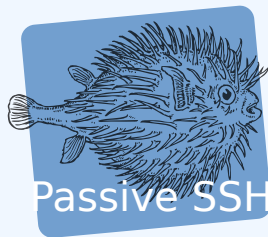


Passive SSH, a Fast-Lookup Database of SSH Key Materials to Support Incident Response

Team CIRCL

<https://www.d4-project.org/>

2020-11-16



- CIRCL (and other CSIRTs) have their own passive DNS¹ and passive SSL² database
- Historical data is a companion to incident response, infrastructure attribution and threat intelligence at large
- **SSH is a major protocol for remote management** (for normal users but also attackers)
- SSH protocol provides a significant **number of fingerprints** to track similar infrastructures (e.g. from banners to key fingerprints)

¹<https://www.circl.lu/services/passive-dns/>

²<https://www.circl.lu/services/passive-ssl/>

- A fast-lookup database to find SSH key per IP, fingerprint or hassh³
- Supporting the storage of the key materials, key types and banners
- **Lightweight design** and supporting different kind of importers (scanner, network capture)
- The system can be used externally (for Internet-wide scan) or internally (for internal network ssh infrastructure scanning)
- Supporting IPv4, IPv6 but also Tor onion addresses or random TCP ports

³<https://github.com/salesforce/hassh>

- Get in touch if you want to get access to the **Passive SSH database** (you need to be a FIRST.org, TF-CSIRT or CNW member)
- Contact: info@circl.lu
- Source code:
<https://github.com/D4-project/passive-ssh> -
https://twitter.com/d4_project