



مع المهندس: علي محمد الجازي



# kali Linux

## مقدمة الدورة

تُعد دورة Kali Linux من أهم الدورات المتخصصة في مجال الأمن السيبراني واختبار الاختراق، حيث تهدف إلى تدريب المشاركين على استخدام نظام Kali Linux وأدواته الاحترافية لفحص الشبكات والأنظمة واكتشاف الثغرات الأمنية بطريقة قانونية وأخلاقية.

سيتعلم المتدرب كيفية تثبيت وإدارة النظام، استخدام أشهر أدوات اختبار الاختراق، تنفيذ عمليات جمع المعلومات وتحليل الثغرات، وتأمين الأنظمة ضد الهجمات الإلكترونية، مع تطبيقات عملية وسيناريوهات حقيقية تؤهل المتدرب لدخول عالم الـ Cyber Security والـ Penetration Testing باحترافية.

## محاور الدورة

### المحور الأول: مقدمة في الأمن السيبراني و Kali Linux

- التعرف على مفاهيم الأمن السيبراني
- الفرق بين Ethical Hacking و Cyber Security
- التعرف على توزيعة Kali Linux
- تثبيت Kali Linux على Virtual Machine
- إعداد بيئة العمل والتهيئة الأساسية

### المحور الثاني: أساسيات نظام Linux

- أوامر Linux الأساسية
- إدارة الملفات والمجلدات
- إدارة المستخدمين والصلاحيات
- التعامل مع الـ Terminal
- إدارة الخدمات والحزم



### المحور الثالث: جمع المعلومات Information Gathering

- التعرف على أهداف الاختبار
- استخدام أدوات :
  - Nmap
  - Whois
  - Netdiscover
  - DNS Enumeration
- فحص الأجهزة والخدمات المفتوحة
- تحليل الشبكات والبنية التحتية

### المحور الرابع: تحليل الثغرات Vulnerability Assessment

- التعرف على أنواع الثغرات الأمنية
- استخدام أدوات تحليل الثغرات
- اكتشاف نقاط الضعف في الأنظمة
- قراءة وتحليل تقارير الفحص

### المحور الخامس: اختبار الاختراق Penetration Testing

- أساسيات اختبار الاختراق
- استغلال الثغرات بشكل عملي
- التعرف على أشهر أنواع الهجمات
- استخدام Metasploit Framework
- إنشاء Sessions والتحكم بالأهداف

### المحور السادس: أمن الشبكات والشبكات اللاسلكية

- تحليل الشبكات
- حماية الشبكات
- اختبار اختراق شبكات Wi-Fi
- التعرف على بروتوكولات الشبكات
- استخدام Wireshark لتحليل الحزم



## المحور السابع: أمن تطبيقات الويب Web Security

- أساسيات Web Application Security
- التعرف على ثغرات :
- SQL Injection
- XSS
- CSRF
- استخدام Burp Suite
- اختبار وتأمين المواقع الإلكترونية

## المحور الثامن: الحماية والتأمين Security Hardening

- طرق حماية الأنظمة
- تأمين السيرفرات والشبكات
- إعداد الجدران النارية Firewall
- تحديث الأنظمة ومعالجة الثغرات
- أفضل ممارسات الأمن السيبراني

## المحور التاسع: المشاريع والتطبيق العملي

- تنفيذ مختبرات عملية
- سيناريوهات حقيقية لاختبار الاختراق
- إعداد تقارير احترافية
- مشروع نهائي شامل

## الفئة المستهدفة

- المبتدئون في الأمن السيبراني
- مسؤولو الشبكات والدعم الفني
- طلاب تقنية المعلومات
- الراغبون بدخول مجال Ethical Hacking
- العاملون في مجال IT والأمن السيبراني



## مخرجات الدورة

بعد الانتهاء من الدورة سيكون المتدرب قادراً على:

- التعامل باحترافية مع Kali Linux
- تنفيذ اختبارات اختراق أساسية و متقدمة
- تحليل الشبكات واكتشاف الثغرات
- استخدام أشهر أدوات الأمن السيبراني
- حماية الأنظمة والشبكات من الهجمات الإلكترونية