دورة الأمن السيبراني – مستوى مبتدئ

هذه الدورة هي مقدمة شاملة في مجال الأمن السيبراني، مصممة للمبتدئين الذين لا يملكون أي خبرة سابقة. تهدف إلى بناء فهم قوي للأساسيات التقنية مثل الشبكات، أنظمة التشغيل، وأساليب الحماية والهجوم السيبراني.

تجمع الدورة بين الجانب النظري والعملي من خلال أمثلة عملية وأدوات مستخدمة في الواقع مثل Kali Linux و Wireshark وNmap، مما يساعد المتدرب على فهم كيفية عمل الهجمات الإلكترونية وكيفية التصدي لها.

بنهاية الدورة، سيكون المتدرب قادرًا على فهم بيئة الأمن السيبراني بشكل عام والاستعداد للانتقال إلى مستويات متقدمة في مجالات مثل اختبار الاختراق (Penetration Testing) أو الدفاع السيبراني (Blue Team)

أهداف الدورة التدريبية:

أولاً: الأهداف المعرفية

- فهم مفهوم الأمن السيبراني وأهميته
- التعرف على أنواع الهجمات الإلكترونية الشائعة
- فهم أساسيات الشبكات (IP – TCP/IP – DNS)
- التعرف على أنظمة التشغيل Linux و Kali Linux

ثانياً: الأهداف المهارية

- استخدام أدوات أساسية مثل :
  - Nmap لفحص الشبكات
  - Wireshark لتحليل حركة البيانات
  - Burp Suite لفهم أمن الويب
- تنفيذ أوامر لينكس الأساسية بكفاءة
- تحليل حركة الشبكة واكتشاف الأنشطة المشبوهة

ثالثاً: أهداف الحماية والدفاع

- فهم كيفية حماية الأنظمة من الهجمات
- التعرف على أساليب كشف الاختراقات
- تحليل السجلات (Logs) بشكل مبسط
- التعرف على أساسيات مراكز العمليات الأمنية (SOC)

رابعاً: الأهداف التطبيقية

- تطبيق سيناريوهات هجوم ودفاع بسيطة
- تشغيل مختبرات افتراضية للتجربة العملية
- فهم دورة الهجوم السيبراني (Recon → Attack → Defense)
- تنفيذ مشروع نهائي لمحاكاة بيئة شركة صغيرة

الفئة المستهدفة للدورة التدريبية:

- الطلاب
- المبتدؤون في الامن السيبراني والشبكات
- المهتمون بتقنية المعلومات
- الموظفون في مجال تقنية المعلومات

متطلبات الدورة التدريبية:

- معرفة بتقنية المعلومات
- معرفة بشبكات CCNA

محتوى الدورة التدريبية

عدد الساعات: 30 ساعة

عدد المحاضرات: 12 محاضرة

مدة المحاضرة: ساعتان ونصف

الأدوات المستخدمة: ipconfig, ping, Wireshark, Nmap, Linux basics, Burp Suite, Metasploit, DVWA, Wazuh, Logs, SIEM tools

المحاضرة 1: مقدمة في الأمن السيبراني

- ما هو الأمن السيبراني؟
- أهمية الأمن السيبراني في العالم اليوم
- أنواع التهديدات الرقمية
- الفرق بين Hacker / Security Analyst / Penetration Tester

التدريب العملي: أمثلة على اختراقات مشهورة (Facebook – Yahoo – etc)

المحاضرة 2: أساسيات الشبكات

- ما هي الشبكات (LAN / WAN / Internet)
- عناوين IP Address / MAC Address
- بروتوكولات TCP / UDP
- مفهوم المنافذ Ports

التدريب العملي: استخدام أوامر: ipconfig / ifconfig

المحاضرة 3: أساسيات نظام التشغيل (Linux)

- مقدمة عن Linux
- أوامر أساسية (ls, cd, pwd, mkdir)
- الصلاحيات (Permissions)
- المستخدمين والجذر root

التدريب العملي: إنشاء ملفات وتغيير صلاحياتها

المحاضرة 4: مقدمة في نظام التشغيل (Kali Linux)

- ما هو Kali Linux ؟
- الأدوات الأساسية في Kali Linux
- استخدام محرر الأوامر Terminal
- تنظيم بيئة العمل

التدريب العملي: تشغيل أدوات بسيطة

المحاضرة 5: أنواع الهجمات السيبرانية

- Phishing
- Malware
- Brute Force
- Man-in-the-Middle
- مقدمة في SQL Injection

التدريب العملي: تحليل أمثلة واقعية

المحاضرة 6: أساسيات التشفير

- ما هو التشفير؟
- التشفير المتزامن والغير متزامن Symmetric vs Asymmetric Encryption
- Hashing (MD5 / SHA)
- أهمية التشفير في الحماية

التدريب العملي: تجربة تشفير نصوص بسيطة

المحاضرة 7: أمن الشبكات

- Firewalls
- IDS / IPS
- VPN
- كيف يتم حماية الشبكات

التدريب العملي: رسم شبكة آمنة

المحاضرة 8: تحليل حركة الشبكة

- مفهوم الحزم Packet
- مقدمة عن Wireshark
- كيف يتم التقاط البيانات
- مراقبة حركة البيانات Traffic

التدريب العملي: تحليل Packets بسيطة

المحاضرة 9: أساسيات اختبار الاختراق

- ما هو اختبار الاختراق Penetration Testing ؟
- مراحل الاختراق (Recon → Exploit → Report)
- الاختراق الاخلاقي Ethical Hacking

التدريب العملي: سيناريو بسيط لاختبار نظام

المحاضرة 10: أمن الويب (Web Security Basics)

- كيف تعمل المواقع
- Cookies / Sessions
- مقدمة لثغرات XSS
- مقدمة في SQL Injection

التدريب العملي: عرض ثغرات بشكل نظري

المحاضرة 11: الحماية والدفاع (Blue Team Basics)

- مراقبة الأنظمة
- تحليل Logs
- اكتشاف الهجمات
- أساسيات SOC

التدريب العملي: قراءة وتحليل Log

المحاضرة 12: مشروع تطبيقي نهائي

- بناء سيناريو شركة وهمية
- هجوم بسيط + دفاع
- تحليل النتائج
- كتابة تقرير أمني

مشروع: Mini SOC

مخرجات الدورة التدريبية:

بعد الانتهاء، سيكون المتدرب قادر على:

- فهم أساسيات الأمن السيبراني
- التعرف على أشهر الهجمات
- استخدام أدوات بسيطة
- فهم كيفية الدفاع عن الأنظمة
- الاستعداد لدورات متقدمة (Intermediate)