



# Extended Detection & Response



## Extended Detection and Response (XDR)

### الكشف والاستجابة الموسعة

إعداد الطلاب:

2020020423	حسين طربوش الصلوي
2020020809	عبدالجليل أمين الطائفي
2020021360	معاذ سمير الوصابي
2020021361	حمزه سمير الوصابي
2019070082	احمد شايف الصلوي
2020020769	غيدان منصور الخضمي

المشرف

د. عدنان المتوكل

تقرير مشروع التخرج مقدم لقسم أمن المعلومات استيفاء لمتطلبات درجة البكالوريوس في الأمن السيبراني

2024

## خلاصة

---

واحدة من أكبر المخاطر المرتبطة بالنمو الكبير واستخدام تكنولوجيا المعلومات المتشابكة مع الإنترنت هي الجرائم السيبرانية. أجبرت الزيادة المقلقة في نشاط المجرمين السيبرانيين على مر السنين المؤسسات على اتخاذ تدابير دفاعية واستخدام أحدث التقنيات دائماً لنفس الغرض. تظهر التطورات الحالية أن الشركات الصغيرة والمتوسطة هي الكيانات الأكثر عرضة لتهديدات وهجمات الأمن السيبراني. يوضح هذا البحث مختلف التحديات المتعلقة بالأمن التي يتعرض لها الشركات الصغيرة والمتوسطة مواجهتها اليوم مع توضيح السيناريوهات لزيادة الوعي حول مدى أهمية التعامل معها وتجنب العواقب.

يتناول بحثنا التحقيق في منهجية المرونة السيبرانية في المؤسسات الصغيرة والمتوسطة الضارة، ويقترح حل شامل يستخدم التحليل التوجيهي للبرامج الضارة واكتشافها والاستجابة لها باستخدام حلول مفتوحة المصدر للكشف عن التهديدات الناشئة الجديدة. من خلال الاستفادة من الحلول والبرامج مفتوحة المصدر، تم تطوير نظام مصمم خصيصاً للشركات الصغيرة والمتوسطة التي تضم ما يصل إلى ٢٥٠ موظفاً، مع التركيز على اكتشاف التهديدات الجديدة. من خلال الاختبارات المكثفة والتحقق من الصحة، بالإضافة إلى التكامل مع التقنيات الفعالة للكشف عن الحالات الشاذة والسلامة والأمن، يتم إثبات فعالية النهج في تعزيز قدرات الدفاع السيبراني للشركات الصغيرة والمتوسطة وتعزيز مرونتها الإلكترونية بشكل عام. تسلط النتائج الضوء على التطبيق العملي وقابلية التوسيع في استخدام الموارد مفتوحة المصدر لمعالجة تحديات الأمن السيبراني الفريدة التي تواجهها الشركات الصغيرة والمتوسطة. يجمع النظام المقترن بين تقنيات تحليل البرامج الضارة المتقدمة ومجازات استخبارات التهديدات في الوقت الفعلي لتحديد وتحليل الأنشطة الضارة داخل شبكات الشركات الصغيرة والمتوسطة. من خلال استخدام أداة **Wazuh** ودمجها مع بعض أدوات الأمان مفتوحة المصدر، يمكن للنظام اكتشاف وتصنيف البرامج الضارة والتهديدات الأمنية بشكل فعال لتقدير فعالية النظام، تم إجراء اختبارات باستخدام مجموعات البيانات والسيناريوهات الواقعية. وتظهر النتائج تحسينات كبيرة في معدلات الكشف عن البرمجيات الخبيثة، حيث نجح النظام في تحديد التهديدات الناشئة التي غالباً ما تغفل عنها التدابير الأمنية التقليدية. يمثل النظام المقترن حلًا عمليًا وقابلًا للتطوير باستخدام أداة **Wazuh** التي يمكن نشرها بسهولة من قبل الشركات الصغيرة والمتوسطة التي تسعى إلى تعزيز قدراتها الدفاعية السيبرانية.

## تفويض

نحن نصرح للجامعة الإماراتية الدولية كلية الهندسة وتكنولوجيا المعلومات بتوفير نسخ من تقرير مشروع التخرج للمكتبات أو المنظمات أو الأفراد عند الطلب.  
كما يحق للكلية استخدامها في المسابقات المحلية أو الدولية.

اسم الطالب	رقم الطالب	التوقيع	التاريخ
حسين طربوش الصلوي	2020020423		2024-06-09
عبدالجليل أمين الطائفي	2020020809		2024-06-09
معاذ سمير الوصابي	2020021360		2024-06-09
حمزة سمير الوصابي	2020021361		2024-06-09
احمد شايف الصلوي	2019070082		2024-06-09
غيدان منصور الخضمي	2020020769		2024-06-09

## شكر وتقدير

---

وأنقدم بخالص التقدير إلى كل من لعب دوراً حاسماً في إنجاح هذا المشروع. أود أن أعرب عن امتناني الكبير لمشرف المشروع، د. عدنان المتوكل، الذي أثرت قيادته التي لا تنزعزع وخبرته العميقة وتوجيهاته الثاقبة بشكل كبير في اتجاه هذا المسعى وتنفيذه. كما أننا نشعر بالامتنان العميق لقادة الأجيال د. مالك الجبري، و د. جميل راشد على توفيرهم الدعم والتشجيع السخي في بناء المشاريع والأبحاث.

ونتوجه بالشكر الخاص إلى زملائنا وأصدقائنا الذين لم يشاركوآراءهم ووجهات نظرهم القيمة فحسب، بل شاركوا في محادثات مفيدة، وقدموا الدعم على وجه التحديد عندما كانت هناك حاجة إليه بشدة، ولعبت مدخلاتهم التعاونية دوراً محورياً في تحسين المفاهيم التي تمت مناقشتها في هذا المشروع.

نعرب عن خالص امتناننا لمؤلفي العديد من المقالات العلمية والكتب والموارد عبر الإنترنوت التي كانت بمثابة مراجع لا تقدر بثمن، مما أدى إلى إثراء عمق بحثنا.

أخيراً، لا يمكننا المبالغة في تقديرنا لعائلتنا، فمساعدتهم الدائمة وتعاطفهم اللامحدود ودعمهم الذي لا ينزعزع، خاصة خلال الفترات الصعبة.

أخيراً، نتوجه بالشكر العميق لكل مساهمن، بغض النظر عن مدى صغر دوره، على تأثيره الجماعي في نجاح هذا المشروع. لقد ترك دعمهم علامة لا تمحى على تطورنا الأكاديمي والشخصي. نحن نوجه خالص الشكر والتقدير حقاً للجميع.

## شهادة المشرف

**I certify that the preparation of this project entitled**

**prepared by** .....

**was mad under my supervision at ..... department in partial  
fulfillment of the requirements of bachelor degree in**

### اسم المشرف

## التوقيع

## تاریخ

## لجنة الممتحنين

عنوان المشروع : .....

### مشرف

التوقيع	الموضع	الاسم	م
			1

### لجنة الممتحنين

التوقيع	الموضع	الاسم	م
			1
			2
			3
			4

رئيس القسم

د. جميل راشد

.....



## جدول المحتويات

II .....	خلاصة .....
III .....	نفيض .....
IV .....	شكر وتقدير .....
V .....	شهادة المشرف .....
VI .....	لجنة الممتحنين .....
١ .....	جدول المحتويات .....
٢ .....	قائمة الأشكال .....
٣ .....	قائمة الجداول .....
٤ .....	قائمة الاختصارات .....
٥ .....	الفصل الأول: مقدمة .....
٥ .....	نظرة عامة .....
٦ .....	بيان المشكلة .....
٨ .....	أهداف وغاية المشروع .....
٨ .....	نطاق المشروع والقيود والمخاطر .....
٨ .....	نطاق المشروع: .....
٩ .....	حدود المشروع: .....
٩ .....	المخاطر .....
١٠ .....	منهجية المشروع .....
١٠ .....	هيكل التقرير .....
١٠ .....	الفصل الثاني: الخلفية ومراجعة الأدبيات .....
١٠ .....	خلفية المشروع .....
١٠ .....	مراجعة الأدبيات .....
٢٠ .....	الفصل الثالث: جمع وتحليل المتطلبات .....
٢٤ .....	الفصل الرابع: تصميم ونمذجة المشروع .....
٣٣ .....	الفصل الخامس: تنفيذ واختبار المشروع .....
٩٣ .....	الفصل السادس: النتائج والمناقشة .....
٩٤ .....	الفصل السابع: الاستنتاجات والتوصيات .....

٩٥	المراجع
٩٦	الملاحق

## قائمة الأشكال

---

قائمة الجداول

---

قائمة الاختصارات

---

## الفصل الأول: مقدمة

### نظرة عامة

تلعب الشركات الصغيرة والمتوسطة دورا حاسما في دفع الابتكار، لكنها تفشل في وضع استراتيجية كافية للدفاع عن الأمان السيبراني. أحد أسباب هذا الإشراف هو التقليل من مخاطر وتأثير الهجمات السيبرانية. غالبا ما يكون هناك اعتقاد خاطئ بأن مجرمي الإنترنت يلحقون فقط المؤسسات الكبيرة رفيعة المستوى. لسوء الحظ، لا يمكن أن يكون هذا أبعد عن الحقيقة. يكشف تقرير التحقيق في خرق البيانات من [Verizon](#) [١] أن ما يقرب من 43٪ من الهجمات الإلكترونية تستهدف الشركات الصغيرة والمتوسطة. سبب آخر لعدم كفاية وضع الأمان السيبراني للشركات الصغيرة والمتوسطة هو أنه بسبب الموارد المالية والبشرية المحدودة، فإنها تكافح لمواكبة التقدم المستمر في هذا المجال سريع التطور. وكثيراً ما تجد المشاريع الصغيرة والمتوسطة الحجم نفسها غير مستعدة لاختيار الأدوات المناسبة لحماية أصولها، مما يعرض للخطر استمرارية أعمالها. منذ تفشي جائحة [COVID-19](#) وعمليات الإغلاق التي تلت ذلك في جميع أنحاء العالم، تبنت المؤسسات العمل عن بعد و يصل الموظفون إلى أنظمة المنظمة عن بعد من منازلهم. وقد خلق هذا فرصة جديدة للجهات الفاعلة الخبيثة ولوحظت زيادة في الهجمات الإلكترونية بعد جائحة [COVID-19](#). وجدت وكالة الاتحاد الأوروبي للأمن السيبراني، [ENISA](#) [٢]، أن تحديات الأمان السيبراني قد تفاقمت أكثر بسبب تأثير جائحة [COVID-19](#) وأن الشركات الصغيرة والمتوسطة لم تكن مستعدة للتعامل مع هذه التحديات. استكشفت دراسة استقصائية حديثة شملت ٨٥ شركة صغيرة ومتوسطة مقرها المملكة المتحدة تهدياتها وتقنيات التكيف مع الهجمات الإلكترونية. كان أحد المخاوف الرئيسية التي أبدتها الشركات الصغيرة والمتوسطة هو الحفاظ على أمان الأجهزة المحمولة وتجنب هجمات التصيد الاحتيالي [٣]. باستخدام استراتيجية الدفاع المتعمق، تنشر المؤسسات عدداً من الحلول الأمنية مثل أنظمة اكتشاف ومنع التسلل من الجيل التالي (NG-IDPS)، وجدران الحماية، وحلول مكافحة الفيروسات، وتجزئة الشبكة، إلخ. يتم نشر هذه الحلول الأمنية عبر البنية التحتية الكاملة للشبكة لضمان الأمان في الوقت الفعلي من خلال المراقبة والاستجابة المستمرة [٤].

على الرغم من توفر مجموعة متنوعة من الحلول الأمنية، يواجه المحتلون صعوبة في مراقبة لوحات معلومات متعددة في وقت واحد وربط الأحداث من أجهزة الأمان المختلفة. علاوة على ذلك، تولد هذه الأجهزة كمية هائلة من الأحداث (السجلات) بتنسيقات متعددة مما يؤدي إلى إرباك إدارة السجل. هذه القضية مهمة بشكل خاص للشركات الصغيرة والمتوسطة التي عادة ما يكون لديها موارد بشرية محدودة وإدارة الأمان يمكن أن تكون في كثير من الأحيان وظيفة بدوام جزئي لفرد واحد [٥]. هذا يجعلهم هدفاً سهلاً لمجرمي الإنترنت. لذلك، فإن النهج العملي للشركات الصغيرة والمتوسطة هو إدارة الأمان الموحدة. يسهل نظام [SIEM](#) ذلك من خلال الجمع الفعال للبيانات من مصادر السجل المتباينة في نظام واحد للتحليل في الوقت الفعلي [٦] يتم تسليميه إلى وحدة تحكم واحدة. نظام [SIEM](#) نفسه ليس جهاز مراقبة نشط في الشبكة ولكنه حل أمني قوي لمراقبة السجلات من أجهزة متعددة وربطها في الوقت الفعلي لمراقبة أي نشاط ضار قد يتم تجاهله بواسطة حلول الدفاع البارا متربة الأخرى للشبكة [٧].

هناك فئتان عريضتان من حلول [SIEM](#)، التجارية والمفتوحة المصدر، مع فوائد وقيود متأصلة. حلول [SIEM](#) التجارية ناضجة تماماً وتتوفر تغطية كاملة على مستوى المؤسسة، وإن كان ذلك بتكليف ترخيص ضخمة. على سبيل المثال، تبدأ التكلفة الإجمالية للملكية (TCO) لمدة ثلاثة سنوات لـ [SolarWinds LEM](#) و [LogRhythm](#) من 50,000 دولار ونفس الشيء بالنسبة لـ [AlienVault USM](#) و [IBM QRadar](#) و [HP ArchSight](#) تبدأ من ٢٥٠,٠٠٠ دولار.

لا تتحمل الحلول مفتوحة المصدر أي تكلفة وهي مفتوحة للتعديل أو التخصيص؛ ومع ذلك، عادة ما تكون مقيدة من حيث الميزات وتفتقر إلى دعم العملاء. هناك عدد من حلول [SIEM](#) مفتوحة المصدر المتاحة في السوق، ومع ذلك،

فإن اختيار حل SIEM الأمثل يمكن أن يكون مهمة صعبة لمعظم الشركات الصغيرة والمتوسطة بسبب نقص الخبرة والموارد لإجراء مقارنات مفصلة واختبار ميزات الأمان والأداء لكل منها.

بصرف النظر عن هذه الزيادة في الهجمات السيبرانية، من المهم ملاحظة أن هذه الهجمات تركز عادة على نقاط النهاية، مثل أجهزة الكمبيوتر وأجهزة الكمبيوتر المحمولة وأجهزة الشبكة وما إلى ذلك. والسبب وراء ذلك هو أنه يُنظر إليها على أنها الحلقة الأضعف في أمن المؤسسة وقد تكون لديها إجراءات أمنية أقل من الأجزاء الأخرى من الشبكة، مع توفير باب للتوسيع إلى الأصول الأخرى للضحية، مثل الخوادم.

من خلال اختراق نقطة النهاية، يمكن للمهاجمين سرقة المعلومات الحساسة ونشر البرامج الضارة واحتراق أجزاء أخرى من الشبكة. لذلك من المهم اكتشاف الجهاز المخترق في أسرع وقت ممكن. ويمكن تحقيق ذلك من خلال نشر أنظمة كشف التسلل، والتي تركز على اكتشاف أنواع متعددة من البرامج الضارة، ومع ذلك، لا يوجد أي منها مستعد تماماً لاكتشاف التهديدات الجديدة أو التي لم يتم اكتشافها.

### بيان المشكلة

هناك العديد من مشكلات الأمان السيبراني التي تواجهها الشركات الصغيرة والمتوسطة في الوقت الحاضر. ونظراً لمحودية الموارد، تصبح هذه المنظمات فريسة للهجمات السيبرانية الداخلية والخارجية. إن الافتقار إلى الأبحاث في هذا المجال بالإضافة إلى النقص الخطير في المعرفة التقنية يجعل من المستحيل تقريراً عليهم الاستعداد بشكل فعال لأي حوادث ومعالجتها. ولهذا السبب، أصبحت الشركات الصغيرة والمتوسطة بشكل متزايد الهدف الرئيسي للتصيد الاحتيالي، وهجمات **DDOS** ، وهجمات البرامج الضارة، وحقن **SQL** وغيرها من الهجمات السيبرانية. يمكن أن تسبب هذه الجرائم أضراراً جسيمة لسمعة منظمة جديدة نسبياً وتتسبب في خسارة الأصول والموظفين ورأس المال. ولجعل الوضع أسوأ، في حالة حدوث حرق أمني، يمكن أيضاً اتخاذ إجراءات قانونية تؤدي إلى غرامة تصل إلى مبلغ يصل إلى ٤ بالمائة من حجم الأعمال السنوي. تجري الشركات الصغيرة عمليات تدقيق داخلية منتظمة تتطلب موظفين إضافيين لمنع حدوث ذلك لإحداث فجوة في جيوبهم.

## Extended Detection and Response

جميع الحلول والمبادئ التوجيهية المقدمة لإدارة الأمان السيبراني قابلة للتطبيق بشكل أكبر على الشركات الكبيرة وغير عملية على الشركات الصغيرة أن تتبناها. ومع ذلك، فإن البحث الذي تم إجراؤه هنا سيوفر حلًا شاملًا للمشاكل التي تمت مناقشتها أعلاه.

### عدم وجود رؤية مركزية:

تعمل أدوات الأمان التقليدية بشكل مستقل وتفقد إلى القدرة على ربط البيانات الأمنية من مصادر مختلفة لأن هذا يتطلب الكثير من الوقت والجهد في المهام اليدوية لجمع وتحليل البيانات التي تشتت الرؤية وتعيق الكشف الفعال عن التهديدات والاستجابة لها. وهذا يجعل من الصعب تتبع الهجمات المعقدة التي تمت عبر أنظمة متعددة.

فرق الأمن غير قادرة على ربط الأحداث من مصادر مختلفة وفهم الصورة الكاملة للتهديد.

### نقص قدرات ربط البيانات:

تفقد أنظمة الأمان التقليدية إلى القدرات الازمة لتوصيل البيانات من مجموعة متنوعة من المصادر، مثل أجهزة الشبكة وأنظمة التشغيل المختلفة وأنظمة التحكم الصناعية.

هذا يحد من قدرة النظام على توفير رؤية شاملة للوضع الأمني واكتشاف التهديدات من مصادر متعددة.

### الاستجابة البطيئة للحوادث:

أوقات الاستجابة للحوادث بطيئة وغير مجدية تقريباً بسبب التأخير، مما تسبب في خسائر كبيرة للمنظمة.

وقد يؤدي ذلك إلى تفاقم الأضرار الناجمة عن الهجوم ومنح المهاجمين مزيداً من الوقت للتصريف.

### حجم تنبيه هائل:

يتطلب الاعتماد على التحليل التقليدي تدخلاً يدوياً مكثفاً لأنه يستغرق وقتاً طويلاً وعرضة للأخطاء، وقد يتم التغاضي عن الأحداث الأمنية الحرجة أو فقدانها وسط كمية هائلة من التنبيهات، مما يترك الأنظمة عرضة للخطر (تجاهل مثل هذه التنبيهات يشكل خطراً أمنياً).

تصدر الأنظمة كمية هائلة من التنبيهات، والتي يمكن أن تغمر فرق الأمن بالبيانات وتجعل من الصعب عليهم تحديد التنبيهات المهمة.

قد يؤدي ذلك إلى تجاهل التنبيهات الحقيقية، مما قد يعرض المنظمة للخطر.

تحتاج أنظمة الأمان إلى ميزات لتحسين أولويات التنبيه بشكل أفضل للمساعدة في التركيز على الأحداث الأكثر أهمية.

### تواجه حلول الأمان الحالية صعوبة في اكتشاف التهديدات المتقدمة:

أصبحت الهجمات الإلكترونية الحديثة أكثر تعقيداً وغالباً ما تتجاوز أنظمة الأمان التقليدية، لذلك تحتاج المؤسسات إلى طريقة لتحليل البيانات الأمنية بعده طرق ومن مصادر مختلفة للحصول على رؤية أمنية أوسع.

### نقص الموارد في الشركات الصغيرة والمتوسطة وارتفاع تكلفة حلول أنظمة الأمن التجاري:

المنظمات الصغيرة ببساطة غير قادرة على تعيين موظفين إضافيين للتعامل بفعالية مع القضايا الأمنية بسبب القيود المالية ولا يمكنها الاستعانة بمصادر خارجية لطرف ثالث بسبب تكلفتها العالية.

### تنسيقات البيانات غير الموافقة:

ترسل أجهزة الشبكة سجلاتها بتنسيقات متعددة، مما يجعل من الصعب على بعض أنظمة الأمان جمعها وتحليلها بكفاءة وإعطاء التقارير، مما يقلل من كفاءة النظام.

### أهداف وغاية المشروع

الغاية من هذا المشروع هو تجسيد والتحقق من أن تقنية **XDR** هي الحل الأنسب لمشاكل الأمان السيبراني التي تواجهها الشركات الصغيرة والمتوسطة حيث سيمثل ذلك بالاعتماد على **Wazuh** أداة العمل الفعلية، وهي ليست مجده فحسب، بل فعالة ومفتوحة المصدر أيضاً وسهلة التنفيذ ويمكن تعديلها وفقاً لمتطلبات أي بيئه صغيرة أو متوسطة الحجم ويهدف هذا المشروع لتنقیل الوقت والجهد الذي يبذله مهندسو الأمان مع العمل اليدوي من خلال:

1. تنفيذ نظام مركزي يجمع ويحلل بيانات الأحداث من جميع مصادر الأحداث ويربطها في نظام مركزي واحد
2. تحسين سرعة الاستجابة: تقليل المهام اليدوية عن طريق أتمتة عملية الاستجابة في الوقت الفعلي للأحداث وتطبيق التقنيات التي تعطي الأولوية للتنبيهات لسهولة الفرز النسائي للأحداث عالية الأهمية.
3. توفير لوحة معلومات شاملة تعرض رؤية موحدة للنشاط الأمني عبر الشبكة: تطوير ميزات متقدمة لربط البيانات والأحداث من مصادر مختلفة مثل قواعد البيانات وحركة مرور الشبكة والتطبيقات الخارجية وغيرها، مما يسهل اتخاذ القرار.
4. تنفيذ نظام قادر على التعامل مع التهديدات الأمنية المتغيرة: تطوير آلية تسمح بتكامل البيانات وربطها بمصادر البيانات الخارجية وذكاء التهديدات باستخدام مجموعة متنوعة من طرق الكشف عن التهديدات مثل الكشف القائم على التوفيق والكشف القائم على السلوك وتقنيات **YARA** وقواعد **MITRE** وقواعد **Virus Total** والموقع الخارجية مثل وغيرها من التقنيات المتنوعة للكشف المبكر عن التهديدات الجديدة والمتقدمة.
5. تنفيذ حلول أمنية فعالة من حيث التكلفة والأداء للمؤسسات والشركات من جميع الأحجام: من خلال تطوير حلول مفتوحة المصدر أو منخفضة التكلفة تتناسب احتياجات المؤسسات الصغيرة.
6. تنفيذ وظائف الإخطار الآلي بالحوادث الأمنية للموظفين المعينين من خلال تكامل خدمات الطرف الثالث مثل رسائل البريد الإلكتروني والرسائل النصية ومنصات التواصل الاجتماعي وغيرها.

### نطاق المشروع والقيود والمخاطر

#### نطاق المشروع:

يهدف مشروع التخرج هذا إلى نشر وتطوير نظام المعلومات الأمنية وإدارة الأحداث والاستجابة لها باستخدام **Wazuh** في بيئه افتراضية. وسيركز المشروع على ما يلي:

1. تصميم وإعداد بيئه افتراضية باستخدام **VMWare Workstation Pro** لمحاكاة البيئه الواقعية.
2. نشر بيئه **Windows Server 2022**، **Active Directory**، **Ubuntu**، بما في ذلك أنظمة **Win10** و**Ubuntu**.
3. تكوين **Wazuh** ونشره على جهاز افتراضي مركزي.
4. إنشاء ودمج قواعد **Wazuh** المخصصة لتحسين المراقبة الأمنية والاستجابة للحوادث.

٥. إعداد قواعد YARA وتكوينها لتحسين الكشف عن التهديدات.

٦. تنفيذ جدار حماية PfSense مع Suricata IDS لمراقبة حركة مرور الشبكة.

٧. اختبار النظام باستخدام سيناريوهات محددة لمحاكاة عمليات الاختراق.

٨. تحليل نتائج الاختبار.

### حدود المشروع:

- التركيز على وظائف **Wazuh** الأساسية: سيعطي هذا المشروع الأولوية لتنفيذ الوظائف الأساسية التي توفرها **Wazuh** ، بما في ذلك التسجيل المركزي وتحليل السجل واكتشاف التهديدات وإدارة التنبؤات. يمكن النظر في القراءات المتقدمة مثل البحث الشامل عن التهديدات والطب الشرعي والاستجابة للحوادث من أجل التحسينات المستقبلية ولكنها لن تكون المحرر الأساسي لهذا التكرار الأولي.

محاكاة بيئة الأمان: نظراً لقيود الموارد، قد يتضمن المشروع إعداد بيئة أمان محاكاة باستخدام أجهزة افتراضية. في حين أن هذا النهج يسمح بالاختبار الفعال للوظائف الأساسية، إلا أنه قد لا يمثل بشكل كامل تعقيدات بيئة الإنتاج في العالم الحقيقي.

تكامل مصدر البيانات المستهدف: سيركز المشروع على التكامل مع مجموعة تمثيلية من مصادر البيانات الشائعة مثل أجهزة الشبكة وأنظمة التشغيل وتطبيقات الأمان. قد لا يكون التكامل مع كل مصدر بيانات محتملاً ممكناً ضمن الإطار الزمني للمشروع. ومع ذلك، سيأخذ تصميم النظام في الاعتبار قابلية التوسيع المستقبلية لعمليات تكامل إضافية.

### المخاطر

يمكن أن تؤثر العديد من المخاطر المحتملة على تنفيذ وتصميم المشروع ويمكن أن تعدل مسار المشروع. ولذلك، فإننا نعتبرها منذ البداية.

**قلة الخبرة في التقنيات المستخدمة:** تؤثر هذه المشكلة على وقت التطوير حيث سيتم تخصيص جزء كبير منه للتعلم. في هذا المشروع، جميع التقنيات المختارة جديدة بالنسبة لي، وبالتالي فهي عقبة كبيرة يجب أخذها بعين الاعتبار.

**استخدام التقنيات الجديدة:** وهذه العقبة مرتبطة بالنقطة السابقة. بعض التقنيات المختارة جديدة نسبياً على سبيل المثال **Wazuh** لذا فإن العثور على المعلومات قد يكون أكثر تعقيداً من المعتاد.

**تعقيد / نطاق المشروع:** بدأ هذا المشروع قبل يوم البدء الرسمي للأطروحة بسبب تعقيده الكبير. لذلك فأنا قد اضطررنا إلى ترك بعض أهداف المشروع وقمنا بإعادة هيكلة المشروع والبدء من جديد، مما أدى ذلك إلى ترك الهدف الرئيسي والجزء الأكثر أهمية وهو الذكاء الاصطناعي وذلك بسبب قلة الخبرة في التعامل مع الذكاء الاصطناعي وضيق الوقت وانعدام الموارد والبيئة المناسبة لنشر واختبار المشروع.

**بيانات غير كافية:** العديد من المقاييس التي يمكن الحصول عليها في نقطة النهاية، ومع ذلك، قد يكون العديد منها متغيراً جداً مما ينبع عنه الكثير من الإيجابيات الخاطئة.

**مشاكل وأخطاء التكوين والكتابة الأكاديمية:** عندما يتم تنفيذ أداة ما، فإن إحدى العقبات الأكثر استهلاكاً للوقت هي أخطاء الترميز، والتي قد يكون من الصعب جداً اكتشافها.

كل هذه المخاطر يمكن أن تؤثر على مدة المشروع، ومع ذلك، يتم المبالغة في تقدير المهام، ويتم استخدام الـ **Agile (1)** والتي تسمح بضبط التخطيط من خلال اجتماعات المتابعة الأسبوعية. ومع ذلك، إذا كانت هذه المخاطر ستتسبب في تأخير

خطير في المهام، فيمكن تخصيص المزيد من الساعات أسبوعياً لإنتهاء المشروع في الوقت المحدد. والا سوف نضطر الى الغائبة.

### منهجية المشروع

حالياً، هناك منهجيات عمل متعددة، لهذا المشروع، الخيار الذي يناسب هذا المشروع هو منهجية **Agile** وتحديداً (1) هذه المنهجية متكررة ومتزايدة. يتم تحديد سلسلة من المهام القصيرة تسمى (قصص المستخدم)، والتي يمكن أن تستمر ما بين 1 إلى 3 أسابيع ولها صعوبة محددة لها. كل سباق يضيف قيمة إلى النتيجة النهائية. تقسم هذه المنهجية الفريق إلى أدوار مختلفة، لكنني سأقوم بالأدوار الثلاثة.

توفر هذه المنهجية المرونة وتسهل التكيف الفعال مع التغييرات. في هذه الحالة، استمرت مدة سباقات السرعة لمدة أسبوع واحد. وهكذا تمكنا من رؤية كيف كان المشروع يسير.

### هيكل التقرير

يقدم الفصل الأول للقارئ القضايا والتحديات التي تواجهها الشركات الصغيرة والمتوسطة في سياق الأمن السيبراني متبرعة بنظرية عامة على الحل المقترن، تكنولوجيا **xdr** ويحدد الأهداف والغايات التي يسعى هذا البحث إلى تحقيقها.

الفصل الثاني هو الخطوط العريضة لجميع الأبحاث الموجودة حول تصميم وتنفيذ **SIEM** وقضايا الأمن في الشركات الصغيرة والمتوسطة على مر السنين. كما أنه يحل الحلول الأخرى التي قدمتها الأبحاث السابقة لتقدير نطاق استخدامها في المستقبل.

## الفصل الثاني: الخلفية ومراجعة الأدبيات

### خلفية المشروع

[https://varularora.medium.com/wazuh-security-information-and-event-\] Wazuh](https://varularora.medium.com/wazuh-security-information-and-event-] Wazuh) [management-siem-for-small-and-medium-sized-enterprises-b2cf1cc7ce0c]

المصدر لإدارة وتحليل الأمان السيبراني، تطورت لتكون من بين الأدوات الرئيسية التي تُستخدم لمراقبة الأنظمة، اكتشاف التهديدات، والاستجابة لها. فيما يلي خلفية عامة عن **Wazuh**

### ١. \*\*الأصل والتطور:\*

- \*\*التأسيس:\*\* بدأ **Wazuh** كمشروع مشتق من **OSSEC (Open Source Security)**, وهو نظام مفتوح المصدر للكشف عن التطفل (HIDS). مع مرور الوقت، تم تطوير **Wazuh** ليصبح منصة شاملة تتضمن ميزات متقدمة لإدارة الأمان السيبراني.
- \*\*التطور:\*\* توسيع المشروع ليشمل قدرات متقدمة مثل تحليل البيانات الأمنية، إدارة الامتثال، والتكامل مع تقنيات أخرى مثل **ELK Stack (Elasticsearch, Logstash, Kibana)**.

### ٢. \*\*الميزات الرئيسية:\*

- \*\*اكتشاف التطفل (IDS):\*\* يوفر **Wazuh** نظاماً لكشف التطفل يعتمد على الوكيل (agent-based) لمراقبة الأنظمة والتطبيقات بحثاً عن الأنشطة المشبوهة.
- \*\*تحليل السجلات:\*\* يجمع **Wazuh** السجلات من مصادر متعددة (أنظمة، تطبيقات، شبكات) ويحللها لاكتشاف الأنماط غير العادية التي قد تشير إلى تهديدات أمنية.
- \*\*إدارة الامتثال:\*\* يساعد المؤسسات على الامتثال للوائح والمعايير التنظيمية من خلال توفير تقارير مفصلة وتحليل الأمان لضمان الامتثال للمعايير مثل **PCI DSS**, **GDPR**, **HIPAA**.
- \*\*التكامل مع ELK Stack:\*\* يستخدم **Elasticsearch** لتخزين السجلات، **Logstash** لمعالجة البيانات، و **Kibana** لعرض البيانات بشكل مرئي وتقديم تقارير مخصصة.
- \*\*مراقبة الأمان في الوقت الفعلي:\*\* يتيح مراقبة الأمان بشكل مستمر في الوقت الفعلي، مما يساعد على اكتشاف التهديدات بسرعة والاستجابة لها.

### ٣. \*\*الاستخدامات الشائعة:\*

- \*\*الحماية من التهديدات:\*\* اكتشاف التهديدات مثل الهجمات الإلكترونية والبرامج الضارة وتحليل الأنشطة المشبوهة.
- \*\*الامتثال التنظيمي:\*\* تقديم تقارير تفصيلية ومراجعة السياسات الأمنية لضمان الامتثال للمعايير التنظيمية.
- \*\*إدارة الحوادث:\*\* تقديم أدوات للتحقيق في الحوادث الأمنية والاستجابة لها بشكل فعال.

### ٤. \*\*التقنيات والمكونات:\*

- \*\*وكلاء Wazuh:\*\* تثبت على الأنظمة المراقبة لجمع البيانات وإرسالها إلى خادم **Wazuh**.
- \*\*خادم Wazuh:\*\* يتولى معالجة وتحليل البيانات الواردة من الوكلاء، وتنسيق المعلومات الأمنية.

- \*\*لوحة التحكم (Dashboard):\*\* واجهة مستخدم تعتمد على **Kibana** لعرض البيانات بشكل مرئي وتقديم تقارير مخصصة، مما يسهل فهم البيانات الأمنية واتخاذ القرارات المناسبة.

### ٥. \*\*الفوائد:\*

- \*\*مرونة وقابلية التوسيع:\*\* يمكن تكييفه مع احتياجات المؤسسات الصغيرة والكبيرة، مما يجعله حلًا مرئيًّا وقابلًا للتطوير.

- \*\*مفتوح المصدر:\*\* كونه مفتوح المصدر يعني أنه يمكن تخصيصه وتعديلاته ليلائم المتطلبات المحددة لكل مؤسسة.

- \*\*مجتمع داعم:\*\* وجود مجتمع كبير من المستخدمين والمطوريين الذين يساهمون في تحسين وتطوير المنصة باستمرار، مما يضمن تحديثات مستمرة وتحسينات جديدة.

باختصار، **Wazuh** هو نظام قوي وشامل لإدارة الأمان السيبراني يوفر أدوات متقدمة لمراقبة الأنظمة، اكتشاف التهديدات، وإدارة الامتثال، مما يجعله خيارًا مثاليًا للمؤسسات التي تبحث عن حلول أمان موثوقة ومرنة.

## ١، مراجعة الأدبيات

نبدأ بسرد مفصل للعملية التي تم اتباعها أثناء اختيار البيانات والبحوث ذات الصلة لغرض هذا التقرير. تلتها إعادة تقييم الدراسات السائدة التي تدور بشكل أساسي حول قضايا أمن المعلومات، والسيناريو الحالي في الشركات الصغيرة والمتوسطة، وتصميم وتنفيذ أدوات **SIEM (Gartner Inc. 2012)** الخاصة بالشركات الصغيرة والمتوسطة. أخيراً، سيعطينا فهماً لمدى فائدته البحث لمزيد من التطوير.

تركز أنظمة مثل **Qradar** و **Splunk** و **ArcSight** على جمع الأحداث الأمنية من مصادر مختلفة وتحليلها لاكتشاف الحوادث الأمنية والاستجابة لها. أكملت الأبحاث في هذا المجال على تحسين التحليل في الوقت الفعلي، وارتباط الأحداث، وأدوات التتبيل.

منصتنا، وهو نظام أساسي مفتوح المصدر لمراقبة وتحليل الأمان، سبقته العديد من جهود البحث والتطوير في مجالات المعلومات الأمنية وإدارة الأحداث **(SIEM)**، وأنظمة كشف التسلل **(IDS)**، وإدارة السجلات.

البحوث السابقة :-

النظام	وظيفته
<b>SIEM Systems</b>	تتركز أنظمة مثل <b>Qradar</b> و <b>Splunk</b> و <b>ArcSight</b> على جمع الأحداث الأمنية من مصادر مختلفة وتحليلها لاكتشاف الحوادث الأمنية والاستجابة لها. أكدت الأحداث في هذا المجال على تحسين التحليل في الوقت الفعلي، وارتباط الأحداث، وآليات التنبية.
<b>Intrusion Detection Systems</b>	تم تطوير أدوات مثل <b>Suricata</b> و <b>Snort</b> لاكتشاف أنماط حركة مرور الشبكة المشبوهة. تضمن البحث هنا تعزيز خوارزميات الكشف، وتقليل النتائج الإيجابية الكاذبة، ودمج معلومات التهديد للحصول على دقة أفضل.
<b>Log Management</b>	تتركز حلول مثل <b>Logstash</b> و <b>Elasticsearch</b> و <b>Kibana</b> (ELK Stack) على التجميع المركزي لبيانات السجل وتخزينها وتحليلها. يهدف البحث إلى قابلية التوسيع والاستعلام الفعال وتصور كميات كبيرة من بيانات السجل.
<b>Open Source Security Tools</b>	كان <b>OSSEC</b> ، وهو نظام كشف التسلل القائم على المضيف (HIDS) مفتوح المصدر، بمثابة مقدمة مهمة لـ <b>Wazuh</b> . تضمنت جهود البحث والتطوير حول <b>OSSEC</b> تحسين تحليل السجل ومراقبة سلامة الملفات والتكامل مع الأنظمة الأساسية المختلفة.

برزت منصتنا باعتباره تطوراً وتكاملاً لهذه المجالات، حيث يوفر إمكانات مراقبة أمنية شاملة من خلال الجمع بين وظائف **SIEM** و **IDS** وإدارة السجل في منصة واحدة.

## ٢، منهجية مراجعة الأدبيات

تتبع مراجعة الأدبيات هذه إرشادات Okoli and Schabram (٢٠١٠)، والتي تقترح إجراء مراجعة الأدبيات الشامل والمنظم والتكراري من ٨ خطوات أكاديميا. بدأ السعي وراء الأدب بهدف واسع في الاعتبار: العثور على بعض المقالات أو الأوراق الأكاديمية المرتبطة بـ **SIEMs**. مكتبة جامعة لوليا والباحث العلمي من **Google** و**ProQuest** ليست سوى أمثلة قليلة على الموارد المفيدة.

بدأ البحث عن الأدبيات بهدف واسع في الاعتبار: العثور على بعض المقالات أو الأوراق الأكاديمية التي تعطي نظرة عامة على **SIEMs** كأداة وقضايا أمنية تواجهها المنظمات في جميع أنحاء العالم. تم استخدام الباحث العلمي من **Google** ومكتبة جامعة **Lulea** و**ProQuest** كموارد. ثم تم تضييق النطاق ليشمل أيضاً البحوث ذات الصلة بتصميم ونشر **SIEM** بمعنى مؤسسة صغيرة إلى متوسطة الحجم.

على الرغم من أن هذه الورقة تستشهد بمجموعة متنوعة من المصادر الثانوية والثالثية للأدبيات المتعلقة بأبحاث **SIEM**، إلا أن المصادر الأولية أو الحسابات المباشرة للبحوث، الواردة في مقالات المجالات العلمية التي تمت مراجعتها من قبل النظارء كانت مفضلة.

بعد العثور على المشاركات المناسبة، تم إجراء بحث عكسي للمراجع المشار إليها في المقالة، متبعاً بحثاً إلى الأمام في **Google Scholar** لتحديد المقالات أو الأوراق التي تشير إلى المقالة الأولية التي تم العثور عليها. تم الإبلاغ عن أوراق المجالات الأكاديمية لمزيد من الفحص. توقف البحث عندما أصبح من الواضح أنه لا يمكن التعرف بسهولة على أي أوراق جديدة، ونقدمت الدراسة إلى مستوى "الفحص من أجل الإدراج". بعد ذلك، تم تقييم كل منها على أساس الجودة وتطبيق النتائج العامة وطريقة البحث والصلة بالموضوع المحدد الذي يهمنا.

بعد ذلك، تمت إعادة النظر في الدراسات البحثية، وتم الانتهاء من نموذج تجميع البيانات لكل ورقة. جمع هذا القسم هدف البحث ومساهمته، ولماذا كان ذا صلة، والنتيجة، والسياق، وأي اقتراحات بحثية محتملة، وأي تعليقات مفيدة (بناء على الملاحظات أو النتائج المثيرة للاهتمام). تم تجميع المعلومات التي تم جمعها وتحليلها وكتابة التقرير التالي.

٣، ٢. البحوث المساعدة: الفهم والتحليل

عنوان البحث	المؤلفون	سنة النشر	الموضوع الرئيسي	ملاحظات
مشكلات أمن المعلومات للشركات الصغيرة والمتوسطة	جامعة ولاية سان دييغو وجامعة بليموث	٢٠٠٤	تحديات أمن المعلومات للشركات الصغيرة والمتوسطة	١٥٪ فقط من الشركات الصغيرة والمتوسطة خصصت ميزانية للأمن
خروقات الأمان السيبراني للشركات الصغيرة والمتوسطة	.Hau et al	٢٠١٦	تحديات أمن المعلومات للشركات الصغيرة والمتوسطة	الشركات لا تدرك أنها تعرضت للاختراق لعدة أشهر
تقرير FireEye عن الهجمات السيبرانية	FireEye [المصدر اسفل الصفحة]	٢٠١٦	تصميم وتنفيذ أداة SIEM	٧٧٪ من الجرائم السيبرانية موجهة إلى الشركات الصغيرة والمتوسطة الحجم
إطار عمل لتقدير وإدارة المخاطر	G. W. P. Chamiekara et al	٢٠١٧	نماذج مختلفة كحلول للتغلب على التحديات	تقييم المخاطر هو الخطوة الأولى لمواجهة مشاكل أمن المعلومات
حلول لإدارة الأمان للشركات الصغيرة والمتوسطة	متعدد غير محدد		نماذج مختلفة كحلول للتغلب على التحديات	معظم الدراسات اقترحت إطار التعامل مع القيود المالية للشركات الصغيرة والمتوسطة

<https://www.mandiant.com/company/press-releases/annual-fireeye-mandiant-m-trends-report-reveals-global-statistics-and-insights-hundreds-diverse-intrusions?hl=ar-001>

استنجدت دراسة أجرتها جامعة ريادة الأعمال والقانون في براغ وجامعة عموم أوروبا في سلوفاكيا علمياً أربعة عوامل حيوية لنجاح تدابير أمن المعلومات في أي مؤسسة:

- الضوابط الأمنية
- امتحان إدارة أمن المعلومات لأنشطة الشركة التجارية
- الوعي التنظيمي
- دعم الإدارة العليا

تظهر نتائج أبحاثهم أن الضوابط الأمنية، والتي تشمل ضوابط أمن المعلومات الإجرائية والتكنولوجية، وإدارة المخاطر هي أهم العوامل في نجاح إدارة أمن المعلومات. دعم الإدارة العليا هو ثاني أكثر العوامل حيوية. على المدى القصير، يعد الوعي التنظيمي هو العامل الأكثر وضوحاً وأهمية لإنجاز إدارة أمن المعلومات، كما يجب على الشركات الصغيرة والمتوسطة تعزيز الوعي التنظيمي في إدارة أمن المعلومات، إلى جانب تطبيق الضوابط الأمنية في خط الدفاع الأول، من أجل الدفاع عن المعلومات، والتي تعد أثمن أصول الشركة.

كان هناك بعض الاهتمام في الأدبيات الأكاديمية حول التعامل مع الحوادث في الشركات الصغيرة والمتوسطة. وعلى الرغم من هذه الخطوة إلى الأمام، لم تسفر البحوث الملموسة بعد عن إطار مقبول على نطاق واسع للاستجابة للحوادث الخاصة بالشركات الصغيرة والمتوسطة. أنتجت الحكومة والصناعة والأوساط الأكاديمية إطار وأدلة الاستجابة للحوادث. يحدد معظمها مراحل الاستجابة للحوادث على النحو التالي:

### ٢.٣.١. جدول مراحل الاستجابة لحوادث أمن المعلومات

الوصف	المرحلة	
قبل وقوع الحادث. (CSIRT) إنشاء فريق داخلي للاستجابة لحوادث أمن المعلومات ( )	الإعداد	المرحلة الأولى
اكتشاف الأحداث الأمنية أو الإبلاغ عنها، وعزل الأنظمة، وتحجيم كلمات المرور، وتطهير الحسابات.	التحقق	المرحلة الثانية
القضاء على مكونات الحادث، واكتشاف المضيفين المتأثرين، وإجراء تحليل البرامج الضارة والطبع الشرعي.	الاستئصال	المرحلة الثالثة
اختبار الأنظمة والفحص المستمر، واستخدام النسخ الاحتياطية لإعادة الأنظمة إلى الإنترنت.	الاسترداد	المرحلة الرابعة
عقد اجتماع ما بعد الحادث لمراجعة الإجراءات وتقييم فعاليتها، وإنشاء ضوابط وعمليات وسياسات جديدة.	المتابعة	المرحلة الخامسة

٢.٣.٢. عقد اجتماع ما بعد الحادث لمراجعة الإجراءات وتقييم فعاليتها، المتابعة بعد التفكير الدقيق، لوحظ أن الكثير من الأدبيات حول مجال الموضوع كانت خاصة بتصميم وتنفيذ SIEM. كانت هناك بعض الموضوعات المشتركة التي تم تحديدها من بين هذه والتي يتم شرحها أدناه:

الوصف	الموضوع	الموضوع ١
يناقش تصميم <b>SIEMs</b> في بيئات الأعمال الكبيرة مع بنية تحتية ضخمة للنظام.	تصميم وتطبيق <b>SIEMs</b> [Coppolino et al. (2011)]	الموضوع ١
يطبق تقنيات استخراج البيانات للكشف عن الأنماط المخفية لنشاط البرامج الضارة.	تطبيق تقنيات متميزة [Gabriel et al. ] (2009) Hadziosmanovic [et al. (2012)]	الموضوع ٢
تصميم <b>SIEMs</b> عبر الأنظمة غير المتجانسة   - يوصي بطرق قابلة للتطبيق لتنفيذ <b>SIEM</b> عبر الأنظمة غير المتجانسة.	تنفيذ <b>SIEMs</b> عبر الأنظمة غير المتجانسة [Kufel et al. ] Sohn ;(2013) et al. (2012)]	الموضوع ٣
تصميمات <b>SIEM</b> ذات الخصائص الجديدة   - يركز على تصميمات <b>SIEM</b> ذات الخصائص الجديدة، مثل الأتمتة لضوابط الأمان ذات الصلة ب <b>ISO 27000</b> . - يناقش تصميمات <b>SIEM</b> المتخصصة، مثل الطلب الشعري الرقمي أو سلسلة <b>NIST</b> لمعايير الأمان.	تصميمات <b>SIEM</b> ذات الخصائص الجديدة [Montesino et al. (2012) Metzger et al. (2011)]	الموضوع ٤

استخدمت هذه الدراسات السابقة أبحاث التصميم كتقنية بحث أساسية، مع التحقق من صحة التصميمات من خلال النماذج الأولية واختبار النظام التجاري. بصرف النظر عن تصميم **Metzger et al (٢٠١١)** الذي تم تطبيقه بشكل فعال في وضع العالم الحقيقي لمدة عام واحد، لم يتم تنفيذ التصميم المدرسوة في سياقاتها المختلط لها، ولم يتم توثيق أي تعلم من التنفيذ، مما قد يستلزم إعادة التصميم. توفر هذه تفاصيل قليلة حول المشاكل أو الخبرة المكتسبة من تنفيذ التصميم.

العديد من الأوراق لا تبني علم التصميم الخاص بها على أي نظرية للعلوم الطبيعية.

الآن هذا يجعل الأمر أكثر وضوحاً لماذا لم يكن البحث الموجود منذ كل هذه السنوات مجزياً في حل المشكلات التي تواجهها الشركات الصغيرة والمتوسطة. بالإضافة إلى ذلك، لا توجد دراسات تتناول على وجه التحديد تصميم **SIEM** في سياق الأعمال التجارية الصغيرة. قد تكون بعض مبادئ تصميم **SIEM** العامة السابقة مفيدة لمصمم **SIEM** في سياق الشركات الصغيرة والمتوسطة، ولكن يبدو أنه لا توجد دراسة في هذا المجال. ومع ذلك، كانت هناك دراسات حديثة تشير إلى تطوير وتصميم حلول مشابهة إلى حد ما لـ **SIEM** خصيصاً للشركات الصغيرة والمتوسطة والتي سيتم مناقشتها في القسم التالي.

الدراسة التي أجرتها الأستاذ الدكتور **O.-K. Rix, Prof. Dr. C. Klayner, T. Detken**. يقترح **SIEM** نموذجاً يعتمد على الهندسة المعمارية المشابهة بشكل ملحوظ لـ **SIEM** يسمى **SIMU**.

يمكن أن يكون هناك العديد من الأسباب التي تجعل **SIEM** غير مناسبة لبيئة الشركات الصغيرة والمتوسطة. بعض الأسباب هي كما يلي:

- تكون تكلفة تركيب **SIEM** أعلى بالنسبة للمؤسسة إذا كانوا يستخدمون **Qradar** و **Splunk** وما إلى ذلك. العملية الأكثر استهلاكاً للوقت هي تكوين نقاط النهاية.
- نظراً لأنه لا يمكن تشغيل **SIEM** من قبل أي شخص، وبالتالي، يلزم وجود خبير يتمتع بالخبرة الفنية المطلوبة لإنشاء القواعد واستكشاف الأخطاء وإصلاحها إذا واجهت **SIEM** أي مشكلة. يجب إنشاء لوحات معلومات متعددة لتحليل السجلات التي تم تحليلها من **SIEM**

ينصب تركيز مشاريع **SIMU** على إنشاء نظام مشابه جداً لـ **SIEM**، لكن **SIMU** ستعزز أمن المنظمة دون تعقيدات **SIEM**. توفر **SIMU** تكاماً أفضل وأسهل للبنية التحتية للمؤسسة، مما يؤدي إلى صيانة أسهل ورؤية السجلات في شبكة المؤسسة. العمل الأساسي لـ **SIMU** هو تماماً مثل أي **SIEM** آخر مما يعني أنه سيعالج جميع السجلات (Karlzen, H., ٢٠٠٩) ويقوم بالارتباط بها، ويكتشف جميع الأحداث من شبكة المنظمة. تماماً مثل **SIEM**، تتم معالجة جميع التدابير في الوقت الفعلي.

تدعي الدراسة أن هذا النموذج سيكون أكثر ملاءمة في سياق بيئة الشركات الصغيرة والمتوسطة، ولكن يمكن للمرء أن يجادل بأن هذا المشروع لا يزال قيد التطوير وفي مراحل التمويل الأولية وقد يستغرق الأمر سنوات للبناء عليه بنجاح وتوعية المنظمات بعملياته. ثانيا، تساعد البنية جزئيا فقط في مشكلة أمان الشركات الصغيرة والمتوسطة حيث لا يوجد دليل واضح يدعم أنها ستساعد في لوائح الامتثال التي تعد أحد الأسباب الرئيسية التي تجعل العديد من المؤسسات تختر تتنفيذ أداة الأمن وإدارة الأحداث.

بقدر ما يتعلق الأمر بالهدف الرئيسي لهذا التقرير، فمن الواضح جدا من مراجعة الأدبيات أعلاه أنه لا يكفي مجرد إيجاد حل وتقديمه نظريا أو إطار مراقبة الأعمال الذي سيساعد في التخفيف من المخاطر التي ينطوي عليها أمن تكنولوجيا المعلومات. تحتاج الشركات الصغيرة والمتوسطة إلى مزيد من الوعي حول هذه الأدوات المتوفرة لها مجانا، ودليل خطوة بخطوة حول كيفية تفيذها والأهم من ذلك كيفية الاستمرار في استخدامها في هذه البيئة الديناميكية. نأمل أن يتمكن هذا التقرير من تحقيق ذلك وتوفير نطاق وإلهام لمزيد من البحث.

## الفصل الثالث: جمع وتحليل المتطلبات

### ١، ٣ مقدمة:

يوضح هذا الفصل تحليل المتطلبات والنماذج لمشروع الكشف والاستجابة الموسعة (XDR) القائم على [Wazuh](#)، يهدف المشروع إلى توفير مراقبة أمنية شاملة واكتشاف التهديدات وقدرات الاستجابة للحوادث للمؤسسات من جميع الأحجام.

### ٢، ٣ نطاق

يركز هذا الفصل على الوظائف الأساسية للمشروع، بما في ذلك جمع البيانات، واكتشاف التهديدات، وتحديد أولويات التهديدات، والاستجابة الآلية للتهديدات، والتكامل مع البنية التحتية الأمنية الحالية، وإعداد التقارير سهلة الاستخدام.

#### ٣.١.١ مواصفات المشروع

يوفّر المشروع مجموعة شاملة من الميزات، بما في ذلك:

- جمع البيانات: يجمع البيانات من مجموعة واسعة من المصادر لتوفير رؤية شاملة للوضع الأمني للمؤسسة.
- اكتشاف التهديدات: يستخدم تقنيات الكشف المتقدمة لتحديد التهديدات المعروفة وغير المعروفة، بما في ذلك الكشف المستند إلى التوقيع واكتشاف الحالات الشاذة والتحليل السلوكي.
- تحديد أولويات التهديدات: يعطي الأولوية للتهديدات المكتشفة بناء على شدتها وتأثيرها المحتمل، مما يمكن مسؤولي الأمان من التركيز على المشكلات الأكثر أهمية.
- الاستجابة التقائية للتهديدات: أتمّة الاستجابات للتهديدات المكتشفة، بما في ذلك عزل نقاط النهاية المصابة، وحظر حركة المرور الضارة، وإنهاء الاتصالات المشبوهة.
- التكامل مع البنية التحتية الأمنية الحالية: يتكامل بسلاسة مع البنية التحتية الأمنية الحالية، بما في ذلك جدران الحماية وأنظمة [IPS](#) [10] وأنظمة الأمانة الخارجية
- واجهة سهلة الاستخدام وإعداد التقارير: يوفر واجهة سهلة الاستخدام لمسؤولي الأمان للوصول إلى الاكتشافات والتصورات والجداول الزمنية والتقارير.

### ٣.٣ المتطلبات الوظيفية

#### ٣.١.١ جمع البيانات

يجب أن يكون المشروع قادر على جمع البيانات من مجموعة واسعة من المصادر، بما في ذلك:

- نقاط النهاية:
  - أنظمة التشغيل: السجلات من **Windows** و **Linux** وأنظمة التشغيل الأخرى.
  - التطبيقات: السجلات من التطبيقات وقواعد البيانات.
  - نشاط النظام: السجلات من أحداث النظام والعمليات واتصالات الشبكة.
- الشبكات:
  - حركة مرور الشبكة: بيانات التقاط الحزم ومراقبة حركة مرور الشبكة.
  - أجهزة الشبكة: السجلات من جدران الحماية وأنظمة **IDS/IPS** [11] وأجهزة أمان الشبكة الأخرى.
- سلوك المستخدم:
  - سجلات نشاط المستخدم: عمليات تسجيل الدخول وتسجيل الخروج والوصول إلى الملفات وإجراءات المستخدم الأخرى.
  - بيانات حماية نقطة النهاية: مقاييس أداء النظام وحالة وكيل الأمان ونتائج فحص الثغرات الأمنية.

#### ٣.١.٢ الكشف عن التهديدات

يجب أن يستخدم المشروع تكتيكات الكشف المتقدمة لتحديد التهديدات المعروفة وغير المعروفة، بما في ذلك:

- الكشف المستند إلى التوقيع:

يحدد التهديدات استنادا إلى التوقيعات أو الأنماط المعروفة في حركة مرور الشبكة وسجلات النظام وسمات الملفات.
- كشف الشذوذ:

يراقب الانحرافات عن السلوك الأساسي المعمول به، ويعرف على الأنشطة غير الطبيعية التي قد تشير إلى انتهاكات أمنية محتملة.
- التحليل السلوكي:

يحلل سلوك البيانات داخل الشبكة، ويبحث عن الأنماط أو الإجراءات التي تتحرف عن القاعدة.

### ٣.١.٣ تحديد أولويات التهديدات

يجب أن تعطي منصة XDR الأولوية للتهديدات المكتشفة بناء على شدتها وتأثيرها المحتمل. وهذا يشمل:

- تقييم المخاطر: تعين درجة مخاطر لكل تهديد تم تحديده، مع الأخذ في الاعتبار شدته وتأثيره المحتمل على المنظمة وصلته بالسياسات الأمنية الحالية.
- التحليل السياقي: توفير سياق حول التهديدات المكتشفة من خلال ربطها بأصول المؤسسة ونقاط الضعف المحتملة والبيانات التاريخية.
- التصنيف الآلي: تصنيف التهديدات إلى مستويات مختلفة (على سبيل المثال ، عالية ومتوسطة وانخفاض) بناء على درجة المخاطر الخاصة بها لتمكين تحديد أولويات الاستجابة بكفاءة.

### ٤.١.٣ متطلبات الاستجابة الآلية للتهديدات

- عزل نقاط النهاية المصابة: عزل نقاط النهاية المختلفة تلقائيا عن الشبكة لمنع الحركة الجانبية للتهديدات.
- حظر حركة المرور الضارة: اتخاذ إجراءات لحظر حركة المرور الواردة أو الصادرة المرتبطة بالتهديدات المحددة.
- إنهاء الاتصالات المشبوهة: قطع الاتصالات أو المعاملات المشبوهة تلقائيا بسبب التهديدات المحتملة.

### ٤.١.٥ التكامل مع أدوات الامن

- جدران الحماية
- أنظمة كشف ومنع التسلل **IPS/IDS**
- **YARA**

**Virus Total**

**Suricata**

### ٣.١.٦ واجهة سهلة الاستخدام ومتطلبات إعداد التقارير

يجب أن يوفر المشروع واجهة سهلة الاستخدام لمسؤولي ومحلي الأمن، بما في ذلك:

- التصور ولوحة القيادة:
  - عرض الاكتشافات الأمنية والحوادث والاتجاهات والبيانات الأساسية الأخرى من خلال التمثيلات الرسومية ولوحات المعلومات البديهية.
- التقارير في الوقت المناسب:
  - إنشاء تقارير مفصلة وموحدة عن الأحداث الأمنية واتجاهات التهديدات ونقاط الضعف لاتخاذ قرارات فعالة.
- تتيهات قابلة للتخصيص:
  - السماح للمستخدمين بتعيين تتيهات مخصصة بناء على معايير أمان محددة أو حوادث ذات أهمية.

## الفصل الرابع: تصميم ونماذج المشروع

### ٤،١. مقدمة

في هذا الفصل سيتم توضيح التخطيط الذي سيتم الاعتماد عليه في تنفيذ المشروع وتوضيح التقنيات التي بناءً عليها سيتم اختبار المشروع.

### ٤،٢. تخطيط وتصميم المشروع

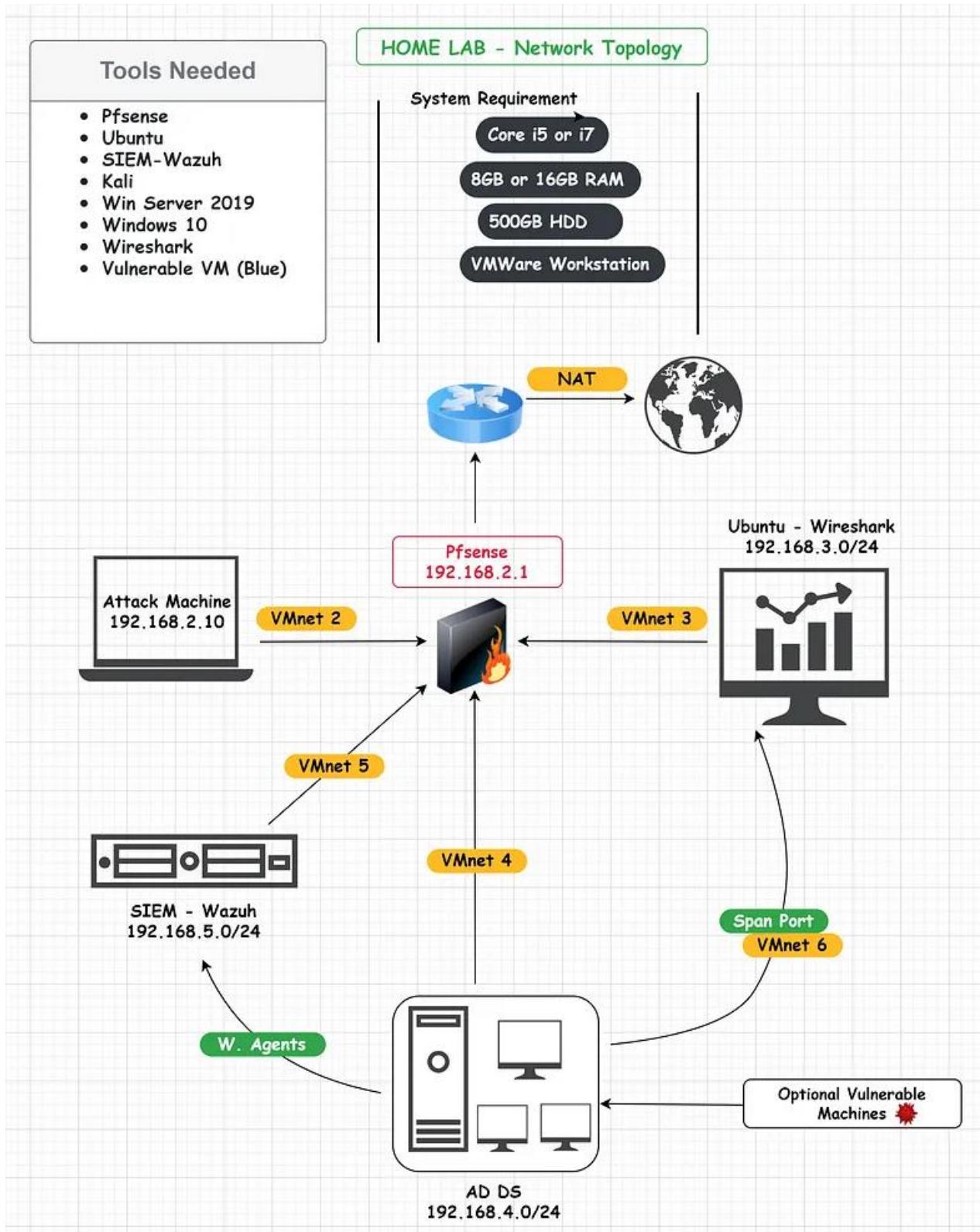
#### ٤،٢،١ طبولوجيا الشبكة

يعد اختيار هيكل الشبكة المناسب أمراً بالغ الأهمية لأنه يحدد كيفية تدفق البيانات وكيفية تواصل الأجهزة. تؤثر الهيكلية على كفاءة المختبر وقابلية التوسيع والمرونة، وتلعب دوراً رئيسياً في إنشاء بيئة واقعية للاختبار والتعلم ومحاكاة سيناريوهات الشبكة المختلفة.

تشير طبولوجيا الشبكة إلى ترتيب أو تخطيط الأجهزة والاتصالات في شبكة الكمبيوتر. ولأغراض معملنا، سيوضح كيفية ترابط العناصر المختلفة، مثل أجهزة الكمبيوتر والخوادم وأجهزة التوجيه والأجهزة الأخرى.

في هذا الباب ان شاء الله سنقوم بتطبيق إطار العمل المقترن باستخدام برنامج **VMware Workstation Pro** باستخدام مجموعة من الأجهزة الافتراضية **Virtual machines** واستخدام **PfSense firewall** ونظام **SIEM**- **Wazuh** واستخدام أداة **Wireshark** ونظام **Windows 10** و **Ubuntu Linux**

## Extended Detection and Response



شكل رقم ( )

### ٤،٢،٢. شرح طوبولوجيا الشبكة:

- **VMware Workstation Pro**: سيتم استخدامه لاستضافة الأجهزة والأنظمة الوهمية ولعمل محاكاة لبيئة عمل واقعية.
- **firewall pfSense**: سيكون جدار الحماية هذا بمثابة حاجز بين قطاعات الشبكة المختلفة داخل الميكل، حيث يتحكم ويراقب حركة المرور الواردة والصادرة ، وتم اختياره بسبب مرونته واستقراره وسهولة التعامل معه ويراقب الحزم والحركة الداخلية والخارجية من الشبكة ويعتبر مفتوح المصدر (مجاني) ، ويعتبر هو حل متعدد الاستخدامات وغني بالمميزات للأفراد والمؤسسات الذين يبحثون عن جدار حماية قوي وقابل للخصيص ، الهدف منه هو تعزيز الأمان عن طريق منع الوصول غير المصرح به وعزل مكونات الشبكة.
- **SIEM-Wazuh**: سيقوم SIEM الخاص بنا هنا بجمع وتحليل بيانات السجل من أنظمة مختلفة عبر الشبكة. وفي مشروعنا، سيساعد في المراقبة في الوقت الفعلي، واكتشاف التهديدات، والاستجابة للحوادث، مما يساهم في اتخاذ موقف أمني استباقي للقليل من الضرر.
- **Wireshark**: محل بروتوكول الشبكة الذي يلقط ويفحص البيانات التي تنتقل ذهاباً وإياباً على الشبكة في الوقت الفعلي. إنه مفيد في فهم سلوك الشبكة وتشخيص المشكلات وتحديد التهديدات والأمنية المحتملة من خلال تحليل الحزم.
- **Active Directory Domain Services (AD DS)**: توفر AD DS آلية مصادقة وتفوض مرکزية. فهو يبسط إدارة الشبكة من خلال تنظيم وإدارة موارد المستخدم ويوفر خدمات ووظائف متنوعة داخل شبكة المؤسسة.
- **OS Kali Linux**: آلة الهجوم سيكون هذا هو نظامنا المخصص لمحاكاة الهجمات الإلكترونية المختلفة. ستتوفر منصة عملية لفهم التكتيكات الهجومية كيفية الدفاع عنها، وبالتالي تعزيز اكتشاف الهجمات التي تحدث في مجال الأمن السيبراني.
- **منفذ SPAN**: تم تكوينه لتكرار حركة المرور من المنفذ الأخرى إلى منفذ واحد محدد. في مختبرنا، سيتم تحسين رؤية الشبكة من خلال السماح لـ Wireshark بالتقاط نسخة من جميع حزم الشبكة لتحليلها. ويساعد ذلك في مراقبة واكتشاف الأنشطة غير العادية أو الضارة على الشبكة.

### ٤،٢،٣. توضيح لما سيتم استخدامه من أجهزة وأنظمة وأدوات وتقنيات:

#### ٤،٢،٣،١. الأجهزة المستخدمة:

Hardware		
الموارد	كمية	المواصفات
جهاز لابتوب	1	CORE-i9, RAM: 32 DDR4, HARD: 1TB SSD,
جهاز لابتوب	1	CORE-i7, RAM: 16 DDR4, HARD: 1TB SSD,

## Extended Detection and Response

٤.٢.٣.٢. أنظمة التشغيل المستخدمة:

OS		
كمية	إصدار	اسم SF
1	22.04.1	Ubuntu
1	2022.4-Installer amd64	Kali Linux
1	2022	Windows Server
1	23H2	Windows 11
2	22H2	Windows 10

٤.٢.٣.٣. جدار الحماية وأنظمة الامن:

أنظمة الامن	
إصدار	اسم
2.7.2	Pfsense firewall
6.0.19	Suricata

٤.٢.٣.٤. التقنيات والأدوات والبرامج المستخدمة:

التقنيات والأدوات	
إصدار	اسم
17.5.1	VMware Workstation
4.7.2	Wazuh
4.4.0	YARA

## Extended Detection and Response

	Windows Defender logs
Website	VirusTotal
4.2.5	Wireshark
Website	monday.com
Website	<b>Trello</b>
	Google meet
95 or later	Chrome
93 or later	Firefox
	draw io

### ٤.٢,٣,٤. لغات البرمجة المستخدمة:

اللغات المستخدمة	
إصدار	اسم
3.12.2	python
	<b>Bash Scripting</b>

### ٣.٤. التقنيات المستخدمة في المشروع

#### ١,٣,٤. أولاً المكونات الأساسية في النظام **Wazuh**

كما نعلم يعمل **Wazuh** بثلاثة مكونات رئيسية مركزية: **الخادم**، **المفهرس**، **لوحة المعلومات**، **والوكيل**

#### ١,٣,٤. **Wazuh indexer**

المفهرس مسؤول عن فهرسة وتخزين التنبیهات الصادرة من خادم **Wazuh**. يمكن تهيئتها كمجموعة أحادية العقد أو متعددة العقد. ثم يتم تخزين البيانات في **JSON**.

## Extended Detection and Response

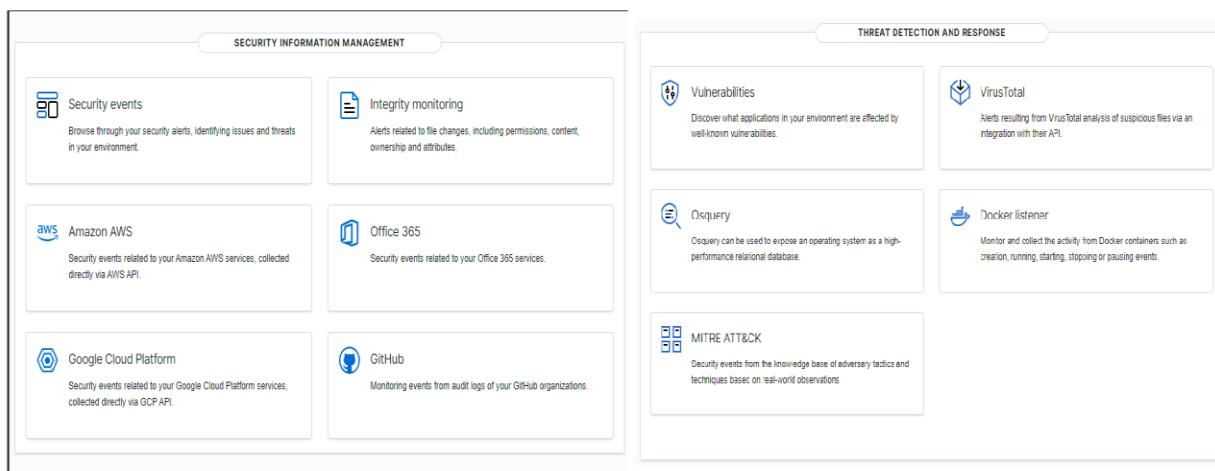
يمكن بدء التفاعل مع المفهرس باستخدام **REST API** الخاص به. تشمل المهام البحث عن المستندات أو إضافتها أو حذفها وتعديل الفهارس والمزيد.

### ٤،٣،١،٢ خادم wazuh

تم تحسين قدرات الكشف الخاصة به من خلال استخدام مصادر استخبارات التهديدات **threat intelligence sources**. يتم أيضًا استخدام إطار عمل **MITRE ATT&CK** ومتطلبات الامتثال التنظيمي مثل **NIST 800-53** و **CIS** و **HIPAA** و **GDPR** و **PCI DSS** لتحسين بيانات التنبية الخاصة بها.

### ٤،٣،١،٣ Wazuh dashboard

يتم تصور البيانات وتحليلها في لوحة المعلومات باستخدام واجهة مستخدم الويب. وهي تشمل لوحات معلومات للأحداث الأمنية، والامتثال التنظيمي، والتطبيقات الضعيفة المكتشفة، وبيانات مراقبة سلامة الملفات، من بين أمور أخرى. تتم أيضًا إدارة تكوين **Wazuh** ومراقبة حالته في لوحة المعلومات.



#### الشكل رقم ()

##### • تصور البيانات وتحليلها

تساعد واجهة الويب المستخدمين على التنقل عبر الأنواع المختلفة من البيانات التي يجمعها وكيل **Wazuh**، بالإضافة إلى التنبية للأمنية التي يولدها خادم **Wazuh**. توفر لوحة المعلومات أيضًا القدرة على إنشاء التقارير وإنشاء تصورات ولوحات معلومات مخصصة.

##### • مراقبة الوكالء وتكتوينهم

تسمح لوحة المعلومات هذه بإدارة تكوين الوكالء ومراقبة الحالة.

# Extended Detection and Response

## ٤،٣،١،٤ Wazuh agents

لكي يتمكن **Wazuh** من أداء قدراته القوية، يتم نشر الوكلاء على نقاط النهاية. تتضمن نقاط النهاية أجهزة الكمبيوتر المحمولة أو أجهزة الكمبيوتر المكتبية أو الخوادم أو **cloud instances** أو الأجهزة الافتراضية. يمكن لل وكلاء العمل على **Linux** ، **Windows** ، **macOS** ، **Solaris** ، **AIX** ، وأنظمة التشغيل الأخرى. تتم حماية هذه الأنظمة بواسطة **agents**، مما يوفر إمكانات منع التهديدات واكتشافها والاستجابة لها.

## ٤،٣،٢ ثانياً التقنيات المستخدمة في النظام

### ٤،٣،٢،١ File integrity monitoring (FIM):

تقوم هذه الوحدة بمراقبة نظام الملفات، والإبلاغ عند إنشاء الملفات أو حذفها أو تعديلها. فهو يتتبع التغييرات في سمات الملف والأذونات والملكية والمحظى. عند وقوع حدث ما، فإنه يلقط تفاصيل من وماذا ومتى في الوقت الفعلي. بالإضافة إلى ذلك، تقوم وحدة **FIM** ببناء قاعدة بيانات وحفظها على معاشرة الملفات المراقبة، مما يسمح بتشغيل الاستعلامات عن بعد.

لا يستطيع **FIM** وحدة اكتشاف وجود برامج ضارة في النظام. ولهذا السبب، يجب دمج **FIM** مع قواعد الكشف عن التهديدات، مثل **YARA** ، ومصادر معلومات التهديدات **threat intelligence** ، **sources**، مثل قائمة **CDB** و **VirusTotal** لتجزئة الملفات الضارة، لاكتشاف الملفات الضارة والأنماط غير الطبيعية التي تظهر وجود برامج ضارة.

### ٤،٣،٢،٢ الكشف عن سلوك الجذور الخفية

تُستخدم هذه الوحدة للكشف عن وجود برامج ضارة عن طريق فحص نقطة النهاية كل ١٢ ساعة، والتي يمكن تهيئتها وفقاً لحاجة البيئة. بعد تثبيت الوكيل في نقطة النهاية، ستقوم وحدة **Rootkit** بفحص الدليل **/dev** ومراقبة المسارات والأدلة وإدخالات التسجيل والنظام المحدد بحثاً عن سلوك غير الطبيعي باستخدام قاعدة بيانات توقيعات **rootkit** الجاهزة، والتي يمكن أيضاً تعديلاً حسب التردد المطلوب. سيتم

إرسال السجلات إلى المدير لفك التشفير المسبق وتحليل فك التشفير ، وستطابق السجلات مع القواعد المحددة مسبقاً.

### VirusTotal integration ٤,٣,٢,٣

بمجرد دمجه مع **VirusTotal** ، يستطيع **Wazuh** اكتشاف الملفات الضارة. يتم تشغيل التنبئات عندما يكتشف **FIM** أي تغيرات في المجلدات المراقبة، مما يؤدي بعد ذلك إلى قيام تكامل **VirusTotal** باستخراج قيمة التجزئة للملف. تتم بعد ذلك مقارنة التجزئة بقاعدة بيانات **VirusTotal** باستخدام واجهة برمجة تطبيقات **VirusTotal**. يتم بعد ذلك تلقي استجابة قد تؤدي إلى تنبئه قد يحتوي على خطأ أو إشارة إلى وجود ملف ضار.

### YARA ٤,٣,٢,٤

أداة لتحديد البرامج الضارة والملفات الضارة عن طريق مطابقة الأنماط والقواعد. عند دمجها مع **FIM** ، الملفات التي تسبب التنبئات ستبدأ **YARA** [12] في إجراء عملية فحص لهذه الملفات واختبارها وفقاً لقواعدها لتحديد ما إذا كانت برمج ضارة أم لا. سيتم إرسال نتائج المسح إلى المدير لفك التشفير والتحليل والتنبئه. و يجب إضافة وحدات فك التشفير إلى الخادم حتى يمكن فك تشفير عمليات الفحص هذه.

### Windows Defender logs collection ٤,٣,٢,٥

سيتم تكوين الوكاء على نقاط نهاية **Windows** لتجميع من سجلات **Windows Defender** تحتوي على حالة الخدمة ونتائج المسح على نقاط النهاية.

### ٤,٣,٢,٦ استجابة نشطة

تساعد هذه القدرة المستجيبين للحوادث على معالجة الأحداث عالية الخطورة بكفاءة من خلال إطلاق استجابات تلقائية بناءً على مشغلات محددة.

يحتوي **Wazuh** على نصوص برمجية افتراضية للاستجابة النشطة لأنواع مختلفة من نقاط النهاية التي قد تؤدي إلى إجراء محدد بناءً على إعدادات التكوين. قد يقوم بتعطيل حساب مستخدم، أو يضيف عنوان **IP** إلى قائمة رفض **iptables** ، أو يضيف عنوان **IP** إلى القائمة المنسللة لجدار الحماية، أو يعيد تشغيل وكيل أو مدير **Wazuh**. هذه ليست سوى عدد قليل من الاستجابات النشطة المضمنة في البرنامج النصي **Wazuh** الافتراضي لـ **Wazuh**.

يمكن أيضاً إنشاء برنامج نصي مخصص للاستجابة النشطة يتم تنفيذه عند تشغيل تنبئه لمعرف قاعدة محدد أو مجموعة قواعد معينة. يمكن استخدام أي لغة برمجة لإنشاء برنامج نصي مخصص.

### Suricata ٤,٣,٢,٧

هو نظام كشف عن التطفلات (IDS) مفتوح المصدر وفعال للغاية تم تصميمه للكشف عن الهجمات الشبكية المعقدة. يمكن استخدام **Suricata** جنباً إلى جنب مع **Wazuh** ، وهو نظام كشف عن التهديدات على المضييف (HIDS) مفتوح المصدر، لتحسين أمان الشبكة والبنية التحتية،

جمع البيانات: إرسال التنبئات: يجمع **Suricata** حزم الشبكة ويحللها للكشف عن أي نشاط ضار، إذا اكتشف **Suricata** أي نشاط ضار، فإنه يرسل تنبئها إلى **Wazuh**.

٤,٣,٤ نيات المستخدمة في النظام

٤,٣,٣,١ Python

في هذا المشروع، يتم استخدام **Python** لجمع السجلات بتنسيق **JSON** باستخدام واجهة برمجة **API** التطبيقات

**psutil**: سكريبت بايثون يجمع معلومات الشبكة خلال فترة زمنية معينة باستخدام مكتبة **network.py** يتم إلهاق البيانات بتنسيق **Json** في الملف **"json.network"**.

٤,٣,٣,٢ **PowerShell**:

تم استخدامه لكتابة نصوص لتنفيذ الهجمات المحاكاة واكتشاف الثغرات.

## الفصل الخامس: تنفيذ واختبار المشروع

### ١. مقدمة

في هذا الفصل سنقوم بعمليه التكوين للمشروع من ناحية تثبيت البيئة وتكونها وتنصيب نظام **Wazuh** والأنظمة الأخرى، ثم نبدأ بعمليه الاختبار.

### ٢. خطوات الأساسية في تكوين عمل المشروع

#### ١.٢.٥. يتم تثبيت VMware Workstation Pro

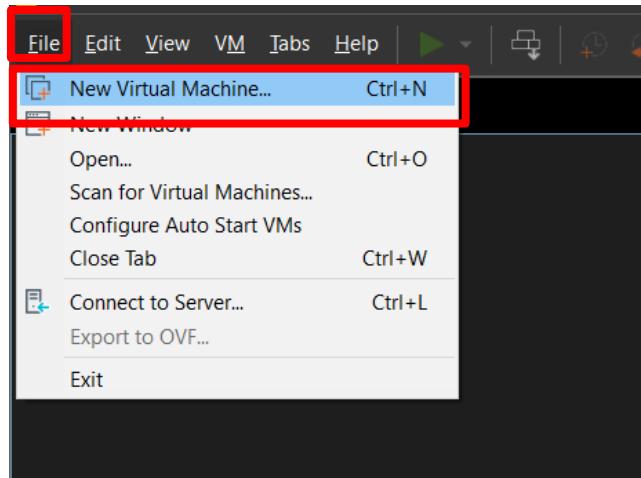
حيث سيتم استخدامه لعمل بيئة وهمية والاستضافة وتشغيل الأنظمة والأدوات التي سنحتاجها في المشروع



#### ٢.٢.٥. تثبيت جدار الحماية في VMware pfsense

نقوم بتنشيف **VMware** ثم انشاء جهاز افتراضي جديد من تبويب **file**

## Extended Detection and Response



شكل رقم (١)

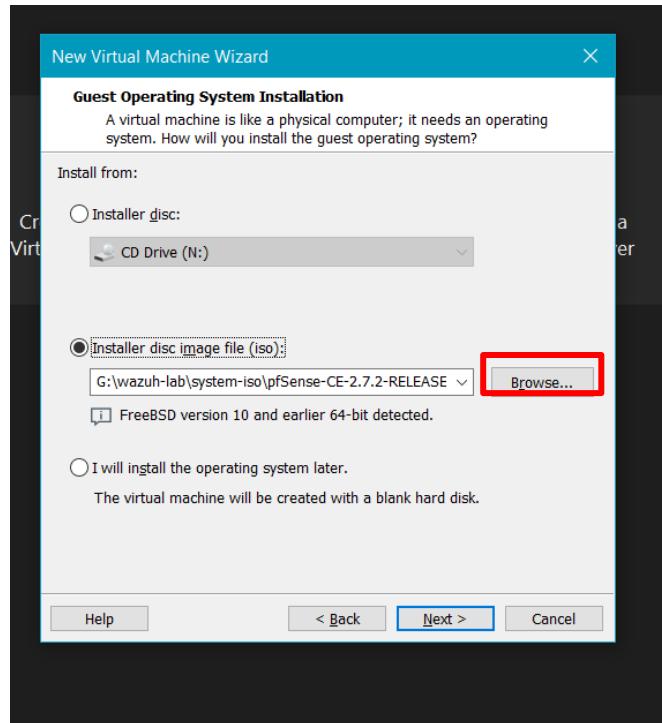
تحديد الاعدادات الافتراضية عن طريق النموذج *typical*



شكل رقم (٢)

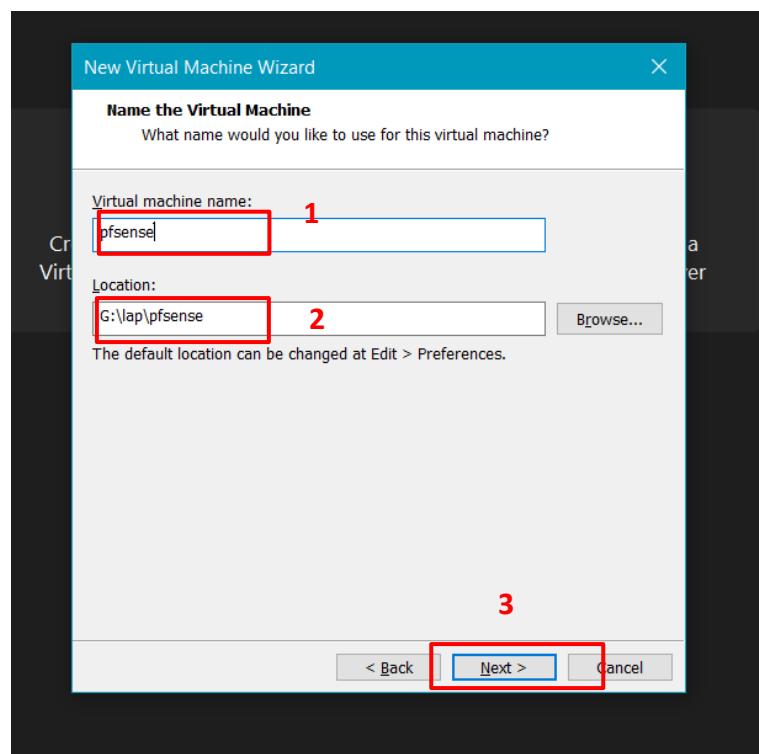
حدد **pfSense iso image** وانقل إلى المجلد المحفوظ في داخلة **Browser**

## Extended Detection and Response



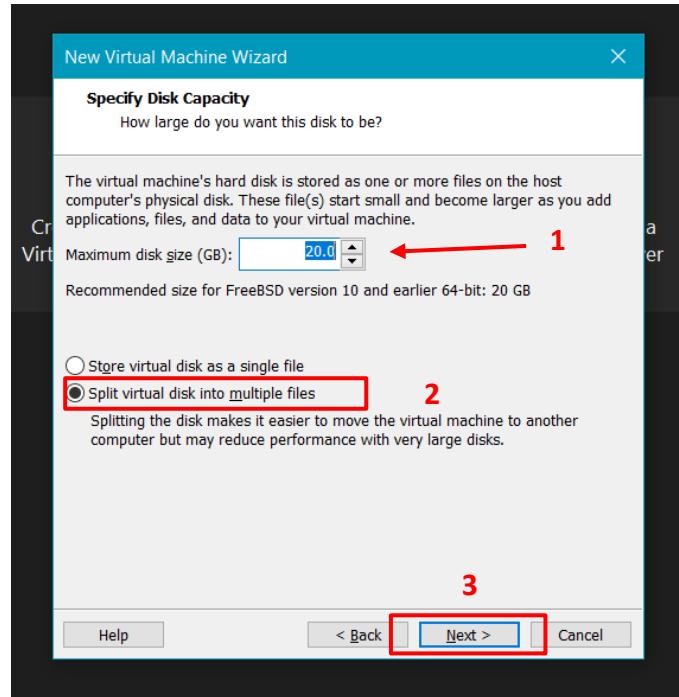
شكل رقم (١)

يوجد هنا خيار لإعادة تسمية جهازك الافتراضي والموقع الذي سيتم حفظ صورة الجهاز الافتراضي فيه على جهازك المضيف. قم بتغيير اسم VM إلى **pfSense** وانقر فوق "التالي".



### شكل رقم ()

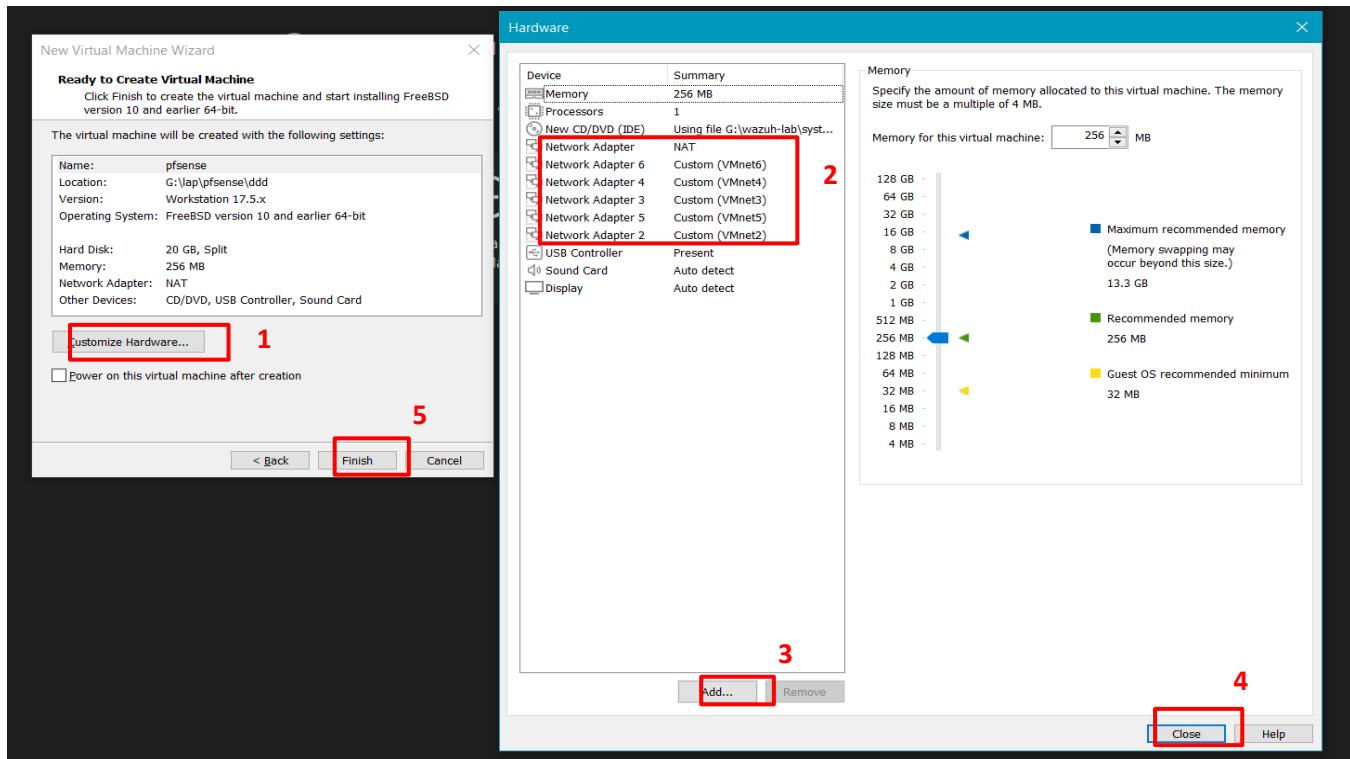
حدد سعة القرص لجهاز **VM** بشكل افتراضي، يكون ٢٠ جيجابايت وهو أمر جيد وانقر فوق "التالي".



### شكل رقم ()

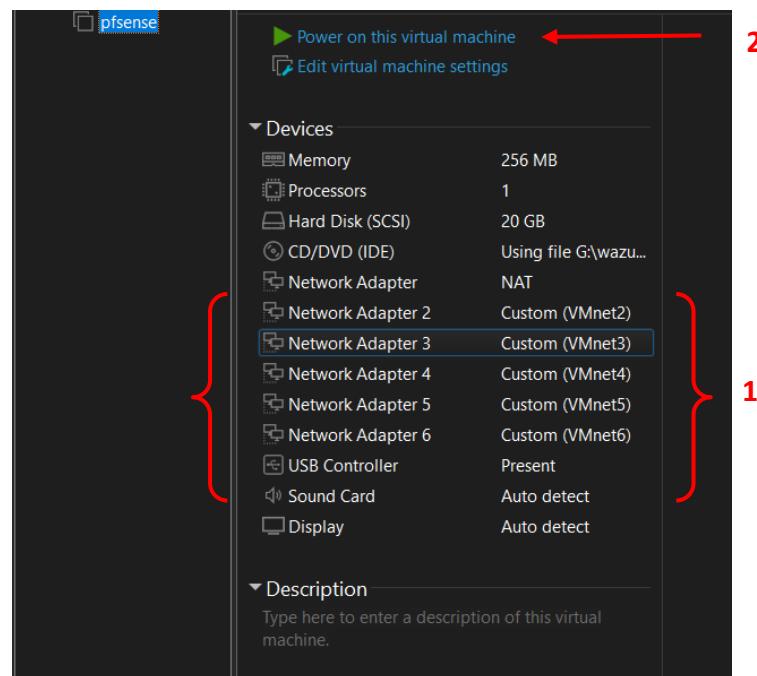
حدد تخصيص الأجهزة **customize hardware** لإجراء تغييرات على الأجهزة. سنضيف خمسة محولات شبكة أخرى كما هو موضح في الهيكل الخاص بنا، وهذا سيساعدنا على تقسيم شبكتنا لحركة مرور مختلفة.

## Extended Detection and Response



شكل رقم ٦

حاليا بعد التثبيت عند ظهور واجهة VMware بهذا الشكل ، نقوم بتأكد من أن كل محول شبكة يتطابق مع شبكة VMnet المقابلة له ، ثم نقوم بالنقر فوق زر الطاقة لتشغيل جهاز VM الخاص ب pfSense



شكل رقم ٧

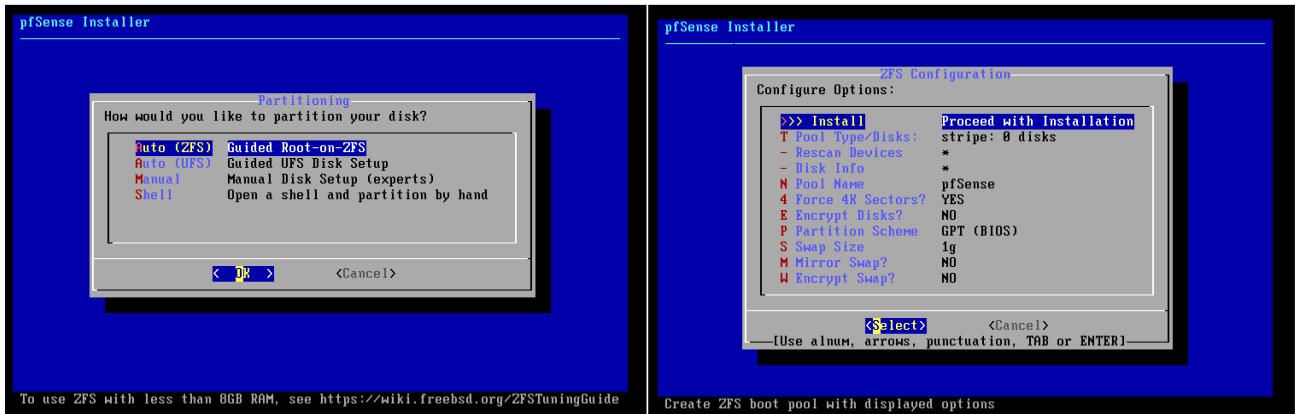
## Extended Detection and Response

والآن تبدأ عملية التثبيت. اضغط على **Enter** لقبول **install**. حدد **Accept** واضغط على **Enter**. حدد **Install pfSense**



شكل رقم ()

لن نقوم بتقسيم **HDD** الخاص بنا. حدد **Auto** واضغط على **Enter**. حدد **Install** واضغط على **Enter**.



شكل رقم ()

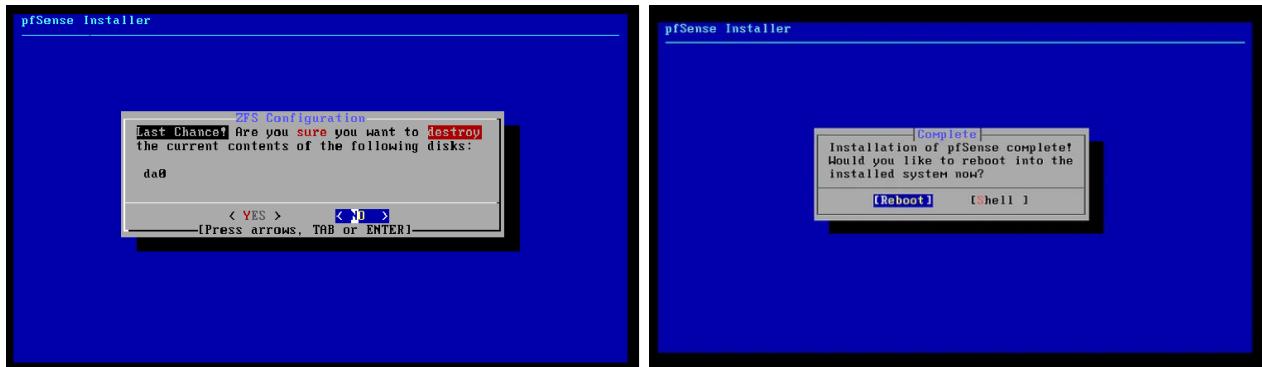
حدد **stripe** واضغط على **Enter** لإضافته قيمه وحدد **ok**.

## Extended Detection and Response



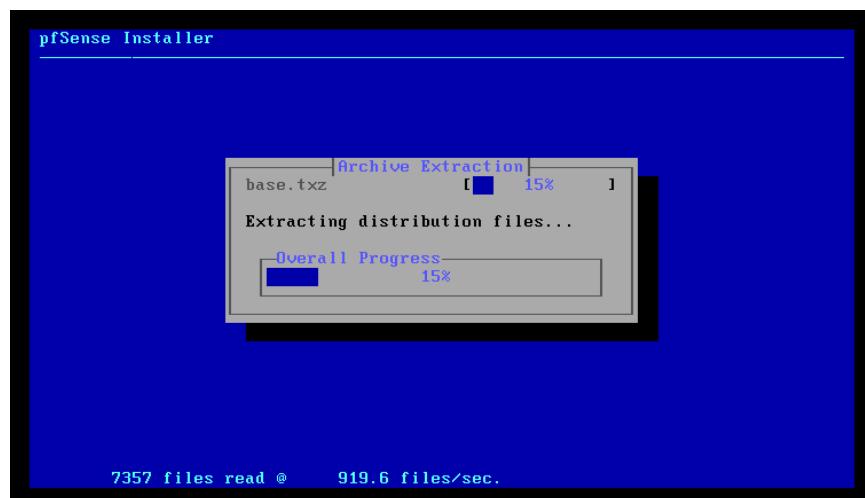
شكل رقم ()

حدد **YES** واضغط على **Enter**. لتنصيب PfSense. حدد إعادة التشغيل واضغط على **Enter**.



شكل رقم ()

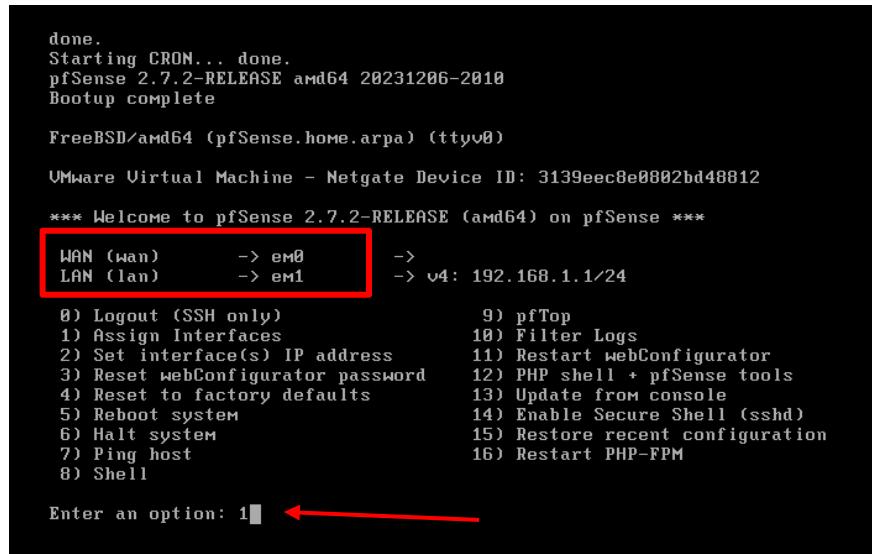
حاليا يقوم بعمليه التنصيب



شكل رقم ()

## Extended Detection and Response

بمجرد تثبيت pfSense بنجاح، سنلاحظ في البداية وجود واجهتين: WAN و LAN تتصل واجهة WAN بمحلول شبكة NAT الخاص بنا، مما يسمح بالوصول إلى الإنترنت. تد واجهة LAN إحدى واجهات الشبكة الأخرى، ولكن قد نرى واحدة فقط في البداية. لتنشيط كافة الواجهات الأخرى على pfSense ، اختر الخيار 1 — تعين الواجهات.



```
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 3139eec8e0802bd48812

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

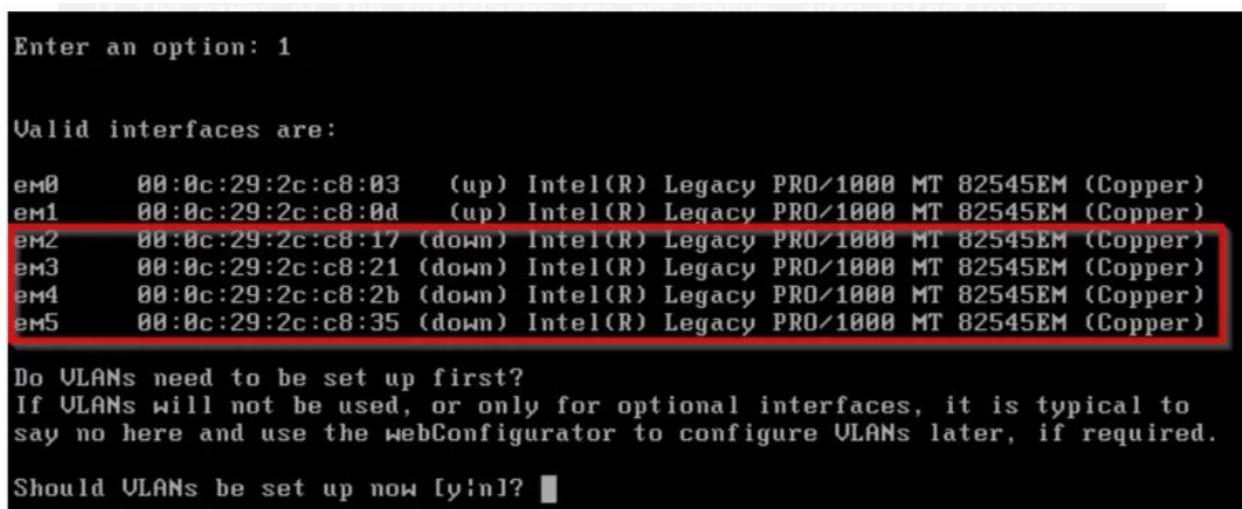
WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)      9) pfTop
1) Assign Interfaces       10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system           14) Enable Secure Shell (sshd)
6) Halt system             15) Restore recent configuration
7) Ping host               16) Restart PHP-FPM

Enter an option: 1
```

شكل رقم ()

من هنا، نرى جميع الواجهات الصالحة مع اثنين منها فقط (WAN & LAN) للأعلى وأربعة منها للأسفل. الخطوة التالية هي تمكين كل هذه الواجهات.



```
Enter an option: 1

Valid interfaces are:

em0  00:0c:29:2c:c8:03  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1  00:0c:29:2c:c8:0d  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em2  00:0c:29:2c:c8:17  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em3  00:0c:29:2c:c8:21  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em4  00:0c:29:2c:c8:2b  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em5  00:0c:29:2c:c8:35  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y:n]? 
```

شكل رقم ()

## Extended Detection and Response

*Should VLANs be set up now [y:n]?: n*

أدخل **em0** أو **em1** أو **em2** أو **em3** أو **em4** أو **em5** على التوالي لكل سؤال متالي. أخيراً، اكتب **(y)** للمتابعة.

```
Should VLANs be set up now [y:n]? n ←

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 em4 em5 or a): em0 ←

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 em4 em5 a or nothing if finished): em1 ←

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 em4 em5 a or nothing if finished): em2 ←

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 em4 em5 a or nothing if finished): em3 ←

Enter the Optional 3 interface name or 'a' for auto-detection
(em4 em5 a or nothing if finished): em4 ←

Enter the Optional 4 interface name or 'a' for auto-detection
(em5 a or nothing if finished): em5 █ ←
```

شكل رقم ()

الآن، يمكننا أن نرى أن جميع الواجهات صالحة ولكن بدون عناوين IP. بعد ذلك يتعين علينا تعيين عناوين IP لكل واجهة ( OPT4 ، OPT3 ، OPT2 ، OPT1 ، LAN ، MIRROR ) وترك SPAN لأن هذه الواجهة ستكون بمثابة منفذ

## Extended Detection and Response

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 3139eec8e0802bd48812

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.181.128
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      ->
OPT2 (opt2)    -> em3      ->
OPT3 (opt3)    -> em4      ->
OPT4 (opt4)    -> em5      ->

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2
```

شكل رقم ()

أدخل الخيار ٢. اتبع هذا وقم بتعيين عنوان IP على واجهة LAN.

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)
4 - OPT2 (em3)
5 - OPT3 (em4)
6 - OPT4 (em5)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.2.1

Subnet Masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0 = 16
      255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

شكل رقم ()

اتبع تكوين تعيين عنوان IP للواجهة أعلاه، وقم بتعيين عناوين IP للواجهات المتبقية.

نقوم بتكرار الطريقة الأولى في وضع عنوان **ip** ونحدد رقم **interface** الذي نريد وضع عنوان له ستكون العناوين كالتالي

**LAN = 192.168.2.1/24,**

**OPT1 = 192.168.3.1/24,**

**OPT2 = 192.168.4.1/24**

**OPT3 = 192.168.5.1/24**

تكوين أول عنوان لجهاز المهاجم

```
Configure IPv6 address LAN interface via DHCP6? (y/n) n ←
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y ←
Enter the start address of the IPv4 client address range: 192.168.2.1 ←
Enter the end address of the IPv4 client address range: 192.168.2.20 ←
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y ←

Please wait while the changes are saved to LAN...
  Reloading filter...
  Reloading routing configuration...
  DHCPD...
  Restarting webConfigurator...

The IPv4 LAN address has been set to 192.168.2.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
  http://192.168.2.1/
Press <ENTER> to continue. █
```

شكل رقم ()

## Extended Detection and Response

### تكوين ثانٍ لجهاز مراقب الشبكة Wireshark

```
Enter an option: 2 ←
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)
4 - OPT2 (em3)
5 - OPT3 (em4)
6 - OPT4 (em5)

Enter the number of the interface you wish to configure: 3 ←
Configure IPv4 address OPT1 interface via DHCP? (y/n) n ←
Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 192.168.3.1 ←

Subnet Masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0 = 16
      255.0.0.0 = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24 ←
```

الشكل رقم ()

### تكوين الثالث عنوان لجهاز إدارة لأجهزة AD DM

```
Configure IPv6 address OPT1 interface via DHCP6? (y/n) n ←
Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) y ←
Enter the start address of the IPv4 client address range: 192.168.3.1 ←
Enter the end address of the IPv4 client address range: 192.168.3.20 ←
Disabling IPv6 DHCPD...

Please wait while the changes are saved to OPT1...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 OPT1 address has been set to 192.168.3.1/24
You can now access the WebConfigurator by opening the following URL in your web
browser:
http://192.168.3.1/ ←

Press <ENTER> to continue. █
```

### الشكل رقم ()

عندما تكون المخرجات بهذا الشكل أي اننا قمنا بأعداد **PfSense** بشكل صحيح وقمنا بتكوين **IP address** *for interfaces of network*

```

http://192.168.5.1/
Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 3139eec8e0802bd48812

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

[ WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.128
  LAN (lan)      -> em1      -> v4: 192.168.2.1/24
  OPT1 (opt1)    -> em2      -> v4: 192.168.3.1/24
  OPT2 (opt2)    -> em3      -> v4: 192.168.4.1/24
  OPT3 (opt3)    -> em4      -> v4: 192.168.5.1/24
  OPT4 (opt4)    -> em5      ->

  0) Logout (SSH only)          9) pfTop
  1) Assign Interfaces          10) Filter Logs
  2) Set interface(s) IP address 11) Restart webConfigurator
  3) Reset webConfigurator password 12) PHP shell + pfSense tools
  4) Reset to factory defaults 13) Update from console
  5) Reboot system              14) Enable Secure Shell (sshd)
  6) Halt system                15) Restore recent configuration
  7) Ping host                  16) Restart PHP-FPM

Enter an option: ■

```

### الشكل رقم ()

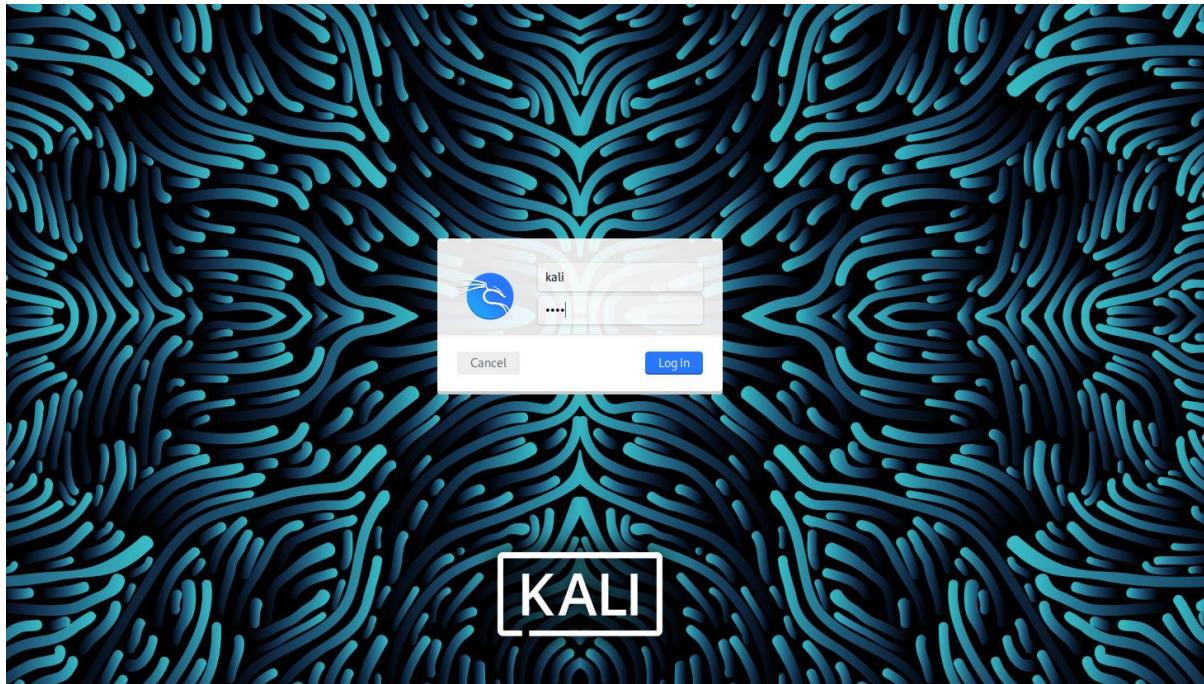
تخيل معملنا هذا كقاعدة للأبطال الخارقين. لذلك، قمنا بتنصيب جدار حماية رائع يسمى **pfSense**، حارسنا الخارق. يمكنك التفكير في الأمر كحارس بوابة له **6** أبواب (**interfaces**) خاصة لأنواع مختلفة من حركة مرور الشبكة.

### ٣،٤،٥. يتم تثبيت kali linux

سنقوم بتنصيب جهاز الهجوم الخاص بنا وكذلك إجراء تكوينات على جدار الحماية الخاص بنا. **NAT Door**: هذا الباب يواجه الإنترنت، مثل النافذة لرؤية ما يحدث هناك وهو الذي يسمح لنا بالاتصال بالإنترنت.

لدينا 5 أبواب إضافية للمهام الخاصة، مثل التأكد من دخول الأشياء الجيدة فقط عن طريق المراقبة. يساعدنا حارس الأبطال الخارجين (PfSense) في مراقبة من يدخل ومن يخرج ويتحكم فيه. إنه مثل وجود وصي لكل جزء من مختبرنا. أو تصور الأمر على هذا النحو: إن نظام PfSense الخاص بنا هو الحارس اليقظ، ونحن، المهندسون المعماريون، قمنا بالوصول إلى واجهات الويب الخاصة به لإعداد القواعد.

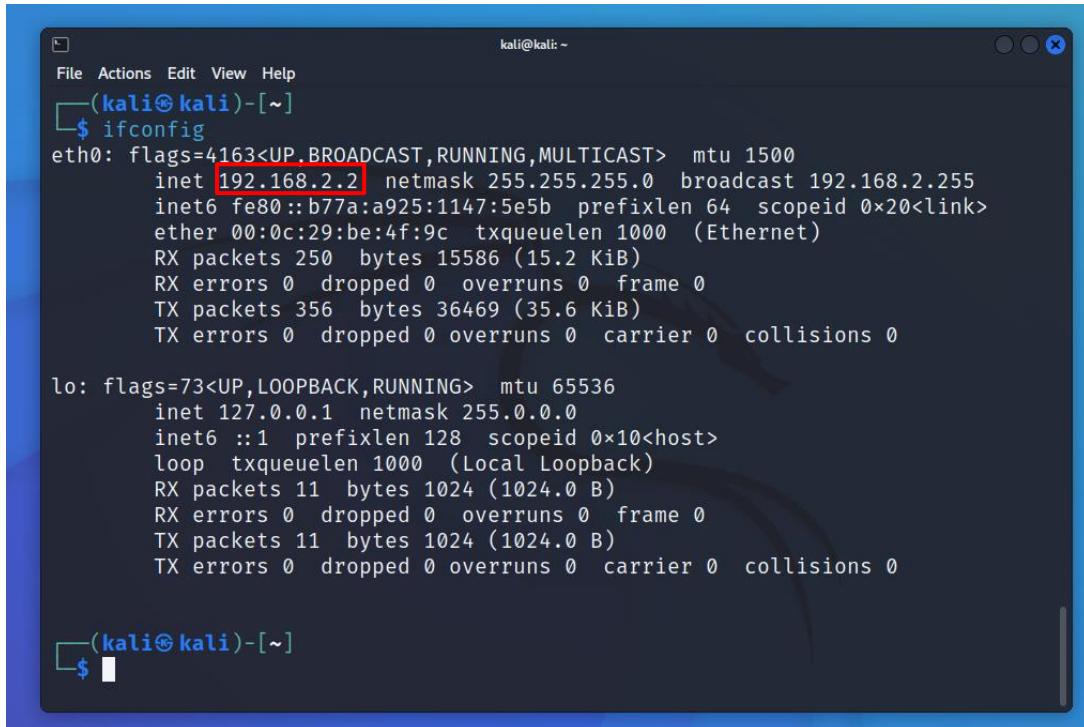
الآن، نحن مستعدون - لتنصيب Kali ، جاسوسنا الخارق بعد إتمام تثبيت النظام، نقوم بدخول للنظام (kali – kali).



الشكل رقم ()

نذهب الى terminal واتكتب الأمر **ifconfig** وهنا، يمكننا أن نرى أن جدار الحماية الخاص بنا قد قام بتعيين عنوان IP 192.168.2.2 لجهاز VM الخاص بالهجوم. بعد ذلك، يتغير علينا الوصول إلى واجهة الويب الخاصة بجدار الحماية.

## Extended Detection and Response



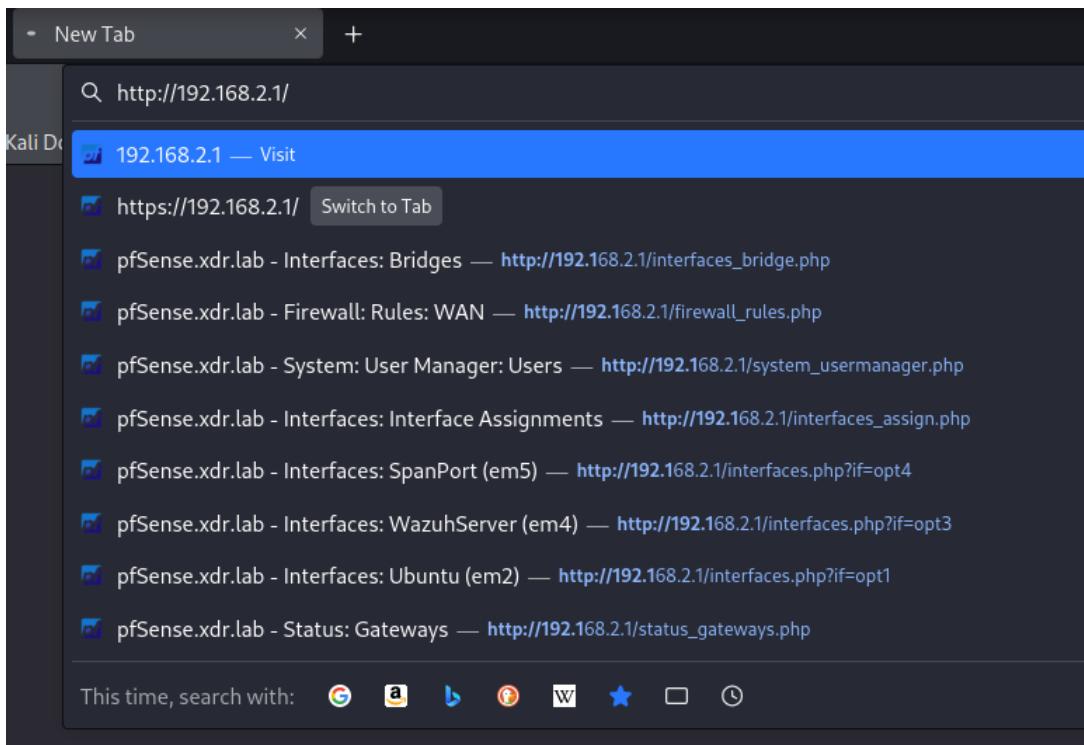
```
File Actions Edit View Help
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.2.2  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::b77a:a925:1147:5e5b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:be:4f:9c  txqueuelen 1000  (Ethernet)
        RX packets 250  bytes 15586 (15.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 356  bytes 36469 (35.6 KiB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

    lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 11  bytes 1024 (1024.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11  bytes 1024 (1024.0 B)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali㉿kali)-[~]
$
```

الشكل رقم ()

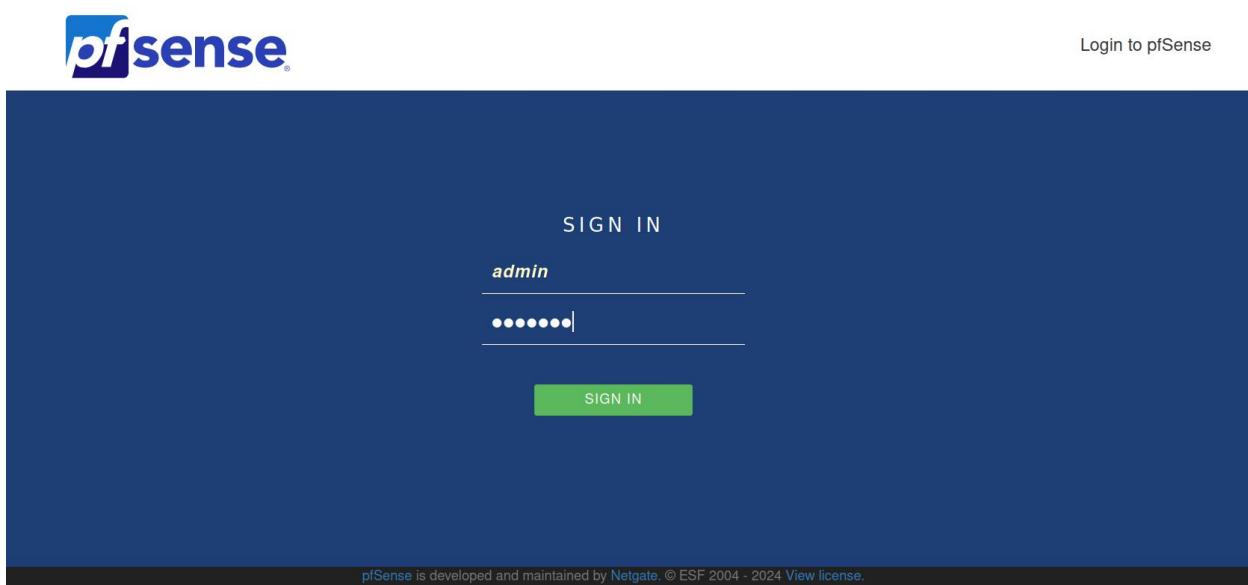
قم بتشغيل Mozilla Firefox واتكتب <http://192.168.2.1> في المتصفح إلى اسم المستخدم وكلمة المرور الافتراضية هما (admin pfsense) ثم اضغط على زر الإدخال.



## Extended Detection and Response

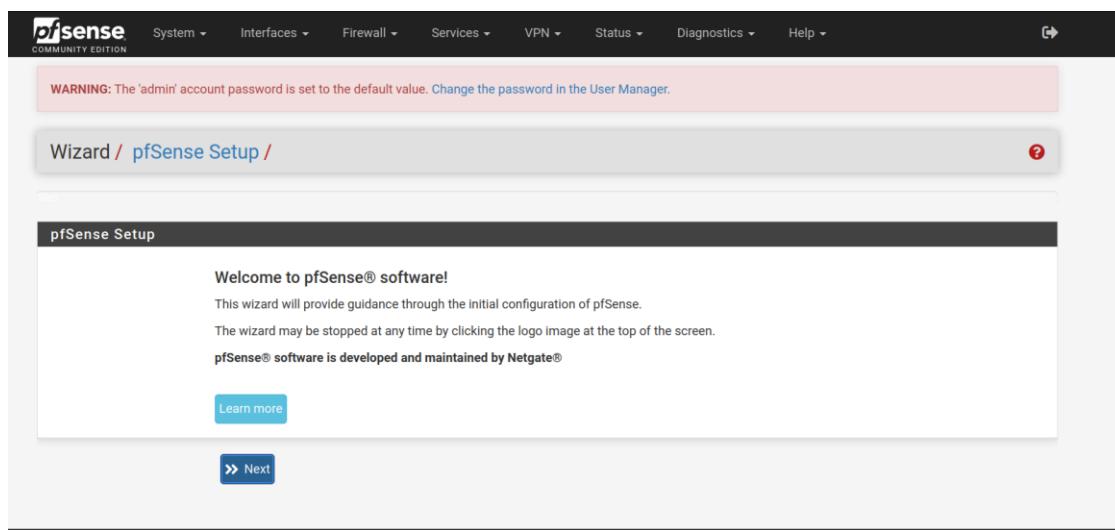
(الشكل رقم ٤)

بعد تسجيل الدخول بنجاح، سيتم الترحيب بك بشاشة ترحيب لإعداد جدار الحماية. انقر على **next**.



(الشكل رقم ٥)

نقوم بوضع **DNS**، واسم للمجال جدار الحماية



(الشكل رقم ٦)

## Extended Detection and Response

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / General Information

Step 2 of 9

**General Information**

On this screen the general pfSense parameters will be set.

**Hostname** pfSense **1**  
Name of the firewall host, without domain part.  
Examples: pfSense, firewall, edgefw

**Domain** home.arpa  
Domain name for the firewall.  
Examples: home.arpa, example.com  
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

**Primary DNS Server** 8.8.8.8 **2**  
**Secondary DNS Server** 4.4.4.4 **3**

**Override DNS**   
Allow DNS servers to be overridden by DHCP/PPP on WAN

**>> Next** **4**

الشكل رقم (١)

هنا، يمكنك اختيار **منطقتك الزمنية** على توقيت اليمن Etc/GMT+3 والنقر على التالي.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

**Time Server Information**

Please enter the time, date and time zone.

**Time server hostname** 2.pfsense.pool.ntp.org  
Enter the hostname (FQDN) of the time server.

**Timezone** Etc/GMT-3 **1**

**>> Next**

الشكل رقم (٢)

## Extended Detection and Response

في الصفحة التالية، قم بالتمرير إلى الأسفل وقم بإلغاء تحديد خيارات **RFC** أدناه وانقر فوق "التالي".

PPTP Dial on demand  Enable Dial-On-Demand mode  
This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

PPTP Idle timeout   
If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

**RFC1918 Networks**

**Block RFC1918 Private Networks**  Block private networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

**Block bogon networks**

**Block bogon networks**  Block non-Internet routed networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

**>> Next**

الشكل رقم ()

على واجهة LAN ، نترك كل شيء افتراضياً ونضغط على "التالي"

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**WARNING:** The 'admin' account password is set to the default value. Change the password in the User Manager.

**Wizard / pfSense Setup / Configure LAN Interface** **?**

Step 5 of 9

**Configure LAN Interface**

On this screen the Local Area Network information will be configured.

**LAN IP Address**  Type dhcp if this interface uses DHCP to obtain its IP address.

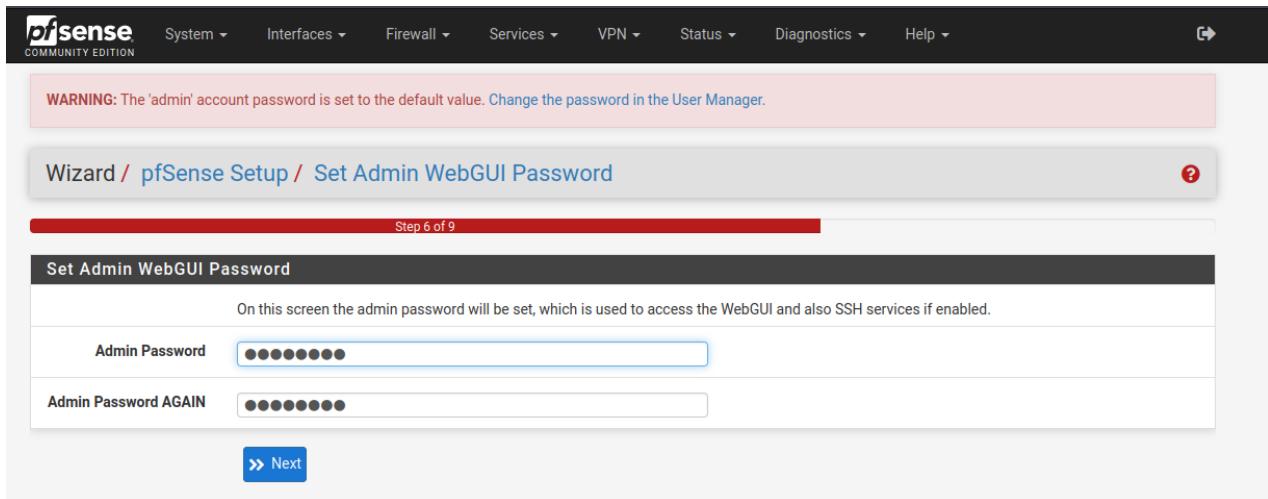
**Subnet Mask**

**>> Next**

الشكل رقم ()

## Extended Detection and Response

الخطوة الأخيرة هي تغيير كلمة المرور الافتراضية وتحديد **next** ستكون (pfSense1)



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

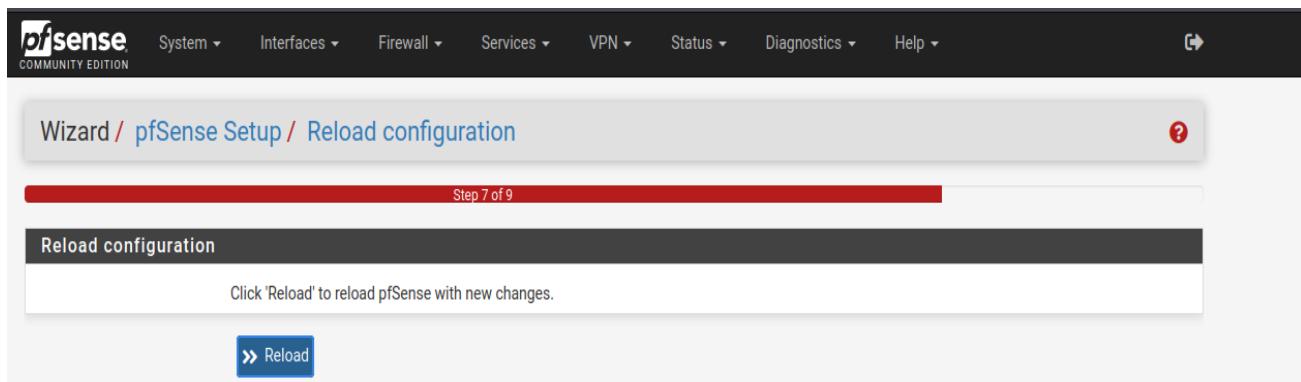
Admin Password:

Admin Password AGAIN:

» Next

(الشكل رقم 1)

ثم حدد إعادة التحميل **reload** و **finish** للانتهاء من تكوين الإعداد الأولي.



Wizard / pfSense Setup / Reload configuration

Step 7 of 9

Reload configuration

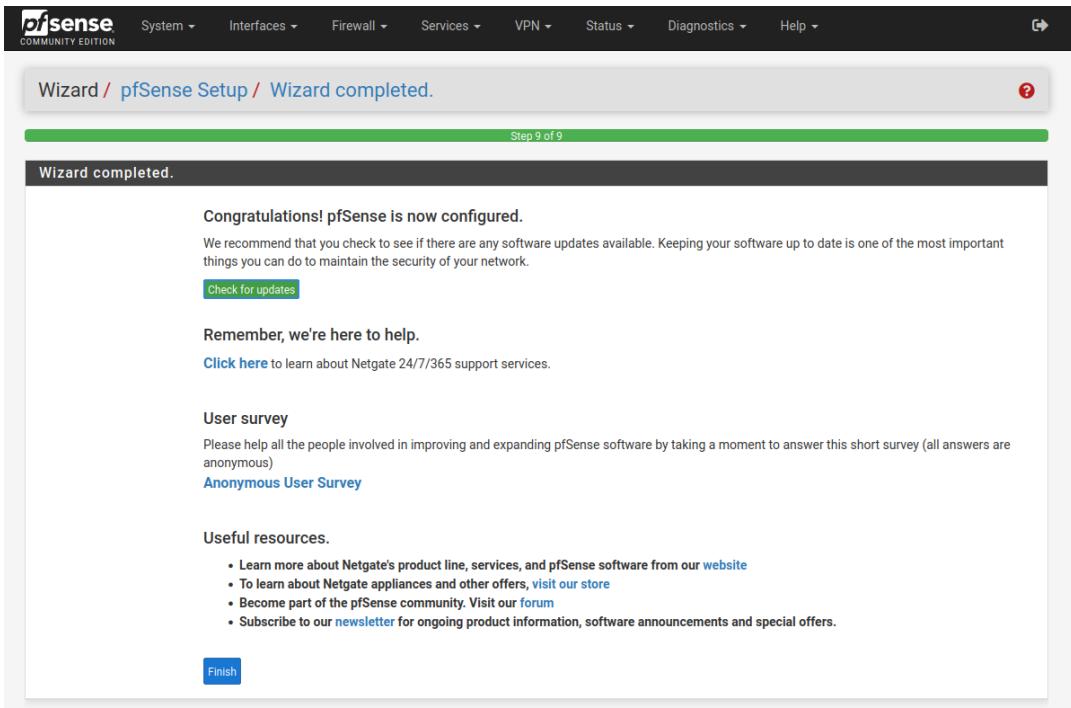
Click 'Reload' to reload pfSense with new changes.

» Reload

(الشكل رقم 2)

## Extended Detection and Response

بعد الإعداد، يجب أن تكون هذه هي لوحة المعلومات الخاصة بك على جدار الحماية.



الشكل رقم ()

## Extended Detection and Response

System Information

Name	pfSense.home.arpa
User	admin@192.168.2.2 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 3139eec8e0802bd48812
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 23:10:00 +03 2023 FreeBSD 14.0-CURRENT
Unable to check for updates	
CPU Type	Intel(R) Core(TM) i5-4300M CPU @ 2.60GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	01 Hour 19 Minutes 57 Seconds
Current date/time	Tue Apr 23 5:08:36 +03 2024
DNS server(s)	• 127.0.0.1 • 192.168.181.2 • 8.8.8.8 • 4.4.4.4
Last config change	Tue Apr 23 5:02:52 +03 2024
State table size	0% (9/19000) <a href="#">Show states</a>
MBUF Usage	1% (5510/1000000)
Load average	1.51, 1.01, 0.83
CPU usage	<div style="width: 29%;">29%</div>

Netgate Services And Support

Retrieving support information

Interfaces

Interface	Duplex	IP Address
WAN	1000baseT <full-duplex>	192.168.181.128
LAN	1000baseT <full-duplex>	192.168.2.1
OPT1	1000baseT <full-duplex>	192.168.3.1
OPT2	1000baseT <full-duplex>	192.168.4.1
OPT3	1000baseT <full-duplex>	192.168.5.1

الشكل رقم ()

الآن، نحن بحاجة إلى تعيين أسماء لجميع الواجهات لذلك، في القائمة العلوية، حدد.

Interfaces

Assignments

WAN	LAN
OPT1	LAN
OPT2	
OPT3	
OPT4	

Netgate Services And Support

Retrieving support information

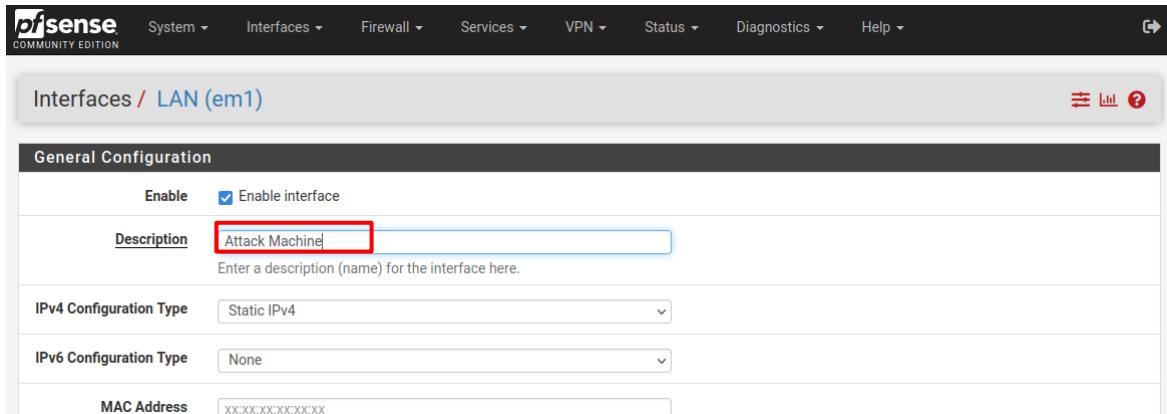
Interfaces

Interface	Duplex	IP Address
WAN	1000baseT <full-duplex>	n/a
LAN	1000baseT <full-duplex>	192.168.2.1
OPT1	1000baseT <full-duplex>	192.168.3.1
OPT2	1000baseT <full-duplex>	192.168.4.1
OPT3	1000baseT <full-duplex>	192.168.5.1

## Extended Detection and Response

الشكل رقم ()

قم بتغيير اسم المضيف إلى Attack Machine، واترك كل شيء افتراضياً وانقر على حفظ وتطبيق التغييرات



الشكل رقم ()

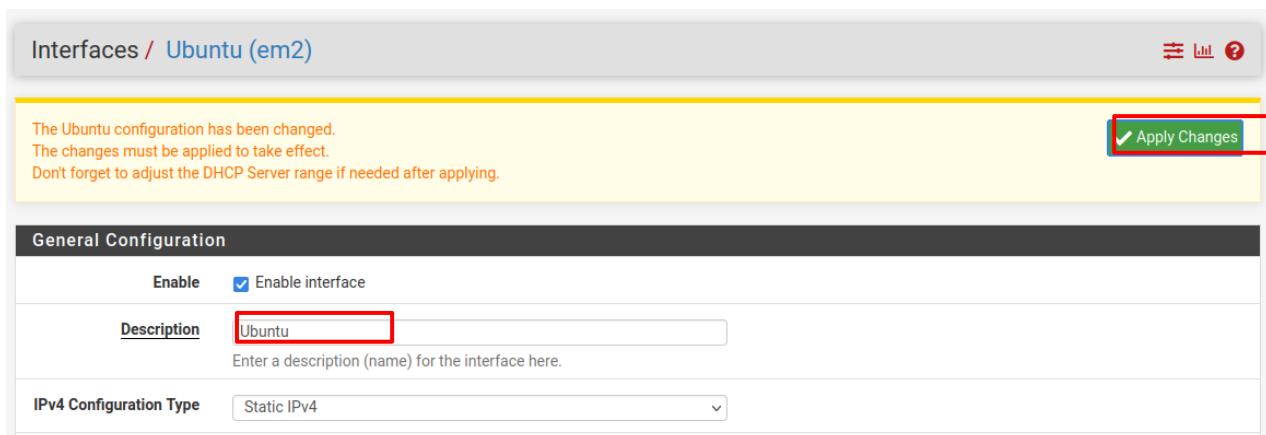
ملاحظة سيتم عمل نفس الشيء مع الواجهات الأخرى

**OPT1 = Ubuntu**

**OPT2 = AD DS**

**OPT3 = SIEM**

**OPT4 = Span Port**



الشكل رقم ()

## Extended Detection and Response

في القائمة العلوية، انقر فوق **Interface > Assignment** يجب أن يسرد هذا جميع الوجهات الموجودة على جدار الحماية الخاص بنا، مع الأسماء المخصصة وعنوان MAC المرتبط.

Interfaces / Interface Assignments

Assignments

WAN

ATTACKMACHINE

UBUNTU

ACTIVE DIRECTORY DS

WAZUH SERVER

SPAN PORT

em1 (00:0c:29:b2:69:ec)

em2 (00:0c:29:b2:69:00)

em3 (00:0c:29:b2:69:0a)

em4 (00:0c:29:b2:69:14)

em5 (00:0c:29:b2:69:1e)

Delete

Delete

Delete

Delete

Delete

Save

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

(الشكل رقم ٤)

نحتاج الآن إلى توصيل الواجهة التي نريد مراقبتها بمنفذ الامتداد span port الخاص بنا. في هذا المشروع، الواجهة التي سنراقبها هي بيئة AD DS الخاصة بنا. انتقل إلى صفحة الوجهات، وانقر على **Bridges**

Interfaces / Bridges

Interfaces Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

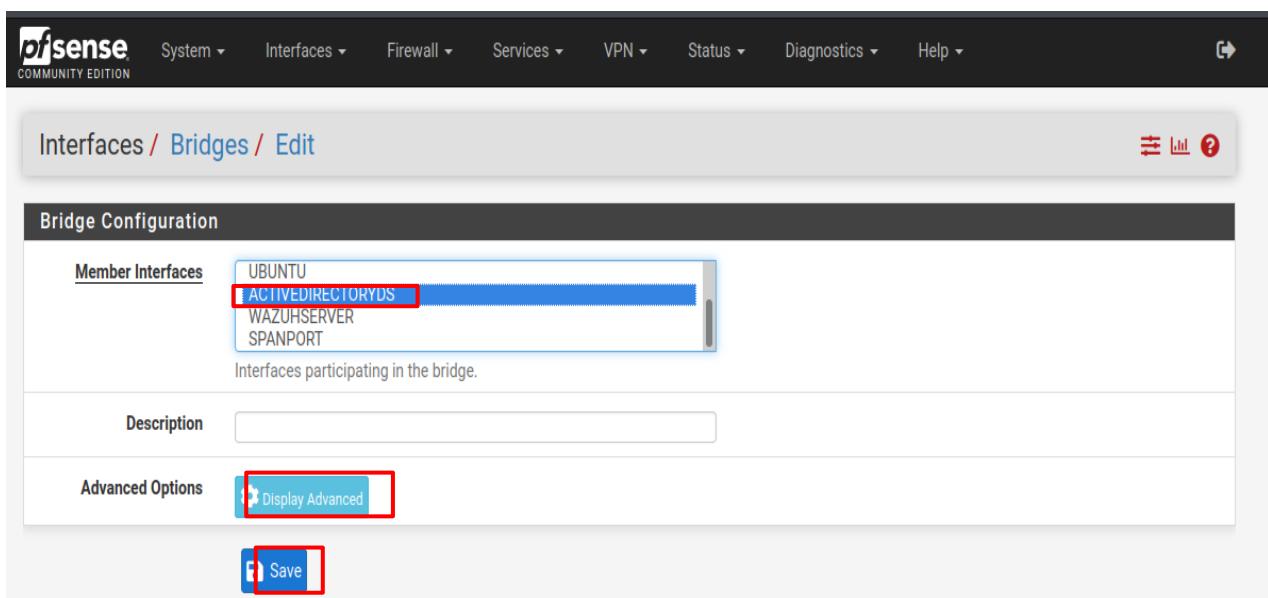
Bridge Interfaces

Interface	Members	Description	Actions
			<b>+ Add</b>

(الشكل رقم ٥)

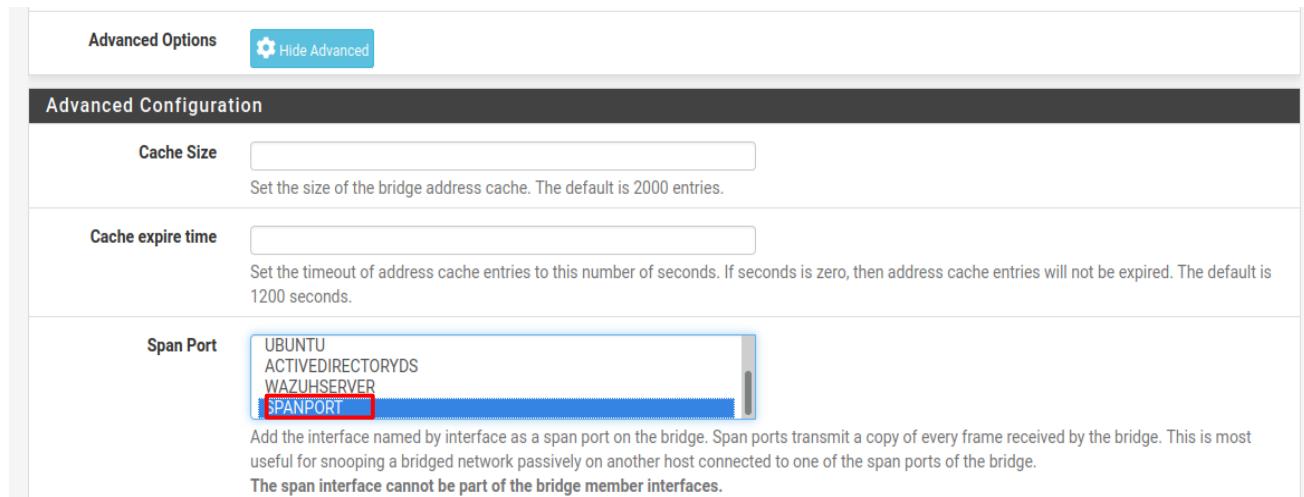
## Extended Detection and Response

حدد الزر "إضافة" "توصيل واجهة AD DS الخاصة بنا بمنفذ Span" وانقر فوق "عرض متقدم" "advanced".



الشكل رقم ()

ضمن التكوين المتقدم advanced configuration ، قم بالتمرير لأسفل إلى منفذ الامتداد span port وأضف تلك الواجهة كـ bridge للمراقبة



الشكل رقم ()

## Extended Detection and Response

سيكون بهذا الشكل بعد الإنشاء

Interfaces / Bridges

Bridge Interfaces

Interface	Members	Description	Actions
BRIDGE0	ACTIVEDIRECTORYDS		

**الشكل رقم ()**

بعد ذلك، نحتاج إلى إعداد قاعدة جدار الحماية على واجهة WAN الخاصة بنا للسماح بالاتصال بالإنترنت. في الجزء العلوي، حدد **firewall**، حدد **Rules > firewall**

Firewall > Rules

Aliases  
NAT  
**Rules**  
Schedules  
Traffic Shaper  
Virtual IPs

**الشكل رقم ()**

ثم حدد  **WAN > Add**

Firewall / Rules / WAN

Floating **WAN** ATTACKMACHINE UBUNTU ACTIVEDIRECTORYDS WAZUHSERVER SPANPORT

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.										
<b>Add</b>										

**الشكل رقم ()**

## Extended Detection and Response

ضمن الإجراء، اختر **Pass** ضمن البروتوكول، حدد **Any** وقم بتطبيق التغييرات لحفظ الإعدادات.

Firewall / Rules / Edit

**Edit Firewall Rule**

**Action**  ←

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**  Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface**  ←  
Choose the interface from which packets must come to match this rule.

**Address Family**  ←  
Select the Internet Protocol version this rule applies to.

**Protocol**  ←  
Choose which IP protocol this rule should match.

الشكل رقم ()

بعد الإضافة والحفظ سيكون بشكل التالي

Firewall / Rules / WAN

The firewall rule configuration has been changed.  
The changes must be applied for them to take effect.

Floating  WAN  ATTACKMACHINE  UBTNTU  ACTIVEDIRECTORYDS  WAZUHSERVER  SPANPORT

**Rules (Drag to Change Order)**

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="checked" type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator

الشكل رقم ()

حاليا يعتبر قد نجحت في إعداد KALI كجهاز افتراضي وتكوين جدار الحماية، مما أدى إلى اتخاذ خطوة مهمة نحو بناء بيئة الشبكة الخاصة بنا

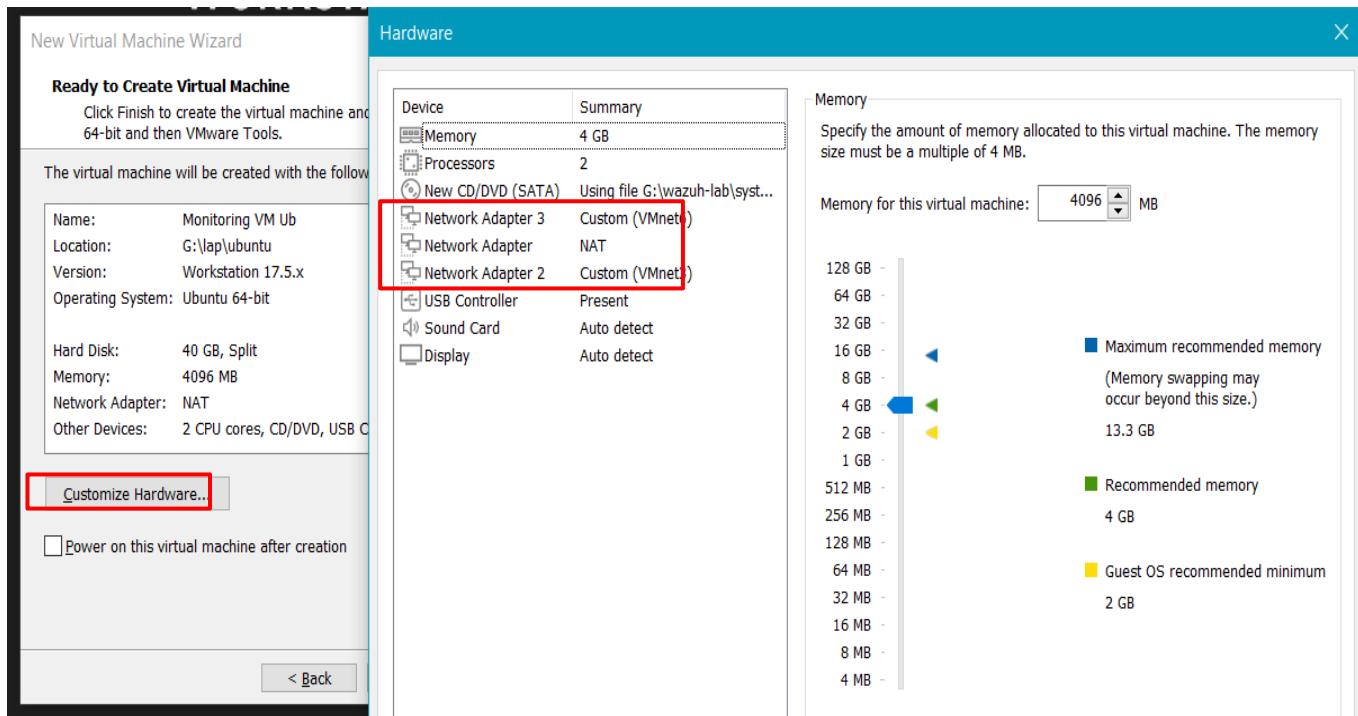
### ٤،٥. يتم تثبيت في هذه المرحلة نظام ubuntu

الآن، الخطوة العقدية؟ سد واجهة span port المنفذ الممتد لدينا. وهذا يشبه إنشاء برج مراقبة فائق، مما يسمح لنا بمراقبة وتدقيق كل حركة في شبكتنا. إنها لعبة استراتيجية لتعزيز دفاعاتنا والبقاء في المقدمة في لعبة الأمن السيبراني.

## • إعداد محلل الشبكة **SETTING UP ANALYST**

سيتم استخدام هذا كجهاز تحليل خاص بنا لرصد حركة مرور الشبكة ومراقبتها من الأجهزة الموجودة داخل بيئة الدليل النشط والتي سنقوم بإعدادها لاحقاً في السلسلة. سنقوم أيضاً بتنصيب **Wireshark** الذي سيمكننا من التعرف على الشبكة لجميع حركة المرور الصادرة والواردة. دعونا أولاً نقوم بتنصيب نظام **ubuntu**

نقوم بنفس عملية التنصيب الذي نحن نعرفها ونقوم بها دائماً، ولكن سنضيف بعض التخصيص **customize** في **network adapter**، ثم بعد ذلك أيضاً نقوم بعملية التنصيب المعروفة



الشكل رقم ()

بعد عملية التثبيت نقوم بدخول إلى النظام. الآن بعد الدخول نحن بحاجة إلى التحقق من واجهاتنا لتعيين IP.

قم بتشغيل المحطة، واتكتب

```
ubuntu@ubuntu-virtual-machine:~$ ifconfig ←
Command 'ifconfig' not found, but can be installed with:
sudo apt install net-tools ←
ubuntu@ubuntu-virtual-machine:~$ sudo apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 279 not upgraded.
Need to get 204 kB of archives.
After this operation, 819 kB of additional disk space will be used.
Get:1 http://ye.archive.ubuntu.com/ubuntu jammy/main amd64 net-tools amd64 1.6
Fetched 204 kB in 16s (13.1 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 161840 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20181103.0eebece-1ubuntu5_amd64.deb
Unpacking net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Setting up net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Processing triggers for man-db (2.10.2-1) ...
ubuntu@ubuntu-virtual-machine:~$
```

(الشكل رقم )

بعد التثبيت، اكتب ifconfig لعرض كافة مهام الواجهة كما هو موضح . يمكننا أن نرى هنا أن جميع الواجهات الثلاث التي قمنا بتعيينها قد ظهرت.

## Extended Detection and Response

```
ubuntu@ubuntu-virtual-machine:~$ ifconfig ←
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.181.129 netmask 255.255.255.0 broadcast 192.168.181.255
inet6 fe80::932b:5db7:614f:9c93 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:7c:bd:63 txqueuelen 1000 (Ethernet)
RX packets 110150 bytes 158878654 (158.8 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 23152 bytes 1619332 (1.6 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens34: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.3.2 netmask 255.255.255.0 broadcast 192.168.3.255
inet6 fe80::5d0b:a461:9d93:5e14 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:7c:bd:6d txqueuelen 1000 (Ethernet)
RX packets 93 bytes 6426 (6.4 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3308 bytes 284775 (284.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens35: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::d5d1:a196:e226:e449 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:7c:bd:77 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 772 bytes 130167 (130.1 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 5527 bytes 523720 (523.7 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 5527 bytes 523720 (523.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

(الشكل رقم ٤)

إلى هنا تكون قد اتمينا تثبيت ubuntu، التالي هو تثبيت Wireshark للاستئشاق sniffing. قم بتحديث الدليل إلى المجلد /opt/ لتنصيب الأداة. ثم اكتب

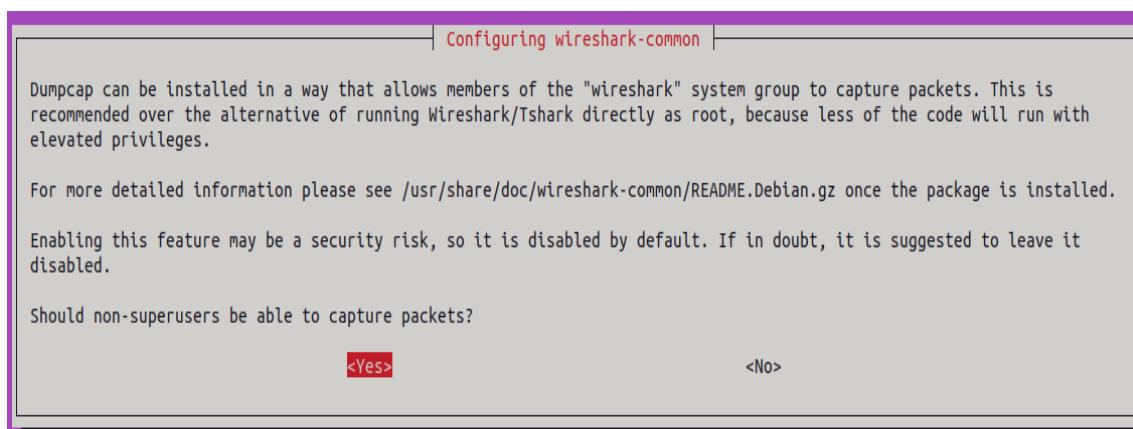
**sudo apt install wireshark-qt**

## Extended Detection and Response

```
ubuntu@ubuntu-virtual-machine:/$ cd /opt/ ←
ubuntu@ubuntu-virtual-machine:/opt$ wireshark ←
Command 'wireshark' not found, but can be installed with:
sudo apt install wireshark-qt
ubuntu@ubuntu-virtual-machine:/opt$ sudo apt install wireshark-qt
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0 libmi
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediasstools5 l
  libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl libsnappy1v5
  libwireshark15 libwiretap12 libwsutil13 libxcb-xinerama0 libxcb-xinput0
  wireshark-common
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate g
  libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0 libmi
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediasstools5 l
  libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl libsnappy1v5
  libwireshark15 libwiretap12 libwsutil13 libxcb-xinerama0 libxcb-xinput0
  wireshark-common wireshark-qt
```

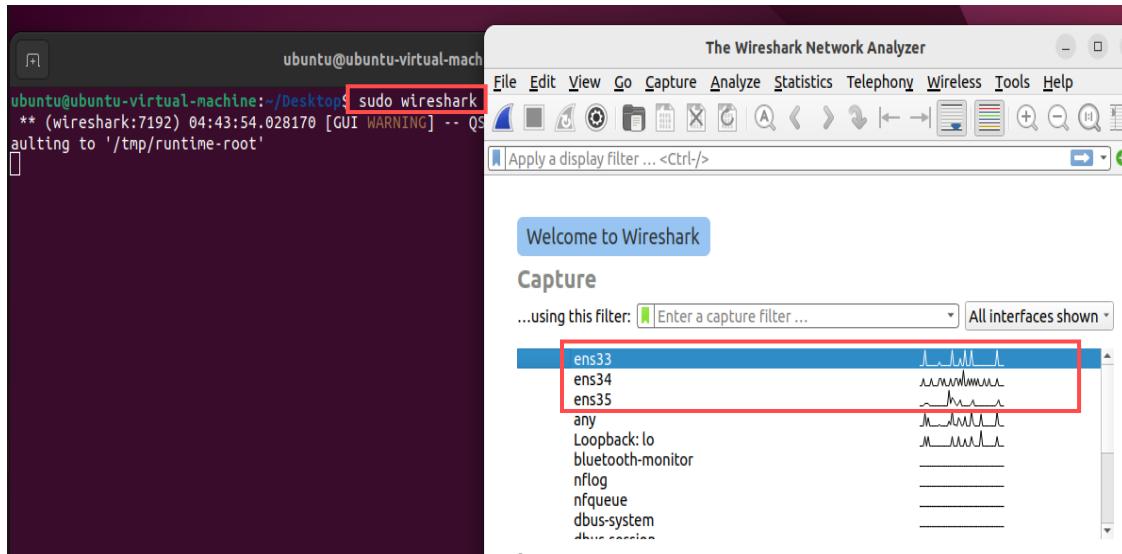
الشكل رقم ()

ثم نحدد yes للموافقة على الحزمة والتنبيت



الشكل رقم ()

بمجرد اكتمال التثبيت، انتقل إلى المحطة الطرفية واتكتب `sudo wireshark`. سوف تحصل على مطالبة بإدخال كلمة المرور الخاصة بك. بعد تسجيل الدخول بنجاح، يجب أن تظهر نافذة Wireshark بكل الواجهات المتاحة. هنا، واجهة الاستئشاق **sniffing** أو **span port** المنفذ الممتد هي **ens34**.

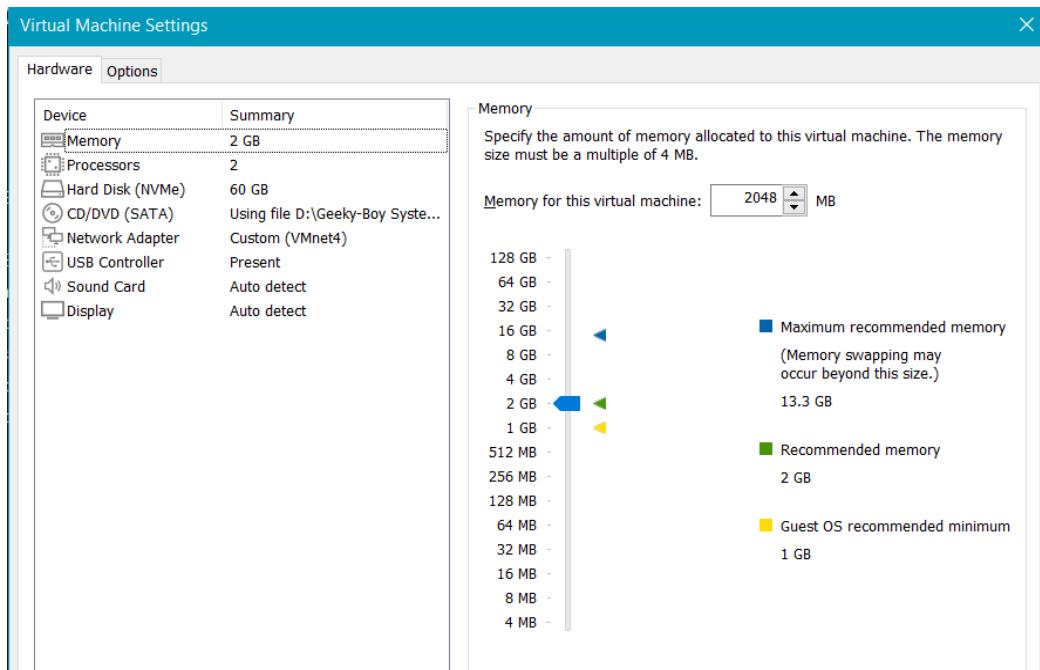


الشكل رقم ()

### ٥.٢.٥. تثبيت WINDOWS SERVER

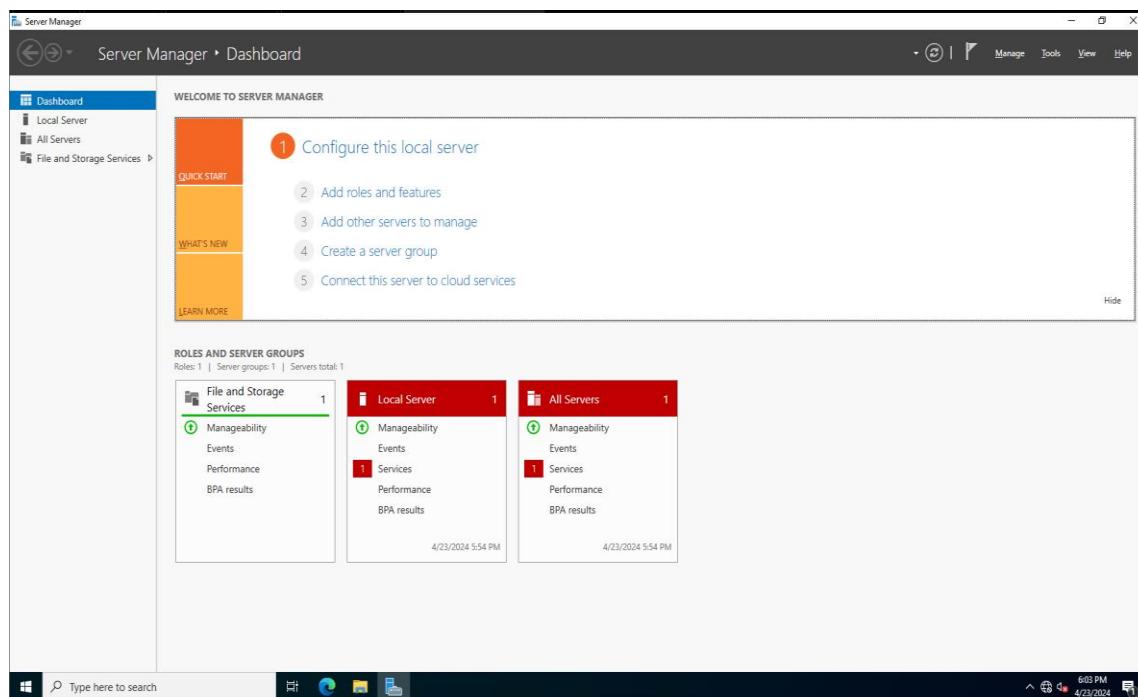
نقوم بفك ضغط الملف **iOS** وفتحه في البيئة كما تعاملنا مع الأنظمة الأخرى ولكن سنقوم بوضع تخصيص **customize**، تأكد من تحديد موارد الأجهزة اللازمة لهذا الجهاز الافتراضي. ثم انقر فوق "إغلاق" وقم بتشغيل **virtual machine** ونبأ بتكوين النظام

## Extended Detection and Response



الشكل رقم (١)

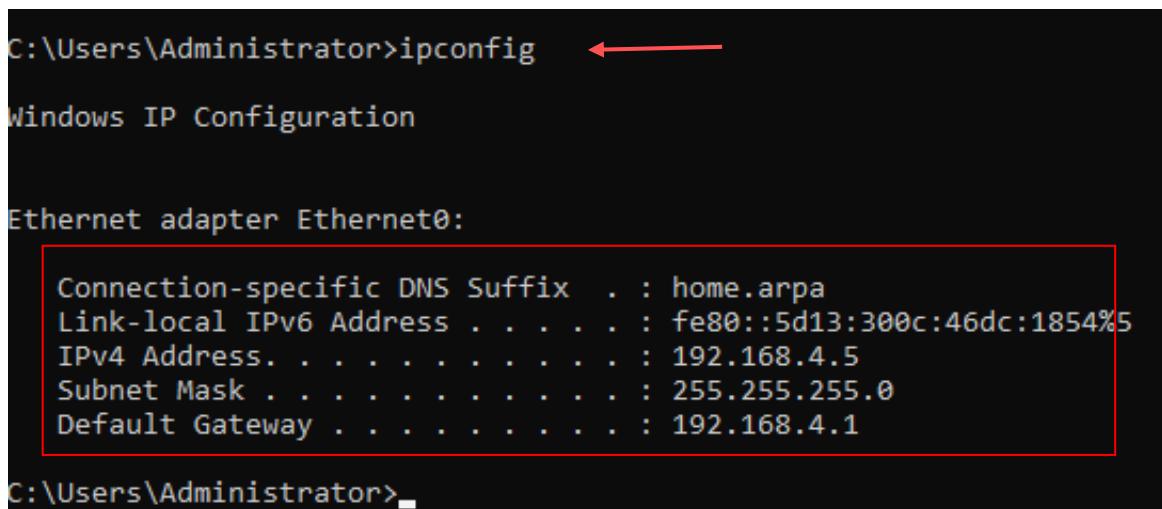
بعد التثبيت الناجح، تظهر شاشة تسجيل الدخول إلى Windows. قم بتسجيل الدخول وانقر على قائمة البداية من هناك. ستكون هذه وحدة التحكم الخاصة بنا لإدارة خادمنا. لتشغيل Server Manager



الشكل رقم (٢)

## Extended Detection and Response

للحصول على إعدادات DHCP الخاصة بـ ADDS، يجب تشغيل cmd وكتابة ipconfig. للتحقق من أن إعدادات DHCP الخاصة بـ ADDS يعمل بشكل جيد، انقر على واجهة cmd.



```
C:\Users\Administrator>ipconfig

Windows IP Configuration

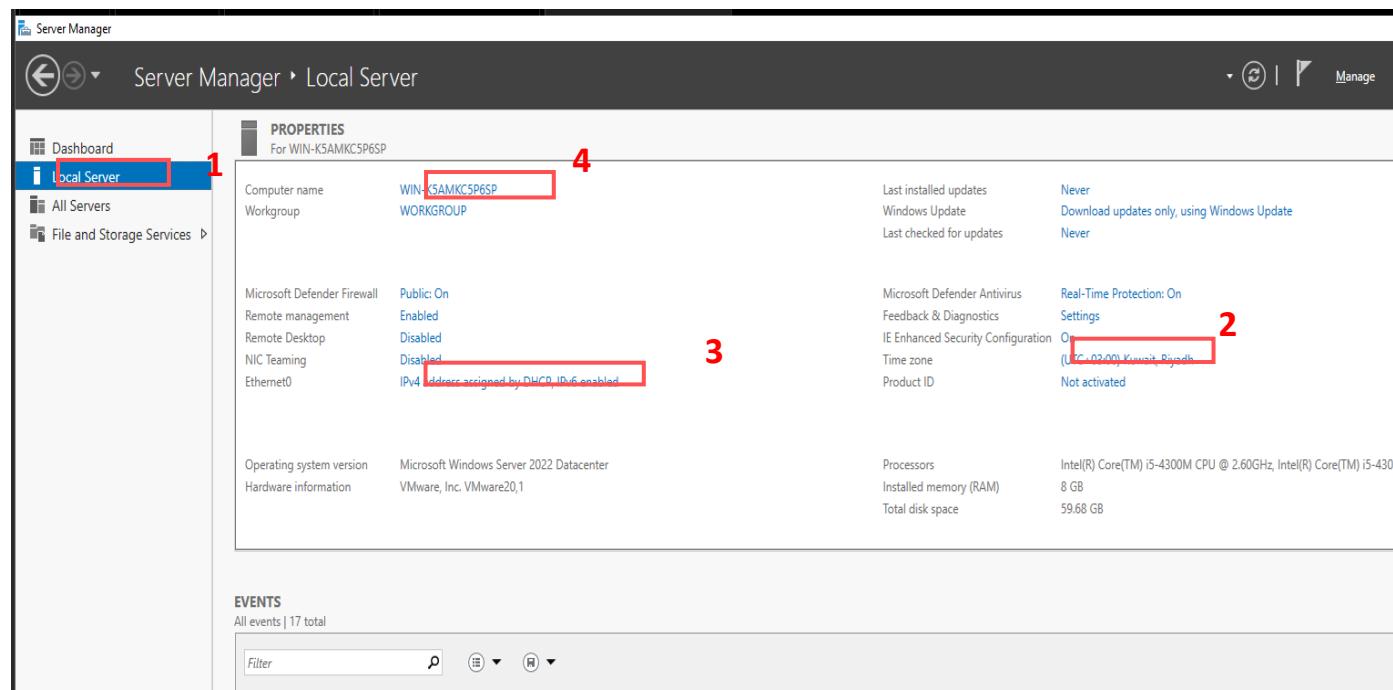
Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . . . : home.arpa
  Link-local IPv6 Address . . . . . : fe80::5d13:300c:46dc:1854%5
  IPv4 Address . . . . . : 192.168.4.5
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.4.1

C:\Users\Administrator>
```

الشكل رقم ()

في مدير الخادم، حدد **local server** ولدينا عرض لخصائص النظام لدينا، هنا سنتعيين علينا إجراء بعض التغييرات لمساعدتنا في تثبيت AD DS والقواعد .Role



Server Manager

Server Manager • Local Server

PROPERTIES

For WIN-K5AMKC5P6SP

1 Local Server

2

3

4

Computer name: WIN-K5AMKC5P6SP

Workgroup: WORKGROUP

Microsoft Defender Firewall: Public: On

Microsoft Defender Antivirus: Real-Time Protection: On

Operating system version: Microsoft Windows Server 2022 Datacenter

Processor: Intel(R) Core(TM) i5-4300M CPU @ 2.60GHz

Hardware information: VMware, Inc. VMware20,1

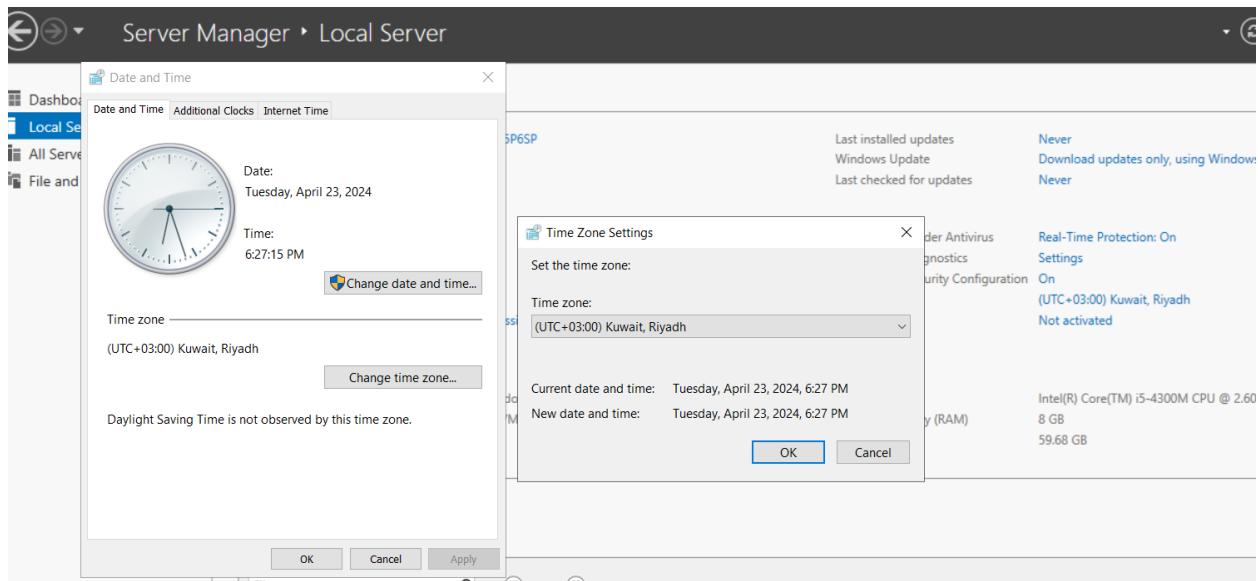
Installed memory (RAM): 8 GB

Total disk space: 59.68 GB

Events: 17 total

الشكل رقم ()

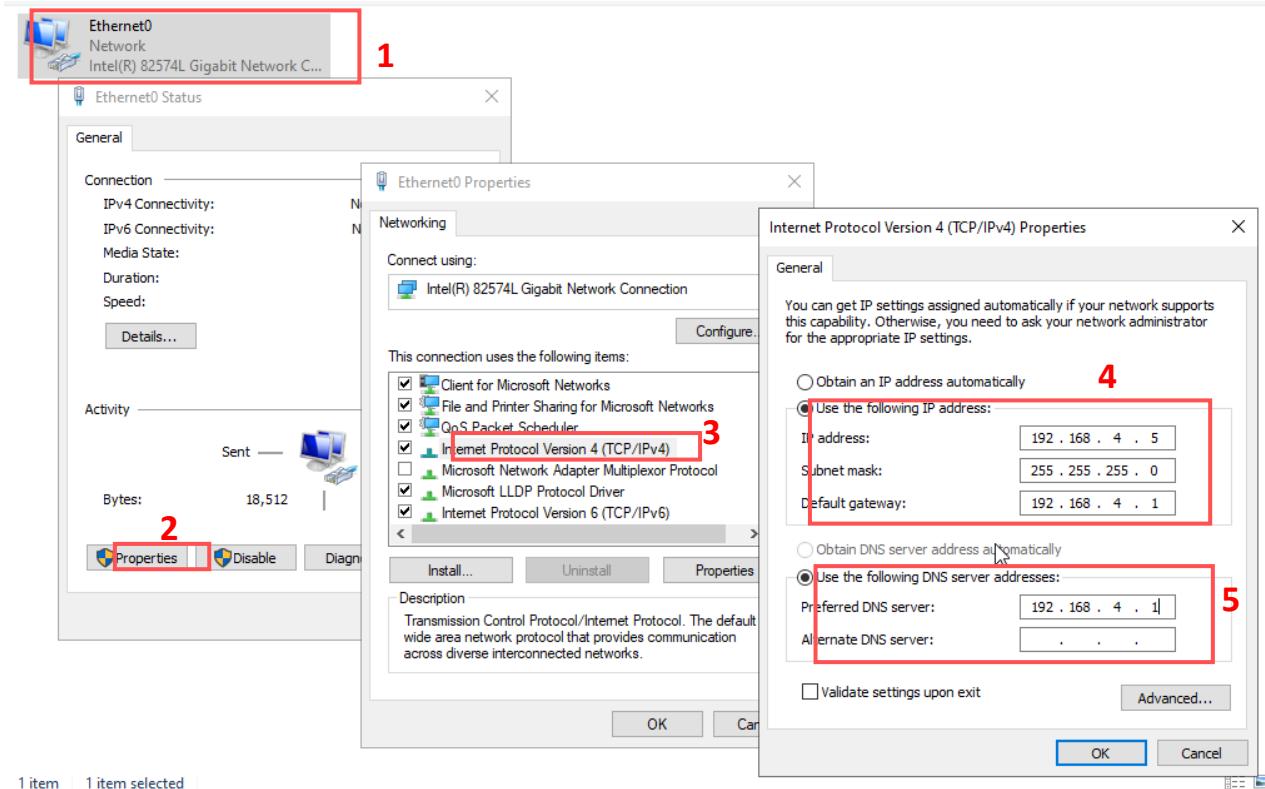
الأول هو تغيير إعدادات المنطقة الزمنية. انقر فوق **تغيير المنطقة الزمنية > UTC** حمافق.



الشكل رقم ()

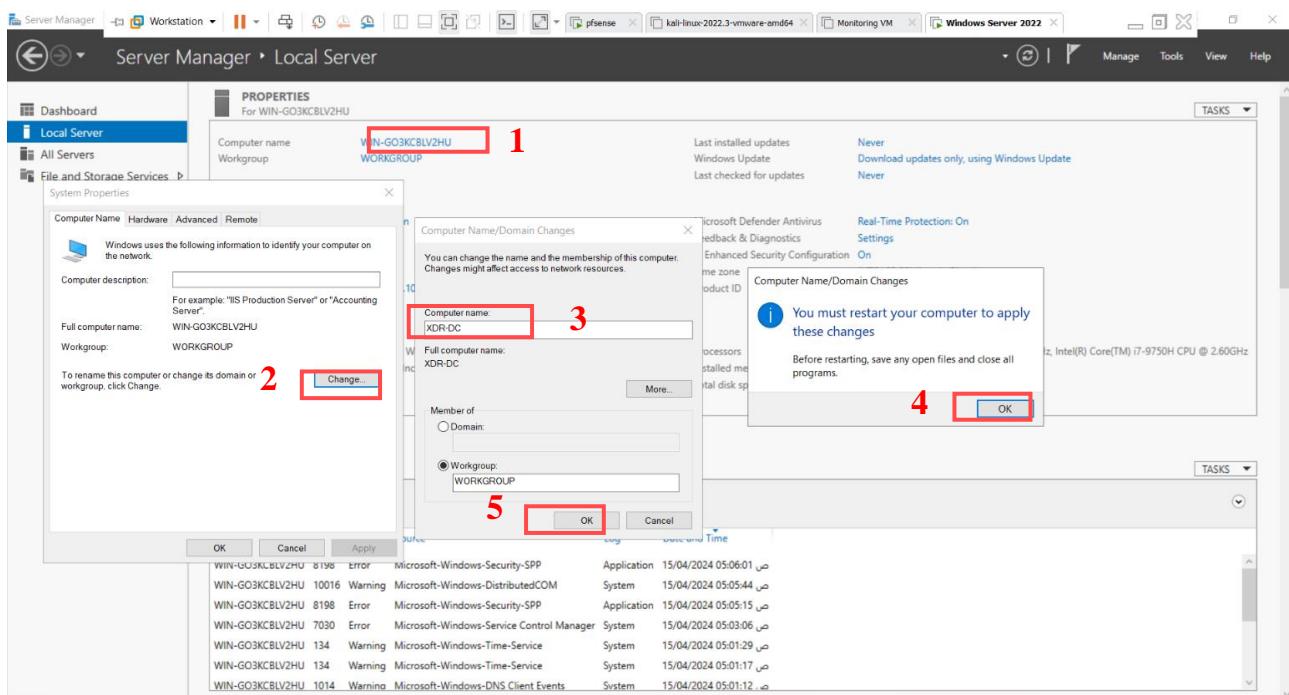
ثانياً، نقوم بتغيير إعدادات **adapter** أو **Ethernet** من وحدة تحكم مدير الخادم، انقر فوق عنوان > **IP** الخصائص > استخدم عنوان **IP** التالي . املأ عنوان **IP** الذي تريده. بعد ذلك، عليك اختيار عنوان **IP** المفضل لديك لخدمات **DNS**. نختار هنا عنوان **IP** للبوابة الافتراضية كما هو موضح أعلاه.

# Extended Detection and Response



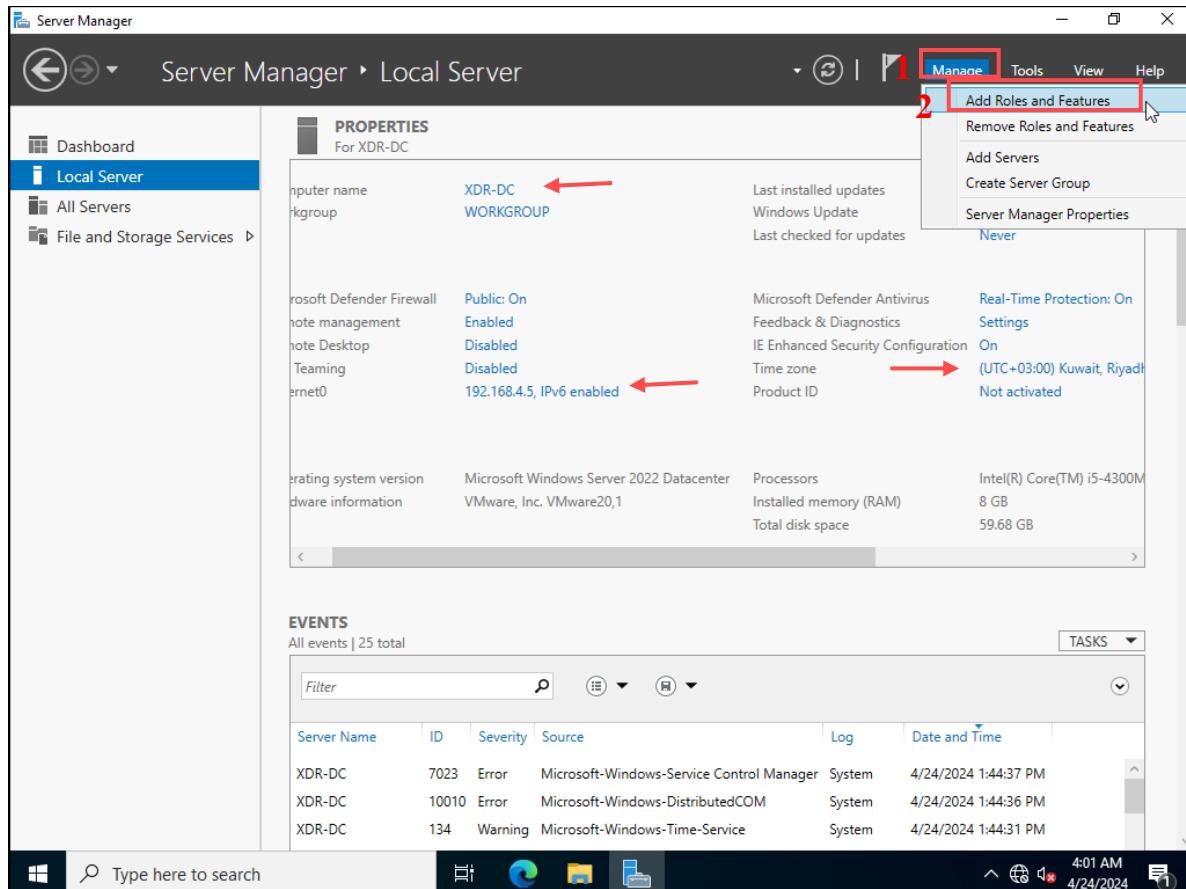
الشكل رقم (١)

التكوين الثالث هو تغيير اسم الكمبيوتر لخادمنا من اسم عام. انقر فوق **computer name > Change > enter the name > Click OK** لإعادة تشغيل الخادم وتطبيق التغييرات.



الشكل رقم ( )

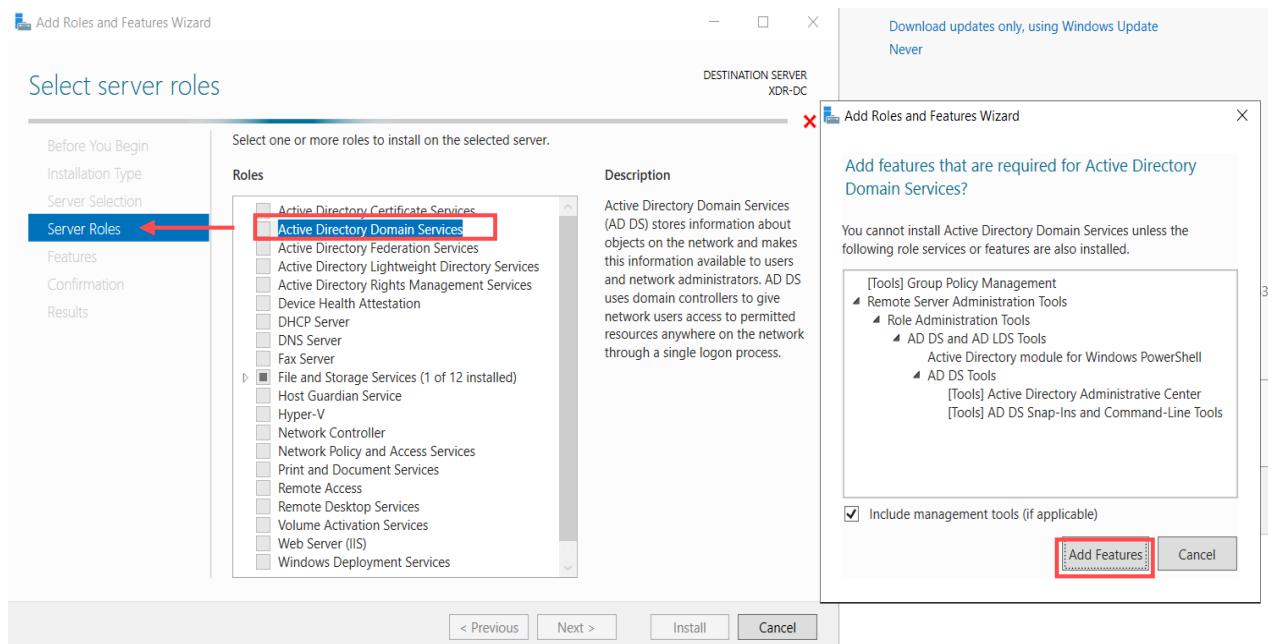
بعد تطبيق كافة التغييرات، يجب أن تكون وحدة تحكم مدير الخادم لديك مشابهة لهذه. الآن، في الزاوية العلوية اليمنى، انقر فوق إدارة **إضافة الأدوار والميزات**. ستفهم بتبثيت **AD AS** كـ **role** في بيئتنا.



### الشكل رقم ( )

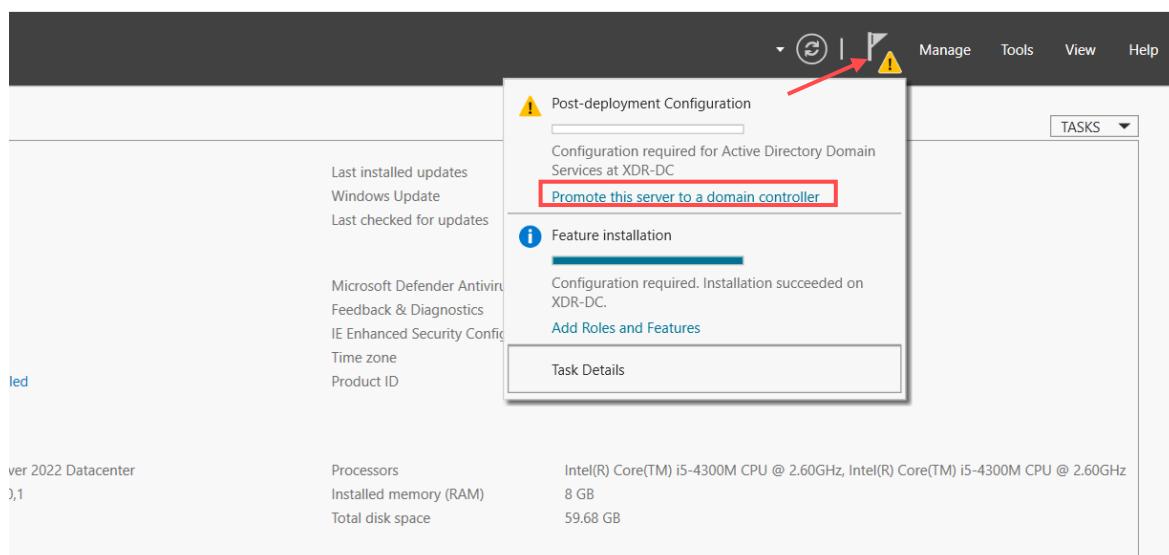
انقر فوق التالي ثلاث مرات لـ **server roles**. حدد مربع خدمات مجال **Services box** > **Add Features** انقر على التالي ثلاث مرات للتأكد.

# Extended Detection and Response



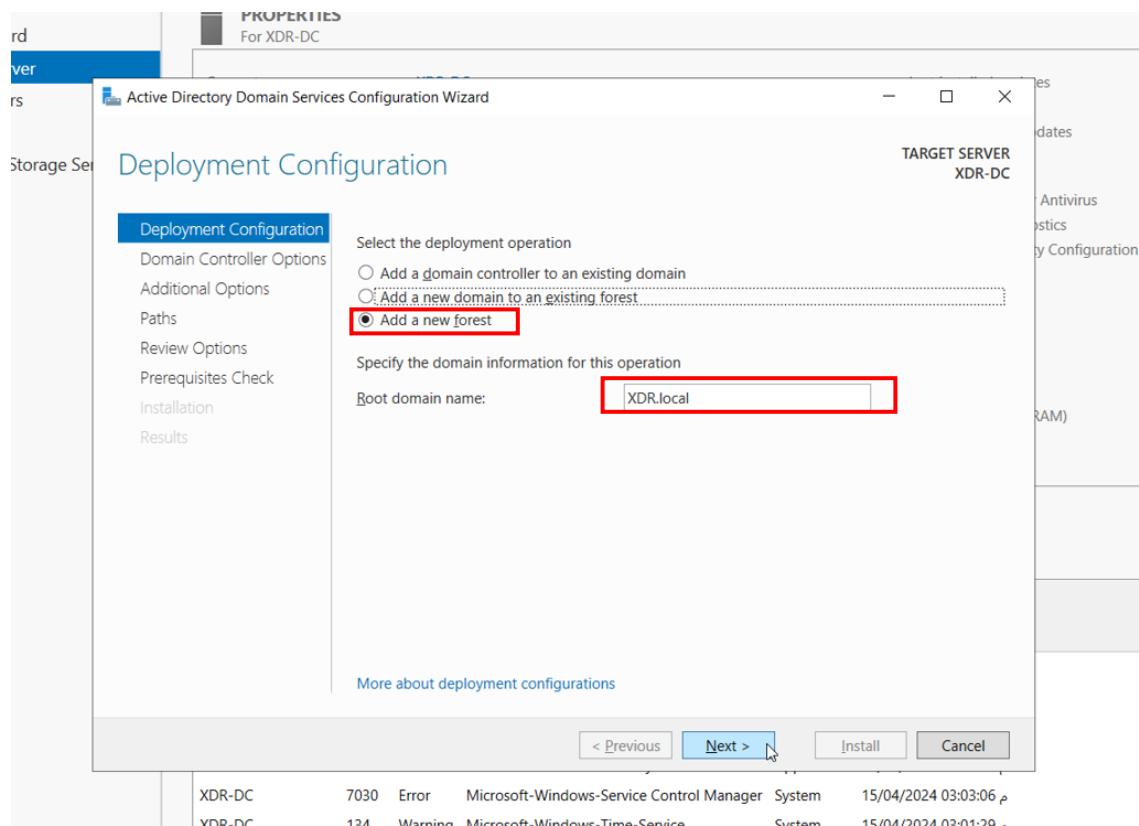
الشكل رقم (١)

بعد التثبيت، انقر فوق مركز الإشعارات الذي يتباهى بشكل تبيه **.promote this server**



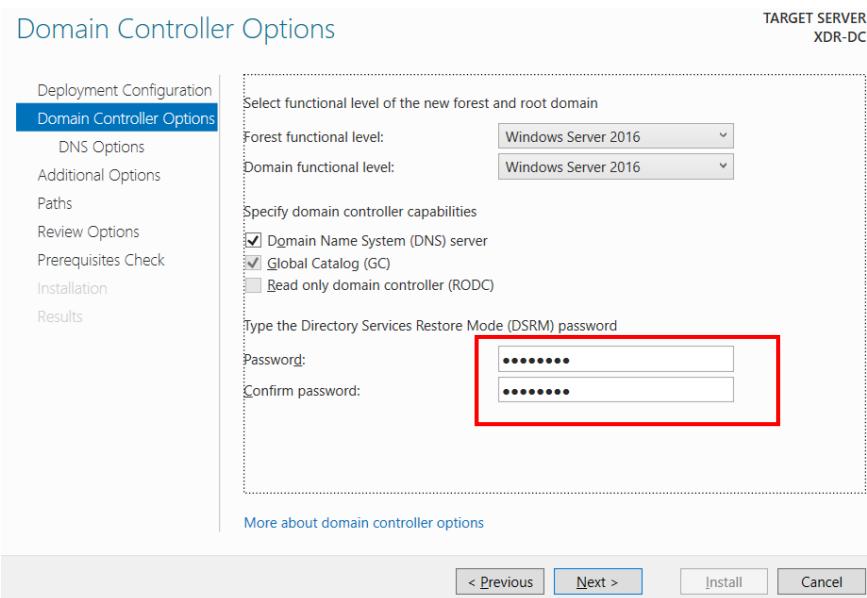
الشكل رقم (٢)

حدد المربع الثالث وحدد اسمًا لوحدة تحكم المجال الخاصة بنا وانقر فوق "التالي".



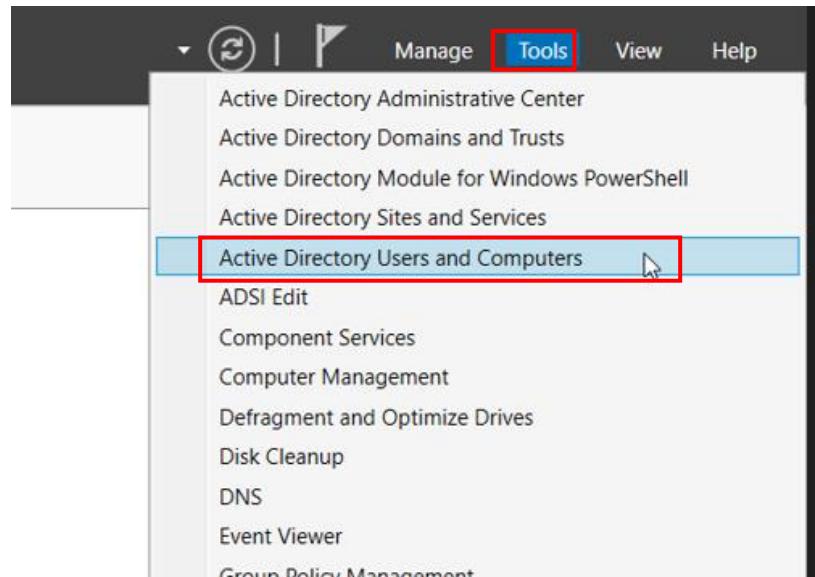
الشكل رقم (١)

أدخل كلمة مرور DSRM الخاصة بنا وسأضعها P@\$\$w0rd وحدد التالي . بعد اكتمال كافة عمليات التحقق من المتطلبات الأساسية، انقر فوق "تثبيت".



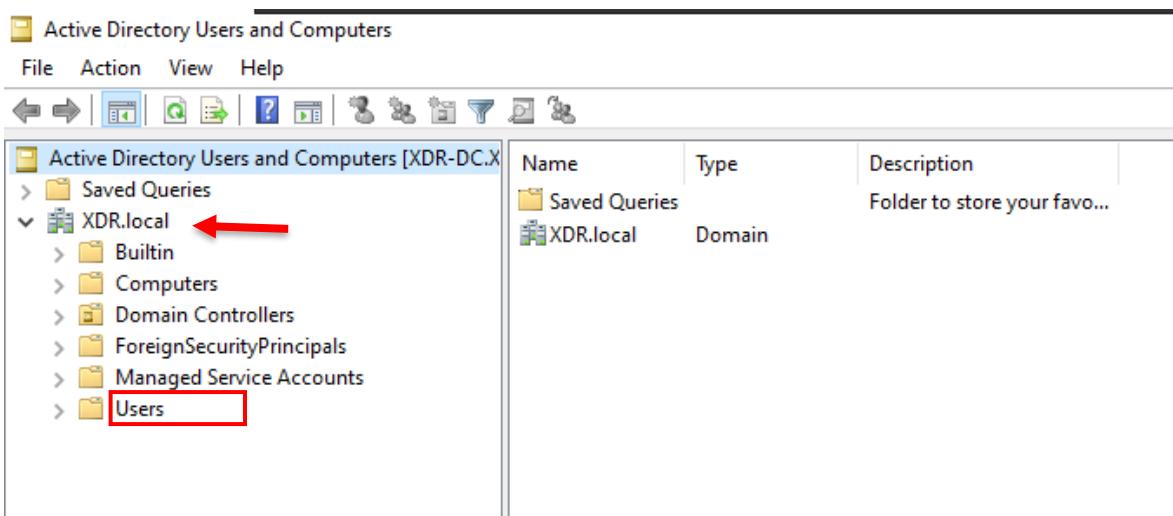
الشكل رقم ()

بعد التثبيت، ستحتاج إلى إعادة تشغيل الخادم لتطبيق كافة التغييرات. بعد إعادة التشغيل، انقر فوق > Active Directory Users and Computers



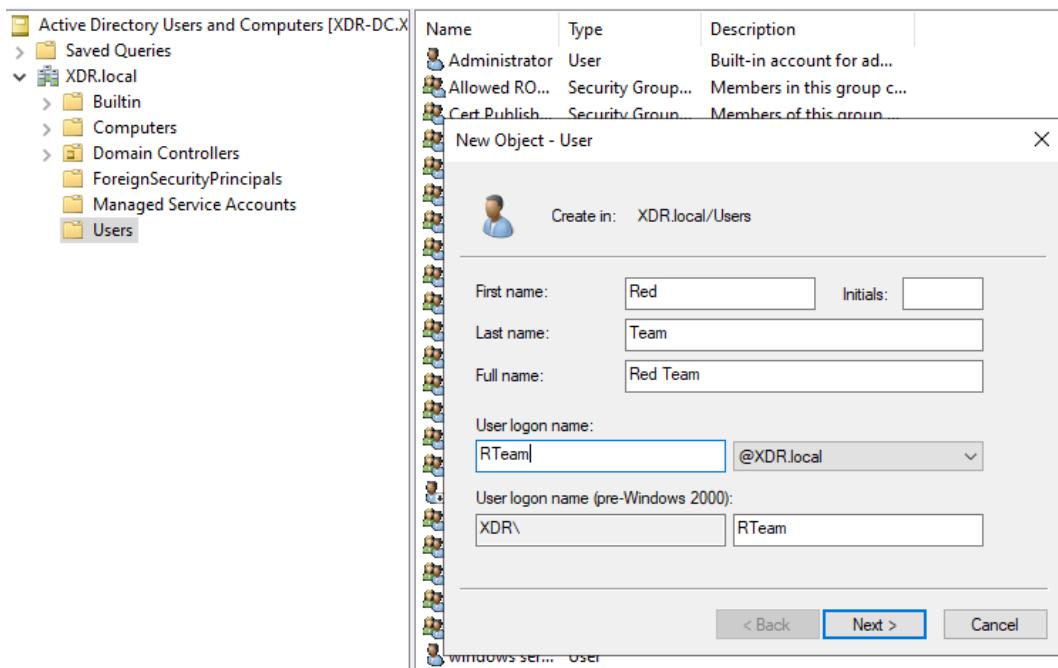
الشكل رقم ()

قم بالتوسيع **domain** وحدد **Users folder**، وانقر بزر الماوس الأيمن واختر **User New > User** لإعداد اسم مستخدم.



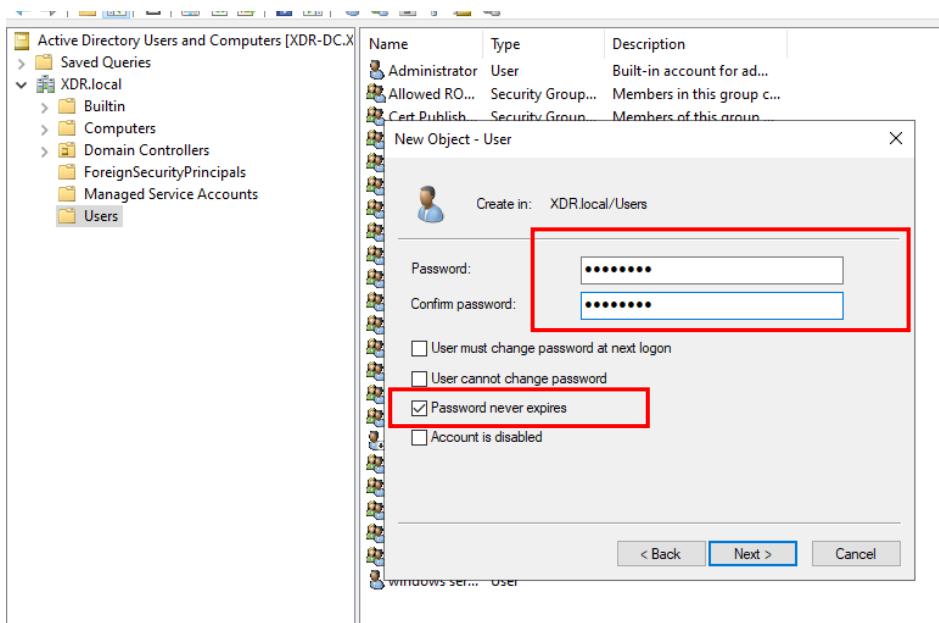
الشكل رقم ()

أنشئ اسم مستخدم



الشكل رقم ()

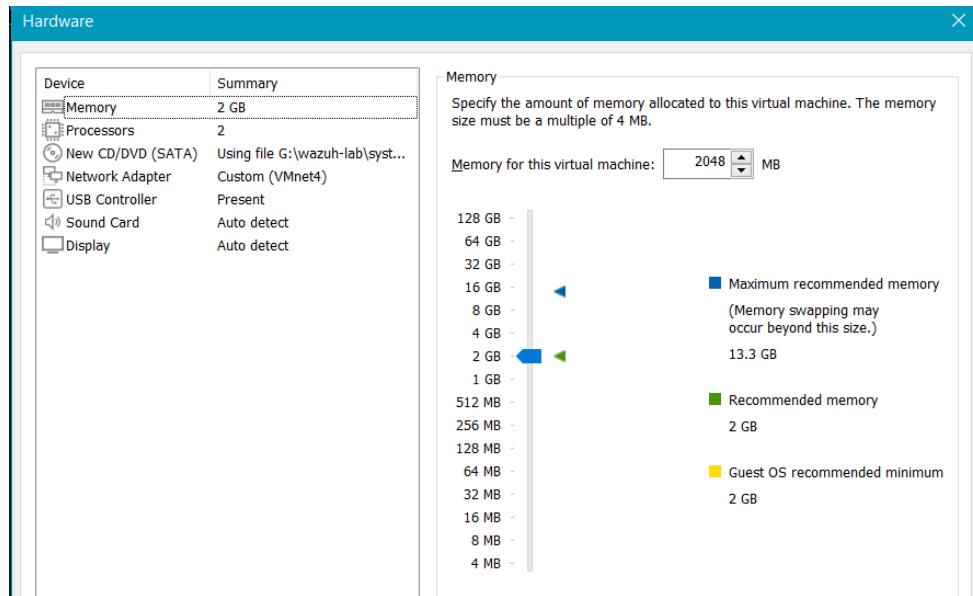
ثم أنشئ كلمة مرور، وحدد المربع "لا تنتهي صلاحية كلمة المرور مطلقاً" وانقر على **next** لقد نجحنا في إنشاء حساب مستخدم على الخادم الخاص بنا. يتعين علينا الآن إعداد جهاز عميل **Window** الخاص بنا وضمه إلى وحدة تحكم المجال الخاصة بنا.



الشكل رقم ()

## ٥.٦. تثبيت عميل Windows

نقوم بفك ضغط الملف iOS وفتحه في البيئة كما تعاملنا مع الأنظمة السابقة ولكن سنقوم بوضع تخصيص customize، تأكّد من تحديد موارد الأجهزة الازمة لهذا الجهاز الافتراضي. ثم انقر فوق "إغلاق" وقم بتشغيل ونبأ بتكونين النظام virtual machine

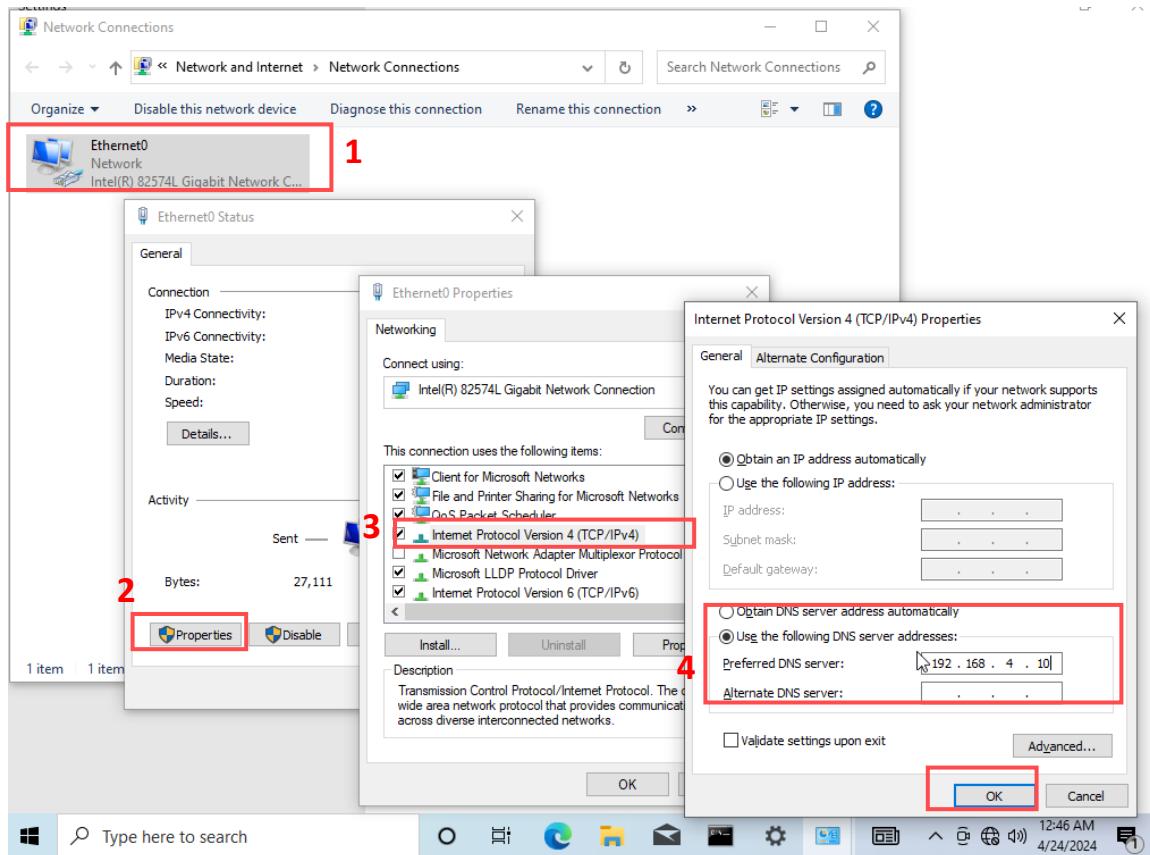


الشكل رقم ()

بعد التثبيت، انتقل إلى cmd وتحقق من إعدادات IP للتأكد من وجود الخادم والعميل على نفس الشبكة الفرعية. انتقل إلى إعدادات الشبكة والإنترنت.

الشكل رقم ()

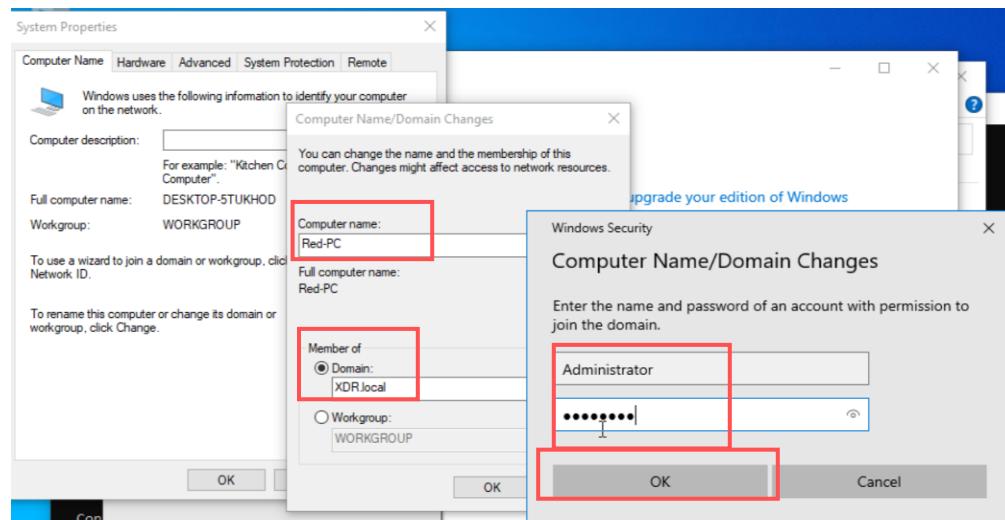
ضمن حالة الشبكة، انقر فوق **change adapter options > Ethernet0 > > Properties > DNS TCP/IPv4 > Use the following IP** . هنا على العميل نقوم بإدخال عنوان IP الخاص بالخادم. وانقر على "موافق" لتطبيق الإعدادات.



الشكل رقم ()

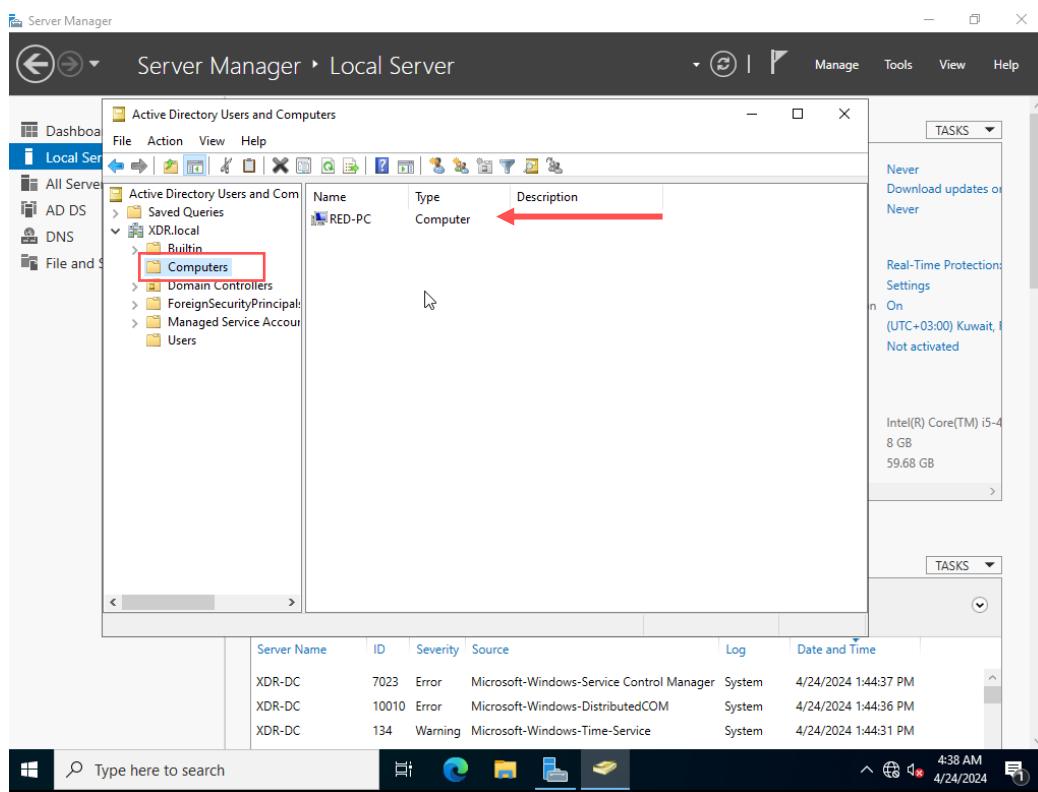
بعد ذلك، من هذا الكمبيوتر حدد الخصائص. ضمن اسم الكمبيوتر، انقر فوق تغيير الإعدادات. ضمن خصائص النظام، اختر **change > computer name** وحدد المربع **Domain** وأدخل اسم المجال الخاص بالخادم. انقر فوق **OK**. التالي هو إدخال بيانات اعتماد المسؤول لإعادة تشغيل الجهاز.

## Extended Detection and Response



الشكل رقم ()

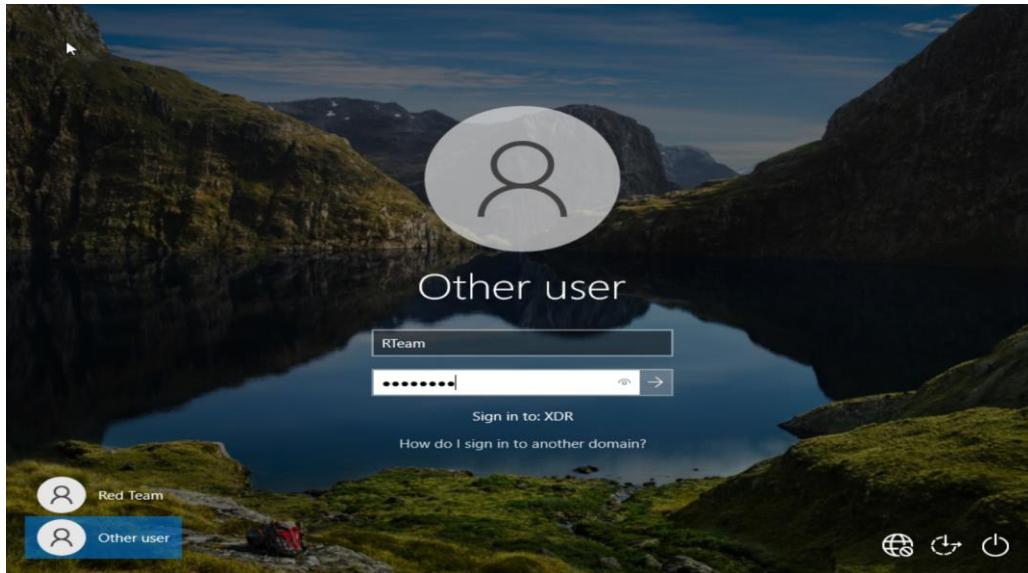
بالنسبة لـ PoC ، يمكننا تحديد جهاز الكمبيوتر العميل (Red-PC) الذي تم اكتشافه في خادمنا ، وهو ما يعني في الأساس أننا نجحنا في ربط جهاز العميل الخاص بنا بالخادم.



الشكل رقم ()

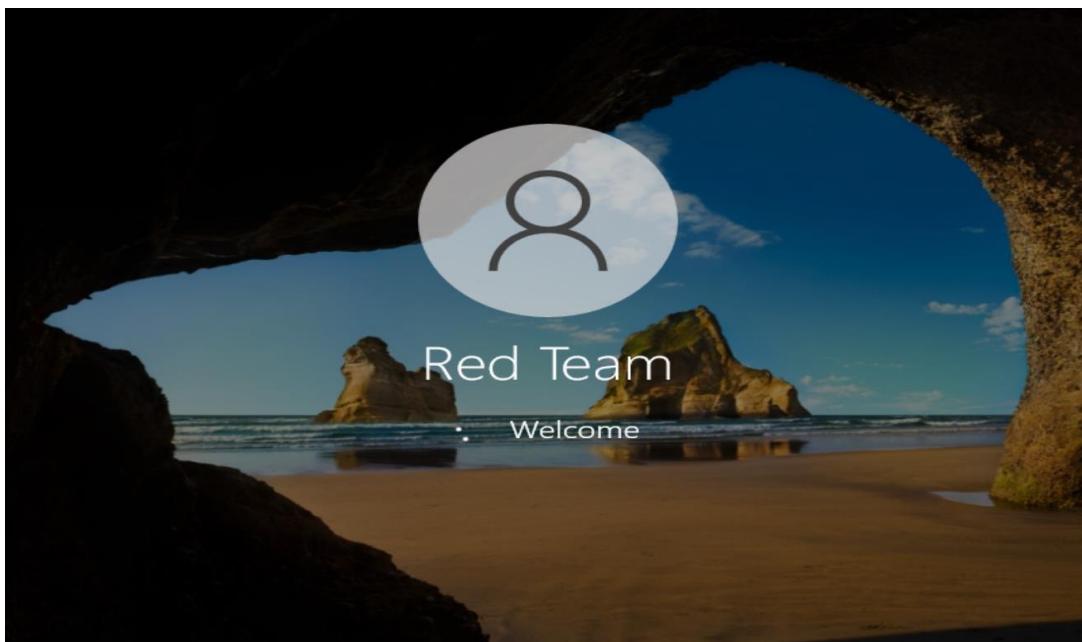
وأخيراً، قم بتسجيل الدخول إلى جهاز العميل عن طريق إدخال بيانات اعتماد المستخدم (RTeam) وكلمة المرور

P@\$\$w0rd



الشكل رقم ()

تم بنجاح الدخول

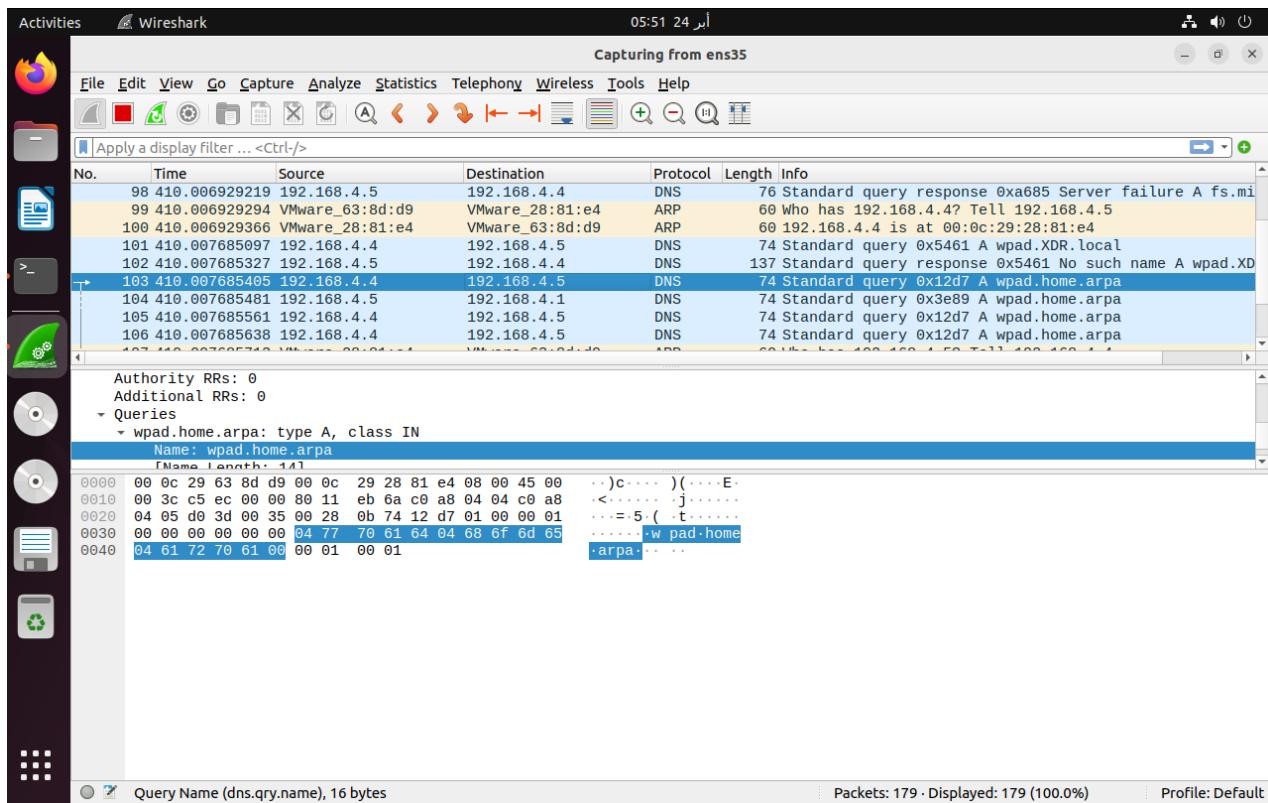


الشكل رقم ()

الآن، نقوم بالتبديل إلى جهاز المراقبة الافتراضي monitoring vm، وفتح الوحدة الطرفية، ثم قم بتشغيل wireshark انقر نقرًا مزدوجًا فوق واجهة المراقبة (ens35) لانتظار حركة المرور من بيئة ADDS العنوان

192.168.4.5

## Extended Detection and Response



(الشكل رقم )

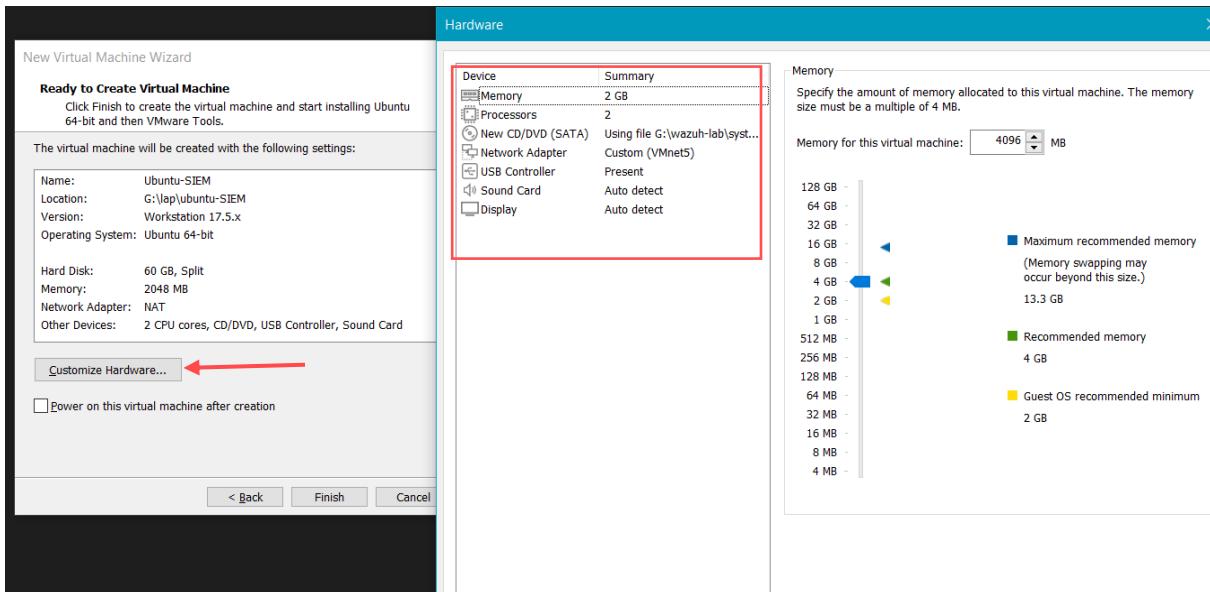
### ٥.٢.٧. تثبيت نظام معلومات الأمان وإدارة الأحداث (SIEM)

سنقوم بهذه المرحلة بإعداد نظام معلومات الأمان وإدارة الأحداث (SIEM) الخاص بنا لمراقبة الأحداث القوية لبيئة Active Directory Domain Services (AD DS) ولكن هذا ليس كل شيء، فنحن نعمل على زيادة الجهد من خلال تكوين قواعد جدار الحماية للتحكم في حركة المرور الواردة والصادرة.

#### • أولاً: سنقوم بإعداد نظام Kali كمضيف لل SIEM — Wazuh

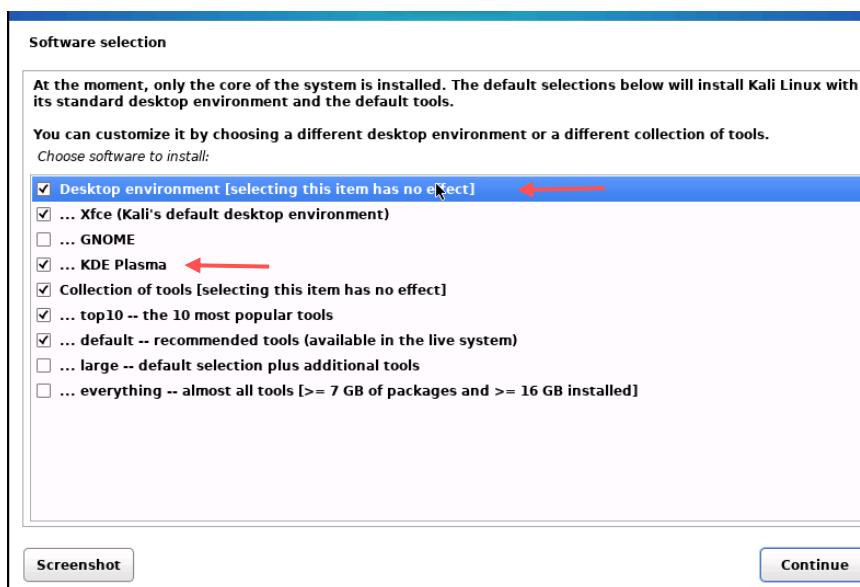
نقوم بفك ضغط الملف **ios** وفتحه في البيئة كما تعاملنا مع الأنظمة السابقة ولكن سنقوم بوضع تخصيص **customize**، تأكد من تحديد موارد الأجهزة اللازمة لهذا الجهاز الافتراضي. ثم انقر فوق "إغلاق" وقم بتشغيل **virtual machine** ونبدأ بتكوين النظام

## Extended Detection and Response



الشكل رقم ()

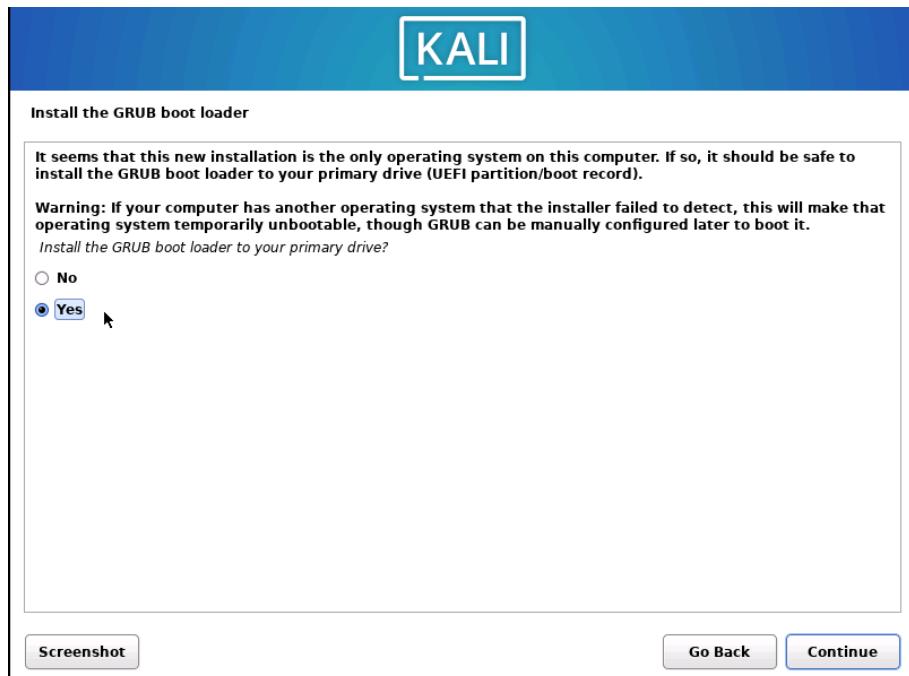
بعد التشغيل، من ضمن عمليات التثبيت والتكوين حدد الخيارات المحدد عليها في الصورة



الشكل رقم ()

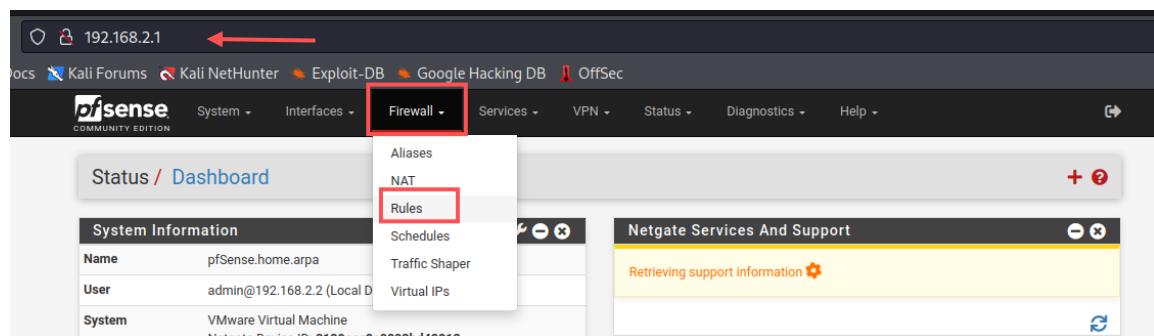
ثم اختر yes لتنصيب أداة تحميل التمهيد.

## Extended Detection and Response



الشكل رقم ()

بعد عملية تسجيل الدخول ننتقل الآن إلى جهاز الهجوم **Attack Machine** وقم بتسجيل الدخول إلى جدار **pfSense** الحماية في القائمة العلوية، انقر فوق جدار الحماية > القواعد. انقر على **SIEM** وحدد إضافة لإضافة قاعدة جديدة.



الشكل رقم ()

## Extended Detection and Response

Firewall / Rules / SIEM

Floating WAN ATTACKMACHINE UBTNU ACTIVEDIRECTORYDS SIEM SPANPORT

Rules (Drag to Change Order)

No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Add Add Delete Toggle Copy Save Separator

الشكل رقم ()

تأكد من السماح بالاتصال واختيار أي لخيارات البروتوكول وحفظ الإعدادات وتطبيقها.

Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled:  Disable this rule  
Set this option to disable this rule without removing it from the list.

Interface: SIEM  
Choose the interface from which packets must come to match this rule.

Address Family: IPv4  
Select the Internet Protocol version this rule applies to.

Protocol: Any  
Choose which IP protocol this rule should match.

Source

Source: Any  
Source Address: /

Destination

Destination: Any  
Destination Address: /

Extra Options

Log:  Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

الشكل رقم ()

- ثانياً: الآن يجب أن يكون لديك إمكانية الوصول إلى الإنترنت. حان الوقت الآن لتنزيل وتنصيب Wazuh System Wazuh في نظام ubuntu

## Extended Detection and Response



الشكل رقم ()

قم بتشغيل الجهاز وقم بتنزيل (Curl) .sudo apt install curl

```
ubuntu@ubuntu-virtual-machine:~$ sudo apt install curl ←
[sudo] password for ubuntu:
Sorry, try again.
[sudo] password for ubuntu:
Sorry, try again.
[sudo] password for ubuntu:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libcurl4
The following NEW packages will be installed:
  curl
The following packages will be upgraded:
  libcurl4
1 upgraded, 1 newly installed, 0 to remove and 278 not upgraded.
Need to get 484 kB of archives.
After this operation, 454 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ye.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libcurl4 amd64 7.81.0-1ubuntu1.1
6 [290 kB]
```

الشكل رقم ()

تاليا ،لقد قمنا بتنزيل وتنزيل **wazuh** باستخدام الأوامر التالية. يبسط هذا البرنامج النصي عملية التثبيت ، ويرشدك خلال إعداد **Wazuh** دون عناء .

## Extended Detection and Response

```
ubuntu@ubuntu-virtual-machine:~$ curl -s0 https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
26/04/2024 00:35:06 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.3
26/04/2024 00:35:07 INFO: Verbose logging redirected to /var/log/wazuh-install.log
26/04/2024 00:35:25 INFO: --- Dependencies ---
26/04/2024 00:35:25 INFO: Installing gawk.
26/04/2024 00:36:06 INFO: Wazuh web interface port will be 443.
26/04/2024 00:36:20 INFO: --- Dependencies ---
26/04/2024 00:36:20 INFO: Installing apt-transport-https.
26/04/2024 00:36:50 INFO: Wazuh repository added.
26/04/2024 00:36:50 INFO: --- Configuration files ---
26/04/2024 00:36:50 INFO: Generating configuration files.
26/04/2024 00:36:59 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
26/04/2024 00:37:00 INFO: --- Wazuh indexer ---
26/04/2024 00:37:00 INFO: Starting Wazuh indexer installation.
26/04/2024 02:21:32 INFO: Wazuh indexer installation finished.
26/04/2024 02:21:33 INFO: Wazuh indexer post-install configuration finished.
26/04/2024 02:21:33 INFO: Starting service wazuh-indexer.
26/04/2024 02:22:19 INFO: wazuh-indexer service started.
26/04/2024 02:22:19 INFO: Initializing Wazuh indexer cluster security settings.
26/04/2024 02:22:31 INFO: Wazuh indexer cluster initialized.
26/04/2024 02:22:31 INFO: --- Wazuh server ---
26/04/2024 02:22:31 INFO: Starting the Wazuh manager installation.
```

الشكل رقم ()

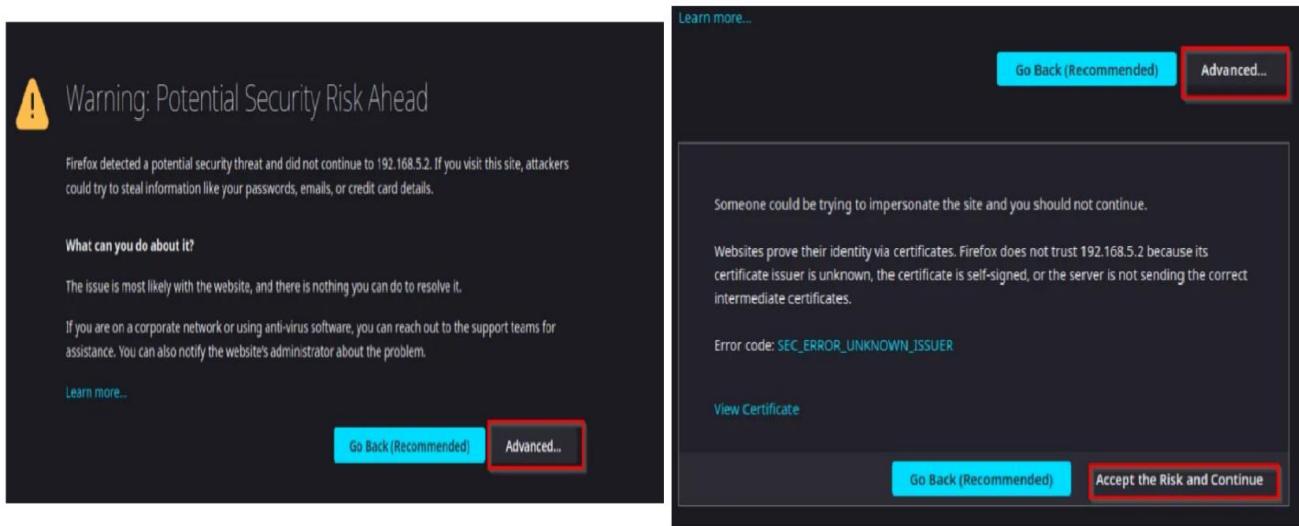
بعد التثبيت، يجب أن يكون لديك اسم المستخدم وكلمة المرور الخاصة بك للوصول إلى Wazuh.

```
26/04/2024 02:28:53 INFO: filebeat service started.
26/04/2024 02:28:53 INFO: --- Wazuh dashboard ---
26/04/2024 02:28:53 INFO: Starting Wazuh dashboard installation.
26/04/2024 02:32:16 INFO: Wazuh dashboard installation finished.
26/04/2024 02:32:16 INFO: Wazuh dashboard post-install configuration finished.
26/04/2024 02:32:16 INFO: Starting service wazuh-dashboard.
26/04/2024 02:32:18 INFO: wazuh-dashboard service started.
26/04/2024 02:33:21 INFO: Initializing Wazuh dashboard web application.
26/04/2024 02:33:23 INFO: Wazuh dashboard web application initialized.
26/04/2024 02:33:23 INFO: --- Summary ---
26/04/2024 02:33:23 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
  User: admin
  Password: REDACTED
26/04/2024 02:33:23 INFO: --- Dependencies ---
26/04/2024 02:33:23 INFO: Removing gawk.
26/04/2024 02:33:23 ERROR: Cannot remove dependency: gawk.
```

الشكل رقم ()

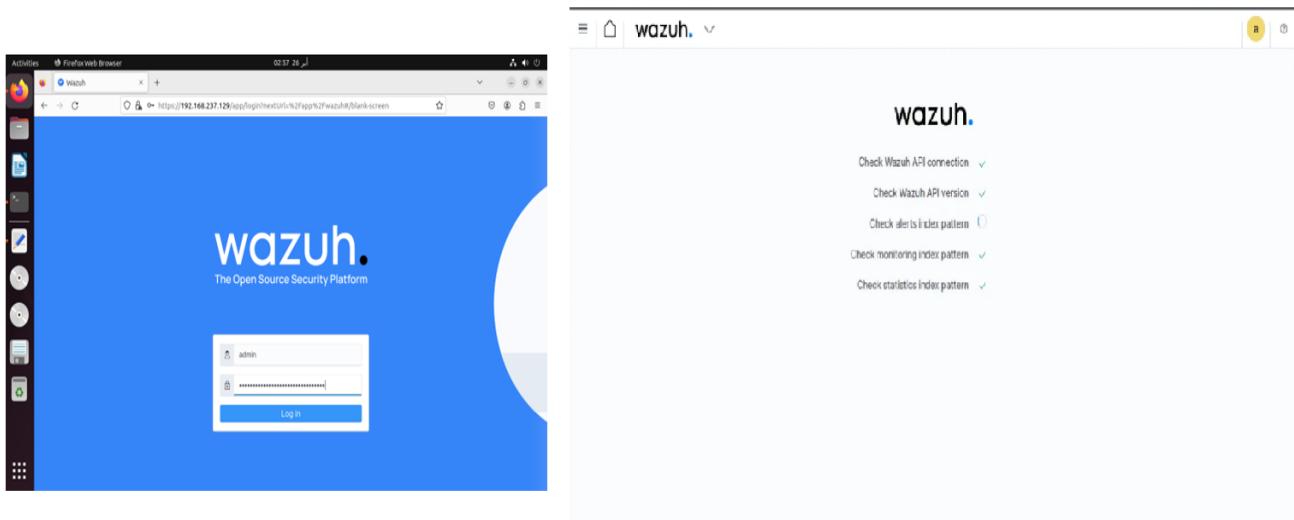
قم بتشغيل المتصفح الخاص بك وأدخل عنوان IP لنظام التشغيل Debian الخاص بك واضغط على Enter. سيتم الترحيب بك من خلال شاشة تحذير. حدد متقدم وقبول المخاطرة للمتابعة.

## Extended Detection and Response



الشكل رقم (١)

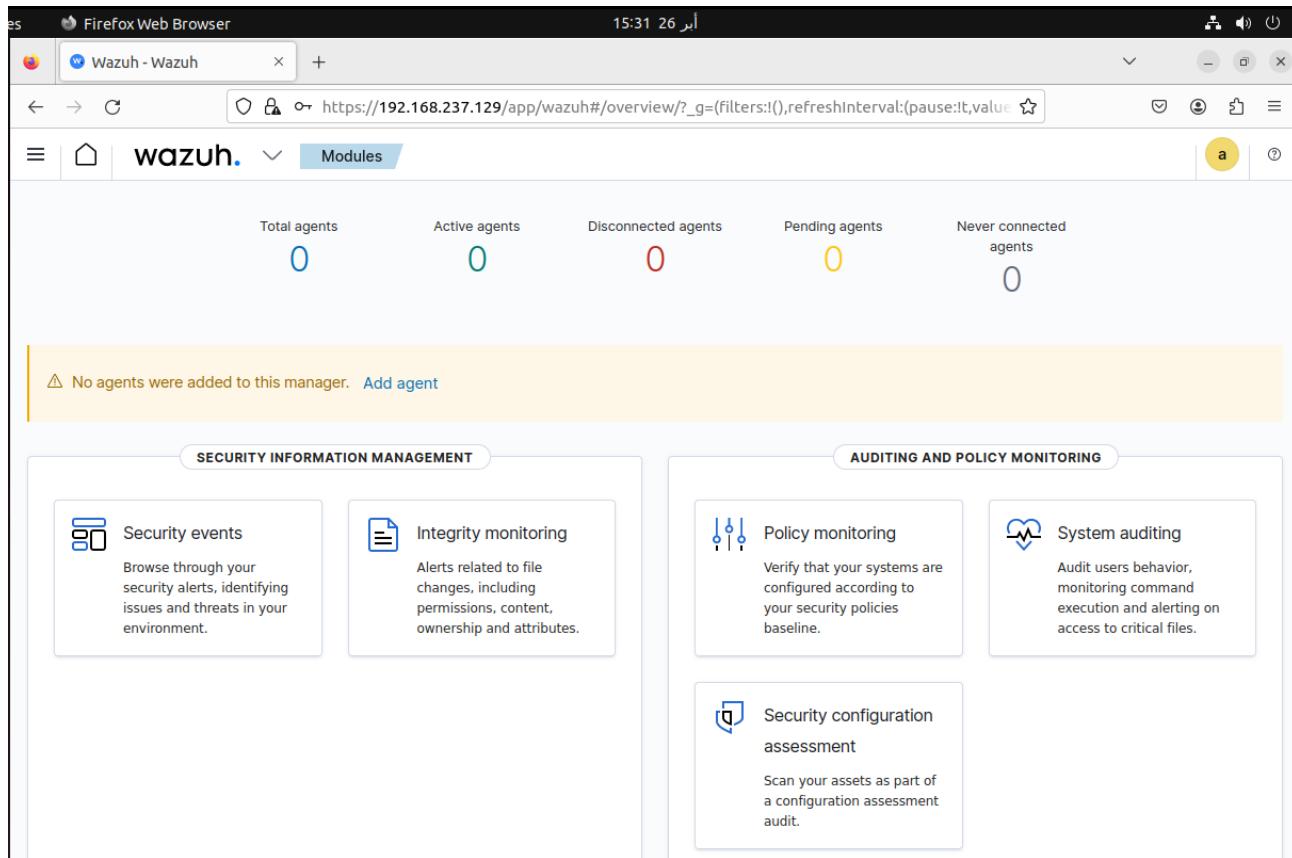
الآن، قم بتسجيل الدخول باستخدام اسم المستخدم وكلمة المرور الافتراضيين لـ Wazuh وانتظر حتى يتحقق من جميع الخدمات المتاحة.



الشكل رقم (٢)

## Extended Detection and Response

بعد التحقق، يجب أن تكون هذه هي واجهة لوحة تحكم.. Wazuh.



15:31 26 ابر

Wazuh - Wazuh

https://192.168.237.129/app/wazuh#/overview/?\_g=(filters:(),refreshInterval:(pause:1,value

wazuh. Modules

Total agents: 0 Active agents: 0 Disconnected agents: 0 Pending agents: 0 Never connected agents: 0

No agents were added to this manager. Add agent

SECURITY INFORMATION MANAGEMENT

- Security events: Browse through your security alerts, identifying issues and threats in your environment.
- Integrity monitoring: Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

- Policy monitoring: Verify that your systems are configured according to your security policies baseline.
- System auditing: Audit users behavior, monitoring command execution and alerting on access to critical files.
- Security configuration assessment: Scan your assets as part of a configuration assessment audit.

الشكل رقم ()

في هذه الخطوة سنقوم بـتغيير كلمة المرور **dashboard wazuh** من خلال الامر

```
curl -so wazuh-passwords-tool. sh https://packages.wazuh.com/4.7/wazuh-passwords-tool.sh
```

```
$ curl -so wazuh-passwords-tool. sh https://packages.wazuh.com/4.7/wazuh-passwords-tool.sh
```

الشكل رقم ()

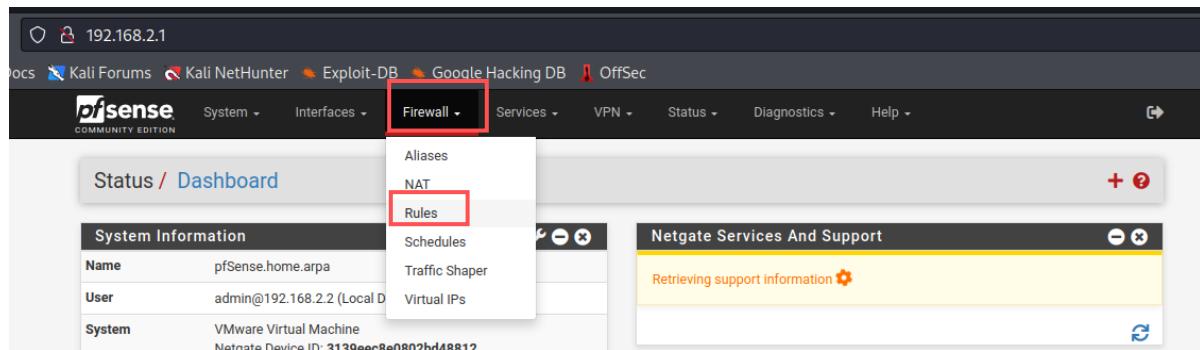
ثم بعد ذلك نقوم بإضافة حساب **admin** وكلمة المرور الجديدة

```
bash wazuh-passwords-tool.sh -u admin -p P@$$w0rd1
```

## Extended Detection and Response

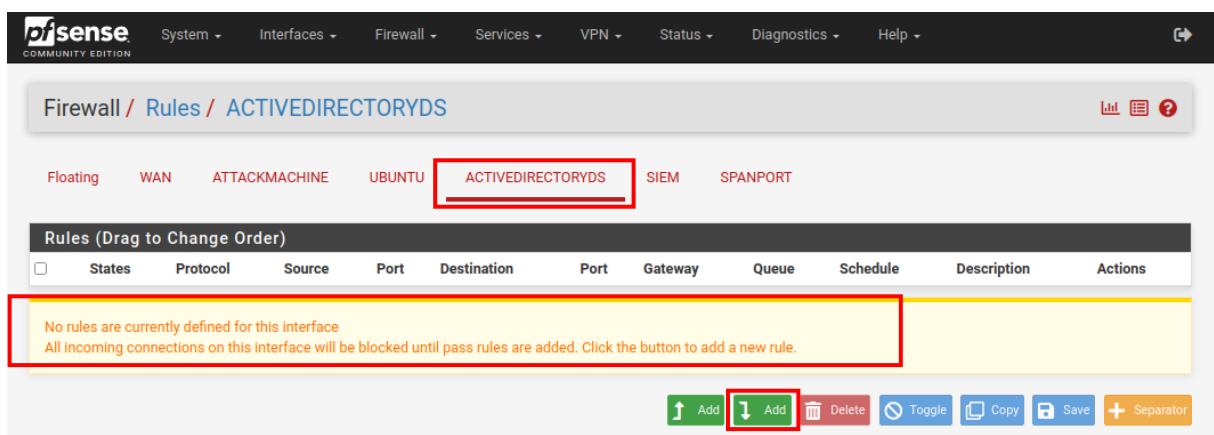
حاليا سنقوم بي **أحداث Forwarding** من خلال الدخول الى جدار الحماية **Windows** إلى **Wazuh**

**Firewall > Rules**، انتقل إلى جدار الحماية، وانقر فوق **Attack Machine** من جهاز **pfSense**



الشكل رقم ()

حدد واجهة **AD DS** وانقر فوق "Add" لإضافة قاعدة جديدة على هذه الواجهة.



الشكل رقم ()

نقوم بالسماح بالاتصال واختيار **Any** لخيارات البروتوكول وحفظ الإعدادات وتطبيقها.

# Extended Detection and Response

Firewall / Rules / Edit

**Edit Firewall Rule**

Action: Pass

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled:  Disable this rule  
Set this option to disable this rule without removing it from the list.

Interface: ACTIVE DIRECTORY DS  
Choose the interface from which packets must come to match this rule.

Address Family: IPv4  
Select the Internet Protocol version this rule applies to.

Protocol: Any

Choose which IP protocol this rule should match.

الشكل رقم (١)

على الخادم AD DS، انقر فوق تغيير خيارات adopter > Ethernet0 > DNS  
أضف عنوان IP الخاص بجدار الحماية باعتباره.

Network Connections

Ethernet0

Ethernet0 Status

Ethernet0 Properties

Internet Protocol Version 4 (TCP/IPv4) Properties

General

IP address: 192.168.4.10  
Subnet mask: 255.255.255.0  
Default gateway: 192.168.4.1

Advanced...

الشكل رقم (٢)

- ثالثاً: الان بعد الانتهاء من انشاء المعمل، سنقوم بعمل ping من جهاز AD وعكس أيضا مع الأنظمة الأخرى كذلك للتأكد من ان عملية الاتصال سليمة

## Extended Detection and Response

```
ubuntu@ubuntu-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.181.129 netmask 255.255.255.0 broadcast 192.168.181.255
        inet6 fe80::943f:2b12:357c:d870 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:6c:81:53 txqueuelen 1000 (Ethernet)
            RX packets 1785 bytes 1921334 (1.9 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1696 bytes 130595 (130.5 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens34: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.1 netmask 255.255.255.0 broadcast 192.168.2.255
        inet6 fe80::7db1:3a63:2c4b:9e0d prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:6c:81:5d txqueuelen 1000 (Ethernet)
            RX packets 40 bytes 4145 (4.1 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 104 bytes 12286 (12.2 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 3929 bytes 414085 (414.0 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 3929 bytes 414085 (414.0 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@ubuntu-virtual-machine:~$ ping 192.168.2.2 ←
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=128 time=0.755 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=128 time=0.794 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=128 time=1.75 ms
64 bytes from 192.168.2.2: icmp_seq=4 ttl=128 time=1.02 ms
64 bytes from 192.168.2.2: icmp_seq=5 ttl=128 time=2.58 ms
64 bytes from 192.168.2.2: icmp_seq=6 ttl=128 time=0.845 ms
64 bytes from 192.168.2.2: icmp_seq=7 ttl=128 time=0.714 ms
64 bytes from 192.168.2.2: icmp_seq=8 ttl=128 time=3.14 ms
```

(الشكل رقم ١)

ثم من جهاز windows server

```
C:\Users\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

(الشكل رقم ٢)

ثم سنقوم بإضافة جهاز windows 10 كمستخدم مع وضع عنوان له في

## Extended Detection and Response

```
Ethernet adapter Ethernet0:
  Connection-specific DNS Suffix . : localdomain
  Link-local IPv6 Address . . . . . : fe80::5912:1189:d37a:b30a%9
  IPv4 Address. . . . . : 192.168.2.3
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

C:\Users\RTeam>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=1ms TTL=128
Reply from 192.168.2.2: bytes=32 time=1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

(الشكل رقم ٤)

```
Ethernet adapter Ethernet1:
  Connection-specific DNS Suffix . : localdomain
  Link-local IPv6 Address . . . . . : fe80::fb:defb:6fc2:165d%25
  IPv4 Address. . . . . : 192.168.3.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

C:\Users\Administrator>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=1ms TTL=64
Reply from 192.168.3.2: bytes=32 time=1ms TTL=64
Reply from 192.168.3.2: bytes=32 time<1ms TTL=64
Reply from 192.168.3.2: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.3.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

(الشكل رقم ٥)

## Extended Detection and Response

```
(kali㉿kali)-[~]
└─$ ifconfig
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.3.2  netmask 255.255.255.0  broadcast 192.168.3.255
        inet6 fe80::147:79bd:804:c9f6  prefixlen 64  scopeid 0x20<link>
          ether 00:0c:29:be:4f:a6  txqueuelen 1000  (Ethernet)
            RX packets 3  bytes 746 (746.0 B)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 15  bytes 1870 (1.8 KiB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
      lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
          inet6 ::1  prefixlen 128  scopeid 0x10<host>
            loop  txqueuelen 1000  (Local Loopback)
            RX packets 4  bytes 240 (240.0 B)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 4  bytes 240 (240.0 B)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

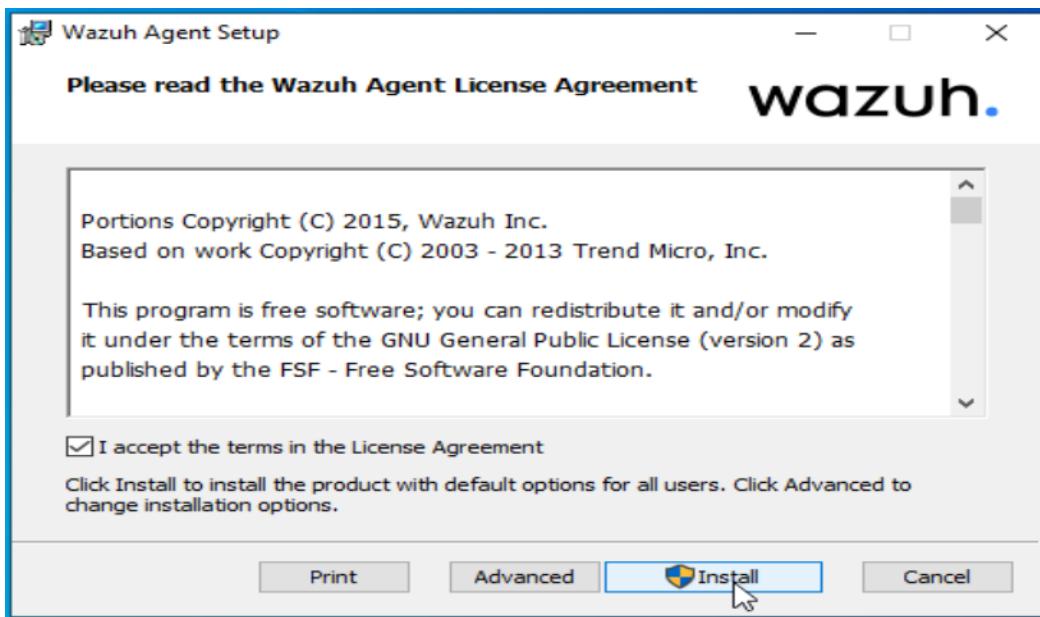
(kali㉿kali)-[~]
└─$ ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
64 bytes from 192.168.3.1: icmp_seq=1 ttl=128 time=0.840 ms
64 bytes from 192.168.3.1: icmp_seq=2 ttl=128 time=0.724 ms
64 bytes from 192.168.3.1: icmp_seq=3 ttl=128 time=0.680 ms
64 bytes from 192.168.3.1: icmp_seq=4 ttl=128 time=0.687 ms
^X@sc64 bytes from 192.168.3.1: icmp_seq=5 ttl=128 time=0.732 ms
64 bytes from 192.168.3.1: icmp_seq=6 ttl=128 time=0.644 ms
^C
— 192.168.3.1 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5101ms
rtt min/avg/max/mdev = 0.644/0.717/0.840/0.061 ms
```

(الشكل رقم ٤)

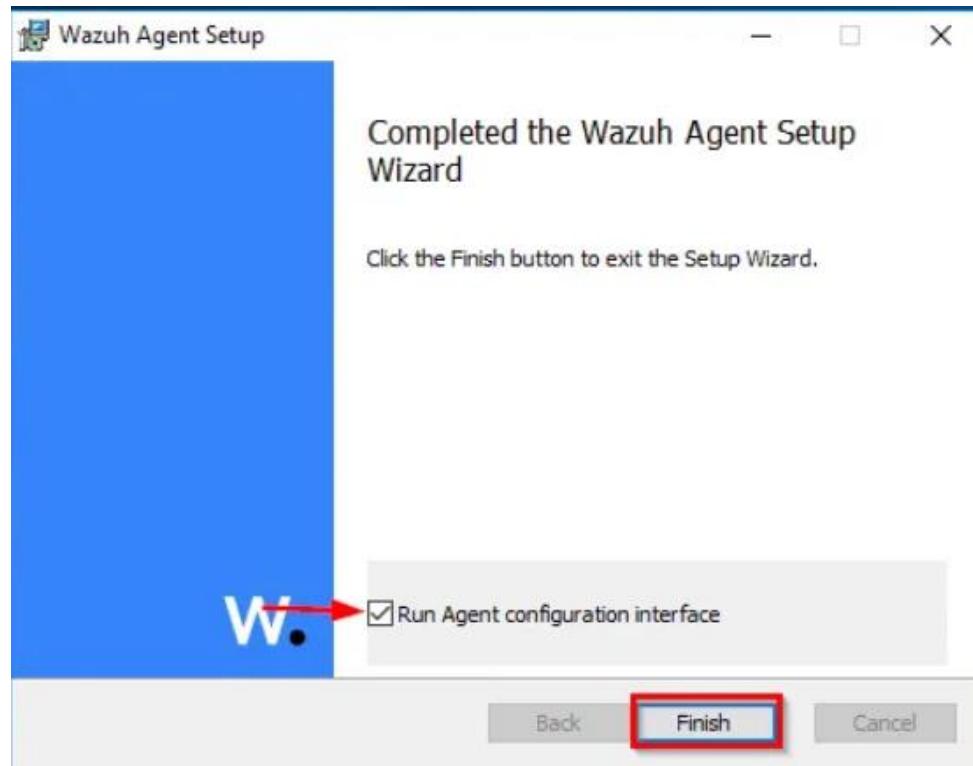
ثم سنقوم بتنزيل **Wazuh-agent** على **Edge** قم بتشغيل متصفح الخاص بك وانتقل إلى <https://packages.wazuh.com/4.x/windows/wazuh-agent-4.5.1-1.msi> وكيل **wazuh** لنظام التشغيل **Windows** وتشغيله.

حدد مربع اتفاقية الترخيص **install** > حدد مربع وكيل التشغيل وانقر فوق "إنهاء".

## Extended Detection and Response



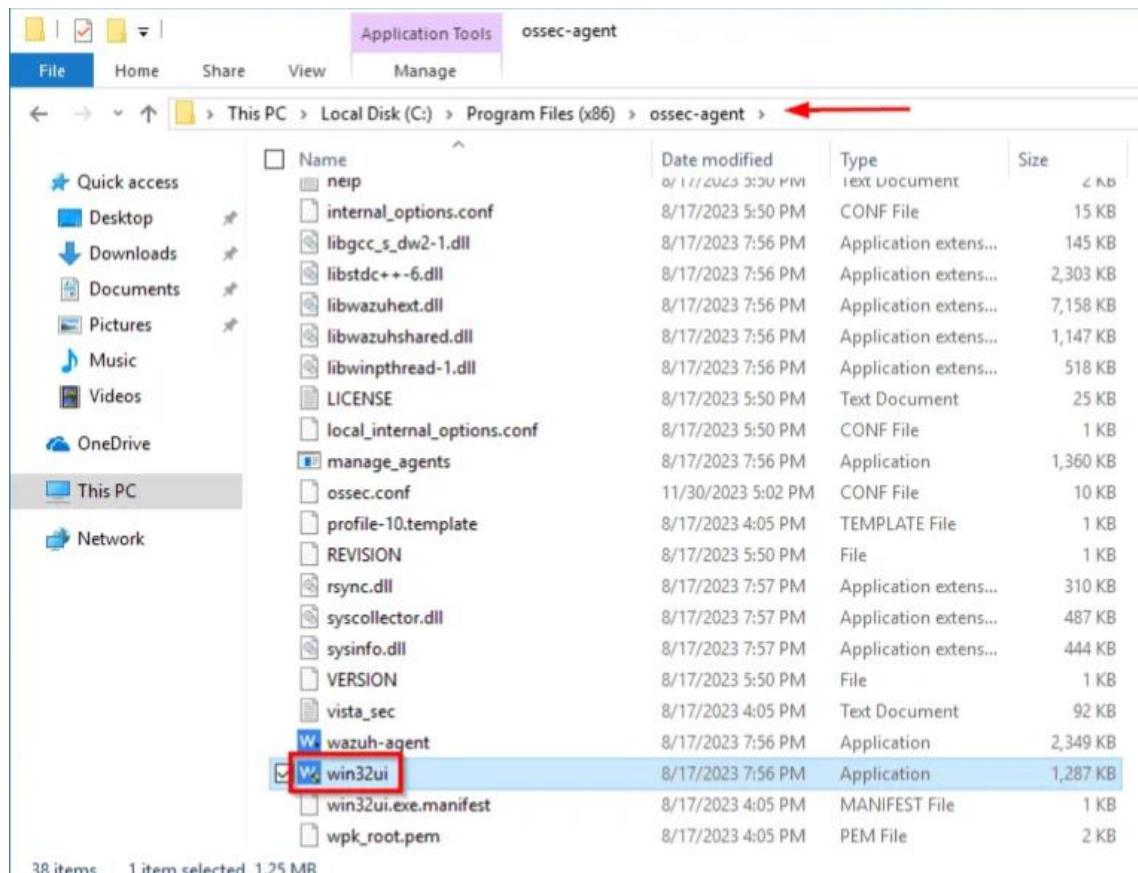
(الشكل رقم ٤)



(الشكل رقم ٥)

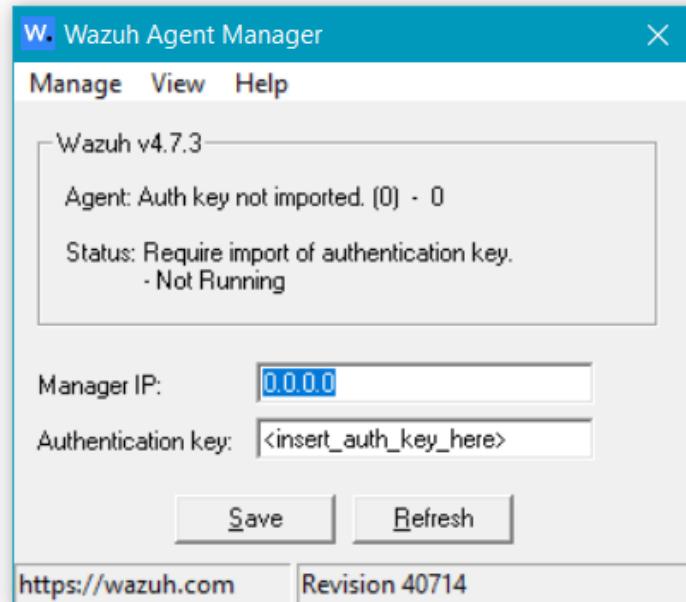
إذا لم تظهر واجهة وكيل wazuh ، فانتقل إلى القرص المحلي وانقر نقرًا مزدوجًا على win32ui.exe لبدء التشغيل.

## Extended Detection and Response



الشكل رقم ()

أدخل عنوان IP الخاص بخادم Wazuh وندعو الله أن تحصل على مفتاح المصادقة. إذا لم يكن الأمر كذلك، أعد تشغيل الخدمة وقم بالتحديث.



(الشكل رقم )

تهانينا، على خادم Wazuh الخاص بنا، يجب أن نرى وكيلًا

## الفصل السادس: النتائج والمناقشة

---

## الفصل السابع: الاستنتاجات والتوصيات

---

## المراجع

---

### 1. (Scrum. Últim accés, 2022)

2. [1] SIEM. Last access: 2023-10-10 url: <https://wazuh.com/platform/siem/>
3. [2] Wazuh. Wazuh. Last access: 2023-11-9. url: <https://wazuh.com/>.
4. [3] DDOS. Last access: 2023-11-12. url: [https://en.wikipedia.org/wiki/Denial-of-service\\_attack](https://en.wikipedia.org/wiki/Denial-of-service_attack)
5. [4] MITRE. Last access: 2023-10-10. url: <https://attack.mitre.org/>
- 6.
7. [5] YARA. Last access: 2024-1-3. url: <https://netenrich.com/glossary/yara-rules>
- 8.
9. [6] VirusTotal. Last access: 2024-1-3. url: <https://infosec-jobs.com/insights/virustotal-explained/>
- 10.
11. [7] Scrum. Scrum. Last access: 2022-10-7. url: <https://www.scrum.org/learning-series/what-is-scrum>
12. [8] What is the Agile methodology. Last access: 2023-10-9 url: <https://www.atlassian.com/agile>
13. [9] XDR. Last access: 2023-10-10. url: <https://wazuh.com/platform/xdr/>
14. [10] ISP. Last access: 2024-1-10 .url: <https://www.ibm.com/topics/intrusion-prevention-system>
15. [11] IDS. Last access: 2024-1-10 .url <https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/>
16. [12] YARA. Last access: 2024-1-10 .url <https://yara.readthedocs.io/en/stable/>

الملاحق

---