2025

# Hacker

## الملـف التعـريـفـي

2025


# Hacker

## الملـــف التعـــريـــفـــي

2025


# من نحن

Hacker

في عالمٍ رقمي تتحكم فيه البيانات، يصبح الأمن السيبراني الحاجز الوحيد بين النظام والفوضى، بين الأمان والاختراق، وبين المعلومة والسر. HACKER ليس مجرد اسم، بل هو عقلية تعتمد على التحليل العميق، التفكير الاستباقي، وكشف ما هو غير مرئي. نحن نعمل على جميع الجبهات الرقمية، من اختبار الاختراق إلى تقييم المخاطر، ومن استخبارات المصادر المفتوحة إلى تنظيف البيانات وحماية الهوية الرقمية.

## نحن لا نقف عند الحماية التقليدية
## بل نـــرى ما وراء الجـــدران النـارية

نفكر كما يفكر المهاجم، ونبحث حيث لا يبحث الآخرون. نؤمن أن الأمن لا يتحقق فقط بامتلاك الأدوات، بل بفهم كيف يعمل الخصم، وكيف يمكن منعه قبل أن يتحرك.

2025

# رؤيتـــنا

Hacker

# نحن لا ننتظر الهجمات لتحدث، بل نستبقها.

رؤيتنا تتمحور حول خلق بيئة آمنة، ليست فقط عبر الدفاع، بل عبر الهجوم الاستباقي، كشف الثغرات، وتحليل المخاطر قبل وقوعها. في عالم تتطور فيه التقنيات بسرعة، لا مجال للركود، بل يجب أن نكون خطوة للأمام دائمًا.

نبحث عن نقـــاط الضعف قبل أن يجدها المهاجمون.

نقيـــم المخـــاطر قبل أن تتحول إلى تهديدات حقيقية

نختبر الدفاعات كما لو كنـــا الخصم نفسه

ننـــــظف البيانات قبل أن تقع في الأيدي الخطأ

2025

# قـــيمـــنا

Hacker

# قـــيمـــنا

## الاحتـــرافية

عمل بمعايير عالية، ونقدم تحليلات وتقـــارير دقيقة قائمة على أساليب علمية وتقنيـــات متقـــدمـــة.

## السـريـة التـــامة

نضمن التعامل مع البيانات بأمان مطلق، ونلتزم بأعلى مستـــويات الخصوصية

## الهجـــوم الاستبـــاقي

لا ننتظر وقوع المشكلة، بل نكشـفها ونعـالجها قبل أن تصبـــح تهديدًا

## التفكـــير كالخصم

لا يمكن حمـاية النظام دون فهم كيـــف يمكن اختراقه، ولهـــذا نختبر الدفاعات بنفس طريقة المهاجمـين الحقيقيين

## الابتكـــار التقـــني

نستخدم أحـــدث الأدوات في الأمن السيبراني، الاختراق الأخلاقي، استخبـــــارات المصادر المفتوحة، وتحليل البيانات لضمان الحمـــاية الفعالة


# لماذا نحن؟

# لماذا نحن؟

01

لأننا نرى الثغرات حيث يراهـــا الآخرون أمانًا.

02

لأننا نـــؤمن أن الحمـــــاية ليست مجرد أنظمة، بل عقلية واستراتيجية.

03

لأننا نعـــرف أن المعلـــومات هي القـــوة، والأمـــن الحقيقي يبدأ بمعرفة كيف يتم استغلالها.

04

لأننا لا نقدم مجرد تقارير، بل نكشف الواقع، ونساعد عملاءنا على اتخاذ قرارات بناءً على بيـــانات حقيقية وتحليل دقيق.


2025
خدمات
هکـــــر
Hacker
10

# البحث السريع – REAL-TIME ACCOUNT LOOKUP
## (خدمة تلقائية عبر الموقع)

- البحث عبر البريد الإلكتروني (EMAIL LOOKUP)
- البحث عبر رقم الهاتف (PHONE SEARCH)
- البحث عبر اسم المستخدم (USERNAME LOOKUP)
- كشف الحسابات المرتبطة (LINKED ACCOUNTS)
- تتبع المستخدم (USER TRACKING)

خدمة فورية تعتمد على الذكاء الاصطنــاعي والـ API المتصلة بمصادر OSINT، للكشـف عن الحسابات المرتبطة بمعلومات معينة مثل:

**المخرجات: تقرير فوري يحتوي على الحسابات المرتبطة بالمعلومة المدخلة.**

# البحث المعمق – ADVANCED OSINT INVESTIGATION
## (خدمة بطلب خاص)

تحليل متقدم ومفصل بناءً على طلب العميل، يتجاوز البحث السطحي ليشمل:

- تحليل شامل للبصمة الرقمية لتحديد جميع الأنشطة المرتبطة بشخص أو جهة معينة.
- استخراج بيانات محذوفة أو مخفية من الإنترنت وأرشيف المواقع.
- التحليل الزمني لنشاط الحسابات لكشف أي روابط خفية بين الأفراد أو المنظمات.
- تحليل البيانات الوصفية (METADATA ANALYSIS) في الصور والملفات الرقمية.
- تحليل الشبكات والعلاقات (NETWORK & RELATIONSHIP ANALYSIS) بين الحسابات والمنصات المختلفة.

**المخرجات: تقرير تفصيلي يشمل جميع البيانات المكتشفة، مع شرح واضح للنتائج والتحليلات**

# كيــف تطـــلب البحث المعمق؟

- قم بمراسلتنا عبر [طريقة التواصل]،
موضحًا المعلومات التي ترغب في البحث عنها ونوع التفاصيل المطلوبة.
- يتم تقييم الطلب وتحديد نطاق البحث المناسب.
- يتم تقديم تقرير شامل خلال [مدة محددة حسب مستوى التحقيق].

# خدمات هـكر ←

## اختـبـار الاخـتـراق
## PENETRATION TESTING

- محاكاة واقعية لاختراق الأنظمة لتحديد الثغرات الأمنية وإصلاحها قبل أن يتمكن المهاجمون من استغلالها.
- تقييم نقاط الضعف في الشبكات والتطبيقات
- اختبار الأنظمة بنفس منهجية المهاجمين الحقيقيين
- تقديم تقرير مفصل بالثغرات المكتشفة والتوصيات الأمنية

## تقييـم المخـاطر
## RISK ASSESSMENT

- تحليل شامل لوضعك الأمني لتحديد المخاطر المحتملة وتقليل احتمالية الاختراقات.
- تحديد وتحليل التهديدات ونقاط الضعف
- تقييم التأثيرات المحتملة للمخاطر على المؤسسة
- تقديم استراتيجيات وقائية لتعزيز الأمن

# خدمات هـكر ←

## فريق الهجوم (RED TEAMING)
## اختبـــار الدفـــاعـــــات الأمنـية

- تنفيذ هجمات إلكترونية محاكية لمعرفة مدى قدرة المؤسسة على التصدي للاختراقات المتقدمة.
- محاكاة سيناريوهات اختراق حقيقية ومتطورة
- تقييم استجابة الأنظمة والأفراد للهجمات المستهدفة
- تقديم تحليل شامل لتحسين إجراءات الحماية

## تنظيف البيـــــانـــــات ومعـــــالجتـها
## DATA CLEANING & SANITIZATION

- إزالة المعلومات الحساسة والبيانات غير الضرورية لحماية الخصوصية وتعزيز الأمان الرقمي.
- حذف البيانات الشخصية من الإنترنت والمنصات المختلفة
- تنظيف قواعد البيانات من المعلومات المكررة أو التالفة
- إزالة البيانات المسربة أو القديمة التي قد تسبب مخاطر أمنية
- تقليل البصمة الرقمية للأفراد والشركات

**المخرجات: تقرير شامل يوضح البيانات التي تم تنظيفها أو إزالتها، وإرشادات حول كيفية الحفاظ على الخصوصية الرقمية**


2025
Hacker