2025

INFORME PENTESTING

EMMANUEL IZAGUIRRE RUIZ

Introducción

Este informe documenta el proceso de detección, explotación controlada, escalamiento de privilegios y mitigación de una vulnerabilidad en un servidor debian comprometido.

Estado inicial del sistema

Presencia de un usuario sospechoso haker así como procesos de ejecución.

Identificación de usuarios sospechosos.

Cat /etc/passwd | grep bash

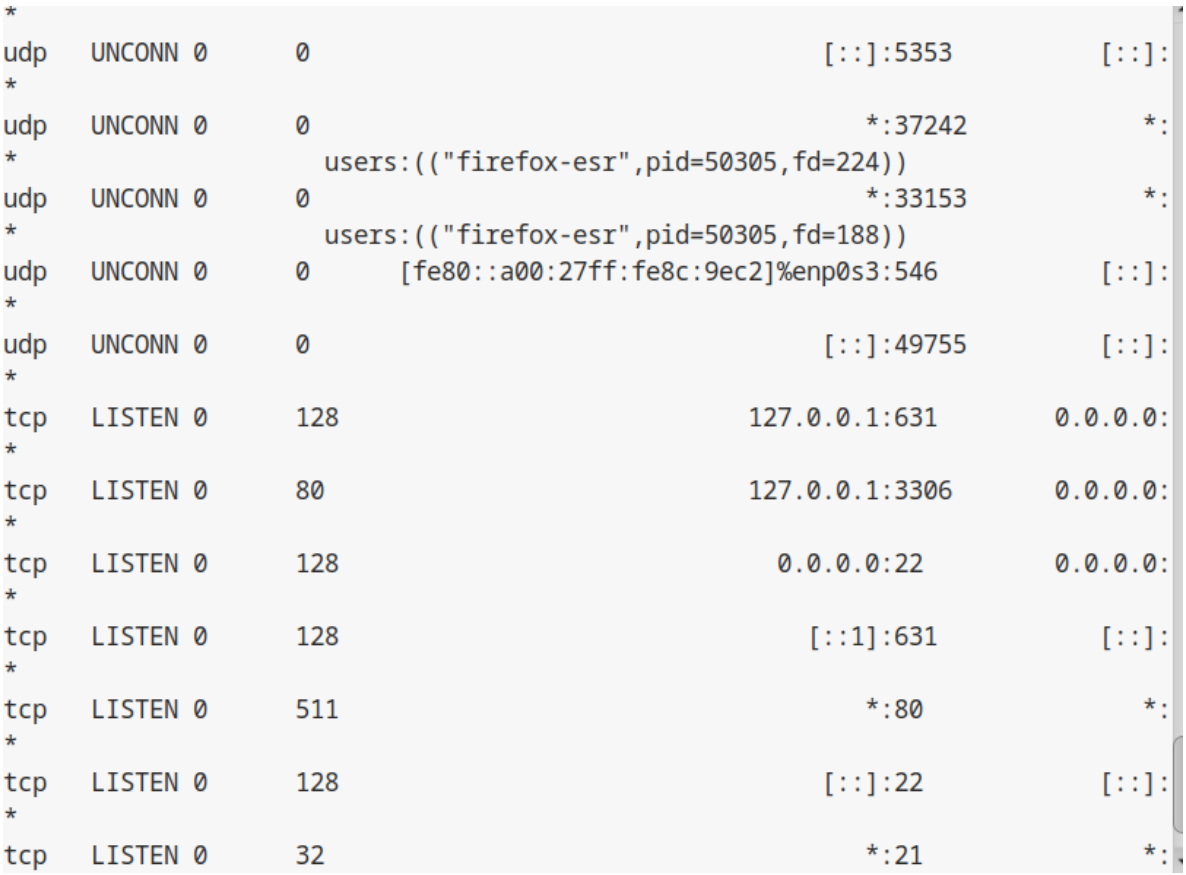
```
debian   pts/1        2025-02-22 20:05
debian   pts/4        2025-02-22 21:14
debian   pts/5        2025-02-24 12:42
debian   pts/6        2025-02-24 12:42
debian   pts/7        2025-02-24 13:13
debian   tty7         :0               Fri Feb 14 21:14    gone - no logout
reboot   system boot  6.1.0-25-amd64   Fri Feb 14 21:14   still running
debian   tty7         :0               Tue Oct  8 17:28 - crash (129+04:45)
reboot   system boot  6.1.0-25-amd64   Tue Oct  8 17:28   still running
debian   tty7         :0               Tue Oct  8 16:48 - crash  (00:40)
reboot   system boot  6.1.0-25-amd64   Tue Oct  8 16:48   still running
debian   tty7         :0               Tue Oct  8 16:44 - crash  (00:03)
reboot   system boot  6.1.0-25-amd64   Tue Oct  8 16:43   still running
debian   tty7         :0               Mon Sep 30 15:13 - crash (8+01:29)
reboot   system boot  6.1.0-25-amd64   Mon Sep 30 15:09   still running
debian   tty7         :0               Mon Sep 30 09:49 - 12:27  (02:38)
reboot   system boot  6.1.0-23-amd64   Mon Sep 30 09:48 - 12:28  (02:39)
debian   tty7         :0               Sat Sep 28 16:40 - crash (1+17:08)
reboot   system boot  6.1.0-23-amd64   Sat Sep 28 16:39 - 12:28 (1+19:48)
debian   tty7         :0               Wed Jul 31 16:45 - 18:18  (01:33)
reboot   system boot  6.1.0-23-amd64   Wed Jul 31 16:45 - 18:19  (01:34)
debian   tty7         :0               Wed Jul 31 16:04 - 16:44  (00:39)
reboot   system boot  6.1.0-23-amd64   Wed Jul 31 16:04 - 16:44  (00:40)
```

Aquí nos muestra que usuarios están conectados actualmente, junto con detalles como su nombre, usuario, actividad, carga del sistema. Así como la lista de usuarios.

IDENTIFICACION DE PROCESOS SOSPECHOSOS

Netstat -tulnp

Ss -tulnp



Nos muestra los últimos 10 procesos que más consumen memoria de la máquina. Así como los puertos que han sido usados.

Escaneo de configuraciones vulnerables

Find / -perm -4000 2>/dev/null

Sudo -l

Cat/etc/sudoers

Ls-la/home/

Los archivos SUID pueden permitir escalamiento de privilegios si están mal configurados.

```
'usr/lib/polkit-1/polkit-agent-helper-1
'usr/lib/dbus-1.0/dbus-daemon-launch-helper
'usr/bin/su
'usr/bin/umount
'usr/bin/chsh
'usr/bin/passwd
'usr/bin/fusermount3
'usr/bin/chfn
'usr/bin/newgrp
'usr/bin/ntfs-3g
'usr/bin/pkexec
'usr/bin/gpasswd
'usr/bin/mount
'usr/bin/sudo
[sudo] password for debian:
Matching Defaults entries for debian on debian:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bir

User debian may run the following commands on debian:
    (ALL : ALL) ALL
cat: /etc/sudoers: Permission denied
total 12
drwxr-xr-x  3 root   root   4096 Jul 31  2024 .
drwxr-xr-x 19 root   root   4096 Feb 22 20:07 ..
drwx------ 14 debian debian 4096 Feb 14 21:14 debian
```

Uso de linpeas

Linpeas.sh

Sirve para mostrar vulnerabilidades y escalamiento de privilegios. Con este comando se puede encontrar ARCHIVOS SIUID peligrosos servicios vulnerables o mal configurados, credenciales en archivos, puertos abiertos y procesos corriendo,.

```
home/debian/.bash_history:sudo apt install curl
home/debian/.bash_history:sudo cp -a /tmp/wordpress/. /var/www/html/
home/debian/.bash_history:sudo chown -R www-data:www-data /var/www/html/
home/debian/.bash_history:sudo chmod -R 755 /var/www/html/
home/debian/.bash_history:sudo mv wp-config-sample.php wp-config.php
home/debian/.bash_history:sudo nano wp-config.php
home/debian/.bash_history:sudo systemctl restart apache2
home/debian/.bash_history:sudo systemctl status apache2
home/debian/.bash_history:sudo apt install php libapache2-mod-php php-mysqli php-gd php-xml php-mbstring ph
home/debian/.bash_history:sudo nano /etc/apache2/sites-available/000-default.conf
home/debian/.bash_history:sudo systemctl restart apache2
home/debian/.bash_history:sudo nano /var/www/html/info.php
home/debian/.bash_history:sudo apt install openssh-server -y
home/debian/.bash_history:sudo systemctl start ssh
home/debian/.bash_history:sudo systemctl enable ssh
home/debian/.bash_history:sudo systemctl status ssh
home/debian/.bash_history:sudo systemctl start apache2
home/debian/.bash_history:sudo grep 'failed' /var/log/auth.log
home/debian/.bash_history:sudo grep 'Failed' /var/log/auth.log
home/debian/.bash_history:[Ñ*[*Ñ*¨**__:--..--.--ñ´+´+}¿'¿'00951||Z¬|@@·~½~½¬¬{{[[[]]}\}\\¸¸~¨^` .·•·µ”“”“„„ç
·• .^~~łĸʾħŋđðßßßæßßæ@æ@Ր€¶ŧ←↓→→ø→øøþþþ¨~~~~~~¸\}][{¬½~·@@||¬¬«»«ç„ç“”¬|@·@~·~½½¬½¬¬{{[{[][]}\¸
home/debian/.bash_history:sudo apt install inattended-upgrades
home/debian/.bash_history:sudo unattended-upgrade --dry-run
home/debian/.bash_history:sudo unattended-upgrade --dry-run
home/debian/.bash_history:sudo apt install unattended-upgrades
home/debian/.bash_history:sudo unattended-upgrade --dry-run
```

Actualizar Apache para mitigar vulnerabilidades

Sudo apt update && sudo apt upgrade apache2

```
debian@debian:~$ sudo apt update && sudo apt upgrade apache2
Hit:1 http://deb.debian.org/debian bookworm InRelease
Get:2 http://security.debian.org/debian-security bookworm-security InRelease [48
.0 kB]
Get:3 http://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Get:4 http://security.debian.org/debian-security bookworm-security/main Sources
[146 kB]
Get:5 http://security.debian.org/debian-security bookworm-security/main amd64 Pa
ckages [246 kB]
Get:6 http://security.debian.org/debian-security bookworm-security/main Translat
ion-en [147 kB]
Fetched 642 kB in 1s (927 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
ld by process 19942 (apt-get)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
```

Se mantiene el Apache actualizado para ayudar a corregir vulnerabilidades conocidas.

Análisis de logs

Para revisar los logs del sistema en busqyeda de accesos sospechosos y determinar los servicios comprometidos.

Cd/ var/log/jornal

```
debian@debian:/var/log/journal$ ls -a
.  ..  41b6de202c3f48fdaa490411748aaaff
debian@debian:/var/log/journal$ cat 41b6de202c3f48fdaa490411748aaaff
cat: 41b6de202c3f48fdaa490411748aaaff: Is a directory
debian@debian:/var/log/journal$ ls 41b6de202c3f48fdaa490411748aaaff
system@000623fd2fdaee7a-88a7ec054264cefd.journal~
system@000623fd40d0cdb2-12f2110dcea1862a.journal~
system@000623fdd1f5eb41-84d1749f27ffe276.journal~
system@00062e24da747954-3013bd9ec8a9be57.journal~
system@a48b40a584d44a45941503ea72502321-0000000000000001-00061e907f44bc23.journ
l
system@a48b40a584d44a45941503ea72502321-00000000000003c1-00061e90811d3e83.journ
l
system@a48b40a584d44a45941503ea72502321-0000000000001411-00062333f849bfca.journ
l
system@a48b40a584d44a45941503ea72502321-000000000000357e-00062e24da73a9aa.journ
l
system@a48b40a584d44a45941503ea72502321-0000000000003971-00062e24db436c06.journ
l
system.journal
user-1000@000623fd41a26005-486efe3d1e3954e3.journal~
user-1000@69bebf5c90b54a418788b8e68ea9e49a-00000000000003c4-00061e90811e245b.jo
rnal
```

Logramos acceder a los logs de segurada del sistema , a revisar la información, cambiamos de privilegios a root y se analizan los logs encontrados.

```
debian@debian:/var/log/journal/41b6de202c3f48fdaa490411748aaaff$ ls -l
total 96984
-rw-r-----+ 1 root systemd-journal 8388608 Oct  8 16:41 system@000623fd2fdaee7a
-8a7ec054264cefd.journal~
-rw-r-----+ 1 root systemd-journal 8388608 Oct  8 16:47 system@000623fd40d0cdb2
-2f2110dcea1862a.journal~
-rw-r-----+ 1 root systemd-journal 8388608 Oct  8 17:28 system@000623fdd1f5eb41
-4d1749f27ffe276.journal~
-rw-r-----+ 1 root systemd-journal 8388608 Oct  8 18:03 system@00062e24da747954
-013bd9ec8a9be57.journal~
-rw-r-----+ 1 root systemd-journal 4353288 Jul 31  2024 system@a48b40a584d44a45
-1503ea72502321-0000000000000001-00061e907f44bc23.journal
-rw-r-----+ 1 root systemd-journal 5769944 Sep 28 16:39 system@a48b40a584d44a45
-1503ea72502321-00000000000003c1-00061e90811d3e83.journal
-rw-r-----+ 1 root systemd-journal 5869744 Sep 30 15:06 system@a48b40a584d44a45
-1503ea72502321-0000000000001411-00062333f849bfca.journal
-rw-r-----+ 1 root systemd-journal 4374976 Feb 14 21:14 system@a48b40a584d44a45
-1503ea72502321-000000000000357e-00062e24da73a9aa.journal
-rw-r-----+ 1 root systemd-journal 3824968 Feb 14 21:15 system@a48b40a584d44a45
-1503ea72502321-0000000000003971-00062e24db436c06.journal
-rw-r-----+ 1 root systemd-journal 8388608 Feb 26 22:18 system.journal
```

Se sospecha que el 8 de octubre hubo inicios de sesión.

Para comprobar los inicios de sesión , revisam,os los archivos y los usuariosa creados por el atacante.

Se utiliza sudo contrab -l para revisar su hay algún programa en el cron, al igual si hay algún proceso en ejecución con el comando ps aux –sort=%cpu

```
debian    108142  0.0  3.6 2405984 74220 ?       Sl   23:32   0:00 /usr/lib/fire
debian    108045  0.0  4.3 2417572 87364 ?       Sl   23:31   0:00 /usr/lib/fire
debian     50435  0.0  5.1 2484008 104556 ?      Sl   16:00   0:09 /usr/lib/fire
mysql        713  0.0  0.1 1547312 3652 ?        Ssl  03:28   0:27 /usr/sbin/mar
root      107245  0.0  0.0      0     0 ?        I    23:14   0:00 [kworker/1:1-
debian    108431  0.0  3.6 2405984 72792 ?       Sl   23:34   0:00 /usr/lib/fire
debian      1143  0.0  1.0 552560 20716 ?        Sl   03:28   0:35 mate-panel
debian      1091  0.0  0.1  10536  2452 ?        S    03:28   0:48 /usr/bin/dbus
debian      1121  0.0  1.0 883312 20932 ?        Sl   03:28   0:59 marco
debian    108463  0.0  3.6 2405724 73956 ?       Sl   23:35   0:00 /usr/lib/fire
root      108394  0.0  0.0      0     0 ?        I    23:33   0:00 [kworker/1:2-
debian     50745  0.1  7.5 2608584 151556 ?      Sl   16:02   0:37 /usr/lib/fire
debian      1394  0.1  0.1 109000  2532 ?        Sl   03:28   1:49 /usr/lib/spee
root       19942  0.1  0.1  72528  2088 ?        S    12:26   1:04 apt-get dist-
debian    104382  0.1  2.5 559420 50908 ?        Sl   22:16   0:08 mate-terminal
debian      1199  0.4  5.6 539580 114444 ?       Sl   03:28   5:59 /usr/bin/pyth
debian     50525  0.5 14.9 2784652 301180 ?      Sl   16:00   2:18 /usr/lib/fire
debian      1442  0.5  0.2 730636  5688 ?        Ssl  03:28   6:48 /usr/bin/spee
debian     52652  0.6  9.7 2706184 195540 ?      Sl   16:34   2:51 /usr/lib/fire
debian     95184  1.1  9.7 2696400 197380 ?      Sl   20:29   2:13 /usr/lib/fire
root         592  1.8  3.4 489244 69864 tty7     Ssl+ 03:28  21:55 /usr/lib/xorg
debian     50305  3.1 17.2 11812160 348244 ?     Sl   16:00  14:15 /usr/lib/fire
debian      1012  3.5  0.5 1703280 11544 ?       S<sl 03:28  42:40 /usr/bin/puls
```

No se encontró detalle alguno.

Creación de usuarios

Posterior, revisamos su existe alguna creación de nuevos usuarios con el comando cat /ect/passwd | grep /bin/bash

```
debian      1012  3.5  0.5 1703280 11544 ?       S<sl 03:28  42:40 /usr/bin/puls
debian@debian:/$ cat /etc/passwd | grep "/bin/bash"
root:x:0:0:root:/root:/bin/bash
debian:x:1000:1000:4geeks,,,:/home/debian:/bin/bash
debian@debian:/$
```

No se a creado nuevos usuarios, ya que solo esta usuario root y el del sistema debian.

Para revisar si se a creado credenciales invalidas utilizamos

Sudo mysql -e ´SELECT user, host, password FROM mysql.user;¨

```
debian@debian:/$ sudo mysql -e "SELECT user, host, password FROM mysql.user;"
[sudo] password for debian:
+---------------+-----------+-------------------------------------------+
| User          | Host      | Password                                  |
+---------------+-----------+-------------------------------------------+
| mariadb.sys   | localhost |                                           |
| root          | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| mysql         | localhost | invalid                                   |
| wordpressuser | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| user          | localhost | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
+---------------+-----------+-------------------------------------------+
```

Se observa que hay un usuario mysql, tiene las credenciales invalidas, a lo que se supone que se a creado por alguien ajeno.

Esta utilizando contraseñas en texto para la ejecución de ataques de fuerza bruta.

```
+-----------------------------------------------------------------------------
-------------------------------------------------------+
| GRANT ALL PRIVILEGES ON *.* TO `mysql`@`localhost` IDENTIFIED VIA mysql_native
_password USING 'invalid' OR unix_socket WITH GRANT OPTION |
| GRANT PROXY ON ''@'%' TO 'mysql'@'localhost' WITH GRANT OPTION
                                                           |
+-----------------------------------------------------------------------------
```

Todos los provilegios están activos, el atacante tiene acceso total al servidor, por lo que es bastante peligroso.

verificamos sus contraseñas.

```
debian@debian:/$ sudo mysql -e "SELECT user, host FROM mysql.user WHERE user='
+-------+-----------+
| User  | Host      |
+-------+-----------+
| mysql | localhost |
+-------+-----------+
debian@debian:/$
```

Se confirma que este usuario , tiene acceso a la maquina local host de forma remota a cualquier otra ip.

Servidor FTP

Para revisar el servidor este operativo utilizamos

Sudo nano /etc/vsftpd.conf

```
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
```

Se detecta que se permite acceso anónimo son autenticación.

Word press

Para revisar si apache esta activo y si el wordpress operando.

```
debian@debian:/$ sudo systemctl status apache2
[sudo] password for debian:
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enab
     Active: active (running) since Fri 2025-02-14 21:14:40 EST; 3 weeks 1 day
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 123509 ExecReload=/usr/sbin/apachectl graceful (code=exited, statu
   Main PID: 653 (apache2)
      Tasks: 6 (limit: 2284)
     Memory: 28.3M
        CPU: 16.548s
     CGroup: /system.slice/apache2.service
             ├─   653 /usr/sbin/apache2 -k start
             ├─123522 /usr/sbin/apache2 -k start
             ├─123524 /usr/sbin/apache2 -k start
             ├─123525 /usr/sbin/apache2 -k start
             ├─123526 /usr/sbin/apache2 -k start
             └─123527 /usr/sbin/apache2 -k start
```

Se verifica que el sistema operativo esta en función. (activo)

Se edita la configuración del archivo SSH utilizando

Sudo nano n/etc/ssh/sshd_config

```
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

En la configuración deshabilitamps el acceso con contraseña y root

```
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

Así como en Password , se cambia laconfiguracion, para evitar la autenticación de contraseñas Root y también ataques de fuerza bruta.

Usuario Mysql en la base de datos.

```
debian@debian:/$ sudo mysql -e "SELECT user, host,password FROM mysql.user;"
+---------------+-----------+-------------------------------------------+
| User          | Host      | Password                                  |
+---------------+-----------+-------------------------------------------+
| mariadb.sys   | localhost |                                           |
| root          | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| wordpressuser | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| user          | localhost | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
+---------------+-----------+-------------------------------------------+
```

Se puede observar que el usuario mysql tiene privilegios elevados y es peligroso.

Se modifica la configuración para que MYSQL no acepte conexiones .

```
#user                   = mysql
pid-file                = /run/mysqld/mysqld.pid
basedir                 = /usr
#datadir                = /var/lib/mysql
#tmpdir                 = /tmp

# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve
```

Recomendaciones para evitar futuros eventos con la seguridad de la empresa.

INFORME DE RECOMENDACIONES PARA EVITAR EVENTOS DE SEGURIDAD

Introducción En este informe se presentan una serie de medidas de seguridad recomendadas para mitigar vulnerabilidades y fortalecer la infraestructura tecnológica de la empresa. A pesar de haber aplicado correcciones a los servicios comprometidos, es fundamental adoptar estrategias preventivas para reducir riesgos futuros y garantizar la protección de los activos digitales.

Recomendaciones de Seguridad

Implementación de Autenticación Multifactor (2FA) y Privileged Access Management (PAM)

- Se recomienda habilitar la autenticación multifactor (2FA) en accesos remotos y administrativos para evitar accesos no autorizados.
- Para conexiones de proveedores, se debe implementar un sistema de Privileged Access Management (PAM), lo que permitirá restringir y auditar el uso de credenciales privilegiadas.

Restricción de Accesos mediante Firewalls y Listas Blancas de IPs

- Configurar reglas en los firewalls para permitir conexiones únicamente desde direcciones IP autorizadas.
- Limitar accesos críticos a través de una VPN corporativa y evitar conexiones directas a servidores sensibles.

Monitoreo de Servicios Críticos y Detección de Anomalías (SIEM)

- Implementar un sistema de Security Information and Event Management (SIEM) para centralizar la recopilación de logs y detectar actividad sospechosa en tiempo real.
- Configurar alertas específicas para detectar creación de usuarios no autorizados en bases de datos como MySQL.

- Utilizar herramientas de Endpoint Detection and Response (EDR) para supervisar la actividad en servidores y estaciones de trabajo.

Hardening de Servidores y Configuraciones de Seguridad

- Crear y aplicar guías de hardening con configuraciones básicas de seguridad para todos los servidores.
- Entre las medidas básicas se incluyen:
    - Deshabilitar protocolos inseguros y servicios innecesarios.
    - Configurar permisos adecuados en servicios FTP, Apache y SSH.
    - Forzar el uso de cifrado TLS 1.2 o superior.
    - Restringir el listado de directorios en servidores web.

Aplicación del Principio de Menor Privilegio

- Implementar el principio de menor privilegio en todos los sistemas y accesos.
- Asegurar que cada usuario tenga permisos mínimos necesarios para desempeñar sus funciones.
- Revisar periódicamente las configuraciones de acceso para evitar privilegios excesivos.

Actualización Periódica de Servicios y Dispositivos

- Implementar un plan de gestión de parches para actualizar software, servidores y dispositivos de red.
- Utilizar herramientas de escaneo de vulnerabilidades para detectar riesgos y corregirlos oportunamente.

Auditorías Internas y Evaluaciones de Seguridad

- Realizar auditorías de seguridad de forma periódica (cada 3 a 6 meses) para evaluar configuraciones y detectar vulnerabilidades.

- Llevar a cabo pruebas de penetración para identificar debilidades antes de que sean explotadas por actores malintencionados.

Concienciación y Formación en Ciberseguridad

- Desarrollar programas de concienciación en ciberseguridad para los empleados.
- Capacitar en temas clave como:
    - Identificación de ataques de phishing.
    - Buenas prácticas en gestión de contraseñas.
    - Importancia del cumplimiento de las políticas de seguridad establecidas.

Conclusión El reciente incidente de seguridad ha demostrado la importancia de fortalecer las medidas de protección en la infraestructura tecnológica de la empresa. La aplicación de estas recomendaciones reducirá significativamente los riesgos de futuras amenazas y mejorará la postura de seguridad de la organización. Adicionalmente, se recomienda continuar con un enfoque proactivo en la gestión de la seguridad informática, promoviendo una cultura de ciberseguridad dentro de la empresa.