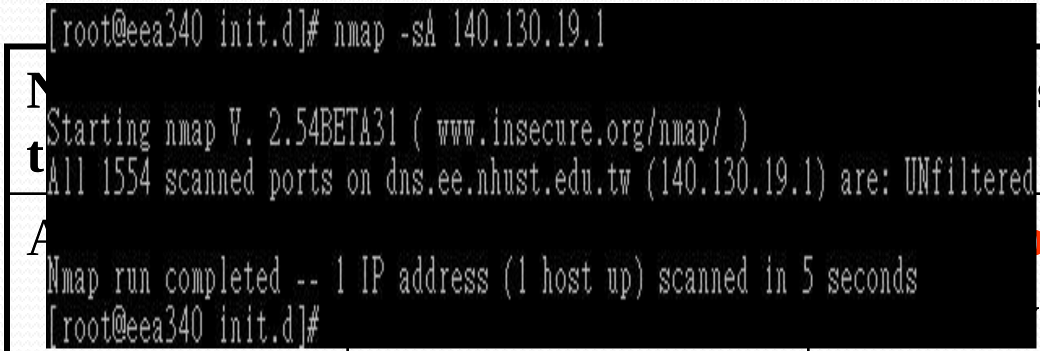
Port Status…

FILTERED ports or when the Firewall drops a packet



ACK Scan

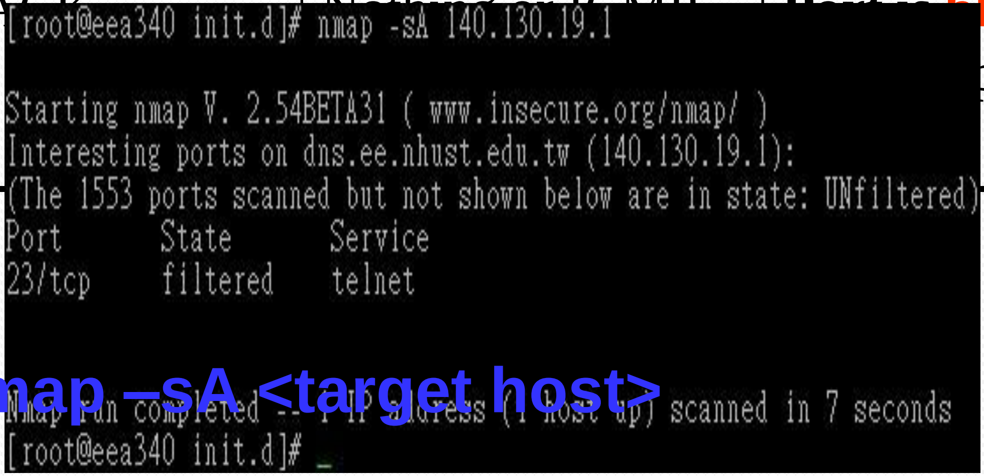
No firewall~



```
[root@eea340 init.d]# nmap -sA 140.130.19.1

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
All 1554 scanned ports on dns.ee.nhust.edu.tw (140.130.19.1) are: UNfiltered

Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds
[root@eea340 init.d]#
```

N t		sumes
A		t firewall-protect be open or closed Host is up
ACK	Nothing or ICMP	Port is blocked by firewall if p

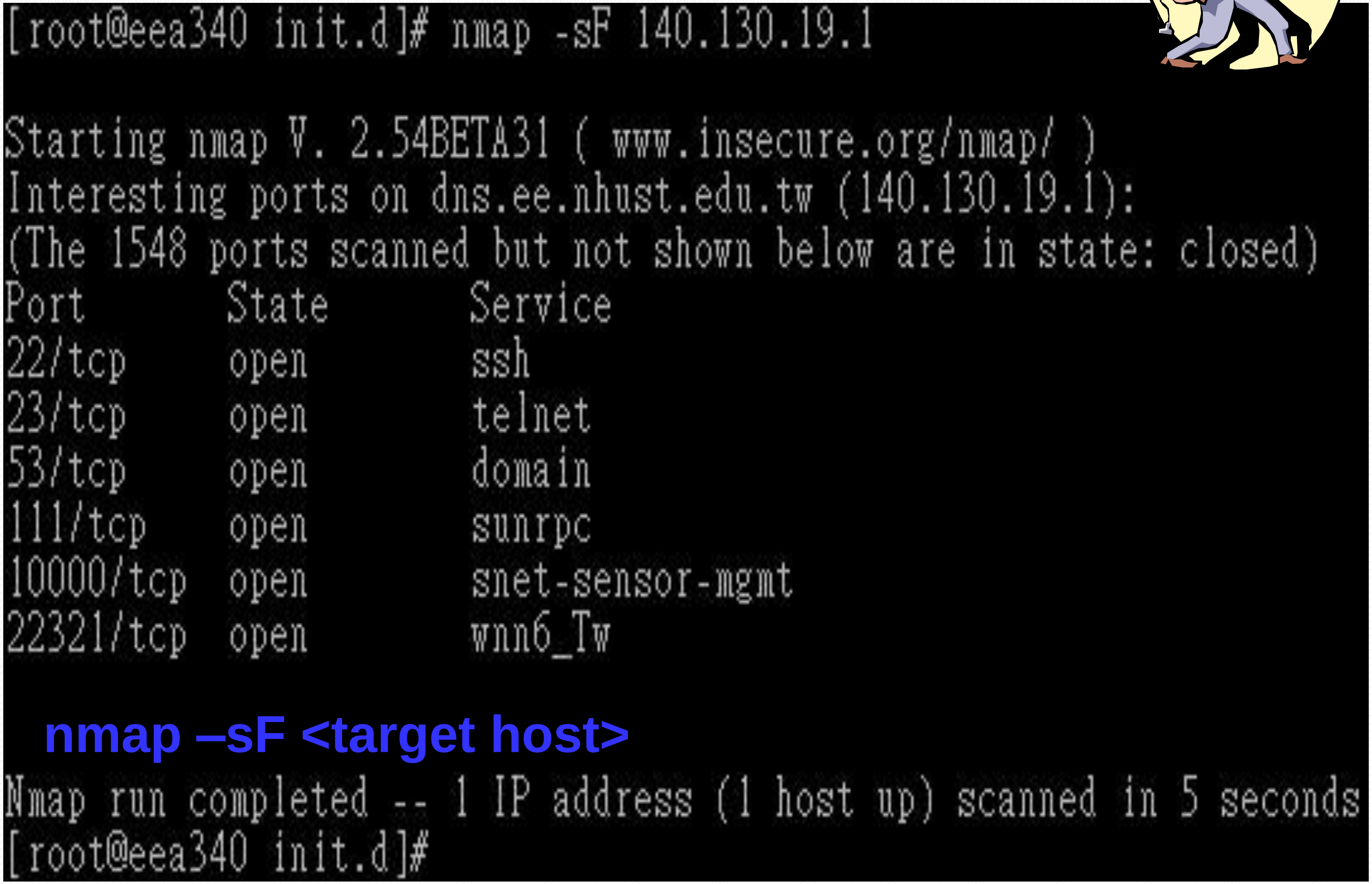
Protected by firewall~



```
[root@eea340 init.d]# nmap -sA 140.130.19.1

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on dns.ee.nhust.edu.tw (140.130.19.1):
(The 1553 ports scanned but not shown below are in state: UNfiltered)
Port       State       Service
23/tcp     filtered    telnet


Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds
[root@eea340 init.d]# _
```

nmap –sA <target host>

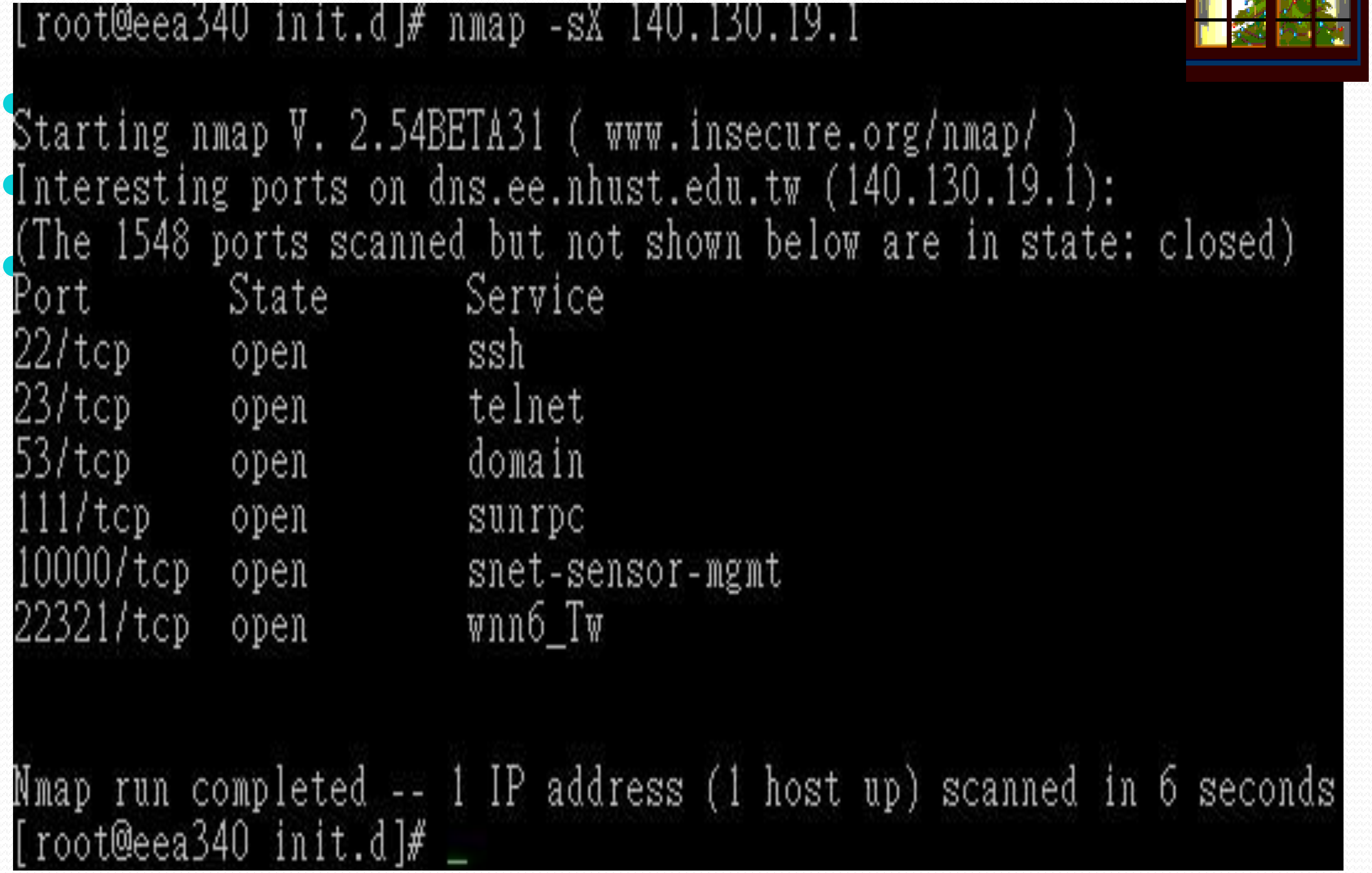
FIN Scan



```
[root@eea340 init.d]# nmap -sF 140.130.19.1

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on dns.ee.nhust.edu.tw (140.130.19.1):
(The 1548 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
23/tcp     open        telnet
53/tcp     open        domain
111/tcp    open        sunrpc
10000/tcp  open        snet-sensor-mgmt
22321/tcp  open        wnn6_Tw

Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds
[root@eea340 init.d]#
```

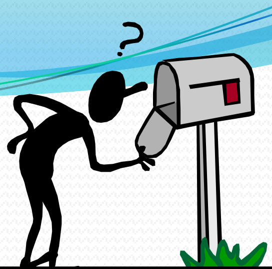
nmap –sF <target host>

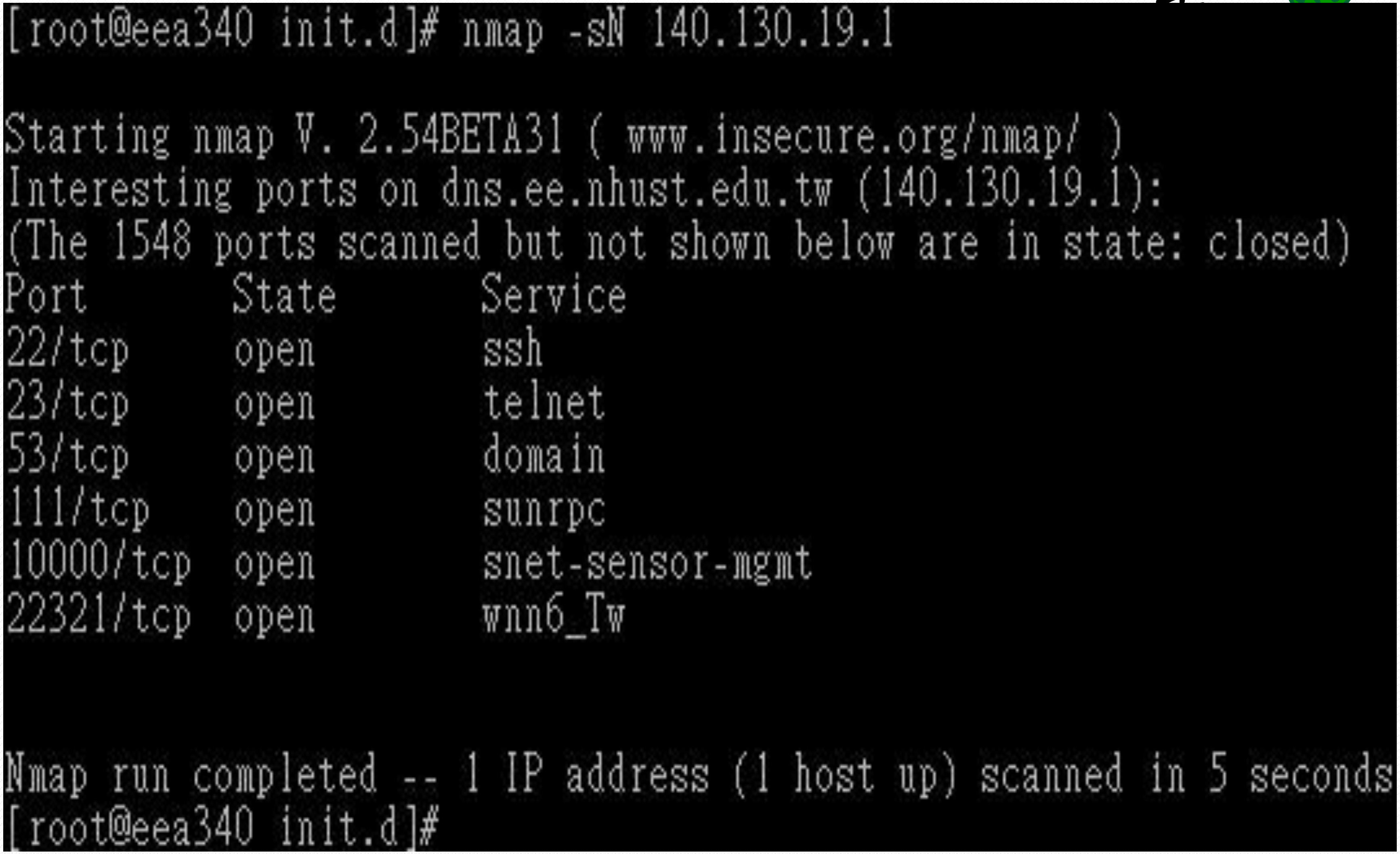
Xmas Scan



```
[root@eea340 init.d]# nmap -sX 140.130.19.1

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on dns.ee.nhust.edu.tw (140.130.19.1):
(The 1548 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
23/tcp     open        telnet
53/tcp     open        domain
111/tcp    open        sunrpc
10000/tcp  open        snet-sensor-mgmt
22321/tcp  open        wnn6_Tw


Nmap run completed -- 1 IP address (1 host up) scanned in 6 seconds
[root@eea340 init.d]# _
```

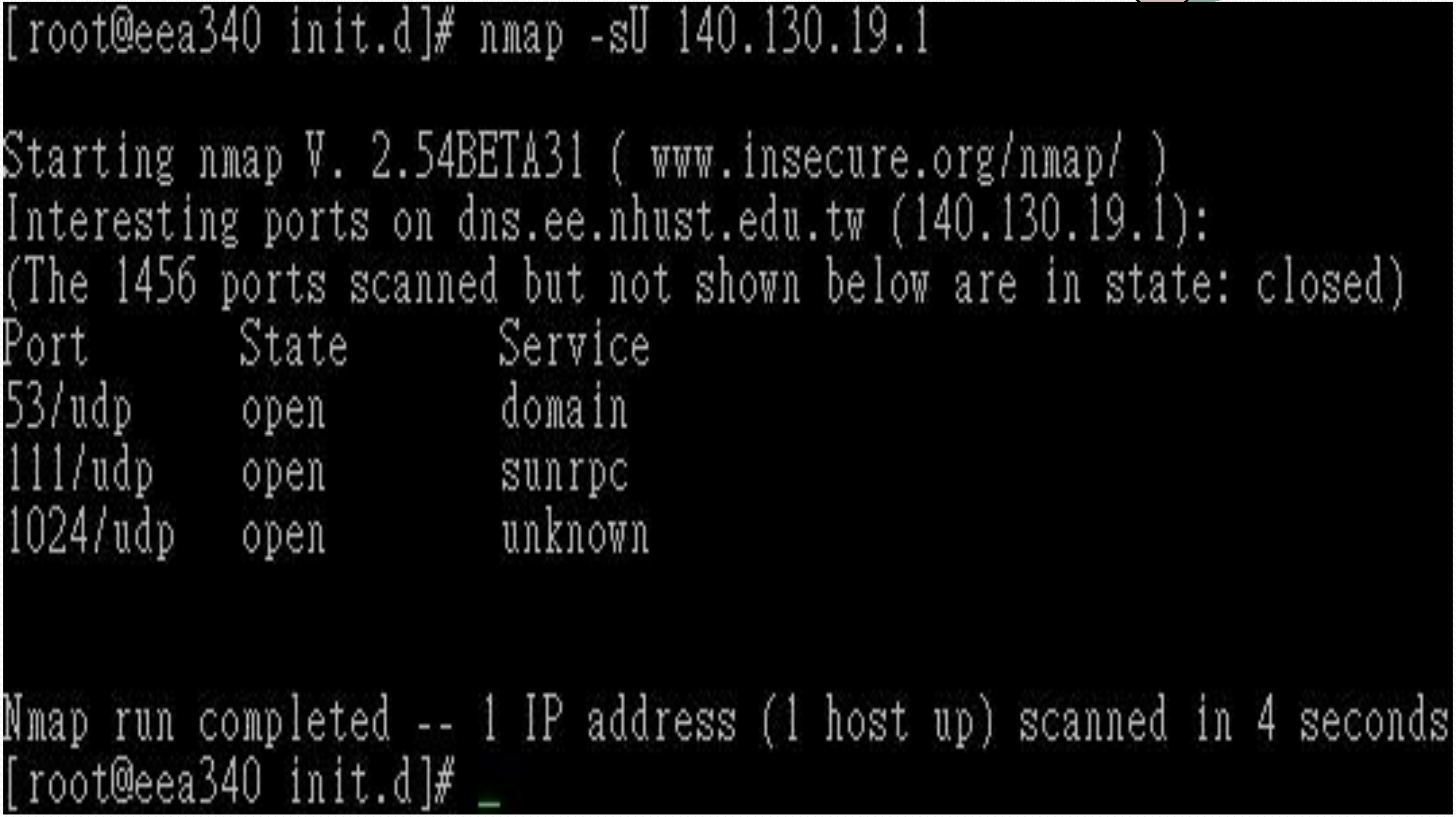
Null scan





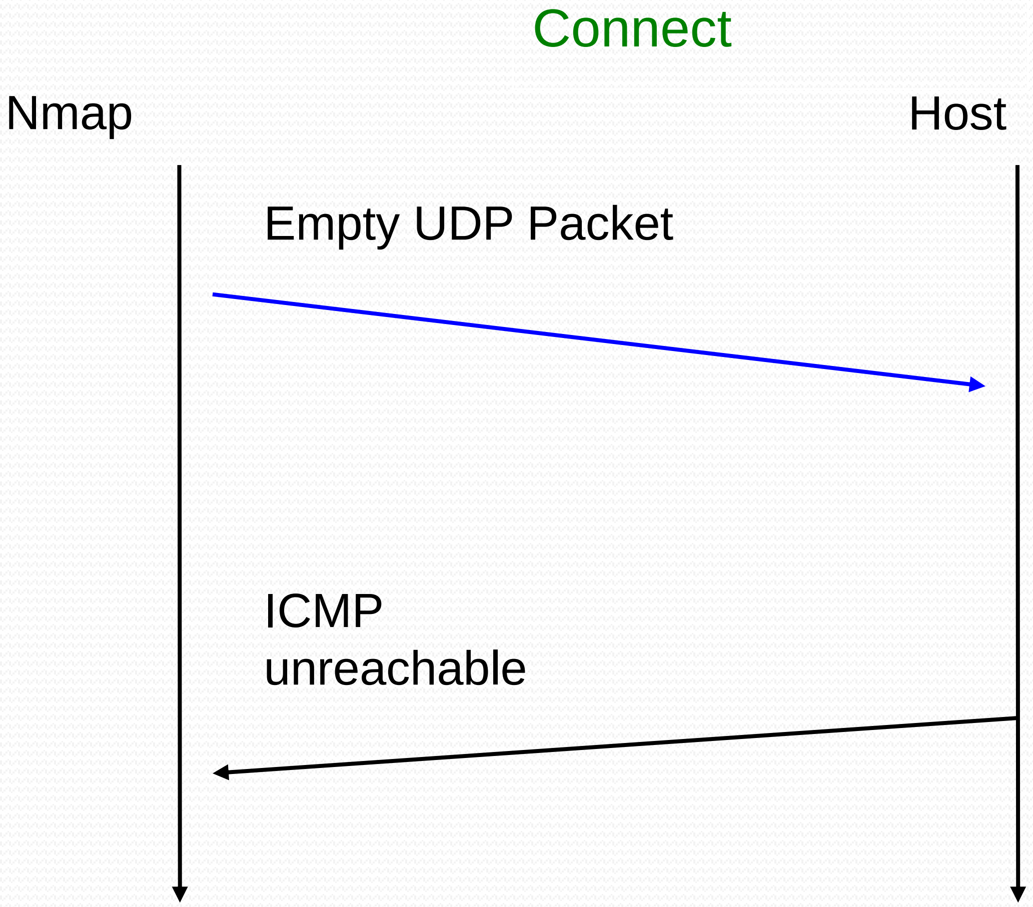
```
[root@eea340 init.d]# nmap -sN 140.130.19.1

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on dns.ee.nhust.edu.tw (140.130.19.1):
(The 1548 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
23/tcp     open        telnet
53/tcp     open        domain
111/tcp    open        sunrpc
10000/tcp  open        snet-sensor-mgmt
22321/tcp  open        wnn6_Tw


Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds
[root@eea340 init.d]#
```

Scanning for UDP Ports



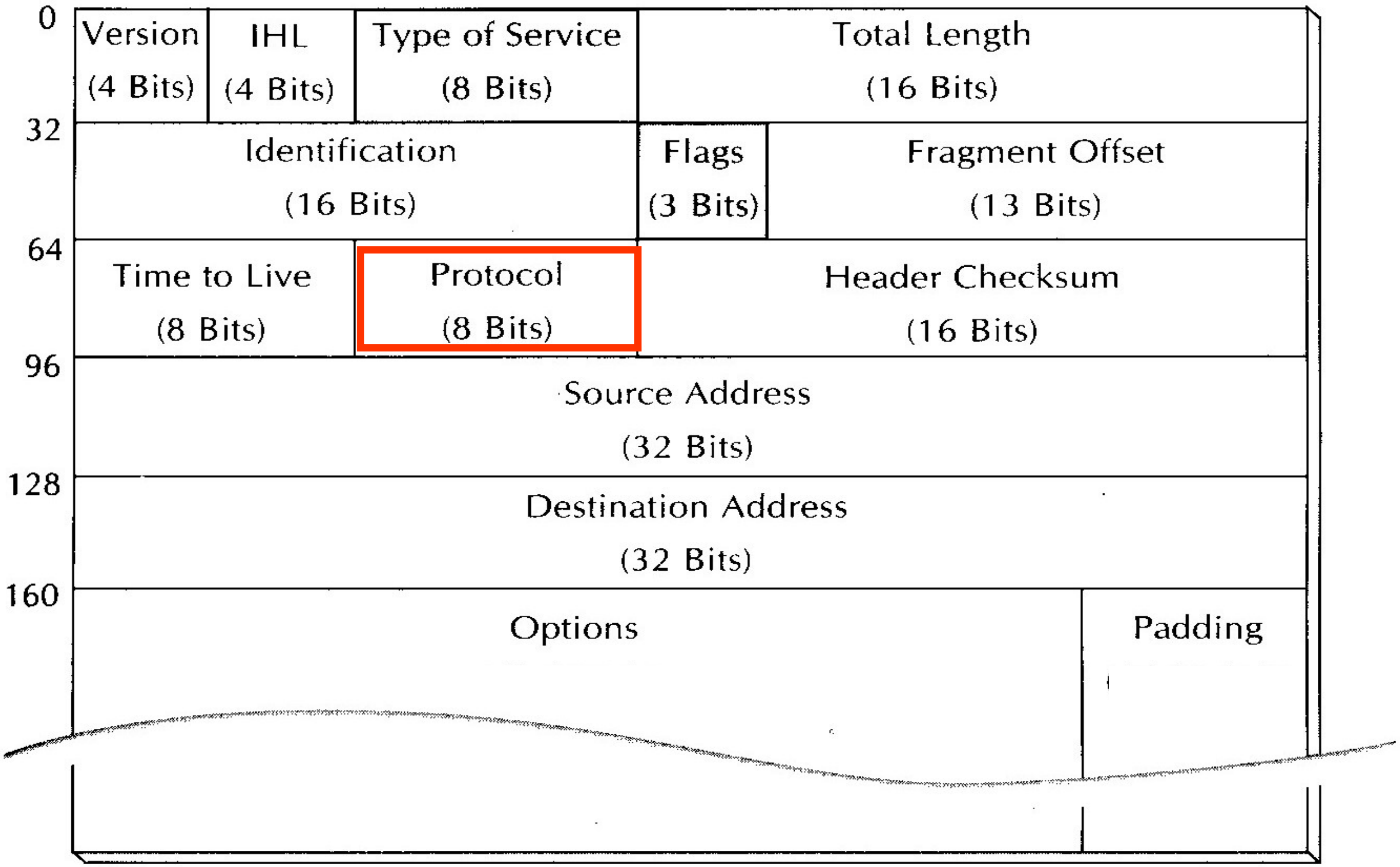
```
[root@eea340 init.d]# nmap -sU 140.130.19.1

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on dns.ee.nhust.edu.tw (140.130.19.1):
(The 1456 ports scanned but not shown below are in state: closed)
Port       State       Service
53/udp     open        domain
111/udp    open        sunrpc
1024/udp   open        unknown


Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds
[root@eea340 init.d]# _
```

Scanning for UDP Ports



Scanning for Protocol

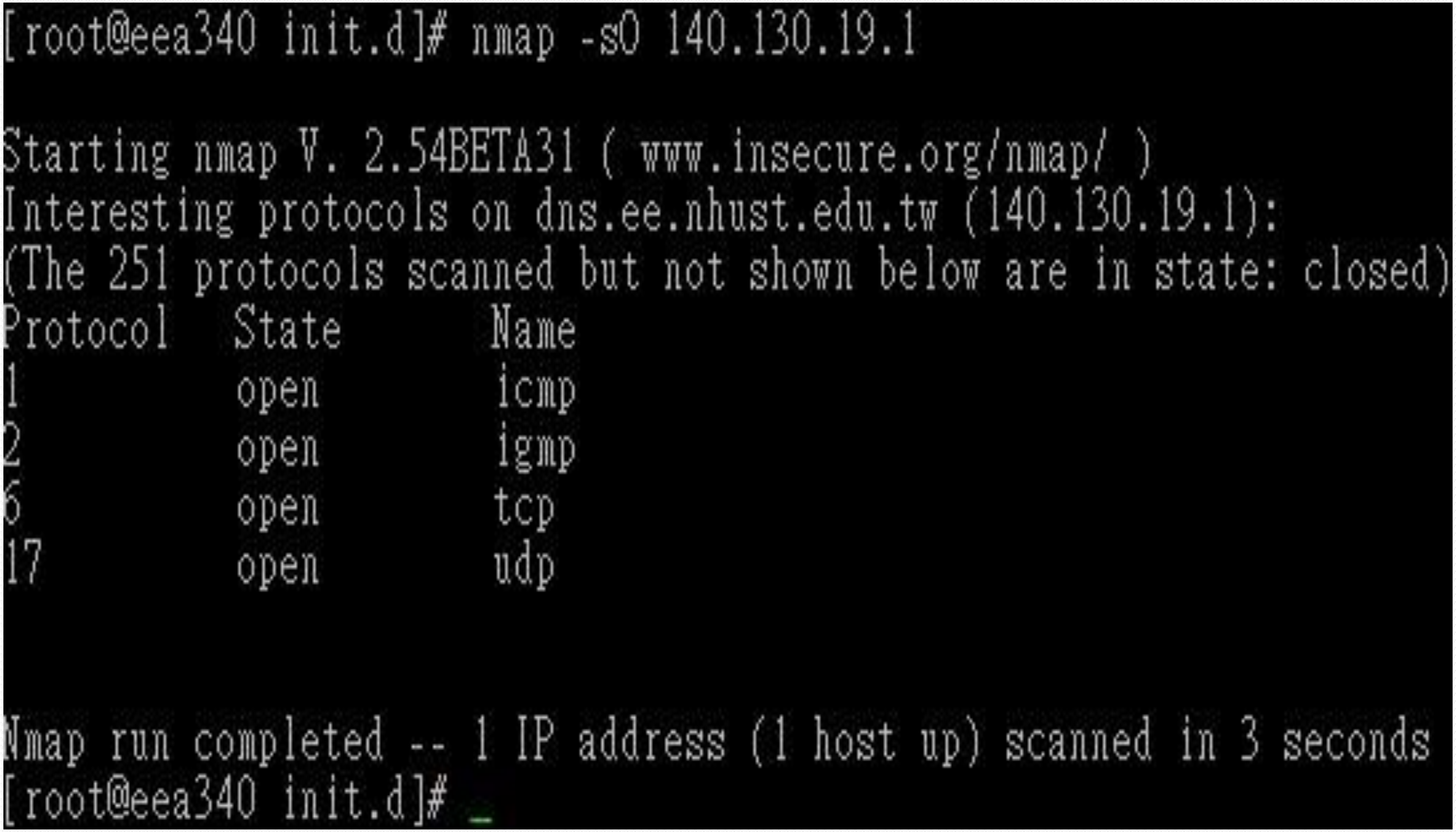
IP Header



0	Version (4 Bits)	IHL (4 Bits)	Type of Service (8 Bits)	Total Length (16 Bits)
32	Identification (16 Bits)	Flags (3 Bits)	Fragment Offset (13 Bits)	
64	Time to Live (8 Bits)	Protocol (8 Bits)	Header Checksum (16 Bits)	
96	Source Address (32 Bits)			
128	Destination Address (32 Bits)			
160	Options	Padding		

Scanning for Protocol

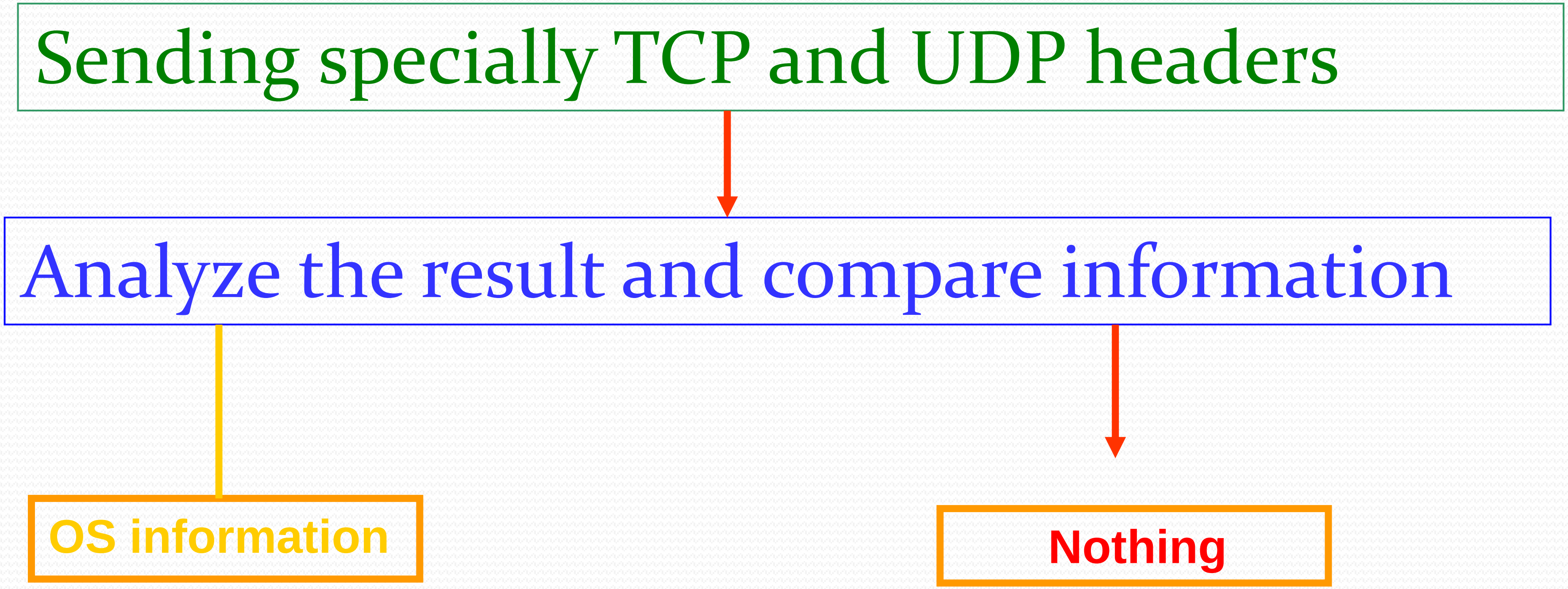
- **nmap –sO <target host>**



```
[root@eea340 init.d]# nmap -sO 140.130.19.1

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting protocols on dns.ee.nhust.edu.tw (140.130.19.1):
(The 251 protocols scanned but not shown below are in state: closed)
Protocol    State       Name
1           open        icmp
2           open        igmp
6           open        tcp
17          open        udp


Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
[root@eea340 init.d]# _
```

OS Fingerprinting

- With –O flag



Sending specially TCP and UDP headers

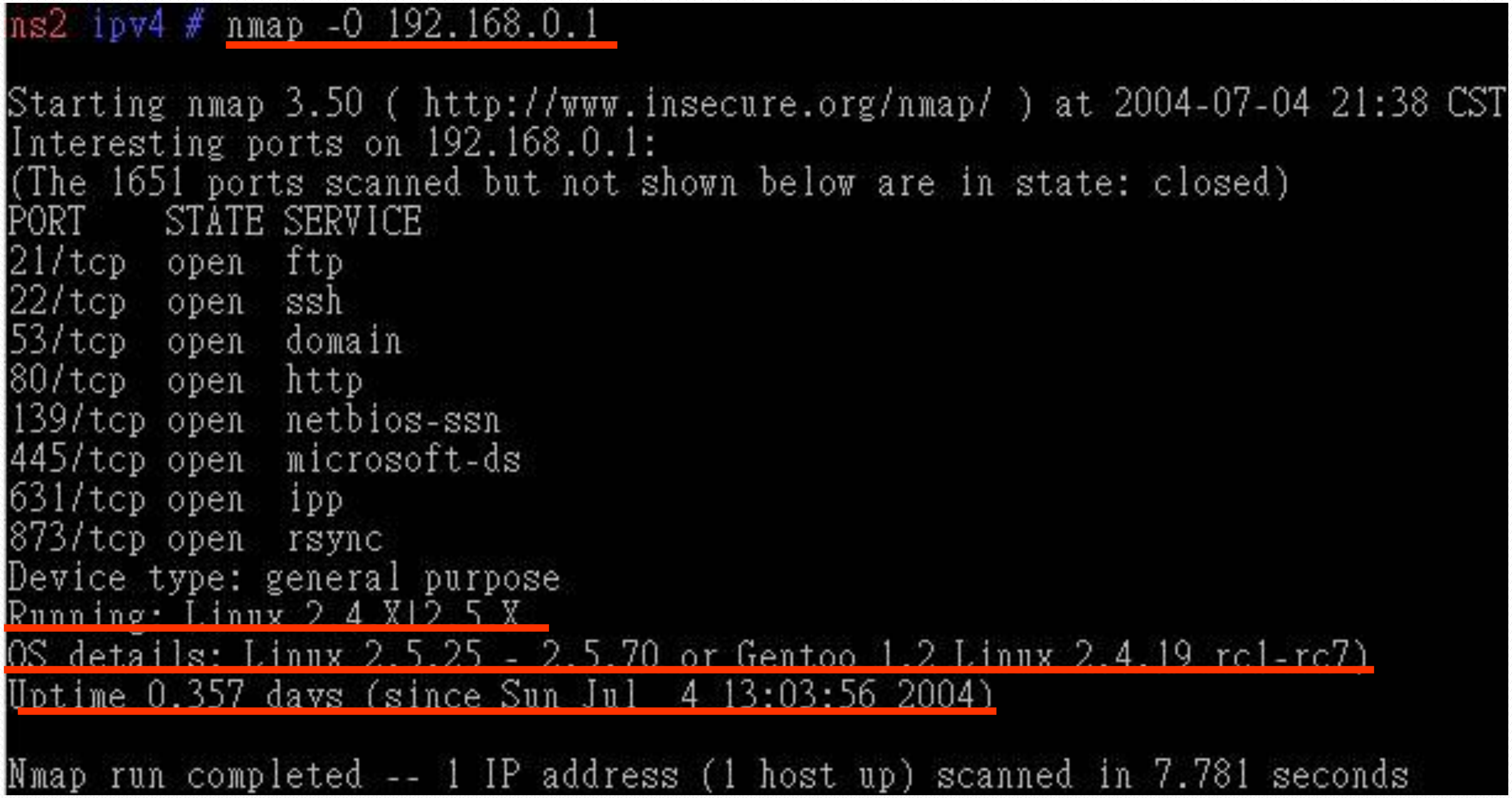
Analyze the result and compare information

OS information

Nothing

OS Detection

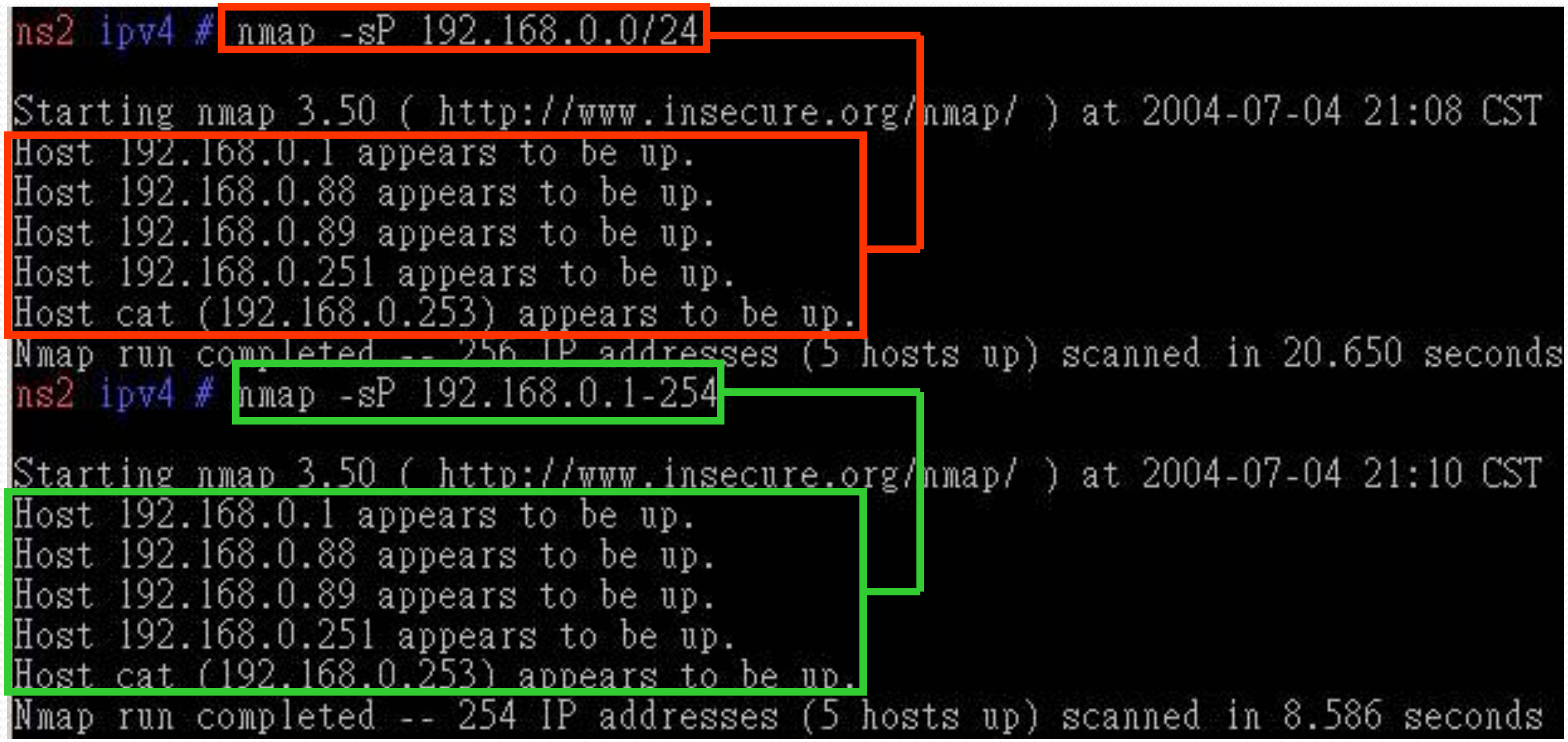
- nmap –O 192.168.0.1



```
ns2 ipv4 # nmap -O 192.168.0.1

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-07-04 21:38 CST
Interesting ports on 192.168.0.1:
(The 1651 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
631/tcp open  ipp
873/tcp open  rsync
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.5.25 - 2.5.70 or Gentoo 1.2 Linux 2.4.19 rc1-rc7)
Uptime 0.357 days (since Sun Jul  4 13:03:56 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 7.781 seconds
```

Mapping Networks

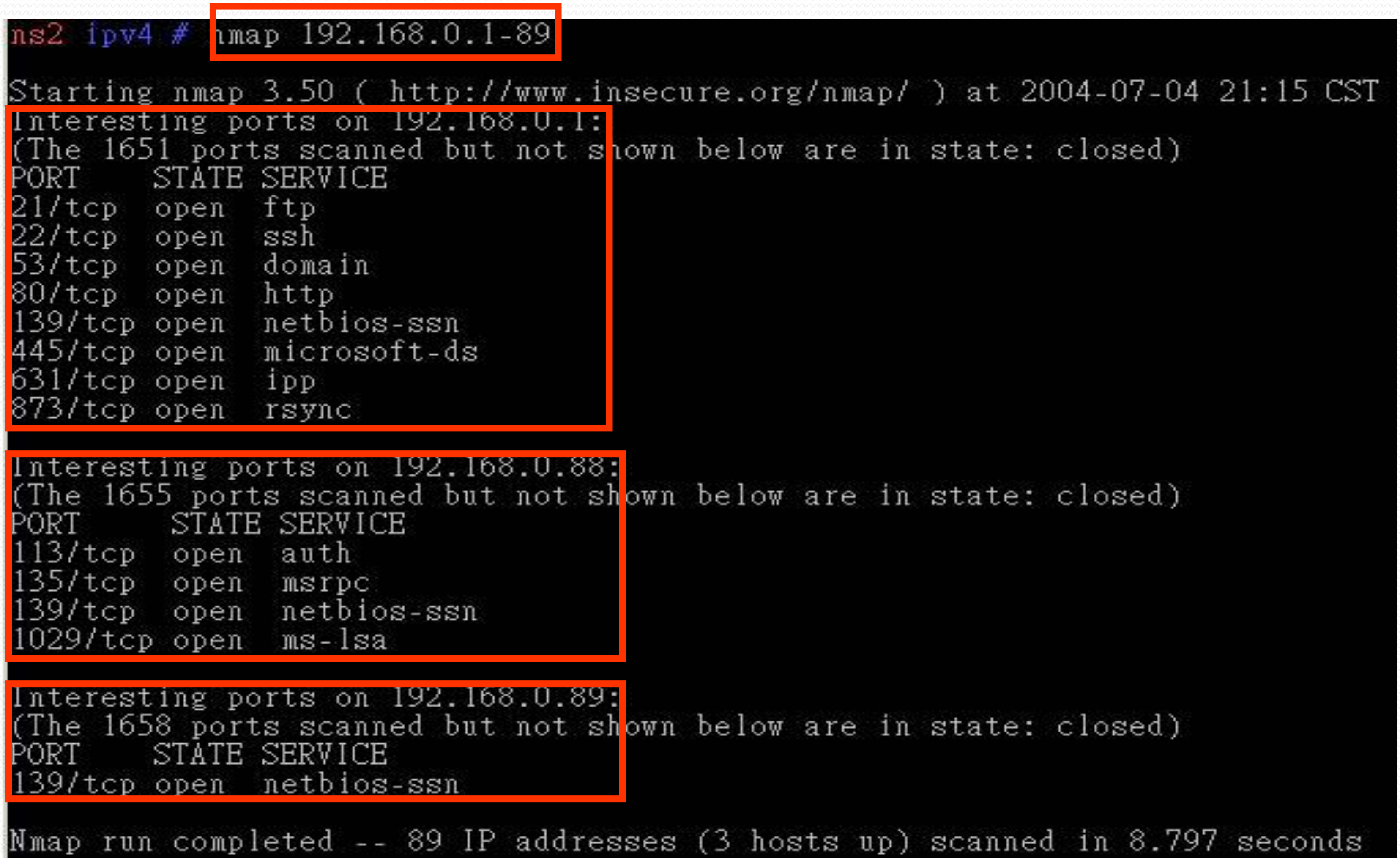
- Scanning a Class C subnet



```
ns2 ipv4 # nmap -sP 192.168.0.0/24

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-07-04 21:08 CST
Host 192.168.0.1 appears to be up.
Host 192.168.0.88 appears to be up.
Host 192.168.0.89 appears to be up.
Host 192.168.0.251 appears to be up.
Host cat (192.168.0.253) appears to be up.
Nmap run completed -- 256 IP addresses (5 hosts up) scanned in 20.650 seconds
ns2 ipv4 # nmap -sP 192.168.0.1-254

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-07-04 21:10 CST
Host 192.168.0.1 appears to be up.
Host 192.168.0.88 appears to be up.
Host 192.168.0.89 appears to be up.
Host 192.168.0.251 appears to be up.
Host cat (192.168.0.253) appears to be up.
Nmap run completed -- 254 IP addresses (5 hosts up) scanned in 8.586 seconds
```

Mapping Networks

- Port scans in IP section



```
ns2 ipv4 # nmap 192.168.0.1-89

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-07-04 21:15 CST
Interesting ports on 192.168.0.1:
(The 1651 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
631/tcp  open  ipp
873/tcp  open  rsync

Interesting ports on 192.168.0.88:
(The 1655 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
113/tcp   open  auth
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
1029/tcp  open  ms-lsa

Interesting ports on 192.168.0.89:
(The 1658 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
139/tcp  open  netbios-ssn

Nmap run completed -- 89 IP addresses (3 hosts up) scanned in 8.797 seconds
```

Tools included in NMAP Package

- **nping – Network packet generation tool / ping utility**
- **ndiff – Utility to compare the results of Nmap scans**
- **ncat – Concatenate and redirect sockets**
- **nmap – The Network Mapper**

EX. >nping -h

Recap

- Nmap (“Network Mapper”)
  - Open source tool
  - Use for network exploration and security auditing
  - Rapidly scan large networks
  - Determine hosts availability on the network
  - Services those hosts are offering
  - Find operating systems and OS versions
  - Find type of packet filters/firewalls are in use

Recap…

* Find Nmap version

nmap -V

*Scan a single IP address When firewall OFF/ON on target PC

Syntax – nmap IP address/hostname

Ex – **nmap 192.168.75.131**

Ex- **nmap google.com**

* Boost up Your nmap Scan – using this command you can decrease scan time

Syntax – **nmap –F IP address**

Ex – **nmap –F google.com**

Recap…

*Scan multiple IP address or subnet

A. scan a range of IP address

Syntax – nmap IP address range

EX- **nmap 192.168.75.1-131**

B. Scan a range of IP address using a wildcard

Ex – **nmap 192.168.75.***

C. Scan Multiple Hosts

Ex. nmap 192.168.0.101 192.168.0.102 192.168.0.103

D. Scan an entire subnet

Ex – **nmap 192.168.75.1/24**

E. Scan Multiple Servers using last octet of IP address

Ex- **nmap 192.168.0.101,102,103**

Recap…

*TCP Xmas scan to check firewall

Ex – **nmap –sX 192.168.75.131**

* UDP Scan – Scan a host for UDP services. This scan is used to view open UDP port.

Ex – **nmap –sU 192.168.75.131**

* Scan for IP protocol – This type of scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines.

Ex – **nmap –sO 192.168.75.131**

*Detect remote services (server / daemon) version numbers

Ex – **nmap –sV 192.168.75.131**

Recap…

* Find out the most commonly used TCP ports using TCP SYN Scan

A. Stealthy scan

Ex – **nmap –sS 192.168.75.131**

B. Find out the most commonly used TCP ports using TCP connect scan

Ex – **nmap –sT 192.168.75.131**

C. Find out the most commonly used TCP ports using TCP ACK scan

Ex – **nmap –sA 192.168.75.131**

Recap…

* Scan turn on OS and version detection

Ex – **nmap –O 192.168.75.131**

* Host Discovery or Ping Scan – Scan a network and find out which servers and devices are up and running

Ex – **nmap –sP 192.168.75.0/24**

* Scan list of Hosts from a File

```
cat > nmaptest.txt
 localhost
 server2.tecmint.com
 192.168.0.101

nmap -iL nmaptest.txt
```