1. tracert <ip>
   1. route of packets and to find ips/locations where they are dropped
2. chmod <permissions> <file>
   1. example uses:
      1. chmod 644 file.txt
         1. sets file permissions (6 – owner can read and write, 4 – group can only read, 4 – others can only read)
         2. same can be achieved with – chmod u=rwx, g=rx, o=rx file.txt
         3. chmod 777 file.txt will give everyone access to this file.
3. nslookup <ip/domain> OR dig (linux)
   1. displays information that can be used to diagnose DNS infrastructure
      1. Two modes
         1. Interactive
         2. Non-interactive
4. tcpdump –i <interface> <protocol> <port>
   1. linux command only
   2. example use
      1. tcpdump –I eth1 tcp port80
         1. this dumps all captured traffic from eth1 on tcp port 80
5. netsh advfirewall firewall
   1. use this command to add or delete firewall rules
   2. example uses:
      1. To enable/disable a program
         1. netsh advfirewall firewall add rule name=<”anyname”> dir=<in or out> action=<allow/block> program=<”path to program”> enable=<yes/no>
      2. To enable/disable a port
         1. netsh advfirewall firewall add rule name=<”anyname”> dir=<in or out> action=<allow/block> protocol=<protocol> localport=<port>
      3. To delete enabled programs or ports
         1. netsh advfirewall firewall delete rule name=<rulename> program=<path-to-program>
         2. netsh advfirewall firewall delete rule name=<rulename> protocol=<protocol> localport=<port>
      4. To enable specific services
         1. Netsh advfirewall firewall set rule group=<”group name”> new enable=<Yes/No>
            1. Netsh advfirewall firewall set rule group=”File and Printer Sharing” new enable=Yes
            2. Netsh advfirewall firewall set rule group=”remote desktop” new enable=Yes
6. netstat
   1. Provides network statistics and other information
      1. To show active connections
         1. netstat –a
      2. Show binaries / Show associated programs associated with connections
         1. netstat –b
      3. Do not resolve domain names
         1. netstat –n
      4. Show connection PIDs
         1. netstat -o
7. netcat or nc
   1. reads or writes to a network
      1. Can listen on port, transfer data, scan ports and send data to port
         1. Check whether a port is open
            1. nc –v <ip or domain> <port>
         2. Port scanning
            1. nc –vzu <ip or domain> <port range>
         3. Listening server
            1. nc –l <any-non-used-port>

To establish connection to the listening server above, use:

nc <ip on machine that ran nc –l cmd > <port>

* + - 1. Transfer a file
         1. On a server, open a listener like in step(3) but attached an output file to save all data received by the port.

ex. nc –l 4444 > output

* + - * 1. On another machine, make or use existing file and send contents of the file to listening server with:

cat file | nc <listening server IP> <port>

If using the example above, it would look like this: cat filename | nc –l 192.168.0.1 4444

This will transfer all contents from file to output on listening server

* + - 1. Binding program to port and access it
         1. Bind CMD program to the port number (SERVER)

nc –nlvp <port> -e <program>

ex. nc –nlvp 4444 –e cmd.exe

* + - * 1. Establish connection with a server ( CLIENT )

nc –nv <ip> <port>

nc –nv 192.168.0.1 4444

* + - * 1. These commands will open a command prompt of the server from the client machine.

1. arp –a
   1. view local ARP(Address Resolution Protocol) table
2. ipconfig(windows) OR ifconfig(linux)
   1. Shows TCP/IP and network adapter information.
   2. ipconfig /all
      1. shows more indepth information such as MAC addresses, DNS servers etc..
3. nmap
   1. used for mapping, port scanning, operating system scan, services scan
   2. examples of common nmap commands:
      1. nmap <IP or Host>
      2. nmap –p <port/portrange> <ip>
      3. nmap –A <ip> - this is for detecting OS and Services
      4. nmap –sV <ip> - Standard service detection
      5. nmap –sV –version-intensity <1-5> <ip> - Aggressiveness of service detection
      6. nmap –sV –sC <ip> - Scan using default safe scripts
      7. nmap –script-help=<script-name> - Get help with a script
      8. nmap –sV –p <port> -script=<script-name.nse> <ip> - Scan using specific NSE script
      9. nmap -p- <host> OR nmap –p0-65535 –T5 – Scan all ports with threads
      10. nmap –sU –sT –p-65535 <host> - Scans all TCP and UDP ports
      11. nmap –script <”exploit”> -p- <host> - Scan all ports to find vulnerabilities aggressively
      12. nmap –sV –script=<script-name\*> <ip> - Scan with a set of scripts “\*”
      13. nmap –script=asn-query,whois,ip-geolocation-maxmind <ip> - Scan to find information about IP address
      14. USE –T1-5 to scan with more threads (faster)
4. pathping
   1. combination of ping and traceroute
      1. First phase runs traceroute
      2. Second phase finds round-trip time and packet loss
5. cat
   1. view contents of a file, create a new file, combine two files into one etc.
      1. cat <filename>
      2. cat > <newfile>
      3. cat <file-name-of-file-to-be-copied> > <destination-filename>
      4. cat <file-which-contents-will-be-appended> >> <file-which-will-be-the-appendee>
   2. can also be used to view contents of file in reverse by using:
      1. tac <filename>
6. grep
   1. Searches for a string in groups of files
      1. Example uses:
         1. grep <”string”> <filename.ext>
            1. grep “mellon” myfile.txt
         2. Common flags
            1. –E – run grep with extended regular expressions
            2. –i – ignore case
            3. –v – return all lines which don’t match the pattern
            4. –w – only matches that form whole words
            5. –c – print count of matching lines
            6. –l – print the name of each file which contains match
            7. –n – print the line number before each line that matches
            8. –r – recursively read all files in given directory and subdirectories