



دليل عملي: بايثون للأمن السيبراني والأختراق الأخلاقي

دليل شامل لاستخدام بايثون في مجال الأمن السيبراني والأختراق الأخلاقي

مقدمة في بايثون للأمن السيبراني



ما هي بايثون؟

- لغة برمجة عالية المستوى ومفسرة ✓
- أُنشئت بواسطة جيدو فان روسم عام 1991 ✓
- تتميز ببنية بسيطة وسهلة القراءة ✓
- تدعم multiple paradigms البرمجة ✓

لماذا بايثون شائعة في الأمن السيبراني؟

- متعددة الاستخدامات - مناسبة لمختلف المهام ✓
- سهلة التعلم - بنية واضحة ومبشرة ✓
- مجتمع كبير - دعم ومكتبات متعددة ✓
- قابلة للتوسيع - تكامل مع أدوات أخرى ✓

لماذا يأتون مناسبة للأمن السيبراني والاختراق الأخلاقي



استقلالية المنصة

تعمل على **مختلف أنظمة التشغيل** دون الحاجة لتعديل الكود

أتمتة المهام

قدرة فائقة على **الأتمتة** للمهام المتكررة مثل تحليل السجلات

تطوير سريع

إنشاء **نماذج أولية** وأدوات مخصصة بسرعة لتلبية الاحتياجات الأمنية

سهولة الاستخدام

بنية **واضحة** وقابلة للقراءة، تركز على حل المشكلات وليس التعقيدات التقنية

مكتبات واسعة

مجموعة **ضخمة** من المكتبات المتخصصة في مهام الأمن السيبراني

تكامل مع الأدوات

يتكون **بسهولة** مع أدوات الأمن السيبراني الأخرى مثل Nmap و Metasploit

مكتبات بايثون الرئيسية للأمن السيبراني



هذه المكتبات تشكل الأساس لأدوات الأمان السيبراني القوية

Requests

لإرسال طلبات HTTP

Scapy

للتلعب بالحزم وتحليل الشبكة

Cryptography

للتشفير وفك التشفير

BeautifulSoup

للزحف الويب

Nmap

لمسح الشبكة

Paramiko

لاتصالات SSH

YARA

لاكتشاف البرمجيات الخبيثة

Pefile

لتحليل الملفات التنفيذية

Pandas

لتحليل البيانات

Socket

لبرمجة الشبكات

حالات الاستخدام العملية: اختبار الاختراق

ETHICAL HACKING & PENETRATION TESTING MAISE



تيجي بايثنون إنشاء أدوات اختراق مخصصة وفعالة

مع التركيز على الجوانب الأخلاقية والقانونية

فحص الثغرات

كتابة سكريبتات مخصصة لاكتشاف الثغرات واستغلالها

Nmap Scapy Socket

*** هجمات القوة الغاشمة

اختبار قوّة كلمات المرور في بيئات خاضعة للرقابة

requests hashlib

أتمتة الاستطلاع

جمع البيانات مثل عناوين IP والمنافذ المفتوحة

Shodan BeautifulSoup requests

تطوير استغلالات مخصصة <>

إنشاء سكريبتات تستهدف ثغرات محددة لاختبارها

Impacket pwntools

معالجة البيانات

تحليل نتائج الاختبار وإعداد التقارير التفصيلية

Matplotlib Pandas

التكامل مع الأدوات <>

التفاعل مع أدوات الأمان السيبراني الحالية

Metasploit W3af Sqlmap

حالات الاستخدام العملية: تحليل البرمجيات الخبيثة



بايثون توفر أدوات قوية لتحليل البرمجيات الخبيثة
وتساعد في فهم سلوكها وآليات عملها

التحليل الдинاميكي

أتمتة تقنيات التحليل مثل الاختبار في
بيئة معزولة

Volatility Cuckoo

اكتشاف الأنماط

تحديد الأنماط المشبوهة والسلوكيات
غير الطبيعية

ClamAV YARA

التحليل الثابت

فك تشفير البرمجيات الخبيثة واستخراج
السلسل النصية

Strings Pefile

الهندسة العكسية

استخدام أدوات متقدمة مع بايثون لفهم
آلية عمل البرمجيات

Ghidra IDA Pro

مسح البيانات

مسح مجموعات البيانات الكبيرة للعثور
على برمجيات خبيثة

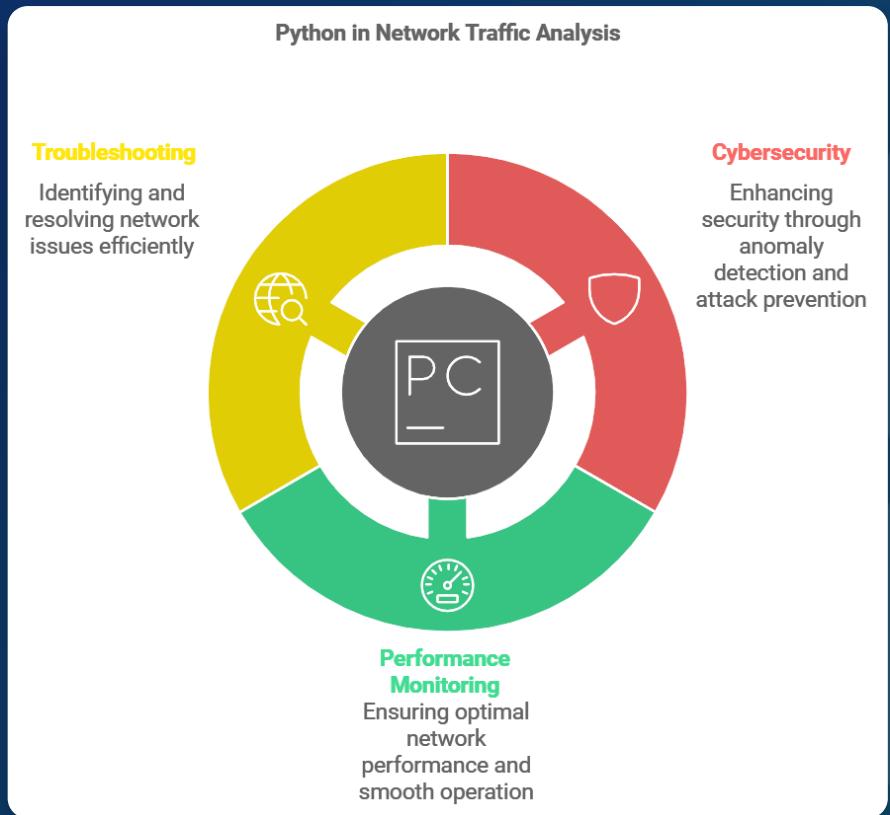
Scikit-learn Dask

أتمتة المهام

أتمتة المهام المتكررة مثل استخراج
المعلومات من الملفات

OS Pandas

حالات الاستخدام العملية: أمن الشبكات



بايثون تمكن من إنشاء أدوات أمن شبكات قوية وتوفر مرونة في تخصيص عمليات الفحص والتحليل

كشف الخدمات

تحديد الخدمات قيد التشغيل وإصداراتها

Scapy python-nmap

مسح المنافذ

تحديد المنافذ المفتوحة ونقاط الدخول المحتملة

Nmap Socket

اكتشاف الشبكة

تحديد الأجهزة وعنوانين IP تلقائياً

Arp-scan Scapy

تقييم الثغرات

التحقق من الثغرات المعروفة في الخدمات المكتشفة

Nessus OpenVAS

أتمتة المسح

دمج نتائج المسح مع معلومات التهديدات

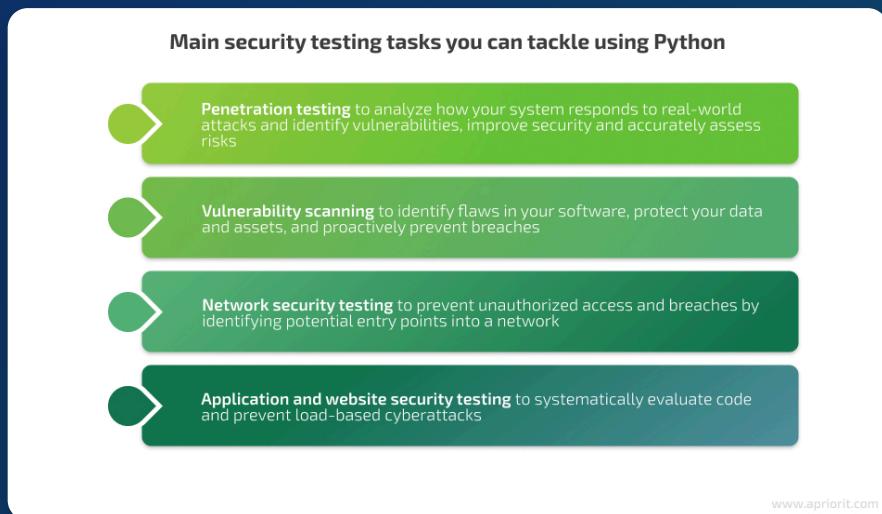
APIs SIEM

تحليل حركة المرور

مراقبة وتحليل حركة مرور الشبكة

PyShark Scapy

حالات الاستخدام العملية: أتمتة الأمان



بايثون تمكن من أتمتة المهام الأمنية المتكررة
مما يوفر الوقت ويقلل من أخطاء الإنسان

مسح الثغرات

أتمتة عمليات المسح والتقييم

Nessus

OpenVAS

تحليل السجلات

معالجة سجلات الأمان تلقائياً

Pandas

Elasticsearch

الاستجابة للحوادث

بناء أدوات مخصصة لجمع وتحليل الأدلة

SOAR

SIEM

مراقبة الشبكة

مراقبة حركة المرور والكشف عن
الأنشطة المشبوهة

PyShark

Scapy

إنشاء التقارير

توليد تقارير تلقائية عن الحوادث الأمنية

Jinja2

Matplotlib

إدارة التصحيحات

أتمتة عملية تطبيق التصحيحات الأمنية

APIs

Ansible

الممارسات المثلثة



اتباع الممارسات المثلث يضمن استخدام بائيون بشكل أخلاقي وفعال في مجال الأمن السيبراني

الترميز الآمن

تجنب الثغرات الشائعة في الكود
استخدام **مكتبات موثوقة** ومعتمدة

الاعتبارات الأخلاقية

الالتزام بالقوانين واللوائح
الحصول على التصاريح الالزامية قبل
الاختبار

التعلم المستمر

مواكبة التطورات في مجال الأمن
السيبراني
المشاركة في **المجتمعات المهنية**

التوثيق والتقارير

توثيق الكود بشكل جيد
إنشاء **تقارير واضحة** عن النتائج

النسخ الاحتياطي

حماية البيانات الهامة
إنشاء **نسخ احتياطية** قبل الاختبارات

البيئات المعزولة

الاختبار في بيئات منفصلة
ضمان **عدم التأثير** على الأنظمة الحية

موارد للتعلم الإضافي



الاستمرار في التعلم والتطوير
هو مفتاح النجاح في مجال الأمن السيبراني

توزيع موارد التعلم



- | | |
|----------|------------|
| دورات | تدريب عملي |
| مجتمعات | كتب |
| مستودعات | مكتبات |
| دروس | وثائق |

مستودعات GitHub

مشاريع مفتوحة المصدر لأدوات الأمان
Secure Code Warrior Python Security

المجتمعات والمنتديات

تبادل المعرفة مع المتخصصين
r/Python r/netsec

دورات مجانية

دورات متخصصة في بایثون والأمن
The Cyber Mentor edX

الوثائق الرسمية

مصادر موثوقة لفهم بایثون ومكتبات الأمان
Scapy وثائق بایثون

كتب متخصصة

كتب متخصصة في بایثون والأمن السيبراني
Black Hat Python Violent Python

منصات التدريب العملي

ممارسة المهارات بشكل عملي
Cybrary OverTheWire

البرمجة من الصفر إلى الاحتراف

دليلك المتكامل العملي لتصبح مبرمجاً محترفاً بلغة بايثون، مع أكثر من 120 تمرين محلول مع محرر أكواد و برنامج بايثون مدمج لتجربة الأكواد مباشرة من المتصفح.

شرح عربي مبسط وعميق من الصفر

أكثر من 120 تمريناً ومشروعًا عمليًا

محرر أكواد و مترجم بايثون مدمج

تجربة تعلم من أي مكان وفي أي وقت

يغطي الأساسيات و OOP المتقدمة

منهج يركز على بناء المشاريع

لماذا هذا الكتاب؟

تشجيع الشباب العربي على الدخول لمجال البرمجة في عصر ثورة الذكاء الاصطناعي، والمساهمة في حل المشاكل المستعصية على الإنسان.

برمجة وتأليف: أحمد بوشفرة

المكتبة الإلكترونية

احصل على الكتاب

مجاني



المزيد من المصادر المجانية

تقييم المصادر المجانية



هذه المصادر توفر لك فرصة للتطور المستمر

وتحقيقك على اطلاع بأحدث التقنيات في مجال الأمن السيبراني

مجاني

قنوات يوتيوب

قنوات متخصصة في الأمن السيبراني
والبرمجة

NetworkChuck
The Cyber Mentor
David Bombal

مجاني

منصات التعلم المجانية

منصات تعليمية عالمية تقدم دورات مجانية

freeCodeCamp
Khan Academy
Codecademy

مجاني

تحديات برمجية

منصات لتحسين مهاراتك البرمجية عبر
التحديات

LeetCode
HackerRank
Codewars

مجاني

مدونات تقنية

مصادر معرفية متخصصة في الأمن السيبراني

Schneier on Security
Krebs on Security
10xdev.blog
Python Blog

مجاني

منتديات نقاش

مجتمعات لتبادل المعرفة والخبرات

Reddit r/netsec
Stack Overflow
webtutpro.com
Reddit r/Python

مجاني

مستندات تقنية

وثائق رسمية لمكتبات بايثون للأمن السيبراني

Scapy Docs
Crypto Library
Requests Docs

ahmedbouchefra.com/library

