CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

CARLOS ANDRÉS JIMÉNEZ FORERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
FACULTAD DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2022

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

CARLOS ANDRÉS JIMÉNEZ FORERO

Documento técnico presentado como requisito para optar al título de Especialista en Seguridad Informática

Director:
Luis Fernando Zambrano

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
FACULTAD DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2022

CONTENIDO

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

BLUETEAM: es un equipo conformado por expertos o especialistas en ciberseguridad que se encarga de analizar el comportamiento de la infraestructura TI de las organizaciones, con el objetivo de identificar vulnerabilidades y luego establecer acciones de mitigación, que impidan la materialización de la amenaza.

CIBERSEGURIDAD: Son todo tipo de acciones o prácticas realizadas con el objetivo de proteger la información digital que es transferida o almacenada en dispositivos electrónicos

COMPUTADOR: Es una maquina electrónica que permite procesar información, y genera resultados a partir de la toma de decisiones, en tiempos mucho más rápidos de lo que podría hacerlo un ser humano.[1]

DELITO: Es una mala conducta o acción realizada por parte de una persona, que va en contra de un orden jurídico en la sociedad, y que se castiga con su correspondiente pena.[2]

HARDENING: Es un conjunto de actividades o procesos, cuya finalidad consiste en fortalecer las medidas de seguridad informática a nivel organizacional, para reducir los riesgos y mitigar posibles amenazas que puedan afectar los activos de información institucionales.

INFORMACIÓN: Son conjuntos de datos organizados, que permiten exponer mensajes basándose en fenómenos, ayudando a la resolución de problemas, todo a partir del conocimiento.[3]

[1] JIMÉNEZ FORERO, Carlos Andrés. Aplicación de software libre para análisis forense mediante data carving, 2020. p.8
[2] Ibid., p.8
[3] Ibid., p.8

INFORMÁTICA: Es una ciencia que a través de un sin número de conocimientos técnicos, permite el análisis de información a través de computadores.

LABORATORIO: Es un lugar físico o virtual, el cual se encuentra dotado con los elementos necesarios para realizar experimentos o investigaciones científicas. También sirve como aula virtual o física para realizar prácticas de un tema en específico.

REDTEAM: es un equipo de expertos encargado de simular ataques a la infraestructura TI de una organización, con el objetivo de encontrar vulnerabilidades críticas.

RESUMEN

Este documento presenta un informe técnico en donde se describe el desarrollo de las actividades realizadas para el seminario de Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

Inicialmente se contextualiza acerca de la legislación vigente que aplica en Colombia, en cuanto a la protección de datos personales y delitos informáticos. Posteriormente comienza el abordaje de los conceptos técnicos aplicados en los equipos azules y rojos, describiendo las diferencias entre ellos, y luego se explica el significado de una prueba de intrusión y sus fases. Así mismo, se documenta una serie de herramientas que son utilizadas en el mundo de la ciberseguridad, tanto para hacer auditorías como para protegerse de ataques cibernéticos.

También se presenta un laboratorio a través de un entorno simulado, en donde a dos máquinas que simulan una situación real, se le realizan actividades que ejecutarían los equipos azules y rojos. Por ejemplo, se ejecuta un ataque de intrusión a una de las máquinas, donde se logra establecer conexión remota al equipo, que correspondería a una actividad red team. Y finalmente, se establecen medidas de contención para que no se vuelva a materializar lo sucedido, tarea que corresponde a los equipos azules.

Palabras clave: ataque cibernético, blu team, ciberseguridad, red team.

INTRODUCCIÓN

Red Team y Blue Team son dos términos que con el pasar de los años, han ido ganando popularidad e importancia debido a la creciente tendencia hacia la conectividad y los avances tecnológicos, lo que, a su vez, ha generado también, un crecimiento y una evolución rápida de las amenazas y ataques cibernéticos. Cuando se habla de protección de datos y de seguridad informática, es donde entran en juego estos dos equipos. Entre los dos, se realiza un trabajo complementario, con el objetivo de detectar vulnerabilidades, de tal manera que se puedan mitigar a tiempo, evitando la materialización de amenazas que afecten de manera negativa los activos e información crítica de las organizaciones.

Con la intención de presentar a la comunidad en general la importancia de los equipos azules y rojos dentro una organización, en este documento se realiza un recorrido de las actividades que estos realizan, iniciando por una contextualización de las implicaciones éticas y legales por las que están regidos, explicación de los factores que diferencian el uno del otro, y posteriormente a través de prácticas de laboratorio en un entorno simulado, se describen actividades específicas que realizarían estos dos equipos en un entorno real, en dónde su función es detectar vulnerabilidades a través de ataques de intrusión (Equipo Rojo) y establecer acciones de mitigación para que no se materialice la amenaza (Equipo Azul).

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Construir un informe técnico que presente un análisis de los aspectos éticos y legales de la ciberseguridad, y que describa las actividades desarrolladas por los Blueteam y Redteam, para la identificación y mitigación de riesgos cibernéticos dentro de una organización.

1.2 OBJETIVOS ESPECÍFICOS

OE1: Evaluar las acciones de los equipos Red Team & Blue Team de una organización a través del análisis e identificación de dichas actividades dentro del marco ético y legal de la normatividad colombiana.

OE2: Demostrar vulnerabilidades en un sistema informático simulado, partiendo del uso de metodologías y técnicas de intrusión, describiendo el paso a paso de lo realizado, que permita a la comunidad en general o a las organizaciones, el conocimiento acerca de las herramientas y procedimientos para la identificación riesgos.

OE3: Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades, que permitan que se minimice el riesgo de materialización de amenazas dentro de una organización.

2 MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES

En Colombia se encuentra vigente la ley 1273 de 2009, “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.”[4]

Dicha ley, tipifica los delitos y decreta las penas que deben pagar los delincuentes ante las diferentes acciones delictivas informáticas que allí se describen. Los delitos tipificados por dicha ley son:

- Acceso abusivo a un sistema informático
- Obstaculización ilegítima de sistema informático o red de telecomunicación
- Interceptación de datos informáticos
- Daño informático
- Uso de software malicioso
- Violación de datos personales
- Suplantación de sitios web para capturar datos personales
- Hurto por medios informáticos y semejantes
- Transferencia no consentida de activos

En la Ley 1273 de 2009, cada tipo de delito está regido por un artículo que describe la forma en la que se produce la acción delictiva para definirse como delito, y al mismo tiempo, describe como se sancionará al delincuente.

Por ejemplo, una persona que acceda abusivamente a un sistema informático, según el artículo 269A, deberá pagar una sanción de entre cuarenta y ocho

[4] ALCALDÍA MAYOR DE BOGOTÁ. [Sitio Web]. Ley 1273 de 2009. [Consultado: 30 de agosto 2022]. Disponible en internet: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

(48) y noventa y seis (96) meses de prisión, y una multa de 100 a 1000 SMLMV.

Así mismo, un delincuente que dañe un sistema informático, borrándolo, destruyéndolo o alterándolo, según el artículo 269D, también deberá pagar una sanción de entre cuarenta y ocho (48) y noventa y seis (96) meses de prisión, y una multa de 100 a 1000 SMLMV.

Y de la misma manera, para cada uno de los delitos mencionados anteriormente, la Ley 1273 de 2009 describe las sanciones penales y económicas a las que deberán someterse los delincuentes que cometan estas acciones.

3 PENTESTING Y SUS ETAPAS

Las pruebas de intrusión son aquellas que simulan ataques a una infraestructura con el objetivo de identificar vulnerabilidades que permitan el ingreso de intrusos o de ataques informáticos. El desarrollo de estas pruebas permite realizar estrategias que aseguran un funcionamiento continuo de la infraestructura y son útiles para saber cuál es la capacidad de identificación y respuesta antes estos ataques. Estas pruebas también permiten complementar las auditorias perimetrales en donde se identifica y analiza el grado de seguridad ante agentes externos.

Las pruebas de intrusión se deben realizar al menos una vez al año y siempre que se realice algún cambio en la infraestructura tecnológica, según las buenas prácticas de seguridad. Lo anterior con la finalidad de estar seguros de que los controles activos siguen siendo eficaces. [5]

3.1 ETAPAS DEL PENTESTING

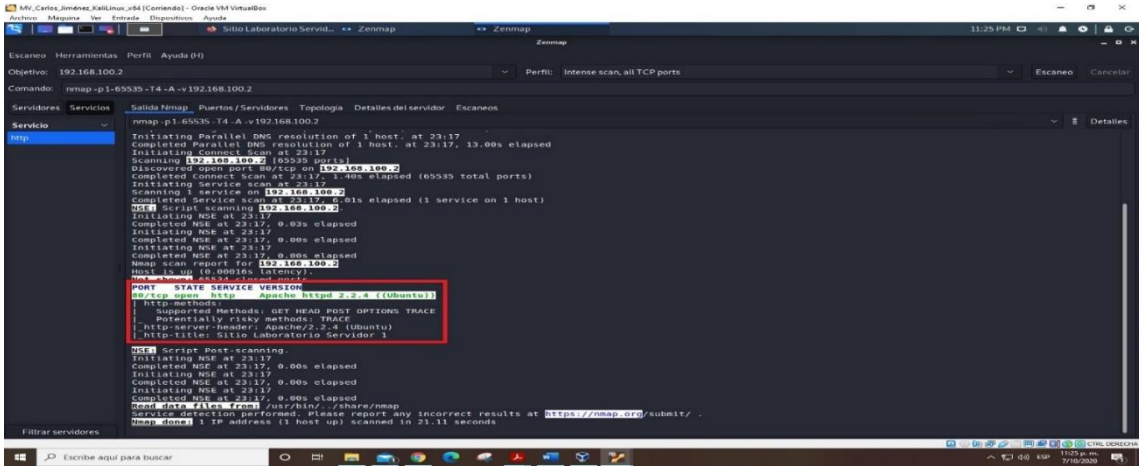
Existen muchas fuentes bibliográficas que describen de diversas maneras las etapas que se pueden llevar a cabo en una prueba de intrusión, sin embargo, la mayoría de ellas apuntan a que el pentestig consta como mínimo de la siguientes cinco (5) grandes etapas:

3.1.1 Recopilación de información. En esta fase lo que se buscar es recopilar la mayor cantidad de información posible. Por ejemplo, escanear dominios, escaneos de puertos, escanear direcciones IP, identificar sistemas operativos que usan los hosts, identificar servicios activos, entre otros.

[5] MONTERO, Victor. Técnicas del Penetration Testing. [En línea]. Septiembre, 2005. [Consultado: 30 de agosto 2022]. Disponible en internet: http://www.cybsec.com/upload/VictorMontero-SeminarioTecnicasdelPenetrationTestingArgentina.pdf

Una herramienta que se puede utilizar en esta etapa es NMAP, la cual permite realizar escaneos de red y puertos. La siguiente figura, muestra como con NMAP e interfaz gráfica ZENMAP, se puede realizar un escaneo para identificar qué puertos y servicios se encuentra utilizando un determinado host. En ella se puede apreciar, que la herramienta identifica que el servidor analizado tiene el puerto 80 en TCP abierto (de 65535 analizados), y que a su vez está utilizando dicho puerto para el servicio de HTTP, bajo apache versión 2.2 y en sistema operativo Ubuntu. Así mismo, se puede evidenciar que se identifica el nombre del sitio WEB alojado en el servicio.

Figura 1. Escaneo de puertos con NMAP



Fuente: Autor del documento

Con esta información recopilada, ya es posible saber, por ejemplo, a que host, por cual puerto, y que se servicio se puede atacar.

3.1.2 Identificación de vulnerabilidades. En esta etapa se identifican las vulnerabilidades a las que está sometido el objetivo de la prueba de intrusión. Se pueden identificar vulnerabilidades tanto lógicas como físicas.

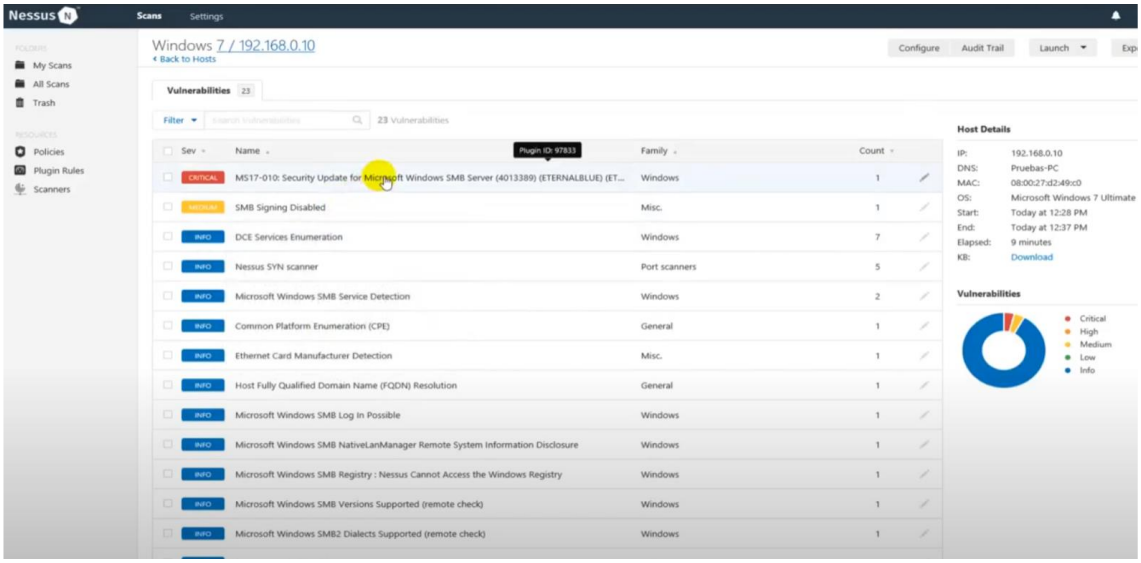
Algunas vulnerabilidades que se pueden encontrar en el objetivo son:

- Ausencia o mal funcionamiento del firewall que gestiona el tráfico de red.
- Sistemas operativos desactualizados.

- Configuración de red defectuosa u obsoleta.
- Ausencia de métodos de autenticación a las diferentes aplicaciones, o de controles de acceso a espacios físicos donde se encuentran los dispositivos de red.
- Fallos criptográficos.

Con la herramienta NESSUS, es posible realizar análisis de vulnerabilidades a un determinado dispositivo. Por ejemplo, como lo muestra la siguiente figura, la herramienta muestra un reporte de vulnerabilidades que encontró después de realizar un análisis a una máquina con Windows 7. Se puede apreciar que existe una vulnerabilidad que el software califica como “crítica” (color rojo) asociada a una actualización de seguridad del servidor SMB de Windows.

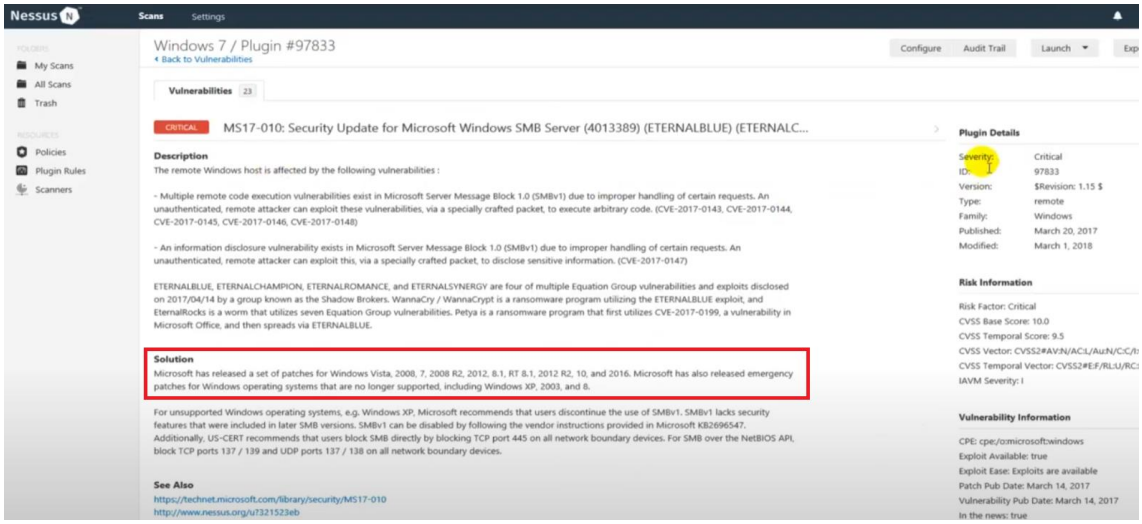
Figura 2. Análisis de vulnerabilidades con NESSUS



Fuente: Autor del documento

Así mismo, como lo muestra la siguiente figura, permite identificar información más específica de la vulnerabilidad encontrada. Por ejemplo, indica como mitigar esta debilidad del sistema.

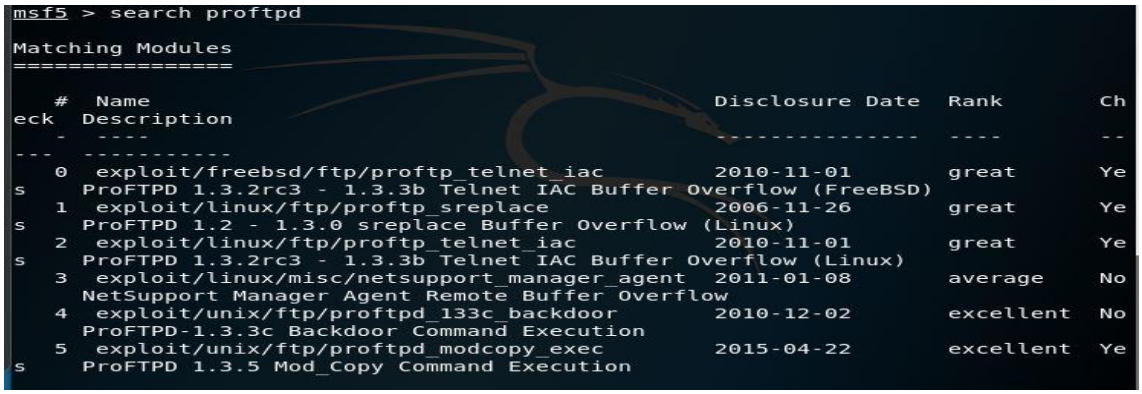
Figura 3. Información específica de vulnerabilidad con NESUS



Fuente: Autor del documento

Con la herramienta Metasploit Framework también es posible identificar vulnerabilidades y los exploits aplicables. La siguiente figura muestra una búsqueda de vulnerabilidades para el puerto FTP de una máquina, a través de comando “search proftpd”, encontrando 5, con sus exploits para ser atacadas.

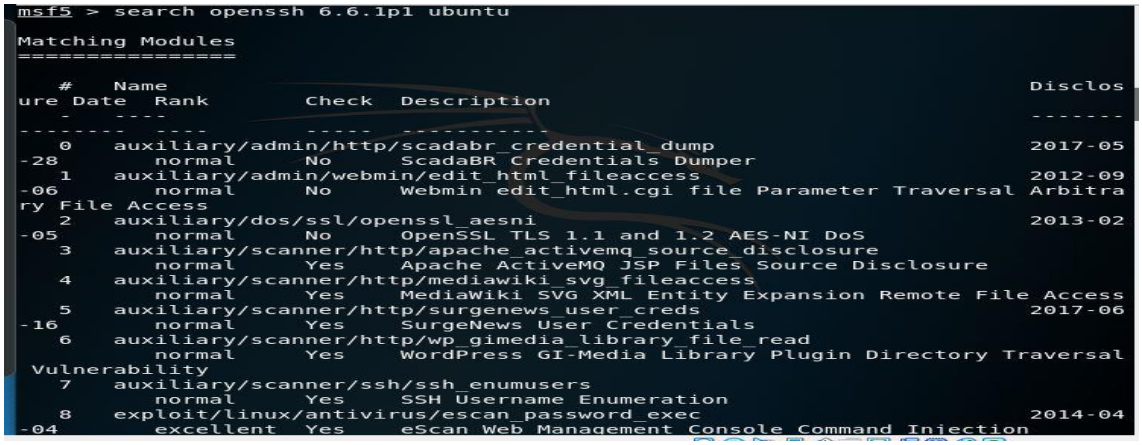
Figura 4. Vulnerabilidades del puerto FTP con Metasploit Framework



Fuente: Autor del documento

También se puede realizar búsqueda de vulnerabilidades para el puerto SSH de una máquina, a través del comando “search openssh”. La siguiente figura describe más de 8 vulnerabilidades, con sus exploits para ser atacadas.

Figura 5. Vulnerabilidades del puerto SSH con Metasploit Framework



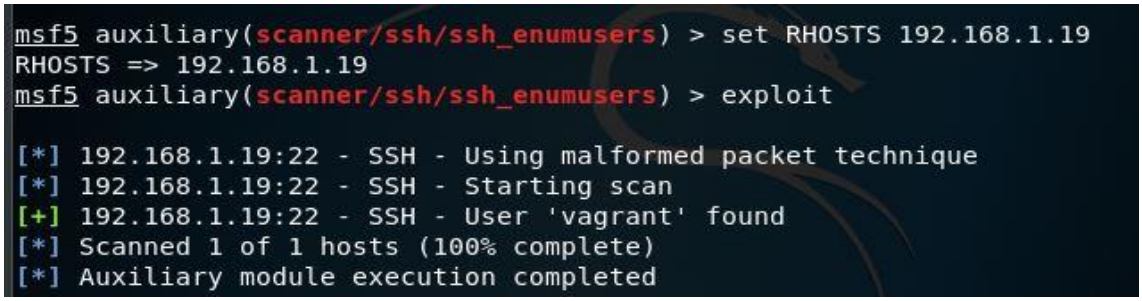
Fuente: Autor del documento

3.1.3 Explotación de vulnerabilidades. En esta fase se explotan las vulnerabilidades encontradas en la fase anterior, a través de exploits o sí se identificaron credenciales, acceder directamente a los sistemas objetivo.

Para explotar vulnerabilidades también se puede usar la herramienta Metasploit Framework. Para este ejemplo, se explotará la vulnerabilidad número 7 encontrada en la imagen anterior, la cual se refiere a una debilidad que permite ver los usuarios configurados por SSH.

Luego de ejecutar una serie de comandos, el resultado es lo que muestra la siguiente figura. Un ataque realizado con éxito, que dio como resultado encontrar que el usuario “vagrant” también está disponible para utilizar el servicio SSH.

Figura 6. Ataque a servicio SSH con Metasploit Framework



Fuente: Autor del documento

3.1.4 Post explotación. Esta etapa no siempre se aplica, sin embargo, consiste en que una vez se logre ingresar al sistema, intentar captar credenciales o permisos de administrador, para obtener control total del sistema, o incluso tratar de vulnerar otros sistemas relacionados y que tengan una mayor importancia.

3.1.5 Informe. Esta es la última etapa, y quizás la más importante de una prueba de intrusión. Aquí es donde se presenta al cliente el resultado de la auditoría. Se debe describir de tal forma que el cliente entienda y comprenda los riesgos reales a los que está expuesta la organización con las vulnerabilidades encontradas, indicándole en donde existen fortalezas de seguridad y también donde se deben adoptar medidas de corrección y mitigación.

Como este informe se presenta y puede ser leído por personal sin conocimientos técnicos, es recomendable hacer dos tipos de informes, un informe ejecutivo donde se realiza una explicación general, y un informe técnico que se enfoca a mostrar detalles más técnicos de la auditoria.

4 HERRAMIENTAS DE CIBERSEGURIDAD

4.1 METASPLOIT FRAMEWORK

Metasploit Framework es una herramienta que se enfoca en realizar pruebas de intrusión, las cuales son realizadas por auditores de seguridad o equipos Blue y Red Team. Este último se encarga de realizar las pruebas de intrusión, mientras que el Blue Team se encarga de las medidas de seguridad, y en sí de toda la defensiva.

Es una herramienta gratuita y multiplataforma, esto quiere decir que se puede usar tanto en Windows como en Linux. [6]

Esta herramienta contiene exploits, que son en otras palabras, vulnerabilidades conocidas, que, a su vez, incorporan payloads que son los encargados de explotar esas debilidades, como se pudo observar en el capítulo anterior de este documento.

4.2 NMAP

NMAP es una de las herramientas más conocidas para realizar escaneo de puertos de red. A través de comandos, permite obtener una gran cantidad de información de los equipos que estén dentro de la red objetivo. Puede escanear hosts activos, identificar qué puertos tiene abiertos, qué sistema operativo usa, qué servicios tiene activos, entre otros.

Es una herramienta gratuita, de código abierto, multiplataforma, de tal manera que se puede usar en Windows, Linux, y macOS.

[6] RIZALDOS, Héctor. Qué es Metasploit framework. [En línea]. Octubre, 2018. [Consultado: 30 de agosto 2022]. Disponible en internet: https://openwebinars.net/blog/que-es-metasploit/

Principalmente su ejecución es a base de consola de comandos, sin embargo, NMAP permite instalar un complemento llamado ZenMAP, el cual es una utilidad que permite operar NMAP con una interfaz gráfica.

Permite realizar diferentes tipos de escaneo de puertos, tales como paquetes ICMP, datagramas UDP y segmentos TCP. Otra característica importante, es que permite realizar los escaneos de manera oculta, lo que dificulta que los firewalls descubran ese tráfico.[7]

4.3 OPENVAS

OpenVAS es otra herramienta interesante para realizar escaneo de vulnerabilidades. Es de código abierto y multiplataforma, y posee un servicio WEB el cual permitirá realizar las búsquedas de vulnerabilidades o los equipos de una red.

Cuenta con una base de datos de más de 50.000 vulnerabilidades conocidas alimentadas a diario, para ser comparadas con lo que se encuentre en el escaneo de los distintos servicios que están en funcionamiento en los equipos de cómputo.

OpenVAS clasifica las vulnerabilidades encontradas en 3 categorías, de alto riesgo (color rojo), que son aquellas que representan una falla de seguridad grave, por tal motivo deben tratarse de inmediato. De medio riesgo (color amarillo) que representan aquellas vulnerabilidades que requieren que el atacante se esfuerce un poco más para lograr su objetivo, y deben tratarse en un mediano o corto plazo. Por último, están las vulnerabilidades de bajo riesgo, que son aquellas que no requieren una intervención para corrección o mitigación inmediata.[8]

[7] DE LUZ, Sergio. Realiza escaneos de puertos con Nmap a cualquier servidor o sistema. [En línea]. Julio, 2022. [Consultado: 30 de agosto 2022]. Disponible en internet: https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

[8] VERA, Rafael. Qué es OpenVAS. [En línea]. Noviembre, 2020. [Consultado: 30 de agosto 2022]. Disponible en internet: https://openwebinars.net/blog/que-es-openvas/

4.4 EXPLOITDB

ExploitDB es una base de datos que colecciona vulnerabilidades públicas y describe como aprovecharse de ellas. Todos los días es alimentada por hackers y por expertos, por lo cual es una plataforma que puede llegar a ser muy útil al momento de ejecutar un test de intrusión, ya que, de allí, se puede consultar los exploits para ejecutarlos en las maquinas objetivo da la auditoría que se esté realizando.

4.5 GLOSARIO DE VULNERABILIDADES Y EXPOSICIONES COMUNES

CVE se trata de una lista de vulnerabilidades y exposiciones de seguridad que son públicas, por tal motivo puede ser de conocimiento o consultadas por cualquier persona.

Se creó en año 1999 por la corporación MITRE con el objetivo de identificar y clasificar vulnerabilidades en software y también en firmware. Como también con el objetivo de facilitar el intercambio de información acerca de vulnerabilidades conocidas, entre organizaciones.

La lista CVE es definida como un diccionario de vulnerabilidades y exposiciones, y no como una base de datos, por tal motivo, sirve como línea base para que las organizaciones se comuniquen y dialoguen entre sí, en torno a vulnerabilidades determinadas.[9]

[9] CIBERSEGURIDAD. [Sitio Web]. ¿Qué es cve? explicación de las vulnerabilidades y exposiciones comunes. [Consultado: 30 de agosto 2022]. Disponible en internet: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

5 HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS

5.1 FIREWALL DE RED

Es un dispositivo de seguridad que permite, bloquea o rechaza paquetes de tráfico de red, a través de reglas personalizadas, que establecen los puertos y protocolos permitidos o bloqueados dentro de la red.

5.2 FIREWALL DE APLICACIÓN

Es una herramienta que permite y bloquea paquetes de tráfico de red, o aplicaciones instaladas en un determinado host. Funciona similar a un firewall de red, pero este comúnmente se encuentra instalado dentro del sistema operativo del equipo, por lo que las aplicaciones o el tráfico que permite y bloquea, son las que pasan por el host.

5.3 ANTIVIRUS

Un antivirus es una herramienta instalada en un dispositivo, capaz de monitorear actividades en tiempo real y hacer verificaciones periódicas, o según el usuario le indique, con el objetivo de buscar o detectar virus o amenazas, para después removerlas del computador. Identifican los virus a través de “firmas” los cuales son patrones que se pueden detectar en archivos, comportamientos o alteraciones no autorizadas en el computador. Es importante que el antivirus permanezca actualizado, ya que los patrones de códigos maliciosos se descubren a diario, y la base de datos de virus puede quedar obsoleta muy rápidamente, y por lo tanto no detectará nuevas amenazas.[10]

[10] TECNOLOGIA+INFORMATICA. [Sitio Web]. Que es un Antivirus? Definición. [Consultado: 01 de octubre 2022]. Disponible en internet: https://www.tecnologia-informatica.com/que-es-un-antivirus-como-funciona/

6 DIFERENCIAS ENTRE UN BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

Un CSIRT es un grupo de expertos especializados en seguridad informática que se encargan de recibir informes de seguridad, analizarlos y responder en tiempo real a la materialización de amenazas, buscando restituir las actividades con el menor impacto negativo posible. Mientras que la función de un Blue Team, es analizar el comportamiento de los sistemas de información de las organizaciones, a través de auditorías que permitan la identificación de riesgos y vulnerabilidades, para después establecer acciones de mitigación que prevengan la materialización de amenazas.

De lo anterior se puede concluir que, la principal diferencia entre un equipo CSIRT y un Equipo Azul, es que el primero es reactivo, es decir, actúa cuando se esté materializando un incidente informático, buscando el mínimo impacto, mientras que un Blue Team, se enfoca más en las labores preventivas, es decir, establecer medidas o procesos que impidan la materialización de amenazas.

Sin embargo, con el pasar de los años, y teniendo en cuenta la naturaleza de un CSIRT, los equipos Blue Team aportan mucho a los CSIRT o trabajan en conjunto, ya que estos últimos, ahora no solo se limitan a gestionar incidentes, sino que también diseñan herramientas de seguridad y recomiendan acciones para prevención de ataques poniendo esa información a disposición de la comunidad.

7 CENTER FOR INTERNET SECURITY - CIS

Los controles CIS son un conjunto de buenas prácticas que indican qué acciones defensivas se pueden ejecutar en la prevención de un ataque informático. Esto quiere decir, que un equipo azul puede hacer uso de tales estrategias, para implementarlas en una organización y de esa manera mantener la seguridad de los activos informáticos o de información.

Son en total veinte (20) controles los propuestos por CIS. Algunos de los controles allí planteados que puede utilizar un equipo azul para establecer medidas de prevención en una organización, son los siguientes:[11]

- Control 3 Gestión continua de vulnerabilidades: Indica que continuamente se debe estar analizando los sistemas con el objetivo de identificar vulnerabilidades potenciales. Adicionalmente, este control dice que los sistemas operativos deben ejecutar las actualizaciones de seguridad más recientes.
- Control 8 Defensas contra malware: Indica que se debe contar con software que bloquee malware y optimizarlo de tal manera que se actualice rápidamente de manera automática.
- Control 9 Limitación y control de puertos de red, protocolos y servicios: Este control indica que se debe contar con un firewall debidamente configurado, que supervise la actividad de los puertos y servicios de la organización.
- Control 11 Configuración segura para dispositivos de red, tales como firewalls, routers y switches: Indica que se debe contar con firewall, routers y switches debidamente configurados de tal manera que se evite configuraciones predeterminadas y conocidas, con las cuales un delincuente puede materializar un ataque a la organización.

[11] MANAGE ENGINE. [Sitio Web]. ¿Qué son y cómo implementar los Controles de CIS (CIS Controls)?. [Consultado: 01 de octubre 2022]. Disponible en internet: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

- Control 17 Implementar un programa de concienciación y capacitación en seguridad: Indica que se debe capacitar a los empleados, quienes son el eslabón más débil de una organización, para que adquieran destrezas que ayuden en la defensa de la seguridad de la información, teniendo en cuenta su rol dentro de la organización.

8 QUE ES UN SIEM, SUS FUNCIONES Y CARACTERÍSTICAS

Un Security Information and Event Management – SIEM, es una solución de seguridad que permite centralizar y tener control total de la seguridad informática de una organización. Es decir, ayuda a las empresas a reconocer vulnerabilidades y amenazas antes de que estas se materialicen interrumpiendo la operación.

Algunas de sus características son: [12]

- Centralización en la vista de amenazas potenciales.
- Identifica las amenazas que son críticas y requieren de atención inmediata, y cuales no son tan importantes.
- Reconocimiento avanzado de amenazas en tiempo real.
- Documenta los eventos ocurridos y como se solucionaron, a través de un registro de auditoría.
- Automatización impulsada por inteligencia artificial.

Existen muchas soluciones SIEM que pueden varias en su capacidad, sin embargo, la mayoría ofrece el siguiente conjunto de funciones: [13]

- Gestión de registros: captura de eventos en las diferentes fuentes de la red de la organización.
- Correlación de eventos y análisis: utiliza análisis avanzados, que proporcionan información que permite localizar y mitigar de manera rápida amenazas a la seguridad de la organización
- Monitoreo de incidentes y alertas de seguridad: como se puede hacer una gestión centralizada de la infraestructura empresarial, SIEM monitorea los incidentes de seguridad en todos los niveles, es decir, todos los usuarios, dispositivos y aplicaciones de la red.
- Gestión de conformidad e informes

[12] HELPSYSTEMS. [Sitio Web]. ¿Qué es un SIEM?. Mayo, 2018. [Consultado: 01 de octubre 2022]. Disponible en internet: https://www.helpsystems.com/es/blog/que-es-un-siem

[13] IBM. [Sitio Web]. ¿Por qué es importante SIEM?. [Consultado: 01 de octubre 2022]. Disponible en internet: https://www.ibm.com/co-es/topics/siem

Algunas herramientas SIEM son las siguientes:[14]

- Fusion SIEM
- Graylog
- IBM QRadar
- LogRhythm
- SolarWinds
- Splunk

[14] PATHACK, Amrita. Las 11 mejores herramientas SIEM para proteger a su organización de ciberataques. [En línea]. Septiembre, 2022. [Consultado: 01 de octubre 2022]. Disponible en internet: https://geekflare.com/es/best-siem-solutions/

9 ANÁLISIS ACUERDO DE CONFIDENCIALIDAD HACKERS SECURITY

9.1 ¿USTED LOGRA EVIDENCIAR ALGÚN PROCESO ILEGAL Y NO ÉTICO QUE SE ESTÉ ESTIPULANDO EN DICHO ACUERDO? SI LA RESPUESTA ES AFIRMATIVA Y USTED ENCONTRÓ ALGÚN PROCESO ILEGAL EN EL ACUERDO DEBERÁ MENCIONAR QUE ARTÍCULOS DE LA LEY 1273 SE PODRÍAN VULNERAR EN DICHO ACUERDO Y ESPECIFICAR PORQUÉ VULNERA ARTÍCULOS DE LA LEY 1273

Efectivamente, se evidencian varias irregularidades en las cláusulas descritas en el acuerdo, las cuales se describen a continuación:

"**Cláusula primera. Objeto**: 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 o sobre procesos ilegales dentro de Hackers Security no podrán ser divulgados**."

Esta cláusula obliga al profesional de ingeniería a guardarse u ocultar información sobres procesos ilegales que ha estado cometiendo Hackers Security. Lo anterior obliga a que el profesional no cumpla con lo que describe el código de ética para el ejercicio de la ingeniería, en el numeral F, Articulo 31, Capitulo II, Título IV de la Ley 842 de 2003, que indica que el profesional debe "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".[15] No cumplir lo anterior constituye una falta disciplinaria y acarrea sanciones como, por ejemplo, que le

[15] COPNIA. [Sitio Web]. Ley 842 de 2003. Septiembre, 2003. [Consultado: 12 de septiembre 2022]. Disponible en internet: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

sea cancelada la matricula profesional y por tal motivo no poder ejercer más su profesión como ingeniero.

"**Clausula segunda. Definición de información confidencial:** se entiende como Información Confidencial, para los efectos del presente acuerdo: Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como **datos de chuzadas**, **interceptación de información, accesos abusivos a sistemas informáticos**"

Esta segunda clausula en su numeral 2, indica que Hackers Security dentro de su información confidencial, tiene datos que ha tomado de chuzadas, de interceptación de información y de accesos abusivos a sistemas informáticos. Lo anterior claramente indica que esta organización ha estado cometiendo los delitos de "Acceso abusivo a un sistema informático" e "Interceptación de datos informáticos", los cuales se encuentran descritos en los artículos 269A y 269C de la ley 1273 de 2009 respectivamente, y los cuales indican que quien los cometa, para el caso del artículo 269A deben pagar una pena de prisión de hasta 96 meses y una multa económica de hasta 1000 SMLMV, y para el articulo 269C una pena de prisión de hasta de 72 meses.[16]

"**Clausula cuarta. Obligaciones de la parte receptora**: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a: 3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros. 4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas."

[16] GOBIERNO DE COLOMBIA. Ley 1273 de 2009. [En línea]. [Consultado: 12 de septiembre 2022]. Disponible en internet: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

En las obligaciones que se describen los numerales 3 y 4 del acuerdo, nuevamente se indica, y esta vez de manera un poco más detallada, que quien firme este acuerdo, no podrá publicar ni denunciar procedimientos, actividades, o información ilegal a la cual tenga acceso o conozca. Esto, como se indicó anteriormente, es una violación al código de ética profesional, descrito en la ley 842 de 2003. Así mismo, el artículo 67 de Ley 906 de 2004, establece como deber genérico, denunciar irregularidades, y su desconocimiento u omisión puede llegar a tener consecuencias de carácter jurídico.

También, en la obligación del numeral 4, se indica, que la organización ha estado cometiendo el delito de "Violación de datos personales", tipificado en el artículo 269F, al indicar que la organización ha hecho chuzadas para capturar información de terceros

"**Cláusula octava. Solución de controversias**: 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 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 Hackers Security."

Por último, esta cláusula octava, es quizás, las más grave, puesto que como se dice coloquialmente, es "echarse la soga al cuello", ya que la organización está indicando que, si el contratista es descubierto por las autoridades con información ilegal, este debe exonerar a la empresa del cualquier culpabilidad o responsabilidad legal, a sabiendas que son actos ilícitos que ya venía realizando la organización previamente, o que son actos que la entidad está indicando realizar.

9.2 ¿USTED COMO EXPERTO EN CIBERSEGURIDAD APLICARÍA A ESTE TRABAJO EN HACKERS SECURITY, DONDE LA ORGANIZACIÓN DISPONE DE UN SUELDO DE $15.000.000 DE PESOS COLOMBIANOS MENSUALES Y CONTRATO VITALICIO?

Un sueldo de $15.000.000 y modalidad de vinculación vitalicia, es una oferta tentadora para cualquier profesional en ciberseguridad en Colombia, puesto que significaría una muy buena estabilidad económica y laboral. Sin embargo, después de leer un acuerdo de confidencialidad como el propuesto por la organización Hackers Security, en dónde explícitamente obligan al profesional a ir en contra de su código de ética e integridad personal y profesional, exponiéndose a sanciones por parte del COPNIA, en las cuales, hasta le podrían cancelar la matrícula profesional, adicionalmente, cosas más graves, como ser coparticipe de acciones delictivas tipificadas en la Ley 1273 de 2009, arriesgándose a problemas legales y resultar en la cárcel, son razones de bastante peso para no aceptar una propuesta laboral como estas.

El autor de este documento considera que siempre debe primar el buen nombre, la honra y la reputación de cada persona, teniendo en cuenta que, en la ceremonia de graduación como profesionales, se jura ante Dios y la Patria, colocar al servicio de la sociedad los conocimientos y principios éticos de manera íntegra y leal en el ejercicio de la profesión.

10 ANÁLISIS OPERACIÓN ANDROMEDA BUGGLY EN LA CIUDAD DE BOGOTÁ

Buggly fue un espacio físico en Bogotá, que inició con el objetivo de construir una comunidad de seguridad informática, o por lo menos así lo querían hacer ver. Allí se reunían jóvenes a jugar videojuegos, compartir sus conocimientos, y a realizar retos técnicos de seguridad informática que no suponían ninguna malicia.

Sin embargo, detrás de todo estaba una unidad de inteligencia del Ejército Nacional de Colombia, en una operación llamada “Andrómeda” que tenía como objetivo “Adquirir conocimientos de informática del hacking ético”. [17]

Todo lo anterior resultó ser una fachada para ocultar de cierta manera, acciones delictivas que se cometían en esas instalaciones, las cuales eran ejecutadas tanto por personal militar, como externos, con alto conocimiento informático, sin control o supervisión alguna. Dentro de esas acciones delictivas se encontraba espionaje y violación de datos personales, los cuales fueron clara evidencia de que se cometían los delitos de “Acceso abusivo a un sistema informático”, “Interceptación de datos informáticos” y “Violación de datos personales” consagrados en los artículos 269A, 269C y 269F de la Ley 1273 de 2009, respectivamente.

Como ha sucedido en muchos casos en Colombia, y en el mundo, todo se fue poniendo aún más oscuro, cuando de esa información interceptada quisieron sacar provecho para lucrarse personalmente. Varios de los militares adscritos a la operación Andrómeda, vendieron parte de la información recopilada, a terceros, obteniendo recompensas económicas. Dentro de la información vendida, se encontraba accesos a correos de miembros de las FARC, acceso a

[17] ENTER.CO. [Sitio Web]. Detrás de Buggly: la historia de la fachada Andrómeda. [Consultado: 12 de septiembre 2022]. Disponible en internet: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

información de desmovilizados de la misma guerrilla, lo que constituyó, por la naturaleza de esta información, en una revelación de secreto público, que según el Artículo 418 del código penal Colombiano “El servidor público que indebidamente dé a conocer documento o noticia que deba mantener en secreto o reserva, incurrirá en multa y pérdida del empleo o cargo público”.[18]

Adicionalmente, según lo consignado en el numeral 2 del Articulo 269H de la Ley 1273 de 2009, a estos militares les aplicaría la agravación punitiva que consiste en el aumento de la mitad a las tres cuartas partes de la pena de los delitos que cometieron, por el hecho de ser servidores públicos. Como también, por lo descrito en el numeral 5 al obtener provecho para sí mismo.

[18] LEYES.CO. [Sito Web]. Código Penal Artículo 418. Revelacion de secreto. [Consultado: 12 de septiembre 2022]. Disponible en internet: https://leyes.co/codigo_penal/418.htm#:~:text=Art%C3%ADculo%20418.,del%20empleo%20o%20cargo%20p%C3%BAblico.

11 ACTIVIDADES BLUE TEAM Y RED TEAM A TRAVÉS DE UN LABORATORIO EN UN ENTORNO SIMULADO PARA LA SOLUCIÓN DE UNA SITUACIÓN PROBLEMA

Para el montaje del entorno simulado se omitirá el paso de descargar e instalar la herramienta Oracle VirtualBox, ya que esto se hizo previamente para el desarrollo de otras actividades de laboratorio para la Especialización en Seguridad Informática.

11.1 SITUACIÓN PROBLEMA

La empresa Hackers Security requiere identificar por qué se está generando una serie de fuga de información la cual se presenta al interior de la organización en dos de sus equipos de cómputo. La información con la que se cuenta es la siguiente: Los equipos de cómputo de los cuales se sospecha cuentan con Windows 7 X86 y X64, estos equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O. y no pueden ser reemplazados porque la aplicación no está migrada con compatibilidad a otros sistemas operativos. Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red. Al momento de la fuga de información (10 de junio de 2022) los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017 preocupando a la organización, porque pueden estar relacionados al fallo de seguridad con identificador CVE-2017-0144, además los equipos de cómputo no tienen instalada la actualización MS17-010.

La organización documenta que no tienen conocimiento cuál de los dos equipos de cómputo es el que está generando la fuga de información, y mencionan también, que en ocasiones uno de esos dos equipos de cómputo suele mostrar un pantallazo azul error de Windows de manera constante.

11.2 HERRAMIENTAS PARA EL DESARROLLO DE LA PRÁCTICA

Las herramientas o aplicaciones que se utilizarán para el desarrollo de esta práctica son las siguientes:

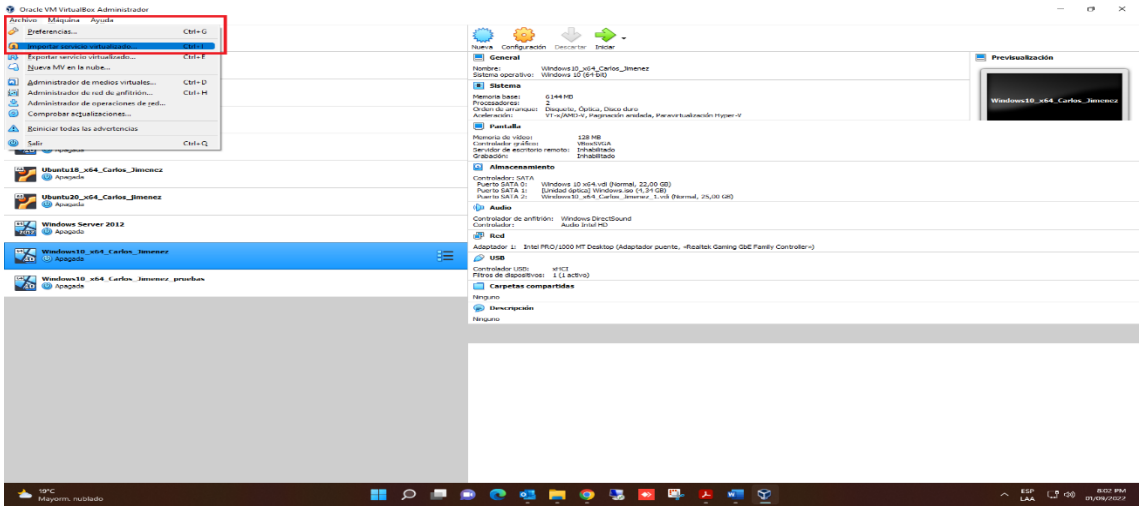
- Oracle VirtualBox: es una herramienta multiplataforma y de código abierto, que permite la virtualización de máquinas que pueden ejecutar diferentes sistemas operativos.
- Kali Linux: es una distribución de Linux diseñada para ejecutar temas de seguridad informática, a través de una variedad de aplicaciones que permiten hacer pentesting, que incluyen análisis de redes, recopilación de información, análisis de vulnerabilidades, herramientas forenses entre otras.
- Metasploit Framework: es una herramienta que se enfoca en realizar pruebas de intrusión, las cuales son realizadas por auditores de seguridad o equipos Blue y Red Team. Esta herramienta contiene exploits, que son en otras palabras, vulnerabilidades conocidas, que, a su vez, incorporan payloads los cuales son los encargados de explotar esas debilidades. Comúnmente se utiliza como una herramienta dentro de Kali Linux.
- NMAP: es una herramienta que, a través de comandos, permite obtener una gran cantidad de información de los equipos que estén dentro de una red objetivo. Puede escanear hosts activos, identificar qué puertos tiene abiertos, qué sistema operativo usa, qué servicios tiene activos, entre otros.

11.3 IMPORTACIÓN DE MÁQUINAS VIRTUALES

En este laboratorio se utilizarán tres (3) máquinas virtuales con diferentes sistemas operativos, una con Windows 7 x64, otra con Windows 7 x86, y otra con Kali Linux.

Para importar el archivo que contiene la máquina virtual (.OVA), dentro la herramienta VirtualBox, se debe dar click en “Archivo” y luego en “Importar servicio Virtualizado”, como lo muestra la siguiente figura.

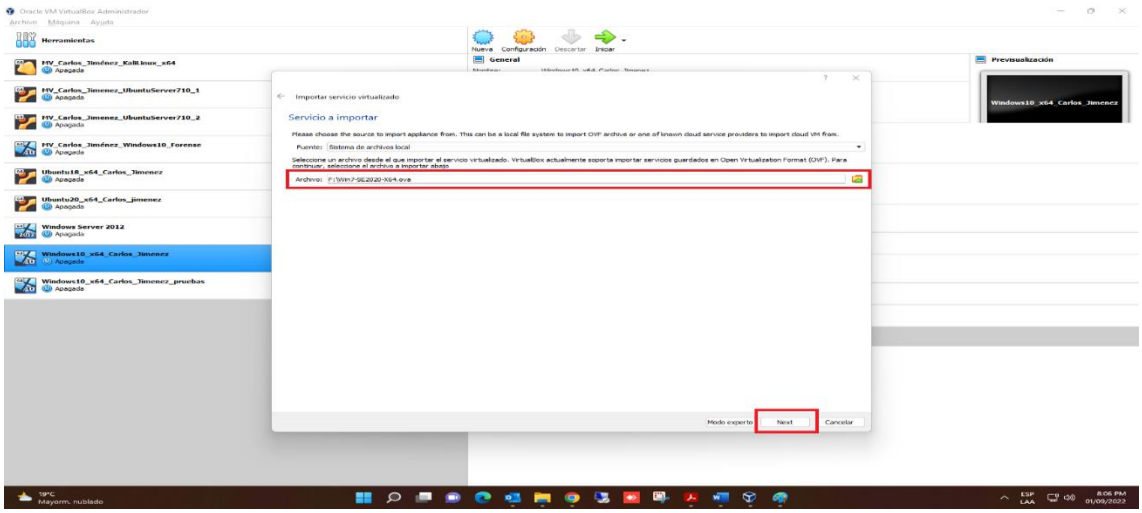
Figura 7. Importación de máquina virtual a Oracle VirtualBox



Fuente: Autor del documento

Luego, dentro del cuadro de dialogo que se abre, se debe seleccionar el archivo .OVA que contiene la primera máquina virtual y se da click en “Next”. La primera máquina que se importará es la de Windows 7 x64, como lo muestra la siguiente imagen.

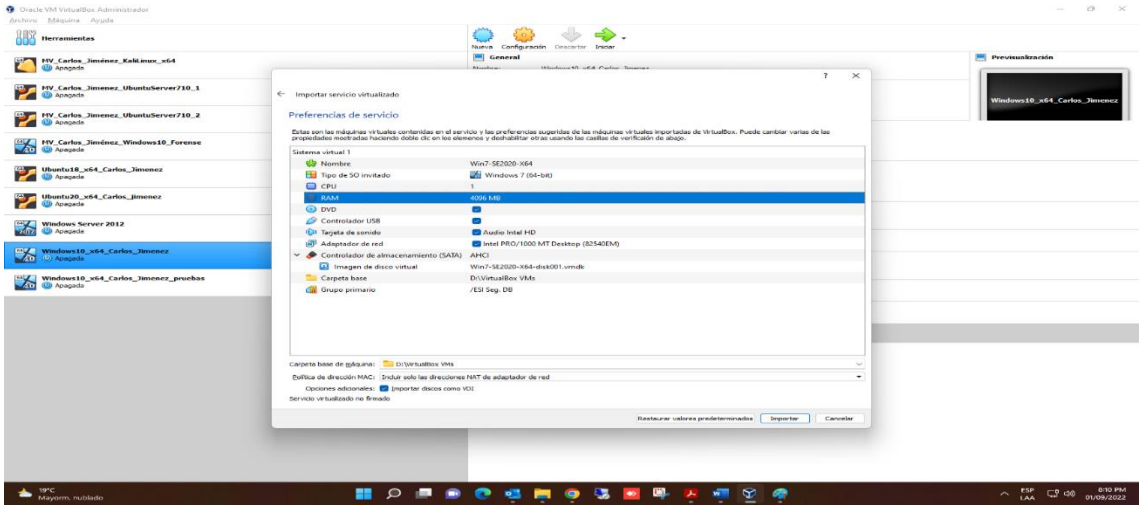
Figura 8. Importación de máquina Windows 7 x64 en Oracle VirtualBox



Fuente: Autor del documento

Ahora, la herramienta mostrará las configuraciones predeterminadas con que se importará la máquina, tales como cantidad de memoria RAM que se asignará, como también la cantidad de núcleos de procesador, si se desea activar el puerto ethernet, entre otras. Estas configuraciones se pueden modificar, pero para esta actividad se dejarán las que tiene asignadas de manera predeterminada.

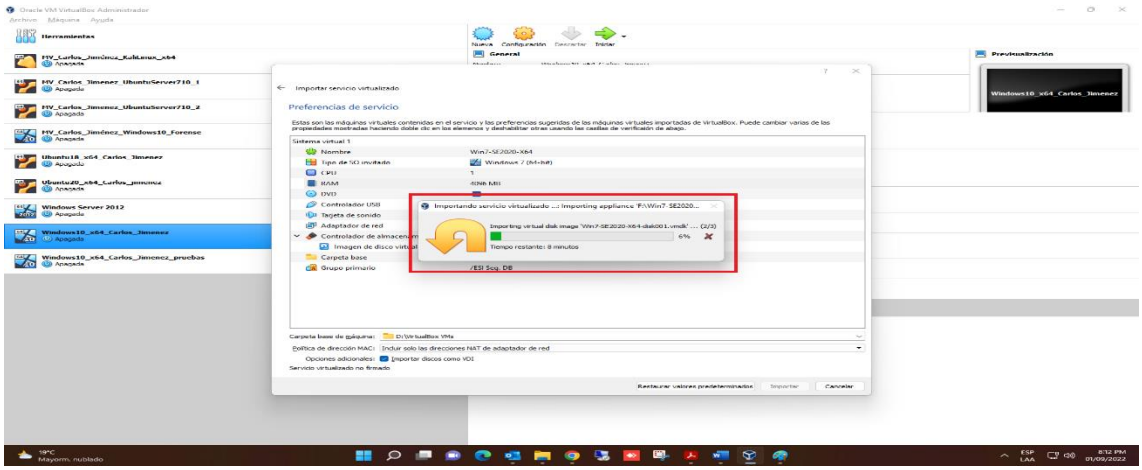
Figura 9. Importación de máquina Windows 7 x86 en Oracle VirtualBox



Fuente: Autor del documento

Al dar click en el botón “Importar”, empezará el proceso de importación de la primera máquina virtual, el cual tarda varios minutos.

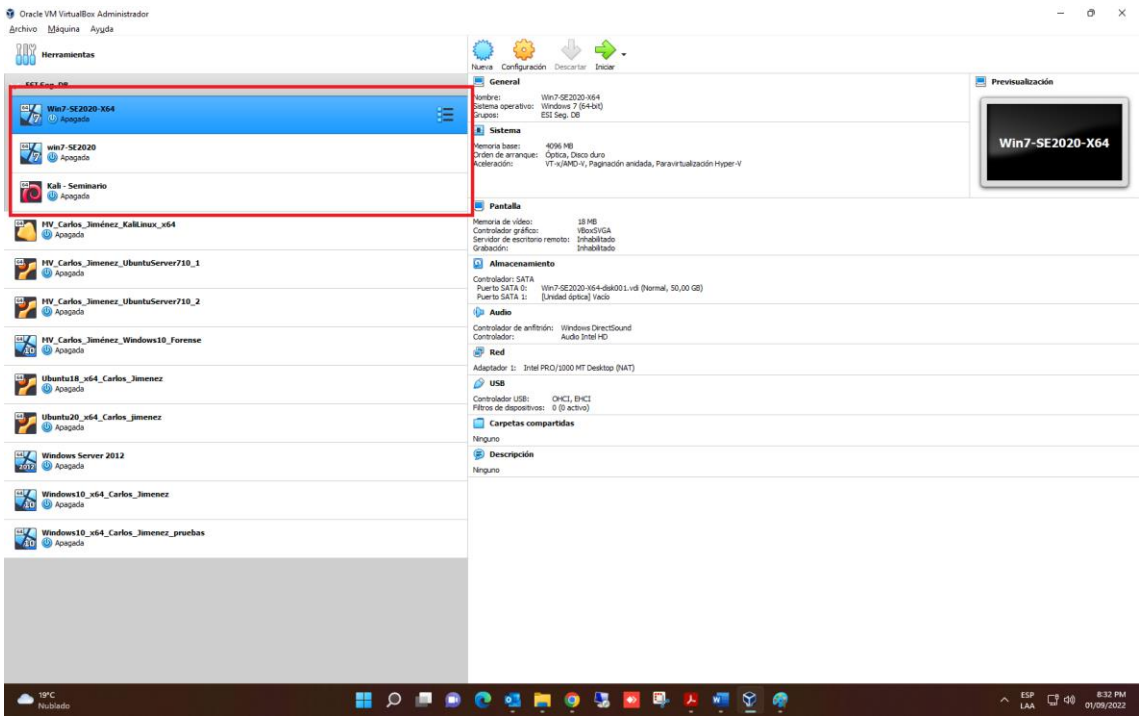
Figura 10. Barra de progreso importación de máquina virtual en VirtualBox



Fuente: Autor del documento

Posteriormente, se repite el mismo proceso de importación para las otras dos máquinas (Windows 7 x86 y Kali Linux), y luego de finalizar las tres (3) importaciones, se observan las máquinas virtuales en la interfaz principal de VirtualBox, como lo muestra la siguiente figura.

Figura 11. Máquinas virtuales importadas en VirtualBox



Fuente: Autor del documento

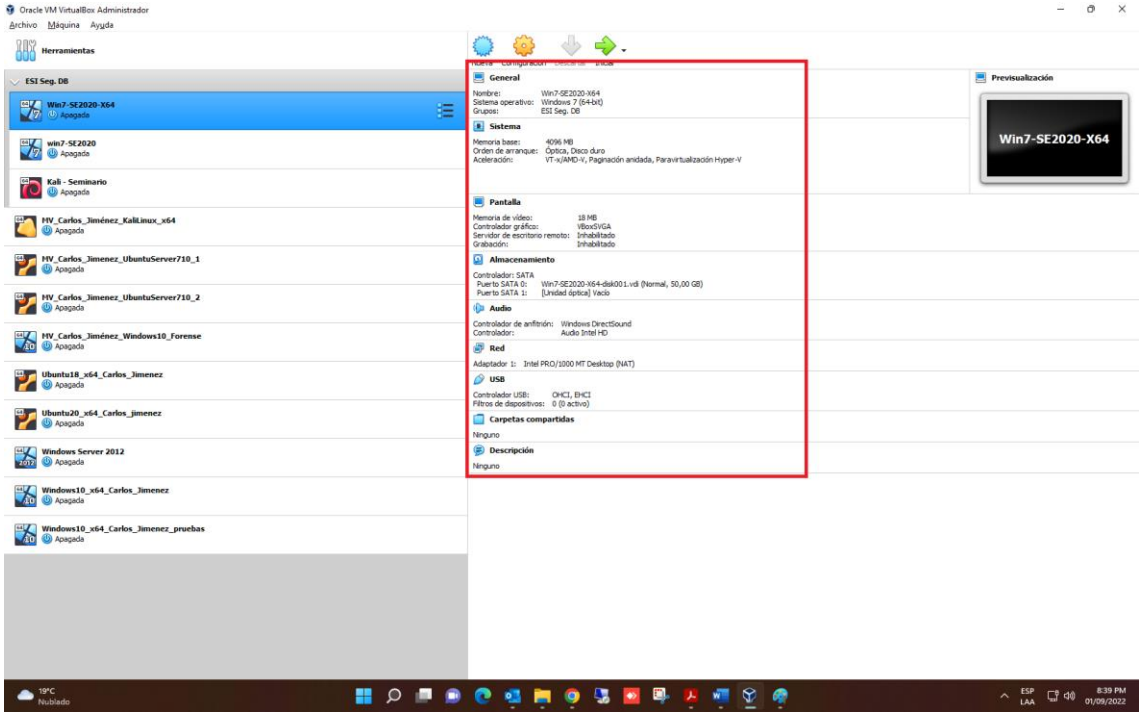
11.4 CONFIGURACIÓN DE LAS MÁQUINAS VIRTUALES

11.4.1 Especificaciones técnicas básicas máquina Windows 7 x64. Las especificaciones técnicas básicas de esta máquina virtual son las siguientes:

- Sistema Operativo: Windows 7 (64-bit)
- Memoria RAM: 4096mb
- Memoria de video: 18mb
- Almacenamiento: 50gb
- Adaptador de red: Intel Pro/1000

La anterior información se puede evidenciar en la siguiente figura.

Figura 12. Especificaciones técnicas máquina virtual con Windows 7 x64



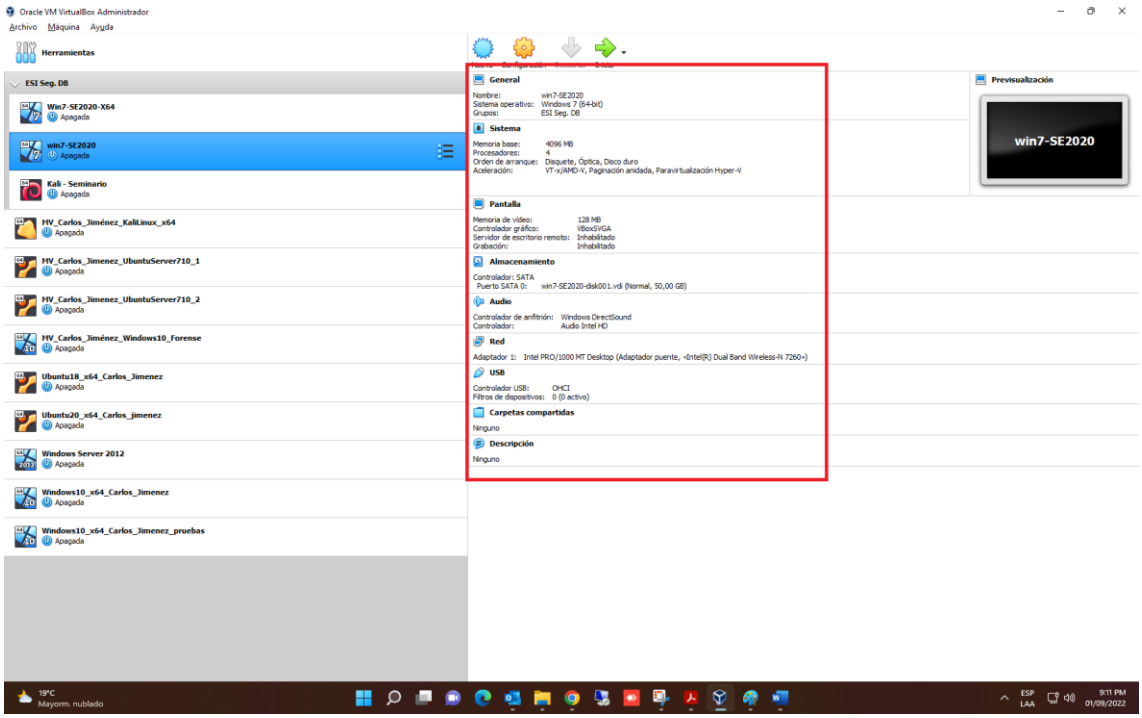
Fuente: Autor del documento

11.4.2 Especificaciones técnicas básicas máquina Windows 7 x86. Las especificaciones técnicas básicas de esta máquina virtual son las siguientes.

- Sistema Operativo: Windows 7 (64-bit)
- Memoria RAM: 4096mb
- Procesadores: 4
- Memoria de video: 128mb
- Almacenamiento: 50gb
- Adaptador de red: Intel Pro/1000

La anterior información se puede evidenciar en la siguiente figura.

Figura 13. Especificaciones técnicas máquina virtual con Windows 7 x86



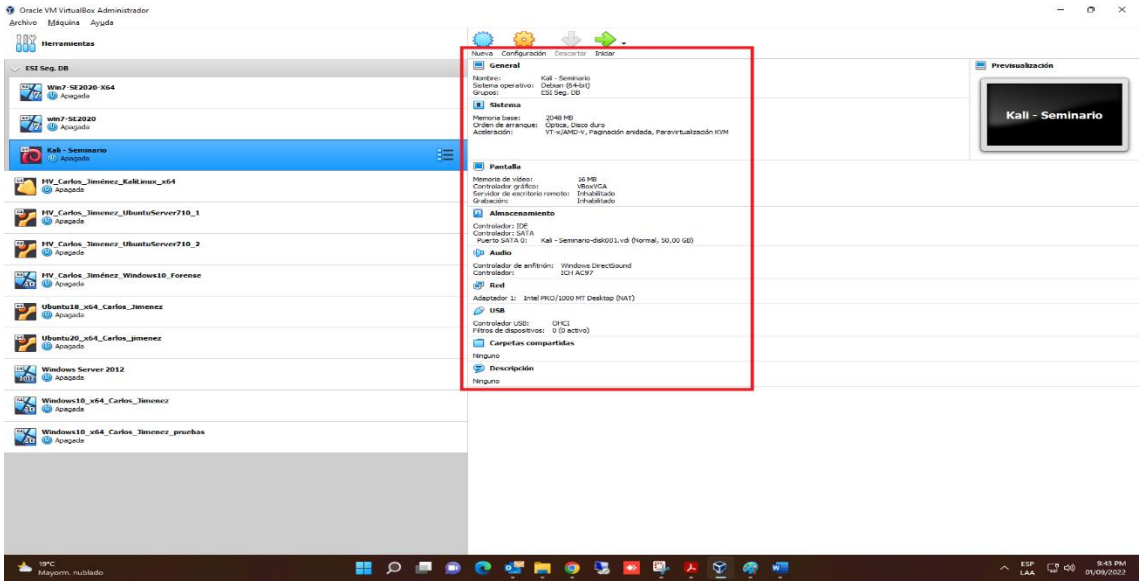
Fuente: Autor del documento

11.4.3 Especificaciones técnicas básicas máquina Kali Linux. Las especificaciones técnicas básicas de esta máquina virtual son las siguientes.

- Sistema Operativo: Debian (64-bit)
- Memoria RAM: 2048mb
- Memoria de video: 16mb
- Almacenamiento: 50gb
- Adaptador de red: Intel Pro/1000

La anterior información se puede evidenciar en la siguiente figura.

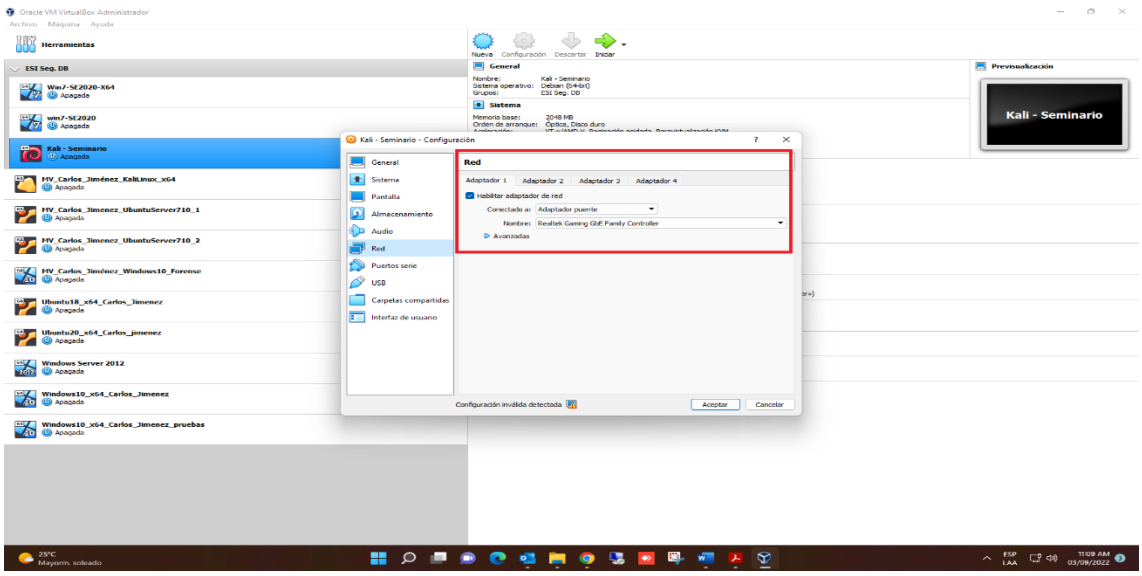
Figura 14. Especificaciones técnicas máquina virtual con Kali Linux



Fuente: Autor del documento

11.4.4 Configuración de red. El adaptador de red para cada una de las máquinas se configura en modo puente. Lo anterior hace que el direccionamiento IP que obtiene cada máquina, sea el que asigne el DHCP del modem al que se encuentra conectado el computador físico. Esta configuración se hace como lo muestra la siguiente figura.

Figura 15. Configuración de adaptador de red en modo puente VirtualBox



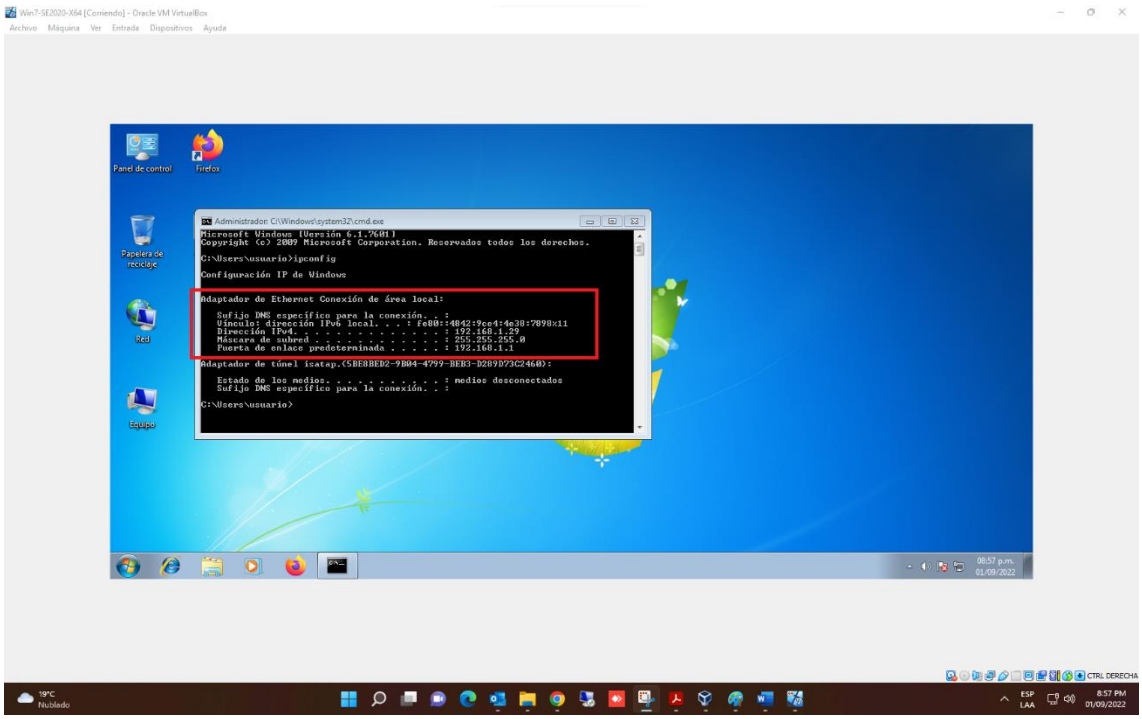
Fuente: Autor del documento

En las máquinas con Windows, se accede a la consola CMD, y con el comando “ipconfig” se consulta el direccionamiento IP asignado a cada una.

Para la máquina con Windows 7 x64, el direccionamiento IP es el siguiente:

- Puerta de enlace predeterminada: 192.168.1.1
- Dirección IP: 192.168.1.29
- Máscara de subred: 255.255.255.0

Figura 16. Direccionamiento IP máquina con Windows 7 x64

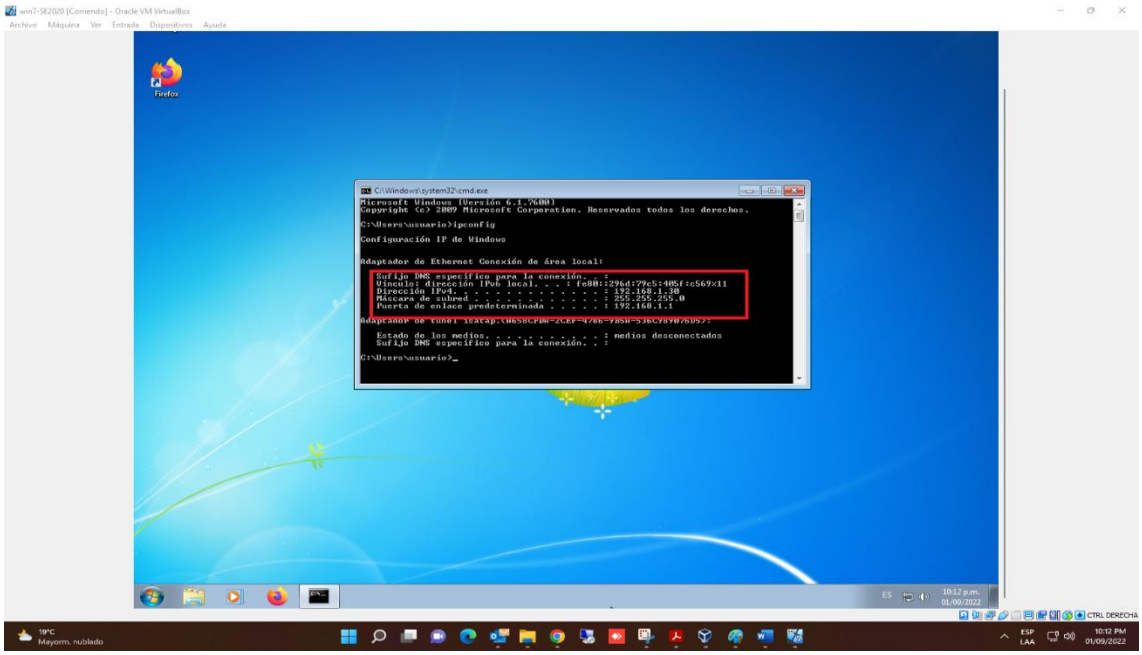


Fuente: Autor del documento

Para la máquina con Windows 7 x86, el direccionamiento IP es el siguiente:

- Puerta de enlace predeterminada: 192.168.1.1
- Dirección IP: 192.168.1.30
- Máscara de subred: 255.255.255.0

Figura 17. Direccionamiento IP máquina con Windows 7 x86

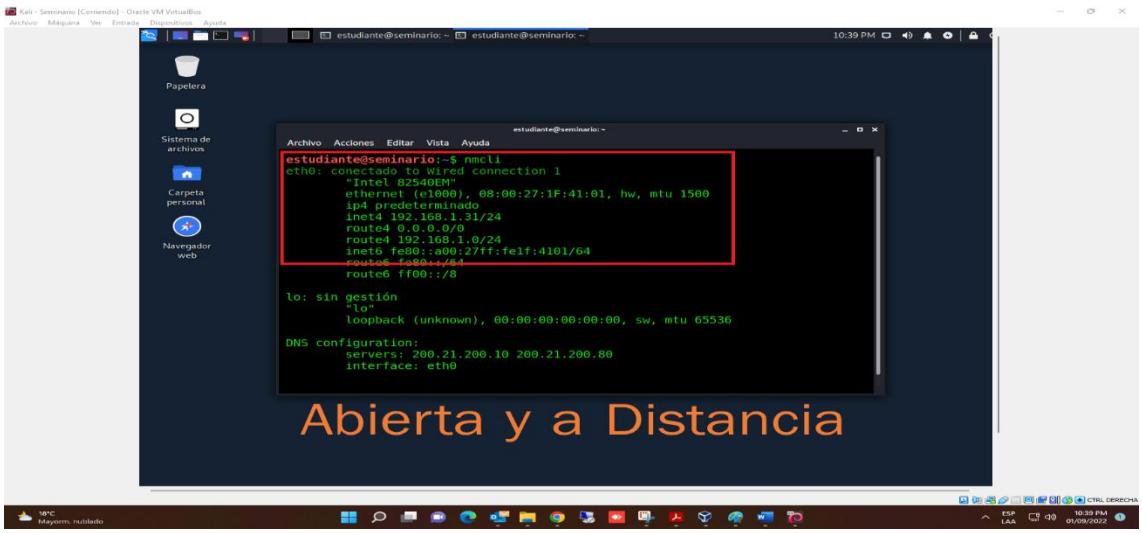


Fuente: Autor del documento

En la máquina con Linux, se accede a la consola, y con el comando “nmcli” se consulta el direccionamiento IP, el cual es el siguiente:

- Dirección IP: 192.168.1.31/24
- Máscara de subred: 255.255.255.0

Figura 18. Direccionamiento IP máquina con Kali Linux



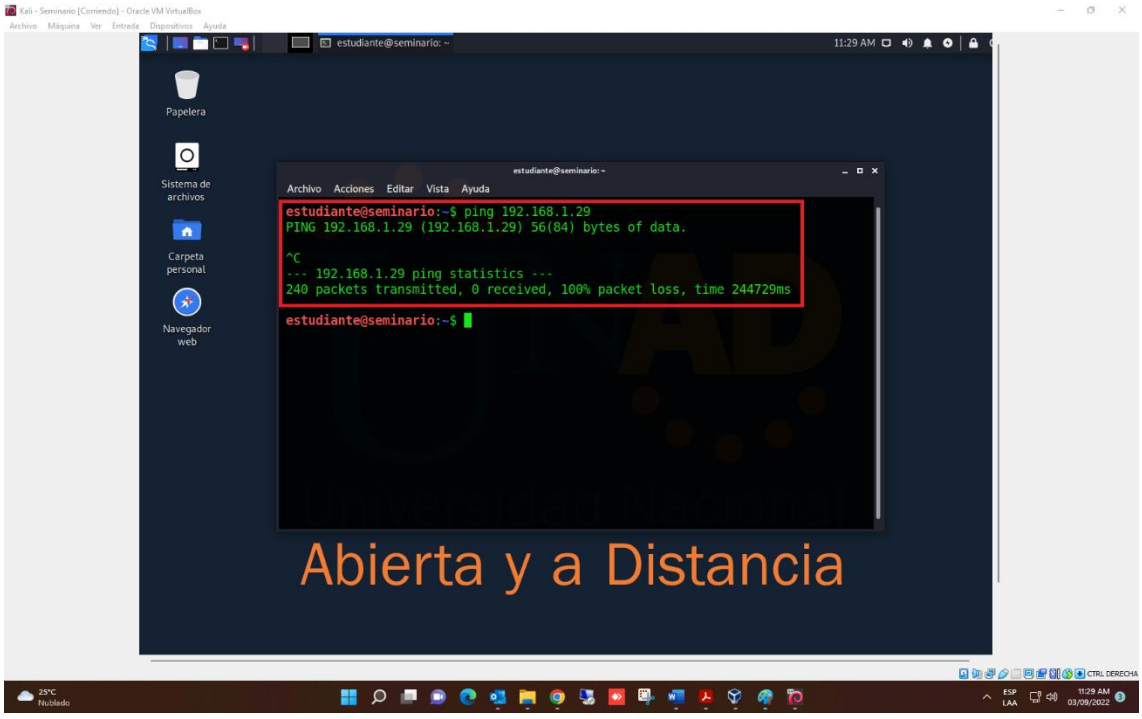
Fuente: Autor del documento

11.5 DIAGNÓSTICO DE COMUNICACIÓN ENTRE MÁQUINAS VIRTUALES

Con el comando “ping” en la consola de ambas máquinas se realiza un diagnóstico de conexión. Esta sintaxis envía tráfico a través del protocolo ICMP, y si existe conexión entre las dos máquinas, el resultado será que el destinario recibió los paquetes, en caso contrario, el mensaje será que no hubo respuesta a los paquetes enviados o se rechazaron.

11.5.1 Comunicación entre máquinas Kali Linux y Windows 7 x64. La siguiente figura describe el diagnóstico de conexión enviando paquetes desde la máquina Kali Linux hacia la máquina con Windows 7 x64.

Figura 19. Diagnóstico de comunicación entre Kali Linux y Windows 7 x64

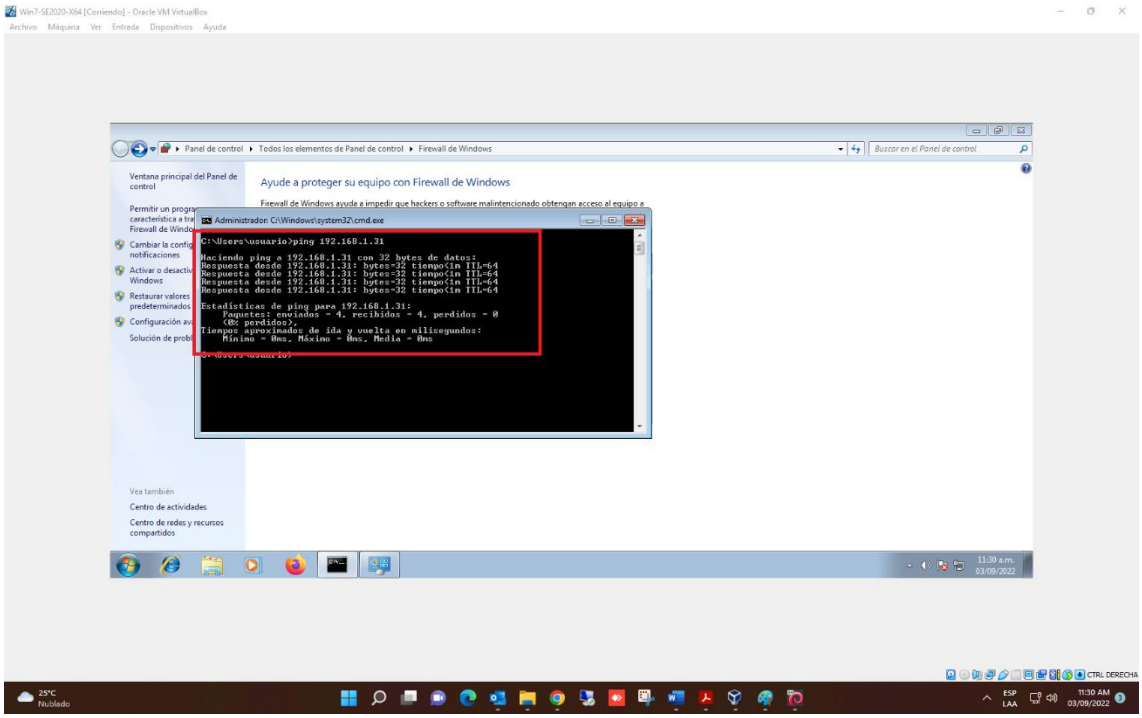


Fuente: Autor del documento

Como se puede apreciar en la figura anterior, se enviaron 240 paquetes desde la máquina Kali Linux, pero no hubo respuesta de parte de la máquina Windows 7 x64. Esto es debido a que el firewall de Windows está bloqueando el tráfico que se transmite a través de ese protocolo (ICMP).

Sin embargo, si se realiza el diagnóstico de conexión desde la máquina Windows 7 x64 hacia Kali Linux, se puede observar que sí existe comunicación entre ellas, ya que los 4 paquetes que se enviaron, fueron recibidos por el destinatario, como lo muestra la siguiente figura.

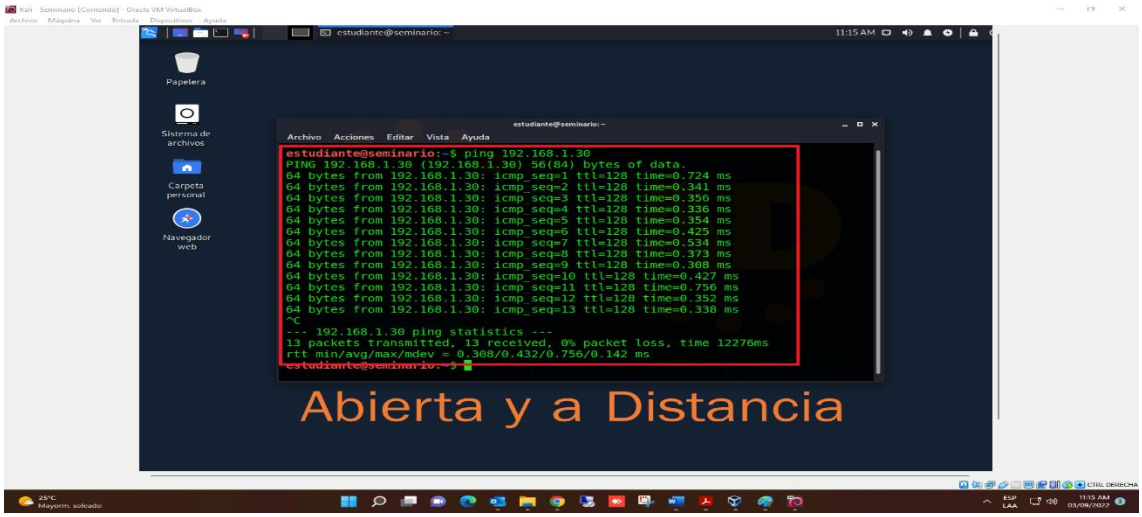
Figura 20. Diagnóstico de comunicación entre Windows 7 x64 y Kali Linux



Fuente: Autor del documento

11.5.2 Comunicación entre máquinas Kali Linux y Windows 7 x86. La siguiente figura describe el diagnóstico de conexión enviando paquetes desde la máquina Kali Linux hacia la máquina con Windows 7 x86.

Figura 21. Diagnóstico de comunicación entre Kali Linux y Windows 7 x86

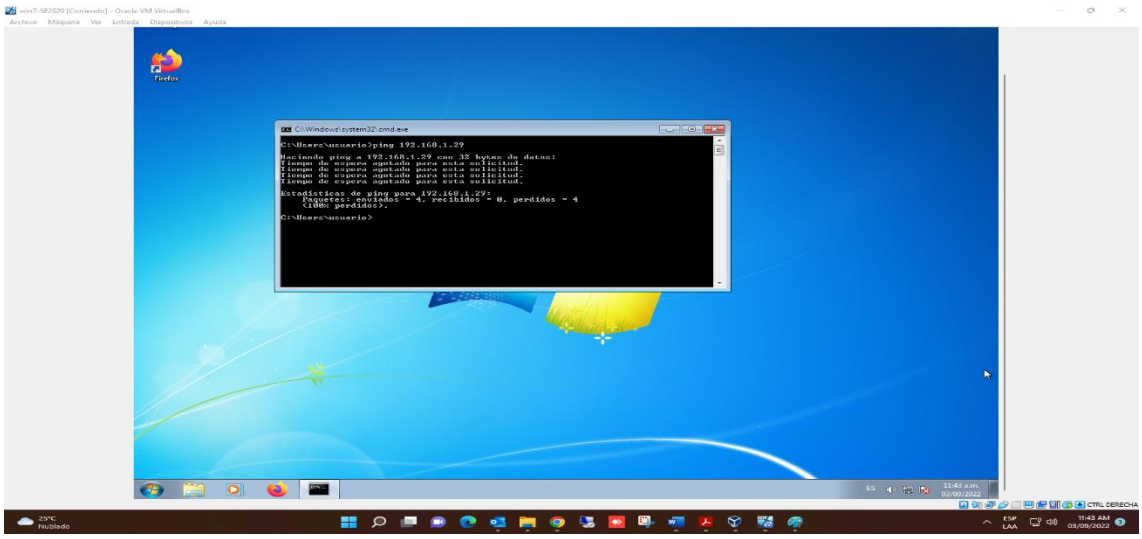


Fuente: Autor del documento

Como se puede observar en la anterior figura, se enviaron 13 paquetes ICMP, de los cuales la máquina con Windows 7 x86, recibió los 13, comprobando que existe comunicación entre ambas máquinas.

11.5.3 Comunicación entre máquinas Windows 7 x64 y Windows 7 x86. La siguiente figura describe el diagnóstico de conexión enviando paquetes ICMP desde la máquina Windows 7 x86 hacia la máquina con Windows 7 x64.

Figura 22. Diagnóstico de comunicación entre Windows 7 x64 y Windows 7 x86

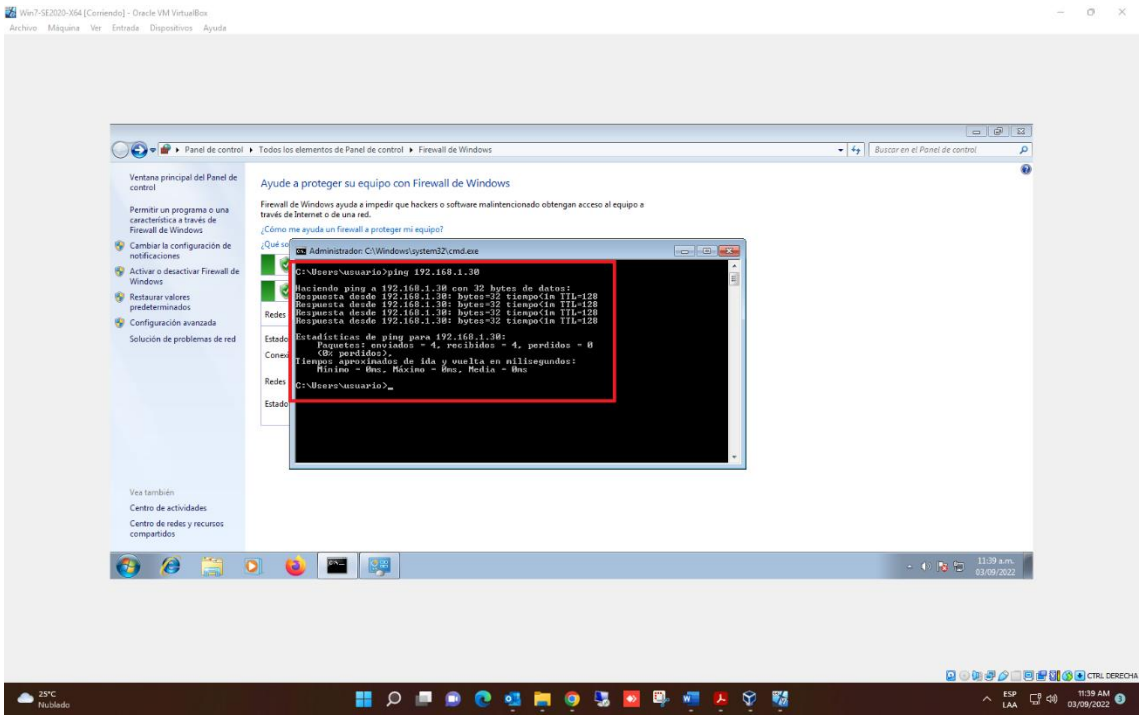


Fuente: Autor del documento

Como ocurrió con el diagnóstico de comunicación entre la máquina con Kali Linux y la Windows 7 x64, nuevamente esta última bloquea el tráfico, debido a la configuración del Firewall de Windows.

Sin embargo, si se realiza el diagnóstico de conexión desde la máquina Windows 7 x64 hacia la máquina con Windows 7 x86, se puede observar que sí existe comunicación entre ellas, como lo muestra la siguiente figura.

Figura 23. Diagnóstico de comunicación entre Windows 7 x64 y Windows 7 x86



Fuente: Autor del documento

11.6 ATAQUE DE INTRUSIÓN A MÁQUINA WINDOWS 7 X64

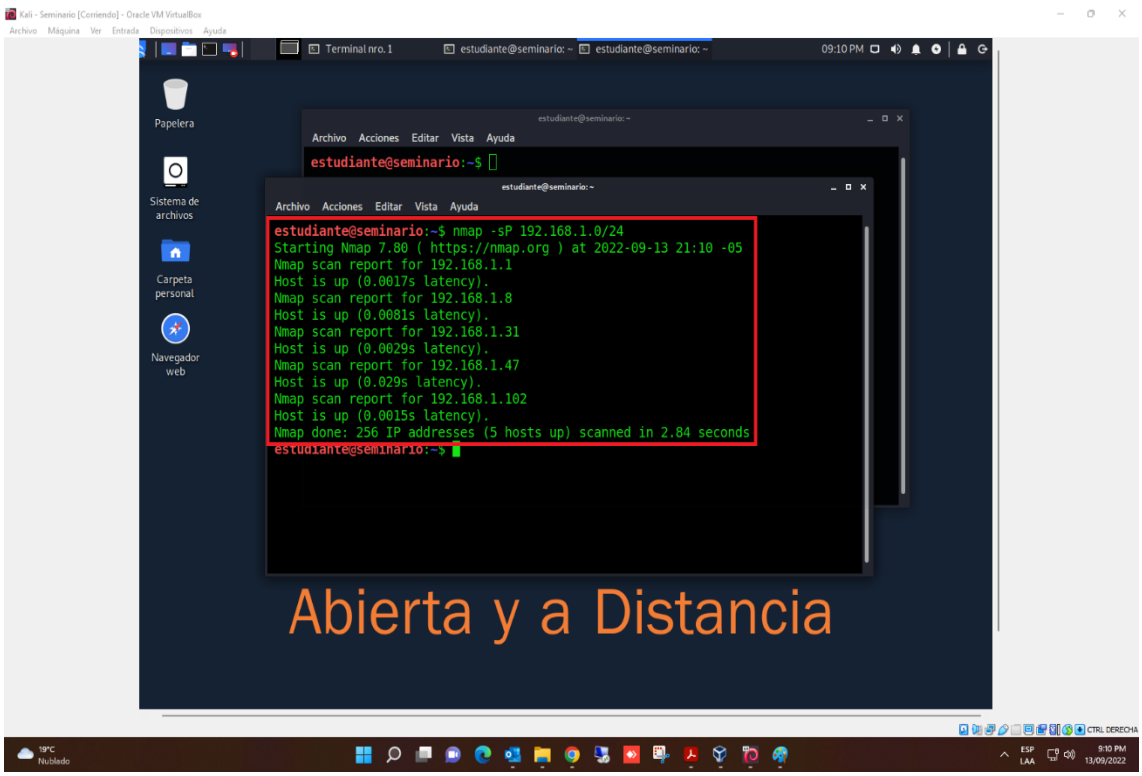
Para recopilar mejores evidencias, esta práctica se va a realizar en dos fases, una primera fase un ataque a una máquina con Windows 7 X64 cuyo Firewall de Windows se encuentra activo, y una segunda fase, un ataque a una máquina con Windows 7 X64 cuyo Firewall de Windows se encuentra Inactivo.

11.6.1 Ataque a máquina Windows 7 X64 con Firewall de Windows activo.

Para dar inicio a un ataque de intrusión, el primer paso o la primera fase es realizar la recopilación de información del objetivo. Para esto, se utilizará la herramienta NMAP.

En primer lugar, se ejecuta la herramienta NMAP en la máquina con Kali Linux. Mediante el comando “nmap -sP 192.168.1.0/24” se realiza un escaneo de hosts para identificar qué equipos se encuentran levantados dentro de la red de área local. Como se puede apreciar en la siguiente figura, luego de ejecutar dicho comando, NMAP lista los hosts que se encuentran activos dentro de la red.

Figura 24. Identificación de hosts activos con NMAP



Fuente: Autor del documento

Se puede apreciar también, que, dentro de los hosts listados, no se encuentra activo o no se identifica la máquina virtual con Windows 7 X64, la cual tiene dirección IP 192.168.1.29. Esto es debido a que el firewall de Windows de esta

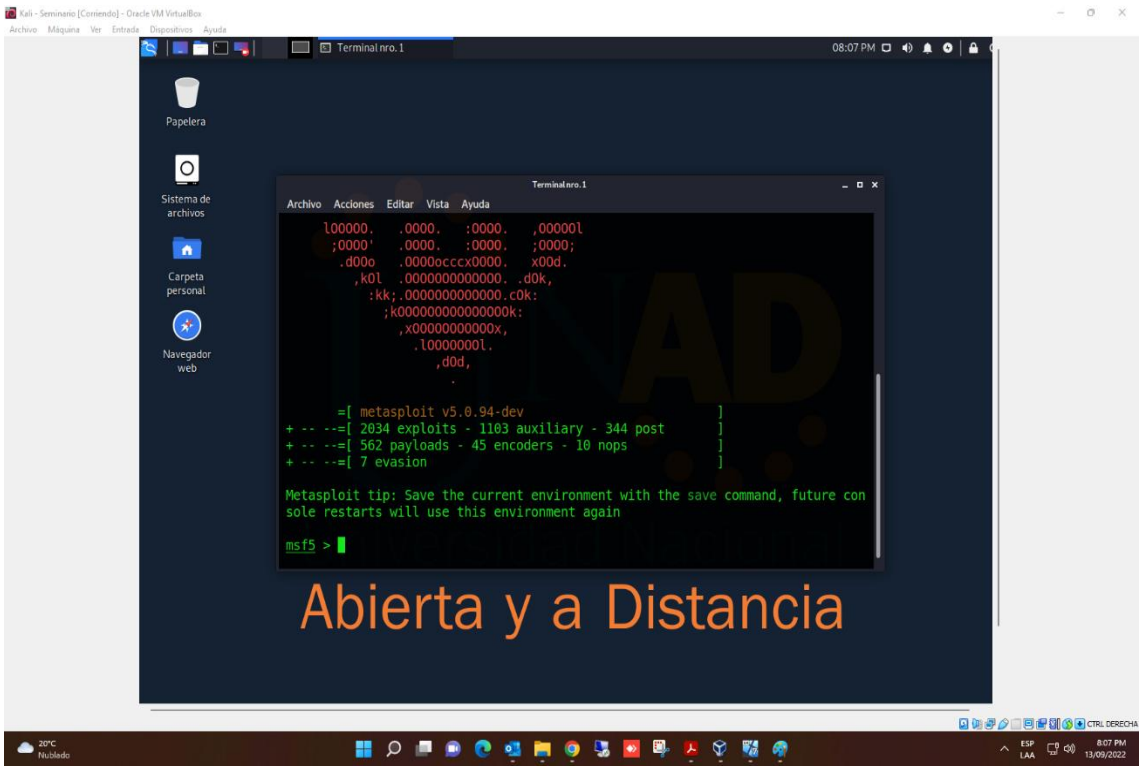
máquina, se encuentra activo, y está bloqueando todo el tráfico a través del protocolo ICMP, el cual es el que se utiliza para validar conexión entre dos máquinas virtuales.

Sin embargo, aprovechando que ya se tenía identificada previamente la dirección IP de la máquina virtual con Windows 7 X64, se intentará realizar el ataque.

Ahora, es turno de la siguiente fase del pestesting, que corresponde a la identificación de vulnerabilidades en el objetivo. Para esto, se utilizará la herramienta Metasploit, la cual, también se encuentra instalada en Kali Linux.

Se ejecuta la herramienta, y su interfaz principal se observa como lo muestra la siguiente figura.

Figura 25. Interfaz principal de Metasploit Framework en Kali Linux

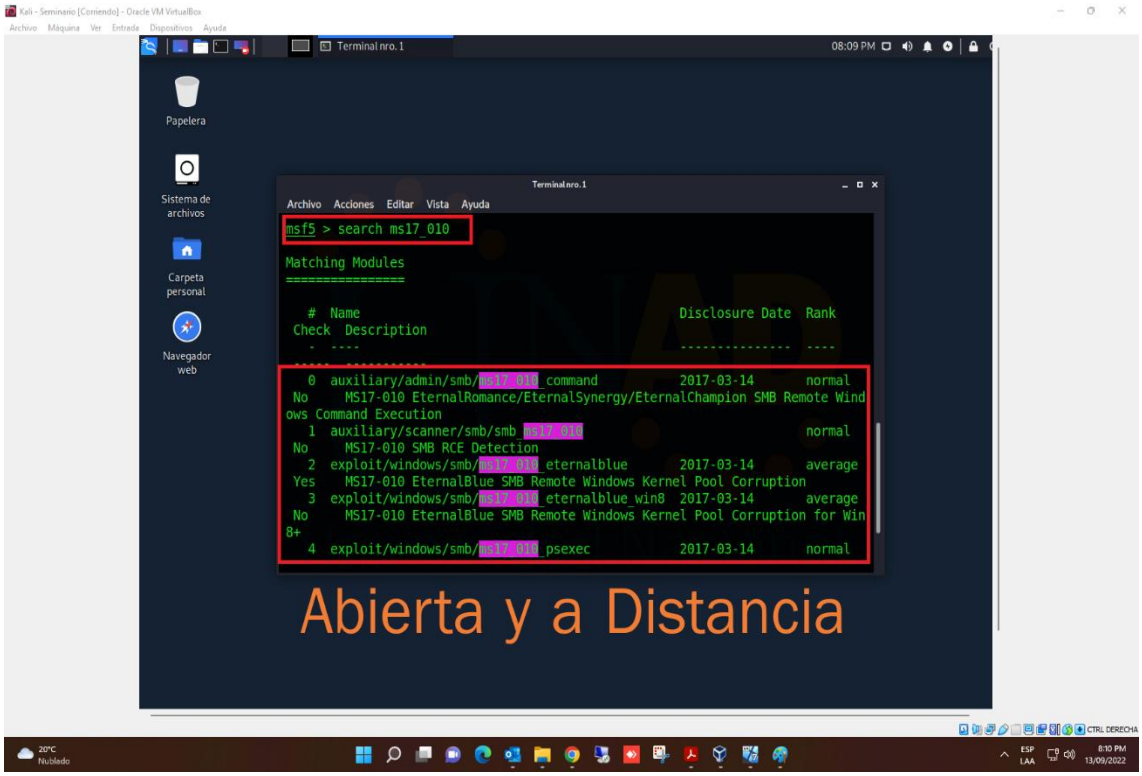


Fuente: Autor del documento

Se sabe desde un principio, que los hosts objetivo de esta práctica, no tienen la actualización MS17-010, la cual es una vulnerabilidad en la que los atacantes pueden aprovechar un fallo en el protocolo SMBv1 para la ejecución remota de código en consola, y acceder al sistema.

Teniendo en cuenta lo anterior, ahora en Metasploit se buscan los exploits que están disponibles para este fallo. Con el comando “search ms17_010”, se le indica a Metasploit, que los busque, y el resultado es lo que muestra la siguiente figura.

Figura 26. Exploits disponibles en Metasploit para vulnerabilidad ms17_010



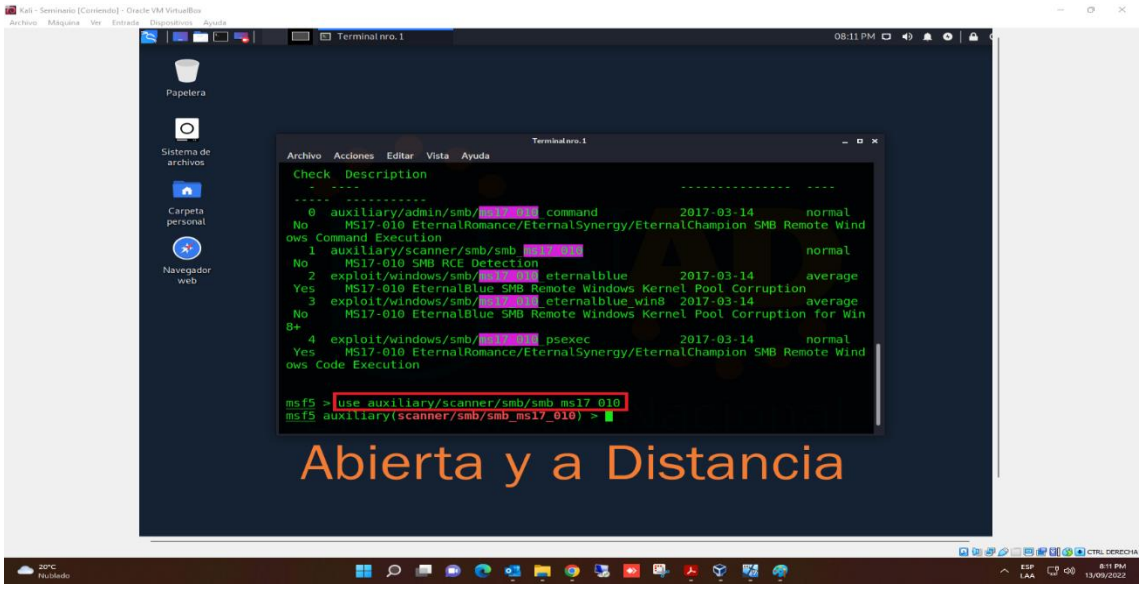
Fuente: Autor del documento

Como se puede observar, la herramienta lista cuatro (4) exploits que se pueden ejecutar para la vulnerabilidad MS17-010.

En primer lugar, se ejecutará el exploit No. 1, que corresponde a un ataque que indica si el objetivo es vulnerable al fallo que corrige la actualización MS17-010.

Para esto, se ejecuta el comando “use auxiliary/scanner/smb/ms17_010_eternalblue”, para seleccionar dicho exploit.

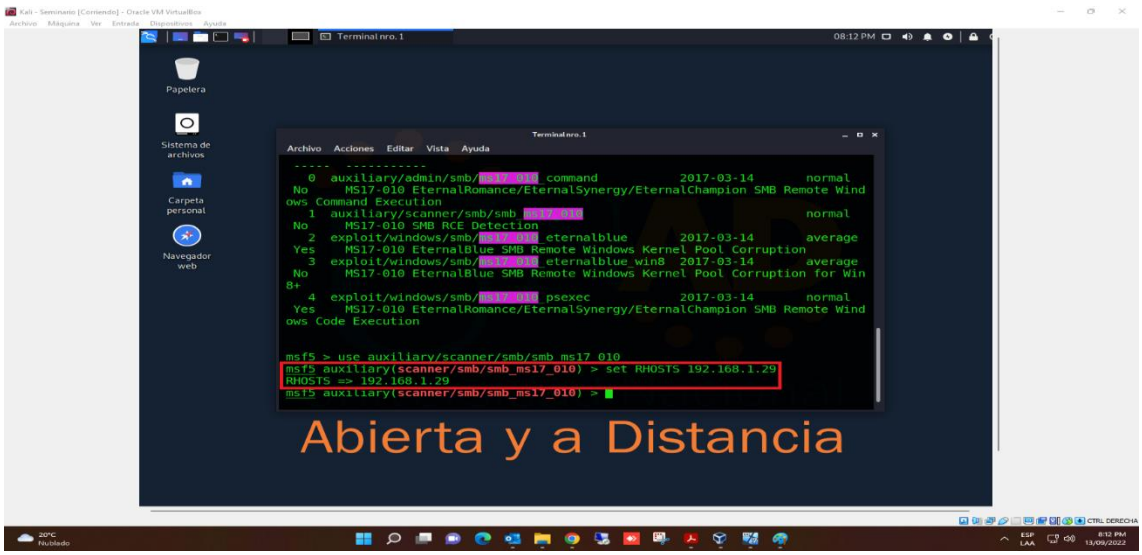
Figura 27. Selección de exploit que escanea si un host el vulnerable a sm17_010



Fuente: Autor del documento

A continuación, se debe establecer la dirección IP de la máquina objetivo. Para esto, se ejecuta el comando “set RHOSTS 192.168.1.29”.

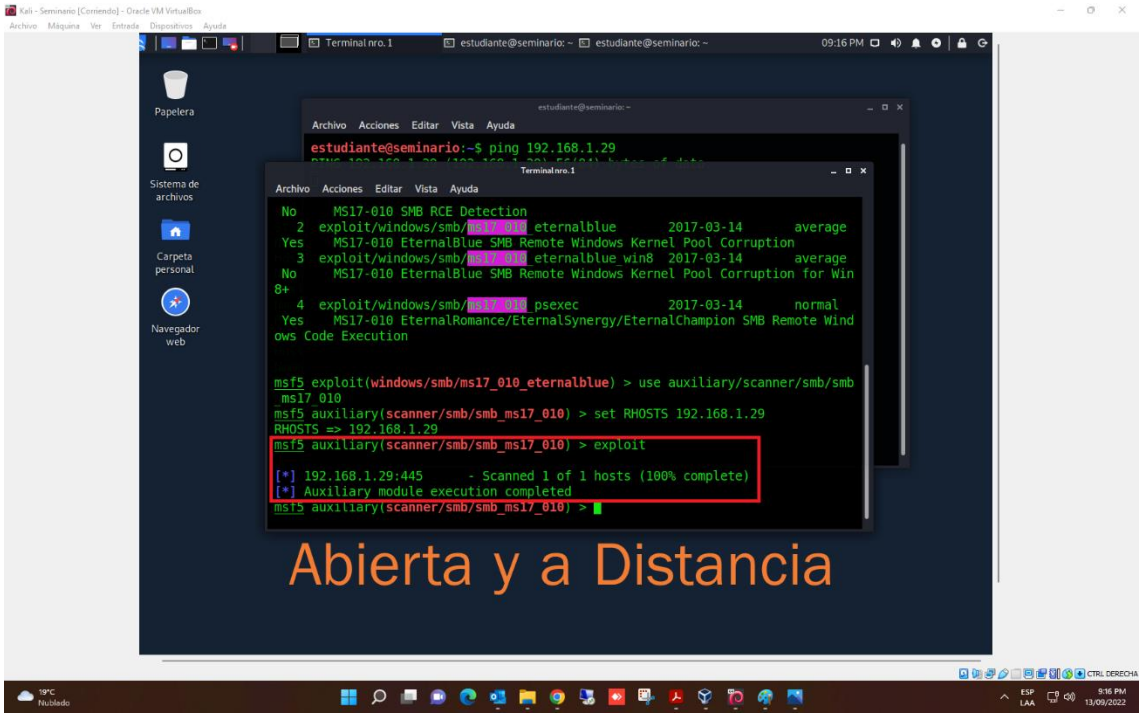
Figura 28. Selección de la dirección IP de la máquina X64



Fuente: Autor del documento

Y, por último, se ejecuta el ataque con el comando “exploit” como lo muestra la siguiente figura.

Figura 29. Ejecución del ataque de escaneo de vulnerabilidad máquina X64

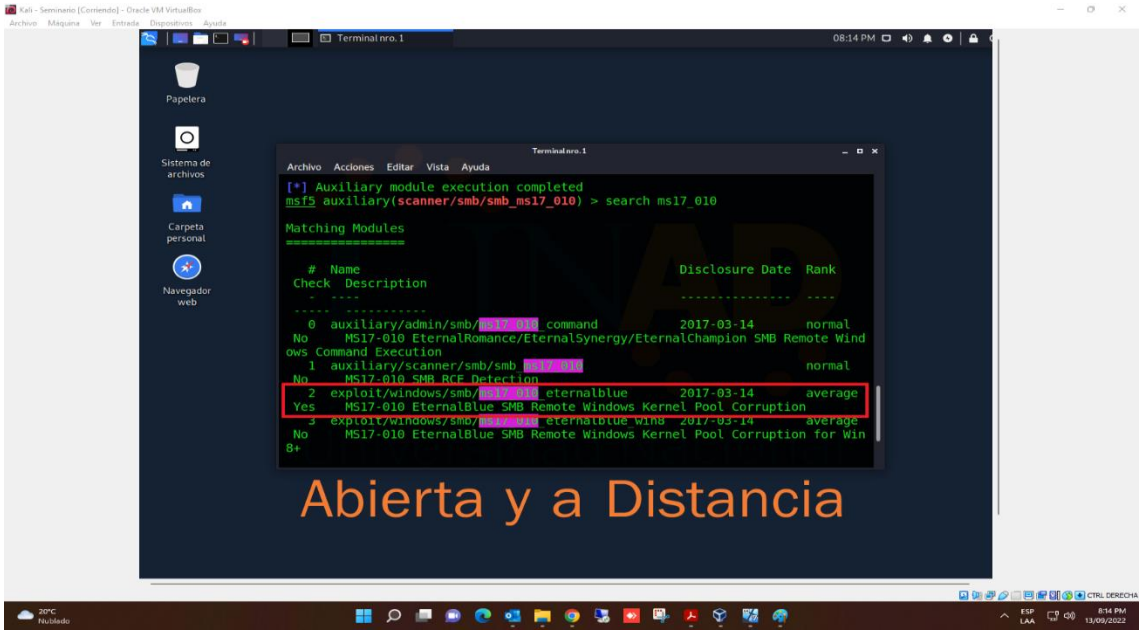


Fuente: Autor del documento

De lo anterior se puede apreciar, que, Metasploit usa el puerto 445 para realizar el ataque, pero nuevamente, el firewall de Windows de la máquina Windows 7 X64, está bloqueando el tráfico de paquetes que utiliza este exploit, porque no se logra identificar si la máquina es vulnerable o no al fallo CVE-2017-0144.

Sin embargo, se intentará acceder a esta máquina con el exploit que aprovecha la vulnerabilidad mencionada anteriormente. Para esto, se utilizará el exploit No. 2, que corresponde al ataque que aprovecha el fallo en el protocolo SMBv1 para establecer conexión remota con la consola de Windows.

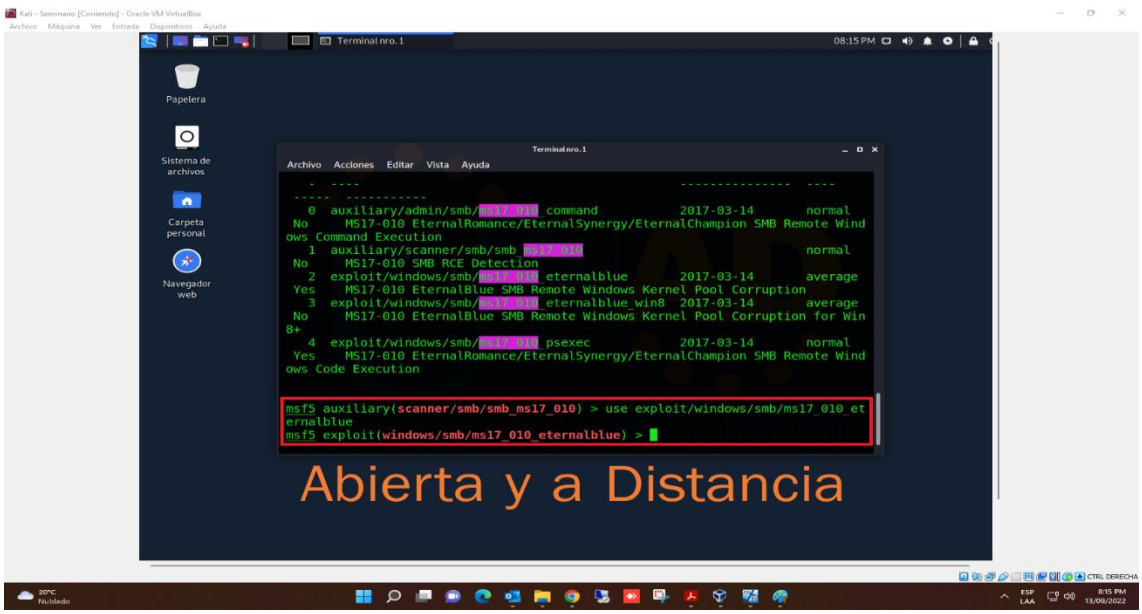
Figura 30. Selección de exploit para ataque de conexión a consola de comandos máquina X64



Fuente: Autor del documento

Nuevamente se usa la sentencia “use”, pero esta vez estableciendo el nuevo exploit que se va a utilizar, como lo muestra la siguiente figura.

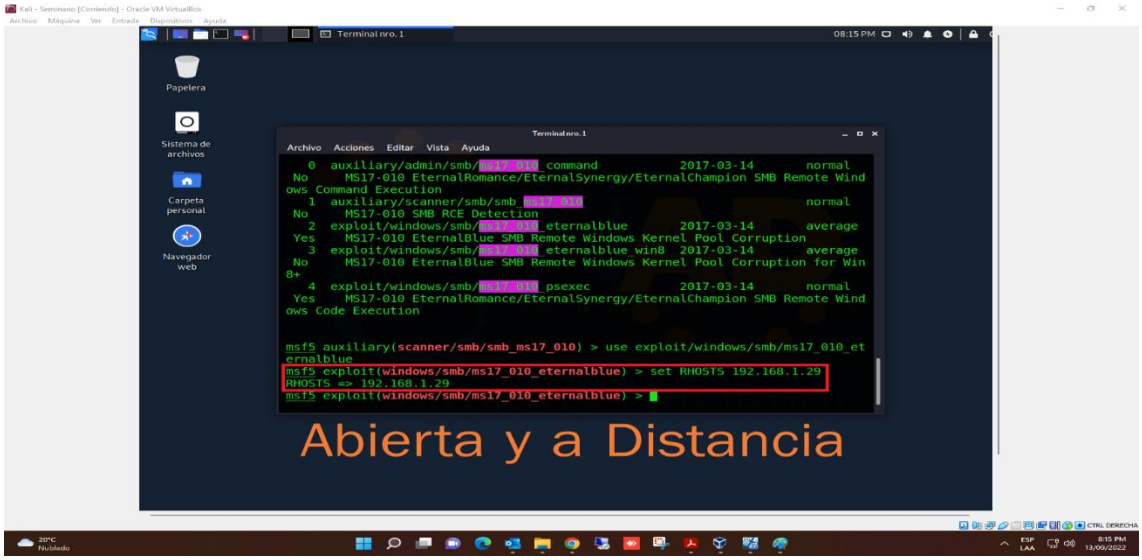
Figura 31. Ejecución del ataque para conexión remota a la consola Windows máquina X64



Fuente: Autor del documento

Ahora, con la sentencia “set RHOSTS”, nuevamente se establece la dirección IP de la máquina objetivo.

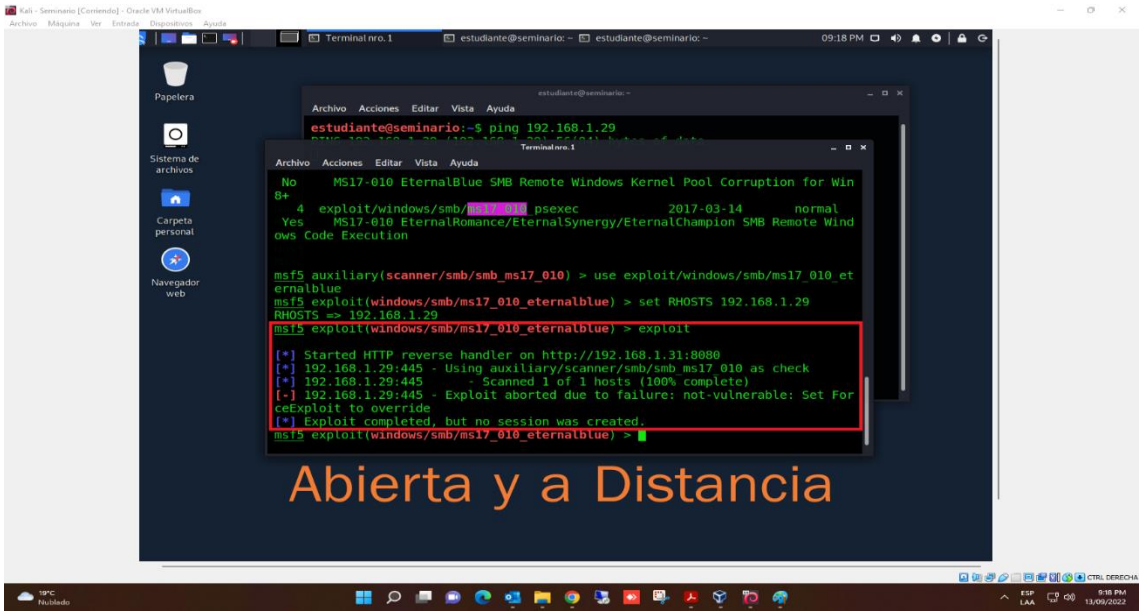
Figura 32. Selección de la dirección IP de la máquina X64



Fuente: Autor del documento

Con la sentencia “exploit” se inicia el ataque, como lo muestra la siguiente figura.

Figura 33. Resultado del ataque al fallo CVE-2017-0144 máquina X64

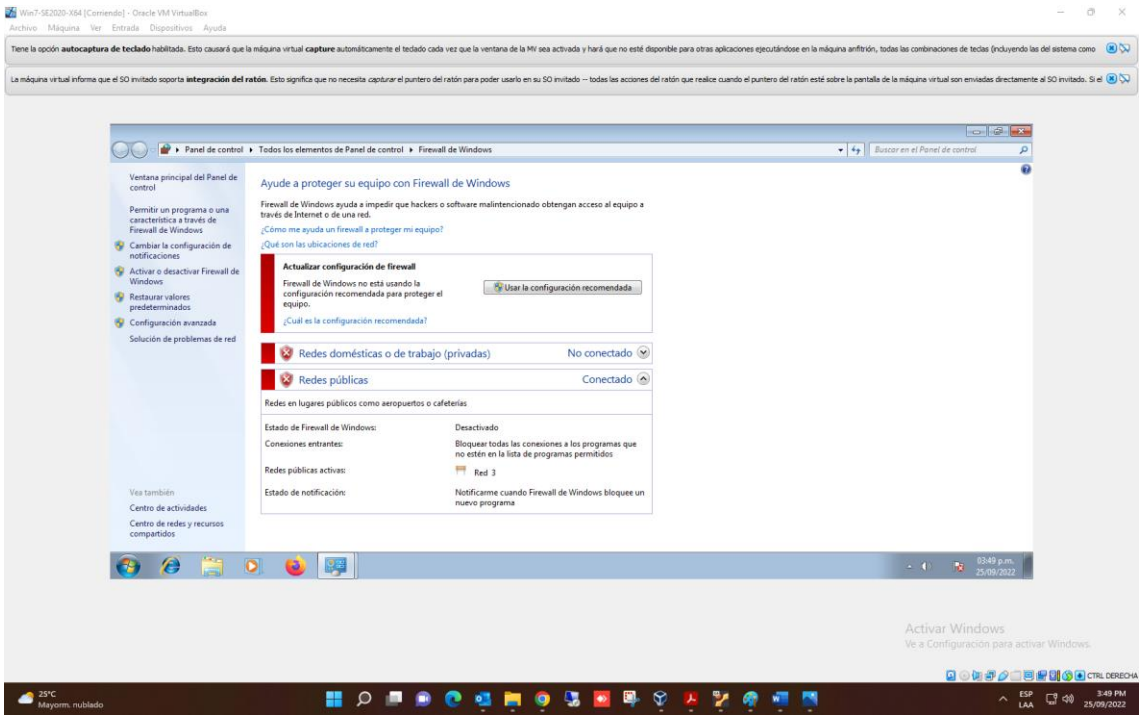


Fuente: Autor del documento

Según lo reflejado en la figura anterior, se puede evidenciar, que el ataque no fue exitoso, y no se logró establecer la conexión remota con la consola de Windows, ya que la máquina objetivo no es vulnerable al fallo CVE-2017-0144. Que un sistema no sea vulnerable a este fallo, es debido a que tiene un firewall que está bloqueando tráfico, o porque sencillamente ya cuenta con la respectiva actualización que corrige esta vulnerabilidad.

11.6.2 Ataque a máquina Windows 7 X64 con Firewall de Windows Inactivo. Para este ataque se va a usar como máquina atacante un Kali Linux en versión 2022, cuya herramienta Metasploit se encuentra en la versión 6. Adicionalmente, se desactivará el Firewall de Windows de la máquina Windows 7, como lo muestra la siguiente figura.

Figura 34. Firewall de Windows desactivado máquina X64

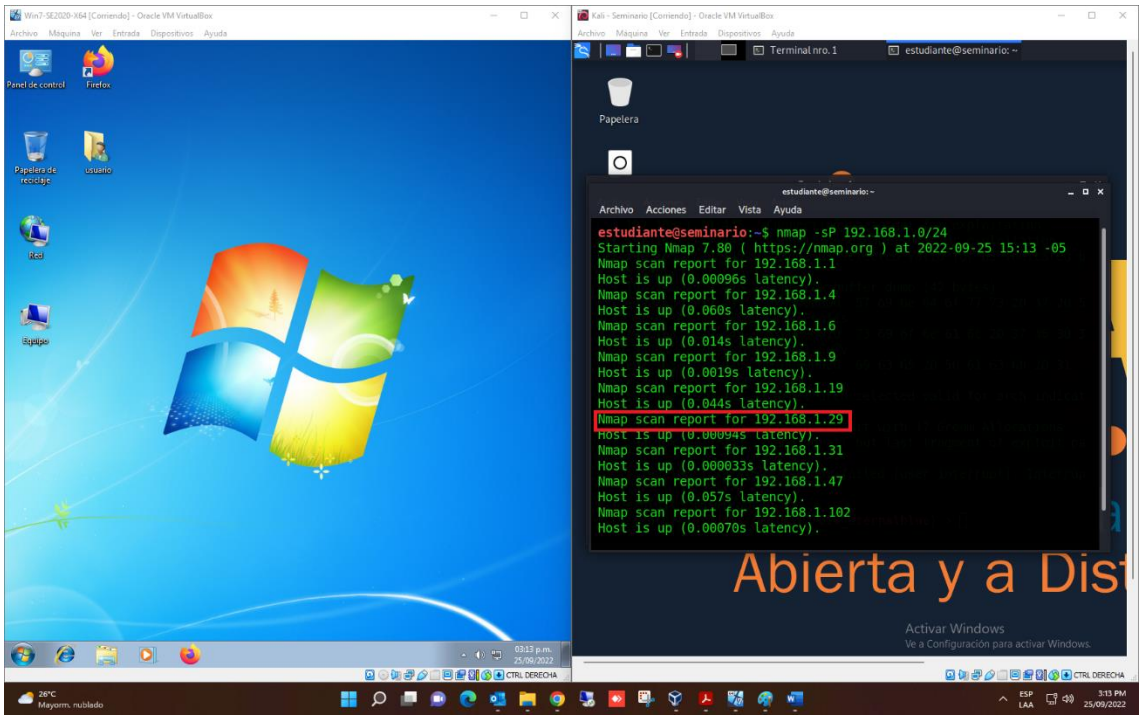


Fuente: Autor del documento

Nuevamente se realiza la recopilación de información del objetivo, usando la herramienta NMAP. Se ejecuta dicha herramienta y mediante el comando

“nmap -sP 192.168.1.0/24” se identifica cuales equipos dentro de esa red, se encuentran activos.

Figura 35. Identificación de hosts X64 activos sin Firewall de Windows



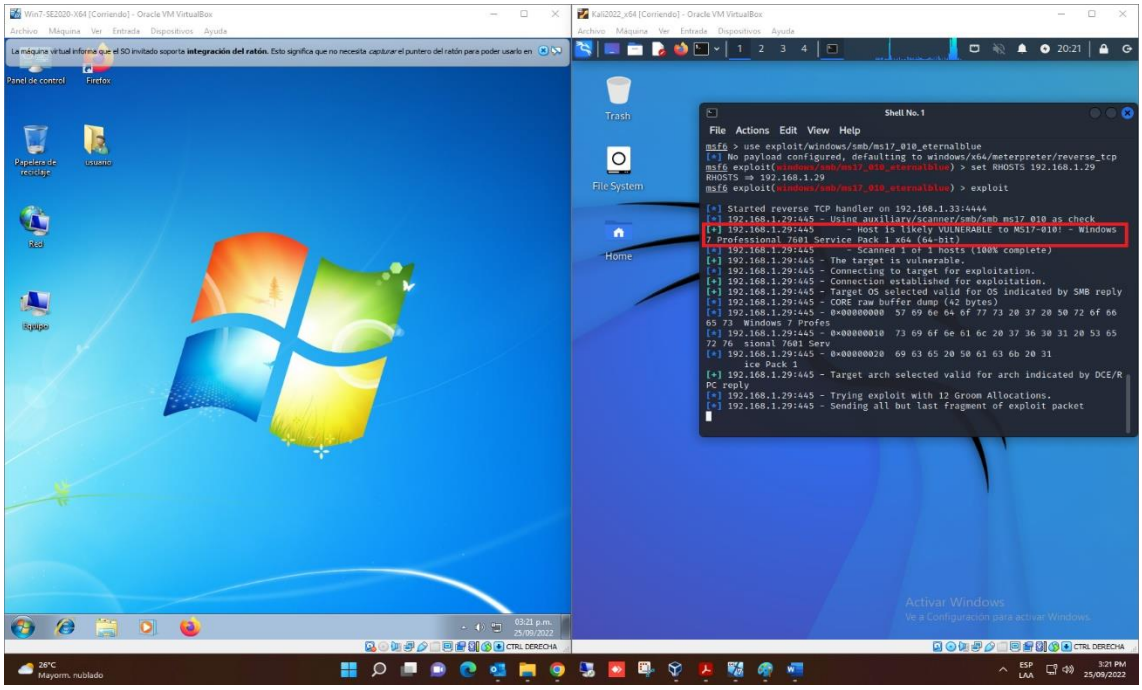
Fuente: Autor del documento

Como se puede apreciar en la figura anterior, debido a que el Firewall de la máquina Windows se encuentra inactivo, dentro de los hosts listados ahora sí se logra identificar que esta máquina se encuentra levantada y activa.

Lo siguiente es ejecutar el ataque del exploit “exploit/windows/smb/ms17_010_eternalblue”. Para no hacer repetitivo este documento, se omitirán los pasos de seleccionar el payload y la máquina objetivo, ya que esto se describió anteriormente.

La siguiente figura muestra el inicio del ataque a la máquina con dirección IP 192.168.1.29, cuyos primeros mensajes indican que el objetivo es vulnerable.

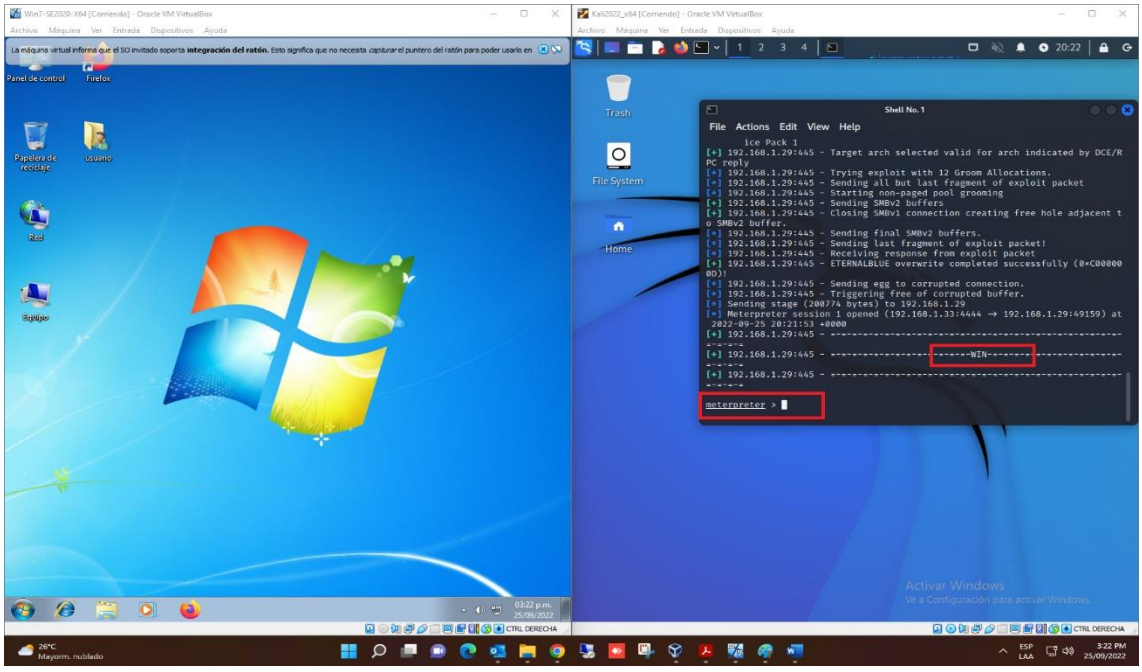
Figura 36. Ejecución de ataque a máquina X64 sin Firewall de Windows



Fuente: Autor del documento

Luego de unos minutos, el ataque es satisfactorio, y se logra establecer conexión remota a la máquina, como lo muestra la siguiente figura.

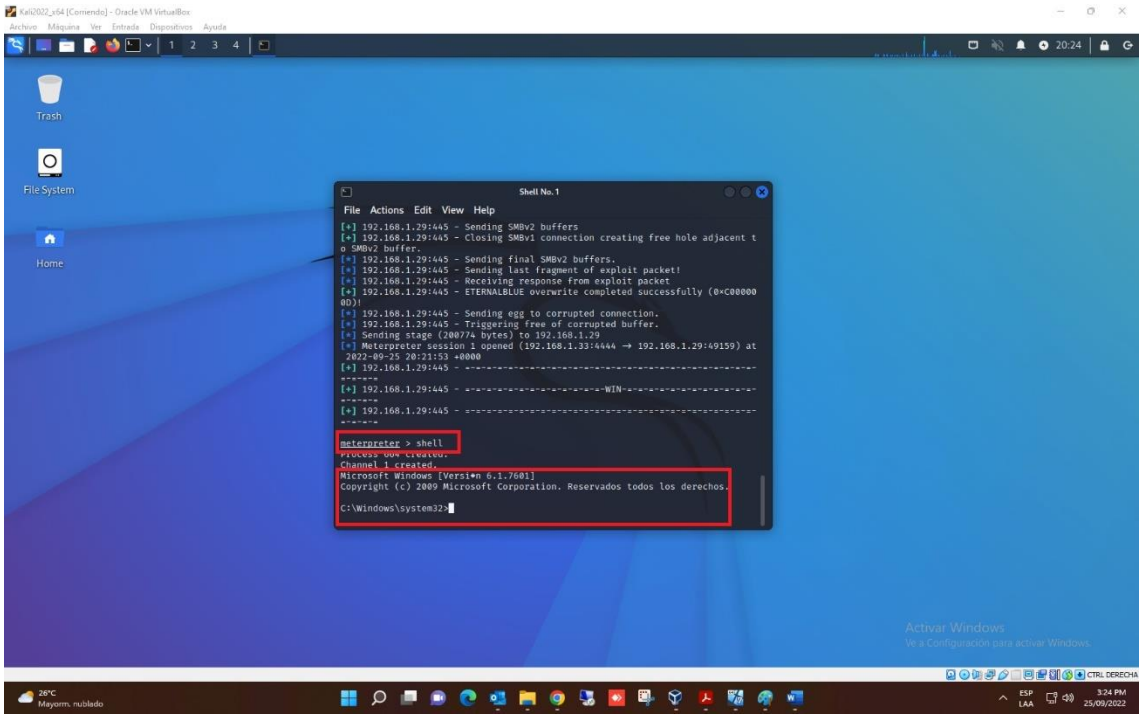
Figura 37. Resultado ataque máquina X64 sin Firewall de Windows



Fuente: Autor del documento

Lo siguiente, es ejecutar la consola de Windows. Para esto, se ejecuta el comando “shell”.

Figura 38. Ejecución de consola de comandos de Windows en ataque a CVE-2017-0144

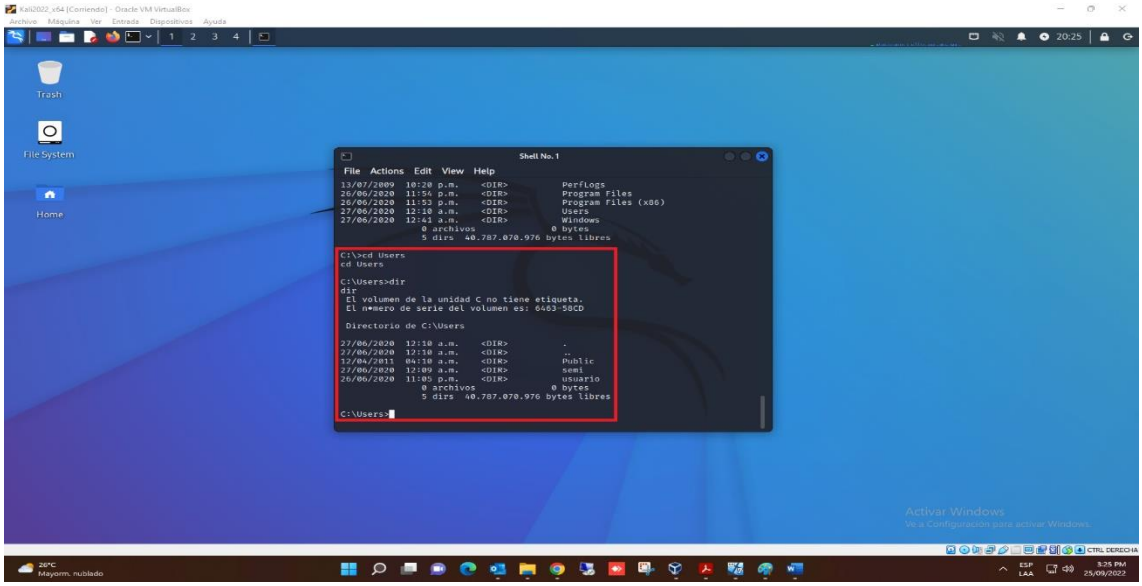


Fuente: Autor del documento

Como se observa, se logra el acceso a la consola de comandos de Windows, y se ubica por defecto en el directorio “Windows/system32”.

Ahora se buscará archivos que existan dentro de los usuarios del sistema de esta máquina. Para ello, se ingresa a la carpeta “users” dentro de la raíz del sistema, como lo muestra la siguiente figura.

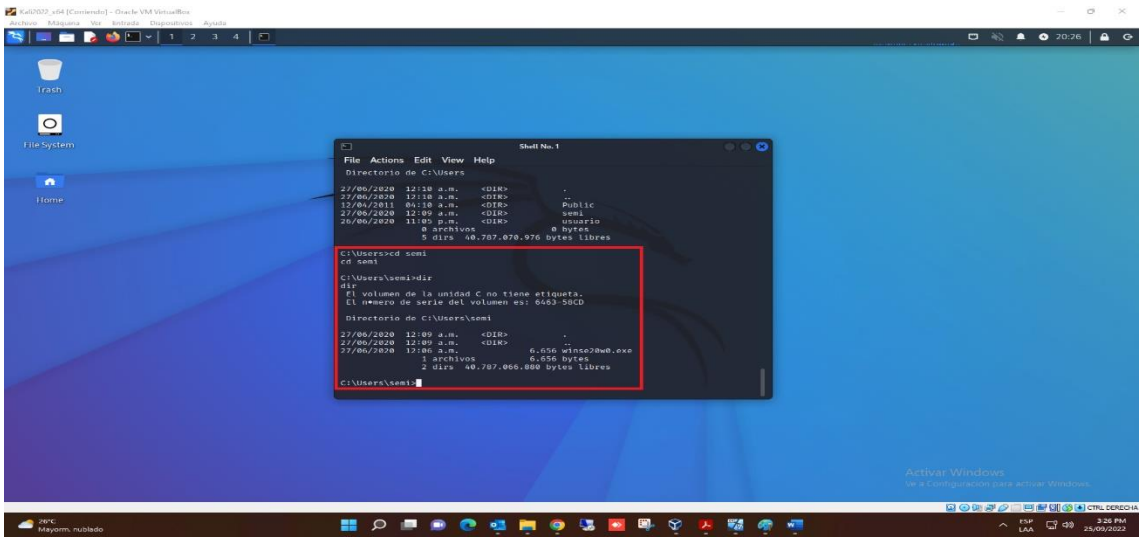
Figura 39. Listado de usuarios disponibles en máquina X64 a través de fallo CVE-2017-0144



Fuente: Autor del documento

Se logra identificar que existen 3 usuarios en el sistema: “public”, “semi” y “usuario”. Ahora se ingresa al directorio de archivos del usuario “semi”, con el comando “cd semi”, y posteriormente con el comando “dir”, se lista los archivos que se encuentran dentro de ese directorio.

Figura 40. Listado de archivos de usuario "semi" máquina X64 a través de fallo CVE-2017-0144

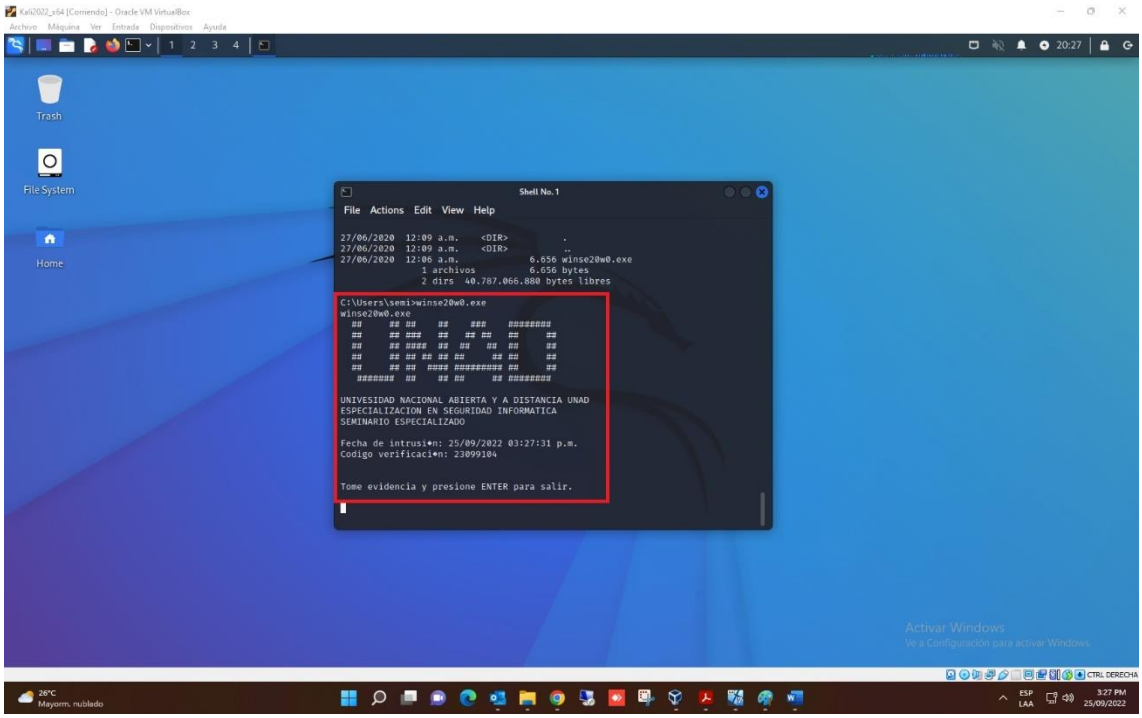


Fuente: Autor del documento

De la anterior figura se puede observar que existe un archivo personal llamado “winse20w0.exe”.

Para finalizar el ataque, se ejecuta dicho archivo dentro de la misma consola de comandos, como lo muestra la siguiente figura.

Figura 41. Ejecución de archivo en máquina X64 a través de fallo CVE-2017-0144



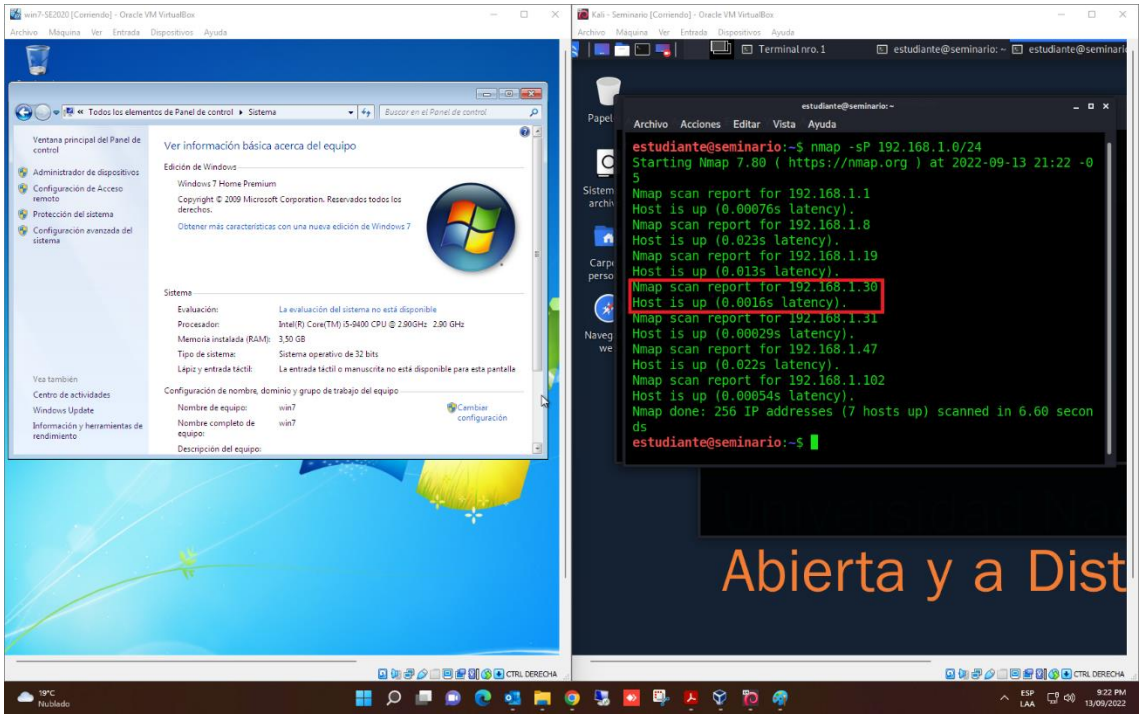
Fuente: Autor del documento

11.7 ATAQUE DE INTRUSIÓN A MÁQUINA WINDOWS 7 X86

Para realizar el ataque a la máquina con Windows 7 X86, se ejecutarán los mismos pasos o fases realizadas en el subcapítulo anterior.

En primer lugar, con NMAP, mediante el comando “nmap -sP 192.168.1.0/24” se realiza un escaneo de hosts para identificar qué equipos se encuentran levantados dentro de la red de área local.

Figura 42. Identificación de hosts X86 activos



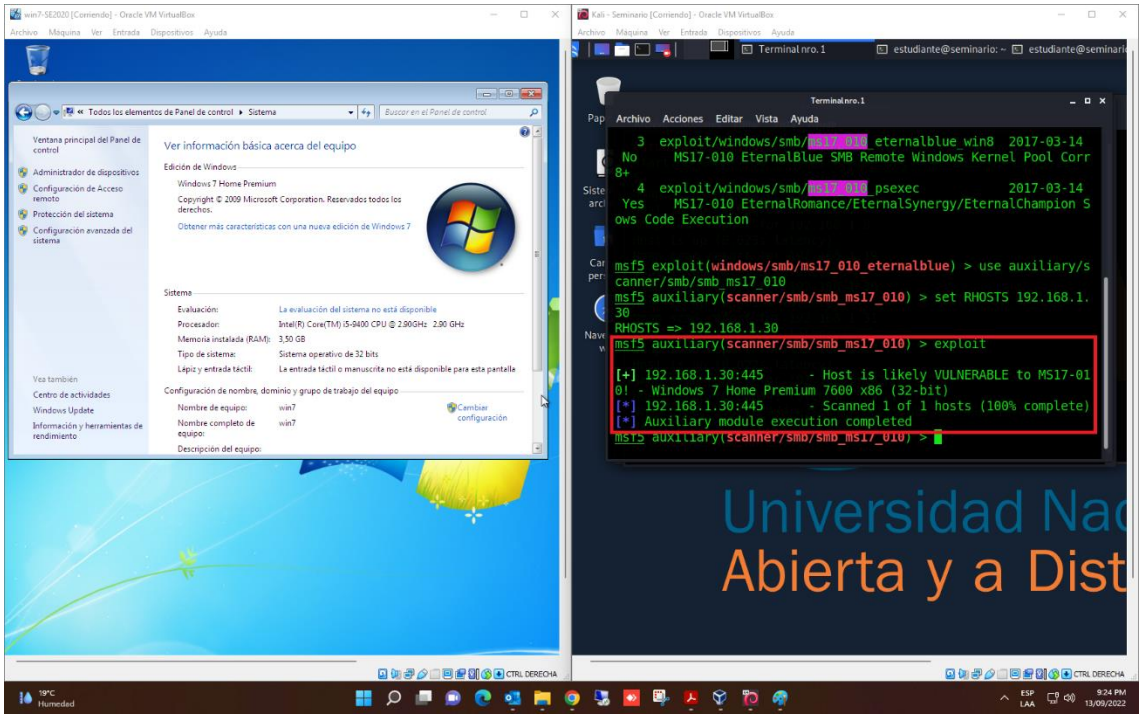
Fuente: Autor del documento

Como se puede observar, la máquina Windows 7 x86, la cual tiene como dirección IP 192.168.1.30, se encuentra activa. No hay un firewall bloqueando o rechazando paquetes.

Para no hacer muy extenso este documento, nuevamente se omitirán los pasos donde se efectúan los comandos para seleccionar los exploit y la dirección IP del objetivo, los cuales sí fueron descritos anteriormente.

Lo siguiente es ejecutar el ataque del exploit “auxiliary/scanner/smb/ms17_010_eternalblue” para identificar si el objetivo es vulnerable al fallo CVE-2017-0144.

Figura 43. Escaneo de vulnerabilidad a fallo CVE-2017-0144 máquina X86

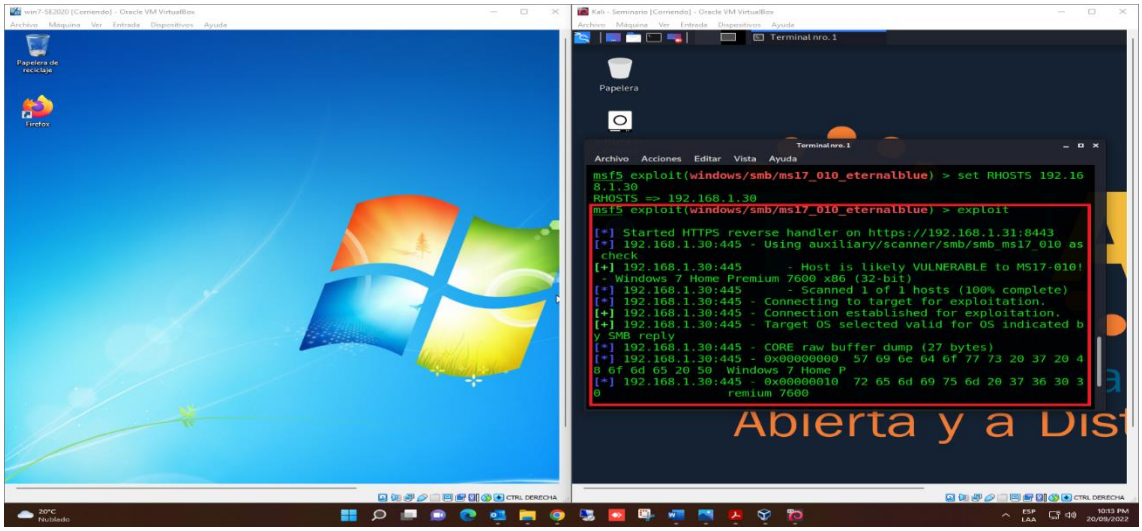


Fuente: Autor del documento

Como se puede observar, usando el puerto 445 en el host destino, metasploit logra identificar que la máquina objetivo probablemente es vulnerable, y además se logra establecer información adicional, como, por ejemplo, que es un Windows 7 Home Premium con arquitectura de 32bit.

En este punto, como se logró identificar que el objetivo es vulnerable a CVE-2017-0144, el siguiente paso es realizar el ataque principal, que consiste en lograr establecer conexión remota a la terminal de Windows a través del protocolo SMBv1 usando su puerto asignado por defecto (445), con el exploit “exploit/windows/smb/ms17_010_eternalblue”, como lo muestra la siguiente figura.

Figura 44. Ejecución de ataque al fallo CVE-2017-0144 máquina X86

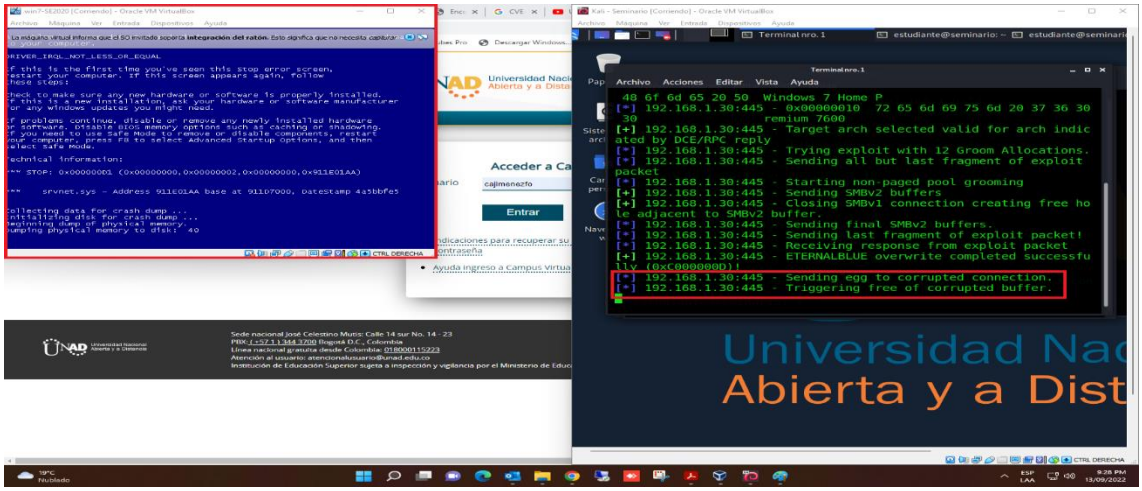


Fuente: Autor del documento

En la figura anterior se puede observar que se inició el ataque.

Unos segundos después, mientras el ataque sigue en progreso, en la máquina objetivo ocurre un error inesperado, saliendo un pantallazo azul que indica que ha ocurrido un desbordamiento de buffer, que hace reiniciar el sistema. Esto es un buen síntoma de que el ataque está siendo satisfactorio parcialmente, ya que se está afectando de manera negativa al objetivo.

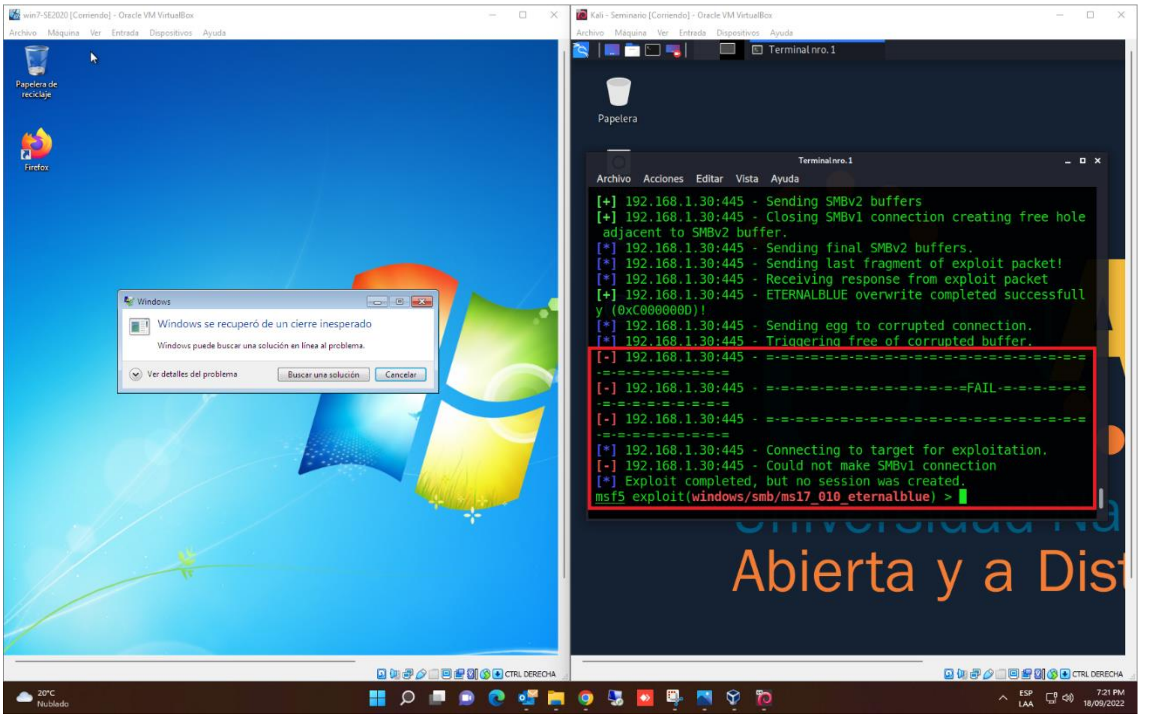
Figura 45. Desbordamiento de buffer ante ataque a CVE-2017-0144 máquina X86



Fuente: Autor del documento

La siguiente acción que debería suceder con el ataque, es que se logre establecer conexión con la terminal de comandos del objetivo. Sin embargo, como se puede evidenciar en la siguiente figura, esta conexión falla y no es satisfactoria.

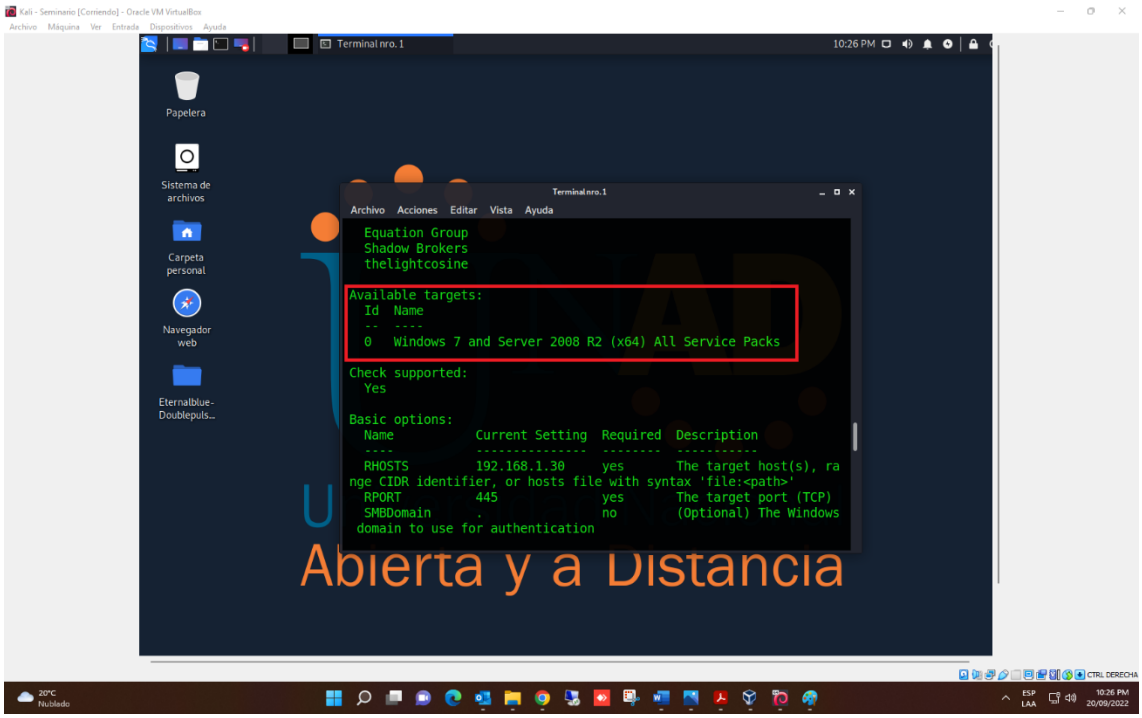
Figura 46. Ataque fallido a la vulnerabilidad CVE-2017-0144 máquina X86



Fuente: Autor del documento

No fue posible establecer la conexión remota, o completar el ataque, debido a que la máquina objetivo cuenta con arquitectura de 32 bit, y este exploit solo está disponible para atacar todos los Service Packs de Windows 7, pero bajo arquitectura de 64 bits. Esto se puede comprobar ejecutando el comando “show info” en el exploit seleccionado, como lo muestra la siguiente figura.

Figura 47. Objetivos disponibles para atacar bajo el exploit eternalblue



Fuente: Autor del documento

Por último, es preciso describir, que el protocolo que es vulnerado en este ataque, es el SMB (Server Message Block) cuyo puerto por defecto es el 445. Este puerto es usado comúnmente para servicios de compartición de impresoras o intercambio en archivos en red.

12 ANÁLISIS DE LAS EVIDENCIAS ENCONTRADAS EN EL ATAQUE DE INSTRUSIÓN ASOCIADO A LA SITUACIÓN PROBLEMA

Luego de realizar los ataques de intrusión a los equipos objetivo se logra identificar lo siguiente:

1) Mientras las máquinas se encuentren con el Firewall de Windows activo, o con la actualización “MS17-010”, no será posible que los atacantes logren vulnerar el fallo de seguridad CVE-2017-0144.
2) El fallo de seguridad CVE-2017-0144 aprovecha una vulnerabilidad de Windows en el protocolo SMBv1, a través del puerto 445, por el cual se establece compartimiento de impresoras y archivos entre diferentes equipos de cómputo.
3) El equipo de cómputo con Windows 7 X64 con el Firewall de Windows inactivo y sin la actualización de seguridad correspondiente, es vulnerable al fallo se seguridad CVE-2017-0144. Por tal motivo se encuentra generando una fuga de información, al permitir que los atacantes logren establecer conexión remota a la consola de comandos de Windows, y, por consiguiente, puedan ejecutar el archivo “winse20w.exe” y extraer la información allí almacenada.
4) El equipo de cómputo con Windows 7 X86 con el Firewall de Windows inactivo y sin la actualización de seguridad correspondiente, es igualmente, vulnerable al fallo se seguridad CVE-2017-0144. Cada vez que los piratas informáticos intenten atacar este equipo, se produce un desbordamiento de buffer, el cual hace que salga un pantallazo azul que reinicia el equipo. Este puede producir que los usuarios pierdan información de producción que no se haya guardado correctamente, antes de iniciado el ataque.
5) Se recomienda que, de manera inmediata, se active el Firewall de Windows, y se instale la actualización de seguridad MS17-010, tanto en

los equipos de 64 bits, como en los de 32 bits, para evitar seguir con la fuga y pérdida de información en la organización.

6) Se recomienda también, que, en la medida de lo posible, se migren los sistemas operativos de los equipos de cómputo de la organización, a un software superior, que tenga soporte por parte de Windows, para que constantemente se esté actualizando con los parches que lanza el fabricante para corregir fallos de seguridad, y no se presente lo que viene sucediendo en la empresa.

12.1 MEDIDAS DE HARDENIZACIÓN PARA MITIGACIÓN DEL ATAQUE A LA ORGANIZACIÓN HACKERS SECURITY

Con el objetivo de que el ataque a la vulnerabilidad CVE-2017-0144 no vuelva a ocurrir en la organización Hackers Security, se pueden tomar medidas de endurecimiento tanto a nivel de red, como a nivel de sistema operativo, las cuales se presentan a continuación.

Para el nivel de red se proponen las siguientes actividades:

- Instalación y configuración adecuada de un Firewall que permita, bloquee o rechace tráfico de red, desde o hacia internet, a través del cierre de puertos que no se usan y apertura de los puertos estrictamente necesarios para los servicios de red de la organización.
- Instalación y configuración de Dispositivos de Detección de Intrusos (IDS) con el objetivo que avisen al CSIRT, posibles anomalías dentro de la red corporativa, en tiempo real.

Para el nivel de sistema operativo se proponen las siguientes actividades:

- En primer lugar, en la medida de lo posible, actualizar los sistemas operativos Windows 7, a una versión superior que cuente con soporte por parte de Microsoft, para que los equipos puedan adquirir actualizaciones de seguridad periódicamente. Una versión recomendable es Windows 10, debido a que el soporte para Windows 8

y 8.1, que es la versión inmediatamente siguiente, finaliza en enero de 2023.[19]

- Instalar en los equipos pertinentes, todas las actualizaciones de seguridad disponibles para el sistema operativo Windows 7, a través de la herramienta Windows Update.
- Instalar en todos los equipos un antivirus que se encargue de detectar, bloquear y eliminar actividades maliciosas en los hosts.
- Activar el Firewall de Windows en todos los equipos de la organización, con el objetivo que este permita o bloquee tráfico de red por puertos específicos, como también permita o bloquee la ejecución de ciertas herramientas instaladas en el host.

12.2 ¿QUÉ SERÍA LO PRIMERO QUE INDAGARÍA Y HARÍA SI LLEGARA A ENCONTRARSE UN ATAQUE EN TIEMPO REAL?

No existe en el mundo de la ciberseguridad una protección 100% efectiva ante los diferentes ataques informáticos, es por tal motivo, que se considera que algo igual, o tal vez más importante que construir un gran “bunker” de seguridad que podría ser vulnerado en cualquier momento, es estar preparados para responder lo más rápido que se pueda, aprender y corregir.

Lo primero es identificar el ataque. Para esto existen dispositivos capaces de detectar tráfico malicioso o intrusos en la red de la organización, llamados comúnmente Dispositivos de Detección de Intrusos (IDS). Estas herramientas monitorean constantemente un host o una red completa, con el objetivo de detectar anomalías y alertar al oficial de seguridad, que está ocurriendo algo extraño para que actúe.

[19] MICROSOFT. [Sitio Web]. Windows 8 and Windows 8.1 end of support and Office. [Consultado: 01 de octubre 2022]. Disponible en internet: https://support.microsoft.com/en-us/office/windows-8-and-windows-8-1-end-of-support-and-office-34e28be4-1e4f-4928-b210-3f45d8215595#:~:text=Windows%208%2C%20Windows%208.1%2C%20and%20other%20versions%20of%20Office&text=The%20same%20will%20be%20true,to%20a%20supported%20operating%20system.

Si no se le logró contener a tiempo el ataque, y ya existen equipos afectados, lo mejor es desconectar las áreas protegidas y que aún no están infectadas, esto quiere decir que hay que sacarlas de la red, ya que, si siguen conectadas, la probabilidad de infectarse va a ser mayor. Así mismo, sacar de la red todo tipo de información valiosa y crítica de la organización.

Lo siguiente es establecer una cuarentena en todas las áreas de la organización, con el objetivo de aislar la amenaza o el virus, esto quiere decir, que todo equipo que esté infectado o del que se tenga sospecha, no debe ser conectado nuevamente a la red, hasta asegurarse que está completamente limpio de amenazas.

Una vez aislado el virus, se debe utilizar software especializado tales como antivirus, para detectar y limpiar los equipos, para posteriormente restablecer la información según lo indique la política de copias de seguridad establecida en la organización.

Luego de todo esto, procede realizar una investigación forense con el objetivo de identificar si la amenaza se materializó con un origen interno o externo, establecer las vulnerabilidades pertinentes, y corregir para que no vuelva a suceder.

13 CONCLUSIONES

Luego de realizar las actividades del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, se puede concluir que:

La normatividad vigente que se aplica en Colombia en torno a delitos informáticos, es la ley 1273 de 2009, la cual tipifica los tipos de delitos, describiendo las sanciones penales y económicas a las que se debe someter quien los cometa.

El pentesting o ataque de intrusión, es una actividad que se realiza en las organizaciones con el objetivo de mantener la seguridad de sus activos informáticos y la información que allí se almacena. Si se realiza una buena aplicación de cada una de sus etapas, el resultado será la identificación de vulnerabilidades que puedan afectar a la empresa, y por tal motivo, tomar medidas de mitigación evitando la posible materialización de ataque informáticos reales.

A través de un ataque de intrusión satisfactorio, se logró comprobar, que la vulnerabilidad CVE-2017-0144, es un fallo que permite a los ciberatacantes, establecer una conexión remota a la consola de comandos Windows, aprovechándose de un fallo en el protocolo SMBv1 de los sistemas operativos Windows, y por consiguiente sería amenaza grave debido a que un escenario real una organización podría tener fuga de información o en el peor de los casos modificación o eliminación de datos.

Para minimizar la materialización de estos ataques, es importante que las organizaciones cuenten con un correcto plan de actualizaciones de los sistemas operativos de los hosts, contar con firewalls de red y de aplicación que bloqueen tráfico de red y aplicaciones maliciosas, acompañado de un buen

plan de concientización y capacitación en medidas de seguridad informática desde el rol de cada uno de los empleados de la empresa.

14 RECOMENDACIONES

En el momento que se está materializando un ataque informático, una de las primeras acciones que de sebe tomar, es evitar que se siga propagando la amenaza, desconectando de la red los computadores que no estén infectados, para de esa manera lograr aislar el virus. Los equipos de respuesta ante incidentes informáticos, son los encargados de apropiarse y resolver con el mínimo impacto la materialización de un incidente de estos.

Sin embargo, para evitar lo anterior, es recomendable establecer medidas de hardenización en las organizaciones, instalando herramientas de contención como por ejemplo firewalls de red o de aplicación, antivirus, seguridad perimetral, y/o instalación de las actualizaciones de seguridad más recientes de los sistemas operativos. Esto es función de los equipos azules, ya que estos se encargan de analizar y evaluar la infraestructura de la organización, para proponer una serie de medidas correctivas necesarias para que no se materialice una amenaza.

BIBLIOGRAFÍA

ALCALDÍA MAYOR DE BOGOTÁ. [Sitio Web]. Ley 1273 de 2009. [Consultado: 30 de agosto 2022]. Disponible en internet: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

CENTER FOR INTERNET SECURITY. [Sitio Web]. The 18 CIS Critical Security Controls. [Consultado: 01 de octubre 2022]. Disponible en internet: https://www.cisecurity.org/controls/cis-controls-list.

CIBERSEGURIDAD. [Sitio Web]. ¿Qué es cve? explicación de las vulnerabilidades y exposiciones comunes. [Consultado: 30 de agosto 2022]. Disponible en internet: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/.

COPNIA. [Sitio Web]. Ley 842 de 2003. Septiembre, 2003. [Consultado: 12 de septiembre 2022]. Disponible en internet: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003.

CVE. [Sitio Web]. CVE-2017-0143. [Consultado: 01 de octubre 2022]. Disponible en internet: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143.

DE LUZ, Sergio. Realiza escaneos de puertos con Nmap a cualquier servidor o sistema. [En línea]. Julio, 2022. [Consultado: 30 de agosto 2022]. Disponible en internet: https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/.

ENTER.CO. [Sitio Web]. Detrás de Buggly: la historia de la fachada Andrómeda. [Consultado: 12 de septiembre 2022]. Disponible en internet:

https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/.

HELPSYSTEMS. [Sitio Web]. ¿Qué es un SIEM?. Mayo, 2018. [Consultado: 01 de octubre 2022]. Disponible en internet: https://www.helpsystems.com/es/blog/que-es-un-siem.

IBM. [Sitio Web]. ¿Por qué es importante SIEM?. [Consultado: 01 de octubre 2022]. Disponible en internet: https://www.ibm.com/co-es/topics/siem.

LEYES.CO. [Sito Web]. Código Penal Artículo 418. Revelación de secreto. [Consultado: 12 de septiembre 2022]. Disponible en internet: https://leyes.co/codigo_penal/418.htm#:~:text=Art%C3%ADculo%20418.,del%20empleo%20o%20cargo%20p%C3%BAblico.

INFOSECMATTER. [Sitio Web]. MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit. [Consultado: 19 de septiembre 2022]. Disponible en internet: https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/smb/ms17_010_psexec.

LOGRHYTHM. [Sitio Web]. Security Information and Event Management (SIEM). [Consultado: 01 de octubre 2022]. Disponible en internet: https://logrhythm.com/solutions/security/siem/.

MANAGE ENGINE. [Sitio Web]. ¿Qué son y cómo implementar los Controles de CIS (CIS Controls)?. [Consultado: 01 de octubre 2022]. Disponible en internet: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html.

MICROSOFT. [Sitio Web]. Windows 8 and Windows 8.1 end of support and Office. [Consultado: 01 de octubre 2022]. Disponible en internet: https://support.microsoft.com/en-us/office/windows-8-and-windows-8-1-end-of-

support-and-office-34e28be4-1e4f-4928-b210-3f45d8215595#:~:text=Windows%208%2C%20Windows%208.1%2C%20and%20other%20versions%20of%20Office&text=The%20same%20will%20be%20true,to%20a%20supported%20operating%20system.

MONTERO, Victor. Técnicas del Penetration Testing. [En línea]. Septiembre, 2005. [Consultado: 30 de agosto 2022]. Disponible en internet: http://www.cybsec.com/upload/VictorMontero-SeminarioTecnicasdelPenetrationTestingArgentina.pdf.

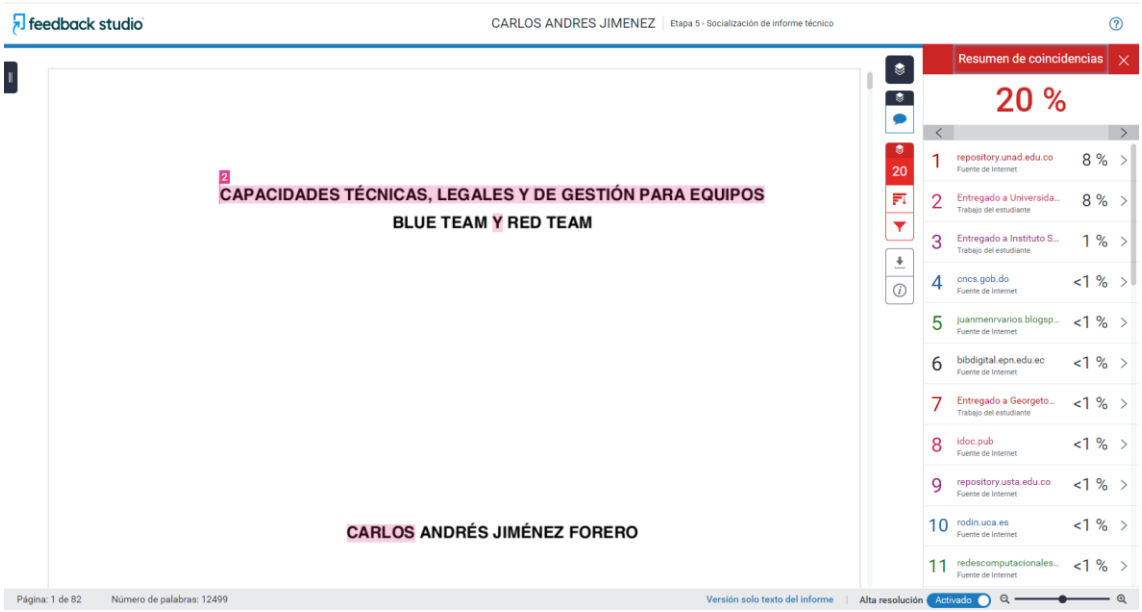
PATHACK, Amrita. Las 11 mejores herramientas SIEM para proteger a su organización de ciberataques. [En línea]. Septiembre, 2022. [Consultado: 01 de octubre 2022]. Disponible en internet: https://geekflare.com/es/best-siem-solutions/.

RIZALDOS, Héctor. Qué es Metasploit framework. [En línea]. Octubre, 2018. [Consultado: 30 de agosto 2022]. Disponible en internet: https://openwebinars.net/blog/que-es-metasploit/

TECNOLOGIA+INFORMATICA. [Sitio Web]. Que es un Antivirus? Definición. [Consultado: 01 de octubre 2022]. Disponible en internet: https://www.tecnologia-informatica.com/que-es-un-antivirus-como-funciona/.

VERA, Rafael. Qué es OpenVAS. [En línea]. Noviembre, 2020. [Consultado: 30 de agosto 2022]. Disponible en internet: https://openwebinars.net/blog/que-es-openvas/.

Anexo A. Prueba anti plagio



Enlace video sustentación: https://drive.google.com/file/d/1SnihjJs67CmAHjCh4NCPxbefEYayv_4F/view?usp=sharing

https://mega.nz/file/uE1BDbrZ#EKPczycljhkS0aY6BVMzPQP5eSgH8n8aT5kEp9_y4yc