المقرر الدراسي – كورس الأمن السيبراني (30 ساعة)

عدد الساعات: 30 ساعة

عدد المحاضرات: 12 محاضرة

مدة المحاضرة: 2.5 ساعة

المستوى: مبتدئ حتى احتراف

الأدوات المستخدمة: Kali Linux، Wireshark، Metasploit، Burp Suite، Nmap، أدوات حماية الشبكات

الوحدة الأولى: مقدمة الأمن السيبراني (5 ساعات)

المحاضرة 1 – التعرف على الأمن السيبراني (2.5 ساعة)

- ما هو الأمن السيبراني ولماذا هو مهم
- أنواع الهجمات الإلكترونية
- التعرف على أساسيات الحماية الشخصية والبيانات
- التدريب العملي: إنشاء كلمات مرور قوية وإدارة الحسابات

المحاضرة 2 – أساسيات الشبكات (2.5 ساعة)

- تعريف الشبكات وأنواعها
- بروتوكولات TCP/IP، HTTP، HTTPS
- عنوان IP وSubnet
- التدريب العملي: فحص الشبكة باستخدام أدوات بسيطة

المهارة

almahara academy

الوحدة الثانية: أدوات وتقنيات الحماية (10 ساعات)

المحاضرة 3 – أنظمة التشغيل الآمنة (2.5 ساعة)

- التعرف على أنظمة Kali Linux وWindows
- إعداد بيئة افتراضية آمنة
- التعامل مع Terminal وCommand Line

المحاضرة 4 – تحليل الشبكات (2.5 ساعة)

- استخدام Wireshark لمراقبة الشبكة
- التعرف على الحزم (Packets) ومصادرها
- التدريب العملي: مراقبة شبكة داخلية

المحاضرة 5 – المراقبة والتقييم الأمني (2.5 ساعة)

- استخدام Nmap لفحص الثغرات
- التعرف على المنافذ المفتوحة وأنواع الهجمات
- التدريب العملي: فحص جهاز كمبيوتر آمن داخل مختبر

المحاضرة 6 – حماية الأنظمة (2.5 ساعة)

- تثبيت الجدران النارية (Firewalls)
- إعداد برامج مكافحة الفيروسات
- التحكم بالوصول إلى الملفات والمجلدات
- التدريب العملي: حماية جهاز كمبيوتر افتراضي

الوحدة الثالثة: الهجمات والتصدي لها (10 ساعات)

المحاضرة 7 – التعرف على الهجمات الشائعة (2.5 ساعة)

- Phishing، Malware، Ransomware
- هجمات الـSQL Injection وCross-Site Scripting
- التدريب العملي: التعرف على محاولات الهجوم في بيئة آمنة

المحاضرة 8 – الاختراق الأخلاقي (Ethical Hacking) (2.5 ساعة)

- التعريف بالاختراق الأخلاقي وأهدافه
- استخدام Metasploit لاختبار الثغرات
- التدريب العملي: تنفيذ اختبار اختراق محدود

المحاضرة 9 – تأمين الشبكات اللاسلكية (2.5 ساعة)

- بروتوكولات Wi-Fi
- إعداد كلمات مرور قوية للشبكات
- الحماية ضد هجمات الـWi-Fi
- التدريب العملي: تأمين شبكة داخلية افتراضية

المحاضرة 10 – التشفير والحماية (2.5 ساعة)

- مبادئ التشفير (Encryption)
- SSL/TLS وVPN
- التدريب العملي: تشفير الملفات وتأمين البريد الإلكتروني

الوحدة الرابعة: مشاريع وتطبيقات عملية (5 ساعات)

المحاضرة 11 – مشروع محاكاة اختراق وحماية (2.5 ساعة)

- إعداد مختبر افتراضي
- تنفيذ سيناريوهات هجوم وحماية
- التدريب العملي: تسجيل جميع الخطوات والتقارير

المحاضرة 12 – مراجعة شاملة وتسليم المشروع النهائي (2.5 ساعة)

- تحليل المشروع النهائي
- تقديم تقرير شامل عن الإجراءات الأمنية
- نصائح لتعزيز المهارات المستمرة في الأمن السيبراني

مخرجات الكورس النهائية

بنهاية الـ30 ساعة، يكون المتدرب قادرًا على:

- فهم أساسيات الأمن السيبراني والشبكات
- التعرف على أدوات الحماية وتحليل الشبكات
- تنفيذ الاختراق الأخلاقي بشكل آمن
- حماية الأنظمة والشبكات من الهجمات الشائعة
- استخدام التشفير وأدوات حماية البيانات
- إعداد مختبر افتراضي لاختبار الأمن السيبراني
- رفع مستوى الحماية الشخصية والمهنية في بيئة العمل