

# Safe(gdb有異常)

```
—# nmap -sCV -A -p 22,80,1337 10.10.10.147
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 08:51 PDT
Nmap scan report for 10.10.10.147
Host is up (0.19s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 6d:7c:81:3d:6a:3d:f9:5f:2e:1f:6a:97:e5:00:ba:de (RSA)
|   256 99:7e:1e:22:76:72:da:3c:c9:61:7d:74:d7:80:33:d2 (ECDSA)
|_  256 6a:6b:c3:8e:4b:28:f7:60:85:b1:62:ff:54:bc:d8:d6 (ED25519)
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
1337/tcp  open  waste?
| fingerprint-strings:
|   DNSStatusRequestTCP:
|     11:51:28 up 5 min, 0 users, load average: 0.16, 0.06, 0.02
|   DNSVersionBindReqTCP:
|     11:51:23 up 5 min, 0 users, load average: 0.00, 0.03, 0.01
|   GenericLines:
|     11:51:10 up 5 min, 0 users, load average: 0.00, 0.03, 0.01
|     What do you want me to echo back?
|   GetRequest:
|     11:51:16 up 5 min, 0 users, load average: 0.00, 0.03, 0.01
|     What do you want me to echo back? GET / HTTP/1.0
|   HTTPOptions:
|     11:51:17 up 5 min, 0 users, load average: 0.00, 0.03, 0.01
|     What do you want me to echo back? OPTIONS / HTTP/1.0
|   Help:
|     11:51:33 up 5 min, 0 users, load average: 0.13, 0.06, 0.02
|     What do you want me to echo back? HELP
|   NULL:
|     11:51:10 up 5 min, 0 users, load average: 0.00, 0.03, 0.01
|   RPCCheck:
|     11:51:18 up 5 min, 0 users, load average: 0.00, 0.03, 0.01
|   RTSPRequest:
|     11:51:17 up 5 min, 0 users, load average: 0.00, 0.03, 0.01
|     What do you want me to echo back? OPTIONS / RTSP/1.0
```

```

I   SSLSessionReq, TerminalServerCookie:
I   11:51:34 up 5 min, 0 users, load average: 0.13, 0.06, 0.02
I   What do you want me to echo back?
I   TLSSessionReq:
I   11:51:35 up 5 min, 0 users, load average: 0.13, 0.06, 0.02
I_  What do you want me to echo back?
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1337-TCP:V=7.94SVN%I=7%D=4/18%Time=66214174%P=aarch64-unknown-linux
SF:-gnu%(NULL,3E,"\x2011:51:10\x20up\x205\x20min,\x20\x200\x20users,\x20\x
SF:x20load\x20average:\x200\x20.00,\x200\x20.03,\x200\x20.01\n")%(GenericLines,63,
SF:"\x2011:51:10\x20up\x205\x20min,\x20\x200\x20users,\x20\x20load\x20aver
SF:age:\x200\x20.00,\x200\x20.03,\x200\x20.01\n\nWhat\x20do\x20you\x20want\x20me\x2
SF:0to\x20echo\x20back\?\x20\r\n")%(GetRequest,71,"\x2011:51:16\x20up\x20
SF:5\x20min,\x20\x200\x20users,\x20\x20load\x20average:\x200\x20.00,\x200\x20.03
SF:,\x200\x20.01\n\nWhat\x20do\x20you\x20want\x20me\x20to\x20echo\x20back\?\x
SF:20GET\x20/\x20HTTP/1\x20.0\r\n")%(HTTPOptions,75,"\x2011:51:17\x20up\x205
SF:\x20min,\x20\x200\x20users,\x20\x20load\x20average:\x200\x20.00,\x200\x20.03,
SF:\x200\x20.01\n\nWhat\x20do\x20you\x20want\x20me\x20to\x20echo\x20back\?\x2
SF:0OPTIONS\x20/\x20HTTP/1\x20.0\r\n")%(RTSPRequest,75,"\x2011:51:17\x20up\x
SF:205\x20min,\x20\x200\x20users,\x20\x20load\x20average:\x200\x20.00,\x200\x20.
SF:03,\x200\x20.01\n\nWhat\x20do\x20you\x20want\x20me\x20to\x20echo\x20back\?
SF:\x200OPTIONS\x20/\x20RTSP/1\x20.0\r\n")%(RPCCheck,3E,"\x2011:51:18\x20up\x
SF:205\x20min,\x20\x200\x20users,\x20\x20load\x20average:\x200\x20.00,\x200\x20.
SF:03,\x200\x20.01\n")%(DNSVersionBindReqTCP,3E,"\x2011:51:23\x20up\x205\x20
SF:min,\x20\x200\x20users,\x20\x20load\x20average:\x200\x20.00,\x200\x20.03,\x20
SF:0\x20.01\n")%(DNSStatusRequestTCP,3E,"\x2011:51:28\x20up\x205\x20min,\x20
SF:\x200\x20users,\x20\x20load\x20average:\x200\x20.16,\x200\x20.06,\x200\x20.02\n"
SF:)%%(Help,67,"\x2011:51:33\x20up\x205\x20min,\x20\x200\x20users,\x20\x20
SF:load\x20average:\x200\x20.13,\x200\x20.06,\x200\x20.02\n\nWhat\x20do\x20you\x20w
SF:ant\x20me\x20to\x20echo\x20back\?\x20HELP\r\n")%(SSLSessionReq,64,"\x2
SF:011:51:34\x20up\x205\x20min,\x20\x200\x20users,\x20\x20load\x20average:
SF:\x200\x20.13,\x200\x20.06,\x200\x20.02\n\nWhat\x20do\x20you\x20want\x20me\x20to\
SF:x20echo\x20back\?\x20\x16\x03\n")%(TerminalServerCookie,63,"\x2011:51:
SF:34\x20up\x205\x20min,\x20\x200\x20users,\x20\x20load\x20average:\x200\x20.
SF:13,\x200\x20.06,\x200\x20.02\n\nWhat\x20do\x20you\x20want\x20me\x20to\x20echo
SF:\x20back\?\x20\x03\n")%(TLSSessionReq,64,"\x2011:51:35\x20up\x205\x20m
SF:in,\x20\x200\x20users,\x20\x20load\x20average:\x200\x20.13,\x200\x20.06,\x200
SF:\x20.02\n\nWhat\x20do\x20you\x20want\x20me\x20to\x20echo\x20back\?\x20\x16
SF:\x03\n");

```

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%),

Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (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 80/tcp)

HOP	RTT	ADDRESS
-----	-----	---------

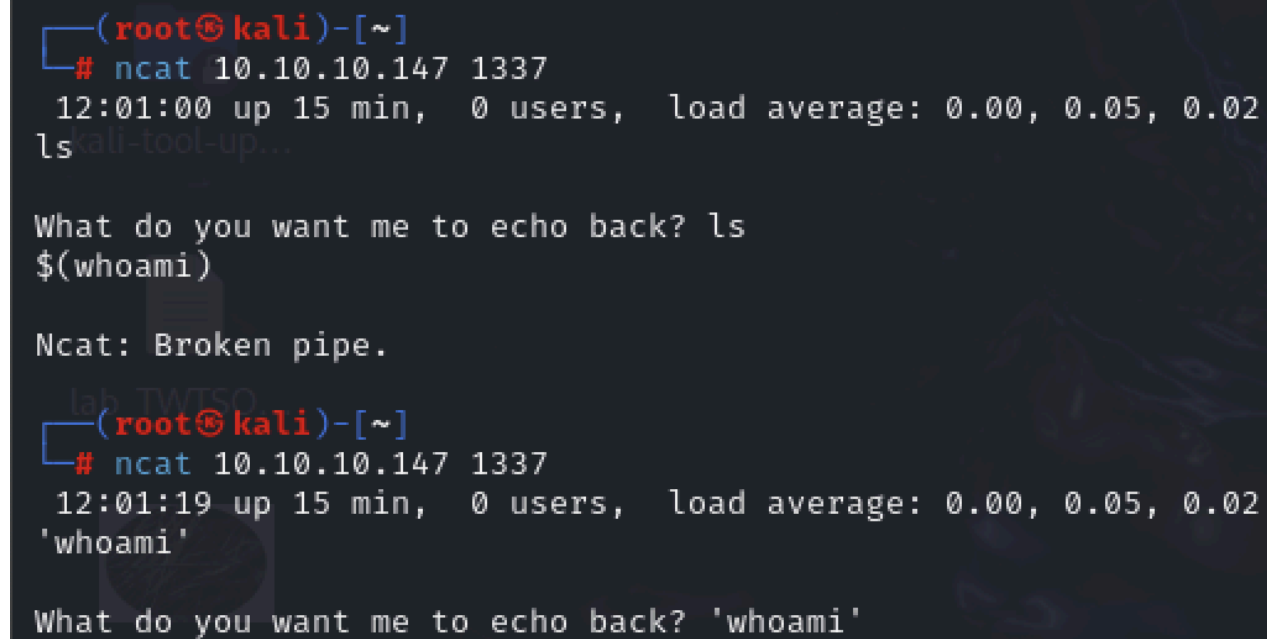
1	212.26 ms	10.10.14.1
---	-----------	------------

2	212.40 ms	10.10.10.147
---	-----------	--------------

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 109.70 seconds

使用nc連線1337輸入文件會被打回



```
(root@kali)-[~]
# ncat 10.10.10.147 1337
12:01:00 up 15 min,  0 users,  load average: 0.00, 0.05, 0.02
ls
What do you want me to echo back? ls
$(whoami)
Ncat: Broken pipe.

(root@kali)-[~]
# ncat 10.10.10.147 1337
12:01:19 up 15 min,  0 users,  load average: 0.00, 0.05, 0.02
'whoami'
What do you want me to echo back? 'whoami'
```

80port網站目錄爆破無東西，

在程式碼找到

```
view-source:http://10.10.10.147/

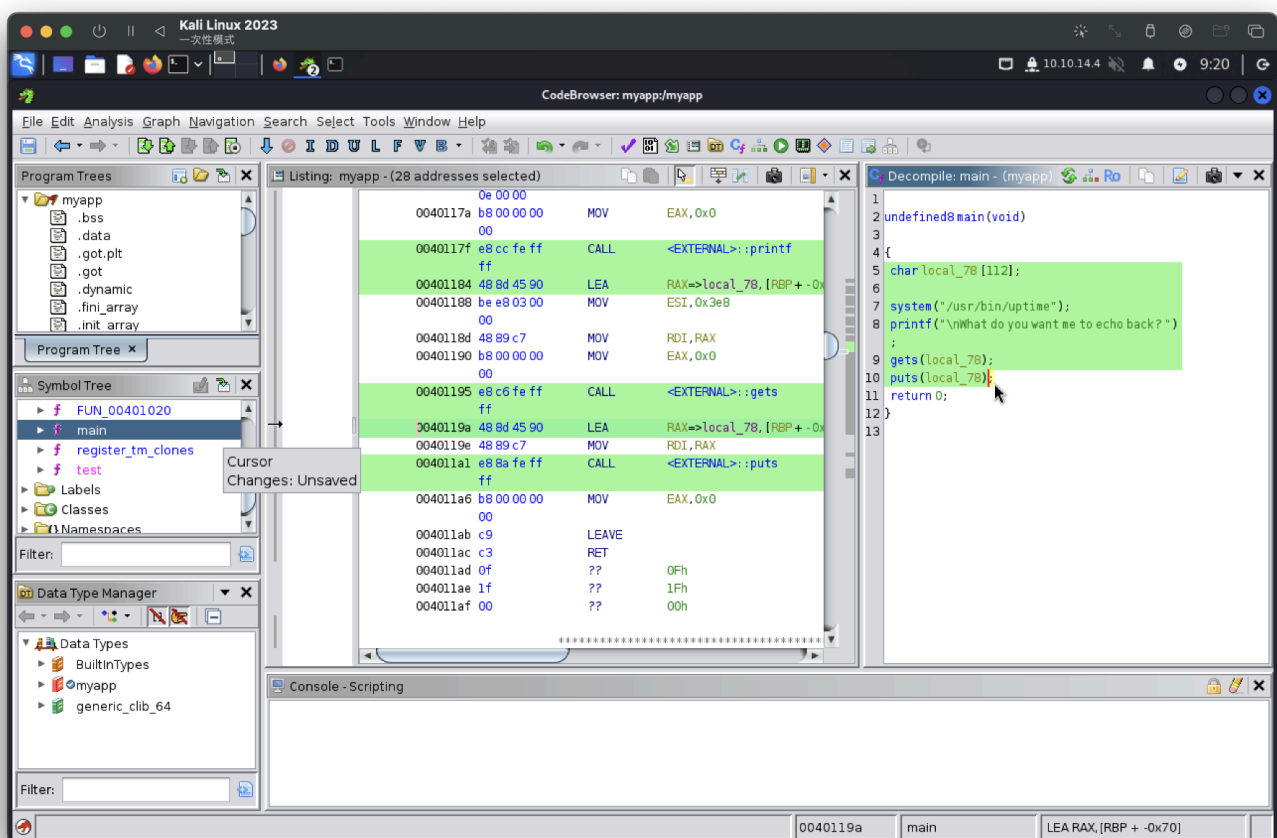
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

1
2 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transiti
3 <html xmlns="http://www.w3.org/1999/xhtml">
4 <!-- 'myapp' can be downloaded to analyze from here
5 its running on port 1337 -->
6 <head>
```

下載下來

```
(root@kali)-[~]
# file myapp
myapp: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]
fcbd5450d23673e92c8b716200762ca7d282c73a, not stripped
```

使用ghidra進行二進制



使用gdb ./myapp 執行緩衝未溢