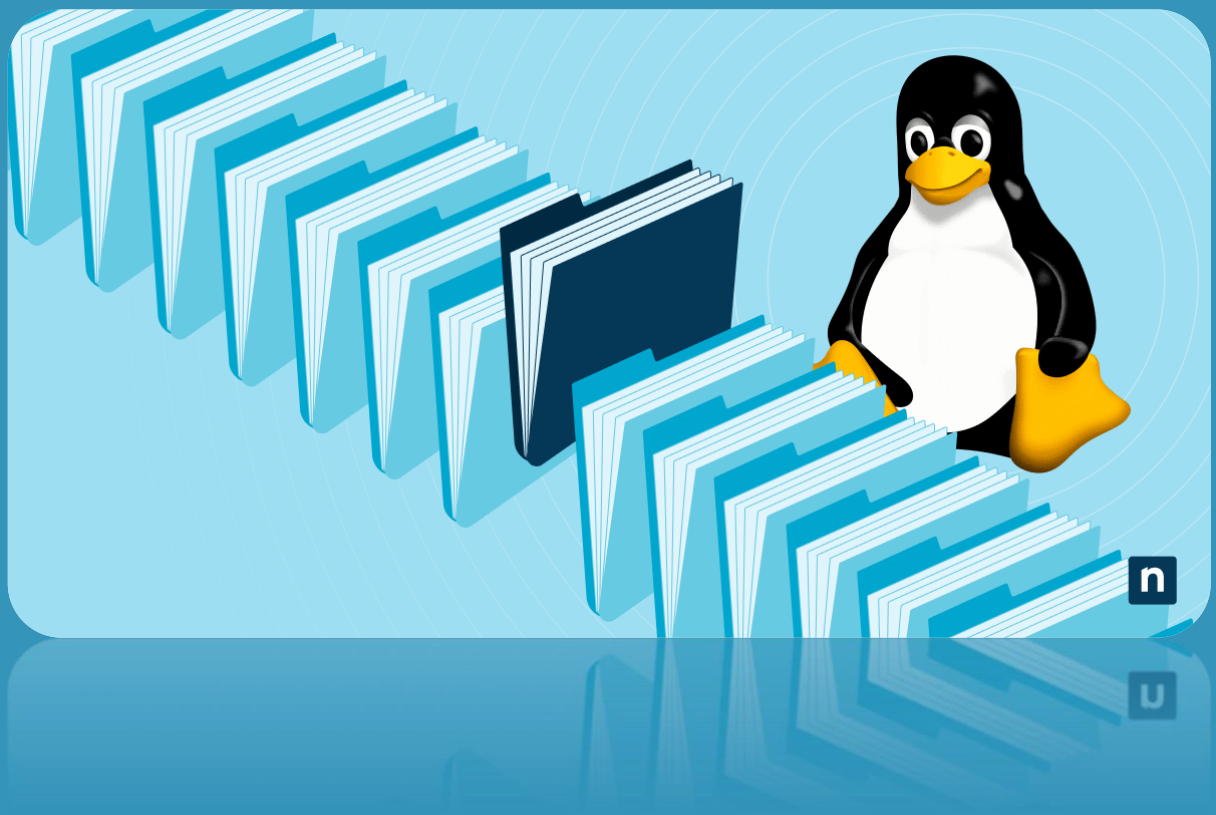
INCIDENTE EN SISTEMA LINUX 1: COMMAND INJECTION



ERIC SERRANO MARÍN

ANÁLISIS FORENSE INFORMÁTICO CETI

Contenido

Contexto

En esta máquina había una aplicación web vulnerable. Dicha aplicación se empleaba de forma remota para hacer un escaneo de la red interna. En uno de los formularios había un campo de texto en el cual se suponía que se debía de introducir una dirección IP y esto haría ping al equipo en dicha dirección. Sin embargo, el campo no estaba bien protegido, y eso posibilitaba que también se introdujeran comandos no deseados.

El 22 de mayo de 2022 sobre las 17:05 (UTC+2), ante la sospecha de que se ha producido un incidente de seguridad en el que se exfiltraron datos sensibles del servidor, el equipo de respuesta ante incidentes manda al técnico Vicente a investigar. Vicente realiza una captura de la memoria RAM, apaga el equipo, realiza una clonación del disco, y se pone analizar dichas evidencias.

Información adicional

```
┌──(kali㉿kali)-[~/Desktop]
└─$ fdisk -l imagen_disco.dd
Disk imagen_disco.dd: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xc3a20c42

Device           Boot  Start      End  Sectors   Size Id Type
imagen_disco.dd1          63   481949   481887 235.3M 83 Linux
imagen_disco.dd2      481950 16771859 16289910   7.8G  5 Extended
imagen_disco.dd5      482013 16771859 16289847   7.8G 8e Linux LVM
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -lh /dev/mapper
total 0
crw------- 1 root root 10, 236 Feb 21 18:31 control
lrwxrwxrwx 1 root root       7 Feb 21 18:49 loop0p1 -> ../dm-0
lrwxrwxrwx 1 root root       7 Feb 21 18:49 loop0p2 -> ../dm-1
lrwxrwxrwx 1 root root       7 Feb 21 18:49 loop0p5 -> ../dm-2

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo file -s /dev/dm-2
/dev/dm-2: LVM2 PV (Linux Logical Volume Manager), UUID: vhgYfH-DLoq-7Ib2-Em2B-W6Nw-IoRj-gdX8k3, size: 8340401664
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo pvdisplay /dev/dm-2
  WARNING: PV /dev/mapper/loop0p5 in VG metasploitable is using an old PV header, modify the VG to updat
e.
  --- Physical volume ---
  PV Name               /dev/mapper/loop0p5
  VG Name               metasploitable
  PV Size               <7.77 GiB / not usable <2.03 MiB
  Allocatable           yes (but full)
  PE Size               4.00 MiB
  Total PE              1988
  Free PE               0
  Allocated PE          1988
  PV UUID               vhgYfH-DLoq-7Ib2-Em2B-W6Nw-IoRj-gdX8k3
```

Pasos a seguir antes de empezar

Se utiliza para montar automáticamente las particiones presentes en una imagen de disco en formato ‘dd’.

```
┌──(kali㉿ kali)-[~/Desktop]
└─$ sudo kpartx -a -v imagen_disco.dd
add map loop0p1 (254:0): 0 481887 linear 7:0 63
add map loop0p2 (254:1): 0 2 linear 7:0 481950
add map loop0p5 (254:2): 0 16289847 linear 7:0 482013
```

El comando lvchange se utiliza para activar o desactivar volúmenes lógicos.

```
┌──(kali㉿ kali)-[~/Desktop]
└─$ sudo lvchange -a y metasploitable
  WARNING: PV /dev/mapper/loop0p5 in VG metasploitable is using an old PV header, modify the VG to update.
```

```
┌──(kali㉿ kali)-[~/Desktop]
└─$ mkdir disco

┌──(kali㉿ kali)-[~/Desktop]
└─$ sudo mount -o ro,noexec,noload /dev/metasploitable/root /home/kali/Desktop/disco

┌──(kali㉿ kali)-[~/Desktop]
└─$ ls
captura_ram.lime.zip  imagen_disco.dd      kali-linux-2023-W40-installer-amd64.iso
disco                 imagen_disco.dd.zip  metasploitable2_perfil_memoria.zip

┌──(kali㉿ kali)-[~/Desktop]
└─$ ls -lh disco
total 96K
drwxr-xr-x  2 root root 4.0K May 14  2012 bin
drwxr-xr-x  3 root root 4.0K Apr 28  2010 boot
lrwxrwxrwx  1 root root   11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  2 root root 4.0K Apr 28  2010 dev
drwxr-xr-x 95 root root 4.0K May 20  2022 etc
drwxr-xr-x  6 root root 4.0K Apr 16  2010 home
drwxr-xr-x  2 root root 4.0K Mar 16  2010 initrd
lrwxrwxrwx  1 root root   32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4.0K May 14  2012 lib
drwx------  2 root root  16K Mar 16  2010 lost+found
drwxr-xr-x  5 root root 4.0K May 20  2022 media
drwxr-xr-x  3 root root 4.0K Apr 28  2010 mnt
-rw-------  1 root root 6.4K May 20  2022 nohup.out
drwxr-xr-x  3 root root 4.0K May 20  2022 opt
dr-xr-xr-x  2 root root 4.0K Apr 28  2010 proc
drwxr-xr-x 13 root root 4.0K May 20  2022 root
drwxr-xr-x  2 root root 4.0K May 20  2022 sbin
drwxr-xr-x  2 root root 4.0K Mar 16  2010 srv
drwxr-xr-x  2 root root 4.0K Apr 28  2010 sys
drwxrwxrwt  4 root root 4.0K May 20  2022 tmp
drwxr-xr-x 12 root root 4.0K Apr 28  2010 usr
drwxr-xr-x 14 root root 4.0K Mar 17  2010 var
lrwxrwxrwx  1 root root   29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

1. Encontrar la zona horaria en la que está configurado el servidor.

```
┌──(kali㉿ kali)-[~/Desktop]
└─$ cat /home/kali/Desktop/disco/etc/timezone
US/Eastern
```

2. Encontrar la aplicación web vulnerable.

Podemos suponer que esta es la página web vulnerable, ya que es la que aparece que se accede en los logs.

```
┌──(kali㉿ kali)-[~/Desktop/disco/var/www]
└─$ ls
dav  dvwa  index.php  mutillidae  passwd.txt  phpinfo.php  phpMyAdmin  ping.php  test  tikiwiki  tikiwiki-old  twiki

┌──(kali㉿ kali)-[~/Desktop/disco/var/www]
└─$ cat ping.php
<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8"/>
        <title>PING</title>
    </head>
    <body>
        <form action="ping.php" method="post" />
            <label for="ping">IP: </label><input type="text" name="ping" value="<?php echo(isset($_POST['ping']) ? $_POST['ping'] : ''); ?>" />
            <br/>
            <input type="submit" value="enviar" />
            <br/>
            <br/>
        <form/>
<?php

if (isset($_POST['ping'])) {
    echo(system('ping -c 1 ' . $_POST['ping']));
}

?>
    </body>
</html>
```

3. Encontrar la IP, el cliente y el SO del equipo empleado por el atacante.

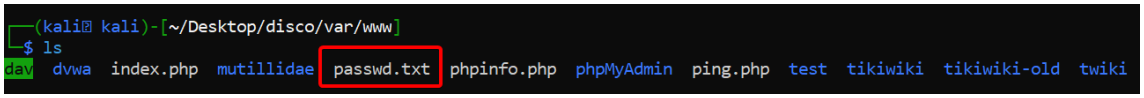
IP: 192.168.1.6.

Sistema operativo: Linux x86_64.

Cliente: Mozilla/5.0.

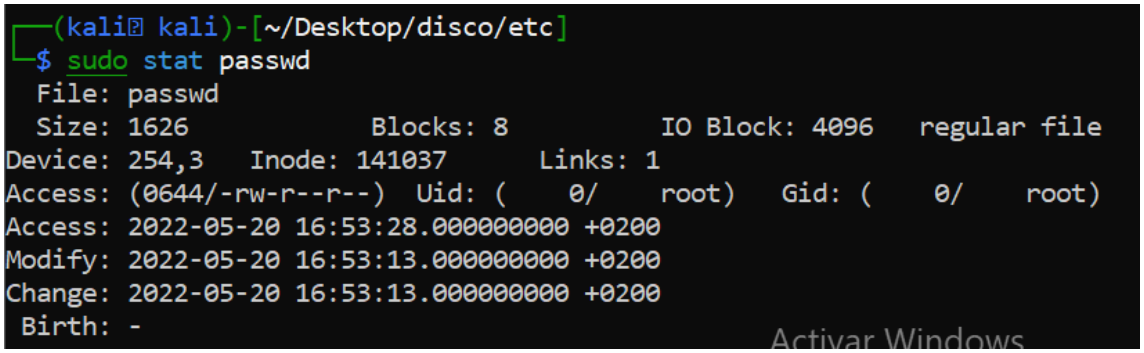
```
┌──(kali㉿ kali)-[~/…/disco/var/log/apache2]
└─$ ls
access.log  error.log  error.log.1

┌──(kali㉿ kali)-[~/…/disco/var/log/apache2]
└─$ cat access.log
127.0.0.1 - - [20/May/2012:15:56:39 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [20/May/2012:15:56:39 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [20/May/2012:15:56:39 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [20/May/2012:15:56:39 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [20/May/2012:15:56:39 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [20/May/2012:15:56:39 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [20/May/2012:15:56:39 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [20/May/2012:15:56:39 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [20/May/2012:15:56:39 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [20/May/2012:15:56:39 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
192.168.1.6 - - [20/May/2022:10:55:21 -0400] "GET / HTTP/1.1" 200 891 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.6 - - [20/May/2022:10:55:21 -0400] "GET /favicon.ico HTTP/1.1" 404 292 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.6 - - [20/May/2022:11:06:21 -0400] "GET /ping.php HTTP/1.1" 200 245 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.6 - - [20/May/2022:11:09:46 -0400] "GET /ping.php HTTP/1.1" 200 392 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.6 - - [20/May/2022:11:09:53 -0400] "POST /ping.php HTTP/1.1" 200 716 "http://192.168.1.28/ping.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.6 - - [20/May/2022:11:11:00 -0400] "POST /ping.php HTTP/1.1" 200 629 "http://192.168.1.28/ping.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.6 - - [20/May/2022:11:11:10 -0400] "POST /ping.php HTTP/1.1" 200 716 "http://192.168.1.28/ping.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.6 - - [20/May/2022:11:12:37 -0400] "POST /ping.php HTTP/1.1" 200 716 "http://192.168.1.28/ping.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.6 - - [20/May/2022:11:13:14 -0400] "POST /ping.php HTTP/1.1" 200 2356 "http://192.168.1.28/ping.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.6 - - [20/May/2022:11:13:49 -0400] "POST /ping.php HTTP/1.1" 200 748 "http://192.168.1.28/ping.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.6 - - [20/May/2022:11:20:50 -0400] "GET / HTTP/1.1" 200 891 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.6 - - [20/May/2022:11:20:40 -0400] "GET /captura_ram.lime HTTP/1.1" 200 1073282112 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.6 - - [20/May/2022:11:21:03 -0400] "GET /metasploitable2.zip HTTP/1.1" 200 345635 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

4. Encontrar qué datos ha exfiltrado el atacante.



Dado que el archivo passwd.txt está ubicado en un directorio web (/var/www/), es una práctica muy arriesgada tener un archivo como este accesible a través de un servidor web, ya que contiene información sensible sobre usuarios del sistema.

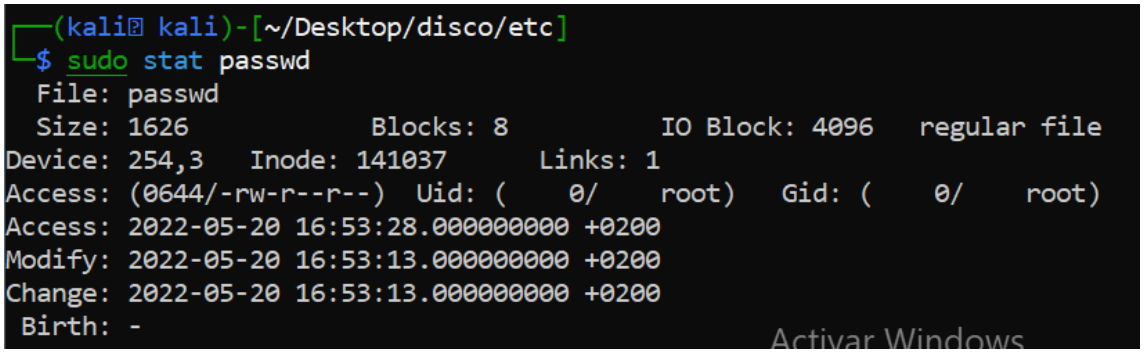
Aunque este fichero de arriba passwd.txt no es el original, el original es el de las capturas de aquí abajo.



Ha sido modificado después del 20 de mayo de 2022 a las 11:09:46 AM.

5. Información sobre los accesos a passwd.txt y su original.

Passwd original.



Passwd copiado.

```
┌──(kali㉿ kali)-[~/Desktop/disco/var/www]
└─$ stat passwd.txt
  File: passwd.txt
  Size: 1626            Blocks: 8          IO Block: 4096   regular file
Device: 254,3   Inode: 67616       Links: 1
Access: (0644/-rw-r--r--)  Uid: (   33/www-data)   Gid: (   33/www-data)
Access: 2022-05-20 17:13:49.000000000 +0200
Modify: 2022-05-20 17:13:49.000000000 +0200
Change: 2022-05-20 17:13:49.000000000 +0200
 Birth: -
```

Son exactamente iguales.

```
┌──(kali㉿ kali)-[~/Desktop/disco/var/www]
└─$ sudo diff passwd.txt /home/kali/Desktop/disco/etc/passwd

┌──(kali㉿ kali)-[~/Desktop/disco/var/www]
└─$
```

6. **Razonar por qué no podemos saber los comandos introducidos por el atacante y cómo se podría arreglar esto en ocasiones posteriores.**

Este script, tal y como su nombre indica (reset_logs.sh) tiene como objetivo eliminar y limpiar los registros de log (archivos de registro) del sistema.

Es una práctica habitual después de comprometer un sistema para cubrir sus huellas y hacer más difícil la detección de su actividad o la investigación forense.

```
┌──(kali㉿ kali)-[~/Desktop/disco/root]
└─$ sudo cat reset_logs.sh
#!/bin/sh

/etc/init.d/sysklogd stop
VARLOGS="auth.log boot btmp daemon.log debug dmesg kern.log mail.info mail.log mail.warn messages syslog udev wtmp"
cd /var/log
for ii in $VARLOGS; do
  echo -n > $ii
  rm -f $ii.? $ii.?.gz
done

/etc/init.d/samba stop
rm -f /var/log/samba/*

rm -f /var/lib/dhcp3/*

for ii in /var/log/proftpd/* /var/log/postgresql/* /var/log/apache2/*; do
  echo -n > $ii
done
```

Sacamos el perfil para ver si aun así encontramos algo.

```
Linuxmetasploitable2_perfil_memoriax86 - A Profile for Linux metasploitable2_perfil_memoria x86
[lab@LAB ~]$ ls
captura_ram.lime  Install volatity2.md                Public
Desktop           metasploitable2_perfil_memoria.zip  Templates
Documents         Music                               Videos
Downloads         Pictures
```

Los poquitos comandos que han quedado han sido los siguientes:

```
[lab@LAB ~]$ vol.py --plugins=. --profile=Linuxmetasploitable2_perfil_memoriax86 -f captura_ram.lime linu
x_bash
Volatility Foundation Volatility Framework 2.6.1
Pid      Name                 Command Time                   Command
-------- -------------------- ------------------------------ -------
    4748 bash                 2022-05-20 14:44:57 UTC+0000   setxkbmap es
    4748 bash                 2022-05-20 14:45:17 UTC+0000   mount /media/cdrom
    4748 bash                 2022-05-20 14:45:49 UTC+0000   cp /media/cdrom /var/tmp
    4748 bash                 2022-05-20 14:46:05 UTC+0000   cp -r /media/cdrom /var/tmp
    4748 bash                 2022-05-20 14:46:12 UTC+0000   umount /media/cdrom
    4748 bash                 2022-05-20 14:46:44 UTC+0000   ip a
    4748 bash                 2022-05-20 14:56:46 UTC+0000   nano
    4748 bash                 2022-05-20 15:07:04 UTC+0000   sudo nano /var/www/ping.php
    4748 bash                 2022-05-20 15:14:20 UTC+0000   ls
    4748 bash                 2022-05-20 15:14:42 UTC+0000   cd /var/tmp/metasploitable2
    4748 bash                 2022-05-20 15:14:56 UTC+0000   sudo ./captura_memoria.sh
```

7. Comprobación del código php con vulnerabilidad.

Tiene una vulnerabilidad de ‘code injection’.

El comando cat /etc/passwd, nos muestra el contenido del archivo passwd, este archivo es una base de datos de usuarios del sistema, que contiene información sobre cada cuenta de usuario.