

Cyber laws in Different Countries

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	http://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	http://www.uspto.gov
	The Electronic Communications Privacy Act	https://www.fas.org
	Foreign Intelligence Surveillance Act	https://www.fas.org
	Protect America Act of 2007	http://www.justice.gov
	Privacy Act of 1974	http://www.justice.gov
	National Information Infrastructure Protection Act of 1996	http://www.nrotc.navy.mil
	Computer Security Act of 1987	http://csrc.nist.gov
	Freedom of Information Act (FOIA)	http://www.foia.gov
	Computer Fraud and Abuse Act	http://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	http://www.ftc.gov

Cyber laws in Different Countries

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	http://www.comlaw.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	http://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.saic.gov.cn
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	http://www.dot.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net

Cyber laws in Different Countries

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	http://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	http://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	http://www.laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	http://www.statutes.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	http://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	http://home.heinonline.org
	Industrial Design Protection Act	http://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	http://www.wipo.int
	Computer Hacking	http://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	http://www.mosstingrett.no
Hong Kong	Article 139 of the Basic Law	http://www.basiclaw.gov.hk

Introduction to Network and Cyber Security

Network:

Network is a collection of Computer and Electronic Devices connected to one another to allow sharing of data, files and other computing resources.

The smallest form of Network is LAN (Local Area Network) which is used by small infra organizations for creating Network which then muzzles up to MAN (Metropolitan Area Network) which generally covers a geographical region of the size of a metro area which then lifts up to WAN (Wide area Network).

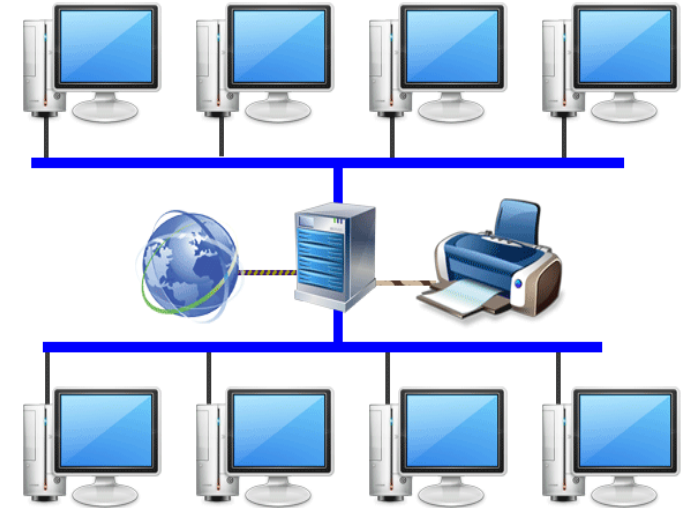
Introduction to Network and Cyber Security

Internet:

Internet is worldwide network of computer networks

How does it work:

- Most computers aren't connected directly to internet
- They are connected to smaller networks
- Which are connected through gateways(Routers/Switches) to the internet backbone



Networking Devices

Network devices are devices used to connect computers or other electronic devices together so that they can share files or resources. These devices move and control network.

Network devices are :

- Network Interface Card
- Switch
- Hub
- Router

Networking Devices



Network Interface Card



Switch



Hub



Router

What is Protocol

- A Protocol is a established set of rules that determine how data is transmitted between different devices in the same network.
- It Defines the Format of Data that is being Sent and Received.
- Some protocols are Designed for Reliable and High-Performance Network communication by Compressing Data.
- Applications like Web Browsers contains a list of software that supports Advance Protocols, necessary for Application to Function.

Introduction to IP Address

- Internet Protocol is a set of rules governing the format of data sent over the internet or the network.
- An IP Address is a 32-bit sequence contains 1's and 0's
- IP is used to identify machines on a network
- IP address consist of four sections
- Each section is 8 bits long
- Each section has range from 0 to 255

Types of IP Address

There are 2 types of IP address

- Static IP Address → IP Address assigned to host manually
- Dynamic IP Address → IP Address assigned by server when host boots

Classification of IP Address

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

Concept of Ports

The term Port can check with either physical or virtual connection points

Example of physical connection port:

Ethernet Port

USB Port

Virtual Port - A port is associated with an IP address of host as well as the type of protocol used for communication. The purpose of ports is uniquely identify different applications or services running on a single computer.

Total number of ports in a computer range from 1 to 65535 (port number 0 is reserved and can't be used)

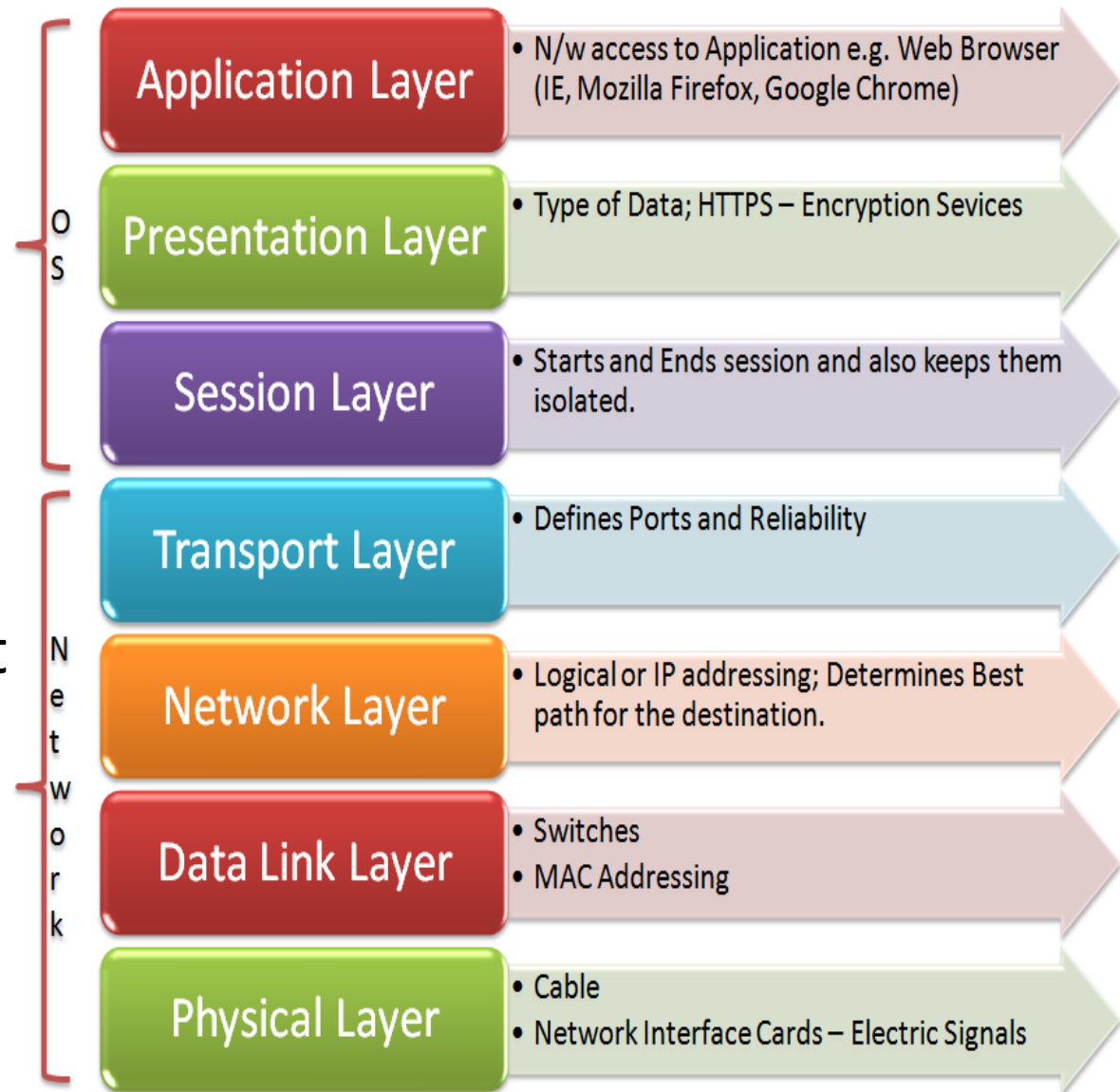
Important Port numbers and Services

ftp	21/tcp	#FTP. control
Ssh	22/tcp	#SSH Remote Login Protocol
telnet	23/tcp	
Smtp	25/tcp	#Simple Mail Transfer Protocol
http	80/tcp	#World Wide Web
kerberos	88/tcp	#Kerberos
pop3	110/tcp	#Post Office Protocol - Version 3
imap	143/tcp	#Internet Message Access Protocol
ldap	389/tcp	#Lightweight Directory Access Protocol
https	443/tcp	#HTTP over TLS/SSL
ftps	990/tcp	#FTP control, over TLS/SSL
telnets	992/tcp	#Telnet protocol over TLS/SSL
imaps	993/tcp	#IMAP4 protocol over TLS/SS

OSI Reference Model

OSI Model:

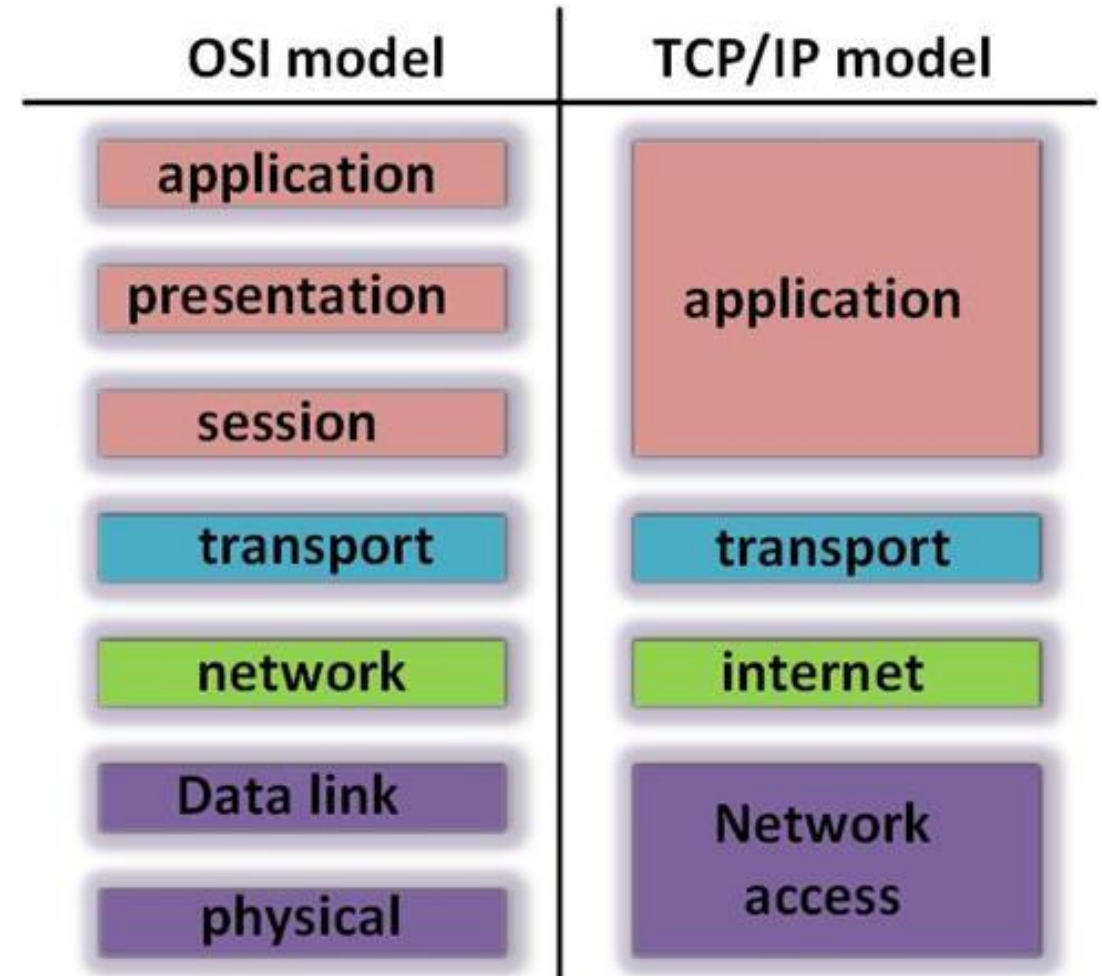
- Open Systems Interconnect (OSI) Model
- Who Made : International standard Organization (ISO)
- OSI isn't a protocol, it's a model for understanding and designing a architecture that's flexible and robust
- The OSI model describes how data flows from one computers, through a network to another computer
- It Consist of 7 Layers



TCP/IP Model

TCP/IP Model:

Networking professionals differ in their opinions on which model to use. Because of the character of the industry it's necessary to become aware of both. Both the OSI & TCP/IP models are going to be mentioned throughout the curriculum. The main target are going to be on the follow: TCP as a OSI Layer 4 protocol IP as a OSI Layer 3 protocol Ethernet as a Layer 2 & Layer 1 technology Remember that there's a difference between a model and an actual protocol that's utilized in networking. The OSI model are going to be used to describe TCP/IP protocols.



Introduction to Kali Linux

- Kali Linux is a Debian based Linux distribution and flavor of Unix OS family
- This OS is maintained and Funded by Offensive Security Limited
- Kali is a Open source and can be download from www.kali.org
- OS is designed for Penetration Testing and Digital Forensics which was developed by Mati Aharoni and Devon Kearns of Offensive Security
- It was Rewrite of Backtrack



Windows / Linux Commands

Below are the list of Basic commands using in Windows / Linux

Ping Command:

This command will help you to know the whether host is live or not

Syntax: ping www.google.com (or) ping <ip>

Administrator: Command Prompt

```
C:\Windows\system32>ping www.google.com

Pinging www.google.com [172.217.167.132] with 32 bytes of data:
Reply from 172.217.167.132: bytes=32 time=24ms TTL=57
Reply from 172.217.167.132: bytes=32 time=15ms TTL=57
Reply from 172.217.167.132: bytes=32 time=15ms TTL=57
Reply from 172.217.167.132: bytes=32 time=15ms TTL=57

Ping statistics for 172.217.167.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 24ms, Average = 17ms

C:\Windows\system32>
C:\Windows\system32>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Windows\system32>
```

```
root@osboxes: ~
root@osboxes:~# ping www.google.com
PING www.google.com (172.217.167.132) 56(84) bytes of data.
64 bytes from www.google.com (172.217.167.132): icmp_seq=1 ttl=57 time=15.3 ms
64 bytes from www.google.com (172.217.167.132): icmp_seq=2 ttl=57 time=15.4 ms
64 bytes from www.google.com (172.217.167.132): icmp_seq=3 ttl=57 time=15.5 ms
^C
--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 15.250/15.394/15.536/0.116 ms
```

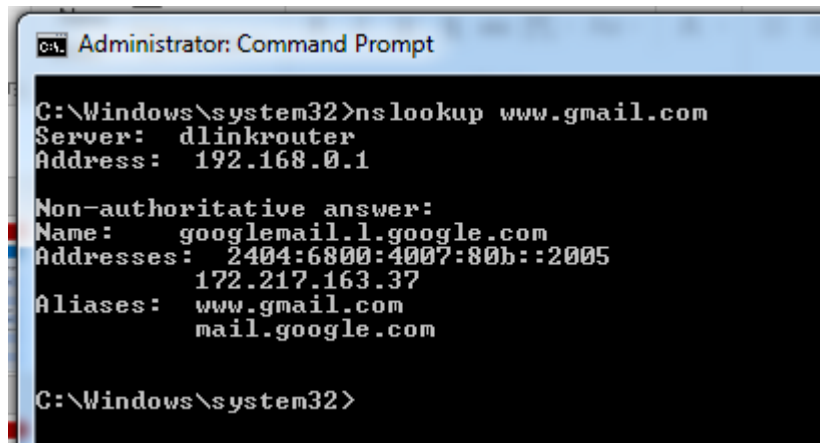
Windows / Linux Commands

Below are the list of Basic commands using in Windows / Linux

nslookup Command:

This command will help you to resolve DNS to IP, let say if you don't know the ip address of website you can use this command

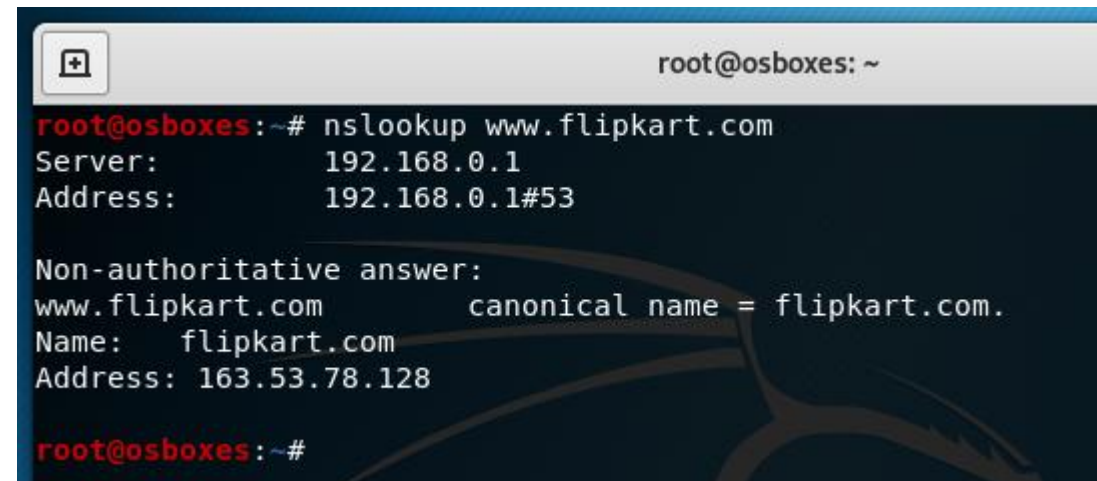
Syntax: nslookup www.google.com



```
C:\Windows\system32>nslookup www.gmail.com
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
Name:     googlemail.l.google.com
Addresses: 2404:6800:4007:80b::2005
          172.217.163.37
Aliases:  www.gmail.com
          mail.google.com

C:\Windows\system32>
```



```
root@osboxes: ~
root@osboxes:~# nslookup www.flipkart.com
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
www.flipkart.com    canonical name = flipkart.com.
Name:   flipkart.com
Address: 163.53.78.128

root@osboxes:~#
```

Windows / Linux Commands

Below are the list of Basic commands using in Windows / Linux

tracert Command:

This command will give you the nodes that packet travels to reach the final destination

Syntax: tracert www.gmail.com (Windows)

Syntax : traceroute www.gmail.com (Linux)

```
Administrator: Command Prompt
C:\Windows\system32>tracert www.learnkarts.com

Tracing route to www.learnkarts.com [172.67.206.91]
over a maximum of 30 hops:
  0  1 ms  <1 ms  <1 ms  dlinkrouter [192.168.0.1]
  1  2 ms  1 ms  1 ms  10.132.0.1
  2  *    *    *    Request timed out.
  3  2 ms  2 ms  2 ms  14.142.71.49.static-hydrabad.vsnl.net.in [14.142.
71.49]
  4  *    *    *    Request timed out.
  5  16 ms  13 ms  12 ms  ix-ae-4-2.tcore1.cxr-chennai.as6453.net [180.87.
36.91]
  6  44 ms  44 ms  44 ms  if-ae-34-2.tcore1.svq-singapore.as6453.net [180.
87.36.41]
  7  112 ms  109 ms  118 ms  120.29.215.101
  8  46 ms  47 ms  59 ms  www.learnkarts.com [172.67.206.91]

Trace complete.
C:\Windows\system32>
```

```
root@osboxes:~# tracert www.learnkarts.com
bash: tracert: command not found
root@osboxes:~# traceroute www.learnkarts.com
traceroute to www.learnkarts.com (172.67.206.91), 30 hops max, 60 byte packets
 1 dlinkrouter (192.168.0.1)  0.805 ms  0.950 ms  2.007 ms
 2 * * *
 3 * * *
 4 * * *
 5 14.142.71.49.static (14.142.71.49)  4.787 ms  4.715 ms  14.142.71.205.static-
hydrabad.vsnl.net.in (14.142.71.205)  4.855 ms
 6 * * *
 7 ix (180.87.36.9)  24.475 ms  24.411 ms  24.350 ms
 8 if (180.87.36.41)  47.968 ms  46.731 ms  46.858 ms
 9 120.29.215.101 (120.29.215.101)  115.507 ms  112.347 ms  113.766 ms
10 www.learnkarts.com (172.67.206.91)  45.538 ms  46.688 ms  46.621 ms
root@osboxes:~#
```


Windows / Linux Commands

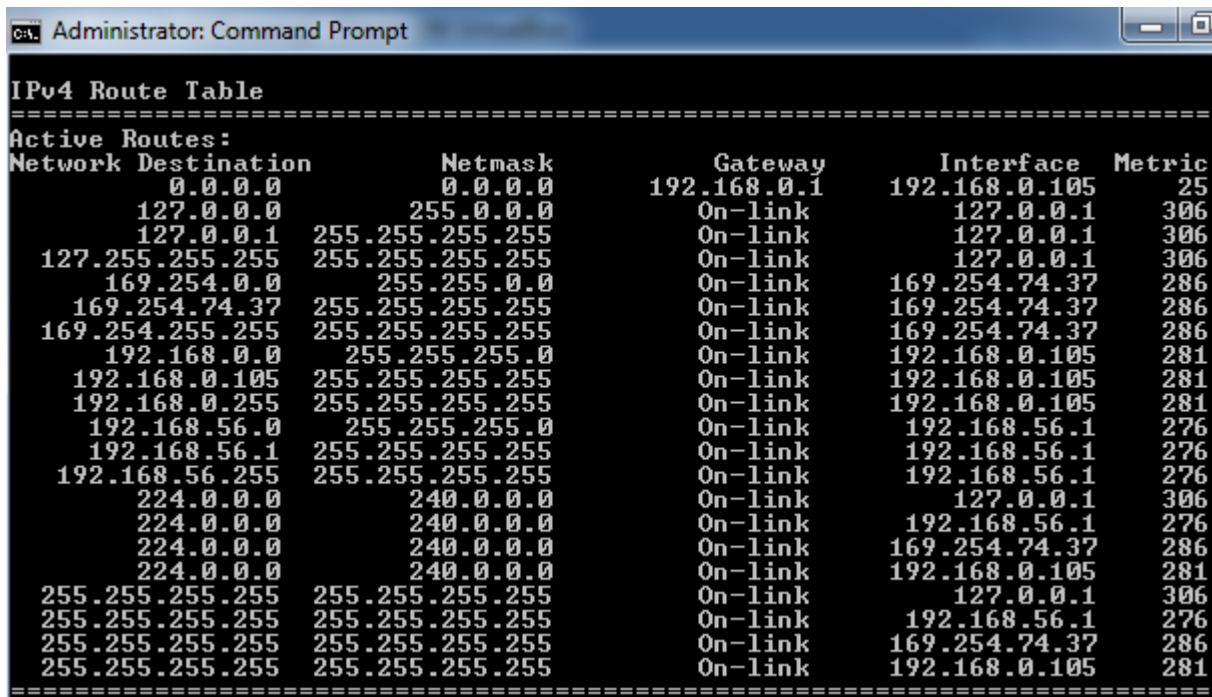
Below are the list of Basic commands using in Windows / Linux

route Command:

This command will give you the routing table , gateways, interfaces and metric of host in a network

Syntax: route print (Windows)

Syntax : route (Linux)



Administrator: Command Prompt

IPv4 Route Table

=====

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.105	25
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
	169.254.0.0	255.255.0.0	On-link	169.254.74.37	286
169.254.74.37	255.255.255.255	255.255.255.255	On-link	169.254.74.37	286
169.254.255.255	255.255.255.255	255.255.255.255	On-link	169.254.74.37	286
	192.168.0.0	255.255.255.0	On-link	192.168.0.105	281
192.168.0.105	255.255.255.255	255.255.255.255	On-link	192.168.0.105	281
192.168.0.255	255.255.255.255	255.255.255.255	On-link	192.168.0.105	281
	192.168.56.0	255.255.255.0	On-link	192.168.56.1	276
192.168.56.1	255.255.255.255	255.255.255.255	On-link	192.168.56.1	276
192.168.56.255	255.255.255.255	255.255.255.255	On-link	192.168.56.1	276
	224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	240.0.0.0	On-link	192.168.56.1	276
224.0.0.0	240.0.0.0	240.0.0.0	On-link	169.254.74.37	286
224.0.0.0	240.0.0.0	240.0.0.0	On-link	192.168.0.105	281
255.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	255.255.255.255	On-link	192.168.56.1	276
255.255.255.255	255.255.255.255	255.255.255.255	On-link	169.254.74.37	286
255.255.255.255	255.255.255.255	255.255.255.255	On-link	192.168.0.105	281

=====



```
root@osboxes:~# route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
default          dlinkrouter    0.0.0.0         UG    100    0      0 eth0
192.168.0.0      0.0.0.0        255.255.255.0   U     100    0      0 eth0
root@osboxes:~#
```

Windows / Linux Commands

Below are the list of Basic commands using in Windows / Linux

Ipconfig / ifconfig Command:

This command will show you ip address of host and gateway, DNS etc.

Syntax: ipconfig(Windows)

Syntax : ifconfig (Linux)

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::91c2:96db:72f6:236e%13  
IPv4 Address. . . . . : 192.168.0.105  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.0.1
```

```
root@osboxes:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.0.106 netmask 255.255.255.0 broadcast 192.168.0.255  
    inet6 fe80::2fd3:d6ce:faf5:2f2d prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:c2:2c:cc txqueuelen 1000 (Ethernet)  
    RX packets 13347 bytes 18199473 (17.3 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 9000 bytes 677033 (661.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 23 bytes 1292 (1.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 23 bytes 1292 (1.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Windows / Linux Commands

Below are the list of Basic commands using in Windows / Linux

Netstat Command:

This command will show you all statistics of network which are connected to host

Syntax: netstat -an

this will combined both of the above

```
C:\Windows\system32>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135               0.0.0.0:0               LISTENING
TCP    0.0.0.0:445               0.0.0.0:0               LISTENING
TCP    0.0.0.0:1025              0.0.0.0:0               LISTENING
TCP    0.0.0.0:1026              0.0.0.0:0               LISTENING
TCP    0.0.0.0:1027              0.0.0.0:0               LISTENING
TCP    0.0.0.0:1028              0.0.0.0:0               LISTENING
TCP    0.0.0.0:1055              0.0.0.0:0               LISTENING
TCP    0.0.0.0:1067              0.0.0.0:0               LISTENING
TCP    0.0.0.0:2869              0.0.0.0:0               LISTENING
TCP    0.0.0.0:7070              0.0.0.0:0               LISTENING
TCP    0.0.0.0:54796             0.0.0.0:0               LISTENING
TCP    127.0.0.1:1037            0.0.0.0:0               LISTENING
TCP    127.0.0.1:1040            127.0.0.1:28918        ESTABLISHED
TCP    127.0.0.1:1041            0.0.0.0:0               LISTENING
TCP    127.0.0.1:1048            0.0.0.0:0               LISTENING
TCP    127.0.0.1:2869            127.0.0.1:3324          TIME_WAIT
TCP    127.0.0.1:2869            127.0.0.1:3325          TIME_WAIT
TCP    127.0.0.1:3332            127.0.0.1:5037          SYN_SENT
```

```
root@osboxes:~# netstat -an

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:68              0.0.0.0:*
raw6       0      0 :::58                    :::*                    7

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type        State         I-Node      Path
unix 2      [ ACC ]     STREAM     LISTENING     22113       @/tmp/dbus-p0dS4AJD
unix 2      [ ACC ]     STREAM     LISTENING     22177       /tmp/.X11-unix/X1
unix 2      [ ACC ]     STREAM     LISTENING     16704       /tmp/.X11-unix/X0
unix 2      [ ACC ]     STREAM     LISTENING     17659       /tmp/.ICE-unix/542
unix 2      [ ACC ]     STREAM     LISTENING     22365       /tmp/ssh-0GQFbXc3R5nQ/agent.1053
unix 2      [ ACC ]     STREAM     LISTENING     22639       /tmp/.ICE-unix/1053
unix 2      [ ACC ]     SEQPACKET  LISTENING     11030       /run/udev/control
unix 2      [ ]       DGRAM      LISTENING     11033       /run/systemd/journal/syslog
unix 2      [ ACC ]     STREAM     LISTENING     22638       @/tmp/.ICE-unix/1053
unix 16     [ ]       DGRAM      LISTENING     11039       /run/systemd/journal/dev-log
unix 2      [ ACC ]     STREAM     LISTENING     16099       @/tmp/dbus-cMk4TbQe
unix 2      [ ACC ]     STREAM     LISTENING     22049       /run/user/0/keyring/control
unix 2      [ ACC ]     STREAM     LISTENING     16703       @/tmp/.X11-unix/X0
```

Windows / Linux Commands

Below are the list of Basic commands using in Windows / Linux

Netuser Command:

This command will show you user account in a system

Syntax: net user (windows)

Syntax: cat /etc/passwd (Linux)

In Linux passwd file stores all the local user accounts in host

```
Administrator: Command Prompt
C:\Windows\system32>net user
User accounts for \\VISHWA-PC

-----
Administrator      Guest              vishwa
The command completed successfully.

C:\Windows\system32>
```

```
root@osboxes:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```


Different OS for hacking Environments

To Learn Ethical Hacking we need to have basics knowledge of different operating system. In our Course will going to use Windows / Kali Linux

Operating Systems:

