Windows Command Line

Windows command line is a CLI **command line interface** and although it seems older in comparison to some modern interfaces, such as PowerShell. But there are advantages to this older style interface such as:
Lower resource usage: Can run on old hardware, no GUI.
Automation: Create batch file scripts and commands that can be automated.
Remote Management: Make it convenient to use SSH to manage remote systems.

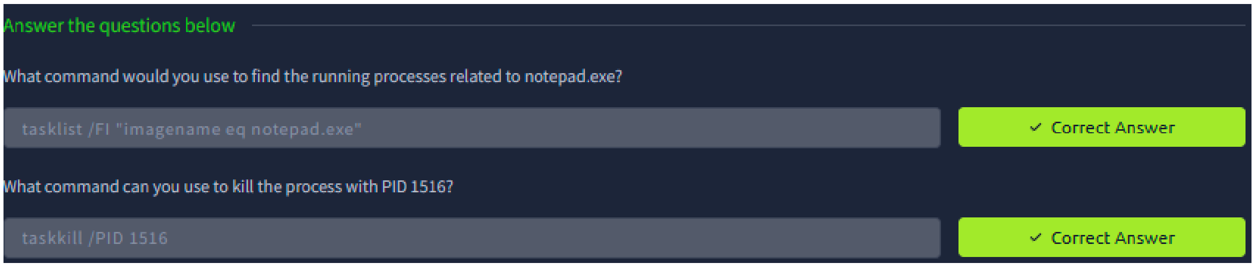
cmd.exe is the command to bring up the console:
cmd.exe

So how do we connect? Example:
ssh <username>@<IP>
<password>

Example:
ssh user@10.10.151.78
Tryhackme123!

Command: set | = Check your path from the command line.
Command: Path= | = Indicated line of path.
Command: systeminfo | = Lists various information about the system such as OS, system details, processor and memory.
Command: driverquery | = Displays additional information.
Command: help | = Help information for a specific command.
Command: cls | = Clear command prompt screen.system
Command: ver | = Version command to display OS version
Command: ipconfig | = Displays IP for the current host, subnet mask, default gateway.
Command: ipconfig /all | = Displays all IP information about your network configuration.
Command: ping | = Send ICMP packet and listen for response. Response = Reachable.
Command: tracert <targetIP> | = Trace network route traversed to reach target.
Command: nslookup <website.com> | = Looks up host domain and returns IP address
Command: netstat -a | = Display all established connections and listening ports.
Command: netstat -b | = Shows programs associated with each listening port connection.
Command: netstat -o | = Reveals processID (PID) associated with connection.
Command: netstat -n | = Uses numerical form for addresses and port numbers.
Command: netstat -h | = Displays netstat help.
Command: netstat -abon | = combines all together, long output but detailed.
Command: cd | = Show directory (“Where am I?”).

Command: dir | = View directories.
Command: dir /a | = Display hidden and system files.
Command: dir /s | = Display files in current directory and subdirectories.
Command: tree | = Visually represent child directories and subdirectories.
Command: cd .. | = Go back.
Command: makedir | = Make Directory.
Command: rmdir | = Remove Directory.
Command: type | = View type of file.
Command: more | = For longer text files.
Command: tasklist | = List running processes.
Command: tasklist /FI “imagename eq sshd.exe” **| =** Show sshd processes.
Command: taskkill | = Terminates process.
Command: chkdsk | = Checks file system and disk for errors and bad sectors.
Command: driverquery | = Display list of installed device drivers.
Command: sfc /scannow | = Scans system files for corruption and repairs them if possible.
Command: shutdown /s | = Shutdown system.
Command: shutdown /r | = System restart.
Command: shutdown /a | = System Abort.



Answer the questions below

What command would you use to find the running processes related to notepad.exe?

```
tasklist /FI "imagename eq notepad.exe"
```

What command can you use to kill the process with PID 1516?

```
taskkill /PID 1516
```