Universitat Oberta de Catalunya

SECURIZANDO MICROSOFT365 Y ENTRA ID

SEGURIDAD INFORMÁTICA

Grado Ingeniería Informática

Tutor de TF

Jorge Miguel Moneo

Profesor Responsable Asignatura

Gerard Farràs Ballabriga

Pablo Martin Prados

Autor

Contenido

Este trabajo de fin de grado está dedicado a:

A mis dos hijas: Leire y Naia, perdonarme por el tiempo que os he robado de estar junto a vosotras jugando en el parque, mientras me he dedicado a conseguir mi meta. Pero habéis sido la gasolina necesaria para lograr un futuro mejor para vosotras.

A mi mujer Rocio, por su inagotable paciencia, amor, cariño y por haberme permitido dedicar parte de mi tiempo libre para que poco a poco pueda ir logrando mis objetivos, gracias por acompañarme en todos los momentos de mi vida.

También quiero dedicárselo a mis suegros Agustín y Ana, por su gran ayuda desde que empezó esta locura, siempre que os he necesitado habéis estado presentes, os habéis comportado como unos verdaderos padres, gracias de corazón.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Protegiendo Microsoft 365 y Entra ID*
Nombre del autor:	*Pablo Martin Prados*
Nombre del director/a:	*Jorge Miguel Moneo*
Nombre del PRA:	Gerard Farràs Ballabriga
Fecha de entrega (mm/aaaa):	*06/2024*
Titulación o programa:	Grado en Ingeniería Informática
Área del Trabajo Final:	*Seguridad Informática*
Idioma del trabajo:	*Castellano*
Palabras clave	*Office365, Azure, Entra ID, Seguridad, Azure Active Directory, Microsoft 365*

Resumen del Trabajo

La finalidad de este trabajo es estudiar el nuevo ciberespacio que nos provee el SaaS (*Software as a Service*) Microsoft 365 y Entra ID como proveedor de seguridad de las identidades digitales. Para ello se va a estudiar qué principales riesgos se generan por el hecho de usar este SaaS y cómo podemos mitigarlos.

Seguidamente, se van a plantear una serie de simulaciones de ataque no a la infraestructura de Azure sino a las malas configuraciones, identidades o políticas por defecto.

Por último, trataremos de analizar cómo podemos proteger la confidencialidad, integridad, disponibilidad y legalidad de los datos de las organizaciones, para lograrlo analizaremos cuales son las mejores medidas de bastionado y buenas prácticas que podemos aplicar para bajar el nivel de riesgo de las organizaciones que están y sus requisitos.

Abstract

The purpose of this paper is to study the new cyberspace provided by SaaS (Software as a Service) Microsoft 365 and Entra ID as a security provider for digital identities.

To do this, we will study what main risks are generated by using this SaaS and how we can mitigate them.

Next, a series of attack simulations will be proposed not on the Azure infrastructure but on bad configurations, identities, or default policies.

Finally, we will try to analyze how we can protect the confidentiality, integrity, availability, and legality of the organizations' data, to achieve this we will analyze what are the best bastion measures and good practices that we can apply to lower the risk level of the organizations that are and their requirements.

1. Introducción

En la era digital actual, la seguridad de la información se ha convertido en una prioridad para las organizaciones de todo el mundo. Con la creciente dependencia de las soluciones basadas en la nube, como Office 365, garantizar la protección de los datos y la identidad del usuario es fundamental. Office 365, una suite de productividad en la nube de Microsoft es utilizada por millones de empresas y particulares en todo el mundo. Aunque ofrece numerosas ventajas en términos de accesibilidad y colaboración, también presenta desafíos únicos en términos de seguridad.

Este trabajo se centrará en explorar las diversas estrategias y medidas que se pueden implementar para proteger Office 365 y la identidad del usuario. Abordaremos temas como la autenticación, los protocolos que usa, desde un punto de vista ofensivo y defensivos. El objetivo es proporcionar una guía completa y accesible para asegurar Office 365 y proteger la identidad del usuario en este entorno digital en constante evolución.

1.1 Contextualización y justificación del problema

Hace años las licencias del producto Microsoft Office se compraban mediante un único pago de la licencia y carecían de actualizaciones de características, solo valían para un único dispositivo. Tampoco incluía almacenamiento online extra y no sé incluía un servicio de soporte. Con la llegada de Microsoft Office 365 el modelo de licenciamiento pasaba a ser una suscripción mensual con las ventajas de que su precio permitía a particulares, pymes, pequeñas empresas y medianas empresas acceder de una manera más sencilla y fácil a toda la suite de Office365. Este cambio fue tan sumamente estratégico que Microsoft Office dejo de ser uno de los productos más pirateados en todo el mundo, que la mayoría de las empresas y particulares accedieron al modelo de suscripción.

Tras este cambio Microsoft, fue introduciendo cambios y servicios que estaban incluidos en la suscripción de la licencia, ya puede ser como Exchange Online, SharePoint y las empresas comenzaron a realizar una “hibridación” de su Active Directory para empezar a usar los servicios que te proporcionaban la licencia. Esta sincronización era el primer paso para dar acceso a los servicios, pero claro también es la que más riesgos lleva porque el contenedor del dato ya no era tu infraestructura, sino que Microsoft te proveía de un Azure Active Directory, o bien, como se llama ahora Entra ID.

Por tanto, esta democratización del acceso a las suscripciones de Microsoft Office 365 ha generado un nuevo contexto y ciberespacio donde existen nuevos riesgos y amenazas donde las organizaciones se enfrentan al reto de proteger los activos digitales. Office365 y sus servicios online se convierte en un objetivo atractivo para os cibercriminales que buscan explotar estas vulnerabilidades, configuraciones por defecto, contraseñas débiles...con el fin de acceder a los datos confidenciales, robo de credenciales o simplemente interrumpir procesos de negocio.

La importancia estratégica que Office365 y Azure Active Directory son componentes de la infraestructura tecnológica de muchas organizaciones. La seguridad de la identidad ya no se limita a las fronteras físicas que tiene una organización, sino que esta adopción de la nube implica una reevaluación de las estrategias de seguridad para proteger las identidades.

Dada esta complejidad técnica y las implicaciones de seguridad asociadas con el uso de Office365 y Azure Active Directory en entornos empresariales, este trabajo de investigación se justifica como una iniciativa para desarrollar estrategias y soluciones técnicas que aborden los desafíos específicos de la protección de la plataforma y gestión de la identidad, con el fin de fortificar la seguridad de los datos corporativos y garantizar la seguridad de los empleados en el acceso a la información.

Recientemente Microsoft renombro sus productos y actualizo ambos *brandings* pasándose a llamar Microsoft 365 para office y Entra ID.

1.2 Objetivos del trabajo

El principal objetivo de este trabajo de fin de grado es investigar y desarrollar estrategias efectivas para proteger la infraestructura de Office365 y Entra ID, mediante la identificación de riesgos y vulnerabilidades e implementaciones de medidas de seguridad efectivas con el fin de fortalecer la seguridad informática en entornos corporativos.

Con el fin de completar el objetivo principal, se proponen los siguientes objetivos operativos específicos:

- Identificar requisitos y procesos de implementación de Office365.
- Identificar los protocolos de autenticación de Office365 y Entra ID.
- Estudiar las herramientas y técnicas para el pentesting contra Office365.
- Conocer cómo crear persistencia en este entorno cloud.
- Realizar una serie de ataques controlados como externos contra Office365 para obtener información de un *tenant*.
- Securizar mediante buenas prácticas el *tenant* de Office365 y Entra ID.

Hay muchos aspectos para tener en cuenta, como los diferentes servicios que provee Office365, así como sus diferentes centros de administración y políticas, herramientas y tecnologías de las que se harán uso en este trabajo, por ello será necesario establecer un máximo nivel de detalle en el objetivo principal del proyecto. Es por ello qué se intentará establecer cierta universalidad a la hora de analizar el resto de los objetivos, con el único fin de asegurar acabar el trabajo según la planificación.

Por ejemplo, no se entrará en los centros de administración de aplicaciones Office365 tales como SharePoint, Teams, que tienen como objetivo proteger el dato y la identidad de los usuarios del *tenant* en base a configuraciones seguras, ya que esto no está dentro el objetivo principal. Aunque en algún momento del trabajo, si se enlazará ciertas parametrizaciones y esto relacionará de manera indirecta a estos aplicativos.

1.3 Enfoque y método seguido

Este proyecto está dirigido para toda aquella organización que usan Office365 y Azure Active Directory y no se han parado a analizar los riesgos que supone tener hibridada la organización con la puerta de entrada en Azure. Entendemos que el modelo de seguridad de los datos en Azure y Office 365 es un modelo compartido y que la seguridad de la infraestructura la pone el fabricante, pero la seguridad del dato es función de los clientes.

En la primera fase entrada se investigarán de manera teórica el concepto de identidad, protocolos, *killchain* y servicios de ataque contra Office365 y Azure Active Directory.

En la segunda fase de desarrollo, se analizará cómo podemos explotar y conseguir información de una organización como un externo de una organización ficticia.

Por último, en la fase de conclusión estaremos en la fase de implementación de cuáles son las mejores prácticas en cuanto a seguridad sin tener el mayor nivel de licenciamiento de Microsoft.

La metodología utilizada para la realización de este proyecto es en cascada. Tenemos un diseño secuencial y cada fase no empezará hasta que la anterior no haya finalizado. Aunque en algún caso si se pueden solapar por la propia índole de las tareas. Se han establecido puntos de control cada mes prácticamente con el director del proyecto.

1.4 Impacto en aspectos de sostenibilidad, ética y diversidad

En el mundo interconectado de hoy, la ciberseguridad se ha convertido en un pilar fundamental para garantizar la integridad, disponibilidad, confidencialidad y legalidad de la información. Sin embargo, al abordar la ciberseguridad, especialmente en entornos como Office 365 y Azure AD, es esencial considerar su impacto en aspectos de sostenibilidad, ética y diversidad.

1.4.1 Comportamiento ético y responsabilidad social.

En este apartado se ha obtenido un impacto positivo, puesto que ayuda a las organizaciones de todo el mundo a mantener uno de los pilares de la seguridad como la privacidad de los datos y el cumplimiento normativo, dotando a las empresas de la posibilidad de implementar unas políticas de privacidad con el fin de proteger el dato.

1.4.2 Sostenibilidad

En esta dimensión se ha obtenido un impacto positivo, puesto que se la reducción del consumo energético y la gestión de los recursos. Para ello Office365 y Azure permite a las empresas reducir su huella de carbono al optimizar el uso de los servidores y recursos informáticos de Microsoft. La migración de algunos servicios cloud como Exchange Online para el servicio del correo electrónico, almacenamiento personal como OneDrive, como el almacenamiento para la empresa SharePoint, sistemas de mensajería y comunicación Teams ayuda a contribuir la sostenibilidad ambiental y reducen el consumo energético asociado a los servidores on-premise. Aunque este consumo se traslada a la nube, la reutilización de recursos energéticos para miles de clientes y el compromiso de Microsoft obteniendo el *Gold LEED*, que es una certificación de los Centro de Procesamiento de Datos (CPD) que hace que sean más sostenibles y ecológicos. Esto es un claro beneficio medioambiental.

(Microsoft, 2017)

1.4.3 Diversidad, género y derechos humanos

En esta dimensión de diversidad, género y derechos humanos se obtiene un resultado positivo, puesto que la democratización de los precios y el acceso a la tecnología de Microsoft Office365 y Azure Active Directory hace que países poco desarrollados también puedan acceder a esta tecnología y dispongan de una experiencia positiva e inclusiva. Además de todo esto, Office365 incluye una serie de facilidades para que personas con diversas discapacidades puedan usar Office365 sin barreras. Algunos ejemplos de ello son lectores de pantalla o diversas funciones de accesibilidad.

1.5 Planificación del trabajo

ID	Tarea	Inicio	Fin
PEC1	**PLANIFICACION**		
1.1	Definir contexto y justificación	01/03/2024	10/03/2024
1.2	Definir objetivos	01/03/2024	10/03/2024
1.3	Definir el impacto en sostenibilidad, ético-social y diversidad	01/03/2024	10/03/2024
1.4	Definir la metodología utilizada	01/03/2024	10/03/2024
1.5	Elaborar el cronograma de hitos y tareas	01/03/2024	10/03/2024
1.6	Definir los contenidos del proyecto	01/03/2024	10/03/2024
1.7	**Entrega plan de trabajo**	**12/03/2024**	**12/03/2024**
	FASE ENTRADA		
PEC2	**INVESTIGACION**		
2.1	Conceptos básicos cloud	15/03/2024	17/03/2024
2.1.1	Responsabilidad compartida en el cloud	18/03/2024	19/03/2024
2.1.2	¿Qué es Microsoft 365?	19/03/2024	20/03/2024
2.1.3	¿Qué es Entra ID?	21/03/2024	23/03/2024
2.1.4	¿Cómo se relaciona Microsoft 365 y Entra ID?	24/03/2024	26/03/2024
2.1.5	¿Qué diferencia Azure Active Directory vs Active Directory?	27/03/2024	29/03/2024
2.1.6	¿Qué es Azure AD Domain Services?	28/03/2024	01/04/2024
2.2	¿Qué es el Cyber Kill Chain?	29/03/2024	30/03/2024
2.2.1	¿Qué es MITRE ATT&CK?	29/03/2024	30/03/2024
2.2.2	¿Cuál es el Kill Chain de Azure AD según MITRE?	29/03/2024	30/03/2024
2.2.3	¿Cuál es el Kill Chain de Office365 según MITRE?	29/03/2024	30/03/2024
2.2.4	Análisis Kill Chain Azure AD	30/03/2024	30/03/2024
2.2.5	Roles importantes de Kill Chain en Azure AD	01/04/2024	01/04/2024
2.2.6	¿Cuáles son los accesos administrativos de Azure AD?		
2.3	Trabajando el concepto de Identidad	01/04/2024	01/04/2024
2.3.1	Identidades: Pure Cloud	02/04/2024	02/04/2024
2.3.2	Identidades: Sincronizadas	03/04/2024	03/04/2024
2.3.3	Identidades: Dispositivos	04/04/2024	04/04/2024
2.3.4	Permisos de las identidades pure cloud o hibridas	05/04/2024	05/04/2024
2.3.5	Permisos en Aplicaciones y Aplicaciones Empresariales	06/04/2024	06/04/2024
2.4	Como atacar Azure AD	07/04/2024	07/04/2024
2.4.1	Robo de Access Token	07/04/2024	07/04/2024
2.4.2	Primary Refresh Token (PTR)	08/04/2024	08/04/2024
2.4.3	Pass The Token (PRT Cookie)	08/04/2024	08/04/2024
2.4.4	Enumeración de objetos con PowerZure	08/04/2024	08/04/2024
	Entrega plan de trabajo	**09/04/2024**	**09/04/2024**
	FASE DESARROLLO		
PEC3	**EXPLOTACIÓN**		
	Investigación herramientas para hacking		
3.1	Preparación del entorno	15/04/2024	15/04/2024
3.2	Enumeración de recursos con PowerZure	27/04/2024	28/04/2024
3.3	Robo de Acces Token: Device Auth Code	29/04/2024	01/05/2024

3.4	Acceso al PTR	02/05/2024	02/05/2024
3.5	Robo PTR Cookie	02/05/2024	02/05/2024
3.6	Conclusiones Post-explotación	04/05/2024	04/05/2024
	FASE CONCLUSIÓN		
PEC4	**IMPLEMENTACION BUENAS PRACTICAS**		
4.1	OSINT para enumerar	10/05/2024	15/05/2024
4.1.1	OSINT AADInternals Web	11/05/2024	11/05/2024
4.1.2	OSINT AADInternals Powershell	11/05/2024	11/05/2024
4.1.3	OSINT Microburst	12/05/2024	12/05/2024
4.1.4	OSINT Como obtener credenciales	13/05/2024	13/05/2024
4.1.5	Ejecutar una estrategia con datos obtenidos via OSINT	14/05/2024	14/05/2024
4.2	Herramientas para auditar AzureAD y Office365	15/05/2024	18/05/2024
4.2.1	PingCastle	15/05/2024	16/05/2024
4.2.2	PurpleKnight	16/05/2024	17/05/2024
4.2.3	Monkey365	17/05/2024	18/05/2024
4.2.4	Crowdstrike Reporting Tool Azure	18/05/2024	19/05/2024
4.2.5	Microsoft Azure AD Assesment	20/05/2024	21/05/2024
4.3	Implementar Conditional Access	22/05/2024	22/05/2024
4.3.1	¿Qué es el Conditional Access?	23/05/2024	23/05/2024
4.3.2	¿Qué debemos implementar con el Conditional Access?	23/05/2024	23/05/2024
4.4	Ver los eventos y log de Azure AD	24/05/2024	25/05/2024
4.4.1	¿Cómo crear casos de uso en Azure AD?	25/05/2024	26/05/2024
4.5	Medidas de seguridad Azure AD	27/05/2024	31/05/2024
	Entrega plan de trabajo	**11/06/2024**	**11/06/2024**
PEC5	**Presentación vídeo**	**12/06/2024**	**18/06/2024**
Preparación, ejecución y grabación del vídeo.			
PEC6	**Defensa TFG**	**24/06/2024**	**28/06/2024**
Finalmente se responderán las cuestiones planteadas por el profesorado.			

1.6 Cronograma del trabajo

Programación	1º Marzo	2º Marzo	3º Marzo	4º Marzo	1º Abril	2º Abril	3º Abril	4º Abril	1º Mayo	2º Mayo	3º Mayo	4º Mayo	1º Junio	2º Junio	3º Junio	4º Junio
Tareas																
Definir contexto y justificación																
Definir objetivos																
Definir el impacto en sostenibilidad, ético-social y diversidad																
Elaborar el cronograma de hitos y tareas																
Definir los contenidos del proyecto																
FASE ENTRADA																
Entrega PEC1																
Conceptos básicos cloud																
¿Qué es el Cyber Kill Chain?																
Modelo de datos compartidos																
¿Cuáles son los accesos administrativos de Azure AD?																
FASE DESARROLLO																
Entrega PEC2																
Investigación herramientas hacking																
Preparación del entorno																
Enumeración recursos																
Robo Access Token																
Acceso al PTR																
Robo PTR Cookie																
Conclusiones																
FASE CONCLUSION																
Entrega PEC3																
OSINT para enumerar																
Herramientas para auditar AzureAD y Office365																
Implementar Conditional Access																
Ver los eventos y log de Azure AD																
Medidas de seguridad Azure AD																
Repaso General TFG																
Entrega PEC4																
Grabación del vídeo PEC5																
Defensa TFG PEC6																

1.7 Estado del arte

Para la realización de este trabajo de fin de grado se ha buscado información general en Internet con el fin de recopilar cuales son las buenas prácticas para proteger una organización que tenga Office365 y Entra ID, que ataques se pueden realizar y como se puede obtener información como externo y cuáles son las mejores prácticas de seguridad frente a los cibercriminales.

Además, se hemos obtenido acceso a diversas guías de referencia y listado de normas que nos permite proteger Office 365 como Azure.

Las guías existentes son: CIS Azure, CIS Office365, y guías ENS 884, 885 [A, B, C, D], CISA Scuba Gear E3 o E5 y por último Azure AD Assesment.

Aunque en todas las fases de este proyecto trabajaremos sobre un *tenant* verdadero de una empresa ficticia, esto nos dará la visibilidad real de como las configuraciones por defecto que nos trae Microsoft, son mejorables en cuanto a seguridad se refiere.

Asimismo, se va a convocar reuniones con Microsoft MVP (*Most Value Professional*) relacionados con el mundo de la seguridad y en esas sesiones vamos a obtener numerosa información de cómo funciona Office365 y Azure AD, la cual se intentará explicar de la mejor manera en este trabajo.

Durante el desarrollo del este trabajo todas las informaciones consultadas están indicadas como cita en cada una de las investigaciones, análisis, implementación y anexos de referencias.

(Center for Internet Security®, 2024) (Center for Internet Security® , 2024) (Centro Criptologico Nacional, 2024) (Cybersecurity and Infrastructure Security Agency, 2023) (Microsoft, 2023)

2. Fase de investigación

2.1 Conceptos básicos Cloud

Primeramente, antes de pasar a analizar los riesgos en una infraestructura moderna de una compañía, hay que explicar el concepto de nube pública y sus características más destacables.

La nube o *cloud* en su forma más primitiva hace referencia a los servidores ubicados en proveedores externos que son accesibles a través de internet. Se trata de un modelo de aprovisionamiento de computación en la nube que permite a los clientes alquilar servidores virtuales, almacenar datos, aplicaciones de terceros y nos ofrece una flexibilidad y escalabilidad de los sistemas.

Esta nube pública trabaja sobre un modelo de computación que ya se viene usando en los entornos *on-premise* llamado virtualización. Este modelo permite la utilización de los servidores físicos para crear máquinas virtuales y con ello conseguir una eficiencia de los recursos, gestión más simple de las máquinas virtuales, una mayor rentabilidad al utilizar al máximo la capacidad del hardware y, por último, una mayor rapidez y agilidad en crear y desplegar máquinas virtuales.

Una vez explicado esto, entendemos que esta computación en la nube existe diferentes tipos de servicios e infraestructuras dependiendo de las necesidades de las organizaciones. Para ello es muy importante saber entender y diferenciar el modelo de *cloud computing* y los riesgos que conlleva cada tipo de implementación de nube. Los modelos de implementación de *cloud computing* son:

- **IaaS (*Infraestrucutre as a Service*) Infraestructura como servicio**
  Este tipo de servicio ofrece los recursos físicos de cómputo, almacenamiento y redes a demanda. Sería el concepto similar servidor local sin gestión del mantenimiento físico de los componentes.

- **PaaS (*Plataform as a Service*) Plataforma como servicio**
  Este tipo de plataforma además de incluir la parte de IaaS incluye la parte software ya preparado para usar por lo que los usuarios se puedes abstraer de la parte de la infraestructura. Algunos de estos casos son como marcos de desarrollo, herramientas que permiten realizar análisis de negocio...

- **SaaS (*Software as a Service*) Software como servicio**
  Este tipo de soluciones integrales dan la solución de manera completa a sus usuarios mediante Internet. Aquí el proveedor de servicios administra tanto el hardware como el software y el coste de iniciación del servicio es mínimo. Algunos ejemplos serían Office365, plataformas de comercio electrónico tipo Shopify que permite crear y administrar tiendas en línea...

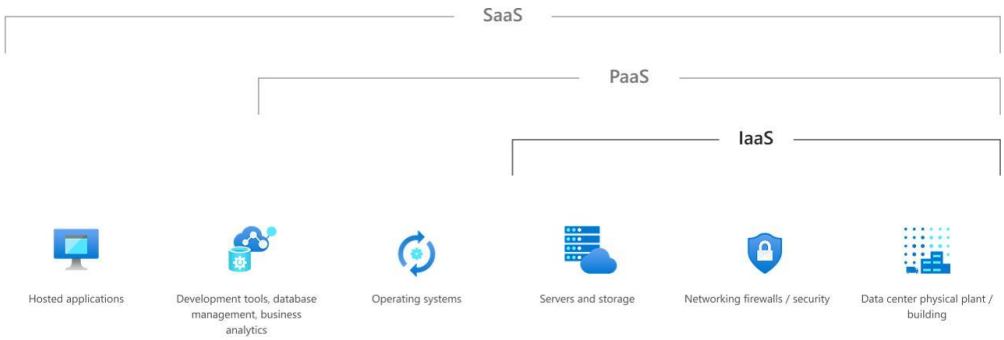


Ilustración 1: Diferencia entra SaaS, PaaS, IaaS (Microsoft, 2024)

2.1.1 Responsabilidad compartida en el cloud

Entendido este modelo de implementaciones es importante considerar los modelos de responsabilidad compartida que conlleva cada una de ellas, y que implicaciones de seguridad administra el proveedor y cuales administra la empresa. En cualquier caso, de implementación el propietario de la información y los datos, dispositivos que se conectan a ellos, cuentas y las identidades es tarea de la empresa que contrata el servicio. En esta ilustración se pude ver más claramente:

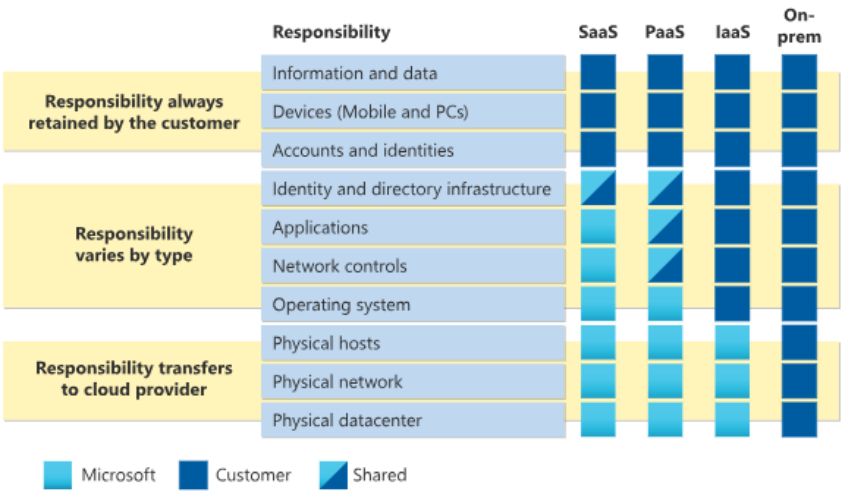


Ilustración 2: Tabla responsabilidad corporativa (Microsoft, 2023)

2.1.2 ¿Qué es Microsoft 365?

Microsoft 365 es un servicio de suscripción basado en el acceso varias aplicaciones de escritorio, así como servicios basados en la nube tipo SaaS. Esta suscripción a Microsoft 365 pretende aumentar la productividad, facilitar el trabajo colaborativo, proporcionando herramientas que permitan a los usuarios trabajar desde cualquier lugar con una conexión a Internet. Este el servicio de suscripción a Microsoft 365 siempre tendremos las versiones más actualizadas y recientes que Microsoft vaya liberando al mercado.

Por concluir, este aplicativo es multiplataforma y es accesible desde tanto en ordenadores, dispositivos móviles o directamente vía web.

2.1.3 ¿Qué es Entra ID?

Entra ID o Azure Active Directory es el servicio de administración de identidades y acceso basado en Azure. Permite que los empleados, usuarios, invitados externos puedan acceder a los recursos internos o externos de una organización. También ofrece herramientas para proteger las identidades y credenciales de los usuarios para cumplir con los requisitos del gobierno del dato.

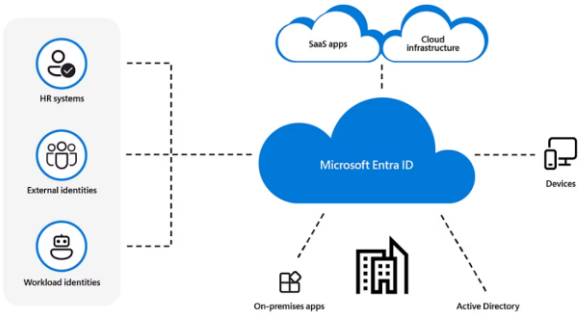


Ilustración 3: Diagrama Microsoft Entra ID (Microsoft, 2024)

2.1.4 ¿Cómo se relaciona Microsoft 365 y Entra ID?

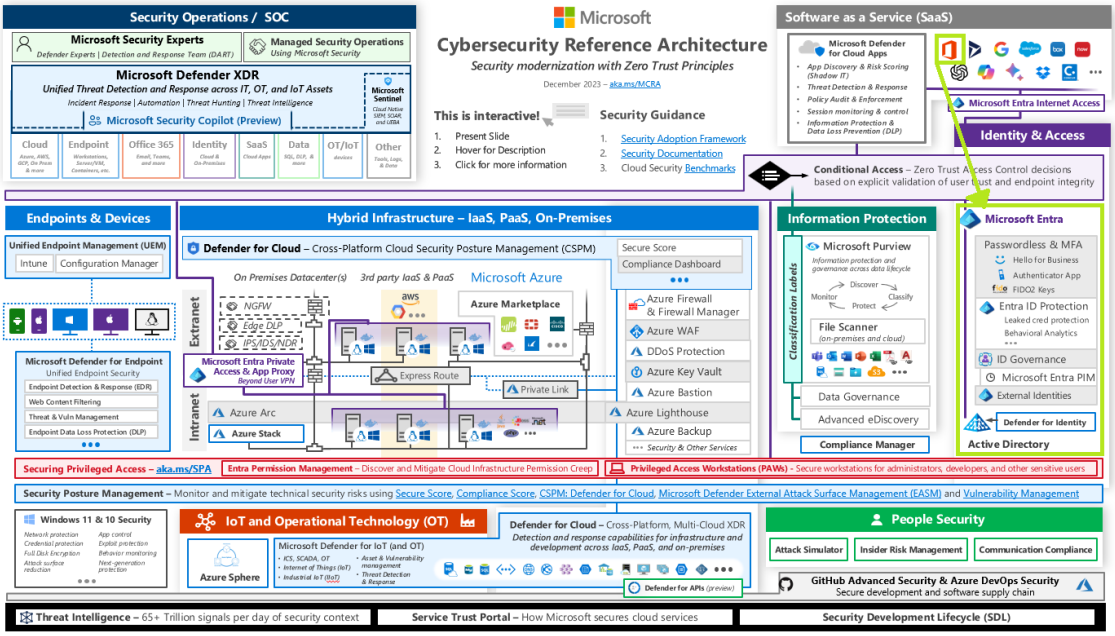


Ilustración 4: Microsoft Cybersecurity Reference Architectures (Microsoft, 2024)

Este diagrama, Microsoft describe como es la arquitectura a nivel de ciberseguridad y las capacidades de cada área.

Si empezamos a describir el diagrama desde el centro, vemos que la mayoría de las organizaciones operan en un entorno multiplataforma mediante servidores Windows y Linux en los CPD. La mayoría de estas arquitecturas comienzan la seguridad con un firewall perimetral para proteger los recursos desde la extranet/intranet.

Estos accesos se lograban mediante dispositivos y estos dispositivos eran gestionados bajo políticas de grupo del Active Directory y la seguridad de las cuentas también dependían de Active Directory.

Las empresas empezaron a adoptar la nube como SaaS y la primera aplicación suele ser Office 365 para el correo electrónico o a veces G Suite. Esta tendencia continua hoy con la adopción de la IA generativa como ChatGPT, Microsoft Copilot o Google Bard. Esto genera una necesidad de control de acceso más allá del firewall perimetral, se requiere utilizar identidades seguras en la nube. Esta identidad juega un papel muy importante en las estrategias de control de acceso.

Muchas organizaciones ya han implementado las identidades únicas e inicios de sesión único a todo su patrimonio empresarial con Entra ID durante la implementación de Office365, puesto que este conecta al sistema de identidad existente a través de Active Directory.

Con toda esta arquitectura podemos decir que Entra Id es el proveedor de seguridad de Office365, aunque no se limite a solo esto, tal y como hemos visto.

2.1.5 ¿Qué diferencia Azure Active Directory versus Active Directory?

Ambos dos sistemas son soluciones de administración de identidades de Microsoft, pero tienen propósitos diferentes.

Active Directory (AD) es un rol del sistema operativo Microsoft Windows Server es usado para administrar usuarios, ordenadores y recursos basados en red. Fue lanzado al mercado en Windows 2000 y desde entonces ha sido el producto *core* de identidad como solución de la mayoría de las empresas. AD almacena información de usuarios, cuentas de equipo, datos de autenticación y autorización y por último políticas de seguridad (*Group Policy)* que permite a los administradores crear determinadas configuraciones a los usuarios de un dominio.

Azure AD provee las mismas características que AD, sin embargo, está diseñado para trabajar en el cloud y con aplicaciones y servicios que no requieren un controlador de dominio. A menudo, Azure AD provee de inicio de sesión único (*Single Sign On*) a los usuarios de un *tenant*, funcionando como un proveedor de identidades (*Identity Provider)* para aplicaciones SaaS.

Esto nos lleva a comparar los conceptos ya conocidos del AD, como se diferencian y trabajan en Azure AD:

Active Directory	Azure Active Directory
LDAP	REST API's
NTLM / Kerberos	OAuth/SAML/OpenID...
Structured Directory (OU Tree)	Flat Structure
GPO's	No GPO's
Super fine-tuned acces controls	Predefined Roles
Domain/Forest	Tenant
Trusts	Guests

Expliquemos sus diferencias para entrar más en el concepto de Azure Active Directory comparándolo con Active Directory.

Cuando por ejemplo en Azure, le decimos que queremos crear un usuario, o por ejemplo iniciar una máquina virtual, lo que vamos a utilizar es la capa 7 del modelo OSI, mediante HTTP, no sobre LDAP. Si explorásemos mediante WireShark estas peticiones no podríamos ver tráfico LDAP ni tampoco SMB, solo veríamos tráfico TLS, porque la API se encuentra cifrada.

En Active Directory cuando se produce una autenticación normalmente veríamos tráfico NTLM o Kerberos, aunque existe algún protocolo más, pero estos serían los principales. En cambio, en Azure AD los protocolos son OAuth, SAML, OpenID...

Mientras que en AD teníamos una estructura arbolada donde podíamos organizar todas las OU (Unidades Organizativas) por ejemplo, para segregar departamentos, sedes, equipos de trabajo, entre otros. Mientras que, en Azure Active Directory tenemos una estructura plana.

En AD teníamos políticas de grupo (GPO) pero en Azure AD no existen como tal. Si existen herramientas como Microsoft Intune para crear políticas, pero estas no están contempladas en Azure AD, sino que se licencia de forma separada.

En AD teníamos controles de acceso a los objetos, por ejemplo, teníamos una carpeta a la que podríamos indicarle los permisos si se podía leer, escribir o eliminar..., y en cambio ahora en Azure AD tenemos roles con permisos.

En AD teníamos un bosque con un/varios dominios en cambio, en Azure Active Directory disponemos de uno o varios *tenant*.

En AD teníamos relaciones de confianza entre varios dominios que permitían el acceso desde otros dominios y en Azure AD tenemos invitados.

En relación con la seguridad de ambos sistemas, podemos decir que el protocolo de autenticación Kerberos, el cual está basado en los usuarios, servicios o aplicaciones y un *Key Distribution Center (*KDC*)* se puede atacar de distintos modos para obtener la información de usuarios, suplantarlos o robar las credenciales de un controlador del dominio. Existen numerosos ataques al protocolo dentro de un AD, tales como *Over The Hash, Pass the Key, Pass The Ticket, Golden o Silver Ticket, Kerberoastaing, ASPEPRoast*. (Tarlogic, 2019)

El hecho de tener un AD implica tener una gran superficie de ataque, que requiere tener un gran control de detección, tener políticas de seguridad que permitan evadir estos ataques y mitigarlos. Es importante ser consciente de que los cibercriminales van a

buscar el AD de la organización para conseguir sus objetivos. La detección de estos ataques no es algo sencillo, requiere un nivel de madurez y conocimiento de la infraestructura y *Threat Intelligence* muy alto para auditar o trazar los movimientos que se producen en el AD. Muchas empresas se centran en fortificar el perímetro de la red y olvidan la fortificación de esa pieza clave. Podemos concluir que un AD puede estar bien configurado y no presentar vulnerabilidades en materia de seguridad y aun así se puede hackear con éxito.

2.1.6 ¿Qué es Azure AD Domain Services?

Por terminar de contextualizar las opciones de Azure AD, en los anteriores puntos hemos hablado de que era Office 365, Azure AD y por último nos faltaría entender que significa Azure AD Domain Services y volver a compararlo con los otros dos para entender sus características.

Azure Active Directory Domain Services en pocas palabras es el controlador del dominio en la nube. Es un SaaS que nos provee Microsoft para poder usar un DC (*Domain Controller*) en la nube, esto lo que nos permite es usar los protocolos de autenticación que teníamos en Active Directory como NTLM, Kerberos, pero en entorno cloud. Domain Services se integra con Azure AD y esto permite a los usuarios iniciar sesión en los servicios y aplicaciones que estaban conectadas al AD. Además, también nos permite usar las características generales como las políticas de grupo o unir al dominio.

Es decir, esto no es un IaaS como podría entenderse de tener un controlador de dominio en una infraestructura pública al cual vamos a promocionarlo, vamos a tener que administrarlo, mantenerlo, instalar sus parches de seguridad.

Si comparásemos las características técnicas de las tres tecnologías nos quedaría un cuadro como este:

Features	Active Directory	Azure AD	Azure AD Domain Services
Extensible Schema	✓	✗	✗
Group Policies	✓	✗	✓
HA	User Created	✓	✓
Kerberos, LDAP, NTLM Support	✓	✗	✓ (Ldap Read Only)
OAuth, SAML, OpenID Support	✗	✓	✗
Dedicated Servers	✓	✗	✗
Cloud Based	IaaS Only	✓	✓
Domin/Enterprise Admin	✓	✗	✗
Domain/Forest Trust	✓	✗	✗

Sintetizando en el caso de una suscripción de Office365 automáticamente tendremos Azure Active Directory. Si nosotros hibridamos o sincronizamos nuestro Active Directory contra Azure Active Directory, es decir, los objetos que tenemos en nuestro entorno *on-*

premise se volcará una copia en Azure AD. En ninguno de estos casos Microsoft nos va a poner un DC en la nube ya que es otro servicio aparte y tiene un coste independiente.

2.2 ¿Qué es el *Cyber Kill Chain*?

En la sección anterior, hemos examinado en detalle los sistemas de Active Directory y Azure Active Directory. Estos sistemas son componentes esenciales en la infraestructura de TI de una organización, proporcionando una plataforma para la gestión de identidades y accesos. Permiten a las organizaciones controlar de manera efectiva quién tiene acceso a qué recursos dentro de la red, y cómo se otorga y se revoca ese acceso.

Sin embargo, como con cualquier sistema tecnológico, Active Directory y Azure Active Directory no están exentos de vulnerabilidades. Los actores malintencionados pueden buscar explotar estas vulnerabilidades para obtener acceso no autorizado a los recursos de la red. Esto puede incluir intentos de obtener credenciales de usuario, explotar debilidades en la configuración del sistema, o aprovechar las vulnerabilidades de seguridad en el software que se utiliza para administrar estos sistemas.

Es en este contexto de potenciales amenazas y vulnerabilidades donde el concepto de la Cyber Kill Chain se vuelve relevante.

El modelo de *Cyber Kill Chain* (cadena de exterminio de la ciberseguridad) fue desarrollado por los analistas Lockheed Martin Corporation (Lockheed Martin Corporation, 2024), fabricante de la industria aeroespacial y militar, derivado de esta industria basado en los modelos de ataques militares fue trasladado al entorno digital, con el fin de comprender, detectar, y prevenir cualquier tipo de ciberamenaza.

Este modelo está dividido en varias etapas y cada una relacionada con un tipo de actividad en la fase del ciberataque. Cada fase de la etapa del ataque es una oportunidad para detectar, reconocer y defenderte del ataque. Las etapas del ataque son:

Ilustración 5:Etapas Cyber Kill Chain (Incibe, 2020)

La primera fase de **reconocimiento** principalmente trata de reunir información sobre el objetivo. Aquí se emplean una amplia variedad de herramientas y técnicas para recopilar

información algunos de ellos son: motores de búsqueda, archivos web, servicios públicos en la nube, registros de dominio, rastreo de red, escaneo de puertos...

En la fase de **preparación** una vez que los ciberdelincuentes hayan reunido suficiente información, se prepara el medio para lanzar el ataque para iniciar la intrusión. Lo lógico es que los atacantes usen todos los puntos de entrada y que obtengan la menor resistencia. Algunos ejemplos de estas técnicas son: Ingeniería social, ataques *man in the middle*, atacantes internos (*insiders),* errores de configuración del sistema...

En la etapa de **distribución** se lanza el ciberataque que se haya preparado, por tanto, aquí entra en juego las medidas que tenga una empresa para detectarlo.

En la **explotación** dependiendo del ataque elegido, estaríamos hablando ante un equipo, un servidor, una aplicación... que se encuentra infectado mediante una bomba lógica. Estas bombas lógicas, muchas veces incluyen una capa de ofuscación para ser invisibles ante cualquier defensa de la empresa.

Durante la **instalación,** si los delincuentes ven fácil realizar ataques en el futuro y controlar la empresa, intentaran instalar un *backdoor*, una puerta trasera, para poder moverse dentro y fuera de la red sin correr riesgo de detección.

En la penúltima fase **Comando y control**, también más conocida como C&C *(Command and Control)* una vez instalada las puertas traseras y con acceso, control y ejecución de los sistemas, los ciberdelincuentes llevaran a cabo cualquier acción maliciosa desde tomar el control del AD, tomar capturas de pantalla para llevarse información confidencial, ver cómo es la red de la empresa...

La última etapa, **acciones sobre los objetivos,** los delincuentes podrán realizar un cifrado de los datos, pedir un rescate económico para recuperar la documentación de la empresa, filtrar sus datos al exterior con el fin de extorsionar y lograr su beneficio, que nos denuncien ante los organismos competentes AEPD (Agencia Española Protección de Datos) por vulnerar los datos de nuestros clientes, proveedores, extorsionar y vigilar a la persona que tiene el poder en la empresa para realizar el pago del rescate...

En definitiva, acabamos de ver las fases de un ciberataque y ver como se produce paso a paso.

2.2.1 ¿Qué es MITRE ATT&CK?

MITRE ATT&CK es una organización sin ánimo de lucre que nace en 1958 en el MIT (*Massachussett Institute of Technology*) financiada por el gobierno de los Estados Unidos. Su objetivo es proveer al gobierno de los Estados Unidos pasos que se usan con tecnología avanzada en asuntos federales. Fueron los primeros en registrar ".org" como sitio para un dominio (https://www.mitre.org).

En 1999 crearon los CVE (*Common Vulnerabilities and Exposures*), que es el sistema para identificar vulnerabilidades en el mundo de la ciberseguridad, enumerando en una escala el nivel de amenaza que supone. (MITRE, 2024)

En 2015 lanzan MITRE ATT&CK es una base de conocimiento que contiene tácticas, técnicas que se producen en los ciberataques. Con el objetivo de desarrollar una ciberseguridad efectiva a cualquier organización sin ningún tipo de coste.

Estos comportamientos de los atacantes se organizan en una serie de tácticas o técnicas según unos determinados objetivos. El enfoque es entender como un delincuente prepara, lanza o ejecuta un ciberataque.

Estos comportamientos se relacionan con CIT (*Cyber Threat Intelligence*) para reconocer a grupos conocidos de delincuentes de APT (*Advanced Persistent Threat*).

Las tácticas describen las infinitas técnicas que un delincuente puede utilizar en diferentes métodos, con diferentes herramientas de pentesting para hackear un sistema.

Según esto realizan dos tipos de análisis muy completos y los ponen a disposición de todo el mundo. Los análisis de comportamientos de ataques y los análisis de la taxonomía de ataque, más conocidos por *Kill Chain*.

Por eso, MITRE nos va a proveer una fuente de información legítima en cuanto a las Kill Chain, usada por casi todos los fabricantes del mundo a nivel de ciberseguridad, en los cuales vamos a poder correlacionar las etapas de los ataques que se puedan producir en una organización.

(MITRE, 2024) (Checkpoint, 2015)

2.2.2 ¿Cuál es el *Kill Chain* de Azure AD según MITRE?

Ilustración 6: KillChain Azure AD (MITRE, 2024)

Tras estudiar cuales son las fases de un ataque a las plataformas de Office365 y Azure AD, podemos determinar que en ambos casos el **acceso inicial** pasa por conseguir unas cuentas válidas. Seguidamente vamos a realizar una **ejecución de comandos** para ver cuáles son las puertas para entrar a Azure AD. Vamos a intentar que métodos tenemos para crear **persistencia.** Una vez creada la persistencia del usuario, vamos a ver la identidad que hemos conseguido vamos a intentar hacerle un usuario con más poderes dentro de la organización **escalando privilegios**. Intentaremos **evadir las defensas** para no ser detectados. Los últimos pasos serán buscar **credenciales válidas** y **descubrir** todo lo que tenemos en Azure AD y para finalmente realizar el **impacto**.

2.2.3 ¿Cuál es el *Kill Chain* de Office365 según MITRE?

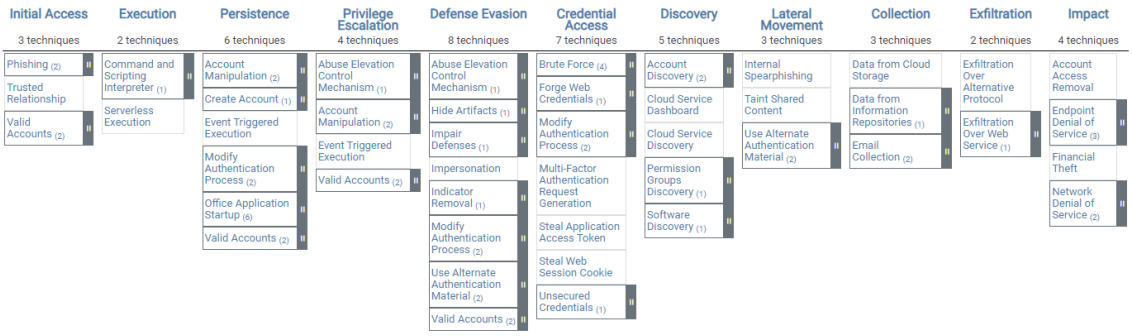


Ilustración 7: KillChain Office 365 (MITRE, 2024)

Según MITRE el **acceso inicial** a Office365 se produce mediante unas cuentas válidas, relaciones de confianza o mediante un phishing. Pero realmente si nos paramos a pensar, cuando un usuario se válida en alguna aplicación de Office365 el proveedor de identidades no es Office365 sino Azure AD. Por tanto, cuando entremos a Office365 estaremos también entrando a Azure AD. **Ejecutaremos** comandos para obtener información del *tenant* y crearemos diferentes **persistencias** dentro de Office365. **Evadiremos las defensas** que existan, seguiremos **buscando credenciales** y accesos, usando técnicas de **descubrimiento**, intentaremos **movernos lateralmente** con el fin de **conseguir** el mayor número de información confidencial y **exfiltrarla** para lanzar el ataque final y generar un **impacto**.

2.2.4 Análisis Kill Chain Azure AD

Finalmente podemos resumir el Kill Chain de Azure AD en roles que existen en Azure AD y cómo se comportan. Por lo general, los atacantes suelen ser externos a la organización y quieren obtener un rol de invitado, ser un usuario interno o mejor un usuario con privilegios de administración del *tenant*. Es decir, lo primero que buscan es una cuenta válida como, no tienen contraseña, necesitan ese acceso inicial tal y como hemos visto en MITRE. Una vez ya tenemos credenciales válidas el objetivo es hacerse con el Global Admin de Azure AD. También existen ataques desde el entorno *on-premise* hacia Azure AD y viceversa.

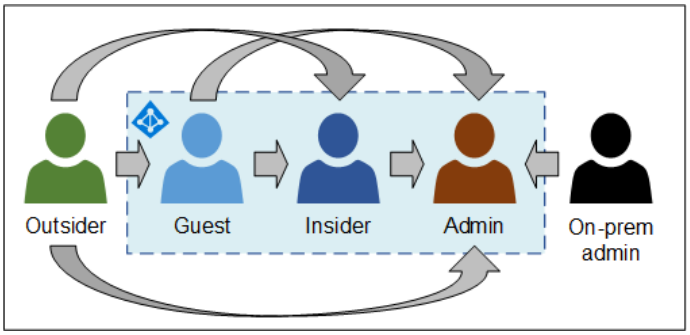


Ilustración 8: KillChain Azure AD (Syynimaa, 2020)

2.2.5 Roles importantes de Kill Chain en Azure AD

Tal y como hemos visto en el punto anterior, lo que los atacantes van a intentar ser Global Admin para hacerse con el control del *tenant*. Por tanto, es necesario explicar de manera breve según la imagen anterior que roles y como forman parte del ciberataque:

Un *outsider* (externo) nos referimos aquel usuario que no tiene acceso al *tenant*. Tenemos que saber que los externos pueden extraer información usando las APIs y lanzando consultas DNS.

Un invitado se refiere a un usuario externo que ha sido invitado a nuestro *tenant*. Estos usuarios tienen accesos restringidos a nuestro Azure AD, pero pueden conseguir numerosa información usando APIs de Microsoft.

Por el usuario, a la identidad que esta alojada en el *tenant* con acceso normal.

Admin, se refiere al Global Administrator, el rol más poderoso dentro de Azure AD. Este tiene acceso ilimitado a todas las funcionalidades de Azure AD y Office 365.

(Microsoft, 2024)

2.2.6 ¿Cuáles son los accesos administrativos de Azure AD?

Si pensamos en atacar o defender Azure AD necesariamente tenemos que saber quiénes son los Global Admin, tal y como hemos visto en el punto anterior. Otro punto importante a conocer es saber cuáles son los accesos administrativos a Azure AD, es decir, cuáles son las puertas de entrada a mi *tenant*.

Por todos es conocido que para acceder a Azure AD el acceso al portal se realiza vía web accediendo a https://portal.azure.com

Pero existen más accesos administrativos, que son los siguientes:

- ✓ Azure Cli
- ✓ AZ Powershell
- ✓ MS Graph API
- ✓ Azure API
- ✓ Internal API
- ✓ vía web
- ✓ Portal.azure.com

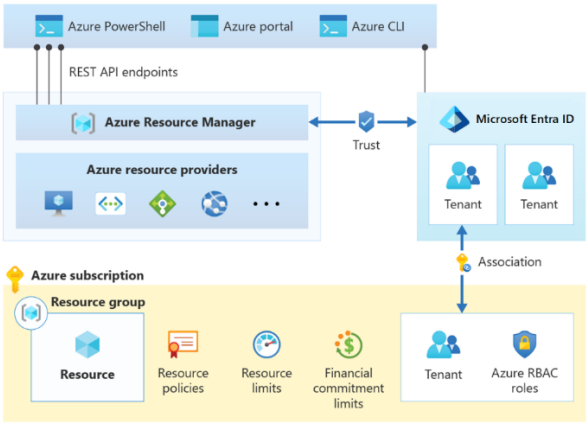


Ilustración 9: Accesos Administrativos Azure (Microsoft, 2024)

2.3 Trabajando sobre el concepto de identidad en Azure AD

Cuando nos referimos a identidad dentro del entorno Azure AD, nos estamos refiriendo a sus objetos. Como hemos visto en puntos anteriores dentro de Azure AD podemos albergar usuarios, dispositivos y aplicaciones. Asimismo, el propio *tenant* de Azure AD también forma parte de una identidad, la cual representa la organización. El objetivo de la identidad es responder a la pregunta de "¿quiénes somos?" cuando nos validamos.

Estas identidades se pueden asociar con una prueba de identidad, es decir una autenticación. Para ello podemos ver en una tabla las maneras en las que podemos autenticar a usuarios, dispositivos o aplicaciones:

Autenticación	Usuario	Dispositivo	Cliente
Username + Password	✓		✓
Authenticator	✓		
FIDO2	✓		
Kerberos Ticket (Seamless SSO)	✓		
SAML Token	✓		
Primary Refresh Token (PRT)	✓	✓	
Refresh Token	✓	✓	
Windows Hello Business	✓	✓	
Certificate	✓	✓	✓

(Microsoft, 2023)

2.3.1 Identidades: Pure Cloud

Hoy en día existen distintos tipos de identidades en función de su origen, es decir, cuando se crean dentro de nuestro *tenant*. Entender el origen y su función, es sumamente importante para entender cómo se pueden atacar y/o proteger. Por un lado, existen las Identidades del tipo ***Pure Cloud*** en Azure con esto nos estamos refiriendo a que son objetos puramente cloud y su identidad está basada en Azure Active Directory.

- **Usuarios**
- **Grupos**
- ***Service Principal:*** es un concepto de entidad que actúan como una aplicación
- **Aplicaciones**: Cuando registramos una aplicación que es personalizada, esto genera un objeto del tipo Aplicación, por ende, esta aplicación necesita un contexto de seguridad para saber quién puede hacer uso de ella y quién no, en determinadas circunstancias. Es decir, cuando registremos una aplicación se crear el objeto App y se asociará la aplicación a un Service Principal.
- **Aplicaciones empresariales**: Cuando instalas una aplicación de terceros, en este caso no alojamos la aplicación en el *tenant* de Azure AD, sino que esta alojada en otro *tenant*.

2.3.2 Identidades: Sincronizadas (hibridas)

En el otro lado existen las identidades híbridas sincronizadas. El concepto de hibrido sincronizado es que integramos nuestro Active Directory contra Azure AD. El objetivo de realizar esta sincronización es disponer de una identidad única, en ambos dos entornos, tanto Azure AD como AD, proporcionar *Single Sing On* a los usuarios de la organización para acceder a las aplicaciones locales, servicios en la nube, aplicaciones empresariales y por supuesto Microsoft, por último, la sincronización de las contraseñas.

Se puede definir que se sincroniza desde el AD y que objetos en función desde las necesidades.

Para ello usamos el *software* de Azure AD Connect o Entra Connect. Este software se conectará al AD con un usuario que tenga suficientes permisos para leer las propiedades del AD y replicará nuestra base de datos contra Azure AD.

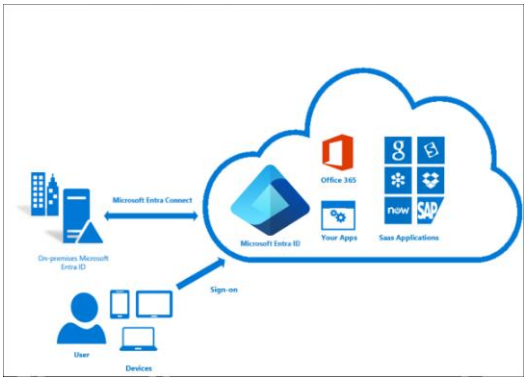


Ilustración 10: Arquitectura Hibrida AD (Microsoft, 2023)

En cuanto a la sincronización de las contraseñas puede trabajar de dos maneras muy distintas *Password Hash Sync*, *Pass-Through* y *Federation Authentication*.

- **Password Hash Sync (PHS)**: Sincroniza los hashes de las contraseñas. Es decir, vuelve a realizar el hash las contraseñas de nuestro AD, para sincronizarlas. Por explicar este punto un poco más, un Active Directory guarda las contraseñas de todos nuestros usuarios en formato NTLM en el controlador del dominio. Esto no es lo que sincroniza, sino que Azure AD Connect, vuelve hacer el *hash* del *hash* la contraseña para replicarlo y hacerlo más seguro.
- **Pass-Through (PTA):** En este caso cuando desde Azure AD se requiera validar a un usuario, la petición bajará a nuestro AD y será el encargado de validar la petición.
- **Federation Authentication**: Los servicios de federación permite usar AD como proveedor de identidad para las autenticaciones en la nueve. Mediante AD FS, se redirigen las peticiones al AD.

2.3.3 Identidad: Dispositivos

Los dispositivos es otro tipo de identidad que forma parte de un *tenant*. El hecho de trabajar con dispositivos en cuanto a ciber seguridad se refiere, es la mejor palanca de

cambio para fortificar una organización haciendo uso del acceso condicional. Para hacer uso del acceso condicional es necesario trabajar con la identidad dispositivos y se hace necesario entender que tipos existen y como se relacionan. El acceso condicional nos permite elaborar políticas de seguridad con una granularidad enorme.

Existen tres tipos de unir a Azure AD un dispositivo, que son *registered, joined o hybrid*. El primero de ellos sería el más sencillo en el que podemos interactuar con el dispositivo exigiéndole cierto nivel de políticas. El segundo *joined* es un dispositivo *full cloud* y forma parte de manera completa de Azure AD. *Hybrid* nos indica que el dispositivo esta unido al AD.

Además, estos dispositivos nos permiten saber desde donde podremos aplicarle las políticas de seguridad que sean definidas y de qué manera van a hacer el proceso de autenticación, si bien contra Azure AD o contra AD. Para esto podemos ver una pequeña tabla resumen:

Join Type	Qué tipos pueden ser	Credenciales	Administración Dispositivos
Registered	-PC Personal -Dispositivos Móviles (personales/empresa) -Cloud-only	-Microsoft Account -Azure AD -Local Account	-Intune
Joined	- PC Empresarial - Cloud-only	-Azure AD	-Intune
Hybrid	- PC Empresarial - Cloud & On-prem	-Active Directory	-Intune -SCCM

2.3.4 Permisos de las identidades pure cloud o hibridas

El control de los permisos de los recursos en la nube es crucial para cualquier entidad que utilice servicios en la nube. El sistema de control de acceso basado en roles de Azure (Azure RBAC) facilita la gestión de los privilegios de acceso a los recursos de Azure, determinando quién puede acceder a ellos, qué acciones pueden realizar y a qué áreas tienen permiso de acceso.

Una entidad de seguridad es un objeto que representa a un usuario, un grupo, una entidad de servicio o una identidad administrada que solicita acceso a recursos de Azure y se le puede asignar un rol a cualquiera de estos.

Ilustración 11: Entidades de seguridad (Microsoft, 2024)

2.3.5 Permisos en Aplicaciones y Aplicaciones Empresariales

Los permisos en Azure AD se dividen en dos tipos: delegados y de Aplicación.

Los permisos delegados son utilizados por las aplicaciones que tienen una interfaz de usuario y están firmadas por un usuario. Es decir, son los permisos que va a tener una aplicación en función del usuario que lo ejecuta.

Los permisos de aplicación son utilizados por aplicaciones que funcionan como servicios en segundo plano sin la necesidad de la interacción del usuario.

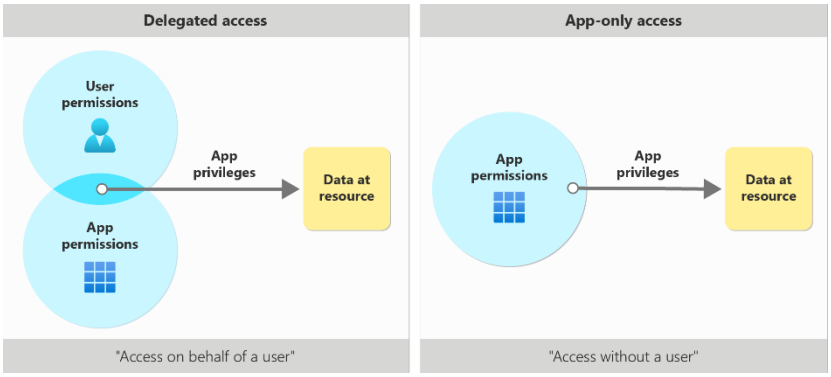


Ilustración 12: Permisos Aplicación (Microsoft, 2023)

2.4 Como atacar Azure AD

Aunque como ya hemos visto en MITRE todos los accesos iniciales pasan por tener una cuenta válida, vamos a ver cómo podemos realizar ataques contra el AD y sin tener que robar credenciales. Hemos podido obtener una visión muy global de cómo trabajan las identidades, protocolos que se usan en Azure AD, tipos de identidades, como se sincronizan las contraseñas desde el AD, etc.

2.4.1 Robo de Access Token: *Device Auth Code*

Desde este punto es necesario explicar técnicamente como se hablan las identidades con Azure AD para saber cómo realizar los ataques comprometiendo las cuentas de las identidades.

Para saber cómo los dispositivos *registered* y *joined* se unen los dispositivos a Azure AD este es el proceso que se produce:

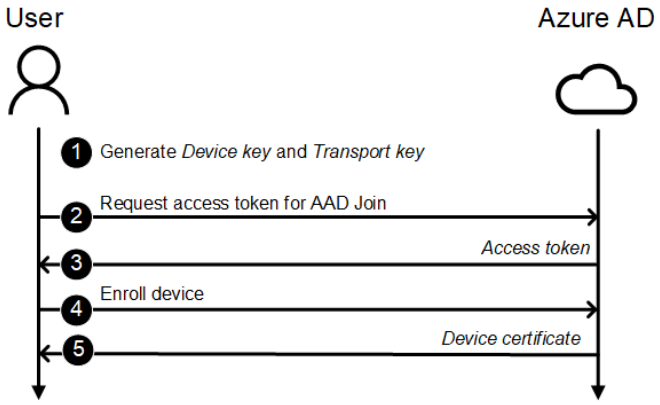


Ilustración 13: Azure AD join (Syynimaa, 2021)

El dispositivo genera una clave de dispositivo y transporte y solicita a Azure AD un *access token*, tras esto, el dispositivo se une y Azure AD le entrega un certificado.

Si hablamos del entorno hibrido, simplemente tenemos que meter un paso más que sería la sincronización entre AD y Azure AD:

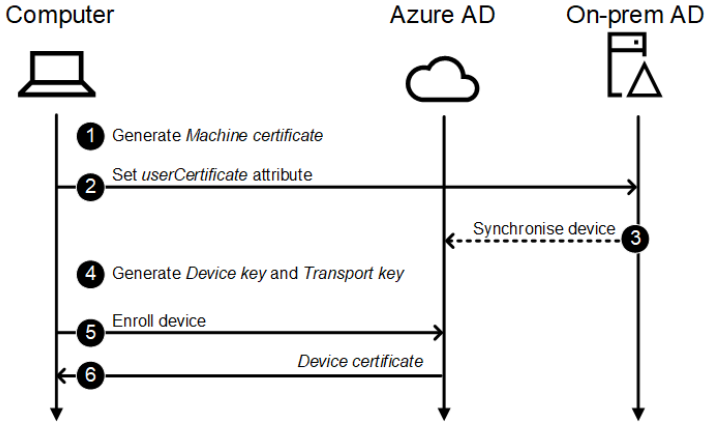


Ilustración 14: OnPrem Active Directory join (Syynimaa, 2021)

Aquí es necesario entender y explicar que son los *access tokens*, estos permiten llamar de forma de segura a las API Web. Estas usan tokens de acceso para hacer la autenticación y autorización. Además, su formato es JSON Web Token.

Por tanto, si alguien es capaz de robar este access token, ya nos estaríamos validando contra Azure AD como un dispositivo.

2.4.2 Primary Refresh Token (PRT)

El PRT podríamos compararlo con un TGS (Ticket Grant Service) Kerberos. El TGS forma parte del proceso de autenticación en Kerberos y es un ticket válido para conectarte contra cualquier servicio donde tienes acceso. El diagrama sería el siguiente:

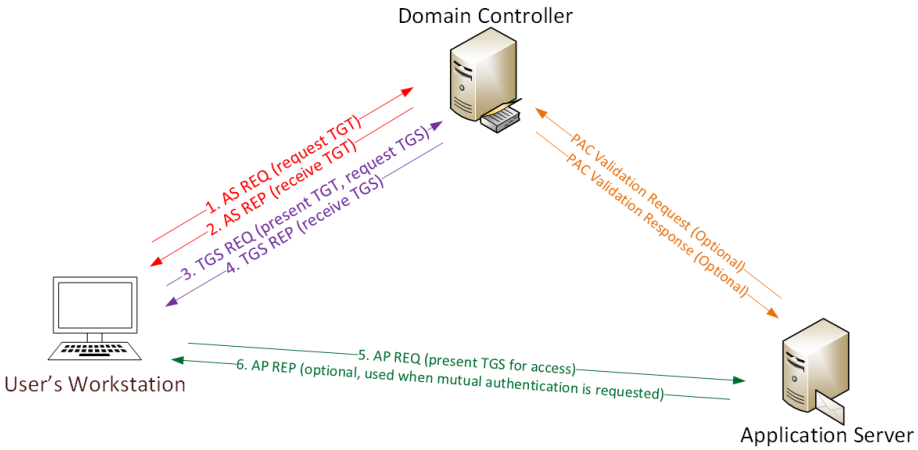


Ilustración 15: Kerberos Proceso Autentiación (ADSecurity, 2015)

En Azure AD, el PRT es un token que nos permite iniciar sesión solo una vez en un dispositivo y luego iniciar sesión de manera automática. Es un token JsonWebToken. El escenario habitual son los ordenadores unidos a la empresa de cualquier manera *(registered, joined o hybrid)*. Contiene la identidad del dispositivo y la clave de sesión. Tiene una duración de 14 días. Se puede saber si tiene un token si usamos el comando dsregcmd /status:

```
Microsoft Windows [Versión 10.0.20348.1129]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>dsregcmd /status

+----------------------------------------------------------------------+
| Device State                                                         |
+----------------------------------------------------------------------+

             AzureAdJoined : NO
          EnterpriseJoined : NO
              DomainJoined : YES
                DomainName : LABORATORIO
               Device Name : dc2022.laboratorio.local
```

Ilustración 16: Comando dsregcmd

Por lo cual si alguien se hiciese con este token podría validarse con una identidad contra Azure AD.

2.4.3 Pass The Token (PRT Cookie)

Este proceso va a tratar de conseguir desde un token la cookie que nos va a permitir robar la sesión web del navegador para validarnos contra Azure AD. Previamente es necesario haber comprometido un ordenador sin que ninguna de las medidas de detección haya sido efectiva.

El diagrama del PRT es el siguiente:

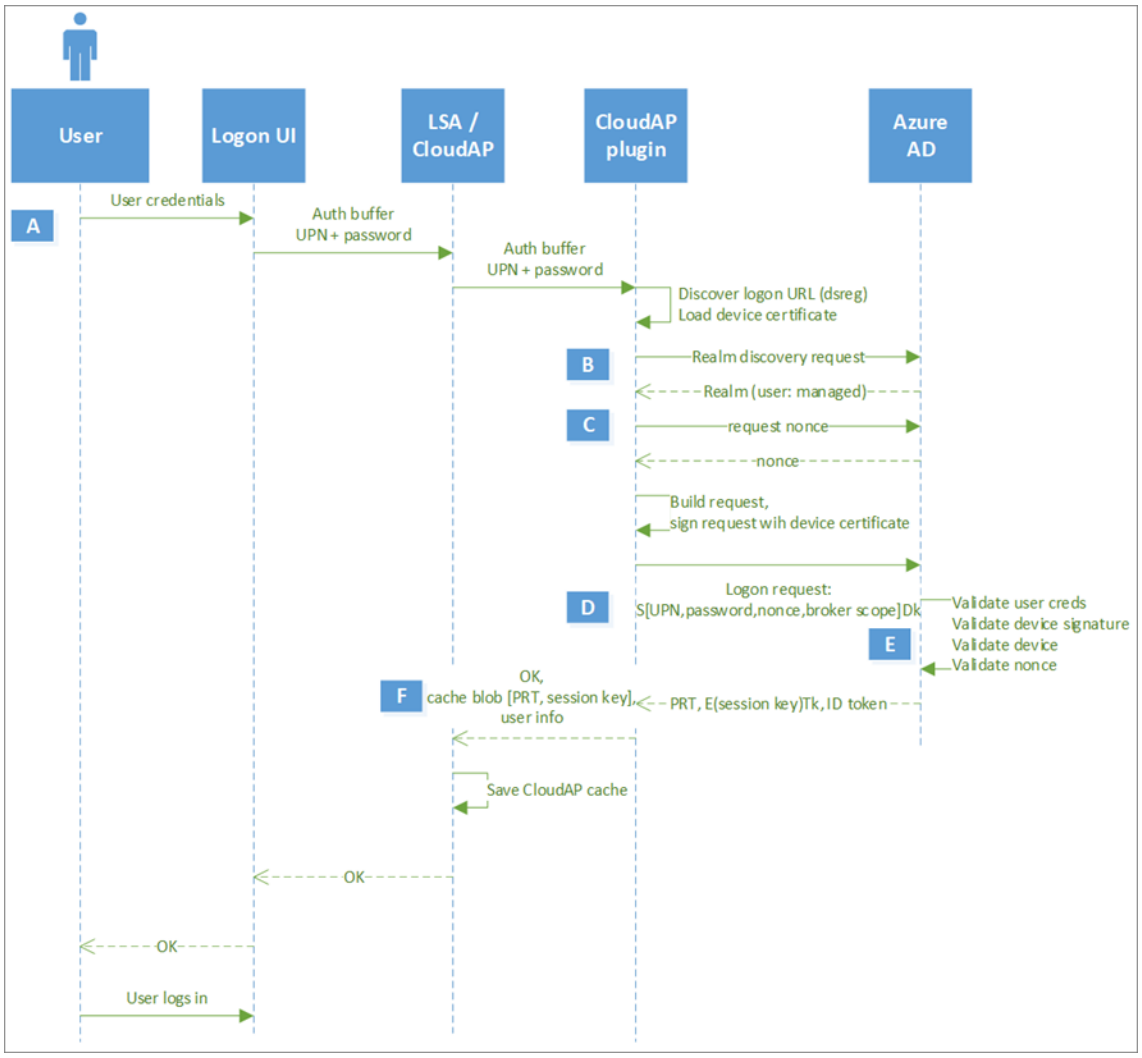


Ilustración 17: PRT Cookie Diagrama (Microsoft, 2024)

El objetivo del hackeo es como el navegador se autentica contra Azure AD y solicita el PRT. Cuando se realiza el get-token, queremos en el intercambio de claves PRT de sesión, obtener el PRT Cookie, y con este PRT Cookie podremos hacer login en cualquier aplicación via web.

2.4.4 Enumeración de objetos con PowerZure

Una de las fases que vimos como parte de un ciberataque es el reconocimiento. Si este punto nos lo llevamos a Azure AD, el reconocer objetos nos va a permitir tener más datos sobre la organización, ¿qué usuario tengo?, ¿quién soy?, ¿qué roles tengo?, ¿existe una política de MFA?, ¿quiénes son los usuarios Global Admin?, ¿qué seguridad, productos existen dentro del *tenant*?, todo este tipo de preguntas nos llevarán en función de las respuestas a realizar una escalada de privilegios.

Algunas de estas funciones nos las va a ofrecer herramientas como PowerZure:

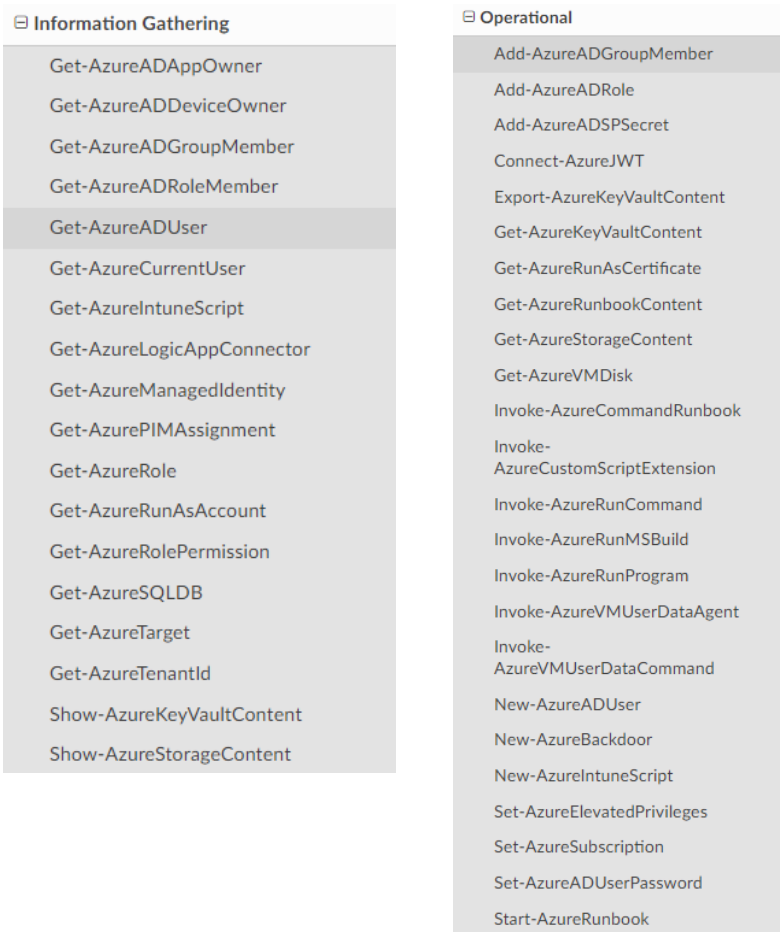


Ilustración 18: Opciones PowerZure (Powerzure, 2024)

3.Explotación

3.1 Preparación del entorno

Para realizar todos estos ejercicios de explotación de Office365 y AzureAD, se ha creado un entorno de cero para que no aparezcan datos confidenciales. Para ello hemos solicitado una licencia de prueba de Microsoft 365 Empresa Premium, desde este enlace: https://www.microsoft.com/es-es/microsoft-365/business/compare-all-microsoft-365-business-products

Una vez seguido el proceso de alta y añadir datos de pago, nos ha generado un *tenant* al finalizar este proceso vamos a obtener el Global Admin:

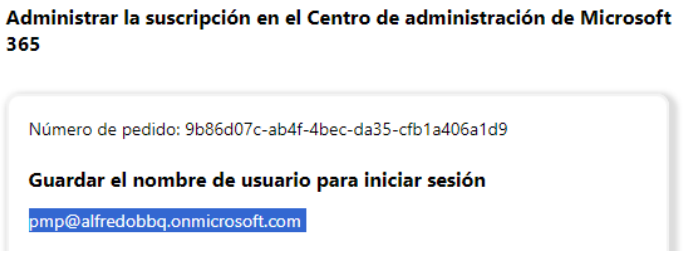


Ilustración 19: Global Admin Tenant Pruebas

Tras entrar en el *tenant*, vamos a generar un usuario sin privilegios para hacer las diferentes simulaciones de ataques:

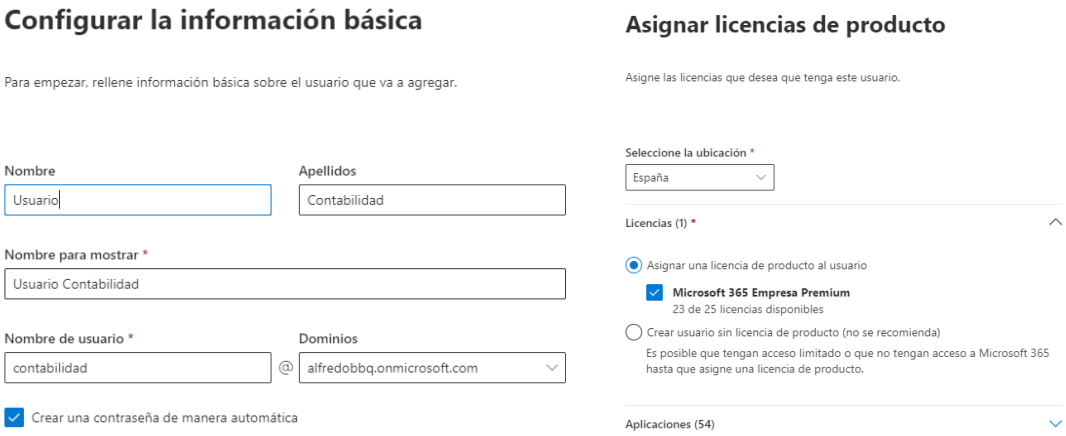


Ilustración 20: Proceso Creación Usuario O365

Lo siguiente para tener en cuenta es que vamos a simular ejercicios ofensivos contra Azure y Office365 con los que vamos a poder hacer tácticas, técnicas y procedimientos (TTP) para ver que nos devuelve con un usuario sin privilegios. Como podremos ver en estos ejercicios ejecutaremos ataques en los que partimos de dos puntos iniciales. El primero de ellos es acceso al *tenant* con unas credenciales válidas. El otro punto de partida es no tener credenciales válidas y entrar al *tenant*.

En este trabajo no se centra en explicar los métodos para encontrar credenciales válidas, en este sentido, existe una parta de la ciberseguridad que se encarga de ello. Por enumerar, algunos ejemplos, podemos encontrar credenciales válidas comprándolas en la *Darkweb*, desde foros de hacking, o porque hemos conseguido comprometer un ordenador y hemos extraído las credenciales del Lsass.exe o del *Credential Manager* o del navegador...

Como se verá luego, tampoco está centrado este trabajo en elaborar ejercicios de ingeniería social para sacar correos que suplanten o que hagan picar a los usuarios. Este trabajo está centrado en ver como hackear la parte técnica y no la parte humana.

3.2 Enumeración de recursos con PowerZure

Para este primer ataque ofensivo vamos, vamos a suponer que ya tenemos unas credenciales válidas en el *tenant*. Esto puede ser bien porque tengamos un usuario legítimo, o porque seamos unos invitados al *tenant*, o simplemente que nos hayamos hecho con el control de un dispositivo con credenciales satisfactorias.

En este primer enfoque vamos a intentar con un usuario sin roles, nos conectarnos a Azure via PowerShell e intentaremos enumerar y descubrir aplicaciones, registradas, usuarios grupos... Para ello primero usaremos la herramienta de PowerZure que podremos descargarla desde GitHub su librería.

(Hausknecht, 2020)

Primero instalamos la Liberia de Azure sobre PowerShell:

```
PowerShell 7.4.2
PS C:\Users\PABLO> Install-Module -Name Az

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): a
```

Ilustración 21: Configuración Powershell Az

Nos conectamos a la cuenta usando Connect-AzAccount

```
PS C:\Users\PABLO> Connect-AzAccount

Account                                SubscriptionName TenantId                             Environment
-------                                ---------------- --------                             -----------
contabilidad@alfredobbq.onmicrosoft.com                 a22bc87f-c762-4fd1-a438-7bc743d99593 AzureCloud


PS C:\Users\PABLO>
```

Ilustración 22: Conexión contra Azure

Importamos la herramienta de PowerZure, para que nos permita usar sus *cmdlet*. Dependiendo de la política de PowerShell que este configurada a veces es necesario modificarla, aquí si fue necesario:

```
PS C:\Users\PABLO\Desktop\PowerZure-master\PowerZure-master> Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope Cu
rrentUser
PS C:\Users\PABLO\Desktop\PowerZure-master\PowerZure-master> Import-Module .\PowerZure.psm1

Advertencia de seguridad
Ejecute solo los scripts de confianza. Los scripts procedentes de Internet pueden ser útiles, pero este script podría
dañar su equipo. Si confía en este script, use el cmdlet Unblock-File para permitir que se ejecute sin este mensaje de
advertencia. ¿Desea ejecutar C:\Users\PABLO\Desktop\PowerZure-master\PowerZure-master\PowerZure.psm1?
[N] No ejecutar  [Z] Ejecutar una vez  [U] Suspender  [?] Ayuda (el valor predeterminado es "N"): S
```

Ilustración 23: Importación cmdlet Powerzure

Ya podemos empezar a ver que hay bajo el *tenant* con los distintos comandos que nos trae PowerZure:

```
PS C:\Users\PABLO\Desktop\PowerZure-master\PowerZure-master> Get-AzureCurrentUser


TenantID               : a22bc87f-c762-4fd1-a438-7bc743d99593
Username               : contabilidad@alfredobbq.onmicrosoft.com
ObjectId               : 8ae29813-cc25-4879-8774-c32af624af9b
AADRoles               : {}
AADGroups              : {All Users, ALFREDOS}
AzureRoles             : {}
Active Subscription    :
Available Subscriptions : {}
```

Ilustración 24: Ejemplo Enumeración 1

Vamos a ver quién tiene el rol de Global Admin:

```
PS C:\Users\PABLO\Desktop\PowerZure-master\PowerZure-master> Get-AzureRoleMember -Role 'Global Administrator'

@odata.type           userPrincipalName             id
-----------           -----------------             --
#microsoft.graph.user pmp@alfredobbq.onmicrosoft.com 9efcf238-9c6a-4621-92a3-e45b2e6bc278
```

Ilustración 25: Ejemplo Enumeración 2

Existen bastantes opciones que podemos invocar con esta opción para ver que se puede hacer:

```
PS C:\Users\PABLO\Desktop\PowerZure-master\PowerZure-master> Invoke-PowerZure -h

                        PowerZure Version 2.2

                             List of Functions

-----------------Info Gathering -------------

Get-AzureAppOwner ----------------- Returns all owners of all Applications in Entra
Get-AzureDeviceOwner ------------- Lists the owners of devices in Entra. This will only show devices that have an owner.
Get-AzureGroupMember ------------- Gathers a specific group or all groups in Entra and lists their members.
Get-AzureRoleMember -------------- Lists the members of a given role in Entra
Get-AzureUser -------------------- Gathers info on a specific user or all users including their groups and roles in Azur
e & AzureAD
Get-AzureCurrentUser ------------- Returns the current logged in user name and any owned objects
Get-AzureIntuneScript ------------ Lists available Intune scripts in Azure Intune
Get-AzureLogicAppConnector ------- Lists the connector APIs in Azure
Get-AzureManagedIdentity ----------- Gets a list of all Managed Identities and their roles.
Get-AzurePIMAssignment ------------ Gathers the Privileged Identity Management assignments. Currently, only AzureRM rol
es are returned.
Get-AzureRole -------------------- Gets the members of an Azure RBAC role.
Get-AzureRunAsAccount ------------ Finds any RunAs accounts being used by an Automation Account
Get-AzureRolePermission ---------- Finds all roles with a certain permission
Get-AzureSQLDB ------------------- Lists the available SQL Databases on a server
Get-AzureTarget ------------------ Compares your role to your scope to determine what you have access to
Get-AzureTenantId ---------------- Returns the ID of a tenant belonging to a domain
Show-AzureKeyVaultContent -------- Lists all available content in a key vault
Show-AzureStorageContent --------- Lists all available storage containers, shares, and tables
```

Ilustración 26: Ejemplos de Enumeración PowerZure

Pensemos que esta herramienta se está ejecutando contra un *tenant* que no tiene nada más que dos usuarios, sin suscripciones, ni aplicaciones, ni grupos, ni roles...por tanto, la enumeración de todas estas funcionalidades queda muy restringida a estos resultados.

Pero la realidad es que cuando estamos dentro de un proceso de auditoría la enumeración es un proceso que nos va a mostrar mucha información valiosa. Si, por ejemplo, tuviésemos aplicaciones registradas podríamos ver los *owner*s de las aplicaciones, que miembros tienen un rol dentro del AAD, listar scripts que están en Intune puede arrojar información confidencial de la empresa, listar las APIs que están publicadas, listar contenedores, los secretos del *KeyVault*.

Aunque existen varias medidas para mitigar esta medida de enumeración la más efectiva es usar Acceso Condicional bloqueando Windows Azure Service Management Api para que ningún usuario sin privilegios pueda de este modo, ni Azure Cli, ni Ms Graph...

Más adelante veremos qué es el acceso condicional y como configurar políticas, desde la parte defensiva.

3.3 Robo de Access Token: Device Auth Code

En esta ocasión el ejercicio ofensivo va a consistir en enviar un correo suplantando alguna identidad con el fin de que registre un dispositivo. Al registrar este dispositivo, capturaremos el token de acceso, lo cual nos permitirá evadir el MFA y estar dentro de la sesión del usuario. Para ello vamos a utilizar las herramientas del Dr. Azure que se llaman AADInternals.

(Syynimaa, 2018)

Permitimos en Powershell la ejecución e importamos los *cmdlet*:

```
PS C:\Users\PABLO\Desktop\AADInternals-master\AADInternals-master> Set-ExecutionPolicy -ExecutionPolicy Unrestricted
PS C:\Users\PABLO\Desktop\AADInternals-master\AADInternals-master> Import-Module .\AADInternals.psd1
PS C:\Users\PABLO\Desktop\AADInternals-master\AADInternals-master>
```

Ilustración 27: Configuración PowerShell

Lo siguiente es modificar el fichero killchain.ps1 para añadir las opciones de envío de correo, con el servidor que vaya a enviar este email falso. En nuestro caso como vamos a usar Hotmail, es necesario configurar el puerto y STARTLS.

```
Send-MailMessage -from martin.prados@hotmail.com -to pmp@alfredobbq.onmicrosoft.com -Subject $Subject -Body $message -SmtpServer $SMTPServer -BodyAsHtml -Encoding utf8 -Port
587 -UseSSL -Credential $cred
```

Ilustración 28: Configuracion Killchain.ps1

Lanzamos el email *phishing* con el siguiente cmdlet:

```
PS C:\Users\PABLO\Desktop\AADInternals-master\AADInternals-master>  Invoke-AADIntPhishing -Recipients pmp@alfredobbq.onm
icrosoft.com -Sender bbqcontabilidad@hotmail.com -SMTPServer outlook.office365.com -SMTPCredentials $cred -SaveToCache

cmdlet Invoke-AADIntPhishing en la posición 1 de la canalización de comandos
Proporcione valores para los parámetros siguientes:
Subject: aa
Code: GL63YLWUT
Mail sent to: pmp@alfredobbq.onmicrosoft.com
....
```

Ilustración 29: Envío email AADinternals

Se recibe el email:

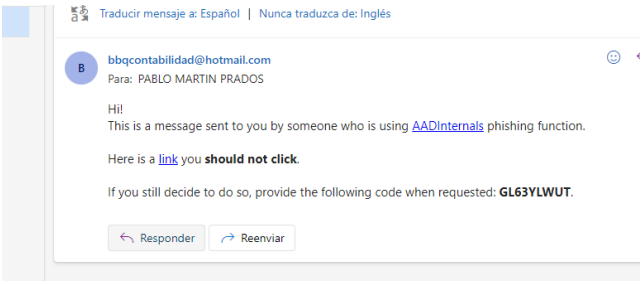


Ilustración 30: Email Phishing

Entramos en el enlace y podemos ver que la web es legítima de Microsoft, y directamente podemos introducir el código que nos enviaron:

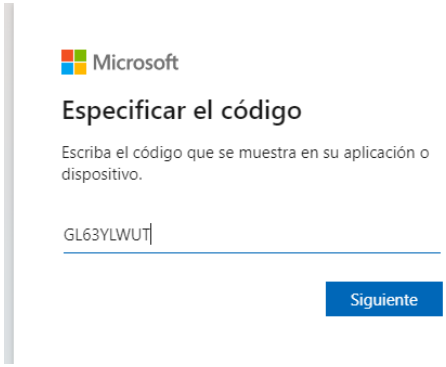


Ilustración 31:Login de Office365

Escogemos la cuenta y si nos fijamos, Microsoft identifica el país desde donde se ha lanzado la petición maliciosa:

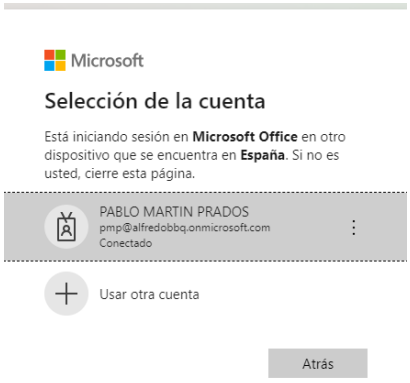


Ilustración 32: Selección de Cuenta Office365

Y finalmente se completa el proceso de alta del "dispositivo":

Ilustración 33: Finalización proceso login Office365

En Powershell lo que podemos evidenciar es que hemos robado este token, que tiene una duración de 14 días:

```
PS C:\Users\PABLO\Desktop\AADInternals-master\AADInternals-master>  Invoke-
icrosoft.com -Sender bbqcontabilidad@hotmail.com -SMTPServer outlook.office

cmdlet Invoke-AADIntPhishing en la posición 1 de la canalización de comando
Proporcione valores para los parámetros siguientes:
Subject: AA
Code: C2NNS4FV4
Mail sent to: pmp@alfredobbq.onmicrosoft.com
...
Received access token for pmp@alfredobbq.onmicrosoft.com
PS C:\Users\PABLO\Desktop\AADInternals-master\AADInternals-master>
```

Ilustración 34: Powershell AADinternals - Token recibido

Y, por ejemplo, para comprobar que como hemos robado un usuario que tiene privilegios, hemos creado un nuevo usuario:

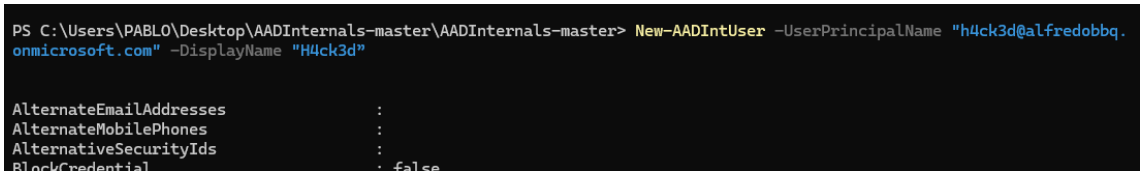


Ilustración 35: Ejemplo de ataque con token recibido

Volvemos a revisar desde el centro de administración de Office365 y comprobamos que se ha creado de manera satisfactoria:

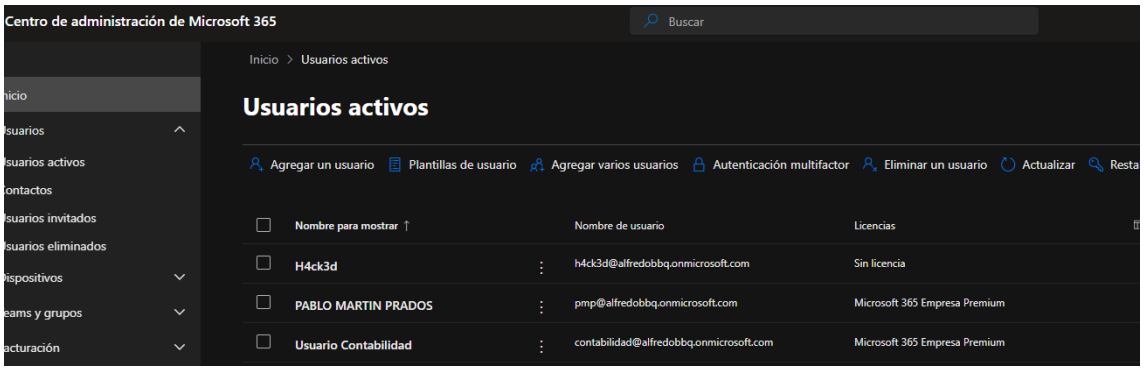


Ilustración 36: Evidencia del ataque con AADInternals

Como hemos podido ver en este ataque, se ha producido el envío de un email que no está personalizado y se ha hecho desde un dominio básico, como Hotmail. Estos ejercicios normalmente se compra un dominio muy similar al del receptor y se suele modificar el cuerpo del correo mediante ingeniería social para que el usuario piqué. Se ha podido evidenciar que, una vez robado el token, el doble factor de autenticación no se ha solicitado en ningún momento, aun siendo un Global Admin.

Para mitigar estos ataques, visto que el doble factor no es una medida suficiente, es necesario hacer uso del acceso condicional, en el cual preguntaremos por la identidad del dispositivo. Si el dispositivo está *hybrid* o está en Intune se permite, sino se bloquea. Otra acción, aunque es más laxa, es la geolocalización, podríamos no permitir el país en función de las necesidades de la organización.

3.4 Acceso al PTR

Tal y como explicamos en los puntos anteriores el PTR (Primary Token Refresh) es lo más parecido al TGS de Kerberos. Es un token que permite iniciar sesión solo una vez en el dispositivo y luego iniciar sesión de manera automática contra AzureAD. El escenario habitual de trabajo de estos tokens, son ordenadores de una organización ya sea del tipo Azure AD *registered,* Azure AD *joined*, o *Hybrid* Azure AD *Joined*. Este token contiene la

identidad del dispositivo y la clave de sesión. Tiene una duración de 14 días y podemos ver su estado lanzando un comando en el equipo unido: dsregcmd /status.

Si partimos del punto anterior en el que hemos comprometido una máquina que este unida a AzureAD o al dominio, podremos extraer el PRT.

Verificamos que el equipo está unido a AzureAD en este caso:

Ilustración 37 Equipo AzureAD Joined

Vamos a usar AADInternals para robar el PRT:

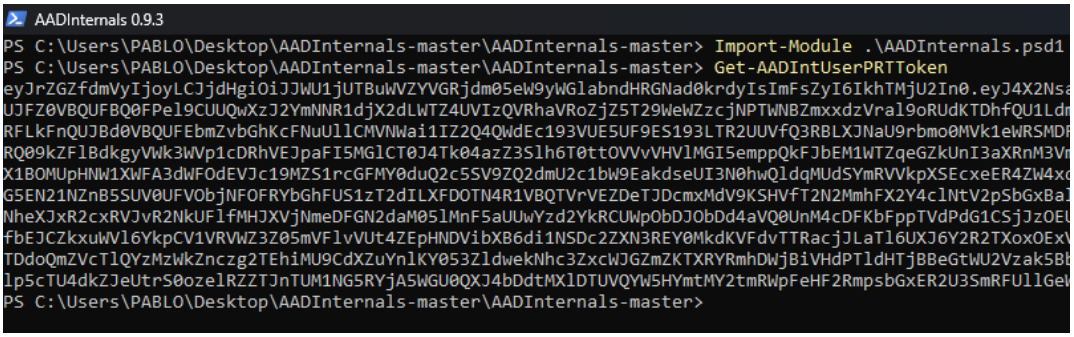


Ilustración 38: Acceso al PRT AADInternals

Con este PRT Token no podemos usarlo para ir a un navegador y hacer login con las credenciales robadas o conectarnos via PowerShell. Para ello vamos a usar otra herramienta para solicitar una cookie de sesión con este PRT.

3.5 Robo PRT Cookie

Para terminar de realizar este ataque usaremos varias herramientas. Previamente en el equipo vamos a necesitar tener instalado, Phyton, Framework 4.5 y VisualStudio Code

Nos bajamos las herramientas de ROADtools y ROADtoken desde GitHub. Procedemos a instalar roadtools con estos comandos:

- pip install roadlib
- pip install roadrecon
- Pip install roadtx

Por último, vamos a compilar el proyecto en VisualStudio de RoadToken para que nos genere el roadtoken.exe que lanzaremos como último paso.

Guardamos el PTR obtenido en el punto anterior y lo primero que vamos a hacer es solicitar un *nonce* que se asocia a una sesión de cliente con un Token ID. Usamos: roadrecon Auth –prt-init

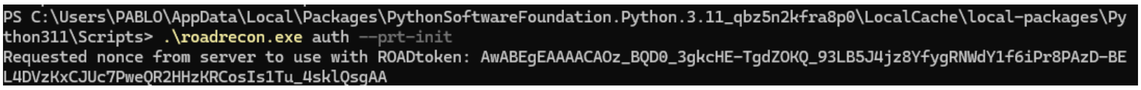


Ilustración 39: Solicitud Nonce PRT

Ahora vamos a obtener el PRT Cookie, para ello vamos a usar roadtoken.exe y el nonce que hemos solicitado:

Ilustración 40: Solicitud PRT Cookie

Vamos a obtener el token de autenticación, para ello usaremos roadrecon Auth –prt-cookie y la cookie obtenida en el paso anterior:

Ilustración 41: Token de autenticación final

Con este token que hemos obtenido ya podemos volver a conectarnos contra AzureAD via PowerShell desde otro ordenador que no sea de la organización. Para ello usaremos comando Connect-AzureAD -AccessToken "token" – AccountID xxxx-xxxx – TenantID xxxxx-xxxxx

Ilustración 42: Conexión AzureAD con PRT robado

Podemos decir que, para fortificar este proceso, tenemos que usar *Conditional Access* como la herramienta más barata y sencilla de implementar, no permitir las conexiones contra AzureAD desde ordenadores que no sean de la compañía. Si el ordenador es de la compañía esta medida no es aplicable a no ser que también lo tengamos bloqueado por defecto. Otra buena medida de detección es con técnicas de EDR (*Endpoint, Detect and*

Response) que si usan herramientas legítimas como PowerShell con las sintaxis que hemos visto que genere una alerta.

Otras dos herramientas que permiten fortificar este ataque es usar la gestión de identidades de Microsoft (*Privileged Identity Management*), con lo que cualquier usuario del cloud debe tener el mínimo de roles y privilegios para que no puedan realizar ninguna tarea, tenemos que asumir un *ZeroTrust* en las identidades.

Usar maquinas bastionadas y fortificadas para cualquier uso administrativo contra AzureAD. (Mollema, 2020)

3.6 Conclusiones post explotación

La fase de post-explotación en el contexto de los ataques a Azure AD ha revelado varias áreas clave que requieren nuestra atención inmediata.

Primero, hemos observado que Azure AD, a pesar de sus robustas medidas de seguridad, no está exento de vulnerabilidades. Se ha demostrado que se puede explotar estas vulnerabilidades para obtener acceso no autorizado a nuestros recursos.

En segundo lugar, nosotros no hemos creado una persistencia en el sistema después de la explotación inicial esto sería el segundo paso de un ataque, a no ser que en la primera localizasen un Global Admin. Esto subraya la necesidad de implementar medidas de seguridad más estrictas y de realizar un seguimiento constante de las actividades sospechosas en nuestra red.

Además, aunque implícitamente no está escrito, pero se evidencia por los ataques realizados, la importancia de la formación en ciberseguridad de los empleados. La falta de conciencia sobre las tácticas de los atacantes puede hacer que nuestros empleados sean un blanco fácil para los ataques de phishing y otras tácticas de ingeniería social.

En resumen, aunque la fase de post-explotación ha revelado varias debilidades en nuestra implementación de Azure AD, también nos ha proporcionado la información necesaria para fortalecer nuestras defensas y proteger mejor nuestra organización contra futuros ataques.

4. Implementación de buenas prácticas

Hasta ahora, hemos explorado en profundidad el funcionamiento de Azure Active Directory, los protocolos que utiliza, el concepto de identidad en el contexto de la ciberseguridad. Hemos identificado y explotado las vulnerabilidades existentes en Azure AD, lo que nos ha proporcionado una comprensión clara de las áreas que requieren nuestra atención.

Ahora, nos encontramos en un punto crucial de nuestro estudio. Después de haber expuesto las debilidades, es el momento de cambiar nuestro enfoque hacia la solución: la implementación de buenas prácticas de seguridad.

En esta sección, vamos a discutir una serie de técnicas y estrategias que pueden ayudar a fortalecer la seguridad de Azure AD. Estas técnicas no solo nos permitirán mitigar los riesgos que hemos identificado, sino que también nos prepararán mejor para enfrentar las amenazas futuras y la detección de muchas de ellas.

Vamos a explorar cómo podemos utilizar las herramientas y características disponibles en Azure AD para mejorar nuestra postura de seguridad. Aunque muchas de estas propuestas se pueden usar en los ambos sentidos de la seguridad, tanto para atacar como para defender, nuestra postura será ver lo que ven y hacen los cibercriminales para tomar una acción defensiva.

4.1 Uso de OSINT para enumerar

OSINT viene de *Open Source Intelligence*. Esta parte de la ciberseguridad hace referencia a la multitud de fuentes abiertas a partir de las cuales podemos obtener información relevante sobre un objetivo. Existen infinidad de fuentes donde se puede obtener esta información desde foros, redes sociales, *DarkWeb, DeepWeb*, bibliotecas, información pública, medios de comunicación... (Incibe, 2014)

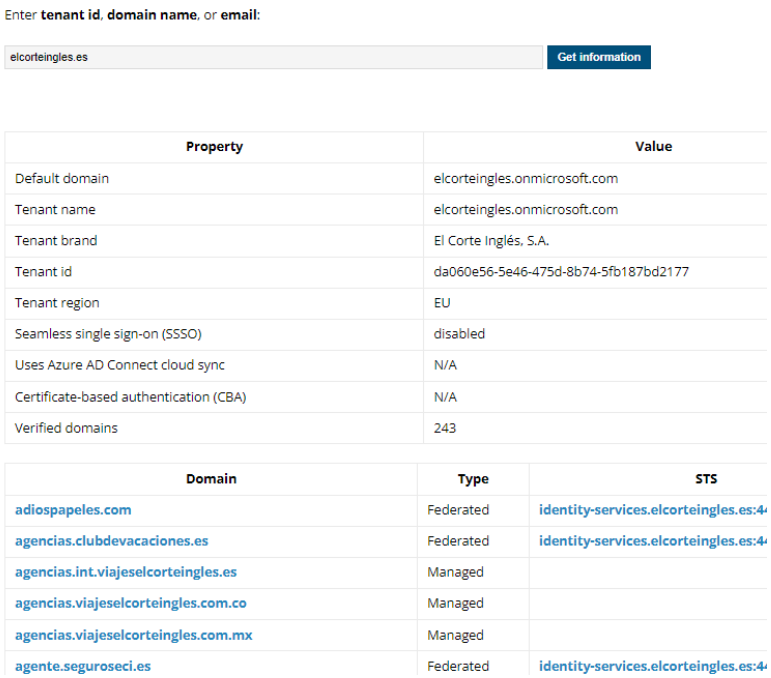
En nuestro caso si nos centramos en que podemos auditar desde fuera de nuestra organización sobre nuestro AzureAD. En ninguno de estos casos tenemos credenciales para analizar el entorno.

4.1.1 OSINT AADInternals Web

Desde AADinternals podemos hacer uso de una herramienta que introduciendo un *tenant* id, email o dominio, nos pintará información sobre el dominio:

https://aadinternals.com/osint/

Para este ejemplo he usado Elcorteingles.es:



Enter **tenant id**, **domain name**, or **email**:

elcorteingles.es

Get information

Property	Value
Default domain	elcorteingles.onmicrosoft.com
Tenant name	elcorteingles.onmicrosoft.com
Tenant brand	El Corte Inglés, S.A.
Tenant id	da060e56-5e46-475d-8b74-5fb187bd2177
Tenant region	EU
Seamless single sign-on (SSSO)	disabled
Uses Azure AD Connect cloud sync	N/A
Certificate-based authentication (CBA)	N/A
Verified domains	243

Domain	Type	STS
adiospapeles.com	Federated	identity-services.elcorteingles.es:4
agencias.clubdevacaciones.es	Federated	identity-services.elcorteingles.es:4
agencias.int.viajeselcorteingles.es	Managed	
agencias.viajeselcorteingles.com.co	Managed	
agencias.viajeselcorteingles.com.mx	Managed	
agente.seguroseci.es	Federated	identity-services.elcorteingles.es:4

Ilustración 43: Ejemplo OSINT Web

4.1.2 OSINT AADInternals PowerShell

Esta herramienta también está disponible desde *command line* (cli). Mediante Invoke-AADIntReconAsOutsider -Domain "nombre" | format-table

En este caso para la UOC:

```
PS C:\Users\PABLO\Desktop\AADInternals-master\AADInternals-master> Invoke-AADIntReconAsOutsider -Domain "uoc.edu" | format-table
Tenant brand:       Universitat Oberta de Catalunya
Tenant name:        uoc0.onmicrosoft.com
Tenant id:          aec762e4-3d54-495e-a8fe-4287dce6fe69
Tenant region:      EU
DesktopSSO enabled: False

Name                  DNS    MX   SPF DMARC  DKIM MTA-STS Type      STS
----                  ---    --   --- -----  ---- ------- ----      ---
pre.uoc.edu         False False False       False   False Federated id-provider.uoc.edu
sso.am.uoc.es        True False  True False False   False Federated id-provider-pre.uoc.edu
uoc.edu              True False  True False False   False Federated id-provider.uoc.edu
uoc0.onmicrosoft.com True  True  True False False   False Managed
```

Ilustración 44: Ejemplo OSINT PS

4.1.3 OSINT Microburst

Con Microburst, nos tenemos que bajar el desde GitHub importar los cmdlet y en este caso realizamos un comando para que no nos bloquee ninguno:

dir -Recurse .\MicroBurst-master | Unblock-File

Import-Module .\MicroBurst.psm1

Invoke-EnumerateAzureSubDomains -Base “lo que queramos buscar” - Verbose

```
PS C:\Users\PABLO\Desktop\MicroBurst-master\MicroBurst-master> Invoke-EnumerateAzureSubDomains -Base UOC -Verbose
DETALLADO: Found site-UOC.scm.azurewebsites.net
DETALLADO: Found UOC.onmicrosoft.com
DETALLADO: Found UOCit.onmicrosoft.com
DETALLADO: Found myUOC.onmicrosoft.com
DETALLADO: Found UOCtest.onmicrosoft.com
DETALLADO: Found UOC.database.windows.net
DETALLADO: Found UOC.mail.protection.outlook.com
DETALLADO: Found UOCit.mail.protection.outlook.com
DETALLADO: Found UOCtest.mail.protection.outlook.com
DETALLADO: Found UOC.queue.core.windows.net
DETALLADO: Found storageUOC.queue.core.windows.net
DETALLADO: Found UOCstorage.queue.core.windows.net
DETALLADO: Found UOCstorageaccount.queue.core.windows.net
DETALLADO: Found UOC.blob.core.windows.net
DETALLADO: Found storageUOC.blob.core.windows.net
DETALLADO: Found UOCstorage.blob.core.windows.net
DETALLADO: Found UOCstorageaccount.blob.core.windows.net
DETALLADO: Found UOC.file.core.windows.net
DETALLADO: Found storageUOC.file.core.windows.net
DETALLADO: Found UOCstorage.file.core.windows.net
DETALLADO: Found UOCstorageaccount.file.core.windows.net
DETALLADO: Found UOC-keys.vault.azure.net
DETALLADO: Found UOC.table.core.windows.net
DETALLADO: Found storageUOC.table.core.windows.net
DETALLADO: Found UOCstorage.table.core.windows.net
DETALLADO: Found UOCstorageaccount.table.core.windows.net
DETALLADO: Found site-UOC.azurewebsites.net
DETALLADO: Found UOC.sharepoint.com
DETALLADO: Found UOC-my.sharepoint.com
DETALLADO: Found UOC-web.sharepoint.com

Subdomain                               Service
---------                               -------
site-UOC.azurewebsites.net              App Services
site-UOC.scm.azurewebsites.net          App Services - Management
UOC.database.windows.net                Databases-MSSQL
UOCtest.mail.protection.outlook.com     Email
UOC.mail.protection.outlook.com         Email
UOCit.mail.protection.outlook.com       Email
UOC-keys.vault.azure.net                Key Vaults
UOC.onmicrosoft.com                     Microsoft Hosted Domain
UOCit.onmicrosoft.com                   Microsoft Hosted Domain
UOCtest.onmicrosoft.com                 Microsoft Hosted Domain
myUOC.onmicrosoft.com                   Microsoft Hosted Domain
UOC-web.sharepoint.com                  SharePoint
UOC-my.sharepoint.com                   SharePoint
UOC.sharepoint.com                      SharePoint
UOCstorageaccount.blob.core.windows.net Storage Accounts - Blobs
```

Ilustración 45: Ejemplo MicroBurst

4.1.4 OSINT Como obtener credenciales

Algunos ejemplos de los cuales también podríamos obtener más información sobre un *tenant*, pero los cuales no vamos a hacer ejercicio técnico. Podríamos obtener usuarios con la técnica de LinkedIn *Scraping* existen varios scripts en Phyton que permiten obtener los datos de contacto de sus empleados, solamente informando de la empresa.

Otra fuente que se suele usar es la web o los sitios públicos de la empresa, si obtenemos la nomenclatura que usa la empresa para sus correos electrónicos, por ejemplo:

Pablo.martin@empresa.com o pmartin@empresa.com o pablo@empresa.com

Con este dato nos podemos generar una lista de los usuarios válidos y sus correos electrónicos. Para verificar si son válidos o no, el propio servidor de correo cuando enviemos un email nos notificará si la dirección a la que hemos enviado existe o no.

Por otro lado, está la obtención de las contraseñas, si ya tenemos el login, tendremos que buscar una información para sacar la contraseña. Podemos utilizar patrones típicos de los usuarios:

- E(mayúscula)mpresa+Año
- E(mayúscula)mpresa+Mes
- E(mayúscula)mpresa+Año+ (carácter especial)
- E(mayúscula)mpresa + (carácter especial) +Año
- E(mayúscula)mpresa+Año+ (carácter especial) + (carácter especial)

Otra opción es usar diccionarios de palabras (*wordlists)* de las contraseñas que más se han visto en las exfiltraciones de datos (*leaked*). Algún ejemplo de ellos lo podemos encontrar en IhvePwnedPassword:

https://www.ncsc.gov.uk/staticjson/static-assets/documents/PwnedPasswordsTop100k.txt

Existen medidas para que los empleados de una organización no usen contraseñas débiles, que hayan sido *leaked*, o bien que contengan palabras que consideramos como débiles debido a nuestro contexto como organización. Si, por ejemplo, trabajásemos en Zumosol, esta palabra no debería estar permitida dentro de la contraseña.

4.1.5 Ejecutar una estrategia con datos obtenidos via OSINT

Una vez logrado conocer cuáles son las posibles credenciales de un objetivo, lo que los cibercriminales intentarán es validar si consiguen unas credenciales válidas para acceder al *tenant*. Para ello establecerán una estrategia existen múltiples, pero principalmente podríamos resumir en 3 las más usadas e importantes:

1. Fuerza bruta
2. *Password Spray*
3. Ataque Dirigido

La primera de ellas es muy clásica y no solo usado en entornos SaaS sino en todos los entornos *on-premise*. Escogemos un usuario y empezamos a probar todas las contraseñas que hemos ido confeccionando.

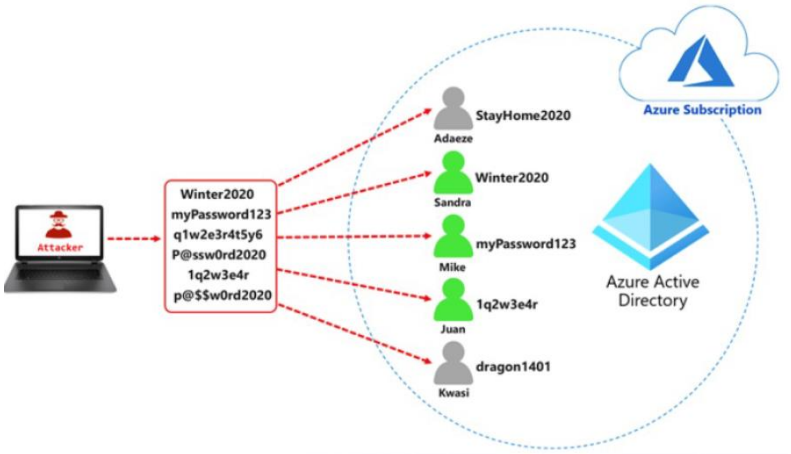


Ilustración 46: Ataque Fuerza Bruta

La segunda de ellas *Password Spray* se trata de un tipo de fuerza horizontal, es decir, buscaremos para una contraseña que usuario la tiene.

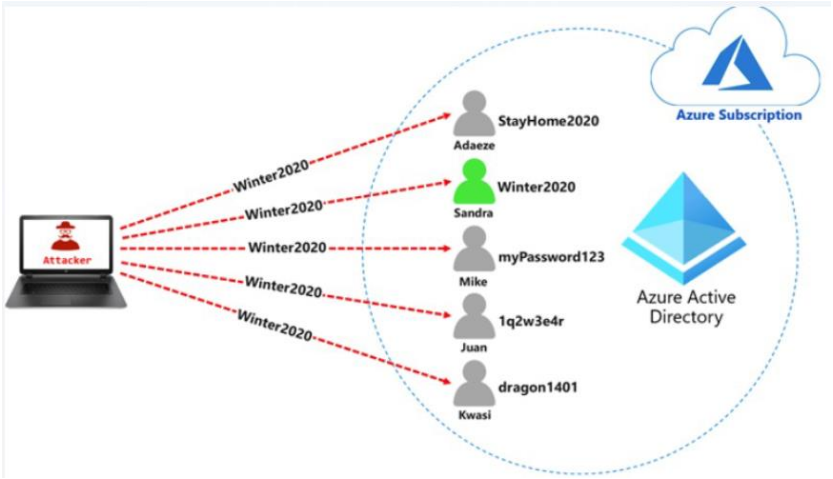


Ilustración 47: Ataque Password Spray

Y, por último, un ataque dirigido, ejecutaran ejercicio de ingeniería social con el objetivo de robar estas credenciales.

4.2 Herramientas para auditar AzureAD y Office365

En el siguiente apartado exploraremos distintas herramientas que están disponibles para auditar AzureAD y Office365. Estas herramientas permiten a las organizaciones conocer el estado de salud de nuestro *tenant*, detectar configuraciones débiles descubrir las puertas traseras que hayamos podido dejar. Al proporcionar esta vista completa del *tenant*, nos permite conocer el estado de la organización y de cómo actuar para proteger los activos digitales.

A lo largo de este trabajo examinaremos varias de estas herramientas, discutiremos sus características, ventajas y proporcionaremos una orientación de cómo pueden ser usadas de manera efectiva para auditar tanto AzureAD como office365.

El objetivo es proporcionar una idea de las opciones disponibles y como pueden ser utilizadas para mejorar la seguridad y gestión de las identidades de la organización.

Todas las herramientas mostradas son de software libre para las empresas y están disponibles para ser utilizadas.

4.2.1 PingCastle

La primera herramienta se denomina PingCastle está disponible desde la página del autor: https://www.pingcastle.com/download/ y dispone de una versión Free en la que vamos a conseguir que nos genere un reporte con los controles que se han verificado. Simplemente nos descargamos el software, lo descomprimimos y lo ejecutamos desde un cmd o powershell. Para auditar AzureAD escogemos la opción 2.

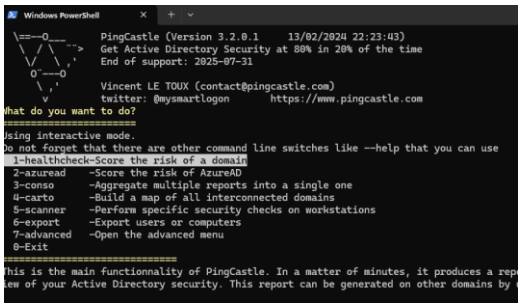


Ilustración 48: Ejecución PingCastle

Podremos hacer login con el PRT o introduciendo credenciales. Para este tipo de herramientas cuantos más privilegios les demos o 'Global Admin', los resultados serán más completos:

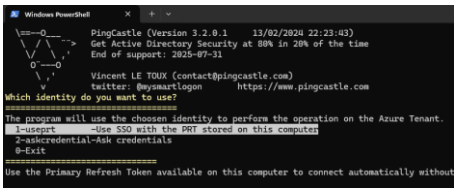


Ilustración 49: Ejecución PingCastle 2

Al finalizar genera un reporte en PDF con todo lo que ha encontrado:

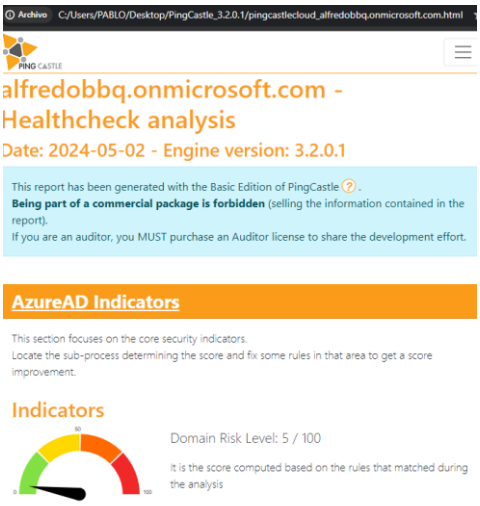


Ilustración 50: Reporte PingCastle

Cabe mencionar que esta herramienta es muy potente para entornos on-premise contra Active Directory. (PingCastle, 2024)

4.2.2 PurpleKnight

PurpleKnight es otra herramienta muy parecida a PingCastle. En este caso es de un fabricante de seguridad llamado Semperis, que está centrado en Active Directory y Azure AD. La mayoría de todos sus productos son bajo licencia de uso, a excepción de PurpleKnight. (Semperis, 2024)

Para descargarla tendremos que rellenar un formulario desde su web y nos enviarán el enlace de descarga a nuestro email: https://www.semperis.com/es/purple-knight/request-form/

Descomprimimos el ZIP y permitimos la ejecución desde PowerShell:
dir -path "ruta" -Recurse | Unblock-File

Como vamos a auditar AzureAD es necesario crear una aplicación y dar permisos:

1. Vamos AzureAD a registro de aplicaciones.
2. Creamos una y le damos un nombre descriptivo. Los *settings* por defecto:

Ilustración 51: Configuración PurpleKnight1

3. Una vez creada vamos a los permisos API y le damos a agregar permisos.
4. Seleccionamos Microsoft Graph y Permisos de aplicación
5. Escogemos todos estos y pulsamos en añadir:

    a. AdministrativeUnit.Read.All
    b. Application.Read.All
    c. AuditLog.Read.All
    d. Device.Read.All
    e. Directory.Read.All
    f. GroupMember.Read.All
    g. Policy.Read.All
    h. PrivilegedAccess.Read.AzureAD
    i. Reports.Read.All
    j. RoleEligibilitySchedule.Read.Directory
    k. RoleManagement.Read.All
    l. RoleManagement.Read.Directory
    m. User.Read.All
    n. UserAuthenticationMethod.Read.All

6. Para finalizar pulsamos conceder consentimiento del administrador:

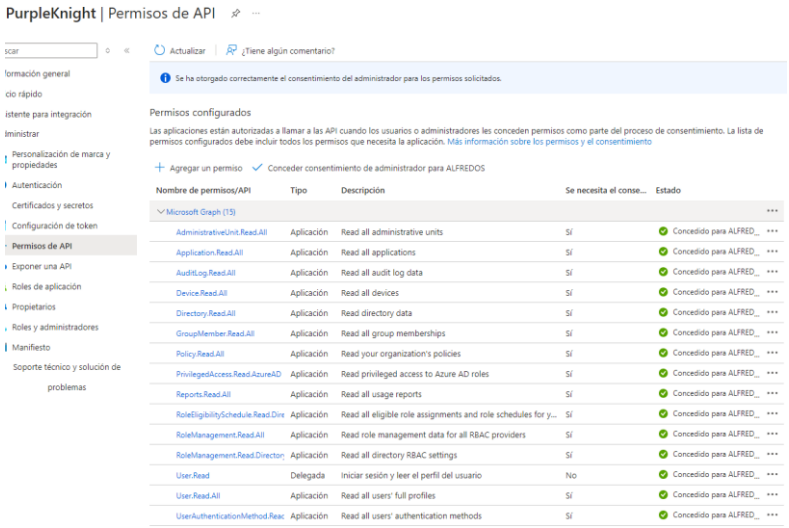


Ilustración 52: Configuración PurpleKnight2

Por último, es necesario crear un *secret* y copiarnos los valores del *tenant* ID, aplicación ID y el valor del *secret*. Para este último vamos a *secret* y generamos uno, nos tendremos que copiar el valor. Para los otros valores basta con copiarlos desde la pestaña de información general.

Ejecutamos PurpleKnight.exe desde los ficheros que descomprimimos, aceptamos los términos de licencia y con los valores del último apartado los rellenamos marcando Azure Active Directory:

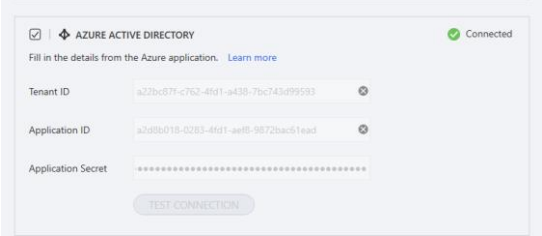


Ilustración 48: Test Connection PurpleKnight

Marcamos todos los test en la siguiente ventana y lanzamos la auditoria:

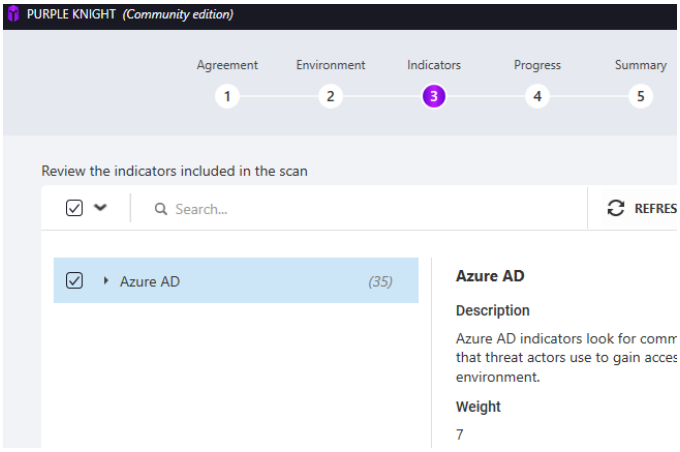


Ilustración 49: Ejecución Auditoria PurpleKnight

Cuando acabe nos devolverá una nota en función de los resultados de nuestro *tenant* y podremos acceder al reporte donde veremos que configuraciones son mejorables:

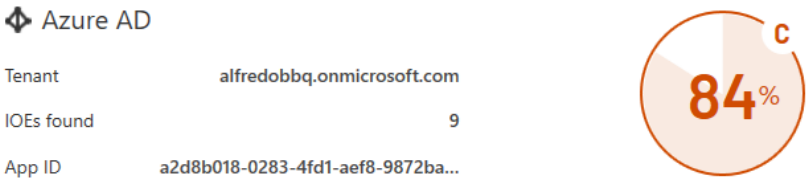


Ilustración 50: Resultados PurpleKnight

4.2.3 Monkey365

Es otra herramienta para auditar AzureAD y todas las posturas en relación con la ciberseguridad de Office365. Su autor es Juan Garrido, más conocido por Tr1ana. Al igual que las otras herramientas de auditoría, Monkey365 nos puede ayudar a buscar configuraciones erróneas y problemas de seguridad en cuentas, de acuerdo con las mejores prácticas de seguridad y siguiendo los estándares CIS en cuanto a Azure, AzureAD y las aplicaciones de Office365. Para empezar, descargaremos desde GitHub: https://github.com/silverhack/monkey365. Es necesario ejecutar este software en Powershell 7, que se puede descargar de aquí: https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell-core-on-linux?view=powershell-7

(Garrido, 2023)

Desbloqueamos los cmdlet: *Get-ChildItem -Recurse "Ruta" | Unblock-File*

Importamos los cmdlet: Import-Module monkey365. Los permisos necesarios para que Monkey365 funcione de manera correcta son:

- AzureAD: Global Reader
- Suscripciones: SecurityReader
- Office365: GlobalReader
- Sharepoint: Sharepoint Administrator

Existe multitud de opciones para auditar dentro, en este caso solamente voy a probar contra Office365:

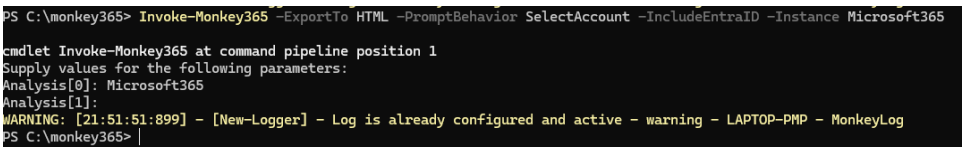


Ilustración 51: Ejecución Monkey365

El resultado lo guardará en la misma carpeta de ejecución en Reports en formato HTML:

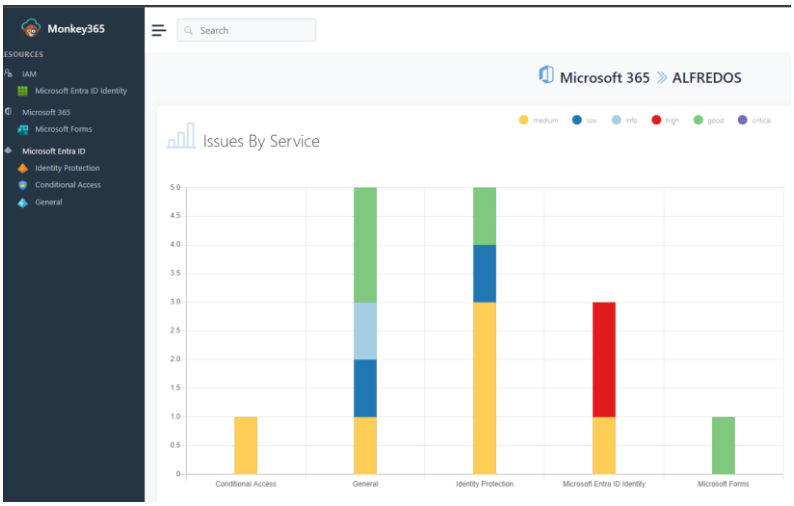


Ilustración 52: Reporte Monkey365

4.2.4 CrowdStrike Reporting Tool for Azure (CRT)

Esta es otra herramienta gratuita para auditar Office365 y AzureAD, pertenece a un fabricante de reconocido nombre en ciberseguridad como CrowdStrike. Esta nos permitirá encontrar debilidades de las configuraciones, permisos excesivos y nos dará consejos para solucionarlo. Es necesario ser GlobalAdmin para que la herramienta muestre los valores de las configuraciones. (CrowdStrike, 2024)

Descargamos desde GitHub el software: https://github.com/CrowdStrike/CRT

Ejecutamos el comando: .\Get-CRTReport.ps1 y nos solicitar que hagamos login con el Global Admin.

```
PS C:\Users\PABLO\Desktop\CRT-main\CRT-main> .\Get-CRTReport.ps1

Advertencia de seguridad
Ejecute solo los scripts de confianza. Los scripts procedentes de Internet pueden ser útiles, pero este scri
dañar su equipo. Si confía en este script, use el cmdlet Unblock-File para permitir que se ejecute sin este
advertencia. ¿Desea ejecutar C:\Users\PABLO\Desktop\CRT-main\CRT-main\Get-CRTReport.ps1?
[N] No ejecutar  [Z] Ejecutar una vez  [U] Suspender  [?] Ayuda (el valor predeterminado es "N"): Z
[2024-05-02 22:05:08Z] - Checking for PowerShell module prerequisites
[2024-05-02 22:05:08Z] - Uninstalling old versions of the ExchangeOnlineManagement module (< 3.1.0)
[2024-05-02 22:05:12Z] - Installing ExchangeOnlineManagement module
NOTE: Using default authentication. This method will prompt you for login credentials multiple times.
```

Ilustración 53: Ejecución CrowdStrike

Una vez finalizado nos dejara ficheros txt y csv con los reportes obtenidos:

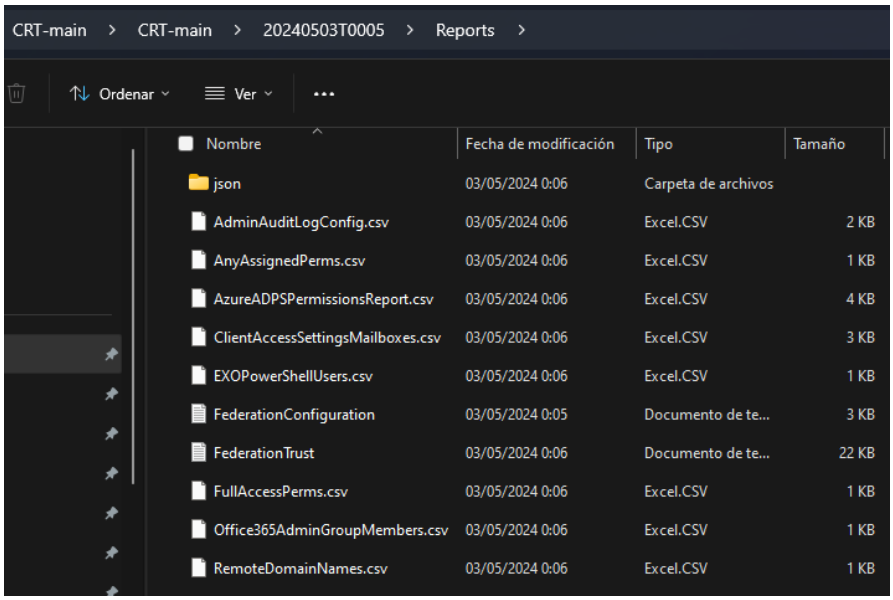


Ilustración 54: Reportes CrowdStrike

4.2.5 Microsoft Azure AD *Assessment*

Por último, exploraremos esta es una herramienta que Microsoft nos facilita para auditarnos y ver los resultados del Audit en PowerBI Desktop. Primero necesitamos crear una aplicación en AzureAD y rellenar la URI con: (Microsoft, 2022)

https://login.microsoftonline.com/common/oauth2/nativeclient

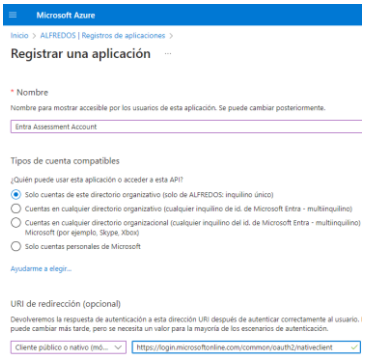


Ilustración 55: Configuración APP Azure AD Assessment

Una vez realizado esto, vamos al apartado de autenticación y marcamos este *flag* como Sí:

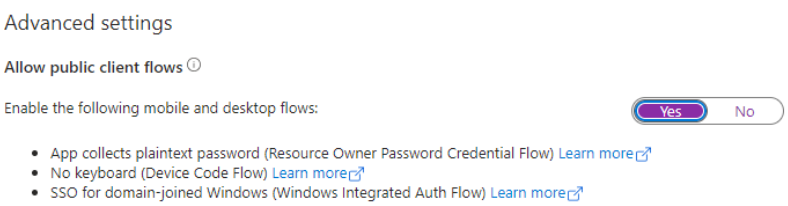


Ilustración 56: Configuración APP Azure AD Assessment 1

Vamos a PowerShell e instalamos el módulo necesario: Install-Module AzureADAssessment -Force -Scope CurrentUser

Nos conectamos con el id de aplicación que hemos generado esto nos solicitará permisos: Connect-AADAssessment -ClientId "App ID"

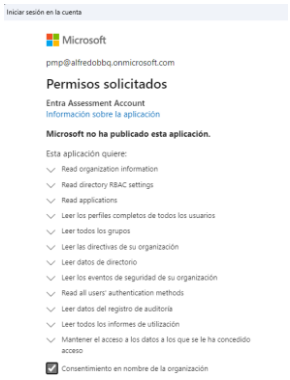


Ilustración 57: Permisos Azure AD Assessment

Y por último ya lanzaremos el proceso de auditoría: Invoke-AADAssessmentDataCollection y completamos el proceso para cargar los datos en nuestro cuadro de mandos:

```
PS C:\Users\PABLO> Invoke-AADAssessmentDataCollection


    Directorio: C:\AzureADAssessment\AzureADAssessmentData


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        03/05/2024      0:25                AAD-alfredobbq.onm
Exporting applications: Completed 1 in 00:00:00
Exporting appRoleAssignments: Completed 16 in 00:00:00
Exporting oauth2PermissionGrants: Completed 2 in 00:00:00
Exporting servicePrincipals (JSON): Completed 3 in 00:00:00
Exporting servicePrincipals (CSV): Completed 3 in 00:00:00
Exporting groups: Completed 0 in 00:00:00
Loading users in lookup cache
Loading users registration details in lookup cache
Exporting UserReport: Completed 1 in 00:00:00
Loading groups in lookup cache
Loading administrative units in lookup cache
Loading applications in lookup cache
Loading service principals in lookup cache
Exporting RoleAssignmentReport: Completed 1 in 00:00:00
Exporting AppCredentialsReport: Completed 1 in 00:00:00
Exporting ConsentGrantReport: Completed 29 in 00:00:00
```

```
PS C:\Users\PABLO> Complete-AADAssessmentReports

cmdlet Complete-AADAssessmentReports en la posición 1 de la canalización de comandos
Proporcione valores para los parámetros siguientes:
Path: C:\AzureADAssessment\AzureADAssessmentData-alfredobbq.onmicrosoft.com.aad
```

Ilustración 58: Audit AzureAD Assesment

Nos descargamos PowerBI desde este enlace y cargamos las plantillas que se han generado:

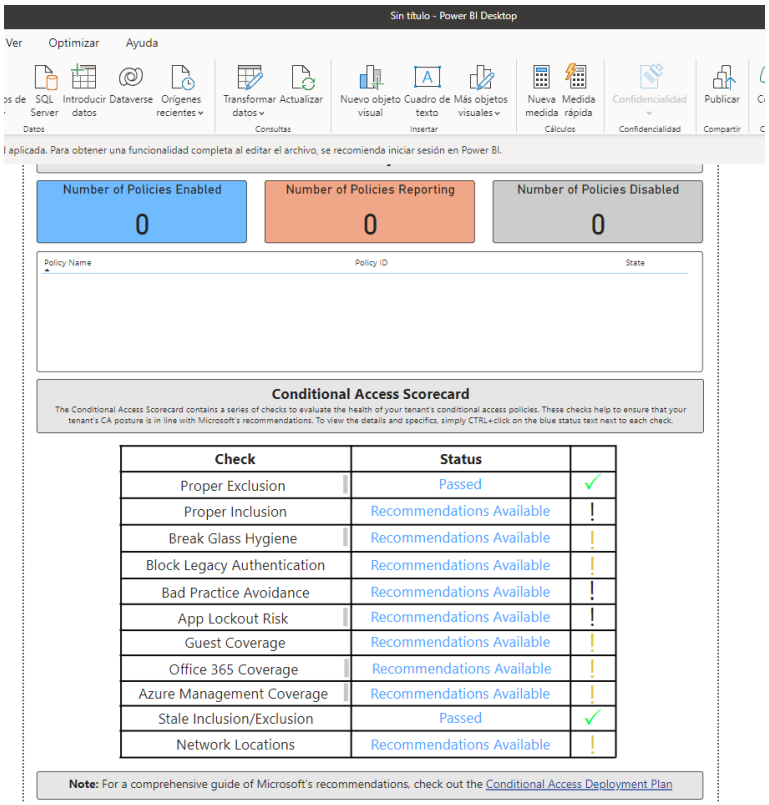


Ilustración 59: Reporte AzureAD Assessment

4.3 Implementar *Conditional Access*

4.3.1 ¿Qué es el Conditional Access?

Durante la fase ofensiva veíamos que muchos de los ataques ofensivos se podían haber mitigado con el acceso condicional. Pero realmente qué es el acceso condicional. Al final si entendemos que el perímetro de seguridad se extiende más allá de usuario y contraseña, que necesitamos saber y conocer más detallas del cómo, quién, en qué momento, desde donde, desde que ordenador, en qué condiciones esta ese ordenado, si a toda esta información la llamamos señales. Al final todas estas señales son las que va a provocar un comportamiento u otro en función de las circunstancias que la organización haya definido. Por ser prácticos, y dar un ejemplo para que se entienda mejor. No es lo mismo que un usuario se conecte en horario laboral desde su ordenador y que acceda a los datos de la organización, que este mismo usuario se me conecte desde un país de baja reputación, desde un ordenador que no se encuentra registrado y usando un método de autenticación poco habitual relacionado con sus labores.

Todas estas políticas de confianza cero (*Zero Trust)* determinarán si el login se permite, no se permite o se permite, pero con restricciones. En el siguiente diagrama podemos ver algunos de los orígenes que podremos usar para validar estas señales:

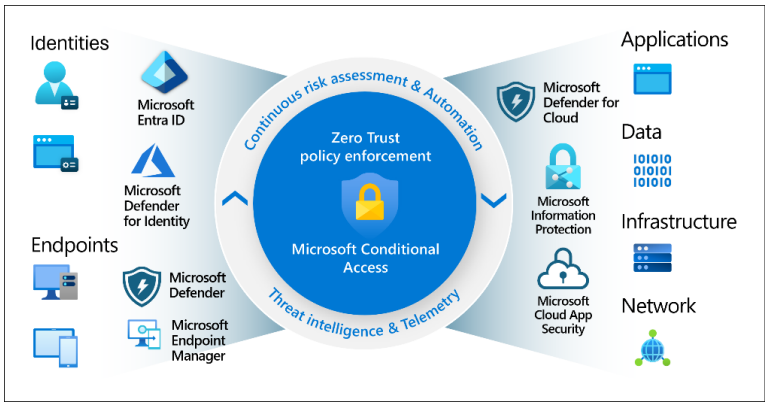


Ilustración 60: Conditional Access Señales (Microsoft, 2024)

Algunos ejemplos de estas señales pueden ser:

- Ser usuario o miembro de grupo: Las políticas pueden ser específicas para ciertos usuarios y grupos, otorgando a los administradores una supervisión más detallada del acceso.

- Geolocalización de la IP: Las empresas pueden crear intervalos de direcciones IP de confianza que se pueden usar al tomar decisiones sobre directivas. Además, se puede permitir o bloquear el flujo de tráfico desde rangos de direcciones IP de países o regiones enteras.

- Tipo de Dispositivo: Los usuarios con dispositivos de sistemas operativos concretas o marcados con un estado concreto se pueden usar al aplicar directivas de acceso condicional.

- Aplicación: Los usuarios que buscan acceder a aplicaciones determinadas pueden desencadenar diversas políticas de acceso condicional.

- Detección de riesgo en tiempo real: Permite supervisar en tiempo real el acceso a las aplicaciones y los login de los usuarios. Esto aumenta la visibilidad y el control en el acceso junto con las actividades dentro de Azure.

- Microsoft Defender para aplicaciones en la nube: Facilita el monitoreo y la gestión en tiempo real del acceso a las aplicaciones y las sesiones de los usuarios. Esto mejora la visibilidad y el dominio sobre el acceso y las acciones llevadas a cabo dentro de Azure.

Por último, cabe mencionar que no existe un requisito mínimo de licenciamiento, Microsoft Entra ID Plan 1 está incluido con cualquier suscripción a Microsoft Cloud como Azure u Office365.

Para configurar estas políticas, entraríamos en Portal.azure.com > AzureAD > Seguridad > Conditional Access > Políticas

4.3.2 ¿Qué debemos implementar con el *Conditional Access*?

Antes de implementar medidas en el acceso condicional que den cobertura a una organización, se debería de contar un mapa de nuestros activos, es decir, conocer lo que se debe proteger. Es fundamental saber dónde están los datos y establecer una política de acceso a ellos. En función de los casos de usos qué se elaboren se deben establecer estas medidas. Como recomendación es empezar en modo "monitor", es decir la medida no tomará acción alguna y podremos ver si se estaría aplicando para nuestro caso de uso y de menos a más, es decir empezar con un grupo pequeña de usuarios o aplicaciones, monitorear e ir ampliando. Es un proceso gradual en ningún caso se recomienda ni bloquear ni permitir todo en un solo intento.

En cuanto a las medidas de seguridad más estándar que podría aplicar a cualquier organización por el mero hecho de usar AzureAD u Office365, es proteger los administradores y los accesos administrativos.

Para el primer caso de protección a los administradores, una buena medida de seguridad es que cualquier miembro con algún tipo de rol o privilegio sobre una suscripción de Azure que sea obligatorio requerirle un doble factor de autenticación fuerte. Para Microsoft existen varios dobles factores de autenticación, en este caso el basado en tokens de hardware es más seguro que el de notificaciones *push*.

Otra buena medida de autenticación es bloquear cualquier acceso de administradores desde ubicaciones que no sean de confianza. Por ejemplo, si sabemos que nuestros administradores no trabajan desde Kuala Lumpur, directamente denegar las conexiones.

Requerir que el acceso como administrador se haga desde una maquina "conocida" es decir o bien este unida al dominio o bien se encuentre bajo Microsoft Intune. También podemos aplicar esta medida a los portales administrativos.

Si hablamos de los accesos administrativos, ya vimos en puntos anteriores y en los ataques ofensivos, que por defecto se encuentran abiertos todos los accesos administrativos para todos los usuarios del *tenant*. Con el acceso condicional podremos bloquear todos los accesos mediante una regla, a excepción de los administradores. Solamente habría que añadirla aplicación: windows azure service management api y portal admins, en la política.

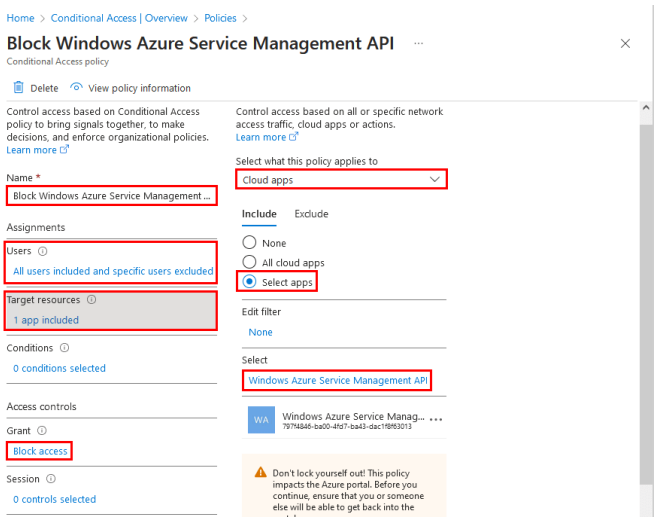


Ilustración 61: Bloqueo portal Admins

Aun haciendo todo esto dejaríamos abierto la conexión via PowerShell a GraphExplorer, para bloquear esto la única forma de bloquearlo también sería escogiendo la opción de todas las aplicaciones y exceptuando aquello que sí que permitimos, según las necesidades que existan por parte de negocio.

4.4 Ver los eventos y log de Azure AD

Tal y como hemos podido ver en los puntos anteriores monitorizar y poder relacionar lo que está ocurriendo en nuestro Azure AD con casos de uso es necesario casi para cualquier organización que este preocupada por la ciberseguridad dentro de AzureAD. Una de las maneras de ver que está ocurriendo en AzureAD es ir a los logs y ver realizar una búsqueda por con los filtros que nos propone Microsoft.
Para llegar a ello tenemos dos tipos de logs. Los que se reflejan en los inicios de sesión (*sing-in logs)* o los Logs de Auditoria (*Audit log*). Ambos dos nos van a aportar una visión de lo que sucede en nuestro *tenant*.

El primero, *sing-in logs,* registra los *i*nicios de sesión de usuario interactivos (realizados por un usuario), inicios de sesión de usuario no interactivos, inicios de sesión de entidad de servicio e inicios de sesión de identidad administrada.

El segundo, los *Audit log,* se centra en eventos del *tenant, mostrando*, fecha y hora en que se produjo el evento, servicio que ha registrado la petición, categoría y actividad, estado de la actividad (OK o NO OK)

Para acceder a ellos basta con ir a Azure Active Directory > *Monitoring* > *Sing-in Logs o Audit Logs*. Es necesario disponer de roles específicos, son varios quién puede dar acceso, o ser global Admin del *tenant*.

Por otro lado, existen una limitación en cuanto a la duración de estos logs en función de nuestro nivel de licenciamiento. Si solamente se dispone de un licenciamiento Microsoft Entra Plan Free los logs se van eliminando cada 7 días. Si se dispone Plan 1 o Plan 2, Microsoft almacena los logs durante 30 días. (Microsoft, 2023)

4.4.1 ¿Cómo crear casos de uso en Azure AD?

Existen soluciones comerciales tipo Administración de eventos e información de seguridad (*Security Information and Event Management*) que son capaces de conectarse con un *tenant* y llevarse estos logs para poder correlacionarlos con determinados casos de uso que se puedan plantear. Por mencionar algunas de las herramientas de pago más usadas, podemos encontrar Splunk o Q-Radar. Por supuesto, Microsoft también dispone de un SIEM, Microsoft Sentinel bastionado sobre Azure, el cual tiene una integración todavía más directa que los SIEM comerciales que hemos mencionado.

Este tipo de herramientas suelen venir con unas reglas por defecto para que son válidas para casi todas las organizaciones. Ninguna empresa debería quedarse solo en ese punto, con las reglas de por defecto, sino intentar crear más casos de uso adhoc a su negocio.

Es importante saber que los SIEM suelen tener un coste elevado para casi cualquier organización de tamaño pequeño-mediano. Muchas de ellas subcontratan a empresas especialistas en ciberseguridad este servicio de equipo de seguridad *(Security Operations Center)* que ya disponen de unos SIEM con el cuál reparten el gasto entre todos sus clientes.

Sin embargo, existe una manera de configurar nuestro *tenant,* sin disponer de un SIEM y que nos permita almacenar estos logs más de 30 días, y correlacionar casos de uso es mediante Azure con un gasto mínimo comparándolo con las herramientas comerciales. Lo único que es necesario es disponer de una suscripción en Azure, que va a ser el coste que tendremos por almacenar los logs.

Creamos un área de trabajo de *log analytic* y lo asociamos a un grupo de recursos. Seguidamente vamos a AzureAD > Configuración del diagnóstico. Agregamos una configuración del diagnóstico. Marcamos *AuditLogs*, *SinginLogs* y escogemos el área de log a*nalytic* que creamos:

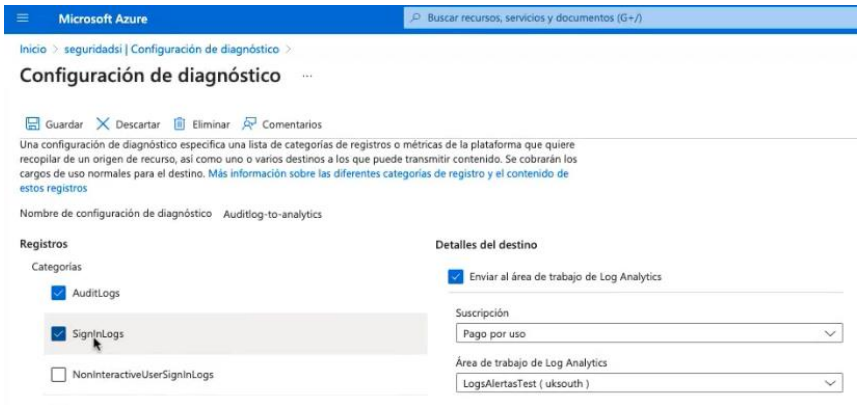


Ilustración 62: Configuración Diagnóstico AzureAD

Una vez hecho esto ya podríamos configurar las reglas de alertas sobre el log analytic de Azure. Azure > Log Analytic > Alertas > Crear Nueva Regla de Alerta

Por ejemplo, uno de los casos de uso típicos que es recomendable configurar una alera, es tener controlado cuando un Global Admin del *tenant* hace login.

4.5 Medidas de seguridad Azure AD

Para finalizar este apartado del trabajo, nos vamos a centrar en medidas de seguridad que podemos ejecutar y son fáciles de implementar desde el lado defensivo. Debemos de entender que una medida por sí sola no va a mitigar ningún ciberataque, sino que va a añadir una complejidad al tener distintas barreras defensivas para que no se logre el objetivo. Algunas de estas medidas las recomienda Microsoft. (Microsoft, 2023)

- Reducir el número de usuarios con privilegios Global Admin, la cifra ideal es de 2 a 5 Global Admin.

- Activar como obligatorio *MultiFactor Authentication* (MFA) para todos los usuarios del *tenant*, administradores e invitados externos.

- Usar contraseñas de más de 24 caracteres para los usuarios Global Admin, es decir, se premia a la longitud de la contraseña. Al final, cuanto mayor compleja, y larga sea la contraseña mayor dificultad tendrán los cibercriminales en robarla.

- Usar máquinas muy bien bastionadas desde el punto de vista de seguridad, que nos permita acceder al *tenant* desde un entorno seguro.

- Evitar el uso de usuarios nominales de trabajo diario para acceder a los centros de administración, es decir, nuestro usuario con el que podemos usar MS Outlook, MS Teams, no debería de ser un usuario con privilegios sobre el *tenant*.

- Usar el privilegio mínimo (*Privileged Identity Management*) para los usuarios que dispongan de un rol cualquiera de administración del *tenant*, de este modo nos aseguramos de que ningún usuario tiene más privilegios que los necesarios en el momento necesario. Este complemento se licencia aparte. (Microsoft, 2023)

- Los usuarios que dispongan roles de administración que sean del tipo *pure cloud* de esta manera al evitar que sean híbridos, eliminamos la posibilidad que, si una cuenta del AD está comprometida, consigan acceso al *tenant*.

- Configurar dentro de Azure AD que cuando se produzca un cambio de contraseña por un administrador notificar a los demás administradores.
  Azure AD > Usuarios > Restablecimiento de contraseña > Reestablecer contraseña

- Escoger una política de contraseñas buenas para los usuarios y establecer un diccionario de palabras prohibidas mediante *Azure Password Protection*. De este modo si, por ejemplo, nuestra empresa se llama UOC, al incluir esta palabra prohibirá a los usuarios hacer uso de ella en cualquiera de sus formas y nomenclaturas (u0c, 2024Uoc, etc.)
  Azure AD > Seguridad > Métodos de Autenticación > Protección con contraseña

- En el caso de disponer de suscripciones en Azure, existe una política que evita que una suscripción pueda ser migrada a otro *tenant*, sin permiso del usuario.
  Azure > Suscripciones > Administrar Directivas

- Revisar las tasas de *login/failed* nos puede ayudar a saber en qué aplicación estamos recibiendo mayor número de ataques.
  Entra Admin Center > Uso e Información > Actividad de la aplicación Microsoft Entra

- Revisar y configurar los métodos de autenticación disponibles.
  Azure AD > Seguridad > Métodos de autenticación > Políticas

- Configurar el bloqueo en el caso de abuso del MFA y alertado en caso de que se produzca el fraude en el *(MFA)*.
  Azure AD > Autenticación Multifactor > Bloqueo de cuenta
  Azure AD > Autenticación Multifactor > Notificaciones

- Revisar que los usuarios no puedan registrar aplicaciones en Azure sin consentimiento.
  Azure AD > Usuarios > Configuración Usuarios

- En caso de que tengamos habilitado el portal de auto restablecimiento de contraseña para los usuarios, requerir otro método para renovar la contraseña.
  Azure AD > Reestablecer contraseña > Métodos de Autenticación

- No permitir la creación de grupo por parte de los usuarios.
  Azure AD > Grupos > Configuración > General

- Requerir MFA para unir equipos nuevos a Azure AD.
  Azure AD > Dispositivos > Configuración de dispositivo

- Revisar y monitorizar de manera frecuente el *Conditional Access* para comprobar que las políticas que tenemos establecidas siguen cumpliendo con las políticas que hemos establecido. Existen software de terceros gratuitos que nos ayudan a evaluar posibles agujeros en función de las políticas configuras como por ejemplo MFA Sweep (dafthack, 2020)

- Restringir el acceso externo y la invitación de externos por parte de los usuarios
  Azure AD > Usuarios > Configuración usuario > Configuración de colaboración externa

5.Conclusiones y trabajos futuros

A lo largo de este trabajo se han abordado y descrito conceptos clave relacionados con el estado actual de la nube pública. Se han identificado como los servicios de Office365 y su proveedor de identidades Azure AD. Se ha podido comparar las diferencias entre el entorno *on-premise* y la nube.

Asimismo, hemos profundizado cual es la cadena de ataque contra Azure AD u Office365 y hemos podido ver la importancia de entender el concepto de identidad, no solamente como unas credenciales para entrar a un sistema.

Como enfoque práctico hemos podido analizar desde un punto de vista ofensivo de la seguridad, como el sistema admite determinadas configuraciones que permite vulnerar la información de una organización.

Con este punto de vista en el que hemos entendido como funciona Azure AD, entender sus debilidades, el principal objetivo del trabajo era ver cómo podemos securizar un entorno de Azure AD y Office365, pero analizándolo desde los dos lados, es decir, si solo nos situamos en el lado defensivo, perdemos de vista como atacan los cibercriminales, que es una parte fundamental para saber cómo te debes defender de las amenazas y saber mitigarlas.

Durante este trabajo se han analizado diversas herramientas tanto defensivas como ofensivas que nos han proporcionado un plus en cuanto a lo que Microsoft nos muestra en el cuadro de mando. Existen infinidad de herramientas disponibles en repositorios para analizar el estado de salud de nuestro *tenant*. Las que se han propuesto en este trabajo han sido solo algunas muy focalizadas en los objetivos a conseguir.

Sin embargo, cabe recordar que cada organización, empresa debe de hacerse un mapa de riesgos, asociar un plan de tratamiento de estos riesgos que cuantifique el riesgo de manera matemática, y que cada organización sea capaz de escoger su umbral de riesgo y establecer las medidas necesarias para estar por debajo de este umbral. El mero hecho de usar una nube pública para usar servicios SaaS como Office365, en sí brinda muchos beneficios a una empresa, pero también trae consigo una serie de riesgos que se deben analizar.

Tal y como hemos podido ver tras la realización de este trabajo, existen multitud de servicios tanto dentro de Office365 como dentro de Azure AD, que se deben proteger y ser muy constante en la monitorización, de qué está ocurriendo en la organización realizando casos de uso, poniendo alertas cuando sean necesarias, estableciendo períodos de auditoría sobre los activos más importantes. Este trabajo no se ha centrado en analizar los casos de uso de Azure AD, ya que las casuísticas son infinitas dependiendo de la organización, es posible que lo que a una empresa le valga como recomendación determinadas opciones y que a otra no por otras características.

6. Bibliografía

ADSecurity, 2015. *Cracking Kerberos TGS Tickets Using Kerberoast – Exploiting Kerberos to Compromise the Active Directory Domain*. [Online]
Available at: https://adsecurity.org/?p=2293
[Accessed Abril 2024].

Center for Internet Security® , 2024. *CIS Microsoft 365 Benchmarks*. [Online]
Available at: https://www.cisecurity.org/benchmark/microsoft_365
[Accessed Abril 2024].

Center for Internet Security®, 2024. *Microsoft Azure*. [Online]
Available at: https://www.cisecurity.org/benchmark/azure
[Accessed Abril 2024].

Centro Criptologico Nacional, 2024. *Guía CCN-STIC*. [Online]
Available at: https://www.ccn-cert.cni.es/es/guias.html
[Accessed Abril 2024].

Checkpoint, 2015. *THE MITRE ATT&CK FRAMEWORK*. [Online]
Available at:
https://community.checkpoint.com/fyrhh23835/attachments/fyrhh23835/spanish/8/4/Check%20Point%20-%20Mitre%20Attack%20Framework%20vFinal%20Check%20Mates.pdf
[Accessed Marzo 2024].

CrowdStrike, 2024. *CRT (CrowdStrike Reporting Tool for Azure)*. [Online]
Available at: https://www.crowdstrike.com/resources/community-tools/crt-crowdstrike-reporting-tool-for-azure/
[Accessed Mayo 2024].

Cybersecurity and Infrastructure Security Agency, 2023. *Secure Cloud Business Applications (SCuBA) Project*. [Online]
Available at: https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project
[Accessed Abril 2024].

dafthack, 2020. *MFASweep*. [Online]
Available at: https://github.com/dafthack/MFASweep
[Accessed Mayo 2024].

Garrido, J., 2023. *Monkey365*. [Online]
Available at: https://github.com/silverhack/monkey365
[Accessed Mayo 2024].

Hausknecht, R., 2020. *PowerZure*. [Online]
Available at: https://github.com/hausec/PowerZure
[Accessed Mayo 2024].

Incibe, 2014. *OSINT - La información es poder*. [Online]
Available at: https://www.incibe.es/incibe-cert/blog/osint-la-informacion-es-poder
[Accessed Mayo 2024].

Incibe, 2020. *CyberKill Chain Las 7 fases ciberataque*. [Online]
Available at: https://www.incibe.es/empresas/blog/las-7-fases-ciberataque-las-conoces
[Accessed Marzo 2024].

Lockheed Martin Corporation, 2024. *Incibe Cyberkill Chain*. [Online]
Available at: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
[Accessed Marzo 2024].

Lockheed Martin, 2024. *Who we are Lockheed Martin*. [Online]
Available at: https://www.lockheedmartin.com/en-us/who-we-are.html
[Accessed Marzo 2024].

Lynn, R., 2024. *2013*. [Online]
Available at: https://www.roguelynn.com/words/explain-like-im-5-kerberos/
[Accessed Abril].

Metcalf, S., 2014. *Kerberos & KRBTGT: Active Directory's Domain Kerberos Service Account*. [Online]
Available at: https://adsecurity.org/?p=483
[Accessed Abril 2024].

Microsoft, 2017. *Gold LEED Microsoft*. [Online]
Available at: https://blogs.microsoft.com/green/2017/11/08/building-operating-greener-datacenters-commitment-leed-gold/
[Accessed Abril 2024].

Microsoft, 2022. *Assessment Reference*. [Online]
Available at: https://github.com/AzureAD/AzureADAssessment/wiki/Assessment-Reference
[Accessed Mayo 2024].

Microsoft, 2022. *Azure Ad Assessment*. [Online]
Available at: https://github.com/AzureAD/AzureADAssessment
[Accessed Mayo 2024].

Microsoft, 2023. *¿Qué es Microsoft Entra Privileged Identity Management?*. [Online]
Available at: https://learn.microsoft.com/es-es/entra/id-governance/privileged-identity-management/pim-configure
[Accessed Mayo 2024].

Microsoft, 2023. *AzureADAssessment*. [Online]
Available at: https://github.com/AzureAD/AzureADAssessment
[Accessed Abril 2024].

Microsoft, 2023. *Información general sobre los permisos y el consentimiento en la Plataforma de identidad de Microsoft*. [Online]
Available at: https://learn.microsoft.com/es-es/entra/identity-platform/permissions-consent-overview
[Accessed Abril 2024].

Microsoft, 2023. *Procedimientos recomendados para los roles de Microsoft Entra*. [Online]

Available at: https://learn.microsoft.com/es-es/entra/identity/role-based-access-control/best-practices
[Accessed May 2024].

Microsoft, 2023. *Reference-reports-data-retention*. [Online]
Available at: https://learn.microsoft.com/es-es/entra/identity/monitoring-health/reference-reports-data-retention
[Accessed Mayo 2024].

Microsoft, 2023. *Responsabilidad compartida en la nube*. [Online]
Available at: https://learn.microsoft.com/es-es/azure/security/fundamentals/shared-responsibility
[Accessed Marzo 2024].

Microsoft, 2023. *What is Microsoft Entra authentication?*. [Online]
Available at: https://learn.microsoft.com/en-us/entra/identity/authentication/overview-authentication
[Accessed Abril 2024].

Microsoft, 2023. *whatis azure ad connect*. [Online]
Available at: https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/whatis-azure-ad-connect
[Accessed Abril 2024].

Microsoft, 2024. *¿Qué es Azure RBAC?*. [Online]
Available at: https://learn.microsoft.com/es-es/azure/role-based-access-control/overview
[Accessed Abril 2024].

Microsoft, 2024. *¿Qué es el acceso condicional?*. [Online]
Available at: https://learn.microsoft.com/es-es/entra/identity/conditional-access/overview
[Accessed Mayo 2024].

Microsoft, 2024. *Azure CLI*. [Online]
Available at: https://learn.microsoft.com/es-es/cli/azure/install-azure-cli
[Accessed Abril 2024].

Microsoft, 2024. *Azure Resource Manager*. [Online]
Available at: https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/get-started/how-azure-resource-manager-works
[Accessed Abril 2024].

Microsoft, 2024. *concept-primary-refresh-token*. [Online]
Available at: https://learn.microsoft.com/es-es/entra/identity/devices/concept-primary-refresh-token
[Accessed Abril 2024].

Microsoft, 2024. *Microsoft Cybersecurity Reference Architectures*. [Online]
Available at: https://learn.microsoft.com/en-us/security/adoption/mcra
[Accessed Marzo 2024].

Microsoft, 2024. *Microsoft Entra Built-in Roles*. [Online]
Available at: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference
[Accessed Abril 2024].

Microsoft, 2024. *Microsoft Entra ID*. [Online]
Available at: https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id
[Accessed Marzo 2024].

Microsoft, 2024. *Presentamos la nueva aplicación de Microsoft 365*. [Online]
Available at: https://www.microsoft.com/es-es/microsoft-365/microsoft-365-faqs
[Accessed Marzo 2024].

Microsoft, 2024. *What is Conditional Access?*. [Online]
Available at: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview
[Accessed Mayo 2024].

Microsoft, 2024. *What Is IaaS*. [Online]
Available at: https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-iaas

MITRE, 2024. *Azure AD Matrix*. [Online]
Available at: https://attack.mitre.org/matrices/enterprise/cloud/azuread/
[Accessed Marzo 2024].

MITRE, 2024. *CVE*. [Online]
Available at: https://cve.mitre.org/
[Accessed Marzo 2024].

MITRE, 2024. *MITRE ATT&CK*. [Online]
Available at: https://attack.mitre.org
[Accessed Marzo 2024].

MITRE, 2024. *Office 365 Matrix*. [Online]
Available at: https://attack.mitre.org/matrices/enterprise/cloud/office365/
[Accessed Marzo 2024].

Mollema, D.-j., 2020. *Abusing Azure AD SSO with the Primary Refresh Token*. [Online]
Available at: https://dirkjanm.io/abusing-azure-ad-sso-with-the-primary-refresh-token/
[Accessed Mayo 2024].

PingCastle, 2024. *PingCastle*. [Online]
Available at: https://www.pingcastle.com/
[Accessed Mayo 2024].

Powerzure, 2024. *Powerzure*. [Online]
Available at: https://powerzure.readthedocs.io/
[Accessed Abril 2024].

Semperis, 2024. *Evaluación de la seguridad de Active Directory.* [Online]
Available at: https://www.semperis.com/es/purple-knight/
[Accessed Mayo 2024].

Syynimaa, D. N., 2018. *AadInternals.* [Online]
Available at: https://aadinternals.com/aadinternals/
[Accessed Mayo 2024].

Syynimaa, D. N., 2020. *AAD Kill chain.* [Online]
Available at: https://aadinternals.com/aadkillchain/
[Accessed Abril 2024].

Syynimaa, D. N., 2021. *Deep-dive to Azure AD device join.* [Online]
Available at: https://aadinternals.com/post/devices/
[Accessed Abril 2024].

Tarlogic, 2019. *Kerberos (I): ¿Cómo funciona Kerberos? – Teoría.* [Online]
Available at: https://www.tarlogic.com/es/blog/como-funciona-kerberos/#%C2%BFQue_es_Kerberos
[Accessed Abril 2024].

Tarlogic, 2023. *Attack Path Management: Securizar el Active Directory.* [Online]
Available at: https://www.tarlogic.com/es/blog/attack-path-management/#31_Tener_en_cuenta_los_errores_de_configuracion
[Accessed Abril 2024].

7. Tabla de Ilustraciones