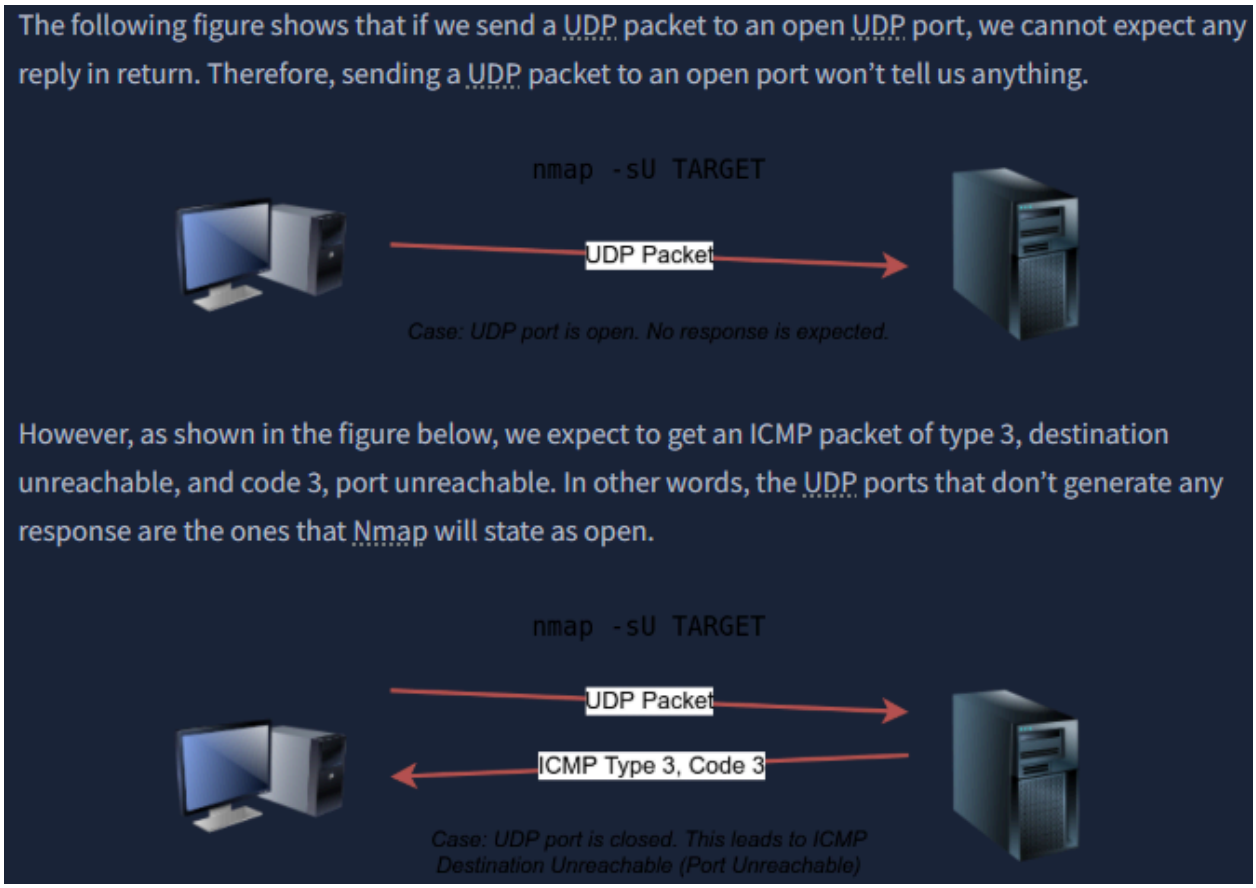
Nmap UDP Scan

A UDP is a connectionless protocol, hence it does not require any handshake for a connection establishment. This particular protocol is commonly associated with streaming services or gaming services, when the data loss isn't really concerning, packets are just sent continuously and some missed packets don't matter.

A service listening on UDP port would respond to our packets, however if a UDP packet is send to a closed port an ICMP port unreachable error (type 3 code 3) is returned. You can select UDP scan by **-sU (UDP SCAN).**



Like so.

```
root@ip-10-10-78-18:~# nmap -sU -F -v 10.10.26.109
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-26 11:23 BST
Initiating ARP Ping Scan at 11:23
Scanning 10.10.26.109 [1 port]
Completed ARP Ping Scan at 11:23, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:23
Completed Parallel DNS resolution of 1 host. at 11:23, 0.00s elapsed
Initiating UDP Scan at 11:23
Scanning ip-10-10-26-109.eu-west-1.compute.internal (10.10.26.109) [100 ports]
```

So when I submit a UDP scan, it creates this and after waiting some time we get this information:

```
Scanning ip-10-10-26-109.eu-west-1.compute.internal (10.10.26.109) [100 ports]
Increasing send delay for 10.10.26.109 from 0 to 50 due to max_successful_tryno
increase to 4
Increasing send delay for 10.10.26.109 from 50 to 100 due to max_successful_tryn
o increase to 5
Increasing send delay for 10.10.26.109 from 100 to 200 due to max_successful_try
no increase to 6
Increasing send delay for 10.10.26.109 from 200 to 400 due to max_successful_try
no increase to 7
Increasing send delay for 10.10.26.109 from 400 to 800 due to max_successful_try
no increase to 8
Discovered open port 111/udp on 10.10.26.109
UDP Scan Timing: About 44.60% done; ETC: 11:25 (0:00:39 remaining)
```

```
UDP Scan Timing: About 44.60% done; ETC: 11:25 (0:00:39 remaining)
Completed UDP Scan at 11:25, 103.45s elapsed (100 total ports)
Nmap scan report for ip-10-10-26-109.eu-west-1.compute.internal (10.10.26.109)
Host is up (0.00055s latency).
Not shown: 98 closed ports
PORT    STATE         SERVICE
68/udp  open|filtered dhcpc
111/udp open          rpcbind
MAC Address: 02:FA:1F:3D:A0:F3 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 103.63 seconds
           Raw packets sent: 223 (8.792KB) | Rcvd: 107 (7.162KB)
root@ip-10-10-78-18:~#
```

After waiting the time required for downloading we have received the following information.
So breaking the information down we used:
Nmap: Network mapper tool command
-sU: Tells us to perform a UDP scan
-F: Fast - Cuts ports from 1000 to 100
-v: Gives us updates from the scan as it progresses

```
nmap -sU -F -v 10.10.26.109
```