

Scanning with Masscan

We'll explore masscan, a powerful and lightning-fast TCP port scanner that can scan the entire Internet in under 6 minutes. While Nmap is the industry standard for network scanning, masscan offers unparalleled speed and efficiency, making it an essential tool in a security professional's arsenal.

Why Use Masscan?

Masscan is designed to scan networks at an extremely high rate, making it ideal for:

- **Scanning large networks or the entire Internet:** Masscan can scan the entire IPv4 address space in under 6 minutes, far surpassing the speed of Nmap.
- **Performing reconnaissance on a large scale:** Masscan allows you to quickly identify live hosts and open ports across vast networks, providing valuable intelligence for further investigation.
- **Evading detection:** Due to its speed, masscan can often evade firewalls and intrusion detection systems that may flag slower scans as malicious activity.
- **Stress testing systems:** Masscan's high-speed scanning capabilities can be used to test the resilience of systems and networks under heavy load.

To use masscan, we have to provide a port number and an IP address or the range of packets.

```
sudo masscan -p 80,22 192.168.29.0/24 --rate=10000
```

In this example, we have only provided a small IP range but masscan has the capability to scan the whole internet in just few minutes. So it is better to use it when we are dealing with a large network. But the thing to keep in mind is that, due to its fast nature it also creates a lot of noise in the network and if the number of packets is greater than the expected amount, then there is a chance that the network might also crash.
