raqyan

للمبتدئين • من الصفر

خارطة طريق الدورة • الأمن السيبراني

أساسيات الاختراق الأخلاقي

Ethical Hacking Foundations

ابدأ من الصفر. افهم الأمن السيبراني. اكتشف مسارك.

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



٩	٢٧	٣	١٢–٧
جلسات مباشرة	ساعة تدريب	أسابيع	مقعدًا فقط

المدرّب • معاذ عفيفي — مهندس أمن سيبراني ومكتشف ثغرات

raqyan.com/course-hacking

لمن الدورة وماذا ستتعلّم

raqyan

لمن هذه الدورة؟

لمن هذه الدورة؟

صُمّمت لتبدأ من الصفر — بغض النظر عن خلفيتك.

- المبتدئون تمامًا في مجال الأمن السيبراني
- الخريجون الجدد
- المهتمون بمجال الاختبار الأخلاقي
- كل من يريد فهم المجال قبل اختيار تخصصه
- طلاب الجامعات
- طلاب تخصصات IT وComputer Science
- الراغبون في دخول مجال الأمن السيبراني

لا يشترط وجود أي خبرة سابقة في الأمن السيبراني.

كل ما تحتاجه: جهاز لابتوب وحب للتعلم — نبدأ معك من الصفر تمامًا.

مخرجات التعلم

بنهاية الدورة، ستكون قادرًا على:

- فهم مجال الأمن السيبراني وأهم تخصصاته ومساراته المهنية
- استخدام أوامر Linux الأساسية
- تنفيذ عمليات استطلاع أساسية
- فهم أشهر ثغرات تطبيقات الويب
- فهم هجمات كلمات المرور والوصول إلى الأنظمة
- اختيار المسار المهني المناسب لك
- فهم كيفية عمل المواقع وتطبيقات الويب
- فهم أساسيات الاختبار الأخلاقي ومنهجيته
- تحليل طلبات HTTP باستخدام Burp Suite
- التعرف على أساليب الهجوم الشائعة
- تحليل حادثة أمنية بسيطة
- معرفة خطوتك التالية في رحلة التعلم

لماذا تتعلّمها في رقيان

تدريب عملي من اليوم الأول

لا محاضرات نظرية جافة — كل جلسة تتضمن تطبيقًا وأدوات حقيقية.

تعلّمها ممن يمارسها فعلًا

مدرّبون يعملون في المجال يوميًا ويشرحون الطريقة نفسها التي يعملون بها.

مجتمع رقيان معك

دعم مستمر بين الجلسات — لن تبقى عالقًا مع إعداد أو أداة.

كيف تتعلّم في هذه الدورة

raqyan

طريقة Jisr

محتوى إنجليزي، وشرح بالعربية

Jisr تعني «جسر»: نشرح لك المحتوى الإنجليزي بالعربية، فتصبح اللغة طريقك إلى المهارة لا عائقاً أمامها. المحتوى والمصطلحات بالإنجليزية، لغة السوق، والشرح كله بالعربية.



المسار

Peak ← Rise ← Ground

١ ٢ ٣ ٤ ٥ ٦ ٧ ٨ ٩

Ground
أساسيات الأمن السيبراني

المفاهيم الأساسية • كيف يعمل الإنترنت والويب • Linux والأدوات

الأسبوع ١ • الجلسات ١–٣

Rise
أساسيات الاختبار الأخلاقي

المنهجية • الاستطلاع • Burp Suite • أشهر ثغرات الويب

الأسبوع ٢ • الجلسات ٤–٦

Peak
الهجمات العملية والمسار المهني

الهندسة الاجتماعية • هجمات كلمات المرور • التحدي النهائي

الأسبوع ٣ • الجلسات ٧–٩

الصيغة
مباشر عن بُعد • ثلاث جلسات أسبوعيًا • بتوقيت المملكة العربية السعودية

المدة
٣ أسابيع • ٩ جلسات • ٢٧ ساعة

المقاعد
من ٧ إلى ١٢ في كل دفعة

الخبرة السابقة
غير مطلوبة إطلاقًا

ما تحتاجه
لابتوب واتصال بالإنترنت فقط

الأدوات
كلها مجانية ومفتوحة المصدر — نجهّز البيئة معًا خلال الدورة

مدرّبك

معاذ عفيفي · مهندس أمن سيبراني ومكتشف ثغرات

مهندس أمن سيبراني ومكتشف ثغرات على منصات **bug bounty** العالمية. متخصص في أمن تطبيقات الويب واختبار الاختراق، ويعمل يوميًا بأدوات المجال (**Burp Suite** و**Nmap** و**Linux**).

الجلسات التسع

raqyan

GROUND أساسيات الأمن السيبراني

الأسبوع ١ • ٣ جلسات • ٩ ساعات

١ مقدمة في الأمن السيبراني

الجلسة ١

ما ستتعلّمه

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

٢ كيف يعمل الإنترنت والويب؟

الجلسة ٢

ما ستتعلّمه

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

٣ Linux وأدوات الأمن السيبراني

الجلسة ٣

ما ستتعلّمه

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

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

الجلسات التسع

raqyan

RISE أساسيات الاختبار الأخلاقي

الأسبوع ٢ • ٣ جلسات • ٩ ساعات

٤ مقدمة في الاختبار الأخلاقي

الجلسة ٤

ما ستتعلّمه

- 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

٥ الاستطلاع وأمن تطبيقات الويب

الجلسة ٥

ما ستتعلّمه

- 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 **Parameters** و**User Input**

٦ أشهر ثغرات تطبيقات الويب

الجلسة ٦

ما ستتعلّمه

- 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 **Authentication** و**Authorization**

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

الجلسات التسع

raqyan

PEAK الهجمات العملية والمسار المهني

الأسبوع ٣ • ٣ جلسات • ٩ ساعات

٧ الهندسة الاجتماعية والهجمات الشائعة

الجلسة ٧

ما ستتعلّمه

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

٨ هجمات كلمات المرور والوصول إلى الأنظمة

الجلسة ٨

ما ستتعلّمه

- كيف ينتقل المهاجم من الثغرة إلى الوصول؟
- هجمات القاموس وقوائم الكلمات **Wordlists**
- كسر كلمات المرور عمليًا 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

٩ التحدي النهائي والمسار المهني

الجلسة ٩

ما ستتعلّمه

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

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

الجانب العملي والمشروع النهائي

raqyan

تدريب عملي

الجانب العملي

خلال الدورة، ستتدرب عمليًا على استخدام:

- Kali Linux
- Linux Terminal
- Burp Suite
- معامل مبسطة لأمن تطبيقات الويب
- تحليل HTTP Requests
- أدوات الاستطلاع الأساسية
- سيناريوهات التصيد الاحتيالي
- تمارين التحقيق في الحوادث الأمنية

المشروع النهائي

محاكاة حادثة أمنية في خمس مراحل

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

١ **اكتشف** — اجمع الأدلة والأثر الأولي للهجوم

← ٢ **حلّل** — افهم ماذا حدث وكيف حدث

← ٣ **حدّد** — اكشف المشكلات الأمنية

← ٤ **اكتب التقرير** — وثّق النتائج بوضوح

← ٥ **اقترح الحلول** — توصيات عملية للتحسين

٣ أسابيع • ٩ جلسات مباشرة • ٢٧ ساعة • من الصفر • مشروع نهائي عملي

شهادة إتمام موثّقة

صادرة عن أكاديمية رقيان • يمكن التحقق منها برقمها على raqyan.com/verify • ليست شهادة معتمدة — المشروع الذي تبنيه هو الدليل الحقيقي على مهارتك

ابدأ من الصفر. افهم الأمن السيبراني. اكتشف مسارك.

احجز مقعدك

الدفعة القادمة ١–٢١ نوفمبر • يُغلق التسجيل ٣٠ أكتوبر

سجّل الآن • raqyan.com/join?course=ethical-hacking

واتساب +966 56 006 6113 — نؤكّد مقعدك خلال ٢٤ ساعة

المدرّب

معاذ عفيفي — مهندس أمن سيبراني ومكتشف ثغرات