الجمهورية اليمنية
جامعة العلوم والتكنولوجيا
كلية الحاسبات وتكنولوجيا المعلومات
قسم تقنية المعلومات – فرع الحديدة

بناء اداه لكسر كلمة مرور Windows 10

إعداد الطلاب:

1. صلاح عبدالله محمد عبد
2. عبدالله نادر عبدالله معجم
3. يحيى محمد يحيى جون

إشراف:

م.م.محمد حسن بامشموس

تم إنجاز هذا البحث كجزء من متطلبات نيل شهادة البكالوريوس في قسم تقنية المعلومات للعام الجامعي 2024-2025م

الخلاصة

تطوير أداة متقدمة لاستعادة كلمة مرور نظام Windows 10 باستخدام لغة Python.

تعمل على استعادة كلمة المرور للنظام في حال تم نسيانها.

تهدف الى دراسة متعمقة في نظام التشغيل والعمل على حماية البيانات من فقدانها.

تعمل هذه الأداة من خلال مكتبات بلغة Python مع استخدام تقنيات التشفير ذات العلاقة بإيجاد كلمة المرور المنسية.

يتم من خلالها الحصول على كلمة المرور التي تم نسيانها وإمكانية إعادة تعيينها بسهولة مما يسمح ذلك بأداء أكثر كفاءة وفعالية للأداة في تعاملها مع نظام التشغيل.

تعزز هذه الأداة أمنية وموثوقية عالية لحماية بيانات النظام الأساسية من الفقدان أو التلف.

الفصل الأول

المقدمة

1.1: تمهيد للموضوع الذي يتناوله المشروع.

تصميم أداة متقدمة باستخدام لغة Python وهي عبارة عن أداة تعمل على استعادة كلمة مرور نظام Windows 10 بطريقة سلسة وأمنة من خلال استخدام مكتبات لغة Python بجانب أليات التشفير الحديثة المرتبطة ببعضها البعض في استرجاعها وإمكانية تعيينها دون حدوث أي فقدان أو تلف لبيانات النظام الأساسي بكفاءة وفاعلية أعلى مما يعزز على رفع مستوى الأمنية والموثوقية في التعامل مع نظام التشغيل Windows.

2.1: المشاكل المراد حلها.

1. إمكانية فقدان أو تلف البيانات الموجودة في النظام.
2. تعدد وتداخل خوارزميات التشفير ببعضها البعض في جانب التشفير وفك التشفير لكلمة المرور.
3. تعقيد الوقت (Time Complexity) الكبير في عملية التخمين لكلمة المرور بسبب قيام نظام التشغيل Windows بعملية التجزئة لها.

3.1: أهداف المشروع.

1. الحصول على كلمة المرور المشفرة بوقت قصير.
2. إمكانية إعادة تعيينها بسلاسة وسهولة أكبر.
3. الحفاظ على البيانات المهمة في نظام Windows من الفقدان أو التلف.
4. رفع مستوى الأمنية وتحقيق الموثوقية العالية.

4.1: نطاق المشروع.

1. **النطاق الزمني للمشروع**: سنة دراسية كاملة.
2. **النطاق المكاني للمشروع**: الشركات التقنية والمنظمات بكافة أنواعها وغيرها من أماكن العمل الأخرى العاملة في الجانب التقني وأيضاً الأفراد (أي المستخدمين النهائيين) لنظام التشغيل Windows10.

5.1: المعوقات والحلول الافتراضي.

1. صعوبة الوصول إلى ملفات النظام الحساسة مثل ملف SAM الذي يحتوي على بيانات كلمة المرور.
2. تعقيد تشفير كلمة المرور وذلك باستخدام خوارزمية تشفير قوية تجعل كسر كلمة المرور امرا صعباً.
3. قيود الامان في النظام مثل BitLocker التي تمنع الوصول الى القرص الصلب عند نسيان كلمة المرور.
4. التحديثات المستمرة لنظام windows التي بدورها تغلق الثغرات المستخدمة في استعادة كلمة المرور.

6.1 :الادوات المستخدمة.

1. لغة البرمجة Python: لاستخدامها في تطوير الأداة وتطبيق تقنيات التشفير العكسي واستغلال الثغرات.
   . مكتبة os في Python: للوصول الى ملفات النظام والتعامل مع التعليمات المتعلقة بل النظام.
   . مكتبة hashlib: لمعالجة وفك تشفير تجزئات كلمات المرور (hashes)عند الحاجة.
   . مكتبة Pywin32: لتفاعل مع Windows API والوصول الى المعلومات المخزنة في النظام.
   . مكتبة cryptography: لتطبيق تقنيات التشفير وفك التشفير عند التعامل مع كلمة المرور.
   . مكتبة winreg: للوصول والتعديل في سجل النظام (Registry) حيث قد تكون معلومات كلمة المرور المشفرة.
2. نظام التشغيل Windows 10.
3. واجهة برمجة التطبيقات Windows API: لاستخدامها لتفاعل مع النظام بشكل مباشر.
4. بيئة التطوير المكتملة (IDE) مثل PyCharm او Visual Studio Code لتطوير واختبار الأداة.
5. اله افتراضية (Virtual Machine) لتجربة الأداة في بيئة معزولة وامنه اثناء عملية البناء.

7.1 : **المنهجية المستخدمة للمشروع.** :

سيتم استخدام منهجية (**XP**) اختصاراً لاسم المنهجية (**Extreme Programming**) وذلك وفقًا للأسباب التالية:

1. تقسيم المشروع إلى دورات تكرارية قصيرة والتي يتم من خلالها التصميم والتطوير والاختبار للمشروع.
2. إمكانية عمل مطوران معًا على نفس الكود البرمجي وتشارك المعارف والخبرات ومساعدة بعضهما البعض على تحقيق الأهداف المشتركة والمعتمدة على مفهوم (Pair Programming).
3. تتسم بالبساطة (Simplicity) بمعنى أنها تسعى جاهدة إلى تنفيذ الحل الأبسط والأمثل الذي يمكنه تلبية مجموعة المتطلبات الحالية [1].
4. إمكانية دمج التعديلات المقترحة على المشروع مما يعزز من قدرة المشروع على التعامل مع التغييرات عن طريق التخطيط المرن والتواصل المستمر والتقييم المنتظم.

8.1 : **تنظيم المشروع**

ويقصد به تحديد الفصول التي يتناولها البحث ومحتوى كل فصل.

تحتوي وثيقة التقرير هذه على ستة فصول بما في ذلك هذا الفصل.

- الفصل الثاني: (الخلفية النظرية)

يحتوي هذا الفصل على الخلفية النظرية لبعض المفاهيم الأساسية التي لها علاقة بالمشروع. ومنها نبذة عن أمن المعلومات وكلمة المرور والتشفير مع استعراض الدراسات السابقة.

- الفصل الثالث: (التحليل)
- الفصل الرابع: (التصميم)
- الفصل الخامس: (التنفيذ)
- الفصل السادس: (الاستنتاجات والتوصيات)

الفصل الثاني

الخلفية النظرية

المقدمة :

في هذا الفصل، سنستعرض الخلفية النظرية التي تشكل الأساس لتصميم أداة لكسر كلمة مرور ويندوز. سيتم تقديم شرح للمفاهيم الأساسية المرتبطة بأمن المعلومات وإدارة كلمات المرور في أنظمة التشغيل، بالإضافة إلى مراجعة الدراسات السابقة المتعلقة بهذا المجال. سنقوم أيضًا بتحليل الأدوات الحالية المستخدمة في كسر كلمات المرور من حيث مزاياها وعيوبها، مع تقديم هذا التحليل في شكل جدول.

2.1 المفاهيم الاساسية :

1.1. 2امن المعلومات.

أمن المعلومات يشير إلى حماية البيانات والمعلومات الحساسة من الوصول غير المصرح به، التعديل، أو التدمير. يشمل ذلك الحفاظ على سرية، تكامل، وتوافر المعلومات.

أهمية أمن المعلومات: في سياق إدارة كلمات المرور، يعتبر أمن المعلومات بالغ الأهمية لأنه يضمن حماية البيانات الشخصية والحسابات من الاختراق.

2.2.1 كلمة المرور:

كلمة المرور هي سلسلة من الأحرف، الأرقام، أو الرموز التي تُستخدم للتحقق من هوية المستخدم عند الوصول إلى نظام معين.

دور كلمات المرور في الأمان: تعتبر كلمات المرور خط الدفاع الأول ضد الوصول غير المصرح به إلى الحسابات والنظم، وبالتالي يجب أن تكون قوية وصعبة التخمين.

3.1.2 التشفير:

التشفير هو عملية تحويل البيانات إلى صيغة غير قابلة للقراءة إلا باستخدام مفتاح أو خوارزمية معينة.

أنواع التشفير المستخدمة في كلمات المرور.

- التشفير المتماثل :(Symmetric Encryption) يستخدم مفتاحًا واحدًا للتشفير وفك التشفير.
- التشفير غير المتماثل :(Asymmetric Encryption) يستخدم مفتاحين، أحدهما للتشفير والآخر لفك التشفير.

• التجزئة :(Hashing) عملية تحويل كلمة المرور إلى سلسلة مشفرة يصعب عكسها. تستخدم خوارزميات مثل MD5 وSHA-256 في تجزئة كلمات المرور.

4.1.2 إدارة كلمات المرور في ويندوز

• ملف :(Security Account Manager) SAM

هو ملف في نظام التشغيل ويندوز يحتوي على حسابات المستخدمين وكلمات المرور الخاصة بهم.

• كيفية عمله: يقوم بتخزين كلمات المرور كقيمة مجزأة (Hashed) ولا يحتفظ بالنص الأصلي لكلمات المرور.

• بروتوكول **:NTLM (NT LAN Manager)**

• التعريفNTLM : هو بروتوكول أمان لشبكات ويندوز يُستخدم للتحقق من هوية المستخدمين.

• كيفية عمله: يعتمد على توليد وتخزين التجزئات لكلمات المرور، والتي تُستخدم للتحقق من صحة كلمة المرور عند تسجيل الدخول.

5.1.2 تقنيات كسر كلمات المرور.

1- لقوة العمياء **:(Brute Force)**

• التعريف: تقنية كسر كلمات المرور عن طريق تجربة جميع التوليفات الممكنة حتى العثور على الكلمة الصحيحة.

• التحديات: تستغرق وقتًا طويلاً خاصة مع كلمات المرور الطويلة والمعقدة.

2 -هجمات قوس قزح **:(Rainbow Tables)**

• التعريف: تقنية تستخدم جداول مُعدة مسبقًا تحتوي على التجزئات وكلمات المرور المقابلة لها لتسريع عملية كسر كلمة المرور.

•التحديات: تتطلب مساحة كبيرة لتخزين الجداول، وفعالة فقط مع كلمات المرور المخزنة باستخدام تجزئة بسيطة.

3 - الهجمات القائمة على التحليل **:(Dictionary Attacks)**

• التعريف: هجمات تستخدم قوائم من الكلمات الشائعة أو كلمات المرور التي تُستخدم في كثير من الأحيان.

• التحديات: غير فعالة مع كلمات المرور الفريدة أو التي تحتوي على تركيبات معقدة

3 - الدراسات السابقة:

تستعرض الدراسات السابقة الأدوات الشائعة مثل chntpw، Ophcrack، John the Ripper،

Abel & Cain، Hashcat مع تقديم تقييم شامل لكل منها بناءً على اراء المستخدمين لهذه الادوات.

وسيتم ذكر كل أداة مع اهم المزايا والعيوب:

الأداة	المزايا	العيوب
chntpw	مفتوحة المصدر.- فعالة في تعديل ملفات SAM.- سهلة الاستخدام بالنسبة للمستخدمين ذوي الخبرة	قد تكون محدودة في التعامل مع كلمات مرور معقدة.- تحتاج إلى خبرة فنية للتشغيل بشكل صحيح.
Ophcrack	تستخدم جداول قوس قزح لاسترجاع كلمات المرور بسرعة .- مجانية وسهلة الاستخدام.- تدعم مجموعة واسعة من أنظمة التشغيل.	- تحتاج إلى مساحة كبيرة لتخزين جداول قوس قزح. - أقل فعالية مع كلمات مرور قوية ومعقدة-. يتطلب إعدادًا معقدًا للجداول.
John the Ripper	- يدعم مجموعة واسعة من أنظمة التشغيل وتنسيقات كلمات المرور - فعال في استخدام تقنيات متعددة مثل القوة العمياء والقاموس-. قابل للتخصيص وفقًا لاحتياجات المستخدم.	- قد يستغرق وقتًا طويلاً مع كلمات المرور المعقدة.- - يتطلب إعدادات متقدمة-. قد يكون صعب الاستخدام للمبتدئين.
Cain & Abel	- واجهة مستخدم سهلة الاستخدام-. تدعم استرجاع كلمات المرور عبر الشبكة.- - تحتوي على أدوات متعددة مثل تحليل الشبكة واستعادة كلمات المرور.	- قد تكون غير فعالة مع كلمات المرور المشفرة بشكل قوي-. - لا تتلقى تحديثات منتظمة-. قد تثير مخاوف تتعلق بالسلامة والأمان.
Hashcat	- واحد من أقوى أدوات كسر كلمات المرور باستخدام تقنيات مختلفة مثل القوة العمياء وقاموس الهجمات.- - يدعم العديد من خوارزميات التجزئة-. يمكن تسريعه باستخدام GPU.	- قد يكون معقدًا للمستخدمين الجدد.- - يتطلب مواصفات عتاد قوية لتحقيق أفضل أداء-. يتطلب إعدادًا دقيقًا.