BashScripting

```
Simple Bash Scripting Cheatsheet
--------------------------------

[+] nano Shortcuts
ctrl v■■■Next page.
ctrl y■■■Previous page.
ctrl w■■■Where is (find).
ctrl k■■■Cut that line of test.
ctrl x     ■■Exit editor.

[+] Create a text file:
touch file■■Creates an empty file.
ifconfig > tmp■pipe the output of a command
nano file

[+] Create a file and append text to it:
ifconfig > tmp
echo >> tmp
ping google.com -c3 >> tmp

[+] How to view a file:
cat file■■Show entire contents of file.
more file■■Show one page at a time.  Space bar for next page and (q) to exit.
head file■■Show the first 10 lines.
head -15 file■Show the first 15 lines.
tail file■■Show the last 10 lines.
tail -15 file■Show the last 15 lines.
tail -f file■Useful when viewing the output of a log file.

[+] pipe
cat tmp | grep Bcast■Feeds the output of one process to the input of another process.

[+] Processes
ps aux■■■Show all running process for all users.
kill -9 PID■■Nicely kill a PID.

[+] Word Count
wc -l tmp2■■Count the number of lines in a file

[+] cut
-d  delimiter
-f  fields

[+] sort
Sort by unique■■sort -u file
sort IP addresses correct■■sort -t . -k 1,1n -k 2,2n -k 3,3n -k 4,4n
cat tmp2 | cut -d '(' -f2 | cut -d ')' -f1 | sort -u■■Isolate the IP address

[+] awk
awk '{print $1}' file ■■Show the 1st column.
awk '{print $1,$5}' file ■Show the 1st and 5th columns.

[+] grep
grep -v■■Remove a single string.
grep -v 'red' file

[+] egrep -v
Remove multiple strings■egrep -v '(red|white|blue)' file

[+] sed
sed 's/FOO/BAR/g' file ■■Replace FOO with BAR.
sed 's/FOO//g' file ■■Replace FOO with nothing.
sed '/^FOO/d' file ■■■Remove lines that start with FOO.

[+] colour
31=red 32=green 33=yellow 34=blue 35=magenta 36=cyan
echo -e "\e[1;34mThis is a blue text.\e[0m"
```

Bash Scripts

[+] Simple bash script:

```
#!/bin/bash
clear
echo
echo
print "Hello world."
```

[+] Make a file executable.

```
chmod +x file
chmod 755 file
```

[+] Variables

```
name=Bob
echo $name
user=$(whoami)
echo $user
echo 'Hello' $name. 'You are running as' $user.
```

```
#!/bin/bash
clear
echo "Hello World"
name=Bob
ip=`ifconfig | grep "Bcast:" | cut -d":" -f2 | cut -d" " -f1`
echo "Hello" $name "Your IP address is:" $ip
```

[+] User Input

```
read -p "Domain: " domain
```

```
#!/bin/bash
echo "Please input your domain:"
read -p "Domain:" domain
ping -c 5 $domain
```

[+] Check For No User Input

```
if [ -z $domain ]; then
■echo
■echo "#########################"
■echo
■echo "Invalid choice."
■echo
■exit
fi
```

[+] For loops

```
#!/bin/bash

for host in $(cat hosts.txt)
do
■command $host
done
```

[+] One Liners

Port Scan:

```
for port in $(cat Ports.txt); do nc -nzv 192.168.0.1 $port & sleep 0.5; done
```

Use a bash loop to find the IP address behind each host:

```
for url in $(cat list.txt); do host $url; done
```

[+] Condition Onliner

```
any command && if work || if not work
type -p massdns && massdns -r resolver.txt -t A -o S sub.txt -w sub.mass || echo "MassDns not installed"
```

[+] Condition Onliner with multiple action

```
any command && { if work; also this; also this } || { if not work; also this; also this }
type -p massdns && { massdns -r resolver.txt -t A -o S sub.txt -w sub.mass; cat sub.mass } || { echo "MassDns not insta
```