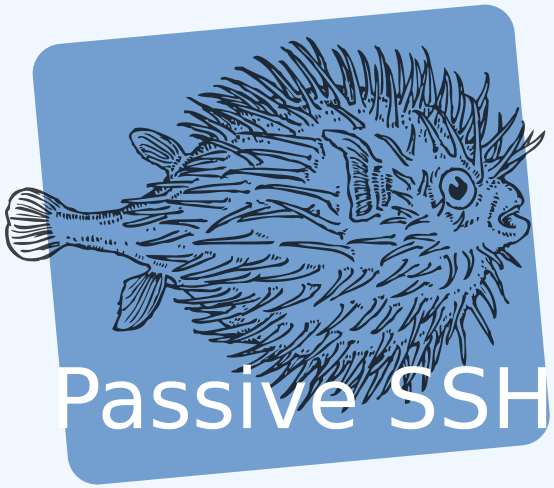
Passive SSH, a Fast-Lookup Database of SSH Key Materials to Support Incident Response

Team CIRCL
https://www.d4-project.org/

2020-11-16



Alexandre Dulaunoy - Aurelien Thirion

Problem statement

- CIRCL (and other CSIRTs) have their own passive DNS[1] and passive SSL[2] 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/

Passive SSH design

- A fast-lookup database to find SSH key per IP, fingerprint or hassh[3]
- 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

Passive SSH open source software

- Software written in Python 3 and released as an open source project[4]
- The database is a **Redis-compatible backend** (you can use Redis, kv-rocks or any compatible Redis backend)
- A sample SSH scanner is included to scan small networks or internal infrastructure
- CIRCL provides a **database with an Internet-wide scan** (access can be requested for FIRST, TF-CSIRT and CNW memmbers)

[4] https://github.com/D4-project/passive-ssh

What's next?

- A MISP module to get Passive **SSH expansion and pivots in MISP project**
- Pcap feeder to Passive SSH
- Review of cryptographic materials[5] from existing Passive SSH database
- Improvement of the Passive SSH code base and release of version 1.0

[5] https://github.com/D4-project/snake-oil-crypto

Contact

- 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`