



Terms

definitions

التعريفات

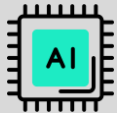
Asset 	An item perceived as having value to an organization	عنصر يُعتبر ذو قيمة للمنظمة
Asset classification 	The process of tracking assets and the risks that affect them	ممارسة تصنيف الأصول بناءً على الحساسية والأهمية للمنظمة
Authentication 	The process of verifying who someone is	عملية التحقق من هوية شخص ما
Authorization 	The concept of granting access to specific resources in a system	مفهوم منح الوصول إلى موارد محددة في النظام
Availability 	The idea that data is accessible to those who are authorized to access it	الفكرة التي تعبر عن أن البيانات يجب أن تكون متاحة للأشخاص المصرح لهم بالوصول إليها
Asymmetric encryption 	The use of a public and private key pair for encryption and decryption of data	استخدام زوج من المفاتيح العامة والخاصة لتشفير وفك تشفير البيانات
Anonymization 	A technique to hide the original identity of users or sensitive data to ensure privacy and protect information	تقنية لإخفاء الهوية الأصلية للمستخدمين أو البيانات الحساسة لضمان الخصوصية وحماية المعلومات
Autonomous Response 	An automatic response to cyberattacks that relies on AI and automation technologies to mitigate threats in real time without human intervention	رد تلقائي على الهجمات السيبرانية يعتمد على تقنيات الذكاء الاصطناعي والأتمتة لتخفيف التهديدات في الوقت الحقيقي دون تدخل بشري

Terms

definitions

التعريفات

AI-powered Cybersecurity



The use of artificial intelligence to analyze security data, identify threats, and make autonomous decisions to enhance system security

استخدام الذكاء الاصطناعي لتحليل البيانات الأمنية، تحديد التهديدات، واتخاذ قرارات تلقائية لتحسين أمان الأنظمة

Antivirus software



A software program used to prevent, detect, and eliminate malware and viruses

برنامج يُستخدم لمنع، كشف، والقضاء على البرمجيات الخبيثة والفيروسات

Adversarial artificial intelligence



A technique that manipulates artificial intelligence (AI) and machine learning (ML) technology to conduct attacks more efficiently

تقنية تُستخدم للتلاعب بتكنولوجيا الذكاء الاصطناعي والتعلم الآلي لتنفيذ الهجمات بكفاءة أكبر

Angler phishing



A technique where attackers impersonate customer service representatives on social media

تقنية ينتحل فيها المهاجمون شخصية ممثلي خدمة العملاء على وسائل التواصل الاجتماعي

Adware



A type of legitimate software that is sometimes used to display digital advertisements in applications

نوع من البرمجيات الشرعية التي تُستخدم أحياناً لعرض الإعلانات الرقمية في التطبيقات

Algorithm



A set of rules used to solve a problem

مجموعة من القواعد المستخدمة لحل مشكلة ما

Access controls



Security controls that manage access, authorization, and accountability of information

ضوابط الأمان التي تدير تفويض الوصول والمساءلة عن المعلومات

Terms

definitions

التعريفات

Analysis 	The investigation and validation of alerts	التحقيق والتحقق من التنبيهات
Active packet sniffing 	A type of attack where data packets are manipulated in transit	نوع من الهجوم حيث يتم التلاعب بحزم البيانات أثناء النقل
Address Resolution Protocol (ARP) 	An instance when a threat actor maintains unauthorized access to a system for an extended period of time	بروتوكول شبكي يستخدم لتحديد عنوان MAC للموجة أو الجهاز التالي على المسار
Anomaly-based analysis 	A detection method that identifies abnormal behavior	طريقة كشف تحدد السلوكيات غير الطبيعية
Application 	A program that performs a specific task	برنامج يؤدي مهمة محددة
Application programming interface (API) token 	A small block of encrypted code that contains information about a user	كتلة صغيرة من الرموز المشفرة التي تحتوي على معلومات عن المستخدم
Advanced Persistent Threat (APT) 	A type of cyberattack where an unauthorized user gains continuous, long-term access to a network to steal sensitive data or spy on the system. These attacks are often attributed to state-sponsored entities	هو نوع من الهجمات السيبرانية التي يتم فيها اختراق الشبكة بشكل مستمر ومتقدم لفترة طويلة من الزمن بهدف سرقة بيانات حساسة أو التجسس على الأنظمة، وغالبًا ما تُنسب هذه الهجمات إلى جهات مدعومة من دول

Terms

definitions

التعريفات

Attack surface 	All the potential vulnerabilities that a threat actor could exploit	جميع النقاط الضعيفة المحتملة التي يمكن للفاعل التهديد استغلالها
Attack tree 	A diagram that maps threats to assets	رسم بياني يربط التهديدات بالأسول
Attack vectors 	The pathways attackers use to penetrate security defenses	المسارات التي يستخدمها المهاجمون لاختراق الدفاعات الأمنية
Attack Chaining 	A series of integrated attacks designed to bypass multiple security layers and achieve a final malicious objective	سلسلة من الهجمات التي تتكامل معًا بهدف تجاوز أنظمة الحماية المتعددة والوصول إلى هدف نهائي
Adaptive Security 	A security model that automatically adapts to continuously changing and evolving threats to ensure system protection	هو نموذج أمني يستخدم التكيف التلقائي مع التهديدات المتغيرة والمتطورة بشكل مستمر لضمان أمان النظام
Access Control List (ACL) 	A list that defines who is allowed to access a system resource and the permissions granted, such as read, write, or modify access	هي قائمة تحدد من يُسمح له بالوصول إلى موارد النظام أو الشبكة، وتحدد أيضًا مستوى الأدونات التي يمكن أن يستخدمها كل كيان (مثل القراءة أو الكتابة أو التعديل)
Anti-forensics 	A set of methods and techniques used by attackers to conceal the traces of their activities and evade detection by digital forensic teams	هي مجموعة من الأساليب والتقنيات التي يستخدمها المهاجمون لإخفاء آثار الهجمات وتجنب اكتشافها من قبل فرق التحقيق الجنائي الرقمي

Terms

definitions

التعريفات

Blue Team



A team responsible for defending an organization's information systems against potential cyber threats, usually in contrast to a red team that acts as an attacker

فريق مسؤول عن الدفاع عن نظم معلومات المؤسسة ضد التهديدات السيبرانية المحتملة، عادةً في مواجهة الفريق الأحمر الذي يقوم بمحاكاة هجمات

Blockchain Security



The application of cryptographic techniques to protect and secure data transactions within a blockchain network

تطبيق تقنيات التشفير لحماية وتأمين المعاملات الرقمية ضمن شبكة سلسلة الكتل

Baiting



A social engineering tactic that tempts people into compromising their security

تكتيك هندسة اجتماعية يغري الأشخاص للتسبب في تعرض أمنهم للخطر

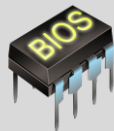
Bandwidth



The maximum data transmission capacity over a network, measured by bits per second

القدرة القصوى لنقل البيانات عبر شبكة محددة بالبتات في الثانية

Basic Input/Output System (BIOS)



A microchip that contains loading instructions for the computer and is prevalent in older systems

شريحة مايكرو تحتوي على تعليمات التحميل للكمبيوتر ومنتشرة في الأنظمة القديمة

Biometrics



The unique physical characteristics that can be used to verify a person's identity

الخصائص الفيزيائية الفريدة التي يمكن استخدامها للتحقق من هوية شخص

Bit



The smallest unit of data measurement on a computer

أصغر وحدة لقياس البيانات في الكمبيوتر

Terms

definitions

التعريفات

Brute force attack



The trial and error process of discovering private information

عملية تجريب وخطأ لاكتشاف معلومات خاصة

Bug bounty



Programs that encourage freelance hackers to find and report vulnerabilities

برامج تشجع القراصنة المستقلين على إيجاد والإبلاغ عن الثغرات الأمنية

Botnet



A collection of computers infected by malware that are under the control of a single threat actor, known as the "bot-herder"

مجموعة من الحواسيب المصابة بالبرمجيات الخبيثة والتي تخضع لسيطرة فاعل تهديدي واحد يُعرف بـ راعي البوت

Broken chain of custody



Inconsistencies in the collection and logging of evidence in the chain of custody

عدم الاتساق في جمع الأدلة وتسجيلها ضمن سلسلة الحيازة

Business continuity



An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans

قدرة المنظمة على الحفاظ على إنتاجيتها اليومية من خلال وضع خطط لاستعادة الكوارث وإدارة المخاطر

Business continuity plan (BCP)



A document that outlines the procedures to sustain business operations during and after a significant disruption

وثيقة تحدد الإجراءات اللازمة للحفاظ على عمليات الأعمال خلال وبعد اضطراب كبير

Business Email Compromise (BEC)



A type of phishing attack where a threat actor impersonates a known source to obtain financial advantage

نوع من هجمات التصيد حيث ينتحل الفاعل التهديدي شخصية مصدر معروف للحصول على ميزة مالية

Terms

definitions

التعريفات

Behavioral Analytics



A method used to detect and respond to anomalies in a user's behavior by analyzing their typical usage patterns

طريقة تُستخدم لاكتشاف الاستثناءات والاستجابة لها في سلوك المستخدم عن طريق تحليل أنماط الاستخدام المعتادة

Black Box Testing



A method of software testing where the tester doesn't know the internal workings of the system and tests the system based only on inputs and outputs

طريقة لاختبار البرمجيات يتم فيها فحص النظام بناءً على المدخلات والمخرجات فقط، دون معرفة العمل الداخلي للنظام

Browser Isolation



A security technique that isolates web browsing activities from the rest of the system to prevent web-based threats from affecting the main environment

تقنية أمان تعزل أنشطة التصفح عن باقي النظام لمنع التهديدات القائمة على الإنترنت من التأثير على البيئة الرئيسية

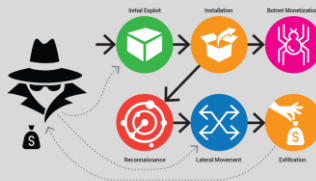
Cryptanalysis



The study of cryptographic systems with the goal of breaking encryption codes and finding weaknesses in cryptographic algorithms

دراسة أنظمة التشفير بهدف كسر الأكواد المشفرة واكتشاف الثغرات في الخوارزميات التشفيرية

Cyber Kill Chain



A framework developed by Lockheed Martin that describes the different stages of a cyberattack, from reconnaissance to data exfiltration

إطار تم تطويره من قبل شركة لوكهيد مارتن يصف المراحل المختلفة للهجوم السيبراني، بدءًا من الاستطلاع وصولاً إلى سرقة البيانات

Terms

definitions

التعريفات

Chain of custody		The process of documenting evidence possession and control during an incident lifecycle	عملية توثيق السيطرة وحيازة الأدلة أثناء دورة حياة الحادث
Chronicle		A cloud-native tool designed to retain, analyze, and search data	أداة سحابية مدمجة مصممة للاحتفاظ وتحليل والبحث في البيانات
Cipher		An algorithm that encrypts information	خوارزمية تقوم بتشفير المعلومات
Cloud-based firewalls		Software firewalls that are hosted by the cloud service provider	جدران حماية برمجية تستضيفها مزودات الخدمات السحابية
Cloud computing		The practice of using remote servers, applications, and network services that are hosted on the internet instead of on local physical devices	استخدام الخوادم والخدمات والتطبيقات والشبكات عن بُعد المستضافة على الإنترنت بدلاً من الأجهزة المحلية
Cloud network		A collection of servers or computers that stores resources and data in remote data centers that can be accessed via the internet	مجموعة من الخوادم أو الحواسيب التي تخزن الموارد والبيانات في مراكز بيانات بعيدة يمكن الوصول إليها عبر الإنترنت
Cloud security		The process of ensuring that assets stored in the cloud are properly configured and access to those assets is limited to authorized users	عملية ضمان أن الأصول المخزنة في السحابة تم تكوينها بشكل صحيح وأن الوصول إلى تلك الأصول يقتصر على المستخدمين المصرح لهم

Terms

definitions

التعريفات

Compliance 	The process of adhering to internal standards and external regulations	عملية الامتثال للمعايير الداخلية واللوائح الخارجية
Command and control (C2) 	The techniques used by malicious actors to maintain communications with compromised systems	تقنيات يستخدمها المهاجمون للحفاظ على التواصل مع الأنظمة المخترقة
Command-line interface (CLI) 	A text-based user interface that uses commands to interact with the computer	واجهة نصية يستخدمها المستخدم للتفاعل مع الكمبيوتر عبر الأوامر
Common Event Format (CEF) 	A log format that uses key-value pairs to structure data and identify fields and their corresponding values	صيغة لتسجيل الأحداث تستخدم أزواج المفتاح والقيمة لتنظيم البيانات
Common Vulnerabilities and Exposures (CVE®) list 	An openly accessible dictionary of known vulnerabilities and exposures	قاموس متاح للجميع يحتوي على الثغرات والتعرضات المعروفة
Common Vulnerability Scoring System (CVSS) 	A measurement system that scores the severity of a vulnerability	نظام لقياس شدة الثغرات
Command 	An instruction telling the computer to do something	تعليمات تُعطى للكمبيوتر لتنفيذ شيء معين

Terms

definitions

التعريفات

Computer security incident response teams (CSIRT)



A specialized group of security professionals that are trained in incident management and response

مجموعة متخصصة من المحترفين الأمنيين المدربين على إدارة الحوادث والاستجابة لها

Computer virus



Malicious code written to interfere with computer operations and cause damage to data and software

كود ضار مكتوب للتدخل في عمليات الكمبيوتر والتسبب في ضرر للبيانات والبرمجيات

Cyber Threat Intelligence (CTI)



Information about potential threats, including tactics, techniques, and procedures (TTPs) used by attackers, which helps organizations proactively defend against cyber threats

معلومات حول التهديدات المحتملة، بما في ذلك التكتيكات والتقنيات والإجراءات التي يستخدمها المهاجمون، مما يساعد المؤسسات على الدفاع الاستباقي ضد التهديدات السيبرانية

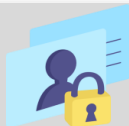
Confidentiality



The idea that only authorized users can access specific assets or data

الفكرة التي تعني أن البيانات يمكن الوصول إليها فقط من قبل المستخدمين المصرح لهم

Confidential data



Data that often has limits on the number of people who have access to it

بيانات غالبًا ما تكون مقيدة بعدد محدود من الأشخاص الذين يمكنهم الوصول إليها

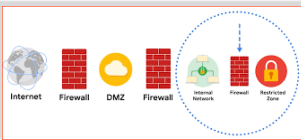
Confidentiality, integrity, availability (CIA) triad



A model that helps inform how organizations consider risk when setting up systems and security policies

نموذج يساعد المنظمات في تقييم المخاطر عند إعداد الأنظمة والسياسات الأمنية

Controlled zone



A subnet that protects the internal network from the uncontrolled zone

شبكة فرعية تحمي الشبكة الداخلية من المنطقة غير الخاضعة للتحكم

Terms

definitions

التعريفات

Cross-site scripting (XSS)



An injection attack that inserts code into a vulnerable website or web application

هجوم إدخال يقوم بإدخال كود في موقع أو تطبيق ويب ضعيف

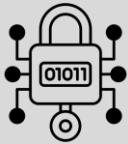
Certificate Authority (CA)



An entity that issues digital certificates, which are used to verify the identity of a user or device in a secure environment

كيان يقوم بإصدار الشهادات الرقمية التي تستخدم للتحقق من هوية المستخدم أو الجهاز في بيئة آمنة

Cryptographic attack



An attack that affects secure forms of communication between a sender and intended recipient

هجوم يستهدف طرق الاتصال الآمنة بين المرسل والمستلم

Cryptographic key



A mechanism that decrypts ciphertext

آلية تُستخدم لفك تشفير النص المشفر

Cryptography



The process of transforming information into a form that unintended readers can't understand

عملية تحويل المعلومات إلى صيغة لا يمكن لغير المستهدفين فهمها

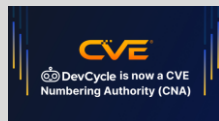
Cryptojacking



A form of malware that installs software to illegally mine cryptocurrencies

نوع من البرمجيات الخبيثة التي تقوم بتنصيب برامج لتعدين العملات الرقمية بشكل غير قانوني

CVE Numbering Authority (CNA)



An organization that volunteers to analyze and distribute information on eligible CVEs

منظمة تتطوع لتحليل وتوزيع المعلومات حول الثغرات المؤهلة في قائمة CVE

Terms

definitions

التعريفات

Cybersecurity (or security)



The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation

ممارسة ضمان السرية والسلامة والتوافر للمعلومات عن طريق حماية الشبكات والأجهزة والأشخاص والبيانات من الوصول غير المصرح به أو الاستغلال الإجرامي

Data



Information that is translated, processed, or stored by a computer

المعلومات التي يتم ترجمتها أو معالجتها أو تخزينها بواسطة الكمبيوتر

Data at rest



Data not currently being accessed

البيانات التي لا يتم الوصول إليها حاليًا

Data in transit



Data traveling from one point to another

البيانات التي تنتقل من نقطة إلى أخرى

Data in use



Data being accessed by one or more users

البيانات التي يتم الوصول إليها من قبل مستخدم واحد أو أكثر

Data controller



A person that determines the procedure and purpose for processing data

شخص يحدد الإجراء والغرض من معالجة البيانات

Data owner



The person who decides who can access, edit, use, or destroy their information

الشخص الذي يقرر من يمكنه الوصول إلى معلوماته أو تعديلها أو استخدامها أو تدميرها

Terms

definitions

التعريفات

Defense in depth



A layered approach to vulnerability management that reduces risk

نهج متعدد الطبقات لإدارة الثغرات يقلل من المخاطر

Denial of service (DoS) attack



An attack that targets a network or server and floods it with network traffic

هجوم يستهدف شبكة أو خادم ويغمره بحركة مرور الشبكة

Distributed denial of service (DDoS) attack



A type of denial or service attack that uses multiple devices or servers located in different locations to flood the target network with unwanted traffic

نوع من هجمات حجب الخدمة يتم فيه استخدام أجهزة أو خوادم متعددة في مواقع مختلفة لإغراق الشبكة بحركة مرور غير مرغوبة

Debugging



The practice of identifying and fixing errors in code

ممارسة تحديد وإصلاح الأخطاء في الكود

Detection



The prompt discovery of security events

الاكتشاف السريع للأحداث الأمنية

Dictionary data



Data that consists of one or more key-value pairs

بيانات تتألف من زوج أو أكثر من أزواج المفتاح والقيمة

Digital certificate



A file that verifies the identity of a public key holder

ملف يتحقق من هوية حامل المفتاح العام

Terms

definitions

التعريفات

Data Loss Prevention (DLP)



A strategy used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users by monitoring, detecting, and blocking potential threats

استراتيجية تُستخدم لضمان عدم فقدان البيانات الحساسة أو إساءة استخدامها أو الوصول إليها من قبل مستخدمين غير مصرح لهم، وذلك عن طريق مراقبة التهديدات المحتملة واكتشافها ومنعها

Decentralized Identity



A digital identity system where control of the identity is not maintained by a central authority but is instead distributed among users and service providers

نظام هوية رقمية لا يتم التحكم فيه من قبل سلطة مركزية، بل يتم توزيعه بين المستخدمين ومزودي الخدمة

Deception Technology



A cybersecurity strategy that deploys decoys and traps to mislead and distract attackers, making it harder for them to identify real targets

استراتيجية في الأمن السيبراني تستخدم الفخاخ والأهداف المزيفة لتضليل المهاجمين وتشتيتهم، مما يجعل من الصعب عليهم تحديد الأهداف الحقيقية

Digital Footprint



The trail of data left behind by users as they interact with various websites, services, and online platforms, which can be used to track and identify them

سلسلة البيانات التي يتركها المستخدمون أثناء تفاعلهم مع مواقع الويب والخدمات والمنصات الإلكترونية، والتي يمكن استخدامها لتتبعهم وتحديد هويتهم

DNS Spoofing



A type of attack where a hacker alters DNS records to redirect internet traffic to malicious websites

نوع من الهجمات حيث يقوم المهاجم بتعديل سجلات DNS لإعادة توجيه حركة مرور الإنترنت إلى مواقع ضارة

Terms

definitions

التعريفات

Digital forensics



The practice of collecting and analyzing data to determine what has happened after an attack

ممارسة جمع وتحليل البيانات لتحديد ما حدث بعد الهجوم

Disaster recovery plan



A plan that allows an organization's security team to outline the steps needed to minimize the impact of a security incident

خطة تتيح لفريق الأمان تحديد الخطوات اللازمة لتقليل تأثير الحادث الأمني

Domain Name System (DNS)



A networking protocol that translates internet domain names into IP addresses

بروتوكول شبكة يترجم أسماء النطاقات على الإنترنت إلى عناوين IP

Dropper



A program or a file used to install a rootkit on a target computer

برنامج أو ملف يستخدم لتثبيت برنامج rootkit على جهاز مستهدف

Encryption



The process of converting data from a readable format to an encoded format

عملية تحويل البيانات من صيغة قابلة للقراءة إلى صيغة مشفرة

Endpoint detection and response (EDR)



An application that monitors an endpoint for malicious activity

تطبيق يراقب نقطة النهاية للكشف عن الأنشطة الخبيثة

Eradication



The complete removal of the incident elements from all affected systems

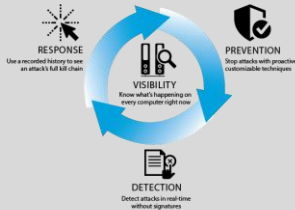
الإزالة الكاملة لعناصر الحادث من جميع الأنظمة المتأثرة

Terms

definitions

التعريفات

Endpoint Detection and Response (EDR)



A security solution that monitors and collects activity data from endpoints to detect and respond to potential security incidents

حل أمني يراقب ويجمع بيانات الأنشطة من نقاط النهاية لاكتشاف والاستجابة للحوادث الأمنية المحتملة

Encryption



The process of converting data into a code to prevent unauthorized access

عملية تحويل البيانات إلى رمز لمنع الوصول غير المصرح به

Exploit



A method or technique used to take advantage of a vulnerability in a system or application

طريقة أو تقنية تُستخدم للاستفادة من ثغرة في النظام أو التطبيق

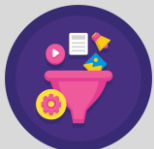
Event



Any observable occurrence in a system or network that may indicate a security incident

أي واقعة قابلة للملاحظة في نظام أو شبكة قد تشير إلى حادث أمني

Eradication



The process of completely removing malicious software or eliminating a security threat from affected systems

عملية إزالة البرمجيات الخبيثة أو القضاء على تهديد أمني من الأنظمة المتأثرة بالكامل

Terms

definitions

التعريفات

Escalation policy



A set of actions that outline who should be notified when an incident alert occurs and how that incident should be handled

مجموعة من الإجراءات التي تحدد من يجب إخطاره عند حدوث تنبيه عن حادث وكيفية التعامل مع هذا الحادث

Event



An observable occurrence on a network, system, or device

حدث يمكن ملاحظته على نظام أو شبكة أو جهاز

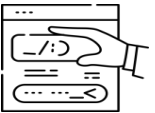
Exception



An error that involves code that cannot be executed even though it is syntactically correct

خطأ ينطوي على كود لا يمكن تنفيذه على الرغم من صحته النحوية

Exploit



A way of taking advantage of a vulnerability

طريقة للاستفادة من الثغرة

Exposure



A mistake that can be exploited by a threat

خطأ يمكن استغلاله من قبل فاعل تهديدي

External threat



Anything outside the organization that has the potential to harm organizational assets

أي شيء خارج المنظمة قد يسبب ضررًا لأصولها

Fileless malware



Malware that does not need to be installed by the user because it uses legitimate programs that are already installed to infect a computer

برمجيات خبيثة لا تتطلب التثبيت من قبل المستخدم لأنها تستخدم برامج مشروعة موجودة بالفعل لإصابة الكمبيوتر

Terms

definitions

التعريفات

False negative



A state where the presence of a threat is not detected

حالة عدم اكتشاف وجود تهديد

False positive



An alert that incorrectly detects the presence of a threat

تنبيه خاطئ يكشف عن وجود تهديد بينما لا يوجد تهديد فعليًا

Filtering



Selecting data that match a certain condition

اختيار البيانات التي تطابق شرطًا معينًا

Firewall



A network security device that monitors traffic to or from a network

جهاز أمان للشبكة يراقب حركة المرور من وإلى الشبكة

Forward proxy server



and restricts a person's access to the internet

خادم ينظم ويقيّد وصول الشخص إلى الإنترنت

Foreign key



A column in a table that is a primary key in another table

عمود في جدول يكون مفتاحًا رئيسيًا في جدول آخر

Function



A section of code that can be reused in a program

جزء من الكود يمكن إعادة استخدامه داخل برنامج

Terms

definitions

التعريفات

Federated Identity Management (FIM)



A system that allows users to access multiple applications or services with a single set of credentials, typically across different organizations

نظام يتيح للمستخدمين الوصول إلى تطبيقات أو خدمات متعددة باستخدام مجموعة واحدة من بيانات الاعتماد، وغالبًا عبر مؤسسات مختلفة

File Integrity Monitoring (FIM)



A security process that involves monitoring files to detect any unauthorized changes, often used to ensure data integrity

عملية أمنية تشمل مراقبة الملفات لاكتشاف أي تغييرات غير مصرح بها، وتستخدم عادة لضمان سلامة البيانات

Forensic Readiness



The ability of an organization to collect, preserve, and analyze digital evidence in preparation for legal or investigative proceedings

قدرة المؤسسة على جمع وحفظ وتحليل الأدلة الرقمية للتحضير للإجراءات القانونية أو التحقيقات

Full Disk Encryption (FDE)



A security measure that encrypts all the data on a hard drive, ensuring that it is protected from unauthorized access

إجراء أمني يقوم بتشفير جميع البيانات على القرص الصلب، لضمان حمايتها من الوصول غير المصرح به

Fuzz Testing (Fuzzing)



A software testing technique that inputs random or invalid data into a program to find vulnerabilities or unexpected behavior

تقنية لاختبار البرمجيات تقوم بإدخال بيانات عشوائية أو غير صالحة في البرنامج لاكتشاف الثغرات أو السلوك غير المتوقع

Terms

definitions

التعريفات

Grayware



Software that is not entirely malicious but can be intrusive or annoying, such as adware or spyware

برمجيات ليست خبيثة بالكامل لكنها قد تكون مزعجة أو متطفلة، مثل برامج الإعلانات أو برامج التجسس

Geofencing



A location-based security feature that creates virtual boundaries to restrict access to data or devices based on physical location

ميزة أمنية تعتمد على الموقع الجغرافي تقوم بإنشاء حدود افتراضية لتقييد الوصول إلى البيانات أو الأجهزة بناءً على الموقع الفعلي

Governance, Risk, and Compliance (GRC)



A framework that helps organizations manage governance, risk, and compliance in an integrated manner to meet business objectives

إطار عمل يساعد المؤسسات في إدارة الحوكمة والمخاطر والامتثال بشكل متكامل لتحقيق الأهداف التجارية

Guest Network



A separate network set up to provide internet access for visitors without compromising the security of the main network

شبكة منفصلة تُنشأ لتوفير الوصول إلى الإنترنت للزوار دون التأثير على أمان الشبكة الرئيسية

Gap Analysis



A process of comparing current security performance to desired performance in order to identify gaps and areas for improvement

عملية مقارنة الأداء الأمني الحالي مع الأداء المطلوب لتحديد الفجوات والمجالات التي تحتاج إلى تحسين

Terms

definitions

التعريفات

Graphical user interface (GUI)



A user interface that uses icons on the screen to manage different tasks on the computer

واجهة مستخدم تستخدم الرموز لإدارة المهام المختلفة على الكمبيوتر

Hacker



Any person or group who uses computers to gain unauthorized access to data

أي شخص أو مجموعة تستخدم أجهزة الكمبيوتر للوصول غير المصرح به إلى البيانات

Hacktivist



A person who uses hacking to achieve a political goal

شخص يستخدم القرصنة لتحقيق هدف سياسي

Hash Collision



An event where two different inputs produce the same hash value, leading to potential security vulnerabilities

حالة تنتج فيها مدخلات مختلفة نفس القيمة التجزئية، مما قد يؤدي إلى ثغرات أمنية محتملة

Hash function



An algorithm that produces a code that can't be decrypted

خوارزمية تنتج رمزًا لا يمكن فك تشفيره

Hash table



A data structure that's used to store and reference hash values

بنية بيانات تُستخدم لتخزين القيم الهاشمية والإشارة إليها

Terms

definitions

التعريفات

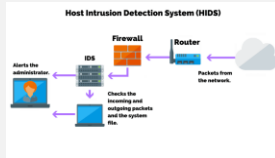
Honeypot



A security mechanism designed to lure attackers by simulating a vulnerable system, allowing defenders to monitor and analyze attacks

آلية أمنية تُصمم لجذب المهاجمين من خلال محاكاة نظام ضعيف، مما يسمح للمختصين بمراقبة وتحليل الهجمات

Host-based Intrusion Detection System (HIDS)



A system that monitors the activity on a specific host or device to detect unauthorized access or malicious behavior

نظام يراقب الأنشطة على جهاز محدد لاكتشاف الوصول غير المصرح به أو السلوكيات الضارة

Hash Function



An algorithm that converts data into a fixed-size hash value, which cannot be reversed to retrieve the original input

خوارزمية تحول البيانات إلى قيمة تجزئة ثابتة الحجم لا يمكن عكسها لاسترجاع المدخل الأصلي

Hypertext Transfer Protocol (HTTP)

http://

An application layer protocol that provides a method of communication between clients and website servers

بروتوكول طبقة التطبيق الذي يوفر وسيلة للتواصل بين العملاء وخوادم الويب

Hypertext Transfer Protocol Secure (HTTPS)



A network protocol that provides a secure method of communication between clients and website servers

بروتوكول شبكة يوفر وسيلة آمنة للتواصل بين العملاء وخوادم الويب

Identity and access management (IAM)



A collection of processes and technologies that helps organizations manage digital identities in their environment

مجموعة من العمليات والتقنيات التي تساعد المنظمات في إدارة الهويات الرقمية داخل بيئاتها

Terms

definitions

التعريفات

Incident response



An organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach

محاولة المنظمة السريعة لتحديد الهجوم، احتواء الضرر، وتصحيح آثار الاختراق الأمني

Incident response plan



A document that outlines the procedures to take in each step of incident response

وثيقة توضح الإجراءات المتخذة في كل خطوة من خطوات الاستجابة للحوادث

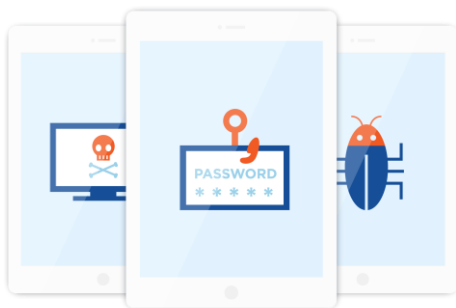
Indicators of attack (IoA)



The series of observed events that indicate a real-time incident

سلسلة من الأحداث الملاحظة التي تشير إلى حادث أمني في الوقت الفعلي

Incident



An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies

حدث يهدد أو ينتهك السرية أو السلامة أو التوفر للمعلومات أو أنظمة المعلومات؛ أو يشكل انتهاكاً أو تهديداً وشيكاً لانتهاك القوانين أو السياسات الأمنية أو إجراءات الأمان أو سياسات الاستخدام المقبول

Incident escalation



The process of identifying a potential security incident, triaging it, and handing it off to a more experienced team member

عملية تحديد حادث أمني محتمل وتصنيفه وتحويله إلى عضو فريق أكثر خبرة

Terms

definitions

التعريفات

Indicators of compromise (IoC)



Observable evidence that suggests signs of a potential security incident

أدلة ملاحظة تشير إلى علامات حادث أمني محتمل

Information privacy



The protection of unauthorized access and distribution of data

حماية البيانات من الوصول غير المصرح به أو توزيعها

Information security (InfoSec)



The practice of keeping data in all states away from unauthorized users

ممارسة حماية البيانات في جميع حالاتها من المستخدمين غير المصرح لهم

Injection attack



Malicious code inserted into a vulnerable application

إدخال كود خبيث في تطبيق ضعيف

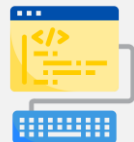
Input validation



Programming that validates inputs from users and other programs

برمجة تتحقق من المدخلات القادمة من المستخدمين أو البرامج الأخرى

Integrated development environment (IDE)



A software application for writing code that provides editing assistance and error correction tools

تطبيق برمجي لكتابة الكود يوفر أدوات مساعدة للتعديل وتصحيح الأخطاء

Integrity



The idea that the data is correct, authentic, and reliable

فكرة أن البيانات صحيحة، موثوقة، وأصلية

Terms

definitions

التعريفات

Internet Control Message Protocol (ICMP)



An internet protocol used by devices to tell each other about data transmission errors across the network

بروتوكول إنترنت يُستخدم لإبلاغ الأجهزة عن أخطاء في نقل البيانات عبر الشبكة

Internet Control Message Protocol flood (ICMP flood)



A type of DoS attack performed by an attacker repeatedly sending ICMP request packets to a network server

نوع من هجمات حجب الخدمة (DoS) حيث يقوم المهاجم بإرسال حزم ICMP بشكل متكرر إلى خادم الشبكة

Internet Protocol (IP)



A set of standards used for routing and addressing data packets as they travel between devices on a network

مجموعة من المعايير المستخدمة لتوجيه ومعالجة حزم البيانات أثناء انتقالها بين الأجهزة على الشبكة

Internet Protocol (IP) address



A unique string of characters that identifies the location of a device on the internet

سلسلة فريدة من الأحرف تحدد موقع جهاز على الإنترنت

Interpreter



A computer program that translates Python code into runnable instructions line by line

برنامج يقوم بترجمة كود بايثون إلى تعليمات قابلة للتنفيذ سطرًا بسطر

Internal hardware



The components required to run the computer

المكونات المطلوبة لتشغيل الكمبيوتر

Terms

definitions

التعريفات

Insider Threat



A security risk that originates from within the organization, typically involving an employee, contractor, or trusted business partner who has access to sensitive information

خطر أمني ينشأ من داخل المنظمة، ويتضمن عادةً موظفًا أو مقاولًا أو شريكًا تجاريًا موثوقًا به لديه وصول إلى معلومات حساسة

IPsec (Internet Protocol Security)



A protocol suite for securing internet communications by authenticating and encrypting each IP packet during a communication session

مجموعة من البروتوكولات لتأمين الاتصالات عبر الإنترنت عن طريق المصادقة وتشفير كل حزمة IP أثناء جلسة الاتصال

Identity Federation



The process that enables users to access multiple applications and services across different organizations using the same login credentials

عملية تتيح للمستخدمين الوصول إلى تطبيقات وخدمات متعددة عبر مؤسسات مختلفة باستخدام بيانات اعتماد تسجيل دخول واحدة

Immutable Infrastructure



An infrastructure design where components (like servers or virtual machines) are never modified after deployment, and any changes require the deployment of new versions

تصميم بنية تحتية حيث لا يتم تعديل المكونات (مثل الخوادم أو الأجهزة الافتراضية) بعد نشرها، وأي تغييرات تتطلب نشر إصدارات جديدة

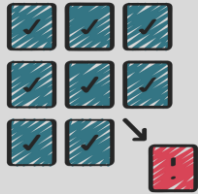
Cyber Security Glossary

Terms

definitions

التعريفات

Isolation



The act of segregating systems, networks, or data from each other to reduce security risks, often used to prevent the spread of malware or restrict unauthorized access

عملية فصل الأنظمة أو الشبكات أو البيانات عن بعضها البعض لتقليل المخاطر الأمنية، وغالبًا ما تُستخدم لمنع انتشار البرمجيات الخبيثة أو تقييد الوصول غير المصرح به

Intrusion detection system (IDS)



An application that monitors system activity and alerts on possible intrusions

تطبيق يراقب نشاط النظام وينبه المستخدمين إلى حالات التطفل المحتملة

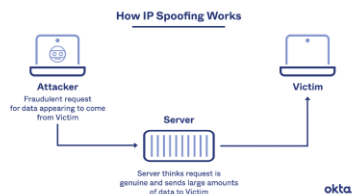
Intrusion prevention system (IPS)



An application that monitors system activity for intrusive activity and takes action to stop the activity

تطبيق يراقب نشاط النظام ليرصد الأنشطة التطفلية ويتخذ إجراءات لإيقافها

IP spoofing



A network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network

هجوم شبكة يقوم فيه المهاجم بتغيير مصدر عنوان IP لحزمة البيانات ليبدو وكأنه نظام موثوق

Jump Box



A secure server that administrators use to connect to and manage other systems within a network, providing a layer of security between external and internal systems

خادم آمن يستخدمه المسؤولون للاتصال وإدارة الأنظمة الأخرى داخل الشبكة، ويوفر طبقة إضافية من الأمان بين الأنظمة الخارجية والداخلية

Terms

definitions

التعريفات

Jailbreaking



The process of removing software restrictions imposed by the manufacturer on devices, such as smartphones, to allow users to install unauthorized apps

عملية إزالة القيود البرمجية التي يفرضها المصنع على الأجهزة، مثل الهواتف الذكية، للسماح للمستخدمين بتثبيت التطبيقات غير المصرح بها

Jamming



A cyberattack aimed at disrupting the communication signals of a device or network by overwhelming it with excessive noise or interference

هجوم إلكتروني يهدف إلى تعطيل إشارات الاتصالات الخاصة بجهاز أو شبكة عن طريق غمرها بالضجيج أو التداخل المفرط

JSON Web Token (JWT)



An open standard used for securely transmitting information between parties as a JSON object, often used in authentication

تكتيك هندسة اجتماعية يغري الأشخاص للتسبب في تعرض أمنهم للخطر

Just-in-Time (JIT) Access



A security approach that grants access to systems or data only when needed, reducing the window of opportunity for unauthorized access

نهج أمني يمنح الوصول إلى الأنظمة أو البيانات فقط عند الحاجة، مما يقلل من فرصة الوصول غير المصرح به

Terms

definitions

التعريفات

Key Escrow



A system where cryptographic keys are stored with a third party to be accessed in case of need, such as data recovery

نظام يتم فيه تخزين مفاتيح التشفير مع طرف ثالث للوصول إليها عند الحاجة، مثل استعادة البيانات

Kerberos



A network authentication protocol that works on the basis of "tickets" to allow nodes to prove their identity securely over a non-secure network

بروتوكول مصادقة شبكي يعتمد على "التذاكر" للسماح للأجهزة بإثبات هويتها بشكل آمن عبر شبكة غير آمنة

Keylogger



A type of spyware that records keystrokes made by a user to capture sensitive information like passwords or credit card numbers

نوع من برامج التجسس يقوم بتسجيل ضربات لوحة المفاتيح التي يقوم بها المستخدم لسرقة معلومات حساسة مثل كلمات المرور أو أرقام البطاقات الائتمانية

Knowledge-Based Authentication (KBA)



A method of verifying identity by asking questions that are based on information the individual knows, such as personal history

طريقة للتحقق من الهوية عن طريق طرح أسئلة تستند إلى معلومات يعرفها الفرد، مثل تاريخه الشخصي

Key Exchange



A process in cryptography where cryptographic keys are exchanged between users or systems securely to establish a shared secret for secure communication

عملية في التشفير يتم فيها تبادل مفاتيح التشفير بين المستخدمين أو الأنظمة بشكل آمن لإنشاء سر مشترك للتواصل الآمن

Terms

definitions

التعريفات

Log



A record of events that occur within an organization's systems

سجل للأحداث التي تحدث داخل أنظمة المؤسسة

Log analysis



The process of examining logs to identify events of interest

عملية فحص السجلات لتحديد الأحداث ذات الأهمية

Logging



The recording of events occurring on computer systems and networks

عملية تسجيل الأحداث التي تحدث على أنظمة الكمبيوتر والشبكات

Log Correlation



is the process of linking related log events from different sources to identify patterns or incidents

هو عملية ربط الأحداث المتعلقة بالسجلات من مصادر مختلفة لتحديد الأنماط أو الحوادث.

Log Retention Policy



A policy that defines how long logs are stored before being deleted. Proper log retention is essential for forensics, compliance, and incident response, ensuring that relevant data is available for analysis when needed

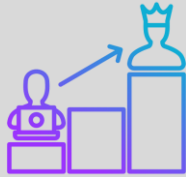
سياسة تحدد المدة الزمنية التي يتم فيها الاحتفاظ بالسجلات قبل حذفها. يعد الاحتفاظ بالسجلات بشكل صحيح ضروريًا للتحقيقات الجنائية الرقمية والامتثال والاستجابة للحوادث

Terms

definitions

التعريفات

Least Privilege



A security principle that restricts users' access rights to only what they need to perform their job functions. By minimizing access, it reduces the risk of unauthorized access or privilege escalation attacks

مبدأ أمني يقضي بمنح المستخدمين أو الأنظمة الحد الأدنى من الصلاحيات التي يحتاجونها للقيام بمهامهم. يهدف إلى تقليل مخاطر الوصول غير المصرح به أو تصعيد الامتيازات

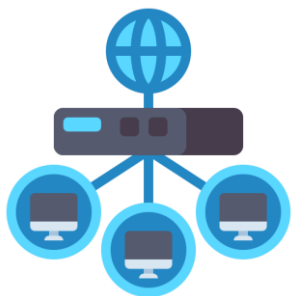
Log Aggregation



The process of collecting and consolidating log data from various sources into a centralized repository for easier analysis, monitoring, and detection of security incidents. This is often done in conjunction with a SIEM solution

عملية جمع وتوحيد بيانات السجلات من مصادر متعددة في مستودع مركزي لتسهيل التحليل والمراقبة والكشف عن الحوادث الأمنية تُستخدم هذه العملية غالبًا مع حلول SIEM

Load Balancer



A device or software application that distributes network or application traffic across multiple servers to ensure reliability, availability, and optimal performance. In cybersecurity, load balancers help protect systems from being overwhelmed by traffic, especially during Distributed Denial of Service (DDoS) attacks

جهاز أو تطبيق برمجي يقوم بتوزيع حركة المرور على الشبكة أو التطبيقات عبر عدة خوادم لضمان الكفاءة والاعتمادية والأداء الأمثل. في الأمن السيبراني، يساعد موازن الحمل في حماية الأنظمة من هجمات DDoS

Log management



The process of collecting, storing, analyzing, and disposing of log data

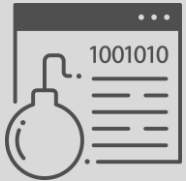
عملية جمع وتخزين وتحليل والتخلص من بيانات السجلات

Terms

definitions

التعريفات

Logic Bomb



A malicious code inserted into a system that remains dormant until triggered by a specific condition, such as a date or event. Once triggered, it can execute harmful actions like deleting files or corrupting data

كود ضار يُدرج في النظام ويبقى خاملاً حتى يتم تفعيله بشروط معينة، مثل تاريخ أو حدث محدد. عند التفعيل، يمكن أن ينفذ إجراءات ضارة مثل حذف الملفات أو إفساد البيانات

Malware



Software designed to harm devices or networks

برامج تم تصميمها لإلحاق الضرر بالأجهزة أو الشبكات

Malware infection



An incident type that occurs when malicious software designed to disrupt a system infiltrates an organization's computers or network

نوع من الحوادث يحدث عندما تتسلل برامج خبيثة إلى أجهزة الكمبيوتر أو الشبكات الخاصة بالمنظمة

Media Access Control (MAC) address



A unique alphanumeric identifier that is assigned to each physical device on a network

معرف أبجدي رقمي فريد يتم تعيينه لكل جهاز مادي على الشبكة

Metrics



Key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application

سمات تقنية رئيسية مثل وقت الاستجابة، التوفر، ومعدل الفشل، التي تستخدم لتقييم أداء تطبيق برمجي

Modem



A device that connects your router to the internet and brings internet access to the LAN

جهاز يربط جهاز التوجيه بالإنترنت ويزود الشبكة المحلية بإمكانية الوصول إلى الإنترنت

Terms

definitions

التعريفات

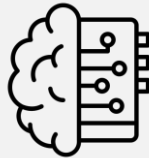
Multi-factor Authentication (MFA)



A security measure that requires users to verify their identity using two or more authentication methods, such as a password and a security token

إجراء أمني يتطلب من المستخدمين التحقق من هويتهم باستخدام طريقتين أو أكثر من طرق المصادقة، مثل كلمة المرور ورمز الأمان

Machine Learning (ML)



A subset of artificial intelligence (AI) that enables systems to learn from data patterns and improve their performance without being explicitly programmed

فرع من الذكاء الاصطناعي يسمح للأنظمة بالتعلم من أنماط البيانات وتحسين أدائها دون الحاجة إلى برمجتها بشكل مباشر

Man-in-the-Middle Attack (MitM)



A type of cyberattack where the attacker intercepts communications between two parties to steal or alter the data being exchanged

نوع من الهجمات السيبرانية حيث يعترض المهاجم الاتصالات بين طرفين لسرقة البيانات أو تغييرها أثناء التبادل

Non-repudiation



The concept that the authenticity of information can't be denied

مفهوم يعني أن مصداقية المعلومات لا يمكن إنكارها

Notebook



An online interface for writing, storing, and running code

واجهة عبر الإنترنت لكتابة وتخزين وتشغيل الكود

Cyber Security Glossary

Terms

definitions

التعريفات

National Institute of Standards and Technology (NIST)
Cybersecurity Framework (CSF)



A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk

إطار عمل طوعي يتكون من معايير وإرشادات وأفضل الممارسات لإدارة مخاطر الأمن السيبراني

National Institute of Standards and Technology (NIST)
Incident Response Lifecycle



A framework for incident response consisting of four phases: Preparation; Detection and Analysis; Containment, Eradication and Recovery, and Post-incident activity

إطار للاستجابة للحوادث يتكون من أربع مراحل: التحضير؛ الكشف والتحليل؛ الاحتواء والإزالة والتعافي؛ والنشاطات اللاحقة للحدث

National Institute of Standards and Technology (NIST)
Special Publication (S.P.) 800-53



A unified framework for protecting the security of information systems within the U.S. federal government

إطار موحد لحماية أمن نظم المعلومات داخل الحكومة الفيدرالية الأمريكية

Network



A group of connected devices

مجموعة من الأجهزة المتصلة مع بعضها البعض

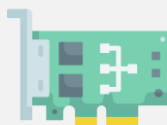
Network data



The data that's transmitted between devices on a network

البيانات التي يتم نقلها بين الأجهزة على الشبكة

Network Interface Card (NIC)



Hardware that connects computers to a network

مكون مادي يربط أجهزة الكمبيوتر بالشبكة

Terms

definitions

التعريفات

Network-based intrusion
detection system (NIDS)



An application that collects and monitors
network traffic and network data

تطبيق يجمع ويراقب حركة مرور الشبكة والبيانات
المتعلقة بالشبكة

Network log analysis



The process of examining network logs to
identify events of interest

عملية فحص سجلات الشبكة لتحديد الأحداث ذات الأهمية

Network protocol analyzer
(packet sniffer)



A tool designed to capture and analyze data
traffic within a network

أداة مصممة لالتقاط وتحليل حركة مرور البيانات داخل
الشبكة

Network protocols



A set of rules used by two or more devices
on a network to describe the order of
delivery and the structure of data

مجموعة من القواعد التي تستخدمها جهازان أو أكثر على
الشبكة لتنظيم تسليم البيانات وهيكلتها

Network security



The practice of keeping an organization's
network infrastructure secure from
unauthorized access

ممارسة حماية بنية الشبكة التحتية للمنظمة من الوصول
غير المصرح به

Network segmentation



A security technique that divides the
network into segments

تقنية أمنية تقسم الشبكة إلى أجزاء segments
لتقليل مخاطر الهجمات

Network traffic



The amount of data that moves across a
network

كمية البيانات التي تنتقل عبر شبكة معينة

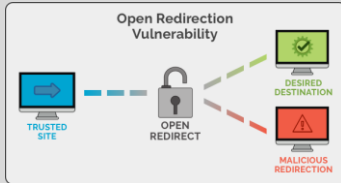
Cyber Security Glossary

Terms

definitions

التعريفات

Open Redirect



A security vulnerability that occurs when a web application accepts user input for URLs without proper validation, allowing attackers to redirect users to malicious sites

ثغرة أمنية تحدث عندما يقبل تطبيق ويب إدخال روابط من المستخدمين دون التحقق المناسب، مما يسمح URL للمهاجمين بإعادة توجيه المستخدمين إلى مواقع ضارة

OWASP Top 10



A globally recognized standard awareness document that lists the top 10 most critical security risks to web applications

مستند توعية معترف به عالميًا يسرد أهم 10 مخاطر أمنية تهدد تطبيقات الويب

OAuth



An open-standard authorization protocol that shares designated access between applications

بروتوكول تفويض مفتوح المعيار يسمح بمشاركة صلاحيات معينة بين التطبيقات

On-path attack



An attack where a malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit

هجوم يضع فيه الفاعل التهديدي نفسه في منتصف اتصال شرعي لاعتراض أو تعديل البيانات أثناء النقل

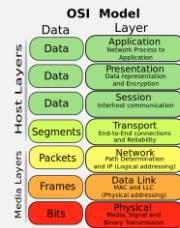
Open-source intelligence (OSINT)



The collection and analysis of information from publicly available sources to generate usable intelligence

جمع وتحليل المعلومات من مصادر متاحة علنًا لتوليد استخبارات قابلة للاستخدام

Open systems interconnection (OSI) model



A standardized concept that describes the seven layers computers use to communicate and send data over the network

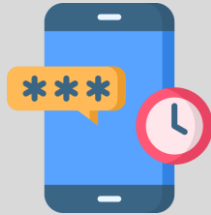
مفهوم معياري يصف الطبقات السبع التي تستخدمها أجهزة الكمبيوتر للتواصل وإرسال البيانات عبر الشبكة

Terms

definitions

التعريفات

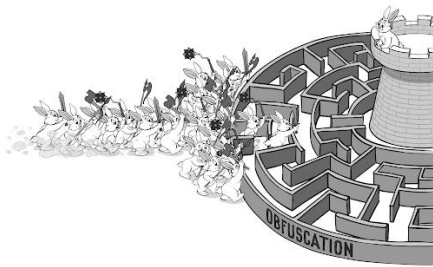
One-time Password (OTP)



A security mechanism that generates a unique password for each login attempt, typically used as part of two-factor authentication (2FA)

آلية أمان تولد كلمة مرور فريدة لكل محاولة تسجيل دخول، وتستخدم عادة كجزء من المصادقة الثنائية 2FA

Obfuscation



A technique used to deliberately make something unclear or difficult to understand, often used in software development to obscure the code and make it harder for attackers to exploit vulnerabilities

تقنية تُستخدم لجعل شيء ما غامضًا أو صعب الفهم عمدًا، وتُستخدم في تطوير البرمجيات لإخفاء الشيفرة وجعل استغلال الثغرات أصعب على المهاجمين

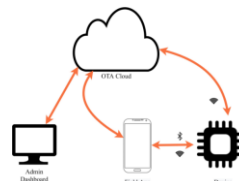
Operational Technology (OT)



Hardware and software systems used to control and monitor industrial operations, often found in critical infrastructure such as power plants and factories

الأنظمة المادية والبرمجية المستخدمة للتحكم في العمليات الصناعية ومراقبتها، وتوجد عادة في البنية التحتية الحيوية مثل محطات الطاقة والمصانع

Over-the-Air (OTA) Updates



The process of delivering software updates, patches, or configuration changes wirelessly to a device, without requiring physical access

عملية إرسال تحديثات برمجية أو تصحيحات أو تغييرات في التكوين إلى جهاز بشكل لاسلكي دون الحاجة للوصول المادي إليه

Cyber Security Glossary

Terms

definitions

التعريفات

Package



A piece of software that can be combined with other packages to form an application

قطعة من البرمجيات يمكن دمجها مع حزم أخرى لتشكيل تطبيق

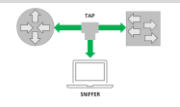
Package manager



A tool that helps users install, manage, and remove packages or applications

أداة تساعد المستخدمين على تثبيت وإدارة وإزالة الحزم أو التطبيقات

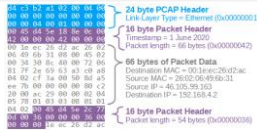
Packet sniffing



The practice of capturing and inspecting data packets across a network

ممارسة التقاط وفحص حزم البيانات التي تنتقل عبر الشبكة

Packet capture (P-cap)



A file containing data packets intercepted from an interface or network

ملف يحتوي على حزم البيانات التي تم اعتراضها من واجهة أو شبكة

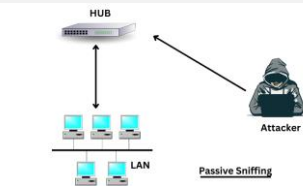
Password Spraying



A type of brute force attack where an attacker tries commonly used passwords across many different accounts, rather than focusing on a single account

نوع من هجمات القوة الغاشمة حيث يحاول المهاجم استخدام كلمات مرور شائعة على عدة حسابات مختلفة بدلاً من التركيز على حساب واحد

Passive packet sniffing



A type of attack where a malicious actor connects to a network hub and looks at all traffic on the network

نوع من الهجمات يقوم فيه الفاعل التهديدي بالاتصال بموزع الشبكة ومراقبة جميع حركة المرور دون تعديلها

Privilege Escalation



A technique where an attacker exploits a vulnerability to gain higher access rights in a system, allowing them to execute unauthorized actions

تقنية يستغل فيها المهاجم ثغرة للحصول على حقوق وصول أعلى في النظام، مما يتيح له تنفيذ إجراءات غير مصرح بها

Terms

definitions

التعريفات

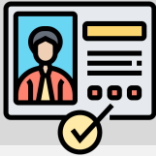
Password attack 	An attempt to access password secured devices, systems, networks, or data	محاولة للوصول إلى الأجهزة أو الأنظمة أو البيانات المحمية بكلمة مرور
Patch update 	A software and operating system update that addresses security vulnerabilities within a program or product	تحديث برمجي لنظام التشغيل أو برنامج آخر لمعالجة الثغرات الأمنية في البرنامج
Penetration test (pen test) 	A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes	هجوم محاكٍ يساعد في تحديد الثغرات في الأنظمة أو الشبكات أو المواقع أو التطبيقات
Payment Card Industry Data Security Standards (PCI DSS) 	Any cardholder data that an organization accepts, transmits, or stores	معايير تتعلق ببيانات حاملي البطاقات التي تقبلها أو تنقلها أو تخزنها أي مؤسسة
Phishing-as-a-Service (PhaaS) 	A cybercrime business model where criminals offer phishing kits and services to other attackers who want to launch phishing campaigns	نموذج تجاري للجريمة الإلكترونية حيث يوفر المجرمون أدوات وخدمات التصيد الاحتيالي للمهاجمين الآخرين الذين يرغبون في إطلاق حملات تصيد
Pseudonymization 	The process of replacing personal identifiers in data with pseudonyms to protect individual privacy while maintaining data utility	عملية استبدال المعلومات الشخصية في البيانات بأسماء مستعارة لحماية خصوصية الأفراد مع الحفاظ على فائدة البيانات
Payload 	The part of a malware program that executes the malicious activity, such as data theft or system damage	الجزء من برنامج البرمجيات الخبيثة الذي ينفذ النشاط الضار، مثل سرقة البيانات أو إتلاف النظام

Terms

definitions

التعريفات

Personally identifiable information (PII)



Any information used to infer an individual's identity

أي معلومات يمكن استخدامها لتحديد هوية فرد معين

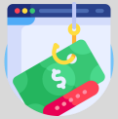
Phishing



The use of digital communications to trick people into revealing sensitive data or deploying malicious software

استخدام اتصالات رقمية لخداع الأشخاص للكشف عن بيانات حساسة أو نشر برمجيات خبيثة

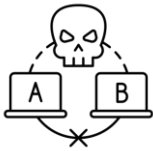
Phishing kit



A collection of software tools needed to launch a phishing campaign

مجموعة من الأدوات البرمجية اللازمة لإطلاق حملة تصيد احتيالي

Physical attack



A security incident that affects not only digital but also physical environments where the incident is deployed

حادثة أمنية تؤثر على البيئة الرقمية والمادية

Physical social engineering



An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location

هجوم يقوم فيه الفاعل التهديدي بانتحال شخصية موظف أو عميل أو مورد للوصول غير المصرح به إلى موقع مادي

Ping of death



A type of DoS attack caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64KB

نوع من هجمات حجب الخدمة (DoS) يحدث عندما يقوم المهاجم بإرسال حزمة بحجم ICMP أكبر من 64 كيلوبايت إلى نظام

Playbook



A manual that provides details about any operational action

دليل يحتوي على تفاصيل الإجراءات التشغيلية

Terms

definitions

التعريفات

Policy



A set of rules that reduce risk and protect information

مجموعة من القواعد التي تقلل من المخاطر وتحمي المعلومات

Port



A software-based location that organizes the sending and receiving of data between devices on a network

موقع قائم على البرامج ينظم إرسال واستقبال البيانات بين الأجهزة على الشبكة

Potentially unwanted application (PUA)



A type of unwanted software that is bundled in with legitimate programs which might display ads, cause device slowdown, or install other software

نوع من البرامج غير المرغوب فيها تأتي مدمجة مع برامج مشروعة، والتي قد تعرض إعلانات أو تبطئ الجهاز أو تثبت برامج أخرى

Port filtering

FILTERED PORTS			ADD	REMOVE	RESET
☐ Port No	Port Type	Filter Type			
☐ 21-22	FTP	BLOCKED			
☐ 23	Telnet	BLOCKED			
☐ 6660-6669	IRC	BLOCKED			

A firewall function that blocks or allows certain port numbers to limit unwanted communication

وظيفة جدار الحماية التي تحجب أو تسمح بأرقام منافذ معينة للحد من الاتصال غير المرغوب فيه

Private data



Information that should be kept from the public

معلومات يجب أن تبقى بعيدة عن العامة

Privacy protection



The act of safeguarding personal information from unauthorized use

عمل يهدف إلى حماية المعلومات الشخصية من الاستخدام غير المصرح به

Terms

definitions

التعريفات

Protecting and preserving evidence



The process of properly working with fragile and volatile digital evidence

عملية التعامل بشكل صحيح مع الأدلة الرقمية الهشة والمتطايرة

Process of Attack Simulation and Threat Analysis (PASTA)



A popular threat modeling framework that's used across many industries

إطار نمذجة التهديدات الشائع استخدامه عبر العديد من الصناعات

Proxy server



A server that fulfills the requests of its clients by forwarding them to other servers

خادم يقوم بتنفيذ طلبات عملائه عن طريق إرسالها إلى خوادم أخرى

Public data



Data that is already accessible to the public and poses a minimal risk to the organization if viewed or shared by others

بيانات متاحة بالفعل للجمهور ولا تشكل أي خطر على المنظمة إذا تم عرضها أو مشاركتها مع الآخرين

Public key infrastructure (PKI)



An encryption framework that secures the exchange of online information

إطار عمل تشفير يُستخدم لتأمين تبادل المعلومات عبر الإنترنت

Programming



A process that can be used to create a specific set of instructions for a computer to execute tasks

عملية إنشاء مجموعة محددة من التعليمات لاتباعها الكمبيوتر لتنفيذ المهام

Terms

definitions

التعريفات

Quantum Cryptography



A method of encryption that leverages the principles of quantum mechanics to secure data against potential eavesdropping or tampering

طريقة للتشفير تستفيد من مبادئ ميكانيكا الكم لتأمين البيانات ضد التنصت أو التلاعب المحتمل

Quarantine



A security process in which potentially harmful files, emails, or devices are isolated from the network or system until they can be analyzed or removed safely

عملية أمنية يتم فيها عزل الملفات أو رسائل البريد الإلكتروني أو الأجهزة التي قد تكون ضارة عن الشبكة أو النظام حتى يمكن تحليلها أو إزالتها بأمان

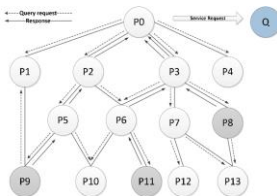
Quantum Key Distribution (QKD)



A secure communication method that uses quantum mechanics to enable two parties to produce a shared, random secret key that can be used to encrypt and decrypt messages

طريقة اتصال آمنة تستخدم ميكانيكا الكم لتمكين طرفين من إنشاء مفتاح سري مشترك عشوائي يُستخدم لتشفير وفك تشفير الرسائل

Query Flooding



A type of denial-of-service attack where an attacker overwhelms a target with a large volume of search or query requests, exhausting system resources

نوع من هجمات حجب الخدمة حيث يقوم المهاجم بإغراق الهدف بعدد كبير من طلبات البحث أو الاستعلام، مما يؤدي إلى استنزاف موارد النظام

Quantum Resistance



The property of a cryptographic algorithm that ensures it remains secure even against an adversary with access to a powerful quantum computer

خاصية في خوارزمية التشفير التي تضمن أنها تظل آمنة حتى في مواجهة خصم لديه إمكانية الوصول إلى حاسوب كمومي قوي

Terms

definitions

التعريفات

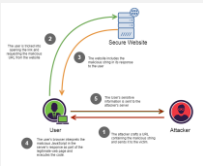
Ransomware



A malicious attack where threat actors encrypt an organization's data and demand payment to restore access

هجوم خبيث يقوم فيه الفاعلون التهديديون بتشفير بيانات المنظمة ويطلبون بدفع فدية لاستعادة الوصول إليها

Reflected XSS attack



An instance when malicious script is sent to a server and activated during the server's response

حالة يتم فيها إرسال كود خبيث إلى الخادم ويتم تنشيطه عند استجابة الخادم

Recovery



The process of returning affected systems back to normal operations

عملية إعادة الأنظمة المتأثرة إلى العمل الطبيعي

Replay attack



A network attack performed when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time

هجوم شبكي يتم فيه اعتراض حزمة بيانات أثناء النقل وإعادة إرسالها لاحقاً للحصول على الوصول غير المصرح به

Resiliency



The ability to prepare for, respond to, and recover from disruptions

القدرة على التحضير والاستجابة والتعافي من الاضطرابات

Reverse proxy server



A server that regulates and restricts the internet's access to an internal server

خادم ينظم الوصول من الإنترنت إلى خادم داخلي

Risk



Anything that can impact the confidentiality, integrity, or availability of an asset

أي شيء يمكن أن يؤثر على السرية أو السلامة أو التوفر لأي أصل

Terms

definitions

التعريفات

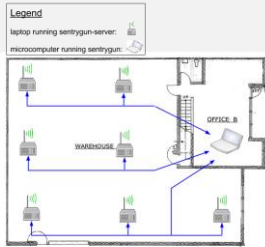
Risk-Based Authentication (RBA)



A security method that adjusts the level of authentication based on the risk factors associated with the user's login attempt, such as location, device, and behavior

طريقة أمنية تعدل مستوى المصادقة بناءً على عوامل الخطر المرتبطة بمحاولة تسجيل الدخول، مثل الموقع والجهاز والسلوك

Rogue Access Point



An unauthorized wireless access point installed on a network, often used by attackers to intercept data or gain access to the network

نقطة وصول لاسلكية غير مصرح بها مثبتة على الشبكة، غالبًا ما يستخدمها المهاجمون لاعتراض البيانات أو الوصول إلى الشبكة

Rootkit



A type of malicious software designed to enable unauthorized access to a computer while concealing its presence from detection

نوع من البرمجيات الخبيثة المصممة لتمكين الوصول غير المصرح به إلى جهاز كمبيوتر مع إخفاء وجودها عن الكشف

Red Teaming



A simulated attack exercise where security professionals act as adversaries to test the effectiveness of an organization's defenses

تمرين محاكاة للهجوم حيث يتصرف المحترفون الأمنيون كخصوم لاختبار فعالية دفاعات المنظمة

Retinal Scan



A biometric authentication method that uses patterns of the retina's blood vessels to verify a user's identity

طريقة للمصادقة البيومترية تستخدم أنماط الأوعية الدموية في شبكية العين للتحقق من هوية المستخدم

Terms

definitions

التعريفات

Risk mitigation



The process of having the right procedures and rules in place to quickly reduce the impact of a risk like a breach

عملية وضع إجراءات وقواعد لتقليل تأثير المخاطر بسرعة، مثل حدوث خرق أمني

Root directory



The highest-level directory in Linux

أعلى مستوى في هيكل الدليل في نظام لينكس

Root user (or superuser)



A user with elevated privileges to modify the system

مستخدم يتمتع بامتيازات عالية تمكنه من تعديل النظام

Router



A network device that connects multiple networks together

جهاز شبكة يربط عدة شبكات معًا ويقوم بتوجيه حركة البيانات بينها

Salting



An additional safeguard that's used to strengthen hash functions

إجراء إضافي يُستخدم لتقوية دوال التشفير

Scareware



Malware that employs tactics to frighten users into infecting their device

برمجيات خبيثة تستخدم تكتيكات التخويف لإقناع المستخدمين بتثبيتها

Terms

definitions

التعريفات

Secure File Transfer Protocol (SFTP)



A secure protocol used to transfer files from one device to another over a network

بروتوكول آمن لنقل الملفات من جهاز إلى آخر عبر الشبكة

Secure shell (SSH)



A security protocol used to create a shell with a remote system

بروتوكول أمني يُستخدم لإنشاء اتصال آمن مع جهاز عن بُعد

Security architecture



A type of security design composed of multiple components, such as tools and processes, that are used to protect an organization from risks and external threats

تصميم أمني يتكون من عدة مكونات، مثل الأدوات والعمليات، لحماية المنظمة من المخاطر

Security audit



A review of an organization's security controls, policies, and procedures against a set of expectations

مراجعة للضوابط والسياسات والإجراءات الأمنية للمؤسسة للتأكد من الامتثال للمعايير

Security controls



Safeguards designed to reduce specific security risks

إجراءات الحماية المصممة لتقليل المخاطر الأمنية المحددة

Security ethics



Guidelines for making appropriate decisions as a security professional

إرشادات لاتخاذ قرارات مناسبة كمحترف في مجال الأمن السيبراني

Terms

definitions

التعريفات

Security operations center (SOC)



An organizational unit dedicated to monitoring networks, systems, and devices for security threats or attacks

وحدة داخل المنظمة مخصصة لمراقبة الشبكات والأنظمة والأجهزة من أجل التهديدات أو الهجمات الأمنية

Security information and event management (SIEM)



An application that collects and analyzes log data to monitor critical activities in an organization

تطبيق يجمع ويحلل بيانات السجلات لمراقبة الأنشطة الحيوية في المنظمة

Security orchestration, automation, and response (SOAR)



A collection of applications, tools, and workflows that use automation to respond to security events

قدرة المنظمة على إدارة دفاعها عن الأصول والبيانات الحرجة والتفاعل مع التهديدات

Security hardening



The process of strengthening a system to reduce its vulnerabilities and attack surface

عملية تعزيز نظام لتقليل الثغرات ومساحات الهجوم

Security posture



An organization's ability to manage its defense of critical assets and data and react to change

قدرة المنظمة على إدارة دفاعها عن الأصول والبيانات الحرجة والتفاعل مع التهديدات

Security frameworks



Guidelines used for building plans to help mitigate risk and threats to data and privacy

إرشادات تُستخدم لبناء خطط للمساعدة في تقليل المخاطر والتهديدات المتعلقة بالبيانات والخصوصية

Security governance



Practices that help support, define, and direct security efforts of an organization

ممارسات تساعد في دعم وتحديد وتوجيه جهود الأمان في المؤسسة

Terms

definitions

التعريفات

Security mindset



The ability to evaluate risk and constantly seek out and identify the potential or actual breach of a system, application, or data

القدرة على تقييم المخاطر باستمرار والبحث عن ثغرات أو خروقات محتملة للنظام أو التطبيق أو البيانات

Security zone



A segment of a company's network that protects the internal network from the internet

جزء من شبكة الشركة يتم تصميمه لحماية الشبكة الداخلية من الإنترنت

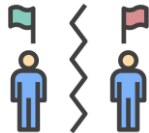
Sensitive personally identifiable information (SPII)



A specific type of PII that falls under stricter handling guidelines

نوع محدد من المعلومات الشخصية القابلة للتعريف تخضع لإرشادات أكثر صرامة

Separation of duties



The principle that users should not be given levels of authorization that would allow them to misuse a system

مبدأ يعني أن المستخدمين لا يجب أن يحصلوا على مستويات من الصلاحيات التي تسمح لهم بإساءة استخدام النظام

Session



a sequence of network HTTP requests and responses associated with the same user

تسلسل من طلبات واستجابات HTTP المرتبطة بالمستخدم نفسه

Session cookie



A token that websites use to validate a session and determine how long that session should last

رمز تستخدمه المواقع للتحقق من الجلسة وتحديد مدة صلاحيتها

Session hijacking



An event when attackers obtain a legitimate user's session ID

حالة يحصل فيها المهاجم على معرف جلسة مستخدم شرعي

Terms

definitions

التعريفات

Session ID



A unique token that identifies a user and their device while accessing a system

رمز فريد يحدد المستخدم وجهازه أثناء الوصول إلى النظام

Shared responsibility



The idea that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security

فكرة أن جميع الأفراد داخل المنظمة يلعبون دورًا في تقليل المخاطر والحفاظ على الأمان المادي والافتراضي

Shell



The command-line interpreter

مفسر الأوامر الذي يسمح للمستخدم بالتفاعل مع نظام التشغيل عبر سطر الأوامر

Signature



A pattern that is associated with malicious activity

نمط مرتبط بالنشاط الخبيث يُستخدم للكشف عن الهجمات

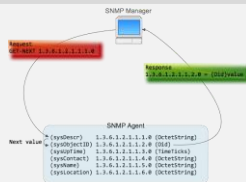
Signature analysis



A detection method used to find events of interest

طريقة كشف تُستخدم للعثور على الأحداث ذات الأهمية بناءً على أنماط معينة

Simple Network Management Protocol (SNMP)



A network protocol used for monitoring and managing devices on a network

بروتوكول شبكة يُستخدم لمراقبة وإدارة الأجهزة على الشبكة

Single sign-on (SSO)



A technology that combines several different logins into one

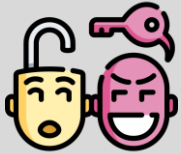
تقنية تدمج عدة تسجيلات دخول في واحد لتسهيل الوصول للمستخدم

Terms

definitions

التعريفات

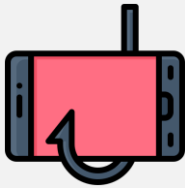
Social engineering



A manipulation technique that exploits human error to gain private information, access, or valuables

تقنية استغلال الخطأ البشري للوصول إلى المعلومات الخاصة أو الوصول غير المصرح به

Social media phishing



A type of attack where a threat actor collects detailed information about their target on social media sites before initiating the attack

نوع من الهجوم يجمع فيه الفاعل التهديدي معلومات مفصلة عن الهدف من مواقع التواصل الاجتماعي قبل بدء الهجوم

Smishing



The use of text messages to trick users to obtain sensitive information or to impersonate a known source

استخدام الرسائل النصية لخداع المستخدمين من أجل الحصول على معلومات حساسة أو لانتحال شخصية مصدر موثوق

Smurf attack



A network attack performed when an attacker sniffs an authorized user's IP address and floods it with ICMP packets

هجوم شبكي حيث يقوم المهاجم بتزوير عنوان IP لمستخدم شرعي ويغمره بحزم ICMP

Spear phishing



A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source

هجوم تصيد احتيالي يستهدف مستخدمًا أو مجموعة محددة من المستخدمين ويبدو أنه يأتي من مصدر موثوق

Spyware



Malware that's used to gather and sell information without consent

برمجيات خبيثة تُستخدم لجمع وبيع المعلومات دون موافقة المستخدم

Terms

definitions

التعريفات

Splunk Enterprise



A self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time

أداة ذات استضافة ذاتية تُستخدم للاحتفاظ ببيانات السجلات وتحليلها ومراقبتها لتقديم معلومات أمان في الوقت الفعلي

Speed



The rate at which a device sends and receives data, measured by bits per second

معدل إرسال واستقبال البيانات، يتم قياسه بالبتات في الثانية

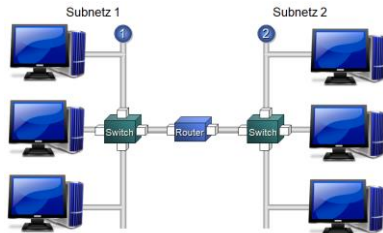
Standards



References that inform how to set policies

مراجع تُستخدم لتوجيه وضع السياسات

Subnetting



The subdivision of a network into logical groups called subnets

تقسيم الشبكة إلى مجموعات منطقية تُسمى الشبكات الفرعية

Syntax



The rules that determine what is correctly structured in a computing language

القواعد التي تحدد كيفية تكوين الأكواد في لغة البرمجة

Terms

definitions

التعريفات

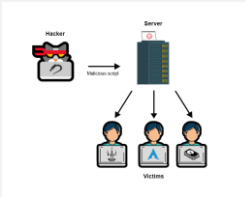
SQL injection



An attack that executes unexpected queries on a database

هجوم يتم فيه تنفيذ استعلامات غير متوقعة على قاعدة بيانات

Stored XSS attack



An instance when malicious script is injected directly on the server

حالة يتم فيها حقن كود خبيث مباشرة في الخادم

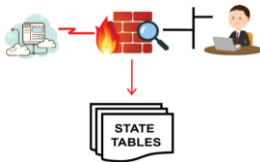
Stakeholder



An individual or group that has an interest in any decision or activity of an organization

فرد أو مجموعة لها مصلحة في أي قرار أو نشاط تقوم به المنظمة

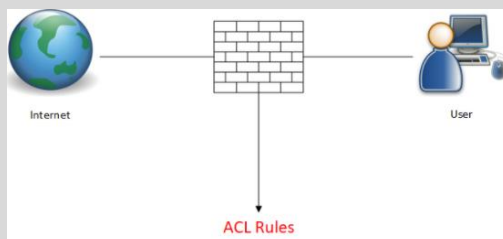
Stateful



A class of firewall that keeps track of information passing through it and proactively filters out threats

نوع من جدران الحماية الذي يتتبع المعلومات المارة من خلاله ويقوم بتصفية التهديدات بشكل استباقي

Stateless



A class of firewall that operates based on predefined rules and that does not keep track of information from data packets

نوع من جدران الحماية الذي يعمل بناءً على قواعد محددة مسبقاً ولا يحتفظ بمعلومات حول الحزم السابقة

Terms

definitions

التعريفات

Supply-chain attack



An attack that targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed

هجوم يستهدف الأنظمة أو التطبيقات أو الأجهزة أو البرامج بهدف إيجاد ثغرة يمكن من خلالها نشر البرمجيات الخبيثة

Suricata



An open-source intrusion detection system, intrusion prevention system, and network analysis tool

أداة مفتوحة المصدر تُستخدم للكشف عن التطفل، منع التطفل، وتحليل الشبكة

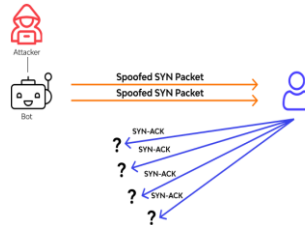
Switch



A device that makes connections between specific devices on a network by sending and receiving data between them

جهاز يقوم بربط الأجهزة المحددة على الشبكة عن طريق إرسال واستقبال البيانات بينها

Synchronize flood attack (SYN)



A type of DoS attack that simulates a TCP/IP connection and floods a server with SYN packets

نوع من هجمات حجب الخدمة يتم فيه محاكاة اتصال TCP /IP وإغراق الخادم بحزم SYN

Symmetric encryption



The use of a single secret key to exchange information

استخدام مفتاح سري واحد لتبادل المعلومات

Terms

definitions

التعريفات

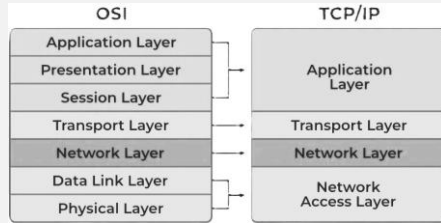
Tailgating



A social engineering tactic in which unauthorized people follow an authorized person into a restricted area

تكتيك هندسة اجتماعية يقوم فيه الأشخاص غير المصرح لهم باتباع أشخاص مصرح لهم للدخول إلى منطقة محظورة

TCP/IP model



A framework used to visualize how data is organized and transmitted across a network

إطار عمل يُستخدم لتصوير كيفية تنظيم ونقل البيانات عبر الشبكات

tcpdump



A command-line network protocol analyzer

محلل بروتوكولات شبكة يعتمد على سطر الأوامر

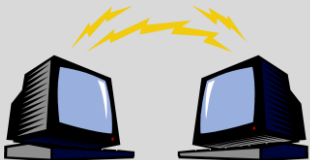
Triage



The prioritizing of incidents according to their level of importance or urgency

عملية تحديد أولوية الحوادث حسب أهميتها أو مدى خطورتها

Transmission Control Protocol (TCP)



An internet communication protocol that allows two devices to form a connection and stream data

بروتوكول اتصال عبر الإنترنت يتيح لجهازين تكوين اتصال وتبادل البيانات

Terms

definitions

التعريفات

Threat



Any circumstance or event that can negatively impact assets

أي ظرف أو حدث قد يؤثر سلبًا على الأصول

Threat actor



Any person or group who presents a security risk

أي شخص أو مجموعة تشكل تهديدًا أمنيًا

Telemetry



The collection and transmission of data for analysis

عملية جمع ونقل البيانات لتحليلها

Threat Intelligence



Information about current or potential attacks that helps organizations understand the risks they face and how to defend against them

معلومات حول الهجمات الحالية أو المحتملة تساعد المؤسسات في فهم المخاطر التي تواجهها وكيفية الدفاع ضدها

Threat modeling



The process of identifying assets, their vulnerabilities, and how each is exposed to threats

عملية تحديد الأصول ونقاط الضعف وكيفية تعرض كل منها للتهديدات

Trojan horse



Malware that looks like a legitimate file or program

برنامج ضار يتنكر كملف أو برنامج مشروع

Terms

definitions

التعريفات

Threat Hunting



The proactive process of searching through networks or systems to detect and isolate advanced threats that evade existing security measures

عملية استباقية للبحث في الشبكات أو الأنظمة لاكتشاف وعزل التهديدات المتقدمة التي تتجاوز التدابير الأمنية القائمة

Tokenization



A data security method that replaces sensitive data, such as credit card numbers, with non-sensitive equivalents (tokens) that have no exploitable value

طريقة أمنية لاستبدال البيانات الحساسة، مثل أرقام البطاقات الائتمانية، بمعادلات غير حساسة (رموز) ليس لها قيمة قابلة للاستغلال

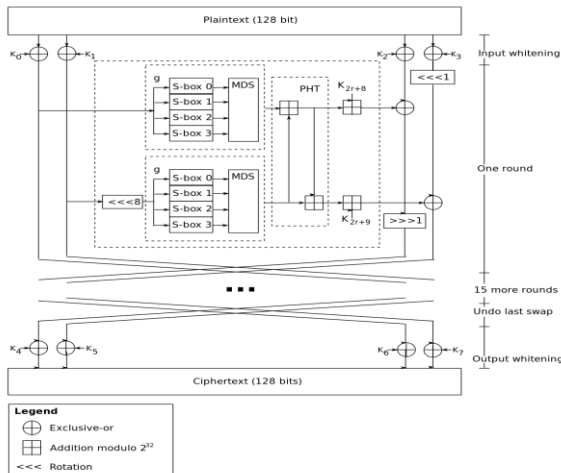
Tunneling



A networking technique used to encapsulate one network protocol within another, allowing secure transmission of data over an unsecured network

تقنية تستخدم لتغليف بروتوكول شبكة داخل بروتوكول آخر، مما يسمح بنقل البيانات بشكل آمن عبر شبكة غير آمنة

Twofish



A symmetric key block cipher used in cryptography, known for its high speed and security, commonly used for file and disk encryption

شيفرة كتلة مفاتيحية متماثلة تُستخدم في التشفير، معروفة بسرعتها العالية وأمانها، وتُستخدم بشكل شائع لتشفير الملفات والأقراص

Terms

definitions

التعريفات

Unauthorized access



An incident type that occurs when an individual gains digital or physical access to a system or application without permission

نوع من الحوادث يحدث عندما يحصل فرد على وصول رقمي أو مادي إلى نظام أو تطبيق دون إذن

Uncontrolled zone



Any network outside your organization's control

أي شبكة تقع خارج نطاق تحكم المنظمة

USB baiting



An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network

هجوم يقوم فيه ممثل التهديد بترك وحده تخزين خبيثة ليقوم الموظف بتوصيلها واصابه الشبكة

User provisioning



The process of creating and maintaining a user's digital identity

عملية إنشاء الهوية الرقمية للمستخدم والحفاظ عليها

User Datagram Protocol (UDP)



A connectionless protocol that does not establish a connection between devices before transmissions

بروتوكول اتصال لا يتطلب إنشاء اتصال بين الأجهزة قبل تبادل البيانات

Terms

definitions

التعريفات

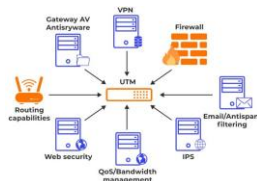
URL Filtering



A technique used to block access to certain websites based on the URLs, often used to prevent access to malicious or inappropriate content

تقنية تُستخدم لحظر الوصول إلى مواقع معينة بناءً على ، وغالبًا ما تُستخدم لمنع الوصول إلى محتوى URL روابط ضار أو غير ملائم

Unified Threat Management (UTM)



An all-in-one security solution that integrates multiple security services, such as firewall, antivirus, and intrusion detection, into a single platform

حل أمني شامل يجمع بين خدمات أمنية متعددة، مثل الجدار الناري ومكافحة الفيروسات وكشف التطفل، في منصة واحدة

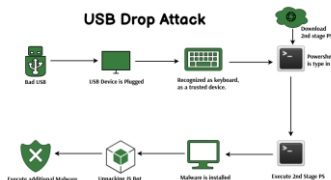
User Behavior Analytics (UBA)



A security process that monitors and analyzes user behavior to detect abnormal activities that may indicate a security threat

عملية أمنية تراقب وتحلل سلوك المستخدم لاكتشاف الأنشطة غير المعتادة التي قد تشير إلى وجود تهديد أمني

USB Drop Attack



A type of social engineering attack where an infected USB drive is left in a public space, hoping that someone will pick it up and plug it into a computer, thus spreading malware

نوع من هجمات الهندسة الاجتماعية حيث يتم ترك وحدة مصابة في مكان عام على أمل أن يقوم USB تخزين شخص ما بالتقاطها وتوصيلها بجهاز كمبيوتر، مما يؤدي إلى انتشار البرمجيات الخبيثة

Unstructured Data



Information that does not have a predefined data model or structure, making it difficult to store, manage, and analyze, such as emails or multimedia files

معلومات لا تحتوي على نموذج بيانات محدد أو هيكل، مما يجعل من الصعب تخزينها أو إدارتها أو تحليلها، مثل رسائل البريد الإلكتروني أو ملفات الوسائط المتعددة

Terms

definitions

التعريفات

Virtual Private Network (VPN)



A network security service that changes your public IP address and hides your virtual location so that you can keep your data private when you are using a public network like the internet

خدمة أمان الشبكات التي تغير عنوان الـ IP العام وتخفي الموقع الافتراضي للحفاظ على خصوصية البيانات عند استخدام شبكة عامة مثل الإنترنت

Virus



Malicious code written to interfere with computer operations and cause damage to data and software

كود ضار مكتوب للتدخل في عمليات الكمبيوتر والتسبب في ضرر للبيانات والبرمجيات

Vulnerability



A weakness that can be exploited by a threat

نقطة ضعف يمكن أن يستغلها الفاعل التهديدي

Vulnerability assessment



The internal review process of an organization's security systems

عملية مراجعة داخلية لنظم أمان المنظمة

Vulnerability management



The process of finding and patching vulnerabilities

عملية اكتشاف الثغرات الأمنية وإصلاحها

Vishing



The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source

استغلال الاتصال الصوتي الإلكتروني للحصول على معلومات حساسة أو لانتحال شخصية مصدر موثوق

Terms

definitions

التعريفات

Virtual Private Cloud (VPC)



A private cloud environment that exists within a shared public cloud, allowing organizations to control and isolate their resources

بيئة سحابية خاصة توجد داخل سحابة عامة مشتركة، تتيح للمؤسسات التحكم في مواردها وعزلها

Virtual Patch



A security solution that provides protection from vulnerabilities without applying the actual software patch, often used when immediate patching is not possible

حل أمني يوفر الحماية من الثغرات دون تطبيق الترقية البرمجي الفعلي، وغالبًا ما يُستخدم عندما يكون من غير الممكن تطبيق التحديث الفوري

Vulnerability scanner



Software that automatically compares existing common vulnerabilities and exposures against the technologies on the network

برنامج يقارن بين الثغرات الأمنية المعروفة والأجهزة الموجودة على الشبكة

Virtual Machine Escape



A vulnerability in a virtualized environment where an attacker can break out of a virtual machine and gain access to the host system or other virtual machines

ثغرة في بيئة افتراضية تتيح للمهاجم الخروج من الآلة الافتراضية والوصول إلى النظام المضيف أو الآلات الافتراضية الأخرى

VirusTotal  VirusTotal

A service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content

خدمة تتيح لأي شخص تحليل الملفات المشبوهة أو النطاقات للتحقق من وجود محتوى IP أو عناوين URL أو عناوين خبيث

Terms

definitions

التعريفات

Wireshark



An open-source network protocol analyzer

أداة مفتوحة المصدر لتحليل بروتوكولات الشبكة

Web Application Firewall (WAF)



A security solution that monitors, filters, and blocks malicious HTTP traffic to and from a web application

حل أمني يقوم بمراقبة وتصفية وحجب حركة HTTP الضارة إلى ومن تطبيق ويب

Watering Hole Attack



A cyberattack where attackers compromise websites frequently visited by their target in order to infect them with malware

هجوم إلكتروني يقوم فيه المهاجمون باختراق مواقع الويب التي يزورها الهدف بشكل متكرر من أجل إصابتهم بالبرمجيات الخبيثة

Whaling



A category of spear phishing attempts that are aimed at high-ranking executives in an organization

نوع من التصيد الاحتيالي يستهدف كبار المسؤولين في المؤسسة

Web-based exploits



Malicious code or behavior that's used to take advantage of coding flaws in a web application

سلوكيات خبيثة تستغل عيوب الترميز في تطبيقات الويب

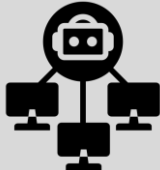
Worm



Malware that can duplicate and spread itself across systems on its own

برمجية خبيثة قادرة على تكرار نفسها والانتشار عبر الأنظمة دون تدخل المستخدم

Cyber Security Glossary

Terms	definitions	التعريفات
XSS (Cross-Site Scripting) 	A type of security vulnerability that allows attackers to inject malicious scripts into webpages viewed by other users, potentially stealing data or hijacking sessions	نوع من الثغرات الأمنية التي تسمح للمهاجمين بحقن نصوص ضارة في صفحات الويب التي يراها المستخدمون الآخرون، مما قد يؤدي إلى سرقة البيانات أو اختطاف الجلسات
Yield Curve Attack 	A type of cyberattack that targets financial institutions by manipulating the yield curve to affect interest rates or bond prices	نوع من الهجمات الإلكترونية التي تستهدف المؤسسات المالية من خلال التلاعب بمنحنى العائد للتأثير على أسعار الفائدة أو أسعار السندات
YARA (Yet Another Recursive Acronym) 	A tool used for identifying and classifying malware samples by writing specific rules that match patterns in files or memory	أداة تُستخدم لتحديد وتصنيف عينات البرمجيات الخبيثة عن طريق كتابة قواعد محددة تتطابق مع أنماط في الملفات أو الذاكرة
Zero-Day Exploit 	A technique used by attackers to exploit a zero-day vulnerability before it is discovered and patched by the vendor	تقنية يستخدمها المهاجمون لاستغلال ثغرة يوم الصفر قبل اكتشافها وتصحيحها من قبل البائع
Zombie Computer 	A computer that has been compromised by a hacker and is used to perform malicious tasks without the owner's knowledge, typically part of a botnet	حاسوب تم اختراقه من قبل مخترق ويُستخدم لتنفيذ مهام ضارة دون علم مالكه، وعادة ما يكون جزءًا من شبكة الروبوتات
Zero-Day Vulnerability 	A software vulnerability that is unknown to the vendor and has no available patch, making it highly exploitable by attackers	ثغرة أمنية في البرمجيات غير معروفة للبائع ولا يوجد لها تصحيح متاح، مما يجعلها عرضة للاستغلال من قبل المهاجمين

Glossary and Practical Examples

67

Asymmetric encryption

تقنية تعتمد على مفتاحين: عام للتشفير وخاص لفك التشفير، تُستخدم لتأمين الاتصالات والمعاملات الرقمية



68

DDoS Attack

هجوم يمنع المستخدمين الشرعيين من الوصول إلى موقع أو خدمة عبر إغراق النظام بالطلبات



69

Firewall

جدار حماية يعمل على منع الوصول غير المصرح به إلى الشبكات وحماية الأنظمة من الهجمات



70

Malware

برمجيات ضارة تُصمم لإلحاق الضرر بالأجهزة أو سرقة البيانات أو تعطيل الأنظمة



71

Phishing Attack

نوع من الهجمات السيبرانية التي تهدف إلى خداع المستخدمين للحصول على بياناتهم الشخصية أو المالية



72

Ransomware

برمجيات خبيثة تقوم بتشفير ملفات المستخدم وتطالب بفدية مالية لإعادة فك التشفير واستعادة الملفات



73

Social Engineering

التلاعب النفسي بالمستخدمين من أجل خداعهم لكشف معلومات حساسة أو تنفيذ إجراءات ضارة



74

Two-factor Authentication (2FA)

إجراء أمني بضيف طبقة إضافية للتحقق من هوية المستخدم من خلال الجمع بين كلمة المرور وطريقة تحقق إضافية



Glossary and Practical Examples

75

Digital Signatures

تقنية تُستخدم للتحقق من صحة وسلامة المستندات الرقمية، وضمان أنها لم تتعرض للتعديل



76

End-to-End Encryption

نوع من التشفير حيث يتم تشفير البيانات من المرسل إلى المستقبل فقط، مما يضمن سرية كاملة للمعلومات



77

Cloud Security

مجموعة من التدابير الأمنية المصممة لحماية البيانات والبنية التحتية المخزنة في الخدمات السحابية



78

Security Patches

ترقيات برمجية تعمل على تصحيح الثغرات الأمنية الموجودة في الأنظمة والبرامج



79

Virtual Private Network

أداة تُستخدم لإنشاء اتصال مشفر بين جهاز المستخدم وخادم عبر الإنترنت، مما يضمن الخصوصية وحماية البيانات



80

IDS/IPS

أنظمة تراقب حركة المرور للكشف عن التهديدات لحماية الشبكة من الاختراقات



81

Encryption Key Management

العملية التي تتعلق بإنشاء، تخزين، وحماية مفاتيح التشفير لضمان أمان البيانات المشفرة



82

Zero-Day Exploit

استغلال ثغرة أمنية غير معروفة للمطورين أو الشركات لحين اكتشافها وإصلاحها، مما يترك الأنظمة عرضة للهجوم



Asymmetric encryption

المزايا والتحديات

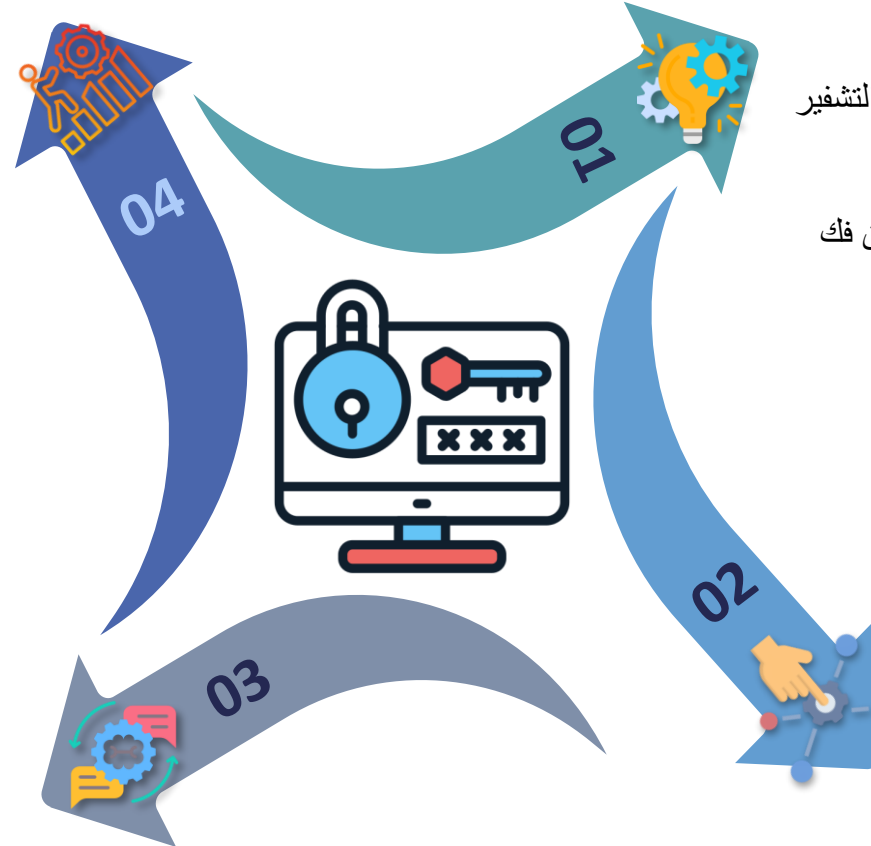
- **المزايا:**
- يوفر أمانًا عاليًا، حيث يمكن فك تشفير البيانات فقط باستخدام المفتاح الخاص
- **التحديات:**
- يتطلب موارد حاسوبية كبيرة وقد يكون إدارة المفاتيح معقدًا

مفهوم التشفير غير المتماثل

- التشفير غير المتماثل يعتمد على مفتاحين: عام للتشفير وخاص لفك التشفير
- **المفتاح العام** يُستخدم لتشفير الرسالة، و**المفتاح الخاص** لفك التشفير
- هذه العملية تضمن أن حتى لو تم اعتراض الرسالة، لن يتمكن أحد من فك تشفيرها سوى الشخص الذي يمتلك المفتاح الخاص

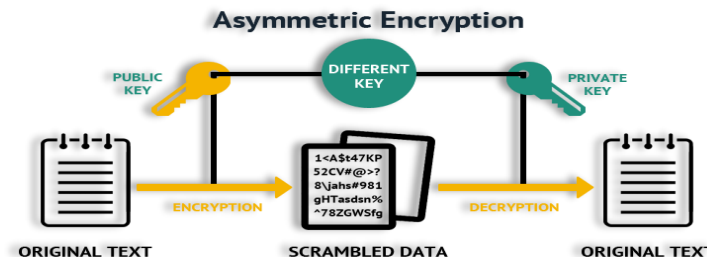
آلية العمل

- يقوم المرسل بتشفير الرسالة باستخدام **المفتاح العام** للمستلم
- المستلم يستخدم **المفتاح الخاص** لفك التشفير وقراءة الرسالة
- يضمن التشفير غير المتماثل أمان البيانات ويمنع أي جهة أخرى من الوصول إلى محتواها



الاستخدامات العملية

- تأمين المعاملات البنكية عبر الإنترنت
- البروتوكولات الأمنية: يعتمد العديد من بروتوكولات الأمان على التشفير غير المتماثل لتأمين الاتصال بين المتصفحات والخوادم
- التوقيعات الرقمية لتأكيد هوية المرسل



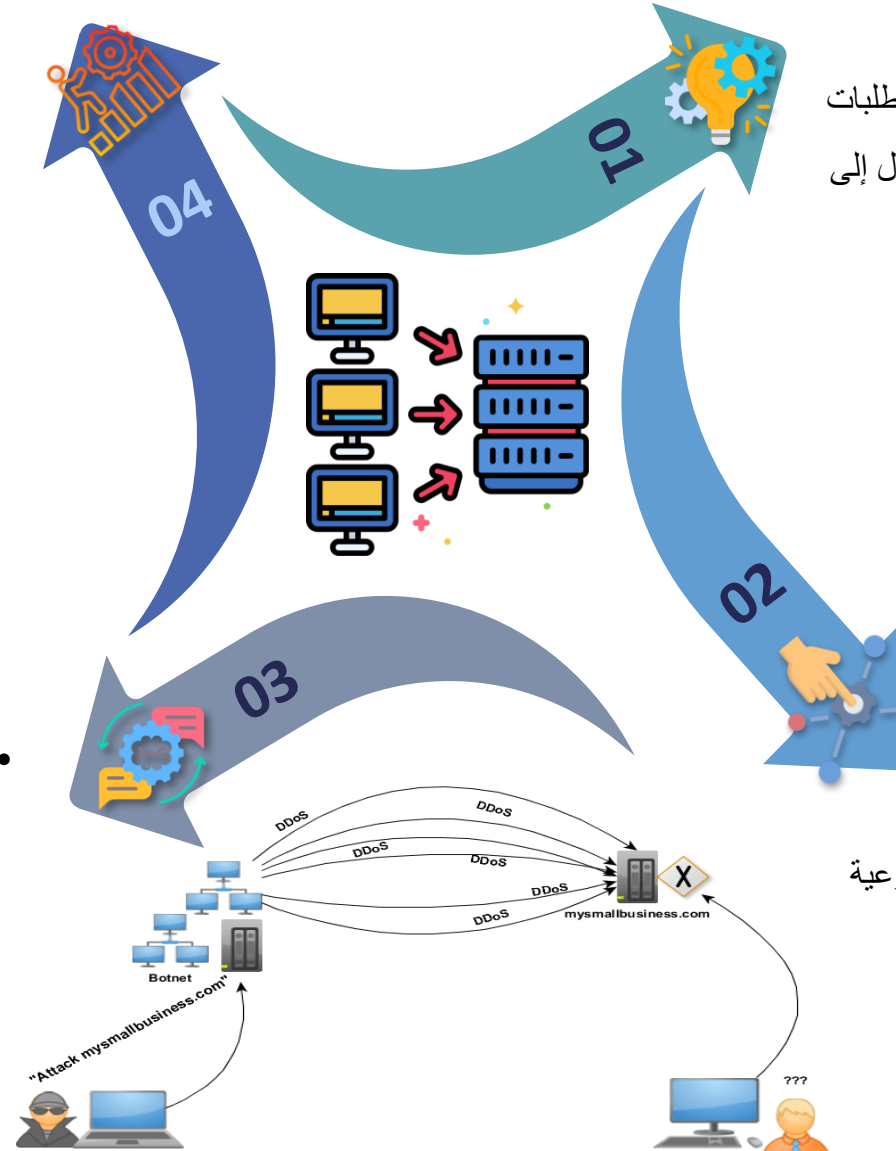
DDoS Attack

مفهوم هجوم DDoS

- هو هجوم سيبراني يتم فيه إغراق الخادم أو الشبكة بعدد ضخم من الطلبات غير الشرعية، مما يؤدي إلى منع المستخدمين الشرعيين من الوصول إلى الخدمات

آلية العمل

- إرسال طلبات ضخمة من عدة أجهزة مخترقة (بوت نت)، مما يؤدي إلى استنزاف موارد الخادم
- تعطيل الخدمة: يصبح الخادم غير قادر على الاستجابة للطلبات الشرعية بسبب الضغط الناتج عن الهجوم



المزايا والتحديات

- **المزايا للمهاجم:** القدرة على إيقاف الخدمة وإلحاق ضرر كبير بسرعة
- **التحديات للمستهدف:** يتطلب الدفاع ضد هذه الهجمات استخدام أنظمة متقدمة لتصفية حركة المرور الضارة

الاستخدامات العملية

- تعطيل الخدمات الإلكترونية مثل المواقع أو التطبيقات المالية لإحداث ضرر اقتصادي أو تشويش على سمعة الشركات

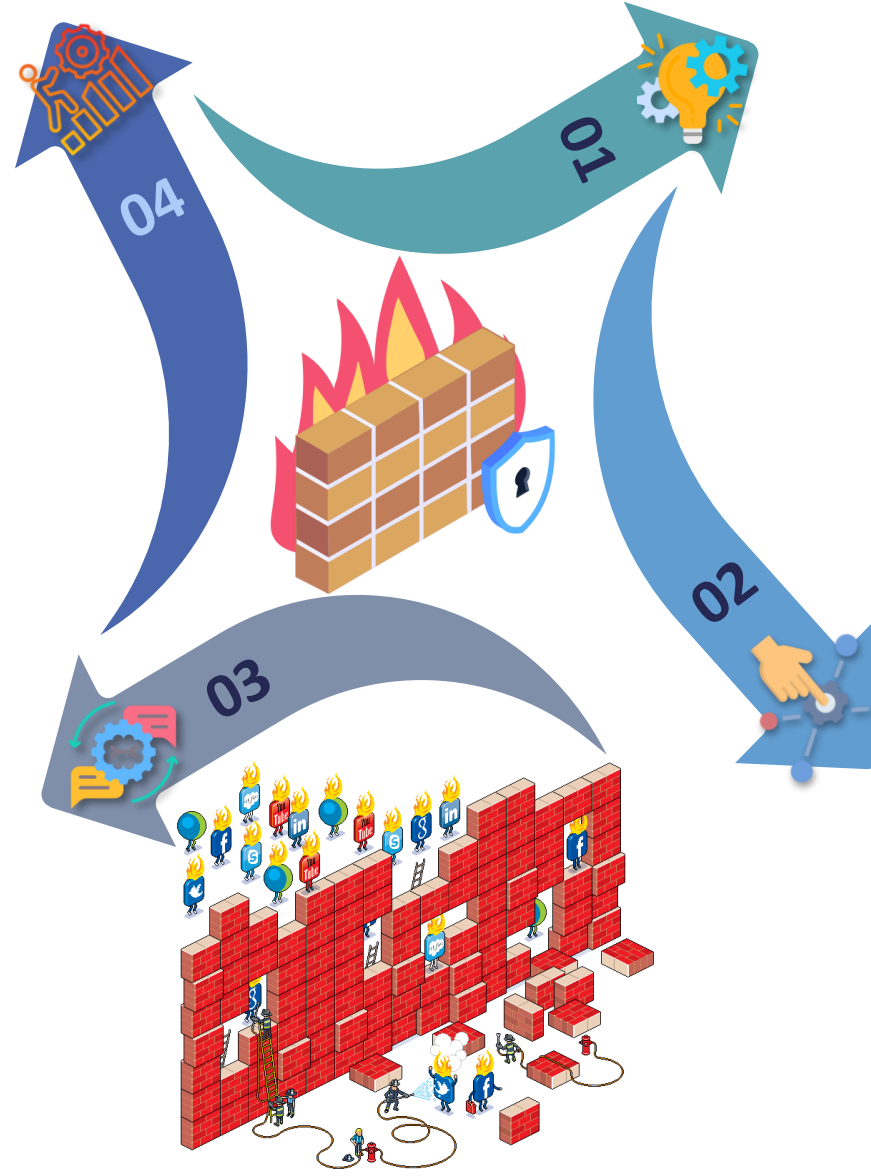
Firewall

المزايا والتحديات

- **المزايا:** يمنع الوصول غير المصرح به ويحافظ على أمان الشبكة
- **التحديات:** قد يكون من الصعب تحديث القواعد باستمرار لمواجهة التهديدات الجديدة

الاستخدامات العملية

- حماية الشبكات الداخلية للشركات من الهجمات الإلكترونية
- تصفية حركة المرور المشبوهة ومنعها من الوصول إلى الأنظمة الحساسة



مفهوم جدار الحماية

- جدار الحماية هو نظام أمني يقوم بمنع الوصول غير المصرح به إلى الشبكات عن طريق مراقبة وتصفية حركة المرور بين الشبكات الداخلية والخارجية

آلية العمل

- يقوم جدار الحماية بتحديد القواعد التي تسمح أو تمنع حركة المرور بناءً على مجموعة من السياسات الأمنية المحددة مسبقًا
- يُستخدم في الشركات والأجهزة الشخصية لحماية البيانات والأنظمة من التهديدات الخارجية

المزايا والتحديات

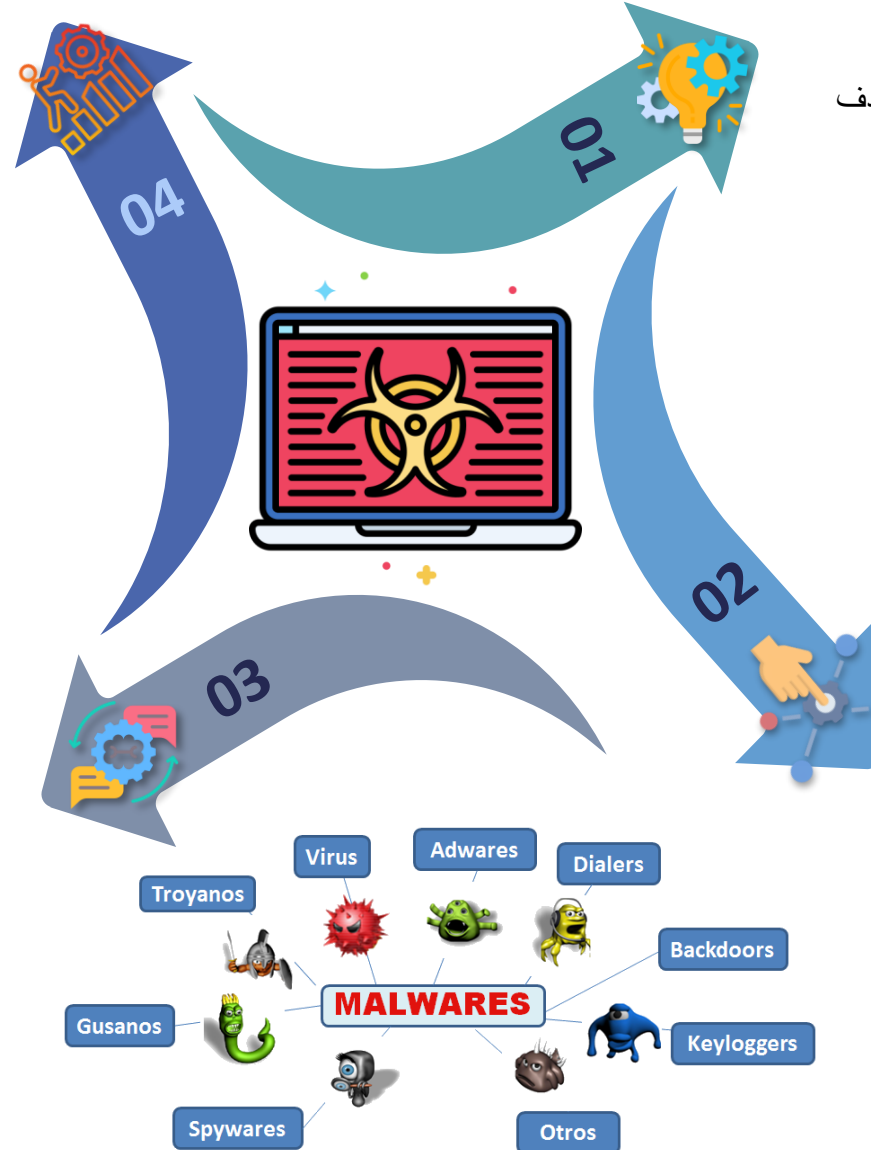
- **المزايا للمهاجم:** يمكن استغلال الثغرات الأمنية للسيطرة على الأنظمة أو سرقة المعلومات
- **التحديات للمستهدف:** حماية الأنظمة تتطلب برامج مضادة للفيروسات وجدران نارية قوية

مفهوم البرمجيات الخبيثة

- البرمجيات الخبيثة هي برامج ضارة مصممة للتسلل إلى الأنظمة بهدف تعطيلها، سرقة البيانات، أو إلحاق الضرر بالجهاز أو الشبكة

آلية العمل

- تدخل البرمجيات الخبيثة النظام من خلال ملفات أو روابط ملوثة، وتقوم بتنفيذ عمليات غير مشروعة مثل سرقة البيانات أو تدمير الملفات



الاستخدامات العملية

- البرمجيات الخبيثة تُستخدم بشكل واسع في الهجمات الإلكترونية بهدف الحصول على بيانات حساسة أو السيطرة على الأنظمة

Phishing Attack

المزايا والتحديات

- **المزايا للمهاجم:** سهل التنفيذ ويمكن استهداف عدد كبير من الأشخاص
- **التحديات للمستهدف:** صعوبة اكتشاف الهجمات نظرًا لتصميم المواقع المزيفة بطرق تشبه المواقع الأصلية

الاستخدامات العملية

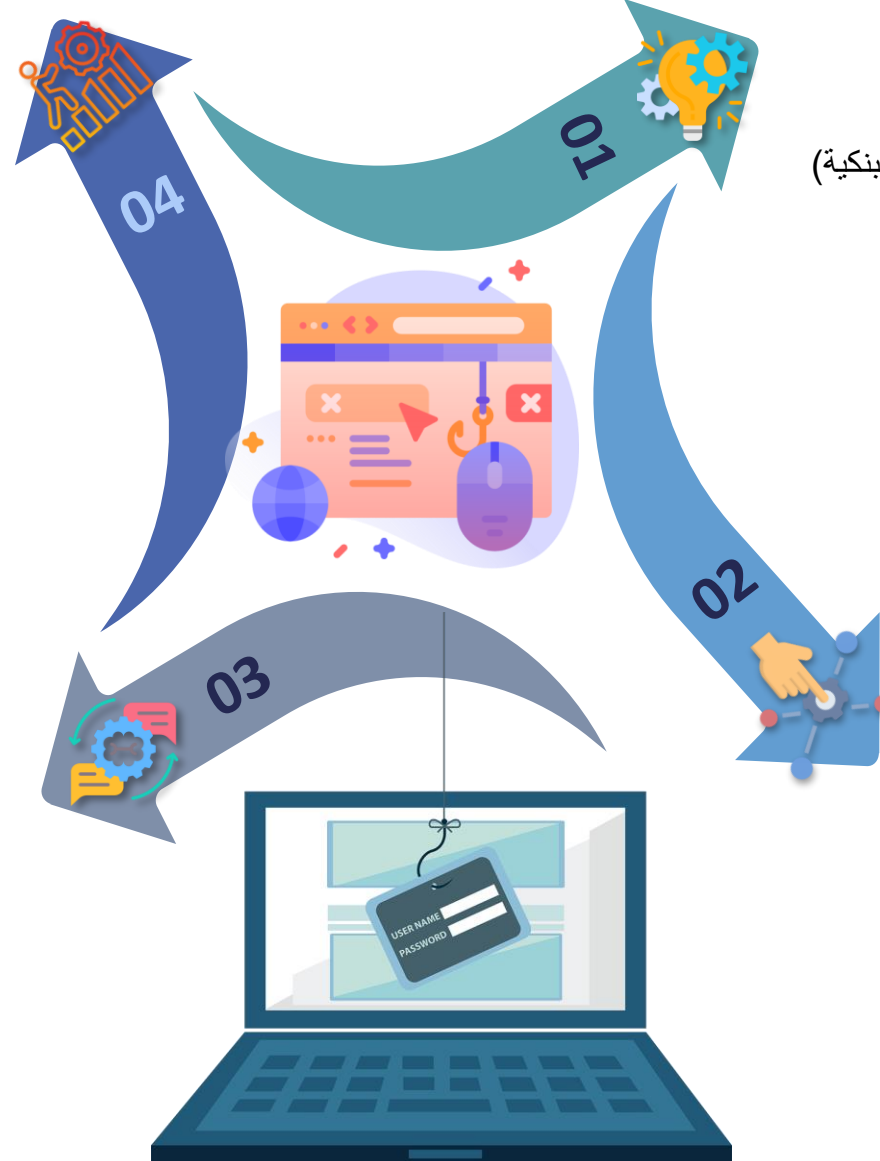
- يتم استخدام هجمات التصيد بشكل واسع لسرقة بيانات تسجيل الدخول، تفاصيل الحسابات البنكية، أو البيانات الشخصية الأخرى

مفهوم هجوم التصيد الاحتيالي

- هجوم تصيد احتيالي هو محاولة خداع المستخدمين للحصول على معلوماتهم الحساسة (مثل كلمات المرور أو بيانات البطاقات البنكية) من خلال رسائل أو مواقع تبدو وكأنها من جهات موثوقة

آلية العمل

- يتم إرسال رسائل بريد إلكتروني أو روابط تبدو شرعية، ولكنها تقود المستخدم إلى موقع مزيف يهدف إلى سرقة المعلومات الشخصية

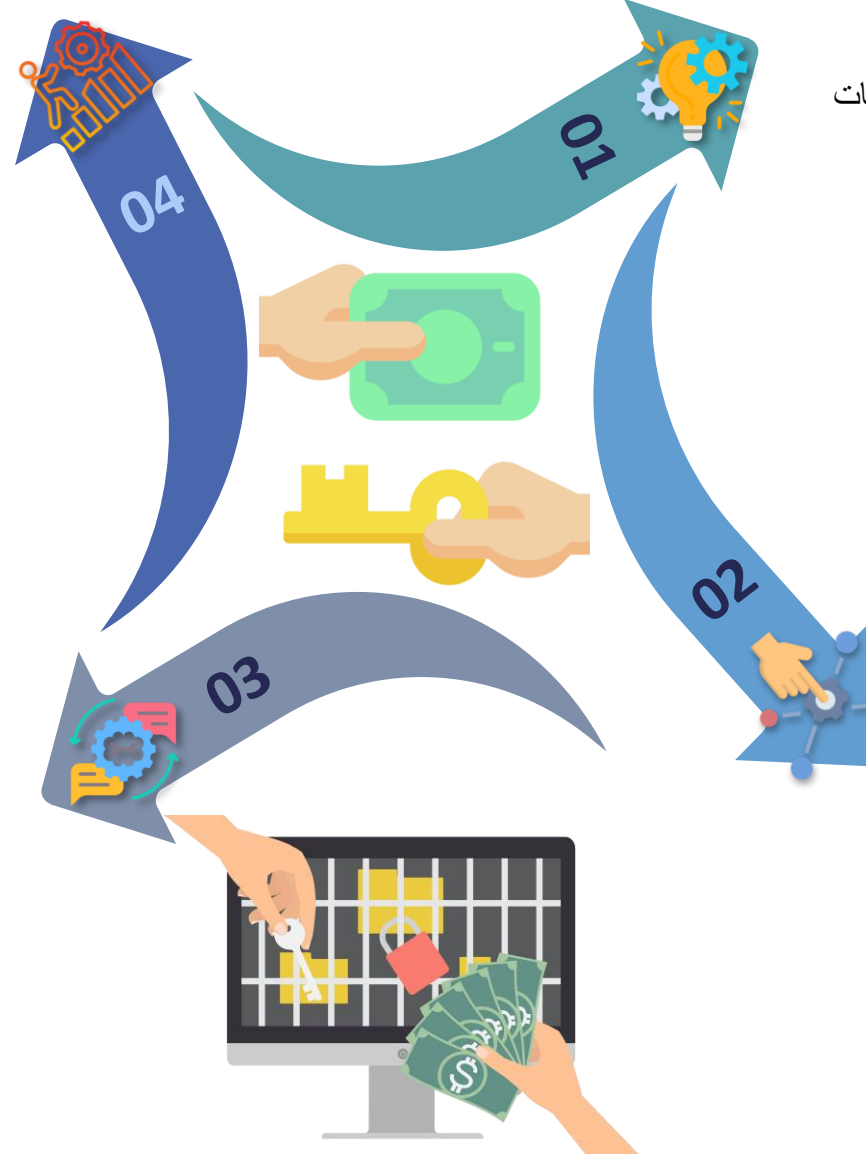


مفهوم برمجيات الفدية

- برمجيات الفدية هي نوع من البرمجيات الخبيثة التي تقوم بتشفير ملفات المستخدم وتطلب دفع فدية مالية مقابل فك التشفير واستعادة الملفات

آلية العمل

- تقوم البرمجية بتشفير الملفات المهمة على جهاز المستخدم، وتُظهر رسالة تطالب بالدفع مقابل الحصول على مفتاح فك التشفير



المزايا والتحديات

- **المزايا للمهاجم:** إمكانية تحقيق مكاسب مالية كبيرة في وقت قصير
- **التحديات للمستهدف:** حتى بعد دفع الفدية، قد لا يستعيد المستخدم ملفاته أو قد يتم استهدافه مجددًا

الاستخدامات العملية

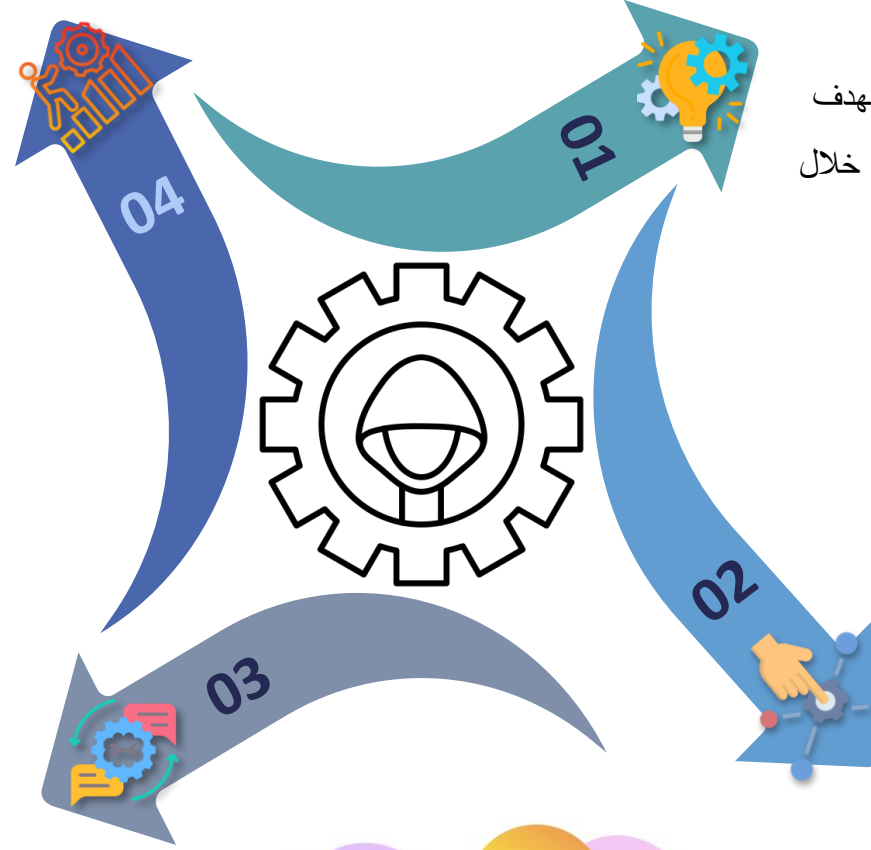
- تُستخدم هذه الهجمات لاستهداف الأفراد أو الشركات لابتزازهم ماليًا مقابل استعادة الوصول إلى بياناتهم

مفهوم الهندسة الاجتماعية

- الهندسة الاجتماعية هي أسلوب يستخدمه المهاجم لخداع الأشخاص بهدف الكشف عن معلومات حساسة أو تنفيذ إجراءات غير مصرح بها من خلال التلاعب النفسي

آلية العمل

- يعتمد المهاجم على استغلال الثقة أو الجهل لدى الأفراد للحصول على معلومات مثل كلمات المرور أو الوصول إلى أنظمة محمية



المزايا والتحديات

- **المزايا للمهاجم:** يعتمد على الضعف البشري بدلاً من نقاط الضعف التقنية، مما يزيد من فرص النجاح
- **التحديات للمستهدف:** يصعب اكتشاف الهجمات لأن الأفراد لا يدركون أنهم مستهدفون حتى بعد وقوع الضرر

الاستخدامات العملية

- تُستخدم الهندسة الاجتماعية بشكل واسع في عمليات التصيد الصوتي أو المكالمات الهاتفية التي تحاول خداع الموظفين للكشف عن بيانات سرية أو فتح ثغرات في النظام

Two-factor Authentication (2FA)

المزايا والتحديات

- **المزايا:** يعزز الأمان بشكل كبير لأنه يتطلب خطوة إضافية بعد كلمة المرور
- **التحديات:** قد يكون مزعجًا للمستخدمين في بعض الأحيان بسبب الحاجة إلى إدخال رمز التحقق في كل مرة

الاستخدامات العملية

- تُستخدم المصادقة الثنائية بشكل شائع في الحسابات البنكية، البريد الإلكتروني، ومنصات التواصل الاجتماعي لتأمين الحسابات الشخصية

مفهوم المصادقة الثنائية

- المصادقة الثنائية هي إجراء أمني يُستخدم لتأكيد هوية المستخدم عن طريق الجمع بين كلمة المرور ووسيلة تحقق إضافية (مثل رمز يُرسل إلى الهاتف المحمول)

آلية العمل

- بعد إدخال كلمة المرور، يطلب النظام من المستخدم إدخال رمز تحقق إضافي يُرسل إلى هاتفه أو يتم توليده عبر تطبيق مخصص لضمان أن الشخص الذي يحاول الوصول هو المالك الشرعي للحساب



Digital Signatures

المزايا والتحديات

- **المزايا:** يضمن التحقق من هوية المرسل وسلامة المستندات
- **التحديات:** يعتمد على الثقة المتبادلة وإدارة المفاتيح الرقمية بشكل آمن

الاستخدامات العملية

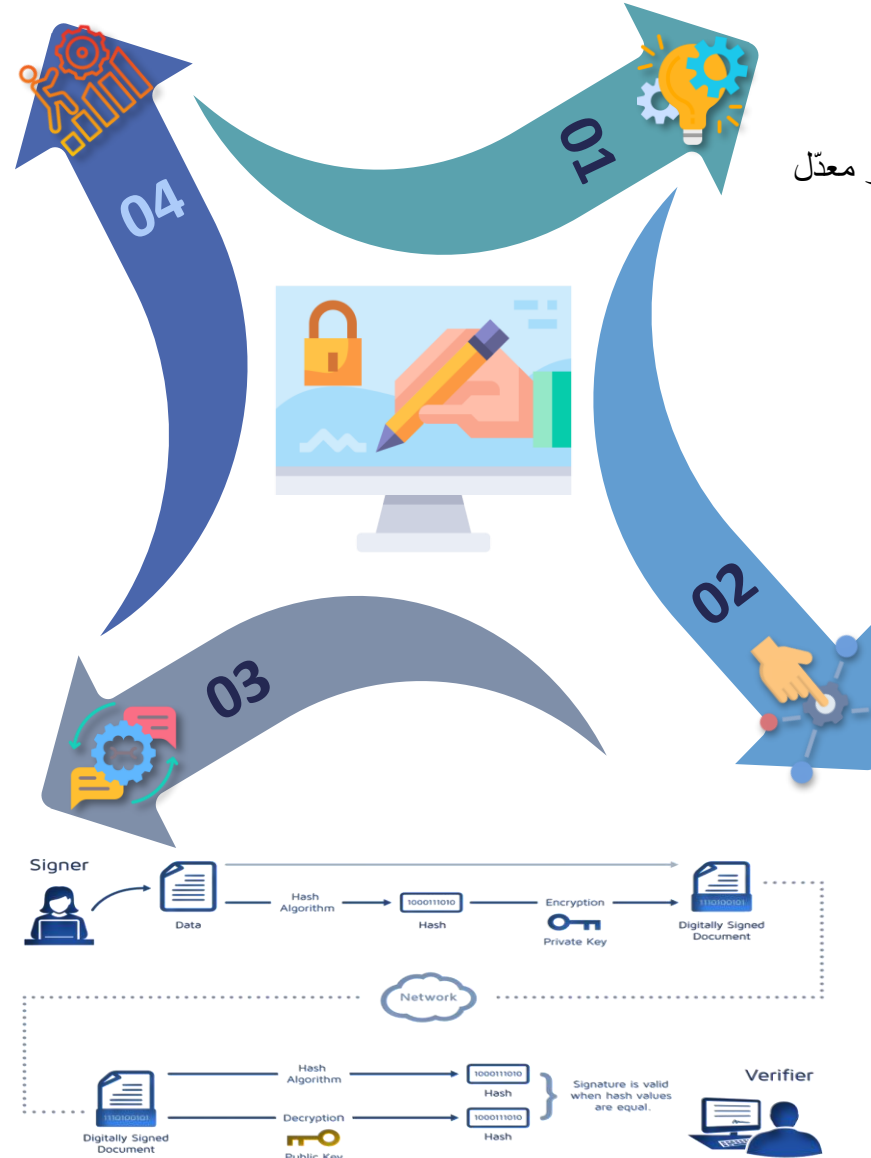
- يُستخدم التوقيع الرقمي على نطاق واسع في المعاملات المالية والعقود القانونية الرقمية لضمان صحة المستندات وعدم العبث بها

مفهوم التوقيعات الرقمية

- التوقيع الرقمي هو تقنية تشفير تستخدم للتحقق من صحة وسلامة المستندات أو الرسائل الرقمية، والتأكد من أن مصدرها أصلي وغير معدّل

آلية العمل

- يقوم المرسل بإنشاء توقيع رقمي باستخدام المفتاح الخاص. عندما يتلقى المستلم الرسالة أو المستند، يقوم باستخدام المفتاح العام للتحقق من صحة التوقيع



End-to-End Encryption

المزايا والتحديات

- **المزايا:** يضمن سرية كاملة للمحادثات ويمنع أي جهة ثالثة من اعتراضها
- **التحديات:** إذا تم فقدان المفتاح الخاص، لا يمكن استعادة الرسائل

الاستخدامات العملية

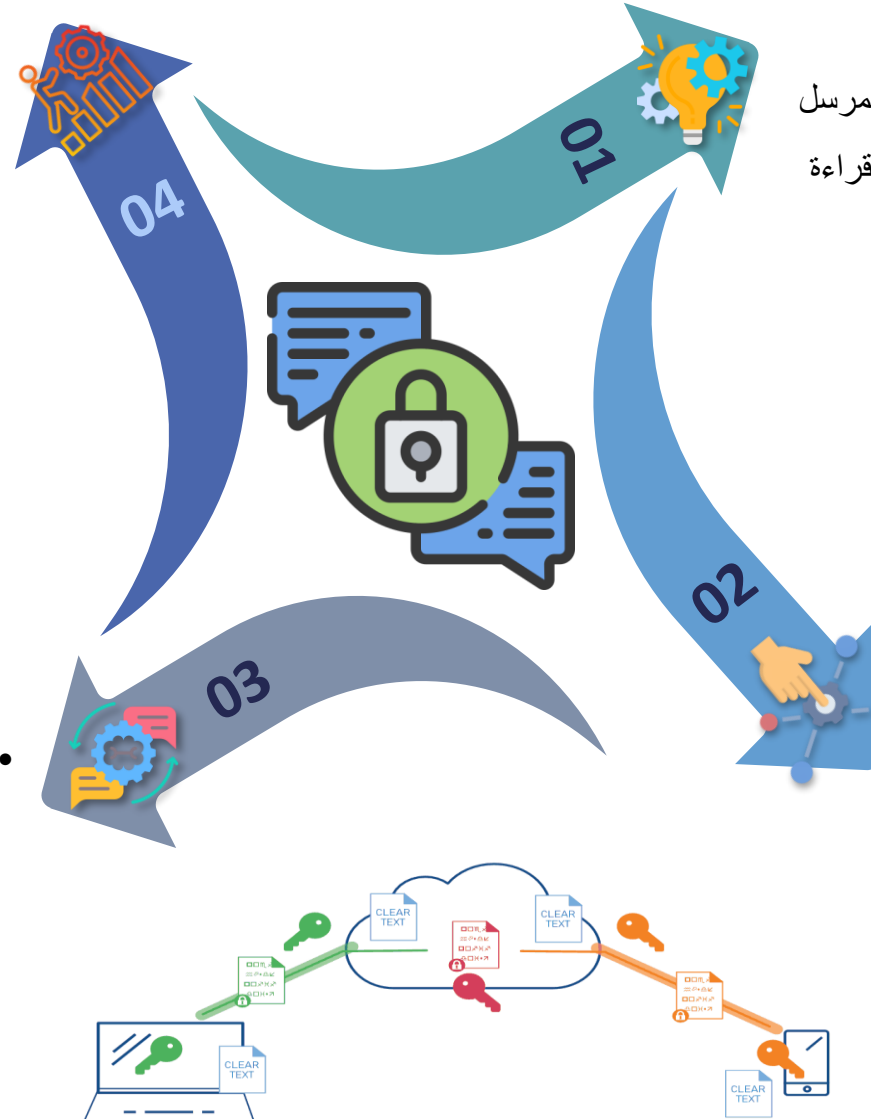
- يُستخدم بشكل شائع في تطبيقات المراسلة مثل لتأمين Signal و WhatsApp الاتصالات بين المستخدمين

مفهوم التشفير من طرف إلى طرف

- هو نوع من التشفير يضمن أن الرسالة أو البيانات يتم تشفيرها من المرسل وفك تشفيرها فقط من قبل المستقبل. حتى مزودي الخدمة لا يمكنهم قراءة أو اعتراض المحتوى

آلية العمل

- يتم تشفير الرسالة باستخدام مفتاح المرسل وفك تشفيرها فقط عند وصولها إلى المستقبل باستخدام مفتاحه الخاص



المزايا والتحديات

- **المزايا:** توفير حماية قوية للبيانات المخزنة في السحابة، مع القدرة على الوصول من أي مكان
- **التحديات:** يعتمد الأمان على مزودي الخدمة السحابية، وقد يكون هناك مخاطر إذا لم يتم إدارة الأذونات بشكل صحيح

الاستخدامات العملية

- تُستخدم في تخزين البيانات الحساسة للشركات عبر خدمات مثل **Amazon Web Services (AWS)** و **Microsoft Azure**

مفهوم الحماية السحابية

- الحماية السحابية هي مجموعة من التدابير الأمنية المصممة لحماية البيانات والبنية التحتية الموجودة في السحابة من الاختراقات والهجمات الإلكترونية

آلية العمل

- تتضمن الحماية السحابية تشفير البيانات المخزنة والمنقولة، استخدام جدران نارية افتراضية، وإدارة حقوق الوصول للمستخدمين



Security Patches

المزايا والتحديات

- **المزايا:** تمنع الهجمات الإلكترونية التي تستغل الثغرات المعروفة في الأنظمة
- **التحديات:** قد يتم تأجيل تثبيت التحديثات من قبل المستخدمين، مما يترك الأنظمة عرضة للهجمات

الاستخدامات العملية

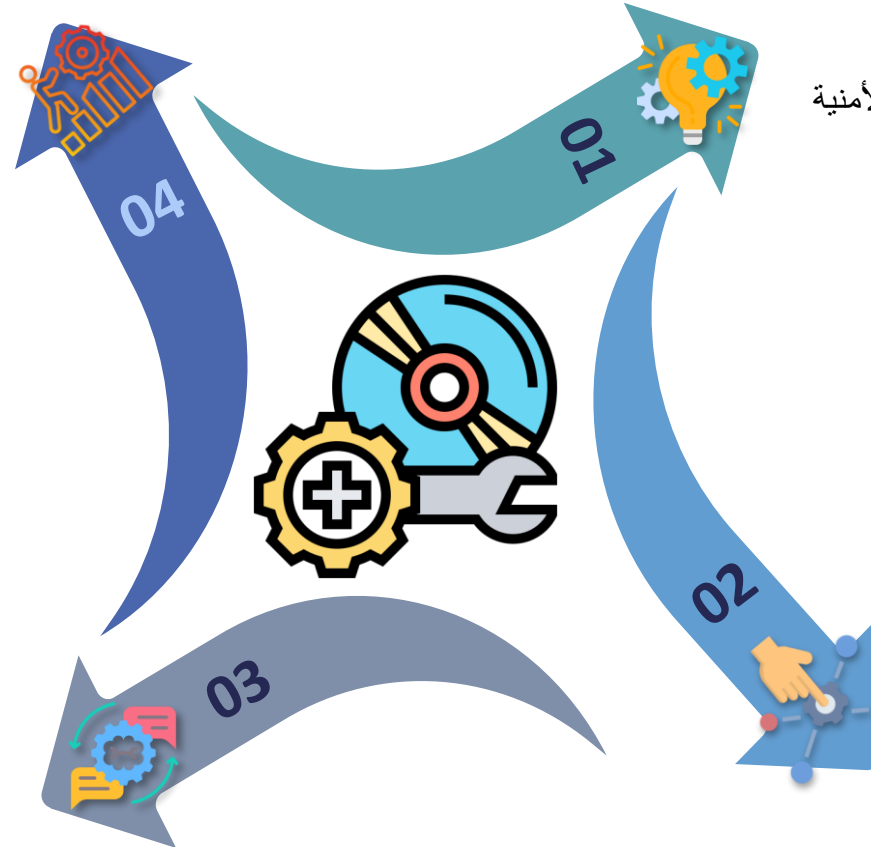
- تُستخدم في جميع الأجهزة والأنظمة لضمان حماية البيانات والمستخدمين من التهديدات المستجدة

مفهوم التحديثات الأمنية

- التحديثات الأمنية هي ترقيات برمجية تهدف إلى تصحيح الثغرات الأمنية التي يتم اكتشافها في الأنظمة أو البرامج

آلية العمل

- يقوم المطورون بإصدار تحديثات تصحيحية تعمل على سد الثغرات وتحسين أمان النظام. يجب على المستخدمين تثبيت هذه التحديثات فور توفرها



Virtual Private Network (VPN)

المزايا والتحديات

- **المزايا:** يحمي الخصوصية ويمنع تتبع النشاط عبر الإنترنت
- **التحديات:** يعتمد على قوة الاتصال وسرعة الإنترنت، وقد يؤدي إلى بطء في التصفح

الاستخدامات العملية

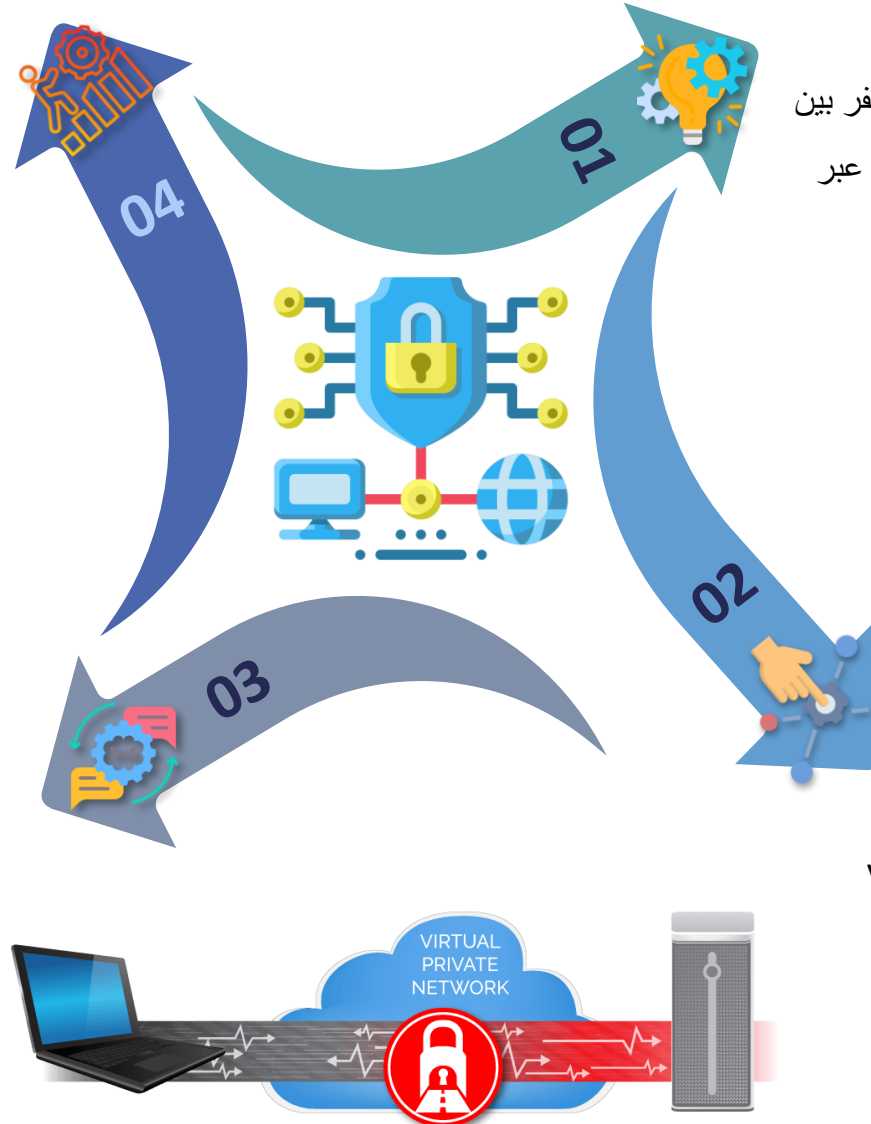
- **التصفح الآمن:** يستخدمه الأفراد والشركات لتصفح الإنترنت بشكل آمن ومجهول
- **الوصول إلى المحتوى المحظور:** يمكن للمستخدمين تجاوز القيود الجغرافية للوصول إلى محتوى محظور في بلدانهم

مفهوم VPN

- الشبكة الافتراضية الخاصة هي أداة تستخدم لإنشاء اتصال آمن ومشفر بين جهاز المستخدم وخادم آخر عبر الإنترنت. يتم توجيه حركة المرور عبر نفق مشفر لضمان الخصوصية وحماية البيانات أثناء التصفح

آلية العمل

- يقوم المستخدم بالاتصال بخادم الشبكة الافتراضية الخاصة مما يخفي عنوان ip الخاص به ويؤمن نقل البيانات
- يتم تشفير جميع البيانات المرسلة والمستلمة بين الجهاز وخادم VPN مما يضمن عدم تمكن الجهات الخارجية من اعتراض البيانات



IDS/IPS Intrusion Detection System/Intrusion Prevention System

المزايا والتحديات

- **المزايا:** يوفر حماية استباقية، حيث يقوم بمنع التهديدات قبل أن تصل إلى النظام
- **التحديات:** قد يؤدي إلى تحذيرات كاذبة ويحتاج إلى ضبط دقيق لتجنب إيقاف حركة المرور الشرعية

الاستخدامات العملية

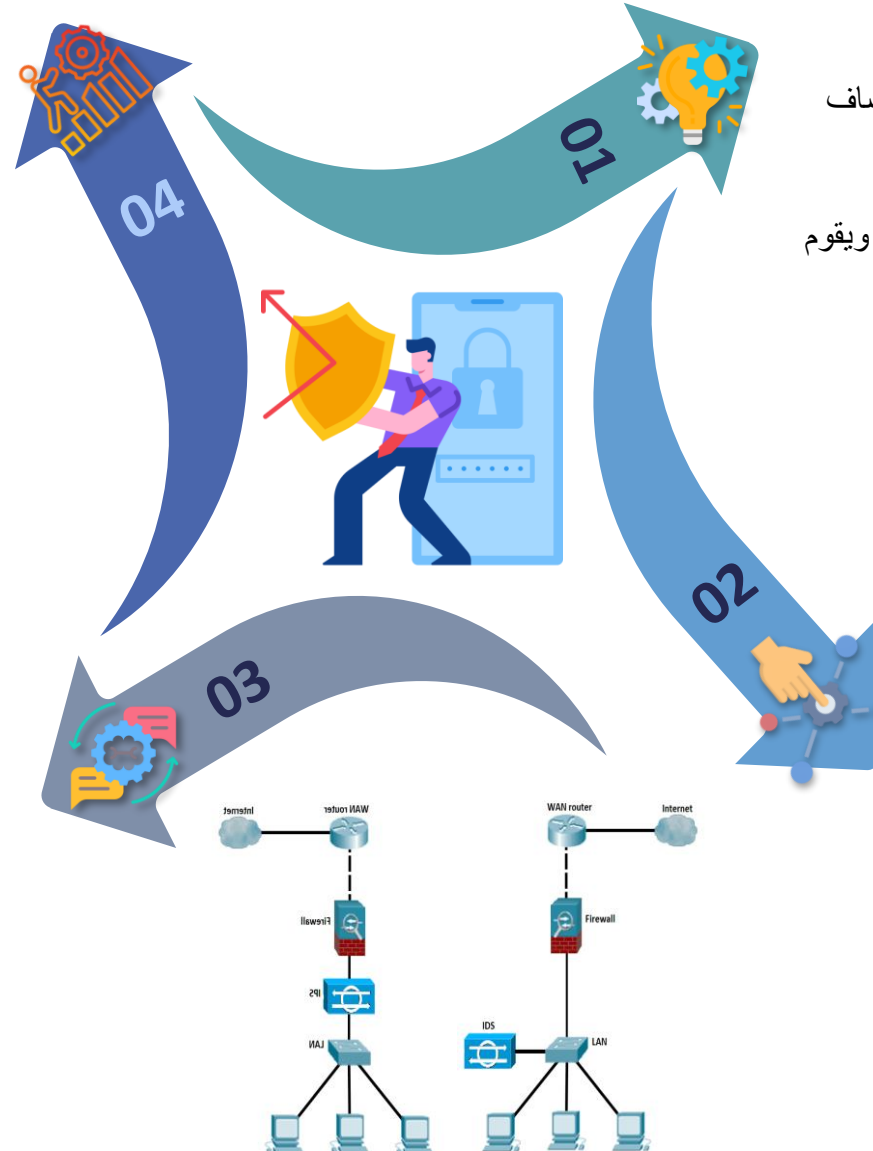
- يُستخدمان في المؤسسات الكبيرة لضمان اكتشاف التهديدات مبكرًا ومنع الاختراقات، خاصة في البيئات الحساسة مثل الشبكات البنكية أو الحكومية

مفهوم IDS/IPS

- **نظام كشف التطفل:** هو نظام يقوم بمراقبة حركة مرور الشبكة لاكتشاف أي نشاط مشبوه أو محاولات اختراق
- **نظام منع التطفل:** هو نظام يقوم بمنع التهديدات تلقائيًا بعد اكتشافها، ويقوم بعرقلة النشاطات غير المشروعة التي تستهدف الشبكة

آلية العمل

- **نظام كشف التطفل:** يراقب حركة المرور ويقوم بتنبيه المسؤولين عند اكتشاف أي محاولة اختراق
- **نظام منع التطفل:** يقوم باتخاذ إجراء فوري لمنع التهديد، مثل قطع الاتصال أو منع الوصول إلى النظام



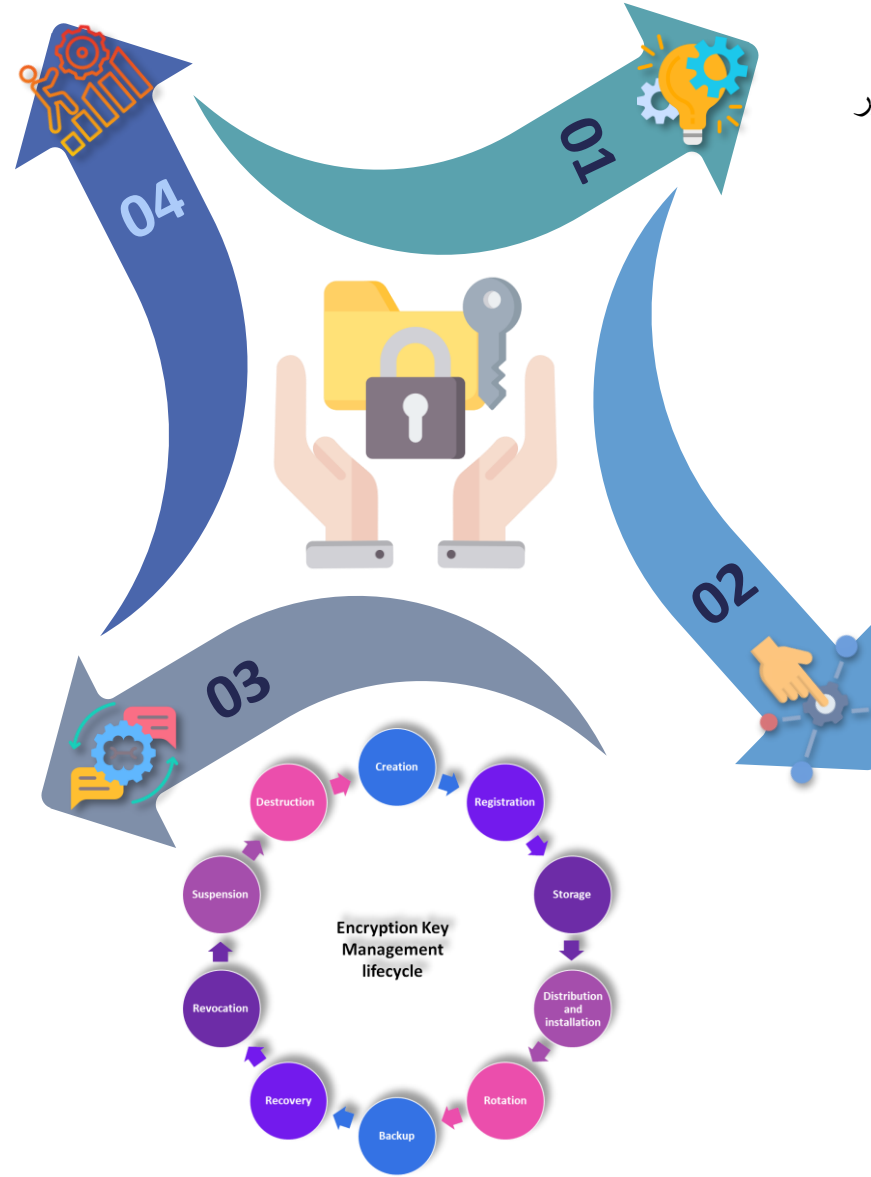
Encryption Key Management

المزايا والتحديات

- **المزايا:** تضمن حماية البيانات حتى في حالة وقوعها في أيدي غير مصرح لهم
- **التحديات:** يتطلب إدارة دقيقة للمفاتيح، وإذا تم فقدان المفتاح، قد يصبح من المستحيل استعادة البيانات المشفرة

الاستخدامات العملية

- تُستخدم في المؤسسات التي تتعامل مع كميات كبيرة من البيانات الحساسة، مثل البنوك، لضمان أمان البيانات المشفرة أثناء النقل والتخزين



مفهوم إدارة مفاتيح التشفير

- إدارة مفاتيح التشفير هي عملية إنشاء، توزيع، وتخزين مفاتيح التشفير بطريقة آمنة لضمان حماية البيانات المشفرة ومنع الوصول غير المصرح به

آلية العمل

- يتم إنشاء مفاتيح تشفير جديدة لحماية البيانات، وتخزينها في أماكن آمنة، وتوزيعها فقط على المستخدمين المصرح لهم للوصول إلى البيانات المشفرة

Zero-Day Exploit

المزايا والتحديات

- المزايا: قدرة على استغلال نقاط ضعف غير معروفة للحماية
- التحديات: من الصعب جدًا حماية النظام ضد ثغرات غير معروفة أو غير مُكتشفة

الاستخدامات العملية

- يستخدمه المهاجمون لاختراق الأنظمة وسرقة البيانات أو تنفيذ أوامر ضارة قبل أن يتم اكتشاف الثغرة وإصلاحها

مفهوم استغلال الثغرات يوم الصفر

- استغلال الثغرات يوم الصفر يشير إلى استغلال ثغرة أمنية غير مكتشفة بعد من قبل المطورين أو الشركات، مما يسمح للمهاجمين باستغلالها قبل أن يتم إصلاحها

آلية العمل

- يتم اكتشاف ثغرة أمنية جديدة في البرنامج أو النظام، ويقوم المهاجم باستغلال هذه الثغرة قبل أن يتمكن المطورون من إصدار تصحيح أمني





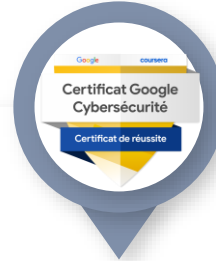
NIST

- [NIST Cybersecurity Framework \(CSF\)](#)
- [NIST Incident Response Lifecycle](#)
- [NIST Special Publication 800-53](#)
- [NIST Guidelines on Security and Privacy Controls](#)



ISO/IEC

- [ISO/IEC 27001 Information Security Management](#)



Google

- [Google Cybersecurity Certificate](#)



EC-Council

- [CEH Certification - EC-Council](#)



Recommendation

- [الهيئة الوطنية للأمن السيبراني](#)
- [المعجم العربي للأمن السيبراني](#)