Ultimate Cheat Sheet: Bash Commands:

Files:

Find:

```
//Find file by name
find . name [name]

//Find file by extension
find . -type f -name ".txt"

//Find file by name with any extension
find . -type f -name "[name].*"

//Find by size (c = bytes)
find . -size [SIZE]c

//Find file by group
find . -group [groupname]

//Find file by user
find . -user [username]
```

Other:

```
//Search for a string in any files:
grep -rnw --exclude-dir=proc 'STRING' / 2>/dev/null
```

Archives:

```
//zip a directory
zip -r [archive name] [directory name]
```

```
//Unzip an archive
unzip [archive name]

//Decompress an archive: gzip
gzip -d [archive name]

//Decompress an archive: bzip2
bzip2 -d [archive name]

//Decompress an archive: POSIX tar archive (GNU)
tar -xvf [archive name]
```

Miscellaneous:

```
//Set environment variables
EXPORT [VAR NAME]=[VALUE]

//Get file types for multiple files at once:
file -s file{0..9}

//Find the only unique line in a file:
sort data.txt | uniq -c | grep -e "1"

//Decode from base64
base64 -d [filename]

//Translate characters in a file (ROT13):
cat data.txt | tr "[a-z]" "[n-za-m]" | tr "[A-Z]"
"[N-ZA-M]"

//Reverse a hexdump:
xxd -r [ORIG] > [OUT FILE]
```

Networking

ssh:

```
//Connect to ssh
ssh -p 22 root@192.168.0.0

//Connect to ssh with private key
ssh -i sshkey.private root@192.168.0.0

//ssh proxy traffic so remote port 80 can be accessed at
localhost:8080
ssh -L 8080:localhost:80 root@192.168.0.0

//Copy from remote host
scp root@192.168.0.0:/etc/password .passwd_file

//Copy to remote host
scp [FILE SOURCE] root@192.168.0.0:[FILE DEST]
```

iproute:

```
//Add network to iproute
ip route add [target network] via [intermediate router]

//Show routes:
route

//Remove route:
```

```
ip route del [target network] via [intermediate router]
```

Netcat:

```
//Send a message:
echo message | nc [ADDR] [PORT]

//Send some data from a file:
nc [ADDR] [PORT] < input.txt

//Listen for inbound connections in the background:
nc -l [ADDR] -p [PORT] &

//Listen for inbound connections, for any address, and be
verbose
nc -lvp [PORT]
```

Tcpdump:

```
//See what interfaces are available for capture
sudo tcpdump -D

//Capture all packets on any interface
sudo tcpdump -i any

//Capture n packets
sudo tcpdump -i [interface] -c [n]

//Capture packets on a specific port
sudo tcpdump -i any port [PORT]
```

```
//Capture and parse headers and data of each packet in hex
sudo tcpdump -i any port [PORT] -xx

//Write capture to a file
sudo tcpdump -i any -w output.pcap

//Capture traffic for specific source or destination host, and a specific portrange
sudo tcpdump -i any host [HOST] and portrange [START PORT]-[END PORT]
```

Misc:

```
//Send message over connection using SSL encryption:
echo message | openssl s_client -connect [ADDR]:[PORT] -ign_eof
```

Bash Scripts

```
//Loop through alphabet:
for x in {A..Z}; do echo "$x"; done

//Loop through all possible 4 digit combinations:
for i in {0000..9999}; do echo $i; done
```

Windows

```
//Compare 2 ascii files
fc /a [FILE 1] [FILE 2]
```

```
//Compare 2 binary files
fc /b [FILE 1] [FILE 2]

//Check network configuration:
ipconfig

//Get network statistics
netstat

//Trace route:
tracert [ADDR]

//Get system info
systeminfo

//List the current directory (ls equiv.)
dir

//Clear the command prompt
cls

//Display the contents of a file:
type [FILE]

//Find all text files in the directory tree
dir /b/s *.txt

//Find  files containing a string using find command
find [SWITCH] "string" [Pathname]

//Show all running processes
tasklist
```