Certificate Transparency Logs

Cheat Sheet

In the sprawling mass of the internet, trust is a fragile commodity. One of the cornerstones of this trust is the `Secure Sockets Layer/Transport Layer Security` (`SSL/TLS`) protocol, which encrypts communication between your browser and a website. At the heart of SSL/TLS lies the `digital certificate`, a small file that verifies a website's identity and allows for secure, encrypted communication.

However, the process of issuing and managing these certificates isn't foolproof. Attackers can exploit rogue or mis-issued certificates to impersonate legitimate websites, intercept sensitive data, or spread malware. This is where Certificate Transparency (CT) logs come into play.

What are Certificate Transparency Logs?

`Certificate Transparency` (`CT`) logs are public, append-only ledgers that record the issuance of SSL/TLS certificates. Whenever a Certificate Authority (CA) issues a new certificate, it must submit it to multiple CT logs. Independent organisations maintain these logs and are open for anyone to inspect.

Think of CT logs as a `global registry of certificates`. They provide a transparent and verifiable record of every SSL/TLS certificate issued for a website. This transparency serves several crucial purposes:

- `Early Detection of Rogue Certificates`: By monitoring CT logs, security researchers and website owners can quickly identify suspicious or misissued certificates. A rogue certificate is an unauthorized or fraudulent digital certificate issued by a trusted certificate authority. Detecting these early allows for swift action to revoke the certificates before they can be used for malicious purposes.
- `Accountability for Certificate Authorities`: CT logs hold CAs accountable for their issuance practices. If a CA issues a certificate that violates the rules or standards, it will be publicly visible in the logs, leading to potential sanctions or loss of trust.
- `Strengthening the Web PKI (Public Key Infrastructure)`: The Web PKI is the trust system underpinning secure online communication. CT logs help to enhance the security and integrity of the Web PKI by providing a mechanism for public oversight and verification of certificates.

▶ Click to expand a technical breakdown of how CT Logs Work

CT Logs and Web Recon

Certificate Transparency logs offer a unique advantage in subdomain enumeration compared to other methods. Unlike brute-forcing or wordlist-based approaches, which rely on guessing or predicting subdomain names, CT logs provide a definitive record of certificates issued for a domain and its subdomains. This means you're not limited by the scope of your wordlist or the effectiveness of your brute-forcing algorithm. Instead, you gain access to a historical and comprehensive view of a domain's subdomains, including those that might not be actively used or easily guessable.

Furthermore, CT logs can unveil subdomains associated with old or expired certificates. These subdomains might host outdated software or configurations, making them potentially vulnerable to exploitation.

In essence, CT logs provide a reliable and efficient way to discover subdomains without the need for exhaustive brute-forcing or relying on the completeness of wordlists. They offer a unique window into a domain's history and can reveal subdomains that might otherwise remain hidden, significantly enhancing your reconnaissance capabilities.

Searching CT Logs

There are two popular options for searching CT logs:

Tool	Key Features	Use Cases	Pros	Cons
crt.sh	User-friendly web interface, simple search by domain, displays certificate details, SAN entries.	Quick and easy searches, identifying subdomains, checking certificate issuance history.	Free, easy to use, no registration required.	Limited filtering and analysis options.
Censys	Powerful search engine for internet-connected devices, advanced filtering by domain, IP, certificate attributes.	In-depth analysis of certificates, identifying misconfigurations, finding related certificates and hosts.	Extensive data and filtering options, API access.	Requires registration (free tier available).

crt.sh lookup

While `crt.sh` offers a convenient web interface, you can also leverage its API for automated searches directly from your terminal. Let's see how to find all 'dev' subdomains on `facebook.com` using `curl` and `jq`:

Certificate Transparency Logs

```
MisaelMacias@htb[/htb]$ curl -s "https://crt.sh/?q=facebook.com&output=json" | jq -r '.[]
  | select(.name_value | contains("dev")) | .name_value' | sort -u

*.dev.facebook.com
*.newdev.facebook.com
*.secure.dev.facebook.com
dev.facebook.com
devvm1958.ftw3.facebook.com
facebook-amex-dev.facebook.com
facebook-amex-sign-enc-dev.facebook.com
newdev.facebook.com
secure.dev.facebook.com
```

- `curl -s "https://crt.sh/?q=facebook.com&output=json"`: This command fetches the JSON output from crt.sh for certificates matching the domain `facebook.com`.
- `jq -r '.[] | select(.name_value | contains("dev")) | .name_value'`: This part filters the JSON results, selecting only entries where the `name_value` field (which contains the domain or subdomain) includes the string "`dev`". The `-r` flag tells `jq` to output raw strings.
- `sort -u`: This sorts the results alphabetically and removes duplicates.

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

- `sort -u`: This sorts the results alphabetically and removes duplicates.

← Previous Next →

Mark Complete & Next