جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الحواسيب والأتمتة

تقييم خصائص جدار النار كوظيفة شبكة افتراضية

Evaluating the Characteristics of Firewall as a Virtualized Network Function

م. عفراء محمد عاقل

د. مفيد الياس حداد

الملخص

يقوم هذا البحث بدراسة خاصتي الأداء والأمان في جدار النار Pfsense و-Sophos UTMويقوم بالمقارنة بين النتائج.

تم تقييم الإنتاجية باستخدام أداة Iperf3 ضمن خمسة سيناريوهات، في السيناريوهات الأربع الأولى تم تكرار كل تجربة مئتا مرة وإجراء الاختبار في حال وجود جدار الحماية Pfsense ومن ثم Sophos UTM. أما في السيناريو الخامس والأخير لم يتم تكرار الاختبار وتم إجراؤه في ثلاث حالات: بدون جدار حماية، ومع وجود جدار حماية Pfsense، ومع وجود جدار حماية Sophos UTM.

وأما بالنسبة للحماية فتم تعريض الجدارين لثلاثة أنواع من الهجمات وهي فحص المنفذ (Port Scan)، والفيضان (TCP-SYN Flooding)، والقوة الغاشمة (Brute Force) مع تكرار كل هجوم خمسين مرة.

أظهرت النتائج أن Sophos-UTM كان أفضل من حيث الإنتاجية ولكن Pfsense كان أفضل من حيث الحماية حيث تصدى لعدد أكبر من الهجمات.

القسم العملي

أولا: في اختبار الإنتاجية تم استخدام ثلاثة أجهزة افتراضية داخل بيئة VMwareوهي العميل وجدار النار والخادم. تم تنصيب نظام التشغيل Lubuntu على كل من جهاز الخادم والعميل، وتم تنصيب أداة iperf3 على كليهما، وتشغيلها بنمط الخادم على جهاز الخادم -s iperf3، وبنمط العميل على جهاز العميل c– iperf3.

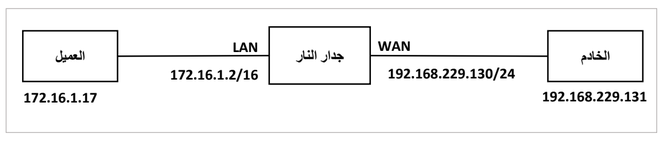
في البداية تم إجراء اختبار في الحالة العادية بدون التعديل على الإعدادات الافتراضية ل iperf3. وهذا يعني أن البروتوكول المستخدم هو TCP، والمنفذ المستخدم هو 5201.

في السيناريو الثاني تم تغيير المنفذ الافتراضي إلى منفذ آخر (تم اختيار منفذ عشوائي وهو ٥٦٠٠) مع الحفاظ على استخدام نفس البرتوكول TCP.

في السيناريو الثالث تم وضع حد لمعدل النقل لكرت الشبكة الافتراضي إلى ١٠٠٠ ميغابت في الثانية مع الإبقاء على البروتوكول TCP.

في السيناريو الرابع تم وضع حد لمعدل النقل لكرت الشبكة الافتراضي إلى ١٠٠٠ ميغابت في الثانية مع تغيير البروتوكول إلى UDP.

في السيناريو الخامس والأخير تم تغيير قيمة معدل النقل لكرت الشبكة الافتراضي بشكل تدريجي اعتبارا من 1Kbps وإلى 1Gbps.



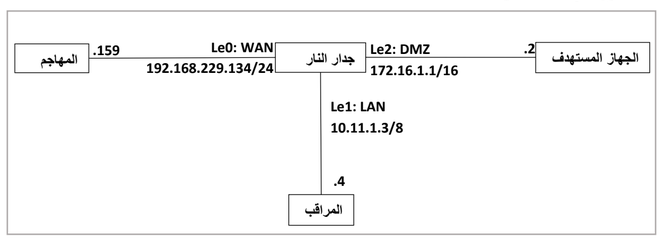
القسم العملي

ثانيا: في اختبار الحماية ركز التقييم على قدرة جدران النار على اكتشاف أنواع مختلفة من الهجمات والاستجابة لها، سواء مع أو بدون تمكين نظام منع التسلل (Intrusion Prevention System). كما تم تكرار كل اختبار خمسون مرة .

جدار النار الذي يفصل بين ثلاث شبكات: الشبكة المحلية LAN الحاوية على جهاز افتراضي منصب عليه نظام التشغيل Lubuntuوالذي يلعب هنا دور المراقب

وفي شبكة ال DMZ يوجد جهاز افتراضي منصب عليه Metasploitable2 وهو جهاز افتراضي يعمل بنظام تشغيل Ubuntu Linuxومعرض للخطر عمداً ومصمم لاختبار الثغرات الأمنية الشائعة. وبالتالي سيكون هذا الجهاز هو الجهاز المستهدف في عملية الهجوم.

وأما في الشبكة الخارجية WANيوجد Kali Linuxوالذي يلعب دور المهاجم الذي يقوم بشن الهجمات.



القسم النظري

في القسم النظري الخاص بهذا البحث تم دراسة بعض المفاهيم النظرية المتعلقة بوظائف الشبكة الافتراضية وجدران النار كما تم التطرق إلى بعض أنواع الهجمات الأمنية التي تتعرض لها الشبكات في وقتنا الحالي.

كما تم استعراض الدراسات المرجعية

النتائج والمناقشة

أشارت النتائج في اختبارات الإنتاجية، إلى أن Sophos UTMيتفوق باستمرار على Pfsenseمن حيث الإنتاجية. حيث حقق Sophos UTMإنتاجية أعلى.

في اختبارات الأمان، أظهر Pfsenseحماية أكثر اتساقاً في هجوم فحص المنافذ من خلال إيقافه بشكل فعال عند تفعيل نظام كشف التسلل. ومع ذلك، أظهر كلا جداري الحماية سلوكاً مشابهاً رداً على هجوم فيضانات TCP-SYNعن طريق إسقاط الرزم دون إيقاف الهجوم تماماً. ولم يمنع أي من جدران النار بشكل فعال هجوم القوة الغاشمة، لكن Pfsenseقام بمنع المهاجم مرة واحدة.

المراجع

[1] Arunwan, M., Laong, T. and Atthayuwat, K. (2016) “Defensive Performance Comparison of Firewall Systems”, MITiCON, Thailand, pp. 221-224.

[2] Azzam, A., Munadi, R. and Mayasari, R. (2019) “Performance Analysis of Firewall As Virtualized Network Function on Vmware ESXi Hypervisor”, Jurnal Infotel, vol. 11, pp. 29-35.

[3] Sampaio, D. and Bernardino, J. (2017) “Evaluation of Firewall Open Source Software Diogo”, WEBIST, Portugal, pp. 356-362.

[4] Salah, K., Elbadawi, K. and Bouaba, R. (2011) “Performance Modeling and Analysis of Network Firewalls”, IEEE, vol. 9, pp. 12-21.

[5] Shahsavari, Y., Shahhoseini, H., Zhang, K. and Elbiaze, H. (2016) “A Theoretical Model for Analysis of Firewalls under Bursty Traffic Flows”, IEEE, vol. 4, pp. 1-11.

[6] Doherty, J. (2016) “SDN and NFV Simplified”, 1st ed, Addison-Wesley Professional.

[7] Stewart, J. (2014) “Network Security Firewalls and Vpns”, 2nd ed, Jones & Bartlett Learning.