REVISTA ELECTRÓNICA SOBRE TECNOLOGÍA, EDUCACIÓN Y SOCIEDAD
ISSN: 2448 - 6493
CTES

Artículos científicos

Uso de AWS Educate para un Laboratorio Virtual de Seguridad en Redes

Using AWS Educate for a Network Security Virtual Lab

Cyntia Eugenia Enríquez Ortiz
Instituto Politécnico Nacional, México
cenriquezo@ipn.mx
https://orcid.org/0000-0003-2597-6205

Raúl Fernández Zavala
Instituto Politécnico Nacional, México
rfernandezz@ipn.mx
https://orcid.org/0000-0001-7231-0209

Carlos De La Cruz Sosa
Instituto Politécnico Nacional, México
cdelacruz@ipn.mx
https://orcid.org/0000-0002-1269-7920

Resumen

La seguridad en redes se ha convertido en un componente crítico en muchas organizaciones, por lo que su enseñanza está ganando popularidad. Tradicionalmente para impartir este tipo de cursos, se utiliza un laboratorio de cómputo con máquinas virtuales, en donde los estudiantes realizan sus prácticas de laboratorios, sin embargo, muchos estudiantes expresan su frustración con este método, principalmente por la limitación del tiempo de uso de laboratorio que tienen disponible para realizar las prácticas y la necesidad de trabajar fuera de las aulas. En respuesta a esta problemática, se propone utilizar los servicios de AWS Educate, el cual es un programa gratuito de Amazon. El objetivo principal de este estudio es explorar la viabilidad de utilizar el programa AWS Educate para la implementación de un laboratorio virtual que permita a los estudiantes de un curso de Seguridad en Redes desarrollar sus prácticas de laboratorio y determinar sus ventajas y desventajas. Este entorno educativo puede ayudar a crear una experiencia de aprendizaje atractiva para los estudiantes y motivarlos a involucrarse en los temas del curso.

Palabras clave: Laboratorio virtual, AWS, Seguridad en Redes.

Abstract

Network Security has become a critical component in many organizations, which is why its teaching is gaining popularity. Traditionally, to teach this type of course, a computer laboratory with virtual machines is used, where students carry out their laboratory practices, however, many students express their frustration with this method, mainly due to the limitation of the time of use of the laboratory that they have available to carry out the practices and the need to work in groups outside the classroom. In response to this problem, AWS Educate services were used, which is a free Amazon program. The main objective of this study was to explore the feasibility of using the AWS Educate program for the implementation of a virtual laboratory that allows students of the Network Security course to develop their laboratory practices and determine their advantages and disadvantages. This educational environment can help create an engaging learning experience for students and motivate them to engage with course topics.

Keywords: Virtual laboratory, AWS, Network Security.

Fecha Recepción: Diciembre 2022 **Fecha Aceptación:** Julio 2022

Introducción

Actualmente, la seguridad en redes es una de las principales preocupaciones de muchas empresas y organizaciones, por lo que, en los últimos años, varias agencias gubernamentales de diferentes países han comenzado a invertir fuertemente en educación y capacitación en esta área (OEA, 2020), (Petersen, et al., 2020). Además, la demanda de profesionales expertos en el área se ha incrementado y es probable que continue de esta forma por mucho tiempo (Pastor, 2022), (Duffy, 2021). Como resultado, la enseñanza de seguridad en redes en la Instituciones de Educación Superior (IES) se ha vuelto vital para poder cubrir la escasez de mano de obra calificada y es ahora uno de los principales objetivos de los programas educativos relacionados con las tecnologías de la información (Habib M.N., et al., 2021). Sin embargo, encontrar herramientas que se puedan usar en el aula para ayudar a los estudiantes a adquirir experiencia práctica es todo un desafío.

Para enseñar seguridad en redes no solo es necesario una pedagogía eficaz y material didáctico adecuado para explicar los conceptos relacionados, sino que se requiere que los estudiantes adquieran experiencia práctica en el área, ya que en el campo laboral, se espera que los estudiantes no solo conozcan las teorías detrás de los problemas de seguridad presentes en una red, sino que deben tener la capacidad de aplicar estas teorías para diseñar, desarrollar e implementar soluciones innovadoras y pertinentes (Masud, Yong, & Huang, 2012).

Tradicionalmente, para proporcionar a los estudiantes esta experiencia práctica, se utilizan laboratorios tradicionales con computadoras interconectadas mediante equipo de red para emular una red en producción, sin embargo, este tipo de laboratorios presentan grandes obstáculos para el cumplimiento de los objetivos pedagógicos y no escalan bien cuando crece el número de estudiantes, además de que se requiere una gran inversión por parte de las IES (Wu, Fulmer, & Johnson, 2014)

Una alternativa es el uso de alguna plataforma de cómputo en la nube como Amazon Web Services (AWS), la cual ofrece diversos recursos para capacitar a los estudiantes con una experiencia práctica, la cual es indispensable en el mundo laboral. Además, AWS ofrece un programa gratuito de acceso libre llamado AWS Educate, el cual permite utilizar los servicios de la nube para crear y trabajar con varias instancias de sistemas operativos y poder virtualizar un laboratorio (Amazon Web Services, 2022).

AWS Educate, ofrece al personal docente y a los estudiantes máquinas virtuales bajo demanda, elásticas, dedicadas, aisladas, prácticamente ilimitadas y fácilmente configurables. Por lo tanto, emplear este tipo de laboratorios puede tener varias ventajas frente a los laboratorios clásicos.

El objetivo de este trabajo es explorar la viabilidad de utilizar el AWS Educate para la implementación de un laboratorio virtual de seguridad en redes analizando sus ventajas y desventaja. Los resultados muestran que AWS Educate presenta varias ventajas útiles para la implementación de un laboratorio virtual de seguridad en redes, entre las que destacan la disponibilidad de los recursos las 24 horas del día, los 7 días de la semana, la independencia de la ubicación del estudiante, y el uso de recursos bajo demanda.

Metodología

La presente investigación se abordó desde un análisis descriptivo, el cual consiste en describir las tendencias claves en los datos existentes y observar las situaciones que conduzcan a nuevos hechos (Hernández S., Fernández C., & Baptista L. , 2016), el propósito principal de este estudio es conocer las opciones que ofrece AWS Educate para la implementación de un laboratorio virtual de seguridad en redes, así como identificar aspectos de relevancia y herramientas útiles en la implementación de este.

Para la recolección de la información se realizó una búsqueda en diversas fuentes, tomando en consideración aspectos pedagógicos propios del uso de laboratorios virtuales, independientemente del área de conocimiento, hasta aspectos específicos de laboratorios virtuales utilizados para la enseñanza de seguridad en redes.

Resultados

En general, el diseño de laboratorios de seguridad de redes requiere características específicas y se tienen que seguir ciertas pautas como se describe en Abler R.T., et. al (2006), Brustoloni (2006) y Nance K. , et al. (2009). En resumen, las computadoras del laboratorio deben tener conectividad a Internet para poder descargar las herramientas necesarias y acceder a información en línea, además deben estar aisladas de la(s) red(es) del campus, el entorno de red debe ser lo más realista posible, el laboratorio debe poder configurarse de manera que sea fácil de administrar, asignar y escalar los recursos para diferentes asignaciones prácticas y tareas, se debe contar los suficiente de técnicos de TI para brindar un mantenimiento adecuado y resolver los problemas que se presenten de forma rápida, y finalmente debe ser accesible desde cualquier lugar donde se encuentren los estudiantes.

En la literatura, se reportan varias formas de implementar laboratorios para la enseñanza de seguridad en redes. Una de ellas es utilizar un entorno de laboratorio tradicional con múltiples máquinas físicas interconectadas a través de dispositivos de red (ruteadores y conmutadores) y utilizando dispositivos de seguridad (firewalls, sistemas de detección de intrusos, honeypots, entre otros). Algunas de estas plataformas de laboratorios se describen en Abler R.T., et al. (2006) y Brustoloni (2006). Una de las principales ventajas de este tipo de laboratorios es la capacidad de proporcionar una experiencia realista con equipos de hardware reales. Sin embargo, este enfoque clásico es muy costoso para las IES y tiene claras desventajas relacionadas con la instalación, configuración y administración del equipo.

Otro enfoque común utilizado para brindar capacitación práctica en seguridad en redes es el uso de herramientas de virtualización para establecer laboratorios de seguridad accesibles de forma remota (Wu, Fulmer, & Johnson, 2014), (Saliah-Hassane, et al., 2011) y (Sultan , 2010) . Estos laboratorios facilitan las prácticas de seguridad en redes, ya que los estudiantes pueden configurar una gran cantidad de máquinas virtuales en red para realizar ataques e implementar contramedidas para defender la infraestructura red. El uso de la tecnología de virtualización para construir laboratorios virtuales de seguridad de redes se describe con detalle en McClure, Scambray, & Kurtz (2012), Mirkovic & Benzel (2012), Nance K., et al. (2009). Uno de los principales inconvenientes que presentan estos entornos de laboratorios virtuales es que no son escalables y no brindan recursos abiertos y de fácil acceso a los estudiantes y personal docente.

Un tercer enfoque es el uso de plataformas de cómputo en la nube, en Alshuwaier, Alshwaier, & Areshe (2012), Boyatt & Sinclair (2013), Huang & Yang (2013), Peng (2013), Masud, Huang, & Yong (2012) y Ali, Smith, & Leslie (2018), se analiza el papel fundamental que puede desempeñar la computación en la nube en la educación y el aprendizaje a distancia. La mayoría de estos trabajos describen cómo la tecnología de cómputo en la nube puede ser un facilitador clave en la educación, destacando los importantes beneficios que ofrece a las instituciones, profesores y estudiantes.

Estas plataformas pueden ser muy atractivas para capacitar a los estudiantes con una experiencia práctica en seguridad en redes que es indispensable en el campo laboral. Según Peng (2013), gracias a los servicios de cómputo en la nube, es posible que los estudiantes de forma remota realicen tareas prácticas y adquieran experiencia. Los laboratorios basados en cómputo en la nube tienen ventajas sobre los laboratorios tradicionales, ya que permiten que los recursos del laboratorio se amplíen o se reduzcan en función del número de estudiantes. Es por esto por lo que muchas IES en el mundo han comenzado a utilizar los servicios en la nube para impartir algunos de sus cursos (Taleb & Mohamed, 2020).

Una de las plataformas de cómputo en la nube más populares en la actualidad es Amazon Web Services (AWS), la cual es una colección de servicios informáticos remotos que Amazon ofrece a través de Internet. AWS ofrece una infraestructura como servicio (IaSS, por sus siglas en inglés), en la que los recursos del sistema se pueden proporcionar a los usuarios en términos de instancias de Elastic Compute Cloud (EC2). Las instancias EC2 son básicamente unidades de cómputo o máquinas virtuales que pueden ejecutar cualquier aplicación de software. Se ofrecen en diferentes tamaños que van desde “t1.micro” con un

núcleo y 613 MB de memoria hasta "h1.4xlarge" con 16 núcleos y 60 GB de memoria (Amazon Web Services, 2022). Las instancias de cualquier tipo se lanzan desde Amazon Machine Images (AMI). Una AMI es una plantilla que contiene un sistema operativo preconfigurado, paquetes de software, herramientas y bibliotecas a elección del usuario. Con una AMI se pueden iniciar una o varias instancias. Amazon proporciona diferentes tipos de AMI que pueden estar basadas en Windows o Linux.

Precisamente, esta característica de AWS, que permite a los usuarios crear sus propias AMI, es un elemento clave en la implementación de laboratorios virtuales. Por ejemplo, para un laboratorio particular, un profesor puede simplemente comenzar con una AMI base, que ya incluye un sistema operativo básico como Windows o Linux, iniciar la respectiva instancia, instalar el software necesario y hacer las pruebas requeridas para asegurarse de que todo el software instalado funcione correctamente. Posteriormente, el profesor puede crear una nueva AMI a partir de esta instancia y ponerla a disposición de los estudiantes (Amazon Web Services, 2022). Cuando los estudiantes inicien la AMI, no será necesario que realicen ningún tipo de instalación, configuración o resolución de problemas, ya que todo el software instalado funcionará correctamente. De esta forma, los profesores y los estudiantes no se distraerán con las actividades de configuración y administración, y pueden concentrarse principalmente en realizar las prácticas de laboratorio que satisfagan de manera adecuada los objetivos del curso.

En un laboratorio de seguridad en redes, la capacidad de crear y utilizar AMI preconfiguradas con las herramientas de seguridad y los paquetes de software necesarios es una gran ventaja, ya que algunas herramientas de ciberseguridad son fáciles de instalar y configurar, tales como Zenmap (2022), Wireshark (2022), OpenSSL (2022) y Openwall (2022), por mencionar algunas. Sin embargo, muchas otras herramientas como Snort (2022), Nessus (2022), Nexpose (2022), Maltego (2022) y Metasploit (2022), entre otras, son conocidas por ser difíciles de instalar y configurar. Por ejemplo, Snort, que es un sistema de prevención y detección de intrusos de código abierto, requiere la instalación y configuración de varias aplicaciones y paquetes de software compatibles tales como, PHP, Libcap, MySQL, Apache Webserver, Daemonlogger, BASE y muchos otros (Snort, 2022). Para los estudiantes que no están familiarizados con Linux, instalar Snort puede ser una tarea abrumadora. Por el contrario, al usar AWS, el profesor simplemente puede desarrollar una AMI que tenga Snort correctamente instalado y ponerla a disposición de los estudiantes. Posteriormente, los

estudiantes solo necesitan lanzar instancias desde esa AMI y realizar directamente las actividades propuestas de Snort.

Hay muchos otros beneficios de utilizar AWS, en primer lugar, los estudiantes pueden asignar recursos y lanzar instancias de forma rápida y elástica. Si las instancias fallan, los estudiantes pueden iniciar rápidamente otras nuevas. Esta es una característica deseable, especialmente cuando se ejecutan herramientas y software de seguridad que a menudo fallan y/o causan problemas a los sistemas operativos. En segundo lugar, las instancias que se ejecutan en la nube no afectan las redes en producción. Por lo tanto, los estudiantes realizan ejercicios de seguridad en redes dentro un entorno seguro y contenido. En tercer lugar, a menudo los gobiernos y las IES bloquean sitios web no deseados que se sabe que contienen contenido malicioso. Al impartir un curso de seguridad en redes, se necesita que los estudiantes accedan a estos sitios para poder descargar herramientas o familiarizarse con sus contenidos. Al utilizar AWS, estos sitios web están disponibles para los estudiantes. En cuarto lugar, los profesores pueden solucionar problemas y calificar el trabajo de los estudiantes de forma remota y efectiva. En quinto lugar, las instituciones pueden evitar la operación de laboratorios físicos, que generalmente implican una gran cantidad de costos administrativos, instalaciones y mantenimiento. Finalmente, en sexto lugar se elimina el problema de los estudiantes que compiten por recursos de laboratorio limitados durante los períodos de mayor demanda (por ejemplo, cuando se acerca la fecha límite de entrega de una tarea o actividad). Como resultado, los estudiantes pueden trabajar en sus tareas de acuerdo con sus propios horarios desde cualquier lugar y en cualquier momento.

Una limitante de AWS es que utiliza un modelo de pago por uso para los recursos de la nube. Para reducir los cargos asociados al uso de AWS, se puede utilizar AWS Educate, que es una plataforma que brinda a los estudiantes la posibilidad de explorar muchos de los servicios de AWS sin costo alguno para ellos o la institución (Amazon Web Services, 2022). Antes de la aparición de AWS educate, cuando los estudiantes querían utilizar los servicios de AWS, tenían que disponer de una tarjeta de crédito e incurrir en costos por usar sus servicios.

Actualmente, para que los estudiantes tengan acceso a todos los recursos en la nube, AWS Educate les proporciona un crédito de $100 que puede aplicarse a cualquier servicio facturable consumido mientras exploran las tecnologías de AWS. Los servicios facturables comunes incluyen la asignación de almacenamiento basada en nube, recursos informáticos que ejecutan servidores basados en la nube y servicios de transferencia de datos. Aunque

AWS proporciona algunos servicios gratuitos, estos servicios son limitados y algunos costos son inevitables, pero pueden ser absorbidos por los créditos otorgados. Si un estudiante consume todos sus créditos, no podrá utilizar servicios adicionales facturables hasta que obtenga crédito adicional, ya sea mediante una asignación anual o mediante alguna otra oferta de créditos para estudiantes (Amazon Web Services, 2022).

AWS Educate también permite a los profesores crear un entorno de aula basado en la nube donde los estudiantes reciben créditos de AWS específicos para esa aula, evitando que consuman los créditos de su cuenta personal. Esto permite que los profesores puedan controlar y supervisar los recursos de los estudiantes para un curso especifico.

Una de las principales ventajas de AWS Educate, es que se elimina la necesidad de que la IES adquiera instalaciones y laboratorios locales para albergar, administrar y mantener el laboratorio, y al mismo tiempo brinda fácil acceso al equipo de laboratorio necesario las 24 horas del día, los 7 días de la semana.

Para poder utilizar AWS Educate, el primer paso es que la Institución se registre como miembro del programa, este proceso es gratuito, pero requiere un signatario autorizado y un punto de contacto central (CPOC, por sus siglas en inglés) en la institución. Este paso solo debe realizarse una vez ya que la membresía no caduca (Amazon Web Services, 2022).

El siguiente paso es que el profesor se registre como instructor y luego solicite la creación de un aula. Durante el proceso de solicitud se le pedirá que ingrese el número del curso, el nombre del curso, el enlace de información del curso, la fecha de inicio y la fecha de finalización. Además de esta información, los profesores deben ingresar un número estimado de estudiantes y solicitar un valor en dólares de créditos AWS. Si la solicitud de créditos es de $50 o menos, no se requiere ninguna justificación adicional, en caso contrario se debe incluir una justificación que contenga las actividades específicas a realizar en el aula y los servicios que se utilizarán, así como los costos estimados (Amazon Web Services, 2022).

Para completar el proceso de solicitud de aula, se debe proporcionar la lista de nombres de estudiantes, así como sus correos institucionales. La cantidad máxima de estudiantes que se pueden invitar a un aula es de 75. Las solicitudes de aula generalmente se aprueban en tres o cuatro días, pero AWS Educate solicita hasta seis días hábiles para completar el proceso (Amazon Web Services, 2022).

Una vez aprobada la solicitud del aula, se enviará a los estudiantes un correo electrónico de invitación. En este se les indica las instrucciones que tiene que seguir para

iniciar sesión en AWS Educate o crear una cuenta si aún no la tienen. Inicialmente el salón de clase estará en un estado inactivo y permanecerá de esa forma hasta que el profesor active la clase. Los estudiantes no pueden ingresar al salón hasta que este activo. Una vez que los estudiantes hayan iniciado sesión, se desplegará una pantalla dando información general de la cuenta y el estudiante puede comenzar a utilizar los servicios de AWS.

Discusión

Entre las principales ventajas de usar como plataforma AWS educate para enseñar seguridad en redes, está la reducción de costos para las IES y los estudiantes, ya que no necesitan comprar una computadora que cumpla con requisitos específicos; lo único que se necesita es una computadora promedio con acceso a Internet, además, las IES no tienen que preocuparse por aumentar las instalaciones de los laboratorios sin importar cuántos estudiantes tengan, ya que esta plataforma es escalable y puede soportar cualquier número de estudiantes. Otra de las ventajas es que los estudiantes no necesitan ningún tipo de software, sistema operativo ni ningún tipo de configuración especial (Leih, 2021).

Además, AWS Educate brinda a los estudiantes la capacidad de explorar muchos servicios de AWS sin costo directo y sin la necesidad de ingresar la información de una tarjeta de crédito. Varios servicios de AWS, como las instancias EC2 se pueden usar sin costo y muchos otros servicios consumen muy pocos créditos de AWS si se administran correctamente.

En un laboratorio tradicional, las tareas de configurar, instalar, programar y administrar equipos de laboratorio y estaciones de trabajo pueden convertirse en una carga excesiva para los técnicos de laboratorio y los profesores, esto no sucede cuando se hace uso de AWS. Además, en este tipo de laboratorios, un gran porcentaje del tiempo del profesor a menudo se dedica a solucionar problemas de configuración ocasionados por los estudiantes. Esto causa que el profesor no pueda concentrarse en los aspectos pedagógicos de su curso. Por otro lado, en este tipo de laboratorios, también los estudiantes pueden frustrarse fácilmente, debido a la presencia de errores de configuración e instalación de las herramientas necesarias para la realización de las prácticas. Otro problema presente es la asignación del uso del laboratorio para clases con un gran número de estudiantes, especialmente antes de las fechas límite de entrega de alguna tarea.

En resumen, con la configuración de un laboratorio clásico, las tareas prácticas pueden desviarse fácilmente de ser ejercicios significativos y enfocados al aprendizaje a convertirse en tareas innecesarias de configuración, instalación, recuperación, administración y programación, tanto para profesores como para estudiantes.

En cuanto a los entornos y plataformas de laboratorios virtuales como los propuestos en Habib M.N., et al. (2021), Kratzke, (2012), Saliah-Hassane, et al. (2011) y Tamer & Lunsford (2017), estos no son escalables y no brindan recursos abiertos y de fácil acceso para estudiantes y profesores. Generalmente, para que los estudiantes puedan establecer una conexión a estos laboratorios, es necesario que configuren su propia VPN de forma apropiada y los permisos correspondientes. Por el contrario, con una nube pública como AWS, no hay necesidad de conexiones VPN porque los accesos a las instancias EC2 siempre están garantizados, la escalabilidad y la elasticidad están aseguradas.

Por lo tanto, un laboratorio implementado en una plataforma de cómputo en la nube como AWS, puede satisfacer y solucionar la mayoría de los requisitos y problemas que se presentan en los laboratorios clásicos.

Amazon Web Services (AWS) ofrece máquinas virtuales (o instancias en el lenguaje de AWS) como infraestructura como servicio (IaaS, por sus siglas en inglés). IaaS es la base de todos los servicios en la nube, por lo que permite aprovisionar y controlar software y recursos informáticos fundamentales, incluidas diversas capacidades de CPU, memoria y disco, así como sistemas operativos, bibliotecas y aplicaciones arbitrarias necesarias para ejercicios prácticos sobre seguridad en redes (Amazon Web Services, 2022). Aunque existen otros modelos de servicios en la nube como la plataforma como servicio (PaaS) y el software como servicio (SaaS), estos solo brindan servicios de aplicaciones y middleware que son administrados y controlados principalmente por proveedores de la nube. Por lo tanto, con PaaS y SaaS, los usuarios (profesores y estudiantes) no pueden tener un control detallado o acceso administrativo sobre los sistemas operativos, las bibliotecas y los servicios de red, que son fundamentales para llevar a cabo cualquier laboratorio útil y práctico de seguridad en redes (Tamer & Lunsford, 2017).

Conclusiones

AWS Educate, ofrece un ambiente aislado, donde los estudiantes reciben un entorno estable con un límite de crédito de AWS establecido, de tal manera que los profesores pueden crear laboratorios de seguridad en redes con un alto nivel de similitud con una red en producción. Además, los estudiantes no necesitan proporcionar información de tarjetas de crédito, ni preocuparse por gastos inesperados ocasionados por la incorrecta administración de los servicios en la nube. Esto sugiere que AWS Educate es un recurso efectivo en el desarrollo de un laboratorio de seguridad en redes, ya que proporciona un entorno excelente para que los estudiantes experimenten ejercicios prácticos.

AWS es una gran alternativa para implementar un laboratorio de seguridad en redes, ya que presenta muchos beneficios, por mencionar algunos: AWS permite que los profesores puedan crear fácilmente AMI preconfiguradas con las herramientas de seguridad y los paquetes de software necesarios solo una vez y reutilizarlas siempre que se requieran. AWS permite a los estudiantes asignar recursos y aprovisionar de forma rápida y elástica las instancias EC2, además de proporcionar un entorno contenido y seguro, en el que las instancias no afectan en absoluto a las redes en producción; asimismo otorga a los profesores la capacidad de monitorear, solucionar problemas y calificar el trabajo de los estudiantes de forma remota y directamente dentro de sus instancias, y finalmente con el uso de AWS las IES evitan las costosas operaciones de mantenimiento y programación de los laboratorios físicos.

Futuras líneas de investigación

En trabajos futuros, se propone la implementación un laboratorio para seguridad en redes basado en AWS Educate, para realizar un estudio que determine el grado de satisfacción de los estudiantes al utilizar este tipo de laboratorios, así como determinar si el uso de AWS Educate mejora el desempeño de habilidades prácticas de los estudiantes en los cursos de seguridad en redes.

Referencias

Abler R.T., Contis D., Grizzard J. B., & Owen, H. (2006). Georgia Tech Information Security Center Hands-On Network Security Laboratory. *IEEE Transaction Education, 49*(1), 82-87. doi:10.1109/TE.2005.858403

Ali, A., Smith, D. T., & Leslie, T. A. (2018). Issues and Challenges Facing the Teaching of Cloud Computing. *Issues in Information Systems, 19*(4), 187-195. doi:https://doi.org/10.48009/4_iis_2018_187-195

Alshuwaier, F., Alshwaier, A., & Areshe, A. (2012). Applications of cloud computing in education. *8th International Conference on Computing and Networking Technology (INC, ICCIS and ICMIC)*, (págs. 26-33).

Amazon Web Services. (2022). Obtenido de Amazon Elastic Compute Cloud Documentation. User Guide: https://docs.aws.amazon.com/ec2/index.html

Amazon Web Services. (5 de 10 de 2022). *AWS Educate.* Obtenido de https://aws.amazon.com/es/education/awseducate/

Amazon Web Services. (5 de 10 de 2022). *Introducción a AWS*. Obtenido de Introducción a Amazon Web Services: https://aws.amazon.com/es/getting-started/

Boyatt, R., & Sinclair, J. (2013). Meeting learners' needs inside the educational cloud. *International Journal of Learning Technology, 8*(1), 61–85. doi:10.1504/IJLT.2013.052827

Brustoloni, J. C. (Diciembre de 2006). Laboratory experiments for network security instruction. *Journal on Educational Resources in Computing, 6*(4), 5-es. doi:10.1145/1248453.1248458

Dijiang Huang, L., & Tsai, W.-T. (2014). Cloud-Based Virtual Laboratory for Network. *IEEE Ttransaction on Education, 57*(3), 145-150. doi: 10.1109/TE.2013.2282285

Duffy, C. (30 de 05 de 2021). *Se busca: millones de expertos en ciberseguridad. Salario: lo que pidas*. Obtenido de CNN español: https://cnnespanol.cnn.com/2021/05/30/se-busca-millones-expertos-ciberseguridad-salario-trax/

Habib M.N., Jamal W., Khalil U., & Khan Z. (2021). Transforming universities in interactive digital platform: case of city university of science and information technology. *Education and Information Technologies, 26*(1), 517-541. doi:10.1007/s10639-020-10237

Hernández S., R., Fernández C., C., & Baptista L. , P. (2016). *Metodología de la Investigación* (6ta. ed.). México: McGraw Hill.

Huang, L., & Yang, Y. (2013). Facilitating education using cloud computing infrastructure. *Journal of Computing Sciences in Colleges, 28*(4), 19–25.

Kratzke, N. (2012). Virtual Labs in Higher Education of Computer Science Why they are Valuable? How to Realize? How much will It Cost? *Scientific & Academic Publishing, 2*(7). doi:10.5923/j.edu.20120207.04

Leih, M. (2021). Leveraging AWS Educate Classrooms in Cloud Computing Courses. *EDSIGCON Proceedings 2021*, (págs. 1-8). Washington DC. Obtenido de https://proc.iscap.info; https://iscap.info

Maltego. (2022). Obtenido de Maltego.com: https://www.maltego.com/?utm_source=paterva.com&utm_medium=referral&utm_campaign=301

Masud, A. H., Yong, J., & Huang, X. (2012). Cloud Computing for Higher Education: A roadmap. *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 552-557. doi:10.1109/CSCWD.2012.6221872

McClure, S., Scambray, J., & Kurtz, G. (2012). *Hacking Exposed 7* (7th Edition ed.). Nueva York, USA: McGraw-Hill.

Metasploit. (2022). Obtenido de Metasploit | Penetration Testing Software, Pen Testing Security: http://www.metasploit. com/

Mirkovic, J., & Benzel, T. (2012). Teaching cybersecurity with DeterLab. *IEEE Security Privacy Magazine, 10*(1), 73-76. doi:10.1109/MSP.2012.23

Nance , K., Hay, B., Dodge, R. C., Seazzu, A., & Burd, S. (2009). Virtual Laboratory Environments: Methodologies for Educating Cybersecurity Researchers. *Methodological Innovations Online, 4*(3), 3-14. doi:10.4256/mio.2010.0002

Nessus. (2022). Obtenido de Dowland Nessus Vulnerabity Assesment: https://www.tenable.com/products/nessus

Nexpose. (2022). Obtenido de Rapid7.com: https://www.rapid7.com/products/nexpose/

OEA. (2020). *Educación en ciberseguridad. Planificación del futuro mediante el desarrollo de la fuerza laboral.* White paper series Edición 9, Organización de los Estados Americanos. Recuperado el 25 de 06 de 2022, de https://www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf

OpenSSL. (2022). Obtenido de https://www.openssl.org/

Openwall. (2022). Obtenido de John the Ripper password cracker: https://www.openwall.com/john/

Pastor, N. (04 de 2022). *España ya tiene déficit de expertos en ciberseguridad y la demanda sigue aumentando*. Obtenido de La Vanguardia: https://www.lavanguardia.com/economia/20220401/8161871/espana-deficit-expertos-ciberseguridad-demanda-sigue-aumentando-nuclio-brl.html

Peng, H. (2013). The Application of Cloud Computing Technology in Distance Education Network. *2013 International Conference on Computer Sciences and Applications*, 681-683. doi:10.1109/CSA.2013.164

Petersen, R., Santos, D., Smith, M., Wetzel, K., & Witte, G. (2020). *Workforce Framework for Cybersecurity (NICE Framework).* National Institute of Standards and Technology. NIST. doi:10.6028/NIST.SP.800-181r1

Salah, K., Hammoud, M., & Zeadally, S. (2015). Teaching Cybersecurity Using the Cloud. *IEEE Transaction on Learning Technologies, 8*(4), 383-392. doi:10.1109/TLT.2015.2424692.

Saliah-Hassane, H., Saad, M., Ofosu, W., Karimou, D., Hassane, A. M., & Amadou, M. D. (2011). Lab@Home: Remote Laboratory Evolution in the Cloud Computing Era. *2011 ASEE Annual Conference & Exposition.* Vancouver, Canada. doi:10.18260/1-2--18691

Snort. (2022). Obtenido de Snort - Network Intrusion Detection & Prevention System: https://snort.org/

Sultan , N. (2010). Cloud computing for education: A new dawn? *International Journal of Information Management, 30*, 109-116. Obtenido de https://www.journals.elsevier.com/international-journal-of-information-management

Taleb, N., & Mohamed, E. (2020). Cloud Computing Trends: A Literature Review. *Academic Journal of Interdisciplinary Studies, 9*(1), 91-104. doi:10.36941/ajis-2020-0008

Tamer, R. O., & Lunsford, P. (2017). Networks Security Lab Support: A Case Study for Problems Facing Distance Education Programs. *Computer Science*. doi:10.18260/1-2--28702

Wireshark. (2022). Obtenido de Wireshark Go Deep: https://www.wireshark.org/

Wu, D., Fulmer, J., & Johnson, S. (2014). Teaching Information Security with Virtual Laboratories. En J. Carroll, *Innovative Practices in Teaching Information Sciences and Technology* (págs. 179–192). Springer. doi:10.1007/978-3-319-03656-4_16

Zenmap. (2022). Obtenido de Zenmap - Official cross-plataform Nmap Security Scanner GUI: https://nmap.org/zenmap/