


# **Load Balancer: Detection and Evasion**

## Intro



A load balancer corresponds to a piece of technology that is located in front of the web servers. This is one of ensuring the availability of web applications and balancing the load in case there is a lot of traffic.

In the case of security, if there is a load balancer we will be able to access the web application behind it, **but we will not be able to see the services run by the machine that is using the web server**. For example, if we launch a service scan with Nmap  to a server that has a load balancer, what we will really see are the services exposed by the machine that is acting as a load balancer and the server that provides the website, because the load balancer will be put in front.

## **Tools to detect load balancers**

### **Load Balancer Detector**

#### Intro

Load balancer detector is a tool that, as its name says, will allow us to detect if a web application has a load balancer. Vine is pre-installed in  Kali and  Parrot, and is used from the terminal

#### Load balancer detector in action

To use this tool it is as simple as placing from terminal **lbd** followed by the web page we want to scan and the result would be like this:

**lbd** <http://website.target/>

```
(kali@kali)~$ lbd https://www.hackthissite.org/
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]:

NOT FOUND

Checking for HTTP-Loadbalancing [Date]: , No date header found, skipping.
Checking for HTTP-Loadbalancing [Diff]: NOT FOUND
https://www.hackthissite.org/ does NOT use Load-balancing.
```

In this way, and as seen in the result, it will tell us whether or not the site we are auditing has a load balancer.

## **Evasion**

In case **YES**, it will display all the IP addresses related to the web server and/or the load balancer, or only the real server. In case more than one is displayed, for example at the DNS level.

Some of them may be the web server and the others may be the load balancer and other addresses, such as we may find that of the web server. What is going to be screened is that of the *load balancer* if you have it.

If a balancer is **well configured** IT CANNOT BE BYPASSED so it does not give us the IP addresses of the web servers we are auditing.

What we could do is use passive information collection techniques using tools such as **Shodan, Censis, etc..** to locate the addresses **public IPs** and from these carry out the exploitation

Still a load balancer **It is not a security piece**. While it is true that it limits our access to certain services that are exposed to the web server, it does not limit us to using Web Hacking techniques such as **SQL injection, Cross Site Scripting**, inter alia.