MASTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIONES

Y

MASTER UNIVERSITARIO EN CIBERSEGURIDAD

TRABAJO FIN DE MASTER

METODOLOGÍA DE ANÁLISIS DE SEGURIDAD EN CLOUD

Autor: Ana Leticia Urbistondo Murua

Director: Antonio Pérez Sánchez

Madrid

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

Metodología de Análisis de Seguridad en Cloud

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el curso académico **2021/22** es de mi autoría, original e inédito y no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido tomada de otros documentos está debidamente referenciada.

Fdo.: Ana Leticia Urbistondo Murua Fecha: 04/07/2022

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Fdo.: Antonio Pérez Sánchez Fecha: 04/07/2022

AUTORIZACIÓN PARA LA DIGITALIZACIÓN, DEPÓSITO Y DIVULGACIÓN EN RED DE PROYECTOS FIN DE GRADO, FIN DE MÁSTER, TESINAS O MEMORIAS DE BACHILLERATO

1º. Declaración de la autoría y acreditación de la misma.

El autor D. **Ana Leticia Urbistondo Murua** DECLARA ser el titular de los derechos de propiedad intelectual de la obra: **Metodología de análisis de seguridad en Cloud**, que ésta es una obra original, y que ostenta la condición de autor en el sentido que otorga la Ley de Propiedad Intelectual.

2º. Objeto y fines de la cesión.

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad, el autor **CEDE** a la Universidad Pontificia Comillas, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, los derechos de digitalización, de archivo, de reproducción, de distribución y de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual. El derecho de transformación se cede a los únicos efectos de lo dispuesto en la letra a) del apartado siguiente.

3º. Condiciones de la cesión y acceso

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia habilita para:

a) Transformarla con el fin de adaptarla a cualquier tecnología que permita incorporarla a internet y hacerla accesible; incorporar metadatos para realizar el registro de la obra e incorporar "marcas de agua" o cualquier otro sistema de seguridad o de protección.
b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.
c) Comunicarla, por defecto, a través de un archivo institucional abierto, accesible de modo libre y gratuito a través de internet.
d) Cualquier otra forma de acceso (restringido, embargado, cerrado) deberá solicitarse expresamente y obedecer a causas justificadas.
e) Asignar por defecto a estos trabajos una licencia Creative Commons.
f) Asignar por defecto a estos trabajos un HANDLE (URL *persistente)*.

4º. Derechos del autor.

El autor, en tanto que titular de una obra tiene derecho a:

a) Que la Universidad identifique claramente su nombre como autor de la misma
b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio.
c) Solicitar la retirada de la obra del repositorio por causa justificada.
d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

5º. Deberes del autor.

El autor se compromete a:

a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.
b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.
c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e intereses a causa de la cesión.
d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción de derechos derivada de las obras objeto de la cesión.

6º. Fines y funcionamiento del Repositorio Institucional.

La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, y con fines de estudio, investigación, o cualquier otro fin lícito. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

- La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.
- La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusive del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.
- La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro.
- La Universidad se reserva la facultad de retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Madrid, a 04 de JULIO de 2022

ACEPTA

Fdo……

Motivos para solicitar el acceso restringido, cerrado o embargado del trabajo en el Repositorio Institucional:

MASTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIONES

Y

MASTER UNIVERSITARIO EN CIBERSEGURIDAD

TRABAJO FIN DE MASTER

METODOLOGÍA DE ANÁLISIS DE SEGURIDAD EN CLOUD

Autor: Ana Leticia Urbistondo Murua

Director: Antonio Pérez Sánchez

Madrid

METODOLOGÍA DE ANÁLISIS DE SEGURIDAD EN CLOUD

Autor: Urbistondo Murua, Ana Leticia.
Director: Pérez Sánchez, Antonio
Entidad Colaboradora: NTT DATA

RESUMEN DEL PROYECTO

Este trabajo consiste en el diseño de una metodología de análisis de seguridad Cloud, donde se ha realizado un análisis exhaustivo sobre los componentes y vulnerabilidades de los principales proveedores del mercado. Con los resultados obtenidos, se ha diseñado listado de ejercicios de análisis, cuya eficiencia se ha verificado mediante una simulación en Cloud.

Palabras clave: Ciberseguridad, Cloud, ataque, análisis, metodología

1. Introducción

"Cloud Computing" se caracteriza, principalmente, en ofrecer acceso a una gran variedad de recursos de manera ágil, flexible y escalable. Actualmente, la gran mayoría de empresas, por no decir en su totalidad, deciden realizar un proceso denominado "**migrar a la nube**" [1] que consiste en trasladar su infraestructura TI fuera de su entorno local, contratando un proveedor de ***"Cloud Computing"*** para almacenar y gestionar su centro de datos. A pesar de los grandes beneficios que proporciona ***"Cloud Computing"***, se debe tener en cuenta las amenazas que puede incorporar estas nuevas tecnologías.

Como consecuencia, se han diseñado a lo largo de los años diversos controles y políticas que se encargan de enriquecer lo máximo posible la seguridad en la nube. Sin embargo, siempre se debe tener en cuenta que existe la posibilidad de que todas las medidas de seguridad, por muy eficaces sean en diseño, en algún momento de su existencia se conviertan en un futuro punto de entrada vulnerable.

Por este motivo, es de vital importancia tener un equipo de ciberseguridad que se centre en realizar diversos ejercicios de análisis ofensivos sobre la infraestructura. Este Trabajo de Fin de Máster se centrará en diseñar metodología de análisis de seguridad Cloud donde, entre otras cosas, se definirán ejercicios que permitan examinar la seguridad implementada en la infraestructura Cloud desde el punto de vista de un adversario. Para ello, se propone realizar el análisis de los tres proveedores de servicios Cloud más influyentes en el mercado actual: **"Google Cloud Platform" (GCP)**, **"Amazon Web Services" (AWS)** y "**Microsoft Azure Cloud**".

2. Definición del proyecto

Como comienzo de este trabajo se propone realizar un primer análisis sobre las estructuras y funcionalidades que presentan los proveedores en sus infraestructuras de Cloud, además de las amenazas y vulnerabilidades que suponen estas implementaciones. A través de este análisis, se busca obtener una visión general del funcionamiento estos proveedores, qué productos y soluciones ofrecen, cuáles son los productos más comúnmente utilizados y, de esta manera, descubrir posibles métodos de ataque.

Realizando una combinación de la información obtenida sobre los proveedores y los diversos métodos de trabajo existentes a la hora de realizar un análisis de ciberseguridad, se puede comenzar, finalmente, con el diseño de la metodología de ciberseguridad en la nube, intentando cubrir las amenazas más comúnmente encontradas entre los tres proveedores.

Tras finalizar con el diseño de esta metodología, se propone realizar una simulación en un entorno de nube para probar tanto las herramientas encontradas en análisis previos, como de comprobar algunos de los procesos de ataque planteados.

3. Descripción del modelo

La metodología final obtenida con este trabajo se ha conseguido a través de las siguientes implementaciones:

- **Planificación de ejercicios de Análisis de Cloud** – donde se elabora en mayor profundidad los participantes, las fases y la planificación de la ejecución de pruebas de seguridad, siguiendo el marco de trabajo de **TIBER-EU** [2].

- **Metodología de *"Cyber Kill Chain"*** – Análisis y explicación de las diferentes fases del marco de trabajo de ***"Cyber Kill Chain"*** [3], con el objetivo de clasificar los diferentes ejercicios de análisis en cada una de las categorías

- **Marco de trabajo de "MITRE ATT&CK"** – Para analizar las técnicas y tácticas de ataque previamente analizadas por analistas y organizaciones externos [4].

- **Sistema de Puntuación de vulnerabilidades** – Por el cual se realiza la puntuación de vulnerabilidades de los resultados obtenidos a través de los ejercicios diseñados [5].

- **Modelado de amenazas en entornos de nube** – Donde se realiza un análisis de los componentes, ataques y herramientas comúnmente encontrados en entornos de Cloud para cada uno de los proveedores planteados.

- **Ejercicios de análisis de seguridad** – Tras el modelado de amenazas realizado, se busca obtener un listado de ejercicios de análisis de seguridad recomendados para los entornos de nube.

La metodología final sigue la siguiente estructura:

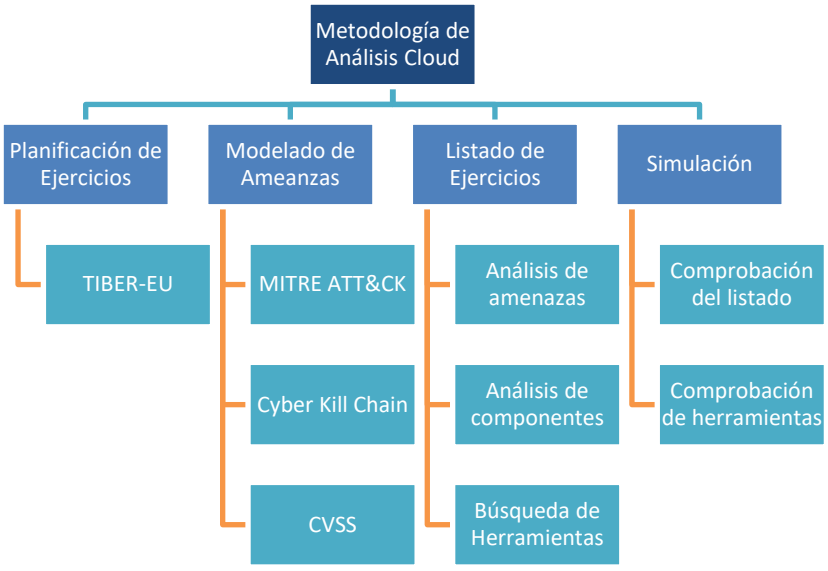

Ilustración 1. Estructura de la metodología diseñada

4. Resultados

Para la comprobación de la efectividad de la metodología diseñada, se ha procedido con la simulación de un análisis de seguridad de un entorno de nube. En él, implementando un diseño de *caja gris*, se ha procedido con la conexión de un entorno de nube, por el cual se han implementado diversos ejercicios y herramientas de análisis de seguridad, todos ellos procedentes de la fase de **Reconocimiento** de la ***"Cyber Kill Chain"***.

Los resultados en la fase de **Reconocimiento** en dicha simulación se muestran en la siguiente tabla, indicando los ejercicios de análisis que han resultado exitosos y, como consecuencia, no han pasado los controles de seguridad asociados:

(CLD-INFO) Reconocimiento		
CLD-INFO-1	Descubrimiento de usuarios	×
CLD-INFO-2	Descubrimiento de cuentas de correo	×
CLD-INFO-3	Enumeración de usuarios y cuentas de usuario predeterminados o adivinables	-
CLD-INFO-4	Enumeración de usuarios con privilegios	×
CLD-INFO-5	Descubrimiento de ***Service Principals***	×
CLD-INFO-6	Descubrimiento de Grupos	×
CLD-INFO-7	Descubrimiento de ***Tenants***	×
CLD-INFO-8	Descubrimiento de Dispositivos	×
CLD-INFO-9	Descubrimiento de Roles	×
CLD-INFO-10	Descubrimiento de Permisos	×
CLD-INFO-11	Descubrimiento de Aplicaciones	×
CLD-INFO-12	Descubrimiento de infraestructura de la nube	×
CLD-INFO-13	Descubrimiento de servicios y componentes	×
CLD-INFO-14	Descubrimiento de objetos de almacenamiento de la nube	×
CLD-INFO-15	Descubrimiento de servicios de red	×
CLD-INFO-16	Descubrimiento de políticas de contraseñas y autenticación	×
CLD-INFO-17	Descubrimiento de políticas de seguridad	×
CLD-INFO-18	Descubrimiento de software	×
CLD-INFO-19	Descubrimiento de información sistemas	×
CLD-INFO-20	Descubrimiento de localización sistemas	×
CLD-INFO-21	Descubrimiento de dominios y subdominios	×
CLD-INFO-22	Descubrimiento de permisos IAM	✓
CLD-INFO-23	Descubrimiento de ***buckets***, junto con sus accesos y permisos.	-
CLD-INFO-24	Enumeración de recursos públicos	×
CLD-INFO-25	Extracción de datos a través del Panel de servicio en la nube	-
CLD-INFO-26	Identificación de rutas de escalada de privilegios	×
CLD-INFO-27	Generación de grafos de ataque	×
CLD-INFO-28	Evaluación de nivel de seguridad	×
CLD-INFO-29	Rastreo de red y eventos	×
CLD-INFO-30	Revisión de fuga de información en comentarios y metadatos	-
CLD-INFO-31	Identificación de puntos de entrada de la aplicación	-
CLD-INFO-32	Reconocimiento del ***framework*** usado en la aplicación	-
CLD-INFO-33	Enumeración de la arquitectura Red y de la Aplicación	-

Tabla 1. Resultados obtenidos en la simulación de análisis de seguridad

5. Conclusiones

Este trabajo no solo ha permitido conocer y estudiar tanto el funcionamiento de entorno de nube, sino que además se ha analizado diversas metodologías, ejercicios y herramientas de ataque comúnmente implementados en entorno de nube, permitiendo trabajar con diversas herramientas de análisis para seguridad Cloud.

En conclusión, se ha conseguido diseñar una nueva metodología de análisis que tiene como objetivo principal: estudiar las nuevas tecnologías, ayudar a empresas y trabajadores a realizar sus análisis de seguridad y, por último, mejorar los niveles de seguridad en cualquier entorno de nube.

6. Referencias

[1] Oracle, «Oracle Cloud Computing» 2022. [En línea]. Available: https://www.oracle.com/es/cloud/what-is-cloud-computing/.

[2] European Central Bank, «What is TIBER-EU?,» European Central Bank | EUROSYSTEM, 2022. [En línea]. Available: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html#:~:text=TIBER%2DEU%20is%20the%20European,carrying%20out%20a%20controlled%20cyberattack..

[3] Lockheed Martin, «The Cyber Kill Chain» 2022. [En línea]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[4] ATT&CK, MITRE, «Getting Started with ATT&CK,» 10 2016. [En línea]. Available: https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf.

[5] NIST, «Vulnerability Metrics,» 2022. [En línea]. Available: https://nvd.nist.gov/vuln-metrics/cvss.

CLOUD SECURITY ANALYSIS METHODOLOGY

Author: Urbistondo Murua, Ana Leticia.
Supervisor: Pérez Sánchez, Antonio.
Collaborating Entity: NTT DATA

ABSTRACT

This work consists of the design of a Cloud security analysis methodology, where an analysis has been carried out on the components and vulnerabilities of the main providers in the current market. With the results obtained, a list of analysis exercises has been designed, whose efficiency has been verified through a simulation on a cloud environment.

Keywords: Cybersecurity, Cloud, attack, analysis, methodology

1. Introduction

"***Cloud Computing***" is commonly characterized by offering access to a wide variety of resources in an agile, flexible, and scalable manner. Currently, a vast majority of companies, if not all of them, decide to carry out a process called "***migration to the cloud***" [1], which consists of moving their IT infrastructure outside their local environment, hiring a "***Cloud Computing***" provider in the process to store and manage their data center. Despite the great benefits provided by "***Cloud Computing***", the threats that these new technologies can incorporate must always be taken into consideration.

Consequently, a vast variety of controls and policies have been designed over the years in order to enrich cloud security as much as possible. However, it should always be borne in mind that there is a possibility that all security measures, no matter how effective by design, may at some point in their existence become a future vulnerable point of entry.

For this reason, it is vitally important to have a cybersecurity team that focuses on performing various offensive analysis exercises on the infrastructure. This Master's Thesis will focus on designing a Cloud security analysis methodology where, among other things, exercises will be defined which will enable the security implemented in the Cloud infrastructure to be examined from the point of view of an adversary. For this, an analysis on the three most influential Cloud service providers in the current market will be carried out: "**Google Cloud Platform" (GCP),** "**Amazon Web Services" (AWS)** and "**Microsoft Azure Cloud**".

2. Project definition

Firstly, an analysis on the structures and functionalities that the providers present in their Cloud infrastructures, in addition to the threats and vulnerabilities associated, will be carried out. Through this analysis, the main objective is to obtain an overview of how these providers work, what products and solutions they offer, which are the most used products and, consequently, discover possible attack methods.

Combining the information obtained on the providers and the various existing work methods carried out regarding cybersecurity analysis, it is possible to finally start with the design of the cybersecurity methodology on Cloud, trying to cover the most commonly found threats and vulnerabilities among these three providers.

Once the design of this methodology is finished, a simulation in a cloud environment will be carried out in order to, on one hand test the tools found in previous analysis and, on the other hand, check some of the proposed attack processes.

3. Model description

The final methodology designed in this project has been achieved through the following implementations:

- **Planning of Cloud Analysis exercises** – where the participants, phases, and planning of the execution of security tests are elaborated in greater depth, following the **TIBER-EU** framework [2].

- "**Cyber Kill Chain" Methodology** – A more profound analysis on the different phases of the "**Cyber Kill Chain**" framework [3] has been carried out in order to classify the different analysis exercises.

- "**MITER ATT&CK" framework** – To analyze attack techniques and tactics previously analyzed by external analysts and organizations [4].

- **Vulnerability Scoring System** –To score the results of the analysis exercises carried out [5].

- **Threat modeling in cloud environments** – Where an analysis on the most common components, attacks and tools in Cloud environment is carried out for each of the previously mentioned providers.

- **Security analysis exercises** – After the threat modeling has been carried out, the main objective is to design a list of security analysis exercises recommended for a Cloud environment.

The final methodology implements the following structure:

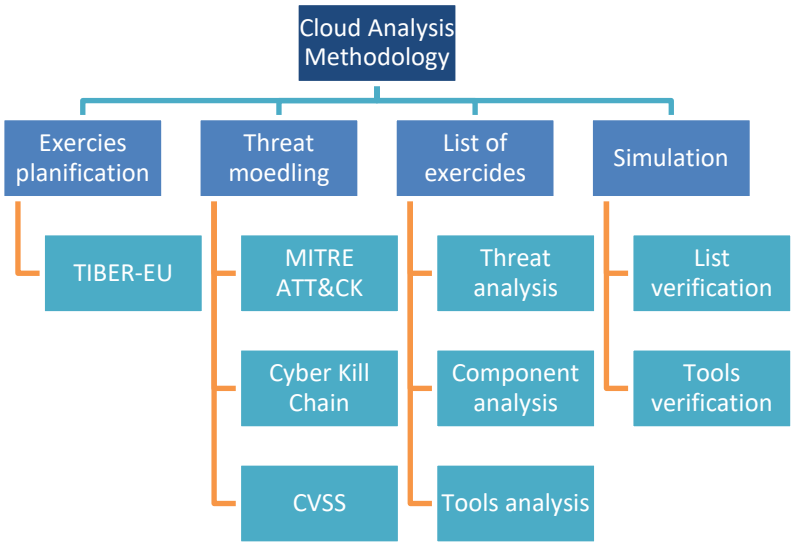

Illustration 1. Structure of the designed methodology

4. Results

To verify the effectiveness of the designed methodology, a security analysis simulation of a cloud environment has been carried out. In it, by implementing a *gray box* design with a connection to an **"Azure**" Cloud environment, various exercises and security analysis tools have been implemented, all of them included on the **Reconnaissance** phase of the "**Cyber Kill Chain**".

The results in the **Reconnaissance** phase obtained through the simulation are shown in the following table, indicating the analysis exercises that have been successful and, consequently, have not passed the associated security controls:

(CLD-INFO) Reconocimiento		
CLD-INFO-1	Descubrimiento de usuarios	×
CLD-INFO-2	Descubrimiento de cuentas de correo	×
CLD-INFO-3	Enumeración de usuarios y cuentas de usuario predeterminados o adivinables	-
CLD-INFO-4	Enumeración de usuarios con privilegios	×
CLD-INFO-5	Descubrimiento de ***Service Principals***	×
CLD-INFO-6	Descubrimiento de Grupos	×
CLD-INFO-7	Descubrimiento de ***Tenants***	×
CLD-INFO-8	Descubrimiento de Dispositivos	×
CLD-INFO-9	Descubrimiento de Roles	×
CLD-INFO-10	Descubrimiento de Permisos	×
CLD-INFO-11	Descubrimiento de Aplicaciones	×
CLD-INFO-12	Descubrimiento de infraestructura de la nube	×
CLD-INFO-13	Descubrimiento de servicios y componentes	×
CLD-INFO-14	Descubrimiento de objetos de almacenamiento de la nube	×
CLD-INFO-15	Descubrimiento de servicios de red	×
CLD-INFO-16	Descubrimiento de políticas de contraseñas y autenticación	×
CLD-INFO-17	Descubrimiento de políticas de seguridad	×
CLD-INFO-18	Descubrimiento de software	×
CLD-INFO-19	Descubrimiento de información sistemas	×
CLD-INFO-20	Descubrimiento de localización sistemas	×
CLD-INFO-21	Descubrimiento de dominios y subdominios	×
CLD-INFO-22	Descubrimiento de permisos IAM	✓
CLD-INFO-23	Descubrimiento de ***buckets***, junto con sus accesos y permisos.	-
CLD-INFO-24	Enumeración de recursos públicos	×
CLD-INFO-25	Extracción de datos a través del Panel de servicio en la nube	-
CLD-INFO-26	Identificación de rutas de escalada de privilegios	×
CLD-INFO-27	Generación de grafos de ataque	×
CLD-INFO-28	Evaluación de nivel de seguridad	×
CLD-INFO-29	Rastreo de red y eventos	×
CLD-INFO-30	Revisión de fuga de información en comentarios y metadatos	-
CLD-INFO-31	Identificación de puntos de entrada de la aplicación	-
CLD-INFO-32	Reconocimiento del ***framework*** usado en la aplicación	-
CLD-INFO-33	Enumeración de la arquitectura Red y de la Aplicación	-

Table 2. Obtained results with the cloud simulation

5. Conclusions

This project not only has enabled us to study the operation of the cloud environment, but additionally various methodologies, exercises and attack tools commonly implemented in the cloud environment have been analyzed, consequently enabling a more profound work with various analysis tools for Cloud security.

In conclusion, it has been possible to design a new analysis methodology whose main objective is to: study new technologies, help companies and workers to carry out their security analysis and, finally, improve the level of security in any cloud environment.

7. References

[1] Oracle, «Oracle Cloud Computing» 2022. [En línea]. Available: https://www.oracle.com/es/cloud/what-is-cloud-computing/.

[2] European Central Bank, «What is TIBER-EU?,» European Central Bank | EUROSYSTEM, 2022. [En línea]. Available: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html#:~:text=TIBER%2DEU%20is%20the%20European,carrying%20out%20a%20controlled%20cyberattack..

[3] Lockheed Martin, «The Cyber Kill Chain» 2022. [En línea]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[4] ATT&CK, MITRE, «Getting Started with ATT&CK,» 10 2016. [En línea]. Available: https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf.

[5] NIST, «Vulnerability Metrics,» 2022. [En línea]. Available: https://nvd.nist.gov/vuln-metrics/cvss.

Índice de la memoria

Índice de figuras

Índice de tablas

Capítulo 1. INTRODUCCIÓN

1.1 INTRODUCCIÓN

"Cloud Computing" se caracteriza, principalmente, en ofrecer acceso a una gran variedad de recursos de manera ágil, flexible y escalable. Actualmente, la gran mayoría de empresas, por no decir en su totalidad, deciden realizar un proceso denominado "**migrar a la nube**" [1] que consiste en trasladar su infraestructura TI fuera de su entorno local, contratando un proveedor de ***"Cloud Computing"*** para almacenar y gestionar su centro de datos. El objetivo final que justifica esta migración es que, como consecuencia, proporciona a las empresas una mayor flexibilidad en el acceso a sus datos, pudiendo acceder a ellos desde cualquier lugar y momento.

A pesar de los grandes beneficios que proporciona ***"Cloud Computing"***, se debe tener en cuenta a su vez las amenazas que puede incorporar estas nuevas tecnologías. Toda la información sensible y crítica de la empresa, dependiendo de su configuración, se encuentra bajo la responsabilidad de terceros y, a pesar del gran beneficio que proporciona el acceso flexible a dichos datos, se debe considerar la existencia de usuarios maliciosos que quieran explotar los servicios proporcionados para fines perjudiciales.

Como consecuencia, se han diseñado a lo largo de los años diversos controles y políticas que se encargan de enriquecer lo máximo posible la seguridad en la nube. Sin embargo, siempre se debe tener en cuenta que todas las medidas de seguridad, por muy eficaces sean en diseño, existe la posibilidad que en un punto de su existencia se conviertan en focos vulnerables para la empresa, ya que con el tiempo se pueden encontrar puntos débiles a ser explotados.

Por este motivo, es de vital importancia tener un equipo de ciberseguridad que se centre en realizar diversos ejercicios de explotación sobre la infraestructura, pudiendo comprobar la veracidad de los controles instalados y, de esta manera, comprobar la verdadera seguridad implementada. Este Trabajo de Fin de Máster se centrará en diseñar una metodología de análisis de seguridad Cloud donde, entre otras cosas, se definirán ejercicios que permitan examinar la seguridad implementada en la infraestructura Cloud desde el punto de vista de un adversario, comprobando aspectos como: acceso ilegítimo a la infraestructura, la sustracción, manipulación y eliminación de la información almacenada, suplantación de los usuarios de la organización, entre otras cosas.

Para realizar el diseño de esta metodología, uno de los objetivos establecidos para este proyecto consiste en el análisis de los tres proveedores de servicios Cloud más influyentes en el mercado actual:

- **"Google Cloud Platform" (GCP)**

- **"Amazon Web Services" (AWS)**
- **"Microsoft Azure Cloud"**.

Además de los distintos proveedores a analizar, se debe tener en cuenta a su vez los diversos formatos de servicios de Cloud que pueden proporcionar dichos proveedores. [2]

1.1.1 SOFTWARE AS A SERVICE – *SAAS*

Software como servicio (***SaaS***) es un modelo de implementación de software en el que el proveedor de la nube aloja las aplicaciones del cliente en su entorno, dando acceso a dicho cliente a través de Internet.

Ejemplos: "***Google Workspace"***, "***Microsoft Dynamics CRM"***, "***IBM Watson Assistant"***, "***Salesforce"***, "***Dropbox"***

1.1.2 CONTAINERS AS A SERVICE – *CAAS*

Los **contenedores como servicio** (***CaaS***) permiten gestionar e implementar aplicaciones utilizando el aislamiento de contenedores. Los proveedores ofrecen el marco, o la plataforma de la organización, donde se realiza toda la implementación y gestión de los contenedores, proporcionando de esta manera la automatización de funciones TI. Este es uno de los servicios más utilizados por desarrolladores ya que facilita el diseño de aplicaciones escalables y seguras mediante contenedores.

Ejemplos**: "*Amazon Elastic Container Service* (ECS)", "*Azure Container Instances* (ACI)"**

1.1.3 PLATFORM AS A SERVICE – *PAAS*

Por otro lado, **Plataforma como servicio** (***PaaS***) proporciona a los clientes el acceso a herramientas de desarrollador necesarias para crear y gestionar aplicaciones (móviles o web) sin tener que invertir en la infraestructura subyacente y evitar procesos de mantenimiento que esto conlleva. El proveedor aloja los componentes de infraestructura y "***middleware***". Por otro lado, el cliente puede acceder a dichos servicios a través de un navegador web.

Ejemplos: "***AWS Elastic Beanstalk***", "***Windows Azure"***, "***Google App Engine***", "***Apache Stratos***", "***OpenShift*** "

1.1.4 FUNCTIONS AS A SERVICE – *FAAS*

Las **funciones como servicio** (***FaaS***) también se conocen como "**arquitecturas sin servidor**" ("***serverless architecture"***), indicando que los servidores se utilizan como un elemento más de la infraestructura. Este tipo de arquitectura permite la ejecución de aplicaciones a través de contenedores creados en el momento, de manera que el desarrollador no ha de preocuparse por la gestión de la infraestructura donde se está ejecutando la función,

centrándose únicamente en la funcionalidad. Se simplifica el ciclo de desarrollo, especialmente en arquitecturas basadas en microservicios.

Ejemplos: "***AWS Lambda***", "***Microsoft Azure Functions***", "***Google Cloud's Functions***", "***IBC Cloud Functions***"

1.1.5 INFRASTRUCTURE AS A SERVICE – IAAS

La **Infraestructura como servicio** (***IaaS***) permite a los clientes acceder a servicios de infraestructura a través de Internet bajo demanda. Una de sus mayores ventajas es que el proveedor de la nube aloja los componentes de la infraestructura que proporcionan capacidad de cálculo, almacenamiento y red para que los suscriptores puedan ejecutar sus cargas de trabajo. El suscriptor es el responsable de instalar, configurar, proteger y mantener el software de la infraestructura basada en la nube (por ejemplo: bases de datos, middleware, aplicaciones).

Ejemplos: **"*Amazon Web Services*"** (**AWS**), "***Microsoft Azure***", "***Google Compute Engine*** (**GCE**)", "***Cisco Metapod***"

1.1.6 METAL AS A SERVICE – MAAS

Metal como Servicio (***MaaS***) es un modelo en el cual se puede utilizar servidores físicos como máquinas virtuales. En este modelo los servidores pueden ser utilizados como un recurso similar a una nube elástica en vez de usarlos individualmente. Está diseñado para ayudar en la facilitación y automatización del despliegue y provisionamiento dinámico de entornos de computación a hiperescala como, por ejemplo, cargas de trabajo de Big Data o de servicios Cloud.

1.2 MOTIVACIÓN DEL PROYECTO

Como se ha podido observar, los diferentes servicios que presenta la migración a la nube suponen una gran ventaja tanto económica como tecnológica para muchísimas empresas. Es más, en muchos casos se puede ver como imprescindible tener al menos un tipo de servicio a la nube integrado. Sin embargo, con lo que respecta en la tecnología y, sobre todo, su evolución, las consecuencias que pueden suponer esta nueva dependencia en la nube son impredecibles.

Debido a la guerra digital que está ocurriendo en la actualidad entre los proveedores de servicios y usuarios maliciosos que quieren explotar los mismos servicios, es de vital importancia mantenerlos lo más actualizados posibles y siempre encontrarse alerta frente a posibles nuevas amenazas así como soluciones relacionadas con la ciberseguridad.

El proceso de análisis de ciberseguridad es el método más eficiente por el cual observar el estado de seguridad que se encuentra implementado en una organización, así como en la infraestructura de la misma. En este proceso, es de vital importancia que los analistas

intercambien los conocimientos que han adquirido a lo largo de su experiencia para poder proporcionar tanto a empresas como usuarios la información necesaria para conocer las diferentes amenazas que pueden conllevar la migración a servicios en la nube y, de esta manera, conocer los procesos necesarios para resolverlo.

Precisamente este trabajo tiene como motivo realizar un primer diseño de una metodología de análisis de ciberseguridad en Cloud, siendo el primer paso la obtención de información acerca de la infraestructura y elementos, así como procesos de seguridad en los servicios en la nube. Este primer diseño tiene como finalidad ayudar a expertos y analistas a realizar los procesos que permitan valorar la seguridad en la nube. A partir de este trabajo, como se ya ha mencionado anteriormente, se puede realizar un proceso de mejora continua al implementar diversas pruebas de seguridad para corroborar y comprobar la información obtenida en este trabajo, actualizando las aplicaciones y herramientas además de posibles nuevos ejercicios que se vayan elaborando en un futuro.

Capítulo 2. ESTADO DE LA CUESTIÓN

Para el desarrollo de este trabajo, el primer paso que se plantea es realizar un análisis tanto sobre el funcionamiento como la estructuración que implementan las plataformas de infraestructuras Cloud previamente mencionadas. Dado que es necesario conocer los posibles puntos débiles de servicios o infraestructura, primero se debe estudiar todas las tecnologías implementadas, además de obtener modelos de estructuración de las mismas para conocer cómo se realiza la interconexión entre ellas. De esta manera, al comprender el funcionamiento genérico que siguen los proveedores Cloud, se podrá diseñar una metodología capaz de implementar y aconsejar ejercicios de análisis de manera más efectiva y eficiente.

En otras palabras, el objetivo de este primer análisis es recopilar la máxima información posible relacionada con los servicios que implementa cada uno de los proveedores para obtener un conocimiento previo sobre sus procesos de funcionamiento. Esta recopilación de información ayudará a asentar las bases de la metodología a diseñar, además de proporcionar un conjunto diverso de posibles técnicas y tácticas que podrán usarse a la hora de diseñar ejercicios de análisis.

2.1 GOOGLE CLOUD

"Google Cloud Platform" (GCP) [3] es una plataforma que ofrece más de 90 servicios de tecnología de información, accesibles tanto para empresa, como profesionales de TI y desarrolladores, para conseguir implementar un trabajo más eficiente, ganar mayor flexibilidad y/u obtener una ventaja estratégica.

Todos los productos de **Google Cloud**, también denominados servicios de tecnologías de la información, se encuentran disponibles "**a la carta**", es decir: los usuarios pueden escoger todos los productos a su disposición de la manera que ellos crean convenientes para desarrollar la infraestructura que necesitan. Una vez seleccionados los servicios deseados; los usuarios simplemente generan un estos a través de la "**GCP Console*"*** basada en la web, pudiendo administrar qué miembros del equipo o administradores tienen acceso a qué servicios.

Los productos que ofrece **Google** Cloud se dividen en las siguientes categorías:

- **Gestión de APIs:** Plataforma de **APIs** "***Apigee"***, "***AppSheet"***, "***HealthAPI"***, "***Cloud Endpoint"***, API de "***Cloud Healthcare"*** y "***API Gateway"***

- **Computación**: Productos que permiten la realización de cálculos computacionales a gran velocidad, ejecución de grandes bases de datos en memoria y creación de

aplicaciones nativas de la nube con máquinas virtuales escalables y rentables. Independientemente de si se eligen máquinas virtuales predefinidas o personalizadas, todas se ejecutan en la infraestructura de "**Google**".

- **Contenedores: *"Cloud Build"***, "***Cloud Run"***, "***Artifact Registry"***, "***Container Registry"***, "***Google Kubernetes Engine*** (**GKE**)" y "***Knative"***

- **Analítica de datos:** "***Google Cloud Smart Analytics*"** es una plataforma de analíticas flexible y abierta que ayuda a convertir empresas a organizaciones basadas en la inteligencia. Se basa en inteligencia artificial y en el desarrollo de servicios a escala de Internet, así como en los mismos principios de tecnología probadas y fiable utilizados por los servicios de "**Google**". Las organizaciones suelen escoger "**Google Cloud**" para crear su nube de datos.

- **Bases de datos**: Proporcionado de base de datos para todo tipo de aplicaciones

- **Herramientas de desarrollo**: Escritura, despliegue y depuración de aplicaciones alojadas en "**Google Cloud**" para desarrolladores de herramientas y equipos de desarrollo

- **Entornos híbridos y multinube**: "***Anthos*"** es una plataforma de modernización de aplicaciones. Ofrece una plataforma uniforme para todos los despliegues de una empresa.

- **Herramientas de gestión**: Proporciona todas las herramientas necesarias para optimizar tareas de gestión de la nube, además de las API y las aplicaciones, con acceso a todas las API de "**Google**", incluida la API de facturación de "**Google Cloud**".

- **Migración**: Proporciona ayuda en el diseño de soluciones de migración más adecuadas para el negocio, tanto para eliminar o reducir centros de datos "***on-premise"***, como para migrar cargas de trabajo, modernizar aplicaciones o cambiar de nube.

- **Redes**: Ofrece una cartera de servicios de redes basados en una infraestructura a escala mundial donde se emplea soluciones de automatización, IA avanzada y programación. Esto permite a las empresas conectarse, escalar sus recursos, protegerse y optimizar sus infraestructuras.

- **Operaciones**: Servidores integrados de monitorización, almacenamiento de registros y trazas para aplicaciones y sistemas que se ejecutan en "**Google Cloud**" y en otros entornos.

- **Seguridad e identidad**: Donde se ofrecen productos de seguridad útiles para cumplir con los objetivos empresariales, normativos y políticas, con una evolución y ampliación continúa del conjunto de controles y funciones.

- **Computación sin servidor**: Se trata de un tipo de aplicación que elimina toda la gestión de la infraestructura, lo que permite simplificar la experiencia del desarrollador.

- **Almacenamiento**: Servicios de almacenamiento basados en la nube que se ejecutan en la infraestructura de "**Google Cloud**". Implementación de "**Google Drive**" para consumidores con el objetivo de compartir archivos. Para el almacenamiento de imágenes, proporciona la plataforma "***Google Fotos***".

2.2 "AMAZON WEB SERVICES" – AWS

"Amazon Web Services" (AWS) [4] ofrece un amplio conjunto de productos globales basados en la nube. Estos servicios ayudan a empresas a avanzar con mayor rapidez, reducir los costes de TI y escalar de manera más eficiente. Se respalda en compañías y empresas emergentes para proveer una amplia variedad de cargas de trabajo, como aplicaciones web y móviles, almacenamiento y procesamiento de datos y, entre otras cosas, el almacenamiento en general o el archivado.

AWS proporciona los siguientes productos:

- **Análisis**: **AWS** ofrece una selección de servicios de análisis de datos para organizaciones de todos los tamaños y sectores. Permite el movimiento y almacenamiento de datos, el análisis de "***Big Data***", el análisis de registro, el análisis de ***"streaming"*** y "***Machine Learning"***, entre otras cosas.

- **Integración de aplicaciones**: Se trata de un conjunto de servicios que permiten la comunicación entre los componentes desacoplados en microservicios, sistemas distribuidos y aplicaciones sin servidor.

- **Informática**: Para cualquier carga de trabajo, donde se proporcionan instancias, contenedores e informática sin servidor.

- **Centro de contacto**: Servicio de atención de clientes con un centro de contacto omnicanal en la nube.

- **Contenedores**: Facilitan la administración de la infraestructura subyacente, ya sea en la nube o en las instalaciones locales. Permite la creación de microservicios y la integración en **AWS** con alta confiabilidad.

- **Base de datos**: Proporciona base de datos personalizadas y completamente administradas.

- **Herramientas para desarrolladores**: Desarrollo de aplicaciones en **AWS** de forma rápida y sencilla. Permite el alojamiento de código, la creación e implementación de aplicaciones. Entre ellas se encuentran: kits de desarrollo de software (**SDK**), los editores de código y los servicios de integración y entrega continuas (**CI/CD**) para el desarrollo de software de "***DevOps"***.

- **Informática para usuarios finales**: Mediante la virtualización de aplicaciones y escritorios nativos en la nube. Con los servidores **AWS EUC**, los empleados pueden realizar su trabajo desde cualquier dispositivo compatible.

- **Servicios de frontend web y móviles**: **AWS** ofrece un conjunto de herramientas y servicios para admitir flujos de trabajo de desarrollo para desarrolladores de "**iOS/Android**", "***React Native***" y "**JavaScript**".

- **Administración y control**: Aprovisionamiento, monitorización y registro, administración de operaciones y servicios administrados para la administración de la configuración. Dispone de un conjunto de herramientas de administración que permiten aprovisionar, monitorizar y automatizar todos los componentes del entorno Cloud mediante programación.

- **Migración y transferencia**: Soluciones de migración a la nube que ayuda en el proceso de migración de cargas de trabajo desde entornos locales, instalaciones de alojamiento u otras nubes públicas.

- **Redes y entregas de contenido**: Seguridad, disponibilidad de la red, rendimiento consistente y cobertura mundial

- **Seguridad, identidad y conformidad**: Asegurar cargas de trabajo y aplicaciones en la nube mediante la protección de datos, detección de amenazas y monitoreo continue, gestión de identidades y accesos, conformidad y privacidad de datos, y protección de red y aplicación.

- **Tecnología sin servidor**: Tecnologías para ejecutar código, administrar datos e integrar aplicaciones, sin la obligación de administrar servidores. Las tecnologías sin servidor incluyen escaldado automático, alta disponibilidad integrada y un modelo de facturación de pago por uso.

- **Almacenamiento**: Almacenamiento confiable, escalable y seguro de datos. Algunas herramientas son: ***Amazon Simple Storage Service*** **(S3)**, ***Amazon Elastic File System*** **(EFS)**, ***Amazon FSx*** y ***Amazon Elastic Block Store*** **(EBS)**. También tiene herramientas de copias de seguridad, transferencia de archivos administrada, migración de datos y almacenamiento en la nube híbrida e informática de borde.

2.3 MICROSOFT "AZURE" CLOUD

"Microsoft Azure" es una plataforma pública de "**Microsoft**" de ***"Cloud Computing"***. Proporciona una gran variedad de servicios Cloud, entre ellos se encuentra la computación, análisis y almacenamiento. Esta plataforma tiene como objetivo ayudar a las empresas a gestionar los desafíos y, además, a cumplir con sus objetivos organizacionales. Ofrece herramientas que soportan todas las industrias (incluyendo "***e-commerce***" y finanzas) y es compatible con tecnologías de fuente abierta. Esto proporciona a los usuarios una flexibilidad de utilizar su herramientas y tecnologías preferentes, pudiendo escoger a su vez entre los 4 diferentes tipos de servicio que ofrece **"Azure"**: ***IaaS***, ***PaaS***, ***SaaS*** y, además, sin servidor.

Una vez que los clientes han finalizado su suscripción, tendrán a acceso a todos los servicios incluidos en el portal de **"Azure"**. Los suscriptores podrán usar estos servicios para generar servicios basados en la nube como, por ejemplo, máquinas virtuales y bases de datos. **"Azure"** funciona de manera "***pay-as-you-go!***, es decir, que todos los suscritores reciben una tarifa cada mes que solo cobra los recursos específicos que se han utilizado.

Entre los productos [5] que ofrece **"Azure"**, se puede encontrar los siguientes:

- **Análisis**: Recolectar, almacenar, procesar, analizar y visualizar datos de cualquier variedad, tamaño o rapidez.

- **Computación**: Acceso a la computación de Cloud con escala bajo demanda

- **Contenedores**: Desarrollo y gestión de las aplicaciones en contenedores a mayor rapidez mediante herramientas integradas

- **Bases de Datos**: Servicios de bases seguras, de nivel empresarial y completamente administradas

- **Herramientas de desarrollo:** Creación, administración y entrega continua de aplicaciones Cloud, implementando cualquier tipo de plataforma o lenguaje.

- **DevOps:** Entrega de innovación rápida con herramientas simples y fiables para la entrega continua.

- **Híbrido y Multicloud**: En esta categoría se ofrece **"Azure Active Directory**", lo que permite que la innovación y agilidad de la computación en la nube en las cargas de trabajo locales.

- **Identidad**: Gestión de las identidades de usuario y de acceso para la protección contra amenazas avanzadas tanto en dispositivos como en datos, aplicaciones e infraestructura.

- **Integración**: Integración de aplicaciones, datos y procesos locales y basades en la nueva en toda la empresa

- **Migración**: Simplificar y acelerar la migración a la nube mediante guías, herramientas y recursos

- **Móvil**: Construir e implementar aplicaciones multiplataforma y nativas para cualquier dispositivo móvil

- **Redes**: Conectar las infraestructuras y servicios locales con Cloud

- **Seguridad**: Protección de la organización contra amenazas avanzadas por todas las cargas de trabajo de Cloud híbrida

- **Almacenamiento**: Conseguir un almacenamiento escalable para datos, aplicaciones y cargas de trabajo

- **Infraestructura de escritorio virtual**: Permite que los empleados trabajen desde cualquier lugar con una infraestructura de escritorio virtual basada en la nube

- **Web**: Creación, implementación y escala de aplicaciones web de manera

2.4 COMPARATIVA ENTRE LOS TRES PROVEEDORES

Como se ha podido observar, los tres proveedores anteriores ofrecen servicios que en muchos casos, o coinciden entre ellos o resultan ser muy similares en funcionamiento, lo que en muchos casos hace cuestionar a usuarios y empresas sobre las diferencias que existen

entre ellos. La realización de un estudio sobre la comparativa entre estos proveedores permitirá conocer cuáles suelen ser los servicios más utilizados, los motivos de la preferencia de los clientes que los contratan y, de esta manera, descubrir posibles puntos de entrada vulnerables.

En el caso de computación, según "***Gartner Peer Insights"*** [6], una plataforma donde se recoge valoraciones y opiniones de diversos clientes con lo que respecta a plataformas y servicios IT, **AWS** y **GCP** ganan ventaja en comparación con **"Azure"**. En el caso de "**Google**", las plantillas de instancia permiten la creación grupos de instancia administrados o, en cambio, instancias individuales con campos de plantilla de instancia de anulación, lo que proporciona la capacidad de restringir la plantilla a la zona de recursos especificada [7]. Por otro lado, la administración de usuarios de **IAM** que proporciona **AWS** permite a los administradores crear usuarios, establecer credenciales de seguridad individuales o solicitar credenciales de usuario temporales.

En lo que respecta a la gestión de usuarios, "**Gartner"** marca a "**Google"** como el líder en este sector. Esto se debe a que **GCP** optimiza las asignaciones de herramientas y, además, gestiona los roles de usuario a nivel de cuenta y contenedor. Asimismo, incorpora una interfaz de usuario tradicional proveniente del propio "**Google**".

En el caso de red, servicios para desarrolladores, herramientas de gestión, e integración empresarial, la lista de "**Gartner"** vuelve a establecer a **"Google Cloud Platform"** como mejor candidato. Por un lado, la disponibilidad de la red se debe gracias al automatismo que ofrece con una subred en cada región implementando rangos IP predefinidos y, además, un modo personalizado que permite el control sobre las mismas. Por otro lado, el portal de desarrollador actúa como un sistema de gestión de contenido para proporcionar un conjunto de módulos que permiten crear contenido y, además, documentación de API. Finalmente, la monitorización, registro y diagnóstico integrados dentro de "**Google Stackdriver"**, junto con la monitorización completa de paquetes, análisis de gestión en tiempo real, monitorización y alerta de excepciones en tiempo real, entre muchas otras muchas herramientas de **"Google Cloud Platform"**, habilitan múltiples características que facilitan la implementación de las diversas herramientas de gestión. En otras palabras, **GCP**, entre los tres servicios, es el que mayor variabilidad de herramientas puede ofrecer.

Cabe destacar que **AWS** tiene sus propias ventajas, como es el caso en la seguridad y cumplimiento, capacidad de escalado, y la habilitación de dispositivos. Las plataformas de seguridad **AWS** incorporan no solo seguridad de infraestructura, sino además mitigación de **DDoS**, criptado de datos, inventario, monitorización y pruebas de penetración, entre muchas otras capacidades. En total, cumple con 34 normas y reglamentos internacionales. Además, **AWS** permite escalar planes para instancias de "**Amazon EC2**", tareas de "**Amazon ECS**", réplicas de "**Amazon Aurora**", entre otras funcionalidades adicionales. Finalmente, "**Amazon DevOps Services"** incluye microservicios y entrega continua, además de entrega de integración continua, herramientas de colaboración, y controles y gestión de configuración de gran precisión para el cumplimiento de seguridad.

A pesar de que los dos proveedores anteriores planteen ciertas ventajas según muestra los análisis de "**Gartner"**, cabe destacar que **"Azure"** también implementa sus propias herramientas que le permiten destacar entre el resto de los proveedores. Por ejemplo, una de las herramientas más implementadas entre los servicios de **"Azure"**, es **"Azure Active Identity"**, integrado a través de "**Micrososft 365"**, **"Azure"** y "**Eneterprise Mobility + Security"**, permitiendo a los administrados identificar de forma centralizada y, además acceder a la gestión a través de dispositivos, datos, aplicaciones e infraestructura. Además, las soluciones de **"Azure *DevOps"*** también incluyen integración continua que permite construir y probar código de forma automática. Por otro lado, el proceso de monitorización de estados de componentes de las plataformas se realiza mediante **"Azure Monitor"**, que trabaja junto de "**Log Analytics"** para la recolección de datos en las instalaciones y en la nube.

Como resumen final de este análisis, en la siguiente tabla se puede observar una comparativa general entre los tres proveedores:

	Tipo de cliente	Coste	Servicios
Google Cloud Platform	Pequeñas y medianas empresas. Se asocia con Cisco para llegar a las empresas	Gartner reconoce a GCP por sus precios centrados en el cliente, incluyendo grandes descuentos y contratos flexibles.	Menos servicios, pero capacidades técnicas avanzadas, con IA / ML y herramientas de análisis de datos por delante de la competencia.
Microsoft Azure	Empresas	Los descuentos basados en condiciones particulares requieren de ayuda para su evaluación.	Infraestructura robusta con capacidades probadas de nube híbrida.
Amazon Web Services	Cualquiera, pero con un enfoque no invasivo debido a su enorme tamaño.	Gartner recomienda el uso de una herramienta de terceros para estimar los precios de manera efectiva.	Grandes opciones, pero centradas en soluciones de nube pública, por lo que la implementación híbrida con centros de datos locales puede ser un reto.

Ilustración 1. Comparativa entre los tres proveedores según Acronis

En conclusión, los tipos de servicio que cubre cada proveedor se resumen en la siguiente tabla:

Tipo de servicio	***AWS***	***Azure***	***GCP***
Grandes volúmenes de datos	X	X	X
Marketing digital	X	X	X
Comercio electrónico	X	X	X
Juegos	X	-	X
Gobiernos	X	X	-
Internet de las cosas (IoT)	X	X	X
Nubes privadas	X	X	X
Reseller Hosting	X	X	X

Tabla 1. Tabla comparativa entre proveedores

Como se ha podido observar a lo largo de este apartado, todos los proveedores ofrecen servicios específicos que cumplen con un tipo de demanda solicitada por parte de los clientes. Para poder obtener una visión general sobre todas las herramientas que ofrece cada proveedor, a continuación se han diseñado una serie de tablas donde se resumen los productos y soluciones que ofrecen cada proveedor para un tipo de funcionalidad específico.

Para **computación**, cada proveedor ofrece los siguientes servicios:

Servicio	***AWS***	***Azure***	***GCP***
IaaS	Elastic Compute Cloud – EC2	Azure Virtual Machines	Compute Engine
PaaS	Elasitc Beanstalk	App Service, Cloud Services	App Engine Estándar Environment, App Engine Flexible environment
Servicios virtuales privados	Lightsail	Virtual Machine Images	-
Servicio Gestionado de contenedores	EC2 Container Service - ECS	-	-
Servicio Gestionado de Kubernetes	Elastic Container Service para Kubernetes – EKS	Azure Kubernetes Service – AKS	Kubernetes Engine
Registro de contenedores Docker	EC2 Container Registry – ECR	Azure Container Registry	Container Registry
Contenedores Serverless	Fargate	Container Instances	-
Servicio gestionado para microservicios	Service Fabric	App Engine	-
Serverless	Lambda	Functions	Cloud Functions
Computación por lotes	AWS Batch	Azure Batch	-
Escalado automático de instancias	AWS Auto Scaling	Virtual Machine Scale Sets, App Service Scale Capability – PAAS, AutoScaling	Instance Groups
Infraestructura de la Cloud en local	AWS Outposts	-	GKE On-Prem

Tabla 2. Comparación de productos relacionados con la computación

En segundo lugar, para **almacenamiento** se observan los siguientes productos:

Servicio	***AWS***	***Azure***	***GCP***
Almacenamiento de objetos	Simple Storage Services – S3	Blob Storage	Google Cloud Storage
Almacenamiento para archivado	S3 Infrequent Accesss – IA, Glacier	Storage – Cool, Storage – Archive	Nearline, Coldline
Disco para instancias	Elastic Block Store – EBS	Disk Storage	Persistent Disk
Almacenamiento de ficheros	Elastic Block Store – EBS	Disk Storage	Cloud Filestore
Transferencia de grandes cantidades de datos a la nube	AWS DataSync, Snowball Edge, Snowmobile	Import/Export, Azure Data Box	Storage Transfer Service
Backup	Glacie, Storage Gateway	Azure Backup	Coldline
Almacenamiento híbrido	Storage Gateway	StorSimple	-
Servicio de Disaster Recovery	Site Recovery	-	-

Tabla 3. Comparación de productos relacionados con el almacenamiento

En tercer lugar, los servicios asociados a **bases de datos** son:

Servicio	***AWS***	***Azure***	***GCP***
Bases de datos relacionales	RDS, Amazon Aurora	SQL Database	Cloud SQL, Cloud Spanner
Almacenamiento de documentos – NoSQL	DynamoDB	Azure Cosmos DB	Cloud Datastore, Cloud Bigtable
Almacenamiento clave-valor – NoSQL	Dynamo DB, SimpleDB	Table Storage	Cloud Datastore
Almacenamiento en caché	ElastiCache	Azure Redis Cache	Cloud Memorystore
Migración de bases de datos	Database Migration Service	Azure Database, Migration Service	-
Data Warehouse gestionado	Redshift	SQL Data Warehouse	Big Query
Bases de datos basado en grafos	Neptune	Azure Cosmos DB	-

Tabla 4. Comparación de productos relacionados con las bases de datos

En relación con las **redes y conectividad**, se pueden contratar los siguientes servicios:

Servicio	***AWS***	***Azure***	***GCP***
Entornos virtuales de red aislados	Virtual Private Cloud	Virtual Network	Virtual Private Cloud
Conexión con entornos on-prem	AWS Managed VPN	VPN Gateway	Cloud VPN
DNS administrado para nombres y registros	Route 53	Azure DNS	Google Cloud DNS
Redirección de tráfico entrante	-	Traffic Manager	-
Red de entrega de contenido global	CloudFront	Content Delivery Network	Cloud CDN
Red dedicada y privada para conectar nube-local	Direct Connect	ExpressRoute	Cloud Interconnect
Balanceo de carga	Elastic Load Balancing	Load Balancer	Cloud Load Balancing

Tabla 5. Comparación de productos relacionados con las redes y conectividad

Las **herramientas para la gestión y control de la Cloud** que ofrece cada proveedor son:

Servicio	***AWS***	***Azure***	***GCP***
Capacidades de asesoramiento Cloud	Trusted Advisor	Azure Advisor	Cloud Platform Security
Aprovisionamiento de recursos y orquestación	OpsWorks - Chef-based, CloudFormation	Azure Automation, Resource Manager, VM extensions	Cloud Deployment Manager
Monitorización y administración de recursos	CloudWatch, X-Ray, Management Console	Azure Portal, Azure Monitor, Azure Application Insights	Stackdriver Monitoring, Cloud Shell, Debugger, Trace, Error Reporting
Facturación	Usage and Billing	Azure Billing API	Stackdriver Monitoring Cloud Billing
Administración	Application Discovery Service, Systems Manager, Personal Health Dashboard	Log Analytics, Operations Management Suite, Resource Health, Storage Explorer	Cloud Console
Seguimiento de actividad de usuarios y uso de APIs	CloudTrail	Log Analytics, Audit Logging en Azure Monitor	Cloud Audit Logging
Evaluación de estado de cargas de trabajo	Well-Architected Tool	-	-

Tabla 6. Herramientas para la gestión y control de la Cloud por proveedor

Finalmente, y estrechamente relacionado con el tema principal de este trabajo, las prácticas y servicios de **seguridad** que aplica cada proveedor son:

Servicio	***AWS***	***Azure***	***GCP***
Autenticación y autorización	Identity and Access Management – IAM, Organizations	Active Directorym Active Directory Premium	Cloud IAM, Cloud Identity-Aware Proxy
Protección de la información	-	Azure Information Protection	-
Cifrado	AWS Key Management Service, CloudHSM	Key Vault	Cloud Key Management Service
Firewall	Web Application Firewall	Application Gateway	-
Evaluación de seguridad	Inspector	Secutiry Center	-
Administración de certificados	Certificate Manager	App Service certificates	-
Servicios de directorio	AWS Directory Service	Active Directory Domain Service	-
Administración de identidades	Cognito	Azure Active Directory B2C	-
Autenticación multifactor	Multi-Factor Authentication	Multi-Factor Authentication	Multi-Factor Authentication
Detección de amenazas y actividades anómalas	GuardDuty, AWS Macie	Azure Advanced Threat Protecion	Cloud Security Command Center
Cumplimiento normativo	Artifact	Service Trust Portal	-
Protección frente DDoS	AWS Shield	DDoS Protection Service	Coud Armor

Tabla 7. Comparación de productos relacionados con la seguridad

Capítulo 3. DEFINICIÓN DEL TRABAJO

3.1 JUSTIFICACIÓN

Actualmente, existen una gran variedad de herramientas implementadas en el proceso de análisis de seguridad. Además, según los resultados de los análisis de los tres proveedores de Cloud establecidos (**"Azure"**, **AWS** y "**Google Cloud**"), los clientes que contratan e implementan estos servicios son tanto usuarios individuales como organizaciones de diversos tamaños y funcionalidades. Cabe destacar que toda la información obtenida a lo largo de este trabajo se encuentra dispersa y expandida por Internet y, en ningún caso, se ha podido encontrar una metodología actual donde se implemente diversos procesos posibles al realizar un análisis de ciberseguridad en un servicio en la nube.

Al realizar este diseño, teniendo en cuenta que éste mismo debe ser actualizado periódicamente con el objetivo de implementar todos los cambios y evoluciones de estas tecnologías, el proceso de análisis de una infraestructura Cloud no solo será más eficiente, sino que a su vez cubrirá un alcance mayor de fallos de seguridad. Este último se debe a que, muchos analistas pueden estar especializados en ciertas ramas de ciberseguridad y, por este motivo, cabe una gran posibilidad de que puedan obtener resultados que difieran del resto.

3.2 OBJETIVOS

Una vez analizado la motivación y el estado del arte de este trabajo, los objetivos que se ha podido extraer y deben ser realizados a través de este trabajo son:

1. Analizar e investigar los 3 proveedores Cloud actuales: **"Amazon Web Services"** (**AWS**), **"Google Cloud Platform"** (**GCP**) y "**Microsoft Azure"**
    - Realizar un análisis de las soluciones y productos que ofrece cada proveedor.
    - Obtener una visión general sobre cómo funcionan y qué componentes utilizan
    - Obtener información sobre las tecnologías y niveles de seguridad que implementan
2. Diseñar y establecer una metodología de trabajo de análisis de seguridad Cloud
    - Realizar un análisis de las vulnerabilidades más comunes encontradas en estas plataformas y analizar los procesos de ataque.

- Investigar explotaciones previas conocidas para obtener cadenas de ataque prácticas y funcionales

- Investigar métricas y metodologías conocidas a implementar en el proyecto

- Establecer un listado de controles y ejercicios a implementar en el análisis de seguridad Cloud

3. Implementar la metodología diseñada en una infraestructura de la nube y analizar resultados

3.3 METODOLOGÍA

Como comienzo de este trabajo se propone realizar un primer análisis sobre las estructuras y funcionalidades que presentan los proveedores en sus infraestructuras de Cloud, además de las amenazas y vulnerabilidades que suponen estas implementaciones. A través de este análisis, se busca obtener una visión general de cómo funcionan estos proveedores, qué productos y soluciones ofrecen a sus clientes, cuáles son los productos más utilizados por ellos y, de esta manera, descubrir posibles métodos de ataque.

Realizando una combinación de la información obtenida sobre los proveedores y los diversos métodos de trabajo existentes a la hora de realizar un análisis de ciberseguridad, se puede comenzar, finalmente, con el diseño de la metodología de ciberseguridad en la nube, intentando cubrir las amenazas más comúnmente encontradas entre los tres proveedores.

Tras finalizar con el diseño de esta metodología, se propone realizar una simulación en un entorno de nube para probar tanto las herramientas encontradas en análisis previos, además de comprobar algunos procesos de ataque previamente explicados. Se debe tener en cuenta que esta simulación será limitada dependiendo del entorno en el que se encuentre y, además, la información sensible que se pueda observar o modificar. Para evitar posibles complicaciones, se propone realizar un análisis de reconocimiento y descubrimiento y, de esta manera, analizar los posibles siguientes pasos a realizar en el análisis de seguridad.

3.4 PLANIFICACIÓN Y ESTIMACIÓN ECONÓMICA

3.4.1 PLANIFICACIÓN

Por último, el cronograma a seguir a lo largo de este trabajo es el siguiente:

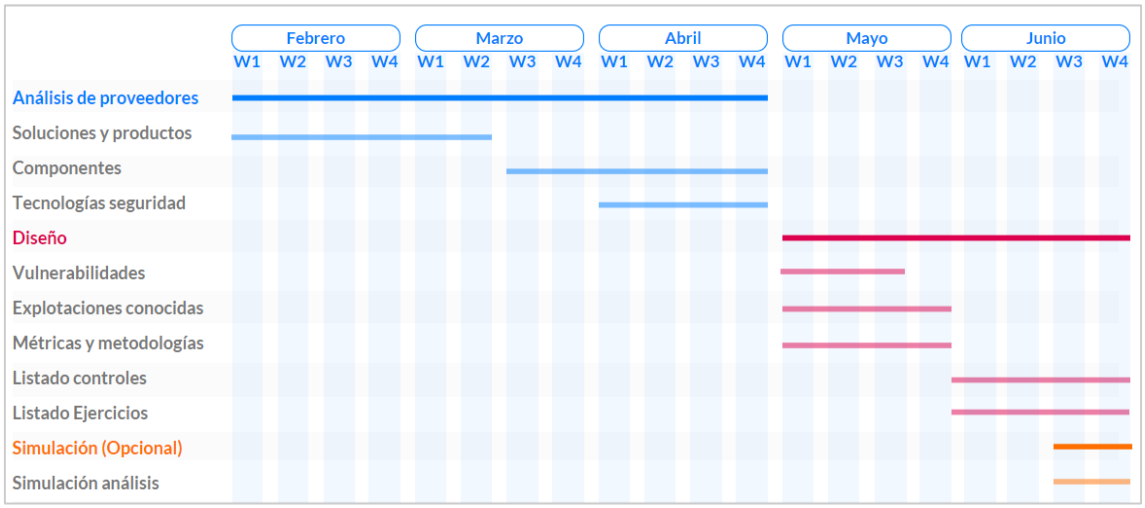

Ilustración 2. Cronograma del Trabajo de Fin de Máster

3.4.2 ESTIMACIÓN ECONÓMICA

Dado que este trabajo se centra primordialmente en la investigación sobre las estructuras y controles implementados en las infraestructuras Cloud, junto con el análisis de vulnerabilidades y ataques previamente realizados en dichas infraestructuras, no existe ningún coste de desarrollo a calcular. El objetivo principal de este trabajo es diseñar una metodología de análisis de seguridad en Cloud y, como se explicará más adelante en trabajos futuros, se implementará en futuros proyectos con diversos analistas para completar esta metodología con información adicional. En otras palabras, no se implementa ningún elemento o diseño de software que requiera un coste adicional sobre este proyecto.

En resumen, dado que se trata de un proceso de diseño, este proyecto no ha proporcionado ningún coste económico en su desarrollo.

Capítulo 4. DISEÑO DEL PROYECTO

4.1 PLANIFICACIÓN DE EJERCICIOS DE ANÁLISIS DE CLOUD

En este apartado, se expone un resumen a alto nivel de los diferentes puntos que se deben contemplar a la hora de realizar una planificación de ejercicios ***"Red Team"*** o, en este caso, un análisis de seguridad en la nube, siguiendo el marco de trabajo **TIBER-EU** [8] como eje central de estos ejercicios.

4.1.1 CONSIDERACIONES INICIALES

A la hora de seguir el marco de trabajo de **TIBER-EU**, se deben tener en cuenta ciertas consideraciones iniciales antes de comenzar la planificación de ejercicios de ***"Red Team"*** a implementar.

4.1.1.1 Destinatarios del marco de trabajo

El marco **TIBER-EU** está diseñado para autoridades nacionales y entidades que forman la infraestructura financiera central, incluidas aquellas entidades cuyas actividades transfronterizas están dentro del ámbito regulatorio de varias autoridades. Es aplicable a entidades no solo en el sector financiero, sino también en cualquier otro sector crítico. Además de una serie de requisitos obligatorios, el marco también incluye opciones que pueden adaptarse a las particularidades de las diferentes jurisdicciones. Esto facilita el reconocimiento mutuo y reduce la carga tanto para las autoridades como para las entidades.

4.1.1.2 Participantes en la ejecución de las pruebas

Los principales participantes en una prueba **TIBER-EU** se asignan a uno de los cinco equipos diferentes según su función y responsabilidades:

- **Equipo azul (*"Blue Team"*):** Personas en la entidad que es el sujeto de la prueba y cuyas capacidades de prevención, detección y respuesta se están probando sin su conocimiento previo.

- **Proveedor de inteligencia de amenazas**: Compañía que analiza el rango de posibles amenazas y realiza un reconocimiento de la entidad.

- **Equipo rojo (*"Red Team"*):** Equipo de expertos (internos o externos) que llevan a cabo la ejecución de las técnicas y tácticas de los adversarios para intentar comprometer las funciones críticas de la entidad.

- **Equipo blanco (*"White Team"*)**: Equipo dentro de la entidad objetivo que son los únicos que saben que se está realizando una prueba y que lidera y administra la misma en colaboración con el equipo de **TIBER**.

- **Equipo cibernético TIBER (opcional):** Equipo dentro de la autoridad responsable de supervisar la prueba y asegurarse de que cumple con los requisitos del marco **TIBER-EU**, lo que permite el reconocimiento mutuo de la prueba por parte de las autoridades relevantes

4.1.1.3 Fases definidas en el marco de trabajo

El marco de trabajo contempla un conjunto de fases que deben llevarse a cabo, siendo tres de ellas de carácter obligatorio y una opcional. En el siguiente diagrama puede apreciarse el conjunto de fases descritas con anterioridad y la evolución de las mismas:

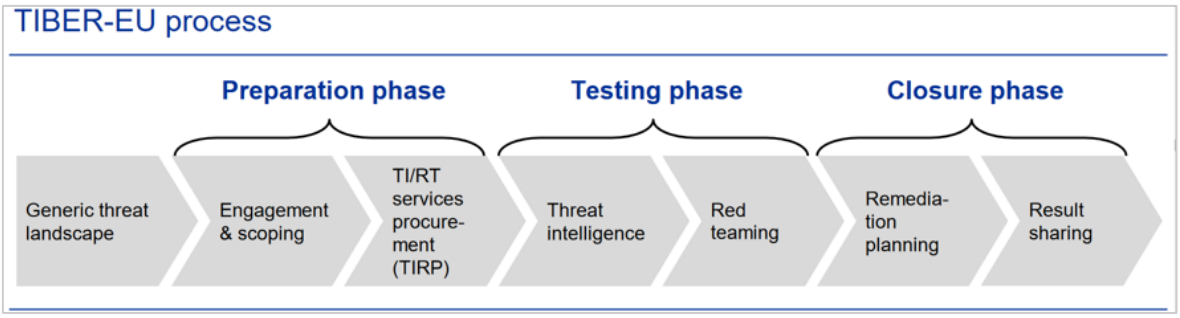

Ilustración 3. Fases de TIBER-EU

Las fases, por tanto, son:

- **Fase de búsqueda de activos expuestos y amenazas**: Esta fase implica una evaluación del panorama de activos expuestos y amenazas, analizando las funciones específicas de la organización, los actores que puedan suponer un riesgo para la misma, así como las tácticas y técnicas o procedimientos a los que puede encontrarse expuesta, como la industria a la que pertenece, su situación geográfica, así como sus relaciones políticas y estratégicas. Con esta información se pretenden generar los posibles escenarios que se ejecutarán posteriormente en los ejercicios.

- **Fase de preparación**: Inicio del ejercicio sobre la organización, en ella se deben establecer los equipos, determinar el alcance y aprobar los ejercicios que se van a ejecutar.

- **Fase de ejecución**: Se realiza un informe por parte del equipo de Inteligencia de Amenazas para identificar los riesgos reales sobre la organización. Este servirá posteriormente al equipo de ***"Red Team"*** para generar aquellos escenarios que van a ejecutarse, obtener información de los sistemas críticos, las personas y procesos de la organización. En algunos casos, cuando las pruebas no han sido exitosas desde un punto externo (Caja Negra) es posible reunirse con el Equipo Blanco (***"White***

Team") y solicitar el acceso a los sistemas para poder continuar las pruebas desde dentro.

- **Fase de cierre**: Se proporcionarán los resultados, tras la ejecución de los ejercicios sobre la organización, y se llevará a cabo una evaluación sobre las capacidades de protección, detección y respuesta ante amenazas de la organización. Esta información debe ser revisada y discutida para preparar un plan de remediación y para dar por finalizadas las pruebas

4.1.2 PLANIFICACIÓN DE LAS PRUEBAS

La planificación de las actividades iniciales de ejercicios de ***"Red Team"*** tienen como objetivo definir con claridad las expectativas del mismo, además de identificar aquellos aspectos que pudieran determinar su éxito. Teniendo en cuenta esta cuestión, se debe realizar al menos las siguientes acciones:

- Definición del alcancen de las pruebas dentro de la organización objetivo
- Establecer el riesgo al que se expondrá la organización durante el periodo de ejecución de las pruebas
- Elección de equipos que van a realizar la identificación de amenazas y la ejecución de las pruebas
- Reconocimiento de la infraestructura de la organización
- Ejecución de las pruebas de ***"Red Team"***
- Análisis de resultados de las pruebas
- Propuestas de planes de remediación y mitigación de las amenazas identificadas

Por otro lado, el tiempo de duración mínimo establecido por **TIBER-EU** para la ejecución de los ejercicios es de **90 días (3 meses)**, dependiendo de los ámbitos acordados.

4.2 MÉTRICAS, FRAMEWORKS Y METODOLOGÍAS

Para el desarrollo de este trabajo, primero se plantea realizar un análisis tanto sobre el funcionamiento como la estructuración que implementan las plataformas de infraestructuras Cloud previamente mencionadas. Dado que es necesario conocer los posibles puntos vulnerables de las aplicaciones o infraestructuras a analizar, primero se debe estudiar todas las tecnologías implementadas, además de obtener modelos de estructuración de las mismas para conocer cómo se conectan entre ellas. De esta manera, al comprender el funcionamiento

genérico que siguen los proveedores Cloud, se podrá diseñar una metodología capaz de implementar y aconsejar ejercicios de análisis de manera más efectiva y eficiente.

Este primer proceso de análisis se divide en dos secciones principales. Primero, se recopilará información sobre las tecnologías e infraestructuras de los proveedores Cloud, por motivos previamente explicados. Segundo, finalmente, se realizará a su vez un análisis sobre las metodologías y métricas existentes, ya que podrán aporta información adicional sobre los diversos procesos de análisis de seguridad comúnmente utilizados. Esta recopilación de información ayudará a asentar las bases de la metodología a diseñar, además de proporcionar diversos puntos de vista a la hora de diseñar ejercicios de análisis.

4.2.1 *"CYBER KILL CHAIN"*

La ***"Cyber Kill Chain"*** [9] se trata de un modelo utilizado por el equipo de respuesta de incidentes, investigadores de forense digital y análisis de malware para trabajar de manera encadenada, junto con los equipos de ***"Red Teaming***" para medir el estado en el que se encuentran los ataques avanzados y persistentes (APT) diseñados. Este proceso permite analizar y modelizar las acciones ofensivas de un ciberataque y, a su vez, puede ayudar a implementar una estructura para realizar un diseño del mismo. Este modelo contiene las fases necesarias para comprender, detectar y prevenir amenazas.

Este modelo se divide en las siguientes fases:

- **Reconocimiento**: Se refiere al proceso de recolectar la mayor información posible relacionada sobre el objetivo a analizar. Este se divide a su vez en reconocimiento pasivo (***footprinting***) y activo (***fingerprinting***).

- **Preparación**: Proceso de desarrollo de un plan de técnicas, utilizando la información obtenida en la fase anterior. En otras palabras, escoger las herramientas y técnicas necesarias para realizar el análisis sobre el objetivo.

- **Distribución** (entrega): Proceso en el cual, con las herramientas previamente listadas, se ejecuta el envío de éstas al objetivo de análisis.

- **Explotación**: Tras enviar (distribuir) el ataque al objetivo, esta fase consiste en la explotación de vulnerabilidades analizadas y encontradas en la víctima objetivo.

- **Instalación**: Proceso de descarga e instalación de ficheros maliciosos en el sistema objetivo.

- **Comando y control**: Proceso de implementación de canales de comunicación con la máquina objetivo, por el cual se realiza la ejecución de instrucciones remotas hacia las máquinas comprometidas. De esta manera, se puede obtener un control parcial o total sobre el sistema objetivo de manera remota.

- **Acción sobre los objetivos**: Una vez obtenido el control sobre la máquina, se procede a realizar las acciones en el objetivo por las que se ha diseñado y ejecutado este proceso.

4.2.2 "MITRE ATT&CK" FRAMEWORK

"**MITRE ATT&CK**" [10] consiste en un centro de información accesible a nivel global basado conjunto de tácticas y técnicas para describir y clasificar los comportamientos adversarios en base a observaciones publicadas por investigadores y profesionales de seguridad de todo el mundo. Se trata de una lista estructurada de comportamientos, expresado tanto en matrices, como a través de **STIX** (***Structured Threat Information Expression***) y **TAXII** (***Trusted Automated Exchange of Ingelligence***).

Por un lado, **STIX** es un lenguaje y formato de serialización utilizado para intercambiar inteligencia de ciber amenazas (***Cyber Threat Intelligence*** – **CTI**). Permite a las organizaciones compartir **CTI** entre ellas de manera consistente y legible por máquinas, proporcionando de esta manera una ayuda a comunidad de seguridad para entender los ataques más probables a recibir, y/o a responder a dichos atasques de manera más rápida y eficiente. [11]

TAXII, por otro lado, es un protocolo de capa de aplicación implementado para la comunicación de información de ciber amenazas de manera simple y escalable. Se utiliza este protocolo para intercambiar inteligencia de ciber amenazas (**CTI**) a través de HTTPS. Además, **TAXII** permite a las organizaciones compartir **CTI** mediante **APIs** que alineen con modelos de uso compartido comunes.

El estudio sobre las matrices **TAXII** y **STIX** puede aportar a este trabajo el entendimiento de las **CTI** compartidas y conocidas por las organizaciones, obteniendo de esta manera diversas recomendaciones para prevenir las vulnerabilidades encontradas en el proceso de análisis. Además, permitirá comprender las distintas implementaciones de seguridad que se pueden encontrar en los proveedores.

De igual forma, el estudio sobre matrices de "**MITRE ATT&CK**" existentes puede ser utilizado como base para el diseño de la metodología propuesta para este trabajo de fin de máster. Para ello, se plantea realizar un análisis en profundidad sobre las matrices **MITRE** diseñadas para los diferentes tipos de servicio que proporciona Cloud, previamente explicados.

4.2.2.1 "MITRE ATT&CK" en Cloud

A continuación se muestra la matriz de **"MITRE ATT&CK"** [12] que contiene información sobre las diversas técnicas de ataque que se pueden implementar en un entorno Cloud:

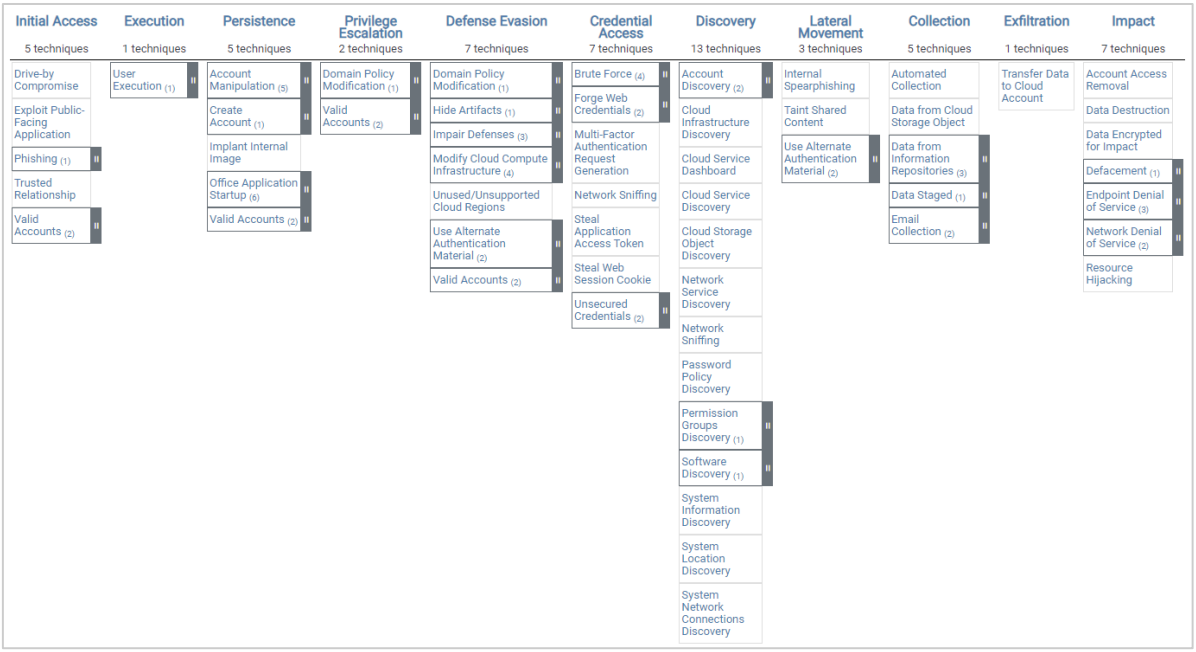

Ilustración 4. Matriz "MITRE ATT&CK" para Cloud

En la parte de **Acceso Inicial**, que se define como la primera fase donde un adversario intenta introducirse en la red privada, las tácticas y técnicas representadas en la matriz para la realización de técnicas de análisis para infraestructuras de la nube son:

- **Compromiso "*Drive-By*"**: Los adversarios pueden obtener acceso a un sistema a través un usuario que, previamente, ha visitado un sitio web durante su curso normal de navegación. Con esta técnica, el objeto de explotación suele ser el navegador web del usuario, aunque algunos adversarios también pueden utilizar páginas web comprometidas para comportamiento de no explotación, como adquirir el ***"token"*** de acceso a la aplicación ("***Application Access token"***)

- **Explotación de aplicaciones públicas**: Se aprovechan vulnerabilidades encontradas en programas, aplicaciones o dispositivos con acceso a Internet. Para ello, utilizan datos, software o comandos para provocar un comportamiento no deseado o imprevisto en el servidor. La debilidad en el sistema puede ser un error, un problema técnico o una vulnerabilidad de diseño. Estas aplicaciones suelen ser sitios web, pero pueden incluir bases de datos (como **SQL**), servicios estándar (como **SMB** o **SSH**), protocolos de gestión y administración de dispositivos de red (como **SNMP** y **Smart Install**) y cualquier otra aplicación con sockets abiertos y accesibles a través de Internet, como servidores web y servicios relacionados.

- ***"Phishing"*:** Los adversarios pueden enviar mensajes de **"*phishing*"** para obtener acceso a los sistemas. Todas las formas de **"*phishing*"** se pueden definir como ingeniería social entregada electrónicamente. El **"*phishing*"** también puede modificar para que sea dirigido, conocido como "***spearphishing"***. En el "***spearphishing"***, el adversario apuntará a una persona, empresa o industria específica. De manera más general, los adversarios pueden realizar **"*phishing*"** no dirigido, como en campañas masivas de spam de malware.

- **Relación de confianza:** Los adversarios pueden violar o aprovecharse de otras organizaciones que tienen acceso a las víctimas objetivo de la organización. El acceso a través de una relación de terceros de confianza explota una conexión existente que puede no estar protegida o recibe menos protección contra los mecanismos estándar para obtener acceso a una red.

- **Cuentas válidas**: Los adversarios pueden obtener y abusar de las credenciales de las cuentas existentes como medio para obtener acceso inicial, persistencia, escalada de privilegios o evasión de defensas implementadas en la organización. Las credenciales comprometidas se pueden usar para eludir los controles de acceso colocados en varios recursos en los sistemas dentro de la red e, incluso, se pueden usar para el acceso persistente a sistemas remotos y servicios disponibles externamente, como **VPN**, **Outlook Web Access** y escritorios remotos. Las credenciales comprometidas también pueden otorgar a un adversario privilegios más elevados para sistemas específicos o, en otro caso, acceso a áreas restringidas de la red. Los adversarios pueden optar por no usar malware o herramientas junto con el acceso legítimo que brindan esas credenciales para dificultar la detección de su presencia.

En segundo lugar, la fase de **Ejecución** consiste en el intento de ejecución de código malicioso. En este caso, la única táctica recomendada es:

- **Ejecución de usuario**: Un adversario puede basarse en acciones específicas de un usuario para lograr la ejecución de código malicioso. Los usuarios pueden estar sujetos a ingeniería social para que ejecuten código como, por ejemplo, abriendo un archivo o enlace de documento malicioso. Estas acciones de usuario generalmente se observarán en comportamientos consecuenciales de técnicas de **"*phishing*"**.

A continuación, las técnicas para **Persistencia** consisten en mantener la ventaja y el punto de apoyo en el proceso de sus ataques. Estas técnicas para la nube son:

- **Manipulación de cuentas**: Los adversarios pueden manipular cuentas para mantener el acceso a los sistemas de las víctimas. La manipulación de cuentas puede consistir en cualquier acción que preserve el acceso del adversario a una cuenta comprometida, como la modificación de credenciales o los grupos de permisos. Estas acciones también podrían incluir actividades diseñadas para subvertir las políticas de seguridad, como realizar actualizaciones de contraseña iterativas para eludir las

políticas de duración de la contraseña y preservar la vida de las credenciales comprometidas.

- **Creación de cuentas**: Los adversarios pueden crear cuentas nuevas para mantener el acceso a los sistemas de las víctimas. Con un nivel suficiente de acceso, se puede utilizar la creación de dichas cuentas para establecer un acceso secundario con credenciales que no requieran la implementación de herramientas de acceso remoto persistente en el sistema.

- **Implantación de una imagen interna:** Los adversarios pueden implantar imágenes de nubes o contenedores con código malicioso para establecer la persistencia después de obtener acceso a un entorno. Se pueden implantar o respaldar **"Amazon Web Services (AWS) Amazon Machine Images (AMI)",** imágenes de **"Google Cloud Platform" (GCP)** e imágenes de **"Azure"**, así como tiempos de ejecución de contenedores populares como "**Docker**". A diferencia de "***Upload Malware***", esta técnica se enfoca en que los adversarios implanten una imagen en un registro dentro del entorno de la víctima.

- **Inicio de aplicación de Office**: Los adversarios pueden aprovechar las aplicaciones basadas en "**Microsoft Office"** para la persistencia entre las empresas emergentes. "**Microsoft Office"** es un conjunto de aplicaciones bastante común en los sistemas operativos basados en "**Windows"** dentro de una red empresarial. Hay varios mecanismos que se pueden usar con "**Office"** para la persistencia cuando se inicia una aplicación basada en "**Office"**; esto puede incluir el uso de complementos y macros de plantillas de "**Office"**.

- **Cuentas válidas**: esta técnica ha sido previamente explicada.

Por otro lado, la fase **Escalada de Privilegios** consiste en la obtención de permisos y privilegios de mayor nivel. En esta fase se muestran:

- **Modificación de la política de dominios**: Los adversarios pueden modificar los ajustes de configuración de un dominio para evadir defensas y/o escalar privilegios en entornos de dominio. Los dominios proporcionan un medio centralizado para administrar cómo los recursos informáticos (p. ej., computadoras, cuentas de usuario) pueden actuar e interactuar entre sí en una red. La política del dominio también incluye opciones de configuración que pueden aplicarse entre dominios en un entorno de varios dominios/bosques. Las modificaciones a la configuración del dominio pueden incluir la alteración de los objetos de directiva de grupo (GPO) del dominio o el cambio de la configuración de confianza para los dominios, incluidas las confianzas de federación.

- **Cuentas válidas**: Esta técnica ha sido previamente explicada.

Para la **Evasión de Defensas** se muestran las técnicas de análisis centrada en la evasión de los procesos de detección implementados en la organización:

- **Modificación de la política de dominios**: Esta técnica ha sido previamente explicada.

- **Ocultación de artefactos**: Los adversarios pueden intentar ocultar artefactos asociados con sus comportamientos para evadir la detección. Los sistemas operativos pueden tener funciones para ocultar varios artefactos, como archivos importantes del sistema y la ejecución de tareas administrativas, para evitar interrumpir los entornos de trabajo de los usuarios y evitar que los usuarios cambien archivos o funciones en el sistema. Los adversarios pueden abusar de estas funciones para ocultar artefactos como archivos, directorios, cuentas de usuario u otra actividad del sistema para evadir la detección.

- **Debilitar las defensas**: Los adversarios pueden modificar maliciosamente los componentes del entorno de una víctima para obstaculizar o desactivar los mecanismos defensivos. Esto no solo implica el deterioro de las defensas preventivas, como los firewalls y los antivirus, sino también las capacidades de detección que los defensores pueden usar para auditar la actividad e identificar el comportamiento malicioso. Esto también puede abarcar tanto defensas nativas como capacidades complementarias instaladas por usuarios y administradores.

- **Modificación la infraestructura de computación de la nube**: Un adversario puede intentar modificar la infraestructura de servicios informáticos de una cuenta en la nube para evadir las defensas. Una modificación de la infraestructura del servicio informático puede incluir la creación, eliminación o modificación de uno o más componentes, como instancias informáticas, máquinas virtuales e instantáneas.

- **Regiones de nube no utilizadas/soportadas**: Los adversarios pueden crear instancias en la nube en regiones de servicios geográficos no utilizados para evadir la detección. El acceso generalmente se obtiene a través de cuentas comprometidas que se utilizan para administrar la infraestructura de la nube.

- **Utilizar material de autenticación alternativo**: Los adversarios pueden utilizar material de autenticación alternativo, como "***hash"*** de contraseñas, ***"tickets"*** de "**Kerberos"** y ***"tokens"*** de acceso a aplicaciones, para moverse lateralmente dentro de un entorno y eludir los controles de acceso normales al sistema.

- **Cuentas válidas**: Esta técnica ha sido previamente explicada.

En **Acceso a Credenciales**, donde se intenta robar nombres y contraseñas de cuentas de usuarios, se encuentran:

- **Fuerza bruta**: Los adversarios pueden usar técnicas de fuerza bruta para obtener acceso a las cuentas cuando se desconocen las contraseñas o cuando se obtienen "***hashes"*** de contraseñas. Sin conocimiento de la contraseña de una cuenta o conjunto de cuentas, un adversario puede adivinar sistemáticamente la contraseña utilizando un mecanismo repetitivo o iterativo. Las contraseñas de fuerza bruta pueden tener lugar a través de la interacción con un servicio que verificará la validez de esas credenciales o fuera de línea con los datos de credenciales adquiridos previamente, como hash de contraseñas.

- **Forjar credenciales web**: Los adversarios pueden falsificar materiales de credenciales que pueden usarse para obtener acceso a aplicaciones web o servicios de Internet. Las aplicaciones y los servicios web (alojados en entornos ***SaaS*** en la nube o servidores locales) a menudo usan cookies de sesión, ***"tokens"*** u otros materiales para autenticar y autorizar el acceso de los usuarios.

- **Generación de solicitudes de autenticación multi-factor**: Los adversarios pueden intentar eludir los mecanismos de autenticación multi-factor (**MFA**) y obtener acceso a las cuentas generando solicitudes de **MFA** enviadas a los usuarios.

- **Rastreo de red**: Los adversarios pueden analizar el tráfico de la red para capturar información sobre un entorno, incluido el material de autenticación que se transmite a través de la red. La detección de redes se refiere al uso de la interfaz de red en un sistema para monitorear o capturar información enviada a través de una conexión por cable o inalámbrica. Un adversario puede colocar una interfaz de red en modo promiscuo para acceder pasivamente a los datos en tránsito a través de la red, o usar puertos de expansión para capturar una mayor cantidad de datos.

- **Robo de *"tokens"* de acceso de aplicación**: Los adversarios pueden robar ***"tokens"*** de acceso a aplicaciones como medio de adquirir credenciales para acceder a sistemas y recursos remotos.

- **Robo de cookies de sesión**: Un adversario puede robar cookies de sesiones de servicios o aplicaciones web y usarlas para obtener acceso a aplicaciones web o servicios de Internet como un usuario autenticado sin necesidad de credenciales. Las aplicaciones y los servicios web a menudo usan cookies de sesión como un ***"token"*** de autenticación después de que un usuario se haya autenticado en un sitio web.

- **Credenciales no seguras**: Los adversarios pueden buscar sistemas comprometidos para encontrar y obtener credenciales almacenadas de forma insegura. Estas credenciales se pueden almacenar o extraviar en muchas ubicaciones de un sistema, incluidos archivos de texto sin formato (p. ej., historial de "**Bash"**), repositorios específicos del sistema operativo o de la aplicación (p. ej., credenciales en el registro) u otros archivos/artefactos especializados (p. ej., claves privadas).

En la fase de **Descubrimiento** se recomienda para averiguar información relacionada sobre el entorno nube las siguientes tácticas:

- **Descubrimiento de cuentas**: Los adversarios pueden intentar obtener una lista de cuentas en un sistema o dentro de un entorno. Esta información puede ayudar a los adversarios a determinar qué cuentas existen para ayudar en el comportamiento de futuros pasos.

- **Descubrimiento de infraestructura de la nube**: Un adversario puede intentar descubrir la infraestructura y los recursos que están disponibles dentro de un entorno de infraestructura como servicio (***IaaS***). Esto incluye recursos de servicios informáticos, como instancias, máquinas virtuales e instantáneas, así como recursos de otros servicios, incluidos los servicios de almacenamiento y base de datos.

- **Panel de servicio en la nube**: Un adversario puede usar una interfaz gráfica de usuario del tablero de servicios en la nube con credenciales robadas para obtener información útil de un entorno operativo en la nube, como servicios, recursos y funciones específicos. Por ejemplo, el Centro de comando de **GCP** se puede usar para ver todos los activos, los hallazgos de posibles riesgos de seguridad y ejecutar consultas adicionales, como encontrar direcciones IP públicas y puertos abiertos.

- **Descubrimiento de servicios de nube**: Un adversario puede intentar enumerar los servicios en la nube que se ejecutan en un sistema después de obtener acceso. Estos métodos pueden diferir desde plataforma como servicio (***PaaS***), infraestructura como servicio (***IaaS***) o software como servicio (***SaaS***). Existen muchos servicios a través de los diversos proveedores de la nube y pueden incluir integración y entrega continua (**CI/CD**), funciones Lambda, **"Azure AD**", entre muchos otros.

- **Descubrimiento de Objetos de almacenamiento de la nube**: Los adversarios pueden enumerar objetos dentro de la infraestructura de almacenamiento en la nube. Los adversarios pueden usar esta información durante el descubrimiento automatizado para dar forma a comportamientos de seguimiento, incluida la solicitud de todos los objetos o de objetos específicos del almacenamiento en la nube. De manera similar al descubrimiento de archivos y directorios en un host local, después de identificar los servicios de almacenamiento disponibles (es decir, el descubrimiento de infraestructura en la nube), los adversarios pueden acceder a los contenidos/objetos almacenados en la infraestructura de la nube.

- **Descubrimientos de servicios de red**: Los adversarios pueden intentar obtener un listado de los servicios que se ejecutan en ***hosts*** remotos y dispositivos de infraestructura de red local, incluidos aquellos que pueden ser vulnerables a la explotación remota de software. Los métodos comunes para adquirir esta información incluyen escaneos de puertos y/o vulnerabilidades utilizando herramientas que se incorporan a un sistema.

- **Rastreo de red**: Esta técnica ha sido previamente explicada

- **Descubrimiento de políticas de contraseñas**: Los adversarios pueden intentar acceder a información detallada sobre la política de contraseñas utilizada dentro de una red empresarial o entorno de nube. Las políticas de contraseñas son una forma de hacer cumplir contraseñas complejas que son difíciles de adivinar o descifrar a través de la fuerza bruta. Esta información puede ayudar al adversario a crear una lista de contraseñas comunes y lanzar ataques de diccionario y/o de fuerza bruta que cumplan con la política (por ejemplo, si la longitud mínima de la contraseña debe ser 8, entonces no probar contraseñas como ***'pass123'***; no verificar para más de 3-4 contraseñas por cuenta si el bloqueo se establece en 6 para no bloquear cuentas).

- **Descubrimiento de grupos de permisos**: Los adversarios pueden intentar encontrar configuraciones de grupos y permisos. Esta información puede ayudar a los adversarios a determinar qué cuentas de usuario y grupos están disponibles, la membresía de los usuarios en grupos particulares y qué usuarios y grupos tienen permisos elevados.

- **Descubrimiento de software**: Los adversarios pueden intentar obtener un listado de software y versiones de software que están instaladas en un sistema o en un entorno de nube. Los adversarios pueden usar la información de "***Software Discovery"*** durante el descubrimiento automatizado para dar forma a comportamientos de seguimiento, incluso si el adversario infecta o no completamente al objetivo y/o intenta acciones específicas.

- **Descubrimiento de información del sistema**: Un adversario puede intentar obtener información detallada sobre el sistema operativo y el hardware, incluida la versión, los parches, las revisiones, los paquetes de servicio y la arquitectura. Los adversarios pueden usar la información del descubrimiento de información del sistema durante el descubrimiento automatizado para dar forma a comportamientos de seguimiento, incluso si el adversario infecta o no completamente al objetivo y/o intenta acciones específicas.

- **Descubrimiento de localización del sistema**: Los adversarios pueden recopilar información en intento para calcular la ubicación geográfica del anfitrión de una víctima. Los adversarios pueden usar la información de "***System Location Discovery***" durante el descubrimiento automatizado para dar forma a comportamientos de seguimiento, incluso si el adversario infecta o no completamente al objetivo y/o intenta acciones específicas.

- **Descubrimiento de conexiones red del sistema**: Los adversarios pueden intentar obtener un listado de las conexiones de red hacia o desde el sistema comprometido

al que están accediendo actualmente o desde sistemas remotos solicitando información a través de la red.

Las técnicas de **Movimiento Lateral** recomendadas para obtener movimiento y acceso a través del entorno de nube son:

- ***Spearphising* interno**: Los adversarios pueden usar el **"*phishing*"** interno para obtener acceso a información adicional, además de poder explotar a otros usuarios dentro de la misma organización después de que ya tengan acceso a cuentas o sistemas dentro del entorno. El **"*phishing*"** interno es una campaña de varias etapas en la que se posee una cuenta de correo electrónico controlando el dispositivo del usuario con malware instalado previamente o comprometiendo las credenciales de la cuenta del usuario. Los adversarios intentan aprovechar una cuenta interna de confianza para aumentar la probabilidad de engañar al objetivo para que caiga en el intento de **"*phishing*"**.

- **Contaminación de contenido compartido**: Los adversarios pueden entregar cargas útiles a sistemas remotos agregando contenido a ubicaciones de almacenamiento compartido, como unidades de red o repositorios de códigos internos. El contenido almacenado en unidades de red o en otras ubicaciones compartidas puede verse contaminado al agregar programas maliciosos, secuencias de comandos o código de explotación a archivos válidos. Una vez que un usuario abre el contenido corrupto compartido, la parte maliciosa se puede ejecutar para ejecutar el código del adversario en un sistema remoto. Los adversarios pueden usar contenido compartido corrupto para moverse lateralmente.

- **Utilizar material de autenticación alternativo:** Esta técnica ha sido previamente explicada

En el proceso de **Recopilación** de información se implementan las siguientes técnicas:

- **Recopilación automatizada**: Una vez establecido dentro de un sistema o red, un adversario puede utilizar técnicas automatizadas para recopilar datos internos. Los métodos para realizar esta técnica podrían incluir el uso de un intérprete de comandos y secuencias de comandos para buscar y copiar información que se ajuste a criterios establecidos, como el tipo de archivo, la ubicación o el nombre en intervalos de tiempo específicos. En entornos basados en la nube, los adversarios también pueden usar API en la nube, interfaces de línea de comandos o servicios de extracción, transformación y carga (**ETL**) para recopilar datos automáticamente. Esta funcionalidad también podría integrarse en herramientas de acceso remoto.

- **Datos obtenidos desde Objetos de almacenamiento de nube**: Los adversarios pueden acceder a los objetos de datos desde un almacenamiento en la nube que no está bien protegido.

- **Datos obtenidos desde Repositorios de información**: Los adversarios pueden aprovechar los repositorios de información para extraer información valiosa. Los repositorios de información son herramientas que permiten el almacenamiento de información, generalmente para facilitar la colaboración o el intercambio de información entre usuarios, y pueden almacenar una amplia variedad de datos que pueden ayudar a los adversarios en otros objetivos o acceso directo a la información de destino. Los adversarios también pueden abusar de las funciones de uso compartido externo para compartir documentos confidenciales con destinatarios fuera de la organización.

- ***Data Staged***: Los adversarios pueden organizar los datos recopilados en una ubicación o directorio central antes de la **Exfiltración**. Los datos pueden guardarse en archivos separados o combinarse en un solo archivo a través de técnicas como **Archivar datos recopilados**. Se pueden usar "***shells***" de comandos interactivos, y se puede usar la funcionalidad común dentro de "***cmd*"** y "***bash"*** para copiar datos en una ubicación de preparación.

- **Recopilación de correos electrónicos**: Los adversarios pueden apuntar al correo electrónico del usuario para recopilar información confidencial. Los correos electrónicos pueden contener datos confidenciales, incluidos secretos comerciales o información personal, que pueden resultar valiosos para los adversarios. Los adversarios pueden recopilar o reenviar correos electrónicos desde servidores o clientes de correo.

Para **Exfiltración** de robo de información, se puede observar las siguientes tácticas:

- **Transferencia de datos a cuentas nube**: Los adversarios pueden exfiltrar datos transfiriéndolos, incluidas las copias de seguridad de entornos en la nube, a otra cuenta en la nube que controlen en el mismo servicio para evitar las típicas transferencias/descargas de archivos y la detección de exfiltración basada en la red.

Finalmente, en la fase de **Impacto** para manipular, interrumpir o destruir sistemas y/o datos se recomiendan las siguientes técnicas:

- **Eliminación de acceso a la cuenta**: Los adversarios pueden interrumpir la disponibilidad de los recursos del sistema y de la red al inhibir el acceso a las cuentas utilizadas por usuarios legítimos. Las cuentas se pueden eliminar, bloquear o manipular (por ejemplo, cambiar las credenciales) para eliminar el acceso a las cuentas. Los adversarios también pueden cerrar sesión posteriormente y/o realizar un apagado/reinicio del sistema para establecer cambios maliciosos en su lugar.

- **Destrucción de datos**: Los adversarios pueden destruir datos y archivos en sistemas específicos o en grandes cantidades en una red para interrumpir la disponibilidad de los sistemas, servicios y recursos de la red. Es probable que la destrucción de datos haga que los datos almacenados sean irrecuperables mediante técnicas forenses

mediante la sobreescritura de archivos o datos en unidades locales y remotas. Los c2omandos comunes de eliminación de archivos del sistema operativo, como "***del"*** y "***rm"***, a menudo solo eliminan los punteros a los archivos sin borrar el contenido de los archivos, lo que hace que los archivos se puedan recuperar mediante la metodología forense adecuada. Este comportamiento es distinto del Borrado del contenido del disco y el Borrado de la estructura del disco porque se destruyen los archivos individuales en lugar de las secciones de un disco de almacenamiento o la estructura lógica del disco.

- **Datos encriptados para el impacto**: Los adversarios pueden cifrar los datos en los sistemas de destino o en una gran cantidad de sistemas en una red para interrumpir la disponibilidad de los recursos del sistema y de la red. Pueden intentar hacer que los datos almacenados sean inaccesibles cifrando archivos o datos en unidades locales y remotas y reteniendo el acceso a una clave de descifrado. Esto se puede hacer para obtener una compensación monetaria de una víctima a cambio del descifrado o una clave de descifrado ("***ransomware"***) o para hacer que los datos sean permanentemente inaccesibles en los casos en que la clave no se guarde o transmita.

- ***"Dafecement"***: Los adversarios pueden modificar el contenido visual disponible interna o externamente a una red empresarial, afectando así la integridad del contenido original. Las razones para la desfiguración incluyen enviar mensajes, intimidar o reclamar crédito (posiblemente falso) por una intrusión. Se pueden usar imágenes perturbadoras u ofensivas como parte de "***Defacement***" para causar molestias al usuario o para presionar el cumplimiento de los mensajes adjuntos.

- **Denegación de servicio en puntos finales**: Los adversarios pueden realizar ataques de denegación de servicio (**DoS**) de punto final para degradar o bloquear la disponibilidad de los servicios para los usuarios. "***Endpoint DoS***" se puede realizar agotando los recursos del sistema en los que están alojados esos servicios o explotando el sistema para causar una condición de bloqueo persistente. Los servicios de ejemplo incluyen sitios web, servicios de correo electrónico, DNS y aplicaciones basadas en web. Se ha observado a los adversarios realizando ataques **DoS** con fines políticos y para apoyar otras actividades maliciosas, incluida la distracción, el "***hacktivismo***" y la extorsión.

- **Denegación de servicio de red**: Los adversarios pueden realizar ataques de denegación de servicio (**DoS**) de red para degradar o bloquear la disponibilidad de los recursos específicos para los usuarios. El **DoS** de red se puede realizar agotando el ancho de banda de la red en el que se basan los servicios. Los recursos de ejemplo incluyen sitios web específicos, servicios de correo electrónico, DNS y aplicaciones basadas en la web.

- ***"Hijacking"* de recursos**: Los adversarios pueden aprovechar y utilizar los recursos de los sistemas cooptados para resolver problemas intensivos en recursos, lo que

puede afectar la disponibilidad del sistema y/o del servicio alojado. De esta manera, los adversarios pueden consumir recursos del sistema para impactar negativamente y/o conseguir que las máquinas afectadas dejen de responder.

Esta matriz de **"MITRE ATT&CK"** se utilizará más adelante para el diseño de la metodología de análisis de seguridad en Cloud.

Además, cabe destacar que esta matriz se compone de otras matrices relacionadas con diferentes proveedores y servicios de nube, que son:

- **"Office 365"**
- **"Azure AD"**
- **"Google Workspace"**
- ***SaaS***
- ***IaaS***

4.2.3 SISTEMA DE PUNTUACIÓN DE VULNERABILIDADES (CVSS)

El Sistema de **Puntuación de Vulnerabilidades** (**CVSS**) [13] se trata de un estándar actual para evaluar la severidad de un fallo de seguridad. Este estándar proporciona una visión objetiva e imparcial del impacto que podría suponer la aparición de una amenaza en la organización.

La **clasificación de la severidad** (***Base Score***) se basa en los 8 siguientes aspectos:

- **Vector de ataque** (**AV**): Analiza dónde debe localizarse el adversario, en relación con el componente afectado, para poder aprovecharse de la vulnerabilidad encontrada. La gravead de mayor nivel se corresponde con aquellos fallos que no requieren que el adversario se encuentre conectado a ninguna red en particular, como una intranet. Por otro lado, el nivel más bajo proviene de los fallos en donde el ataque requiere tener un acceso físico y autenticado al sistema donde reside el componente. Los diversos niveles de esta métrica, de más alto a más bajo, son: Red (***Network - N***), Adyacente (***Adjacent - A***), Local ***(L***) y Físico (***Physical – P***)

- **Complejidad del ataque** (**AC**): En este caso se analiza la fiabilidad con la que se puede explotar la vulnerabilidad de seguridad y, a su vez, si existen factores más allá del control de los adversarios necesarios para ejecutar el ataque con éxito. En otras palabras, los fallos de alta complejidad (***High – H***) van a requerir pasos adicionales para asegurar que el ataque tenga éxito, mientras que aquellos con complejidad baja (***Low – L***) siempre pueden ser explotados.

- **Privilegios requeridos** (**PR**): analiza el nivel de acceso necesario para llegar al componente vulnerable, desde aquellos donde no se filtra por ningún proceso de autenticación (***None – N***), a una autenticación básica (***Low – L***) o a una a nivel administrativo (***High – H***)

- **Interacción del usuario** (**UI**): Analiza si es necesario que un usuario perteneciente al componente impactado deba realizar una acción específica para explotar el fallo de seguridad con éxito como (***Required – R***), por ejemplo, acceder a una URL maliciosa. Los fallos de alta severidad se corresponden con aquellos donde ningún usuario deba realizar ninguna acción (***None – N***).

- **Alcance** (**S**): analiza si el componente vulnerable y el impactado se encuentra alienados, es decir, si se encuentran gestionados por la misma autoridad. Los componentes vulnerables que únicamente afectan a aquellos gestionados por la misma autoridad (***Unchanged – U***) se considera un nivel de severidad menor en comparación con aquellos que afectan a componentes adicionales en diferentes contextos de seguridad (***Changed – C***)

- **Confidencialidad** (**C**): analiza el impacto en la confidencialidad e los recursos de información gestionados por un componente de software vulnerable. La confidencialidad se refiere a la limitación del acceso y la divulgación de la información únicamente a usuarios autorizados, categorizándose el impacto como ninguno (***None – N***), bajo para los casos donde el atacante no tenga control sobre la cantidad o el tipo de información que está observando (***Low - L***) y alto para aquellos casos donde sí tiene el control (***High – H***)

- **Integridad** (**I**): analiza la capacidad de los atacantes de manipular la información gestionada por un componente vulnerable tras ser explotado, categorizándose en casos donde no tenga capacidad de modificación (***None – N***), pueda modificar ciertos datos sin tener control de las consecuencias de dicha alteración (***Low – L***) y, finalmente, donde se haya perdido completamente la integridad de la información (***High – H***)

- **Disponibilidad** (**A**): mide el impacto en la disponibilidad del componente afectado tras sufrir una explotación. Se refiere al nivel de pérdida de disponibilidad del propio componente como servicio en red, pudiendo ser inexistente dada a su robustez (***None – N***), una pérdida parcial o temporal (***Low – L***) o una perdida completa de disponibilidad (***High – H***)

A su vez, existen unas **métricas temporales** (***Temporal Score***) que miden el estado actual de las técnicas de explotación o la disponibilidad de código, la existencia de parches o soluciones, o la fiabilidad que se tiene en la descripción de un fallo de seguridad:

- **Madurez del código de explotación** (**E**): mide la probabilidad de que el fallo de seguridad se explotado y se suele basar en el estado actual de las técnicas de explotación, la disponibilidad de código de explotación o la explotación activa, "***in-the-wild***"

- **Nivel de remediación** (**RL**): la implementación de soluciones temporales (o **"*hotfixes*"**) ofrecen una solución provisional hasta que se publique un parche o una actualización oficial que arregle el problema de seguridad.

- **Indicador de fiabilidad** (**RC**): mide el grado de confianza en la existencia de fallos de seguridad y, además, la credibilidad de los detalles técnicos ya conocidos. Esta métrica sugiere también el nivel de conocimiento técnico del que disponen los atacantes.

La **severidad de fallos** de seguridad encontrados se obtendrá a partir del cálculo de esta tabla de criticidad, que viene definida de la siguiente forma:

Criticidad CVSS 3.1	
Crítica	Trazas con valor entre 9.0 – 10.0
Alta	Trazas con valor entre 7.0 – 8.9
Media	Trazas con valor entre 4.0 – 6.9
Baja	Trazas con valor entre 0.1 – 3. 9
Informativa	Trazas con valor 0.0

Tabla 8. Criticidad CVSS 3.1

Este sistema de puntuación se implementará en la metodología diseñada para indicar el nivel de severidad de cada una de las posibles vulnerabilidades encontradas a informar.

4.3 MODELADO DE AMENAZAS

En este apartado se procede a realizar el análisis de los ejercicios de análisis de seguridad ofensiva más comúnmente utilizados para cada uno de los tres proveedores. En este modelado de amenazas, a su vez se realizará un estudio sobre los componentes de la infraestructura de la nube de mayor relevancia, además de aquellos que estén relacionados con un tipo de ataque. Por último, se realizará una búsqueda exhaustiva de posibles herramientas actuales que puedan proporcionar ayuda e información adicional en el análisis de seguridad.

4.3.1 "GOOGLE CLOUD PLATFORM" – GCP

4.3.1.1 Componentes

4.3.1.1.1 Google IAM

La **herramienta de Gestión de Identidades y Accesos (IAM)** de **GCP** [14] permite crear y administrar permisos para los recursos de "**Google Cloud"**. **IAM** unifica el control de acceso para los servicios de "**Google Cloud"** en un solo sistema y, además, presenta un conjunto de operaciones coherente. En otras palabras, proporciona visibilidad y control de acceso pormenorizados para gestionar de forma centralizada los recursos en la nube.

Algunas de sus características son:

- Una única interfaz para controlar el acceso
- Control pormenorizado – concede a los usuarios acceso a nivel de recursos en lugar de solo a nivel de proyecto
- Recomendaciones automáticas para controlar el acceso
- Acceso contextual
- Roles flexibles
- Acceso web, programático y por línea de comandos
- Registro de auditorías integrado
- Compatibilidad con "**Cloud Identity"**

4.3.1.1.2 Google Cloud Storage buckets

"Google Cloud Storage" es el lugar de almacenamiento de archivos de "**Google"**. La denominación de ***"bucket"*** se les asigna a los contenedores lógicos para el guardado de objetos, es decir, como una carpeta raíz donde se conservan los datos [15]. Todo lo que se almacene en "**Google Cloud Storage"** se debe contener en un ***"bucket"***.

4.3.1.1.3 Resource Manager

"Resource Manager" [16] se trata de una herramienta de "**Google Cloud"** que ayuda en la organización de recursos, permitiendo la agrupación y organización de manera jerárquica de los recursos de "**Google Cloud"**. De esta manera, es posible administrar los recursos de contenedor para administrar a su vez aspectos como el control de acceso y la configuración.

4.3.1.1.4 GCP Command Center

"GCP Security Command Center" es la plataforma de gestión de riesgos y seguridad de "**Google Cloud"**. Se trata de un servicio centralizado de informes de vulnerabilidades y amenazas [17], realizando una evaluación de la superficie de ataque de datos y seguridad.

Sus funcionalidades principales son:

- Descubrimiento e inventario de recursos
- Prevención de amenazas

4.3.1.1.5 Google Cloud CLI – *"gcloud"*

La "**CLI de Google Cloud"** [18] es un conjunto de herramientas para crear y administrar recursos de "**Google Cloud"**. Se puede utilizar esta herramienta para realizar múltiples tareas comunes en la plataforma desde la línea de comandos o, en otro caso, a través de secuencias de comandos y otras automatizaciones.

Algunas instancias que se pueden crear y administrar a través de esta **CLI** son:

- Instancias de máquina virtual de "**Google Compute Engine"** y otros recursos
- Instancias de **Cloud SQL**
- Clústeres de **Google** "**Kubernetes Engine"**
- Clústeres y trabajos de "**Dataproc"**
- Zonas administradas y conjuntos de registros de **Cloud DNS**

- Implementaciones de "**Cloud Deployment Manager**"

Por otro lado, también se puede usar la **CLI** de ***"gcloud"*** para implementar aplicaciones "**App Engine"**, administrar la autenticación, personalizar la configuración local y realizar otro tipo de tareas.

4.3.1.2 Fases

4.3.1.2.1 Reconocimiento y Descubrimiento

Descubrimiento de Cuentas

La utilización de herramientas automatizadas puede resultar de ayuda para el descubrimiento de cuentas de organización. Algunos ejemplos son:

- **"ShimRatReporter"** – lista todos las cuentas privilegiadas y no privilegiadas disponibles en una máquina

- **"XCSSET"** – realiza el descubrimiento de cuentas de varias localizaciones como: "**Evernote**", "**AppleID"**, "**Telegram"** y "**Skype"**.

Cloud Service Dashboard

Un adversario, a través del uso de credenciales previamente obtenidas, puede usar "***Cloud Service Dashboard GUI"*** para obtener información adicional como, por ejemplo, servicios, recursos y funciones. En el caso de "**Google"**, se puede utilizar "**GCP Command Center**" para observar todos los activos, los hallazgos de posibles riegos de seguridad y, además, para ejecutar consultas adicionales, como encontrar direcciones IP públicas y puertos abiertos.

Descubrimiento de Cloud Service

Una vez obtenido el acceso a la nube, es posible realizar la enumeración de los servicios de nube ejecutándose en el sistema.

Descubrimiento de Grupos de Permisos

A través de ciertas herramientas, es posible hallar la configuración de grupos y permisos. Esto permite descubrir información sobre las cuentas de usuario y grupos que se encuentran disponibles, además de los usuarios que forman parte de un grupo y cuáles tienen permisos elevados.

Algunas de estas herramientas son:

- **"IceID"** – identificar los miembros de "**Workgroup"**

- **"MURKYTOP"** – obtener información sobre grupos

- **"ShimRatReporter"** – obtener los privilegios locales en el host infectado
- **"Siloscape"** – chequea los permisos de un nodo "**Kubernetes**"
- **"TA505"** – usa "**TinyMet"** para enumerar miembros de grupos privilegiados
- **"TrickBot"** – puede identificar los grupos a los que pertenece un usuario en un host comprometido

Descubrimiento de Software

El hallazgo de las versiones de ***software*** implementados en una aplicación puede permitir el descubrimiento de versiones desactualizadas y vulnerables a ciertos ataques. En resumen, obtener información adicional para escoger el procedimiento de ataque a seguir.

Algunos ataques que aprovechan esta vulnerabilidad son:

- **"Bazar"** – realiza llamadas a "***Registry***" para descubrir aplicaciones instaladas
- **"BRONZE BUTTLER"**
- **"Bundlore"** – enumerar qué navegador se está utilizando además de la versión
- **"CharmPower"** – lista todas las aplicaciones instaladas en un host comprometido
- **"Cobalt Strike"**
- **"ComRAT"**
- **"Dridex"**
- **"DustySky"**
- **"HotCroissant"**
- **"Inception"**
- **"InvisiMole"**

4.3.1.2.2 Enumeración

Si se consigue autenticarse en "**Google"** con ***"gcloud"***, uno de los pasos más importantes es obtener información sobre la infraestructura Cloud. Las diversas enumeraciones [19] que se pueden realizar con ***"gcloud"*** son:

- Máquinas Virtuales
- Proyectos y repositorios
- ***"Buckets"*** de almacenamiento
- Aplicaciones web y **SQL**
- Red
- Contenedores
- Funciones sin servidor ("**Lambda**")
- Bases de datos

4.3.1.2.3 Acceso Inicial

Phising

El método principal para la obtención de información, credenciales y, en general, primer paso para el acceso inicial es a través de **"*phishing*"**. En el caso de "**Google"**, existe un ataque específico denominado "***Inyección de eventos de calendario"***.

"Google Calendar" se trata de una de las múltiples funcionalidades que ofrece "**Google"** con las cuentas de correo. Este servicio puede crear eventos con cierto nivel de urgencia con el objetivo de alertar a usuarios sobre un evento que se encuentra almacenado en el calendario. La herramienta "**MailSniper"** incluye unos módulos que permite inyectar eventos en calendarios objetivo. De esta manera, se puede realizar una alerta a un usuario que le redirecciona a una página de autenticación de "**Google"** falsa, pudiendo obtener de esta manera sus credenciales de usuario.

Cuentas válidas

El uso de cuentas de usuarios que ya no formen parte de la organización pero que sigan funcionando dentro de la infraestructura puede resultar un punto de interés para obtener acceso. Especialmente en el caso de credenciales de usuarios que ya no utilicen la cuenta, ya que será menos probable que el robo sea detectado.

4.3.1.2.4 Escalada de privilegios

Robo de "tokens" de Acceso

Un método para obtener credenciales es a través del robo de ***"tokens"*** de acceso implementados en aplicaciones. Los ***"tokens"*** de acceso de aplicaciones se utilizan para realizar peticiones de API autorizadas en nombre de un usuario o aplicación para obtener acceso a recursos en la nube y otras aplicaciones basadas en contenedores. Con el robo de ***"tokens"*** API de cuentas en la nube y en entornos contenedorizados es posible también acceder a datos y realizar acciones con los permisos de las cuentas obtenidas, lo que puede conducir a escalado de privilegios.

En el caso de "**Google"**, se utiliza "**Google JSON *tokens"***, para el acceso de cuentas de servicio a **GCP**, y "***credentials.db"***, donde se almacenan las credenciales de autenticación con ***"gcloud"***. Los ***"tokens"*** de **JSON** también se utilizan para autenticar con ***"gcloud"*** y "**ScoutSuite"**.

Robo de Cookies de sesión

Un adversario puede robar cookies de sesión de servicios o aplicaciones web y usarlas para obtener acceso a aplicaciones web o servicios de Internet como un usuario autenticado sin necesidad de utilizar credenciales. Las aplicaciones y los servicios web a menudo usan cookies de sesión como un ***"token"*** de autenticación tras la autenticación de un usuario en una aplicación web. La comprobación del tiempo de expiración de las cookies puede ayudar a observar si existe un máximo tiempo de vida o si se mantienen abiertas hasta la terminación de la sesión.

***Generación de peticiones de* MFA**

Un método de prevención de robo de credenciales es la implementación de Autenticación Multi-Factor (**MFA**). Sin embargo, es posible "***bypasear***" esta prevención al abusar la generación automática de notificaciones para los servicios **MFA** como "**Duo Push"**, "**Microsoft Authenticator"**, "**Okta"** u otros servicios similares. En algunos casos, los adversarios pueden repetir continuamente los intentos de inicio de sesión para bombardear a los usuarios con notificaciones automáticas de **MFA**, mensajes **SMS** y llamadas telefónicas, lo que puede resultar en que el usuario finalmente acepte la solicitud de autenticación en respuesta a la "**fatiga de *MFA***".

4.3.1.2.5 Movimiento Lateral

Spearphising interno

Al adquirir información adicional sobre la infraestructura interna, es posible diseñar ataques de **"*phishing*"** más elaborados y dirigidos a usuarios concretos, lo que se denomina como "***spearphising"***. Este método permite obtener acceso a información adicional o, por otro lado, realizar la explotación de otros usuarios que se encuentran dentro de una misma

organización. Al introducir archivos maliciosos o enlaces a páginas web de autenticación falsas, es posible obtener credenciales de otros usuarios con acceso a otras zonas de la organización o, incluso, con privilegios más elevados.

Utilización de Material de autenticación alternativo

Es posible utilizar material de autenticación alternativo, como ***hash*** de contraseñas, ***"tickets"*** de "**Kerberos"** y ***"tokens"*** de acceso a aplicaciones, para moverse lateralmente dentro de un entorno y eludir los controles de acceso.

Los procesos de autenticación generalmente requieren una identidad válida (p. ej., nombre de usuario) junto con uno o más factores de autenticación (p. ej., contraseña, **PIN**, tarjeta inteligente física, generador de ***"tokens"***, etc.). Los sistemas generan material de autenticación alternativo tras la autenticación de un usuario o una aplicación, proporcionando una identidad válida y los factores de autenticación requeridos. También se puede generar material de autenticación alternativo durante el proceso de creación de identidad.

El almacenamiento en caché de material de autenticación alternativo permite que el sistema verifique que una identidad se haya autenticado con éxito sin pedirle al usuario que vuelva a ingresar los factores de autenticación. Debido a que el sistema debe mantener la autenticación alternativa, ya sea en la memoria o en el disco, puede correr el riesgo de ser robada a través de las técnicas de acceso de credenciales. Al robar material de autenticación alternativo, los adversarios pueden eludir los controles de acceso al sistema y autenticarse en los sistemas sin conocer la contraseña de texto sin formato ni ningún factor de autenticación adicional.

4.3.1.2.6 Persistencia

Manipulación de cuentas

Consiste en la manipulación de las cuentas para mantener el acceso a los sistemas de las víctimas. La manipulación de cuentas puede consistir en cualquier acción que preserve el acceso del adversario a una cuenta comprometida, como la modificación de credenciales o grupos de permisos. Estas acciones también podrían incluir actividad de la cuenta diseñada para subvertir las políticas de seguridad, como realizar actualizaciones de contraseña iterativas para eludir las políticas de duración de la contraseña y preservar la vida de las credenciales comprometidas.

Para crear o manipular cuentas, es necesario tener suficientes permisos en los sistemas o el dominio. Sin embargo, la manipulación de cuentas también puede dar lugar a una escalada de privilegios en la que las modificaciones otorgan acceso a funciones adicionales, permisos o cuentas válidas con mayores privilegios.

4.3.1.2.7 Minado de datos

Obtención de datos de Repositorios de Información

Se puede aprovechar los repositorios de información para extraer información valiosa. Los repositorios de información son herramientas que permiten el almacenamiento de información, generalmente para facilitar la colaboración o el intercambio de información entre usuarios, y pueden almacenar una amplia variedad de datos que pueden ayudar a los adversarios en otros objetivos u obtener acceso directo a la información de destino. Los adversarios también pueden abusar de las funciones de uso compartido externo para compartir documentos confidenciales con destinatarios fuera de la organización.

La siguiente es una breve lista de información de ejemplo que puede tener un valor potencial para un adversario y que también se puede encontrar en un repositorio de información:

- Políticas, procedimientos y estándares
- Diagramas de red físicos/lógicos
- Diagramas de arquitectura del sistema
- Documentación técnica del sistema
- Credenciales de prueba/desarrollo
- Cronogramas de trabajo/proyecto
- Fragmentos de código fuente
- Enlaces a redes compartidas y otros recursos internos

La información almacenada en un repositorio puede variar según la instancia o el entorno específico. Los repositorios de información comunes específicos incluyen plataformas basadas en web como "**Sharepoint"** y "**Confluence"**, servicios específicos como repositorios de códigos, bases de datos IaaS, bases de datos empresariales y otra infraestructura de almacenamiento como "**SQL Server"**.

4.3.1.3 Herramientas

4.3.1.3.1 PurplePanda

"PurplePanda" es una herramienta [20] que obtiene recursos de diferentes aplicaciones de Cloud/SaaS centrándose en los permisos para identificar rutas de escalada de privilegios y permisos peligrosos en las configuraciones de Cloud/***SaaS***. Busca tanto rutas de escalada de privilegios dentro de una plataforma como entre diferentes plataformas.

4.3.1.3.2 Hayat

"Hayat" [21] es un script de auditoría y refuerzo para los servicios de **"Google Cloud Platform"** como:

- Gestión de acceso e identidad (**IAM**)
- Registro y monitorización
- Redes
- Máquinas virtuales
- Almacenamiento en Instancias de **Cloud SQL**
- Clústeres de "**Kubernetes**"

4.3.1.3.3 GCPbucketBrute

"GCPbucketBrute" [22] enumera ***"buckets"*** de "**Google Storage"**, determinar que accesos se tienen a ellos y determinar si se pueden escalar los privilegios.

- Este script (opcionalmente) acepta las credenciales de la cuenta de servicio/usuario de **GCP** y una palabra clave.
- Se generará una lista de permutaciones a partir de esa palabra clave que luego se usará para buscar la existencia de depósitos de almacenamiento de **Google** con esos nombres.
- Si se proporcionan las credenciales, la mayor parte de la enumeración se seguirá realizando sin autenticación, pero para cualquier depósito que se descubra a través de la enumeración no autenticada, intentará enumerar los permisos del depósito mediante la "***API TestIAMPermissions"*** con las credenciales proporcionadas. Esto ayudará a encontrar depósitos a los que se pueda acceder mientras estén autenticados, pero no mientras no estén autenticados.
- Independientemente de si se proporcionan o no las credenciales, la secuencia de comandos intentará enumerar los permisos del depósito mediante la ***API*** "***TestIAMPermissions"*** mientras no esté autenticado. Esto significa que si no se implementa las credenciales, solo se mostrarán los privilegios que tiene un usuario no autenticado, pero si ingresa las credenciales, se verá qué acceso tienen los usuarios autenticados en comparación con los usuarios no autenticados.

- ADVERTENCIA: si se proporcionan credenciales, el nombre de usuario puede divulgarse en los registros de acceso de cualquier grupo que se descubra.

4.3.1.3.4 GCP IAM Collector

"GCP IAM Collector" [23] es un conjunto de scripts de "**Python"** diseñados para colectar y visualizar permisos de "**GCP IAM"**. Se genera un diagrama "**GCP IAM"** que se visualizará en una página **HTML**.

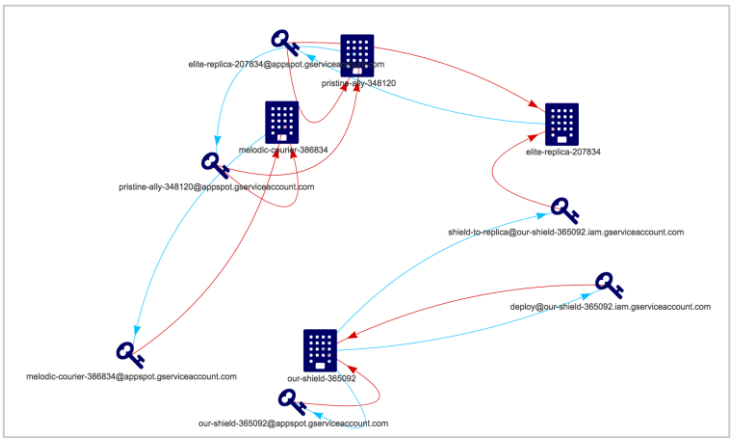

Ilustración 5. Ejemplo resultado GCP IAM Collector

El "**GCP IAM Collector"** itera sobre los proyectos mediante la API de "**Google Cloud Resource Manager"** y los vuelca en archivos **CSV**:

- Todos los proyectos **GCP** disponibles
- Permisos de **IAM** de proyectos
- Cuenta de servicio de proyectos y sus claves
- **LCA** de conjuntos de datos de **BigQuery**
- **LCA** de depósitos de "**Cloud Storage**"

Actualmente, el gráfico de **IAM** es compatible con:

- Proyectos de **GCP** y sus permisos
- Cuentas de servicio y sus permisos

4.3.1.3.5 GCP Firewall Enum

"GCP Firewall Enum" [24] es una herramienta que analiza la salida de diferentes comandos de ***"gcloud"*** para determina que instancias de computación tiene puertos de red expuestos al público. Durante el análisis se generan diversos archivos:

- ***"Applied-rules.csv"*** – Muestra el nombre de la instancia de computación, la dirección IP externa, los puertos TCP permitidos, los puertos UDP permitidos
- ***"Open-rules.csv"*** – Muestra el enlace completo a las reglas de firewall que exponen todos los puertos
- ***"Run-nmap.sh"*** – Una secuencia de comandos "***nmap***" dirigida para escanea cada instancia solo en los puertos expuestos
- ***"Run-masscan.sh"*** – Un script "***Masscan***" dirigido para escanear todos los puertos TCP en instancias de computación con reglas que exponen todo el rango de puertos TCP

4.3.1.3.6 Cloud Enum

"Cloud Enum" [25] es una herramienta "***Multi-Cloud OSINT***". Enumera los recursos públicos en **AWS**, **"Azure"** y "**Google Cloud**".

Para cada proveedor, enumera los siguientes recursos:

- **AWS**: S3 ***"buckets"*** abiertos/protegidos y **AWSAPPs** (WorkMail, WorkDocs, Connect, entre muchos otros)
- **Microsoft "Azure"**: Cuentas de almacenamiento, Contenedores de almacenamiento Blob abiertos, Bases de datos alejados, máquinas virtuales y aplicaciones web
- **GCP**: "**GCP *buckets"*** abiertos/protegidos, Bases de datos a tiempo real de "**Firebase"** abiertos/protegidos, sitios de "**Google App Engine"** y Funciones Cloud

4.3.1.3.7 ScoutSuite

"ScoutSuite" [26] es una herramienta de auditoría de seguridad de código abierto compatible para múltiples nubes, que permite la evaluación del nivel de seguridad de los entornos de nube. Usando las API expuestas por los proveedores de la nube, "**ScoutSuite"** recopila información de configuración para la inspección manual y resalta las áreas de riesgo. En lugar de pasar por docenas de páginas en las consolas web, "**ScoutSuite"** presenta automáticamente una vista clara de la superficie de ataque.

4.3.1.3.8 MailSniper

"MailSniper" [27] es una herramienta de penetración para buscar términos específicos (contraseñas, información privilegiada, información de arquitectura de red, etc.) en el correo electrónico en un entorno de "**Microsoft Exchange**". Puede ser utilizado como usuario no administrativo para buscar su propio correo electrónico o por un administrador de "**Exchange"** para buscar en los buzones de correo de cada usuario en un dominio.

"MailSniper" también incluye módulos adicionales para rociar contraseñas, enumerar usuarios y dominios, recopilar la Lista global de direcciones (**GAL**) de **OWA** y **EWS** y verificar los permisos de buzón para cada usuario de "**Exchange**" en una organización.

4.3.2 "AMAZON WEB SERVICES" – AWS

4.3.2.1 Componentes

4.3.2.1.1 AWS IAM

"AWS Identity and Access Management (IAM)" [28] es un servicio web que ayuda a controlar el acceso a los recursos **AWS**. En resumen, controla: quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.

Algunas de las características de **IAM** son:

- Acceso compartido a la cuenta de **AWS** – Es posible conceder permiso a otras personas para administrar y utilizar los recursos de la cuenta de **AWS** sin tener que compartir contraseña o clave de acceso

- Permisos detallados – Es posible conceder diferentes permisos a diferentes personas para diferentes recursos.

- Acceso a los recursos de **AWS** para aplicaciones que se estén ejecutando en "**Amazon EC2"** – Es posible utilizar características de **IAM** para proporcionar credenciales para las aplicaciones que se encuentren ejecutando en instancias **EC2**. Estas credenciales proporcionan permisos a la aplicación para obtener acceso a otros recursos de **AWS**.

- **Autenticación Multi-Factor (MFA)**

- Identidad federada – Permitir que los usuarios que se encuentren registrado en otros lugares (como en una red corporativa o en un proveedor de identidad e Internet), puedan obtener acceso temporal a la cuenta de **AWS**

- Información de identidad para realizar un control – Si se implementa de manera complementaria "**AWS CloudTrail"**, se mandarán registros de log que incluyen información sobre los usuarios que realizaron solicitudes de recursos en la cuenta.

- Conformidad con "**DSS de PCI"** – **IAM** permite el procesamiento, almacenamiento y la transmisión de datos de tarjetas de crédito por parte de un comerciante o proveedor de servicios. Se encuentra validado conforme el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (**PCI DSS**)

- Integración con otros servicios de **AWS** – **Amazon** proporciona un listado [29] de servicios y acciones de **AWS** que son compatibles con **IAM**

4.3.2.1.2 Amazon Simple Storage Service (S3)

"Amazon Simple Storage Service (**Amazon S3**)" [30] es un servicio de almacenamiento de objetos. Este servicio de **AWS** ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento a los servicios de nube de una organización. Da la posibilidad de almacenar datos para cualquier vaso de uso, como lagos de datos, aplicaciones nativas en la nube y las aplicaciones móviles. Cuenta con diversas características que le permite organizar y administrados los datos con el objetivo de permitir casos de uso específico, obtener rentabilidad, reforzar la seguridad y/o satisfacer los requisitos normativos.

Los datos se almacenan como objetos dentro de los recursos llamados "***Amazon buckets"***. Estos ***"buckets"*** [31] son fundamentalmente contenedores de objetos donde, como ya se ha mencionado, se almacena datos en "**Amazon S3"**. Cada uno de los objetos tiene una clave (o nombre de clave) que se trata del identificador único dentro del ***"bucket"***.

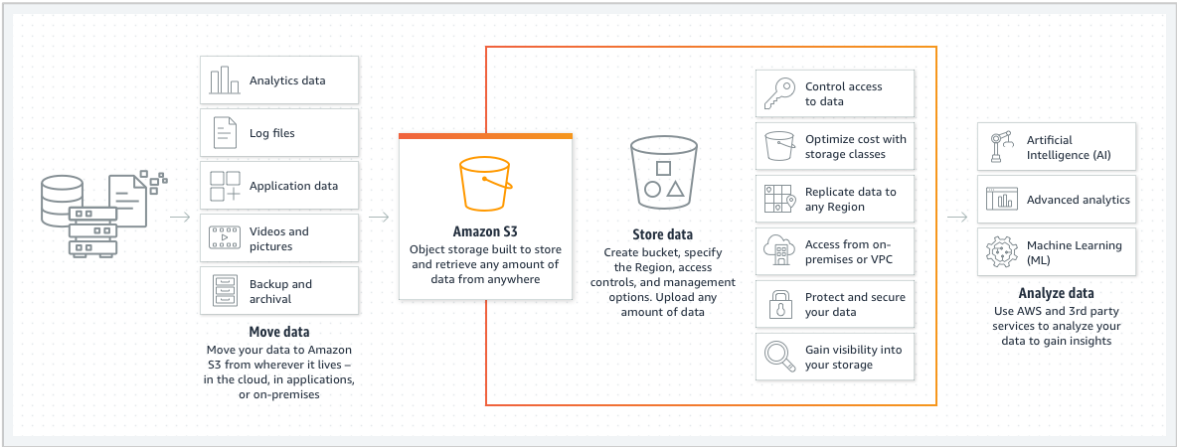

Ilustración 6. Funcionamiento Amazon Simple Storage Service (S3)

Algunos casos de uso de "**Amazon S3"** son:

- Creación de un lago de datos
- Copia de seguridad y restauración de datos fundamentales
- Archivos de datos
- Ejecución de aplicaciones en la nube

4.3.2.1.3 Amazon Elastic Compute Cloud (Amazon EC2)

"Amazon Elastic Compute Cloud (Amazon EC2)" [32] ofrece una plataforma de computación con la posibilidad de elegir el procesador, almacenamiento, redes, sistema operativo y modelo de compra más reciente. Una instancia de "**Amazon EC2"** se trata de un servidor virtual en "**Amazon Elastic Compute Cloud"** que tiene como funcionalidad

ejecutar aplicaciones en la infraestructura de **AWS**. En resumen, ofrece una capacidad de computación segura y de tamaño ajustable para cualquier tipo de carga de trabajo.

4.3.2.1.4 Amazon Elastic Block Store (EBS)

"Amazon Elastic Block Store" (**EBS**) [33] es un servicio de almacenamiento en bloque para "**Amazon Elastic Compute Cloud** (**Amazon EC2**)". Un volumen de "**Amazon EBS"** [34] es un dispositivo de almacenamiento de nivel de bloque duradero que puede ser adjuntado a instancias.

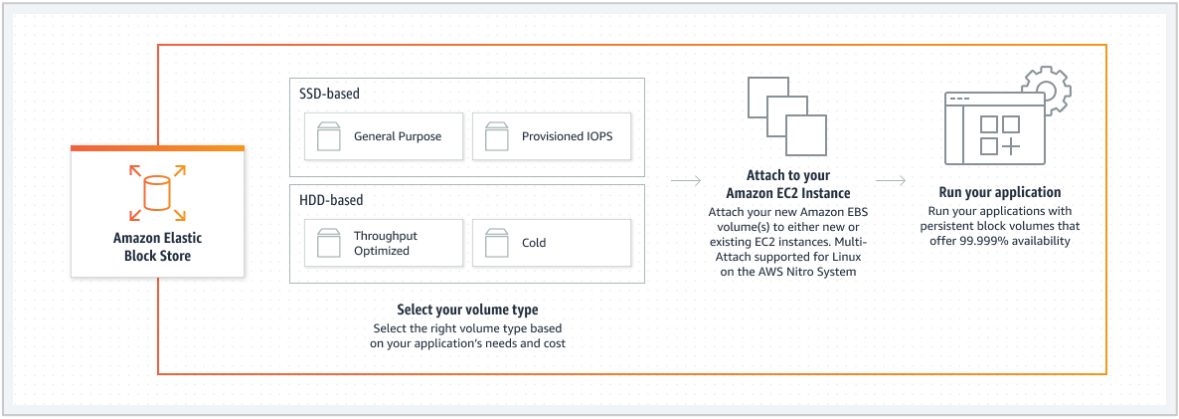

Ilustración 7. Funcionamiento Amazon Elastic Block Store

Algunos casos de uso son:

- Creación de **SAN** en la nube para aplicaciones de uso intensivo de **E/S**
- Ejecución de bases de datos relacionales o **NoSQL**
- Ajuste del tamaño de motores de análisis de "**Big Data"**

4.3.2.1.5 Amazon Cognito

"Amazon Cognito" [35] ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web. Los dos componentes principales de "**Amazon Cognito"**, que se pueden implementar de forma conjunta o separada, son:

- Los grupos de usuario: Son directorios de usuarios que proporcionan a los usuarios de las aplicaciones opciones para la inscripción e inicio de sesión.
- Los grupos de identidades: Permite conceder a los usuarios acceso a otros servicios de **AWS**

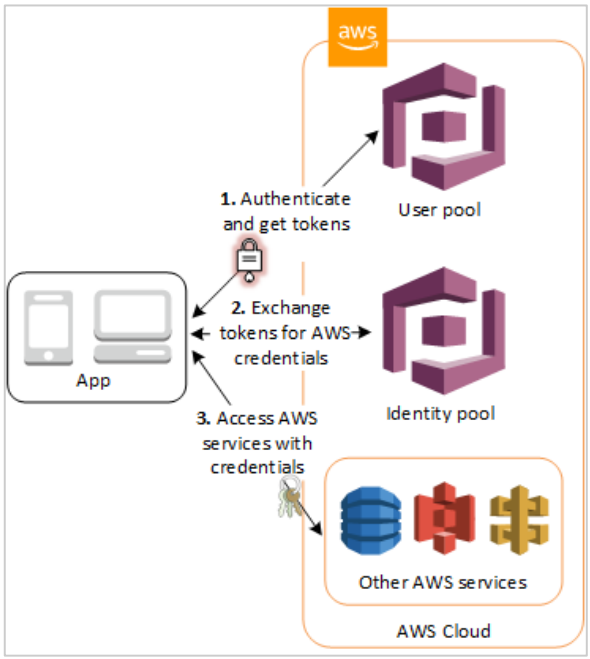

Ilustración 8. Funcionamiento Amazon Cognito

Las funcionalidades principales que ofrece "**Amazon Cognito"** son:

- Almacén de identidades – Los grupos de usuario de "**Amazon Cognito"** proporcionan un almacén de identidades y permiten una configuración más accesible

- Identidades federadas sociales y empresariales – Permite el inicio de sesión mediante proveedores de identidades sociales como "**Google2**, "**Facebook"** y "**Amazon"**

- Autenticación basada en estándares – Los grupos de usuarios se tratan de un proveedor de identidades basados en estándares y, por tanto, admiten administración de accesos e identidades, como: "**OAuth 2.0"**, "**SAML 2.0"** y "**OpenID Connect"**

- Seguridad para las aplicaciones y usuarios – Admite el sistema de seguridad **MFA** y el cifrado de datos. "**Amazon Cognito"** reúne condiciones establecidas por **HIPAA** y cumple con los requisitos de diversas normas de seguridad.

- Control de acceso a los recursos **AWS** – Ofrece soluciones para controlar el acceso a recursos **AWS** desde una aplicación. Puede definir los roles y asignar usuarios a diferentes roles para que una aplicación únicamente pueda acceder a los recursos autorizados para cada usuario.

4.3.2.1.6 AWS Lambda

"AWS Lambda" [36] es un servicio informático sin servidor y basado en eventos. Permite ejecutar código para una alta variedad de aplicaciones o servicio "***backend"*** sin necesidad de aprovisionar o administrar los servidores. En otras palabras, permite la escritura y ejecución de código sobre la infraestructura de **AWS**. Algunos ejemplos de implementación de "**AWS Lambda"** son:

- Procesamiento de archivos: Con la colaboración de S3 para desencadenar el procesamiento de datos de "**AWS Lambda"** en tiempo real después de una carga o, en otro caso, conectarse a un sistema de archivos de "**Amazon EFS"** existente para habilitar el acceso compartido

- Procesamiento de transmisiones: Se implementa "**AWS Lambda"** y "**Amazon Kinesis"** para procesar datos en ***"streaming"*** en tiempo real para el seguimiento de actividad de aplicaciones, procesamiento de pedidos de transacciones, análisis de lujo de "***clicks"*** y entre muchas otras funcionalidades.

- Aplicaciones web: Combinar "**AWS Lambda"** con otros servicios de **AWS** para crear aplicaciones web

- ***"Backends"*** para **IoT**: Creación de "***backends"*** sin servidor con "**AWS Lambda"** para administrar solicitudes web, móviles del **IoT** y de **API**s de terceros

- ***"Backends"*** móviles: Creación de ***backends*** con "**AWS Lambda"** y **"Amazon API Gateway"** para autenticar y procesar solicitudes de API.

4.3.2.1.7 Amazon CloudFront

"Amazon CloudFront" [37] es un servicio de red de entrega de contenido (**CDN**) creado para ofrecer alto rendimiento, seguridad y comodidad para los desarrolladores que implementan **AWS**. Su objetivo principal es entregar contenidos de forma segura con baja latencia y alta velocidad de transferencia.

"CloudFront" se centra en reducir la latencia mediante la entrega de datos a través de más de 310 puntos de presencia (***PoP***) repartidos por sus interconexiones de "**Amazon"** con mapeo de red automatizado y enrutamiento inteligente. Se implementa además para mejorar la seguridad a través del cifrado de tráfico y controles de acceso, junto con la herramienta "**AWS Shield Standard"** para defenderse contra los ataques de ***DDoS***.

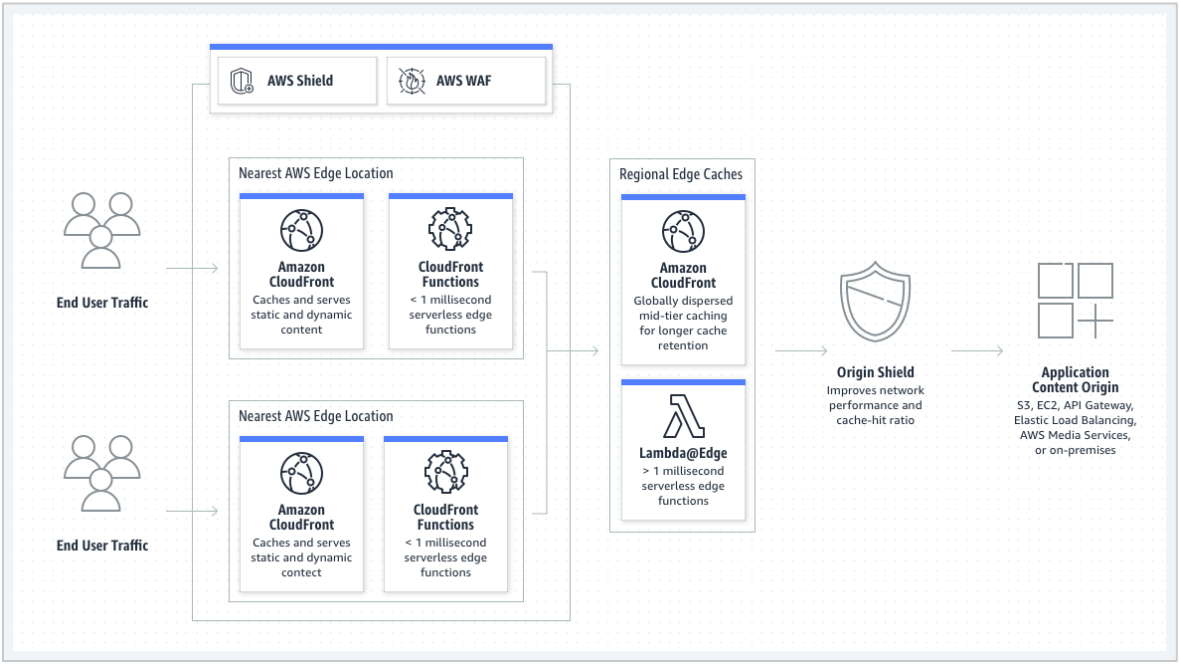

Ilustración 9. Funcionamiento Amazon CloudFront

Los casos de uso más vistos de "**CloudFront"** son:

- Entrega de sitios web rápidos y seguros
- Aceleración de la entrega de contenidos dinámicos y **APIs**
- Transmisión de vídeo en directo y en diferido
- Distribución de parches y actualizaciones

4.3.2.1.8 DynamoDB

"Amazon DynamoDB" [38] es una base de datos de documentos y valores clave que ofrece un rendimiento de milisegundos de un solo dígito a cualquier escala. Es una base de datos duradera, multiactiva, multirregión y completamente administrada con seguridad integrada, copia de seguridad y restauración, y almacenamiento en caché en memoria para aplicaciones a escala de Internet. "**DynamoDB"** puede manejar más de 10 billones de solicitudes por día y puede admitir picos de más de 20 millones de solicitudes por segundo.

4.3.2.1.9 SSM Agent

El agente de "**AWS Systems Manager (SSM Agent)"** [39] es un software de "**Amazon"** que se ejecuta en diversas instancias, como "**Amazon Elastic Compute Cloud (Amazon EC2)",** máquinas virtuales o servidores locales, para permitir que "**Systems Manager"** actualice, administre y configure estos recursos. El agente procesa las solicitudes desde el

servicio de "**Service Manager"** en la nube de **AWS** y, entonces, las ejecutar tal y como se especifica en la solicitud. A continuación, "**SSM Agent"** devuelve información de estado y de ejecución al servicio de "**Systems Manager"** mediante el "**Amazon Message Delivery Service"** (prefijo de servicio: "***ec2messages"***).

4.3.2.1.10 Patrones AWS

A continuación se muestra en la siguiente tabla los patrones de direcciones URL que sigue **AWS** al implementar un tipo de servicio específico:

Servicio	**URL**
s3	https://{user_provided}.s3.**Amazon**AWS.com
cloudfront	https://{random_id}.cloudfront.net
ec2	ec2-{ip-seperated}.compute-1.**Amazon**AWS.com
es	https://{user_provided}-{random_id}.{region}.es.**Amazon**AWS.com
elb	http://{user_provided}-{random_id}.{region}.elb.**Amazon**AWS.com:80/443
elbv2	https://{user_provided}-{random_id}.{region}.elb.**Amazon**AWS.com
rds	mySQL://{user_provided}.{random_id}.{region}.rds.**Amazon**AWS.com:3306
rds	postgres://{user_provided}.{random_id}.{region}.rds.**Amazon**AWS.com:5432
route 53	{user_provided}
execute-api	https://{random_id}.execute-api.{region}.**Amazon**AWS.com/{user_provided}
cloudsearch	https://doc-{user_provided}-{random_id}.{region}.cloudsearch.**Amazon**AWS.com
transfer	sftp://s-{random_id}.server.transfer.{region}.**Amazon**AWS.com
iot	mqtt://{random_id}.iot.{region}.**Amazon**AWS.com:8883
iot	https://{random_id}.iot.{region}.**Amazon**AWS.com:8443
iot	https://{random_id}.iot.{region}.**Amazon**AWS.com:443

mq	https://b-{random_id}-{1,2}.mq.{region}.**Amazon**AWS.com:8162
mq	ssl://b-{random_id}-{1,2}.mq.{region}.**Amazon**AWS.com:61617
kafka	b-{1,2,3,4}.{user_provided}.{random_id}.c{1,2}.kafka.{region}.**Amazon**AWS.com
kafka	{user_provided}.{random_id}.c{1,2}.kafka.useast-1.**Amazon**AWS.com
cloud9	https://{random_id}.vfs.cloud9.{region}.**Amazon**AWS.com
mediastore	https://{random_id}.data.mediastore.{region}.**Amazon**AWS.com
kinesisvideo	https://{random_id}.kinesisvideo.{region}.**Amazon**AWS.com
mediaconvert	https://{random_id}.mediaconvert.{region}.**Amazon**AWS.com
mediapackage	https://{random_id}.mediapackage.{region}.**Amazon**AWS.com/in/v1/{random_id}/channel

Tabla 9. Direcciones de URL comunes en AWS

4.3.2.2 Fases

4.3.2.2.1 Reconocimiento y Descubrimiento

En esta fase de reconocimiento, las principales recomendaciones a realizar para obtener la máxima información posible sobre la organización **AWS** son:

- Comprobar las aplicaciones web ya que algunas pueden obtener contenido directamente de ***"bucket* S3"**. También se recomienda localizar donde se cargan los recursos para determinar si se está implementando ***"buckets* S3**"

- Implementar herramientas para la intercepción de tráfico para analizar el intercambio de peticiones, como "**Burp Suite"**. Este análisis de tráfico puede ayudar además identificar si existen llamadas a servicios específicos de **AWS**.

Subdominos

Se pueden utilizar herramientas automatizadas para realizar la búsqueda de todos los subdominios que utiliza una organización. Algunas de ellas son:

- **"Assetfinder"**

- A través de fuerza bruta con "**DNSRecon"**
- Búsquedas invernas de **DNS**
- Búsquedas de **AWS *"buckets"*** con **Slurp** o **Ruby**
- **"Smogcloud"** para la búsqueda de recursos **IAM**
- **"Dufflebag"** para encontrar datos secretos en **EBS** públicos
- Implementar **"bucketFinder** para buscar todos los "**Bucktes AWS"** públicos, además de realizar un listado de ellos y descargar todos los archivos en caso de que el indexado se encuentre habilitado
- **"Cloudmapper"** ayuda a analizar los entornos de **AWS**
- **"weirdAAL"** es una librería de ataque **AWS**

4.3.2.2.2 Acceso Inicial

S3 bucket Pillaging

Este ataque consiste en localizar los depósitos de "**Amazon S3"** para, entonces, buscar y obtener datos de interés. Generalmente, el proceso de este ataque consiste en realizar la identificación de "**S3 *buckets"*** accesibles y públicos de una organización y, tras esta identificación, se procede a realizar la enumeración de su contenido, además de la descarga de los archivos alojados.

Inyección de código S3

Muchas aplicaciones web de **AWS**, al cargar contenido de un **S3**, puede ser vulnerable a ataques de "***Cross-Site Scripting"*** y generar puertas traseras por "**Javascript**.

Secuestro de domino S3

En el caso de que una aplicación web esté utilizando un domino **S3** que ha dejado de existir, es posible suplantar dicho dominio por uno propio al introducir el mismo nombre y región. De esta manera, se puede generar un "**S3 *bucket"*** con contenido malicio al que las aplicaciones web realizarán llamadas para solicitar dicho contenido.

Metadata Server-Side Request Forgery (SSRF)

Un ataque de falsificación de solicitud del lado del servidor (**SSRF**) involucra el abuso de la funcionalidad del servidor para acceder o modificar sus recursos. El atacante se dirige a una aplicación o, que admite la importación o lectura de datos desde una dirección **URL**. En

otras palabras, se trata de una vulnerabilidad de seguridad web que permite a un atacante inducir a la aplicación del lado del servidor a realizar solicitudes a una ubicación no deseada. En un ataque **SSRF** típico, el atacante puede hacer que el servidor establezca una conexión con servicios únicamente internos dentro de la infraestructura de la organización. En otros casos, pueden obligar al servidor a conectarse a sistemas externos arbitrarios, lo que podría filtrar datos confidenciales como, por ejemplo, credenciales de autorización.

Se puede explotar esta vulnerabilidad a través de **EC2** para obtener información de metadatos, ya sea de nombres de dominios a credenciales de usuarios. Este proceso se realiza, una vez se ha accedido a la sección de metadatos de **IAM**, realizando una búsqueda de los roles asignados a la instancia y, con el nombre encontrado, extraer las claves temporales de dicho rol.

Otro punto donde se puede realizar este ejercicio de **SSRF** es a través del "**Container Service**" de **Amazon**, denominado "**Fargate"**. Si se consigue obtener la variable "***AWS_CONTAINER_CREDENTIALS_RELATIVE_URI***" del servicio, se puede realizar un proceso de autenticación a través de los parámetros "**AccessKey"** y "**SecretKey"** de la dirección de autenticación de la aplicación.

Algunas otras llamadas a **AWS APIs** que devuelven credenciales son:

- ***chime:createapikey***
- ***codepipeline:pollforjobs***
- ***cognito-identity:getopenid"token"***
- ***cognito-identity:getopenid"token"fordeveloperidentity***
- ***cognito-identity:getcredentialsforidentity***
- ***connect:getfederation"token"***
- ***connect:getfederation"tokens"***
- ***ecr:getauthorization"token"***
- ***gamelift:requestuploadcredentials***
- ***IAM:createaccesskey***
- ***IAM:createloginprofile***
- ***IAM:createservicespecificcredential***

- ***IAM:resetservicespecificcredential***
- ***IAM:updateaccesskey***
- ***lightsail:getinstanceaccessdetails***
- ***lightsail:getrelationaldatabasemasteruserpassword***
- ***rds-db:connect***
- ***redshift:getclustercredentials***
- ***sso:getrolecredentials***
- ***mediapackage:rotatechannelcredentials***
- ***mediapackage:rotateingestendpointcredentials***
- ***sts:assumerole***
- ***sts:assumerolewithsaml***
- ***sts:assumerolewithwebidentity***
- ***sts:getfederationtoken***
- ***sts:getsessiontoken***

Explotación de vulnerabilidades de configuración

Se recomienda utilizar la implementación de herramientas automatizadas para realizar la búsqueda de posibles vulnerabilidades de configuración implementadas en la nube **AWS**, como, por ejemplo, servicios desactualizados. Una de las herramientas recomendadas para este apartado es "**PACU",** que realiza la explotación de fallos de configuración dentro del entorno **AWS**.

4.3.2.2.3 Enumeración

Enumeración de usuarios con privilegios

Si se ha podido comprometer un usuario con permisos de solo lectura en unos servicios **IAM**, es posible implementar la herramienta "**SkyArk"** para realizar una enumeración de los

usuarios con mayores privilegios en el entorno **AWS** escaneado, incluyendo los **AWS** "**Shadow Admins"**.

Enumeración de permisos IAM

Existe una herramienta denominada "**enumerate-IAM**" que permite enumerar los permisos asociados con el conjunto de credenciales **AWS**

EC2 Shadow Copy Attack

Implementando la herramienta "**CloudCopy**", implementando credenciales previamente obtenidas con permisos mínimos de "***EC2:CreatSnapshot***", es posible robar información y, además, generar una nueva "**Linux EC2"** con una "***snapshot"*** almacenada en **AWS**.

4.3.2.2.4 Escalada de privilegios

Golden SAML Attack

Usando información previamente extraída, es posible generar un ***"token* SAML"** falsificado como un usuario arbitrario para realizar la autenticación en "**Office 365**", sin conocer la contraseña de dicho usuario. Este ataque también pasa por alto cualquier requisito de **MFA**.

Los requisitos para realizar este ataque son:

- Clave privada de firma de ***"tokens"***
- Certificado público **IdP**
- Nombre **IdP**
- Nombre del rol a asumir

Acceso a tablas DynamoDB

Al obtener acceso a las tablas "**DynamoDB"**, es posible listar su contenido y obtener las credenciales de los usuarios que tenga almacenados. Algunas acciones que se pueden realizar son:

- Listar tablas
- Enumerar contenido de una tabla

Shadow Admin

AWS trabaja con unos ciertos permisos con los que, en ciertas circunstancias, es posible realizar acciones con permisos equivalentes a un rol de administrador. Algunas de ellas son:

- ***"AdministratorAccess"***

- ***"ec2:AssociateIAMInstanceProfile"***

- ***"IAM:CreateAccessKeyIAM:CreateAccessKey"*** – Esto permite crear una nueva clave de acceso a otra cuenta de administrador **IAM**

- ***"IAM:CreateLoginProfile"*** – Añade una nuevo perfil de acceso basado en contraseña, lo que permite crear una nueva contraseña para una identidad y hacerse para por ella

- ***"IAM:UpdateLoginProfile"*** – Permite resetear contraseñas de acceso de usuarios **IAM**

- ***"IAM:AttachUserPolicy", "IAM:AttachGroupPolicy"*** o ***"IAM:AttachRolePolicy"*** – Permite adjuntar políticas de administrador existentes a cualquier otra entidad que posea el usuario

- ***"IAM:PutUserPolicy, IAM:PutGroupPolicy o IAM:PutRolePolicy"*** – Las políticas añadida des en línea permite otorgar privilegios adicionales a entidades previamente comprometidas

- ***"IAM:CreatePolicy"*** – Permite añadir una política de administrador oculta

- ***"IAM:AddUserToGroup"*** – Permite añadir un usuario al grupo de administradores de la organización.

- ***"IAM:UpdateAssumeRolePolicy + sts:AssumeRole"*** – Permite cambiar los permisos asumidos por un rol privilegiado y luego asumirlo como una cuenta sin privilegios

- ***"IAM:CreatePolicyVersion & IAM:SetDefaultPolicyVersion"*** - Permite cambiar las políticas gestionadas por usuarios y, además cambiar entidades no privilegiadas a unas privilegiadas..

- ***"lambda:UpdateFunctionCode"*** – Permite dar acceso a privilegios asociados con roles de servicio Lambda que se encuentren adjuntos a esa función

- ***"glue:UpdateDevEndpoint"*** – Permite dar acceso a privilegios asociados con los roles adjuntos a puntos finales de específicos entornos "**Glue"**

- ***"IAM:PassRole + ec2:CreateInstanceProfile/ec2:AddRoleToInstanceProfile"*** – Permite crear un nuevo perfil de instancia y adjuntarlo a una instancia EC2 comprometida que ya posea.

- ***"IAM:PassRole + ec2:RunInstance"*** – Da acceso a un conjunto de permisos que tiene un perfil o rol, que a su vez puede escalar de un perfil sin privilegios a uno con acceso de administrador a una cuenta **AWS**

- ***"IAM:PassRole + lambda:CreateFunction + lambda:InvokeFunction"*** – Da a un usuario acceso a privilegios asociados a cualquier rol de un servicio "**Lambda"** que exista en la cuenta

- **"*IAM:PassRole + glue:CreateDevEndpont"*** – Permite dar privilegios asociados a cualquier rol de servicio "**Glue"** que exista en la cuenta

4.3.2.2.5 Movimiento Lateral

Ejecución de comandos con SSM

El "**SSM Agent"** se encuentra preinstalado, por defecto, en las siguientes "**Amazon Machine Images" (AMIs):**

- **"Windows Server 2008-2012 R2 AMI**s" publicado en noviembre de 2016 o posterior

- **"Widows Server"** 2016 and 2019

- **"Amazon Linux"**

- **"Amazon Linux 2"**

- **"Ubuntu Server 16.04"**

- **"Ubuntu Server 18.04"**

- **"Amazon ECS-Optimized"**

Cuando se desinstala el SSM **agente**, la cuenta de usuario **SSM** (***ssm-user***) no se elimina del sistema.

Obtener acceso a consola AWS a través de claves API

"AWS Consoler" [40] se trata de una herramienta que permite convertir credenciales **AWS CLI** en acceso a consolas de **AWS**.

Algunas características de "**AWS Consoler"** son:

- Carga de credenciales desde la línea de comandos o desde fuentes Boto3 ("**envvars**, perfiles, "**IMDS"**)
- Coordinación de la comunicación con "**AWS Federation"**
- Selección del punto final apropiado según la partición
- Carga de la URL resultante en el navegador implementado por el usuario

4.3.2.2.6 Persistencia

Deshabilitar CloudTrail

Este proceso permite deshabilitar eventos de monitorización de servicios globales. También se puede aplicar esta función a regiones específicas.

Cubrir el rastro al ofuscar logs de Cloudtrail y Guard Duty

Mediante la herramienta "**PACU"**, se puede "***bypassear***" este problema al definir un "**User-Agent"** customizado. Se debe tener en cuenta que al utiliza "**AWS CLI"** en **"Kali Linux"**, "**Pentoo"** o "**Parrot Linux"**, se genera un registro basado en el usuario agente.

4.3.2.3 Herramientas

4.3.2.3.1 Enumerate IAM

"Enumerate IAM" [41] se trata de un código de "**Python**" que intenta aplicar fuerza bruta a todas las llamadas API permitidas por la política de **IAM** para enumerar todos los permisos accesibles.

4.3.2.3.2 CloudCopy

"ClodCopy" [42] es una herramienta que implementa una versión de nube del ataque "**Shadow Copy"** contra los controladores de dominios que se ejecutan en **AWS**. Cualquier usuario de **AWS** que posea el permiso "***EC2:CreateSnapshot***" puede robar los "***hash***" de todos los usuarios del dominio al crear una ***"snapshot***" del "**Domain Controller".** Entonces, puede montarla en una instancia que puede ser controlada y, además. exportar el archivo de subárbol de registro de "**NTDS.dit"** y "**SYSTEM"** a usar con el proyecto "**secretsdump"** de "**Impacket"**.

4.3.2.3.3 SkyArk

"SkyArk" [43] es una herramienta que tiene, como objetivo principal, descubrir los usuarios más privilegiados en el entorno **AWS** escaneado, incluyendo los "**AWS Shadow Admins"**. Se trata de un proyecto de nube que tiene dos módulos principales de escaneo:

- **"AzureStealth"**, se encarga de escanear los entornos **"Azure"**
- **"AWStealth"**, se encarga escanear los entornos **AWS**

4.3.2.3.4 Pacu

La herramienta "**Pacu"** [44] se centra en explotar vulnerabilidades de configuración en el entorno **AWS** a través de este conjunto de módulos. Se trata de un "***framework"*** de explotación de código fuente abierto, diseñado para el testeo de seguridad ofensiva en entornos de nube. Creado y gestionado por "**Rhino Security Labs"**, "**Pacu"** permite a analistas de seguridad a explotar fallos de configuración dentro de una cuenta **AWS**, utilizando módulos que le permite expandir fácilmente su funcionalidad.

Algunos ataques que permiten estos módulos:

- Escalado de privilegios
- Puertas traseras de usuarios **IAM**
- Ataque contra funciones Lambda vulnerables

4.3.2.3.5 BucketFinder

"BucketFinder" [45] realiza la búsqueda de ***"buckets"*** públicos, los enumera y, además realiza la descarga de todos los archivos si el directorio tiene el indexado habilitado. Al implementar una lista de posibles nombres, esta herramienta simplemente verifica si existe un ***"bucket"*** que coincida con algunos de los nombres, además de descubrir si se trata de un ***"bucket"*** público, privado o redireccionado.

4.3.2.3.6 Principal Mapper

"Principal Mapper" [46] es herramienta utilizada para evaluar los permisos de **IAM** en **AWS**. se trata de una librería y código centrada en identificar riesgos en la configuración de **IAM** para cuentas de **AWS** o de la propia organización. Modela los diferentes usuarios y roles de **IAM** directamente como un grafo por el cual realiza la prueba de escalaba de privilegios o caminos alternativos a tomar para obtener acceso a un recurso o acción en **AWS**.

Incluye mecanismos de consulta que utilizan una simulación local del comportamiento de autorización de **AWS**. A la hora de utilizar una consulta para determinar si un principal tiene acceso a una cierta acción o recurso, "**Principal Mapper"** también comprueba si el usuario o el role podría acceder a otros usuarios o roles que tengan acceso a esa acción o recurso.

4.3.2.3.7 Cloudsplaining

"Cloudsplaining" [47] se trata de una herramienta de "**AWS IAM Security Assessment"** que identifica las violaciones de menor privilegio y, con ello, genera un informe de riesgo priorizado. Puede escanear todas las políticas de una cuenta **AWS** o, en caso contrario, simplemente escanear un único archivo de políticas.

Ayuda a identificar acciones **IAM** que no implementan limitaciones a recursos. También ayuda a priorizar el proceso de remediación al marcar las políticas **IAM** que presentan algunos de los siguientes riesgos a la cuenta **AWS**:

- Exfiltración de datos
- Modificación de infraestructura
- Exposición de recursos
- Escalado de privilegios

"Cloudsplaining" también identifica las funciones de **IAM** que puedan ser asumidos por "**AWS Compute Services"** (como **EC2**, **ECS**, **EKS** o **Lambda**), ya que pueden presentar un mayor riesgo que las funciones definidas por el usuario, especialmente si el "**AWS Compute Services"** está en una instancia que se encuentre directa o indirectamente expuesta a Internet. Marcar estos roles es particularmente útil para los evaluadores de penetración (o atacantes) en ciertos escenarios. Por ejemplo, si un atacante obtiene privilegios para ejecutar "***ssm:SendCommand***" y hay instancias **EC2** privilegiadas con el agente **SSM** instalado, este usuario puede obtener los privilegios de esas instancias **EC2**. La ejecución remota de código a través del agente de "**AWS Systems Manager"** ya era una previamente ruta conocida para el escalado o explotación, pero "**Cloudsplaining"** puede facilitar este proceso de identificación.

También puede especificar un archivo de exclusiones personalizado para filtrar los resultados que hayan resultado ser falsos positivos. Por ejemplo, las políticas de usuario son permisivas por diseño, mientras que los roles del sistema generalmente son más restrictivos. También se puede implementar exclusiones que sean específicas para la estrategia de varias cuentas de una organización o de la arquitectura de aplicaciones de **AWS**.

4.3.2.3.8 weirdAAL

"WeirdAAL" [48] se trata de una librería centrada para realizar ataques **AWS**. Implementa una gran variedad de módulos, todos ellos centrados en los diferentes servicios que puede ofrecer **AWS**.

4.3.2.3.9 CloudMapper

"CloudMapper" [49] es una herramienta que permite realizar un análisis de los entornos **AWS**. Previamente, su objetivo principal era generar y visualizar diagramas de red. Actualmente, incluye una mayor variedad de funcionalidades, entre ellas la realización de auditorías de problemas de seguridad.

4.3.2.3.10 Dufflebag

"Dufflebag" [50] es una herramienta que realiza una búsqueda de "***snapshots"*** públicos de "**Elastic Block Storage**" (**EBS**) de **AWS** que puedan contener posibles secretos, como por ejemplo credenciales, que hayan sido accidentalmente expuestos.

4.3.3 MICROSOFT AZURE CLOUD

4.3.3.1 Componentes

4.3.3.1.1 Azure Active Directory

"Azure Active Directory" (**"Azure AD"** o **AAD**) [51] es un servicio de "**Microsoft**" basado en Cloud para la gestión de acceso e identidades. Propone una solución de Identidad como Servicio (***IDaaS***) que cubre todos los aspectos de seguridad y gestión de identidades y accesos. **"Azure AD"** se puede utilizar para acceder tanto a los recursos externos (como **"Azure Portal"** o "**Office 365"** entre otros) como a los recursos internos de la organización (como, por ejemplo, las aplicaciones "***on-premises"***).

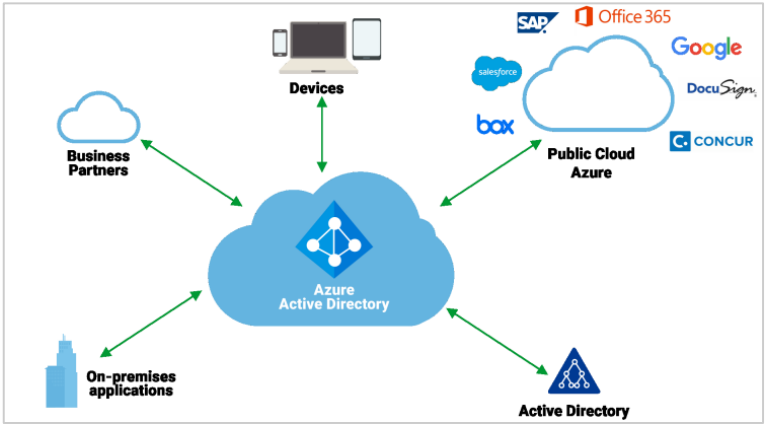

Ilustración 10. Estructura "Azure Active Directory"

Algunos de los servicios que ofrece **"Azure AD"** se muestran representados en la siguiente imagen:

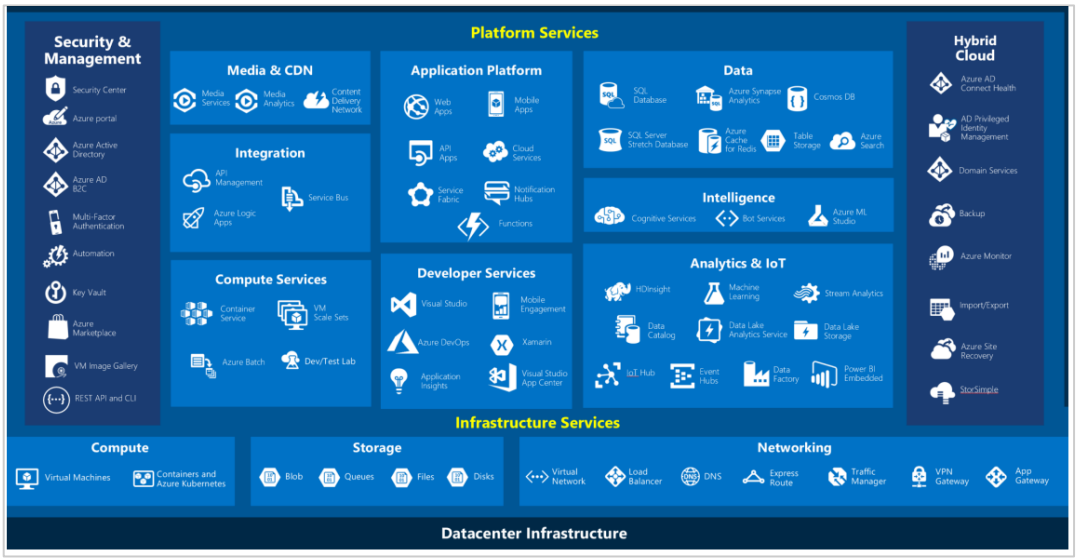

Ilustración 11. Servicios de "Azure Active Directory"

4.3.3.1.2 Azure Resource Manager (ARM)

"Azure Resource Manager (ARM)" [52] es el servicio de implementación y administración que se utiliza para el ciclo de gestión (crear, actualizar y eliminar) y el control de acceso de todos los recursos implementados por la organización. Proporciona una capa de administración que permite crear, actualizar y eliminar recursos de la cuenta de **"Azure"**. Las plantillas de **ARM** se utilizan para el redespliegue coherente y definida de recursos.

Para proteger y organizar los recursos tras la implementación, se utilizan las características de administración como, por ejemplo, el control de acceso, la auditoría y las etiquetas

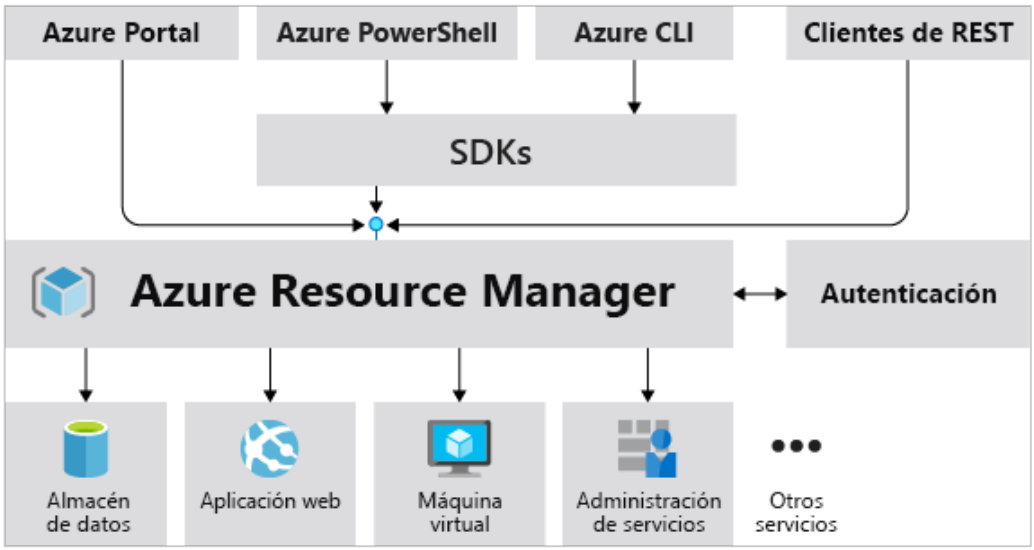

Ilustración 12. Azure Resource Manager (ARM)

4.3.3.1.3 Azure Portal

"Azure Portal" [53] proporciona a organizaciones un panel para compilar, administrar y supervisar todas las aplicaciones implementadas en **"Azure"**. A través de **"Azure Portal"**, es posible administrar una suscripción de **"Azure"** mediante la interfaz gráfica de usuario. Es capaz de compilar, administrar y supervisar desde aplicaciones web hasta implementaciones más complejas en la nube.

Dado que se trata de una consola unificada en web, el acceso a esta aplicación puede no suponer solo un descubrimiento completo de las aplicaciones, configuraciones y suscripciones implementadas dentro de la organización mediante **"Azure"**, sino que además permite realizar cambios de configuración que puede terminar en accesos no autorizados a usuarios malintencionados.

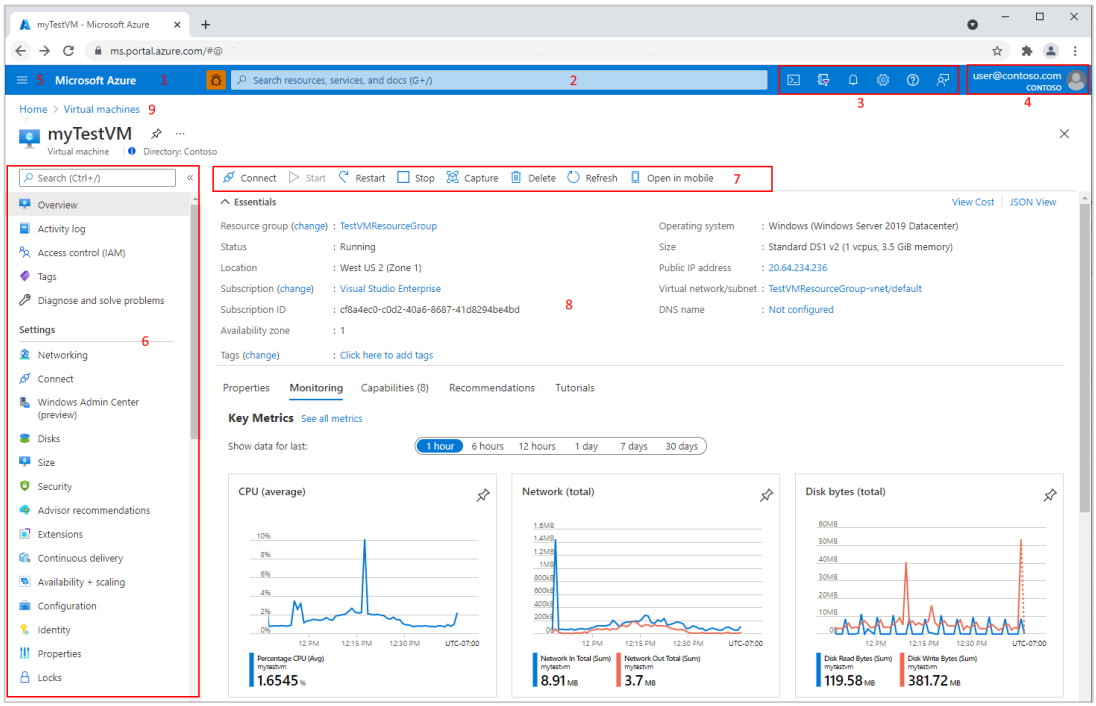

Ilustración 13. Vista de "Azure" Portal

Alguna de las enumeraciones que pueden realizar a través de **"Azure Portal"** son:

- Usuarios registrados en un ***"Tenant"***
- Grupos
- Dispositivos
- Roles de directorio

- Aplicaciones empresariales

4.3.3.1.4 Microsoft Graph

"Microsoft Graph" [54] es la puerta de enlace de datos y la inteligencia de "**Microsoft 365**". Proporciona un modelo de programación unificado que puede ser utilizado para acceder a los datos de "**Microsoft 365"**, "**Windows"** y "**Enterprise Mobility + Security"**.

Los tres componentes principales en los que se basa **Microsoft Graph** son:

- La **API** de "**Microsoft Graph"** para ofrecer un único punto de conexión para proporcionar acceso en la nube de Microsoft a datos y perspectivas centradas en las personas.

- Los conectores de "**Microsoft Graph"** para la entrega de datos externos a la nube de Microsoft en servicios y aplicaciones de "**Microsoft Graph"**. Proporciona conectores para diversos orígenes de datos, como: "**Box"**, "**Google Drive"**, "**Jira"** y "**Salesforce"**

- Finalmente, "**Microsoft Graph Data Connect"** proporciona un conjunto de herramientas para simplificar la entrega de datos segura y escalable a "**Microsoft Graph"** a almacenamientos de datos populares de **"Azure"**.

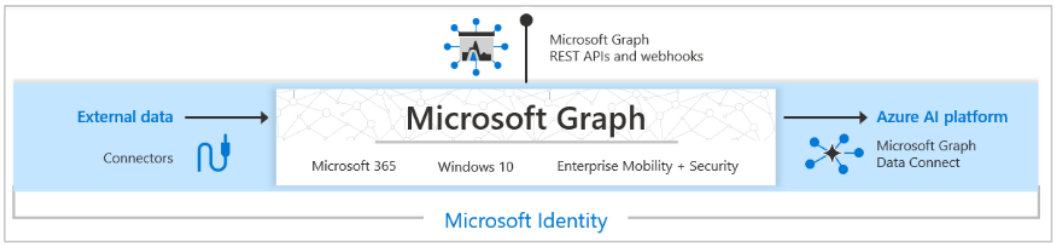

Ilustración 14. Microsoft Graph

4.3.3.1.5 Azure Functions

"Azure Functions" [55] es un servicio en la nube disponible a petición que proporciona la infraestructura y recursos necesarios para la ejecución de las aplicaciones de **"Azure"**. Este modelo permite a los usuarios centrarse en partes de código que le sean de interés y, en paralelo, **"Azure Functions"** se ocupa del resto. Se trata de una solución sin servidor donde la infraestructura de **"Azure"** en la nube permite mantener todos los recursos necesarios actualizados para ejecutar las aplicaciones.

4.3.3.1.6 Azure Blob Storage

"Azure Blob Storage" [56] es la solución de almacenamiento de objetos de "**Microsoft"** para la nube. Este almacenamiento de blobs está optimizado para grandes cantidades de

datos no estructurados, es decir, datos que no se basan en una definición o modelo de datos concretos (Videos, archivos o audio).

Los tres tipos de archivos que se pueden encontrar en **"Blob Storage"** son:

- Cuentas de almacenamiento ("**Storage account"**)
- Contenedores en la cuenta de almacenamiento
- Blob en un contenedor, donde se almacena la información.

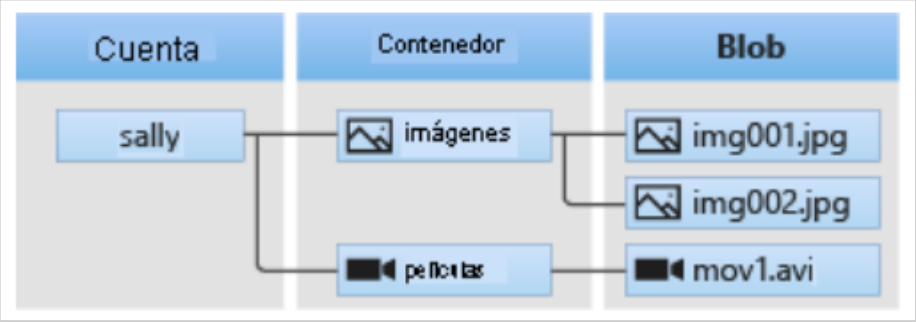

Ilustración 15. Recursos "Blob Storage"

Dado que los usuarios o aplicaciones cliente pueden acceder a los objetos de **"Blob Storage"** a través de **HTTP/HTTPS**, **"Azure"** implementa diferentes maneras para controlar el acceso a las cuentas de almacenamiento:

- Credenciales de **"Azure AD**"
- Clave compartida donde se utilizan claves de acceso para obtener acceso completo a las cuentas de almacenamiento
- Firma de acceso compartida (**SAS – *Shared Access Signature***) – proporciona un acceso limitado tanto tiempo como en permisos.

4.3.3.1.7 Azure Automation – Azure Runbooks

El servicio de automatización de **"Azure"** [57] proporciona la automatización de tareas de recursos de **"Azure"**, ya sea en la premisa o en otros proveedores de nube. El proceso de automatización utiliza **"Runbooks"**, que contiene lógica de automatización y código que se desea ejecutar. **"Azure"** proporciona **"Runbooks"** tantos gráficos como textuales ("**Powershell**", "**Powershell Workflow"** y "**Python"**).

En muchos casos, algunos **"Runbooks"** tienen credenciales que no se encuentran almacenados en los recursos compartidos y pueden resultar de interés para los ejercicios de análisis. Además, las cuentas de automatización pueden resultar de interés especialmente en

la escala de privilegios. Estas cuentas de **"Automation"** permiten aislar los recursos, **"Runbooks"**, activos y configuraciones de **"Automation"** de los recursos de otras cuentas.

4.3.3.1.8 Key Vaults

"Azure Key Vault" [58] es el servicio de **"Azure"** para almacenar secretos como contraseñas, cadenas de conexiones, certificados o, entre muchos otros, claves privadas. Con los permisos y accesos adecuados, los recursos de **"Azure"** que utilicen identidades administradas (**VMs**, Servicios de Aplicaciones, Funciones, Contenedores) pueden acceder a **"Key Vaults"** para obtener secretos.

Los tipos de objeto disponibles a través de **"Key Vaults"** son:

- Claves criptográficas
- Secretos, como contraseñas o cadenas de conexiones
- Certificados
- Claves de cuentas de almacenamientos

El acceso a un "**Key Vault"** se controla a través de dos medios:

- Plano de gestión – donde se maneja las políticas de la **Key Vault** y las políticas de acceso. Solo los roles basados en control de acceso (**RBAC**) pueden trabajar en este plano
- Plano de datos – para gestionar datos (claves, secretos y certificados) en la **Key Vault**.

Se debe tener en cuenta que el rol de "**Contribuidor**" que tiene permisos para gestionar políticas de acceso puede acceder a los secretos simplemente modificando las políticas de acceso.

4.3.3.1.9 Intune

"Intune" [59] es un servicio de Administración de Dispositivos Móviles (**MDM** – ***Mobile Device Management***) y de Administración de Aplicaciones Móviles (**MAM** – ***Mobile Application Management***). Está diseñada para proteger los datos de la organización a nivel de aplicación, ya sea con aplicaciones diseñadas o proporcionadas por la tienda de Microsoft.

Para que los dispositivos se encuentren completamente gestionados por Intune, deben estar primero registrados en **"Azure"**. Esto permite un:

- Control de acceso utilizando Políticas de Acceso Condicionales

- Control sobre las aplicaciones instaladas, acceder información, implementar agentes de protección contra amenazas, y muchas otras.

4.3.3.1.10 Azure Active Directory Application Proxy

"Azure Active Directory Application Proxy" [60] proporciona acceso remoto y seguro a aplicaciones de web locales. Tras realizar un inicio de sesión en **"Azure"**, los usuarios pueden acceder a aplicaciones locales y en la nube a través de una dirección **URL** externa o mediante un portal de aplicaciones interno. Algunos de los accesos que proporciona "**Application Proxy"** son: "**Sharepoint"**, "**Teams"**, Escritorio remoto y/o aplicaciones de línea de negocio (**LOB**), entre muchos otros.

El servicio "**Application Proxy"** se ejecuta en la nube y, por otro lado, su conector se ejecuta en un servidor local. Estas dos tecnologías realizan un proceso de intercambio de ***"tokens"*** para realizar los inicios de sesión de **"Azure AD"** para obtener el acceso a las aplicaciones solicitadas.

4.3.3.1.11 Azure Hybrid Identity – Azure AD Connect

La autenticación de paso a través (**PTA** – ***Pass Through Authentication***) se implementa en **"Azure"** primordialmente para la sincronización de identidad en la nube, sin utilizar de ninguna forma sincronización de hashes de contraseñas. Es útil a la hora de aplicar políticas de contraseñas en premisa, ya que es allí donde se realiza la validación de la autenticación. Por otro lado, la comunicación con la nube se realiza a través de un agente de autenticación, implementando únicamente comunicaciones salientes del agente de autenticación a **"Azure AD"**.

Como el agente de autenticación se comunica con **"Azure AD"** por parte del DC de premisa, si se consigue comprometer dicho agente, sería posible verificar autenticaciones para cualquier usuario sincronizado, incluso si su contraseña es errónea.

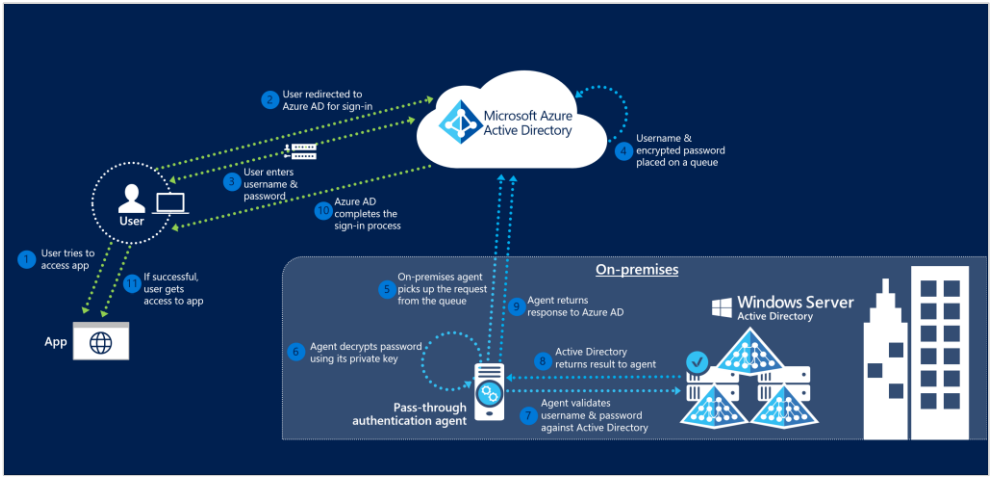

Ilustración 16. PTA con "Azure AD"

4.3.3.1.12 Azure AD Federation

La **"Azure AD Federation"** [61] es un conjunto de dominios con los que se ha establecido una relación de confianza, donde este nivel de confianza puede variar entre ellos, pero generalmente se incluyen la autenticación y, casi siempre, la autorización. Un ejemplo de federación típica podría incluir un número de organizaciones que han establecido confianza para el acceso compartido a un conjunto de recursos.

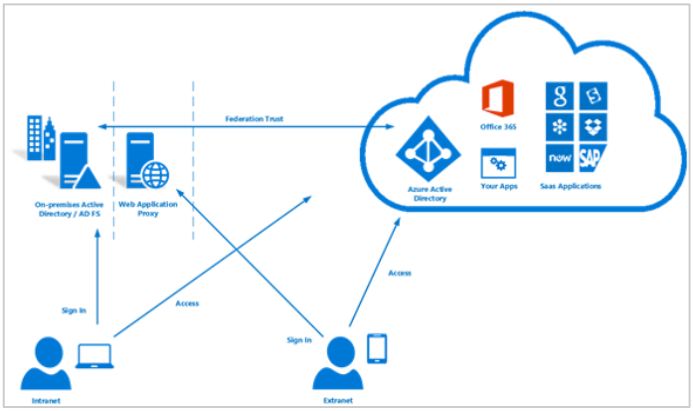

Ilustración 17. Federación "Azure AD"

Se puede federar el entorno local con **"Azure AD"** y, de esta manera, usar esta federación para los procesos de autenticación y autorización. Ese método de inicio de sesión garantiza que toda la autenticación de usuario se realiza de forma local.

En cualquier federación se presentan las siguientes partes:

- Usuario o Cliente
- Proveedor de Identidad (**IdP – *Identity Provider***): autentica al usuario. Se utiliza "***Security Assertion Markup Language***" (**SAML**) para intercambiar información de autenticación y de autorización entre los proveedore.
- Proveedor de Servicio (**SP – *Service Provider***): proporciona el servicio al usuario

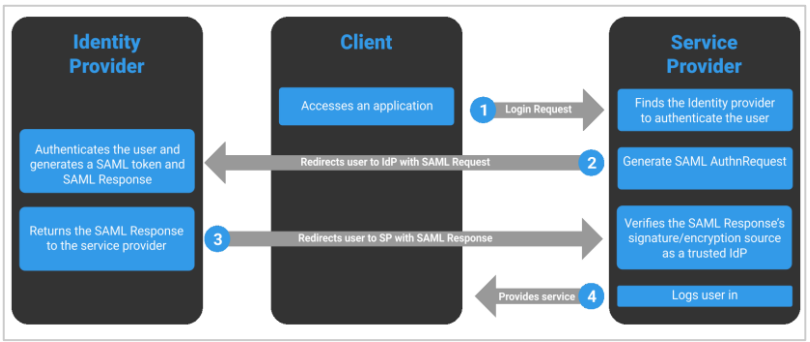

Ilustración 18. Proveedores de la federación

4.3.3.1.13 AdminSDHolder

"AdminSDHolder" [62] es un objeto en "**Active Directory"** que actúa como una plantilla de descriptor de seguridad para cuentas y grupos protegidos en un dominio de "**Active Directory"**. En otras palabras, "**AdminSDHolder"** permite a usuarios gestionar las listas de control de acceso de miembros de grupos **AD** privilegiados e integrados.

4.3.3.2 Fases

4.3.3.2.1 Reconocimiento

Este proceso de reconocimiento y descubrimiento de **"Azure"** se centra principalmente en obtener y extraer información relacionada con la ***"Tenant"*** de la organización a analizar. En este proceso, también se pueden realizar ejercicios para la obtención de las direcciones email de la organización que está implementando **"Azure"**.

Información interesante que se puede descubrir en esta sección:

- Descubrir si una organización utiliza **"Azure *Tenant"***. Se pueden realizar pruebas mediante su ***"Tenant"*** ID o por nombre
- Descubrir el tipo de autenticación que está implementando
- Dominios utilizados por la organización
- Los servicios **"Azure"** utilizados por la organización
- Obtener los **IDs** de correos electrónicos

En este proceso se recomienda utilizar las herramientas:

- **"ADDInternals"** para obtener información según el dominio de la organización
- **"O365creeper"** (o herramientas similares) para comprobar si una dirección de correo electrónico pertenece a un **"Azure *Tenant"***
- **"MicroBurst"**, que utiliza las herramientas "**Az", "AzureAd"**, "**AzurRM"** y "**MSOL"** para enumerar y descubrir los servicios **"Azure"** implementados por la organización

4.3.3.2.2 Acceso inicial

Tras finalizar la sección anterior, en este apartado se pueden realizar una gran variedad ejercicios según la información obtenida en el paso anterior.

Fuerza Bruta o Password-Spray

Utilizar herramientas de fuerza bruta para probar diferentes contraseñas para un mismo usuario; o, el caso contrario, utilizar la misma contraseña para diferentes usuarios implementando ***"password-spraying"***. Se debe tener en cuenta que este apartado puede ser el más ruidoso y llegar a ser detectado por los sistemas de seguridad de la organización.

Alguno de los "**APIs endpoints**" donde se puede aplicar las herramientas de ***"password-spraying"*** son:

- **"Azure AD Graph"**
- **"Microsoft Graph"**
- **"Office 365 Reporting Webservices"**

En la recomendación de herramientas a implementar para ***password-spray*** son:

- **"MSOLSpray"** para las cuentas descubiertas en el proceso de descubrimiento

Credenciales por defecto

Un usuario normal puede tener ciertos niveles permisos que pueden ser interesantes al analizar **"Azure AD"**. Como, por ejemplo:

- Leer todos los usuarios, grupos, aplicaciones, dispositivos, roles, suscripciones y, además, las propiedades públicas
- Invitar a usuarios Invitados
- Crear grupos de seguridad
- Leer miembros de Grupos no-ocultos
- Añadir invitados a grupos pertenecientes
- Crear nuevas aplicaciones
- Añadir hasta 50 dispositivos a **"Azure"**

Al realizar ejercicios de credenciales por defecto, especialmente para usuarios con rol de administrador, puede permitir el acceso al panel de administración de **"Azure"**.

Otorgación de consentimiento ilícito

Algunas aplicaciones pueden solicitar permisos a usuarios para acceder a sus datos como, por ejemplo, un paso de autenticación básica.

Implementando herramientas para el abuso de consentimiento ilícito (como por ejemplo "**365-stealer**"), se puede obtener ***"token"*** de acceso de los usuarios que se hayan autenticado en el link malicioso enviado. Este proceso se puede realizar mediante **"*phishing*"** o, también, se pueden utilizar herramientas como **Microburst** para encontrar las aplicaciones disponibles en **"Azure"**.

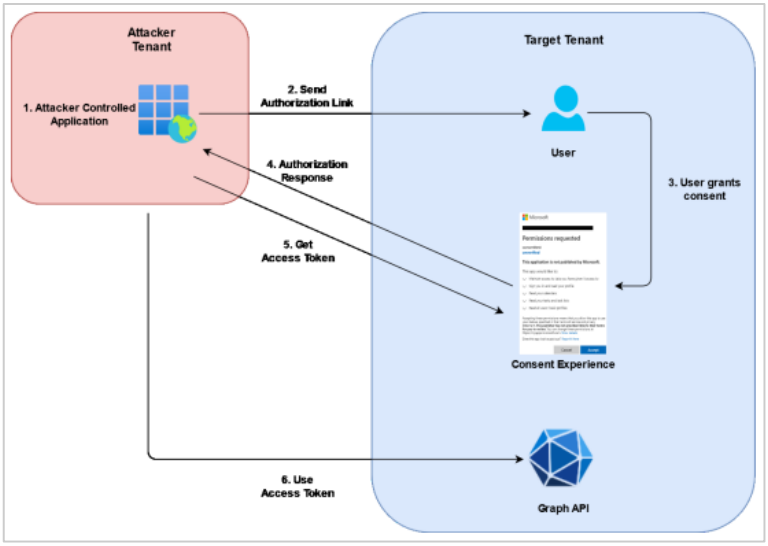

Ilustración 19. Diagrama de Otorgación de consentimiento ilícito

Explotación de Servicios de Aplicación

En caso de que alguna de las aplicaciones proporcionadas a través de la nube **"Azure"** no se encuentren bien diseñadas, se puede realizar una explotación de código para encontrar vulnerabilidades y obtener acceso a distintos recursos que se encuentran en la nube.

Algunas de las vulnerabilidades que se pueden explotar en aplicaciones de **"Azure"** son:

- Subida de archivos inseguros – Para obtener ejecución remota de comandos o robar ***"tokens"*** de acceso
- Inyección de plantillas en el lado servidor (**SSTI** – ***Server Side Template Injection***) – Abusar sintaxis de plantillas para inyectar datos en las plantillas utilizadas por el servidor.
- Inyección de comandos **OS**

Phising

Se recomienda también utilizar herramientas de ***"phishing"*** (como, por ejemplo, "**Evilginx2"**) para realizar el envío de links maliciosos por los cuales se pueden obtener nombres de usuario, credenciales o, además, el robo de cookies de sesión y autenticación.

4.3.3.2.3 Enumeración

En este proceso se puede implementar diversas herramientas relacionadas con **"Azure"** que permiten realizar una enumeración tanto de los usuarios registrados, como de las aplicaciones, roles, grupos y dispositivos conectados en la nube.

Algunas de las herramientas recomendadas son:

- **"Azure AD Powershell module"**
- **"Az Powershell Module"**
- **"Az CLI"**
- **"RoadTOOLS"**
- **StormSpotter**
- **"BloodHound"**

4.3.3.2.4 Escalada de privilegios

Una vez obtenido acceso como un usuario en la nube de **"Azure"**, en este apartado se estudian diversos métodos para realizar una escala de privilegios.

Cuentas de automatización – "Azure" "Automation"

Uno de los puntos de interés a analizar para la escala de privilegios es estudiar los **"Runbook"** de automatización utilizados por **"Azure AD"**. Las cuentas de automatización pueden dar puntos de entrada en diferentes aspectos como:

- ***"Run as Account"*** es el contribuidor por defecto en muchas suscripciones y es probable que tenga permisos de contribuidor en otras suscripciones del ***"Tenant"***
- En algunos casos, se pueden encontrar credenciales en texto claro guardados en los **"Runbooks"**
- Las cuentas de automatización tienen acceso a conexiones, como, por ejemplo, con **"Key Vaults"** a **"Runbooks"**

- Habilidad de ejecutar comandos en **VMs** en premisa si se están utilizando trabajadores híbridos

- Habilidad de ejecutar comandos en **VMs** que utilizan DSC como gestor de configuración.

"Key Vaults"

Otro posible método de escalada de privilegios es aprovechar vulnerabilidades de los roles de un usuario que tiene acceso a un "**Key Vault"**. De esta manera, se pueden obtener secretos y/o acceso a otros usuarios o recursos.

Built-in Role	Description	Can access secrets?
Key Vault Contributor	Can manage key vaults	No
Key Vault Administrator	Perform all data plane operations. Cannot manage role assignment.	Yes
Key Vault Certificates Officer	Perform any action on certificates. Cannot manage permissions.	Yes (Certificates)
Key Vault Crypto Officer	Perform any action on keys. Cannot manage permissions.	Yes (Keys)
Key Vault Secrets Officer	Perform any action on secrets. Cannot manage permissions.	Yes (Secrets)
Key Vault Secrets User	Read secret contents.	Yes (Secrets)
Key Vault Crypto Service Encryption User	Read metadata and perform wrap/unwrap operations on keys	No
Key Vault Crypto User	Perform cryptographic operations using keys	No
Key Vault Reader	Read metadata of key vaults and its certificates, keys, and secrets.	No

Ilustración 20. Roles en un "Key Vault"

Además, también se puede escalar privilegios abusando vulnerabilidades de aplicaciones con secretos de usuarios. Si, mediante este método, se obtiene un usuario que tiene como rol de administrador de aplicación, es posible crear una contraseña de aplicación para autenticarse en el "***Tenant"*** como un **"Service Principal"**. De esta manera, se puede:

- Evitar **MFA**

- Acceder a todos los recursos asignados al **"Service Principal"** autenticado

- Añadir credenciales a aplicaciones como método de persistencia tras comprometer a un ***"Tenant"***

Plantillas ARM

Se puede obtener información interesante en el historial de despliegue de **"Azure"**. Permite obtener información sobre todos los recursos que no se encuentran actualmente desplegados,

pero pueden estarlo en el futuro. En caso de que un parámetro que contenga información sensible (como secretos) no tenga el tipo de "**SecureString**" sino el "**String**" implementado, se podrá obtener el secreto en texto claro.

Despliegue Continuo

Debido a que **"Azure Functions"** implementa la funcionalidad despliegue continuo, en caso de estar activado, una actualización del código fuente dispara un despliegue en **"Azure"**.

Las fuentes de código que soporta **"Azure"** son:

- Repositorios **"Azure"**
- "**GitHub**"
- *"**Bitbucket"***

Una mala configuración de una aplicación defunción que se despliega directamente en producción, puede ser explotada para asumir y robar la identidad de la aplicación.

4.3.3.2.5 Movimiento lateral

Máquinas conectadas a "Azure AD" – Pass the PRT

Se puede obtener un movimiento lateral en caso de comprometer máquinas unidas a **"Azure AD"** y, además, se haya podido extraer su "***Primary Refresh Token"*** (**PRT** – utilizados para solicitar ***"tokens"*** de acceso para una aplicación en particular), junto con otras claves para el usuario. En caso de obtener un acceso administrativo a otras máquinas unidas, se puede realizar el movimiento hacia otras máquinas.

En otras palabras, obteniendo un **PRT** y una clave de sesión, se puede solicitar ***"tokens"*** de acceso para cualquier aplicación.

Pass-the-Certificate

En caso de obtener las claves de una máquina unida por **"Azure AD"**, se puede solicitar certificados para un usuario y, modificando dicho certificado, generar un nuevo usuario administrativo en otra máquina conectada.

Cloud a On-Prem – Intune

Utilizando un "**Endpoint Manager"**, un usuario con roles de Administrador Global o Administrador Intune puede ejecutar scripts de Powershell en un dispositivo Windows registrado. Dicho script se ejecuta con privilegios de **SYSTEM** y, generalmente, no se puede observar la salida del script y, además, no se puede volver a ejecutar el script a no ser que sea modificado. Mediante este proceso, se puede realizar la ejecución de scripts PowerShell

en máquinas que se encuentran en la infraestructura de la organización para añadir nuevos usuarios administrativos a dicha máquina.

Grupos Dinámicos

Por defecto, cualquier usuario puede invitar a otros usuarios en **"Azure AD"**. Si una regla de un grupo dinámico de **"Azure AD"** permite añadir usuarios basándose en atributos que un usuario invitado puede modificar, se pueden abusar las reglas de dos maneras:

- Antes de unirse al ***"Tenant"*** como invitado, pudiendo enumerar atributos utilizadas en una regla (como por ejemplo el correo), se puede utilizar dicho atributo para invitar a un usuario

- Después de unirse al ***"Tenant"*** como invitado, dado que los invitados pueden administrar su propio perfil, pueden modificar su correo alternativo o su Manager.

Application Proxy

A pesar de que la funcionalidad de "**Applicaiton Proxy"** proporciona medidas de seguridad adicionales (autenticación prestada por **"Azure AD"** y Accesos Condicionales, entre otros), si el código de la aplicación en premisa presenta alguna vulnerabilidad de código, ésta puede ser explotada para obtener un movimiento Lateral de Cloud a infraestructura.

Skeleton Key – PTA

Como se ha mencionado previamente, en el proceso de **PTA**, si se consigue comprometer el agente de autenticación de **"Azure AD"**, sería posible verificar autenticaciones para cualquier usuario sincronizado, sin importar si su contraseña es errónea o no. En otras palabras, mediante este ejercicio, simplemente al implementar un "***userPrincipalName"*** válido, se podría utilizar cualquier contraseña que el Agente de Autenticación comprometido la verificaría como válida. Además, si se consiguiera comprometer un Administrador Global, sería posible realizar la instalación de un agente de autenticación en nuestra propia infraestructura, lo que permitiría autorizar todos los intentos de inicio de sesión.

Golden SAML attacks – Federación "Azure AD"

El modelo de federación de **"Azure"** utiliza **AD FS**, que se trata de un modelo de identidad basado en afirmaciones. En otras palabras, utiliza afirmaciones sencillas (como nombre, identidad o grupo) hechas sobre los usuarios que se utilizan primordialmente para autorizar el acceso a aplicaciones basadas a su vez en afirmaciones. Estas afirmaciones de usuarios se escriben dentro de ***"tokens"*** de **SAML** y una vez finalizadas, son firmadas para proporcionar confidencialidad por parte del **IdP**. Se identifica a un usuario mediante el parámetro ***ImmutableID***, que es globalmente único y se almacena en **"Azure AD"**.

La respuesta **SAML** es firmada por un certificado de firmas de ***"tokens"***. Si dicho certificado se ve comprometido, es posible realizar el proceso de autenticación a **"Azure AD"** como

cualquier usuario sincronizado a la nube. Dicho certificado puede ser extraído del servidor **ADFS** con privilegios de **DA**, pudiendo autenticarse con cualquier contraseña para un usuario sincronizado a la nube, al igual que en el ejercicio de **PTA**.

4.3.3.2.6 Persistencia

En estos procesos de persistencia se busca principalmente puntos donde se pueda modificar y/o crear recursos y/o permisos o, además, obtener un acceso que se encuentre limitado en tiempo.

Dado que Microsoft recomienda unir el servidor **"Azure AD Connect"** al **AD** de premisa, los mecanismos de persistencia (como, por ejemplo, "**Golden Ticket"**, "**Silver Ticket"**, "**ACL Backdoor"**, entre muchos otros) permitirían obtener **GA** en **"Azure AD"** bajo demanda.

Los abusos implementados para persistencia son:

- **PHS** para extraer credenciales
- **PTA** para instalar el agente
- Para federación, se puede extraer el certificado del servidor **ADFS** utilizando **AD**

PTA y PHS

Si el autoservicio de reseteo de contraseña se encuentra habilitado (lo que permite a los usuarios resetear sus propias contraseñas de **"Azure AD"**) y el reseteo se propaga por el **AD** en premisa mediante la reescritura de la contraseña, se presenta un escenario interesante de persistencia.

Si el **AD** en premisa se ha visto ya comprometido, se puede proporcionar altos permisos ("**DCSync"** usando "**AdminSDHolder**") a un usuario sincronizado que puede ser controlado y resetear su contraseña de **"Azure AD"**. Esto proporcionará privilegios DA en premisa que se pueden utilizar para obtener **GA** en **"Azure AD"**. Como **"Azure AD Connect"** no permite resetear las contraseñas de las cuentas con "***admincount"***, es necesario realizar ataques de permisos como "**FullControl/DCSyncs"** utilizando "**AdminSDHolder"**

Federación – Dominio de confianza

Si se obtienen privilegios GA en un ***"Tenant"***, se puede añadir un nuevo dominio (tras un proceso de validación), configurar su tipo de autenticación a Federado y configurar el dominio para confiar en un certificado y proveedor específico.

Federación – Certificado de firma de "tokens"

Con privilegios **DA** en la premisa **AD**, es posible crear e importar nuevas firmas de ***"tokens"*** y certificados de descifrado de ***"tokens"***, que tienen una validez alta. Esto permite iniciar sesión con cualquier usuario de "***ImutableID"*** conocida.

Claves de acceso de la cuenta de almacenamiento

Dado que las claven proporcionan permisos equivalentes a los de un administrador en una cuenta de almacenamiento. Existen dos claves de acceso que no se rotan automáticamente, a no ser que la "**Key Vault"** administre dichas claves, lo cual proporciona acceso persistente a las cuentas de almacenamiento. Además, también se puede generar **URL SAS** utilizando dichas claves de acceso.

Aplicaciones y "Service Principals"

Se pueden utilizar "**Aplicaciones Enterprise" de "Azure AD" ("Service Principal"**) y Registros de Aplicación (aplicaciones) para la persistencia. Con permisos de Administrador de Aplicación, GA, o rol personalizado con permisos de "***micrososft.directory***", aplicaciones, credenciales o actualización, se puede añadir credenciales (secretos o certificados) a una aplicación existente.

Analizando una aplicación con altos permisos es un método útil para la persistencia, que además también permite saltar **MFA**. Por otro lado, también se puede añadir una nueva aplicación con altos permisos y utilizarla para la persistencia. Con privilegios **GA**, se puede crear una aplicación con el rol de Administrador de Autenticación Privilegiado, lo que permite resetear la contraseña de Administradores Globales.

Otorgación de consentimiento ilícito

Por defecto, cualquier usuario puede registrar una aplicación en **"Azure AD"**. De esta manera, se puede registrar una aplicación que necesite altos permisos de alto impacto con el consentimiento de administrador como, por ejemplo, enviando un email suplantando al usuario.

Azure VMs y NSGs

Obteniendo un acceso remoto a una **"Azure VM**", dado que estas también implementan la gestión de identidades, proporcionaría una puerta de acceso a recursos de **"Azure"** adicionales. Realizando una captura del disco de la **VM** ejecutando, se pueden extraer, por otro lado, secretos almacenados en el disco. También es posible adjuntar un disco modificado/comprometido a una **VM** apagada para, por ejemplo, añadir un administrador local. Finalmente, la modificación de **"Azure Network Groups** (**NSGs)"** permitiría un acceso desde direcciones IP que se pueden controlar y gestionar.

Roles "Azure AD" customizados

En caso de obtener un "**General Availability (GA)"** en un **"*tenant*"**, se puede modificar un rol customizado y asignárselo a un usuario que se pueda controlar.

Modificación de despliegue

Si se obtienen accesos persistentes a un recurso externo, como repositorios de "**GitHub"** que forman parte de la cadena de despliegue, sería posible obtener una persistencia continua en el ***"Tenant"*** objetivo.

4.3.3.3 Herramientas

4.3.3.3.1 Azure AD Powershell

El módulo **"Azure AD Powershell"** [63] se utiliza para gestionar y administrar **"Azure AD"**. A pesar de que no muestre todas las propiedades de objetos de **"Azure AD"** ni tenga una documentación detallada, se puede utilizar este módulo para interaccionar con **"Azure AD**", pero no para acceder a sus recursos.

Las diversas acciones que se pueden realizar con **"Azure AD Powershell"** son:

- Comprobar el estado de la sesión
- Obtener detalles sobre el ***"Tenant"***
- Para usuarios:
    - Enumeración de todos los usuarios
    - Enumeración de información de un usuario específico
    - Realizar la búsqueda de usuarios por nombre
    - Listar los atributos de un usuario
    - Buscar atributos de todos los usuarios por nombre
    - Todos los usuarios que se encuentres conectados desde la premisa
    - Todos los usuarios que sean de **"Azure AD"**
    - Objetos creados por cualquier usuario
    - Objetos pertenecientes a un usuario específico

- Listar todos los grupos

- Para grupos:
  - Listar todos los grupos
  - Enumerar un grupo específico
  - Buscar un grupo por nombre
  - Obtener grupos que permitan la pertenencia dinámica
  - Todos los grupos que se encuentres conectados desde la premisa
  - Todos los grupos que sean de **"Azure AD"**
  - Obtener los miembros de un grupo
  - Obtener los grupos y roles pertenecientes a un usuario
- Para roles:
  - Obtener todas las plantillas de roles disponibles
  - Obtener todos los roles
  - Enumerar los usuarios asignados a un rol
- Para dispositivos:
  - Obtener todos los dispositivos registrados a **"Azure"**
  - Obtener el objeto de configuración del dispositivo
  - Listar todos los propietarios registrados de todos los dispositivos
  - Listar todos los usuarios registrados a todos los dispositivos
  - Listar todos los dispositivos pertenecientes a un usuario
  - Listar todos los dispositivos registrados por un usuario
- Para aplicaciones:

- Obtener todos los objetos de aplicación registrados para un ***"Tenant"***
- Obtener todos los detalles sobre una aplicación
- Obtener una aplicación por su nombre
- Mostrar las aplicaciones con una contraseña de aplicación
- Obtener el propietario de una aplicación
- Obtener las aplicaciones donde un usuario tiene un rol
- Obtener las aplicaciones donde un grupo tiene un rol

- Para **"Service Principals"**:
  - Enumerar los **"Service Principals"**
  - Obtener todos los **"Service Principals"**
  - Obtener detalles sobre un **"Service Principal"**
  - Obtener un **"Service Principal"** por nombre

Por otro lado, a pesar de que **"Azure AD**" no puede solicitar ***"tokens"***, sí que permite utilizados para "**AADGraph"** o "**Microsoft Graph"**

4.3.3.3.2 Az Powershell Module

"Az Powershell" [64] es un módulo de "**Microsoft**" implementado para gestionar recursos de **"Azure"**. Mediante este módulo de línea de comandos, también se pueden generar scripts de automatización que funcionan con **"Azure Resource Manager"** (**ARM**).

Esta herramienta suele ser utilizada para enumerar tanto **"Azure AD"** y, especialmente, recursos de **"Azure"**. Algunos ejemplos que permite enumerar son:

- Todos los contextos actuales y disponibles
- Enumerar suscripciones, recursos y roles
- Enumeración de usuarios, grupos, miembros, aplicaciones y **"Service Principals"**
- Además, puede enumerar otros puntos de interés como cuentas de almacenamiento y **"Key Vaults"**

Además, también se puede utilizar este módulo para el robo de ***"tokens"*** de acceso implementados en **"Azure"**.

4.3.3.3.3 AZ CLI

"Azure CLI" (***az cli***) [65] es un conjunto de comandos utilizados para crear y gestionar recursos de **"Azure"**. Este módulo puede ser instalado en múltiples plataformas y, además, se puede utilizar con varias nubes.

Algunos procesos de enumeración que se pueden conseguir mediante esta herramienta son:

- Comandos comúnmente utilizados para **VMs**
- Usuarios, información sobre "***Tentant"*** y/o suscripciones, grupos, miembros, aplicaciones, propietarios, aplicaciones con credenciales y **"Service Principals"**,

4.3.3.3.4 RoadTOOLS

"RoadTOOLS" [66] es una herramienta utilizada para enumerar entornos de **"Azure AD".**

Los tres pasos implementados en **"RoadTOOLS"** para el robo de credenciales son:

- Autenticación
- Recopilación de datos
- Exploración de datos

4.3.3.3.5 StormSpotter

Se trata de una herramienta de "**Microsoft"** [67] utilizada para crear grafos de ataque para recursos de **"Azure"**. Utiliza la base de datos de "**Neo4j"** para crear grafos de relaciones en **"Azure"** y **"Azure AD**".

Los módulos que trae esta herramienta son:

- **"*Backend*"**: para inyectar los datos en la base de datos de "**Neo4j"**
- **"*Frontend*"**: aplicación web, para visualizar los datos
- **"*Collector*"**: utilizado para recolectar datos de **"Azure"**

4.3.3.3.6 AzureHound

"AzureHound" de **"BloodHound"** [68] utiliza los módulos de **"Azure AD"** y "**Az Powershell"** para recolectar datos. Se trata de una aplicación web de "**Javascript"**

construido por encima de "**Linkurious"**, compilado con "**Electron"** y con una base de datos "**Neo4j"** alimentado por un colector de datos **C#**.

"AzureHound" utiliza la teoría de grafos para revelar relaciones escondidas y, en muchos casos, no intencionados dentro de "**Active Directory"** o del entorno **"Azure"**. Se suele utilizar esta herramienta para identificar caminos de ataque altamente complejos. En otras palabras, se utiliza para encontrar y obtener un mejor entendimiento sobre las relaciones de privilegios en un "**Active Directory"** o entorno **"Azure"**

4.3.3.3.7 O365Creeper

"O365Creeper" [69] es un código de "**Python"** utilizado para validar cuentas de correo que pertenecen a ***"tenants"*** de "**Office 365".** Puede implementar un listado de correos o uno único para realizar esta búsqueda.

4.3.3.3.8 MSOLSpray

"MSOLSpray" [70] es una herramienta de "***sparying passwords***" para cuentas de "**Microsoft Online"** (**"Azure"** o **O365**). Este código registra si:

- Una credencial de usuario es válida
- **MFA** se encuentra habilitado
- Un ***"Tenant"*** no existe
- Un usuario no existe
- La cuenta está bloqueada
- La cuenta está deshabilitada.

4.3.3.3.9 Microburst

Microburst [71] es un kit de herramientas de "**Powershell"** para ataques de **"Azure"**. Incluye funciones y códigos que ayudan en el reconocimiento de Servicios **"Azure"**, auditoria de configuración débil y acciones de post explotación como volcado de credenciales.

4.3.3.3.10 Azucar

"Azucar" [72] es una herramienta que ayuda a realizar la evaluación de seguridad en un entorno de **"Azure"** Cloud. Este script no realiza cambios en ningún recurso implementado en la subscripción de **"Azure"**, simplemente genera un archivo "**Excel"** final con los resultados obtenidos.

Alguna de las funcionalidades que incluyen son:

- Devuelve una serie de atributos sobre equipos, usuarios, grupos, contactos y, entre muchos otros, eventos desde **"Azure Active Directory"**.
- Búsqueda de cuentas de alto nivel en un **"Azure *Tenant*"**" específico, incluidos **"Azure Active Directory",** administradores clásicos y roles de directorio (**RBAC**).
- Compatibilidad con "***Multi-Threading***".
- Compatibilidad con otros "***plugins***".
- Los activos soportados por "**Azúcar"** son:
    - **"*Azure SQL Databases*"**, incluidos bases de datos **MySQL** y **PostgreSQL**.
    - ***"Azure Active Directory"***
    - ***"Storage Accounts"***
    - ***"Classic Virtual Machines"***
    - ***"Virtual Machines V2"***
    - ***"Security Status"***
    - ***"Security Policies"***
    - ***"Role Assignments (RBAC)"***
    - ***"Missing Security Patches"***
    - ***"Missing Security Baseline"***
    - ***Web Application Firewall"***
    - ***"Network Security Groups"***
    - ***"Classic Endpointsy"***
    - ***"Azure Security Alerts"***
    - ***"Azure KeyVault"***

Capítulo 5. DESARROLLO Y ANÁLISIS DE RESULTADOS

5.1 EJERCICIOS DE "RED TEAM"

Los ejercicios de ***"Red Team"*** consisten en la simulación de un ataque dirigido o **APT** (***Advanced Persistent Threat***) sobre una determinada organización, utilizando para ello las mismas técnicas, tácticas y procedimientos que serían aplicados por un adversario o grupo real. Para el correcto desarrollo de estas pruebas es necesario, por lo tanto, que todas las acciones sean realizadas de igual forma a como serían ejecutadas durante un ataque dirigido contra la organización por un adversario real.

Por ello, no se busca identificar el mayor número de vulnerabilidades, sino lograr el acceso a la organización, comprometer sus principales activos y demostrar cual sería el nivel de riesgo e impacto que tendría la ejecución sobre la organización, así como su capacidad de detección y respuesta frente a la amenaza que se haya diseñado.

Finalmente, la necesidad de la ejecución de estas simulaciones reales se usa para realizar una comprobación global donde se verifique el riesgo y capacidades reales de la organización para hacer frente a una amenaza. Los beneficios directos del desarrollo de ejercicios de ***"Red Team"*** en la organización serían la identificación de vectores críticos, evaluación del nivel de exposición y riesgo, capacidad de prevención y detección de amenazas, eficiencia de los procedimientos internos y, por último, la identificación de principales vulnerabilidades y debilidades de la organización.

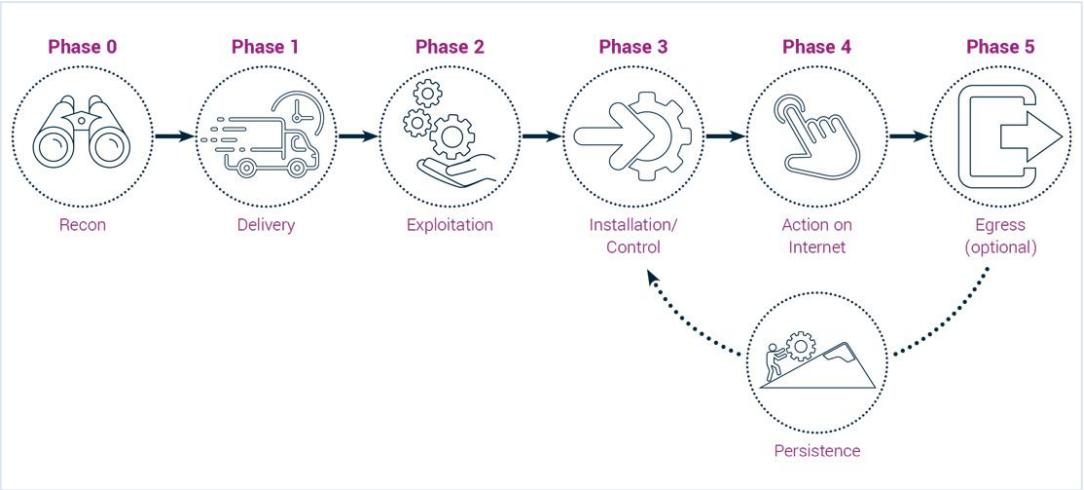

Tabla 10. Fases de "Red Team"

5.1.1 TTPS: TÉNICAS, TÁCTICA Y PROCEDIMIENTOS

Las técnicas, tácticas y procedimientos (**TTPs**) pasos que realiza el adversario durante el desarrollo y ejecución de la amenaza contra la organización. Durante la ejecución de los ejercicios de ***"Red Team"***, se emplean los mismos y permite desarrollar un vector completo con el que realizar un seguimiento en detalle de las acciones que ha realizado el adversario durante el proceso de intrusión.

Estas tácticas y técnicas pueden obtenerse, de forma general, a partir de la matriz de **"MITRE ATT&CK"**.

5.1.2 AUTOMATIZACIÓN DE INFRAESTRUCTURA DE *"RED TEAM"*

La creación de infraestructuras automatizadas para la ejecución de ejercicios de ***"Red Team"***, es un punto necesario que permite agilizar el inicio de los trabajos. Para ello es necesario contar con un entorno en la nube donde desplegar todos los componentes que van a usarse durante los ejercicios. El diagrama, que se muestra a continuación, ofrece un claro ejemplo de cómo componer este tipo de infraestructuras.

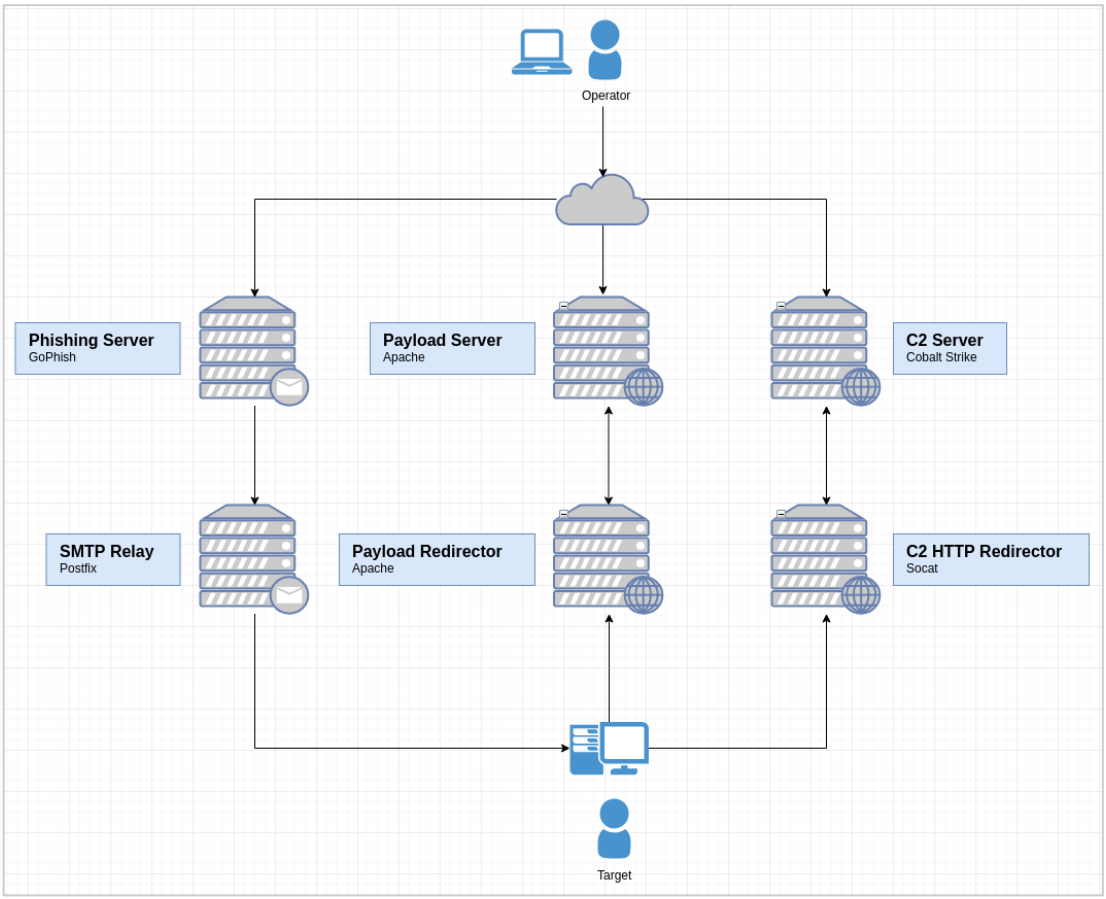

Ilustración 21. Infraestructura de "Red Team"

5.2 METODOLOGÍA DE ANÁLISIS DE SEGURIDAD CLOUD

Una vez finalizado con el proceso de análisis, tanto de componentes como de ataques y vulnerabilidades, a continuación, se muestra el listado final con los controles recomendados para realizar el proceso de análisis de seguridad en Cloud. Se debe tener en cuenta que en esta metodología no solo se encuentra los ejercicios comúnmente utilizados en análisis de Cloud, sino además se han implementado los recomendados en **"MITRE ATT&CK"**, analizados y explicados en apartados previos.

El resultado final es el siguiente:

(CLD-INFO) Reconocimiento	
CLD-INFO-1	Descubrimiento de usuarios
CLD-INFO-2	Descubrimiento de cuentas de correo
CLD-INFO-3	Enumeración de cuentas de usuario predeterminados o adivinables
CLD-INFO-4	Enumeración de usuarios con privilegios
CLD-INFO-5	Descubrimiento de ***"Service Principals"***
CLD-INFO-6	Descubrimiento de Grupos
CLD-INFO-7	Descubrimiento de ***"Tenants"***
CLD-INFO-8	Descubrimiento de Dispositivos
CLD-INFO-9	Descubrimiento de Roles
CLD-INFO-10	Descubrimiento de Permisos
CLD-INFO-11	Descubrimiento de Aplicaciones
CLD-INFO-12	Descubrimiento de infraestructura de la nube
CLD-INFO-13	Descubrimiento de servicios y componentes
CLD-INFO-14	Descubrimiento de objetos de almacenamiento de la nube
CLD-INFO-15	Descubrimiento de servicios de red
CLD-INFO-16	Descubrimiento de políticas de contraseñas y autenticación
CLD-INFO-17	Descubrimiento de políticas de seguridad
CLD-INFO-18	Descubrimiento de software
CLD-INFO-19	Descubrimiento de información sistemas
CLD-INFO-20	Descubrimiento de localización sistemas
CLD-INFO-21	Descubrimiento de dominios y subdominios
CLD-INFO-22	Descubrimiento de permisos **IAM**
CLD-INFO-23	Descubrimiento de ***"buckets"***, junto con sus accesos y permisos.
CLD-INFO-24	Enumeración de recursos públicos
CLD-INFO-25	Extracción de datos a través del Panel de servicio en la nube
CLD-INFO-26	Identificación de rutas de escalada de privilegios
CLD-INFO-27	Generación de grafos de ataque
CLD-INFO-28	Evaluación de nivel de seguridad
CLD-INFO-29	Rastreo de red y eventos
CLD-INFO-30	Revisión de fuga de información en comentarios y metadatos
CLD-INFO-31	Identificación de puntos de entrada de la aplicación
CLD-INFO-32	Reconocimiento del ***framework*** usado en la aplicación
CLD-INFO-33	Enumeración de la arquitectura Red y de la Aplicación

(CLD-PREP) Preparación	
CLD-PREP-1	Prueba de ***bucket Pillaging***
CLD-PREP-2	Inyección de código
CLD-PREP-3	Secuestro de domino
CLD-PREP-4	Explotación de cuentas de automatización
CLD-PREP-5	Explotación de conexión a ***Key Vauls***
CLD-PREP-6	Explotación de plantillas ARM
CLD-PREP-7	Explotación de despliegue continuo
CLD-PREP-8	Prueba de ataque de ***Pass the PRT***
CLD-PREP-9	Prueba de ataque de ***Pass the Certificate***
CLD-PREP-10	Explotación de grupos dinámicos
CLD-PREP-11	Explotación de aplicaciones Proxy
CLD-PREP-12	Prueba de ataque de ***Skeleton Key***
CLD-PREP-13	Análisis de códigos de error
CLD-PREP-14	Análisis de trazas de excepción
(CLD-DIST) Distribución	
CLD-DIST-1	Pruebas sobre la política de nombres de usuario
CLD-DIST-2	Prueba de ataque de ***Phising***
CLD-DIST-3	Prueba de ataque de ***Spearphising*** interno
CLD-DIST-4	Contaminación de contenido compartido
CLD-DIST-5	Utilización de material de autenticación alternativo
CLD-DIST-6	Prueba de ataque de ***Shadow Copy***
CLD-DIST-7	Prueba de ataque de ***Golden SAML***
CLD-DIST-8	Prueba de ataque de ***Shadow Admin***
CLD-DIST-9	Pruebas de verificación y validación de cuentas
CLD-DIST-10	Pruebas de robo de credenciales
CLD-DIST-11	Pruebas de Cuentas Válidas
(CLD-EXPL) Explotación	
CLD-EXPL-1	Prueba de compromiso ***Drive By***
CLD-EXPL-2	Explotación de aplicaciones públicas
CLD-EXPL-3	Relación de Confianza
CLD-EXPL-4	Prueba de fuerza Bruta
CLD-EXPL-5	Prueba de forjado de credenciales web
CLD-EXPL-6	Generación de solicitudes de autenticación multi-factor:
CLD-EXPL-7	Robo de ***"tokens"*** de acceso de aplicación
CLD-EXPL-8	Robo de cookies de sesión
CLD-EXPL-9	Credenciales no seguras (como ***password spraying***)
CLD-EXPL-10	Credenciales por defecto
CLD-EXPL-11	***Metadata Server-Side Request Forgery (SSRF)***
CLD-EXPL-12	Explotación de vulnerabilidades de configuración
CLD-EXPL-13	Explotación de base de datos
CLD-EXPL-14	Otorgación de consentimiento ilícito
CLD-EXPL-15	Transmisión de credenciales sobre canal cifrado
CLD-EXPL-16	Pruebas de recordatorio de contraseña y restablecimiento
CLD-EXPL-17	Pruebas sobre los mecanismos pregunta/respuesta de seguridad

CLD-EXPL-18	Pruebas sobre el tiempo de expiración de sesión
CLD-EXPL-19	Pruebas de CSRF
(CLD-INST) Instalación	
CLD-INST-1	Implantación de una imagen interna
CLD-INST-2	Inicio de aplicación de Office
(CLD-CMCN) Comando y Control	
CLD-CMCN-1	Ejecución de usuario
CLD-CMCN-2	Manipulación de cuentas
CLD-CMCN-3	Creación de cuentas
CLD-CMCN-4	Modificación de política de dominios
CLD-CMCN-5	Ocultación de artefactos
CLD-CMCN-6	Debilitar defensas
CLD-CMCN-7	Modificación de la infraestructura de computación de la nube
CLD-CMCN-8	Regiones de nube no utilizadas/soportadas
CLD-CMCN-9	Ejecución de comandos SSM
CLD-CMCN-10	Acceso de consola a través de claves API
CLD-CMCN-11	Cubrir rastro a través de ofuscación de logs
CLD-CMCN-12	Explotación de dominios de confianza
CLD-CMCN-13	Explotación de certificados de firma de ***"tokens"***
CLD-CMCN-14	Robo de claves de acceso de la cuenta de almacenamiento
(CLD-ACOB) Acciones sobre objetivo	
CLD-ACOB-1	Recopilación automatizada
CLD-ACOB-2	Datos obtenidos desde objetos de almacenamiento de nube
CLD-ACOB-3	Datos obtenidos desde repositorios de información
CLD-ACOB-4	Prueba de ***Data Staged***
CLD-ACOB-5	Recopilación de correos electrónicos
CLD-ACOB-6	Transferencia de datos a cuentas de nube
CLD-ACOB-7	Eliminación de acceso a la cuenta
CLD-ACOB-8	Destrucción de datos
CLD-ACOB-9	Datos encriptados para el impacto
CLD-ACOB-10	Prueba de ***Dafecement***
CLD-ACOB-11	Denegación de servicio en puntos finales
CLD-ACOB-12	Denegación de servicios de red
CLD-ACOB-13	Prueba de ***Hijacking*** de recursos

Tabla 11. Metodología de análisis de seguridad Cloud

5.3 SIMULACIÓN SOBRE ENTORNO AZURE

En este apartado, tras finalizar con el diseño de la metodología propuesta para este trabajo de fin de máster, se procede a realizar análisis de seguridad en un entorno de **"Azure"**. Dado que este entorno se ha realizado en una infraestructura privada, no se ha podido obtener la oportunidad de realizar ejercicios más avanzados, como de explotación y distribución, ya que podían suponer una modificación o eliminación de componentes que se encontrase en uso.

Por este motivo, se ha procedido a realizar la prueba de los ejercicios planteados en la metodología anterior, utilizando a su vez herramientas recomendadas en el apartado de **"Modelado de amenazas"**, que se corresponden únicamente a la fase de reconocimiento. De esta manera, se realizará una simulación únicamente extrayendo información de la infraestructura, para de esta manera indicar posibles siguientes pasos para la continuación del análisis, sin comprometer ningún componente privado de la organización.

En la siguiente imagen se puede mostrar la conexión realizada a un ***"Tenant"*** de **"Azure"**:

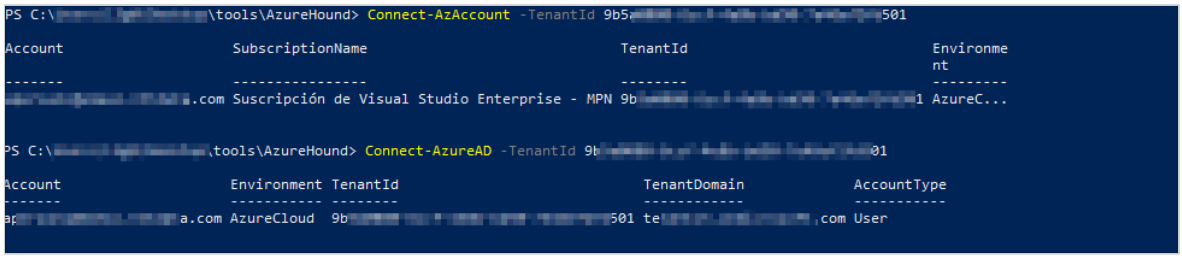

Ilustración 22. Conexión con el entorno "Azure"

5.3.1 "AZUREHOUND"

La primera herramienta para probar en esta simulación es ""**AzureHound**"" que, como bien se ha explicado en apartados anteriores, utiliza la teoría de grafos para revelar relaciones escondidas y no intencionadas dentro del entorno de **"Azure"**. Generalmente, se suele utilizar esta herramienta para identificar posibles vectores que permitan obtener mayor acceso a la organización.

En la siguiente captura se puede observar la implementación de la herramienta de **"AzureHound"** donde, además, se muestra los mensajes resultantes al realizar el análisis del entorno **"Azure"** conectado:

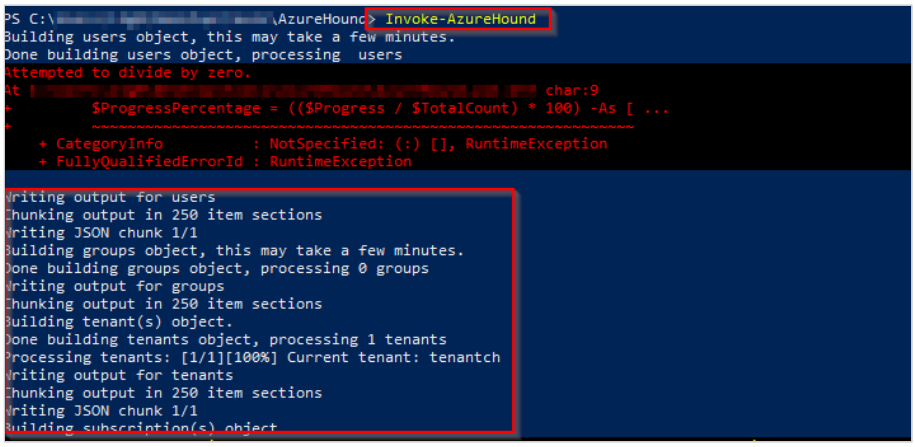

Ilustración 23. Ejecución de "AzureHound" en un entorno de "Azure"

Al finalizar el comando, este devuelve un fichero comprimido con los resultados finales obtenidos:

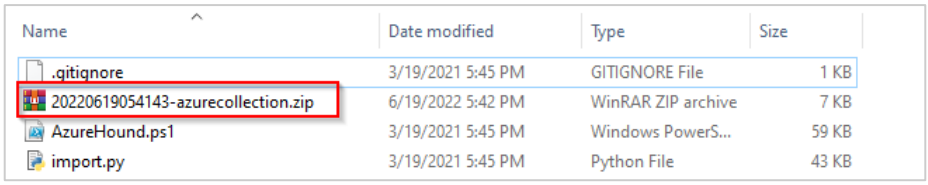

Ilustración 24. Fichero obtenido al finalizar "AzureHound"

Para obtener los grafos de las relaciones obtenidas, se debe implementar dicho fichero en la aplicación de **"BloodHound"**. Esta utilizará los datos introducidos para dibujar todas las relaciones.

Los grafos mostrados a continuación se han obtenido a partir de los objetos **"Azure"** encontrados en pasos anteriores. Dichos objetos son los siguientes:

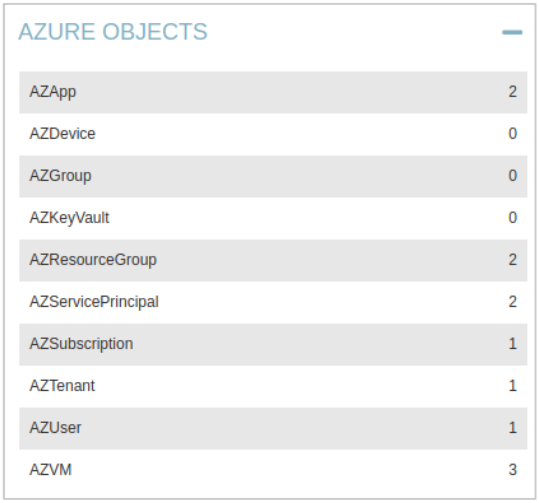

Ilustración 25. Objetos "Azure" obtenidos mediante "AzureHound"

A partir de esta información, la aplicación **"BloodHound"** puede realizar el diseño de grafos donde se muestran la relación entre estos objetos.

En primer lugar, se ha obtenido el identificador del ***"Tenant* Azure"** que se está analizando, la suscripción que tiene asignada y, para dicha subscripción, los grupos de recursos generados:

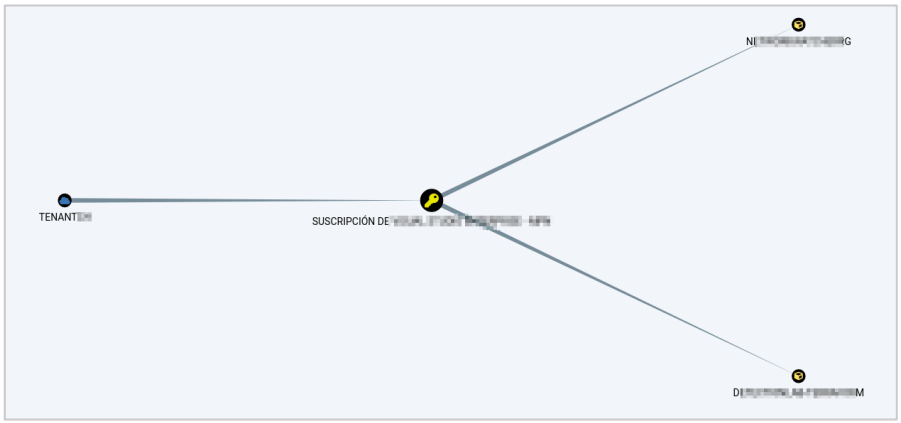

Ilustración 26.Grafo de "AzureHound" con TenantID, Subscripción y grupos de recursos

En uno de los grupos de recursos, se ha podido encontrar que tiene asignado un total de 3 máquinas virtuales, las cuales también se encuentran conectadas a un ***"Service Principal"***.

- Las máquinas virtuales encontradas son: **DC.WINDOMAIN.LOCAL**, **WEF.WINDOMAIN.LOCAL** y **WIN10.WINDOMAIN.LOCAL**
- ***"Service Principal"*** con privilegios es representado por el símbolo del robot gris.
- El grupo de recurso asignado está representado por una caja de color amarillo

El grafo mencionado se muestra a continuación:

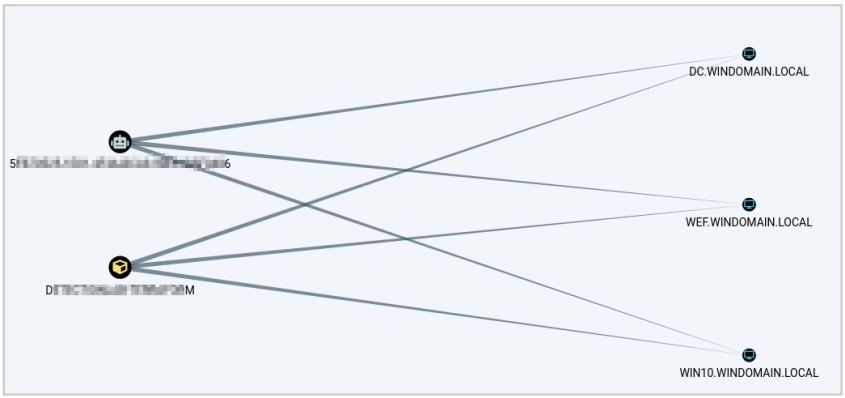

Ilustración 27. Grafo de "AzureHound" con las máquinas virtuales, Grupo de recursos y "Service Principal"

Además de realizar la representación de relaciones entre objetos, **"AzureHound"** también permite la enumeración de aplicaciones encontradas en el entorno **"Azure"**. En esta simulación se han podido encontrar dos en concreto: la primera se trata de una aplicación propia de la organización y, por otro lado, la segunda se corresponde a una aplicación **"Azure CLI"**.

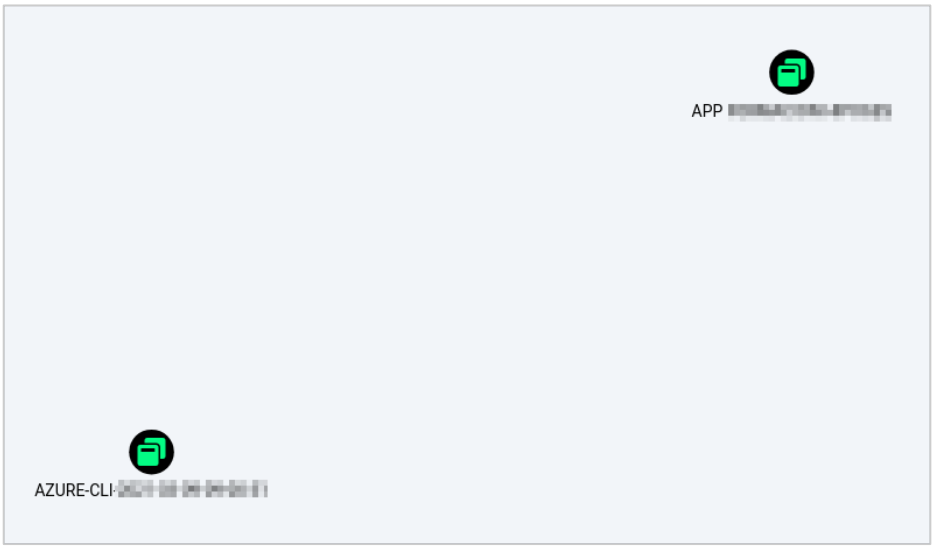

Ilustración 28. Grafo con las aplicaciones encontradas mediante "AzureHound"

Finalmente, se ha podido encontrar que, para una de las aplicaciones, existe un usuario propietario asignado a dicha aplicación:

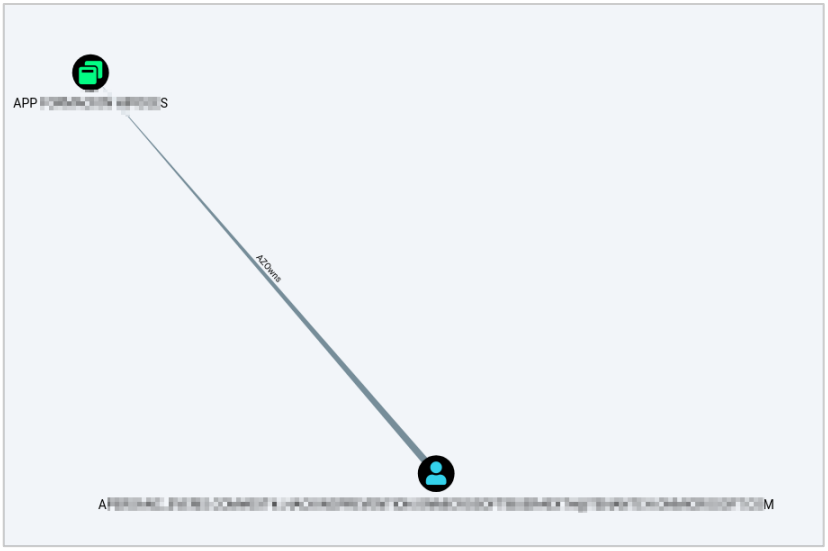

Ilustración 29. Grafo de "AzureHound" con el usuario propietario de una aplicación

5.3.2 AZUCAR

Por otro lado, la segunda herramienta a examinada en esta simulación es "**Azucar"** que, en este caso, se centra en la evaluación de seguridad de un entorno de **"Azure"**.

Al ejecutar dicha herramienta, se pueden observar los siguientes mensajes en la consola de comandos:

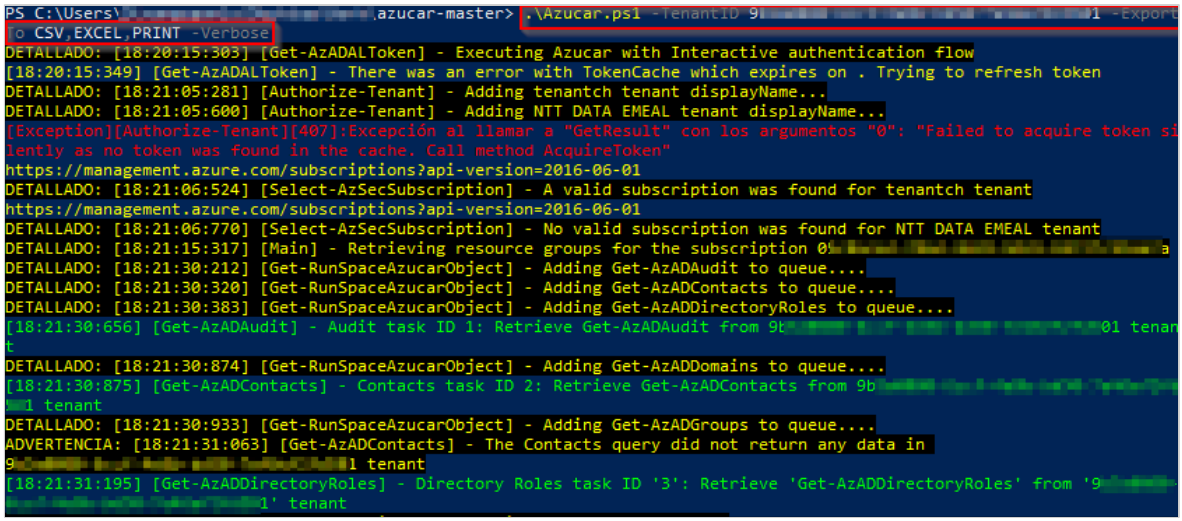

Ilustración 30. Ejecución de la herramienta Azucar

Tras finalizar su ejecución, devuelve un documento Excel con información relacionada con el entorno analizado:

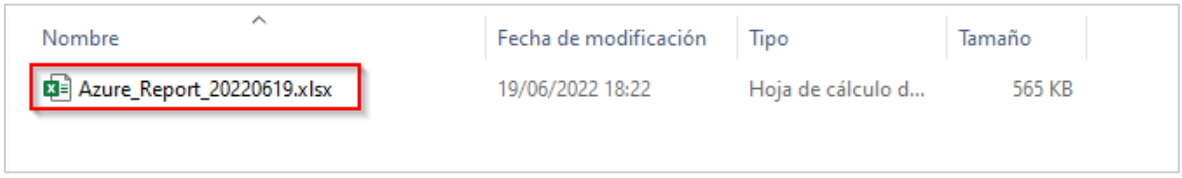

Ilustración 31. Archivo Excel obtenido mediante Azucar

En el mismo Excel, como bien se puede comprobar en la siguiente imagen, se puede observar los siguientes atributos:

- Atributos relacionados con los equipos, usuarios, grupos, contactos y eventos desde **"Azure Active Directory"**
- Búsqueda de cuentas
- Compatibilidad con "***Multi-Threading"***
- Compatibilidad con otros "***plugins"***

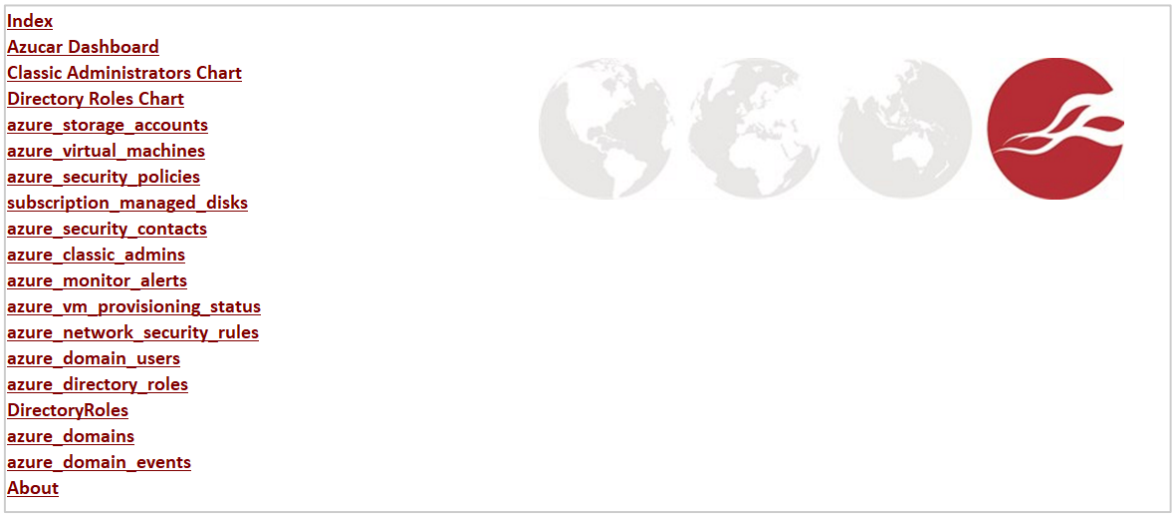

Ilustración 32. Índice de resultados mediante "Azucar"

Algunos ejemplos de los resultados obtenidos son, por un lado, la enumeración de cuentas de almacenamiento:

	name	location	ResourceGroupName	Kind	SkuName	SkuTier	CreationTime	primaryLocation	statusofPrimary
2	d…5	westeurope	D…m	StorageV2	Standard_LRS	Standard	2022-06-13T10:11:45.6494084Z	westeurope	available

Ilustración 33. Descubrimiento de cuentas de almacenamiento

Por otro lado, la enumeración de máquinas virtuales, junto con su localización, ID, tipo de sistema operativo y versión:

	VMName	resourceGroupName	Location	VMID	Type	osType	osOffer	adminusername
2	d…l	D…M	westeurope	8…ff	Standard_D1_v2	Windows	WindowsServer 2016-Datacenter	
3	w…l	D…M	westeurope	6…4	Standard_D1_v2	Windows	WindowsServer 2016-Datacenter	
4	v…l	D…M	westeurope	6…	Standard_D1_v2	Windows	Windows-10 19h1-pron	

Ilustración 34. Enumeración de máquinas virtuales

A continuación, también se muestra las políticas de seguridad implementadas en los diversos servicios de la nube:

	name	policyLevel	unique	logCollection	Security Contacts Emails	Security Contacts Phone	Last Saved Policy	Enabled Notifications	Send emails to Subscription Owner
2	d…t	Subscription	Off	Off				False	False
3	N…G	ResourceGroup	Off	Off				False	False
4	D…m	ResourceGroup	Off	Off				False	False

Ilustración 35. Políticas de seguridad

Como último ejemplo, también de muestra los usuarios encontrados en el domino:

	objectId	accountEnabled	department	displayName	mail
2	3…d	True		a…m	

Ilustración 36. Enumeración de usuarios encontrados

Mediante esta herramienta, como bien se puede observar en el índice de la ***Ilustración 27***, se ha podido obtener una mayor cantidad de información relacionada con el entorno **"Azure"** que, para evitar la posible fuga de datos, se ha optado por limitar la información expuesta en este trabajo.

Sin embargo, se puede concluir que esta herramienta permite recopilación de información de gran utilidad para comprender el funcionamiento del entorno **"Azure"** al que se encuentra conectado, además de poder realizar el descubrimiento de roles, usuarios, recursos y, entre otras cosas, eventos capturados dentro de dicho entorno.

Toda esta información es de gran ayuda para determinar posibles pasos futuros, como:

- Explotación de recursos expuestos para intentar obtener una conexión remota con alguna de ellas
- Explotación a las cuentas de almacenamiento para obtener datos
- Usurpación de identidad de usuarios
- Explotación de las políticas de seguridad implementadas en los servicios para obtener acceso a ellos

5.3.3 "ROADTOOLS" – "ROADRECON"

Otra herramienta para la enumeración del entorno de **"Azure"** es la que se muestra a continuación, **"RoadTOOLS"**. En este caso, se ha utilizado el módulo **"RoadRECON"** para la enumeración y descubrimiento del entorno:

Ilustración 37. Ejecución del módulo "RoadRECON" de "RoadTOOLS"

Para facilitar el uso de esta herramienta, se puede implementar una interfaz de usuario gráfica:

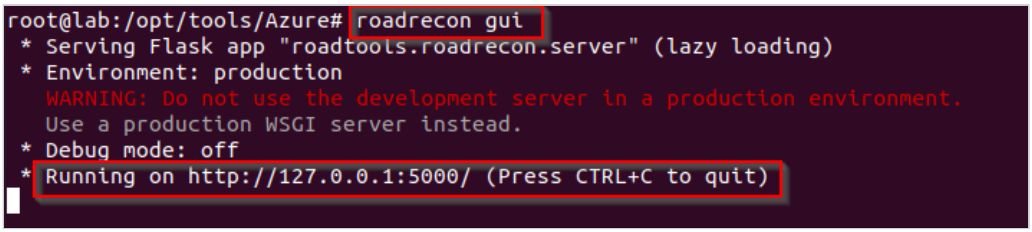

Ilustración 38. Interfaz de usuario gráfica de "RoadRECON"

Al finalizar la ejecución de **"RoadRECON"** y acceder al puerto donde se encuentra la misma interfaz gráfica, se ha podido obtener información sobre el entorno de **"Azure"**.

En este caso, como bien se puede observar en la siguiente imagen, dicha información está relacionada con la enumeración y descubrimiento de:

- Usuarios
- Grupos
- Dispositivos
- Roles de Directorio
- Aplicaciones
- ***""Service Principals"***
- Roles de aplicaciones
- Permisos
- ***"Tenants"***

En la siguiente imagen se puede observar información sobre el ***"Tenant"*** del entorno **"Azure"**:

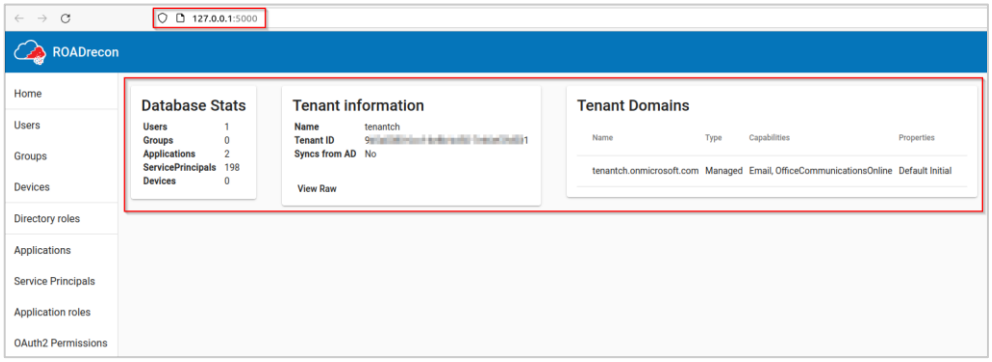

Ilustración 39. Información obtenida a través de "RoadRECON"

Como ya se ha mencionado, en esta aplicación también se puede observar las aplicaciones implementadas en el entorno **"Azure"**, junto con información relacionada como su "**ID"** y ***"Service Principal"***. En la siguiente imagen se muestra el ejemplo con la aplicación de **"Azure CLI"** instalado:

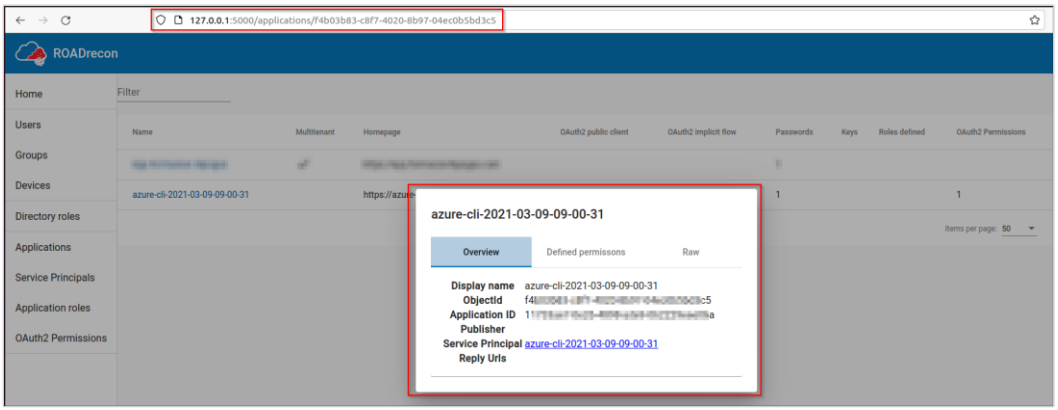

Ilustración 40. Información sobre aplicaciones obtenida mediante "RoadRECON"

Esta información, junto con la herramienta anterior, añade más información relacionada con el entorno **"Azure"** objetivo, lo que permite implementar una mayor variedad de ejercicios para la continuación del análisis como, por ejemplo:

- Explotación de las aplicaciones implementadas, mediante inyección de código, otorgación de consentimiento ilícito u otros ejercicios de análisis.

- Explotación de los roles asignados a dichas aplicaciones mediante, por ejemplo, el robo de ***"tokens"*** de acceso o de cookies de sesión

- Usurpación de usuarios con diversos privilegios a través de ***"phishing"*** tras descubrir sus nombres

5.3.4 MICROBURST

Finalmente, se ha probado el kit de herramientas de "**Powershell Microburst"** para obtener, en este caso, contraseñas almacenadas en **"Azure"**.

En la siguiente captura se muestra la importación del módulo a "**Powershell"**:

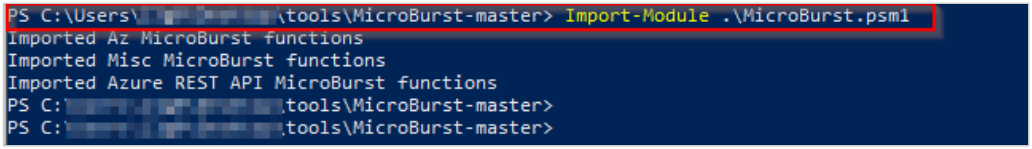

Ilustración 41. Implementación de la herramienta "Microburst"

En este ejemplo, se ejecuta el código de "***Get-AzPasswords"*** para obtener las contraseñas almacenadas en **"Azure"**:

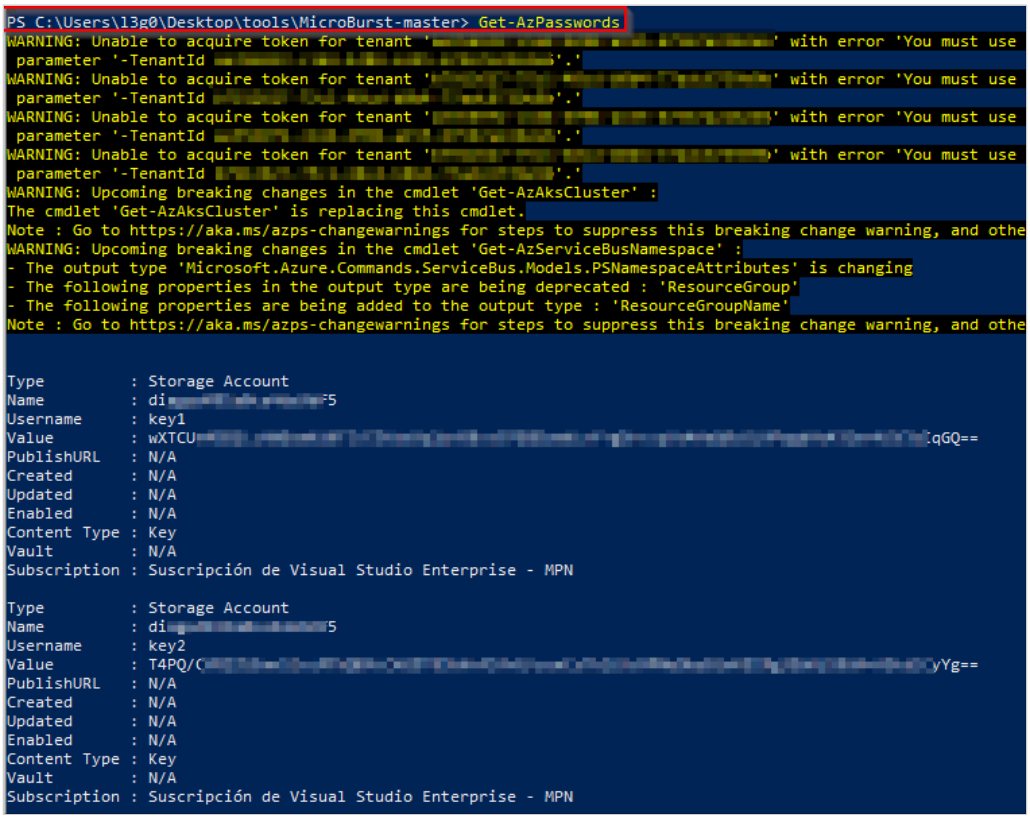

Ilustración 42. Resultado de Get-AzPasswords mediante Microburst

Como se ha podido observar en la imagen anterior, se ha podido conseguir las credenciales de dos cuentas de almacenamiento, lo que nos puede permitir obtener acceso a dichas cuentas y, como consecuencia, acceso completo a la información que tiene almacenada.

5.3.5 ANÁLISIS DE RESULTADOS

Con las herramientas anteriores, se ha conseguido completar los siguientes pasos recomendados en la metodología diseñada:

(CLD-INFO) Reconocimiento		
CLD-INFO-1	Descubrimiento de usuarios	×
CLD-INFO-2	Descubrimiento de cuentas de correo	×
CLD-INFO-3	Enumeración de usuarios y cuentas de usuario predeterminados o adivinables	-
CLD-INFO-4	Enumeración de usuarios con privilegios	×
CLD-INFO-5	Descubrimiento de ***"Service Principals"***	×
CLD-INFO-6	Descubrimiento de Grupos	×
CLD-INFO-7	Descubrimiento de ***"Tenants"***	×
CLD-INFO-8	Descubrimiento de Dispositivos	×
CLD-INFO-9	Descubrimiento de Roles	×
CLD-INFO-10	Descubrimiento de Permisos	×
CLD-INFO-11	Descubrimiento de Aplicaciones	×
CLD-INFO-12	Descubrimiento de infraestructura de la nube	×
CLD-INFO-13	Descubrimiento de servicios y componentes	×
CLD-INFO-14	Descubrimiento de objetos de almacenamiento de la nube	×
CLD-INFO-15	Descubrimiento de servicios de red	×
CLD-INFO-16	Descubrimiento de políticas de contraseñas y autenticación	×
CLD-INFO-17	Descubrimiento de políticas de seguridad	×
CLD-INFO-18	Descubrimiento de software	×
CLD-INFO-19	Descubrimiento de información sistemas	×
CLD-INFO-20	Descubrimiento de localización sistemas	×
CLD-INFO-21	Descubrimiento de dominios y subdominios	×
CLD-INFO-22	Descubrimiento de permisos **IAM**	✓
CLD-INFO-23	Descubrimiento de ***"buckets"***, junto con sus accesos y permisos.	-
CLD-INFO-24	Enumeración de recursos públicos	×
CLD-INFO-25	Extracción de datos a través del Panel de servicio en la nube	-
CLD-INFO-26	Identificación de rutas de escalada de privilegios	×
CLD-INFO-27	Generación de grafos de ataque	×
CLD-INFO-28	Evaluación de nivel de seguridad	×
CLD-INFO-29	Rastreo de red y eventos	×
CLD-INFO-30	Revisión de fuga de información en comentarios y metadatos	-
CLD-INFO-31	Identificación de puntos de entrada de la aplicación	-
CLD-INFO-32	Reconocimiento del ***framework*** usado en la aplicación	-
CLD-INFO-33	Enumeración de la arquitectura Red y de la Aplicación	-

Tabla 12. Controles expuestos en la simulación

Además, con la última herramienta se ha podido realizar un paso de la fase de explotación y distribución que, en este caso, se refiere a la obtención de credenciales de una cuenta de almacenamiento.

El único paso que no se ha podido realizar, ya que no se ha podido implementar un análisis más exhaustivo de las cuentas obtenidas es la obtención de rutas de escalada de privilegios. El resto de los casos no aplican a este estudio ya que este análisis se ha realizado con una conexión directa al entorno **"Azure"** y, por este motivo, no ha sido necesario realizar un análisis de seguridad de las aplicaciones que se encuentran públicas y conectadas a la nube.

Capítulo 6. CONCLUSIONES Y TRABAJOS FUTUROS

6.1 CONCLUSIONES

A lo largo de este trabajo, se ha podido observar que las debilidades que presentan cada uno de los tres proveedores planteados en este proyecto dependen enormemente del tipo de servicio que estén implementando, sus versiones, los niveles de seguridad y, además, las tecnologías que se utilizan en cada una de sus infraestructuras. De esta manera, el primer análisis realizado en este trabajo sobre las soluciones que ofrece cada proveedor, además de la comparativa final entre ellos, ha permitido obtener un mayor entendimiento sobre las características que presenta que proveedor, además de las diversas funcionalidades que presentan sus productos.

Por otro lado, tras realizar un segundo análisis sobre las vulnerabilidades y ataques más comúnmente utilizados contra estos proveedores, se ha procedo a realizar la metodología de análisis. Además, tomando como ejemplo metodologías existentes como **"MITRE ATT&CK"**, se ha podido obtener información adicional que ha permitido completar la metodología diseñada. Se debe tener en cuenta que con esta nueva metodología se busca realizar una guía genérica basada en controles para ayudar y guiar a analistas a realizar sus ejercicios de análisis de ciberseguridad en Cloud, por lo que la implementación de diversos marcos de trabajo, normativas y vulnerabilidades previamente conocidas sobre los entornos Cloud, ha sido posible definir diversos aspectos en la nueva metodología diseñada, como la planificación y estructura de los ejercicios de análisis de seguridad.

Con el objetivo de poder realizar una comprobación de la efectividad tanto de la metodología diseñada como de las herramientas recomendadas, en este trabajo se ha mostrado los resultados obtenidos tras realizar una simulación de un análisis de seguridad en un entorno de **"Azure"**. Como se ha podido observar en los resultados obtenidos, todas las herramientas implementadas han resultado ser exitosas al completar los pasos propuestos en la metodología, pudiendo incluso contemplar apartados de fases no correspondientes a la fase de **Reconocimiento** planteada para la simulación.

En conclusión, mediante este proyecto ha sido posible diseñar una nueva metodología que incluye un total de **106** ejercicios de análisis para seguridad Cloud, junto con un total de **27** herramientas actuales que pueden ayudar en dicho proceso y un estudio exhaustivo de **28** componentes de cada proveedor, además de una comparativa entre todo ellos. Por otro lado, dado que los controles y herramientas propuestas para el análisis de seguridad han resultado ser altamente efectivos en la simulación, se puede concluir que la implementación de esta metodología, junto con la **Planificación de ejercicios de Análisis de Cloud** y **el Sistema de Puntuación de Vulnerabilidades (CVSS)** también propuestos en este trabajo, pueden ser de gran ayuda y contribución en los procesos y auditorias de análisis de seguridad en Cloud.

6.2 TRABAJOS FUTUROS

En este trabajo, solo ha sido posible realizar una primera simulación con el entorno de nube **"Azure"**, incluyendo únicamente la fase de **Reconomiento** de la ***"Cyber Kill Chain***" para evadir la posible modificación de parámetros confidenciales. Para trabajos futuros, no solo se recomienda trabajar con diversos analistas para implementar sus conocimientos y experiencia en esta metodología, sino además probar con entornos pertenecientes a los otros dos proveedores, **"Google Cloud Platform"** y **"Amazon Web Services"**, para analizar de esta manera las herramientas y vulnerabilidades analizadas en un mayor nivel de profundidad.

Por otro lado, se recomienda una actualización continua y periódica de esta nueva metodología. De esta manera, se podrán modificar las herramientas que se encuentren obsoletas debido a nuevas actualizaciones, además de incluir nuevos diseños que vayan surgiendo en el futuro. En otras palabras, para mantener un nivel de seguridad óptimo dentro de una infraestructura, es de vital importancia actualizar periódicamente todas las metodologías, análisis, normativas y marcos de trabajo que se estén implementando en los procesos análisis de seguridad, incluyendo a su vez las versiones de ***software*** y las herramientas con las que se trabajan.

Capítulo 7. BIBLIOGRAFÍA

[1] Oracle, «Oracle Cloud Computing,» 2022. [En línea]. Available: https://www.oracle.com/es/cloud/what-is-cloud-computing/.

[2] SalesForce, «SalesForce Cloud Compuring,» 2022. [En línea]. Available: https://www.salesforce.com/mx/cloud-computing/.

[3] Google Cloud, «Google Cloud,» Google, 2022. [En línea]. Available: https://cloud.google.com/?hl=es.

[4] Amazon Web Services, «Amazon Web Services (AWS),» Amazon, 2022. [En línea]. Available: https://aws.amazon.com/es/.

[5] Microsoft Azure, «Microsoft Azure Products,» Microsoft , 2022. [En línea]. Available: https://azure.microsoft.com/en-us/services/.

[6] Gartner, «Cloud Infrastructure and Platform Services Reviews and Ratings,» Gartner, Inc, 2022. [En línea]. Available: https://www.gartner.com/reviews/market/public-cloud-iaas.

[7] Acronis, «Comparación: los mejores servicios en la nube 2020,» 15 03 2019. [En línea]. Available: https://www.acronis.com/es-es/blog/posts/cloud-services-comparison/.

[8] European Central Bank, «What is TIBER-EU?,» European Central Bank | EUROSYSTEM, 2022. [En línea]. Available: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html#:~:text=TIBER%2DEU%20is%20the%20European,carrying%20out%20a%20controlled%20cyberattack..

[9] Lockheed Martin, «Cyber Kill Chain,» 2022. [En línea]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[10] ATT&CK, MITRE, «Getting Started with ATT&CK,» 10 2019. [En línea]. Available: https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf.

[11] Oasis, «Oasis CTI Documentation,» 2021. [En línea]. Available: https://oasis-open.github.io/cti-documentation/.

[12] MITRE ATT&CK, «Cloud Matrix,» 01 04 2022. [En línea]. Available: https://attack.mitre.org/matrices/enterprise/cloud/.

[13] NIST, «Vulnerability Metrics,» 2022. [En línea]. Available: https://nvd.nist.gov/vuln-metrics/cvss.

[14] Google Cloud, «Documentación de Identity and Access Management,» Google, 2022. [En línea]. Available: https://cloud.google.com/iam/docs.

[15] Google Cloud, «Términos Clave - Buckets,» Google, 2022. [En línea]. Available: https://cloud.google.com/storage/docs/key-terms#buckets.

[16] Google Cloud, «Documentación de Resource Manager,» Google, 2022. [En línea]. Available: https://cloud.google.com/resource-manager/docs.

[17] Google Cloud, «Documentación de Security Command Center,» Google, 2022. [En línea]. Available: https://cloud.google.com/security-command-center/docs.

[18] Google Cloud, «Descripción general de la CLI de gcloud,» Google, 15 06 2022. [En línea]. Available: https://cloud.google.com/sdk/gcloud.

[19] Pentest Book, «GCP Pentesting,» 02 2022. [En línea]. Available: https://pentestbook.six2dez.com/enumeration/cloud/gcp.

[20] carlospolop, «PurplePanda,» GitHub, 30 05 2022. [En línea]. Available: https://github.com/carlospolop/PurplePanda.

[21] DenizParlak, «Hayat,» GitHub, 07 01 2020. [En línea]. Available: https://github.com/DenizParlak/hayat.

[22] SpenGietz, «GCPBucketBrute,» GitHub, 3 06 2020. [En línea]. Available: https://github.com/RhinoSecurityLabs/GCPBucketBrute.

[23] marcin-kolda, «GCP IAM Collector,» GitHub, 23 04 2017. [En línea]. Available: https://github.com/marcin-kolda/gcp-iam-collector.

[24] C. Moberly, «GCP Firewall Enum,» GitLab, 2021. [En línea]. Available: https://gitlab.com/gitlab-com/gl-security/threatmanagement/redteam/redteam-public/gcp_firewall_enum.

[25] N7WEra, «Cloud Enum,» GitHub, 19 04 2022. [En línea]. Available: https://github.com/initstring/cloud_enum.

[26] alessandrogonzalez, «ScoutSuite,» GitHub, 10 03 2022. [En línea]. Available: https://github.com/nccgroup/ScoutSuite.

[27] L1ghtn1ng, «MailSniper,» GitHub, 28 01 2022. [En línea]. Available: https://github.com/dafthack/MailSniper.

[28] Amazon Web Services , «AWS IAM,» Amazon, 2022. [En línea]. Available: https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/introduction.html.

[29] Amazon Web Services, «Servicios de AWS que funcionan con IAM,» Amazon , 2022. [En línea]. Available: https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html.

[30] Amazon Web Services , «Amazon S3,» Amazon, 2022. [En línea]. Available: https://aws.amazon.com/es/s3/.

[31] Amazon Web Services , «What is Amazon S3?,» Amazon, 2022. [En línea]. Available: https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html.

[32] Amazon Web Services , «Amazon Elastic Compute Cloud,» Amazon, 2022. [En línea]. Available: https://aws.amazon.com/es/ec2/.

[33] Amazon Web Services , «Amazon Elastic Block Store,» Amazon, 2022. [En línea]. Available: https://aws.amazon.com/es/ebs/.

[34] Amazon Web Services, «Amazon Compute Cloud,» Amazon, 2022. [En línea]. Available: https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/ebs-volumes.html.

[35] Amazon Web Services , «Amazon cognito,» Amazon, 2022. [En línea]. Available: https://aws.amazon.com/es/cognito/.

[36] Amazon Web Services , «AWS Lambda,» Amazon, 2022. [En línea]. Available: https://aws.amazon.com/es/lambda/.

[37] Amazon Web Services, «Amazon CloudFront,» Amazon, 2022. [En línea]. Available: https://aws.amazon.com/es/cloudfront/.

[38] Amazon Web Services, «¿Qué es Amazon DynamoDB?,» Amazon, 2022. [En línea]. Available: https://docs.aws.amazon.com/es_es/amazondynamodb/latest/developerguide/Introduction.html.

[39] Amazon Web Services, «Uso de SSM Agent,» Amazon, 2022. [En línea]. Available: https://docs.aws.amazon.com/es_es/systems-manager/latest/userguide/ssm-agent.html.

[40] aph3rson, «AWS Consoler,» GitHub, 14 04 2020. [En línea]. Available: https://github.com/NetSPI/aws_consoler.

[41] andresriancho, «Enumerate IAM permissions,» GitHub, 27 11 2019. [En línea]. Available: https://github.com/andresriancho/enumerate-iam.

[42] test1212121212121212, «CloudCopy,» GitHub, 02 11 2019. [En línea]. Available: https://github.com/Static-Flow/CloudCopy.

[43] Hechtov, «SkyArk,» GitHub, 13 02 2022. [En línea]. Available: https://github.com/cyberark/SkyArk.

[44] rjulian, «Pacu,» GitHub, 17 03 2022. [En línea]. Available: https://github.com/RhinoSecurityLabs/pacu.

[45] R. Wood, «BucketFinder,» DigiNinja, [En línea]. Available: https://digi.ninja/projects/bucket_finder.php.

[46] E. Steringer, «PMapper,» GitHub, 04 02 2022. [En línea]. Available: https://github.com/nccgroup/PMapper.

[47] kmcquade, «Cloudsplaining,» GitHub, 13 02 2022. [En línea]. Available: https://github.com/salesforce/cloudsplaining.

[48] C. Gates, «weirdAAL,» GitHub, 20 05 2018. [En línea]. Available: https://github.com/carnal0wnage/weirdAAL/wiki.

[49] 0xdabbad00, «CloudMapper,» GitHub, 12 04 2022. [En línea]. Available: https://github.com/duo-labs/cloudmapper.

[50] dan-bishopfox, «Dufflebag,» GitHub, 05 02 2020. [En línea]. Available: https://github.com/BishopFox/dufflebag.

[51] Microsoft Azure, «Azure Active Directory,» Microsoft , 2022. [En línea]. Available: https://azure.microsoft.com/en-us/services/active-directory/#features.

[52] Microsoft Azure, «Microsoft Azure Resource Manager,» Microsoft , 13 06 2022. [En línea]. Available: https://docs.microsoft.com/es-es/azure/azure-resource-manager/management/overview.

[53] Microsoft Azure, «Introducción a Azure Portal,» Microsoft , 21 04 2022. [En línea]. Available: https://docs.microsoft.com/es-es/azure/azure-portal/azure-portal-overview#:~:text=Azure%20Portal%20es%20una%20consola,una%20interfaz%20gr%C3%A1fica%20de%20usuario..

[54] Microsoft Azure, «Información general de Microsoft Graph,» Microsoft , 16 06 2022. [En línea]. Available: https://docs.microsoft.com/es-es/graph/overview.

[55] Microsoft Azure, «Microsoft Azure Functions,» Microsoft, 30 05 2022. [En línea]. Available: https://docs.microsoft.com/es-es/azure/azure-functions/functions-overview.

[56] Microsoft Azure, «Azure Blob Storage,» Microsoft, 2022. [En línea]. Available: https://azure.microsoft.com/es-es/services/storage/blobs/#overview.

[57] Microsoft Azure, «Azure Automation Runbooks,» Microsoft , 02 05 2022. [En línea]. Available: https://docs.microsoft.com/es-es/azure/automation/automation-security-overview.

[58] Microsoft Azure, «Azure Key Vault,» Microsoft, 06 03 2021. [En línea]. Available: https://docs.microsoft.com/en-us/azure/key-vault/general/basic-concepts.

[59] Microsoft Azure, «Azure Intune,» Microsoft, 31 03 2022. [En línea]. Available: https://docs.microsoft.com/es-es/mem/intune/fundamentals/what-is-intune.

[60] Microsoft Azure, «Azure Active Directory Application Proxy,» Microsoft, 02 06 2022. [En línea]. Available: https://docs.microsoft.com/es-es/azure/active-directory/app-proxy/application-proxy.

[61] Microsoft Azure, «Azure AD Federation,» Microsoft , 02 06 2022. [En línea]. Available: https://docs.microsoft.com/es-es/azure/active-directory/hybrid/whatis-fed.

[62] D. Murphy, «What is an AdminSDHolder Attack and How to Defend Against it?,» Lepide, 17 06 2020. [En línea]. Available: https://www.lepide.com/blog/what-is-an-adminsdholder-attack-and-how-to-defend-against-it/#:~:text=Essentially%2C%20the%20AdminSDHolder%20is%20an,built%2Din%20privileged%20AD%20groups..

[63] Microsoft Azure, «Azure Active Directory PowerShell for Graph,» Microsoft, 29 04 2022. [En línea]. Available: https://docs.microsoft.com/en-us/powershell/azure/active-directory/overview?view=azureadps-2.0.

[64] Microsoft Azure, «Introducing the Azure Az PowerShell module,» Microsoft, 06 10 2022. [En línea]. Available: https://docs.microsoft.com/en-us/powershell/azure/new-azureps-module-az?view=azps-8.0.0.

[65] Microsoft Azure, «Azure Command-Line Interface (CLI) documentation,» Microsoft, 2022. [En línea]. Available: https://docs.microsoft.com/en-us/cli/azure/.

[66] dirkjanm, «ROADTools,» GitHub, 14 02 2022. [En línea]. Available: https://github.com/dirkjanm/ROADtools.

[67] legra-ms, «Stormspotter,» GitHub, 17 11 2021. [En línea]. Available: https://github.com/Azure/Stormspotter.

[68] rvazarkar, «BloodHound,» GitHub, 31 05 2022. [En línea]. Available: https://github.com/BloodHoundAD/BloodHound.

[69] kmackinley, «O365Creeper,» GitHub, 12 07 2016. [En línea]. Available: https://github.com/LMGsec/o365creeper.

[70] dafthack, «MSOLSpray,» GitHub, 16 03 2020. [En línea]. Available: https://github.com/dafthack/MSOLSpray.

[71] kfosaaen, «MicroBurst,» GitHub, 24 05 2022. [En línea]. Available: https://github.com/NetSPI/MicroBurst.

[72] sivlerhack, «Azucar,» GitHub, 23 01 2021. [En línea]. Available: https://github.com/nccgroup/azucar.

[73] Clarcat, «Comparativa: Amazon Web Services (AWS) vs. Microsoft Azure vs. Google Cloud Platform,» 12 08 2021. [En línea]. Available: https://www.clarcat.com/comparativa-aws-vs-microsoft-azure-vs-google-cloud-platform/.

[74] clarketm, «s3recon,» GitHub, 22 03 2020. [En línea]. Available: https://github.com/clarketm/s3recon.

[75] Oracle, «Oracle Cloud Computing,» 2022. [En línea]. Available: https://www.oracle.com/es/cloud/what-is-cloud-computing/.

ANEXO – OBJETIVOS DE DESARROLLO SOSTENIBLE (ODS) DE NACIONES UNIDAS

Desde el 25 de septiembre de 2015, los "**Objetivos de Desarrollo Sostenible (*ODS*)"** de **Naciones Unidas** han marcado profundamente el comportamiento de muchos sectores, sociedades, organizaciones e incluso gobiernos al intentar contribuir en estas metas contra la pobreza, desigualdad y/o contaminación, entre muchos otros temas que abarcan estos objetivos.

Con este trabajo de fin de master, también se quiere contribuir en esta ayuda en el desarrollo sostenible. En este caso, al diseñar esta metodología de seguridad, se han podido cumplir dos de los 17 objetivos globales planteados por Naciones Unidas:

- **Objetivo 8: Trabajo decente y Crecimiento económico** – Gracias a esta metodología, es posible implementar procesos de análisis de seguridad más eficientes, proporcionando a su vez una ayuda a aquellos analistas que no estén todavía familiarizados con alguno de los entornos. Además, al plantear trabajos futuros donde se realicen mejoras continuas sobre esta metodología, la efectividad de los análisis aumentará, por lo que las infraestructuras Cloud objetivo, ya sean propias o de terceros, serán más seguras.

- **Objetivo 9: Industria, Innovación e Infraestructura** – Al igual que el objetivo anterior, con esta metodología se busca tanto mejorar el proceso de análisis de seguridad como ayudar a analistas a realizas su trabajo de manera más sencilla y eficiente. Por otro lado, la mejora continua plantea además un estudio continuo sobre las nuevas tecnologías, metodologías o normativas que puedan influir de alguna manera los niveles de seguridad de una organización en la nube.

En conclusión, este trabajo plantea una nueva metodología de análisis que tiene como objetivo principal: estudiar las nuevas tecnologías de seguridad, ayudar a empresas y trabajadores a realizar sus análisis y, por último, mejorar los niveles de seguridad en cualquier entorno de nube.