Slow Network Recon Service

Jako shodan, ale …

About project

SNER is a proactive network monitoring service operated by CESNET for network security and research purposes within the CESNET2 network.

The service continuously maps enrolled networks, performs service discovery, and conducts fingerprinting similar to Shodan, Censys, and Shadowserver services. Participating networks can enhance their visibility within their address space and potentially receive early warnings about possible vulnerabilities.

- GitHub project: https://github.com/bodik/sner4
- Scanning Sources: Dynamic and identifiable via DNS as snerXX.flab.cesnet.cz.
- Scanning Techniques:
  - IP enumeration
  - DNS enumeration
  - TCP SYN scan
  - UDP service discovery
  - Service version fingerprinting
  - JA3/JARM scanning
  - TLS scanning
  - Vulnerability scanning (Nuclei)
- Data Mining Techniques:
  - Service version extraction
  - CPE-CVE correlation

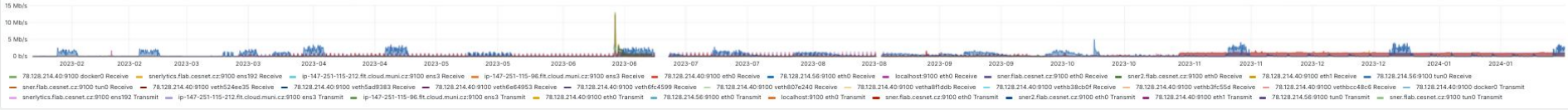
storage stats

hosts	services	vulns	notes
4170	12228	0	34611

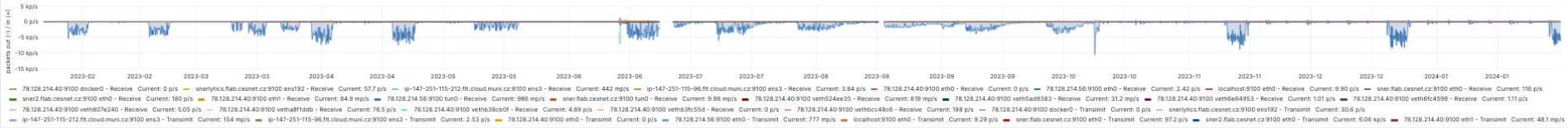
job stats

jobs failed	jobs finished	jobs running	jobs stale
0	1	6	0

Network Traffic Basic



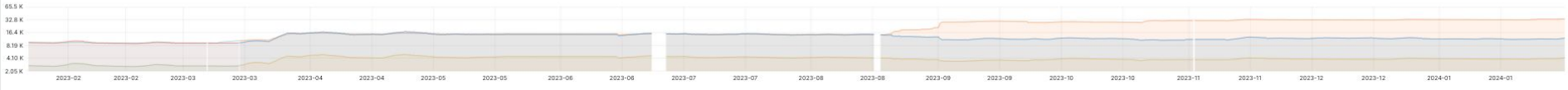
Network Traffic by Packets



jobs

queues

storage



Use-cases

1 External tenants

Enrolled organizations can utilize the SNER service to expand the visibility of their respective infrastructure's Internet attack surface. External users can access available data through the API.

1.1 Setup shell

Get API token in web interface on user profile page (*user > profile > apikey generate*). Setup shell environment for calling API:

```
export APIKEY=""
export URL="https://sner.flab.cesnet.cz/sner"
alias snerapi='curl -s -H "X-API-KEY: $APIKEY"'
```

1.2 Get information about single host

Any service SHOULD NOT be visible from public Internet on core IdP or Directory controllers.

```
snerapi -XPOST \
  "$URL/api/v2/public/storage/host" \
  --json '{"address": "203.0.113.50"}' | jq
```

```
{
  "address": "203.0.113.50",
  "hostname": "dc1.example.org",
  "services": [
    {
      "info": "extrainfo: Anonymous bind OK",
      "notes": [
        {
```

Table of contents

SNER - Slow Network Recon Service

Enrollment procedure

To enroll, please send your initial enrollment requests to flab@cesnet.cz. Your application should include the following:

- IPv4 ranges
- IPv6 ranges
- A list of individuals who will be using the service (eduID.cz attributes eduPersonUniqueId and email are required).

After your application is accepted, users will be able to login via eduID.cz federation SSO to access the web interface and use the service as described in use-cases.