Hacking ético para IoT: problemas de seguridad, desafíos, soluciones y recomendaciones

Cristhian Soto
Ingeniería de Sistemas
Universidad San Buenaventura
Cali, Colombia

***Abstract*—El artículo aborda los crecientes desafíos de seguridad en el Internet de las Cosas (IoT), con un enfoque en el hacking ético como una estrategia para evaluar y mejorar la seguridad de los dispositivos, servidores y aplicaciones de IoT. Se destaca la necesidad de pruebas periódicas de penetración y simulaciones éticas para abordar las vulnerabilidades en diferentes niveles. El trabajo se basa en métodos y herramientas de piratería ética para proporcionar soluciones prácticas y recomienda el uso de aprendizaje automático para fortalecer la detección temprana de vulnerabilidades.**

I. Introducción

La revolución digital ha dado lugar a la aparición de tecnologías disruptivas que transforman fundamentalmente la manera en que interactuamos con el mundo que nos rodea. En este contexto, el Internet de las Cosas (IoT) emerge como una pieza clave, desencadenando una red interconectada de dispositivos, sensores y sistemas ciberfísicos que colaboran para recolectar, intercambiar y utilizar datos de manera inteligente. Esta nueva era tecnológica no solo impulsa la conectividad a niveles sin precedentes, sino que también redefine la forma en que concebimos y utilizamos la información.

Los sistemas de IoT, en esencia, abarcan una diversidad de entornos, desde dispositivos domésticos inteligentes hasta aplicaciones industriales avanzadas. Estos sistemas ciberfísicos combinan la ingeniería informática con la física, permitiendo la interacción directa entre el mundo digital y el mundo físico. A través de la integración de sensores sofisticados y dispositivos conectados, los sistemas de IoT tienen el potencial de optimizar procesos, mejorar la toma de decisiones y ofrecer soluciones innovadoras en diversos sectores.

Sin embargo, este panorama tecnológico no está exento de desafíos significativos. La interconexión masiva de dispositivos también expone estos sistemas a amenazas cibernéticas potenciales. La seguridad de los sistemas de IoT se convierte así en una prioridad crucial, ya que la vulnerabilidad de estos dispositivos puede tener consecuencias directas en la privacidad, la integridad de los datos y, en algunos casos, la seguridad física.

En este sentido, comprender a fondo los aspectos relacionados con la ciberseguridad en sistemas de IoT se vuelve imperativo. Desde la identificación y mitigación de vulnerabilidades hasta la aplicación de medidas especializadas para preservar la integridad de estos sistemas, la seguridad cibernética se erige como un pilar fundamental para el desarrollo sostenible y seguro de la era del Internet de las Cosas. Este artículo explora los desafíos y las soluciones en el ámbito de la ciberseguridad, destacando la necesidad de abordar estos aspectos críticos en la evolución constante de los sistemas de IoT y sistemas ciberfísicos.

La presente síntesis explora de manera exhaustiva diversos aspectos cruciales vinculados a la ciberseguridad y la guerra cibernética, abordando un espectro amplio de temas de relevancia contemporánea.La obra proporciona una panorámica completa y detallada de diversos aspectos relevantes de la ciberseguridad y la guerra cibernética, consolidando una comprensión integral de estos fenómenos contemporáneos.

Además, la síntesis abordará las ideas principales del artículo, como las principales diferencias entre el hacking ético y las pruebas de penetración y como estas se han convertido en un elemento necesario para poder identificar los posibles fallos o violaciones de seguridad que tiene los sitemas loT, y como estas a su vez en su proceso de verificación pueden aportar soluciones o maneras de compensar o fortaleces los sitemas de defensa de loT.

II. Importancia de los sistemas IoT (Internet de las Cosas)

A. Contexto y visión General de IoT

Esta sección, el texto proporciona una visión integral de dos temas cruciales: el Internet de las Cosas (IoT) y la ciberseguridad, específicamente el hacking ético. Se incia con la exploración en el auge de los dispositivos y dominios IoT, destacando la necesidad de mejoras en aspectos como el rango inalámbrico, rendimiento y facilidad de uso. Se plantea la posibilidad evolutiva de IoT 2.0 como la ”Inteligencia de las Cosas”.

Luego, se introduce y explica el hacking ético y las pruebas de penetración, detallando cómo estas prácticas contribuyen a evaluar y fortalecer la seguridad de los sistemas, cabe mencionar que el texto hace énfasis en la diferencia de ambos términos, ya que se acostumbran a confundirse, por un lado, el hacking ético hace referencia a aquellos ataques simulados los cuales tienen por objetivo identificar los fallos y vulnerabilidades de seguridad del sistema y asi mismo, brindar unos mecanismos para protegerlo ante cualquier posible brecha, por otro lado, las pruebas de penetración al ser un aspecto del hacking ético, tiene un eje central mas enfocado en verificar la seguridad como la portección de los sistemas de defensa de loT.

En ese orden de ideas, tambien se examina la arquitectura avanzada de prueba para sistemas IoT, con aplicaciones específicas en campos como la salud, la industria y lo militar. También se presenta el concepto de ”Internet de las Cosas Éticas” (IoEHT) o Hacking Ético para IoT (EHIoT).

El Hacking Ético se emplea con el propósito de evaluar la seguridad de los sistemas IoT y detectar posibles vulnerabilidades. Además, se exploran medidas de seguridad adaptadas a distintos tipos de sistemas IoT, como los sistemas de hogar inteligente, donde se pueden implementar soluciones específicas, como la autenticación de dos factores y el cifrado de extremo a extremo, con el fin de asegurar la protección de los datos.

La sección plantea las vulnerabilidades comunes en sistemas IoT y se exponen las herramientas especializadas de pruebas de penetración diseñadas para abordar estos desafíos. Además, clasifica a los hackers según sus objetivos, explorando motivaciones políticas, patrióticas, religiosas y racistas que impulsan los ataques IoT.

Finalmente, se analizan las ganancias del hacking, abordando aspectos económicos, financieros, personales y políticos para los hackers y como estos tiene así una relacioón e impacto en organizaciones y en la economía en general. La sección ofrece una perspectiva completa y aplicada de los desafíos de IoT y las medidas de ciberseguridad, incorporando ejemplos prácticos y aplicaciones en diferentes dominios.

B. Vulnerabilidades comunes en dispositivos IoT

Para este apartado, se mencionan diversas vulnerabilidades que podrían ser aprovechadas por atacantes para comprometer la seguridad del sistema. Entre las vulnerabilidades más destacadas se encuentran:

Falta de actualizaciones de seguridad: Muchos dispositivos IoT carecen de actualizaciones de seguridad periódicas, lo que implica que las vulnerabilidades descubiertas no se abordan. Esta ausencia de actualizaciones deja a los dispositivos expuestos y facilita que los atacantes aprovechen estas debilidades en la seguridad.

Contraseña débil o predeterminada: Hace referencia a aquella vulnerabilidad común que radica en el uso de contraseñas débiles o predeterminadas en muchos dispositivos IoT. Estos dispositivos a menudo se distribuyen con contraseñas predeterminadas o permiten contraseñas débiles predefinidas, facilitando a los atacantes obtener acceso no autorizado. Además, la falta de cambio de contraseña por parte de los usuarios incrementa aún más el riesgo de brechas de seguridad.

Comunicación no segura: Como consecuencia de la carencia de mecanismos de seguridad en la comunicación entre dispositivos IoT y otros sistemas puede dar lugar a la interceptación y manipulación de datos. Esta situación compromete la integridad y seguridad de la información transmitida, poniendo en riesgo la privacidad del usuario.

Protección de privacidad deficiente: En algunos dispositivos IoT recopilan grandes cantidades de datos personales, como información de ubicación, hábitos de consumo y preferencias personales. La falta de una adecuada protección de estos datos puede resultar en violaciones de privacidad y en el mal uso de la información personal de los usuarios.

Estas vulnerabilidades expuetas suponen serias implicaciones para la seguridad y privacidad. Un atacante podría aprovechar estas debilidades para obtener acceso a información confidencial, alterar el comportamiento del dispositivo, llevar a cabo ataques de denegación de servicio o conseguir acceso no autorizado a los sistemas conectados. La conciencia y abordaje de estas vulnerabilidades son esenciales para mitigar los riesgos asociados con los dispositivos IoT y garantizar un entorno de uso seguro y protegido.

C. Prácticas de seguridad óptimas en IoT

Teniendo en cuenta los desafíos y las amenazas de seguridad inherentes a los sistemas IoT, resulta necesario implementar soluciones y llevar a cabo mejoras de seguridad en estos dispositivos. De ese modo, a continuacion se exponen algunas soluciones y recomendaciones destacadas:

Establecimiento de estándares de seguridad: Es fundamental desarrollar estándares sólidos de seguridad para los dispositivos IoT. Estos estándares abordarán aspectos cruciales como la autenticación, el cifrado de datos, la gestión de claves y la salvaguarda de la privacidad. Estas directrices contribuirán significativamente a asegurar la integridad y la interoperabilidad de los dispositivos IoT.

Actualizaciones de seguridad periódicas: Los fabricantes deben proporcionar actualizaciones regulares de seguridad para sus dispositivos IoT, incluyendo parches para abordar vulnerabilidades conocidas. Además, es esencial concientizar a los usuarios sobre la importancia de aplicar estas actualizaciones para resguardar efectivamente sus dispositivos.

Autenticación y autorización sólidas: La implementación de sólidos mecanismos de autorización y autenticación es esencial en los dispositivos IoT. Esto implica la utilización de contraseñas robustas, autenticación de dos factores y certificados digitales para asegurar que solo los usuarios autorizados puedan acceder y controlar los dispositivos.

Cifrado de datos: Para brindar garantía de la integridad de la seguridad de los datos transmitidos entre dispositivos y servidores de IoT, el cifrado adecuado toma un papel de vital importancia. Por ello, Se deben emplear algoritmos de encriptación fuertes, asegurando la protección de los datos tanto en el almacenamiento como durante la transmisión.

Seguridad de red: La implementación de medidas de seguridad en la red es esencial para proteger los dispositivos IoT. Esto abarca el uso de firewalls, detección de intrusos y segmentación de la red con el objetivo de prevenir el acceso no autorizado y limitar el impacto de posibles ataques.

Educación y conciencia: La educación y concientización desempeñan un papel clave en el mantenimiento de la seguridad en los sistemas IoT. Los usuarios deben recibir información sobre las mejores prácticas de seguridad, tales como la relevancia de cambiar contraseñas predeterminadas, evitar la descarga de aplicaciones o software no confiables y estar alerta ante posibles amenazas.

Estas soluciones y recomendaciones representan solo algunas de las medidas que pueden implementarse para fortalecer la seguridad de los sistemas IoT. Es esencial que fabricantes, usuarios y organizaciones colaboren estrechamente para ase-

gurar la protección de estos dispositivos y reducir los riesgos asociados con los ciberataques en el entorno de IoT.

III. Ciberataques dirigidos al IoT

En esta sección se exponen diversos tipos de ciberataques dirigidos a sistemas de IoT (Internet de las cosas). La clasificación de los ataques variará según sus objetivos, como la red, el firmware, los usuarios/personal, el dispositivo o la aplicación. Se resalta que los ciberataques contra IoT son diversos y no se limitan a un solo aspecto o clasificación. El artículo cubre tipos de ciberataques en tres categorías principales: ataques web, ataques de aplicaciones y ataques de red.

Ataques Web:

- Secuestro de Cookies: Robar cookies de autenticación de usuarios.
- Ataques basados en CoAP: Dirigidos al Protocolo de Aplicación Constricta con varios tipos de ataques.
- Ataques basados en DTLS: Explotar vulnerabilidades del protocolo Datagram Transport Layer Security.
- Secuestro de Sesiones: Acceso no autorizado a sesiones de información de dispositivos IoT.
- Ataques de Falsificación: Obtener acceso no autorizado utilizando una identidad de red falsa.
- Desbordamiento de Búfer: Sobrepasar el límite de un búfer para provocar anomalías en el programa.
- Suplantación de Sitios Web: Crear sitios web falsos para engañar a los usuarios.
- Ataques de Inyección de Código Malicioso: Explotar aplicaciones web mal configuradas para usuarios de IoT.
- Ataques de Inyección de SQL: Manipulación de bases de datos SQL a través de diversos métodos de inyección.
- Cross-Site Scripting (XSS): Explotar vulnerabilidades de aplicaciones web mediante la inyección de código.
- Cross-Site Request Forgery (CSRF): Explotar la falta de autorización en aplicaciones web.

Ataques de Aplicaciones:

- Scareware: Utilizar el miedo para engañar a los usuarios y que descarguen/software peligroso.
- Spyware: Monitorización encubierta del comportamiento en línea/fuera de línea de las víctimas sin su conocimiento.
- Troyanos: Software malicioso que se disfraza como software legítimo para obtener acceso no autorizado.
- Botnets: Explotar dispositivos IoT para lanzar varios ataques, como DDoS.
- Virus: Propagación de host a host, ya sea mediante interacción humana o sin ella.
- Rootkit: Obtener acceso remoto de nivel administrador mediante la explotación de vulnerabilidades.

Ataques de Red:

- Espionaje: Intercepción pasiva de la comunicación para robar información.
- Reproducción: Transmitir repetidamente la comunicación segura interceptada.
- Hombre en el Medio (MITM): Interceptar y alterar activamente las comunicaciones entre dos partes.
- Captura de Paquetes: Capturar tráfico para leer datos no cifrados.
- Cracking de Contraseñas: Romper contraseñas para obtener acceso a sistemas.
- Análisis de Tráfico: Interceptar y examinar el tráfico de red para obtener información.
- Interferencia Inalámbrica: Comprometer entornos inalámbricos bloqueando tráfico legítimo.
- Agujero Negro: Ataque de eliminación de paquetes en un ataque de denegación de servicio.
- Ataques Bizantinos: Control malicioso de dispositivos autenticados para interrumpir servicios de red.
- DoS/DDoS: Impedir que usuarios legítimos accedan a servicios mediante solicitudes excesivas.

La sección también discute la ciberactividad contra IoT, incluyendo ciberdelitos, ciberespionaje, ciberterrorismo y ciberwarfare. Se resaltan las vulnerabilidades de diferentes sectores, como organizaciones, bancos, empresas, gobiernos, hospitales y sitios web militares, frente a diversas amenazas cibernéticas.

IV. EVENTOS REALES RELACIONADOS CON IOT

En esta sección, se explican los eventos de seguridad en tiempo real que ocurrieron contra servidores, pasarelas y dispositivos finales de IoT, incluyendo vulnerabilidades y explotación de bases de datos reales, junto con eventos reales de ciberataques. Además, se distinguen algunas posibles medidas de seguridad. Aquí hay un resumen de la sección "REAL-CASE IOT-RELATED EVENTS":

A. Explotación de Vulnerabilidades en Casos Reales

Incidente de Adobe Flash (2013, 2015): Brecha de seguridad en Adobe en 2013, con ataques a Adobe Flash en 2015. Vulnerabilidades explotadas: CVE2015-5119, CVE-2015-5122 y CVE-2015-5123.

Incidente de Brecha de Datos de Equifax (marzo de 2017): Vulnerabilidad no parcheada en Apache Struts (CVE2017-5638) en servidores web de Equifax. Destaca la importancia del enfoque de confianza cero para la Gestión de Acceso Privilegiado (PAM). Brecha comprometió información de 143 millones de consumidores, costando alrededor de $3 mil millones.

Incidentes de Exploits de CVE Variants: Ataques a Microsoft Exchange Server en 2020 (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065). Inyección de códigos maliciosos en recursos del servicio Exchange Offline Address Book.

Incidentes de Exploits Específicos (CVE-2020-1472, CVE-2020-0688, 05-2022-0438.doc): Vulnerabilidades críticas de Microsoft explotadas para escalada de privilegios y ejecución de código. Destacan la importancia de actualizaciones de seguridad y detección temprana.

Tendencia de Aumento de Ataques:

Según el informe de CISCO de 2021, aumentaron los ataques de (Spear) Phishing en un 40% y los ataques de ransomware en un 48%.

B. Evaluación de Vulnerabilidades

Vulnerabilidades en Sistemas IoT no Probados: Los sistemas no probados son más vulnerables a ataques, destacando la importancia de evaluar las vulnerabilidades.

Herramientas de Evaluación de Vulnerabilidades: Diversas herramientas, como las de Penetration Testing (VAPT), son esenciales para evaluar vulnerabilidades y realizar pruebas éticas.

Categorías de Vulnerabilidades:

Vulnerabilidades de Seguridad de TI (ITSec):

- Falta de mecanismos de control de acceso.
- Aplicaciones de terceros no confiables.
- Programas de puerta trasera.

Vulnerabilidades Técnicas y Operativas:

- Privilegios del sistema.
- Dispositivos con recursos limitados.
- Software de proveedores sin consideraciones de seguridad.
- Falta de evaluación de aplicaciones.

Vulnerabilidades de Hardware:

- Falta de protección física para componentes.
- Equipos frágiles y no resistentes a manipulaciones.
- Otros Factores de Vulnerabilidad:

Falta de habilidades de TI.

- Accidentes, ya sean intencionales o no.
- Falta de entrenamiento CERT.

La sección expone eventos reales de explotación de vulnerabilidades en IoT, se realiza hincapié en la importancia de la evaluación de vulnerabilidades y presenta categorías clave de vulnerabilidades en sistemas IoT, desde problemas de software hasta desafíos operativos y de hardware.

V. Hacking Ético

A. Ciclo de Vida del Hacking Ético

Reconocimiento:

Descripción: Se utilizan procesos y técnicas para recopilar información sobre sistemas, usuarios, servidores, dispositivos, etc., mediante el mapeo de redes, ya sea de manera encubierta o deliberada.

Objetivo Ético: Obtener detalles relacionados con el IoT, como Wi-Fi, tipos de dispositivos conectados, software, hardware y sistema operativo.

Exploración (Scanning):

Descripción: Busca brechas o vulnerabilidades de seguridad en el IoT, como puertos abiertos o no utilizados, hosts activos, configuraciones inseguras en firewalls, sistemas de detección/prevención de intrusiones (IDS/IPS), routers y switches.

Objetivo Ético: Identificar posibles brechas de seguridad que podrían ser explotadas. Obtención de Acceso:

Descripción: Simula el acceso no autorizado a un sistema IoT mediante herramientas y técnicas de prueba de penetración.

Objetivo Ético: Probar la autorización o autenticación del sistema sin causar daño real.

Mantenimiento de Acceso:

Descripción: Después de obtener acceso, se pueden explotar los recursos del sistema para buscar otros dispositivos vulnerables.

Objetivo Ético: Evaluar la resistencia del sistema a ataques adicionales y buscar dispositivos comúnmente vulnerables.

Informes de Seguridad:

Descripción: Después de completar las fases anteriores, se presenta un informe de seguridad que destaca las vulnerabilidades, cómo fueron explotadas o podrían serlo, y se sugieren métodos de evaluación de riesgos y vulnerabilidades. Objetivo Ético: Mejorar las medidas de seguridad y reducir el riesgo de exposición a ciberataques.

B. Herramientas de Hacking Ético

Se utilizan diversas herramientas para realizar pruebas éticas de hacking en sistemas IoT, clasificadas en cuatro categorías principales:

Basadas en Web: Escanean aplicaciones y servidores web. Basadas en la Nube: Realizan seguimiento de ataques y supervisan el rendimiento en entornos en la nube. Basadas en Red: Monitorean y escanean redes IoT en busca de vulnerabilidades y prueban la fuerza de contraseñas/encriptación. Basadas en Aplicaciones: Evalúan el nivel de seguridad de las aplicaciones IoT y recuperan artefactos en caso de ataques.

C. Desafíos del Hacking Ético

Se identifican varios desafíos en el ámbito del hacking ético:

Desafíos de Capacidad y Habilidad: La falta de experiencia y habilidades en los equipos de hacking ético, con diferencias significativas entre los equipos.

Desafíos de Costo: La ejecución de pruebas de penetración puede ser costosa, desde la identificación de vulnerabilidades hasta la implementación de medidas de seguridad adicionales.

Desafíos Legales: La necesidad de cumplir con acuerdos legales, como acuerdos de no divulgación (NDA), para evitar procesamientos legales.

Desafíos de Conocimiento: Dificultad para detectar nuevos tipos de ataques, como ataques de día cero, y para manejar malware polimórfico y servicios de cifrado en constante cambio.

D. Problemas del Hacking Ético

Además de los desafíos, se identifican problemas adicionales asociados con el hacking ético, como problemas de privacidad, seguridad, confianza, legales, forenses, presupuestarios y de compatibilidad. Estos problemas resaltan la complejidad y la necesidad de abordar múltiples aspectos éticos, legales y técnicos al realizar pruebas de seguridad éticas, especialmente en el entorno del IoT.

VI. Prueba de Penetración

A. Conexión entre Prueba de Penetración y Hackers Éticos

Descripción: La prueba de penetración requiere la presencia de hackers éticos de manera certificada y profesional para garantizar la seguridad tanto de ellos como de la organización en el dominio del IoT.

Objetivo Ético: Evaluar los niveles de seguridad e inmunidad de sistemas de información y no informáticos, así como del personal, contra posibles vulnerabilidades explotables.

B. Herramientas de Prueba de Penetración

Descripción: Se utilizan diferentes herramientas para llevar a cabo pruebas de penetración efectivas en el IoT. Estas herramientas se presentan y comparan en la tabla IX.

Objetivo Ético: Garantizar pruebas efectivas y exitosas mediante el uso de herramientas específicas.

C. Tipos de Conocimiento en Prueba de Penetración

1) Pruebas de Caja Blanca (White-Box Testing):: Descripción: Se basa en un conocimiento completo del sistema IoT y sus componentes de software y firmware. Menos tiempo consumido debido al conocimiento previo.

Objetivo Ético: Verificar decisiones lógicas, realizar comprobaciones de sintaxis y probar algoritmos.

2) Pruebas de Caja Gris (Grey-Box Testing):: Descripción: Se basa en un conocimiento parcial del sistema IoT y su programación interna. Menos intrusivo y menos riesgo de conflictos.

Objetivo Ético: Evaluar el sistema sin un conocimiento exhaustivo, no adecuado para probar algoritmos.

3) Pruebas de Caja Negra (Black-Box Testing):: Descripción: Los testers no tienen conocimiento previo del sistema IoT. Se realiza desde la perspectiva del usuario.

Objetivo Ético: Evaluar el sistema sin conocimiento interno, aunque es más tiempo consumidor y menos útil para probar algoritmos.

D. Aplicación de Pruebas de Penetración

Descripción: La prueba de penetración se aplica a diferentes dominios del IoT, como pruebas de aplicaciones, pruebas de red interna/externa y pruebas de nube.

Objetivo Ético: Identificar y prevenir posibles vulnerabilidades y ataques en aplicaciones, redes y la infraestructura en general.

E. Soluciones Existente

1) Hacking Ético:: Descripción: Se presenta como un método esencial para simular el ciclo de vida de un hacker y realizar ataques simulados contra sistemas IoT.

Objetivo Ético: Proporcionar soluciones y enfoques para la detección y prevención de amenazas basadas en técnicas éticas de hacking.

2) Prueba de Penetración:: Descripción: Es esencial para revelar vulnerabilidades y evaluar la efectividad de las medidas de seguridad adoptadas en sistemas o redes IoT.

Objetivo Ético: Ofrecer soluciones y metodologías para realizar pruebas de penetración efectivas, identificando riesgos y vulnerabilidades.

3) Evaluación de Vulnerabilidades:: Descripción: Se presentan soluciones para evaluar y evaluar amenazas en sitios web, redes, sistemas operativos/aplicaciones y dispositivos IoT mediante ataques de simulación.

Objetivo Ético: Utilizar herramientas de evaluación de vulnerabilidades para prevenir la explotación de posibles amenazas.

La sección destaca la importancia de la prueba de penetración, las herramientas utilizadas, los tipos de conocimiento involucrados y las soluciones existentes para garantizar la seguridad en entornos IoT, tanto desde la perspectiva ética como técnica.

VII. Procedimientos de Seguridad y Seguridad en IoT

A pesar de las diversas medidas preventivas y de seguridad recomendadas para el Internet de las cosas (IoT), es necesario considerar varios pasos para garantizar que las medidas de seguridad y seguridad adoptadas se apliquen y se introduzcan correctamente en el dominio del IoT. La sección destaca la importancia de los primeros respondedores a incidentes y la necesidad de clasificarlos para asegurar la respuesta adecuada ante eventos específicos. Después de esta clasificación, se deben implementar medidas de seguridad preventivas y protectoras para una mayor protección. Finalmente, estas medidas de seguridad deben mantenerse para garantizar el nivel correcto de protección, respetando los objetivos principales de seguridad.

A. Política de Seguridad de la Información

Se enfatiza la importancia de los procedimientos de seguridad y se menciona que cada empleado debe respetar y adherirse a ellos en cualquier dominio de IoT. Esto se logra a través de capacitación y conciencia continuas, manteniendo la responsabilidad individual. Se presentan varios aspectos de las políticas involucradas en este proceso:

Adopción de Estándares de Ciberseguridad para IoT: Se destaca la importancia de seguir estándares que sean compatibles con el mercado y el dominio del IoT. Ejemplos incluyen:

ETSI EN 303 645: Un estándar global para la ciberseguridad del IoT que ofrece recomendaciones y requisitos obligatorios para establecer una línea base de seguridad.

NISTIR 8259: Ofrece orientación para fabricantes y terceros que diseñan, prueban y admiten dispositivos IoT, con documentos que cubren capacidades técnicas y de soporte.

B. Respuesta ante Incidentes

En caso de un incidente, se activa automáticamente una respuesta. Los respondedores son llamados ante la ocurrencia de un evento de seguridad para responder con las medidas y

contramedidas adecuadas y mitigar cualquier ataque dirigido al dominio del IoT en tiempo real, reduciendo la ocurrencia y la probabilidad de riesgos. Las respuestas pueden ser activas, pasivas o híbridas, dependiendo de la formación, habilidades, experiencia y recursos disponibles de los respondedores, así como de los motivos y ganancias del atacante. Se pueden adoptar medidas de seguridad preventivas y protectoras, como el uso de encriptación simétrica, incluida la criptografía post-cuántica, para proteger la red, el sistema y los datos de los usuarios de IoT.

VIII. Lecciones Aprendidas

Se destacan varias lecciones aprendidas:

Soluciones de Seguridad Estándar: Se requieren soluciones de seguridad estándar y se deben aplicar medidas de seguridad (contra) más especializadas, ya que las vulnerabilidades difieren entre dispositivos, sistemas o protocolos de IoT debido a su naturaleza heterogénea.

Entrenamiento Continuo de Seguridad/Conciencia: Se recomienda el entrenamiento continuo de seguridad y concienciа, especialmente en la adopción de pautas de seguridad especializadas, dependiendo de las capas de IoT, sistemas, dispositivos, etc., así como la realización de seminarios y sesiones de capacitación para mantener a los usuarios informados y actualizados.

Diseños de Seguridad Mejorados: Son esenciales antes de su implementación y adopción utilizando herramientas de hacking ético y pruebas de penetración para IoT, que pueden construirse sobre soluciones de inteligencia artificial (IA) basadas en aprendizaje automático (ML) para garantizar una mayor precisión y reducir falsos positivos y negativos con un tiempo de respuesta menor.

Más Inversión: Se necesita más inversión en este dominio, lo que requiere un presupuesto más alto para aumentar la conciencia, capacitar al personal uniforme/no uniforme, afirmar la responsabilidad y la rendición de cuentas, así como para capacitar a más hackers éticos y probadores de penetración.

Autorización Legal: Las leyes deben proteger y respaldar a los hackers éticos durante sus ataques simulados, donde se deben establecer acuerdos previos y posteriores para mantener legalmente su seguridad.

Conocimiento Forense: Se requiere más conocimiento y experiencia en forense para realizar pruebas de penetración más efectivas y eficientes.

IX. Direcciones Futuras de Investigación

Aunque se ha avanzado mucho en la seguridad de los sistemas IoT en los últimos años, aún existen varios desafíos. La seguridad, la seguridad y la privacidad siguen siendo un desafío serio, ya que un atacante puede explotar maliciosamente estos dispositivos finales de IoT. Se presentan varias direcciones de investigación futura para mejorar las pruebas de penetración en sistemas IoT:

Habilitar Soluciones Basadas en IA: Especialmente porque la IA juega un papel clave para habilitar soluciones innovadoras de pruebas de penetración y hacking ético.

Habilitar Soluciones de PT Automatizadas Inteligentes: Que deben habilitarse de manera efectiva en tiempo real para lograr las funcionalidades necesarias de las entidades y requisitos de aplicación de IoT.

Soluciones Correctivas Mejoradas para IoT: Deben mantenerse para ”corregir” y superar las vulnerabilidades de seguridad de IoT detectadas.

X. Sugerencias y Recomendaciones

A pesar de tener diferentes medidas de seguridad IoT disponibles, se presentan varias sugerencias y recomendaciones para apoyar el ámbito del hacking ético y mejorar las pruebas de penetración para sistemas IoT:

Mantener la Privacidad: Respetar la privacidad, especialmente de los usuarios y empresas de IoT durante la realización de procesos éticos de hacking y pruebas de penetración.

Autenticación Multifactorial: Debe adoptarse para prevenir el acceso no autorizado o el uso legal abusivo de sistemas o dispositivos IoT.

Mecanismos de Seguridad Ligeros: Se pueden aplicar a dispositivos de IoT con recursos limitados para garantizar su protección contra eventos maliciosos.

Policies Reforzadas: La adopción de políticas de identificación, autorización y autenticación evita que entidades/usuarios no autorizados accedan a sistemas IoT.

Aislamiento en Tiempo Real: Implementar mecanismos de seguridad/salvaguardia proactivos y en tiempo real que desconecten instantáneamente o apaguen forzosamente cualquier dispositivo IoT comprometido ante una amenaza de seguridad detectada.

Diseños de IoT más Seguros: Todos los sistemas, aplicaciones, sistemas operativos y dispositivos finales de IoT deben someterse a una prueba de verificación de seguridad antes y después de alcanzar el diseño requerido.

Cubrir Brechas de Habilidades: Se necesita más publicidad y campañas de reclutamiento para alentar y educar a más personas para unirse al ámbito del hacking ético.

Entrenamiento Especializado: Especialmente el entrenamiento en seguridad debe asignarse para cada categoría de personal/empleados para superar y abordar diferentes tipos de ataques que podrían encontrar en sus campos.

Intercambio Internacional y Competencias: Se necesitan para mejorar la experiencia y habilidades que se pueden adquirir a través de desafíos de juegos, junto con el establecimiento de nuevos fundamentos para que los hackers éticos (potenciales) sigan.

Inteligencia de Amenazas Cibernéticas: Debería considerarse como un medio para mitigar principalmente las amenazas externas (e internas) mediante el enfoque en el conocimiento, la experiencia y las habilidades adquiridas en ataques previos.

XI. Conclusiones

En este documento, se destaca y se discute exhaustivamente la importancia de realizar pruebas de penetración en sistemas IoT y la dependencia de hackers éticos confiables para realizar ataques simulados. Esto permite evaluar el nivel de seguridad

contra amenazas y ataques comunes de IoT y proporciona una mejor comprensión de la evaluación, evaluación y mitigación de cualquier riesgo dado contra el dominio de IoT, incluidas opciones para detectar, parchar y actualizar sistemas IoT. Además, se resaltan las diferencias clave entre el hacking y el hacking ético en sistemas IoT, y se describen las operaciones de los hackers según sus objetivos, metas, motivos y beneficios. Se presentan varias taxonomías y marcos como una visión general del dominio del hacking en general, comunes con el dominio del IoT. Finalmente, se proponen muchas recomendaciones y sugerencias para capacitar aún más a los empleados, personal de TI y personal de seguridad, además de ideas sobre el trabajo futuro para proteger los sistemas IoT mediante soluciones automatizadas inteligentes de hacking ético y pruebas de penetración.

La seguridad en IoT es un desafío dinámico y en constante evolución que requiere enfoques proactivos y soluciones innovadoras. Al adoptar prácticas de hacking ético, pruebas de penetración avanzadas y tecnologías emergentes, podemos fortalecer la resiliencia de los sistemas IoT y garantizar un futuro más seguro en la era de la conectividad inteligente.

REFERENCES

[1] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," Internet Things Cyber-Physical Syst., vol. 3, pp. 280–308, Jan. 2023, doi: 10.1016/j.iotcps.2023.04.002.

[2] Jean-Paul A Yaacoub, Hassan N Noura, Ola Salman, and Ali Chehab. Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. International Journal of Information Security, pages 1–44, 2021.

[3]] Jean-Paul A Yaacoub, Hassan N Noura, Ola Salman, and Ali Chehab. Advanced digital forensics and anti-digital forensics for iot systems: Techniques, limitations and recommendations. Internet of Things, page 100544, 2022.

[4] Dorothy E Denning. Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. Networks and netwars: The future of terror, crime, and militancy, 239:288, 2001.