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

JOSE RAFAEL NIÑO ORDOÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, SEMINARIO ESPECIALIZADO
PROGRAMA ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
CEAD POPAYÁN
2020

RESUMEN

En el desarrollo de las actividades encomendadas por la empresa WHITEHOUSE SECURITY con el fin de llevar a cabo el reclutamiento de personal se desarrollaron actividades con el fin de analizar los siguientes puntos.

Instalación y configuracion del banco de trabajo suministrado por la empresa en un ambiente controlado con el fin de iniciar el análisis
Análisis de la OPERACIÓN ANDROMEDA BUGGLY y del contrato que tiene WHITEHOUSE SECURITY con el fin de verificar observar los aspectos éticos y legales que fueron violados tanto el caso Buggly como por el contrato que la empresa envía a para reclutar a su nuevo personal de seguridad
Análisis Red Team de la Fuga de información de la que fue objeto la empresa para lo cual se suministraron las imágenes de los sistemas operativos y el ambiente controlado en la fase 1 del banco de trabajo enviado por WHITEHOUSE SECURITY
Contención de ataques y Hardenizacion en esta fase se demostró cómo se evite el ataque que se presentó en las maquinas aplicando procesos sencillos como las actualizaciones respectivas de los sistemas operativos y la configuracion adecuada de la seguridad en los equipos de cómputo como la actualización y configuracion del antivirus, cerrar los diferentes puertos abiertos y la activación y configuracion de los cortafuegos de cada equipo.
Realización del informe técnico del proceso realizado con los equipos en una ambienté controlado con el fin de localizar la falla y el archivo que el atacante introdujo y ocasionó la perdida de la información.

TABLA DE CONTENIDO

Pág.

Listado de Imágenes.

Listado de Tablas

pág.

GLOSARIO

LEY: que establece los principios esenciales de una regulación, consagrada en el artículo 4 del código civil en Colombia.

INTERCEPTACIÓN: Acción y efecto de interceptar para este análisis se refiere a la interceptación de las comunicaciones y mensajes.

EXPLOIT. Es un programa o código que "explota" una vulnerabilidad del sistema.

NMAP: programa de código abierto que sirve para efectuar rastreo de puertos.

AUDITORIA: Revisión exhaustiva de todos los Procesos Realizados dentro de una entidad para verificar si se están cumpliendo.

FRAMEWORK: entorno o marco de trabajo. Es un conjunto de conceptos, de prácticas y criterios estandarizados a seguir.

HARDENIZACION: proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad.

INTRODUCCIÓN

En este trabajo se construirá el informe técnico de las situaciones planteadas por WHITEHOUSE SECURITY quien lo solicita como actividad final del trabajo planteado por la empresa durante el periodo de prueba con el fin de que el analista seniors de la empresa lo estudie para poder tomar una buena decisión al momento de realizar la vinculación del nuevo personal experto que requieren dentro de la organización.

OBJETIVOS

OBJETIVO GENERAL

Analizar y Describir que ley se infringió y Técnicamente por qué los atacantes lograron realizar la instrucción a la empresa, que fallas de seguridad había al interior de esta al momento de presentarse el ataque.

OBJETIVO ESPECIFICO

- Aspectos legales que fueron violados con la intrusión dentro Whitehouse Security.
- Reconocimiento de las características de las Maquinas.
- Análisis con NMAP de la red en busca de las direcciones IP de los Equipos y puestos abiertos.
- Escaneo de las vulnerabilidades de cada equipo y explotación con Metasploit framework.
- Explotación de las vulnerabilidades encontradas.

DESARROLLO DEL INFORME TECNICO.

Sesión uno: análisis de la parte legal y ética al realizar el análisis del caso se puede observar que en el Anexo 4 – Escenario 3 entregado por la empresa que se cometieron actos en contra de la LEY 1273 de 2009 en cuanto a los Artículos relacionados al acceso abusivo a un sistema Informático y el uso de Software malicioso

Artículo 269A[1]: Acceso abusivo a un sistema informático.

Artículo 269E[2]: Uso de software malicioso.

Luego de Realizar una revisión de las leyes y el código de ética del ingeniero que se infringieron tanto en el contrato que plantea Whitehouse Security en su Anexo 3 – Acuerdo como en el caso Andrómeda se procede a realizar el análisis en el ambiente simulado y controlado de las máquinas que sufrieron la intrusión que la empresa entrega y de las cuales se sospecha tienen un archivo el cual fue utilizado en la sustracción de la información tal como lo indica en su Anexo 4 – Escenario 3

Clausulas donde se viola el código de ética del ingeniero copnia en la cláusula cuarta donde textualmente dice:
CAPITULO 3
Dentro del copnia código de ética del profesional se establece en este capítulo que el profesional debe denunciar ente todas las actividades sospechosas de espionaje y la apropiación de información de terceros. Algo que muchos ingenieros por el dinero que les ofrecen omiten violando asi el código de ética

---

[1] Artículo 269A: *Acceso abusivo a un sistema informático*. <Ver Notas del Editor> El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

[2] Artículo 269E: *Uso de software malicioso*. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Sesión dos: análisis de características y vulnerabilidades de las máquinas entregadas:

Tabla 1 Equipo Win7

Equipo 1 Información de las Características de la Maquina software y hardware	
Nombre del Equipo	Win7
Sistema Operativo	Windows 7 Home Premium
Arquitectura del sistema	X86
Software Instalado	Mozilla , winrar ambos de 32 bits
Estado del Firewall de Windows	Desativado
Antivirus instalado	Windows defender
Estado del Antivirus	Fallo de la Actualización código 800b0109 fecha 23/06/2020
Actualizaciones del sistema	Agente de Windows update 7,6,76000,256 fecha 06/10/2020
Estado de Windows Update	Sin Activar
Recursos compartidos	Activo
Dirección IP	192.168.0.25
Tipo de Maquina	Virtualizada

Fuente: Propia de la actividad.

Se analiza el visor de eventos del dia 10/06/2020 debido a que la empresa informa que ese dia se presentó el incidente de la fuga de información

Tabla 2 Equipo PC202006

Equipo 2 Información de las Características de la Maquina software y hardware	
Nombre del Equipo	PC202006
Sistema Operativo	Windows 7 Profesional service pack 1
Arquitectura del sistema	X64
Software Instalado	No tiene Software instalado
Estado del Firewall de Windows	Desativado
Antivirus instalado	Windows defender
Estado del Antivirus	Sin Actualización
Actualizaciones del sistema	Actualización KB2534111 fecha 26/06/2020 Actualización KB976902 fecha 20/11/2010
Estado de Windows Update	Sin Activar
Recursos compartidos	Activo
Dirección IP	192.168.0.49
Tipo de Maquina	Virtualizada

Fuente: Propia de la actividad.

Sesión tres: uso de NMAP con el fin de realizar la búsqueda de las Direcciones IP desde la maquina kalilinux y de los puertos abiertos y su respectivo sistema operativo de las maquinas mencionadas en el Anexo 4 – Escenario 3 que nos facilitó la empresa.
con el fin de determinar cuál maquina fue la utilizada para sustraer la información a la empresa para lo cual se aplicarán las 5 fases del análisis forense de acuerdo al anexo 4 escenario 3 que nos brinda la empresa podemos hacer un análisis y saber que fallas de seguridad tenían los equipos, las cuales posiblemente fueron utilizadas para llevar a cabo la instrucción con este análisis se determinara cual fue la maquina atacada y se realizar un análisis del porque una de las maquinas presenta problemas de pantalla azul mensaje del Kernel panic.

Herramientas software utilizadas.
NMAP: herramienta la cual fue utilizada para obtener las direcciones IP de los equipos al realizar el mapeo de la red
Fases del Trabajo.

Fase 1: Reconocimiento Pasivo y Activo
Herramienta software utilizada en esta fase se trata virtual box herramienta que nos permite montar las diferentes maquinas suministradas por la empresa WHITEHOUSE SECURITY en un ambiente controlado para realizar las pruebas necesarias con el fin de lograr cumplir los requerimientos realizados por la empresa.

Fase 2: Escanear con la información suministrada en la fase anterior en el anexo 4 escenario 3 y el montaje las máquinas virtuales
Herramienta software utilizada para en esta fase **NMAP** con el fin de reconocer el escenario además de realizar el montaje de las máquinas virtuales, Por lo tanto, se procede a escanear la red con NMAP filtrando el puerto para localizar las máquinas de forma rápida con el comando sudo Nmap –p 445 –O --open 192.168.0.1/24

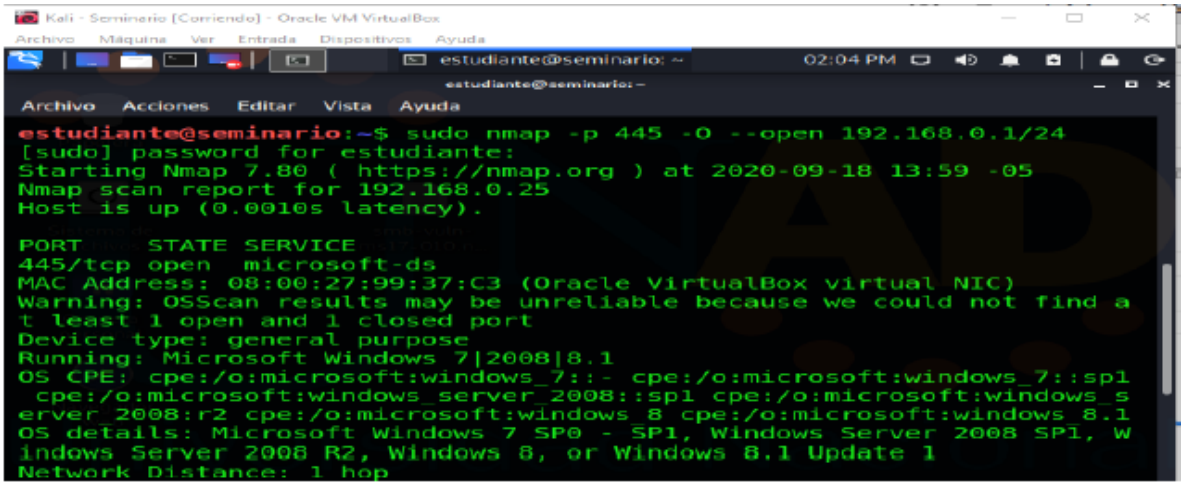
Con –p este filtro en Nmap solo escaneara –p 445 le indicamos a Nmap qué puerto queremos mapear sobre los objetivos y mapeara la información de los equipos que tengas el puerto 445.

Con la –O NMAP obtendrá información del sistema operativo de un host y nos permitirá validar que el sistema operativo coincide con lo que menciona el anexo 4 escenario 3 que indica que el sistema operativo es Windows 7 y el rango de IP para que escanee toda la red en busca de los equipos que tengan el puerto abierto.

Con --open Muestra en la salida los puertos identificados como (posiblemente) abiertos, obviando aquellos con otros estados (filtrados o cerrados).

Con 192.168.0.1/24 requerimos que escanee todos los equipos de la red 192.16.0

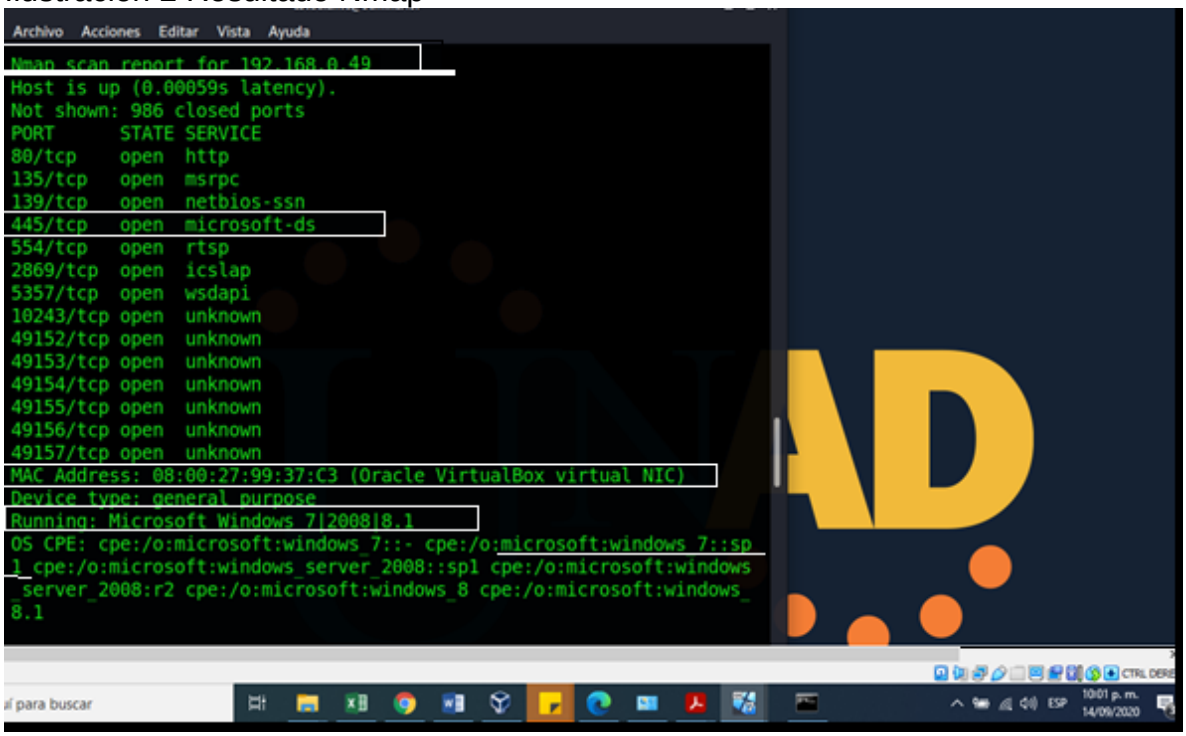
Ilustración 1 NMAP



Fuente: Propia de la actividad.

Se adjunta imagen del resultado del escaneo de la red y se observan las maquinas enviadas por la organización con sus respectivas IP y Puertos Abiertos la información de la maquina 192.168.0.49 se adjunta asi mismo arrojo la información de la otra maquina

Ilustración 2 Resultado Nmap



Fuente: Propia de la actividad.

Obsérvanos el informe que nos arroja NMAP sobre el equipo que tiene el puerto 445 abierto del cual podemos observar la dirección IP 192.168.0.49 que también es una tarjeta de red virtual y que también tiene el sistema operativo Windows 7 SP1
Por lo tanto, ya con estos datos de las direcciones IP y sabiendo que ambos tienen la tarjeta virtual podemos concluir que se trata de los equipos mencionados en el
Con NMAP obtuvimos las direcciones IP y logramos constatar cuales eran los equipos a analizar mencionados en el anexo por lo tanto procederemos a realizar el análisis para ver que herramientas utilizaremos para explotar las fallas mencionadas en el anexo 4 escenario 3 que indican, fallo de seguridad con identificador CVE-2017-0144, además los equipos de cómputo no tienen instalada la actualización MS17-010.

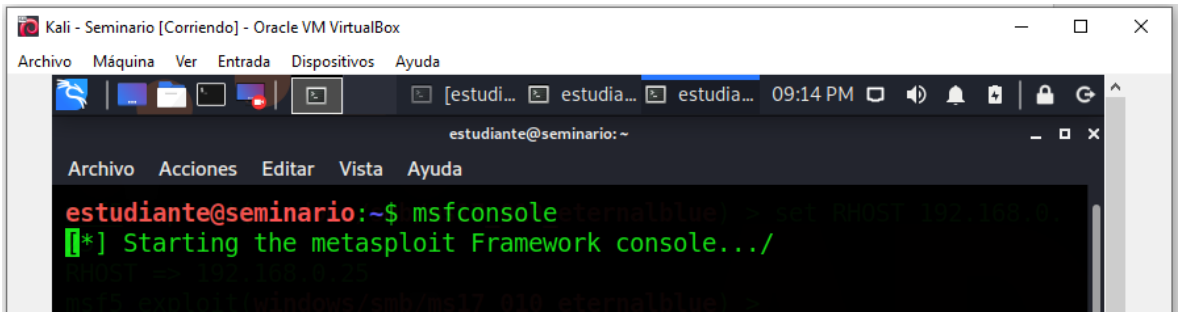
El otro Equipo Observamos que tiene la IP 192.168.0.25 que el sistema operativo que tiene es Windows 7 que la dirección MAC es de una tarjeta virtual NIC de virtual box por lo tanto podemos afirmar que se trata de uno de los equipos que nos menciona el anexo 4 escenario 3

Fase 3: con las direcciones IP capturadas procedemos a realizar un escaneó de las vulnerabilidades de cada equipo.

Procederemos a realizar el análisis para ver que herramientas utilizaremos para explotar las fallas mencionadas en el anexo que indican: fallo de seguridad con identificador CVE-2017-0144, además los equipos de cómputo no tienen instalada la actualización MS17-010.

Como primera medida se trató de atacar la máquina de Windows
7 X86 de 32 bits atacando la debilidad de seguridad que se presenta en el informe smb y ya que en el informe se menciona que los equipos cuentan con Los equipos de cómputo cuentan con un SMBv1 para compartir archivos dentro de la red
Desde kalilinux empezamos las pruebas de instrucción para lo que utilizaremos el comando msfconsole con el cual corremos el Metasploit Framework Msfconsole

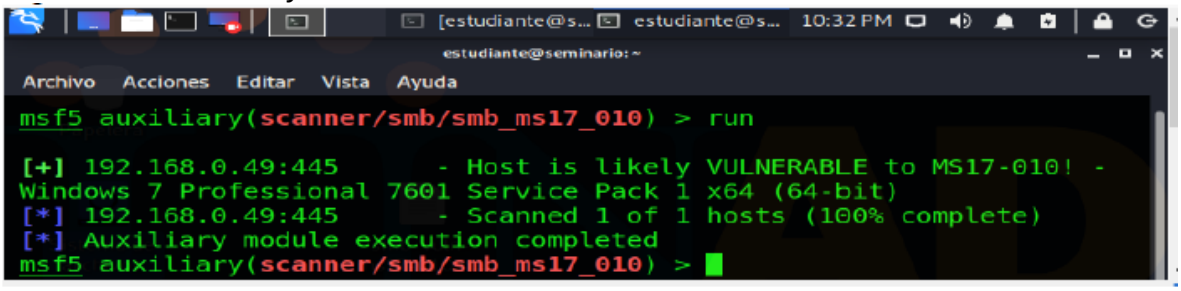
Ilustración 3 msfconsole



Fuente: Propia de la actividad.

Le damos las indicaciones del exploit que utilizaremos con el comando use auxiliary/scanner/smb/smb_ms17_010 y procedemos a configurar la IP del RHOST la cual encontramos con el escáner NMAP en la máquina de Windows X64 y es la IP 192.168.0.49 Lo ejecuto puede ser con el comando run o exploit para observar si esta máquina es vulnerable y tal como se nos indicó en el anexo 4 esta máquina tiene la vulnerabilidad MS17-010 y con Nmap descubrimos que el puerto 445 está abierto y este es el utilizado por el protocolo SMBv1 de Windows para compartir impresora y archivos y observamos el sistema operativo que tiene la maquina es w7 profesional x64.
Este mismo proceso se realiza con la otra máquina de IP 192.168.0.25

Ilustración 4 Auxiliary

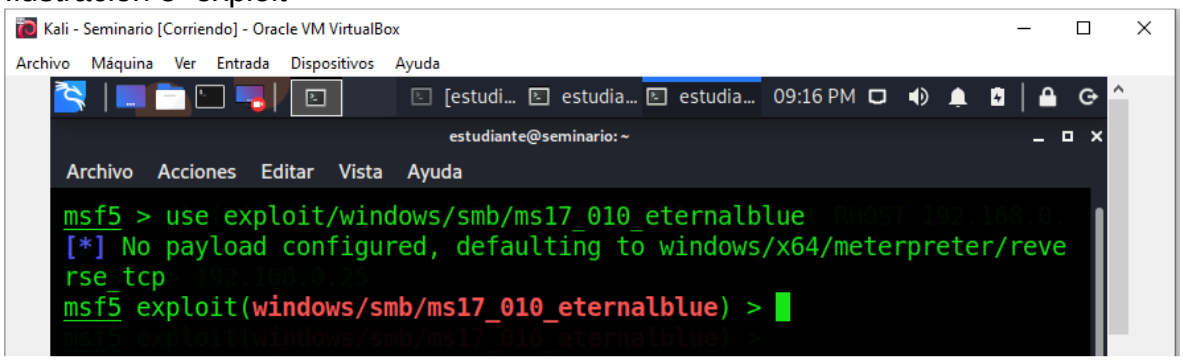


Fuente: Propia de la actividad.

Ahora al utilizar el Auxiliary y confirmar la vulnerabilidad existente en los equipos tal como se menciona en el anexo 4 escenario 3 nos indican que los equipos no tienen instalada la actualización MS17-010 que es una vulnerabilidad del Sistema operativo por lo tanto al no tener la actualización del parche para esta falla, la podremos utilizar entonces para buscar como explotar la vulnerabilidad y procedemos a observar si en kalilinux tenemos el exploit para poder utilizar esta vulnerabilidad y aprovecharla para ingresar al equipo con el intérprete de comandos meterpreter usando el exploit eternalblue desde kalilinux.

Fase 4: Explotación de las vulnerabilidades encontradas con el auxiliary scanner las cuales son confirmadas por la documentación entregada por WHITEHOUSE SECURITY en el anexo 4 escenario 3 entonces ya sabemos que utilizaremos el exploit/Windows/smb/ms17_010_eternalblue.

Ilustración 5 exploit



Fuente: Propia de la actividad.

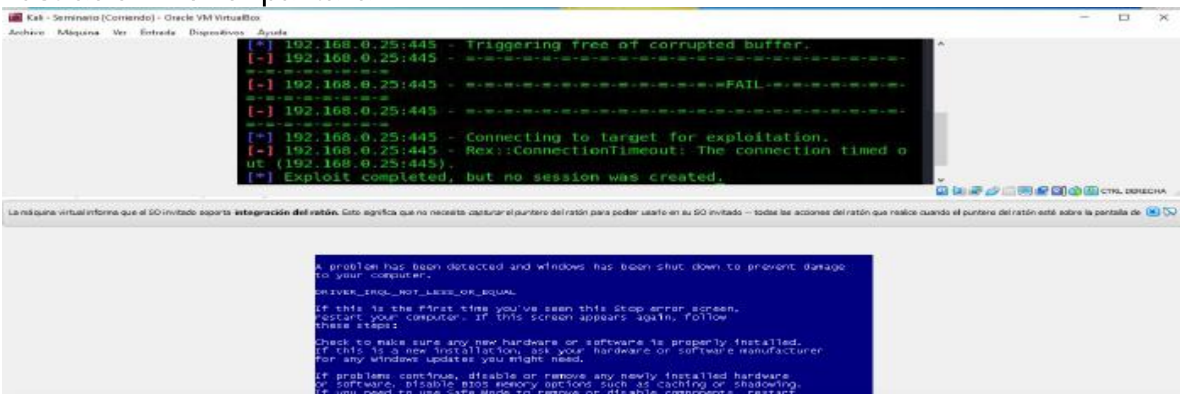
Configuramos los parámetros que se requieren para la explotación
SET RHOST: IP de la máquina obtenida con Nmap set 192.168.0.25
RPORT: aquí utilizaremos el puerto 4444 set RPORT 4444
PAYLOAD: set payload Windows/x64/meterpreter/reverse_tcp

Ilustración 6 Meterpreter

Fuente: Propia de la actividad.

observamos que ya se ingresó al meterpreter lo que me indica que ya tenemos acceso a la máquina de Windows x64 de nombre equipo PC202006 al ingresar procederemos a buscar el archivo winse20w0.exe el cual es mencionado en el anexo 4 escenario 3, este mismo proceso se desarrolló con la otra máquina de nombre win7, pero no se obtuvo acceso presento falla en la pantalla el sistema se reinicia y muestra pantalla azul el cual es mencionado en el anexo y sale el mensaje que indica que Windows se ha recuperado de un cierre inesperado la posible causa de esta falla fue el ataque a la que fue sometida que afecto los archivos del sistema debido a que esta máquina es de 32 bits arquitectura obsoleta que hace que al explotar la vulnerabilidad provoca el volcamiento de memoria y genera el error de pantalla azul

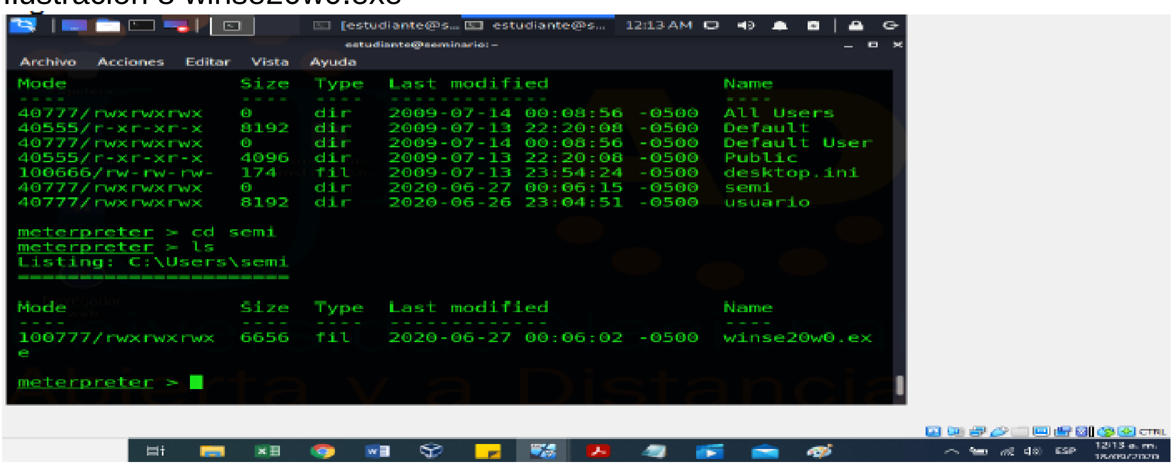
Ilustración 7 error pantalla



Fuente: Propia de la actividad.

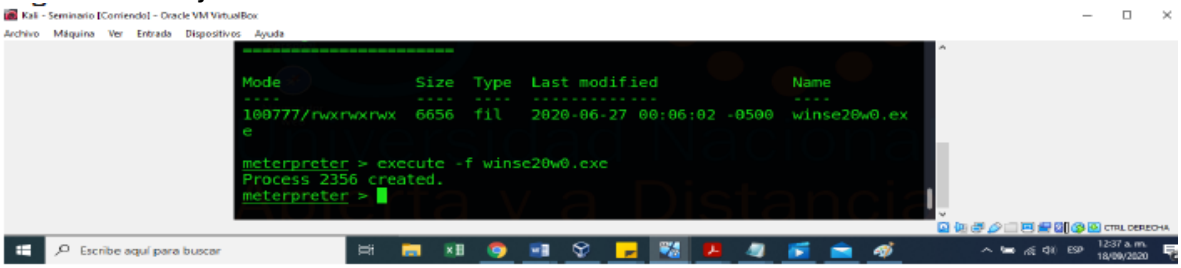
Sección cuatro: Procedemos a buscar el Archivo winse20w0.exe indicado en el anexo 4 escenario 3 para lo cual procedemos a utilizar el comando **pwd** para saber dónde estamos ubicados en este momento en la maquina víctima y podemos observar que en este momento no encontramos en c:\windows\system32 donde nos ubicamos dentro de la máquina de Windows x64 de nombre equipo PC202006 procedemos a llegar al archivo buscando con los comando cd .. , pwd, cd, ls comando de consola hasta localizar el archivo mencionado,
Con el comando Shell también se procedió a realizar la búsqueda mediante el DOS del sistema operativo Windows mediante los comandos dir, cd, cd..

Ilustración 8 winse20w0.exe



Fuente: Propia de la actividad.

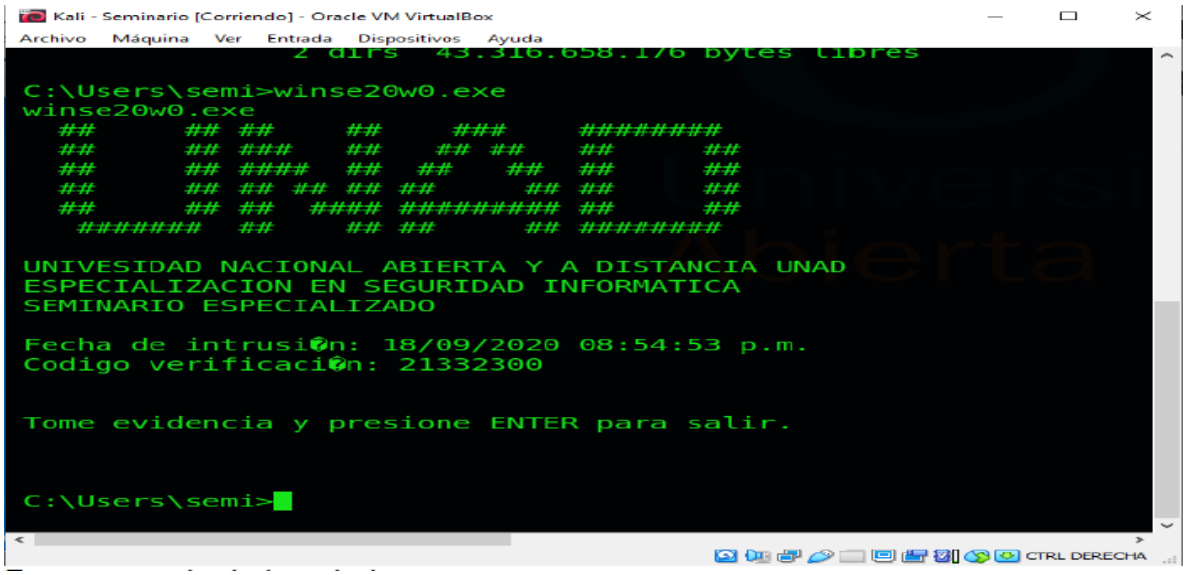
Ilustración 9 ejecución



Fuente: Propia de la actividad.

Al hacer uso del comando desde meterpreter, pero usando el Shell vamos hasta la ruta donde se encuentra el archivo mediante la consola de Windows C:\users\semi\ y dentro encontramos el archivo que no sindica el anexo procedemos a ejecutarlo desde DOS con el fin de observar que es lo que hace el software tomamos el pantallazo como evidencia

Ilustración 10 Evidencia Acceso



Fuente: Propia de la actividad.

Es evidente que al firmar el acuerdo dentro de la empresa no hay ética ya que hace responsable directamente al contratista en caso se ser encontrado con evidencias y le obliga a contratar abogados por su parte y a no denunciar las violaciones a la ley de protección de datos que al interior se cometen es cierto que la firma se debe respetar el código de ética del ingeniero y se acoge a lo estipulado legalmente en el contrato, pero se viola el código de ética del ingeniero estipulado en copnia al firmar dicho contrato

CONCLUCIONES

Se puede concluir que la empresa fue víctima de este ataque debido a que su equipo de seguridad al interior de la empresa omitió varias políticas de seguridad o no las tenían implantadas dentro de la empresa por esta razón los equipos no se encontraban actualizados respecto a:

1. los parches de seguridad de los sistemas.
2. La actualización del antivirus con el cual contaban los equipos no eran actualizados.
3. La arquitectura de sistema operativo de uno de los sistemas instalados no era adecuada.
4. No se encontró Activadas las actualizaciones automáticas en los equipos.
5. Configuracion adecuada de las reglas en firewall al compartir impresoras y archivos.
6. Política de trasferencia de archivos con extensión .exe

Es muy importante mantener dentro de la entidad una constante actualizaciones los sistemas tanto a nivel operativo con sus respectivos parches como de la actualización y migración de los sistemas y sus respectivas aplicaciones debido a que el no hacerlo deja la maquina vulnerable a ataques.

RECOMENDACIONES.

Se recomienda a la empresa establecer políticas de seguridad al interior y contar con un equipo blue Team con el fin de que estén pendiente de las fallas dentro de la empresa o sea contratado personal que realice esta labor trimestralmente.

Realizar una concientización al personal de sistemas de la importancia que tiene mantener al interior de la empresa las maquinas actualizadas con sus respectivos parches de seguridad si no se hace manualmente al menos mantener bien configurados los equipos para que la actualización sea automática.

Que tanto el personal de sistemas mantenga actualizado el antivirus y lo ejecute o capacite al personal a escanear los equipos constantemente para detectar los archivos riesgosos dentro de la maquinas.

Recomendable hacer auditorías internas con el fin de observar que fallas se están cometiendo en cuanto a la seguridad de los equipos de cómputo y de la red dentro de la empresa.

ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM

Dentro de toda empresa los siguientes aspectos aportan al desarrollo de las estrategias de RedTeam y BlueTeam.

- Policitas de seguridad.
- Políticas de monitorio o auditoria
- Compromiso inicial con la seguridad.
- Definición del Nivel de riesgo dentro de la empresa.
- Capacidad de detención.
- Capacidad de análisis.
- Capacidad de respuesta.
- Evaluación de privilegios
- Reconocimiento de la infraestructura interna.

RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN

Para que no se tengan problemas se recomienda hacer uso de la estructura de controles CIS asi como establecer dentro de la organización políticas de seguridad y al mismo tiempo que este cuente con un plan de auditoria que verifique que se cumpla.

Recomiendo a la empresa de acuerdo a La estructura de controles CIS ya que esta me facilita la validación de la implementación de controles y subcontroles recomendados de acuerdo a la denominación que se tenga de la infraestructura de la empresa si es crítica o no utilizando de los 20 grupos de controles los siguientes:

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Continuous Vulnerability Assessment and Remediation
- Controlled Use of Administrative Privileges

CONCLUSIONES QUE PERMITAN LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD

Se ve la importancia de contar con una política en cuanto a la actualización de los parches en los sistemas operativos.

Se observa la necesidad de mantener los antivirus actualizados y bien configurados para evitar los códigos maliciosos.

Se da entender a la empresa la importancia de tener dentro de la empresa un plan de migración de las aplicaciones para que funcionen con las nuevas tecnologías.

La empresa debe saber que la actualización y modernización de la arquitectura hardware y del software dentro de la empresa ya que todo evoluciona y la empresa debe estar a la vanguardia por seguridad.

Lo importante que es tener dentro de la empresa personal que realice actividades de Hardenizacion en los equipos.

La importancia de tener personal profesional que se encargue de la seguridad y de velar porque se cumplan las políticas de seguridad al interior.

LINK VIDEO SUSTENTACION.

https://youtu.be/dH4vr3Si2qQ

RECIBO Y PORCENTAJE TURNITIN.

Ilustración 11 Turnitin

turnitin

Recibo digital

Este recibo confirma que Turnitin ha recibido tu trabajo. A continuación, encontrarás la información del recibo perteneciente a tu entrega.

Autor de la entrega	JOSE RAFAEL NINO
Identificador del trabajo de Turnitin (Identificador de referencia)	1413980170
Título de la Entrega	borrador final
Título del ejercicio	ECBTI - Draftbank 2
Fecha de entrega	13/10/20, 10:05

Imprimir

Fuente. https://campus126.unad.edu.co/

Ilustración 12 porcentaje revisión

	Título de la Entrega	Identificador del trabajo de Turnitin	Entregado	Similitud	Calificación	Nota general	
Ver recibo digital	borrador final	1413980170	13/10/2020 10:05	14%	N/A	--	Entregar Trabajo

Usted se ha identificado como JOSE RAFAEL NINO (Salir)
855A_476

Fuente: https://campus126.unad.edu.co/

BIBLIOGRAFIA.

A continuación, relaciona la bibliografía consultada desde el inicio del proceso

COPNIA, Código de ética, Consejo profesional de ingeniería, Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., [versión 23.3 en línea].disponible en: https://dle.rae.es.

Naciones Unidas, El informe que sacudió el caso de la fachada Andrómeda, (2015). Disponible en: https://www.hchr.org.co/index.php/compilacion-de-noticias/155-espionaje/5697-el-informe-que-sacudio-el-caso-de-la-fachada-andromeda.

Naciones Unidas, Nexo de Andrómeda y 'hacker', clave en proceso de coroneles, (2014). Disponible en: https://www.hchr.org.co/index.php/compilacion-de-noticias/155-espionaje/5141-nexo-de-andromeda-y-hacker-clave-en-proceso-de-coroneles.

Fiscalía General de la Nación. (2015). *Informe Caso Andrés Sepúlveda hacker de la operación Andrómeda.* Disponible en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/20170111.pdf.

Revista Hacking Ético: FASES DEL PENTESTING Aprende Como Hacer Auditoria De HACKING A Empresas obtenido de : https://www.revistahackingetico.com/2019/09/fases-del-pentesting-aprende-como-hacer.html.

Gordon Lyor, NMAP Network Scanning, una Guía Oficial del escáner de seguridad, Disponible en: https://nmap.org/book/preface.html.

Pablo González, Metasploit & Hacking Ético RootedLAB, (2018). Disponible en: https://rootedcon.com/docs/trainings/rootedvlc2018-rlv1-metasploit_hacking_etico.pdf.

CIS Controls, Cloud Companion Guide
Disponible en: https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/

IBM QRadar Security Information and Event Management (SIEM)
Disponible en: https://www.ibm.com/ar-es/products/qradar-siem.

Imperva, Gestión de eventos e información de seguridad (SIEM) disponible en: https://www.imperva.com/learn/application-security/siem/.

Grammatech. (2016). Software Hardening. 2016, de grammatech.com. Disponible en: https://www.grammatech.com/software-hardening.

SANCHEZ, Z. (2011). Desarrollo de una guía para selección y endurecimiento (hardening) de sistemas operativos para un centro de datos, Disponible en: http://tesis.ipn.mx/jspui/handle/123456789/8466.

ADMIN,(2013) Tutorial Nmap para Kali Linux, 2013, Disponible en: http://kalilinux.foroactivo.com/t12-tutorial-nmap-para-kali-linux

IPAUDITA,(2013), Top 30 de Nmap ejemplos de comandos para SYS / Red Admins, disponible en:https://ipaudita.wordpress.com/2013/02/13/top-30-de-nmap-ejemplos-de-comandos-para-sys-red-admins/

CABALLERO, Alonso,(2015), Hacking con Kali Linux, Disponible en: http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf