

CYBERSECURITY · TECHNOLOGY

ابدأ رحلتك من الصفر

أساسيات الاختراق الأخلاقي

Ethical Hacking Fundamentals

دورة مبسطة وعملية ومناسبة للمبتدئين، تقدّم مقدمة شاملة في الأمن السيبراني والاختبار الأخلاقي — دون الحاجة إلى أي خبرة سابقة.

مبتدئ

بدون أي خبرة سابقة

27

ساعة تدريب

9

أيام تدريبية

3

أسابيع

WEEK 3 · PEAK

الهجمات العملية والمسار المهني

الهندسة الاجتماعية · هجمات كلمات المرور
· التحدي النهائي

WEEK 2 · RISE

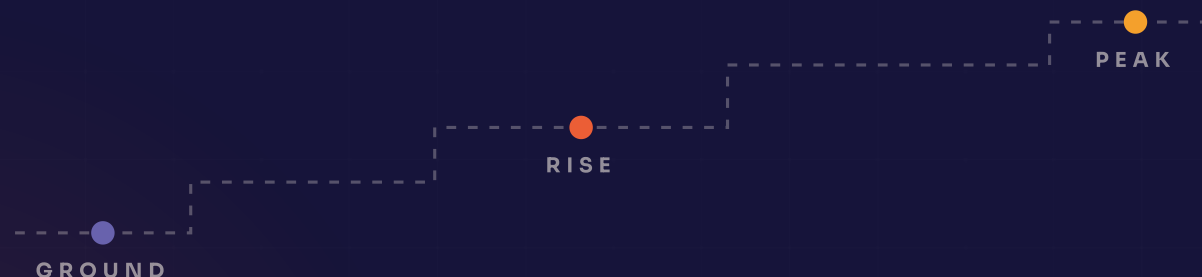
أساسيات الاختبار الأخلاقي

المنهجية · الاستطلاع · Burp Suite · أشهر
ثغرات الويب

WEEK 1 · GROUND

أساسيات الأمن السيبراني

المفاهيم الأساسية · كيف يعمل الإنترنت والويب
Linux والأدوات



?WHO IS THIS FOR

لمن هذه الدورة؟

صُمِّمت لتبدأ من الصفر — بغض النظر عن خلفيتك.

الخريجون الجدد ✓

طلاب الجامعات ✓

المبتدئون تماماً في مجال الأمن السيبراني ✓

الراغبون في دخول مجال الأمن السيبراني ✓

المهتمون بمجال الاختبار الأخلاقي ✓

طلاب تخصصات IT و Computer Science ✓

كل من يريد فهم المجال قبل اختيار تخصصه ✓

لا يشترط وجود أي خبرة سابقة في الأمن السيبراني.
كل ما تحتاجه: جهاز لابتوب وحب للتعلم — نبدأ معك من الصفر تماماً.



LEARNING OUTCOMES

مخرجات التعلم

بنهاية الدورة، ستكون قادراً على:

✓ فهم كيفية عمل المواقع وتطبيقات الويب

✓ فهم مجال الأمن السيبراني وأهم تخصصاته ومساراته المهنية

✓ فهم أساسيات الاختبار الأخلاقي ومنهجيته

✓ استخدام أوامر Linux الأساسية

✓ تحليل طلبات HTTP باستخدام Burp Suite

✓ تنفيذ عمليات استطلاع أساسية

✓ التعرف على أساليب الهجوم الشائعة

✓ فهم أشهر ثغرات تطبيقات الويب

✓ تحليل حادثة أمنية بسيطة

✓ فهم هجمات كلمات المرور والوصول إلى الأنظمة

✓ معرفة خطواتك التالية في رحلة التعلم

✓ اختيار المسار المهني المناسب لك

اليوم الأول

01

مقدمة في الأمن السيبراني

- ما هو الأمن السيبراني؟
- الأمن السيبراني في العالم الحقيقي
- التحديات والثغرات والمخاطر
- المسارات والتخصصات المهنية في المجال
- لماذا يعتبر الأمن السيبراني مهماً؟
- أشهر أنواع الهجمات السيبرانية
- الفرق بين **Blue Team** و **Red Team**

اليوم الثاني

02

كيف يعمل الإنترنت والويب؟

- كيف يعمل الإنترنت؟
- النطاقات و **DNS**
- HTTP** و **HTTPS**
- Sessions** و **Cookies**
- المواقع وتطبيقات الويب
- عناوين **IP** والمنافذ — المفاهيم الأساسية
- الطلبات والاستجابات
- مقدمة في أمن تطبيقات الويب

اليوم الثالث

03

Linux وأدوات الأمن السيبراني

- مقدمة في **Linux**
- أهم أوامر **Linux** الأساسية
- التعامل مع **Terminal**
- إعداد بيئة تدريب أساسية للأمن السيبراني
- نظام الملفات في **Linux**
- الملفات والمستخدمون والصلاحيات
- مقدمة في **Kali Linux**

بنهاية الأسبوع الأول صورة واضحة عن مجال الأمن السيبراني ومساراته، وفهم كامل لكيفية عمل الإنترنت والويب — وبيئة **Linux** تدريبية جاهزة على جهازك.

اليوم الرابع

04

مقدمة في الاختبار الأخلاقي

- ما هو الاختبار الأخلاقي؟
- الجوانب القانونية والأخلاقية
- منهجية الاختبار الأخلاقي
- اكتشاف الثغرات
- كتابة التقارير الأمنية
- الفرق بين الاختبار الأخلاقي والاختراق الضار
- مقدمة في اختبار الاختراق
- جمع المعلومات والاستطلاع
- مفهوم استغلال الثغرات

اليوم الخامس

05

الاستطلاع وأمن تطبيقات الويب

- ما هو الاستطلاع؟
- جمع المعلومات
- تحديد نقاط الدخول في تطبيقات الويب
- اعتراض وتحليل HTTP Requests
- فهم Attack Surface
- النطاقات الفرعية والتقنيات المستخدمة
- مقدمة في Burp Suite
- فهم User Input و Parameters

اليوم السادس

06

أشهر ثغرات تطبيقات الويب

- ما هي ثغرات تطبيقات الويب؟
- Cross-Site Scripting (XSS)
- Broken Access Control / IDOR — المفهوم الأساسي
- أمثلة وتطبيقات عملية مبسطة على الثغرات
- التحقق من المدخلات Input Validation
- SQL Injection — المفهوم الأساسي
- الفرق بين Authorization و Authentication

بنهاية الأسبوع الثاني تفكر كمختبر أخلاقي: استطلاع احترافي، وتحليل طلبات HTTP بـ Burp Suite، وفهم عميق لأشهر ثغرات تطبيقات الويب.

اليوم السابع

07

الهندسة الاجتماعية والهجمات الشائعة

- ما هي الهندسة الاجتماعية؟
- سرقة بيانات تسجيل الدخول
- هجمات كلمات المرور
- التصيد الاحتيالي **Phishing**
- الروابط والمرفقات الخبيثة
- كيف يخدع المهاجمون المستخدمين؟

اليوم الثامن

08

هجمات كلمات المرور والوصول إلى الأنظمة

- كيف ينتقل المهاجم من الثغرة إلى الوصول؟
- هجمات القاموس وقوائم الكلمات **Wordlists**
- كسر كلمات المرور عملياً داخل بيئة التدريب
- ما بعد الوصول **Post-Exploitation** – المفهوم الأساسي
- الهجمات بالقوة الغاشمة **Brute Force**
- الهاش **Hashing** – كيف تُخزَّن كلمات المرور
- أدوات هجمات كلمات المرور في **Kali Linux**
- رفع الصلاحيات **Privilege Escalation** – المفهوم الأساسي

اليوم التاسع

09

التحدي النهائي والمسار المهني

- تحدي عملي في الأمن السيبراني
- تحديد المشكلات الأمنية
- اقتراح التحسينات الأمنية
- المسارات المهنية: **AppSec** · **SOC** · **Offensive Security**
- Cloud Security** · **GRC**
- بناء خارطة طريق شخصية في الأمن السيبراني
- تحليل هجوم سيبراني محاكي
- إجراء تحقيق أساسي
- مراجعة أهم المفاهيم التي تم تعلمها
- كيف تكمل رحلة التعلم؟

بنهاية الأسبوع الثالث تفهم كيف تُنفَّذ الهجمات فعلياً – من الاستطلاع إلى الوصول – وتخرج بخارطة طريق مهنية شخصية لخطوتك التالية.

HANDS-ON PRACTICE

الجانب العملي

خلال الدورة، ستتدرب عملياً على استخدام:

W

معامل مبسطة لأمن تطبيقات الويب

B

Burp Suite

_<

Linux Terminal

K

Kali Linux

I

تمارين التحقيق في الحوادث الأمنية

P

سيناريوهات التصيد الاحتيالي

R

أدوات الاستطلاع الأساسية

H

تحليل HTTP Requests

المشروع النهائي

سيعمل الطلاب على سيناريو مبسط يحاكي حادثة أمنية حقيقية، يمرون خلاله بالمراحل التالية – صُمم التحدي لقياس استيعاب المفاهيم الأساسية دون الحاجة إلى مهارات تقنية متقدمة.

05

اقترح الحلول

توصيات عملية للتحسين

04

اكتب التقرير

وثّق النتائج بوضوح

03

حدّد

اكتشف المشكلات الأمنية

02

حلّل

افهم ماذا حدث وكيف حدث

01

اكتشف

اجمع الأدلة والأثر الأولي للهجوم

مجتمع رقبان معك

دعم مستمر بين الجلسات – لن تبقى عالقاً مع إعداد أو أداة.

تعلمها ممن يمارسها فعلاً

مدربون يعملون في المجال يومياً ويشرحون الطريقة نفسها التي يعملون بها.

تدريب عملي من اليوم الأول

لا محاضرات نظرية جافة – كل يوم يتضمن تطبيقاً وأدوات حقيقية.

3 أسابيع · 9 أيام تدريبية · 27 ساعة · من الصفر · مشروع نهائي عملي

ابدأ من الصفر. افهم الأمن السيبراني. اكتشف مسارك.

اسأل عن الدفعة القادمة وسجّل مقعدك الآن.

raqyan.com

سجّل الآن عبر واتساب · +966 56 006 6113