class JO

Network Security Fundamentals

مع المهندس: علي محمد الجازي

Network Security Fundamentals

تهدف دورة ❖❖Network Security Fundamentals❖❖ إلى تزويد المشاركين بالمعرفة والمهارات الأساسية اللازمة لفهم وتأمين الشبكات الحديثة ضد التهديدات والهجمات الإلكترونية المتزايدة.

تركّز الدورة على أحدث مفاهيم أمن الشبكات، وأساليب الحماية، وتقنيات اكتشاف الاختراقات، بالإضافة إلى تطبيقات عملية تساعد المتدربين على التعامل مع بيئات العمل الحقيقية بكفاءة واحترافية.

خلال الدورة سيتعرف المشاركون على مبادئ أمن المعلومات، وأنواع الهجمات الإلكترونية، وآليات تأمين الشبكات السلكية واللاسلكية، وإدارة الجدران النارية، وأنظمة كشف ومنع الاختراق، إضافة إلى أفضل الممارسات العالمية لحماية البيانات والبنية التحتية الرقمية.

تُعد هذه الدورة مناسبة للطلاب، ومسؤولي الشبكات، وفنيي الدعم التقني، وكل من يرغب ببناء أساس قوي في مجال أمن الشبكات والانطلاق نحو التخصصات الاحترافية في الأمن السيبراني.

محاور الدورة

1. مقدمة في أمن الشبكات

- مفهوم أمن المعلومات والشبكات
- عناصر الحماية الأساسية (Confidentiality, Integrity, Availability)
- أنواع التهديدات والهجمات الإلكترونية
- مبادئ إدارة المخاطر الأمنية

2. أساسيات الشبكات وعلاقتها بالأمن

- مراجعة مفاهيم الشبكات الأساسية
- بروتوكولات TCP/IP
- نموذج OSI وتأثيره على الأمن
- تحليل حركة البيانات داخل الشبكة

3. التهديدات والهجمات الإلكترونية

- Malware و Ransomware
- هجمات Phishing والهندسة الاجتماعية
- هجمات DoS / DDoS
- هجمات Man-in-the-Middle
- هجمات كلمات المرور والاختراق

4. تأمين الشبكات السلكية واللاسلكية

- حماية الشبكات المحلية LAN
- أساسيات Wireless Security
- بروتوكولات WPA2 و WPA3
- تأمين نقاط الوصول اللاسلكية

5. الجدران النارية وأنظمة الحماية

- مفهوم Firewall وأنواعه
- إعدادات الجدار الناري الأساسية
- أنظمة IDS و IPS
- التحكم بالوصول Access Control

6. التشفير وأمن البيانات

- أساسيات التشفير Encryption
- التشفير المتماثل وغير المتماثل
- الشهادات الرقمية و SSL/TLS
- حماية البيانات أثناء النقل والتخزين

7. الشبكات الافتراضية الخاصة VPN

- مفهوم VPN واستخداماته
- أنواع بروتوكولات VPN
- إعداد وتأمين الاتصال البعيد

8. إدارة الهوية والصلاحيات

- Authentication و Authorization
- سياسات كلمات المرور
- المصادقة متعددة العوامل MFA
- إدارة حسابات المستخدمين

9. مراقبة الشبكات والاستجابة للحوادث

- أدوات مراقبة الشبكات
- تحليل السجلات الأمنية Logs
- اكتشاف الحوادث الأمنية
- أساسيات الاستجابة للحوادث Incident Response

10. أفضل الممارسات الأمنية

- Security Policies
- النسخ الاحتياطي والتعافي
- تحديث الأنظمة وإدارة الثغرات
- التوعية الأمنية للمستخدمين

11. تطبيقات عملية ومختبرات

- إعداد جدار ناري عملي
- تحليل الهجمات واكتشافها
- تأمين شبكة صغيرة
- سيناريوهات محاكاة واقعية

مخرجات الدورة

بنهاية الدورة سيكون المتدرب قادراً على:

- **فهم أساسيات أمن الشبكات والأمن السيبراني**
- **التعرف على التهديدات والهجمات الشائعة**
- **تطبيق تقنيات الحماية الأساسية للشبكات**
- **إعداد أدوات الحماية والمراقبة**
- **التعامل مع الحوادث الأمنية الأولية بكفاءة**
- **بناء أساس قوي للتخصص في مجالات الأمن السيبراني المتقدمة**