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

JUAN CAMILO USAMA VALENCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LA DORADA
2022

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

JUAN CAMILO USAMA VALENCIA

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Luis Fernando Zambrano Hernández
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LA DORADA
2022

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

AMENAZAS: son los posibles daños que pueden ocurrir, perjudicar sustancialmente el sistema de información de la empresa en caso de suceder y que derivarían en la pérdida de activos como información y dinero. Algunas de las amenazas que enfrentan diariamente las empresas a nivel informático son: Exposición de información confidencial, robo de contraseñas, phishing, spam, malware, redes zombie, exploit, ataques día cero, virus informáticos, denegación de servicios, caballos de troya, interceptación, entre otros.

ANTIVIRUS: es un software de computador, dispositivos móviles, tabletas y Mac, desarrollado para contrarrestar las infecciones maliciosas en los equipos. Tiene características para la protección de archivos, navegación segura en internet, almacenamiento de contraseñas, protección de la red, filtros anti-spam, defensa ante sitios web maliciosos y firewall. Ejecutar este software aumenta el nivel de seguridad frente a los virus dispersos por la red o embebidos en otros programas.

ATACANTES: son usuarios que poseen conocimientos en informática y aprovechan internet, para realizar estafas, daños, propagar virus, robar dinero, espiar personas o provocar daños en los computadores con la distribución de malware.

AUTENTICACIÓN: es un proceso mediante el cual el usuario que desee ingresar a los programas de la empresa, deberá suministrar un usuario y contraseña habilitados, para confirmar que efectivamente es la persona indicada y poder acceder a los recursos informáticos.

CORTAFUEGOS: es un software o dispositivo informático que previene el ingreso no autorizado de usuarios y/o programas a la red interna de la empresa. Se debe implementar una configuración para instaurar unas restricciones y autorizaciones para que los equipos se comuniquen de forma segura.

GUSANOS: son un tipo de software diseñado para introducirse y propagarse entre los equipos a través de la red. No necesitan la intervención del usuario para ejecutarse, sino que se distribuyen de manera completa por la red consumiendo un gran ancho de banda llegando a bloquear el equipo infectado, ralentizar los accesos a los programas y disminuir el rendimiento de las computadoras.

HACKER: en el ambiente popular se conocen como personas que se cuelan en los bancos y roban dinero de manera virtual, bloquean páginas web, atacan a los gobiernos y crean inestabilidad mundial. Pero nada más alejado de lo que se dice en los medios de comunicación. Un Hacker es una persona que tiene avanzados conocimientos en informática, lenguajes de programación, estrategias de seguridad, interés y motivación, para desarrollar nuevas tecnologías, poner a prueba las medidas de seguridad en las empresas, proteger datos y encontrar fallos de

seguridad para brindar soluciones que salvaguarden la información y privacidad de las personas.

IDS: los Sistemas de detección de intrusos son programas que permiten a las organizaciones identificar accesos no autorizados a la red o a una determinada computadora. Uno de los IDS más común es Snort, ya que su licencia libre y gratuita lo hace una alternativa interesante para su implementación.

INGENIERÍA SOCIAL: es la nueva habilidad desarrollada por delincuentes que se basa en artimañas y conversaciones amenas para obtener de los empleados información confidencial acerca de la empresa. Mediante el engaño o suplantación de algún personal de alto nivel en la organización, establecen comunicaciones o envían correos solicitando usuarios y contraseñas de los sistemas para obtener lucro de la información sustraída. También, suelen llamar haciéndose pasar por personal de soporte técnico que solicita información de los equipos de red, módem, routers y switches, o solicitando la instalación de programas remotos para acceder a los computadores.

LAMMER: son reconocidos como novatos pero que se consideran expertos informáticos sin poseer los conocimientos que acrediten dicho nivel de experiencia técnica y que presumen de eso aplicando herramientas que han desarrollado especialistas en programación.

MALWARE: software de mucho cuidado, ya que su creación es malintencionada (virus, troyanos o gusanos) con el fin de introducirse en la computadora y provocar daños en el sistema de múltiples formas.

PHISHING: se considera una suplantación o falsificación ingeniosa en la que se presenta una página web como oficial, haciendo creer al usuario que puede ingresar sus credenciales de autenticación (usuario y contraseña) para ser recolectados y utilizados en fraudes. El nivel de similitud de las páginas es alto, pero se diferencia de las originales por errores ortográficos que se les pueden pasar a los delincuentes, porque la dirección URL apunta a otro servidor, porque no tienen los certificados de seguridad válidos, entre otros.

SEGURIDAD INFORMÁTICA: son el conjunto de estrategias, políticas, procesos y medidas que protegen la información circulante al interior y exterior de la empresa a través de equipos de cómputo, red local e internet con el fin de evitar que sea capturada por personal ajeno.

SNIFFER: son programas de computadora operados por personas que cuentan con el conocimiento en redes para analizar el tráfico de una red para y obtener información de los paquetes que se envían.

SNORT: es un software que opera bajo una licencia comercial y libre que permite configurarse tanto para la detección de intrusos como su prevención.

SPOOFING: esta técnica de hacerse pasar por otro o suplantación, suele estar relacionado con usos maliciosos consistentes en sustituir las direcciones IP de los computadores de la empresa para que la información sea enviada al host del atacante y capturar el tráfico entre los computadores atacados.

SPYWARE: los programas espías que tienen como finalidad capturar información de la navegación del usuario en internet para que terceros obtenga algún beneficio de ella.

TROYANOS: es un software malicioso en apariencia inofensivo pero que facilita el acceso remoto a la computadora de la víctima, para que el atacante tome el control y pueda ver todo lo que hace el usuario sin que se percate de lo sucedido. Son los programas informáticos de mayor peligro en la red internet.

VIRUS: son programas que se propagan en los equipos de cómputo con la finalidad de infectarlos, agotar sus recursos de funcionamiento, bloquear los equipos, estropear el funcionamiento del ordenador o simplemente inutilizarlo.

VPN: la red privada virtual permite brindar un nivel de seguridad superior al simple hecho de tener un antivirus y contraseñas de más de 8 caracteres en la empresa. Esta red virtual permite conectar una o más computadoras agrupándolas en una red con conexiones más seguras para aumentar la seguridad cuando se navega en internet.

VULNERABILIDAD: es un fallo lógico o físico en los programas informáticos que se ejecutan en las computadoras y que comprometen la seguridad del sistema. Por consiguiente, los programas deben actualizarse desde la página web del fabricante periódicamente para corregir estos errores.

RESUMEN

En el presente informe técnico se presentan los procedimientos desarrollados para la consecución de cada uno de los objetivos planteados por la empresa Hackers Security en la conformación de los equipos Red Team y Blue Team. En este proceso se evidencian varias etapas que inician con la conformación del banco de trabajo, la identificación de leyes colombianas frente a delitos informáticos, el análisis de la actuación ética y legal del profesional frente a un acuerdo que vulnera los principios de integridad y confidencialidad de la información, la ejecución de una prueba de intrusión, pentesting, explotación de vulnerabilidades y posteriormente contención de ataques informáticos. Lo anterior, con el fin de formar al profesional en los ámbitos técnicos, estratégicos, éticos y legales en el desarrollo de su trabajo en ciberseguridad.

PALABRAS CLAVE

Ciberseguridad, contención, explotación, pentesting, seguridad, vulnerabilidad,

ABSTRACT

This technical report presents the procedures developed to achieve each of the objectives set by the company Hackers Security in the formation of the Red Team and Blue Team teams. In this process, several stages are evidenced that begin with the creation of the workbench, the identification of Colombian laws against computer crimes, the analysis of the ethical and legal performance of the professional against an agreement that violates the principles of apparatus and confidentiality of the information, the execution of an intrusion test, pentesting, exploitation of vulnerabilities and later containment of computer attacks. The foregoing, in order to train the professional in the technical, strategic, ethical and legal fields in the development of their work in cybersecurity.

1 INTRODUCCIÓN

En la actualidad, se están generando oportunidades tecnológicas que involucran cada vez más la implementación de equipos informáticos al interior de las organizaciones para procesar información, analizar datos, generar estadísticas y evaluar propuestas que permitan ser competitiva a la organización. Este crecimiento tecnológico e informático trae consigo unos desafíos frente a la responsabilidad de proteger la información, su integridad, disponibilidad y confidencialidad de ataques informáticos realizados por ciberdelincuentes. Así mismo, la protección de los activos informáticos de cualquier intrusión, amenaza, vulnerabilidad o explotación, que conlleve a la indisponibilidad de servicios prestados por la empresa o robo de información. Por consiguiente, es fundamental contar con personal que constantemente esté realizando monitoreo a la red, actualizando los sistemas operativos, instalando los parches de seguridad, validando los accesos a los sistemas informáticos e informando a los usuarios sobre nuevas amenazas. Es allí, donde la conformación al interior de las organizaciones de los equipos Red Team y Blue Team, cobra gran relevancia, ya que estos permiten desarrollar medidas de seguridad y estrategias de protección informáticas, a través de la realización de pentesting para encontrar fallas o debilidades en la infraestructura de TI de la organización con el fin de corregirlas, protegerse de virus, ransonware, malware o phishing, que son variantes maliciosas de software que comprometen el funcionamiento de las empresas.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Construir un informe técnico en el que se establezcan las estrategias de seguridad aplicadas en la conformación de los equipos estratégicos en ciberseguridad Red Team y Blue Team, para la contención de incidentes informáticos mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

2.2 OBJETIVOS ESPECÍFICOS

- Realizar la identificación de la normatividad legal vigente sobre delitos informáticos y protección de datos personales para establecer las responsabilidades del equipo Red Team y Blue Team.

- Identificar herramientas y vulnerabilidades dentro del sistema que permita a los equipos Red Team y Blue Team instaurar las medidas de protección frente a un ataque informático.

- Definir las herramientas informáticas que permiten contener un incidente informático en tiempo real sin llegar a comprometer la infraestructura TI de la organización.

3 MARCO REFERENCIAL

Actualmente, tanto las empresas como los usuarios almacenan grandes volúmenes de información en los computadores. Los mismos, son utilizados para realizar operaciones comerciales, ejecutar compras por internet, ventas en la web, consultar cuentas bancarias, efectuar transferencias, comunicarse con clientes e intercambiar información. Ambos campos, particular y empresarial, tienen a su disposición equipos conectados a internet que ayudan a optimizar sus procesos productivos. Dada la importancia que supone para los organismos mencionados la información con la que estén trabajando, cualquier fallo de software y hardware puede derivar en una pérdida económica, pérdida de información, corrupción en las bases de datos, una interceptación de mensajes, un robo de claves, una suplantación de identidad o un secuestro de datos a cambio de dinero por parte de cibercriminales, de modo que es muy importante procurar por un correcto funcionamiento de los sistemas y redes informáticas.

Por otro lado, no se puede seguir considerando la falsa creencia de muchos usuarios, de que no les puede pasar nada ya que no tienen información importante como para llamar la atención de cibercriminales. Este pensamiento es erróneo y equivocado, porque, aunque no se aprecie a simple vista, los datos personales, son ahora la mina de oro para ciberdelincuentes. Por consiguiente, afrontar esta problemática desde el interior de las organizaciones, es un desafío que debe afrontarse con planeación, previsión, estrategias, medias de seguridad, políticas y talento humano que se encargue de implementar soluciones que fortalezcan la seguridad informática en la organización y es allí, donde los equipos Red Team y Blue Team, tienen la responsabilidad de proteger la infraestructura TI.

3.1 DESARROLLO DEL INFORME

3.1.1 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.

En la actualidad, el auge de la tecnología y su incidencia en los diferentes campos de la vida cotidiana de las personas (compras, ventas, transacciones, servicios, negocios, entre otros) han dado lugar a que criminales cometan intrusiones, estafas, suplantaciones y fraudes, que comprometen la información no solo a nivel personal sino también empresarial, causando caídas en los servicios, indisponibilidad de aplicaciones y pérdidas económicas. Por consiguiente, en Colombia se han sancionado leyes sobre delitos informáticos y protección de datos personales, que se han tipificado con el fin de promover la seguridad de la

información y castigar las infracciones. Algunas de las leyes que conforman el marco legal son:

- Ley 603 de 2001, “contempla solicitar a las empresas un informe de gestión donde se expone el estado de cumplimiento de las normas de propiedad intelectual y derechos de autor”[1], es decir, listando el licenciamiento correcto del software que se ejecuta en las computadoras.

- Ley estatutaria 1266 del 31 de diciembre de 2008, “en esa 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”[2].

- Ley 1273 del 5 de enero de 2009, en esta ley se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado: “de la protección de la información y de los datos”[3] - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. Además, se describen delitos como: Artículo 269A. Acceso abusivo a un sistema informático, acontecimiento en el que un individuo sin autorización o sin consentimiento acordado, acceda a todo o a una parte del sistema de informático protegido con medidas de seguridad, incurrirá en una sanción penal de cuarenta y ocho (48) a noventa y seis (96) meses y una sanción económica de 100 a 1000 salarios mínimos legales vigentes.

- **Artículo 269B. Obstaculización ilegitima de sistema informático o red de telecomunicación**, a quién sin estar autorizado para ello, impida el correcto funcionamiento o acceso normal a un sistema informático, o a los datos de la red, incurrirá en una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses de prisión y una sanción económica de 100 a 1000 salarios mínimos legales vigentes.

[1] Kennertech. Ley 603 del 2000 tecnología de la información. [Sitio web]. Bogotá. [Consulta 04 de septiembre de 2022]. https://www.kennertech.com.co/ley-603-del-2000-tecnologia-de-la-informacion/

[2] Congreso de la república. 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, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [Sitio web]. Bogotá. [Consulta 05 de septiembre de 2022]. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[3] Policía Nacional. Normatividad sobre delitos informáticos. Ley 1273 de 2009. [Sito Web]. [Consulta 04 de septiembre de 2022]. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Artículo 269C. Interceptación de datos informáticos, el individuo que no esté facultado judicialmente e intercepte los datos en un sistema informático, incurrirá en una pena de prisión de treinta y seis (36) a setenta y dos (72) meses. **Artículo 269D.** Daño informático, persona que destruya, dañe, suprima, deteriore o altere datos informáticos, o un sistema de información, o alguna de sus partes, incurrirá en una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses de prisión y una sanción económica de 100 a 1000 salarios mínimos legales vigentes. **Artículo 269E**. **Uso de software malicioso**, la persona que produzca, trafique, adquiera, comercialice, introduzca o extraiga software malicioso que afecte los equipos de computación, incurrirá en una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses de prisión y una sanción económica de 100 a 1000 salarios mínimos legales vigentes. **Artículo 269F. Violación de datos personales**, cuando una persona se aproveche de un tercero, para obtener, sustraer, vender, intercambiar, divulgar o modificar, o emplee datos personales incluidos en ficheros, bases de datos, entre otros incurrirá en una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses de prisión y una sanción económica de 100 a 1000 salarios mínimos legales vigentes violación de datos personales. **Artículo 269G. Suplantación de sitios web para capturar datos personales**, cuando un individuo con habilidades informáticas sin estar autorizado desarrolla páginas electrónicas falsas o modifique los sitios de ingresos seguro a plataformas virtuales del usuario haciéndole creer que está en la página oficial de una entidad y capture de manera ilegal datos personales con la finalidad de vender, traficar o estafar. Incurrirá en una pena señalada. **Artículo 269H. Circunstancias de agravación punitiva,** las penas se aumentarán de la mitad a tres cuartas partes si los daños son cometidos sobre redes o sistemas informáticos estatales, por servidor público en realización de sus funciones, aprovechándose de la confianza otorgada por quién tuviese una relación contractual, revelando información en perjuicio de otro, obteniendo provecho para sí mismo o un tercero, utilizando la información con fines terroristas y aprovechándose de un tercero. **Artículo 269I. Hurto por medios informáticos y semejantes**, el que, superando las medidas de seguridad informáticas, manipulando un sistema informático o suplantando a un usuario en los sistemas de autenticación y autorización, incurrirá en una pena de prisión de 3 a 8 años. **Artículo 269J. Transferencia no consentida de activos,** cuando un individuo con fines lucrativos y valiéndose de artimañas, consiga la transferencia no consentida de cualquier activo perjudicando a un tercero constituirá un delito.

- Ley 44 de 1993, “en esta ley específica penas entre dos y cinco años de cárcel, así como el pago de indemnizaciones por daños y perjuicios a quienes cometan el delito de piratería de software”[4]. Se considera delito el uso o reproducción de un programa de computador de manera diferente a como está estipulado en la

[4] El Congreso de Colombia. Ley 44 de 1993 Nivel Nacional. [Sitio web]. Bogotá. [Consulta 05 de septiembre de 2022]. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3429&dt=S

licencia. Los programas que no tengan licencia son ilegales y es necesaria una licencia por cada copia instalada en los computadores. A partir del mes de julio de 2001, y gracias a la reforma hecha al Código de procedimiento penal, “quien sea encontrado usando, distribuyendo o copiando software sin licencia estará supeditado pena carcelaria por un período de cinco (5) años”[5].

- Ley 890 de 2004, “esta ley presenta las normas que regulan y sancionan la ilegalidad o piratería de software en Colombia: Código Penal: El Art. 271. Reformado por la Ley 890 de 2004: Hace referencia a quien sin autorización previa y expresa reproduzca, alquile, distribuya programas de ordenador”[6] incurrirá en prisión de 2 años y 8 meses a 7 años y 6 meses y multa de 20 a 1000 salarios mínimos legales.

- Ley 1581 de 2012 Ley de protección de datos personales en Colombia. El derecho al abeas data o derecho a la información, constituyen el marco general de la protección de datos en Colombia. Esta ley dictamina que los responsables de la recolección de información deberán suministrar una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación o supresión. Así mismo, como explicar los fines de la recolección de la información y la previa solicitud de la autorización de la persona para su posterior tratamiento. No se podrán utilizar medios engañosos o fraudulentos para recolectar y realizar tratamiento de datos personales. En este sentido, las PYMES también están llamadas al cumplimiento de esta ley, cuando se solicita al titular del dato determinada información, deberán explicar el tratamiento al cuál serán sometido los datos personales, la finalidad del mismo y convendrán dejar por escrito previa autorización del usuario. La PYME deberá velar e implementar estrategias de seguridad para salvaguardar la información, ya que, de lo contrario, puede ser objeto de sanciones. Así mismo, resaltar que los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales asentados en cualquier base de datos que los conciba aptos de aplicar algún tratamiento por empresas públicas o privadas. De esta manera, cada vez que una base de datos vaya a ser transferida a un tercero, deberá previamente haber sido informada y autorizada por el titular.

[5] EL CONGRESO DE COLOMBIA, Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. [Sitio web]. Colombia. [Consulta: 04 de septiembre de 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0044_1993.html.

[6] El Congreso de Colombia. Ley 890 de 2004. [Sitio web]. Bogotá. [Consulta de septiembre de 2022]. http://www.secretariasenado.gov.co/senado/basedoc/ley_0890_2004.html

3.1.2 Definir cada una de las etapas del pentesting.

“El pentesting es una prueba de acceso legal y autorizado a sistemas de información, con el objetivo de hacerlos más seguros, mediante herramientas para la identificación y explotación de vulnerabilidades”[7]. Las etapas del pentesting son:

- Reconocimiento. En esta fase el profesional en seguridad define los objetivos de la prueba, plantea el alcance técnico al que se espera llegar, recopila información de la empresa a través de sitios web que contengan datos de la empresa, redes sociales, blogs y plataforma digitales. Una de las herramientas que se utiliza para obtener información acerca de las empresas es WHOIS, que brinda datos acerca del dominio de la organización, cuando fue creado, como se administra, ciudad, información de contacto, dominios, correo electrónico, entre otros. Así mismo, NETCRAF, es una página web que permite analizar rápidamente servidores y subdominios, a partir de un dominio web, para identificar que versiones de sistemas se están utilizando, vulnerabilidades, fallos de seguridad, errores de configuración y versiones desactualizadas.

- Escaneo. En esta fase se pretende recolectar datos relevantes a través del cliente o fuentes externas. Identificar protocolos, sistemas y servidores con vulnerabilidades. Algunas de las aplicaciones más conocidas en esta fase son: NESSUS, OPENVAS Y NMAP, siendo NMAP una de las más utilizadas ya que permite efectuar rastreo de puertos, descubrir servicios y servidores en una red informática a través de un llamado ping, identifica puertos abiertos en las computadoras, servicios que se están ejecutando, sistemas operativos y algunas características del hardware.

- Explotación. En esta fase se pretende identificar información clave sobre nuestros objetivos. En este proceso se accede a los sistemas vulnerables identificados, se pretende obtener privilegios (usuarios y contraseñas). La herramienta más conocida es METASPLOIT, esta permite aprovechar un motor de base de datos y payloads, para explotar las vulnerabilidades encontradas. De igual forma, ARMITAGE, es otra herramienta que permite ingresar una dirección IP de la consola que se está atacando e identificar puertos abiertos, sistemas operativos y correr los diferentes ataques que se encuentran (ftp, http, irc, samba, ssh, vnc, entre otros) después del escaneo.

[7] ZULUAGA MATEUS, Allen David. HACKING ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la Rama Judicial, seccional Armenia.[En línea]. Trabajo de grado aplicado. Universidad Nacional Abierta y a Distancia, 2017. [Consulta 05 de septiembre de 2022]. Disponible en https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf.

- Post explotación. Después de aprovechar las vulnerabilidades encontradas se pretende seguir escalando hacia otros sistemas y generar nuevos accesos, crear puertas traseras, mantener, conservar el acceso y privilegios. METERPRETER¸ es una herramienta que permite establecer conexiones remotas programadas y SHELLTER sirve para encubrir las huellas de la explotación.

- Reporte. Es la etapa en la que se revisa la información obtenida del proceso de pentesting. Se revisa la información base obtenida a través de fuentes internas y externas. Se documentan las vulnerabilidades. Se presentan los resultados de las explotaciones, computadores a los que se logra el acceso y se documentan las puertas traseras creadas. Así mismo, como redactar el documento de acuerdo a la persona que vaya a leerlo para que sea comprendido de la mejor forma.

3.1.3 Herramientas de ciberseguridad. Existe una gran variedad de herramientas informáticas o distribuciones como Kali Linux, que reúnen un conjunto de programas que se utilizan en la realización de pentesting. Algunas de las herramientas más populares en la implementación de estas pruebas son: Metasploit, herramienta de seguridad que permite aprovechar las características de un sistema para que funcione de una manera diferente a la que fue diseñada. Encontrar vulnerabilidades y explotarlas. El programa ejecuta una base de datos con scripts que se corren sobre las vulnerabilidades encontradas en el sistema que se está auditando. Así mismo, cuenta con una serie de módulos como: Auxiliary, payloads, exploits, nops, post, enconders y evasión que se utilizan para lograr el objetivo planteado en el pentesting. La forma de implementar la herramienta en una distribución Kali Linux es a través de la instalación del gestor de bases de datos que usa esta herramienta, denominado postgresql sudo apt-get install -y postgresql. Nmap, es una desarrollada para auditoría de seguridad y exploración de redes, protocolos UPD, TCP y ARP, para detectar equipos activos. Con la herramienta podemos realizar un tipo de escaneo ICMP echo scanning/ping sweep. La herramienta se puede ejecutar a través de la distribución Kali Linux y se pueden ejecutar un comando nmap -sp 192.168.3.0/24 para escanear los equipos en una red. Nmap es compatible con la mayoría de sistemas operativos, ofrece un conjunto de herramientas para usuarios iniciales y avanzados.

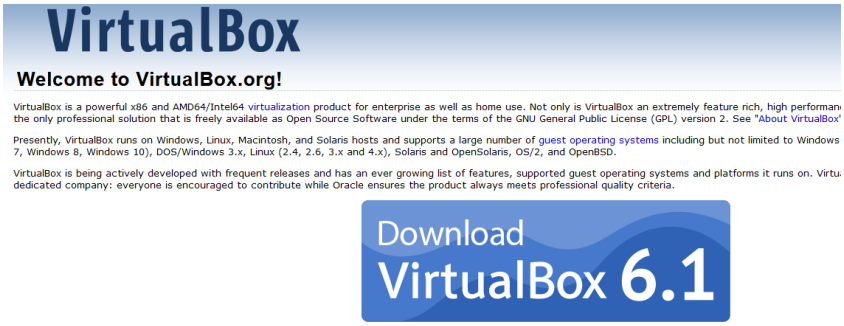
Las aplicaciones son variadas, desde pruebas de pentesting, tareas de seguridad informática, hacking, verificación de aplicaciones no autorizadas en la red, auditar la seguridad de la red, entre otros. OpenVas, “es una herramienta de escaneo de vulnerabilidades conocidas en los sistemas de cómputo de una empresa, tiene una interfaz web con varios ítems para realizar diferentes tareas”[8]. Una de sus funcionalidades es categorizar las vulnerabilidades encontradas en alto riesgo, medio riesgo y bajo riesgo. Al finalizar el escaneo se genera un reporte con la información de los huecos de seguridad encontrados. ExploitDB, es una herramienta para identificar debilidades en la red informática de la empresa y mantener actualizados los controles de seguridad con el fin de evitar ataques a la infraestructura tecnológica. De igual manera, es utilizado en pruebas de pentesting por profesionales en seguridad informática.

CVE, recoge una lista de nombres estandarizados de vulnerabilidades y exposiciones de seguridad de la información conocidas públicamente. Su objetivo es permitir el intercambio de información sobre vulnerabilidades conocidas entre organizaciones y puede contribuir a que las organizaciones establezcan parámetros base para evaluar el alcance de sus herramientas de seguridad.

[8] OPENWEBINARS. ¿Qué es OpenVAS?. [Sitio web]. Sevilla. [Consulta: 06 de septiembre]. Disponible en: https://openwebinars.net/blog/que-es-openvas/

3.1.4 Banco de trabajo. Descargar la herramienta virtualizadora “VirtualBox” en su última versión. Se procede a realizar la descarga de la herramienta virtual box ingresando en el link https://www.virtualbox.org/ para virtualizar las imágenes OVAS propuestas en el momento inicial.

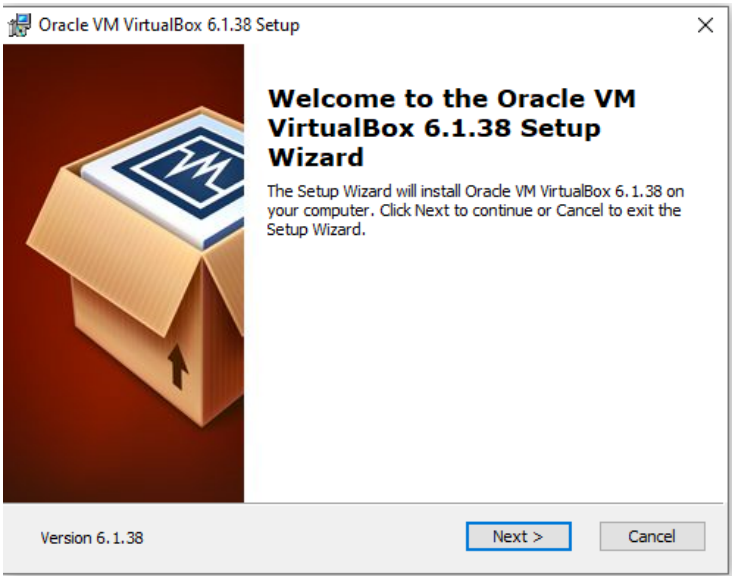
Ilustración 1. Descarga virtualbox



Fuente 1: Juan usama

Se procede con la instalación de VirtualBox

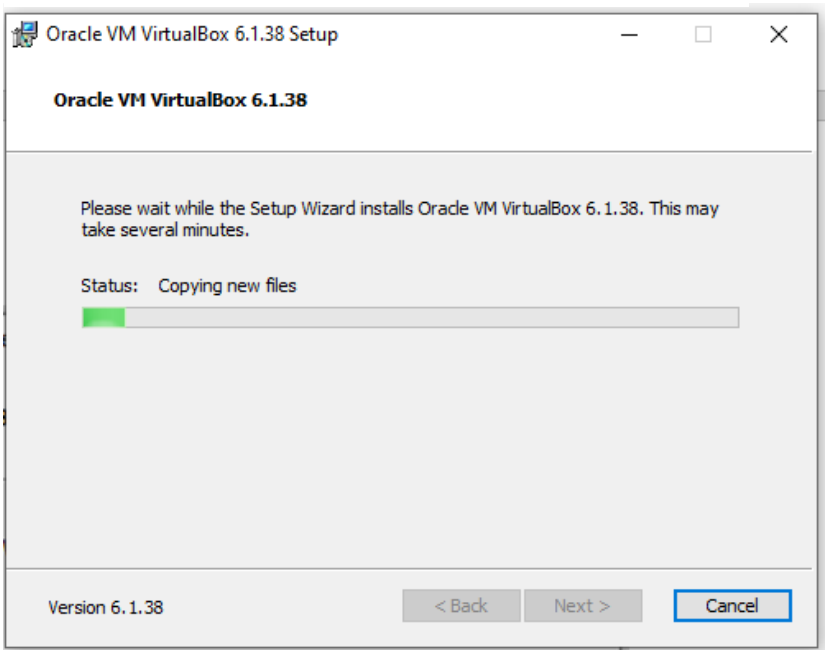
Ilustración 2. Instalación virtual box



Fuente 2: Juan usama

Se continua con el asistente de la instalación

Ilustración 3. Proceso instalación Virtualbox



Fuente 3. Juan usama

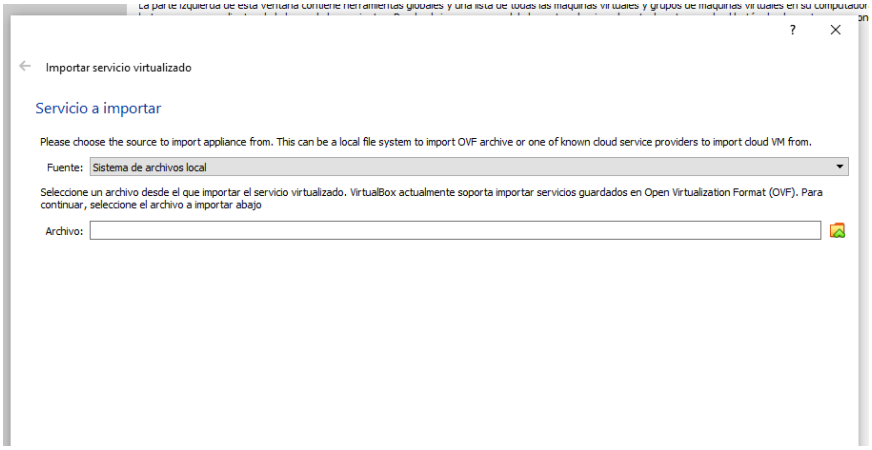
Finaliza la instalación.

Ilustración 4. Virtualbox instalado

Fuente 4. Juan usama

Carga de imágenes entorno virtualizado. Se inicia con Windows 7 x32

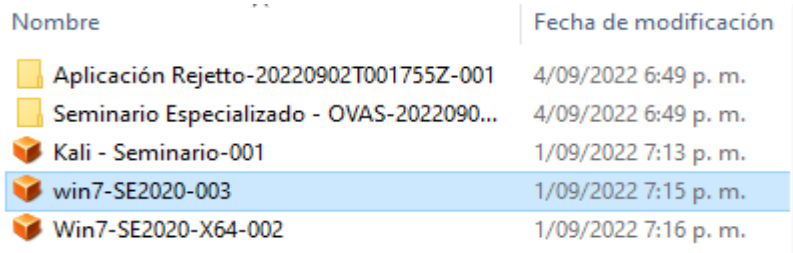
Ilustración 5. Importe windows 7 x32



Fuente 5. Juan usama

Seleccionamos la imagen a importar.

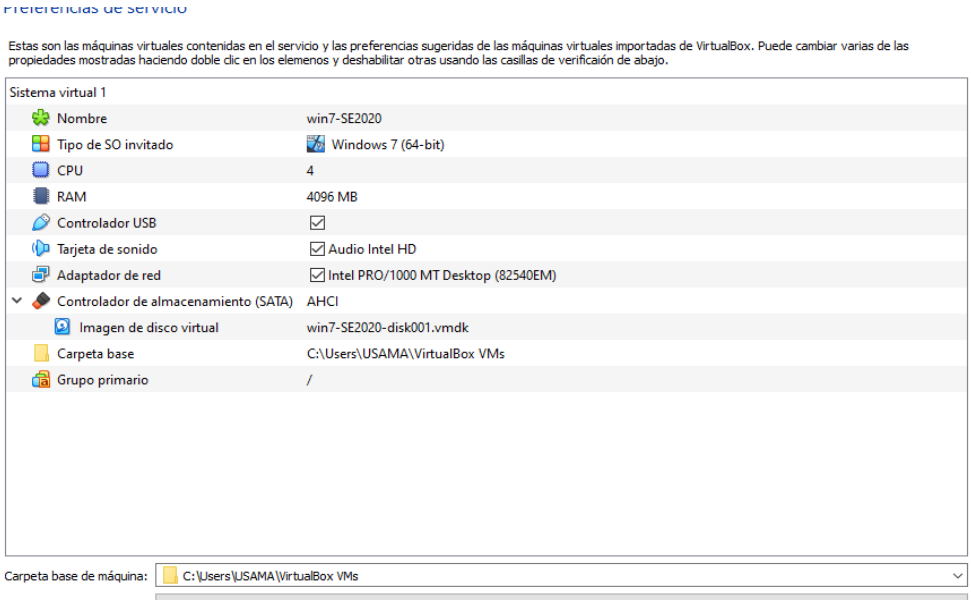
Ilustración 6. Selección imagen OVA



Fuente 6. Juan usama

Se visualizan las características de la imagen importada.

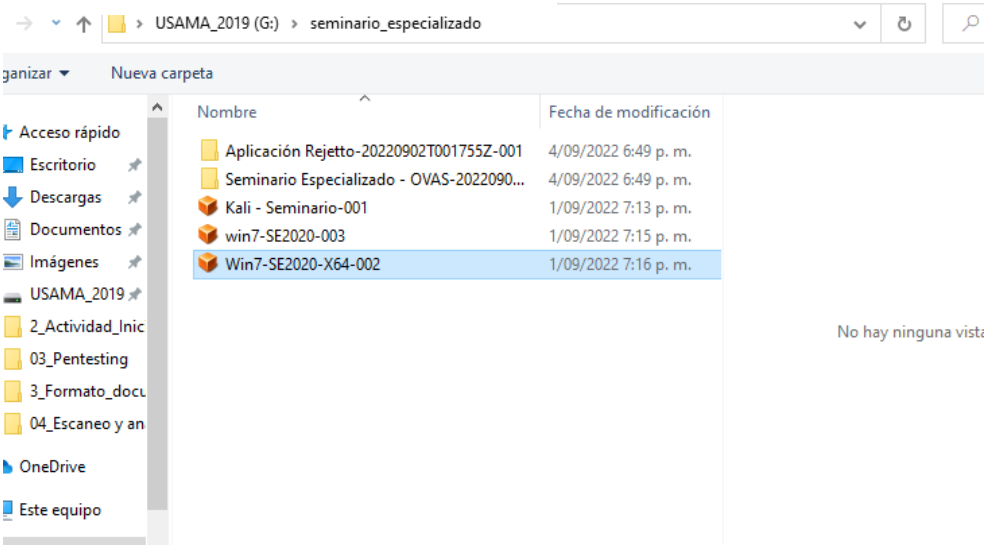
Ilustración 7. Requerimientos sistema



Fuente 7. Juan usama

Se procede a importar la segunda imagen de Windows 7 x64.

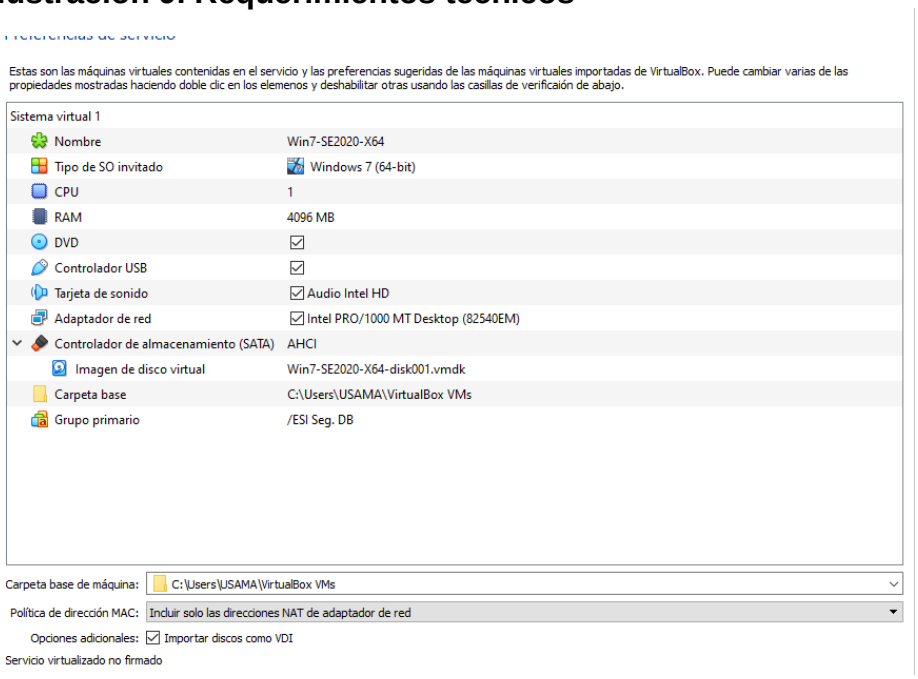
Ilustración 8. Importe windows 7 x64



Fuente 8. Juan usama

Se observan los requerimientos de la segunda imagen OVA.

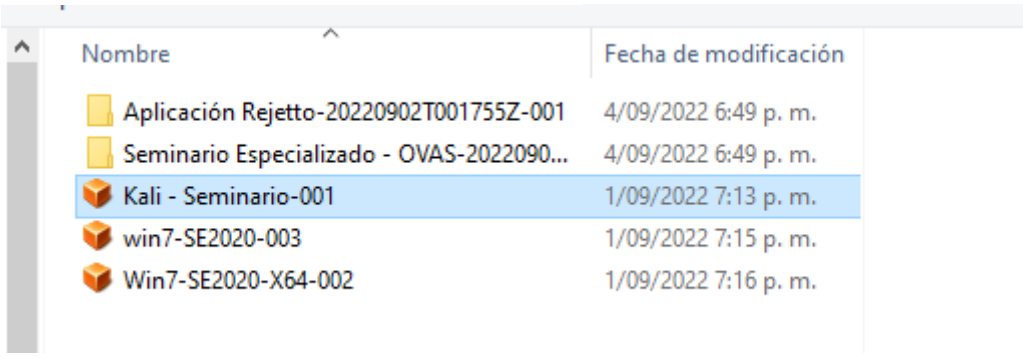
Ilustración 9. Requerimientos técnicos



Fuente 9. Juan usama

Se finaliza importando la imagen de Kali linux

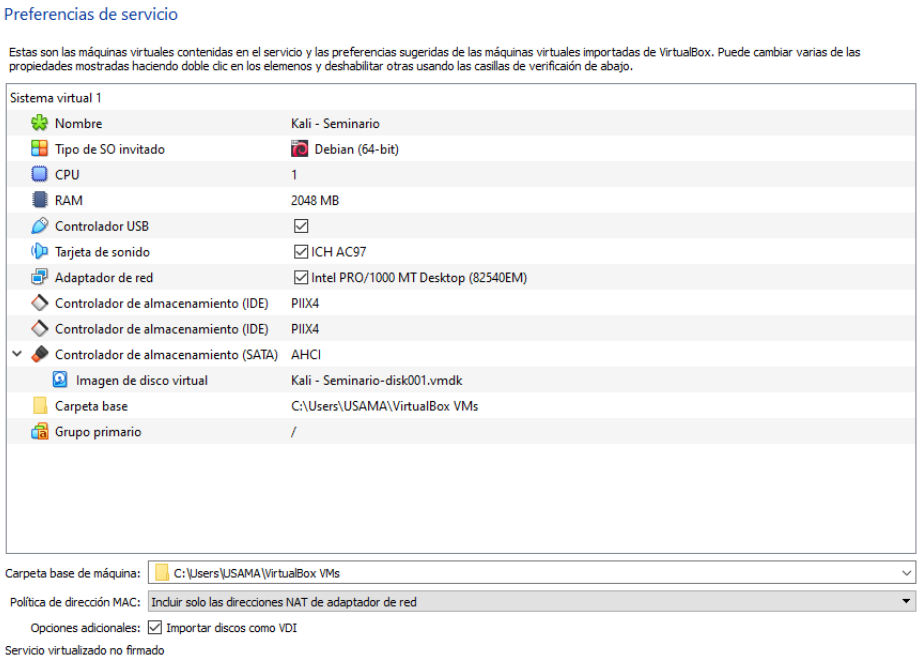
Ilustración 10. Importe kali linux



Fuente 10. Juan usama

Se observan los requerimientos de la segunda imagen OVA.

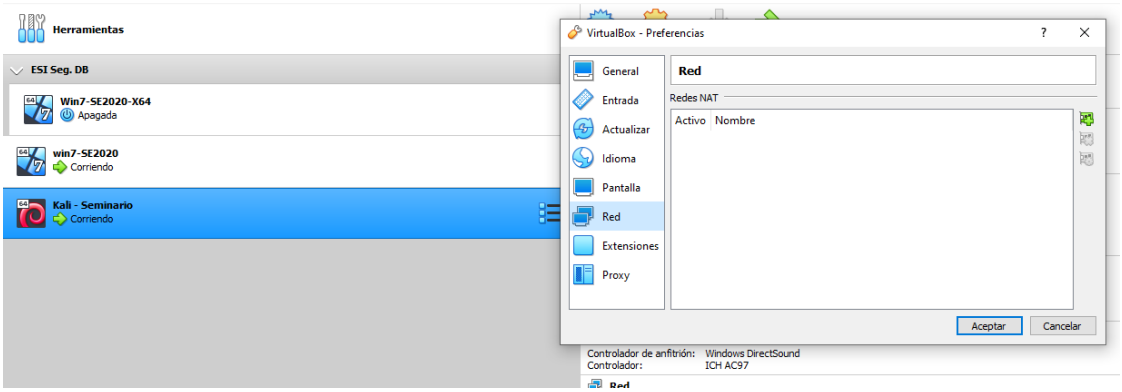
Ilustración 11. Requerimientos kali linux



Fuente 11. Juan usama

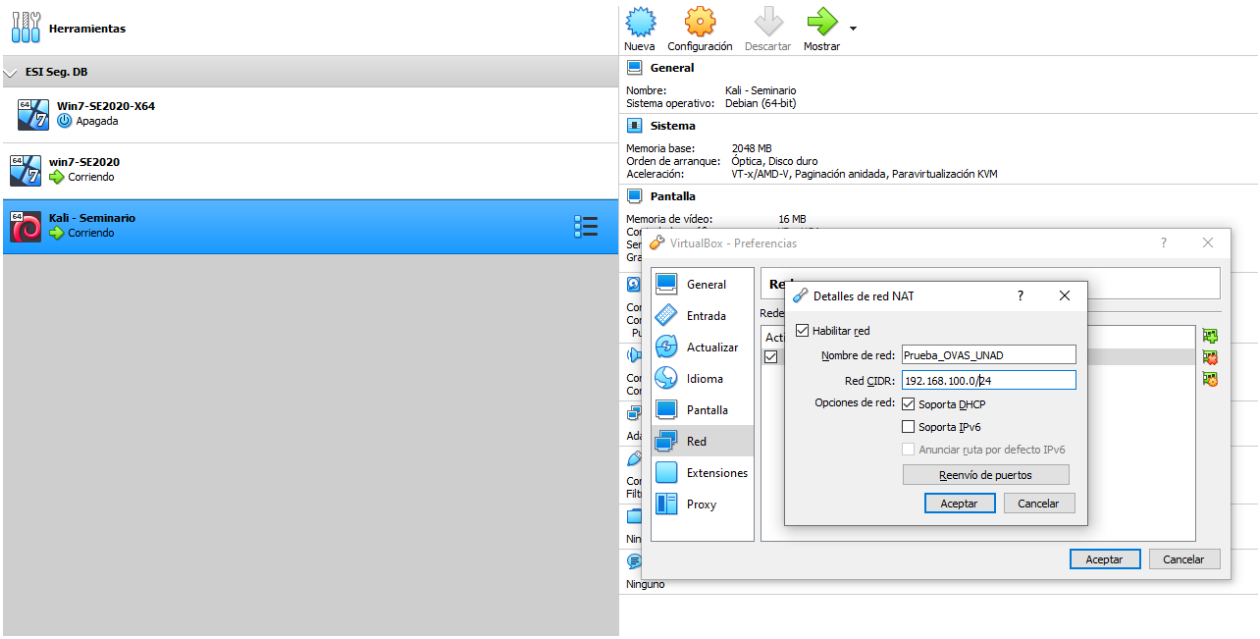
Validar comunicación entre las máquinas virtuales. Procedemos a crear una nueva red NAT ingresando en el menú **archivo – preferencias - red**

Ilustración 12. Crear red



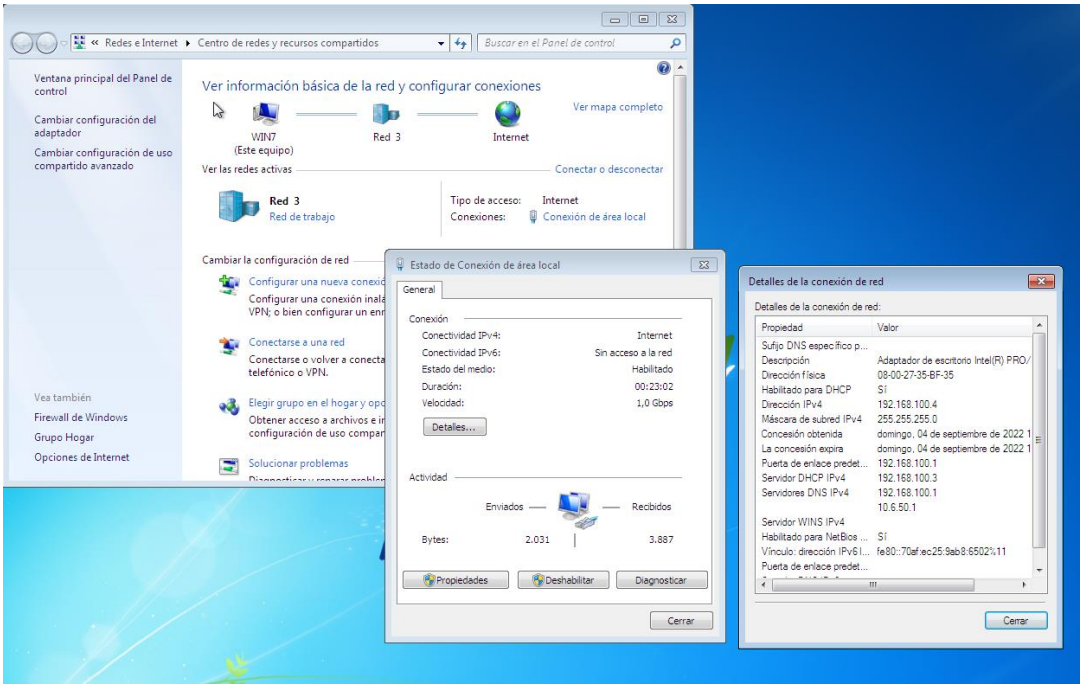
Fuente 12. Juan usama

Ilustración 13. Se asigna segmento de red



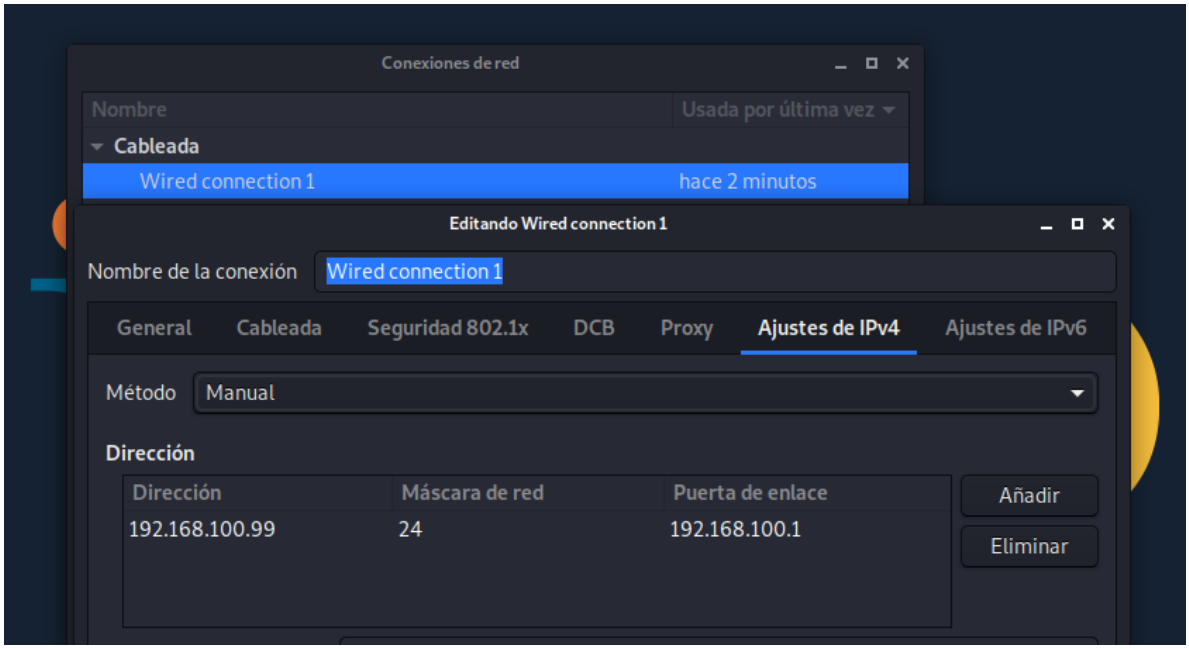
Fuente 13. Juan usama

Ilustración 14. Direcciones ip fijas



Fuente 14. Juan usama

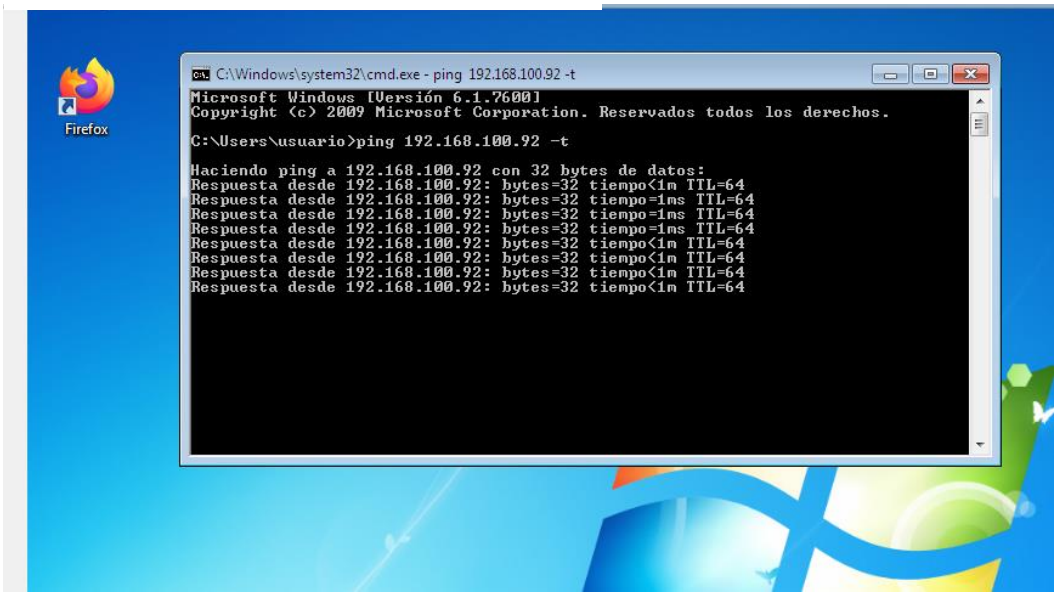
Ilustración 15. Dirección fija Kali



Fuente 15. Juan usama

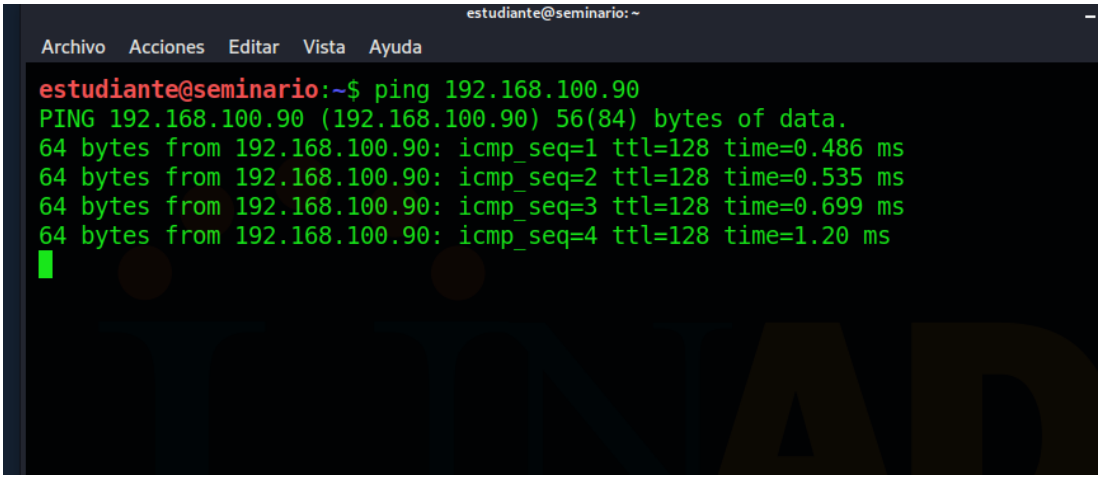
Se debieron cambiar las ip fijas y se procede a realizar el ping de comunicación.

Ilustración 16. Ping windows a kali



Fuente 16. Juan usama

Ilustración 17. Ping kali a windows



Fuente 17. Juan usama

3.2 DE MANERA INDIVIDUAL DEBERÁ LEER EL PROBLEMA QUE SE ENCUENTRA EN EL ANEXO 2 – ESCENARIO 2.

3.2.1 Evaluar si usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo. Argumentar respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

El anexo 2. Análisis legal, a simple deja dimensionar algunos procesos de irregularidad que se desarrollan al interior de la organización, el hecho de que el abogado fuera despedido por encontrar procesos ilícitos permite inferir que, aunque Hackers Secutiry sea una organización con reconocimiento mundial en procesos de asesoría en ciberseguridad, no escapa a caer en procesos de dudosa implementación o ilegalidad.

En el anexo 3. Acuerdo, se pueden encontrar algunos apartados que mencionan situaciones ilegales y no éticas que pueden comprometer la integridad del aspirante al equipo de seguridad, que sin experiencia o experticia puede caer en este tipo de situaciones problemáticas. En los respectivos anexos se destacan las siguientes situaciones:

Cláusula primera. La parte receptora **“se obliga a no divulgar la información confidencial o sobre procesos ilegales dentro de Hackers Security no podrán ser divulgados”**. En relación a la no divulgación de información confidencial que se crea, procesa y circula al interior de la organización producto del funcionamiento legal de la misma y el libre desarrollo de su actividad económica, es una normativa que comúnmente se encuentra en los procesos de incorporación a la vida laboral,

ya que al interior de las organizaciones se tratarán datos (nombre, direcciones, teléfonos, identificaciones, cuentas bancarias, entre otros) sensibles que pueden comprometer la integridad de la empresa de no ser salvaguardados y procesados para los fines netamente relacionados al objetivo comercial. Partiendo de esta premisa inicial, el objeto de la cláusula enmarca lo correspondiente a la legalidad. Sin embargo, cuando se obliga a no divulgar procesos ilegales desarrollados al interior de la empresa, el contexto cambia y la connotación de las actividades desarrolladas dan un rumbo hacia la permisividad de cometer actos ilícitos e ilegales, que no hacen parte de la labor de la empresa, por ejemplo: vender datos de los clientes a terceros. Así mismo, extralimitarse en las funciones de ciberseguridad para las cuáles fueron contratados y aprovecharse de las vulnerabilidades encontradas con fines lucrativos a espaldas de los clientes, por ejemplo: crear puertas traseras o vender fallos de seguridad encontrados a terceros.

Cláusula segunda. Entender como información confidencial **"datos secretos como datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"**. Dentro del marco de la legalidad, este tipo de interceptaciones, intrusiones o penetraciones a redes informáticas deben estar fundamentadas en órdenes jurídicas que pasaron por un proceso legal en el país donde se desarrollan. Así mismo, cumplir la normatividad para que se ordene realizar este tipo de seguimientos a usuarios u organizaciones.

Por otro lado, los accesos a los sistemas informáticos de las empresas deben estar organizados legalmente con acuerdos entre las partes, que permitan identificar el alcance, el objetivo y los resultados de las intrusiones con el fin de mejorar la seguridad informática de la empresa. Cuando estas actividades de interceptaciones y accesos abusivos no tienen un fundamento legal, inherentemente serán considerados ilegales y estarán sujetas a la aplicación de las leyes de delitos informáticos.

Cláusula tercera. Cuando se obtiene información confidencial **"independiente de su fuente o soporte"**, puede dar lugar a la situación en la que la empresa consiga obtener datos sin importar los medios utilizados porque el fin los justifica.

Cláusula cuarta. Punto cuatro. Cuando se obliga a **"no denunciar ante las autoridades actividades sospechosas"**, esta situación compromete el libre desarrollo del trabajo por parte del aspirante, ya que le coarta, prohíbe y restringe, la posibilidad de realizar alguna acción frente a este tipo de actividades ilegales. Lo somete a ser un posible cómplice de actos delictivos informáticos y compromete su estabilidad laboral. Sin embargo, se ha evidenciado que tomar una actitud contraria frente a estas situaciones no ha sido nada beneficiosa para las personas que deciden denunciar estos actos delictivos. Así fue el caso Richard Maok Riaño Botina, exfuncionario del CTI, que en agosto de 2002 pasó de ser un investigador

de bajo perfil a protagonista de un escándalo del que salió bautizado como el 'Hacker de la Fiscalía'. Este funcionario, descubrió y denunció una serie de conexiones entre paramilitares, políticos y la fiscalía. Por su denuncia, su vida se complicó y el mundo se le vino encima, ya que fue despedido de la institución, condenado por la Corte Suprema por filtrar información reservada y terminó exiliado en Canadá.

Cláusula cuarta. Punto siete. **"Responder por el mal uso que le den sus representantes a la información confidencial"**. Enunciado absolutamente comprometedor y desproporcionado, ya que no es responsabilidad de la persona asumir consecuencias derivadas del mal uso de la información que otro individuo pueda darle. Consecuentemente, el carácter de confidencialidad designa una tratamiento especial y cuidados frente a la manera de procesarla. Aunque, observando la manera de operar de la organización, no es extraño encontrar este tipo de cláusulas en las que encaminan la culpabilidad de alguna situación hacia los subalternos.

Cláusula cuarta. Punto ocho. **"Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento"**. Este enunciado incrimina directamente al empleado frente a un proceso judicial que se adelante en la empresa, ya que lo hace directamente responsable ante las autoridades y desliga la responsabilidad de la empresa de afrontar un proceso legal. Es una cláusula que tiene mucha desventaja para el empleado, no permite tener una tranquilidad emocional y laboral estable, ya que en cualquier momento puede ser incriminado en un delito informático.

Cláusula cuarta. Punto nueve. **"La parte receptora se obliga a no transmitir la información confidencial o ilegal"**. Contar con el agravante de estar cometiendo actos ilegales y adicionalmente, obligar a la persona a no transmitir información sin previa autorización de Hackers Security, es un abuso de autoridad.

Cláusula octava. Controversias. **"En caso que la información ilegal o confidencial sea encontrada en manos del receptor" este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Hackers Security"**. En esta cláusula la empresa está cargando toda responsabilidad legal y penal en el empleado. La responsabilidad debe ser mutua, asumir las investigaciones y enfrentar las sanciones económicas y judiciales a que dieran lugar en el proceso de indagación. No se puede señalar únicamente al empleado, ya que él labora bajo las indicaciones que la organización designa realizar. Sin embargo, esta empresa deja claro que realiza operaciones ilícitas y descarga dichas responsabilidades en los trabajadores. Es una empresa deshonesta.

3.2.2 En caso de ser afirmativa la respuesta y encontró algún proceso ilegal en el anexo 3 – Acuerdo. Indicar los artículos de la ley 1273 se podrían vulnerar en dicho acuerdo. En relación al anexo 3. Acuerdo y los artículos de la ley 1273 que propenden por la protección de la información y de los datos. En su capítulo 1. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, podemos encontrar que este **acuerdo**, vulnera:

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. Porque en el apartado número dos (2) de la definición de información confidencial se está manifestando que parte de la información obtenida por la empresa proviene de chuzadas, interceptaciones de información y accesos no autorizados a sistemas informáticos. Por consiguiente, se está cometiendo un delito informático.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. Porque el acuerdo manifiesta la realización ilegal de interceptación de información sin ninguna orden judicial previa que autorice la realización de dicho procedimiento. Por el contrario, el acuerdo deja al descubierto esta práctica informática ilegal.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. Porque se obliga al receptor a no denunciar ante las autoridades competentes ninguna irregularidad o actividad sospechosa frente a la intervención o apropiación de información de terceros.

3.2.3 ¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? ¿Cómo experto en ciberseguridad aplicaría a este trabajo en Hackers Security, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio? En primer lugar, revisando el anexo 3. Acuerdo, se puede evidenciar que existen apartados que son poco confiables, presentan textualmente la realización de acciones ilegales para obtener información de terceros, obligan a la parte receptora a no denunciar actos ilícitos de espionaje, exigen al estudiante responder por el mal uso que le den sus representantes a la información confidencial, asumir responsabilidades judiciales frente a procesos de allanamientos y aún más descaradamente, solicitar a la parte receptora asumir total responsabilidad frente a los perjuicios morales y económicos que puedan derivar del no cumplimiento de este acuerdo dejando el nombre de Hackers Security limpio y exonerado de cualquier responsabilidad.

En segundo lugar, no estaría interesado en aplicar para este trabajo, mucho menos para firmar un acuerdo de esta índole, así, el contrato salarial sea vitalicio por la cantidad de dinero mencionada. Considero, que cada una de las personas que inicia una carrera profesional lo hace con el firme objetivo de lograrla, conseguirla, culminarla y posteriormente, salir a un mercado laboral, poner en práctica los conocimientos adquiridos, ganar experiencia en la profesión y contribuir al mejoramiento de la calidad de vida de los seres humanos. Por

ejemplo, el admitido a una carrera de medicina, en su buen juicio no se profesionaliza para salir a asesinar pacientes en una clínica, su objetivo será propender por la vida y salud de los mismos, el ingeniero constructor, no se profesionaliza para realizar estructuras que se derrumben y comprometan la integridad de las personas, el especialista en seguridad informática, no debería acceder abusivamente a sistemas informáticos sin los consentimientos legales permitidos, por el contrario, su objetivo será implementar estrategias que salvaguarden los activos informáticos en una organización. Así mismo, cada profesional cumplirá las normativas éticas y legales que lo reglamentan. En tercer lugar, el profesional en el área de ingenierías o afines, cuenta con un organismo como el Consejo Profesional Nacional de Ingeniería, el cual, presenta un código de ética para el ejercicio de su profesión. En ese código, se establecen las conductas profesionales que los individuos deben tener consigo mismo, con su entorno y su carrera, tales como, cuidar los bienes asignados, denunciar los delitos, evitar comisiones con beneficios hacia terceros de forma ilegal, cometer actos de violencia, malos tratos, incumplir con sus obligaciones laborales, ocasionar daños intencionales que deriven en la pérdida de información y demás actitudes que puedan comprometer la integridad física, moral, social y económica de las personas. Así mismo, se pueden encontrar las prohibiciones e inhabilidades que pueden aplicarse en caso de cometer una falta ética. Pues bien, este acuerdo presentado por la empresa Hackers Security, puede derivar en consecuencias graves para un profesional, puede ocasionar una amonestación escrita, una suspensión de la matrícula profesional y una cancelación de la misma, imposibilitando ejercer de forma legal la profesión por la cual el individuo se ha esforzado durante mucho tiempo. Por consiguiente, no firmar este acuerdo sería una buena decisión, ya que para nada beneficia al profesional, no tiene criterios éticos, legales y no pretende enaltecer la profesión ejercida. En conclusión, el profesional no puede dejarse deslumbrar por un monto económico que exige realizar unas acciones que van en contra de las normativas éticas en el ejercicio de la profesión y que en cualquier momento pueden convertirse en una pesadilla. Por el contrario, el código de ética con sus responsabilidades, deberes y prohibiciones debe ser el pilar fundamental que oriente las acciones del profesional en el ámbito laboral.

3.2.4 Buscar la noticia sobre el caso “OPERACIÓN ANDROMEDA BUGGLY” en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar.

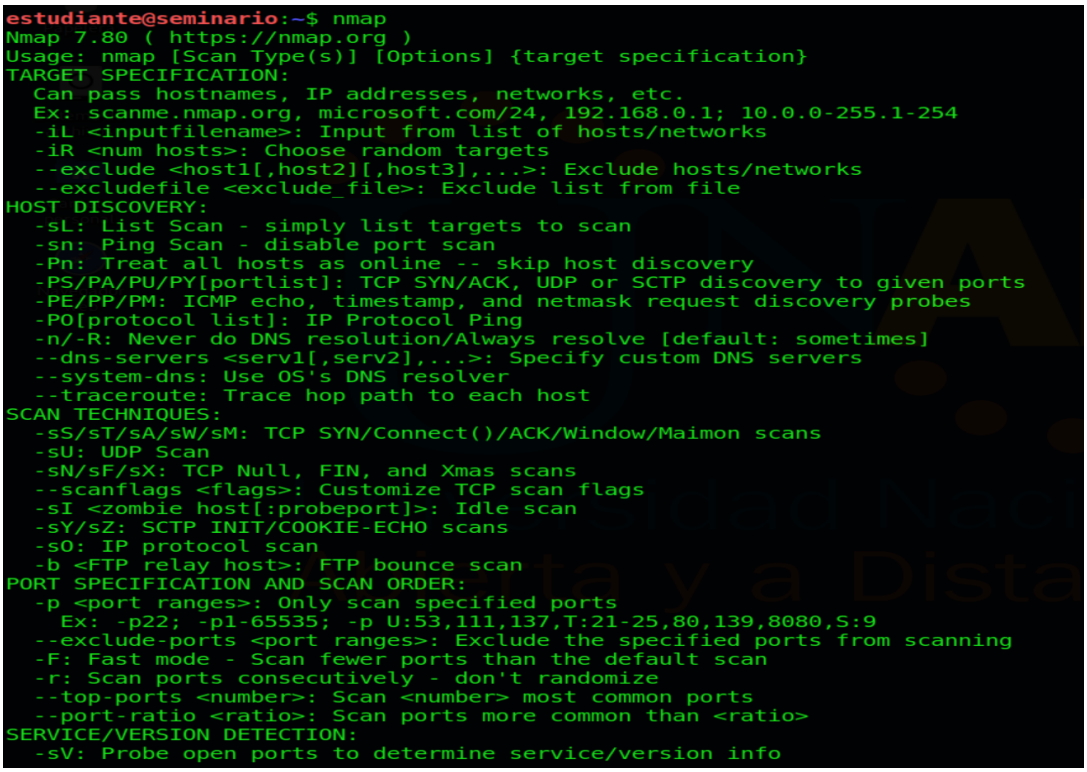
Andrés Sepúlveda, es un personaje que se vio envuelto en un escándalo informático y político del que no salió bien librado y terminó pagando algunos años de cárcel por unos delitos informáticos que le fueron imputados. Como cualquier persona con afinidad hacia la informática trabaja en ese campo promoviendo campañas publicitarias en sitios web. El problema se formó cuando estando trabajando para el candidato presidencial Iván Zuluaga en la promoción de la campaña, decidió cambiar el rumbo de su requerimiento laboral y empezó a realizar unas actividades totalmente diferentes, como interceptaciones ilegales de las conversaciones que el grupo armado de las FARC-EP desarrollaba en La Habana, Cuba. Lo anterior, a petición del candidato presidencial con el fin de acceder a la información confidencial que se pudiera almacenar en los dispositivos tecnológicos de los negociadores y aprovechar esa información para una estrategia política. Andrés Sepúlveda, estaba consciente de afrontar lo que podía pasar por las interceptaciones realizadas. Así mismo, frecuentaba una locación en la ciudad de Bogotá que tenía la fachada de restaurante pero que en realidad era una central de inteligencia ilegal conocida como ANDROMEDA desde la cual se realizaban seguimientos, interceptaciones y persecuciones ilícitas a ciudadanos. Esta situación, permitía a Andrés, intercambiar beneficios e información confidencial para el beneficio de la campaña política. En este punto, ocurre una situación bastante compleja en la que se infiltra la campaña Iván Zuluaga y se orquesta un montaje para inculpar a Andrés Sepúlveda de adelantar tareas de espionaje ilegales con las fuerzas militares Colombianas para la campaña del candidato presidencial y es allí donde su vida toma un rumbo diferente y se complica. En relación a esta situación, podría mencionarse que Andrés es una persona talentosa en el campo informático, cuenta con habilidades, técnicas y la pericia necesaria para destacar en alguno de los equipos red & blue team. Sin embargo, su actitud, fue lo que cambió el rumbo de su futuro, paso de ser un reconocido personaje en la redes sociales por realizar legalmente su trabajo a un ciberdelincuente que probablemente por ofrecimientos económicos traicionó sus ideales de trabajo ético y se cambió al lado de las interceptaciones ilegales, chuzadas, irrupción de sistemas informáticos, comercialización ilícita de datos confidenciales y demás acciones que van en contra del código de ética del profesional en ingeniería. Las consecuencias de estos actos derivaron en una condena carcelaria, en una celda donde todo el tiempo llevaba un chaleco antibalas y tenía un catador de alimentos porque vivía con la zozobra de que lo pudieran envenenar. En conclusión, el profesional debe procurar tener comportamientos éticos y legales en el cumplimento de sus labores diarias, no debe dejarse influenciar por beneficios económicos, reconocimientos superficiales o promesas que compliquen su buena actitud, no vale la pena incurrir en situaciones que atenten contra el código de ética, porque al final pueden terminar perjudicando la vida del profesional.

3.3 DEMOSTRAR VULNERABILIDADES EN UN SISTEMA INFORMÁTICO

3.3.1 Describir de forma específica las herramientas de software utilizadas en el desarrollo del Anexo 4. Escenario 3.

• **NMAP: "**Es una herramienta utilizada para realizar escaneos sobre de la red, permitiendo identificar puertos abiertos, servicios configurados, versión de sistema operativo"[9]. Al ejecutar el comando NMAP identificamos los tipos y opciones de comandos que se pueden ejecutar. Así mismo, se utiliza para realizar un sondeo en la red de los equipos de cómputo.

Ilustración 18. Entorno NMAP



Fuente 18. Juan usama

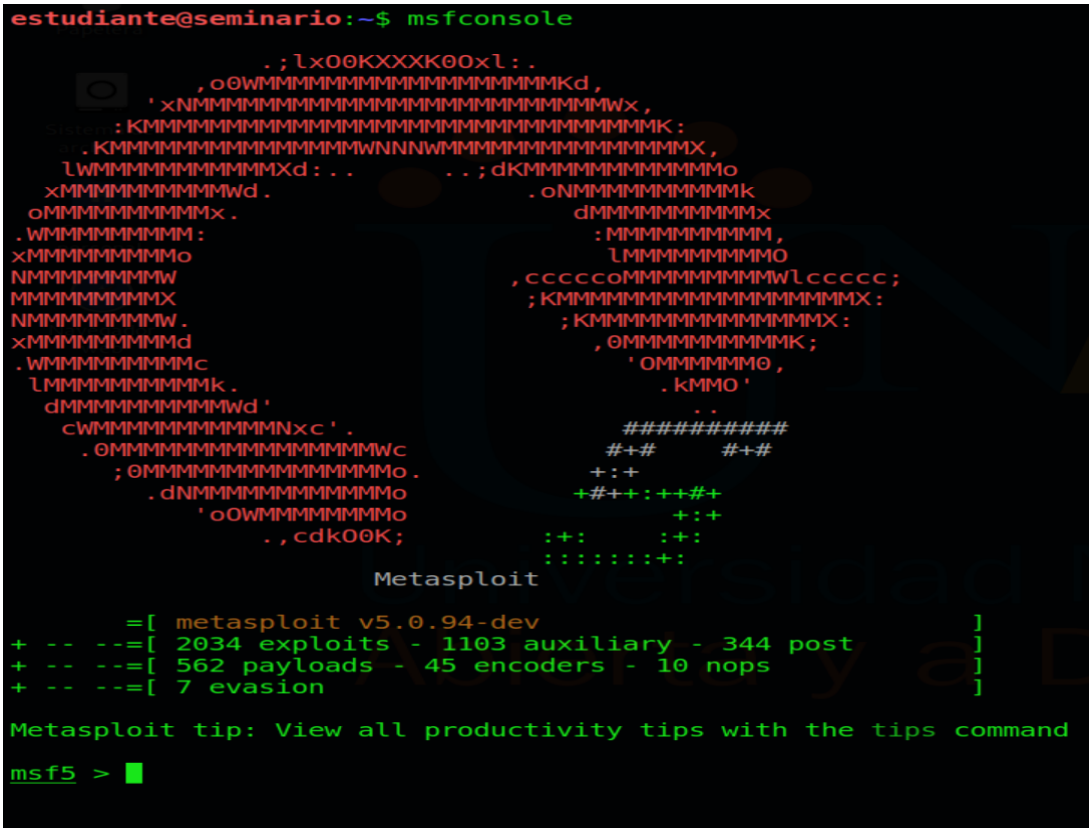
[9] LYON GORDON. Nmap: Discover your network. [Sitio web]. Estados Unidos. [Consulta: 29 de septiembre de 2022]. Disponible en: https://nmap.org/

Ilustración 19. Identificación IP

Fuente 19. Juan usama

• **METASPLOIT:** Es una herramienta para probar las vulnerabilidades de los sistemas informáticos. Se utiliza también para ingresar a sistemas remotos y realizar auditorías informáticas.

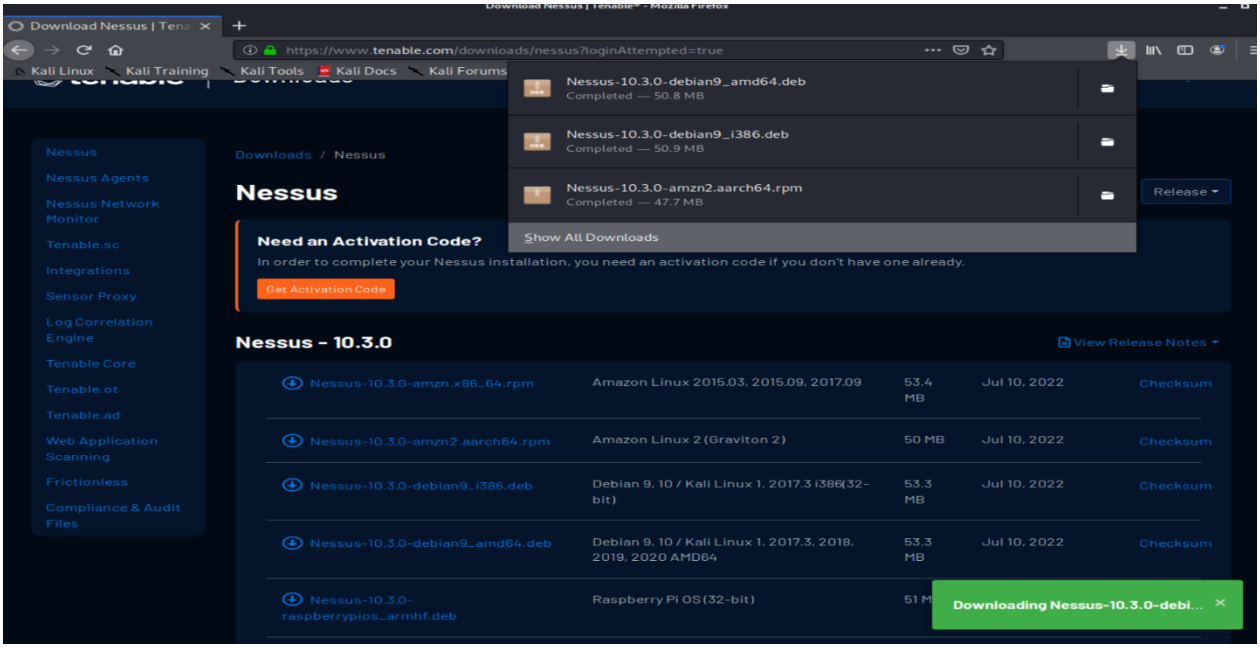
Ilustración 20. Metasploit



Fuente 20. Juan usama

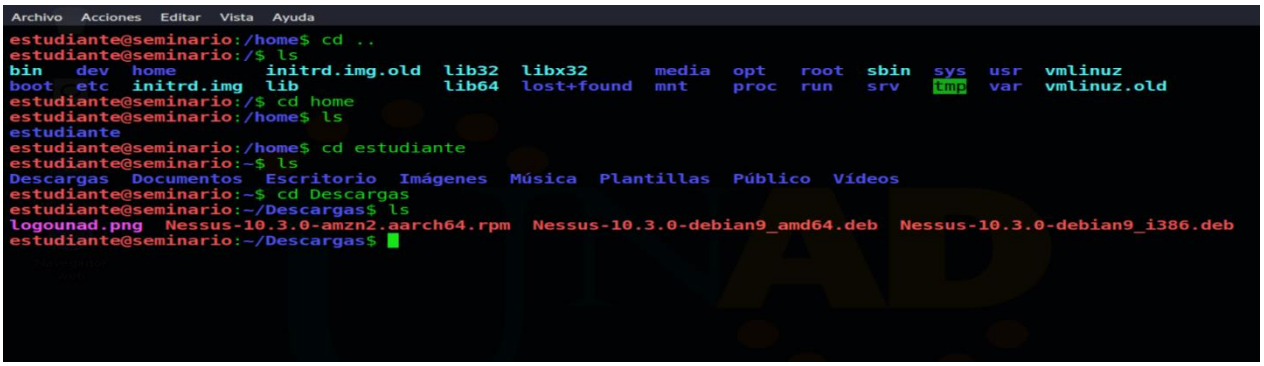
- **NESSUS:** Se utiliza esta herramienta en procesos de escaneo, búsqueda de alguna vulnerabilidad en la red y sus posibles soluciones. Así mismo, permite proporcionar resultados mediante un informe final done se clasifica cada uno de los análisis

Ilustración 21. Descarga Nessus



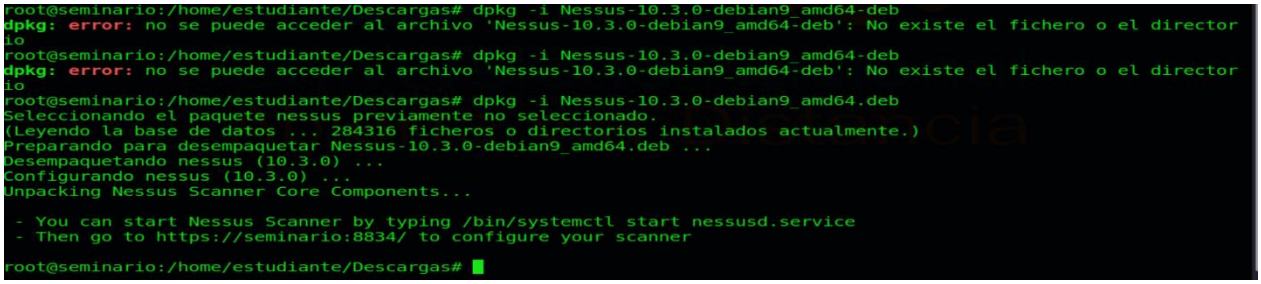
Fuente 21. Juan usama

Ilustración 22. Instalación Nessus



Fuente 22. Juan usama

Ilustración 23. Instalación finalizada



Fuente 23. Juan usama

3.3.2 Fase recolección de información. Una vez se ha instalado las diferentes herramientas, se procede a realizar la explotación de las diferentes vulnerabilidades en las máquinas virtuales.

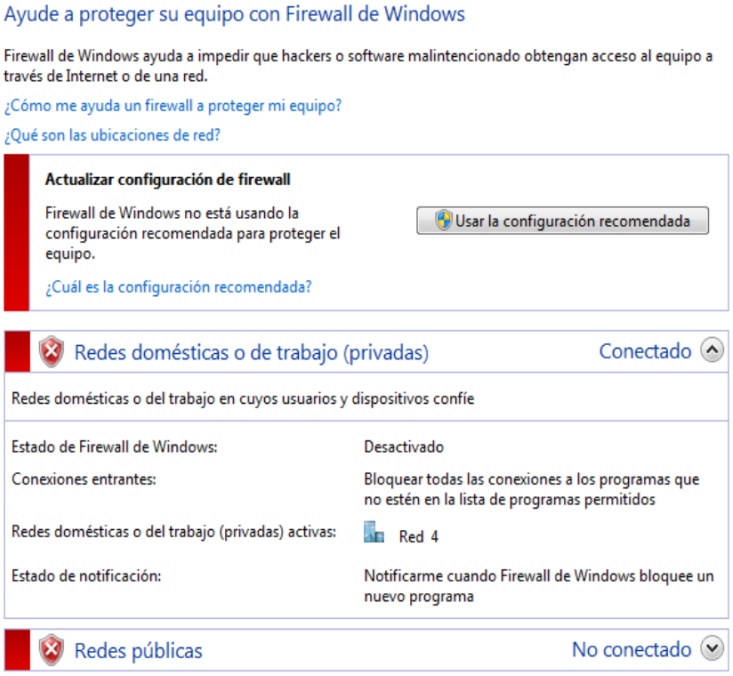
Desde kali Linux se escanean las vulnerabilidades a través de nmap, nessus y metasploit.

En las máquinas virtuales se procede a desactivar el firewall-.

Ilustración 24. Desactivar firewall

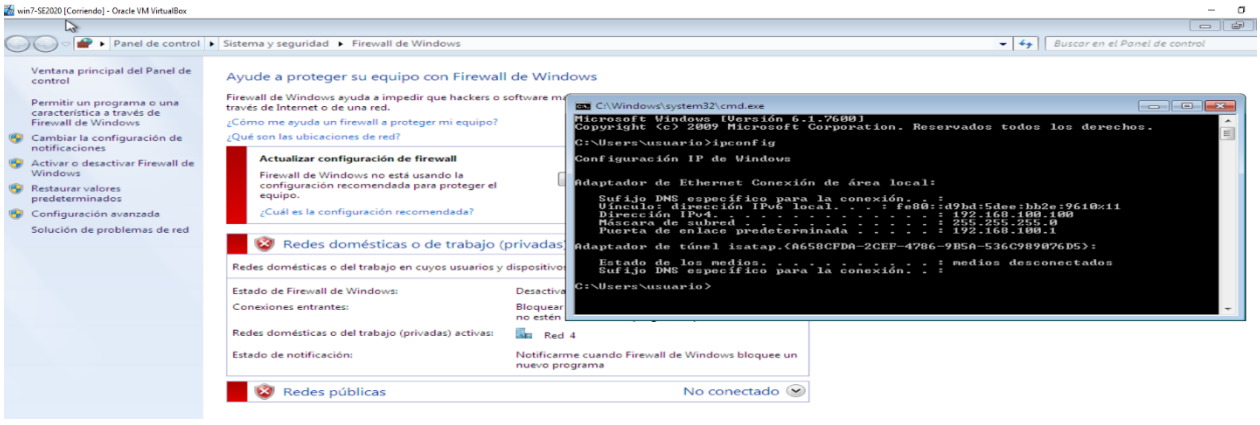
Fuente 24. Juan usama

Ilustración 25. Firewall desactivado



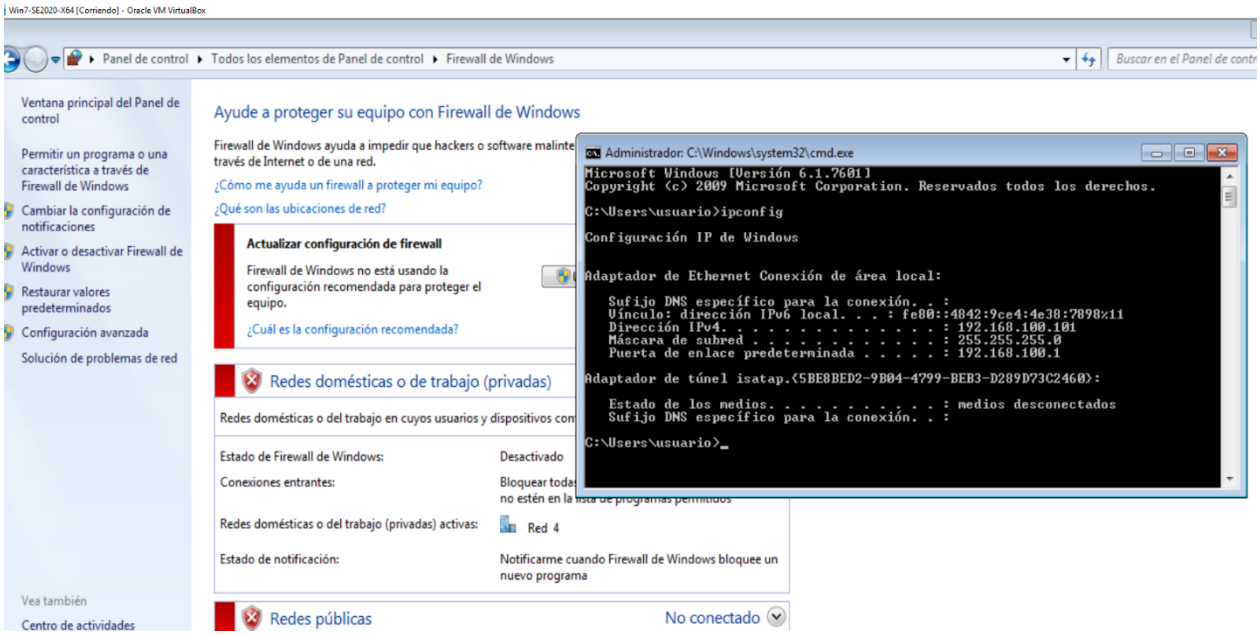
Fuente 25. Juan usama

Ilustración 26. Windows 7 x86



Fuente 26. Juan usama

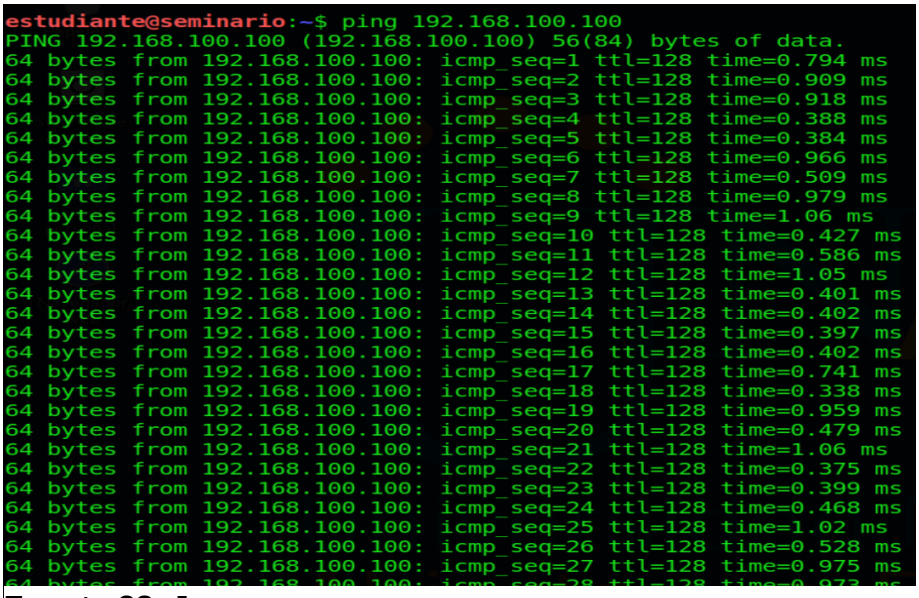
Ilustración 27. Windows 7 x64



Fuente 27. Juan usama

Se procede con la identificación de enrutamiento y verificación de que existe comunicación entre las máquinas virtuales.

Ilustración 28. Comunicación máquina virtual



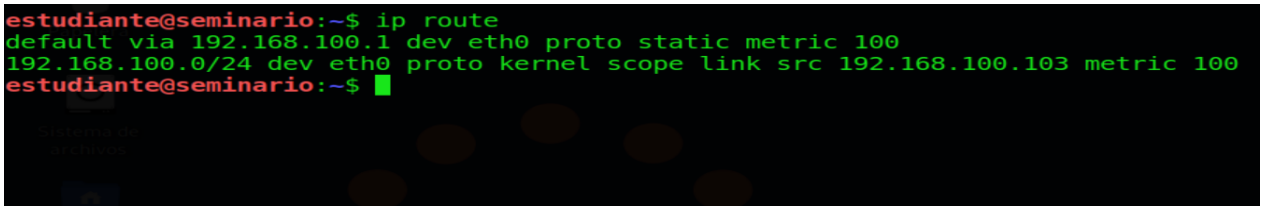
Fuente 28. Juan usama

Ilustración 29. Comunicación máquina virtual

Fuente 29. Juan usama

Procedemos a identificar el enrutamiento.

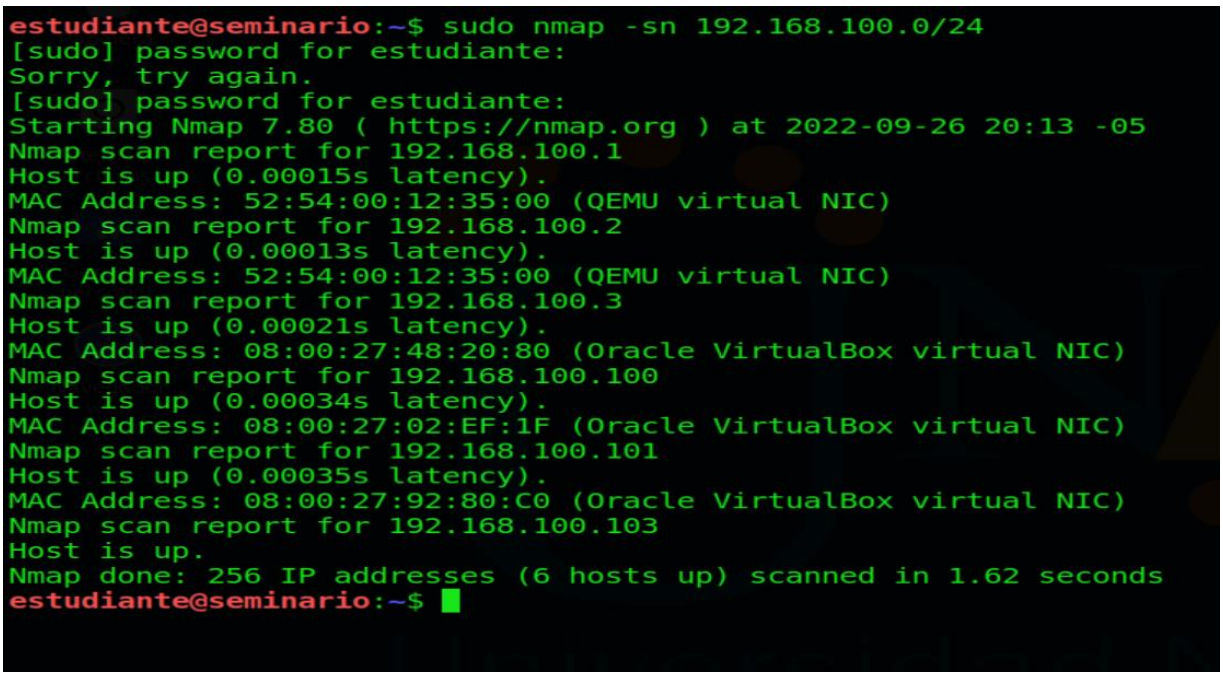
Ilustración 30. Enrutamiento



Fuente 30. Juan usama

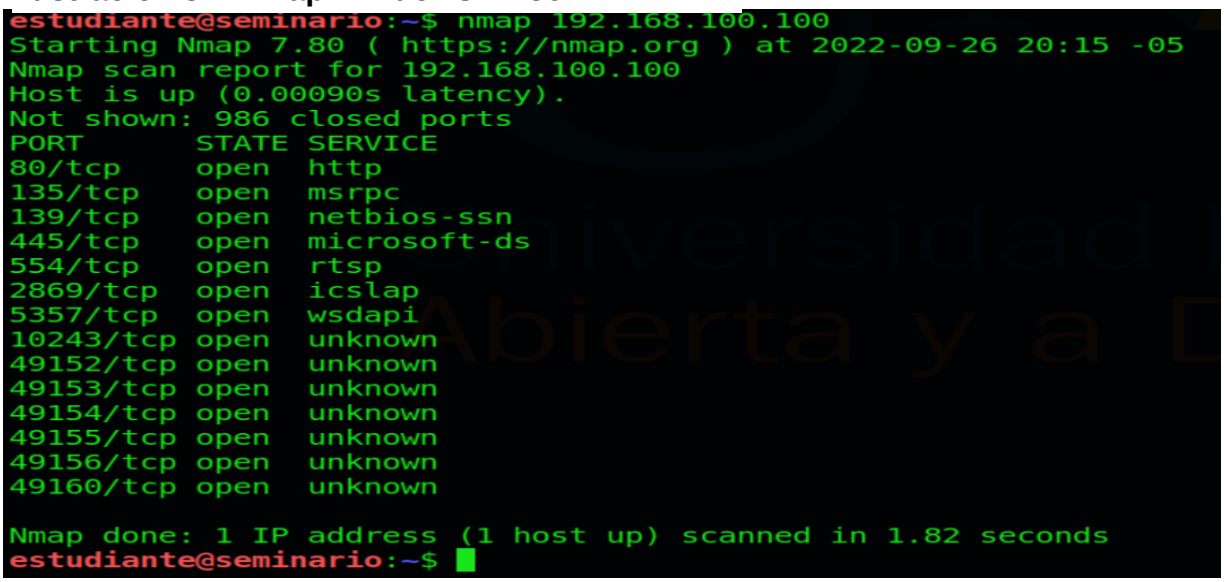
Se identifican los dispositivos conectados a la red.

Ilustración 31. Dispositivos en red



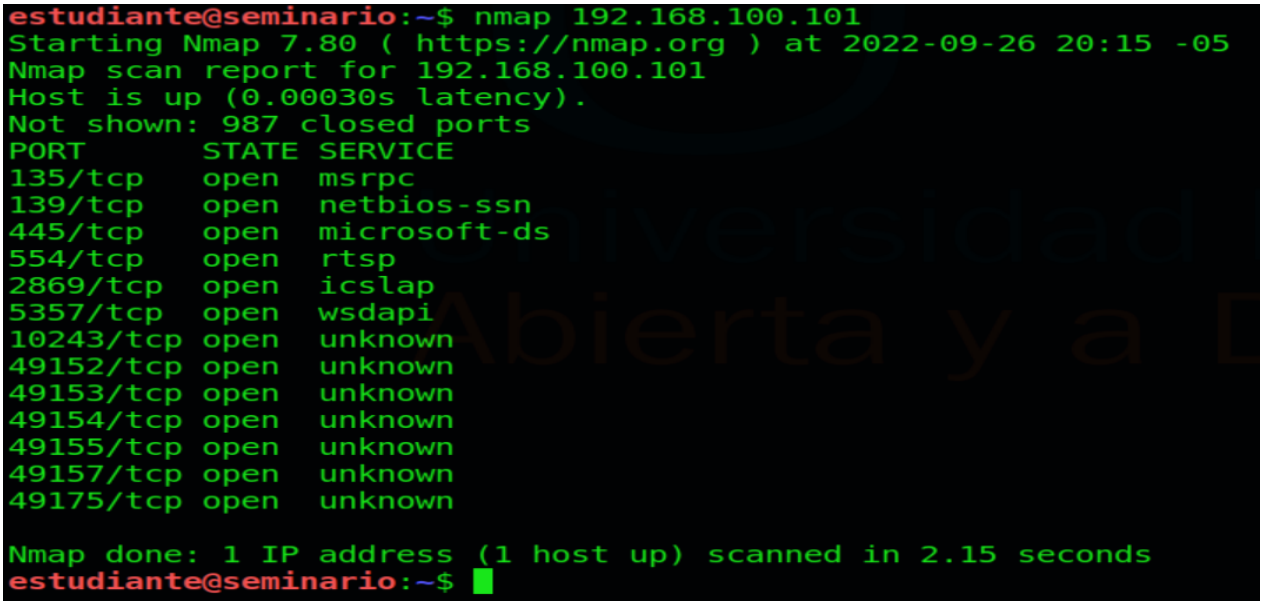
Fuente 31. Juan usama

Ilustración 32. Nmap Windows 7 x86



Fuente 32. Juan usama

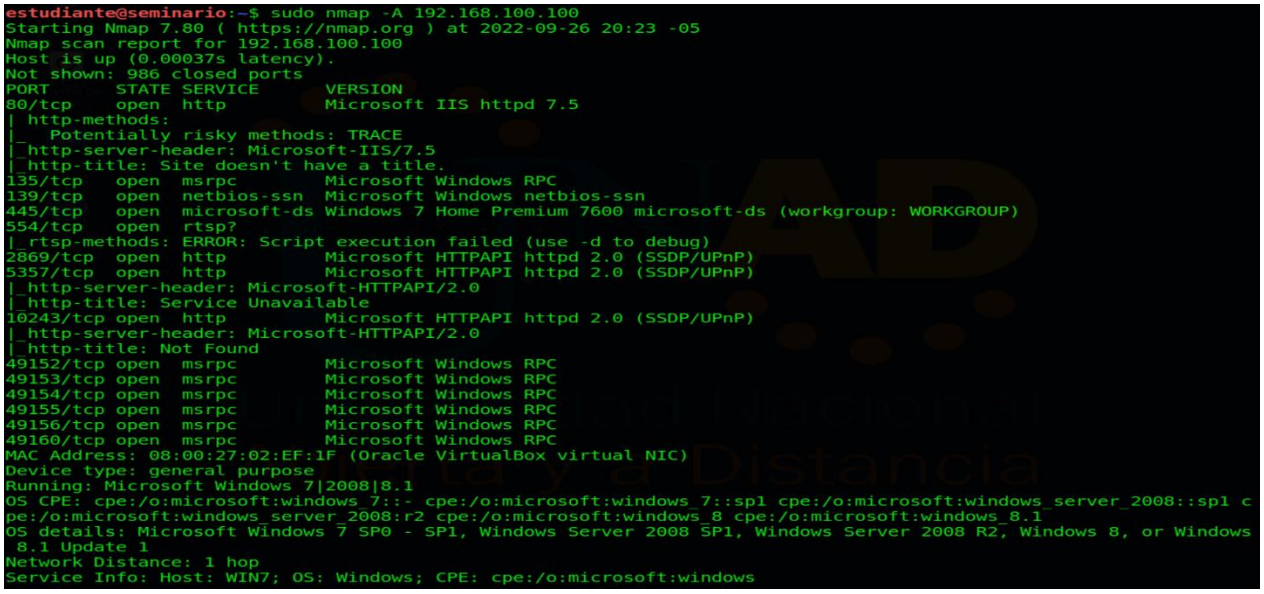
Ilustración 33. Nmap Windows



Fuente 33. Juan usama

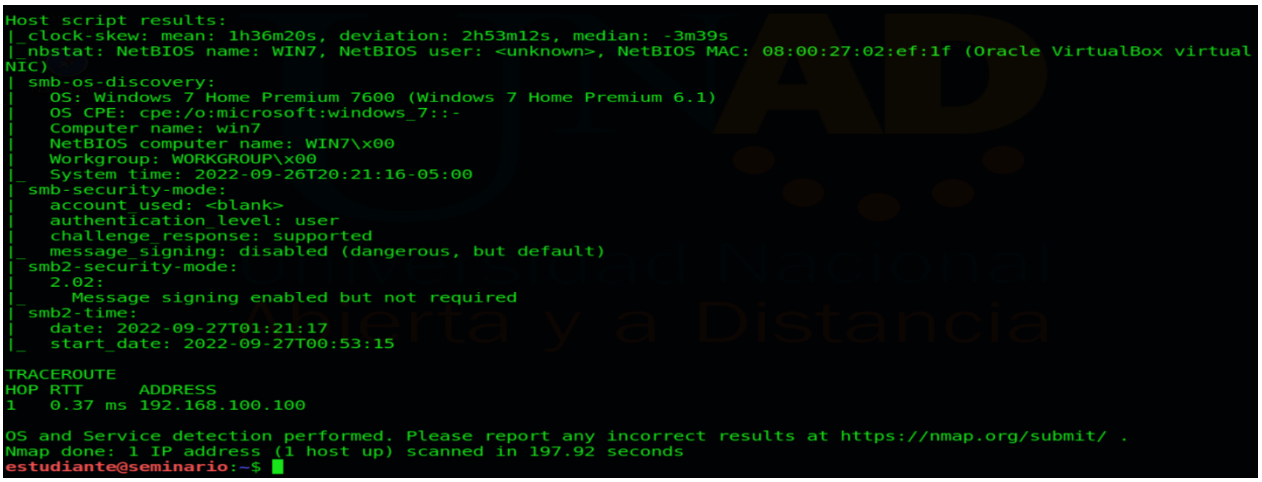
Se puede evidenciar la identificación de puerto en Win7 x86

Ilustración 34. Puertos Win7 x86



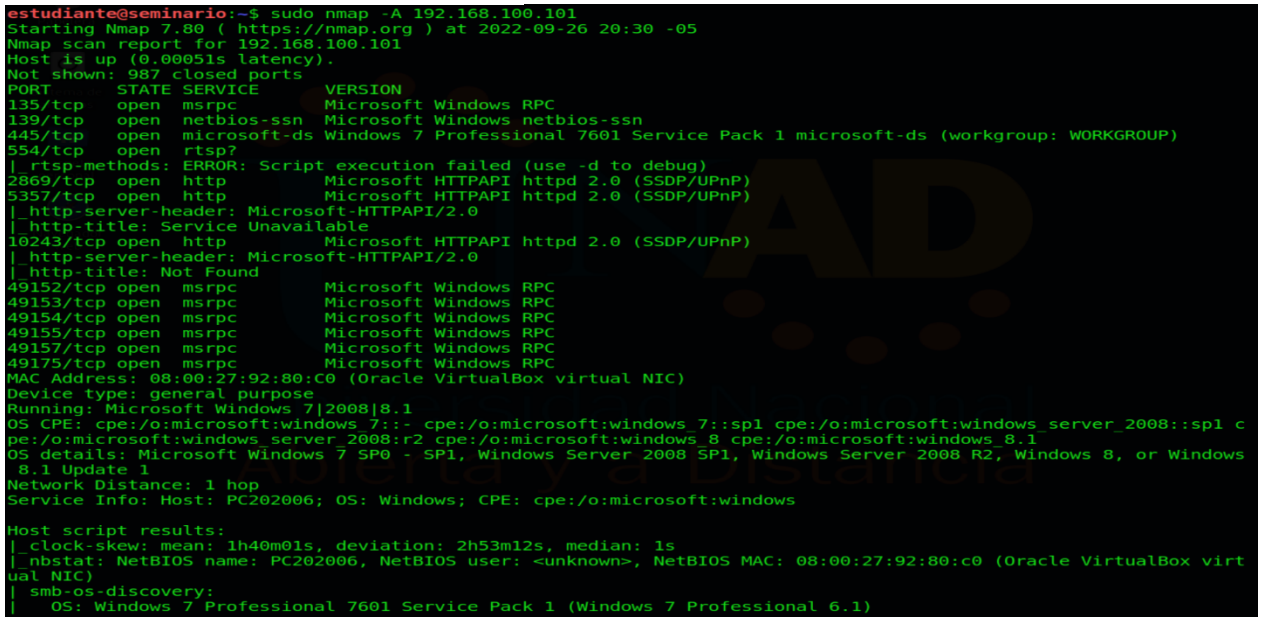
Fuente 34. Juan usama

Ilustración 35. Complemento puertos Win7 x86



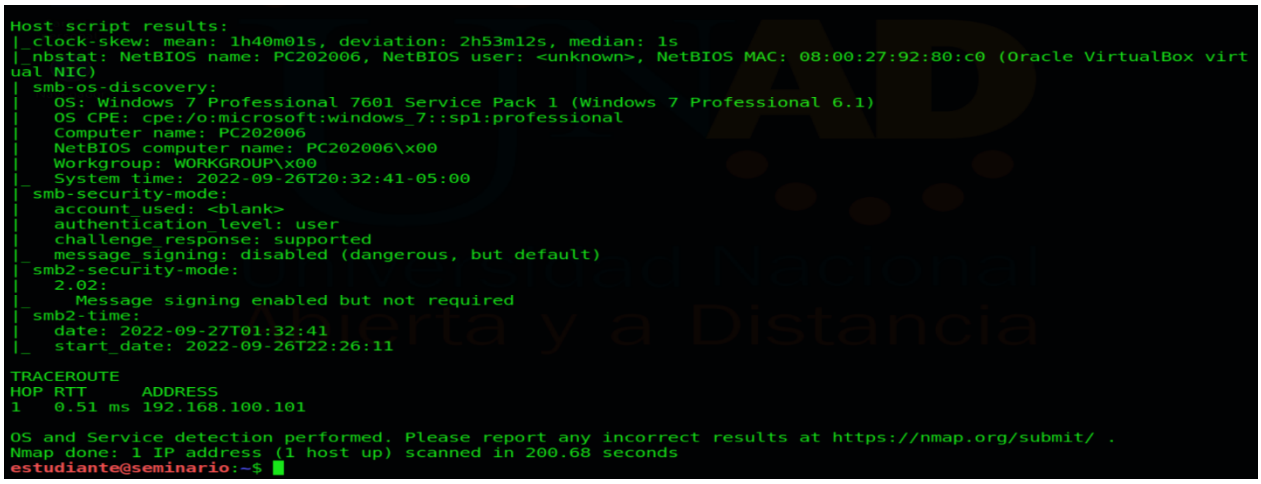
Fuente 35. Juan usama

Ilustración 36. Puertos Win7 x64



Fuente 36. Juan usama

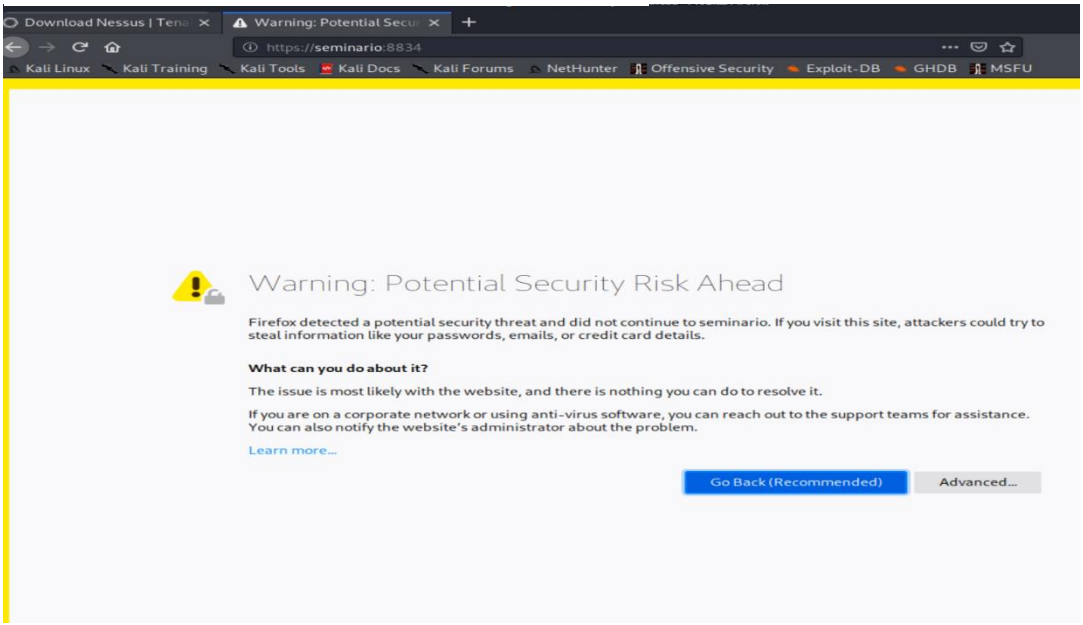
Ilustración 37. Complemento puertos Win7 x64



Fuente 37. Juan usama

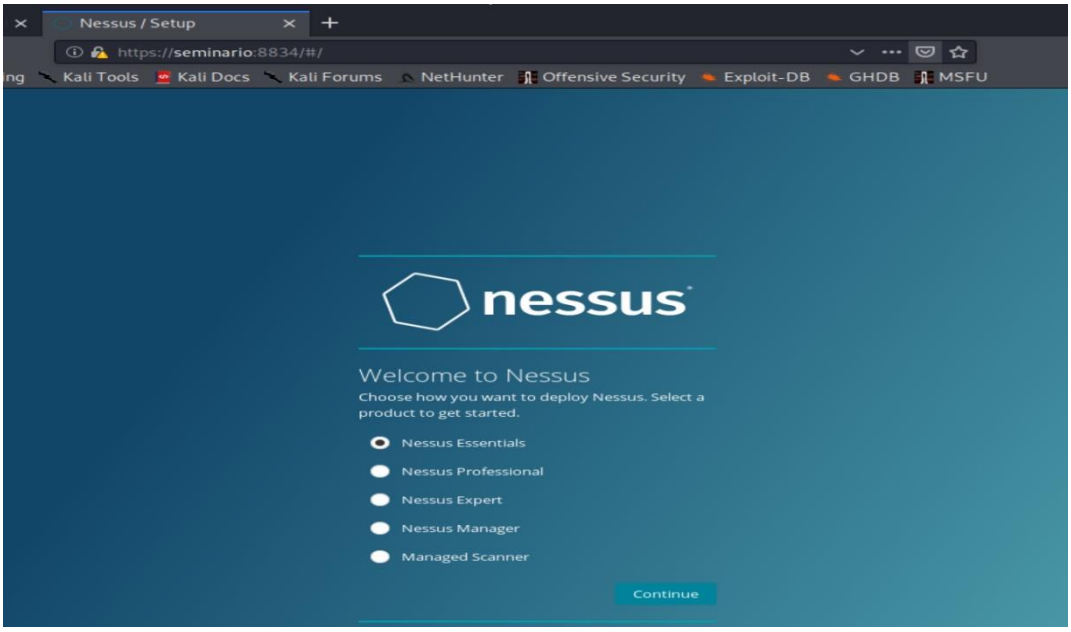
3.3.3 Fase de análisis de vulnerabilidades. En este punto se valoran las estrategias de análisis de vulnerabilidades. Las herramientas a implementar para este proceso fueron Nessus – Nmap.

Ilustración 38. Inicio Nessus



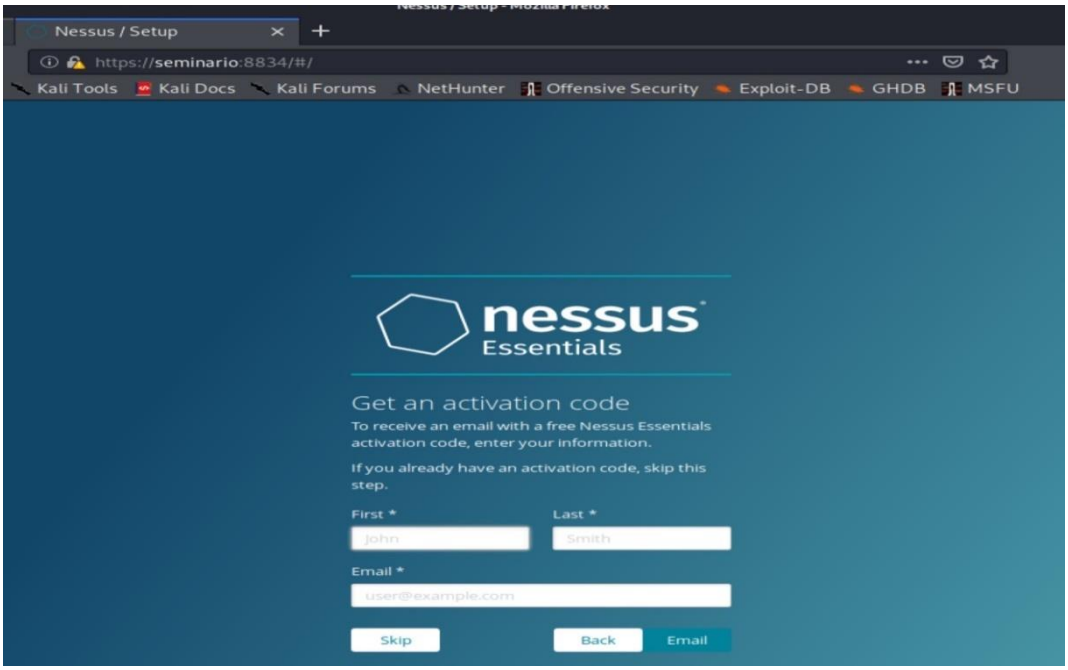
Fuente 38. Juan usama

Ilustración 39. Configuración Nessus



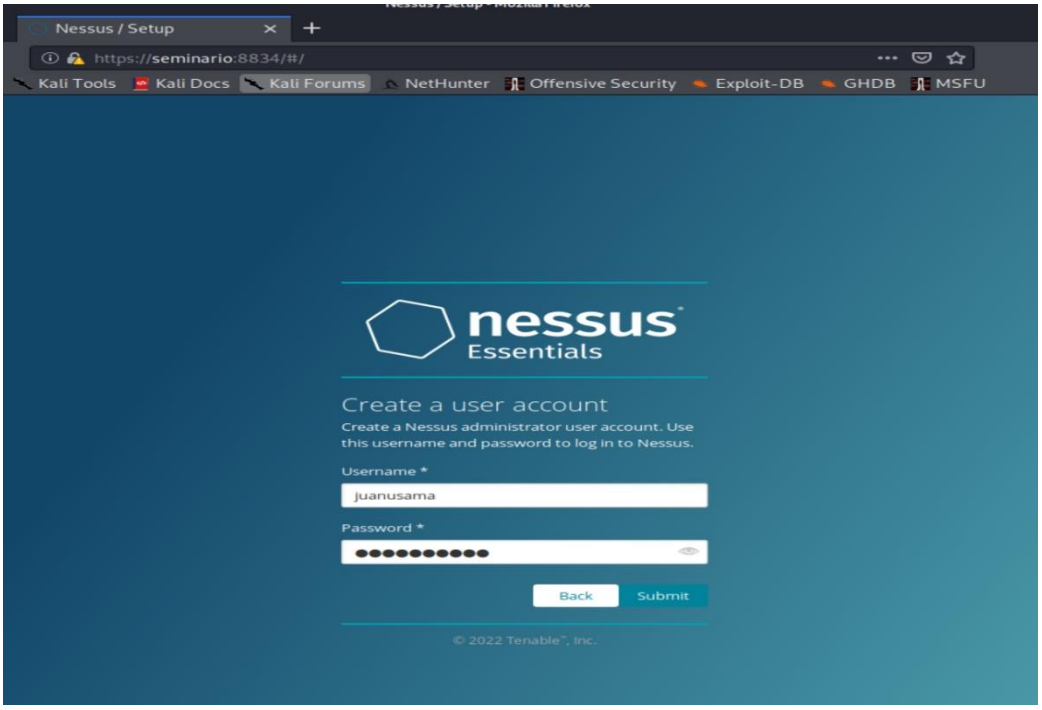
Fuente 39. Juan usama

Ilustración 40. Activación Nessus



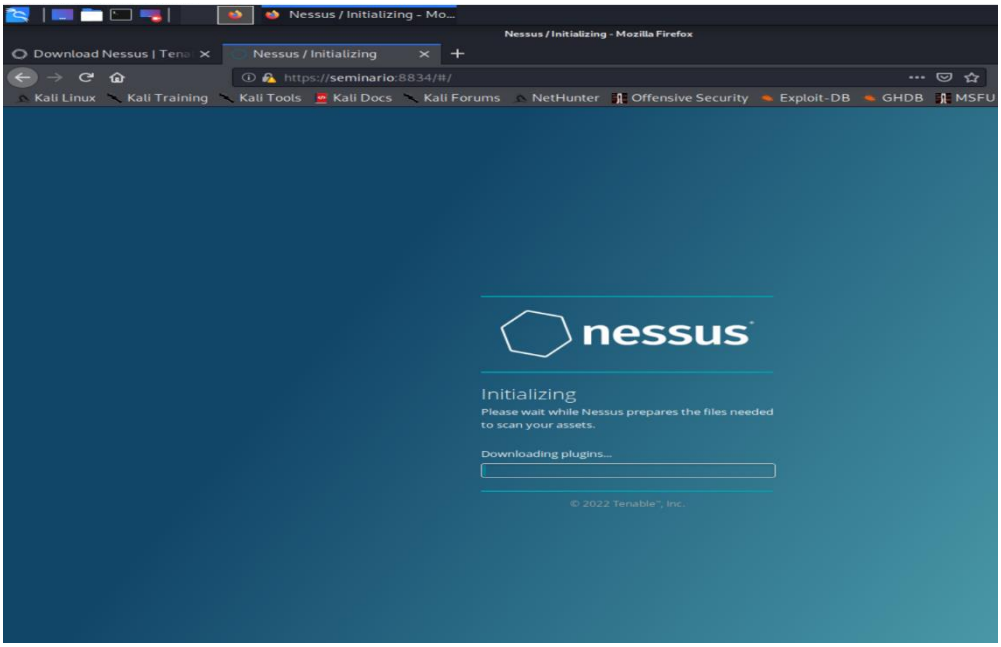
Fuente 40. Juan usama

Ilustración 41. Asignación usuario



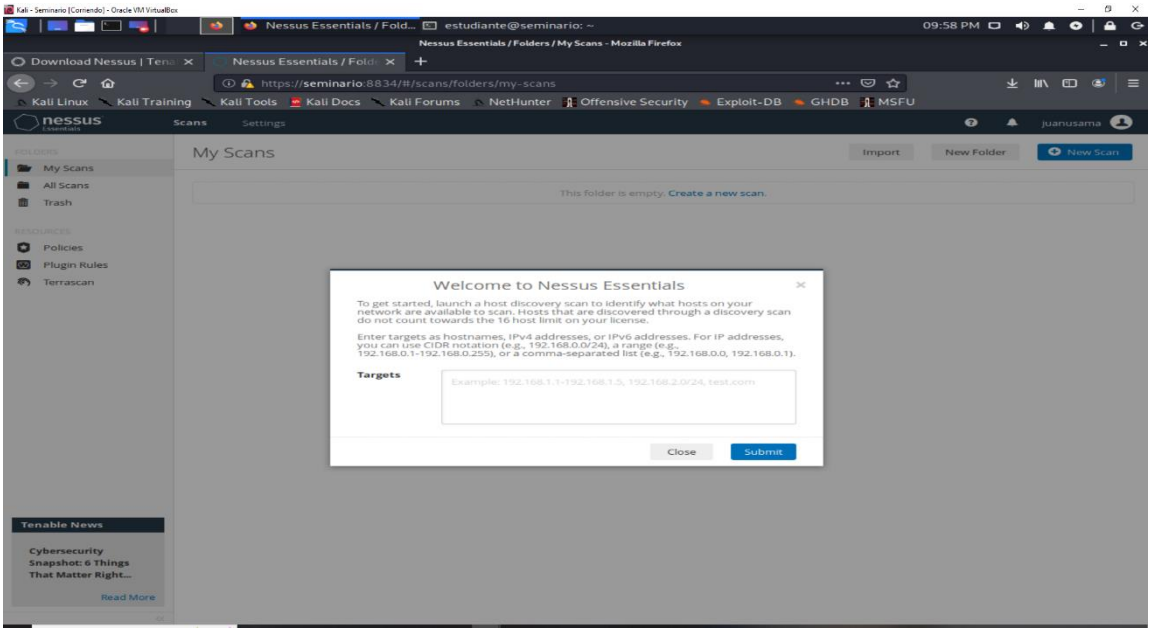
Fuente 41. Juan usama

Ilustración 42. Descarga plugins



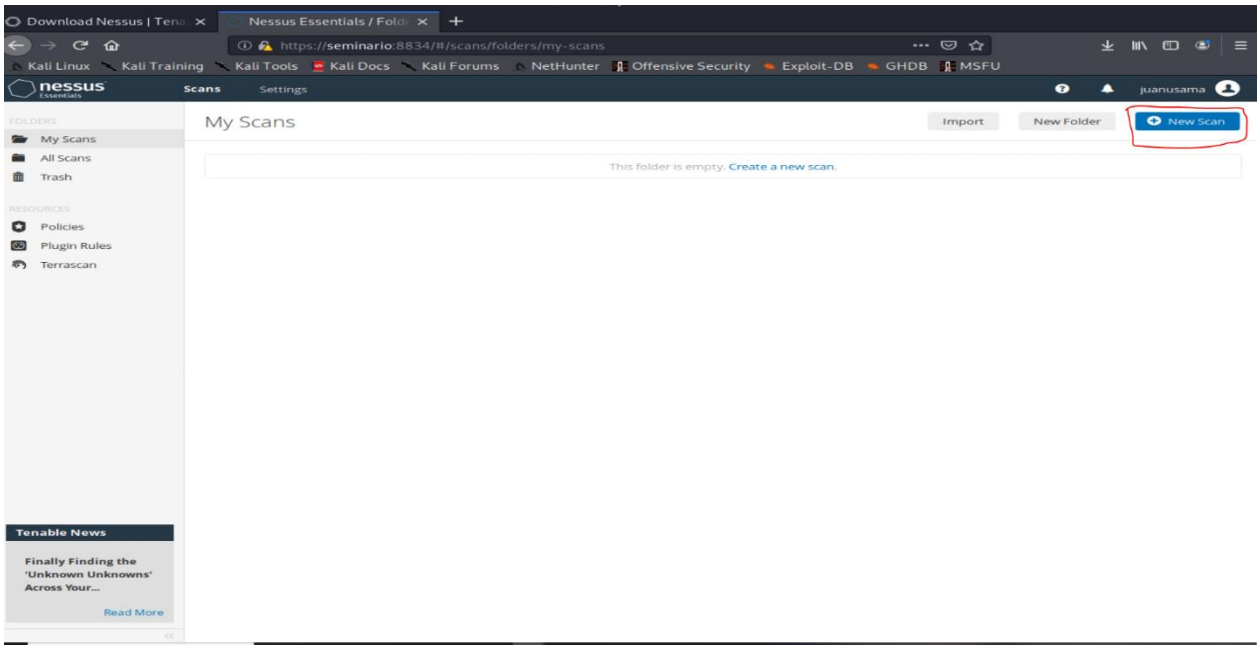
Fuente 42. Juan usama

Ilustración 43. Interfaz Nessus



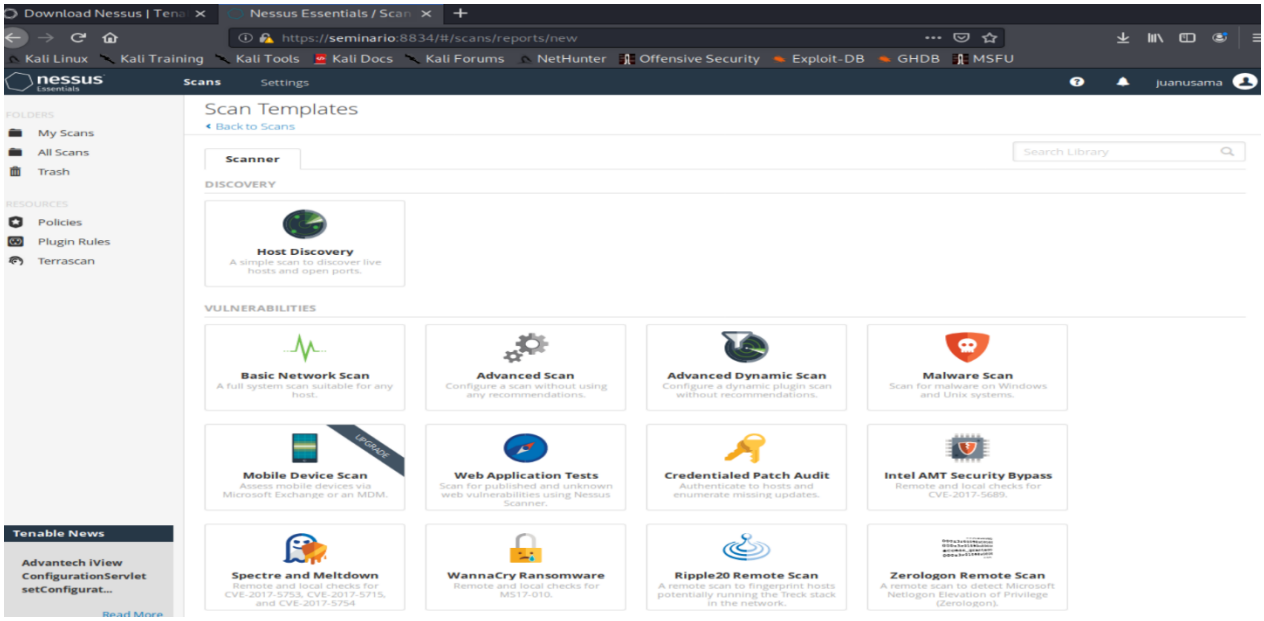
Fuente 43. Juan usama

Ilustración 44. Nuevo escaneo



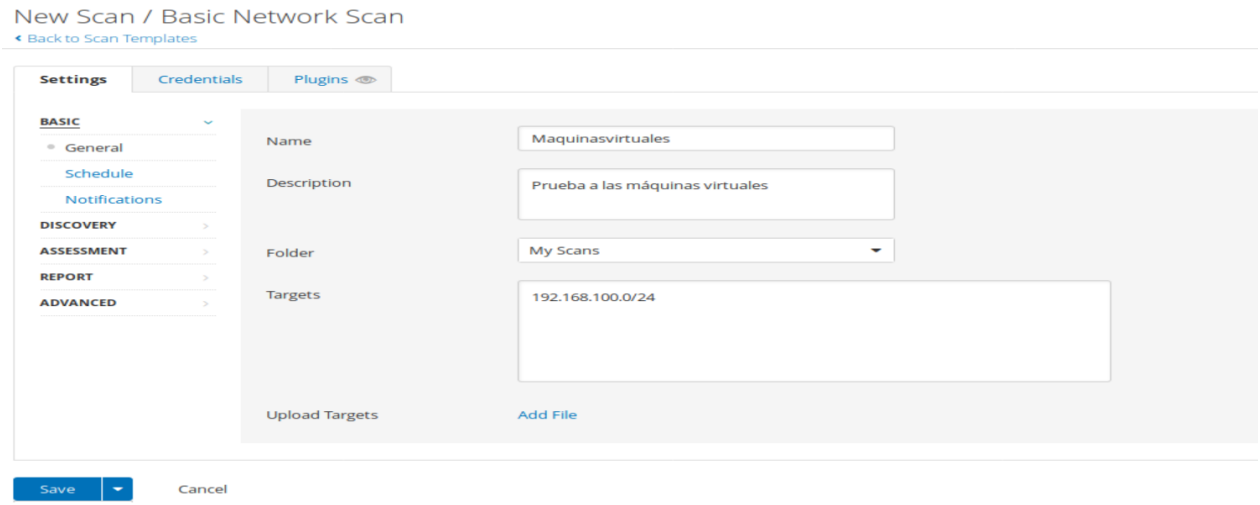
Fuente 44. Juan usama

Ilustración 45. Interfaz escaneo



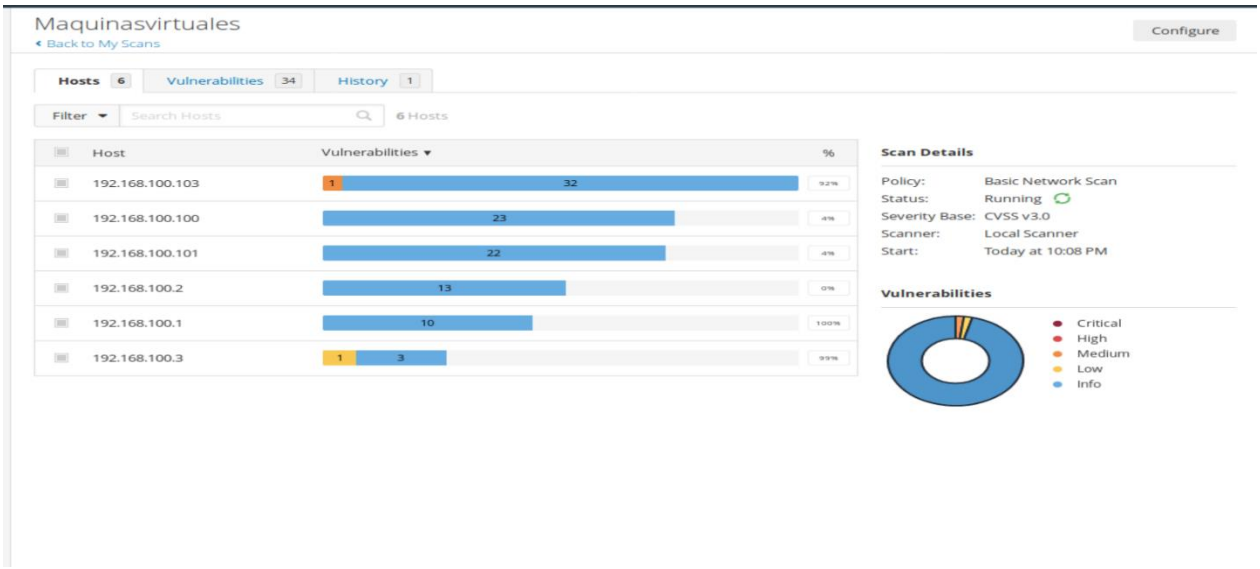
Fuente 45. Juan usama

Ilustración 46. Programación escaneo



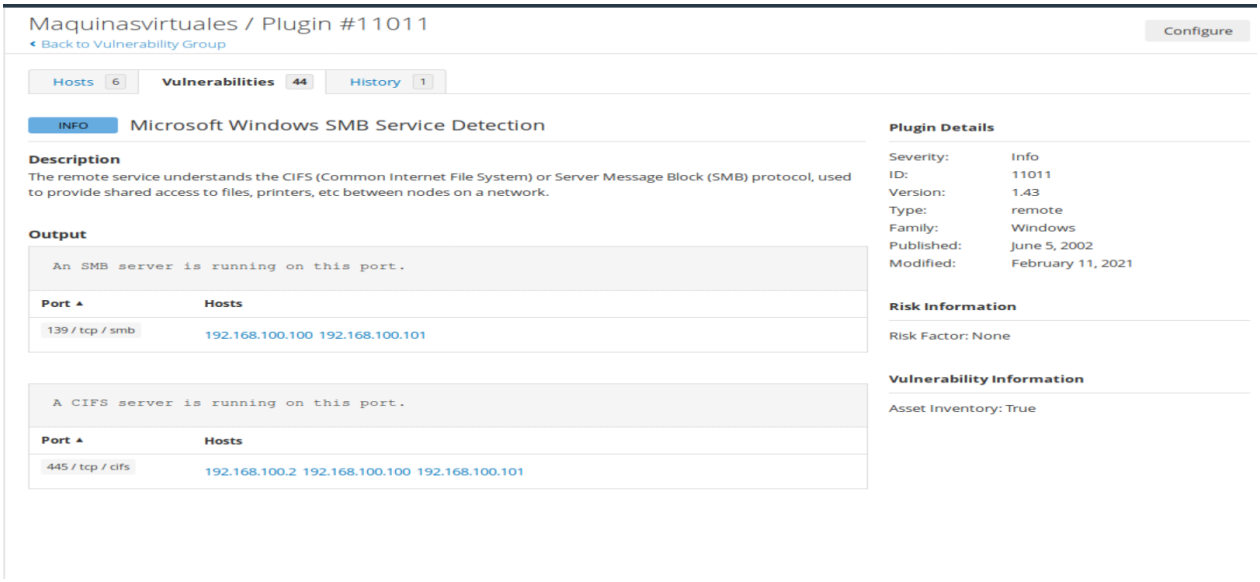
Fuente 46. Juan usama

Ilustración 47. Informe escaneo



Fuente 47. Juan usama

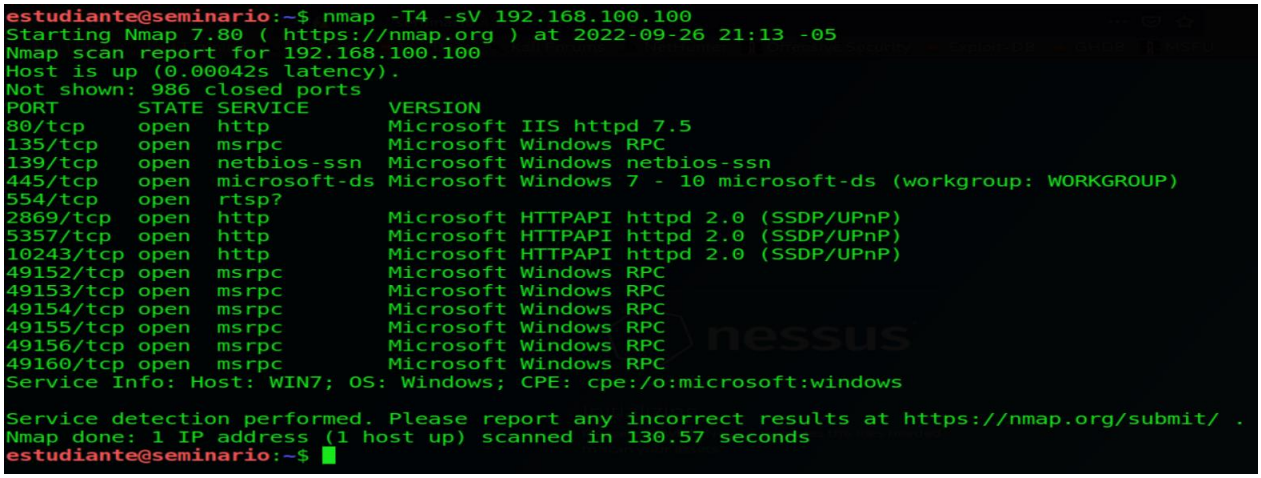
Ilustración 48. Revisión vulnerabilidad



Fuente 48. Juan usama

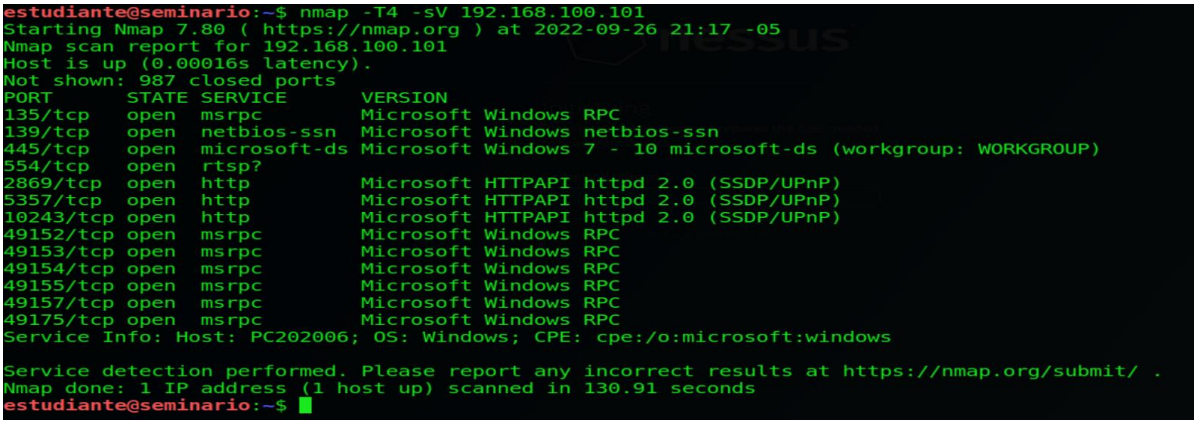
Verificamos puertos y servicios en las máquinas virtuales Windows 7

Ilustración 49. Puertos verificados



Fuente 49. Juan usama

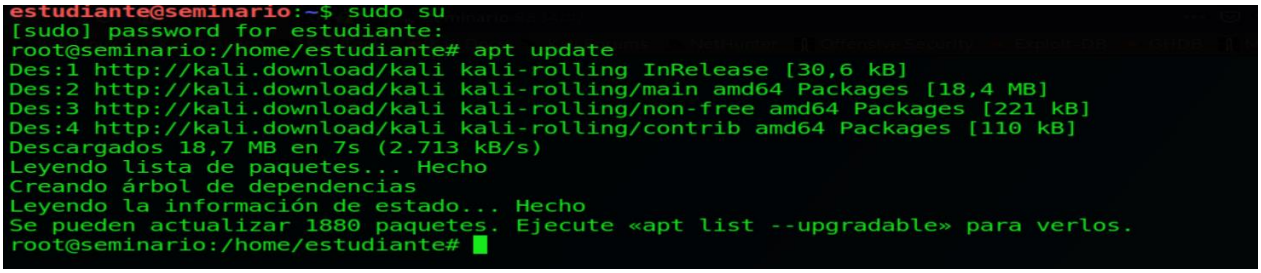
Ilustración 50. Puertos revisados



Fuente 50. Juan usama

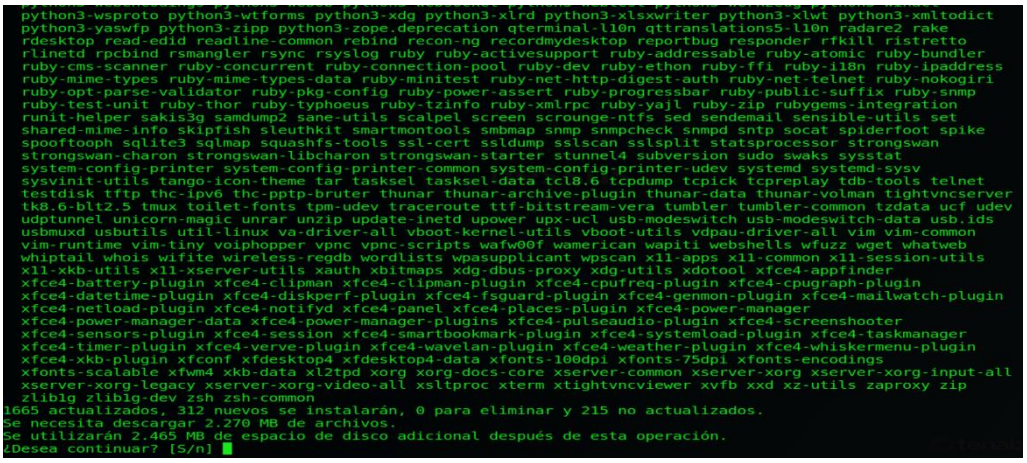
Actualizamos el entorno en kali linux

Ilustración 51. Actualización



Fuente 51. Juan usama

Ilustración 52. Proceso actualización

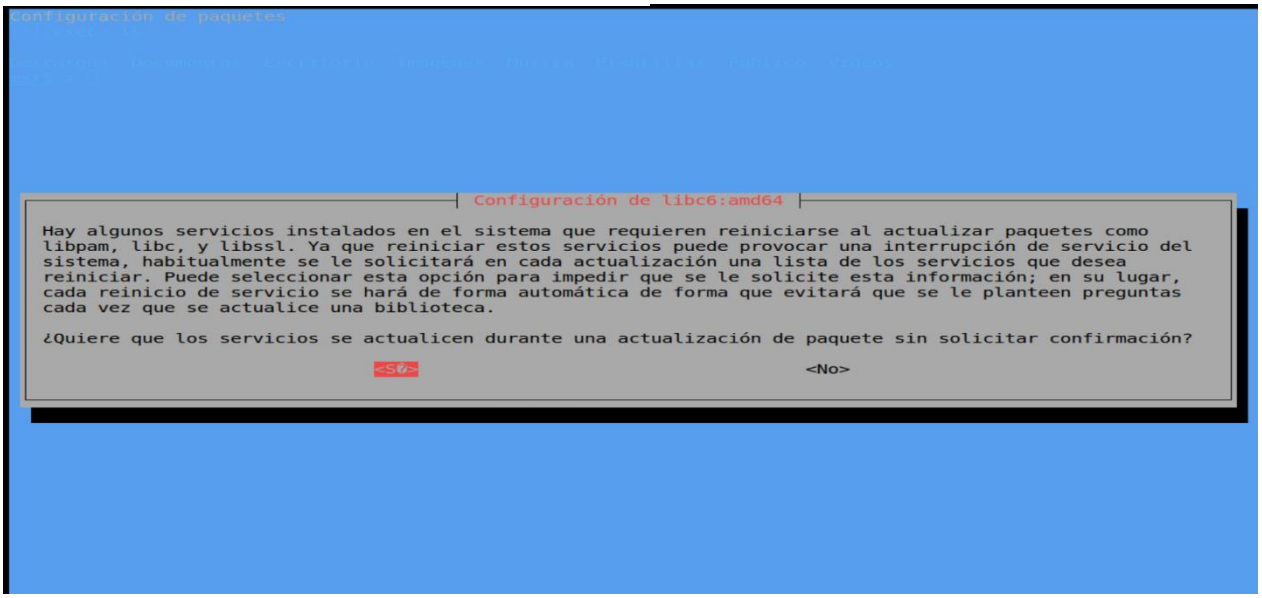


Fuente 52. Juan usama

Ilustración 53. Actualización finalizada

Fuente 53. Juan usama

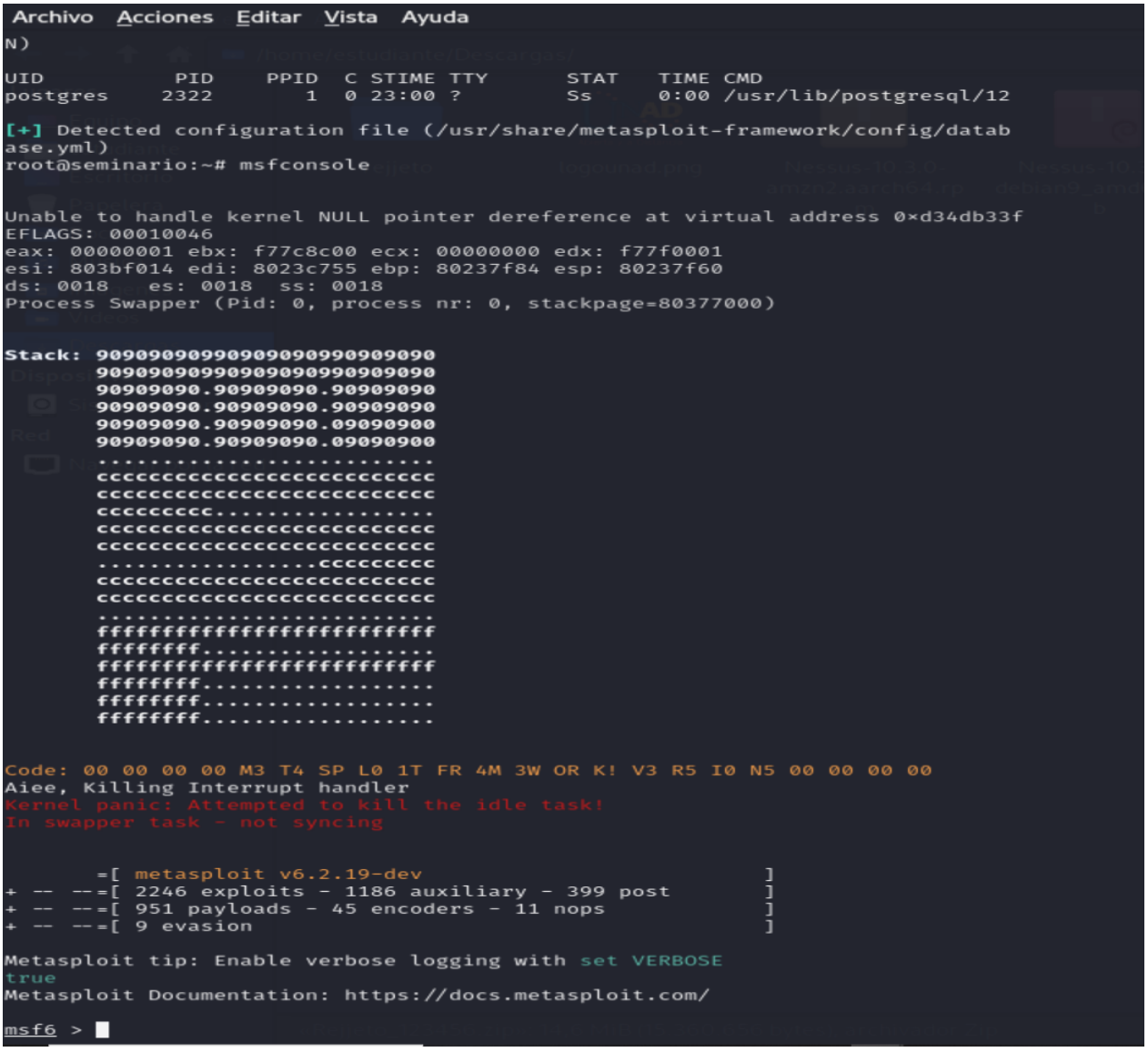
Ilustración 54. Reinicio del sistema



Fuente 54. Juan usama

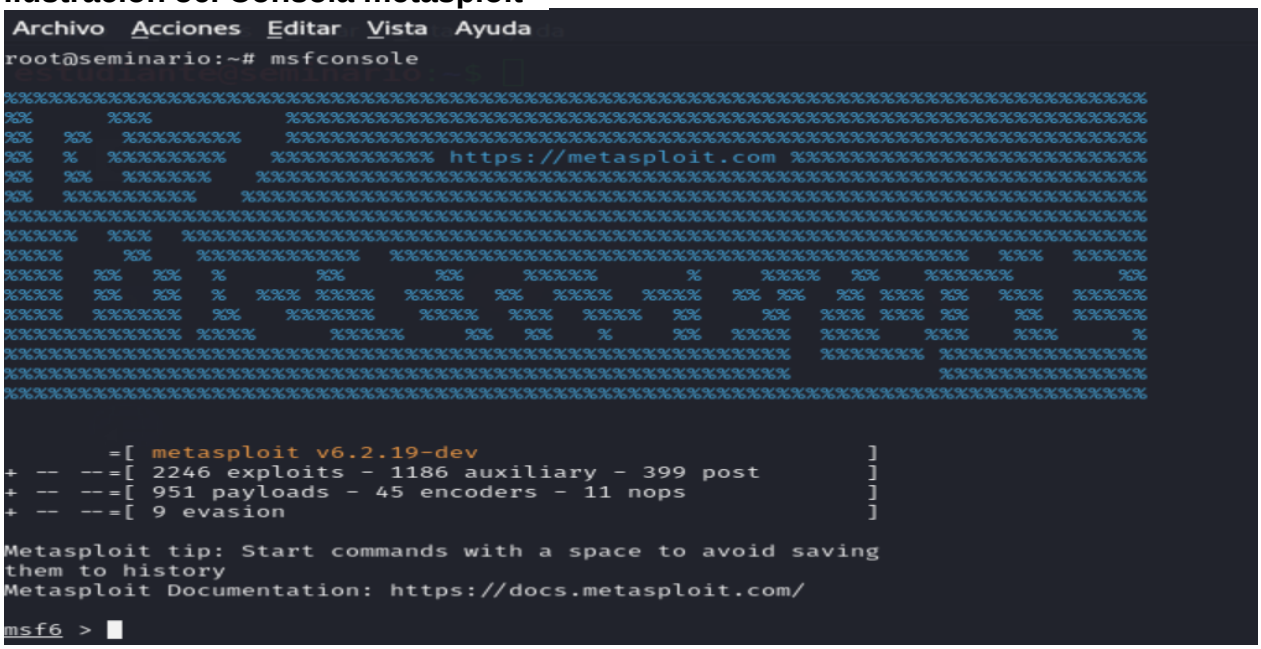
Iniciamos el metasploit

Ilustración 55. Metasploit



Fuente 55. Juan usama

Ilustración 56. Consola metasploit

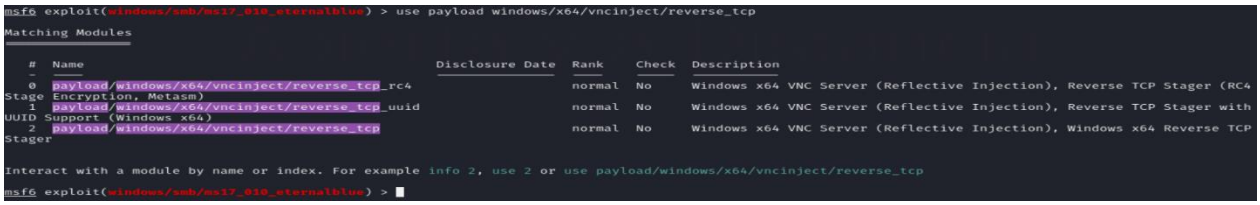


Fuente 56. Juan usama

Ilustración 57. Configuración

Fuente 57. Juan usama

Ilustración 58. Aplicación



Fuente 58. Juan usama

3.3.4 Presentar la información más relevante del anexo 4. Escenario 3 que fue de ayuda en la identificación del fallo de seguridad.

- Los computadores sobre los cuáles se tienen las sospechas tienen instalado Windows 7 x86 – x64.

- Los equipos de cómputo tienen activo el “SMBv1, el cuál es un protocolo para compartir impresoras y archivos dentro de la red informática de la empresa utilizado por Microsoft Windows con más de treinta (30) años de antigüedad”[10]. El SMBv1, es un protocolo que pertenece a la capa de aplicación en el modelo TCP/IP y utiliza el puerto 445/TCP.

- La fuga de información se presenta el 10/junio/2022.

- Los sistemas operativos no se encuentran actualizados y la última actualización del sistema operativo fue el 05 de febrero de 2017, demasiado tiempo sin la realización periódica de las actualizaciones.

- Los equipos pueden estar relacionados al fallo de seguridad CVE-2017-0144.

- Los computadores no tienen instalada la actualización MS17-010. Dicha actualización resuelve vulnerabilidades en sistemas operativos Microsoft Windows. La más grave de las vulnerabilidades podría permitir la ejecución remota de código si un atacante envía mensajes especialmente a un servidor Microsoft Server Message Block 1.0 (SMBv)

[10] UNIVERSITY INFORMATION TECHNOLOGY SERVICES. About the SMBv1 retirement. [Sitio web]. Estados Unidos. [Consulta: 03 de octubre de 2022]. Disponible en: https://kb.iu.edu/d/aumn#overview

3.4 CONTENCIÓN ATAQUES INFORMÁTICOS

3.4.1 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Argumentar respuesta técnicamente.

En la mayoría de los ámbitos de la vida, es mejor prevenir que curar, y la seguridad no es una excepción. Tratar en la medida de lo posible prevenir, se deseará evitar que, en primer lugar, se produzcan incidentes de seguridad. En caso de ocurrir, se debe garantizar el mínimo impacto posible.

Uno de los objetivos principales de los equipos Red Team y Blue Team, al interior de las organizaciones es proteger la infraestructura y la información de ataques informáticos. Por consiguiente, es importante contar con planes de acción que permitan gestionar, reaccionar, enfrentar los incidentes de seguridad y reestablecer el funcionamiento de la empresa en el menor tiempo posible y con el mínimo daño posible. Así mismo, contar con un Sistema de Gestión de Incidentes de Seguridad Informática disminuirá el riesgo de que algún ciberdelincuente irrumpa en la infraestructura tecnológica de la empresa.

Por otro lado, al momento de una organización sufrir un ataque informático en tiempo real, una de las primeras acciones a realizar serían las siguientes:

Prevenir. La prevención es una de las estrategias más esenciales de la seguridad informática, ya que nos permite preparar y transmitir a los usuarios información sobre los métodos y estrategias que se tengan al interior de la organización para enfrentar los ataques informáticos. La prevención puede abarcar capacitaciones, definición de una política de seguridad informática, definición de roles y niveles de acceso a la información, sistemas de control de acceso, buenas prácticas en los sistemas informáticos, charlas e instrucciones a la hora de afrontar un incidente. En este apartado, se pueden aplicar medidas preventivas en los sistemas informáticos como las copias de seguridad, tener activados los servicios de actualizaciones del sistema (“para corregir vulnerabilidades de día zero que permitan escalar privilegios a los atacantes tomando control de la seguridad de los equipos”[11], instalar y actualizar el antivirus, establecer restricciones de acceso a la información, tener cuentas de usuarios con contraseñas robustas, cerrar puertos y servicios no utilizados, instalar y mantener actualizado el antivirus, examinar los equipos periódicamente e instalar software licenciado.

Detectar y analizar. En este apartado, se espera que el equipo informático, identifique el tipo de ataque, el tipo de vulnerabilidad que se está explotando, destaque lo que está sucediendo, determine el impacto generado, nivel de

[11] KREBSON SECURITY. Microsoft patch Tuesday, October 2022. Estados Unidos. [Consulta: 11 de octubre de 2022]. Disponible en: https://krebsonsecurity.com/2022/10/microsoft-patch-tuesday-october-2022-edition/#more-61528

afectación al sistema, nivel de prioridad, analice de donde proviene el ataque, aparte el hardware y software que se está viendo comprometido (computadores, páginas web, servidores, impresoras, entre otros) con el fin de implementar la estrategia de contención adecuada frente al incidente. Así mismo, revisar el firewall de los equipos de cómputo, revisar los dispositivos conectados a la red, identificar puertos abiertos, validar actualizaciones y parches de seguridad instalados, examinar los computadores con el antivirus, inspeccionar configuraciones de red, separándolos y evaluándolos individualmente. De igual forma, en el proceso de detección se debe tener en cuenta el tipo de ataque que está sufriendo la organización. Lo anterior, con el fin de realizar un perfil del alcance y posible daño que se está sufriendo en la información de los equipos. Cabe destacar que existen diferentes ataques informáticos muy comunes en la actualidad, a saber: **Acceso no autorizado,** cuando un ciberdelincuente obtiene acceso lógico o físico sin autorización del administrador del sistema, **virus** (Manipulan, estropean archivos, generan errores y sobre cargan el sistema), **troyanos** ("registran pulsaciones de los teclados, leen contraseñas, abren puertas traseras, eliminan datos, bloquean información, secuestran información"[12], modifican datos, interrumpen el funcionamiento de los computadores en la red, ejecutan malware malicioso y toman el acceso de computadores de forma remota), **ransonware** ("tipo de software malicioso que irrumpe en computadoras, servidores y otros dispositivos bloqueando el acceso, eliminando datos y borrando aplicaciones"[13]), **phishing,** ("delito de engañar a las personas para que compartan información confidencial"[14],suplantación de identidad, recepción de correos fraudulentos, robo de información, robo datos personales y sustitución de páginas web bancarias oficiales), Denegación DoS ("Ataques que tienen como objetivo inhabilitar un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el cual está predestinado"[15]).

Contención. Busca la detención del incidente con el fin de que no se propague y pueda aumentar el daño en la información o infraestructura de TI en la organización, para facilitar esta tarea la empresa debe poseer una estrategia de contención frente a los ataques informáticos más comunes realizados por ciberdelincuentes, por ejemplo: apagar el internet, desconectar el sistema, desconectar los equipos de la red, deshabilitar servicios, separar los equipos afectados. Sin embargo, las estrategias de contención varían según el tipo de

[12] KASPERSKY LAB. ¿Qué es un troyano y qué daño puede causar?. [Sitio web]. España. [Consulta: 14 de septiembre de 2022]. Disponible en: https://www.kaspersky.es/resource-center/threats/trojans.

[13] BEYONDTRUST. What is Ransonware?. [Sitio web]. Estados Unidos. [Consulta: 11 de octubre de 2022]. Disponible en: https://www.beyondtrust.com/resources/glossary/ransomware

[14] MALWAREBYTES. ¿Qué es phishing?. [Sitio web]. Irlanda. [Consulta: 29 de septiembre de 2022]. Disponible en: https://es.malwarebytes.com/phishing/.

[15] OFICINA DE SEGURIDAD INFORMÁTICA. ¿Qué son los ataques DoS y DDoS?. [Sitio web]. España. [Consulta: 28 de septiembre de 2022]. Disponible en: https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

incidente que se pueda presentar, una buena estrategia es tener una buena documentación de los pasos a seguir frente a esta situación para facilitar y agilizar la contención del incidente.

Erradicación y recuperación. Una vez el incidente ha sido contenido se debe realizar un proceso de erradicación y eliminación de cualquier rastro dejado por el incidente, como virus, código malicioso, puertas traseras, contraseñas vulneradas, modificación de información, intermitencia de servicios, indisponibilidad de recursos, caídas de servidores y páginas web, entre otros. Posteriormente, se procede a la recuperación del funcionamiento de la infraestructura de TI a través de las restauraciones de los sistemas y servicios, copias de seguridad, puntos de restauración, formateo de equipos, parcheo de vulnerabilidades, robustecimiento de firewall y fortalecimiento de los sistemas con medidas de seguridad reforzadas.

Actividades post incidente. Una vez ha finalizado el proceso de detección, contención, erradicación y recuperación, la siguiente de las etapas a realizar en la organización, es analizar toda la información recolectada en el incidente, con el fin de aprender, mejorar e implementar nuevas estrategias de seguridad informática. Así mismo, como desarrollar un aprendizaje constante de las experiencias obtenidas que aportan al crecimiento del equipo de seguridad. No solo basta con defenderse frente al ataque y finalizar el proceso, sino, más bien, tener una documentación, compartir la experiencia, socializar y tomar decisiones con los entes responsables sobre cómo, cuándo, dónde y porque sucedió el incidente de seguridad. Las organizaciones, no están exentas de sufrir estos incidentes, unos leves, otras más graves y peligrosos, pero al final todos con la finalidad de perjudicar y comprometer la infraestructura de TI. Es allí, donde todos los esfuerzos realizados en la defensa de un incidente informático deben ser claramente abordados y tratados eficientemente, es decir, aplicar políticas de seguridad, revisiones periódicas de los sistemas, actualizaciones constantes en los equipos, antivirus funcionando, permisos restringidos, IDS (Sistemas de detección de intrusiones), pentesting e inversión en programas de seguridad.

3.4.2 Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team. ¿Qué medidas de hardenización propondría para que el ataque no se repita?

Como medidas de hardenización (“entendiéndose como el proceso de asegurar un sistema a través herramientas, técnicas y mejores prácticas para reducir las vulnerabilidades”[16]) para fortalecer el sistema, reducir y evitar las amenazas y los peligros de este, como los fallos presentados en la máquina virtual del laboratorio anterior, se pueden implementar los siguientes procesos:

[16] BEYONDTRUST. What is Systems Hardening?. [Sitio web]. Estados Unidos. [Consulta: 11 de octubre de 2022]. Disponible en: https://www.beyondtrust.com/resources/glossary/systems-hardening

- Establecer claramente y poner en práctica todas las directivas y procedimientos de seguridad informática.
- Configuración correcta de los dispositivos de seguridad, como pueden ser el firewall o los sistemas de autenticación.
- Evaluar de forma regular las vulnerabilidades de la infraestructura de TI.
- Realizar una auditoría informática por un experto regularmente.
- Mantener los sistemas operativos actualizados.
- Desarrollar, implementar y poner en práctica una directiva que requiera contraseñas seguras.
- Monitorear el tráfico de la red y rendimiento del sistema.
- Verificar que las copias de seguridad se almacenen y funcionen correctamente.
- Cerrar los puertos que no son utilizados ni necesarios en el funcionamiento del sistema.
- Desinstalar el software que no está siendo utilizado.
- Cambiar las claves que se tengan por defecto.
- Dar de baja a los usuarios que no son necesarios.
- Deshabilitar servicios que no estén siendo utilizados.
- Instalar un firewall.
- Actualizar los sistemas operativos con los parches de seguridad disponibles a la fecha.
- Concientizar a los usuarios sobre la importancia de la seguridad informática.
- Realizar capacitación sobre seguridad informática a los usuarios.
- No abrir archivos desconocidos.

- No descargar información de páginas no oficiales relacionadas al trabajo realizado.

- Establecer permisos y niveles de acceso a las carpetas compartidas en la empresa.

- Realizar actualizaciones de firmware en los equipos.

- Establecer contraseñas para el ingreso al BIOS.

- Desactivar el acceso remoto.

- Bloquear puertos.

- Establecer en el sistema operativo 2 particiones, una para la instalación de los programas y otras para el almacenamiento de la información.

- Crear dos usuarios en los computadores, un usuario administrador para todo lo relacionado a actualizaciones y cambios, y otro usuario estándar para el trabajo del empleado.

- Contar con el bloqueo de cuentas tras varios intentos fallidos.

- Programar un sistema de respaldo de información.

3.4.3 Describa con sus palabras las diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos.

El equipo Blue Team está defendiendo a la organización de ataques informáticos de una manera proactiva, es decir, es el equipo que está realizando una vigilancia constante en los activos informáticos de la organización, está reuniendo datos sobre todo activo que se deba proteger, está evaluando riesgos, está analizando informes de seguridad, patrones, comportamientos de usuarios e indicadores que se pueden obtener del funcionamiento normal de la red. Lo anterior, con el fin de establecer estrategias de seguridad que permitan estar alerta frente a cualquier cambio de comportamiento en la red. Así mismo, el equipo Blue Team trabaja en la mejora continua de la seguridad informática en la organización, buscando incidentes, estableciendo medidas de detección para futuros casos, reforzando las políticas de seguridad informática, identificando ataques, analizando los sistemas y las aplicaciones utilizadas para encontrar fallos o vulnerabilidades que comprometan a la empresa. De igual forma, el equipo Blue Team verifica que las medidas de seguridad aplicadas propendan por salvaguardar la integridad, disponibilidad y autenticidad de la información.

El equipo de respuesta a incidentes informáticos es quien enfrenta el problema de forma directa en tiempo real para darle solución. Este equipo se encarga utilizar herramientas de hardware y software para contener el incidente, erradicarlo y recuperar el sistema informático de la empresa en el mejor tiempo posible y con el menor impacto o daños sobre la infraestructura de TI. Son los encargados de brindar una solución “quirúrgica” sin interrumpir el desarrollo normal de las labores empresariales.

Por otro lado, el equipo Blue Team establece las estrategias defensivas para los sistemas informáticos de la organización, y cuando se presentan los incidentes informáticos el equipo de respuesta enfrenta la problemática presentada.

El equipo de respuesta a incidentes informáticos y blueteam pueden tener características muy similares en relación a la protección de los activos informáticos en la organización, ambos equipos procuran la seguridad en la empresa y cuentan con una serie de diferencias, a saber:

Tabla 1. Comparativa Blue Team y respuesta a incidentes

EQUIPO BLUE TEAM	EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS
Se enfoca en la seguridad defensiva.	Se enfoca en incidentes informáticos.
Realiza vigilancia constante y permanente analizando los comportamientos comunes de la red.	Analiza las causas de los incidentes y sus consecuencias.
Trabaja en la mejora continua de la seguridad.	Gestiona los incidentes.
Caracteriza la efectividad de las medidas de seguridad.	Detecta, contiene, erradica los incidentes y recupera el sistema.
Rastrea incidentes de ciberseguridad.	Documenta los procesos de contención de incidentes.

Fuente 1. Juan usama

3.4.4 ¿Si dentro de un equipo Blue Team le indican que debe trabajar con CIS "CENTER FOR INTERNET SECURITY" usted lo utilizaría para qué fin?

El Center for Internet Security (CIS), es una organización que tiene como objetivo mantener la seguridad de internet, realizando actividades como identificar, ejecutar, validar y proporcionar soluciones correspondientes a procesos de ciberdefensa. La implementación de CIS contribuye a desarrollar una estructura fundamental para la seguridad de la información en la empresa, a través, del cumplimiento de estándares y certificaciones legales que se centran en prácticas recomendadas reconocidas y evaluadas a nivel mundial en la aplicación de medidas de protección cibernéticas. Dentro del equipo Blue Team, el CIS contribuye en la utilización de los procedimientos establecidos para la seguridad contra ataques cibernéticos. Algunos de los procesos destacados del CIS son: Ofrecer soluciones de seguridad a nivel mundial, prevenir y responder a los incidentes informáticos, promover las mejores prácticas en ciberseguridad y liderar entornos de confianza en el ciberespacio. Así mismo, el Center For Internet Security lo utilizaría para desarrollar evaluaciones de vulnerabilidad; monitoreo y análisis de redes en la organización.

3.4.5 Explique y redacte las funciones y características principales de lo que es un SIEM.

El SIEM (Security Information and Event Management) o información sobre seguridad y gestión de eventos, es un sistema que busca brindar a las empresas una respuesta rápida y precisa para descubrir y responder ante cualquier amenaza sobre el sistema informático. Así mismo, como proporcionar una "visión global de la seguridad de las tecnologías de la información"[17]. Una solución SIEM permite controlar la seguridad informática de la empresa, ya que obtiene información y administración de los eventos que suceden en segundo plano para detectar patrones fuera de lo común. Un SIEM permite analizar en tiempo real los logs y eventos del sistema, permitiendo una mayor visibilidad a los administradores de lo que sucede en la red de la empresa. "Entre los objetivos de un SIEM, se puede encontrar, la detección de amenazas que se presenten en las organizaciones de manera potencial y resolverlas de manera eficiente en un corto tiempo"[18].

Funciones principales:

- Permite resolver de manera eficiente y eficaz cualquier tipo de amenaza.

[17] AMBIT TEAM. ¿Qué significa SIEM y cómo funciona? [Sitio web]. Barcelona- [Consulta: 03 de octubre de 2022]. Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona#

[18] KEEPCODING. ¿Qué es SIEM?. [Sitio web]. España. [Consulta: 29 de septiembre de 2022]. Disponible en: https://keepcoding.io/blog/que-es-siem-ciberseguridad/.

- Analiza en tiempo real los ataques que se presentan en el hardware y software.
- Detecta amenazas, ataques, vulnerabilidades.
- Monitorea las amenazas que afectan la seguridad informática de un sistema.
- Permite centralizar toda la información de amenazas con el fin de agilizar los procedimientos de respuesta frente a un ciberataque.
- Facilita el reporte de vulnerabilidades.

Características principales:

- Se integra a herramientas contra amenazas que permiten implementar aplicaciones para la seguridad (IDS o IPS)
- Valida eventos sospechosos para ser evaluados y priorizar el de mayor impacto y riesgo.
- Recolecta información de los casos generados, ya que permite manejar bases de datos.
- Cumple con las regulaciones de la industria.
- Evita y minimiza las consecuencias de un ataque.
- Fomenta la base de conocimientos a través de los registros y documentación de los incidentes.
- Disminuye el tiempo en la detección de ataques.
- Brinda información precisa para la realización de análisis forenses.
- Permite mejorar el manejo del riesgo.
- Permite identificar las violaciones de seguridad.

3.4.6 Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

A continuación, se presentan las herramientas que permiten realizar la contención de ataques informáticos:

- **OSSEC**, es una herramienta que permite monitorizar y detectar intrusos en una red informática. Puede realizar cualquier tipo de identificación de ataques para la mayor parte del sistema operativo.

- **SNORT**, es un IDS (Sistema de detección de intrusos) que tiene la capacidad de analizar el tráfico de la red en tiempo real y reaccionar a patrones detectados, permitiéndole detectar conexiones realizadas hacia el exterior que no deberían ejecutarse o ataques desde el exterior de la red como DoS y DDoS. Su principal funcionalidad es detectar exploit, la exploración de puertos y el bloque de las amenazas a través del análisis del tráfico de la red.

- **OPENWISP,** es un IPS (Sistema de prevención de intrusión) que permite la detección y prevención de intrusiones en el sistema inalámbrico a través de sensores que capturan el tráfico y lo envía al servidor para ser analizado. Posteriormente, analiza los datos de los sensores y responde a los ataques. También registra y produce alertas en caso de detectar un ataque. Detecta ataques de desasociación, en el que un atacante provoca la desconexión de los usuarios conectados a un AP.

4 CONCLUSIONES

- Los equipos Red Team y Blue Team son una excelente estrategia de seguridad al interior de la organización, ya que con sus procesos técnicos están brindando seguridad a la infraestructura TI. Así mismo, están monitoreando y evaluando constantemente la capacidad de protección frente a ataques cibernéticos con el fin de tomar las correcciones debidas y salvaguardar los activos informáticos.

- Se logran identificar las leyes y decretos de la ley colombiana sobre delitos informáticos y protección de datos personales. En ellas se evidencias las sanciones y multas a las que pueden ser acusados los infractores de las mismas. Las leyes colombianas exponen las consecuencias profesionales que pueden aplicar sobre las personas que incurran en alguno de los delitos.

- La postura ética y legal de los profesionales en la aplicación de pruebas de pentesting debe estar orientada a la solución de las vulnerabilidades encontradas y a la implementación de estrategias que le permitan a la organización salvaguardar las integridad, disponibilidad y confidencialidad de la información. Por ningún motivo, las vulnerabilidades encontradas podrán ser utilizadas por el profesional en beneficio propio.

- El mundo de la ciberseguridad exige el compromiso completo de los profesionales para combatir a los delincuentes que atentan contra la infraestructura informática de las empresas. De allí, que el profesional ejecute su mayor experiencia en la consecución de salvaguardar a la organización de posibles ataques.

- La ciberseguridad es una actividad dinámica, nunca estática y siempre debe estar sujeta a revisiones, auditorías, pruebas y soluciones para las vulnerabilidades encontradas.

- El profesional debe tener claro el compromiso de desarrollar sus actividades laborales fundamentado en el código de ética y legalidad. Allí se puede encontrar información acerca de los deberes, compromisos, responsabilidades, prohibiciones y sanciones de carácter valioso que orientan el actuar de las personas en el ejercicio de la ingeniería.

- Las herramientas de pentesting permiten recolectar información sensible de las organizaciones cuando no se cuenta con medidas de protección informática adecuadas.

- Se logra establecer que para las empresas enfrentar a los ciberdelincuentes deben procurar aplicar unos procesos fundamentales en la defensa contra los ataques

informáticos, como la realización de prevención, detección, análisis, contención, erradicación, recuperación y documentación del incidente. Lo anterior, con el fin de obtener experiencia de esos incidentes y poder responder eficientemente frente a eventos futuros.

- Las empresas deben procurar diseñar e implementar medidas de seguridad que logren minimizar el impacto de ataques o amenaza sobre el sistema informático de la empresa.

- El equipo de seguridad debe encargarse de robustecer la seguridad de los sistemas informáticos en la empresa, instalar software legal, instalar las actualizaciones y parches de seguridad, implementar IDS y estar evaluando constantemente las medidas adoptadas.

5 RECOMENDACIONES

Es fundamental que las organizaciones cuenten con un conjunto de medidas que permitan estar monitoreando el sistema informático con el fin de prevenir los ataques informáticos y las indisponibilidades en los servicios prestados.

Realizar las actualizaciones periódicas al software, mantener el sistema operativo al día e instalar periódicamente los parches de seguridad, son una de las normas más esenciales en procura de la seguridad informática en la organización.

Las organizaciones deben procurar tener instalado software legal en sus equipos de cómputo. Así mismo, implementar una consola de administración de antivirus que permita rastrear los computadores de la red y validar las irrupciones que se puedan presentar por software malicioso, phishing, troyanos y malware que pretenda irrumpir en la organización.

Las empresas deben contar con personal capacitado en temas de seguridad informática que se encuentre alerta a las diferentes amenazas que puedan materializarse y comprometer la información de la empresa. Se deben realizar capacitaciones a los usuarios para fortalecer el conocimiento y las condiciones de respuesta frente a ataques informáticos.

Realizar un monitoreo y revisión continua, cumpliendo con intervalos regulares de auditoria que permitan identificar oportunamente cualquier novedad sobre los sistemas operativos.

Al interior de las organizaciones deben existir políticas de respaldo de información que orienten a los usuarios en la forma correcta de salvaguardar la información como medida preventiva en caso de ocurrir un incidente informático. Es común apreciar como en ocasiones las empresas no cuentan con estas medidas y cuando ocurren los incidentes se pierde información sensible y confidencial.

Establecer un procedimiento de ingreso seguro a los sistemas operativos, para ello se debe por lo tanto implementar o hacer uso (si ya existe) de directorio activo con el fin de centralizar la información de los usuarios que pueden acceder a los sistemas operativos.

Actualizar los programas a las versiones recientes, ya que traen parches de seguridad que corrigen vulnerabilidades.

La seguridad de la información en las organizaciones es un requisito relevante que debe fundamentarse en la implementación de protocolos que salvaguarden su integridad, disponibilidad, confidencialidad y autenticidad.

6 BIBLIOGRAFÍA

AMBIT TEAM. ¿Qué significa SIEM y cómo funciona? [Sitio web]. Barcelona- [Consulta: 03 de octubre de 2022]. Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona#

BEYONDTRUST. What is Ransonware?. [Sitio web]. Estados Unidos. [Consulta: 11 de octubre de 2022]. Disponible en: https://www.beyondtrust.com/resources/glossary/ransomware

BEYONDTRUST. What is Systems Hardening?. [Sitio web]. Estados Unidos. [Consulta: 11 de octubre de 2022]. Disponible en: https://www.beyondtrust.com/resources/glossary/systems-hardening

CONGRESO DE LA REPÚBLICA. 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, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [Sitio web]. Bogotá. [Consulta 05 de septiembre de 2022]. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

EL CONGRESO DE COLOMBIA, Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. [Sitio web]. Colombia. [Consulta: 04 de septiembre de 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0044_1993.html.

EL CONGRESO DE COLOMBIA. Ley 44 de 1993 Nivel Nacional. [Sitio web]. Bogotá. [Consulta 05 de septiembre de 2022]. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3429&dt=S

EL CONGRESO DE COLOMBIA. Ley 890 de 2004. [Sitio web]. Bogotá. [Consulta de septiembre de 2022]. http://www.secretariasenado.gov.co/senado/basedoc/ley_0890_2004.html

KASPERSKY LAB. ¿Qué es un troyano y qué daño puede causar?. [Sitio web]. España. [Consulta: 14 de septiembre de 2022]. Disponible en: https://www.kaspersky.es/resource-center/threats/trojans

KEEPCODING. ¿Qué es SIEM?. [Sitio web]. España. [Consulta: 29 de septiembre de 2022]. Disponible en: https://keepcoding.io/blog/que-es-siem-ciberseguridad/

KENNERTECH. Ley 603 del 2000 tecnología de la información. [Sitio web]. Bogotá. [Consulta 04 de septiembre de 2022]. https://www.kennertech.com.co/ley-603-del-2000-tecnologia-de-la-informacion/

KREBSON SECURITY. Microsoft patch Tuesday, October 2022. Estados Unidos. [Consulta: 11 de octubre de 2022]. Disponible en: https://krebsonsecurity.com/2022/10/microsoft-patch-tuesday-october-2022-edition/#more-61528

LYON GORDON. Nmap: Discover your network. [Sitio web]. Estados Unidos. [Consulta: 29 de septiembre de 2022]. Disponible en: https://nmap.org/

MALWAREBYTES. ¿Qué es phishing?. [Sitio web]. Irlanda. [Consulta: 29 de septiembre de 2022]. Disponible en: https://es.malwarebytes.com/phishing/

OFICINA DE SEGURIDAD INFORMÁTICA. ¿Qué son los ataques DoS y DDoS?. [Sitio web]. España. [Consulta: 28 de septiembre de 2022]. Disponible en: https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

OPENWEBINARS. ¿Qué es OpenVAS?. [Sitio web]. Sevilla. [Consulta: 06 de septiembre]. Disponible en: https://openwebinars.net/blog/que-es-openvas/

POLICIA NACIONAL. Normatividad sobre delitos informáticos. Ley 1273 de 2009. [Sito Web]. [Consulta 04 de septiembre de 2022]. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

UNIVERSITY INFORMATION TECHNOLOGY SERVICES. About the SMBv1 retirement. [Sitio web]. Estados Unidos. [Consulta: 03 de octubre de 2022]. Disponible en: https://kb.iu.edu/d/aumn#overview

ZULUAGA MATEUS, Allen David. HACKING ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la Rama Judicial, seccional Armenia.[En línea]. Trabajo de grado aplicado. Universidad Nacional Abierta y a Distancia, 2017.

[Consulta 05 de septiembre de 2022]. Disponible en https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

7 ENLACE VIDEO

https://youtu.be/Mas4ZCdYwcM