THE DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
計算機科學及工程學系

香港科技大學
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

COMP 4632
Practicing Cybersecurity: Attacks and Counter-measures

Week 2 Lab Exercise

***Topic:** Network Basics and Footprinting*

Lab Objective

In this lab, we are going to perform basic network analysis:

- Use **a series of commands** to understand the network basics (e.g. IP address, DNS, traceroute etc)
- Perform network based discovery using network tools
- Install **Wireshark** and **Networkminer** to examine the network traffic
- Install **Nmap** to initiate network traffic via port scanning
- Demonstrate the Wireless setup with hidden SSID and its related security setting as well as concerns

Task 1 – Understand the network basics (15 minutes)

Run the correct one in the following commands at your command prompt and answer the following questions:

- **ipconfig**
- **ipconfig /all**
- **ifconfig**

Task 1.1 What is your machine's IP address

Task 1.2 What is your virtual machine (Kali)) IP address

Turn on Kali VM (user: root, pwd: toor)

Task 1.3 What is the MAC address of your machine and your virtual machine (Kali)?

Your Machine:

Kali VM:

Task 1.4 How can a computer determine if the computer is located in the same subnet?

Task 2 – Domain information (30 mins)

Nslookup.exe is a command-line administrative tool for testing and troubleshooting DNS servers.

Launch 'nslookup' at your command prompt and answer the following questions:
(Hint: Typing "help" or "?" at the command prompt will generate a list of available commands)

Task 2.1. What is the current DNS server used to get the domain information?

Task 2.2 Use nslookup to look up the hostname of your machine?
Run 'hostname' at command prompt to check hostname

Task 2.3 Use nslookup to look up the hostname of your neighbors' machine, what are the addresses?

Task 2.4 Use nslookup to look up different data types for the domain "www.google.com". What is/are the address(es) of www.google.com?

Task 2.5 What are the canonical names for www.google.com?
(Hint: use "set type = CNAME" before look up)

Task 2.6 Is there any mail servers owned by www.google.com? Give your supporting information?
(Hint: use "set type = MX" before look up)

Task 2.7 Obtain an authoritative DNS record of www.google.com?
(Hint: use "set type = any" before look up)

Task 2.8 Can you trace back the domain of IP address 61.93.205.178? Any supporting information?

Task 3 – Routing (15 mins)

This exercise is to enable you to understand more about routing
Run 'traceroute" at your Kali command prompt and answer the following questions:

Task 3.1 What is the routing path to www.google.com?

Task 3.2 What is the routing path to your neighboring IP address?

Task 3.3 Is there any firewall, router between your machine and your neighboring machine? How can you determine?

Task 3.4 Is there any firewall, router between your machine and www.google.com? How can you determine?

Task 4 – Passive Network Information Gathering (Passive Footprinting) (60 mins)

Passive footprinting focuses on identifying information about the organization without the organization being aware that the information has been accessed. The passive methods to collect information include but not limited to the following ways

- Mining commonly available information from internet
- Capturing network packets for analysis via sniffing

Task 4.1 Collect the network information using the Internet tools

## Question 1: Provide results to the following. (1.5 marks)

Analyze the following website with the web tools listed in the reference section

Websites:

i. www.yahoo.com

1. **Who owns the domain name of the website? What is the IP address used to host the website?**
2. **What countries are they reported in from open source information?**
3. **Where is the server hosting the website?**
4. **If there are images at website, where are they?**
5. **Provide the email server, DNS server information**

ii. www.ewalker.com.hk

1. Who owns the domain name of the website? What is the IP address used to host the website?
2. What countries are they reported in from open source information?
3. Where is the server hosting the website?
4. If there are images at website, where are they?
5. Provide the email server, DNS server information

iii. www.cathaypacific.com

1. Who owns the domain name of the website? What is the IP address used to host the website?
2. What countries are they reported in from open source information?
3. Where is the server hosting the website?
4. If there are images at website, where are they?
5. Provide the email server, DNS server information

Task 4.2 Collect the network information using Kali

1. Install theHarvester through terminal with the following command
   - git clone https://github.com/laramies/theHarvester.git
2. Search the information about cse.ust.hk.

## Question 2: Which search database can find out most IP address of cse.ust.hk? (1 mark)

Launch “tcpdump” at your kali command prompt and answer the following questions: (Hint: Using "man" page at the command prompt will give you a detail explanation of the command)

Task 4.3. What command is used to test the available interface in Unix/Linux platform through “tcpdump”?

***Please ensure the network is connected through the NAT mode**

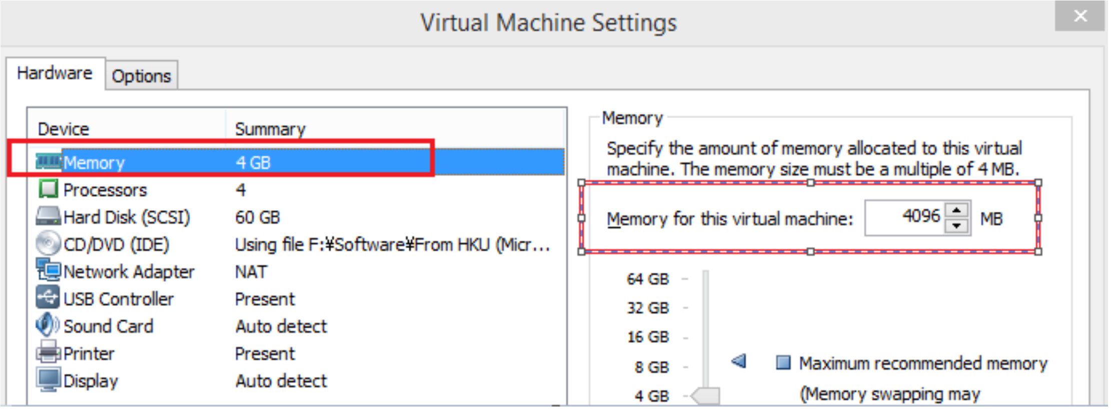
Task 4.2 What command is used to show tcp packet in verbose version using tcpdump?

Task 4.3 What command is used to read in a pcap file in tcpdump?

We are going to use “Wireshark” and “Networkminer” for the following tasks:

Preparation

- Before turn on the Windows 7 VM, change the memory setting to 4096MB
  - ➢ Run **VMware Player** -> Select **Win7 VM** -> Select **VM** tab -> Select **Setting**



Device	Summary
Memory	4 GB
Processors	4
Hard Disk (SCSI)	60 GB
CD/DVD (IDE)	Using file F:¥Software¥From HKU (Micr…
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

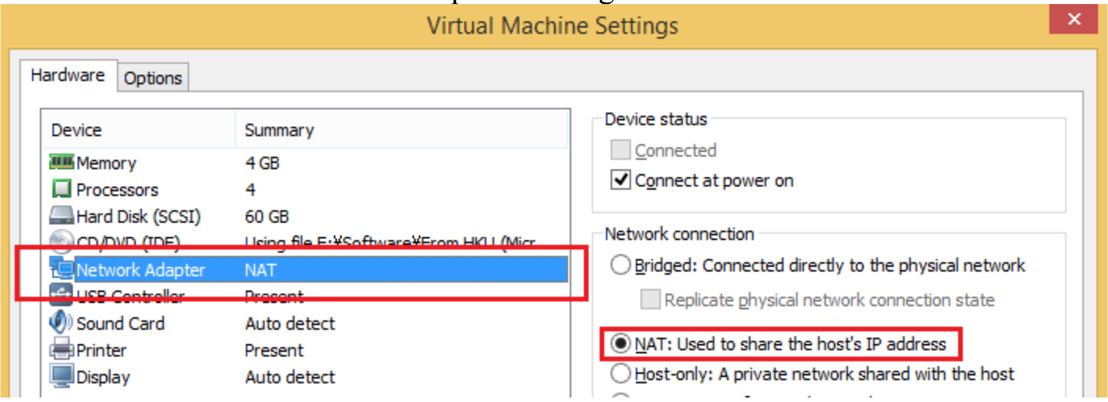
Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 4096 MB

◀ ■ Maximum recommended memory
(Memory swapping may

- Make sure that the network adapter is changed to **NAT** mode.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	4 GB
Processors	4
Hard Disk (SCSI)	60 GB
CD/DVD (IDE)	Using file E:¥Software¥From HKU (Micr
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Network connection

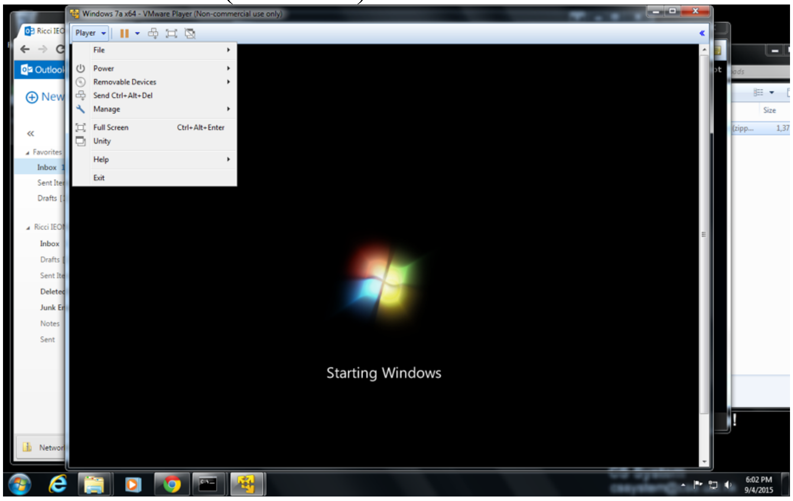
○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

● NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

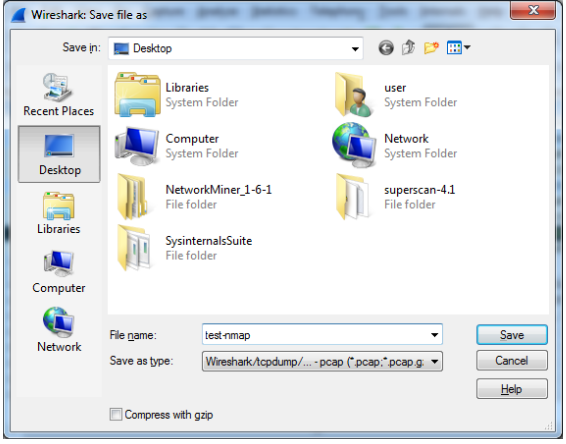
- Login to Windows 7 VM (user: user)



Task 4.4 Run "Wireshark" in Windows. How to select which interface in Wireshark to monitor the traffic between the VMs?

You can simply provide answer in this format: xxxxx -> xxxxx -> xxxxx

- Use "Wireshark" in Windows to capture the network traffic. (try to ping some servers or machines you can connect to)
- Afterwards, save the captured packet in pcap format



Wireshark: Save file as

Save in: Desktop

File name: test-nmap

Save as type: Wireshark/tcpdump/... - pcap (*.pcap;*.pcap.g:

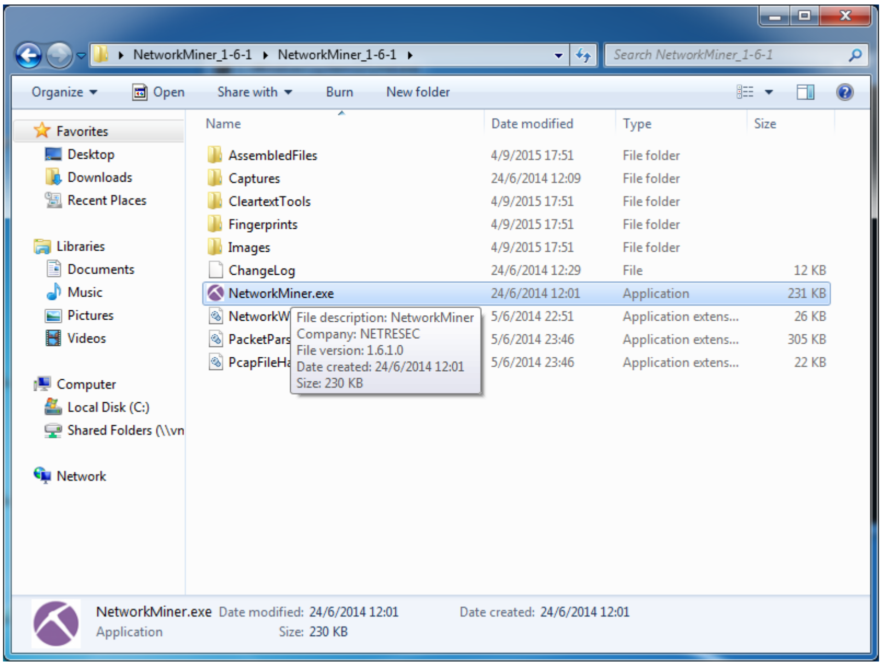
□ Compress with gzip

Task 4.5 Capture the web browsing traffic using Wireshark? How to show only HTTP content in Wireshark?

Capture the network traffic when you browse to web site (e.g. www.cse.ust.hk, www.ust.hk)

Task 4.6 How to capture only HTTP content in Wireshark? What is the difference between this method against Task 4.5?

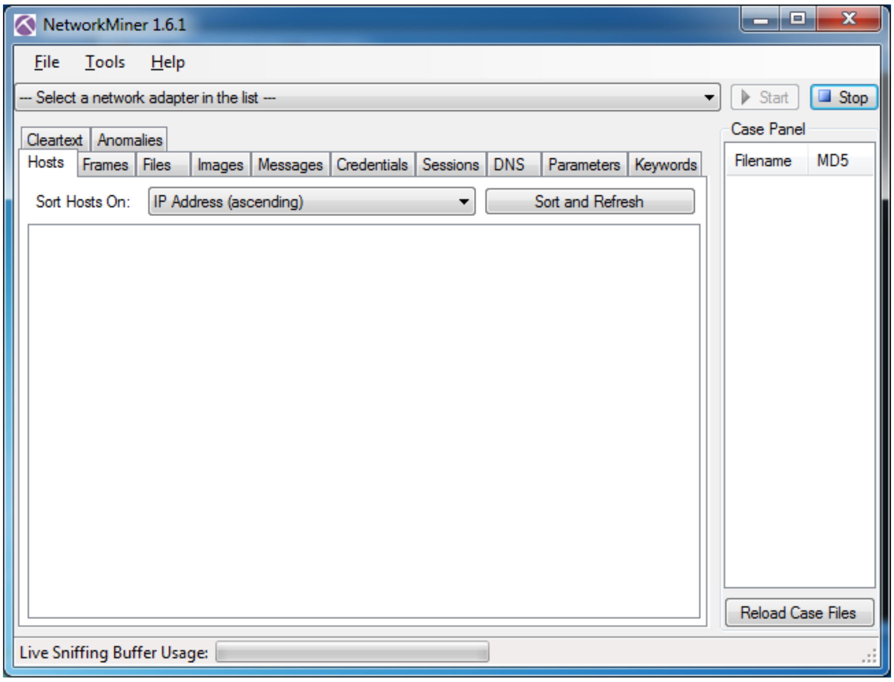
- Install networkminer (http://sourceforge.net/projects/networkminer/)
- After captured the network packets, open the captured network packets in the Networkminer.



Name	Date modified	Type	Size
AssembledFiles	4/9/2015 17:51	File folder	
Captures	24/6/2014 12:09	File folder	
CleartextTools	4/9/2015 17:51	File folder	
Fingerprints	4/9/2015 17:51	File folder	
Images	4/9/2015 17:51	File folder	
ChangeLog	24/6/2014 12:29	File	12 KB
NetworkMiner.exe	24/6/2014 12:01	Application	231 KB
NetworkW	5/6/2014 22:51	Application extens...	26 KB
PacketPars	5/6/2014 23:46	Application extens...	305 KB
PcapFileHa	5/6/2014 23:46	Application extens...	22 KB

File description: NetworkMiner
Company: NETRESEC
File version: 1.6.1.0
Date created: 24/6/2014 12:01
Size: 230 KB

NetworkMiner.exe Date modified: 24/6/2014 12:01 Date created: 24/6/2014 12:01
Application Size: 230 KB



Sort Hosts On: IP Address (ascending)

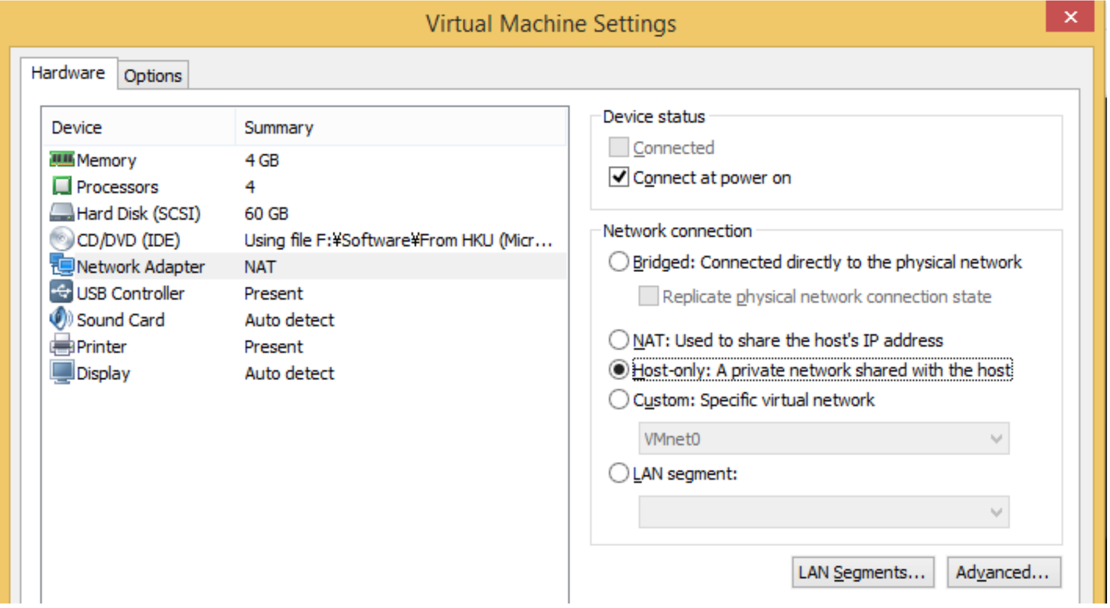
#Bonus Question 1: How can Wireshark and Networkminer determine network traffic streams? (1 mark)

Task 5 – Active Network Information Gathering (Active Footprinting) (30 mins)

Active footprinting requires to touch the device or network. With active footprinting, we may know how big the target network is and some general information about its makeup. However, in contrast with passive footprinting, active footprinting may start setting off alarms of target and actually send alerts and so forth. In this task, we are going to use "Nmap" to perform port scanning which is a kind of active footprinting technique.

Preparation

- Change the network connection of both Windows VM and Kali VM to host-only mode. You may need to reboot the virtual machines.



Device	Summary
Memory	4 GB
Processors	4
Hard Disk (SCSI)	60 GB
CD/DVD (IDE)	Using file F:¥Software¥From HKU (Micr…
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status
□ Connected
☑ Connect at power on

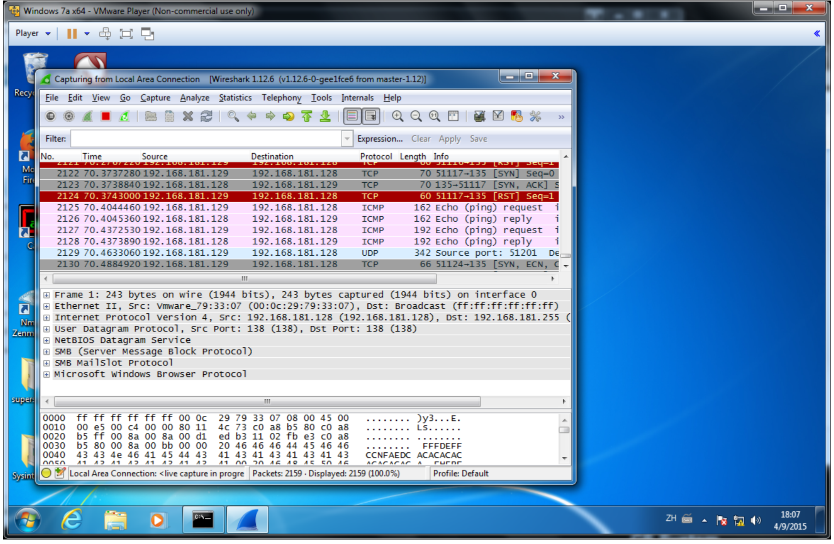
Network connection
○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
○ NAT: Used to share the host's IP address
● Host-only: A private network shared with the host
○ Custom: Specific virtual network
VMnet0
○ LAN segment:

- Check and verify the ip address of the Kali and Windows VM are of the same IP address range.

Launch 'Kali' and windows VM and answer the following questions with 'Nmap' (Reference Website: insecure.org)

Task 5.1 Perform scanning at the target Windows VM with Wireshark enabled and then perform nmap scanning in Kali VM.

- Use Wiresharks to capture the nmap scanning traffic in the Windows VM



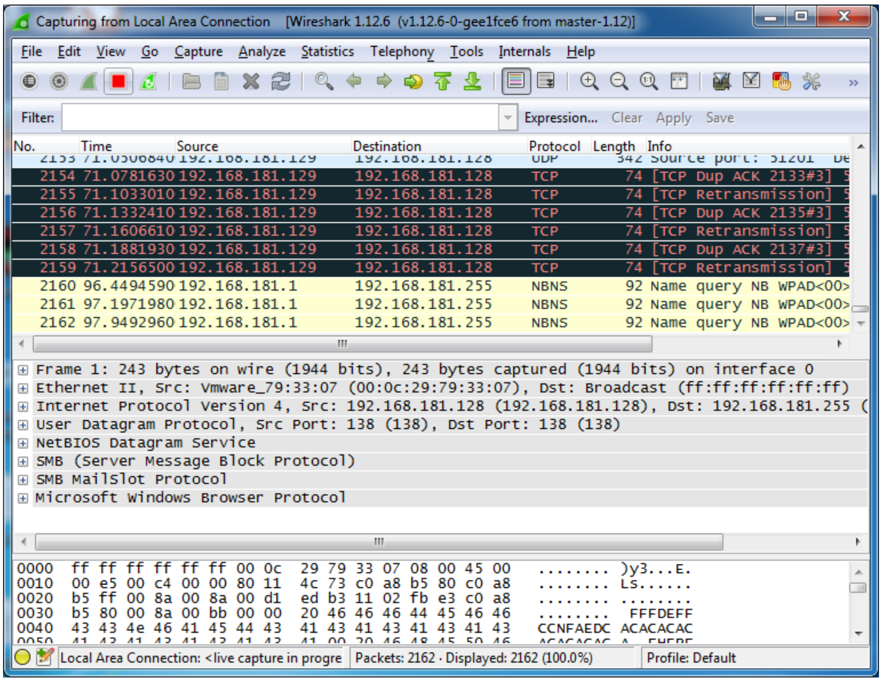
Windows 7a x64 - VMware Player (Non-commercial use only)
Player
Capturing from Local Area Connection [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time       Source          Destination     Protocol Length Info
2122 70.3737280 192.168.181.129 192.168.181.128 TCP        70 51117→135 [SYN] Seq=0
2123 70.3738840 192.168.181.128 192.168.181.129 TCP        70 135→51117 [SYN, ACK] S
2124 70.3743000 192.168.181.129 192.168.181.128 TCP        60 51117→135 [RST] Seq=1
2125 70.4044460 192.168.181.129 192.168.181.128 ICMP      162 Echo (ping) request  i
2126 70.4045360 192.168.181.128 192.168.181.129 ICMP      162 Echo (ping) reply    i
2127 70.4372530 192.168.181.129 192.168.181.128 ICMP      192 Echo (ping) request  i
2128 70.4373890 192.168.181.128 192.168.181.129 ICMP      192 Echo (ping) reply    i
2129 70.4633060 192.168.181.129 192.168.181.128 UDP       342 Source port: 51201  De
2130 70.4884920 192.168.181.129 192.168.181.128 TCP        66 51124→135 [SYN, ECN, C

⊞ Frame 1: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface 0
⊞ Ethernet II, Src: Vmware_79:33:07 (00:0c:29:79:33:07), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 192.168.181.128 (192.168.181.128), Dst: 192.168.181.255 (
⊞ User Datagram Protocol, Src Port: 138 (138), Dst Port: 138 (138)
⊞ NetBIOS Datagram Service
⊞ SMB (Server Message Block Protocol)
⊞ SMB MailSlot Protocol
⊞ Microsoft Windows Browser Protocol

0000  ff ff ff ff ff ff 00 0c  29 79 33 07 08 00 45 00   ........ )y3...E.
0010  00 e5 00 c4 00 00 80 11  4c 73 c0 a8 b5 80 c0 a8   ........ Ls......
0020  b5 ff 00 8a 00 8a 00 d1  ed b3 11 02 fb e3 c0 a8   ........ ........
0030  b5 80 00 8a 00 bb 00 00  20 46 46 46 44 45 46 46   ........  FFFDEFF
0040  43 43 4e 46 41 45 44 43  41 43 41 43 41 43 41 43   CCNFAEDC ACACACAC

Local Area Connection: <live capture in progre | Packets: 2159 · Displayed: 2159 (100.0%) | Profile: Default
```



Capturing from Local Area Connection [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

```
No.    Time       Source            Destination       Protocol  Length  Info
 2153 71.0506840 192.168.181.129   192.168.181.128   UDP          342  Source port: 51201  De
 2154 71.0781630 192.168.181.129   192.168.181.128   TCP           74  [TCP Dup ACK 2133#3] 5
 2155 71.1033010 192.168.181.129   192.168.181.128   TCP           74  [TCP Retransmission] 5
 2156 71.1332410 192.168.181.129   192.168.181.128   TCP           74  [TCP Dup ACK 2135#3] 5
 2157 71.1606610 192.168.181.129   192.168.181.128   TCP           74  [TCP Retransmission] 5
 2158 71.1881930 192.168.181.129   192.168.181.128   TCP           74  [TCP Dup ACK 2137#3] 5
 2159 71.2156500 192.168.181.129   192.168.181.128   TCP           74  [TCP Retransmission] 5
 2160 96.4494590 192.168.181.1     192.168.181.255   NBNS          92  Name query NB WPAD<00>
 2161 97.1971980 192.168.181.1     192.168.181.255   NBNS          92  Name query NB WPAD<00>
 2162 97.9492960 192.168.181.1     192.168.181.255   NBNS          92  Name query NB WPAD<00>
```

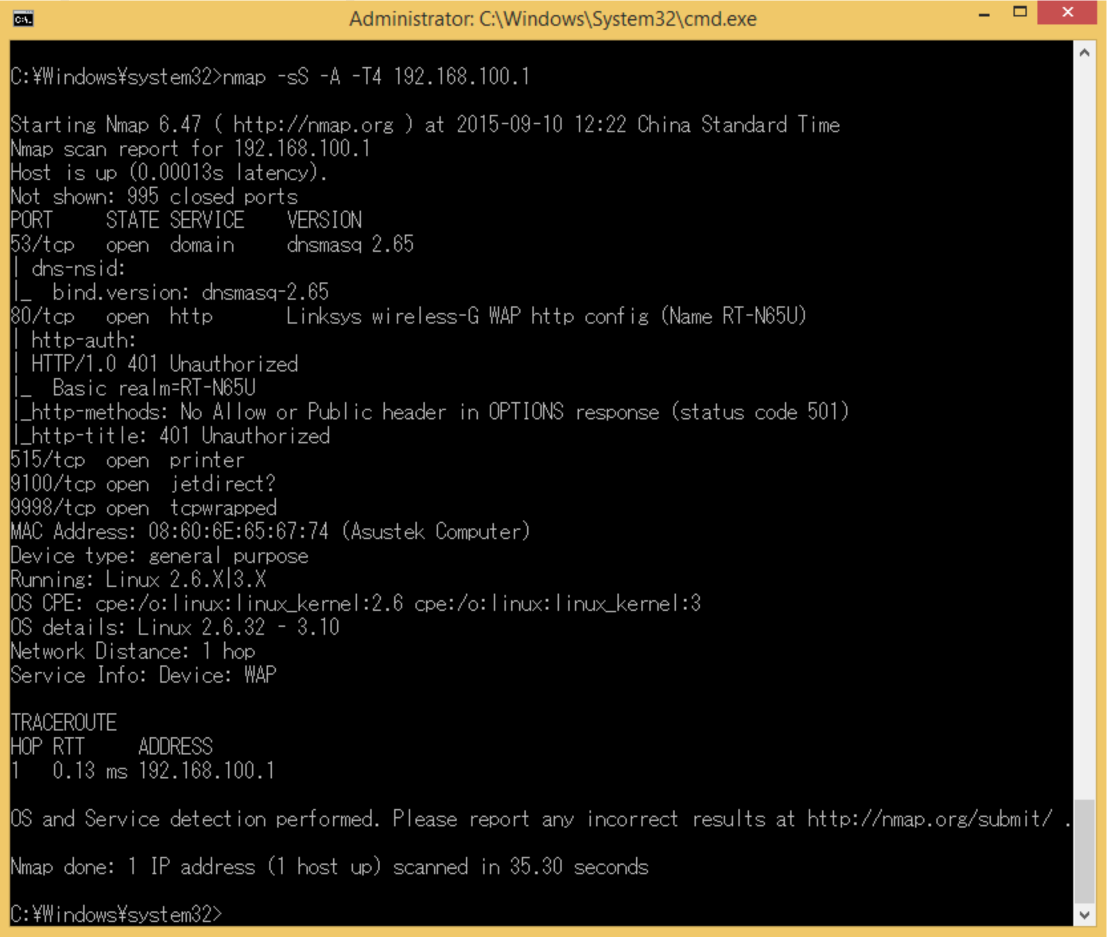
```
⊞ Frame 1: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface 0
⊞ Ethernet II, Src: Vmware_79:33:07 (00:0c:29:79:33:07), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 192.168.181.128 (192.168.181.128), Dst: 192.168.181.255 (
⊞ User Datagram Protocol, Src Port: 138 (138), Dst Port: 138 (138)
⊞ NetBIOS Datagram Service
⊞ SMB (Server Message Block Protocol)
⊞ SMB MailSlot Protocol
⊞ Microsoft Windows Browser Protocol
```

```
0000  ff ff ff ff ff ff 00 0c  29 79 33 07 08 00 45 00   ........ )y3...E.
0010  00 e5 00 c4 00 00 80 11  4c 73 c0 a8 b5 80 c0 a8   ........ Ls......
0020  b5 ff 00 8a 00 8a 00 d1  ed b3 11 02 fb e3 c0 a8   ........ ........
0030  b5 80 00 8a 00 bb 00 00  20 46 46 46 44 45 46 46   ........  FFFDEFF
0040  43 43 4e 46 41 45 44 43  41 43 41 43 41 43 41 43   CCNFAEDC ACACACAC
0050  41 43 41 43 41 43 41 43  41 00 20 46 48 45 50 46   ACACACAC A. FHEPF
```

Local Area Connection: <live capture in progre | Packets: 2162 · Displayed: 2162 (100.0%) | Profile: Default

- Use “Nmap” to perform simple port scanning with the following command in the Kali VM
  - ➢ nmap –sS –A <target IP address>

Sample Result from Nmap



Administrator: C:\Windows\System32\cmd.exe

```
C:¥Windows¥system32>nmap -sS -A -T4 192.168.100.1

Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-10 12:22 China Standard Time
Nmap scan report for 192.168.100.1
Host is up (0.00013s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE    VERSION
53/tcp   open  domain     dnsmasq 2.65
| dns-nsid:
|_  bind.version: dnsmasq-2.65
80/tcp   open  http       Linksys wireless-G WAP http config (Name RT-N65U)
| http-auth:
| HTTP/1.0 401 Unauthorized
|_  Basic realm=RT-N65U
|_http-methods: No Allow or Public header in OPTIONS response (status code 501)
|_http-title: 401 Unauthorized
515/tcp  open  printer
9100/tcp open  jetdirect?
9998/tcp open  tcpwrapped
MAC Address: 08:60:6E:65:67:74 (Asustek Computer)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop
Service Info: Device: WAP

TRACEROUTE
HOP RTT     ADDRESS
1   0.13 ms 192.168.100.1

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 35.30 seconds

C:¥Windows¥system32>
```

## Question 3: What parameters and options to be used in Nmap commands to perform the following tasks? (0.5 mark)
(Hint: Check the manual)

i. SYN scan

ii. Operating system guessing

iii. Port 1-1024

iv. Output txt file

Task 5.2 Perform the following scan at your host machine and determine the characteristic features of various scans

i. TCP SYN

ii. TCP ACK

iii. UDP

iv. TCP Connect

v. TCP XMAS

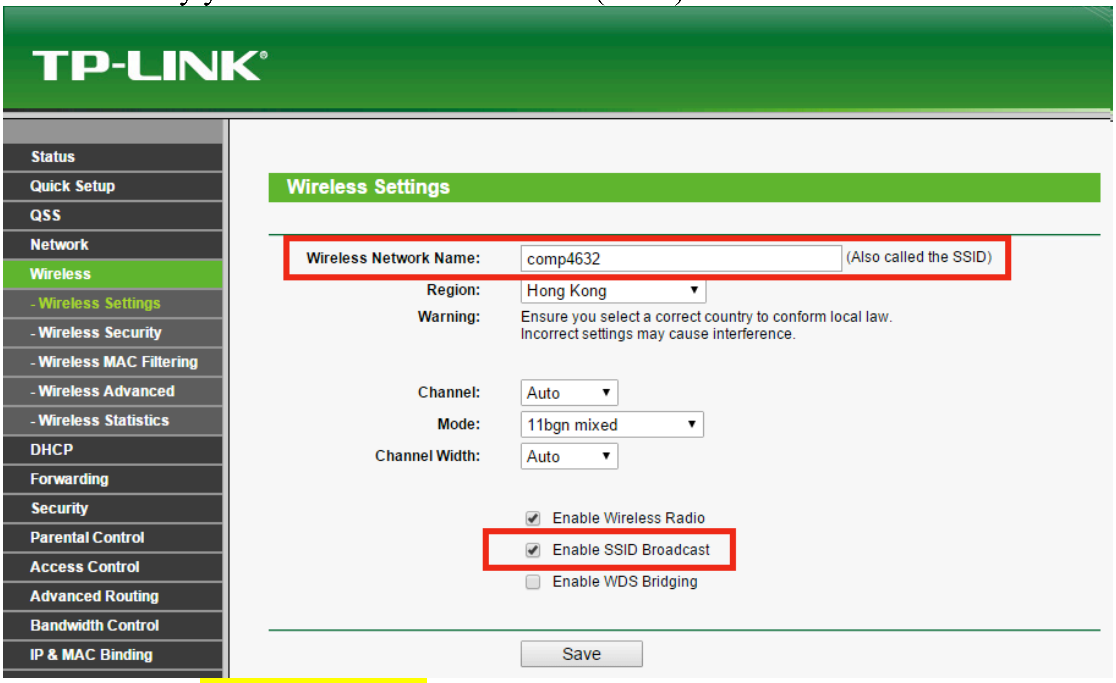
vi. TCP RST

Task 6 – Wireless Setup (20 mins)

Wireless network is almost implemented everywhere nowadays and its security concerns come to all levels of users. The following section is going to introduce the basic security setting for wireless network setup. The demonstration below uses a TP-LINK router as reference, and please be noted that the actual graphical user interfaces (GUI) may be different from your router.

Task 6.1 Setup Wi-Fi with WPA preshared key

- Navigate to your router's management interface via browser
    - Refer to your router's default access (e.g. 192.168.0.1)
- Select Wireless on left navigation panel -> "Wireless Settings"
- Modify your Wireless Network Name (SSID)



Wireless Settings

Wireless Network Name: comp4632 (Also called the SSID)

Region: Hong Kong

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

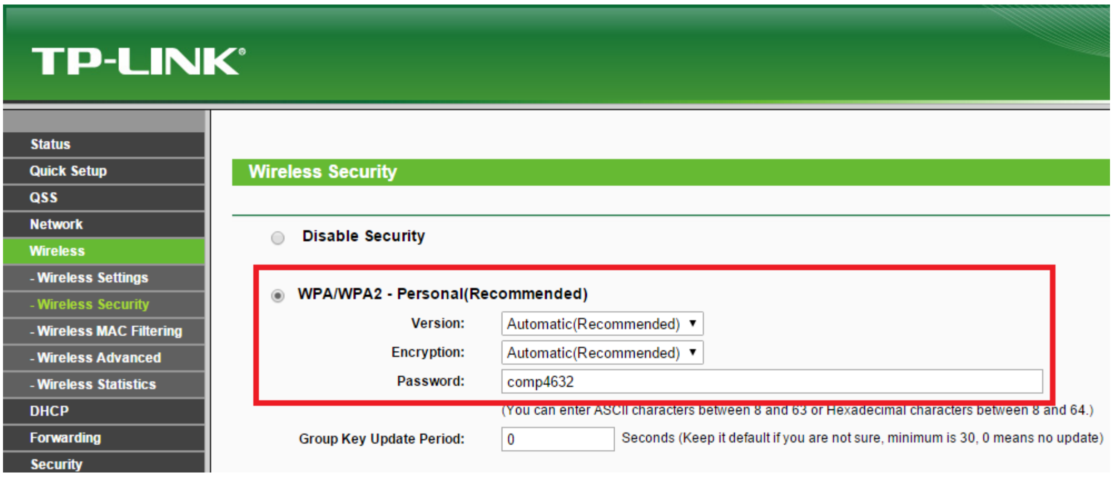
Channel: Auto

Mode: 11bgn mixed

Channel Width: Auto

☑ Enable Wireless Radio
☑ Enable SSID Broadcast
□ Enable WDS Bridging

- Select "Wireless Security" and set the WPA password (Preshared key)



TP-LINK

Wireless Security

○ Disable Security

● WPA/WPA2 - Personal(Recommended)

Version: Automatic(Recommended)

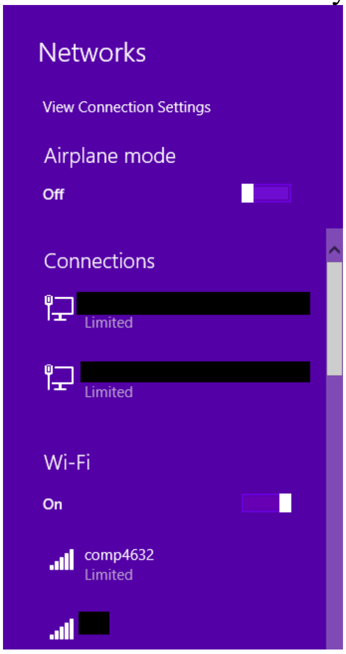
Encryption: Automatic(Recommended)

Password: comp4632

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: 0 Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

- You should be able to detect the Wi-Fi SSID in your PC



Networks

View Connection Settings

Airplane mode

Off

Connections

[redacted]
Limited

[redacted]
Limited

Wi-Fi

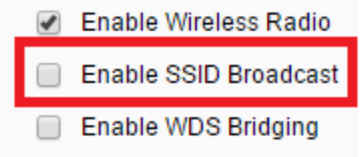
On

comp4632
Limited

[redacted]

Task 6.2 Setup Wi-Fi with hidden SSID

- Uncheck the “Enable SSID Broadcast” in “Wireless Setting”



☑ Enable Wireless Radio

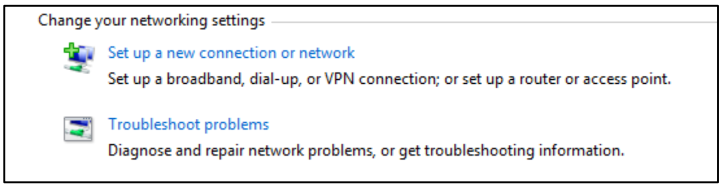
☐ Enable SSID Broadcast

☐ Enable WDS Bridging

- You should not be able to detect the Wi-Fi SSID in your PC normally

Task 6.3 Connect to a Wi-Fi with hidden SSID

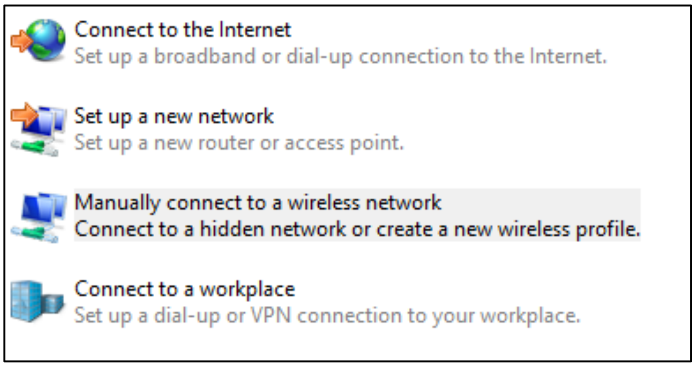
- Go to Network and Sharing Center -> Set up a new connection or network -> Manually connect to a wireless network



Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

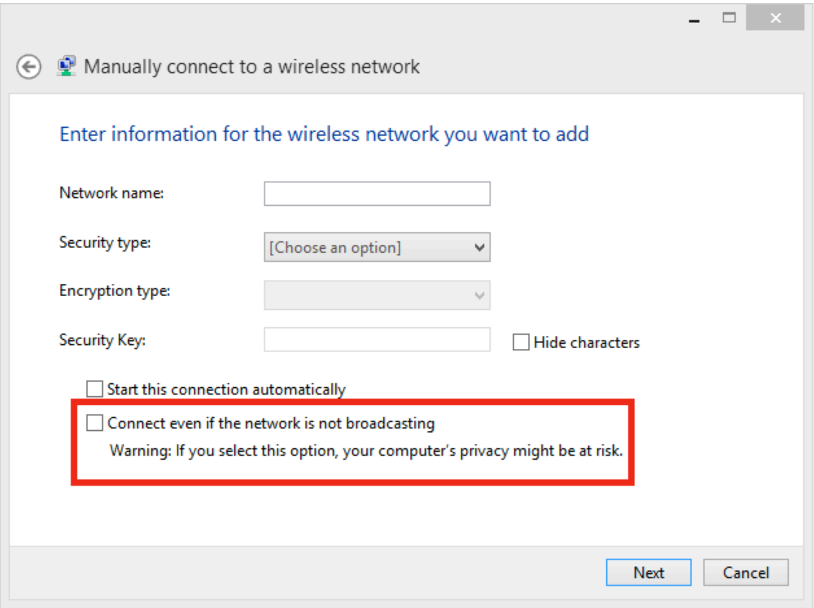


Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type: [Choose an option]

Encryption type:

Security Key: □ Hide characters

□ Start this connection automatically

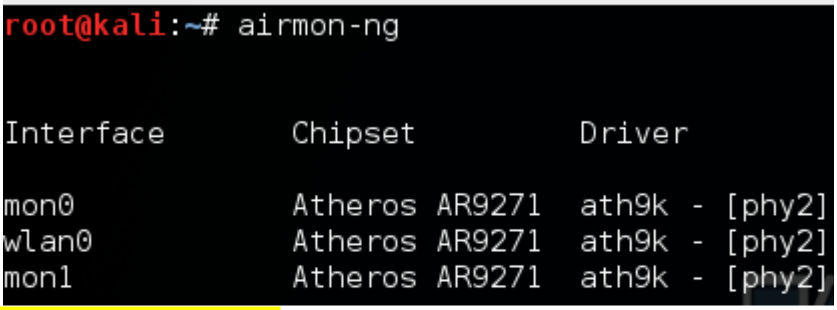
□ Connect even if the network is not broadcasting
Warning: If you select this option, your computer's privacy might be at risk.

- You should be able to connect to the hidden network after the configuration

#Bonus Question 2: If network is not broadcasting, what will be stopped or prevented from being broadcast? (0.5 marks)

Task 6.4 Find out the hidden SSID

- Launch Kali Linux -> Open Terminal
- Run "airmon-ng" in terminal to check available wireless interfaces



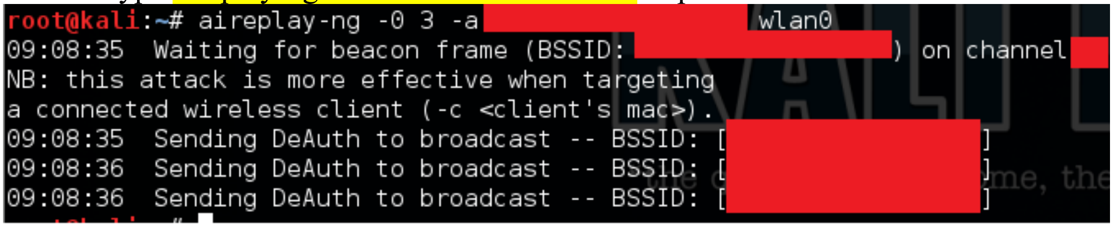
```
root@kali:~# airmon-ng


Interface       Chipset         Driver

mon0            Atheros AR9271  ath9k - [phy2]
wlan0           Atheros AR9271  ath9k - [phy2]
mon1            Atheros AR9271  ath9k - [phy2]
```

- Run airmon-ng start wlan0 to enable monitoring mode on the selected interface
- Run airodump-ng wlan0 to capture the packet of raw 802.11 frames

- Find out the BSSID of the target
- Type aireplay-ng -0 3 –a <BSSID> wlan0 to perform deauthentication



```
root@kali:~# aireplay-ng -0 3 -a [redacted] wlan0
09:08:35  Waiting for beacon frame (BSSID: [redacted]) on channel [redacted]
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
09:08:35  Sending DeAuth to broadcast -- BSSID: [[redacted]]
09:08:36  Sending DeAuth to broadcast -- BSSID: [[redacted]]
09:08:36  Sending DeAuth to broadcast -- BSSID: [[redacted]]
```

- The client will be disconnected and reconnect again
- The SSID will be found in airodump-ng terminal

Task 7. PCAP File analysis exercise

From the pcap file, please answer the following questions:

Task 7.1 Observe the network device and activity performed from the PCAP file

#Bonus question 3: What was the IP address of the scanner? (0.5 mark)

Task 7.2. For the FIRST port scan that scanner conducted, what type of port scan was it?

(Hints: the scan consisted of many thousands of packets.) Select one of the following:

a) TCP SYN

b) TCP ACK

c) TCP Connect

d) TCP XMAS

e) TCP RST

f) UDP

# Bonus question 4: What is the First port scan conducted? (1 mark)

References

[1] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ipconfig.mspx?mfr=true

Web-based checking tools

http://www.checkdomain.com
http://www.traceroute.net
http://www.netcraft.com
http://www.tcpiputils.com
http://www.all-nettools.com/toolbox
http://www.zoneedit.com/lookup.html?ad=whois
http://www.opus1.com/www/traceroute.html
http://shodanhq.com/
http://www.zone-h.org/

http://coffer.com/mac_find/
http://www.nabber.org/projects/geotrace/

Looking Glass web tools
http://lg.eurorings.net/
http://noc.ilan.net.il/LG/
http://lg.cern.ch/
http://www.belwue.de/ueberuns/netz/looking.html
http://drift.uninett.no/cgi-bin/lg.cgi

Entity	**Type of Information**	**Web Site**
Electronic Data Gathering, Analysis, and Retrieval system (EDGAR)	System providing companies information pertaining to registration details, periodic reports, and other activities specific to legal aspects	http://www.sec.gov/edgar.shtml
Glass Door/Simply Hired	Online repositories providing information about companies work culture, jobs including salaries, employees reviews, etc.	http://www.glassdoor.com/ http://www.simplyhired.com/
Name Check/Background Check	Information about usernames and background verification of targets	http://namechk.com/ http://www.advancedbackg-roundchecks.com/
Central Operations/Robtex	Information about domain names, IP address allocation, and registrars	http://centralops.net http://www.robtex.com
Intelius	Public records of individuals	http://www.intelius.com/
Jigsaw/LinkedIn	Employees information	http://www.jigsaw.com/ http://www.linkedin.com/
Spokeo	Personal information such as phone numbers	http://www.spokeo.com/
Hoovers	Corporate information including industry analysis	http://www.hoovers.com/

E-mail Sherlock	Specific e-mail patterns search	http://www.emailsherlock.com/
Pastebin	Underground disclosures, wiki leaks, and sensitive information disclosure from various online attacks	http://pastebin.com/
Github	Source codes and other software centric information	http://www.github.com
Google Dorks Database	Database for finding exposed network devices and servers on the Internet	http://www.hackersforcharity.org/ghdb/ http://www.exploit-db.com/google-dorks/
Google Blogosphere	Content (blog posts) released by the target	http://www.blogspot.com
Pentest Tools	Network information gathering tools repository	http://pentest-tools.com
iSeek	Target information by querying various resources and presenting in graph format	http://iseek.com/
Wigle	Information about WiFi networks	https://wigle.net/
Whois	Details about the registered domains and associated organizations	http://www.internic.net/whois.html
Institute of Electrical and Electronics Engineers (IEEE)	Information about research papers, journals, conferences proceedings, and associated people	http://www.ieee.org/index.html
Internet Assigned Numbers Authority (IANA)	Information about DNS root servers, IP address allocations, and Internet protocol resources	https://www.iana.org/

End of Lab 2