Nmap UDP Scan

Now we have gone over the various scans we can do, it's important to process some other vital information. For example,
Specific port list to scan eg. 22,80,443 would be specific as **-p22,80,443.**
Or scanning a port range eg. 1-1023 inclusively would be **-p1-1023.**

-p- = Scan all ports /65535
-F = Scan 100 most common ports
–top-ports 10 = Sca 10 most common ports
-T<0-5> = Scan timing

-T0 = Slowest (paranoid)
-T5 = Fastest

SPEED TEMPLATES:
Paranoid (0)
Sneaky (1)
Polite (2)
Normal (3)
Aggressive (4)
Insane (5)

To avoid IDS alerts -T0 / -T1 is considered. But **-T0 scans 1 port at a time. Waiting 5 minutes between each probe.**

Nmap uses normal -T3. -T5 is the fastest but can affect accuracy of the data increasing the chance of packet loss. -T4 is often used during CTFs and learning to scan on practice targets. Whereas -T1 is used on real engagements where stealth is required.

You can also change the packet rate using –min-rate <number> to control how many packets you are sending per second. Eg –max-rate 10 = No more than 10 a second.

Probing: Controlling the paralleliztion using –min-parallelism <numprobes> and –max-parallelism <numprobes>

Questions:

What is the option to scan TCP ports between 5000-5500? = -p5000-5500

How can you ensure Nmap will run at least 64 probes in parallel? = –min-parallelism=64

What option would you add to make Nmap very slow and paranoid? = -T0

Port Scan Type	Example Command
TCP Connect Scan	`nmap -sT 10.10.26.109`
TCP SYN Scan	`sudo nmap -sS 10.10.26.109`
UDP Scan	`sudo nmap -sU 10.10.26.109`

These scan types should get you started discovering running TCP and UDP services on a target host.

Option	Purpose
`-p-`	all ports
`-p1-1023`	scan ports 1 to 1023
`-F`	100 most common ports
`-r`	scan ports in consecutive order
`-T<0-5>`	-T0 being the slowest and T5 the fastest
`--max-rate 50`	rate <= 50 packets/sec
`--min-rate 15`	rate >= 15 packets/sec
`--min-parallelism 100`	at least 100 probes in parallel

Conclusion:

Port scanning is pivotal during reconnaissance, because it allows us to identify which ports are open on a service, and by using the specific speed control such as -T0 or -T1 we can configure Nmap to run at a pace that keeps it discrete. Whereas we can alternatively manipulate it to run faster such as -T5 but we are generating more noise as well as inaccuracies, risking packet loss and reducing reliability. Additionally we can also change the packet limit, such as not sending more than 10 packets, reducing the activity. Overall this is a fantastic introducing to the tools we can use to obtain vital data of services running.