Ch3 Linux Network & Tools

Cite http://www.techomag.com/

謝明志(Jimin Hsieh)

Agenda

- 3-1 Basic Utilities
- 3-2 Set up your IP
- 3-3 SSH
- 3-4 Telnet
- 3-5 Wireshark
- 3-6 Nmap

3-1 Basic Utilities

- Local

1. # ifconfig

    1.1. # ifconfig [interface]

    1.2. # ifconfig [interface] down/up

    1.2. # ifconfig [interface] [ip]

2. # route

3. # netstat

3.1. option:"-a"

Internet connections

vs.

UNIX domain sockets

3.2. # netstat | grep [strings]

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 JiminLab.local:ssh     JiminNB.local:46717     ESTABLISHED
udp6       0      0 localhost:47189        localhost:47189         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    5888     /var/run/xrdp/xrdp_sesman_00000
```

3-1 Basic Utilities

```
root@JiminNB:~# ifconfig
eth0      Link encap:Ethernet  HWaddr f0:de:f1:e1:39:6e
          inet addr:163.13.127.130  Bcast:163.13.127.255  Mask:255.255.255.0
          inet6 addr: fe80::f2de:f1ff:fee1:396e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39940 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36885 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:39065309 (37.2 MiB)  TX bytes:6995928 (6.6 MiB)
          Interrupt:42 Base address:0x6000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1687 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1687 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:128032 (125.0 KiB)  TX bytes:128032 (125.0 KiB)

wlan0     Link encap:Ethernet  HWaddr 44:6d:57:18:55:39
          inet addr:192.168.0.101  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::466d:57ff:fe18:5539/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:351 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32224 (31.4 KiB)  TX bytes:6617 (6.4 KiB)
```

3-1 Basic Utilities

- Remote

1. # ping [ip-address]: send ICMP packet
    1.1. option: -i [integer]
        ping with specific interval
    1.2. option: -s [packet size]
2. # traceroute [ip-address]: show the route

- Other

1. # wget [IP + file]: download file from Internet

3-2 Set up your IP

1. DHCP

1.1. IP address

/etc/network/interfaces

auto [interface]

allow-hotplug [interface]

iface [interface] inet dhcp

2. Static IP

1.1. IP address

/etc/network/interfaces

auto [interface]

iface [interface] inet static

address [IP]

netmask [mask]

gateway [Gateway IP]

2.2. DNS IP address

/etc/resolve.con

nameserver [IP]

3-3 SSH

- Secure Shell

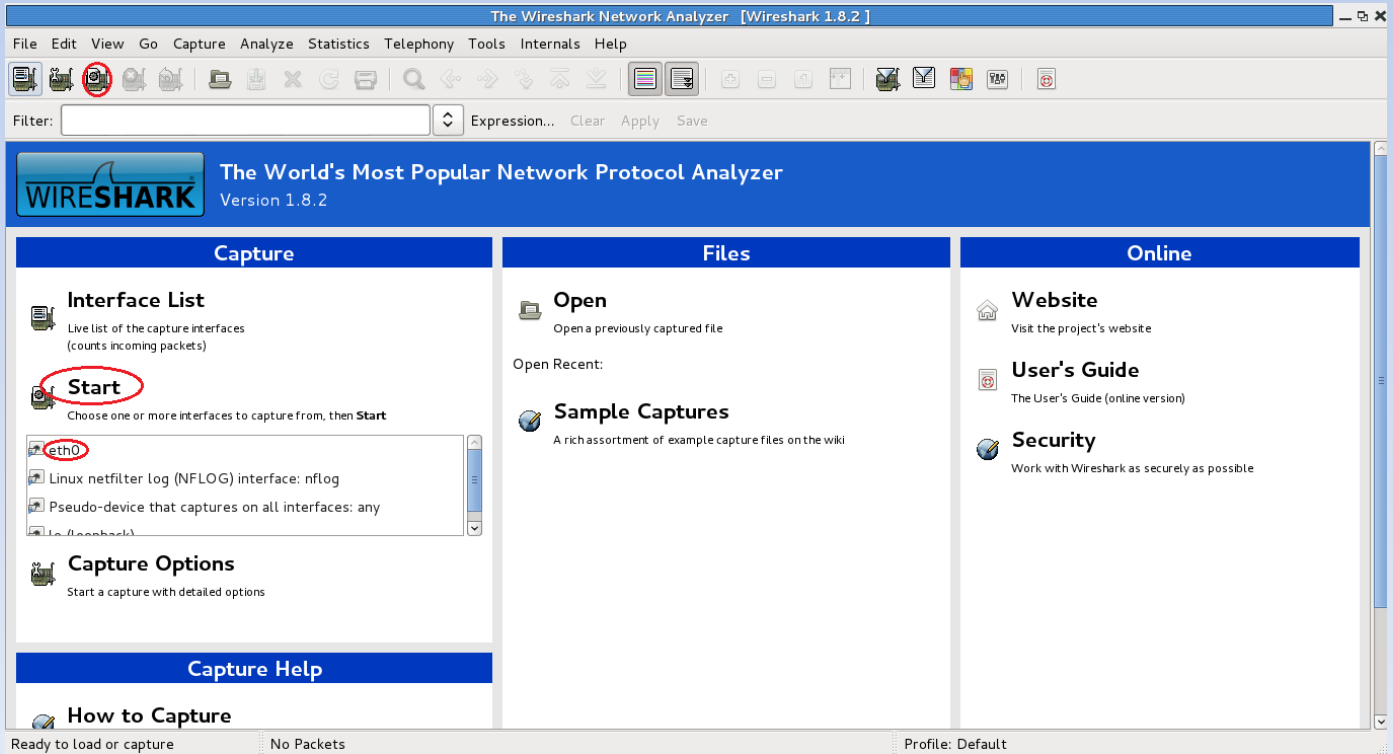
1. ssh server: openssh-server
2. ssh client(Linux):
    2.1. # ssh user@ip-address
    2.2. Remote to Local: # scp [-r] user@ip-address:[file] [location of local]
    2.3. Local to Remote: # scp [-r] [file/directoy] user@ip-address:[location of remote]
3. ssh client(Win): putty

3-4 Telnet

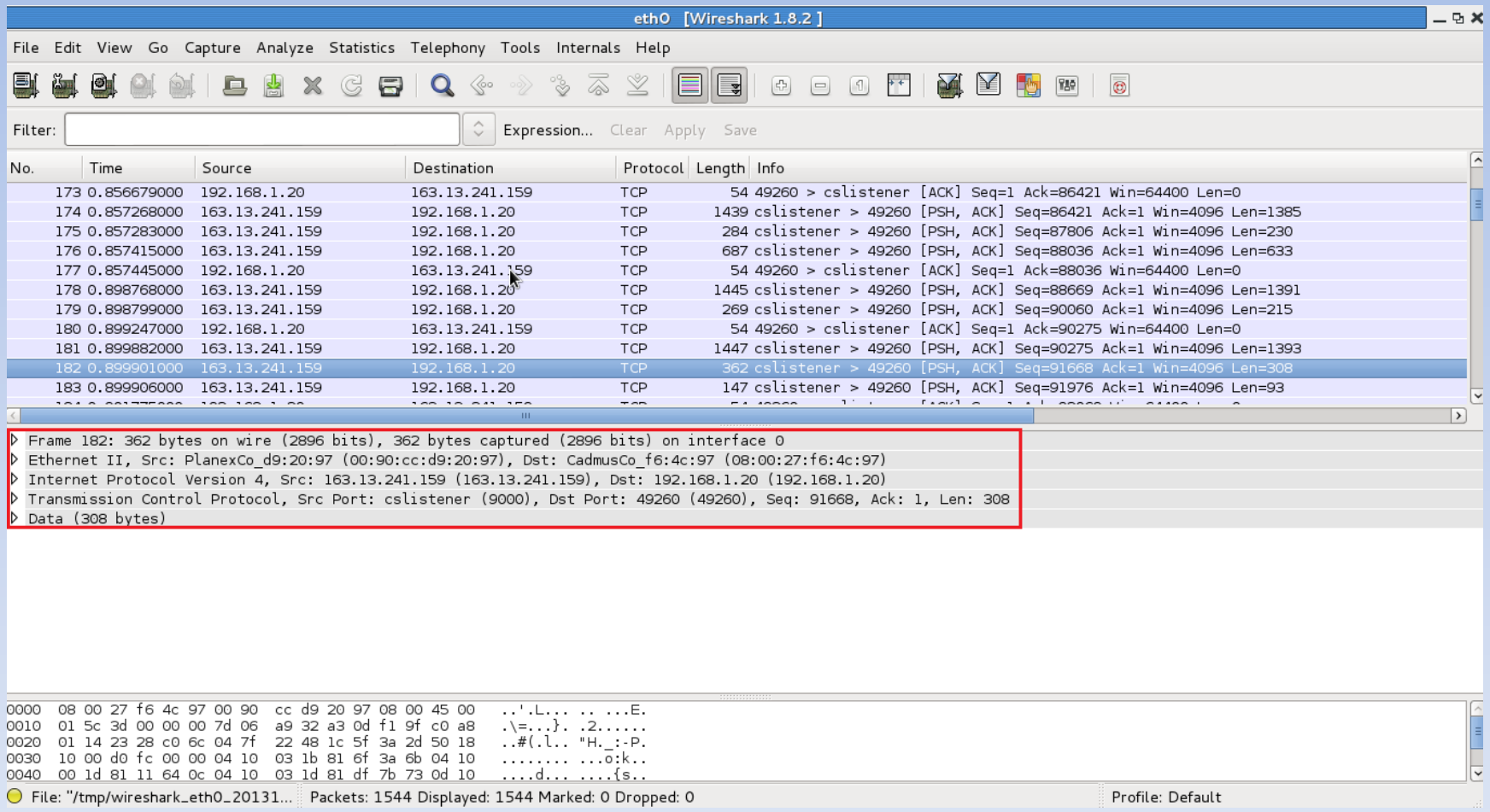
1. telnet server: telnetd or telnetd-ssl
2. telnet client(Linux)
   2.1. # telnet user@[ip-address]
   2.2. putty
3. telnet client(Win): putty

3-5 Wireshark

- Packet analyzer
- Using privilege of root to open in console
- # wireshark

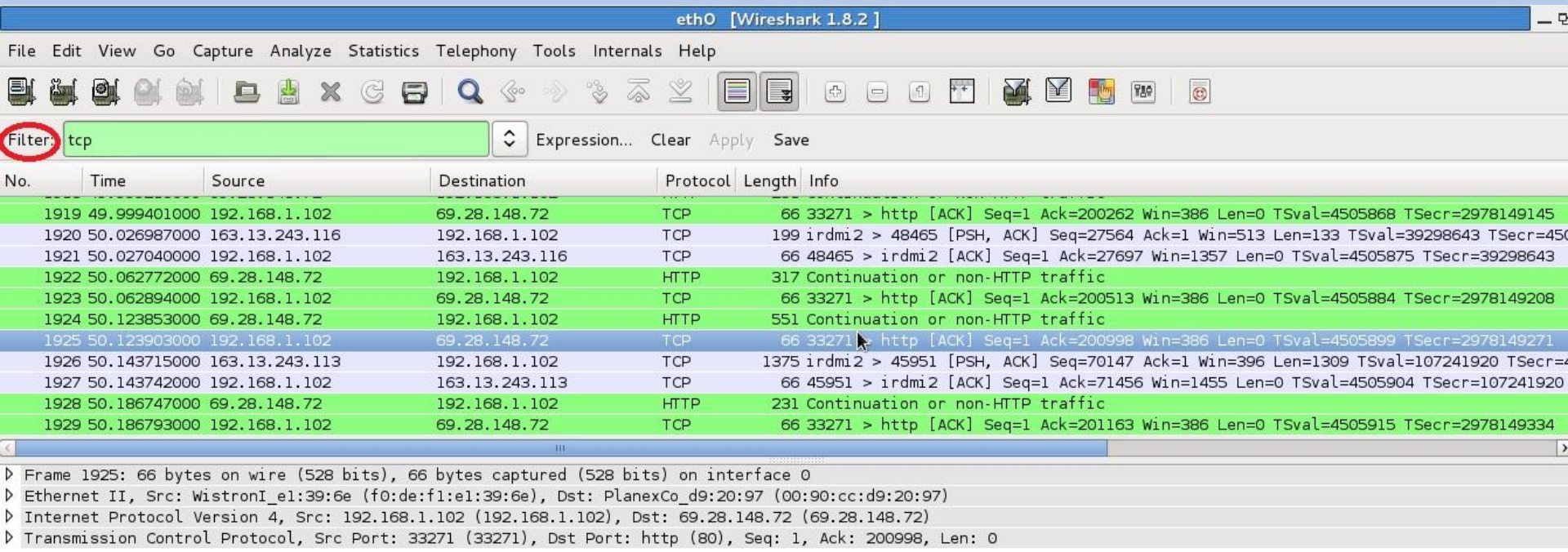


CH3-5 Wireshark



CH3-5 Wireshark

Filter: tcp, udp, icmp…etc



3-6 Nmap

Nmap (Network mapper) – Network Scanner

- # nmap [IP]

1. option: "-O" enable OS detect

   # nmap –O [IP]

2. option: "-sn"/ "-sP" scan PC through ICMP

   # nmap -sn 192.168.1.0/24

3. option: "-sT" scan TCP port

   # nmap -sT [IP]

4. option: "-sU" scan UDP port

3-6 Nmap

```
root@JiminLab:~# nmap -O www.facebook.com

Starting Nmap 6.00 ( http://nmap.org ) at 2013-11-06 09:11 CST
Nmap scan report for www.facebook.com (31.13.68.8)
Host is up (0.027s latency).
rDNS record for 31.13.68.8: edge-star-shv-01-hkg1.facebook.com
Not shown: 997 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp open   https
843/tcp closed unknown
Device type: storage-misc
Running (JUST GUESSING): Linksys Linux 2.6.X (88%)
OS CPE: cpe:/o:linux:kernel:2.6.18
Aggressive OS guesses: Linux 2.6.18 (88%)
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 9.04 seconds
```

```
Starting Nmap 6.00 ( http://nmap.org ) at 2013-11-06 09:22 CST
Nmap scan report for [redacted]
Host is up (0.0057s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49155/tcp open  unknown
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista
OS CPE: cpe:/o:microsoft:windows_vista::sp1:home_premium
OS details: Microsoft Windows Vista Home Premium SP1

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.27 seconds
```

Q&A

Thanks for you attentions!