JUN 6, 2024

Extended Detection & Response

by
Hussein Alselwi

Republic of Yemen
Emirates International University
Engineering and IT Faculty
Dep.Information Security

الجمهورية اليمنية
الجامعة الإماراتية الدولية
كلية الهندسة وتكنولوجيا المعلومات
قسم أمن المعلومات

Extended Detection and Response (XDR)

الكشف والاستجابة الموسعة

إعداد الطلاب:

حسين طربوش الصلوي	2020020423
عبدالجليل أمين الطائفي	2020020809
معاذ سمير الوصـــابي	2020021360
حمزه سمير الوصـــابي	2020021361
احمد شـــايف الصلـــوي	2019070082
غيدان منصور الخضمي	2020020769

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 دائما 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 يتعين على 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 الحجم، 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 خصيصا للشركات الصغيرة والمتوسطة التي تضم ما يصل إلى ٢٥٠ موظفا، 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 التوسع في استخدام الموارد مفتوحة المصدر لمعالجة تحديات الأمن السيبراني الفريدة التي تواجهها الشركات الصغيرة والمتوسطة. يجمع النظام المقترح بين تقنيات تحليل البرامج الضارة المتقدمة وموجزات استخبارات التهديدات في الوقت الفعلي لتحديد وتحليل الأنشطة الضارة داخل شبكات الشركات الصغيرة والمتوسطة. من خلال استخدام اداة Wazuh ودمجها مع بعض أدوات الامن مفتوحة المصدر، يمكن للنظام اكتشاف وتصنيف البرامج الضارة والتهديدات الامنية بشكل فعال لتقييم 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 غالبا ما تغفل عنها التدابير الأمنية التقليدية. يمثل النظام المقترح حلا عمليا وقابلا للتطوير باستخدام اداة 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
حمزه سمير الوصابي	2020021361		2024-06-09
احمد شايف الصلوي	2019070082		2024-06-09
غيدان منصور الخضمي	2020020769		2024-06-09

شكر وتقدير

وأتقدم 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 تتزعزع 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 يشاركوا آراءهم 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 الإنترنت التي كانت بمثابة مراجع لا تقدر بثمن، مما أدى إلى إثراء عمق بحثنا.

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

أخيراً، نتوجه بالشكر العميق لكل مساهم، 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 حقا 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

تاريخ

لجنة الممتحنين

عنوان المشروع : .....

مشرف

م	الاسم	الموضع	التوقيع
1			

لجنة الممتحنين

م	الاسم	الموضع	التوقيع
1			
2			
3			
4			

رئيس القسم

د. جميل راشد

.....

جدول المحتويات

خلاصة II

تفويض III

شكر وتقدير IV

شهادة المشرف V

لجنة الممتحنين VI

جدول المحتويات ١

قائمة الأشكال ٢

قائمة الجداول ٣

قائمة الاختصارات ٤

الفصل الأول: مقدمة ٥

نظرة عامة ٥

بيان المشكلة ٦

أهداف وغاية المشروع ٨

نطاق المشروع والقيود والمخاطر ٨

نطاق المشروع: ٨

حدود المشروع: ٩

المخاطر ٩

منهجية المشروع ١٠

هيكل التقرير ١٠

الفصل الثاني: الخلفية ومراجعة الأدبيات ١٠

خلفية المشروع ١٠

مراجعة الأدبيات ..... **خطأ! الإشارة المرجعية غير معرّفة.**

الفصل الثالث: جمع وتحليل المتطلبات ٢٠

الفصل الرابع: تصميم ونمذجة المشروع ٢٤

الفصل الخامس: تنفيذ واختبار المشروع ٣٣

الفصل السادس: النتائج والمناقشة ٩٣

الفصل السابع: الاستنتاجات والتوصيات ٩٤

المراجع ٩٥
الملاحق ٩٦

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 الأمن السيبراني. أحد أسباب هذا الإشراف هو التقليل من مخاطر وتأثير الهجمات السيبرانية. غالبا ما يكون هناك اعتقاد خاطئ بأن مجرمي الإنترنت يلاحقون 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 الأمن السيبراني للشركات الصغيرة والمتوسطة هو أنه بسبب الموارد المالية والبشرية المحدودة، فإنها تكافح لمواكبة التقدم المستمر في هذا المجال سريع التطور. وكثيرا 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 ويصل الموظفون إلى أنظمة المنظمة عن بعد من منازلهم. وقد خلق هذا فرصا جديدة للجهات الفاعلة الخبيثة ولوحظت زيادة في الهجمات الإلكترونية بعد جائحة COVID-19. وجدت وكالة الاتحاد الأوروبي للأمن السيبراني، ENISA [٢]، أن تحديات الأمن 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 تهديداتها وتقييمات 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 عددا 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 المحللون صعوبة في مراقبة لوحات معلومات متعددة في وقت واحد وربط الأحداث من أجهزة الأمان المختلفة. علاوة على ذلك، تولد هذه الأجهزة كمية هائلة من الاحداث (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 الأمن يمكن أن تكون في كثير من الأحيان وظيفة بدوام جزئي لفرد واحد [٥]. هذا يجعلهم هدفا سهلا لمجرمي الإنترنت. لذلك، فإن النهج العملي للشركات الصغيرة والمتوسطة هو إدارة الأمن الموحدة. يسهل نظام SIEM ذلك من خلال الجمع الفعال للبيانات من مصادر السجل المتباينة في نظام واحد للتحليل في الوقت الفعلي [٦] يتم تسليمه 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 مترية الأخرى للشبكة [٧].

هناك فئتان عريضتان من حلول SIEM، التجارية والمفتوحة المصدر، مع فوائد وقيود متأصلة. حلول SIEM التجارية ناضجة تماما وتوفر تغطية كاملة على مستوى المؤسسة، وإن كان ذلك بتكاليف ترخيص ضخمة. على سبيل المثال، تبدأ التكلفة الإجمالية للملكية (TCO) لمدة ثلاث سنوات ل LogRhythm وSolarWinds LEM من 50,000 دولار ونفس الشيء بالنسبة ل 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 للتوسع إلى الأصول الأخرى للضحية، مثل الخوادم.

من خلال اختراق نقطة النهاية، يمكن للمهاجمين سرقة المعلومات الحساسة ونشر البرامج الضارة واختراق 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 الأمن السيبراني التي تواجهها الشركات الصغيرة والمتوسطة في الوقت الحاضر. ونظراً لمحدودية 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 تقريبًا 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 أضرارًا جسيمة لسمعة منظمة جديدة نسبيًا وتتسبب في خسارة الأصول والموظفين ورأس المال. ولجعل الوضع أسوأ، في حالة حدوث خرق أمني، يمكن أيضًا 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.

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

عدم وجود رؤية مركزية:

تعمل أدوات الأمان التقليدية بشكل مستقل وتفتقر 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 تمتد عبر أنظمة متعددة.

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

نقص قدرات ربط البيانات:

تفتقر أنظمة الأمان التقليدية إلى القدرات اللازمة 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 تقريبا بسبب التأخير، مما تسبب في خسائر كبيرة للمنظمة.

وقد يؤدي ذلك إلى تفاقم الأضرار الناجمة عن الهجوم ومنح المهاجمين مزيدا من الوقت للتصرف.

حجم تنبيه هائل:

يتطلب الاعتماد على التحليل التقليدي تدخلا يدويا مكثفا لأنه يستغرق وقتا طويلا 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 خطرا أمنيا).

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 تعقيدا وغالبا ما تتجاوز أنظمة الأمان التقليدية، لذلك تحتاج المؤسسات إلى طريقة لتحليل البيانات الأمنية بعدة 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 متنوعة، 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 الأمن السيبراني التي تواجهها الشركات الصغيرة والمتوسطة حيث سيتم اثبات ذلك بالاعتماد على **Wazuh** أداة العمل الفعلية، وهي ليست مجدية فحسب، بل فعالة ومفتوحة المصدر أيضًا وسهلة التنفيذ ويمكن تعديلها وفقًا لمتطلبات أي بيئة صغيرة او متوسطة الحجم ويهدف هذا المشروع لتقليل الوقت والجهد الذي يبذله مهندسو الأمن 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 التلقائي 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 المتطورة: تطوير آلية تسمح بتكامل البيانات وربطها بمصادر البيانات الخارجية وذكاء التهديدات باستخدام مجموعة متنوعة من طرق الكشف عن التهديدات مثل الكشف القائم على التوقيع والكشف القائم على السلوك وتكتيكات MITRE وقواعد YARA والمواقع الخارجية مثل Virus Total 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 تناسب احتياجات المؤسسات الصغيرة.
6. تنفيذ وظائف الإخطار الآلي بالحوادث الأمنية للموظفين المعنيين 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 بيئة افتراضية. وسيركز المشروع على ما يلي:

١. تصميم وإعداد بيئة افتراضية باستخدام Workstation Pro VMWare لمحاكاة البيئة الواقعية.

٢. انشر بيئة Active Directory Windows Server 2022، بما في ذلك أنظمة Win10 وUbuntu.

٣. تكوين **Wazuh** ونشره على جهاز افتراضي مركزي.

٤. 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 التنبيهات. يمكن النظر في القدرات المتقدمة مثل البحث الشامل عن التهديدات والطب الشرعي والاستجابة للحوادث من أجل التحسينات المستقبلية ولكنها لن تكون المحور الأساسي لهذا التكرار الأولي.

- محاكاة بيئة الأمان: نظرا 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 محتمل ممكنا ضمن الإطار الزمني للمشروع. ومع ذلك، سيأخذ تصميم النظام في الاعتبار قابلية التوسع 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 فأننا قد اضطررنا الى ترك بعض اهداف المشروع وقمنا بإعادة هيكلة المشروع والبدء من جديد، مما أدى ذلك الى 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 ينتج عنه الكثير من الإيجابيات الخاطئة.

مشاكل وأخطاء التكوين والكتابة الأكواد: 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 الية ***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 لإنهاء المشروع في الوقت المحدد. والا سوف نضطر الى الغائها.

منهجية المشروع

حالياً، هناك منهجيات عمل متعددة، لهذا المشروع، الخيار الذي يناسب هذا المشروع هو منهجية ***Agile*** وتحديدا *scrum* (1) هذه المنهجية متكررة ومتزايدة. يتم تحديد سلسلة من المهام القصيرة تسمى (قصص المستخدم)، والتي يمكن أن تستمر ما بين ١ إلى ٣ 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 متبوعة بنظرة عامة على الحل المقترح، 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 يحلل الحلول الأخرى التي قدمتها الأبحاث السابقة لتقييم نطاق استخدامها في المستقبل.

الفصل الثاني: الخلفية ومراجعة الأدبيات

خلفية المشروع

Wazuh [https://varularora.medium.com/wazuh-security-information-and-event-management-siem-for-small-and-medium-sized-enterprises-b2cf1cc7ce0c] هو منصة مفتوحة 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:** توسع 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** نظامًا لكشف التطفل يعتمد على الوكيل (**agent-based**) لمراقبة الأنظمة والتطبيقات بحثًا 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 **HIPAA ،GDPR**، و**PCI DSS**.

- **التكامل مع ELK Stack:** يستخدم **Elasticsearch** لتخزين السجلات، و**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:** تُثبت 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 التوسع:** يمكن تكيفه مع احتياجات المؤسسات الصغيرة والكبيرة، مما يجعله حلاً مرنًا وقابلًا للتطوير.

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

- **مجتمع داعم:** وجود مجتمع كبير من المستخدمين والمطورين 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.

٢,١ مراجعة الأدبيات

تبداء بسرد مفصل للعملية التي تم اتباعها أثناء اختيار البيانات والبحوث ذات الصلة لغرض هذا التقرير. تليها 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. أخيرا، سيعطينا فهما لمدى فائدة البحث لمزيد من التطوير.

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

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

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

٢,٢ 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 ب **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 أيضا 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 المجلات العلمية التي تمت مراجعتها من قبل النظراء كانت مفضلة.

بعد العثور على المشاركات المناسبة، تم إجراء بحث عكسي للمراجع المشار إليها في المقالة، متبوعا ببحث إلى الأمام في **Google Scholar** لتحديد المقالات أو الأوراق التي تشير إلى المقالة الأولية التي تم العثور عليها. تم الإبلاغ عن أوراق المجلات الأكاديمية لمزيد من الفحص. توقف البحث عندما أصبح من الواضح أنه لا يمكن التعرف بسهولة على أي أوراق جديدة، وتقدمت 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.

٢,٣ البحوث السائدة: الفهم والتحليل

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

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

- الضوابط الأمنية
- امتثال 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 وضوحا 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 أطر وأدلة الاستجابة للحوادث. يحدد معظمها مراحل الاستجابة للحوادث على النحو التالي:

٢.٣.١. جدول مراحل االستجابة لحوادث أمن المعلومات

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

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:

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

استخدمت هذه الدراسات السابقة أبحاث التصميم كتقنية بحث أساسية، مع التحقق من صحة التصميمات من خلال النماذج الأولية واختبار النظام التجريبي. بصرف النظر عن تصميم **Metzger et al** (٢٠١١) الذي تم تطبيقه بشكل فعال في وضع العالم الحقيقي لمدة عام واحد، لم يتم تنفيذ التصاميم المدروسة في سياقاتها المخطط 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 وضوحا لماذا لم يكن البحث الموجود منذ كل هذه السنوات مجزيا 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 ل **SIEM** خصيصا للشركات الصغيرة والمتوسطة والتي سيتم مناقشتها في القسم التالي.

الدراسة التي أجراها الأستاذ الدكتور **K.–O. Detken**، **T. Rix**، **Prof. Dr. C. Klayner**، **B. Hellmann**، **L. Renners** نموذجا يعتمد على الهندسة المعمارية المشابهة بشكل ملحوظ ل **SIEM** يسمى مشروع **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 **Splunk** و**Qradar** وما إلى ذلك. العملية الأكثر استهلاكا للوقت هي تكوين نقاط النهاية.

· نظرا 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 جدا ل **SIEM**، لكن **SIMU** ستعزز أمن المنظمة دون تعقيدات **SIEM**. توفر **SIMU** تكاملا أفضل وأسهل للبنية التحتية للمؤسسة، مما يؤدي إلى صيانة أسهل ورؤية السجلات في شبكة المؤسسة. العمل الأساسي ل **SIMU** هو تماما مثل أي **SIEM** آخر مما يعني أنه سيعالج جميع السجلات (**Karlzen**، **H.**، ٢٠٠٩) ويقوم بالارتباط بها، ويكتشف جميع الأحداث من شبكة المنظمة. تماما 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 تختار تنفيذ 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 المتاحة لها مجانا، ودليل خطوة بخطوة حول كيفية تنفيذها 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

٣,١ مقدمة:

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

٣,٢ 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

يوفر 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 التلقائية للتهديدات: أتمتة 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]** والأنظمة الأمنية الخارجية
- واجهة سهلة الاستخدام وإعداد التقارير: يوفر واجهة سهلة الاستخدام لمسؤولي الأمان للوصول إلى الاكتشافات والتصورات والجداول الزمنية والتقارير.

٣,٣ المتطلبات الوظيفية

٣.١.١جمع 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.

٣.١.٢الكشف عن التهديدات

يجب أن يستخدم المشروع تقنيات 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، ويتعرف على الأنشطة غير الطبيعية التي قد تشير إلى انتهاكات أمنية محتملة.

- التحليل السلوكي:

يحلل سلوك الكيانات داخل الشبكة، ويبحث عن الأنماط أو الإجراءات التي تنحرف عن القاعدة.

٣.١.٣تحديد أولويات التهديدات

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

- تقييم المخاطر:

تعيين 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 ومنخفضة) بناء على درجة المخاطر الخاصة بها لتمكين تحديد أولويات الاستجابة بكفاءة.

٣.١.٤متطلبات الاستجابة الآلية للتهديدات

- عزل نقاط النهاية المصابة:

عزل نقاط النهاية المخترقة 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.

٣.١.٥التكامل مع أدوات الامن

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

- **Virus Total**
- **Suricata**

٣.١.٦واجهة سهلة الاستخدام ومتطلبات إعداد التقارير

يجب أن يوفر المشروع واجهة سهلة الاستخدام لمسؤولي ومحللي 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 وموجزة عن الأحداث الأمنية واتجاهات التهديدات ونقاط الضعف لاتخاذ قرارات فعالة.

- تنبيهات قابلة للتخصيص:

السماح للمستخدمين بتعيين تنبيهات مخصصة بناء على معايير أمان محددة أو حوادث ذات أهمية.

الفصل الرابع: تصميم ونمذجة 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.

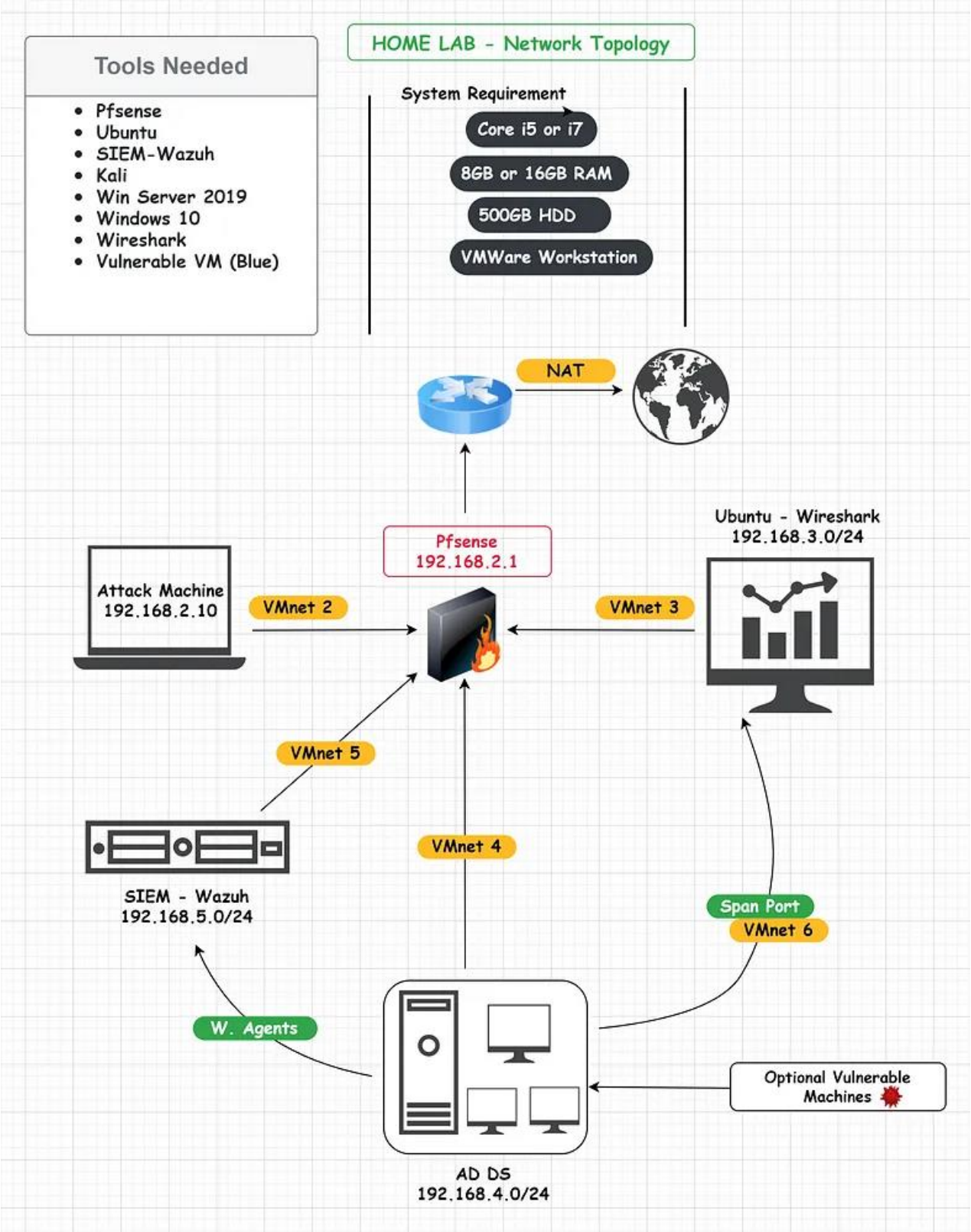
٤,٢. تخطيط وتصميم المشروع

٤,٢,١. طوبولوجيا الشبكة

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

تشير طوبولوجيا 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 المقترح باستخدام برنامج **VMware Workstation Pro** باستخدام مجموعة من الاجهزة الافتراضية **machines Virtual** واستخدام **firewall PfSense** ونظام **SIEM-Wazuh** واستخدام أداة **Wireshark** و**Active Directory Domain Services (AD DS)** ونظام **kali Linux** و**Ubuntu** و**windows 10**


Tools Needed
Pfsense
Ubuntu
SIEM-Wazuh
Kali
Win Server 2019
Windows 10
Wireshark
Vulnerable VM (Blue)
HOME LAB - Network Topology
System Requirement
Core i5 or i7
8GB or 16GB RAM
500GB HDD
VMWare Workstation
NAT
Pfsense
192.168.2.1
Ubuntu - Wireshark
192.168.3.0/24
Attack Machine
192.168.2.10
VMnet 2
VMnet 3
VMnet 5
VMnet 4
SIEM - Wazuh
192.168.5.0/24
Span Port
VMnet 6
W. Agents
Optional Vulnerable Machines
AD DS
192.168.4.0/24

شكل رقم ()

٤,٢,٢. شرح طوبولوجيا الشبكة:

- **VMware Workstation Pro:** سيتم استخدامه لاستضافه الأجهزة والأنظمة الوهمية ولعمل محاكاة لبيئة عمل واقعية.
- **firewall pfsense: سيكون جدار الحماية** هذا بمثابة حاجز بين قطاعات الشبكة المختلفة داخل الهيكل، حيث يتحكم ويراقب حركة المرور الواردة والصادرة ، وتم اختياره بسبب مرونته واستقراره وسهوله التعامل معه ويراقب الحزم والحركة الداخلة والخارجة من الشبكة ويعتبر مفتوح المصدر (مجاني) ، ويعتبر هو حل متعدد الاستخدامات وغني بالميزات للأفراد والمؤسسات الذين يبحثون عن جدار حماية قوي وقابل للتخصيص ، الهدف منه هو تعزيز الأمن 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 للتقليل من الضرر.
- **Wireshark:** محلل بروتوكول الشبكة الذي يلتقط ويفحص البيانات التي تنتقل ذهابًا وإيابًا على الشبكة في الوقت الفعلي. إنه مفيد في فهم سلوك الشبكة وتشخيص المشكلات وتحديد التهديدات الأمنية المحتملة من خلال تحليل الحزم.
- Active Directory Domain Services (AD DS)**:** توفر **AD DS** آلية مصادقة وتفويض مركزية. 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. ستوفر 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 المنافذ 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		
المواصفات	كمية	الموارد
CORE-i9, RAM: 32 DDR4, HARD: 1TB SSD,	1	جهاز لابتوب
CORE-i7, RAM: 16 DDR4, HARD: 1TB SSD,	1	جهاز لابتوب

٤,٢,٣,٢. انظمة التشغيل المستخدمة:

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

٤,٢,٣,٣. جدار الحماية وأنظمة الامن:

أنظمة الامن	
اسم	إصدار
Pfsense firewall	**2.7.2**
Suricata	6.0.19

٤,٢,٣,٤. التقنيات والأدوات والبرامج المستخدمة:

التقنيات والادوات	
اسم	إصدار
VMware Workstation	17.5.1
Wazuh	4.7.2
YARA	4.4.0

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

٤,٢,٣,٥. لغات البرمجة المستخدمة:

اللغات المستخدمة	
اسم	إصدار
python	**3.12.2**
Bash Scripting	

٤,٣. التقنيات المستخدمة في المشروع

٤,٣,١ أولا المكونات الأساسية في النظام **Wazuh**

كما نعلم يعمل **Wazuh** بثلاثة مكونات رئيسية مركزية**: الخادم، والمفهرس، ولوحة المعلومات، والوكيل**

٤,٣,١,١ **Wazuh indexer**

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

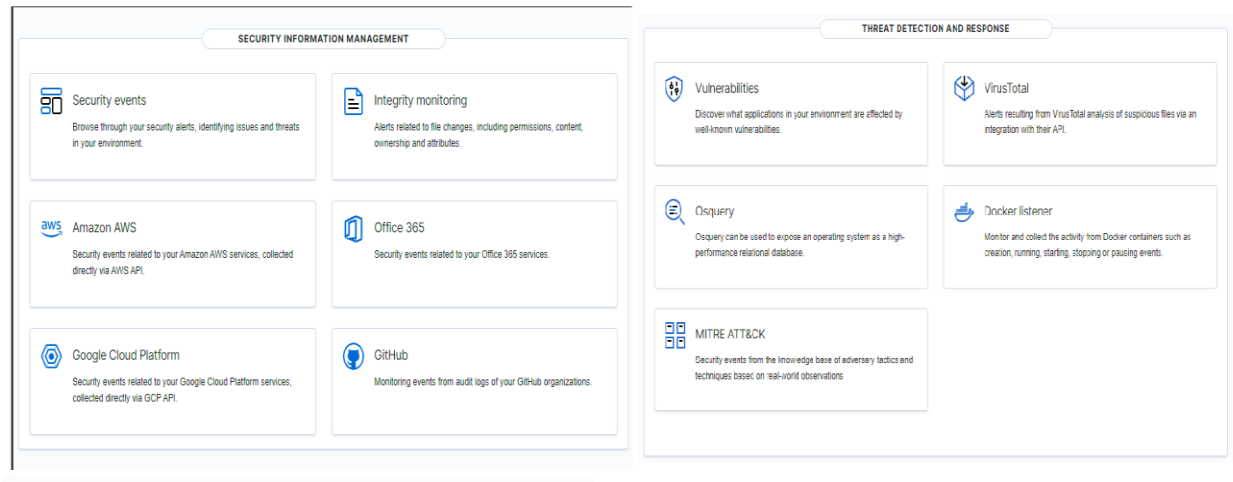
يمكن بدء التفاعل مع المفهرس باستخدام **REST API** الخاص به. تشمل المهام البحث عن المستندات أو إضافتها أو حذفها وتعديل الفهارس والمزيد.

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 **PCI DSS** و **GDPR**و **HIPAA**و **CIS**و **NIST 800-53** لتحسين بيانات التنبيه 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.



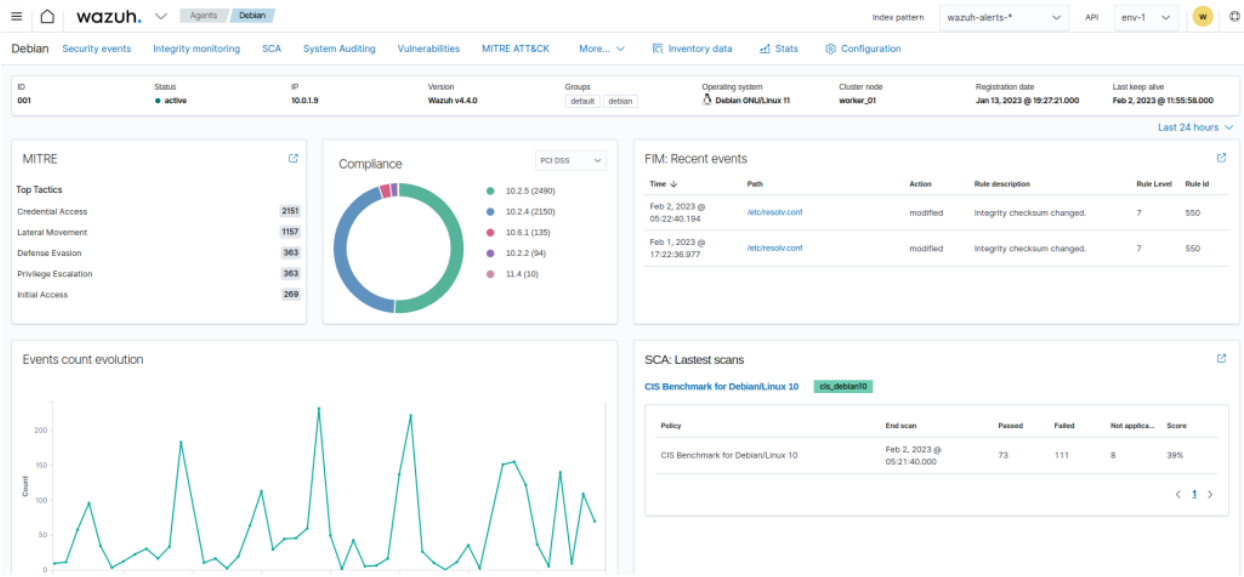
الشكل رقم ()

- تصور البيانات وتحليلها

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

- مراقبة الوكلاء وتكوينهم

تسمح لوحة المعلومات هذه بإدارة تكوين الوكلاء ومراقبة الحالة.



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 للوكلاء العمل على**Linux** ، و**Windows**، و**macOS**، و**Solaris**، و**AIX**، وأنظمة التشغيل الأخرى. تتم حماية هذه الأنظمة بواسطة **agents**، مما يوفر إمكانات منع التهديدات واكتشافها والاستجابة لها.

٤,٣,٢ ثانيا 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 والمحتوى. عند وقوع حدث ما، فإنه يلتقط تفاصيل من وماذا ومتى في الوقت الفعلي. بالإضافة إلى ذلك، تقوم وحدة **FIM** ببناء قاعدة بيانات والحفاظ عليها مع حالة الملفات المراقبة، مما يسمح بتشغيل الاستعلامات عن بعد.

لا يستطيع **FIM** وحده 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 **VirusTotal** و **CDB**لتجزئة الملفات **hashing**، لاكتشاف الملفات الضارة والأنماط غير الطبيعية التي تظهر وجود برامج ضارة.

٤,٣,٢,٢ الكشف عن سلوك الجذور الخفية Rootkit

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

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

٤,٣,٢,٣ VirusTotal integration

بمجرد دمجه مع**VirusTotal** ، يستطيع **Wazuh** اكتشاف الملفات الضارة. يتم تشغيل التنبيهات عندما يكتشف **FIM** أي تغييرات 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 تنبيه قد يحتوي على خطأ أو إشارة إلى وجود ملف ضار.

٤,٣,٢,٤ YARA

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

٤,٣,٢,٥ Windows Defender logs collection

سيتم تكوين الوكلاء على نقاط نهاية **Windows** لتجميع من سجلات**Windows Defender** ، التي 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 المنسدلة لجدار الحماية، أو يعيد تشغيل وكيل أو مدير **.Wazuh** هذه ليست سوى عدد قليل من الاستجابات النشطة المضمنة في البرنامج النصي الافتراضي لـ**.Wazuh**

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

٤,٣,٢,٧ Suricata

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

جمع البيانات**:** ارسال التنبيهات: يجمع **Suricata** حزم الشبكة ويحللها للكشف عن أي نشاط ضار، إذا اكتشف **Suricata** أي نشاط ضار، فإنه يرسل تنبيهًا إلى **.Wazuh**

٤,٣,٣ نيات **المستخدمة في النظام**

٤,٣,٣,١ **Python**

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

network.py: سكريبت بايثون يجمع معلومات الشبكة خلال فترة زمنية معينة باستخدام مكتبة **psutil** يتم إلحاق 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

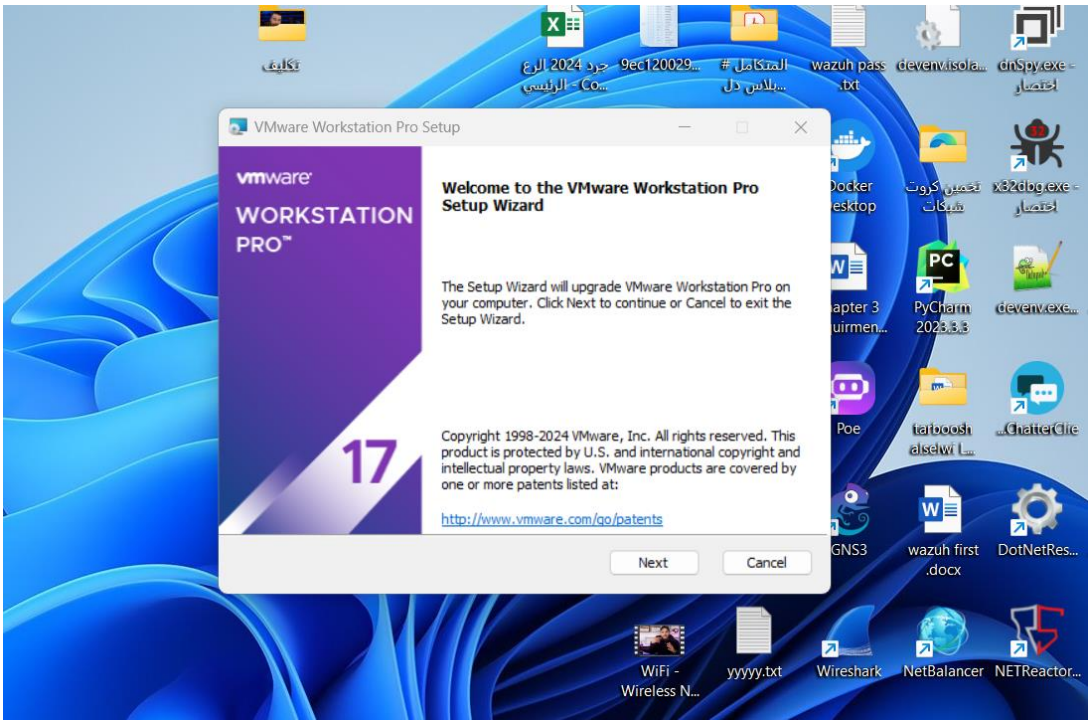
٥,١. مقدمة

في هذا الفصل سنقوم بعمليه التكوين للمشروع من ناحية تثبيت البيئة وتكوينها وتثبيت نظام **Wazuh** والأنظمة الاخرى، ثم نبدأ بعمليه الاختبار.

٥,٢. خطوات الأساسية في تكوين عمل المشروع

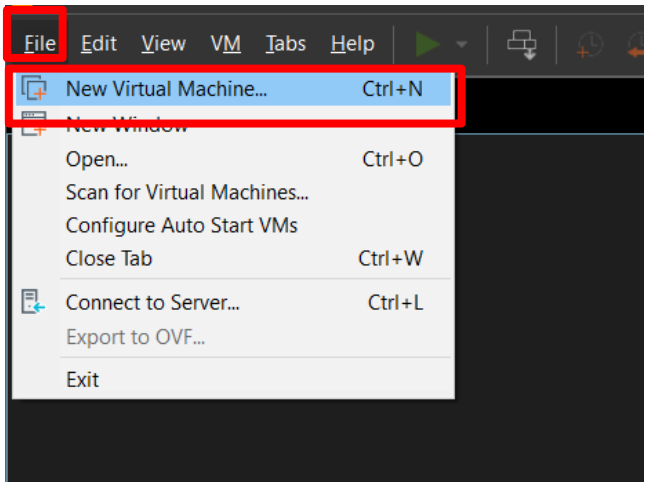
٥,٢,١. يتم تثبيت VMware Workstation Pro

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



٥,٢,٢. تثبيت جدار الحماية pfsense في VMware

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

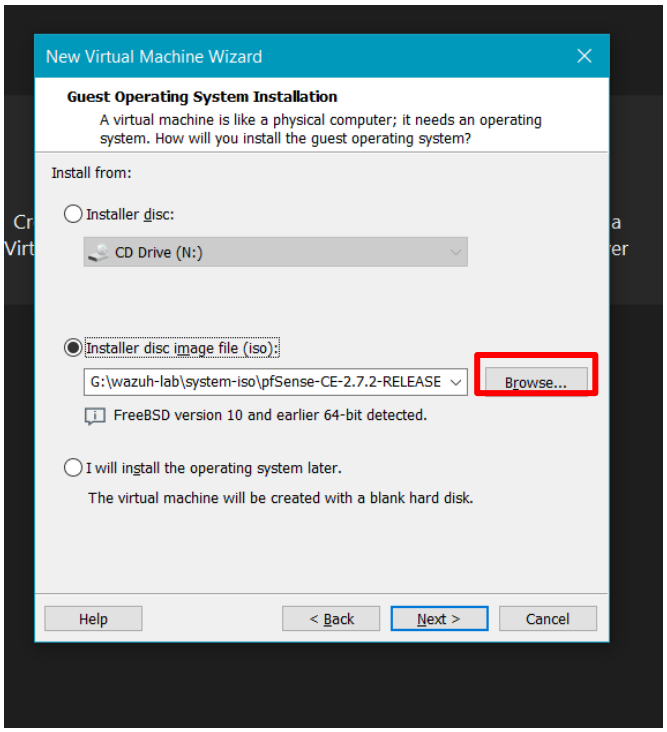


شكل رقم ()

تحديد الاعدادات الافتراضية عن طريق النموذج ***typical***

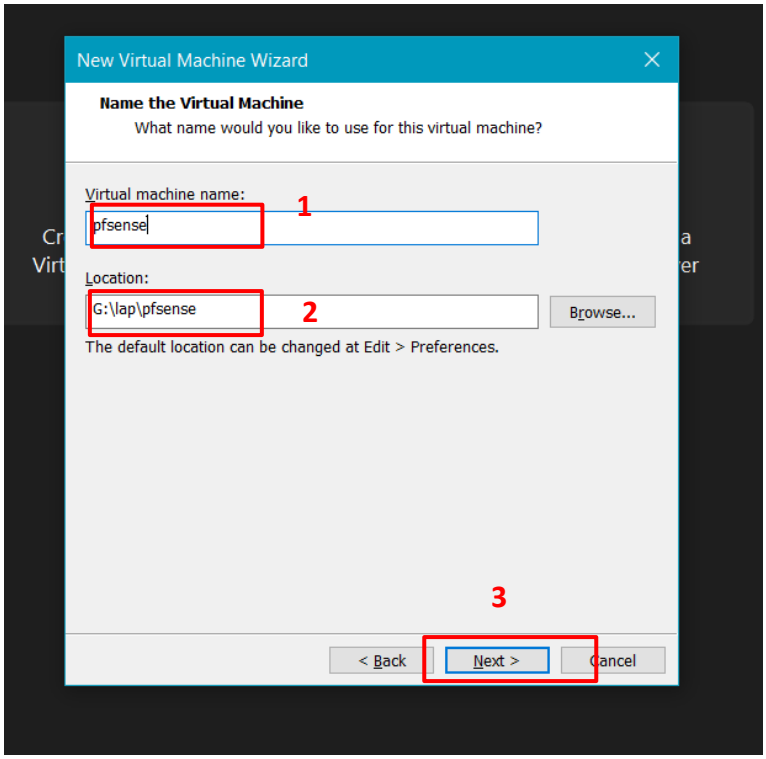
شكل رقم ()

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



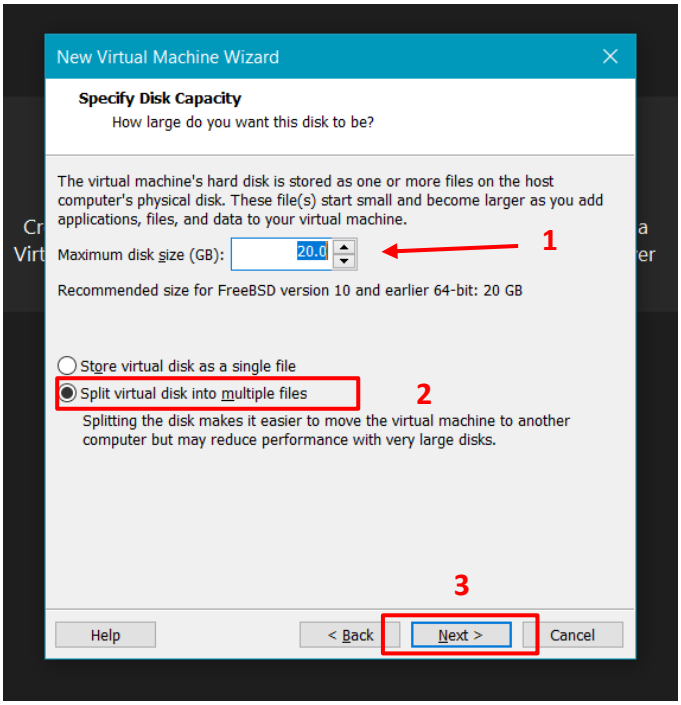
شكل رقم ()

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."



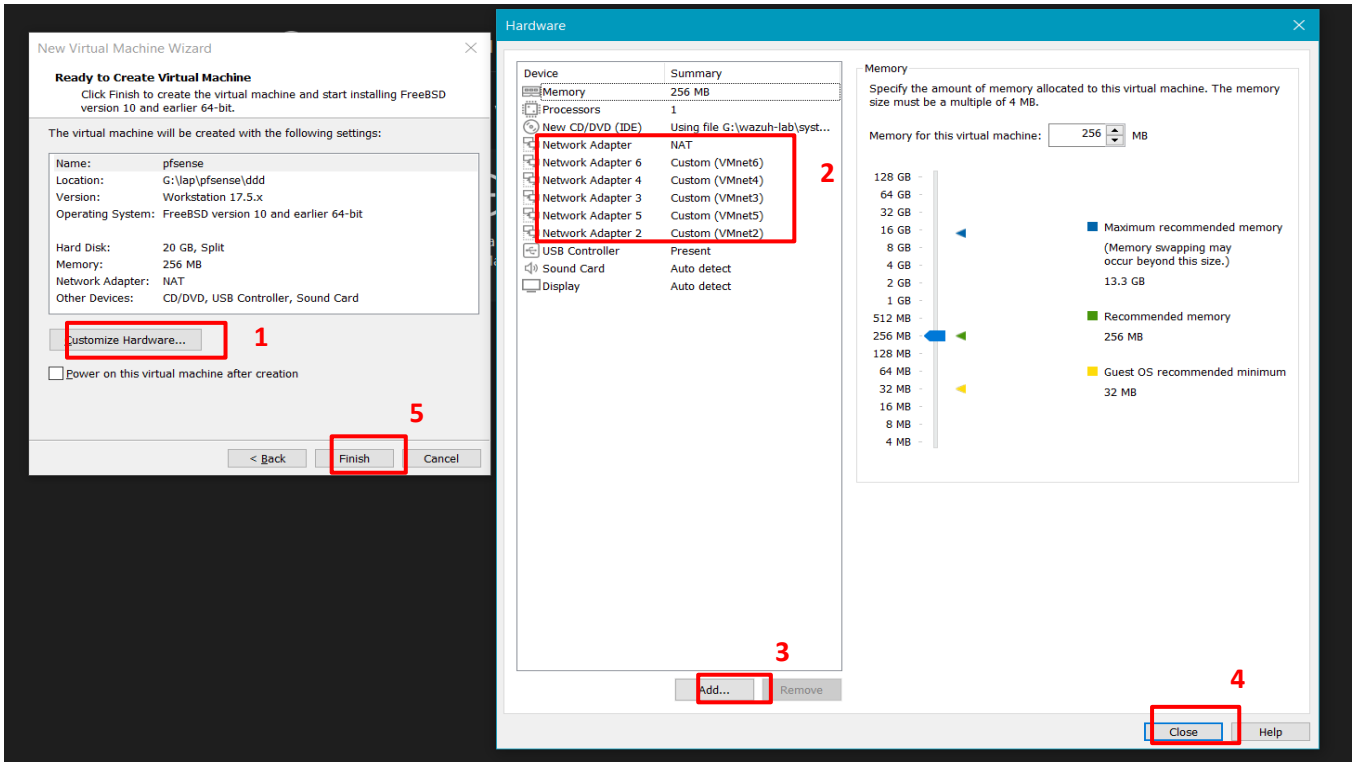
شكل رقم ()

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



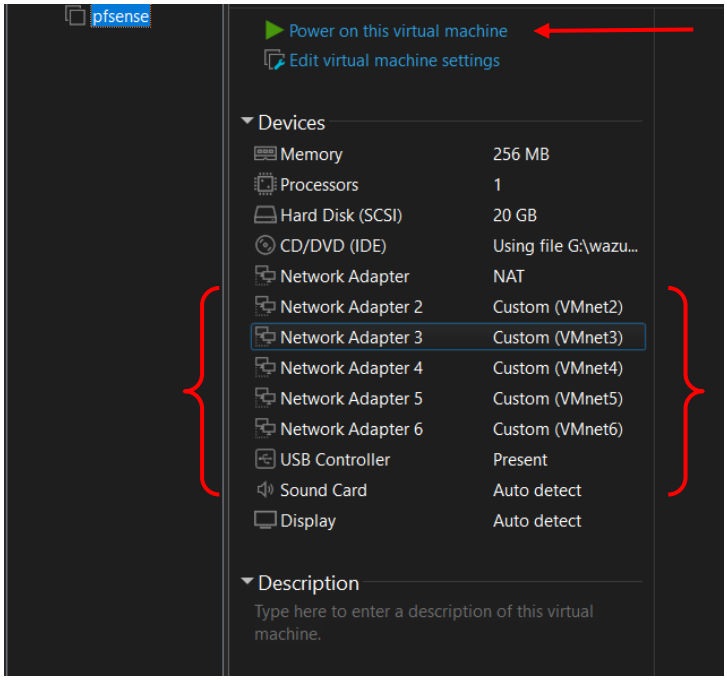
شكل رقم ()

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.



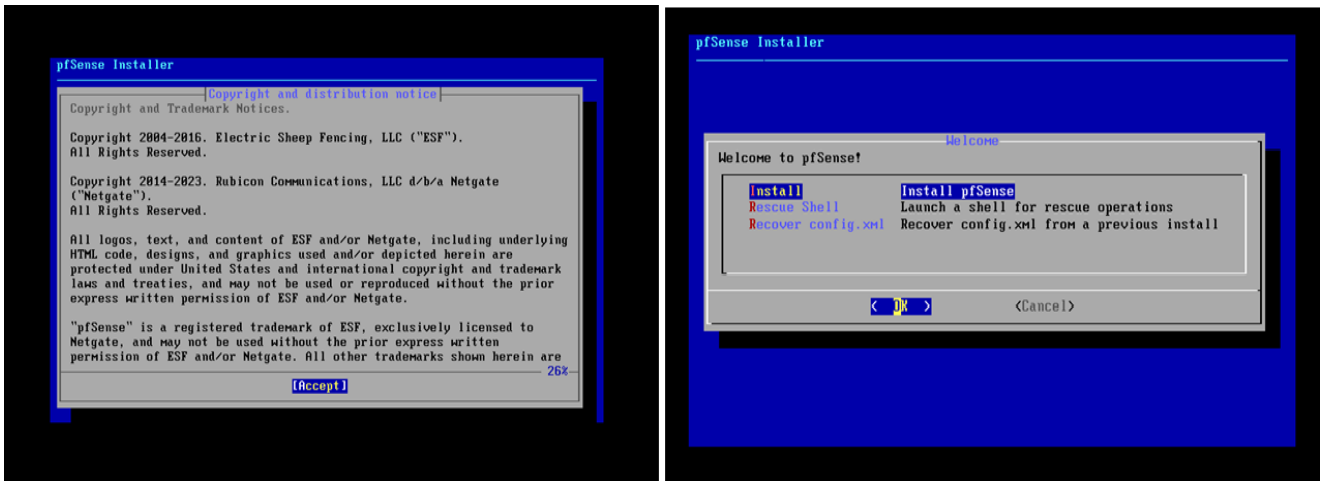
شكل رقم ()

حاليا بعد التثبيت عند ظهور واجهة **VMware** بهذا الشكل ، *نقوم* بـتأكد 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 ()

والآن تبدأ عملية التثبيت. اضغط على ***enter*** للقبول Accept. حدد install واضغط على ***Enter***لكي يثبت install pfSense

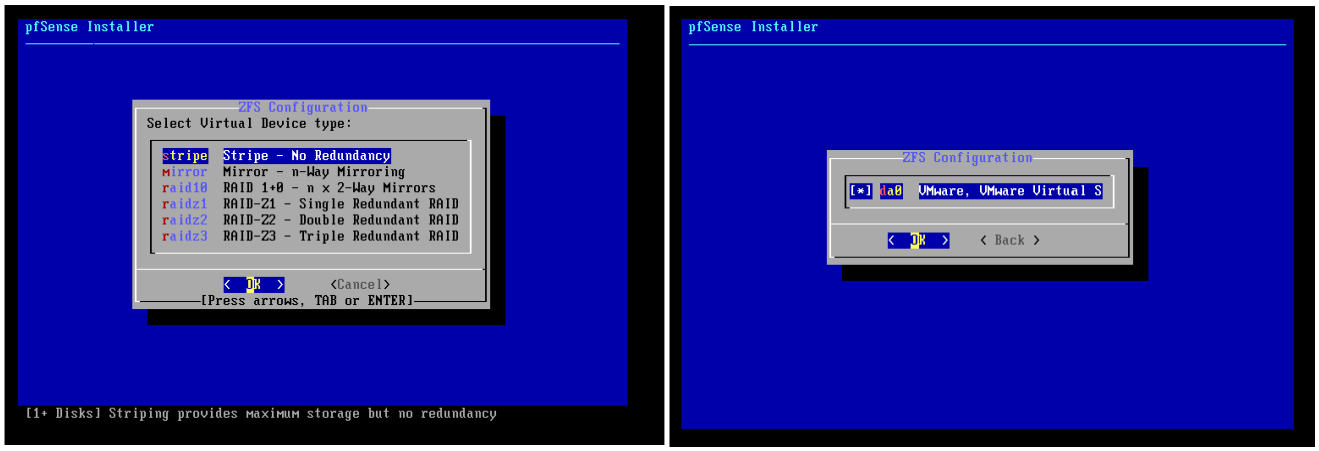


شكل رقم ()

لن نقوم بتقسيم vHDD الخاص بنا. حدد Auto واضغط على **enter** حدد install واضغط على ***Enter.***

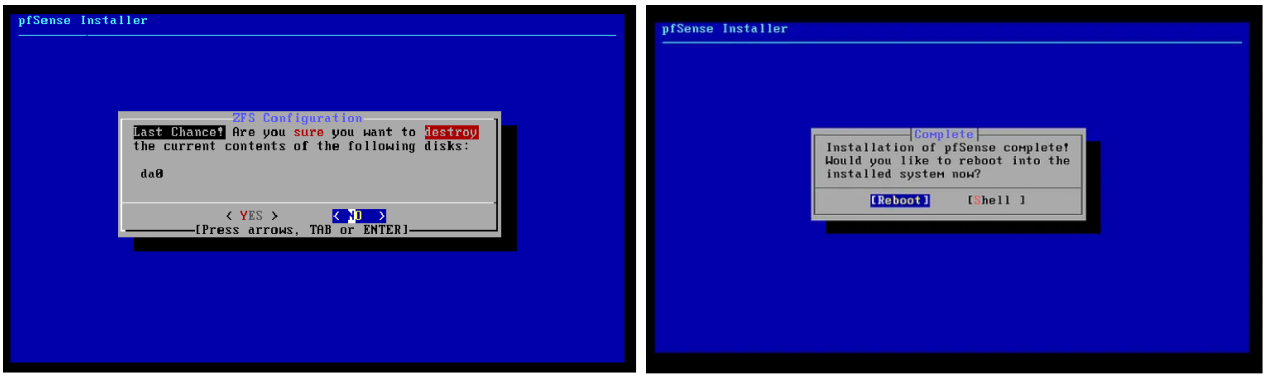
شكل رقم ()

حدد الشريط stripe واضغط على ***Enter*** اضغط على ***space bar*** لأضافه قيمه وحدد ok.



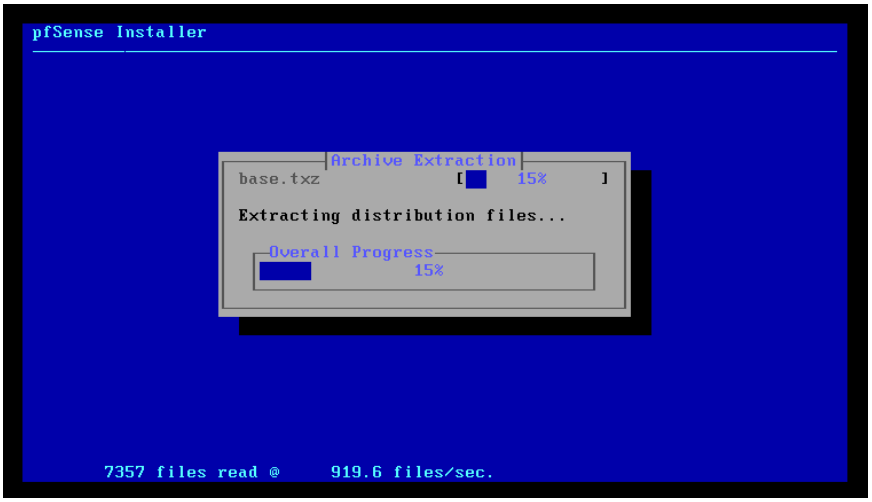
شكل رقم ()

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



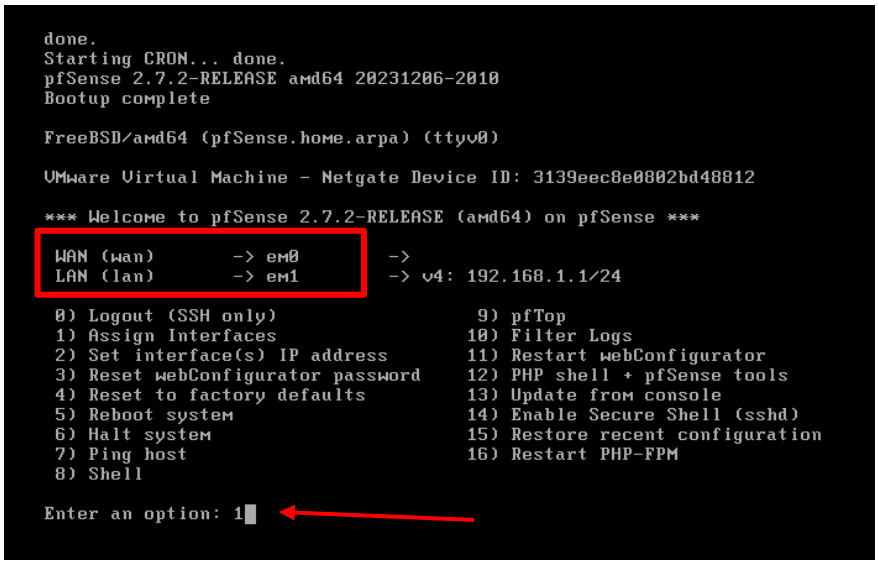
شكل رقم ()

حاليا يقوم بعمليه التثبيت



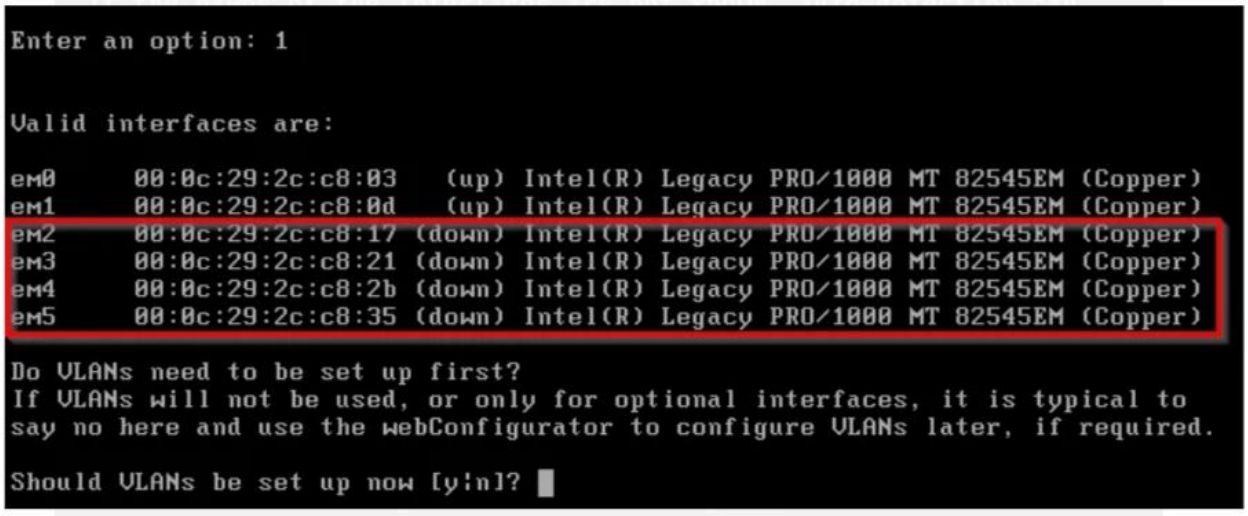
شكل رقم ()

بمجرد تثبيت pfSense بنجاح، سنلاحظ في البداية وجود واجهتين: WAN و LAN تتصل واجهة WAN بمحول شبكة NAT الخاص بنا، مما يسمح بالوصول إلى الإنترنت. تعد واجهة LAN إحدى واجهات الشبكة الأخرى، ولكن قد نرى واحدة فقط في البداية. لتنشيط كافة الواجهات الأخرى علىpfSense ، اختر الخيار ١ — تعيين الواجهات.



شكل رقم ()

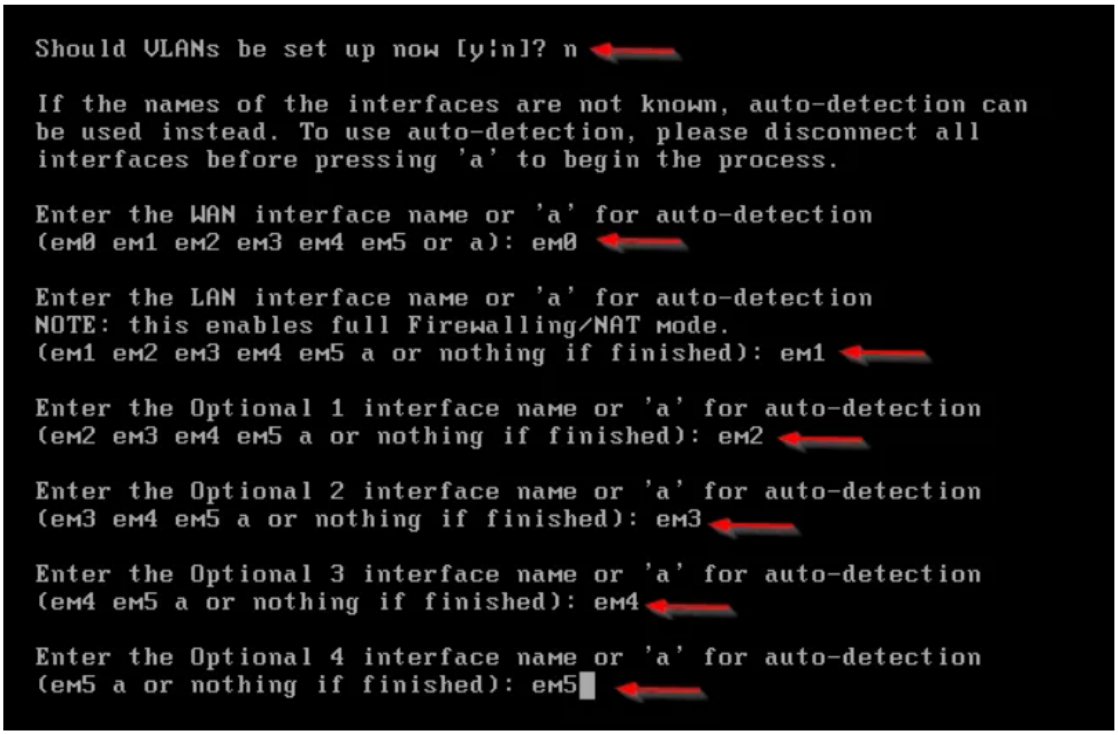
من هنا، نرى جميع الواجهات الصالحة مع اثنتين منها فقط ***(WAN & LAN)***للأعلى وأربعة منها للأسفل. الخطوة التالية هي تمكين كل هذه الواجهات.



شكل رقم ()

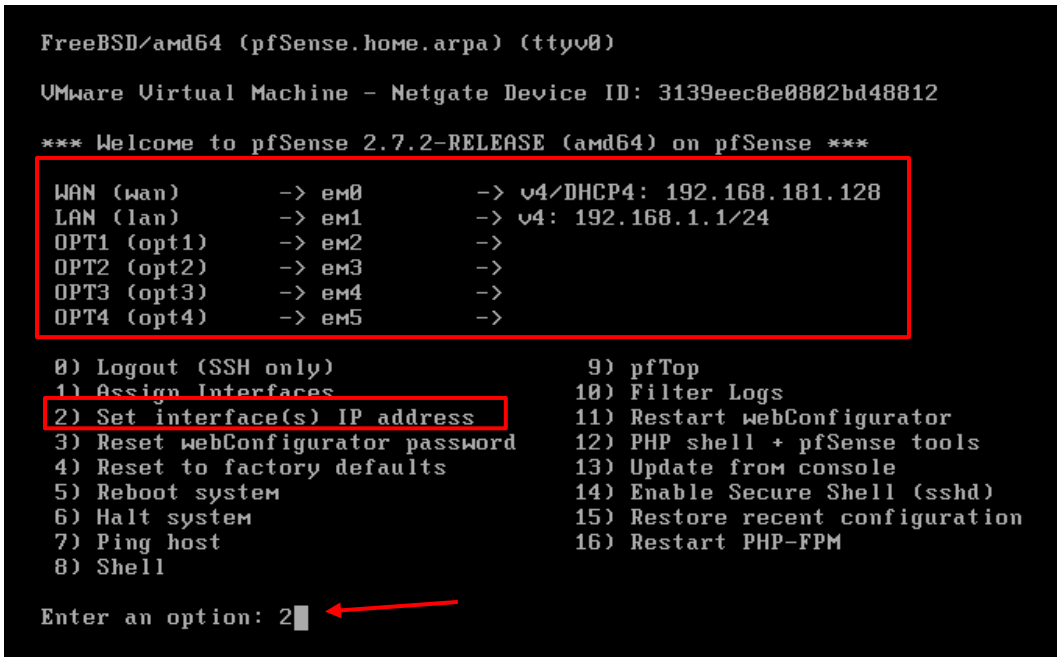
Should VLANS be set up now [y:n]?: *n*

أدخل ***em0*** *و* ***em1*** *و* ***em2*** *و* ***em3*** *و* ***em4*** *و* ***em5*** على التوالي لكل سؤال متتالي. أخيرًا، اكتب ***(y)***للمتابعة.



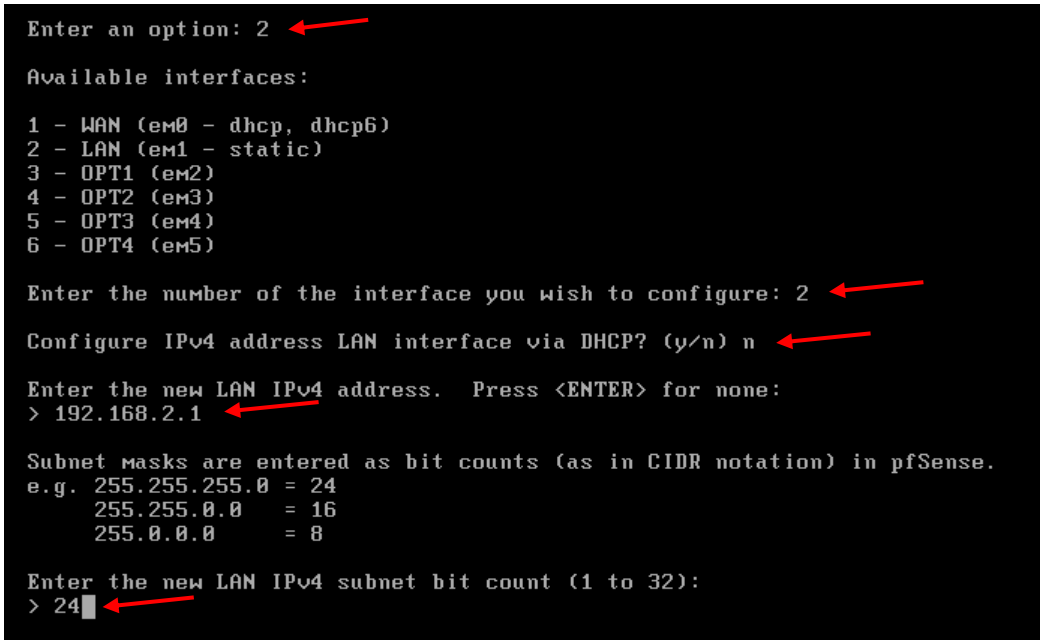
شكل رقم ()

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



شكل رقم ()

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



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

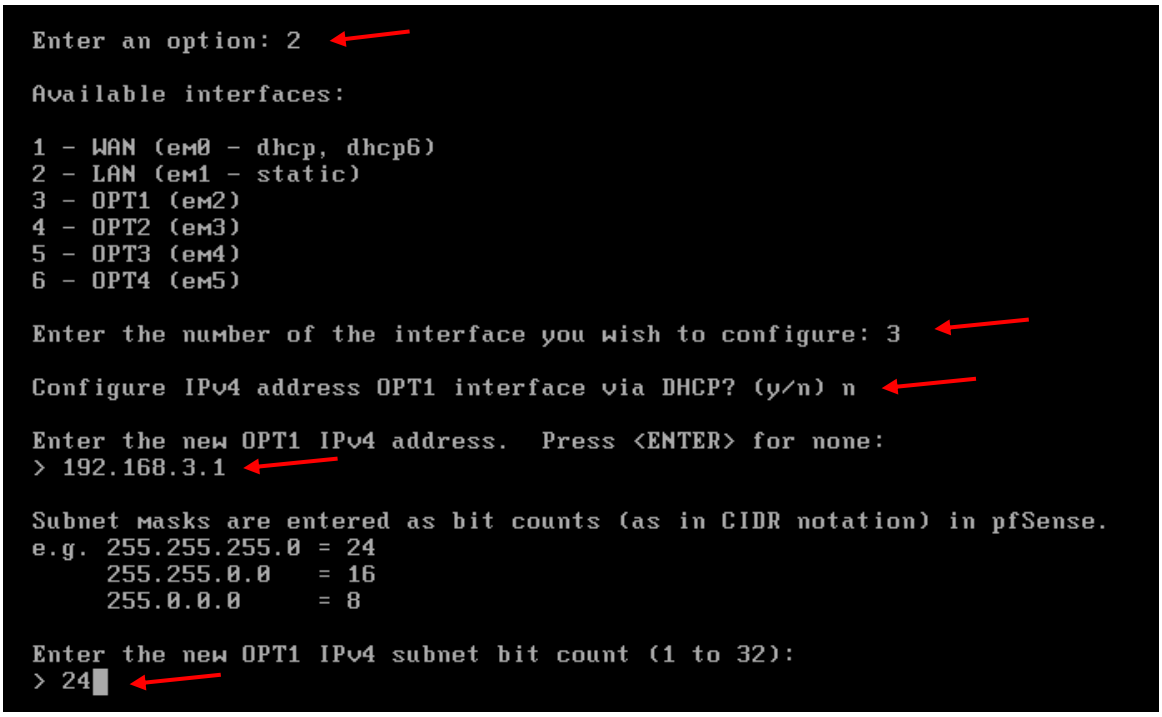
OPT3 = 192.168.5.1/24

تكوين اول 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.
```

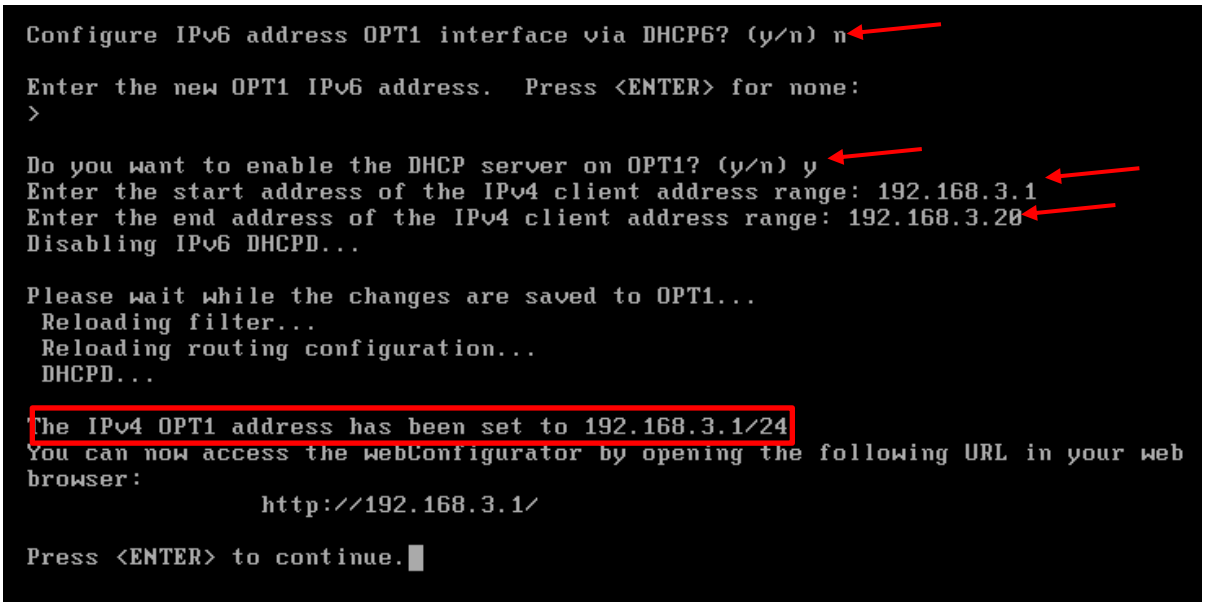
شكل رقم ()

تكوين ثاني عنوان لجهاز مراقب الشبكة Wireshark



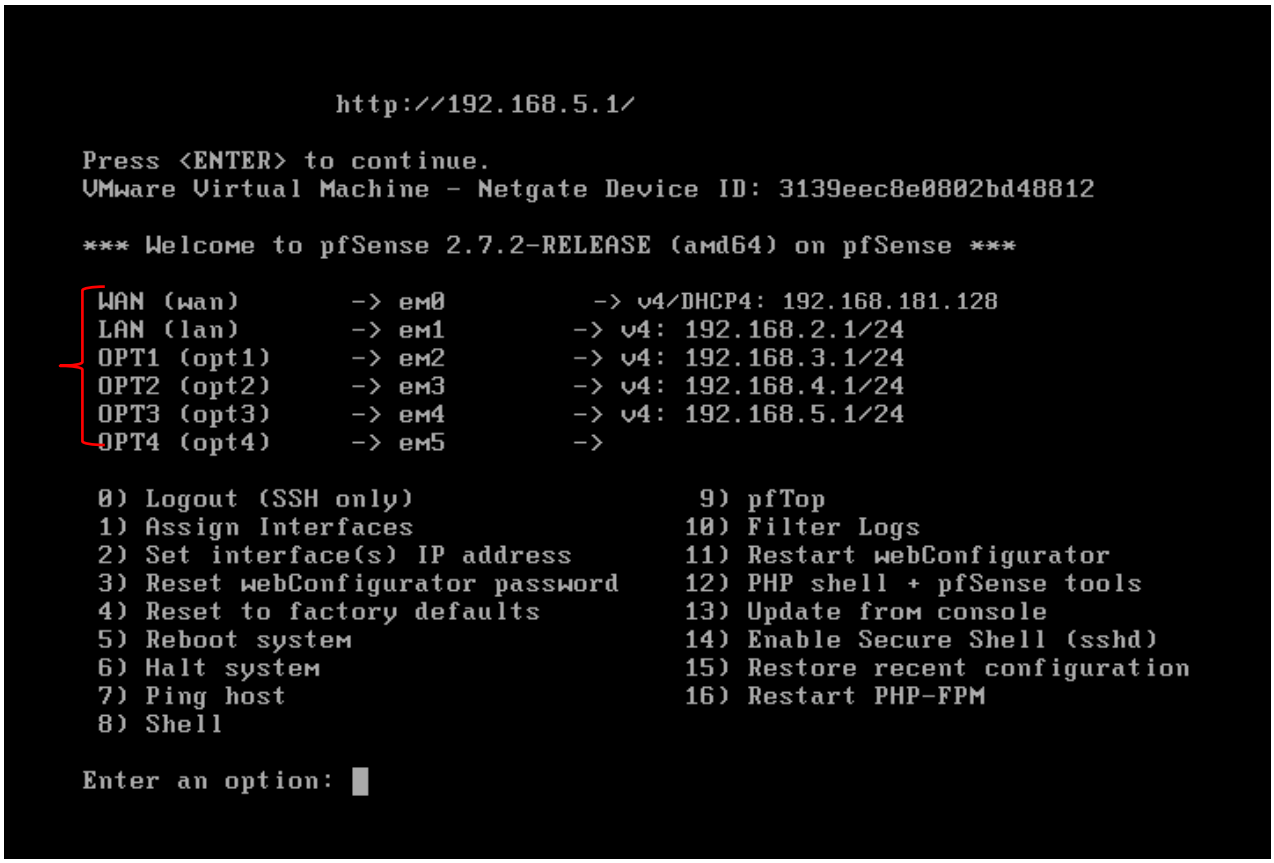
الشكل رقم ()

التكوين الثالث عنوان لجهاز إدارة لأجهزة AD DM



الشكل رقم ()

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



الشكل رقم ()

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

٥,٢,٣. يتم تثبيت kali linux

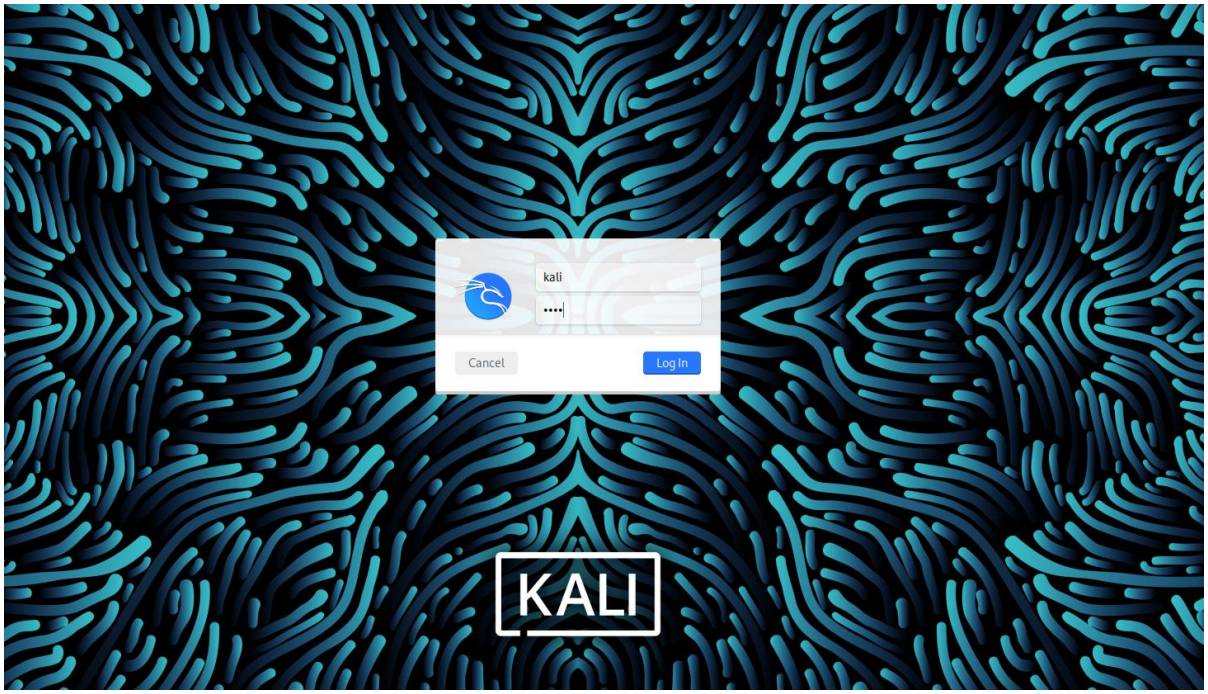
سنقوم بتثبيت جهاز الهجوم الخاص بنا وكذلك إجراء تكوينات على جدار الحماية الخاص بنا

NAT Door: هذا الباب يواجه الإنترنت، مثل النافذة لرؤية ما يحدث هناك وهو الذي يسمح لنا بالاتصال بالأنترنت.

Other Doors: لدينا **5** أبواب إضافية للمهام الخاصة، مثل التأكد من دخول الأشياء الجيدة فقط عن طريق المراقبة.

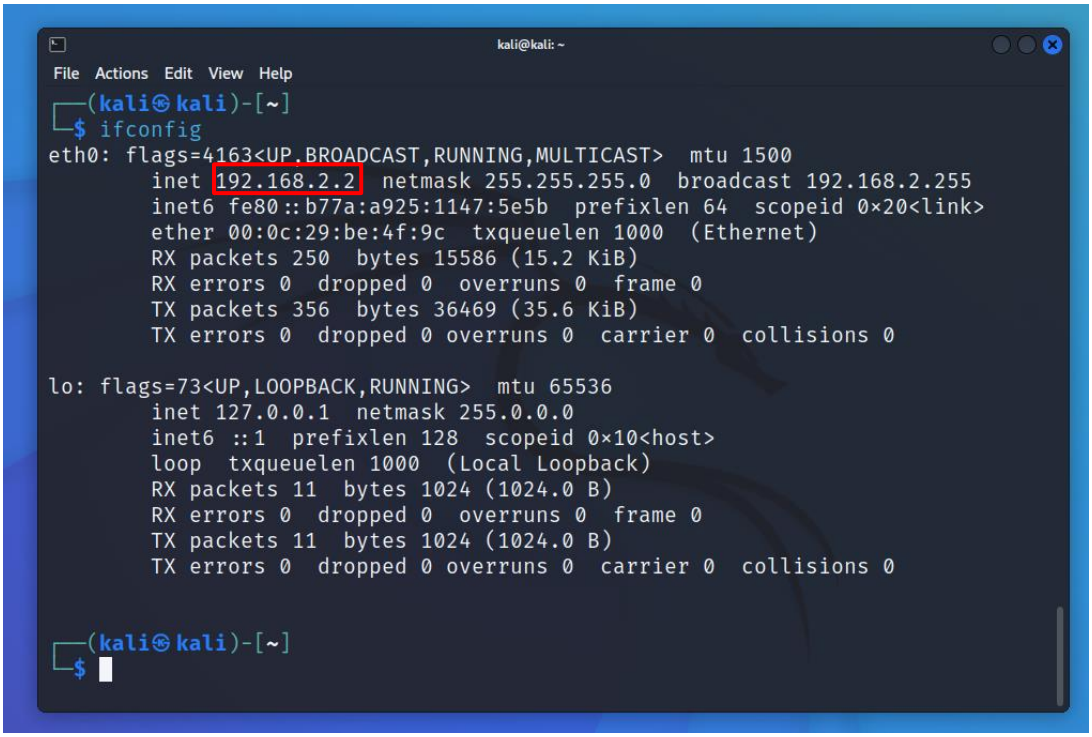
يساعدنا حارس الأبطال الخارقين **(PfSense)** في مراقبة من يدخل ومن يخرج ويتحكم فيه. إنه مثل وجود وصي لكل جزء من مختبرنا. او تصور الأمر على هذا النحو: إن نظام **PfSense** الخاص بنا هو الحارس اليقظ، ونحن، المهندسون المعماريون، قمنا بالوصول إلى واجهات الويب الخاصة به لإعداد القواعد.

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



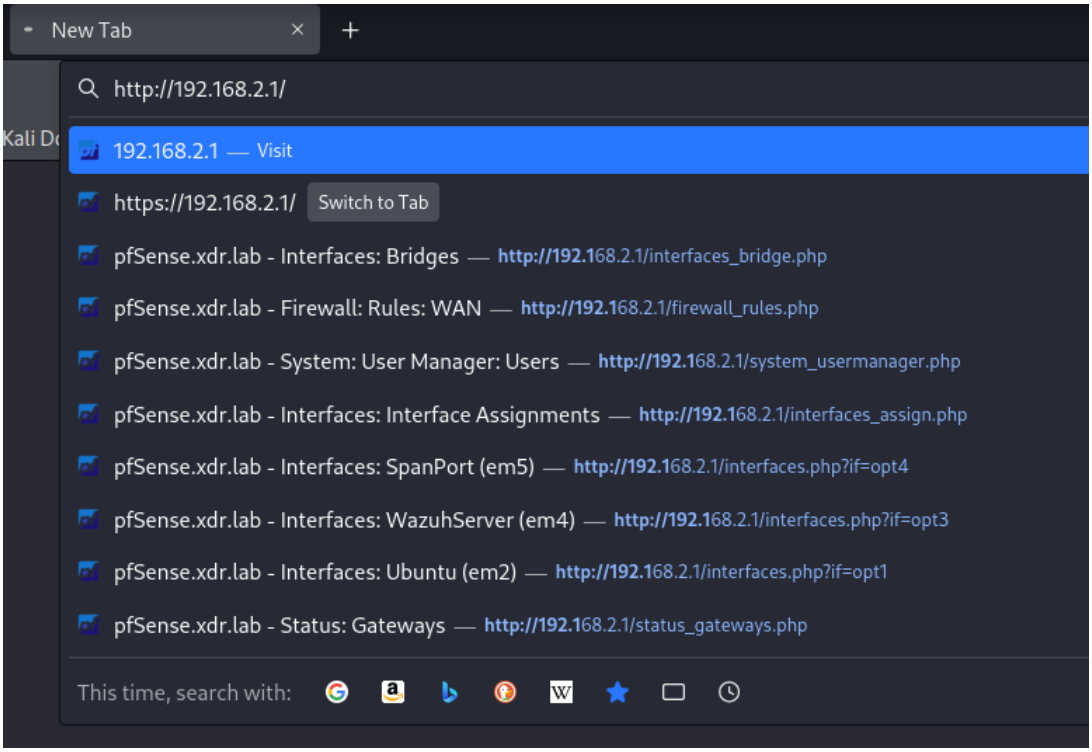
الشكل رقم ()

نذهب الى terminal واكتب 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، يتعين علينا الوصول إلى واجهة الويب الخاصة بجدار الحماية.



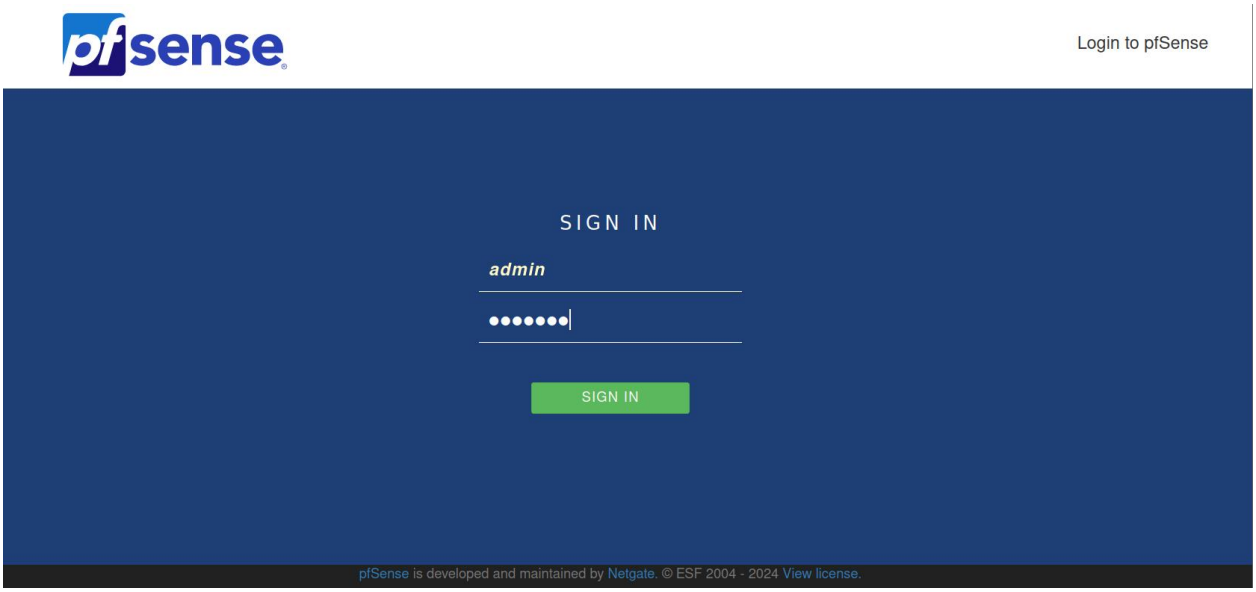
الشكل رقم ()

قم بتشغيل Mozilla Firefox واكتب http://192.168.2.1 للوصول إلى pfSense. اسم المستخدم وكلمة المرور الافتراضية هما **(admin pfsense)** ثم اضغط على زر الإدخال.



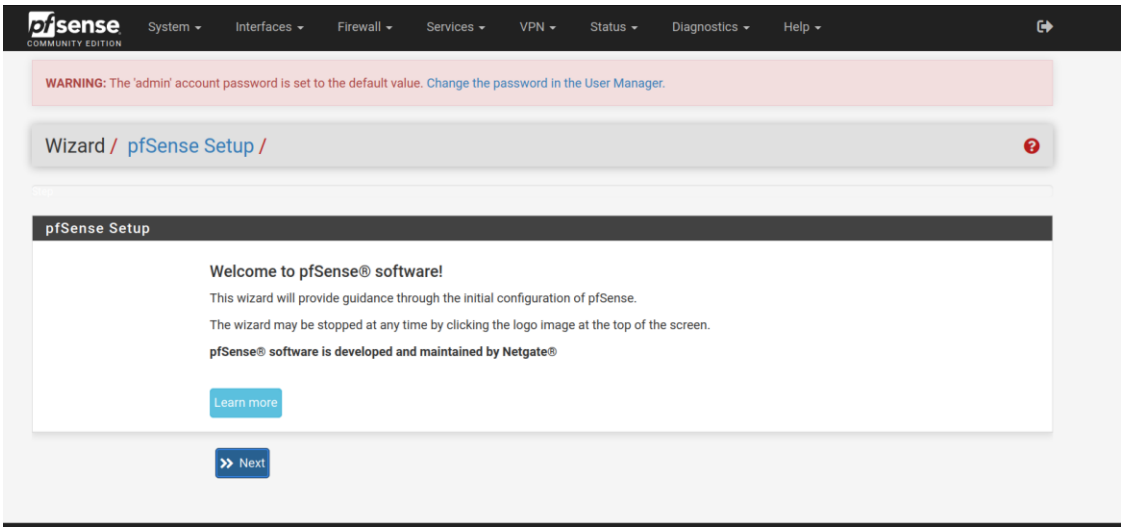
الشكل رقم ()

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

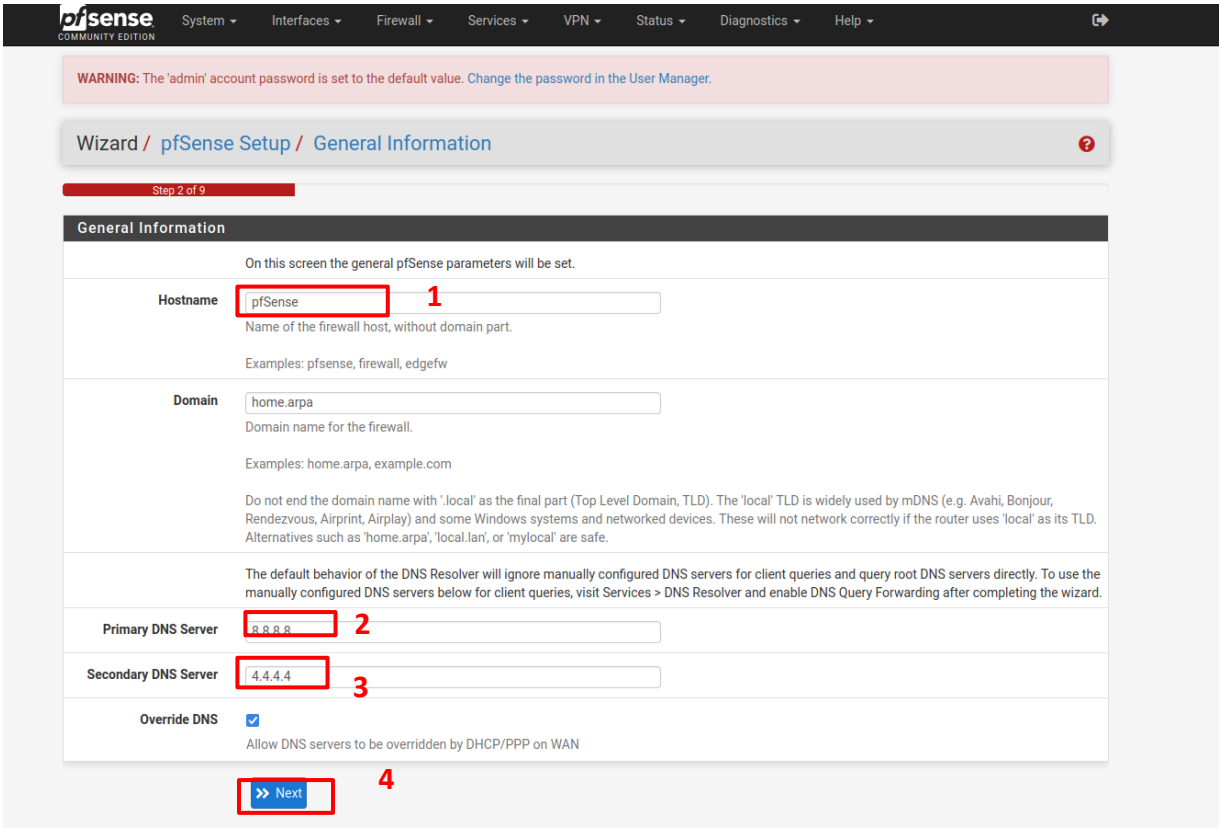


الشكل رقم ()

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

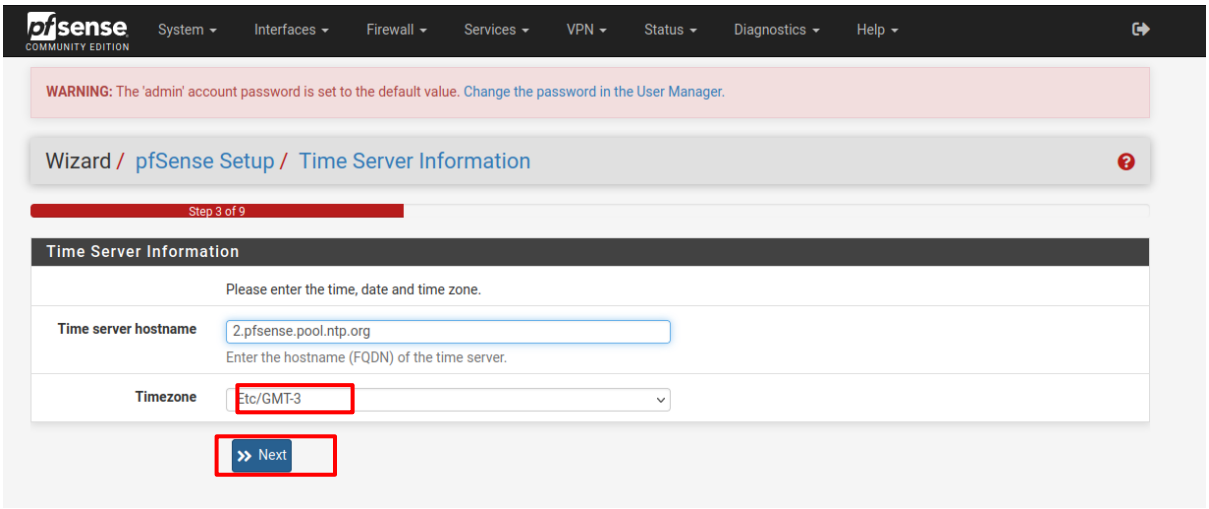


الشكل رقم ()



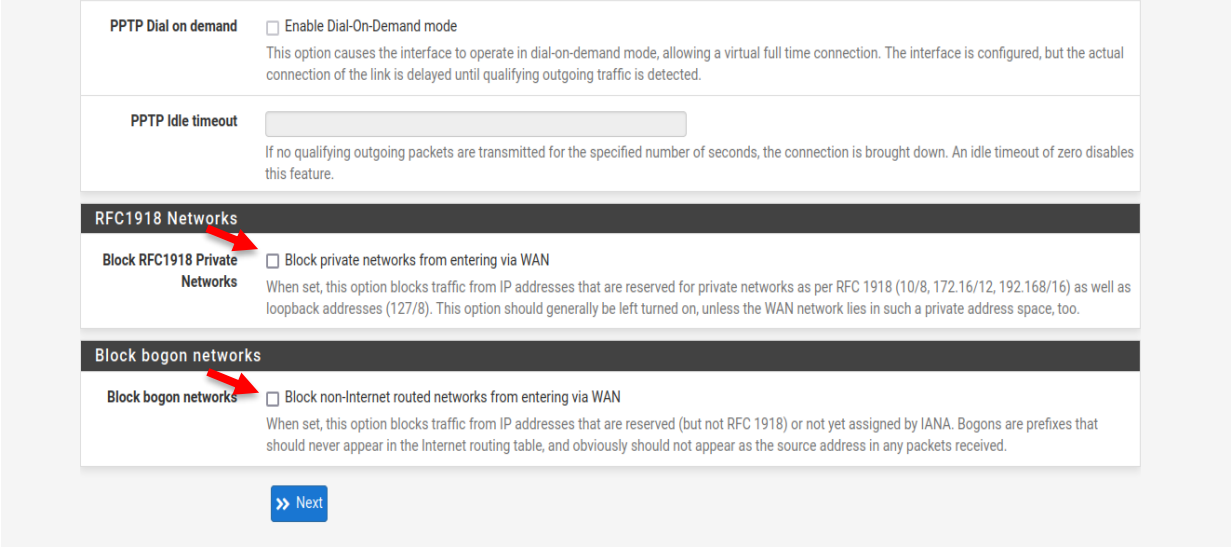
الشكل رقم ()

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



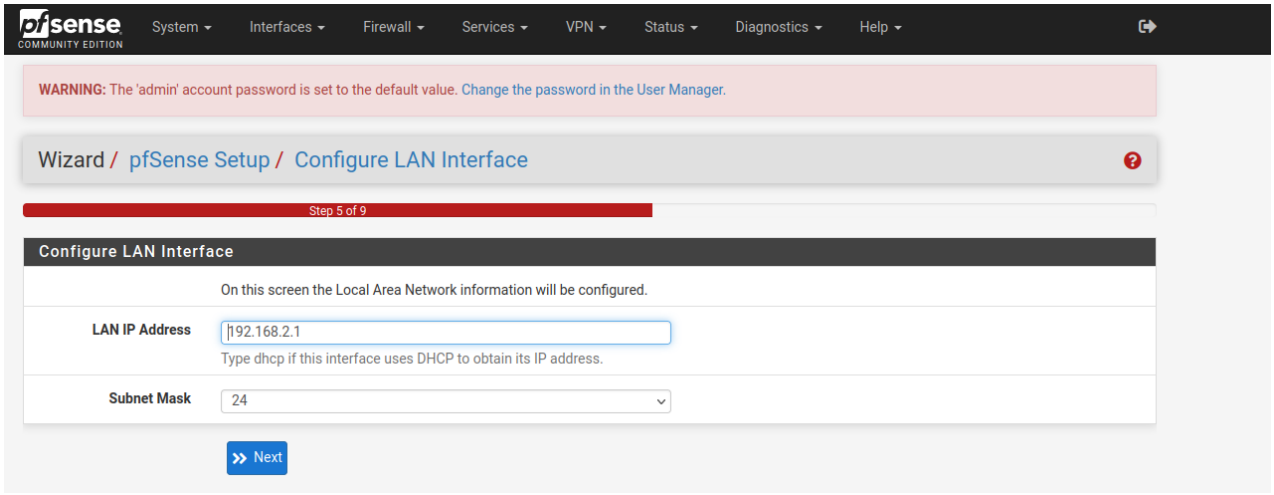
الشكل رقم ()

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



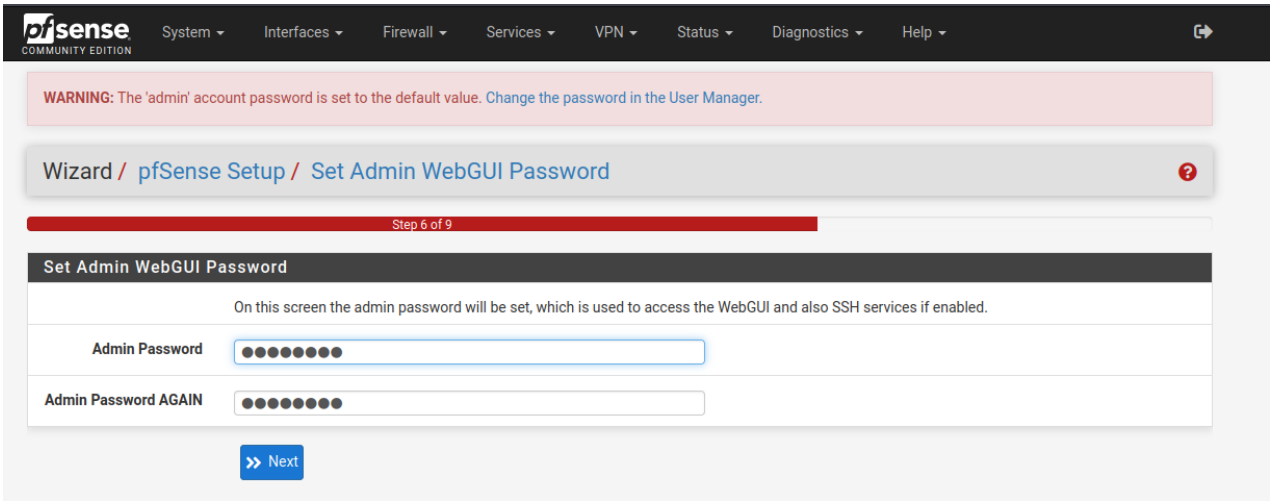
الشكل رقم ()

على واجهةLAN ، نترك كل شيء افتراضيًا ونضغط على "**التالي**"



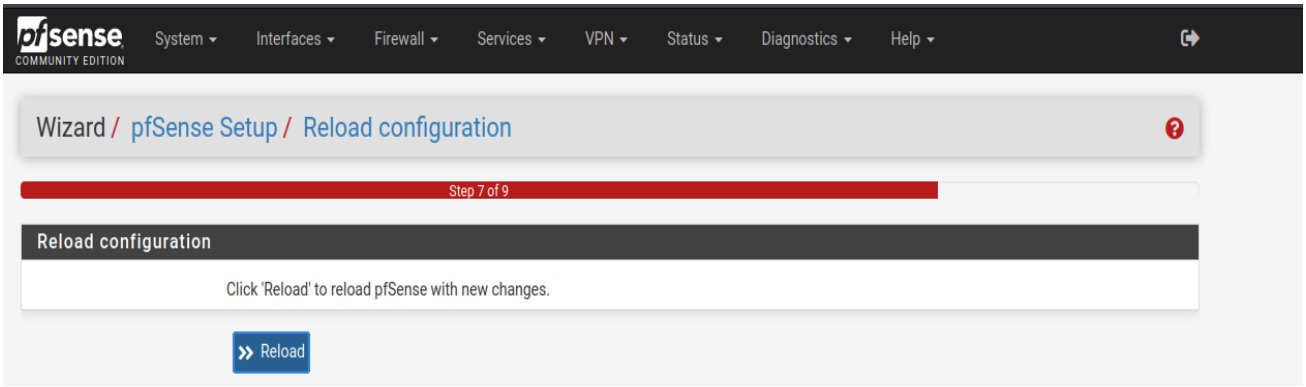
الشكل رقم ()

الخطوة الأخيرة هي تغيير كلمة المرور الافتراضية وتحديد **next ستكون (pfsense1)**



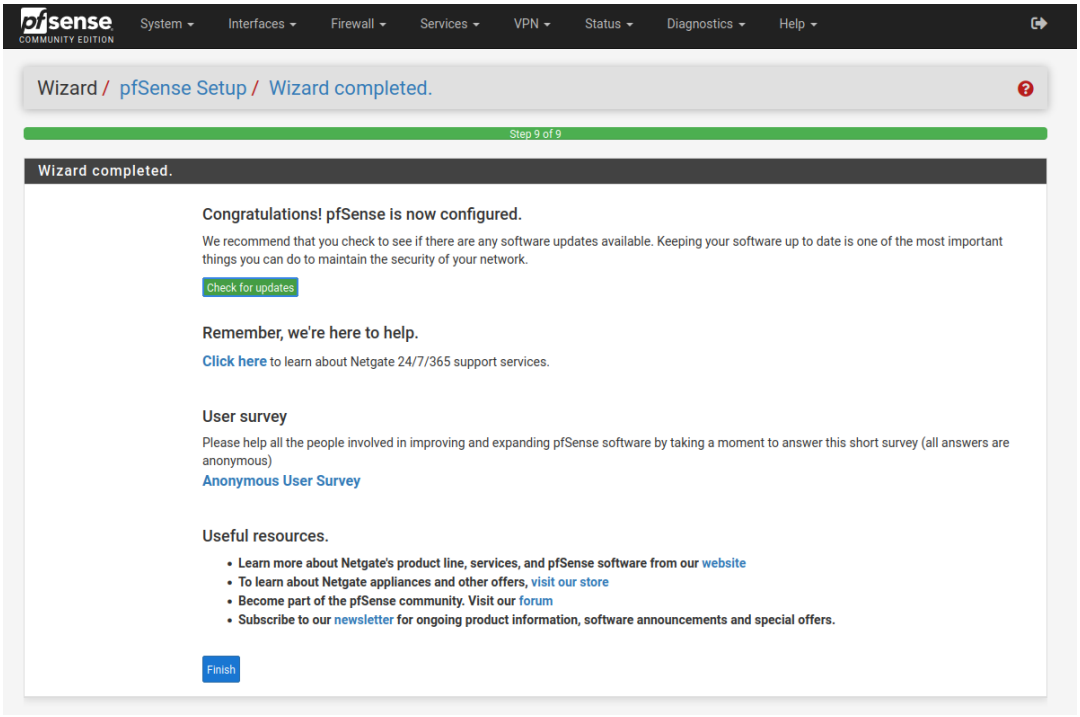
الشكل رقم ()

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

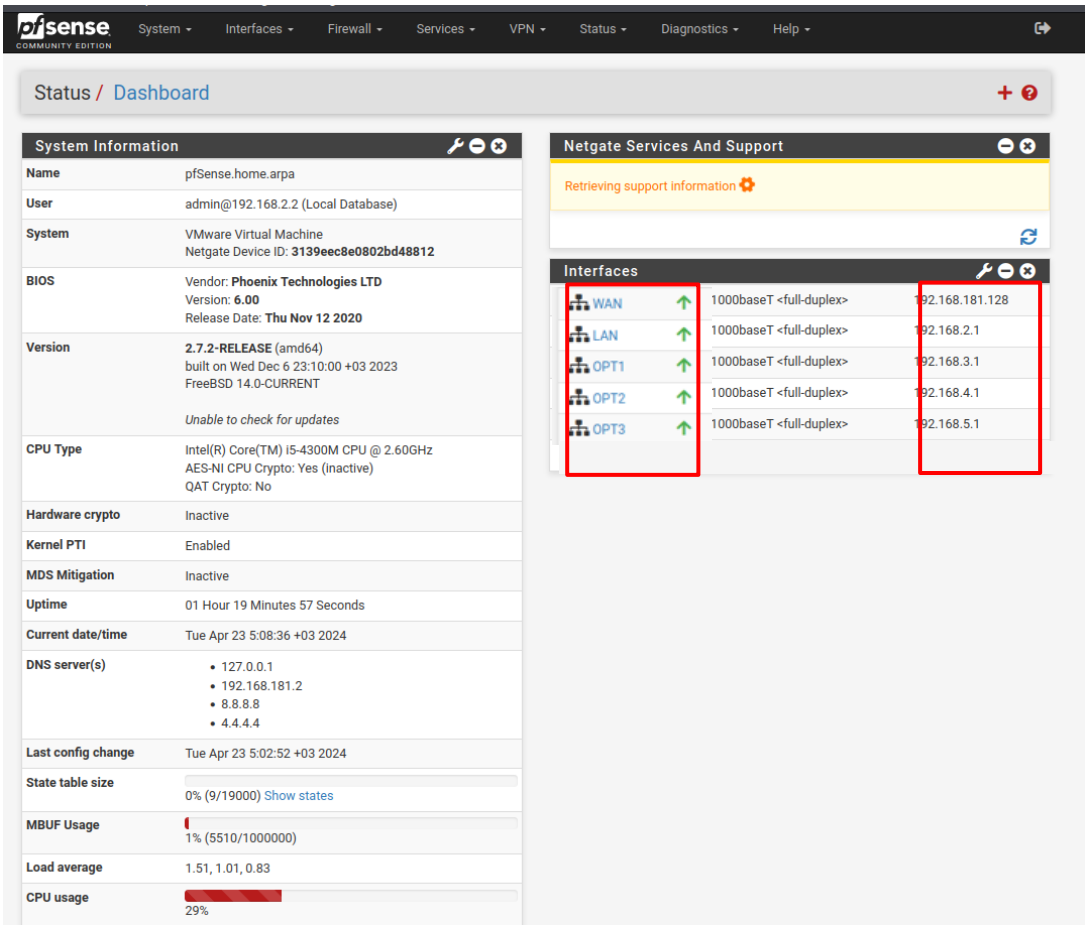


الشكل رقم ()

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

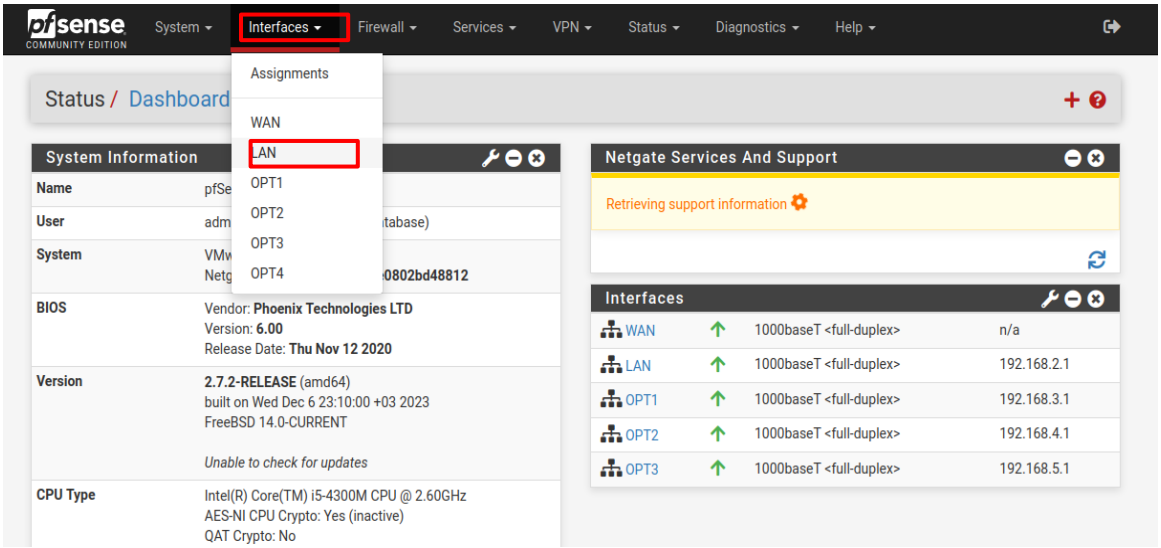


الشكل رقم ()



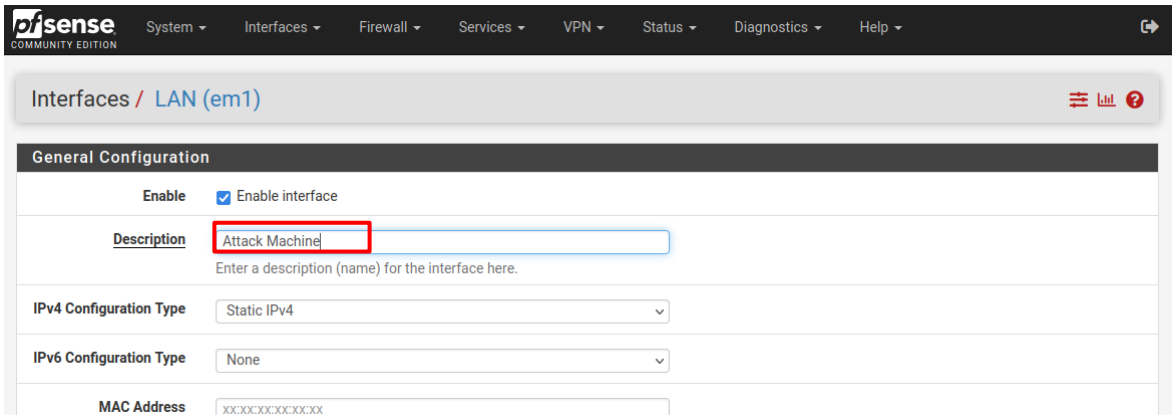
الشكل رقم ()

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



الشكل رقم ()

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



الشكل رقم ()

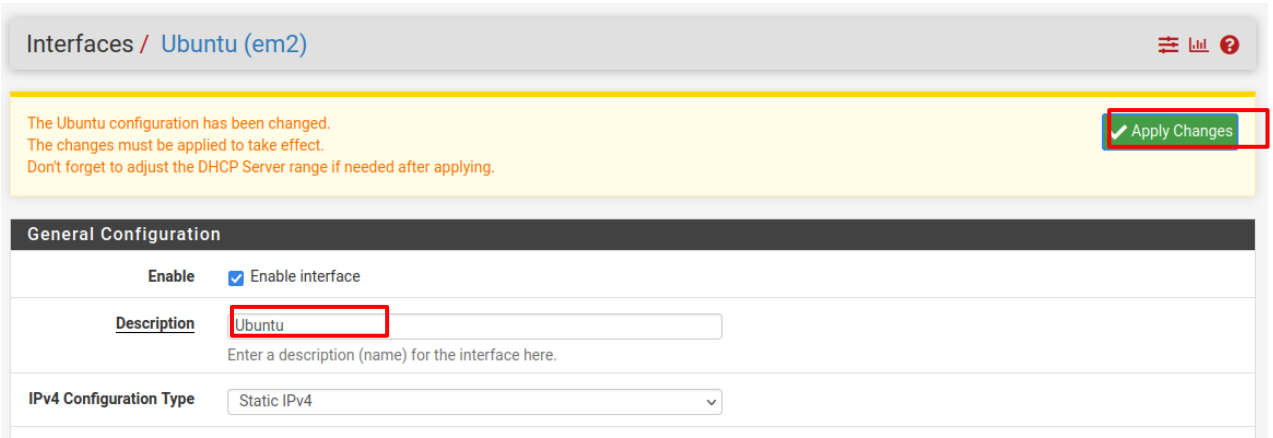
ملاحظة سيتم عمل نفس الشيء مع الواجهات الأخرى

OPT1 = Ubuntu

OPT2 = AD DS

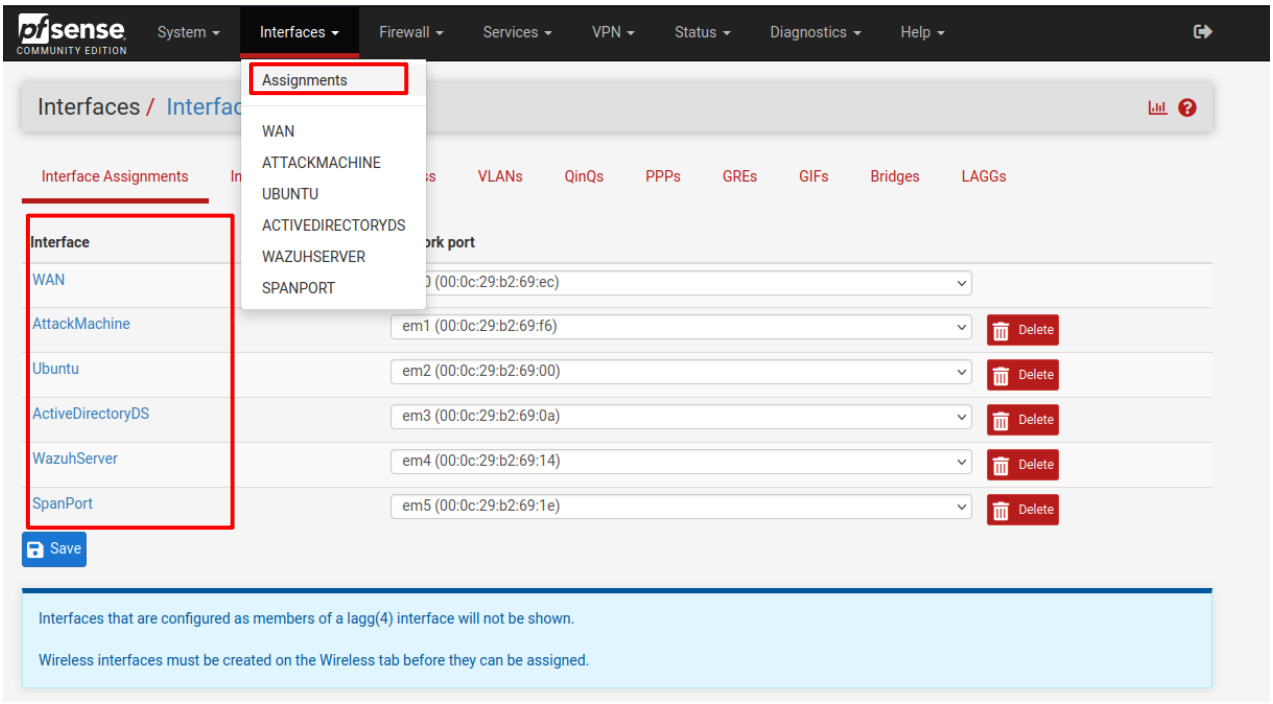
OPT3 = SIEM

OPT4 = Span Port



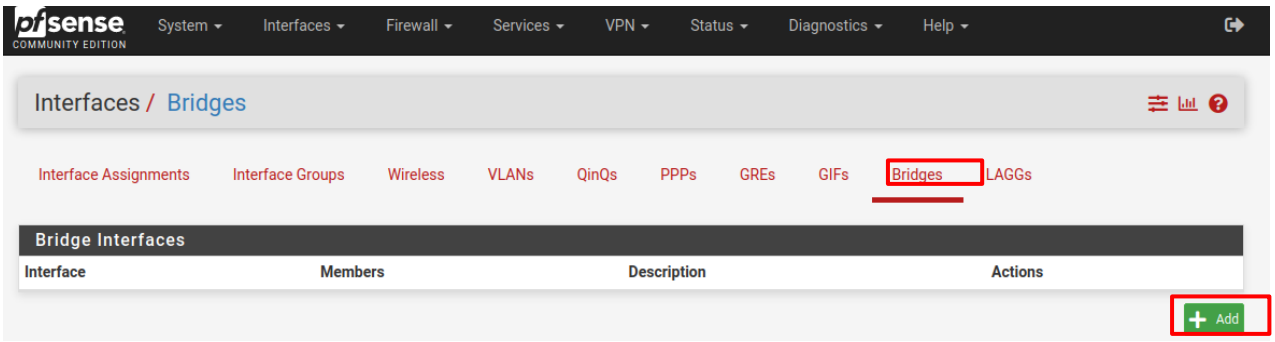
الشكل رقم ()

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



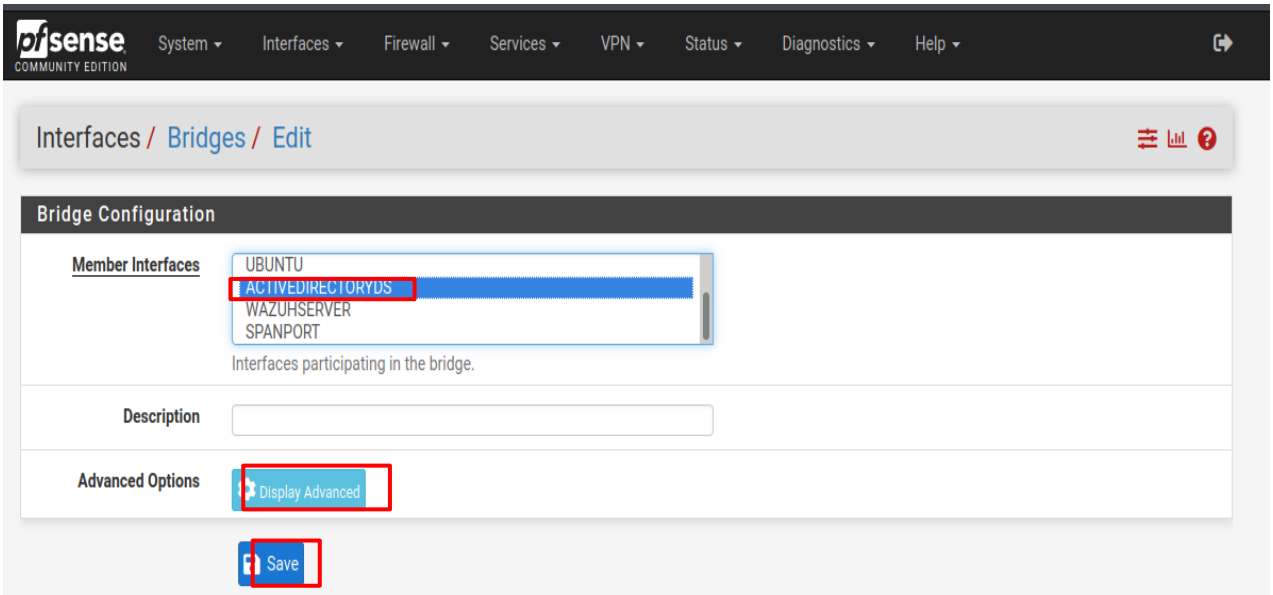
الشكل رقم ()

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 الواجهات، وانقر على **Brides**



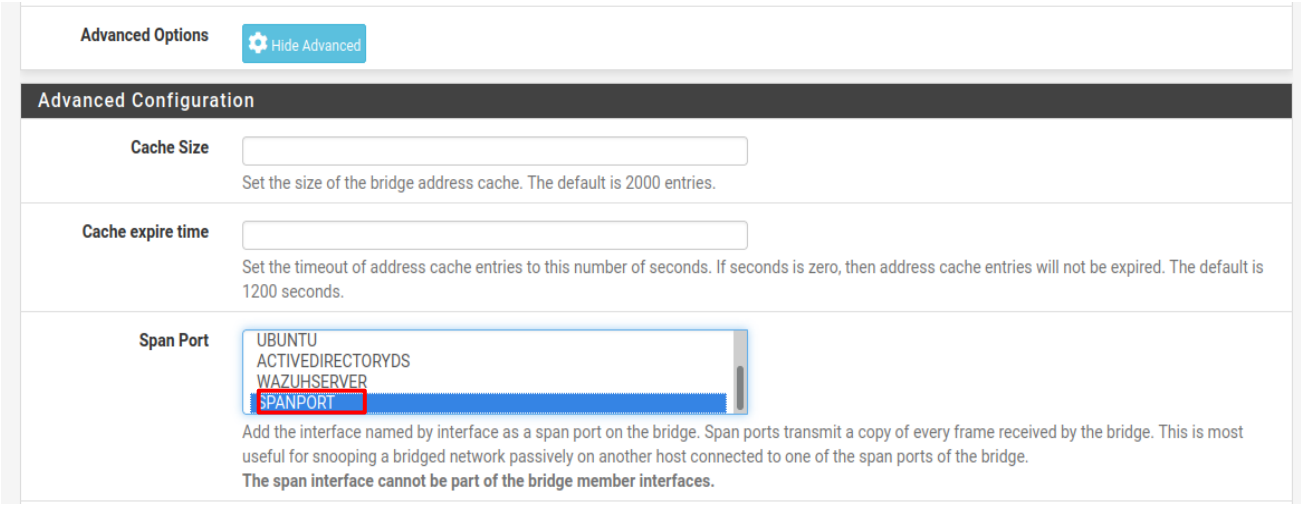
الشكل رقم ()

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



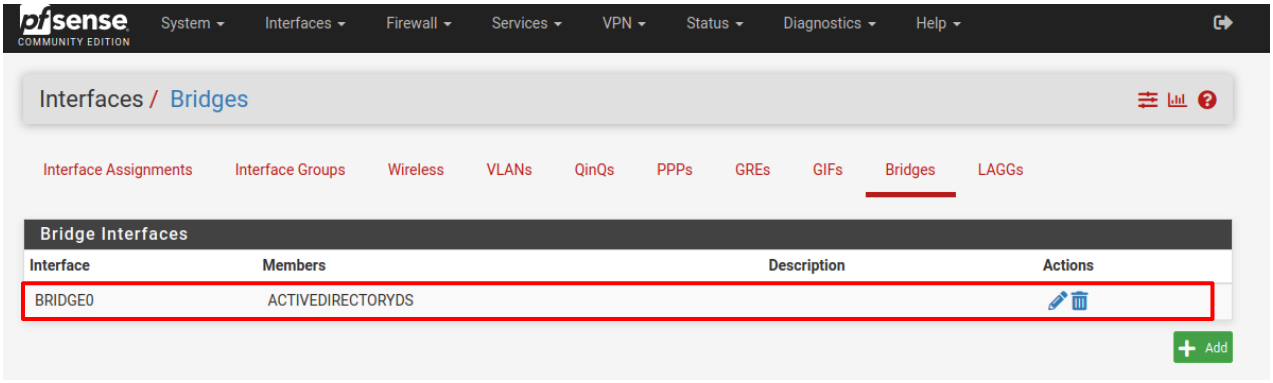
الشكل رقم ()

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



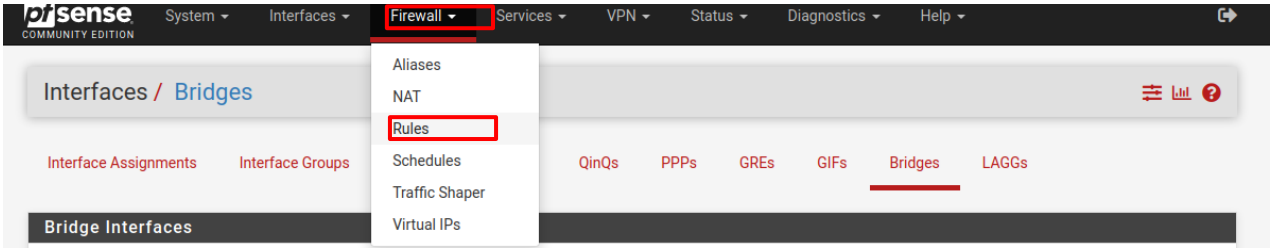
الشكل رقم ()

سيكون بهذا الشكل بعد الانشاء



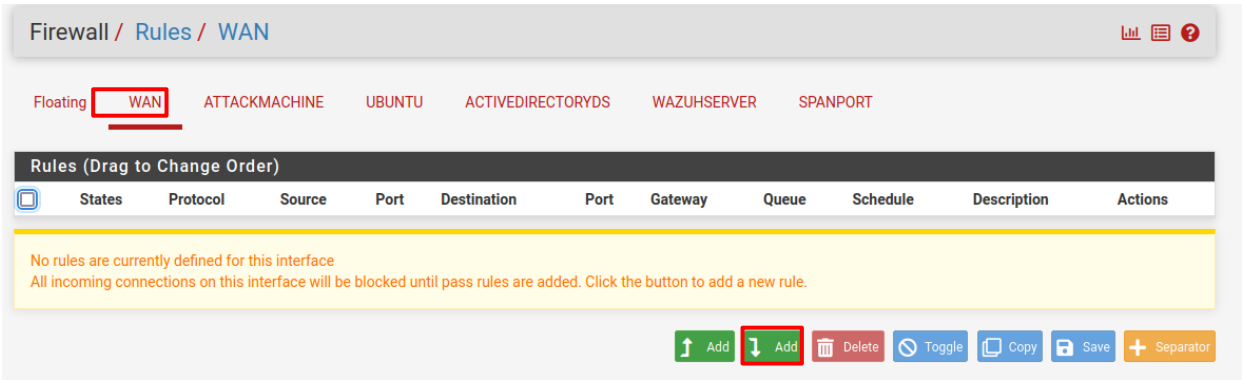
الشكل رقم ()

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



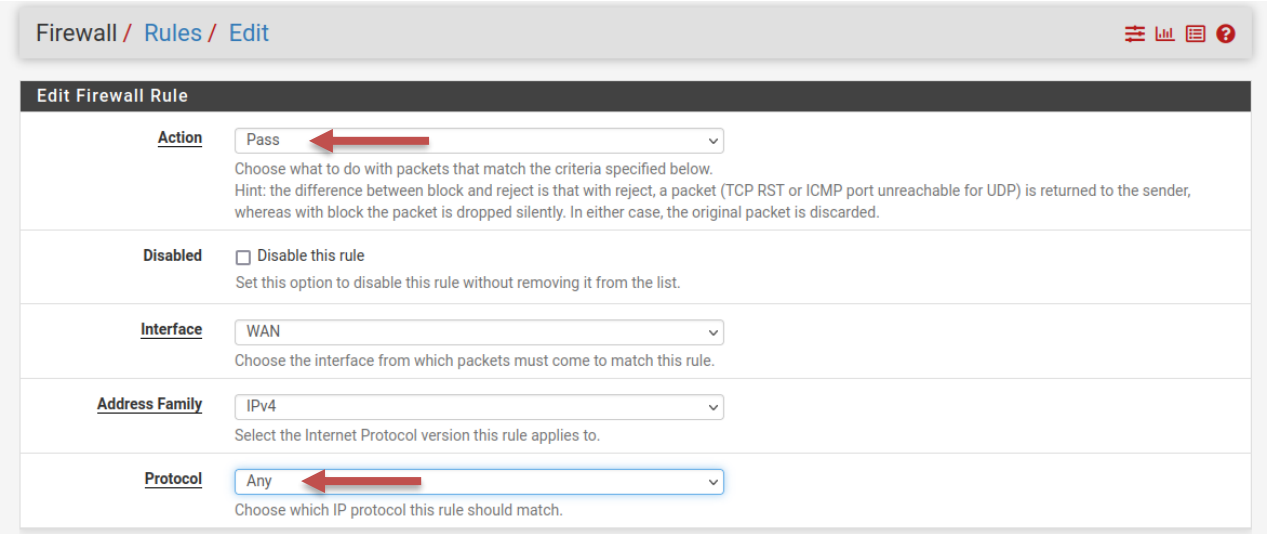
الشكل رقم ()

ثم حدد **الشبكة** wan > **Add**



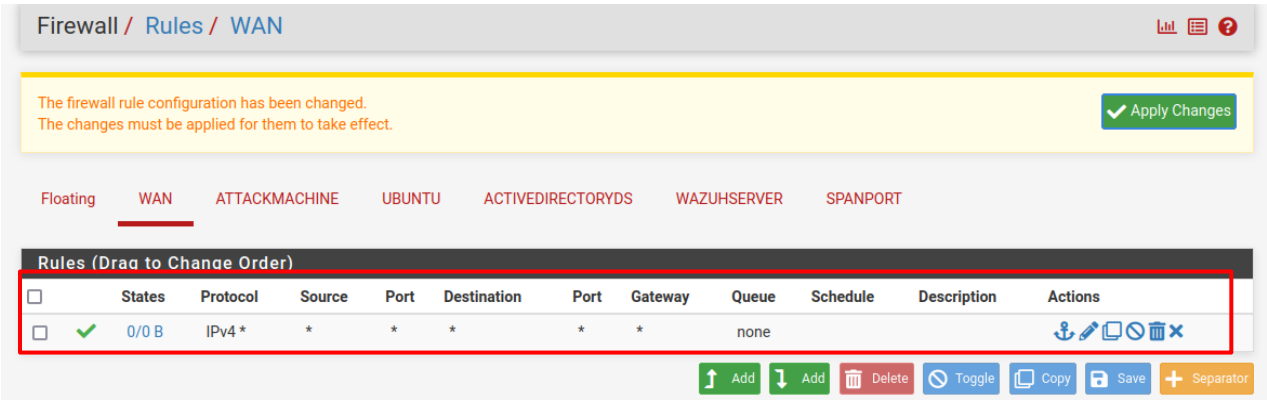
الشكل رقم ()

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



الشكل رقم ()

بعد الإضافة والحفظ سيكون بشكل التالي



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

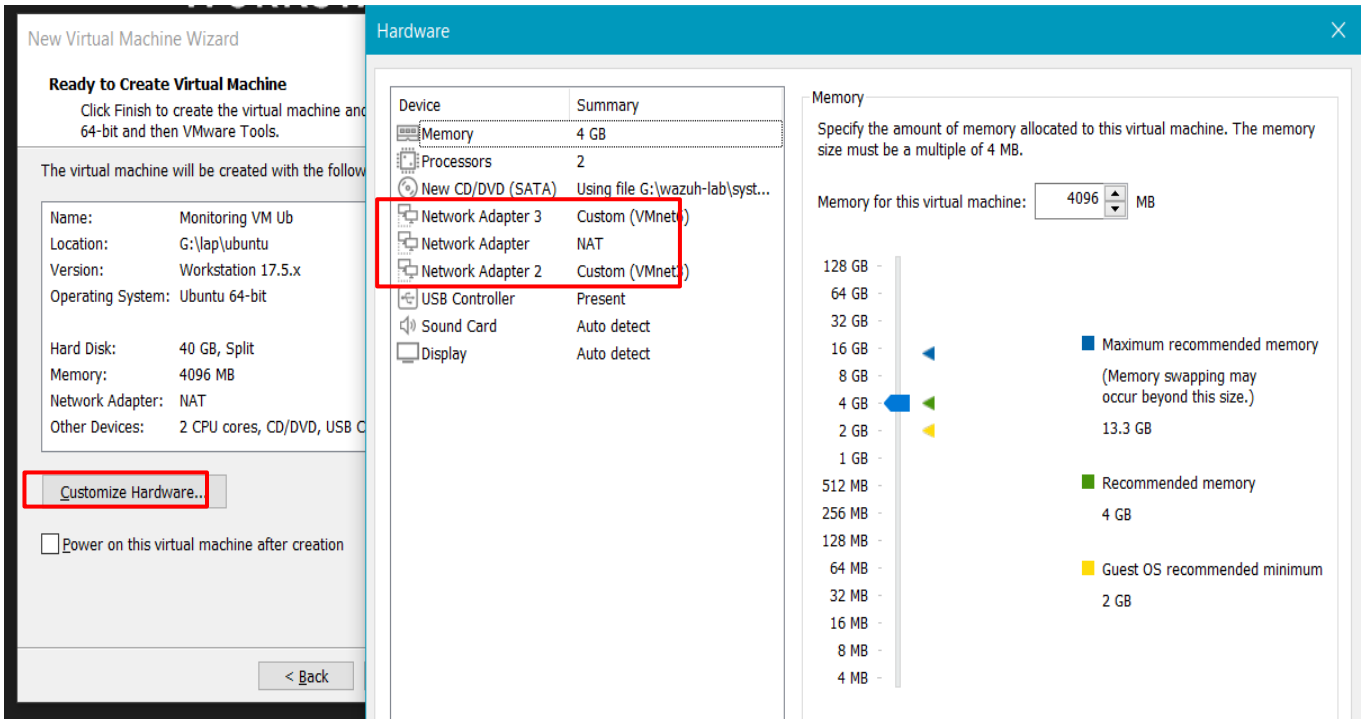
٥,٢,٤. يتم تثبيت في هذي المرحلة نظام ubuntu

الآن، الخطوة العبقرية؟ 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 لاحقًا في السلسلة. سنقوم أيضًا بتثبيت **Wireshark** الذي سيمكننا من التعرف على الشبكة لجميع حركة المرور الصادرة والواردة. دعونا أولا نقوم بتثبيت نظام **ubuntu**

نقوم بنفس عمليه التثبيت الذي نحن نعرفها ونقوم بها دائما، ولكن سنضيف بعض التخصيص **customize** في **network adapter**، ثم بعد ذلك أيضا نقوم بعمليه التثبيت المعروفة



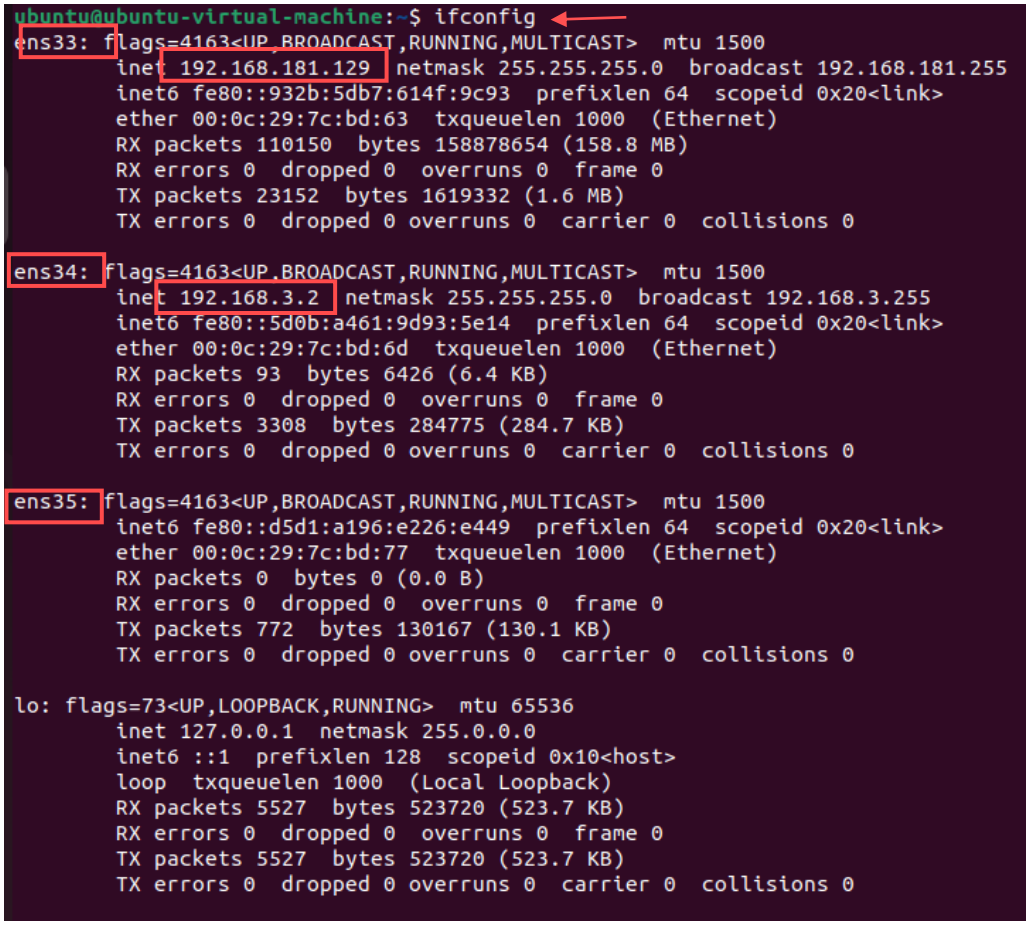
الشكل رقم ()

بعد عمليه التثبيت نقوم بدخول الى النظام. الآن بعد الدخول نحن بحاجة إلى التحقق من واجهاتنا لتعيين .IP قم بتشغيل المحطة، واكتب ***sudo apt install net-tools***.

```
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.



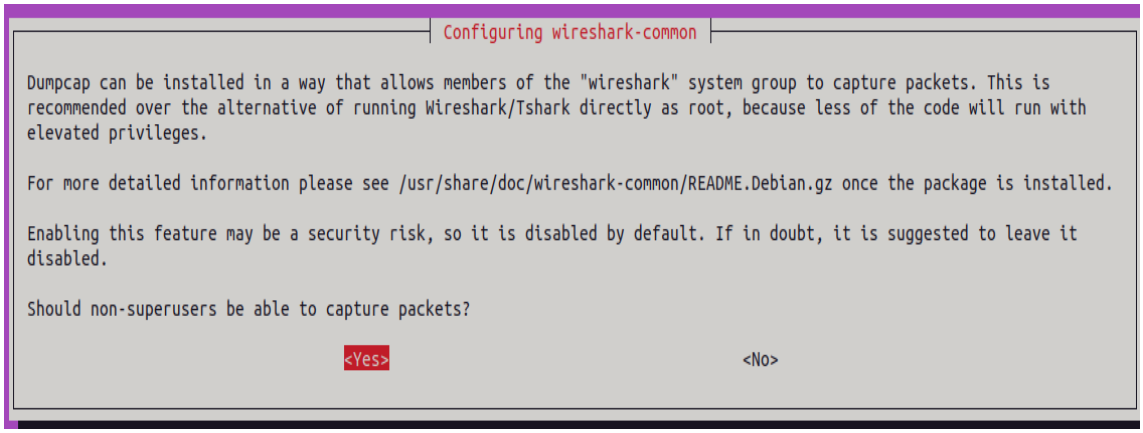
الشكل رقم ()

الى هنا نكون قد اتممنا تثبيت ubuntu، التالي هو تثبيت Wireshark للاستنشاق sniffing. قم بتغيير الدليل إلى المجلد **/opt/** cd لتثبيت الأداة. ثم اكتب **sudo apt install–wireshark–qt**

```
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 libqt5multimediagsttools5 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 libqt5multimediagsttools5 l
  libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl libsnappy1v5
  libwireshark15 libwiretap12 libwsutil13 libxcb-xinerama0 libxcb-xinput0
  wireshark-common wireshark-qt
```

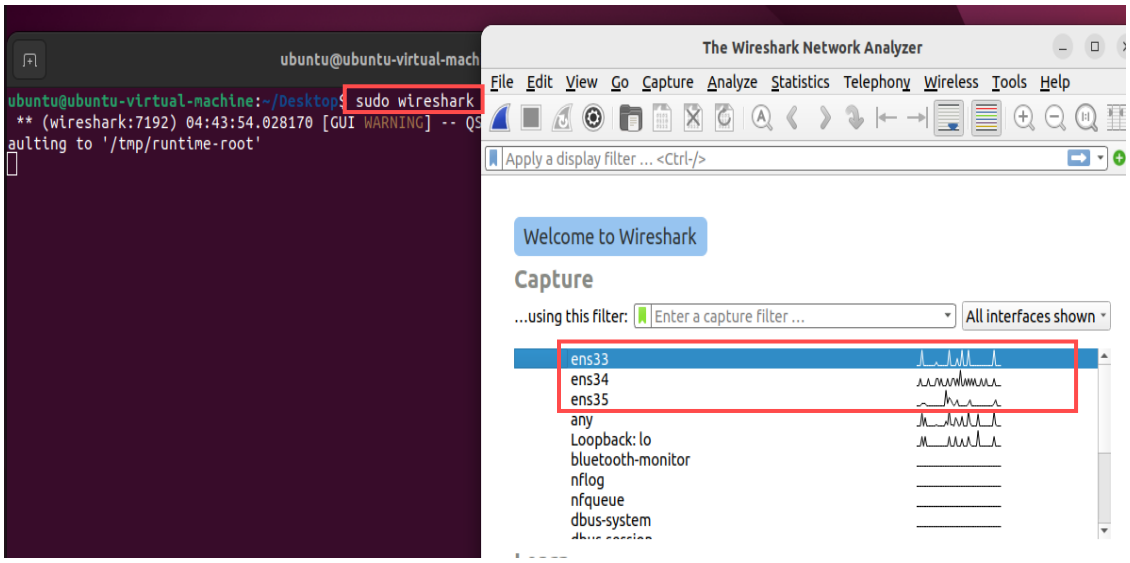
الشكل رقم ()

ثم نحدد **yes** للموافقة على الحزمة والتثبيت



الشكل رقم ()

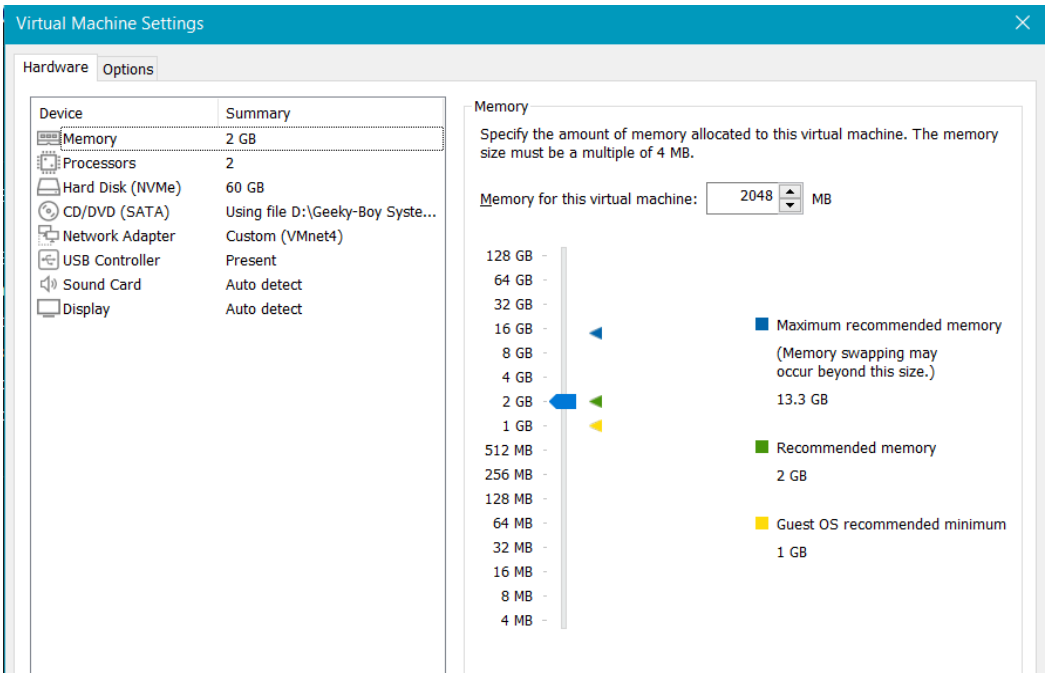
بمجرد اكتمال التثبيت، انتقل إلى المحطة الطرفية واكتب sudo **wireshark**. سوف تحصل على مطالبة بإدخال **كلمة المرور** الخاصة بك. بعد تسجيل الدخول بنجاح، يجب أن تظهر نافذة Wireshark بكل الواجهات المتاحة. هنا، واجهة الاستنشاق sniffing أو **span port** المنفذ الممتد هي **ens34**.



الشكل رقم ()

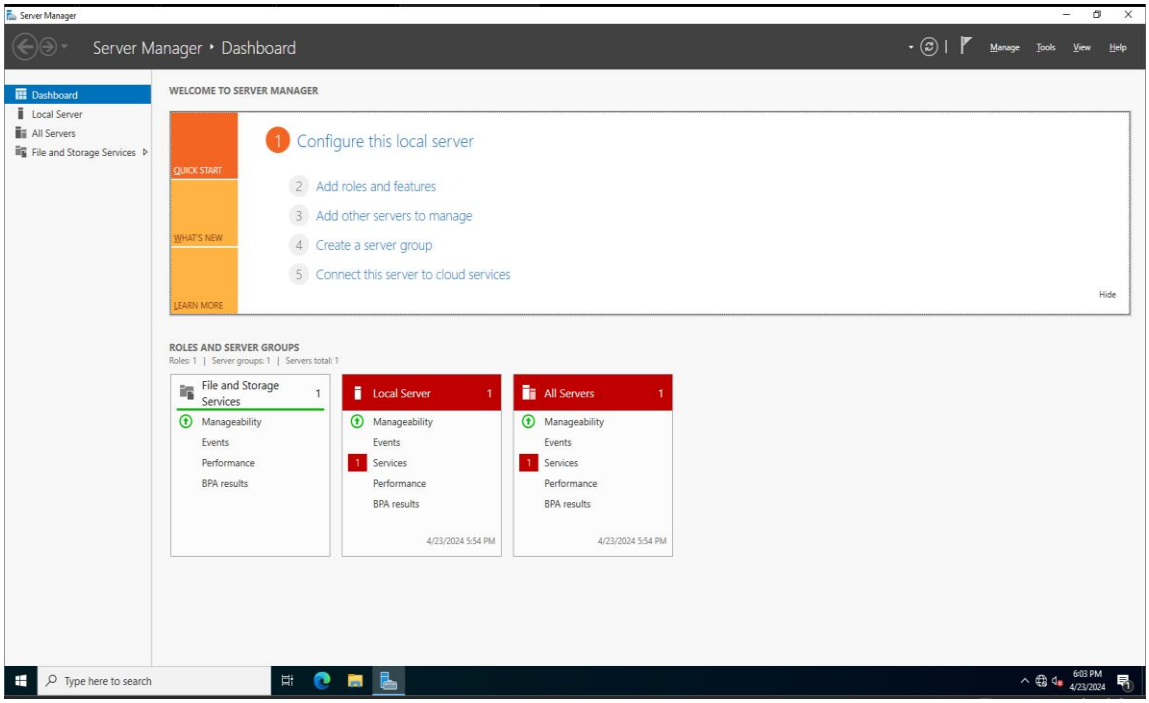
٥,٢,٥. تثبيت WINDOWS SERVER

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 ونبدأ بتكوين النظام



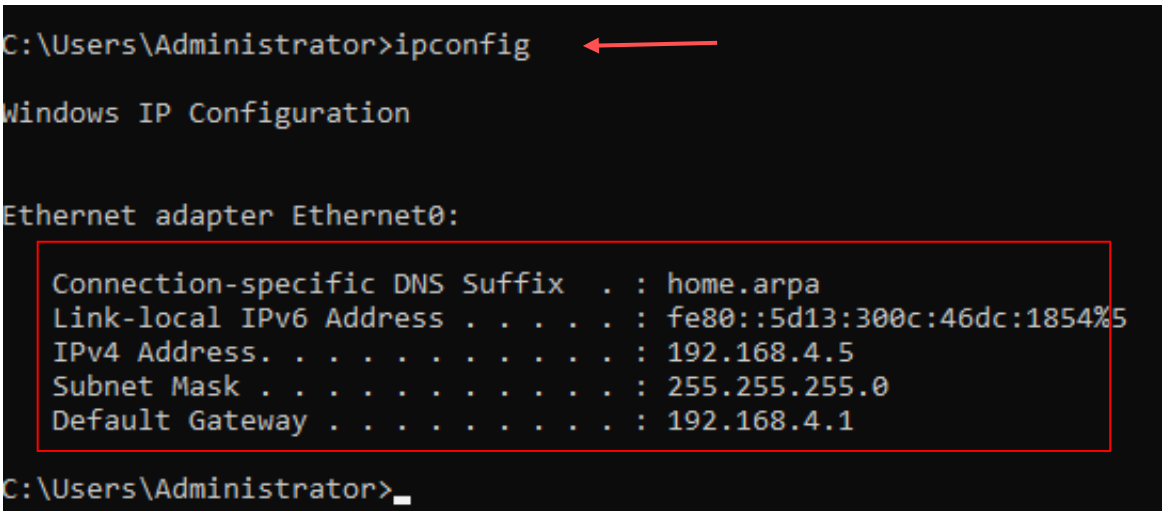
الشكل رقم ()

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



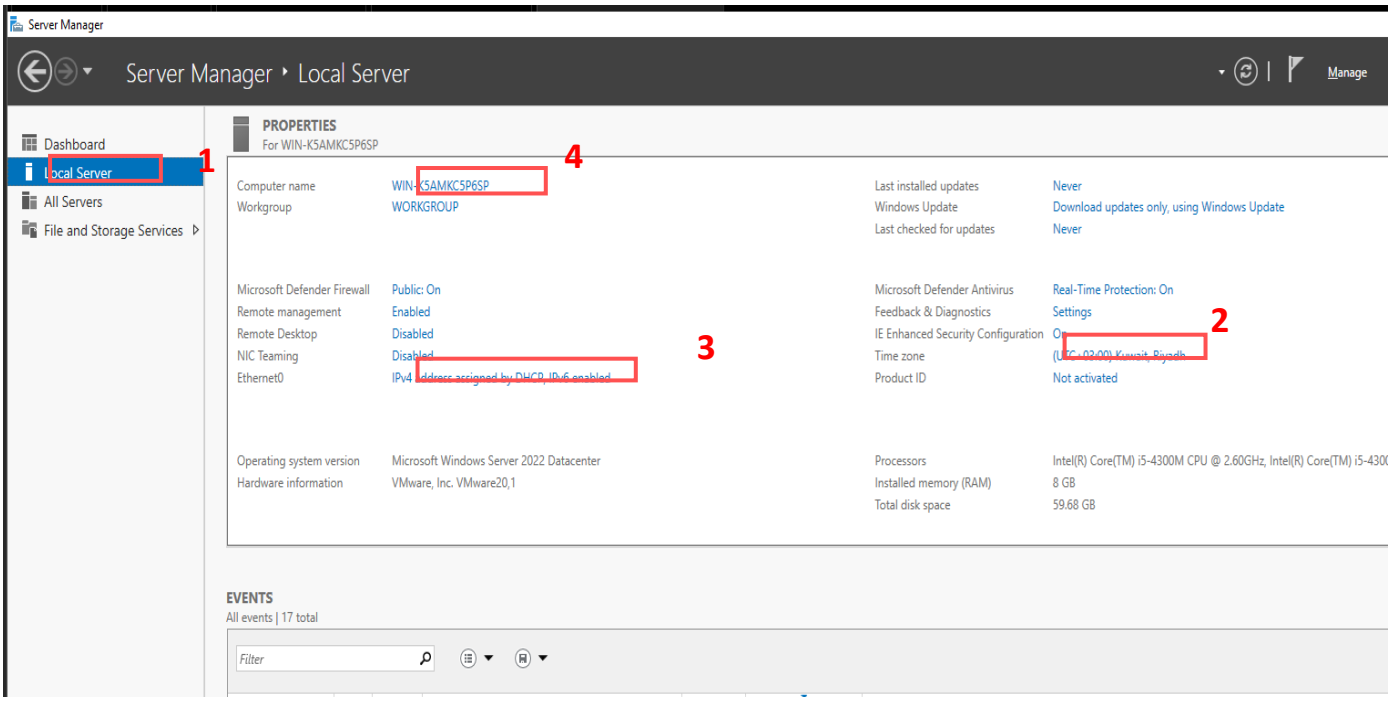
الشكل رقم ()

للتحقق من أن تكوين DHCP الخاص بنا على واجهة ADDS يعمل، نقوم بتشغيل cmd واكتب **ipconfig** يجب أن تشير الإعدادات إلى أن DHCP الخاص بنا يعمل بشكل جيد.



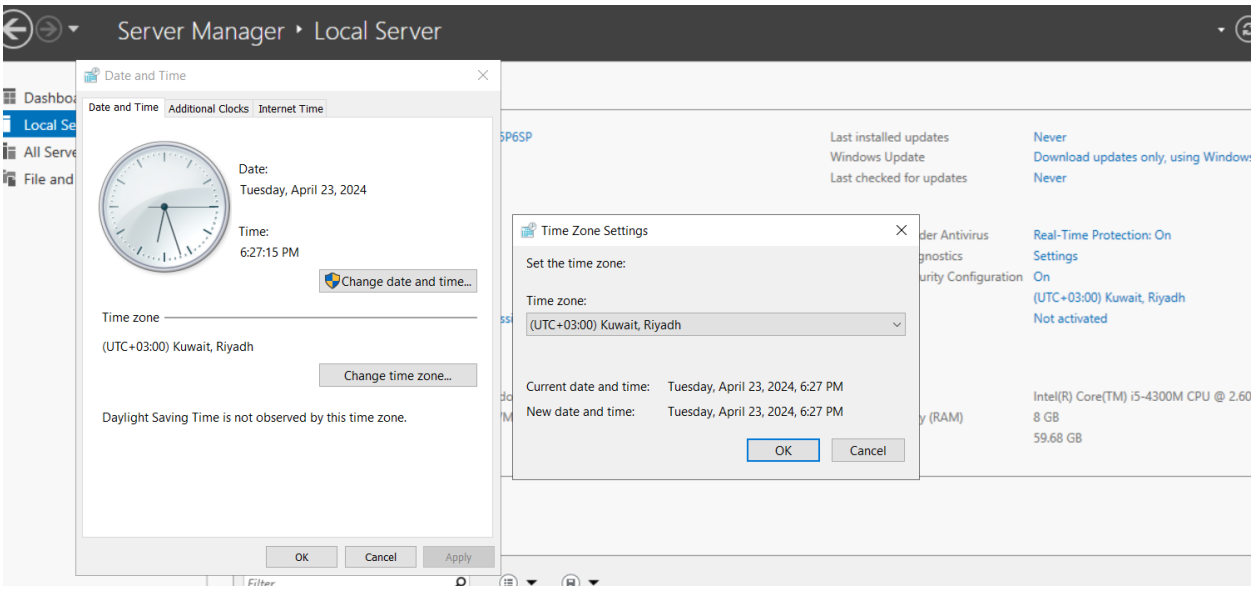
الشكل رقم ()

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



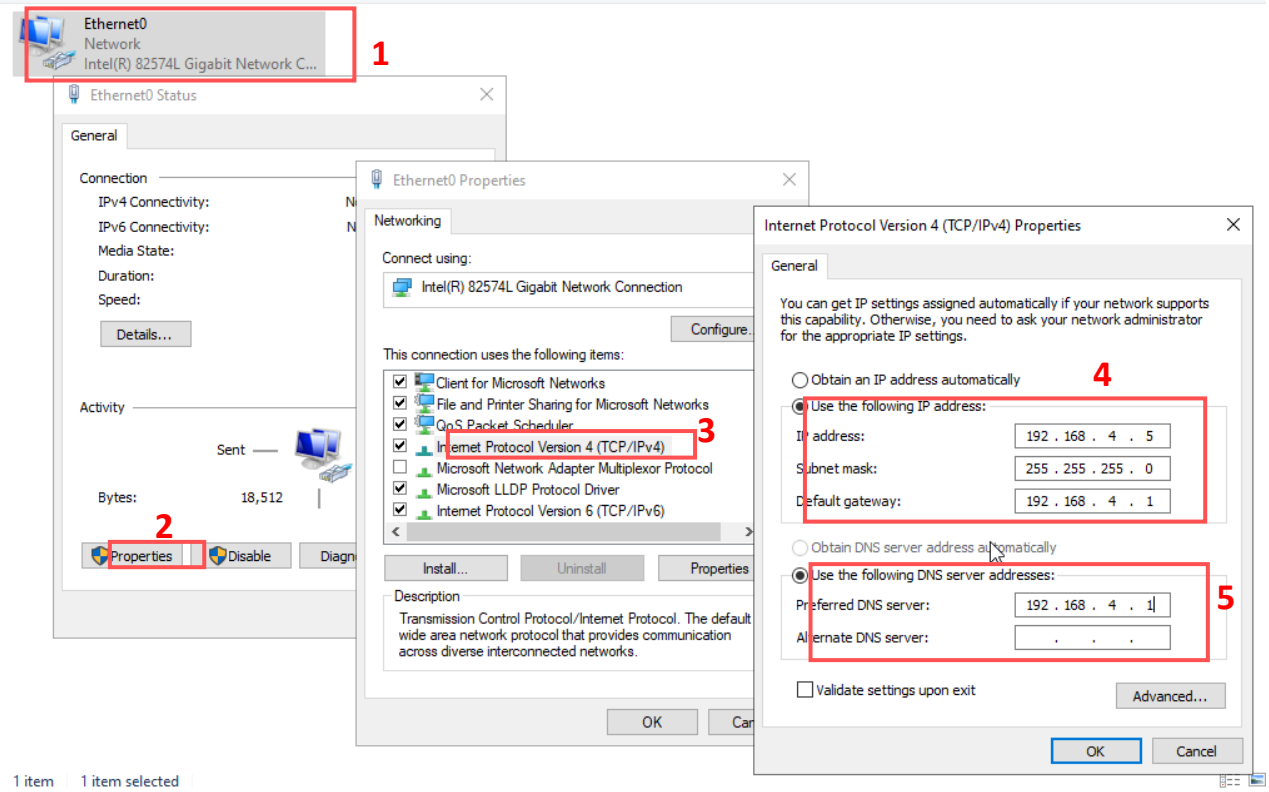
الشكل رقم ()

الأول هو تغيير إعدادات المنطقة الزمنية. انقر فوق ***تغيير المنطقة الزمنية*** ***< UTC حموافق.***



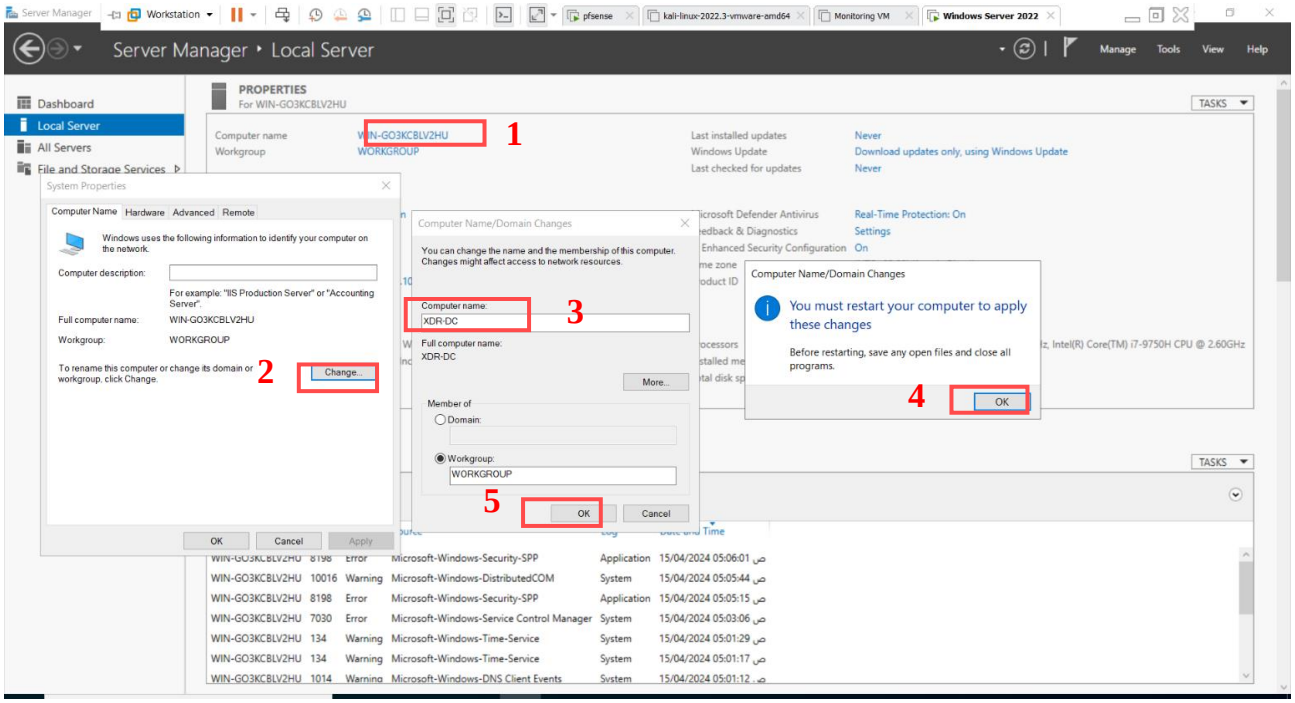
الشكل رقم ()

ثانيا، نقوم بتغيير إعدادات **Ethernet** أو **adapter** من وحدة تحكم مدير الخادم، انقر فوق عنوان **IP >** **Ethernt0 >** الخصائص **< TCP/IPv4 >** 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.



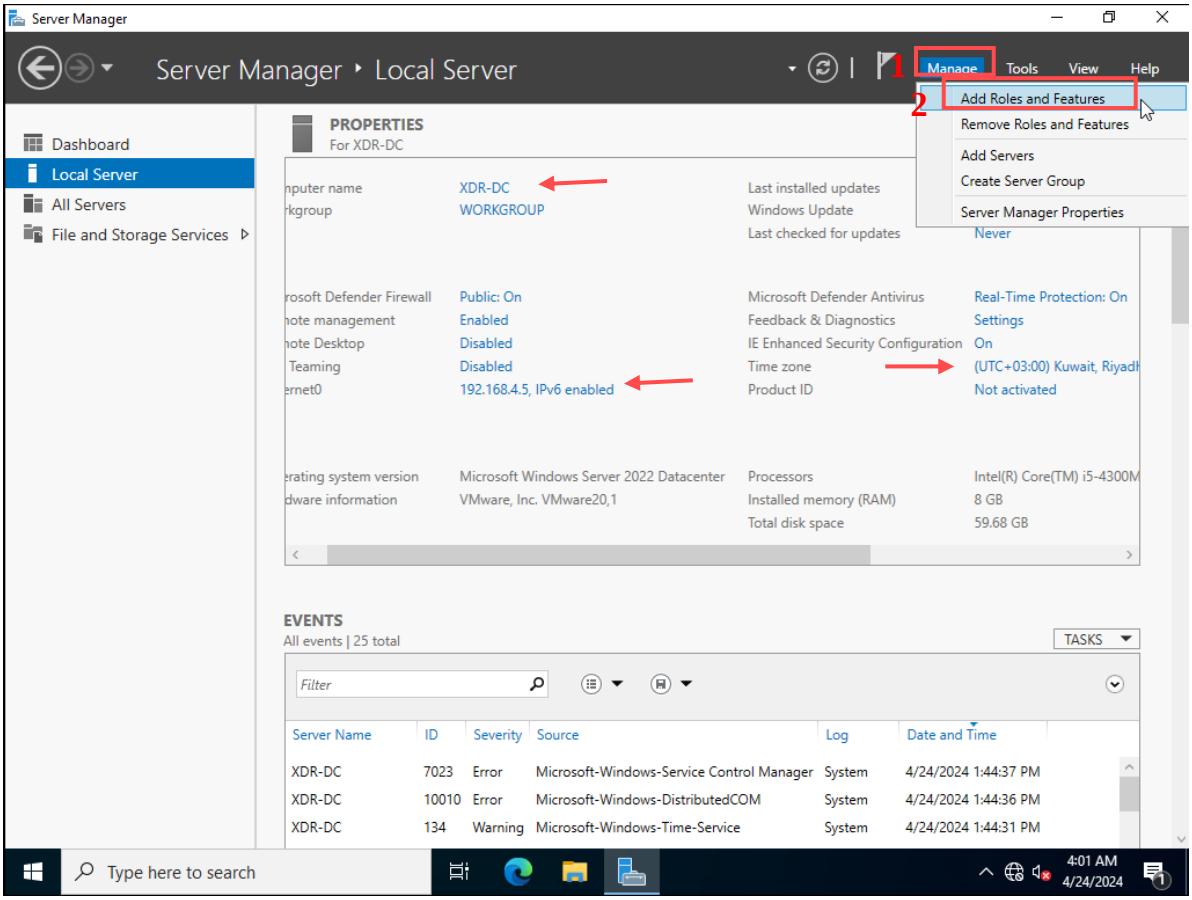
الشكل رقم ()

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.



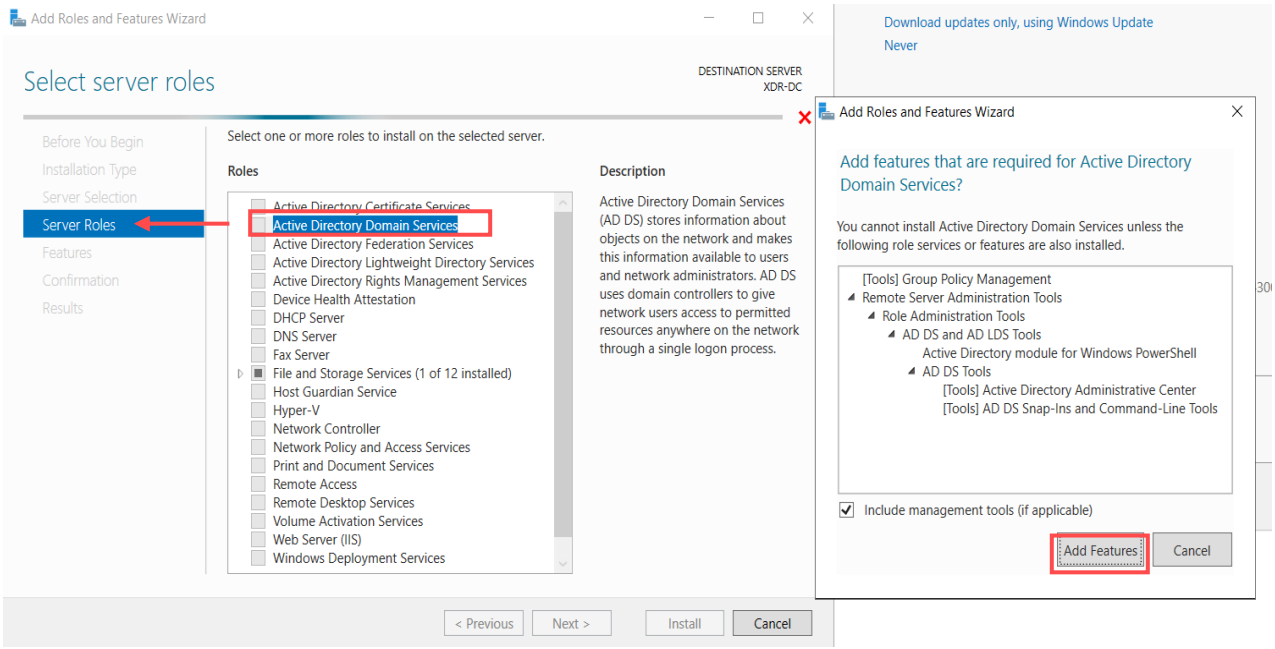
الشكل رقم ()

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 .سنقوم بتثبيت **AD AS** ك **role** في بيئتنا.



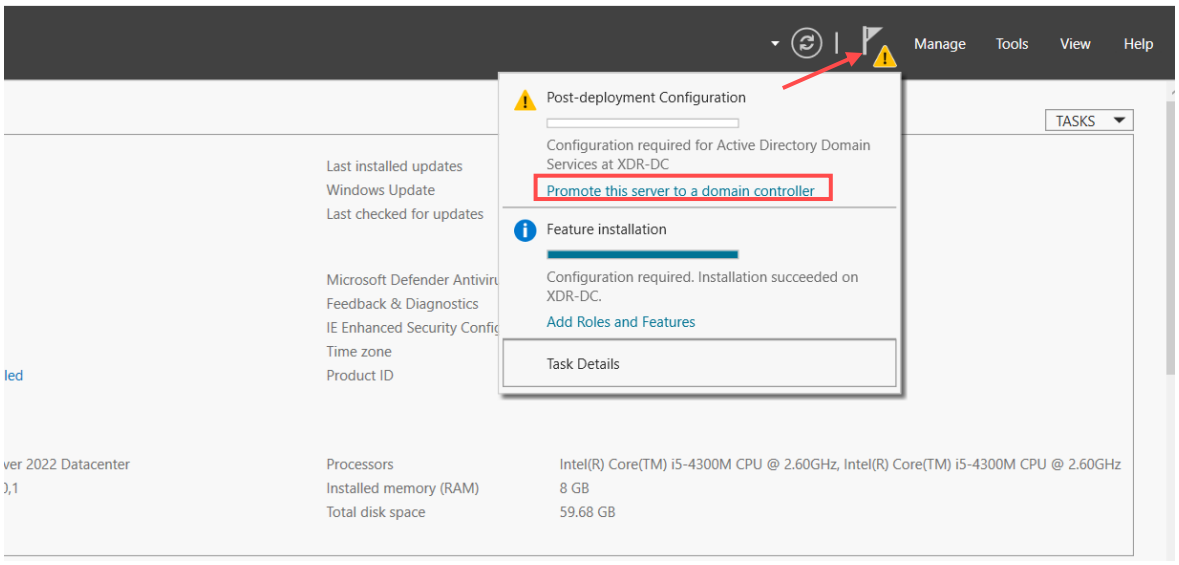
الشكل رقم ()

انقر فوق **التالي** ثلاث مرات لل server roles. حدد **مربع خدمات مجال Active Directory Domain Services box > Add Features** انقر على التالي ثلاث مرات **للتأكيد**.



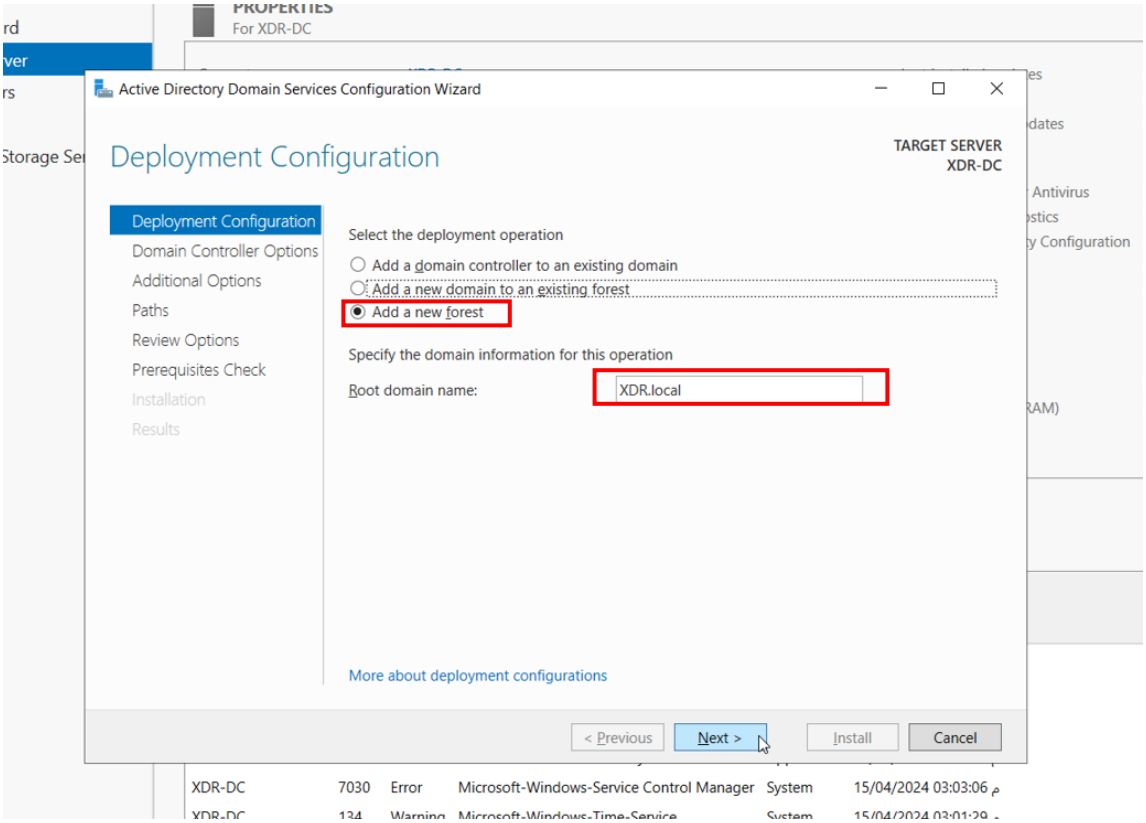
الشكل رقم ()

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



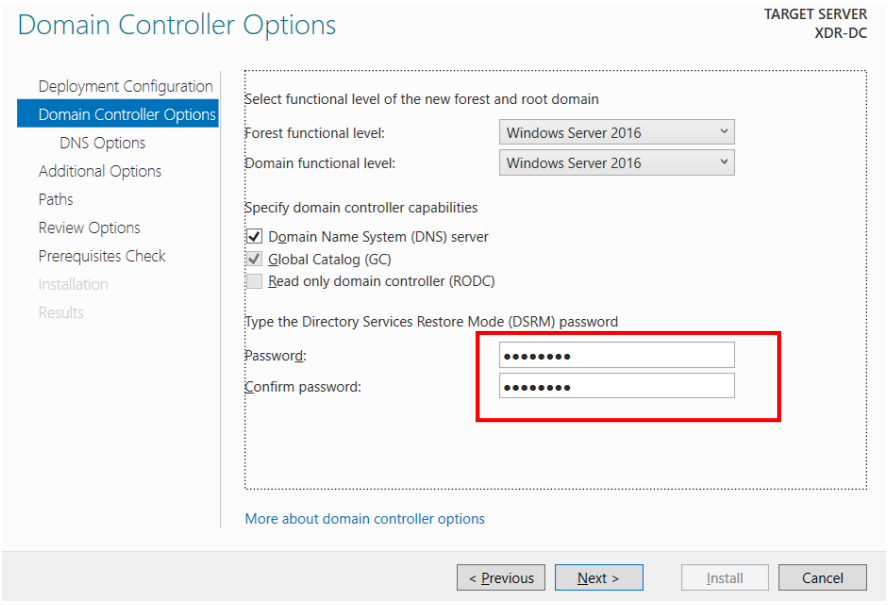
الشكل رقم ()

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



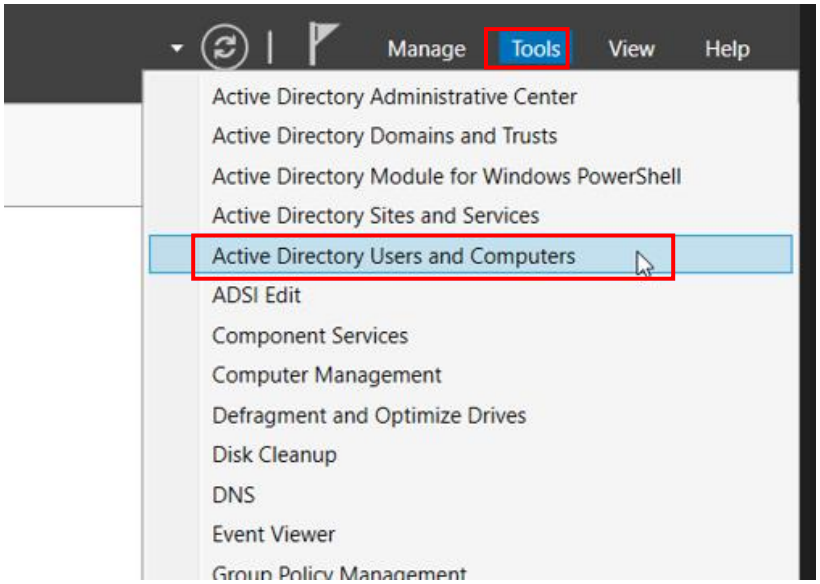
الشكل رقم ()

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



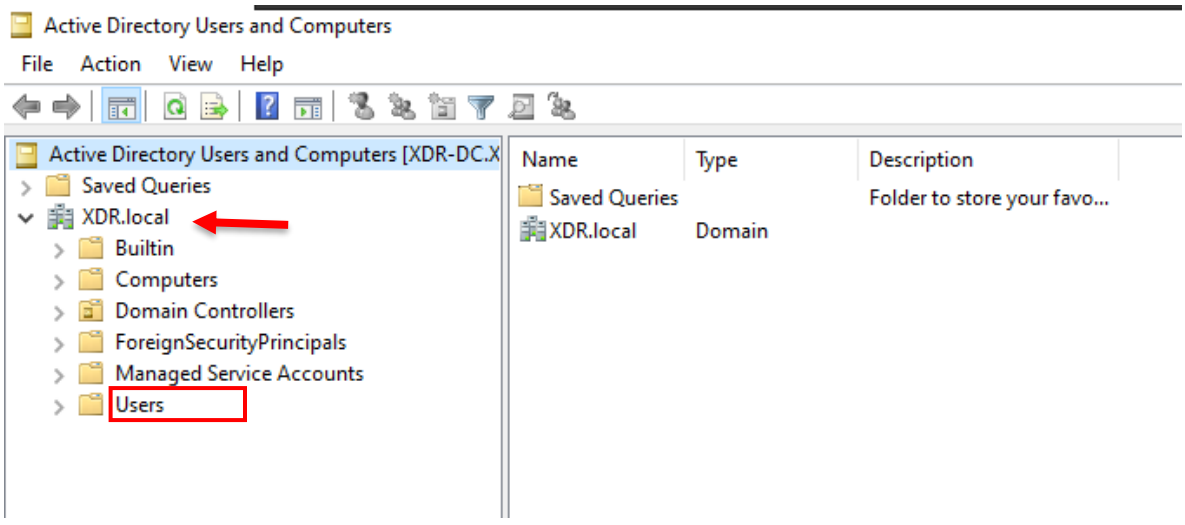
الشكل رقم ()

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



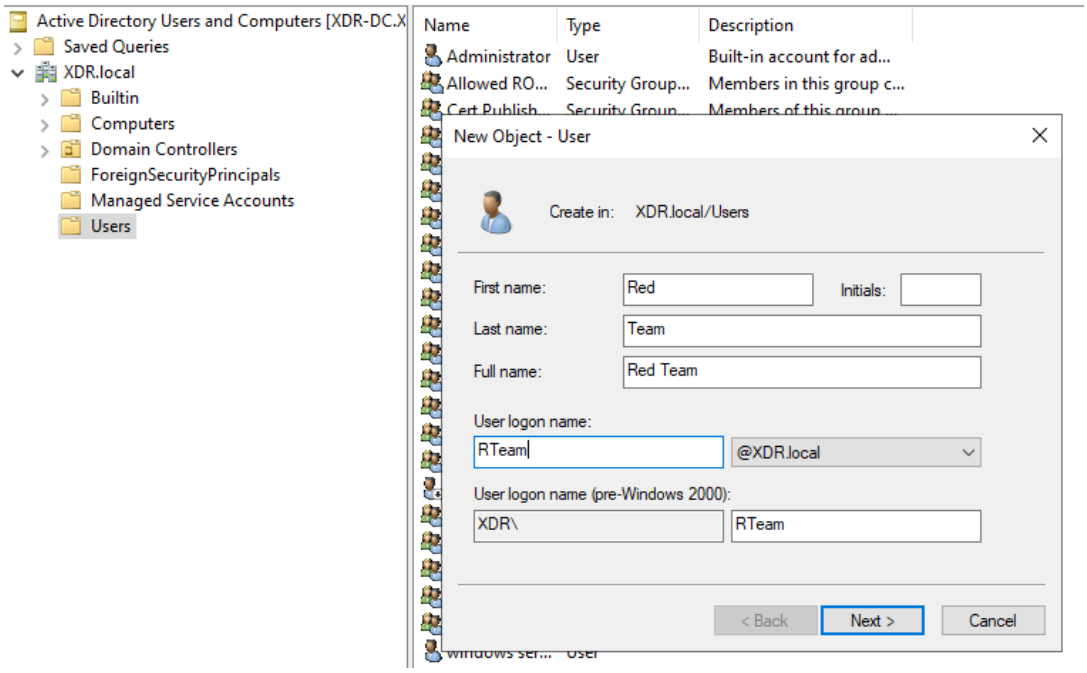
الشكل رقم ()

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



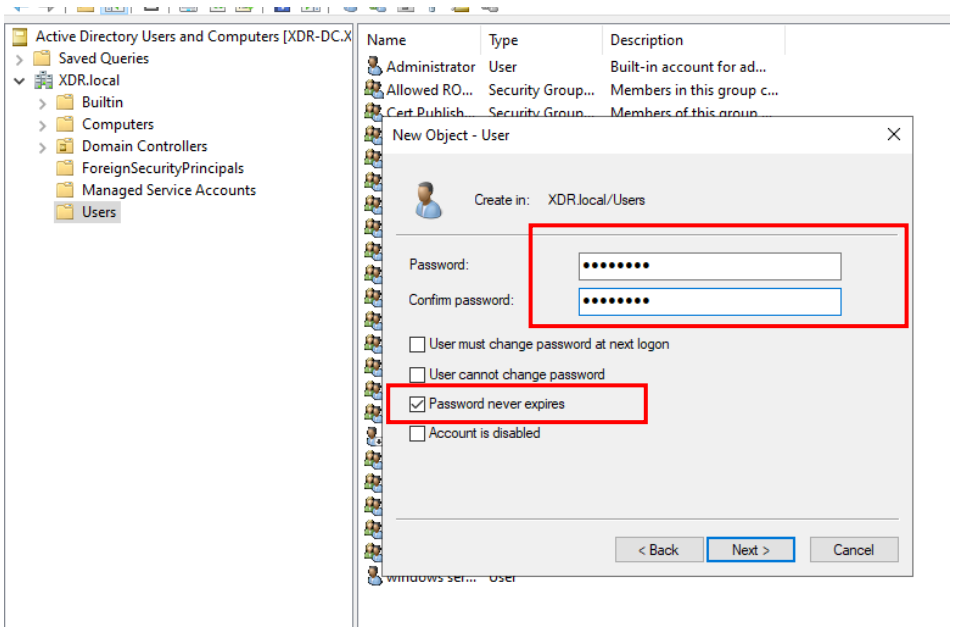
الشكل رقم ()

أنشئ اسم مستخدم



الشكل رقم ()

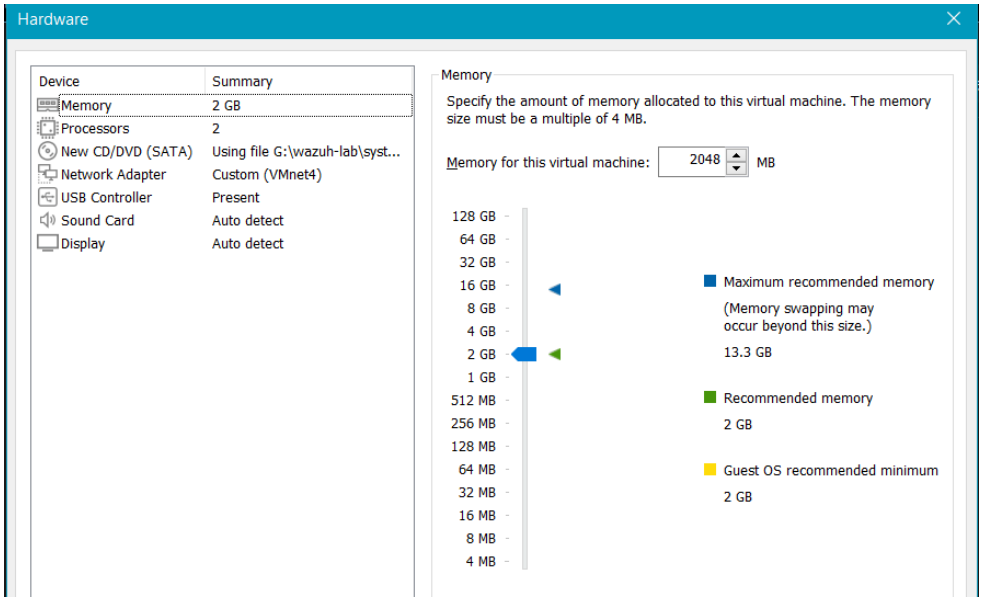
ثم أنشئ كلمة مرور، وحدد المربع "لا تنتهي صلاحية كلمة المرور مطلقًا" وانقر على **next** لقد نجحنا في إنشاء حساب مستخدم على الخادم الخاص بنا. يتعين علينا الآن إعداد جهاز عميل **Window** الخاص بنا وضمه إلى وحدة تحكم المجال الخاصة بنا.



الشكل رقم ()

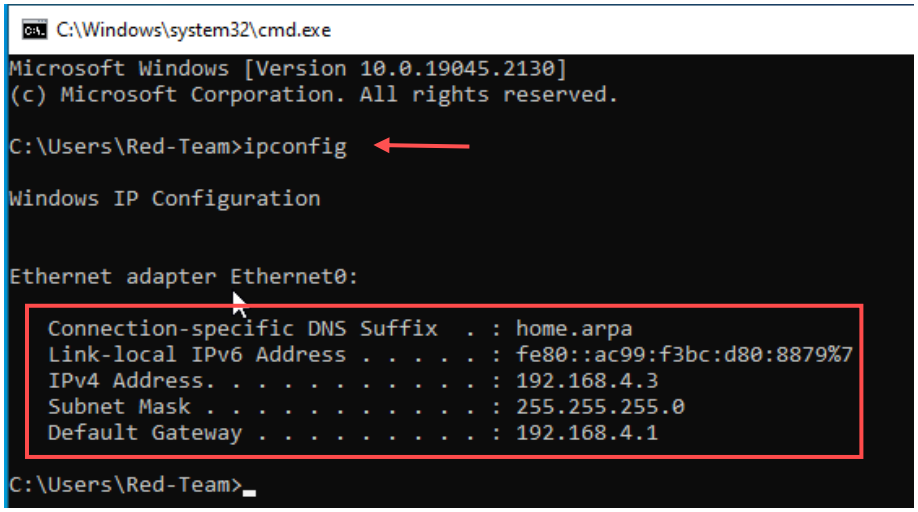
٥,٢,٦. تثبيت عميلWindows

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 machineونبدأ بتكوين النظام



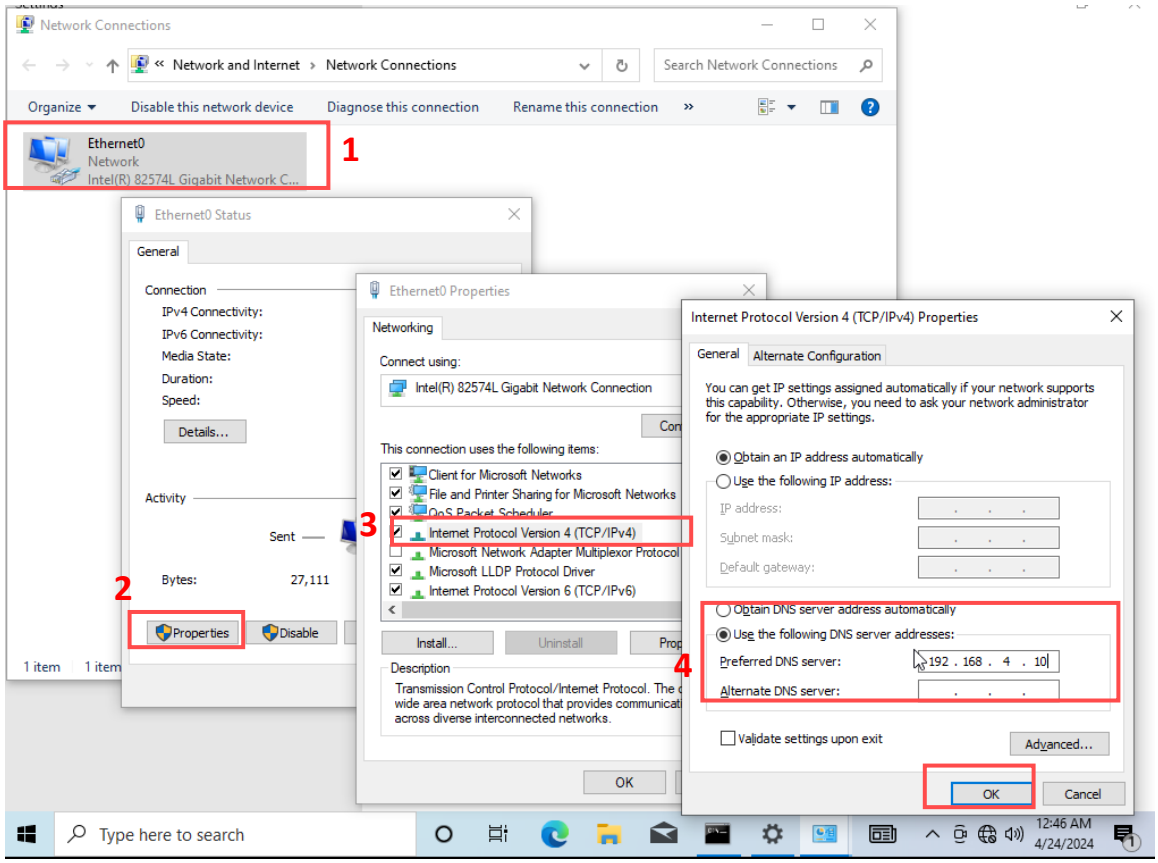
الشكل رقم ()

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



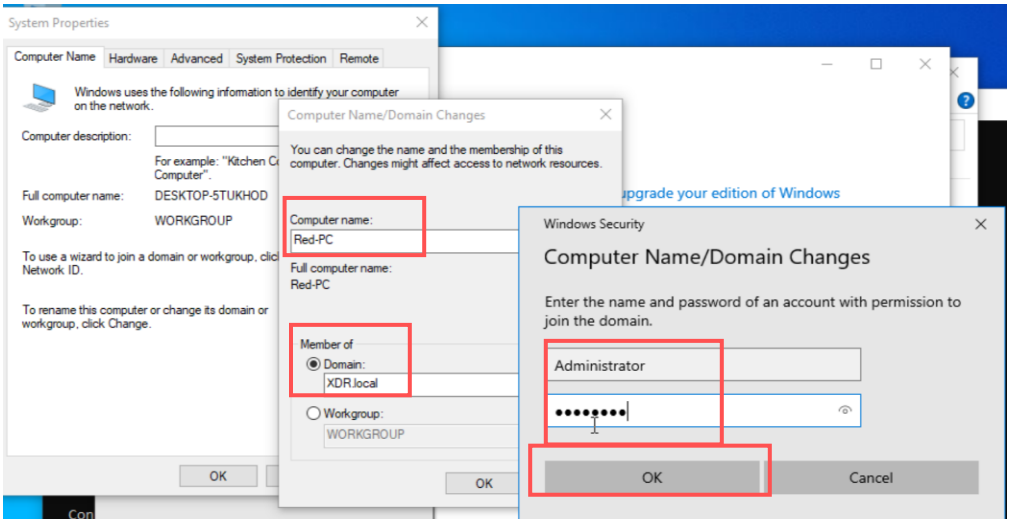
الشكل رقم ()

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



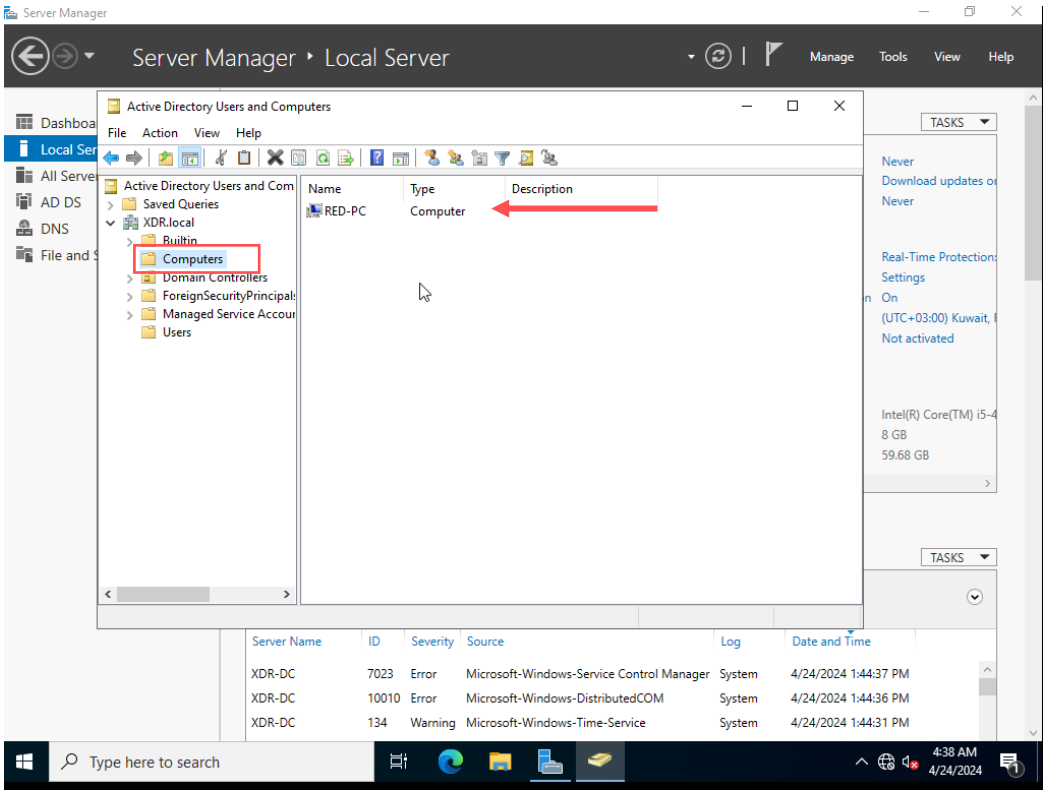
الشكل رقم ()

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.



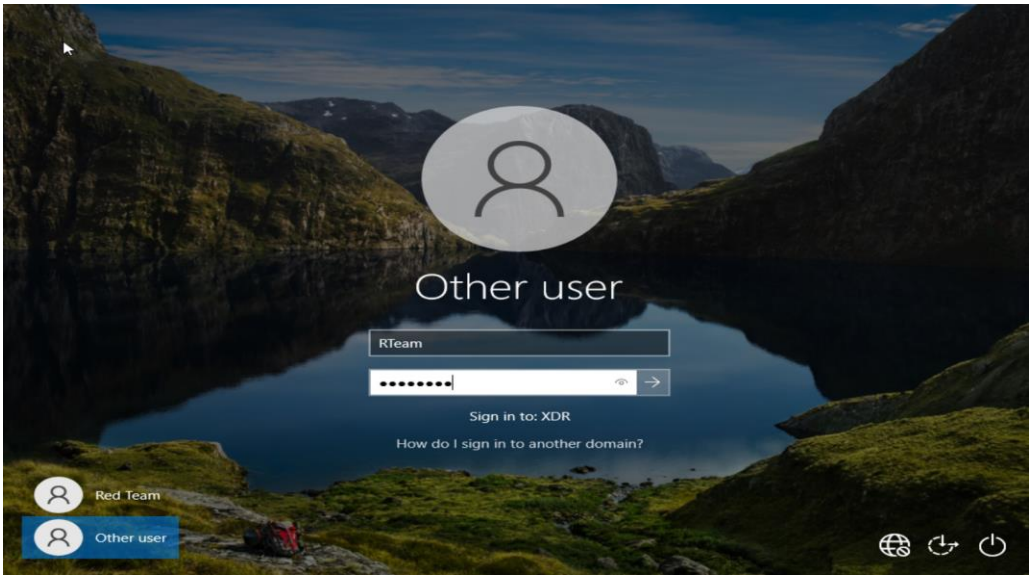
الشكل رقم ()

بالنسبة لـPoC ، 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.



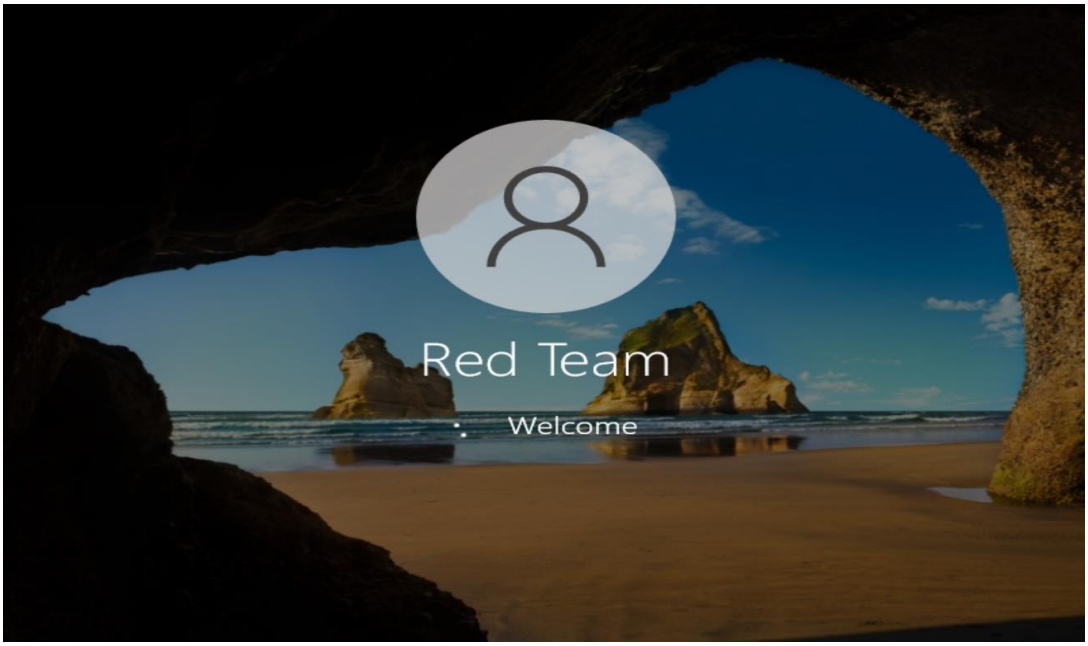
الشكل رقم ()

وأخيرًا، قم بتسجيل الدخول إلى جهاز العميل عن طريق إدخال بيانات اعتماد المستخدم (RTeam) وكلمة المرور P@$$w0rd



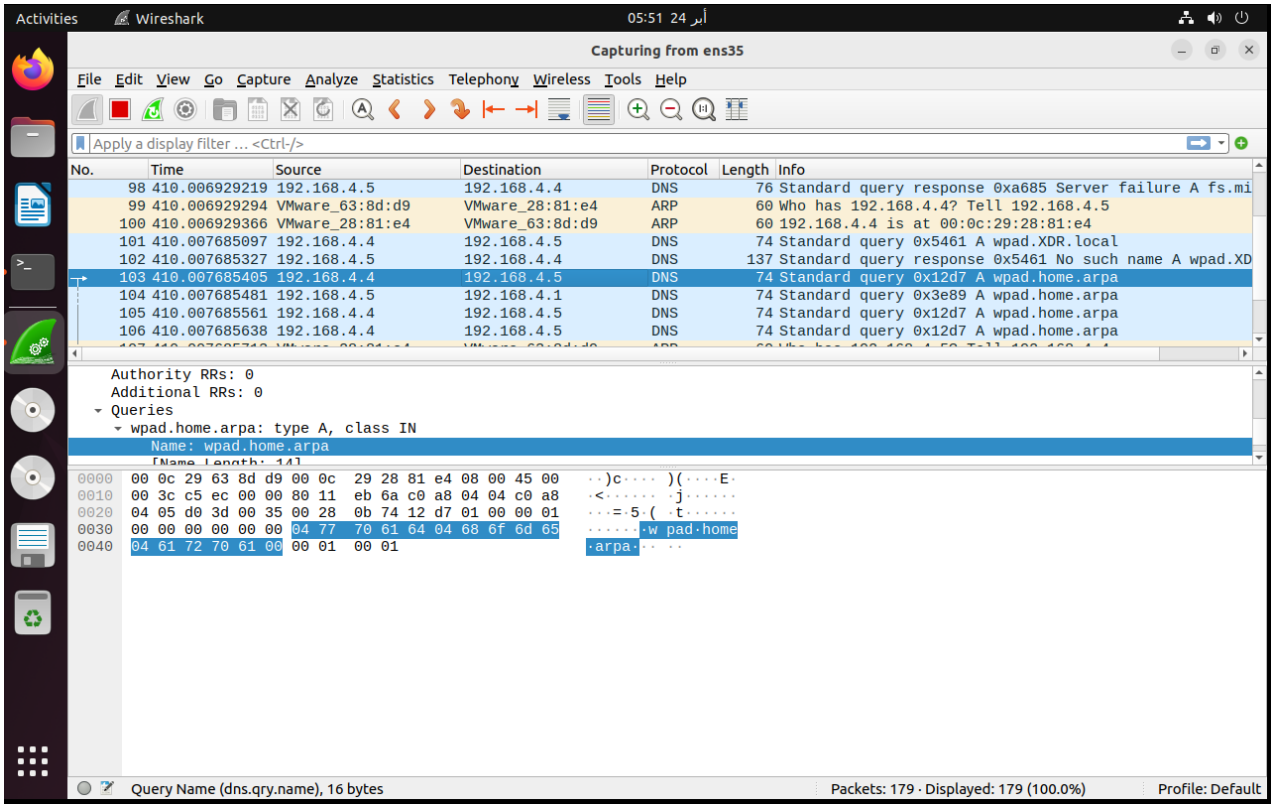
الشكل رقم ()

تم بنجاح الدخول



الشكل رقم ()

الآن، نقوم بالتبديل إلى جهاز المراقبة الافتراضي monitoring vm، وافتح الوحدة الطرفية، ثم قم بتشغيل wireshark انقر نقرًا مزدوجًا فوق واجهة المراقبة **(ens35)** لالتقاط حركة المرور من بيئةADDS العنوان 192.168.4.5



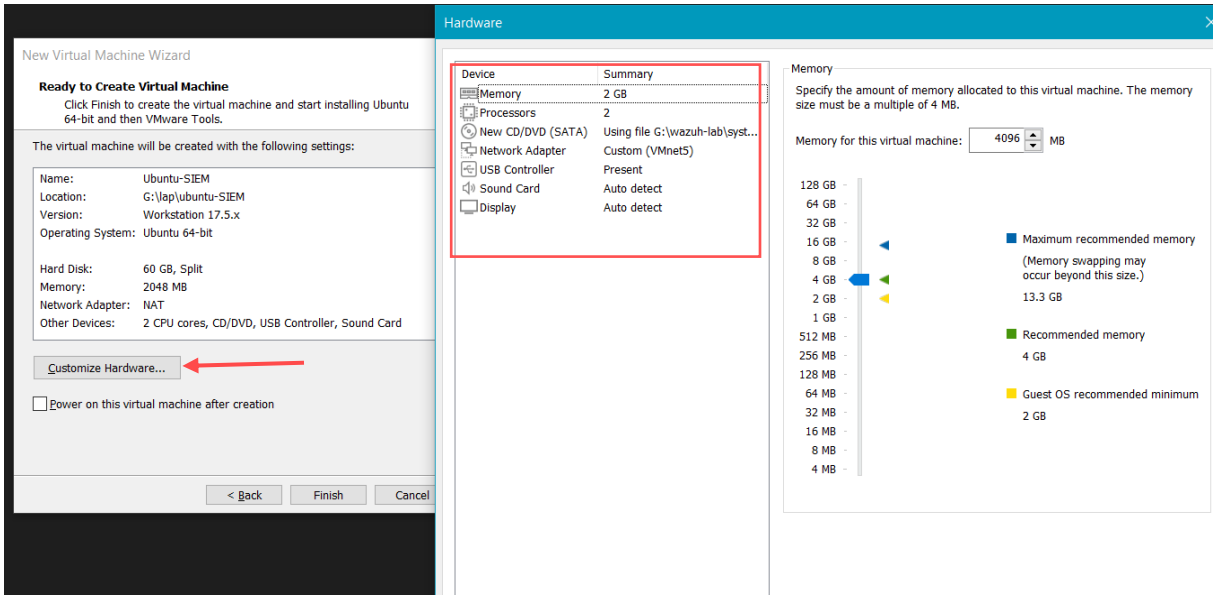
الشكل رقم ()

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.

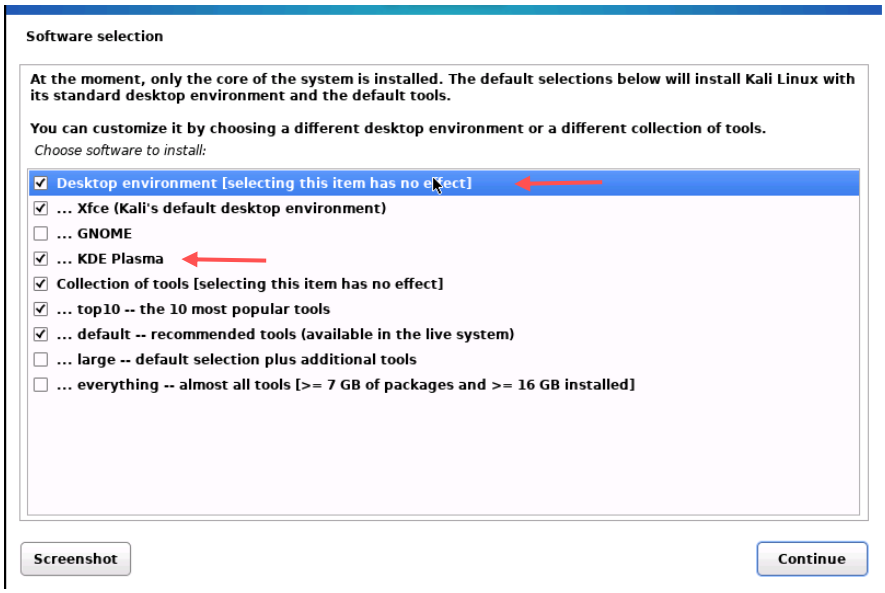
- **أولا:** سنقوم بأعداد نظام **Kali** كمضيف لل **SIEM — Wazuh**

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



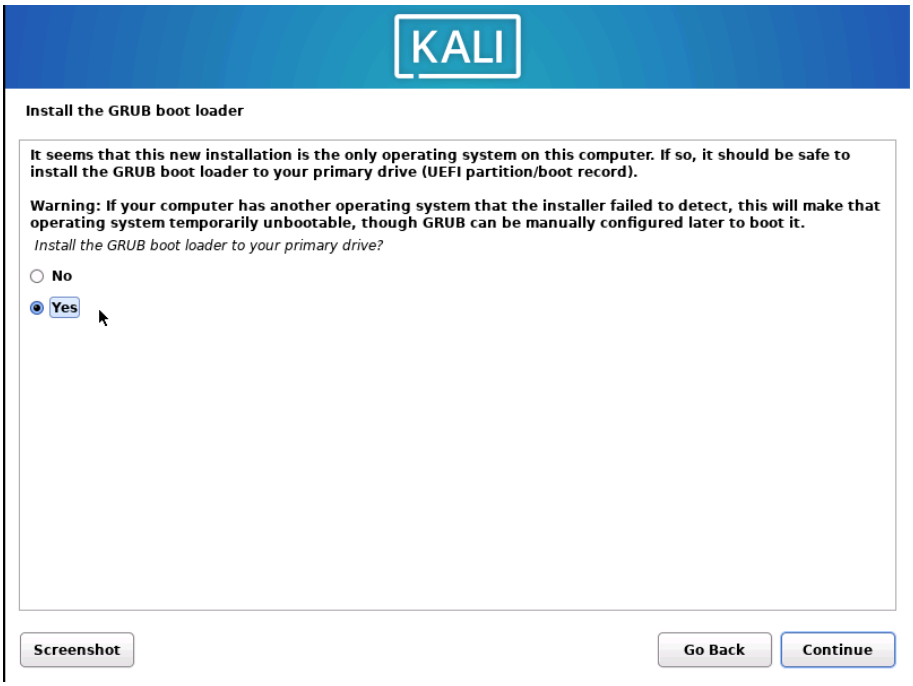
الشكل رقم ()

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



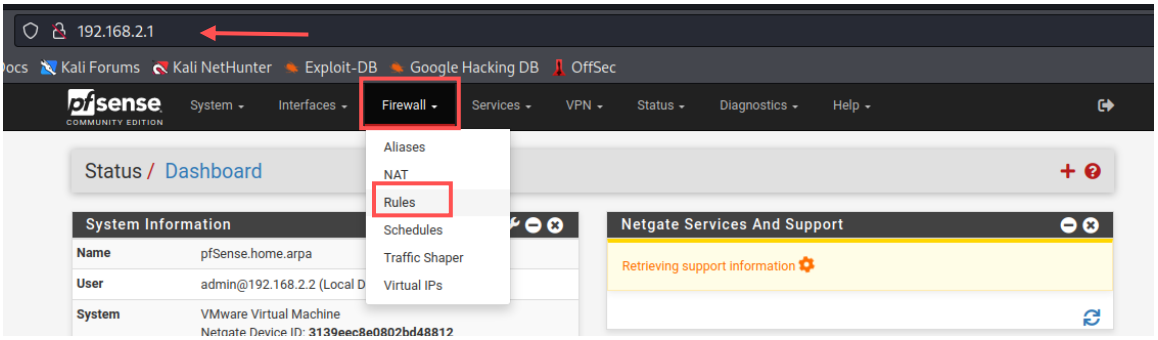
الشكل رقم ()

ثم اختر yes لتثبيت أداة تحميل التمهيد.GRUB

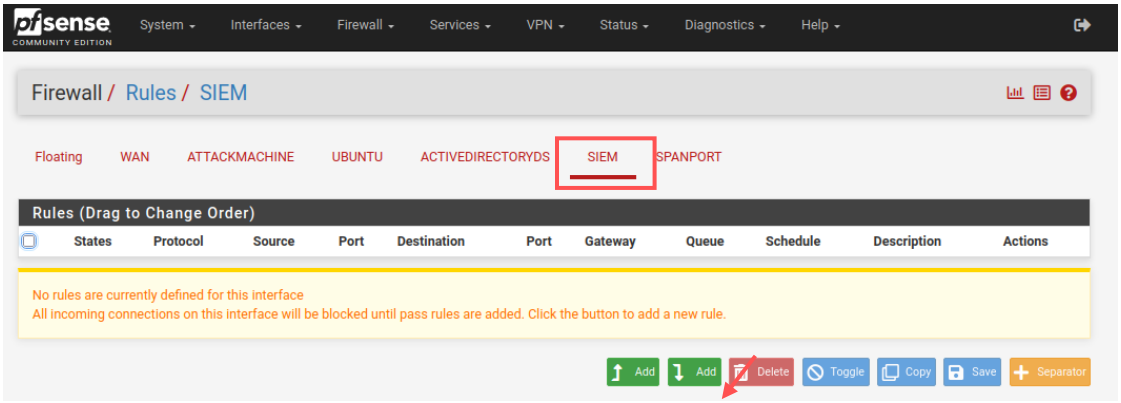


الشكل رقم ()

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

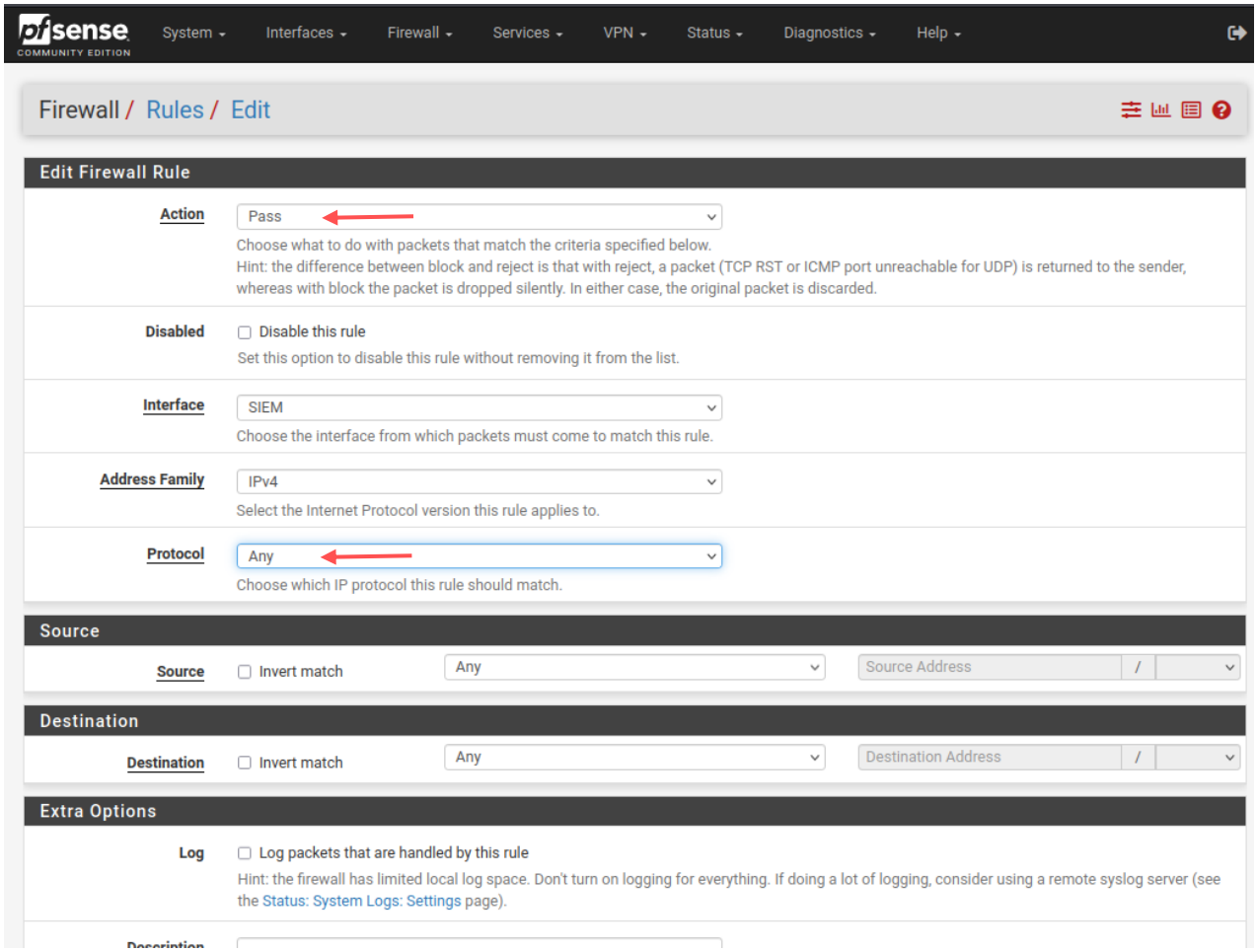


الشكل رقم ()



الشكل رقم ()

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

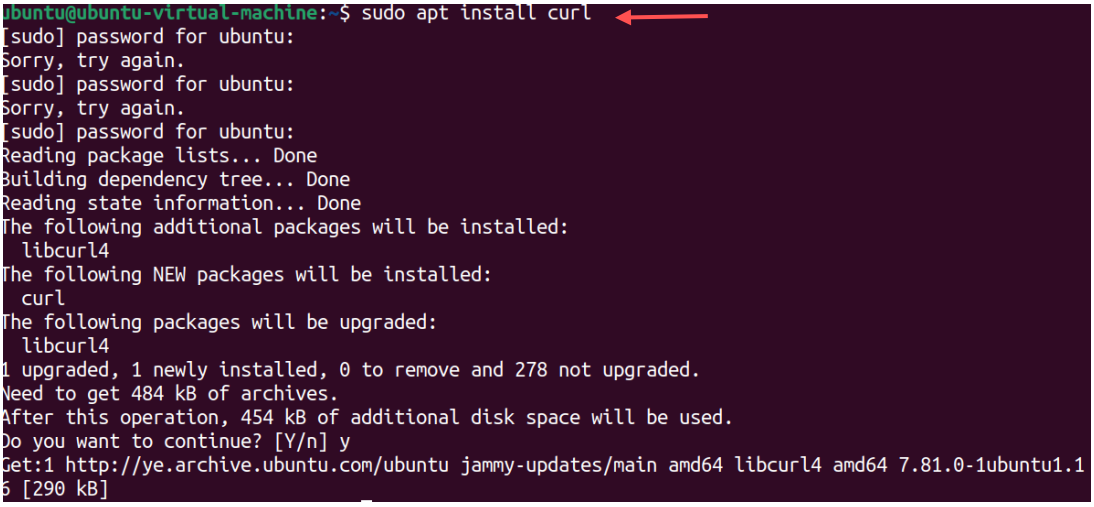


الشكل رقم ()

- **ثانيا:** الآن يجب أن يكون لديك إمكانية الوصول إلى الإنترنت. حان الوقت الآن لتنزيل وتثبيت Wazuh سنقوم بتثبيته في نظام ubuntu

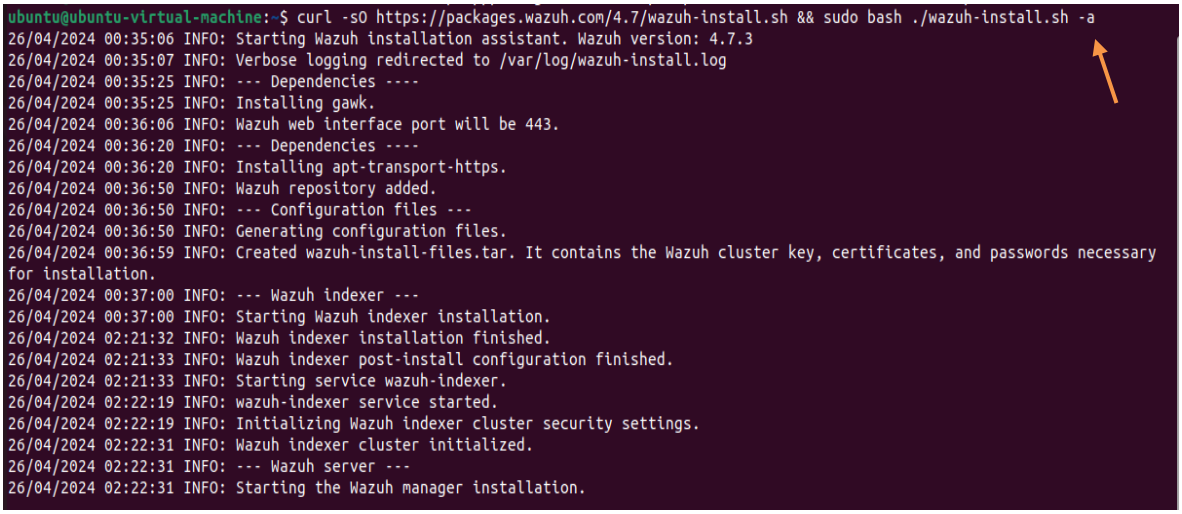
الشكل رقم ()

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



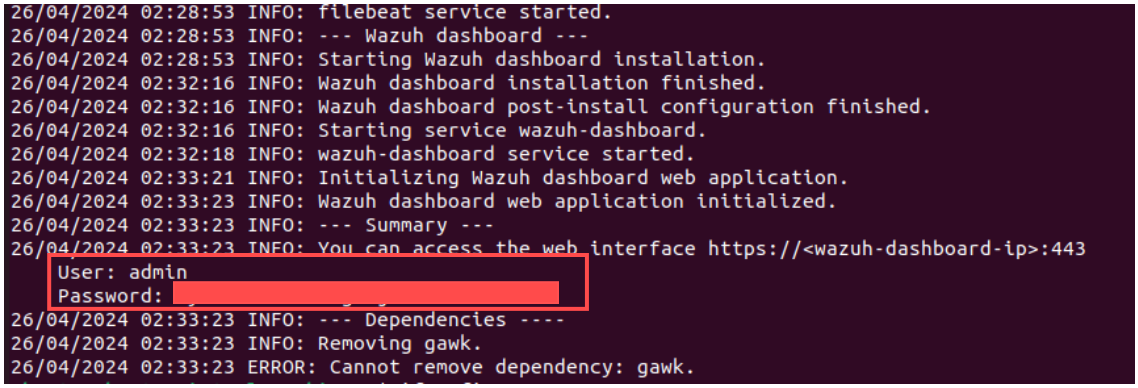
الشكل رقم ()

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



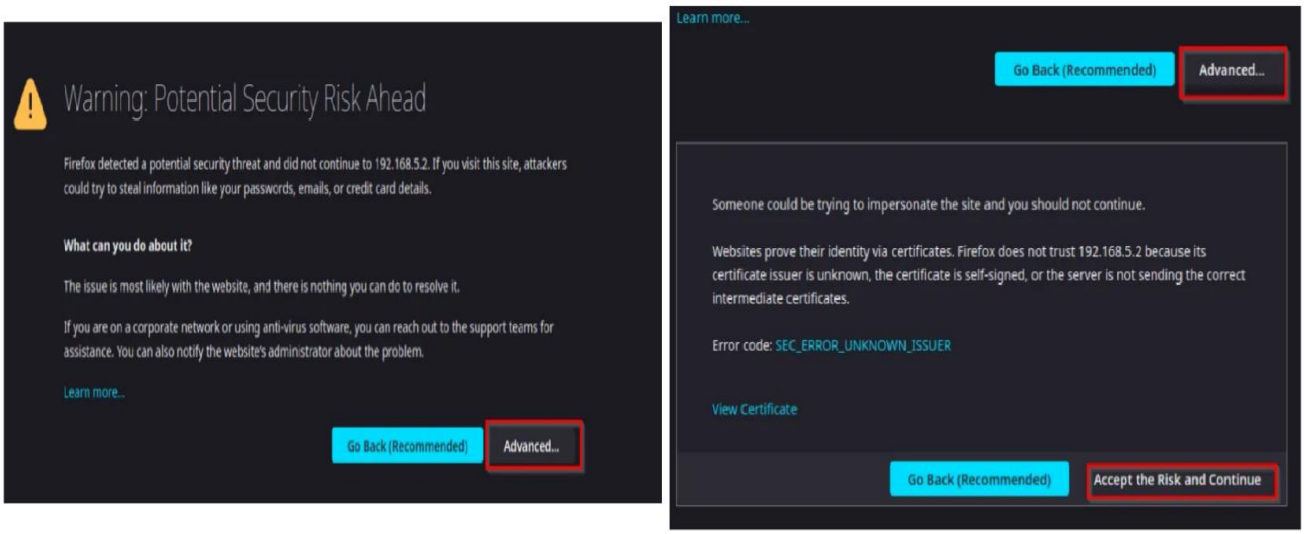
الشكل رقم ()

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



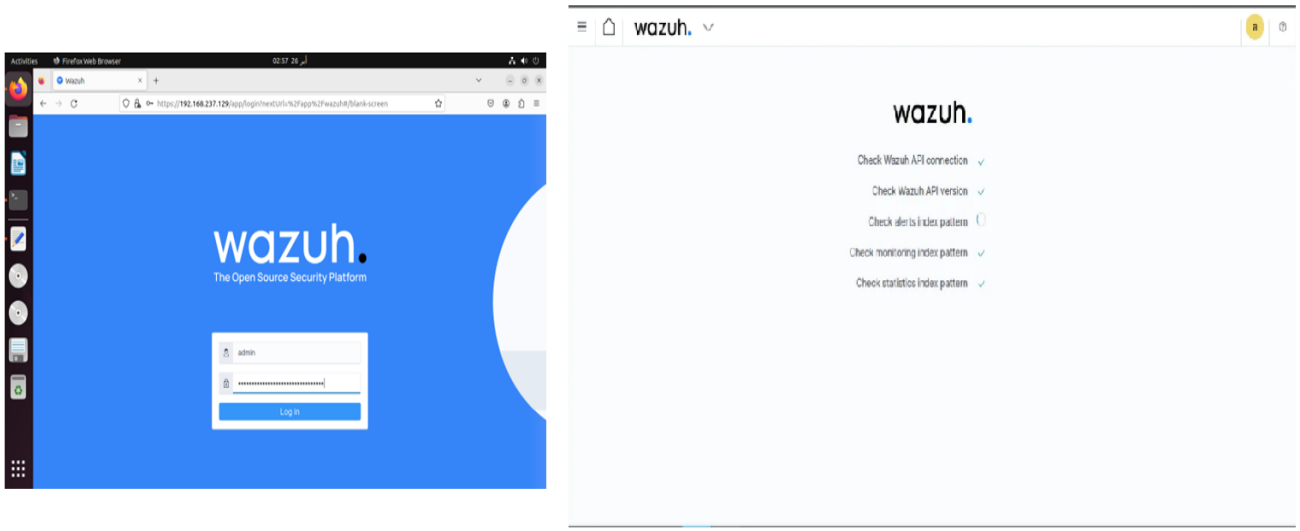
الشكل رقم ()

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.



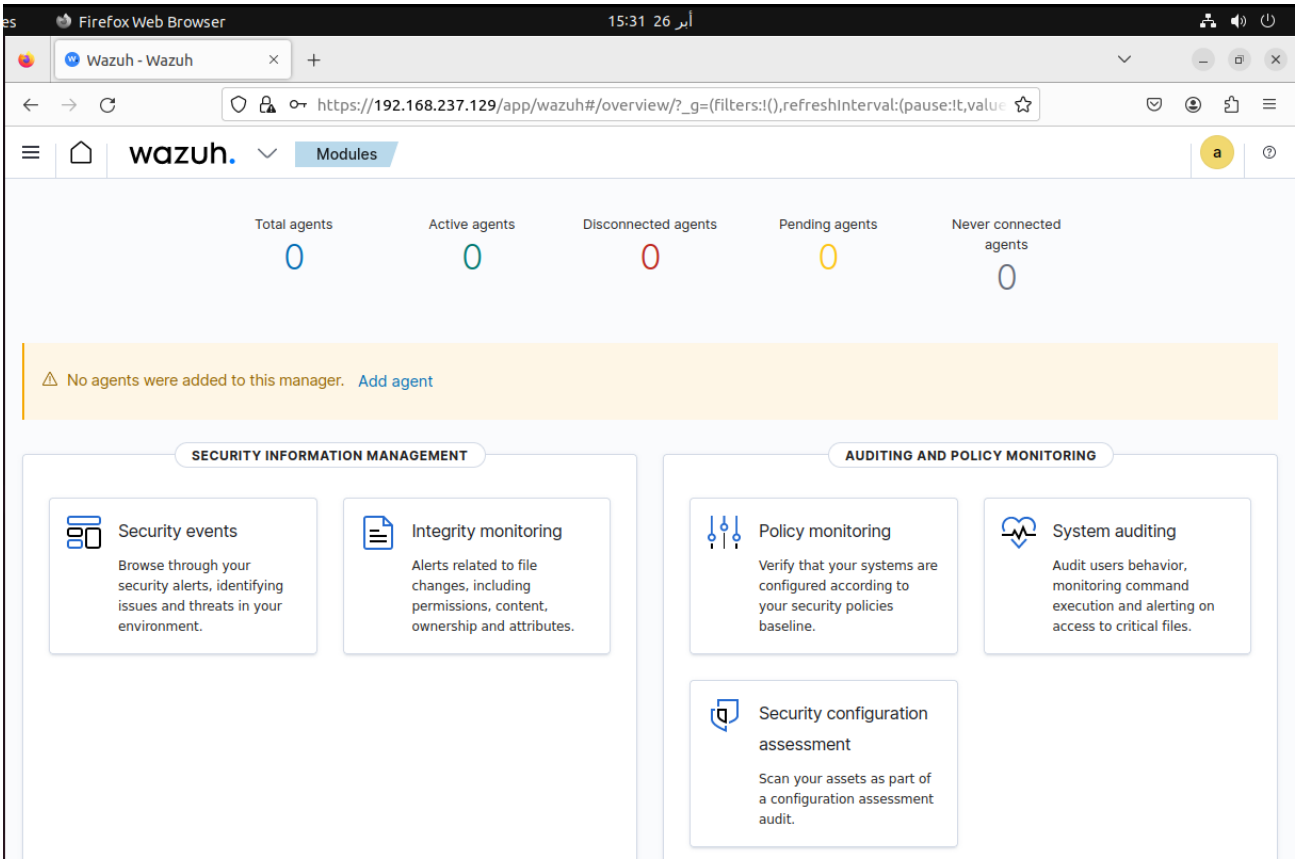
الشكل رقم ()

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



الشكل رقم ()

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



الشكل رقم ()

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

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

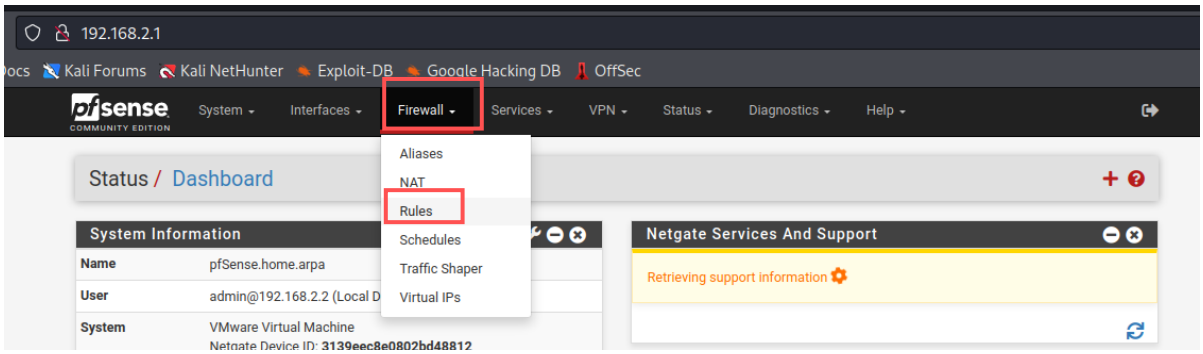
```
~$ curl -so wazuh-passwords-tool. sh https://packages.wazuh.com/4.7/wazuh-passwords-tool.sh
```

الشكل رقم ()

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

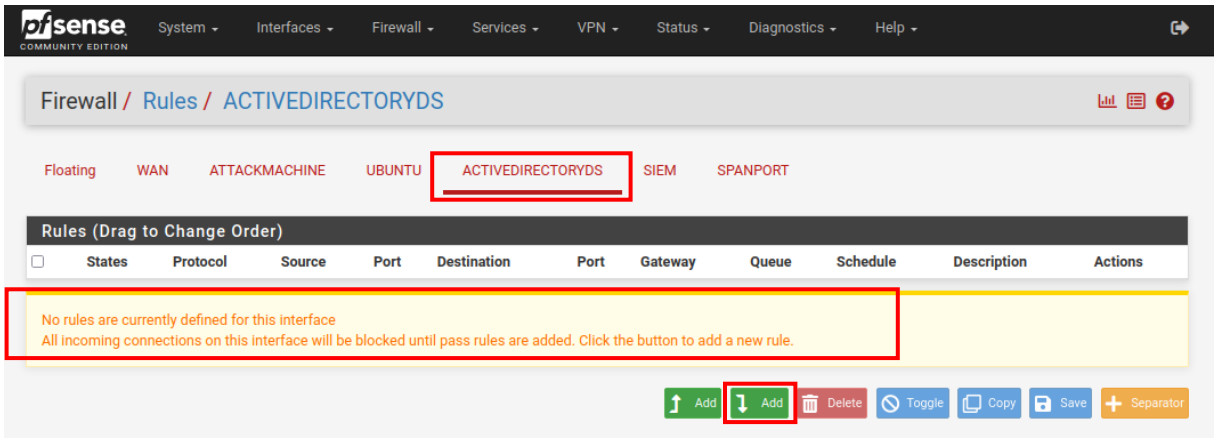
bash wazuh–passwords–tool.sh –u admin –p P@$$w0rd1

حاليا سنقوم بي **Forwarding** أحداث **Windows** إلى**Wazuh** من خلال الدخول الى جدار الحماية **pfsense** من جهاز **Attack Machine**، انتقل إلى جدار الحماية، وانقر فوق **Firewall > Rules**



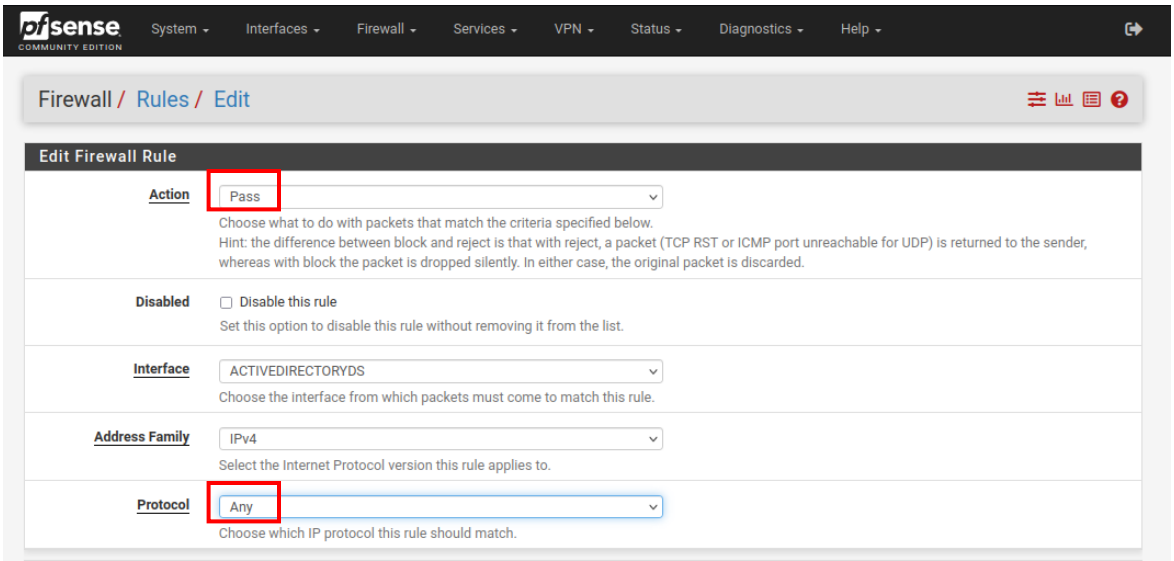
الشكل رقم ()

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



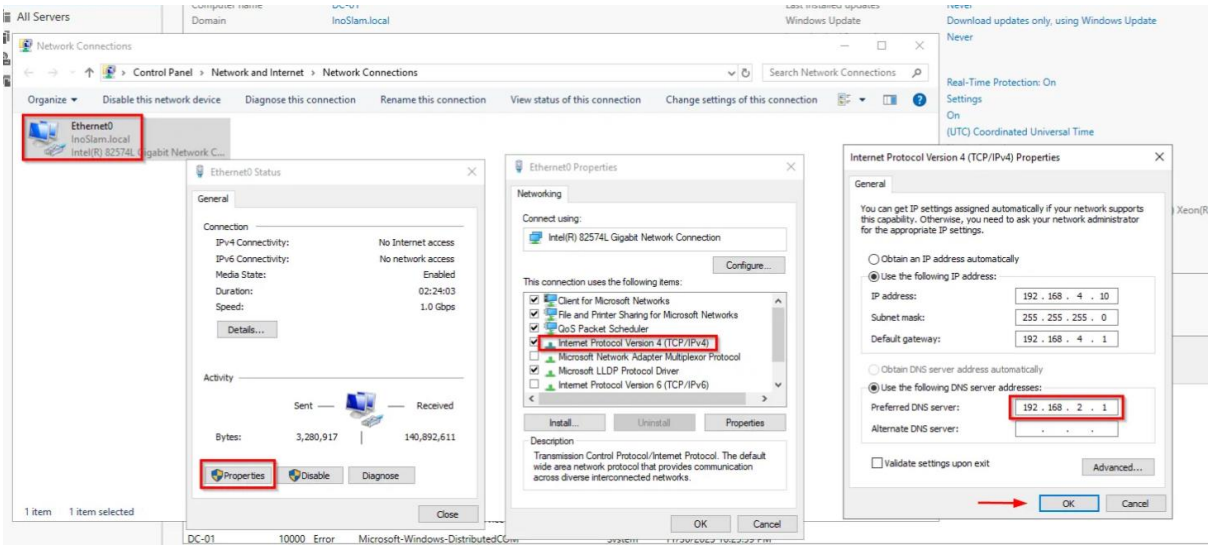
الشكل رقم ()

نقوم بالسماح بالاتصال واختيار Any لخيارات البروتوكول وحفظ الإعدادات وتطبيقها.



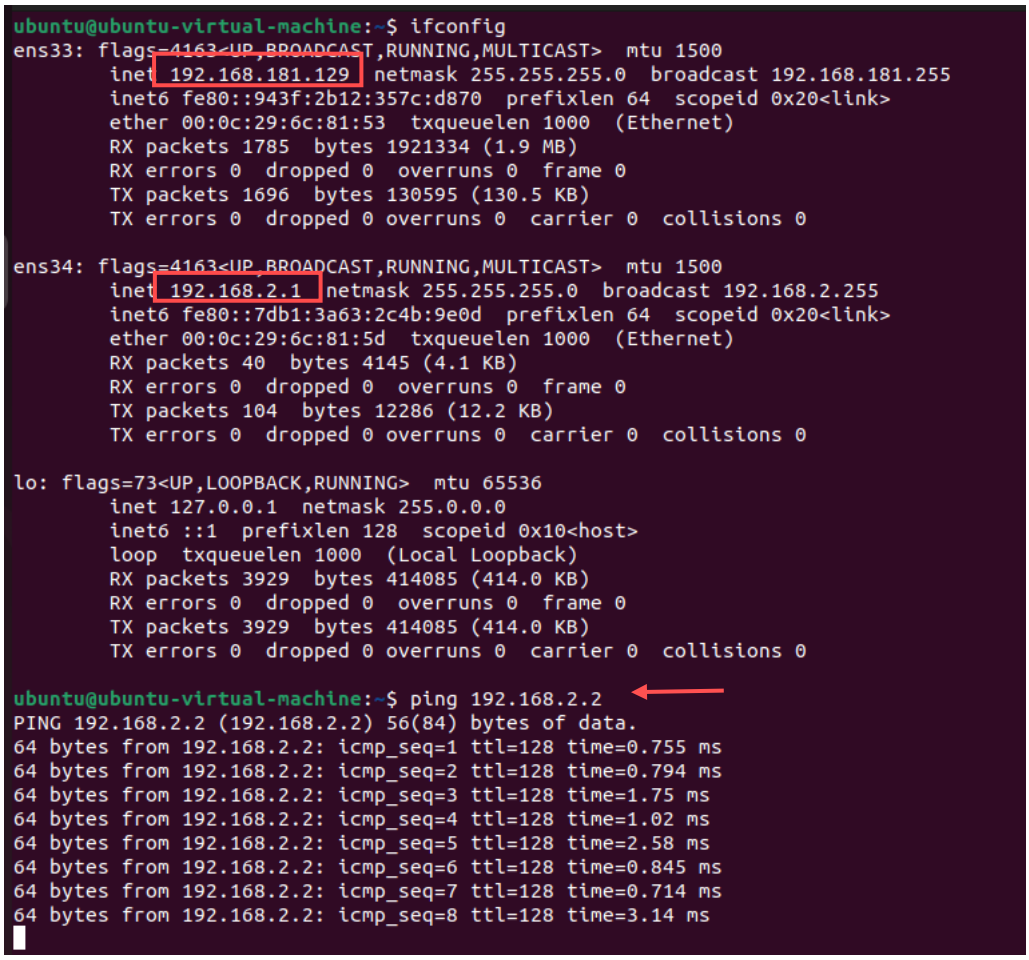
الشكل رقم ()

على الخادم AD DS، انقر فوق تغيير خيارات < Ethernet0 < adopter الخصائص < TCP/IPV4 < أضف عنوان IP الخاص بجدار الحماية باعتباره.DNS



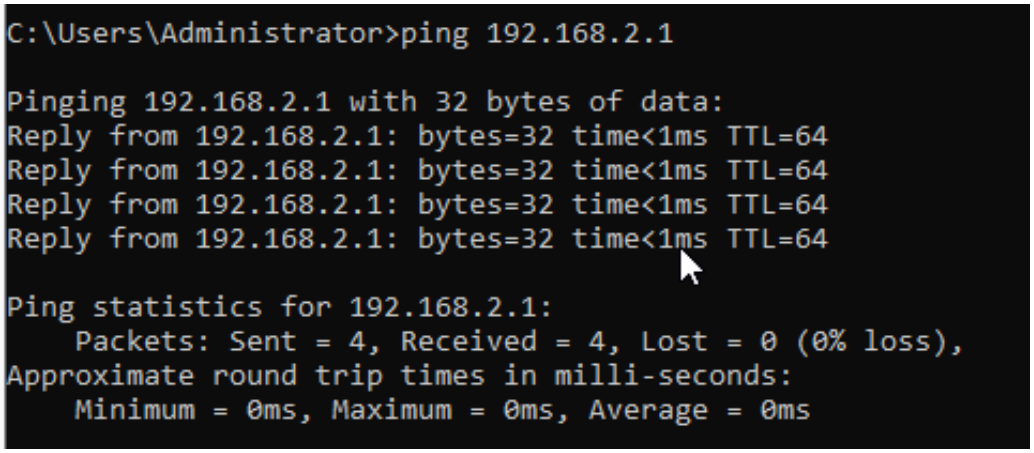
الشكل رقم ()

- **ثالثا:** الان بعد الانتهاء من انشاء المعمل، سنقوم بعمل **ping** من جهاز **ubuntu-wazuh** الى **AD** والعكس أيضا مع الأنظمة الأخرى كذلك للتأكد من ان عملية الاتصال سليمة



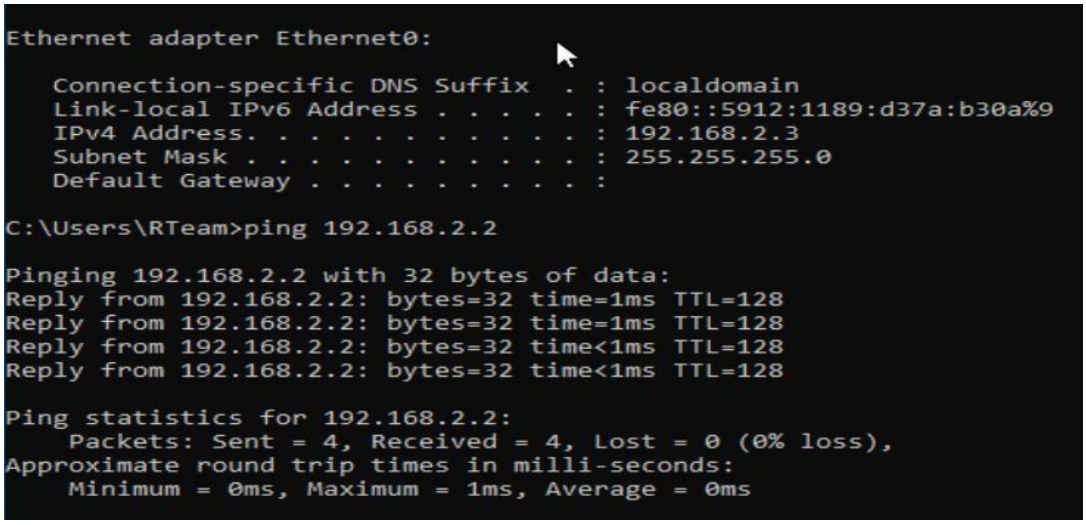
الشكل رقم ()

ثم من جهاز **windows server**

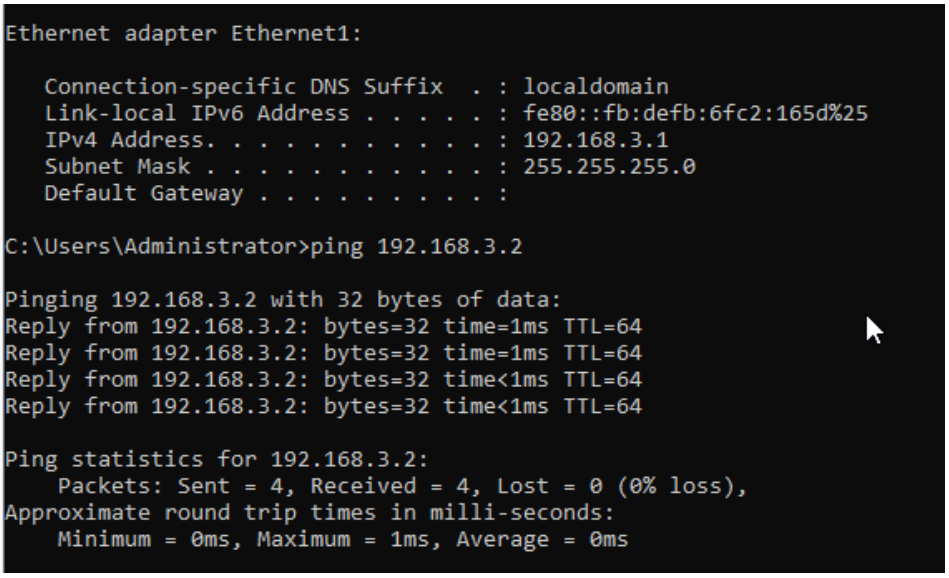


الشكل رقم ()

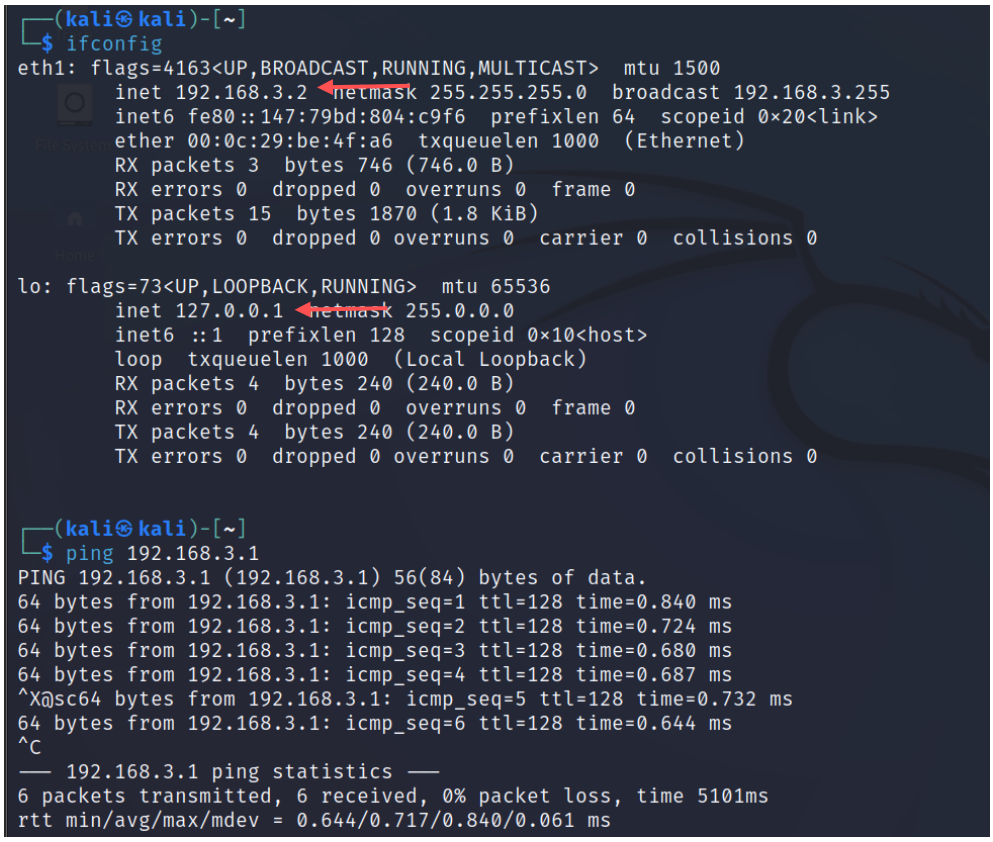
ثم سنقوم بإضافة جهاز **windows 10** كمستخدم مع وضع عنوان له في **windows server**



الشكل رقم ()



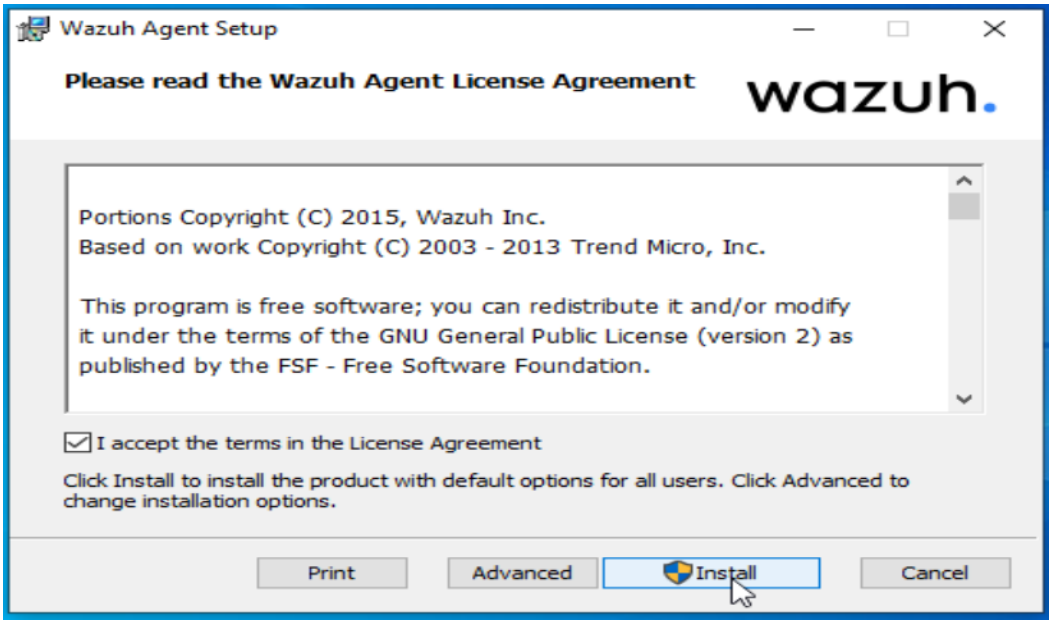
الشكل رقم ()



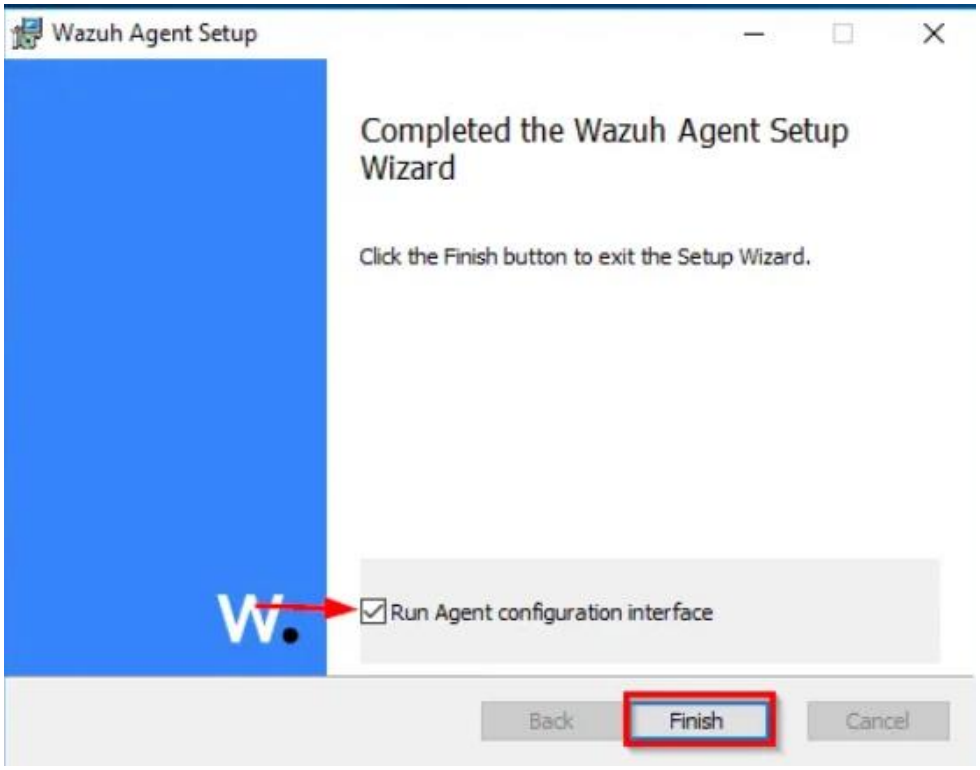
الشكل رقم ()

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

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

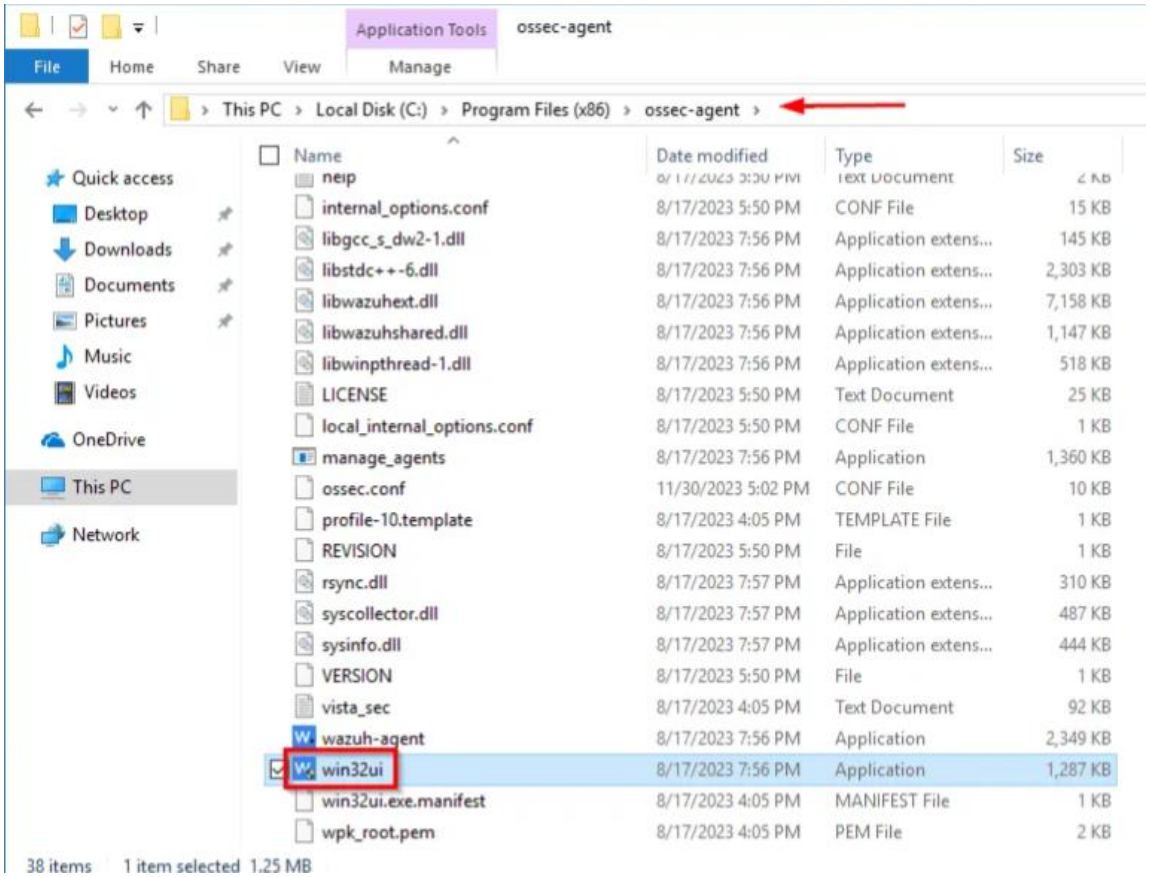


الشكل رقم ()



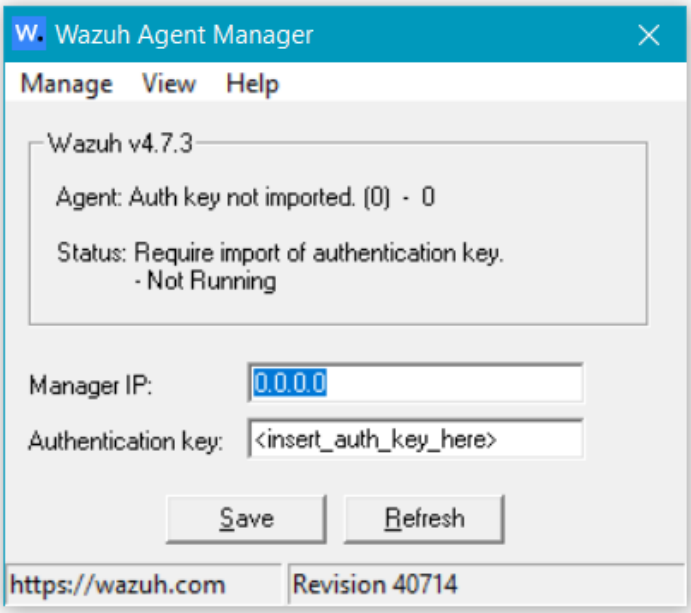
الشكل رقم ()

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



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**
5. [4] **MITRY. 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