4Geeks Academy

Análisis Forense Digital

Por: Juan Cervantes Simón

Informe de Análisis de Incidencia

Introducción

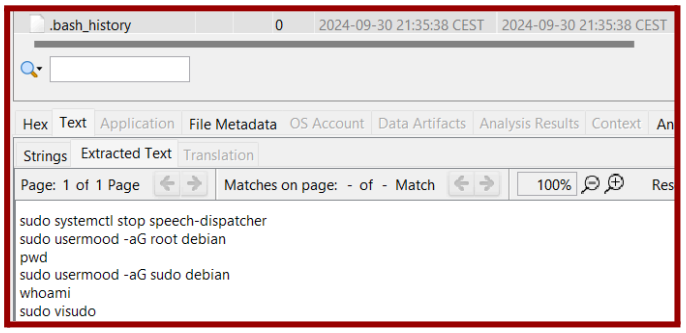
En este documento se recoge la reconstrucción de los hechos que tuvieron lugar en el equipo presentado que ocasionaron la falla de seguridad del equipo.
Se llevarán a cabo análisis de comportamiento de los usuarios del sistema, así como una reconstrucción teórica de los hechos haciendo uso del historial de comandos de los usuarios del sistema con objetivo de entender cómo se ocasionó la vulnerabilidad y de qué forma la aprovechó el atacante.

Herramientas Utilizadas

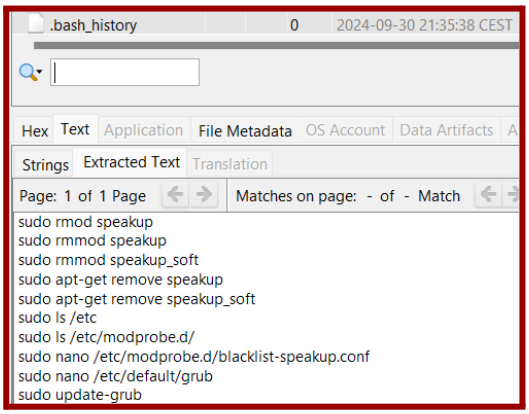
Para el análisis de las evidencias se utilizarán herramientas de Kali Linux como ***john the ripper***, ***grep*** y ***hashcat*** entre otras para poder extraer y listar la mayor cantidad de datos posible.

Evidencias Relevantes

- ***Archivos Manipulados***
  - Habiendo indagado en el historial de comandos, se comprueba que el usuario debian trató de realizar una escala de privilegios bastante tosca, haciendo uso de ***usermod*** y ***sudo visudo***, para hacer a *debian* un usuario con privilegios de administrador:



Del mismo modo, se intentaron realizar modificaciones en ***grub***, el bootmanager del sistema, así como en varios elementos de accesibilidad del kernel del sistema:



Tras esto, se realizó una instalación de ***apache2***, junto con ***mariaDB*** y ***MySQL***, así como la aplicación de la configuración por defecto de una página web de wordpress en dicho servicio, la instalación de ambas bases de datos es signo o de falta de conocimiento técnico, o de intención de crear vulnerabilidades, puesto que instalar ambos modelos de bases de datos en el sistema puede generar incompatibilidades entre ellos.

```
sudo apt install apache2 -y
sudo systemctl enable apache2
sudo systemctl start apache2
sudo systemctl status apache2
sudo apt install mysql-server php php-mysqli -y
sudo apt install mariadb-server -y
sudo systemctl start maria-db
sudo apt install mariadb-server
sudo systemctl start mariadb-server
sudo systemctl start mariadb
sudo systemctl enable mariadb
sudo mysql_secure_installation
sudo mysql -u root -p
cd /tmp
curl -O https://wordpress.org/latest.tar.gz
sudo apt install curl
curl -O https://wordpress.org/latest.tar.gz
tar xzvf latest.tar.gz
sudo cp -a /tmp/wordpress/. /var/www/html/
sudo chown -R www-data:www-data /var/www/html/
sudo chmod -R 755 /var/www/html/
cd /var/www/html/
sudo mv wp-config-sample.php wp-config.php
sudo nano wp-config.php
ip a
sudo systemctl restart apache2
sudo systemctl status apache2
```

Línea de Tiempo

Basándose en el comportamiento eximido en la línea de comandos y en la configuración observada en los servicios prestados, así como las modificaciones al kernel que el usuario ha intentado realizar, se puede considerar que el atacante era alguien con pocos conocimientos técnicos, que aprovechó la vaga configuración inicial de la que partía la máquina para tratar de ganar privilegios en el sistema, todo ello sin éxito, siendo que los resultados obtenidos en las pruebas de pentesting indican que el atacante logró entrar por la fragilidad de la contraseña.

Medidas correctivas aplicadas

Para reparar la mayoría de vulnerabilidades se ha realizado una actualización completa del sistema, por medio de ***sudo apt-get update && sudo apt-get full-upgrade -y***, de esta forma se han eliminado todas las vulnerabilidades de carácter crítico y alto, volviendo el sistema mucho más seguro, del mismo modo se ha actualizado la contraseña de usuario a una mucho más resistente para poder aguantar mejor ataques de fuerza bruta.

Para futura revisión, la máquina tiene la contraseña: @#@1RonBr1dge987@#@