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

JOHN YEFERSON VALBUENA CAMACHO

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

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

JOHN YEFERSON VALBUENA CAMACHO

LUIS FERNANDO ZAMBRANO
Director del Curso

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

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

pág

GLOSARIO

Ciberseguridad: se le llama a la ciberseguridad a cualquier tipo de práctica la cual sea el de los sistemas, programas y redes de aquellos ataques digitales. Estos ciberataques por lo general apuntan a acceder, modificar o eliminar la información, en algunas ocasiones también con el fin de extorsionar a los usuarios.

Delito informático: Se considera un delito cibernético o ciberdelito a toda acción antijuridica la cual es utilizada en ambientes digitales con fines ilegales.

Pentesting: Una prueba de penetración consiste en realizar un ataque controlado a un sistema informático con el fin de encontrar vulnerabilidades en los sistemas.

Vulnerabilidades: A una falla o debilidad en un sistema informático se le denomina vulnerabilidad, lo cual puede ser aprovechada por algún individuo que pueda explotarla.

RESUMEN

Actualmente para la transmisión de la información se utiliza diversos canales, ya sean físicos o virtuales, todo con el fin de obtener una mayor visibilidad y disponibilidad de esta misma, sin embargo cada vez que se utilice estos medios para dicha transmisión, se crean también brechas de seguridad el cual son vulneradas por individuos, organizaciones e inclusive por Gobiernos para extraer y obtener información que pueda ser utilizada con el fin de extorsionar o en muchas ocasiones para desestabilizar políticamente países, por tal motivo, el trabajo para reglamentar y formalizar leyes que castiguen cualquier delito que atente con la integridad, confidencialidad y disponibilidad de la información en una empresa siempre debe de ser ejemplar para que no se justifique dichos actos.

Para muchas empresas la implementación de seguridad basada en informática es un campo de carácter obligatorio lo cual considera la protección de sus datos, información e infraestructura tecnológica.

Esta implementación se considera una inversión lo cual debe ser siempre apoyado por las altas gerencias en cada empresa, contribuyendo con las áreas de tecnología en el desarrollo de los objetivos de la compañía junto con su modelo de negocio.

Por tal razón en Colombia el sector empresarial y gubernamental cada vez esta más comprometido con la Seguridad informática, esto ha ayudado a que estemos en una posición la cual nos comprometa a dedicar más esfuerzos con el fin de contrarrestar ataques y fugas de información.

En el presente informe se enfoca en analizar los términos legales que encierra los delitos informáticos que actualmente se brinda en la norma colombiana y los parámetros también internacionales, así mismo se realizó pruebas de ejecución de ciberseguridad bajo escenarios controlados y los diferentes medios para contenerlos.

Con lo anterior podemos validar la importancia de que una empresa pueda contemplar en sus equipos de trabajo, expertos en seguridad informática que ayuden fomentar la protección de la información mediante técnicas de aseguramiento a la infraestructura y a sus servicios más críticos.

PALABRAS CLAVE

Ciberseguridad, confidencialidad, explotación, hardenizacion, Pentesting, vulnerabilidades.

INTRODUCCIÓN

El uso del internet y la trasmisión de datos por los diferentes canales utilizados por las empresas, sin importar su modelo de negocio, se volvió un tema tan importante ya que muchas de sus operaciones se manejan mediante el uso de tecnologías.

Todo uso que se realice mediante trasmisión electrónica genera en muchas ocasiones gastos de infraestructura y desarrollo de aplicaciones o bases de datos, infraestructura que debe de protegerse al igual que la información que contenga.

Ante lo anterior la seguridad informática busca poder proteger estos activos que son tan importantes para una empresa ya que ayudan en el desarrollo de los objetivos principales de la compañía, teniendo como base los pilares principales de la información que son disponibilidad, integridad y confidencialidad.

En Colombia los delitos informáticos son más comunes de lo que la gente del común puede imaginarse, en el marco de la emergencia sanitaria provocada por el Covid 19, hubo un incremento significativo frente a los delitos informáticos, obligando no solo a Colombia si no a países de todo el mundo a reforzar los temas de ciberseguridad trabajando en conjunto con el sector empresarial lineando políticas que hagan más segura la protección de la información.

En el presente informe se busca citar la legislación colombiana frente a los delitos informáticos y protección de datos, de igual forma tener la información de dispositivos y controles que protejan la infraestructura como también la correcta toma de decisiones al momento de vincular personal a una empresa.

De igual forma en la ejecución de pruebas sobre escenarios controlados las cuales fueron realizadas, lograron identificar ciertas vulnerabilidades para que el equipo encargado de implementar soluciones logre realizar el desarrollo de reparación de dichas vulnerabilidades.

OBJETIVOS

OBJETIVO GENERAL

Exponer en el informe técnico los aspectos a resaltar para destacar las actividades que se desarrollaron en el seminario sobre equipos estratégicos en ciberseguridad: RedTeam & BlueTeam.

OBJETIVOS ESPECÍFICOS

- ✓ Realizar una consulta sobre las leyes y normatividad vigente en Colombia para analizar cada uno de sus artículos que formalizan los delitos informáticos y protección de datos

- ✓ Ejecutar los métodos de pentesting para explotar las vulnerabilidades encontradas en el banco de trabajo.

- ✓ Construir un informe a partir de las pruebas de pentesting y recomendaciones realizadas para tener claridad en los resultados obtenidos del seminario.

1 DESARROLLO DE LA ACTIVIDAD

1.1 ETAPA 1 CONCEPTOS EQUIPOS DE SEGURIDAD

1.1.1 Margen legal en Colombia

1.1.2 Delitos Informáticos

En Colombia actualmente frente a la legislación que nos regula, tenemos la ley 1273 de 2009, el cual modifica el código penal y se crea un bien tutelado “de la protección de la información y de los datos”, en esta normatividad se preservan los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Dentro de dicha ley se encuentra 2 capítulos los cuales se integran de la siguiente manera:

Capitulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

En este capítulo la ley condena delitos referente a la manipulación de la información y personal mediante el uso de dispositivos y sistemas informáticos, en el capítulo de condenan delitos como el acceso abusivo a un sistema informático, la obstaculización ilegitima de un sistema informático, interceptación de datos, captura de datos personales mediante la suplantación de sitios Web, daño informático y el uso del Software malicioso, cada uno de estos delitos comprende pena de prisión de cuarenta y ocho (48) a noventa y seis (96) mese y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Capitulo Segundo: De los atentados informáticos y otras infracciones.

Mencionando este capítulo se complementa la ley acuerdo a delitos que contenga el hurto y la trasferencia no permitida de la información, delitos cuya pena van desde los cuarenta y ocho (48) a los ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

1.1.3 Protección de datos Personales

Los datos personales es toda aquella información que nos asocia y nos identifica como persona ante cualquier entidad privada o pública. Esta información en Colombia se encuentra tanto en bancos, empresas privadas y en entidades públicas entre otras, las disposiciones legales que regulan la protección de datos personales es la ley estatutaria 1581 de 2012, la cual tiene como objeto reconocer el derecho constitucional de las personas a conocer, actualizar y rectificar toda información que se haya recogido sobre ellas en cualquier base de datos y la cual sea protegida y regulada acuerdo a la legislación.

1.1.4 Etapas del pentesting

Como estrategias de ciberseguridad resulta de gran oportunidad para una empresa conocer y poner a prueba de manera constante todos los procesos tecnológicos y los usuarios que la utilizan, esto con el fin de realizar un escenario similar al de un ataque, con el propósito de saber cómo resolver este tipo de situaciones. Estas actividades son realizadas por personas capacitadas en el área con el propósito de descubrir fallas en la compañía.

1.1.5 Tipos de Pentesting

1.1.5.1 Pentesting de Caja Blanca:

En este caso el profesional o el pentester realiza un análisis completo e integral en donde evalúa toda la infraestructura ya que se le entrega toda la información con respecto a la seguridad de la empresa.

1.1.5.2 Pentesting de Caja Negra:

Para este caso el pentester no tiene ningún tipo información sobre la entidad y su actuar es el de un ciberdelincuente con el fin de detectar las fallas sobre el sistema.

1.1.5.3 Pentesting de Caja Gris:

En este caso el pentester no posee información específica sobre la información o dispositivos a realizar la prueba, lo cual le puede conllevar mas tiempo y recurso en poder identificar el objetivo para resaltar las vulnerabilidades.

1.1.6 Las fases de un Pentesting

1.1.6.1 Recopilación de la Información

En esta fase la cual se considera como la principal del pentest, se recolecta toda la información posible el cual tengamos el objetivo, en donde se utiliza varias técnicas como:

- Escaneo de puertos
- Escaneo de Versiones de Sistemas operativos
- Escaneo de Ips
- Filtrado de Metadatos

De las herramientas open source más utilizadas para este tipo de escaneo encontramos la Nmap.

1.1.6.2 Análisis de Vulnerabilidades

En la fase del análisis de vulnerabilidades realizamos las acciones disponibles con el fin de poder comprometer a el objetivo, a los usuarios y su información, entre las vulnerabilidades más encontradas son:

- Diseño no seguro
- Fallos en la autenticación
- Integridad de los datos
- Fallos en el desarrollo del software
- Componentes no seguros
- Pérdida del control de acceso

Entre las herramientas que se pueden utilizar para dicho análisis de esta fase esta Nessus

1.1.6.3 Explotación de Vulnerabilidades

En esta fase el pentesting se encarga de explotar las vulnerabilidades encontradas en la fase anterior mediante los mecanismos utilizados, se puede utilizar diversos exploits contras las vulnerabilidades identificadas o mediante el uso de credenciales encontradas, para tener acceso podemos utilizar la herramienta OpenVAS o Metasploit Franework

1.1.6.4 Post Explotación

En algunos casos no siempre se aplica esta fase, consiste en que una vez se haya completado las fases anteriores con éxito y se haya logrado vulnerar algún sistema u obtenido credenciales o permisos de administrador, se logre como objetivo escalar privilegios con el fin de obtener todos los accesos posibles, de las herramientas que se puede utilizar en esta fase esta Empire o Enumdb.

1.1.6.5 Reporte

En la última fase del pentesting lo que realizamos es entregar un reporte o informe de vulnerabilidades, en donde se comunica todo lo realizado y las diferentes vulnerabilidades encontradas, también se plasma las recomendaciones con el fin se subsanar los inconvenientes que pueda presentar la empresa en caso de un ataque, para la elaboración de dichos informes podemos usar la herramienta Dradis o Faraday.

1.1.7 Herramientas y servicios de Seguridad

1.1.7.1 Metasploit Framework

Podemos considerar a Metasploit como una herramienta útil enfocada en auditorias de seguridad y equipos de Red Team y Blue Team, desarrollada en perl y ruby, sus principales características se enfocan en tener varios exploits los cuales son vulnerabilidades conocidas, encontramos módulos llamados payloads en donde se contiene códigos con el fin de explotar estas vulnerabilidades.

1.1.7.2 Nmap

Nmpa en un software de código libre el cual se puede utilizar para el rastreo de puertos, originalmente fue creado para Linux sin embargo en la actualidad es multiplataforma.

1.1.7.3 OpenVas

Con OpenVas podemos encontrar una suite de software diseñado como un marco de trabajo en donde se agrupa varios servicios y herramientas que se especializan en el escaneo de las vulnerabilidades y su gestión, bajo pruebas autenticadas y no autenticadas, lo cual contiene un poderoso lenguaje de programación interno en donde facilita implementar cualquier tipo de prueba de vulnerabilidad.

1.1.7.4 ExploitDB

Con el servicio de Exploit Database (ExploitDB) el cual es consultado en línea, podemos encontrar una base de datos de exploits con fines de seguridad pública en donde explica lo que se puede encontrar en la base de datos. Este servicio resulta ser muy útil ya que se pueden identificar debilidades en la Red y también se es útil al momento de estar actualizado sobre los ataques que actualmente afectan diferentes redes.

1.1.7.5 CVE

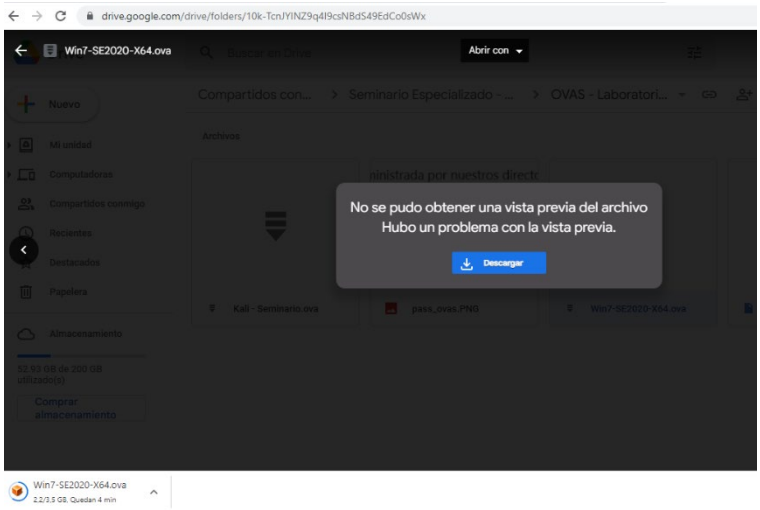
CVE (Vulnerabilidades y exposiciones comunes) es un servicio en línea muy reconocido por albergar en sus bases de datos varias vulnerabilidades expuestas por expertos en seguridad a fin de identificar los riesgos que se exponen en la Red.

1.1.8 Banco de Trabajo

Para la elaboración de la arquitectura del Banco de Trabajo se realizará bajo un ambiente virtualizado el cual se instalará dos Sistemas operativos de tipo Windows 7 y una distribución basada en Debian más conocida como Kali Linux para el desarrollo de auditoría y seguridad informática.

Se realiza la importación de la primera Máquina Virtual Windows 7 x 64 desde la ruta enviada al foro

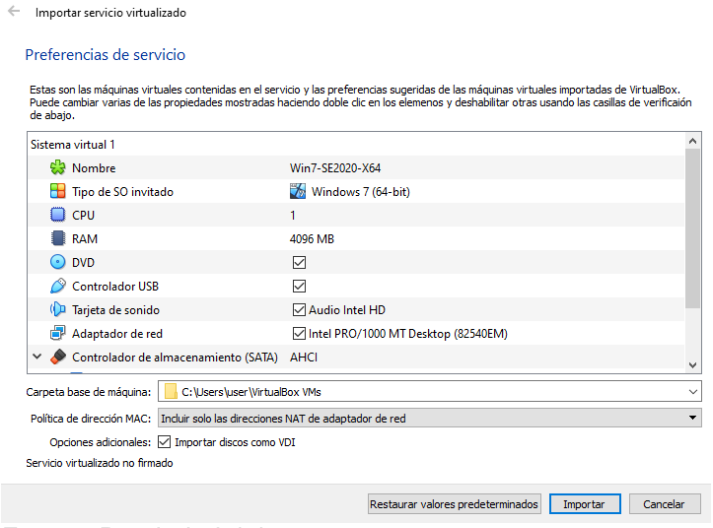
Ilustración 1: Descarga Archivo OVA Win 7x64



Fuente: Propiedad del Autor

Se realiza la importación del archivo al ambiente virtualizado en VirtualBox

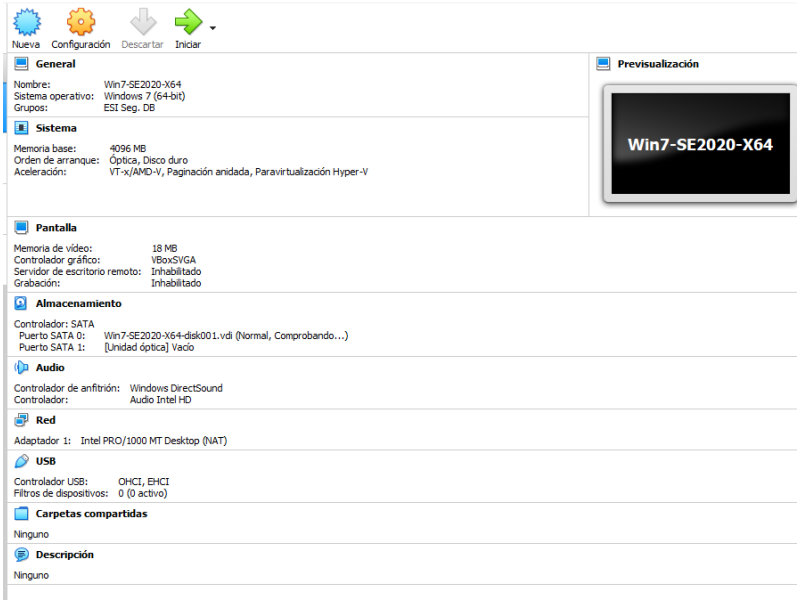
Ilustración 2: Importación archivo OVA



Fuente: Propiedad del autor

Una vez importada al ambiente virtualizado validamos los aspectos técnicos

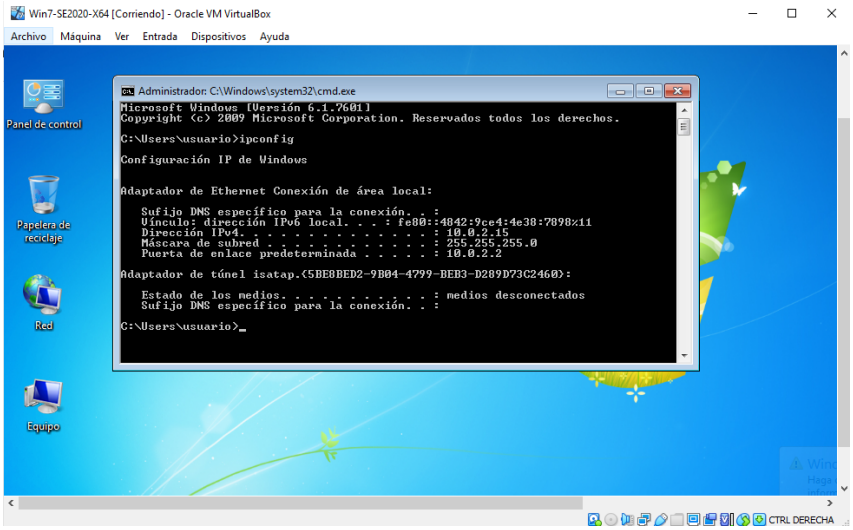
Ilustración 3: Revisión detalle técnico



Fuente: Propiedad del autor

Iniciamos la máquina virtual para probar su funcionamiento y consultamos su ip para comprobar red

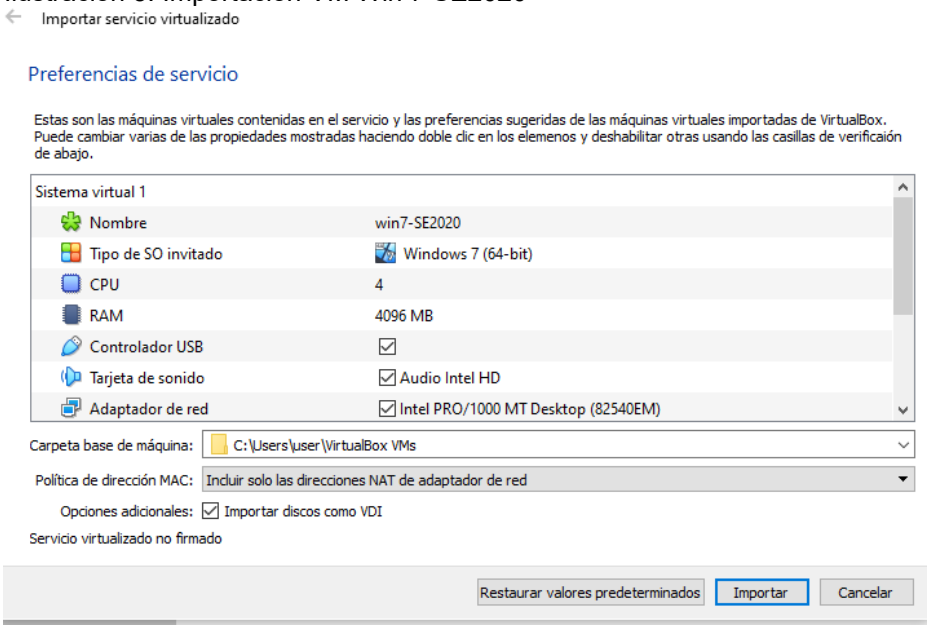
Ilustración 4: Inicio Windows 7 x 64



Fuente: Propiedad del Autor

Para la segunda máquina virtual Win 7 SE2020 realizamos el mismo procedimiento, descargamos el archivo para la importación en el ambiente virtualizado.

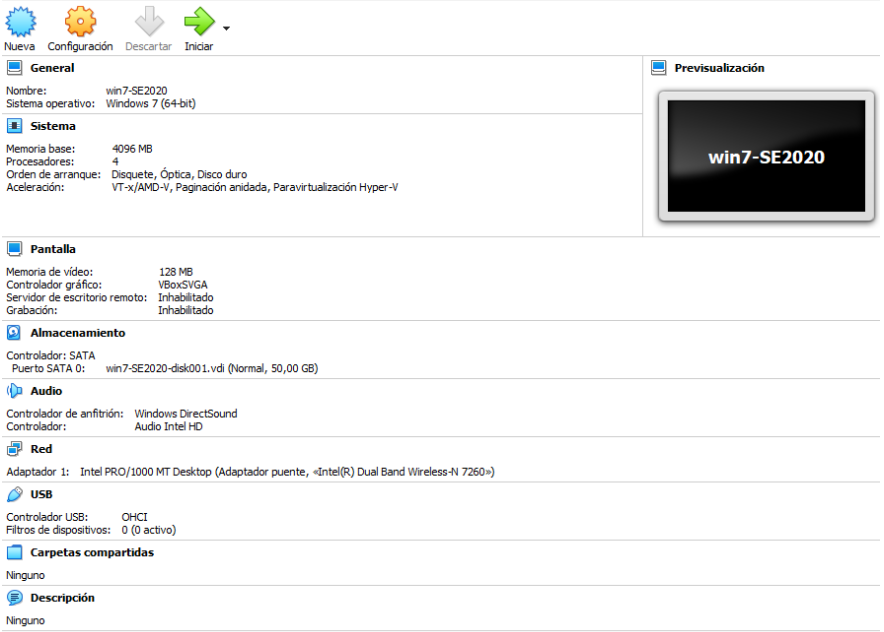
Ilustración 5: Importación VM Win 7 SE2020



Fuente: Propiedad del Autor

Validamos la configuración de la maquina una vez importada

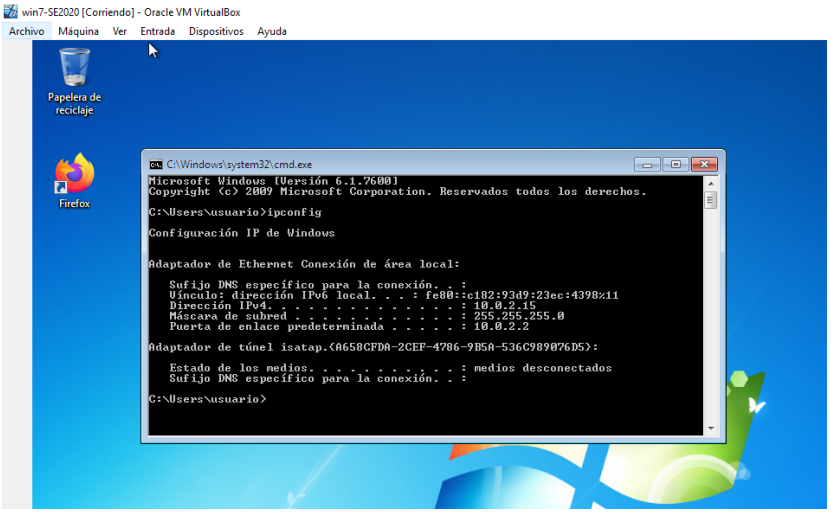
Ilustración 6: Configuración VM



Fuente: Propiedad del Autor

Iniciamos la maquina y validamos que tenga RED con un ipconfig

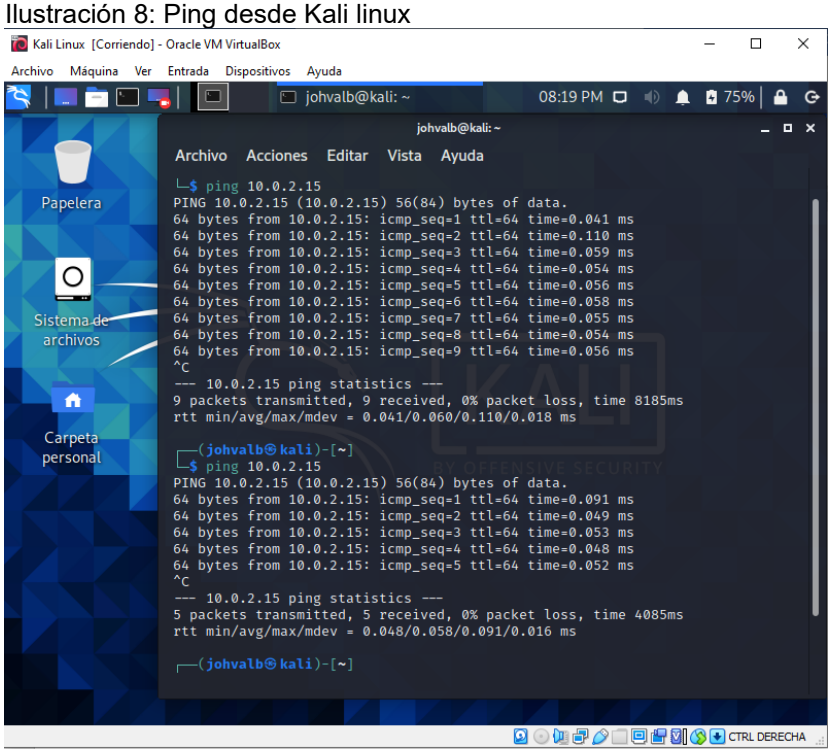
Ilustración 7: validación VM Win 7 SE2020



Fuente: Propiedad del Autor

Desde la máquina de Kali Linux ya instalada en el ambiente virtualizado realizamos pruebas de ping a los Windows 7

Ilustración 8: Ping desde Kali linux



Fuente: Propiedad del Autor

Es de tener presente que una vez tenida solo una máquina de Windows encendida esta toma la ip designada desde el router

1.2 ETAPA 2 ACTUACIÓN ÉTICA Y LEGAL

1.2.1 Escenario 2 y acuerdo de confidencialidad

La presente tiene como finalidad validar el escenario 2 y el acuerdo de confidencialidad con respecto a la problemática propuesta.

1.2.1.1 Escenario 2

Se debe de tener en cuenta que en las empresas los contratos deben ser elaborados por un abogado de oficio y que labore actualmente en la compañía con experiencia en contratación, debido a que el contrato del escenario 2 fue elaborado por un abogado que ya no labora y que además fue despedido por encontrar procesos sospechosos e ilegales podemos evidenciar la falta de revisión por parte de la alta gerencia detectando así que no está cumpliendo con sus funciones trasparentes, debiendo realizar una revisión detallada a la documentación elaborada por dicho abogado

1.2.1.2 Acuerdo de confidencialidad

En relación con el anexo 3 el cual hace referencia al acuerdo de confidencialidad podemos mencionar algunas inconsistencias que relacionan a continuación:

En la cláusula primera resalta la parte el cual indica “se obliga a no divulgar directa, indirecta, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados. Con lo anterior podemos deducir que la empresa incumple con la ética del profesional ya que lo obliga a no difundir en el momento en que detecte algún echo ilegal en la empresa.

En la cláusula segunda en donde se hace referencia a la información confidencial en el ítem 2 nombran los datos secretos a las chuzadas e interceptación ilegal, cabe aclara que este tipo de técnicas solo son permitidas por una endita judicial competente y siempre y cuando cuente con una orden judicial.

En la cláusula cuarta en donde dice que “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.” Se obliga al profesional a la falta de ética para que este no denuncie si hay actividades ilegales en la empresa, de igual cabe resaltar que estas actividades solo corresponden a entidades judiciales autorizadas.

De igual manera en el numeral 9 misma clausula se refiere a la no divulgación de la información sin previa autorización, se debe de considerar este numeral y agregar que la información debe ser suministrada si una entidad judicial la solicita para entes de investigación.

1.2.2 Análisis frente a la legalidad vigente en Colombia ley 1273 de 2009

Una vez realizada la lectura de la ley 1273 de 2009, el acuerdo de confidencialidad, podemos deducir las siguientes irregularidades:

En la cláusula segundad vemos como se vulnera el artículo 269A “ACCESO ABUSIVO A UN SISTEMA INFORMATICO” ya que con dicha cláusula se define la información confidencial, como Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

En el anexo 3 es claro que en algunas cláusulas viola el Artículo 269B. “OBSTACULIZACION ILEGITIMA DE SISTEMA INFORMATICO”, en donde no se le permite al profesional a divulgar procesos ilegales.

Articulo 269C. “INTERCEPTACION DE DATOS INFORMATICOS”, en la cláusula segunda ítem 2, hace referencia a la información confidencial como datos secretos, como datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos.

En el anexo 3 se menciona la manipulación de la información en varios de sus cláusulas, siendo una violación al Artículo 269F. “VIOLACION DE DATOS PERSONALES”, en ese sentido manipular dicha información para bien propio y sin poder denunciar actos ilegales, se está contribuyendo a que la información no tenga el manejo adecuado.

1.2.3 Revisión de la Propuesta laboral

Para el caso de la revisión del contrato laboral, siendo profesional en la rama de la ingeniería de sistemas y seguridad informática, no sería procedente aceptar dichas clausulas y firmar el contrato pese a que este carece de trasparencia y no está acorde a la norma vigente colombiana, siendo un riesgo para el profesional y falta de ética en varias de sus conductas.

Teniendo como presente el código de ética COPNIA establecido en la ley 842 del 2003 el cual se compone por tres capítulos donde se refieren a las disposiciones como los deberes, las obligaciones y prohibiciones en conjunto con las inhabilidades e incompatibilidades aplicadas al personal profesional en la rama de la Ingeniería, teniendo en cuenta lo anterior y revisada cada una de las cláusulas del acuerdo, en la mayoría se contempla acciones ilegales que va en contra de la integridad de la información.

1.2.4 Operación Andromeda Buggly

La fachada Andrómeda de inteligencia militar, el caso del hacker Andrés Sepúlveda, la filtración de documentos secretos y la existencia de una polémica lista de correos escandalizaron al país.[1]

En el informe que entregado por una comisión especial del Ministerio de Defensa por el caso Andrómeda comienza por una fachada de inteligencia que, revelada por la revista Semana en febrero del año 2014, desató una serie de investigaciones ya que presuntamente desde aquel lugar se habrían realizado actividades contra los negociadores del proceso de paz. Según la investigación, este arrojo que allí se encontraron grandes fallas de seguridad en donde evidenciaron indisciplina y una falta de control del personal el cual visitaba la dependencia. No se tenía ningún tipo control sobre las actividades que se realizaban por el personal militar y civil el cual era ajeno a la Operación Andrómeda. Varias de estas personas que ingresaban, tenían un alto conocimiento y diferentes capacidades en el área de informática, sin embargo, lo hacían sin ningún tipo de sin supervisión alguna.

A pesar de que la operación Andrómeda tenía fundamento bajo la Ley 1621 de 2013, Plan Nacional de Inteligencia para identificar amenazas contra el Estado; el ejército en su defensa aseguró que no haría interceptaciones con el fin de sabotear el proceso de paz, adicionado a esto, el caso reveló la información obtenida por la operación Andrómeda.

En dicha operación se evidencio la falta de seguridad y control en los procesos que fueron ejercidos por el ejército, lo anterior demuestra que la información y la privacidad de las personas es vulnerada, dejando un vacío y cuestionando la información que ha obtenido el gobierno de sus ciudadanos y con el fin que se ha utilizado, a pesar de que varios sitios web o correos electrónicos nos aseguran tener la privacidad y seguridad de la información, nunca es confiable el uso que se le da, ya que como vimos en esta operación, es vulnerada por hackers, o personas comunes, pero también por personas que están vinculadas al Estado.[2]

---

[1] Semana. (2015, enero 24). El informe que sacudió el caso de la fachada Andrómeda. {Sitio Web} (02/09/2022) Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3

[2] José Luis Peñarredonda. (2015, December 9). Detrás de Buggly: la historia de la fachada Andrómeda • ENTER.CO. {Sitio Web} (02/09/2022) Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

1.3 ETAPA 3 EJECUCIÓN PRUEBAS DE INTRUSIÓN

1.3.1 Herramientas para utilizar en el Laboratorio

1.3.1.1 Kali linux

Kali Linux es una distribución de Linux desarrollada a partir de Debian que puede utilizarse principalmente para detectar brechas de seguridad en ordenadores o conexiones a Internet, recuperar datos perdidos o analizar contraseñas.[3]

1.3.1.2 Metasploit

Metsploit es una herramienta para el desarrollo y ejecución de exploits contra una máquina remota, le permite realizar auditorías de seguridad, probar y desarrollar sus propios exploits. Originalmente creado en el lenguaje de programación Perl, Metasploit Framework ha sido completamente reescrito en el lenguaje Ruby.[4]

1.3.1.3 Nmap

Nmap es un software de código abierto que se utiliza para escanear una red y sus puertos con el objetivo de obtener información importante sobre la misma para controlar y gestionar su seguridad. Es una aplicación que se utiliza normalmente para realizar auditorías de seguridad y monitoreo de redes.[5]

1.3.2 Escenario 1. Máquina virtual win7-SE2020

Realizando la verificación de la configuración de la VM WIN7-SE2020 validamos la tiene la siguiente conectividad:

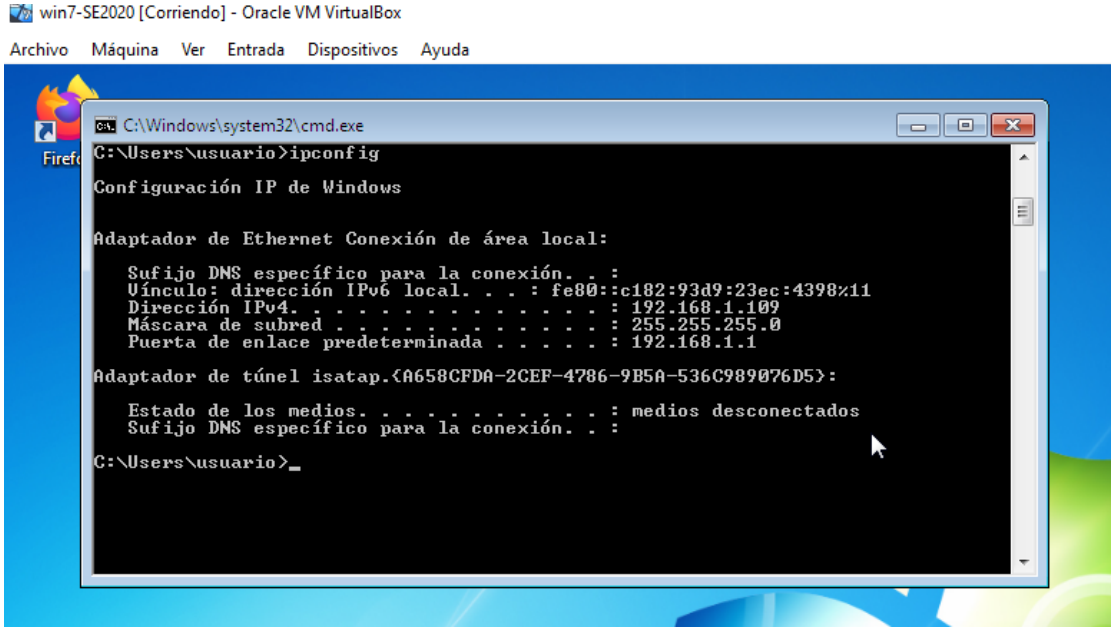
---

[3] Kali Linux: ¿qué es Linux para hackers?. (2022). {Sitio Web} (19/09/2022) {Disponible en }https://www.ionos.es/digitalguide/servidores/configuracion/kali-linux/

4 Metasploit: ¿qué es y cómo usarlo?. (2018). {en línea} (19/09/2022) {Disponible en:} https://www.funinformatique.com/es/que-es-metasploit-y-como-usarlo-bien/

5 Abrie, A. (2022). Nmap: Análisis de puertos y monitorización de redes - ICM., {en línea} (19/09/2022) {Sitio Web:} https://www.icm.es/2022/05/06/nmap-analisis-de-puertos-y-monitorizacion-de-redes/

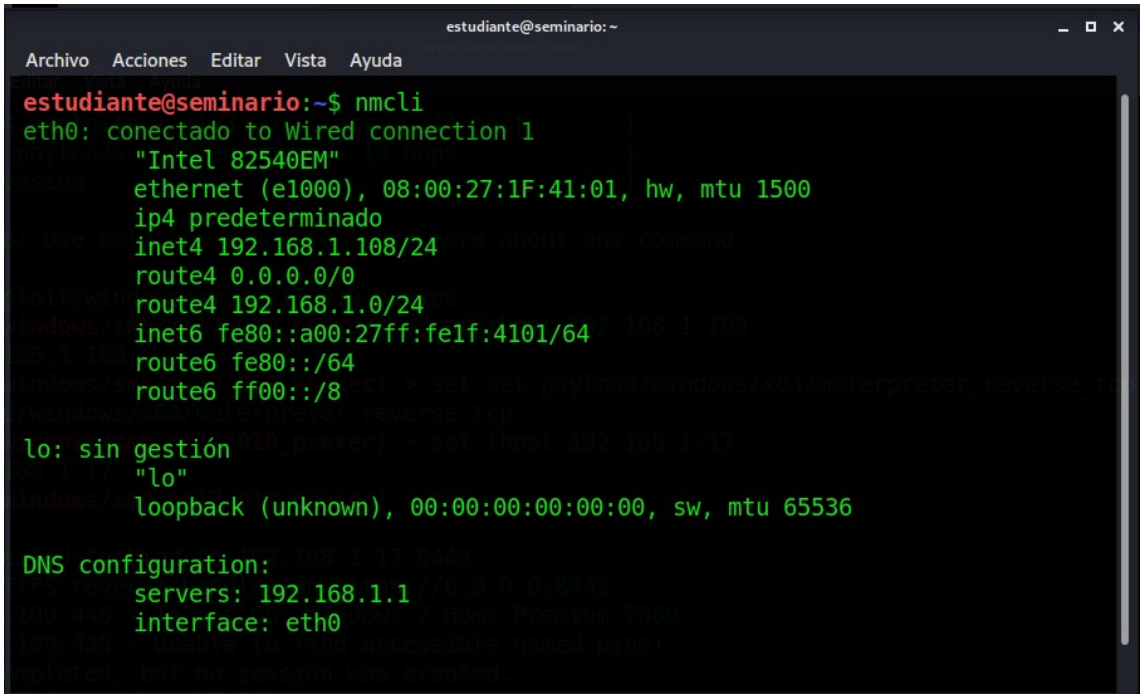
Ilustración 9: IP VM WIN7-SE2020



Fuente: Propiedad del Autor

Y de igual forma validamos la configuración de red de la VM de kali linux la cual es de donde se realizará el ataque:

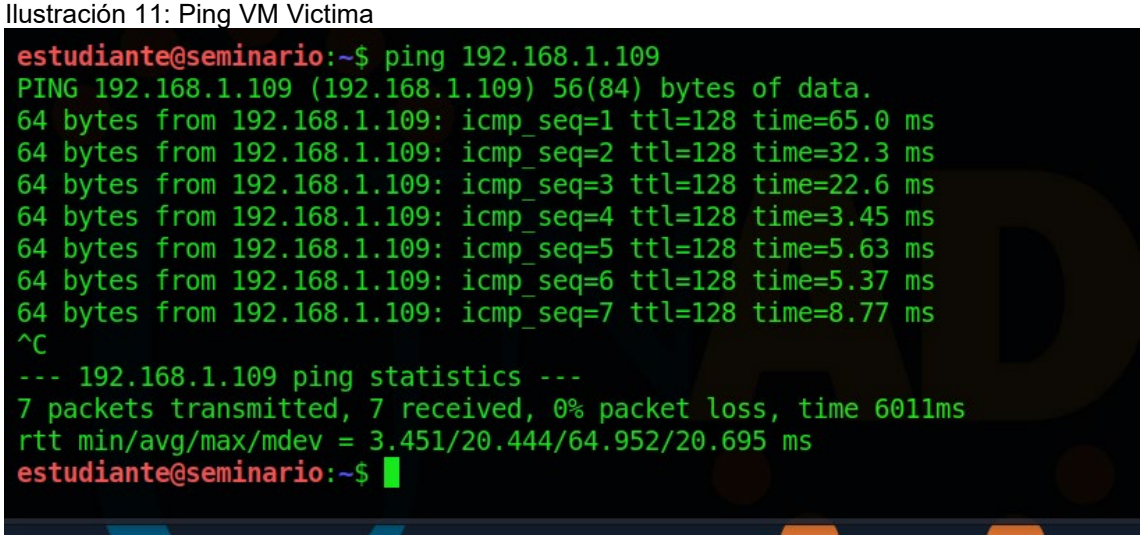
Ilustración 10: IP Kali lunux



Fuente: Propiedad del autor

Desde la maquina atacante de valido que tuviera comunicación con la maquina victima

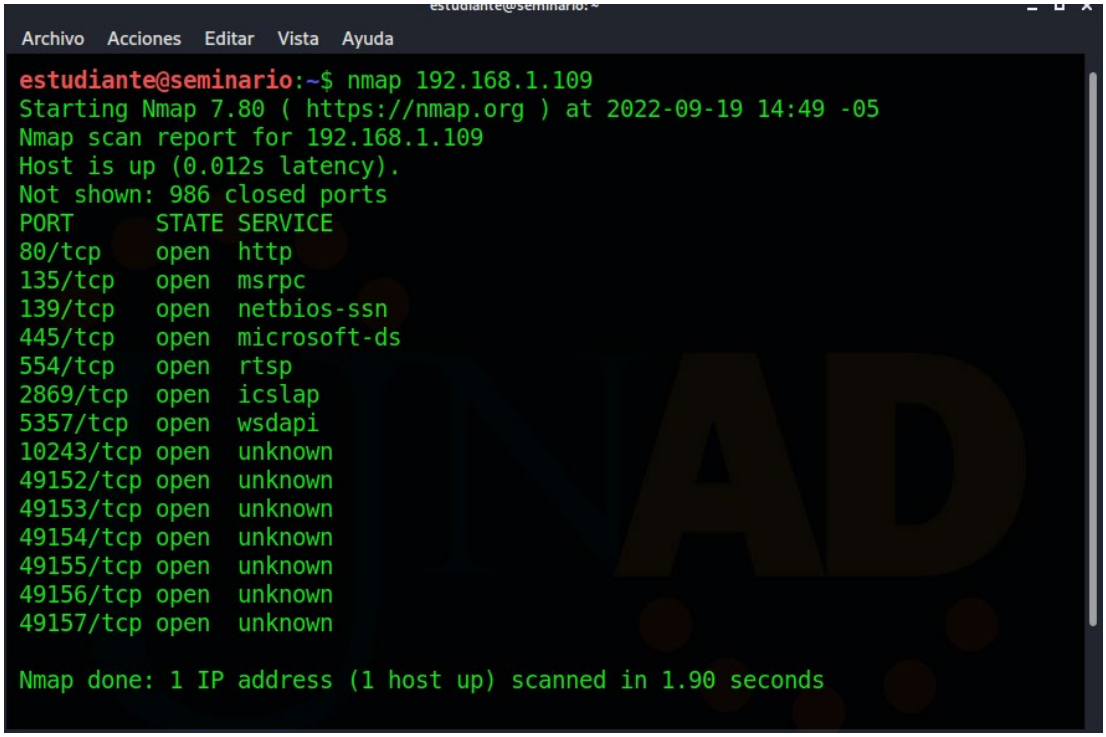
Ilustración 11: Ping VM Victima



Fuente: Propiedad del Autor

Realizamos el escaneo con nmpa para conocer que puertos tiene abierto

Ilustración 12: NMAP 192.168.1.109

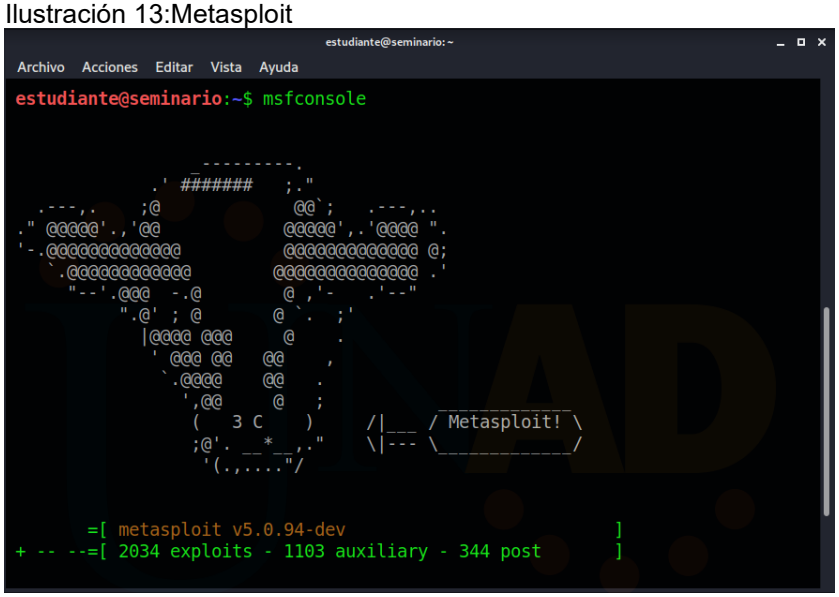


Fuente: Propiedad del autor

En el anterior escaneo se puede observar que el puerto 445 se encuentra abierto, este puerto es asignado a NetBIOS, Network Basic Input / Output System para lo cual es una gran vulnerabilidad ya que tampoco está maquina cuenta con actualizaciones recientes, ante lo anterior podemos realizar un ataque.

Iniciamos metasploit desde la maquina atacante

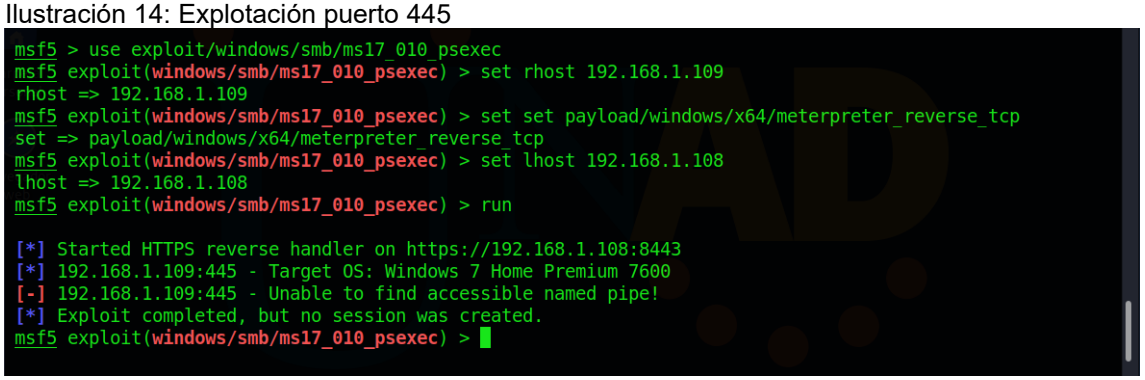
Ilustración 13:Metasploit



Propiedad del Autor

Una vez identificada la vulnerabilidad e iniciado nuestras herramientas para empezar el ataque, lo siguiente es ejecutar uno a uno los comandos de explotación:

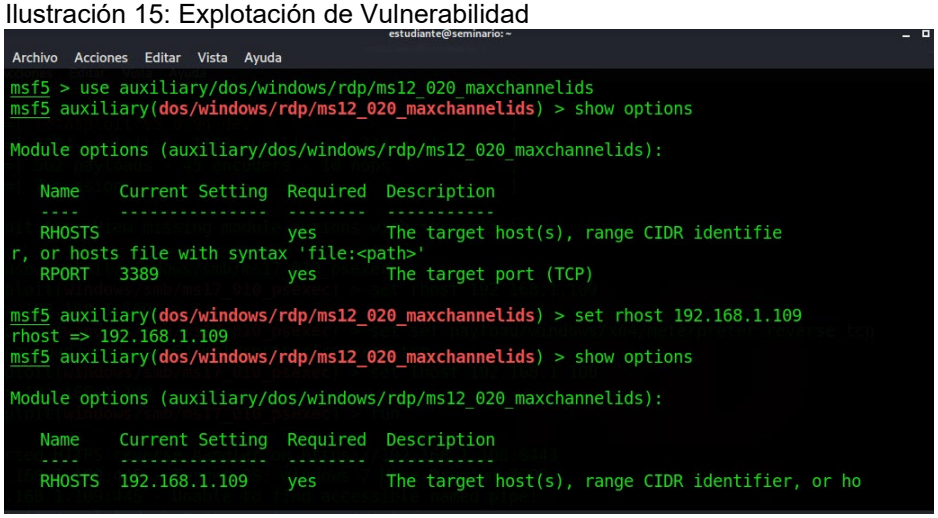
Ilustración 14: Explotación puerto 445



Fuente: Propiedad del Autor

Y después de estos ejecutamos el exploit lo nos dará el error de la pantalla azul en la maquina víctima:

Ilustración 15: Explotación de Vulnerabilidad

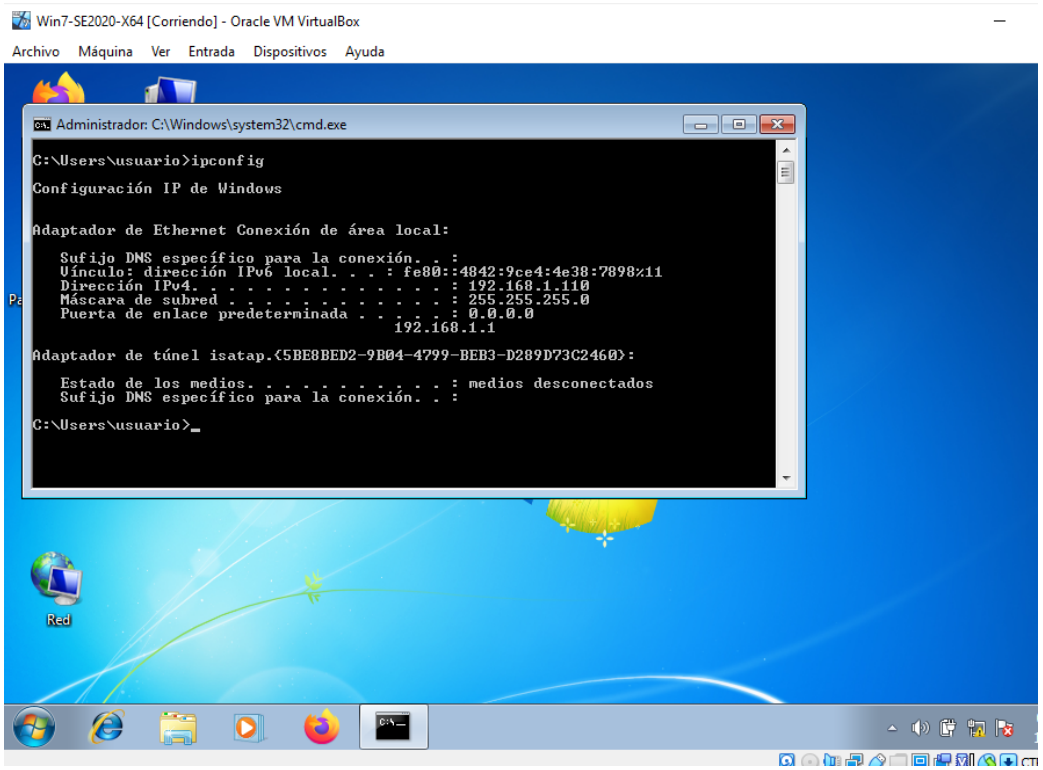


Fuente: Propiedad del Autor

1.3.3 Escenario 2 Win7-SE2020-X64

Realizando la verificación de la configuración de la VM WIN7-SE2020 validamos la tiene la siguiente conectividad:

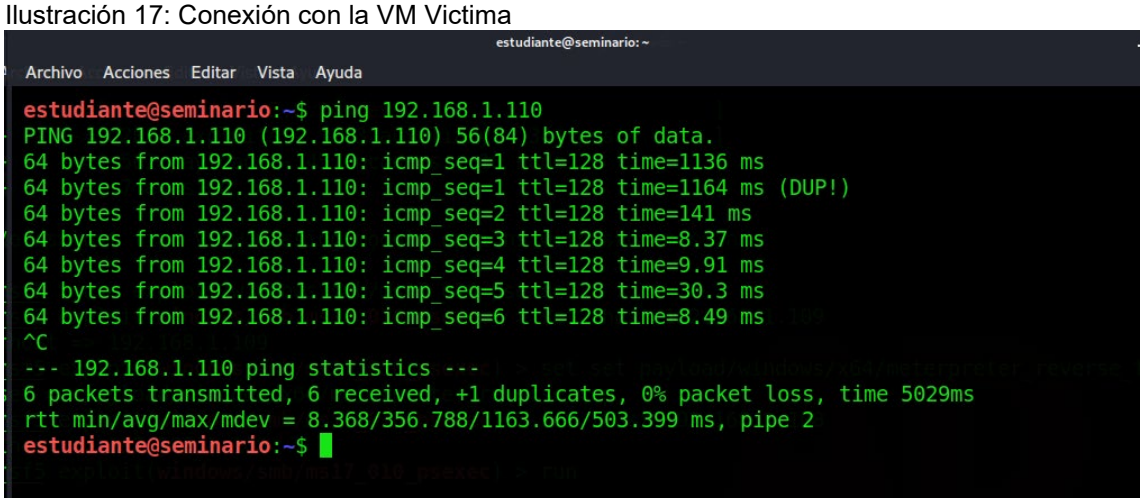
Ilustración 16: IP VM WIN7-SE2020-X64



Fuente: Propiedad del Autor

Desde la maquina atacante se valido que tuviera comunicación con la maquina victima

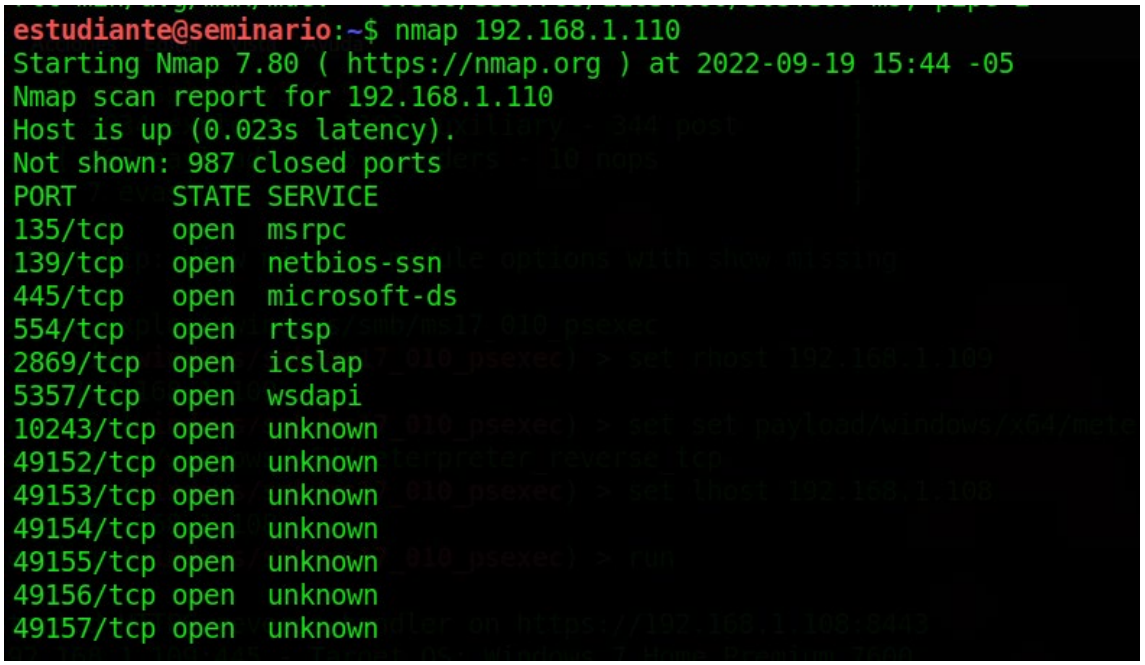
Ilustración 17: Conexión con la VM Victima



Fuente: Propiedad del Autor

Realizamos el escaneo de vulnerabilidades con nmap

Ilustración 18: Escaneo NMAP

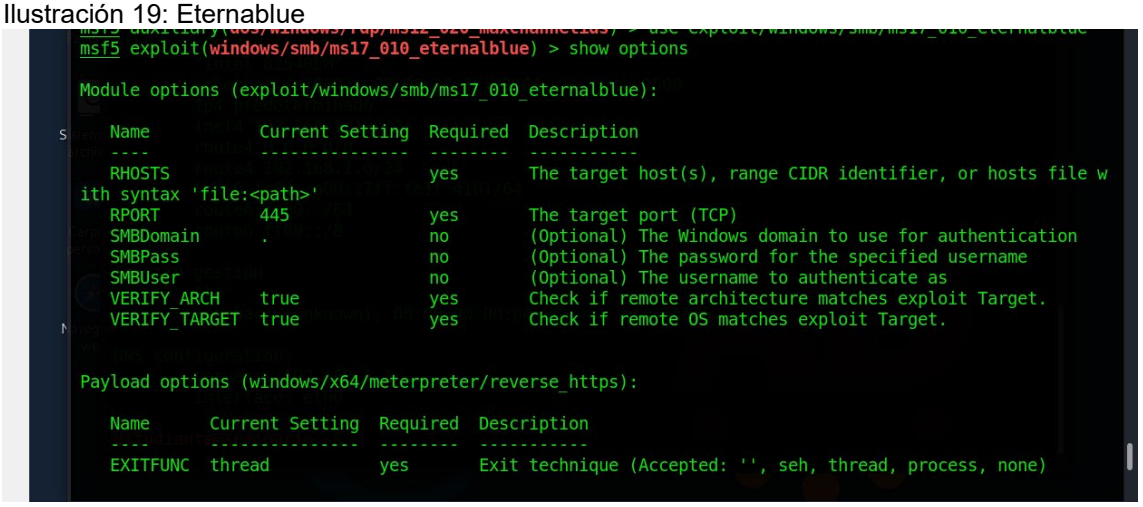


Fuente: Propiedad del autor

Para realizar la explotación de la vulnerabilidad iniciamos metasploit y ejecutamos el exploit EternalBlue, este exploit solo afecta a los sistemas operativos Windows, cualquier cosa que use el protocolo de intercambio de archivos SMBv1 (Server Message Block versión 1) está técnicamente en riesgo de ser objetivo de ransomware y otros ciberataques.[6]

[6] ¿Qué es EternalBlue y por qué el exploit MS17-010 sigue siendo relevante? (2022). {Sitio Web} (19/09/2022) {Disponible en:} https://www.avast.com/es-es/c-eternalblue

Ilustración 19: Eternablue

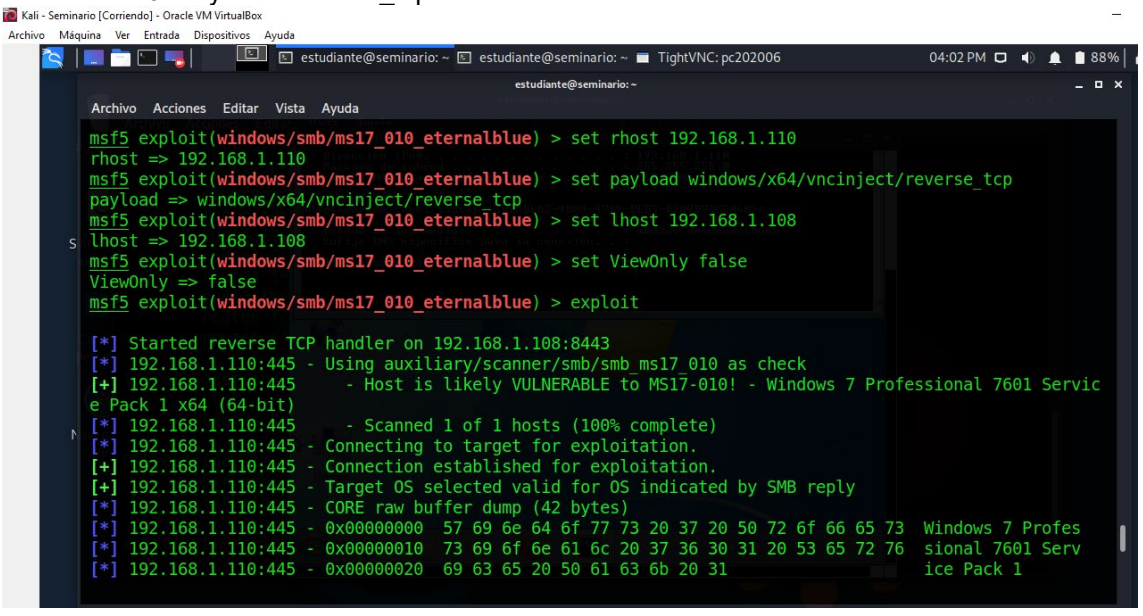


Fuente: Propiedad del Autor

Realizamos una consulta a las opciones para ejecutar el ataque acuerdo a las vulnerabilidades encontradas

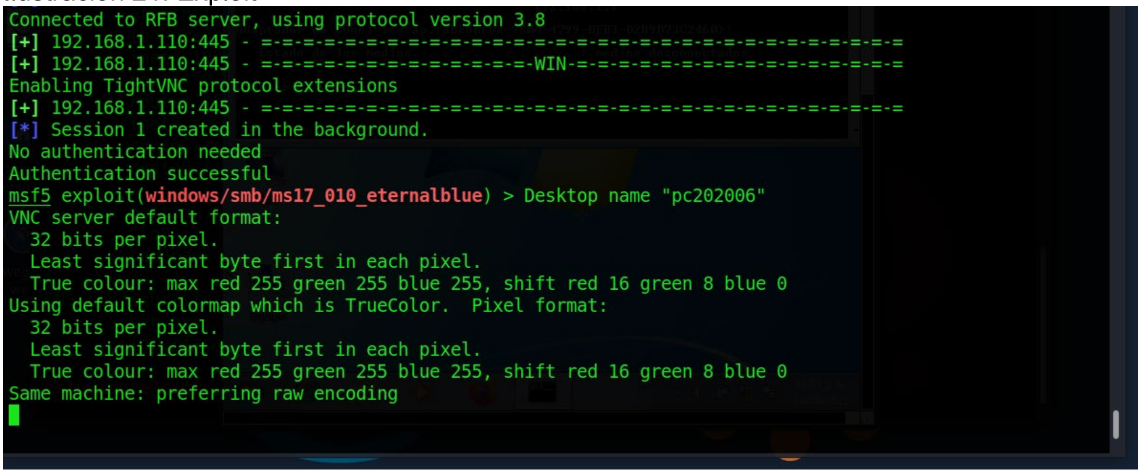
Para lo anterior configuramos el Rhost con la ip de la VM Victima para ejecutar el Payload Reverse_tcp e iniciar el exploit

Ilustración 20: Payload Reverse_tcp



Fuente: Propiedad del Autor

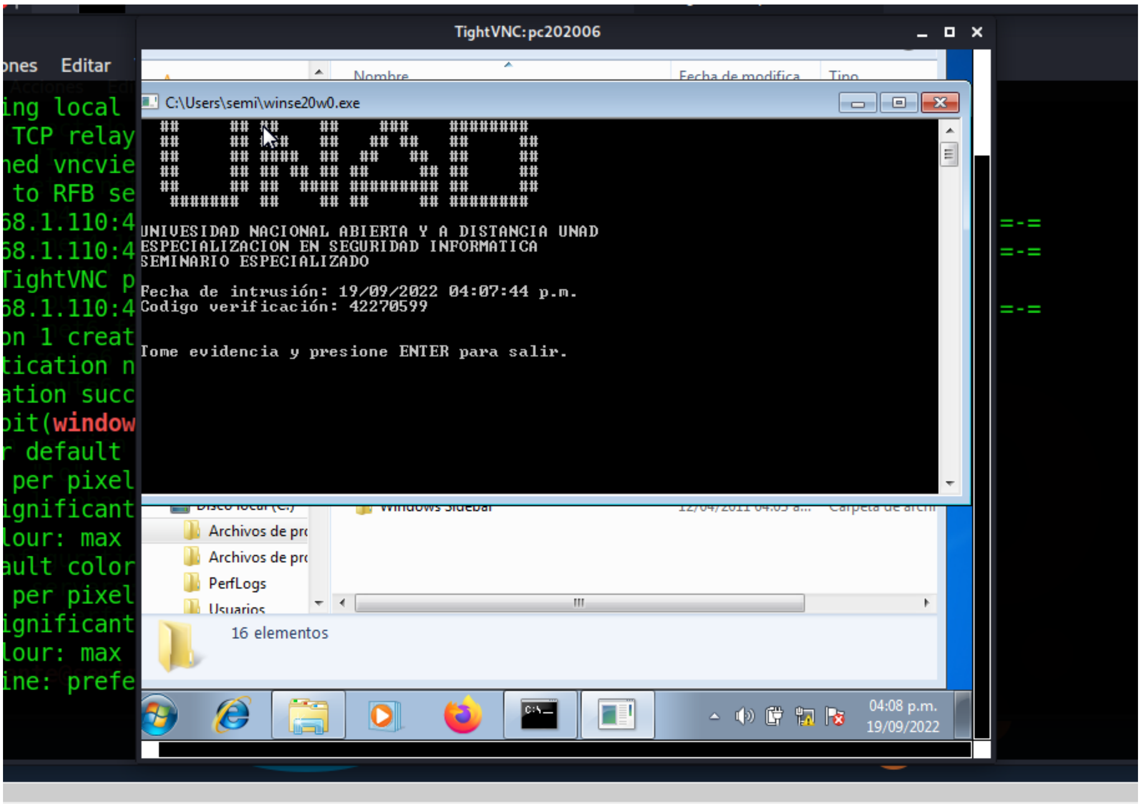
Ilustración 21: Exploit



Fuente: Propiedad del Autor

Una vez ya dentro de la máquina de la víctima buscamos y ejecutamos el archivo winse20w0

Ilustración 22: winse20w0

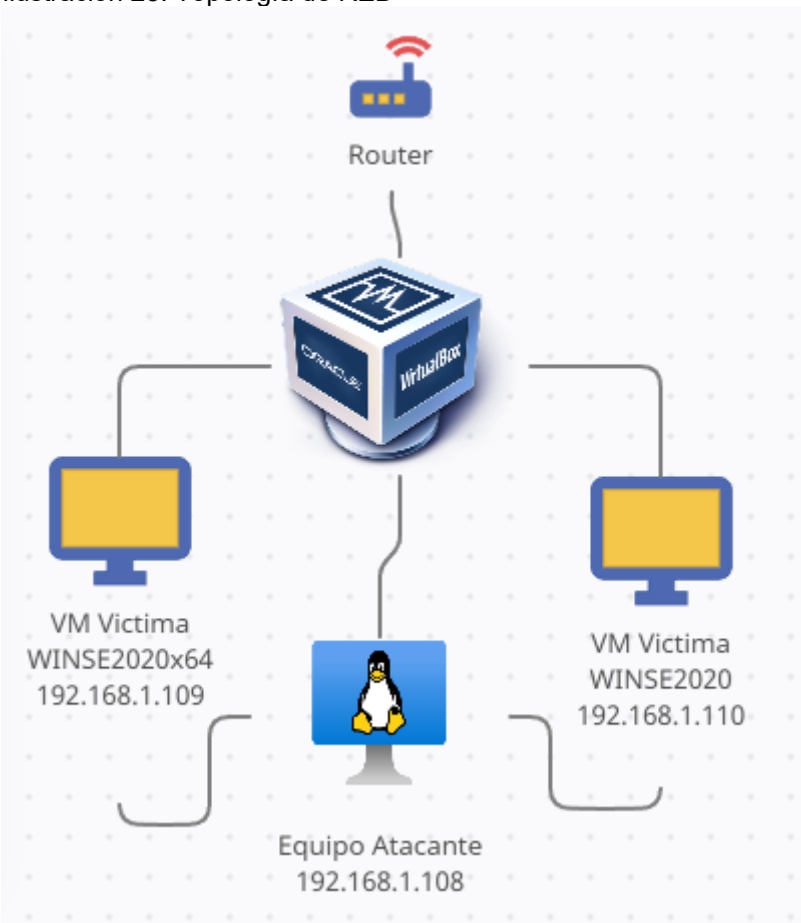


Fuente: Propiedad del autor

Con lo anterior evidenciamos como se está generando la fuga de información de la empresa.

1.3.4 Topología de Red

Ilustración 23: Topología de RED



Fuente: Propiedad del Autor

1.4 ETAPA 4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

1.4.1 Ataque en Tiempo real

Para poder entender la situación que se pueda presentar en una empresa en caso de un ataque cibernético, debemos tener claro los actores que pueden estar detrás de este ataque:

Personas: En este caso los llamados hackers quienes actúan de forma independiente, buscando de algún modo algún tipo de beneficio económico.

Grupos Organizados: Normalmente son grupos quienes buscan diferentes finalidades como lo son ideológicas o activistas, sin embargo, también suelen buscar el terrorismo.

Gobiernos: Son ataque que se enfocan en desestabilizar algún gobierno o país dentro de una estrategia de ciberguerra, en donde su objetivo son los sistemas de información.

Empresas privadas: Son ataques dirigidos a infraestructuras privada con el fin de conseguir información privada en lo que se denomina el ciber espionaje.[7]

Ya identificado lo anterior, es muy importante la acción que tomemos en caso de presentarnos frente a un ataque cibernético, lo siguiente son recomendaciones que se pueden realizar para dicho fin:

- Contener el ataque: En esta etapa se debe de realizar un escaneo de los dispositivos que están siendo atacados o que son objetivos del ataque y se deben de aislar para no afectar toda la red.

- Eliminar las causas: Con un escaneo exhaustivo en busca de la amenaza de sebe de eliminar cualquier posible causa que haya permitido el ataque.

- Determinar el alcance: Determinamos el alcance que haya tenido del ataque, identificando los equipos y dispositivos afectados como la información que pudo haberse afectado e incluso sustraído.

- Asegurar la continuidad del servicio: Se debe garantizar que la continuidad del servicio sin afectar los objetivos del negocio.

[7] Johnson, L. (2020). Security component fundamentals for assessment. Security Controls Evaluation, Testing, and Assessment Handbook {Sitio Web } ({Disponible en}. https://doi.org/10.1016/b978-0-12-818427-1.00011-2

Ante lo anterior debemos de determinar los niveles a articularse frente a un ataque:

- ✓ Aspecto Técnico: Con el fin de restablecer el servicio desde lo operativo
- ✓ Aspecto Legal: Con el fin de evaluar las implicaciones legales frente a los usuarios y las notificaciones a las autoridades competentes
- ✓ Gestión de Crisis: Se debe de manejar la correcta comunicación frente a los clientes y medios de comunicación con el fin de no impactar la reputación de la empresa.

1.4.2 Propuestas medidas de hardenización ante el ejercicio de Redteam

Hadernizar o robustecer cualquier medida de seguridad es la prioridad que se debe de tener en la organización, a continuación, se listan algunas de las recomendaciones más comunes que se deben de tener en cuenta frente a un ataque:

- ✓ Instalar un Sistema Operativo actualizado en las maquinas junto con los parches de seguridad recomendados
- ✓ Tener un antivirus potenciado que monitoreo los dispositivos que están en la red frente a las bases de datos de las amenazas actuales
- ✓ Realizar un escaneo de puertos determinando cuales se encuentran abiertos y que puedan representar una amenaza.
- ✓ Realizar auditorías periódicas
- ✓ Implementar y administrar dispositivos de seguridad que filtren el tráfico antes de entrar a la RED como lo es un IPS y un Firewall
- ✓ Cambio de contraseñas seguras periódicamente en los dispositivos
- ✓ Realizar bloqueos para la instalación de software desconocido en las maquinas
- ✓ Restringir la navegación a sitios no permitidos por la institución

Ante lo anterior también es importante que la empresa cuente con Direcciones de Tecnología que implementen un SGSI con políticas a implementar y que sean de estricto cumplimiento tales como:

- Política de protección de Datos
- Política de Clasificación de la Información
- Política de la Seguridad de la Información
- Política para la destrucción de la información
- Copia y respaldo de la información
- Política de Navegación
- Uso de correo electrónico
- Gestión de Incidentes y Vulnerabilidades
- Gestión de Activos
- Gestión de Riesgos
- Control de Acceso
- Contraseñas Seguras

Sin embargo y acuerdo al anexo la empresa no cuenta con suficiente presupuesto para lo cual el equipo de profesionales debe de recomendar y utilizar herramientas con licencia GPL, con el fin de optimizar recursos y de igual forma proteger la RED, herramientas como:

- Aircrack: herramienta que contiene una suite de aplicaciones de seguridad informática que contienen un crackeador de redes, captor de paquetes de red entre otros.
- Burp Suite Scanner: Plataforma útil para realizar auditoria y hallar vulnerabilidades de seguridad en las aplicaciones Web.
- Fern Wifi Cracker: Herramienta para realizar escaneos en la red en busca de vulnerabilidades
- GNU MAC Changer: Herramienta que facilita la modificación y manipulación de las direcciones MAC en las interfaces de la RED de la empresa con el fin de proteger la privacidad del sistema.
- Wireshark: Herramienta que podemos utilizar para el análisis de la red.[8]

1.4.3 Diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos

Para poder argumentar la anterior interrogante debemos entender el objetivo que tiene cada equipo, un CSIRT se encarga de la optimización de tiempo para restaurar los servicios, en la mejor productividad creando bases de conocimiento y que pueda estar disponible para cualquier cliente que enfrente los mismos incidentes o vulnerabilidades. Para la ejecución de un CSIRT el equipo de trabajo debe estar lo suficientemente preparado con el fin de atender situaciones críticas que se puedan presentar, para que puedan realizar acciones preventivas y actuar de la forma más rápida. [9]

Los CSIRT son temas de tendencia junto con la ciberseguridad el cual influye gran importancia para las organizaciones que se cada vez demuestran más interés en temas de Seguridad ya que toman más conciencia en los grandes riesgos a los que se deben enfrentar una vez tengan su negocio interconectado. BlueTeams es un equipo también conformado por profesionales en Ciberseguridad en donde su función es defender las organizaciones de ataques, a diferencia del concepto anterior este equipo únicamente actúa de forma defensiva, realizando monitoreo constante y trabajando en la mejora continua. Su función se cumple en la medida que identifican vulnerabilidades y son expuestas, se caracterizan principalmente por detectar las vulnerabilidades con eficiencia y eficacia y estudiar a los atacantes junto con su comportamiento.[10]

---

[8] RedTeam Security. (2022). Retrieved October 1, 2022, {Sitio Web } {Disponible en:} Redteamsecure.com website: https://www.redteamsecure.com

9 Red Team vs Blue Team Penetration Testing — CyberSecurity Services. (2022)., {Sitio Web } (27/09/2022) {Disponible en:} https://www.emagined.com/red-team-and-blue-team

[10] Red Team y Blue Team - Funciones y Diferencias en Ciberseguridad. {Sitio Web } (27/09/2022) {Disponible en:} https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

1.4.4 CIS “Center For Internet Security”

Los Controles de Seguridad Críticos de CIS (Controles de CIS) son un conjunto priorizado de Salvaguardas para mitigar los ataques cibernéticos más frecuentes contra sistemas y redes. Están mapeados y referenciados por múltiples marcos legales, regulatorios y de políticas[11]
Una vez entendido lo anterior podemos definir que CIS es un conjunto de mejores practicas en Seguridad Cibernetica, para lo cual seria un gran aliado para el equipo de Blueteams, esto con el fin de alcanzar los objetivos propuestos con mayor claridad, permitiendo realizar los análisis y auditorias de forma mas útil siguiendo los lineamientos legales, estas practicas puede enfocar el equipo en seguir una línea mas efectiva para mejorar la defensa de la organización. [12]

1.4.5 Sistema SIEM

La información sobre seguridad y gestión de eventos o SIEM (Security Information and Event Management) es un sistema de seguridad que persigue proporcionar a las empresas una respuesta rápida y precisa para detectar y responder ante cualquier amenaza sobre sus sistemas informáticos.[13]

Su función principal es la de lograr la recopilación de información y la detección eventos sospechosos en tiempo real mediante el monitoreo, gracias a esto su acción es inmediata permitiendo minimizar los riesgos.

Características que podemos encontrar en un SIEM:

- ✓ Identificación de amenazas
- ✓ Diferencia entre falsos positivos y falsos negativos
- ✓ Monitoreo constante de amenazas potenciales
- ✓ Trabajo en tiempo real
- ✓ Documenta incidentes de seguridad
- ✓ Cumplimiento de las normas vigentes

---

[11] CIS Controls Version 8. (2022, Febrero 4) {Sitio Web} (27/09/2022) {Disponible en:} https://www.cisecurity.org/controls/v8

[12] CIS Controls Version 8. (2022, Febrero 4) {Sitio Web} (27/09/2022) {Disponible en:} https://www.cisecurity.org/controls/v8

[13] TEAM, A. (2021). ¿Qué significa SIEM y cómo funciona? {en línea} (27/09/2022) {Disponible en:} https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

1.4.6 herramientas de contención de ataques informáticos

Firewall: Un firewall es una herramienta que resulta bastante importante y útil en una empresa puesto que nos ayuda a filtrar todo el tráfico de red que entra y también que sale evitando así la intrusión de amenazas y la detección de intrusos, se administra por medio de políticas que permitan el tráfico ya que la función principal de un firewall es denegar todo. También una de las funciones importantes es la de centralizar, integra y automatizar las redes a través de su software, siendo así más fácil de monitorear.[14]

Antivirus: Por políticas de seguridad la implementación de antivirus en los equipos y dispositivos es de suma importancia ya que esto nos permite contener cualquier amenaza que quiera afectar un equipo por medio de la ejecución de programas no autorizados, se debe de tener siempre actualizado ya que su sincronización con las bases de datos permitirá tener al día un filtro de las ultimas amenazas que afectan las redes.

Filtrado Email: Un filtro email nos permitirá bloquear o Dropear todos aquellos correos que contengan archivos maliciosos como phishing y spam, los cuales pueden afectar la integridad de los dispositivos y las cuentas en una organización, en el mercado existen una gran variedad de soluciones las cuales brindan esta protección, entre ellas podemos mencionar a Forcepoint o el ESA de Cisco. [15]

Filtrado Web: Un filtro Web lo podemos utilizar para el filtro de la navegación de los usuarios en una organización en una empresa, con el fin de evitar que naveguen a sitios altamente peligrosos en donde se descarga archivos maliciosos que puedan afectar la red, en el mercado podemos encontrar herramientas que prestan este servicio como lo es el módulo de protección Web de Forcepoint o el URL filtering de paloalto. [16]

---

[14] Reimagine the Firewall. (2022, August). Retrieved October 02, 2022, {Sitio Web} {Disponible en:}: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

[15] Kastner, E. (2021). What Is Email Filtering and How Does It Work? Retrieved October 03, 2022, {Sitio Web} (27/09/2022) {Disponible en:}: https://www.soscanhelp.com/blog/what-is-email-spam-filtering-and-how-does-it-work

[16] Arista. (2016, January 21). Web Filter | Edge Threat Management - Arista. Retrieved October 05, 2022{Sitio Web} {Disponible en:}: https://www.untangle.com/shop/web-filter/

CONCLUSIONES

Cada vez se necesita que todo tramite se pueda realizar de forma más ágil y sencilla, todo mediante el uso de internet, lo cual nos lleva a que nuestra información sea cada vez mas vulnerable a cualquier tipo de divulgación o ataque.

Esto obliga a que las grandes empresas tengan que invertir en desarrollo tecnológico ya sea para desarrollar aplicaciones, bases de datos y servicios web los cuales son consultados por los usuarios.

Los ciberdelincuentes ven esto como grandes oportunidades para cometer cualquier tipo violación a la información.

En virtud a lo anterior es importante que las empresas inviertan en recursos tecnológicos en donde se logre cerrar brechas de seguridad que permitan a cualquier intruso lograr vulnerar los sistemas y poder afectar los objetivos o el modelo de negocio de cualquier compañía.

Lo realizado en el presente documento, nos deja como conclusión importante que la realización de pruebas de pentesting son de gran ayuda para poder definir y encontrar aquellas vulnerabilidades que pueda tener una infraestructura en cualquier entidad, de igual formar el poder contrarrestar estos ataques desde el informe técnico que brinda dichas pruebas, nos ayuda a fortalecer y cerrar esas brechas que podamos evidenciar y así poder evitar futuros complicaciones.

RECOMENDACIONES

El área de seguridad informática puede emplear diversos factores los cuales pueden incluir la seguridad de la información y de la infraestructura, es una responsabilidad ante cualquier entidad establecer mecanismos que protejan lo anteriormente mencionado, un profesional en esta rama debe:

Tener claro la normatividad vigente y la legislación en cuanto a la ciberseguridad, estar en constante actualización sobre los cambios en los estándares que se derivan a nivel nacional e internacional.

Entender cualquier tipo de situación que involucre los servicios que pueda prestar como profesional en el ambiente de seguridad informática

Preparar escenarios controlados los cuales permiten realizar laboratorios de penetración con el fin de buscar posibles vulnerabilidades en la infraestructura tecnológica.

Documentar toda acción, procedimiento y política que se implemente con el fin de salva guardar la información de cualquier empresa, esto con el fin de garantizar el profesionalismo a resaltar en cada situación que realice.

LINK DEL VIDEO DE SUSTENTACION

https://youtu.be/GPG1rm7YWIs

PANTALLAZO DEL NIVEL DE AUTENTICIDAD

BIBLIOGRAFÍA

Semana. (2015, enero 24). El informe que sacudió el caso de la fachada Andrómeda. {Sitio Web} (02/09/2022) Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

José Luis Peñarredonda. (2015, December 9). Detrás de Buggly: la historia de la fachada Andrómeda • ENTER.CO. {Sitio Web} (02/09/2022) Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Kali Linux: ¿qué es Linux para hackers?. (2022). {Sitio Web} (19/09/2022) {Disponible en: }https://www.ionos.es/digitalguide/servidores/configuracion/kali-linux/

Metasploit: ¿qué es y cómo usarlo? (2018). {Sitio Web} (19/09/2022) {Disponible en:} https://www.funinformatique.com/es/que-es-metasploit-y-como-usarlo-bien/

IMF Smart Education. (2019, Agosto 12). ¿En qué consiste el trabajo de un pentester? • IMF. {Sitio Web} (25/08/2022) {Disponible en:} https://blogs.imf-formacion.com/blog/tecnologia/en-que-consiste-el-trabajo-de-un-pentester-201908/

Abrie, A. (2022). Nmap: Análisis de puertos y monitorización de redes - ICM., {en línea} (19/09/2022) {Disponible en:} https://www.icm.es/2022/05/06/nmap-analisis-de-puertos-y-monitorizacion-de-redes/

¿Qué es EternalBlue y por qué el exploit MS17-010 sigue siendo relevante? (2022). {Sitio Web} (19/09/2022) {Disponible en:} https://www.avast.com/es-es/c-eternalblue

CIS Controls Version 8. (2022, Febrero 4) {Sitio Web} (27/09/2022) {Disponible en:} https://www.cisecurity.org/controls/v8

TEAM, A. (2021). ¿Qué significa SIEM y cómo funciona? {Sitio Web} (27/09/2022) {Disponible en:} https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

Red Team y Blue Team - Funciones y Diferencias en Ciberseguridad. {en línea} (27/09/2022) {Disponible en:} https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

CIS Controls Version 8. (2022, February 4). 2022, obtenido de: https://www.cisecurity.org/controls/v8

Reimagine the Firewall. (2022, August). Retrieved October 02, 2022, {Sitio Web} (27/09/2022) {Disponible en:}: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Johnson, L. (2020). Security component fundamentals for assessment. Security Controls Evaluation, Testing, and Assessment Handbook {Sitio Web } ({Disponible en}. https://doi.org/10.1016/b978-0-12-818427-1.00011-2

Red Team vs Blue Team Penetration Testing — CyberSecurity Services. (2022)., {Sitio Web } (27/09/2022) {Disponible en:} https://www.emagined.com/red-team-and-blue-team

RedTeam Security. (2022). Retrieved October 1, 2022, {Sitio Web } {Disponible en:} Redteamsecure.com website: https://www.redteamsecure.com