**TESIS**

**Motivación: Análisis de mercado, soluciones actuales**

Considerando la multitud , prestancia y relevancia que ofrecen los servidores Linux a nivel global, y lo vital de mantenerlos seguros, nos hemos sentido motivados a contribuir con un granito de arena en poder suministrar una herramienta que ayude a los administradores de arquitecturas en Linux a poder evaluar los riesgos de seguridad de sus implementaciones, en eras de poder “auto corregirse” y de minimizar de manera preventiva alguna configuración, o niveles de permisos que pudieran constituirse en posibles puertas de acceso de ciber delincuentes o que permitan fuga de información, etc.

Nos llamó de sobremanera la atención lo módulos: 4: Seguridad en Arquitecturas Linux y 5: Seguridad en Redes corporativas, dado la practicidad de su contenido y el enfoque del tutor, todo ello nos llevo a inclinar basar nuestra tesis en estos atractivos módulos del master.

Realizando un análisis de mercado encontramos la siguiente información referente a Linux:

* El 96,3% del millón de servidores más importantes del mundo se ejecutan en Linux.
* El 90% de la carga de trabajo de la nube pública se ejecuta en Linux.
* En 2021, el 100% de las 500 supercomputadoras más importantes del mundo funcionan con Linux.
* El 36,7% de los sitios web con sistemas operativos conocidos utilizan Linux en 2021.
* El 83,1% de los desarrolladores dice que Linux es la plataforma en la que prefieren trabajar.

Con respecto a soluciones actuales con alguna funcionalidad similar a la que proponemos en nuestra tesis tenemos:

* Unicornscan.- Es una de las principales herramientas de recopilación de información para la investigación de seguridad, similar a nuestra tesis detección de banner, detección de aplicaciones y componentes, soporte para salida relacional SQL.
* DMitry .- Aplicación de línea de comandos de UNIX / (GNU) Linux codificada en C, tiene la capacidad de recopilar tanta información como sea posible sobre un host. Posee una característica que pretendemos emular como la de ser modular y que permite añadir nuevos escaneos o funcionalidades al usuario.

**ESPECIFICACIÓN DE REQUISITOS**

Requisitos de Software:

* Windows 7 en adelante
* Linux
* MAC.

Requisitos de Hardware:

* Pentium 4 en adelante.
* Arquitectura de 32 o 64 bits.
* 512 de RAM en adelante
* 1GB de espacio en disco duro.

**HIPÓTESIS**

Nuestra tesis toma en base a los datos levantados y análisis del alcance del proyecto y soluciones del mercado que podremos aportar de manera significativa a los administradores de TI en arquitecturas en Linux con una herramienta sencilla y eficaz que les permitirá obtener sugerencias realistas de mejoras de seguridad en sus servidores Linux.

Nuestro objetivo es que la herramienta analice logs, obtenga servicios levantados, con que usuarios son ejecutados, niveles de acceso de dichos usuarios, realización de varias pruebas con los usuarios encontrados para determinar posibles brechas de seguridad o expuestas a ataques y sugerencias.

Se parte con la premisa de que a mayor nivel de acceso de usuario utilizado para el Login de le herramienta la misma podrá analizar a mayor profundidad los servidores especificados.

Conceptualmente hablando nuestra herramienta debe ser capaz de mediante los usuarios encontrados saber que podría hacer un atacante si pudiera ejecutar software con nivel de acceso similar y en base a ello poder diagnosticar o predecir que tipo de ataque pudiera realizar y dar soluciones para evitarlo o mitigarlo.

Pretendemos poder almacenar la información recopilada (los comandos ejecutados para ello) en una base de datos y poder o bien graficarla en un reporteador propio o en su defecto crear un plugin o interfaz con alguna herramienta de reportería de terceros.

Finalmente, nuestra herramienta pretende permitir a lo sea a los usuarios o a nosotros como dueños del productos comandos o funciones adicionales para ir robusteciendo a la herramienta en el tiempo.

Bibliografía:

Motivación: Análisis del mercado

<https://hostingtribunal.com/blog/linux-statistics/#:~:text=96.3%25%20of%20the%20world's%20top,best%20cloud%20hosts%20use%20it>

<https://tools.kali.org/information-gathering/dmitry>

<https://github.com/dneufeld/unicornscan>