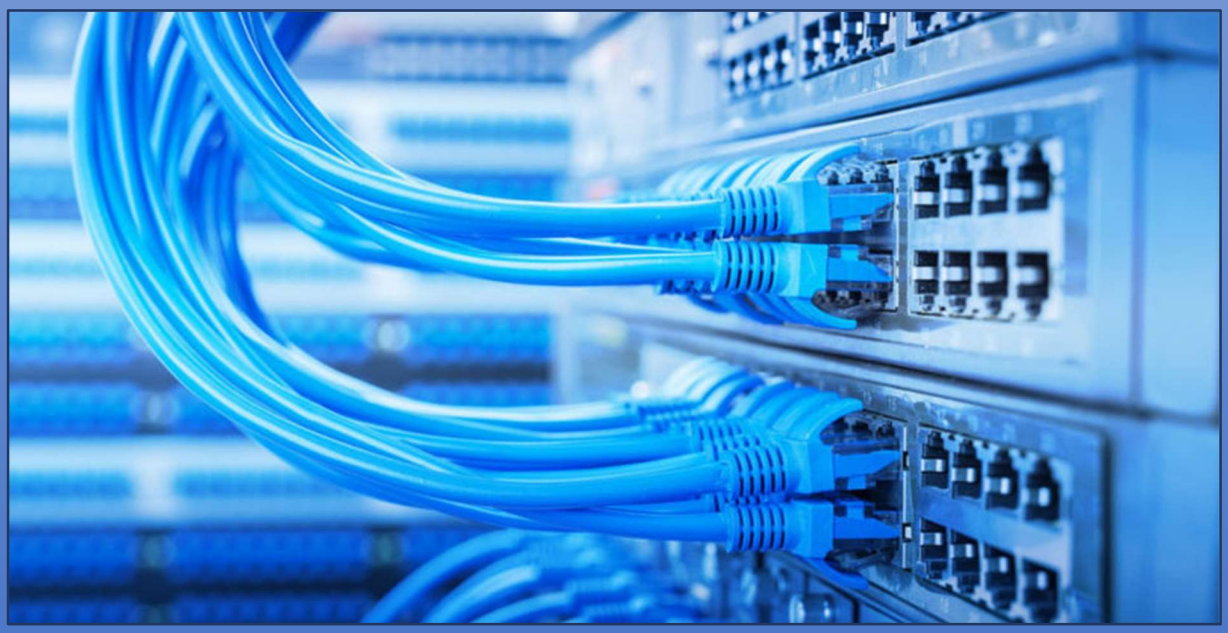


Informe de vulnerabilidad detectada en sistema Linux

Jesús Díaz

Índice

1. INFORME EJECUTIVO

1.1 INTRODUCCIÓN

Se ha identificado una posible brecha de seguridad en uno de los sistemas Linux de la organización. A través de una prueba de acceso, fue posible entrar en una sección del sistema que no estaba debidamente protegida, lo que permitió obtener credenciales de acceso.

Esto demuestra una debilidad en la configuración del sistema que podría ser usada por un atacante y poner en riesgo la seguridad de la información. El presente informe expone lo ocurrido, su posible impacto y las medidas recomendadas para corregirlo.

1.2 ALCANCE

En el análisis se realizó un acceso no autorizado al sistema, que permitió ver y extraer información sensible desde un panel de administración oculto. En concreto, se accedió a un panel desde el que fue posible obtener credenciales de usuario, implicando esto la capacidad de actuar dentro del sistema con permisos válidos.

Este acceso no sólo compromete la confidencialidad de los datos, sino que también representa una puerta de entrada que podría ser utilizada para escalar privilegios, alterar configuraciones, o afectar la disponibilidad de servicios críticos.

Riesgos asociados

- **Robo de información**: Las credenciales obtenidas podrían utilizarse para acceder a otros sistemas o servicios internos.

- **Alteración de sistemas**: El acceso administrativo podría permitir la modificación o borrado de configuraciones y archivos críticos.

- **Persistencia del atacante**: Si no se detecta, este acceso podría mantenerse en el tiempo sin ser advertido.

- **Falta de visibilidad**: El hecho de que esta forma de acceso no estuviera documentada indica posibles deficiencias en la monitorización del sistema.

El acceso, aunque puntual, demuestra la posibilidad real de que un atacante externo comprometa la seguridad del sistema sin ser detectado. Por ello, se considera prioritaria la revisión completa de los servicios expuestos y la implementación de controles adicionales para prevenir accesos similares en el futuro.

1.3 PROBLEMAS ENCONTRADOS

Durante el análisis del sistema Linux comprometido se han detectado algunos problemas que podrían aumentar el riesgo de intrusión y comprometer la seguridad general del sistema. Estos fallos de forma combinada permitirían un acceso no autorizado.

Problemas detectados

1. Existencia de una forma de acceso al sistema que no está documentada ni protegida adecuadamente. Este punto de entrada ha sido clave para la intrusión.

2. Falta de control y supervisión de servicios expuestos, ya que el sistema Linux permite conexiones desde el exterior sin filtros ni restricciones, lo que ha facilitado su descubrimiento y posterior explotación.

3. El sistema contiene una un panel de administración oculto pero accesible, sin medios de autenticación ni protección, lo que facilita el acceso a información sensible.

4. Las credenciales de acceso obtenidas no estaban cifradas, lo que ha facilitado su extracción y posterior utilización.

5. No existen sistemas de monitorización ni alertas que avisen de conexiones anómalas o accesos sospechosos.

Estos problemas, tomados en conjunto, indican una deficiencia en la gestión de la seguridad del sistema afectado.

1.4 SOLUCIONES O RECOMENDACIONES

Tras analizar los problemas identificados en el sistema Linux comprometido, se proponen una serie de soluciones y buenas prácticas para corregir las debilidades detectadas y mejorar la seguridad general de la organización:

1. Cierre y revisión de accesos no documentados

Todos las formas de entrada al sistema deben estar documentadas, bajo control y justificadas. Cualquier servicio o acceso no autorizado o no documentado debe ser eliminado inmediatamente.

2. Aplicación de un firewall

Implementando reglas que limiten las conexiones entrantes únicamente a los servicios necesarios, reduciendo así la superficie expuesta a posibles atacantes.

3. Fortalecimiento de la autenticación

- Proteger cualquier interfaz de administración con autenticación robusta (por ejemplo, autenticación en dos pasos o 2FA).

- Asegurarse de que las credenciales se almacenen de forma segura y utilizar sistemas de gestión de contraseñas.

4. Monitorización y alertas de seguridad

Configurar sistemas de registro de actividad (logs) y herramientas de monitorización que alerten sobre accesos no autorizados, conexiones anómalas o cambios sospechosos en el sistema.

5. Auditorías de seguridad periódicas

Realizar auditorías regulares para identificar servicios innecesarios, vulnerabilidades activas y configuraciones débiles antes de que puedan ser explotadas.

6. Documentación y control de cambios

Mantener un registro actualizado de todos los servicios, puertos y configuraciones activas en los servidores. Cualquier cambio en el sistema debe pasar por un proceso de revisión y aprobación.

7. Formación al personal

Capacitar y concienciar tanto a los administradores de sistemas como a los usuarios de los mismos en conceptos básicos de ciberseguridad, gestión segura de servicios y detección de configuraciones inseguras.

Estas recomendaciones sirven para corregir el incidente detectado, y también para establecer una cultura de seguridad preventiva que reduzca la probabilidad de intrusiones y facilite una respuesta rápida ante los mismos.

2. INFORME TÉCNICO

2.1 INTRODUCCIÓN

Este informe técnico documenta el análisis realizado sobre el sistema Linux de la organización tras detectarse un tráfico de red anómalo que ha permitido descubrir una vía de entrada insegura al mismo. El objetivo del análisis ha sido identificar el origen de la brecha, las vulnerabilidades explotadas y evaluar su alcance.

2.2 HERRAMIENTAS EMPLEADAS

Kali Linux

Kali Linux es una distribución de sistema operativo basada en Debian, diseñada específicamente para tareas de auditoría de seguridad, análisis forense y pruebas de penetración. Incluye una gran cantidad de herramientas preinstaladas para análisis de red, explotación de vulnerabilidades, ingeniería inversa y otras tareas relacionadas con la ciberseguridad.

Se utilizó como entorno principal de trabajo por su versatilidad y amplio conjunto de herramientas, lo que permitió realizar todas las fases del análisis desde una sola plataforma.

Wireshark

Wireshark es una herramienta de análisis de protocolos de red que permite capturar y examinar en detalle el tráfico que circula por una red. Ofrece una interfaz gráfica intuitiva para visualizar paquetes, filtrar información relevante y analizar posibles anomalías.

Se empleó para capturar y analizar el tráfico de red del sistema Linux comprometido y ha sido clave para detectar el tráfico anomalo, lo que permitió identificar el punto de entrada al sistema.

Netcat

Netcat es una utilidad de red muy versátil que permite leer y escribir datos a través de conexiones de red, utilizando los protocolos TCP o UDP. Se utiliza para establecer conexiones o crear túneles de comunicación entre máquinas.

Se utilizó para conectarse directamente al servicio expuesto en el sistema Linux objetivo a través del puerto detectado, simulando el comportamiento que podría realizar un atacante externo. Gracias a Netcat fue posible interactuar con el sistema y acceder a una interfaz de administración que no requería autenticación.

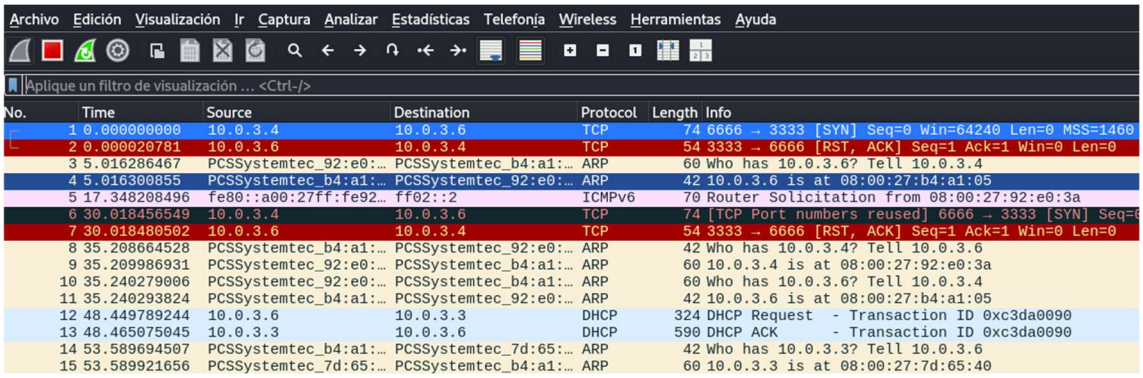
2.3 EXPLOTACIÓN

En este apartado se detalla el proceso de explotación del sistema Linux objetivo paso a paso hasta la obtención de credenciales válidas. El objetivo ha sido simular un ataque que permita detectar fallos en la seguridad del sistema y evidenciar los riesgos asociados.

Paso 1: Captura y análisis de tráfico con Wireshark

Se inició la monitorización del tráfico de red utilizando Wireshark, lo que permitió detectar comunicaciones sospechosas entre el sistema Linux y la máquina Kali. Al aplicar filtros de análisis, se observó tráfico dirigido a un puerto inusual no documentado.

Trafico capturado por Wireshark:



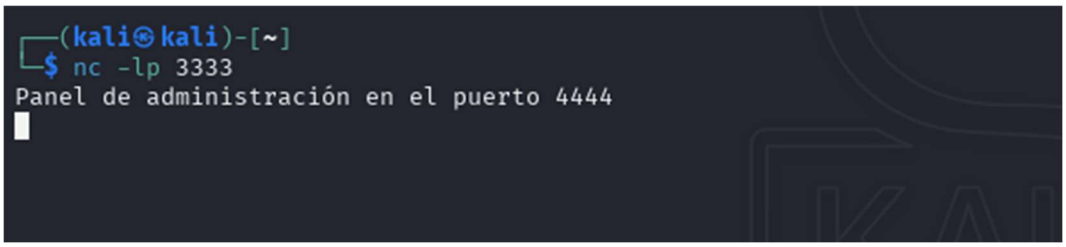
Tráfico filtrado por TCP:

Se observa envío periódico de paquetes desde la IP 10.0.3.4 (sistema Linux) por el puerto 6666 hacia la IP 10.0.3.6 (máquina Kali) por el puerto 3333.

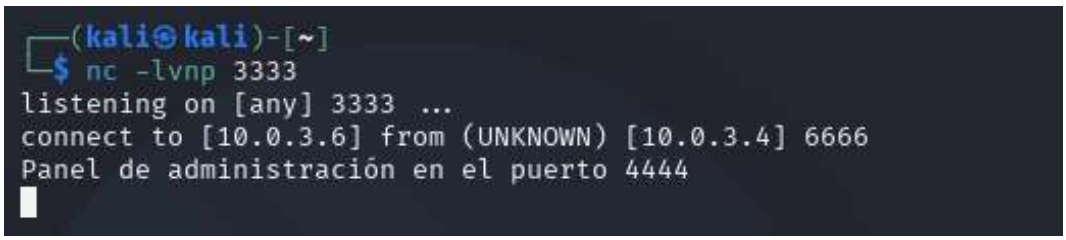
Este hallazgo sugiere la existencia de un servicio activo que podría estar expuesto sin medidas de protección.

Paso 2: Descubrimiento del servicio oculto

Mediante la herramienta netcat escuchamos por el puerto 3333 de la máquina Kali para comprobar si se recibe alguna información:



Tras unos instantes de espera, la escucha por el puerto 3333 mostró la existencia de un panel de administración oculto en el sistema Linux por el puerto 4444.



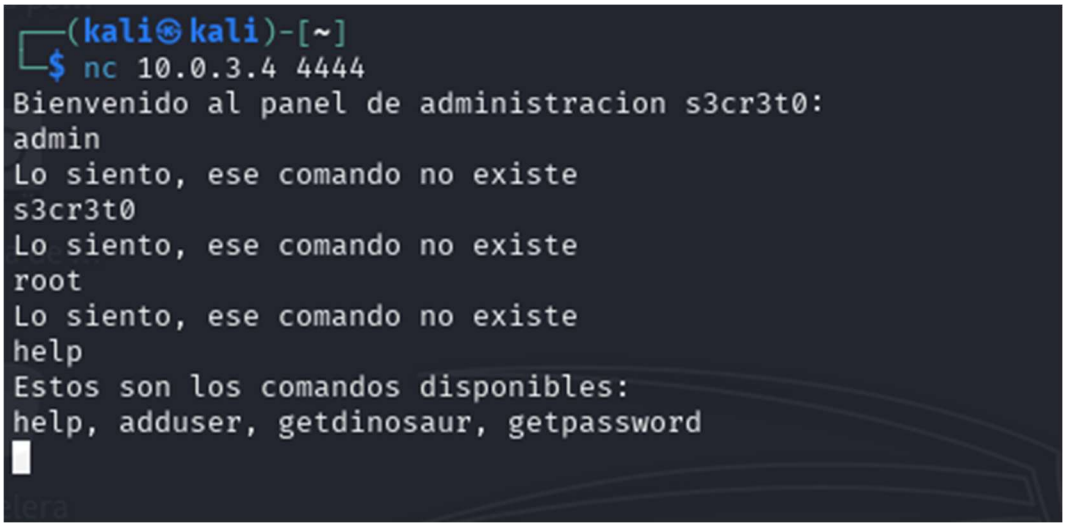
De esta forma se confirmó que el puerto 4444 estaba abierto en el sistema Linux.

Paso 3: Conexión al servicio usando Netcat

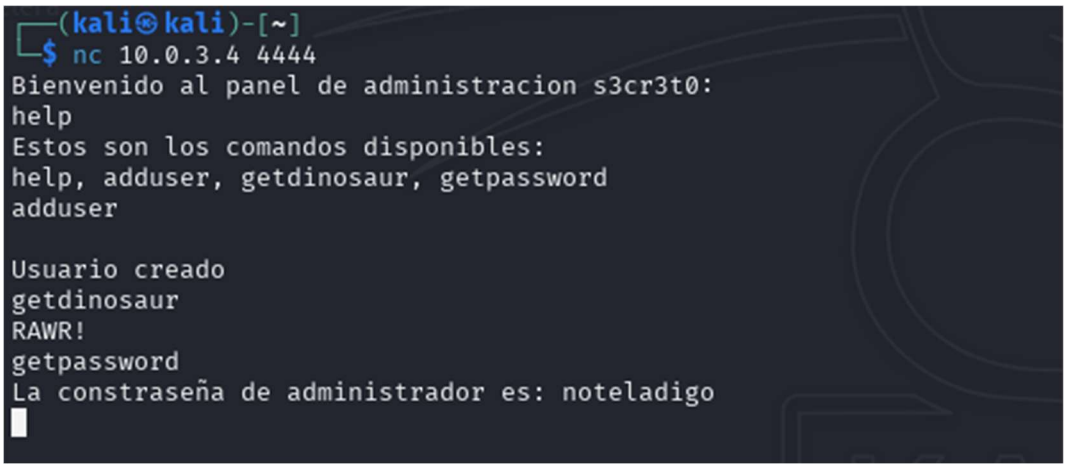
Utilizando de nuevo la herramienta netcat, se estableció una conexión manual al puerto descubierto.

La conexión fue exitosa y reveló una interfaz de administración, sin ningún tipo de autenticación ni cifrado:

Se prueba de forma aleatoria con diferentes palabras que podrían ser posibles comandos para dicho panel de administración, y se obtiene resultado con la palabra help, que al introducirla muestra el resto de comandos disponibles: help, adduser, getdinosaur y getpassword:



Se ejecutan cada uno de los cuatro comandos disponibles, siendo getpassword el más relevante:



Paso 4: Acceso a credenciales

Tras explorar el panel de administración, el comando getpassword mostró credenciales de acceso. Las credenciales aparecían en texto plano y no estaban protegidas mediante cifrado.

El mensaje que muestra getpassword sugiere que las credenciales de acceso al sistema Linux podrían ser:

```
user: administrador
pass: noteladigo
```

Probamos dichas credenciales en el sistema Linux y conseguimos acceso:

Este hallazgo confirma la posibilidad de que un atacante pueda obtener acceso al sistema y posiblemente a otros recursos internos de la organización.

Resultado final de la explotación

- Se obtuvo acceso remoto no autorizado al sistema.
- Se accedió a un panel de administración sin protección.
- Se extrajeron credenciales válidas almacenadas en texto plano.
- No hubo alertas o bloqueos por parte del sistema Linux objetivo durante la explotación.

Se demuestra así, cómo un atacante podría comprometer el sistema sin necesidad de técnicas complejas, simplemente aprovechando una configuración insegura y una ausencia de control de acceso. La explotación fue exitosa y pone de manifiesto la urgencia de aplicar medidas correctivas.