UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERIA

ESCUELA DE COMPUTACION



**“CASO DE ESTUDIO I**

**ANALISIS DE VULNERAVILIDADES”**

**PRESENTADO POR:**

Abrego Herrera, Giovanny Misael

Ardón Rivas, Christian Rodrigo

Santos Martínez, Edwin Alexander

**DOCENTE:** ING. DOUGLAS ALONSO FLORES VILLALOBOS

**CICLO/AÑO:**  02/2021

**Objetivo General**

Interpretar los conocimientos básicos para comprender como funcionan las herramientas para identificar vulnerabilidades en cualquier sistema complejo.

**Objetivos específicos**

* Explicar de manera clara las características de cada herramienta
* Demostrar el resultado y comprender el funcionamiento de la herramienta NEXPOSE.

**Estándares CVSS y las listas de CVE**



**¿Qué es vulnerabilidad ?**

Es una debilidad que se encuentra en un activo o en un control y que puede ser explotada por una o más amenazas, lo que deriva en un riesgo de seguridad, ademas que la seguridad se enfoca en reducir los riesgos a un nivel que resulte aceptable, razón por la cual una de las actividades a las que se recurre con frecuencia consiste en identificar y evaluar debilidades asociadas a las plataformas de software y hardware

**Conociendo esto podemos conocer que es CVSS**

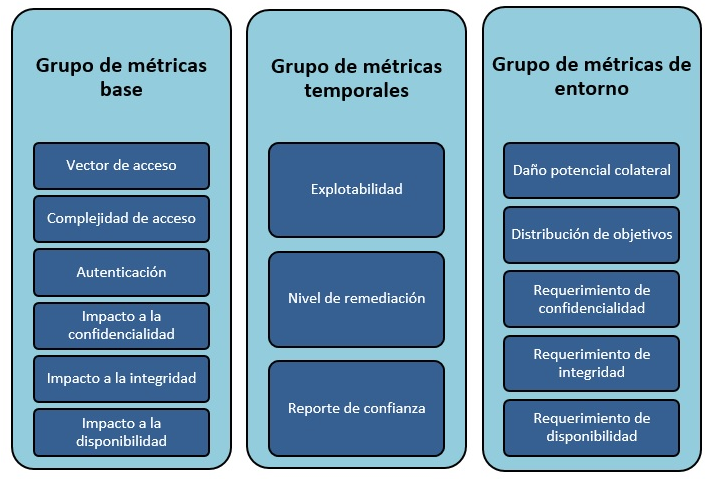


Para lo cual es un sistema de puntaje diseñado para proveer un método abierto y es un estándar que permite estimar el impacto derivado de vulnerabilidades identificadas en Tecnologías de Información, es decir, contribuye a cuantificar la severidad que pueden representar dichas vulnerabilidades.

**¿Como puedo implementarlo?**

* Al entender qué es CVSS, para determinar el impacto que representa una vulnerabilidad se utiliza una escala que va del 0 al 10.
* La severidad se considera baja si el puntaje obtenido luego de aplicar la fórmula CVSS resulta entre 0.0 y 3.9.
* El impacto es medio si el resultado se ubica entre 4.0 y 6.9. Se considera alto cuando el puntaje cae dentro del rango 7.0 y 10.0.

Para calcular un puntaje asociado a una vulnerabilidad, CVSS utiliza tres grupos de métricas: base, temporal y de entorno, cada una se conforma a su vez de un conjunto de otras métricas, como lo veremos a continuación.



**¿Como funciona CVSS en nexpose?**

*X:\doc\aa_graphics\rapid7_logo_200.jpg*

Debemos conocer de ante mano que Rapid7 Nexpose implementa el estándar Common Vulnerability Scoring System (CVSS) calculando el índice de puntuación CVSS para lo cual seutiliza la versión 2 (CVSS v2) para cada vulnerabilidad descubierta.

Este índice, que es administrado por el Foro de Equipos de Seguridad de Incidencia y Respuesta (FIRST), proporciona un marco abierto para determinar la gravedad relativa de las vulnerabilidades y un formato estandarizado para comunicar las características de las vulnerabilidades.

Un algoritmo de Nexpose calcula cada puntuación de CVSS según el nivel de gravedad, la facilidad de explotación, la capacidad de ejecución remota, el requisito de acceso con credenciales y otros criterios.

Nexpose muestra las puntuaciones CVSS en todos los listados de vulnerabilidades en la interfaz web de la consola de seguridad de Nexpose. Cada vulnerabilidad se enumera con su puntuación CVSS y un identificador de Enumeración de vulnerabilidad común (CVE) correspondiente siempre que haya un identificador CVE disponible.

Los usuarios tienen en cuenta la puntuación CVSS, las clasificaciones de gravedad y las puntuaciones de riesgo en función de modelos de puntuación temporales o ponderados para priorizar las tareas de corrección de vulnerabilidades. Nexpose incluye la puntuación CVSS en todas sus plantillas de informes ademas de permitir que las vulnerabilidades se cuantifiquen según el nivel de gravedad y la clasificación CVSS facilita una reparación más rápida. Por ejemplo, los informes que incluyen la sección Detalles de vulnerabilidad de mayor riesgo enumeran las vulnerabilidades de mayor riesgo e incluyen sus categorías, puntajes de riesgo y sus puntajes CVSS.

Los informes que incluyen la sección Índice de vulnerabilidades incluyen el nivel de gravedad y la clasificación CVSS para cada vulnerabilidad.

La puntuación CVSS es el factor principal para determinar si un dispositivo determinado cumple con los estándares de la industria de tarjetas de pago (PCI). Nexpose incorpora puntuaciones CVSS en su Informe de auditoría de PCI, que proporciona resultados detallados de la auditoría de cumplimiento de PCI. La sección Detalles de la vulnerabilidad de PCI del Informe de auditoría de PCI contiene información detallada sobre cada vulnerabilidad descubierta durante el análisis de Auditoría de PCI. Cada vulnerabilidad descubierta se clasifica según su puntuación CVSS.

Nexpose es una herramienta autorizada por la industria de tarjetas de pago (PCI) para realizar auditorías de cumplimiento, y Rapid7 es un proveedor de escaneo aprobado (ASV). Los clientes de Rapid7 pueden aprovechar aún más sus inversiones en Nexpose con escaneos continuos para rastrear sus puntajes CVSS en preparación para las auditorías PCI trimestrales. Esta cobertura completa de CVSS proporciona a las empresas un sólido apoyo en la toma de decisiones, lo que reduce los tiempos de respuesta para las vulnerabilidades detectadas.

Además de la puntuación CVSS real, Nexpose permite a los usuarios configurar su propia puntuación de riesgo personalizada en función de las necesidades específicas de su entorno único. La puntuación de riesgo personalizada, junto con la puntuación CVSS estandarizada, brinda una oportunidad única para que los administradores de seguridad administren su exposición al riesgo con la mayor granularidad y precisión disponible en nuestra industria.

**Dado todo lo anterior podemos conocer que es CVE**



Sin duda alguna procedemos con Common Vulnerability Enumeration® (CVE) el cual apoya mucho a CVSS y es una especificación que describe una nomenclatura y un diccionario de fallas de software relacionadas con la seguridad

Los CVE permiten que los especialistas en TI coordinen sus iniciativas para priorizar y solucionar los puntos vulnerables, y para mejorar la seguridad de los sistemas informáticos.

**¿Cómo funciona el sistema de CVE?**

Para su administracion tenemos que MITRE Corporation se encarga de supervisar las CVE con la financiación de la Agencia de Seguridad de Ciberseguridad e Infraestructura, que forma parte del Departamento de Seguridad Nacional de Estados Unidos.

Las entradas de CVE son breves y no incluyen datos técnicos ni información sobre riesgos, efectos o soluciones. Ese tipo de información aparece en otras bases de datos, como la National Vulnerability Database (NVD) de los Estados Unidos, la CERT/CC Vulnerability Notes Database y diversas listas que mantienen los proveedores y otras empresas. Los números de identificación de CVE ofrecen a los usuarios una forma confiable de diferenciar cada falla de seguridad en los distintos sistemas.

**¿Como funciona CVE en nexpose?**

**X:\doc\aa_graphics\l_nexpose.png**

Rapid7 Nexpose implementa el estándar Common Vulnerability Enumeration (CVE) asignando y mostrando un identificador CVE para cada vulnerabilidad para la que existe un identificador. CVE es un formato para describir las vulnerabilidades y exposiciones de seguridad de la información.

Cada vulnerabilidad que Nexpose descubre en el proceso de análisis aparece en la base de datos de vulnerabilidades. Esta extensa base de datos de texto completo con capacidad de búsqueda también almacena información de corrección en parches y correcciones descargables, así como contenido de referencia que describe cada debilidad de seguridad.

La base de datos ha sido certificada para ser compatible con el índice Common Vulnerabilities and Exposures (CVE) de MITRE Corporation. MITRE Corporation estandariza los nombres de las vulnerabilidades en diversos productos y proveedores de seguridad.

Los usuarios pueden buscar vulnerabilidades en la base de datos a través de la interfaz web de Nexpose Security Console utilizando identificadores CVE como criterios de búsqueda.

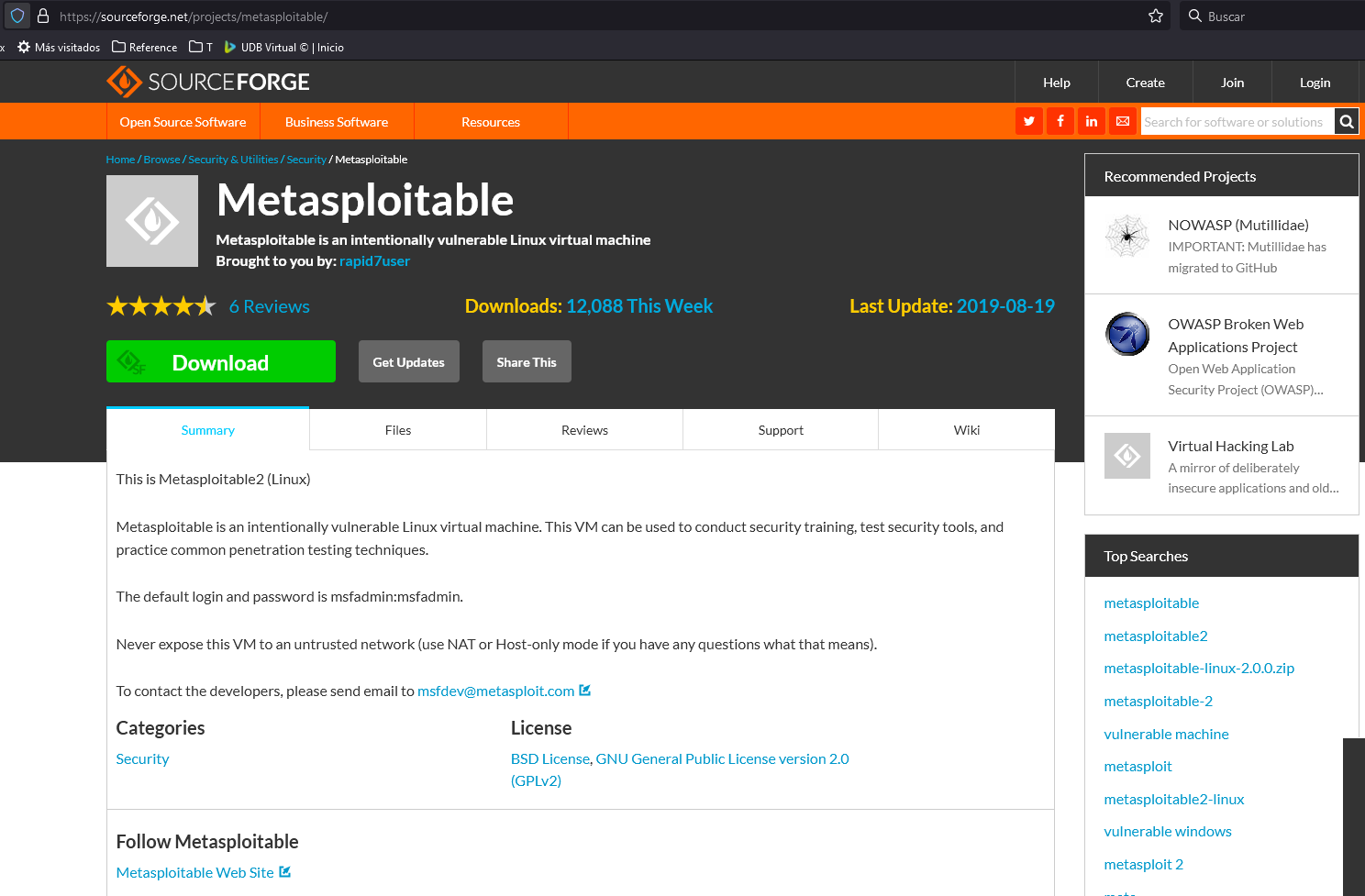
Cada nueva versión de Nexpose utiliza la lista CVE más actual. Cada seis horas, Nexpose actualiza sus definiciones de vulnerabilidad a través de un servicio de suscripción que modifica las definiciones existentes y agrega enlaces para nuevos identificadores CVE.

Además, Nexpose incorpora continuamente la lista de CVE más actualizada de la lista de correo de CVE y el registro de cambios. Las capacidades de actualización de múltiples vectores garantizan que Nexpose siempre realice un escaneo de vulnerabilidades con los identificadores y descriptores CVE más nuevos.

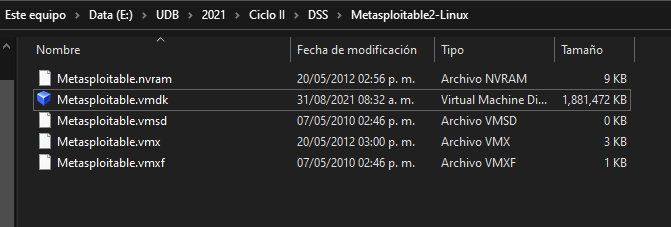
La interfaz web proporciona un centro centralizado para ver listas y descripciones completas de todas las instancias de parches faltantes, fallas de software y vulnerabilidades descubiertas en los sistemas de destino, junto con cada uno de los identificadores CVE correspondientes disponibles.

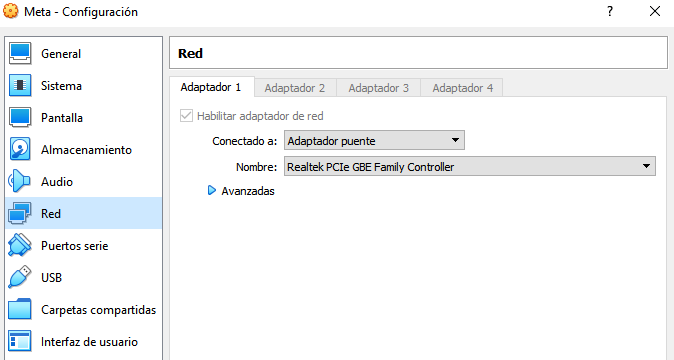
Los identificadores son enlaces de hipertexto a avisos externos en la base de datos nacional de vulnerabilidad del Instituto Nacional de Estándares (NIST), donde se puede encontrar información adicional relevante. Los identificadores CVE se muestran en las secciones de Vulnerabilidades descubiertas de los informes de Nexpose.

Instalación Metasploit.

Antes de iniciar se establece un entorno vulnerable que podamos analizar con la herramienta, para ello se descarga la máquina virtual del sitio <https://sourceforge.net/projects/metasploitable/> 

Al finalizar la descarga y descomprimir el archivo, se obtiene una carpeta con los archivos de disco de la máquina virtual.

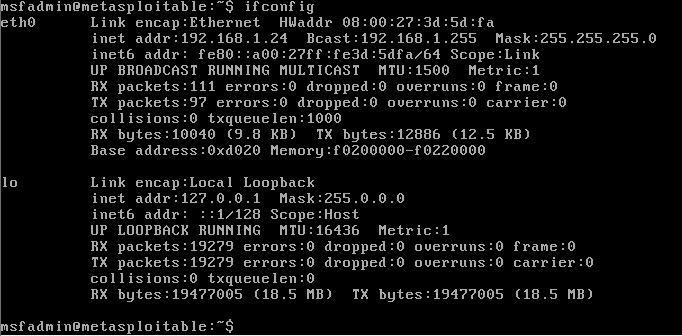


Al crear una nueva máquina virtual Linux, se selecciona el archivo .vmdk como almacenamiento y la red se configura como adaptador puente para establecer una conexión con la máquina anfitrión.

Finalmente se arranca la máquina virtual y se accede con las credenciales por defecto msfadmin:msfadmin.

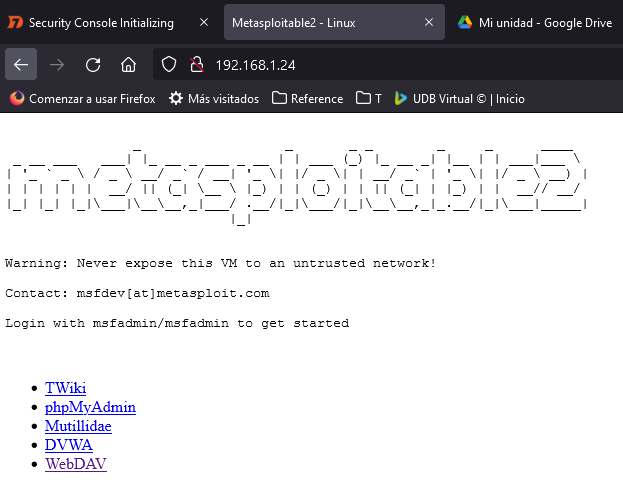


Una vez dentro se utiliza el comando ifconfig para obtener la dirección ip a analizar con el software NEXPOSE.



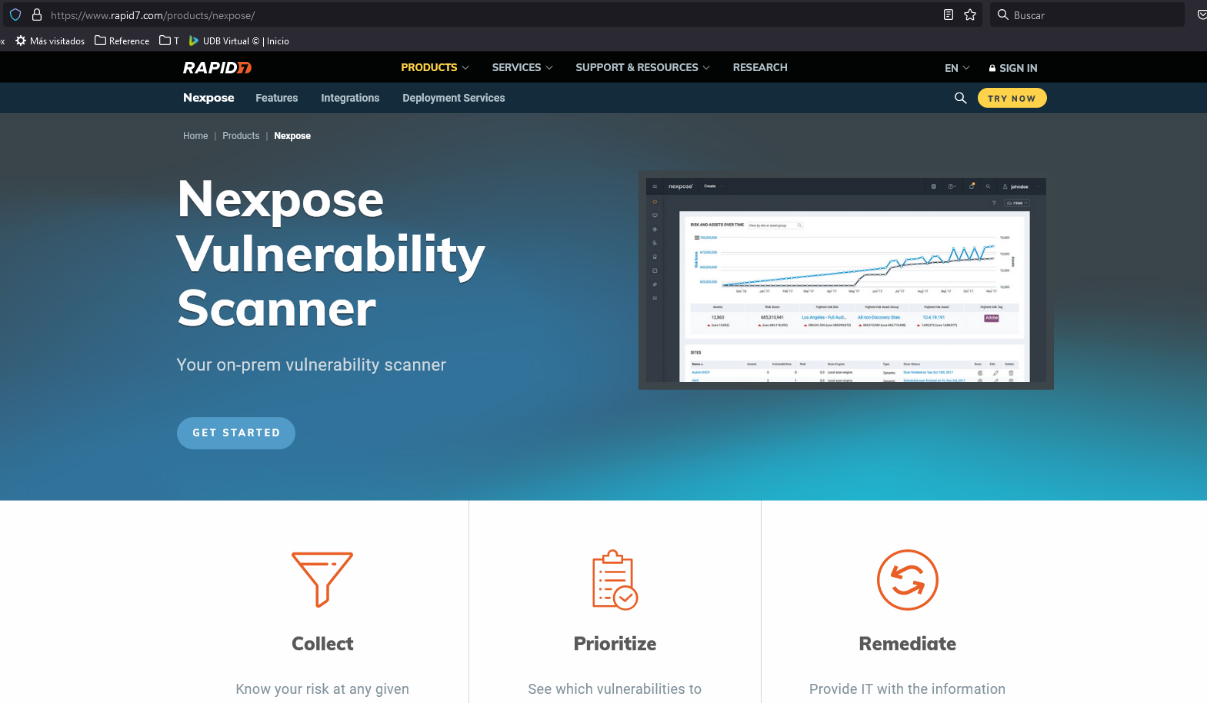
La ip obtenida (192.168.1.24) puede probarse en el navegador de la máquina anfitrión para asegurar que exista

conexión.

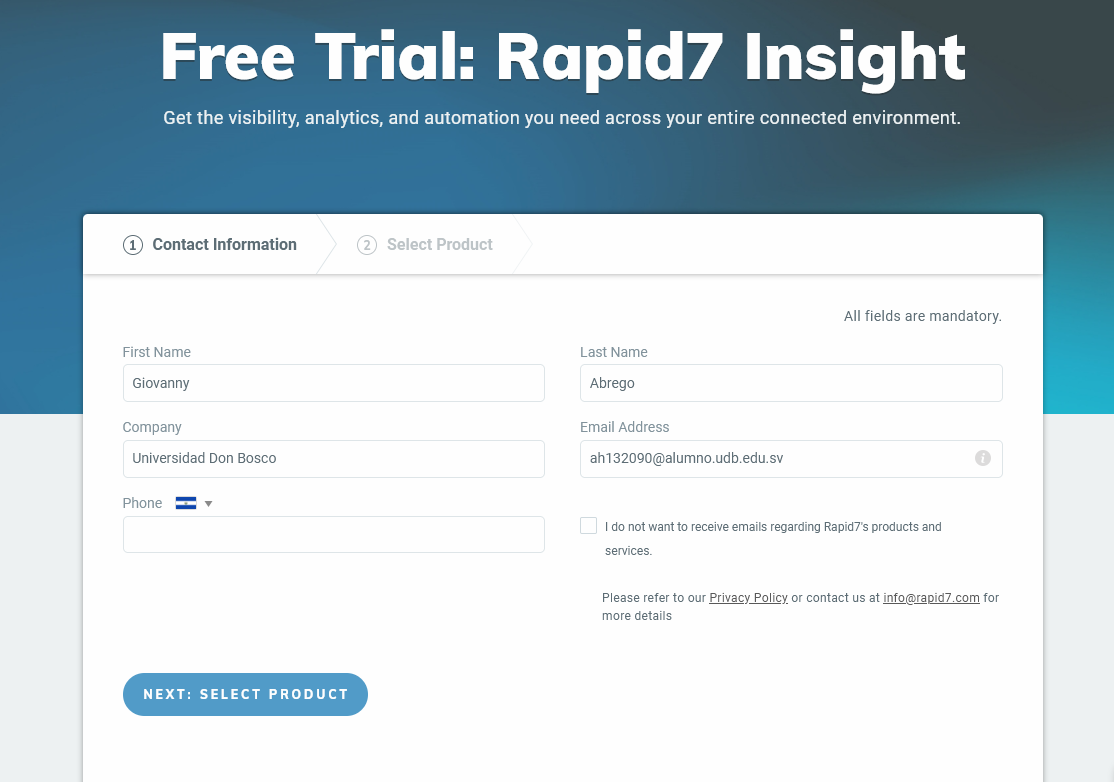


Instalación NEXPOSE.

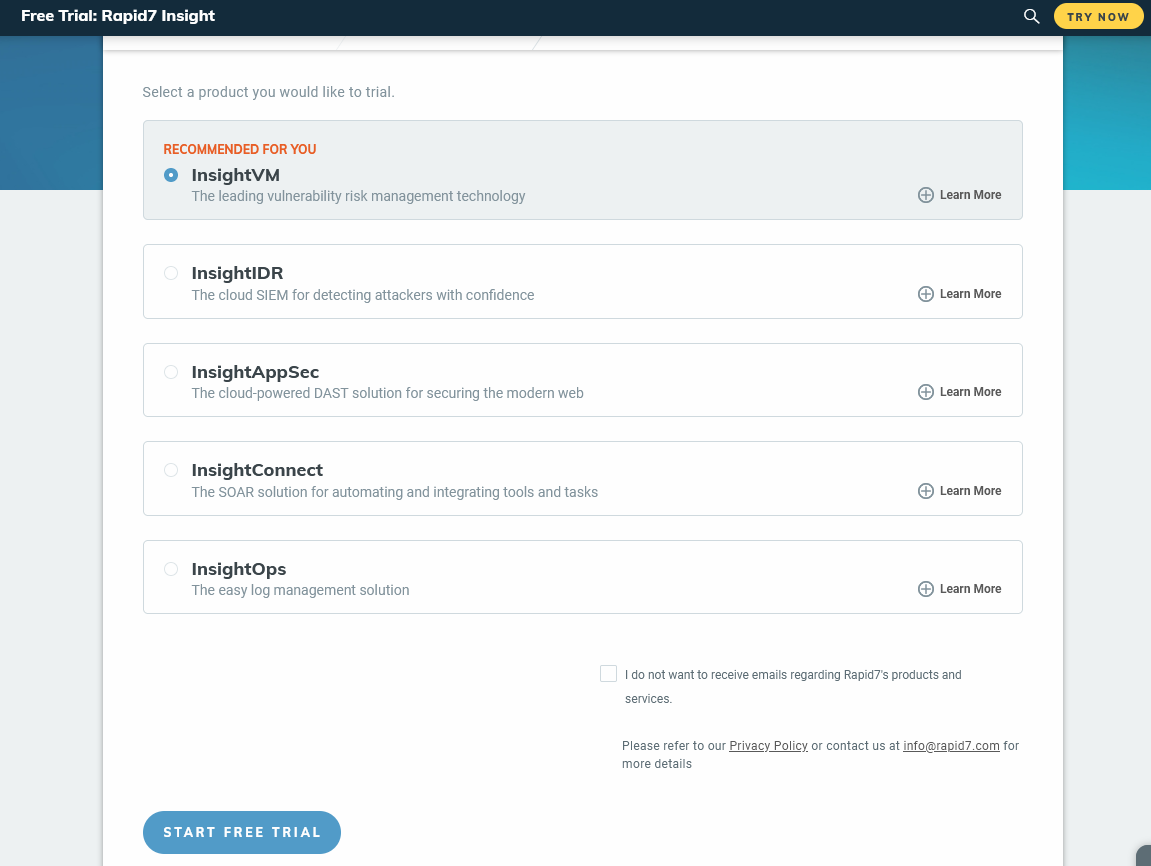
Para instalar Nexpose se ingresa al sitio <https://www.rapid7.com/products/nexpose/> y selecciona la opción Try Now.



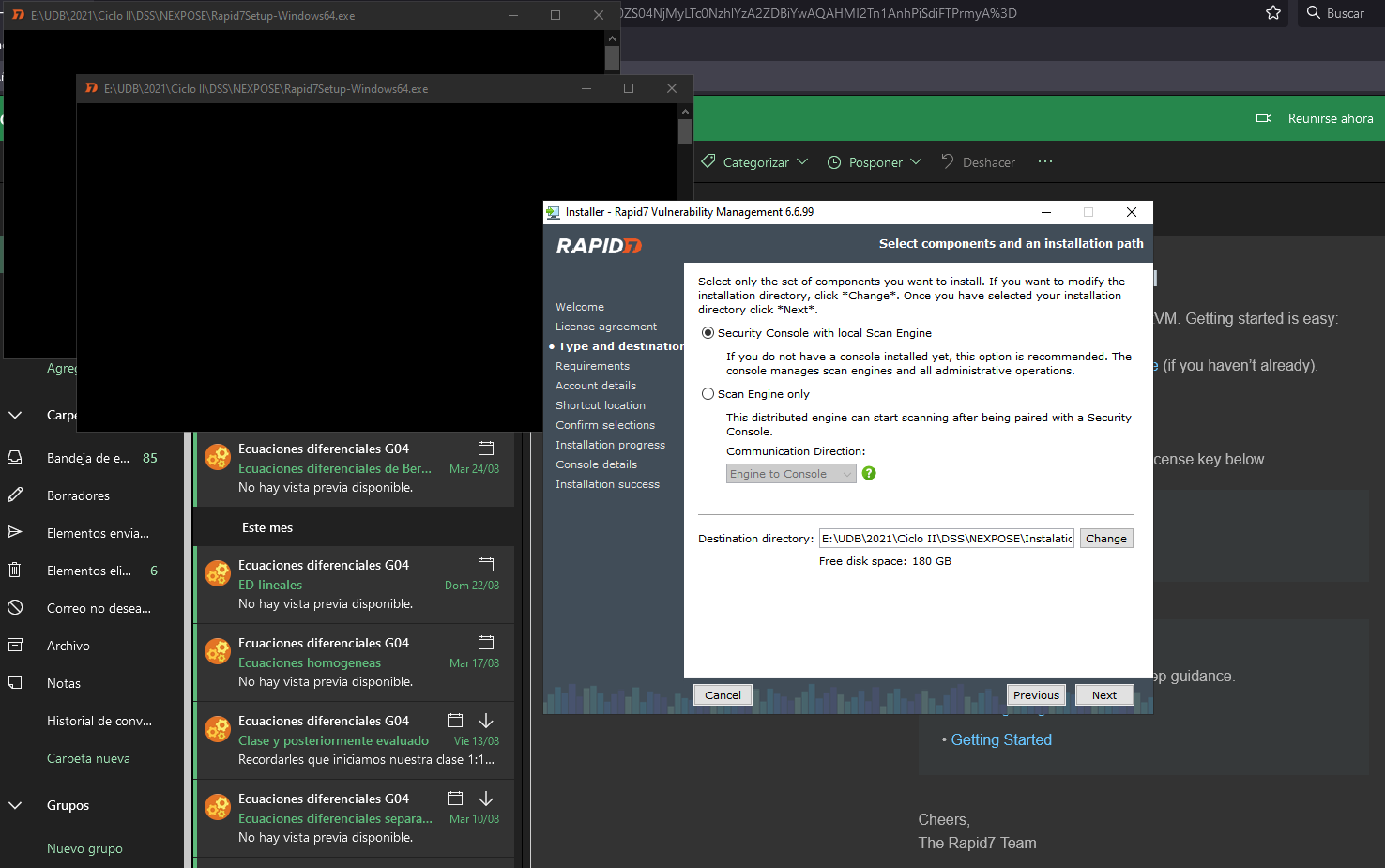
Se ingresa la información en el registro tomando en cuenta que el correo solicitado debe ser un correo institucional para que se envíe un código de activación.



Se selecciona el producto recomendado, y se descarga el paquete de instalación de acuerdo a la arquitectura del sistema operativo en el que se instalará.

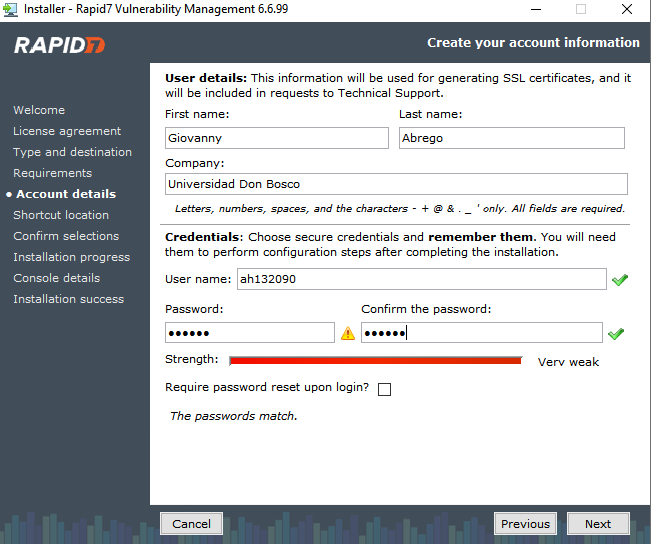


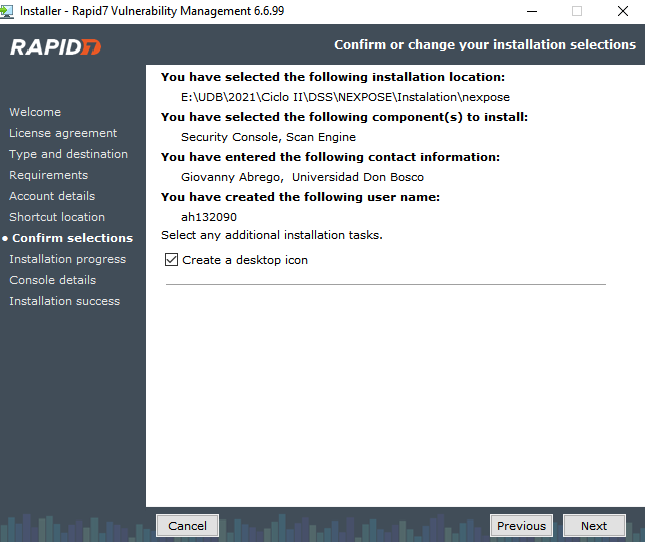
Al iniciar el instalador se selecciona la carpeta donde se guardarán los archivos de instalación, es recomendable desactivar el firewall del antivirus ya que puede interferir con el proceso de instalación.



Se configura el perfil de usuario a utilizar para entrar al software.

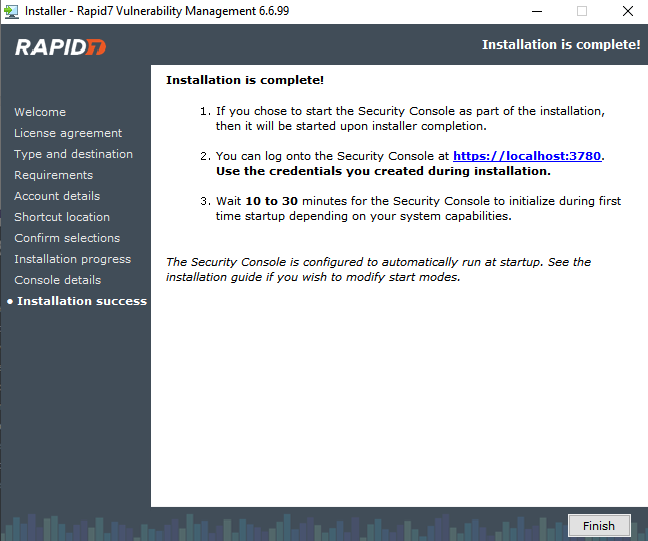
Username:ah132090 Password:123456

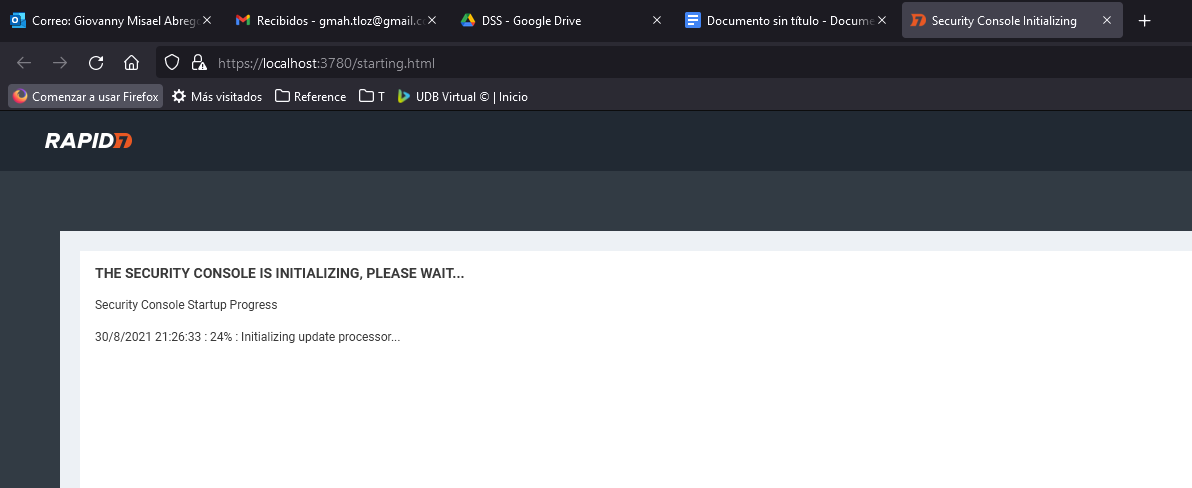


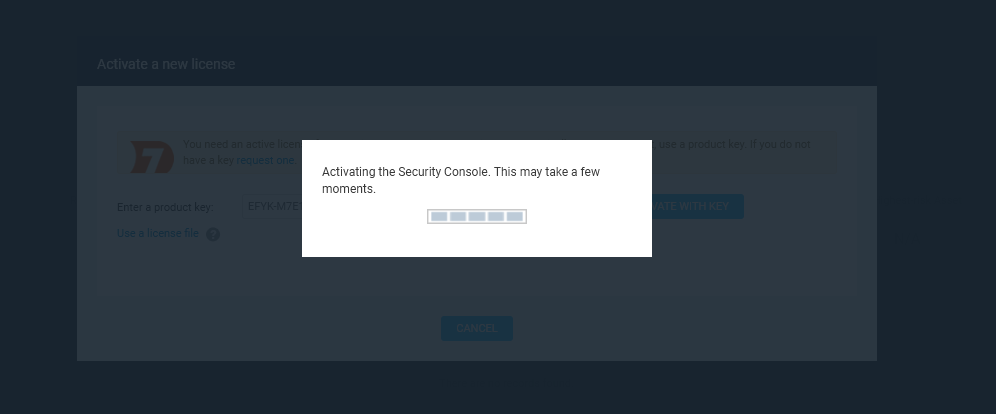


Se confirman los detalles de instalación.

Finalmente, solo resta esperar a que finalice la instalación, luego de confirmar los puertos que utiliza el software.

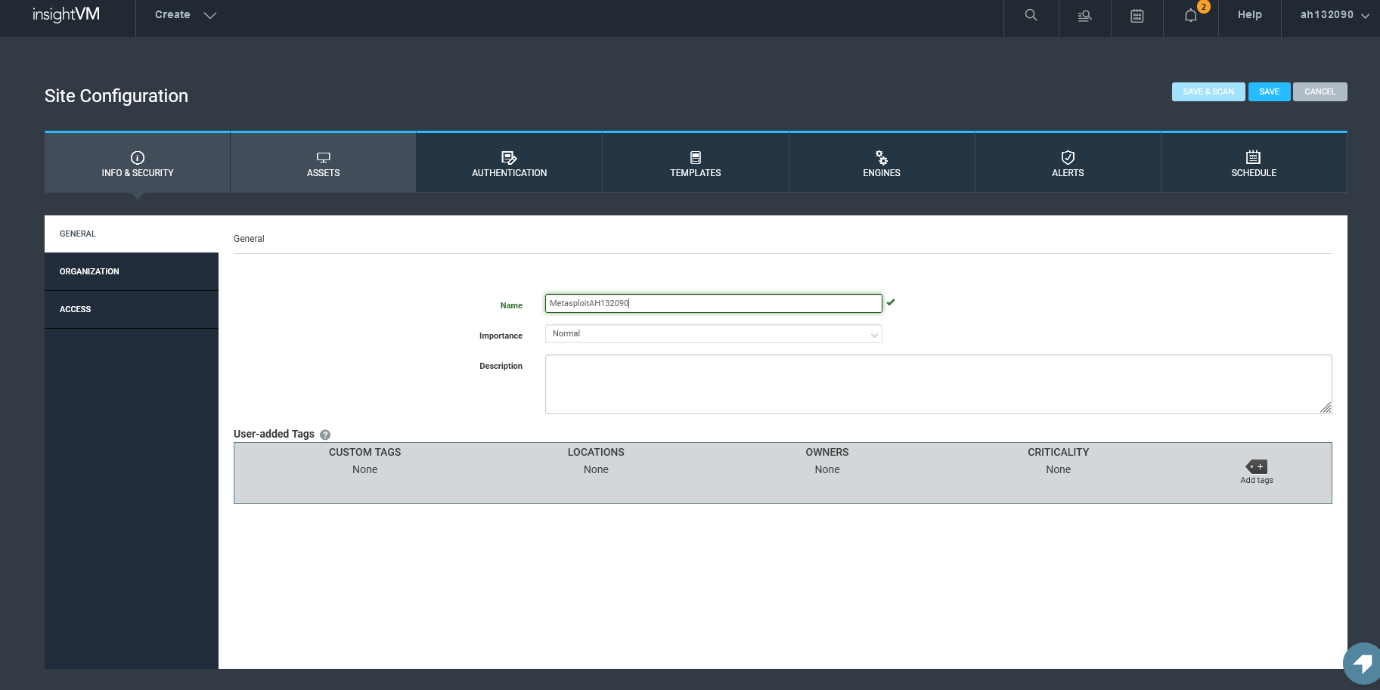


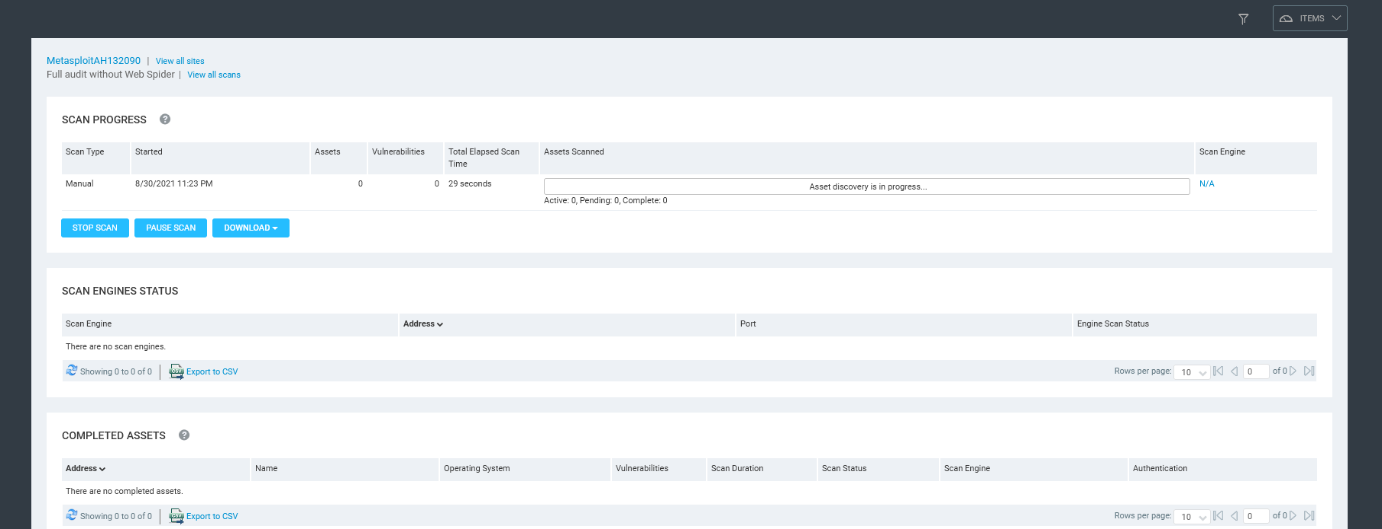
Al finalizar la instalación el sistema debe reiniciarse, luego de esto la inicialización del software puede tardar hasta 30 minutos dependiendo de la capacidad del sistema.

Una vez  ingresado en el software se requerirá el código de activación que fue enviado al correo institucional que se registró en el sitio del software y así finalizar la instalación.

Escaneo de sitio.

Para configurar un sitio a escanear primero debe ingresar el nombre que se le dará a este sitio en particular, luego selecciona la pestaña ASSETS donde se escribe la ip a analizar, finalmente se guarda y ejecuta el análisis





**Conclusiones**

Se comprende de manera clara cuales son las características de la mayoría de herramientas que existen en el mercado para verificar e identificar vulnerabilidades.

Se demuestra con éxito el análisis de vulnerabilidades con la herramienta NEXPOSE y se comprende de manera clara su manera de operar.

**Referencias**

* <https://www.welivesecurity.com/la-es/2014/08/04/vulnerabilidades-que-es-cvss-como-utilizarlo/>
* <https://www.redhat.com/es/topics/security/what-is-cve>