**Man, Base64 and Hex**

**Man** – brings up the manual page for a command

* Man ls
* Brings up manual for ls

Q – to quit

**Getting man pages for system calls**

Sudo apt-get install -y libattr1-dev

8 sections, section 1 is usr commands

Section 2 is system calls

* Man 2 write
* Gives the manual page for write

1 – Usr commands

2 – Sys calls

3 – C library functions

4 – Devices

5 – File formats

6 – Games

7 – Misc

8 - Admin

**Base64**

A way to convert binary text into a transferrable form

* Allows you to transfer binary from one system to another without transferring it in its raw form
* Like a form of encryption

Echo -n ‘Red Team Nation!’ | base64

* Gives string

Echo ‘string’ | base64 -d

* -d, decode

e.g., transfer ls cmd via base64

cat /bin/ls | base64 > ls.txt

* Running ls.txt wont do anything as its not an executable

Cat ls.txt | base64 -d > ls

* Decode the base64 output into a file called ‘ls’

Chmod -x ls

* Changes ls file to an executable

./ls

* Will run as normal
* Exchanged data from system to system

**Hex**

**Representation of binary in an ASCII format**

* Working with exploits, memory, bugs, file binary modifications

Xxd

* Hex converter

Echo ‘Red Team Nation!’ | xxd -p

* -p, principal format

Echo -n ‘hex string’ | xxd -r -p

* -r, reverse
* Decodes from hex

Cat bin/ls/ | xxd -p > lsnew.hex

Cat lsnew.hex

* Shows hex

Cat lsnew.hex | xxd -r -p > lsnew

* Reverses hex and pipes it into lsnew file

Chmod -x lsnew

* Creates the executable

./lsnew

* Will work like ls
* ./ execute locally

Can rename commands or execute commands without typing in the whole thing

Allows you to get around some command logging

Uname -a

* Shows system information