

مراقبة الشبكات وتوثيقها

د/ خالد السيد عبدالحق

د/ دعاء محمود عبدالعال

جدول المحتويات

٧	مقدمة
١١	الفصل الأول: مقدمة في مراقبة الشبكات وأساسياتها
١٣	تعريف مراقبة الشبكات وأهميتها في أمن المعلومات
١٥	أهداف مراقبة الشبكة ودورها في حماية البيانات
١٨	الفرق بين مراقبة الشبكة من الناحية المادية والمنطقية
٢١	أنواع أنظمة المراقبة
٢٥	الفرق بين التصنت القانوني والتجسس غير القانوني
٢٨	أساسيات بروتوكولات الشبكات وتأثيرها على المراقبة
٣١	لمحة عن الأدوات والتقنيات المستخدمة في مراقبة الشبكات
٣٥	الفصل الثاني: تقييم الشبكة وتحديد مواقع المراقبة
٣٧	طرق تقييم أداء الشبكة وتحديد نقاط الضعف
٤٠	أهمية تحديد مواقع تثبيت أجهزة الاستشعار (المراقبة)
٤٣	العوامل المؤثرة في اختيار نقاط المراقبة داخل الشبكة
٥٥	تحليل البنية التحتية للشبكات السلكية واللاسلكية
٥٩	طرق جمع وتحليل بيانات الشبكة بشكل فعال
٦٣	تأثير توجيه البيانات (Routing) على مراقبة الشبكة
٦٦	مقارنة بين تقنيات المراقبة في الشبكات المحلية (LAN) وشبكات المناطق الواسعة (WAN)
٧٧	الفصل الثالث: تصفية وتحليل حركة مرور المعلومات
٧٩	مفهوم حركة مرور البيانات (Traffic) وأهميتها في المراقبة
٨٣	طرق تصفية البيانات وتحديد الحزم المهمة
٨٧	الامتثال لقوانين التصنت الإلكتروني ومعايير الأمان
٩٣	تقنيات تحليل حركة المرور للكشف عن الأنشطة المشبوهة
٩٥	تحليل حركة المرور في شبكات TCP/IP و UDP
٩٨	الكشف عن الهجمات السيرانية من خلال تحليل البيانات
١٠١	تطبيقات الذكاء الاصطناعي في تحليل حركة المرور

- ١٠٥..... الفصل الرابع: أمن الشبكات وإخفاء محطات المراقبة
- ١٠٧..... أهمية تأمين محطات المراقبة لحمايتها من الهجمات العكسية
- ١١٤..... طرق إخفاء وجود محطة المراقبة على الشبكة
- ١١٧..... تقنيات إخفاء العناوين (MAC Address Spoofing)
- ١٢٠..... تشفير البيانات أثناء المراقبة لضمان الخصوصية
- ١٢٣..... استراتيجيات الحماية من الهجمات العكسية والتطفل
- ١٢٦..... كيفية كشف محاولات الاختراق والتلاعب ببيانات الشبكة
- ١٢٩..... دور الجدران النارية (Firewalls) وأنظمة كشف التسلل (IDS) في تعزيز الأمان
- ١٣٣..... الفصل الخامس: تحليل المحتوى المناسب لحركة مرور المعلومات
- ١٣٦..... الفرق بين البيانات المفيدة والضوضاء المعلوماتية
- ١٣٩..... طرق تصنيف وتحليل البيانات الملتقطة
- ١٤٢..... تقنيات الفلتر المتقدمة لتحديد المعلومات ذات الأهمية
- ١٤٥..... تحليل سجلات الدخول والخروج من الشبكة
- ١٤٧..... استخراج وتحليل الرسائل الإلكترونية والملفات المنقولة عبر الشبكة
- ١٥١..... أدوات تحليل المحتوى النصي والوسائط المتعددة
- ١٥٣..... دراسة حالات لتوضيح كيفية تحليل البيانات بشكل فعال
- ١٥٩..... الفصل السادس: تكوين ومراقبة الشبكات في بيئة ويندوز
- ١٦١..... نظرة عامة على أدوات مراقبة الشبكة في ويندوز
- ١٦٣..... إعداد واستخدام نظام التعرف الآلي لمراقبة الشبكة
- ١٦٦..... تحليل والتحقق من البيانات التي يتم جمعها في بيئة ويندوز
- ١٦٩..... تثبيت وضبط برامج المراقبة في أنظمة ويندوز
- ١٧٠..... فحص استخدام المنافذ المفتوحة (Port Scanning) في ويندوز
- ١٧١..... استخدام أوامر Windows PowerShell في تحليل الشبكات
- ١٧١..... مقارنة بين أدوات المراقبة في Windows وLinux
- ١٧٣..... الفصل السابع: برمجيات تحليل الشبكات في بيئة ويندوز ويونيكس
- ١٧٥..... مقدمة عن الأدوات المستخدمة في تحليل الشبكات

١٧٧.....	تثبيت واستخدام برنامج Wireshark لتحليل بروتوكولات الشبكات
١٨١.....	برنامج WinPcap وآلية عمله في التقاط وتحليل الحزم
١٨٤.....	تحليل الشبكات في بيئة يونيكس باستخدام TCPDump
١٨٦.....	أدوات إضافية مثل Nmap و Ettercap وفوائدها
١٨٧.....	كيفية تحليل البروتوكولات المختلفة مثل HTTP و DNS و FTP
١٨٨.....	دراسة تطبيقية لاستخدام أدوات تحليل الشبكات في سيناريوهات حقيقية
١٩٣.....	الفصل الثامن: تطبيقات عملية في مراقبة الشبكات
١٩٥.....	دراسة حالات واقعية لمراقبة الشبكات في الشركات والمؤسسات
١٩٨.....	تحليل بيانات حركة المرور لاكتشاف محاولات الاختراق
٢٠٠.....	كيفية كشف البرمجيات الخبيثة باستخدام تقنيات المراقبة
٢٠٣.....	تطبيقات مراقبة الشبكات في أنظمة الحوسبة السحابية
٢٠٦.....	التعامل مع الحوادث الأمنية والاستجابة لها
٢٠٩.....	تحليل البيانات الضخمة في مراقبة الشبكات باستخدام تقنيات الذكاء الاصطناعي
٢١٢.....	مستقبل مراقبة الشبكات في ظل التطورات التكنولوجية الحديثة
٢١٧.....	الفصل التاسع: القوانين والأخلاقيات في مراقبة الشبكات
٢١٩.....	نظرة عامة على القوانين الدولية المتعلقة بمراقبة الشبكات
٢٢٢.....	الفروق بين القوانين في الدول المختلفة حول التصنت الإلكتروني
٢٢٥.....	المبادئ الأخلاقية لمراقبة الشبكات وضوابط الاستخدام
٢٢٨.....	تأثير المراقبة على خصوصية الأفراد وحقوق المستخدمين
٢٣٢.....	متطلبات الامتثال التنظيمي مثل (PCI-DSS ، HIPAA ، GDPR)
٢٣٥.....	مسؤولية الشركات تجاه تأمين البيانات واحترام الخصوصية
٢٣٩.....	حدود الاستخدام القانوني لمراقبة الشبكات في المؤسسات
٢٤٣.....	الفصل العاشر: التوجهات المستقبلية في مراقبة وتحليل الشبكات
٢٤٥.....	تقنيات الذكاء الاصطناعي والتعلم الآلي في تحليل البيانات
٢٤٨.....	دور الحوسبة السحابية في مراقبة الشبكات عن بُعد
٢٥١.....	تأثير شبكات الجيل الخامس (5G) على تحليل حركة المرور

- ٢٥٥ أتمتة عمليات المراقبة والاستجابة للحوادث الأمنية
- ٢٥٦ دور تقنية البلوكشين في تعزيز أمان الشبكات
- ٢٥٨ تحديات المستقبل في مجال أمن المعلومات ومراقبة الشبكات
- ٢٦٠ التوصيات المستقبلية لتطوير أنظمة مراقبة أكثر كفاءة

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 وفعال 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 وإخفاء حمايتها من الهجمات العكسية، مع شرح تقنيات التشفير وإخفاء العناوين.

في الفصول اللاحقة، نتمتع 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.