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

ROSA MELINA MURILLO COCUNUBO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
EL ESPINO
2020

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

ROSA MELINA MURILLO COCUNUBO

M.Sc. JOHN FREDDY QUINTERO
Director de curso.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
EL ESPINO
2020

CONTENIDO

pág.

LISTA DE TABLAS

pág.

GLOSARIO

ACCESO NO AUTORIZADO: es cuando alguien obtiene acceso a un servidor, sitio web u otros datos confidenciales utilizando los detalles de la cuenta de otra persona.

ADMINISTRACIÓN DE PARCHES: es una estrategia que se implementa para administrar actualizaciones para aplicaciones de software.

ADWARE: software que muestra o descarga material automáticamente cuando un usuario está desconectado.

AMENAZA: es una acción o evento que puede comprometer la seguridad.

AMENAZAS PERSISTENTES AVANZADAS: cuando un usuario no autorizado invade una red, permanece durante un período prolongado de tiempo y roba datos sin dañar la red.

ANTIVIRUS O ANTIMALWARE: es un software que opera en diferentes sistemas operativos y que se utiliza para evitar software malicioso.

ATAQUE DE FUERZA BRUTA: cuando un atacante ingresa muchas contraseñas con la esperanza de que finalmente las adivine correctamente.

ATAQUE: es un asalto a la seguridad del sistema que una persona o máquina envía a un sistema. Viola la seguridad.

BLUE TEAM: El grupo de defensa en un simulacro de ataque a la seguridad cibernética. El Equipo Azul defiende los sistemas de información de la empresa mientras que el Equipo Rojo ataca.

CORTAFUEGOS: es un software o hardware que se utiliza para filtrar el tráfico de red según las reglas.
DDoS: abreviatura de denegación de servicio distribuida, un ataque que se produce cuando varios sistemas se infiltran en una red objetivo. Normalmente, un ataque global.

EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS (CIRT): Un equipo de investigadores centrado en las brechas de seguridad de la red. Su función es analizar

cómo ocurrió el incidente y qué información se ha visto afectada / perdida. Luego usan esta información para proporcionar una respuesta.

ETHICAL HACKING: la práctica de localizar vulnerabilidades y debilidades en los sistemas de información y las computadoras duplicando las acciones y la intención de los piratas informáticos malintencionados que buscan eludir la seguridad y buscar brechas en los sistemas que pueden explotarse.

EVALUACIÓN DE RIESGOS: El proceso de identificación, análisis y evaluación de riesgos.

EXPLOIT: El acto de aprovechar una vulnerabilidad en un sistema de información. También se usa para describir una técnica que se usa para violar la seguridad de la red.

GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD (SIEM): Proceso en el que se agrega, ordena y correlaciona la información de la red para detectar actividades sospechosas.

INCIDENTE: Cualquier incumplimiento de las reglas de seguridad de un sistema o servicio. Esto incluye los intentos de obtener acceso no autorizado, el uso no autorizado de sistemas para el procesamiento o almacenamiento de datos, interrupción maliciosa o denegación de servicio y cambios en el firmware, software o hardware de un sistema sin el consentimiento del propietario.

INGENIERÍA SOCIAL: es una técnica que utiliza un pirata informático para robar datos de una persona con diferentes fines mediante la manipulación psicológica combinada con escenas sociales.

PHARMING: Un ataque a la infraestructura de la red donde un usuario es redirigido a un sitio web ilegítimo, a pesar de haber ingresado la dirección correcta.

PHISHING: método para obtener información del usuario a través de comunicaciones fraudulentas dirigidas directamente a personas. Esto generalmente se hace a través de correos electrónicos disfrazados como provenientes de una fuente legítima, pero entrega la información del objetivo a la fuente real del hacker.

PRIVILEGIO DE ADMINISTRADOR: tener el control máximo de cualquier sistema dado.

PROTECCIÓN DE DATOS: también conocida como privacidad de datos y privacidad de la información, el proceso de salvaguardar la información para que no caiga en las manos equivocadas.

PRUEBAS DE PENETRACIÓN: Una prueba diseñada para explorar y exponer las debilidades de seguridad en un sistema de información para que puedan solucionarse.

PUERTA TRASERA: una forma alternativa de acceder a software o hardware, normalmente no autorizado e implantado por agencias de inteligencia.

RANSOMWARE: una forma de malware que se utiliza para amenazar a las víctimas al bloquear, publicar o corromper sus datos a menos que se pague el rescate.

RED PRIVADA VIRTUAL (VPN): Enlace (s) entre computadoras o redes de área local a través de diferentes ubicaciones utilizando una red de área amplia a la que otros usuarios de la red de área extensa no pueden acceder ni a la que pueden acceder.

RED TEAM: Un grupo autorizado y organizado para emular las capacidades de ataque o explotación de un adversario potencial contra la postura de seguridad cibernética de una empresa.

RIESGO: Algo que podría provocar que una organización no cumpla con alguno de sus objetivos.

SERVIDOR: Computadora que proporciona datos o servicios a otras computadoras a través de una red.

VECTOR DE ATAQUE: técnica que utiliza un pirata informático para obtener acceso a una computadora o red con el fin de lograr un resultado malicioso.

VULNERABILIDAD: es una debilidad, un problema de diseño o un error de implementación en un sistema que puede conducir a un evento inesperado e indeseable con respecto al sistema de seguridad.

RESUMEN

En el presente documento encontramos el consolidado total del desarrollo de las diferentes fases que se llevaron a cabo a lo largo de las 8 semanas de trabajo, actualmente se mencionan los términos de "Red Team" y "Blue Team". Donde un grupo de estos profesionales son quienes se encargan de imitar diferentes técnicas de ataque que comúnmente los enemigos pueden usar, el otro equipo hace la función de defensiva.

Los profesionales en Red Team están en la capacidad de detectar y responder a un ataque en tiempo real, en el desarrollo practico se realizó una penetración utilizando la herramienta de escaneo Nmap, conocida herramienta de examen de puertos, el escaneo es regularmente una parte del período de observación de una prueba de penetración en este documento se encuentra la información obtenida plasmada en un informe técnico para la organización WhiteHose Security.

En este informe técnico se encuentra plasmado las conclusiones del desarrollo de las 4 etapas del desarrollo del seminario, y todas las recomendaciones sobre los hallazgos que se encontraron a lo largo del desarrollo del ejercicio practico y las consecuencias legales que acarreara el incumplimiento de la ley 1273 de 2009, normatividad colombiana sobre los delitos informáticos, protección de datos personales. Todo profesional debe seguir su ejercicio profesional dentro de un contexto ético y legal para evitar ser atraído por actos ilegales ya que estamos regidos por un marco normativo bastante amplio y de ser más grave e incurrir en un concurso de delitos nos regirá el código y procedimiento penales.

Palabras Claves: Blue Team, Red Team, Pentesting, Vulnerabilidades. .

ABSTRACT

In this document we find the total consolidation of the development of the different phases that were carried out throughout the 8 weeks of work, currently the terms "Red Team" and "Blue Team" are mentioned. Where a group of these professionals are the ones in charge of imitating different attack techniques that enemies can commonly use, the other team performs the defensive function.

Professionals in Red Team are able to detect and respond to an attack in real time, in the practical development a penetration was performed using the Nmap scanning tool, a well-known port examination tool, the scan is regularly a part of the period From the observation of a penetration test in this document is the information obtained reflected in a technical report for the WhiteHose Security organization.

This technical report contains the conclusions of the development of the 4 stages of the development of the seminar, and all the recommendations on the findings that were found throughout the development of the practical exercise and the legal consequences that the breach of law 1273 would entail 2009, Colombian regulations on computer crimes, protection of personal data. All professionals must follow their professional practice within an ethical and legal context to avoid being attracted by illegal acts since we are governed by a fairly broad regulatory framework and if it is more serious and incurring a crime contest, we will be governed by the criminal code and procedure .

Keywords: Blue Team, Red Team, Pentesting, Vulnerabilities.

INTRODUCCIÓN

El informe de prueba de penetración del ejercicio práctico del seminario especializado sobre seguridad ofensiva contiene todos los esfuerzos que se realizaron para aprobar el curso. Este informe contiene todos los datos de laboratorio en el formato de plantilla de informe técnico. El propósito de este informe es asegurar que el estudiante tenga una comprensión completa de las metodologías de pruebas de penetración, así como el conocimiento técnico.

El grupo de profesionales que integran el Blue Team y Red Team dentro de sus funciones están probar controles en tiempo real y simulando el tipo de enfoque que es probable que los intrusos utilicen en un ataque real. Esto cambia la prueba de pasiva a activa. En lugar de trabajar para burlarse unos de otros, los equipos pueden aplicar los entornos de ataque más agresivos y llevar a cabo escenarios hipotéticos más complejos a través de los cuales los controles y procesos de seguridad se pueden comprender de manera más completa y corregir antes de un compromiso.

Una implementación básica se puede completar fácilmente en menos de un día, proporcionando al Blue Team un mecanismo de detección adicional que se integra con el entorno operativo. Esto crea más oportunidades para detectar cuándo los profesionales de Red Team pasa por alto un control defensivo, lo que obliga a los miembros del equipo a ser más deliberados con sus acciones y hace que los escenarios de ataque simulados sean más realistas. También ofrece una prueba más real de la capacidad de recuperación de la pila de seguridad de la organización y los procesos que tiene para responder a un incidente.

Las pruebas de penetración son una herramienta fundamental para analizar la seguridad de los sistemas de TI. Este informe técnico nos habla del uso adecuado de las pruebas de penetración. Las pruebas de penetración deben verse como un método para obtener seguridad en los procesos de evaluación y gestión de vulnerabilidades de su organización, no como un método principal para identificar vulnerabilidades.

JUSTIFICACIÓN

El delito informático o el ciberdelito es la acción ilegal que involucra una computadora y una red. Para estos delitos las conductas delictivas que se realizan son: acceder, impedir, interceptar, borrar, alterar, traficar, vender, extraer, producir, compilar, divulgar, hurtar, transferir, suplantar, violar, dañar, programar estas conductas se pueden cometer contra cualquier persona u organización.

Los delitos informáticos que no solo afectan a Colombia si a todos los países del mundo, debido al crecimiento de los sistemas de información y el uso de medios electrónicos y el estado nacional colombiano modifico el código penal colombiano en aras de especificar mejor los delitos informáticos y cuáles son sus limitaciones, que van en contra la de los pilares de la seguridad de la información confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Este trabajo de grado se ocupa de aclarar las disposiciones legales de los delitos informáticos teniendo en cuenta el crecimiento de equipos tecnológicos e inteligentes y su dependencia de la red inalámbrica esto generando aumento en la vulnerabilidad frente a los ataques cibernéticos y lo que busca el gobierno es combatir y castigar el delito informático e incluyéndolo en el derecho penal colombiano.

1 OBJETIVOS

1.1 OBJETIVOS GENERAL

Elaborar una guía para la identificación del problema específico en temas técnicos que se ejecutan en equipos Blue Team y Red Team a lo largo del desarrollo del seminario especializado.

1.2 OBJETIVOS ESPECÍFICOS

- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

- Presentar informe técnico sobre el ejercicio planteado en el curso de Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

- Sustentar el informe técnico mediante un video

2 MARCO TEORICO

En Colombia existen leyes que velan por el amparo de la información. Para delitos informáticos existe la Ley 1273 de 2009 publicada el 5 de enero, la cual influye en el amparo de la información. Inmersa a esta ley, existen datos puntuales nombrados en artículos, que citan y dan a conocer las reglamentaciones y las sensaciones a las que están expuestas las personas que cometan dicho delito.

Artículo 269A: Acceso abusivo a un sistema informático: En este artículo exponen el abuso al ingresar a un sistema informático y extraer sus datos.

Artículo 269C: Interceptación de datos informáticos: cualquier personal que, sin ordenanza legal, ni permiso de la entidad, intercepte datos personales de los usuarios para beneficio propio que le permita enriquecerse de manera fraudulenta viola la normatividad expuesta en el artículo 269C.

Artículo 269F: Violación de datos personales. es pertinente extraer a este documento lo relacionado en el artículo 269F ya que la persona que cometa delito utilizando para provecho propio la información privada de los usuarios y en algún caso su cuenta bancaria para extraer dinero. Implica una violación de información personal y deberá cumplir una condena de 4 a 8 años de cárcel y 100 a 1000 salarios vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales: se expresa que la persona que envié un link para cometer actividades ilegales, hacer ingresar al usuario a una IP diferente u otro sitio que pueda obtener los resultados del delito planeado será sancionado y, por ende, debe pagar una condena de 4 a 8 años de cárcel. A eso sumarle 100 a 1000 salarios mínimos mensuales

Artículo 269I: este menciona que robo que es realizado por medios digitales e iguales, al burlar la seguridad informática, hace relación este artículo la conducta y manipulación de los sistemas informáticos, los sistemas electrónicos u cualquier medio similar, o herramientas que suplanten a usuarios de los parámetros de autenticación establecidos y esto puede incurrir en el artículo 240 donde se habla de las penas de prisión de 6 a 14 años por delitos establecidos.

Artículo 269J: Transferencia no consentida de activos: Es de saber que las transferencias de activos no autorizada o realizadas arbitrariamente es un delito y esto incluye cumplir una condena de 4 años a 10 años de cárcel.

Ley 1712 del 6 de marzo de 2014 Es la ley de acceso a la información pública, donde la transparencia en la información hacia todos los personales y mecanismo de protección de otros derechos fundamentales.
El acceso de la información y transparencia ubicada dentro de las plataformas electrónicas y se debe implementar en todas las entidades públicas, los empleados deben conocer de bien cerca que tipo de información si es publica y de igual forma dar acceso con transparencia a los usuarios protegiendo los datos personales.

2.1 ¿QUÉ SON LAS PRUEBAS DE PENETRACIÓN?

Definiremos las pruebas de penetración como: "Un método para obtener seguridad en la seguridad de un sistema de TI al intentar violar parte o toda la seguridad de ese sistema, utilizando las mismas herramientas y técnicas que un adversario. " Las pruebas de penetración deben verse como un método para obtener seguridad en los procesos de evaluación y gestión de vulnerabilidades de su organización, no como un método principal para identificar vulnerabilidades.

¿Qué tipo de sistema debería probarse?

La prueba de penetración es un método apropiado para identificar los riesgos presentes en un sistema operativo específico que consta de productos y servicios de múltiples proveedores. También podría aplicarse de manera útil a sistemas y aplicaciones desarrollados "internamente". Las pruebas de penetración son una herramienta fundamental para analizar la seguridad de los sistemas de TI, pero no es una fórmula mágica.

Normalmente, las pruebas de penetración se utilizan para identificar el nivel de riesgo técnico que emana de las vulnerabilidades de software y hardware. Exactamente qué técnicas se utilizan, qué objetivos están permitidos, cuánto conocimiento del sistema se da a los probadores de antemano y cuánto conocimiento de la prueba se da a los administradores del sistema pueden variar dentro del mismo régimen de prueba. Una prueba de penetración bien definida puede dar confianza en que los productos y controles de seguridad probados se han configurado de acuerdo con las buenas prácticas y que

no existen vulnerabilidades comunes o conocidas públicamente en los componentes probados, en el momento de la prueba.

2.1.1 Tipos de pruebas

Los probadores de penetración se pueden utilizar para realizar una amplia gama de pruebas. La siguiente lista es ilustrativa, no exhaustiva.

- Base de prueba

Las pruebas pueden ser realizadas por probadores armados con diferentes cantidades de información sobre su sistema:

Prueba de caja blanca: la información completa sobre el objetivo se comparte con los probadores. Este tipo de prueba confirma la eficacia de la evaluación de vulnerabilidades internas y los controles de gestión al identificar la existencia de vulnerabilidades de software conocidas y configuraciones erróneas comunes en los sistemas de una organización.

Prueba de caja negra: no se comparte información con los probadores sobre las partes internas del objetivo. Este tipo de prueba se realiza desde una perspectiva externa y tiene como objetivo identificar formas de acceder a los activos de TI internos de una organización. Esto modela con mayor precisión el riesgo que enfrentan los atacantes que son desconocidos o no están afiliados a la organización objetivo. Sin embargo, la falta de información también puede provocar que las vulnerabilidades permanezcan sin descubrir en el tiempo asignado para las pruebas.

- Tipo de prueba

Cada una de las pruebas descritas a continuación se puede ejecutar como una operación de caja negra o caja blanca:

Identificación de vulnerabilidades en software a medida o de nicho: más comúnmente utilizado en aplicaciones web. Este tipo de prueba debe brindar retroalimentación a los desarrolladores sobre las prácticas de codificación que evitan introducir las categorías de vulnerabilidad identificadas.

Pruebas basadas en escenarios destinadas a identificar vulnerabilidades: los probadores de penetración exploran un escenario en particular para descubrir si conduce a una vulnerabilidad en sus defensas. Los escenarios incluyen: computadora portátil perdida, dispositivo no autorizado conectado a la red interna y host DMZ comprometido, pero hay

muchos otros posibles. Debe considerar, basándose en incidentes anteriores, qué escenarios son más relevantes para su organización.

Pruebas basadas en escenarios de la capacidad de detección y respuesta: en esta versión de las pruebas basadas en escenarios, el objetivo es también medir las capacidades de detección y respuesta que tiene su organización. Esto le ayudará a comprender su eficacia y cobertura en el escenario particular. Esta es un área de trabajo actual del NCSC, más información estará disponible en breve, comuníquese con nosotros si tiene una necesidad particular en esta área.

2.2 METODOLOGIA

Para que se pudiere realizar cada una de las pruebas técnicas para el desarrollo de este seminario especializado se contaron con una serie de etapas necesarias donde se estableció una metodología de desarrollo para el pentesting como se describe a continuación.

2.2.1 Metodología de prueba planteada

Para iniciar el desarrollo de la ejecución de pentesting de la empresa WHITEHOSE SECURITY como se muestra en el siguiente diagrama siendo estas las etapas consideradas para el desarrollo del ejercicio.

Ilustración 1. Metodología propuesta

Fuente: Autor

Reconocimiento

Esta es una etapa muy importante ya que es donde se recopila la mayor información posible acerca de lo que va ser nuestro objetivo, equipos, servidores, dominios de páginas web, DNS, rangos de IP, ISP, versiones de los S.O, versiones de aplicaciones que se utilizan, correos electrónicos, nombres de personas u o empresas, direcciones o cualquier dato que pueda ser muy útil, con esta información podemos ver e identificar si existe alguna vulnerabilidad la cual podamos explotar para lograr un objetivo. El conocer estas versiones puede dejar ver por dónde podemos iniciar a la hora de hacer el pentesting o en algún momento determinado, se puede usar el Free Mind para organizar la información mediante un mapa mental, en esta fase de reconocimiento se clasifica en dos; el reconocimiento pasivo y reconocimiento activo, el reconocimiento pasivo es el que nosotros recabamos información sin tener interactuar con el objetivo es esa información pública en internet y el reconocimiento activo implica interactuar con el objetivo como enviar correos para recolectar información.

Escaneo

En esta segunda fase ya tenemos una visión general de nuestro objetivo y se inicia a identificar las vulnerabilidades o fallas que están en evidencia y a las que se puede acceder si se encuentran brechas de seguridad o puertos abiertos.

La etapa de escaneo implica el uso de herramientas automatizadas para analizar los sistemas de destino. Los pentesters comúnmente realizan análisis estático o análisis dinámico, verificando el código del sistema en busca de errores o brechas de seguridad. También ejecutan análisis de vulnerabilidades en busca de componentes antiguos o sin parches que puedan ser vulnerables a exploits conocidos.

Explotación

Es donde ya iniciamos el pentesting, obtener acceso para explotar alguna vulnerabilidad que fue previamente identificada, este parte del proceso se hace mediante el uso de una herramienta de exploit, cabe resaltar que existen tres clases de exploit como son: remotos, local, cliente.
En esta parte del proceso podemos se puede hacer uso de Fuerza bruta, captura de información de la red, buscar lanzar exploit conocidos a servicios encontrados, escalar privilegios, Dum de formación entre otras con el fin de recolectar información para general un informe final.

Basado en la etapa anterior, el pentester selecciona un punto débil en el sistema de destino que puede usar para penetrar. Pueden realizar ataques de fuerza bruta o de descifrado de contraseñas para atravesar una autenticación débil, realizar inyección de SQL o secuencias de comandos entre sitios para ejecutar código malicioso en el sistema de destino o enviar malware a un sistema dentro del perímetro de seguridad.

Pos explotación

El pentester normalmente actuará como una amenaza persistente avanzada (APT), buscando formas de escalar privilegios y realizar movimientos laterales para obtener acceso a activos sensibles. De esta manera, pueden ayudar a la organización a descubrir vulnerabilidades de los sistemas internos (no solo los implementados en el perímetro de seguridad o en el borde de la red) y la capacidad del equipo de seguridad para detectar actividad maliciosa dentro de la red.

Reporte

En esta última fase se hace la realización del informe donde se alerta a la organización si se encontró algún fallo crítico, se presenta la definición de modelo para la tabla de riesgos, informe técnico ejecutivo y finalmente efectuar la sustentación de los resultados obtenidos del trabajo.
Al final de la prueba de penetración, el pentester compilará un informe que detalla qué vulnerabilidades descubrieron en su prueba (incluidas aquellas que no fueron realmente explotadas), cómo violaron el sistema, qué sistemas internos o datos confidenciales pudieron comprometer, si fueron detectados y cómo respondió la organización. Luego, la organización puede usar estos datos para remediar vulnerabilidades, reforzar los procesos de seguridad y ajustar la configuración de las herramientas de seguridad.

2.2.2 Descripción del banco de trabajo

El banco de trabajo debe estar basado en herramientas software Opensource, la recursividad será vital en este proceso.

- Un windows 7 X86.
- Un windows 7 X64.
- Máquina virtual con distribución de Kali Linux.

La máquina de donde se harán los ataques será desde la maquina Kali Linux y las maquinas Un Windows 7 X86, Un Windows 7 X64 serán los objetivos.

2.2.3 Herramientas

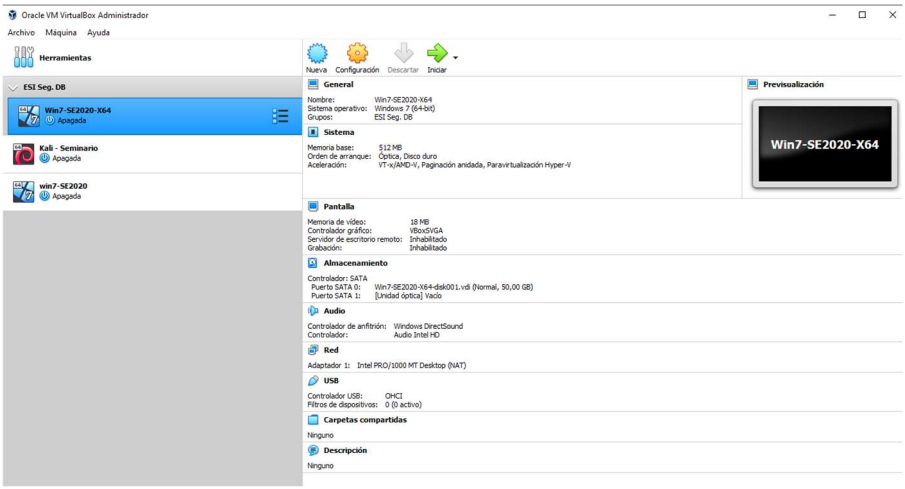
En este apartado se describe de forma general las principales herramientas que fueron utilizadas por el equipo de seguridad ofensiva en la ejecución de prueba técnica.

Virtual box:

VirtualBox es una GUI y una herramienta de línea de comandos que hace posible implementar servidores, escritorios y sistemas operativos integrados como VM. Un solo host de VirtualBox puede implementar tantas VM invitadas como el hardware del host pueda manejar.

VirtualBox consta de anfitriones e invitados. El host aloja el software VirtualBox que luego puede implementar a los invitados. Un invitado es cualquier sistema operativo compatible que se ejecute como una máquina virtual. Un host de VirtualBox se puede ejecutar en Linux, Windows o macOS, mientras que un invitado de VirtualBox puede consistir en cualquier distribución de Linux, Solaris, macOS, BSD, IBM OS / 2 o Windows. Para ejecutar macOS o Windows como una máquina virtual, debe tener una copia con licencia del sistema operativo en cuestión.

Imagen 1. Pantalla inicial de Virtual Box

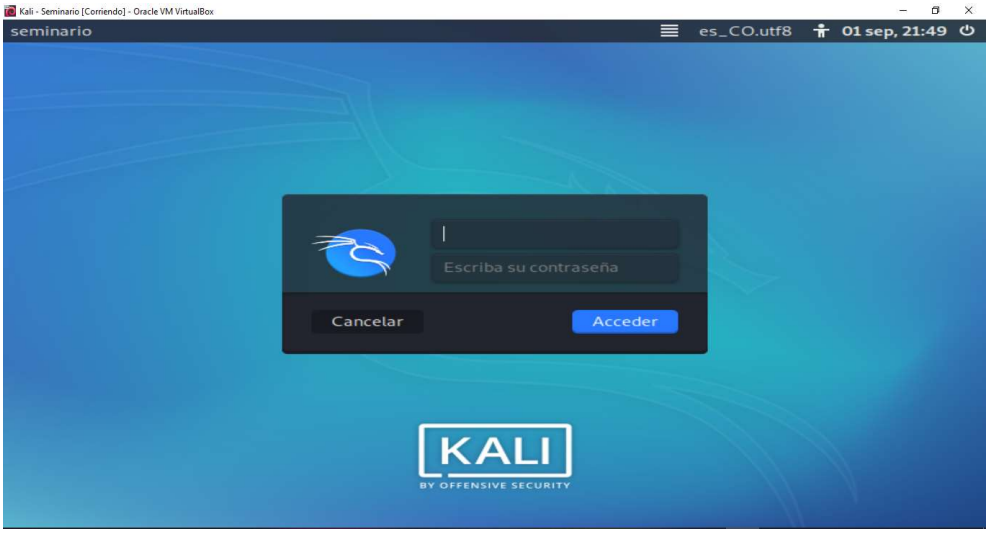


Fuente: Autor

Kali Linux

Kali Linux es una versión basada en Debian del sistema operativo Linux, que se ha creado específicamente para pruebas de penetración y análisis forense digital. Uno de los aspectos principales de Kali Linux es su conjunto de herramientas de seguridad preinstaladas que se puede utilizar para una variedad de propósitos de ciberseguridad, incluidas las pruebas de penetración y la explotación. Kali Linux se puede descargar gratis.

Imagen 2. Pantalla inicial de Kali linux

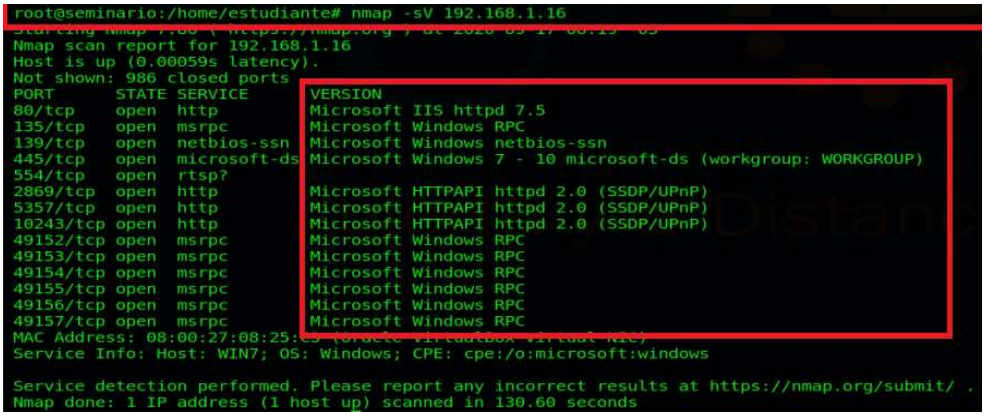


Fuente: Autor

Nmap

Se puede definir como una herramienta de exploración de red y auditoría de seguridad. Resulta útil para los administradores de sistemas y de comunicaciones, para la realización de tareas como inventario de red o monitorización de sistemas y servicios. La herramienta puede averiguar los hosts que están levantados, los servicios que ofrecen y el sistema operativo de los mismos. La herramienta está soportada por múltiples sistemas operativos: Windows, Linux, Microsoft, Mac OS X entre otros.

Imagen 3. Escaneo con Nmap



Fuente: Autor

Metasploit

Metasploit es una plataforma de pruebas de penetración que le permite encontrar, explotar y validar vulnerabilidades La herramienta Metasploit es una herramienta de código abierto que se usa para desarrollar y ejecutar código de explotación. Estos exploits se utilizan contra un objetivo remoto. El objetivo puede ser cualquier máquina. El

Metasploit frameworks contiene una gran cantidad de bases de datos de exploits disponibles para el público. Estos exploits se prueban y funcionan correctamente. Metasploit tiene buenas disposiciones para la recopilación de información y el escaneo de vulnerabilidades, debido a su integración con el marco drivers y configuración con varios controladores de bases de datos, como MySQL, SQLite y PostgreSQL.

Imagen 4. Inicio con Metasploit

Fuente: Autor

2.2.4 Plan de trabajo

Tabla 1. Plan de actividades a desarrollar

TAREA POR DESARROLLAR	DURACIÓN	FECHA
Descubrimiento	3 días	10 de septiembre
Escaneo de servicios y vulnerabilidades	3 días	17 de septiembre
Explotación de vulnerabilidades	10 días	27 de septiembre
Reportes	10 días	8 octubre

Fuente: Autor

3 INFORME TECNICO

3.1 RESUMEN EJECUTIVO

A continuación, se describe en el informe técnico que muestra el nivel, la descripción, la alerta y las recomendaciones principalmente sobre los hallazgos encontrados y validados.

Los resultados del proceso de ejecución por parte de los profesionales a WhiteHouse Security hacia la infraestructura evaluada, se permite concluir que se encuentra el un nivel de riesgo alto de acuerdo con los hallazgos y vulnerabilidades que se encontraron en el proceso; de igual forma se recomienda a WhiteHouse Security validar los hallazgos del nivel critico y aplicar los respectivos controles y de esa forma mitigar el riesgo latente.

Respecto a las vulnerabilidades encontradas que representan un riesgo crítico para WhiteHouse Security, se observa que no cuenta con actualización del sistema operativos y de igual forma no cuenta con parches.

los nodos Windows identificados son vulnerables a WannaCry, Petya y demás programa maligno que abusan de la vulnerabilidad existente en el protocolo Microsoft Server Message Block 1.0 (SMBv1), debido al mal manejo de algunas solicitudes. Un atacante remoto y sin la necesidad de autenticarse puede explotar dichas vulnerabilidades. (CVE-2017-0143, CVE-2017-0144.

En conclusión, las vulnerabilidades encontradas permiten la conexión remota de un atacante, teniendo el control total del nodo y existe un alto riesgo del cifrado de la información.

3.2 HALLAZGOS CRÍTICOS DEL ANÁLISIS DE VULNERABILIDADES

Se realizó un escaneo con Nmap

Durante la fase 3 se realizó el análisis de vulnerabilidades se realizaron las siguientes acciones:

- Identificación de nodos dentro del prefijo definido, intento de establecer conexiones con diferentes clientes por puertos TCP estándar (1-1024), identificación del versiona miento de los servicios.

- Identificación de Servicios vulnerables sin llegar a explotar dicha(s) vulnerabilidad(es).

3.3 RESULTADOS

Tras el análisis de vulnerabilidades se lograron identificar algunas vulnerabilidades de nivel bajo, medio y alto

Tabla 2 Resumen de Vulnerabilidades

Título	Descripción	Riesgo
MS17-010: Security Update for Microsoft Windows SMB Server	Vulnerable a ejecución remota de código	Alto
Microsoft Windows SMBv1 Multiple Vulnerabilities	Vulnerabilidad que permite al atacante armar un paquete SMBv1 para el robo de información sensible	Alto

Fuente: Autor

3.4 DETALLES DE LAS VULNERABILIDADES CRÍTICAS ENCONTRADAS

3.4.1 MS17-010: Security Update for Microsoft Windows SMB Server

El nodo Windows puede está “afectado por las siguientes vulnerabilidades: Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido a manejo inadecuado de ciertas solicitudes. Un atacante remoto puede explotar estas vulnerabilidades, sin estar autenticado, a través de un paquete especialmente hecho para ejecutar código arbitrario”[1].

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY son cuatro vulnerabilidades de un múltiple Grupo de ecuaciones reveladas en 2017/04/14 por un grupo conocido como los Shadowbrokers. WannaCry/WannaCrypt es un ransomware que utiliza el exploit ETERNALBLUE y EternalRocks es un gusano que utiliza siete grupos de ecuaciones de vulnerabilidades. Petya es un programa de

[1] Varias vulnerabilidades de Microsoft Windows SMBv1

ransomware que utiliza primero CVE-2017-0199, una vulnerabilidad en Microsoft Office y, a continuación, se propaga vía ETERNALBLUE.

Para más información:
“https://technet.microsoft.com/library/security/MS17-01
http://www.nessus.org/u?321523eb
http://www.nessus.org/u?7bec1941
http://www.nessus.org/u?d9f569cf
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
https://support.microsoft.com/en-us/kb/2696547
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?36fd3072
http://www.nessus.org/u?4c7e0cf3
https://github.com/stamparm/EternalRocks/
http://www.nessus.org/u?59db5b5b”[2]

3.4.1.1 Solución:

Microsoft ha lanzado un conjunto de “parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también ha parches de emergencia para los sistemas operativos Windows que no tienen soporte, incluyendo Windows XP, 2003 y 8. Para sistemas operativos Windows no compatibles, p. Windows XP, Microsoft recomienda que los usuarios interrumpan el uso de SMBv1. SMBv1 carece de características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 puede deshabilitado siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT recomienda que los usuarios bloqueen SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de frontera de la red. Por SMB sobre la API de NetBIOS, bloquea puertos TCP 137/139 y puertos UDP 137/138 en todos los dispositivos de frontera de red”[3].

3.4.1.2 Factor de Riesgo:
Critical / CVSS Base Score : 10.0

[2] Varias vulnerabilidades de Microsoft Windows SMBv1 [en línea] [citado el 25 de septiembre, 2020] disponible en: https://www.tenable.com/plugins/nessus/100464

[3] Análisis de vulnerabilidades de la infraestructura tecnológica de la organización caso de estudio. [en línea] [citado el 25 de septiembre, 2020] disponible en: https://repository.unad.edu.co/bitstream/handle/10596/25715/%20macarvajalav.pdf;jsessionid=6E3740103C64A6D1F8CC856AA55EED88.jvm1?sequence=4

(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
Exploit público disponible: Sí

3.4.2 Microsoft Windows SMBv1 Multiple Vulnerabilities

El nodo Windows tiene Microsoft Server Message Block 1.0 (SMBv1) habilitado, por lo tanto, es afectado por múltiples vulnerabilidades:

Existen múltiples "vulnerabilidades de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido a manipulación incorrecta de paquetes SMBv1. Un autenticado, atacante remoto puede explotar estas vulnerabilidades, a través de paquete SMBv1 especialmente diseñado para divulgar información. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE2017-0274, CVE-2017-0275, CVE-2017-0276). Varias vulnerabilidades de denegación de servicio (DoS) existen en Microsoft Server Message Block 1.0 (SMBv1) debido a manejo inadecuado de las solicitudes. Un autenticado, atacante remoto puede explotar estas vulnerabilidades, a través de solicitud SMB especialmente diseñada, para que el sistema dejar de responder. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280)"[4].

Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido a manipulación incorrecta de paquetes SMBv1. Un autenticado, atacante remoto puede explotar estas vulnerabilidades, a través de especialmente diseñado paquete SMBv1, para ejecutar arbitrario código. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279).

Para más información:
"http://www.nessus.org/u?c21268d4
http://www.nessus.org/u?b9253982
http://www.nessus.org/u?23802c83
http://www.nessus.org/u?8313bb60
http://www.nessus.org/u?7677c678
http://www.nessus.org/u?36da236c
http://www.nessus.org/u?0981b934
http://www.nessus.org/u?c88efefa
http://www.nessus.org/u?695bf5cc

[4] Boletín de vulnerabilidades. [en línea] [citado el 25 de septiembre, 2020] disponible en: https://www.incibe-cert.es/content/boletin-vulnerabilidades-134

http://www.nessus.org/u?459a1e8c
http://www.nessus.org/u?ea45bbc5
http://www.nessus.org/u?4195776a
http://www.nessus.org/u?fbf092cf
http://www.nessus.org/u?8c0cc566”[5]

3.4.2.1 Solución:
“Aplica el siguiente parche de actualización según la versión de Windows que maneje:
Windows Server 2008: KB4018466
Windows 7: KB4019264
Windows Server 2008 R2: KB4019264
Windows Server 2012: KB4019216
Windows 8.1 / RT 8.1.: KB4019215
Windows Server 2012 R2: KB4019215
Windows 10: KB4019474
Windows 10 Version 1511: KB4019473
Windows 10 Version 1607: KB4019472
Windows 10 Version 1703: KB4016871
Windows Server 2016: KB4019472”[6]

3.4.2.2 Factor de Riesgo:
Critical / CVSS Base Score: 10.0
(CVSS2#AV: N/AC: L/Au: N/C:C/I:C/A:C)
Exploit público disponible: Sí

[5] Varias vulnerabilidades de Microsoft Windows SMBv1 [en línea] [citado el 25 de septiembre, 2020] disponible en: https://www.tenable.com/plugins/nessus/100464
[6] Ibid. 1

CONCLUSIONES

- La actividad permitió ampliar los conocimientos acerca del Pentesting y sus diferentes etapas y herramientas que pueden ser utilizadas de manera adecuada en cada una de las fases que se deben llevar a cabo durante su ejecución de manera ordenada.

- En Colombia contamos con esta ley 1273 de 2009 que si bien sabemos falta algunas cosas por complementar pero es bastante clara en los límites que se deben cumplir en cuanto a quien pueda acceder a información privada y debe contar con orden judicial por que una buena inteligencia se protege y así poder luchar contra la criminalidad y está enmarcado dentro de la ley 1273 de 2009 pero aquel que transgreda esas fronteras y su actuación será ilegal con fines oscuros que recaiga sobre el todo el peso de la ley.

- Las pruebas de penetración son una forma especializada de evaluación del control de seguridad en la que el evaluador de seguridad asume el papel de un atacante e intenta superar las medidas de seguridad establecidas para proteger el sistema de información.

- Por tanto, hemos utilizado con éxito el marco Metasploit para ingresar al servidor remoto de Windows 7 y obtener acceso que se puede usar para controlar la máquina remota y realizar cualquier tipo de operación.

- Es importante determinar el estado de preparación para responder a un incidente de seguridad cibernética y cree una capacidad de respuesta a incidentes de seguridad (adaptada a la organización).

- Responder y hacer un seguimiento de los incidentes de seguridad cibernética en muchas organizaciones aún enfrenta desafíos importantes, por ejemplo, en términos de presupuesto, recursos, habilidades técnicas, apoyo e influencia.

- Las pruebas de penetración valen la pena la inversión para cualquier PYME que desee la tranquilidad de saber que la red es segura y que las operaciones comerciales diarias pueden continuar en caso de una interrupción del servicio. Las pruebas de penetración se pueden comparar con productos que se prueban antes de su lanzamiento al mercado.

- Las pruebas de penetración con respecto a las intrusiones en la red funcionan de la misma manera. Si no prueba los controles de seguridad y el entorno de red antes de su uso, es imposible garantizar la seguridad en caso de que los piratas informáticos cometan una explotación. Es por eso que las pruebas de penetración tienen sentido para organizaciones de todos los tamaños.

RECOMENDACIONES

- Se debe mantener actualizados los S.O y antivirus

- Capacitar a los empleados de la organización para que no accedan a links adjuntos o den respuesta a correos de dudosa procedencia, no descargar archivos desconocidos.

- Verificar continuamente las firmas de IPS del fabricante con la finalidad de que esta habilite el modo bloqueo reduciendo esta forma de explotación de vulnerabilidades.

- El análisis de dichas acciones puede llevar a la definición de comportamientos bases para definir un Sistema de Gestión de la Seguridad Informática (SGSI), el cual consta de políticas y procedimientos para administrar sistemáticamente la información sensible de una organización.

- La gestión de la seguridad de la información trata de la protección de los activos de información frente a posibles infracciones de seguridad. Se refiere a todo tipo de información, incluidos los formatos tanto electrónicos como de papel. Estos sistemas determinan cómo se procesa, almacena, transfiere, archiva y destruye la información.

BIBLIOGRAFÍA

ARMERDING, T. Self-taught hackers' rule. [en línea] [citado el 25 de septiembre, 2020] disponible en: http://www.csoonline.com/article/2146363/security-leadership/self-taughthackers-rule.html

CATOIRA, F. Penetration Test, ¿en qué consiste? WeLiveSecurity. [2020] [en línea] [citado el 25 de septiembre, 2020] Disponible en: https://www.welivesecurity.com/la-es/2012/07/24/penetration-testen-que consiste/

Centre, N. C. Scheme Penetration Testing. [en línea] [citado el 25 de septiembre, 2020] disponible en: https://www.ncsc.gov.uk/scheme/penetration-testing

Chicano, T. E. (2014). Gestión de incidentes de seguridad informática (mf0488_3) (pp 7-310). Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/44101

CISCO. Contención rápida de amenazas de Cisco [En línea]. [Consultado: 02 de octubre de 2020]. Disponible en: https://www.cisco.com/c/dam/global/shared/assets/pdf/cisco_firesight_management_center.pdf

CISCO. Contención rápida de amenazas de Cisco [En línea]. [Consultado: 02 de octubre de 2020]. Disponible en: https://www.cisco.com/c/en/us/solutions/enterprise-networks/rapid-threat-containment/index.html

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273(05, enero, 2009). Por medio

de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". [en línea]. Santa Fe de Bogotá, D.C. En: diario oficial. Enero 2009. 4p. [Consulta: 10 septiembre 2020]. Disponible en: https://mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341 (30, julio, 2009) de 2009"Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones". [en línea]. Santa Fe de Bogotá, D.C. En: diario oficial. julio 2009. 34p. [Consulta: 10 septiembre 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/3707:Ley-1341-de-2009

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1712 (06, marzo, 2014). “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”. [en línea]. Santa Fe de Bogotá, D.C. En: diario oficial. marzo 2014 [Consulta: 10 septiembre 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/7147:Ley-1712-de-2014

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1928 (24, julio, 2018). Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest. [en línea]. Santa Fe de Bogotá, D.C. En: diario oficial. Julio 2018. 49p. [Consultado: 10 septiembre de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

COLOMBIA. MINISTERIO DE COMERCIO, INDUTRIA Y TURISMO. Decreto 1377 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. [en línea]. Santa Fe de Bogotá, D.C El Ministerio, 2013. 11 p. [Consulta: 10 septiembre 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

DICCIONARIO DE LA REAL ACADEMIA DE LA LENGUA ESPAÑOLA. [término de búsqueda: información]. [en línea -HTML]. España: La academia, 2013. [Consulta: 10 septiembre 2020]. p. 1. Disponible en: http://www.rae.es/

FRANCO, David A. PEREA, Jorge L. PUELLO, Plinio, Metodología para la detección de vulnerabilidades en redes de datos [2020] [en línea] [citado el 25 de septiembre, 2020] Disponible en: http://bibliotecavirtual.unad.edu.co:2139/eds/pdfviewer/pdfviewer?vid=1&sid=8cd37457-4010-4308-a0ad-b3b98f16c321%40pdc-v-sessmgr03

GGI LAN GUARD 12. Vulnerabilidades y exposiciones comunes (CVE). [2020] [en línea] [citado el 25 de septiembre, 2020] Disponible en: https://manuals.gfi.com/es/languard/content/acm/topics/appendix/common_vulnerabilities_and_exposures__cve_.htm

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. (2018). (p. 14 - 27) Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

INFORMATICA JURIDICA. [sitio web]. Legislación Informática de Colombia. [Consulta: 10 septiembre 2020]. Disponible en: http://www.informatica-juridica.com/legislacion/colombia/

INFORMÁTICA. Kali Linux: Una distribución Linux especializada. [2020] [en línea] [citado el 25 de septiembre, 2020] Disponible en: https://inforseguridad.wordpress.com/2016/11/09/kali-linux-que-es-para-que-seutiliza-las-diez-aplicaciones-mas-importantes-que-integra/

INFOSECURITY. Malware bytes. [En línea] [Consultado: 02 de octubre de 2020]. Disponible en: http://www.infosecurityvip.com/newsletter/toolbox_jun15.html

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. ICONTEC (2018). NTC1486: Documentación presentación trabajos académicos. Protocolo. Bogotá D.C.: ICONTEC. Páginas 1-48. Disponible en: http://stadium.unad.edu.co/stadium/pdf_bd/Guia%20ingreso%20a%20BD%20ICONTEC.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. ICONTEC (2016). NTC 6166: Referencias bibliográficas. contenido, forma y estructura. Bogotá D.C.: ICONTEC. Páginas 1-62. Disponible en: https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/normavw.aspx?ID=5538

MICROSOFT. Acuerdos de Licencia Microsoft. [2020] [en línea] [citado el 25 de septiembre, 2020] Disponible en: https://www.microsoft.com/Argentina/PUBLIC/KIT_BASE/LICENCIAMIENTO/LICSEMGT/mslicns/EULAs.htm

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Esq.(pp. 31-63) Disponible en: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

SECURITY HACKLABS. el sistema de detección de versiones de nmap. [2020] [en línea] [citado el 25 de septiembre, 2020] disponible en: https://securityhacklabs.net/articulo/el-sistema-de-deteccion-de-versiones-de-nmap

SHEWARD, M. The Art of Writing Penetration Test Reports. [en línea] [citado el 25 de septiembre, 2020] disponible en: http://resources.infosecinstitute.com/writing-penetration-testing-reports/

SMITH, E. Reporting. [en línea] [citado el 25 de septiembre, 2020] disponible en: http://www.penteststandard.org/index.php/Reporting