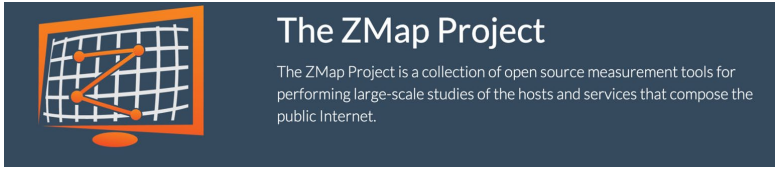
ZMap Project Updates and Feedback

Phillip Stephens - Stanford University

U.S. National Science Foundation
Pathways to Enable Open-Source Ecosystems

Empirical Security Research Group

- ZMap - Fast L4 Packet Scanner



The ZMap Project

The ZMap Project is a collection of open source measurement tools for performing large-scale studies of the hosts and services that compose the public Internet.

ZMap

ZMap is a fast single-packet network scanner optimized for Internet-wide network surveys. On a computer with a gigabit connection, ZMap can scan the entire public IPv4 address space on a single port in under 45 minutes. With a 10gigE connection and PF_RING, ZMap can scan the IPv4 address space in 5 minutes.

ZGrab

ZGrab is a stateful application-layer scanner. ZGrab is written in Go and supports HTTP, HTTPS, SSH, Telnet, FTP, SMTP, POP3, IMAP, Modbus, BACNET, Siemens S7, and Tridium Fox. For example, ZGrab can perform a TLS connection and collect the root HTTP page of all hosts ZMap finds on TCP/443.

ZDNS

ZDNS is a utility for performing fast DNS lookups, such as completing an A lookup for all names in a zone file, or collecting CAA records for a large number of websites. ZDNS contains its own recursive resolver and supports A, AAAA, ANY, AXFR, CAA, CNAME, DMARC, MX, NS, PTR, TXT, SOA, and SPF records.

LZR

LZR is a scanner that efficiently identifies what protocol an Internet service runs. LZR can identify 99% of unexpected Internet services in five handshakes. It runs as shim between ZMap and ZGrab.

ZCrypto

ZCrypto is a TLS and X.509 library for researchers. It is based on Go's standard library, but supports a more extensive set of cipher suites, extra lenient ASN.1 and X.509 parsing, and handshake transcription.

ZLint

ZLint is an X.509 certificate linter that checks for conformity with X.509 RFCs, CA/Browser Forum baseline requirements, root store policies, and ETSI standards.

ZCertificate

ZCertificate is a command-line utility that parses X.509 certificates, performs browser validation and ZLint tests, and produces a JSON encoding of the certificate.

ZAnnotate

ZAnnotate is a utility that annotates IPs with additional metadata, such as Maxmind GeoIP2 locations and routing data from a TABLE_DUMPv2 MRT file.

ZIterate

ZIterate is a utility that will produce random permutations of the IPv4 address space. It supports selecting IPs from a set of networks and sharding across multiple servers.

ZBlocklist

ZBlocklist allows quickly filtering out IP addresses that belong to a set of network blocks. It can be used to remove organizations who have requested exclusion from scans.

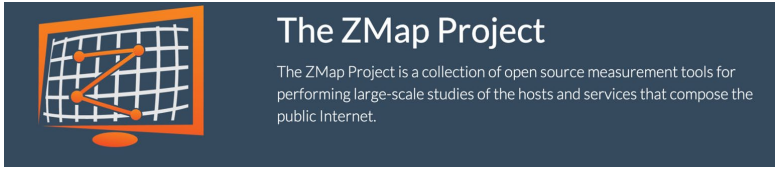
ZTee

ZTee is a custom version of the Linux utility tee that can efficiently buffer large amounts of scan data between different phases of a scan. It also produces metadata and updates on progress.

ZSchema

ZSchema is a high-level programming language for describing database schemas. Schemas can be used to validate datasets and be compiled into schemas for other databases.

- ZMap - Fast L4 Packet Scanner
- ZDNS - “dig for bulk lookups”



The ZMap Project

The ZMap Project is a collection of open source measurement tools for performing large-scale studies of the hosts and services that compose the public Internet.

ZMap

ZMap is a fast single-packet network scanner optimized for Internet-wide network surveys. On a computer with a gigabit connection, ZMap can scan the entire public IPv4 address space on a single port in under 45 minutes. With a 10gigE connection and PF_RING, ZMap can scan the IPv4 address space in 5 minutes.

ZGrab

ZGrab is a stateful application-layer scanner. ZGrab is written in Go and supports HTTP, HTTPS, SSH, Telnet, FTP, SMTP, POP3, IMAP, Modbus, BACNET, Siemens S7, and Tridium Fox. For example, ZGrab can perform a TLS connection and collect the root HTTP page of all hosts ZMap finds on TCP/443.

ZDNS

ZDNS is a utility for performing fast DNS lookups, such as completing an A lookup for all names in a zone file, or collecting CAA records for a large number of websites. ZDNS contains its own recursive resolver and supports A, AAAA, ANY, AXFR, CAA, CNAME, DMARC, MX, NS, PTR, TXT, SOA, and SPF records.

LZR

LZR is a scanner that efficiently identifies what protocol an Internet service runs. LZR can identify 99% of unexpected Internet services in five handshakes. It runs as shim between ZMap and ZGrab.

ZCrypto

ZCrypto is a TLS and X.509 library for researchers. It is based on Go's standard library, but supports a more extensive set of cipher suites, extra lenient ASN.1 and X.509 parsing, and handshake transcription.

ZLint

ZLint is an X.509 certificate linter that checks for conformity with X.509 RFCs, CA/Browser Forum baseline requirements, root store policies, and ETSI standards.

ZCertificate

ZCertificate is a command-line utility that parses X.509 certificates, performs browser validation and ZLint tests, and produces a JSON encoding of the certificate.

ZAnnotate

ZAnnotate is a utility that annotates IPs with additional metadata, such as Maxmind GeoIP2 locations and routing data from a TABLE_DUMPv2 MRT file.

ZIterate

ZIterate is a utility that will produce random permutations of the IPv4 address space. It supports selecting IPs from a set of networks and sharding across multiple servers.

ZBlocklist

ZBlocklist allows quickly filtering out IP addresses that belong to a set of network blocks. It can be used to remove organizations who have requested exclusion from scans.

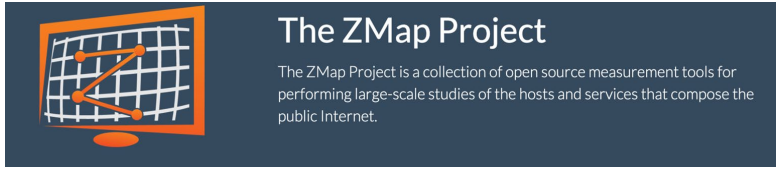
ZTee

ZTee is a custom version of the Linux utility tee that can efficiently buffer large amounts of scan data between different phases of a scan. It also produces metadata and updates on progress.

ZSchema

ZSchema is a high-level programming language for describing database schemas. Schemas can be used to validate datasets and be compiled into schemas for other databases.

- ZMap - Fast L4 Packet Scanner
- ZDNS - “dig for bulk lookups”
- ZGrab2 - L7 application scanner



The ZMap Project

The ZMap Project is a collection of open source measurement tools for performing large-scale studies of the hosts and services that compose the public Internet.

ZMap

ZMap is a fast single-packet network scanner optimized for Internet-wide network surveys. On a computer with a gigabit connection, ZMap can scan the entire public IPv4 address space on a single port in under 45 minutes. With a 10gigE connection and PF_RING, ZMap can scan the IPv4 address space in 5 minutes.

ZGrab

ZGrab is a stateful application-layer scanner. ZGrab is written in Go and supports HTTP, HTTPS, SSH, Telnet, FTP, SMTP, POP3, IMAP, Modbus, BACNET, Siemens S7, and Tridium Fox. For example, ZGrab can perform a TLS connection and collect the root HTTP page of all hosts ZMap finds on TCP/443.

ZDNS

ZDNS is a utility for performing fast DNS lookups, such as completing an A lookup for all names in a zone file, or collecting CAA records for a large number of websites. ZDNS contains its own recursive resolver and supports A, AAAA, ANY, AXFR, CAA, CNAME, DMARC, MX, NS, PTR, TXT, SOA, and SPF records.

LZR

LZR is a scanner that efficiently identifies what protocol an Internet service runs. LZR can identify 99% of unexpected Internet services in five handshakes. It runs as shim between ZMap and ZGrab.

ZCrypto

ZCrypto is a TLS and X.509 library for researchers. It is based on Go's standard library, but supports a more extensive set of cipher suites, extra lenient ASN.1 and X.509 parsing, and handshake transcription.

ZLint

ZLint is an X.509 certificate linter that checks for conformity with X.509 RFCs, CA/Browser Forum baseline requirements, root store policies, and ETSI standards.

ZCertificate

ZCertificate is a command-line utility that parses X.509 certificates, performs browser validation and ZLint tests, and produces a JSON encoding of the certificate.

ZAnnotate

ZAnnotate is a utility that annotates IPs with additional metadata, such as Maxmind GeoIP2 locations and routing data from a TABLE_DUMPv2 MRT file.

ZIterate

ZIterate is a utility that will produce random permutations of the IPv4 address space. It supports selecting IPs from a set of networks and sharding across multiple servers.

ZBlocklist

ZBlocklist allows quickly filtering out IP addresses that belong to a set of network blocks. It can be used to remove organizations who have requested exclusion from scans.

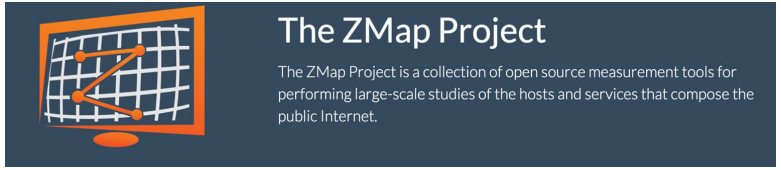
ZTee

ZTee is a custom version of the Linux utility tee that can efficiently buffer large amounts of scan data between different phases of a scan. It also produces metadata and updates on progress.

ZSchema

ZSchema is a high-level programming language for describing database schemas. Schemas can be used to validate datasets and be compiled into schemas for other databases.

- ZMap - Fast L4 Packet Scanner
- ZDNS - “dig for bulk lookups”
- ZGrab2 - L7 application scanner
- ZLint - Web PKI Certificate Linter



The ZMap Project

The ZMap Project is a collection of open source measurement tools for performing large-scale studies of the hosts and services that compose the public Internet.

ZMap

ZMap is a fast single-packet network scanner optimized for Internet-wide network surveys. On a computer with a gigabit connection, ZMap can scan the entire public IPv4 address space on a single port in under 45 minutes. With a 10gigE connection and PF_RING, ZMap can scan the IPv4 address space in 5 minutes.

ZGrab

ZGrab is a stateful application-layer scanner. ZGrab is written in Go and supports HTTP, HTTPS, SSH, Telnet, FTP, SMTP, POP3, IMAP, Modbus, BACNET, Siemens S7, and Tridium Fox. For example, ZGrab can perform a TLS connection and collect the root HTTP page of all hosts ZMap finds on TCP/443.

ZDNS

ZDNS is a utility for performing fast DNS lookups, such as completing an A lookup for all names in a zone file, or collecting CAA records for a large number of websites. ZDNS contains its own recursive resolver and supports A, AAAA, ANY, AXFR, CAA, CNAME, DMARC, MX, NS, PTR, TXT, SOA, and SPF records.

LZR

LZR is a scanner that efficiently identifies what protocol an Internet service runs. LZR can identify 99% of unexpected Internet services in five handshakes. It runs as shim between ZMap and ZGrab.

ZCrypto

ZCrypto is a TLS and X.509 library for researchers. It is based on Go's standard library, but supports a more extensive set of cipher suites, extra lenient ASN.1 and X.509 parsing, and handshake transcription.

ZLint

ZLint is an X.509 certificate linter that checks for conformity with X.509 RFCs, CA/Browser Forum baseline requirements, root store policies, and ETSI standards.

ZCertificate

ZCertificate is a command-line utility that parses X.509 certificates, performs browser validation and ZLint tests, and produces a JSON encoding of the certificate.

ZAnnotate

ZAnnotate is a utility that annotates IPs with additional metadata, such as Maxmind GeoIP2 locations and routing data from a TABLE_DUMPv2 MRT file.

ZIterate

ZIterate is a utility that will produce random permutations of the IPv4 address space. It supports selecting IPs from a set of networks and sharding across multiple servers.

ZBlocklist

ZBlocklist allows quickly filtering out IP addresses that belong to a set of network blocks. It can be used to remove organizations who have requested exclusion from scans.

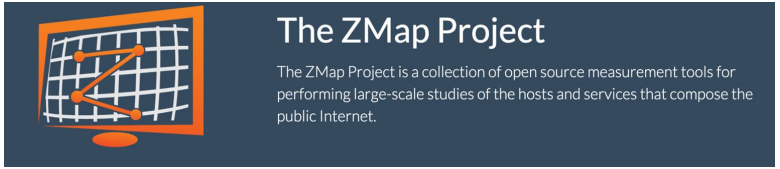
ZTee

ZTee is a custom version of the Linux utility tee that can efficiently buffer large amounts of scan data between different phases of a scan. It also produces metadata and updates on progress.

ZSchema

ZSchema is a high-level programming language for describing database schemas. Schemas can be used to validate datasets and be compiled into schemas for other databases.

- ZMap - Fast L4 Packet Scanner
  - Multiple ports in single scan
- ZDNS - “dig for bulk lookups”
  - Library API
  - -all-nameservers mode
- ZGrab2 - L7 application scanner
  - Bring your own dialer
  - New Application modules



The ZMap Project

The ZMap Project is a collection of open source measurement tools for performing large-scale studies of the hosts and services that compose the public Internet.

ZMap

ZMap is a fast single-packet network scanner optimized for Internet-wide network surveys. On a computer with a gigabit connection, ZMap can scan the entire public IPv4 address space on a single port in under 45 minutes. With a 10gigE connection and PF_RING, ZMap can scan the IPv4 address space in 5 minutes.

ZGrab

ZGrab is a stateful application-layer scanner. ZGrab is written in Go and supports HTTP, HTTPS, SSH, Telnet, FTP, SMTP, POP3, IMAP, Modbus, BACNET, Siemens S7, and Tridium Fox. For example, ZGrab can perform a TLS connection and collect the root HTTP page of all hosts ZMap finds on TCP/443.

ZDNS

ZDNS is a utility for performing fast DNS lookups, such as completing an A lookup for all names in a zone file, or collecting CAA records for a large number of websites. ZDNS contains its own recursive resolver and supports A, AAAA, ANY, AXFR, CAA, CNAME, DMARC, MX, NS, PTR, TXT, SOA, and SPF records.

LZR

LZR is a scanner that efficiently identifies what protocol an Internet service runs. LZR can identify 99% of unexpected Internet services in five handshakes. It runs as shim between ZMap and ZGrab.

ZCrypto

ZCrypto is a TLS and X.509 library for researchers. It is based on Go's standard library, but supports a more extensive set of cipher suites, extra lenient ASN.1 and X.509 parsing, and handshake transcription.

ZLint

ZLint is an X.509 certificate linter that checks for conformity with X.509 RFCs, CA/Browser Forum baseline requirements, root store policies, and ETSI standards.

ZCertificate

ZCertificate is a command-line utility that parses X.509 certificates, performs browser validation and ZLint tests, and produces a JSON encoding of the certificate.

ZAnnotate

ZAnnotate is a utility that annotates IPs with additional metadata, such as Maxmind GeoIP2 locations and routing data from a TABLE_DUMPv2 MRT file.

ZIterate

ZIterate is a utility that will produce random permutations of the IPv4 address space. It supports selecting IPs from a set of networks and sharding across multiple servers.

ZBlocklist

ZBlocklist allows quickly filtering out IP addresses that belong to a set of network blocks. It can be used to remove organizations who have requested exclusion from scans.

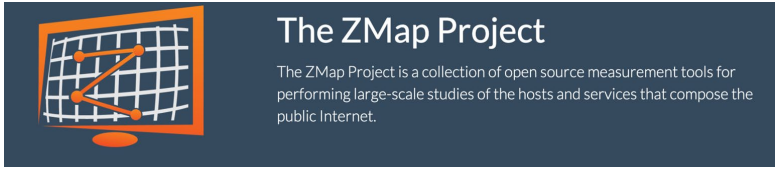
ZTee

ZTee is a custom version of the Linux utility tee that can efficiently buffer large amounts of scan data between different phases of a scan. It also produces metadata and updates on progress.

ZSchema

ZSchema is a high-level programming language for describing database schemas. Schemas can be used to validate datasets and be compiled into schemas for other databases.

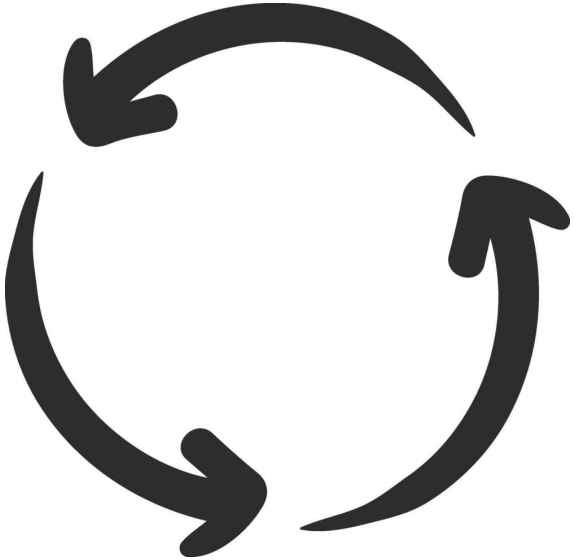
- National Science Foundation
  - Pathways to Enable Open-Source Ecosystems - POSE
- User/Ecosystem Discovery
  - Users
  - Contributors
  - Maintainers
  - Successful Open-Source Projects
  - Commercial Users



Sustainability

- Open-Source “crowd sourced” development

- Commercial users contributing engineer hours / recurring monetary contributions
  - ZLint
  - Dual-licensing?
  - Industry affiliates program?



Empirical Security Research Group

What we've learned so far (n = 80)

- Things are working for people (broadly)
- Cross-tool Documentation
  - Using tools *together* to solve use cases
  - New website?
- ZMap
  - Inconsistent versioning across pkg managers + source
  - Performance tuning guidance
- ZGrab
  - Making HTTP module *just work* out-of-the-box


HETEMEEL.COM
I WANT YOU
TO TALK WITH ME ABOUT
THE ZMAP PROJECT!