Which tools can be used for command shell execution?

LUCY comes with three tools that will access the windows command shell and enable you to execute commands:

- **ConsolePost**: Enables you to automatically execute one or multiple commands within the Windows shell on the target computer and send back the output to LUCY.
- **ConsoleOutlook**: Execute commands and send the output back via Outlook (access Outlook hidden via MAPI) to a predefined email address. It also has the ability as a PoC to send back the subject line from last received email in Outlook.
- **ConsoleInteractive**: This tool allows you to establish a reverse HTTP/HTTPS channel to LUCY. Once the file has been executed, you can see the session in “Sessions”. The tool only runs in the memory (called “file” in Process View). After the termination, the session can no longer be established. You can click on the IP and start executing commands within the Windows shell. The output should appear after a few seconds automatically. This Tool only works with Windows 7/8 in combination with IE and Firefox.
- **Macro Simulation “POST ONLY**: this tool is described here.

What are the limitations?

In the community edition you might be only able to execute the following commands:

- whoami
- date
- time
- date /T
- time /T
- ipconfig

In the commercial edition, there are no limitations. Commercial editions allow any command to be executed using this syntax:

cmd.exe /c "YOUR COMMAND GOES HERE" (some commands in Windows are not executable. They are built into the command line. Example of command with executable: whoami. If you need to use a command which is a built-in command line, then you should call cmd directly. Example of requesting the directory content: “cmd /c dir”).

So, for example, standard cmd.exe commands are accessible like: * dir (list directory contents) * md (create directory) * etc