Technical Report

Injection Machine

Víctor Moreno Pérez

Contents

1 Background

Downloaded from **DockerLabs**

DockerLabs is a collection of hands-on tutorials and interactive learning resources designed to help users learn about Docker and containerization technologies. It provides a practical, hands-on approach to understanding Docker's core concepts, tools, and workflows. Users can explore various topics, such as building and deploying applications in containers, managing container orchestration with tools like Kubernetes, and optimizing container performance. Docker Labs aims to make learning accessible for developers, DevOps engineers, and anyone interested in modern application development and deployment practices.

2 Reconnaissance

First of all, we use **nmap** to make a general port scan over the victim machine.

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 13:10 CEST
Initiating ARP Ping Scan at 13:10
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 13:10, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:10
Scanning 172.17.0.2 [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 13:10, 0.83s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000050s latency).
Scanned at 2024-10-05 13:10:37 CEST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Figure 1: Nmap General View

We can see that there are two opened ports : **80 (HTTP)** and **22(SSH)**. We are going to try with nmap, another scan, but this time a bit more exhaustive scan.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 13:21 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00017s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 72:1f:e1:92:70:3f:21:a2:0a:c6:a6:0e:b8:a2:aa:d5 (ECDSA)
|_  256 8f:3a:cd:fc:03:26:ad:49:4a:6c:a1:89:39:f9:7c:22 (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Iniciar Sesi\xC3\xB3n
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.12 seconds
```

Figure 2: Nmap Specific View

This second scan is reporting us first of all that the machine is a **Linux** machine. We could also see it in the previous scan, as it has a 64 TTL. Also, we can see the **HttpOnly** flag is not set which means the client cookie could be accesed by an script.

3 Vulnerability identification and explotation

When you first land in the Http site, you can see a Login page. In this Login if you insert a boolean clause to see if it is vulnerable to SQLI, you gain access in the login page. Boolean clause used:

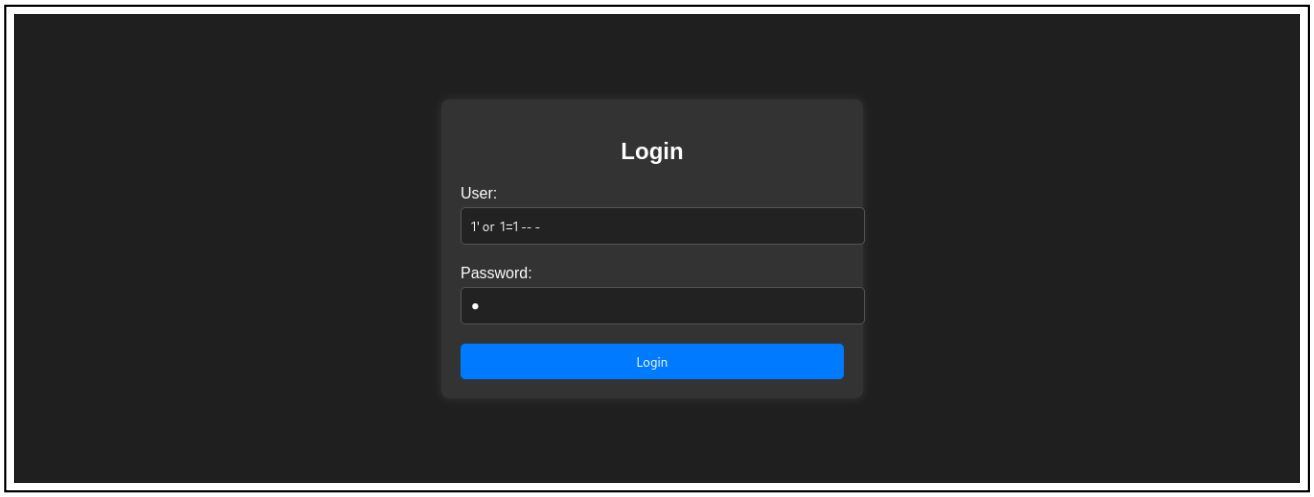

Figure 3: Login View

You are redirected by the login and you can find Dylan's credentials. This credentials you can use them later to gain access to **Injection** machine via **ssh**.

4 Privilege escalation

Once we are inside the machine we are going to search files with SUID active. If root has files we can execute as him, then we may pivot from dylan to root. We use **find** commnand for this.

We found some files with SUID. In this case **env** commnand can be executed as root, so we can give ourselves a privileged sh using : **env /bin/sh -p**.

Now we have full access to **Injection** machine