1. What LPIC certifications are, how they can help you.
2. General overview of LPIC 2
    1. Commands for troubleshooting, capacity planning
        1. Iostat - shows system input/output and can troubleshoot failing harddrives, failing swap, bad ram, throughput bottlenecks. It shows two different reports, CPU utilization, and a device report. When first run it shows the average input/output average since boot. After that, it will run every X seconds, specified on the command line before run. Each subsequent run displays average input/output since the last display.
            1. Iostat <#interval> <#reports>
            2. CPU Utilization report -c
                a. %user - % cpu used by user processes like firefox, chrome, thunderbird, etc
                b. %nice - % cpu utilization by user processes running with a nice value. Nice is a way to prioritize different processes, telling which ones should get a larger slice of cpu usage.
                c. %system - % cpu used by system processes such as X11, cron, various OS functions
                d. %iowait - % cpu time where the cpu was idle waiting on disk input/output. If this is high you may want to consider SSDs.
                e. %steal - % cpu time where the virtual cpu was waiting on the hypervisor to service another virtual CPU
                f. %idle - % cpu time where there was no outstanding requests so the cpu sat idle and alone.
            3. Device Utilization Report -d <Device>
                a. Device queried
                b. Tps is transfers per second, no set size on transfer
                c. Blk/Kb/Mb read per second
                d. Blk/Kb/Mb written per second
                e. Blk/Kb/Mb total read
                f. Blk/Kb/Mr total written
                g. Rrqm is number of read requests merged per sec queued to the device. Merged means the OS grouped multiple logical requests into a single one
                h. Wrqm is number of write requests merged per sec queued to the device
                i. Rsec is number of blocks read per second to the device
                j. Wsec is number of blocks written to the device per second
                k. Await is the average milliseconds to wait before a request is served by the device
                l. Avgrq-sz is average size in sectors of requests queued to the devuce
                m. Avgqu-sz is the average queue length of requests issues to the device
                n. R_await is the average time in milliseconds to wait for a read request to be served by the device
                o. W_await is the same ar R_await, only for Write requests

        p. Svctc is the average time waited for an input/output request to be served by the device
        q. %util is the percentage of elapsed time input/output requests were issued to the device in the time period
    4. -h makes it human-readable
    5. -k/-m shows stats in kilo, or megabytes per second
2. Vmstat - Reports information on memory, paging, block input/output, traps, disks, cpu activity. Like iostat, the first report is averages since boot, the subsequent reports are for the previous interval.
    1. Iostat <#interval> <#reports>
    2. -s/--stats displays some extended summary stats that does not repeat
    3. -d/--disk shows detailed per-device statistics on memory, cpu, input/output
3. netstat is the swiss army knife for networking statistics now being superseded by ss with which YMMV, but I will try to include ss exact and similar options. These tools get most info from directories and files under /proc/net
    1. Netstat - shows open sockets by default
    2. -t/-u uses tcp or udp
    3. -r shows routing table (now ip route)
    4. -n shows numerical data instead of using lookup tables like /etc/services for ports
    5. --interface=, -I=, -i specifies which interface to display info on
    6. Output
        a. Proto used by the socket
        b. Recv-Q is the bytes waiting and not acknowledged the user program yet
        c. Send-Q is for sending bytes
        d. Local address:port
        e. Remote address:port
        f. State
            i. Established means the 3-way handshake successfully completed
            ii. SYN sent means the first packet of a 3-way handshake was sent. Multiple SYN packets are used by DDoS tools to get the attention of remote computers and leave them hanging, waiting for a connection.
            iii. SYN Recv means a SYN packet was received
            iv. FIN Wait 1 & 2 are for when a connection is shutting down, and shutting down waiting for a reply to it’s FIN packet

        v. CLOSED means the socket is in use
        vi. CLOSE WAIT is when a socket is closed, and just waiting for a response from the other end of the connection
        vii. LAST ACK is when the socket has shut down and is waiting for an acknowledgement
        viii. LISTENING is waiting for a connection
        ix. CLOSING is when both ends of the connection are closed, but some data is not sent yet
        x. UNKNOWN is just that!
    g. User is UID of the owner of the socket
    h. Program PID is the PID of the program using the socket
4. Pstree is a program that will print out processes, their PIDs, and parent/child relationships in a text user interface.
    1. Pstree with no arguments displays ALL processes and parent/child relationships
    2. Pstree <pid> prints that process and it's parent child relationships
    3. -Z shows selinux context for each process
5. Ps shows running processes, and ones in other states as well.
    1. Ps -ef | ps aux is common to show all running processes
    2. 'a' means don't just list your own processes
    3. -A/-e selects all processes
    4. -f does a full listing of process stats
    5. 'x' means list even processes without a tty console session
    6. -p/--pid allows specifying a process id
    7. -M shows selinux context
    8. 'f' or --forest displays an ascii art forest of process id's and relationships
    9. -e selects all processes
6. W is a common command that displays some basic info on the system included users on the system, current time, and system load for 1, 5, and 15 minutes
7. Lsof lists info on files that are open and what processes have them opened
    1. Outputs
        a. Command, name of the program
        b. PID of processes running
        c. User running process
        d. FD is the file descriptor describing the type of file
        e. TYPE for the type of node associated with the file
        f. DEVICE major and minor numbers used by the kernel to find device drivers
        g. SIZE/OFF is the size of the file

        h. NODE is the inode of the file, the filesystem specific pointer to the metadata kept on a file
        i. NAME is the name of the mount point and filesystem where a file resides
8. Top is a common tool used for troubleshooting. It easily displays programs taking up the most CPU, and Memory. It is very useful at identifying memory leaks in programs who request more memory than they need and relinquish less than they requested upon exit. It provides a live, constantly updating, realtime view of processes running.
    1. Output
        a. Pid of the process
        b. User running/owning the process
        c. PR is the priority of the process
        d. NI is the nice value of the process, used to moderately alter the priority of the process
        e. VIRT is virtual memory, the memory being used by the process. All code, data, libraries, and pages whether they are swapped to disk or not.
        f. RES is the process' physical memory used
        g. SHR is the shared memory available to a process, not all resident
        h. %CPU is the % cpu used by the process
        i. %MEM is the % physical memory used by the process
        j. TIME is cpu time used by the process since it started
    2. Keys
        a. H is for help
        b. L displays system load per process
        c. T displays cpu time used by the system processes
        d. M shows memory usage by the processes
        e. < and > changes the column used to sort the display
        f. K kills a process
        g. R modifies the nice value for processes, called renice
9. Uptime is a simple program that does more one thing than tell how long the system has been running! Uptime displays the time the system has been up, the number of users logged in, the time, and average load on the system for the past 1, 5, and 10 minutes.
    1. --pretty displays a little less verbose information. An easily human readable string of how long the system has been up, nothing else. X days, X hours, and X minutes
    2. --since is passed an SQL DateTime string of YYYY-MM-DD HH:MM:SS to tell how many years, months, days, hours, minutes, and seconds have passed since the datetime passed in. Not sure how accurate this as, as it did not work for me.

10. Sar writes various system counters to stdout that are written over time to the standard system activity daily data files located in /var/sa with the names sa##.
    1. -P ALL displays counters for system activity for all cpus
        a. %user, %nice,%system,%iowait,%steal,%idle
    2. -A displays extended statistics about all activity written to the activity files
        a. %steal is time the cpu waits while the hypervisor services another machine
        b. %irq is the time spent servicing system interrupts
        c. %soft is time spent servicing software interrupts such as a special instruction in an instruction set or exception in the cpu itself
        d. %guest is time spent running a virtual processor
        e. %gnice is time spent servicing a guest with a nice value increasing/decreasing it's priority
        f. %idle
        g. Processes per second
        h. Cswch, context switches per second where a thread is suspended and restored
        i. Lots of paging statistics such as - pgpgin/s pgpgout/s fault/s majflt/s pgfree/s pgscank/s pgscand/s pgsteal/s %vmeff
        j. Lots of in-depth memory statistics - kbmemfree kbmemused %memused kbbuffers kbcached kbcommit %commit kbactive kbinact kbdirty
        k. In depth info on swapping - kbswpfree kbswpused %swpused kbswpcad %swpcad
        l. In depth network interface stats - rxpck/s txpck/s rxkB/s txkB/s rxcmp/s txcmp/s rxmcst/s
        m. Hugepages, filesystem stats
        n. pswpin/s pswpout/s
        o. pgpgin/s pgpgout/s fault/s majflt/s pgfree/s pgscank/s pgscand/s pgsteal/s %vmeff
        p. tps rtps wtps bread/s bwrtn/s
        q. frmpg/s bufpg/s campg/s
        r. kbmemfree kbmemused %memused kbbuffers kbcached kbcommit %commit kbactive kbinact kbdirty
        s. kbswpfree kbswpused %swpused kbswpcad %swpcad
        t. kbhugfree kbhugused %hugused
        u. dentunusd file-nr inode-nr pty-nr
        v. runq-sz plist-sz ldavg-1 ldavg-5 ldavg-15 blocked
        w. rcvin/s xmtin/s framerr/s prtyerr/s brk/s ovrun/s

x. Raw hardware device usage - tps rd_sec/s wr_sec/s avgrq-sz avgqu-sz await svctm %util
y. rxpck/s txpck/s rxkB/s txkB/s rxcmp/s txcmp/s rxmcst/s
z. rxerr/s txerr/s coll/s rxdrop/s txdrop/s txcarr/s rxfram/s rxfifo/s txfifo/s
aa. call/s retrans/s read/s write/s access/s getatt/s
bb. scall/s badcall/s packet/s udp/s tcp/s hit/s miss/s sread/s swrite/s saccess/s sgetatt/s
cc. totsck tcpsck udpsck rawsck ip-frag tcp-tw