Pentesting en la Industria 5.0: Metodología y Tecnologías

Cristina Alcaraz
Departamento de Lenguajes y Ciencias de la Computación
Universidad de Málaga, Spain
alcaraz@uma.es

José J. Sánchez
Departamento de Lenguajes y Ciencias de la Computación
Universidad de Málaga, Spain
sanchezg@uma.es

Javier López
Departamento de Lenguajes y Ciencias de la Computación
Universidad de Málaga, Spain
javierlopez@uma.es

***Resumen*—Se puede observar cada vez más cómo las nuevas tecnologías se adaptan a los ecosistemas industriales para ir modernizando los procesos operativos, y en función de los nuevos paradigmas, ajustarse a las condiciones establecidas. En el caso de la Industria 5.0, estas condiciones están reguladas por tres objetivos prioritarios: la centralidad del humano, la sostenibilidad y la resiliencia. Cualquier violación de estas condiciones supone un daño directo a la Industria 5.0, y a su correcto funcionamiento. Para evitar este problema, las acciones de *pentesting* son claves para prevenir situaciones, sin embargo, las metodologías existentes carecen de capacidades para recoger todas las condiciones de la Industria 5.0, por lo que se hace también imprescindible proponer una nueva metodología que adapte las metodologías clásicas con las nuevas condiciones. Por esta razón, este artículo presenta la metodología *Pentesting 5.0*, y hace una revisión de los requisitos que se deben tener en cuenta a la hora desplegar futuras plataformas con apoyo en las nuevas tecnologías, haciendo, además, una revisión de las ventajas y desventajas que estas pueden tener en el proceso.**

***Index Terms*—Pentesting, Industria 5.0, ciberseguridad**

Tipo de contribución: *Investigación original*

I. Introducción

El *pentesting* proviene de la terminología inglesa *penetration testing*, test de penetración, que hace referencia a la práctica de realizar distintas pruebas y ataques controlados a un sistema, con la intención de identificar las distintas vulnerabilidades existentes en el mismo, así como la explotación de éstas, buscando explorar, de forma controlada, el alcance de un ataque real derivado de la explotación de las mismas. Esta práctica es llevada a cabo por un profesional o conjunto de ellos, los *pentester* o auditores, aumentando de forma considerable la resistencia a posibles ciberataques de un sistema en particular, al actuar desde el punto de vista del posible atacante, permitiendo identificar las posibles vías de entrada y vulnerabilidades que éste podría explotar.

El *pentesting*, a pesar de su apariencia relativamente moderna, tiene sus orígenes durante el siglo pasado [1], con los *tiger teams* del departamento de defensa de los Estados Unidos. Hasta la actualidad, esta práctica se ha extendido, siendo prácticamente obligatoria su realización como base para asegurar la ciberseguridad en los distintos sistemas informáticos conectados a Internet. Son muchos los *frameworks* de *pentesting* existentes en la actualidad, que consideran los distintos campos de la tecnología de la información, tales como: OWASP [2], enfocado al *pentesting* de aplicaciones web; metasploit, con un enfoque general y desarrollo de exploits; o las distintas matrices del MITRE ATT&CK [3], enfocadas en los distintos entornos existentes. A pesar del extendido uso de estos *frameworks*, lo cual ha derivado en la existencia de guías estandarizadas y a menudo reguladas por los distintos organismos relevantes, tales como el NIST (*National Institute of Standards and Technology*) [4] o la ENISA (*European Union Cybersecurity Agency*) [5], esta práctica se enfoca mayoritariamente en los entornos propios de las IT, tomando como secundarios los entornos industriales.

Considerando esto, es de vital importancia mencionar el surgimiento en los pasados años de la actualmente más que afianzada revolución industrial de cuarta generación, o Industria 4.0 [6], y la nueva Industria 5.0 [7], las cuales suponen una mayor automatización en los sistemas industriales, con la intención de aumentar la productividad y rendimiento económico de la Industria, derivando en una mayor integración de tecnologías dentro del panorama OT, lo que resulta en un aumento de las interconexiones de estos sistemas industriales con otros, y una mayor exposición dentro de la red. Nos encontramos, por tanto, que en la actualidad, sistemas OT que comúnmente estaban aislados [8], usando protocolos específicos, se han adaptado a los protocolos y tecnologías propias del IT, resultando en la existencia de entornos híbridos IT-OT, que son el foco de este artículo. De hecho, esta integración de los sistemas OT, ha supuesto un aumento en los distintos ataques dirigidos a la Industria, siendo ejemplos de relevancia el ataque al software de control Orion, de Solarwinds o el ataque a KASEYA, mediante ransomware [9], que afectaron a diversas organizaciones industriales. Más allá de estos casos particulares, se puede comprobar en base a los distintos informes de ciberataques existentes, que el número de ataques a la Industria es cada vez mayor [10].

En consecuencia, consideramos el *pentesting* una herramienta necesaria para asegurar la nueva Industria 5.0, en base la criticidad, alta resiliencia y fiabilidad requerida. A lo largo de este artículo, se presenta una particularización del *pentesting* en el ámbito de la nueva Industria 5.0, proponiendo incluso una metodología adaptada a la nueva conceptualización industrial y denotada aquí como *Pentesting 5.0*. En la sección II, se describen los objetivos de la Industria 5.0, así como una metodología específica para esta práctica considerando los requisitos de la misma. En la sección III, se hace un resumen de las herramientas que posibilitan el ejercicio del *pentesting* en el ámbito industrial moderno, considerando las tecnologías de vanguardia actuales y las capacidades que proveen. Seguidamente, en la sección IV, se hará un análisis de las posibles implicaciones negativas del uso de estas tecnologías, así como las consideraciones a tener

en cuenta al hacer uso de estas. Finalmente, en la sección V, se presentan las distintas conclusiones, relacionando las distintas tecnologías planteadas con la metodología propuesta.

II. Pentesting en la Industria 5.0

Esta sección trata de conectar los objetivos del *pentesting* a los nuevos criterios operativos de la Industria 5.0, por lo que se introducen a continuación dichos criterios para más tarde mapearlos a las acciones metodológicas que suelen abordar los procesos de *pentesting*, pero adaptados a los nuevos contextos operativos. Como un resultado una nueva metodología se propone capaz de habilitar operaciones esenciales en búsqueda de vulnerabilidades suceptibles a ataques potenciales.

II-A. Objetivos prioritarios de la Industria 5.0

La industria 4.0, con la inclusión de las nuevas tecnologías IT en entornos industriales supuso un gran cambio en los procesos operacionales, fomentando el rendimiento, la automatización y la eficiencia de las tecnologías OT mediante el aumento de la conexión y la adaptación de las IT-OT en entornos operativos, proporcionando, además, nuevas formas para mejorar las funciones primarias del sistema y nuevos modos de operar en el campo. Sin embargo, la influencia social y los requisitos para priorizar las necesidades humanas en tales contextos, hace que surja un nuevo concepto de industria en línea a las prioridades de la Sociedad 5.0 [11], y correspondiente a la bien recibida Industria 5.0 [12].

Este nuevo concepto industrial, supone una transición implícita entre paradigmas, apuntando a la necesidad de intensificar y personalizar la interconexión máquina-humano, proteger la globalización de sistemas en entornos operativos, y permitir una mayor agilización para recopilar y tratar datos en tiempo real [13]. A todo esto contribuyen el amplio conjunto de nuevas tecnologías de interconexión, de las que como ejemplos podemos mencionar el IoT (*Internet of Things*), IoP (*Internet of People*), IIoT (*Industrial Internet of Things*). Todas estas tecnologías se encuentran englobadas dentro del llamado IoE (*Internet of Everything*), que expande el concepto de Internet, conectando a las personas y los dispositivos dentro de una misma red [14]. De esta forma, podemos derivar que la Industria 5.0 no es más que un concepto que surge como una extensión de la Industria 4.0 para integrarse en una sociedad altamente interconectada e inteligente donde se priorizan las necesidades humanas y las interacciones máquina-humano, actuando las máquinas bajo las decisiones humanas y realizando acciones iterativas.

Todo estos nuevos objetivos están también remarcados en [7], en donde además se extraen tres condiciones prioritarias cuando la industria en general transita hacia la Industria 5.0. Estas nuevas condiciones son las siguientes:

1. **Centralidad en el humano.** Mientras que la Industria 4.0 buscaba la completa automatización de los procesos mediante el uso de distintas tecnologías, la Industria 5.0 busca incluir de nuevo a la persona en el lugar que se merece, considerando al ser humano como un activo más en el proceso de transformación digital de la industria. De esta forma, se desea llegar en este nuevo paradigma a un compromiso entre la automatización tecnológica y la capacidad de toma de decisiones y razonamiento propios del ser humano.

Figura 1. Objetivos prioritarios de la Industria 5.0

2. **Resiliencia.** El nuevo paradigma de la Industria 5.0 incluye la resiliencia como una característica necesaria que engloba condiciones específicas relativas a la disponibilidad, fiabilidad, respuesta a errores, rendimiento y ciberseguridad de los sistemas [15, 12]. Todas estas características hacen referencia a las capacidades del sistema de funcionar correctamente independientemente de su situación, y, por tanto, de forma continuada, sin afectaciones debido a fallos internos o intencionados contra el funcionamiento del sistema.
3. **Sostenibilidad.** El concepto de sostenibilidad se asocia al ámbito ecológico de la palabra, deseando, por tanto, minimizar el impacto ambiental de la industria. Para ello, un sistema industrial, deberá cumplir las siguientes características: escalabilidad, extensibilidad, interoperabilidad, mantenibilidad y la propia resiliencia [15, 12]. Consideramos la escalabilidad, extensibilidad y mantenibilidad del sistema, requisitos fundamentales en un sistema sostenible, permitiendo realizar las adiciones y cambios pertinentes dentro de la arquitectura del sistema o sobre los distintos activos sin la necesidad de grandes modificaciones. De esta forma, se asegura la permanencia del sistema al lo largo del tiempo, evitando paradas y reinicios innecesarios, que conllevarían pérdidas, tanto temporales como energéticas. Se ha considerado además necesaria la interoperabilidad de los activos del entorno, permitiendo así la inclusión de nuevos dispositivos de cara a un futuro sin la necesidad de reemplazar equipamiento.

La Figura 1 ilustra la influencia de estos tres objetivos de la Industria 5.0, que constituyen las bases de despliegue de las nuevas tecnologías IT-OT. Sin embargo, estos tipos de despliegues sin controles de seguridad apropiados a cada entorno, y sin explorar de manera adecuada las vulnerabilidades conocidas o desconocidas, pueden provocar serias violaciones a esta triada de objetivos, poniendo en peligro a su vez las condiciones de la Industria 5.0, y a las personas que la integran. Por esta razón, y tomando en consideración estas bases y las distintas características identificadas como necesarias en los entornos industriales, a continuación se propone una metodología de *pentesting* capaz de automatizar todo el proceso de exploración, identificación y mitigación de vulnerabilidades, independientemente de su naturaleza, ideal incluso para entornos altamente interconectados de la Industria 5.0, en el que vulnerabilidades desconocidas pueden ser el principal objetivo de ataque.

II-B. Metodología propuesta: Pentesting 5.0

El *pentesting*, tal y como se ha comentado anteriormente, es una práctica históricamente limitada a entornos IT. Hasta la fecha, existen distintas metodologías, como son el PTES (Penetration Testing Execution Standard) [16] o el OSSTMM (Open Source Security Testing Methodology Manual) [17]. Todos ellos definen de manera estandarizada las distintas fases y procesos típicos del *pentesting*, que siguen generalmente unos procesos de ejecución comunes, alineadas también por trabajos académicos existentes [18, 19, 20]. Básicamente, existen unas primeras fases de (i) negociación y acuerdos con el cliente, planteamiento y obtención de información, seguidas por una (ii) serie de fases técnicas en las que el *pentester* interactúa con el sistema para identificar aquellas vulnerabilidades típicas, ejecutando ciertos ataques para verificarlas. Las fases finales se centran (iii) en elaborar una serie de informes y recomendaciones de buenas prácticas o de mitigación.

Esta linealidad entre trabajos relacionados, no resulta tan factible para entornos basados en IT-OT, ya que la herencia de vulnerabilidades se multiplica por el despliegue tecnológico y la complejidad del contexto . Todo esto pone de relieve el interés actual por los adversarios en explotar vulnerabilidades desconocidas (referenciadas aquí como *zero-days* o ZDV, por sus siglas *Zero-Day Vulnerability*), y los múltiples ataques de tipo "*Advanced Persistent Threat*" (APT) [21], forzando la necesidad de crear metodologías recursivas basadas en la iteración, a fin de intensificar el descubrimiento y su prevención. Para ello, y tomando en consideración tanto las bases de la Industria 5.0 como las distintas metodologías y *frameworks* de *pentesting* existentes, se propone a continuación una metodología específica para dichos contextos industriales, bajo el nombre de "*Pentesting 5.0*". Esta nueva metodología, toma como referencia la establecida por PTES [16], por ser considerada una de las metodologías más extendidas a día de hoy y viable para los diversos escenarios de aplicación de tipo IT [22, 23].

El *Pentesting 5.0*, consta de seis fases fundamentales tal como se representa también en la Figura 2:

1. **Preparación.** Esta primera fase comprende el diseño y planteamiento de los tests de penetración, fijando los objetivos a cumplir y su temporización Para el diseño de estos tests, y la correcta realización de las acciones en las siguientes fases, será necesario, además, por parte del auditor/a el conocimiento de información general acerca del sistema a auditar, tales como los objetivos y requisitos de la compañía, así como los distintos empleados. Además, será conveniente tener una visión a nivel general de la arquitectura del sistema y su relación con los distintos usuarios. Todo esto supondrá un plan de actuación más específico y completo. Una vez obtenido este plan de actuación, es necesario informar detalladamente al cliente acerca de las pruebas a realizar, así como los riesgos que deberá asumir en función del alcance esperado, resultando en un acuerdo o contrato firmado, que fijará el ámbito y alcance de las pruebas realizadas por el *pentester* en las fases posteriores.
2. **Identificación de activos IT/OT, incluyendo las personas.** Durante esta fase, será necesario la identificación de las diversas características del sistema auditado, tales como (i) la arquitectura del sistema, (ii) la topología de red IT-OT, (iii) los servicios ofrecidos, y (iv) los activos IT/OT del sistema, que incluyen, entre otras cosas: los dispositivos a nivel *hardware* y *software*, configuraciones IT/OT o de seguridad, dependencias con otros activos e interacciones con usuarios, etc. Durante esta fase, diversas consultas a los distintos responsables de la gestión de las áreas del entorno pueden también plantearse, como, por ejemplo, qué tipos de herramientas específicas de escaneo se aplican, tanto pasivas (no intrusivas) como activas (intrusivas), elementos de seguridad, qué usuarios son los responsables y sus permisos o usuarios que pueden ser susceptibles a riesgos debido a las interacciones máquina-humano, y otras muchas consultas para intensificar los elementos a ser explorados.
3. **Análisis de vulnerabilidades.** Haciendo uso de la información obtenida acerca de los activos del sistema y sus relaciones, el *pentester* deberá realizar un análisis de las posibles vulnerabilidades existentes en el sistema, haciendo uso manual o automático de los existentes repositorios externos, como pueden ser el MITRE CVE (*Common Vulnerabilities and Exposures*) [24], o la *National Vulnerability Database* (NVD) del NIST [25]. También, puede ser conveniente el análisis de configuraciones y relaciones entre activos, para identificar otras posibles vulnerabilidades, y haciendo referencia a otros repositorios como el *MITRE ATT&CK* [3], o el *OWASP Top Ten* [26]. En entornos industriales es necesario abordar el gran predominio de ataques APT, cuyos atacantes se sustentan principalmente de la búsqueda y explotación de ZDV para su penetración, persistencia e intrusión. Por tanto, será necesario realizar ciertas hipótesis acerca de la existencia de ZDV, analizando el comportamiento de los distintos activos (IT, OT, IT-OT) del sistema, con la intención de encontrar posibles vías de ataque.
4. **Explotación y verificación.** Las vulnerabilidades descubiertas en la fase anterior deberán ser verificadas, bajo la realización controlada de ataques y tendiendo presente los principios del *hacking* ético. El *pentester* deberá verificar que tanto (i) las vulnerabilidades existen dentro del sistema, como (ii) el posible alcance de un ataque derivado de sus respectivas explotaciones - p. ej. el efecto en cascada entre componentes IT, OT e IT-OT. De igual forma, serán de especial interés para su posterior consideración los vectores de ataque, datos expuestos como consecuencia de la explotación, y aún más importante en el ámbito de la industria, las posibles consecuencias en la disponibilidad y rendimiento del sistema final. Respecto a la búsqueda de ZDV, la existencia de estas deberá ser comprobada, haciendo uso de técnicas existentes como el *fuzzing* [27], el lanzamiento de bombas lógicas, o el abuso sistemático y riguroso de *exploits* en los diferentes elementos del sistema. Esta fase y la fase de análisis de vulnerabilidades están estrechamente relacionadas, pudiendo ser descubiertas o planteadas nuevas ZDV durante la explotación de

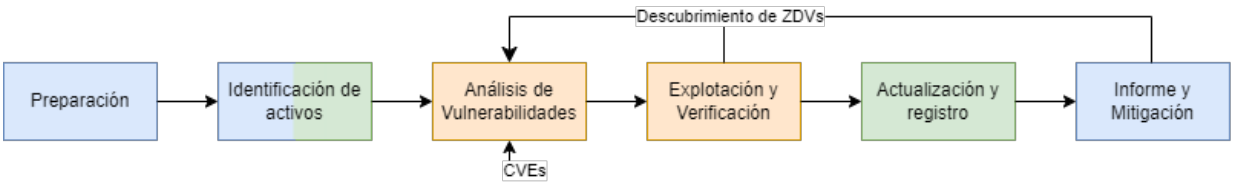

Figura 2. Metodología *Pentesting 5.0*, y sus fases para ser aplicadas en entornos de tipo IT-OT

vulnerabilidades, las cuales deberán volver a ser analizadas en profundidad y en amplitud, obteniendo cierta recursividad entre ambas fases.

5. **Actualización y/o registro.** Tras la obtención de la información de los distintos activos del sistema y sus vulnerabilidades asociadas, el siguiente paso es registrar o actualizar la información encontrada, además de las distintas acciones realizadas. Esta información podrá ser usada en futuras iteraciones del proceso de *pentesting*, evitando al *pentester* tener que comenzar todo el proceso desde cero. Será de interés en esta fase, además, la generación de distintas métricas acerca de las vulnerabilidades, teniendo en cuenta su implicación en el sistema y las posibles consecuencias de la explotación de éstas. Estas métricas podrán ser generadas a partir de información obtenida de los repositorios de referencia ya mencionados, u otros más específicos tales como el CVSS (*Common Vulnerability Scoring System*) [28].
6. **Informe, mitigación y post-explotación.** Para finalizar, una vez concluidas las distintas fases de identificación y explotación de vulnerabilidades, estos datos deberán ser procesados, con la intención de proporcionar al cliente la información necesaria acerca de las distintas vulnerabilidades identificadas y acciones realizadas en el sistema. De igual forma, será conveniente proporcionar información acerca de la importancia de las distintas vulnerabilidades, de acorde a las métricas obtenidas en la fase anterior. Estas métricas, junto a una serie de recomendaciones acerca del procedimiento recomendado para la solventación de las distintas vulnerabilidades, serán usadas por el cliente para planificar el proceso de mitigación. Tras la mitigación, el proceso puede culminar con una última fase de verificación (la post-explotación) con el objeto de testimoniar la corrección de la vulnerabilidad, o en su caso, el descubrimiento de nuevas, causadas por la propia corrección.

La Figura 2 también muestra un mapeo directo y a nivel de colores entre las fases del *Pentesting* 5.0 y los tres objetivos de la Industria 5.0. De forma que la preparación, informe y mitigación son dos fases que si se elaboran de forman correcta y completa, beneficia las tareas del auditor/a. También las fases de identificación de activos y registro ayudan a reducir los escaneos y el gastos continuados de recursos, favoreciendo con esto la sostenibilidad del contexto de aplicación, y la búsqueda en profundidad y en amplitud de vulnerabilidades, junto con sus posteriores fases de verificación, benefician a la bien esperada resiliencia de la Industria 5.0.

II-C. Adaptación del Pentesting 5.0 de acuerdo a requisitos

Esta subsección se centra en proporcionar los requisitos fundamentales que ayuden a adaptar la metodología planteada en los diversos contextos de la Industria 5.0, atendiendo, además, en las capacidades que las futuras plataformas de *pentesting* deberían aportar en el ámbito de la metodología y a la Industria 5.0, y que incluye la automatización, la iteración entre fases y el descubrimiento de ZVD, el desacoplamiento de acciones, y la resiliencia frente amenazas potenciales.

	Persona	Sostenibilidad	Resiliencia
Supervisión y decisiones	*		*
Automatización	*		
Interoperabilidad	*	*	
Rendimiento		*	*
Escalabilidad de datos		*	*
Escalabilidad de sistema		*	*
Inmutabilidad del entorno		*	*
Seguridad	*	*	*
Descubrimiento de activos			*
Descubrimiento de ZDVs	*	*	*
Almac. de activos y vuln.	*	*	
Gestión de activos y vuln.	*	*	
Generación de Informes	*		
Trazabilidad de acciones	*		*
Parámetros Infor. Autom.	*		
Adaptabilidad	*		*
Respuesta a errores		*	*
Desacoplamiento		*	*

Tabla I
REQUISITOS DEL PENTESTING 5.0 EN RELACIÓN A LOS OBJETIVOS DE LA INDUSTRIA 5.0

Es por ello que la Tabla I muestra un mapeo entre los requisitos del *pentesting 5.0* con los tres objetivos prioritarios de la Industria 5.0. De la tabla, extraemos varias aspectos, por ejemplo, y comenzando con de la persona en el centro de todo, podemos destacar la necesidad de que la persona sea consciente en todo momento de qué ocurre en el sistema, mediante la generación de distintos **parámetros informativos** e **informes** de forma automatizada, permitiendo al cliente y al auditor/a la correcta **supervisión y toma de decisiones** con respecto a las acciones relevantes que realizará el sistema, siguiendo además su **trazabilidad**. Estas acciones podrán ser realizadas de una forma más sencilla para el/la auditor/a, incluyendo métodos de **automatización**. Son también necesarias la **interoperabilidad** de la plataforma con los distintos activos existentes dentro de los sistemas auditados, así como la **adaptabilidad** a las distintas arquitecturas y situaciones a las que pueda ser aplicada.

Teniendo en cuenta la sostenibilidad, podemos ver cómo será necesario el **almacenamiento de activos y vulnerabilidades** en el sistema, evitando la repetición de las tareas de **descubrimiento** de forma innecesaria.

Se consideran necesidades derivadas tanto de la sostenibilidad como de la resiliencia, un sistema de auditoría con capacidades de **escalabilidad**, tanto a nivel de datos como del propio sistema, evitando malgastar recursos, y funcionar de forma incorrecta o con retrasos, lo cual podría afectar negativamente al sistema auditado y la **inmutabilidad del entorno**, la cual consideramos una característica necesaria, además del correcto **rendimiento** del mismo. En adición a esto, el sistema deberá integrar mecanismos de **respuesta a errores**, los cuales se pueden producir durante el proceso de *pentesting*. Como consecuencia de esto, la plataforma de *pentesting* deberá estar, además, **desacoplada** del entorno auditado.

Finalmente, consideramos requisitos de especial interés la propia **seguridad** de la plataforma, evitando que la propia plataforma sea una vía de entrada de ataques sobre el entorno auditado. Además, vemos como el **descubrimiento de ZDV** tiene especial impacto en los distintos objetivos de la Industria 5.0. Las ZDV pueden incitar a atacantes a liderar acciones contra: (i) las personas que conforman la organización (p. ej. mediante la exfiltración de datos sensibles), (ii) la sostenibilidad, puesto que se podrían provocar acciones contra el buen funcionamiento del sistema y su correcto consumo energético, pero también el bienestar de aquellos componentes gestionando elementos físicos críticos o peligrosos (ej. radiación, químicos, etc.), y, por último, (iii) la resiliencia, puesto que un atacante podría actuar sobre el correcto funcionamiento de los distintos activos IT/OT del sistema, haciendo uso, por ejemplo, de ataques DoS (*Denegation of Service)*. Las consecuencias, sin duda, pueden ser devastadoras y poner en peligro la reputación y seguridad de la organización, la seguridad de las personas, y el bienestar de la sociedad y su economía como un todo.

III. Tecnologías para el Pentesting 5.0

Como ya hemos comentado en las secciones anteriores, el *Pentesting 5.0* tiene una serie de nuevos requisitos respecto a el *pentesting* convencional, enfocado a las distintas redes IT. Hasta ahora, el *pentesting* ha hecho uso de una serie de tecnologías tradicionales, habilitando la correcta realización de las distintas fases de este proceso acorde a las distintas metodologías mencionadas. Especial relevancia tienen:

- **Herramientas externas (HE).** El uso de herramientas ya desarrolladas facilita al *pentester* la fácil realización del proceso de *pentesting*, evitando la realización de ciertas tareas tediosas o repetitivas de forma manual, siendo estas frecuentemente automatizadas. De igual forma, el uso prácticamente estandarizado de algunas de estas herramientas, suele limitar la existencia de fallos las mismas. Podemos destacar, como ejemplos, aquellos sistemas operativos dedicados al *pentesting*, tales como *Kali Linux* o *BlackArch*; herramientas de pentesting web, tales como *OWASP ZAP* o *Burpsuite*; de crackeo de contraseñas, como *John the Ripper*; o de análisis de red, como *Wireshark*. Y respecto a la gestión de los activos del entorno auditado, herramientas del tipo *Bill of Materials* (BOM), tales como *CycloneDX*, que permiten la gestión de los activos del entorno y sus relaciones, especialmente a nivel de *software* (SBOM) [29].
- **Repositorios y APIs conocidos (REP).** Se hace uso, además de las distintas herramientas mencionadas de repositorios de vulnerabilidades conocidas, tales como el MITRE CVE [24] o el NVD [25], ampliamente usados en la industria de ciberseguridad a modo de referencia, asociando versiones de hardware y/o software con las distintas vulnerabilidades conocidas asociadas a éstos.

El cumplimiento de los requisitos de la subsección II-C en línea con las futuros despliegues tecnológicos de *pentesting* en el nuevo panorama industrial, puede ser únicamente factible si se considera la inclusión de las nuevas IT para la realización de acciones y el apoyo en las distintas fases descritas de la metodología *Pentesting 5.0*, detallada en la sección II-B. Es por ello que procedemos a enumerar en la siguiente subsección las distintas tecnologías disruptivas que estando muy valoradas en la Industria 5.0, benefician también el cumplimiento de los requisitos del *Pentesting 5.0*.

III-A. Automatización y autonomía

Incluye las tecnologías de Inteligencia Artificial (IA) más relevantes en el panorama actual. Dentro de éstas, se distinguen las **generativas** (**GEN**), especializadas en la generación de distintos tipos de datos, siguiendo unas reglas establecidas. Esta tecnología puede ser útil para la generación de informes y métricas acerca del funcionamiento y las acciones realizadas en el sistema, así como para la generación de ciertas recomendaciones. De igual forma, se deben tener en cuenta aquellas tecnologías de **Machine Learning** (**ML**), algoritmos y modelos estadísticos que permiten a sistemas informáticos completar ciertas tareas sin ser programados para ellas de forma explícita [30]. La tecnología de ML será usada en la plataforma para la mejora de las capacidades en ciertas fases del proceso, por medio de la gestión de datos complejos difícilmente interpretables haciendo uso de las tecnologías tradicionales, permitiendo así la mejora del descubrimiento de activos IT/OT o la posibilidad del descubrimiento automático o asistido de ZDV. Destacamos también su implicación de cara a la interoperabilidad del sistema, siendo capaz de detectar los distintos protocolos y sintaxis utilizados, y gestionando la adaptación de la plataforma a estos. Finalmente, es de especial interés destacar en adición a todo esto, las capacidades de esta tecnología para el despliegue de mecanismos de control de errores y escalabilidad del sistema.

Finalmente, los **agentes software** (**AS**), "*programas autocontenidos, capaces de controlar su propia toma de decisiones y actuaciones en función de su percepción del entorno, buscando completar uno o más objetivos*" [31]. Estos permitirían la automatización de ciertas tareas del sistema haciendo uso de las otras tecnologías disponibles, estando la automatización limitada en todo caso por la aprobación de las acciones a realizar por parte del *pentester*. De esta forma, aquellas acciones recurrentes y tediosas, y sin grandes implicaciones sobre el sistema auditado, como el descubrimiento de activos, podrían recaer exclusivamente en esta tecnología inteligente.

III-B. Despliegue distribuido

Cloud computing (**CL**) o ***edge computing*** (**ED**) pueden reducir las implicaciones que pueden conllevar el uso de las distintas herramientas de *pentesting* al entorno auditado.

	GEN	ML	AS	CL/ED	SIM	SD	DT	AR	VR	BD	BCH	REP	HE
Supervisión y toma decisiones			*		*	*		*	*			*	
Automatización			*				*			*		*	*
Interoperabilidad		*	*	*	*								*
Rendimiento		*		*	*				*	*			
Escalabilidad de datos		*		*						*		*	
Escalabilidad de sistema		*		*						*			*
Inmutabilidad sobre el entorno				*	*	*			*	*			*
Seguridad			*	*	*	*			*		*		*
Descubrimiento de activos		*	*							*	*	*	*
Descubrimiento de ZDVs	*	*	*	*	*	*	*	*	*	*	*	*	*
Almac. de activos y vuln.				*						*	*		*
Gestión de activos y vuln.	*	*			*	*	*				*	*	*
Generación de Informes	*				*	*	*	*	*	*	*	*	
Trazabilidad de acciones	*							*		*	*		
Parámetros Inf.	*					*	*	*	*	*		*	
Adaptabilidad		*		*									*
Respuesta a errores		*		*	*		*						
Desacoplamiento				*	*								

Tabla II
REQUISITOS DEL PENTESTING 5.0 EN RELACIÓN A LOS OBJETIVOS DE LA INDUSTRIA 5.0

Dado que el despliegue se realiza en dispositivos independientes al entorno IT-OT auditado, todo el procesamiento de *pentesting* quedaría relegado en componentes externos [32]. Por tanto, este híbrido de soluciones es lo que responde a la disponibilidad, rendimiento y escalabilidad de las plataformas de *Pentesting 5.0*, dando garantías de mayor eficacia de los recursos disponibles, y proporcionando una mayor capacidad de procesamiento y medidas de respuesta a errores bajo una arquitectura desacoplada del entorno auditado, limitando las posibles implicaciones en cadena al sistema crítico auditado.

III-C. Virtualización

Engloban todas aquellas tecnologías de virtualización que permiten integrar, dentro de un entorno virtual, los distintos dispositivos del entorno IT-OT. Dentro de estas tecnologías, destacamos aquellas asociadas con la **simulación** (**SIM**) y sus derivados como el ***Digital Shadow*** (**DS**) y ***Digital Twins*** (**DT**) [15], capaces de emular mediante modelos específicos, los estados y comportamientos reales de cada activo del sistema. Unido con los objetivos del *pentesting*, podemos apreciar que la simulación pueden ayudar a predecir estados e identificar nuevos descubrimientos de vulnerabilidades sin impactar en el rendimiento del sistema final. Digamos que la simulación puede ser un modo atractivo para extraer ideas concebidas del estado real de un sistema sin que esto suponga una agresión directa a su integridad y disponibilidad; mientras que los DS y DT permiten al auditor/a obtener información en tiempo real acerca del funcionamiento real por el cual comenzar la simulación, y en su caso responder de manera autónoma, como es el caso del DT. Como es evidente, todas estas tecnologías, optimizan la información proporcionada a los distintos actores del entorno, ya sea al *pentester* como al cliente, y en tiempo real o a posteriori, a través de informes detallados con demostraciones simuladas.

III-D. Visualización

Existen tecnologías cuyos fines son la mejora o la extensión de la realidad, o incluso, el reemplazo de la realidad física con una puramente virtual y simulada. En este sentido, encontramos tres tecnologías principales [33]: ***Virtual Reality*** (**VR**), ***Augmented Reality*** (**AR**) y ***Mixed Reality*** (**MR**). Mientras que el fin de AR es modificar la percepción del mundo real superponiendo información digital sobre ella [34], la VR, por su parte, surge con el fin de crear una realidad puramente virtual, fiel o no a la realidad física. Por último, la MR fusiona los conceptos de AR y VR, superponiendo datos y objetos virtuales funcionales en el mundo real.

Cierto es, que estos conceptos están estrechamente relacionados con las tecnologías de virtualización mencionadas en la subsección III-C, las cuales hacen uso en mayor o menor medida de los conceptos de VR y AR para su implementación. Sin embargo, en el ámbito de este artículo se tratan las tecnologías de realidad extendida considerando la posibilidad de su uso para otros fines, enfocados en el proceso del *pentesting* en sí, tales como la superposición de información del proceso del *pentesting* y el sistema en tiempo real, así como la capacidad de proporcionar posibles consejos y métricas de interés al auditor/a o información de interés al cliente final.

III-E. Gestión de grandes volúmenes de datos

Contempla todas aquellas técnicas relativas al **Big Data** (**BD**) junto con sus correspondientes analíticos, los cuales son capaces de procesar la inmensa ingesta de datos de una parte o el entero sistema auditado. Ya existen trabajos que demuestran su aplicación para entornos industriales, como es el caso de Stepanova *et al.* [35], quienes proponen el uso de BD para la automatización del proceso de *pentesting* en entornos IT-OT, dentro de los cuales se podrían incluir aquellos entornos híbridos propios de la Industria 5.0. De igual forma, su uso en el ámbito de la detección de ZDV es una posibilidad muy interesante, permitiendo al sistema disponer de medios para la detección de aquellos cambios leves en el rendimiento o en el comportamiento del entorno industrial, los cuales no podrían ser detectados haciendo uso de tecnologías típicas.

III-F. Almacenamiento de la información

Comprende todas aquellas tecnologías que dan garantías de registro y transparencia de datos de una forma confiable y segura. En este caso se toma como referencia las redes de **blockchain**, las cuales permiten el almacenamiento distribuido bajo restricciones de consensos e inmutabilidad gracias en parte al tipo de encadenamiento controlado por

hashes [36]. Estas características unidas con las fases de registro del *pentesting*, dan también garantía de trazabilidad y auditoría, ya que el *pentester* o el cliente pueden trazar las secuencias de acciones realizadas. Cualquier cambio que se realice dentro de la cadena de transacciones tiene un impacto en su inmutabilidad, permitiendo al *pentester* o al cliente identificar violaciones en el proceso de *pentesting*.

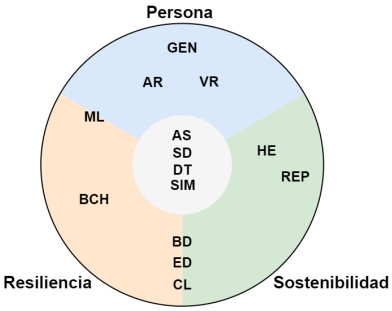

Figura 3. Tecnologías del Pentesting 5.0 en la Industria 5.0

Para concluir esta sección, la Figura 3 muestra cómo el conjunto de las distintas tecnologías consideradas cubren los tres objetivos prioritarios de la Industria 5.0, remarcando visualmente, que se es posible alcanzar la compatibilidad esperada para cumplir la propuesta de *Pentesting 5.0*.

IV. Implicaciones de las IT en el Pentesting 5.0

A pesar de que las nuevas IT mencionadas dan soporte al *Pentesting 5.0*, permitiendo nuevas posibilidades respecto a aquellas metodologías clásicas, el uso de éstas implica la necesidad de tener en cuenta ciertas consideraciones y limitaciones, que pueden poner en peligro el rendimiento de los entornos auditados, la gestión de una cantidad masiva de datos sensibles, y la seguridad del sistema. Para entender estas implicaciones, se tendrá en cuenta: (i) los tres requisitos de seguridad más populares dentro de la ciberseguridad, como la confidencialidad, integridad y disponibilidad, y en términos de datos y recursos; (ii) los requisitos específicos de la Industria 5.0, como la centralidad del humano, la sostenibilidad y la resiliencia, (iii) pero también el nivel de criticidad del propio entorno de aplicación [15]. Mientras que el cumplimiento de todos estos requisitos y condiciones favorecen la protección del propio sistema auditado, la plataforma no debería perjudicar de ninguna forma la operatividad del entorno en el que se ejecuta. Es por ello que a continuación se realiza un análisis de estas implicaciones y en relación a las nuevas tecnologías de información, ofreciendo igualmente un conjunto de recomendaciones para prevenirlos:

- *Automatización y autonomía*. La implicación de estas tecnologías será principalmente para la gestión y tratamiento de la información obtenida del entorno. Se debe considerar que estas tecnologías frecuentemente hacen uso de la información tratada para su propio aprendizaje, lo cual podría resultar en problemas de cara al futuro sobre la privacidad de los datos que han sido tratados, en caso posibles ataques [37]. Por tanto, para evitar problemas de privacidad, será recomendable considerar las distintas técnicas para la protección de la privacidad en este ámbito que están siendo estudiadas en la actualidad, tal y como recoge el trabajo de Liu *et al.* [38].
- *Despliegue distribuido*. A pesar de las mejoras que implican estas tecnologías, es también importante considerar que la clara exposición de estas tecnologías en infraestructuras ajenas al entorno privado, supone un mayor riesgo a la confidencialidad, además de otras amenazas como la disponibilidad de los datos, siendo una solución el despliegue de infraestructuras puramente privadas donde el *pentester* y el cliente tengan el máximo control de los datos, además de desplegar soluciones distribuidas, y a ser posible redundantes, que beneficien el acceso independientemente de la amenaza [39]. De igual forma, se deberán considerar otros posibles ataques, derivados de malas prácticas en la implementación, p.ej. en las APIs, o el uso de credenciales poco seguras [40]. Se deberán asegurar correctamente tanto las comunicaciones como la propia arquitectura distribuida, evitando así las posibles consecuencias en el sistema.
- *Virtualización*. En lo referido a estas tecnologías, es importante considerar que mientras que la simulación se realiza de forma independiente, tanto los gemelos digitales como las sombras digitales, a pesar de estar ejecutados, intercambian datos con la realidad en tiempo real. Como posibles ataques a estas tecnologías son de consideración, además de aquellos de denegación de servicio, tanto a nivel de comunicación como de sistema, aquellos derivados de modificaciones indebidas en los datos recibidos, tales como el *tampering* o el envenenamiento de los datos [41]. De igual forma, Alcaraz *et al.* [15] recogen las distintas vulnerabilidades existentes en estos sistemas, en las distintas capas que conforman un sistema de este tipo, siendo comunes tanto el escalado de privilegios o el acceso no autorizado a los modelos. Se hace entonces de vital importancia, proteger el uso de dicha tecnología y tener prudencia en su propio uso para el análisis, descubrimiento y corrección automática de vulnerabilidades, permitiendo al *pentester* tomar el control de las acciones tras las simulaciones.
- *Procesamiento y visualización*. Consideramos derivados del uso de la realidad extendida o BD, aquellas vulnerabilidades propias debidas al manejo de información que pueden ocultar o entorpecer el proceso de *pentesting*. Es por ello que se recomienda gestionar medidas de autenticación, control de acceso y cifrado, pero también medidas que den garantías de confianza (p. ej. "*¿los datos/vulnerabilidades que estoy viendo son confiables?*").
- *Almacenamiento seguro y distribuido*. La tecnología de blockchain presenta aún múltiples desafíos de investigación, recayendo principalmente en la escalabilidad de los datos y la seguridad de los mismos, poniendo incluso en peligro su utilidad en los procesos de *pentesting* y dependiendo del número de nodos en la red, puede también impactar en la sostenibilidad de la Industria 5.0. Independientemente de que esta tecnología se centre en salvaguardar la integridad de los datos, se debe proteger también la privacidad de los mismos, algo no soportado por defecto. Por tanto, se recomienda buscar

alternativas para gestionar el almacenamiento coherente (p. ej. técnicas de Merkle) y mecanismos criptográficos que potencien la privacidad y anonimato [36].

V. Conclusiones

La metodología de *Pentesting 5.0* planteada cubre las distintas fases de ejecución acorde a los requisitos de los modernos sistemas industriales. Como se ha descrito a lo largo de este artículo, en el ámbito industrial, se deben considerar no sólo aquellas vulnerabilidades ampliamente conocidas (CVE), sino que además, se debe hacer especial hincapié en aquellas vulnerabilidades comúnmente explotadas en el ámbito tratado, como son las *Zero-Days Vulnerabilities*, resultando en una metodología recursiva. Con respecto a las tecnologías tratadas y que pueden dar cobertura a las fases de *Pentesting 5.0*, son de especial interés para el entorno de la Industria 5.0 las nuevas tecnologías disruptivas, englobando la Inteligencia Artificial en sus distintas formas, aquellas tecnologías propias del manejo masivo de datos (*Big Data*), de despliegue distribuido, y aquellas destinadas a la mejora de la realidad y la simulación. Por tanto, es destacable el carácter habilitador de estas nuevas tecnologías para el desarrollo del *pentesting* en vista de la tríada de bases que conforman la Industria 5.0.

Agradecimientos

El trabajo ha sido principalmente financiado por el proyecto eMAPA 4.0 II (AEI-010500-2022b-78) del Ministerio de Industria, Comercio y Turismo dentro del programa AEI para contribuir a la mejora de la competitividad de la industria española, y con el apoyo de la Unión Europea a través del Plan de Recuperación, Transformación y Resiliencia; y, asimismo, por el proyecto SecTwin 5.0 (TED2021-129830B-I00) financiado por el Ministerio de Ciencia e Innovación, Agencia Estatal de Investigación (10.13039/501100011033), and European Union "NextGenerationEU"/Plan de Recuperación, Transformación y Resiliencia.

Referencias

[1] Nivedita James Palatty. *A Brief History of Penetration Testing*. Dic. de 2022. URL: https://www.getastra.com/blog/security-audit/history-penetration-testing/.

[2] OWASP Foundation. *The OWASP Testing Framework*. 2023. URL: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/.

[3] MITRE. *ATT&CK*. URL: https://attack.mitre.org/.

[4] NIST. *Technical Guide to Information Security Testing and Assessment*. 2008. URL: https://csrc.nist.gov/pubs/sp/800/115/final.

[5] European Network and Information Security Agency (ENISA). *ENISA*. 2024. URL: https://www.enisa.europa.eu/.

[6] Juan E. Rubio, Rodrigo Roman y Javier Lopez. "Analysis of cybersecurity threats in Industry 4.0: the case of intrusion detection". En: *The 12th Int. Conference on Critical Information Infrastructures Security*. Vol. 10707. Springer, 2018, págs. 119-130.

[7] European Commission. "Industry 5.0 : towards a sustainable, human-centric and resilient European industry." En: (2021). URL: https://op.europa.eu/en/publication-detail/-/publication/468a892a-5097-11eb-b59f-01aa75ed71a1/.

[8] Cristina Alcaraz et al. "Secure SCADA Framework for the Protection of Energy Control Systems". En: *Concurrency and Computation Practice & Exp.* 23.12 (2011), págs. 1414-1430. ISSN: 1532-0626.

[9] BlueVoyant. *Supply Chain Attacks: 7 Examples and 4 Defensive Strategies*. URL: https://www.bluevoyant.com/knowledge-center/supply-chain-attacks-7-examples-and-4-defensive-strategies.

[10] Arctic Wolf Labs. *2024 Threat Report*. URL: https://arcticwolf.com/resource/aw/arctic-wolf-labs-2024-threat-report.

[11] Mayumi Fukuyama et al. "Society 5.0: Aiming for a new human-centered society". En: *Japan Spotlight* 27.5 (2018), págs. 47-50.

[12] Cristina Alcaraz y Javier Lopez. "Protecting Digital Twin Networks for 6G-enabled Industry 5.0 Ecosystems". En: *IEEE Network* 37.2 (2023), págs. 302-308.

[13] Hitachi-UTokyo Laboratory. *Society 5.0*. SpringerOpen, 2020.

[14] Viviane Cunha Farias da Costa, Luiz Oliveira y Jano de Souza. "Internet of Everything (IoE) Taxonomies: A Survey and a Novel Knowledge-Based Taxonomy". En: *Sensors* 21 (2021), pág. 568.

[15] Cristina Alcaraz y Javier Lopez. "Digital Twin: A Comprehensive Survey of Security Threats". En: *IEEE Communications Surveys & Tutorials* 24.thirdquarter 2022 (2022), págs. 1475-1503.

[16] *Penetration Testing Execution Standard (PTES)*. 2014. URL: http://www.pentest-standard.org/index.php/Main_Page.

[17] Pete Herzog. *OSSTMM3, The Open Source Security Testing Methodology Manual*. 2010.

[18] Ankur Chowdhary et al. "Autonomous Security Analysis and Penetration Testing". En: *2020 16th International Conference on Mobility, Sensing and Networking (MSN)*. 2020, págs. 508-515.

[19] Jean-Paul A Yaacoub et al. "A survey on ethical hacking: issues and challenges". En: *arXiv preprint arXiv:2103.15072* (2021).

[20] Hessa Mohammed Zaher Al Shebli y Babak D. Beheshti. "A study on penetration testing process and tools". En: *IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. 2018, págs. 1-7.

[21] Juan E Rubio, Cristina Alcaraz y Javier Lopez. "Preventing advanced persistent threats in complex control networks". En: *22nd European Symposium on Research in Computer Security*. Springer. 2017, págs. 402-418.

[22] Bingchang Liu et al. "Software vulnerability discovery techniques: A survey". En: *Proceedings - 2012 4th International Conference on Multimedia and Security, MINES 2012* (2012), págs. 152-156.

[23] Farah Abu-Dabaseh y Esraa Alshammari. "Automated penetration testing: An overview". En: *The 4th international conference on natural language computing, Copenhagen, Denmark*. 2018, págs. 121-129.

[24] MITRE. *Common Vulnerabilities and Exposures (CVE)*. URL: https://cve.mitre.org/.

[25] NIST. *National Vulnerability Database*. URL: https://nvd.nist.gov/.

[26] OWASP. *Top 10*. 2021. URL: https://owasp.org/Top10.

[27] Wei You et al. "Profuzzer: On-the-fly input type probing for better zero-day vulnerability discovery". En: *2019 IEEE symposium on security and privacy (SP)*. IEEE. 2019, págs. 769-786.

[28] FIRST. *Common Vulnerability Scoring System 4.0*. 2023. URL: https://www.first.org/cvss/.

[29] Vandana Verma Sehgal y P. S. Ambili. "A Taxonomy and Survey of Software Bill of Materials (SBOM) Generation Approaches". En: *AGC 2023*. Ed. por Suparna Dhar et al. Cham: Springer Nature Switzerland, 2024, págs. 40-51. ISBN: 978-3-031-50815-8.

[30] Batta Mahesh. "Machine learning algorithms-a review". En: *International Journal of Science and Research (IJSR).[Internet]* 9.1 (2020), págs. 381-386.

[31] Nick Jennings y Michael Wooldridge. "Software agents". En: *IEE Review* 42 (1 1996), págs. 17-20.

[32] Wazir Zada Khan et al. "Edge computing: A survey". En: *Future Generation Computer Systems* 97 (ago. de 2019), págs. 219-235.

[33] Leonor Adriana Cárdenas-Robledo et al. "Extended reality applications in industry 4.0. – A systematic literature review". En: *Telematics and Informatics* 73 (sep. de 2022), pág. 101863.

[34] Shaveta Dargan et al. "Augmented Reality: A Comprehensive Review". En: *Archives of Computational Methods in Engineering* 30 (2 mar. de 2023), págs. 1057-1080.

[35] Taiana Stepanova, Alexander Pechenkin y Daria Lavrova. "Ontology-based big data approach to automated penetration testing of large-scale heterogeneous systems". En: *Proceedings of the 8th International Conference on Security of Information and Networks*. 2015, págs. 142-149.

[36] Cristina Alcaraz, Juan E. Rubio y Javier Lopez. "Blockchain-Assisted Access for Federated Smart Grid Domains: Coupling and Features". En: *Journal of Parallel and Distributed Computing* 144 (2020), págs. 124-135. ISSN: 0743-7315.

[37] Maria Rigaki y Sebastian Garcia. "A Survey of Privacy Attacks in Machine Learning". En: *ACM Computing Surveys* 56 (4 abr. de 2023), págs. 1-34.

[38] Bo Liu et al. "When Machine Learning Meets Privacy". En: *ACM Computing Surveys* 54 (2 mar. de 2021), págs. 1-36.

[39] Ryhan Uddin, Sathish A.P. Kumar y Vinay Chamola. "Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions". En: *Ad Hoc Networks* 152 (2023), pág. 103322.

[40] Umer Ahmed Butt et al. "Cloud Security Threats and Solutions: A Survey". En: *Wireless Personal Communications* 128 (1 ene. de 2023), págs. 387-413.

[41] Yuntao Wang et al. "A Survey on Digital Twins: Architecture, Enabling Technologies, Security and Privacy, and Future Prospects". En: *IEEE Internet of Things Journal* 10 (17 sep. de 2023), págs. 14965-14987.