Facultad de Ingeniería en Electricidad y Computación

Genesis Encalada
genmaenc@espol.edu.ec

Miguel Neira
migannei@espol.edu.ec

Solución de Seguridad mediante PENTEST en aplicaciones IoT, usando herramientas Open Source, para un sistema de agricultura de precisión en ambiente simulado

PROBLEMA

Las empresas de agricultura que han desarrollado tecnología IoT para implementar a sus cultivos con agricultura de precisión, dan más valor a los aplicativos funcionales y eficientes, sin medir minuciosamente la seguridad de los mismos.

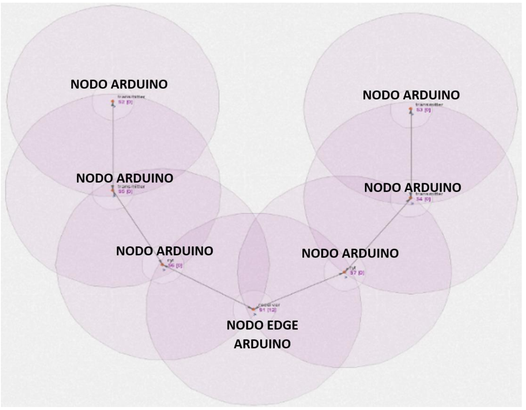


Figura 1. Simulación del Problema

OBJETIVO GENERAL

Evaluar la seguridad de un sistema de agricultura de precisión simulado a través de pentests usando herramientas Open Source para la determinación de las brechas de vulnerabilidad existentes.

.

PROPUESTA

Se estableció un escenario base, tomando en cuenta las condiciones de campo, en donde no hay señal de internet ni telefónica, por este motivo los nodos que recolectan información se comunican entre ellos por radiofrecuencia, y únicamente un nodo, llamado nodo Gateway es quien sube esta información a la nube para ser procesada.

En base a lo mencionado, es que se crean tres tipos de pruebas, en donde se realizan ataques al nodo Gateway, implementado con una tarjeta electrónica Arduino, y conectado a internet tanto de forma inalámbrica como directa, para comparar resultados.

Las tres pruebas fueron: DoS o denegación de servicio, MitM u hombre en medio y Suplantación de DNS, todas tres fueron realizadas desde una computadora que alojaba el sistema operativo de Kali Linux, que tiene el rol de atacar al nodo Gateway.

La finalidad de las pruebas es encontrar si existen vulnerabilidad, y si es así, explotarlas, para poder dar una retroalimentación de mejora del sistema

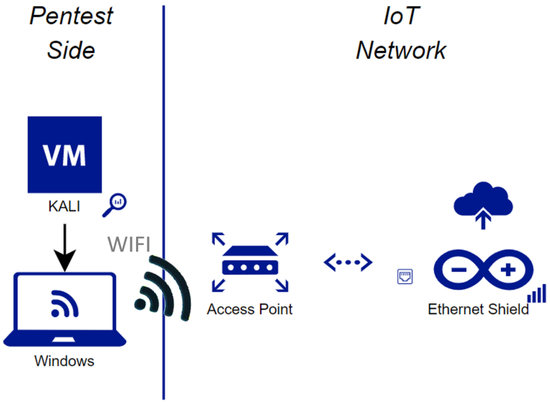
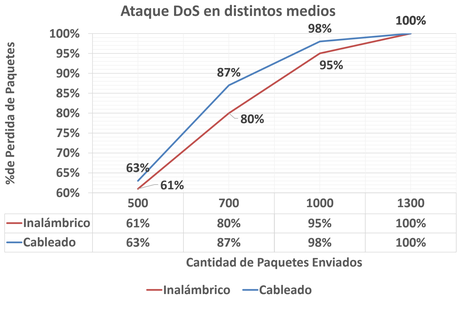


Figura 2. Esquema de las pruebas

RESULTADOS

En la denegación de servicio se comprobó que si se realiza por medios cableados el sistema cae como media un 8% más rápido que si fuera inalámbricamente usando la misma cantidad y tamaño de paquetes.



	500	700	1000	1300
Inalámbrico	61%	80%	95%	100%
Cableado	63%	87%	98%	100%

Figura 3. Gráfico comparativo entre medios de ataque del DoS

Tanto en el ataque MitM y Suplantación de DNS se logro interceptar las comunicación y alterar la dirección DNS que alojaba la pagina donde se mostraba las transmisiones, vulnerabilidades que pudieron evitarse con cierre de puertos y encriptación de datos.

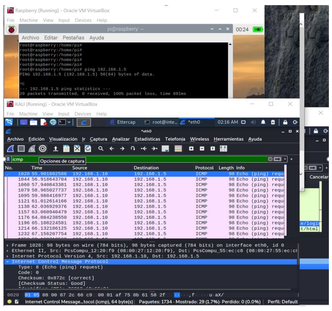


Figura 4. Paquetes capturados de la trasmisión del Nodo Gateway

CONCLUSIONES

- Después de realizar la prueba de DoS en la capa de Edge por medio alámbrico, se observó que, al aumentar la tasa de paquetes enviados, el sistema llega a colapsar de manera proporcional, lo que provoca indisponibilidad en el servidor, de aproximadamente 2 minutos
- Los ataques de MitM y Suplantación DNS, afectan a la integridad de los datos. En el caso de MitM, mantiene una escucha pasiva aprovechando la falta de seguridad del protocolo HTTP obteniendo los datos de navegación a la vez de escuchar la transmisión del nodo con los datos recolectados de la agricultura de precisión.