# Commands

## ifconfig

* -a display all interfaces which are currently available, even if down
* -s display a short list (like netstat -i)
* -v be more verbose for some error conditions

# IP

* -V, -Version Print the version of the IP utility and exit.
* -h, -human, -human-readable output statistics with human readable values followed by suffix.
* -b, -batch <FILENAME>= Read commands from provided file or standard input and invoke them. First failure will cause termination of IP.
* -force Don't terminate IP on errors in batch mode. If there were any errors during execution of the commands, the application return code will be non-zero.
* -s, -stats, -statistics Output more information. If the option appears twice or more, the amount of information increases. As a rule, the information is statistics or some time values
* -d, -details Output more detailed information.

# Listing File Permissions

* Ls -altr <file name/extension> This will display all file permissions along with when and who it was create by and file size.
* File permissions are an 8-bit set of data
* 0 – no permission
* 1 – execute
* 2 – write
* 3 – write and execute
* 4 – read
* 5 – read and execute
* 6 – read and write
* 7 – read, write, and execute

# File Editing

## Touch

* Touch file1 | Used to create, change, and modify files.

## Gedit

Used for editing documents within a GUI

## Vim

Like Gedit, used for editing documents within a GUI. This is less resource heavy, however. I to insert text, ESC to stop editing, :q! to quit without saving and :wq! To quit with saving.

## Nano <File Name>

Used to create and modify files In a GUI format, like both Gedit and vim. In-between vim and Gedit on resource usage and works more like vim using keyboard commands and no mouse input.

# Zipping Files

## 7zip

* 7z a <file.7z> <file to be zipped> | Zipping the File
* 7z e <file.7z> | Extracting the file

# Creating a file hash

## XXD

* Xxd <filename> | produces a file hash based on file contents

# Extracting Metadata

Exiftool <Filename.Extension>

# Google Dorking

Dorking techniques are used to expose credentials and information.

## Searching through websites

Site:port.ac.uk

## Finding Exposed Documents

Site:port.ac.uk ext:doc| ext:docx | ext:odt | ext:rtf | ext:sxw | ext:psw | ext:ppt | ext:csv

## Finding Directory Listings

site:port.ac.uk intitle:index.of

## Finding login pages

site:port.ac.uk inurl:login | inurl:signin | intitle:Login | intitle:"sign in" | inurl:auth

## Finding Config Files

site:port.ac.uk ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf | ext:rdp | ext:cfg | ext:txt | ext:ora | ext:ini | ext:env

## Finding Database Files

site:port.ac.uk ext:sql | ext:dbf | ext:mdb

## Searching public storage sites

site:pastebin.com | site:paste2.org | site:pastehtml.com | site:slexy.org | site:snipplr.com | site:snipt.net | site:textsnip.com | site:bitpaste.app | site:justpaste.it | site:heypasteit.com | site:hastebin.com | site:dpaste.org | site:dpaste.com | site:codepad.org | site:jsitor.com | site:codepen.io | site:jsfiddle.net | site:dotnetfiddle.net | site:phpfiddle.org | site:ide.geeksforgeeks.org | site:repl.it | site:ideone.com | site:paste.debian.net | site:paste.org | site:paste.org.ru | site:codebeautify.org  | site:codeshare.io | site:trello.com "port.ac.uk"

## Searching repositories

site:stackoverflow.com "port.ac.uk"

## Finding Routers

intitle:"SpeedStream Router Management Interface"

inurl:”level/15/exec/-/show”

## Network Cameras

intitle:"Device(" AND intext:"Network Camera" AND "language:" AND "Password"

# Domain Name System (DNS) Enumeration

## ping -c 4 google.com

Packet InterNet Groper (PING), used for testing for network connectivity. The -c option specifies the number of ECHO request packets

## traceroute port.ac.uk

We can also trace the route that packets take to reach its destination We can query Internet Name Servers for information about hosts and domains using the nslookup tool.

## nslookup port.ac.uk

Name server, registrar, and, in some cases, full contact information about a domain name can be found in a Whois database. Each registrar must maintain a Whois database containing all contact information for the domains they host. A central registry Whois database is maintained by the [InterNIC](http://www.internic.net/). We can use the whois client tool to access the Whois server via TCP port 43.

## whois port.ac.uk

## We can also perform reverse lookups

## whois 148.197.254.1

The host command is a DNS lookup utility.

## host port.ac.uk

Use it to discover both the DNS and mailservers.

#### host -t ns port.ac.uk ## ns == nameserver

#### host -t mx port.ac.uk ## mx == mailserver

Forward Lookup Brute Force

For the next part, we will automate the Forward DNS Lookup of common hostnames by writing a bash script.

Create a text file that contains common hostnames e.g.

## echo -e 'www\nftp\nmail\nsoc\nicg\nicp' > list.txt

We will write simple bash one liner that runs the host command on every item in the list

## for ip in $(cat list.txt);do host $ip.port.ac.uk;done

Reverse Lookup Brute Force

We can also probe the range of IP addresses that were found during our forward lookup. We will employ the use of Bash scripting again.

## for ip in $(seq 1 254);do host 148.197.8.$ip;done |grep -v "not found"

##We use seq to generate a range between 1 to 254

## We use grep -v to remove instances where the information was not found