CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

JESUS DAVID DUARTE PRADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD). ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERA ESPECIALIZACION SEGURIDAD INFORMATICA

MEDELLIN

2022

CONTENIDO

TABLA DE ILUSTRACIONES

RESUMEN

El desarrollo de este informe se centra en las diferentes estrategias que podrían llegar a ser adoptadas por “WhiteHose Security” en su búsqueda de personal e implementación de los equipos de Redteam y Blueteam según la metodología escogida, en busca del aseguramiento y garante de soluciones tecnológicas enfocadas en el sector de los servicios informáticos. Para el desarrollo de este ejercicio se realizará un caso ficticio sobre la organización “WhiteHose Security”, la cual, está en medio de la implementación de un equipo propio de Redteam y Blueteam necesitando el seleccionar herramientas, personal y cambiando su enfoque legal para el proceso con el fin de garantizar la disponibilidad, integridad y confidencialidad de sus servicios, así como la integridad y legalidad del proceso.

INTRODUCCIÓN

La sociedad actual y los acontecimientos a nivel mundial resultado de la pandemia de Covid-19 han causado un gran cambio en los paradigmas sociales relacionados a la forma en cómo se interactúa y se realizan las tareas del día a día, acciones que van desde consignación bancaria, compra de alimentos/servicios e incluso la interacción personal, han llevado a una mayor integración de la industria de la informática en cada uno de los aspectos fundamentales y funcionales del individuo moderno. Este cambio trae como consecuencia un gran crecimiento del entorno funcional de sistemas, cada servicio necesita ser diseñado, desarrollado e implementado de forma tal que siga ciertos parámetros y leyes que buscan proteger la confidencialidad, integridad y disponibilidad de los servicios, así como de la información personal y empresarial que este almacena. En busca de esa seguridad necesitada se han desarrollado múltiples tipos de controles y un mejoramiento continuo en todo el proceso de despliegue de un servicio, uno de los aspectos más importantes “La Auditoria de sistemas”.

La auditoría de sistemas es un proceso en donde se busca que cada uno de los servicios informáticos, activos de software/hardware y redes de comunicaciones sean lo más seguras posible, este rastrea cada uno de los componentes por medio de herramientas informáticas o flujos de código, seguimiento de línea base de seguridad y análisis de entorno, estos llevan al descubrimiento y posterior ejecución de la remediación en aras del aseguramiento de los servicios ofrecidos. Entre las tantas iniciativas que se encuentran en estos procesos de auditoria encontramos los Redteam y Blueteam, estos equipos son un grupo curricular que cumple ciertas funciones activas de auditoría sobre el entorno corporativo, su función está en un continuo sistema de ataque y detección de vulnerabilidades sobre las piezas que componen los servicios y su entorno, de tal manera que llegan a simular situaciones de alto riesgo y que pudieran llegar a causar la afectación en cualquiera de sus participantes. Estos equipos no son de fácil implementación y requieren una gran cantidad de trabajo y exactitud en cuanto a temas metodológicos y legales, por ello es necesario una correcta definición del mismo para no incurrir en problemas durante su implementación y desarrollo.

GLOSARIO

Software Libre: La organización GNU describe el software libre como "software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software."[1], esto comprende que cada una de las piezas catalogadas como software libre pueden ser usadas, modificadas o distribuidos sin necesidad de una licencia o pago por la misma.

Proyecto de software libre: Estos proyectos son librerías que cumplen funciones específicas dentro de un marco de funcionamiento mucho mayor, es decir, son programas que cumplen tareas específicas y tienen una licencia de software libre.

Amenaza: El instituto nacional de seguridad de España[2], describe una amenaza como el aprovechamiento de una vulnerabilidad, es decir, el uso de una vulnerabilidad de manera activa donde se atenta con la seguridad informática o de la información.

Redteam: La escuela de negocios ESIC[3], define Redteam como un equipo externo que realiza una constante amenaza a los activos de software e información de una organización, estos se deben dedicar a manipular, filtrar, robar información, denegación del servicio o fraude de manera controlada y dando como resultado un informe para su posterior remediación.

Blueteam: Es un equipo enfocado en la prevención de incidentes de seguridad, este estudio los comportamientos de los sistemas informáticos y de sus usuarios. Según IT digital security[4] este debe ser conformado por un grupo de especialistas multidisciplinares con el conocimiento necesario para administrar cada uno de los frentes de ataque en sus servicios.

Hardening: La acción de Hardening consiste en tomar todas aquellas vulnerabilidades encontradas en el entorno corporativo, en las definiciones del CISET[5] el Hardening comprende cada uno de los componentes de software y

[1] GNU. ¿Qué es el software libre? 2021 Free Software Foundation, Inc [Sitio web] (30/03/2022). Disponible en: https://www.gnu.org/philosophy/free-sw.es.html
[2] INCIBE, Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? INCIBE, 2019. [Sitio web] (30/03/2022). Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
[3] ESIC, ed team: qué es, estrategias y ejemplo de un caso real. ESIC, 2018. [Sitio web] (30/03/2022). Disponible en: https://www.esic.edu/rethink/tecnologia/red-team-experiencia-en-ataque
[4] IT DIGITAL SECURITY, ¿Qué es un Blue Team y cómo trabaja? IT DIGITAL SECURITY, 2018. [Sitio web] (30/03/2022). Disponible en: https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja
[5] CISET, Hardening. CISET, 2020. [Sitio web] (30/03/2022). Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening.

hardware existentes, que, debido al cambio continuo y deficiencias de componentes debe ser mejorado.

Pentesting: INCIBE define el pentesting como “conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades”[6], este utiliza herramientas de descubrimiento y auditoria que son capaces de reconocer de manera escalonada características del sistema en busca de fallos en los mismos.

Vulnerabilidad: Una vulnerabilidad es un componente de código o software que presenta defectos, pero, estos defectos deben permitir que un tercero “atacante” pueda sacar provecho de ellos en un entorno corporativo a que no pertenece como lo indica Software LAB[7].

CVE: INCIBE[8] define CVE como “Common Vulnerabilities and Exposures, siglas CVE, es una lista de información registrada sobre conocidas vulnerabilidades de seguridad, donde cada referencia tiene un número de identificación único.1 De esta forma provee una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.”.

Intrusión: UUS Seguridad integral[9] en su artículo sobre intrusión y sistemas de prevención resume intrusión como “un ingreso no autorizado a un sistema, red o dispositivo”, pero, es necesario aclarar que esta se realiza por medio del aprovechamiento de una vulnerabilidad, haciendo latente una amenaza de seguridad.

Entorno corporativo: Es el conjunto de tecnologías, personas y espacios que hacen parte del desarrollo comercial de una empresa, Nuria Estruga[10] lo comprende como todo aquel participante en el desarrollo sea tecnología o persona, y que puede ser usado por un tercero para su propio beneficio.

---

[6] INCIBE, ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE, 2019. [Sitio web] (30/03/2022). Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

[7] SOFTWARE LAB, ¿Qué es una vulnerabilidad informatica? SOFWARE LAB, 2018. [Sitio web] (30/03/2022). Disponible en: https://softwarelab.org/es/que-es-una-vulnerabilidad-informatica/

[8] INCIBE, Vocabulario General CVE. INCIBE, 2015. [Sitio web] (30/03/2022). Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=2142.html

[9] USS Seguridad integral. Sistema de detección de intrusos: tipos y ejemplos. USS, 2019. [Sitio web] (30/03/2022). Disponible en: https://uss.com.ar/preguntas-frecuentes/sistema-de-deteccion-de-intrusos/.

[10] ESTRUGA NURIA, La importancia de la seguridad informática en el entorno empresarial. EALDE, 2020. [Sitio web] (30/03/2022). Disponible en: https://www.ealde.es/importancia-seguridad-informatica-empresas/

OBJETIVOS

OBJETIVO PRINCIPAL

- Presentar de manera formal las falencias encontradas en el proceso de captación de talento e implementación de equipos de Redteam y Blueteam, así como de los escenarios de ataque presentados.

OBJETIVOS ESPECIFICOS

- Referenciar las políticas del país en cuanto a los temas relacionados a seguridad informática que podrían llegar a afectar los procesos de contratación y formación de equipos de Redteam y Blueteam.
- Reconocer las falencias presentadas en el proceso de contratación de la entidad en cuanto a la aplicación de las diferentes normas legales vigentes.
- Explorar los escenarios objetivo-presentados y presentar las falencias encontradas en las máquinas virtuales de estudio entregadas.
- Presentar un resumen de las vulnerabilidades encontradas y como solventarlas dando a conocer recomendaciones de remediación.

CASO 1: ACTUACIÓN ETICA Y LEGAL

LEGISLACIÓN VIGENTE

Como primer paso, se pasará a reconocer la Ley 1273 de 2009[11] como única legislación vigente en Colombia para el tema de ciberseguridad, lo cual hace bastante pobre le control del país sobre este tema en comparación con otros países de Latinoamérica y el mundo. Este documento se encuentra abordado de manera general y poco detallada en su mayoría las posibles acciones que podría realizar un ciberdelincuente las cuales son presentadas como:

- Acceso abusivo a sistemas informáticos: Todo actor que ingrese de manera abusiva a un sistema de información de cualquier tipo será penado por el artículo 269A con entre 100 y 1000 salarios mínimos vigentes y posiblemente 48 a 96 meses de prisión.

- Obstaculización no autorizada de sistemas informáticos: Todo actor que altere de cualquier manera el funcionamiento de un sistema informático será penado por el articulo 269B con entre 100 y 1000 salarios mínimos vigentes y posiblemente 48 a 96 meses de prisión.

- Interceptación no autorizada de datos: Todo actor que acceda a información confidencial o sensible será penado por el articulo 269C con entre 32 y 72 meses de prisión.

- Daños a sistemas informáticos: Todo actor que sin ser parte de un entorno corporativo o se encuentre en funciones sobre el mismo realice un daño sobre un sistema informático será penado por el articulo 269D con entre 100 y 1000 salarios mínimos vigentes y posiblemente 48 a 96 meses de prisión.

- Uso de software malicioso: Todo actor que use, implemente, cree o distribuya software malicioso será pena por el articulo 269E con entre 100 y 1000 salarios mínimos vigentes y posiblemente 48 a 96 meses de prisión.

- Violación de datos personales: Todo actor que obtenga, compile, substraiga o utilice a beneficio propio datos personales o sensibles de terceros será penado por el articulo 269F con entre 100 y 1000 salarios mínimos vigentes y posiblemente 48 a 96 meses de prisión.

[11] SCIELO, Delitos informáticos y entorno jurídico vigente en Colombia. SCIELO, 2018. [Sitio web] (30/03/2022). Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

- Suplantación de sitios web: Todo actor que suplante un sitio web oficial será penado por el articulo 269G con entre 100 y 1000 salarios mínimos vigentes y posiblemente 48 a 96 meses de prisión.

ACCIONAR DE LOS EQUIPOS DE REDTEAM Y BLUETEAM

Como segundo paso se pasará a determinar las acciones éticas que deberían cumplir los profesionales pertenecientes a los equipos de en Colombia según COPNIA (Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares) que es la base legal en este dominio:

- Deberes generales de los profesionales: El articulo 31 en sus numerales e, f y g determinan que los profesionales en cualquiera de sus funciones deben colaborar con las autoridades competentes según se requiera para la ejecución de sus investigaciones.

- Deberes generales y prohibiciones de los profesionales: Los artículos 32,34,35 y 40 hablan sobre las prohibiciones y actos que no deben ser realizados por un profesional que actúe correctamente de manera ética y moral:

    - Artículo 32: No aceptar ningún tipo de soborno o compensación por realizar acciones fuera de su alcance o de manera ilícita.

    - Artículo 34: No aceptar trabajos que vayan contra la disposición legal actual.

    - Articulo 35 y 40: Respetar y hacer respetar su profesión cumplido a cabalidad las disposiciones legales en Colombia.

OTROS ASPECTOS EN EL DESARROLLO DE SUS FUNCIONES[12]

Como tercer paso se tendrá en cuenta algunos accionares de los equipos de Redteam y Blueteam que deben ser tenidos en cuenta para el correcto cumplimiento de las leyes anteriormente expuestas:

- Dado que las acciones realizadas por el Redteam comprenden acciones que van contra la ley es necesario el plasmar por medio de documentación las

[12] MISAZA719, Metodologías y Herramientas de Ethical Hacking. MISAZA719, 2013. [Sitio web] (30/03/2022). Disponible en: https://seguridadinformaticahoy.blogspot.com/2013/02/metodologias-y-herramientas-de-ethical.html

funciones y el alcance que tiene el equipo, dando previa autorización para su desarrollo.

- El equipo de Blueteam tiene como función el prevenir e identificar los comportamientos penados por la ley tanto del equipo de Redteam, como de usuarios internos.

- El proceso de equipos Redteam y Blueteam debe ser continuo, esto lleva a que en cualquier momento puedan ser encontradas vulnerabilidades y fallos de seguridad que comprometan la infraestructura de la organización, lo cual permita un modelo de mejora continua que lleve el nivel de seguridad a nuevos niveles.

- Todas las herramientas que se usarán y expondrán para este ejercicio deberán dar de software libre con licencia OpenGL tanto en sistemas operativos, como en formas de descubrimiento y herramientas administrativas.

FUNCIONES EQUIPO REDTEAM[13]

Para el ejercicio y como parte de la exposición y limitación de funciones del equipo Redteam se definen sus funciones como:

- Descubrimiento de sistemas: El equipo podrá realizar exploración externa de los equipos de la organización con tal de reconocer e identificar posibles vulnerabilidades tanto por sistemas operativos, exposición de información, escaneo de puertos u otros que vengan al caso.

- Comprobación de casos de vulnerabilidad: Para las vulnerabilidades encontradas podrán el verificar por medio de código, practicas o exploits que el sistema operativo o software encontrado es definitivamente vulnerable.

- Mapeo de activos o servicios: El equipo de Redteam deberá intentar hacer un mapa de la organización con la información conseguida en estos escaneos, lo cual será de gran ayuda para conocer la información que podría obtener un atacante.

- Diseño y plan de acción: Durante el proceso, el equipo de Redteam puede conseguir mayo información sobre los activos, versión u otros softwares, es necesario el cambiar el modelo y tipo de explotación para obtener mejores resultados.

[13] KEEPCODING, ¿Qué es Red Team en Ciberseguridad? KEEPCODING, 2018. [Sitio web] (30/03/2022). Disponible en: https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

- Comunicación de resultados: El equipo de Redteam realizará un informe por el cual será llevado al equipo de Blueteam en busca de solventar los hallazgos.

- Para estos ejercicios no habrá implicaciones de acceso físico o ingeniería social.

FUNCIONES EQUIPO BLUETEAM[14]

Para el ejercicio y como parte las funciones internas del equipo de Blueteam se determinan que las tareas a realizar comprenden:

- Descubrimiento de sistemas: El equipo podrá realizar exploración interna de los equipos de la organización con tal de reconocer e identificar posibles vulnerabilidades tanto por sistemas operativos, exposición de información, escaneo de puertos u otros que vengan al caso.

- Comprobación de casos de vulnerabilidad: El equipo de Blueteam comunicara las posibles vulnerabilidades al equipo Redteam para su exploración.

- Diseño y plan de acción: Al recibir el informe del Redteam, Blueteam pasará a el hardening y solución de las vulnerabilidades encontradas por lo cual deberá documentar el proceso y realizar registro sobre los cambios realizados.

- Auditoria: Garantizar los controles y su correcta aplicación, así como realizar control de auditoria SIEM.

- Cumplimiento línea base: Es necesario el tener sistemas operativos con línea base de seguridad

FALLAS ENCONTRADAS EN EL PROCESO DE CONTRATACIÓN

En el anexo 2.1(Generalidades del proceso): Como la falta más evidente está el continuo uso de un contrato no revisado de origen dudoso (dada la situación de quien lo redacto y reviso) en un proceso tan delicado como lo es el manejo y trata de equipos de Redteam y Blueteam, dado que estos equipos obtienen y manejan información privilegiada que debe tener un estricto control y manejo legal. En este tipo de contratos se debe delimitar de forma correcta las funciones y alcance de

[14] IT DIGITAL SECURITY, ¿Qué es un Blue Team y cómo trabaja? IT DIGITAL SECURITY, 2018. [Sitio web] (30/03/2022). Disponible en: https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja

cada equipo, así como la especificación de procesos en herramientas y alcance permisitos, trata de información y posibles afecciones a casuar, el dejar este tipo de contrato sin revisión lleva a que la empresa no tenga ese control estricto necesario y pueda en algunos escenarios llegar a incurrir en delitos informáticos. También está el tema de exposición de recursos en la prueba, considero que es más una mala práctica dado que están dando información de las herramientas y posible estructura interior.

En el anexo 2.2 (Contrato Legal): En el contrato se observa una falta ética y legal gigante con este anexo “en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados” que de por si lleva a intentar esta sobre la ley por medio de cláusulas en contratos, están buscando mantener como secreta interceptaciones ilegales y que no van con el código de ética, laboral o legal del país e ignora completamente a contraprestación las obligaciones legales del mismo.

En el anexo 3 se hace referencia directamente a procesos ilegales en un anexo de confidencialidad “en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados” lo cual es una clara falta que busca estar por encima de la ley y va contra el código tanto de ética como legal “Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.” Dado que en el contrato se referencia posteriormente a que se tratan datos de terceros y otros procesos no especificados; también vemos que es de completa responsabilidad del profesional la información manejada, por tanto intentan zafarse de su responsabilidad legal lo cual se refleja en “Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.” Lo que también va contra el código profesional “Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder; teniendo en cuenta que una de las cláusulas dice que no podría denunciar actos ilegales dentro de la empresa, estaría violando es inciso.”

En general vulnera toda la ley dado que no hay un alcance en el proceso, pero, si fuéramos a ser específicos según el contrato seria obtención de datos de medios informáticos de un tercero.

POSIBLES METODOLOGIAS A USAR EN EL PROCESO

ISSAF (INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK)[15]: Marco de trabajo en el cual se define un plan de pruebas, donde ciertos dominios cubren procesos tecnológicos específicos consignados en un documento general guía. Es una de las metodologías de mayor uso en entidades financieras, de servicios y tecnológicas en cuanto a gestión de su seguridad interna y aseguramiento de procesos, esta busca el reconocimiento de las fortalezas u debilidades mediante el desarrollo de una auditoría a las entidades, donde, una serie de dimensiones a evaluar genera un perfil resumen de seguridad. Entre las dimensiones evaluadas encontramos:

- Políticas y procedimientos de seguridad.
- Áreas de comercio y servicio TI.
- Pentesting y análisis de vulnerabilidades.
- Modelos de evaluación generales o controles de seguridad (Configuraciones, riesgos, procesos de negocio y tecnológicos).

Este modelo se centra en el cumplimiento y aplicación de políticas tales como ISO27000 y practicas relacionadas como pueden ser los marcos de trabajo como SCRUM. Donde unas etapas de preevaluación dan una vista general del nivel de seguridad y necesidades de implementación,

OS (OFFENSIVE SECURITY)[16]: Esta metodología consiste en a la ejecución ordenada de una serie de herramientas con fin de probar el nivel de seguridad de un entorno corporativo y su infraestructura, es más practica y menos analítica. Las herramientas seleccionadas den estar orientadas a reconocer las falencias de seguridad, vulnerabilidades, malas prácticas y ser agresivas con el entorno objetivo de tal manera que causen cambios significativos en su comportamiento al verse comprometidas. Esta metodología busca el emular a un 100% un ataque real como parte de un proceso de evaluación de seguridad, por tanto, también se reflejarán las

[15] OISSG. Information Systems Security Assessment Framework (ISSAF). OISSG, 2006. [Sitio web] (30/03/2022). Disponible en: https://untrustednetwork.net/files/issaf0.2.1.pdf

[16] IN-NOVA. Hacking Ético y Técnicas de Hacking Avanzadas sobre Windows. IN-NOVA, 2020. [Sitio web] (30/03/2022). Disponible en: https://www.in-nova.org/es/soluciones-y-servicios/formacion-y-entrenamiento/formacion-activa/hacking-etico-tecnicas-hacking-windows

consecuencias y alcance de este, esto con el fin de conocer a detalle el nivel de seguridad sin saltar sobre ningún control a implementar.

Esta metodología sigue una serie de pasos, donde, por medio de una pregunta se definirá el ambiente desde donde se lanzará el ataque como primera fase, se reconocerán los resultados en la segunda y se realizara un reporte de resultados como fase final, estos pasos son:

- Posicionamiento: ¿Dónde estará ubicado el atacante? ¿Será externo o interno? ¿Cómo se espera lograr con el ataque?
- Visibilidad: ¿Qué información inicial se dará al atacante? ¿Qué tipo de activos intentara atacar?
- Perfil adoptado: ¿Qué tipo de perfil tomara el atacante? ¿Cuál es la necesidad del ataque? ¿Qué tipo de acceso tendrá el atacante?
- Reconocimiento pasivo: ¿Se entregó la información necesaria? ¿Conoce el atacante la información? ¿Es el perfil muy poco para las tareas a realizar? ¿Cómo se accederá al objetivo?
- Reconocimiento activo superficial: ¿Qué puntos son necesarios al reconocer el camino al objetivo? ¿Qué más activos se verán afectados durante el ataque?
- Reconocimiento activo en profundidad: ¿Qué protocolos serán usados? ¿Cuál es el canal principal del ataque? ¿Qué aplicaciones se verán involucradas?
- Análisis de vulnerabilidades: ¿Qué vulnerabilidades fueron encontradas? ¿Qué puertos están expuestos? ¿Cuál es el alcance de cada vulnerabilidad? ¿Están las vulnerabilidades encontradas realmente en el sistema objetivo?
- Explotación o ataque puro: ¿fueron las vulnerabilidades encontradas realmente explotables? ¿Que alcance tuvo el ataque final? ¿Cuáles fueron las herramientas más efectivas?

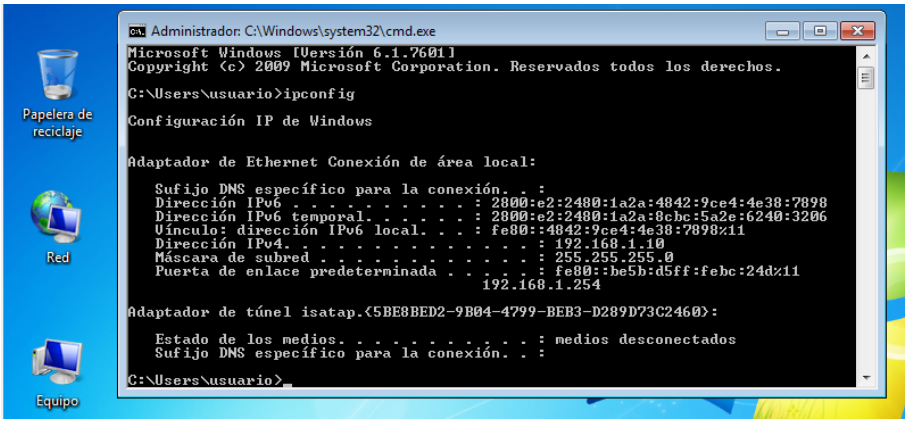
Como pasos finales pasamos a reconocer aquellos pasos prácticos donde se busca la terminación del proceso y su informe:

- Consolidación: Consiste en acoplar y juntar los diferentes tipos de información y resultados del proceso.
- Borrado de rastros: Se busca el ocultar las huellas del proceso.
- Reportes: es un resumen general de todo el proceso, donde, son presentados resultados y posibles resultados de auditoría sobre el sistema objetivo u entorno corporativo estudiado.

CASO 2: ANALISIS DEL ATAQUE

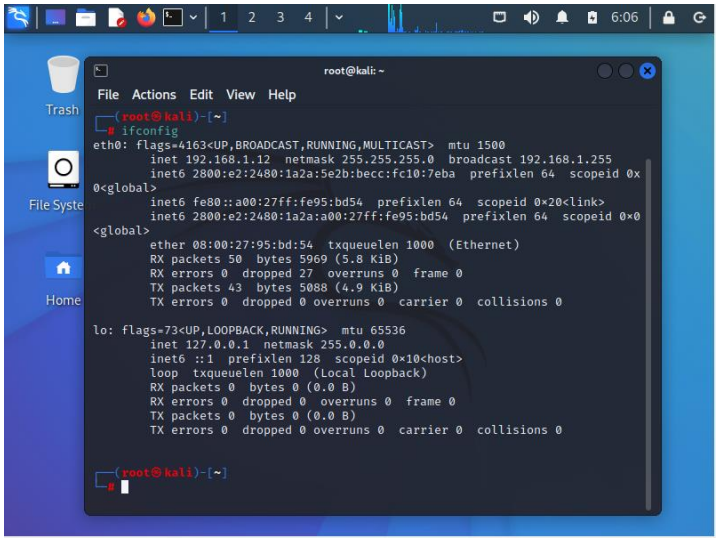
PASOS INICIALES: Características/exploración del laboratorio.
Como primer paso se muestra la información asociada a las maquinas pertenecientes al laboratorio realizado:

Imagen 1. Windows 7 x64.



Fuente: propia

Imagen 2. Kali Linux.

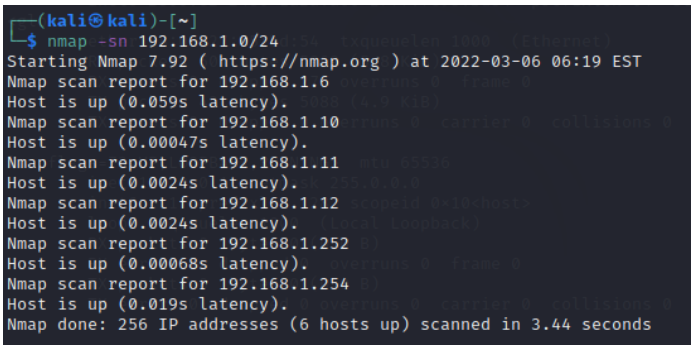


Fuente: propia

Para la realización de este ejercicio pasaremos a usar 2 software libres presentes en el sistema operativo Kali Linux, por un lado, para el escaneo de puertos se utilizará NMAP y para el escaneo de vulnerabilidades en sistema operativo y software presentaremos metaexploit.

NMAP es una herramienta bastante popular usada en temas de descubrimiento de activos sobre la red. En este caso y para simular el ataque vamos a verificar como seria la fase de descubrimiento y el posterior escaneo con la herramienta. Para esto comenzamos descubriendo los activos disponibles en la red con el comando “nmap -sn 192.168.1.0/24”

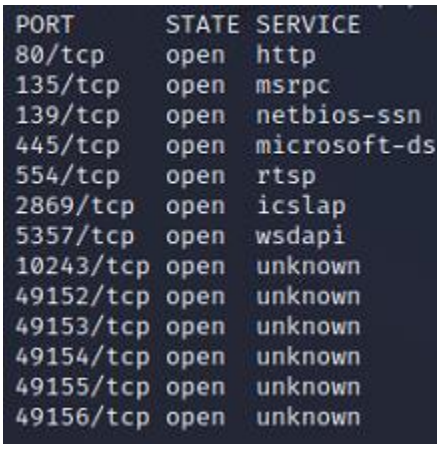
Imagen 3. Escaneo inicial.



Fuente: propia

Podemos ver que se encuentra el escaneo de la máquina de Windows 7 x64 la cual está por su IP, se procede a realizar un escaneo de puertos de las maquinas objetivo.

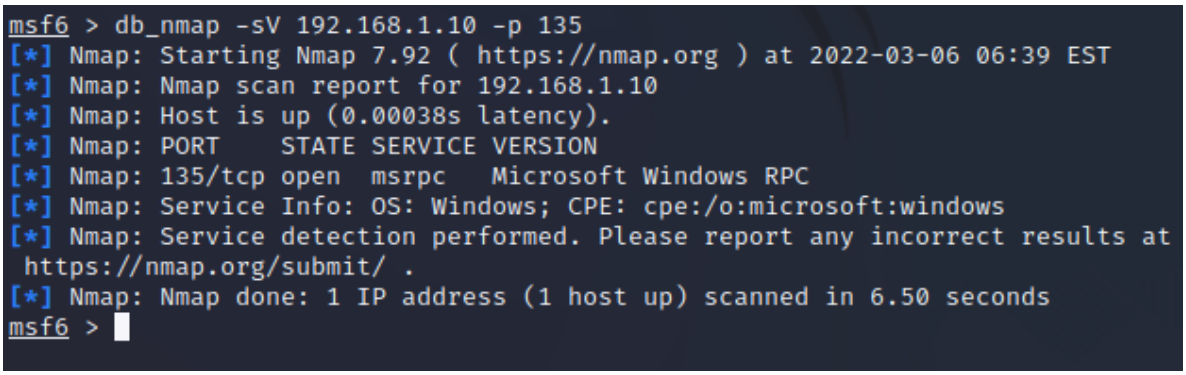
Imagen 4. Escaneo de puertos w7x64.



Fuente: propia

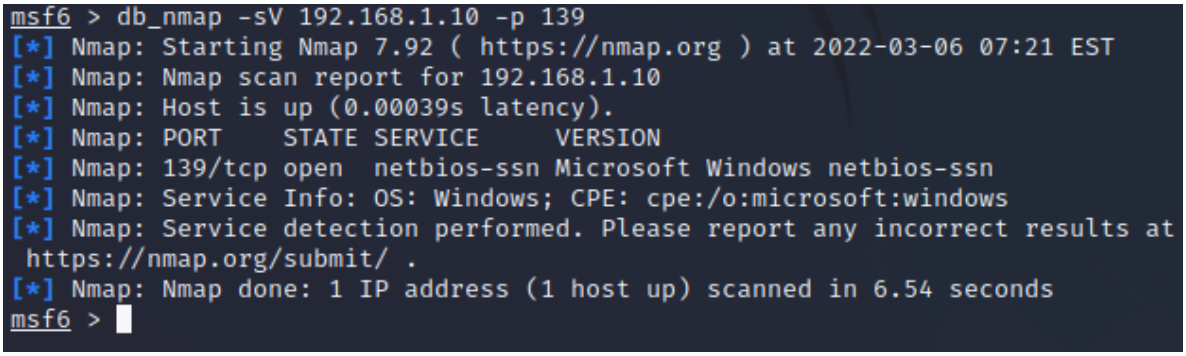
Identificando ya los puertos de la maquina pasaremos con metaexploit a verificar el servicio específico y versión en cada uno de ellos.

Imagen 5. Escaneo puerto 135.



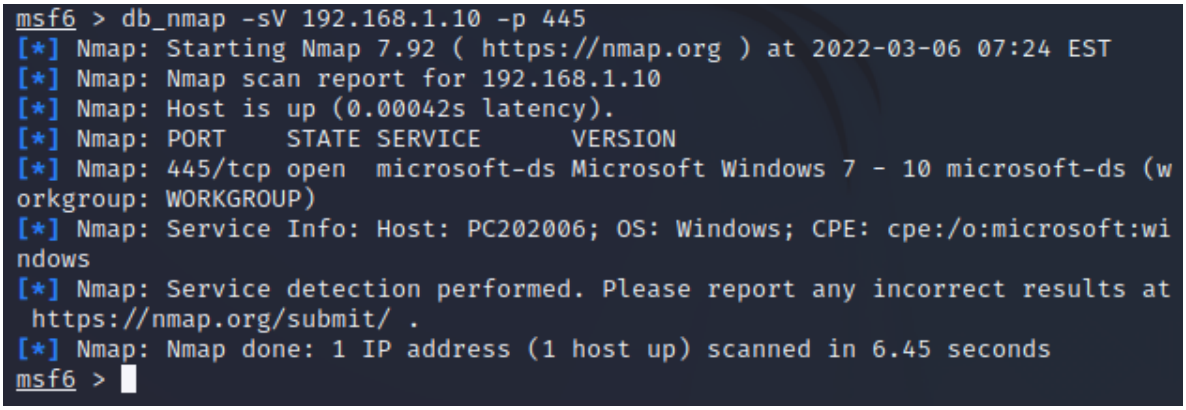
Fuente: propia

Imagen 6. Escaneo puerto 139.



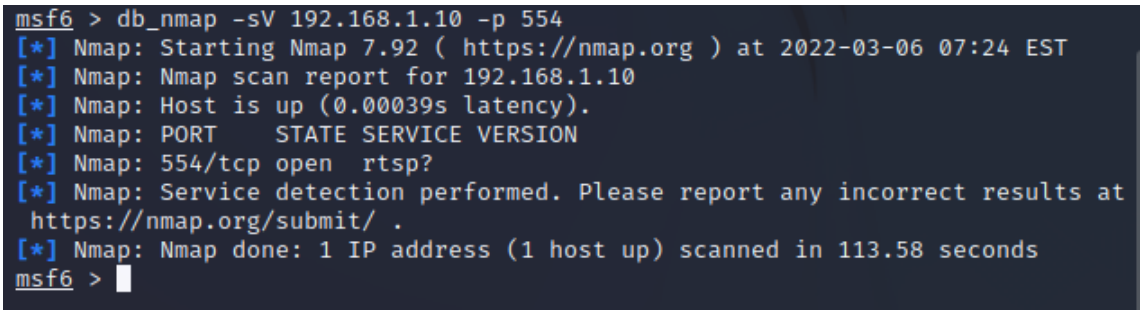
Fuente: propia

Imagen 7. Escaneo puerto 445.



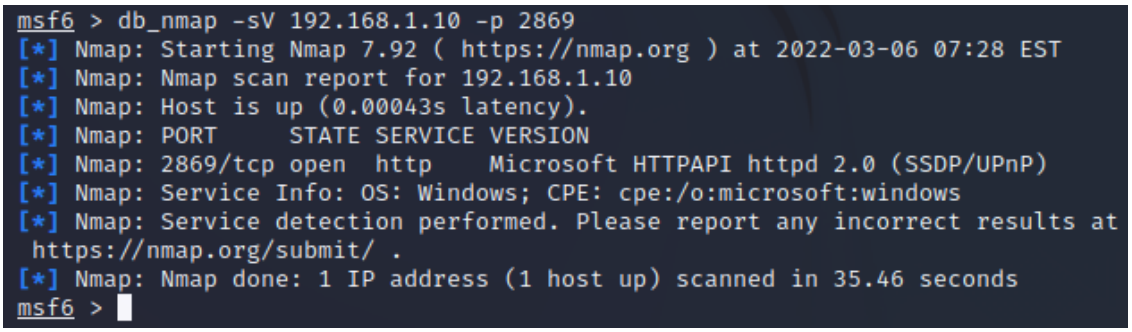
Fuente: propia

Imagen 8. Escaneo puerto 554.



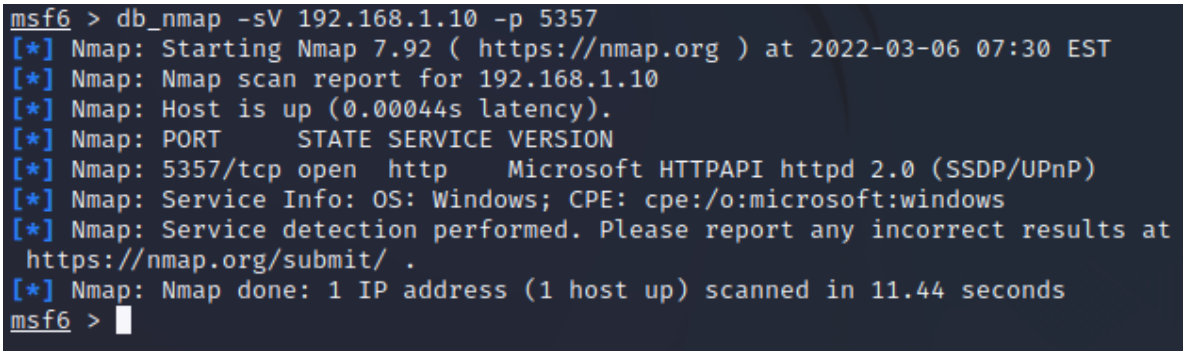
Fuente: propia

Imagen 9. Escaneo puerto 2869.



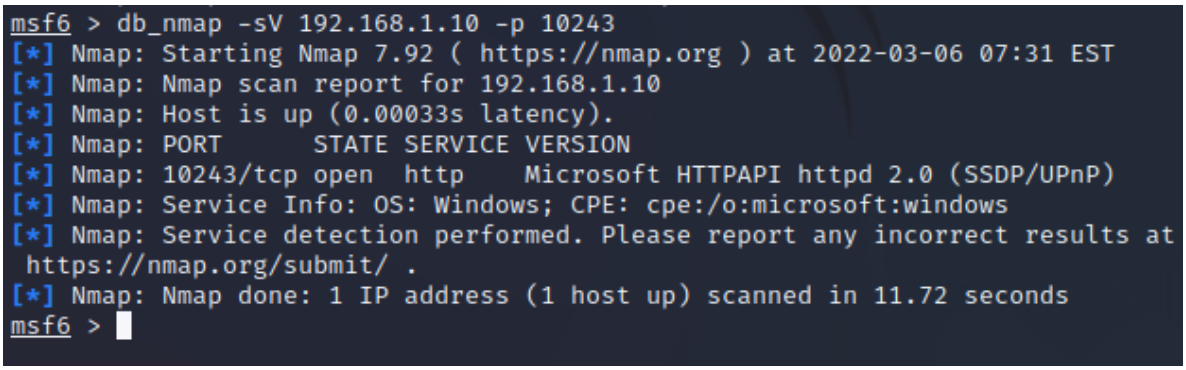
Fuente: propia

Imagen 10. Escaneo puerto 5357.



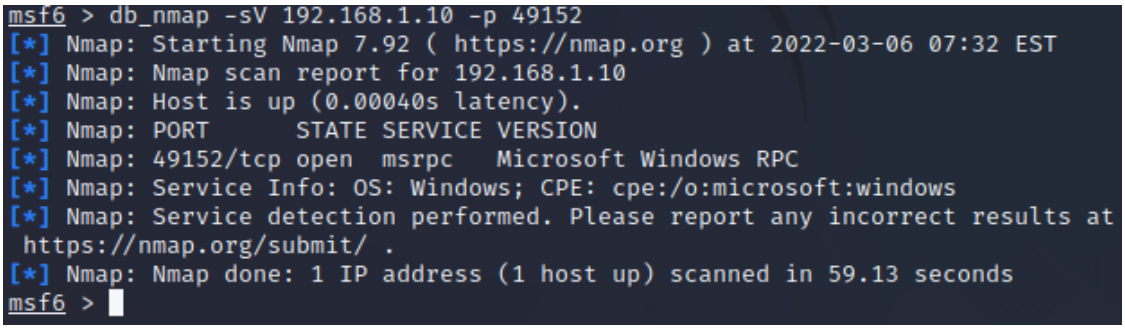
Fuente: propia

Imagen 11. Escaneo puerto 10243.



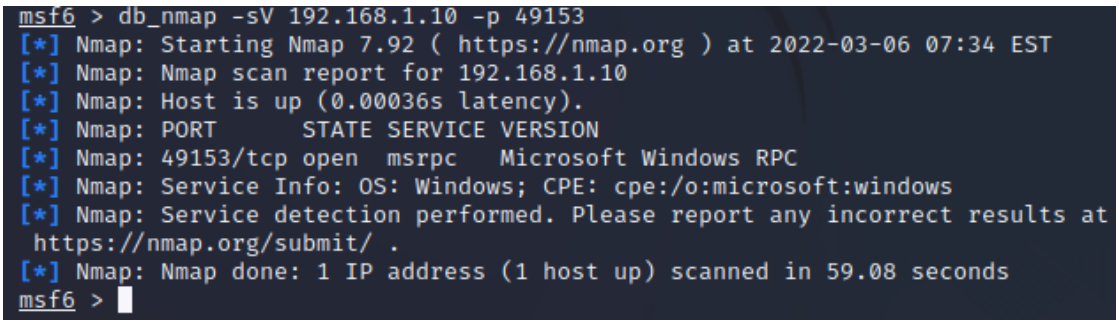
Fuente: propia

Imagen 12. Escaneo puerto 49152.



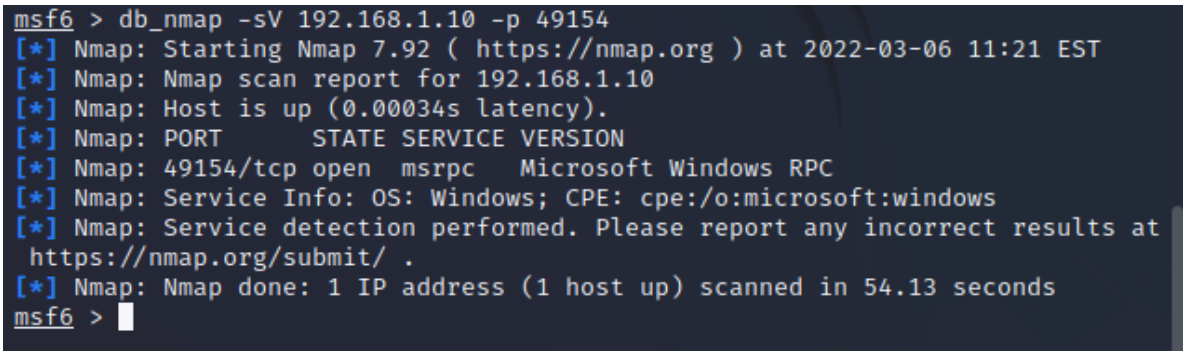
Fuente: propia

Imagen 13. Escaneo puerto 49153.



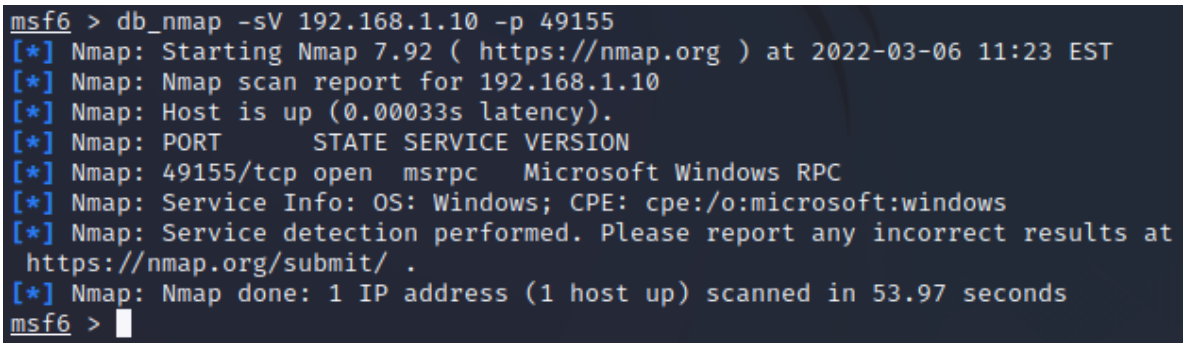
Fuente: propia

Imagen 14. Escaneo puerto 49154.



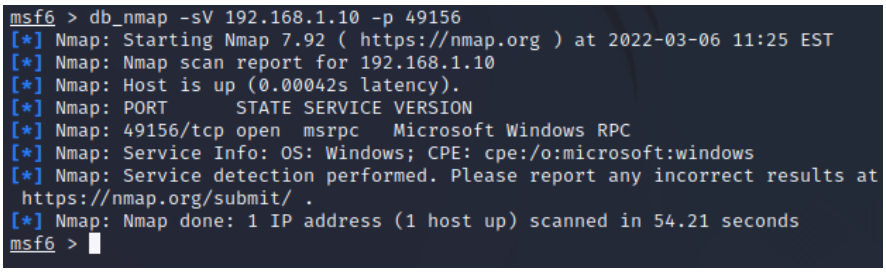
Fuente: propia

Imagen 15. Escaneo puerto 49155.



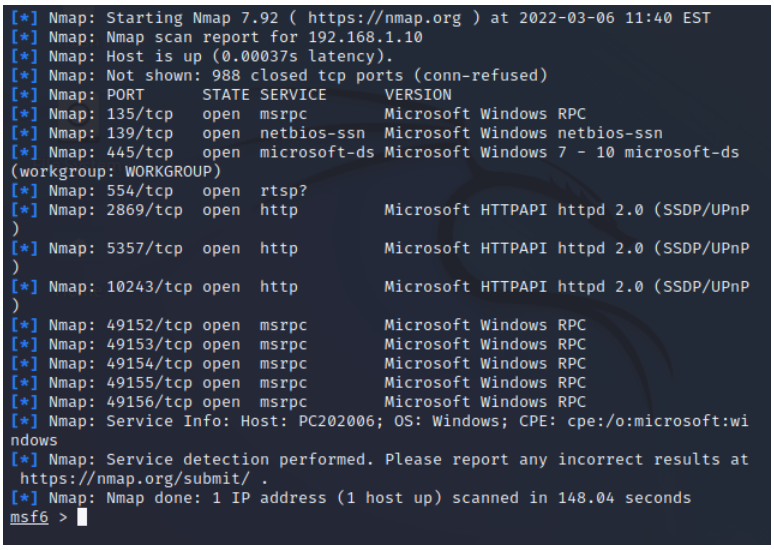
Fuente: propia

Imagen 16. Escaneo puerto 49156.



Fuente: propia

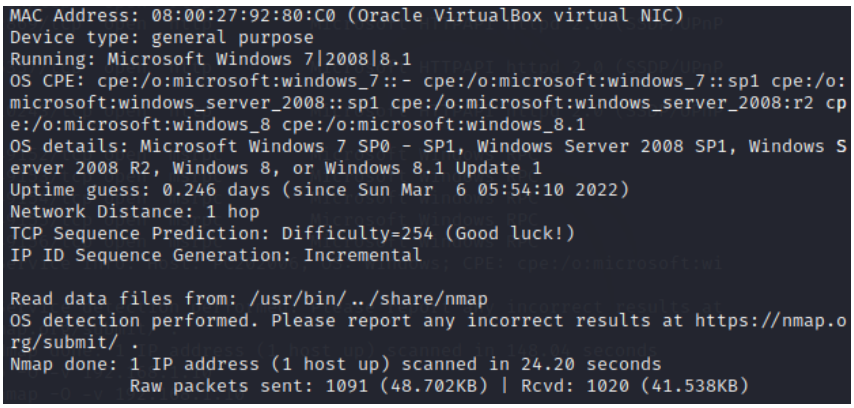
Imagen 17. Escaneo resumen 1.



Fuente: propia

Esa es la información que un atacante pudo extraer de la máquina previa al ataque, además, se puede obtener el sistema operativo de la maquina a manera de perfilamiento del ataque.

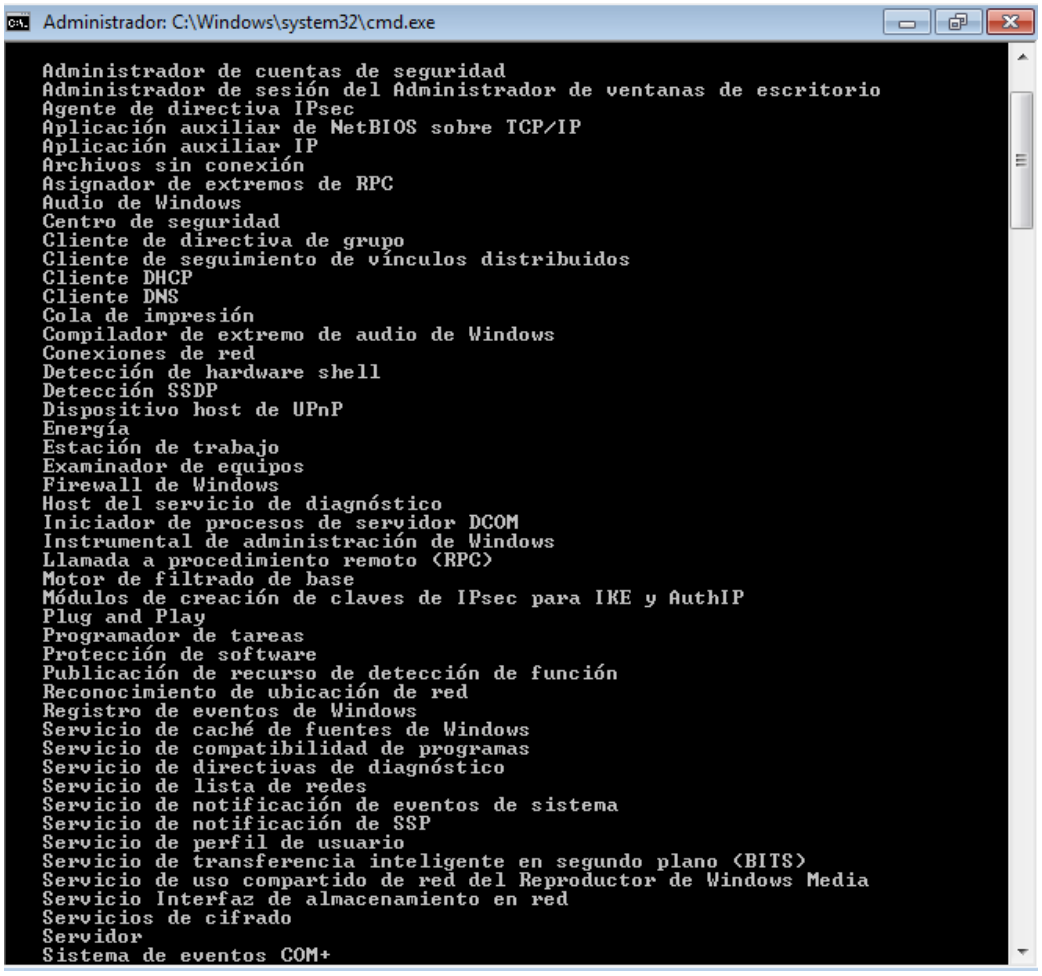
Imagen 18. Escaneo resumen 2.



Fuente: propia

Se buscan los servicios que actualmente tiene la maquina en ejecución.

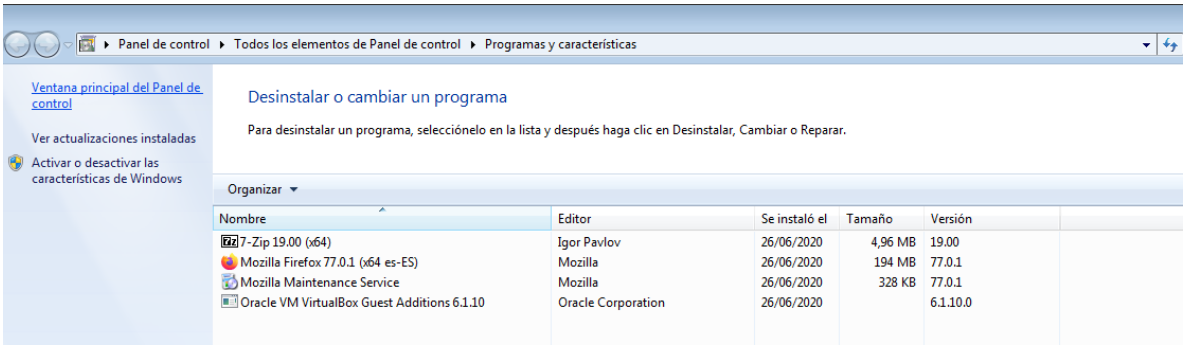
Imagen 19. Servicios en la máquina.



Fuente: propia

En cuanto a los programas instalados en la máquina no veo ninguna referencia a los que muestra en el anexo aun cuando la vulnerabilidad mencionada persiste:

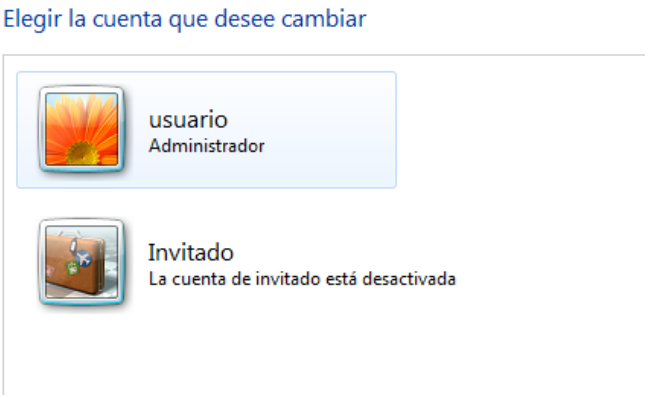
Imagen 20. Programas.



Fuente: propia

Se busca el tema de los usuarios administradores, se evidencia un único usuario administrador y ningún otro habilitado.

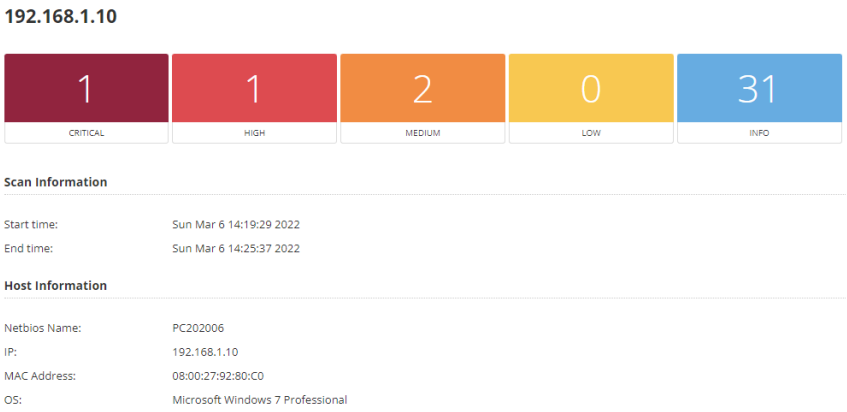
Imagen 21. Usuarios en equipo objetivo.



Fuente: propia

Se pasa a hacer un escaneo de vulnerabilidades completo en busca de la forma en como atacaron esta máquina para obtener todas las vulnerabilidades en la misma. Se obtiene la siguiente información de la maquina:

Imagen 22. Resultados del Scan.



Fuente: propia

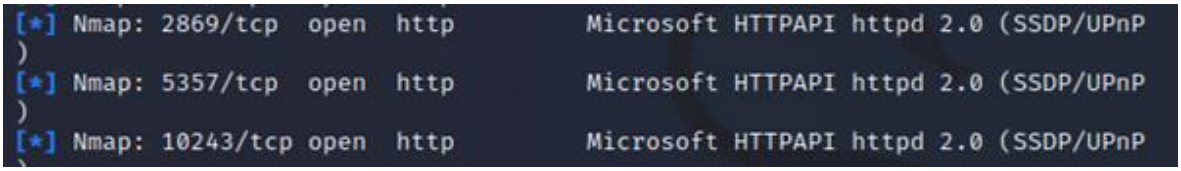
Nos enfocaremos en las 2 vulnerabilidades Critica y alta, además, de un servicio HTTP abierto por el puerto 80 que se puede llegar a observar por medio del software

Rejetto en su ejecución, es necesario el aclarar que este software se maneja como servicio por tanto no se observara instalado.

POSIBLE ATAQUE 1: Rejetto.
CVE-2014-6287(CVSS 3.1: 8.3 Alta): findMacroMarker en parserLib.pas en Rejetto HTTP File Server (también conocido como HFS o HttpFileServer) 2.3x anterior a 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda.

Teniendo en cuenta su descripción se buscará cada puerto relacionado a HTTP entre los que podemos observar:

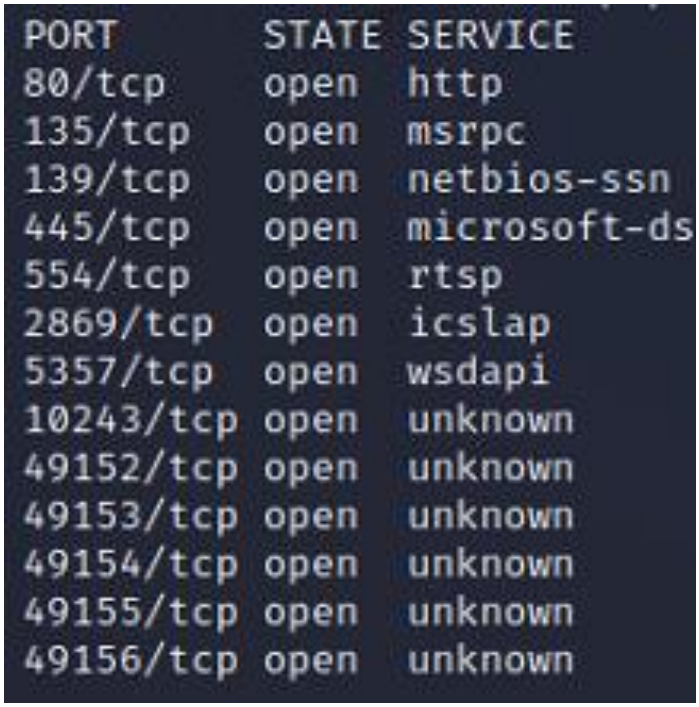
Imagen 23. Puertos abiertos.



Fuente: propia

La información de un usuario administrador coincidía con la maquina provista en la fase 1. Entre los puertos abiertos encontramos:

Imagen 24. Puertos abiertos.

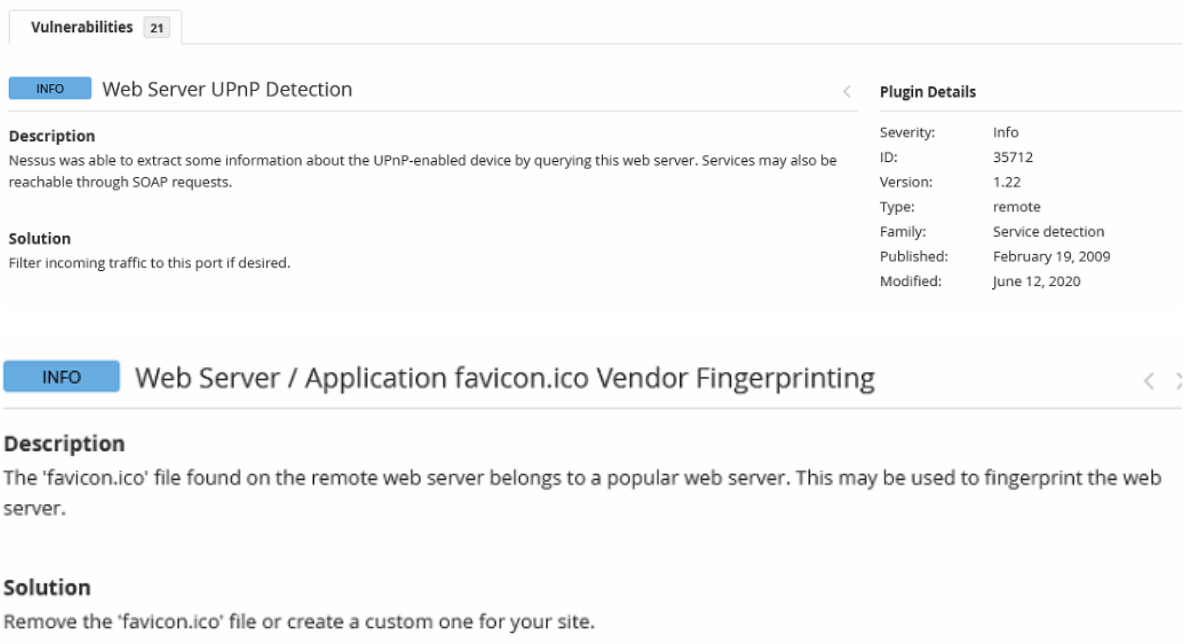


Fuente: propia

Se identifica una máquina de Windows 7 x64 SP1 y no se encuentra rastros de los servicios mencionados en los anexos. Se encuentra que la pista de meterpreter da una vulnerabilidad de SMBv1 que podría ser explotable.

Como pista dan también el nombre Rejetto, que puede dar pistas sobre la vulnerabilidad y exploit con el mismo nombre.

Imagen 25. BD metaexploit HTTP Rejetto.

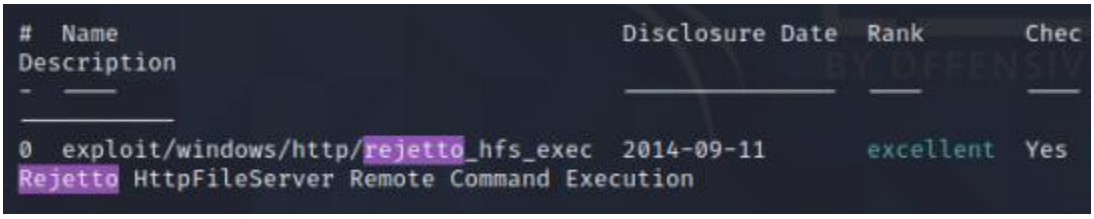


Fuente: propia

Entre los hallazgos encontramos también puertos HTTP abiertos, y como tenemos un rastro con el nombre Rejetto pasaremos a buscar y aplicar los exploits relacionados. Como primer paso identificamos el CVE y posible modo de explotación (Información provista en la etapa de descubrimiento). Es necesario realizar la búsqueda de en las bases de datos de metaexploit para saber cuáles serían los conjuntos de exploits y configuraciones necesarias a realizar sobre los puertos objetivos.

Se encuentra que la configuración de metaexploit provee el siguiente paquete de explotación para esta vulnerabilidad: “exploit/Windows/http/rejetto_hfs_exec”

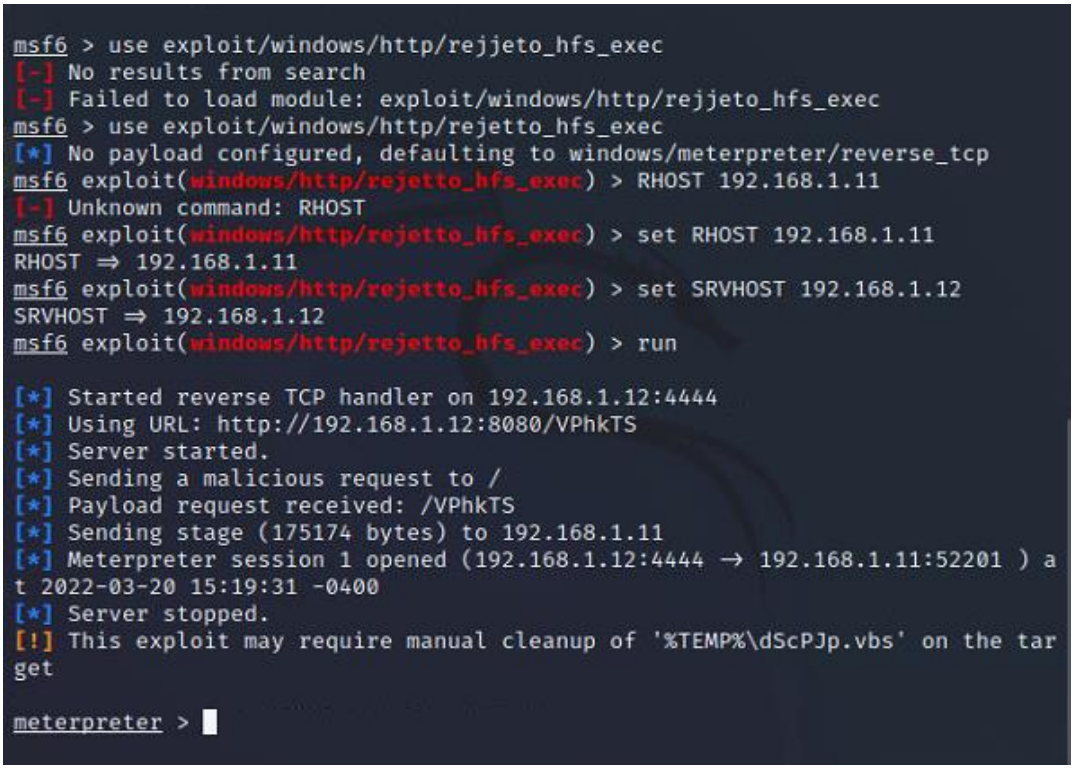
Imagen 26. BD metaexploit HTTP Rejetto.



Fuente: propia

Para su explotación pasamos a ejecutar los comandos y configuraciones de IP y del script obteniendo este resultado:

Imagen 27. Exploit ejecutado.



Fuente: propia

POSIBLE ATAQUE 2: EternalBlue.
Esta vulnerabilidad de criticidad alta comprende los siguientes CVE:

- **CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148 (CVSS 3.1: 8.1 Alta):** El servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a los atacantes remotos ejecutar código arbitrario a través de paquetes crafteados.

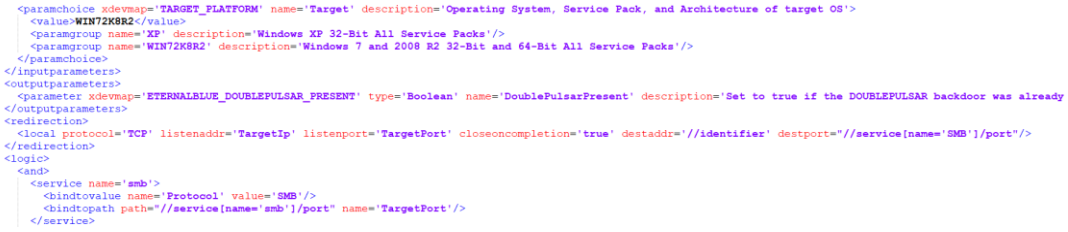
- **CVE-2017-0147(CVSS 3.1:5.9 Media):** El servidor SMBv1 de Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a los atacantes remotos obtener información sensible de la memoria del proceso a través de un paquete crafteado.

- **CVE-2017-0199(CVSS 3.1: 7.8 Alta):** Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 permiten a atacantes remotos ejecutar código arbitrario a través de un documento crafteado.

Para explicar cómo funcionaria se tomará como ejemplo a EternalBlue, un malware que hace uso de esta vulnerabilidad para instalarse. Estos son los datos asociados a esta vulnerabilidad:

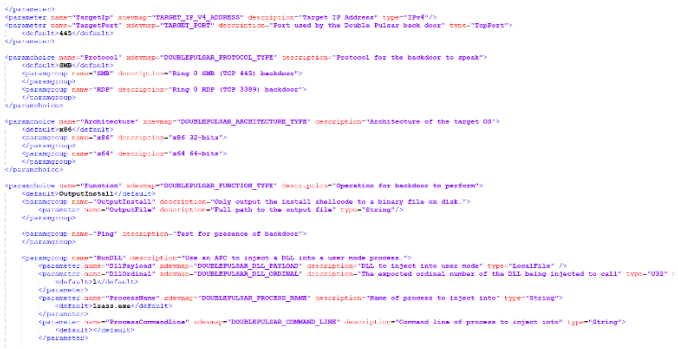
- **Brecha de infección:** Archivos personalizados.
- **Puerto:** TCP_445.
- **Protocolo:** SMBv1.
- **Método:** El malware utiliza el puerto abierto SMBv1 y se instala por medio de un código predefinido que puede venir ligado a archivos adjuntos a correo de Phishing, unidades de almacenamiento u otros hosts previamente infectados. En muchas ocasiones utilizan servidores de comando y control para realizar descarga e instalación de otros malware, por ejemplo, WannaCry quien fue el que hizo famoso este método.
- **Comandos usados:** se encuentran de manera predeterminada esta configuración:

imagen 28. Payload inicial.



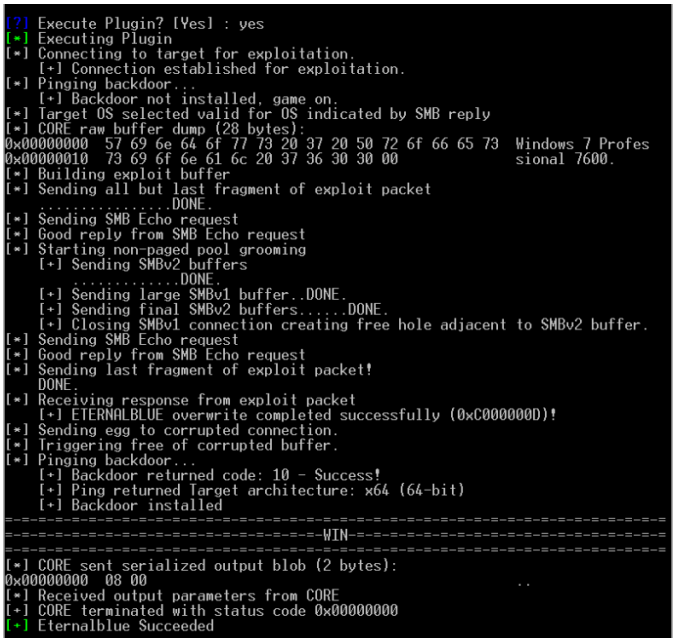
Fuente: NETSKOPE. “Stepping Stone Attack launches EternalBlue Internally”[17].

Imagen 29. Payload configurado.



Fuente: NETSKOPE. “Stepping Stone Attack launches EternalBlue Internally”.

Imagen 30. Payload ejecutado.



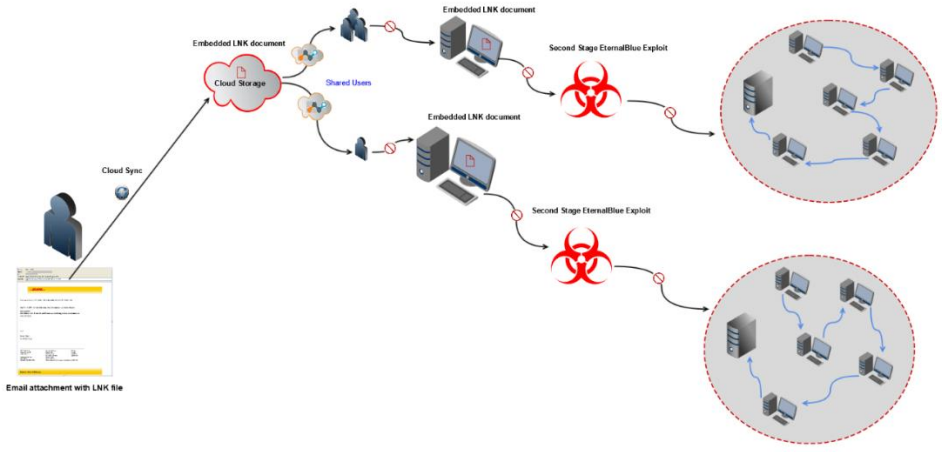
Fuente: NETSKOPE. “Stepping Stone Attack launches EternalBlue Internally”.

[17] NETSKOPE. “Stepping Stone Attack launches EternalBlue Internally”. [Sitio web] (30/03/2022). Disponible en: https://www.netskope.com/es/blog/stepping-stone-attack-launches-eternalblue-internally.

- **Método de propagación:** El malware de manera inmediata buscara el instalarse en otros dispositivos, lo que lleva a que haga una exploración de red en buscar de otros dispositivos con el puerto TCP_445 abierto como es el caso de la maquina objetivo del análisis. Esto llevara a una perdida masiva de información dependiendo de la carga usada junto a a la explotación de esta vulnerabilidad que generalmente en un Ransomware.

- **Remediación:** Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también ha publicado parches de emergencia para los sistemas operativos Windows que ya no son compatibles, como Windows XP, 2003 y 8. Para los sistemas operativos Windows no soportados, por ejemplo, Windows XP, Microsoft recomienda que los usuarios dejen de utilizar SMBv1. SMBv1 carece de las características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 se puede desactivar siguiendo las instrucciones del proveedor que figuran en Microsoft KB2696547. Además, el US-CERT recomienda que los usuarios bloqueen SMB directamente mediante el bloqueo del puerto TCP 445 en todos los dispositivos de frontera de la red. Para SMB a través de la API NetBIOS, bloquee los puertos TCP 137 / 139 y los puertos UDP 137 / 138 en todos los dispositivos de límite de red.

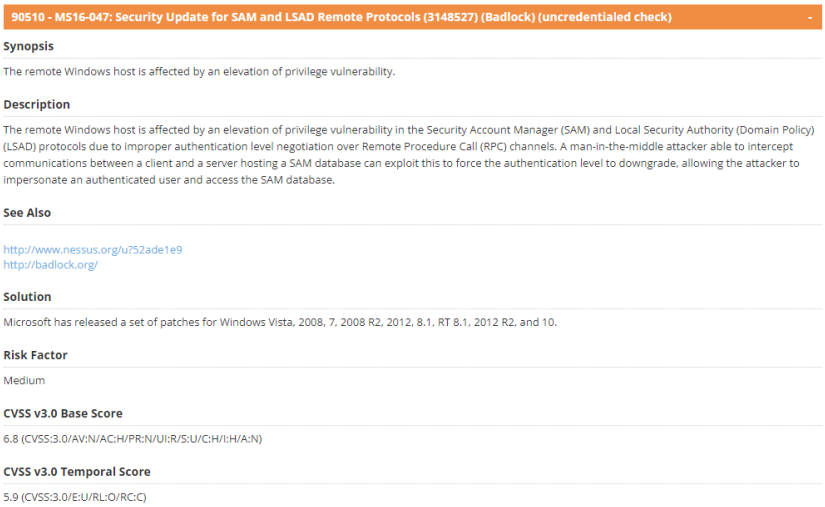
imagen 31. Método de infección.



Fuente: NETSKOPE. “Stepping Stone Attack launches EternalBlue Internally”.

- **Consideraciones adicionales:** En el caso de la maquina hay 2 vulnerabilidades medias que colaboran en facilitar la explotación de esta vulnerabilidad, donde se presenta que no hay necesidad de usuario para autenticarse en SMBv1 y es posible saltarse la autenticación del mismo. Estas son resumidas como:

Imagen 32. Vulnerabilidad de elevación de privilegios.



90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) -

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

See Also

http://www.nessus.org/u?52ade1e9
http://badlock.org/

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Risk Factor

Medium

CVSS v3.0 Base Score

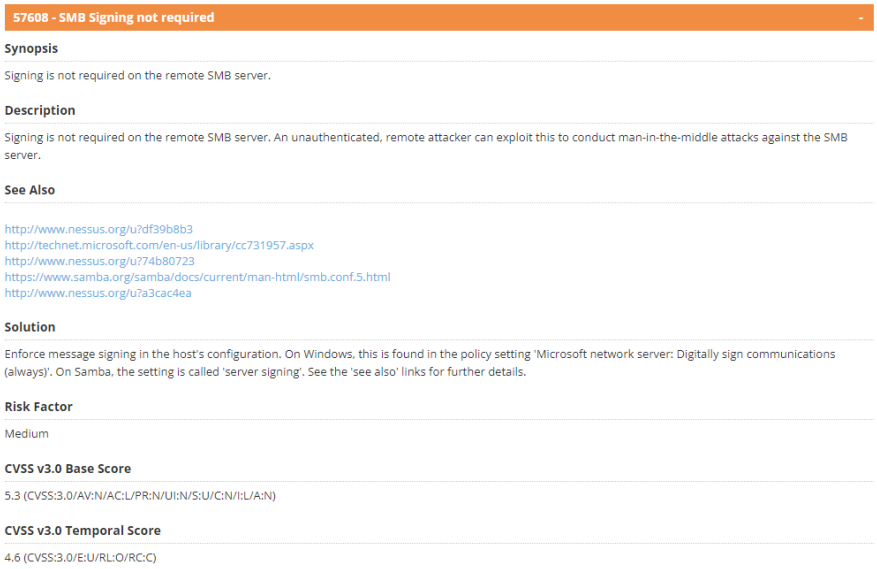
6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

Fuente: Propia.

Imagen 33. Vulnerabilidad de usuario abierto.



57608 - SMB Signing not required -

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

http://www.nessus.org/u?df39b8b3
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

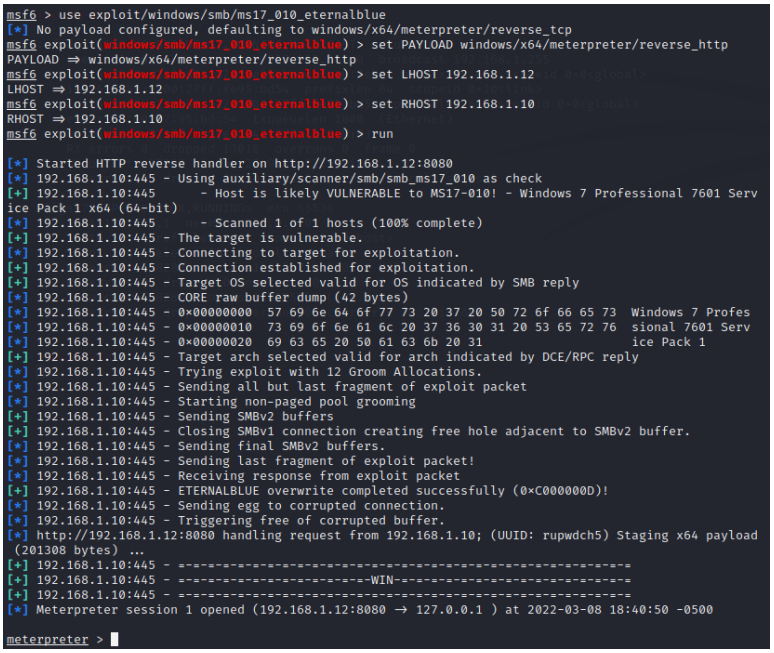
CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

Fuente: Propia.

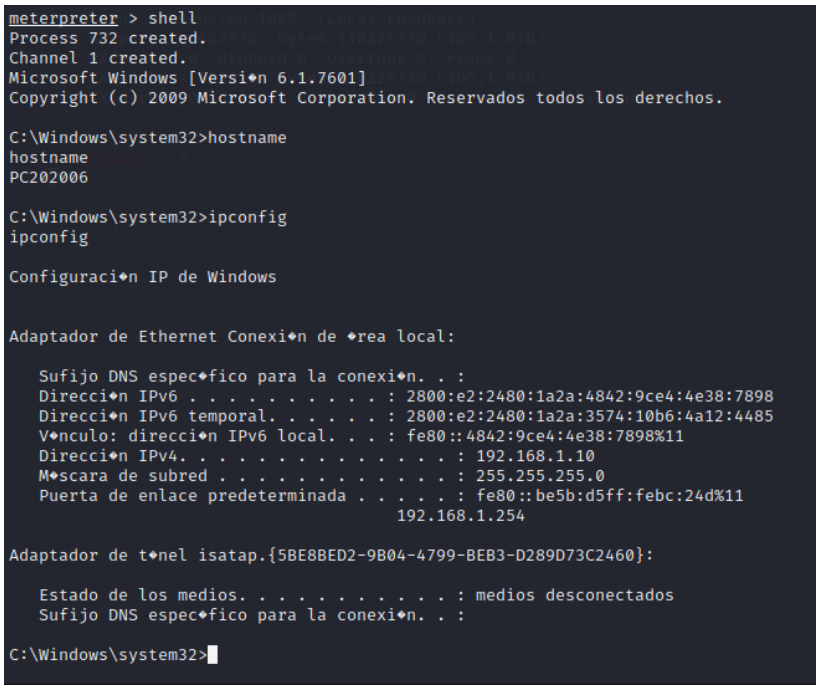
- **Explotación de la vulnerabilidad:** Se ejecuta el payload http inverse->meterpeter correspondiente a la vulnerabilidad por medio de metaexploit, aprovechando la vulnerabilidad encontrada:

Imagen 34. Explotación de la vulnerabilidad.



Fuente: Propia.

Imagen 35. Información maquina explotada. **Fuente**: Propia.

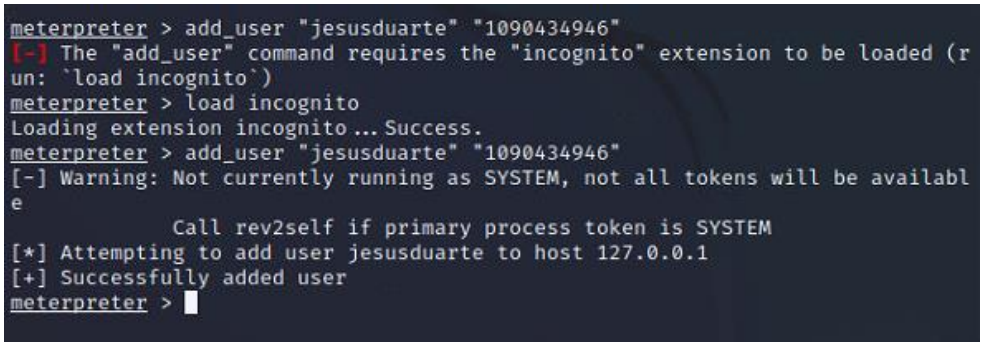


Fuente: Propia.

APLICACIÓN DE PERMISOS ADMINISTRATIVOS: Meterpreter

En el ejercicio se hace referencia a que el atacante crea un usuario administrativo, aquí se muestra el proceso de creación de este usuario:

Imagen 36. Creación de usuario.



Fuente: Propia.

Para tener acceso completo a la maquina pasaremos a asignar a este usuario un grupo con permisos administrativos. Como primer paso es necesario identificar los grupos de seguridad y perfiles que se pueden obtener en la máquina, pasaremos a identificar directamente cual podría ser administrador:

Imagen 37. Lista de grupos de seguridad. **Fuente**: Propia.

Fuente: Propia.

Como paso final se pasa a agregar el usuario administrativo al grupo de seguridad de administradores, completando de esta manera el atraque y dejando la máquina a completa disposición del atacante.

Imagen 38. Grupo añadido.

```
meterpreter > add_localgroup_user "Administradores" "jesusduarte"
[-] Warning: Not currently running as SYSTEM, not all tokens will be availabl
e
             Call rev2self if primary process token is SYSTEM
[*] Attempting to add user jesusduarte to localgroup Administradores on host
127.0.0.1
[+] Successfully added user to local group
meterpreter >
```

Fuente: Propia.

Imagen 39. Resumen usuarios.

Fuente: Propia.

Como último punto se referencia la posible remediación para esta vulnerabilidad:

- Es necesario el actualizar el software Rejetto a la versión más reciento o por mínimo la versión 2.3G.
- Evitar el uso de HTTP como protocolo en cualquier servicio negando los servicios por el puerto 80 y el uso del protocolo en si.
- Evitar el uso de puertos por defectos y la identificación de servicios por red.

CONCLUSIONES

La implementación de equipos de Redteam y Blueteam que se presenta en los casos de expuestos es completamente vacía y no tiene bases legales o técnicas para su implementación, lo recomendado en este proceso es una buena asesoría legal y conocimiento de los alcances en el proceso. Como parte de este proceso es necesario la creación de toda documentación legal que se relacione al proceso que limite, dicte roles y sea completamente subsecuente a las normas legales del país.

De manera adicional se deberá realizar un estudio sobre el funcionamiento que tendrían los equipos a implementar, lo que lleva a escoger herramientas y metodologías que se adapten con el ambiente a simular, integrar y auditar, dado que hay gran variedad de la mismas y se debe tener claro y direccionado que se va a hacer.

Los casos expuestos en la maquina vulnerada muestra una falta de control total sobre las implementaciones del entorno corporativo donde se encuentra, por ello es necesario una implementación inmediata desde línea base, pasando a controles de seguridad y de terminando en procesos de actualización y descubrimiento que hagan de la infraestructura interna segura.

Los equipos de Redteam y Blueteam son necesarios en ciertos tipos de organizaciones, pero, no es un gasto que deberían hacer empresas pequeñas, por ello es necesario buscar cual es el nivel necesario de seguridad requerido en cada caso para la prestación de servicio objetivo; aun así, se recomienda implementarlo o contratarlo con un tercero en caso de ser necesario.

RECOMENDACIONES

Es necesario tener claro que no solo las herramientas nombradas en el desarrollo del documento son las que se pueden usar para estos procesos, aunque son las mas comunes. Es necesario buscar y adaptar herramientas para cada uno de los casos, en preferencia evitando problemas de licenciamiento.

Como parte adicional del proceso de contratación se recomienda realizar estudio de los aspirantes a modo de antecedentes, esto con el fin de tener un poco mas de seguridad en cuanto a que tipo de persona esta entrando en un tema tan sensible como es la ciberseguridad.

Es necesario reconocer múltiples controles de ciberseguridad que lleven a saber posibles implementaciones a realizar al dar soluciones, por ello se recomienda que el personal de estos equipos tenga no solo experiencia en programación y herramientas de explotación, si no, en controles perimetrales y telecomunicaciones.

BIBLIOGRAFIA

BONET SANTIAGO, Observatorio plástico, 2019. Problemas detectados en la difusión del Software Libre en las empresas. [Sitio web] (30/03/2022). Disponible en: https://www.observatorioplastico.com/ficheros/articulos/103085459S-4042.pdf.

CARLES JOAN, GEEKLAND, 2019. Desafíos y problemas del software libre en la actualidad. [Sitio web] (30/03/2022). Disponible en: https://geekland.eu/problemas-del-software-libre/.

CISET, Hardening. CISET, 2020. [Sitio web] (30/03/2022). Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening.

Computerhoy, Qué es Kali Linux y qué puedes hacer con él. [Sitio web] (30/03/2022). Disponible en: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671

ESIC, ed team: qué es, estrategias y ejemplo de un caso real. ESIC, 2018. [Sitio web] (30/03/2022). Disponible en: https://www.esic.edu/rethink/tecnologia/red-team-experiencia-en-ataque

ESTRUGA NURIA, La importancia de la seguridad informática en el entorno empresarial. EALDE, 2020. [Sitio web] (30/03/2022). Disponible en: https://www.ealde.es/importancia-seguridad-informatica-empresas/

FBI. The Morris Worm. FBI, 2018. [Sitio web] (30/03/2022). Disponible en: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

GNU. ¿Qué es el software libre? 2021 Free Software Foundation, Inc. [Sitio web] (30/03/2022). Disponible en: https://www.gnu.org/philosophy/free-sw.es.html

IMPERVA, Penetration Testing. IMPERVA, 2017. [Sitio web] (30/03/2022). Disponible en: https://www.imperva.com/learn/applicationsecurity/penetration-testing/

INCIBE, ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE, 2019. [Sitio web] (30/03/2022). Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

INCIBE, Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? INCIBE, 2019. [Sitio web] (30/03/2022). Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INCIBE, Vocabulario General CVE. INCIBE, 2015. [Sitio web] (30/03/2022). Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=2142.html

INFOCYTE, 2021. [Sitio web] (30/03/2022). Disponible en: https://www.infocyte.com/es/blog/2019/06/18/7-risks-posed-by-open-source-software-and-how-to-defend-yourself/

IN-NOVA. Hacking Ético y Técnicas de Hacking Avanzadas sobre Windows. IN-NOVA, 2020. [Sitio web] (30/03/2022). Disponible en: https://www.in-nova.org/es/soluciones-y-servicios/formacion-y-entrenamiento/formacion-activa/hacking-etico-tecnicas-hacking-windows

ISECOM. OSSTMM 3 – The Open Source Security Testing Methodology Manual. ISECOM 2021. [Sitio web] (30/03/2022). Disponible en: https://www.isecom.org/OSSTMM.3.pdf

IT DIGITAL SECURITY, ¿Qué es un Blue Team y cómo trabaja? IT DIGITAL SECURITY, 2018. [Sitio web] (30/03/2022). Disponible en: https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja

KEEPCODING, ¿Qué es Red Team en Ciberseguridad? KEEPCODING, 2018. [Sitio web] (30/03/2022). Disponible en: https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

MISAZA719, Metodologías y Herramientas de Ethical Hacking. MISAZA719, 2013. [Sitio web] (30/03/2022). Disponible en: https://seguridadinformaticahoy.blogspot.com/2013/02/metodologias-y-herramientas-de-ethical.html

OAS. Breve historia de la informatica. OAS, 2017. [Sitio web] (30/03/2022). Disponible en: https://www.oas.org/cotep/GetAttach.aspx?lang=En&cId=449&aid=678

OISSG. Information Systems Security Assessment Framework (ISSAF). OISSG, 2006. [Sitio web] (30/03/2022). Disponible en: https://untrustednetwork.net/files/issaf0.2.1.pdf

OWASP, OWASP Web Security Testing Guide. OWASP, 2021. [Sitio web] (30/03/2022). Disponible en: https://owasp.org/www-project-web-security-testing-guide/

RECOVERY LABS, Virus Mydoom. RECOVERY LABS, 2020. [Sitio web] (30/03/2022). Disponible en: https://www.recoverylabs.com/ayuda-y-soporte/data-recovery-white-papers/informes-de-investigacion/virus-mydoom/

SCIELO, Delitos informáticos y entorno jurídico vigente en Colombia. SCIELO, 2018. [Sitio web] (30/03/2022). Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

SG, La Ética en el Hacking. SG, 2017. [Sitio web] (30/03/2022). Disponible en: https://sg.com.mx/revista/48/la-etica-el-hacking.

SOFTWARE LAB, ¿Qué es una vulnerabilidad informatica? SOFWARE LAB, 2018. [Sitio web] (30/03/2022). Disponible en: https://softwarelab.org/es/que-es-una-vulnerabilidad-informatica/

TARLOGIC. Blue Team Servicio de evaluación y respuesta proactiva frente a amenazas. TARLOGIC,2020. [Sitio web] (30/03/2022). Disponible en: https://www.tarlogic.com/blackarrow-servicios-seguridad-ofensiva/blue-team/.

TECHTARGET. Prueba de penetración. TECHTARGET, 2018. [Sitio web] (30/03/2022). Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Prueba-de-penetracion-pen-test

TICNEGOCIOS. Qué es el hacking ético. TICNEGOCIOS, 2020. [Sitio web] (30/03/2022). Disponible en: https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-el-hacking-etico/

USS Seguridad integral. Sistema de detección de intrusos: tipos y ejemplos. USS, 2019. [Sitio web] (30/03/2022). Disponible en: https://uss.com.ar/preguntas-frecuentes/sistema-de-deteccion-de-intrusos/.

ENLACE VIDEO SUSTENTACIÓN

https://youtu.be/NIKpUd5RmWo