**Active Recon – Port Scanning**

**Port scans can be very loud and obvious, they could even bring down a network**

**So be careful**

**Nmap**

* Port scanner
* Scans first 1000 ports by default

**TCP**

* Full 3-way handshake
* No ACK packet received, won’t come back as port is open

-sS

* Doesn’t complete 3-way handshake, receives ACK and leaves it open

-sF

* Just sends a FIN packet, if port is closed, no response, if open, REST packet receipt

**UDP**

Some services run on UDP and not TCP

Takes longer than TCP scanning

-sU

* Just sends a FIN packet, if port is closed, no response, if open, REST packet receipt

-sX

* Sets bits in packet to push, fin and urgent
* Can sometimes bypass firewall rules or filters
* V obvious packet
* Unless a firewall is specifically looking for it, it might just let it through

Nmap usually makes assumptions on port services rather than actually testing to see what services are running on the port

-sV

* Banner grab / actual connection to port and then check what the service or banner is

-O

* Tries to ID the OS

-A

* Equiviolent of -sV -O
* TCP handshake, banner grabbing and OS query

-o

* Output
* oN – standard nmap output
* oX – xml format
* or pipe > scan.txt
* oG – provides a greppable outcome
* oA – dumps data in an nmap file with no particular formatting

**Specific ports and specific scripts**

Nmap -p80 192.168.1.1 –script=https\*

* https is the script
* \* means use any module