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

RICARDO MENDEZ BARCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATTEGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
ARAUCA
2020

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

RICARDO MENDEZ BARCO
Curso: 202337164A_780

TRABAJO ACTUACION ETICA Y LEGAL

M.sc. JOHN FREDDY QUINTERO
Director curso: Seminario Especializado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATTEGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
ARAUCA
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Arauca y Fecha (16, 10,2020)

Dios, por haberme dado la vida el cual me guio en el duro camino de mi formación profesional.

AGRADECIMIENTOS

Dios, por haberme dado la vida el cual me guio en el duro camino de mi formación profesional.

A mi esposa, por ser el apoyo moral más importante demostrándome siempre su cariño incondicional, sin importar los fracasos que pude haber tenido.

A mi madre, a pesar de su prematura ausencia, siento que siempre está conmigo, aunque me faltaron muchos momentos especiales por vivir juntos, sé que este momento hubiera sido tan especial para ella como lo es para mí.

A mis hijos, que día a día, con mi ejemplo les pude enseñar que con disciplina el camino más difícil siempre conduce al Éxito, y camino fácil al fracaso.

A mis tutores de la UNAD porque sin ellos, no hubiéramos logrado esta meta

CONTENIDO

Pág.

INTRODUCCIÓN 10
1. OBJETIVOS 11
1.1 OBJETIVO GENERAL 11
1.2 OBJETIVOS ESPECÍFICOS 11
2 DESARROLLO DEL INFORME 12
2.1 MARCO LEGAL 12
2.1.1 Delitos Informáticos Ley 1273 de 2009 12
2.1.2 Datos Personales Decreto 1377 de 2013 13
2.1.3 Código de Ética Profesional Ley 842 de 2003 13
2.1.4 Acuerdo de Confidencialidad 14
2.2 CASO ANDROMEDA 14
2.3 CASO FUGA DE INFORMACION – Equipo Red Team 16
2.3.1 Comunicación Previa 17
2.3.2 Recogida de Información 18
2.3.3 Modelo de Amenazas 19
2.3.4 Análisis de vulnerabilidad 22
2.3.5 Explotación 23
2.4 ACCIONES DURANTE UN ATAQUE INFORMATICO EN TIEMPO REAL – Equipo Blue Team 24
2.4.1 Estrategia de Ciberseguridad Nacional. 24
2.4.2 Plan de Respuesta de Incidentes 25
2.4.3 Identificación de la intrusión en Tiempo Real 26
2.4.4 Aplicación de Solución 26
2.4.5 Maquina Windows 7x86 28
2.4.6 Link Video https://youtu.be/1wWX6Y9x3Pk 28
3 CRONOGRAMA 29
CONCLUSIONES 30
RECOMENDACIONES 31
BIBLIOGRAFÍA 33

LISTA DE IMAGENES

Figura 1 Fases Estándar PTES 16
Figura 2 Entorno Controlado Máquinas Virtuales 19
Figura 3 Identificación de Vulnerabilidades Windows 7 x 64 21
Figura 4 Identificación del Exploit - Windows 7x64 22
Figura 5 Acceso Objetivo - Maquina Windows 7x64 23
Figura 6 Instituciones para Informar ataques o delitos cibernéticos 24
Figura 7 Modelo de Gestión de Incidentes 25
Figura 8 Desactivar Protocolo SMBv1 27
Figura 9 Exploit después de desactivar el protocolo SMBv1 27

GLOSARIO

Exploit[1]: Código o programa, que se aprovecha de una falla de seguridad en una aplicación o sistema

Nmap[2]: Mapeador de Redes, es una herramienta para la exploración de redes, auditoria y seguridad.

Metasploit[3]: Es una herramienta para validación de vulnerabilidades y explotación para pruebas de penetración.

Payload[4]: Es la carga que se ejecuta en una vulnerabilidad, es decir la carga que se actica a la hora de aprovechar una vulnerabilidad (Exploit)

Red Team[5]: Sistemas y personal para analizar vulnerabilidades y realizar un ataque dirigido con herramientas ofensivas a medida, con el objetivo final de infiltrarse en una organización y sustraer información sin ser detectados.

Blue Team: Equipo que realiza una evaluación inicial de la amenaza, con el objetivo de contenerla para reducir el riesgo. Una vez contenida se procede a mitigar el riesgo hasta obtener una solución definitiva que permita asegurar la continuidad del negocio en el mínimo tiempo posible.

[1] WELIVESECURITY, ¿Sabes qué es un exploit y cómo funciona?). [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/
[2] NAMAP, Guía de referencia de Nmap (Página de manual). [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://nmap.org/man/es/index.html#man-description
[3] RAPID7, Quick Start Guide. [Sitio WEB]. La entidad [03, septiembre, 2020]. Disponible en: https://docs.rapid7.com/metasploit/
[4] OPENWEBINARS, Qué es un Payload.). [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://openwebinars.net/blog/que-es-payload/
[5] GLOBETESTIN, Red Team y Blue Team. [Sitio WEB]. La entidad [14, octubre, 2020]. Disponible en: https://www.globetesting.com/static_block/red-team-blue-team/

RESUMEN

El presente trabajo permite desarrollar una serie de actividades dentro un marco legal y en un ambiente controlado donde el equipo Red Team y Blue Team resolvieron un incidente de seguridad informática.

En la primera parte de este trabajo se identificará un marco legal que contempla delitos informáticos, datos personales, código de ética y acuerdo de confidencialidad.

Una segunda parte se realizará una síntesis del caso de Andrómeda dentro un marco legal y ético.

Seguido a esta, en una tercera parte se realizará la descripción de las acciones realizadas dentro el caso de fuga de información, contemplando la metodología y herramientas asociadas dentro un ambiente controlado en ejercicio de Red Team y Blue Team.

Finalmente se realiza las correspondientes conclusiones y recomendaciones.

PALABRAS CLAVE: Metasploit, exploit, payload, Blue Team, Red Team

INTRODUCCIÓN

En la actualidad la información es considerado uno activo crítico, que permiten a las empresas utilizarla como recursos para el crecimiento del negocio.

Se considera delito informático cuando una persona se apropia de información confidencial almacena en cualquier medio electrónico o digital. Incurrir en los delitos informáticos tienen sanciones que están contemplados bajo la ley 1273 del año de 2009, denominada “de la protección de la información y de los datos”.

De igual forma se reglamenta la conducta de los profesionales en ingeniería y las profesiones afines, dentro de un marco de código de tética en donde la violación a este se sancionará mediante los procedimientos establecidos.

De acuerdo a lo anterior todo ejercicio de pentesting o equipos Red Team se debe fundamentar en un marco legal y metodológico cuyo fin es de poner aprueba las capacidades de una organización para defenderse efectivamente de ataques cibernéticos dentro un entorno real pero controlado simulando las diferentes tácticas, técnicas y procedimientos tanto ofensivas como defensivas.

De igual manera es necesario saber las acciones que se deben tomar en el caso de que se identifique una intrusión o cualquier incidente de ciberseguridad en un sistema de la organización

1. OBJETIVOS

1.1 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.

1.2 OBJETIVOS ESPECÍFICOS

1. Describir el marco legal asociado a los delitos Informáticos.
2. Describir el caso de Andrómeda
3. Describir el caso de fuga de información dentro de la organización
4. Describir acciones durante el ataque en tiempo real

2 DESARROLLO DEL INFORME

2.1 MARCO LEGAL

2.1.1 Delitos Informáticos Ley 1273 de 2009[6]

- Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO cárcel de (48) a (96) meses y un castigo económico entre 100 a 1000 SMLMV.

- Artículo 269B: OBSTACULACION ILEGITIMA DE UN SISTEMA INFORMATICO O RED DE TELECOMUNICACIONES, cárcel de (48) a (96) meses y una sanción económica de 100 a 1000 SMLMV.

- Artículo 269C: INTERSECCION DE DATOS INFORMATICOS, cárcel de (36) a (72) meses.

- Artículo 269D: DAÑO INFORMATICO, cárcel de (48) a (96) meses y un castigo económico de 100 a 1000 SMLMV

- Artículo 269E: USO DE SOFTWARE MALICIOSO, cárcel de (48) a (96) meses y un castigo económico de 100 a 1000 SMLMV.

- Artículo 269F: VIOLACION DE DATOS PERSONALES, cárcel de (48) a (96) meses y un castigo económico de100 a 1000 SMLMV.

- Artículo 269G: SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES, castiga con cárcel de (48) a (96) meses y una sanción económica de 100 a 1000 SMLMV.

- Artículo 269H: Considera que la CIRCUNSTANCIA DE GRAVACION PUNITIVA, se aumentara del 50% al 75% si el delito se cometiere en:
  1. Sistemas informáticos o redes de comunicaciones en entidades del estado o privadas ya sean del sector financiero nacionales o extranjeros
  2. En el ejercicio de sus funciones como servidor publico
  3. Falta a la confianza del dueño de la información o si existiera una relación contractual

[6] MINTC, Ley 1273 de 2009. [Sitio WEB]. La entidad 14, octubre, 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

4. Perjuicio de otro cuando revela o da a conocer el contenido de la información.
5. Situaciones donde beneficie a tercero o así mismo
6. Situaciones de Terrorismos y pusiera en peligro la seguridad nacional
7. La buena fe de un tercero utilizando como mecanismo delictivo
8. En el ejercicio de sus funciones como responsable de la administración, control y manejo de dicha información tendrá una inhabilidad hasta 3 años, para ejercer su profesión si está relacionada con sistemas de información o equipos computacionales.

- Artículo 269I: HURTO POR MEDIOS INFORMATICOS SEMENJATES, sanción penal de acuerdo al artículo 240 del presente código.

- Artículo 269J: TRANSFERENCIA NO CONCENTIDA DE ACTIVOS, cárcel de (48) a (120) meses, con un castigo económico de 200 a 1500 SMLMV.

2.1.2 Datos Personales Decreto 1377 de 2013[7]

El Ministerio de Comercio, industria y Turismo y mediante el presente decreto reglamenta parcialmente la Ley 1581 de 2012, con el fin de facilitar la implementación y cumplimiento de aspectos relacionados con la autorización del Titular de Información para el tratamiento de los datos personales, las Políticas y responsabilidades frente al Tratamiento de Datos Personales como el ejercicio de los derechos y las responsabilidades de los derechos de los titulares de la información

2.1.3 Código de Ética Profesional Ley 842 de 2003[8]

Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones.

[7] MINTC, Decreto 1377 de 2013. [Sitio WEB]. La entidad 14, octubre, 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/4274:Decreto-1377-de-2013
[8] COPNIA, Ley 842 de 2003. [Sitio WEB]. La entidad 14, octubre, 2020]. Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

El cumplimiento de las disposiciones del Código de Ética, permite que el ejercicio profesional será guiado por criterios, conceptos y unos fines que velan por el comportamiento del ingeniero.

2.1.4 Acuerdo de Confidencialidad

Documento que por medio del cual las partes interesadas se comprometen a no revelar información de carácter confidencial la cual afecte los intereses de la empresa, para un profesional es importante que este acuerdo este bajo el marco de la Ley y el Código de Ética que este fundamentada su profesión.

Los acuerdos de confidencialidad permiten por lo general regular lo siguiente:

- Se debe describir cual información debe ser considerada como confidencial
- Motivos por los cuales la información deja de ser confidencial
- Casos en las que la información confidencial puede ser divulgada a terceros, así mismo cuando esta se vuelve pública, o por requerimiento judicial;
- Cláusulas generales, como término de duración, aplicación de leyes, mecanismos que permitan la solución de controversias, cláusulas penales, entre otros.

2.2 CASO ANDROMEDA[9]

Se trata de una fachada del ejército, en un edificio donde trabajaban personal civil, hackers expertos, personal retirado del Ejercicito, militares activos de diferentes rangos como oficiales y suboficiales que se encargaban de reclutar jóvenes talentosos. Las investigaciones determinaron que desde allí se realizaban seguimiento a los correos electrónicos y a los chats a personajes de la vida pública que en su momento estaban dedicados a las negociaciones del proceso de paz en la Habana y atentaban contra la seguridad nacional. , los hackers tenían tareas para conseguir las contraseñas de correos electrónicos, números de pin del BlackBerry, intercepciones telefónicas y una lista de 1.000 correos electrónicos con el fin de ser hackeados, sin ninguna orden judicial.

[9] SEMANA, Atrapados en la Andrómeda, [Sitio WEB]. La entidad [10 septiembre, 2020]. Disponible en: https://www.semana.com/opinion/articulo/maria-jimena-duzan-atrapados-en-la-andromeda/377305-3/

Dentro de la investigación esta el caso del “hacker” Andrés Fernando Sepúlveda, y el patrullero de la Sijin Ignacio David Parra Amin, el cual será procesado por delitos de espionaje, cohecho propio y violación de datos personales.

A su vez aprovechándose de la confianza del estado colombiano como en el caso del CITEC - Central de Inteligencia Técnica del Ejército y la CIME – Central de Inteligencia Militar, revelaron y dieron a conocer información en perjuicio de terceros.

Igualmente se demostró que se afectaron físicamente activos de información que permitían entorpecer las investigaciones.

El caso de Andrómeda es fehaciente en que se violaron los siguientes artículos correspondientes a la Ley 1273 de 2009:

- Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMATICO
- Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS
- Artículo 269D. DAÑO INFORMÁTICO
- Artículo 269E. USO DE SOFTWARE MALICIOSO
- Artículo VIOLACIÓN DE DATOS PERSONALES
- Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.
- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS

De Igual forma también se violo el Código de Ética COPNIA así:

- Artículo 31. Deberes generales de los profesionales en su literal b). custodiar y cuidar los bienes, valores, documentación e información.
-
- Artículo 34. Prohibiciones especiales a los profesionales respecto a la sociedad y en su literal a). dispone que ofrecer o aceptar trabajos en contra la normativa laboral vigente o aceptar tareas que excedan su profesión.

- Artículo 36. Deberes de los profesionales para con la dignidad de sus profesiones en su literal d). En donde se realizó avisos exagerados sobre su especialidad o idoneidad profesional

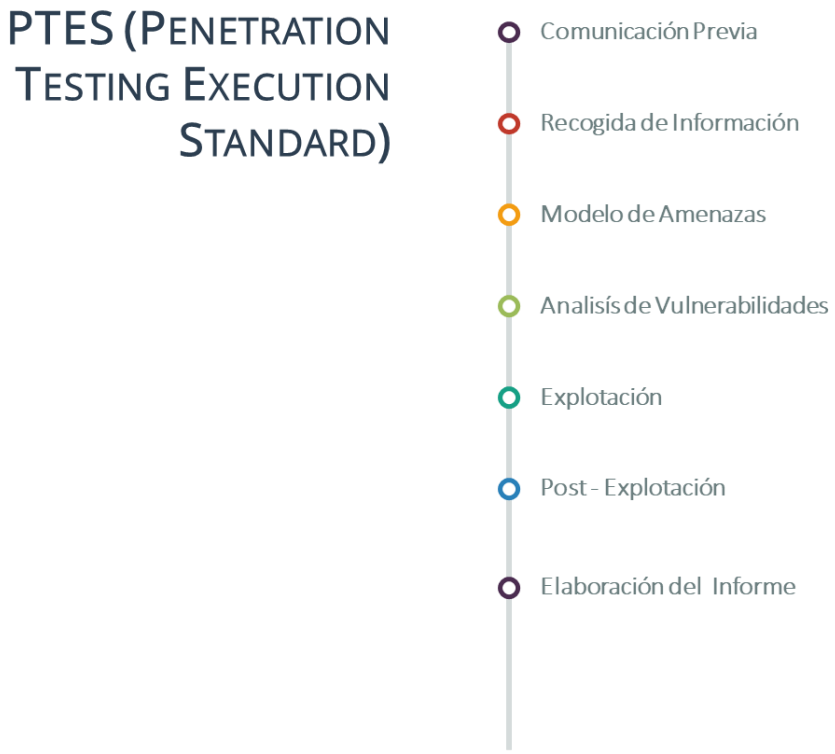
- Artículo 38. Prohibiciones a los profesionales respecto de sus colegas y demás profesionales en su literales c) y d)

2.3 CASO FUGA DE INFORMACION – Equipo Red Team

A continuación, se realiza una descripción de cada una de las actividades que se desarrollaron por parte del equipo Red Team, con el fin de identificar vulnerabilidad en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

El equipo Red Team tiene como tarea identificar porque medio o proceso se está generando una serie de fuga de información dentro de una organización, el cual para cumplir su objetivo se utilizó como base el estándar PTES[10] (Penetration Testing Execution Standart) la cual se desarrollará a continuación, de igual forma aplicando herramientas Open Source, especializadas en pentesting.

Figura 1 Fases Estándar PTES



Fuente: http://www.pentest-standard.org/index.php/Main_Page

[10] PENTEST-STANDARD, High Level Organization of the Standard. [Sitio WEB]. La entidad [14, Octubre, 2020]. Disponible en: http://www.pentest-standard.org/index.php/Main_Page

2.3.1 Comunicación Previa

- Duración del Proyecto (fecha de inicio, fecha final, tiempo extra):
  El proyecto se inició 20/agosto/2020 y como entregable un informe técnico para el día 16/octubre/2020.

- Actividades a realizar y el alcance de las mismas:
  Se utilizará el estándar PETS (Penetration Testing Execution Standart) de pruebas de penetración, consta de 7 secciones principales
  - Interacciones previas al compromiso
  - La recogida de información
  - Modelado de amenazas
  - Análisis de vulnerabilidad
  - Explotación
  - Después de la explotación
  - Reportando

- Activos del cliente implicados:
  El cliente define los siguientes activos que serán objetivos, los cuales serán debidamente verificados que pertenezcan a la organización, con el fin de evitar consecuencias legales.

  - Un equipo de cómputo con sistema operativo Windows 7 x64
  - Un equipo de cómputo con sistema operativo Windows 7 x86

- Metas
  Se evidencia le logro de las siguientes metas
  - Principal: lograr identificar porqué medio o proceso se está generando una serie de fuga de información.
  - Secundaria: logra acceder al equipo de cómputo de manera intrusiva deberá encontrar el archivo mencionado y tomar pantalla de la información.

- Contacto entre el cliente y el prestador de servicios:
  Se estableció como contacto por parte del cliente al Ingeniero M.sc. John Freddy Quintero, el cual tenía la responsabilidad de tomar decisiones con respecto a la metodología con la que se desarrolla las pruebas y se tendrá una comunicación permanente y segura del intercambio de la información.

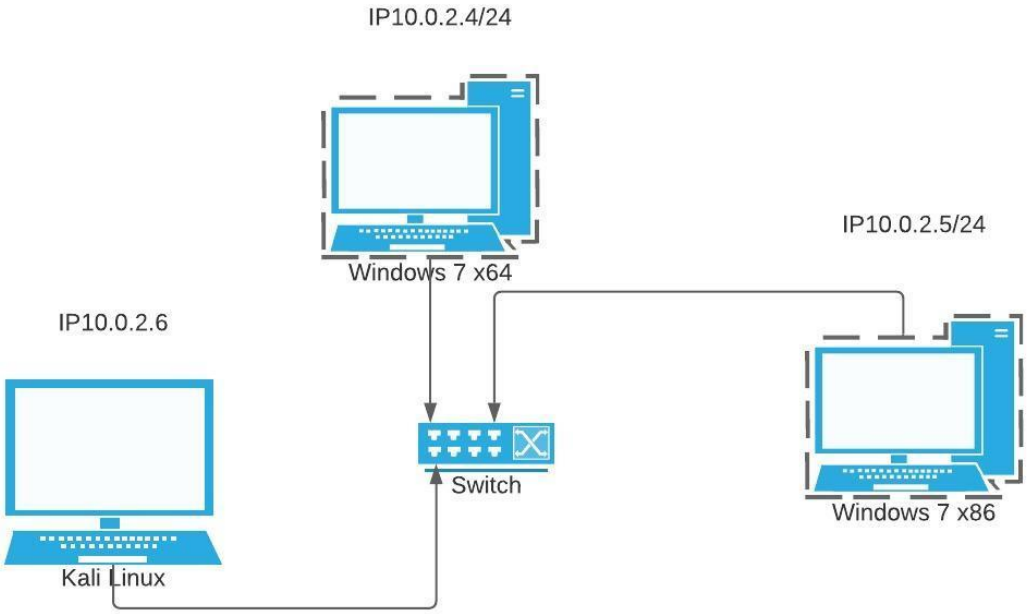
- Reglas de negocio:
  Se evidencio las siguientes reglas:
  - Línea de tiempo: se tomó la agenda académica, con el fin hacer seguimiento al tiempo empleado, y tomar en cuenta los horarios y condiciones donde se realizarán las pruebas.
  - Localización de activos:
    Los activos siempre estuvieron ubicados dentro de la organización en cada una de sus dependencias, y con fin de agilizar el proceso de investigación WhiteHose Security facilito escenarios controlados para los equipos de cómputo sospechosos y un escenario controlado con un S.O orientado al testeó de seguridad lo que permitió el trabajo de investigación sin alterar la infraestructura de producción de la organización.
  - Uso de la Información Sensible:
    Durante las pruebas de intrusión, la información que se encuentro como sensible se mantendrá de acuerdo a los acuerdos de confidencialidad
  - Profundidad en la obtención de la información:
    Se tomo como evidencia el archivo que contiene la información que han estado extrayendo con el nombre de “winse20w0.exe”, accediendo al equipo de cómputo de manera intrusiva tomando pantallazo de la información.

2.3.2 Recogida de Información

La organización suministro toda la información necesaria mediante el Anexo 4 – Escenario 3

Los equipos de cómputo de los cuales se sospechaba cuentan con Windows 7 X86 y X64, estos equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O. y no pueden ser reemplazados porque la aplicación no está migrada con compatibilidad a otros sistemas operativos. Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red. Al momento de la fuga de información (10 de junio de 2020) los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017 preocupando a la organización, porque pueden estar relacionados al fallo de seguridad con identificador CVE-2017-0144, además los equipos de cómputo no tienen instalada la actualización MS17-010.

Figura 2 Entorno Controlado Máquinas Virtuales



Fuente: Diseño WhiteHose – Entorno Controlado

2.3.3 Modelo de Amenazas

A partir de la información recogida previamente se realizaron las consultas pertinentes, lo que permitió prepara la estrategia para realizar de forma efectiva la intrusión a los equipos de cómputos comprometidos así:

Descripción Server Message Block (SMB) es un protocolo de red de capa de aplicación que opera a través de los puertos TCP 139 y 445, que se utilizan ampliamente para compartir archivos e impresoras y acceder a servicios remotos.

Mediante al fallo de seguridad con identificador CVE-2017-0144[11], el cual se consulto en la página web https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144 donde se detalla en qué consiste la vulnerabilidad que se ha descubierto, qué

[11] COMMON VULNERABILITIES AND EXPOSURES, CVE-2017-0144. [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

versiones del software están afectadas así como la posible solución a este fallo (si existe) o cómo configurar los equipos para mitigar la vulnerabilidad.

Impacto

Vector de acceso: A través de red
Complejidad de Acceso: Media
Autenticación: No requerida para explotarla
Tipo de impacto: Compromiso total de la integridad del sistema + Compromiso total de la confidencialidad del sistema + Compromiso total de la disponibilidad del sistema

De igual forma se ingresó a la página web https://www.exploit-db.com/exploits/42031, donde es un directorio web que contiene registros de vulnerabilidades de aplicaciones y cómo aprovecharse de ellas, con instrucciones detalladas para realizar la intrusión. Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)

Así mimos se consulto la pagina web https://nvd.nist.gov/vuln/detail/CVE-2017-0144 , en donde se describe aspectos como la criticidad o impacto.

La página de Microsoft https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010, también nos proporciona información técnica relacionada con la clasificación de gravedad de la vulnerabilidad y software afectado, como también la actualización de seguridad para el servidor SMB de Microsoft Windows (4013389).

Por ultimo se consulto en la pagina web https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/, que permite identificar detalles y realiza recomendaciones para mitigar el fallo de seguridad como los siguientes

Recomendamos que se tomen las siguientes acciones[12]:

- Aplique los parches adecuados proporcionados por Microsoft a los sistemas vulnerables inmediatamente después de realizar las pruebas correspondientes.
- Desactive SMBv1 en todos los sistemas y utilice SMBv2 o SMBv3 después de las pruebas adecuadas.
- Ejecute todo el software como un usuario sin privilegios (uno sin privilegios administrativos) para disminuir los efectos de un ataque exitoso.

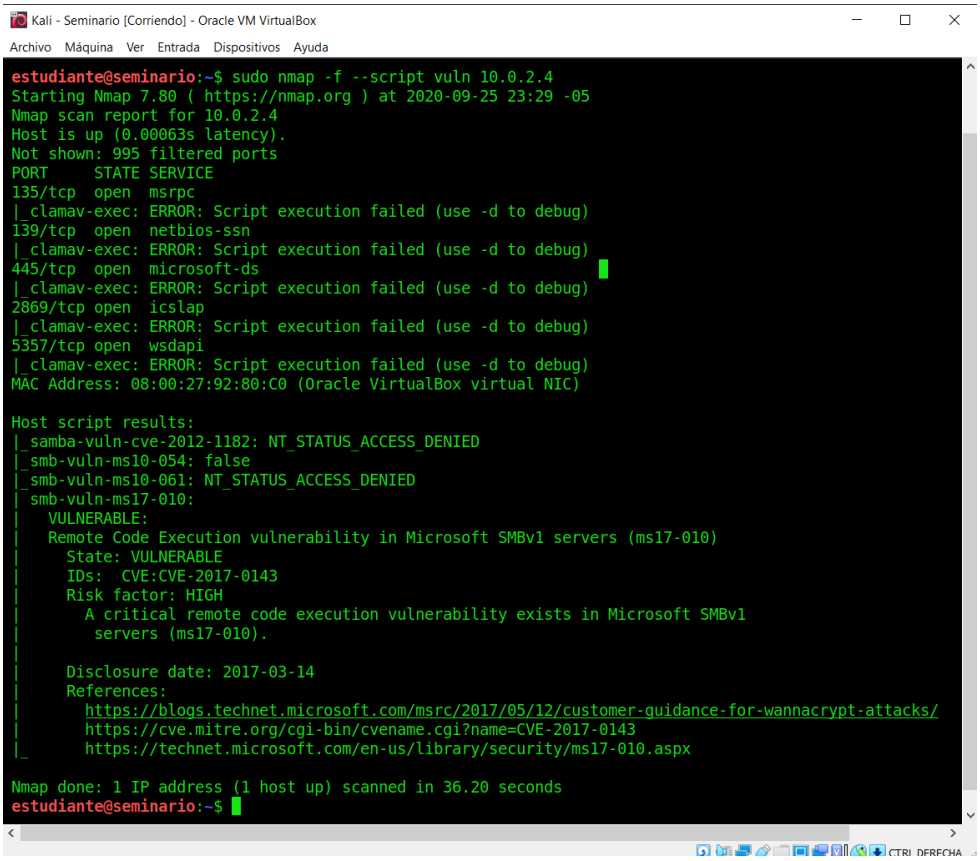
[12] CISECURITY, Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution. [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/

- Recuerde a los usuarios que no deben visitar sitios web que no sean de confianza ni seguir enlaces proporcionados por fuentes desconocidas o no confiables.
- Informar y educar a los usuarios sobre las amenazas que plantean los enlaces de hipertexto contenidos en correos electrónicos o archivos adjuntos, especialmente aquellos de fuentes no confiables.
- Aplicar el principio de privilegio mínimo a todos los sistemas y servicios.
- Aplique o instalar manualmente la actualización correspondiente 4013389

Se utilizo la herramienta nmap que permite identificar vulnerabilidades, por medio de esta herramienta se pudo establecer con precisión la información suministrada correspondiente a la incidencia que presentaban los equipos de cómputo.

En la imagen siguiente se evidencia el fallo de vulnerabilidad CVE-2017-0143 el cual está contemplado en la vulnerabilidad CVE-2017-0144, de igual forma el comando nos arroja la información asociada al protocolo SMBv1, el cual es un protocolo de red de capa de aplicación que opera a través de los puertos TCP 139 y 445.

Figura 3 Identificación de Vulnerabilidades Windows 7 x 64

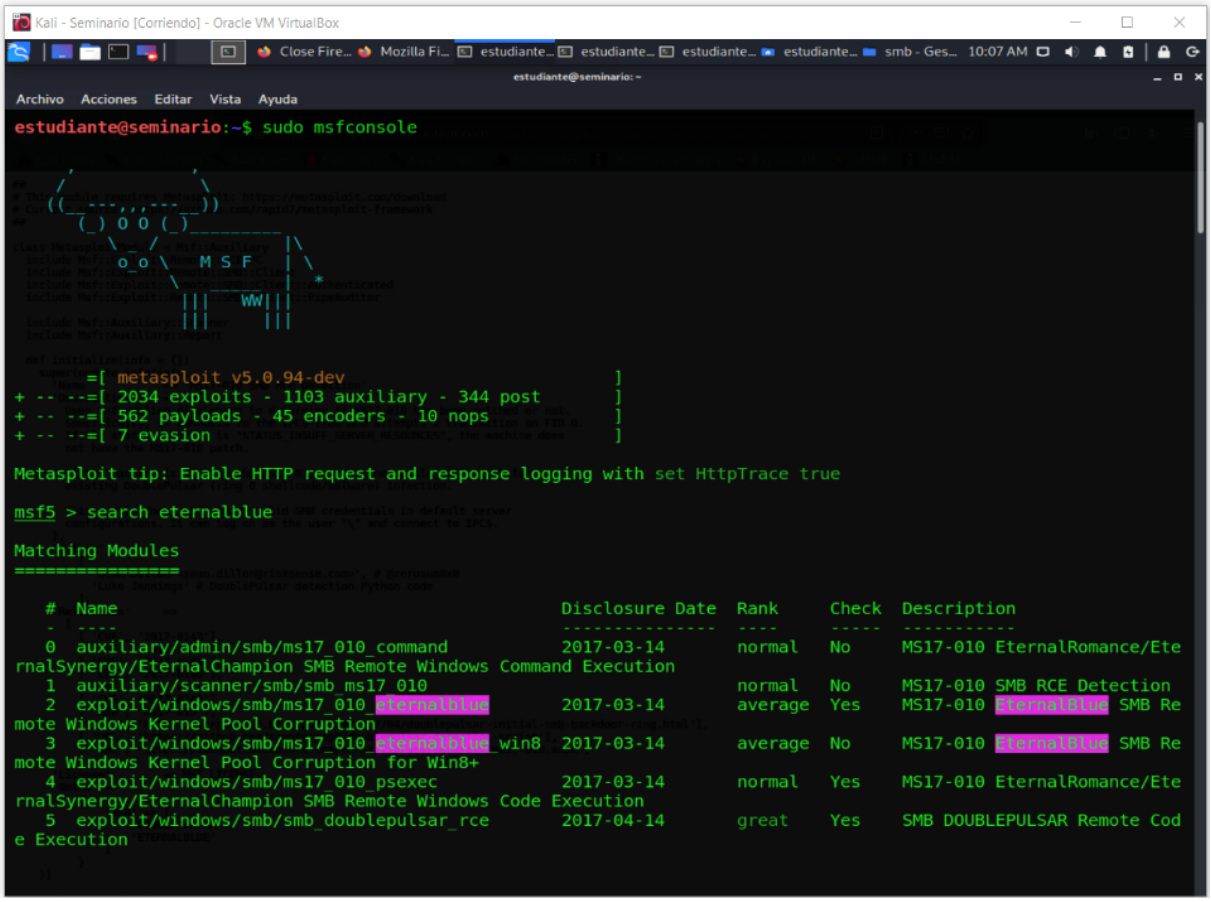


Fuente: Ejecución comando herramienta Nmap

2.3.4 Análisis de vulnerabilidad

Mediante la herramienta Metasploit[13] se pudo identificar que tiene las capacidades de configuración necesarias con el fin de lograr la intrusión a la maquina Windows 7 x64, en la imagen siguiente muestra eternablue, que es el exploit correspondiente a la vulnerabilidad MS17-010, el cual fue identificado en la página web https://www.exploit-db.com/exploits/42031

Figura 4 Identificación del Exploit - Windows 7x64



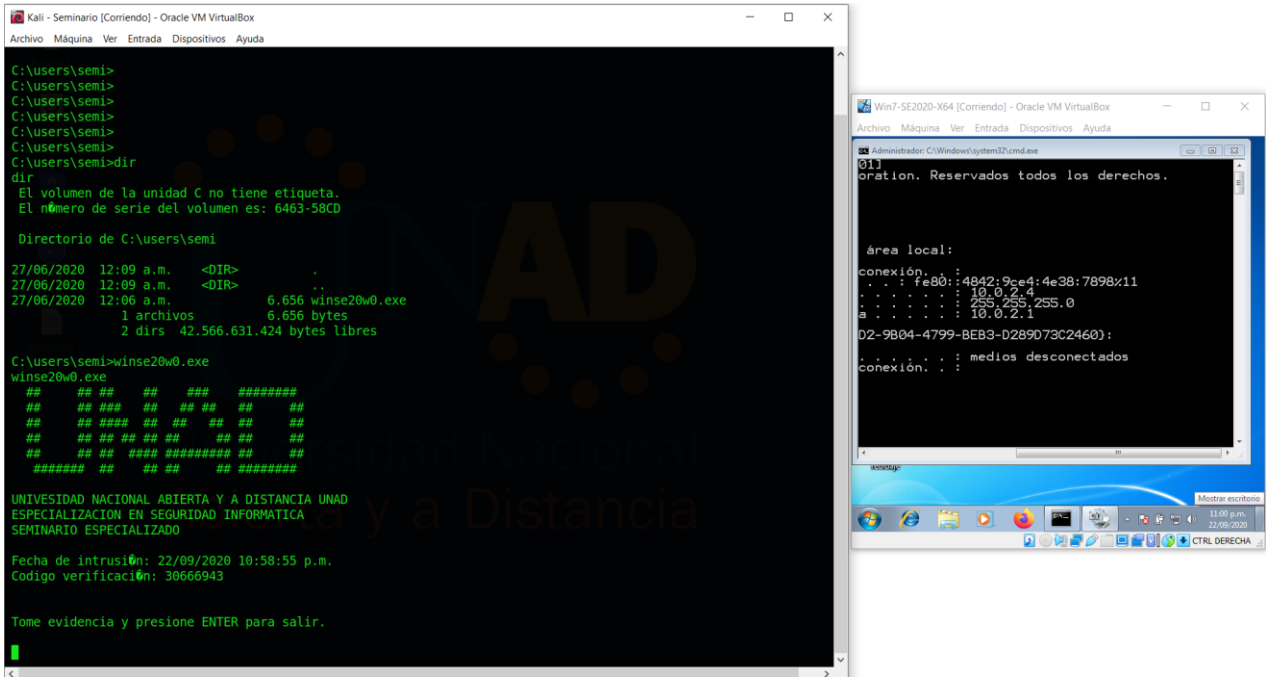
Fuente: Ejecución comando Herramienta Metasploit

[13] METASPLOIT, The world's most used penetration testing framework. [Sitio WEB]. La entidad [14, octubre, 2020]. Disponible en: https://www.metasploit.com/

2.3.5 Explotación

En esta fase se logró tener acceso a la maquina victima con Windows 7 x64, como evidencia se muestra en la siguiente imagen el objetivo alcanzado.

Figura 5 Acceso Objetivo - Maquina Windows 7x64



Fuente: Toma de evidencia – Intrusión maquina victima

2.4 ACCIONES DURANTE UN ATAQUE INFORMATICO EN TIEMPO REAL – Equipo Blue Team

2.4.1 Estrategia de Ciberseguridad Nacional[14].

Mediante del CONPES 3854 se crea la política nacional de seguridad cibernética en la que establecen lineamientos, recomendaciones y las mejores prácticas internacionales relacionadas con la gestión de riesgos de seguridad digital.

De igual forma el gobierno colombiano ha creado tres instituciones que conforman los equipos de respuestas ante incidentes de seguridad informática (CSIRT)

Figura 6 Instituciones para Informar ataques o delitos cibernéticos

Fuente: https://www.ccoc.mil.co/quienes_somos_funciones_deberes

- Centro cibernético policial (CCP): organismo encargado de la ciberseguridad del territorio colombiano, el cual ofrece el apoyo y protección ante los delitos cibernéticos https://caivirtual.policia.gov.co/
- Grupo de respuesta de emergencias cibernéticas de Colombia (COLCERT): Es el organismo clave en defensa y seguridad cibernética, su labor se basa como un mecanismo de respuesta a incidentes cibernéticos de las organizaciones, frente a emergencias de ciberseguridad que comprometan la seguridad y defensa nacional http://www.colcert.gov.co/

[14] MINTIC, Lo que usted debe saber del Conpes de Seguridad Digital. [Sitio WEB]. La entidad [05, octubre, 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/15410:Lo-que-usted-debe-saber-del-Conpes-de-Seguridad-Digital .

- Comando cibernético conjunto (CCOC): Su principal función es de prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética y pertenece al Comando de las Fuerzas Militares. https://www.ccoc.mil.co/

2.4.2 Plan de Respuesta de Incidentes

Un plan de respuesta de incidentes es un documento en donde se describe una metodología estructurada, con el cual se puede manejar y mitigar las consecuencias de incidentes de seguridad.

Con un plan bien definido, se tiene de forma clara de los activos de información a proteger, como el manejo más eficiente posible de los eventos.

Mediante la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información[15] emitida por el Ministerio de las Tecnologías y las Comunicaciones – MINTIC, se plantea una serie de actividades para dar cumplimiento con el ciclo de vida de la gestión y respuesta a un incidente de seguridad

Figura 7 Modelo de Gestión de Incidentes

Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

De acuerdo a lo anterior se recomienda que las organizaciones cuenten con un equipo de atención de incidentes de seguridad de información, los cuales tendrán la capacidad de definir los procedimientos de atención de incidentes de la misma forman tendrán a cargo lo siguiente:

[15] MINTIC, Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [Sitio WEB]. La entidad [05, octubre, 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- **Detección de Incidentes de Seguridad:** Mediante el monitoreo y la verificación de los controles poder detectar incidentes de seguridad de la información.
- **Atención de Incidentes de Seguridad:** De acuerdo con los procedimientos establecidos debe de recibir y resolver los incidentes de seguridad.
- **Recolección y Análisis de Evidencia Digital:** Cuando se requiera se debe tomar, preservar, documentar y analizar las evidencias
- **Anuncios de Seguridad:** Debe informar a los grupos de interés con todo lo relacionado con nuevas vulnerabilidades, actualizaciones y recomendaciones de seguridad.
- **Configuración y Administración de Dispositivos de seguridad Informática:** Administrara adecuadamente los elementos de seguridad informática.
- **Clasificación y priorización de servicios expuestos:** Identificara los servicios sensibles y aplicaciones expuestas con el fin de prevención y remediación de ataques.
- I**nvestigación y Desarrollo:** El equipo debe estar en constante búsqueda de productos o desarrollo de nuevas herramientas de protección con l fin de reducir las brechas de seguridad.

2.4.3 Identificación de la intrusión en Tiempo Real

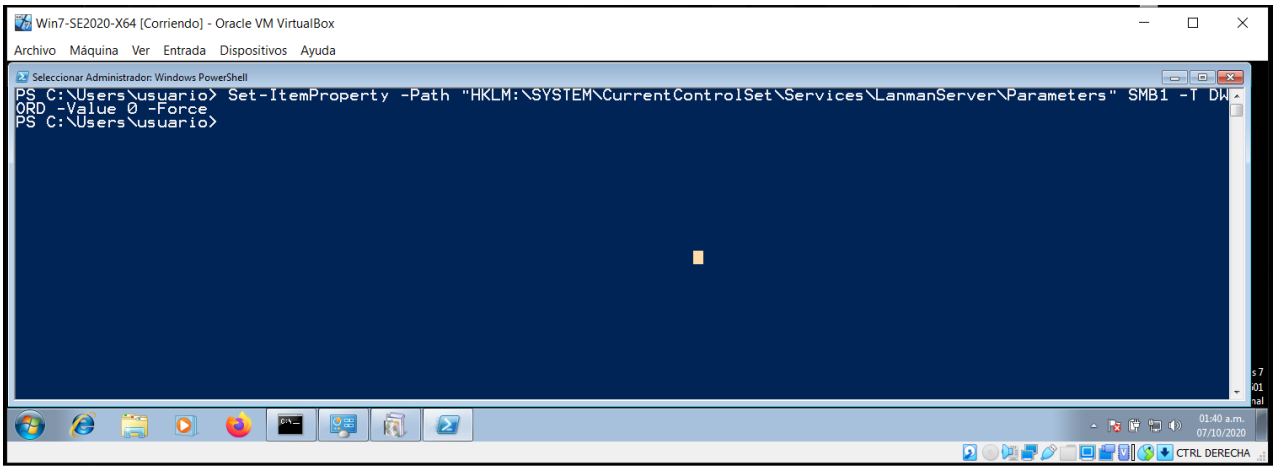
El Equipo Blue Team, en cargo de la parte ofensiva, pudo contener al ataque utilizando las herramientas y comandos propios del Sistema Operativo Windows 7, como la consola CMD y el comando NetStat y la consola del administrador de tareas, que permite identifica las conexiones que establecieron en el equipo victima

2.4.4 Aplicación de Solución

De acuerdo a la página web página web https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/, realiza las recomendaciones para mitigar el fallo de seguridad, se aplicó la siguiente acción.

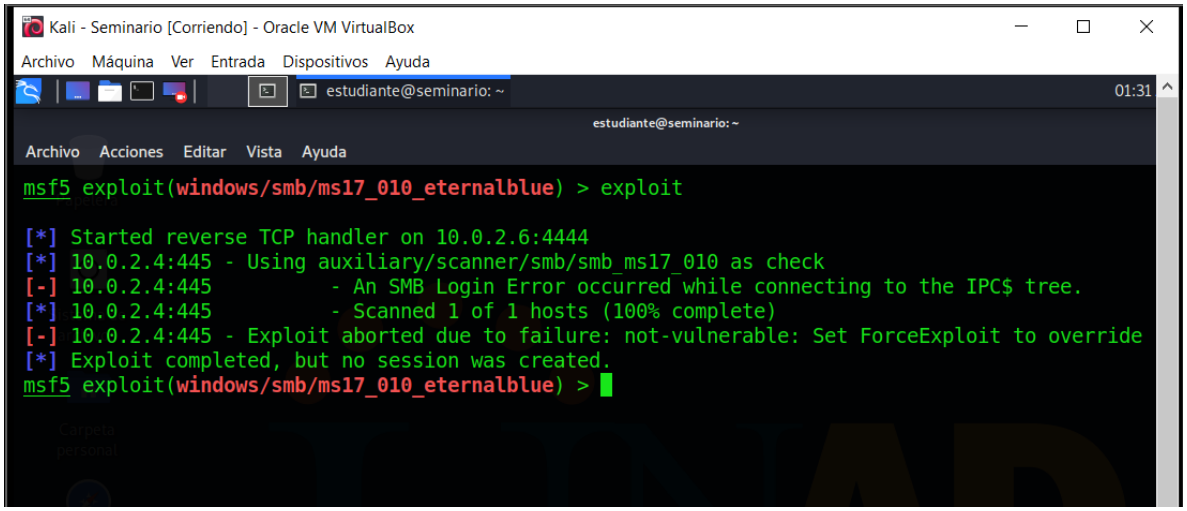
Desactive SMBv1 en todos los sistemas y utilice SMBv2 o SMBv3 después de las pruebas adecuadas.

Figura 8 Desactivar Protocolo SMBv1



Fuente: Aplicación del Comando que desactiva el protocolo

Figura 9 Exploit después de desactivar el protocolo SMBv1



Fuente: Resultado de ejecutar el comando exploit a la maquina Windows 7 x64

- Ejecute todo el software como un usuario sin privilegios (uno sin privilegios administrativos) para disminuir los efectos de un ataque exitoso.
- Recuerde a los usuarios que no deben visitar sitios web que no sean de confianza ni seguir enlaces proporcionados por fuentes desconocidas o no confiables.
- Informar y educar a los usuarios sobre las amenazas que plantean los enlaces de hipertexto contenidos en correos electrónicos o archivos adjuntos, especialmente aquellos de fuentes no confiables.
- Aplicar el principio de privilegio mínimo a todos los sistemas y servicios

2.4.5 Maquina Windows 7x86

Teniendo en cuenta que esta máquina presentaba problemas de pantalla azul al realizar la intrusión se determinó por su incompatibilidad con el exploit por motivos de arquitectura la cual es de 32 bits.

2.4.6 Link Video https://youtu.be/1wWX6Y9x3Pk

3 CRONOGRAMA

Momento de la e-evaluación	Nombre de la unidad	Nombre de la actividad	Descripción de la actividad	Tipo de actividad	Peso evaluativo (en puntajes)	Actividad inicia en:	Actividad finaliza en:	Alerta de cierre en:	Fecha de entrega realimentación
Final	-	Etapa 5 - Socialización de informe técnico	*Construye un informe técnico. Elabora un vídeo sustentado. *Entorno del aula donde se realiza: entorno de aprendizaje. Resultado: informe técnico y elaboración de un vídeo.	Individual	125	08/OCT/2020 00:00	16/OCT/2020 23:55		17/OCT/2020 - 23/OCT/2020

CONCLUSIONES

Para que el equipo Red Team lograra identificar porqué medio o proceso se está generando una serie de fuga de información al interior de la organización, tomo como apoyo una metodología estructurada que mediante a la ejecución de cada etapa ordena, logro realizar la intrusión con la ayuda imprescindible de herramientas especializadas en pestenting y auditoria en seguridad informática.

Así mismo el equipo Blue Team logro identificar a través las vulnerabilidades los fallos de seguridad que los equipos afectados presentaban, de igual forma con herramientas propias del sistema operativo pudo contener el ataque oportunamente.

De igual forma ambos equipos el Red Team y Blue Team, se apoyaron en páginas web especializadas en ciberseguridad, que les permitieron conocer en detalle las características de la vulnerabilidad y el fallo de seguridad que presentaba los equipos involucrados en el incidente.

Se utilizaron las siguientes herramientas en el desarrollo del ejercicio: VirtualBox Versión 6.1.12 r139181 (Qt5.6.2), Kali Linux, Nmap, Metasploit, Consola CMD de Windows.

RECOMENDACIONES

Fortalecer las 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 la organización.

Implementar soluciones de hardware o software que contemple herramientas SIEM (información de seguridad y gestión de eventos), con el fin de generar la identificación, el análisis y la recuperación más rápida de los eventos de seguridad, en donde la finalidad de esta herramienta es detectar y prevenir amenazas, previenen ataques antes que se realicen gracias a la información que se recopila y se centraliza correlacionando información de diferentes fuentes las actividades y procesos y las conexiones de redes que estén cubiertas por el SIEM.

Apoyarse en la página web CIS “CENTER FOR INTERNET SECURITY”, que mediante la aplicación de sus controles aplican un estándar y las mejores prácticas reconocidas para proteger las infraestructuras TI y gestionando los riesgos de ciberseguridad.

Implementar medidas de Hardening o endurecimiento informático, con el fin de realizan ajustes para la de reducción de vulnerabilidades en el sistema, estableciendo medidas y aumentando su nivel de seguridad, con el fin de estar preparados o mitigar para un ataque informático como:

- Cambiar todas las claves que tengamos por defecto
- Deshabilitar el acceso remoto
- Desinstalación de todo el software que sea innecesario
- Dar de baja todos los usuarios que sean innecesarios
- Deshabilitar todos los servicios que no se estén utilizando
- Aumentar la seguridad de los servicios o procesos que se utilizaran
- Cerrar puertos que se encuentren sin uso
- Hacer copias de seguridad
- Instalar un Firewall
- Actualizar Sistemas Operativos para obtener los parches de seguridad

    - Protege contra los exploit
- Eliminar lo innecesario del Sistema
- Conciencia en seguridad informática en los usuarios
    - No abrir archivos desconocidos
    - Tener contraseñas robustas
    - Tener cuidado con los correos electrónicos
    - Tener actualizado el sistema operativo
    - Tener activo el programa antivirus
- Establecer permisos y niveles de acceso
    - Protege contra intrusos

De igual forma se recomienda las siguientes páginas web que están en constante actualización en temas de vulnerabilidades y seguridad informática como:

- https://www.cisecurity.org/: Center for Internet Security
- https://nvd.nist.gov/ : National Vulnerability Database
- https://attack.mitre.org/: MITRE ATT&CK®
- https://www.exploit-db.com/ : Exploit Databse
- https://www.metasploit.com/ : Penetration Testing Framework

BIBLIOGRAFÍA

ATTACK.MITRE,Enterprise Matrix. [Sitio WEB]. La entidad 14, octubre, 2020]. Disponible en: https://attack.mitre.org/matrices/enterprise/

COMMON VULNERABILITIES AND EXPOSURES, CVE-2017-0144. [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

COPNIA, Ley 842 de 2003. [Sitio WEB]. La entidad 14, octubre, 2020]. Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

CISECURITY, Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution. [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/

CISECURITY, MS-ISAC Security Primer – EternalBlue. [Sitio WEB]. La entidad [14, octubre, 2020]. Disponible en: https://www.cisecurity.org/white-papers/ms-isac-security-primer-eternal-blue/

ESCUELA POLITECNICA NACIONAL, MS17-010 EternalBlue SMB Remote Windows. [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://www.csirt-epn.edu.ec/servicios/vulnerabilidades/58-ms17-010

EXPLOIT-DB,Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010).[Sitio WEB]. La entidad [14, octubre, 2020]. Disponible en: https://www.exploit-db.com/exploits/42031

GLOBETESTIN, Red Team y Blue Team. [Sitio WEB]. La entidad [14, octubre, 2020]. Disponible en: https://www.globetesting.com/static_block/red-team-blue-team/

METASPLOIT, The world's most used penetration testing framework. [Sitio WEB]. La entidad [14, octubre, 2020]. Disponible en: https://www.metasploit.com/

MICROSOFT, Microsoft Security Bulletin MS17-010 – Critical. [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010?redirectedfrom=MSDN

MINTC, Ley 1273 de 2009. [Sitio WEB]. La entidad 14, octubre, 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

MINTC, Decreto 1377 de 2013. [Sitio WEB]. La entidad 14, octubre, 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/4274:Decreto-1377-de-2013
MINTIC, Lo que usted debe saber del Conpes de Seguridad Digital. [Sitio WEB]. La entidad [05, octubre, 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/15410:Lo-que-usted-debe-saber-del-Conpes-de-Seguridad-Digital.

MINTIC, Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [Sitio WEB]. La entidad [05, octubre, 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

NAMAP, Guía de referencia de Nmap (Página de manual). [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://nmap.org/man/es/index.html#man-description
NATIONAL VULNERABILITY DATABASE, CVE-2017-0144 Detail [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2017-0144

OPENWEBINARS, Qué es un Payload. [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://openwebinars.net/blog/que-es-payload/

OPENWEBINARS, Qué es un Payload.). [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://openwebinars.net/blog/que-es-payload/

PENTEST-STANDARD, High Level Organization of the Standard. [Sitio WEB]. La entidad [14, Octubre, 2020]. Disponible en: http://www.pentest-standard.org/index.php/Main_Page
RAPID7, Quick Start Guide. [Sitio WEB]. La entidad [03, septiembre, 2020]. Disponible en: https://docs.rapid7.com/metasploit/

SEMANA, Atrapados en la Andrómeda, [Sitio WEB]. La entidad [10 septiembre, 2020]. Disponible en: https://www.semana.com/opinion/articulo/maria-jimena-duzan-atrapados-en-la-andromeda/377305-3/

SUPPORT.MICROSOFTWindows de 32 y 64 bits: preguntas frecuentes. [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://support.microsoft.com/es-co/help/15056/windows-32-64-bit-faq

THEHACKERWAY, Conceptos Básicos de Meterpreter – MetaSploit Framework. [Sitio WEB]. La entidad [21, septiembre, 2020]. Disponible en: https://thehackerway.com/2011/04/26/conceptos-basicos-de-meterpreter-metasploit-framework/#:~:text=Meterpreter%20es%20un%20interprete%20de,antivirus%2C%20firewall%20o%20IDS%20ya

WELIVESECURITY, ¿Sabes qué es un exploit y cómo funciona?). [Sitio WEB]. La entidad [22, septiembre, 2020]. Disponible en: https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/