مجلة العلوم البحتة والتطبيقية
Journal of Pure & Applied Sciences
www.Suj.sebhau.edu.lyISSN 2521-9200
Received 20/04/2020 Revised 07/08/2020 Published online 05/10/2020

تقنية مصائد الاختراق لمكافحة جرائم الانترنت

*أبوعجيلة دغمان و موسى فنير و أحمد حمزة و رجب محمد و مروان حسين
قسم الشبكات–كلية تقنية المعلومات–جامعة الزنتان، ليبيا
*للمراسلة abuajila@uoz.edu.ly

الملخص أصبح التحدي الأساسي في يومنا هذا في مجال أمن الشبكات هو مواكبة أنماط التهديدات التي تتطور وتزداد بشكل يومي، وذلك من أجل تأمين الحل الأفضل لحماية أي منظومة، هنالك العديد من آليات الحماية التقليدية كالجدران النارية وأنظمة كشف الاختراق. لكن هذه لا تؤمن كشف أنواع جديدة من الهجمات لذلك تم اللجوء إلى مصائد الاختراق للكشف عن الهجمات الغير معروفة.مصائد الاختراق هي عبارة عن نظام يتم بناؤه وتكوينه من أجل أن يتم اختراقه، لذلك يتم نشرها داخل المنظومة لكي تساعد على استهلاك موارد المهاجم واستغلال وقته وصرف انتباهه بعيدا عن الأنظمة الفعلية، كما يؤمن بيئة عمل لدراسة التقنيات والطرق المتبعة من قبل المتطفلين على المنظومة. يقدم هذا البحث تقنية مصائد الاختراق لمحاكاة خدمات FTP,SSH ,HTTP ,Telnet...الخ بالكامل والتفاعل مع المهاجم Attackerلكي تساعد على استهلاك موارد المهاجم واستغلال وقته واستخلاص أكبر قدر ممكن من المعلومات القيمة عن المهاجم وتقنياته المتبعة و الأدوات البرمجية المستخدمة وصرف انتباهه بعيدا عن الأنظمة الفعلية. سنقوم باستخدام Modern Honey Network وهو خادم مركزي يستخدم لنشر وإدارة مصائد مخترقي الشبكات، وقد تم تطبيق إطار العمل المقترح باستخدام هجوم التخمين Brute-Force على بروتوكول SSH باستخدام أداة Nmap والاتصال المباشر مع باقي الخدمات.

الكلمات المفتاحية: مصائد الاختراق، نظم كشف الاختراق، منطقة مؤمَنة، خادم مصائد الاختراق، و جدار الحماية.

Honeypots Technology To Control Cybercrime

*A. Dogman, M. Faneer, A. Hamza, R. Mohammed, and M. Huseen.
Department of Computer Network, Faculty of Information Technology, University of AL-zentan
*Corresponding author: abuajila@uoz.edu.ly

Abstract Today, the main challenge in the field of network security is to keep pace with the types of threats that are developing and increasing on a daily basis, in order to provide the best solution to protect any system. There are many traditional protection mechanisms such as firewalls and penetration detection systems. But it does not guarantee the detection of new types of attacks, so Honeypots techniques have been used to reveal unknown attacks. Honeypots techniques are a system that is built and configured in order to be penetrated. Therefore, it is deployed within the system in order to consume the attacker's resources, exploit his time and divert his attention away from the actual systems. They also provide a working environment for studying techniques and methods used by intruders on the system. This research introduces Honeypots techniques to simulate ... Telnet, HTTP, FTP, SSH etc. and interact with the Attacker to help to consume the attacker's resources, use his time and extract as much possible valuable information about the attacker, its techniques, and the software tools used, and divert his attention away from the actual systems. We will be using Modern Honey Network, which is a central server used to deploy and manage honeypots. The proposed framework has been implemented using the Brute-Force attack on the SSH protocol using the Nmap tool.

Keywords: Honeypots , IDS, DMZ, MHN, and Firewall.

المقدمة

تمثل قضايا أمن الشبكات حجر الأساس في بناء أي منظومة شبكية مهما كان حجمها وذلك بسبب تزايد وتنوع التهديدات الجديدة والتي نجدها دائما في حالة من التطور والتقدم السريع.وفقا لموقع [1] cybintsolutions.com، يحدث هجوم على أحد الأجهزة المتصلة بالإنترنت بمعدل مرة كل 39 ثانية. ووفقا للفريق الأمني في شركتي "بي تي " التي تعمل في مجال تشغيل الشبكات وتقديم خدمة الإنترنت يكتشف 100 ألف عينة من البرمجيات الخبيثة كل يوم[1]. ولمواجهة هذه التهديدات نحتاج إلى حلول أمنية متطورة والتي لم تعد متوفرة عبر طرق الحماية التقليدية مما شكل تحديا أساسيا في تأمين الحماية اللازمة لأي منظومة شبكية. هذا التحدي يتمثل في معرفة كيفية كشف ومنع المتسللين الذين في وضعية تطور مستمر من ناحية التقنيات والأساليب المستخدمة وبالرغم من كثرة الأبحاث و المشاريع التي تتصدى لهذه المسائل إلا أن المكلفين بحماية أمن الشبكة مايزالون غير قادرين على جعلها أكثر أمناً و حماية من أي تطفل أو هجوم أو اختراق[1][2].تقنيات الحماية التقليدية مثل

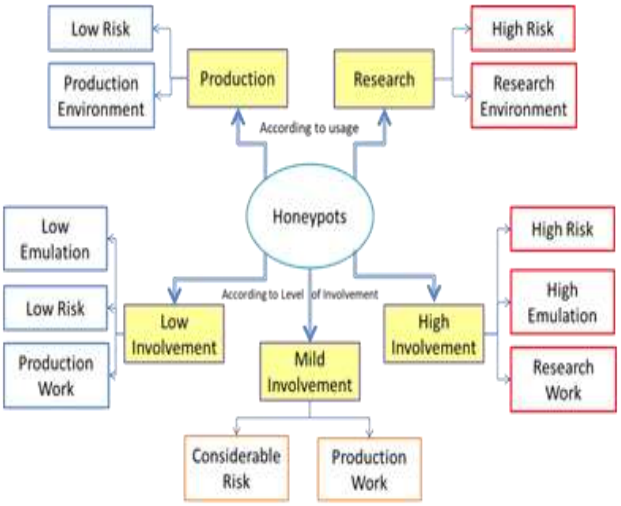
الجدران النارية Firewalls و أنظمة كشف الاختراق IDS يمكن اعتبارها أجهزة جيدة في حماية الشبكة الحاسوبية كما يسعى الباحثون في هذا المجال إلى تطويرها باستمرار لكن هذا لم يعد كافيا على مواكبة التطور السريع للمهاجمين وتقنياتهم المتبعة حيث عانت بشكل أساسي من عجزها عن كشف أو وقف الهجمات غير المعروفة لذلك أصبح من الضروري أن يتم تحقيق مستوى جيد من الأمن والذي لم تستطع تأمينه تلك الأدوات التقليدية [3]. كما من المفترض أيضا أن لا يتركز الاهتمام فقط على آليات الدفاع إنما يجب الاعتماد على خداع المهاجم والمبادرة إلى كشف هجومه الجديد قبل أن يستهدف أي جزء من المنظومة الشبكية.يجب ألا تقتصر آليات الدفاع عن أمن الشبكات الحاسوبية على التصرف عند كشف محاولة هجوم ماءبل يجب أن تمتلك القدرة على توقع سلوك المهاجم وإمكانية إنشاء أنواع جديدة من الهجمات اعتمادا على تحليل سلوك وتسلسل العمليات الخاصة بكل هجمة. لذا فأن مصائد الاختراق والتي عبارة عن نمط خداعي يستخدم لجذب المهاجم وصرف انتباهه بعيدا عن الأنظمة الإنتاجية الفعلية كما يؤمن بيئة عمل لدراسة التقنيات والطرق المتبعة من قبل المهاجمين على المنظومة ومنعهم من إنشاء هجوم خارجي لأنظمة أخرى[4].

مصائد الاختراق (Honeypots):

مع تزايد المخاطر التي تتعرض لها أي شبكة بشكل كبير وتأثيرها على عمل المنظومة عموماً، وبالرغم من تواجد آليات و أدوات للحد منها ومنعها من أحداث الإضرار في الشبكة إلا أنه لا يمكن القول بأنه هنالك منظومة خالية من المخاطر أو قادرة على الاستمرار في ذلك. فوجود مضادات الفيروس والجدران النارية وأنظمة كشف الاختراق لا يعني أن الشبكة ستكون بمنأى عن وصول المهاجم إليها، كل ذلك بسبب وجود فيروسات وهجمات جديدة تعتمد على طرق وتقنيات متنوعة لاختراق البنية التحتية الأمنية الخاصة بالشبكة والتي لا يمكن اكتشافها عبر التقنيات المتواجدة والمذكورة سابقا[2][3]. ولتفادي هذه المشكلة وعدم تفاقمها بات من الضروري أن تتواجد بعض التقنيات التي يتم تصميمها من أجل أن تكون مصيدة للمهاجم وذلك لتكون قادرة على تعلم التقنيات الجديدة التي يستخدمها وتحفيزها على التفاعل معها بشكل أكبر للحصول على أكبر كمية من المعلومات القيمة. لذلك ظهرت الحاجة لوجود مصائد الاختراق Honeypots حيث كان الهدف الرئيسي من التصميم هو خداع المهاجم عبر نظم تشغيل وخدمات مقلدة لما هو موجود ضمن المنظومة وذلك للتفاعل معها واستخلاص أكبر قدر ممكن من المعلومات القيمة عن المهاجم وتقنياته المتبعة و الأدوات البرمجية المستخدمة حيث أن أي حركة بيانات مع مصائد الاختراق تعتبر حركة مشبوهة وذلك لعدم تواجد أي مورد أمني ضمنها ولعدم تأمينها أي خدمة حقيقية[4][5].

تصنيف مصائد الاختراقHoneypots:

يبين الشكل التالي النواحي التي يتم تصنيف Honeypots بالنسبة إليها:



شكل 1: تصنيفHoneypots [4]

1. من ناحية الغرض المستخدم:

بشكل عام يتم تصنيف Honeypots إلى أغراض إنتاجية Productionوأغراض بحثية Research [4] .

1.1 مصائد الاختراق الإنتاجية:

تستخدم لتخفيف المخاطر حيث تعتمد على تقليد نظم التشغيل مع خدماتها تتميز هذه المصائد بسهولة تصميمها وتنفيذها. تكثر استخداماتها في الشركات التجارية، تساعد على الحماية من المخاطر التي تولد أوتوماتيكيا، تعمل على إبطاء عملية فحص الشبكة التي يعتمدها المهاجم مما يعني إضاعة وقته كما تمنع حدوث بعض الهجمات بشكل تام.

2.1 مصائد الاختراق البحثية:

تعتمد على أنظمة تشغيل وخدمات حقيقة يتعامل معها المهاجم بشكل فعلي مما يستدعي خطورة أكبر على المنظومة، لكن بالمقابل تستخدم لإدراك المعلومات حول الهجمات الجديدة من فيروسات أو نشاطات خبيثة والتقنيات التي يستخدمها المهاجم وآليات الاختراق التي اتبعها، مما يعطي نظرة عامة عن المنظومة ونقاط ضعفها. كما تستطيع تأمين كشف وضع الهجوم بالإضافة إلى معلومات عن آلية الرد بالاعتماد على سجل المعلومات المخزنة عن هذا الهجوم.هذا النوع لا يقدم قيمة مباشرة للمنظومة، إنما يؤمن معلومات إضافية ذات قيمة عالية من أجل وضع سياسات حماية جديدة تحمي هذه المنظومة

مستقبليا لكنه يتطلب وقت كبير للتصميم والتنفيذ ويعاني من صعوبة الصيانة، وبشكل عام يستخدم هذا النوع في الأوساط العسكرية والحكومية مع المهاجم لاكتشاف ثغرات جديدة مثل ثغرات Zero-day[5][4].

كما تصنف مصائد الاختراق حسب الإمكانية التي تتيح للمهاجم أن يتعامل معها إلى ثلاثة تصنيفات[4][5]:

1.2مصائد الاختراق منخفضة التفاعل

هنا لا يوجد نظام تشغيل لكي يتعامل معه المهاجم، إنما هي عبارة عن أدوات برمجية يتم تنصيبها من أجل تقليد نظم التشغيل والخدمات المتاحة والتي تقوم بدورها بالتعامل مع المهاجمين والشفرات الخبيثة، هذه الخدمات يتم التصنت عليها عبر منفذ معين مثل التصنت على المنفذ رقم 80 لبروتوكول تصفح الانترنتHTTP وتوثيق حركة مرور البيانات عبرها بالكامل هذه الآلية تمكن من التعرف على حركة المرور الواردة إلى الشبكة عبر منفذ معين وتخزينها لكنها لا تنجح دائما وخصوصا مع البروتوكولات المعقدة مثل عملية التصافح Handshakeفي بروتوكول نقل البريد الالكترونيSMTP، وذلك لأن الخدمة التي تقوم بعملية الرد لا يمكن التصنت عليها. هذا الصنف يعتبر مشابها لأنظمة كشف الاختراق IDS حيث أن كلاهما يعتمد على التصنت فقط ولا يؤمن التفاعل مع المهاجم. يتم استخدام هذا النوع فقط لتوليد إنذارات لأي نشاط مشبوه وارد إلى الشبكة مطابق لما هو مخزن مسبقا أي يمكن اعتبارها كاتصال باتجاه واحد فقط يتم التصنت عليه لكن لا يتم الرد. هذا الأسلوب يخفف من الخطر على المنظومة، إنما من الممكن كشفه من قبل مهاجم محترف بنسبة كبيرة، ويتضمن عدة خيارات مثل أدوات فحص المنفذ، إنشاء قاعدة بيانات عن الهجمات السابقة وتحليل اتجاه الهجوم، وكمثال عليها HONEYD وهو عبارة عن برمجية مفتوحة المصدر تقوم بإنشاء مضيفين افتراضيين ويتم تشغيل خدمات وهمية عليها وأنظمة تشغيل مقلدة لما هو موجود على الواقع، كل مضيف يستطيع أن يستغل عدة عناوين انترنتIPs غير مستخدمة ضمن الشبكة فعلى سبيل المثال منظومة تحتوي على أنظمة تشغيل وخدمات وموجهات يمكن تشكيلها افتراضياً عبر مضيف واحد بعدة عناوين منطقية، فمثلاً يمكن أن تُستخدم لمراقبة منافذ برتوكول التحكم بالارسال TCP إما للتصنت أو لمراقبة محاولات المهاجم لإنشاء اتصال مع الخدمة المُقلدة. يؤمن HONEYD حماية مستقرة عبر تأمين آلية كشف وتقدير للمخاطر كما يعمل على إعاقة المهاجمين عبر النظم الحقيقية [4].

2.2 مصائد الاختراق متوسطة التفاعل

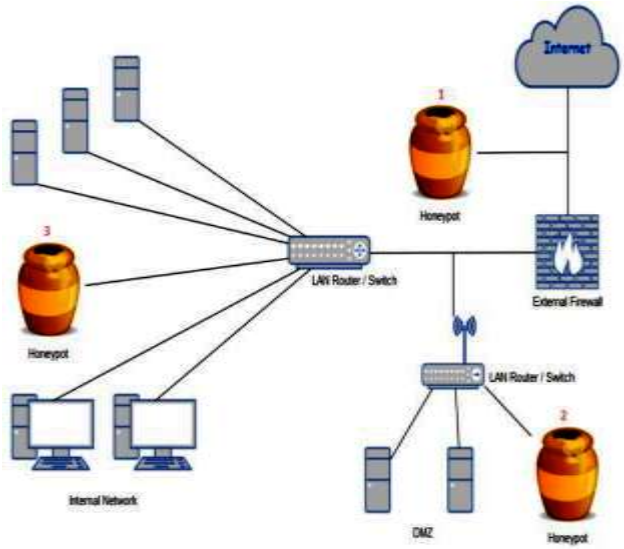
هذا النوع شبيه بمصائد الاختراق منخفضة التفاعل من حيث عدم تواجد نظم تشغيل وخدمات حقيقية، إنما يؤمن مستوى تفاعل أكبر ويستهلك وقت أطول مع زيادة في التعقيد، وهنا يتم التعامل مع مهاجمين أكثر خطورة ولديهم معرفة حول الخدمات المتاحة، مما يستدعي زيادة الخطر أي زيادة احتمالية اكتشاف ثغرة في المنظومة واستغلالها بشكل عام. كلما زادت نسبة التفاعل مع المهاجم كلما زادت احتمالية الخطر على المنظومة في حين أن كمية وقيمة المعلومات المستخلصة من الهجوم سوف تزداد وكمثال علي هذا النوع:[7] Cowrie [6]-Dionea

3.2 مصائد الاختراق عالية التفاعل

هنا يتعامل المهاجم مع أنظمة تشغيل حقيقة وخدمات فعلية مما يزيد من الخطورة على المنظومة، لكن بالمقابل تزداد كمية وفعالية المعلومات المستخلصة عن المهاجم بالإضافة إلى كشف نقاط ضعف الشبكة. إن هدف المهاجم لاختراقه لشبكة ما هو الحصول على مسار ثابت للوصول إلى ضحيته. هذا النمط من المصائد يوفر للمهاجم هذه البيئة لكن بأسلوب مخادع من أجل أن يتم التفاعل الكلي معه، حيث يتم تأمين هذا الشكل الوهمي للأنظمة عبر تنصيبها باستخدام بيئة عمل ظاهرية VMware، مما يستدعي قيام المهاجم بتشغيل شفرات مخصصة لإنشاء هجوم زمني على هذه البيئة الافتراضية دون الضرر بالبنية التحتية الأمنية للمنظومة. هذا النمط يستغرق وقت طويل ويحتاج إلى مراقبة دائمة. بمعنى آخر يتطلب وجود آلية تحكم شمولية ومتينة من أجل منع أي اختراق من قبل المهاجم، وكمثال على هذا النوع Honeynets وهو عبارة عن شبكة متعددة الأنظمة يمكن أن تجمع معلومات عميقة عن المهاجمين مثل جلسات العمل و التقنيات المستخدمة للهجوم و استكشاف نقاط ضعف المنظومة[8].

مواضع تواجد مصائد الاختراقHoneypots:

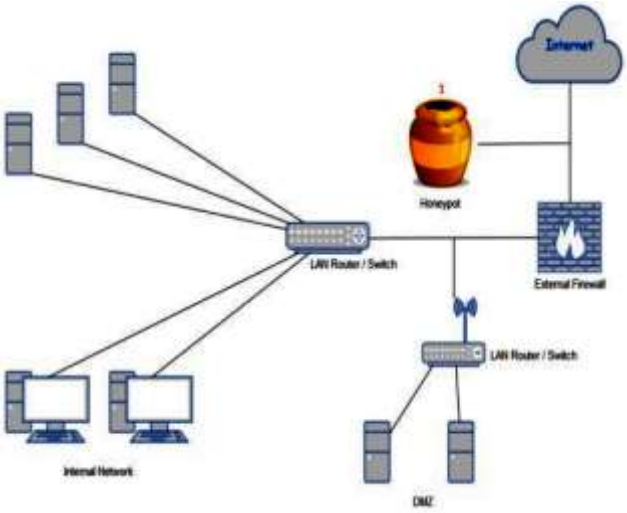
لا تحتاج مصائد الاختراق Honeypotsإلى بيئة محددة لكي تتأقلم معها لأنها تعتبر كنظم معيارية دون أي احتياجات محددة، حيث بإمكانها أن تتموضع في أي مكان ضمن الشبكة حسب التصميم المطلوب ومستوى الحماية المراد تحقيقه. لكن بالرغم من ذلك هنالك بعض الأماكن يفضل أن تتواجد فيها أكثر من غيرها، سوف نستعرض في الشكل التالي ثلاثة مناطق رئيسة يمكن أن تتواجد فيها المصائد[4].



شكل 2: تموضع Honeypots[4]

1. أمام الجدار الناري:

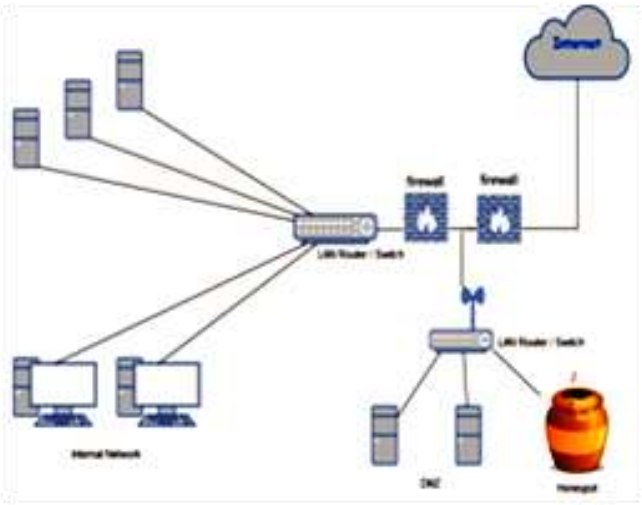
عند وضع مصائد الاختراق أمام الجدار الناري فإن الخطر على الشبكة الداخلية لا يزداد وإن تواجد نظام خبيث خلفه يصبح أمرا غير ممكنا، ولكن يمكن أن يسبب ذلك مشكلة خاصة في حال لم تتواجد جدران نارية داخلية أخرى تحمي بعض الموارد الهامة من أي هجوم داخلي.في هذه الوضعية تقوم المصائد بتوثيق جميع النشاطات غير المرغوب بها والواردة من خارج الشبكة مثل آلية تفحص المنافذ (Port Scaning)، عندها فإن هذه الأنشطة لن يتم توثيقها من قبل الجدار الناري أو نظام كشف الاختراق IDS لذلك لن يتم توليد إنذارات داخلية. بشكل عاملا يزيد هذا النموذج خطر على الشبكة بل أنه يقلل من احتمالية التعرض لهجوم جديد، إلا أن المشكلة الوحيدة تكمن في حال تواجد مهام داخلية فإنه بالإمكان إحداث ضرر بسهولة داخل الشبكة وخصوصا إذا كان الجدار الناري يمنع مرور البيانات من داخل الشبكة إلى[4][3]Honeypots.



شكل3: تموضع Honeypots أمام الجدار الناري

2. داخل Demilitarized Zone Router:

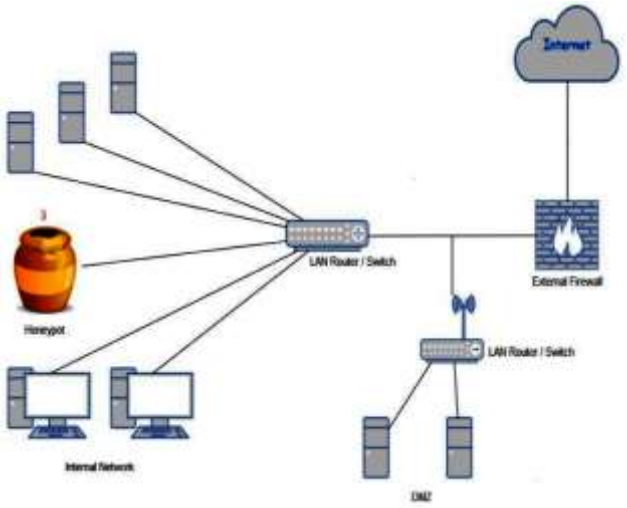
وجود مصائد الاختراق داخل DMZ من أفضل الحلول حيث تكون جميع الخدمات مؤمنة وغير متاحة للوصول إليها من مهاجم خارجي أو داخلي بالإضافة لذلك فإنها تسهل عملية تقليد هذه الخدمات، ولكن من الضروري في حالة تواجد المصائد خلف الجدار الناري أن يتم فتح كل المنافذ عبر الجدار الناري، مما يستدعي خطورة أكبر ووقت أطول، لكن بوجودها داخل DMZ يتم التخلص من هذه المخاطر. تكمن السيئة الوحيدة هنا في زيادة العبء والطلب على هذه الأجهزة مما يتطلب إدارة مكثفة[4][3].



شكل4: تموضع Honeypots داخل DMZ

3. خلف الجدار الناري :

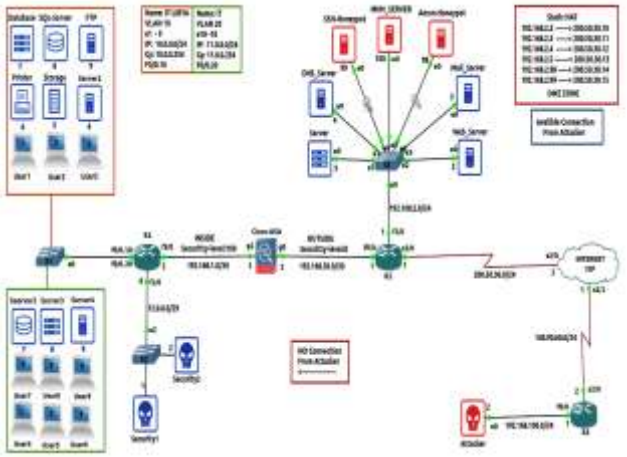
السبب وراء ذلك هو كشف الهجمات الداخلية التي من الممكن أن تتعرض لها الشبكة، تؤمن مصائد الاختراق العديد من الخدمات الوهمية، ومن أجل أن يتم اختراقها يجب ضبط قواعد الجدار الناري للسماح بهذه النشاطات بالمرور عبرها، وعدم توليد إنذارات كلما هوجمت مصائد الاختراق. تكمن الخطورة هنا في فشل المصائد وقدرة المهاجم على دخول الشبكة، عندها تصبح كمنفذ للمهاجم إلى داخل الشبكة وعندها لا يمكن للجدار الناري كشف ذلك لأنه قد اعتبرها مسبقا تابعة للمصائد وسمح لها بالعبور، لذلك تكمن أهمية حماية الشبكة داخليا وجعل هذه الحماية إجبارية وخصوصا إذا كانت المصائد ذات المستوى عالي التفاعل[4][3].



شكل5: تموضع Honeypots خلف الجدار الناري

إطار العمل المقترح

في هذه الدراسة تم برمجة الشبكة كما مبين بالشكل (6) بحيث يستطيع المهاجمAttacker الوصول إلى شبكة مصائد الاختراق Honeypots ولا يستطيع الوصول إلى الشبكة الداخلية وذلك لوجود الجدار الناريFirewall وقوائم نظام الدخولACL. حتى ولو تم اختراق خوادم Honeypots وباقي الخوادم الحقيقية لن يستطيع الوصول إلى الشبكات الداخلية لان شبكة DMZ معزولة تماما عن الشبكة الداخلية.الشبكة الداخلية تستطيع الوصول إلى شبكة DMZ ولكن شبكة DMZ لا تستطيع الوصول إلى الشبكة الداخلية.



شكل6: إطار العمل المقترح

كذلك تم استخدام الخادم مركزي MHN وهو خادم مفتوح المصدر يستخدم لإدارة وجمع البيانات من مصائد مخترقي الشبكات. تم تطوير MHN من قبل Threat Stream في سنة 2015 و يتميز بسهولة نشر أجهزة الاستشعار بسرعة وجمع البيانات فورا وعرضها في واجهة الويب[9].

أنواع مصائد الاختراق المستخدمة في إطار العمل

- **مصيدة الاختراق Cowrie**

هي عبارة عن أداة مكتوبة بلغة البايثون Python تقوم بعمل محاكاة لخادمSSH بالكامل ويمكن للأداة التفاعل مع المستخدم ومواصلة الخدعة معه قبل الهجوم وبعد الهجوم بحيث يقوم بمحاولة كسر عملية تسجيل الدخول إلى خادمSSH وإذا كان مدير الخادم يريد له أن ينجح سوف يجعل كلمة المرور سهلة ثم يسمح له بالدخول إلى نظام ملفات وهمي يحتوي على نسخه طبق الأصل من نظام الملفات الموجود على الخادم الحقيقي حيث يستطيع الدخول إلى مجلد etc ويسحب ملف كلمات المرورpassword ويصنع ما يريد من إنشاء ملفات وحذف والعديد من الأمور بهذا كله سوف يقوم مدير الخادم بمعرفة ماذا يريد المهاجم من الخادم وماهي الملفات ونوع المعلومات التي يريد سحبها وما هو غرض الاختراق والكثير من المعلومات[10][11].

- **مصيدة الاختراق Amun**

هي أول مصيدة اختراق منخفضة التفاعل مبنية على لغة البايثون Python، يتم تشغيل خدمات وهمية عليها وتعتمد على التنصت فقط ولا تؤمن تفاعل مع المهاجم يتم استخدامها فقط لتوليد إنذارات لأي نشاط مشبوه وارد إلى الشبكة. هذه الخدمات يتم التنصت عليها عبر منفذ معين مثل التنصت على المنفذ رقم 80 لبروتوكول تصفح الانترنت HTTP أي يمكن اعتبارها كاتصال باتجاه واحد فقط يتم التنصت عليه لكن لا يتم الرد. هذا الأسلوب يخفف من الخطر على المنظومة عن طريق صرف انتباه المهاجم واستغلال وقته[12].

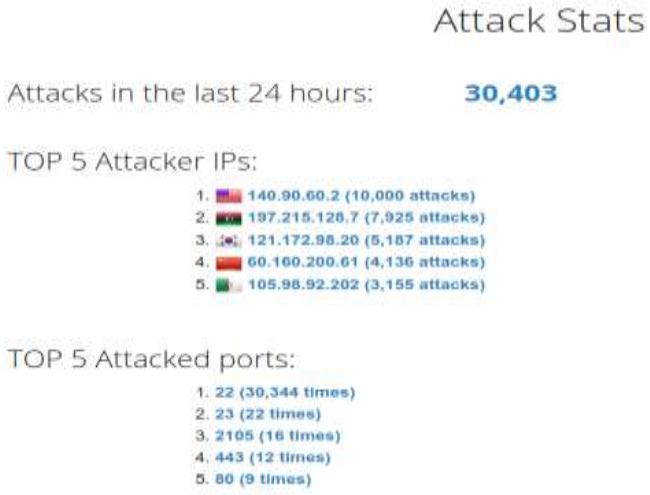
النتائج العملية

في هذه الدراسة قمنا بعدة تجارب كل منها كان يهدف إلى قيام المهاجمAttacker بمهاجمة الشبكة واستغلال كل الثغرات والمعلومات التي تحصل عليها من عمليات الفحص وذلك من خلال الخطوات التالية:

1. فحص الشبكة Network Scanning اذا كانت نشطة أو لا Online or Offline.
2. فحص المنفذ Port Scanning والاطلاع على الخدمات النشطة.
3. فحص الخدمات Service Scanning والهجوم على اى منها.

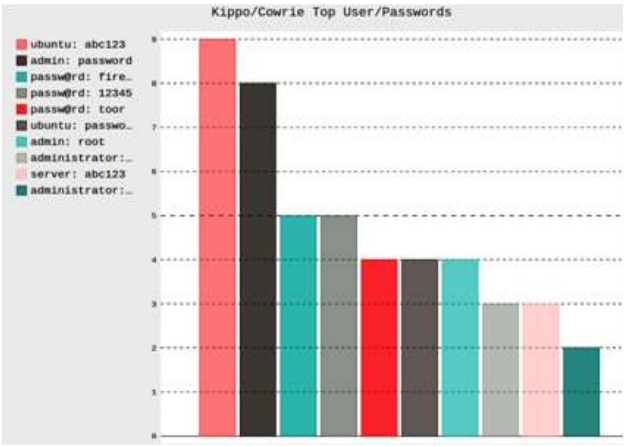
بعد قيام المهاجم بمحاولات الاختراق ندخل إلى الخادم-M Server للإطلاع على النتائج. كما مبين في الشكل (7) نلاحظ انه خلال 24 ساعة تم تسجيل 30,403 محاولة اختراق كان

العدد الأكبر منها مصدره USA بحوالي 10000 هجمة بينما سجلت 3155 هجمة من الجزائر.في حين أن العدد الأكبر من الهجمات كانت من خلال المنفذ 22 بينما سجل المنفذ رقم 80 عدد 9 هجمات فقط.

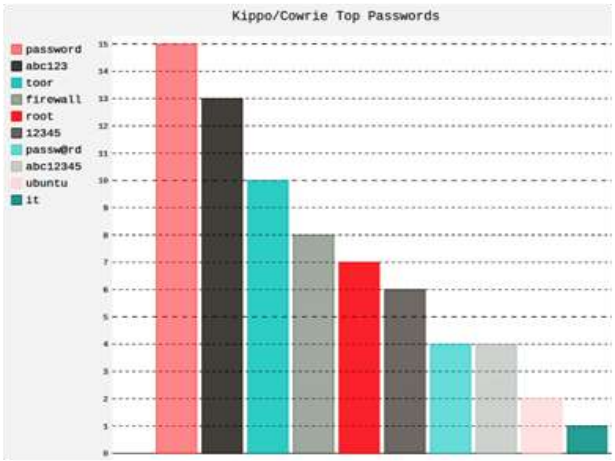


شكل 7: تقرير عن عدد الهجمات.

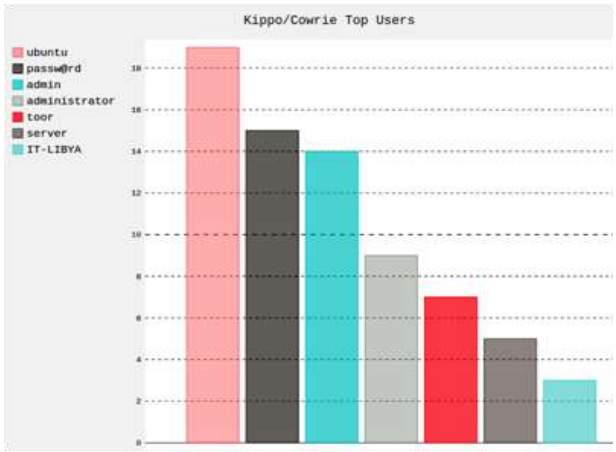
الأشكال البيانية (8) – (10) تبين تفاصيل عدد المحاولات التي قام بها المهاجم Attacker وذلك لمحاولة معرفة كلمة المرور الحقيقية من خلال استخدام العديد من أسماء المستخدمين وكلمات المرور. حيث أن المهاجم في كل محاولة يستخدم كلمة مرور مع اسم مستخدم إلى أن يصل إلى اسم المستخدم وكلمة المرور الخاصة بالخادم. وبهذا قد تم جمع المعلومات التي استخدمها المهاجم Attackerلتسجيل الدخول. على سبيل المثال تم استخدام أسم المستخدم ubuntu وكلمة المرور abc123 من قبل 9 مهاجمين في حين تم استخدام Admin كأسم مستخدم وroot كلمة مرور من قبل 4 مهاجمين كما موضح بالشكل (8). الشكل (9) يبين عدد الهجمات التي تم فيها استخدام كلمات مرور مختلفة فعلى سبيل المثال كان أعلى استخدام لكلمة المرور Passwordبحوالي 15 هجمة بينما استخدمت كلمة المرور it مرتين فقط. يوضح الشكل (10) عدد المحاولات التي تم فيها استخدام أسماء مستخدمين مختلفة فبينما لم يستخدم IT-LIBYA كأسم مستخدم إلا في ثلاث هجمات فقط ، سجلت في المقابل 19 هجمة مستخدمين اسم المستخدم ubuntu. من خلال النتائج المبينة في الأشكال (8) – (10) ،فإن إطار العمل المقترح باستخدام مصائد الاختراق المذكورة سابقا تمت من خلاله استخلاص أسماء المستخدمين وكلمات المرور الأكثر استخداما في الهجمات. هذا يبين بأن الإطار المقترح أسهم وبشكل فعال بضرورة بناء نظام يعتمد على اختيار أسماء مستخدمين وكلمات مرور غير متداولة وضرورة تحديثها من وقت إلى آخر. الدراسة اعتمدت على تحليل ما يستخدمه المهاجم للدخول إلى الشبكة وليس على تحليل نوع الهجمة حسب ماتمت دراسته في [4]والذي يعتمد على تهجين مصائد الاختراق للتحليل نوع واحد من الهجمات وهو DoS.



شكل8: محاولات الاختراق باستخدام كلمات المرور وأسماء المستخدمين

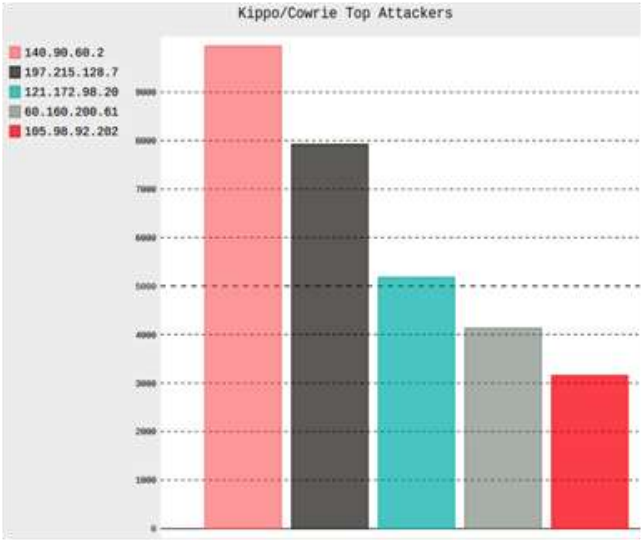


شكل 9: محاولات الاختراق باستخدام كلمات المرور



شكل 10: محاولات الاختراق باستخدام أسماء المستخدمين

الدراسة لم تعتمد على استخلاص أسماء المستخدمين وكلمات المرور كما تمت دراسته في [5] بل أيضا تم استخلاص عناوين الـــ IP الخاصة بالمهاجمين.يبين الشكل (11) عناوين الـــ IP الخاصة بالمهاجمين وعدد محاولات الهجمات التي تمت من كل عنوان. كانت عدد هجمات العنوان 140.90.60.2 حوالي 10000 مسجلة أعلى معدل هجمات بينما سجل العنوان 105.98.92.202 اقل معدل هجمات مسجلا حوالي 3155 هجمة. من خلال هذه النتائج يتم فورا إتباع الإجراءات اللازمة لمنع المهاجم من محاولة الاتصال بالشبكة مرة أخرى ويتم إضافة عنوان الـــIPالخاص به إلى قائمة الحظرBlockLIST في الجدار الناري Firewall.



شكل 11: العناوين المنطقية للمهاجمين

في داخل خادمMHN-Server توجد كذلك أداة مميزة تسمى (Honey-map). هذه الأداة هي عبارة عن خريطة تستخدم لتوضيح مصدر الهجمات التي تحصل في الوقت الحقيقي بناءً على عنوان IP Address. يتم الاستفادة من هذه الخاصية وذلك بالدخول إلى خريطة مصيدة الاختراقHoney-map عن طريق كتابة عنوان الـــ IP مع رقم المنفذ Port:3000 كما هو موضح في الشكل (12)

شكل 12: أداة Honey - map

الخلاصة

في هذه الدراسة تم تصميم أنظمة مصائد اختراقHoneypotsباستخدام هجوم التخمين Brute-Force على بروتوكول SSH باستخدام أداة Nmap وذلك لخداع المهاجم عن طريق إنشاء نظم تشغيل وخدمات وهمية وذلك لاستدراج المهاجم Attacker وصرف انتباهه بعيداً عن الأنظمة الإنتاجية الفعلية. من خلال نتائج هذه الدراسة أثبتت أنظمة مصائد الاختراقHoneypots كفاءتها من خلال معرفة الطرق والأساليب التي يستخدمها المهاجم Attackersليتمكن من الوصول إلى معلومات حساسة في المنظومة الشبكية. هذا وقد تم استخدام المعلومات التي تم الحصول عليها من اجل تحسين وتطوير أنظمة الحماية لتجنب أي محاولات أخرى لاختراق الشبكة.

المراجع

[1]- عقبه عباس (2019) "تحسين أداء نظم كشف الاختراق في الشبكات المعرفة برمجيا باستخدام تعلم الآلة" ، أطروحة ماجستير، المعهد العالي للعلوم التطبيقية والتكنولوجيا، الجامعة العربية السورية.

[2]- محمد حمدان (2017) "تحسين أداء أنظمة كشف الاختراق باستخدام المنطق العصبي الترجيحي"، المعهد العالي للعلوم التطبيقية والتكنولوجيا.

[3]- بشرى ديوب (2015) "دراسة ومقارنة أنظمة كشف الاختراقات المفتوحة المصدر" ، مجلة جامعة تشرين للبحوث والدراسات العلمية، سلسلة العلوم الهندسية المجلد (37) ، العدد (5).

[4]- حازم عدنان سلوم (2017) "تحسين نظم كشف الاختراق باستخدام تقنية مصائد الاختراق الهجينة"، أطروحة

ماجستير، المعهد العالي للعلوم التطبيقية والتكنولوجيا، الجامعة العربية السورية.

[5]- S. Bhanu, G. Khilari, and V. Kumar (2014) "Analysis of SSH attacks of Darknet using Honeypots", International Journal of Engineering Development and Research, Vol (3), Issue (1).

[6]- MichelOosterhof (2020)," Cowrie Documentation Release19.10.0" [Online] available at:https://github.com/cowrie/cowrie.

[7]- "Dionaea's documentation" (2020) available at: https://dionaea.readthedocs.io/en/latest/

[8]- The Honeynets Project (2020),available at:http://www.honeynet.org/tools/sebek/.

[9]- Modren Honeypots Network [Online] available athttps://github.com/pwnlandia/mhn

[10]- Joshua Faust (2018)," Distributed Analysis of SSH Brute Force and Dictionary Based Attacks", St. Cloud State University.

[11]- R. Mahmoud and J. Pedersen (2019) "Deploying a University Honeypot: A case study", research paper pp 27-38.

[12]- Amun: Python Honeypot [Online] available athttp://amunhoney.sourceforge.net