# Using MSDOS for Security Testing

MSDOS is a scripting that was the original command line interface used by Microsoft Windows. There are some basic commands like

| | |
|---|---|
| **copy** | - Copy the contents of a file |
| **rename** | - Rename a file or directory |
| **pwd** | - Print current working directory |
| **cd** | - Change working directory |
| **mkdir** | - Make/create working directory |
| **erase** | - Delete a file/directory |

Other useful commands include

| | |
|---|---|
| **arp** | - View the arp table on the target system |
| **cacls** | - View the Access Control (ACL) associated with a file |
| **echo** | - Display a message |
| **findstr** | - Searches for a test string within a file |
| **net** | - View/Edit system and network setting |
| **ipconfig** | - Query IP configuration |
| **nslookup** | - Make a DNS query |
| **ping** | - Send an ICMP echo request |

We can create MSDOS programs in what we call batch (.bat) files. Within a MSDOS script we can make use of loops.

- Syntax-FOR-Files
    - `FOR %%parameter IN (set) DO command`
- Syntax-FOR-Files-Rooted at Path
    - `FOR /R [[drive:]path] %%parameter IN (set) DO command`
- Syntax-FOR-Folders
    - `FOR /D %%parameter IN (folder_set) DO command`
- Syntax-FOR-List of numbers
    - `FOR /L %%parameter IN (start,step,end) DO command`
- Syntax-FOR-File contents
    - `FOR /F ["options"] %%parameter IN (filenameset) DO command`
    - `FOR /F ["options"] %%parameter IN ("Text string to process") DO command`
- Syntax-FOR-Command Results
    - `FOR /F ["options"] %%parameter IN ('command to process') DO command`

We can also make use of if statements to control the flow of execution. Performs conditional processing in batch programs.

- `IF [NOT] string1==string2 command`
- `IF [NOT] EXIST filename command`
- `IF CMDEXTVERSION number command`

Where compare-op may be one of:

```
EQU - equal
NEQ - not equal
LSS - less than
LEQ - less than or equal
GTR - greater than
GEQ - greater than or equal
```