ZMap: The Internet Scanner

ZMap Team

Abstract

ZMap is a fast single packet network scanner designed for Internet-wide network surveys. https://github.com/zmap/zmap

1 Introduction

ZMap is a fast stateless single packet network scanner designed for Internet-wide network surveys. On a typical desktop computer with a gigabit Ethernet connection, ZMap is capable of scanning the entire public IPv4 address space on a single port in under 45 minutes. For example, sending a TCP SYN packet to every IPv4 address on port 25 to find all potential SMTP servers running on that port. With a 10gigE connection and netmap or PF_RING, ZMap can scan the IPv4 address space in under 5 minutes.

ZMap operates on GNU/Linux, Mac OS, and BSD. ZMap currently has fully implemented probe modules for TCP SYN scans, ICMP, DNS queries, UPnP, BACNET, and can send a large number of UDP probes. If you are looking to do more involved scans (e.g., banner grab or TLS handshake), take a look at ZGrab2, ZMap's sister project that performs stateful application-layer handshakes.

2 What is this document?

This is a placeholder file used for tracking papers that use ZMap, but do not cite the original ZMap paper (e.g., to support the type of metrics provided in *Ten Years of ZMap*). The content here mirrors Github.

Please do not directly cite this document.