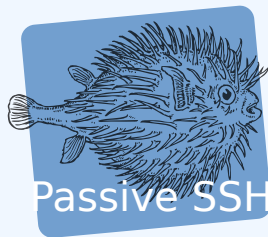


# Passive SSH, a Fast-Lookup Database of SSH Key Materials to Support Incident Response

Team CIRCL

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

2020-11-16



- CIRCL (and other CSIRTs) have their own passive DNS<sup>1</sup> and passive SSL<sup>2</sup> 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)

---

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

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

- A fast-lookup database to find SSH key per IP, fingerprint or hassh<sup>3</sup>
- 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

---

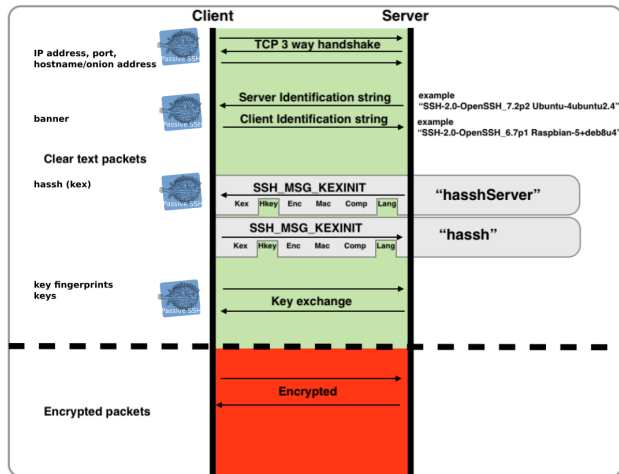
<sup>3</sup><https://github.com/salesforce/hassh>

- Software written in Python 3 and released as an open source project<sup>4</sup>
- 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 from an Internet-wide scan** (access can be requested for FIRST, TF-CSIRT and CNW members)

---

<sup>4</sup><https://github.com/D4-project/passive-ssh>

# WHAT DO YOU STORE? OR WHAT CAN I LOOKUP?



```
1 curl -s http://127.0.0.1:8500/banners | jq .
2 {
3   "banners": {
4     "SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3": 14522,
5     "SSH-2.0-OpenSSH_7.4": 8036,
6     "SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2": 4563,
7     "SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8": 4464,
8     "SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7": 4301,
9     "SSH-2.0-OpenSSH_5.3": 2930,
10    "SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1": 2901,
11    "SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10": 2669,
12    "SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u8": 2295,
13    "SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u6": 1192,
14    "SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13": 1107,
15    "SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u3": 1024,
```

```
1 curl -s "http://127.0.0.1:8500/banner/hosts/SSH-2.0-  
    OpenSSH_6.7p1%20OVH-rescue" | jq .  
2 {  
3     "banner": "SSH-2.0-OpenSSH_6.7p1 OVH-rescue",  
4     "hosts": [  
5         "188.165.216.153",  
6         "137.74.204.16",  
7         "188.165.233.197",  
8         "188.165.199.211",  
9         "188.165.192.121",  
10        "137.74.204.58",  
11        "188.165.224.149",  
12        "188.165.211.205",  
13        "188.165.216.162",  
14        "188.165.216.155",  
15        "188.165.194.193",
```

```
1 curl -s "http://127.0.0.1:8500/banner/hosts/SSH-2.0-lancom"  
    | jq .  
2 {  
3   "banner": "SSH-2.0-lancom",  
4   "hosts": [  
5     "89.1.181.237",  
6     "89.0.231.177",  
7     "91.0.158.6",  
8     "91.0.54.88",  
9     "91.0.146.13",  
10    "91.1.54.42",  
11    "91.1.23.189",  
12    "89.1.29.178",  
13    "91.0.184.142",  
14    "89.1.183.80",  
15    "89.1.142.156",  
16    "89.1.31.148",
```



```

1  curl -s "http://127.0.0.1:8500/host/ssh/89.1.181.237" | jq .
2  {
3    "first_seen": "20201116",
4    "last_seen": "20201116",
5    "port": 22,
6    "banner": [
7      "SSH-2.0-lancom"
8    ],
9    "hassh": {
10     "deabc869d8b35c2fbef0831b838bf196": [
11       "{ \"key\": [\"rsa-sha2-512\", \"rsa-sha2-256\", \"ssh-rsa\", \"ssh-dss\"], \"
12         encrypt\": [\"aes256-ctr\", \"aes192-ctr\", \"aes128-ctr\", \"aes256-cbc\",
13         \"aes192-cbc\", \"aes128-cbc\", \"blowfish-ctr\", \"
14         blowfish-cbc\", \"arcfour256\", \"arcfour128\", \"arcfour\", \"3des-ctr\", \"3des-cbc\"],
15         \"mac\": [\"hmac-sha2-512\", \"hmac-sha2-512-96\", \"hmac-sha2-256\", \"hmac-sha2
16         -256-96\", \"hmac-sha1\", \"hmac-sha1-96
17         \", \"hmac-md5\", \"hmac-md5-96\"], \"compress\": [\"none\", \"zlib\"], \"lang\": [ ]}"
18     ]
19   },
20   "keys": [
21     {
22       "type": "ssh-rsa",
23       "fingerprint": "af:80:1e:6f:5a:cf:f3:6e:7d:2a:aa:a5:f3:05:0e:1b"
24     },
25     {
26       "type": "ssh-dss",
27       "fingerprint": "8a:b9:c0:a6:b3:20:de:86:f6:10:97:8e:27:be:f1:ea"
28     }
29   ]
30 }

```

```
1 curl -s "http://127.0.0.1:8500/fingerprint/all/af:80:1e:6f
   :5a:cf:f3:6e:7d:2a:aa:a5:f3:05:0e:1b" | jq .
2 {
3   "type": "ssh-rsa",
4   "first_seen": "20201116",
5   "last_seen": "20201116",
6   "base64": "ssh-rsa AAAAB3NzaC1yc2EAAAABEQAAAEAwE/8
   ooNGMyQCYTYcdLAAj1Da3e4uPbLNBA7zs/
   oKdeS9JhuJB05oN0rwKk9B7Y429AL3OHHZUPVQMj2Rt+fEf0bYtLt
   +BI+289/DYdddUNxX3gU80rF4qiz1uQJ1FjcyW+
   LN1y219DE9rSshjY6aNPUSHdhRuGnBxS
7   NMJCl3pM6uxPnUhirccpobnHz09C2cFAIMRGuy1/iJM/
   fwngGAlxYqtPJ8Pff7rTTcDrPF7YB7STSQXvBTgiwCHVEuxyQaX7Aik5BM0A
   +01W8j1b+lN+yzT4+EZbQJ4kQKfNb8aGWAcHacjs9V0fr4w79ynz/
   lPQ==",
8   "fingerprint": "af:80:1e:6f:5a:cf:f3:6e:7d:2a:aa:a5:f3
   :05:0e:1b",
9   "hosts": [
10    "89.1.181.237"
11  ]
12 }
```

# WHAT'S NEXT?

- A MISP module to get Passive **SSH expansion and pivots in MISP project**
- Add SSH correlation in AIL framework for crawled Tor hidden services<sup>5</sup>
- Pcap feeder to Passive SSH
- Review of cryptographic materials<sup>6</sup> from existing Passive SSH database
- Improvement of the Passive SSH code base and release of version 1.0

---

<sup>5</sup><https://github.com/ail-project/ail-framework>

<sup>6</sup><https://github.com/D4-project/snake-oil-crypto>

- 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](mailto:info@circl.lu)
- Source code:  
<https://github.com/D4-project/passive-ssh> -  
[https://twitter.com/d4\\_project](https://twitter.com/d4_project)