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

JHONATAN FERNANDO VEGA CALDERON

UNIVERSIDAD NACIONAL A BIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
FLORENCIA - CAQUETA
ABRIL DE 2023

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

JHONATAN FERNANDO VEGA CALDERON

Trabajo de momento final etapa 5 del seminario especializado para optar al título de Especialización de Seguridad Informática

JOHN FREDDY QUINTERO
DIRECTOR DEL CURSO

UNIVERSIDAD NACIONAL A BIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
FLORENCIA - CAQUETA
ABRIL DE 2023

TABLA DE CONTENIDO

TABLAS

ILUSTRACIONES

1. RESUMEN

El presente documento se expone como un resumen del momento final de la etapa 5 de los equipos de seguridad del seminario especializado de Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team en donde se encuentran los detalles de la Guía de Actividades y Rubrica inicial.

La seguridad informática en el marco de la ciberseguridad demarca todos los esfuerzo, alcances y mitigación de riesgos para lograr la integridad de la información de una organización, por este motivo en esta actividad lograremos identificar la normatividad vigente y los casos legales de contratación indebida, además del análisis de los casos más importantes de seguridad digital en la historia de Colombia.

2. INTRODUCCION

Actualmente nos encontramos en el crecimiento acelerado de un mundo globalizado y más competitivo, el cual la ciberseguridad es la tendencia que determina nuevos desafíos empresariales en la búsqueda alternativas para obtener unas acciones sostenibles en el tiempo. La información, así como los equipos de cada entidad, se están viendo amenazados por vulnerabilidades de seguridad, ataques y delitos informáticos, problemas de violaciones, virus informáticos y cualquier otro tipo de contingencias, eventualidad y grandes catástrofes, con el objetivo de eliminación, interceptación, captura y pérdida de información.

Las leyes vigentes de protección de la información y de los datos en Colombia, establecen normas y comportamientos específicos para ayudar a proteger la seguridad digital de una organización, protegiendo el acceso abusivo, la obstaculización ilegítima, la interceptación de datos, el daño Informático, el uso de software malicioso, la violación de datos personales, la suplantación de sitios web para capturar datos personales, la circunstancias de agravación punitiva, el hurto por medios informáticos y semejantes y la transferencia no consentida de activos en un sistema informático.

La industria y las ciencias cada día proyecta las diferentes tecnologías emergentes para avanzar a pasos agigantados hacia una era vanguardista en donde la información se consolida como el activo más importante dentro de todo el contexto operacional de las transacciones y procesos en el mundo, sin duda alguna aunque existen muchos estudios y avances, el gran reto es la adopción correcta de soluciones digitales que permitan al individuo proteger su información, para esto es necesario tener en cuenta que la vulnerabilidades deben ser identificadas y normalizadas a nivel mundial con el fin de tener herramientas que prevengan los ataques cibernéticos.

3. GLOSARIO

Leyes: Es la máxima acción constitucional, emanada por el congreso de la república para llevar el control de la conducta de los ciudadanos establecida con carácter permanente.

Delitos informáticos: Es la acción que viola la seguridad de los entornos digitales de manera local ó remota, ocasionando la interrupción de las leyes informáticas.

Protección de datos personales: Es la acción de control de la información que permite mitigar el impacto negativo ante una explotación.

Ciberataque: Es la acción de eliminar, exponer, desestabilizar, destruir, alterar y obtener acceso sin autorización a las tecnologías de información.

Vulnerabilidad: Es una debilidad existente de los entornos físicos ó digitales, que puede ser utilizada para comprometer la seguridad.

Tipos de ataques cibernéticos: Algunos ataques en el mundo son: el Phishing, Spear Phishing, aplicaciones de malware, Whaling entre otros.

OWASP: Es un proyecto sin ánimo de lucro, el cual se encarga de definir e identificar vulnerabilidades a través guías de seguridad para la prevención de ataques cibernéticos en el mundo.

Pentesting: Es una prueba de penetración realizada para determinar vulnerabilidades críticas de los sistemas.

KaliLinux: Es un sistema operativo basado en Linux el cual contiene variedad de software para ejecutar pruebas de penetración de diferentes niveles de seguridad.

Reverse SHELL: Conexión que arranca en un servidor y que finalizad en un cliente, se utiliza para controlar un cliente hasta obtener credenciales con altos privilegios.

Máquina Virtual: Entorno digital de virtualización lógica para ejecución de sistemas operativos sobre maquinas físicas.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Establecer los criterios de aprendizaje del entorno de seguridad dentro de los equipos RedTeam y BlueTeam dentro del seminario especializado que permitan responder a las diferentes vulnerabilidades del mundo digital, preparando las acciones ante un inminente ataque cibernético en las empresas, además de la identificación de acciones propias y la competencia en el manejo de las conductas éticas para evitar acciones de infracción a las normatividades que atenten contra la seguridad de las tecnologías e información.

4.2. OBJETIVOS ESPECIFICOS

- Definir los Aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam..
- Definir las estrategias que contribuyen al trabajo de los equipos de RedTeam y BlueTeam
- Definir las estrategias que permiten endurecer los aspectos de seguridad de la información en la organización.
- Definir otras herramientas que permiten contener ataques informáticos
- Definir los aspectos legales a tener en cuenta por parte de los grupos de trabajo RedTeam y BlueTeam
- Sustentación del desarrollo del seminario mediante en un video mínimo 8 minutos.

5. DESARROLLO DEL INFORME

A continuación, se da la presentación del informe técnico que plasmará cada proceso de los escenarios propuesto en cada etapa ejecutada, en cual contiene los diferentes laboratorios que enumera según su etapa:

5.1. ETAPA 1: CONCEPTOS DE EQUIPOS DE SEGURIDAD

5.1.1. MARCO LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES.

La legislación colombiana en la actualidad cuenta con dos normatividades para mitigar los delitos informáticos y el apoyo a las organizaciones con el fin de no permitir impunidad a nivel nacional e internacional.

Tabla 1. Delitos y artículo de la Ley 1273 de 2009

Delito	Legislación
Acceso abusivo a un sistema informático	Artículo 269A, Sin autorización o por fuera de lo acordado; incurrirá en pena de prisión en (48) a (96) meses una multa de 100 a 1000 salarios mínimos legales mensuales vigentes
Obstaculización de un sistema informático o red de comunicaciones	Artículo 269B, Sin estar facultado para ello; incurrirá en pena de prisión en (48) a (96) meses una multa de 100 a 1000 salarios mínimos legales mensuales vigentes
Espionaje de datos informáticos	Artículo 269C, Sin orden judicial previa; Incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
Daño informático	Artículo 269D, Sin estar facultado para ello; incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Uso de software malicioso (Malware)	S Artículo 269E, in estar facultado para ello; incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Violación de datos personales	Artículo 269F, Sin estar facultado para ello; incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Suplantación de sitios web para la captura de datos personales	Artículo 269G, Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
Hurto por medios informáticos	Artículo 269I, Incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.
Transferencia no consentida de activos	Artículo 269J, Incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.
Infracciones por propiedad intelectual	Artículo 270 y 271, Especialmente la copia y distribución no autorizados, incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis puntos sesenta y seis (26.66) a mil (1.000) salarios mínimos legales mensuales vigentes

Fuente: El autor

Tabla 2. Comparativa de normas nacionales e internacionales.

Legislación	
Nacional	Internacional
• Art 269A, 269D, 269F ley 1273 de 2009 • Ley 1581 de 2012 Por la cual se dictan disposiciones generales	• Alemania: la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 • Austria:

para la protección de datos personales	Ley de reforma del Código Penal de 22 de diciembre de 1987 • Francia: Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático • Estados Unidos: Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) • Holanda: Ley de los Delitos Informáticos • Venezuela: Ley Especial contra los delitos Informáticos por Asamblea Nacional de la República Bolivariana de Venezuela • España: • Ley Orgánica de Protección de Datos de Carácter Persona • Ley de Servicios de la Sociedad de la Información y Comercio Electrónico • Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal • Ley General de Telecomunicaciones • Ley de Propiedad Intelectual • Ley de Firma Electrónica
• Art 269A, 269D, 269F, 269J ley 1273 de 2009 • Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales	
• Art 269A, 269D, 269F, 269J ley 1273 de 2009 • Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales	
• Ley 44 de 1993, Cap II art 6, Cap IV art 51. • Art 61Constitucion política de Colombia, Protección a la propiedad Intelectual. • Ley 23 1982 art, 1, 2 • Ley 599 de 2000 art 270, 271, 272. • Art 269A, 269D, 269F, 269J ley 1273 de 2009 • Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales	

5.1.2. ETAPAS DEL PENTESTING EN EL MUNDO DE LA CIBERSEGURIDAD

Las diferentes vulnerabilidades se deben identificar y se mitigar a través de las metodologías de penetración – Pentesting y sus etapas.

5.1.2.1. INFORMATION GATHERING

En esta etapa, se ejecuta la recolección de la información de la víctima, haciendo uso de diversas técnicas y herramientas automatizadas, algunas de ellas son: Nmap, Recon-ng, Dnsrecon, SubFinder y Dnsmap.

5.1.2.2. VULNERABILITY ANALYSIS

En esta etapa, se ejecuta las acciones posibles que permita comprometer a la víctima, la información y/o los usuarios. Algunas de las herramientas más utilizadas son: OWASP Zap Proxy, Nessus, BugBounty Recon, BurpSuite y Vega.

5.1.2.3. EXPLOITATION

En esta etapa, se ejecutan pruebas de intrusión a través de Exploits para aprovechar las vulnerabilidades con el fin de obtener acceso a los sistemas de la víctima. Algunas de las herramientas más usadas son: Metasploit Framework, OpenVAS, Nessus, BeEF, BurpSuite, SQLMap, Xarp, Canvas, Routersploit, SPARTA y PowerSploit.

5.1.2.4. POST EXPLOITATION

Esta etapa, es opcional. Se ejecuta para escalar altos privilegios sobre el sistema de la víctima. Algunas de las herramientas son las siguientes: Enumdb, Mimikatz, Poet, AutoSploit, GhostPack, Metasploit, RemoteRecon, Pwnat, Arpag, ShellPop, TheFatRat y Empire.

5.1.2.5. REPORTING

Es la última etapa, es donde se detalla y se reportan los hallazgos dentro de las pruebas de penetración - Pentesting. Algunas de las herramientas utilizadas para elaborar informes de vulnerabilidades son: Dradis, Faraday y Simple Vulnerability Manager.

5.1.3. DEFINICION DE HERRAMIENTAS DE CIBERSEGURIDAD

Para continuar, se define algunas herramientas para la exploración de vulnerabilidades de seguridad digital, las cuales son las siguientes:

- Nmap: Es una herramienta para exploración y auditoría de seguridad de las redes..

- OpenVas: Es un Framework que integra herramientas y servicios para escaneo y gestión de vulnerabilidades de seguridad.

- Metasploit: Es una herramienta que permite testear vulnerabilidades, ejecutar ataques con la ayuda de la metodologías y etapas del "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

- CVE: Es el portal que publica y controla el histórico de la lista de vulnerabilidades de seguridad conocidas en el mundo, con el fin de determinar la posible solución al fallo ó como mitigar la vulnerabilidad.

- ExploitDB: Es la database de exploits y es utilizada para la seguridad pública con el fin de identificar posibles vulnerabilidades en la red con actualizaciones de los ataques actuales que ocurren en todo el mundo.

5.1.4. CONFIGURACION DE BANCO DE TRABAJO – ANEXO 1

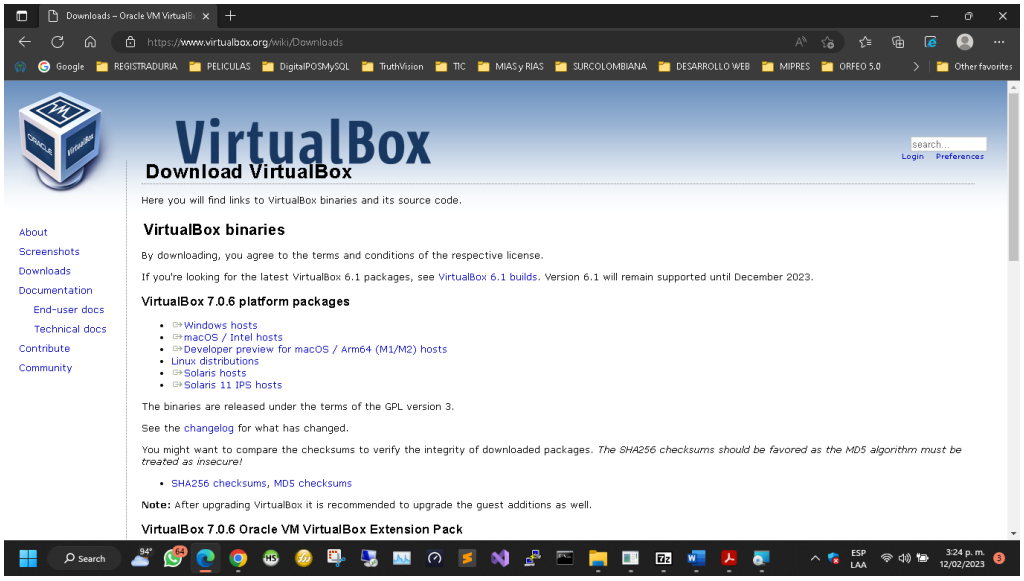
Para finalizar esta actividad es importante que usted reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1

– Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1 - escenario 1 es lo siguiente:

- **Paso A**: Descargar la herramienta virtualizadora “VirtualBox” en su última versión(7.0.6-155176).

Se realiza la descarga del aplicativo desde la fuente oficial de Oracle.

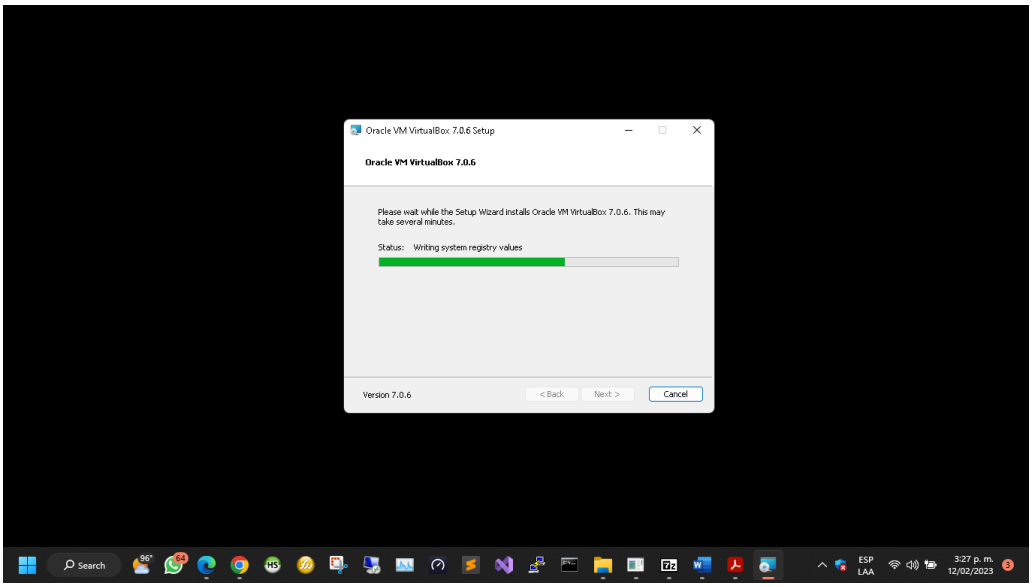
Ilustración 1. Portal de Descarga de VirtualBox



Fuente: https://www.virtualbox.org/wiki/Downloads

Se procede a realizar la instalación en Win11 x64 con la versión de arquitectura requerido para el paquete descargado.

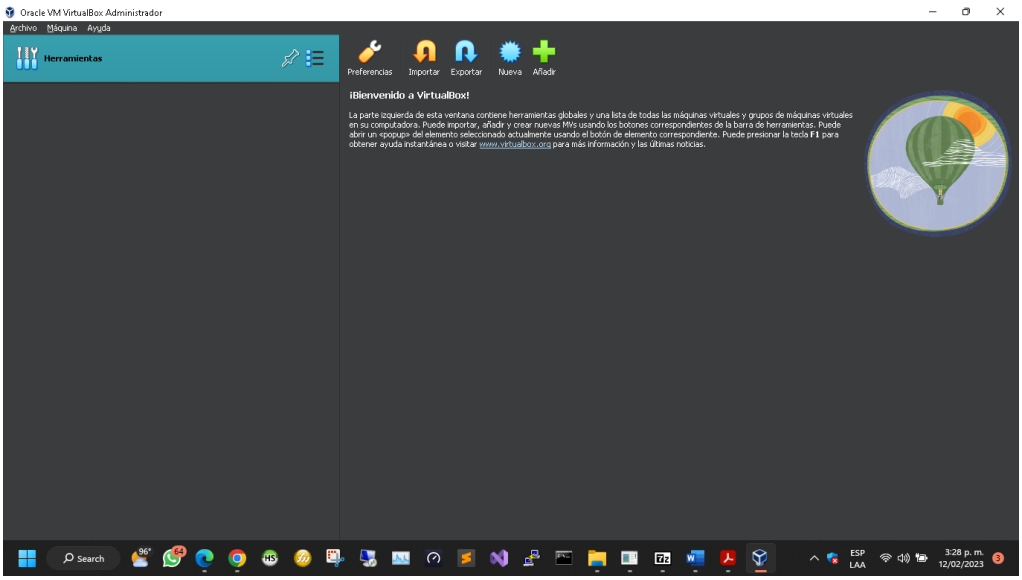
Ilustración 2. Instalación de VirtualBox-7.0.6-155176-Win_X64.exe



Fuente: Implementación en equipo personal

Se comprueba que la herramienta queda instalada de manera correcta, además se instala el paquete de extensión Oracle_VM_VirtualBox_Extension_Pack-7.0.6a-155176.vbox-extpack.

Ilustración 3. Inicio de VirtualBox después de instalarlo.



Fuente: Implementación en equipo personal

5.2. ETAPA 2: ACTUACIÓN ETICA Y LEGAL

5.2.1. ¿UNA VEZ LEÍDO EL ANEXO 2 – ESCENARIO 2 Y EL ANEXO 3 – ACUERDO USTED LOGRA EVIDENCIAR ALGÚN PROCESO ILEGAL Y NO ÉTICO QUE SE ESTÉ ESTIPULANDO EN DICHO ACUERDO? DEBERÁ ARGUMENTAR SU RESPUESTA Y SEÑALAR LOS FRAGMENTOS ILEGALES DEL ANEXO ACUERDO EN CASO DE EXISTIR ALGUNA IRREGULARIDAD.

De acuerdo a análisis del documento Acuerdo de Confidencialidad de la empresa WhiteHouse Security el cual pretender establecer unos procedimientos que no son éticos e ilegales que según el código de ética del COPNIA a través de la Ley 842 de 2003[1] establece sus artículos determinan los deberes y obligaciones generales de los profesionales, entre los que se encuentra:

(f) Denunciar los delitos, contravenciones y faltas contra este Código de Etica, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder.

b) Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones.

Por consiguiente, el acuerdo de confidencialidad presenta actuaciones ilegales que involucran la ética de los profesionales de ingeniería en los siguientes fragmentos:

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 ó de sus subalternos o funcionarios, autoridades legales, asesores ó cualquier persona relacionada con ella, la información confidencial o* ***sobre procesos ilegales*** *dentro de Whitehouse Security no podrán ser divulgados.*"[2]

Segunda. Definición de información confidencial:

[1] Ley 842 (2003). Establece que los Ingenieros, Profesionales afines y auxiliares, actúen con compromiso y honestidad con el fin de brindar un ejercicio ético de su profesión. https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

[2] Anexo 3 (Página 2). Acuerdo de confidencialidad entre Estudiante y whitehouse security. https://campus107.unad.edu.co/ecbti116/pluginfile.php/5613/mod_folder/content/0/Anexo 3 - Acuerdo.pdf?forcedownload=1

"*2. 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**"*[3]

Cuarta. Obligaciones de la parte receptora:

"*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]

"*4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.*"[5]

"*9. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security."*[6]

Quinta. Obligaciones de la parte reveladora:

"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 Whitehouse Security."

[3] Anexo 3 (Página 3). Acuerdo de confidencialidad entre Estudiante y whitehouse security. https://campus107.unad.edu.co/ecbti116/pluginfile.php/5613/mod_folder/content/0/Anexo 3 - Acuerdo.pdf?forcedownload=1

[4] Anexo 3 (Página 4). Acuerdo de confidencialidad entre Estudiante y whitehouse security. https://campus107.unad.edu.co/ecbti116/pluginfile.php/5613/mod_folder/content/0/Anexo 3 - Acuerdo.pdf?forcedownload=1

[5] Anexo 3 (Página 4). Acuerdo de confidencialidad entre Estudiante y whitehouse security. https://campus107.unad.edu.co/ecbti116/pluginfile.php/5613/mod_folder/content/0/Anexo 3 - Acuerdo.pdf?forcedownload=1

[6] Anexo 3 (Página 4). Acuerdo de confidencialidad entre Estudiante y whitehouse security. https://campus107.unad.edu.co/ecbti116/pluginfile.php/5613/mod_folder/content/0/Anexo 3 - Acuerdo.pdf?forcedownload=1

Para concluir, se determina que la empresa WhiteHouse Security en su acuerdo está violando las leyes vigentes y pretenden librarse de toda responsabilidad en caso que los delitos sean denunciados.

5.2.2. SI LA RESPUESTA ES AFIRMATIVA Y USTED ENCONTRÓ ALGÚN PROCESO ILEGAL EN EL ANEXO 3 – ACUERDO, DEBERÁ MENCIONAR QUE ARTÍCULOS DE LA LEY 1273 SE PODRÍAN VULNERAR EN DICHO ACUERDO Y ESPECIFICAR PORQUÉ VULNERA ARTÍCULOS DE LA LEY 1273.

De acuerdo a la respuesta anterior que es afirmativa, se puede inferir que la empresa WhiteHouse Security en su acuerdo de confidencialidad está vulnerando la ética de los profesionales en ingeniería y atentando contra la ley 1273 de 2009[7] en sus artículos:

- Artículo 269A: Acceso abusivo a un sistema informático. En su artículo 3, del acuerdo de confidencialidad, que dice: "*…la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona ó de sus subalternos o funcionarios, autoridades legales, asesores ó cualquier persona relacionada con ella, la información confidencial o* ***sobre procesos ilegales*** *dentro de Whitehouse Security no podrán ser divulgados.*"

- Artículo 269C: Interceptación de datos informáticos. En su artículo 2, del acuerdo de confidencialidad, que dice: "*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****".*

- Artículo 269F: Violación de datos personales. En su artículo 3, del acuerdo de confidencialidad, que dice: "*No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."*

  Además de otras que se enuncian sobre delitos, por lo que teniendo en cuenta la normatividad, se determina un gran entorno ilegal de actividades que ponen en riesgo de condenas que van desde los 4 a 8

[7] Ley 1273 (2009). Se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos".
http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

años por cada delito cometido por el profesional de ingeniería que firme este acuerdo.

5.2.3. ¿EXISTIENDO PROCESOS POCO CONFIABLES EN EL ANEXO 3 – ACUERDO? ¿USTED COMO EXPERTO EN CIBERSEGURIDAD APLICARÍA A ESTE TRABAJO EN THE WHITEHOUSE, DONDE LA ORGANIZACIÓN DISPONE DE UN SUELDO DE $15.000.000 DE PESOS COLOMBIANOS MENSUALES Y CONTRATO VITALICIO? DEBE ARGUMENTAR SU RESPUESTA YA SEA AFIRMATIVA O NEGATIVA Y TENER EN CUENTA EN LA ARGUMENTACIÓN LO QUE SE DISPONE EN COPNIA EN SU CÓDIGO DE ÉTICA PARA INGENIEROS.

En conclusión, al análisis del Acuerdo de Confidencialidad de la empresa WhiteHouse Security en donde se determinan actuaciones como la interceptación indebida, violación de datos personales, acceso abusivo a los sistemas de información de terceros y la responsabilidad directa con la búsqueda de un abogado privado para la defensa, se establece que de acuerdo al código de Ética de COPNIA en concordancia con la Ley 842, como experto en ciberseguridad NO APLICARIA a este trabajo que tiene una oferta en dinero, estabilidad y competitividad muy favorable para un profesional en ingeniería en nuestra economía Colombia, debido a que estaría infringiendo las leyes 842 de 2003, 1273 de 2009 y 1581 de 2012 en materia de ética profesional, delitos informáticos y protección de datos en Colombia, acarreándome penas privativas de mi libertad y la suspensión de mi título para ejercer mi profesión.

5.2.4. DEBERÁ BUSCAR LA NOTICIA DEL CASO “OPERACIÓN ANDROMEDA BUGGLY” EN LA CIUDAD DE BOGOTÁ, Y REDACTAR SU PUNTO DE VISTA TENIENDO EN CUENTA LAS IMPLICACIONES LEGALES Y ÉTICAS QUE ALLÍ SE PUDIERON GENERAR.

De acuerdo al análisis del artículo Operación Andrómeda Buggly de la revista digital en la revista enter.co[8], se puede determinar que fue una operación en cubierto de la inteligencia militar el cual pretendía estudiar y controlar a las personas que tenía intereses por la ciberseguridad sin importar su nivel,

[8] Detrás de Buggly: la historia de la fachada Andrómeda (2015). Revista digital ENTER.CO. https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

creando una comunidad de hacker éticos que compartían los mismos intereses por la seguridad informática, su vulnerabilidad y la importancia de mitigar el impacto. Esta operación tenia todo el respaldo del gobierno nacional con su unidad de inteligencia para la seguridad nacional en los altos mandos del ejército nacional, el cual gozaba de financiación de dineros del estado que gozan de libertad de gastos sin reportarlos para brindar las actuaciones de seguridad. Lo cierto de este caso es que se manejaron actividades sin controles estrictos de seguimiento y control a cada persona que manipulaba información ó ejecutaba procesos de interceptaciones, ya que personal al servicio del estado violaron sus funciones y cometieron delitos al vender información clasificada y reserva dentro del proceso de inteligencia para la seguridad nacional. Queda claro que por primera vez en Colombia se da por descubierto la operación más importante de ciberseguridad nacional poniendo al estado a luz de la ciudadanía con sus procesos internos que dan lugar a investigaciones con ó sin autorización de la rama judicial que permita hacer uso de interceptaciones legales. Es preciso, determinar que la seguridad informática es un tema que requiere más atención en nuestro país, con la definición de protocolos y seguimientos seguros que garanticen la protección de datos y el seguimiento legal que ayude a la seguridad nacional, es de vital importancia que las entidades del estado evoluciones y generen institucional con líderes en estos temas que reconozcan la importancia y seguridad, teniendo en cuenta que los CIO ó CISO transitan una línea entre la legalidad e ilegalidad.

Sin embargo, queda una la realidad sin aclarar debido a que precisamente esta operación fue descubierta en una etapa de campañas políticas el cual fue utilizado al chivo espiratorio Hacker Sepúlveda en donde se volcó todos los medios de comunicaciones a generar una cortina de humo con las intenciones del gobierno actual del presidente Juan Manuel Santos para debilitar su poder y su apoyo político a su candidato que no era del Uribismo, a Sepúlveda se encontró directamente involucrado en la campaña del Uribista Oscar Iván Zuluaga. La pregunta queda, ¿será que el estado no tiene la capacidad para controlar sus operaciones de inteligencia y seguridad nacional ó será que si es un problema mediático político?, por el momento nos tocará seguir esperando que avancen las investigaciones.

5.3. ETAPA 3: EJECUCIÓN PRUEBAS DE INTRUSIÓN

5.3.1. DESCRIBA DE MANERA ESPECÍFICA LAS HERRAMIENTAS SOFTWARE QUE UTILIZÓ PARA LLEVAR A CABO EL ANEXO 4 – ESCENARIO 3 ENFOCADO A REDTEAM. DEBERÁ ADJUNTAR EVIDENCIA DE LOS COMANDOS UTILIZADOS Y RESULTADOS QUE ARROJÓ CADA

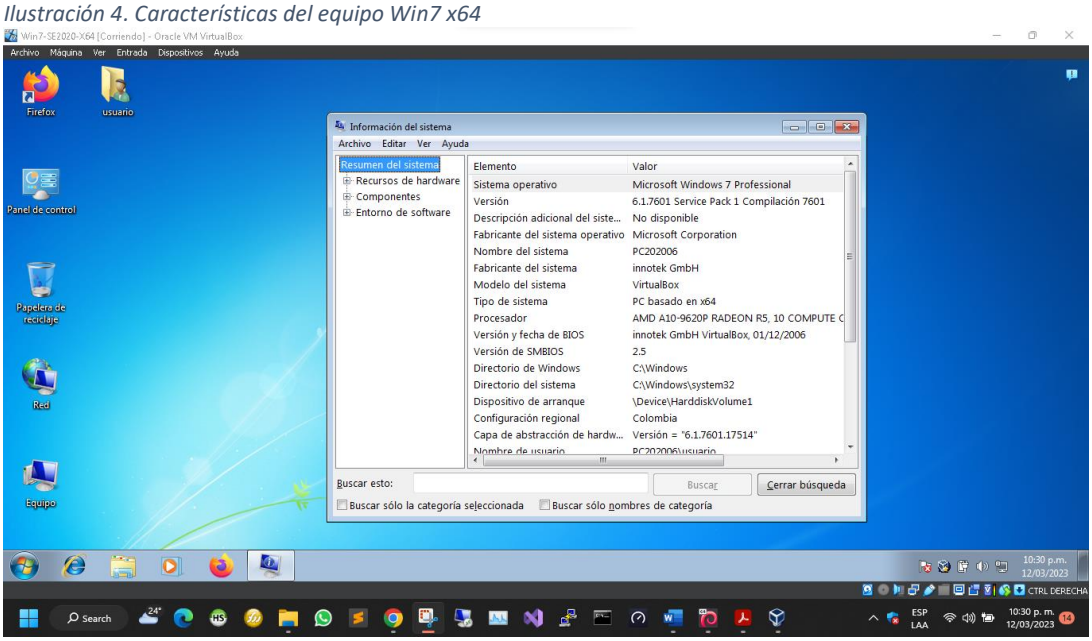
HERRAMIENTA UTILIZADA, ESTAS HERRAMIENTAS DEBEN ESTAR CLASIFICADAS SEGÚN LOS PASOS DE UN PENTESTING.

5.3.1.1. Fase de recolección de información:

Al iniciar esta fase, se identifica que este equipo tiene instalado el sistema operativo Windows 7 Pro SP1 6.1.7601.17514 con arquitectura x64 con nombre PC202006, el cual tiene instalado la aplicación Rejetto v2.3.

Es preciso resaltar que esta versión actualmente no cuenta con actualizaciones de seguridad por Microsoft desde enero de 2020, debido a que se acabo el periodo de soporte para esta versión y así dar paso a las siguientes versiones tales como 8, 8.1, 10 y 11.

Ilustración 4. Características del equipo Win7 x64

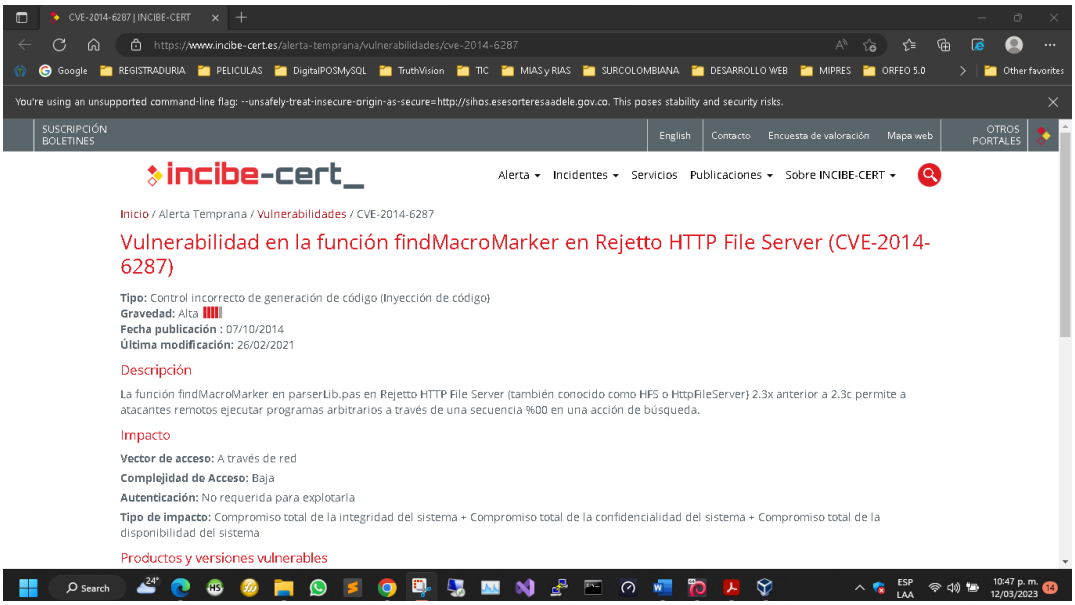


Fuente: Propia desde VirtualBox

5.3.1.2. Fase de Búsqueda de vulnerabilidades.

Dentro del anexo 4, se contempla que se cuenta con una aplicación, se investiga acerca de la aplicación Rejetto v2.3 que es un HTTP file server, es un servidor web host portable para compartir datos. Sin embargo, tiene vulnerabilidades findMacroMarker que permite a atacantes remotos iniciar softwares e inyectar códigos arbitrarios en secuencias de búsquedas.

Ilustración 5. Vulnerabilidad 2014-6287 (Rejetto v. 2.3)



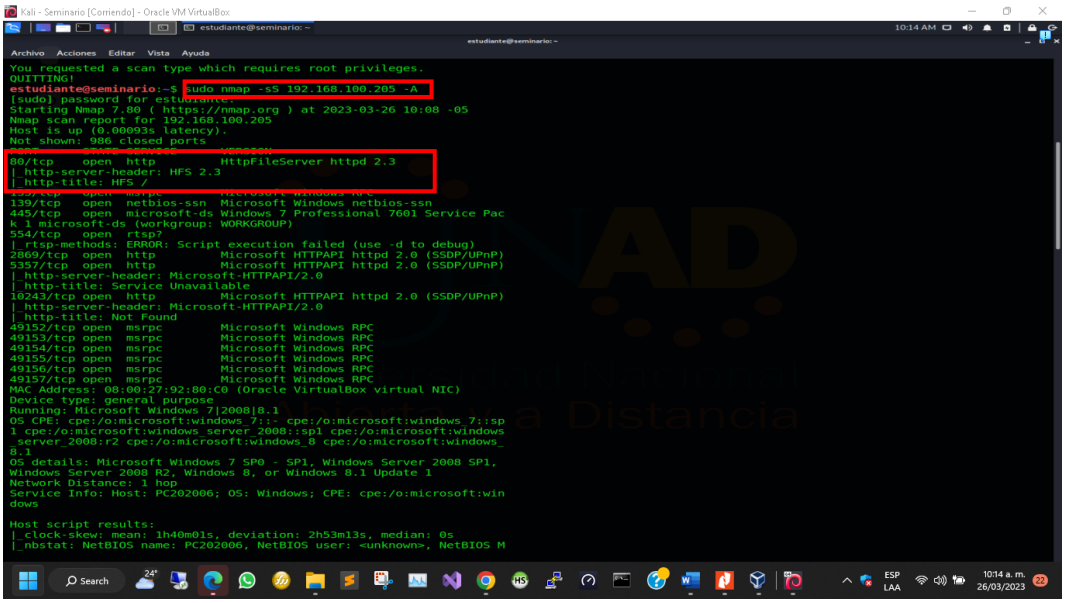
Fuente: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

5.3.1.3. Fase de Explotación de vulnerabilidades

Se inician las máquinas virtuales entregadas para el análisis, el cual cuenta con Windows 7 x64 (victima) con el software Rejetto v2.3 y una maquina con Kali Linux (atacante), los cuales se ejecutan sobre el mismo segmento de red 192.168.100.0/24, en donde se pretende localizar la vulnerabilidad y también interpretar la operación de este fallo de seguridad.

Al analizar el equipo de la víctima con Windows 7 x64 desde el equipo atacante con KaliLinux, procedemos a utilizar Nmap donde se identifica varios puertos abiertos los cuales pueden ser aprovechados para hacer acceso remoto a la dirección en Windows 192.168.100.205:

Ilustración 6, Escaneo puertos con Nmap a 192.168.100.205

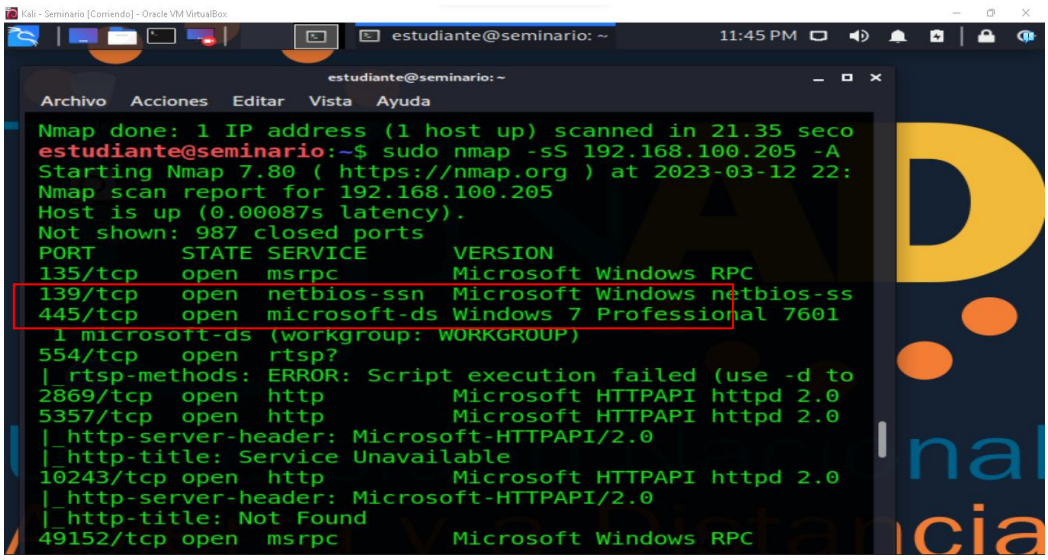


Fuente: KaliLinux

Con el siguiente comando, se logra identificar los puertos abiertos y el sistema operativo que se ejecuta en la máquina de la víctima:

sudo nmap -sS 192.168.100.205 -A

Ilustración 7. NMAP: Prueba y estado de puertos



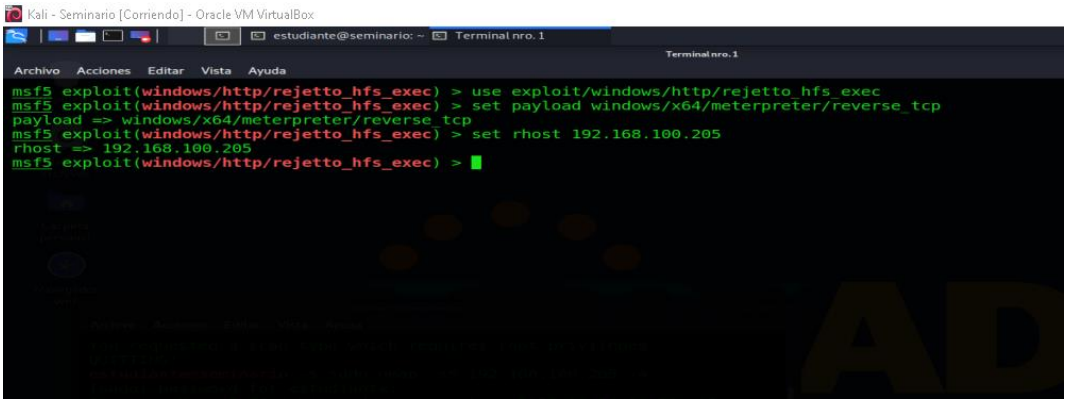
Fuente: KaliLinux

5.3.1.4. Fase Post-explotación

Se utiliza el exploit rejetto v2.3, se procede a iniciar los payload.

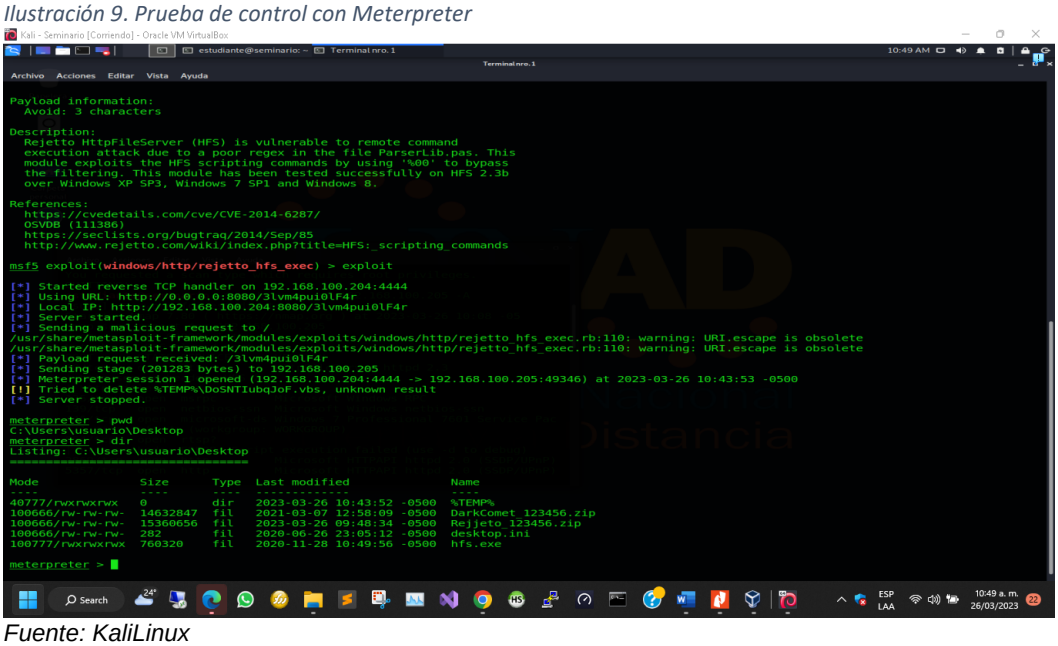
> use exploit/windows/http/rejetto_hfs_exec
> set payload windows/x64/meterpreter/reverse_tcp
> set rhost 192.168.100.205

Ilustración 8. Ejecución de Xploit (Rejetto)



Fuente: KaliLinux

Ilustración 9. Prueba de control con Meterpreter

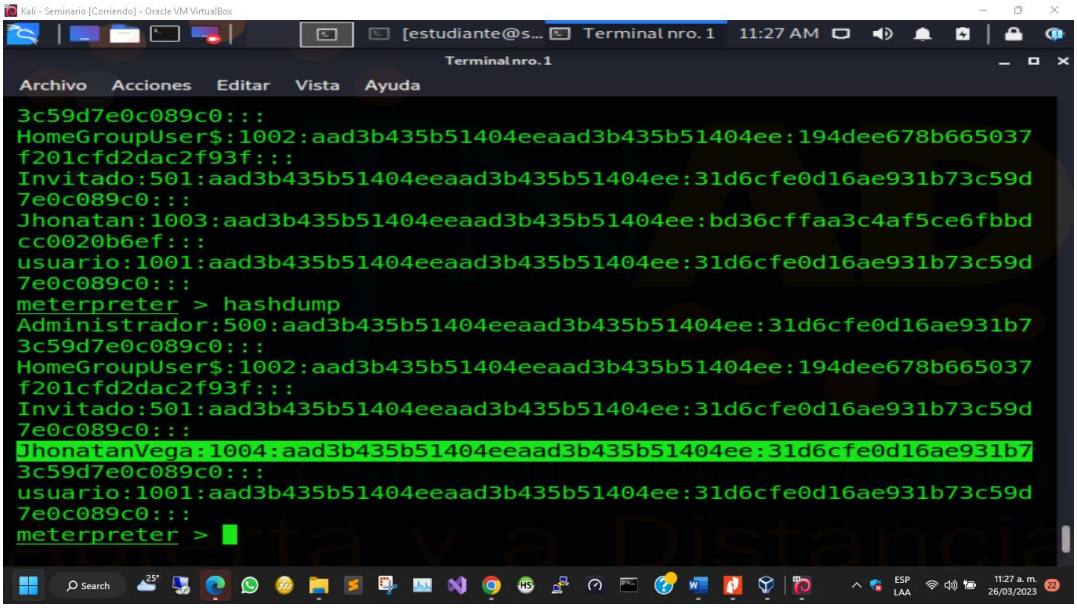


Fuente: KaliLinux

En esta fase, se logró penetrar con el exploit el cual se tomó el control de la máquina de la víctima y se utilizó el Meterpreter con el fin de hacer uso de su Shell inverso para explorar la máquina de la víctima y lograr tener control de

los archivos con información privilegiada. Igualmente se logra tener acceso con usuario JhonatanVega como administrador y permisos elevados.

Ilustración 10. Detención de Usuarios de la Victima



Fuente: KaliLinux

5.3.1.5. Fase de Informe

En esta fase, se logra aclarar las vulnerabilidades de la máquina de la víctima el cual se identificó un gran acceso remoto y lograr explorar toda la información de vital importancia, se identifica que bajo el sistema operativo Windows 7 x64 no tenía actualizaciones recientes de seguridad y el Firewall se encontraba sin políticas fuertes para evitar dicha vulnerabilidades, fue muy fácil tomar el control con la identificación del CVE de Rejetto v2.3 el cual permite tener un puerta de entrada para el ataque.

5.3.2. A CONTINUACIÓN, LISTE Y DESCRIBA LOS DATOS E INFORMACIÓN DEL ANEXO 4 – ESCENARIO 3 QUE LE FUERON DE AYUDA PARA IDENTIFICAR EL FALLO DE SEGURIDAD ESPECÍFICO EL CUAL ATACA A LA MÁQUINA WINDOWS 7 X64.

De acuerdo a la información base del caso, en donde se evidencia que existe una de fuga de datos al interior de la organización en uno equipo especifico. Se procede a identificar que se cuenta con una maquina que es la que se

esta presentando la fuga de datos el cual opera con Windows 7 x64 y ejecuta el software Rejetto v2.3.

Se inicia con la identificación de puertos abiertos el cual se visualiza que sobre el puerto 80 corre el software HTTP File Server HFS 2.3 de Rejetto v2.3, el cual es un WebServer para compartir datos, libre de malware pero con vulnerabilidades críticas, que se pueden ejecutar exploits de Shell reversa para obtener sesiones abiertas con el Meterpreter.

En este escenario critico por acceso remoto, se presenta por mala gestión en las políticas de seguridad al dejar el Firewall inactivo y sus puertos TCP/IP abiertos el cual genera múltiples amenazas a la seguridad de los datos en la organización.

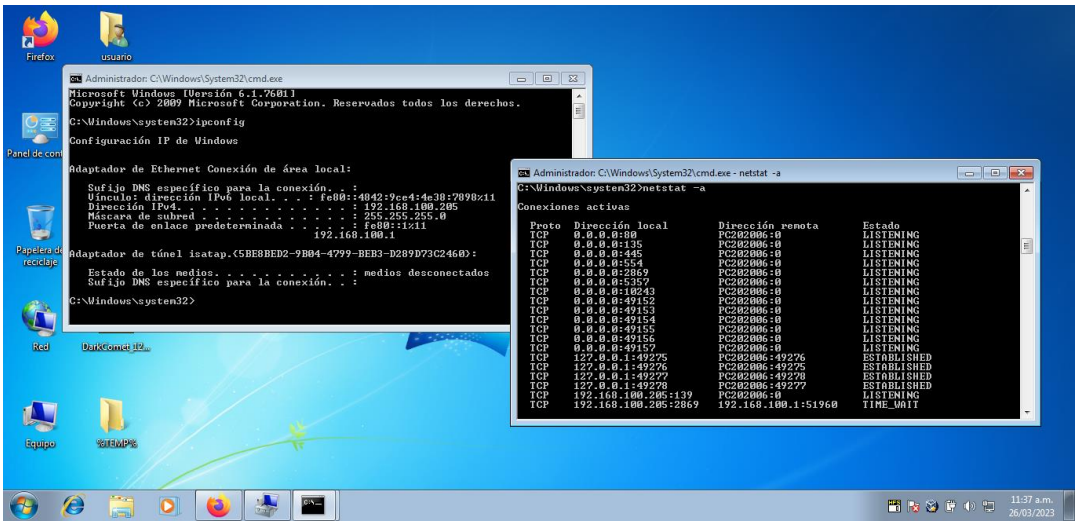
5.3.3. ¿QUÉ HERRAMIENTA UTILIZÓ PARA PODER IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA “MÁQUINA WINDOWS 7”? ¿QUÉ PUERTO ABRE LA APLICACIÓN ESPECÍFICA EN EL ANEXO?

La máquina con sistema operativo Windows 7 x64, tiene servicios ejecutándose como servicio y el cual acepta conexiones entrantes, dado que se detecta que su firewall no las bloquea.

Se procede a abrir el CMD y ejecutar el comando ***ipconfig***, en donde se identifica que la maquina tiene configurada la dirección física: 192.168.100.205, continuamos ejecutando el comando ***netstat -a*** donde se identifica los puertos que están abiertos.

Se identifica el software HTTP File Serve HFS 2.3 (Rejetto 2.3) está ejecutándose a través del puerto 192.168.100.25:80, esta aplicación tiene una vulnerabilidad critica conocida a través del acceso remoto.

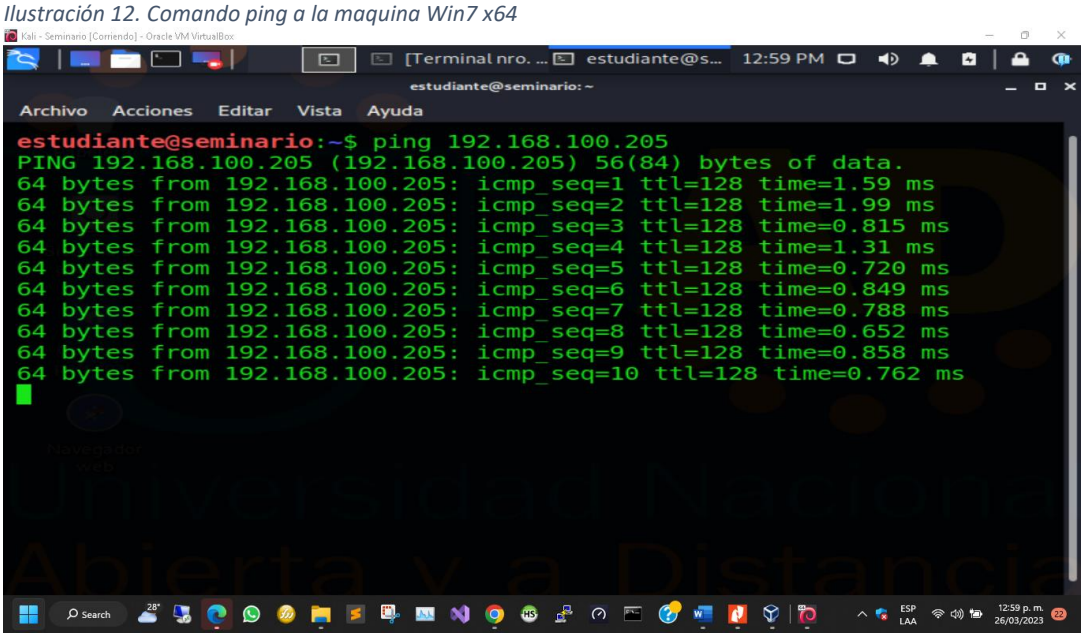
Ilustración 11. Puerto 80 escuchando Rejetto v2.3



Fuente: Victima – Windows 7 x64

Se procede a ejecutar en CMD el comando **ping**, en donde se identifica que existe comunicación y respuesta de ECHO del puerto 7 en la máquina de la víctima, en la siguiente imagen:

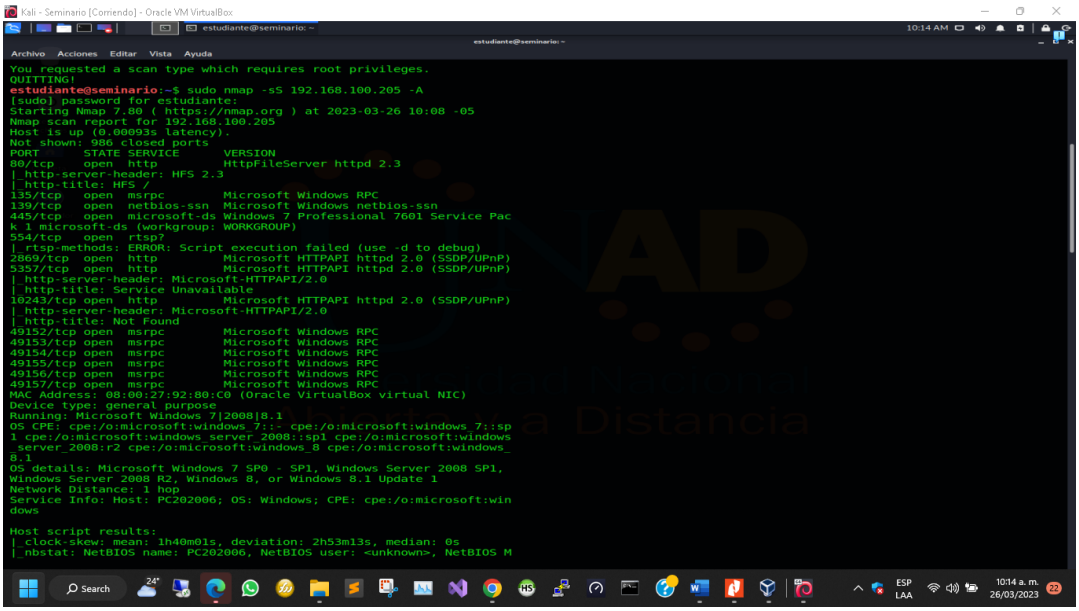
Ilustración 12. Comando ping a la maquina Win7 x64



Fuente: KaliLinux

Con NMAP, se puede detectar los puertos abiertos y los servicios que están corriendo en la maquina de la victima.

Ilustración 13. NMAP: Puerto 80 ejecutando Rejetto 2.3



Fuente: KaliLinux

5.3.4. EXPLIQUE CON SUS PALABRAS Y DE MANERA ESPECÍFICA CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 7 X64), HAGA USO DE GRÁFICOS PARA EXPLICAR EL ATAQUE.

Teniendo en cuenta la vulnerabilidad critica encontrada en la máquina de la víctima el cual comprende del uso de software que es utilizado para compartir datos en una organización el cual no había sido testeada en sus niveles de seguridad, además acompañada de la falta de políticas de seguridad para la protección lógica a través de Firewall seguros. Por tal motivo el atacante al escanear el segmento 192.168.100.0/24 se identificó los equipos conectados que respondieron al echo del puerto 7 y se encuentra que el equipo objetivo está en la dirección física 192.168.100.205 en donde con el uso de herramienta NMAP se escanean los puertos y se identifica los servicios que se ejecutan encontrándose el software HTTP File Server HFS 2.3.

Actualmente se logra identificar la vulnerabilidad critica, el cual permite hacer un ataque con acceso remoto al equipo de la víctima con el fin de utilizar Exploit que permite Shell Reverse y esto a su vez ejecutar código arbitrario al cargar un archivo con secuencias que se interpretan como macro ejecutables tomando el control de la máquina de la víctima y el acceso a todos los directorios del disco duro con el fin de obtener su información vital.

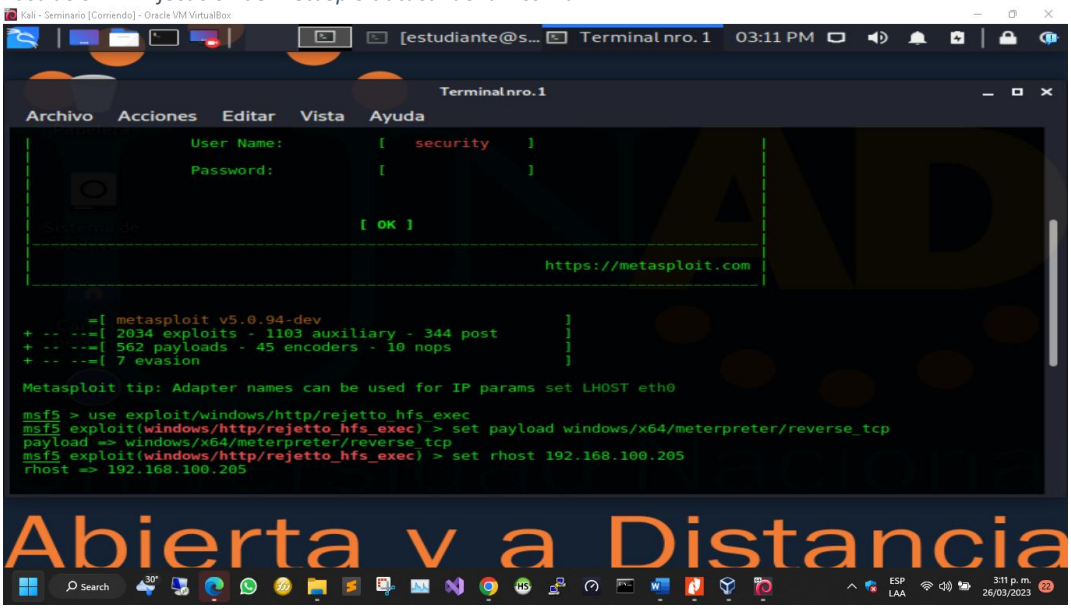
5.3.5. DOCUMENTE CADA UNO DE LOS PASOS QUE EJECUTÓ Y SUS RESPECTIVAS EVIDENCIAS PARA EXPLOTAR LA VULNERABILIDAD EN LA MÁQUINA WINDOWS 7.

Teniendo en cuenta que, dentro del análisis forense, se conoce en primera medida que el equipo victima tiene un Software con vulnerabilidades y Listening en el puerto 192.168.100.205:80, se procede a generar para lograr acceso remoto a una Shell Inversa, para controlar el servidor.

Se utiliza el MetaSploit Framework el cual se ejecuta el exploit rejetto v2.3 para proceder a iniciar los payload.

> use exploit/windows/http/rejetto_hfs_exec
> set payload windows/x64/meterpreter/reverse_tcp
> set rhost 192.168.100.205

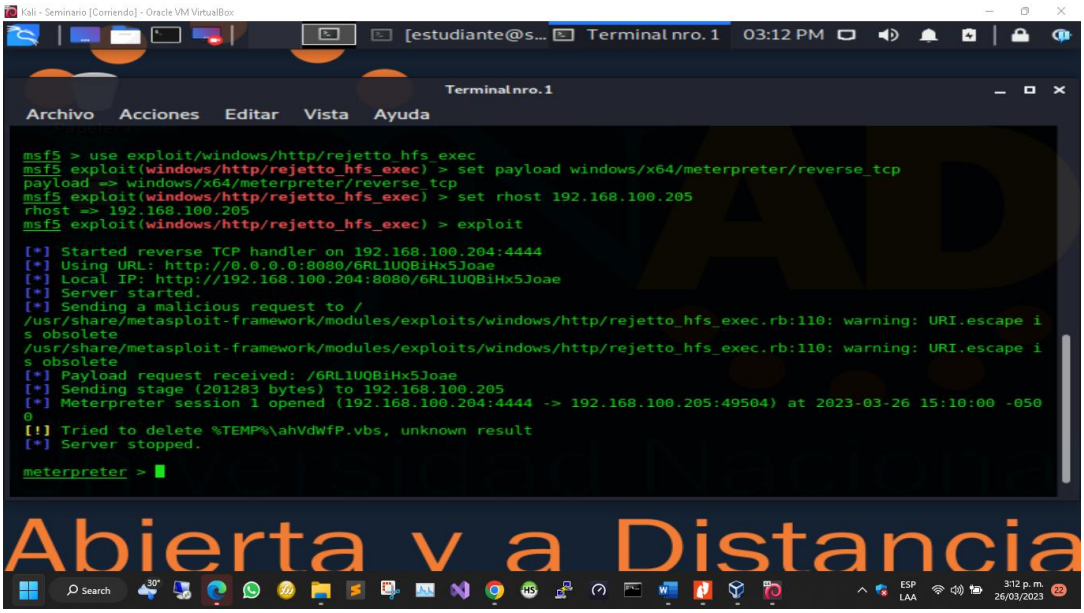
Ilustración 14. Ejecución de MetaSploit atacando la victima



Fuente: Máquina Virtual Windows x64

Una vez se ejecutan los parámetros establecidos, se procede a explotar la vulnerabilidad:

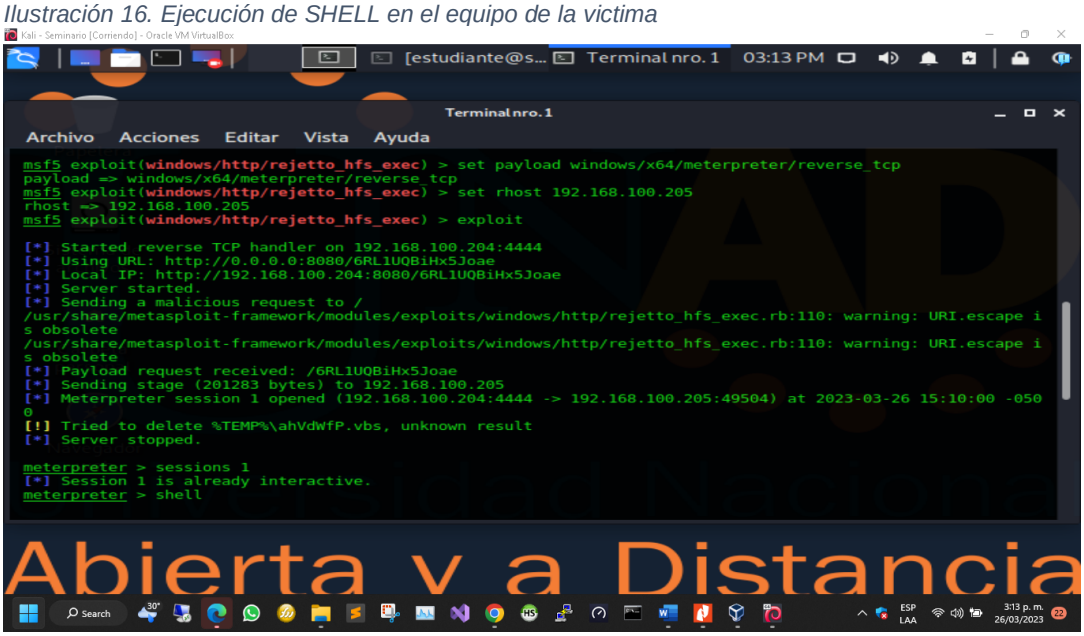
Ilustración 15. Ejecución de MetaSploit con sesion de Meterpreter



Fuente: KaliLinux

Como se observa, el equipo atacante con Kali Linux se logra establecer conexión con la víctima al 192.168.100.25:49504. Se procede a ejecutar el Shell de Windows, que me permite ejecutar comandos dentro de la maquina victima:

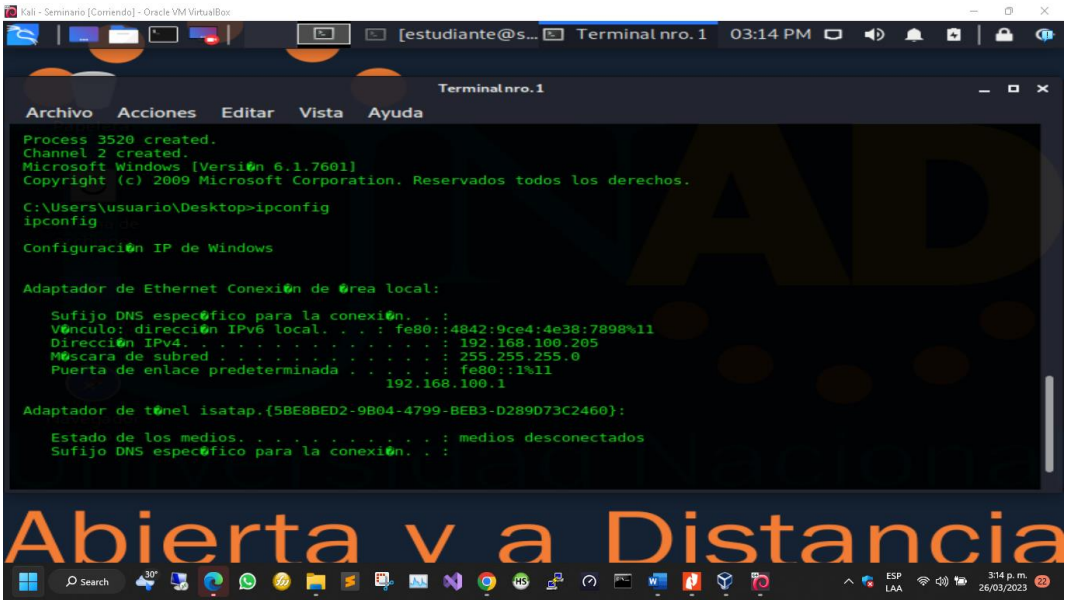
Ilustración 16. Ejecución de SHELL en el equipo de la victima



Fuente: KaliLinux

Una vez se logra ingresar al SHELL se puede ejecutar comando **ipconfig** para asegurarnos que estamos dentro del equipo víctima y se reconoce la dirección física de la red 192.168.100.205.

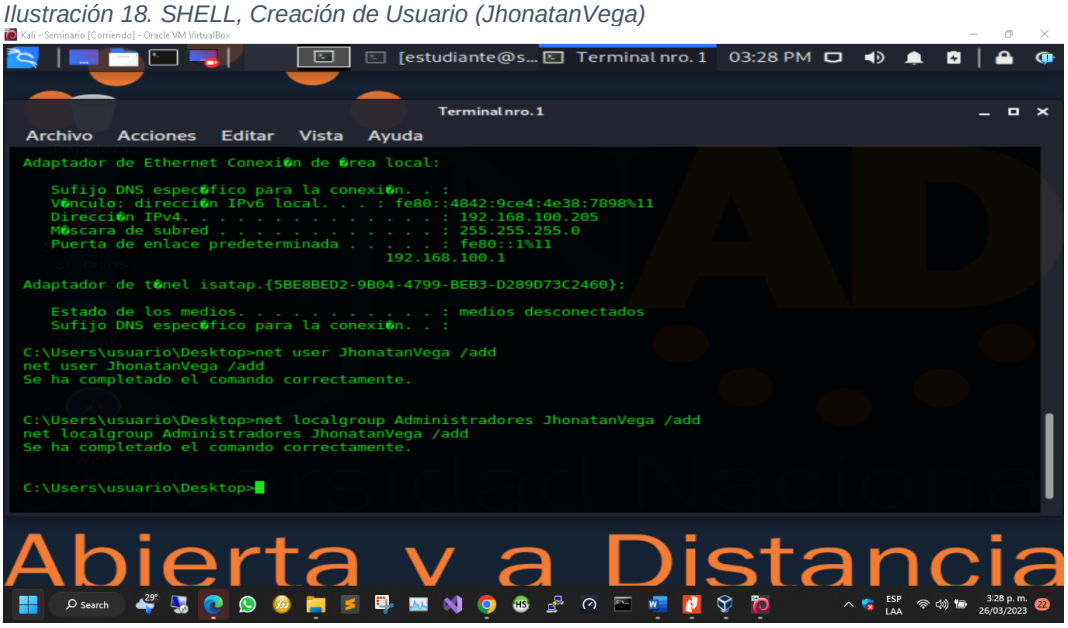
Ilustración 17. Sesión en SHELL de la victima



Fuente: KaliLinux

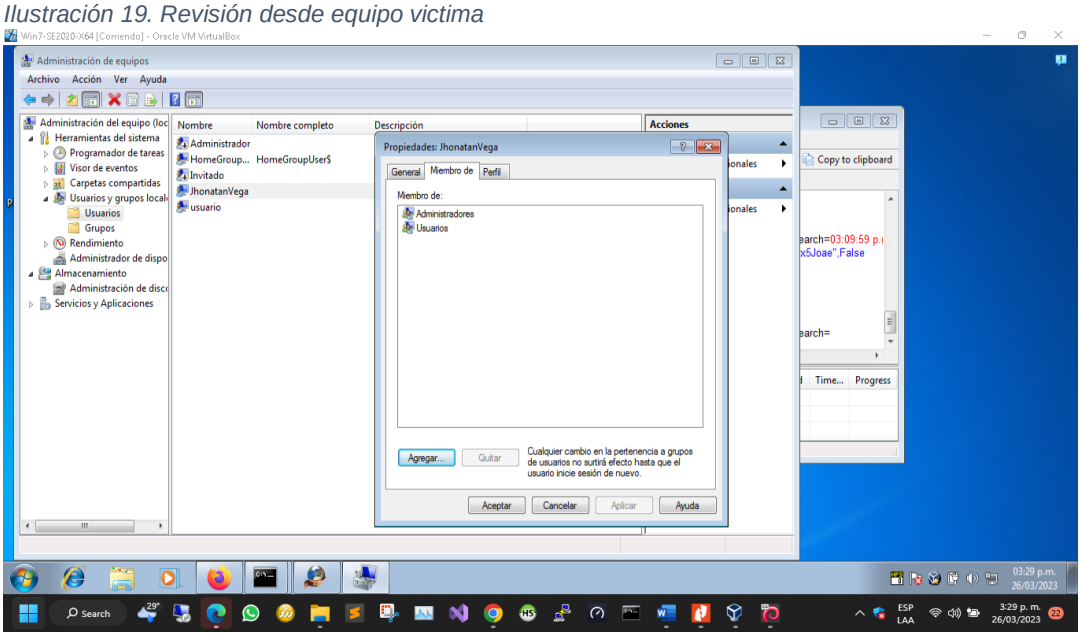
Se identifica que a través del software Rejetto v2.3 con exploit, permite el acceso a través del puerto :80 se puede tener una vulnerabilidad en la seguridad y una fuga de los datos de la organización, al encontrarse abierto :80 se lograr ejecutar un ataque exitoso. Se procede a ejecutar la explotación de la vulnerabilidad, creando un usuario con privilegios dentro del grupo local de Administradores el siguiente usuario con el primer nombre del estudiante: Jhonatan y primer apellido: Vega para demostrar la falla a los altos directivos de la organización.

Ilustración 18. SHELL, Creación de Usuario (JhonatanVega)



Fuente: KaliLinux

Ilustración 19. Revisión desde equipo victima



Fuente: Windows 7 x64

Finalmente, se presenta y se demuestra a los altos directivos de la organización que por medio de la aplicación Rejetto v2.3 el cual es utilizada para compartir datos y que por motivos de tener un sistema operativo sin soporte de actualizaciones de parches de Microsoft, se está comprometiendo la seguridad lógica de la entidad, debido a la vulnerabilidad del equipo dentro de la organización que de manera remota puede ser atacado dentro de la entidad ó por fuera si es publicado en internet este servidor, igualmente se demuestra tener el control total del WebServer con la creación del usuario **JhonatanVega** con altos privilegios administrativos.

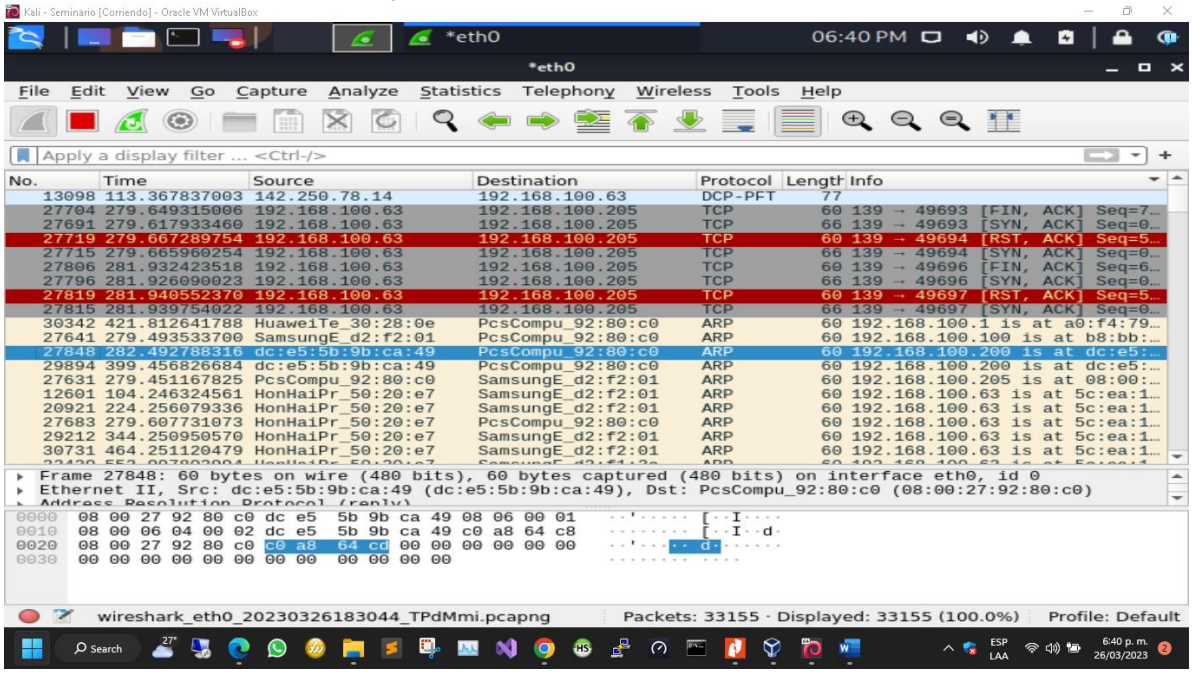
5.4. ETAPA 4: CONTENCIÓN DE ATAQUES INFORMATICOS

5.4.1. CONTECION DE ATAQUE EN TIEMPO REAL

En primera medida, se identifica que el equipo victima se debe generar test de vulnerabilidades de la red para identificar los puertos abiertos y la descripción de los servicios que corren en ellos, para esto utilizaremos la herramienta WireShark que se encargará de escanear el segmento 192.168.100.0/24 el cual encuentra nuestro

equipo de la victima con la dirección física 192.168.100.205 el cual alerta en color rojo que tiene vulnerabilidades en los puertos de transmisión.

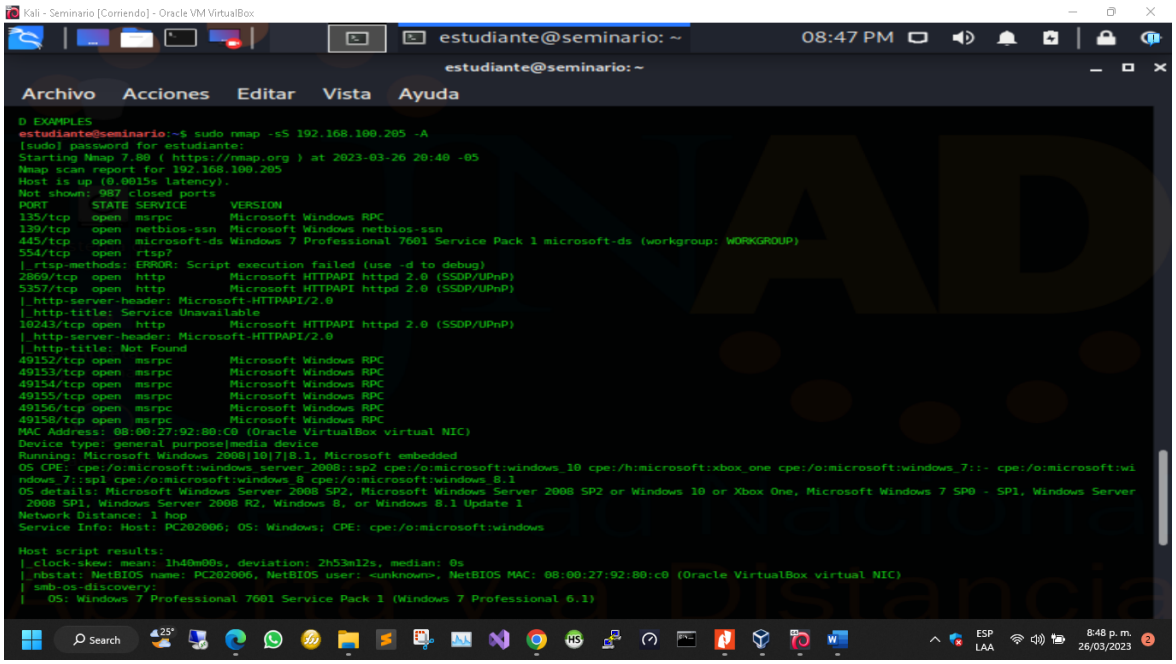
Ilustración 20. Primer escaneo de la red para encontrar vulnerabilidades con WireShark



Fuente: KaliLinux – WireShark

Se continua con el análisis utilizando una segunda herramienta el cual es NMAP con el fin de buscar vulnerabilidades en los puertos, servicios, la ruta y el sistema operativo de la máquina, el cual no arroja que se encuentran muchos puertos en estado LISTENING con sus respectivos servicios, el cual debemos evaluar algunos procesos de seguridad que están posiblemente desactivados.

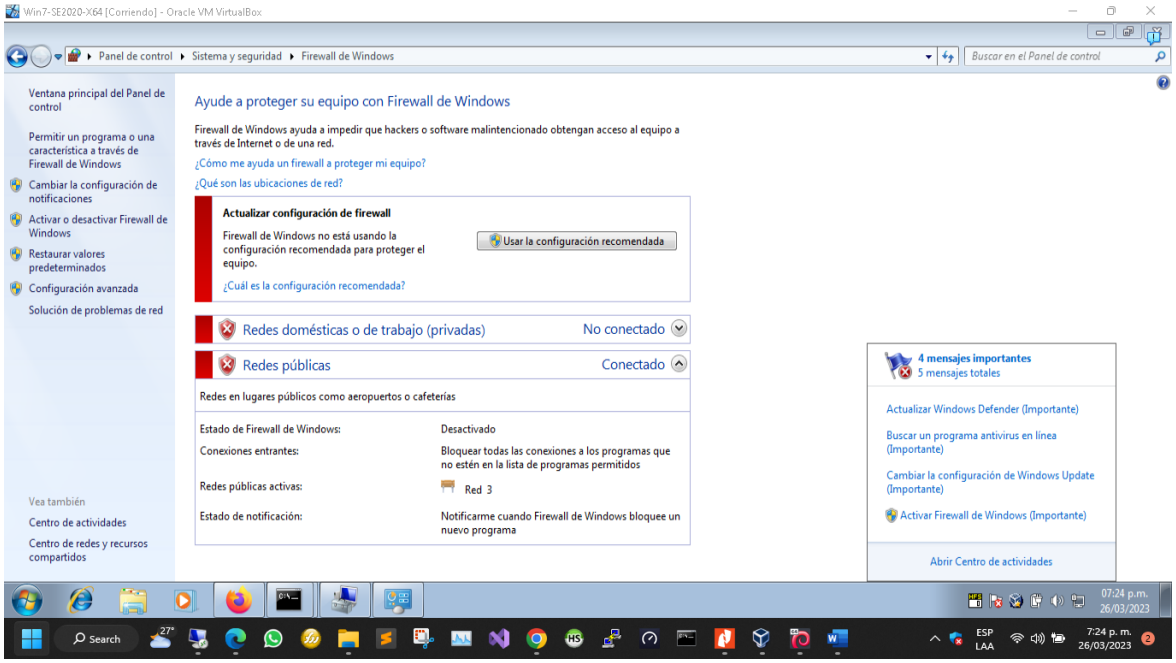
Ilustración 21. Primer escaneo de puertos abiertos y servicios



Fuente: KaliLinux – NMAP

Se identifica que el Firewall de Windows se encuentra en estado desactivado, el cual permite libremente tener vulnerabilidades para posibles ataques.

Ilustración 22. Firewall de Windows desactivado

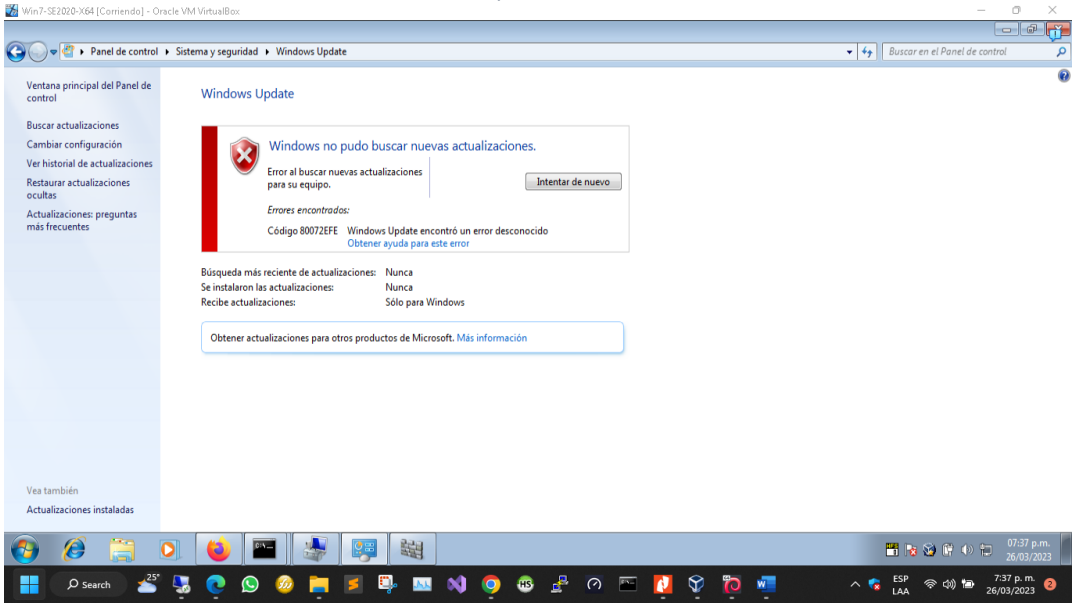


Fuente: Equipo victima Win7 x64

Se procede a revisar las actualizaciones de seguridad de la maquina, en donde se identifica que no se pueden hacer uso de actualizaciones recientes debido a que a

nivel mundial este sistema operativo ya termino su soporte técnico el pasado 14/01/2020.

Ilustración 23. Error de Actualización del Sistema Operativo



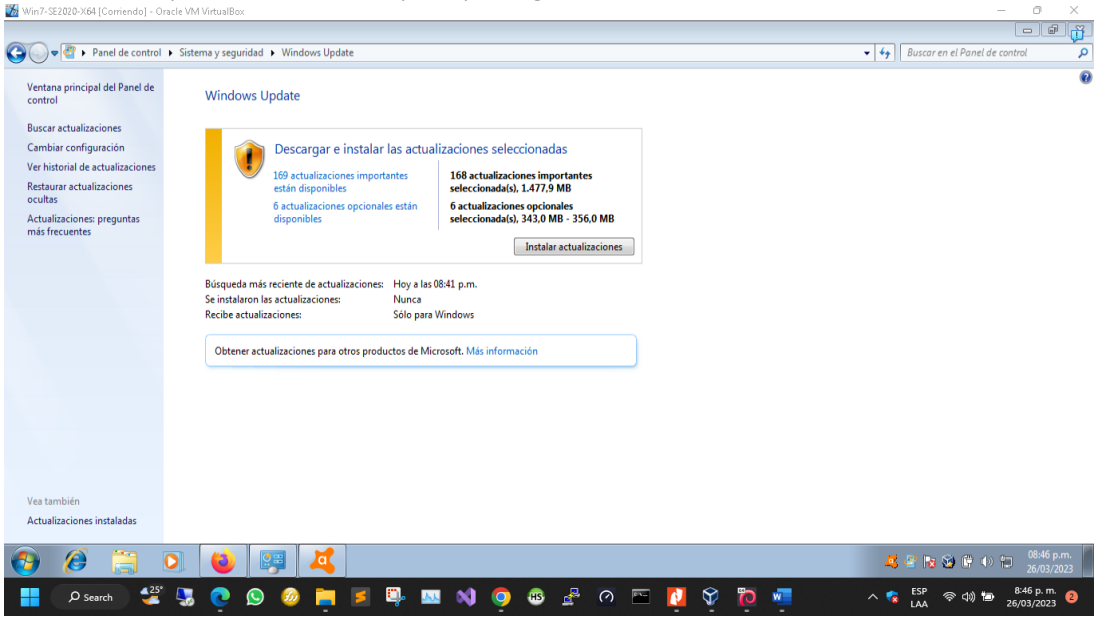
Fuente: Equipo victima Win7 x64

Se procede a ejecutar acciones para obligar al sistema operativo ser actualizado directamente con las actualizaciones del portal genuino de Microsoft, se establece que debe tener instalado SP1 - Service Pack 1.

- Detener el servicio: **Windows Update**
- Eliminar las carpetas dentro del directorio C:\Windows\SoftwareDistribution
- Detener el servicio: de **Servicios de Cifrado**
- Eliminar la carpeta **catroot2** dentro del directorio C:\Windows\System32\catroot2
- Iniciar nuevamente el servicio: de **Servicios de Cifrado**
- Cambiar a inicio automático el servicio: **Servicio de transferencia inteligente en segundo plano (BITS)**
- Reiniciar el servicio: **Servicio de transferencia inteligente en segundo plano (BITS)**
- Cambiar a inicio automático el servicio: **Windows Update**
- Iniciar el servicio: **Windows Update**
- Reiniciar el servicio: **Windows Update**
- Descargar la actualización KB3138612

Se identifica que el sistema operativo después de seguir los pasos anteriores, ya permite recibir actualizaciones del portal genuino de Microsoft y se inicia a actualizarlo con el fin de mejorar su seguridad.

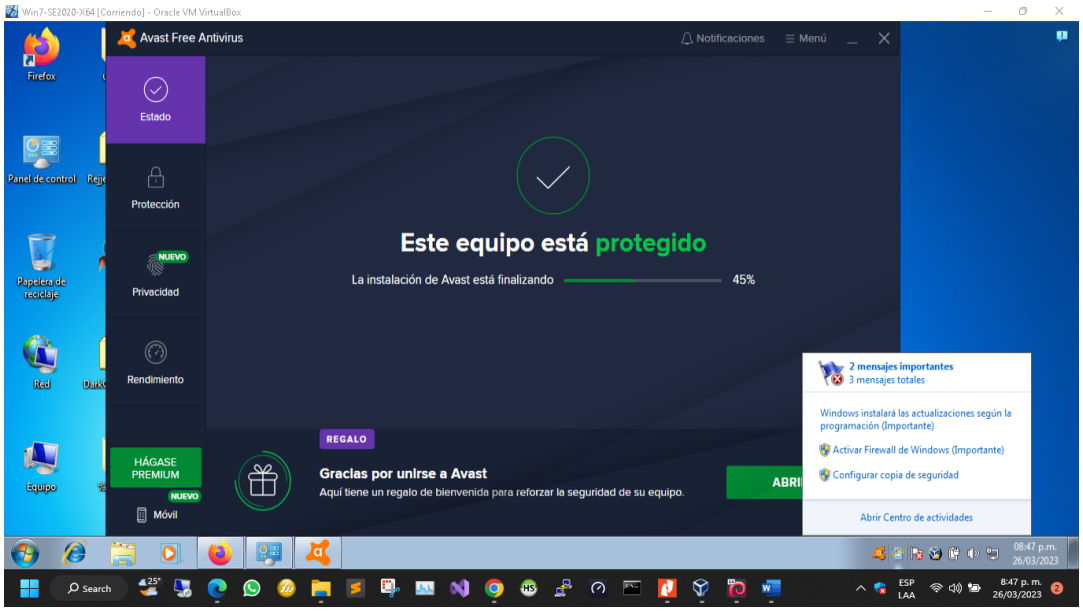
Ilustración 24. Reparación de Windows Update para lograr actualizaciones en 2023



Fuente: Equipo victima Win7 x64

Igualmente se procede a realizar la instalación de un Antivirus con el fin de proteger en contra de vulnerabilidades, además la alerta de recomendación de Windows ya se desaparece.

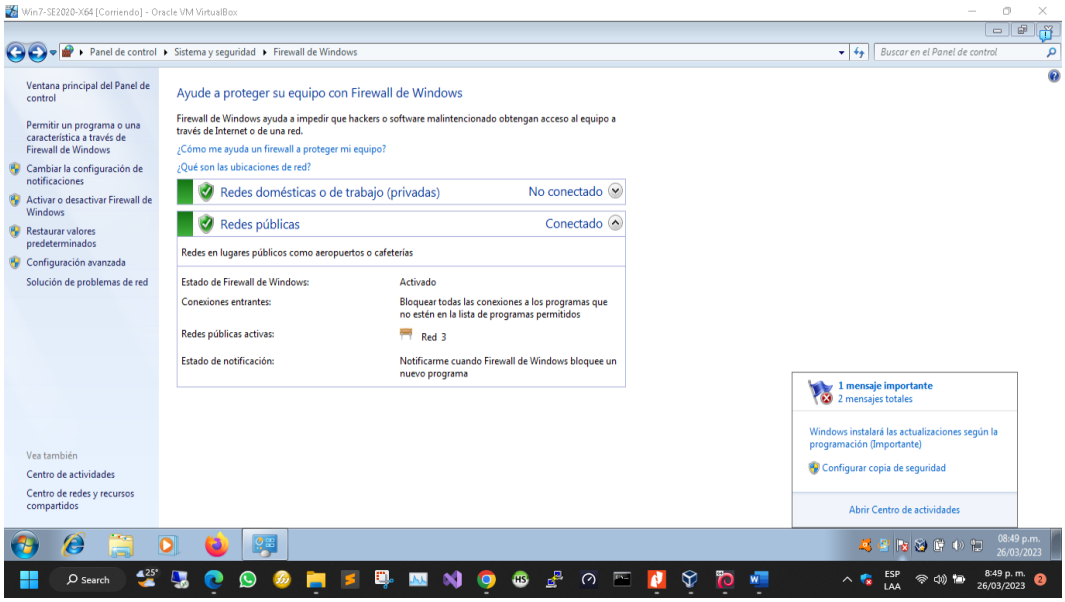
Ilustración 25. Instalación de Antivirus



Fuente: Equipo victima Win7 x64

Se procede a realizar la activación del Firewall de Windows con el fin de tener contención a los ataques y restringir los puertos estrictamente necesarios.

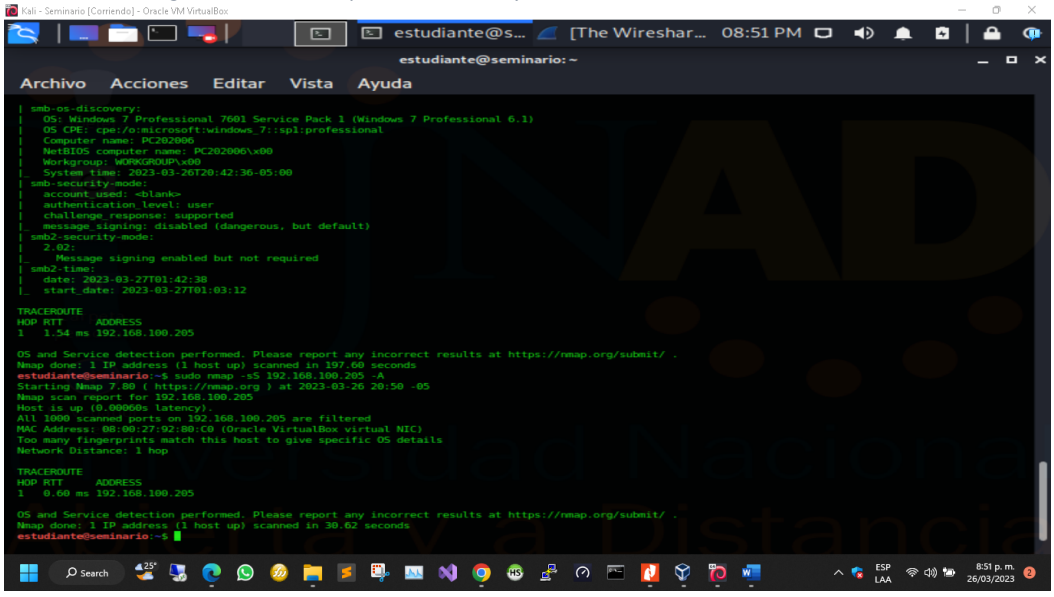
Ilustración 26. Activación de Firewall de Windows



Fuente: Equipo victima Win7 x64

Una vez asegurado el sistema operativo, con prácticas y procesos básicos para blindar de ataques, se procede a realizar por segunda vez un test de nmap para visualizar las vulnerabilidades existen en donde se detalla que no es posible encontrar porque ya se aplicó el Firewall, Antivirus y Actualizaciones de seguridad del sistema operativo.

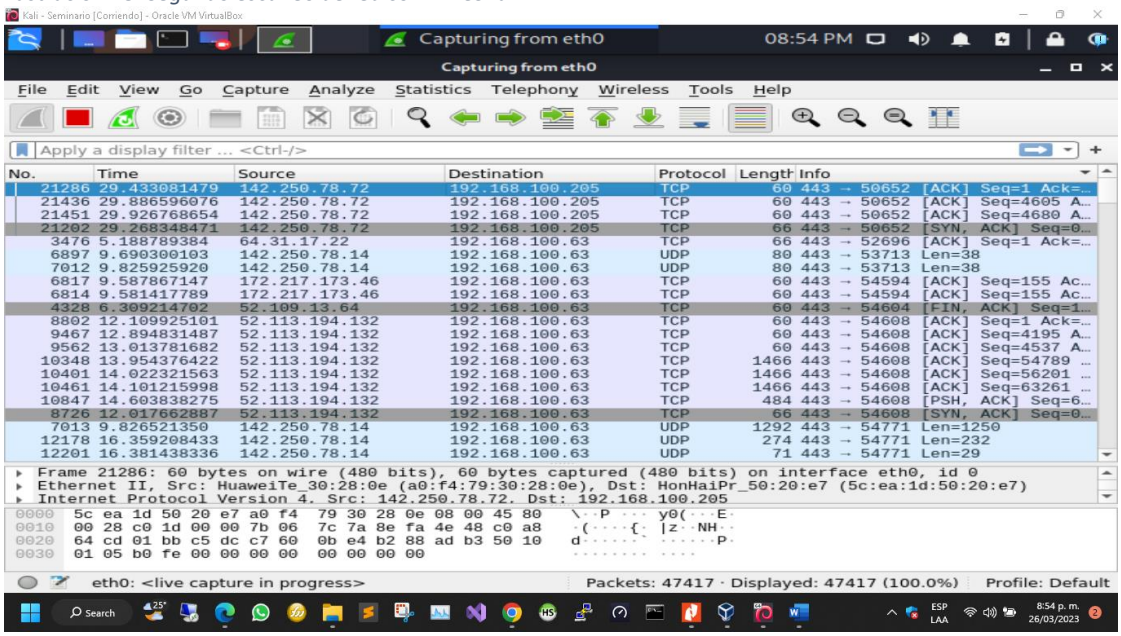
Ilustración 27. Segundo escaneo de puertos abiertos y servicios



Fuente: Equipo victima Win7 x64

Se realiza un segundo escaneo con WireShark en donde ya no se tiene alerta criticas en color rojo del equipo en la dirección física 192.168.100.205.

Ilustración 28. Segundo escaneo de red con WireShark



Fuente: Equipo victima Win7 x64

5.4.2. ¿QUÉ SERÍA LO PRIMERO QUE INDAGARÍA Y HARÍA SI LLEGARA A ENCONTRARSE UN ATAQUE EN TIEMPO REAL? ESPECIFIQUE SU RESPUESTA CON ARGUMENTOS TÉCNICOS.

Al encontrarme con un ataque en tiempo real dentro de una organización, en primer lugar, debería guardar la calma para iniciar los procesos de mitigación del impacto donde se identifica el tipo y entrada del ataque con el fin aislar los equipos que han sido atacados para evitar propagación a los demás equipos de la red interna, luego iniciaría a analizar el tráfico de la red interna y externa con WireShark para identificar flujos de tráfico sospechosos con errores e interceptados, debido a que en esta herramienta permite monitorear la transmisión dentro de nuestra red y si alguno de estos presenta algún error o intercepción podríamos priorizar de acuerdo al color critico de la amenaza para iniciar a cerrar las puertas de entrada de los atacantes.

Una vez identificado y aislados los equipos atacados, iniciaría con la detección e identificación del tipo de ataque con el fin de salvaguardar la información que se puede recuperar con el fin de proceder a realizar mantenimiento correctivo de hardware, firmware y sistema operativo de la maquina atacada en bajo nivel con el fin de liberar la máquina de cualquier vulnerabilidad que se puede propagar.

Posteriormente, se debe promover una etapa de aseguramiento de políticas y procesos en la seguridad lógica para cerrar las brechas de vulnerabilidades encontradas y otras que pueda originar otro tipo de ataque, seguido a este proceso se garantiza una etapa de restablecimiento de servicios a través de copias de seguridad que permita volver a la normalidad en menor tiempo posible.

5.4.3. ¿TENIENDO EN CUENTA EL ATAQUE EJECUTADO DESDE EL EJERCICIO DE RED TEAM QUÉ MEDIDAS DE HARDENIZACIÓN PROPONDRÍA PARA QUE EL ATAQUE NO SE REPITA?

De acuerdo al ataque ejecutado desde el ejercicio de RedTeam con la maquina en Windows 7 x64 con las vulnerabilidades existen y para evitar a que se repita un nuevo ataque, propondría los siguiente:

- Actualización de Firmware de MainBoard, disco duro y unidades de entradas.
- Seguridad en arranque seguro y sistema de archivos GPT.
- Actualización de sistemas operativos y parches de vulnerabilidades.
- Niveles superiores de contraseñas y cambio obligatorio programado.
- Activación y segmentación estricta de puertos locales del Firewall del sistema operativo.
- Creación de VLAN para conexiones de redes.
- Utilización de Antivirus y políticas de actualizaciones.
- Utilización de la encriptación de datos a nivel del sistema operativo.
- Utilización de IDS-IPS para tener alertas sobre eventos sospechosos.
- Utilización de UTM para segmentar las interfaces y políticas de tráfico de datos en la red.

5.4.4. ¿DESCRIBA CON SUS PALABRAS LAS DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS?

La seguridad de la información en las organizaciones se debe complementar con equipos que ayuden a mitigar el impacto y resolver en el menor tiempo la continuidad del servicio, por este motivo es necesario encontrar las diferencias en los equipos de respuesta y monitoreo (BlueTeam e Incidentes Informaticos).

EQUIPO BLUETEAM	EQUIPO CISRT
Los equipos BlueTeam son los encargados de monitorear y fortalecer la seguridad digital de una organización, analizando e implementando constantemente acciones que promuevan el endurecimiento de los sistemas informáticos con el fin encontrar vulnerabilidades para tomar acciones rápidas con el fin de evitar un ataque cibernético y minimizar el impacto de la afectaciones, igualmente se encargan del análisis forense del ataque, a diferencia del CISRT este se centra solo en los activos informáticos de la organización.	Los equipos de respuesta a incidentes informáticos (CISRT, se encarga ejecutar medidas preventivas y reactivas ante eventos de incidentes de seguridad en los activos de información de las organizaciones, se encarga de impedir que un ataque se propague en menor tiempo posible evitando que cause más daños, a diferencia de los equipos BlueTeam este se centra en análisis y monitoreo constante de vulnerabilidades.

5.4.5. ¿SI DENTRO DE UN EQUIPO BLUETEAM LE INDICAN QUE DEBE TRABAJAR CON CIS “CENTER FOR INTERNET SECURITY” USTED LO UTILIZARÍA PARA QUÉ FIN?

Si dentro de un equipo de BlueTeam me indican que debo trabajar con CIS (Center for Internet Security) que es una organización encargada de emitir constantemente lineamientos, estándares y mejores prácticas de seguridad informática en las organizaciones. Por tal motivo, lo utilizaría como un marco de referencia en la implementación de buenas prácticas dentro de la organización, el cual permitiría tener manuales y guías de acciones de los equipos BlueTeam y CSIRT para garantizar que la organización esta protegida ante ataques informáticos, adicionalmente por ser una organización sin ánimo de lucro se puede hacer uso de las herramientas de manera gratuita, lo que disminuye costos de implementación.

El CIS promueve la documentación para correcta ejecución de herramientas de seguridad para la prevención, detección y explotación de amenazas que atentan sobre las vulnerabilidades de la organización.

5.4.6. EXPLIQUE Y REDACTE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE LO QUE ES UN SIEM.

SIEM (Security, Information and Event Management), se encarga de monitorear los activos informáticos en tiempo real con el fin de encontrar posibles amenazas y vulnerabilidades para un posible ataque cibernético.

Se componen de los siguientes sistemas:

- (LMS): Encargado de la administración centralizada de logs de los activos informáticos.

- (SIM): Encargado de la recolección de logs y su almacenamiento a largo plazo con prácticas de análisis y reporte de los datos.

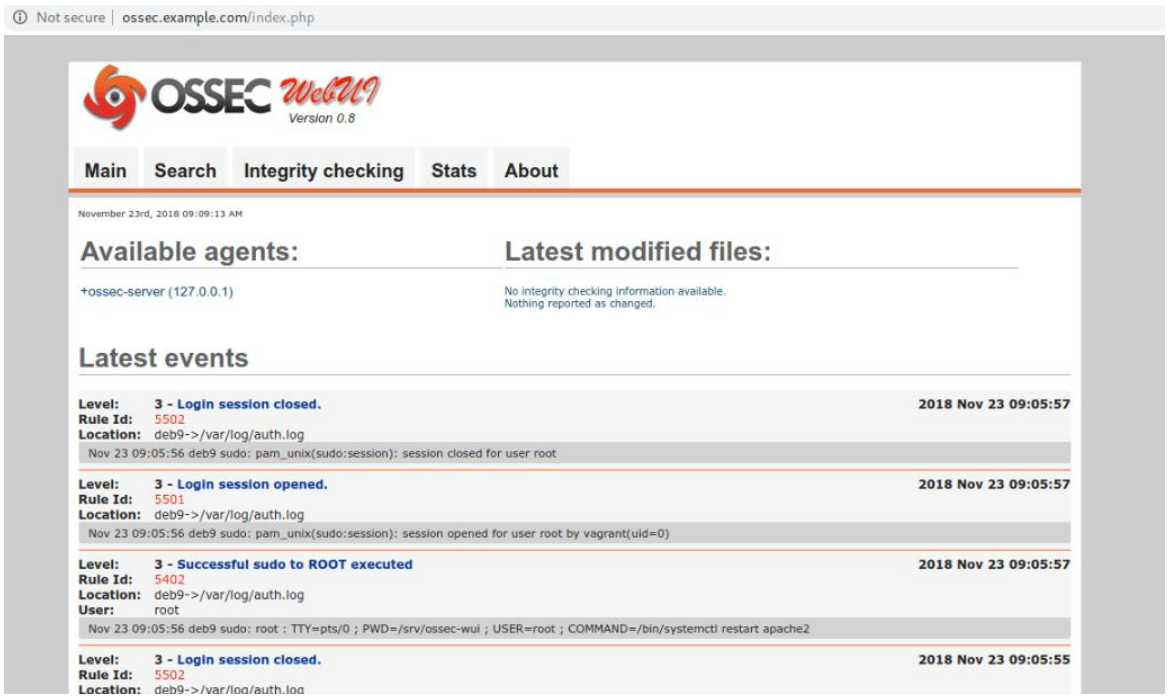
- (SEM): Encargado de administrar los eventos de seguridad, permitiendo monitorear en tiempo real.

Estos tres sistemas se encargan de analizar la información recolectada para identificar cambios de los parámetros de los diferentes sistemas informáticos que comprometen la protección ante vulnerabilidades informáticas.

5.4.7. DEFINA POR LO MENOS 3 HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS “HARDWARE O SOFTWARE”, RECUERDE QUE LAS HERRAMIENTAS DE CONTENCIÓN SON DIFERENTES A LAS HERRAMIENTAS DE DETECCIÓN.

OSSEC: Sistema de detección de intrusos gratuito que realiza supervisión del registro de Windows, comprobación de integridad, alertas basadas en el tiempo, detección de rootkits, análisis de registro y respuesta activa.

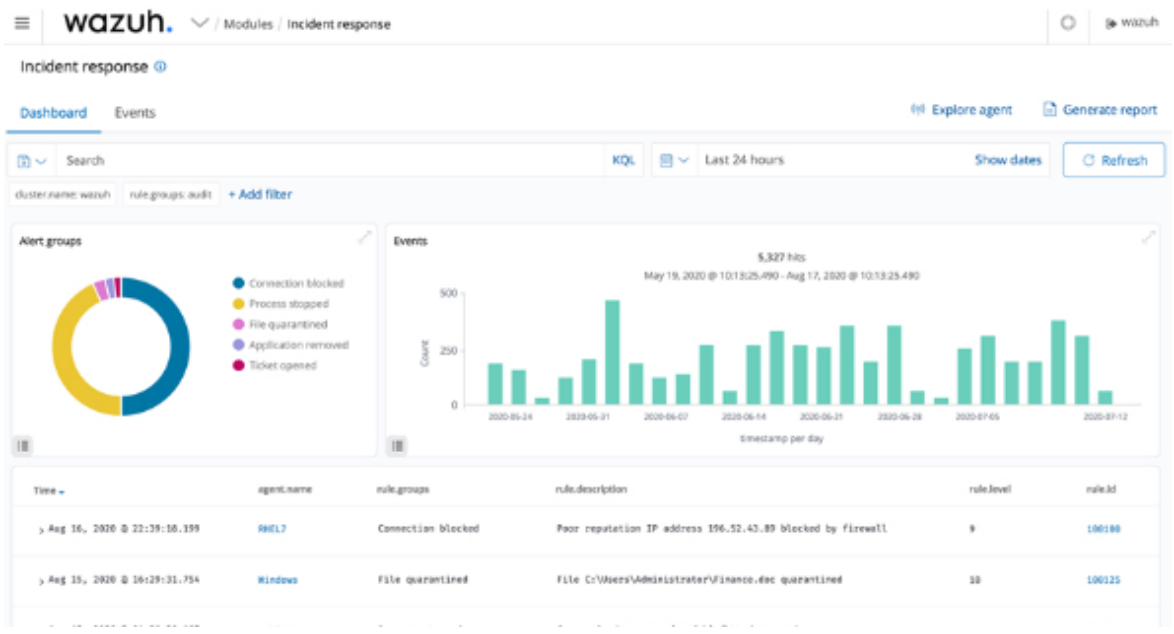
Ilustración 29. OSSEC: sistema de detección de intrusos basado en host gratuito y de código abierto



Fuente: https://www.ossec.net/

WAZUH: Sistema de detección de intrusos gratuito que realiza supervisión del registro de Windows, comprobación de integridad, alertas basadas en el tiempo, detección de rootkits, análisis de registro y respuesta activa.

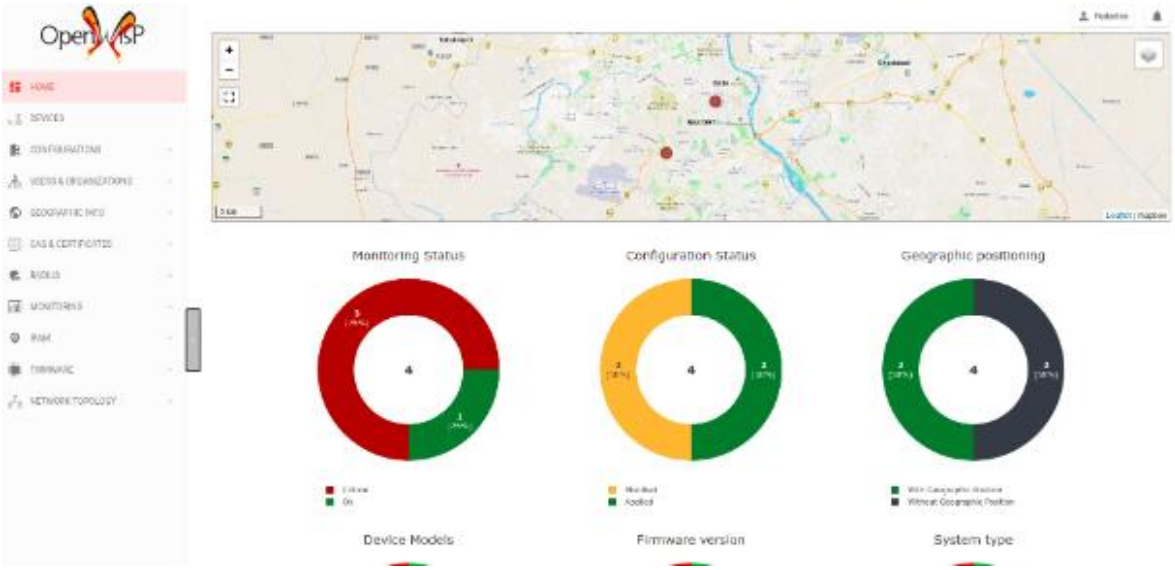
Ilustración 30. WAZUH: sistema de detección de intrusos basado en host de código abierto y libre



Fuente: https://wazuh.com/

OPENWIPS: Es un sistema de detección de intrusos que permite administrar y automatizar varios aspectos de la implementación, el monitoreo y la administración de la red de TI.

Ilustración 31. OPENWISP: Sistema de prevención de intrusiones



Fuente: https://openwips-ng.org/

5.5. ESTRATEGIAS QUE CONTRIBUYEN AL TRABAJO DE LOS EQUIPOS DE REDTEAM Y BLUETEAM

Existen varias estrategias que pueden contribuir al trabajo de los equipos de Red Team y Blue Team. A continuación, se describen algunas de ellas:

En la actualidad las empresas y personas se han visto afectadas para la inseguridad dentro de los procesos digitales, es por esto que los equipos de Blue Team y Red Team se pueden apoyar dentro de la organización con el CIS (CENTER FOR INTERNET SECURITY) porque es la encargada de emitir constantemente lineamientos, estándares y mejores prácticas de seguridad informática en las organizaciones. Por tal motivo, contribuirá como un marco de referencia en la implementación de buenas prácticas, el cual permitiría tener manuales y guías de acciones de los equipos BlueTeam y CSIRT para garantizar que la organización este protegido ante ataques informáticos, adicionalmente por ser una organización sin ánimo de lucro se puede hacer uso de las herramientas de manera gratuita, lo que disminuye costos de implementación.

El CIS promueve la documentación para correcta ejecución de herramientas de seguridad para la prevención, detección y explotación de amenazas que atentan sobre las vulnerabilidades de la organización.

Al continuar con las estratégicas, es necesarios de implementar el SIEM (Security, Information and Event Management), el cual se encarga de monitorear los activos informáticos en tiempo real con el fin de encontrar posibles amenazas y vulnerabilidades para un posible ataque cibernético.

El SIEM, se componen de los siguientes sistemas:

- (LMS): Encargado de la administración centralizada de logs de los activos informáticos.

- (SIM): Encargado de la recolección de logs y su almacenamiento a largo plazo con prácticas de análisis y reporte de los datos.

- (SEM): Encargado de administrar los eventos de seguridad, permitiendo monitorear en tiempo real.

Estos tres sistemas se encargan de analizar la información recolectada para identificar cambios de los parámetros de los diferentes sistemas informáticos que comprometen la protección ante vulnerabilidades informáticas.

5.6. ESTRATEGIAS QUE PERMITEN ENDURECER LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN

De acuerdo a lo ejecutado en el seminario y con el fin de endurecer los aspectos de seguridad de la información en la organización por parte de los equipos Red Team y Blue Team, se deben determinar las medidas a nivel del personal, los estaciones de trabajo y la red, de la siguiente manera:

A NIVEL DE PERSONAL

Para lograr identificar y mitigar las vulnerabilidades dentro de una organización, es necesario tener capacitado el personal que labora para la entidad, con alto grados de conocimientos de las amenazas y los procesos a seguir para reportar el incidente

informático con el fin de ayudar a poner en marcha algún plan de alerta y cuidado sobre las tecnologías e información.

Por consiguiente, es necesario conformar equipos internos con altos conocimientos de:

- Uso y apropiación de internet.
- Manejo dispositivos electrónicos extraíbles.
- Identificación de ataques cibernéticos y el phishing.
- Buenas practicas en el uso de las estaciones de trabajo.
- Identificación de acciones antes, durante y posterior a un ataque.
- Conocimiento de las principales vulnerabilidades.

A NIVEL DE ESTACIONES DE TRABAJO

Para lograr minimizar el alto impacto que se presenta con la explotación de vulnerabilidades existen en la tecnología, es preciso determinar la Metodologia de Seguridad y Privacidad de la Información con el fin de asegurar configuraciones esenciales para hacer más difícil la intrusión en un ataque cibernético. A continuación de detallan criterios importantes los cuales son:

- Instalación y actualización periódicas de sistemas operativos con medios oficiales para evitar que traigan virus ó que se presente una vulnerabilidad.

- Implementación de servidores de dominios y ldap con servicios de políticas estrictas a usuarios y grupos de usuarios (cuentas limitadas).

- Implementación de antivirus, antimalware con firewall para sistema operativo con el fin de dejar puertos de comunicación exclusivos.

- Particionamiento lógico de disco duro para separar el sistema operativo y a información de usuarios, con el fin obtener oportunidad de salvaguardar la información en el caso de presentarse una falla de hardware ó ataque cibernético.

- Control de ejecución de aplicaciones y/o macros con políticas de sistema operativo.

- Restricción de puertos de entrada y/o captura para evitar que se propaguen virus.

- Implementación de herramientas de monitoreo y detección de instrucciones.

- Auditoria y Testeo rutinario de puertos y servicios que se ejecutan de manera innecesarias.

A NIVEL DE RED DE DATOS

Para lograr mitigar el alto impacto en las redes de transmisión de datos lógicos, es necesario optar por ejecutar políticas de seguridad digital, las cuales se detallan a continuación.

- Implementación de FW – Firewall sectorizados y en clúster con el fin de definir políticas e interfaces que permitan proteger la entrada y salida del tráfico.

- Implementación de software o hardware de monitoreo y detección de instrucciones (IDS, IPS, SIEM, etc.), los cuales analizan el tráfico de los datos.

- Implementación de VLAN de comunicación por segmentos de redes.

- Implementación de acciones preventivas con la auditoria de la transmisión de datos.

5.7. OTRAS HERRAMIENTAS QUE PERMITEN CONTENER ATAQUES INFORMÁTICOS

Para lograr tener control de los ataques informáticos, los equipos de Blue Team y Red Team deben tener presente que se contar con la implementación de soluciones de seguridad lógica soportada en empresas con alto grado de robustes en los procesos de monitoreo y control de tráfico de la red.

Para lograr esto, es necesario contar con UTM - Unified Threat Management que les permita segmentar la red interna y la creación de políticas de control de acceso al tráfico con certificados de inspección en tiempo real de vulnerabilidades existentes a nivel mundial con el fin de proteger los activos digitales 24/7 de la organización, contemplando todos los frentes: despliegue, estrategia, optimización y gestión para que opere con tranquilidad y asi resguardar la estabilidad y continuidad del negocio.

Igualmente es necesario de la tener presente los IDS (Intrusion Detection System) que permitiría identificar de manera reactiva los accesos no autorizados a una estación de trabajo y la red, ya que son sistemas que monitorean y cotejan el tráfico entrante con la base de datos actualizada de ataque conocidos. Ante cualquier actividad sospechosa, emiten una alerta anticipatoria de posible intrusión para tomar las medidas oportunas, pero no mitigan la intrusión.

Además de se puede contemplar los IPS (Intrusion Prevention System) ya que es un software utilizado para proteger los ataques e intrusiones, acompañados de acciones preventivas, al ejecutar análisis en tiempo real del tráfico y los protocolos para anticipar a un posible evento de incidente de seguridad, identifica ataques según anomalías, patrones o comportamientos y permitiendo el control del tráfico entrante y saliente de la red.

Otra solución serían los SIEM (Security Information and Event Management) ya que es alternativa híbrida centralizada que conectan tres (3) sistemas (LMS): es el encargado de la administración centralizada de logs de los activos informáticos, SIM: es el encargado de la recolección de logs y su almacenamiento a largo plazo con prácticas de análisis y reporte de los datos y SEM es el encargado de administrar los eventos de seguridad, permitiendo monitorear en tiempo real.

Estas herramientas les permiten a los equipos BlueTeam y RedTeam, la opción de prepararse y enfrentarse, de forma pasiva (automatizada) ó de forma activa por las amenazas a las vulnerabilidades que afecten el buen funcionamiento de las tecnologías e información, ya que ayudan a detectar en tiempo real las intrusiones con el fin de neutralizarlas

5.8. ASPECTOS LEGALES A TENER EN CUENTA POR PARTE DE LOS GRUPOS DE TRABAJO RED TEAM Y BLUE TEAM

Los equipos Red Team y Blue Team, en general, deben tener en cuenta los siguientes aspectos legales:

- Consentimiento informado: Antes de ejecutar cualquier tipo de prueba de seguridad y/o pentesting, es necesario obtener permisos de la organización o cliente para ejecutar dicha prueba.

- Limitaciones legales: Deben estar familiarizados con las normatividades vigentes que se aplican a las pruebas de seguridad, para evitar cometer cualquier delito.

- Protección de datos: Deben ser consciente de las leyes de protección de datos y asegurarse de no utilizar información personal o confidencial durante el testeo.

- Propiedad intelectual: Deben asegurarse de no infringir la propiedad intelectual de la organización durante la realización de pruebas de intrusión.

- Confidencialidad: Mantener la confidencialidad de la información obtenida durante las pruebas de seguridad, especialmente si se trata de información sensible.

- Responsabilidad: Deben ser responsables de sus acciones para no causar daños a la organización durante la realización de pruebas de intrusión.

En general, es importante que tanto el equipo Red Team como el Blue Team estén informados y actualizados sobre las normatividades aplicables a su trabajo. Igualmete, es recomendable que las organizaciones contraten a profesionales legales para asegurarse de que todo se realiza de acuerdo a la ley.

5.9. SUSTENTA EL DESARROLLO DE SEMINARIO ESPECIALIZADO MEDIANTE VIDEO DONDE SE PUEDA EVIDENCIAR ROSTRO DE LE ESTUDIANTE CON UNA DURACIÓN MÍNIMA DE 8 MINUTOS, EL ESTUDIANTE DEBERÁ HACER PÚBLICO EL VÍDEO HACIENDO USO DE ALGUNA PLATAFORMA CLOUD O EN YOUTUBE.

https://www.youtube.com/playlist?list=PLEnrPrGJOZxOYp0URmvYO3J2BCeryYfQV

6. CONCLUSIONES

Las organizaciones en el escenario actual de modernización tecnológica y automatización de procesos rutinarios que ayuda a mejorar la producción y agilidad en su ejecución, están enfrentados día a día a una gran amenaza que atenta contra la continuidad y operación del negocio, para mejorar y mitigar estas situaciones se debe tener un equipo de acción inmediata ó preventiva para contrarrestar las amenazas.

Los equipos de BlueTeam y RedTeam son los encargados en gestionar la seguridad informática de la organización haciendo análisis y auditoria con el fin de fortalecer las acciones en conjunto para mitigar los riesgos inminentes que se encuentra diariamente. Estos equipos deben ser conformados por personal idóneo con el fin de salvaguardar cualquier vulnerabilidad que se presente en los parámetros de los entornos físicos y lógicos.

Además de tener claridad en la normatividad vigente para permita ejecutar sus acciones dentro del marco de la ley y con el consentimiento de las pruebas de intrusión que se puedan ejecutar.

7. RECOMENDACIONES

De acuerdo a la dinámica de los avances tecnológicos que exigen los ciudadanos en todo el mundo para que las empresas se modernicen y automaticen sus procesos para hacer más ágil y recuperar el tiempo perdido, es necesario que se invierta en seguridad digital debido a los grandes vulnerabilidades en las tecnologías que se desarrollan que son creados por humanos que igualmente puede comerte errores en su desarrollo, es por esto que las organización debe estar preparadas con la adopción de políticas, implementación de software y hardware que ayude a mitigar el impacto ante un ataque cibernético el cual podría comprometer el activo más importantes, la información.

Se recomienda hacer uso de herramientas que ayuden a monitorizar el trafico sospechoso en la red con el fin de ejecutar acciones preventivas para evitar tener vulnerabilidades activas y permita el ingreso de un ataque.

La retroalimentación del personal de los equipos RedTeam y BlueTeam, además de todos los funcionarios para que puedan identificar una amenaza y poder ser controlada antes de su propagación.

8. BIBLIOGRAFIA

- Ley 1581 (2012). Disposición general para la protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

- Ley 1273 (2009). se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

- MUÑOZ, Helmer, et al. Informática forense y auditoría forense: Nuevas perspectivas en tiempos de COVID-19. (2020). http://w.revistaespacios.com/a20v41n42/a20v41n42p32.pdf

- Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

- MAYORGA, Andrés Muñoz,. Pentesting sobre aplicaciones web basado en la metodología OWASP utilizando un cluster conformado por dispositivos SBC de bajo costo. Revista Ibérica de Sistemas e Tecnologias (2018). https://search.proquest.com/openview/dbbd49840c44c5de39b3c29c7f68c586/1?pq-origsite=gscholar&cbl=1006393

- Añazco Bedón, JD (2021). Sistema de gestión de eventos e información de seguridad (SIEM) de la infraestructura tecnológica de la Universidad Internacional SEK del Ecuador. https://repositorio.uisek.edu.ec/handle/123456789/4385

- Vulnerabilidad findMacroMarker en Rejetto (CVE-20146287). (2014). https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

- Revista Seguridad. (2018). Pruebas de penetración: Explotando una vulnerabilidad con Metasploit Framework. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

- ERROR 80072EFE de Windows Update Windows 7 NO ACTUALIZA ⊳ SOLUCIÓN (2022). https://www.youtube.com/watch?v=j5Eps87j0oA

- Ley 842 (2003). Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Etica Profesional y se dictan otras disposiciones. https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

- Basic Exploitation with Metasploit: Windows: HTTP File Server, (2021), https://www.youtube.com/watch?v=YQUcyQ4WT6w

- Cavelty, M. D. (2010). Cyber-security. In The Routledge handbook of new security studies (pp. 154-162). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780203859483-19/cyber-security-myriam-dunn-cavelty

- BACUDIO, Aileen G., et al. An overview of penetration testing. International Journal of Network Security & Its Applications, (2011). https://search.proquest.com/openview/911a51c6546eb7400e083f17edca89c9/1.pdf?pq-origsite=gscholar&cbl=646392

- HERNÁNDEZ, Miguel, et al. Approach to the State of the Art of Ciberdelincuence in Colombia. International Journal of Applied Engineering Research, (2018). https://www.researchgate.net/profile/Miguel-Hernandez-Bejarano/publication/331718784_Approach_to_the_State_of_the_Art_of_Ciberdelincuence_in_Colombia/links/6108b3c41e95fe241aa5bae3/Approach-to-the-State-of-the-Art-of-Ciberdelincuence-in-Colombia.pdf.

- NAJERA-GUTIERREZ, Gilberto; ANSARI, Juned Ahmed. *Web Penetration Testing with Kali Linux:*. Packt Publishing Ltd, (2018). https://books.google.com.co/books?hl=es&lr=&id=yulODwAAQBAJ&oi=fnd&pg=PP1&dq=kali+linux+penetration+testing&ots=oWBctI4TKF&sig=8oUT3JBcAzN8ga5YUzEvJAdmJTk