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

JAMER JOSÉ ZARATE VERGARA

UNAD

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ECBTI

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA ELECTRÓNICA

BOGOTA - COLOMBIA

2021

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

JAMER JOSÉ ZARATE VERGARA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

ASESOR: JOHN FREDDY QUINTERO TAMAYO

UNAD

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ECBTI

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA ELECTRÓNICA

BOGOTA - COLOMBIA

2021

AGRADECIMIENTOS

Primeramente, nos permitimos agradecer a Dios por permitirno tener vida y salud para desarrollar esta especializacion, a nuestras familias quienes nos brindaron el apoyo y acompañamiento en el trascurso de este proceso educativo, lo cual fue de gran importancia y motivación para realizar de la mejor manera esta etapa de fortalecimiento académico y profesional.

En segunda instancia nos permitimos manifestarle nuestro agradecimiento a la Universidad Nacional Abierta y a Distancia junto con su personal administrativo y cuerpo de docentes, los cuales contribuyeron con sus conocimientos y compromiso a lo largo de nuestra formación académica.

En tercera instancia le manifestamos nuestros agradecimientos al ingeniero John Freddy Quintero Tamayo por brindarnos su apoyo, haciendo uso de sus conocimientos, experiencia y demás cualidades, las cuales fueron de bastante apoyo para el desarrollo de este estudio de viabilidad.

NOTA DE ACEPTACION

_____
_____
_____
_____
_____

_____

Primer jurado.

_____

Segundo jurado.

OBSERVACIONES

INDICE

GLOSARIO

Vulnerabilidad: Es el riesgo que puede sufrir un sistema ante un peligro inminente.

Exploit: Un error en el software que representa una brecha de seguridad.

Antivirus: Software utilizado para eliminar programas elaborados con intención destructiva.

Kali Linux: Es una distribución orientada a la seguridad informática, por lo que con ella podrás ejecutar todo tipo de herramientas con las que poner a prueba la seguridad de tus sistemas y redes.

Sistema Operativo (OS): Es el conjunto de programas responsables de la conexión entre los recursos materiales de un ordenador y las aplicaciones informáticas del usuario.

CIS SECURITY: “Center for Internet Security” 1.

Blue Team: son equipos multidisciplinares de expertos en ciberseguridad especializados en analizar el comportamiento de los sistemas de una empresa y estudiar cómo se comportan sus usuarios y equipos para poner al descubierto de forma rápida cualquier incidente que pueda haber pasado inadvertido para el resto de los sistemas de seguridad.

Red Team: Es un grupo independiente que ayuda a una organización a mejorarse a sí misma al oponerse al punto de vista de la organización a la que están ayudando. Por medio de la realización de ataques a un objetivo, se estudian sus debilidades.

Malware: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información.

Parche: Programa que se encarga de hacer cambios en busca de la corrección de vulnerabilidades de seguridad.

Virus: Programa diseñado para que, al ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo.

MDCMAGAZINE: “6 formas de prevenir un ataque cibernético” 2.

Autenticación: El procedimiento de verificar la identidad que reclama un sujeto mediante una validación en un sistema de control de acceso**.**

Dirección IP: Es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en la red de un dispositivo que utilice el protocolo o, que corresponde al nivel de red del modelo TCP/IP.

VirtualBox: Oracle VM VirtualBox es un software de virtualización para arquitecturas x86/amd64. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización.

Criptografía: Es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado.

Confidencialidad: Previene del uso no autorizado o revelación de información, asegurándose que la información es accesible únicamente para aquellos que tengan autorizado su uso.

CCN CERT: “Guía de seguridad de las TIC” 3.

DDos: Es un tipo de ataque en el que el atacante inicia ataques de negación de servicio simultáneamente desde muchos sistemas.

Firewall: Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios.

Delito informático: Los delitos informáticos son aquellas acciones u omisiones realizadas a través de medios informáticos y que son penados por la Ley.

Hacking: Es la aplicación de tecnología o conocimientos técnicos para superar alguna clase de problema u obstáculo.

Pentesting: O test de penetración consiste en atacar un sistema informático para identificar fallos, vulnerabilidades y demás errores de seguridad existentes, para así poder prevenir los ataques externos.

Hacker: Es alguien que descubre las vulnerabilidades de una computadora o un sistema de comunicación e información.

RESUMEN

La tecnología va de la mano con los acontecimientos en la industria, ciencia, educación entre otros. Esto ha llevado a que las aplicaciones permiten la simplificación de los procesos, pero esto lleva un riesgo a que los datos personales o de proceso sea afectado y la seguridad quede en duda generando la duda de las aplicaciones creadas.

Los sistemas de información presentan riegos en las sesiones de los usuarios donde los delincuentes cibernéticos se aprovechan de este para suplantar y realizar gestiones que el usuario registrado no hace, ocasionando pérdida de información confidencial de las organizaciones públicas y/o privadas en donde se presentan denuncias de robo de información.

La ciberseguridad es la buena práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. La seguridad de la información protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito.

En los últimos años la seguridad de las redes computacionales han sido el blanco preferido de hackers y de los ataques de seguridad en el medio informático.

La información que viaja cada día por este medio representa un valor más alto y es conveniente darle prioridad para conocer y prevenir las vulnerabilidades de estos medios de acceso y de manejo de la información y darle un ambiente seguro para su tratamiento.

De lo expresado anteriormente surge la necesidad de lograr que las empresas conozcan que la ventaja de instalar aplicaciones en los servidores de red, radican en el mejoramiento de los diferentes procesos, pero de igual manera son esta empresa debe implementar políticas de seguridad necesarias que garanticen el cuidado de la información, la confiabilidad del cliente y la sostenibilidad de la empresa al momento de manipular los datos sensibles de cada uno de los usuarios que de una u otra manera han confiado en el servicio que se está ofertando.

Consecuentemente, muchas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones con el objeto de obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas. Esto puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

INTRODUCCIÓN

Este informe técnico, describe detalladamente las vulnerabilidades asociadas al sistema en la cual se hizo explotación de dicha falla al igual que también se presentan conductas a tomar para corregir esta falla y no se vuelva a presentar otro ataque. El desarrollo de los contenidos está basado en los pasos para realizar y protegerse de un pentesting, las herramientas de uso para realizar y contener ataques informáticos y aprendizaje de nuevos conocimientos de seguridad informática. Además, el trabajo contiene la realización de una aplicación práctica en un entorno de pruebas suministrado para su ejecución.

JUSTIFICACIÓN

Ante la evidente problemática que se presenta con gran impacto en todo el mundo y ahora mas por la emergencia sanitaria que afecta al planeta, se han evidenciado ahora con mas frecuencia ataques informaticos de todo tipo, troyano, ingenieria social, phishing, rasomware entre otros.

Estos tipos de amenazas afectan el desarrollo comercial y personal de las personas y empresas que cada dias estan mas en riego de sufrir un atque informatico, directamente afectada los datos e informacion que se manipula lo cual constituye el activo mas importante, por lo cual el desarrollo de este trabajo permite tener un conocimiento mas amplio, de esta manera tener el pensamiento de un ciber delicuente para asi protegerse y evitar una vulnerabilidad al sistemas de informacion, hardware y software.

OBJETIVOS

Objetivo General

- Desarrollar competencias para planificar estrategias basadas en metodologías de ciberseguridad defensivas y ofensivas, que permitan hacer frente a un evento o incidente informático en una infraestructura TI, teniendo presente el cumplimiento de normas éticas y legales con el fin de mejorar el esquema de ciberseguridad de una organización.

Objetivos Especificos

- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.
- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.
- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.
- Presentar informes técnicos de pruebas de pentesting y medidas de contención de ataques informáticos.

MARCO TEORICO

Antecedentes

La Seguridad Informática ha experimentado un profundo cambio en los últimos años. Inversiones aisladas llevadas a cabo con el objetivo de fortalecer la seguridad en puntos muy concretos han dado paso a inversiones para asegurar el bien más valioso de la empresa, la información, enfocando la seguridad hacia los procesos de negocio de la empresa.

OPENIT: “¿Que es el hardening de sistemas operativos?” 4.

- Microsoft y la suspensión del soporte para Windows 7

  El 2019 fue un año que comenzó con el anuncio por parte de Microsoft de que el 14 de enero del 2020 dejará de lanzar actualizaciones de seguridad y de dar soporte gratuito para el sistema operativo Windows 7. La dificultad de concientizar a las personas de que había llegado la hora de actualizar al nuevo sistema operativo.

MINTIC: “Seguridad y privacidad de la información” 5.

- Vulnerabilidad en WinRAR

  En el segundo mes del año se conoció la noticia sobre el hallazgo de una vulnerabilidad crítica en todas las versiones de un popular software como WinRAR. Si bien la compañía detrás de este programa para comprimir archivos lanzó una actualización que solucionaba el fallo, al poco tiempo de conocerse el fallo comenzaron a detectarse campañas que intentaban aprovecharse de este error en equipos que no hubieran actualizado para distribuir desde un backdoor hasta un ransomware. Incluso en foros comenzaron a ofrecerse herramientas para crear archivos RAR maliciosos. Entre las campañas que se aprovecharon de este fallo, investigadores de ESET descubrieron una campaña dirigida a departamentos financieros en los Balcanes (que distribuía un backdoor y un RAT) que explotaba este fallo en WinRAR para comprometer los equipos de sus víctimas.

IT DIGITAL SECURITY: “¿Qué es un blue team y como trabaja?” 6.

- Ransomware dirigido: una tendencia que se confirmó
  Continuando con el tema del ransomware, algo que se consolidó este año fue la tendencia de los ataques de ransomware dirigidos, algo que los especialistas de ESET predijeron en Tendencias 2019. Entre los varios ataques de ransomware dirigidos que se vieron este año, se destaca el que afectó a 23 agencias gubernamentales en Texas, los que impactaron tanto a Cadena SER, la consultora Everis y Prosegur en España, y el ataque dirigido a la petrolera estatal mexicana Pemex.

INCIBE: “Auditando la seguridad de tus sistemas” 7.

- Problemas para Facebook
  La red social estuvo envuelta en varios temas relacionados a la seguridad en 2019. Uno de los hechos más importante fue el que estuvo relacionado con el bloqueo de su VPN, “Facebook research”, por violar las políticas de Apple al hacer uso de certificados emitidos por la compañía de la manzana para realizar acciones que van en contra de la política de la compañía. Facebook research había sido utilizada por la compañía de Zuckerberg para recolectar datos de los teléfonos que la utilizaran. Poco después del incidente con Apple, Facebook eliminó la aplicación de Google Play.

- Ciber espionaje en América Latina
  Otra de las investigaciones más importantes de este año tuvo que ver con el descubrimiento de la reciente actividad de una nueva versión del programa maligno Machete, ya que se develó que los operadores detrás de esta amenaza continúan en actividad realizando tareas de espionaje contra organismos gubernamentales de Ecuador, Colombia, Nicaragua y Venezuela. Según los hallazgos de los investigadores de ESET, los ataques de Machete permitieron robar grandes cantidades de información y datos confidenciales.

CSIRT: “Equipos de repuesta frente a incidencias de seguridad informática” 8.

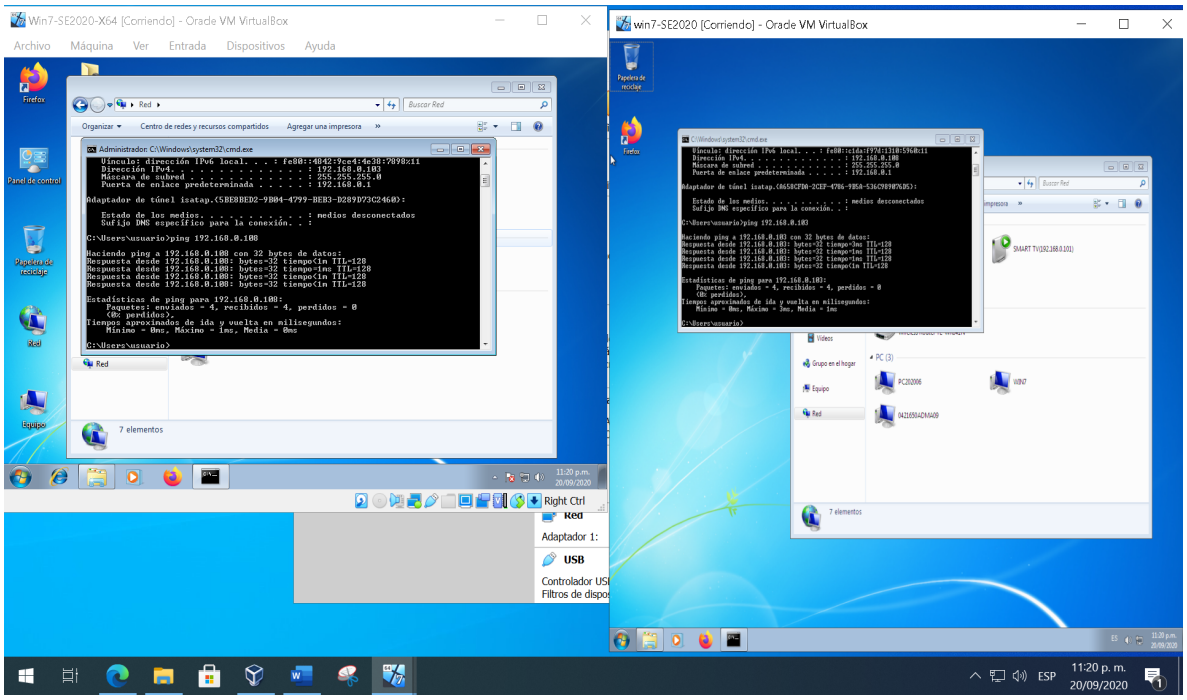
- Grupo de APT The Dukes continúa activo
  Uno de los hallazgos más relevantes de este año fue el descubrimiento de que el grupo de APT “The Dukes”, acusado de haberse infiltrado en el Comité Nacional Demócrata de EUA, continúa activo pese a haberse mantenido durante largo tiempo lejos de los radares de detección. Investigadores de ESET confirmaron que, lejos de haber detenido sus actividades, el grupo de cibercriminales ha estado activo comprometiendo blancos gubernamentales.

HACKNOID: “5 Herramientas de seguridad informática claves en empresas” 10.

Desarrollo de informe

Como primera acción perteneciente al grupo Red Team realizamos una prueba de instrucción a la estación de trabajo establecido por 2 equipos de cómputos con sistemas operativos Windows 7 64 y 32 bits, como lo muestra la siguiente imagen.

Imagen 1. Descripcion de los equipos de computo de la estacion de trabajo.



Fuente Elaboracion propia.

De acuerdo con los pasos clasificados para la realización del pestesting empezamos con el **paso 1 que es la recopilación de información y paso 2 búsqueda de vulnerabilidades.** Después de leer el anexo 4 escenario 3 se ha identificado varias fallas y problemas vulnerabilidad en el sistema, para continuar con las etapas de recopilación de información y búsqueda de vulnerabilidades utilizaremos la herramienta **NMAP** ya que nos permite tener información de los equipos y vulnerabilidades del sistema.

Esta herramienta nos permite obtener información del sistema muy específica e importante ya que nos da un ingreso a vulnerar el sistema.

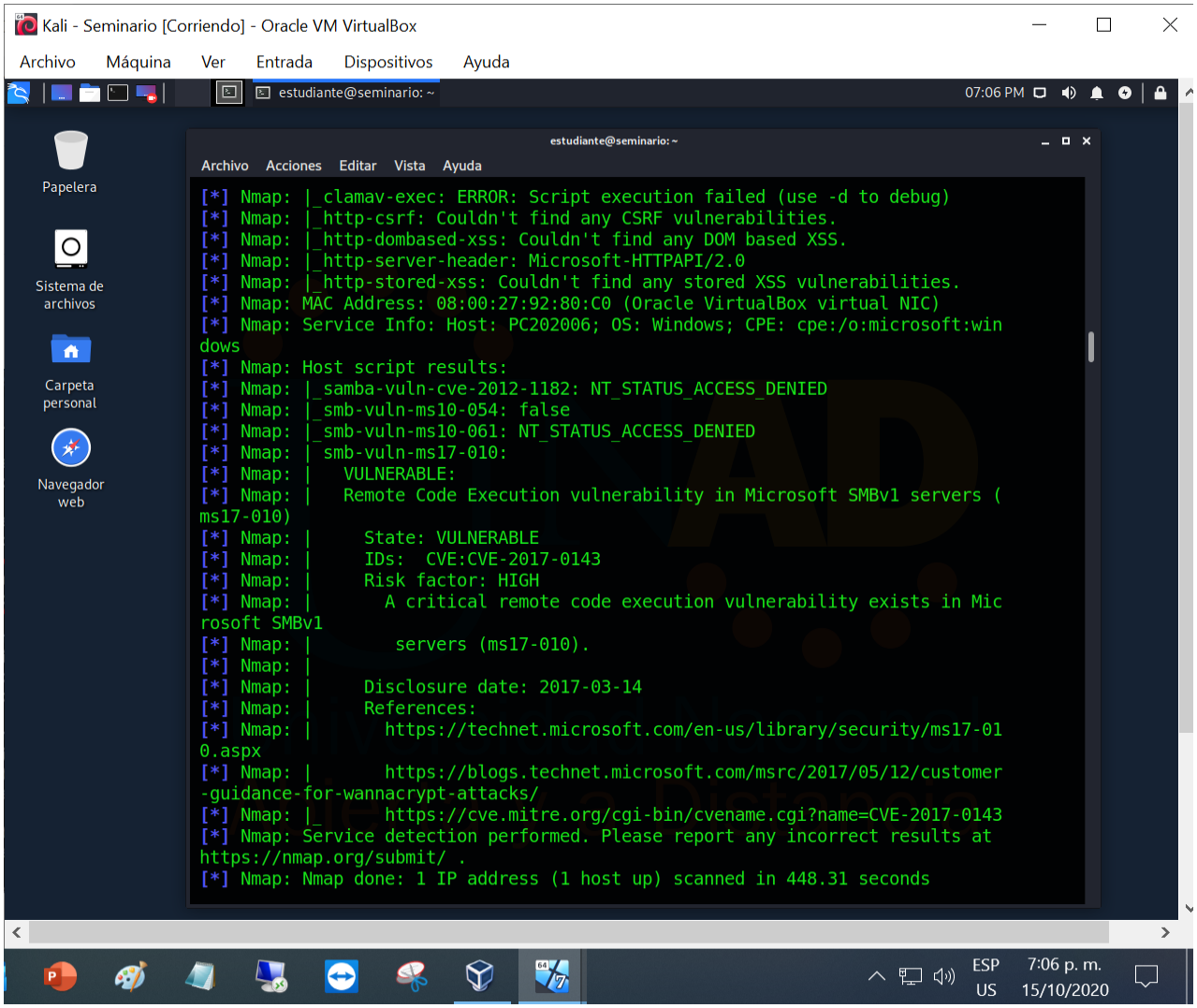
Abrimos la herramienta Nmap y ejecutamos el comando **nmap 192.168.0.0/24** para que nos realice un escaneo de la red de los equipos conectado y de esta forma obtener información de todos los equipos conectados a la red.

La información que nos muestra esta herramienta son los puertos que tienen abiertos cada equipo y al igual que su sistema operativo.

Este reporte generado es de gran importancia porque nos permite conocer las entradas al sistema es decir conociendo esta información podemos identificar la forma de como vulnerar el equipo y atacarlo.

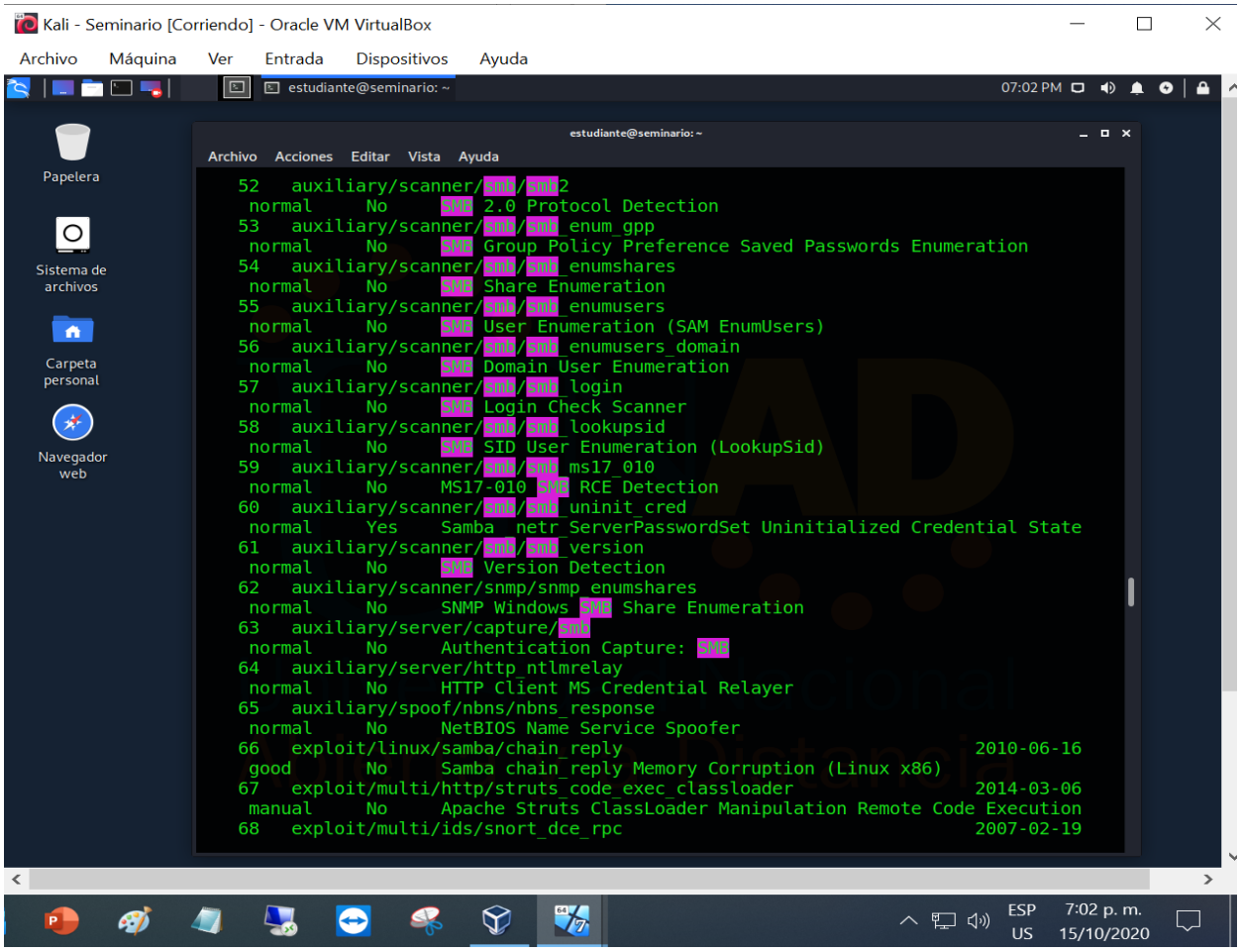
A continuación, podemos visualizar el reporte generado por la herramienta Nmap en Kali Linux.

Imagen 2. Reporte de escaneo de posibles vulnerabilidades al sistema con Nmap.



Fuente Elaboracion propia.

Imagen 3. Vulnerabilidades existente en el sistema listas para explotar.



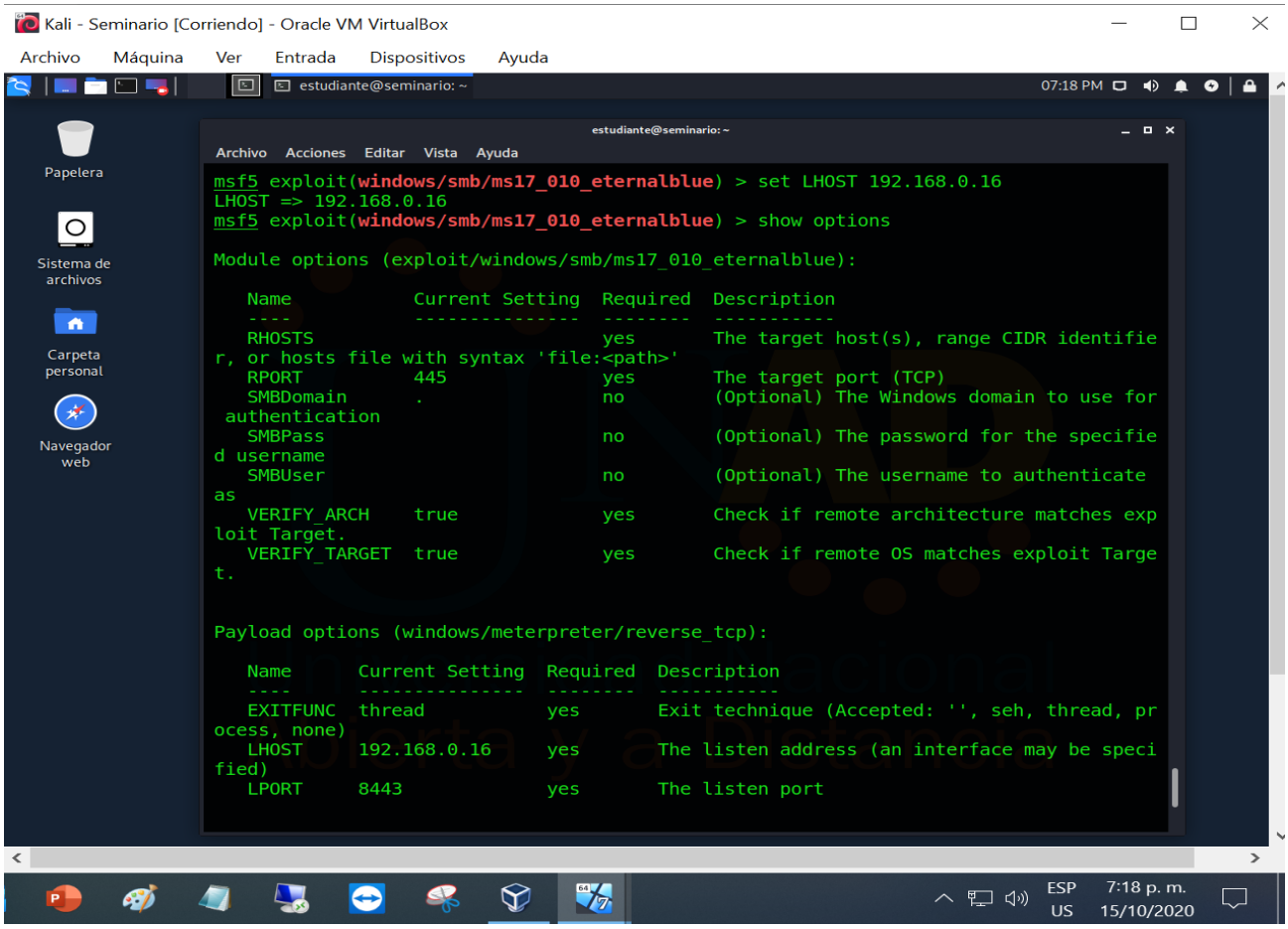
Fuente. Elaboracion propia.

COBDC: “Todos los sistemas informáticos tienes vulnerabilidades” 12.

Los datos de los equipos de la empresa con sistema operativo Windows 7 tienen la IP 192.168.0.16 y 192.168.0.17. Conociendo estas fallas avanzamos a la **etapa 3 que es la de explotación de vulnerabilidades,** en la imagen siguiente imagen se vera el proceso de ejecución.

MORENO, PATRICIO: “Técnicas de detención de ataques informáticos” 14.

Imagen 4. Ejecucion de vulnerabilidad realizada en Metaexploit.

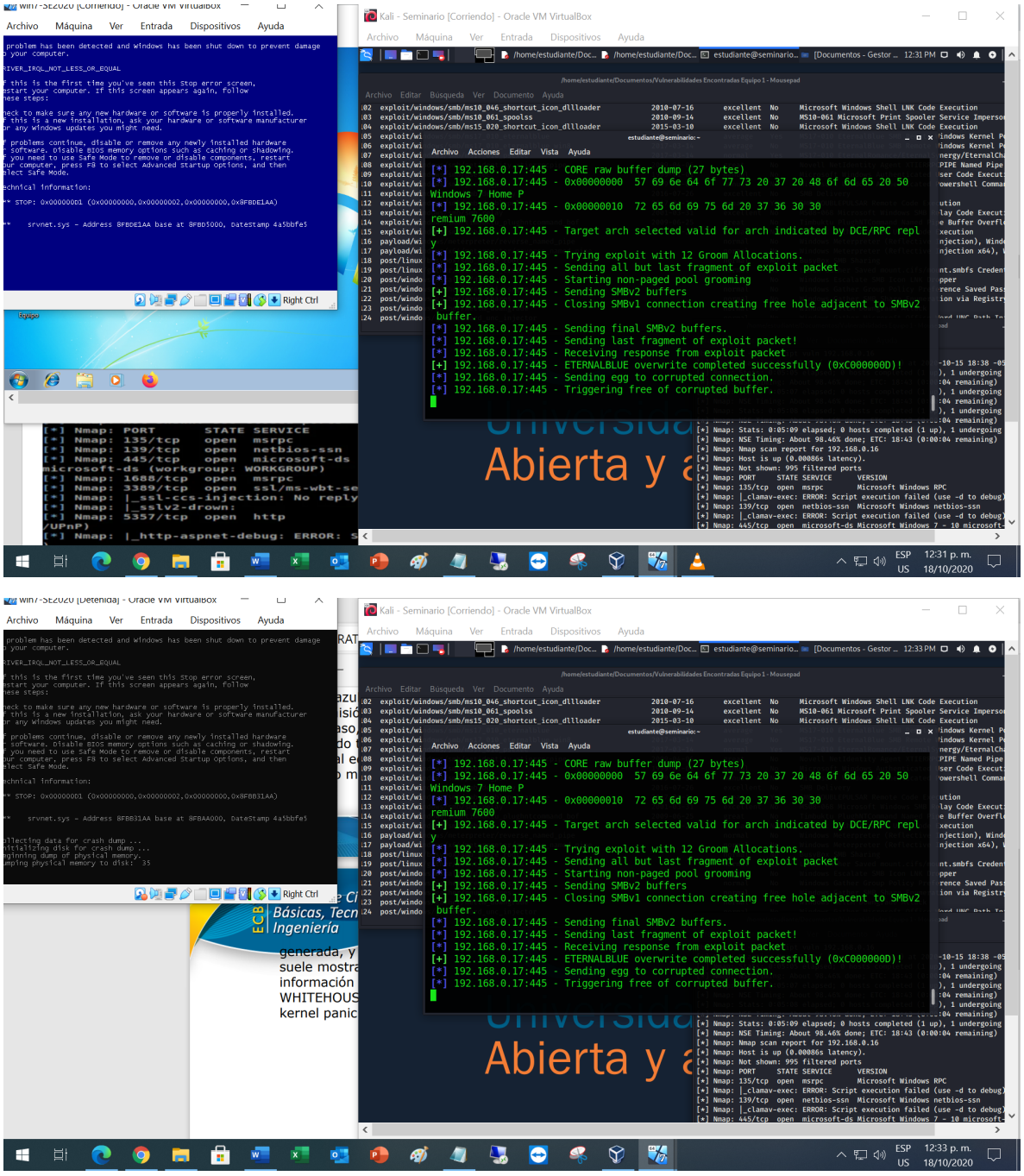


Fuente Elaboracion propia.

CISCO: “¿What is cybersecurity?” 15.

En la siguiente imagen se muestra la vulenrabilidad explotada al equipo con IP 192.168.0.17, el cual es el equipo que presenta el fallo de seguridad

Imagen 5. Vulnerabilidad explotada satisfactoriamente en el sistema. Fuente.



Elaboracion propia.

Después de encontrar este fallo de seguridad perteneciente al grupo Red Team procedemos a buscar soluciones a esta vulnerabilidad como miembro del grupo Blue Team.

Teniendo en cuenta en el ataque realizado en la cual se encontró el fallo de seguridad en los sistemas operativos se presenta a continuación la medida de contención para evitar posibles ataques informáticos.

- Como primera medida a implementar para evitar que se repita el ataque es actualizar el sistema operativo ya que el sistema presente se encuentra obsoleto con muchas fallas de seguridad.
- Como segunda media se instalaría un antivirus en los equipos para estén más seguros monitoreando posibles archivos o datos maliciosos.
- Como tercera media esta siempre actualizando el sistema operativo instalando los parches de seguridad para así evitar que las vulnerabilidades sean explotadas.
- Como cuarta medida siempre estar realizado backup de la información, es lo más recomendable tener siempre un respaldo de los datos para en caso de un ataque critico no se vean afectados de gravedad nuestros archivos.

Es primordial y no debe falta como medidas de contención estas acciones y herramientas de gran importación en nuestro sistema y se define a continuación.

RAPID SEVEN: “Vulnerability & Exploit Database” 16.

Antivirus: es una aplicación o un conjunto de programas que detectan y eliminan virus de ordenadores y redes. Los virus informáticos son una amenaza constante en todas las plataformas, el software antivirus actuales están diseñados para ofrecer protección en todos los sistemas operativos y a todos los dispositivos conectados a la red de internet.

Firewall: también conocido como cortafuegos, es un elemento informático que trata de bloquear el acceso, a una red privada conectada a Internet, a usuarios no autorizados. El funcionamiento de un firewall es muy importante, ya que, de no ser por él, un ordenador o red de ordenadores podría ser atacado e infectado con bastante frecuencia ya que neutraliza los ingresos no deseados.

Actualización del sistema e instalación de parches de seguridad: Mantener siempre actualizado el sistema es una forma de contrarrestar el ataque de cualquier intruso ya que les cerramos las puertas a su ingreso actualizando las vulnerabilidades existentes en el sistema. Lo mismo sucede al instalar el parche de seguridad cuando el inquilino explota una vulnerabilidad, el parche instalado bloquea el ingreso progresivo del atacante de esta manera contrarresta su ataque.

AVAST: “What Is Eternal Blue and Why Is the MS17-010 Exploit Still Relevant?” 17.

CONCLUSIONES

Tras la finalización de este seminario, se han logrado todos los objetivos propuestos. Por un lado, se ha realizado una labor de investigación sobre la mayoría de los aspectos que rodean una prueba de penetración y como protegerse. Como resultado de esta investigación, se ha obtenido un aprendizaje profesional y aplicativo para el desarrollo de la actividad.

- Se analiza la importancia de los equipos de Red y Blue Team, de esta manera se hace mas segura la organización en constante actualizacion a cualquier evento de seguridad.
- Se ha adecuado un entorno teorico practico para el desarrollo y ejecucion de pruebas de seguridad en informatica en la cual se evidencia vulnerabilidades en el sistema, aprendiendo a identificar y conocer los distintos ataques y amenazas existentes.
- Se implementa un plan de contingencia basado en las pruebas de pentesnting realizadas para asi contener, evitar y contrarrestar ataques y vulnerabilidades en el sistema.
- Se realiza un registro detallado de todas las pruebas, actividades y acciones ejecutadas en el desarrollo de cada una de las pruebas de penetracion realizadas, de igual forma se dan a conocer las correcciones y mejoras para mantener la organización mas segura y confiable.

RECOMENDACIONES

Para tener un sistema estable con medidas de seguridad de ataques informático-óptimos se recomienda implementas las siguientes recomendaciones:

- Todo sistema es susceptible de ser atacado, por lo que conviene prevenir esos ataques.
- Conectarse a la red desde una red privada y segura.
- Conocer las técnicas de ataque ayuda a defenderse más eficientemente.
- Elegir SOs con poco énfasis en la seguridad, puede suponer un auténtico infierno.
- Utilizar antivirus y herramientas de contención de ataques.
- La seguridad basada en la ocultación no existe.
- Mantener siempre los equipos organizados.
- Tras realizar el trabajo propuesto, deberías ser capaz de: Reconocer la importancia de la seguridad en la informática.
- Utilizar contraseñas seguras.
- Reconocer amenazas e identificar atacantes.
- Instalar programas oficiales, seguros y de fuentes confiables.
- Utilizar el vocabulario básico sobre "malware".
- Controlar acceso a la red o a dominio de sistema.
- Saber qué medidas son las oportunas para prevenir ataques.
- Tener paciencia y sentido común.
- Reconocer la importancia de las copias de seguridad y saber planificarlas.
- Controlar el acceso a la red de los dispositivos móviles.

SEARCHDATACENTER (CSIRT): “MS17-010 Eternal Blue SMB Remote Windows” 18.

BIBLIOGRAFÍA

- 1 CIS SECURITY. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/.
- 2 MCD MAGAZINE, (2020). 6 formas de prevenir un ataque cibernético. https://mdcmagazine.com/articulos/planners-tips/digital-tools/6formasde-prevenir-un-ataque-cibernetico.
- 3 CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29) https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html.
- 4 OPENIT, (2020). ¿Qué es el hardening de sistemas operativos?. https://www.openit.com.ar/que-es-el-hardening-de-sistemas-operativos/.
- 5 MINTIC, (2018). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información, (p.14 - 27) https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf.
- 6 IT DIGITAL SECURITY, (2018). ¿Qué es un Blue Team y cómo trabaja? https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja.
- 7 INCIBE. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas.
- 8 SEARCH DATA CENTER (CSIRT), (2019). Equipo de Respuesta frente a Incidencias de Seguridad Informática. https://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT.
- 9 MINTIC, (2018). Guía de aseguramiento del Protocolo IPv6. (pp. 21-35) https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf.
- 10 HACKNOID, (2019) 5 herramientas de seguridad informática claves en empresas. https://hacknoid.com/hacknoid/5-herramientas-de-seguridad-informatica-claves-en-empresas/.
- 11 MINTIC, (2018). Guía de Auditoria. Mintic. (pp. 12-19) https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf.
- 12 COBDC, (2019) Vulnerabilidades: actualizar el software para corregir los agujeros de seguridad. http://www.cobdc.net/programarilliure/vulnerabilidades-seguridad/.
- 13 MINTIC, (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57) https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf.

- 14 Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63) http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf
- 15 CISCO, (2020) What Is Cybersecurity? https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.
- 16 RAPID SEVEN, (2019). Vulnerability & Exploit Database. https://www.rapid7.com/db/?type=metasploit.
- 17 AVAST, (2018). What Is Eternal Blue and Why Is the MS17-010 Exploit Still Relevant? https://www.avast.com/c-eternalblue.
- 18 SEARCHDATACENTER (CSIRT), (2019). MS17-010 Eternal Blue SMB Remote Windows. https://www.csirt-epn.edu.ec/servicios/vulnerabilidades/58-ms17-010.