Overview!

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

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

- Phase 1
  - The instructor announces a time limit for phase 1.
  - In phase 1, place your group # in a cell only if you can answer the question. **Do not answer the question in the space provided.** Place your group # 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 group from among the group #s in a given cell.
  - The group chosen describes the answer to the question. The other groups verify that the solution works. Points are awarded/deducted.
  - Once a correct answer has been given, we'll move on to the next cell. **But first, the group that answered correctly should fill in the cell with the answer.** Throughout the semester, this document can be a great resource to refer back to.
  - Phase 2 continues until all answers have been found or until groups 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?	dir	ls
2. Find my machine name?	hostname	hostname
3. Start an admin console session?	Right click on cmd - run as admin	su
4. Find which processes use the most CPU or memory?	*Launch task manager*	top
5. Stop/Kill a process?	Launch task manager, choose a process, then click on End Process.	*kill <PID>*
6. Find out how much disk space is free?	Open up the Start Screen and click on “Computer” In right panel.	df df -h // human readable
7. Find out who is logged in?	whoami	whoami
8. Find a log of recent logins and login	Event viewer	last (Can specify a username as optional arg)

attempts?		Optional flag for number of attempts: last -#
9. Find my IP and MAC addresses?	ipconfig /all	ifconfig
10. List all open network connections?	**admin command prompt, netstat -an | findstr /c:"ESTABLISHED"**	*Netstat -tun*
11. Find the process responsible for each open network connection?	netstat -oan	netstat -A inet -p
12. Find the binary executable responsible for each open network connection?	*Netstat -b*	*Netstat -tulpn*
13. Reset my network interface?	netsh winsock reset	*sudo /etc/init.d/networking restart* *Ifup <connection> ifdown <connection>*
14. Examine my OS name and version?	*Start+dxdiag*	*lsb_release -a*
15. Find kernel version?	ver on command prompt PC properties on GUI (search "about")	*uname* *Add -v flag for verbose output*
16. Examine which programs run at system boot time?	Task manager startup tab	initctl list
17. Stop a program from running at system boot time?	msconfig	*sudo update-rc.d -f [program name] remove*

18. Find my default IP gateway?	Ipconfig If you search through the output you can find the default gateway	ip route | grep default ip route allows you to manage your routing tables. Pipe the full output of ip route through grep to search for your default gateway. Reference
19. Find my default name server?	Ipconfig /all | findstr /R "DNS\ Servers"	**cat** /etc/resolv.conf
20. Examine contents of the ARP cache?	arp -a	**sudo arp**
21. Add an entry to the ARP cache?	arp -s *<ip address> <ethernet (MAC) address>*	sudo arp -s 10.0.0.2
22. Examine contents of the DNS cache?	Ipconfig -displaydns	No OS local DNS cache by default. Install *dnsmasq* in order to use `*dig*` command.
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?	Windows + R certmgr.msc	cat /etc/ca-certificates.conf ls /etc/ssl/certs
25. Remove a trusted certificate from my system?	certutil -delstore CertificateStoreName CertId	certmgr -del -c -v -m Trust CERTHASH (another) way to do this: sudo dpkg-reconfigure ca-certificates Or just sudo vi /etc/ca-certificates.conf. If you edit

		this file manually, you must do: sudo update-ca-certificates Another option: security remove-trusted-cert [certFile]