# <https://app.hackthebox.com/profile/1321956>

# Machine: Shoppy Type:Easy

1)Ping to machine IP address

Text

Description automatically generated

2)Conduct a Nmap scan

-Sv determine the version of the service running on port  
-V verbosity level  
-SC Scan with default NSE script

Text

Description automatically generated

continue

Text

Description automatically generated

3)Adjust host files to include shoppy.htb in host file.



Graphical user interface

Description automatically generated with low confidence

4)Enumerate the directories of the website. We found a login and admin.

Text

Description automatically generated

Lets try to login.

Graphical user interface, website

Description automatically generated

5)Using noSQL injection to login

Username: admin’||’1==1

Password:admin

A screenshot of a phone

Description automatically generated with medium confidence

I successfully authenticated and entered the website. Here we can view the products category and their respective prices.

Graphical user interface, application

Description automatically generated

6)Under the search user, Inject the same command previously admin’||’1==1

Text

Description automatically generated with medium confidence

7)Download export appeared.

A picture containing text

Description automatically generated

8)Download report.

Graphical user interface, text

Description automatically generated

Text

Description automatically generated with low confidence

There are 2 accounts; admin and josh.It seems that the password are being hashed(MD5 hashed). These password can be cracked using a decipher in the internet. Im using crackstation.net

I manged to crack for Josh. The password is “remembermethisway”

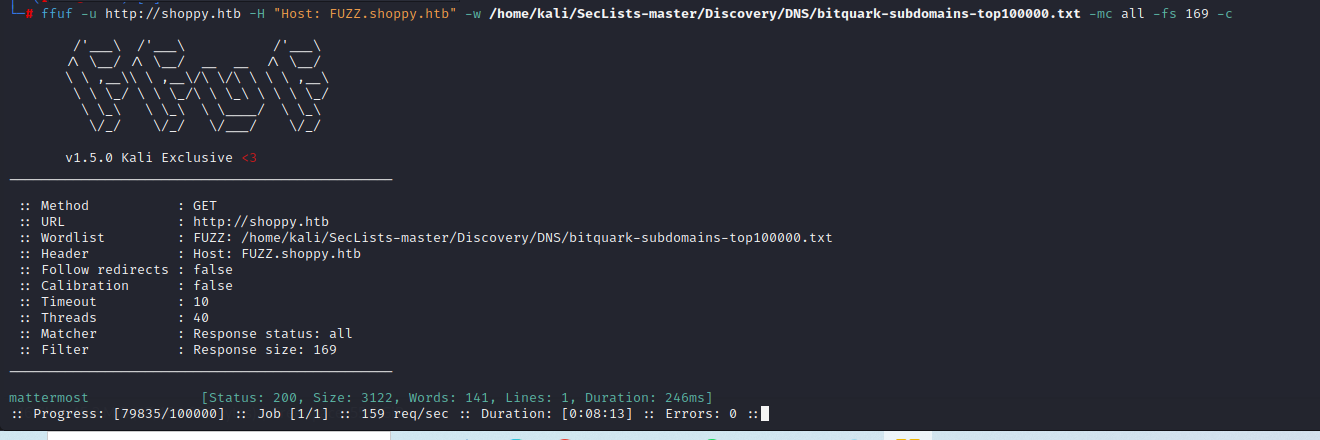
Graphical user interface, application

Description automatically generated

Graphical user interface

Description automatically generated

9)We discover a subdomain called mattermost.



Mattermost.shoppy.htb/login

Graphical user interface, application, Teams

Description automatically generated

10)Using the credential, we discovered previously. Username: Josh Password: remembermethisway

Graphical user interface, application, Teams

Description automatically generated

In the section “Deploy Machine”, there is a conversation between Jaeger and Josh. Jaeger shared that credentials for the deploy machine.

Username:jaeger

Password: Sh0ppyBest@pp!

Graphical user interface, text, application

Description automatically generated

11)Using ssh to enumerate as jeager

Text

Description automatically generated

12)Sudo -l to check on jaeger privileges.

Text

Description automatically generated

13)Print out the content in passwd file.

Text

Description automatically generated

14) Print the passwd and traverse each line that ends with “sh” . looking for shell scripts

Text

Description automatically generated

15)Tried to login using fake password. Access denied.

Text

Description automatically generated

16)Using string command to extract the text inside the data file.

Text

Description automatically generated

Text

Description automatically generated

Text

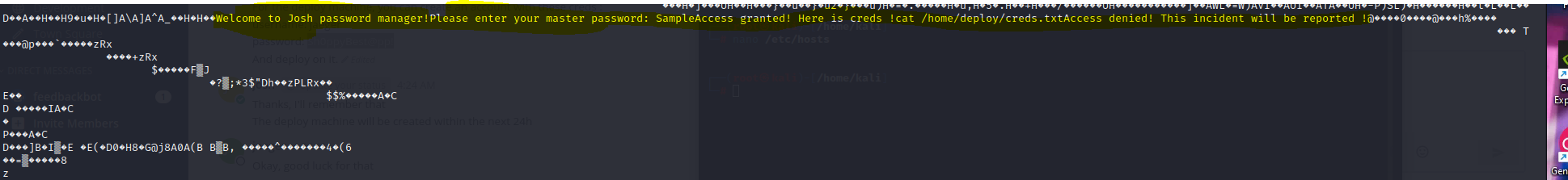
Description automatically generated

17) Reading and printing the contents of password-manager file.

Text

Description automatically generated

18)Focus on the highlighted sentence. The Password is “Sample”.



19)Enter password “Sample”

Text

Description automatically generated

20) Successfully entered Josh Password Manager

Text

Description automatically generated

21) I found that the user belongs to a particular docker group 998( docker). I searched under <https://gtfobins.github.io/> and I found that I can use a shell script to break out from restricted environment by spawning an interactive s

A picture containing table

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

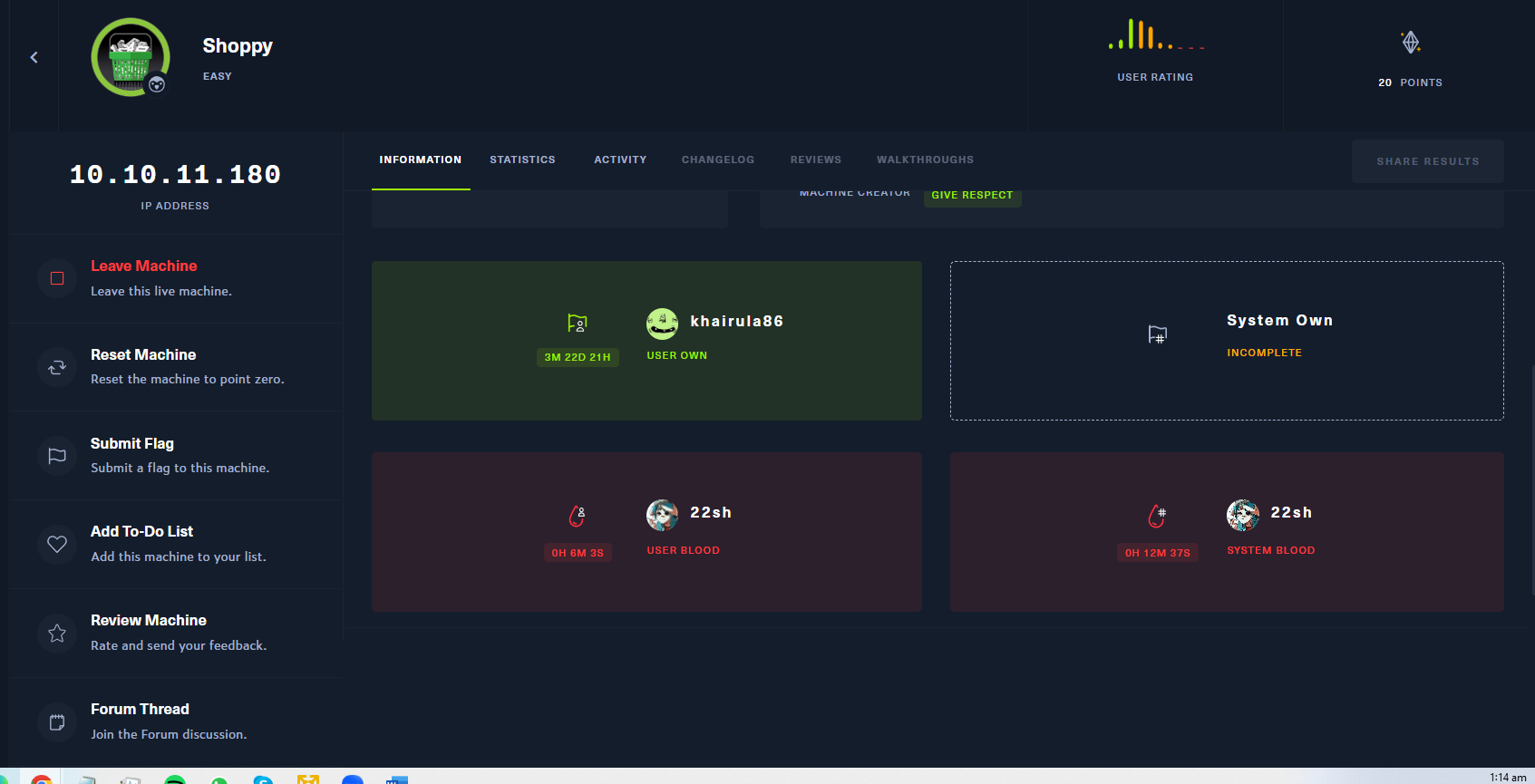
22)

Text

Description automatically generated

User.txt=de2e156a1b0b9bf91ebb9b4fe6f6a12c

Root.txt=b11b518f6b5ab5798887c35e56789186



A screenshot of a computer

Description automatically generated with medium confidence

# References:

<https://book.hacktricks.xyz/pentesting-web/nosql-injection>

<https://gtfobins.github.io/gtfobins/docker/#shell>

<https://gtfobins.github.io/>

<https://www.techrepublic.com/article/how-to-quickly-give-users-sudo-privileges-in-linux/#:~:text=To%20use%20this%20tool%2C%20you,%2Fsudoers%20file%20for%20editing).&text=Save%20and%20close%20the%20file,full%20range%20of%20sudo%20privileges>.

<https://book.hacktricks.xyz/pentesting-web/nosql-injection>

<https://www.imperva.com/learn/application-security/nosql-injection/#:~:text=The%20main%20differences%20between%20NoSQL,don't%20use%20standardized%20languages>.

<https://github.com/danielmiessler/SecLists>

<https://portswigger.net/web-security/file-path-traversal>

<https://github.com/pentestmonkey/php-reverse-shell>