Workshop Task – Command Line Familiarisation B

Networking utilities

Note: Use command line for this exercise. For Windows – go to Start > Programs > Accessories > Command prompt – and click on the icon to open OR click the Start button and type *cmd* in the search field.

Ipconfig (**`ipconfig`** for Windows and **`ifconfig`** for Linux)
Internet protocol configuration is a utility used to display all the current values of the host's TCP/IP network configuration.

Try
`ipconfig`

ipconfig flags

Flag	Description
/?	Displays help on ipconfig
/all	*Display full configuration information.*
/release	*Release the IP address for the specified adapter*
/renew	*Renew the IP address for the specified adapter*
/flushdns	*Purges the DNS Resolver cache*
/registerdns	*Refreshes all DHCP leases and re-registers DNS names*
/displaydns	*Display the contents of the DNS Resolver Cache*
/showclassid	*Displays all the dhcp class IDs allowed for adapter*
/setclassid	*Modifies the dhcp class id*

Ping

Ping is a utility used to test the reachability of a networked object (host or IP) and to measure the round-trip time of messages from sender to receiver. It sends ICMP (internet control message protocol) echo request packets to the target object and receives an ICMP echo reply. Returned statistics also include TTL (time to live – number of hops after which probe is discarded). So if TTL = 126, you can't ping a host 127 hops away from you.

e.g., two computers on a network cannot communicate if they can't ping each other. Are there any exceptions?

Try

```
ping www.chester.ac.uk
ping 195.195.128.100
```

Enter *195.195.128.100* on any browser. What do you see?

ping flags

Flag	Description
/?	Displays help on ping
-t	Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C
-a	Resolve addresses to hostnames
-n count	Number of echo requests to send
-l size	Send buffer size
-f set	Don't Fragment flag in packet
-i TTL	Time To Live
-v TOS	Type Of Service.
-r count	Record route for count hops.
-s count	Timestamp for count hops.
-j host-list	Loose source route along host-list.
-k host-list	Strict source route along host-list.
-w timeout	Timeout in milliseconds to wait for each reply.

Trace route (`tracert` for Windows and `traceroute` for Linux)

A diagnostic tool used to display a route or path to a particular destination and to measure the associated timing information (delays).

Try

```
tracert www.chester.ac.uk
tracert www.yahoo.com
tracert www.bbc.co.uk
tracert 195.195.128.100
```

tracert flags (for Windows)

Flag	Description
/?	Displays help on tracert
-d	Do not resolve addresses to hostnames
-h maximum_hops	Maximum number of hops to search for target
-j host-list	Loose source route along host-list
-w timeout	Wait timeout milliseconds for each reply

Netstat (network statistics)

Find out about this one

netstat flags

Flag	Description
/?	Displays help on netstat
-a	Displays all connections and listening ports
-b	Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.
-e	Displays Ethernet statistics. This may be combined with the -s option.
-n	Displays addresses and port numbers in numerical form
-o	Displays the owning process ID associated with each connection
-p protocol	Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, protocol may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-r	Displays the routing table
-s	Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
-v	When used in conjunction with -b, will display sequence of components involved in creating the connection or listening port for all executables
interval	Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once

Exercise

1. Open the command prompt and type – **`ipconfig /all`** (for Windows)
   i. What is the MAC address of the PC you are using?
   ii. What is the IP address of the PC you are using?
   iii. What is the name of your default gateway?
   iv. What other information is displayed?
   v. What is hierarchy of the DNS lookup?
   vi. Compare the information you obtain with that of your neighbour. Is it the same or different?
   vii. Can you view the same information using - Control Panel and Network Connections?

2. Type **`netstat -a`**
   i. Discuss your result

3. Using ARP
   i. Try the following using the command prompt:- type **`arp -a`**

ii. Try using help with a command **`arp -?`**

a. Discuss your finding

b. Is the information displayed useful to a hacker?