مراقبة الشبكات وتوثيقها

د/ خالد السيد عبدالحق

د/ دعاء محمود عبدالعال

جدول المحتويات

في عصر التكنولوجيا المتسارع، أصبحت الشبكات بمختلف أنواعها عصب الحياة الحديثة، حيث تعتمد عليها المؤسسات والأفراد في نقل المعلومات وإدارة العمليات الحيوية. ومع هذا الاعتماد المتزايد على الشبكات، برزت الحاجة إلى مراقبتها بشكل دقيق وفعّال لضمان أمن البيانات وسلامة العمليات. تُعد مراقبة الشبكات أحد الركائز الأساسية في أمن المعلومات، حيث تساهم في الكشف عن التهديدات المحتملة، وتحليل حركة المرور، وحماية البنية التحتية للشبكات من الاختراقات والهجمات السيبرانية.

يهدف هذا الكتاب إلى تقديم دليل شامل ومتكامل حول مراقبة الشبكات وتوثيقها، بدءًا من المفاهيم الأساسية ووصولًا إلى التطبيقات العملية والتوجهات المستقبلية. نستعرض في الفصول الأولى المبادئ الأساسية لمراقبة الشبكات، بما في ذلك تعريفها وأهميتها، وأنواع أنظمة المراقبة المختلفة، سواء كانت سلبية أو نشطة أو استباقية. كما نناقش الفرق بين التصنت القانوني والتجسس غير القانوني، ونلقي نظرة على البروتوكولات الشبكية وكيفية تأثيرها على عمليات المراقبة.

يتطرق الكتاب أيضًا إلى تقييم الشبكات وتحديد نقاط المراقبة المناسبة، مع التركيز على تحليل البنية التحتية للشبكات السلكية واللاسلكية. نستعرض طرق جمع البيانات وتحليلها بشكل فعال، وكيفية استخدام هذه البيانات للكشف عن الأنشطة المشبوهة أو الهجمات السيبرانية. بالإضافة إلى ذلك، نناقش أهمية تأمين محطات المراقبة وإخفائها لحمايتها من الهجمات العكسية، مع شرح تقنيات التشفير وإخفاء العناوين.

في الفصول اللاحقة، نتعمق في تحليل حركة مرور البيانات، وطرق تصفية المعلومات المفيدة من الضوضاء المعلوماتية، وكيفية استخدام الذكاء الاصطناعي في تحليل البيانات. كما نستعرض الأدوات والبرمجيات المستخدمة في مراقبة الشبكات، سواء في بيئة ويندوز أو يونيكس، مع تقديم أمثلة تطبيقية لاستخدام هذه الأدوات في سيناريوهات حقيقية.