مقـدمة

هل تريد أن اقص عليك قصة ، أم أسألك سؤالا ؟!

حسنا

السؤال هو : هل تريد أن تتسلق السلم درجة تلو الثانية أم تريد أن تقفز مباشرة الى المستوى الأعلى ؟

إن كانت أجابتك هي ان تتسلق السلم تدريجيا فهذا الكتاب لك !

أما ان كنت تريد القفز المباشر فلابد ان تبحث عن القصة في هذا الكتاب !!

لمن هذا ؟

إذا كنت مهتمًا بتثقيف نفسك ومعرفة معلومات كافية عن الامن المعلوماتي، أو كنت تحضر لاجتياز شهادة CompTIA Security+ وأن تصبح معتمدًا في مجال أمن الشبكات والمعلومات فستساعدك المعلومات الواردة أدناه في تعلم المفاهيم الأساسية لأمن المعلومات والتحضير للامتحان فسوف نتعرف معا على التهديدات الأمنية الشائعة ، والأدوات الأمنية المستخدمة لصدها ، ونقاط الضعف الموجودة في الأنظمة الحالية ،وأيضًا معلومات اخرى حول التحكم في الوصول وإدارة الهويات والحقوق ومنح الصلاحيات وأساسيات التشفير ، والأمان المادي وأمان الأجهزة ، وتثقيف المستخدمين وحمايتهم وما الى ذلك ، وأكثر بإذن الله تعالى وذلك بإسلوب سهل واضح وبسيط ، وبمجرد أن تتعلم هذه المهارات ستكون مستعدًا إن شاء الله لاختبار CompTIA Security+ SY0-501

لماذا هذا ؟

بالنظر الى إنتشار التقنيات المختلفة وتنوعها الكبير وللاعتمادية الكبيرة في الوقت الحالي على شبكات الحاسب كأفراد او مؤسسات وحكومات تظهر أهمية الامن المعلوماتي لحماية هذه الشبكات وما تحتويه من معلومات كثيرة وهامة ومتنوعة ، ولقلة الموارد العربية التي تهتم بتبسيط المعلومات خصوصا الأساسية منها كان هذا الكورس مساهمة لإثراء المحتوى العربي في هذا المجال الهام , نسأل الله القبول ونسألكم الدعاء .

معلومات أم بيانات .... أو كلاهما ؟

حسنا دعونا نعرج على تعريف أمن المعلومات أولا من عدة مصادر :

فلو قلنا أن أمن المعلومات هو علم مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها.

هذا بحسب التعريف المنشور على ويكيبيديا

تعريف اخر يقول ان امن المعلومات هو حماية المعلومات والبيانات المتداولة عبر شبكة الإنترنت من العبث والتخريب والتبديل، أو من أي خطر يهددها .

بينما نجد في بعض الكتب والمصادر الأخرى ان الامن المعلوماتي هو مجموعة الإجراءات والتدابير الوقائية التي تستخدم لتامين المعلومات ومصادر البيانات وحماياتها من أي تهديدات او تجاوزات غير مشروعة ومن مخاطر الكوارث الطبيعية المحتملة التي تؤدي الى الفقدان أو التلف أو التأثير على نوع ومستوى الخدمة المقدمة .

إذا فقد ورد هنا مصطلح معلومات وبيانات!

قد يخطأ البعض أحياناً في استخدام البيانات والمعلومات كمعنى واحد، غير أن معنى الكلمتين مختلف تماماً، فما معنى البيانات؟ وما هي المعلومات؟

وما أهمية البيانات والمعلومات؟

مفهوم البيانات !

يمكن تعريف البيانات على انها مجموعة من الحقائق والقياســـات والمشـــاهدات والتي غالبا ما تأتي على شكل أرقام وحروف ورموز وأشكال خاصّـة، ولا يكون لها معنى (فما معنى الرقم ٢٥ بالنسبة لك ؟ وما معنى رمز =)

مفهوم المعلومات !

هي نتاج معالجة البيانات التي ليس لها معنى محدد بتصنيفها وتنظيمها وتحليلها، أو التعديل عليها حتى تصبح ذات معنى

مثال توضيحي .

ترفع سماعة الهاتف لتتصل بوحدة الأرصاد الجوية في بلدك للاستفسار عن حالة الطقس فيرد الموظف المختص ويخبرك بان غدا منخفض ٣٥ شمالية شرقية ١٥ عقدة ٢٢% ١٧ بار خفيفة الى متوسطة .....

حسنا مذا فهمت الان !؟

الموظف هنا قام بتزويدك ببيانات الطقس وهي دقيقة جدا بالمناسبة لكنك لم تفهم شيئا منها !!

ببساطة لأننا حينما نريد الاستفسار عن حالة الطقس ، لا يجب أن نحصل على بيانات درجة الحرارة وحركة الرياح وقياس نسبة الرطوبة وحركة الغيوم وما الى ذلك بل لابد ان نحصل على معلومة مستخلصة من كل البيانات السابقة ؟

ومن هنا يمكن معرفة ما تمثله البيانات من أهمية بالغة في عملية استخلاص المعلومات .

إذا وببساطة شديدة البيانات هي المادة الخام للمعلومات ويجب حمايتها أيضا .

أقسام الحماية

يمكن تقسيم الحماية داخل إطار أمن المعلومات الى ثلاث اقسام

أ- الحماية **الفيزيائية** Physical Security

يقصد بها حماية الأجهزة والبرامج والشبكات والبيانات من الأحداث الفيزيائية التي يمكن ان تسبب خسائر وأضرار ، مثل الحرائق والكوارث الطبيعية وعمليات السطو والتخريب وما الى ذلك ، من خلال استخدام أنظمة مراقبة وتتبع وانذار مبكر وغيرها .

ب – الحماية التشغيلية Operational security

وتعتمد بشكل كبيرة على برامج وأنظمة التشغيل كالجدران النارية ومكافح الفيروسات ومراقب النظام وعمليات فحص المنافذ وما الى ذلك .

ج –الإدارة والسياسات **Management and policies**

وهي مجموعة القوانين والإجراءات المعتمدة في المنشاة لتأمين البيانات والمعلومات الخاصة بها كسياسة كلمات المرور وصلاحيات الوصول وإدارة الملفات ، وكلما كانت هذه السياسات قوية كلما زادت قوة أمن المعلومات في هذه المنشاة .

عناصر وأهداف أمن المعلومات CIA

هناك ثلاث عناصر رئيسية لابد أن تكون في كل التدابير والسياسات والعمليات والاجراءات المستخدمة في تامين البيانات والمعلومات بحيث يتم بها تحقيق الأمن المعلوماتي .

هذه العناصر تختصر في الرمز **CIA كالتالي :**

الخصوصية او السرية : Confidentiality

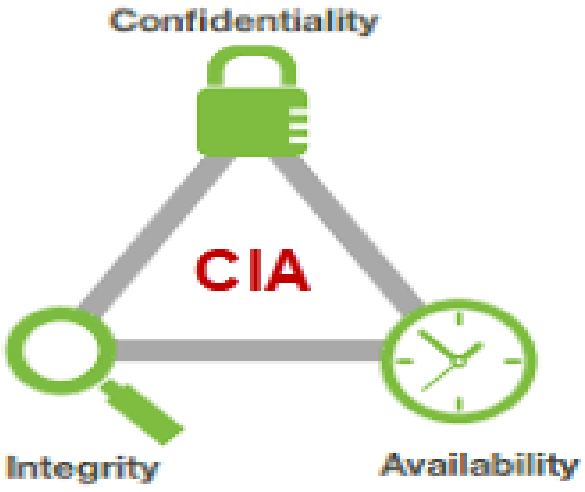
وهي منع غير المصرح لهم من الاطلاع او الحصول على البيانات والمعلومات .

السلامة : Integrity

وهي منع غير المصرح لهم من التعديل على البيانات والمعلومات .

الاتاحة : Availability

يقصد بها توفر إمكانية الوصول الى البيانات والمعلومات للأشخاص المصرح لهم .



هذه العناصر الثلاث يجب أن تمر من خلال **التحقق والتفويض والمحاسبة** وهو ما يطلق عليه معيار " **AAA** "

وهذا المفهوم أيضا يجب ان يستخدم عند تصميم او بناء أي خطة امنية لان معظم بروتوكولات أمن المعلومات قائمة في الأساس على هذا المفهوم.

والان لنتوقف قليلا لفهم هذا الـ "AAA"

يعبر كل حرف من هذه الأحرف الثلاث لمصطلحات ثلاث هي Accounting / Authorization / Authentication

التحقق Authentication : هي الهوية الرقمية التي تمنح لك في عالم أمن المعلومات ولا تخلو من أن تكون

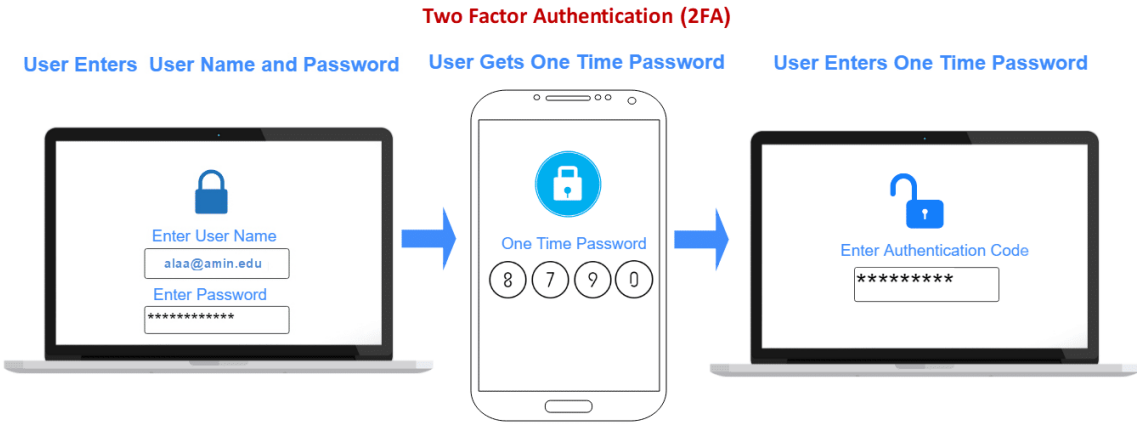
1- شيئا تعرفه ككلمة مرور أو رمز دخول
2- شيئا تملكه مثل كارت ممغنط او مفتاح مشفر
3- شيئا يعبر عنك كبصمة الاصبع او العين أو بصمة صوتية

في أمن المعلومات نستخدم أشكال عديده للوصول لمعيار التحقق كأجهزة الـ Biometric مثلا والشهادات الرقمية والبروتوكولات التي يتم التركيز عليها غالبا ، كما ان معيار التحقق نفسة هو الاخر يأتي في عده أشكال .

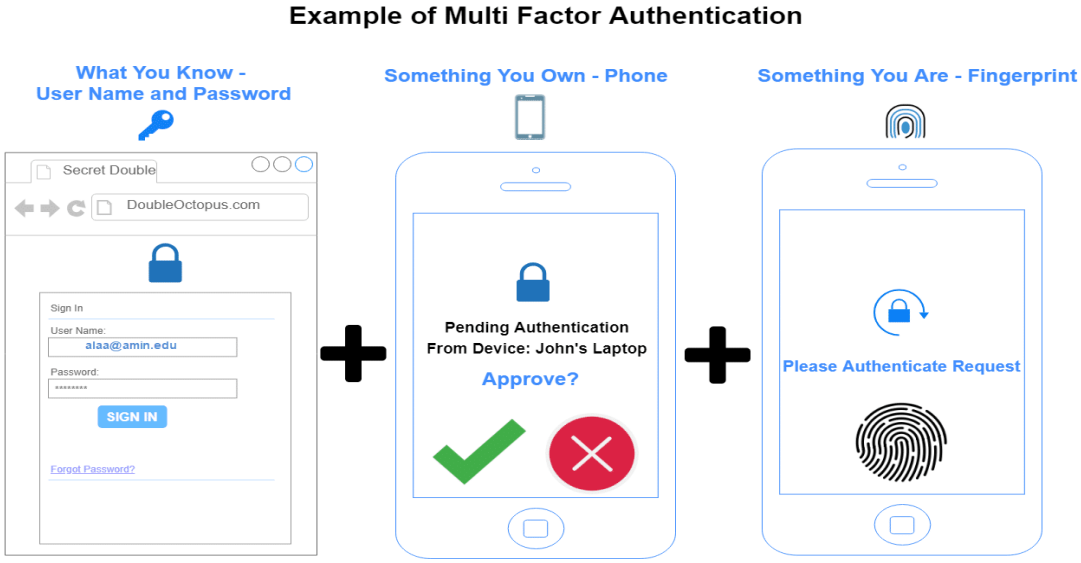
فقد يأتي الـ Authentication في صورة نوع واحد كبروتوكول (SFA) Single-Factor Authentication

والذي يعني ببساطة مطابقة الهوية بما هو موجود في قاعدة البيانات المخزنة كما في الشكل

أو بدمج نوعين معا وهو ما يعرف بـ Two Factor Authentication (2FA)



أو بتداخل الأنواع كلها معا وهو ما يعرف بـ Multi-Factor Authentication (MFA) .



التفويض Authorization : وهو المصطلح الثاني في مفهوم (AAA) ويعني التفويض ويأتي مباشرة بعد التحقق ومن خلاله يتبين ما الذي يمكن لهويتك فعله وما لا يمكن .

ثم تأتي عملية المحاسبة Accounting لتتبع وتأكيد عمليات الـ Authentication و الـ Authorization فهي تسجل وتراقب وتتابع جميع العمليات كتسجيل الدخول وأوقاتها والصلاحيات الممنوحة وتعد مرجعا واثباتا لمسئول أمن المعلومات في حالات التسلل والعبث

الآن قم بإخراج بطاقة الصراف الالي ATM الخاص بك لنطبق عليها عناصر امن المعلومات وكذلك مفهوم الـ "AAA"

- هل يمكن لأي شخص غيرك الحصول على بيانات المبالغ بداخل البطاقة ؟ ..... (السرية) يعززها (Authentication)
- هل يمكن اجراء تعديل على كلمة السر الخاصة بالبطاقة دون علمك ؟ ..... (السلامة) يقابلها (Authorization)
- هل تتمكن من استخدام البطاقة في أي وقت طالما هي معك ؟ ..... (الإتاحة) يراقبها (Accounting)

Authentication Protocols بروتوكولات التحقق

نحن كبشر نقوم بعملية التحقق بعدة طرق باستخدام نعم الله علينا كالسمع والبصر ، فنحن ندرك وجوه بعضنا البعض عندما نلتقي ، و نتعرف على أصوات بعضنا البعض على الهاتف أيضا ، لكن كيف سيتم الأمر مع الآلات ؟

حسنا

قد ذكرنا فيما سبق ان معيار " **AAA** " والذي يرمز الى Accounting / Authorization / Authentication يستخدم لتحقيق أهداف أمن المعلومات (**CIA**) وذكرنا أيضا ان المقصود بالـ Authentication هو عملية التوثيق أو التحقق الرقمي من الهويات والتي على ضوئها تتم عملية الـ Authorization لمنح الصلاحيات بعد ذلك .

اذا لابد حتى امنح صلاحيات ان استوثق من هويات أصحابها .... أليس كذلك ؟

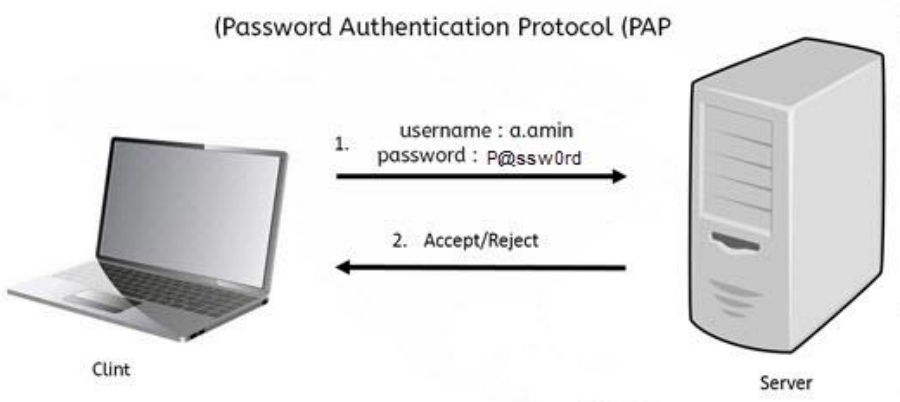
هنا يأتي دور بروتوكولات التحقق Authentication Protocols

وفيما يلي سنتطرق لأشهر وأهم البروتوكولات التي تستخدم في عملية التحقق تلك .

بروتوكول المصادقة بكلمة السر Password Authentication Protocol (PAP)

هو أبسط بروتوكول يستخدم في عملية التوثيق وآليه عملة ببساطة هي ان يرسل المستخدم اسم الدخول وكلمة المرور فيرد الخادم بعد فحص المدخلات بالسماح أو الرفض .

و بروتوكول الـ PAP يقوم بتسجيل جميع تفاصيل المصادقة في نص واضح دون أي تشفير ، مما يجعل هذا البروتوكول عرضة للقرصنة، ولذلك يجب تعطيل بروتوكول الـ PAP ما لم يكن هناك حاجة ماسة للعمل به في كوسيط لا يدعم كلمات المرور المشفرة.



بروتوكول المصادقة بكلمة السر المشفرة Shiva Password Authentication Protocol SPAP

هو نسخة مطورة من الـ PAP وأعلى امانا منه حيث يتم تشفير كلمة المرر بين المستخدم وخادم التوثيق الا انه لم يزل عرضه للقرصنة حيث يمكن الوصول لبيانات المصادقة وفك تشفيرها ومن ثم استخدامها .

بروتوكول المصادقة بمصافحة التحدي Challenge Handshake Authentication Protocol CHAP

يعد الـ CHAP من البروتوكولات الأكثر امانا لقيامه بتشفير بيانات المصادقة وعدم اعتمادها الا بعد اجتياز تحدي ما يرسله الخادم المسئول عن عملية المصادقة الى العميل . وقد يكون التحدي هذا سؤالا عن العمر او النوع أو مسألة حسابية بضرب عددين مثلا او جمعهما وحتى يسمح للعميل بالدخول لابد ان يقوم أولا بالإجابة .

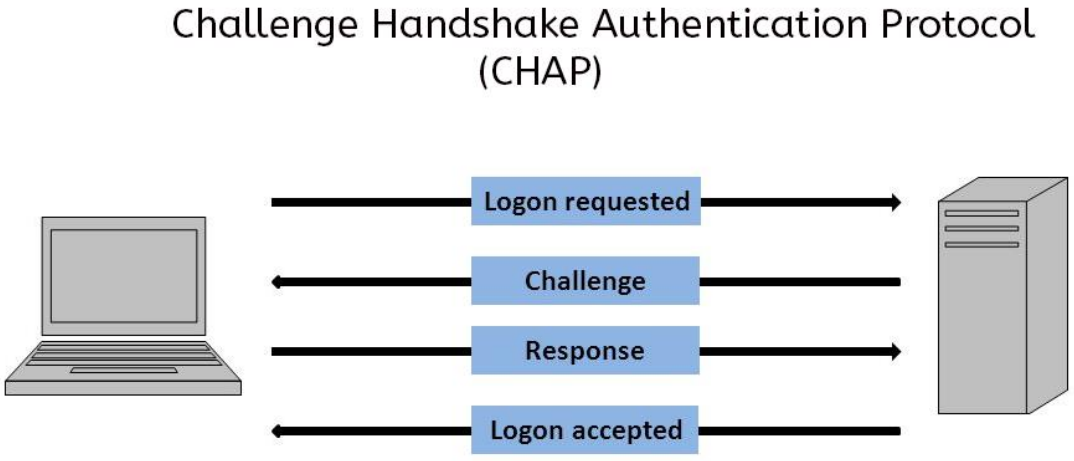
آلية العمل ببساطه كالتالي :

يرسل المستخدم طلبا للدخول

يرد الخادم بارسال تحدي لهذا المستخدم

يستجيب المستخدم للتحدي ويرسل الطلب مره أخرى للخادم

يرد الخادم بعد التحقق من النتيجة والبيانات بالقبول أو الرفض



التوثيق بكلمة مرور لمرة واحدة Time-based One-Time Password (TOTP)

يعتبر بروتوكول الـ TOTP حديثا واكثر امانا بالمقارنة مع البروتوكولات السابقة وقد شاع استخدامه بكثره خصوصا مع انتشار الهجمات الإلكترونية وعمليات الاحتيال في الآونة الأخيرة، ويعتمد الـ TOTP على طريقة التحقق بخطوتين (2FA) Two Factor Authentication باستخدام كلمة مرور محددة بمدة زمنية .

آلية عمل **بروتوكول الـ TOTP** كالتالي :

يرسل المستخدم طلبا للدخول باستخدام بيانات اعتماده

يرد الخادم بعد التحقق من بيانات الاعتماد بإرسال كلمة مرور مؤقتة

يستخدم العميل كلمة المرور المؤقتة ويرسل الطلب مره أخرى للخادم

يقوم الخادم بعملية التحقق من صحة كلمة المرور فيرد بالقبول او الرفض

ويستخدم الـ **TOTP الان من قبل كبرى الشركات مثل جوجل وفيس بوك وميكروسوفت وغيرها الكثير .**

بروتوكول الـ Kerberos

هو بروتوكول تحقق ضمن بيئة الشبكة وهو مصمم لتوفير مصادقة قوية بين العميل/الخادم "Client/Server

وكلمة Kerberos تشير الى أسطورة يونانية قديمة لكلب حراسه بثلاثة رؤوس .

ومن هنا جاءت تسمية هذا البروتوكول ، حيث أن لديه ثلاث خطوات هامه " تشير الى الثلاث رؤوس " للمصادقة على كل عمليه من خلال

اولاً - Key Distrbution center KDC

ثانيا - Authentication Service

ثالثاً - Ticket Granting Server TGS

حيث يجب على المستخدم ارسال هويته للخادم والذي يقوم بالتحقق من صحة هذه الهوية و يرسل تذكرة دخول أولية مشفرة مع مفتاح فك الشفرة ، فيقوم المستخدم بعد ذلك بالدخول باستخدام هذه التذكرة الممنوحة له .

تتكون آلية عمل kerberos على الشكل الأتي :

١- يطلب المستخدم المصادقة على هويته بإدخال كلمة المرور واسم الدخول الخاص به

٢- يتحقق خادم المصادقة من وجود هذا المستخدم في قاعدة البيانات لديه ثم يحيله لمركز التوزيع

٣- يضع مركز التوزيع شفرة ومفتاح سري على الطلب ويحيل الطلب لمركز التذاكر

٤- يقوم مركز التذاكر بتصدير تذكرة TGT و مفتاح بين المستخدم والخادم .

٣- يقوم المستخدم بعد ذلك باستخدام هذه الـ تذكرة للحصول على إذن الدخول لخدمة ما .

٤- باستخدام تذكرة الدخول يمنح المستخدم تذكرة جديدة للوصول للخدمة المطلوبة وجميع هذه العمليات تتم في أجزاء من الثانية وتكون مشفرة تماما.

Access Control Models نماذج التحكم في الوصول

من المفترض اننا فهمنا الان كيف يتم التحقق من الهويات في البيئة الرقمية , لكن كيف يتم منح تصاريح الوصول للذين تم التحقق من هوياتهم الرقمية ؟ أليس هذا ما يعرف بـ Authorization

حسنا يجب أن نعلم أن هناك أكثر من نموذج للتحكم في الوصول سنتناول أهمها وأكثرها انتشارا واستخداما في البيئة الرقمية .

التحكم الإلزامي في الوصول (MAC) Mandatory Access Control

هو استراتيجية أمنية تتم من خلال مسئول النظام فقط وتقيد قدرة المستخدمين الاخرين على منح أو رفض الوصول إلى الكائنات والموارد .

و يتم تعريف معايير الـ MAC بواسطة مسؤول النظام باعتباره صاحب السلطة العليا والمخول بذلك ، بينما يتم فرضها بشكل صارم بواسطة نظام التشغيل نفسة (OS) أو نواة الأمان بداخل نظام التشغيل ، ولا يمكن تغيير هذه المعايير من قبل المستخدمين الآخرين.
وبالتالي الـ MAC هو أعلى مستوى من التحكم في الوصول بالنسبة لمستويات الوصول الأخرى لأنه لا يمنح هذا الحق الا لمسئول النظام فقط أو من خلاله .

التحكم التقديري في الوصول (DAC) Discretionary access control

يأتي هذا النموذج عكس النموذج الالزامي لأنه يسمح بمنح صلاحيات وصول للبيانات بحسب تقدير مالكها وقد يكون الوصل محدود او وصول كامل عبر سياسة وصول يحددها المالك , أو بمعنى آخر يحدد المالك امتيازات الوصول إلى ما يملك .

التحكم في الوصول المستند الى الدور (RBAC) Role-based access control

يقصد بالدور هنا هو الدور الوظيفي الذي يقوم به المستخدم , وبالتالي يعتمد الوصول داخل RBAC على وظيفة او دور المستخدم داخل جهة العمل , وعلى ضوء ذلك ، يتم تعيين أذونات للتحكم في الوصول.

على سبيل المثال ، سيتم تعيين محاسب في شركة لدور "محاسب" ، اذا سيقوم الـ RBAC بمنحه اذن للوصول إلى جميع الموارد المسموح بها لجميع المحاسبين على النظام. وبالمثل ، عندما يتم تعيين مهندس برمجيات لدور المطور سيتم منحه الاذن لموارد البرامج والتطبيقات وهكذا .

التحكم في الوصول المستند الى الدور (RBAC) Rule-based access control

يأتي مصطلح الـ Rule بمعنى قاعدة وهي التي تحكم ما هو مسموح به وما هو غير مسموح به من خلال جدار الحماية. وبالتالي تعمل القاعدة بإحدى طريقتين: إما السماح أو المنع .

حسنا جدا الان سنتعرف معا على المخاطر والتهديدات الوارد حدوثها والتي يجب ان نستخدم سياسة أمن المعلومات

وبروتوكولات التحقق للحد منها وتحجيمها ، **لكن دعونا نراجع أولا ما تعلمناه .**