Glosario básico de termos de ciberseguridade

20 de marzo de 2024

AES: Advanced Encryption Standard (Estándar de Cifrado Avanzado), un algoritmo de cifrado simétrico amplamente empregado para asegurar datos sensibles.

Algoritmo de cifrado: Unha serie de pasos matemáticos ou lóxicos utilizados para cifrar e descifrar mensaxes.

Ataque de denegación de servizo distribuído (ataque de DDOS): Actividade maliciosa na que atacantes informáticos utilizan varias computadoras (ás veces milleiros) para participar nun ataque sincronizado sobre un sistema específico. Os atacantes adoitan lanzar ataques de DDOS desde botnets, unha colección de dispositivos infectados con malware que actúan en resposta ás ordes dun comando e control de botnet. Os atacantes sobrecargan o sistema obxectivo con solicitudes espurias, dificultando ou facendo imposible que os usuarios lexítimos accedan ao sistema.

Ataque de explotación de vulnerabilidades do DNS: Ataque no cal o atacante aproveita unha vulnerabilidade (por exemplo, un erro ou un fallo de seguridade) no software do servidor do DNS. Algúns atacantes usan esta forma de ataque para desactivar un servidor de nome. Por exemplo, poden crear unha mensaxe non ortodoxa do DNS para facer que o servidor de nome colapse.

Autenticación: O proceso de verificar a identidade dun usuario ou sistema antes de permitir o acceso a recursos.

Autenticidade: A propiedade que verifica que a fonte dunha mensaxe é auténtica e non foi falsificada.

Botnet: Unha colección de ordenadores inocentes comprometidos por código malicioso co fin de executar un axente de control remoto que concede ao atacante a capacidade de aproveitar remotamente os recursos do sistema para realizar accións ilícitas ou criminais. Estas accións inclúen ataques de inundación DoS, aloxamento de falsos servizos web, suplantación de DNS, transmisión de correo non desexado, escoita de comunicacións en rede, gravación de comunicacións VOIP e intentos de quebrantar cifrados ou contrasinais. As botnets poden estar formadas por ducias ou máis dun millón de ordenadores individuais. O termo "botnet" é unha forma abreviada de rede robótica.

Certificado dixital: Unha forma de identificación electrónica que confirma a autenticidade dunha entidade ou sitio web.

Ciberocupación, cybersquatting: Forma de uso indebido na cal unha parte rexistra intencionalmente un nome de dominio que coincide cunha marca comercial ou

o nome dunha persoa coñecida. Despois de adquirir o nome de dominio, o ciberocupante xeralmente ofrece vender o nome ao titular lexítimo a un prezo excesivo.

Ciberseguridade: O conxunto de medidas e prácticas que protexen os sistemas, as redes e os datos en liña contra ameazas e ataques cibernéticos.

Cifrado de chave pública: Un sistema criptográfico no que se utilizan dúas claves relacionadas pero distintas, unha para cifrar e outra para decifrar.

Cifrado simétrico: Un tipo de cifrado no que se utiliza a mesma clave tanto para cifrar como para decifrar a mensaxe.

Clave: Un valor utilizado como entrada para un algoritmo de cifrado, que determina como se realiza a codificación e a decodificación.

Criptografía de curva elíptica: Unha rama da criptografía que utiliza operacións sobre puntos dunha curva elíptica para realizar operacións criptográficas.

Criptografía: O estudo e a práctica de técnicas para a seguridade da información mediante a codificación e decodificación de mensaxes.

DES: O Data Encryption Standard (Estándar de Cifrado de Datos), un algoritmo de cifrado simétrico que foi amplamente utilizado antes da adopción do AES.

Devasa ou firewall: Unha barreira de seguridade que controla o tráfico de rede para protexer os sistemas e as redes de accesos non autorizados ou ameazas externas.

Encriptación: O proceso de codificación de información sensible ou datos para protexelos de accesos non autorizados ou intrusións durante a transmisión.

Enxeñaría Social: Unha táctica de manipulación psicolóxica utilizada para enganar ou convencer a xente a revelar información confidencial ou realizar accións non desexadas.

Lista branca: Un mecanismo de seguridade que prohibe a execución de calquera programa que non estea nunha lista preaprobada de software. A lista branca é frecuentemente un rexistro co nome do ficheiro, a ruta, o tamaño do ficheiro e o valor hash do software aprobado. Calquera código que non estea na lista, xa sexa benigno ou malicioso, non poderá executarse no sistema protexido.

Lista negra: Un mecanismo de seguridade que prohibe a execución daqueles programas que figuran nunha coñecida lista de software malicioso ou non desexado. A lista negra é un rexistro de ficheiros específicos que se sabe que son maliciosos ou, de calquera maneira, non desexados. Calquera programa presente na lista ten prohibido executarse, mentres que calquera outro programa, xa sexa benigno ou malicioso, pode executarse por defecto.

Malware: Programa informático malicioso deseñado para danar ou controlar un sistema.

Parche: Unha actualización de software que soluciona unha vulnerabilidade ou problema de seguridade.

Pharming: Forma de fraude na cal un atacante dirixe aos usuarios de Internet a un sitio web fraudulento coa intención de roubarlles credenciais de inicio de sesión e outros datos sensibles.

Phishing: Unha forma de ataque cibernético onde os estafadores intentan obter información sensible, como contrasinais ou datos financeiros, facéndose pasar por entidades fiables a través de mensaxes enganosas ou sitios web falsos.

PKI: A Infraestrutura de Chave Pública (Public Key Infrastructure), un conxunto de políticas, procedementos e tecnoloxías para xerar, xestionar e verificar claves públicas e privadas.

Protocolo de seguridade: Un conxunto de regras e procedementos que se aplican para garantir a seguridade das comunicacións e interaccións en liña.

Ransomware: Un tipo de malware que cifra os datos dun sistema e esixe un rescate para recuperar o acceso a eles.

RSA: Un algoritmo de cifrado de chave pública amplamente utilizado que leva o nome dos seus creadores, Ron Rivest, Adi Shamir e Leonard Adleman.

Seguridade de rede: As medidas e políticas implementadas para protexer a seguridade das redes informáticas.

Sinatura dixital: Unha técnica criptográfica que utiliza claves públicas e privadas para verificar a autenticidade e integridade dunha mensaxe.

Troco de chaves: O proceso de compartir chaves criptográficas entre as partes que desexan comunicarse de forma segura.

Troiano: Un programa que parece legítimo pero contén unha funcionalidade maliciosa oculta.

Verme ou worm: Un tipo de malware que se propaga automaticamente a través de redes sen necesidade dunha acción do usuario.

Virus: Un tipo de malware que se replica e infecta outros ficheiros e programas.