معجم امن المعلومات

Information Security Glossary

عبدالله الحمداني

ABDULLAH AL-HAMADANI

معجم أمن المعلومات

عبدالله الحمداني

مرحبًا بكم في معجم أمن المعلومات - يهدف المعجم إلى إزالة التعقيد عن أمن المعلومات في اللغة العربية. يعد هذا المعجم بمثابة مورد لأي شخص في مشهد للأمن السيبراني، حيث يقدم تعريف واضح وتفسيرات موجزة لمجموعة شاملة من المصطلحات. سواء كنت محترف في مجال الأمن السيبراني، أو طالبًا يتعمق في عالم الأمن ، أو خبير في المجال يسعى إلى تعزيز فهمك، فإن هذا المعجم يوفر دليلاً منظمًا وسهل الوصول إليه. ويغطي المفاهيم الأساسية.

تم إعداد هذا المسرد بدقة وحسب الابجدية الانكليزية A-Z ليس فقط لتوضيح معنى مصطلحات الأمن السيبراني ولكن أيضًا لتقديم نظرة لتطبيقاتها العملية. مما يضمن أن المستخدم يكتسب أيضًا فهم تطبيقي للمصطلحات. يتم تحديث المعجم كل فترة لمواكبة مشهد الأمن السيبراني المتطور باستمرار.

الفهرست

A

التحكم بالوصول Access Control

السياسات والإجراءات والآليات التي تحدد من يُسمح له بالوصول إلى موارد محددة أو استخدامها في الكومبيوتر. يضمن التحكم في الوصول أن المستخدمين المصرح لهم فقط هم من يمكنهم الوصول إلى ملفات أو أنظمة أو شبكات معينة.

قائمة التحكم في الوصول Access Control List - ACL

آلية أمان تستخدم لتحديد وإدارة صلاحيات الموارد مثل الملفات أو الدلائل أو أجهزة الشبكة في نظام الكمبيوتر أو الشبكة.

خدمة التحكم في الوصول Access Control Service - ACS

آلية أمنية تحكم وتدير التفويض والأذونات الممنوحة للمستخدمين أو الكيانات التي تحاول الوصول إلى الموارد داخل النظام أو الشبكة.

الاعتماد Accreditation

الاعتراف الرسمي والتفويض الممنوح من قبل سلطة معترف بها لكيان ما، مثل منظمة أو نظام أو فرد، مما يؤكد امتثاله لمعايير ومتطلبات أمنية محددة.

التعليم النشط Active Learning

نهج ديناميكي استباقي يشارك فيه الأفراد أو الأنظمة في الاكتساب المستمر للمعرفة والمهارات لتعزيز قدرتهم على اكتشاف التهديدات الأمنية ومنعها والاستجابة لها.

الشبكة المخصصة Ad Hoc

بنية تحتية للاتصالات اللامركزية والمؤقتة يتم تشكيلها تلقائيًا بين مجموعة من الأجهزة دون الاعتماد على بنية تحتية للشبكة محددة مسبقًا أو تنسيق مركزي.

اختطاف الحساب Account Hijacking

الاستيلاء على حساب المستخدم عبر الإنترنت، عادةً من قبل جهات خبيثة يمكنها الوصول إلى بيانات اعتماد تسجيل الدخول من خلال وسائل مختلفة مثل التصيد أو اختراق كلمة المرور أو استغلال الثغرات الأمنية.

اكيملو Accumulo

نظام قاعدة بيانات NoSQL مفتوح المصدر وموزع مصمم خصيصًا لتخزين البيانات ومعالجتها على نطاق واسع مع التركيز على ميزات الأمان.

تحليل التشفير الصوتي Acoustic cryptanalysis

شكل من أشكال هجوم القناة الجانبية الذي يتضمن تحليل انبعاثات الصوت التي ينتجها نظام أو جهاز أثناء تشغيله لاستخراج المعلومات الحساسة، وخاصة مفاتيح التشفير. تعتمد هذه التقنية على حقيقة أن المكونات الإلكترونية، مثل المعالجات أو أجهزة التشفير، تبعث إشارات صوتية دقيقة عند معالجة المعلومات. ومن خلال التقاط هذه الانبعاثات الصوتية وتحليلها، قد يستنتج المهاجمون الأنماط أو يستنتجون معلومات أساسية، مما يعرض أمن عمليات التشفير للخطر.

الدفاع النشط Active Defense

مجموعة من الحلول والاستراتيجيات الأمنية الاستباقية التي تتخذها المؤسسات لاكتشاف تهديدات الأمن السيبراني والاستجابة لها والتخفيف من حدتها.

تقنيات التهرب المتقدمة Advanced Evasion Techniques- AET

الأساليب المتطورة التي يستخدمها المهاجمون للتحايل على الحلول الأمنية والتهرب منها، وخاصة أجهزة أمن الشبكات وأنظمة كشف/منع التسلل.

المرفقات التكنلوجية المتقدمة Advanced Technology Attachment ATA

واجهة لتوصيل أجهزة التخزين، مثل محركات الأقراص ومحركات الأقراص القابلة للازالة ، بأنظمة الكمبيوتر.

تمييز المجموعات الخبيثة Adversary group naming

ممارسة تعيين أسماء أو تسميات مميزة لمجموعات منظمة أو أفراد ذوي نوايا خبيثة يشاركون في التهديدات السيبرانية أو الهجمات أو التجسس. تساعد هذه الأسماء، التي غالبًا ما يصاغها الباحثون أو المحللون أو وكالات الاستخبارات في مجال الأمن السيبراني، في تصنيف وتحديد الجهات الفاعلة في مجال التهديد بناءً على تكتيكاتها وتقنياتها وإجراءاتها (TTPs).

الذكاء الاصطناعي Artificial Intelligence

تطبيق الخوارزميات المتقدمة وتقنيات التعلم الآلي لتعزيز قدرات أنظمة الأمن والدفاعات. يلعب الذكاء الاصطناعي دورًا مهما في أتمتة تحليل كميات هائلة من البيانات، وتحديد الأنماط، واكتشاف الحالات الشاذة التي قد تشير إلى تهديدات أمنية محتملة.

ارهاق التنبيه Alert fatigue

الحالة التي يصبح فيها الأفراد مرهقين بسبب الحجم الكبير من التنبيهات الأمنية الناتجة عن أنظمة المراقبة.يتم استخدام العديد من الأدوات والتقنيات للكشف عن الحوادث الأمنية المحتملة والإبلاغ عنها. ومع ذلك، عندما تولد هذه الأنظمة عددًا كبيرًا من التنبيهات، والتي قد يكون الكثير منها إيجابيات كاذبة أو مشكلات ذات أولوية منخفضة، يمكن أن يعاني موظفو الأمن من إرهاق التنبيه.

كشف الشذوذ Anomoly Detection

عملية تحديد السلوكيات أو الأحداث التي تنحرف بشكل كبير عن المعايير المعمول بها داخل النظام أو الشبكة. تعتبر هذه التقنية ضرورية لاكتشاف التهديدات الأمنية المحتملة أو الأنشطة غير النظامية التي قد تشير إلى نوايا خبيثة.

اداة Anonymizer

أداة أو خدمة مصممة لتعزيز الخصوصية عبر الإنترنت عن طريق إخفاء أو تغيير المعلومات التعريفية للمستخدمين، مما يجعل من الصعب تتبع أنشطتهم عبر الإنترنت للوصول إلى هويتهم الحقيقية.

التشفير غير المتماثل Asymmetric Encryption

نظام تشفير يستخدم زوجًا من المفاتيح المرتبطة رياضيًا للاتصال الآمن للبيانات. يتكون زوج المفاتيح من مفتاح عام، يتم توزيعه ومعروف للآخرين، ومفتاح خاص، يحتفظ به مالك المفتاح. تستخدم عملية التشفير المفتاح العام للمستلم لتشفير البيانات، ولا يمكن فك تشفيرها إلا للمفتاح الخاص المقابل.

الطبقة المجردة Abstraction Layer

واجهة بين مكونات أو طبقات مختلفة في النظام، وهي مصممة لإخفاء تعقيد التفاصيل ذات المستوى الأدنى وتوفير واجهة مبسطة وموحدة للوظائف ذات المستوى الأعلى.

فيروس الاعلانات Adware

البرامج التي تعرض إعلانات على جهاز المستخدم دون موافقته أو علمه.

الفيروس المدرع Armored virus

نوع من الفيروسات يستخدم تقنيات متقدمة لتجنب اكتشافه بواسطة برامج مكافحة الفيروسات والإجراءات الأمنية الأخرى.

سرقة الصراف ATM skimming

تقنية يستخدمها المجرمين لالتقاط وسرقة المعلومات المالية الحساسة بشكل غير قانوني من الاشخاص الذين يستخدمون أجهزة الصراف الآلي (ATMs). يقوم المجرمون بتوصيل أجهزة صغيرة غير واضحة تسمى الكاشطات بفتحة قارئ البطاقة الموجودة في ماكينة الصراف الآلي. تم تصميم هذه الكاشطات لتسجيل بيانات الشريط المغناطيسي سرًا وفي بعض الأحيان التقاط أرقام التعريف الشخصية التي يدخلها المستخدمون.

حركة الهجوم Attack traffic

بيانات الشبكة او الاتصال التي يتم إنشاؤها كجزء الهجمات الإلكترونية على أنظمة الكمبيوتر أو الشبكات أو التطبيقات. تشمل حركة المرور هذه مجموعة واسعة من الأنشطة، بما في ذلك محاولات الوصول غير المصرح ، واستغلال نقاط الضعف، وهجمات حجب الخدمة الموزعة (DDoS)، وغيرها من الإجراءات الضارة التي تهدف إلى المساس بسلامة الأصول الرقمية أو سريتها أو توفرها.

البرمجة التعسفية Arbitrary Code Execution - ACE

مفهوم أمني مهم يشير إلى قدرة المهاجم على تنفيذ تعليمات برمجية عشوائية على نظام أو تطبيق مستهدف، وغالبًا ما يكون ذلك نتيجة لاستغلال نقاط الضعف أو العيوب في البرنامج.

سطح الهجوم Attack surface

جميع النقاط المحتملة التي قد يكون فيها النظام أو التطبيق أو الشبكة عرضة للاستغلال من قبل المهاجم. يشمل سطح الهجوم على نقاط دخول وواجهات وتفاعلات مختلفة يمكن استهدافها بالأنشطة الضارة.

نقطة الوصول Access Point

جهاز أو برنامج يمكّن الأجهزة من الاتصال بشبكة سلكية أو لاسلكية للوصول إلى مواردها وخدماتها. تستخدم نقطة الوصول بشكل شائع في الشبكات اللاسلكية، وتعمل كجسر بين الأجهزة، مثل أجهزة الكمبيوتر أو الأجهزة المحمولة.

ادارة الحساب Account Management

الإشراف على حسابات المستخدمين داخل نظام الكمبيوتر أو الشبكة أو التطبيق. تتضمن هذه العملية إنشاء حسابات المستخدمين وتعديلها وحذفها، بالإضافة إلى تحديد امتيازات وأذونات الوصول وتنفيذها.

الدليل النشط Active Directory

خدمة مركزية تم تطويرها بواسطة مايكروسوفت، وتعمل كأساس لإدارة الهوية والوصول في انظمة الويندوز. وهي تعمل كقاعدة بيانات تقوم بتخزين وتنظيم المعلومات حول موارد الشبكة، بما في ذلك حسابات المستخدمين وأجهزة الكمبيوتر المختلفة.

الاستطلاع النشط Active Recon

أسلوب استباقي لجمع المعلومات يستخدمه متخصصو الأمن أو الجهات الخبيثة لتقييم الوضع الأمني للنظام أو الشبكة المستهدفة. على النقيض من الاستطلاع السلبي، الذي يتضمن جمع البيانات المتاحة للجمهور دون التفاعل المباشر مع الهدف، يتضمن الاستطلاع النشط التحقيق والاستفسار بشكل فعال عن أنظمة الهدف لتحديد نقاط الضعف والمنافذ المفتوحة ونقاط الدخول المحتملة.

اسمبلي Assembly

لغة برمجة منخفضة المستوى ترتبط ارتباطًا وثيقًا ببنية وحدة المعالجة المركزية للكمبيوتر (CPU). على عكس لغات البرمجة عالية المستوى التي تكون أكثر قابلية للقراءة من قبل الإنسان، تتكون لغة اسمبلي من تمثيلات رمزية لتعليمات الكود .

الاختبار التكيفي Adaptive Testing

تقييم ديناميكي يستخدم لتقييم كفاءة الفرد أو النظام في معرفة أو مهارات الأمن السيبراني. يكيف هذا النهج صعوبة أسئلة الاختبار بناءً على إجابات المستجيب السابقة، ويصمم التقييم وفقًا لمستوى الكفاءة المثبت .

التهديد المستمر المتقدم Advanced Persistent Threat - APT

هجوم متطور وطويل الأمد يتم تنسيقه من قبل مهاجم ذو مهارات عالية ومنظم بهدف أساسي هو التسلل والحفاظ على الوصول غير المكتشف إلى الشبكة أو النظام المستهدف على مدى فترة طويلة. غالبًا ما تشتمل التهديدات المستمرة المتقدمة (APTs) على مجموعة من التقنيات المعقدة، مثل الهندسة الاجتماعية، وعمليات يوم الصفر، والبرامج الضارة المخصصة، لاختراق الدفاعات الأمنية.

الاستشاري Advisory

اتصال رسمي صادر عن خبراء أو سلطات أمنية لإبلاغ الجمهور أو المنظمات أو الأفراد حول نقاط الضعف أو التهديدات أو المشكلات الأمنية المحتملة. توفر النصائح الأمنية عادةً معلومات تفصيلية حول طبيعة المشكلة الأمنية وتأثيرها المحتمل وإرشادات حول كيفية تخفيف المشكلة أو معالجتها.

التنبيه Alert

إشعار أو تحذير يتم إنشاؤه بواسطة أنظمة الأمان أو أدوات المراقبة استجابة للحوادث الأمنية المكتشفة أو المشتبه فيها. تعمل التنبيهات كمؤشرات فورية للتهديدات المحتملة أو الأنشطة غير المصرحة أو الحالات المشبوهة داخل الشبكة أو النظام.

مضاد المالوير Anti-Malware

تطبيقات الأمان المتخصصة المصممة لاكتشاف المالوير ومنعها وإزالتها، والمعروفة عمومًا بالبرامج الضارة. يعمل لحماية البيئات الرقمية من خلال استخدام مجموعة متنوعة من الآليات، بما في ذلك الكشف بالتوقيع، والتحليل الإرشادي، ومراقبة السلوك، لتحديد وتحييد مجموعة واسعة من التعليمات البرمجية الضارة مثل الفيروسات والديدان وأحصنة طروادة وبرامج التجسس.

مضاد الفيروسات Anti-Virus

تطبيقات الأمان المصممة لاكتشاف الفيروسات خصيصا ومنعها وإزالتها من أنظمة الكمبيوتر والشبكات.

الاصول Asset

أي مورد قيم، ماديًا أو رقميًا، له أهمية بالنسبة للمؤسسة ويتطلب الحماية من التهديدات أو المخاطر المحتملة. يمكن أن تشمل الأصول مجموعة واسعة بما في ذلك المعلومات والبيانات والأجهزة والبرامج والملكية الفكرية والموظفين.

توقيع الهجوم Attack Signature

نمط أو خاصية مرتبطة بنوع معين من الهجمات السيبرانية. هذه التوقيع عبارة عن معرف فريد تستخدمه أنظمة الأمان، مثل أنظمة كشف التسلل والوقاية منه، للتعرف على التهديدات المعروفة والتخفيف من حدتها.

سجل التدقيق Audit Log

السجل الزمني أو المسار الإلكتروني الذي يوثق ويخزن الأنشطة أو الأحداث أو المعاملات ذات الصلة داخل نظام الكمبيوتر أو الشبكة.

مصفوفة الوصول Access Matrix

نموذج أمان يوفر تمثيلاً شاملاً لحقوق الوصول والأذونات داخل نظام الكمبيوتر أو الشبكة.

حصاد الحساب Account Harvesting

ممارسة خبيثة في مجال الأمن السيبراني حيث يقوم المهاجم بجمع وتجميع عدد كبير من حسابات المستخدمين أو بيانات الاعتماد من مصادر مختلفة بشكل منظم. يتضمن هذا غالبًا تقنيات آلية، مثل استخدام الروبوتات أو السكربت، لاستغلال نقاط الضعف في الأنظمة أو مواقع الويب أو قواعد البيانات عبر الإنترنت.

المحتوى النشط Active content

العناصر الديناميكية والقابلة للتنفيذ المضمنة في المحتوى الالكتروني ، مثل صفحات الويب أو المستندات، التي تتمتع بالقدرة على تنفيذ الإجراءات أو تنفيذ التعليمات البرمجية عند الوصول إليها أو التفاعل معها من قبل المستخدمين.

مراقب النشاط Activity Monitors

أدوات أو أنظمة أمنية مصممة لتتبع وتسجيل أنشطة وسلوكيات المستخدمين داخل شبكة الكمبيوتر أو النظام. تلتقط هذه الشاشات مجموعة من المعلومات، بما في ذلك أحداث تسجيل الدخول/الخروج، والوصول إلى الملفات، واستخدام التطبيقات، واتصالات الشبكة، وتفاعلات المستخدم الأخرى.

بروتوكول تحليل العنوان Address Resolution Protocol - ARP

بروتوكول اتصال يستخدم في شبكات الكمبيوتر لتعيين أو تحليل عنوان بروتوكول إنترنت معروف (IP) إلى عنوان التحكم في الوصول إلى الوسائط (MAC) المقابل.

معيار التشفير المتقدم Advanced Encryption Standard - AES

خوارزمية تشفير متماثلة معتمدة على نطاق واسع أنشأها المعهد الوطني للمعايير والتكنولوجيا (NIST). يتم استخدام AES لتشفير البيانات الحساسة في تطبيقات مختلفة، بما في ذلك تأمين قنوات الاتصال، وحماية المعلومات المخزنة، وضمان سرية عمليات نقل البيانات.

الخوارزمية Algorithm

مجموعة من التعليمات أو الإجراءات المصممة لتنفيذ مهمة أو عملية حسابية محددة.

التشفير غير المتماثل Asymmetric cryptography

معروف أيضًا باسم تشفير المفتاح العام، هو نظام تشفير يستخدم أزواجًا من المفاتيح المرتبطة رياضيًا للاتصال الآمن.

الحرب غير المتكافئة Asymmetric warfare

نوع من الصراع حيث تمتلك القوى المتحاربة قدرات واستراتيجيات وموارد عسكرية مختلفة، مما يؤدي إلى ديناميكية قوة غير متكافئة. في هذا الشكل من الحرب، يستخدم أحد الأطراف عادةً تكتيكات غير تقليدية، وغالبًا ما يستفيد من المزايا غير المتكافئة مثل حرب العصابات أو التمرد أو الإرهاب أو الحرب السيبرانية، لتعويض نقاط القوة التقليدية لخصم أكثر قوة.

التدقيق Auditing

الفحص والتقييم المنظم لأنظمة المعلومات والعمليات والضوابط الخاصة بالمؤسسة لضمان الامتثال للسياسات واللوائح وأفضل الممارسات الأمنية. الهدف الأساسي من التدقيق هو تقييم فعالية الحلول الأمنية المعمول بها، وتحديد نقاط الضعف، والتحقق من التنفيذ السليم للضوابط الأمنية. تشمل عمليات تدقيق الأمان مجموعة من الأنشطة، بما في ذلك مراجعة سجلات الوصول وفحص التكوينات وتقييم سلامة البيانات وتقييم المرونة العامة للوضع الأمني للمؤسسة

تجميد الحساب Account Freezing

تقييد وصول المستخدم إلى حسابه أو موارده المالية. غالبًا ما يتم اتخاذ هذا الإجراء من قبل المؤسسات المالية أو المنصات عبر الإنترنت أو مقدمي الخدمات ردًا على الأنشطة المشبوهة أو المخاوف الأمنية أو انتهاك شروط الخدمة. عندما يتم تجميد الحساب، عادةً ما يكون صاحب الحساب غير قادر على إجراء معاملات معينة أو الوصول إلى الأموال أو استخدام الحساب حتى يتم حل المشكلة. تجميد الحساب هو إجراء أمني يتم تنفيذه لحماية كل من صاحب الحساب ومقدم الخدمة من الأنشطة الاحتيالية المحتملة. ومن الضروري لأصحاب الحسابات التواصل مع المؤسسة ذات الصلة لمعالجة سبب التجميد واتخاذ الخطوات اللازمة لإعادة تنشيط الحساب.

الدفاع السيبراني النشط Active Cyber Defence

منهج شامل واستباقي للأمن السيبراني يتضمن اتخاذ حلول فعالة لاكتشاف التهديدات السيبرانية ومنعها والاستجابة لها في نفس الوقت. على عكس استراتيجيات الدفاع السلبية التي تركز على تحصين محيط الشبكة، يؤكد الدفاع النشط ACD على المراقبة المستمرة والاستجابة السريعة واستخدام التقنيات المتقدمة لتعطيل التهديدات السيبرانية بشكل فعال. قد تتضمن استراتيجيات ACD استخبارات التهديدات، والاستجابة الآلية للحوادث، والتحليلات الأمنية، واختبار الاختراق، وتكامل تقنيات الخداع لتضليل المهاجمين وإرباكهم.

المسؤول Administrator

شخص مسؤول عن مراقبة وإدارة عمليات أنظمة الكمبيوتر أو الشبكات أو المؤسسات. يلعبون دورا مهما في ضمان سير العمل وأمن بيئات المعلومات. ومكلفون بتكوين وصيانة الأجهزة والبرامج، ومعالجة المشاكل الفنية، وتنفيذ الحلول الأمنية. اعتمادًا على دورهم المحدد، قد يركز المسؤولون على الأنظمة أو الشبكات أو قواعد البيانات أو البنية التحتية الشاملة لتكنولوجيا المعلومات.

الذكاء الصناعي Artificial Intelligence - AI

فرع من علوم الكمبيوتر يركز على إنشاء آلات ذكية قادرة على أداء المهام التي تتطلب عادة الذكاء البشري. وتشمل هذه المهام التعلم من الخبرة، وفهم اللغة البشرية، والتعرف على الأنماط، وحل المشاكل، والتكيف مع المواقف الجديدة. تم تصميم أنظمة الذكاء الاصطناعي لتقليد الوظائف المعرفية، تتجاوز احيانا القدرات البشرية في مجالات محددة. يشمل هذا المجال مناهج مختلفة، مثل التعلم الآلي، والذي يتضمن خوارزميات التعلم من البيانات لإجراء تنبؤات أو قرارات، والتعلم العميق، المستوحى من الشبكات العصبية للدماغ البشري.

قائمة المسموحات Allow List

قائمة بالعناصر أو الكيانات المعتمدة التي تم السماح لها أو منحها حق الوصول إلى نظام أو خدمة أو شبكة. تعمل كإجراء أمني من خلال تحديد ما هو مسموح به، ويتم منح الإذن فقط للاشخاص الموجودين في القائمة، بينما يتم رفض كل شيء آخر تلقائيًا. يُستخدم هذا الأسلوب بشكل شائع في مجالات مختلفة، مثل أمان الكمبيوتر أو تكوينات الشبكة، للتحكم في الوصول إلى موارد معينة وتقييده.

اندرويد Android

نظام تشغيل تم تطويره بواسطة جوجل للأجهزة المحمولة مثل الهواتف الذكية والأجهزة اللوحية. يوفر اندرويد واجهة سهلة الاستخدام، ويدعم مجموعة واسعة من التطبيقات، وهو معروف بخيارات التخصيص الخاصة به. وهو نظام تشغيل مفتوح المصدر (Open Source)، مما يعني أن الكود المصدري الخاص به متاح مجانًا، يسمح لمصنعي الأجهزة بتخصيصه وتكييفه مع أجهزتهم المحددة.

انتي فايروس Anti-Virus

نوع من البرامج المصممة لحماية أجهزة الكمبيوتر والأجهزة من المالوير (البرامج الضارة). تشتمل البرامج الضارة على الفيروسات والديدان وأحصنة طروادة وبرامج التجسس وغيرها من المالوير التي يمكن أن تلحق الضرر بوظائف الكمبيوتر أو تسرق معلومات حساسة أو تعرض الأمان للخطر.

التطبيق Application

برنامج كمبيوتر مصمم لأداء مهام أو وظائف محددة للمستخدم. يمكن تشغيل التطبيقات على منصات مختلفة مثل أجهزة الكمبيوتر والهواتف الذكية والأجهزة اللوحية والأجهزة الأخرى. وتخدم

أغراضًا متنوعة، بدءًا من أدوات زيادة الانتاجية وتطبيقات الاتصال إلى الترفيه والبرامج المتخصصة لوظائف وصناعات محددة.

التهديد المستمر المتقدم APT

هجوم سيبراني متطور وموجه حيث يتمكن المخترق من الوصول إلى شبكة أو نظام بقصد البقاء دون أن يتم اكتشافه لفترة طويلة. غالبًا ما تتميز هجمات APT باستمرارها وتقنياتها المتقدمة والاختيار الدقيق لأهداف محددة، مثل الوكالات الحكومية أو المؤسسات الكبيرة أو البنية التحتية .

ادارة الاصول Asset Management

إدارة تتبع أصول المؤسسة وصيانتها وتحسينها طوال دورة حياتها. يمكن أن تشمل الأصول عناصر مادية مثل المعدات والبنية التحتية، بالإضافة إلى الأصول غير الملموسة مثل الملكية الفكرية البرامج. في سياق تكنولوجيا المعلومات والأمن السيبراني، تتضمن إدارة الأصول على وجه التحديد تحديد وتصنيف وإدارة الأصول الرقمية مثل الأجهزة والبرامج والبيانات وموارد الشبكة. تساعد هذه العملية المؤسسات على فهم مخزون الأصول لديها، وتقييم المخاطر، والتخطيط للترقيات أو الاستبدالات، وضمان الامتثال للمتطلبات التنظيمية.

شجرة الهجوم Attack Tree

تمثيل رسومي يستخدم في الأمن السيبراني لرسم وتحليل الطرق المحتملة التي يمكن من خلالها اختراق نظام أو شبكة أو مؤسسة بسبب التهديدات السيبرانية. وهو يصور بشكل مرئي مسارات وسيناريوهات الهجوم المختلفة التي قد يستخدمها المهاجمون لاستغلال نقاط الضعف وتحقيق أهدافهم.

ناقل الهجوم Attack Vector

المسار أو الطريقة المحددة التي يستخدمها المهاجم السيبراني لاستغلال نقاط الضعف واختراق نظام الكمبيوتر أو الشبكة أو التطبيق. نواقل الهجوم هي الوسيلة التي يتم من خلالها تنفيذ الهجوم، ويمكن أن تتخذ أشكالًا مختلفة مثل التصيد والمالوير والهندسة الاجتماعية وغيرها.

المهاجم Attacker

فرد أو مجموعة أو كيان يسعى إلى تعريض أمن أنظمة الكمبيوتر أو الشبكات أو البيانات للخطر. عادةً ما يتم تحفيز المهاجمين بأهداف مختلفة، بما في ذلك الوصول غير المصرح به إلى المعلومات الحساسة، أو تحقيق مكاسب مالية، أو تعطيل الخدمات، أو مجرد التسبب في الضرر.

المصادقة Authentication

عملية التحقق من هوية المستخدم أو النظام أو الكيان للتأكد من هويته كما يدعي. بشكل عام، تتضمن المصادقة تقديم بيانات ، مثل اسم المستخدم وكلمة المرور، إلى نظام أو خدمة. يقوم النظام بعد ذلك بفحص بيانات الاعتماد هذه مقابل المعلومات المخزنة لمنح الوصول أو رفضه. تساعد هذه العملية على منع الوصول غير المصرح به، وحماية المعلومات الحساسة، والحفاظ على أمان الموارد الرقمية.

الاصالة Authenticity

التأكد من أن معلومات معينة هي معلومات مشروعة وحقيقية ولم يتم تغييرها أو التلاعب بها.

التفويض Authorization

عملية منح أو رفض أذونات محددة وحقوق الوصول للاشخاص أو الأنظمة بناءً على هويتهم الموثقة.

نظام الحكم الذاتي Autonomous System

مجموعة من شبكات بروتوكول الإنترنت IP وأجهزة التوجيه المتصلة تحت منظمة أو كيان واحد يقدم سياسة توجيه مشتركة للإنترنت.

التوفر Availability

حالة إمكانية الوصول للبيانات وقابليتها للاستخدام عند الحاجة، مما يضمن أن المعلومات والأنظمة والموارد متاحة بشكل موثوق ومستمر للمستخدمين المصرح لهم.

التشغيل التلقائي AutoRun

ميزة في أنظمة التشغيل تقوم تلقائيًا بتنفيذ برنامج أو برنامج نصي معين عند توصيل جهاز تخزين قابل للإزالة، مثل فلاش ميموري USB أو قرص DVD، أو إدخاله في جهاز كمبيوتر. تم تصميم ميزة التشغيل التلقائي لتعزيز راحة المستخدم من خلال تشغيل التطبيقات أو عرض المحتوى دون تدخل يدوي. ومع ذلك، فقد تم استغلالها من قبل البرامج الضارة، ولأسباب أمنية، تم إهمالها أو تعطيلها إلى حد كبير في العديد من أنظمة التشغيل.

B

الباب الخلفي Backdoor

وسيلة سرية للوصول إلى نظام كمبيوتر أو تطبيق أو شبكة، وتجاوز آليات المصادقة أو الأمان العادية. وهي عادة نقطة دخول تمكن الاشخاص أوالجهات الخبيثة من الوصول عن بعد أو الوصول إلى النظام، وغالبًا ما يكون ذلك دون اكتشافهم.

النسخ الاحتياطي BackUp

عملية إنشاء نسخ مكررة من البيانات للحماية من الفقدان أو الفساد أو الحذف بالخطأ، وتسهيل عملية الاسترداد في حالة وقوع أحداث غير متوقعة.

خط الاساس Baselining

عملية إنشاء معيار أو خط أساس للسلوك الطبيعي والمتوقع داخل نظام الكمبيوتر أو الشبكة أو التطبيق. يتضمن ذلك توثيق وتحليل الأنماط النموذجية لأنشطة المستخدم وأداء النظام وحركة مرور الشبكة خلال فترة محددة.

النطاق الترددي Bandwidth

الحد الأقصى لمعدل نقل البيانات أو سعة قناة الاتصال. يتم قياسه عادةً بالبت في الثانية (bps) ويمثل كمية البيانات التي يمكن إرسالها عبر الشبكة خلال إطار زمني محدد.

مكافئة الثغرات Bug Bounty

مبادرة للأمن السيبراني حيث تقوم المؤسسات بدعوة الباحثين الأمنيين لتحديد الثغرات الأمنية في برامجها أو مواقعها الإلكترونية أو تطبيقاتها والإبلاغ عنها. وفي مقابل الكشف بشكل عن نقاط الضعف هذه، يمكن للمشاركين الحصول على مكافآت مالية أو تقدير أو حوافز أخرى.

اللافتة Banner

رسالة أو معلومات معروضة على نظام كمبيوتر أو جهاز شبكة أو تطبيق برمجي يوفر تفاصيل حول تكوين النظام أو إصداره أو حالته التشغيلية.

فحص الصندوق الاسود Black Box Testing

طريقة لاختبار البرامج حيث لا تكون الأعمال الداخلية وبنية التعليمات البرمجية للنظام الذي يتم اختباره معروفة أو يتم الكشف عنها للمختبر. يركز المختبر على تقييم السلوك الخارجي للنظام، واستجابات المدخلات والمخرجات، والوظائف دون الوصول إلى كود المصدر الداخلي.

الثقب الاسود Blackhole

تقنية أو مكون يستخدم لتجاهل حركة مرور الشبكة الضارة أو استيعابها بصمت. غالبًا ما يتم استخدام الثقب الأسود كإجراء دفاعي، حيث تم تصميمه لإعادة توجيه البيانات الضارة أو حركة المرور إلى مسار فارغ مما يمنعها من الوصول إلى وجهتها المقصودة.

بوت كت Bootkit

نوع من البرامج الضارة التي تصيب عملية التمهيد لنظام تشغيل الكمبيوتر، وعادةً ما تستهدف سجل التمهيد الرئيسي (MBR) أو واجهة (UEFI).

متجر البوتات Botshop

منصة أو خدمة تعمل كوسيط بين الذين يمتلكون أو يتحكمون في شبكات الروبوتات (شبكات أجهزة الكمبيوتر المخترقة التي تستخدم غالبًا للأنشطة الضارة) والعملاء المحتملين.

القائمة السوداء Blacklist

قائمة شاملة بالكيانات أو المجالات أو التطبيقات المحظورة أو التي تم وضع علامة عليها باعتبارها مخاطر أمنية محتملة.

المعسكر التدريبي Bootcamp

برنامج تدريبي مكثف يركز على تعزيز مهارات المشاركين ومعارفهم في مجال الأمن السيبراني. تم تصميم هذه البرامج لتوفير تجربة تعليمية مركزة وعملية، وغالبًا ما تغطي مجموعة واسعة من المواضيع مثل القرصنة الأخلاقية واختبار الاختراق والاستجابة للحوادث وغيرها من تخصصات الأمن السيبراني الهامة.

المصادقة الاساسية Basic Authentication

طريقة بسيطة ومستخدمة على نطاق واسع لمصادقة المستخدم في شبكات الكمبيوتر وتطبيقات الويب. تتضمن نقل اسم المستخدم وكلمة المرور في نموذج مشفر من العميل إلى الخادم.

تحليل السلوك Behaviour analysis

فحص الإجراءات والأنشطة داخل بيئة الكومبيوتر لتحديد وفهم السلوك العادي أو المتوقع واكتشاف الانحرافات التي قد تشير إلى تهديدات أمنية محتملة.

برنامج BIND

برنامج BIND، وهو اختصار لـ "Berkeley Internet Name Domain"، هو برنامج مفتوح المصدر ينفذ بروتوكول (DNS) لترجمة أسماء النطاقات التي يمكن قراءتها بواسطة الإنسان إلى عناوين IP والعكس.

البت Bit

الوحدة الأساسية للمعلومات الرقمية ولبنة البناء الأساسية لجميع البيانات الرقمية. يمكن للبت أن يتواجد الحالتين،0 أو 1، مما يمثل الطبيعة الثنائية للاتصالات الرقمية.

البيانات الضخمة Big data

الحجم الهائل والتنوع والسرعة للمعلومات التي يتم إنشاؤها وجمعها ومعالجتها داخل البنية التحتية الأمنية. تتضمن مجموعة البيانات الواسعة والمعقدة هذه السجلات والأحداث والمعلومات الأخرى المتعلقة بالأمان من مصادر متنوعة مثل أجهزة الشبكة والتطبيقات وأنشطة المستخدم.

الفريق الازرق Blue Team

مجموعة أو فريق من المتخصصين والخبراء في مجال الأمن المسؤولين عن الدفاع عن أنظمة وشبكات تكنولوجيا المعلومات الخاصة بالمؤسسة وحمايتها. يعمل الفريق الأزرق بشكل استباقي لتنفيذ الحلول الأمنية، واكتشاف الحوادث والاستجابة لها، وضمان المرونة الشاملة للبنية التحتية للمنظمة.

القبعة السوداء Black hat

الاشخاص أو المجموعات الذين ينخرطون في أنشطة خبيثة بقصد استغلال نقاط الضعف وتعريض أنظمة الكمبيوتر للخطر وتجاوز آليات الأمان لتحقيق مكاسب شخصية أو دوافع مالية أو أغراض ضارة أخرى.

معنى Brushing

ممارسة خادعة حيث يرسل البائعون عبر الإنترنت منتجات غير مرغوب فيها إلى الأفراد دون علمهم أو موافقتهم، وغالبًا ما تكون مصحوبة بمراجعات مزيفة. الدافع الأساسي وراءه هو التلاعب بالتقييمات والمراجعات عبر الإنترنت من خلال خلق مظهر العملاء المنبهرين بالخدمة.

بروتوكول البوابة الحديدية Border Gateway Protocol - BGP

بروتوكول بوابة خارجية يستخدم في مجال الشبكات والأمن السيبراني لتسهيل تبادل المعلومات وإمكانية الوصول بين الأنظمة المستقلة المختلفة على الإنترنت.

الجسر Bridge

جهاز يربط ويدير الاتصال بين قسمين أو أكثر من قطاعات الشبكة، ويعمل في طبقة ارتباط البيانات لنموذج الشبكات OSI.

البث Broadcast

نقل البيانات من مصدر واحد إلى جميع الأجهزة داخل شبكة أو شبكة فرعية معينة.

برنامج Burp Suite

منصة متكاملة لاختبار أمان تطبيقات الويب. وهو يوفر مجموعة شاملة من الأدوات لإجراء تقييمات الأمان وتحديد نقاط الضعف في تطبيقات الويب.

عنوان البث Broadcast Address

معرف محدد داخل الشبكة يحدد الإرسال الذي سيتم استقباله بواسطة جميع الأجهزة داخل تلك الشبكة.

ثغرة Buffer Overflow

ثغرة أمنية تحدث عندما يحاول برنامج أو عملية تخزين المزيد من البيانات في مخزن مؤقت، أو منطقة تخزين بيانات مؤقتة، أكثر مما تم تخصيصه للاحتفاظ به. يمكن أن يؤدي هذا التدفق الزائد للبيانات إلى تلف مواقع الذاكرة المجاورة، مما قد يتسبب في تصرف البرنامج بشكل غير متوقع أو السماح بالهجوم.

خطة استمرارية العمل Business Continuity Plan - BCP

استراتيجية شاملة مصممة من قبل المؤسسات لضمان التشغيل المستمر لوظائف العمل الحيوية في مواجهة الأحداث أو الكوارث المعطلة.

تحليل تأثير الاعمال Business Impact Analysis - BIA

عملية منهجية لتقييم وقياس التأثير المحتمل الذي قد تحدثه الاضطرابات أو الكوارث على العمليات التجارية للمؤسسة.

بروتوكول الحدود Border Gateway Protocol - BGP

بروتوكول الحدود BGP يساعد أجزاء مختلفة من الإنترنت على التواصل مع بعضها البعض ومعرفة أفضل المسارات لنقل البيانات من مكان إلى آخر. يتم استخدام BGP بواسطة أجهزة الشبكة لمشاركة المعلومات حول أفضل الطرق، مما يضمن وصول اتصالك عبر الإنترنت إلى وجهته بكفاءة.

القياسات البيومترية Biometrics

التحليل الإحصائي للخصائص الجسدية والسلوكية الفريدة للأشخاص. يمكن أن تشمل هذه الخصائص بصمات الأصابع، وملامح الوجه، وأنماط القزحية أو شبكية العين، والصوت، وحتى طريقة الكتابة. تُستخدم تقنية القياسات البيومترية للتحقق من الهوية والمصادقة عليها، والاستفادة من السمات المميزة والقابلة للقياس للناس لمنح الوصول إلى الأنظمة أو الأجهزة أو المواقع الآمنة. يتم استخدامه بشكل شائع في أنظمة الأمان والأجهزة المحمولة وآليات التحكم في الوصول، مما يوفر بديلاً أكثر أمانًا وملاءمة لطرق المصادقة التقليدية مثل كلمات المرور أو أرقام التعريف الشخصية.

البايوس BIOS

اختصار لعبارة "نظام الإدخال/الإخراج الأساسي". وهي عبارة عن برامج ثابتة مضمنة للكمبيوتر والتي توفر الإرشادات الأساسية والتحكم اللازم للنظام لتشغيل مكونات الأجهزة وتهيئتها. يعد البايوس مسؤولاً عن مهام مثل بدء تشغيل أجهزة الكمبيوتر وتحميل نظام التشغيل إلى ذاكرة الكمبيوتر.

البلوتوث Bluetooth

تقنية اتصالات لاسلكية تتيح تبادل البيانات بين الأجهزة عبر مسافات قصيرة. يتم استخدامه بشكل شائع لتوصيل أجهزة مثل الهواتف الذكية والأجهزة اللوحية وأجهزة الكمبيوتر والسماعات والأجهزة الأخرى دون الحاجة إلى كابلات . تستخدم تقنية بلوتوث موجات الراديو لإنشاء اتصال آمن قصير المدى، مما يسمح للأجهزة بالتواصل ومشاركة المعلومات بسلاسة.

بوت نت Botnet

شبكة من أجهزة الكمبيوتر المخترقة، والتي يشار إليها غالبًا باسم "الروبوتات" أو "الزومبي"، والتي تخضع لسيطرة كيان واحد، يُعرف باسم بوت ماستر "botmaster". عادةً ما تكون أجهزة الكمبيوتر المخترقة هذه مصابة بالفيروسات، غالبًا دون علم أصحابها. يمكن للبوت ماستر التحكم عن بعد في أنشطة أجهزة الكمبيوتر المصابة وتنسيقها لأغراض خبيثة مختلفة، مثل شن هجمات حجب الخدمة (DDoS)، أو نشر الفيروسات، أو سرقة المعلومات الهامة.

الانتهاك Breach

الوصول غير المرغوب فيه إلى نظام الكمبيوتر أو الشبكة أو البيانات. ويحدث ذلك عندما يتمكن شخص، غالبًا ما يكون مدفوع لاغراض خبيثة، من الدخول إلى بيئة آمنة دون الحصول على اذن. يمكن أن يؤدي الانتهاك إلى كشف المعلومات الحساسة أو سرقتها أو اختراقها، بما في ذلك البيانات الشخصية أو

السجلات المالية أو الملكية الفكرية. تهدف المنظمات الى منع الانتهاكات من خلال حلول أمنية قوية، مثل جدران الحماية والتشفير وضوابط الوصول.

المتصفح Browser

تطبيق يسمح للمستخدمين بالوصول إلى شبكة الويب والتنقل فيها. ويعرض محتوى الويب، بما في ذلك النصوص والصور ومقاطع الفيديو والوسائط المتعددة الأخرى، عن طريق جلب صفحات الويب وعرضها. امثلة على متصفحات الويب الشهيرة جوجل كروم وفايرفوكس.

هجوم Brute Force

أسلوب للأمن السيبراني يقوم من خلاله المهاجم بتجريب جميع الانواع الممكنة من كلمات المرور أو مفاتيح التشفير بشكل منظم حتى يتم العثور على الكلمة الصحيحة. تُستخدم هذه الطريقة غالبًا للوصول غير المصرح به إلى حسابات المستخدمين أو الأنظمة أو البيانات المشفرة. يستغرق الهجوم وقتًا طويلاً والكثير من الموارد، لانه تنطوي على محاولة عدد كبير من الكلمات.

البيانات المجمعة Bulk Data

بيانات تحتوي على حجم كبير من المعلومات أو البيانات التي تتم معالجتها أو تخزينها أو نقلها بشكل جماعي. غالبًا ما يستخدم هذا المصطلح في سياق إدارة البيانات والتحليلات والتخزين. قد تشمل البيانات أنواعًا مختلفة من المعلومات، بما في ذلك النصوص أو الأرقام أو الصور أو أي محتوى اخر، ويتم التعامل معها عادةً على دفعات أو بكميات كبيرة.

مفهوم BYOD

يعني BYOD اختصار لعبارة Bring Your Own Device او "اجلب جهازك الخاص"، ويشير إلى سياسة أو ممارسة يستخدم فيها الموظفون أجهزتهم الشخصية، مثل الهواتف الذكية أو الأجهزة اللوحية أو أجهزة الكمبيوتر ، للمهام المتعلقة بالعمل داخل المؤسسة. يسمح هذا المنهج للاشخاص باستخدام الأجهزة التي يشعرون بالارتياح تجاهها ويقلل من حاجة أصحاب العمل إلى توفير أجهزة مخصصة.

C

شهادة Certificate

اعتراف يُمنح للاشخاص الذين اكملوا بنجاح كورس تدريبي محدد في مجال الأمن السيبراني. وهي بمثابة دليل على أن حامل الشهادة يمتلك المعرفة والمهارات في مختلف جوانب الأمن السيبراني، مثل تأمين الشبكات، أو إدارة المخاطر، أو استخدام أدوات محددة للأمن السيبراني. غالبًا ما يتم إصدار هذه الشهادات من قبل المؤسسات التعليمية أو منظمات التدريب أو هيئات إصدار الشهادات المعترف بها في المجال.

شات Chat GPT

نموذج ذكاء صناعي متقدم تم إنشاؤه بواسطة شركة OpenAI. مصمم لفهم وإنشاء نص يشبه الإنسان بناءً على المدخلات التي يتلقاها.يستطيع شات GPT المشاركة في المحادثات والإجابة على الأسئلة وتقديم معلومات حول مجموعة واسعة من المواضيع.

الخدمة السحابية Cloud

شبكة من الخوادم البعيدة المتصلة عبر الإنترنت والتي تقوم بتخزين البيانات وإدارتها وتشغيل التطبيقات وتقديم خدمات متنوعة. فبدلاً من الاعتماد على الخوادم المحلية أو أجهزة الكمبيوتر الشخصية، يمكن للمستخدمين الوصول إلى موارد الكومبيوتر مثل التخزين والمعالجة وتطبيقات البرامج عبر الانترنت. فيوفر المرونة وقابلية التوسع ، مما يسمح للاشخاص والمؤسسات بتخزين المعلومات والوصول إليها وتشغيل التطبيقات والتعاون عبر الإنترنت دون الحاجة إلى اجهزة تخزين واسعة . أصبحت الخدمات السحابية جزءًا لا يتجزأ من تقنية المعلومات الحديثة.

نظام ادارة المحتوى Content management system - CMS

أداة تعمل على تبسيط إنشاء المحتوى الرقمي وتنظيمه ونشره على مواقع الويب. يوفر واجهة سهلة الاستخدام ، حتى بدون مهارات تقنية متقدمة، لإدارة النصوص والصور ومقاطع الفيديو لموقع الويب. باستخدام نظام إدارة المحتوى (CMS)، يمكن للمستخدمين تحديث المحتوى وتحريره وتنظيمه بسهولة، مما يجعل صيانة موقع الويب أكثر كفاءة. تشمل منصات CMS الشائعة وورد بريس وجوملا .

ادارة التكوينات Configuration Management

إدارة وتنظيم العناصر المختلفة للنظام أو البرنامج بشكل منهجي لضمان التنسيق والموثوقية والفعالية. ويتضمن تتبع التغييرات التي تطرأ على الأجهزة والبرامج والوثائق والمكونات الأخرى والتحكم فيها طوال دورة حياة النظام. الهدف هو الحفاظ على بيئة مستقرة ويمكن التنبؤ بها من خلال تسجيل عناصر التكوينات وإدارتها، وفرض السياسات والمعايير، وتسهيل الوصول للتحديثات أو التعديلات.

سلسلة الادلة Chain of Evidence

التوثيق الدقيق والحفاظ على التسلسل الزمني للأحداث والأنشطة المتعلقة بحادث أمني أو قضية قانونية. تعتبر هذه السلسلة ضرورية للحفاظ على سلامة ومقبولية الأدلة الرقمية في المحكمة.

الاستجابة للتحدي Challenge-Response

آلية تستخدم للتحقق من هوية المستخدمين أو الكيانات من خلال طرح تحدي، عادة في شكل طلب أو سؤال، ويتطلب استجابة محددة للتحقق. تضيف هذه الطريقة طبقة إضافية من الأمان من خلال التأكد من أن الكيان الذي يحاول الوصول يمتلك بيانات الاعتماد أو المعرفة اللازمة للاستجابة بشكل صحيح.

الرئيس التنفيذي للمعلومات Chief Information Officer - CIO

مسؤول عن الإشراف على إستراتيجية وسياسات وأنظمة تكنولوجيا المعلومات (IT) الخاصة بالمؤسسة. يلعب مدير تكنولوجيا المعلومات دور مهم في ضمان سرية وسلامة وتوافر الأصول الرقمية للمؤسسة.

الرئيس التنفيذي لأمن المعلومات Chief Information Security Officer

مدير تنفيذي رفيع المستوى مسؤول عن إنشاء وصيانة استراتيجية وسياسات أمن المعلومات في المنظمة. يعد CISO قائدًا رئيسيًا مكرسًا لحماية سرية الأصول الرقمية وسلامتها وتوافرها. يتضمن هذا الدور الإشراف على تنفيذ الحلول الأمن القوية، وإدارة الحوادث الأمنية، وضمان الامتثال للوائح ومعايير الصناعة.

الرئيس التنفيذي للتكنلوجيا Chief Technology Officer - CTO

أحد كبار المسؤولين التنفيذيين المسؤول عن قيادة استراتيجية التكنولوجيا ومبادرات الابتكار في المنظمة. دور CTO في مواءمة التقدم التكنولوجي مع الحلول الأمنية لضمان مرونة الأنظمة الرقمية.

قواعد السلوك Code of Conduct - CoC

مجموعة من المبادئ التوجيهية الأخلاقية والمعايير السلوكية المحددة مسبقًا والتي من المتوقع أن يلتزم بها الأفراد أو الكيانات داخل مجتمع أو منظمة معينة. تحدد هذه المدونة السلوك المقبول وغير المقبول، مع التركيز على مبادئ مثل النزاهة والاحترام والمسؤولية.

هندسة الفوضى Chaos engineering

مجال ضمن مجال الأمن يتضمن الإدخال المتعمد الأخطاء أو الظروف غير المتوقعة في نظام برمجي أو شبكة لتقييم مرونتها وتحديد نقاط الضعف المحتملة.

التصيد بالاستنساخ Clone phishing

أسلوب هجوم إلكتروني يقوم من خلاله المهاجم بإنشاء نسخة متماثلة تقريبًا أو "مستنسخة" من بريد إلكتروني أو موقع ويب أو وسيلة اتصال حقيقية لخداع المستلمين لإفشاء معلومات حساسة أو اتخاذ إجراءات ضارة.

قواعد الاخلاق Code of Ethics

مجموعة من المبادئ والمعايير التي تحدد السلوك المقبول والمسؤول للأفراد أو المنظمات في هذا المجال. تضع هذه المدونة إطارًا للسلوك الأخلاقي، مع التركيز على قيم مثل النزاهة والسرية واحترام الخصوصية.

تشويش الكود Code obfuscation

أسلوب أمني يستخدم لإخفاء أو جعل كود المصدر أكثر صعوبة في الفهم، أو إجراء هندسة عكسية، أو تحليله. تتضمن العملية تطبيق تحويلات على الاكواد البرمجية دون تغيير وظائفها، بهدف إحباط محاولات الخصوم للحصول على رؤى حول منطق البرنامج أو تصميمه.

التشفير السحابي Cloud encryption

ممارسة تأمين البيانات المخزنة في البيئات السحابية عن طريق تحويلها إلى تنسيق محمي وغير قابل للقراءة باستخدام خوارزميات التشفير.

الاستخابات السحابية Cloud intelligence

استخدام التحليلات المتقدمة والتعلم الآلي والرؤى المستندة إلى البيانات داخل بيئات الحوسبة السحابية لتعزيز الأمان والأداء والكفاءة.

التعهد الجماعي Crowdsourcing

ممارسة الذكاء الجماعي والمهارات والمساهمات لمجموعة كبيرة ومتنوعة من الاشخاص لمواجهة تحديات أو مهام أمنية محددة.

هجوم الاقلاع البارد Cold Boot Attack

نوع من الهجوم الأمني حيث يحصل المهاجم على وصول غير مصرح إلى المعلومات الحساسة المخزنة في ذاكرة الوصول العشوائي للكمبيوتر (RAM) عن طريق الوصول فعليًا إلى الجهاز واسترداد البيانات حتى بعد إيقاف تشغيل النظام.

خادم القيادة والتحكم Command and control server - C2

مكون اساسي في البنية التحتية للهجمات الإلكترونية، حيث يعمل بمثابة النقطة المركزية التي من خلالها يقوم المهاجم بإدارة الأجهزة أو الشبكات المخترقة والتحكم فيها عن بعد.

نقاط الضعف الشائعة Common Vulnerabilities and Exposures - CVE

نظام موحد لتحديد وتسمية نقاط الضعف المعروفة في أنظمة البرامج والأجهزة بشكل فريد.

نقاط تسجيل الثغرات الشائعة Common Vulnerability Scoring System

إطار موحد يستخدم في مجال الأمن السيبراني لتقييم وقياس مدى خطورة نقاط الضعف في البرامج أو الأنظمة. يوفر نظام CVSS منهج منظم ومتسق لتقييم التأثير المحتمل للعيوب الأمنية من خلال تعيين درجات بناءً على عوامل مثل قابلية الاستغلال، والتأثير على السرية، والنزاهة، والتوفر، بالإضافة إلى مدى تعقيد الهجوم.

بيانات الاعتماد Credentials

عبارة عن أجزاء من المعلومات، تستخدم لإثبات الهوية والوصول إلى الأنظمة أو الحسابات أو الخدمات. تعمل هذه المفاتيح الرقمية كآليات مصادقة، للتحقق من أن الشخص الذي يطلب الوصول هو المستخدم الشرعي. تلعب بيانات الاعتماد دورًا أساسيًا في تأمين مختلف المنصات عبر الإنترنت، مثل حسابات البريد الإلكتروني ووسائل التواصل الاجتماعي والخدمات المصرفية عبر الإنترنت. من الضروري للأفراد حماية بيانات الاعتماد الخاصة بهم لمنع الوصول وحماية هوياتهم الرقمية والمعلومات الحساسة من التهديدات الأمنية المحتملة.

حشو بيانات الاعتماد Credential stuffing

هو هجوم للأمن السيبراني حيث يستخدم الهاكرز أدوات آلية لاختبار كميات كبيرة من مجموعات البريد الالكتروني وكلمة المرور بشكل منظم، والتي تم الحصول عليها من خروقات سابقة لمنصات مختلفة عبر الإنترنت. الهدف هو استغلال الاشخاالذين يعيدون استخدام نفس بيانات الاعتماد عبر حسابات متعددة. في حالة نجاح الهجوم، يحصل المهاجمون على وصول إلى حسابات المستخدمين، مما يشكل مخاطر على المعلومات الشخصية أو البيانات المالية أو الخدمات الحساسة عبر الإنترنت.

البنية الوطنية الحيوية Critical National Infrastructure - CNI

الأنظمة والأصول المادية والافتراضية الأساسية التي تعتبر حيوية لعمل الدولة وأمنها ورفاهيتها الاقتصادية. وتشمل هذه قطاعات مثل الطاقة والنقل وإمدادات المياه والرعاية الصحية والاتصالات وغيرها.

التشفير Cryptography

يعتبر كالرمز السري للحفاظ على أمان المعلومات. يتضمن تقنيات لتحويل البيانات العادية القابلة للقراءة إلى تنسيق سري مشفر لا يمكن فهمه إلا من قبل أولئك الذين لديهم المفتاح الصحيح لفك تشفيره. تساعد هذه العملية على ضمان سرية المعلومات وسلامتها وصحتها، خاصة في مجال الاتصالات الرقمية وتخزين البيانات. يُستخدم التشفير على نطاق واسع في التقنيات اليومية، مثل تأمين المعاملات عبر الإنترنت، وحماية البيانات الحساسة، والحفاظ على خصوصية الاتصالات.

فرق CSIRT

هي فرق من الخبراء الذين يأتون للإنقاذ عند وقوع حادث أمني، مثل هجوم إلكتروني أو اختراق للبيانات. يحققون في هذه الحوادث ويحللونها ويستجيبون لها، ويعملون على تقليل الأضرار واستعادة الأنظمة المخترقة ومنع الهجمات المستقبلية.

مسابقات التقاط العلم Capture The Flag - CTF

مسابقة للأمن السيبراني يتحدى المشاركين لحل سلسلة من الألغاز أو المهام أو التحديات المتعلقة بالأمن داخل بيئة خاضعة للرقابة. تشمل هذه التحديات مجالات مختلفة، بما في ذلك التشفير والهندسة العكسية وأمن الويب والشبكات.

اطار التقييم السيبراني Cyber Assessment Framework - CAF

قائمة مرجعية تساعد المؤسسات على تقييم أمنها السيبراني وتحسينه. يحدد نهجًا منظمًا لتقييم قدرات المنظمة ونقاط الضعف فيها، ويغطي مجالات مثل إدارة المخاطر والسياسات الأمنية والاستجابة للحوادث. باستخدام CAF، يمكن للمؤسسات تحديد نقاط القوة والضعف في وضع الأمن السيبراني الخاص بها، مما يسهل تنفيذ تدابير الحماية من التهديدات السيبرانية المحتملة وتعزيز المرونة الشاملة.

النقر الاحتيالي Click fraud

إنشاء نقرات احتيالية على الإعلانات عبر الإنترنت بقصد تضخيم تكاليف الإعلان بشكل مصطنع أو التلاعب بمقاييس الأداء. غالبًا ما يستخدم المهاجمين ادوات اوتماتيكية أو شبكات من الأجهزة المخترقة للنقر على الإعلانات دون اهتمام حقيقي من المستخدم.

الهجوم السيبراني Cyber Attack

هجوم رقمي على أجهزة الكمبيوتر أو الشبكات أو الأنظمة بهدف التسبب في ضرر أو سرقة المعلومات أو تعطيل العمليات الروتينية. يتضمن الوصول للبيانات أو التلاعب بها أو تدميرها باستخدام طرق مختلفة مثل البرامج الضارة أو التصيد أو استغلال نقاط الضعف في البرامج. يمكن أن تستهدف الهجمات السيبرانية أفرادًا أو مؤسسات أو حتى دولًا بأكملها، مما يشكل مخاطر على المعلومات الشخصية والأصول المالية والبنية التحتية الحيوية.

الاساسيات السيبرانية Cyber Essentials

اطار اساسي وفعال لتعزيز الأمن السيبراني. يساعد الشركات على تنفيذ الحلول الأمنية الأساسية للحماية من التهديدات الشائعة عبر الإنترنت. من خلال الحصول على شهادة Cyber Essentials، تثبت المؤسسات التزامها بحماية أنظمتها وبياناتها. يركز البرنامج على الممارسات الأمنية الأساسية، مثل التكوين الآمن والتحكم في الوصول والحماية من البرامج الضارة، مما يجعله في متناول الشركات من جميع الأحجام.

التجسس السيبراني Cyber espionage

شكل من أشكال جمع المعلومات الاستخبارية السرية التي يتم إجراؤها من خلال استخدام الأدوات والتقنيات الرقمية. وهو ينطوي على الوصول غير المصرح إلى المعلومات الحساسة وجمعها وتسريبها من الأفراد أو المنظمات أو الحكومات المستهدفة بهدف الحصول على معلومات استخباراتية استراتيجية أو سياسية أو اقتصادية أو عسكرية.

المصدر المغلق Closed Source

برامج الكمبيوتر أو التطبيقات التي لا يتوفر كود مصدرها للمستخدمين. كود المصدر، وهو الكود الذي يمكن قراءته من البرنامج ، يظل سريًا من قبل مطوري البرنامج أو البائعين.

حقن الاوامر Command Injection

ثغرة أمنية تحدث عندما يتمكن المهاجم من التعامل مع الأوامر التي ينفذها أحد التطبيقات البرمجية.

التكريك Cracking

محاولة لكسر الحلول الأمنية المطبقة في البرامج أو الأنظمة أو الشبكات. غالبًا ما يرتبط هذا المصطلح بعملية تجاوز حماية كلمة المرور أو التشفير للوصول إلى الموارد الرقمية.

الامن السيبراني Cyber Security

يتضمن استراتيجيات وحلول لحماية أجهزة الكمبيوتر والشبكات والبيانات من الوصول غير المصرح به والهجمات والأضرار.يعد بمثابة درع ضد التهديدات السيبرانية مثل الهاكرز والفيروسات والأنشطة الضارة الأخرى التي يمكن أن تضر معلوماتنا وتعطل حياتنا الرقمية. من خلال تنفيذ ممارسات الأمن السيبراني، مثل استخدام كلمات مرور قوية، وتحديث البرامج، وتوظيف جدران الحماية، يضمن الأفراد والمنظمات سلامة وسلامة أصولهم الرقمية، مما يساهم في خلق بيئة آمنة وجديرة بالثقة عبر الإنترنت.

الاستراتيجية السيبرانية Cyber Strategy

خطة تم إعدادها بعناية تحدد كيف يريد الاشخاص أو الشركات أو المؤسسات الدفاع ضد التهديدات السيبرانية والرد عليها. ويتضمن تحديد الأهداف وتقييم المخاطر وتنفيذ الحلول لحماية الأصول والبيانات والأنظمة الرقمية. تأخذ الإستراتيجية الإلكترونية القوية في الاعتبار نقاط الضعف المحتملة، وتتضمن أفضل الممارسات الأمنية، وغالبًا ما تتضمن خطط الاستجابة للحوادث لتقليل تأثير الحوادث الإلكترونية المحتملة. سواء بالنسبة لفرد أو شركة كبيرة، تساعد الإستراتيجية السيبرانية المحددة جيدًا على التنقل في المشهد المعقد للأمن السيبراني، مما يضمن اتباع نهج استباقي وفعال للدفاع الرقمي.

التهديد السيبراني Cyber Threat

خطر محتمل في العالم الرقمي، يهدف إلى استغلال نقاط الضعف وإلحاق الضرر بأجهزة الكمبيوتر أو الشبكات أو البيانات. يشمل مخاطر مختلفة، بما في ذلك البرامج الضارة وهجمات التصيد والأنشطة الضارة الأخرى التي يمكن أن تعرض أمن وسلامة الأنظمة الرقمية للخطر.

البرمجة العابرة للمواقع Cross-site scripting - XSS

نوع من ثغرات الأمن الموجودة بشكل شائع في تطبيقات الويب، حيث يقوم المهاجمون بإدخال اكواد برمجية ضارة في صفحات الويب التي يشاهدها المستخدمون . يحدث هذا عندما يسمح تطبيق الويب بتضمين مدخلات المستخدم غير الموثوق بها في صفحات الويب دون التحقق من صحتها منها. يتم بعد ذلك تنفيذ الكود الذي تم إدخاله في متصفح الضحية، مما يؤدي إلى الوصول أو سرقة البيانات، أو أنشطة ضارة أخرى.

الذاكرة المؤقتة Cache

نوع عالي السرعة ومتقلب من ذاكرة الكمبيوتر التي تخزن بشكل مؤقت البيانات أو التعليمات التي يتم الوصول إليها بشكل متكرر، مما يسمح باسترجاع أسرع وتحسين أداء النظام.

حشو الذاكرة المؤقتة Cache cramming

أسلوب هجوم معقد حيث يتلاعب المهاجم بالذاكرة المؤقتة للنظام لتخزين تعليمات برمجية أو بيانات ضارة. تستغل هذه التقنية نقاط الضعف في آليات التخزين المؤقت لنظام الكمبيوتر، بهدف إغراق الذاكرة بمحتوى ملغوم يتجاوز قدرتها . ومن خلال القيام بذلك، يسعى المهاجم إلى إجبار النظام على تنفيذ أو معالجة البيانات التي تم التلاعب بها، مما يؤدي إلى انتهاكات أمنية محتملة.

تسميم الذاكرة المؤقتة Cache Poisoning

هجوم حيث يقوم المهاجم بإدراج بيانات خاطئة أو مضللة في ذاكرة التخزين المؤقت. يهدف هذا النوع من الهجمات إلى تعريض سلامة المعلومات المخزنة مؤقتًا للخطر، مما يؤدي إلى ثغرات أمنية محتملة.

التحكم في قبول المكالمات Call admission control - CAC

إجراء لإدارة الشبكة وأمنها مصمم لتنظيم جلسات اتصال جديدة داخل بيئة الاتصالات أو VoIP (بروتوكول نقل الصوت عبر الإنترنت).

المصادقة ذات الشهادة Certificate-Based Authentication

طريقة للتحقق من هوية مستخدم أو جهاز أو خدمة، باستخدام الشهادات الرقمية. تعتمد آلية المصادقة هذه على تبادل شهادات التشفير والتحقق من صحتها، عادةً ضمن البنية التحتية للمفتاح العام (PKI). يمتلك كل كيان شهادة رقمية فريدة تحتوي على مفتاح عام ومعلومات أخرى ذات صلة، موقعة من هيئة تصديق موثوقة (CA).

واجهة البوابة العامة Common Gateway Interface

بروتوكول يمكن التفاعل بين خوادم الويب والبرامج الخارجية. تسهل الاتصال بين خادم الويب والتطبيقات، وغالبًا ما تكون مكتوبة بلغات مثل بيرل أو بايثون.

المجموع الاختباري Checksum

قيمة يتم حسابها من البيانات لاكتشاف الأخطاء أو التلاعب أثناء النقل أو التخزين. وهي خوارزمية رياضية تولد قيمة ذات حجم ثابت بناءً على محتوى البيانات. عند إرسال البيانات أو تخزينها، يتم حساب المجموع عند طرفي المرسل والمستقبل. عند استلام البيانات، يقوم المستلم بإعادة حساب المجموع ومقارنته بالمجموع الاصلي. إذا تطابقت القيم، فهذا يشير إلى أنه من المحتمل أن يتم إرسال البيانات دون أخطاء أو تلاعب. ومع ذلك، إذا كان هناك تناقض، فهذا يشير إلى مشكلات محتملة، مثل تلف البيانات أو التداخل .

سايفر Cipher

طريقة تستخدم لتشفير المعلومات لتأمينها من الوصول أو الاعتراض. تحول النص العادي إلى نص مشفر من خلال سلسلة من الخطوات المحددة جيدًا والقابلة للتكرار.

نص سايفر Ciphertext

المخرجات المشفرة للبيانات الطبيعية التي خضعت لعملية تحويل تشفير باستخدام خوارزمية ومفتاح محددين. وهو الشكل الأصلي للبيانات الذي يمكن قراءته، يظهر النص المشفر كتسلسل مشوش وغير مفهوم من الأحرف. الغرض الأساسي من إنشاء النص المشفر هو حماية سرية وسلامة المعلومات الحساسة أثناء النقل أو التخزين.

شبكة Circuit Switched Network

شبكة اتصالات حيث يتم إنشاء مسار أو دائرة اتصال مخصصة وحجزها لمدة المحادثة أو الجلسة.

التصادم Collision

الحالة التي تتقاطع فيها حزمتان أو أكثر من حزم البيانات أو الإشارات، مما يؤدي إلى فقدان محتمل لسلامة المعلومات أو انقطاع في الاتصال.

الاستخبارات التنافسية Competitive Intelligence

جمع وتحليل وتفسير المعلومات حول المنافسين واتجاهات السوق والصناعة بشكل منظم للحصول على ميزة استراتيجية في الأعمال التجارية.

فريق الاستجابة لطؤارئ الكومبيوتر Computer Emergency Response Team CERT

مجموعة متخصصة مسؤولة عن الاستجابة لحوادث وطوارئ الأمن السيبراني والتخفيف من آثارها.

فريق الاستجابة لحوادث الكومبيوتر Computer Incident Response Team CIRT

مجموعة متخصصة من المهنيين داخل منظمة مسؤولة عن إدارة حوادث الأمن السيبراني والاستجابة لها. يُعرف أيضًا باسم فريق الاستجابة للحوادث (IRT) أو فريق الاستجابة لحوادث أمن الكمبيوتر (CSIRT)، ويتولى فريق CIRT مهمة اكتشاف الحوادث الأمنية وتحليلها والتخفيف من آثارها بسرعة لتقليل التأثير على الأصول والمعلومات الرقمية للمؤسسة.

تضارب المصالح Conflict of Interest

الموقف الذي يواجه فيه الفرد أو الكيان مصالح متنافسة يمكن أن تؤثر على موضوعيته أو حكمه المهني أو عمليات صنع القرار في المسائل المتعلقة بالأمن. ينشأ هذا الصراع عندما تتداخل الاعتبارات الشخصية أو المالية أو غيرها من الاعتبارات الخارجية مع القدرة على إعطاء الأولوية للمصالح الفضلى للمنظمة أو أصحاب العمل.

السرية Confidentiality

مبدأ وممارسة حماية المعلومات الحساسة من الوصول غير المصرح به أو الكشف عنها . يعد أحد الجوانب الأساسية لأمن المعلومات هو التأكد من أن الأفراد أو الأنظمة أو العمليات المصرح لهم فقط هم من يمكنهم الوصول إلى البيانات السرية أو الخاصة.

ملفات تعريف الارتباط Cookie

جزء صغير من البيانات المخزنة على جهاز المستخدم بواسطة متصفح الويب، وغالبًا ما يحتوي على معلومات حول نشاط التصفح الخاص بالمستخدم أو تفضيلاته أو تفاصيله.

الاجراءات المضادة Countermeasure

عملية أو تقنية استباقية يتم تنفيذها لاكتشاف التهديدات الأمنية أو نقاط الضعف المحتملة أو منعها أو تخفيفها. تعتبر الإجراءات المضادة مكونات أساسية لاستراتيجية أمنية شاملة، تهدف إلى حماية أنظمة المعلومات والشبكات والأصول من الوصول والاضطرابات.

سلسلة القتل السيبراني Cyber Kill Chain

مفهوم يستخدم لوصف مراحل الهجوم السيبراني بدءًا من الاستطلاع وحتى تحقيق أهداف المهاجم. يقوم النموذج بتقسيم دورة حياة الهجوم إلى مراحل ، بما في ذلك الاستطلاع، والتسليح، والتسليم، والاستغلال، والتثبيت، والقيادة والسيطرة، والتنفيذ. من خلال فهم وتحليل كل مرحلة، يمكن لمحترفي الأمن تطوير استراتيجيات استباقية لاكتشاف التهديدات السيبرانية ومنعها والاستجابة لها .

القنوات المخفية Covert Channels

قنوات الاتصال غير المرخصة والمخفية التي تم إنشاؤها داخل نظام كمبيوتر أو شبكة، مما يسمح بنقل المعلومات بطريقة تتحايل على الضوابط الأمنية. تستغل هذه القنوات موارد النظام أو البروتوكولات المختلفة لنقل البيانات بشكل خفي، وغالبًا ما تتجنب اكتشافها بواسطة آليات الأمان التقليدية.

برامج الجريمة Crimeware

البرامج الضارة المصممة والمنتشرة خصيصًا بهدف تسهيل الأنشطة الإجرامية. على عكس البرامج الضارة التقليدية، التي قد يكون لها مجموعة متنوعة من الأغراض، يتم إنشاء البرامج الإجرامية بشكل صريح لتمكين مجرمي الإنترنت من القيام بأنشطة مثل الاحتيال أو سرقة الهوية أو السرقة المالية أو غيرها من العمليات الخبيثة.

تحليل الشفرات Cryptanalysis

علم وفن تحليل أنظمة التشفير بهدف فهم آليات الأمان الخاصة بها أو استغلالها أو كسرها.

الفحص الدوري للتكرار Cyclic Redundancy Check - CRC

نوع من أكواد التحقق من الأخطاء المستخدمة لاكتشاف الأخطاء أو التغييرات في البيانات أثناء النقل.

D

البيانات الخاملة Data At Rest

المعلومات المخزنة والتي لا يتم استخدامها أو نقلها بشكل نشط. يمثل البيانات الثابتة الموجودة على أجهزة التخزين مثل الهارد درايف او USB أنواع أخرى من وسائط التخزين. عندما تكون البيانات في حالة سكون، قد يتم تشفيرها أو حمايتها باستخدام إجراءات أمنية لمنع الوصول غير المصرح به أو التعرض للخطر.

مركز البيانات Data Centre

يعمل كمستودع مركزي مجهز لتخزين ومعالجة وإدارة ونشر كميات كبيرة من البيانات. يضم أنظمة الكمبيوتر والخوادم ومعدات الشبكات وموارد التخزين التي تدعم مختلف عمليات تكنولوجيا المعلومات والعمليات التجارية. يوفر مركز البيانات خدمات الحوسبة واستضافة مواقع الويب وتشغيل التطبيقات وتخزين المعلومات الرقمية للمؤسسات.

البيانات قيد النقل Data In Transit

المعلومات التي تنتقل بشكل نشط من موقع إلى آخر عبر شبكة أو قناة اتصال. أثناء هذا النقل، تكون البيانات في حالة ديناميكية، حيث يتم نقلها بين الأجهزة أو الأنظمة. تتضمن أمثلة البيانات أثناء النقل رسائل البريد الإلكتروني التي يتم إرسالها، والملفات التي يتم تحميلها أو تنزيلها، والمعلومات المتدفقة عبر اتصالات الإنترنت.

الويب المظلم Dark web

جزء من الإنترنت تم إخفاؤه ولا يمكن الوصول إليه من خلال متصفحات الويب خاصة مثل Tor. تعمل شبكة الويب المظلمة على شبكات مشفرة وتتميز بميزات إخفاء الهوية والخصوصية.

هجوم اجتياز الدليل Directory traversal attack

نوع من الهجوم الأمني حيث يتلاعب المهاجم ببيانات الإدخال للوصول إلى الملفات خارج النطاق المقصود لنظام ملفات تطبيق الويب يحدث اجتياز الدليل عندما لا يقوم التطبيق بالتحقق من صحة مدخلات المستخدم أو تعقيمها بشكل صحيح، مما يسمح للمهاجم بالتنقل خارج الدلائل المحددة والحصول على وصول إلى الملفات الحساسة أو موارد النظام.

هجوم حجب الخدمة DDoS

يشير DDoS إلى عبارة "حجب الخدمة الموزعة"، في هجوم DDoS، تقوم أجهزة الكمبيوتر هذه، التي غالبًا ما تشكل شبكة تسمى الروبوتات، بإغراق النظام المستهدف، مثل موقع الويب أو الخدمة عبر الإنترنت، بكمية هائلة من حركة المرور. تم تصميم التدفق الهائل للطلبات لتعطيل الهدف أو تعطيله مؤقتًا، مما يتسبب في رفض الخدمة للمستخدمين الحقيقيين.

فك التشفير Decryption

عملية تحويل البيانات المشفرة مرة أخرى إلى شكلها الأصلي القابل للقراءة. يُستخدم التشفير لتأمين المعلومات الحساسة عن طريق تحويلها إلى تنسيق مشفر، وفك التشفير هو العملية العكسية التي تسمح للمستخدمين أو الأنظمة المصرح لها بالوصول إلى البيانات وفهمها.

الشيطان Daemon

عملية أو خدمة في الخلفية تعمل بشكل مستمر على نظام الكمبيوتر، وتؤدي مهام مختلفة دون تدخل مباشر من المستخدم. تلعب برامج الشيطان دور رئيسي في الحفاظ على وظائف النظام، وتنفيذ العمليات الأساسية في الخلفية، والاستجابة لأحداث أو طلبات محددة.

تجميع البيانات Data aggregation

عملية جمع ودمج وتلخيص مجموعات متنوعة من المعلومات من مصادر مختلفة في مستودع مركزي. يتم استخدام هذه العملية بشكل شائع لأغراض تحليلية، مما يمكّن متخصصي الأمن من الحصول على رؤى شاملة حول الأنماط والاتجاهات والتهديدات المحتملة داخل النظام أو الشبكة.

امين البيانات Data Custodian

فرد مكلف بمسؤولية إدارة وحماية مجموعات محددة من البيانات. يتضمن هذا الدور الإشراف على تخزين المعلومات ومعالجتها وحمايتها وفقًا لسياسات الأمان المعمول بها والمتطلبات التنظيمية.

التحليلات الرقمية Digital forensics

مجال متخصص في الأمن السيبراني يتضمن التحقيق والتحليل والحفاظ على الأدلة الرقمية لكشف وفهم الجرائم الإلكترونية أو الحوادث الأمنية. يستخدم مجموعة من التقنيات والأدوات والمنهجيات لفحص الأجهزة والبيانات الرقمية، مثل أجهزة الكمبيوتر والخوادم والأجهزة المحمولة وحركة مرور الشبكة، لإعادة بناء الأحداث وتحديد نقاط الضعف وإسناد الأنشطة الضارة.

التطوير والعمليات DevOps

نهج متكامل لتطوير البرمجيات وعمليات تكنولوجيا المعلومات التي تركز على الاتصال والأتمتة والمسؤوليات المشتركة.

تصوير القرص Disk Imaging

عملية إنشاء نسخة طبق الأصل دقيقة وكاملة لمحتويات جهاز التخزين بالكامل. هذه النسخة لا تلتقط الملفات والمجلدات فحسب، بل تلتقط أيضًا البنية والأقسام وحتى المساحة غير المستخدمة على القرص.

معيار تشفير البيانات The Data Encryption Standard - DES

خوارزمية معترف بها على نطاق واسع كمعيار تشفير تأسيسي في مجال أمان الكمبيوتر. تم تطوير DES بواسطة IBM في السبعينيات وتم اعتماده لاحقًا كمعيار فدرالي في الولايات المتحدة.

تنقيب البيانات Data mining

عملية استخلاص رؤى وأنماط قيمة من كميات كبيرة من البيانات لتحديد التهديدات الأمنية المحتملة أو الحالات المشبوهة.

مالك البيانات Data Owner

فرد يتحمل المسؤولية النهائية عن مجموعات محددة من البيانات داخل المؤسسة.

تخزين البيانات Data Warehousing

عملية جمع وتخزين وإدارة كميات كبيرة من البيانات المنظمة والبيانات التاريخية من مصادر متنوعة في مستودع واحد مركزي.

مخطط البيانات Datagram

حزمة بيانات مستقلة ومكتفية ذاتيًا يتم إرسالها عبر شبكة، عادةً في بروتوكول اتصال مثل UDP.

عجز الكشف Detection deficit

الحالة التي تفشل فيها الحلول والأنظمة الأمنية في تحديد أو التعرف على الأنشطة الضارة أو التسلل أو الخروقات الأمنية داخل الشبكة أو بيئة الحوسبة.

فك التغليف Decapsulation

عملية فك أو إزالة الطبقات الخارجية للبيانات المغلفة في اتصال الشبكة. تحدث هذه العملية عادةً عند الطرف المتلقي لارتباط الاتصال وتتضمن إزالة رؤوس البروتوكول المختلفة وطبقات التغليف التي تمت إضافتها أثناء نقل البيانات.

التشويه Defacement

التخريب لموقع ويب أو تطبيق أو أصول رقمية، لأغراض خبيثة وضارة. يتضمن هذا النشاط تعديل المظهر أو المحتوى للكيان المستهدف، بهدف نقل رسالة، أو تعطيل العمليات العادية.

الدفاع في العمق Defense In-Depth

استراتيجية للأمن السيبراني تتضمن تنفيذ طبقات متعددة من الحلول الأمنية لحماية أنظمة الكمبيوتر والشبكات والبيانات. ويدرك هذا النهج أن الحل الأمني الوحيد غير كافٍ لمواجهة الطبيعة المتنوعة والمتطورة للتهديدات السيبرانية.

الشهادة الرقمية Digital Certificate

بيانات اعتماد مشفرة تعمل كوسيلة آمنة للتحقق من هوية شخص ما في الاتصالات .

الظرف الرقمي Digital Envelope

مفهوم أمني يستخدم في التشفير لحماية البيانات الحساسة أثناء الإرسال. يتضمن الظرف الرقمي تشفير بيانات النص العادي باستخدام خوارزمية تشفير متماثلة.

التوقيع الرقمي Digital Signature

أسلوب تشفير يستخدم للتحقق من صحة وسلامة الرسائل أو المستندات أو المعاملات الالكترونية. على غرار التوقيع المكتوب بخط اليد في العالم المادي، يعد التوقيع الرقمي معرف فريد مرتبطًا بمرسل الاتصال الالكتروني.

خوارزمية التوقيع الرقمي Digital Signature Algorithm - DSA

خوارزمية تشفير غير متماثلة مصممة لإنشاء التوقيع الرقمي والتحقق منه.

معيار التوقيع الرقمي Digital Signature Standard - DSS

معيار تشفير تم تطويره بواسطة المعهد الوطني للمعايير والتكنولوجيا (NIST) لإنشاء التوقيعات الرقمية والتحقق منها. يعتمد على خوارزمية التوقيع الرقمي، ويحدد استخدام أحجام مفاتيح محددة وخوارزميات التجزئة لضمان الأمان.

التفكيك Disassembly

عملية تحويل الكود القابل للتنفيذ إلى تمثيل لغوي يمكن قراءته بواسطة لغة الانسان الطبيعية. غالبًا ما يستخدم متخصصو الأمن والباحثون التفكيك كأسلوب لتحليل وفهم وظائف البرامج، خاصة في مجال الهندسة العكسية.

خطة التعافي من الكوارث Disaster Recovery Plan - DRP

إطار عمل شامل ومنظم يحدد الإجراءات والاستراتيجيات للمؤسسة لاستعادة العمليات التجارية الهامة وأنظمة تكنولوجيا المعلومات بسرعة وفعالية في أعقاب حدث مدمر.

التحكم التقديري في الوصول Discretionary Access Control - DAC

نموذج أمان يمكّن ملف أو نظام، من التحكم بشكل صريح في من يمكنه الوصول إلى هذا المورد وما هي الإجراءات التي يمكنه تنفيذها.

التعطيل Disruption

التدخل المتعمد أو غير المتعمد في الأداء الطبيعي لأنظمة الكمبيوتر أو الشبكات أو الخدمات الرقمية.

عامل المسافة Distance Vector

خوارزمية تستخدمها أجهزة التوجيه لتحديد المسار الأمثل للوصول إلى الوجهة داخل الشبكة.

المسح الموزع Distributed Scans

أنشطة المسح المنسقة والمتزامنة التي تجريها أجهزة أو أنظمة متعددة متصلة بالشبكة عبر مواقع مختلفة. غالبًا ما يتم استخدام هذه التقنية من قبل المهاجم الذي يسعى إلى تحديد نقاط الضعف في الشبكة أو النظام المستهدف.

اختطاف النطاق Domain Hijacking

الاستيلاء على اسم النطاق المسجل من قبل مهاجم. يتضمن هذا عادةً معالجة إعدادات تسجيل النطاق أو الوصول إلى حساب مسجل النطاق. بمجرد الاستيلاء على السيطرة، يمكن للمهاجم إعادة توجيه النطاق إلى موقع ويب مختلف، أو تعطيل الخدمات ، أو المشاركة في أنشطة التصيد .

اداة DumpSec

أداة تدقيق الأمان المصممة لاسترداد وتقديم معلومات مفصلة حول إعدادات الأمان لنظام ويندوز. تسمح لمتخصصي الأمن بإجراء تقييمات أمنية شاملة عن طريق استخراج البيانات من المكونات المختلفة لنظام الويندوز، بما في ذلك حسابات المستخدمين وأذونات الملفات وإعدادات التسجيل والمزيد.

الغوص في القمامة Dumpster Diving

العملية المتمثلة في البحث في المواد المهملة، مثل المستندات الورقية أو المعدات الإلكترونية، لاستخراج معلومات حساسة أو سرية. غالبًا ما يتم استخدام هذه التقنية من قبل المهاجمين الذين يسعون إلى جمع معلومات استخباراتية حول عمليات المنظمة أو موظفيها أو ممارساتها الأمنية.

مكتبة الارتباط الديناميكي Dynamic Link Library DLL

ملف يحتوي على تعليمات برمجية وبيانات تستخدمها برامج متعددة في وقت واحد. تسمح ملفات DLL لمختلف التطبيقات بمشاركة الموارد، مثل الوظائف أو الإجراءات، دون تكرار التعليمات البرمجية في كل برنامج.

بروتوكول التوجيه الديناميكي Dynamic Routing Protocol

بروتوكول شبكة يمكّن أجهزة التوجيه من تبادل المعلومات تلقائيًا حول هيكل الشبكة والمسارات، مما يسمح بالتكيف الديناميكي مع التغييرات في الشبكة.

قائمة الرفض Deny List

القائمة السوداء الرقمية للعناصر أو الكيانات المحظورة من الوصول إليها أو استخدامها. في الأمن السيبراني، غالبًا ما يتم استخدام قائمة الرفض لتقييد الوصول إلى مواقع ويب معينة أو عناوين IP أو محتوى محدد يعتبر ضارًا أو غير مصرح به.

الويب العميق Deep Web

الإنترنت الذي لم تتم فهرسته بواسطة محركات البحث ولا يمكن لعامة الناس الوصول إليه بسهولة. على عكس الويب السطحي، الذي يتضمن مواقع الويب والمحتوى الذي يمكن العثور عليه بسهولة من خلال محركات البحث، يشتمل الويب العميق على محتوى مخفي عمدًا أو محمي بكلمات مرور أو موجود على شبكات خاصة.

التزييف العميق Deep Fake

شكل متطور من الهجوم القائم على الذكاء الاصطناعي والذي يتضمن إنشاء محتوى مرئي واقعي ومخادع في كثير من الأحيان، مثل مقاطع الفيديو أو التسجيلات الصوتية أو الصور، من خلال استخدام خوارزميات التعلم العميق. تقوم هذه الخوارزميات بتحليل وتجميع البيانات المرئية والسمعية الموجودة لإنشاء محتوى مزيف ومقنع ويتم التلاعب به، وغالبًا ما يظهر اشخاص يقولون أو يفعلون أشياء لم يفعلوها أبدًا.

هجوم القاموس Dictionary Attack

محاولة منظمة لتخمين كلمات المرور من خلال تجربة كلمات من قائمة مجمعة مسبقًا، في هذا النوع من الهجمات السيبرانية، يقوم المهاجم بأتمتة عملية تجربة العديد من كلمات المرور المحتملة، على أمل العثور على الكلمة الصحيحة.

البصمة الرقمية Digital Footprint

تواجد وأنشطة فرد أو مؤسسة على الإنترنت. ويشمل جميع المعلومات الرقمية والتفاعلات المرتبطة بشخص ما، مثل منشورات وسائل التواصل الاجتماعي وعمليات البحث عبر الإنترنت وزيارات موقع الويب والمشاركات الأخرى عبر الإنترنت. يتم إنشاء هذه البصمة وتراكمها عندما يستخدم الأفراد الأجهزة والمنصات الرقمية.

التوقيع الرقمي Digital Signiture

ختم افتراضي لأصالة المستندات أو الرسائل الإلكترونية. يتضمن استخدام تقنيات التشفير لإنشاء معرف فريد يتحقق من أصل المحتوى الرقمي وسلامته. تضمن التوقيعات الرقمية أن المرسل هو الشخص الذي يدعي أنه لم يتم تغيير المحتوى أثناء الإرسال. وهي طريقة آمنة للتأكد من صحة الملفات الرقمية، والتي تُستخدم عادةً في المعاملات والعقود والاتصالات الحساسة عبر الإنترنت. تتضمن العملية مفتاحًا خاصًا لإنشاء التوقيع ومفتاحًا عامًا للتحقق، مما يوفر طريقة موثوقة لضمان سلامة المعلومات الرقمية ومصداقيتها.

توقيع DKIM

توقيع رقمي لرسائل البريد الإلكتروني. وهي ميزة أمان تساعد في التحقق من صحة المرسل وتضمن عدم العبث بمحتوى البريد الإلكتروني أثناء الإرسال. يعمل DKIM عن طريق إضافة توقيع رقمي إلى رأس البريد الإلكتروني باستخدام مفتاح خاص مرتبط بنطاق الإرسال. يمكن لخادم البريد الإلكتروني للمستلم بعد ذلك استخدام المفتاح العام المنشور في سجلات DNS الخاصة بالمجال للتحقق من التوقيع.

الوصول المباشر للذاكرة DMA - Direct Memory Access

يعد الوصول المباشر للذاكرة بمثابة مساعد لمعالج الكمبيوتر (CPU). بدلاً من معالجة وحدة المعالجة المركزية شخصيًا لكل جزء من البيانات التي يجب نقلها بين الأجهزة (مثل التخزين أو الشبكة) والذاكرة، يسمح DMA لوحدة تحكم متخصصة بتولي المسؤولية. فكر في الأمر كخدمة بريد سريع: تخبر وحدة المعالجة المركزية DMA بما يجب نقله وأين، وتقوم DMA بنقل البيانات بكفاءة مباشرة بين الأجهزة والذاكرة دون إزعاج وحدة المعالجة المركزية. ويساعد ذلك على تسريع عمليات نقل البيانات، مما يجعل جهاز الكمبيوتر الخاص بك أكثر كفاءة عن طريق تحرير وحدة المعالجة المركزية للتركيز على المهام الهامة الأخرى.

مفهوم DMARC

المراسلة المستندة إلى النطاق وتوافق التقارير (DMARC) بمثابة معيار أمان لرسائل البريد الإلكتروني. فهو يساعد على منع انتحال البريد الإلكتروني والتصيد من خلال السماح لمرسلي البريد الإلكتروني بتحديد كيفية مصادقة رسائل البريد الإلكتروني الخاصة بهم والإجراءات التي يجب اتخاذها في حالة فشل المصادقة.

المنطقة منزوعة السلاح A Demilitarized Zone - DMZ

تضم المنطقة المجردة من السلاح عادةً خوادم وخدمات يجب الوصول إليها من الإنترنت، مثل خوادم الويب أو خوادم البريد الإلكتروني، مع إبقائها منفصلة عن الشبكة الداخلية الأكثر حساسية. يضيف هذا الإعداد طبقة إضافية من الأمان من خلال التحكم في حركة المرور من وإلى الإنترنت ومراقبتها، مما يقلل من مخاطر الهجمات المباشرة على الشبكة الداخلية.

نظام اسم المجال Domain Name System- DNS

نظام يترجم أسماء النطاقات سهلة الاستخدام، مثل Google. com، إلى عناوين IP الرقمية التي تستخدمها أجهزة الكمبيوتر للتعرف على بعضها البعض على الإنترنت. عندما تكتب اسم موقع ويب في متصفحك، يساعد DNS جهازك في العثور على عنوان IP الصحيح، مما يسمح لك بالاتصال بموقع الويب المطلوب أو الخدمة عبر الإنترنت.

النطاق Domain

عنوان فريد لموقع ويب على الإنترنت. هو الاسم سهل الاستخدام الذي تكتبه في متصفحك للوصول إلى موقع معين، مثل Google. com. يرتبط النطاق بعنوان IP رقمي تستخدمه أجهزة الكمبيوتر لتحديد موقع بعضها البعض على الإنترنت.

هجوم التحميل Download Attack

فخ وضعه الهاكرز لخدع المستخدمين لتنزيل المالوير والفايروسات وتثبيتها على أجهزتهم. غالبًا ما تتضمن هذه الهجمات إخفاء البرامج الضارة كملفات حقيقية أو إغراء المستخدمين بمحتوى يبدو غير ضار. بمجرد قيام المستخدم بتنزيل الملف وتنفيذه، يمكن أن يصيب البرنامج الضار الجهاز، مما يؤدي إلى عواقب مختلفة مثل سرقة البيانات أو اختراق النظام أو الوصول غير المصرح به.

E

الهجوم الكهرومغناطيسي Electromagnetic Attack

محاولة لتعطيل الأنظمة والأجهزة الإلكترونية أو تعريضها للخطر عن طريق إصدار إشعاعات أو نبضات كهرومغناطيسية. يمكن لهذا النوع من الهجمات أن يستهدف مجموعة واسعة من المعدات الإلكترونية، بما في ذلك أنظمة الاتصالات وأجهزة الكمبيوتر والأنظمة المدمجة، من خلال استغلال قابليتها للتداخل الكهرومغناطيسي.

التصنت Eavesdropping

اعتراض الاتصالات ومراقبتها ، وعادةً ما يكون ذلك في شكل إشارات إلكترونية أو إشارات اتصالات، بهدف الوصول إلى معلومات خاصة أو حساسة. تتضمن تقنية المراقبة السرية هذه الاستماع خلسة إلى البيانات المنقولة عبر الشبكات أو التقاطها، مثل المكالمات الهاتفية أو تبادل البريد الإلكتروني أو أشكال أخرى من الاتصالات الرقمية.

النقطة النهائية Endpoint

اي جهاز على شبكة تعمل كنقطة وصول للمستخدمين أو الاتصالات. ويشمل أجهزة مثل أجهزة الكمبيوتر واللابتوب والهواتف الذكية والأجهزة اللوحية والخوادم.

تصفية الخروج Egress Filtering

مراقبة حركة الشبكة الصادرة من الشبكة الداخلية للمؤسسة الى الإنترنت. يتضمن تنفيذ القواعد والسياسات على محيط الشبكة لفحص وتقييد البيانات الخارجة من الشبكة الداخلية.

الذكاء الالكتروني Electronic Intelligence - ELINT

فرع من ذكاء الإشارات (SIGINT) يركز بشكل خاص على جمع وتحليل الإشارات الكهرومغناطيسية غير المتعلقة بالاتصالات. تتضمن عمليات ELINT اعتراض وتفسير الانبعاثات الإلكترونية المختلفة، مثل إشارات الرادار، أو عمليات إرسال الإلكترونية، أو التوقيعات الإلكترونية الأخرى المنبعثة من أجهزة الاستشعار أو الأنظمة.

تحليل الانبعاثات Emanations Analysis

مفهوم أمني يتضمن دراسة وتحليل الإشارات أو الانبعاثات غير المقصودة التي يمكن استغلالها لجمع معلومات حول الأنظمة الإلكترونية. قد تتضمن هذه الانبعاثات إشارات ترددات راديوية غير مقصودة (RF)، أو مجالات كهرومغناطيسية، أو إشارات صوتية تنتجها الأجهزة الإلكترونية أثناء التشغيل.

الضغط التنفيذي Executable compression

أسلوب أمني يتضمن ضغط الملفات القابلة للتشغيل لتقليل حجمها وتحسين تخزينها أو نقلها. لا تهدف عملية الضغط إلى تقليل حجم الملف فحسب، بل يمكن استخدامها أيضًا كشكل من أشكال التشويش لجعل التحليل والهندسة العكسية للملف القابل للتنفيذ أكثر صعوبة بالنسبة للخصوم المحتملين.

التغليف Encapsulation

تغليف البيانات أو البروتوكولات أو الوظائف الحساسة ضمن إطار أو حاوية آمنة لحمايتها من الوصول أو التلاعب بها.

التسلل Exfiltration

عملية استخراج البيانات أو نقلها بشكل غير مصرح وخفي من نظام أو شبكة بواسطة مهاجم. يعد التسلل مرحلة من الهجوم السيبراني حيث يتم نقل المعلومات الحساسة، مثل البيانات السرية أو الملكية الفكرية أو بيانات اعتماد تسجيل الدخول، بشكل غير قانوني خارج النظام المستهدف.

المنفذ المؤقت Ephemeral Port

منفذ شبكة مؤقت يستخدمه نظام العميل للاتصال بالخادم. في الشبكات، تعد المنافذ معرفات رقمية مرتبطة بعمليات أو خدمات محددة على الجهاز. عادةً ما يتم استخدام المنافذ المؤقتة بواسطة تطبيقات العميل لإنشاء اتصالات صادرة بالخوادم.

ضامن كلمات المرور Escrow Passwords

ممارسة أمنية يقوم فيها طرف ثالث موثوق به بالاحتفاظ بكلمات المرور أو مفاتيح التشفير وإدارتها نيابة عن المستخدمين أو المؤسسات.

خوارزمية التراجع الاسي Exponential Backoff Algorithm

استراتيجية اتصالات شبكية تُستخدم في بروتوكولات مختلفة لإدارة وتخفيف مشاكل الازدحام أو التنافس في الأنظمة الموزعة. في المواقف التي تحاول فيها أجهزة متعددة الوصول إلى مورد مشترك في وقت واحد، يمكن أن تحدث تصادمات أو تنافس، مما يؤدي إلى عدم الكفاءة واحتمال ازدحام الشبكة. تعالج خوارزمية التراجع الأسي هذه المشكلة من خلال تقديم فترة انتظار تزداد بشكل كبير مع كل محاولة غير ناجحة للوصول إلى المورد.

التعرض Exposure

التعرض لخطر التهديدات الأمنية أو نقاط الضعف التي قد تؤدي إلى الوصول أو اختراق البيانات أو غيرها من أشكال التسوية.

التعداد Enumeration

عملية استخراج المعلومات من نظام مستهدف للحصول على فهم أفضل لتكوينه وموارده ومستخدميه. وهي مرحلة مهمة في جمع المعلومات لتقييم الأمن أو اختبار الاختراق.

بروتوكول المصادقة القابل للتوسع EAP Extensible Authentication Protocol

إطار عمل شائع الاستخدام في بروتوكولات مصادقة الشبكة لدعم طرق المصادقة المختلفة ضمن بنية مرنة وقابلة للتوسيع.

بروتوكول البوابة الخارجية EGP Exterior Gateway Protocol

بروتوكول شبكة يسهل تبادل معلومات التوجيه وإمكانية الوصول بين الأنظمة الذاتية (AS) في سياق الإنترنت.

التشفير Encryption

تحويل البيانات القابلة للقراءة بيانات مشفرة قابلة للفتح لأي شخص ليس لديه المفتاح الصحيح . وهي طريقة لحماية المعلومات الحساسة، مثل كلمات المرور أو الرسائل، من الوصول غير المصرح به أو التجسس أثناء الإرسال.

المستخدم النهائي End User

الجهاز الذي تستخدمه للوصول إلى المعلومات أو تصفح الإنترنت أو إرسال الرسائل أو تشغيل التطبيقات , مثل الكمبيوتر أو الهاتف او التابلت.

المؤسسات Enterprise

شركة أو مؤسسة كبيرة تعمل على نطاق واسع. وهي كيان كبير ومنظم يشارك في أنشطة مختلفة، غالبًا مع أقسام وموظفين متعددين. سواء في التصنيع أو الخدمات أو أي صناعة أخرى، مصمم لتحقيق أهداف محددة على مستوى جوهري. يستخدم هذا المصطلح بشكل شائع لوصف الشركات المعقدة والراسخة التي تلعب دورًا مهمًا في الأسواق الخاصة بها.

الضمان Escrow

مساحة تخزين آمنة للأشياء أو المستندات المهمة والقيمة أثناء المعاملة. عندما يشارك طرفان في صفقة ما، خاصة في العقارات أو المعاملات المالية الكبيرة، فقد يستخدمان الضمان.فهو يعمل كطرف ثالث محايد يحتفظ مؤقتًا بالأصول أو الأموال أو المستندات المهمة حتى يتم استيفاء شروط معينة أو اكتمال المعاملة. وهذا يضيف طبقة من الأمان والثقة، مما يضمن وفاء الطرفين بالتزاماتهما قبل تحرير الأصول أو المستندات من الضمان.

إيثرنت Ethernet

إحدى تقنيات الشبكات المستخدمة على نطاق واسع والتي تسهل الاتصال السلكي. وهو يتضمن نظامًا من الكابلات والبروتوكولات التي تربط أجهزة الكمبيوتر والطابعات وأجهزة التوجيه والأجهزة الأخرى، مما يسمح لها بمشاركة البيانات والموارد. تشتهر شبكة ايثرنت بموثوقيتها وكفاءتها في نقل

البيانات، مما يجعلها خيارًا شائعًا لكل من الشبكات المنزلية وشبكات الأعمال. تستخدم الأجهزة المتصلة عبر ايثرنت بروتوكولات اتصال موحدة لضمان تبادل البيانات بشكل سلس وسريع. أصبحت هذه التكنولوجيا عنصرًا أساسيًا في الشبكات الحديثة، حيث توفر بنية تحتية مستقرة لمختلف الأنشطة الرقمية داخل منطقة جغرافية محدودة.

الاستغلال Exploit

جزء محدد من البرامج أو التعليمات البرمجية أو التقنية المصممة للاستفادة من نقاط الضعف في نظام الكمبيوتر أو التطبيق أو الشبكة. يستخدم الهاكرز عمليات الاستغلال لاختراق النظام المستهدف أو الوصول أو تنفيذ إجراءات ضارة. غالبًا ما تستهدف برامج الاستغلال نقاط الضعف المعروفة التي قد تتوفر تصحيحات أو تحديثات أمنية لها.

F

الرفض الكاذب False Rejects

الحالات التي يرفض فيها النظام البيومتري أو نظام المصادقة بشكل غير صحيح الوصول إلى مستخدم حقيقي. يحدث هذا النوع من الأخطاء عندما يفشل النظام في التعرف على بيانات الاعتماد الصالحة أو البيانات البيومترية الصالحة المقدمة من قبل مستخدم معتمد وقبولها.

العلامة المزيفة False Flag

تكتيك خادع حيث يخفي المهاجم هويته الحقيقية ، مما يجعلها تبدو كما لو أن الهجوم أو العملية قد تم إجراؤها بواسطة كيان آخر.

نظام الملفات الصحيح Fast File System

نظام ملفات مصمم لأنظمة التشغيل المشابهة لليونكس لإدارة البيانات وتخزينها على القرص .

تقنية Fast Flux

تقنية مستخدمة في الهجمات السيبرانية لتغيير الارتباط بين أسماء النطاقات وعناوين IP بسرعة. يساعد تكوين الشبكة والمتغير بسرعة الجهات الخبيثة على تجنب الكشف من قبل أنظمة الأمان.

هجوم خط الخطأ Fault Line Attacks

فئة من الهجمات التي تستغل نقاط الضعف في الأجهزة أو البرامج الناشئة عن أخطاء في النظام. يمكن إحداث هذه الأخطاء عمدًا، مثلاً من خلال الوسائل المادية مثل معالجة الجهد الكهربي أو تغيرات درجة الحرارة أو الإشعاع، مما يؤدي إلى أخطاء في تنفيذ التعليمات البرمجية أو عمل مكونات الأجهزة.

نسخة التحقيق Forensic Copy

النسخ الدقيق للبيانات الرقمية، عادةً من جهاز تخزين مثل محرك الأقراص الثابتة أو محرك الأقراص المحمول، والذي يتم إجراؤه بطريقة سليمة من الناحية الجنائية. تضمن هذه العملية إنشاء نسخة طبق الأصل دون تغيير البيانات الأصلية.

بروتوكول نقل الملفات FTP File Transfer Protocol

بروتوكول شبكة يستخدم لنقل الملفات بين المستخدم والخادم على شبكة الكمبيوتر.

الطوفان Flooding

هجوم يتم فيه إغراق الشبكة أو النظام بكمية كبيرة من حركة المرور أو البيانات، مما يعطل عملها الطبيعي.

الدليل الرسمي Formal Proof

إثبات صارم بأن نظامًا أو برنامجًا أو خوارزمية تشفير معينة تلتزم بخصائص أو متطلبات أمنية محددة. تتضمن هذه العملية استخدام أساليب رسمية ومنطق رياضي واستدلال دقيق للتحقق من أن النظام يتصرف على النحو المنشود وخالي من الثغرات الأمنية أو العيوب الأمنية.

المصادقة المستندة الى نموذج Form-Based Authentication

آلية أمان شائعة على مواقع الويب للتحقق من هوية المستخدمين أثناء عملية تسجيل الدخول. وهو يتضمن تقديم نموذج على شبكة الإنترنت للمستخدمين، يتضمن عادةً حقولًا لإدخال اسم المستخدم وكلمة المرور.

البحث الامامي Forward Lookup

مصطلح في إدارة الشبكات ونظام اسم المجال (DNS) يشير إلى عملية ترجمة أسماء النطاقات التي يمكن قراءتها بواسطة الإنسان إلى عناوين IP .

هجوم تداخل الاجزاء Fragment Overlap Attack

نوع من هجمات الشبكة التي تستغل الثغرات الأمنية في معالجة الحزم المجزأة بواسطة أجهزة الشبكة. في هذا الهجوم، يتلاعب الهاكر بعملية التجزئة، مما يؤدي إلى إنشاء أجزاء متداخلة قد تربك أو تعطل عملية إعادة التجميع الصحيحة للحزمة الأصلية بواسطة النظام المستهدف.

التجزئة Fragmentation

عملية تقسيم حزم البيانات إلى أجزاء أصغر للإرسال عبر شبكة قد يكون لها أحجام مختلفة لوحدة الإرسال (MTU). وهذا مهم بشكل خاص عند إرسال البيانات عبر شبكات ذات إمكانيات مختلفة أو من خلال الأجهزة التي تفرض قيودًا على الحجم على الحزم المرسلة.

الاطر Frames

الوحدات الأساسية للبيانات المنقولة عبر الشبكة باستخدام طبقة ارتباط البيانات في نموذج OSI. تقوم هذه الاطر بتغليف البيانات بمعلومات الرأس والمقطورة، بما في ذلك عناوين المصدر والوجهة، وأكواد التحقق من الأخطاء، ومعلومات التحكم، مما يسهل الاتصال الموثوق والفعال بين الأجهزة في الشبكة.

مفهوم FIDO2

اختصار لـ Fast Identity Online 2، هي طريقة حديثة وآمنة للمصادقة عبر الإنترنت. تمثل مجموعة من المعايير المفتوحة التي تمكن المستخدمين من الوصول إلى الخدمات عبر الإنترنت باستخدام أساليب مصادقة قوية بدون كلمة مرور. يستخدم FIDO2 التشفير العام لتعزيز الأمان، مما يسمح للمستخدمين بمصادقة أنفسهم باستخدام القياسات الحيوية، مثل بصمات الأصابع أو التعرف على الوجه، أو من خلال أجهزة خارجية مثل مفاتيح الأمان. وتهدف هذه التقنية إلى تقليل الاعتماد على كلمات المرور ، التي تكون عرضة للتهديدات السيبرانية المختلفة، وتوفر نهجًا أكثر قوة وسهولة في الاستخدام للتحقق من الهوية عبر الإنترنت.

قارئ البصمات fingerprint reader

جهاز بيومتري يلتقط ويحلل بصمة الشخص، مما يؤدي إلى إنشاء توقيع رقمي مميز. فهو يحول بصمة إصبعك إلى مفتاح آمن وشخصي للوصول إلى الأجهزة أو الأنظمة أو التطبيقات. تُستخدم قارئات بصمات الأصابع بشكل شائع في تطبيقات الأمان المختلفة، بما في ذلك فتح الهواتف الذكية، أو تأمين الوصول إلى المباني، أو التحقق من صحة الهويات للمعاملات المهمة. وتوفر هذه التقنية طريقة آمنة للتوثيق، حيث أن بصمة كل شخص فريدة، مما يجعلها طريقة مصادقة بيومترية موثوقة ومعتمدة.

الجدار الناري Firewall

حاجز رقمي يحمي شبكات الكمبيوتر من الوصول والتهديدات السيبرانية. وهو بمثابة نقطة تفتيش أمنية، حيث يقوم بمراقبة حركة مرور الشبكة الواردة والصادرة بناءً على قواعد أمنية محددة . يقوم جدار

الحماية بتحليل البيانات التي تنتقل بين شبكة خاصة والإنترنت، مما يسمح بها أو يحظرها وفقًا للمعايير المحددة.

فيرم وير Firmware

شكل من أشكال البرامج المضمنة في الأجهزة لمساعدتها على العمل . تعتمد الأجهزة مثل الكاميرات والهواتف المحمولة وبطاقات الشبكة ومحركات الأقراص الضوئية والطابعات وأجهزة التوجيه والماسحات الضوئية وأجهزة التحكم عن بعد الخاصة بالتلفزيون على البرامج الثابتة المضمنة في ذاكرتها لتعمل بسلاسة.

الازدواج الكامل Full Duplex

وضع الاتصال في الشبكات حيث يمكن نقل البيانات في كلا الاتجاهين في وقت واحد. في نظام الاتصال مزدوج الاتجاه، يمكن للأجهزة إرسال واستقبال البيانات بشكل مستقل، مما يتيح الاتصال ثنائي الاتجاه مع القدرة على إرسال واستقبال البيانات بشكل متزامن.

تقنية Fuzzing

تقنية اختبار برمجية تستخدم في الأمن للكشف عن نقاط الضعف في النظام من خلال إخضاعه لوابل من بيانات الإدخال غير المتوقعة أو المشوهة أو العشوائية.

G

المراقبة الحكومية Government surveillance

المراقبة المنتظمة والسرية وجمع وتحليل المعلومات من قبل الجهات الحكومية حول الأفراد أو المجموعات أو الأنشطة ضمن الولاية القضائية لبلد ما. يمكن أن تتخذ هذه المراقبة أشكالًا مختلفة، بما في ذلك اعتراض الاتصالات، وتتبع الأنشطة عبر الإنترنت، واستخدام كاميرات الدوائر التلفزيونية المغلقة (CCTV)، وجمع البيانات الوصفية المتعلقة بالمكالمات الهاتفية أو رسائل البريد الإلكتروني أو استخدام الإنترنت.

القبعة الرمادية Grey Hat

فرد أو مهاجم يعمل بمزيج من الممارسات الأخلاقية وغير الأخلاقية . على عكس قراصنة القبعة البيضاء، الذين يستخدمون مهاراتهم بشكل أخلاقي لتحديد الثغرات الأمنية وإصلاحها، وقراصنة

القبعة السوداء، الذين ينخرطون في أنشطة خبيثة لتحقيق مكاسب شخصية ، فإن قراصنة القبعة الرمادية يقعون في مكان ما بينهما.

فحص الصندوق الرمادي Gray box testing

أسلوب اختبار برمجيات يجمع بين عناصر منهجيات اختبار الصندوق الأسود والصندوق الأبيض. في اختبار الصندوق الرمادي، يكون لدى المختبرين معرفة جزئية بالأعمال الداخلية وبنية التطبيق الذي يتم تقييمه. ويعتبر هذا المستوى من المعلومات متوسطا، إذ يقع بين الشفافية الكاملة في اختبار الصندوق الأبيض، حيث يكون الكود الداخلي معروفا بشكل كامل، وبين النقص التام في المعرفة في اختبار الصندوق الأسود.

البوابة Gateway

المدخل أو الجسر الرقمي الذي يربط بين شبكات الكمبيوتر المختلفة، مما يتيح الاتصال فيما بينها. تعمل البوابة كوسيط، حيث تقوم بترجمة البيانات بين الشبكات التي تستخدم بروتوكولات اتصال مختلفة، مما يضمن نقل البيانات بسلاسة.

الكفاءة ضد التخمين Guessing entropy

قياس عدم القدرة على التنبؤ أو تعقيد المعلومات التي قد يحتاجها المهاجم لتخمين كلمة المرور أو بيانات اعتماد المصادقة بشكل صحيح.

الامن المتدرج Graduated Security

تنفيذ متعدد الطبقات للحلول الأمنية، مع زيادة مستويات الحماية مع اقتراب المرء من الأصول الأساسية أو الهامة للنظام أو المؤسسة.

نظام GNU

نظام تشغيل مجاني ومفتوح المصدر ومجموعة واسعة من الأدوات البرمجية التي تم تطويرها كجزء من مشروع GNU.

جيت هب GitHub

موقع ومستودع للتحكم في البرامج والاصدارات يستخدم على نطاق واسع لتطوير البرامج .يسمح للمطورين باستضافة وإدارة الاكواد البرمجية الخاصة بهم، والتعاون في المشاريع، وتتبع التغييرات التي تم إجراؤها على قواعد التعليمات البرمجية.

نوتيلا Gnutella

بروتوكول وشبكة لامركزية لمشاركة الملفات(P2P) تتيح للمستخدمين مشاركة الملفات مباشرة مع بعضهم البعض دون الحاجة إلى خادم مركزي.

الصورة الذهبية Golden Image

قالب موحد ومكون مسبقًا لنظام كمبيوتر تم تكوينه بدقة ليكون بمثابة خط بداية لنشر نسخ متعددة من نفس البيئة.

H

الهاكر Hacker

خبير كمبيوتر ماهر يستكشف الأعمال الداخلية لأنظمة الكمبيوتر والشبكات، وغالبًا ما يكون لديه فهم عميق للبرامج والأجهزة. في حين أن المصطلح له دلالات مختلفة، فإنه يشير عمومًا إلى الاشخاص الذين يستخدمون معرفتهم التقنية للوصول غير المصرح به إلى أنظمة الكمبيوتر أو الشبكات، إما لأغراض ضارة أو لاختبار وتعزيز الأمن السيبراني.

التجزئة Hashing

اشبه بإنشاء توقيع رقمي فريد للبيانات. فهي تتضمن استخدام خوارزمية محددة لتحويل أي كمية من البيانات إلى سلسلة ذات حجم ثابت من الأحرف، تسمى التجزئة. هذه التجزئة هي تمثيل متميز للبيانات الأصلية وتعمل بمثابة نوع من البصمة الرقمية.

هاش كات Hashcat

أداة قوية ومتعددة الاستخدامات لكسر كلمات المرور مصممة لاستعادة كلمات المرور المفقودة أو المنسية من خلال استخدام هجوم القاموس Dictionary Attack.

التصليب Hardening

عملية تأمين نظام الكمبيوتر أو الشبكة من خلال تنفيذ الحلول التي تقلل من نقاط الضعف وتقوي الدفاعات ضد التهديدات السيبرانية المحتملة. يتضمن هذا النهج الأمني الاستباقي تكوين البرامج والأجهزة ومكونات الشبكة للالتزام بأفضل الممارسات وتقليل سطح الهجوم.

هادوب Hadoop

إطار عمل مفتوح المصدر مصمم للتخزين الموزع ومعالجة مجموعات البيانات الكبيرة باستخدام مجموعة من الأجهزة .

هجوم الاختطاف Hijack Attack

عمل ضار يقوم فيه طرف بالسيطرة على نظام أو قناة اتصال أو عملية لأغراض خبيثة. في مجال الأمن السيبراني، عادةً ما يتضمن هجوم الاختطاف التلاعب أو تحويل البيانات أو الأنظمة أو جلسات المستخدم.

قرد العسل Honey monkey

أداة أو نظام أمني متخصص مصمم لاكتشاف وتحليل التهديدات المستندة إلى الويب، خاصة تلك التي تتضمن مواقع ويب ومحتوى ملغوم. وهو يعمل من خلال التنقل بشكل مستقل عبر الإنترنت، وزيارة مواقع الويب التي يحتمل أن تكون خطرة، وتحليل سلوك هذه المواقع لتحديد وفهم أنواع مختلفة من الهجمات المستندة إلى الويب، مثل التنزيلات من الأقراص، أو التصيد ، أو توزيع البرامج الضارة.

القفزات Hops

النقاط المتعاقبة التي تعبرها حزم البيانات أثناء تحركها عبر شبكة الكمبيوتر. تمثل كل قفزة نقطة نقل، تتضمن عادةً أجهزة توجيه أو محولات، وتساهم في المسار العام الذي تتخذه البيانات من مصدرها إلى وجهتها.

الهب Hub

جهاز شبكة أساسي يربط أجهزة متعددة في شبكة محلية (LAN). يعمل في الطبقة المادية لنموذج OSI ويفتقر إلى الذكاء اللازم لإعادة توجيه البيانات بشكل انتقائي إلى المستلم المقصود فقط. وبدلاً من ذلك، يقوم المركز ببث البيانات إلى جميع الأجهزة المتصلة، مما يجعله أقل كفاءة وأكثر عرضة للمخاطر الأمنية، مثل التنصت والوصول .

الهجوم المختلط Hybrid Attack

هجوم إلكتروني معقد ومتعدد الأوجه يجمع بين تقنيات ومنهجيات متعددة لاستغلال نقاط الضعف في النظام أو الشبكة المستهدفة.

التشفير المختلط Hybrid Encryption

أسلوب تشفير يجمع بين نقاط قوة التشفير المتماثل وغير المتماثل لتحقيق توازن الكفاءة والأمان في الاتصال الآمن. في التشفير المختلط، يتم إنشاء مفتاح متماثل فريد لكل جلسة اتصال، مما يوفر كفاءة التشفير المتماثل السريع للبيانات المجمعة.

هايبرلينك Hyperlink

عنصر قابل للنقر مضمن في المستندات الإلكترونية، عادة ما يكون نصًا أو صورًا، والذي، عند الضغط عليه، يعيد توجيه المستخدم إلى موقع آخر.

تهرب المضيف Host Evasions

التقنيات المعقدة التي تستخدمها البرامج الضارة أو الجهات الخبيثة لتجنب الكشف والتحليل بواسطة آليات الأمان على نظام مضيف مستهدف.

لغة Hypertext Markup Language - HTML

لغة الترميز المستخدمة في تطوير الويب لإنشاء المحتوى وتنظيمه على الإنترنت. وتتكون من مجموعة من العناصر الممثلة بالعلامات التي تحدد بنية وعرض محتوى صفحة الويب، بما في ذلك النصوص والصور والروابط والوسائط المتعددة.

بروتوكول Hypertext Transfer Protocol - HTTP

يعد بروتوكول (HTTP) أساس اتصالات البيانات على شبكة الويب، مما يسهل نقل النصوص والصور والملفات والموارد الأخرى بين خوادم الويب والعملاء.

مصيدة العسل Honeypot

هو مفهوم للأمن السيبراني مصمم لجذب واكتشاف الأنشطة الضارة داخل الشبكة. وهوبمثابة فخ، حيث يجذب المهاجمين بنقاط ضعف مغرية أو بيانات مزيفة لتحويل انتباههم عن البيانات الحقيقية. تحاكي مصيدة العسل هدفًا قيمًا، مثل الخادم أو جزء الشبكة، وتراقب أي محاولات غير مصرح بها للوصول إليه أو استغلاله. الغرض الأساسي من مصيدة الجذب هو جمع معلومات حول التكتيكات والتقنيات والإجراءات التي يستخدمها المهاجمون، مما يسمح لمحترفي الأمن السيبراني بتعزيز فهمهم للتهديدات الناشئة وتعزيز الدفاعات ضدها.

الاستضافة Host

أي جهاز أو نظام كمبيوتر يشارك في الشبكة ويتم تعيين عنوان IP فريد له لتسهيل الاتصال داخل تلك الشبكة.

نقطة الاتصال HotSpot

موقع أو منطقة معينة، عادة داخل مساحة عامة، حيث يتم توفير الوصول إلى الإنترنت اللاسلكي للمستخدمين، مما يمكنهم من الاتصال بالإنترنت عبر شبكة الوايفاي.

برنامج Hypervisor

معروف أيضًا باسم (VMM)، هو برنامج أو جهاز يتيح إنشاء الأجهزة الافتراضية (VMs) وإدارتها على جهاز كمبيوتر. ويسمح لأنظمة تشغيل متعددة بالعمل بشكل متزامن على جهاز حقيقي واحد، كل منها ضمن بيئته الافتراضية المعزولة.

I

الهوية Identity

المعلومات الفريدة التي يمكن التحقق منها والتي تحدد تميز كيان ما، مثل فرد أو نظام أو جهاز. يعد إنشاء الهويات وإدارتها جانبًا مهمًا للأمن السيبراني، بما في ذلك عمليات مصادقة المستخدم والترخيص.

الحادث Incident

حدث سلبي يشكل تهديدًا محتملاً لسرية المعلومات ونظم المعلومات أو سلامتها أو توفرها.

النسخ الاحتياطي التصاعدي Incremental Backups

نوع من إستراتيجية النسخ الاحتياطي للبيانات التي تتضمن فقط نسخ البيانات التي تم تغييرها أو إضافتها منذ آخر نسخة احتياطية، سواء كانت نسخة احتياطية كاملة أو نسخة احتياطية تزايدية سابقة.

الهجوم الاستدلالي Inference Attack

نوع من التهديد الأمني الذي يستنتج فيه الخصم معلومات حساسة من خلال تحليل البيانات التي تبدو غير ضارة أو غير حساسة.

انظمة كشف التسلل IDS Intrusion Detection System

تقنية أمنية مصممة لمراقبة وتحليل أنشطة الشبكة أو النظام بحثًا عن علامات السلوك المشبوه. يعمل من خلال فحص حركة مرور الشبكة أو سجلات النظام لحظة بلحظة، والبحث عن الحالات الشاذة التي قد تشير إلى تهديد أمني.

حرب المعلومات Information Warfare

مفهوم استخدام تكنولوجيات المعلومات والاتصالات لتحقيق أهداف استراتيجية في الصراعات أو السيناريوهات الجيوسياسية.

تصفية الدخول Ingress Filtering

ممارسة أمنية يتم تنفيذها في شبكات الكمبيوتر للتحكم في حركة مرور البيانات الواردة والتحقق من صحتها. تتضمن هذه العملية فحص الحزم التي تدخل الشبكة والسماح بها أو حظرها بناءً على معايير محددة مسبقًا، مثل عناوين IP أو البروتوكولات أو أرقام المنافذ.

هجمات تحقق الادخال Input Validation Attacks

فئة من التهديدات الأمنية حيث تستغل الجهات الخبيثة نقاط الضعف في النظام عن طريق إرسال بيانات غير متوقعة أو معدة خصيصًا كمدخلات لخدع التطبيق المستهدف أو اختراقه.

النزاهة Integrity

ضمان بقاء البيانات أو المعلومات دون تغيير وجديرة بالثقة طوال دورة حياتها، بدءًا من إنشائها وحتى تخزينها ونقلها.

بروتوكول Internet Control Message Protocol ICMP

بروتوكول متكامل لمجموعة بروتوكولات الإنترنت (IP)، وهو مصمم بشكل أساسي لتبادل رسائل التحكم وإشعارات الأخطاء بين أجهزة الشبكة.

فريق عمل هندسة الانترنت The Internet Engineering Task Force - IETF

مجتمع عالمي من المتطوعين والمهنيين المخصصين لتطوير وتعزيز المعايير المفتوحة للإنترنت. تأسست IETF في عام 1986، وتعمل من خلال مجموعات عمل تركز على مجالات محددة من تكنولوجيا الإنترنت، وتتعاون لإنشاء وتحسين معايير البروتوكولات والتطبيقات والأنظمة.

بروتوكول Internet Message Access Protocol - IMAP

بروتوكول لاسترداد البريد الإلكتروني يمكّن المستخدمين من الوصول إلى رسائل البريد الإلكتروني المخزنة على خادم البريد وإدارتها.

المقاطعة Interrupt

الإشارة المرسلة بواسطة جهاز أو برنامج لمقاطعة التدفق الطبيعي لتنفيذ المعالج.

الشبكة الخاصة Intranet

الإنترانت (انتبه , ليس الانترنت !) هي شبكة كمبيوتر خاصة داخل مؤسسة تستخدم تقنيات الإنترنت لتسهيل تبادل المعلومات والتعاون والتواصل بين أعضائها. على عكس شبكة الإنترنت العامة، تقتصر شبكة الإنترانت على المستخدمين داخل المؤسسة وغالبًا ما تكون محمية بإجراءات أمنية مثل جدران الحماية وعناصر التحكم في الوصول.

كشف التسلل Intrusion Detection

آلية للأمن السيبراني مصممة لتحديد الأنشطة غير المصرح بها أو الضارة داخل نظام الكمبيوتر أو الشبكة والرد عليها. يتضمن هذا النهج الأمني الاستباقي مراقبة وتحليل أحداث النظام والشبكة لحظة بلحظة لاكتشاف الأنماط التي تشير إلى حوادث أمنية محتملة.

المنظمة الدولية للمعايير ISO

هيئة عالمية تعمل على تطوير ونشر المعايير الدولية في مختلف الصناعات، بما في ذلك أمن المعلومات. في سياق الأمن، توفر معايير ISO، وخاصة تلك الواردة في سلسلة ISO/IEC 27000، إطارًا لإنشاء نظام إدارة أمن المعلومات (ISMS) وتنفيذه وصيانته وتحسينه باستمرار.

انظمة التحكم الصناعية Industrial Control Systems - ICS

هي أنظمة متخصصة لإدارة العمليات الصناعية والبنية التحتية الحيوية والتحكم فيها. تُستخدم هذه الأنظمة في قطاعات مختلفة مثل التصنيع والطاقة ومعالجة المياه والنقل لأتمتة العمليات المعقدة ومراقبتها.

مزود الهوية Identity Provider

هو خدمة أو نظام مركزي يسهل عمليات المصادقة والترخيص للمستخدمين داخل الشبكة أو بيئة الإنترنت. وتتمثل الوظيفة الأساسية لمزود الهوية في إدارة هويات المستخدمين والتحقق منها، مما يسمح للأفراد بالوصول إلى التطبيقات أو الخدمات أو الموارد المختلفة بشكل آمن.

ادارة الحوادث Incident management

هي أسلوب منظم ومنسق لتحديد الأحداث التخريبية والاستجابة لها وحلها داخل المنظمة. يمكن أن تشمل هذه الحوادث مجموعة واسعة من المواقف، بما في ذلك الخروقات الأمنية أو فشل النظام أو الكوارث الطبيعية أو أي أحداث أخرى غير متوقعة قد تؤثر على العمليات التجارية الطبيعية.

ضمان المعلومات Information assurance

نهج شامل واستراتيجي لإدارة وحماية أصول المعلومات داخل المنظمة. الهدف منه هو ضمان سرية المعلومات وسلامتها وتوافرها وصحتها طوال تواجدها. يشمل هذا المجال مجموعة من الممارسات

والسياسات والتقنيات التي تهدف بشكل جماعي إلى حماية البيانات الحساسة من الوصول أو التغيير أو التدمير.

البنية التحتية كخدمة Infrastructure as a Service

هي نموذج سحابي يوفر موارد كومبيوتر افتراضية عبر الإنترنت. في بيئة IaaS، يقدم موفرو خدمات الطرف الثالث الاجهزة الأساسية لتكنولوجيا المعلومات، مثل الأجهزة الافتراضية والتخزين والشبكات.

الخطر الداخلي Insider Threat

المخاطر التي يتعرض لها أمن المنظمة من قبل الأفراد داخل المنظمة، مثل الموظفين أو المقاولين أو شركاء الأعمال، الذين لديهم إمكانية الوصول إلى معلومات حساسة وقد يعرضونها للخطر عن قصد أو عن غير قصد. يمكن أن تظهر التهديدات الداخلية بأشكال مختلفة، بما في ذلك الوصول غير المصرح إلى البيانات، أو سرقة الملكية الفكرية، أو التخريب، أو الكشف غير المقصود عن معلومات سرية.

انترنت الاشياء Internet of Things

شبكة من الأجهزة المترابطة والمركبة وغيرها من الأشياء المضمنة مع أجهزة الاستشعار، مما يتيح لها جمع البيانات وتبادلها. يمكن لهذه الأجهزة، التي يشار إليها غالبًا بالأجهزة "الذكية"، التواصل مع بعضها البعض ومع الأنظمة المركزية عبر الإنترنت، مما يؤدي إلى إنشاء نظام بيئي واسع من الكيانات المترابطة.

بروتوكول الانترنت Internet Protocol

اي بي وهو اختصار لـ Internet Protocol، عبارة عن مجموعة من القواعد التي تحكم تنسيق البيانات ونقلها عبر الشبكة، مثل الإنترنت. وهو بمثابة بروتوكول الاتصال الأساسي لتوصيل الأجهزة في الشبكة عن طريق تعيين عناوين رقمية فريدة، تُعرف باسم عناوين IP، لكل جهاز.

عنوان الايبي IP Address

هو تسمية مخصصة لكل جهاز متصل بشبكة كمبيوتر تستخدم بروتوكول الإنترنت للاتصال. يعمل عنوان الاي بي كمعرف فريد، ويسمح للأجهزة بإرسال واستقبال البيانات داخل الشبكة وعبر الإنترنت.

حماية الايبي IPSec

أو Internet Protocol Security، عبارة عن مجموعة من البروتوكولات المستخدمة لتأمين وتوثيق اتصالات الإنترنت في طبقة الشبكة. فهو يوفر إطارًا لتشفير وتوثيق حزم البيانات المتبادلة بين الأجهزة داخل الشبكة، مما يضمن سرية وسلامة وصحة المعلومات المرسلة.

مزود الانترنت ISP

شركة أو مؤسسة توفر الوصول إلى الإنترنت والخدمات ذات الصلة للاشخاص والشركات والكيانات الأخرى. يقدم مزودو خدمات الإنترنت أنواعًا مختلفة من الاتصال بالإنترنت، بما في ذلك النطاق العريض، وDSL، والكابلات، والألياف الضوئية، والاتصالات اللاسلكية، مما يسمح للمستخدمين بالاتصال بالإنترنت من منازلهم أو مكاتبهم.

J

جلبريك Jailbreak

عملية التحايل على قيود البرامج التي تفرضها الشركات المصنعة للأجهزة أو أنظمة التشغيل على الأجهزة المحمولة، مثل الهواتف الذكية أو الأجهزة اللوحية. يرتبط كسر الحماية عادةً بأجهزة ابل التي تعمل بنظام ايوس، مثل ايفون وايباد، ويتضمن استغلال الثغرات الأمنية للوصول إلى الجذر أو الامتيازات الإدارية، مما يسمح للمستخدمين بتثبيت تطبيقات طرف ثالث غير مصرح بها، وتخصيص مظهر الجهاز، والوصول إلى الميزات المقيدة .

الارتعاش Jitter

الاختلاف في وقت وصول حزم البيانات عبر الشبكة. وهو مقياس لعدم القدرة على التنبؤ أو عدم انتظام توقيت تسليم الحزمة.

حقيبة القفز Jump Bag

مجموعة جاهزة للاستخدام تحتوي على الأدوات والمعدات والإمدادات الأساسية التي يحملها متخصصو الأمن أو المستجيبون للطوارئ للاستجابة السريعة للحوادث أو حالات الأزمات.

جافا سكربت Javascript

واحدة من اشهر لغات البرمجة في العالم , وتستخدم بشكل أساسي لتعزيز التفاعل والوظائف في متصفحات الويب. تسمح للمطورين بإنشاء واجهات مستخدم ديناميكية وسريعة الاستجابة. ومع ذلك، من منظور الأمن السيبراني، يمكن أن تشكل الجافا سكربت مخاطر أمنية إذا لم تتم إدارتها بشكل صحيح.

التشويش Jamming

التداخل المتعمد والخبيث مع إشارات الاتصالات اللاسلكية، مما يؤدي إلى تعطيل النقل الطبيعي للبيانات بين الأجهزة أو الأنظمة.

K

كيلوجر keylogger

هو اختصار لعبارة keystroke logger او مسجل ضغطات المفاتيح، هو نوع من البرامج أو الأجهزة المصممة لتسجيل ومراقبة ضغطات المفاتيح التي يقوم بها المستخدم على جهاز كمبيوتر أو جهاز إدخال آخر. يقوم برنامج الكيلوجر بالتقاط المعلومات التي يتم إدخالها عبر لوحة المفاتيح، بما في ذلك كلمات المرور وأسماء المستخدمين وأرقام بطاقات الائتمان وغيرها من البيانات الحساسة، دون علم المستخدم. في حين أن بعض برامج الكيلوجر هي أدوات شرعية تُستخدم لاستكشاف أخطاء النظام وإصلاحها أو مراقبة نشاط المستخدم في سياقات محددة، إلا أن الكيلوجر الضار غالبًا ما يتم نشرها من قبل المهاجمين لجمع معلومات سرية خلسة لأغراض خبيثة.

خدمة ادارة المفاتيح KMS

نظام أو منصة مركزية مصممة لإنشاء مفاتيح التشفير وتخزينها وتوزيعها بشكل آمن لعمليات التشفير وفك التشفير. تلعب KMS دورًا في إدارة مفاتيح التشفير، وضمان سريتها وسلامتها وتوافرها. تستخدم المؤسسات KMS لإنشاء دورة حياة مفاتيح آمنة وفعالة، بما في ذلك إنشاء المفاتيح وتوزيعها وتخزينها وتدويرها والتخلص منها.

كيربرس Kerberos

بروتوكول مصادقة شبكة مصمم لتوفير مصادقة آمنة وفعالة لتطبيقات خادم العميل في بيئة حوسبة موزعة.

النواة Kernel

المكون الأساسي لنظام التشغيل الذي يدير موارد النظام ويعمل كوسيط بين التطبيقات والأجهزة. النواة مسؤولة عن المهام الأساسية مثل إدارة العمليات وتخصيص الذاكرة واتصالات الأجهزة.

L

شبكة المنطقة المحلية LAN Local Area Network

شبكة من أجهزة الكمبيوتر والأجهزة المترابطة داخل منطقة جغرافية محدودة، مثل مبنى واحد أو مكتب أو حرم جامعي. تسهل الشبكات المحلية (LAN) مشاركة الموارد، مثل الملفات والطابعات واتصالات الإنترنت، بين الأجهزة المتصلة.

نموذج اللغة الكبير Large Language Model

يشير نموذج اللغة الكبير إلى نظام ذكاء اصطناعي متطور مصمم لفهم وإنشاء نص يشبه الإنسان. يتم تدريب هذه النماذج، مثل GPT-3، على مجموعات بيانات واسعة النطاق تحتوي على أنماط ومعلومات لغوية متنوعة. يشير المصطلح "كبير" إلى العدد الهائل من معلمات النموذج، مما يسمح له بالتقاط الهياكل اللغوية المعقدة والسياق والفروق الدقيقة. تُظهر نماذج اللغات الكبيرة قدرات معالجة متقدمة للغة البشرية، مما يمكنها من أداء مهام مثل إكمال النص والترجمة والتلخيص والإجابة على الأسئلة. لديهم تطبيقات في مجالات مختلفة، بما في ذلك إنشاء المحتوى، وأتمتة دعم العملاء، ومساعدة المستخدمين في المهام التي تنطوي على فهم اللغة والإنتاج. وينطوي تدريب مثل هذه النماذج على الاستفادة من الموارد الحسابية القوية لمعالجة كميات هائلة من البيانات، والمساهمة في قدرتها على فهم اللغات الدقيقة وتوليدها.

السجل Logging

عملية تسجيل الأحداث أو الإجراءات أو الرسائل التي يتم إنشاؤها بواسطة نظام أو تطبيق. تلتقط هذه السجلات المعلومات ذات الصلة مثل الأخطاء أو التحذيرات أو أنشطة المستخدم أو أحداث النظام. يعد التسجيل ممارسة مهمة لمسؤولي النظام والمطورين وموظفي الدعم لأنه يساعد في استكشاف الأخطاء وإصلاحها وتصحيح الأخطاء ومراقبة أداء نظام البرنامج وأمانه.

بروتوكول إعادة التوجيه من الطبقة الثانية L2F Layer 2 Forwarding Protocol

بروتوكول شبكة مصمم لتسهيل الاتصال الآمن والسلس للمستخدمين البعيدين بشبكة خاصة عبر الإنترنت. يعمل L2F في طبقة ارتباط البيانات من OSI ويمكّن المستخدمين من إنشاء اتصالات شبكة خاصة افتراضية (VPN).

التؤام الشرير Evil Twin

شبكة لاسلكية مزيفة تحاكي شبكة واي فاي حقيقية ، تهدف إلى خدع المستخدمين للاتصال بها، معتقدين أنها نقطة وصول موثوقة. تشترك هذه الشبكة الضارة عادةً في اسم مشابه أو متطابق

(SSID) مع شبكة حقيقية ، مثل نقطة اتصال وايفاي عامة، ويتم إعدادها بواسطة المهاجمين للتنصت على بيانات المستخدمين أو تنفيذ هجمات .

الصلاحيات الاقل Least Privilege

مبدأ يدعو إلى تقييد المستخدمين أو العمليات أو الأنظمة بالحد الأدنى من مستوى الوصول أو الأذونات اللازمة لأداء مهامهم المشروعة. ويؤكد المفهوم على قصر الامتيازات على الوظائف الأساسية المطلوبة لدور المستخدم، مما يقلل التأثير المحتمل للحوادث الأمنية أو الإجراءات غير المصرح بها.

بروتوكول LDAP Lightweight Directory Access Protocol

بروتوكول يستخدم على نطاق واسع في بيئات الشبكات للوصول إلى خدمات معلومات الدليل الموزعة وإدارتها.

حالة الارتباط Link State

الحالة التشغيلية الحالية وخصائص رابط الشبكة، وهو مسار اتصال بين نقطتين في الشبكة. تتضمن معلومات حالة الارتباط تفاصيل مثل ما إذا كان الارتباط لأعلى أم لأسفل، وعرض النطاق الترددي الخاص به، وأي مقاييس شبكة مرتبطة به.

قص السجل Log Clipping

الإزالة المتعمدة أو اقتطاع إدخالات السجل في نظام الكمبيوتر أو التطبيق. غالبًا ما ترتبط هذه الممارسة بأنشطة خبيثة تهدف إلى إخفاء أدلة الوصول غير المصرح به أو اختراقات النظام أو الحوادث الأمنية الأخرى.

القنبلة المنطقية Logic bombs

شكل من أشكال البرامج الضارة التي يتم إدخالها بشكل استراتيجي في نظام الكمبيوتر أو تطبيق برمجي بهدف تنفيذ إجراء ضار عند استيفاء شروط محددة.

لينكس Linux

نواة نظام تشغيل مفتوح المصدر ويعمل كمكون أساسي للعديد من أنظمة التشغيل المستندة إلى لينوكس. يشتهر لينكس باستقراره وحمايته وتعدد استخداماته، وقد أصبح الاساس للخوادم والأنظمة المدمجة وبيئات سطح المكتب .

عنوان الاسترجاع Loopback Address

عنوان IP محجوز يسمح للجهاز بالاتصال بنفسه. في الشبكات، يتم استخدام عنوان الاسترجاع لاختبار الشبكة على جهاز محلي دون إشراك شبكات خارجية.

M

تعليم الالة Machine Learning

هو مجال فرعي من الذكاء الاصطناعي (AI) يتضمن تطوير الخوارزميات والنماذج الإحصائية التي تمكن أنظمة الكمبيوتر من أداء المهام دون برمجة دقيقة. يكمن جوهر التعلم الآلي في قدرة الأنظمة على التعلم من البيانات والتعرف على الأنماط واتخاذ القرارات أو التنبؤات بناءً على هذا التعلم. وهو يشمل تقنيات مختلفة، بما في ذلك التعلم الخاضع للإشراف، والتعلم غير الخاضع للإشراف، والتعلم المعزز، وكل منها يخدم أغراضًا مختلفة مثل التصنيف، والتجميع، والتحسين. في التعلم الآلي، تعمل النماذج على تحسين أدائها بمرور الوقت عن طريق ضبط وتحسين معلماتها من خلال التعرض للبيانات الجديدة.

ماكرو Macro

يشير الماكرو إلى مجموعة من الإرشادات أو الأوامر المحددة مسبقًا والتي تمثل سلسلة من الإجراءات التي سيتم تنفيذها. تُستخدم وحدات الماكرو بشكل شائع لأتمتة المهام المتكررة وتبسيط العمليات المعقدة داخل التطبيقات مثل معالجات النصوص أو برامج جداول البيانات أو البرامج الأخرى.

الاعلانات الضارة Malvertising

عبارة عن مجموعة من الإعلانات المصممة عمدًا لتقديم برامج ضارة أو استغلال نقاط الضعف في كمبيوتر المستخدم أو جهازه. قد تظهر الإعلانات الضارة على المواقع ويمكن أن تستغل ثغرات التسليم المختلفة، مثل اللافتات أو النوافذ المنبثقة أو البرامج النصية المضمنة. الهدف من الإعلانات الضارة هو خداع المستخدمين للتفاعل مع الإعلانات، مما يؤدي إلى التثبيت غير المقصود للبرامج الضارة على أنظمتهم.

المالوير Malware

اختصار لعبارة malicious software او البرامج الضارة، هي مصطلح واسع يشمل أي نوع من البرامج المصممة عمدًا لاغراض خبيثة مثل الضرر بأنظمة الكمبيوتر أو الشبكات أو المستخدمين أو استغلالها أو تعريضها للخطر.

عنوان التحكم في الوصول إلى الوسائط MAC Media Access Control

معرف فريد يتم تعيينه لوحدة تحكم واجهة الشبكة (NIC) للاتصال على الشبكة. عادةً ما يتم تعيين هذا العنوان، المعروف أيضًا باسم عنوان الجهاز أو العنوان الفعلي، من قبل الشركة المصنعة للجهاز ويستخدم لتعريف الجهاز بشكل فريد داخل مقطع الشبكة.

هجوم الرجل في الوسط MitM Man-in-the-Middle Attack

هجوم أمني حيث يعترض المهاجم ويحتمل أن يغير الاتصال بين طرفين دون علمهما. يضع المهاجم نفسه بين الكيانات المتصلة، ويعمل كوسيط. يمكن للمهاجم التنصت على الاتصالات، أو تعديل البيانات التي يتم تبادلها، أو إدخال محتوى ضار.

هجوم التنكر Masquerade Attack

نوع من التهديد الأمني حيث يتنكر المهاجم كمستخدم أو نظام حقيقي للحصول على وصول أو خداع الآخرين داخل الشبكة.

ميتاسبلويت Metasploit

إطار عمل احترافي لاختبار الاختراق مفتوح المصدر يستخدم على نطاق واسع في مجال الأمن السيبراني لإجراء تقييمات الأمان والقرصنة الأخلاقية وأبحاث الثغرات الأمنية.

مفهوم MITRE ATT&CK

قاعدة معرفية وإطار يوفر خريطة شاملة ومفصلة للتكتيكات والتقنيات والإجراءات (TTPs) التي يستخدمها المهاجم خلال المراحل المختلفة للهجوم السيبراني.

نظام الماك macOS

نظام تشغيل خاص تم تطويره بواسطة شركة ابل لأجهزة كمبيوتر ماكنتوش الخاص بها. يشتهر نظام ماك بواجهته سهلة الاستخدام وجمالياته وتكامله مع أجهزة ابل ، وقد تم تصميمه لتوفير تجربة حوسبة سلسة وآمنة.

خوارزمية MD5

خوارزمية تجزئة تشفيرية تنتج قيمة تجزئة ذات حجم ثابت 128 بت، ويتم التعبير عنها عادةً كرقم سداسي عشري مكون من 32 حرفًا.

مقاييس الفعالية MOE Measures of Effectiveness

المقاييس الكمية أو النوعية المستخدمة لتقييم نجاح وتأثير الحلول والاستراتيجيات الأمنية داخل المنظمة.

الثقافة الاحادية Monoculture

الاستخدام لمجموعة واحدة من التقنيات أو المنصات أو البرامج عبر عدد كبير من الأنظمة أو المنظمات.

دودة موريس Morris Worm

واحدة من أقدم الأمثلة على المالوير المصممة للانتشار عبر شبكات الكمبيوتر. كان الهدف من الدودة أن تكون بمثابة تجربة لقياس حجم الإنترنت ولكنها تسببت عن غير قصد في اضطراب واسع . لقد استغلت نقاط الضعف في الأنظمة المستندة إلى يونكس، وكررت نفسها وأثقلت أجهزة الكمبيوتر، مما أدى إلى تباطؤ كبير في الأنظمة المتصلة بالشبكة.

البث المتعدد Multi-Cast

نقل البيانات من مرسل واحد إلى عدة مستلمين في وقت واحد. على عكس البث الأحادي، الذي يرسل البيانات من مرسل واحد إلى مستلم واحد محدد، أو البث، الذي يرسل البيانات إلى جميع الأجهزة الموجودة على الشبكة، يكون البث المتعدد أكثر كفاءة في عرض النطاق الترددي لأنه يستهدف مجموعة مختارة من المستلمين.

تعدد الارسال Multiplexing

أسلوب في الشبكات والاتصالات يسمح بدمج إشارات أو تدفقات بيانات متعددة ونقلها عبر قناة اتصال مشتركة. تتيح هذه العملية الاستخدام الفعال لموارد الشبكة عن طريق إرسال تدفقات بيانات متعددة بشكل متزامن.

ادارة الاجهزة المحمولة MDM Mobile Device Management

نهج شامل لإدارة الأجهزة المحمولة والتحكم فيها، مثل الهواتف الذكية والأجهزة اللوحية، داخل المؤسسة. تتيح حلول MDM لمسؤولي تكنولوجيا المعلومات مراقبة الأجهزة المحمولة وتأمينها وإدارتها عبر منصات وأنظمة تشغيل متنوعة.

ميتا ديتا Metadata

ميتا ديتا او البيانات الوصفية هي المعلومات التي تصف البيانات الأخرى. وهي تتضمن مجموعة من المعلومات المنظمة التي تصف الجوانب المختلفة لجزء من البيانات، مثل أصلها أو تنسيقها أو تاريخ

إنشائها أو تأليفها أو موقعها. في سياق المحتوى الرقمي، يمكن أن تشمل البيانات التعريفية أيضًا تفاصيل حول خصائص الملف، أو بنية المستند، أو حتى معلومات حول كيفية ترابط البيانات.

التخفيف Mitigation

الإجراءات والحلول الإستراتيجية المتخذة لتقليل أو تخفيف تأثير التهديدات أو المخاطر المحتملة. الهدف من التخفيف هو المعالجة الاستباقية وتقليل الآثار الضارة للمخاطر المحددة على الأفراد أو المنظمات أو الأنظمة.

المراقبة Monitoring

المراقبة المستمرة والمنهجية لمختلف الجوانب داخل الشبكة أو النظام أو التطبيق لتقييم الأداء واكتشاف الحالات المشبوهة وضمان الأداء الأمثل. تتضمن هذه العملية جمع البيانات ذات الصلة وتحليلها وتفسيرها، مثل مقاييس النظام وسجلات الأخطاء وأنشطة المستخدم. تعد المراقبة ضرورية لتحديد المشاكل ومعالجتها على الفور، وتحسين استخدام الموارد، ومنع الاضطرابات أو الفشل المحتمل.

N

المركز البريطاني للامن السيبراني National Cyber Security Centre

منظمة حكومية مكرسة لتعزيز وضع الأمن السيبراني في المملكة المتحدة. يلعب المركز دورًا هاما في توفير التوجيه والخبرة والدعم في مجال الأمن السيبراني للوكالات الحكومية وكيانات البنية التحتية الحيوية والقطاع الخاص. وتشمل مهمتها تطوير سياسات الأمن السيبراني، وتوفير المعلومات المتعلقة بالتهديدات، وتنسيق الاستجابة للحوادث، ونشر أفضل الممارسات للحماية من التهديدات السيبرانية.

الشبكة Network

مجموعة من الكمبيوتر أو الأجهزة أو الأنظمة المترابطة التي تتواصل وتتشارك الموارد مع بعضها البعض. يمكن أن تكون الشبكات مادية، مثل الاتصالات السلكية أو اللاسلكية التي تربط الأجهزة القريبة، أو افتراضية، مثل الاتصالات التي يتم إنشاؤها عبر الإنترنت. الغرض من الشبكة هو تمكين تبادل البيانات أو المعلومات أو الموارد بين مكوناتها.

تقطيع الشبكة Network slicing

مفهوم في الاتصالات والشبكات يتضمن إنشاء شبكات افتراضية ومعزولة متعددة ضمن بنية تحتية فعلية واحدة للشبكة. تسمح الخدمة بتخصيص شبكة محددة ومعلمات الأداء والوظائف لتلبية المتطلبات المتنوعة لمختلف الخدمات أو مجموعات المستخدمين.

ترجمة عنوان الشبكة NAT Network Address Translation

إحدى تقنيات الشبكات الأساسية المستخدمة لتعزيز الأمان وإدارة عناوين IPv4.

المعهد الوطني للمعايير والتكنلوجيا National Institute of Standards and Technology - NIST

وكالة اتحادية أمريكية بارزة تلعب دورًا اساسيا في تطوير وتنفيذ المعايير والمبادئ التوجيهية وأفضل الممارسات عبر مختلف الصناعات، بما في ذلك أمن المعلومات.

قناع الشبكة Netmask

قيمة رقمية تستخدم في شبكات الكمبيوتر لتحديد جزء عنوان IP الذي يمثل الشبكة والجزء الذي يمثل الأجهزة المضيفة داخل تلك الشبكة.

رسم الشبكة Network Mapping

عملية لاكتشاف ورسم البنية والاتصالات داخل شبكة الكمبيوتر. يستخدم متخصصو الأمن رسم خرائط الشبكة كعنصر في تقييم نقاط الضعف واختبار الاختراق للحصول على رؤى شاملة حول بنية الشبكة.

حنفية الشبكة Network Taps

أجهزة متخصصة تستخدم في الأمن السيبراني ومراقبة الشبكة لاعتراض حركة مرور الشبكة ونسخها.

نظام كشف التسلل المعتمد على الشبكة Network-Based Intrusion Detection System - IDS

آلية للأمن السيبراني مصممة لمراقبة وتحليل حركة مرور الشبكة بحثًا عن علامات الأنشطة المشبوهة أو الضارة. يعمل هذا النوع من IDS على مستوى الشبكة، حيث يقوم بفحص الحزم وأنماط حركة المرور لتحديد التهديدات الأمنية المحتملة.

الان ماب Nmap

أداة قوية مفتوحة المصدر تستخدم لاكتشاف الشبكة والتدقيق الأمني. تم تطوير الان ماب لاستكشاف الشبكات واكتشاف الاستضافة وتحديد المنافذ والخدمات المفتوحة، وهو يوفر معلومات تفصيلية حول الأجهزة الموجودة على الشبكة.

بروتوكول وقت الشبكة NTP Network Time Protocol

بروتوكول شبكات يستخدم لمزامنة ساعات أنظمة الكمبيوتر عبر الشبكة. يمكّن NTP الأجهزة من الحفاظ على وقت دقيق ومتزامن، وهو أمر اساسي لمختلف العمليات، بما في ذلك تسجيل الأحداث والمصادقة وضمان الإجراءات المنسقة في الأنظمة .

عدم التنصل Non-Repudiation

مفهوم أمني يضمن سلامة وصحة المعاملات الرقمية من خلال منع الأطراف المعنية من إنكار أفعالهم أو صحة المعاملة.

الجلسة الفارغة Null Session

اتصال مجهول تم إنشاؤه لمشاركة شبكة ويندوز دون الحاجة إلى أي شكل من أشكال مصادقة المستخدم أو بيانات الاعتماد.

O

اطار OAuth

يعني OAuth، أو Open Authorization، هو إطار مصادقة مفتوح يسمح لتطبيقات الطرف الثالث بالوصول بشكل آمن إلى موارد المستخدم دون الكشف عن بيانات الاعتماد الخاصة به. يعمل OAuth من خلال تمكين المستخدمين من منح وصول محدود إلى مواردهم الموجودة على موقع ويب أو تطبيق واحد إلى موقع ويب أو تطبيق آخر.

شركات OEM

الشركة المصنعة للمعدات الأصلية، هي شركة تنتج وتبيع المنتجات أو المكونات التي تستخدمها شركة أخرى في منتجها النهائي. في هذا السياق، يصف المصطلح عادة الشركة المصنعة للمكونات المادية أو البرمجية التي يتم دمجها في المنتج النهائي بواسطة شركة مختلفة. غالبًا ما يتخصص مصنعو المعدات الأصلية في مكونات أو تقنيات معينة، ويقومون بتزويدها لمختلف الصناعات. يتم بعد ذلك إعادة تسمية المنتجات المقدمة من قبل مصنعي المعدات الأصلية أو دمجها في عروض الشركة المشترية.

المصدر المفتوح Open-source

نموذج تطوير وتوزيع البرامج حيث يتم إتاحة الكود للبرنامج مجانًا للجميع ، مما يسمح للمستخدمين بعرض الكود وتعديله وتوزيعه. يشجع هذا النهج التعاون والشفافية، حيث يساهم مجتمع المطورين بشكل جماعي في تحسين البرنامج وابتكاره. عادةً ما يتم ترخيص البرامج مفتوحة المصدر بطريقة تمنح المستخدمين حرية استخدام البرنامج وتعديله وتوزيعه وكود مصدره. ويعزز هذا النموذج بيئة تطوير تعاونية وشاملة، مما يؤدي إلى إنشاء حلول قوية وفعالة من حيث التكلفة في كثير من الأحيان. تتبع العديد من البرامج المستخدمة على نطاق واسع، بما في ذلك أنظمة التشغيل مثل لينكس، وخوادم الويب مثل اباتشي، ولغات البرمجة مثل بايثون، نموذج المصدر المفتوح.

استخبارات المصادر المفتوحة OSINT Open Source Intelligence

جمع وتحليل المعلومات من المصادر المتاحة للجميع لجمع الأفكار وتقييم المخاطر وتعزيز الوعي الظرفي في مجال الأمن السيبراني والاستخبارات.

الامن التشغيلي Operational security

الأمن التشغيلي، الذي غالبًا ما يتم اختصاره بـ OPSEC، هي العملية المنهجية والاستراتيجية لتحديد المعلومات الحساسة والتحكم فيها وحمايتها لمنع الخصوم أو الكيانات غير المصرح لها من الحصول على معلومات استخباراتية يمكن أن تعرض أمن العملية أو نجاحها للخطر.

نظام التشغيل Operating System OS

هو أحد مكونات الأساسية التي تعمل كوسيط بين أجهزة الكمبيوتر وتطبيقات المستخدم، وإدارة وتنسيق موارد النظام المختلفة لتمكين التنفيذ الفعال والآمن للمهام. يوفر واجهة مستخدم للتفاعل ويسهل تنفيذ البرامج من خلال تخصيص وإدارة وحدة المعالجة المركزية والذاكرة والتخزين .يدعم نظام التشغيل الوظائف الأساسية مثل جدولة العمليات، وإدارة الملفات، واتصالات الشبكة. تتضمن أمثلة أنظمة التشغيل الشهيرة مايكروسوفت ويندوز , ماك ولينكس.

التشفير الاحادي One-Way Encryption

عملية تشفير تقوم بتحويل البيانات إلى سلسلة ذات حجم ثابت من الأحرف، عادةً ما تكون قيمة تجزئة، باستخدام خوارزمية. على عكس التشفير ثنائي الاتجاه، الذي يتضمن عمليات عكسية تتطلب مفتاحًا للتشفير وفك التشفير، تم تصميم التشفير أحادي الاتجاه بحيث لا رجعة فيه.

مفهوم OSPF Open Shortest Path First

فتح أقصر مسار أولاً (OSPF) هو بروتوكول توجيه شائع الاستخدام في شبكات الكمبيوتر لتسهيل تبادل معلومات التوجيه بين أجهزة التوجيه وتحديد المسارات الأكثر كفاءة لنقل البيانات.

نموذج الربط البيني للأنظمة المفتوحة Open Systems Interconnection OSI

إطار مهم جدا في الشبكات يعمل على توحيد وتنظيم وظائف نظام الاتصالات أو الحوسبة في سبع طبقات . تتوافق كل طبقة في نموذج OSI مع مجموعة محددة من الوظائف، ويعمل النموذج لتصميم وتنفيذ وفهم بنيات الشبكة.

الحمل الزائد Overload

الحالة التي يتعرض فيها النظام أو مورد الشبكة لطلب أو تحميل يتجاوز قدرته، مما يؤدي إلى تدهور الأداء أو فشله.

المصدر المفتوح Open source

منهج تطوير حيث يتم إتاحة الكود المصدري للبرنامج مجانًا ويمكن للعامة الوصول إليه. وهذا يعني أن المستخدمين ليس لديهم الحق في استخدام البرنامج فحسب، بل يحق لهم أيضًا عرض كود المصدر الخاص به وتعديله وتوزيعه.

مشروع OWASP

منظمة غير ربحية تركز على تحسين أمان البرامج. يوفر OWASP الموارد والأدوات والمبادئ التوجيهية لمساعدة المؤسسات والمطورين على بناء تطبيقات ويب أكثر أمانًا.

التكنلوجيا التشغيلية Operational Technology OT

أنظمة الأجهزة والبرامج التي تدير وتتحكم في العمليات المادية في مختلف الصناعات، مثل التصنيع والطاقة والبنية التحتية. على عكس تكنولوجيا المعلومات (IT)، التي تتعامل في المقام الأول مع البيانات ومعالجة المعلومات، تركز التكنولوجيا التشغيلية (OT) على التحكم في الأجهزة والعمليات المادية وأتمتتها. تشمل التكنولوجيا التشغيلية مجموعة واسعة من التقنيات، بما في ذلك أنظمة التحكم الصناعية وأجهزة التحكم المنطقية القابلة للبرمجة وأجهزة الاستشعار والأجهزة الأخرى التي تراقب العمليات الصناعية وتتحكم فيها.

P

بايثون Python

لغة برمجة عالية المستوى ومتعددة الاستخدامات معروفة بقابليتها للقراءة وسهولة الاستخدام. يتم استخدام بايثون في العديد من تطبيقات الأمن السيبراني، بما في ذلك البرمجة والأتمتة وتطوير أدوات الأمان.

عبارة المرور PassPhrase

عبارة عن سلسلة من الكلمات أو مجموعة من الكلمات والأحرف المستخدمة كبيانات اعتماد أمنية لمصادقة هوية المستخدم والوصول إلى نظام أو شبكة أو بيانات مشفرة. على عكس كلمات المرور التقليدية، عادةً ما تكون عبارات المرور أطول وتتكون من كلمات متعددة أو عبارة ذات معنى، مما يجعلها أكثر مرونة ضد الهجمات.

كلمة المرور Password

هي سلسلة سرية وفردية من الحروف والأرقام والرموز، والتي تعمل كوسيلة للتحقق من هوية المستخدم للوصول إلى نظام كمبيوتر أو تطبيق أو حساب رقمي. تُستخدم كلمات المرور عادةً كإجراء أمني، وتعمل كحاجز أمام الدخول غير المصرح به، مما يساعد على حماية المعلومات الحساسة وضمان خصوصية بيانات المستخدم.

مدير كلمات المرور Password Manager

هو أداة برمجية مصممة لتخزين بيانات اعتماد تسجيل الدخول المختلفة للمستخدم وتنظيمها وإدارتها بشكل آمن، مثل أسماء المستخدمين وكلمات المرور لحسابات وخدمات مختلفة عبر الإنترنت.

نشر كلمة المرور Password spraying

أسلوب هجوم إلكتروني حيث يحاول المهاجم الحصول على وصول إلى نظام أو شبكة من خلال تجربة عدد قليل من كلمات المرور شائعة الاستخدام بشكل منهجي ضد العديد من حسابات المستخدمين.

التصحيح Patching

عملية تطبيق التحديثات أو الإصلاحات أو التعديلات على البرامج أو أنظمة التشغيل أو التطبيقات لمعالجة نقاط الضعف أو تحسين الوظائف أو حل الأخطاء.

بيغاسوس Pegasus

برنامج تجسس معقد للغاية ومثير للجدل طورته شركة NSO Group. يشتهر بقدراته المتقدمة، وقد تم تصميمه لإصابة الأجهزة المحمولة والتحكم فيها عن بعد، مما يمنح مشغليه إمكانية الوصول إلى كميات كبيرة من البيانات الشخصية، بما في ذلك المكالمات والرسائل ورسائل البريد الإلكتروني ونشاط الجهاز.

معلومات التعريف الشخصية Personally Identifiable Information PII

معلومات يمكن استخدامها لتحديد هوية الفرد. ويشمل ذلك بيانات مثل الأسماء والعناوين وأرقام الضمان الاجتماعي والسجلات المالية والبيانات البيومترية وغيرها من التفاصيل التي يمكن ربطها بشخص معين.

ما بعد الاختراق Post-compromise

حادث سيبراني يحدث بعد تعرض نظام أو شبكة للاختراق عن طريق الوصول غير المصرح أو البرامج الضارة أو التهديدات الأمنية الأخرى. خلال هذه المرحلة، يهدف المهاجم في إلى الحفاظ على وجوده المستمر، وتصعيد الصلاحيات، وتحقيق أهدافها داخل البيئة المعرضة للخطر.

البرامج الغير مرغوب فيها Potentially Unwanted Program PUP

برامج تعرض سلوكيات أو ميزات قد يعتبرها المستخدمون غير مرغوب فيها أو متطفلة، على الرغم من عدم تصنيفها على أنه برامج ضار بشكل علني. غالبًا ما تأتي البرامج PUPs مرفقة بتنزيلات برامج ثانية أو يتم إخفاءها كتطبيقات مفيدة ولكنها قد تشارك في أنشطة مثل عرض إعلانات أو جمع بيانات المستخدم دون موافقة أو تغيير إعدادات المتصفح.

الصلاحيات Privilege

مستوى الوصول أو الحقوق أو الأذونات الممنوحة للمستخدم أو النظام أو التطبيق داخل بيئة تكنولوجيا المعلومات.

الحزمة Packet

وحدة منفصلة من البيانات المنقولة عبر الشبكة. وهي لبنة البناء الأساسية للاتصالات في شبكات تبديل الحزم، حيث يتم تقسيم كميات كبيرة من البيانات إلى حزم أصغر يمكن التحكم فيها من أجل النقل الفعال.

شبكة تبديل الحزم Packet Switched Network

نوع من شبكات البيانات حيث يتم تقسيم المعلومات إلى حزم منفصلة قبل الإرسال ثم يتم توجيهها بشكل مستقل عبر الشبكة بناءً على عناوين الوجهة.

الاقسام Partitions

أقسام منفصلة داخل نظام كمبيوتر أو شبكة تتيح عزل المكونات أو التطبيقات أو مجموعات البيانات المختلفة. تعمل الأقسام كوسيلة لتعزيز الأمن من خلال تقييد الوصول وتخفيف التأثير المحتمل للحوادث الأمنية.

تصعيد الصلاحيات Privilege Escalation

رفع لامتيازات المستخدم أو النظام، مما يمكّن المهاجم من الوصول إلى مستويات أعلى من الأذونات التي تم تعيينها في الأصل.

بروتوكول مصادقة كلمات المرور PAP Password Authentication Protocol

أحد أساليب المصادقة القديمة المستخدمة بشكل شائع في الشبكات، خاصة في سياق اتصالات بروتوكول نقطة إلى نقطة. يعمل بروتوكول PAP عن طريق إرسال بيانات اعتماد المستخدم، مثل اسم المستخدم وكلمة المرور، عبر الشبكة بتنسيق واضح وسهل القراءة.

تكريك كلمة المرور Password Cracking

محاولة مهاجم فك تشفير كلمة المرور أو اكتشافها، عادةً من خلال أدوات أو تقنيات آلية. الهدف الأساسي من تكريك كلمة المرور هو الوصول إلى نظام أو شبكة أو حساب من خلال استغلال الثغرات الأمنية في أمان كلمة المرور.

اختلاس كلمة المرور Password sniffing

يتضمن اعتراض مراقبة حركة الشبكة لالتقاط المعلومات الحساسة، وتحديدًا أسماء المستخدمين وكلمات المرور.

اللغم Payload

المكون الضار أو الاكواد البرمجية الموجودة ضمن التهديد ، مثل فيروس متنقل أو حصان طروادة، المصمم لتنفيذ إجراءات محددة على نظام مستهدف بعد نجاح التسلل .

التقليب Permutation

ترتيب اندماجي للعناصر، مثل الأحرف أو الأرقام بترتيب معين. في سياق أمان كلمة المرور، تستخدم في إنشاء كلمات مرور قوية وغير متوقعة.

جدران الحماية الشخصية Personal Firewalls

برامج أمنية أو أجهزة مصممة لحماية أنظمة الكمبيوتر الفردية من الوصول والأنشطة الضارة. تعمل جدران الحماية هذه على مراقبة حركة المرور الواردة والصادرة، وتفرض قواعد أمان محددة مسبقًا للسماح بحزم البيانات أو حظرها بناءً على مصدرها ووجهتها ونوعها.

التزييف Pharming

هجوم إلكتروني يقوم فيه المهاجم بالتلاعب بنظام اسم النطاق (DNS) أو اختراقه لإعادة توجيه المستخدمين إلى مواقع ويب اخرى دون علمهم أو موافقتهم.

هجوم Ping of Death

هجوم يستغل نقاط الضعف في بروتوكولات الشبكة، وخاصة بروتوكول رسائل التحكم في الإنترنت (ICMP)، لتعطيل أنظمة الكمبيوتر.

بروتوكول PPP Point-to-Point Protocol

بروتوكول اتصالات الشبكة يُستخدم بشكل شائع في إنشاء اتصال مباشر بين نقطتين، عادةً عبر خطوط اتصال تسلسلية أو روابط مخصصة أخرى.

تعدد الاشكال Polymorphism

مفهوم برمجي حيث يمكن لوظيفة أو طريقة أو نوع بيانات واحد أن يعمل على أنواع مختلفة من البيانات أو الكائنات.

المنفذ Port

نقطة نهاية معينة أو نقطة نهاية اتصال في شبكة الكمبيوتر. يتم تحديد المنافذ بقيم رقمية، وهي تسهل تبادل البيانات بين الأجهزة أو الخدمات المختلفة داخل الشبكة.

فحص المنافذ Port Scan

تقنية فحص يستخدمها المهاجمون أو متخصصو الأمن لتحديد المنافذ المفتوحة على نظام الكمبيوتر أو الشبكة. تتضمن العملية إجراء فحص منظم لمجموعة من منافذ الشبكة على نظام مستهدف لتحديد المنافذ النشطة والتي يحتمل أن تكون عرضة للاستغلال.

بروتوكول مكتب البريد POP3 Post Office Protocol, Version 3

بروتوكول استرداد البريد الإلكتروني المستخدم في اتصالات الشبكة، يسهل POP3 تنزيل رسائل البريد الإلكتروني من خادم البريد إلى العميل.

البروكسي Proxy Server

يعمل كوسيط بين الأجهزة والإنترنت، ويخدم اشياء مختلفة في اتصالات الشبكة وأمنها. يعيد توجيه الطلبات من العملاء إلى خوادم الويب وينقل الاستجابات مرة أخرى إلى العملاء.

المفتاح العام Public Key

مكون أساسي في خوارزميات التشفير غير المتماثلة. وهو جزء من زوج مفاتيح إلى جانب المفتاح الخاص . يتم توزيع المفتاح العام بحرية واستخدامه للتشفير، مما يسمح لأي شخص بإرسال رسائل أو بيانات آمنة إلى مالك المفتاح الخاص المقابل. في حين أن البيانات المشفرة باستخدام المفتاح العام لا يمكن فك تشفيرها إلا بواسطة المفتاح الخاص، فإن المفتاح العام نفسه لا يعرض أمان النظام للخطر.

البنية التحتية للمفتاح العام Public Key Infrastructure PKI

إطار عمل شامل يدير إنشاء وتوزيع واستخدام وتخزين وإلغاء الشهادات الرقمية والمفاتيح العامة والخاصة المرتبطة بها.

اختبار الاختراق Pentest

تقييم منظم ومنهجي ومحاكى للأمن السيبراني يجريه المخترق الاخلاقي لتقييم أمان نظام الكمبيوتر أو الشبكة أو التطبيق. الهدف الأساسي من اختبار الاختراق هو تحديد نقاط الضعف ونقاط الضعف التي يمكن للجهات الفاعلة الضارة استغلالها.

امان الطاقم Personnel security

مجموعة السياسات والإجراءات والحلول التي تنفذها المنظمات للحماية من المخاطر التي يشكلها الأفراد داخل القوى العاملة لديها.

مفهوم Pharming

أسلوب هجوم إلكتروني يتضمن إعادة توجيه حركة موقع الويب إلى مواقع ويب مزيفة أو ضارة دون علمهم أو موافقتهم.

التصيد Phishing

أسلوب للهجوم عبر الإنترنت يستخدم فيه المهاجمون اتصالات احتيالية، غالبًا في شكل رسائل بريد إلكتروني أو رسائل أو مواقع ويب، لخدع الناس لإفشاء معلومات حساسة مثل أسماء المستخدمين أو كلمات المرور أو التفاصيل المالية.

الامن المادي Physical security

الحلول والاستراتيجيات المطبقة لحماية الأصول الملموسة للمنظمة وموظفيها ومرافقها من الوصول أو الضرر أو الأذى. وهو يشمل مجموعة واسعة من حلول الحماية، بما في ذلك أنظمة التحكم في الوصول، وأنظمة المراقبة، وأفراد الأمن، والحواجز، والضوابط البيئية.

النص العادي Plaintext

البيانات أو المعلومات غير المشفرة والتي يمكن قراءتها بسهولة والتي يتم تقديمها في شكلها الأصلي الذي يمكن للإنسان قراءته. في سياق التشفير وأمن المعلومات، النص العادي هو عكس النص المشفر، وهو البيانات التي خضعت للتشفير لحمايتها من الوصول غير المصرح به.

المنصة Platform

مجموعة شاملة ومتكاملة من مكونات البرامج والأجهزة التي توفر أساسًا لتطوير وتنفيذ التطبيقات أو الخدمات أو الحلول. غالبًا ما تشتمل الأنظمة الأساسية على نظام تشغيل وبرامج وسيطة وأطر برمجية أخرى تمكن المطورين من إنشاء ونشر وإدارة أنواع مختلفة من تطبيقات البرامج

المنصة كخدمة Platform as a Service

هو نموذج خدمة سحابية يوفر نظامًا أساسيًا شاملاً يسمح للمطورين ببناء التطبيقات ونشرها وإدارتها دون تعقيدات إدارة البنية التحتية. توفر PaaS بيئة جاهزة تحتوي على أدوات ومكتبات وخدمات، مما يؤدي إلى تبسيط عملية التطوير والسماح للمطورين بالتركيز على وظائف البرمجة والتطبيقات.

باورشل PowerShell

عبارة عن سطر أوامر ولغة برمجة نصية قوية وقابلة للتوسيع تم تطويرها بواسطة مايركوسوفت لأتمتة المهام وإدارة التكوين وإدارة النظام على أنظمة تشغيل ويندوز.

البروتوكول Protocol

مجموعة من القواعد والاصطلاحات المحددة مسبقًا والتي تحدد كيفية إرسال البيانات واستقبالها بين الأجهزة أو الأنظمة في شبكة الكمبيوتر. تحكم هذه القواعد تنسيق البيانات المتبادلة وتوقيتها وتسلسلها والتحكم في الأخطاء فيها لضمان الاتصال الموثوق.

Q

الكاز QAZ

نوع من فيروسات الكمبيوتر أو البرامج الضارة. ينتشرعادةً من خلال مرفقات البريد الإلكتروني الضارة أو تنزيلات البرامج المصابة، ويعرض سلوكيات ضارة مختلفة، بما في ذلك سرقة البيانات وتعطيل النظام والوصول.

تصيد الكيو ار QR code phishing

هجوم الإلكتروني يستغل رموز الاستجابة السريعة (QR) لخداع الناس لزيارة مواقع ويب ملغومة أو تنزيل محتوى ضار. في هذا النوع من هجمات التصيد ، يقوم المهاجم بإنشاء رموز QR التي، عند مسحها بواسطة كاميرا الجهاز المحمول، تعيد توجيه المستخدمين إلى مواقع الويب المصممة لسرقة المعلومات.

R

فيروس الفدية Ransomware

نوع من المالوير المصممة لتشفير ملفات المستخدم أو منع الوصول إلى نظام الكمبيوتر الخاص به، مما يجعله غير قابل للاستخدام حتى يتم دفع فدية لمرتكبي الجريمة. عادةً ما يطلب المهاجمون الدفع بالعملة المشفرة لتزويد الضحية بمفتاح فك التشفير أو لفتح النظام المخترق.

فيروس الفدية كخدمة Ransomware as a Service

هي نموذج أعمال للهاكرز حيث يمكن لذوي الخبرة الفنية المحدودة استئجار أو شراء برامج الفدية من مطورين أو موزعين أكثر مهارة. في هذا العمل غير المشروع ، يقوم المطورون بإنشاء برامج الفدية وصيانتها، وتقديمها كخدمة للمجرمين الأقل كفاءة من الناحية التقنية، الذين يقومون بعد ذلك بنشر البرامج الضارة ضد الأهداف.

حالة السباق Race Condition

ثغرة أمنية تحدث عندما يعتمد سلوك نظام برمجي على توقيت الأحداث أو تسلسلها. وينشأ ذلك عندما تحاول عمليات أو سلاسل عمليات متعددة الوصول إلى الموارد المشتركة أو تعديل البيانات بشكل متزامن، مما يؤدي إلى نتائج غير مقصودة وغير متوقعة.

قائمة قوس القزح Rainbow Table

جدول محسوب مسبقًا يستخدم في التشفير لتكسير اجزاء كلمة المرور بكفاءة.

الاستطلاع Reconnaissance

المرحلة الأولى من الهجوم السيبراني حيث يقوم المهاجم بجمع معلومات حول نظام أو شبكة أو منظمة مستهدفة. تتضمن هذه المرحلة أساليب جمع البيانات مثل جمع المعلومات الاستخبارية مفتوحة المصدر، ومسح الشبكة، والتحقيق، لتحديد نقاط الضعف المحتملة، وبنية النظام، والأصول.

السجل Registry

قاعدة بيانات مركزية وهرمية تستخدمها أنظمة التشغيل لتخزين إعدادات وتفضيلات النظام والمعلومات حول التطبيقات والأجهزة المثبتة.

تحليل الانحدار Regression Analysis

طريقة إحصائية تستخدم لتقييم ونمذجة العلاقة بين المتغيرات. يمكن تطبيق تحليل الانحدار لفحص تأثير العوامل المختلفة على مقاييس الأمان، مثل تحديد الارتباطات بين اعدادات النظام وسلوكيات المستخدم والحوادث الأمنية.

طلب التعليق RFC Request for Comment

سلسلة مستندات يحتفظ بها فريق عمل هندسة الإنترنت (IETF) والتي تشمل المواصفات والإرشادات والمقترحات المتعلقة بمعايير الإنترنت و البروتوكولات.

استنفاذ الموارد Resource Exhaustion

نوع من الهجوم حيث يستهلك المهاجم أو يستنزف موارد النظام الهامة مثل وحدة المعالجة المركزية أو الذاكرة لتقليل أداء أو توفر الجهاز المستهدف.

الفريق الاحمر Red Team

مجموعة من المهنيين المهرة المكلفين بمحاكاة أدوار المهاجمين لتقييم واختبار الحلول الأمنية لمنظمة أو نظام أو عملية.

المقاومة Resilience

قدرة النظام أو المنظمة أو البنية التحتية على الصمود والتكيف والتعافي من الظروف المعاكسة أو الاضطرابات أو الحوادث الأمنية. يتميز النظام المرن بقدرته على استيعاب تأثير الأحداث غير المتوقعة، والحفاظ على الوظائف الأساسية، والعودة بسرعة إلى حالة التشغيل العادية.

فيروس طروادة للتحكم RAT Remote Access Trojan

نوع من البرامج التي توفر وصولاً سريًا إلى كمبيوتر الضحية أو شبكته. يعمل بشكل خفي، مما يتيح للمهاجم التحكم عن بعد والمراقبة. بمجرد تثبيته على نظام مستهدف يقوم بإنشاء اتصال بخادم القيادة والسيطرة، مما يسمح للمهاجم بتنفيذ الأوامر، والتقاط ضغطات المفاتيح، والوصول إلى الملفات، والتحكم في جهاز الضحية من مكان بعيد

الهندسة العكسية Reverse Engineering

عملية تشريح وتحليل تطبيق برمجي أو جهاز أو نظام لفهم أعماله الداخلية ووظائفه وتصميمه. قد يستخدم متخصصو الأمن تقنيات الهندسة العكسية للكشف عن نقاط الضعف وتحديد المخاطر الأمنية المحتملة وتطوير إجراءات مضادة ضد الأنشطة الخبيثة.

تجنب المخاطر Risk Averse

ميل الفرد أو المنظمة لتجنب أو تقليل التعرض للمخاطر المحتملة. يؤكد النهج الذي يتجنب المخاطرة في مجال الأمن على الحذر واتخاذ القرارات المحافظة وتنفيذ الحلول لتقليل احتمالية وتأثير التهديدات الأمنية.

خوارزمية Rivest-Shamir-Adleman RSA

خوارزمية تشفير غير متماثلة تستخدم في تأمين الاتصالات والبيانات الرقمية. تتضمن خوارزمية RSA زوجًا من المفاتيح - مفتاح عام للتشفير ومفتاح خاص لفك التشفير. يعتمد أمن RSA على الصعوبة العملية المتمثلة في تحليل ناتج رقمين أوليين كبيرين، مما يجعل من غير الممكن حسابيًا للمهاجمين استخلاص المفتاح الخاص من المفتاح العام.

الجذر Root

أعلى مستوى من الوصول الإداري أو الامتيازات في نظام التشغيل لينكس (والاندرويد المبني على اللينكس). يتمتع الروت بتحكم غير مقيد في النظام بأكمله، بما في ذلك القدرة على تعديل ملفات النظام، وتثبيت البرامج، وتنفيذ الأوامر بامتيازات مرتفعة.

الجذور الخفية Rootkit

نوع سري من البرامج المصممة لإخفاء وجودها وأنشطتها على نظام الكمبيوتر، عادةً عن طريق اختراق النظام على مستوى الجذر أو النواة. تشتهر الجذور الخفية بمنح الوصول غير المصرح به والمستمر في كثير من الأحيان إلى النظام، مما يسمح للمهاجمين بتنفيذ هجماتهم والتلاعب بوظائف النظام والحفاظ على التحكم مع تجنب الكشف عن طريق الحلول الأمنية.

بروتوكول معلومات التوجيه RIP Routing Information Protocol

بروتوكول توجيه يستخدم في شبكات الكمبيوتر لتسهيل تبادل معلومات التوجيه ومساعدة أجهزة التوجيه على اتخاذ قرارات بشأن المسارات المثلى لنقل البيانات.

حلقة التوجيه Routing Loop

ظاهرة شبكية حيث يتم تداول حزم البيانات بلا نهاية بين أجهزة التوجيه أو عقد الشبكة بسبب معلومات التوجيه غير الصحيحة أو غير المتسقة.

الاجهزة القابلة للازالة Removable media

أجهزة التخزين التي يمكن فصلها بسهولة عن جهاز كمبيوتر أو جهاز إلكتروني، مما يسمح للمستخدمين بنقل البيانات ونقلها بسهولة.

طلب التعليقات Request for Comments

مصطلح نشأ داخل المجتمع التقني، خاصة في سياق الإنترنت وشبكات الكمبيوتر. RFC هو مستند يعرض المواصفات أو السياسات أو المنهجيات ذات الصلة بعمل الإنترنت وبروتوكولاتها.

تحديد موجات الراديو RFID Radio-Frequency Identification

تقنية تستخدم الاتصالات اللاسلكية لتحديد وتتبع وإدارة الأشياء أو الأشخاص أو الحيوانات. تتكون أنظمة RFID من علامات أو ملصقات تحتوي على معلومات مخزنة إلكترونيًا وقارئات RFID أو ماسحات ضوئية تستخدم إشارات الترددات الراديوية لاسترداد البيانات الموجودة على العلامات ومعالجتها.

الخطر Risk

الضرر المحتمل الناتج عن التهديدات أو نقاط الضعف في النظام أو البيئة. ويتضمن تحليل عوامل مختلفة، بما في ذلك احتمالية حدوث خرق أمني، والتأثير الذي قد يحدثه على الأصول أو العمليات، وفعالية الضمانات الحالية.

الرغبة في المخاطرة Risk Appetite

مستوى المخاطر المحدد مسبقًا الذي تكون المنظمة أو الكيان على استعداد لقبوله أو تحمله في السعي لتحقيق أهدافه. وهو بمثابة دليل إرشادي استراتيجي يساعد في تحديد الحدود التي تشعر المؤسسة بالارتياح للعمل من خلالها فيما يتعلق بالتهديدات الأمنية المحتملة.

ادارة المخاطر Risk management

العملية المنهجية لتحديد وتقييم وتحديد الأولويات وتخفيف المخاطر المحتملة على أصول المنظمة ومعلوماتها وعملياتها. يتضمن هذا النهج الاستراتيجي تحليل التهديدات الأمنية ونقاط الضعف والتأثير المحتمل للحوادث لوضع حلول فعالة لتخفيف المخاطر والسيطرة عليها.

مالكك الخطر Risk Owner

فرد أو كيان داخل منظمة يتم تعيينه لمسؤولية الإشراف على مخاطر أمنية محددة وإدارتها. ويكون مالك المخاطر مسؤولاً عن تحديد المخاطر وتقييمها والتخفيف من حدتها، مما يضمن اتخاذ التدابير المناسبة لمعالجة التهديدات الأمنية أو نقاط الضعف المحتملة.

الراوتر Router

جهاز شبكة يعمل كبوابة، لتوجيه حركة مرور البيانات بين شبكات الكمبيوتر المختلفة.

S

الملح Salt

في الأمان، يشير "الملح" إلى قيمة عشوائية وفريدة من نوعها تتم إضافتها إلى البيانات قبل تجزئتها. الغرض الأساسي من استخدام الملح في تجزئة التشفير هو تعزيز أمان تخزين كلمة المرور.

التعقيم Sanitisation

عملية إزالة المعلومات الحساسة أو السرية بشكل شامل وآمن من النظام أو وسيط التخزين لمنع الوصول أو الكشف غير المصرح به. تعد هذه الممارسة ضرورية لحماية البيانات السرية أو الشخصية عند إيقاف تشغيل الأجهزة أو الملفات أو وسائط التخزين أو إعادة استخدامها أو مشاركتها.

افتراض الامن Security By Default

مبدأ في الأمن السيبراني يؤكد على تصميم الأنظمة أو البرامج أو التكوينات لتكون آمنة بطبيعتها منذ البداية، دون الحاجة إلى تدخل إضافي من المستخدم. في هذا النهج، تعطي الإعدادات والتكوينات الافتراضية للنظام الأولوية للتدابير الأمنية لتقليل نقاط الضعف وأسطح الهجوم المحتملة.

التخزين الامن Secure storage

تنفيذ الحلول والبروتوكولات لحماية البيانات الحساسة أو السرية من الوصول غير المصرح به أو التغيير أو الكشف عنها. يتضمن ذلك استخدام التشفير، وضوابط الوصول، وآليات الأمان الأخرى لضمان بقاء المعلومات المخزنة محمية، سواء أثناء الراحة أو أثناء نقل البيانات.

المراقبة الامنية Security monitoring

عملية شاملة واستباقية في مجال الأمن السيبراني تتضمن المراقبة والتحليل والتقييم المستمر لأنظمة معلومات المنظمة لاكتشاف التهديدات الأمنية المحتملة والاستجابة لها. تستخدم هذه الممارسة مجموعة من الأدوات الآلية والتقنيات والخبرة البشرية لمراقبة أنشطة الشبكة وسجلات النظام ومصادر البيانات الأخرى ذات الصلة بالأمان.

استخبارات الاشارات SIGINT Signals Intelligence

جمع المعلومات الاستخبارية التي تتضمن اعتراض وتحليل أنواع مختلفة من الإشارات والاتصالات وعمليات الإرسال. يشمل هذا النوع من جمع المعلومات الاستخبارية مجموعة واسعة من الأنشطة، بما في ذلك مراقبة الاتصالات اللاسلكية، واعتراض عمليات نقل البيانات الإلكترونية، وتحليل انبعاثات الرادار.

المعاملة الالكترونية الامنة Secure Electronic Transactions - SET

بروتوكول تشفير مصمم لتعزيز أمان معاملات الدفع الإلكترونية التي تتم عبر الإنترنت. تم تطوير SET في منتصف التسعينيات من قبل شركات بطاقات الائتمان الكبرى مثل فيزا وماستر كارد، وهو يوفر إطارًا قويًا لتأمين المعاملات المالية عبر الإنترنت.

سبلونك Splunk

منصة قوية ومستخدمة بشكل نطاق واسع مصممة لجمع البيانات التي تم إنشاؤها آليًا وفهرستها والبحث فيها وتحليلها، بما في ذلك السجلات وبيانات الأحداث من مصادر مختلفة.

اطفال السكربت Script kiddie

شخص يفتقر إلى المهارات التقنية المتقدمة ولكنه يشارك في القرصنة أو الهجمات الإلكترونية باستخدام اكواد أو أدوات تم تطويرها بواسطة قراصنة أكثر مهارة. يعتمد أطفال السكربت عادةً على أدوات استغلال وأدوات تلقائية متاحة بسهولة بدلاً من إنشاء برامج هجوم خاصة بهم.

التجزئة Segment

ممارسة أمنية تتضمن تقسيم شبكة أكبر إلى أجزاء أو شبكات فرعية أصغر، وغالبًا ما تستخدم جدران الحماية أو أجهزة الشبكة الأخرى، لتعزيز الأمان والتحكم بشكل عام.

المعلومات الحساسة Sensitive Information

البيانات السرية والتي قد يؤدي الكشف عنها إلى إلحاق الضرر بالمنظمات أو الكيانات. تشمل هذه الفئة معلومات التعريف الشخصية (PII)، والسجلات المالية، والسجلات الصحية، والأسرار التجارية، والملكية الفكرية، وأشكال أخرى من المعلومات التي تتطلب الحماية من الوصول أو الإفصاح أو التغيير.

توزيع الواجبات Separation of Duties

مبدأ أمنيً وممارسة تنظيمية مصممة لتعزيز التحكم وتخفيف المخاطر من خلال توزيع المهام والمسؤوليات بين أفراد أو أدوار متعددة داخل النظام أو عملية الأعمال.

الجلسة Session

الفترة التي يتفاعل خلالها المستخدم مع نظام أو تطبيق، عادةً من بدء تسجيل الدخول إلى تسجيل الخروج . تشمل الجلسة مدة وصول المستخدم إلى مورد أو خدمة أو تطبيق معين وتتميز بمعرف جلسة فريد.

السيرفر Server

جهاز كمبيوتر أو تطبيق برمجي مصمم لتوفير الخدمات أو الموارد أو البيانات لأجهزة الكمبيوتر الأخرى، المعروفة باسم العملاء، داخل الشبكة. تلعب الخوادم دورًا مهما في تسهيل الاتصال وإدارة تخزين البيانات ودعم التطبيقات المختلفة.

تقنية الظل Shadow IT

استخدام أنظمة أو تطبيقات أو خدمات تكنولوجيا المعلومات داخل المؤسسة دون موافقة صريحة أو إشراف من قسم تكنولوجيا المعلومات. غالبًا ما يتم اعتماد هذه التقنيات غير المصرح بها من قبل موظفين فرديين أو أقسام تسعى إلى تلبية احتياجات محددة أو تحسين الإنتاجية، دون الالتزام بسياسات تكنولوجيا المعلومات الرسمية أو معايير الأمان الخاصة بالمؤسسة.

سيم SIEM Security Information and Event Management

سيم SIEM، أو المعلومات الأمنية وإدارة الأحداث، هو نهج شامل للأمن السيبراني يتضمن تكامل إدارة المعلومات الأمنية (SIM) وإدارة الأحداث الأمنية (SEM). تقوم أنظمة SIEM بجمع وتحليل بيانات السجل التي تم إنشاؤها عبر البنية التحتية التقنية للمؤسسة، بما في ذلك الشبكات والتطبيقات والأجهزة.

الدخول الموحد SSO Single Sign-On

عملية مصادقة تمكن المستخدمين من الوصول إلى تطبيقات أو خدمات متعددة باستخدام مجموعة واحدة من بيانات اعتماد تسجيل الدخول. باستخدام تسجيل الدخول الموحد (SSO)، يقوم المستخدمون بالمصادقة مرة واحدة، عادةً من خلال موفر هوية مركزي، والوصول إلى العديد من الأنظمة المتصلة دون الحاجة إلى إدخال أسماء المستخدمين وكلمات المرور بشكل متكرر لكل تطبيق.

اختطاف الجلسة Session Hijacking

هجوم أمني يقوم فيه المهاجم باعتراض جلسة مستخدم نشطة أو التحكم فيها داخل نظام كمبيوتر أو تطبيق. يستغل هذا النوع من الهجوم نقاط الضعف في آليات إدارة الجلسة، مما يسمح للمهاجم بالوصول إلى بيانات اعتماد جلسة المستخدم أو معرف الجلسة.

مفتاح الجلسة Session Key

مفتاح تشفير مؤقت يتم إنشاؤه واستخدامه أثناء جلسة اتصال محددة بين كيانين، مثل العميل والخادم، لتأمين سرية وسلامة البيانات المتبادلة خلال تلك الجلسة.

ملفات المرور المظللة Shadow Password Files

آلية أمان مستخدمة في أنظمة التشغيل لتعزيز حماية بيانات اعتماد المستخدم. بدلاً من تخزين كلمات مرور المستخدم مباشرةً في ملف كلمة المرور والذي يمكن الوصول إليه من خلال عمليات نظام معينة، تقوم ملفات كلمات مرور الظل بتخزين هذه المعلومات الحساسة في ملف منفصل ومقيد مع ضوابط وصول أكثر قوة.

تحليل الاشارات Signals Analysis

عملية اعتراض واستخراج معلومات ذات معنى من إشارات الاتصال، عادةً في سياق الاتصالات الإلكترونية أو نقل البيانات. يتم استخدام هذه التقنية التحليلية في مجالات أمنية مختلفة، بما في ذلك ذكاء الإشارات والأمن السيبراني.

بروتوكول ادارة الشبكة SNMP Simple Network Management Protocol

بروتوكول مستخدم على نطاق واسع يسهل مراقبة الأجهزة وإدارتها داخل الشبكة. يسمح SNMP لمسؤولي الشبكة بجمع المعلومات من أجهزة الشبكة ومراقبة الأداء والتحكم في الاعدادات.

البطاقة الذكية Smartcard

بطاقة مزودة بشريحة دائرة متكاملة يمكنها تخزين البيانات ومعالجتها. تُستخدم هذه البطاقات بشكل شائع للمصادقة الآمنة والتحكم في الوصول والمعاملات المالية.

سنيفر Sniffer

برنامج مصمم لالتقاط وتحليل حركة الشبكة. ويقوم باعتراض وفحص حزم البيانات التي تعبر شبكة الكمبيوتر لمراقبة المعلومات الحساسة أو تحليلها أو التقاطها مثل بيانات اعتماد تسجيل الدخول أو محتوى البريد الإلكتروني أو البيانات الأخرى المنقولة عبر الشبكة.

الاستنشاق Sniffing

الاعتراض ومراقبة حركة الشبكة، عادةً لغرض التقاط معلومات حساسة. يتم تنفيذ هذا النشاط باستخدام أدوات خاصة والتي تلتقط حزم البيانات وتحللها أثناء مرورها بشبكة الكمبيوتر.

حقن قواعد البيانات SQL Injection

هجوم يستغل الثغرات الأمنية في تطبيقات الويب عن طريق حقن سطور برمجية خبيثة في مدخلات المستخدم. يحدث هذا الهجوم عندما يفشل أحد التطبيقات في التحقق من صحة البيانات المقدمة من المستخدم أو تنظيفها بشكل صحيح قبل دمجها في استعلامات SQL التي تتفاعل مع قاعدة البيانات.

التخفي Stealthing

ممارسة جعل نظام الكمبيوتر أو الشبكة أقل وضوحًا وأكثر صعوبة في اكتشافها من قبل المهاجمين . غالبًا ما يرتبط هذا المصطلح بالتقنيات المستخدمة لإخفاء أو تمويه وجود نظام ما على الشبكة، مما يجعل من الصعب على الجهات الخبيثة تحديد واستهداف نقاط ضعف معينة.

تحليل الاخفاء Steganalysis

اكتشاف وتحليل الرسائل أو البيانات أو البرامج الضارة المخفية المخبأة داخل ملفات أو وسائط تبدو غير ضارة.

اخفاء المعلومات Steganography

أسلوب يستخدم في الأمن السيبراني لإخفاء المعلومات ضمن بيانات أخرى تبدو غير ضارة، بهدف ضمان سرية الرسالة المخفية. على عكس التشفير، الذي يركز على جعل الرسالة غير مفهومة للأطراف غير المصرح لها، فإن إخفاء المعلومات يخفي وجود الرسالة نفسها.

الحافز Stimulus

حدث أو عامل أو حالة قد تؤثر على الوضع الأمني لنظام أو مؤسسة أو شبكة. يمكن أن تشمل المحفزات مجموعة واسعة من العوامل، بما في ذلك التهديدات الخارجية، أو نقاط الضعف، أو التغييرات التنظيمية، أو التقدم التكنولوجي، أو التحولات التنظيمية.

تشفير التدفق Stream Cipher

خوارزمية التشفير المستخدمة في التشفير لتأمين البيانات الرقمية عن طريق تشفيرها بت واحد أو بايت في المرة الواحدة أثناء الإرسال. على عكس تشفير الكتل، الذي يعالج كتل البيانات ذات الحجم الثابت، تعمل تشفير التدفق على وحدات فردية من البيانات في تدفق مستمر.

السويتش Switch

جهاز شبكة يعمل في طبقة ارتباط البيانات لنموذج OSI وهو مصمم لتوصيل أجهزة متعددة داخل شبكة محلية.تعد أكثر ذكاءً في إعادة توجيه البيانات، وتتخذ القرارات بناءً على عناوين (MAC) للأجهزة المتصلة.

الروابط الرمزية Symbolic Links

ملفات تعمل كمؤشرات أو مراجع لملفات أو أدلة أخرى في نظام الكمبيوتر.

المفتاح المتماثل Symmetric Key

مفتاح تشفير يُستخدم لكل من تشفير وفك تشفير البيانات في التشفير المتماثل.

التزامن Synchronization

تنسيق العمليات أو البيانات أو الأنظمة لضمان الاتساق والدقة في تفاعلاتها.

سنورت Snort

نظام مفتوح المصدر لكشف التسلل ومنعه (IDPS) في أمان الشبكة. تم تطوير سنورت بواسطة سيسكو ويتم استخدامه بشكل واسع لتحليل حركة المرور لحظة بلحظة وتسجيل الحزم لاكتشاف ومنع مجموعة متنوعة من التهديدات الأمنية، بما في ذلك هجمات الشبكة والفيروسات والأنشطة المشبوهة الأخرى.

سجل النظام Syslog

بروتوكول وتنسيق رسائل يستخدم لتسجيل الأحداث المختلفة داخل نظام الكمبيوتر. فهو يوفر طريقة لأجهزة الشبكة والخوادم والتطبيقات لإنشاء رسائل السجل وإرسالها إلى خادم أو مستودع مركزي.

ضابط أمن النظام SSO System Security Officer

مسؤول عن مراقبة وإدارة الإجراءات الأمنية المطبقة داخل نظام الكمبيوتر أو الشبكة. يتضمن دوره تطوير وتنفيذ وإنفاذ السياسات والإجراءات والضوابط الأمنية لحماية سرية المعلومات والموارد وسلامتها وتوافرها.

التصيد برسائل الهاتف Smishing

هجوم الأمن السيبراني الذي يستخدم فيه المهاجم الرسائل النصية SMS لتصيد ضحاياه والكشف عن معلومات حساسة أو تنفيذ إجراءات معينة. غالبًا ما تبدو هذه الرسائل النصية وكأنها واردة من مصدر موثوق ، مثل بنك أو وكالة حكومية، وتحتوي على محتوى يشجع المستلمين على النقر على الروابط الضارة أو تقديم معلومات سرية مثل كلمات المرور أو التفاصيل المالية.

مركز العمليات الامنية SOC Security Operations Center

منشأة مركزية مجهزة بفريق متخصص من متخصصي الأمن السيبراني المسؤولين عن مراقبة الحوادث الأمنية واكتشافها والاستجابة لها داخل المؤسسة.

الهندسة الاجتماعية Social engineering

تقنية تلاعب يستخدمها الهاكرز لاستغلال علم النفس البشري للكشف عن معلومات حساسة، أو توفير وصول ، أو تنفيذ إجراءات تهدد الأمن. يعتمد هذا النوع من الخداع على استغلال ثقة الإنسان أو فضوله أو خوفه أو إلحاحه للتلاعب بالأفراد للكشف عن معلومات سرية مثل كلمات المرور أو التفاصيل المالية أو بيانات مهمة.

وسائل التواصل الاجتماعي Social media

المنصات والتطبيقات عبر الإنترنت التي تمكن المستخدمين من إنشاء ومشاركة وتبادل المحتوى في شكل نصوص وصور ومقاطع فيديو وروابط داخل مجتمع افتراضي. تشمل منصات الوسائط الاجتماعية الشهيرة فيسبوك واكس وانستغرام ولنكد ان.

الامن الاجتماعي Sociotechnical security

نهج شامل للأمن السيبراني يعترف بالتفاعل بين الأنظمة التكنولوجية والعوامل البشرية في حماية المعلومات والأصول. وهو يقر بأن فعالية الأمن لا تعتمد فقط على الحلول التكنولوجية ولكن أيضًا على فهم ومعالجة الجوانب الاجتماعية والسلوكية للمستخدمين والمنظمات. ويؤكد هذا النهج على تكامل الضوابط التكنولوجية مع الممارسات التي تركز على الإنسان، مثل التدريب على الوعي الأمني، وتحليل سلوك المستخدم، وتقييمات الثقافة التنظيمية.

التطبيق كخدمة software as a service

نموذج للحوسبة السحابية يوفر للمستخدمين إمكانية الوصول إلى تطبيقات البرامج عبر الإنترنت دون الحاجة إلى التثبيت أو الإدارة المحلية. في نموذج SaaS، تتم استضافة التطبيقات وصيانتها بواسطة سيرفر خدمة خارجي، مما يسمح للمستخدمين بالوصول إلى البرنامج واستخدامه على أساس الاشتراك.

رسائل سبام Spam

الرسائل الإلكترونية غير المرغوب فيها والتي غالبًا ما تكون غير ذات صلة أو ضارة يتم إرسالها بكميات كبيرة عبر الإنترنت. عادة عبر البريد الإلكتروني، ولكن يمكن أن يظهر أيضًا في أشكال أخرى، مثل الرسائل الخاصة أو التعليقات على مواقع الويب. تتمثل الأغراض الأساسية للسبام في تقديم إعلانات غير مرغوب فيها، أو نشر عمليات التصيد ، أو توزيع البرامج الضارة، أو المشاركة في أنشطة أخرى.

التصيد الدقيق Spear phishing

شكل من هجمات التصيد حيث يقوم الهاكرز بتخصيص هجوم على فرد أو منظمة أو مجموعة معينة. على عكس محاولات التصيد العامة التي تلقي شبكة واسعة، يتضمن التصيد الدقيق أسلوبًا أكثر تخصيصًا، وغالبًا ما يستفيد من المعلومات المجمعة حول الهدف لصياغة رسائل مقنعة للغاية وذات صلة .

الانتحال Spoofing

ممارسة يتنكر فيها شخص أو جهاز أو نظام ككيان آخر بقصد التلاعب أو خداع الأفراد أو الأنظمة أو الشبكات. يمكن أن يتخذ الانتحال أشكالًا مختلفة، مثل انتحال البريد الإلكتروني أو انتحال عنوان IP أو انتحال هوية المتصل.

فيروس التجسس Spyware

نوع من المالوير المصممة لجمع المعلومات سرًا من جهاز كمبيوتر أو جهاز دون علم المستخدم أو موافقته. يتم تسليم برامج التجسس عادةً من خلال التنزيل أو رسائل التصيد أو مواقع الويب المصابة، وتعمل في الخفاء، وتجمع البيانات الحساسة مثل الكتابة وبيانات اعتماد تسجيل الدخول وعادات التصفح والمعلومات الشخصية.

نظام الإشارة 7 (SS7)

مجموعة من بروتوكولات الاتصالات المستخدمة للتحكم في وإدارة الإشارات وتوجيه المكالمات داخل شبكات الهاتف العامة (PSTN). تم تصميم SS7 في الأصل للاتصال بين عناصر الشبكة، وقد أصبح هدفًا للمخاوف الأمنية بسبب نقاط الضعف التي يمكن استغلالها للوصول والتلاعب بالبنية التحتية للاتصالات.

طبقة SSL

بروتوكول تشفير مصمم لضمان الاتصال الآمن والمشفر عبر شبكة الكمبيوتر. تعمل الطبقة من خلال إنشاء اتصال آمن بين متصفح الويب الخاص بالمستخدم والخادم، مما يسهل التبادل الآمن للمعلومات الحساسة مثل بيانات اعتماد تسجيل الدخول أو البيانات الشخصية أو المعاملات المالية.

T

التكتيكات والتقنيات والاجراءات TTP Tactics, Techniques, and Procedures

إطار يستخدم في الأمن السيبراني والسياقات العسكرية لوصف المنهجيات والاستراتيجيات والأساليب المحددة التي تستخدمها جهات التهديد في تنفيذ الهجمات أو تحقيق الأهداف.

الاطاحة Takedown

الجهود المنسقة لتعطيل أو تفكيك أو تحييد الكيانات أو الأنشطة الضارة، مثل شبكات الروبوت أو مواقع التصيد أو البنية التحتية للمالوير. عادةً ما يتم تنفيذ عملية الاطاحة من قبل خبراء الأمن أو وكالات القانون أو منظمات الأمن السيبراني.

الربط Tethering

استخدام جهاز واحد، عادةً ما يكون هاتفًا ذكيًا، لتوفير الوصول إلى الإنترنت لجهاز آخر، مثل الكمبيوتر المحمول أو الكمبيوتر اللوحي. ويتم ذلك غالبًا عن طريق إنشاء نقطة اتصال لاسلكية أو عن طريق توصيل الأجهزة باستخدام USB.

استخبارات التهديدات Threat Intelligence

المعرفة والأفكار المكتسبة من تحليل تهديدات الأمن السيبراني ونقاط الضعف، مما يوفر للمؤسسات فهمًا استباقيًا للمخاطر المحتملة لأنظمة المعلومات الخاصة بها. وتشمل هذه المعلومات الاستخباراتية معلومات حول الجهات الخبيثة وتكتيكاتها وتقنياتها وإجراءاتها ، فضلاً عن التهديدات السيبرانية الحديثة.

التلاعب Tamper

التدخل غير المصرح أو التلاعب أو التغيير في نظام أو جهاز أو بيانات بقصد المساس بسلامتها أو وظائفها أو أمنها.

التورنت Torrent

بروتوكول مشاركة الملفات لتوزيع الملفات الكبيرة عبر الإنترنت. تعمل ملفات التورنت حين يقوم المستخدمون بتنزيل وتحميل أجزاء من الملف في وقت واحد، مما يؤدي إلى إنشاء نظام توزيع لا مركزي وفعال.

بروتوكولات TCP/IP

مجموعة من بروتوكولات الشبكات التي تشكل أساس الاتصال على الإنترنت. وهو يشمل مجموعة من البروتوكولات التي تحكم نقل البيانات وتوجيهها واستقبالها عبر الشبكات المترابطة. يضمن TCP تسليم البيانات بشكل موثوق ومنظم، بينما يتولى IPعنونة وتوجيه حزم البيانات بين الأجهزة.

اداة TCPDump

محلل حزم شبكةريعمل على أنظمة لينكس. يسمح للمستخدمين بالتقاط وتحليل حركة مرور الشبكة لحظة بلحظة أو حفظها في ملف لفحصها لاحقًا.

تقييم المخاطر Threat Assessment

التقييم والتحليل المنهجي للمخاطر ونقاط الضعف المحتملة التي يمكن أن تعرض سرية أو سلامة أو توفر المعلومات أو الأصول أو الأنظمة للخطر.

نموذج التهديد Threat Model

أسلوب لتحديد وتحليل وتوثيق التهديدات ونقاط الضعف المحتملة التي قد يواجهها النظام أو التطبيق أو المؤسسة. وهو ينطوي على النظر في عوامل مختلفة مثل المهاجمين المحتملين، ونواقل الهجوم، ونقاط الضعف المحتملة في تصميم النظام أو تنفيذه.

عنصر التهديد Threat Vector

المسار أو الوسيلة التي يتم من خلالها تسليم التهديد السيبراني إلى نظام أو شبكة أو فرد مستهدف.

الطوبولوجيا Topology

الترتيب المادي أو المنطقي لمكونات الشبكة وكيفية اتصالها ببعضها البعض. تحدد طوبولوجيا الشبكة بنية وتخطيط الأجهزة، مثل أجهزة الكمبيوتر والخوادم وأجهزة التوجيه والمحولات، داخل الشبكة.

بروتوكول التحكم في الارسال TCP Transmission Control Protocol

بروتوكول اتصال أساسي ضمن مجموعة بروتوكول الإنترنت (IP) الذي يضمن تسليم البيانات بشكل موثوق ومنظم بين الأجهزة الموجودة على الشبكة.

حماية طبقة النقل TLS Transport Layer Security

بروتوكول تشفير مصمم لتوفير اتصال آمن عبر شبكة الكمبيوتر، وهو يعمل في طبقة النقل ويضمن سرية وسلامة البيانات المتبادلة بين تطبيقين متصلين.

محاكاة التهديد Threat Emulation

إجراء أمني يتضمن محاكاة وتكرار التهديدات السيبرانية الحقيقية لتقييم فعالية دفاعات المنظمة.

التوصيل Trunking

دمج قنوات اتصال متعددة أو تدفقات بيانات في خط أو رابط واحد عالي السعة. تعمل هذه العملية على تحسين استخدام النطاق الترددي وتسهيل نقل البيانات بكفاءة بين أجهزة الشبكة.

النفق Tunnel

مسار اتصال آمن ومشفر يتم إنشاؤه عبر البنية التحتية الحالية للشبكة. تُستخدم الأنفاق عادةً لنقل المعلومات الحساسة أو الخاصة بشكل آمن بين نقطتي نهاية، وغالبًا ما يكون ذلك عبر شبكة عامة أو غير موثوقة مثل الإنترنت.

الاختناق Throttling

التباطؤ المتعمد أو تقييد معدلات نقل البيانات على الشبكة. غالبًا ما يستخدم مسؤولو الشبكات أو مقدمو خدمات الإنترنت (ISP) هذه التقنية للتحكم في استخدام النطاق الترددي وإدارة الشبكة وتحديد أولويات التطبيقات أو الخدمات المهمة.

امن طبقة النقل Transport Layer Security

بروتوكول تشفير مصمم لضمان الاتصال الآمن عبر شبكة الكمبيوتر، عادةً الإنترنت. يحل TLS محل طبقة SSL الأقدم ويعمل عن طريق إنشاء اتصال مشفر بين متصفح الويب الخاص بالمستخدم والسيرفر (او الخادم).

الرمز المميز Token

جزء صغير من البيانات أو المعلومات المستخدمة كبيانات اعتماد مصادقة للتحقق من هوية المستخدم أو الجهاز أو النظام. غالبًا ما يتم استخدام الرموز المميزة في آليات أمنية مختلفة، مثل المصادقة الثنائية (2FA) أو أنظمة التحكم في الوصول.

مراقبة المعاملات Transaction monitoring

المراقبة والتحليل المستمر للمعاملات المالية داخل المنظمة لاكتشاف ومنع الأنشطة المشبوهة. يتضمن هذا النهج الاستباقي تتبع بيانات المعاملات وفحصها لحظة بلحظة، عادة داخل الخدمات المصرفية أو التجارة الإلكترونية أو الأنظمة المالية الأخرى.

فيروس طروادة Trojan

نوع من الفيروسات التي تتنكر كبرنامج حقيقي لكنه ملغوم مع فيروس مخفي. سُميت على اسم الحصان الخيالي من الأساطير اليونانية، وغالبًا ما تتنكر أحصنة طروادة في شكل تطبيقات أو ملفات أو مرفقات بريد إلكتروني غير ضارة، مما يخدع المستخدمين لتنزيلها.

التحقق بخطوتين 2SV Two-Step Verification

التحقق بخطوتين (2SV)، والمعروف أيضًا باسم المصادقة الثنائية (2FA)، عبارة عن عملية أمنية تضيف طبقة إضافية من الحماية لحسابات المستخدمين من خلال طلب عاملي مصادقة مختلفين أثناء عملية تسجيل الدخول.

U

يونكس Unix

نظام تشغيل قوي وواسع تم تطويره في الأصل في الستينيات والسبعينيات. يشتهر يونكس باستقراره وميزاته الأمنية وقدراته على تعدد المستخدمين، وقد كان منصة أساسية للعديد من أنظمة التشغيل الأخرى، بما في ذلك لينكس وماك.

بروتوكول تخطيط البيانات User Datagram Protocol UDP

بروتوكول طبقة نقل في مجموعة بروتوكول الإنترنت (IP)، مصمم للاتصالات الخفيفة. على عكس بروتوكول التحكم في الإرسال (TCP)، لا يقوم UDP بإنشاء اتصال موثوق ومنظم قبل إرسال البيانات.

وبدلاً من ذلك، تقوم بتسليم البيانات في حزم منفصلة، تُعرف باسم مخططات البيانات، دون ضمانات التسليم أو التسلسل.

V

الجهاز الافتراضي Virtual Machine

محاكاة برمجية لجهاز كمبيوتر افتراضي يعمل داخل نظام اخر حقيقي. تتيح تقنية الجهاز الافتراضي إمكانية إنشاء وتنفيذ أجهزة افتراضية متعددة على جهاز حقيقي واحد، من منظور أمني، تُستخدم الأجهزة الافتراضية لعزل التطبيقات أو الخدمات وتقسيمها، مما يوفر طبقة من الحماية بين مكونات البرامج المختلفة.

الفيروس Virus

نوع من المالوير او البرامج الضارة المصممة لاعادة توليد نفسها والانتشار إلى الانظمة الأخرى عن طريق الارتباط ببرامج أو ملفات نظيفة. على عكس البرامج ، تعتمد الفيروسات على الملفات المضيفة للتنفيذ والنشر، دون علم المستخدم أو موافقته.

توقيع الفيروس Virus Signature

نمط أو خاصية فريدة ويمكن التعرف عليها مرتبطة بفيروس كمبيوتر معين أو سلالة برامج ضارة. هذا النمط هو في الأساس بصمة رقمية تستخدمها برامج مكافحة الفيروسات للتعرف على وجود تعليمات برمجية ضارة معروفة داخل الملفات أو الأنظمة واكتشافها.

الشبكة الافتراضية VPN Virtual Private Network

اتصال آمن ومشفر يتم إنشاؤه عبر الإنترنت، مما يمكّن المستخدمين من الوصول إلى شبكة خاصة أو الإنترنت بشكل آمن، بغض النظر عن موقعهم . تُستخدم شبكات VPN بشكل شائع لتعزيز الخصوصية والأمان عبر الإنترنت من خلال تشفير البيانات المنقولة بين جهاز المستخدم وخادم (سيرفر) VPN. يحمي هذا التشفير المعلومات الحساسة من التنصت أو الاعتراض المحتمل من قبل جهات الخبيثة.

الثغرة Vulnerability

ضعف أو خلل في نظام أو شبكة أو تطبيق أو عملية يمكن استغلالها من قبل الجهات الخبيثة لتعريض أمنها للخطر. يمكن أن تنشأ نقاط الضعف من عيوب التصميم، أو أخطاء البرامج، أو الاعدادات الخاطئة، أو نقاط الضعف الأخرى التي قد تكون موجودة عن غير قصد في التكنولوجيا.

التصيد الصوتي Vishing

تقنية الهندسة الاجتماعية حيث يستخدم المهاجمون الاتصال الصوتي، عادةً عبر المكالمات الهاتفية، لخداع الناس لإفشاء معلومات حساسة، مثل تفاصيل الهوية الشخصية أو كلمات المرور أو المعلومات المالية.

الجدار الناري الصوتي Voice Firewall

حل أمني مصمم لحماية شبكات الصوت عبر بروتوكول الإنترنت (VoIP) وأنظمة الاتصالات من التهديدات والهجمات السيبرانية المختلفة.

انظمة منع التسلل الصوتي IPS Voice Intrusion Prevention System

حل أمني مصمم لتحديد ومنع وتخفيف الأنشطة غير المصرح بها أو الضارة التي تستهدف شبكات بروتوكول الصوت عبر الإنترنت (VoIP).

W

اتحاد شبكة الويب العالمية W3C The World Wide Web Consortium

مجتمع عالمي يطور ويحافظ على معايير مفتوحة لضمان النمو على المدى الطويل وإمكانية الوصول إلى شبكة الويب العالمية. تلعب دورًا مهما في وضع المبادئ التوجيهية والمواصفات لتعزيز أمان تقنيات الويب.

الشبكة الواسعة WAN Wide Area Network

البنية التحتية للشبكة التي تمتد على منطقة جغرافية كبيرة، وتربط شبكات محلية متعددة (LAN) أو أجهزة فردية عبر مسافات طويلة.

بروتوكول التطبيقات اللاسلكية WAP Wireless Application Protocol

معيار تقني يمكّن الأجهزة المحمولة من الوصول إلى خدمات الإنترنت والتفاعل معها.

الثغرة المائية Watering hole

تكتيك خبيث حيث يقوم المهاجم باختراق موقع ويب أو منصة على الإنترنت يرتادها جمهور مستهدف محدد. الهدف هو إصابة أجهزة الأفراد الذين يزورون الموقع المخترق، وتحويله إلى مصدر لتوزيع البرامج الضارة.

صيد الحيتان Whaling

شكل متطور ومستهدف من هجمات التصيد التي تستهدف على وجه التحديد الأفراد البارزين داخل المؤسسة، مثل المديرين التنفيذيين أو الإدارة العليا أو صناع القرار. وخلافاً لهجمات التصيد العامة، التي تلقي شبكة واسعة ، فإن صيد الحيتان ينطوي على صياغة رسائل شخصية ومقنعة مصممة لاستغلال الأدوار والمسؤوليات ونقاط الضعف المحددة للأفراد المستهدفين.

الوايفاي Wif-Fi

تقنية تتيح الاتصال اللاسلكي بين الأجهزة، مما يسمح لها بتبادل البيانات عبر شبكة محلية (LAN) دون الحاجة إلى كابلات .

وايرشارك Wireshark

محلل بروتوكول شبكة مفتوح المصدر يسمح للمستخدمين بالتقاط وفحص البيانات المتدفقة عبر شبكة الكمبيوتر لحظة بلحظة.

الممسحة Wiper

نوع من البرامج المصممة بقصد تدميري يتمثل في محو البيانات الموجودة على الأنظمة المصابة أو استبدالها، مما يجعلها غير قابلة للاستخدام.

الدودة Worm

نوع من البرامج التي تتكاثر ذاتيًا وتنتشر عبر شبكات الكمبيوتر، عادةً دون الحاجة إلى تدخل المستخدم. تستغل الديدان نقاط الضعف في البرامج أو بروتوكولات الشبكة للانتشار بشكل مستقل من نظام إلى آخر، وإنشاء نسخ من نفسها أثناء تنقلها.

شبكة الويب العالمية The World Wide Web WWW

منظمة عالمية تتيح للمستخدمين الوصول إلى المحتوى ومشاركته عبر الإنترنت من خلال بروتوكولات موحدة مثل HTTP.

ويندوز Windows

أحد أنظمة التشغيل الأكثر استخدامًا لأجهزة الكمبيوتر الشخصية والخوادم. يشمل مجموعة إصدارات لأجهزة الكمبيوتر المكتبية وأجهزة الكمبيوتر المحمولة والأجهزة اللوحية والخوادم.

وين دمب Windump

أداة لرصد حركة مرور الشبكة لأنظمة تشغيل ويندوز. مشتق من الأداة مفتوحة المصدر المعروفة Tcpdump المستخدمة في انظمة اللينكس، يتيح وين دمب للمستخدمين التقاط وتحليل الحزم المتدفقة عبر الشبكة لحظة بلحظة.

الخصوصية السلكية WEP Wired Equivalent Privacy

بروتوكول أمان شبكة لاسلكية قديم مصمم لتوفير مستوى من الأمان مماثل لمستوى الشبكات السلكية.

التصنت الهاتفي Wiretapping

اعتراض أو مراقبة إشارات الاتصالات، عادةً الاتصالات الهاتفية أو عبر الإنترنت، دون معرفة أو موافقة الأطراف المعنية.

Y

يارا YARA

مجموعة من قواعد مطابقة الأنماط المستخدمة في الأمن السيبراني لتحديد وتصنيف البرامج الضارة أو الملفات الأخرى المشبوهة.

Z

يوم الصفر Zero-Day

ثغرة أمنية في البرنامج لم تكن معروفة من قبل ولم يتم إصلاحها والتي يستغلها المهاجم قبل أن يعلم بها صاحب البرنامج أو يصدر تحديث لحلها. يشير مصطلح "يوم الصفر" إلى أنه لا يوجد أي يوم من الحماية للمستخدمين من وقت اكتشاف الثغرة الأمنية حتى يتوفر التصحيح الأمني .

الثقة المعدومة Zero Trust

مفهوم امني يتحدى نموذج الأمان التقليدي القائم على ثقة الانسان بالمحيط من خلال افتراض أنه لا ينبغي الوثوق بأي كيان، سواء داخل الشبكة أو خارجها.

التصفير Zeroisation

عملية محو البيانات الحساسة أو مفاتيح التشفير بشكل كامل وغير قابل للنقض من الأجهزة أو الأنظمة الإلكترونية. يضمن هذا الإجراء عدم بقاء أي أثر للمعلومات السرية في ذاكرة الجهاز أو وحدة تخزينه، مما يجعله غير قابل للوصول وآمنًا ضد الوصول غير المصرح به أو محاولات استعادة البيانات.

الزومبي Zombie

يشير مصطلح الزومبي في الأمن السيبراني إلى جهاز مخترق ، وغالبًا ما يكون جزءًا من شبكة الروبوتات التي يتحكم فيها مهاجم عن بعد.