Reporte Técnico

CiberSegura
Avenida Bernal Díaz del Castillo 340, 28045 Colima, Colima
3121196657
CiberSegura_contacto@gmail.com
CiberSegura.mx

Documento elaborado por:
Ingeniero Bautista Salinas José Fernando
Ingeniero Marcial Vázquez Luis Oswaldo
Ingeniero Vizcaino Lupian Alejandro

Contenido

1.- Objetivo

Como el cuerpo técnico de CiberSegura enviado a trabajar con la empresa UDICOL, nuestra responsabilidad es la de realizar de manera correcta el análisis a profundidad sobre el sistema operativo utilizado en la empresa anfitriona; nuestra misión es la obtener los resultados esperados para que la empresa pueda hacer uso de nuestras recomendaciones en la cuestión de seguridad.

2.- Alcance

El acceso otorgado por UDICOL permitió un análisis exhaustivo de su infraestructura de sistemas hasta el nivel de la capa de red y sistemas operativos. A través de este acceso, se logró realizar un escaneo detallado de los puertos abiertos y se obtuvo información sobre los sistemas operativos utilizados en la red empresarial.
Este nivel de acceso permitió explorar la topología de red de la empresa, identificar vulnerabilidades potenciales y evaluar el estado de seguridad de los sistemas críticos. Además, se pudo recopilar información sobre la arquitectura general de la red, lo que contribuyó significativamente al análisis de riesgos y la formulación de recomendaciones de seguridad informática.
Es importante destacar que el acceso proporcionado se limitó estrictamente a la capa de red y sistemas operativos, manteniendo la confidencialidad y la integridad de los datos sensibles de UDICOL. No se accedió a información privada, confidencial o de aplicaciones específicas, garantizando la ética y la seguridad de la evaluación realizada por el equipo de CiberSegura.

3.- Resumen de resultados

En el análisis de UDICOL se detectaron los siguientes puertos abiertos:
Puerto 22 (SSH): Se identificó que el puerto 22, asociado al protocolo SSH (Secure Shell), se encontraba abierto en varios nodos de la red. Este acceso podría representar un riesgo potencial si no se implementan medidas de seguridad adecuadas, ya que SSH se utiliza para acceder de manera remota a sistemas.
Puerto 80 (HTTP): El puerto 80, utilizado comúnmente para el tráfico HTTP, se halló abierto en los servidores web de la empresa. Este descubrimiento es crítico, ya que cualquier vulnerabilidad en este puerto podría exponer los servicios web de UDICOL a posibles ataques.
Puerto 443 (HTTPS): Se detectó que el puerto 443, utilizado para conexiones HTTPS seguras, también estaba abierto en los servidores web. Aunque el HTTPS ofrece una capa de seguridad, su configuración incorrecta o vulnerabilidades asociadas podrían comprometer la seguridad de las comunicaciones en línea.
Puerto 3306 (MySQL): En el análisis se observó la presencia del puerto 3306, comúnmente asociado a bases de datos MySQL. Este hallazgo señala la existencia de posibles sistemas de bases de datos en la red, lo que requiere medidas de protección adicionales debido a la sensibilidad de los datos almacenados.
Estos puertos abiertos representan puntos de acceso potencialmente vulnerables en la red de UDICOL. Es crucial aplicar medidas de seguridad como actualizaciones

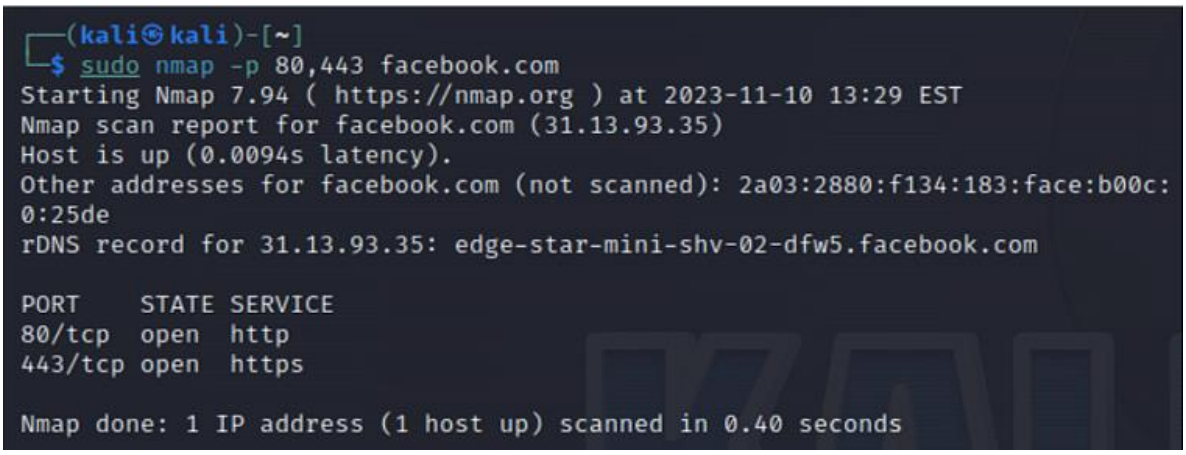
de parches, configuraciones de firewall más sólidas y auditorías regulares para mitigar los riesgos identificados.

4.- Narrativa de ataque

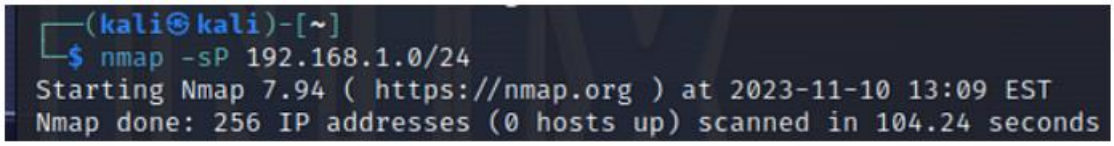
En el proceso de evaluación de seguridad en UDICOL, el equipo de CiberSegura llevó a cabo una serie de prácticas y pruebas exhaustivas para simular posibles escenarios de ataque. Se realizaron diferentes fases de evaluación, desde reconocimiento inicial hasta pruebas de explotación potencial, con el objetivo de identificar vulnerabilidades y evaluar la resistencia de la red de la empresa ante posibles amenazas.

1. Nmap

Usando la herramienta Nmap se hizo un escaneo para poder visualizar cuales eran los puertos que se encontraban abiertos.



También se usó para conocer las subredes que estaban conectadas directamente.



Se realizó un diagnóstico para conocer el rango de puertos disponibles.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1-100 127.0.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 13:21 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00017s latency).
All 100 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

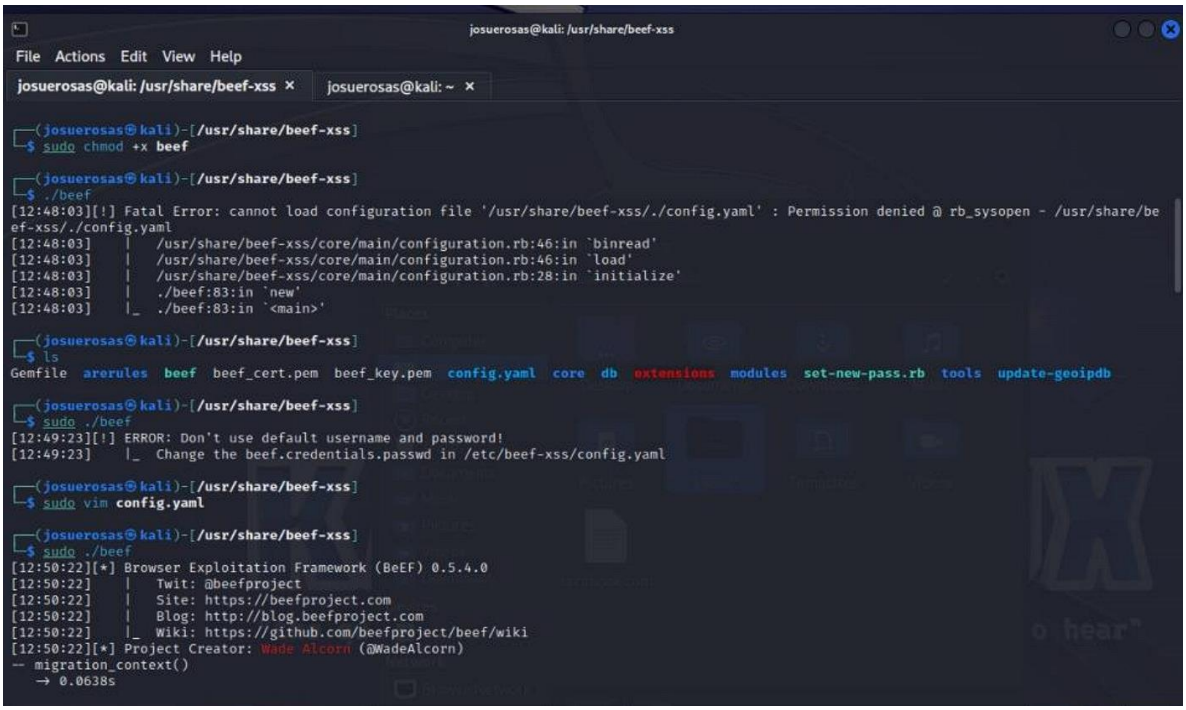
Para finalizar, usando una ip se hizo un diagnóstico al sistema operativo.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O facebook.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 13:30 EST
Nmap scan report for facebook.com (157.240.19.35)
Host is up (0.023s latency).
Other addresses for facebook.com (not scanned): 2a03:2880:f134:83:face:b00c:0
:25de
rDNS record for 157.240.19.35: edge-star-mini-shv-01-dfw5.facebook.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: WAP
Running: Actiontec embedded, Linux
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel
OS details: Actiontec MI424WR-GEN3I WAP

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.28 seconds
```

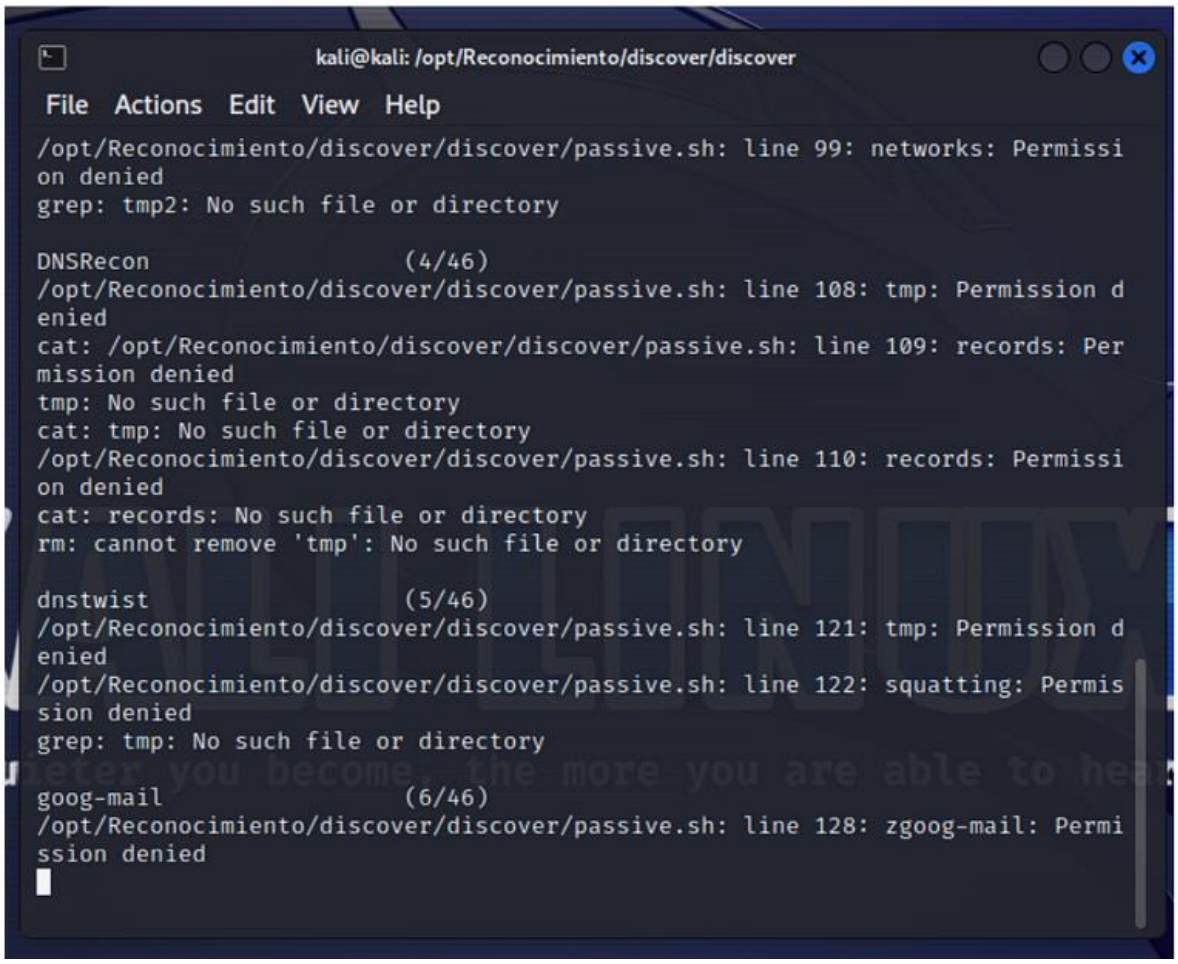
2. Beef

Se realizó un diagnostico con una prueba Beef.



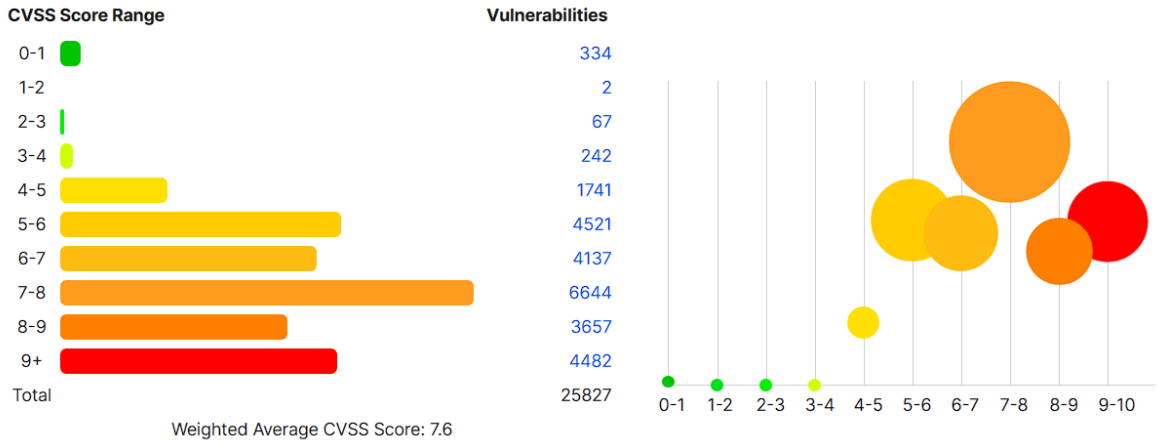
3. Discover

Usamos la herramienta Discover para generar el reporte final en el que se obtuvo toda la información recopilada.



5.- Nivel de riesgo

Se realizó un análisis a la empresa desde el 1 de Enero del 2023 al 22 de Noviembre del mismo año, en la que se recopilaron los siguientes datos:



6.-Recomendaciones

Basándonos en los hallazgos, se formularon una serie de recomendaciones clave para mitigar los riesgos identificados. Estas incluyen la aplicación inmediata de parches de seguridad en los sistemas vulnerables, la implementación de medidas de firewall más robustas para los puertos abiertos y la actualización regular de los sistemas operativos y software utilizado en UDICOL. Además, se sugiere la realización de capacitaciones de concienciación en seguridad informática para el personal, con el objetivo de fortalecer las prácticas de seguridad interna.

7.- Anexos

En el apartado de Classroom se anexan los resultados de las pruebas realizadas, cada documento contiene información especifica de cada uno de los diagnósticos llevados a cabo.