

lbd

The LBD (Load Balancer Detector) tool in Linux is a utility designed to detect the presence of load balancers in front of a web server. It helps in identifying if a server is being load balanced, which can be useful for network administrators, security professionals, and researchers. LBD relies on specific detection techniques and might not detect all types of load balancers, especially more modern or proprietary solutions. If you require more thorough analysis, consider using additional tools or services specializing in network analysis and security.

➤ **DNS-based Load Balancing Detection:**

- LBD checks if multiple IP addresses are returned when resolving a domain name. If multiple IP addresses are found, it indicates that DNS-based load balancing might be in use.
- DNS-based load balancing distributes traffic across different servers by providing different IP addresses for the same domain name.

➤ **HTTP-based Load Balancing Detection:**

- LBD sends multiple HTTP requests to the server and analyzes the responses to see if they come from different backend servers. This is determined by variations in HTTP headers, cookies, and other response characteristics.
- HTTP-based load balancing involves distributing HTTP requests across multiple servers, often using different backends to handle each request.

Example: -

1. To check weather a domain is using load balancer over its DNS and HTTP server or not use lbd command along with the target domain.

```
lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
Written by Stefan Behte (http://ge.mine.nu)
Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
gws
NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 16:39:11, 16:39:12, 16:39:12, 16:39:12, 16:39:12, 16:39:13, 16:39:13, 16:39:20, 16:39:21, 16:39:21, 16:39:21, 16:39:22, 16:39:22, 16:39:23, 16:39:23, 16:39:23, 16:39:24, 16:39:24, 16:39:24, 16:39:25, 16:39:25, 16:39:25, 16:39:25, 16:39:26, 16:39:26, 16:39:26, 16:39:27, 16:39:27, 16:39:27, 16:39:28, 16:39:28, 16:39:28, 16:39:28, 16:39:29, 16:39:29, 16:39:29, 16:39:30, 16:39:30, 16:39:30, 16:39:31, 16:39:31, 16:39:31, 16:39:32, 16:39:37, 16:39:37, 16:39:37, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-NdInK-e7Xd0gXARwD-xZBQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http;report-uri https://csp.withgoogle.com/csp/gws/other-hp
> Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-h1jz8NeEfplHuUXntd9Q' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http;report-uri https://csp.withgoogle.com/csp/gws/other-hp

google.com does Load-balancing. Found via Methods: HTTP[Diff]
```

In the above example google is using load balancer on both HTTP and DNS server as we can see multiple IP addresses and varying HTTP response headers.

2. Now in this we will perform the same on a domain that is not using load balancer over DNS server.

```
(kali@kali)-[~]
$ sudo lbd

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
Written by Stefan Behte (http://ge.mine.nu)
Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
Apache/2.4.52 (Ubuntu)
NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 16:40:44, 16:40:44, 16:40:45, 16:40:45, 16:40:46, 16:40:46, 16:40:47, 16:40:47, 16:40:53, 16:40:54, 16:40:54, 16:40:55, 16:40:56, 16:40:58, 16:40:59, 16:41:02, 16:41:10, 16:41:14, 16:41:14, 16:41:15, 16:41:15, 16:41:16, 16:41:16, 16:41:17, 16:41:17, 16:41:19, 16:41:19, 16:41:19, 16:41:20, 16:41:20, 16:41:21, 16:41:21, 16:41:23, 16:41:30, 16:41:31, 16:41:32, 16:41:33, 16:41:34, 16:41:34, 16:41:35, 16:41:35, 16:41:36, 16:41:36, 16:41:38, 16:41:38, 16:41:43, 16:41:44, 16:41:59, 16:42:03, 16:42:03, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< HTTP/1.1 301 Moved Permanently
< Server: Apache/2.4.52 (Ubuntu)
< Location: ht
< Connection: close
< Content-Type: text/html; charset=iso-8859-1
<

does Load-balancing. Found via Methods: HTTP[Diff]
```