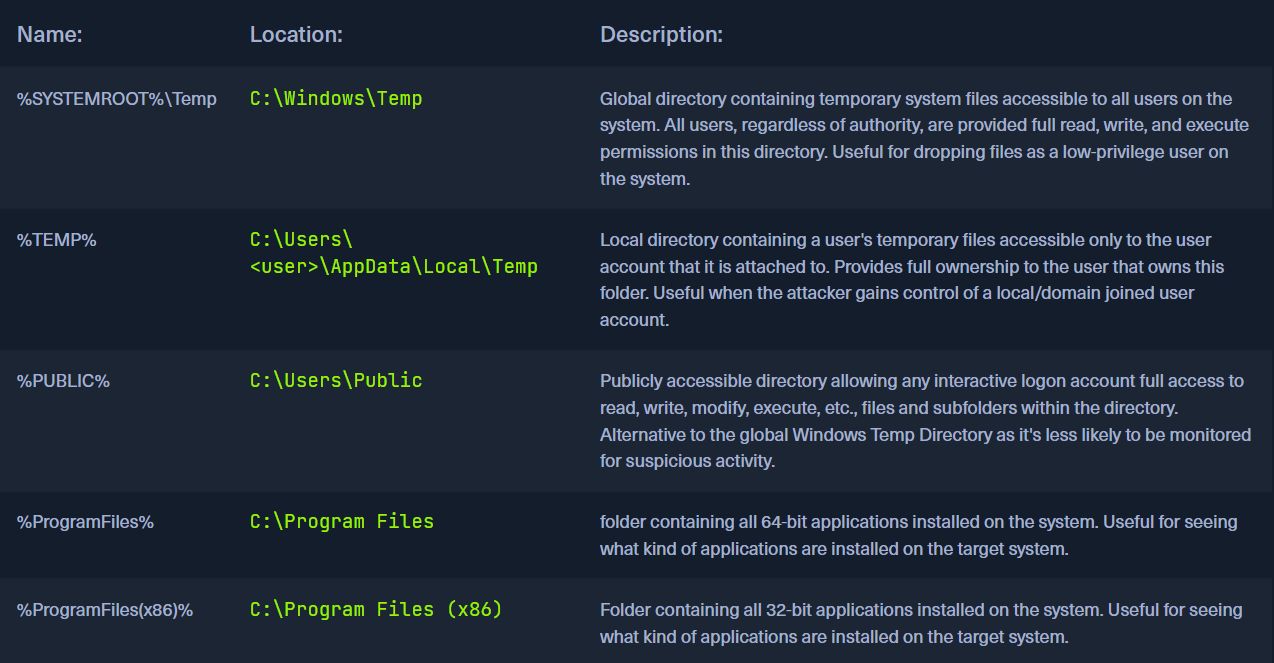
Command Prompt

C:\ is the root directory of all Windows machines and has been determined so since it is inception in the MS-DOS and Windows 3.0 days. The "C:\" designation was used commonly as typically "A:\" and "B:\" were recognized as floppy drives, whereas "C:\" was recognized as the first internal hard drive of the machine.

**Some important dir from an attacker’s perspective :-**

****

**Xcopy and robocopy:-**

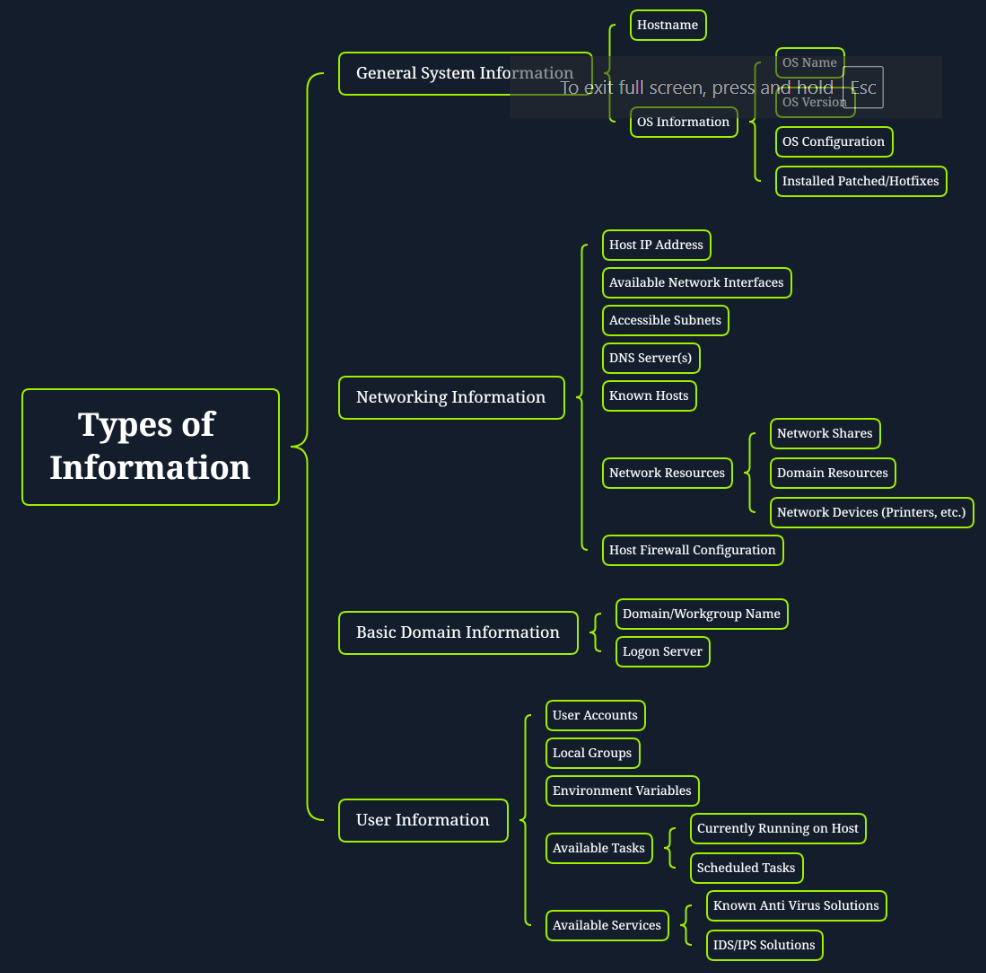
When performing the duplication, **xcopy** will reset any attributes the file had. If you wish to retain the file's attributes ( such as read-only or hidden ), you can use the /K switch.

Robocopy is made for moving large directories and drive syncing.  
Moving files can be problematic if we do not have the **SeBackupPrivilege** and **auditing privilege** attributes. We can utilize the **/MIR** switch to permit ourselves to copy the files we need temporarily. Be aware that it will mark the files as a system backup and hide them from view. We can clear the additional attributes if we add the **/A-:SH** switch to our command. Be careful of the /MIR switch, as it will mirror the destination directory to the source. Any file that exists within the destination will be removed. Ensure you place the new copy in a cleared folder. Above, we also used the **/L** switch. This is a what-if command. It will process the command you issue but not execute it; it just shows you the potential result.

**Working in dir :-**

* Using > this way will create the file if it does not exist, or it will overwrite the specified file's contents. To append to an already populated file, we can utilize >>.
* we can use < like this to search for keywords or strings in large text files, sort for unique items, and much more. Another route we can take is to feed the output from a command directly into another command with the | called pipe.
* Ifwe wish to have two commands executed in succession. We can issue the command and follow it with & and then our next command. We can utilize && to say run command A, and if it succeeds, run command B.
* We can also accomplish the opposite of this with ||. By using (pipe pipe), we are saying run command A. If it fails, run command B.

**Host Enumeration:-**

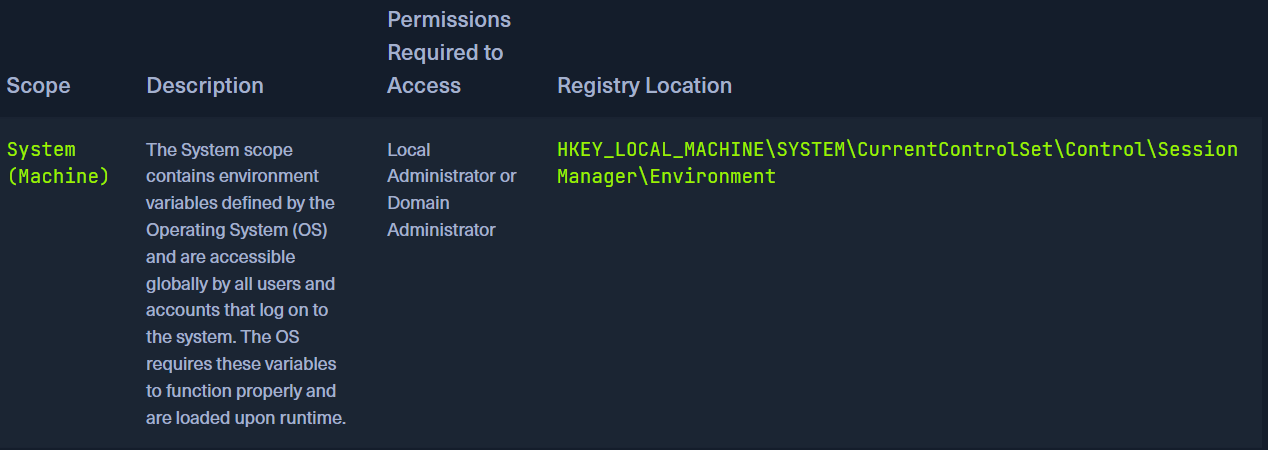
Chart of useful information in a windows system.****

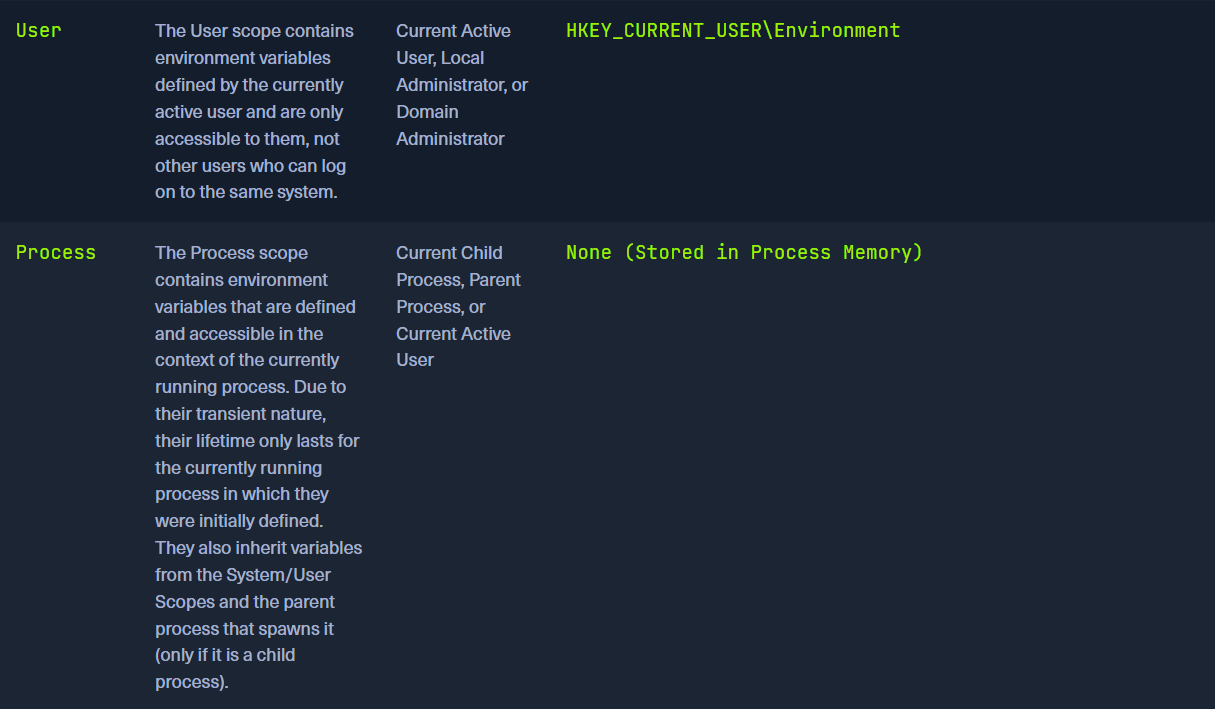
In the **whoami** command If the current user is not a domain-joined account, the NetBIOS name will be provided instead. The current hostname will be used in most cases.

# **cmd /c** to run CMD commands in powershell and close CMD after running the it or **cmd /k** to keep CMD open afterwards.

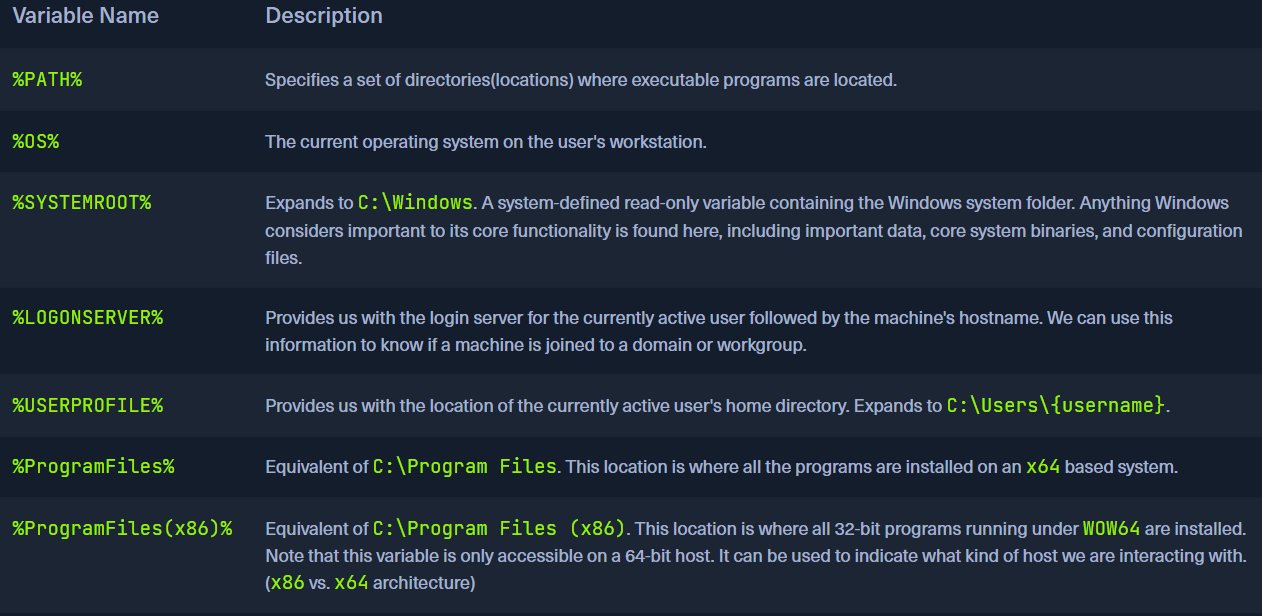
Use **where /r** to search directories, it might take time for longer directories but worth it!

**Environment variable scopes:-**

****

****

**Some important environment variables:-**

****

<https://ss64.com/nt/syntax-variables.html> - more windows environment variables.

**Service Controller:-**

>sc query type= service.

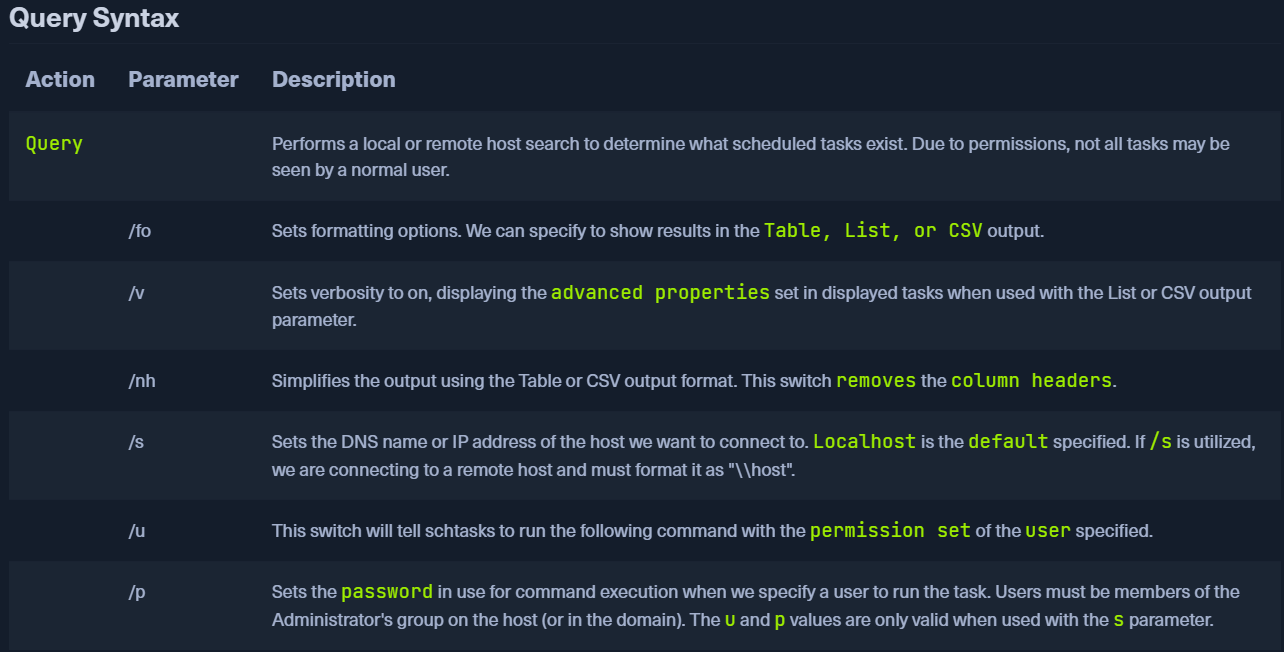
List active services

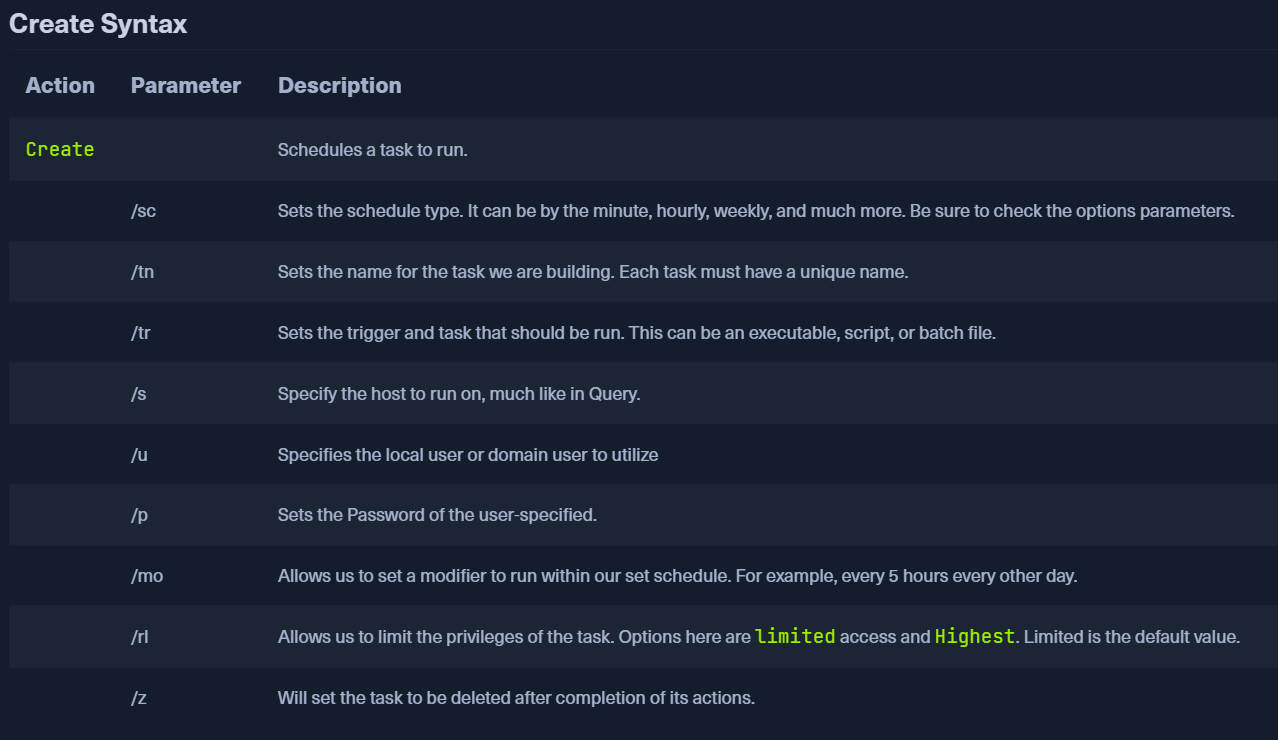
The spacing for the optional query parameters is crucial. For example, type= service, type=service, and type =service are completely different ways of spacing this parameter. However, only type= service is correct in this case.

**Wuauserv** -> windows update service   
**Bits** -> background intelligence transfer service

**SCHTASK:-**

To see tasks that already exist on the host



To create a new task   


To change the properties of the task

