FORTINET
NSE Training Institute

Términos clave de ciberseguridad

Administración de eventos e información de seguridad (SIEM): también conocida como administración de eventos e incidentes de seguridad. Proporciona una vista integral y centralizada del estado de la seguridad de una infraestructura de TI para identificar, supervisar, registrar y analizar eventos o incidentes de seguridad en tiempo real. La mayoría de los sistemas SIEM implementan varios agentes de recopilación para reunir información sobre eventos relacionados con la seguridad de dispositivos de usuarios finales, servidores, equipos de red y equipos de seguridad especializada como los firewalls, los AV/AM o los IPS. Los recopiladores remiten los eventos a una consola de administración centralizada, la cual realiza inspecciones, indica anomalías y notifica al Equipo de respuesta a incidentes sobre eventos que violan la seguridad.

Amenaza persistente avanzada (APT): un ataque a una red mediante el cual una persona obtiene acceso a esta sin autorización y permanece allí sin que se le detecte por un período largo. En general, su intención es robar datos en lugar de causarle daño a la red o a la organización. Estos ataques se dirigen a empresas de sectores que contienen información de alto valor, como la defensa nacional, la producción y la industria financiera.

Antivirus/anti-malware (AV / AM): proporciona protección contra virus, spyware y otros tipos de ataques de malware en la web, en correos electrónicos y en el tráfico de transferencias de archivos. Se encarga de detectar, eliminar e informar sobre el código malicioso. Mediante la interceptación y la inspección del tráfico y el contenido basado en aplicaciones, la protección antivirus garantiza la detección de las amenazas maliciosas escondidas en contenido legítimo de las aplicaciones y su eliminación de los flujos de datos antes de que puedan causar daños. La protección AV/AM en dispositivos y servidores del cliente es una capa adicional de seguridad.

Ataque de abrevadero: un ataque en el que el atacante observa los sitios web frecuentados por una persona o grupo en particular y los infecta con malware.

Ataque de denegación de servicio distribuido (DDoS): la manipulación sistemática de una gran cantidad de sistemas en riesgo repartidos en Internet (vea Botnets) que generan solicitudes de red a un sistema objetivo con rapidez. Este flujo de solicitudes sobrecarga el servidor objetivo y este se vuelve incapaz de responder a las solicitudes legítimas.

Ataque pasivo: un ataque real cometido por una fuente de amenaza intencional que busca aprender información de un sistema o utilizarla sin intención de alterar el sistema o sus recursos, datos y operaciones.

Autenticación: el proceso mediante el cual se determina si alguien o algo es en verdad lo que afirma ser. En redes informáticas, el fin de la autenticación es garantizar que tengan acceso a la red solo personas y dispositivos autorizados. (Compárelo con Autorización).

Autorización: el mecanismo de seguridad que determina los privilegios del usuario/cliente o sus niveles de acceso en cuanto a recursos del sistema como son programas informáticos, archivos, servicios, datos y funciones de la aplicación. En general, la autorización es posterior a la autenticación para verificar la identidad del usuario.

Baiting: el agente de amenaza deja en un lugar público un dispositivo portátil de almacenamiento, como una unidad USB, con una etiqueta llamativa. Cuando la víctima conecta el dispositivo a su computadora, esta se infecta.

Baiting de USB: las unidades USB comprometidas pueden utilizarse para inyectar un código malicioso, redirigir al usuario hacia sitios web que practican la suplantación de identidad o dar acceso a un hacker a la computadora de un usuario.

Bot / Botnet: una red de computadoras privadas infectadas con software malicioso y controladas en conjunto sin el conocimiento del propietario y que se utilizan para llevar a cabo ataques de DDoS, robar datos o enviar spam. Al agente de amenaza que controla un botnet se lo denomina “pastor de bots”.

Caballo de Troya: un tipo de malware en el que una carga útil maliciosa se incrusta en un archivo benigno del host para engañar al usuario y lograr que descargue e instale el malware. Cuando un usuario accede al archivo del host, la carga útil maliciosa se deposita de forma automática en su sistema informático y le permite al cibercriminal llevar a cabo distintos ataques como el robo o la destrucción de datos, la instalación de otros malwares, la modificación de archivos, la supervisión de la actividad del usuario o la denegación de servicio (DoS) en direcciones web objetivo.

Cifrado: el proceso mediante el cual la información legible se convierte en un código ininteligible para proteger la privacidad de los datos.

Cifrado: un algoritmo criptográfico que se utiliza para cifrar información o datos.

Clickbait: anuncios en línea, que pueden ser falsos, cuyo mayor propósito es atraer usuarios a otro sitio web. A veces, este sitio web o el anuncio en sí contienen malware.

Código malicioso: código de programación creado para llevar a cabo una función o un proceso no autorizado que impacta de forma adversa sobre la confidencialidad, la integridad o la disponibilidad de un sistema de información.

Compromiso del correo electrónico empresarial (BEC): vea Suplantación de identidad dirigida.

Deepfake: un audio o un video editado y manipulado para que parezca real o creíble. Logran convencer con facilidad a las personas para que crean ciertas historias o teorías que pueden tener consecuencias políticas o financieras.

Descarga oculta: se refiere a la descarga involuntaria de un virus o software malicioso (malware) a una computadora o dispositivo móvil. Una descarga oculta suele aprovechar (o “vulnerar”) un buscador, una aplicación o un sistema operativo que es obsoleto y tiene defectos de seguridad. El primer código que se descarga suele ser muy pequeño (para que no lo note). En general, su función es contactar a otra computadora donde pueda desplegar el resto del código en su smartphone, tableta o computadora. Las páginas web suelen contener distintos tipos de códigos maliciosos con la expectativa de que alguno de ellos coincida con una debilidad de su computadora.

Detección de amenazas avanzadas (ATP): se basa en varios tipos de productos, estudios y tecnologías de seguridad. Si bien cada uno de ellos desempeña una función diferente, trabajan juntos de forma fluida para combatir los ataques desde el núcleo de la red hasta el dispositivo del usuario final. El concepto de este marco tripartito es simple: prevenir, detectar y mitigar. Sin embargo, abarca un amplio conjunto de herramientas avanzadas y tradicionales para la seguridad de la red, de la aplicación y del endpoint, así como para la detección y la mitigación de amenazas.

Engaño por redes sociales: un atacante manipula contenido y crea perfiles en línea falsos.

Filtrado web: le da la opción de permitir sitios web de forma explícita o de pasar tráfico web sin inspección desde sitios web conocidos y confiables y hacia ellos para acelerar el flujo de tráfico. La tecnología de filtrado web más avanzada permite una gran variedad de acciones para inspeccionar, calificar y controlar el perímetro de tráfico web en detalle. Esta tecnología de filtrado de contenido web le permite a las appliances clasificar y filtrar el tráfico web según distintas categorías preestablecidas o personalizadas.

Firewall: una aplicación de software o appliance de hardware cuyo fin es prevenir el acceso no autorizado o evitar que un malware ilícito escriba en una computadora, dispositivo o red.

Firewall de próxima generación (NGFW): un tipo de firewall, de software o hardware, que puede detectar y bloquear ataques complicados mediante la aplicación de las medidas de seguridad a nivel de protocolo, puerto y aplicación.

Firma de virus: es la huella dactilar de un virus. Es un conjunto de datos únicos o trozos de código que permiten su identificación. Una firma puede contener varias firmas de virus, las cuales son algoritmos o hashes que identifican de forma única a cada virus. El software antivirus utiliza firmas de virus para encontrarlos en un sistema de archivos informáticos y así detectarlos, ponerlos en cuarentena y eliminarlos.

Firmas de ataque: un patrón de ataque distintivo o característico que puede investigarse mediante un conjunto automatizado de reglas que se relacionan a ataques identificados con anterioridad.

Fraude del CEO: vea Suplantación de identidad dirigida.

Gestión unificada de amenazas (UTM): un enfoque de la seguridad de la información que combina varios elementos clave de hardware y software de seguridad de red en una solución de seguridad integral, que incluye un solo punto de administración y elaboración de informes para el administrador de seguridad. Se opone al método tradicional que utiliza puntos de soluciones para cada función de seguridad.

Gusano: un tipo de malware que se replica se propaga y se contiene a sí mismo y que utiliza mecanismos de red para difundirse entre otros sistemas. Por lo general, el daño de un gusano es indirecto ya que su replicación y distribución consume todos los recursos del sistema. Un gusano puede usarse para depositar otras formas de malware en los sistemas que encuentre.

Ingeniería social: el arte de manipular a las personas para obtener información confidencial o para lograr que hagan algo que no querían hacer.

Inspección de tráfico cifrado en capa de sockets seguros (SSL): protege a los clientes endpoint y a los servidores web y de aplicaciones contra amenazas potenciales ocultas. La inspección SSL intercepta e inspecciona el tráfico cifrado en busca de amenazas antes de enrutarlo a su destino. Puede aplicarse al tráfico orientado al cliente, como los usuarios conectados a través de un sitio basado en una nube o al tráfico de un servidor web o de aplicaciones. Este tipo de inspección permite aplicar la política sobre contenido web cifrado para prevenir la invasión potencial del tráfico malicioso oculto en el contenido de SSL. Si bien esta inspección aumenta la seguridad mediante la examinación de amenazas que intentan eludir las protecciones viajando en tráfico cifrado, el efecto negativo es la disminución en la velocidad de rendimiento.

Inspección profunda de paquetes (DPI): la examinación de la porción de datos de un paquete de red a medida que pasa por un firewall u otro dispositivo de seguridad. La DPI identifica el tráfico de redes y lo clasifica según las firmas en la porción de datos. Busca errores de protocolo, virus, spam, intrusiones o violaciones de políticas.

Inyección de SQL: un ataque informático mediante el cual se incrusta un código malicioso en una aplicación con un diseño rústico y luego se lo pasa a la base de datos backend. Los datos maliciosos producen resultados de consultas de la base de datos o acciones que jamás debieron ejecutarse.

Juice jacking: una vulneración de la seguridad en la que se utiliza un puerto de carga USB infectado para poner en riesgo los dispositivos que se conectan.

Malware: un software malicioso que daña un sistema informático. Algunos tipos de malware son los gusanos, virus, troyanos, spyware, adware y ransomware.

Monitoreo de comportamiento: la observación de la actividad de los usuarios, de los sistemas de información y de los procesos, y la medición de las actividades que trasgreden políticas y normativas empresariales, referencias de actividad normal, márgenes y tendencias.

Pretexteado: una situación inventada para convencer a la víctima de revelar información privilegiada.

Puntos de acceso no autorizados: un punto de acceso inalámbrico que se instaló en una red segura sin la autorización de un administrador de la red local ya sea por parte de un empleado bien intencionado o de un atacante malicioso.

Ransomware: un tipo de programa de malware que infecta un sistema, lo bloquea o toma el control de él y que exige una recompensa para revertir la acción. El ransomware ataca e infecta una computadora con el fin de extorsionar a su propietario para que pague. El correo electrónico es el mayor vector de ataque ya que necesita de un solo clic para eludir los controles. Otros nombres del ransomware son criptovirus, criptotroyano o criptogusano.

Recolección de credenciales (o cuentas): un ataque dirigido que roba gran cantidad de nombres de usuario, contraseñas y direcciones de correo electrónico.

Red privada virtual (VPN): una herramienta que extiende una red privada a una red pública y que permite a los usuarios enviar y recibir datos mediante redes compartidas o públicas como si sus computadoras estuvieran conectadas de forma directa a la red privada. El cifrado es habitual en la conexión VPN, aunque no es inherente a ella.

Registrador de pulsaciones de teclas: la tecnología que hace un seguimiento de las pulsaciones consecutivas de teclas de un teclado y las registra.

Relleno de credenciales: un ataque de suplantación de identidad dirigida que utiliza credenciales robadas que suelen monetizarse en foros de la web profunda y son provechosas para apuntar a otras cuentas de alto valor, en especial, empleados de departamentos ejecutivos y financieros, para recolectar sus credenciales y obtener acceso no autorizado a dispositivos y redes.

Robo de identidad: el robo de información de identificación personal (PII), en general, por un beneficio económico.

Rootkit: otro tipo de malware que permite a los cibercriminales controlar su computadora de forma remota. Los rootkits son en especial dañinos porque son difíciles de detectar y es posible que vivan en su computadora por un período largo.

Sandbox: un mecanismo de seguridad que separa los programas en ejecución en un área apartada del sistema operativo y de las aplicaciones del dispositivo/red. Se utiliza para ejecutar códigos que no se han sometido a prueba o programas no confiables de terceros, proveedores, usuarios y sitios web no confiables que no se han verificado. La sandbox limita las acciones y los recursos disponibles para el elemento restringido y permite su evaluación a la vez que previene cualquier daño hacia el sistema host, los datos relacionados o los dispositivos de almacenamiento.

Scripting entre sitios (XSS): el proceso de agregar código malicioso a un sitio web genuino para reunir información de los usuarios con fines maliciosos. Los ataques XSS son posibles debido a las vulnerabilidades de seguridad que se encuentran en aplicaciones web. En general, estas se aprovechan introduciendo un script del lado del cliente. Si bien suele utilizarse JavaScript, algunos atacantes utilizan VBScript, ActiveX o Flash.

Secure Web Gateway: un servicio de seguridad local o en la nube. En medio de los usuarios e Internet, los secure web gateways proporcionan una protección avanzada de la red mediante la inspección de solicitudes web que contravienen las políticas de las empresas para asegurar el bloqueo de las aplicaciones y los sitios web maliciosos y volverlos inaccesibles. Una secure web gateway contiene tecnologías de seguridad esenciales como filtrado URL, control de aplicaciones, prevención de pérdida de datos, antivirus e inspección de https para brindar una seguridad web sólida a las empresas.

Sistema de detección de intrusiones (IDS): el software que alerta de forma automática a los administradores cuando algo o alguien intenta poner un sistema en peligro.

Sistema de prevención de intrusiones (IPS): el sistema que supervisa una red en busca de actividad maliciosa registra la información, intenta bloquear tal actividad y la informa.

Smishing: también conocido como suplantación de identidad por SMS. Ocurre cuando un teléfono celular recibe un mensaje SMS (mensaje instantáneo o IM) de una entidad o persona falsa. El usuario desprevenido responde el mensaje SMS falso y utiliza una URL sin advertir que está descargando un malware e instalando un troyano. La suplantación de identidad busca extraer información útil, por lo tanto, en la suplantación de identidad por SMS, el troyano recolecta las áreas de datos del celular y se las transmite lo antes posible a la persona que creó el troyano.

Software de seguridad no autorizado: se convence a la víctima de adquirir un desinstalador de malware falso, pero en realidad se instala un malware en su dispositivo.

Spam: el abuso de los sistemas de mensajería electrónica, como el correo electrónico, los mensajes de texto, las redes sociales o VoIP para enviar mensajes masivos no deseados de forma indiscriminada. La mayoría del SPAM es publicitario, pero algunos pueden contener códigos, hipervínculos o archivos adjuntos maliciosos.

Spyware: un malware utilizado para infiltrarse en el sistema de un usuario sin su conocimiento, con el fin de supervisar su actividad, recopilar pulsaciones de teclas y contraseñas y recolectar datos (información de cuenta, inicios de sesión y datos financieros). El spyware vulnera al usuario y la aplicación y suele adjuntarse a las descargas de software en línea gratuito o en vínculos que los usuarios cliquean. También se utiliza para desactivar un firewall o software anti-malware mientras consume actividad de la CPU para aumentar la vulnerabilidad del endpoint ante el ataque.

Superficie de ataque: la suma de todos los puntos desde los cuales un usuario no autorizado puede intentar ingresar a un entorno informático y atacarlo. Si bien en el contexto de la ciberseguridad se refiere al software y hardware de un entorno informático, el concepto de superficie de ataque se puede aplicar a otros ámbitos. Por ejemplo, las puertas y las ventanas representan la superficie de ataque de una casa porque son puntos por los cuales un intruso puede ingresar.

Suplantación: una práctica maliciosa o fraudulenta en la que se envían comunicaciones desde una fuente desconocida disfrazada de una fuente conocida para el receptor. Su fin es obtener una ventaja o la confianza de este. Es más frecuente en mecanismos de comunicación que carecen de un nivel de seguridad alto, como la dirección IP, la dirección MAC y la dirección de correo electrónico.

Suplantación de identidad: la presentación de una interfaz engañosa que se muestra como una entidad confiable para lograr que los usuarios proporcionen información confidencial de forma voluntaria como es el nombre de usuario, la contraseña, información de la tarjeta de crédito, etc. Suele enviarse por correo electrónico.

Suplantación de identidad de altos cargos: vea Suplantación de identidad dirigida.

Suplantación de identidad dirigida, suplantación de identidad de altos cargos, fraude del CEO y compromiso del correo electrónico empresarial (BEC): formas de ataque de ingeniería social que se dirigen a víctimas que tienen una relación digital existente con una entidad en línea como un banco o un sitio web de ventas. Los mensajes de suplantación de identidad dirigida suelen enviarse por correo electrónico, aunque también por mensaje de texto y VoIP, ya que estos parecen medios de comunicación legítimos de una entidad confiable. El ataque engaña a la víctima para que haga clic en un hipervínculo del sitio web de la empresa que lo redirige a una versión falsa de este operada por los atacantes. El sitio web falso suele lucir y operar de la misma forma en que lo hace su versión legítima y tiene como fin lograr que la víctima proporcione sus credenciales de acceso y otro tipo de información personal como las respuestas de las preguntas de seguridad, el número de cuenta, el número de seguridad social, la dirección de correo, la dirección de correo electrónico o el número de teléfono. El objetivo de un ataque de suplantación de identidad particular es robar la información de la identidad para robarla o para tomar el control de una cuenta.

Suplantador: una persona que finge ser alguien más para entretener o estafar.

Tailgating: una persona no autorizada que elude los controles de acceso físicos, en general, generando una distracción y siguiendo de cerca a una persona autorizada hacia una habitación o un edificio controlado.

Token de autenticación: también conocido como token de hardware, token de seguridad, token USB, token criptográfico, token de software, token virtual o dispositivo físico. Se utiliza para probar la identidad de una persona de forma electrónica. El token se utiliza como medida adicional a una contraseña o como un reemplazo de esta para una mejor autenticación que pruebe que la persona es quien dice ser.

Violación: el momento en que un hacker logra vulnerar una computadora o un dispositivo y obtiene acceso a sus archivos y red.

Virus: un tipo de malware cuyo fin es corromper, borrar o modificar información de una computadora antes de propagarse en otras computadoras.

Vishing: una forma de suplantación de identidad que ocurre en VoIP. En este ataque, el atacante utiliza sistemas VoIP para llamar a cualquier número de teléfono sin cargo. El atacante suele falsificar su identificador de llamada para hacer creer a la víctima que esta proviene de una fuente legítima o confiable como un banco, una tienda minorista, las fuerzas policiales o una organización benéfica. Las víctimas no necesitan usar el VoIP ellas mismas para sufrir el ataque de vishing por medio de su sistema telefónico.

Vulnerabilidad de seguridad: una aplicación o script malicioso utilizado para beneficiarse de la vulnerabilidad de una computadora.

Vulnerabilidades de día cero: el aprovechamiento de errores de software que antes no eran conocidos para la comunidad de seguridad general a fin de obtener acceso a un sistema informático o aumentar privilegios en este.