Asignatura	Datos del alumno	Fecha
Delitos Informáticos	Apellidos: Paz López	05/12/2021
	Nombre: Angel Ramón	

Contenido

INTRODUCCION

Vivimos en una época donde la tecnología se convierte en un arma de doble filo, que puede ayudar a los negocios y empresas a su cumplimiento de objetivos y metas, pero a la vez también la tecnología se puede convertir en un medio donde personas no autorizadas puedan realizar actividades ilícitas que vayan en contra de los objetivos y metas de la organización. Es por ello que toda empresa y organización deben una planificación en cuanto a la seguridad de todos los sistemas de información y comunicación para evitar riesgos y vulnerabilidades que prevengan, eviten y mitiguen las amenazas para proteger sus activos, mediante mecanismos de seguridad y herramientas que puedan prevenir cualquier tipo de delitos.

OBJETIVO

Realizar un documento con 7 herramientas tecnológicas que ayudaran a prevenir y detectar cualquier tipo de amenazas y delitos informáticos, además de realizar un análisis de datos digitales que ayudaran en ciertos casos a un análisis forense para presentar informe a autoridades o a quienes correspondan sobre las actividades delictivas que se hayan encontrado además de realizar un análisis exhaustivo de cada herramienta, desde su justificación tecnológica, financiera y legal.

HERRAMIENTAS TECNOLÓGICAS PARA LA PREVENCIÓN DEL DELITO

Herramienta	Delito que se previene	Justificación tecnológica	Respaldo (casos de éxito)
Firewall	- Accesos no autorizados a y a la vez controla las comunicaciones autorizadas en la red con nuestros ordenadores - Visualizar y bloquear aplicaciones sospechosas.	Viene integrado en cada Sistema Operativo, también llamado cortafuegos el cual proporciona seguridad limitando o impidiendo el acceso no autorizado a su ordenador desde Internet. Cuya función es prevenir y proteger nuestra red privada permitiendo el tráfico entrante y saliente que se da en nuestro ordenador con las demás redes e Internet	Caso 1: La empresa Vila's Motor contrato servicios de Firewall de Entel Empresas y han tenido extraordinarios resultados con beneficios importantes y grandes mejoras en el negocio. "La preocupación inicial era poner en riesgo la información ya que no había un control donde los empleados visitaban cualquier tipo de páginas y al tener una red abierta y sin dominio los usuarios podrían realizar actividades sospechosas que pudieran poner en riesgo cualquier activo de la empresa. (*Caso de éxito*, s. f.)
EnCase Forensic	- Ayuda a resolver casos de investigación con respecto diferentes delitos informáticos. - Encuentra evidencias para sumar cargos	Es una herramienta poderosa para investigación a delitos informáticos recolectando datos digitales y entre otros, crea un índice completo en varios idiomas, permite consultas, es compatible con todos los sistemas	Caso 1: Se llevo un caso en el departamento de policía de una pequeña ciudad del sudeste de California donde denunciaron un robo de una cartera a una víctima, al arrestar al criminal se le incauto una

	- Crea una extensa base de información vinculada a la investigación.	operativos, ofrece capacidades de programación EnScript orientada a objetos similar a C++ y Java lo cual permite crear aplicaciones personalizados para automatizar las actividades que se realizan al momento de una investigación de un caso.	computadora y mediante En Case Forensic los investigadores encontraron evidencia de una serie de robos similares con distintos grupos y bandas delictivas, infracciones de posesión de armas y drogas con esto la policía logro sumar más cargo al delito inicial con una condena más larga. (EnCase Forensic)
Autopsy	- Para realizar investigaciones digitales, es una herramienta utilizada para el análisis de datos de sistemas sospechosos. - Analiza archivos y directorios, incluyendo archivos eliminados	Es una plataforma fácil de instalar, los módulos que proporciona son: - Modulo de linea de tiempo donde se visualiza los eventos - Filtrado de hash: donde muestra para marcar los archivos defectuosos e ignorar los archivos buenos. - Búsquedas por palabra clave - Artefactos Web: extrae las cookies, historiales de los navegadores web - Recupera datos eliminados - Multimedia, extracción de imágenes - Escaneo de computadoras con STIX	- Casos de uso militares y fuerzas del orden. - Examinadores corporativos

		Autopsy se basa en HTML y en lo cual se puede conectar a autopsy desde cualquier plataforma, el cual proporciona una interfaz de manejador de archivos y muestra detalles de archivos eliminados y la estructura de sistemas de archivos.	
Malwarebytes Endpoint Security	- Detección y desinfección de malware - Bloqueo de sitios webs maliciosos - Bloqueo de Ransomware - Protección sobre exploits	La herramienta posee una protección multivectorial en la cual proporciona un método por capas que incluye técnicas de detección tanto dinámicas como estáticas desde la cadena de ataques para así garantizar una protección segura a las diferentes amenazas que existen y a las futuras. La tecnología de la herramienta comprende un refuerzo a las aplicaciones reduciendo las vulnerabilidades y aumentando la capacidad de recuperación a cualquier ataque, da protección a las webs, mitigación de exploits detectando y bloqueando los intentos de aprovechamientos de la	Caso 1: Malwarebytes evita que el Ransomware afecte a los servicios de emergencia en la comisaría de policía de Cheshire. (Cheshire Constabulary closes the case) Caso 2: Malwarebytes rastrea, bloquea, y protege los sistemas de ataques de malwares repetitivos en el Departamento de Asuntos del Consumidor en California. (California Department of Consumer Affairs)

		vulnerabilidades de los sistemas y ejecución de códigos remotos en una terminal, mitigación de Ransomware detectándolo e impidiendo cifrar archivos mediante tecnologías de supervisión sin firmas basadas en comportamientos, tecnología de reparación propia de desinfección que identifica y elimina todos los malwares y aplicaciones sospechosas	
Honeypot	- Exposición de vulnerabilidades de los sistemas - Detección de intrusos - Detección de patrones y comportamientos en el sistema - Captar amenazas internas - Engañar a atacantes informáticos	Los honeypots son sistemas informáticos con aplicaciones y datos cuyo objetivo es de servir como señuelo para los hackers y recabar información sobre estos cibercriminales, los métodos que utilizan en el ataque y el comportamiento o para distraerlos de otros objetivos. Los honeypots están configurados de manera que no tengan mecanismos de protección haciéndolo un sistema con vulnerabilidades, es una herramienta que nos ayudara a comprender y detectar la aparición de	Caso: Investigadores de 360 Netlab publicaron el 12 de marzo un análisis sobre un nuevo ataque de malware, a la que nombraron como ZHtrap. Una de las características que emplea este malware es la utilización de técnicas que vemos en los honeypots para capturar ataques. (*Honeypots del lado del mal*, 2021)

		amenazas, una vez que los hackers están dentro del sistema trampa, se les puede rastrear, analizar de dónde vienen, analizar el nivel de amenaza, el modus operandi que están utilizando, que datos o aplicaciones son el objetivo, y analizar la eficacia de las medidas que tiene la organización para detener este tipo de ciberataques.	
Wireshark	- Captura de paquetes - Rastreo de conexiones - Supervisar contenido de transacciones en la red sospechosas - Identificación de ráfagas de trafico de red. - Descubrir brotes de virus en la red y ataques DOS	Es un analizador de protocoles de red , sus funciones más importantes son: Captura de paquetes, en la cual escucha una conexión real y captura los paquetes de flujo completos de tráfico, también tiene la función de filtrado con el cual puede cortar o seleccionar mediante filtros datos aleatorios para analizar los datos y obtener la información que se necesita ver y por último la función de visualización lo cual nos permite sumergirse en un paquete de red en la cual se pueden ver conversaciones completas y transmisiones de red.	Caso: Se obtuvo un problema de no se podia encontrar YouTube, pero con Wireshark ayudo a determinar que hubo problema con el enrutamiento Lo que se descubrió mediante el Wireshark fue identificar la versión del TLS que el navegador y YouTube estaban usando para encriptar cosas. Curiosamente, el cifrado cambió a TLS versión 1.2 durante la escucha.

		Para usar esta herramienta y entender todo el proceso que esta realiza se tiene que tener primero el conocimiento de como funciona una red comprender el protocolo de enlace TCP de tres vías y entre otros protocolos como TCP, UDP, DHCP y ICMP. Wireshark solo puede rastrear conexiones entre la computadora local y el sistema remoto con el que se puede tener comunicación, tiene que quedar en claro que esta herramienta no es un IDS para detectar intrusos, solo nos funciona para identificar problemas que se puedan dar en el tráfico de red.	
Cofense PhishMe	- Phishing	La misma herramienta sirve para capacitación y concientización sobre phishing, herramientas anti phishing y simulaciones de amenazas para que el personal este preparado contra este tipo de amenazas e informar los correos electrónicos de phishing de inmediato y detectar las amenazas, con todas estas	La herramienta PhishMe es usada por más de 800 clientes a nivel mundial incluyendo la mitad de las empresas presentes en la lista Fortune 100 para involucrar proactivamente a miles de empleados en simulaciones con el fin de aprender a detectar y reportar amenazas de phishing.

		actividades de capacitación y concientización, la herramienta sirve también para mitigar el riesgo, ya que con la herramienta Cofense Reporter ayuda a los usuarios a crear informes y tasas de resistencias que es uno de los factores más importantes en la defensa contra el phishing, y con dichos informes creados se pueden tomar decisiones importantes como monitorear el desempeño de los programas, los datos, y el cambio de resiliencia de la organización. También se ofrece paquete completo de defensa contra el phishing para detectar y reparar las amenazas de phishing en los correos electrónicos, reducir la carga de las operaciones de seguridad mediante respuesta automatizadas a los ataques de phishing	

FIREWALL

Un Firewall de Seguridad es uno de las mejores alternativas para poder proteger nuestras redes ya que es un dispositivo que se instala entre la red privada de una compañía y la red pública de internet, ya que nos permite gestionar y controlar todas las conexiones que se realizan desde y hacia la red interna generando una capa de seguridad perimetral con el objetivo de minimizar vulnerabilidades y proteger los servidores y equipos conectados en una red.

JUSTIFICACION TECNOLOGICA

La función del Firewall es prevenir y proteger nuestra red privada permitiendo el tráfico entrante y saliente que se da en nuestro ordenador con las demás redes e Internet, sus siguientes beneficios son:

1. VPN: Crea conexiones encriptadas creando un medio seguro de comunicación entre los dispositivos.
2. Antivirus: Protege de virus, programas maliciosos, spyware y muchas amenazas más.
3. Antispam: Sirve como un filtro para detectar correos no deseados
4. IPS: Detección y prevención de vulnerabilidades en la red.
5. Filtros Web y Aplicativos: Restringe el acceso a sitios web y aplicativos webs con el fin de reducir riesgos.
6. Filtrado de Paquetes y de Aplicación: Con el filtrado de paquetes se inspeccionan todos los paquetes entrantes y salientes que se dan en las conexiones en la red y en función a determinadas reglas de filtrado se aceptan o se rechazan y con el de Aplicación es capaz de controlar aplicaciones específicas.

JUSTIFICACION FINANCIERA

El firewall es una herramienta que debe estar instalado en los entornos corporativos para el logro de sus objetivos y protección de sus activos. Debido a que el valor de estos activos es muy importante es objeto de riesgos y amenazas como el robo, fraude, divulgación o destrucción causando pérdidas millonarias para las empresas y de igual forma pueden ocasionar pérdida de confianza de los clientes y proveedores.

Como consecuencia a todo esto la empresa invertirá altos costos para corregir y mitigar todos los daños ocasiones por el ataque y amenazas que aun presentes y lo más importante para prevenir futuras filtraciones u otros ataques informáticos.

JUSTIFICACION LEGAL

Las actividades delictivas de descubrimiento y revelación de secreto industrial y comercial el cual quien obtenga información secreta por medio de cualquier dato, documentos escritos o electrónicos u otros objetos que se refieran al mismo, intercepción de comunicaciones es castigado con pena de prisión de dos a cuatro años y sumado el castigo de multa por una cantidad igual o hasta el triple del beneficio obtenido. Articulo 398 (CodigoPenalNo.130-2017) Honduras.

ENCASE FORENSIC

Es una plataforma poderosa de investigación que recolecta datos digitales, capacidad de realizar análisis de los datos recopilados, informes sobre descubrimiento y los preserva en un formato valido para efectos legales. Puede recolectar información y datos de cualquier actividad de internet desde chats, correos electrónicos, documentos digitales, tiene la función de recuperar archivos eliminados de discos duros formateados, memorias usb, permite también revisar y tener acceso a archivos del sistema y a datos cifrados.

JUSTIFICACION TECNOLOGICA

Es una herramienta poderosa para investigación a delitos informáticos recolectando datos digitales y entre otros, crea un índice completo en varios idiomas, permite consultas, es compatible con todos los sistemas operativos, ofrece capacidades de programación EnScript orientada a objetos similar a C++ y Java lo cual permite crear aplicaciones personalizados para automatizar las actividades que se realizan al momento de una investigación de un caso.

JUSTIFICACION FINANCIERA

Al momento de usar EnCase Forensic ayuda a acortar el ciclo de vida de investigación ayudando a la organización a ahorrarse una cantidad de dinero y así a la reducción de riesgos de responsabilidades, así como la utilización de filtros que permiten búsquedas flexibles,

filtros predefinidos y secuencia de comandos presentando informes automáticos de datos relevantes a la investigación lo cual es ahorro de tiempo y de dinero para los investigadores.

JUSTIFICACION LEGAL

Una vez terminada todas las actividades de investigación de un determinado caso EnCase Forensic crea informes con formato valido para efectos legales y apto para la presentación en los tribunales, u otra autoridad legal.

AUTOPSY

Es un navegador forense cuya plataforma es una interfaz gráfica para el análisis de investigación digital en linea de comandos contenida en Sleuth Kit, el cual pueden analizar discos UNIX y Windows, es Open Source, es una herramienta que se utiliza en investigaciones forenses para el análisis de sistemas sospechosos, analiza archivos y directorios incluyendo archivos eliminados

JUSTIFICACION TECNOLOGICA

Es una plataforma fácil de instalar, los módulos que proporciona son:

- Modulo de linea de tiempo donde se visualiza los eventos
- Filtrado de hash: donde muestra para marcar los archivos defectuosos e ignorar los archivos buenos.
- Búsquedas por palabra clave
- Artefactos Web: extrae las cookies, historiales de los navegadores web
- Recupera datos eliminados
- Multimedia, extracción de imágenes
- Análisis de Metadatos: nos muestra los detalles de los archivos y directorios.
- Análisis de Unidades: es donde se almacenan el contenido de los archivos.
- Escaneo de computadoras con STIX
- Manejo de Casos: Las investigaciones son agrupadas en casos, el cual contienen uno o mas hosts el cual puede contener uno o más imágenes de sistemas de archivos para el análisis.

Autopsy se basa en HTML y en lo cual se puede conectar a autopsy desde cualquier plataforma, el cual proporciona una interfaz de manejador de archivos y muestra detalles de archivos eliminados y la estructura de sistemas de archivos.

JUSTIFICACION FINANCIERA

Autopsy es una herramienta gratuita, a medida que los presupuestos disminuyen, las soluciones forenses son cada vez más rentables y esenciales en las investigaciones y esta herramienta ofrece los mismos servicios que muchas herramientas comerciales ofrecen como ser el análisis de artefactos web, análisis de registros y entre otras funciones esenciales de las herramientas forenses.

JUSTIFICACION LEGAL

El objetivo de toda herramienta forense es examinar los medios digitales con el objetivo de identificar, preservar, recuperar, analizar e informar hechos y opiniones sobre la información digital, todo esto se asocia a las investigaciones de una amplia gama de delitos informáticos en la cual las herramientas forenses están diseñadas para crear un seguimiento de auditoria legal mediante sus técnicas y propias pautas.

MALWAREBYTES ENDPOINT SECURITY

Es una herramienta que proporciona tecnología de protección y desinfección a amenazas, es un modelo de defensa multicapa con protección multivectorial que incluye técnicas de detección y desinfección avanzadas de malwares, bloqueos de sitios webs maliciosos, bloqueos de Ransomware y protección a ataques de exploits.

JUSTIFICACION TECNICA

La herramienta posee una protección multivectorial en la cual proporciona un método por capas que incluye técnicas de detección tanto dinámicas como estáticas desde la cadena de ataques para así garantizar una protección segura a las diferentes amenazas que existen y a las futuras. La tecnología de la herramienta comprende un refuerzo a las aplicaciones reduciendo las vulnerabilidades y aumentando la capacidad de recuperación a cualquier ataque, da protección a las webs, mitigación de exploits detectando y bloqueando los intentos de aprovechamientos de la vulnerabilidades de los sistemas y ejecución de códigos remotos en una terminal, mitigación de Ransomware detectándolo e impidiendo cifrar archivos mediante tecnologías de supervisión sin firmas basadas en comportamientos, tecnología de reparación propia de desinfección que identifica y elimina todos los malwares y aplicaciones sospechosas

JUSTIFICACION FINANCIERA

El valor de mercado de la herramienta va desde $3 .33 a los $8.33 mensuales el precio depende según el plan que se contrate. Los servicios que ofrece la herramienta en el mejor plan son: Prevención de amenazas, neutralización de Ransomware, protección contra sitios webs maliciosos, limpia y elimina malware, mejoras en VPN como ser en la privacidad online, encripta las conexiones WIFI, crea una dirección IP Virtual, permite elegir una geolocalización. Esto son los costos para obtener la herramienta y prevenir cualquier ataque, ahora mencionamos los costos que se pudieran suscitar cuando no tenemos ninguna herramienta y la organización es atacada mediante un Ransomware:

Durante el 2017, uno de los casos de ataques de Ransomware el suceso de WannaCry que fue un ciberataque global que inicio mediante la compañía telefónica en España y concluyó infectando a 300 mil computadoras a lo largo de 150 países lo cual termino significando un gran impacto económico de mas de mil millones de dólares. Un calculado del precio de rescate de la información de un ataque de Ransomware viene entre los 133 mil dólares esto dependiendo si es una organización grande, si fuera una organización pequeña estaría en el rango de los 13 mil a 70 mil dólares, evidentemente que los costos de los rescates de la información por un ataque de Ransomware exceden a los valores de contratación de la herramienta para su prevención. (Conzultek, s. f.)

JUSTIFICACION LEGAL

Los ataques de Ransomware específicamente integran una conducta de delictiva de daños y sabotajes lo cual es castigado en el código Penal en cualquier país.

Las actividades delictivas de descubrimiento y revelación de secreto industrial y comercial el cual quien obtenga información secreta por medio de cualquier dato, documentos escritos o electrónicos u otros objetos que se refieran al mismo, intercepción de comunicaciones es castigado con pena de prisión de dos a cuatro años y sumado el castigo de multa por una cantidad igual o hasta el triple del beneficio obtenido. Articulo 398 (CodigoPenalNo.130-2017) Honduras.

Código Penal en España: el tipo actual del artículo 264 del Código Penal (CP) castiga las conductas recaídas sobre datos, programas informáticos o documentos electrónicos ajenos, mientras que las referidas al normal funcionamiento de un sistema informático ajeno se sancionan en el nuevo artículo 264 bis CP. Además, el artículo 264.2 CP (Barrio, 2019)

Código Federal Penal en México: Derecho en Tecnologías de la Información y Comunicaciones en cuanto a los Sabotajes tenemos

Artículo 140.- Se impondrá pena de dos a veinte años de prisión y multa de mil a cincuenta mil pesos, al que dañe, destruya o ilícitamente entorpezca vías de comunicación, servicios públicos, funciones de las dependencias del Estado, organismos públicos descentralizados, empresas de participación estatal o sus instalaciones; plantas siderúrgicas, eléctricas o de las industrias básicas; centros de producción o distribución de artículos de consumo necesarios de armas, municiones o implementos bélicos, con el fin de trastornar la vida económica del país o afectar su capacidad de defensa. (*Justia México | Código Penal Federal | Capítulo VII | Título Primero | Libro Segundo | Ley de México*, s. f.)

HONEYPOT

Los honeypots son sistemas informáticos con aplicaciones y datos cuyo objetivo es de servir como señuelo para los hackers y recabar información sobre estos cibercriminales, los métodos que utilizan en el ataque y el comportamiento o para distraerlos de otros objetivos.

JUSTIFICACION TECNOLOGICA

Los honeypots están configurados de manera que no tengan mecanismos de protección haciéndolo un sistema con vulnerabilidades, es una herramienta que nos ayudara a comprender y detectar la aparición de amenazas, una vez que los hackers están dentro del sistema trampa, se les puede rastrear, analizar de donde vienen, analizar el nivel de amenaza, el modus operandi que están utilizando, que datos o aplicaciones son el objetivo, y analizar la eficacia de las medidas que tiene la organización para detener este tipo de ciberataques.

Distintos tipos de Honeypot y cómo funcionan

1. **Trampas de correo electrónico:** o también llamadas trampas spam, estas colocan como trampa una dirección de correo electrónico falso en un lugar oculto para atraer a los atacantes y caigan para ver todo tipo de spam que caerá en el correo para su debido análisis o simplemente para evitar que el correo electrónico legitimo este fuera del alcance de los riesgos y ataques, en la actualidad están abandonadas o no validadas.

2. **Honeypot de Malware:** se utilizan para detectar malware imitando las aplicaciones o APIS para atraer a los ataques de malwares de los ciberdelincuentes. El objetivo de esto es analizar la información obtenida de los ataques de malwares que han recibido para así desarrollar software antimalware para resolver las vulnerabilidades que contenga la API original.

3. **Honeypot para arañas:** con el fin de detectar y rastrear rastreadores web creando páginas web y vínculos para que los rastreadores caigan en la trampa con el fin de aprender de como bloquear los bots maliciosos.

También podemos definir los honeypot como:

1. **Alta Dirección:** el objetivo es que el hacker permanezca el tiempo máximo posible dentro del sistema trampa y así nos brinde la mayor información posible como ser el comportamiento y los objetivos, su modus operandi, las vulnerabilidades que aprovecho para ingresar al sistema, las herramientas que esta utilizando y los procesos que está explotando y un sinfín de información.
2. **Baja Interacción:** Son fáciles de configurar usando protocolos de TCP IP, consta de servicios de red básicos y sus características son que **se** utiliza menos recursos y que se consigue la información básica de los atacantes, nivel de amenaza, el tipo de amenaza, su procedencia.

Los sistemas de Honeypots más conocidos son:

1. Honeypots SSH: como **Kippo** escrito en Python para detectar y registrar ataques, **Cowrite** funciona emulando una Shell
2. Honeypots HTTP: **Glastopf** detecta ataques de aplicaciones web, **Nodepot** se centra en Node JS, **Google Hacks Honeypot** emula ser una aplicación web para atraer a los rastreadores,
3. Honeypots de correo electrónico: **Honeymail, Mailoney, SpamHAT**
4. Honeypots de IOT: **HoneyThing, Kako**
5. Honeypots de base de datos**: ElasticHoney, HoneyMysql, MongoDB-HoneyProxy**

JUSTIFICACION FINANCIERA

La inversión que una organización podría realizar para la implementación de un Honeypot dependería del tipo de equipamiento en donde se quisiera montar el honeypot, la red puede estar formada por sistemas virtuales o físicos.

- Honeypot Físicos: se trata de que se utiliza equipos físicos dispuestos para ser atacados desde el exterior para atraer a los atacantes con el fin de recopilar la información del ataque. El precio de estos es elevado ya que se ocupa invertir en hardware como software el cual lleva también un mantenimiento mayor por el equipo que se estará utilizando. Una de las ventajas que ofrece este tipo de honeypot es que brinda un mayor realismo y el atacante no identificaría con facilidad de que se tratase de un sistema trampa, ya que seria una maquina real en la red, este tipo de honeypots son ideales para los honeypots de alta dirección.
- Honeypot Virtuales: se trata de un sistema real pero ejecutado de manera virtual ya sea en una máquina virtual, utilizando el mínimo recursos y son ideales para los honeypots de baja dirección, la ventaja que nos ofrece son escalabilidad y fácil mantenimiento, son muy baratos ya que no disponen de equipos reales sino de virtualización, ejecución rápida.

JUSTIFICACION LEGAL

El objetivo de los Honeypots es engañar a los ciberdelincuentes para que lleven acabo su ataque a los sistemas de nuestra organización y mantener a parte los sistemas legítimos para mayor protección, al engañar a estos delincuentes se pueden obtener la información de dicho ataque al sistema trampa sobre sus métodos de ataque, sus objetivos y todo detalle del ataque la cual se puede utilizar con fines forenses y legales.

WIRESHARK

Es un analizador de protocolos de red el cual nos permite ver lo que esta sucediendo en su red, es el rastreador de paquetes que más se utiliza en la actualidad para la conversión de paquetes binarios a un formato que pueda ser legible, resolución de problemas en la red, analizar el rendimiento de la red, registro de trafico en la red, descubrimiento de brotes de virus o ataques DOS, validar las políticas de seguridad de la empresa y para fines educativos

JUSTIFICACION TECNOLOGICA

Es un analizador de protocoles de red , sus funciones más importantes son: Captura de paquetes, en la cual escucha una conexión real y captura los paquetes de flujo completos de tráfico, también tiene la función de filtrado con el cual puede cortar o seleccionar mediante filtros datos aleatorios para analizar los datos y obtener la información que se necesita ver y por último la función de visualización lo cual nos permite sumergirse en un paquete de red en la cual se pueden ver conversaciones completas y transmisiones de red.

Para usar esta herramienta y entender todo el proceso que esta realiza se tiene que tener primero el conocimiento de cómo funciona una red comprender el protocolo de enlace TCP de tres vías y entre otros protocolos como TCP, UDP, DHCP y ICMP. Wireshark solo puede rastrear conexiones entre la computadora local y el sistema remoto con el que se puede tener comunicación, tiene que quedar en claro que esta herramienta no es un IDS para detectar intrusos, solo nos funciona para identificar problemas que se puedan dar en el tráfico de red.

Características Wireshark

- Rastreo de paquetes TCP, ver la información de cada paquete aplicar filtros a los mismos sin perder el flujo de datos.
- Decodificar los paquetes binarios a un formato entendible.
- Ver estadísticas de los paquetes capturados incluyendo un resumen.
- Análisis informativo mediante nombres MAC, por red etc.
- La herramienta Wireshark viene incluyendo otros programas de apoyo para ayudarle a la manipulación, evaluación y la creación de archivos de captura como ser: Tshark, Editcap, Mergecap, Txt2pcap, Capinfos, Dumcap.

JUSTIFICACION FINANCIERA

El costo de la utilización de la herramienta Wireshark es gratuita pero comparado con otros productos comerciales de analizadores de red la única diferencia es la presentación de informes. Wireshark cuenta con una comunidad de usuarios y colaboradores que ofrecen contenido, discusiones, blogs que permiten ayudar a la utilización de esta herramienta de manera gratuita.

JUSTIFICACION LEGAL

Para utilizar un sniffer lo recomendable primero es leer las políticas de seguridad de la empresa ya que en varias organizaciones en sus políticas esta restringido el uso de los analizadores de red. Pero en aquellas empresas donde prestan servicios de consultorías de seguridad para clientes se confirma que no está prohibido el uso de los sniffer en sus reglamentos. Si las políticas y el reglamento no esta claro para el uso de los analizadores de red antes de usarlos se debe obtener el permiso por escrito de los departamentos correspondientes antes de usarlos para no tener problemas de violación de las políticas y reglamento de la organización.

COFENSE PHISHME

Es una herramienta para la resistencia al phishing organizacional en la cual se realiza capacitación y concientización sobre el phishing, ofrece libro de jugadas que permiten configurar un programa completo de 12 meses con diferentes escenarios de simulación para entrenamiento de identificación de las diferentes amenazas actuales sobre phishing con esto se aprenderá a:

- Detectar amenazas en tiempo real
- Concientizar y condicionar a los empleados frente a las amenazas
- Analizar y responder a las amenazas de phishing
- Como detener los ataques de phishing

JUSTIFICACION TECNOLOGICA

La misma herramienta sirve para capacitación y concientización sobre phishing, herramientas anti phishing y simulaciones de amenazas para que el personal este preparado contra este tipo de amenazas e informar los correos electrónicos de phishing de inmediato y detectar las amenazas, con todas estas actividades de capacitación y concientización, la herramienta sirve también para mitigar el riesgo, ya que con la herramienta Cofense Reporter ayuda a los usuarios a crear informes y tasas de resistencias que es uno de los factores más importantes en la defensa contra el phishing, y con dichos informes creados se pueden tomar decisiones importantes como monitorear el desempeño de los programas, los datos, y el cambio de resiliencia de la organización. También se ofrece paquete completo de

defensa contra el phishing para detectar y reparar las amenazas de phishing en los correos electrónicos, reducir la carga de las operaciones de seguridad mediante respuesta automatizadas a los ataques de phishing

JUSTIFICACION FINANCIERA

Cofense PhishMe consta de una versión gratuita y una versión de pago cuyo valor es de 10,00 US$/año. También ofrece una prueba gratis

Estas son conclusiones clave del estudio sobre el coste del phishing en 2021:

- La pérdida de productividad es una consecuencia del phishing que implica mayor coste.
- Según Informes de Phishme el 93% de los Emails Phishing son Ransomware donde empresas han tenido pérdidas millonarias enormes.
- Los costos para la resolución de problemas ocasionados por el malware se han duplicado desde el 2015 hasta la actualidad, ahora solucionar estos problemas viene costando un calculado de media de unos 807.506 dólares, frente a los 338.098 dólares que suponía en 2015.
- También los costes por compromiso de credenciales han aumentado drásticamente desde el año 2015 de 381.920 dólares a 692.531 dólares en 2021.

JUSTIFICACION LEGAL

Como estamos tocando el phishing y el objetivo de este ataque es adquirir información mediante el uso de la tecnología y se pueden dar diferentes actividades delictivas como ser fraude, sabotaje y las sanciones que castigan también están enmarcadas en el Código Penal Federal.

Con respecto al fraude tenemos: “Artículo 386.- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido.

El delito de fraude se castigará con las penas siguientes:

I.- Con prisión de 3 días a 6 meses o de 30 a 180 días multa, cuando el valor de lo defraudado no exceda de diez veces el salario;

II.- Con prisión de 6 meses a 3 años y multa de 10 a 100 veces el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario;

III.- Con prisión de tres a doce años y multa hasta de ciento veinte veces el salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario." computadoras, etc. El modus operandi de los cibercriminales es mediante herramientas tecnológicas o de ingeniería social, hacerse de los datos de las víctimas y posteriormente hacer mal uso de ellas u obtener algún beneficio económico.

En cuanto a espionaje a instituciones gubernamentales tenemos el Artículo 128.- Se aplicará la pena de prisión de cinco a veinte años y multa hasta de cincuenta mil pesos, al mexicano que, teniendo en su poder documentos o informaciones confidenciales de un gobierno extranjero, los revele a otro gobierno, si con ello perjudica a la Nación Mexicana.

Artículo 129.- Se impondrá la pena de seis meses a cinco años de prisión y multa hasta de cinco mil pesos al que, teniendo conocimiento de las actividades de un espía y de su identidad, no lo haga saber a las autoridades.

Bibliografía

- ✓ *Malwarebytes Caso 1*. (s.f.). Obtenido de https://es.malwarebytes.com/pdf/casestudies/CaseStudyCheshire.pdf
- ✓ *Malwarebytes Caso 2*. (s.f.). Obtenido de https://es.malwarebytes.com/pdf/casestudies/CaseStudyCA_Dept_ConsumerAffairs.pdf
- ✓ *ondata*. (s.f.). Obtenido de https://www.ondata.es/recuperar/encase/spanish_webready_forensicforle-brochure.pdf
- ✓ *Poder Judicial Honduras*. (s.f.). Obtenido de https://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/CodigoPenalNo.130-2017(actualizadojulio2020).pdf

- ✓ *Caso de éxito: Protección de la red con un Firewall de seguridad | Entel Comunidad Empresas*. (s. f.). Caso de éxito: Protección de la red con un Firewall de seguridad. Recuperado 2 de diciembre de 2021, de https://ce.entel.cl/grandes-empresas/articulos/caso-de-exito-firewall-de-seguridad/
- ✓ *¿Por qué es necesario el firewall en entornos corporativos?* (2014, julio 29). WeLiveSecurity. https://www.welivesecurity.com/la-es/2014/07/29/por-que-necesario-firewall-entornos-corporativos/
- ✓ *EnCase Forensic Software: Características y Funciones*. (s. f.). Ondata International. Recuperado 2 de diciembre de 2021, de https://www.ondata.es/
- ✓ *Autopsia*. (s. f.). Recuperado 3 de diciembre de 2021, de https://www.sleuthkit.org/autopsy/
- ✓ Barrio, M. (2019, noviembre 7). *Tribuna | La respuesta del Derecho frente a los ataques «ransomware»*. Cinco Días. https://cincodias.elpais.com/cincodias/2019/11/06/legal/1573063068_861999.html
- ✓ Conzultek. (s. f.). *El costo financiero de los ataques ransomware*. Recuperado 4 de diciembre de 2021, de https://blog.conzultek.com/ciberseguridad/costo-financiero-ataques-ransomware
- ✓ *Honeypots del lado del mal: El reciente caso de ZHtrap*. (2021, marzo 17). Una al Día. https://unaaldia.hispasec.com/2021/03/honeypots-del-lado-del-mal-el-reciente-caso-de-zhtrap.html

- ✓ *Justia México | Código Penal Federal | Capítulo VII | Título Primero | Libro Segundo | Ley de México*. (s. f.). Recuperado 4 de diciembre de 2021, de https://mexico.justia.com/federales/codigos/codigo-penal-federal/libro-segundo/titulo-primero/capitulo-vii/
- ✓ *Justia México | Código Penal Federal | Capítulo VII | Título Primero | Libro Segundo | Ley de México*. (s. f.). Recuperado 4 de diciembre de 2021, de https://mexico.justia.com/federales/codigos/codigo-penal-federal/libro-segundo/titulo-vigesimo-segundo/capitulo-iii/

- ✓ *Justia México | Código Penal Federal | Capítulo VII | Título Primero | Libro Segundo | Ley de México*. (s. f.). Recuperado 4 de diciembre de 2021, de https://mexico.justia.com/federales/codigos/codigo-penal-federal/libro-segundo/titulo-primero/capitulo-ii/
- ✓ *Capacitación y herramientas de concienciación sobre el phishing | Simulaciones de phishing*. (s. f.). Recuperado 5 de diciembre de 2021, de https://cofense-com.translate.goog/product-services/phishme/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sc