Proyecto final Sistemas Operativos: Análisis de Vulnerabilidades en Sistemas Operativos de Dispositivos IoT mediante Shodan

Valeria Ballestero Ortiz
valeria.ortizp@udea.edu.co

Sara Lorena Duque
sara.duque1@udea.edu.co

Isaac Esteban Uribe
isaac.uribej@udea.edu.co

Profesor:

Henry Alberto Arcila Ramírez

Modalidad:

Presencial

22/10/2024

Universidad de Antioquia

Sistemas Operativos

Resumen

En este documento se dará a conocer el proyecto en el cual abordaremos la temática "***Análisis de Vulnerabilidades en Sistemas Operativos de Dispositivos IoT mediante Shodan***". Contextualizaremos el tema mediante una introducción, agregaremos un marco teórico que relaciona las vulnerabilidades de dispositivos IoT y las estrategias Hardening. Posteriormente se darán a conocer el objetivo general y los objetivos específicos del proyecto; además, se especifica la metodología y el diseño de experimentos. Finalmente, se observa un cronograma que estipule las actividades a realizar y las referencias de donde obtuvimos la información.

Introducción

La seguridad en los dispositivos de Internet de las Cosas (IoT) se ha convertido en una preocupación crítica para las empresas y personas que hacen uso de estos dispositivos. Es a medida que los dispositivos de IoT se integraron en diversas aplicaciones o aparatos que se usan a diario que van desde la automatización del hogar hasta la gestión industrial. Este proyecto se centra en el "hardening" de sistemas operativos de dispositivos IoT, un proceso que implica la implementación de medidas de seguridad para mitigar riesgos y mejorar la resistencia ante amenazas.
El objetivo principal es deshabilitar funciones innecesarias que podrían servir como vectores de ataque, como el inicio del sistema desde unidades no autorizadas y la conexión de dispositivos externos, tales como USB y ópticos. Además, el proyecto evaluará el rendimiento del sistema operativo tras aplicar estas medidas, analizando el tiempo de arranque y la eficiencia operativa con un enfoque en una instalación mínima que excluya componentes no esenciales.

Marco teórico

Vulnerabilidades en Dispositivos IoT

Los dispositivos IoT, como los asistentes de voz, routers y otros dispositivos conectados, son cada vez más comunes en entornos domésticos y empresariales. Jackson y Orebaugh identifican varios problemas de seguridad y privacidad asociados con dispositivos como el Amazon Echo, subrayando que muchos usuarios son inconscientes de si sus dispositivos han sido comprometidos, ya que un ataque exitoso no necesariamente degrada el rendimiento del dispositivo[1]. Esta falta de conciencia puede llevar a una exposición prolongada a amenazas cibernéticas.
Un ejemplo notable de las repercusiones de la falta de "hardening" es el ataque DDoS del botnet Mirai en 2016, que afectó a más de 600,000 dispositivos IoT, causando interrupciones significativas en sitios web importantes como Amazon y Netflix[2].

Estrategias de Hardening

El "hardening" implica la aplicación de diversas estrategias para reducir la superficie de ataque y mejorar la seguridad general del dispositivo. Estas estrategias incluyen la desactivación de funciones innecesarias, como el inicio desde unidades externas o la

conexión de dispositivos USB, así como la implementación de configuraciones mínimas que eviten la instalación de componentes no esenciales[3]. Estas medidas son cruciales para proteger los datos sensibles que pueden ser vulnerables a ataques.

Además, es fundamental considerar las características específicas del firmware en dispositivos IoT. A menudo, estos sistemas operativos carecen de las protecciones robustas que se encuentran en plataformas más complejas, lo que los hace susceptibles a ataques que explotan vulnerabilidades conocidas[4]. Por lo tanto, el "hardening" no solo debe enfocarse en configuraciones externas, sino también en asegurar el software subyacente.

Objetivos

Objetivo General

Evaluar el impacto de las estrategias de "hardening" en el rendimiento de sistemas operativos de dispositivos IoT mediante un diseño experimental que permita medir variables clave relacionadas con la eficiencia y la seguridad.

Objetivos Específicos

1. **Analizar el tiempo de arranque del sistema operativo antes y después de implementar medidas de "hardening".**
    - Este objetivo se centra en medir el tiempo que tarda el dispositivo en iniciar, lo que permitirá determinar si las prácticas de seguridad afectan negativamente al rendimiento inicial del sistema.

2. **Evaluar la eficiencia del sistema de archivos utilizado en el dispositivo IoT tras aplicar configuraciones mínimas y de seguridad.**
    - Se medirá el rendimiento del sistema de archivos en términos de velocidad de acceso y procesamiento de datos, comparando los resultados antes y después del "hardening".

3. **Determinar el impacto de la desactivación de dispositivos externos (como USB y ópticos) en la velocidad y estabilidad del sistema operativo.**
    - Este objetivo implica realizar pruebas que midan cómo la restricción de accesos externos afecta el rendimiento general del dispositivo, así como su estabilidad durante operaciones normales.

Metodología

Se pretende utilizar la plataforma shodan.io para la exploración de dispositivos por medio de sus IP. Además, se empleará la metodología hardening para mejorar las vulnerabilidades presentadas.

1. En la plataforma se ingresarán las IP de dispositivos tales como routers, módems, entre otros. Esta herramienta nos ayudará a tener información general, de red, tecnologías y vulnerabilidades en diversos términos incluyendo el SO.
2. Al obtener los resultados, nos enfocaremos en lo que concierne los SO.
3. Aplicaremos reforzamiento de las vulnerabilidades observadas por medio de hardening para los SO que nos conciernen.
4. Crearemos estadísticas partiendo de la información obtenida.
5. Agregaremos estadísticas y resultados al informe final donde se detallará todo.

Diseño de Experimentos

Objetivos del experimento

- Evaluar el impacto del hardening
- Comparar configuraciones

Variables

Variables independientes

- Configuración del sistema operativo (predeterminada vs. hardening).
- Desactivación de dispositivos externos (USB, ópticos).

Variables dependientes

- Tiempo de arranque del sistema operativo.
- Eficiencia del sistema de archivos (velocidad de acceso y procesamiento).
- Estabilidad del sistema durante operaciones normales.

Métodos

1. Selección de dispositivos
2. Configuraciones iniciales (configuración predeterminada)
3. Implementación de Hardening
    a. Desactivar funciones innecesarias.
    b. Restringir inicio desde unidades externas.

Procedimiento experimental

1. Medir el tiempo de arranque y la eficiencia del sistema operativo con la configuración predeterminada.
2. Implementar las medidas de seguridad definidas en la metodología.
3. Repetir las mediciones de tiempo de arranque y eficiencia del sistema operativo tras aplicar el hardening.

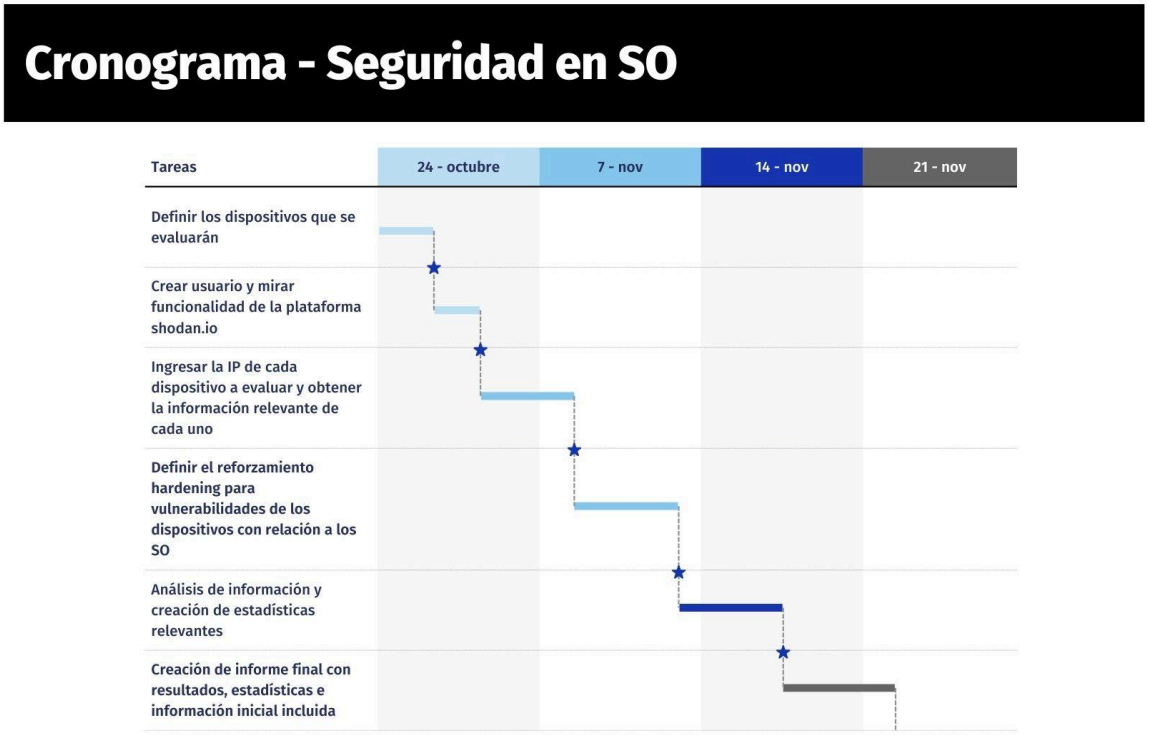
Análisis estadístico

- Utilizar análisis de varianza (ANOVA) para comparar los resultados antes y después del proceso de hardening.
- Evaluar las estadísticas de los cambios observados en el rendimiento.

Resultados esperados

Se espera que las medidas de hardening no solo mejoren la seguridad, sino que también mantengan o incluso optimicen el rendimiento del sistema operativo, aunque al principio se pueda pensar que el tiempo de arranque aumentará debido a las nuevas restricciones.

Cronograma



Referencias

[1] https://www.khoury.northeastern.edu/home/noubir/publications-local/GN2021.pdf

[2]https://pubs.aip.org/aip/acp/article-abstract/2802/1/090004/3126652/Cyber-security-study-of-Amazon-Echo-in-home-and?redirectedFrom=fulltext

[3]https://www.ciso.inc/blog-posts/the-surveillance-invasion-iot-and-smart-devices-stealing-corporate-secrets/

[4] https://red8.com/iot-security-issues-how-devices-like-alexa-challenge-networks/

[5] https://www.cloudflare.com/learning/security/glossary/iot-security/

[6]https://ovic.vic.gov.au/privacy/resources-for-organisations/internet-of-things-and-privacy-issues-and-challenges/

TIPS TECNOLÓGICOS, DE CONFIGURACIÓN Y NEGOCIO QUE COMPLEMENTAN TU SEGURIDAD

Choi, S. K., Yang, C. H., & Kwak, J. (2018). System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats. *KSII Transactions on Internet and Information Systems (TIIS)*, *12*(2), 906-918.

Kelly, C., Pitropakis, N., McKeown, S., & Lambrinoudakis, C. (2020, June). Testing and hardening IOT devices against the Mirai botnet. In *2020 international conference on cyber security and protection of digital services (cyber security)* (pp. 1-8). IEEE.