مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (١١) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (11) 2025

آلية تقييم أمني قائمة على التوأم الرقمي وتحليل البينية في بيئة Active Directory

د. بسيم صالح برهوم *

م. علي حسن إبراهيم **

(تاريخ الإيداع ٢٠٢٥/٨/٧ . قُبِل للنشر في ٢٠٢٥/٩/١٧)

□ ملخّص□

تحلل هذه الدراسة بيئة Active Directory باستخدام قاعدة البيانات البيانية Neo4j، حيث تم حساب البينية لكل عقدة ودراسة تأثير إزالة العقد ذات البينية الأعلى، تُعد بيئة Active Directory مكوناً أساسياً في البنية التحتية للمؤسسات، إذ تُدير المستخدمين والمجموعات والوحدات التنظيمية والموارد المختلفة.

يُعد فهم هيكل هذه البيئة أمراً ضرورياً لتعزيز الأمن السيبراني وتقليل المخاطر المحتملة، أظهرت النتائج أن إزالة العقد ذات البينية العالية تؤدي إلى إعادة توزيع المسارات داخل البيئة ، مما يزيد من بينية العقد المتبقية. ومع ذلك، لم يكن هذا التأثير طردياً، حيث لوحظ أن بعض العقد قد تشهد ارتفاعاً أكبر في بينيتها عند إزالة عقدة مركزية ذات بينية أقل مقارنة بإزالة عقدة ذات بينية أعلى و يشير ذلك إلى أن بعض العقد التي قد تبدو غير مركزية تزداد أهميتها عند إزالة العقد الرئيسية بغض النظر عن ترتيب هذه العقد الرئيسية من حيث البينية.

بناءً على هذه النتائج، تم اقتراح آلية لتقييم الأمان تعتمد على مزيج من البينية والأوزان الأمنية للعقد، مما يوفر تصنيفاً أكثر دقة للنقاط الحيوية داخل البيئة ويسهم في تحسين سياسات الأمن السيبراني.

الكلمات المفتاحية :التوأم الرقمي، الأمن السيبراني ، الخوارزميات البينية، تقييم المخاطر، تحليل الرسم البياني،العقد الحرجة، درجة الأمان.

* أستاذ مساعد في قسم البرمجيات ونظم المعلومات، كلية الهندسة المعلوماتية ، جامعة اللاذقية ، اللاذقية ،سورية

**طالب دراسات عليا (ماجستير) ، قسم البرمجيات ونظم المعلومات ، كلية الهندسة المعلوماتية ،جامعة اللاذقية ، اللاذقية ، سورية

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (١١) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (11) 2025

A Security Assessment Mechanism Based on Digital Twin and Interface Analysis in an Active Directory Environment

Dr. Bassem Saleh Barhoum *
Eng. Ali Hassan Ibrahim **

(Received 7/8/2025 . Accepted 17/9/2025)

□ **ABSTRACT** □

This study analyzes the Active Directory environment using the graph database Neo4j. Betweenness centrality was calculated for each node, and the impact of removing nodes with the highest betweenness was examined. Active Directory is a core component of an organization's infrastructure, managing users, groups, organizational units, and various resources.

Understanding the structure of this environment is essential for enhancing cybersecurity and reducing potential risks. The results showed that removing nodes with high betweenness leads to a redistribution of paths within the environment, increasing the betweenness of the remaining nodes. However, this effect was not linear. It was observed that some nodes experienced a greater increase in betweenness when a centrally located node with lower betweenness was removed compared to the removal of a node with higher betweenness. This indicates that some nodes, which may appear non-central, gain significance when main nodes are removed, regardless of the ranking of those main nodes by betweenness.

Based on these findings, a security assessment mechanism was proposed that combines betweenness and the security weights of the nodes. This provides a more accurate classification of critical points within the environment and contributes to improving cybersecurity policies.

Keywords: Digital Twin, Cybersecurity, Betweenness Centrality, Risk Assessment, Graph Analysis, Critical Nodes, Security Score.

Assistant Professor, Department of Software Engineering and Information Systems, Faculty of Informatics Engineering, University of Latakia, Latakia, Syria
Postgraduate Student (Master's Degree), Department of Software Engineering and Information Systems, Faculty of Informatics Engineering, University of Latakia, Latakia, Syria

١. المقدمة:

في العصر الرقمي الحالي يُعد الأمن السيبراني عنصراً أساسياً في حماية البنية التحتية الرقمية للمؤسسات، وتلعب أنظمة إدارة الهوية والتحكم في الوصول دوراً حيوياً في تأمين الأنظمة ومنع التهديدات السيبرانية. تُعتبر Active Directoryمن أكثر الأنظمة استخداماً لإدارة المستخدمين والمجموعات والموارد في بيئات تكنولوجيا المعلومات، حيث توفر نظاماً مركزياً لإدارة الهويات والأذونات داخل المؤسسات، مما يسهل التحكم في الوصول إلى البيانات الحساسة والموارد المهمة[1] .

تواجه Active Directory تحديات أمنية متزايدة، حيث تُعد هدفاً رئيسياً للهجمات الإلكترونية، مما يجعل تأمينها أمراً بالغ الأهمية، يسعى المهاجمون إلى استغلال نقاط الضعف في هذه الأنظمة للوصول غير المصرح به إلى المعلومات الحساسة. وفقاً لتقرير صادر عن وزارة الدفاع الأمريكية يُعد اكتشاف وتخفيف اختراقات Active Directory أمراً ضرورياً لحماية الأنظمة المؤسسية من التهديدات السيبرانية المتطورة [2].

تتسم Active Directory ببنية معقدة تتكون من وحدات تنظيمية، مستخدمين، مجموعات، وموارد أخرى، حيث تتفاعل هذه العناصر فيما بينها وفقاً لسياسات وصول وصلاحيات محددة ، يمكن تحليل هذه البيئة من خلال تقنيات تحليل البيانات البيانية التي تسمح بفهم العلاقة بين المكونات المختلفة. في هذا السياق، توفر قاعدة البيانات البيانية Neo4j أدوات فعالة لاكتشاف المسارات المحتملة للهجمات وتحليل مدى تأثير العقد المختلفة على الأمن السيبراني للمؤسسة. على سبيل المثال، يوفر مشروع مفتوح المصدر[1] على GitHub أدوات متقدمة لتحليل بيئات Active Directory وتحديد الثغرات الأمنية المحتملة باستخدام تقنيات تحليل البيانات البيانية [3].

إن فهم بيئة Active Directory من منظور بياني لا يقتصر على تحديد المسارات الحرجة فحسب، بل يمتد ليشمل تقييم الدور الذي تلعبه كل عقدة ضمن النظام، سواء كانت مستخدماً عادياً، مجموعة إدارية، أو وحدة تنظيمية. وهذا البعد يفتح المجال أمام تطوير معايير جديدة لتصنيف درجة الأمان بناءً على الخصائص الوظيفية والسياقية للعقدة، إلى جانب مؤشرات القياس الكمية. وعليه، فإن البحث في هذه الاتجاهات لا يساهم فقط في تعزيز الأمان السيبراني للمؤسسات، بل يُمكّن أيضاً من تطوير استراتيجيات دفاعية ديناميكية تستبق الهجمات بدلاً من الاكتفاء بردعها بعد وقوعها.

٢. الدراسات المرجعية:

لقد تناولت العديد من الدراسات بيئة Active Directory من منظور أمني، حيث استخدمت أدوات متقدمة مثل BloodHound التي تستند إلى تقنيات الرسم البياني من أجل تحديد المسارات الحرجة داخل الشبكة، والكشف عن نقاط يمكن استغلالها في الهجوم [٤]. ورغم قوة هذه الأدوات في التحليل الكمي لعلاقات العقد والمسارات المحتملة، إلا أن معظم هذه الدراسات افتقرت إلى دمج السياق الأمني والوظيفي للعقدة، مثل دورها الحقيقي في النظام أو طبيعة الصلاحيات الموكلة إليها، وهو ما يُضعف من دقة التقييم الأمني ويجعل نتائجه غير كافية لاتخاذ قرارات استراتيجية.

من ناحية أخرى، برزت بعض النماذج العامة في إدارة المخاطر مثل OCTAVE التي اقترحها Alberts وDorofee، والتي تقوم على دمج أكثر من مؤشر لتقييم مستوى المخاطر الأمنية بشكل شامل [٥]. ومع ذلك، فإن هذه النماذج لم تُطبّق بعمق على بيئة Active Directory بما تحمله من تعقيد وتداخل بين العقد، كما أنها

غالباً ما اعتمدت على سيناريوهات نظرية أو قواعد بيانات غير واقعية، مما يحد من قدرتها على محاكاة التفاعلات الفعلية في الشبكات الكبيرة والمؤسسية.

[1] https://github.com/neo4j-graph-examples/cybersecurity

إضافةً إلى ذلك، فإن القليل من الأبحاث السابقة تناولت بشكل منهجي تأثير إزالة العقد أو تغيير أوزانها داخل الرسم البياني على تماسك البنية الشبكية ومسارات الهجوم المحتملة. وهذا الجانب الديناميكي يُعد بالغ الأهمية، إذ يمكن أن يكشف عن العقد الأكثر حساسية التي يؤدي استهدافها إلى انهيار أجزاء واسعة من النظام.

انطلاقاً من هذه الفجوة البحثية، يسعى هذا البحث إلى محاكاة بيئة Active Directory باستخدام بنية التوأم الرقمي، ودمج مقياس Betweennessمع تحليل نوع العقدة عبر نظام أوزان محدد، واقتراح معادلة تصنيف لدرجة الأمان تأخذ بعين الاعتبار البُعدين الكمي والسياقي معاً. وبهذا النهج، لا يقتصر التحليل على الأرقام والمؤشرات، بل يشمل أيضاً فهم الدور الوظيفي لكل عقدة وتأثيرها الأمني، مما يتيح الوصول إلى تقييم أكثر واقعية ودقة لمستوى أمان البنية التحتية الرقمية.

٣. أهمية البحث و أهدافه:

يهدف هذا البحث إلى تقديم آلية تقييم أمني تعتمد على الجمع بين التحليل الكمي، الذي يعتمد على مقاييس المركزية لاكتشاف أهم العقد في النظام، والتحليل النوعي، الذي يأخذ في الاعتبار الأهمية الأمنية الفعلية للعقد، وبذلك من الممكن تحقيق تصنيف أمني أكثر دقة يعزز من استراتيجيات الدفاع السيبرانية ويساهم في الحد من التهديدات الإلكترونية المحتملة.

٤. الموارد وطرق البحث

تم استخدام قاعدة بيانات [2] مقدمة من منصة neo4j مخصصة للمطورين في مجال الأمن السيبراني وتشغيلها على الحاسوب الشخصي ، مما أتاح فرصة تحليل بنية ال Active Directory وتقييم المخاطر السيبرانية بدقة. فيما يلي تفاصيل الموارد والطرق التي تم اعتمادها :

4.1 الموارد

- العقد (Nodes) :
  - قاعدة البيانات تحتوي على ٩٥٣ عقدة تمثل مكونات البيئة.
  - شملت العقد :

الجدول (١):أنواع العقد وأعدادها.

نوع العقدة	العدد
Computer	301
Group Policy Objects (GPO)	22
Domain	1
Group	308
User	300
High Value	6
Organizational unit (OU)	21

[2] https://sandbox.neo4j.com/?usecase=cybersecurity

ملاحظة :يوجد بعض العقد تندرج تحت مسميين (labels) مثل مسمى مجموعة ومسمى ذات قيمة عالية في نفس الوقت لذلك يختلف العدد الكلي للعقد عن مجموع عدد العقد في كل الفئات معاً.

- العلاقات(Relationships) :
  - يوجد ٤٧١٦ علاقة تربط بين العقد المختلفة، مما يعكس الترابط والتكامل بين مكونات النظام.

الجدول (2): شرح شامل لجميع أنواع العلاقات.

العلاقة	الوظيفة
ADMIN_TO	تمثل الصلاحيات الإدارية التي يمتلكها كيان معين على جهاز أو كيان آخر.
ALLOWED_TO_DELEGATE	السماح بتمرير تفويضات المصادقة، والتي يمكن أن يتم استغلالها لانتحال هوية مستخدمين آخرين.
CAN_RDP	تحديد الكيانات القادرة على الوصول عبر بروتوكولRDP (Remote Desktop Protocol) .
CONTAINS	تمثيل البنية الهرمية في الشبكة من خلال ربط الوحدات التنظيمية بمكوناتها.
DC_SYNC	من خلال هذه العلاقة، يمكن تحديد الكيانات التي لديها القدرة على تنفيذ عملية مزامنة البيانات.
EXECUTE_DCOM	تنفيذ أوامر DCOM (Distributed Component Object Model) عن بعد باستخدام هذه العلاقة، وهي مفيدة في تحليل الهجمات المتقدمة.
GENERIC_ALL	تمييز الكيانات التي تمتلك صلاحيات كاملة على كائنات أخرى.
GENERIC_WRITE	تعديل خصائص معينة في كائن ما، والتي قد تؤدي إلى تصعيد الامتيازات.
GET_CHANGES	مراقبة تغييرات Active Directory .
GET_CHANGES_ALL	تمتلك صلاحيات موسعة لجلب التغييرات بما في ذلك كلمات المرور.
GP_LINK	ربط السياسات الأمنية (GPOs) بالوحدات التنظيمية أو Domain.
HAS_SESSION	تحديد الجلسات النشطة للمستخدمين على الأجهزة، مما يشير لإمكانية الوصول الفعلي .
MEMBER_OF	تحديد علاقات العضوية داخل المجموعات، مما يساهم في تحليل وراثة الصلاحيات .
OWNS	تحديد الملكية بين الكيانات، مثل امتلاك جهاز معين.
WRITE_DACL	تعديل قائمة التحكم بالوصولDACL (Discretionary access control list)لكائنات أخرى .
WRITE_OWNER	تغيير مالك كائن معين، وهي وسيلة محتملة لتصعيد الامتيازات.

توفر هذه الموارد نظرة شاملة على توزيع مكونات البيئة [6] .

4.2 طرق البحث

٤,٢,١ تحميل وتشغيل قاعدة البيانات:

تم تحميل قاعدة البيانات من منصة neo4j وتشغيلها محليا، مما وفر بيئة نموذجية لتحليل بنية Active Directory دون الحاجة لإعادة بناء القاعدة من الصفر [6] .

والتي تمثل نموذجاً افتراضياً يحاكي البنية الحقيقية للنظام باستخدام كافة العقد والعلاقات المتوفرة، يساعد هذا النموذج في تصور سيناريوهات الهجمات وتحليل تأثير تعطيل العقد الحرجة على أداء النظام.

٤,٢,٢ تكوين رسم بياني لمسارات الهجوم:

تم في هذه المرحلة بناء رسم بياني شامل يوضح جميع المسارات المحتملة التي قد يسلكها المهاجم للوصول إلى العقد الحساسة في النظام، والتي تم تعريفها كعقد ذات قيمة عالية . (HighValue)تم تنفيذ الاستعلام التالي باستخدام لغة Cypher :

```
MATCH (crownJewel:HighValue)
MATCH (source) WHERE NOT source:HighValue
MATCH path = shortestPath((source)-[*..100]->(crownJewel))
UNWIND apoc.coll.pairsMin(nodes(path)) AS pair
WITH pair[0] AS a, pair[1] AS b
MERGE (a)-[r:ATTACK_PATH]->(b)
RETURN count(r)؛
```

الشكل (١): استعلام بلغة cypher يقوم بإعادة جميع مسارات الهجوم المحتملة التي قد يسلكها المهاجم.

حيث يتم أولاً تحديد جميع العقد من نوع HighValue كمراكز مستهدفة(Crown Jewels) ، ثم يتم البحث عن أقصر المسارات الممكنة التي تصل إليها من جميع العقد الأخرى في الرسم البياني باستثناء العقد المصنفة أصلاً كـ(HighValue) .

الاستعلام يعتمد على وظيفة shortestPath للعثور على المسارات بحد أقصى ١٠٠ قفزة، ومن ثم تُستخدم مكتبة APOC لاستخراج جميع أزواج العقد الموجودة داخل كل مسار، ليتم في النهاية إنشاء علاقات جديدة تحمل الوسم ATTACK_PATH بين هذه الأزواج. هذا يُمكّن من إعادة استخدام هذه العلاقات لاحقاً في التحليلات أو التصورات البصرية.

وقد أسفر هذا الاستعلام عن 2730 مسار هجوم محتملاً (بين أزواج العقد)، تم تمثيلها كعلاقات جديدة ضمن الرسم البياني. ويُمثل هذا العدد الكبير من المسارات مؤشراً على تعقيد بنية النظام وتعدد النقاط التي قد تُستغل للوصول إلى الأصول الحساسة.

يُعتبر هذا الرسم البياني أداة مركزية لتحليل الأمان السيبراني، حيث يمكن من خلاله:

- تحديد العقد الوسيطة ذات الدور المحوري في إيصال المهاجم إلى الأهداف.
- دعم قرارات تعزيز الأمان عبر تحديد المسارات الواجب تأمينها أو قطعها.

هذا التحليل التمهيدي يمهد الطريق لاستخدام تقنيات أكثر تقدمًا مثل تحليل المركزية Betweenness) (Centrality لتحديد تأثير كل عقدة على مستوى مسارات الهجوم، و إجراء محاكاة لتأثير إزالة العقد ذات الخطورة العالية.

٤,٢,٣ تطبيق خوارزمية"Betweenness" :

بعد تطبيق خوارزمية Betweenness Centrality باستخدام مكتبة Graph Data Science في Neo4j، تم تحليل مدى مركزية كل عقدة داخل بيئةActive Directory ، بهدف تقييم أهميتها الأمنية بناءً على دورها كوسيط في المسارات المحتملة للهجوم.

أظهرت النتائج تباينا في القيم بين **9و١٠٥٢**، مما مكّن من تحديد العقد الأكثر تأثيراً، والتي تمثل نقاطاً مركزية في البنية وتُعد أهدافًا حرجة. تمر عبر هذه العقد عدد كبير من المسارات، ما يجعل استهدافها وسيلة فعالة للمهاجم في التنقل داخل البيئة.

٤,٢,٤ تحليل تأثير تعطيل العقد الحرجة وإعادة حساب قيم"Betweenness" :

تم في هذه المرحلة من الدراسة تحليل تأثير تعطيل العقد الحرجة ذات القيم العالية من حيث قيمة البينية (Betweenness)على عدد مسارات الهجوم داخل البيئة، بالإضافة إلى تقييم مدى إعادة توزيع التأثير بعد إزالة كل عقدة على حدى. وقد أظهرت النتائج وجود علاقة طردية واضحة بين قيمة البينية للعقدة وعدد المسارات المرتبطة بها، حيث إن تعطيل العقد ذات القيم المرتفعة يؤدي إلى تقليص عدد مسارات الهجوم بشكل ملحوظ، بينما تؤدي إزالة العقد الأقل أهمية إلى تغييرات هامشية في بنية الشبكة من حيث عدد المسارات.

على سبيل المثال، بلغ عدد مسارات الهجوم الأصلية الكاملة من أي عقدة الى العقد ذات الأهمية العالية 568وعند إزالة العقدة ADMINS@TestCompany.Local التي تمتلك أعلى قيمة بينية وهي 1052، انخفض عدد المسارات إلى 426، ما يمثل تقليصاً حاداً يدل على التأثير الكبير لهذه العقدة في تسهيل الاتصال بين عناصر البيئة. وتم تسجيل نفس عدد المسارات 426 عند إزالة العقدة TestCompany.Local، التي تبلغ قيمة بينيتها 544، مما يشير إلى أن التأثير لا يعتمد فقط على القيمة العددية للبينية، بل على الموقع البنيوي للعقدة داخل الرسم البياني العام.

أما بالنسبة للعقد التي تملك قيم بينية أقل مثل:

- FLLABDC@TestCompany.Local (297)
- CA_USERS@TestCompany.Local (254)
- IT00161@TestCompany.Local (211)

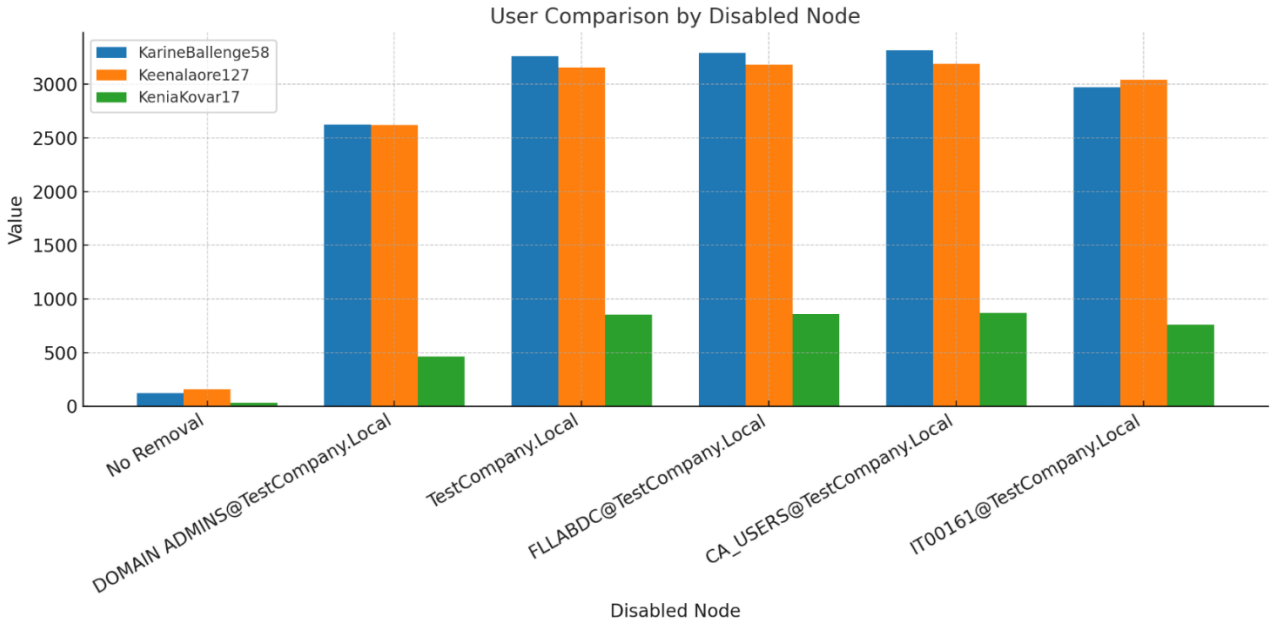
فإن عدد مسارات الهجوم الناتج بعد إزالة كل منها كان 564، مما يدل على محدودية دور هذه العقد في الربط بين المسارات الرئيسية. إلا أن ذلك لا يعني تجاهلها تماماً، حيث يمكن أن تؤثر على مسارات محلية معينة أو على استراتيجيات الوصول غير المباشرة.

ولفهم أعمق لتأثير إزالة كل عقدة حرجة، تم اعتماد القيم الجديدة لمؤشر البينية لثلاث عقد مختارة عشوائياً بعد كل عملية إزالة. العقد الثلاثة هي:

١. KarineBallenge58@TestCompany.Local
٢. Keenalaore127@TestCompany.Local
٣. KeniaKovar17@TestCompany.Local

الجدول (3): نتائج التغير الكبير في البينية بعد إزالة العقد الحرجة.

العقدة المعطلة	بينية العقدة المعطلة	بينية العقدة المختبرة الأولى KeniaKovar17	بينية العقدة المختبرة الثانية Keenalaore127	بينية العقدة المختبرة الثالثة KarineBallenge58
بدون إزالة	–	30	156	120.75
DOMAIN ADMINS@TestCompany.Local	١٠٥٢	462	2620.56	2626.8
TestCompany.Local	544	853.87	3160	3265.55
FLLABDC@TestCompany.Local	297	860.53	3184	3292.38
CA_USERS@TestCompany.Local	254	867.20	3192.3	3319.71
IT00161@TestCompany.Local	211	757.60	3040	2971.50



الشكل (٢): يظهر نتائج إزالة العقد الحرجة على بينية ثلاث عقد تم اختيارها عشوائيا.

يتضح من هذه القيم أن إزالة العقد الحرجة تؤدي إلى ارتفاع كبير في قيمة البينية للعقد الثلاث الأخرى. على سبيل المثال، عند إزالة العقدة TestCompany.Local، ارتفعت قيمة KarineBallenge58 من 120.75إلى 3265.55، مما يشير إلى انتقال تأثير الشبكة إليها وتحملها عبء أكبر في تمرير البيانات أو المسارات. وهذا يشير إلى أن بعض العقد تصبح "بدائل حيوية" عند إزالة العقد الأساسية، وهو أمر بالغ الأهمية عند التفكير في استراتيجيات الدفاع، حيث يمكن للمهاجمين استغلال هذا الانتقال في المركزية للوصول إلى الأهداف عبر مسارات بديلة.

من جانب آخر، يُبرز هذا التحليل أن ارتفاع قيمة البينية لعقدة معينة لا يعني بالضرورة أنها تمثل الخطر الأمني الأكبر. فالأهمية الأمنية للعقدة قد تكون مرتبطة بشكل أكبر بموقعها البنيوي داخل الرسم البياني العام، بالإضافة إلى نوعها (كمستخدم، خادم، وحدة تنظيمية...). بمعنى آخر، قد تكون هناك عقد ذات قيمة بينية منخفضة، ولكنها تؤدي دورًا حاسماً في ربط أجزاء معينة من الشبكة أو في تسهيل الوصول إلى موارد حساسة.

لذلك، فإن تقييم التهديدات الأمنية يجب ألا يعتمد فقط على المؤشرات الكمية مثل"Betweenness" ، بل لا بد من دمجها مع معلومات سياقية دقيقة حول طبيعة العقد ووظائفها ضمن البيئة. هذا التكامل بين التحليل الهيكلي والمحتوى السياقي يمنح رؤية أكثر واقعية ودقة في تحديد النقاط الأكثر عرضة للاستهداف. في النهاية، توضح النتائج أن حماية الشبكة بشكل فعّال لا يكفي أن نركز فقط على العقد الأهم أو نُعطّلها، بل يجب أن نفهم كيف ستتغير البيئة بالكامل بعد هذه الإجراءات. فعند إزالة أو تأمين عقدة مهمة، قد تنتقل أهميتها إلى عقد أخرى، وهذا قد يفتح مسارات جديدة يمكن أن يستغلها المهاجمون. لذلك من الضروري مراقبة هذه التغيرات وفهم تأثيرها الكامل، حتى نتمكن من تصميم نظام حماية أكثر ذكاءً وقادر على التكيّف مع التهديدات الجديدة.

٤,٢,٥ اقتراح أوزان للعقد حسب نوع العقدة:

ضمن إطار هذا البحث، قمت باقتراح نظام أوزان عددي لتصنيف أهمية العقد الأمنية في بيئة Active Directory، اعتماداً على نوع كل عقدة، وليس فقط على موقعها في الرسم البياني أو قيمتها من حيث البينية . (Betweenness)يهدف هذا النظام إلى توفير مؤشر نوعي إضافي يُستخدم مع المؤشرات الكمية لتحديد مدى خطورة أو أهمية العقد المختلفة، وهو ما يساهم في تقييم درجة الأمان بشكل أكثر شمولية وواقعية.

تم تخصيص الأوزان من 1إلى ٧ وفقًا للخطورة النسبية لكل نوع عقدة، وذلك كما يلي:

الجدول (4): الأوزان المقترحة للعقد.

نوع العقدة	الوزن	المبرر الأمني
ذات قيمة عالية(High Value)	٧	تحتوي على بيانات حساسة أو معلومات إدارية حيوية للشبكة، مثل بيانات الاعتماد، البيانات المالية ،ما يجعلها من أهم أهداف المهاجمين في أي بيئة رقمية [7].
الدومين(Domain)	٦	يتحكم بإدارة المستخدمين والصلاحيات، لكنه لا يحتوي على بيانات حساسة بدرجة عالية مثل عقد"High Value" .[8]
كائن نهج المجموعة(GPO)	٥	يفرض السياسات الأمنية، لكنه يعتمد على "الدومين" للنشر. له سيطرة أقل على الوصول والصلاحيات مقارنة بـ"الدومين" [9].
جهاز (Computer)	٤	يمثل نقاط وصول فردية ولكنه يؤثر على عدد أقل من العقد إذا تم اختراقه مقارنة بالسياسات الشاملة مثل GPO أو Domain[10].
مجموعة(Group)	٣	تدير امتيازات المستخدمين ولكنها لا تستطيع تنفيذ السياسات أو حماية الأجهزة بمفردها، لذا تأثيرها أقل من "Computer" [11].
وحدة تنظيمية(OU)	٢	تُعرّف البنية التنظيمية فقط، ودورها إداري بحت. نادراً ما يكون لها تأثير مباشر على الأمن [12].
مستخدم(User)	١	يعتمد تأثير المستخدمين على الصلاحيات والسياسات المُحددة من عقد أعلى. تأثيرهم الأمني ضئيل ما لم يكن لديهم صلاحيات مرتفعة [11].

٤,٢,٦ اقتراح معادلة تصنيف "درجة الأمان" (Security Score):

استناداً إلى التحليل الكمي (قيمة البينية) والتحليل النوعي (أوزان أنواع العقد)، قمنا باقتراح معادلة رياضية لحساب درجة الأمان لكل عقدة في بيئةActive Directory ، تهدف هذه المعادلة إلى تحقيق توازن بين المركزية البينية للعقدة وأهميتها السياقية ضمن البيئة:

$$\text{Security Score} = \beta \times \log(\text{Betweenness} + 1) + \alpha \times \text{Weight}$$

حيث:

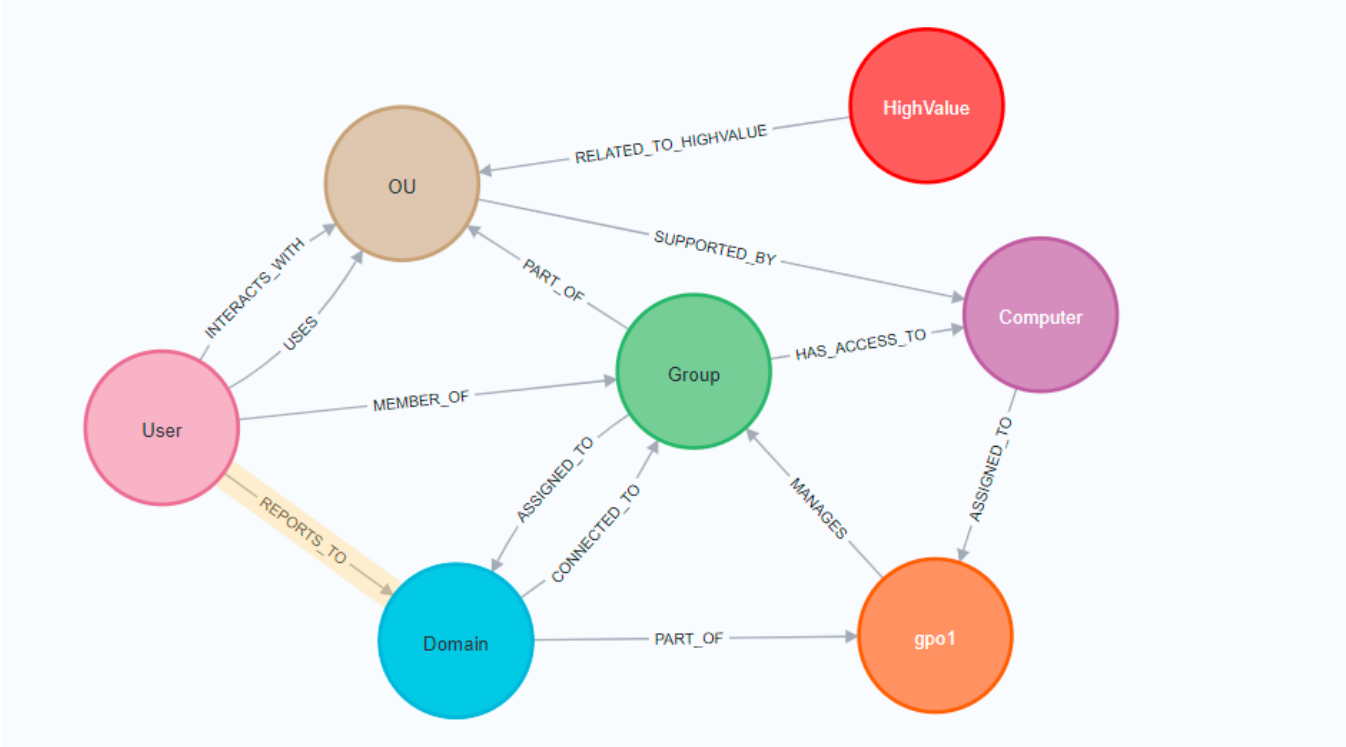
- Betweenness:تمثل عدد المسارات عبر العقدة.
- Weight:تمثل الأهمية النسبية لنوع العقدة مثل Domain أوUser .
- αوβ: ثوابت تتراوح بين ٠ و١، تُستخدم لضبط تأثير كل معامل حسب طبيعة البيئة.

تعتمد المعادلة المقترحة لحساب درجة الأمان لكل عقدة في بيئة Active Directory على مبادئ مستخدمة في عدة أبحاث علمية حديثة. فقد أشار Noel وآخرون إلى أن استخدام مقياس البينية (Betweenness Centrality)يُعد مؤشراً فعّالاً لتحديد العقد الحرجة في الشبكات من حيث احتمالية استغلالها في مسارات الهجوم [13]. كما أن اعتماد التحجيم اللوغاريتمي لقيمة البينية، كما هو مستخدم يساعد في تقليل الانحراف الناتج عن القيم الكبيرة جداً، وهو أمر موصى به في دراسات تحليل الشبكات الاجتماعية مثل دراسة Freeman [14] .

أما إدراج الأوزان المرتبطة بأنواع العقد (مثلUser ، Computer، Domain) فقد تمت الإشارة إليه في منصة التحليل الأمني CyGraph، والتي تبني نماذج المخاطر استناداً إلى خصائص العقد وسياقها ضمن بيئة العمل [15]. كما أن استخدام معاملات قابلة للتخصيص مثل α و β يتماشى مع الأساليب المعتمدة في نماذج تقييم المخاطر الديناميكية، حيث يمكن ضبط هذه المعاملات لتتناسب مع طبيعة كل بيئة على حدة.

2.2.7 مثال تطبيقي على المعادلة المقترحة :

تم تطبيق هذه المعادلة على رسم بياني جزئي يمثل سيناريو نموذجي داخل بيئةActive Directory ، حيث تتضمن العقد من أنواع مختلفة مثل: مستخدم، مجموعة، وحدة تنظيمية، جهاز، دومين، GPO، وعقدة ذات قيمة عالية.



الشكل (3): رسم بياني جزئي يمثل سيناريو نموذجي .

وباستخدام بيانات البينية والأوزان الخاصة بكل عقدة، تم احتساب درجة الأمان النهائية لكل عقدة .

	Node	betweenness	Weight	SecurityScore
1	"gpo1"	7.0	5	3.539720770839918
2	"hv1"	0.0	7	3.5
3	"domain1"	1.5	6	3.4581453659370776
4	"computer1"	6.5	4	3.0074515102711326
5	"group1"	9.333333333333334	3	2.667687457908518
6	"ou1"	4.666666666666667	2	1.867300527694053
7	"user1"	0.0	1	0.5

7 properties, started streaming 7 records after 1 ms and completed after 9 ms.

الشكل (4): يظهر نتائج درجة الأمان النهائية للعقد وتنفيذه على نظام neo4j.

يعكس هذا الجدول العلاقة بين قيمة البينية والوزن الأمني، حيث نجد على سبيل المثال أن عقدة مثل **gpo1** ذات بينية عالية ووزن متوسط حققت أعلى درجة أمان نسبية، في حين أن عقدة **user1** ذات

الوزن الأدنى والبينية الصفرية حصلت على أقل تقييم.

في حال استخدام منهجية [٤] المعتمدة على أدوات مثلBloodHound ، كان التقييم سيُظهر gpo1 كعقدة حرجة فقط لارتفاع البينية، لكنه لن يأخذ بعين الاعتبار السياق الوظيفي للعقدة. في المقابل، كانت العقدة user1ستظهر أيضاً كعقدة غير مهمة فقط لعدم وجود مسارات تمر عبرها، دون النظر إلى أهميتها النوعية المحتملة.

أما في حالة نموذج إدارة المخاطر التقليدي [٥] مثلOCTAVE ، فإن التقييم كان سيركز على الوزن النوعي للعقدة(Domain ، User، GPO...) لكنه لن يتمكن من تمييز العقد الوسيطة عالية البينية مثل gpo1التي تُشكّل نقاط مرور استراتيجية في مسارات الهجوم.

٥ النتائج والمناقشة

أظهرت نتائج الدراسة أن العقد التي تُعتبر "حرجة" وتمتلك أعلى قيمة في مقياس البينية، لها تأثير مباشر وكبير على عدد المسارات التي قد يستخدمها المهاجم داخل بيئة Active Directory على سبيل المثال، عند تعطيل عقدة مثلADMINS@TestCompany.Local ، انخفض عدد المسارات من ٥٦٨ إلى ٤٢٦، مما يعني أن هذه العقدة كانت تمرّ من خلالها الكثير من المسارات الحيوية.

لكن الملفت للنظر أن تعطيل هذه العقدة أدى إلى ارتفاع أهمية عقد أخرى كانت تُعتبر أقل أهمية في البداية. فعقدة مثل KarineBallenge58@TestCompany.Local ارتفعت قيمة البينية لديها بشكل كبير بعد إزالة العقدة الأساسية، مما يجعلها نقطة عبور جديدة للمهاجمين. وهذا يشير إلى أن حماية البيئة ليست عملية ثابتة، بل تتغير باستمرار حسب التعديلات التي تتم على هيكل النظام ،لذلك من الضروري متابعة وفحص العقد بشكل مستمر وليس فقط التركيز على العقد الواضحة أو المعروفة بأنها "مهمة".

وكما أظهرت نتائج تطبيق المعادلة المقترحة لقياس درجة الأمان Security Score أن دمج مقياس البينية مع الأوزان السياقية يوفر تصنيفاً أكثر دقة للعقد داخل البيئة على سبيل المثال، حققت العقد التي تجمع بين قيمة بينية مرتفعة ونوع حساس مثل GPO أو Domain أعلى درجات الأمان وفقاً للمعادلة،هذه النتائج تتوافق مع ما أشار إليه Herranz وآخرون [٤] حول فعالية البينية في تحديد العقد الحرجة، ولكنها تضيف بعداً جديداً وهو دمج السياق الأمني والوظيفي للعقد، كما أن إدراج مفهوم الأوزان المستندة إلى نوع العقدة يتقاطع مع المبادئ التي بنيت عليها نماذج إدارة المخاطر مثل [5] OCTAVE، إلا أن تطبيقه في بيئة واقعية ومعقدة مثل Active Directoryيُعد مساهمة إضافية لهذا البحث.

٦ الاستنتاجات والتوصيات

الاستنتاجات:

١. بعد إزالة عقدة مهمة، يمكن أن تصبح عقد أخرى أكثر أهمية من الناحية الأمنية.

٢. الدمج بين مقياس البينية ونوع العقدة (من خلال الوزن) يعطي تقييمًا أكثر دقة لدرجة الأمان.

التوصيات:

- استخدام نظام يراقب تغيّرات البينية بشكل دائم بعد أي تعديل في البيئة.
- توسيع الدراسة مستقبلاً لتشمل بيئات أكثر تعقيداً مثل البيئات السحابية.

٧ الخاتمة

توضح هذه الدراسة أهمية استخدام تقنيات تحليل الرسم البياني مثل خوارزمية البينية لفهم كيفية نقل الهجمات داخل الشبكة. من خلال بناء نموذج توأم رقمي لبيئة Active Directory وتحليل تأثير إزالة العقد الحرجة، تبين أن الشبكة تتغير بشكل ديناميكي.

إن استخدام معادلة تجمع بين التحليل الكمي (كقيمة البينية) والتحليل النوعي (مثل نوع العقدة)، يعطي رؤية أوضح وأكثر توازنا لتحديد أولويات الحماية. وتُعدّ هذه الخطوة تمهيداً لتصميم أنظمة حماية ذكية قادرة على التكيّف مع التغيرات البنيوية داخل الشبكات.

٨ المراجع:

1. Microsoft, *"Active Directory Domain Services Overview,"* Microsoft Learn, Feb. 20, 2025. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
2. U.S. Department of Defense, *Detecting and Mitigating Active Directory Compromises*, Defense Technical Information Center, 2024. [Online]. Available: https://media.defense.gov/2024/Sep/25/2003553985/-1/-1/0/CTR-Detecting-and-Mitigating-AD-Compromises.PDF
3. GitHub, *"neo4j-graph-examples/cybersecurity,"* GitHub Repository. Retrieved on May 17, 2025. [Online]. Available: https://github.com/neo4j-graph-examples/cybersecurity
4. Herranz Oliveros, D., Tejedor Romero, M., Gimenez Guzman, J. M., and Cruz Piris, L., *"Unsupervised Learning for Lateral Movement Based Threat Mitigation in Active Directory Attack Graphs," Electronics*, vol. 13, no. 19, Article 3944, Oct. 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/19/3944
5. Alberts, C. J., and Dorofee, A. J., *Managing Information Security Risks: The OCTAVE Approach*, Software Engineering Institute, Carnegie Mellon University, 2001. [Online]. Available: https://insights.sei.cmu.edu/documents/17/2001_012_001_51564.pdf
6. Neo4j, *"Cybersecurity Sandbox,"* (n.d.). Retrieved on May 17, 2025. [Online]. Available: https://sandbox.neo4j.com/?usecase=cybersecurity
7. National Institute of Standards and Technology (NIST), *Zero Trust Architecture*, NIST Special Publication 800-207, 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207
8. Ferraiolo, D. F., and Kuhn, D. R., *"Role-Based Access Controls," arXiv*, Mar. 2009. [Online]. Available: https://arxiv.org/abs/0903.2171
9. Microsoft, *"Group Policy Overview,"* Microsoft Learn. Retrieved on May 17, 2025. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/group-policy-overview
10. Microsoft, *"Endpoint Protection Overview,"* Microsoft Learn. [Online]. Available: https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-protection-overview
11. National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Rev. 5, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
12. Petri IT Knowledgebase, *"Mastering Active Directory OU: A Comprehensive Guide,"* Sep. 27, 2023. [Online]. Available: https://petri.com/active-directory-ou/
13. Noel, S., Jajodia, S., O'Berry, B., and Jacobs, M., *"Efficient Minimum-Cost Network Hardening via Exploit Dependency Graphs," Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC)*, 2010.
14. Freeman, L. C., *"Centrality in Social Networks: Conceptual Clarification," Social Networks*, vol. 1, no. 3, pp. 215–239, 1979.
15. Jajodia, S., Noel, S., and O'Berry, B., *CyGraph: A Knowledge Graph-Based Cybersecurity Analytics Platform*, Springer, 2017.