**UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA**

**UNAN-León**

****

**Facultad de Ciencias y Tecnología**

**Departamento de Computación**

**Ingeniería en Telemática**

**Componente:** Seguridad de Redes

**Docente:** Aldo Martínez

**Tema:** System Hacking

**Fecha:** 29-04-2019

**Integrante:** Jonathan Eduardo Ochoa Velasquez 15-01898-0

**¡A la libertad por la Universidad!**

**Lab 3: Auditoría de la contraseña del sistema usando L0phtCrack**

L0phtCrack es una herramienta de auditoría de contraseña que contiene características como programación, extracción de hash desde versiones de Windows de 64 bits, algoritmos de multiprocesador y monitoreo de redes.

Escenario del laboratorio:

Porque la seguridad y la conformidad son prioridades importantes para todas las organizaciones, los ataques a sistemas computacionales de organizaciones se pueden hacer de distintas maneras, como spoofing, Ataques de denegación de servicio. Estos ataques son designados para dañar el uso de los sistemas operacionales.

El crackeo de contraseñas es un término usado para describir la penetración de una red, un sistema o un recurso con o sin el uso de herramientas de desbloqueo a un recurso que ha sido asegurado con una contraseña. En este laboratorio, vamos a ver que es el crackero de contraseñas, por que lo utilizan los hackers, como ellos logran sus metas y que puedes hacer para protegerte. Mediante una examinación a diferentes escenarios, en este laboratorio vamos a describir algunas de las técnicas que ellos utilizan y las herramientas que usan para crackear contraseñas

Objetivos del Laboratorio:

* Usar la herramienta L0phtcrack para obtener contraseñas que pueden ser fáciles de crackear.

Desarrollo del Laboratorio:

Para desarrollar este laboratorio necesitas:

* Herramienta L0phtCrack
* Windows Server 2012 corriendo como máquina host
* Windows Server 2008 corriendo en una máquina virtuales
* Ejecutar las herramientas como administrador.