

(أنشطة – ومشروع) نادي الأمن السيبراني

الفهرس

رقم الصفحة	العنوان
2	تحليل البيانات النصية
5	تحليل البيانات الضارة
8	مشروع: تأمين شبكة منزلية باستخدام أدوات وتقنيات متعددة

تحليل البيانات النصية

فك تشفير النصوص

-النص الأول:

النص المشفر: SGVsbG8hIFRoaXMgaXMgYSBzZWNyZXQgbWVzc2FnZS

•التقنية المستخدمة: Base64

•فك التشفير: import base64

```
encoded_text1 = "SGVsbG8hIFRoaXMgaXMgYSBzZWNyZXQgbWVzc2FnZS"
```

```
decoded_text1 = base64.b64decode(encoded_text1).decode('utf-8')
```

```
print(decoded_text1)
```

النص الناتج:

"Hello! This is a secret message"

-النص الثاني:

النص المشفر: RkxBR3tZMHVfY2FuX2RIY29kZV90aGlzfQ

•التقنية المستخدمة: Base64

•فك التشفير:

```
encoded_text2 = "RkxBR3tZMHVfY2FuX2RIY29kZV90aGlzfQ"
```

```
decoded_text2 = base64.b64decode(encoded_text2).decode('utf-8')
```

```
print(decoded_text2)
```

النص الناتج: "FLAG{0hucandHcode_this}"

-النص الثالث:

النص المشفر: VGhpcyBpcyBhIHRlc3Qgb2YgZW1lcmdlbmN5IG1lc3NhZ:

•التقنية المستخدمة: Base64

• فك التشفير:

```
encoded_text3 = "VGhpcyBpcyBhIHRlc3Qgb2YgZW1lcmdlbmN5IG1lc3NhZ"
```

```
decoded_text3 = base64.b64decode(encoded_text3).decode('utf-8')
```

```
print(decoded_text3)
```

النص الناتج : "This is a test of emergency message"

- تحليل محتوى النصوص

-النصوص المستخرجة:

1. "Hello! This is a secret message"

•الموضوع: رسالة سرية.

•الأسلوب اللغوي: مباشر وبسيط، يستخدم أسلوب التعريف.

2. "FLAGR{0hucandHcode_this}"

•الموضوع: يبدو أنها تنتمي إلى تحدي أو مسابقة.(Flag)

•الأسلوب اللغوي: مزيج من الحروف والأرقام، مما يدل على تقنية تشفير أو تحدي.

3. "This is a test of emergency message"

•الموضوع: اختبار لرسالة طوارئ.

•الأسلوب اللغوي: واضح ومباشر، يستخدم لغة بسيطة.

- الرسالة الرئيسية

الرسالة الرئيسية التي يمكن استنتاجها من النصوص هي أهمية التواصل السري والاختبارات المتعلقة بالأمان. النص الثاني يشير إلى تحديات البرمجة أو الأمن السيبراني.

- اقتراحات لتحسين أمان التشفير

1- استخدام تقنيات تشفير أقوى:

• الانتقال من تقنيات بسيطة مثل Base64 إلى تقنيات تشفير أكثر تعقيدًا مثل AES (Advanced Encryption Standard).

2- تطبيق مفاتيح سرية:

• استخدام مفاتيح سرية لتشفير وفك تشفير الرسائل بدلاً من الاعتماد على خوارزميات بسيطة.

3- تقييم أمان النظام بانتظام:

• إجراء اختبارات اختراق دورية لضمان عدم وجود ثغرات في نظام التشفير.

4- التشفير متعدد الطبقات:

• استخدام طبقات متعددة من التشفير لضمان حماية البيانات بشكل أفضل.

5- توعية المستخدمين:

• تثقيف المستخدمين حول مخاطر الأمان وكيفية التعامل مع البيانات الحساسة بشكل آمن.

بهذه الطريقة، يمكن تحسين أمان التشفير المستخدم في النصوص وضمان حماية أفضل للمعلومات.

تحليل البرمجيات الضارة

تقرير تحليل البرمجيات الضارة

- تحليل الملف

- وصف السيناريو

تم اكتشاف ملف مشبوه في شبكة المؤسسة، ويُعتقد أنه يحتوي على برنامج ضار. تم اختيار ملف بامتداد .exe. لتحليله.

- أدوات التحليل المستخدمة

• لتحليل الملف ضد قاعدة بيانات ضخمة من البرمجيات الضارة: VirusTotal

• لتحليل سلوك البرنامج في بيئة معزولة: Cuckoo Sandbox

• لمراقبة الأنشطة التي يقوم بها البرنامج عند التشغيل: Process Monitor (ProcMon)

• لمراقبة حركة الشبكة الناتجة عن الملف: Wireshark

• لتحديد نوع الحماية المستخدمة في الملف التنفيذي: PEiD

- خطوات التحليل

1- رفع الملف إلى VirusTotal للتحقق من وجود أي تقارير سابقة حول الملف.

2- تشغيل الملف في Cuckoo Sandbox لمراقبة السلوكيات مثل إنشاء ملفات جديدة، تعديل السجل، أو الاتصالات الشبكية.

3- استخدام Process Monitor لتسجيل الأنشطة مثل العمليات، والملفات، والتغييرات في السجل.

4- مراقبة حركة الشبكة باستخدام Wireshark لرصد أي اتصالات غير عادية قد يقوم بها البرنامج.

- تحديد نوع البرمجية الضارة

سلوك الملف

بعد التحليل، لوحظ أن الملف يقوم بما يلي:

- إنشاء ملفات جديدة في مجلدات النظام.
- تعديل مفاتيح السجل المتعلقة بالتشغيل التلقائي.
- إجراء اتصالات خارجية إلى عناوين IP مشبوهة.

- نوع البرنامج الضار

استنادًا إلى السلوكيات المذكورة، يمكن تصنيف هذا البرنامج كفيروس أو دودة .

- الفيروس: يتطلب وجود ملف مضيف وينتشر عن طريق نسخ نفسه إلى ملفات أخرى.
- الدودة: يمكن أن تنتشر عبر الشبكة دون الحاجة إلى ملف مضيف.

- كيفية التعرف على هذا النوع من البرامج الضارة

- الفيروسات عادة ما تتطلب تفاعل المستخدم (مثل فتح ملف).
- الدود تنتشر بشكل مستقل عبر الشبكات وتقوم بإصابة أنظمة أخرى.

- طرق التخفيف

- توصيات للحماية

1- استخدام برامج مكافحة الفيروسات:

- تثبيت وتحديث برامج مكافحة الفيروسات بانتظام لضمان الكشف عن البرمجيات الضارة.

2- تطبيق جدران الحماية:

- استخدام جدران الحماية لتقييد حركة المرور غير المصرح بها ومنع الاتصالات المشبوهة.

3- تحديث النظام والبرامج:

- التأكد من تحديث نظام التشغيل والبرامج بشكل دوري لسد الثغرات الأمنية.

4- التوعية والتدريب:

- تقديم دورات تدريبية للموظفين حول كيفية التعرف على البرمجيات الضارة وطرق تجنبها، مثل عدم فتح مرفقات البريد الإلكتروني غير المعروفة.

5- النسخ الاحتياطي المنتظم:

- إجراء نسخ احتياطي منتظم للبيانات الهامة لضمان استعادة البيانات في حالة التعرض لهجوم برمجي.

6- تقييد الامتيازات:

- تطبيق مبدأ أقل امتياز، بحيث يتم منح المستخدمين الحد الأدنى من الحقوق اللازمة لأداء مهامهم.

الخاتمة:

من خلال التحليل الدقيق للملف المشبوه واستخدام الأدوات المناسبة، تم تحديد نوع البرمجية الضارة المقترنة بالملف وتقديم توصيات فعالة للتخفيف من المخاطر.

الالتزام بهذه الإجراءات سيساعد في حماية الشبكة والنظام من الهجمات المستقبلية.

المشروع

تأمين شبكة منزلية باستخدام أدوات وتقنيات متعددة

المقدمة

في عصر التكنولوجيا الحديثة، أصبحت الشبكات المنزلية هدفًا متزايدًا للهجمات الإلكترونية. يهدف هذا المشروع إلى تصميم وتطبيق استراتيجية شاملة لتأمين شبكة منزلية، مع التركيز على إعداد أمن الشبكات، البرمجة الآمنة، وتطبيقات التشفير.

أهداف المشروع

- 1- تحليل التهديدات المحتملة: تحديد أنواع الهجمات التي قد تستهدف الشبكة المنزلية.
- 2- إعداد الشبكة: تكوين جهاز التوجيه (Router) بشكل آمن.
- 3- تنفيذ البرمجة الآمنة: تطوير تطبيق ويب بسيط يستخدم لتسجيل الدخول إلى الشبكة.
- 4- تطبيق التشفير: استخدام بروتوكولات التشفير لحماية البيانات المتداولة.

خطوات تنفيذ المشروع

1- تحليل التهديدات

• إجراء دراسة حول أنواع الهجمات الشائعة مثل:

- هجمات التصيد (Phishing)
- هجمات رفض الخدمة (DDoS)
- هجمات الاختراق (Hacking)

2- إعداد الشبكة

• تكوين جهاز التوجيه:

• تغيير كلمة المرور الافتراضية لجهاز التوجيه.

• تعطيل WPS (Wi-Fi Protected Setup).

• استخدام تشفير WPA3 إذا كان متاحًا.

• تحديث البرامج الثابتة: التأكد من تحديث البرامج الثابتة لجهاز التوجيه.

3- البرمجة الآمنة

• تطوير تطبيق ويب بسيط باستخدام HTML و PHP يتضمن:

• نموذج تسجيل دخول آمن.

• استخدام تقنيات مثل حماية XSS و CSRF.

مثال على كود تسجيل الدخول:

```
<?php
session_start();
if ($_SERVER["REQUEST_METHOD"] == "POST") {
$username = htmlspecialchars($_POST['username']);
$password = htmlspecialchars($_POST['password']);
// تحقق من صحة المستخدم وكلمة المرور
}
?>
<form method="POST" action="">
<input type="text" name="username" required>
<input type="password" name="password" required>
<input type="submit" value="Login">
</form>
```

4- تطبيق التشفير

- استخدام بروتوكولات HTTPS لتأمين الاتصال بين المستخدم والتطبيق.
- تطبيق تشفير البيانات الحساسة باستخدام AES (Advanced Encryption Standard).

التحديات والحلول

- التحدي 1: إعداد جهاز التوجيه بشكل آمن
- الحل: البحث عن أفضل الممارسات لتأمين أجهزة التوجيه وتنفيذها خطوة بخطوة.
- التحدي 2: تأمين التطبيق من الثغرات
- الحل: استخدام مكتبات أمان معروفة وتطبيق تقنيات التحقق من المدخلات.
- التحدي 3: فهم بروتوكولات التشفير
- الحل: دراسة مفاهيم التشفير المختلفة وتجربة تنفيذها في التطبيق.

النتائج

- تم تأمين الشبكة المنزلية بشكل فعال، مما قلل من مخاطر الهجمات.
- تم تطوير تطبيق ويب آمن يمكن استخدامه في البيئات المنزلية.
- تم تعزيز فهمي لمجالات متعددة في أمن السيبراني.

الخاتمة

يعتبر هذا المشروع خطوة مهمة نحو تعزيز مهاراتي في مجال أمن السيبراني. من خلال تنفيذ هذا المشروع، تمكنت من فهم التحديات الحقيقية التي تواجه الأمن السيبراني وتطوير حلول فعالة لها.

عرض المشروع النهائي

• تقديم عرض تقديمي يتضمن:

- شرح الأهداف والخطوات المتبعة.
- عرض النتائج والتحديات التي تم التعامل معها.
- الإجابة على الأسئلة من الزملاء والمدرسين.