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

CARLOS WILBER FRANCO VELASCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

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

CARLOS WILBER FRANCO VELASCO

Director:
JOHN FREDDY QUINTERO

Tutor:
LUIS FERNANDO ZAMBRANO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

CONTENIDO

pág.

LISTA DE FIGURAS

GLOSARIO

BLUE TEAM: equipo de una empresa u organización, encargado de velar por la seguridad informática de manera defensiva y proactiva.

CSIRT: siglas en inglés “Computer Security Incident Response Team”, es el equipo de respuesta a incidentes de seguridad informática.

CVE: siglas en inglés para “Common Vulnerabilities and Exposures”, es una lista de fallas de seguridad informática conocidas.

DELITO INFORMÁTICO: conducta punible en la que el sujeto activo utilice método o técnica de carácter informático en su ejecución.

EXPLOIT: es un código o programa informático que aprovecha una vulnerabilidad para comprometer la seguridad de un sistema.

EXPLOITDB: apocope de Exploit Database, es una de las bases de datos de exploits gratuitas más populares en internet.

EXPLOTACION: hacer efectiva la vulnerabilidad de un sistema informático.

FIREWALL: es un dispositivo o también un software, encargado de monitorear el tráfico de una red o equipo.

HACKER: persona con altos conocimientos en informática, que utiliza sus conocimientos para superar obstáculos en un sistema.

HARDENIZACIÓN: conjunto de técnicas, disciplinas o procedimientos, que consisten en reducir las superficies de ataque de los sistemas.

HIDS: siglas en inglés para “Host Intrusion Detections System” o sistema de detección de intrusos.

INTRUSION: es el acceso a un sistema informático de manera no autorizada utilizando para tal fin una vulnerabilidad detectada.

METASPLOIT: herramienta de código abierto que ofrece recursos para desarrollar códigos e investigar vulnerabilidades de seguridad

NESSUS: aplicación utilizada por administradores de red y pentesters para escanear y detectar las vulnerabilidades presentadas en las redes y los equipos que la componen.

OPENVAS: es un escáner de vulnerabilidades WEB mantenido y distribuido por Greenbone Networks.

PENTESTING: abreviatura de “Penetration Testing”, o prueba de penetración, es un ataque a un sistema informático destinado a encontrar vulnerabilidades.

PHISHING: es un tipo de ataque informático que suplanta una página web o aplicación, con el fin de robar datos personales.

RED TEAM: es un equipo de seguridad informática de una empresa u organización encargada de simular ataques informáticos a la misma, para encontrar vulnerabilidades

VULNERABILIDAD: es un fallo de seguridad en un sistema informático que puede ser utilizado para comprometer el equipo o infraestructura tecnológica.

RESUMEN

Este documento presenta un informe técnico, de las actividades realizadas en el "Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team" el cual se ha desarrollado como opción de grado, para optar por el título de "Especialista en Seguridad Informática" de la Universidad Nacional Abierta y a Distancia UNAD; en el cual se conocieron temas como concepto de equipos de seguridad Red Team y Blue Team y su actuación ética y legal, en donde se aprendió la normatividad vigente sobre delitos informáticos en Colombia, además se realizó ejercicios de pentesting como desarrollo a escenarios propuestos de actuación de equipos Red Team, en un entorno virtualizado y controlado, y la respuesta de su contraparte el Equipo Blue Team, además se aprendió sobre algunas herramientas existentes, para la ejecución de detección de vulnerabilidades como Nessus, también herramientas para efectuar pruebas de penetración como Metasploit Framework y algunos de sus módulos, esto aplicado a un entorno controlado con máquinas virtuales y algunas vulnerabilidades conocidas en una de las maquinas, simulando ataques de intrusión mediante un sistema operativo Kali Linux.

INTRODUCCION

Este trabajo escrito, es el desarrollo de la actividad de la “Etapa 5 – socialización informe técnico”, el cual corresponde a la evaluación final del Seminario Especializado: Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team, en donde se realiza un recorrido de los aspectos más importantes desarrollados durante el seminario y se aporta unas recomendaciones y conclusiones importantes para la construcción de teoría concerniente a la temática analizada; se aborda una extracción de los conceptos más importantes del desarrollo del seminario, entre los cuales se encuentra, el análisis de la normatividad vigente, relacionada con delitos informáticos y protección de datos personales, además de las actuaciones éticas por parte de los equipos Red Team y Blue Team, por otra parte se abordaron tópicos enfocados al conocimiento de las fases del pentesting o pruebas de penetración, orientadas a la ejecución de ataques en entornos controlados, y la contención de los mismos, además del conocimiento de las herramientas existentes para este tipo de actividades.

OBJETIVOS

OBJETIVO GENERAL

Formular estrategias de mitigación de los riesgos en un sistema informático mediante el análisis de las vulnerabilidades en una infraestructura de tecnología.

OBJETIVOS ESPECÍFICOS

Proponer Aspectos que aporten al desarrollo de estrategias de los equipos Red Team y Blue Team.

Emitir sugerencias para el trazado de estrategias que permitan fortalecer la seguridad tecnológica en una organización

Aportar conclusiones que coadyuven a la construcción del conocimiento desde el enfoque de la ciberseguridad.

1. LEGISLACIÓN COLOMBIANA SOBRE DELITOS INFORMÁTICOS Y DATOS PERSONALES

Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación “leyes, decretos” existen actualmente y las características principales de cada ley.

Con la evolución del conocimiento de la humanidad, y su consiguiente proceso de crecimiento tecnológico, se puede percibir que de forma paralela también se incrementa esa manifestación de la conducta social del hombre de querer transgredir los bienes reconocidos de manera individual y colectiva; en este contexto, se genera de manera constante una necesidad latente de establecer normas, prohibiciones y restricciones, que no solo protejan esos bienes jurídicos establecidos, sino que también se adapten de manera secuencial al comportamiento evolutivo de sociedad, y en este sentido el derecho como ciencia social ha debido estar en sincronía con las ciencias y la tecnología y su cambio o desarrollo evolutivo, en consecuencia, podemos decir que de manera universal la información es un bien reconocido, y esta debe ser jurídicamente protegido, al igual que las herramientas que permiten su creación, manejo, transporte y almacenamiento; es viable en este momento citar el concepto de informática, como “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores” (Diccionario de la Real Academia Española, DRAE), y traigo esta reseña a colación, dado que se hace necesario para comprender de una manera más amplia el contexto de delitos informáticos; según Henry William Torres abogado de la Universidad Católica de Colombia Magister en Teleinformática, el delito informático se define como: “Toda conducta punible en la que el sujeto activo utilice método o técnica de carácter informático en su ejecución que tenga como medio o instrumento elementos integrantes de un sistema informático o telemático o intereses jurídicos tutelados por el derecho a la intimidad, a la propiedad intelectual y el software a que sin estar reconocida por nuestro legislador es aceptada por tratadistas internacionales como Infracción Informática”[1]

1.1 LEY 1273 DEL 5 DE ENERO DE 2009

La Ley 1273 es la norma 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

[1] OJEDA, Jorge, RINCON, Arias, Delitos informáticos y entorno jurídico vigente en Colombia. Cuad. Contab. [online]. 2010, vol.11, n.28, pp.41-66. ISSN 0123-1472, http://www.scielo.org.co/scielo.php?pid=S0123-14722010000200003&script=sci_abstract&tlng=es

de los datos"[2] - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Esta Ley adiciona al Código Penal el Título VII BIS, el cual se titula "De la Protección de la información y de los datos", y consta de dos capítulos con los siguientes artículos:

- Capitulo primero: "de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos".
    - Artículo 269a. "acceso abusivo a un sistema informático".
    - Artículo 269b. "Obstaculización ilegítima de sistema informático o red de telecomunicación".
    - Artículo 269c. "Interceptación de datos informáticos".
    - Artículo 269d. "Daño informático".
    - Artículo 269e. "Uso de software malicioso".
    - Artículo 269f. Violación de datos personales.
    - Artículo 269g. "Suplantación de sitios web para capturar datos personales".
    - Artículo 269h. "Circunstancias de agravación punitiva".
- Capitulo segundo: "de los atentados informáticos y otras infracciones"
    - Artículo 269i. "Hurto por medios informáticos y semejantes".
    - Artículo 269j: "transferencia no consentida de activos".

[2] Ley 1273 de 2009, De la Protección de la información y de los datos, 5 de enero de 2009, D.O. No. 47.223 (Colombia) http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

1.2 LEY 1266 DE 2008 QUE DEFINE LAS CLASES DE DATOS DE CARÁCTER PERSONAL

Mediante esta Ley, "se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".[3]

1.3 LEY 1581 DE 2012 QUE ESTABLECE PARÁMETROS PARA EL TRATAMIENTO DE DATOS PERSONALES

Mediante esta ley, "se dictan disposiciones generales para la protección de datos personales. Establece unas categorías especiales de datos personales, como lo son los datos sensibles y lo datos personales de los niños, niñas y adolescentes".[4]

1.4 DECRETO 1377 DEL 27 DE JUNIO DE 2013

Mediante este Decreto, el Ministerio de Comercio, Industria y Turismo, "reglamenta parcialmente la Ley 1581 de 2012, y se dictan disposiciones generales para la protección de datos personales".[5]

1.5 CIRCULAR EXTERNA 014 DE 17 DE ABRIL DE 2008

Mediante esta Circular, "la Superintendencia Financiera de Colombia regula la Información sobre Transacciones efectuadas a través de los canales de distribución dispuestos por las entidades vigiladas".[6]

---

[3] Ley 1266 de 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, diciembre 31 de 2008, D.O. 47.219 (Colombia), https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488#:~:text=por%20la%20cual%20se%20dictan,y%20se%20dictan%20otras%20disposiciones.

[4] Ley Estatutaria 1581, Disposiciones generales para la protección de datos personales, D.O. 48.587, (Colombia), http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

[5] Decreto 1377, Reglamenta Ley 1581 de 2012, "Tratamiento de datos personales", 27 de junio de 2013, D.O. 48834 MINTIC, (Colombia), https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

[6] Circular Externa 014, Superintendencia Financiera de Colombia, información detallada sobre las transacciones, 17 de abril de 2008, https://www.superfinanciera.gov.co/inicio/normativa/normativa-general/circulares-externas-cartas-circulares-y-resoluciones-desde-el-ano-/circulares-externas/-20146

1.6 DECRETO 1360 DE 23 DE JUNIO DE 1989

Mediante este decreto, "el Gobierno Nacional, define algunos términos y reglamenta la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor".[7]

2 FASES DE UN TEST DE PENETRACIÓN

A continuación, se exponen los pasos o etapas que todo experto en ciberseguridad o miembro de un equipo dedicado a la seguridad digital de una empresa u organización debe aplicar para una correcta ejecución de lo que comúnmente se conoce como prueba de penetración o pentesting.

2.1 FASE DE RECOLECCIÓN DE INFORMACIÓN

La fase de recolección de información o también llamada fase de reconocimiento, está enfocada en obtener la mayor cantidad de información del objetivo, la cual se utilizará al realizar las pruebas de intrusión durante las fases de búsqueda y posterior explotación de las vulnerabilidades, en esta fase se debe obtener la mayor cantidad de información posible, con el ánimo de conocer todos los vectores de ataque que puedan hacer vulnerable el objetivo.

2.1.1 Inteligencia de código abierto (OSINT)

La inteligencia de código abierto (OSINT) es una forma de gestión de recopilación de información que implica encontrar, seleccionar y adquirir información de fuentes disponibles públicamente y analizarla para producir inteligencia o información procesable.

Las fuentes OSINT se pueden dividir en seis categorías diferentes de flujo de información:

- Medios de comunicación, periódicos impresos, revistas, radio y televisión.

[7] Decreto 1360, reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor, 23 de junio de 1989, D.O. 38.871, (Colombia), https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=10575

- Internet, publicaciones en línea, blogs, grupos de discusión, redes sociales como YouTube Facebook, Twitter, Instagram, etc.).

- Datos públicos de entidades gubernamentales, datos prensa, discursos, informes gerenciales, presupuestos, audiencias, directorios telefónicos o sitios web; se puede entender que estas fuentes son de uso oficial, pero son utilizables, por estar abiertas al público.

- Publicaciones académicas y profesionales, revistas, simposios, trabajos académicos, conferencias, tesis, monografías, entre otras.

- Datos e imágenes comerciales, estimaciones industriales y financieras, y bases de información empresariales.

- Lo que comúnmente se denomina literatura gris, patentes, boletines, informes técnicos, trabajos escritos, documentos comerciales, trabajos inéditos, etc.

Se debe tener en cuenta que OSINT puede no ser preciso u oportuno, dado que las fuentes de información pueden manipularse de forma deliberada o accidental para reflejar datos erróneos, la información puede volverse obsoleta con el paso del tiempo o simplemente estar incompleta.[8]

2.1.2 Aspectos a tener en cuenta en la fase de recolección de Información

2.1.2.1 Selección de objetivo

En esta etapa se Identifica y se da una denominación al objetivo, comprendiendo el alcance de la auditoria, el domino de la empresa u organización, la duración de las pruebas y el objetivo final.

2.1.2.2 Tipo de Información a recolectar

- Información Corporativa

  - Información sobre Instalaciones Físicas
  - Información Lógica

[8] WIKIMEDIA FOUNDATION, Inc, Open-source intelligence, consultado el 22 de febrero de 2022, recuperado de: https://en.wikipedia.org/wiki/Open-source_intelligence

- Organigrama
- Información Electrónica
- Activos de Infraestructura
- Información Financiera

- Información Individual

Empleados: Hojas de Vida, perfiles en redes sociales, presencia en internet, localización física, informaciones de pago

Algunas herramientas a destacar en la fase de recolección de información son:

Nmap (escaneo de puertos).
FOCA (análisis de metadatos).
PassiveRecon (para webs).

2.2 FASE DE BÚSQUEDA DE VULNERABILIDADES

2.2.1 Modelado de Amenazas

Para una empresa u organización es muy importante la clasificación de sus activos de información, y por lo tanto, se debe tener en cuenta estas prioridades al momento de la ejecución de las pruebas de penetración, establecer un modelo de amenazas acorde a la priorización establecida por la compañía, permite enmarcar rutas de acción adecuadas a los objetivos y controles establecidos.

Para un proceso de modelado de amenazas, se requiere las siguientes acciones:

- Reunir la documentación pertinente.
- Identificar y categorizar activos primarios y secundarios.
- Identificar y categorizar amenazas y vectores de amenaza.
- Mapear los vectores de amenaza contra activos primarios y secundarios.

2.2.2 Análisis de Vulnerabilidades

Paso seguido al modelado de amenazas se requiere, el análisis de vulnerabilidades, el cual consta de pruebas activas y pasivas, la validación y la investigación:

Un atacante puede vulnerar de muchas maneras un sistema informático, por esta razón, se hace necesario la búsqueda y enumeración de las fallas que se puedan presentar en dicho sistema, estas fallas pueden variar desde malas configuraciones,

aplicaciones mal diseñadas, puertos y servicios mal configurados, entre muchas otras, cabe anotar que existen muchos procesos diferentes para la realización de este tipo de análisis, algunos técnicos y otros manuales, y la aplicación de uno u otro método depende del componente particular que está siendo objeto de análisis.

2.2.3 Pruebas Activas

Según The PTES team, "Las pruebas activas implican una interacción directa con el componente que se está probando en busca de vulnerabilidades de seguridad. Estos podrían ser componentes de bajo nivel, como la pila TCP en un dispositivo de red, o podrían ser componentes más altos en la pila, como la interfaz basada en web utilizada para administrar dicho dispositivo"[9]

2.2.4 Pruebas Pasivas

Este tipo de prueba no representa una interacción directa con los componentes a analizar, sino una observación de información registrada en algún lugar determinando, como por ejemplo los metadatos, configuraciones de clusters entre otros.

2.2.5 Validación

Correlación entre Herramientas

Existen dos formas de correlación que se deben utilizar cuando se abaja con distintas herramientas, la correlación específica y la correlación categórica de los elementos, ambos son útiles según el tipo de información, métrico y estadístico que intenta recopilar en un objetivo determinado.

La correlación específica se relaciona con un problema definible específico, como ID de vulnerabilidad, CVE, OSVDB, números de indexación de proveedores, problema conocido con un producto de software, etc. y se puede agrupar con micro factores como nombre de host, IP, FQDN, dirección MAC, etc. un ejemplo de esto sería agrupar los resultados del host x por número de CVE, ya que indexarían el mismo problema en varias herramientas.

La correlación categórica se relaciona con una estructura para problemas tales como marcos de cumplimiento (es decir, NIST SP 800-53, DoD 5300 Series, PCI,

[9] The PTES Team, The Penetration Testing Execution Standard Documentation , Release 1.1, Jun 16, 2021, consultado el 20 de marzo de 2022, recuperado de: https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf

HIPPA, OWASP List, etc.) que le permiten agrupar elementos por factores macro como tipos de vulnerabilidad, problemas de configuración, etc. Un ejemplo de esto sería agrupar todos los hallazgos de hosts con contraseñas predeterminadas en un grupo para complejidad de contraseña dentro de NIST 800-53 (IA-5).

Prueba manual/Protocolo específico

Fingerprinting

El Fingerprinting es útil para determinar el tipo de dispositivo VPN y la versión correcta del código liberado instalado. Al tomar con precisión las huellas dactilares del dispositivo, se pueden realizar investigaciones y análisis adecuados contra el sistema de destino.

Autenticación

Los dispositivos VPN pueden operar con varias formas de autenticación. El uso de kits de herramientas de VPN que no forman parte de las herramientas de evaluación de vulnerabilidades convencionales permite la identificación adecuada de los mecanismos de autenticación y determina las debilidades que pueden existir, como claves previamente compartidas o ID de grupo predeterminados.

Citrix

Enumeración

Muchas instalaciones predeterminadas y dispositivos Citrix mal configurados proporcionan un medio para enumerar aplicaciones publicadas y determinar nombres de usuario válidos que están configurados para autenticarse en el dispositivo. Esta información se vuelve crucial durante los ataques de fuerza bruta y los intentos de romper perfiles predefinidos para usuarios autorizados.

DNS

Una fuente importante de información para los atacantes son los sistemas de nombres de dominio los cuales pueden brindar un listado exhaustivo de posibles objetivos además de la fuga de información importante en este tipo de análisis.

Web

Los administradores pueden centrar su refuerzo en los puertos comunes para servicios web o directorios publicados y descuidar el endurecimiento adecuado de

atributos adicionales. Los servicios web siempre deben revisarse de forma manual, ya que las herramientas de evaluación automatizadas no son capaces de identificar la mayoría de las debilidades de sus servicios.

Correo

Los servidores de correo pueden proporcionar una gran cantidad de información sobre una organización de destino. Usando funciones inherentes en el dispositivo de destino, se puede realizar la confirmación de cuentas válidas, así como desarrollar una lista de posibles nombres de usuario para ataques adicionales en otros sistemas. Las vulnerabilidades, como la retransmisión de correo, se pueden aprovechar para ataques adicionales a la organización, como el phishing. A menudo, los servidores de correo proporcionarán una interfaz web para el acceso remoto que puede ser objeto de campañas de fuerza bruta.

Herramientas que automatizan más el proceso de búsqueda de vulnerabilidades son:

Acunetix y Nessus

2.3 FASE DE EXPLOTACIÓN DE VULNERABILIDADES

En esta fase el atacante busca como su nombre lo indica, explotar las vulnerabilidades encontradas, lograr efectuar el ingreso al sistema comprometido, esto dependiendo de la fase anterior donde se establecieron las vulnerabilidades específicas del sistema, inicialmente los que se pretende es individualizar el punto de acceso principal, y posteriormente establecer los objetivos principales o de alto valor para la empresa u organización.

2.3.1 Contramedidas

Las contramedidas estas definidas como todas aquellas tecnologías que de una u otra forma impiden la ejecución efectiva del ataque o de la explotación de la vulnerabilidad, por ejemplo, un sistema de detección de intrusiones con base en el host, por lo anterior, es pertinente la ejecución de alternativas que permitan la explotación de la vulnerabilidad.

De manera general, el propósito es permanecer sigiloso cuando se realiza el ataque, evitando disparar las alarmas, a costo de que el nivel de la evaluación podría disminuir. Si es posible, las contramedidas se deben enumerar antes de la activación del exploit.

2.3.2 Evasión

La Evasión consiste en la utilización de mecanismos que permitan eludir las técnicas de seguridad de los sistemas, como por ejemplo los “sistemas de Detección de intrusos o IDS”, “los sistemas de prevención de intrusiones” o los firewalls, básicamente se debe establecer el mínimo riesgo para la evasión de estas tecnologías.

2.3.3 Ruta de Explotación Personalizada

Dependiendo de cada vulnerabilidad, el ataque debe ser pertinentemente preparado para lograr una efectividad elevada, no todos los exploits funcionan a cualquier vulnerabilidad, por lo tanto estos deben adaptarse dependiendo de cada escenario específico.

Por ejemplo, si se realiza una prueba de penetración inalámbrica y se está utilizando una tecnología específica, es necesario identificarlos y atacarlos en función de las tecnologías existentes. Tener una comprensión clara de cada escenario y la aplicabilidad de un exploit es uno de los atributos más importantes de esta fase del pentesting.

2.3.4 Ángulo de día cero

En ciertos escenarios, la investigación puede llevarse a cabo para realizar ingeniería inversa, fuzzing o realizar un descubrimiento avanzado de vulnerabilidades que no se han descubierto. En caso de que este tipo de ataque sea aplicable, asegúrese de que se reproduzca el entorno según el mejor conocimiento de los atacantes para incluir tecnología de contramedidas.

Para que los exploits de día cero tengan éxito (o cualquier exploit), tener el mismo sistema operativo, parches y contramedidas es muy importante para el éxito. A veces, esta información puede no estar disponible según el nivel de acceso o enumeración que se haya producido.

2.3.5 Ejemplos de vías de ataque

En cualquier escenario, se debe tener en cuenta las formas específicas para la explotación de las vulnerabilidades; A continuación, se muestra una lista de varias vías de ataque a considerar según el escenario, pero de ninguna manera es una lista completa.

Ataques a aplicaciones web, Ingeniería social, Vías de ataque físico, Exploits basados en la memoria, Hombre en el medio, Salto de VLAN, Implementación de USB/Flash Drive, Ingeniería inversa, Ángulo de día cero, Ataque al usuario, Cifrado, Cracking, Unidad de procesamiento de gráficos (GPU), Análisis de tráfico, Firewire, Protocolos de enrutamiento, Phishing.

Una vez más, estos ejemplos son solo vías básicas de ataque basadas en el escenario que está realizando para la organización. El valor de una prueba de penetración proviene de la creatividad y la capacidad de identificar exposiciones y explotarlas de manera precisa.

Una herramienta a destacar en la fase de explotación es Metasploit Framework

2.4 FASE DE POST EXPLOTACIÓN

El principal objetivo de la fase de post explotación es la de mantener en control de una máquina que logramos vulnerar para su uso futuro, además de analizar el valor que tiene esta máquina dentro de la infraestructura, para aprovechar nuevas vulnerabilidades y realizar un escalamiento y comprometer otros equipos en la red.

El propósito de la fase posterior a la explotación es determinar el valor de la máquina comprometida y mantener el control de la máquina para su uso posterior. El valor de la máquina está determinado por la sensibilidad de los datos almacenados en ella y la utilidad de la máquina para comprometer aún más la red. Los métodos descritos en esta fase están destinados a ayudar al pentester a identificar y documentar datos confidenciales, identificar ajustes de configuración, canales de comunicación y relaciones con otros dispositivos de red que se pueden usar para obtener más acceso a la red y configurar uno o más métodos de acceder a la máquina en un momento posterior.

3 HERRAMIENTAS DE CIBERSEGURIDAD

A continuación, se describirán algunas de las herramientas más utilizadas en las diferentes fases de la una prueba de intrusión o pentesting.

3.1 METASPLOIT

Metasploit es una herramienta de código abierto que ofrece recursos para desarrollar códigos e investigar vulnerabilidades de seguridad. Permite a los

administradores de red reconocer las amenazas de seguridad para romper su red y también documentar qué vulnerabilidad deben definirse primero.

Es un tipo de proyecto que facilita el software de prueba Pen (Penetración). Además, ofrece herramientas para automatizar la comparación de una vulnerabilidad de un programa y su versión parcheada (reparada). También ofrece herramientas avanzadas de evasión y anti-forense. Algunas de estas herramientas se crean en el marco de Metasploit.

3.1.1 Metasploit Framework

Metasploit Framework es un entorno de software para desarrollar, probar y ejecutar exploits. Podría usarse para crear herramientas para pruebas de seguridad, explotar módulos y como un sistema de prueba de penetración. Originalmente, fue desarrollado en 2003 como una herramienta de red móvil por HD Moore. Este marco es una herramienta muy fuerte. Puede ser aplicado por Hackers Eticos y ciberdelincuentes para sondear susceptibilidades sistemáticas en servidores y redes. Debido a que es un marco de código abierto, se puede usar y personalizar fácilmente con varios sistemas operativos. El grupo de pruebas de penetración puede aplicar código personalizado o prefabricado y abordarlo en una red para detectar puntos débiles con Metasploit. Una vez que las fallas se documenten e identifiquen como otro tipo de caza de amenazas, la información podría usarse para priorizar soluciones y abordar las debilidades sistémicas.[10]

3.1.2 VENTAJAS DE METASPLOIT

- Código abierto

Se desarrolla activamente y el código abierto es la razón más importante por la que preferimos Metasploit. Existen varias otras herramientas pagas para llevar a cabo el proceso de prueba de penetración. Sin embargo, Metasploit permite a los usuarios agregar sus módulos personalizados y acceder a su código. La versión Metasploit Pro es de pago, aunque, en aras de ganar, se prefiere principalmente la edición comunitaria.

[10] JAVA T POINT, s.f., What is Metasploit, consultado el 5 de marzo de 2022, recuperado de: https://www.javatpoint.com/what-is-metasploit

- Convención de nomenclatura fácil y soporte para probar redes grandes

Metasploit es fácil de usar. Sin embargo, aquí esta característica define las convenciones de nomenclatura fáciles de muchos comandos. Metasploit facilita la construcción de una gran red de pruebas de penetración. Por ejemplo, supongamos que tenemos que probar cualquier red que tenga 200 sistemas. En lugar de probar todos los sistemas uno por uno, Metasploit puede probar todo el rango automáticamente.

Con parámetros como Classless Inter-Domain Routine (abreviatura de CIDR) y valores de subred, Metasploit puede probar todos los sistemas para explotar la susceptibilidad. Sin embargo, en cualquier método de explotación manual, es posible que necesitemos definir los exploits en 200 sistemas manualmente. Por lo tanto, Metasploit está ahorrando una gran cantidad de energía y tiempo.

- Entorno de GUI

Metasploit proporciona instancias de terceros y una GUI amigable como Armitage . Estos tipos de interfaces pueden facilitar los proyectos de pruebas de penetración al facilitar servicios como funciones con un clic de botón, gestión de vulnerabilidades sobre la marcha y espacios de trabajo fáciles de cambiar.

- Salidas más limpias

Metasploit puede hacer una salida más limpia a través de un sistema. Es un aspecto importante si sabemos que este servicio no se reiniciará inmediatamente. Además, brinda muchas funciones para la explotación posterior, como la persistencia, que podría ayudar a mantener el acceso a un servidor de forma permanente.

3.2 NMAP

Nmap es una herramienta de exploración de red que utiliza paquetes IP para identificar todos los dispositivos conectados a una red y proporcionar información sobre los servicios y sistemas operativos que se ejecutan.

El programa se usa más comúnmente a través de una interfaz de línea de comandos (aunque también hay interfaces GUI disponibles) y está disponible para muchos sistemas operativos diferentes, como Linux, Free BSD y Gentoo. Su popularidad

también se ha visto reforzada por una comunidad de soporte de usuarios activa y entusiasta.[11]

Nmap fue desarrollado para redes de escala empresarial y puede escanear a través de miles de dispositivos conectados. Sin embargo, en los últimos años Nmap está siendo utilizado cada vez más por empresas más pequeñas. El auge de IoT, en particular, ahora significa que las redes utilizadas por estas empresas se han vuelto más complejas y, por lo tanto, más difíciles de proteger.

Esto significa que Nmap ahora se usa en muchas herramientas de monitoreo de sitios web para auditar el tráfico entre servidores web y dispositivos IoT. La reciente aparición de botnets de IoT, como Mirai, también ha estimulado el interés en Nmap, sobre todo por su capacidad para interrogar a los dispositivos conectados a través del protocolo UPnP y para resaltar cualquier dispositivo que pueda ser malicioso.

3.3 OPENVAS

El Sistema abierto de evaluación de vulnerabilidades (OpenVAS) es un escáner de vulnerabilidades mantenido y distribuido por Greenbone Networks. Está destinado a ser todo en uno con una variedad de pruebas integradas y una interfaz web diseñada para configurar y ejecutar escaneos de forma rápida y sencilla, al mismo tiempo que proporciona un alto nivel de capacidad de configuración para el usuario.[12]

3.3.1 Características principales de OPENVAS

Escaneo concurrente de múltiples nodos.
Soporte SSL.
Soporte para WMI.
Escaneo automático temporizado.
Reportes en múltiples formatos (XML, HTML, LaTeX, entre otros)
Servidor web integrado.
Multiplataforma.
i18n.

[11] PETTERS, Jeff, Varonis, Inside Out Security, Data Security, consultado el 5 de marzo de 2022, recuperado de: https://www.varonis.com/blog/nmap-commands
[12] POSTON, Howard, Infosec, A brief introduction to the OpenVAS vulnerability scanner, consultado el 5 de marzo de 2022, recuperado de: https://resources.infosecinstitute.com/topic/a-brief-introduction-to-the-openvas-vulnerability-scanner/

3.4 EXPLOIT DATABASE (EXPLOITDB)

"Exploit Database es una de las bases de datos de exploits gratuitas más populares, conocida como 'Exploit DB'. Este proyecto de Offensive Security pretende ser una colección de exploits públicos y software vulnerable disponible para fines de investigación de vulnerabilidades y pruebas de penetración. Día a día, la lista de exploits se amplía recopilando exploits de fuentes públicas y privadas, y se presenta en una interfaz fácil de usar que permite buscar rápidamente en la base de datos. Desde esta área es posible buscar tanto exploits como aplicaciones vulnerables, e incluso crear filtros para personalizar la búsqueda por autor, tipo de plataforma, etiquetas y mucho más"[13].

3.5 CVE

Common Vulnerabilities and Exposures más conocido como CVE, "es una lista de fallas de seguridad informática conocidas, que se encuentra disponible al público. Cuando alguien habla de un CVE, se refiere a una falla a la cual se le asignó un número de identificación".[14]

Periódicamente se emiten diferentes identificadores o CVE Con el fin de permitir a los especialistas en Tecnologías de la Información, realizar coordinaciones con el ánimo de generar iniciativas de solución a las vulnerabilidades detectadas en procura de mejorar la seguridad de los equipos informáticos.

Los CVE son supervisados por MITRE Corporation, la cual es financiada por la agencia de Ciberseguridad y Seguridad de la infraestructura, que hace parte del Departamento de Seguridad Nacional de Estados Unidos.

4 MONTAJE DE UN BANCO DE TRABAJO

A continuación, se efectuará el paso a paso y explicación para el montaje de un laboratorio o banco de trabajo, el cual permitirá efectuar pruebas de penetración en un entorno controlado, permitiendo asimilar los conceptos analizados en el presente, sin tener que vulnerar la seguridad de equipos reales, ya sea en el centro educativo, trabajo o equipos personales.

[13] Exploit Database, OffSec Services Limited 2022, Exploit Database By Offensive Security, consultado el 21 de marzo de 2022, recuperado de: https://www.exploit-db.com/

[14] Red Hat, Inc., What is a CVE, consultado el 21 de marzo de 2022, recuperado de: https://www.redhat.com/en/topics/security/what-is-cve

4.1 CARACTERÍSTICAS TÉCNICAS DEL EQUIPO HOST

Para el desarrollo de esta actividad se utilizará la herramienta VirtualBox, instalada en un equipo portátil que hará las veces de Host, el cual tiene las siguientes características las cuales se pueden corroborar en la Figura 1:

Equipo portátil marca "Hewlett Packard"
Sistema Operativo "Windows 10 Home Single Language" 64 bits
Procesador Intel(R) Core (TM) i7-7500U CPU @ 2.70GHz 2.90 GHz
Memoria RAM de 16 GB

Figura 1 Especificaciones del dispositivo host

Fuente: el autor.

4.2 CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS VIRTUALIZADOS

En este banco de trabajo se virtualizarán tres máquinas con las siguientes características:

4.2.1 Equipo Virtualizado 1

Nombre: Kali - Seminario
Sistema Operativo: "Debian" (64-bits)
Memoria Base: 2048 MB

4.2.2 Equipo Virtualizado 2

Nombre: "Win7-SE2020-X64"
Sistema Operativo: "Windows 7" (64-bits)
Memoria Base: 4096 MB

4.2.3 Equipo Virtualizado 3

Nombre: “win7-SE2020”
Sistema Operativo: “Windows 7” (64-bits)
Memoria Base: 4096 MB

4.3 HERRAMIENTA DE VIRTUALIZACIÓN VIRTUALBOX

4.3.1 Descarga e instalación de VirtualBox

A. En la página https://www.virtualbox.org/wiki/Downloads se debe dar clic en “Windows hosts”, esto iniciará la descarga del instalador, ver Figura 2.

Figura 2: Descarga de VirtualBox

Fuente: el autor.

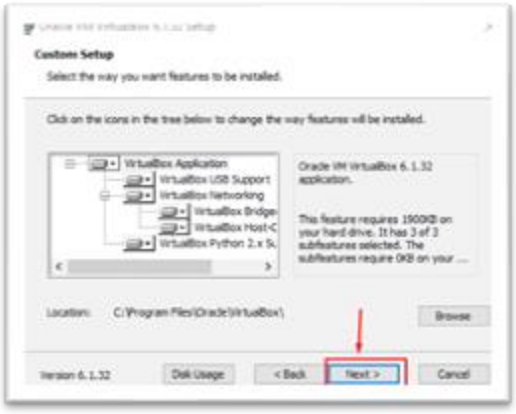
B. Una vez descargado el archivo instalador, en este caso “VirtualBox-6.1.32-149290-Win.exe”, se debe dar doble clic en él, para iniciar la instalación, y luego en el botón “Next >”, ver Figura 3.

Figura 3: Cuadro de Dialogo instalación 1

Fuente: el autor.

C. Como se puede observar en la Figura 4, en el siguiente cuadro de dialogo, se puede seleccionar algunas opciones de instalación y el directorio donde se instalará el programa, en este caso se deja todo como está y se da clic en el botón Next>.

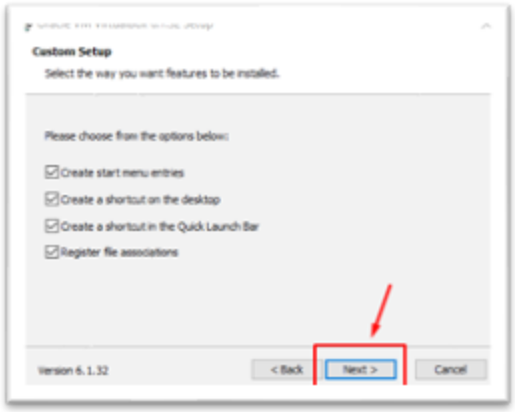
Figura 4: Opciones de Instalación



Fuente: el autor.

D. Seguido a esto, como se aprecia en la figura 5, aparece otro cuadro de configuración donde se puede seleccionar la opción de creación de iconos del programa accesos directos y asociación de archivos relacionados, en este caso se deja todo como está y se da clic en Next>.

Figura 5: Cuadro de dialogo instalación 2



Fuente: el autor.

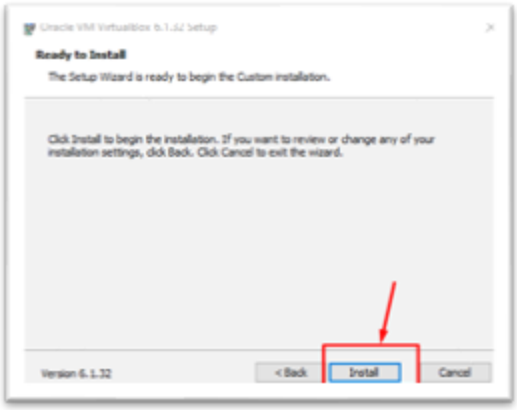
E. Ahora aparece un cuadro de dialogo, donde indica que se va a resetear la interface de red, esto con el fin de instalar la interface del programa de virtualización, ver figura 6.

Figura 6: Cuadro de dialogo estación red

Fuente: el autor.

F. Luego aparece el cuadro de dialogo que indica que se dará inicio a la instalación del programa, ver figura 7, a continuación, dar clic en “Install”.

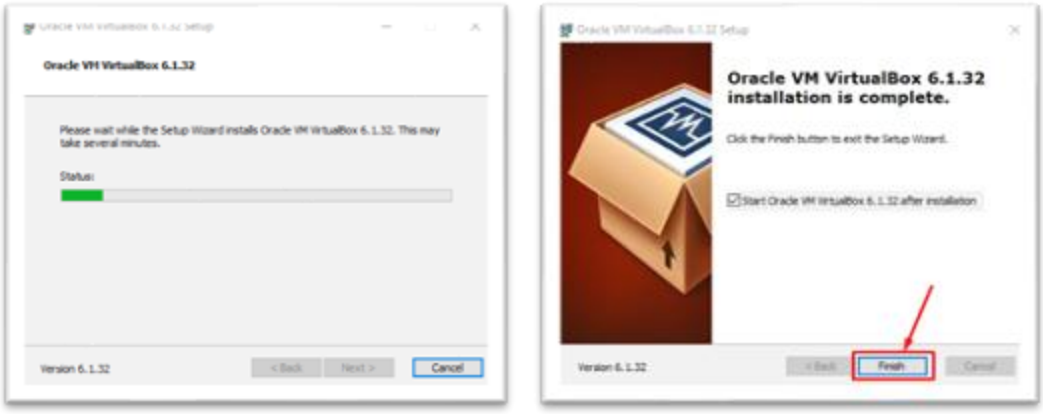
Figura 7: Cuadro de Dialogo inicio de Instalación.



Fuente: el autor.

G. Seguido a eso, se puede observar el avance de la instalación, como se observa en la figura 8, luego de terminar se debe dar clic en “Next>” para iniciar el programa VirtualBox.

Figura 8: cuadro de dialogo avance de instalación



Fuente: el autor.

H. Luego de esto aparece la pantalla principal del VirtualBox.

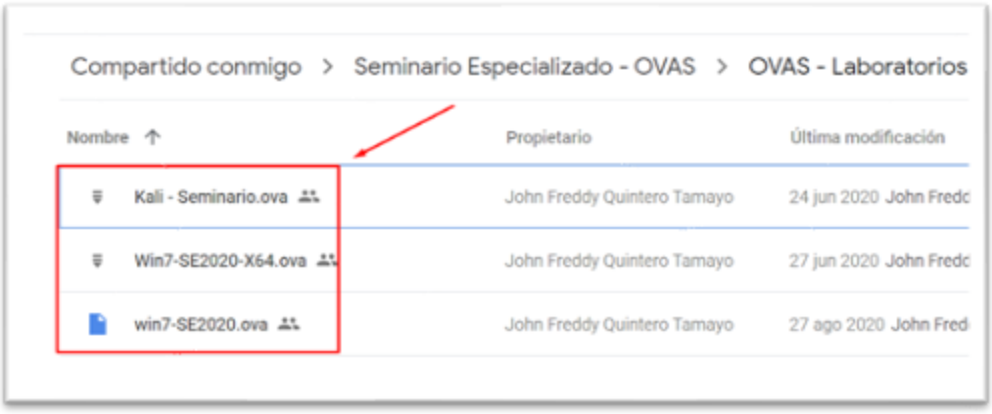
Figura 9: Ventana principal de VirtualBox

Fuente: el autor.

4.4 CREACIÓN DE LAS MÁQUINAS VIRTUALES PARA EL BANCO DE TRABAJO

A. Conforme a las indicaciones de la actividad, se descargan las máquinas virtuales suministradas por el tutor en el link: https://drive.google.com/drive/folders/1UnqXahzkNJbrnEKMnI3wF1zRMEulDwUI

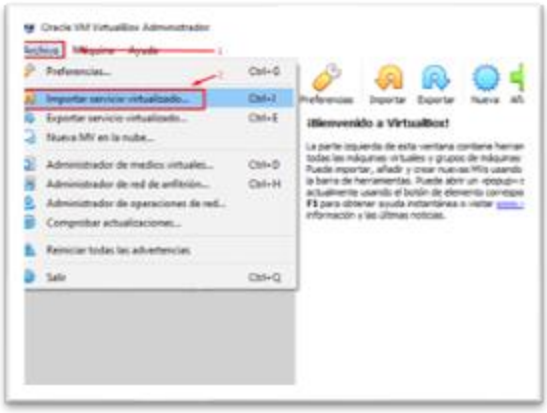
Figura 10: Descarga de máquinas virtuales



Fuente: el autor.

B. En el programa VirtualBox, se debe dar clic en “Archivo” y luego “Importar Servicio Virtualizado”.

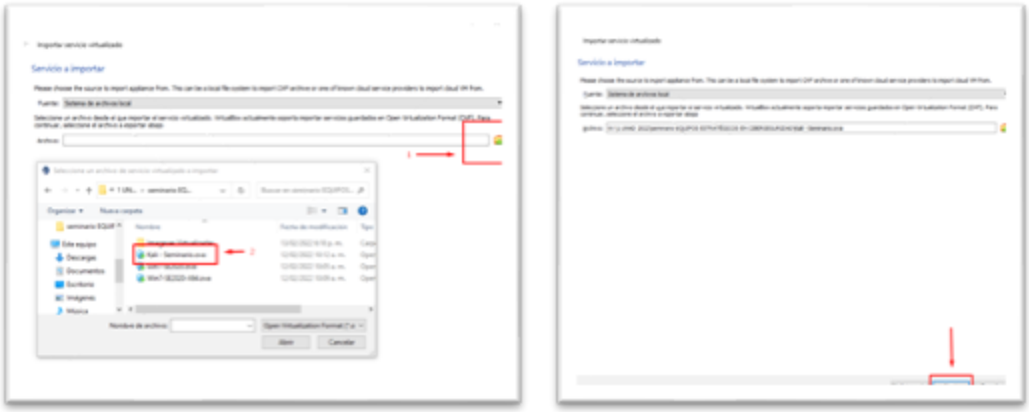
Figura 11: Importación de Servicio Virtualizado



Fuente: el autor.

C. Dar clic en el icono de la imagen, y seguido seleccionar la máquina virtual a importar, en este caso se importará la maquina “Kali – Seminario”, se debe tener en cuenta que las máquinas virtuales deben tener extensión “OVA”; Luego dar clic en “Abrir” y en el cuadro siguiente, presionar el botón “Next” como se observa en la figura 12.

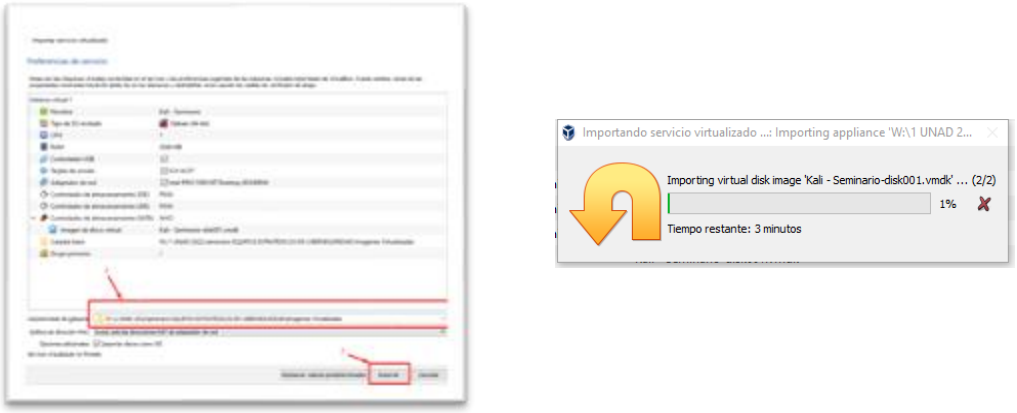
Figura 12: Importación máquinas virtualizadas



Fuente: el autor.

D. En el cuadro siguiente, se observará las características de la máquina virtual, y también es posible cambiar la ruta donde se ubicará el disco duro virtual, acto seguido se debe dar clic en “Importar” para iniciar la importación.

Figura 13: Importación



Fuente: el autor.

E. Una vez finalizada la importación, la máquina virtual estará lista para su inicialización.

Figura 14: Finalización de la importación

Fuente: el autor.

F. Con las otras máquinas virtuales, el procedimiento es exactamente el mismo que el anterior, en la figura 15 podemos observar las máquinas virtuales ya importadas.

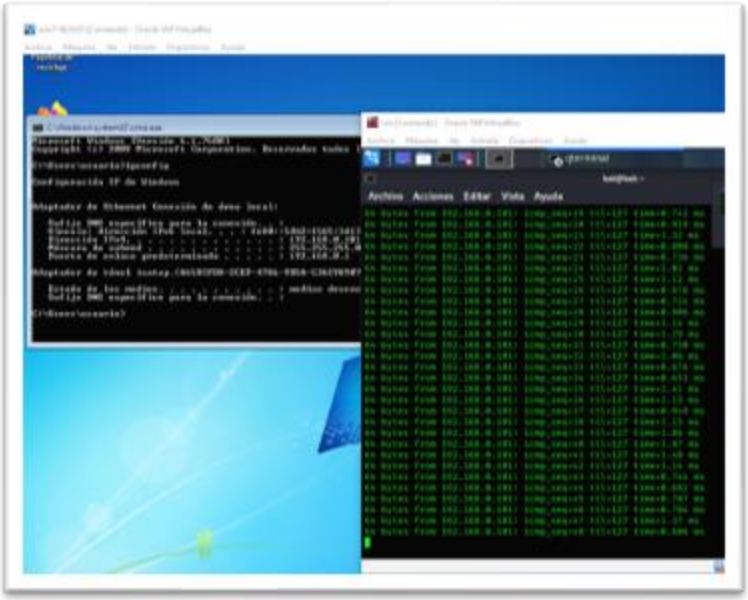
Figura 15: Máquinas importadas

Fuente: el autor.

4.5 VERIFICACIÓN DE LA COMUNICACIÓN ENTRE LAS MÁQUINAS VIRTUALES

Para verificar que, si existe comunicación entre Kali y las maquinas Windows, se hace un ping, y se observa la respuesta, ver figura 16.

Figura 16: Comunicación entre la maquina Kali y la maquina Windows



Fuente: el autor.

5. ANÁLISIS DE LOS ANEXOS ESCENARIO 2 Y ACUERDO DESDE EL PUNTO DE VISTA LEGAL Y NO ÉTICO Y RELACIÓN A LA VULNERACIÓN DE LA LEY 1273.

Una vez leído el documento "Anexo tres – Acuerdo", se puede observar varios apartados, que sin lugar a duda se pueden etiquetar como ilegales o no éticos, a saber:

En la cláusula primera denominada objeto, se puede apreciar, que la parte receptora, es decir el estudiante o aspirante se obligaría a no divulgar a, entre otros, a "autoridades legales" la información confidencial o procesos ilegales que se conozcan en Whitehouse Security, esto es una arbitrariedad y va en contravía de la norma legal vigente, ya que según lo obliga la Ley 906 del 2004 la cual expide el código de procedimiento penal, en su artículo 67, reza: *"DEBER DE DENUNCIAR. Toda persona debe denunciar a la autoridad los delitos de cuya comisión tenga conocimiento …"*[15], en este punto concreto, no podríamos aceptar esta cláusula, ya que es un deber normado, y el hecho de aceptar nos convertiría en cómplices de los delitos cometidos que conozcamos y no denunciemos, esto último, también sustentado en la Ley 599 del 2000 que expide el código Penal colombiano, y en su artículo 446, reza: "*FAVORECIMIENTO: El que tenga conocimiento de la comisión de la conducta punible, y sin concierto previo, ayudare a eludir la acción de la autoridad o a entorpecer la investigación correspondiente, incurrirá en prisión de dieciséis (16) a setenta y dos (72) meses … "*[16], por tal motivo el conocer de una actividad ilegal y no reportar o denunciar ante las autoridades competentes, nos convertiría en participes del delito, y tendríamos responsabilidad penal, y por ende podríamos ser condenados por ello, esta arbitrariedad también se puede apreciar en otros fragmentos del acuerdo como la cláusula cuarta, donde se recalca el hecho de la obligación de no denunciar actividades ilícitas, camuflando el termino en la frase "Información confidencial".

Por otro lado, al analizar la cláusula segunda, donde se define "información confidencial", en el ítem número dos, indica entre otras definiciones, que la información confidencial corresponde a "*datos secretos como datos de chuzadas, interceptación de información, accesos abusivos a datos informáticos*", se observa claramente que estas definiciones corresponden a delitos puntualmente tipificados

[15] Ley 906 de 2004, Por la cual se expide el Código de Procedimiento Penal, 31 de agosto, D.O. No. 45.658 (Colombia) http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004_pr001.html#:~:text=DEBER%20DE%20DENUNCIAR.,que%20deban%20investigarse%20de%20oficio.

[16] Ley 599 de 2000, Por la cual se expide el Código de Penal, 24 de julio de 2000, D.O. No. 44.097 (Colombia) http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr017.html#446

en la Ley 1273 del 5 de enero de 2009[17] "de la protección de la información y de los datos", los cuales se precisan a continuación:

Interceptación de datos informáticos (esto equivale a lo que en el texto figura como datos secretos de chuzadas): este delito se encuentra estipulado en el artículo 269C de la Ley 1273 de 2009 y corresponde al hecho de recopilar información de una comunicación en un sistema, esto puede ser desde donde se origina, a donde va destinada o en su intermedio.

Acceso abusivo a sistemas informáticos: en la Ley 1273 de 2009 este delito se encuentra normado en el artículo 269ª y nos precisa que la comisión de este delito se presenta en el momento que se ingrese a un sistema informático, sin la autorización del propietario o encargado del mismo, así el sistema se encuentre protegido o no con alguna forma de seguridad.

En igual forma, al analizar la Cláusula cuarta, en el ítem tres, se hace mención a la obligación de la parte receptora es decir del estudiante, de "*No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros ...*"; en este contexto, es pertinente mencionar, que la actividad de "espionaje", se cataloga claramente como una actividad ilegal, y esto se sustenta en el artículo 463 de la Ley 599 Código Penal, el cual indica que la actividad de espionaje se define como: "*El que indebidamente obtenga, emplee o revele secreto político, económico o militar relacionado con la seguridad del Estado …*"[18].

En le ítem 8 de la misma cláusula cuarta, en el texto "*Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento*.", también se puede apreciar un desafuero total ya que al aceptar esto, The WhiteHouse estaría instigando al estudiante a auto incriminarse en las posibles actividades antijurídicas o ilegales que se pudiesen detectar.

6. ANÁLISIS DE LA PROPUESTA LABORAL, TENIENDO PRESENTE EN CUENTA LA REVISIÓN DESDE EL PUNTO DE VISTA LEGAL Y ÉTICO.

A la pregunta concreta de que si aceptaría yo el trabajo ofrecido en The WhiteHouse, y analizando el anexo dos escenario dos – situación problema, este aclara que el acuerdo del anexo 3, fue elaborado por un abogado que ya no trabaja

[17] Ley 1273 de 2009, De la Protección de la información y de los datos, 5 de enero de 2009, D.O. No. 47.223 (Colombia) http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[18] Ley 599 de 2000, Por la cual se expide el Código de Penal, 24 de julio de 2000, D.O. No. 44.097 (Colombia) https://leyes.co/codigo_penal/463.htm

en The WhiteHouse porque fue despedido por encontrar procesos irregulares y que la compañía como tal no ha revisado dicho acuerdo, mi respuesta sería que sí, siempre y cuando se elabore un acuerdo desde cero donde no se incurra en las irregularidades detectadas al analizar el documento y acto seguido les expondría mis motivos, y las ilegalidades que presenta el actual contrato, esto me daría la oportunidad de demostrar mi ética, mis principios y valores como persona y como ingeniero de sistemas, y poner desde un principio las pautas morales de mi actuar, esto en el entendido de que la compañía desconocía como tal las actuaciones y los alcances del abogado que elaboró el acuerdo y que poseía principios éticos dudosos.

En el caso de que The WhiteHouse persista con la idea de que debo firmar el acuerdo y acatar lo que allí se estipula, mi respuesta ante la oferta de empleo sería un rotundo y radical no, dado que lo que estaría aceptando va en contravía no solo de mis principios morales y éticos como profesional sino también como persona; además es imperativo conocer que en el momento que me gradué como ingeniero de sistemas, acepté y recayó sobre mí, unos compromisos conductuales, para con la sociedad, y esto está plasmado en la Ley 842 del 9 de octubre de 2003[19], en el título IV, Código de Ética Profesional para los ingenieros y profesiones a fines y auxiliares, el cual pretende estandarizar el comportamiento de estos ante la sociedad e invita a mostrar un comportamiento integro, en el ejercicio de la profesión.

Para citar un ejemplo de lo anterior, en el artículo 31 el cual se titula Deberes generales de los Profesionales, en el literal (f) se cita que es mi deber: "*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…"*

Aunado a lo anterior, en el artículo 32 que lleva por título prohibiciones generales a los profesionales, en el literal (b), se cita como prohibición "*Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley*".

Además, mi formación ética, se ha estructurado en aplicar mis conocimientos en pro del avance científico y tecnológico en procura de mejorar procesos y procedimientos en el lugar donde me desempeñe, de una manera estructurada en búsqueda delos objetivos trazados, pero sobre todas las cosas, de una manera ética y legal.

[19] Ley 842 DE 2003, Código de Ética Profesional, 14 de octubre de 2003, D.O. No. 45.340 (Colombia) http://www.secretariasenado.gov.co/senado/basedoc/ley_0842_2003.html

7. ANÁLISIS DEL CASO “OPERACIÓN ANDROMEDA BUGGLY”, TENIENDO EN CUENTA LOS ASPECTOS LEGALES Y ÉTICOS.

Buggly etical hacking

La operación Andrómeda Buggly, fue un caso muy mediático que ocurrió en la ciudad de Bogotá entre los años 2012 y 2014, en donde la central de inteligencia técnica del ejército Nacional, instauró un local público de nombre “Buggly Ethical Hacking” , como parte de una iniciativa de actividad de inteligencia, en donde se promocionaban actividades relacionadas con la seguridad informática y se alentaba a la comunidad de jóvenes entusiastas de la tecnología a participar en eventos relacionados con tecnología, hacking ético, modding de videojuegos entre otras actividades[20], en la figura 17 se puede observar la fachada del establecimiento.

Figura 17: Fachada de Buggly Ethical Hacking

Fuente: https://www.noticiasrcn.com/nacional-justicia/fiscalia-capturo-tres-militares-vinculados-sala-andromeda

El objetivo principal de esta “fachada” era la de interactuar con jóvenes expertos en seguridad informática para adquirir conocimientos de hacking ético, y según Ejército Nacional[21], este establecimiento en su orden de operaciones, no tenía ninguna intención de producir productos de inteligencia más allá que el conocimiento que podrían aportar los jóvenes entusiastas por la seguridad informática, en materia de

[20] ENTER.Co, Detrás de Buggly: la historia de la fachada Andrómeda, consultado el 20 de febrero de 2022, recuperado de: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

[21] EL TIEMPO, Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue, OffSec Services Limited 2022https://www.eltiempo.com/archivo/documento/CMS-15141236

hacking ético, y todo se financiaba con el rublo de gastos reservados que aportaba la Central de Inteligencia Técnica del Ejército Nacional.

Pero todo esto se desbocó, cuando se interpusieron varias denuncias, las cuales daban cuenta de que en este lugar de manera paralela se realizaban actividades ilegales, como interceptaciones a miembros activos del gobierno nacional, también que se manejaba software malicioso para efectuar intrusiones a equipos de cómputo específicos y substraer información de los mismos, además de esto, hay acusaciones de la venta a terceros, para lucro personal, de 100 correos de miembros de las FARC y las bases de datos de los desmovilizados.

Este complejo caso, que aún es motivo de investigación por parte de la Fiscalía[22], en mi concepto personal, demuestra que existe una delgada línea entre la legalidad y la ilegalidad, y que la manera de cruzarla es fácil, pero ponen en vilo la honra, la moral y la ética de los profesionales; ahora bien, es fácil juzgar a priori que una acción de inteligencia se efectúa de manera ilegal, sin conocer el contexto de la actividad, pero si la acción que se realiza está enmarcada bajo unos requisitos legales, y con el visto bueno de la autoridad competente, y procedimientos adecuados y estandarizados, es algo totalmente valido, y permitido ante la legislación colombiana.

8. EFECTUANDO PRUEBAS DE PENETRACIÓN

Una vez realizada la lectura del "anexo 4 - escenario 3", se da inicio a la elaboración de las pruebas de penetración al sistema de cómputo con sistema operativo Windows 7 con arquitectura x64, esto elaborado en el banco de trabajo configurado en el capítulo 5 con las siguientes características:

Equipo Host:
Equipo portátil marca "Hewlett Packard"
Sistema Operativo "Windows 10 Home Single Language" 64 bits
Procesador Intel(R) Core (TM) i7-7500U CPU @ 2.70GHz 2.90 GHz
Memoria RAM de 16 GB

Maquina objetivo
Nombre: "Win7-SE2020-X64"
Sistema Operativo: Windows 7 (64-bits)
Memoria Base: 4096 MB

[22] Ibit, p. 10

Maquina Atacante (Pentest)
Nombre: “Kali -linux 2020-1”
Sistema Operativo: Debian (64-bits)
Memoria Base: 2048 MB

Luego de ser configurada la estación de trabajo o laboratorio, se da inicio a las fases de penetración, utilizando las siguientes herramientas de software:

Metasploit Framework

Es una herramienta “open source” que permite a los analistas de seguridad o pentester, investigar vulnerabilidades de seguridad en entornos informáticos, a través de exploits y payloads preestablecidos en la herramienta[23].

Nmap

Es una herramienta, que permite a los pentester o administradores de seguridad de una red, escanear los equipos de una red y los puertos y servicios en cada uno de ellos[24].

Nessus

Es una aplicación utilizada por administradores de red y pentesters para escanear y detectar las vulnerabilidades presentadas en las redes y los equipos que la componen, por otra parte, Nessus permite hacer comparativas de las vulnerabilidades detectadas, con sus bases de datos en línea, las cuales están siendo constantemente actualizadas y brindan información de las mismas de sus variantes y posibles soluciones[25].

8.1 INFORMACIÓN DISPONIBLE

Una vez realizada la lectura del anexo suministrado, se logra establecer que se está presentado una fuga de información en un equipo que tiene instalado un sistema operativo Windows 7 con la arquitectura x64,en le cual se encuentra instalado una aplicación llamada “rejetto versión 2.3”; que permite la ejecución de un exploit para

[23] RAPID 7, Metasploit - The world’s most used penetration testing framework, consultado el 8 de marzo de 2022, recuperado de: https://www.metasploit.com/

[24] NMAP, Nmap Security, consultado el 8 de marzo de 2022, recuperado de: https://nmap.org/

[25] NESSUS, Conozca sus vulnerabilidades e interrumpa las rutas de ataque, consultado el 8 de marzo de 2022, recuperado de: https://es-la.tenable.com/products/nessus

la ejecución de una “Shell reversa” mediante el módulo de meterpreter, además también se presenta escalamiento de la vulnerabilidad mediante la creación de usuarios con roles de administrador.

8.2 IDENTIFICACIÓN DE FALLOS DE SEGURIDAD

Para la identificación de los fallos de seguridad en el equipo “Windows 7 x64”, se utilizó las herramientas Nmap, para la identificación del equipo objetivo, los puertos abiertos en el mismo y los servicios con su correspondiente versión; de igual forma se usó la herramienta Nessus, la cual brinda un informe detallado de las vulnerabilidades presentadas en la red, y en especial en el equipo objeto del análisis.

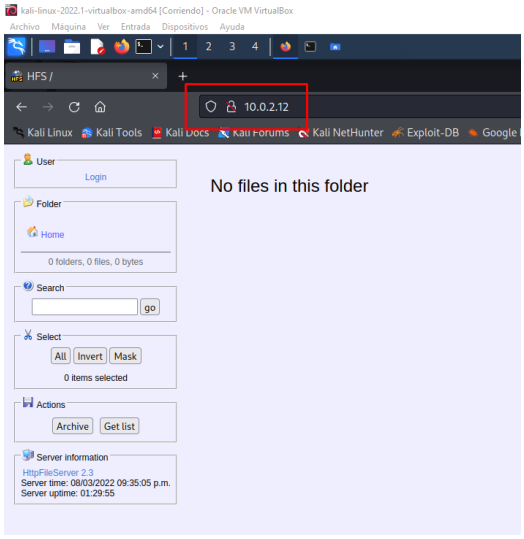
Se detectó que la vulnerabilidad se presenta en el puerto 80 / tcp, en el cual corre un servicio denominado “Http FileServer httpd 2.3”, que es el servicio que se crea cuando se inicia la aplicación “hfs.exe” en la maquina “Windows 7 x64”

8.3 COMO AFECTA EL ATAQUE A LA MAQUINA “WINDOWS 7 X64”

Cuando la víctima ejecuta el archivo “hfs.exe - Http FileServer 2.3”, en la maquina Windows 7 x64, se crea un servidor web de archivos, el cual permite a usuario compartir y recibir archivos hacia ubicaciones remotas, solamente introduciendo la ip de dicho servidor en el navegador, en la figura 18 se muestra el servidor en el navegado de Kali Linux[26]:

[26] REJETTO, media wiki, consultado el 8 de marzo de 2022, recuperado de: https://www.rejetto.com/wiki/index.php?title=HFS:_Introducci%C3%B3n#:~:text=*%20comunica%20a%20tus%20amigos%20la,pega'%20y%20envia%20la%20direcci%C3%B3n.

Figura 18: Servidor web de archivos HFS

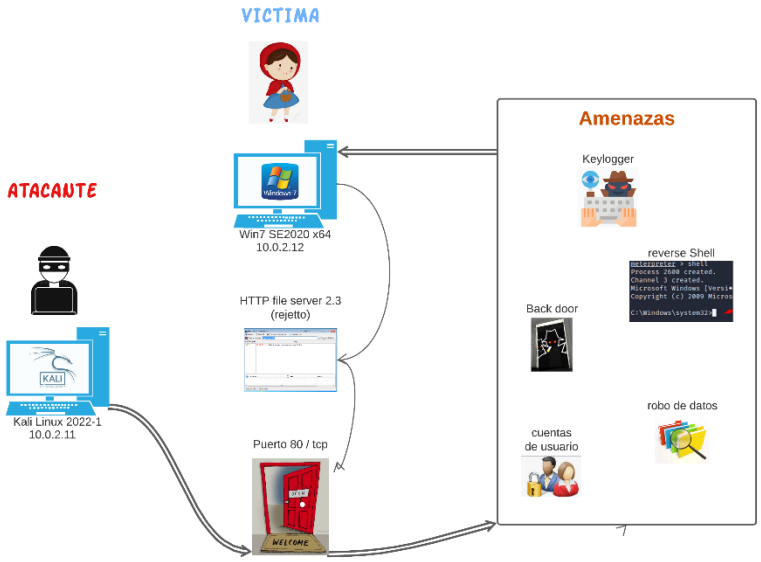


Fuente: el autor

Una vez se ha ejecutado la aplicación, se abre una vulnerabilidad, en el equipo, consistente en correr el servicio "Http FileServer httpd 2.3" en el puerto 80 / tcp de la máquina, el cual, según incibe-cert.es [27] se ejecuta la función findMacroMarker en parserLib.pas, catalogada en la nomenclatura estándar para identificación de la vulnerabilidad con el código CVE-2014-6287, que da la posibilidad al atacante de ejecutar códigos maliciosos en la maquina afectada, que permiten el robo de información, escalamiento de privilegios y creación de usuarios con roles de administrador, creación de Shell reversa entre muchas otras amenazas, ver figura 19.

[27] INCIBE-CERT, Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287), consultado el 8 de marzo de 2022, recuperado de: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

Figura 19: Como afecta el ataque en la maquina Windows.



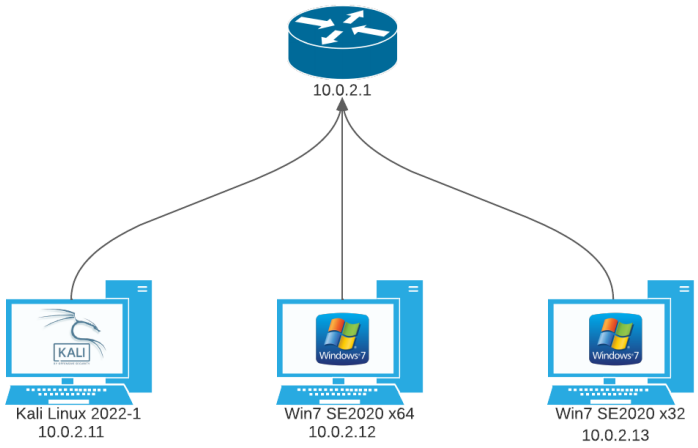
Fuente: el autor

8.4 PASOS PARA LA EXPLOTACION DE LA VULNERABILIDAD EN EL EQUIPO WINDOWS 7 X64

8.4.1 Preparación del laboratorio

Es adecuado recordar que el presente laboratorio consta de dos equipos Windows, uno x64 y otro x32 y un equipo Linux con la distribución Kali versión 2022-1, los tres equipos virtualizados en el programa VirtualBox, pero para efectos prácticos, en este laboratorio se realizaran las pruebas en las maquinas Windows 7 x64 y Kali Linux 2022-1, la siguiente figura muestra el esquema de red.

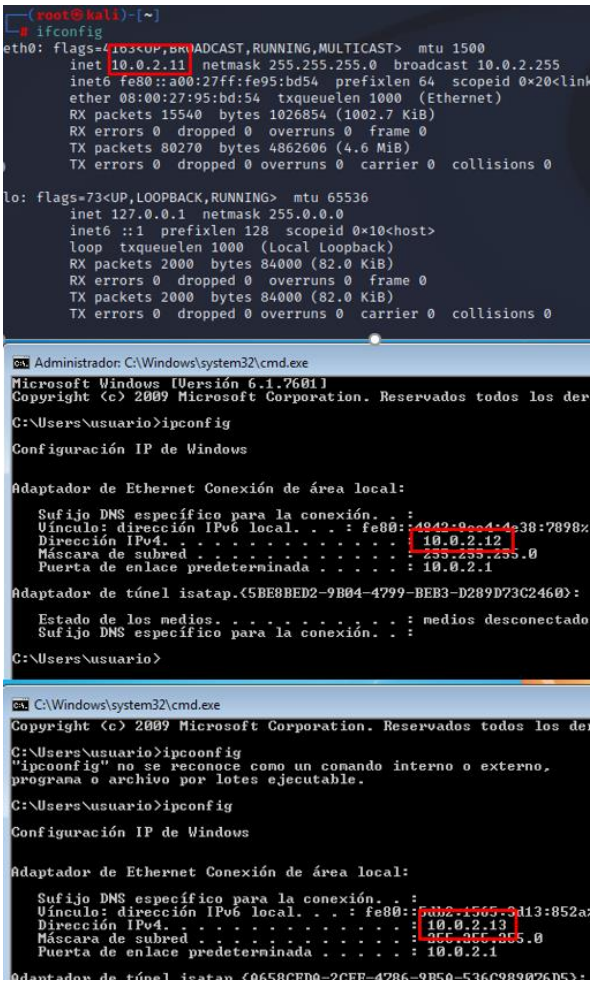
Figura 20: Esquema de red Laboratorio



Fuente: El autor

Una vez iniciado el laboratorio, con las máquinas virtuales corriendo, se debe abrir una consola en la maquina “Kali”, teniendo en cuenta estar logeado como usuario “administrador” o “root” una vez hecho esto, podemos identificar la ip de nuestra máquina con el comando “ifconfig” o también con el comando “*ip a*“, en el caso de las maquinas Windows esto se puede hacer con el comando “*ipconfig”, ver figura 2.*

Figura 21: Verificación ip's de las Maquinas.



Fuente: el autor

Luego de esto, se verifica que las maquinas tengan comunicación entre sí, mediante el comando “ping”, y ya estaríamos listos para iniciar el laboratorio.

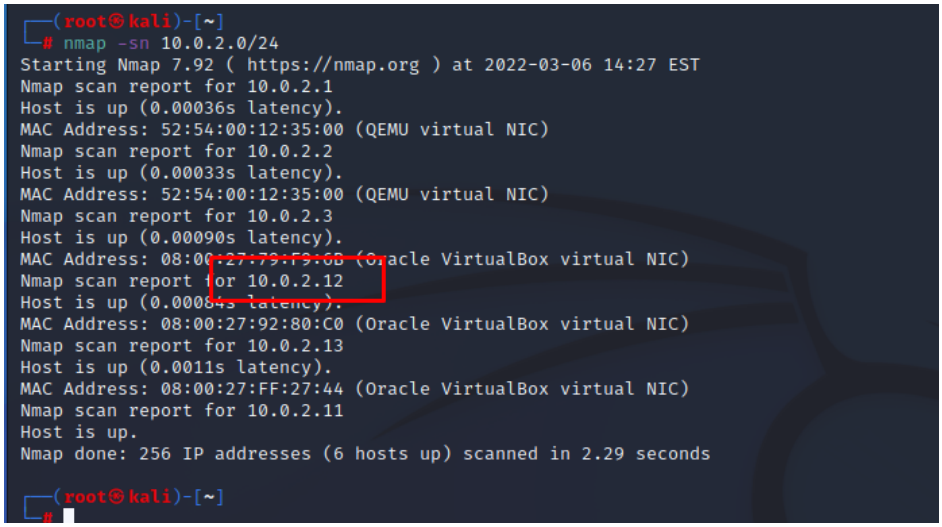
8.4.2 Fase de Reconocimiento

Se ha recolectado una información inicial, donde se establece que existe una maquina desde donde se genera una fuga de información, la cual posee un sistema operativo “Windows 7” con arquitectura x64, en la cual se encuentra una aplicación llamada “rejetto v2.3”.

Para la fase de reconocimiento se utilizará la herramienta NMAP, la cual es una herramienta gratuita y de código abierto, que permite realizar un "mapeo de la red", en donde se puede identificar los hosts activos en la red, el estado de los puertos, los servicios que corren en ellos y el sistema operativo entre otras cosas[28].

Continuamos esta fase, realizando un escaneo de los hosts activos para identificar el objetivo, esto se efectúa con el comando "*nmap -sn 10.0.2.0/24*"; donde la opción "*-sn*", nos permite listar los equipos que se encuentran activos en ese rango de ip's indicado, sin realizar escaneo de puertos.

Figura 22: Reconocimiento de objetivo.



Fuente: el autor

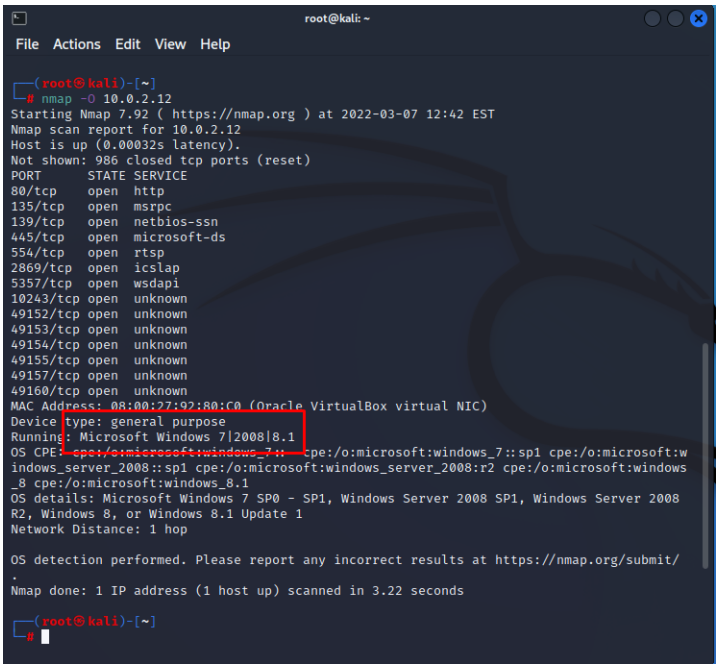
En la figura anterior se puede observar el reconocimiento de los tres hosts activos con las ip's 10.0.2.11, 10.0.2.12 y 10.0.2.13, donde la ip 10.0.2.11 pertenecería al equipo desde el cual se va a hacer la auditoria con el sistema operativo Kali Linux, y la maquina con la ip 10.0.2.12, sería la maquina objetivo, donde se está presentando la vulnerabilidad.

8.4.2.1 Identificando el sistema Operativo

Para la identificación del sistema operativo utilizado en la maquina objetivo utilizaremos el comando "*nmap –O 10.0.2.12*", donde la opción *"-O*", nos permite observar cual es el sistema operativo del host escaneado.

[28] Ibit, p. 27

Figura 23: Identificación del Sistema Operativo de la maquina objetivo

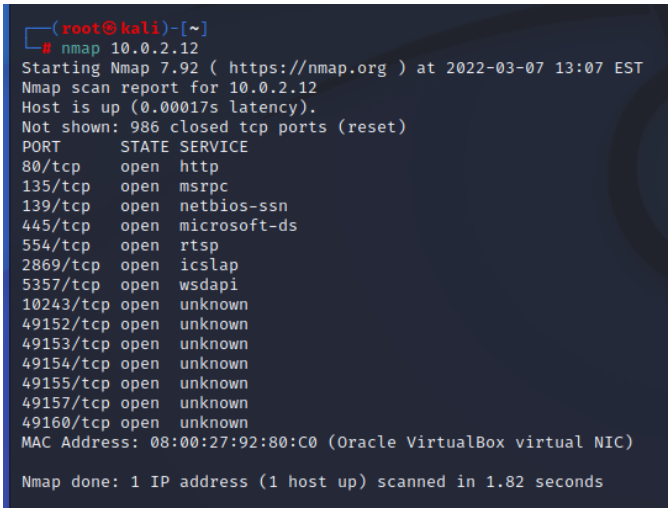


Fuente: el Autor

8.4.2.2 Escaneo de Puertos

Paso seguido, se realizael escaneo de puertos de la máquina, con el comando "*nmap 10.0.2.12*" el cual nos permite observar cuales son los puertos en la máquina, y el tipo de servicio que corre en cada uno de los puertos.

Figura 24: Escaneo de puertos abiertos

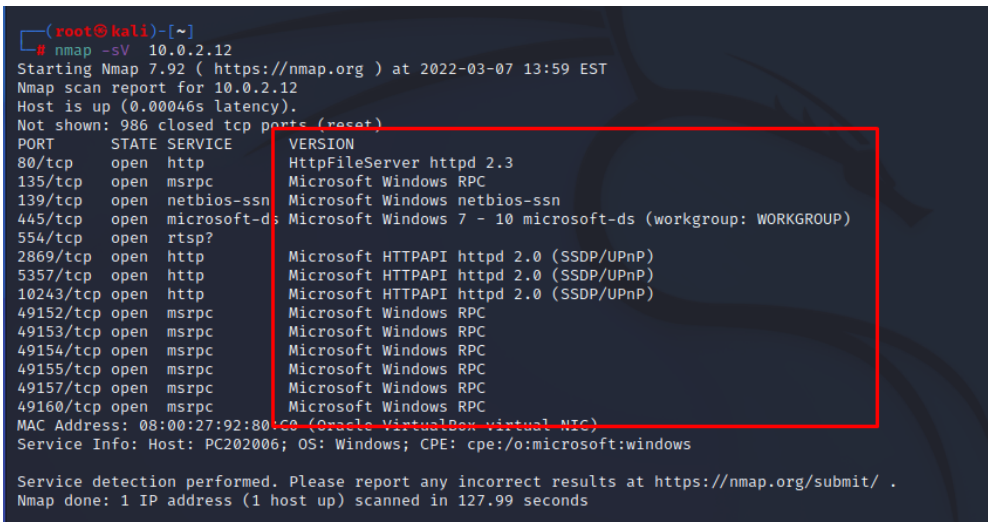


Fuente: el autor

8.4.2.3 Versión del servicio que corre en cada puerto

Si se requiere saber la versión del servicio que corre en cada puerto se utiliza el comando "*nmap –sV 10.0.20.12*", adicionando el parámetro *"–sV*", obtendremos la versión del servicio que está corriendo en cada puerto, esto se puede apreciar en la siguiente figura:

Figura 25: Escaneo de puertos con la versión de los servicios.



Fuente: el autor

8.4.3 Fase de Análisis de Vulnerabilidades

Una vez identificado el objetivo y habiendo enumerado los servicios activos y su correspondiente versión, podemos avanzar a la siguiente fase del pentesting que es el análisis de vulnerabilidades.

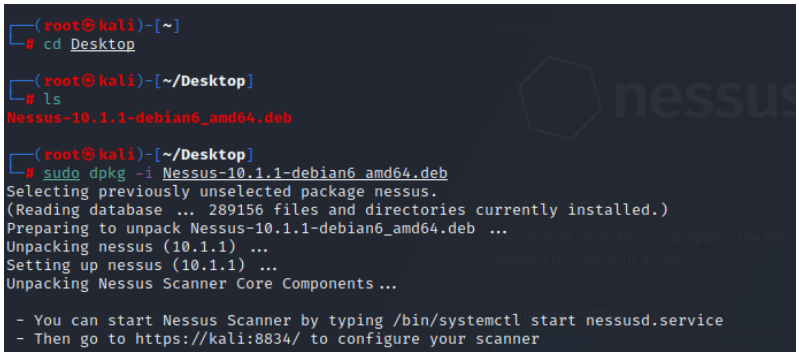
8.4.3.1 Análisis de Vulnerabilidades con la herramienta Nessus

Una de las herramientas más versátiles al momento de efectuar un análisis de vulnerabilidades es la herramienta Nessus, que como se expuso anteriormente, nos permite escanear y detectar las vulnerabilidades presentadas en las redes y los equipos.

- Instalación de Nessus

Desde la página https://www.tenable.com/downloads/nessus?loginAttempted=true descargamos el archivo correspondiente para el sistema operativo, en nuestro caso Nessus-10.1.1-debian6_amd64.deb, una vez descargado, en la ubicación del archivo, lo ejecutamos con el comando "sudo dpkg", para instalarlo[29].

Figura 26: Instalación de Nessus.

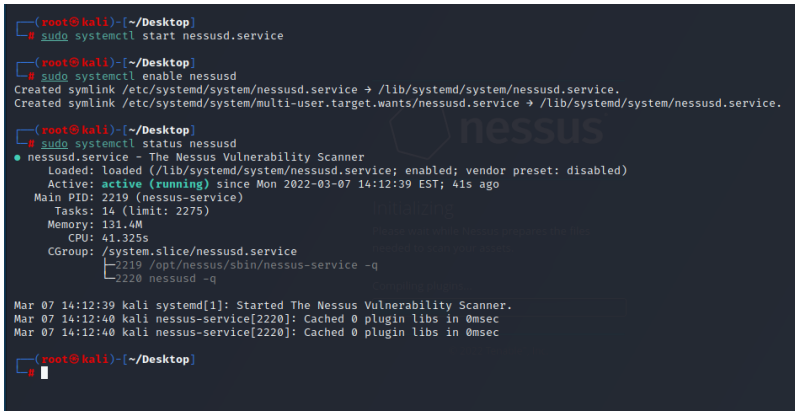


Fuente: el autor

Una vez finalizada la instalación, hacemos la primera ejecución, la cual nos permitirá realizar las configuraciones pertinentes, con el comando "*sudo systemctl start nessusd.service*" y luego el comando "*sudo systemctl enable Nessus"*

[29] NOVIELLO, Cómo instalar y configurar Nessus Vulnerability Scanner en Kali Linux, consultado el 8 de marzo de 2022, recuperado de: https://noviello.it/es/como-instalar-y-configurar-nessus-vulnerability-scanner-en-kali-linux/

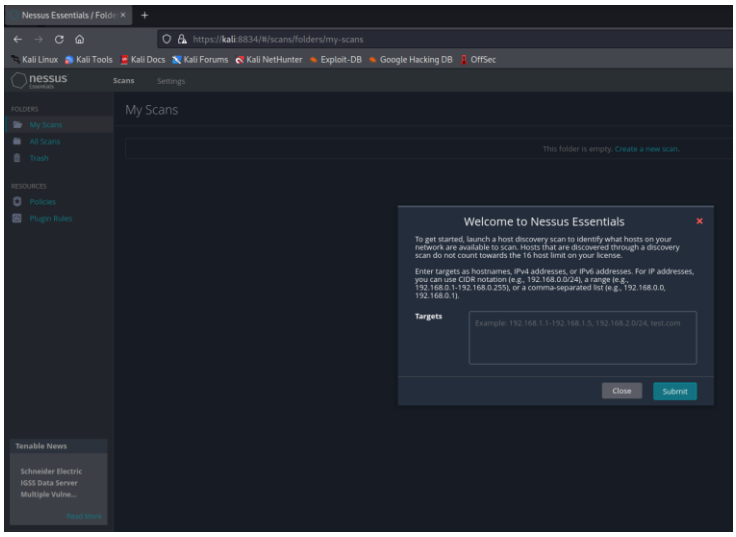
Figura 27: Configuración inicial de Nessus.



Fuente: el autor

Posteriormente podemos ir al navegador e iniciar la interface web que proporciona Nessus para interactuar con la herramienta e iniciar el escaneo.

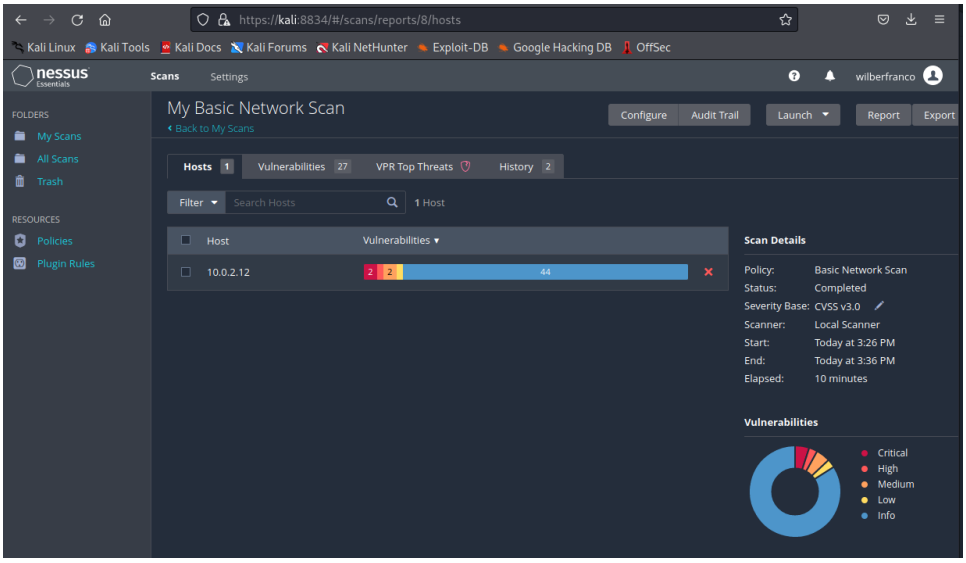
Figura 28: Interface web de Nessus



Fuente: el autor

Una vez realizado el análisis de vulnerabilidades se puede observar una estadística de las vulnerabilidades presentadas en el host objetivo, el cual, como se había enunciado anteriormente tiene la ip 10.0.2.12, a saber, se detectaron 27 Vulnerabilidades, de las cuales el 5% son críticas, el 3% son altas, el 5% son medias y el 3% son bajas, como se observa en la siguiente figura:

Figura 29: Análisis de Vulnerabilidades con Nessus

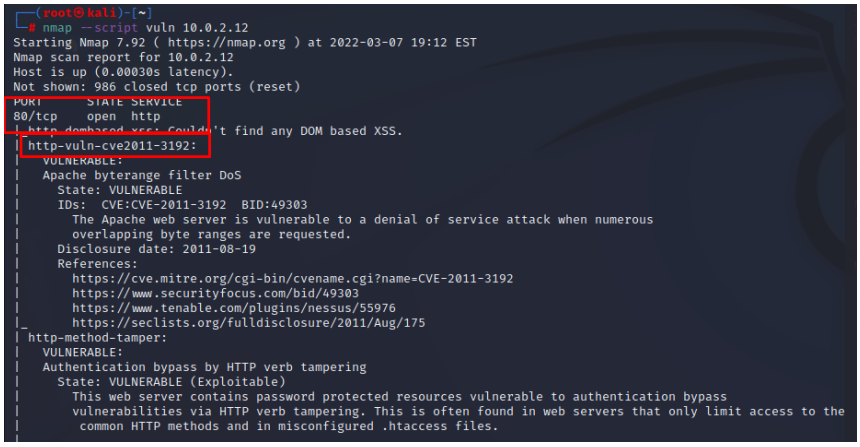


Fuente: el autor

8.4.3.2 Análisis de Vulnerabilidades con la herramienta Nmap

Por otro lado, con la herramienta nmap, también es posible efectuar un análisis de vulnerabilidades ejecutando el comando "*nmap --script vuln 10.0.2.12*" desde la consola de Kali Linux, esto nos permite observar que la maquina objetivo posee varias vulnerabilidades, entre ellas, la que se había detectado en el puerto 80 del servicio http:

Figura 30: Análisis de vulnerabilidades con Nmap.



Fuente: el autor

En la figura anterior podemos evidenciar que se presenta la vulnerabilidad en el puerto 80 /tcp el cual está abierto, y dicha vulnerabilidad tiene la denominación CVE (Vulnerabilidades y exposiciones comunes): "http-vuln-cve2011-3192"[30].

8.4.4 Fase de Explotación

Para la fase de explotación se utilizará la herramienta Metasploit Framework, la cual es una herramienta para pruebas de penetración desarrollado por la empresa Rapid 7, escrito en el lenguaje de programación Ruby y Perl, está disponible para plataformas Windows y Linux, pero en este caso la utilizaremos en la Distribución Linux, como se había mencionado anteriormente.[31]

Actualmente Metasploit incluye más de 1677 exploits organizados en 25 plataformas, incluidas Android, PHP, Python, Java, Cisco y más. El Framework también incluye más de 500 Payloads, algunos de los cuales incluyen:

Payloads de shell de comandos que permiten a los usuarios ejecutar secuencias o comandos aleatorios contra un host.

---

[30] CVE-MITRE, National Vulnerability Database (NVD), consultado el 8 de marzo de 2022, recuperado de: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192

[31] Ibit. Pag 27

Payloads dinámicos que permiten a los pentesters generar payloads personalizados para evadir el software antivirus.

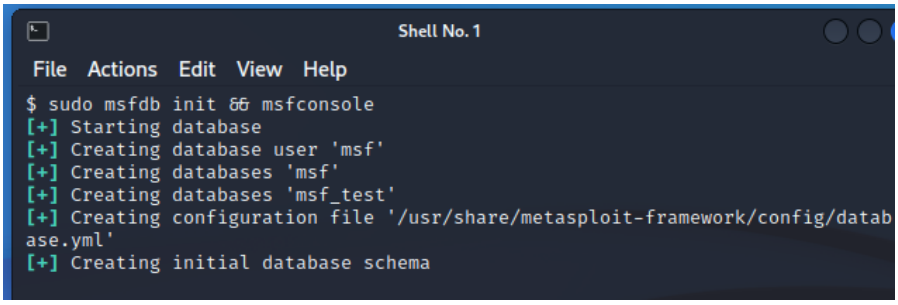
Payloads de Meterpreter que permiten a los usuarios realizar monitoreo de dispositivos usando VMC y tomar el control de sesiones o cargar y descargar archivos.

Payloads que permiten el reenvío de puertos y las comunicaciones entre redes[32].

8.4.4.1 Explotación de la vulnerabilidad con la herramienta Metasploit

Cuando se inicia por primera vez la herramienta metasploit, es necesario realizar la creación de las bases de datos requeridas para la utilización del framework, para esto se utiliza el comando "sudo msfdb init && msfconsole", como se muestra en la siguiente figura:

Figura 31: Creación de las Bases de datos de metasploit e inicio de la consola.



Fuente: el autor

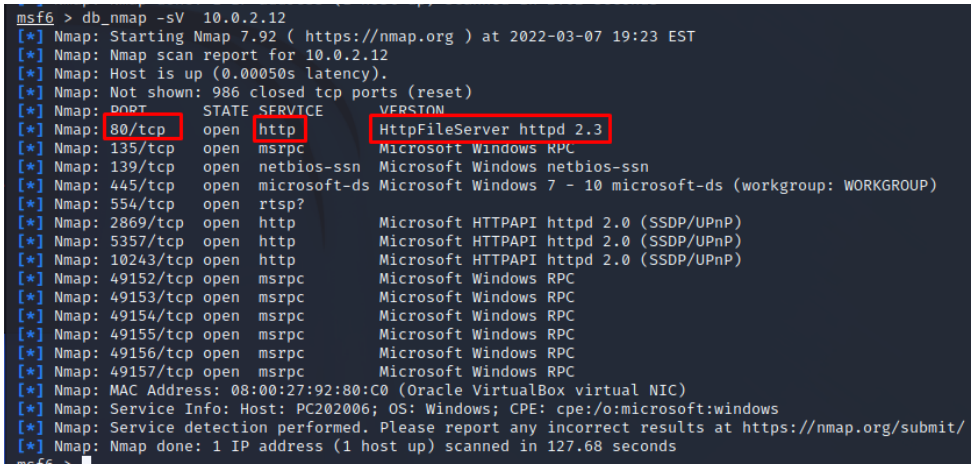
[32] JEFF petters, Varonis, What is Metasploit? The Beginner's Guide, consultado el 8 de marzo de 2022, recuperado de: https://www.varonis.com/blog/what-is-metasploit

Figura 32: Pantalla inicial de Metasploit Framework.

Fuente: el autor

Acto seguido se ejecutará la consola del framework de metasploit en línea de comandos para dar inicio al test de penetración; cabe anotar, que en la consola de metasploit, también es posible ejecutar comandos de nmap, esto con el fin de brindarnos la posibilidad de registrar en la base de datos de metasploit framework las actividades de testeo realizadas desde la herramienta, con el comando "*db_nmap -sV 10.0.2.12*" identificar el puerto y el servicio donde se encuentra la vulnerabilidad, que registramos en la fase de recolección de información, en este caso, el servicio servidor http HttpFileServer httpd 2.3 en el puerto 80/tcp.

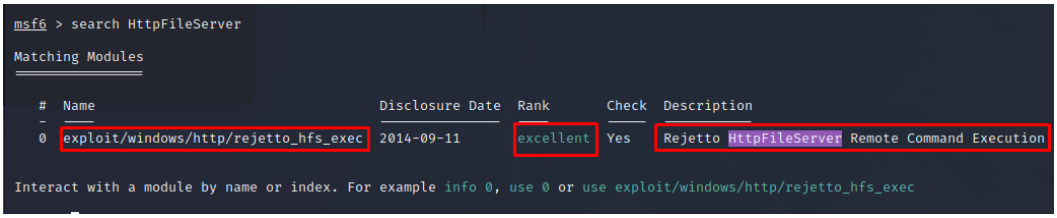
Figura 33: Identificación de la Vulnerabilidad desde metasploit framework



Fuente: el autor

Una vez identificada, la posible vulnerabilidad, con el comando "*search HttpFileServer*", realizaremos una búsqueda de los exploits, asociados a la vulnerabilidad detectada, en este caso se encontró el exploit "exploit/windows/http/rejetto_hfs_exec" que permite la ejecución de comandos de manera remota en la maquina objetivo.

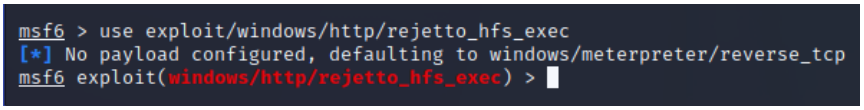
Figura 34: búsqueda del exploit para la vulnerabilidad en HttpFileServer



Fuente: el autor

Para utilizar este exploit y dar inicio a la explotación de la vulnerabilidad, se ingresa el comando use seguido del nombre del exploit "use exploit/windows/http/rejetto_hfs_exec", o simplemente se indica el identificador #, "use 0".

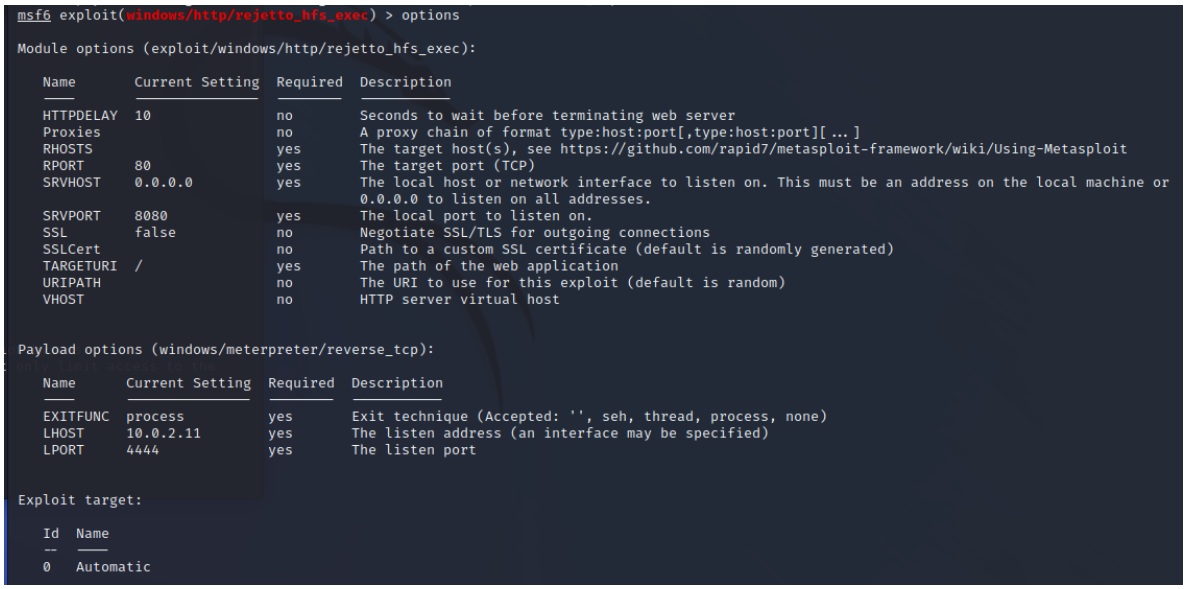
Figura 35: selección del exploit



Fuente: el autor

Una vez se ha seleccionado el exploit, se debe configurar las opciones que permitan efectuar de manera exitosa la explotación, con el comando "options" podremos ver cuáles son las opciones del exploit seleccionado

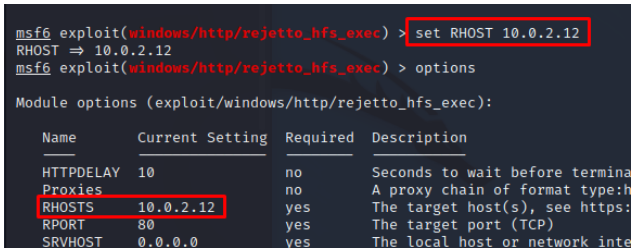
Figura 36: opciones de configuración del exploit seleccionado.



Fuente: el autor.

En este caso solo hace falta configurar el RHOSTS o host remoto, que sería la ip de la maquina objetivo, en este caso 10.0.2.12, esto se realiza con el comando “set RHOST 10.0.2.12”

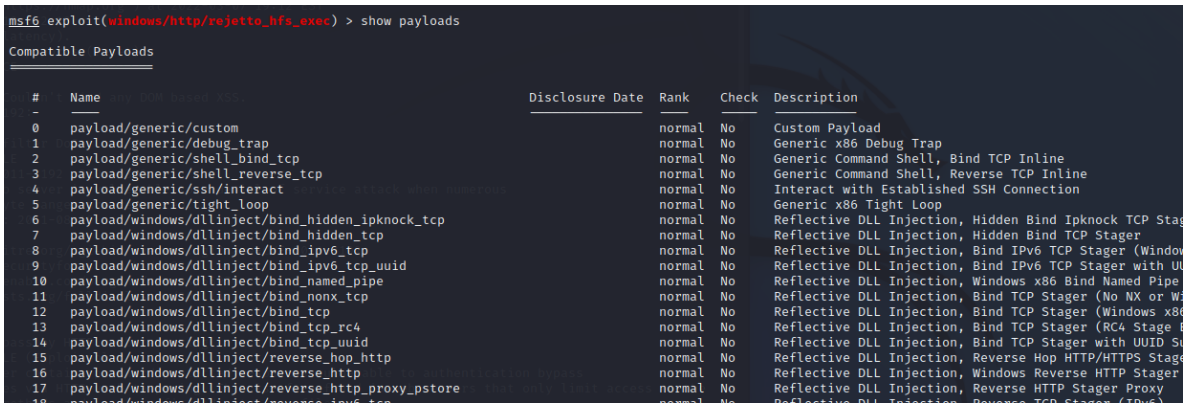
Figura 37: configuración del exploit.



Fuente el autor.

Una vez configurado el exploit, podemos seleccionar el payload o carga útil que junto con el exploit nos permitiría realizar la explotación de la vulnerabilidad; esto se realiza, primero mirando los payloads disponibles para el exploit seleccionado con el comando “show payloads”, y posteriormente cargándolo con set + el nombre del payload, dependiendo del payload seleccionado se efectuará su configuración.

Figura 38: lista de Payloads para el exploit seleccionado

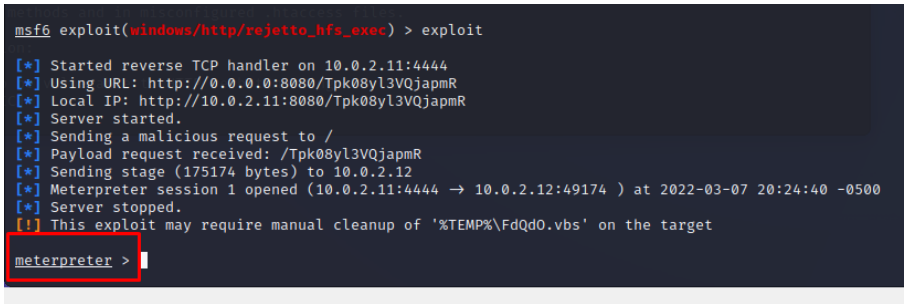


Fuente el autor

8.4.4.2 Usando Meterpreter

Para dar inicio a la explotación, se ejecuta el payload mediante el comando “exploit”, esto dará inicio al ataque a la maquina objetivo y abrirá una Shell de comandos con un módulo meterpreter que es un payload que permite la ejecución de comandos de manera remota en la maquina objetivo, permitiendo extraer información de la misma, tomar el control del teclado y mouse, observar su cámara web, crear usuarios, entre otras cosas.

Figura 39: Inicio de la Explotación.



Fuente: el autor

A continuación, se listarán algunas acciones que se pueden realizar mediante la Shell de meterpreter:

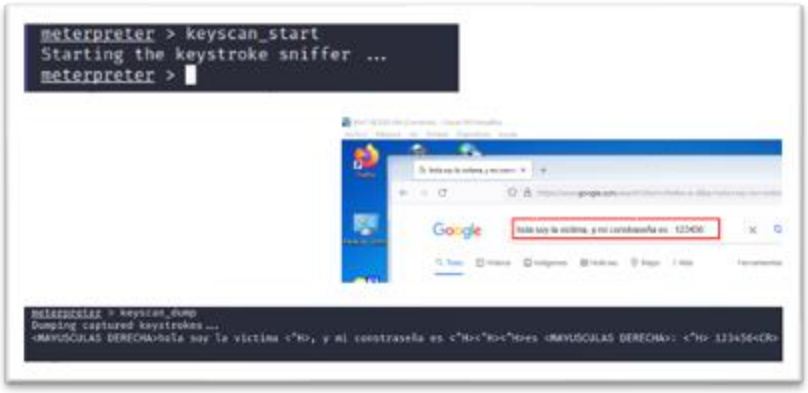
- Ejecutar programas en la maquina víctima mediante el comando “execute”:

Figura 40: Ejecución del programa calc.exe en la maquina objetivo

Fuente el autor

- Iniciar un keylogger con el comando “keyscan_start” y recuperar todo lo digitado por el usuario con el comando “keyscan_dump”:

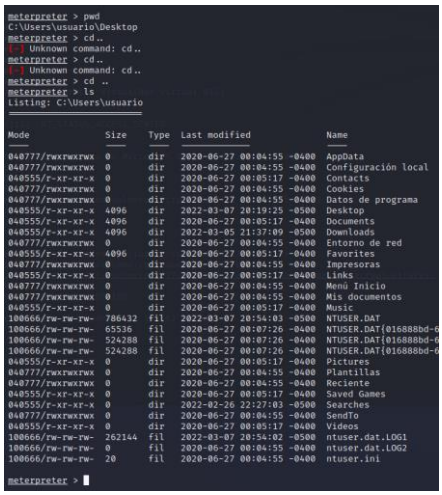
Figura 41: Keylogger en la maquina objetivo.



Fuente: el autor.

- Ver los archivos de la maquina objetivo.

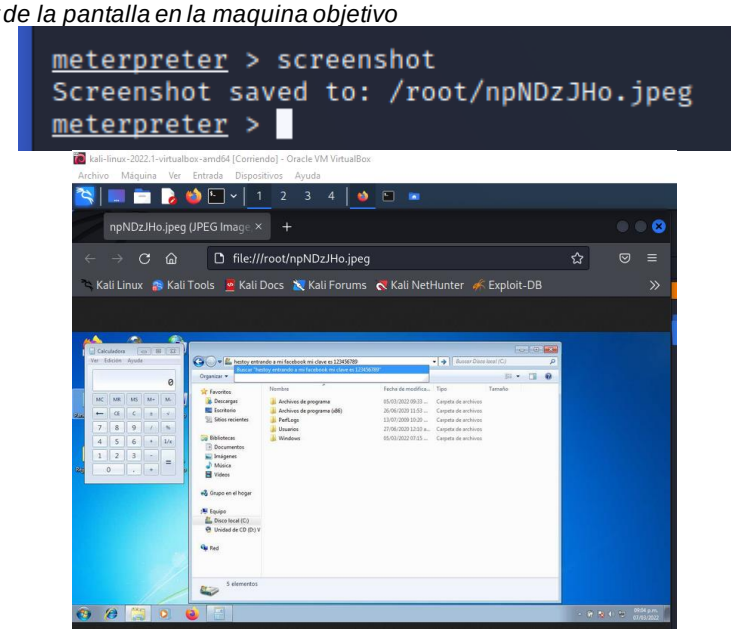
Figura 42: archivos en la maquina objetivo



Fuente: el autor.

- Tomar capturas de pantalla de la maquina comprometida con el comando “screenshot”:

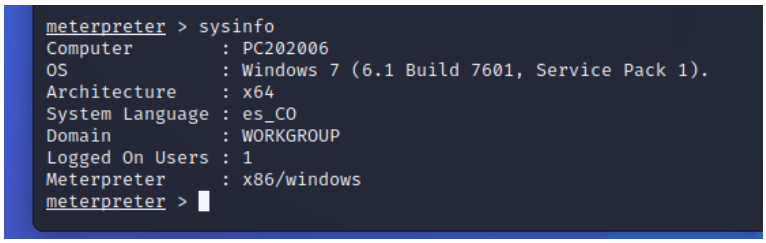
Figura 43: Screenshot de la pantalla en la maquina objetivo



Fuente: el autor

- Ver la información del sistema

Figura 44: información del sistema en la maquina objetivo

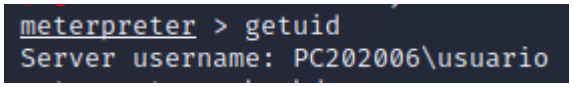


Fuente: el autor

8.4.5 Fase de Elevación de privilegios o Post - explotación

Con el comando “getuid”, observamos el nombre del usuario actual, el cual en este caso es “usuario”.

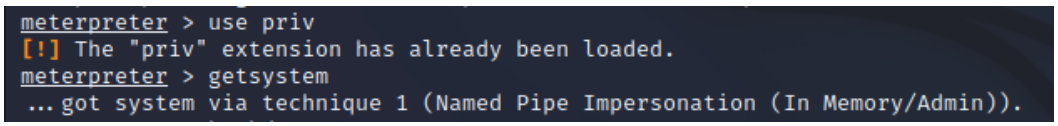
Figura 45: Comando getuid



Fuente: el autor

Usamos el módulo “priv”, para poder elevar los privilegios con el comando “getsystem”

Figura 46: elevación de privilegios con el comando getsystem



Fuente: el autor

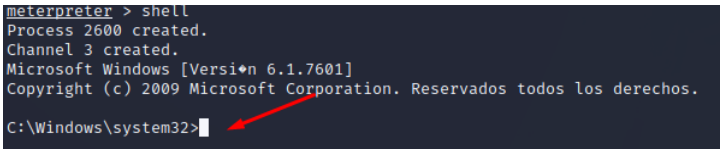
Verificamos que se hayan elevado los privilegios, ahora tenemos privilegios system, que es el equivalente a root en Linux

Figura 47: Privilegios System

Fuente: el autor

Acto seguido creamos una Shell, esto abrirá una interface idéntica a la que usa el usuario de la maquina comprometida:

Figura 48: Creación de una Shell



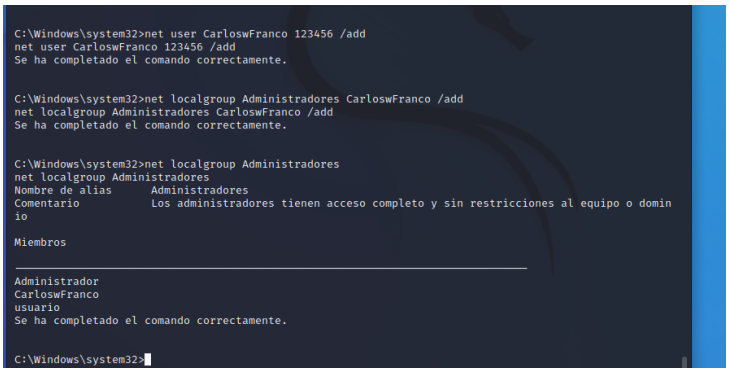
Fuente: el autor

8.4.5.1 Creación de usuario con privilegios de administrador

Una vez la "shell" se esté ejecutando, seguimos los pasos de creación de usuarios, como si estuviéramos trabajando en el equipo de forma local:

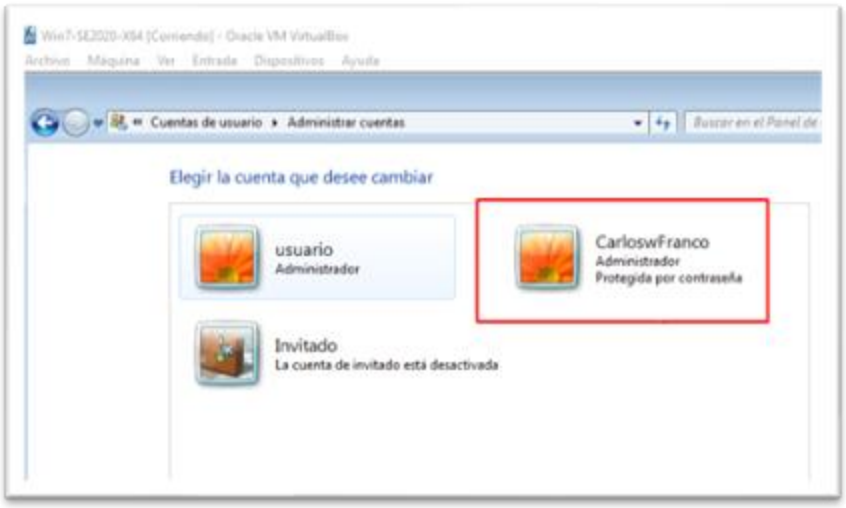
- net user CarloswFranco 123456 /add
- net localgroup Administradores CarloswFranco /add
- net localgroup Administradores

Figura 49: creación de usuario administrador



Fuente: el autor

Figura 50: Evidencia de la creación de usuario administrador



Fuente: el autor

9. ACTUACIONES DEL EQUIPO BLUE TEAM

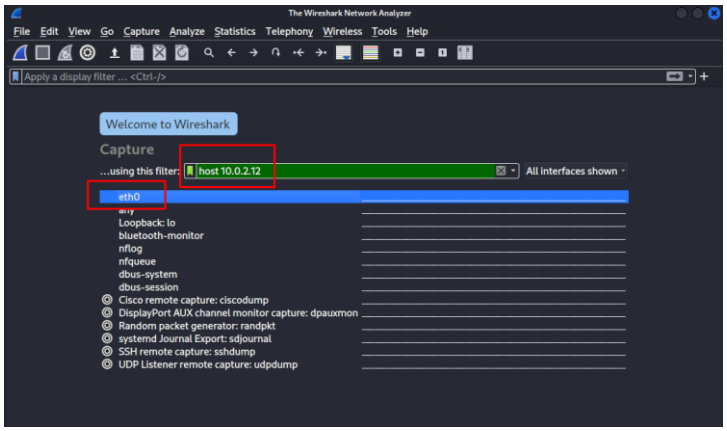
Una vez que se ha informado al equipo blue team de un posible "ataque informático", se debe recopilar la mayor información relacionada con la maquina víctima, en donde se está presentando el ataque, con el fin de detectar la vulnerabilidad explotada y la amenaza que presenta, con el fin de limitar el daño realizado por el atacante.

Como información inicial se conoció que el ataque se está llevando a cabo en tiempo real, en un host identificado que tiene un sistema operativo Windows 7 con arquitectura x64, en este caso concreto tiene la ip. 10.0.2.12, en este momento el paso a seguir es realizar un análisis del tráfico de red con el fin de identificar la maquina atacante, y el puerto y servicio que se está utilizando para la explotación de la vulnerabilidad, esto se realiza con la herramienta Wireshark.

Wireshark, es una herramienta que nos permite analizar los paquetes que viajan por una red y sus respectivos protocolos, esta utilidad, nos da la posibilidad de capturar todo el tráfico generado desde o hacia un host especifico, y permite guardarlo para su posterior análisis, brindándonos la posibilidad de ver el contenido de cada uno de los paquetes capturados, para percibir el tipo de servicio que los genera.

Como se está presentando un ataque en tiempo real lo primero que se puede hacer es dar inicio a la captura de paquetes con Wireshark para analizar el trafico que involucra al equipo afectado, podemos realizar la captura aplicando un filtro a la ip 10.0.2.12 la cual pertenece al equipo vulnerado:

Figura 51: Ventana Inicial de Wireshark.

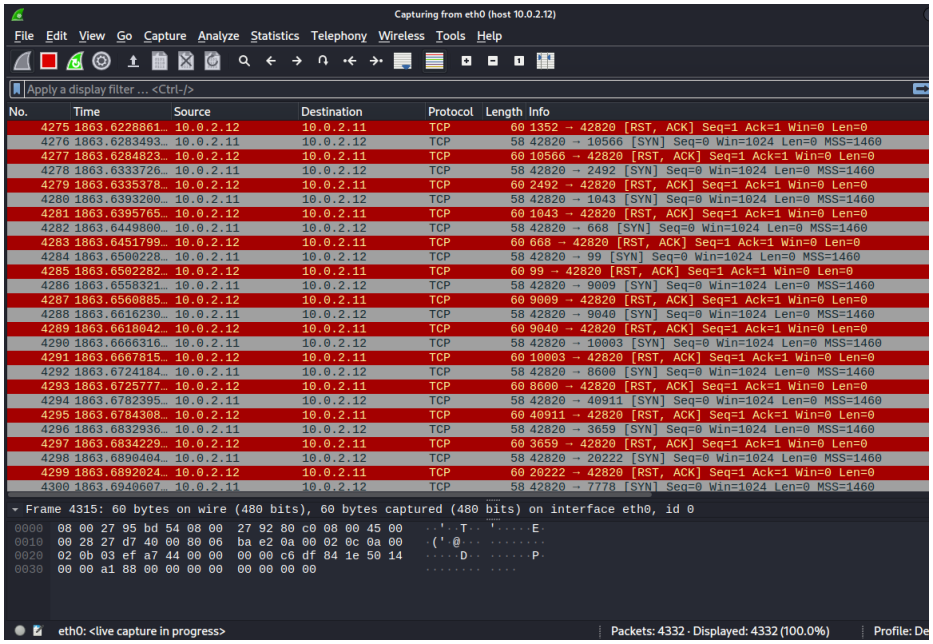


Fuente: el autor

Una vez iniciada la captura por parte de la herramienta Wireshark, y realizando un análisis de las tramas enviadas se puede observar y podemos inducir que el ataque

se está presentando desde un equipo en la red identificado con la ip 10.0.2.11, desde donde se están generando peticiones y respuestas mediante segmentos TCP y paquetes ICMP.

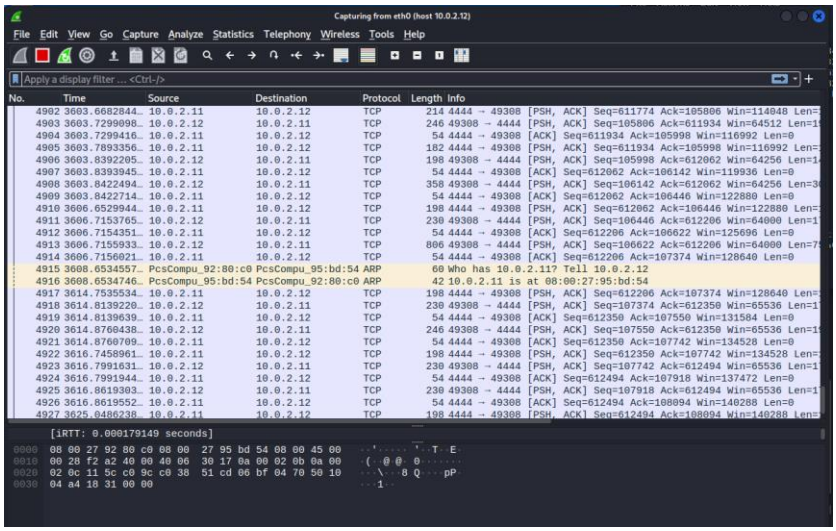
Figura 52: Captura de paquetes con Wireshark.



Fuente: el autor

Durante el ataque se puede observar que la comunicación se mantiene activa entre los dos hosts y hay constantes peticiones por parte de la maquina 10.0.2.11 (atacante) y respuesta por parte del host 10.0.2.12 (victima).

Figura 53: Comunicación víctima - atacante.



Fuente: el autor

9.1 MEDIDAS DE HARDENIZACION PROPUESTAS

Luego de realizar el ejercicio de análisis practico de los casos propuestos, simulando un Red Team y Blue team en la empresa WhiteHouse Security; se procede a realizar algunas recomendaciones de Hardenizacion para poder alcanzar un entorno más seguro.

Antes de continuar, cabe lugar a definir el término de Hardenizacion; según López[33], el hardening es un conjunto de técnicas, disciplinas o procedimientos, que consisten en reducir las superficies de ataque de los sistemas mitigando los riesgos a los que estamos expuestos, eliminar vulnerabilidades en las aplicaciones y servicios, para mejorar la seguridad de los sistemas de información.

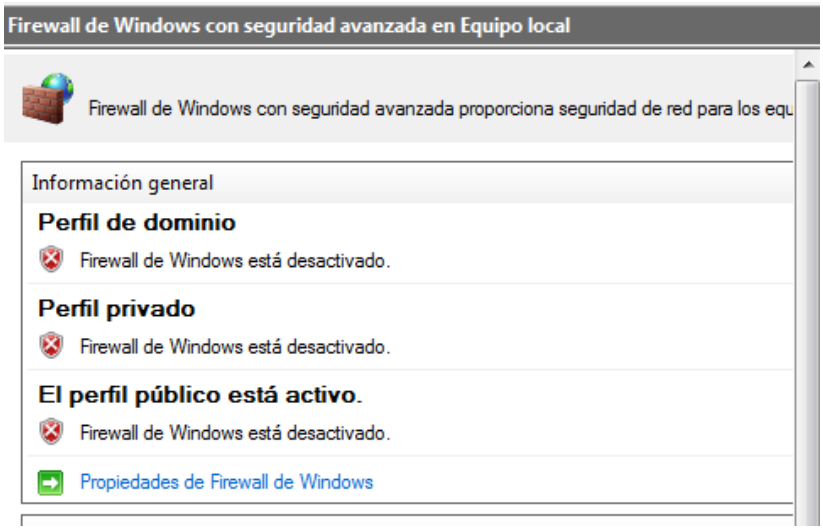
En el caso propuesto de la empresa WhiteHouse, durante el ejercicio de Red Team, se logró evidenciar una vulnerabilidad, la cual dio paso a la explotación de varias amenazas, esto debido a que el equipo presenta algunas fallas identificadas las cuales se pueden mitigar o diezmar siguiendo algunos pasos de fortalecimiento, como se enuncia a continuación.

[33] LOPEZ, Alberto, Tech Tips, consultado el 15 de marzo de 2022, recuperado de: https://www.youtube.com/watch?v=BBMS-WgluOA

- Activación y configuración de firewall.

Como se pudo descubrir, en los ejercicios desarrollados, el firewall de la maquina víctima se encuentra desactivado, al activarlo y configurarlo correctamente en los correspondientes perfiles de dominio, privado y público, se puede controlar los intentos de conexión tanto entrantes como salientes que no estén autorizados por la compañía o que sea innecesarios, para el ejercicio de las actividades de la empresa.

Figura 54: Firewall de la maquina victima desactivado.

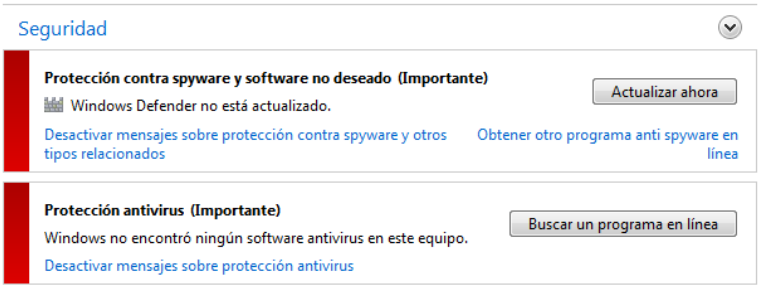


Fuente: el autor

- Software antivirus

Se pudo evidenciar que el equipo vulnerable, no cuenta con software antivirus, y que además la aplicación Windows Defender de Windows se encuentra desactivado, por tal motivo es necesario inicialmente activar dicho servicio y configurarlo de una manera adecuada para la protección del sistema, además se propone la adquisición de un software antivirus adecuado a las necesidades de la compañía.

Figura 55: Windows defender desactivado.

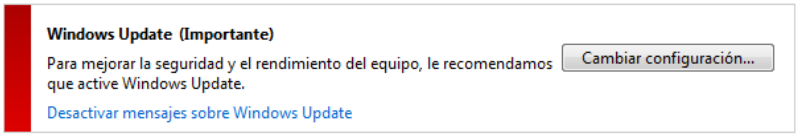


Fuente: el autor

- Actualizaciones de Software (programas y Sistema Operativo)

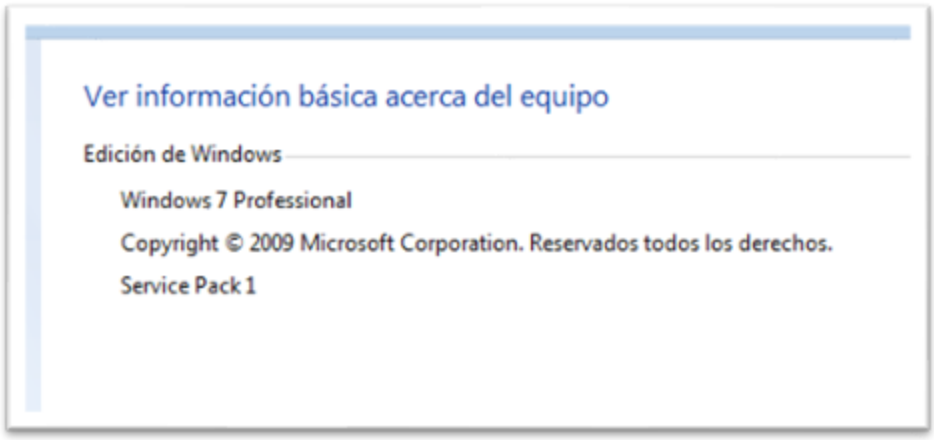
En este caso, el equipo analizado no cuenta con las actualizaciones correspondientes, y se encuentra desactivado el gestor de actualizaciones "Windows Update", es importante que tanto los programas así como el sistema operativo se encuentren con las correspondientes actualizaciones de seguridad, ya que esto permite que los fallos de seguridad que se vallan detectando sean reparados y debidamente parcheados, se puede evidenciar que la maquina objeto de análisis tiene instalado un Sistema Operativo Windows 7 x64, el cual es un sistema operativo obsoleto, dado que la empresa Microsoft ya no brinda soporte ni actualizaciones a este desde el día 14 de enero de 2020, por lo tanto se recomienda actualizar a otro sistema operativo más reciente, como Windows 10 o Windows 11.

Figura 56: Windows Update desactivado



Fuente: el autor

Figura 57: Información del Sistema Operativo obsoleto

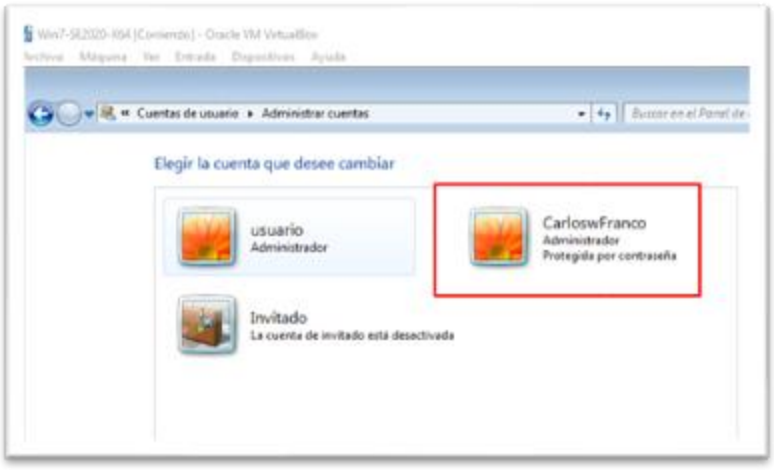


Fuente: el autor

- Políticas de usuarios y privilegios

Es importante que en las cuentas de usuarios sean acordes a los roles de cada uno de los trabajadores de la compañía así como los accesos y privilegios de los mismos, por tal motivo se debe verificar que las cuentas existentes, sean de usuarios reales y que estas no tengan privilegios excesivos, en el caso de la maquina objeto de estudio, esta posee dos usuarios con rol de Administrador, y si bien es cierto, una fue creada como producto del ataque, la cual debe ser eliminada inmediatamente, la otra debería ser degradada a usuario de tipo estándar.

Figura 58: Cuentas de usuarios en la maquina Victima.

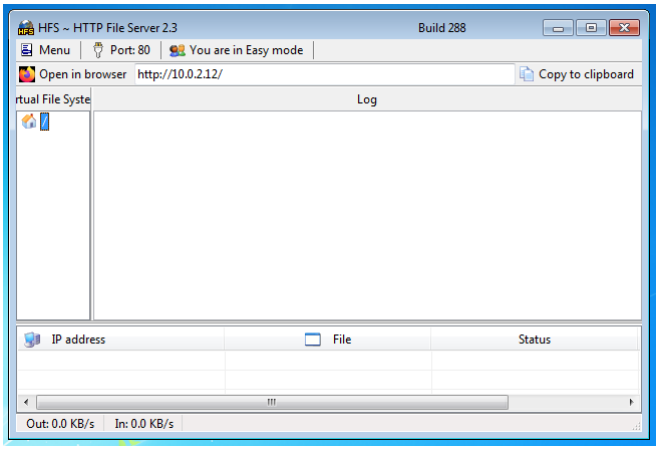


Fuente: el autor

- Restricción y Desinstalación de software innecesario

Es evidente para este estudio, que la brecha de seguridad descubierta por el equipo atacante, se originó a partir de una aplicación que iniciaba una vulnerabilidad, es por eso que es muy aconsejable la desinstalación de todos aquellos programas que sean innecesarios para el funcionamiento de la compañía, como es el caso de la aplicación HttpFileServer httpd 2.3 (rejetto), que genera una vulnerabilidad en el puerto 80/tcp, además de esto es importante generar políticas de restricción de instalación de aplicaciones por parte de los trabajadores de la empresa sin el respectivo análisis del área de seguridad de la información de quien haga sus veces.

Figura 59: Aplicación HttpFileServer

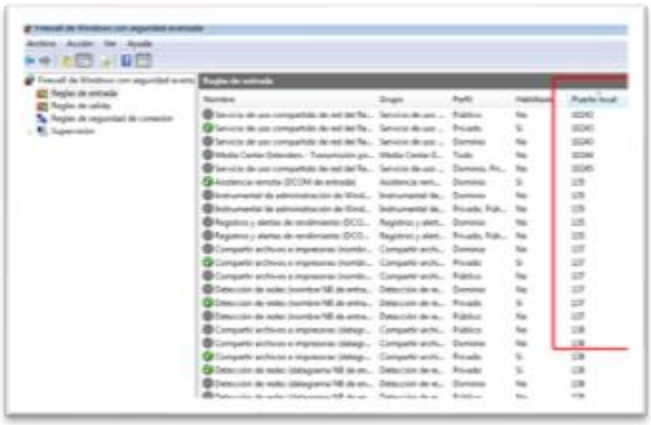


Fuente: el autor

- Monitoreo de puertos y servicios

Es importante efectuar un análisis periódico de los puertos y servicios que se encuentran abiertos en los equipos de la compañía, con el fin de restringir los servicios y puertos innecesarios.

Figura 60: Configuración de puertos y servicios en el firewall de Windows



Fuente: el autor

9.2 DIFERENCIAS ENTRE UN EQUIPO BLUE TEAM Y UN EQUIPO DE RESPUESTAS A INCIDENTES INFORMÁTICOS

Partiendo de la funcionalidad de los dos grupos, podríamos indicar que la finalidad puede estar relacionada e incluso confundir las funciones de un grupo con el otro, pero en el caso del equipo de respuesta a incidentes de seguridad o CSIRT por sus siglas en inglés "Computer Security Incident Response Team"[34] estos actúan de una manera más reactiva, ósea cuando se produce el evento, por ejemplo, un CSIRT debe atender los incidentes de seguridad reales que se presentan en la organización, y tomar acciones inmediatas, además de esto, un CSIRT debe velar por la generación de la cultura de seguridad informática en la organización y en comunicación con los CSIRT de otras organizaciones, generar constantemente alertas sobre las nuevas amenazas de seguridad que van surgiendo.
Por otra parte los equipos Blue Team, actúan de una manera más proactiva, identificando las falencias o vulnerabilidades que se puedan presentar para proteger

[34] Logsign, What is CSIRT? What are CSIRT Roles and Responsibilities?, consultado el 15 de marzo de 2022, recuperado de: https://www.logsign.com/blog/what-is-csirt-what-are-csirt-roles-and-responsibilities/

los activos críticos de una organización, y de la mano con los equipos Red Team, fortalecen los activos de información, realizando las pruebas necesarias para llevar a cabo dicha labor, dentro de las actividades de los equipos Blue Team encontramos, la realización de auditorías a los servidores de DNS, con el fin de prevenir algún ataque en la modalidad de phishing, y otras vulnerabilidades, realizar seguimiento y control a las políticas de manejo de usuarios y sus acceso a los sistemas, controles de seguridad de detección y prevención mediante software IDS e IPS, entre muchas otras más, pero siempre enfocado a la prevención y desde el interior de la organización.

10. CIS "CENTER FOR INTERNET SECURITY"

El CIS "Center For Internet Security" o centro para la seguridad en internet, es una entidad que se encarga de velar por la seguridad en el ciber espacio, utilizando las ventajas de la globalización de las tecnologías de la información a su favor, para mitigar las amenazas en las organizaciones tanto públicas como privadas[35].

El CIS utiliza como estrategia principal, la ayuda colaborativa y la comunicación constante con las diferentes organizaciones a nivel mundial, encargadas de la ciberseguridad de las organizaciones y de los gobiernos, coadyuvando a la generación de mejores prácticas y nuevas herramientas de seguridad cibernética, a través de frameworks, guías, controles y estándares entre otras herramientas.

Si dentro de mi equipo Blue Team me piden que trabaje con el "Center For Internet Security", utilizaría esta oportunidad para articular con todas las organizaciones participantes para conocer y estar a la vanguardia de todas las nuevas amenazas y vulnerabilidades en materia de ciberseguridad que día a día van surgiendo en el mundo, además apoyaría de manera activa en la generación de nuevo conocimiento y la cooperación con el centro, con los hallazgos de mi grupo; aunado a esto, aplicaría los conocimientos y la experiencia generada en la participación para fortalecer la organización con buenas prácticas en ciberseguridad.

[35] CIS, Center For Internet Security, consultado el 15 de marzo de 2022, recuperado de: https://www.cisecurity.org/

11. SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

Los sistemas SIEM, por sus siglas en ingles de “Security Information And Event Management”, es un software que se especializa en realizar un control de los eventos de seguridad presentados en un sistema y efectuar un análisis en tiempo real de todas las alertas de seguridad que generan las aplicaciones y los dispositivos de seguridad de la red[36]; este funciona centralizando todos los datos de registro que son generados por los diferentes equipos, firewalls, y antivirus entre otros, al igual que las alertas y eventos de seguridad.

Luego de esta recopilación y análisis de datos, el sistema genera una ponderación con base al nivel de amenaza detectada, siguiendo unos parámetros y reglas preestablecidas.

Entre muchas de sus ventajas encontramos la detección oportuna de amenazas de ciberseguridad, la reducción de los tiempos de respuesta ante posibles ataques, optimización del personal de respuesta a incidentes y la evaluación en tiempo real de seguridad de la organización, entre otras[37].

12. HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS

12.1 WAZUH

Wazuh es una herramienta de tipo EDR “Endpoint Detection and Response”, de código abierto y gratuita que se especializa en la monitorización de la red con el fin de detectar intrusiones o ataques evaluando la integridad de la misma y ofreciendo una respuesta a incidentes oportuna y precisa.

12.2 RAPID7 INSIGHTIDR

Según geekflare[38], Rapid7 InsightIDR, es una herramienta que permite el análisis, la respuesta y contención en tipo real de amenazas de seguridad en la red,

[36] Fireeye, What is SIEM and how does it work?, consultado el 15 de marzo de 2022, recuperado de: https://www.fireeye.com/products/helix/what-is-siem-and-how-does-it-work.html

[37] Mcafee, What Is Security Information and Event Management (SIEM)?, consultado el 15 de marzo de 2022, recuperado de: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-siem.html

[38] KINGATÚA, Amos, Geekflare; Las 9 mejores herramientas de respuesta a incidentes de seguridad para pequeñas y empresas consultado el 15 de marzo de 2022, recuperado de: https://geekflare.com/es/security-incident-response-

reconociendo entre muchos otros tipos de ataques y amenazas como phishing, malware, robo de credenciales y reconocimiento entre otros, dando la posibilidad de generar una respuesta rápida y oportuna al incidente.

12.3 OSSIM

OSSIM, siglas en inglés para “Open Source Security Information Management - Herramienta de Código Abierto para la Gestión de Seguridad de la información”, es una herramienta para la administración de ciberseguridad que está compuesta por varias herramientas que centralizan su actividad de detección, análisis, visualización y contención de todos los eventos de seguridad que se puedan presentar en una infraestructura de IT[39].

tools/#:~:text=Las%20herramientas%20de%20respuesta%20a,de%20seguridad%20internas%20y%20externas.

[39] BRAVO, ángel, VILLAFUERTE álvaro 7 September 2016' Escuela Superior Politecnica del Litoral'

CONCLUSIONES

Con el desarrollo de las actividades contenidas en el “seminario especializado equipos estratégicos en ciberseguridad red team & blue team”, se logró conocer la importancia de que una empresa u organización y su equipo o personal de seguridad de la información, conozca la legislación vigente relacionada con los delitos informáticos y los criterios para cada una de las actuaciones de la compañía en materia de ciberseguridad, y las implicaciones legales que conlleva el incumplimiento, la omisión o la extralimitación en actividades relacionadas con la seguridad informática, además es muy importante saber que todo profesional en tecnologías de la información, ingenieros y profesiones a fines, cuentan con un código de ética contenido en la Ley 842 de 2003, donde se estandariza el comportamiento, en el ejercicio de la profesión ante la sociedad.

Del mismo modo, se logró evidenciar, de manera práctica y bajo ambientes controlados, los riesgos a los que está expuesto un equipo o infraestructura de red, cuando se recibe un ataque por parte de un ciberdelincuente, y el rol que cumplen los equipos Red Team y Blue Team, al demostrar las vulnerabilidades de una infraestructura de TI, y la forma correcta de hardenizacion, endurecimiento o aseguramiento de la las tecnologías de la compañía, con el fin de mitigar los riesgos desde un punto de vista preventivo y correctivo, previniendo que se llegue a explotar alguna vulnerabilidad por parte de un atacante, esto aplicando las diferentes fases establecidas para la ejecución de un proceso de pentesting.

Aunado a lo anterior, cabe destacar, la importancia de conocer las herramientas disponibles en materia de ciberseguridad, las cuales nos permiten evaluar y analizar la infraestructura tecnológica de la organización, desde el punto de vista de un posible atacante y del mismo modo herramientas existentes que permiten el fortalecimiento de esta infraestructura y la mitigación de sus posibles vulnerabilidades.

RECOMENDACIONES

Toda organización, en donde, en sus actividades diarias tenga involucrados sistemas de información, tiene una alta susceptibilidad de presentar ataques por parte de ciber-delincuentes, con el ánimo de comprometer la seguridad de la información y de la infraestructura tecnológica de la compañía, esto, con diferentes fines maliciosos, y con el pasar del tiempo este riesgo se incrementa dado el increíble crecimiento de la capacidad de cómputo y las diferentes tecnologías que surgen día a día; es por ello que se recomienda a cualquier organización, la creación de equipos de seguridad informática que sean la primera barrera de contención para neutralizar o mitigar las vulnerabilidades que se puedan convertir en riesgos latentes para la integridad de la información de la compañía; dichos equipos se deben capacitar inicialmente en temas normativos, que permitan a la compañía conocer las implicaciones legales de las actuación de los trabajadores de la compañía, en especial de los equipos de ciberseguridad, en temas relacionados con delitos informáticos y violación de datos personales.

Por otra parte, es pertinente que los equipos de seguridad informática que se conformen en una compañía, empresa u organización, tengan conocimientos en las diferentes fases de los procesos de pentesting o pruebas de penetración, con el fin de desarrollar actividades de auto análisis de su infraestructura tecnológica, con el fin de identificar las vulnerabilidades que se puedan presentar, y poder coadyuvar a la compañía a fortalecer sus procesos desde el punto de vista tecnológico, esto con la ayuda de las diferentes herramientas tecnológicas existentes para la consecución de este propósito.

BIBLIOGRAFIA

BRAVO, ángel, VILLAFUERTE álvaro 7 September 2016' Escuela Superior Politecnica del Litoral'

Circular Externa 014, Superintendencia Financiera de Colombia, información detallada sobre las transacciones, 17 de abril de 2008, https://www.superfinanciera.gov.co/inicio/normativa/normativa-general/circulares-externas-cartas-circulares-y-resoluciones-desde-el-ano-/circulares-externas/-20146

CIS, Center For Internet Security, consultado el 15 de marzo de 2022, recuperado de: https://www.cisecurity.org/.

CVE-MITRE, National Vulnerability Database (NVD), consultado el 8 de marzo de 2022, recuperado de: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192

Decreto 1360, reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor, 23 de junio de 1989, D.O. 38.871, (Colombia), https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=10575

Decreto 1377, Reglamenta Ley 1581 de 2012, “Tratamiento de datos personales”, 27 de junio de 2013, D.O. 48834 MINTIC, (Colombia), https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

EL TIEMPO, Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue, OffSec Services Limited 2022https://www.eltiempo.com/archivo/documento/CMS-15141236

ENTER.Co, Detrás de Buggly: la historia de la fachada Andrómeda, consultado el 20 de febrero de 2022, recuperado de: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Exploit Database, OffSec Services Limited 2022, Exploit Database By Offensive Security, consultado el 21 de marzo de 2022, recuperado de: https://www.exploit-db.com/

Fireeye, What is SIEM and how does it work?, consultado el 15 de marzo de 2022, recuperado de: https://www.fireeye.com/products/helix/what-is-siem-and-how-does-it-work.html

INCIBE-CERT, Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287), consultado el 8 de marzo de 2022, recuperado de: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

JAVA T POINT, s.f., What is Metasploit, consultado el 5 de marzo de 2022, recuperado de: https://www.javatpoint.com/what-is-metasploit

KINGATÚA, Amos, Geekflare; Las 9 mejores herramientas de respuesta a incidentes de seguridad para pequeñas y empresas consultado el 15 de marzo de 2022, recuperado de: https://geekflare.com/es/security-incident-response-tools/#:~:text=Las%20herramientas%20de%20respuesta%20a,de%20seguridad%20internas%20y%20externas.

Ley 599 de 2000, Por la cual se expide el Código de Penal, 24 de julio de 2000, D.O. No. 44.097 (Colombia) http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr017.html#446

Ley 842 DE 2003, Código de Ética Profesional, 14 de octubre de 2003, D.O. No. 45.340 (Colombia) http://www.secretariasenado.gov.co/senado/basedoc/ley_0842_2003.html

Ley 906 de 2004, Por la cual se expide el Código de Procedimiento Penal, 31 de agosto, D.O. No. 45.658 (Colombia) http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004_pr001.html#:~:text=DEBER%20DE%20DENUNCIAR.,que%20deban%20investigarse%20de%20oficio.

Ley 1266 de 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, diciembre 31 de 2008, D.O. 47.219 (Colombia), https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488#:~:text=por%20la%20cual%20se%20dictan,y%20se%20dictan%20otras%20disposiciones.

Ley 1273 de 2009, De la Protección de la información y de los datos, 5 de enero de 2009, D.O. No. 47.223 (Colombia) http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Ley Estatutaria 1581, Disposiciones generales para la protección de datos personales, D.O. 48.587, (Colombia), http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

Logsign, What is CSIRT? What are CSIRT Roles and Responsibilities?, consultado el 15 de marzo de 2022, recuperado de: https://www.logsign.com/blog/what-is-csirt-what-are-csirt-roles-and-responsibilities/

LOPEZ, Alberto, Tech Tips, consultado el 15 de marzo de 2022, recuperado de: https://www.youtube.com/watch?v=BBMS-WgluOA

Mcafee, What Is Security Information and Event Management (SIEM)?, consultado el 15 de marzo de 2022, recuperado de: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-siem.html

NESSUS, Conozca sus vulnerabilidades e interrumpa las rutas de ataque, consultado el 8 de marzo de 2022, recuperado de: https://es-la.tenable.com/products/nessus

NMAP, Nmap Security, consultado el 8 de marzo de 2022, recuperado de: https://nmap.org/

NOVIELLO, Cómo instalar y configurar Nessus Vulnerability Scanner en Kali Linux, consultado el 8 de marzo de 2022, recuperado de: https://noviello.it/es/como-instalar-y-configurar-nessus-vulnerability-scanner-en-kali-linux/

OJEDA, Jorge, RINCON, Arias, Delitos informáticos y entorno jurídico vigente en Colombia. Cuad. Contab. [online]. 2010, vol.11, n.28, pp.41-66. ISSN 0123-1472, http://www.scielo.org.co/scielo.php?pid=S0123-14722010000200003&script=sci_abstract&tlng=es

PETTERS, Jeff, Varonis, Inside Out Security, Data Security, consultado el 5 de marzo de 2022, recuperado de: https://www.varonis.com/blog/nmap-commands

POSTON, Howard, Infosec, A brief introduction to the OpenVAS vulnerability scanner, consultado el 5 de marzo de 2022, recuperado de: https://resources.infosecinstitute.com/topic/a-brief-introduction-to-the-openvas-vulnerability-scanner/

RAPID 7, Metasploit - The world's most used penetration testing framework, consultado el 8 de marzo de 2022, recuperado de: https://www.metasploit.com/

Red Hat, Inc., What is a CVE, consultado el 21 de marzo de 2022, recuperado de: https://www.redhat.com/en/topics/security/what-is-cve

REJETTO, media wiki, consultado el 8 de marzo de 2022, recuperado de: https://www.rejetto.com/wiki/index.php?title=HFS:_Introducci%C3%B3n#:~:text=*%20comunica%20a%20tus%20amigos%20la,pega'%20y%20envia%20la%20direcci%C3%B3n.

The PTES Team, The Penetration Testing Execution Standard Documentation , Release 1.1, Jun 16, 2021, consultado el 20 de marzo de 2022, recuperado de:

https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf

WIKIMEDIA FOUNDATION, Inc, Open-source intelligence, consultado el 22 de febrero de 2022, recuperado de: https://en.wikipedia.org/wiki/Open-source_intelligence

ANEXO 1

LINK A VIDEO PARA SUSTENTACIÓN:

https://youtu.be/-lzE7mGee34