Internet wide scanning has proven to be valuable methodology for security research. While it is possible to perform an internet-wide scan, this method has been more accessible to attackers as compared to researchers and tools like Nmap take a lot of time. Zmap is capable of scanning ipv4 address upto 1300x faster than Nmap thanks to its architecture. It can help reveal new vulnerabilities, monitor deployment of mitigation and shed light on things that were previously unknown. tracking and adopting defensive mechanisms. This paper discusses the architecture of the scanner, profile its performance and efficiency and explore the offensive defensive implications of internet-wide network surveys. This paper also urges to be a responsible of the internet.

The paper compares Nmap with Zmap since it was very much similar to Zmap. It tells us the ways in which Zmap is better than Nmap. It focusses on difference in probing methodologies, state of the connection, the retransmission policies. We performed several experiments to compare ZMap to Nmap in Internet-wide scanning applications, focusing on coverage and elapsed time to complete a scan. Nmap and ZMap are optimized for very different purposes. Nmap is a highly flexible, multipurpose tool that is frequently used for probing a large number of open ports on a smaller number of hosts, whereas ZMap is optimized to probe a single port across very large numbers of targets. We chose to compare the two because recent security studies used Nmap for Internet-wide surveys [10, 14], and because, like ZMap, Nmap operates from within user space on Linux [23].

ZMap uses a modular design. One of ZMap’s most important architectural features is that sending and receiving packets take place in separate threads that act independently and continuously throughout the scan. ZMap uses a simple and inexpensive method to traverse the address space, which lets it scan in a random permutation while maintaining only negligible state. The technique used by Zmap allows the sending thread to store the selected permutation and progress through it with only three integers: the primitive root used to generate the multiplicative group, the first scanned address, and the current address. Certain address ranges need to be excluded. Excluded ranges can be specified through a configuration file in case of performance reasons and to honor requests from their owners to discontinue scanning. ZMap is optimized to send probes as quickly as the source’s CPU and NIC can support. While the sending and receiving components of ZMap operate independently, we ensure that the receiver is initialized prior to sending probes and that the receiver continues to run for a period (by default, 8 seconds) after the sender has completed in order to process any delayed responses. Zmap uses inexpensive checks to prevent the incorrect reporting of unintended packets and this design ultimately allows the receiver to validate responses while sharing only the scan secret and the initial configuration with the sending component.

A complete scan of the public IPv4 address space takes approximately 44 minutes on an entry-level server with a gigabit Ethernet connection. We estimate that a single-packet scan can detect approximately 98% of instantaneously listening hosts, and we measure a 1300x performance improvement over Nmap for Internet-wide scanning, with equivalent coverage. The paper also experimentally confirms that Zmap can handle scanning 1.4M packets per seconds and that by sending a single SYN packet it covers upto 98% of the hosts. Given that Zmap performs scans so quickly the impact of the time of the day is also taken into consideration and the highest response rate was observed around 7am est mostly due to network congestion.

The ability to scan the IPv4 address space in under an hour opens an array of new research possibilities, including the ability to gain visibility into previously opaque distributed systems, understand protocol adoption at a new resolution, uncover security phenomenon only accessible with a global perspective, monitoring outages, private communication to a group of people. However, high-speed scanning also has potentially malicious applications, such as finding and attacking vulnerable hosts en masse. Furthermore, many developers have the preconceived notion that the Internet is far too large to be fully enumerated, so the reality of high speed scanning may disrupt existing security models, such as by leading to the discovery of services previously thought to be well hidden.

Aware of the scale associated with Zmap, the paper responsibly provides a set of guidelines to follow when using such an application and makes the user aware of the kind of problems that one may run into. It also rightfully stresses on the point of being responsible internet citizens. The paper also shows the kind of responses received during the study ranging from simply ignoring to downright retaliation. The paper acknowledges the recent work in the similar space and clearly present how Zmap excels in all the aspects of the previous techniques by staying in the limits and acting responsibly. The paper points out the that there is additional work required when it comes to scaling up zmap for ipv6, increased ethernet speeds and intelligently excluding hosts that do not wish to participate.