# Overview!

Who doesn’t like games? Below are tables that contain questions for the class to answer. A correct answer earns you 1 point; an incorrect answer will cause you to lose 1 point.

There’s a catch! Each question can be answered correctly by at most one person. The game will proceed as follows.

* Phase 1
  + The instructor announces a time limit for phase 1.
  + In phase 1, place your name in a cell only if you can answer the question. Place your name in as many cells as you like, but remember that you’ll lose a point if you are chosen and answer incorrectly.
* Phase 2
  + In phase 2, the instructor chooses one from among the names in a given cell.
  + The person chosen gets a chance to demonstrate an answer. Points are awarded/deducted.
  + Once a correct answer has been given, we’ll move on to the next cell.
  + Phase 2 continues until all answers have been found or until names are exhausted.

There are no restrictions on resources that can be used to answer questions. Good luck!

|  |  |  |
| --- | --- | --- |
| **How do I?** | **… in Windows** | **… in Debian/Linux** |
| 1. List directory contents? | Jon: Open command prompt, enter “dir” | Jon: similar, but “ls” |
| 2. Find my machine name? | Open command prompt, enter “hostname” | Open command prompt, enter “hostname”. |
| 3. Start an admin console session? | Search for “cmd”, right-click, and select “Run as Administrator” | Open command prompt, enter “su -”. You can also use “sudo” for individual commands. |
| 4. Find which processes use the most CPU or memory? | Open the Task Manager and examine which running process is consuming the most memory. | Open command prompt, enter “top”. |
| 5. Stop/Kill a process? | Open the Task Manager, locate the running process, and then select End Task. | Open command prompt, use “ps” to find the running process, and then enter “kill [pid of running process]”. |
| 6. Find out how much disk space is free? | Look at properties of the C drive and find the available free space. (i.e. Right-click and select Properties) | Open command prompt, enter “df -h”. |
| 7. Find out who is logged in? | whoami | *“whoami” list the current user*  *“who” list all users* |
| 8. Find a log of recent logins and login attempts? | Look in Event Viewer. Filter the results for the id of the specific event you are looking for. | Open command prompt, enter “last”, or  *sudo less /var/log/auth.log* |
| 9. Find my IP and MAC addresses? | “ipconfig /all” | “ifconfig” |
| 10. List all open network connections? | “Netstat -an”, search for connection that are ESTABLISHED | “Netstat -tun” |
| 11. Find the process responsible for each open network connection? | “netstat -oan” | “netstat -tupn” |
| 12. Find the binary executable responsible for each open network connection? | *Netstat -b* | *netstat -tulpn*  *netstat -peanut*  *And ‘which’ or ‘find’ commands* |
| 13. Reset my network interface? | *netsh winsock reset* | “ifdown” and “ifup” (usually eth0 or -a for all connections) |
| 14. Examine my OS name and version? | My Computer->Properties | *Lsb\_release -a* |
| 15. Find kernel version? | *Same as above* | “uname -a” |
| 16. Examine which programs run at system boot time? | Msconfig.exe, click services tab | “Ls /etc/rc\*.d” |
| 17. Stop a program from running at system boot ti | Disable the Startup tasks via the Task Manager, startup tab | *sudo update-rc.d -f <prg name> remove* |
| 18. Find my default IP gateway? | “ipconfig /all” | “ifconfig -a”  netstat -rn  Look for route entry with destination 0.0.0.0 |
| 19. Find my default name server? | command prompt, nslookup (will show a default), or Network and Sharing Center, pull properties on network connection, then Details, or ipconfig /all | “cat /etc/resolv.conf” |
| 20. Examine contents of the ARP cache? | “arp -a” | Arp -a |
| 21. Add an entry to the ARP cache? | arp -s IP ADDRESS MAC ADDRESS | “arp -s [IP address] [MAC address]” |
| 22. Examine contents of the DNS cache? | ipconfig /all  ipconfig -displaydns | Linux does not maintain a DNS cache |
| 23. Make a local DNS query respond with an IP of my choosing? | C:\Windows\System32\drivers\etc\hosts, add a line (ip, name), ping name | Add entry to  /etc/hosts |
| 24. Find the list of trusted certificates installed on my system? | run certmgr.msc utility | “Ls /etc/ssl/certs” |
| 25. Remove a trusted certificate from my system? | *Open certmgr.msc, navigate to certificate, delete* | in Terminal -- sudo dpkg-reconfigure ca-certificates (gives list that you can select from) OR sudo update-ca-certificates (to edit file manually) then, remove desired certificate |