

**Informe de Actividades**

**Máquina CTF "Brooklyn Nine Nine"**

**Fecha: 12 de julio de 2023**

**Realizado Por: Msc. Angel R. Paz**

**Introducción**

El presente informe detalla las actividades realizadas en el marco del desafío CTF "Brooklyn Nine Nine". El objetivo de este desafío es obtener acceso a la máquina y obtener privilegios de root para tener control total sobre la misma. Durante el proceso, se llevaron a cabo diversas etapas, como la exploración inicial de servicios, el análisis de código fuente y el uso de técnicas de esteganografía para descubrir información oculta. Además, se logró el acceso a la máquina utilizando las credenciales encontradas y se obtuvieron privilegios de root mediante la explotación de una vulnerabilidad en el comando "sudo nano".

El informe proporcionará un resumen detallado de cada etapa, incluyendo los resultados obtenidos, las herramientas utilizadas y las recomendaciones para futuras acciones. Es importante destacar que todas las actividades se llevaron a cabo siguiendo las pautas éticas y cumpliendo con las regulaciones legales establecidas.

A continuación, se presentarán los hallazgos y resultados obtenidos en cada fase del desafío, así como las recomendaciones para continuar avanzando hacia la resolución completa de la máquina.

Esta introducción establece el propósito y el alcance del informe, proporcionando una visión general del desafío CTF "Brooklyn Nine Nine". En las secciones posteriores del informe, se profundizará en los detalles de cada etapa y se brindarán recomendaciones para avanzar en el acceso y obtención de privilegios de root.

**Exploración Inicial:**

Se llevó a cabo una exploración en la máquina CTF "Brooklyn Nine Nine" utilizando la herramienta NMAP. Se identificaron los siguientes servicios y puertos abiertos:

* Puerto 21/tcp: Servicio FTP (vsftpd 3.0.3)
* Puerto 22/tcp: Servicio SSH (OpenSSH 7.6p1 Ubuntu)
* Puerto 80/tcp: Servicio HTTP (Apache httpd 2.4.29)

***Comandos:***

* ***nmap -sS -sV <IP>***

**Esteganografía:**

Se descubrió una pista en el código fuente de la página web, indicando el uso de esteganografía para resolver la máquina. Se extrajo información oculta de la imagen "brooklyn99.jpg" utilizando la herramienta "stegcracker". El contenido extraído fue el siguiente:

***Archivo: brooklyn99.jpg.out***

***Contenido:***

***Holts Password:***

***fluffydog12@ninenine***

***Comandos:***

* ***steghide extract -sf imagen.jpg***
* ***stegcracker imagen.jpg***
* ***cat brooklyn99.jpg.out***

**Acceso a la Máquina:**

Se utilizaron las credenciales encontradas para el usuario Holt y se logró un acceso exitoso a través del servicio SSH.

***Comandos:***

* ***ssh holt@ <IP>***

**Privilegios de Root:**

Al ejecutar el comando "Ssudo -l", se identificó que era posible ejecutar el comando "nano" con privilegios de root. Mediante el uso de la técnica "GTOBINS", se encontró el comando que proporciona privilegios de root:

***sudo nano***

***^R^X***

***reset; sh 1>&0 2>&0***

Este comando permitió obtener una shell con privilegios de root en la máquina.

**Recomendaciones Futuras:**

Aunque se ha logrado obtener privilegios de root en la máquina, es importante seguir investigando y explorando para identificar cualquier otro posible vector de ataque o área de interés. A continuación, se sugieren algunas recomendaciones futuras:

* Realizar un análisis de seguridad más exhaustivo para identificar y corregir cualquier posible vulnerabilidad o brecha de seguridad en la configuración de los servicios y en el sistema operativo.
* Documentar detalladamente cada paso realizado durante el proceso de acceso y obtención de privilegios de root.
* Explorar y analizar los archivos y configuraciones del sistema en busca de información adicional o pistas que puedan llevar a nuevos desafíos o a la obtención de información confidencial.
* Mantener una ética responsable y cumplir con todas las regulaciones legales aplicables durante todas las actividades realizadas en el marco de este desafío.