3.1 مقدمة عن املشاكل ألمنية اليت تعاين منها شبكات SDN : صحيح أن عملية فصل طبقة املعطيات عن طبقة التحكم أ دت إىل قفزة نوعية يف عامل الشبكات، ه وخالل الفرتة السابقة، اخلطوة إىل نشوء ثغرات جديدة مل تكن موجودة يف الشبكات التقليدية، جه حقيقي ملعاجلة قضاياي ألمن والوثوقية ضمن شبكات SDN ، االهتمام بشكل أكرب وأصبح هنالك تو بدأت العديد من ألحباث تتناول هذه ألخطار ونقاط الضعف والتهديدات اليت جنمت عن هذه التقنية اجلديدة، دم هذه ألحباث بعض احللول اليت ينبغي أخذها بعني االعتب وبدأت تق ار منذ اخلطوة ألولىل يف بناء شبكة SDNواليت قد تساهم بتفادي تلك التهديدات ومواجهتها وختفيف خطرها. تتمتع الشبكات التقليدية مبناعة طبيعية ضد اهلجمات الشائعة نظرا جتانس الربجميات والتحكم الالمركزي، ل أحد املهامجني نقطة ضعف لألجهزة امل تتأثر على اعتبار أنا تتبع لشركات مصن SDN فوجود بروتوكول Flow Open املشرتك بني مجيع الشركات سوف يزيد من خطورة التهديدات ونشر أعطال مشرتكة ، شبكات SDN فكرة رائعة يف عامل الشبكات لكن قامت بزايدة سطح اخلطر والتهديدات، قضاياي ألمن والوثوقية dependability and security واحللول الواجب أخذها بعني االعتبار عند تصميم شبكة 3.2 التهديدات وألخطار اليت تعاين منها شبكات SDN : متتلك شبكات SDN مستني أساسيتني جتلعها مصدر جذب للمهامجني واملخرتقني ومصدر قلق ألصحاب هذه برجمة الشبكة ابستخدام برجميات software 2 . الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا ألحد املتحكمات يعين الوصول والتحكم بكامل الشبكة. شبكات SDN واليت جنمعها يف الشكل)3-1)مع احللول البسيطة املقرتحة:]40، يف الشبكة أو من خالل مهاجم خبيث يستخدم أحد مكوانت الشبكة)موجه، إلطالق طرود أبعداد كبرية من أجل حتقيق هجوم قطع اخلدمة DoS(Service of Denial)واليت قد تكون مثالً ضد املبدالت اليت تعمل بربوتوكول Flow Open وذلك من أجل استهالك مجيع الذواكر) TCAM Ternary Memory Addressable Content)املوجودة ضمن املبدل. للمشكلة ب Intrusion Detection System((مدعومة أبنظمة معرفة السبب احلقيقي املسب ـRoot Runtime Analysis Cause وذلك لكشف السلوك الغري طبيعي لعناصر الشبكة،َ د معني ملعدل طلبات التحكم(. الديناميكي بسلوك املبدل)مثالً: وضع ح الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا إمكانية: جتاهل طرد ما، إعادة توجيه طرد ما إىل وجهة خاطئة، الشبكة أو حبت حقن معطيات أو طلبات ومهية يف الشبكة وذلك إلسقاط املتحكمات أو املبدالت اجملاورة. احلل املقرتح: استخدام آليات من أجل إجراء عمليات املصادقة على الربامج مثل أنظمة إدارة الثقة الذاتية والذي قد ي DoS أو لسرقة معطيات. مت استخدام تقنية التعمية SSl/TLS من أجل هكذا اتصاالت، وخاصة وأن هنالك العديد من ألحباث تشري إىل نقاط الضعف اخلاصة بـ SSL/TLS حيث أنا تعتمد على بنية أمن هذه االتصاالت يكون قوايً وة PKI(Infrastructure Key Public) لتبادل املفاتيح العامة.ً، أو جهة غري آمنة متنحً أضعف خطوطها أو عناصرها، هذا الضعف انمجا شهادات موق عة ذاتيا ْن يش ن هجوم قطع خدمة موزع جتميع قوة كافية) وحبسب عدد املبدالت اليت سوف تصبح حتت متناول يد ه(أ ذلك ميكن استخدام آليات ديناميكة ومضمونة لربط ألجهزة وذلك لضمان الثقة بني أجهزة طبقة التحكم د التهديدات خطورة يف شبكات SDN . خلل وحدة حتكم واحدة أو إصابتها هبجوم خبيث،ً، ألنه من الصعب إجياد التجميعة كشف التسلل IDS(System Detection Intrusion)قد ال يكون كافيا الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا الدقيقة لألحداث اليت قد تؤدي إىل توليد سلوك معني،ً، ميكن للتطبيقات اخلبيثة يف الشبكة أن تفعل ما حيلو هلا يف الشبكة على اعتبار أنُ املتحكمات فقط هي اليت تزود الشبكة رت البلتجريدات اليت ت جم إىل أوامر حتكمية إىل البنية التحتية. تو ظيف مسألة التنوع)للمتحكمات،ً االسرتداد)التحديث الدوري للنظام للوصول إىل احلالة املوثوقة والسليمة(. مفاتيح التشفري مثالً(. وألوامر اليت تستطيع هذه التطبيقات توليدها لربجمة الشبكة. املتحكمات والتطبيقات إىل القدرة على إقامة عالقات ثقة. الطريقة اليت ت ا الشهادة، استخدام آليات إلدارة الثقة ذاتيا البلتطبيقات طوال فرتةً ما تكون موجودة ضمن الشبكات التقليدية، هنا أيضا SDN للنفاذ إىل املتحكم البلشبكة، فإن هذا اخلطر سو ف يزداد بشكل دراماتيكي يف شبكات SDN ، السهل إعادة برجمة الشبكة وذلك من مكان واحد. الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا طلب النفاذ إىل املتحكم يتطلب تفويض من قبل شخصني اثنني(. آليات اسرتداد مضمونة لضمان حالة موثوقة بعد إعادة التشغيل. معلومات موثوقة من مجيع ألجزاء واجملالات املكونة للشبكة. مفيدة فقط إذا كانت مضمونة الوثوقية، االسرتداد السريع والصحيح لعناصر الشبكة إىل احلالة اليت كانت تعمل فيها. فع الة فإّنا جيب أن الُمتحى أو أن تكون غري قابلة للتغيري. 3.3 ألمن والوثوقية ضمن شبكات SDN : يناقش املؤلفون يف]40، جيب أخذها بعني االعتبار عند تصميم منصة آمنة وموثوقة للتحكم ضمن شبكات SDN. ال يوجد حبت اليوم حبسب رأي املؤلفني أي متحكم SDN يراعي قضاياي ألمن والوثوقية، تقنيات

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي

حتقق بسيطة أو حبت نسخ معطيات التحكم بني املتحكمات املنسوخة، لضمان ارتباط متحكم ـ مبدل موثوق، آليات للتأكد من سالمة وسرية املعطيات املتناقلة بني املتحكمات. الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا املفاتيح لضمان نظام قوي للغاية هو التسامح أو حتمل اخلطأ وأعباء التسلل الغري شرعي إىل النظام.ً مها نوذج التحً للخطا طم ونوذج بيزنطة . أيضا يعترب إنشاء بىن حتمل التسلل) tolerant–Intrusion architecture)خطوة يف طريق بناء ناذج ألمنية الذاتية، صحيح وتبقى قادرة على ضمان اخلواص مثل السرية، نتحدث فيما يلي عن احللول واملقرتحات لبناء منصة حتكم موثوقة وآمنة ضمن شبكات SDN: ق م املؤلفون يف [6 [التصميم العام املقرتح ملنصة حتكم بشبكة SDN آمنة وموثوقة،ً نظرة مبسطة لبن سوف نعرض بعض سوف سنسرد فيمايلي أهم الطرق اليت مت اقرتاحها من أجل احلصول على منصة حتكم بشبكة SDN آمنة الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا ت واحدة من أهم آلليات املستخدمة يف أتمني الوثوقية يف شبكات SDN ،ً. إىل جانب تكرار املتحكم يف الشكل، نسخ املتحكم إىل ثالثة متحكمات،ً نالحظ تكرار التطبيق B أيض ن ا يف مجيع نسخ املتحكمات. إ إجرائية اخللط هذه تضمن اجلزأين الصلب والربجمي كانت ألعطال مقصودة أو عرضية ألعطال وعزل التطبيقات أو املتحكمات اخلبيثة أو املعطلة. التطبيق B و على برجمة مجيع املبدالت على عكس التطبيق مع وجود خوارزميات اتساق مناسبة قادرا A. يع التنوع طريقة أخرى من أجل إكساب املتانة والقوة إىل ألنظمة ذات الوثوقية وألمن، هذه التقنية هو جتنب ألخطاء املشرتكة)مثل نقاط الضعف الربجمية أو خلل برجمي(. املعروف أن أنظمة التشغيل من العائالت املختلفة متتلك العديد من نقاط الضعف الغري مشرتكة، د من التأثري الكلي للهجمات عليها ألن هنالك هجمات تؤثر على نقاط ضعف التنوع يف أنظمة التشغيل حي معينة يف نظام تشغيل ما دون أن تؤثر على نظام تشغيل ما آخر. إلدارة متحكمات خمتلفة مثل تطبيقات API Northbound. :Self–Healing mechanisms الذايت التعايف آليات. ميكن ابستخدام االسرتداد التفاعلي أو االستباقي)recovery reactive or proactive)أن يتم جلب النظام إىل طور العمل الصحيح وذلك ابستبدال ألجزاء املتضررة واحملافظة عليها تعمل ابلشكل السليم أكثر وقت ممكن. عندما يتم استبدال ألجزاء، الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا االسرتداد وأن نعزز الدفاع ضد اهلجمات اليت تستهدف نقاط د إذا كان لدينا مبدل مرتبط مع متحكم وحيد controller ، التحكم هبذا املب ل غري متسامح أو دل القدرة على االرتباط بشكل ديناميكي بعدة حباجة إىل االرتباط مبتحكم آخر، مثالً ابستخدام التشفري وذلك لكشف املتحكمات اخلبيثة والتحقق منها وملواجهة متحكمات و بطريقة آمنة) : د أحد ألخطار الشهرية وهو هجوم الرجل يف الوسط(. صل بعدة متحكمات قادرا على التسامح املتحكمات ميكن استخدامها يف توزيع احلمل)balancing load)وتقليل أتخري التحكم ابستخدام املتحكم ذو ت بناء الثقة بني ألجهزة واملتحكمات مهما املستوى التحكمي بشكل كامل، حيث ينبغي أن يتم السماح ألجهزة الشبكة ابالرتباط بشكل ديناميكي ابملتحكمات لكن بشكل ال يسبب ختفيض مستوى العالقات املوثوقة. إ اخليار آلخر هو الثقة جبميع املبدالت بشكل عام حبت الوصول إىل دل ما)نتيجة لسلوك غري طبيعي جنم عنه(، حالة ينبغي فيها التحقق من مدى وثوقية مب املب الت د الوثوقية اخلاصة به بشكل دقيق. أو املتحكمات ابالعتماد على خوارزميات ع دة لكشف الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا املتحكمات وأصبحت جتميد هذا املبدل أو إجراء حجر صحي ع أوتوماتيكي من قبل مجيع ألجهزة واملتحكمات. مبا أ ن الربجميات تعاين حبد ذاهتا من مسائل: االستخد ام الطويل ألمد، املسائل وغريها أوجبت إجياد نوذج ثقة ديناميكي. يدعم إدارة الثقة الذاتية يف أنظمة الربجميات. أن يقيم مقدار الثقة ابجلهاز املطلوب الثقة به من خالل مراقبة سلوكه وقياس موصفات اجلودة مثل: التوافر، العالقات بني كياانت النظام. اجملالالت ألمنية املعزولة هي نوع شائع من التقاانت املستخدمة يف خمتلف أنواع ألنظمة.ُسمح للتطبيقات اليت مبستوى املستخدم حتقيق العزل يف منصات التحكم بشبكات SDN عن طريق استخدام تقنيات مشاهبة للصناديق الرملية sandboxes أو الفصل االفرتاضي virtualization . التعريف اجليد للواجهات interfaces اليت تسمح أبقل عدد ممكن من االتصالالت والعمليات بني اجملالالت ألمنية د املكوانت آلمنة واحدة من أهم اللبنات ألساسية يف بناء نظام آمن وموثوق. لتوفري قواعد احلوسبة املوثوقة TCB) Base Computing Trusted) لضمان خواص أمنية مثل السرية. الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا نه اليوجد أي برانمج خا من العيوب أو نقاط الضعف، واملوثوقة للربجميات مهمة جدا حجم نقاط الضعف. ابلتحديثات بطريقة سلسلة وآمنة.)آلليات املقرتحة مع التهديدات اليت تواجهها. الثقة بني ألجهزة واملتحكمات 3، الثقة بني التطبيقات واملتحكمات 5، التحديث والرتميم السريع واملوثوق للربجميات 6، وجيمل املؤلفون يف[6[ابلقول أبنه للحصول على نظام آمن وموثوق يف شبكات SDN فإنه ينبغي توخي السمات واالرتباط الديناميكي لألجهزة. الفصل الثالث نقاط ف ضعف الشبكات املعر

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي

ة برجمياُعن مبسألة األمن والوثوقية بشبكات SDN ، مثالً بعض املشاكل اليت جاءت مع اخرتاع فكرة SDN ويتحدث عن نقاط هامة أخرى مثل مراعاة البحث [7، أمن نظام التشغيل system operating ، إىل تبديل أو تدمري مكوانت الشبكة أو تدمري كامل نظام التشغيل لعناصر الشبكة مثل املتحكمات واملسريات،ً التالعب بربجميات الشبكة إىل ويقرتح ضمان أمن نظام التشغيل عن طريق استخدام أنظمة TCB .ً. إ ن خلل نظام التشغيل أو الربجميات خترييب عمل مكوانت الشبكة وميكن ضمان أمنها ابستخدام TCB أيضاِ برأي املؤلف سوف يؤدي إىل خلل يف كامل طبقات شبكة SDN، ويصنف املؤلفون األخطاء بشكل عام إىل الربجمية قد تؤثر على كامل طبقات الشبكة أما األخطاء الصلبة فتؤثر فقط على طبقيت املعطيات والتحكم.ِ ويذهب املؤلفون أبعد من ذلك فواً اهلجمات وحي ددوا الطبقات اليت تؤثر عليها، DoS يؤثر على الطبقات الثالثة، د املهاجم فيه إبدخال طرد ذو حجم معني ليستكشف جدول الدفق rules flow لدى املب ل وذلك عن طريق حتليل الزمن الذي استغرقه املبدل ملعرفة القاعدة اليت سوف يطبقها على هذا الطرد، يطرح هنا املؤلف مسألة محاية املتحكم ألنه يعُّ وجيعل الطرود تتدفق إليه بدالً الرئيسي، خدمات أو حبت بروتوكوالت مفتوحة. الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجمياً يتحدث املؤلف عن اهلجوم على املعطيات املتدفقة يف الشبكة، طريق التشفري وعن طريق استخدام آليات للتحقق وإعطاء الصالحيات وذلك لتجنب اهلجوم channel side ، ويؤكد أيضا مكوانت الشبكة أل ن استغالل نقطة ضعف أايً منها،ً الوصول إىل األجزاء الرئيسية من الشبكة مثل املتحكم، أن تتم محايتها فيزايئيا IPS و IDS أيضا املؤلف عن اهلجوم على طبقة التطبيقات، اخلدمة يف سائر الشبكة، واستخدام ترامیز آمنة وذلك عن طريق وجود توقيع رقمي خاص هبا. يف ورقة البحث [8 [يقرتح املؤلفون محاية االتصاالت بني املبدل واملتحكم ابستخدام TLS أيضا املتبادل لشهاديت الطرفني من خالل مفتاح خاص يول certificate root ،ً عن أ ن هنالك العديد من الشركات تتجن أيضا ب مسألة تضمني TLS لتكلفتها وصعوبتها،ً جيب توليد شهاً ويف حال غيابً ال يوجد طريقة ليتحقق املتحكم فيها من املب حيث يقوم هذا النموذج بتقسيم الشبكات إىل شرائح، فقط جزء من الشبكة سوف يتأثر ولن تتأثر األجزاء األخرى ألن visor flow سوف يعيد كتابة القاعدة بناء الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجمياً يقرتح املؤلفون وجود د أيضا checksum لكل القواعد املو جودة ضمن جدول الت الت ي ل بشكل بديل القواعد أو مت التالعب هبا. يوجد العديد من التصاميم للمتحكمات اهلادفة إىل جتاوز نقاط الضعف وأتمني هذه املتحكمات، د املتحكمات FlowDayLight واليت القت العديد من نقاط الضعف نسرد بعضها: 1- املتحكم أيمر املب ل إبرسال الطرود multicast إليه يف كل مرة، 2 ـيتم ترحيل مجيع الطرود احلاملة لعنوان فيزايئي غري معروف إىل املتحكم. ضد Spoofing MAC ،ً يستطيع ملء ذواكر املتحكمات مبثل هذه الطرود العشوائية، حتمل عناوين فيزايئية عشوائية. يوجد آليات ملنع Spoofing MAC ووضع حمددات لعدد الطر ود اليت حتمل عناوين غري معروفة ووضع قواعد من التطبيقات يف الشبكات املعر والتحسينات املضافة إليها: ات اسة يف الشبكة إىل طرف اثلث. صاالت التطبيقات اجلنوبية إلرسال معلومات حس حي ذر منها املتحكم توفري نظام حتقق AAA(Accounting, الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا قاموا إبجراء العديد من السيناريوهات لعرض احلاالت اليت ميكن من خالهلا استغالل نقاط الضعف يف طبقة التطبيقات اخلاصة هبذه املت ه وابستخدام برانمج خبيث صغري، د الشبكات املعر ابلكامل. الشبكات املعر حيث يعتمد الباحثون على استغالل مركزية التحكم وقابلة الرب جمة يف هذه الشبكات إلجراء مراقبة دورية ملع وحدة املعاجلة املركزية ملختلف التطبيقات،ً يف احلاالت غري الطبي أوامر القراءة أو الكتابة أو التعديل أو غريها مً الشبكات املعر كما يقوم بنمذجة سلوكها، فة برجميا ات كشف بشكل أوتوماتيكي، يقوم ابستخدام منهجيات تعل م آلة لتحقيق غرض التحليل والكشف. ة برجميا حيث أّنم قادرون على إيقاف التطبيقً الشبكات املعرف وتقوم مبنعها من هكذا حماوالت قبل أن تبدأ هبا، للمنهجية يف بيئة اب استخدام مكتبة مفتوحة املصدر للتعامل مع واص الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجمياً تطرح ورقة البحث [9 [نقاط ضعف ومشاكل أخرى تتعلق بطبقة التطبيقات يف شبكات SDN وتع هذه من التحدايت الصعبة واخلطرية ملوضوع األمن بشبكات SDN ، ب. متتلك التطبيقات القدرة على الو صول إىل الذاكرة الداخلية لشبكات SDN :حيث أ ن املتحكمات تتشارك الذواكر متتلك إمكانية الوصول إىل املوارد الداخلية يف الشبكة، الذواكر الداخلية لشبكات SDN. ج. التطبيقات مسؤولة عن بعض رسائل التحكم: إ ن رسائل التحكم مسؤولة عن أتمني االتصال بني وذلك مبسح جداول التوجيه املب الت. ميكن أن تتشارك التطبيقات اخلبيثة من أجل تعطيل الشبكة كاملة عن طريق استهالك الذواكر أو وحدة املعاجلة املركزية CPU أو ميكن أن تقوم هذه التطبيقات بتنفيذ أمر الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا وأيضا التطبيقات من ضعف التصميم حيث ميكن استغالل هذه التطبيقات

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي

بسهولة للتالعب أ. مشكلة الطرد الوارد in-packet :يسمى الطرد الوارد والذي ال يوجد قاعدة خاصة به لتوجيهه ضمن ل يسمى بـ in-packet ، بار أنه ال يوجد مب الت موثوقة ف يمكن أن يستغل أحد املهامجني نقطة الضعف هذه ً ابستخدام طرود مزيفة أن يتم إلرسال الكثري من الطرود in-packet وإسقاط املتحكم. تسميم نظرة املتحكم للشبكة وذلك إبرسال طرود ARP عشوائية لعناوين فيزايئية غري موجودة. ً تسميم اكتشاف طوبولوجيا الشبكة وذلك عن طريق أيضا التالعب خبدمة اكتشاف اخلط. ب. التضارابت يف إعدادات املتحكمات: حيث يوجد لدينا ضمن اجملال الواحد عدة متحكمات وعدة ب flow open ابلتايل من املمكن أن ال يكون هنالك تزامن بعمل هذه املكوانت مع بعضها. هنا لتبديل حمتوى رسائل التحكم بني طبقة التحكم وطبقة املعطيات وختريب حمتوى جدول التوجيه، تكون عرضة للتنصت سواء ال أو غري الفعال وذلك عن طريق التجسس على قناة التحكم حيث ميكن ً للمتحكم تعل أن تكون عرضة من خالل التجسس على رسائل التحكم. الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا هلجمات مستوى الـ TCP حيث ال يؤمن استخد ام TLS محاية ملستوى TCP ً هنا اليوجد معيار موح د الطاقة االستيعابية احملدودة للمب دالت اخلبيثة أنه صاحب العنوان العنوان املنطقي والعنوان الفيزايئي لألجهزة املوثوقة وذلك لكشف عمليات spoofing ، املتحكم أ ن هنالك عنوان فيزايئي جلهاز غري موثوق يقوم بتجاهله. spoofing ARP يف حال مل نكن نستخدم SSL . النماذج املستخدمة يف شبكات SDN واملطبقة يف بروتوكول Edge Validation ُ ، Flow Open Address source ض من يف املتحكمات، اخلاصة ابلطرود اخلارجية والغري مس ج ه،)موثوقة(ملقارنة العناوين مع قواعد معينة إما للتجاهل أو للمعاجلة أو للتسيري. الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا أن يكون قادرا كما يف حال شبكات ً Address Network) NAT على عزل شبكته احمللية عن الشبكة اخلارجية Translation) حيث ميكن أن يكون لدى املتحكم جدول لرتمجة العناوين اخلارجية إل عناوين داخلية. السماح لبعض ألشخاص الغري مصر ن بفحص دوري لطرق التشفري واالتصاالت. إ املشكلة ألساسية ابستخدام TLS هي أنه إجراء اختياري يف ن بروتوكول flow open وأ الكثري من الشركات اليت تقوم بصنع املتحكمات ال تدعم TLS . اهلدف من هكذا هجمات هو ليس التخريب أو إلساءة إل معلومات الشبكة، ابلدرجة ألول واالستفادة منها. ُستخدم عند اخلطوة ألول يف هكذا هجوم، ألدوات املسح scanning واليت من املعروف أنا ت من التنجيزات املستخدمة يف بروتوكو ل Flow Open ملواجهة أدوات املسح هذه. القوائم البيضاء والسوداء لرتشيح التدفقات الشبكية، والفيزايئية للفلرتة وميكن تعميمها يف بنية Flow Open إلنشاء قوائم بيضاء وسوداء يف جداول التوجيه على هنالك العديد من االقرتاحات والنماذج اليت عىن ابحلماية من هجوم قطع اخلدمة وقياس دوري حلجم الطرود الواردة، الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا التدفق أن هنالك هجوم قطع خدمة قادم. لكن بسمات خمتلفة قليالً يقرتح املؤلف هنا استخدام Firewall عن تلك املوجودة يف الشبكات التقليدية حيث أن املتحكم هنا هو املسؤول الرئيسي عن تسيري الطرود. ّدمة يف ألحباث السابقة: 3.5 مناقشة سريعة للحلول املق ابلنسبة للتهديد ألول اخلاص ابلطرود الزائفة، ن أنظمة حتليل وأنظمة ملعرفة املسبب احلقيقي للحدث، ولكن أرى أ هذ ا احلل غري انجح إال يف الشبكات ً، ففي حال استطاع املهاجم الوصول لعدة أجهزة متناثرة يف الشبكة واستغالهلا إلرسال طرود ومهية وزائفة، ً يف معرفة مسب هذه ألنظمة لن جتدي نفعا ب اهلجوم، د املؤلفون يف التهديد ً العديد من التطبيقات والفريوسات اليت تستطيع تنفيذ عملية access remote: . الثاين ماهي نقاط الضعف اليت يرون أن استخدام أنظمة إلدارة الثقة بني أجهزة الشبكة قد تفيد يف تفاديها، أن يتم وضع املب ل switch يف أماكن بعيدة املنال عن أ سمح د أقرتح ابلوصول إليهم إال بعد أخذه لتصريح من قبل ثالثة أشخاص من نفس فريق العمل، interfaces حمدود حبسب احلاجة وحبسب الدراسة املفضية إل تركيب هذا املبدل، ابلشبكة يتم تركيب واجهات حسب احلا ستغل أحد وج جة فقط حىت ال ي ود واجهة فارغة ويوصل جهازه فيها اثلثا مهامجة اتصاالت طبقة التحكم، أن حيصل املبدل فيها على درجة من الوثوقية مث بعد ذلك يقوم ابلعمل والتواصل مع طبقة التحكم، الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجمياً : يف حال استخدمنا طريقة النسخ، سوف يفضي إل بطئ يف عملية التسيري. ً ما هي نقاط ضعف املتحكمات ألخرى املثيلة. إضايف عدم السماح ألحد للولوج إل املتحكم إال بتصريح من قبل عدة اختصاصيني من نفس اجملال. خامسا عدم وجود آلية لضمان الثقة بني التطبيق واملتحكم، ً ابلتأكد من صحة شهادة التطبيق مث بعد ذلك يستجيب ألوامره. ً يقوم املتحكم بداية : املمكن أن يكون هنالك اتفاق بني هؤالء املصر ح هلم، ً لتسجيل حركة الولوج إل املتحكمات ومن هم ألشخاص الذين قاموا إبعطاء التصرحيات. من أجل التهديد السابع وجود نظام تعقب و تسجيل!!! لكن يف حال وقوع الشبكة ابلكامل، أرى أن جيب أن يكون هنالك نظام مراقبة عام لدى احملطة ألساسية ملراقبة كل ما جيري من الشبكة وأنظمة

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي

تنبؤ ابألفعال الغري اعتيادية، هجمات معروفة وتقليدية ملقارنة سلوك الشبكة معها بشكل دائم ملعرفة املشكلة قبل وقوعها. ابلنسبة لطرحهم اخلاص ببناء منصة حتكم آمنة وموثوقة، استغالل أحد املب الت للوصول إىل املتحكم املرتبط معها د اآلخر ليس نسخة عن املتحكم املصاب(، ابلتايل حنن حباجة إىل أتمني املب الت أوالً بعد ذلك نستطيع استخدام يكون هنالك إجرائية فحص لألمان يقوم هبا املتحكم لكل مبدل يرغب ابالرتباط معه. الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا ابلنسبة للحل الذي ينص على بناء الثقة بني املتحكم واألجهزة: ما هي اآلليات اليت ميكن استخدامها ملثل هكذا أمر؟؟ وما مدى أتثريها على جودة وسرعة الشبكة على اعتبار أن كل جهاز جديد حباجة للدخول للشبكة سوف يكون هنالك حاجة إىل التحقق منه ونسبه إىل القائمة البيضاء أو وضعه بطور التجميد أو حىت رميه دالت عن الوثوقية اخلاصة هبا يف دالت مث سؤال أحد املب مت اقرت احه هو إعطاء الثقة لكامل املب فذ هجمته مث مل يعد يهتم بعد ذلك ال إلعطاء دليل وثوقية وال حىت للعودة للشبكة من جديد. ؟ أما يف ورقة البحث [8 [فعندما اقرتح املؤلف أن يكون هنالك checksum جلدول التوجيه. checksum ميكن تبديله بسهولة حيث حىت لو مت التالعب ابلقواعد، checksum لذلك أقرتح أن يتم إضافة عملية التهشري function hash لضمان عدم التالعب هنا.ً عند اقرتاحه العمل بربوتوكول من النماذج املطروحة لبناء املتحكمات، االتصاالت ملشكلة هجوم الرجل يف الوسط middle-the-in-man. ؟ أما يف ورقة البحث [9 [يطرح املؤلفون عدة نقاط ضعف جديدة لكن دون حتديد ألساليب املمكنةً، أو أن يكون لكل تطبيق وقت حمدد و التطبيقات تعمل بشكل منفصل دائما يتم توزيع املوارد بشكل متساوي بني التطبيقات يف كل حيز زمين time slot .ُطى الصالحية للنفاذ إىل أن يكون هنالك إجرائية تسمح بداية ابلتحقق من وثوقية هذا التطبيق مث بعد ذلك يعً إجرائيات لوضع عتبة معينة لعدد الطرود الواردة واليت وذلك لتبيان املنبع الذي تصدر منه هذه الطرود، الفصل الثالث نقاط ف ضعف الشبكات املعر ة برجميا وأن يكون املب ل متصل مع أكثر من متحكم، ل برقم تسلسلي ما، يوجد الكثري من ألحباث اليت بدأت ابلتوجه حنو مسأليت ألمن والوثوقية يف شبكات SDN .ّ تؤخذ هذه الدراسات بعني االعتبار بل الشركات املصنعة أو اخلرباء والباحثني املعنيني إبدارة شبكات َد املؤلفون آليات ابالسم ملواجهة مشكالت حمددة ومسألة التنوع وهذه نقطة جيدة هامة، النسخ إىل نظام أكثر متانة وقوة.

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي