Análisis y recomendaciones según el tipo de vulnerabilidad en los servicios de infraestructura cloud computing usando simulaciones de ataques a los servicios cloud.

Trabajo de grado presentado para optar al título de:
Ingeniero de telecomunicaciones

Sergio Andrés Cardona Osorio

Tutor
Juan Pablo Urrea Duque

Universidad de Antioquia
Facultad de Ingeniería, Departamento de ingeniería electrónica y telecomunicaciones.
Pregrado
Medellín, Colombia.
2022

Resumen

En la actualidad la trasformación digital ha cambiado la visión de empresas y clientes a la hora de dar o consumir un servicio, dejando obsoletas algunas tecnologías que se venían utilizando. Una alternativa que ayuda a mejorar y dar mejores análisis a procesos en busca de optimizarlos con nuevas tecnologías es el Cloud Computing, dando beneficios con implementación de plataformas ágiles con altos rendimientos y gran capacidad de almacenamiento que satisface las necesidades de empresas y usuarios de un mundo cada vez más moderno.

Uno de los principales riesgos de manejar información o datos de clientes, es la filtración de estos, lo cual conlleva, a grandes problemas ya sea para proveedores como clientes de un servicio. La infraestructura Cloud Computing puede ser afectada con varios vectores de ataques por lo que es de gran importancia simular los impactos que tienen estos servicios para mitigar las falencias y vulnerabilidades y así evitar pérdidas a futuro.

Es importante conocer las principales amenazas y vulnerabilidades del cloud computing en cuanto a sus tácticas y técnicas de ataque para diferentes servicios y tomar una mejor decisión para mitigar sus impactos. Una de las alternativas es simular estos ataques y experimentar su impacto sin correr riesgo alguno. Infection Monkey es un simulador de uso gratuito para algunas plataformas el cual nos permite configurar, leer resultados y generar reporte de amenazas y vulnerabilidades de forma técnica, lo cual, nos ayuda a mejorar el servicio. La ventaja de usar un simulador es la capacidad de analizar estos resultados de forma minuciosa que permitan tomar decisiones adecuadas, y así mejorar y tener más confianza en los servicios Cloud Computing, al diseñar un plan de gestión de riesgos para protección de servicios en la nube.

Los resultados obtenidos con el simulador Infection Monkey son satisfactorios debidos a su completo reporte de seguridad y su fácil manejo, permitiendo tener más claridad en configuración de máquinas virtuales y redes desplegadas en la nube, por lo que es recomendable el uso de un simulador con fines prácticos ya sea para clientes finales como proveedores del servicio.

Introducción

En términos simples, la computación en la nube significa almacenar y acceder a datos y programas a través de Internet en lugar del disco duro de una computadora. En última instancia, la "nube" es solo una metáfora de Internet. Para que se considere "computación en la nube", se debe acceder a los datos o programas a través de Internet, o al menos, tener esos datos sincronizados con otra información en la web.

La computación en la nube en la actualidad afecta a consumidores individuales como: hogares, negocios pequeños, oficinas, etc. Aunque el mayor impacto ya sea por beneficios o algún tipo de amenazas recaerá sobre grandes empresas que optan por este servicio.

Dentro de los servicios encontramos servicio cloud por Software (SaaS), plataforma de servicio (PaaS) e infraestructura como servicio (IaaS). Los cuales, como cualquier servicio están expuestos a ataques y vulnerabilidades de seguridad por quienes quieren generar algún beneficio o malestar a estas plataformas. Por lo que es importante analizar dichas vulnerabilidades y de esta forma realizar simulaciones para llegar a recomendaciones puntuales que vayan generando una mayor confiablidad en los servicios Cloud Computing.

Dentro del análisis para garantizar confiabilidad del servicio es importante recrear estas vulnerabilidades con el fin de conocer a fondo sus fortalezas y debilidades, y es vital la utilización de herramientas de trabajo donde se pueda interactuar para la obtención de resultados. Es por esto que la utilización de simuladores que permiten evaluar entornos parecidos al servicio cloud computing son de gran importancia antes de entrar a la etapa de desarrollo.

Objetivos

Objetivo general:

Implementar un escenario de ataque usando herramientas de simulación para analizar las amenazas y vulnerabilidades derivadas de la tecnología de los servicios cloud computing, según el modelo de implementación en nube pública y privada con el servicio de infraestructura IaaS, a través, de diferentes escenarios de riesgo y vectores de ataque.

Objetivos específicos:

- Identificar las principales amenazas y vulnerabilidades de cloud computing de acuerdo al modelo de servicio público y privado en la infraestructura IaaS.

- Evaluar en un entorno virtual de carácter experimental, amenazas derivadas de la tecnología y vulnerabilidades presentes en el modelo y servicio cloud computing IaaS.

- Analizar los resultados a partir de estrategias dentro de un plan de gestión de riesgos para mitigación y protección de cloud computing.

- Generar recomendaciones para minimizar los riesgos dentro de los servicios de cloud computing.

Marco Teórico

El cloud computing o computación en la nube es un tipo de tecnología que tiene una variedad de servicios en los cuales se encuentran el acceso remoto a software, almacenamiento de archivos, procesamiento de datos, escritorios virtuales, copias de seguridad, etc (CINTEL, 2010, pág. 6). Por lo cual no hay necesidad de instalar aplicaciones locales en un computador físico dejando que todo el manteamiento y actualizaciones recaigan sobre quien ofrece el servicio. El cloud computing no está libre de vulnerabilidades, riesgo y ataques, ya sean por agentes internos o externos, es por esto que se tratan de encontrar las estrategias que mitiguen las amenazas para dar un mejor servicio y ofrecer un servicio confiable con esta nueva tecnología (INCIBE, 2011, págs. 1-10).

El cloud computing o concepto de nube se fortalece con los grandes proveedores de internet como Google, Amazon AWS, Microsoft, etc. A partir del 2006 este servicio en la nube se ofrece de forma comercial a pequeñas, medianas y grandes empresas que paulatinamente comienzan a migrar los servicios, fortaleciendo el Cloud Computing año tras año. Una de las ventajas del cloud computing es que el proveedor del servicio es quien se encarga de dar soporte, ahorrando gasto al cliente. Pero conforme avanza el fortalecimiento del Cloud Computing con arquitecturas que gestionan mejor el servicio, siendo más rápidas o con mayor capacidad de manejo de archivos también aparecen los ataques, riesgos o vulnerabilidades para dichos datos, por lo que es importante saber el tipo de riesgo y como se manejan antes de escoger alguno de estos servicios.
En la actualidad hay muchos estudios y recopilación de información para caracterizar los diferentes tipos de ataques, algunos se clasifican en (UCATOLICA, 2019, pág. 7):

- ATAQUE DE DENEGACION DE SERVICIO DoS
- MALWARE DE INYECCION DE ATAQUE
- ATAQUES DE CANAL LATERAL
- ATAQUES DE AUTENTICACION

- ATAQUES CRIPTOGRÁFICOS

Otro concepto importante que aparece con el cloud computing es la vulnerabilidad con la cual vienen el riesgo y las amenazas potenciales dadas por fallos en el sistema o errores de configuración. Uno de los avances más significativos que se ha tenido en el campo del Cloud Computing es el desarrollo de herramientas de simulación que permiten evaluar algunas arquitecturas de la nube logrando así que los clientes hagan una evaluación previa y ajusten parámetros ya sea para mejorar el rendimiento, y reducir costos por el servicio prestado por el proveedor; así mismo, el proveedor por medio de estos simuladores puede crear diferentes escenarios de consumo controlando cargas que se reflejarán en diferentes escenarios de costos por lo que puede ofrecer mayor beneficio y optimización de recursos a sus clientes (UC3M, 2011, págs. 20-30).

Es importante, ofrecer al público una visión más amplia del concepto de Cloud Computing, su aplicabilidad, ventajas y desventajas, pero desde una perspectiva más objetiva que crítica. Es por ello que se trata de dar una serie de etapas a seguir con el fin de que el proveedor como el cliente pueda ofrecer o disfrutar el servicio. En este caso se espera identificar, evaluar, analizar y generar una serie recomendaciones para lograr que el cliente haga una selección óptima del servicio Cloud Computing que el mercado ofrece reduciendo la desconfianza en esta tecnología.

En la etapa de Identificación se recopila la información necesaria, en cuanto a ataques y vulnerabilidades de las arquitecturas más utilizadas de los servicios más conocidos, esto con el fin de que el cliente tenga un panorama más global de todos los servicios que hoy en día se ofrecen (UNIRIOJA, 2015, págs. 46-51).

En la etapa de Evaluación se hace un diagnóstico o una guía en el manejo de simuladores para algunos servicios de Cloud Computing con el fin de que el cliente tenga una opción de controlar algunos parámetros para reducir costos.

En la etapa de Análisis se observan los resultados de forma objetiva con el fin de disminuir el sesgo que se tenga por preferencia de algunos servicios que existen en el mercado.

Y como etapa final se generan recomendaciones con el fin de mejorar el servicio tanto para el cliente como para el proveedor a la hora de usar la nube para una determinada tarea.

Existen diferentes modelos de servicio de Cloud Computing, que se adaptan a diferentes necesidades y requisitos según lo requieran las empresas o usuarios que necesiten el servicio. Estos modelos son los siguientes (UNIPILOTO, 2015, págs. 1-7):

Software como servicio (SaaS): Es un modelo de prestación de software basado en la nube, en el cual el proveedor de nube desarrolla y mantiene un software de aplicaciones de nube, es el más usado por el cliente final.

Plataforma como Servicio (PaaS): Es un conjunto de servicios basados en la nube que permite a los desarrolladores y usuarios empresariales crear aplicaciones a una velocidad que las soluciones en las instalaciones no pueden alcanzar.

Infraestructura como Servicio (IaaS): Es un tipo de servicio de informática en la nube que ofrece recursos esenciales de proceso, almacenamiento y redes a petición que son de pago por uso (UTA, 2016, pág. 2).

Herramientas de Simulación de ataques: La simulación de ataques reales permiten revisar resultados y tomar medidas que ayuden a mejorar la infraestructura donde se ejecuta el servicio. Algunos de los simuladores más usados son:

- **Cymulate:** Es una plataforma basada en SaaS que automatiza la validación del control de seguridad bajo imitación de actores de amenazas bajo escenarios integrales (Seguridad América, s.f. , párrafo 1).

- **Infección Monkey:** Herramienta de código abierto que se instala en el sistema operativo como Windows, Debian y Docker. Ejecuta simulación por ataque automático por robo de credenciales, configuración incorrecta, etc. Dentro de los beneficios están: simulación de ataques no intrusivos, informe completo con recomendaciones, visualización de red y mapa de atacantes (GEEKFLARE, 2021, párrafo 1-2).

- **Randori:** Plataforma para simulación de ciberataques con un sistema automatizado y confiable con el fin de probar sistemas de seguridad. Dentro de los beneficios están: evaluación de soluciones, suministro de información, simulación de ataques reales, análisis en tiempo real, etc (MITRE ATT&CK, 2020).

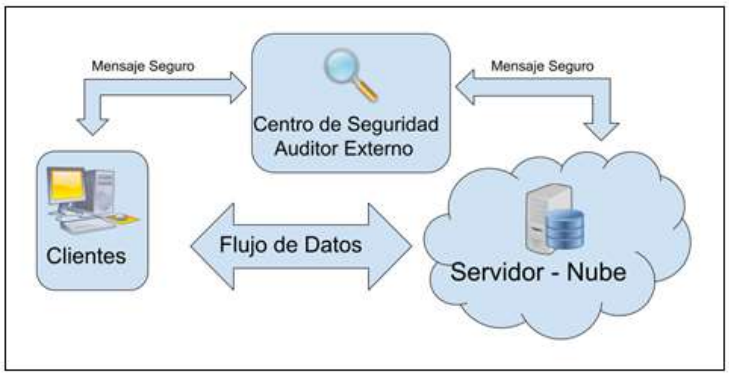


Figura 1. Arquitectura - Servicio Cloud Computing

Metodología

Actividades necesarias para alcanzar los objetivos planteados.

- **Etapa 1: Identificar las principales amenazas y vulnerabilidades de cloud computing de acuerdo al modelo de servicio público y privado en la infraestructura IaaS.**

  - ***Actividad 1.1:*** *Recolección de información de vulnerabilidades y ataques en seguridad como un factor de riesgo dado por diferentes escenarios de ataque como:*
    - ***Ejecución:*** En esta categoría los atacantes ejecutan los códigos maliciosos durante el tiempo de ataque (MITRE ATT&CK, 2020).
      - ***Interfaz de línea de comando:*** Esta ofrece una forma de interactuar con un sistema informático y así ejecutar software.
      - ***Ejecución a través de Módulo de carga:*** Se puede indicar al cargador de módulos de Windows que cargue archivos DLL desde rutas locales arbitrarias y rutas de red arbitrarias de la Convención de nomenclatura universal (UNC).
      - ***Ejecución a través de API:*** Funciones como las API permiten que programas y scripts ejecuten procesos en rutas adecuadas.
      - ***Powershell:*** Permite a los administradores de sistemas automatizar tareas de manera total sobre servidores y equipos sin necesidad de instalar un fichero para iniciar el ataque por lo que hace que sistemas de seguridad convencional no lo puedan detectar.
      - ***Scripting:*** Son códigos maliciosos que acceden a cookies, token e información confidencial que ayudan a la apertura de sesión que van ligados al navegador web.
      - ***Ejecución de Servicio:*** Los ataques usan el administrador de servicios de Windows para ejecutar comandos o instalar o manipular servicios, a menudo con niveles elevados de privilegios.

- ***Persistencia:*** Son técnicas que utilizan los atacantes para mantener el acceso a los sistemas a través de reinicios, cambios de credenciales y otras interrupciones para restringir el acceso (MITRE ATT&CK, 2020).
    - ***.bash_profile y. bashrc****: Son* scripts de shell que contienen comandos de shell y se ejecutan en el contexto de un usuario cuando se abre un nuevo shell o cuando un usuario inicia sesión.
    - ***Creación de Cuenta:*** En el ataque se crea una cuenta para mantener el acceso a los sistemas de las víctimas.
    - ***Archivos y directorios ocultos:*** Para ocultar archivos en el sistema para persistencia y evadir un análisis típico de usuario o sistema.
    - ***Programación de trabajos locales:*** Capacidad de crear trabajos en segundo plano periódicos y preprogramarlos usando varios mecanismos existentes.
    - ***Perfil PowerShell:*** Es una secuencia de comandos que se ejecuta cuando se inicia PowerShell (Interfaz de comandos) y se puede usar como secuencia de comandos de inicio de sesión para personalizar los entornos de los usuarios
    - ***Tarea programada:*** Existen utilidades dentro de todos los principales sistemas operativos para programar programas o scripts para que se ejecuten en fecha y hora específicas.
    - ***Setuid y Setgid:*** Permiten a los usuarios ejecutar un ejecutable con los permisos del sistema de archivos del propietario o grupo del ejecutable respectivamente y cambiar el comportamiento en los directorios.
- ***Evasión de defensa:*** Los atacantes eluden la detección ofuscando scripts maliciosos, escondiéndose en procesos confiables y deshabilitando el software de seguridad, entre otras estrategias (MITRE ATT&CK, 2020).
    - ***BITS de Trabajo:*** Servicio de transferencia inteligente en segundo plano (BITS), se encarga de simplificar y coordinar la carga y descarga de archivos de gran tamaño.
    - ***Modificación de permisos de archivos:*** Los adversarios pueden modificar los permisos/atributos de archivos o directorios para

evadir las listas de control de acceso (ACL) y acceder a archivos protegidos.

- ***Acceso de credenciales:*** Consiste en técnicas para robar credenciales como nombres de cuenta y contraseñas (MITRE ATT&CK, 2020).
    - ***Fuerza Bruta:*** Utiliza prueba y error para adivinar la información de inicio de sesión, las claves de cifrado o encontrar una página web oculta.
    - ***Inclinar Credenciales:*** Se intenta volcar las credenciales porque se puede usar para realizar movimientos laterales y acceder a información restringida.
    - ***Llaves Privadas:*** son ataques a sistemas informáticos que usan sistemas criptográficos en los que se buscan claves criptográficas privadas en la memoria del computador o en la memoria no volátil que se pueden utilizar para descifrar o firmar datos.

- ***Detección:*** Los atacantes conocen las herramientas de protección que tienen los usuarios y se desarrollan conforme a esto para poder pasar los controles de seguridad existentes (MITRE ATT&CK, 2020).
    - ***Detección de sistemas remotos:*** Los adversarios pueden intentar obtener una lista de otros sistemas por dirección IP, nombre de host u otro identificador lógico en una red que pueda usarse para el movimiento lateral del sistema actual.
    - ***Detección de sistemas de información:*** Se intenta obtener información detallada sobre el sistema operativo y el hardware, incluida la versión, los parches, las revisiones, los paquetes de servicio y la arquitectura.
    - ***Detección de configuración de red del sistema:*** Los adversarios pueden buscar detalles sobre la configuración y los ajustes de la red, como direcciones IP y/o MAC, de los sistemas a los que acceden o a través del descubrimiento de información de sistemas remotos.

- ***Movimiento lateral:*** El movimiento lateral es un medio para un fin donde se usan técnicas para identificar, obtener acceso y exfiltrar datos confidenciales (MITRE ATT&CK, 2020).
    - ***Explotación de servicios remotos:*** La explotación de una vulnerabilidad de software ocurre cuando el atacante aprovecha de un error de programación en un programa, servicio o dentro del software del sistema operativo.
    - ***Paso de hash:*** Es un método de autenticación como usuario sin tener acceso a la contraseña de texto claro por el usuario.
    - ***Copia de filas remotas:*** Los archivos pueden copiarse desde un sistema externo controlado por el atacante a través del canal de comando y control.
    - ***Servicios remotos:*** Los atacantes pueden usar cuentas válidas para iniciar sesión en un servicio diseñado específicamente para aceptar conexiones remotas.
- ***Colección:*** El atacante trata de recopilar datos de interés para cumplir su objetivo (MITRE ATT&CK, 2020).
    - ***Sistema local de datos:*** Los atacantes pueden hacer esto utilizando un intérprete de comandos y secuencias de comandos , como cmd , que tiene la funcionalidad de interactuar con el sistema de archivos para recopilar información.
- ***Control y Comandos:*** Consiste en técnicas que los atacantes pueden usar para comunicarse con los sistemas bajo su control dentro de una red de ataque (MITRE ATT&CK, 2020).
    - ***Proxy de conexión:*** Los adversarios pueden usar un proxy de conexión para dirigir el tráfico de red entre sistemas o actuar como intermediario para las comunicaciones de red a un servidor de comando y control.
    - ***Puertos de uso poco común:*** Los atacantes pueden usar puertos no estándar para filtrar información.
    - ***Multi-hop Proxy:*** En el caso de la infraestructura de red, particularmente los enrutadores, es posible que un atacante aproveche múltiples dispositivos comprometidos para crear una

cadena de proxy de múltiples saltos dentro de la red de área amplia (WAN).

- ***Exfiltración:*** Son técnicas que los adversarios pueden usar para robar datos de su red (MITRE ATT&CK, 2020).
  - ***Exfiltración sobre el canal de comando y control***: Los atacantes pueden robar datos exfiltrándolos a través de un canal de comando y control existente.

Es importante subrayar que las tácticas expuestas hacen referencia a nivel empresarial, debido a que, también existen a nivel móvil el cual manejan otras técnicas de ataques.

En la tabla 1 de Ejecución muestra una recopilación de los tipos de ataques según cada táctica. En esta encontramos las técnicas de ataques para empresas como para dispositivos móviles en diferentes plataformas como sistemas operativos Windows, Mac OS, Linux, Nube, Red. Para cada táctica las técnicas de ataques pueden variar, pero es importante conocerlos para tener una idea de los riesgos potenciales a los que puede estar expuesta cualquier plataforma. En anexo 1 se muestran todas las tablas de las tácticas con sus técnicas de ataques.

Tabla 1. Táctica de ejecución y técnicas de ataque (MITRE ATT&CK, 2020).

Execution						
PowerShell	JavaScript	Component Object Model	Cron	Software Deployment Tools	Malicious File	At (Windows)
AppleScript	Network Device CLI	Dynamic Data Exchange	Launchd	System Services	Malicious Image	Inter-Process Communication
Windows Command Shell	Container Administration Command	Native API	Scheduled Task	Launchctl	Windows Management Instrumentation	Python
Unix Shell	Deploy Container	Scheduled Task/Job	Systemd Timers	Service Execution	Malicious Link	Shared Modules
Visual Basic	Exploitation for Client Execution	At (Linux)	Container Orchestration Job	User Execution	No aplica	No aplica

- ***Actividad 1.2**: Filtrado de información con respecto a servicio público y privado en el servicio IaaS.*

  La infraestructura para servicio IaaS ofrece recursos como: Redes virtuales, almacenamiento virtual y máquinas virtuales accesibles a través de Internet. En la actualidad las organizaciones utilizan este tipo de servicio para aumentar los entornos locales como de nube privada.

  Una de las ventajas del servicio IaaS es la escalabilidad y flexibilidad de hardware y por esta razón la infraestructura puede expandirse si el cliente lo desea o reducirse en caso de querer cambiarlo, lo cual, no es posible hacer escalabilidad a nivel de hardware local.

  Los ataques a este tipo de servicio, cuyo objetivo principal es secuestrar recursos, puede terminar en denegación del servicio con el fin de robar documentos, archivos para filtración, etc.

  Es importante resaltar que el cliente es responsable de sus datos, accesos, aplicaciones, configuración sistema operativo, tráficos de red, etc. En cuanto a las organizaciones los errores más comunes están sobre los datos sin cifrar los cuales son vulnerables para los atacantes. También están los errores de configuración que influyen directamente sobre los recursos de la nube los cuales son los más comunes, servicios de sombra cuentas ocultas en la nube y permisos basados en roles de usuarios que restringen los usuarios para acceder a las credenciales (MITRE ATT&CK, 2020).

  El proveedor junto con el profesional de las tecnologías de la información son los encargados de ofrecer protección de los recursos y dar soporte a puertos de entrada, autenticación multifactor, cifrado, acceso abierto a almacenamiento a internet, etc.

  Los problemas de seguridad en las organizaciones se dan por el uso de varios servicios como IaaS, PaaS y SaaS de varios proveedores debido a que las soluciones de seguridad están diseñadas para un tipo de nube

específico. Para solucionar estos problemas de seguridad se tienen las siguientes soluciones:

- **Agentes de seguridad de acceso a la nube:** Conocido como puerta de enlace de seguridad en la nube, encargado de controlar recursos en la nube, monitoreo de actividades de usuario, detección de malware y pérdidas de datos y cifrados.
- **Plataformas de protección de cargas de trabajo en la nube:** Encargado de descubrir cargas de trabajo y contenedores aplicando protección contra malware.
- **Plataformas de seguridad de redes virtuales**: Da soluciones de tráfico de red incluyendo detección y prevención de intrusiones en la red.
- **Gestión de posturas de seguridad en la nube:** Encargado de auditar los entornos de nube de IaaS en busca de problemas de seguridad.

Una de las cosas importantes es evaluar los proveedores de las IaaS por medio de los administradores de las tecnologías de la información en función de:

- Permisos de acceso físico
- Auditorías de cumplimiento
- Herramientas de seguimiento y registro
- Especificaciones y mantenimiento del hardware

En la tabla 2 se observa claramente que las técnicas que más prevalecen son las que están ligadas a la nube debido a que la arquitectura IaaS prevalece más en esta.

En el anexo 2 se presentan tablas de diferentes plataformas alojadas en la nube donde se encuentran las tácticas más usadas con sus diferentes técnicas de ataques.

Tabla 2. Táctica y técnicas de ataque para IaaS (MITRE ATT&CK, 2020).

Acceso Inicial	Ejecución	Persistencia	Escalada de privilegios	Evasión de defensa	Acceso a Credenciales	Descubrimiento	Movimiento lateral	Colección	exfiltración	Impacto
Aprovechar la aplicación orientada al público	Ejecución de usuario	Manipulación de cuenta	Cuentas Válidas	Debilitar defensas	Fuerza bruta	Descubrimiento de cuenta	Usar material de autenticación alternativo	Datos del objeto de almacenamiento en la nube	Trasferir datos a la cuenta de la nube	Destrucción de datos
Relación de confianza		Crear cuenta		la infraestructura informática en la nube	Forjar credenciales web	Descubrimiento de infraestructura en la nube		Datos de repositorios de información		Datos cifrados para impacto
Cuentas Válidas		Imagen interna del implante		Regiones de la nube no utilizadas o no admitidas	Credenciales no seguras	Tablero de servicios en la nube		Datos por etapas		Desfiguración
		Cuentas Válidas		Usar material de autenticación		Detección de servicios en la nube				Denegación de servicio de punto final
				Cuentas Válidas		Detección de objetos de almacenamiento en la nube				Denegación de servicio de red
						Escaneo de servicios de red				Secuestro de recursos
						Descubrimiento de políticas de contraseñas				
						Descubrimiento de grupos de permisos				
						Descubrimiento de software				
						Descubrimiento de información del sistema				
						Descubrimiento de la ubicación del sistema				
						Detección de conexiones de red del sistema				

- ***Actividad 1.3**: Análisis de información para mostrar en escala el impacto y las vulnerabilidades en la nube.*

  En la tabla 3 se observa los ataques en plataformas alojadas en la nube, y la cantidad de técnicas que se han utilizado entre octubre de 2018 y Julio de 2019 (MITRE ATT&CK, 2020), del cual, la plataforma bajo la arquitectura IaaS es la que más ataques tiene.

Tabla 3. Técnicas y tácticas para plataformas en Nube (MITRE ATT&CK, 2020).

Plataforma Nube	Office 365	Azure AD	Google Workspace	SaaS	IaaS
Técnicas de Ataque	28	19	24	23	40

En la figura 2 se muestra un gráfico de la tabla 3, el cual, expone con detalle lo anteriormente expuesto.

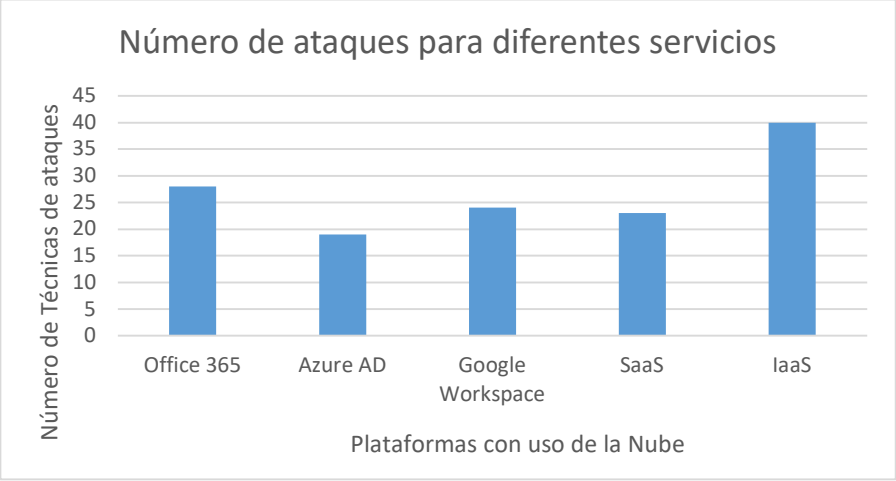


Figura 2. Plataformas – Uso de nube y ataques

A continuación, se muestran las gráficas de cada una de las plataformas y la cantidad de ataques y la relevancia que presentaron entre los años 2018 y 2019 (MITRE ATT&CK, 2020). En estas gráficas se observa el

comportamiento de los ataques, según las tácticas y como varían por plataforma en la cantidad de técnicas usadas.

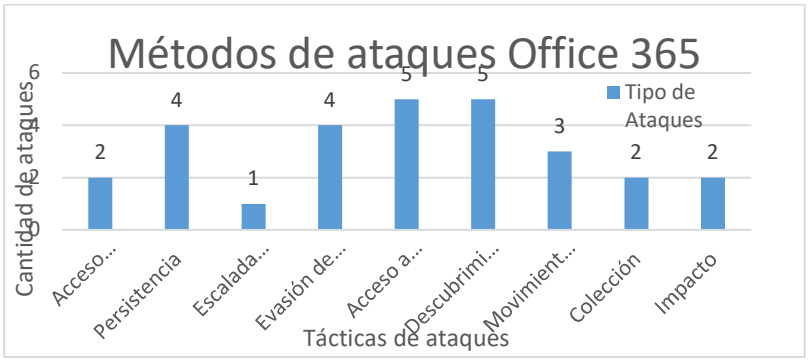


Figura 3. Gráfico métodos de ataques - Office 365

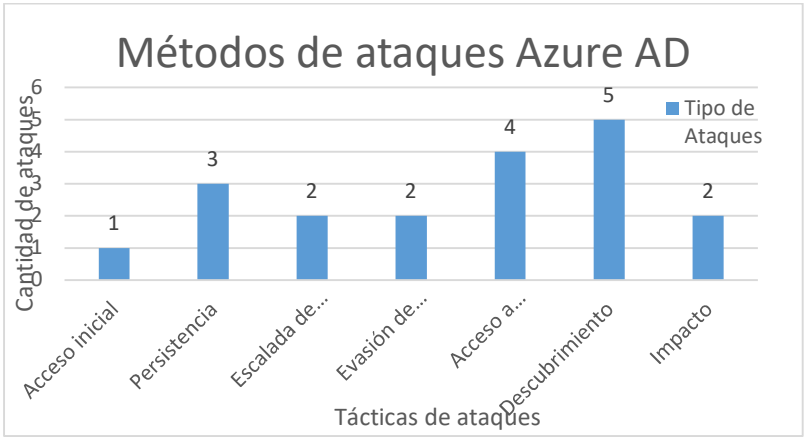


Figura 4. Gráfico métodos de ataques – Plataforma Azure AD.

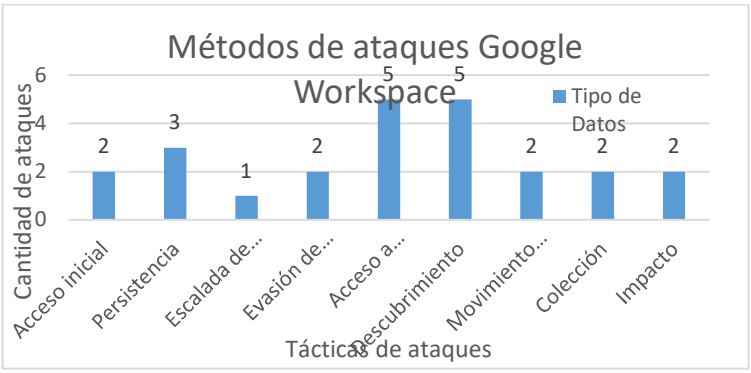


Figura 5. Gráfico métodos de ataques – Plataforma Google

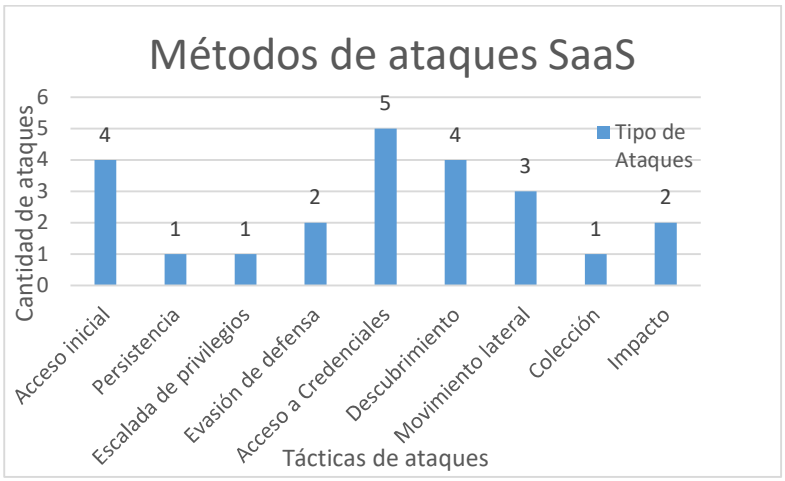


Figura 6. Gráfico métodos de ataques – Estructura SaaS

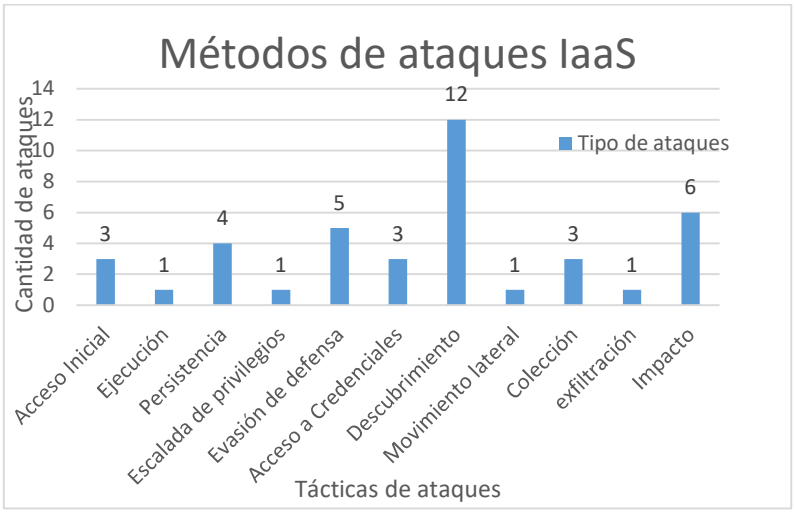


Figura 7. Gráfico métodos de ataques – Estructura IaaS.

- **Etapa 2: Evaluar en un entorno virtual de carácter experimental amenazas derivadas de la tecnología y vulnerabilidades presentes en el modelo y servicio cloud computing IaaS.**

  - ***Actividad 2.1***: *Presentación del simulador para análisis de ataque en el servicio IaaS.*

Infection Monkey: Es un proyecto de código abierto que sirve como herramienta de simulación de ataque y violación de los entornos de basados en la nube sin importar si son públicos o privados. Este simulador proporciona varios beneficios para las organizaciones que empleen la herramienta generando resultados cuantificables que ayudan a evaluar los riesgos y vulnerabilidad de la seguridad que tenga una organización (ITCOMUNICACIONES, 2020).

Con infection Monkey se pueden resumir 3 pasos a la hora de evaluar la seguridad:

1. Simulación de ataque automático: En este caso podemos simular la infección de una máquina de manera aleatoria y descubrir los riesgos de seguridad. Se pueden simular varias técnicas de ataque como robo de credenciales, manipulación de cuentas, etc.
2. Evaluación Continua y segura: El simulador puede ejecutarse las 24 horas del día evaluando nuevos riesgos validando los controles de seguridad que tenga la máquina.
3. Recomendaciones procesales: Da como resultado un informe detallado con mapa visual de red con sugerencias de corrección de seguridad.

- ***Actividad 2.2****: Tutorial de manejo y lectura de resultados del simulador.*

El simulador Infection Monkey puede implementarse en diferentes entornos como a nivel local en sistemas operáticos como Windows y Linux, también puede usarse en plataformas Docker que emplean contenedores virtualizados en un sistema operativo. Una de las ventajas que también tiene Infection Monkey es poder desplegarse en servicios que usan la Nube como Azure y AWS lo cual nos permite simular ataques a estas plataformas y conocer los resultados de seguridad para verificar su viabilidad a la hora adquirir sus servicios (GUARDICORE, s.f.).

Dada la importancia del uso de la nube para el despliegue de apps y administración de servicios que se ha dado en los últimos años, y que tanto AWS como Azure son los que mayor infraestructura y despliegue pueden

ofrecer, Infection Monkey se adecua perfectamente para este tipo de análisis ya que su implementación en estos servicios es relativamente sencilla. Para este caso se ha tomado como referencia el Servicio en la nube de AWS tanto para simulación, evaluación y recomendaciones haciendo énfasis que para Azure el procedimiento es similar.
A continuación, se muestran los pasos para implementar Infection Monkey en AWS.

1. Crear cuenta en AWS

   Ingresamos a la página oficial de AWS, https://aws.amazon.com/es. El registro en AWS es relativamente sencillo, pero, se recomienda tener cuidado al elegir el tipo de suscripción ya que hay algunas que son gratuitas y otras que generan un cobro a la tarjeta de crédito inscrita. En el apéndice 1 se muestra una guía para la correcta suscripción.

2. Suscripción y configuración Infection Monkey en AWS Marketplace.

   AWS Marketplace es una tienda de catálogo digital en línea, fácil de comprar y rápida implementación. Las ventajas de este catálogo consisten en que sus softwares están optimizados para funcionar en AWS por lo que se facilita su configuración y uso. La suscripción de la puede hacer en https://aws.amazon.com/marketplace y seguir los pasos que indica la plataforma como los mostrados en la figura 8. Para una correcta configuración se debe tener en cuenta:

   Elección de Instancia: Es la capacidad que tiene la máquina virtual y sus prestaciones en cuanto a CPU, memoria RAM, almacenamiento, etc. Una característica importante es que dependiendo de la potencia de esta máquina virtual incrementara el costo por su uso.

   Configuración de instancia: Es una parte importante debido a que se escoge el sistema operativo, arquitectura, versión y región donde se encuentra esta máquina virtual.

   Configuración VPC: Consta de crear una red para la instancia creada en donde se aloja el simulador y de donde iniciara el ataque. Se

recomienda tener conocimiento previo en implementación de máquinas virtuales y configuración de red VPN

Entrada de tráfico y puertos: Se configura la entrada o salida de tráfico, para el caso de esta simulación se habilita todo el flujo de datos, lo cual es una desventaja ya que el atacante tiene vía libre para atacar.

Dashboard de Infection Monkey: Si la configuración se realizó de forma correcta bastará con escribir la siguiente dirección https://Ip_local_instancia:5000 en un navegador Web para poder ingresar y comenzar a usar el simulador. En el apéndice 2 se muestra un guía para la correcta suscripción y configuración.

Figura 8. Diagrama – Configuración Infection Monkey

3. Montaje de red en la nube de AWS.

   Como Infection Monkey se configuró en AWS podemos aprovechar para diseñar una red básica en la nube con el fin de hacer la simulación de ataque. A continuación, se presenta una red simple que consta de 3 máquinas virtuales 2 Linux y 1 Windows con sus respectivas IP como se muestra en la figura 9.

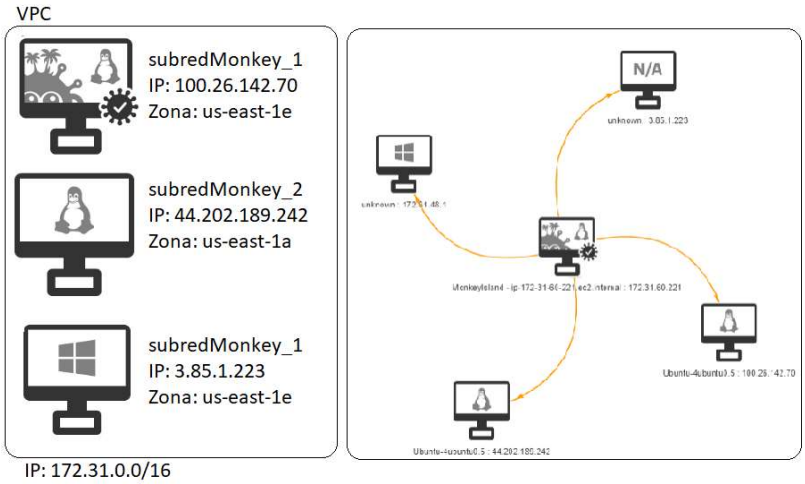


Figura 9. Configuración de Red – Simulación

En la figura 10 se puede configurar ciertos parámetros para que el simulador comience con la red antes configurada. En este caso se puede dar información la IP de la red principal, como también usuarios, contraseñas y dirección de repositorios simulando que el atacante intuye cierta información para que el ataque sea más certero.

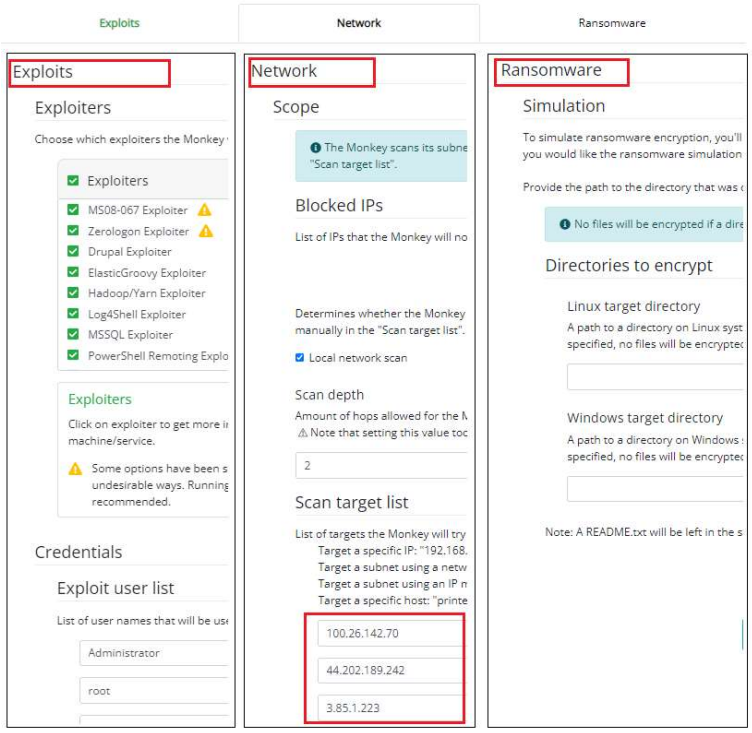


Figura 10. Configuración Infection Monkey – Simulación

- ***Actividad 2.3**: Tabla de amenazas y vulnerabilidades a simular.*

  En la figura 11 se puede observar que tipo de tácticas y técnicas de ataques usa Infection Monkey y los clasifica de la siguiente manera.

  - ✓ Rojo: Usó con éxito la técnica de simulación.
  - ✓ Amarillo: Se trató de usar la técnica, pero fallo.
  - ✓ Gris oscuro: No probó la técnica por no tener relevancia.
  - ✓ Gris Claro: No probó la técnica porque no está configurada.

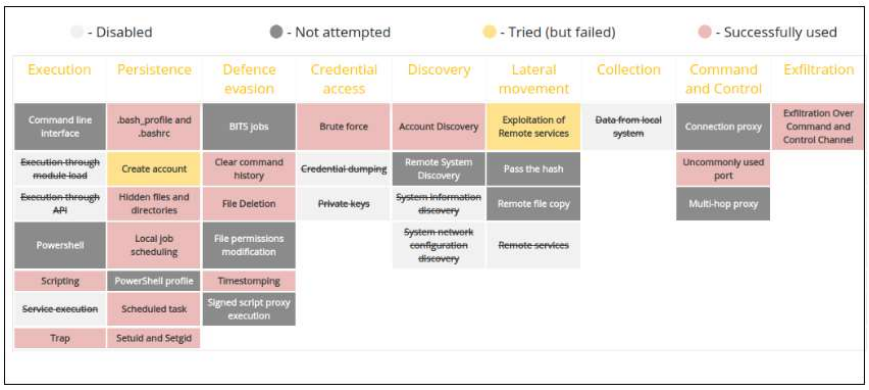


Figura 11. Tabla de tácticas y técnicas de ataque (GUARDICORE, s.f.)

- ***Actividad 2.4**: Recolección de información de forma ordenada para posterior análisis.*

  De la figura 12 se puede observar que muchas de las tácticas de ataques no se ejecutaron como: Ejecución, persistencia, evasión de defensa y colección. En cambio, las tácticas acceso con credenciales, descubrimiento, movimiento lateral, exfiltración y comando y control se ejecutaron de forma adecuada, aunque no todas sus técnicas fueron usadas.

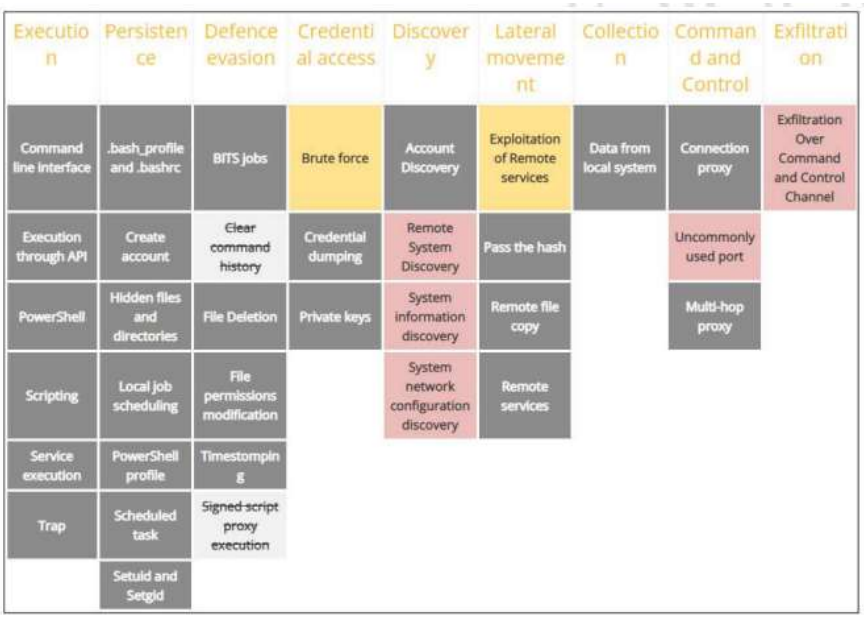


Figura 12. Tabla de resultados de ataques – Simulación (GUARDICORE, s.f.)

En la tabla 4 se muestra una descripción detallada de las tácticas y ténicas usadas en la simulación de ataque a la red que se configuro previamente.

Tabla 4. Técnicas y tácticas – Resultados simulador

Táctica	Técnica	Observación Simulador
Acceso con credenciales	*Fuerza bruta*	Usó la fuerza bruta en algunos servicios, pero falló.
Descubrimiento	*Descubrimiento de Sistemas Remotos*	Encontró máquinas en la red de forma fácil y rápida.
	Descubrimiento de información del sistema	Reunió información del sistema de las máquinas en la red de forma fácil
	Detección de configuración de red del sistema	Reunió configuraciones de red en los sistemas de la red de manera fácil.
Movimiento lateral	*Explotación de servicios remotos*	Buscó servicios remotos en la red, pero no pudo explotar ninguno.

Comando y control	*Puerto de uso común*	Usó el puerto 5000 para comunicarse con el servidor EC2 lo cual le da acceso directo.
Exfiltración	*Exfiltración sobre canal de comando y control*	Extrajo información a través del canal de comando y control lo cual lo hace vulnerable.

- **Etapa 3: Analizar los resultados a partir de estrategias dentro de un plan de gestión de riesgos para mitigación y protección de cloud computing.**

  - ***Actividad 3.1****: Presentación de* resultados *de forma gráfica de fácil compresión para proveedor y cliente*.

    El simulador Infection Monkey emplea el marco de seguridad Zero Trust (confianza Zero). El objetivo de Zero Trust es proteger los datos usando múltiples componentes que impidan la filtración a terceros (ONISTEC, 2021). Estos componentes como se observa en la figura 13 están distribuidos de tal forma que todos los dispositivos y usuarios se clasifican como no fiables permitiendo así primero hacer una validación, dar privilegios mínimos, y asumir siempre que hay atacantes dentro o fuera de la red. Con el modelo Zero Trust podemos encontrar 4 áreas a proteger que son:

    1. Personas: empleados, invitados a la oficina, socios, clientes, actores maliciosos
    2. Cargas de trabajo: aplicaciones, movimiento y procesamiento de datos
    3. Redes: los datos de las rutas digitales se mueven a lo largo del ciclo de vida.
    4. Dispositivos: móvil, computadora de escritorio, tableta o cualquier dispositivo que se conecte a Internet.
    5. Datos: el contenido real que Zero Trust se centra en proteger.

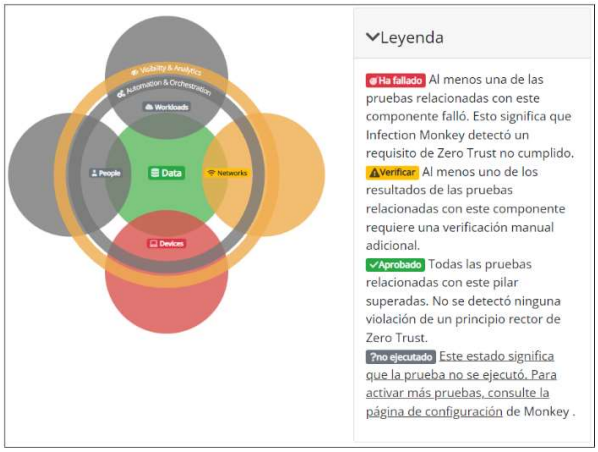


Figura 13. Infection Monkey - Zero Trust

- ***Actividad 3.2:*** *Hacer un diagnóstico general del potencial riesgo en cuanto amenazas y vulnerabilidades según los resultados de simulación.*

  Infection Monkey hace un reporte de seguridad compuesto por:

  - Reporte de secuestro de datos
    - ✓ Incumplimiento: Cuando una máquina que este dentro de la red el ataque de secuestro de datos comienza. En este caso inicia el ataque en la red con IP privada 172.31.60.221 que corresponde a la red del VPC donde se conectan los demás equipos.

    - ✓ Movimiento lateral: Una vez el atacante descubre un segmento de la red vulnerable, comienza el ataque lateral con el fin de comprometer otros segmentos de red. En este caso Infection Monkey no consigue vulnerar ninguna de las 6 máquinas que están dentro de la red como se observa en la figura 14.

Figura 14. Reporte secuestro de datos-Movimiento lateral

- ✓ Ataque: Una vez el atacante tiene acceso a las redes intentará poner en riesgo los datos cifrándolos con el fin de pedir rescate al usuario. Para este caso Infection Monkey no ha conseguido cifrar ningún archivo.

- Reporte de seguridad

  Una visión de conjunto en la red configurada muestra que no se presentaron problemas críticos de seguridad, a pesar de que los ataques se propagaron por toda la red. El simulador intentó acceder por fuerza bruta con usuarios y contraseñas dadas. Infection Monkey uso los siguientes métodos de explotación para vulnerar la seguridad inspeccionando las IP dadas en la configuración previa.

  - ✓ Explotador de PYMES
  - ✓ Explotador de WMI
  - ✓ Explotador de SSH
  - ✓ Explotador Log4Shell
  - ✓ Explotador de ShellShock
  - ✓ Explotador SambaCry
  - ✓ Explotador Groovy Elástico
  - ✓ Explotador de Struts2
  - ✓ Explorador de Oracle WebLogic
  - ✓ Hadoop/explotador de hilos
  - ✓ Explotador de puerta trasera VSFTPD
  - ✓ Explotador de MSSQL
  - ✓ Explotador de servidor Drupal
  - ✓ Explotador remoto de PowerShell
  - ✓ Explotador de conficker
  - ✓ Explotador de inicio de sesión cero

  En forma general Infection Monkey no descubrió amenazas, pero si algunos problemas de seguridad debido a una segmentación de red débil.

- Reporte de cero confianzas
  El informe de confianza cero está compuesto de 7 pilares, los cuales, infection Monkey inspecciona de forma individual y los resultados son como se muestra en la tabla 5. En el apéndice C se muestran los resultados con más detalle.

Tabla 5. Áreas y estados – Zero Trust

ítem	Área	Estado
1	Datos	Aprobado
2	Usuarios	No ejecutado
3	Redes	Verificar
4	Dispositivos	Fallado
5	Carga de trabajo	No ejecutado
6	Visibilidad y análisis	Verificar
7	Automatización y orquestación	No ejecutado

En forma general se observa que la configuración de red, equipos y el tráfico por la red son vulnerables.

- Reporte de tácticas y técnicas de ataques.
  En este reporte como se puede observar de la tabla 6, Infection Monkey detalla los resultados de las técnicas usadas para los ataques indicando el estado de la técnica y su posible mitigación que el usuario debe hacer. En el apéndice D se muestran los resultados con más detalle.

Tabla 6. Reporte técnicas y ataques

Táctica	Técnica	Estado Técnica	Mitigación
Acceso con credenciales	*Fuerza bruta*	Verificación Fallida	No aplica
Descubrimiento	*Descubrimiento de Sistemas Remotos*	Verificación Exitosa	Identificar las utilidades de los sistemas innecesarios para adquirir información en los sistemas disponibles.
	Descubrimiento de información del sistema	Verificación Exitosa	Identificar las utilidades de los sistemas innecesarias para adquirir información sobre los sistemas operativos.
	Detección de configuración de red del sistema	Verificación Exitosa	Identificar las utilidades de los sistemas innecesarias para adquirir información sobre configuración de red de un sistema.
Movimiento lateral	*Explotación de servicios remotos*	Verificación Fallida	No aplica
Comando y control	*Puerto de uso común*	Verificación Exitosa	Diseñe secciones de red para aislar sistemas, funciones o recursos críticos. Usar firmas de detección de intrusos para bloquear tráfico.
Exfiltración	*Exfiltración sobre canal de comando y control*	Verificación Exitosa	Usar firmas de detección de intrusos para bloquear tráfico en los límites de la red.

- **Etapa 4: Generar recomendaciones para minimizar los riesgos dentro de los servicios de cloud computing.**

  - ***Actividad 4.1**: Enumerar las recomendaciones que estén dirigidas al cliente final.*

    Es claro notar que cualquier vulnerabilidad en los servicios cloud deben ser abordados de una forma responsable, que garantice la fiabilidad de los datos que los clientes manejen.

    Según las simulaciones de Infection Monkey sobre AWS y las configuraciones que se hacen a la red se toman basado en el reporte de seguridad que el simulador da. Vistas desde el cliente serían las siguientes:

    - Reporte de secuestro de datos
      - ✓ El ataque comenzó sobre la red principal y las maquinas conectadas a ella, por lo que es primordial segmentar las redes para que el atacante no tenga control de todo el sistema.
      - ✓ Luego de acceder a la red el atacante identifica las máquinas conectadas a ellas, en la simulación el atacante descubrió 6 máquinas conectadas, aunque no tuvo éxito a la hora de violar la seguridad por lo que es importante cifrar los archivos con usuarios y contraseñas.
      - ✓ Una vez el atacante descubre las máquinas conectadas intentó acceder a los archivos, pero sin éxito.

    - Reporte de seguridad

      En este caso el atacante encuentra posibles problemas de seguridad, aunque en la simulación no logra explotarlas, pero logra identificar un problema en la red de segmentación débil. Por lo que se recomienda hacer una segmentación de red con el fin de evitar que las máquinas tengan una comunicación entre sí.
    - Informe de confianza cero
      - ✓ Datos: El atacante intenta tener acceso a los servidores sin cifrar, por lo que se recomienda tener datos cifrados o tener copias de seguridad en caso de daño de estos.

- ✓ Gente: Se intenta crear un nuevo usuario para acceder por medio de él, por lo que se recomienda tener un proceso de autenticación seguro.
- ✓ Redes: El atacante intenta escanear la red con el fin de explotar su vulnerabilidad por lo que se recomienda escanear el tráfico de red en busca de actividad maliciosa.
- ✓ Dispositivos: El atacante intenta explotar las máquinas que encontró en la red e intenta explotar su vulnerabilidad para comenzar un ataque conjunto a todas las máquinas. En este caso se recomienda tener un antivirus de seguridad en los endpoints.
- ✓ Cargas de trabajo: El atacante creará un usuario para tener comunicación con la red y llegar a las máquinas, por lo que se recomienda tener una autenticación segura.
- ✓ Visibilidad y análisis: El atacante realiza acciones maliciosas en la red como canalizar el tráfico de red para poder explotar su vulnerabilidad por lo que se recomienda analizar el tráfico, tener permisos de usuarios y un inicio de sesión seguro.
- ✓ Automatización y registro: Se intenta buscar problemas en a la seguridad del servicio por lo que se recomienda tener un monitoreo e inicio de sesión en los recursos de la red.

- Reporte de tácticas y técnicas de ataques
  En este caso el simulador da puntualmente ciertas recomendaciones a seguir para mitigar la técnica de ataque echa por el atacante. Muchas de estas fueron expuestas en la tabla 6 o el apéndice D.

➢ ***Actividad 4.1**: Enumerar las recomendaciones que estén dirigidas al proveedor.*

En el caso del proveedor dentro de los servicios en la nube y su configuración se dan las siguientes recomendaciones:

A pesar de que la mayoría de configuraciones las puede hacer el usuario en el caso de AWS, no todas son intuitivas y se necesita tener un conocimiento previo de manejo de redes, seguridad, sistemas operativos, máquinas virtuales, etc. Lo que conlleva al cliente a cometer errores de configuración que más tarde pueden ser aprovechados por los atacantes.

Es por esta razón que estos servicios deberían ser segmentados de tal forma que dependiendo del cliente o empresa se le dé una asesoría adecuada para un manejo correcto de los servicios ofrecidos.

Resultado y análisis

La simulación de ataques a un sistema cloud computing directamente relacionado con la configuración de la red, configuración del simulador y lectura correcta de resultados.

Configuración de la red: Una de las principales recomendaciones al momento de implementar una red es la segmentación de esta, con el fin de evitar una propagación del ataque a todos los sistemas que componen esta red. En el caso de la simulación se implementa una red simple sin segmentar conformada por una red principal y 3 máquinas virtuales alojadas en la nube con sistemas operativos diferentes con el fin de darle vía libre al atacante y tener un mayor impacto en las vulnerabilidades de seguridad del sistema.

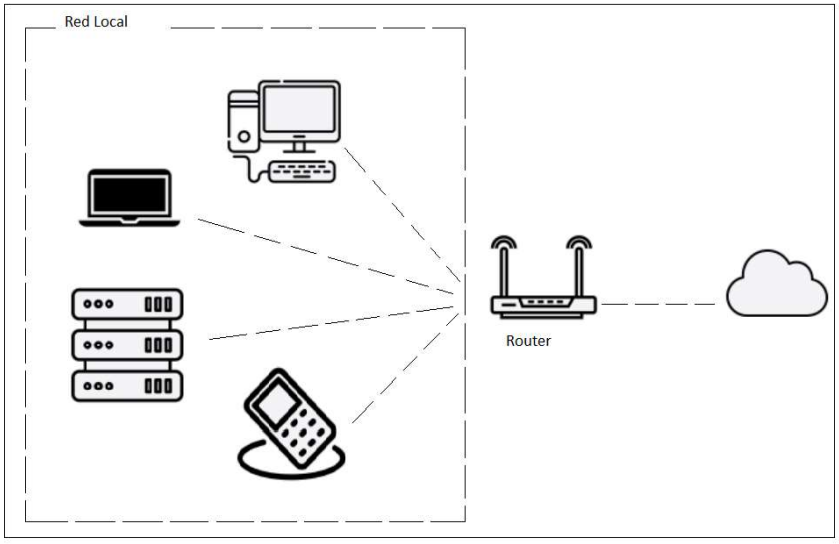


Figura 36. Configuración red – Sin segmentación

En la figura 36 se observa una configuración típica de red, el cual el atacante una vez identifique la red intenta vulnerar su seguridad para tener acceso a los dispositivos los cuales están interconectados entre sí.

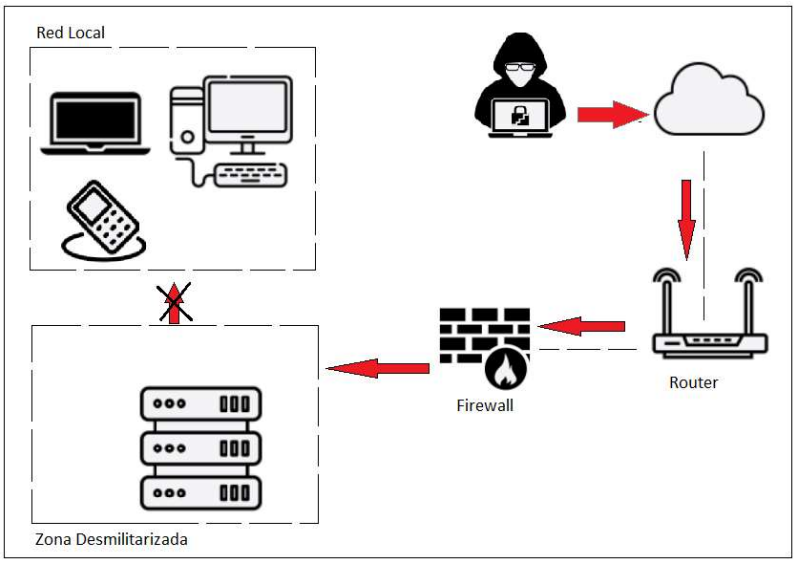


Figura 37. Configuración red – Con segmentación

En la figura 37 se puede observar un tipo de red segmentada con una zona desmilitarizada que es una red aislada que se encuentra dentro de la red interna con recursos accesibles a la nube. Por el contrario, las conexiones desde la zona desmilitarizada con la red local no están permitidas. Es importante puntualizar que en el caso de AWS se pueden hacer todas estas configuraciones de red con el fin de mitigar el riesgo a que atacantes puedan acceder a las máquinas y tener el control de estas.

Simulación y resultados: El funcionamiento correcto del simulador está muy ligado a la correcta configuración de la red y montaje de la máquina virtual donde se implemente Infection Monkey. Es importante resaltar que para la configuración es necesario tener conocimiento previo del manejo de servicios en AWS, lo que facilita el despliegue del simulador de forma adecuada. Uno de los temas a profundizar es la configuración de EC2 (Elastic Compute Cloud) el cual permite alquilar o usar computadoras virtuales para ejecutar aplicaciones o servicios. También es importante la configuración correcta del VPN (red privada virtual) que sirve para conectar dos o más redes con el fin de que empresas o usuarios puedan conectarse a diferentes redes.

Infection Monkey se despliega correctamente si, las configuraciones fueron correctas y nos permite el ingreso por medio de su Dashboard, que se

encuentra alojada en la red VPN principal por medio del puerto 5000. La configuración del simulador está basada en explotar vulnerabilidades de las máquinas por medio nombres, usuarios, y contraseñas usando fuerza bruta de SSH (Secure Shell). Dentro de las configuraciones está el escaneo de red a ser vulneradas, por lo que se le da la IP de la VPN principal, simulando que conocemos dicha IP con anterioridad. Y como configuración final está la de secuestro de datos (ransomware) que permite penetrar en un directorio y cifrar su contenido para tener control de los archivos o documentos que contenga dicho directorio. Estas configuraciones son importantes debido a que ayudan al usuario hacer un seguimiento con puntos específicos del ataque.
Dentro de los resultados el simulador da un informe de seguridad muy detallado, siendo necesario tener un conocimiento previo del tema para poder comprender y aplicar las recomendaciones hechas, y de esta forma, mejorar la seguridad a futuro.

Simulador como alternativa de seguridad: Una vez generada una tabla de resultados se puede inferir que la presencia de ataques es inevitable, por lo que es importante tener control de la seguridad o hacer un análisis previo de los riesgos que puede tener la red donde se despliegan los servicios debido a que pueden estar en riesgo archivos, datos, usuarios, etc. Infection Monkey muestra una serie de resultados para su posterior análisis y da una idea general de las vulnerabilidades presentes, por lo que se puede tener como alternativa de seguridad un servicio de simulador de ataques, con el fin de mitigar los riesgos que se pueden presentar antes de prestar un servicio a un cliente final.

Precios por el servicio de simulación:
Los precios de del simulador están ligados a la plataforma de servicios donde se despliegue, en este caso se hace referencia a AWS.

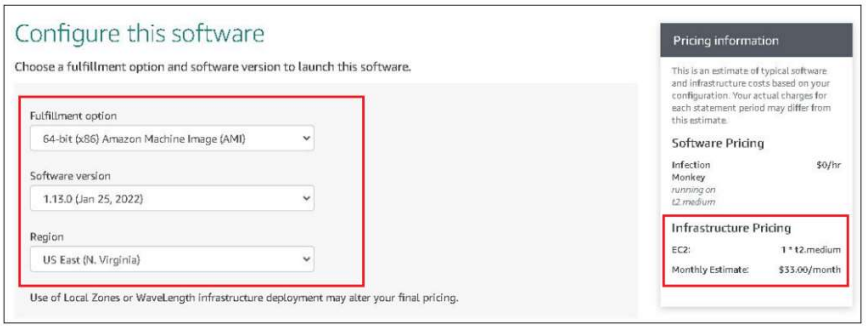


Figura 38. Precio – Infection Monkey

En la figura 38 se muestra el precio de la implementación de máquina virtual, como la suscripción a infection Monkey. Es importante recalcar que el precio varía dependiendo de los servicios y la infraestructura de la máquina virtual. Para este caso se ha escogido una configuración de bajo costo con prestaciones básicas lo cual da los resultados esperados, que como cliente final o proveedor es para tomarlo a consideración.

Conclusiones

Dentro de todo el proceso de conocer, aplicar y verificar los resultados y vulnerabilidades en un sistema cloud computing usando un simulador se tiene las siguientes conclusiones.

- Existen una gran variedad de servicios de cómputo en la nube, pero los más conocidos son AWS, Google Cloud y Azure.

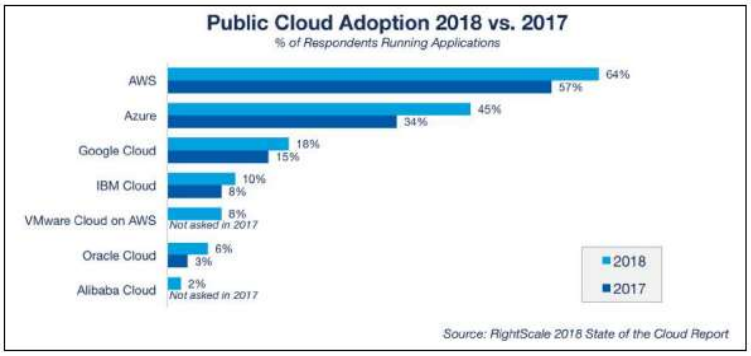


Figura 39. Técnicas y tácticas de ataque – Exfiltración (SEEKING ALPHA, 2018)

En la figura 39 se puede analizar que existen otros servicios en la nube, los cuales se pueden explorar y poner a prueba sus sistemas de seguridad y tener mejor elección como usuario final.

- Una de las cosas a tener en cuenta son los servicios ofrecidos por cada plataforma y cuáles son sus ventajas y desventajas a la hora de poner en marcha un servicio. Para esto se hace un comparativo entre las 3 plataformas más usadas.

  Pros y contras de AWS

  - ✓ AWS es una empresa dominante de servicios en la nube debido a que es el que más tiempo lleva en el mercado.
  - ✓ Tiene una gran cobertura esto es debido a la gran cantidad y variedad de servicios que ofrece.
  - ✓ Una relativa desventaja es el costo por adquirir sus servicios, aunque hay muchos de uso gratuito o de costo mínimo.

  Pros y contras de Microsoft Azure

  - ✓ Un gran salto por parte de Microsoft es la reutilización de sus servicios como Windows server, office, SQL serve, etc. Estos ya existían, pero fueron implementados para que funcionen en la nube.
  - ✓ Una característica importante de Azure es que sus servicios se implementan en el sistema operativo Windows lo que hace que sus servicios y los de Microsoft se integren de una forma más versátil para el usuario. En cuanto a nivel empresarial muchos optan por tener licencias del sistema operativo Windows, y se puede adquirir paquetes completos con servicios Cloud con un descuento en sus servicios.
  - ✓ En muchas comunidades a nivel global existen quejas con los servicios cloud y problemas de soporte técnico, documentación, etc.

Pro y contras de Google Cloud

- ✓ Dentro de los servicios están computación para Big Data e inteligencia artificial, con tiempos de respuesta rápido.
- ✓ Una de las principales desventajas es los pocos servicios ofrecidos, debido a su reciente ingreso al mercado Cloud.

- La configuración de seguridad del servicio Cloud Computing basado en la plataforma de AWS es relativamente fácil, debido a que en la consola se presentan todas las herramientas necesarias para dicha configuración. Es necesario tener un conocimiento básico de manejo de máquinas virtuales y configuración de red debido a que, de esto depende la seguridad de los datos o información importante que se debe proteger. En el caso de AWS se puede inferir que parte de las vulnerabilidades de seguridad están dadas por una mala configuración por parte del usuario o cliente final.

- La implementación y puesta en marcha del servicio es una de las grandes ventajas de este simulador debido a su fácil configuración y lectura de resultados, debido a que, Infection Monkey da un detallado y ordenado informe de resultados con sus respectivas recomendaciones. Igualmente se recomienda tener un conocimiento básico del tema para poder interpretar de forma adecuada el informe de resultados y no pasar por alto cualquier recomendación que más tarde implicará grandes costos por filtración de datos o información importante.

Referencias bibliográficas

Cintel. (2010). *CLOUD COMPUTING UNA PERSPECTIVA PARA COLOMBIA* [versión PDF]. Cintel Gobierno Digital: https://cintel.co/

Geekflare. (2021). *9 Cyber Attack Simulation Tools to Improve Security*. cyberattack-simulation-tools: https://geekflare.com/

Guardicore. (s.f.). *INFECTION MONKEY DOCUMENTATION HUB*. docs: https://www.guardicore.com/

Guardicore. (s.f.). *MITRE ATT&CK REPORT*. docs: https://www.guardicore.com/

INCIBE. (2011). *RIESGOS Y AMENAZAS EN CLOUD COMPUTING* [versión PDF]. Seguridad en cloud, seguridad asequible: https://www.incibe.es/

Itcomunicaciones. (2020). *Infection Monkey, asegura fuerza de trabajo remota*. Canales TI: https://itcomunicacion.com.mx/

Mitre att&ck. (2020). *Enterprise tactics*. Obtenido de Enterprise: https://attack.mitre.org/

ONISTEC. (2021). *¿Qué es el marco de seguridad Zero Trust?*. Soluciones: https://www.onistec.com/

Seeking alpha. (2018). *Microsoft Is Closing In On Amazon In The Cloud*. Summary: https://seekingalpha.com/

Seguridad América. (s.f.). *Cymulate*. Obtenido de Soluciones: https://www.seguridadamerica.com/

UC3M. (2011). *Gestor de entornos de simulación de cloud computing* [vesión PDF]. Biblioteca: https://e-archivo.uc3m.es/

Ucatolica. (2019). *Meta-Análisis de vulnerabilidades y gestión de riesgo en arquitecturas cloud*. Catálogo biblioteca: https://repository.ucatolica.edu.co/

Unipiloto. (2015). *COMPUTACIÓN EN LA NUBE Y SU SEGURIDAD*. Obtenido de Polux: http://polux.unipiloto.edu.co/

Unirioja. (2015). *COMPUTACIÓN EN LA NUBE*. Dialnet: https://dialnet.unirioja.es/

UTA. (2016). *Tecnología de Cloud Computing para Servicios de Infraestructura (IaaS)*. Repositorio Universidad Técnica de Ambato: https://repositorio.uta.edu.ec/

ANEXOS

Anexo 1

Tablas de táctica y técnicas de ataque para diferentes plataformas de empresas como dispositivos móviles.

A continuación, se hace una recopilación de técnicas de ataques principalmente para s Windows, Mac OS, Linux, Nube, Red

A1.1 Táctica de persistencia y técnicas de ataque

Persistence						
Registry Run Keys / Startup Folder	Kernel Modules and Extensions	Plist Modification	Boot or Logon Initialization Scripts	Startup Items	Domain Account	Windows Service
Authentication Package	Re-opened Applications	Print Processors	Logon Script (Windows)	Browser Extensions	Cloud Account	Launch Daemon
Time Providers	LSASS Driver	XDG Autostart Entries	Logon Script (Mac)	Compromise Client Software Binary	Create or Modify System Process	Event Triggered Execution
Winlogon Helper DLL	Shortcut Modification	Active Setup	Network Logon Script	Create Account	Launch Agent	Change Default File Association
Security Support Provider	Port Monitors	Login Items	RC Scripts	Local Account	Systemd Service	Screensaver
Outlook Forms	Network Device Authentication	Office Test	COR_PROFILER	Path Interception by PATH Environment Variable	Services File Permissions Weakness	DLL Side-Loading
Outlook Home Page	Office Application Startup	Domain Controller Authentication	Implant Internal Image	Path Interception by Search Order Hijacking	Services Registry Permissions Weakness	Dylib Hijacking
Pluggable Authentication Modules	Office Template Macros	Password Filter DLL	Modify Authentication Process	Path Interception by Unquoted Path	DLL Search Order Hijacking	Executable Installer File Permissions Weakness

Windows Management Instrumentation Event Subscription	Unix Shell Configuration Modification	Trap	LC_LOAD_DYLIB Addition	Netsh Helper DLL	Dynamic Linker Hijacking	PowerShell Profile
Emond	Accessibility Features	AppCert DLLs	AppInit DLLs	Application Shimming	Image File Execution Options Injection	Component Object Model Hijacking
External Remote Services	Hijack Execution Flow	No aplica	No aplica	No aplica	No aplica	No aplica

A1.2 Táctica de evasión de defensa y técnicas de ataque

Defense Evasion						
Setuid and Setgid	Make and Impersonate Token	Create Process with Token	Token Impersonation/Theft	Disable or Modify System Firewall	Timestomp	Compile After Delivery
Bypass User Account Control	Parent PID Spoofing	Access Token Manipulation	Elevated Execution with Prompt	Indicator Blocking	Indirect Command Execution	Software Packing
Sudo and Sudo Caching	Environmental Keying	Run Virtual Instance	Path Interception by Search Order Hijacking	Disable or Modify Cloud Firewall	Masquerading	Modify Registry
SID-History Injection	Exploitation for Defense Evasion	VBA Stomping	Path Interception by Unquoted Path	Disable Cloud Logs	Invalid Code Signature	Rundll32
BITS Jobs	File and Directory Permissions Modification	Email Hiding Rules	Services File Permissions Weakness	Safe Mode Boot	Right-to-Left Override	Verclsid
Build Image on Host	Windows File and Directory Permissions Modification	Resource Forking	Services Registry Permissions Weakness	Downgrade Attack	Rename System Utilities	Mavinject
Deobfuscate/Decode Files or Information	Linux and Mac File and Directory	Hijack Execution Flow	COR_PROFILER	Indicator Removal on Host	Masquerade Task or Service	Reduce Key Space

	Permissions Modification					
Deploy Container	Hide Artifacts	DLL Search Order Hijacking	Impair Defenses	Clear Windows Event Logs	Match Legitimate Name or Location	Disable Crypto Hardware
Direct Volume Access	Hidden Files and Directories	DLL Side-Loading	Disable or Modify Tools	Clear Linux or Mac System Logs	Space after Filename	XSL Script Processing
Domain Policy Modification	Hidden Users	Dylib Hijacking	Disable Windows Event Logging	Clear Command History	Double File Extension	Patch System Image
Group Policy Modification	Hidden Window	Executable Installer File Permissions Weakness	Impair Command History Logging	File Deletion	Modify Authentication Process	Downgrade System Image
Domain Trust Modification	NTFS File Attributes	Dynamic Linker Hijacking	Pluggable Authentication Modules	Network Share Connection Removal	Domain Controller Authentication	Network Boundary Bridging
Execution Guardrails	Hidden File System	Path Interception by PATH Environment Variable	Network Device Authentication	Modify Cloud Compute Infrastructure	Password Filter DLL	Network Address Translation Traversal
HTML Smuggling	Asynchronous Procedure Call	Rootkit	Signed Script Proxy Execution	Traffic Signaling	Valid Accounts	Obfuscated Files or Information
Pre-OS Boot	Thread Local Storage	Signed Binary Proxy Execution	PubPrn	Port Knocking	Default Accounts	Binary Padding
System Firmware	Ptrace System Calls	Compiled HTML File	Subvert Trust Controls	Trusted Developer Utilities Proxy Execution	Domain Accounts	Create Snapshot
Component Firmware	Proc Memory	Control Panel	Gatekeeper Bypass	MSBuild	Local Accounts	Create Cloud Instance
Bootkit	Extra Window Memory Injection	CMSTP	Code Signing	Unused/Unsupported Cloud Regions	Cloud Accounts	Delete Cloud Instance
ROMMONkit	Process Hollowing	InstallUtil	SIP and Trust Provider Hijacking	Use Alternate Authentication Material	Virtualization/Sandbox Evasion	Revert Cloud Instance
TFTP Boot	Process Doppelgänging	Mshta	Install Root Certificate	Application Access Token	System Checks	Steganography

Process Injection	VDSO Hijacking	Msiexec	Mark-of-the-Web Bypass	Pass the Hash	User Activity Based Checks	Regsvr32
Dynamic-link Library Injection	Reflective Code Loading	Odbcconf	Code Signing Policy Modification	Pass the Ticket	Time Based Evasion	Indicator Removal from Tools
Portable Executable Injection	Rogue Domain Controller	Regsvcs/Regasm	Template Injection	Web Session Cookie	Weaken Encryption	Modify System Image
Thread Execution Hijacking	MMC	No aplica	No aplica	No aplica	No aplica	No aplica

A1.3 Táctica de acceso a credenciales y técnicas de ataque

Credential Access						
LLMNR/NBT-NS Poisoning and SMB Relay	Password Spraying	Windows Credential Manager	Web Cookies	Modify Authentication Process	OS Credential Dumping	Steal or Forge Kerberos Tickets
ARP Cache Poisoning	Credential Stuffing	Password Managers	SAML Tokens	Domain Controller Authentication	LSASS Memory	Golden Ticket
Brute Force	Credentials from Password Stores	Exploitation for Credential Access	Input Capture	Password Filter DLL	Security Account Manager	Silver Ticket
Password Guessing	Keychain	Forced Authentication	Keylogging	Pluggable Authentication Modules	NTDS	Kerberoasting
Password Cracking	Securityd Memory	Forge Web Credentials	GUI Input Capture	Network Device Authentication	LSA Secrets	AS-REP Roasting
Credentials In Files	Credentials from Web Browsers	Cloud Instance Metadata API	Web Portal Capture	Network Sniffing	Cached Domain Credentials	Steal Web Session Cookie
Credentials in Registry	/etc/passwd and /etc/shadow	Group Policy Preferences	Credential API Hooking	Two-Factor Authentication Interception	DCSync	Proc Filesystem
Bash History	Steal Application Access Token	Container API	Private Keys	Unsecured Credentials	No aplica	No aplica

A1.4 Táctica de descubrimiento y técnicas de ataque

Discovery						
Local Account	Cloud Storage Object Discovery	Peripheral Device Discovery	System Location Discovery	System Checks	System Owner/User Discovery	Query Registry
Domain Account	Container and Resource Discovery	Permission Groups Discovery	System Language Discovery	User Activity Based Checks	System Service Discovery	Remote System Discovery
Email Account	Domain Trust Discovery	Local Groups	System Network Configuration Discovery	Time Based Evasion	System Time Discovery	Software Discovery
Cloud Account	File and Directory Discovery	Domain Groups	Internet Connection Discovery	Network Share Discovery	Virtualization/Sandbox Evasion	Security Software Discovery
Application Window Discovery	Group Policy Discovery	Cloud Groups	System Network Connections Discovery	Network Sniffing	Cloud Service Discovery	System Information Discovery
Browser Bookmark Discovery	Network Service Scanning	Process Discovery	Cloud Service Dashboard	Password Policy Discovery	Cloud Infrastructure Discovery	No aplica

A1.5 Táctica de movimiento lateral y técnicas de ataque

Lateral Movement						
Exploitation of Remote Services	RDP Hijacking	SSH	Taint Shared Content	Web Session Cookie	Pass the Hash	SSH Hijacking
Internal Spearphishing	Remote Services	VNC	Use Alternate Authentication Material	Replication Through Removable Media	Pass the Ticket	SMB/Windows Admin Shares
Lateral Tool Transfer	Remote Desktop Protocol	Windows Remote Management	Application Access Token	Software Deployment Tools	Distributed Component Object Model	Remote Service Session Hijacking

A1.6 Táctica de colección y técnicas de ataque

Collection						
Adversary-in-the-Middle	Automated Collection	Data from Information Repositories	Local Data Staging	Input Capture	Credential API Hooking	Data Staged
LLMNR/NBT-NS Poisoning and SMB Relay	Browser Session Hijacking	Confluence	Remote Data Staging	Keylogging	Screen Capture	Audio Capture
ARP Cache Poisoning	Clipboard Data	Sharepoint	Email Collection	GUI Input Capture	Video Capture	Email Forwarding Rule
Archive Collected Data	Data from Cloud Storage Object	Code Repositories	Local Email Collection	Web Portal Capture	Data from Network Shared Drive	Network Device Configuration Dump
Archive via Utility	Data from Configuration Repository	Data from Local System	Remote Email Collection	Archive via Custom Method	Data from Removable Media	SNMP (MIB Dump)

A1.7 Táctica de control y comando y técnicas de ataque

Command and Control						
Application Layer Protocol	Junk Data	Asymmetric Cryptography	Internal Proxy	Traffic Signaling	Communication Through Removable Media	Protocol Tunneling
Web Protocols	Steganography	Fallback Channels	External Proxy	Port Knocking	Data Encoding	DNS Calculation
File Transfer Protocols	Protocol Impersonation	Ingress Tool Transfer	Multi-hop Proxy	Web Service	Standard Encoding	Encrypted Channel
Mail Protocols	Dynamic Resolution	Multi-Stage Channels	Domain Fronting	Dead Drop Resolver	Non-Standard Encoding	One-Way Communication
DNS	Fast Flux DNS	Non-Application Layer Protocol	Remote Access Software	Bidirectional Communication	Data Obfuscation	Proxy
Symmetric Cryptography	Domain Generation Algorithms	Non-Standard Port	No aplica	No aplica	No aplica	No aplica

A1.8 Táctica de exfiltración y técnicas de ataque

Exfiltration						
Automated Exfiltration	Exfiltration Over C2 Channel	Scheduled Transfer	Exfiltration Over Web Service	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Exfiltration Over Bluetooth	Exfiltration Over Alternative Protocol
Traffic Duplication	Exfiltration Over Other Network Medium	Transfer Data to Cloud Account	Exfiltration to Code Repository	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Exfiltration Over Physical Medium	Exfiltration over USB
Data Transfer Size Limits	Exfiltration to Cloud Storage	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	No aplica	No aplica	No aplica	No aplica

A1.9 Táctica de impacto y técnicas de ataque

Impact						
Account Access Removal	External Defacement	Firmware Corruption	Reflection Amplification	Endpoint Denial of Service	Transmitted Data Manipulation	Application or System Exploitation
Data Destruction	Disk Wipe	Inhibit System Recovery	Resource Hijacking	OS Exhaustion Flood	Runtime Data Manipulation	Stored Data Manipulation
Data Encrypted for Impact	Disk Content Wipe	Network Denial of Service	Service Stop	Service Exhaustion Flood	Defacement	Internal Defacement
Data Manipulation	Disk Structure Wipe	Direct Network Flood	System Shutdown/Reboot	Application Exhaustion Flood	No aplica	No aplica

A1.10 Táctica de reconocimiento y técnicas de ataque

Reconnaissance						
Active Scanning	Client Configurations	Domain Properties	Determine Physical Locations	DNS/Passive DNS	Spearphishing Attachment	Search Open Websites/Domains

Scanning IP Blocks	Gather Victim Identity Information	DNS	Business Relationships	WHOIS	Spearphishing Link	Social Media
Vulnerability Scanning	Credentials	Network Trust Dependencies	Identify Business Tempo	Digital Certificates	Search Closed Sources	Search Engines
Gather Victim Host Information	Email Addresses	Network Topology	Identify Roles	CDNs	Threat Intel Vendors	Search Victim-Owned Websites
Hardware	Employee Names	IP Addresses	Phishing for Information	Scan Databases	Purchase Technical Data	Gather Victim Org Information
Software	Gather Victim Network Information	Network Security Appliances	Spearphishing Service	Firmware	Search Open Technical Databases	No aplica

A1.11 Táctica de desarrollo de recursos y técnicas de ataque

Resource Development						
Acquire Infrastructure	Botnet	Stage Capabilities	Obtain Capabilities	Digital Certificates	Email Accounts	Exploits
Domains	Web Services	Upload Malware	Malware	Exploits	Compromise Infrastructure	Vulnerabilities
DNS Server	Develop Capabilities	Upload Tool	Tool	Establish Accounts	Domains	Link Target
Virtual Private Server	Malware	Install Digital Certificate	Code Signing Certificates	Social Media Accounts	DNS Server	Server
Server	Code Signing Certificates	Drive-by Target	Digital Certificates	Email Accounts	Virtual Private Server	Social Media Accounts
Botnet	Compromise Accounts	Web Services	No aplica	No aplica	No aplica	No aplica

A1.12 Táctica de acceso inicial y técnicas de ataque

Initial Access						
Drive-by Compromise	Valid Accounts	Compromise Software Supply Chain	Replication Through Removable Media	Spearphishing Attachment	Local Accounts	Hardware Additions
Exploit Public-Facing Application	Default Accounts	Compromise Hardware Supply Chain	Supply Chain Compromise	Spearphishing Link	Cloud Accounts	Phishing

External Remote Services	Domain Accounts	Trusted Relationship	Compromise Software Dependencies and Development Tools	Spearphishing via Service	No aplica	No aplica

A1.13 Táctica de escalada de privilegios y técnicas de ataque

Privilege Escalation						
Abuse Elevation Control Mechanism	Winlogon Helper DLL	Launch Agent	Netsh Helper DLL	Path Interception by Unquoted Path	At (Linux)	DLL Search Order Hijacking
Setuid and Setgid	Security Support Provider	Systemd Service	Accessibility Features	Services File Permissions Weakness	At (Windows)	DLL Side-Loading
Bypass User Account Control	Kernel Modules and Extensions	Windows Service	AppCert DLLs	Services Registry Permissions Weakness	Cron	Dylib Hijacking
Sudo and Sudo Caching	Re-opened Applications	Launch Daemon	AppInit DLLs	COR_PROFILER	Launchd	Executable Installer File Permissions Weakness
Elevated Execution with Prompt	LSASS Driver	Domain Policy Modification	Application Shimming	Process Injection	Scheduled Task	Dynamic Linker Hijacking
Access Token Manipulation	Shortcut Modification	Group Policy Modification	Image File Execution Options Injection	Dynamic-link Library Injection	Systemd Timers	Path Interception by PATH Environment Variable
Token Impersonation/Theft	Port Monitors	Domain Trust Modification	PowerShell Profile	Portable Executable Injection	Container Orchestration Job	Path Interception by Search Order Hijacking
Create Process with Token	Plist Modification	Escape to Host	Emond	Thread Execution Hijacking	Valid Accounts	Ptrace System Calls

Make and Impersonate Token	Print Processors	Event Triggered Execution	Component Object Model Hijacking	Asynchronous Procedure Call	Default Accounts	Proc Memory
Parent PID Spoofing	XDG Autostart Entries	Change Default File Association	Exploitation for Privilege Escalation	Thread Local Storage	Domain Accounts	Extra Window Memory Injection
SID-History Injection	Active Setup	Screensaver	Hijack Execution Flow	VDSO Hijacking	Local Accounts	Process Hollowing
Boot or Logon Autostart Execution	Login Items	Windows Management Instrumentation Event Subscription	Create or Modify System Process	Scheduled Task/Job	Cloud Accounts	Process Doppelgänging
Registry Run Keys / Startup Folder	Boot or Logon Initialization Scripts	Unix Shell Configuration Modification	RC Scripts	Logon Script (Mac)	LC_LOAD_DYLIB Addition	Time Providers
Authentication Package	Logon Script (Windows)	Trap	Startup Items	Network Logon Script	No aplica	No aplica

Anexo 2

Tablas de táctica y técnicas de ataque para plataformas alojadas en la nube.

A continuación, se presenta las técnicas de ataques para Office 365, Azure AD, Google Workspace, servicio SaaS, servicio IaaS.

A2.1 Táctica y técnicas de ataque para Office 365

Acceso inicial	Persistencia	Escalada de privilegios	Evasión de defensa	Acceso a Credenciales	Descubrimiento	Movimiento lateral	Colección	Impacto
suplantación de identidad	Manipulación de cuentas	Cuentas Válidas	Ocultar artefactos	Fuerza bruta	Descubrimiento de cuenta	Pesca submarina interna	Datos de Repositorios de Información	Denegación de servicio de punto final
Cuentas Válidas	Crear cuenta		Debilitar las defensas	Forjar credenciales web	Tablero de servicios en la nube	Contenido compartido corrupto	Colección de correo electrónico	Denegación de servicio de red
	Inicio de aplicaciones de Office		Usar material de autenticación alternativo	Robar token de acceso a la aplicación	Detección de servicios en la nube	Usar material de autenticación alternativo		
	Cuentas Válidas		Cuentas Válidas	Robar cookie de sesión web	Descubrimiento de grupos de permisos			

				Credenciales no seguras	Descubrimiento de software			

A2.2 Táctica y técnicas de ataque para Azure AD

Acceso inicial	Persistencia	Escalada de privilegios	Evasión de defensa	Acceso a Credenciales	Descubrimiento	Impacto
Cuentas Válidas	Manipulación de cuenta	Modificación de política de dominio	Modificación de política de dominio	Fuerza bruta	Descubrimiento de cuenta	Denegación de servicio de punto final
	Crear cuenta	Cuentas Válidas	Cuentas Válidas	Forjar credenciales web	Tablero de servicios en la nube	Denegación de servicio de red
	Cuentas Válidas			Robar token de acceso a la aplicación	Detección de servicios en la nube	
				Credenciales no seguras	Descubrimiento de grupos de permisos	
					Descubrimiento de software	

A2.3 Táctica y técnicas de ataque para Google Workspace

Acceso inicial	Persistencia	Escalada de privilegios	Evasión de defensa	Acceso a Credenciales	Descubrimiento	Movimiento lateral	Colección	Impacto

suplantación de identidad	Manipulación de cuenta	Cuentas Válidas	Usar material de autenticación alternativo	Fuerza bruta	Descubrimiento de cuenta	Pesca submarina interna	Datos de repositorios de información	Denegación de servicio de punto final
Cuentas Válidas	Crear cuenta		Cuentas Válidas	Forjar credenciales web	Tablero de servicios en la nube	Usar material de autenticación alternativo	Colección de correo electrónico	Denegación de servicio de red
	Cuentas Válidas			Robar token de acceso a la aplicación	Detección de servicios en la nube			
				Robar cookie de sesión web	Descubrimiento de grupos de permisos			
				Credenciales no seguras	Descubrimiento de software			

A2.4 Táctica y técnicas de ataque para SaaS

Acceso inicial	**Persistencia**	**Escalada de**	**Evasión de defensa**	**Acceso a Credenciales**	**Descubrimiento**	**Movimiento lateral**	**Colección**	**Impacto**

		privilegios						
Compromiso de conducción	Cuentas Válidas	Cuentas Válidas	Usar material de autenticación alternativo	Fuerza bruta	Descubrimiento de cuenta	Pesca submarina interna	Datos de Repositorios de Información	Denegación de servicio de punto final
suplantación de identidad			Cuentas Válidas	Forjar credenciales web	Detección de servicios en la nube	Contenido compartido corrupto		Denegación de servicio de red
Relación de confianza				Robar token de acceso a la aplicación	Descubrimiento de grupos de permisos	Usar material de autenticación alternativo		
Cuentas Válidas				Robar cookie de sesión web	Descubrimiento de software			
				Credenciales no seguras				

APÉNDICE

Apéndice A

Suscripción en los servicios de computación en la nube AWS (Amazon Web Services).

Figura A.1 Suscripción AWS – nivel gratuito

Figura A.2 Suscripción AWS – registro de datos

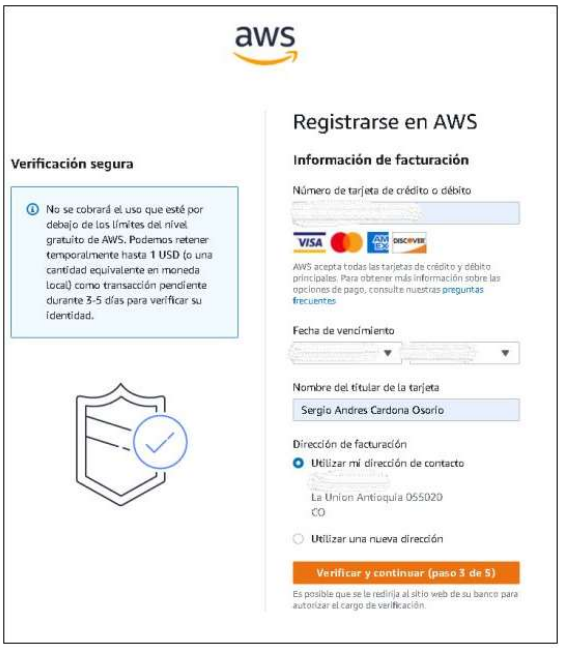


Figura A.3 Suscripción AWS – registro cuenta bancaria

Figura A.4 Suscripción AWS – registro gratuito básico

Apéndice B

Suscripción al catálogo digital de Marketplace de AWS (Amazon Web Services).

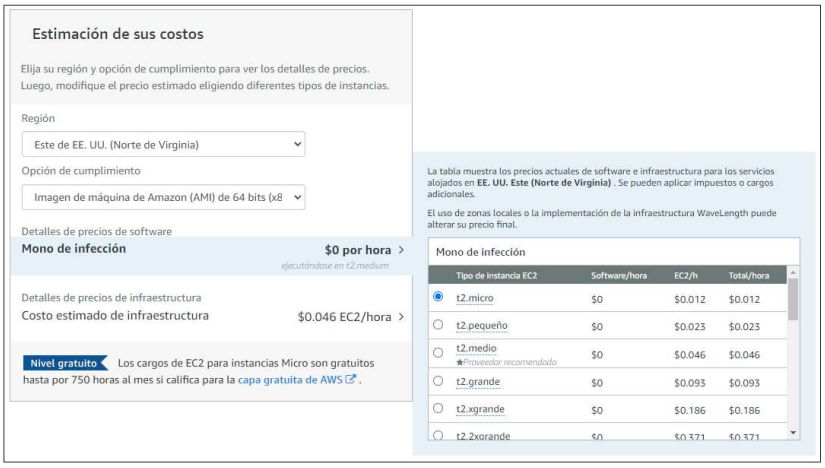


Figura B.1 Configuración – Estimación costos AWS

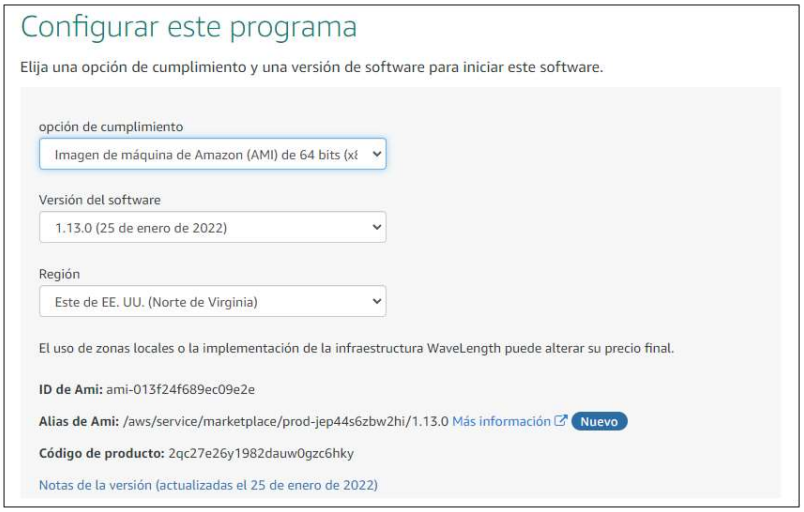


Figura B.2 Configuración – Máquina virtual y región

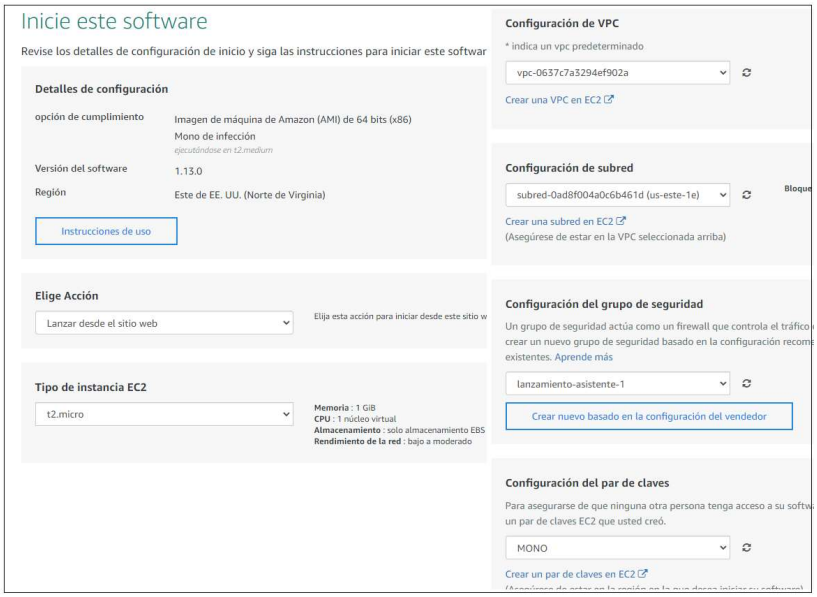


Figura B.3 Configuración – VPC, subred, grupo, llaves

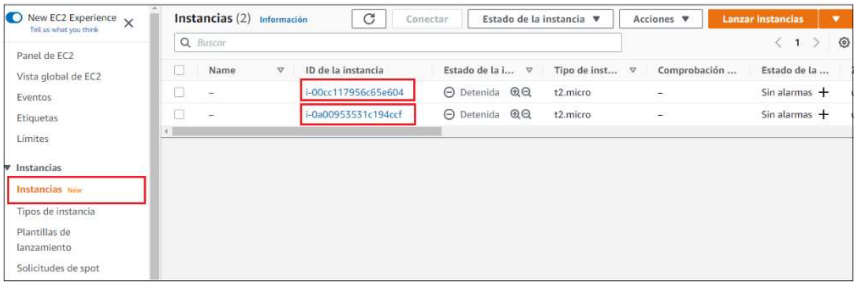


Figura B.4 Instancia EC2 – Tipo de instancia

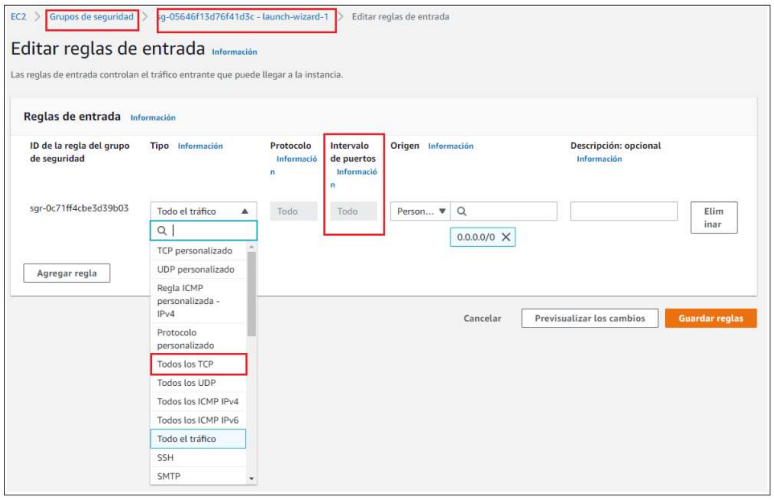


Figura B.5 Instancia EC2 – Entrada de tráfico y puertos

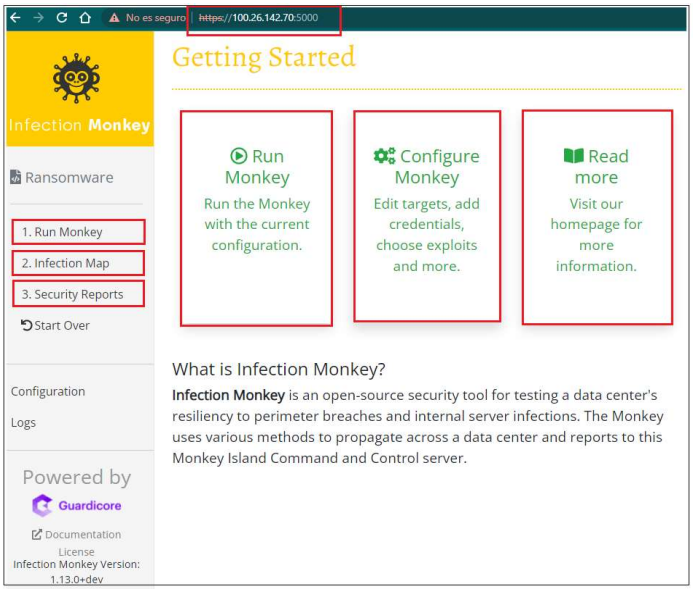


Figura B.6 Infection Monkey – IP para Dashboard

Apéndice C

Informe de confianza cero está compuesto de 7 pilares fundamentales, el cual, Infection Monkey inspección da un reporte detallado.

Datos: Aprobado

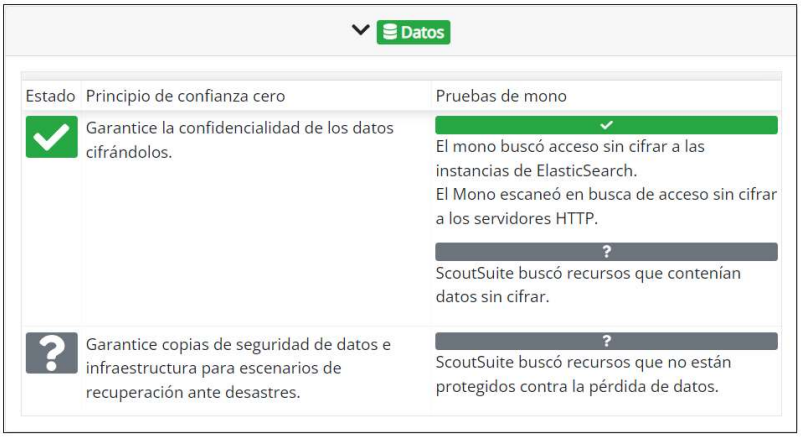


Figura C.1. Reporte cero confianza – Datos

Gente: No ejecutado

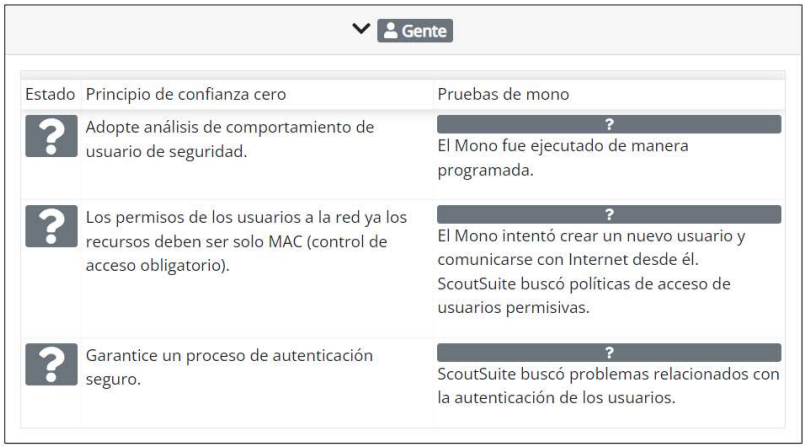


Figura C.2 Reporte cero confianza – Gente

Redes: Verificar

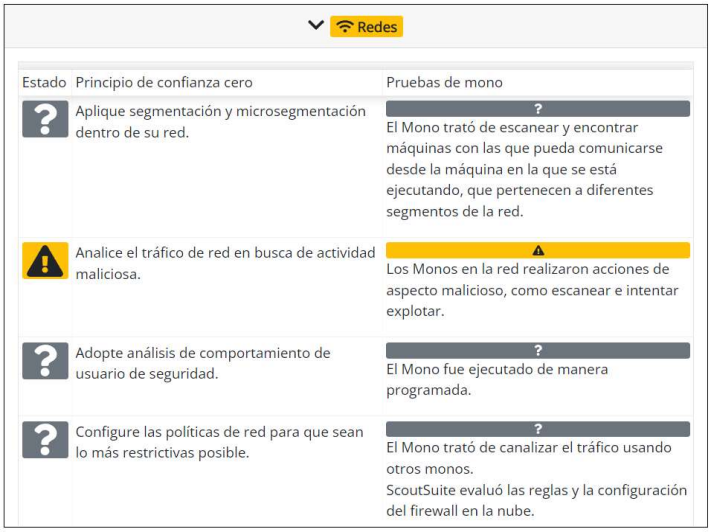


Figura C.3 Reporte cero confianza – Redes

Dispositivos: Ha fallado

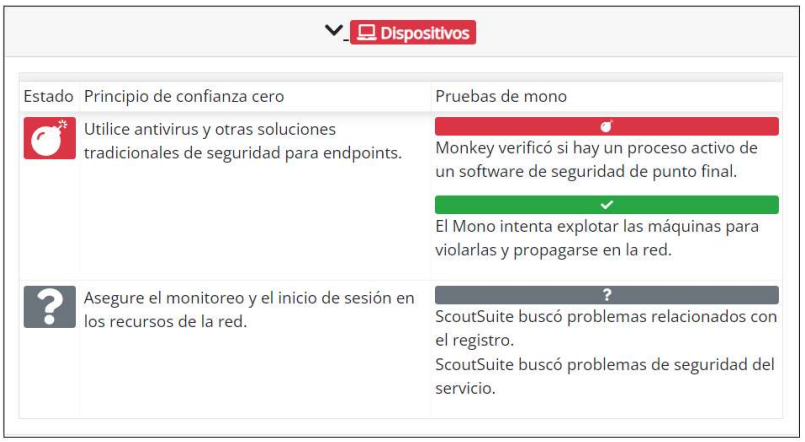


Figura C.4 Reporte cero confianza – Dispositivos

Cargas de trabajo: No ejecutado

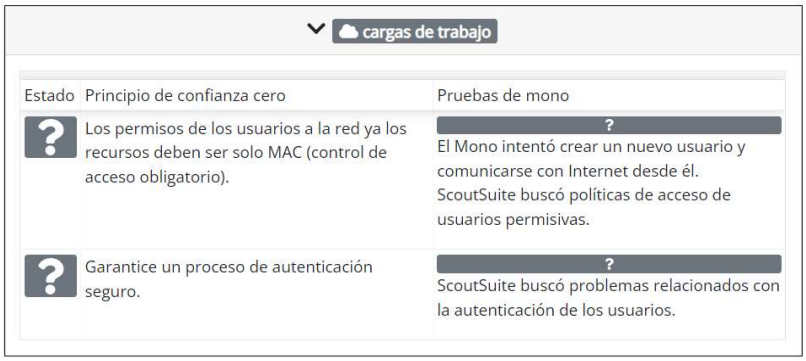


Figura C.5 Reporte cero confianza – Cargas de trabajo

Visibilidad y análisis: Verificar

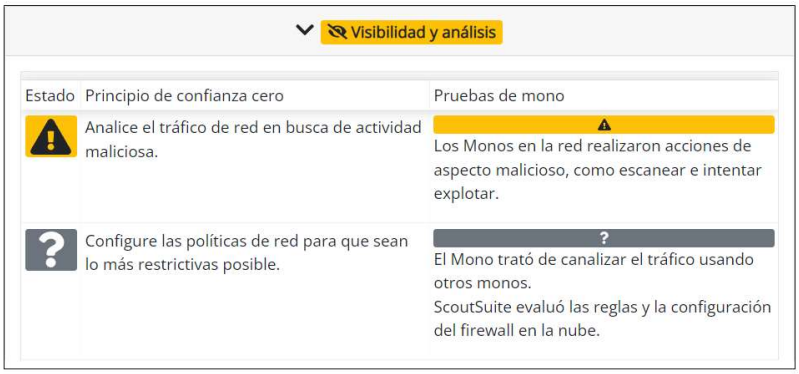


Figura C.6 Reporte cero confianza - Visibilidad

Automatización y Orquestación: No ejecutado

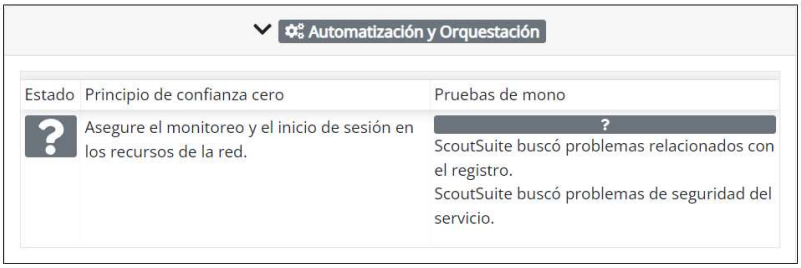


Figura C.7 Reporte cero confianza – Automatización

Apéndice D

Informe de seguridad que muestra el estado de las tácticas y técnicas de ataque con recomendación para mitigación de riesgo.

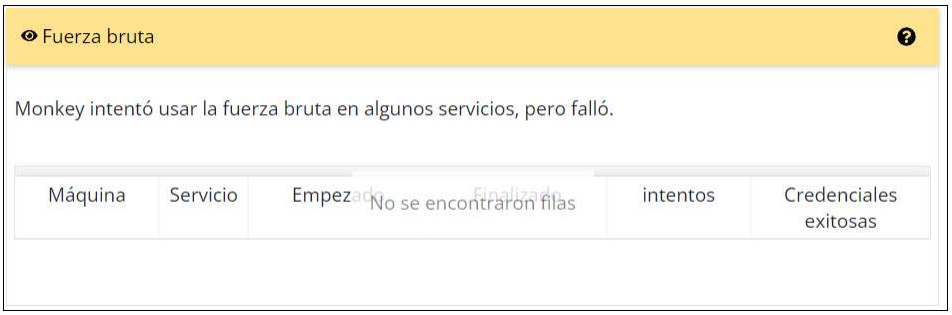


Figura D.1 Técnicas y tácticas de ataque – Fuerza bruta

Figura D.2 Técnicas y tácticas de ataque – Sistemas remotos

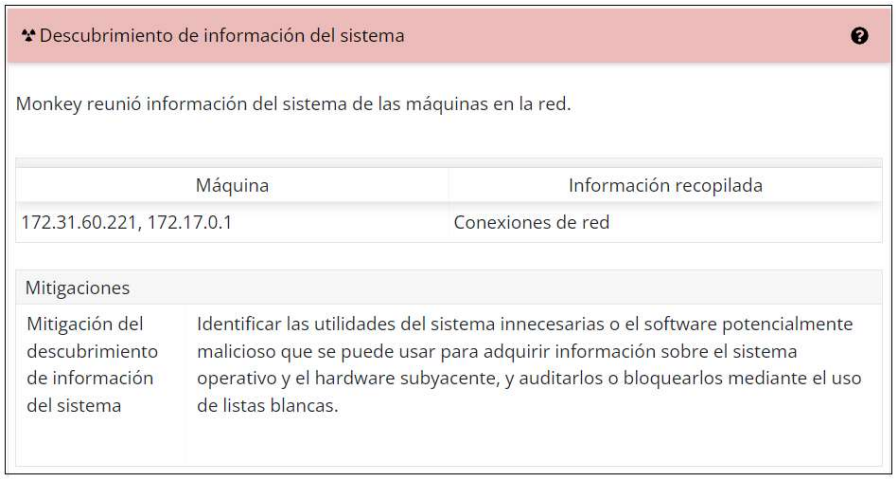


Figura D.3 Técnicas y tácticas de ataque – Descubrimiento

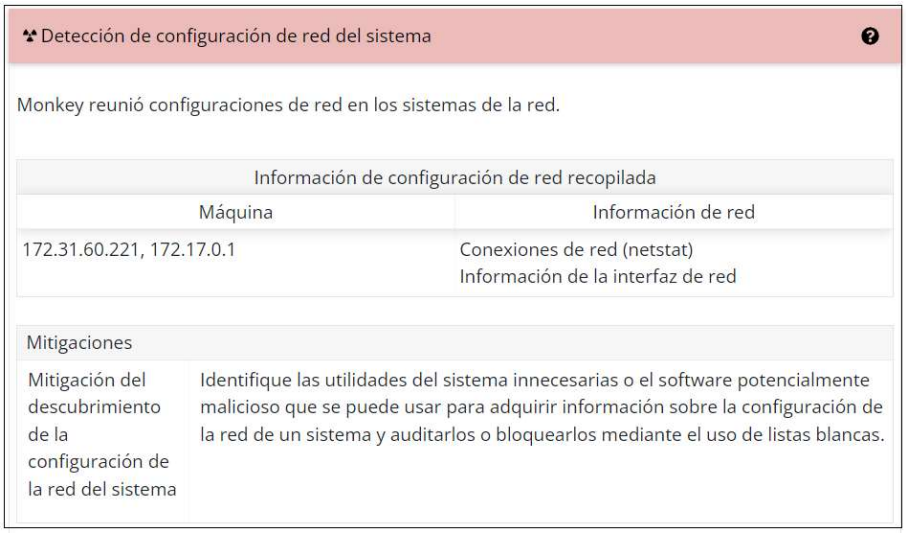
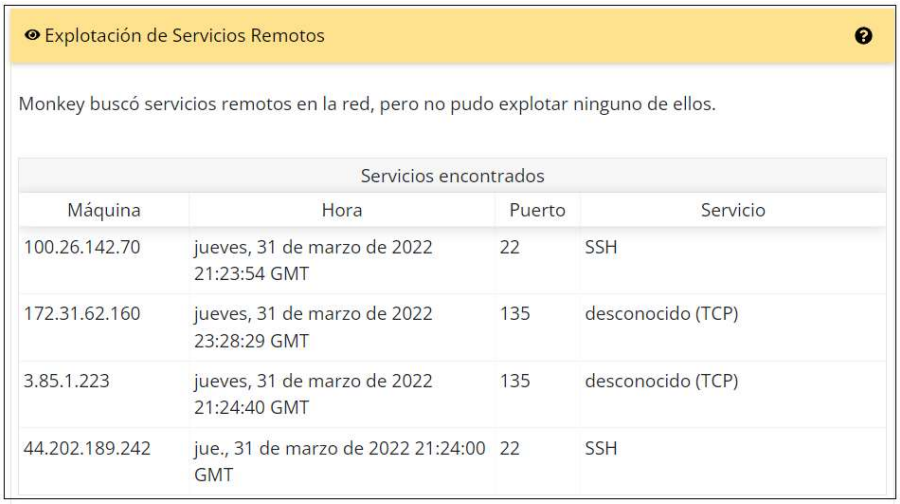


Figura D.4 Técnicas y tácticas de ataque - Detección

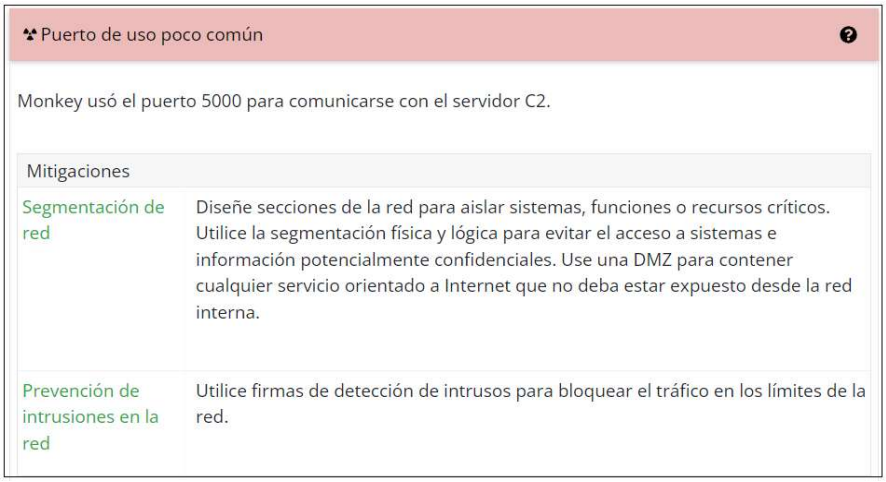


Explotación de Servicios Remotos

Monkey buscó servicios remotos en la red, pero no pudo explotar ninguno de ellos.

Servicios encontrados			
Máquina	Hora	Puerto	Servicio
100.26.142.70	jueves, 31 de marzo de 2022 21:23:54 GMT	22	SSH
172.31.62.160	jueves, 31 de marzo de 2022 23:28:29 GMT	135	desconocido (TCP)
3.85.1.223	jueves, 31 de marzo de 2022 21:24:40 GMT	135	desconocido (TCP)
44.202.189.242	jue., 31 de marzo de 2022 21:24:00 GMT	22	SSH

Figura D.5 Técnicas y tácticas de ataque – Explotación



Puerto de uso poco común

Monkey usó el puerto 5000 para comunicarse con el servidor C2.

Mitigaciones	
Segmentación de red	Diseñe secciones de la red para aislar sistemas, funciones o recursos críticos. Utilice la segmentación física y lógica para evitar el acceso a sistemas e información potencialmente confidenciales. Use una DMZ para contener cualquier servicio orientado a Internet que no deba estar expuesto desde la red interna.
Prevención de intrusiones en la red	Utilice firmas de detección de intrusos para bloquear el tráfico en los límites de la red.

Figura D.6 Técnicas y tácticas de ataque – Puerto

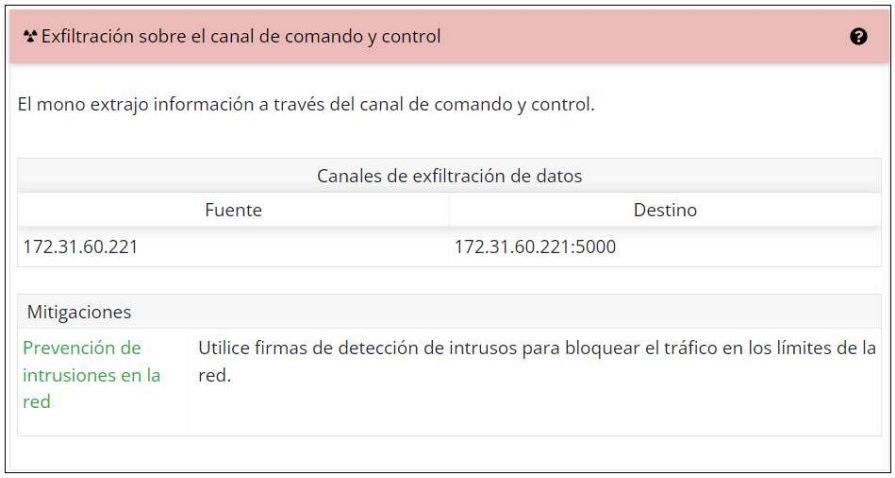


Figura D.7 Técnicas y tácticas de ataque - Ex