Glosario

Ciberseguridad

Términos y definiciones del certificado.

A

Ruta absoluta del archivo: La ruta completa del archivo, que comienza desde la raíz.

Controles de acceso: Controles de seguridad que gestionan el acceso, la autorización y la responsabilidad de la información.

Olfateo activo de paquetes: A Tipo de ataque en el que se manipulan paquetes de datos en tránsito.

Protocolo de resolución de direcciones (ARP): Un protocolo de red utilizado para determinar la dirección MAC del siguiente enrutador o dispositivo en la ruta.

Amenaza persistente avanzada (APT): Un caso en el que un actor de amenazas mantiene acceso no autorizado a un sistema durante un período prolongado de tiempo.

Inteligencia artificial (IA) adversaria: Una técnica que manipula la tecnología de inteligencia artificial (IA) y aprendizaje automático (ML) para realizar ataques de manera más eficiente.

Programa publicitario: Un tipo de software legítimo que a veces se utiliza para mostrar anuncios digitales en aplicaciones.

Algoritmo: Un conjunto de reglas utilizadas para resolver un problema.

Análisis: La investigación y validación de alertas.

Phishing de pescadores: Una técnica donde los atacantes se hacen pasar por representantes de servicio al cliente en las redes sociales

Análisis basado en anomalías: Un método de detección que identifica comportamientos anormales.

Software antivirus: Un programa de software utilizado para prevenir, detectar y eliminar malware y virus.

Solicitud: Un programa que realiza una tarea específica.

Token de interfaz de programación de aplicaciones (API): Un pequeño bloque de código cifrado que contiene información sobre un usuario.

Argumento (Linux): Información específica que necesita un comando

Argumento (Python): Los datos incorporados a una función cuando se llama.

Formación: Un tipo de datos que almacena datos en una lista ordenada separada por comas.

Evaluar: El quinto paso del NIST RMF que significa determinar si los controles establecidos se implementan correctamente

Activo: Un elemento percibido como de valor para una organización.

Clasificación de activos: La práctica de etiquetar activos según la sensibilidad y la importancia para una organización.

Inventario de activos: Un catálogo de activos que deben protegerse

Gestión de activos: El proceso de seguimiento de los activos y los riesgos que los afectan.

Cifrado asimétrico: El uso de un par de claves pública y privada para cifrar y descifrar datos.

Superficie de ataque: Todas las vulnerabilidades potenciales que un actor de amenazas podría explotar

Árbol de ataque: Un diagrama que mapea las amenazas a los activos

Vectores de ataque: Las vías que utilizan los atacantes para penetrar las defensas de seguridad

Autenticación: El proceso de verificar quién es alguien.

Autorización: El concepto de otorgar acceso a recursos específicos en un sistema.

Autorizar: El sexto paso del NIST RMF que se refiere a ser responsable de los riesgos de seguridad y privacidad que puedan existir en una organización.

Automatización: El uso de la tecnología para reducir el esfuerzo humano y manual para realizar tareas comunes y repetitivas.

Disponibilidad: La idea de que los datos son accesibles para quienes están autorizados a acceder a ellos.

B

Cebo: Una táctica de ingeniería social que tienta a las personas a comprometer su seguridad

Ancho de banda: La capacidad máxima de transmisión de datos a través de una red, medida en bits por segundo.

Configuración de referencia (imagen de referencia): Un conjunto documentado de especificaciones dentro de un sistema que se utiliza como base para futuras compilaciones, lanzamientos y actualizaciones.

Intento: El shell predeterminado en la mayoría de las distribuciones de Linux.

autenticación básica: La tecnología utilizada para establecer la solicitud de un usuario para acceder a un servidor.

Sistema básico de entrada/salida (BIOS): Un microchip que contiene instrucciones de carga para la computadora y que prevalece en sistemas más antiguos.

Biometría: Las características físicas únicas que se pueden utilizar para verificar la identidad de una persona.

Poco: La unidad más pequeña de medida de datos en una computadora.

Datos booleanos: Datos que sólo pueden ser uno de dos valores: ya sea `Verdadero` o `FALSO`

Cargador de arranque: Un programa de software que inicia el sistema operativo.

Red de bots: Un conjunto de computadoras infectadas por malware que están bajo el control de un único actor de amenaza, conocido como "bot-herder".

Notación entre corchetes: Los índices colocados entre corchetes

Cadena de custodia rota: Inconsistencias en la recolección y registro de pruebas en la cadena de custodia

Ataque de fuerza bruta: El proceso de prueba y error para descubrir información privada

Recompensa de errores: Programas que alientan a los piratas informáticos independientes a encontrar e informar vulnerabilidades

Función incorporada: Una función que existe dentro de Python y se puede llamar directamente

Continuidad del negocio: La capacidad de una organización para mantener su productividad diaria mediante el establecimiento de planes de recuperación de riesgos ante desastres.

Plan de continuidad del negocio (BCP): Un documento que describe los procedimientos para sostener las operaciones comerciales durante y después de una interrupción significativa.

Compromiso de correo electrónico empresarial (BEC): Un tipo de ataque de phishing en el que un actor de amenazas se hace pasar por una fuente conocida para obtener una ventaja financiera.

do

Clasificar por categorías: El segundo paso del NIST RMF que se utiliza para desarrollar procesos y tareas de gestión de riesgos.

CentOS: Una distribución de código abierto muy relacionada con Red Hat

Unidad Central de Procesamiento (CPU): El procesador principal de una computadora, que se utiliza para realizar tareas informáticas generales en una computadora.

Cadena de custodia: El proceso de documentar la posesión y el control de la evidencia durante el ciclo de vida de un incidente.

Crónica: Una herramienta nativa de la nube diseñada para retener, analizar y buscar datos

Cifrar: Un algoritmo que cifra la información

Cortafuegos basados en la nube: Firewalls de software alojados por el proveedor de servicios en la nube

Computación en la nube: La práctica de utilizar servidores, aplicaciones y servicios de red remotos alojados en Internet en lugar de en dispositivos físicos locales.

Red en la nube: Una colección de servidores o computadoras que almacena recursos y datos en centros de datos remotos a los que se puede acceder a través de Internet.

Seguridad en la nube: El proceso de garantizar que los activos almacenados en la nube estén configurados correctamente y que el acceso a esos activos esté limitado a usuarios autorizados.

Dominio: Una instrucción que le dice a la computadora que haga algo.

Mando y control (C2): Las técnicas utilizadas por actores maliciosos para mantener comunicaciones con sistemas comprometidos

Interfaz de línea de comandos (CLI): Una interfaz de usuario basada en texto que utiliza comandos para interactuar con la computadora.

Comentario: Una nota que hacen los programadores sobre la intención detrás de su código

Formato de evento común (CEF): Un formato de registro que utiliza pares clave-valor para estructurar datos e identificar campos y sus valores correspondientes.

Vulnerabilidades y exposiciones comunes (CVE®) lista: Un diccionario de acceso abierto sobre vulnerabilidades y exposiciones conocidas

Sistema de puntuación de vulnerabilidad común (CVSS): Un sistema de medición que puntúa la gravedad de una vulnerabilidad.

Cumplimiento: El proceso de adhesión a normas internas y regulaciones externas.

Equipos de respuesta a incidentes de seguridad informática (CSIRT): Un grupo especializado de profesionales de seguridad capacitados en gestión y respuesta a incidentes.

Virus informático: Código malicioso escrito para interferir con las operaciones de la computadora y causar daños a los datos y al software.

Declaración condicional: Una declaración que evalúa el código para determinar si cumple con un conjunto específico de condiciones.

Confidencialidad: La idea de que solo los usuarios autorizados puedan acceder a activos o datos específicos

Datos confidenciales: Datos que a menudo tienen límites en la cantidad de personas que tienen acceso a ellos.

Tríada de confidencialidad, integridad y disponibilidad (CIA): Un modelo que ayuda a informar cómo las organizaciones consideran el riesgo al configurar sistemas y políticas de seguridad.

Archivo de configuración: Un archivo utilizado para configurar los ajustes de una aplicación.

Contención: El acto de limitar y prevenir daños adicionales causados por un incidente.

Zona controlada: Una subred que protege la red interna de la zona no controlada.

Secuencias de comandos entre sitios (XSS): Un ataque de inyección que inserta código en un sitio web o aplicación web vulnerable

Colaboración colectiva: La práctica de recopilar información utilizando el aporte y la colaboración del público.

Ataque criptográfico: Un ataque que afecta formas seguras de comunicación entre un remitente y el destinatario previsto.

Clave criptográfica: Un mecanismo que descifra texto cifrado

Criptografía: El proceso de transformar la información en una forma que los lectores no deseados no puedan entender.

Criptojacking: Una forma de malware que instala software para extraer criptomonedas ilegalmente

Autoridad de Numeración CVE (CNA): Una organización que se ofrece como voluntaria para analizar y distribuir información sobre CVE elegibles.

Ciberseguridad (o seguridad): La práctica de garantizar la confidencialidad, integridad y disponibilidad de la información mediante la protección de redes, dispositivos, personas y datos contra el acceso no autorizado o la explotación delictiva.

D

Datos: Información traducida, procesada o almacenada por una computadora.

Datos en reposo: Actualmente no se está accediendo a los datos

Base de datos: Una colección organizada de información o datos.

Responsable del tratamiento: Persona que determina el procedimiento y finalidad del tratamiento de los datos.

Custodio de datos: Cualquier persona o cosa que sea responsable del manejo, transporte y almacenamiento seguro de la información.

Exfiltración de datos: Transmisión no autorizada de datos desde un sistema

Datos en tránsito: Datos que viajan de un punto a otro.

Datos en uso: Datos a los que acceden uno o más usuarios

Propietario de los datos: La persona que decide quién puede acceder, editar, utilizar o destruir su información.

Paquete de datos: Unidad básica de información que viaja de un dispositivo a otro dentro de una red.

Punto de datos: Un dato específico

Procesador de datos: Una persona que es responsable del tratamiento de datos por cuenta del responsable del tratamiento.

Delegado de protección de datos (DPO): Una persona que es responsable de monitorear el cumplimiento de los procedimientos de protección de datos de una organización.

Tipo de datos: Una categoría para un tipo particular de elemento de datos

Datos de fecha y hora: Datos que representan una fecha y/u hora.

Depurador: Una herramienta de software que ayuda a localizar el origen de un error y evaluar sus causas.

Depuración: La práctica de identificar y corregir errores en el código.

Defensa en profundidad: Un enfoque en capas para la gestión de vulnerabilidades que reduce el riesgo

Ataque de denegación de servicio (DoS): Un ataque que tiene como objetivo una red o servidor y lo inunda con tráfico de red.

Detectar: Una función central del NIST relacionada con la identificación de posibles incidentes de seguridad y la mejora de las capacidades de monitoreo para aumentar la velocidad y la eficiencia de las detecciones.

Detección: El rápido descubrimiento de eventos de seguridad.

Datos del diccionario: Datos que constan de uno o más pares clave-valor.

Certificado digital: Un archivo que verifica la identidad del titular de una clave pública.

Forense digital: La práctica de recopilar y analizar datos para determinar qué sucedió después de un ataque.

Directorio: Un archivo que organiza dónde se almacenan otros archivos.

Plan de recuperación de desastres: Un plan que permite al equipo de seguridad de una organización delinear los pasos necesarios para minimizar el impacto de un incidente de seguridad.

Ataque distribuido de denegación de servicio (DDoS): Un tipo de ataque de denegación de servicio que utiliza múltiples dispositivos o servidores ubicados en diferentes ubicaciones para inundar la red objetivo con tráfico no deseado.

Distribuciones: Las diferentes versiones de Linux

Documentación: Cualquier forma de contenido grabado que se utilice para un propósito específico.

Ataque XSS basado en DOM: Un caso en el que existe un script malicioso en la página web que carga un navegador

Sistema de nombres de dominio (DNS): Un protocolo de red que traduce nombres de dominio de Internet en direcciones IP.

Cuentagotas: Un tipo de malware que viene empaquetado con código malicioso que se entrega e instala en un sistema de destino.

Y

Parcela de ascensor: Un breve resumen de su experiencia, habilidades y antecedentes.

Encapsulación: Un proceso realizado por un servicio VPN que protege sus datos envolviendo datos confidenciales en otros paquetes de datos.

Cifrado: El proceso de convertir datos de un formato legible a un formato codificado.

Punto final: Cualquier dispositivo conectado a una red.

Detección y respuesta de endpoints (EDR): Una aplicación que monitorea un punto final en busca de actividad maliciosa

Erradicación: La eliminación completa de los elementos del incidente de todos los sistemas afectados.

Política de escalamiento: Un conjunto de acciones que describen a quién se debe notificar cuando ocurre una alerta de incidente y cómo se debe manejar ese incidente.

Evento: Un suceso observable en una red, sistema o dispositivo.

Excepción: Un error que involucra código que no se puede ejecutar aunque sea sintácticamente correcto

Operador exclusivo: Un operador que no incluye el valor de comparación.

Explotar: Una forma de aprovechar una vulnerabilidad

Exposición: Un error que puede ser aprovechado por una amenaza.

Amenaza externa: Cualquier cosa fuera de la organización que tenga el potencial de dañar los activos de la organización.

F

Falso negativo: Un estado donde no se detecta la presencia de una amenaza

Falso positivo: Una alerta que detecta incorrectamente la presencia de una amenaza

Malware sin archivos: Malware que no necesita ser instalado por el usuario porque utiliza programas legítimos que ya están instalados para infectar una computadora.

Ruta del archivo: La ubicación de un archivo o directorio.

Estándar de jerarquía del sistema de archivos (FHS): El componente del sistema operativo Linux que organiza los datos.

Filtración: Seleccionar datos que coincidan con una determinada condición

Informe final: Documentación que proporciona una revisión integral de un incidente.

Cortafuegos: Un dispositivo de seguridad de red que monitorea el tráfico hacia o desde una red.

Datos flotantes: Datos que consisten en un número con un punto decimal.

Clave externa: Una columna en una tabla que es una clave principal en otra tabla

Servidor proxy directo: Un servidor que regula y restringe el acceso de una persona a Internet.

Función: Una sección de código que se puede reutilizar en un programa.

GRAMO

Variables globales: Una variable que está disponible en todo el programa.

Interfaz gráfica de usuario (GUI): Una interfaz de usuario que utiliza iconos en la pantalla para gestionar diferentes tareas en la computadora.

h

Hacker: Cualquier persona que utilice computadoras para obtener acceso a sistemas, redes o datos informáticos.

Hacktivista: Una persona que utiliza la piratería para lograr un objetivo político.

Disco duro: Un componente de hardware utilizado para la memoria a largo plazo.

Hardware: Los componentes físicos de una computadora.

Colisión de hash: Un caso en el que diferentes entradas producen el mismo valor hash

Función hash: Un algoritmo que produce un código que no se puede descifrar

tabla hash: Una estructura de datos que se utiliza para almacenar y hacer referencia a valores hash.

Ley de Responsabilidad y Portabilidad del Seguro Médico (HIPAA): Una ley federal de EE. UU. establecida para proteger la información de salud de los pacientes

Mielero: Un sistema o recurso creado como señuelo vulnerable a ataques con el propósito de atraer a posibles intrusos.

Sistema de detección de intrusiones basado en host (HIDS): Una aplicación que monitorea la actividad del host en el que está instalada.

Centro: Un dispositivo de red que transmite información a todos los dispositivos de la red.

Protocolo de transferencia de hipertexto (HTTP): Un protocolo de capa de aplicación que proporciona un método de comunicación entre clientes y servidores de sitios web.

Protocolo seguro de transferencia de hipertexto (HTTPS): Un protocolo de red que proporciona un método seguro de comunicación entre clientes y servidores de sitios web.

I

Identificar: Una función central del NIST relacionada con la gestión del riesgo de ciberseguridad y su efecto en las personas y los activos de una organización.

Gestión de identidades y accesos (IAM): Una colección de procesos y tecnologías que ayuda a las organizaciones a gestionar identidades digitales en su entorno.

IEEE 802.11 (Wi-Fi): Un conjunto de estándares que definen la comunicación para LAN inalámbricas.

Inmutable: Un objeto que no se puede cambiar después de crearlo y asignarle un valor.

Implementar: El cuarto paso del NIST RMF que significa implementar planes de seguridad y privacidad para una organización

Uso inadecuado: Un tipo de incidente que ocurre cuando un empleado de una organización viola las políticas de uso aceptable de la organización.

Incidente: Un suceso que, real o inminentemente, ponga en peligro, sin autoridad legal, la confidencialidad, integridad o disponibilidad de la información o de un sistema de información; o constituye una violación o amenaza inminente de violación de la ley, políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

Escalada de incidentes: El proceso de identificar un posible incidente de seguridad, clasificarlo y entregárselo a un miembro del equipo con más experiencia.

Diario del manejador de incidentes: Una forma de documentación utilizada en la respuesta a incidentes.

Respuesta al incidente: El intento rápido de una organización de identificar un ataque, contener el daño y corregir los efectos de una violación de seguridad.

Plan de respuesta a incidentes: Un documento que describe los procedimientos a seguir en cada paso de la respuesta a un incidente.

Operador inclusivo: Un operador que incluye el valor de comparación.

Sangría: Espacio agregado al comienzo de una línea de código.

Índice: Un número asignado a cada elemento en una secuencia que indica su posición.

Indicadores de ataque (IoA): La serie de eventos observados que indican un incidente en tiempo real.

Indicadores de compromiso (IoC): Evidencia observable que sugiere signos de un posible incidente de seguridad.

Privacidad de la información: La protección del acceso no autorizado y la distribución de datos.

Seguridad de la información (InfoSec): La práctica de mantener los datos en todos los estados alejados de usuarios no autorizados.

Ataque de inyección: Código malicioso insertado en una aplicación vulnerable

Validación de entrada: Programación que valida entradas de usuarios y otros programas.

Datos enteros: Datos formados por un número que no incluye punto decimal.

Entorno de desarrollo integrado (IDE): Una aplicación de software para escribir código que proporciona asistencia de edición y herramientas de corrección de errores.

Integridad: La idea de que los datos son correctos, auténticos y fiables.

Hardware interno: Los componentes necesarios para ejecutar la computadora.

Amenaza interna: Un empleado actual o anterior, proveedor externo o socio de confianza que represente un riesgo para la seguridad.

Protocolo de mensajes de control de Internet (ICMP): Un protocolo de Internet utilizado por los dispositivos para informarse entre sí sobre errores de transmisión de datos a través de la red.

Inundación del protocolo de mensajes de control de Internet (inundación ICMP): Un tipo de ataque DoS realizado por un atacante que envía repetidamente paquetes de solicitud ICMP a un servidor de red.

Protocolo de Internet (IP): Un conjunto de estándares utilizados para enrutar y direccionar paquetes de datos mientras viajan entre dispositivos en una red.

Dirección de protocolo de Internet (IP): Una cadena única de caracteres que identifica la ubicación de un dispositivo en Internet.

Intérprete: Un programa informático que traduce el código Python en instrucciones ejecutables línea por línea.

Sistema de detección de intrusos (IDS): Una aplicación que monitoriza la actividad del sistema y alerta sobre posibles intrusiones

Sistema de prevención de intrusiones (IPS): Una aplicación que monitorea la actividad del sistema en busca de actividad intrusiva y toma medidas para detener la actividad.

Suplantación de IP: Un ataque de red realizado cuando un atacante cambia la IP de origen de un paquete de datos para hacerse pasar por un sistema autorizado y obtener acceso a una red.

Declaración iterativa: Código que ejecuta repetidamente un conjunto de instrucciones.

k

KALILINUX™: Una distribución de código abierto de Linux que se utiliza ampliamente en la industria de la seguridad.

Núcleo: El componente del sistema operativo Linux que gestiona los procesos y la memoria.

Par clave-valor: Un conjunto de datos que representa dos elementos vinculados: una clave y su valor correspondiente.

Sistema operativo heredado: Un sistema operativo obsoleto pero que aún se utiliza

Reunión de lecciones aprendidas: Una reunión que incluye a todas las partes involucradas después de un incidente importante.

Biblioteca: Una colección de módulos que proporcionan código al que los usuarios pueden acceder en sus programas.

Linux: Un sistema operativo de código abierto

Concatenación de listas: El concepto de combinar dos listas en una colocando los elementos de la segunda lista directamente después de los elementos de la primera lista.

Datos de lista: Estructura de datos que consta de una colección de datos en forma secuencial.

Cargador: Un tipo de malware que descarga cepas de código malicioso de una fuente externa y las instala en un sistema de destino.

Red de área local (LAN): Una red que abarca áreas pequeñas como un edificio de oficinas, una escuela o una casa.

variables locales: Una variable asignada dentro de una función.

Registro: Un registro de eventos que ocurren dentro de los sistemas de una organización.

Análisis de registros: El proceso de examinar registros para identificar eventos de interés.

Explotación florestal: El registro de eventos que ocurren en sistemas y redes informáticas.

Error de lógica: Un error que se produce cuando la lógica utilizada en el código produce resultados no deseados

Gestión de registros: El proceso de recopilación, almacenamiento, análisis y eliminación de datos de registro.

Condición del bucle: La parte de un bucle que determina cuándo termina el bucle.

Variables de bucle: Una variable que se utiliza para controlar las iteraciones de un bucle.

METRO

Malware: Software diseñado para dañar dispositivos o redes.

Infección de malware: Un tipo de incidente que ocurre cuando software malicioso diseñado para interrumpir un sistema se infiltra en las computadoras o la red de una organización.

Dirección de control de acceso a medios (MAC): Un identificador alfanumérico único que se asigna a cada dispositivo físico en una red.

Método: Una función que pertenece a un tipo de datos específico.

Métrica: Atributos técnicos clave, como el tiempo de respuesta, la disponibilidad y la tasa de fallas, que se utilizan para evaluar el rendimiento de una aplicación de software.

INGLETE: Una colección de centros de investigación y desarrollo sin fines de lucro.

Módem: Un dispositivo que conecta su enrutador a Internet y brinda acceso a Internet a la LAN

Módulo: Un archivo Python que contiene funciones, variables, clases y cualquier tipo de código ejecutable adicionales.

Monitor: El séptimo paso del NIST RMF que significa estar al tanto de cómo funcionan los sistemas

Autenticación multifactor (MFA): Una medida de seguridad que requiere que un usuario verifique su identidad de dos o más formas para acceder a un sistema o red.

norte

nano: Un editor de archivos de línea de comandos que está disponible de forma predeterminada en muchas distribuciones de Linux.

Marco de ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST): Un marco voluntario que consta de estándares, directrices y mejores prácticas para gestionar el riesgo de ciberseguridad.

Ciclo de vida de respuesta a incidentes del Instituto Nacional de Estándares y Tecnología (NIST): Un marco para la respuesta a incidentes que consta de cuatro fases: preparación; Detección y Análisis; Contención, Erradicación y Recuperación, y Actividad posterior al incidente

Publicación especial (S.P.) 800-53 del Instituto Nacional de Estándares y Tecnología (NIST): Un marco unificado para proteger la seguridad de los sistemas de información dentro del gobierno federal de EE. UU.

Red: Un grupo de dispositivos conectados

Sistema de detección de intrusos basado en red (NIDS): Una aplicación que recopila y monitorea el tráfico de la red y los datos de la red.

Datos de red: Los datos que se transmiten entre dispositivos en una red.

Tarjeta de interfaz de red (NIC): Hardware que conecta computadoras a una red.

Análisis de registros de red: El proceso de examinar los registros de la red para identificar eventos de interés.

Analizador de protocolos de red (rastreador de paquetes): Una herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red.

Protocolos de red: Un conjunto de reglas utilizadas por dos o más dispositivos en una red para describir el orden de entrega y la estructura de los datos.

Seguridad de la red: La práctica de mantener la infraestructura de red de una organización segura contra el acceso no autorizado.

Segmentación de red: Una técnica de seguridad que divide la red en segmentos

Tráfico de red: La cantidad de datos que se mueven a través de una red.

No repudio: El concepto de que no se puede negar la autenticidad de la información

Computadora portátil: Una interfaz en línea para escribir, almacenar y ejecutar código.

Datos numéricos: Datos que consisten en números.

EL

OAuth: Un protocolo de autorización de estándar abierto que comparte el acceso designado entre aplicaciones.

Objeto: Un tipo de datos que almacena datos en una lista de pares clave-valor separados por comas

Ataque en ruta: Un ataque en el que un actor malicioso se coloca en medio de una conexión autorizada e intercepta o altera los datos en tránsito.

Inteligencia de código abierto (OSINT): La recopilación y análisis de información de fuentes disponibles públicamente para generar inteligencia utilizable.

Modelo de interconexión de sistemas abiertos (OSI): Un concepto estandarizado que describe las siete capas que usan las computadoras para comunicarse y enviar datos a través de la red.

Proyecto abierto de seguridad de aplicaciones web/Proyecto abierto mundial de seguridad de aplicaciones (OWASP): Una organización sin fines de lucro enfocada en mejorar la seguridad del software.

Sistema operativo (SO): La interfaz entre el hardware de la computadora y el usuario.

Operador: Un símbolo o palabra clave que representa una operación.

Opciones: Entrada que modifica el comportamiento de un comando

Orden de volatilidad: Una secuencia que describe el orden de los datos que deben conservarse desde el primero hasta el último.

Top 10 de OWASP: Un documento de concientización estándar reconocido mundialmente que enumera los 10 riesgos de seguridad más críticos para las aplicaciones web.

PAG

Paquete: Una pieza de software que se puede combinar con otros paquetes para formar una aplicación.

Administrador de paquetes: Una herramienta que ayuda a los usuarios a instalar, administrar y eliminar paquetes o aplicaciones.

Captura de paquetes (P-cap): Un archivo que contiene paquetes de datos interceptados desde una interfaz o red.

Olfateo de paquetes: La práctica de capturar e inspeccionar paquetes de datos a través de una red.

Parámetro (Python): Un objeto que está incluido en una definición de función para su uso en esa función.

Loro: Una distribución de código abierto que se usa comúnmente para seguridad.

Análisis: El proceso de convertir datos a un formato más legible.

Olfateo pasivo de paquetes: Un tipo de ataque en el que un actor malintencionado se conecta a un centro de red y analiza todo el tráfico de la red.

Ataque de contraseña: Un intento de acceder a dispositivos, sistemas, redes o datos protegidos con contraseña

Actualización del parche: Una actualización de software y sistema operativo que aborda las vulnerabilidades de seguridad dentro de un programa o producto.

Estándares de seguridad de datos de la industria de tarjetas de pago (PCI DSS): A conjunto de estándares de seguridad formados por las principales organizaciones de la industria financiera

Prueba de penetración (prueba de penetración): Un ataque simulado que ayuda a identificar vulnerabilidades en sistemas, redes, sitios web, aplicaciones y procesos.

Guía de estilo PEP 8: Un recurso que proporciona pautas de estilo para programadores que trabajan en Python.

Dispositivos periféricos: Componentes de hardware conectados y controlados por el sistema informático.

Permisos: El tipo de acceso otorgado a un archivo o directorio.

Información de identificación personal (PII): Cualquier información utilizada para inferir la identidad de un individuo.

Phishing: El uso de comunicaciones digitales para engañar a las personas para que revelen datos confidenciales o implementen software malicioso.

Kit de phishing: Una colección de herramientas de software necesarias para lanzar una campaña de phishing

Ataque físico: Un incidente de seguridad que afecta no sólo a los entornos digitales sino también físicos donde se despliega el incidente.

Ingeniería social física: Un ataque en el que un actor de amenazas se hace pasar por un empleado, cliente o proveedor para obtener acceso no autorizado a una ubicación física.

Ping de la muerte: Un tipo de ataque DoS causado cuando un hacker hace ping a un sistema enviándole un paquete ICMP de gran tamaño que supera los 64 KB.

Libro de jugadas: Un manual que proporciona detalles sobre cualquier acción operativa.

Política: Un conjunto de reglas que reducen el riesgo y protegen la información.

Puerto: Una ubicación basada en software que organiza el envío y la recepción de datos entre dispositivos en una red.

Filtrado de puertos: Una función de firewall que bloquea o permite que ciertos números de puerto limiten la comunicación no deseada

Actividad posterior al incidente: El proceso de revisión de un incidente para identificar áreas de mejora durante el manejo del incidente.

Aplicación potencialmente no deseada (PUA): Un tipo de software no deseado que se incluye con programas legítimos que pueden mostrar anuncios, ralentizar el dispositivo o instalar otro software.

Datos privados: Información que debe mantenerse oculta al público

Preparar: El primer paso del NIST RMF relacionado con las actividades necesarias para gestionar los riesgos de seguridad y privacidad antes de que se produzca una infracción

Declaración preparada: Una técnica de codificación que ejecuta sentencias SQL antes de pasarlas a una base de datos.

Clave primaria: Una columna donde cada fila tiene una entrada única

Principio de privilegio mínimo: El concepto de otorgar solo el acceso y la autorización mínimos necesarios para completar una tarea o función.

Protección de la privacidad: El acto de salvaguardar la información personal del uso no autorizado.

Procedimientos: Instrucciones paso a paso para realizar una tarea de seguridad específica

Proceso de Simulación de Ataques y Análisis de Amenazas (PASTA): Un marco de modelado de amenazas popular que se utiliza en muchas industrias.

Programación: Un proceso que se puede utilizar para crear un conjunto específico de instrucciones para que una computadora ejecute tareas.

Proteger: Una función central del NIST utilizada para proteger una organización mediante la implementación de políticas, procedimientos, capacitación y herramientas que ayudan a mitigar las amenazas a la ciberseguridad.

Información de salud protegida (PHI): Información que se relaciona con la salud o condición física o mental pasada, presente o futura de un individuo.

Proteger y preservar la evidencia: El proceso de trabajar adecuadamente con evidencia digital frágil y volátil

Servidor proxy: Un servidor que cumple con las solicitudes de sus clientes reenviándolas a otros servidores.

Datos públicos: Datos que ya son accesibles al público y representan un riesgo mínimo para la organización si otros los ven o los comparten.

Infraestructura de clave pública (PKI): Un marco de cifrado que asegura el intercambio de información en línea

Biblioteca estándar de Python: Una extensa colección de código Python que a menudo viene empaquetado con Python.

q

Consulta: Una solicitud de datos de una tabla de base de datos o una combinación de tablas.

Qué para quién: Un tipo de cebo utilizado para engañar a alguien haciéndole creer que será recompensado a cambio de compartir acceso, información o dinero.

R

Mesa arcoíris: Un archivo de valores hash pregenerados y su texto sin formato asociado.

Memoria de acceso aleatorio (RAM): Un componente de hardware utilizado para la memoria a corto plazo.

ransomware: Un ataque malicioso en el que los actores de amenazas cifran los datos de una organización y exigen un pago para restaurar el acceso.

Informe: Una relación amistosa en la que las personas involucradas entienden las ideas de los demás y se comunican bien entre sí.

Recuperar: Una función central del NIST relacionada con el regreso de los sistemas afectados a su funcionamiento normal.

Recuperación: El proceso de devolver los sistemas afectados a sus operaciones normales.

Red Hat® Enterprise Linux® (también denominado simplemente Red Hat en este curso)**:** Una distribución de Linux basada en suscripción diseñada para uso empresarial

Ataque XSS reflejado: Un caso en el que se envía un script malicioso a un servidor y se activa durante la respuesta del servidor.

Expresión regular (regex): Una secuencia de caracteres que forma un patrón.

Regulaciones: Reglas establecidas por un gobierno u otra autoridad para controlar la forma en que se hace algo

Base de datos relacional: Una base de datos estructurada que contiene tablas relacionadas entre sí.

Ruta de archivo relativa: Una ruta de archivo que comienza desde el directorio actual del usuario.

Ataque de repetición: Un ataque de red que se realiza cuando un actor malintencionado intercepta un paquete de datos en tránsito y lo retrasa o lo repite en otro momento.

Resistencia: La capacidad de prepararse, responder y recuperarse de las disrupciones.

Responder: Una función central del NIST relacionada con garantizar que se utilicen los procedimientos adecuados para contener, neutralizar y analizar incidentes de seguridad e implementar mejoras en el proceso de seguridad.

Declaración de devolución: Una declaración de Python que se ejecuta dentro de una función y envía información a la llamada de función.

Servidor proxy inverso: Un servidor que regula y restringe el acceso a Internet a un servidor interno.

Riesgo: Cualquier cosa que pueda afectar la confidencialidad, integridad o disponibilidad de un activo.

Mitigación de riesgos: El proceso de contar con los procedimientos y reglas adecuados para reducir rápidamente el impacto de un riesgo como una infracción.

Directorio raíz: El directorio de más alto nivel en Linux

rootkit: Malware que proporciona acceso administrativo remoto a una computadora

Usuario root (o superusuario): Un usuario con privilegios elevados para modificar el sistema.

Enrutador: Un dispositivo de red que conecta varias redes juntas

S

Salazón: Una protección adicional que se utiliza para fortalecer las funciones hash

Scareware: Malware que emplea tácticas para asustar a los usuarios para que infecten su dispositivo

Lenguaje de procesamiento de búsqueda (SPL): lenguaje de consulta de Splunk

Protocolo seguro de transferencia de archivos (SFTP): Un protocolo seguro utilizado para transferir archivos de un dispositivo a otro a través de una red.

Cáscara segura (SSH): Un protocolo de seguridad utilizado para crear un shell con un sistema remoto.

Arquitectura de seguridad: Un tipo de diseño de seguridad compuesto por múltiples componentes, como herramientas y procesos, que se utilizan para proteger una organización de riesgos y amenazas externas.

Auditoría de seguridad: Una revisión de los controles, políticas y procedimientos de seguridad de una organización frente a un conjunto de expectativas.

Controles de seguridad: Salvaguardas diseñadas para reducir riesgos de seguridad específicos

Ética de seguridad: Pautas para tomar decisiones adecuadas como profesional de la seguridad

Marcos de seguridad: Directrices utilizadas para elaborar planes que ayuden a mitigar los riesgos y las amenazas a los datos y la privacidad.

Gobernanza de la seguridad: Prácticas que ayudan a respaldar, definir y dirigir los esfuerzos de seguridad de una organización.

Refuerzo de seguridad: El proceso de fortalecer un sistema para reducir sus vulnerabilidades y superficie de ataque.

Información de seguridad y gestión de eventos (SIEM): Una aplicación que recopila y analiza datos de registro para monitorear actividades críticas en una organización.

Mentalidad de seguridad: La capacidad de evaluar el riesgo y buscar e identificar constantemente la violación potencial o real de un sistema, aplicación o datos.

Centro de operaciones de seguridad (SOC): Una unidad organizativa dedicada a monitorear redes, sistemas y dispositivos en busca de amenazas o ataques a la seguridad.

Orquestación, automatización y respuesta de seguridad (SOAR): Una colección de aplicaciones, herramientas y flujos de trabajo que utilizan la automatización para responder a eventos de seguridad.

Postura de seguridad: La capacidad de una organización para gestionar su defensa de activos y datos críticos y reaccionar ante el cambio.

Zona de seguridad: Un segmento de la red de una empresa que protege la red interna de Internet.

Seleccionar: El tercer paso del NIST RMF que significa elegir, personalizar y capturar la documentación de los controles que protegen una organización.

Datos sensibles: Un tipo de datos que incluye información de identificación personal (PII), información confidencial de identificación personal (SPII) o información de salud protegida (PHI).

Información sensible de identificación personal (SPII): Un tipo específico de PII que se rige por pautas de manejo más estrictas.

Separación de funciones: El principio de que a los usuarios no se les deben dar niveles de autorización que les permitan hacer un mal uso de un sistema.

Sesión: una secuencia de solicitudes y respuestas HTTP de red asociadas con el mismo usuario

Cookie de sesión: Un token que los sitios web utilizan para validar una sesión y determinar cuánto tiempo debe durar esa sesión.

Secuestro de sesión: Un evento en el que los atacantes obtienen la ID de sesión de un usuario legítimo

ID de sesión: Un token único que identifica a un usuario y su dispositivo mientras accede a un sistema.

Establecer datos: Datos que constan de una colección desordenada de valores únicos.

Responsabilidad compartida: La idea de que todos los individuos dentro de una organización desempeñan un papel activo para reducir el riesgo y mantener la seguridad física y virtual.

Caparazón: El intérprete de línea de comandos

Firma: Un patrón asociado con actividad maliciosa

Análisis de firma: Un método de detección utilizado para encontrar eventos de interés.

Protocolo simple de administración de red (SNMP): Un protocolo de red utilizado para monitorear y administrar dispositivos en una red.

Inicio de sesión único (SSO): Una tecnología que combina varios inicios de sesión diferentes en uno

aplastando: El uso de mensajes de texto para engañar a los usuarios para que obtengan información confidencial o se hagan pasar por una fuente conocida.

Ataque pitufo: Un ataque de red realizado cuando un atacante huele la dirección IP de un usuario autorizado y la inunda con paquetes ICMP.

Ingeniería social: Una técnica de manipulación que aprovecha el error humano para obtener información privada, acceso u objetos de valor.

Phishing en redes sociales: Un tipo de ataque en el que un actor de amenazas recopila información detallada sobre su objetivo en sitios de redes sociales antes de iniciar el ataque.

Phishing de lanza: Un ataque de correo electrónico malicioso dirigido a un usuario o grupo de usuarios específico, que parece provenir de una fuente confiable

Velocidad: La velocidad a la que un dispositivo envía y recibe datos, medida en bits por segundo.

Nube Splunk: Una herramienta alojada en la nube que se utiliza para recopilar, buscar y monitorear datos de registro.

Empresa Splunk: Una herramienta autohospedada que se utiliza para retener, analizar y buscar datos de registro de una organización. para proporcionar información de seguridad y alertas en tiempo real

Software espía: Malware que se utiliza para recopilar y vender información sin consentimiento

SQL (lenguaje de consulta estructurado): Un lenguaje de programación utilizado para crear, interactuar y solicitar información de una base de datos.

Inyección SQL: Un ataque que ejecuta consultas inesperadas en una base de datos

Tenedor de apuestas: Un individuo o grupo que tiene interés en cualquier decisión o actividad de una organización.

Error estándar: Un mensaje de error devuelto por el sistema operativo a través del shell

Entrada estándar: Información recibida por el sistema operativo a través de la línea de comando.

Salida estándar: Información devuelta por el sistema operativo a través del shell

Estándares: Referencias que informan cómo establecer políticas.

Método ESTRELLA: Una técnica de entrevista utilizada para responder preguntas conductuales y situacionales.

Con estado: Un tipo de firewall que realiza un seguimiento de la información que pasa a través de él y filtra las amenazas de forma proactiva.

Apátrida: Una clase de firewall que opera según reglas predefinidas y que no realiza un seguimiento de la información de los paquetes de datos.

Ataque XSS almacenado: Un caso en el que se inyecta un script malicioso directamente en el servidor

Concatenación de cadenas: El proceso de unir dos hilos.

Datos de cadena: Datos que consisten en una secuencia ordenada de caracteres.

Guía de estilo: Un manual que informa sobre la redacción, el formato y el diseño de documentos.

Subredes: La subdivisión de una red en grupos lógicos llamados subredes.

Subcadena: Una secuencia continua de caracteres dentro de una cadena.

sudo: Un comando que otorga temporalmente permisos elevados a usuarios específicos

Ataque a la cadena de suministro: Un ataque dirigido a sistemas, aplicaciones, hardware y/o software para localizar una vulnerabilidad donde se pueda implementar malware.

suricata: Un sistema de detección de intrusiones de código abierto, un sistema de prevención de intrusiones y una herramienta de análisis de red.

Cambiar: Un dispositivo que realiza conexiones entre dispositivos específicos en una red enviando y recibiendo datos entre ellos.

Cifrado simétrico: El uso de una única clave secreta para intercambiar información.

Sincronizar (SYN) ataque de inundación: Un tipo de ataque DoS que simula una conexión TCP/IP e inunda un servidor con paquetes SYN.

Sintaxis: Las reglas que determinan lo que está correctamente estructurado en un lenguaje informático

Error de sintaxis: Un error que implica el uso no válido de un lenguaje de programación.

t

Seguir de cerca: Una táctica de ingeniería social en la que personas no autorizadas siguen a una persona autorizada a un área restringida.

Modelo TCP/IP: Un marco utilizado para visualizar cómo se organizan y transmiten los datos a través de una red.

tcpdump: Un analizador de protocolos de red de línea de comandos

Habilidades técnicas: Habilidades que requieren conocimiento de herramientas, procedimientos y políticas específicas.

Telemetría: La recopilación y transmisión de datos para su análisis.

Amenaza: Cualquier circunstancia o evento que pueda impactar negativamente los activos.

Actor de amenaza: Cualquier persona o grupo que presente un riesgo para la seguridad.

Caza de amenazas: La búsqueda proactiva de amenazas en una red

Inteligencia de amenazas: Información sobre amenazas basada en evidencia que proporciona contexto sobre amenazas existentes o emergentes.

Modelado de amenazas: El proceso de identificación de activos, sus vulnerabilidades y cómo cada uno está expuesto a amenazas.

Habilidades transferibles: Habilidades de otras áreas que pueden aplicarse a diferentes carreras.

Protocolo de control de transmisión (TCP): Un protocolo de comunicación de Internet que permite que dos dispositivos formen una conexión y transmitan datos.

Triaje: La priorización de incidentes según su nivel de importancia o urgencia.

caballo de Troya: Malware que parece un archivo o programa legítimo

Verdadero negativo: Un estado en el que no se detecta actividad maliciosa

Verdadero positivo Una alerta que detecta correctamente la presencia de un ataque

Datos de tupla: Estructura de datos que consta de una colección de datos que no se pueden cambiar.

Error de tipo: Un error que resulta del uso de un tipo de datos incorrecto

EN

Ubuntu: Una distribución de código abierto y fácil de usar que se utiliza ampliamente en seguridad y otras industrias.

Acceso no autorizado: Un tipo de incidente que ocurre cuando un individuo obtiene acceso digital o físico a un sistema o aplicación sin permiso.

Zona no controlada: Cualquier red fuera del control de su organización

Interfaz de firmware extensible unificada (UEFI): Un microchip que contiene instrucciones de carga para la computadora y reemplaza al BIOS en sistemas más modernos.

Cebo USB: Un ataque en el que un actor de amenazas deja estratégicamente una memoria USB con malware para que un empleado la encuentre. e instalar para infectar una red sin saberlo

Usuario: La persona que interactúa con una computadora.

Protocolo de datagramas de usuario (UDP): Un protocolo sin conexión que no establece una conexión entre dispositivos antes de las transmisiones.

Función definida por el usuario: Una función que los programadores diseñan para sus necesidades específicas.

Interfaz de usuario: Un programa que permite al usuario controlar las funciones del sistema operativo.

Aprovisionamiento de usuarios: El proceso de creación y mantenimiento de la identidad digital de un usuario.

V

Variable: Un contenedor que almacena datos.

Máquina virtual (VM): Una versión virtual de una computadora física.

Red privada virtual (VPN): Un servicio de seguridad de red que cambia su dirección IP pública y oculta su ubicación virtual para que pueda mantener sus datos privados cuando utiliza una red pública como Internet.

Virus: Código malicioso escrito para interferir con las operaciones de la computadora y causar daños a los datos y al software.

Total de virus: Un servicio que permite a cualquier persona analizar archivos, dominios, URL y direcciones IP sospechosos en busca de contenido malicioso.

Deseando: La explotación de la comunicación de voz electrónica para obtener información confidencial o hacerse pasar por una fuente conocida.

Panel visual: Una forma de mostrar varios tipos de datos rápidamente en un solo lugar

Vulnerabilidad: Una debilidad que puede ser explotada por una amenaza.

Evaluación de vulnerabilidad: El proceso de revisión interna de los sistemas de seguridad de una organización.

Gestión de vulnerabilidades: El proceso de encontrar y parchear vulnerabilidades.

Escáner de vulnerabilidades: Software que compara automáticamente las vulnerabilidades y exposiciones comunes existentes con las tecnologías de la red.

EN

Ataque al abrevadero: Un tipo de ataque cuando un actor de amenazas compromete un sitio web visitado con frecuencia por un grupo específico de usuarios.

Explotaciones basadas en web: Código o comportamiento malicioso que se utiliza para aprovechar las fallas de codificación en una aplicación web.

Ballenero: Una categoría de intentos de phishing dirigido a ejecutivos de alto rango de una organización.

Red de área amplia (WAN): Una red que abarca un área geográfica grande como una ciudad, estado o país.

Acceso protegido Wi-Fi (WPA): Un protocolo de seguridad inalámbrico para que los dispositivos se conecten a Internet.

Comodín: Un carácter especial que se puede sustituir por cualquier otro carácter.

Tiburón de alambre: Un analizador de protocolos de red de código abierto

Archivo grabable mundialmente: Un archivo que cualquier persona en el mundo puede modificar

Gusano: Malware que puede duplicarse y propagarse entre sistemas por sí solo

Y

NIÑOS-L: Un lenguaje informático utilizado para crear reglas para buscar a través de datos de registro ingeridos.

CON

Día cero: Un exploit que antes era desconocido